

FortiWLC (SD)

設定ガイド

Rel 8.2.4



2016 年 9 月

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet® および特定のその他のマークは、Fortinet, Inc. の米国およびその他の管轄区域内における登録商標です。また、その他本書に記載されているフォーティネット関連の名称もフォーティネットの登録商標 / 慣習法に基づく商標の可能性があります。その他の製品名または社名は各社の商標です。本書に記載の性能およびその他の測定基準は、最適条件のもと、社内ラボテストで得られたものであり、実際のパフォーマンスおよびその他の結果は変動する可能性があります。ネットワーク変数、ネットワーク環境やその他の条件の違いにより、パフォーマンス結果が異なる場合があります。本書はフォーティネットによる拘束力のある約束を示すものではありません。また、フォーティネットは、フォーティネットの法律顧問が署名した書面による契約を締結し、指定の製品が明示的に指定されたパフォーマンス評価基準に準じたパフォーマンスを示すことを買い手に対して明示的に保証した場合を除き、明示的か黙示的かを問わず、一切の責任を負わないものとします。また、上記に該当する場合には、書面の契約書で明示的に指定されたパフォーマンス評価基準についてのみ、フォーティネットが法的に拘束されるものとします。上記の保証は、フォーティネット社内の実験施設でのテストと同じ理想的な条件下でのパフォーマンスに限られるものとします。いかなる場合でも、フォーティネットは、将来の成果物、機能、または開発に関して一切約束を行わないものとします。また、状況に変化が生じ、本書の将来の見通しに関する記述が正確ではない可能性があります。フォーティネットは、明示的か黙示的かを問わず、本書に記載されている誓約、表明、保証をすべて完全に放棄します。フォーティネットは、予告なく本書を変更、修正、移譲する権利、あるいはその他の形態で改訂する権利を有します。

サポート

サポートが必要な場合には、フォーティネットのカスタマ サービス & サポート (24 時間対応、電話番号: +1 408-542-7780) または [お近くの連絡先](#) までお問い合わせください。サポート ポータル (<https://support.fortinet.com/>) をご利用いただくこともできます。

フォーティネットのカスタマ サービス & サポートは、エンド ユーザと販売パートナーからの以下のお問い合わせに対応しています。

- テクニカル サポート
- ソフトウェア アップデート
- 部品交換サービス

フォーティネット製品ライセンス契約 /EULA および保証条項



WiFi ネットワークをセキュリティで確実に保護するために、フォーティネットハードウェア（コントローラおよびアクセスポイント）は、フォーティネットによって開発された専用のファームウェアでのみ動作するように設計されています。認定されたフォーティネットアクセスポイントのみがフォーティネットコントローラに構成できます。また、逆も同じです。サードパーティ製のアクセスポイントおよびソフトウェアは、フォーティネットハードウェアで構成できません。

商標と著作権に関する宣言

Fortinet®, FortiGate®, FortiGuard® は、Fortinet, Inc. の登録商標であり、他のフォーティネット名もフォーティネットの登録済み商標または商標である可能性があります。他の製品名または企業名は、それぞれの所有者の商標である可能性があります。Copyright © 2015 Fortinet, Inc., All Rights reserved. 本書の内容および条項については、事前の通知が行われることなく、フォーティネットによって変更されることがあります。米国で 1976 年に発行された著作権保護法で規定されているように、Fortinet, Inc. の許可なく、本文書の一部を、どのような形態または手段であっても複製すること、または翻訳、変容、または改作などの派生物を作成するために使用することは禁止されません。

製品ライセンス契約

本契約の当事者は、お客様、エンド顧客、および (i) 製品を米国国内で購入された場合は Fortinet, Inc. または (ii) 米国国外で購入された場合は Fortinet Singapore Private Limited のいずれか（以降、「フォーティネット」）です。以降の法律契約（「本契約」または「本 EULA」）をよくお読みください。フォーティネットの製品およびすべての更新プログラム、さらにはフォーティネットによって同梱されているハードウェアアプライアンス、ソフトウェアおよびファームウェア、フォーティネットによって販売されているスタンドアロンのソフトウェア製品（総称して「製品」）を使用またはインストールすると、お客様は本契約の条項に同意したとみなされます。また、フォーティネットは、その自由裁量において、これらの製品の機能が追加された、または更新されたバージョンを発行できる権利を有し、将来にわたって追加または更新できるものとします。フォーティネットは、フォーティネットの法務顧問により署名付き書面で明示的に同意されている場合を除いて、あらゆる注文書、引き渡し指示書、注文請書、他の類似文書、および書面または口頭でのコミュニケーションのあらゆる追加規定および / または競合する規定に拘束されないものとします。本契約のすべての条項に同意されない場合、インストールプロセスを開始したり、製品を使用したりすることは禁止されます。本契約の条項に同意されない場合、即座に、および製品の受取日から 5 暦日以内に、フォーティネットの法務チーム (LEGAL@FORTINET.COM) に本契約の変更を書面にて依頼してください。

1. ライセンスの許諾。

本契約は、販売契約ではなく、お客様とフォーティネットとの間のライセンスです。本契約で使用されている「ソフトウェア」という用語には、フォーティネットのアプライアンスと共に、または組み込まれてお客様に提供されているすべてのフォーティネットおよびサードパーティのフォー

ムウェアとソフトウェア、およびフォーティネットによってお客様に提供されているスタンダードソフトウェアが含まれます。ただし、フォーティネットの製品に含まれているオープンソースソフトウェアは除きます。オープンソースソフトウェアの詳細については、セクション 15 で説明されます。さらに、「ソフトウェア」という用語には、お客様の選択によりフォーティネットによってお客様に提供される、あらゆる付属文書、ソフトウェアまたはファームウェアの更新バージョンまたは拡張バージョンが含まれます。フォーティネットは、お客様が内部的なビジネス目的のためだけにソフトウェアを使用することを可能にする、譲渡不能（以降のセクション 5「譲渡」およびセクション 15「オープンソースソフトウェア」に記載されている場合を除く）、非排他的、および失効可能（本契約の条項をお客様が遵守しなかった場合または該当する製品の対価がフォーティネットに適切に支払われなかった場合）のライセンスを、お客様に許諾します（ビジネスの本質的な目的がマネージドサービスプロバイダーのサービスをお客様のエンド顧客に提供することである場合、本契約に記載されている他の制約の下で、FortiGate およびサポート対象ハードウェアアプライアンスに内蔵されているソフトウェアを使用してそれらのサービスを提供できます）。本ライセンスは、本契約に記述されている条項およびフォーティネット文書のさらなる制約に従って、(i) フォーティネットアプライアンス上で、(ii) ブレード、CPU、またはデータベースの場合、フォーティネットがソフトウェアをインストールした単一のブレード、CPU、またはデータベース上で、(iii) スタンダードソフトウェアの場合、ソフトウェアの設計対象となっているオペレーティングシステムの適切にライセンスが許諾されているコピーが動作している単一のコンピュータ上、またはブレード、CPU、またはデータベースの場合、単一のブレード、CPU、またはデータベース上で、ソフトウェアの使用を許可します。明確にするために言い換えると、本契約の別段の定めにかかわらず、適用できる場合は、ブレード、CPU、またはデータベースにインストールされるソフトウェアのすべてのライセンスは、単一ブレード（同一シャーシにインストールされる可能性のある複数のブレードに対してではなく）、単一 CPU、または単一データベースに対して許諾されます。ソフトウェアは、どのフォーティネットアプライアンスであっても、その一時メモリ (RAM) にロードされると、「使用されている」とみなされます。このセクション 1 で許諾される特定の制限付きライセンス権利以外に、ソフトウェアに対するライセンス権利を受け取らないことに、お客様は同意します。

2. 使用上の制限。

お客様は、次の (a) ~ (d) の項目を試行してはいけません。また、お客様が企業である場合、従業員またはコントラクターが試行しないようにする責任があります。(a) ソフトウェアの変更、翻訳、リバースエンジニアリング、デコンパイル、逆アセンブル、ソフトウェアに基づく派生物の作成、サブライセンス、または配布。(b) いかなる形態であっても、第三者に対するソフトウェア権利の貸し出しまたはリース、または他のいかなる形態であっても、第三者がソフトウェアを利用できるようにまたはアクセスできるようにすること。(c) セクション 5 に記載されている場合を除いて、他の個人または組織への権利の割り当てまたはサブライセンスの譲渡。(d) ソフトウェア、製品、およびコンテナ上のいずれかの通知、ラベル、またはマークの除去。

3. 専用権利。

ソフトウェアおよびお客様によって作成されたあらゆるコピーに対するすべての権利、権原、利益、およびすべての著作権は、フォーティネットに引き続き属します。ソフトウェアまたは他の製品の知的所有権に対するあらゆる権原はお客様に譲渡されず、前掲のセクション 1「ライセンスの許諾」で明示的に記載されている特定のライセンスを除いてソフトウェアまたは他の製品をお客様は取得しないことに、お客様は同意します。お客様は、フォーティネットのすべての機密情報を秘匿し、

そのような情報はフォーティネットが開示した目的でのみ使用することに同意します。

4. 期間と終了。

評価およびベータライセンスの場合、または評価 / ベータ、他の契約、または注文書に従ってライセンスの期間が制限されているライセンスの場合を除いて、ライセンスの期間は、ソフトウェアに関するフォーティネットの著作権の期間です。お客様が本契約のいずれかの条項を侵害するか遵守しなかった場合、フォーティネットは本契約およびここに記載されているライセンスおよび他の権利を、お客様に通知することなく即座に終了することがあります。かかる終了時に、ソフトウェアおよびあらゆる製品の使用を停止し、フォーティネット文書のすべてのコピーを粉砕するか、すべての対象物をフォーティネットに返却することに、お客様は同意します。本契約者の本規定は、セクション 1「ライセンスの許諾」で許諾されているライセンスを除いて、終了後も有効性を保ちます。

5. 譲渡。

お客様が製品に関するフォーティネットの契約または認定再販業者または代理店である場合、お客様は次の条件の下で、1 人のエンドユーザーにソフトウェアを使用期限なしで譲渡できます。ただし、フォーティネットによって書面で特に同意された場合を除いて貸し出しまたはリースすることはできません。(i) お客様は、自身の顧客およびエンドユーザーが本契約のコピーを受け取り、本条項に確実に拘束されるようにします。また、お客様は製品またはソフトウェアを販売した場合に、本契約の条項にかかるエンドユーザーに強制することに同意します。(ii) お客様は常に、該当するすべての米国輸出管理法令を遵守します。(iii) 製品をお客様から購入したエンドユーザーが本契約の条項に同意せず、したがって本契約に従って製品を返却したい場合、お客様はエンドユーザーがお客様に支払った料金を払い戻すことに同意します。さらに、お客様が製品の非認定再販業者である場合、製品またはソフトウェアを販売することは承認されません。ただし、それにもかかわらず、製品またはソフトウェアを販売する場合、本契約に記載されている制限および義務、さらには次の各項に拘束されることにお客様は同意します。(i) 自身の顧客およびエンドユーザーが本契約のコピーを受け取り、本条項の制限と義務に確実に拘束されるようにします。(ii) かかる顧客および / またはエンドユーザーに本契約の制限と義務を強制します。(iii) 該当するすべての米国輸出管理法令および他のすべての該当する法令を遵守します。(iv) 製品をお客様から購入したお客様の顧客および / またはエンドユーザーが本契約の制限と義務に同意せず、したがって本契約に従って製品を返却したい場合、お客様は顧客および / またはエンドユーザーがお客様に支払った料金を払い戻します。本契約の別段の定めにかかわらず、代理店、再販業者、および他のフォーティネットパートナーは、(a) フォーティネットの代理人ではなく、(b) どのような形態でもフォーティネットを拘束することはできません。

6. 限定保証。

フォーティネットは、製品をフォーティネット、認定再販業者、または認定代理店から最初に購入し、かかる製品の対価を支払った単一のエンドユーザーとなる個人または企業に対してのみ、その製品の本限定保証を許諾します。本保証は、フォーティネットのサポート Web サイト (<https://support.fortinet.com>) またはフォーティネットによって提供されているその他の Web サイトで登録されている製品、またはフォーティネットのポリシーに従って

保証が開始される製品に対してのみ有効です。これ以降で説明される保証期間は、<http://www.fortinet.com/aboutus/legal.html> またはフォーティネットによって提供されているその他の Web サイトに掲載されているフォーティネットのポリシーに従って開始されます。フォーティネットの代理店または再販業者は、製品がフォーティネットから最初に出荷された日付を明確にエンドユーザーに伝える責任があります。エンドユーザーは、製品の購入先当事者から最初の出荷日付に関する情報を取得し理解する責任を持ちます。保証に関するすべてのお問い合わせは、保証期間が

期限切れとなる前にフォーティネットに書面で発行する必要があります。それ以外の場合、かかるお問い合わせは完全に放棄されます。フォーティネットは、あらゆるベータ製品、寄贈製品、または評価製品、エンドユーザーによってフォーティネットから直接に購入されていないあらゆる予備部品、またはあらゆるスタンダードソフトウェアに対して保証を提供しません。フォーティネットは、特に断りのない限り予備部品を含めて、製品のハードウェア部分（「ハードウェア」）が、機能仕様と比較して組み立て上の欠陥がないことを保証します。本保証は、次に示す製品タイプに適用可能な期間（「ハードウェア保証期間」）において有効です。（a）予備部品、電源、およびアクセサリを除くハードウェア（FortiAP および Meru AP の室内 Wi-Fi アクセスポイントハードウェアアプライアンス製品、および FortiSwitch-5000 シリーズを除く FortiSwitch ハードウェアアプライアンス製品に限定（両方とも予備部品、電源、およびアクセサリを除く））については、365 日の限定保証です。ここに記載されている保証は、前掲の保証期間の開始日から公表されている製品のエンドオブライフ日付以降 5 年間です。（b）予備部品、電源、およびアクセサリについては、90 日のみの限定保証です。フォーティネットは、欠陥のあるハードウェアに関して、最初の所有者に対して無償でハードウェアの修理または交換を行う義務のみを負います。かかる義務には、輸送、作業、取り外し、インストール、再構成、または返却および梱包に関する費用は含まれず、それらに関してフォーティネットは一切の義務を負いません。かかる修理または交換は、フォーティネット指定の認定フォーティネットサービス施設でフォーティネットにより行われます。交換ハードウェアが、新品、あるいは同じ型、モデル、または部品であるとは限りません。フォーティネットは、その自由裁量において、欠陥ハードウェアに関してすべての機能面でフォーティネットが実質的に同等（またはそれ以上）であると合理的に判断した再調整済み製品を使用して、欠陥ハードウェア（またはその部品）を交換することがあります。修理済みまたは交換済みハードウェアのハードウェア保証期間は、残余ハードウェア保証期間または修理済みまたは交換済みハードウェアの到着日から 90 日の長い方です。フォーティネットは、その合理的な自由裁量において、欠陥製品を修理できない、または欠陥ハードウェアを修理または交換することが実践的ではないと判断した場合、欠陥ハードウェアの最初の購入者によって支払われた金額を、欠陥ハードウェアがフォーティネットに返却された際に払い戻します。フォーティネットにより交換されたすべての欠陥ハードウェア（またはそれらの部品）または購入価格が払い戻された欠陥ハードウェアは、交換または払い戻しの時点でフォーティネットの資産となります。フォーティネットは、ハードウェア製品と一緒に最初に出荷されたソフトウェアが、認定ハードウェアに適切にインストールされ、その文書の記述に従って運用された場合に、該当する文書の記述に従って 90 日間（「ソフトウェア保証期間」）、出荷時最新のフォーティネットのソフトウェアに対する仕様に実質的に準拠することを保証します。フォーティネットの義務は、準拠していないソフトウェアの修理またはフォーティネットの機能仕様に実質的に準拠する交換ソフトウェアの提供のみです。かかる義務には、輸送、作業、取り外し、インストール、再構成、または返却および梱包に関する費用は含まれず、それらに関してフォーティネットは一切の義務を負いません。フォーティネットにより書面で同意されている場合を除いて、保証交換ソフトウェアは、最初にライセンスが許諾されたユーザーに対してのみ提供され、フォーティネットによって許諾されているラインセスのソフトウェアに関する条項遵守の対象になります。ソフトウェア保証期間は、保証交換ソフトウェアの到着日から 90 日間に延長されます。フォーティネットは、その合理的自由裁量において、非準拠ソフトウェアを修理できない、または非準拠ソフトウェアの修理または交換が実践的ではないと判断した場合、非準拠ソフトウェアについて最初にライセンスが許諾されたユーザーによって支払われた金額を、非準拠ソフトウェア（およびそのすべてのコピー）がフォーティネットに最初に返却された際に払い戻します。払い戻しが行われたソフトウェアに関して許諾されていたライセンスは、払い戻しが行われた際に即座に自動的に失効します。前掲のハードウェアおよびソフトウェアの保証に関して、「機能仕様」という用語は、フォーティネットによって認定および公表されており、本契約の本セクション 6 で参照されている機能仕様であるとかかる仕様で明示的に宣言されている仕様のみを意味します。かかる仕様がソフトウェアまたはハードウェアに付随してお客様に提供されていない場合、かかるソフトウェアに対する保証は一切提供されません。

7. その他の保証および制約の否認。

前掲のセクション 6 で指定されている限定保証の場合を除いて、製品とソフトウェアはあらゆる種類の保証を伴わずに「そのままの状態」で提供されます。かかる保証には、あらゆる黙示的保証、商品性の黙示的または明示的保証、または特定の用途への適合性および非侵害の保証が含まれますが、これらの保証に限定されるものではありません。製品が販売されているいずれかの地域において黙示的保証が否認されない場合、かかる黙示的保証の期間は、製品がフォーティネットから最初に出荷された日付から 90 日に制限されます。本契約で提供されている限定保証の下で明示的に対象となっている場合を除いて、製品の品質、選択、および実行に関する全体的なリスクは、製品の購入者に帰属します。本契約の別段の定めにかかわらず、前掲のハードウェア保証期間は特定のフォーティネット製品に適用されません。かかる製品には FortiToken があり、保証期間はフォーティネットの施設から出荷された日から 365 日です。また、ソフトウェア保証は、Fortigate-ONE および VDOMNET ソフトウェアなどの特定のフォーティネット製品に適用されません。ここに、お客様は、いずれのベンダーも完全なセキュリティを保証できないことを認めて同意します。本契約のいずれの内容も、セキュリティの保証を示唆するとみなしてはいけません。前掲のセクション 6 の保証は、ソフトウェア、製品、またはソフトウェアの使用が承認されているその他のいずれかの機器が、次の条件のいずれかに当てはまる場合、適用されません。(a) フォーティネットまたはフォーティネットの認定代理人以外によって変更されている、(b) フォーティネットによって提供されている指示に従わずに、インストール、運用、修復、最新版に更新、または保守されている、(c) 異常な物理的または電気的ストレス、誤使用、過失、または事故にさらされている、(d) ベータ、評価、寄贈、テスト、またはデモの目的でライセンスが許諾されているか、フォーティネットが購入費用またはライセンス料金を請求していない。エンドユーザーは、ソフトウェアまたは製品がベータ、テスト、評価、または寄贈の目的で提供されているか、または無料で提供されている場合、かかるソフトウェアまたは製品には、システム障害、データ損失、

および他の問題を引き起こす可能性のあるバグまたはエラーが含まれている可能性があることを認めて同意します。また、エンドユーザーは、かかるソフトウェアまたは製品が、いかなる保証も付随せずに「そのままの状態」で提供され、フォーティネットはいかなる保証および責務からも免責されることに同意します。エンドユーザーがソフトウェアまたは製品の評価版またはベータ版を使用できるのは、フォーティネットによって書面で同意されている場合を除いて、最初に出荷されてから 30 日間です。

8. 準拠法。

本契約またはフォーティネットの限定保証に関して発生する紛争については、法原則の抵触と関係なく、米国カリフォルニア州法に準拠します。本契約またはフォーティネットの限定保証に関して紛争が発生した場合は、各当事者は、カリフォルニア州サンタクララ郡の連邦および州の裁判所の管轄権に付託するものとします。

9. 責任の制限。

法律によって許される最大の限度で、本契約の別段の定めにかかわらず、フォーティネットは、製品またはサービスの使用機会の損失または次に示すあらゆる種類の損害に関して、いかなる契約、過失、不法行為、無過失、侵害、またはその他の法理論または衡平法理論の責任も負わないこととします。かかる損害には、製品の使用による、保証サービスに関連して、または前掲のセクション 6 の限定保証のいかなる侵害により発生した直接的、特別的、付随的、または結果的な損害であるかどうかに関係なく、信用の損失、利益の損失、機会の損失、リスクの高いアクティビティに関連する製品またはサービスの使用に関連する損失または損害、取り外しとインストールの料金と費用、人的損害または不動産に対する損害、業務停止、コンピュータの障害または異常動作、コン

コンピュータのセキュリティ侵害、コンピュータウイルスへの感染、保証サービスに関連してフォーティネットに返却された製品に含まれていた、格納されていた、または製品に統合されていた情報またはデータの損失が含まれますが、これに限定されるものではありません。かかる損害の可能性についてフォーティネットが助言を得ていたとしても責任は負わないこととします。限定保証の侵害に対する救済手段は、特に前掲のセクション6に記載されているように、欠陥のある、または仕様に準拠していない製品の修理、交換、または払い戻しのみです。

10. 輸入 / 輸出要件 : FCPA 準拠。

お客様には、製品が米国輸出管理規制および他の輸出入関連法の対象である可能性があることが通知されます。米国の法律および規制に反する行為は禁止されています。お客様は、米国および他の政府により発行され、製品に加えて、エンドユーザー、最終用途、および宛先への制限に適用されるすべての国際法および国内法に準拠することに同意します。米国輸出規制の詳細については、www.bis.doc.gov を参照してください。フォーティネットは、輸出入に関する必要な認証をお客様が取得できないことに

関して、いかなる責任も負いません。また、いずれかの輸出入規制違反が合理的に疑われる場合には、出荷、サービス、およびサポートを終了または一時停止する権利をフォーティネットは留保します。米国商務省産業安全保障局およびその他のいかなる政府機関もお客様に対して制裁措置を発行していないこと、およびお客様の輸出権利の一時停止、失効、または拒否を行っていないことを、お客様は表明します。米国政府によって規制または特定の文書でのライセンスによって承認されている場合を除いて、核兵器、生物化学兵器、またはミサイル技術に関連して使用したり、これらの使用が予見される第三者に譲渡したりしないことに、お客様は同意します。また、製品の直接的または間接的な輸出、輸入、または転送を、かかる輸出、輸入、転送、または使用に関する司法権を持つその他のあらゆる政府機関の法律または規制に反して行わないことに、お客様は同意します。さらに、米国海外汚職行為防止法およびその他のすべての適用可能な法律のすべての要件を理解し遵守することに同意することを、お客様は表明します。ペータ、テスト、評価、寄贈、または無料の製品および / または関連するサービスの場合、次の (a) ~ (c) の項目について、お客様はフォーティネットに対して同意、表明、および保証します。(a) 製品および / またはサービスの受け取りは、すべてのポリシーに準拠しており、かかる製品および / またはサービスに関して必要なすべての承認をお客様は取得しています。(b) 製品および / またはサービスは、フォーティネットが現在のビジネスを維持するため、または新しいビジネス機会のための見返りとして提供されていません。(c) 製品および / またはサービスは、いずれの政府機関、代表者、または関連組織の利益のために受け取っておらず、かかる組織に譲渡されません。

11. 米国政府がエンドユーザーである場合。

ソフトウェアおよび付随する文書は、それぞれ DFAR セクション 227.7202 および FAR セクション 12.212 に従って「商用コンピュータソフトウェア」および「商用コンピュータソフトウェア文書」としてみなされます（該当する場合）。米国政府によって行われるソフトウェアおよび付随する文書の使用、変更、複製、引き渡し、実行、表示、または開示は、本契約の条項によってのみ統治され、本契約およびその後継文書によって明示的に許可されている場合を除いて禁止されます。

12. 納税義務。

お客様は、この取引で随時課せられる販売税または使用税の支払いに対して責任があることに同意します。

13. 総則。

前掲のセクション5「譲渡」で特に許可されているか要求されている場合を除いて、フォーティネットの事前の書面による同意なしに、本契約の割り当て、または本契約支配下の権利または義務の譲渡を行わないことにお客様は同意します。本契約は、当事者の承継者および許可された譲受者に対して拘束力があり、また本契約の利益はこれらの者に帰属します。国際物品売買契約に関する国際連合条約は、明示的に除外されます。本契約および他のフォーティネット契約は、両当事者の利益となることを目的とする署名された同意を明示的に参照する書面によってのみ改正または補完されます。または、本契約の場合、前掲のセクション1の前の前置きで明示的に提供されているように、本契約の別段の定めにかかわらず、前掲のセクション1の前の前置きで明示的に提供されているように本契約が改正または更新される場合を除いて、フォーティネットに対して拘束をもたらしあらゆる改正または他の同意は、フォーティネットの法務顧問の署名が必要になります。権利の履行または不履行は、権利放棄を主張される側の一方当事者が書面により署名したものでない限り、権利放棄とみなされることはなく、権利放棄としての効力也没有。本契約に履行できない部分がある場合、かかる部分は本契約の範囲で許される限り最大限の履行を強制されるものであり、本契約の残りの部分は完全に強制され、効力を持ちます。お客様は、本契約を読み、内容を理解し、本契約の条項により拘束されることに合意します。

14. プライバシー。

お客様の個人情報に関するフォーティネットの収集、使用、および転送のポリシーの詳細については、フォーティネットの Web サイト (<http://www.fortinet.co.jp/aboutus/privacy.html>) で提供されている「Fortinet プライバシーポリシー」を参照してください。

15. オープンソースソフトウェア。

フォーティネットの製品には、GNU 一般公衆利用許諾契約書、バージョン 2 (1991 年 6 月版) (「GPL」) または GNU 劣等一般公衆利用許諾書、バージョン 2.1 (1999 年 2 月版) (「LGPL」)、または他の権利とともにユーザーにモジュールまたはモジュールの一部の使用、コピー、変更、および再配布を許可する他のオープンソースソフトウェアライセンスの下で、ユーザーにライセンス (またはサブライセンス) されており、帰属の開示やソースコードへのアクセスを要求することもあるソフトウェアモジュール (「オープンソースコード」) が含まれていることがあります。GPL は、GPL の下でライセンスされるいずれのオープンソースソフトウェアも、不特定多数のユーザーに実行可能バイナリ形式で配布され、かかるユーザーがソースコードも利用できるようにすることを要求しています。GPL の下でライセンスされるいずれのオープンソースソフトウェアも、ソースコードは本 CD に含まれているか、またはダウンロードパッケージとして利用できます。いずれかのオープンソースソフトウェアライセンスが、オープンソフトウェアプログラムの使用、コピー、または変更に関して本契約で許可されるよりも広範な権利をフォーティネットが提供することを要求する場合、かかる権利は、本契約の権利や制約よりも優先されます。フォーティネットは、標準の配布費用が反映された料金の下で、変更されたソフトウェアモジュールの完全にコンピュータが読み取り可能なコピーを提供します。完全にコンピュータが読み取り可能なコピーを取得する必要がある場合は、かかる要求の記載された文書に 25.00 米ドルの小切手を添えて、General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA 宛てに送付してください。変更済みソフトウェアモジュールを受け取るには、次の情報も書面に記載されている必要があります。(a) 名前、(b) 住所、(c) 電話番号、(d) 電子メールアドレス、(e) 購入済み製品 (該当する場合)、(f) 製品のシリアル番号 (該当する場合)。すべてのオープンソースソフトウェアモジュールは、無料でライセンスが許諾されます。適用可能な法律で許可される範囲において、かかるモジュールに保証は一切提供されません。著作権保有者は、これらのソフトウェアモジュールを「そのままの状態」で、明示的にも黙示的にも一切の保証なく提供します。オープンソースソフトウェアの著作権保有者は、いかなる場合も、お客様の損害に対して責任を負いません。

かかる損害には、ソフトウェアモジュールの使用または使用不可に起因する特別損害、付随的損害、または結果損害が含まれます。かかる損害の可能性についてかかる所有者が助言を得ていたとしても責任を負わないこととします。本ライセンスの完全コピーは、フォーティネットの特定の製品に適用可能な追加のオープンソースソフトウェアライセンス開示および第三者ライセンス開示を含めて、フォーティネットの法務部門(legal@fortinet.com)に問い合わせることにより入手できます。

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the

whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it..Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3.You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it.For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable.However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4.You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License.Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5.You are not required to accept this License, since you have not signed it.However, nothing else grants you permission to modify or distribute the Program or its derivative works.These actions are prohibited by law if you do not accept this License.Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions.You may not impose any further restrictions on the recipients' exercise of the rights granted herein.You are not responsible for enforcing compliance by third parties to this License.

7.If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all.For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices.Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8.If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded.In such case, this License incorporates the limitation as if written in the body of this License.

9.The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time.Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.Each version is given a distinguishing version number.If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10.If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make

exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library".The executable is therefore covered by this License.Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work.(Executables containing this object code plus portions of the Library will still fall under Section 6.)Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6.Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6.As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications.You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License.You must supply a copy of this License.If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License.Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.(It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library.A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.For an executable, the required form of the "work that uses the Library" must

include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this

License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

目次

サポート	2
本ガイドについて	29
対象読者	29
その他の関連情報	29
Web リソース	30
フォーティネットのマニュアル	30
表記規則	30
構文表記	31
お問い合わせ	32
カスタマ サービス & サポート	32
CLI の概念	33
CLI の開始	33
CLI コマンド モード	34
ユーザ EXEC モード	34
特権 EXEC モード	34
グローバル設定モード	35
コマンド ラインのみのコマンド	35
コマンドの省略形	37
コマンドの no フォームと default フォームの使用	38
ヘルプの表示	38
コマンド ヒストリの使用	39
コマンド ヒストリ バッファのサイズのセット	40
コマンドの呼び出し	40
コマンド ヒストリ機能の無効化	41
show コマンドの出力における語句の検索	41

CLI プロンプトのカスタマイズ	41
デフォルトの CLI プロンプト	41
CLI プロンプトをカスタマイズするためのコマンド	42
端末特性の操作	42
端末設定の表示	42
端末画面の長さとの幅のセット	42
セッションの終了	43
Web UI の概念	45
GUI と CLI コマンドの関係	46
ブラウザ	48
Internet Explorer のキャッシュ設定	49
Network Manager とは	50
システム ファイルの管理	53
CFS について	53
ローカル ディレクトリでの作業	54
ディレクトリとファイルの情報の表示	54
異なるディレクトリへの変更	55
Web UI によるファイルの管理	56
AP Init Script	56
Diagnostics	57
Image	58
syslog	59
設定ファイルの操作	60
現行の設定の変更	60
起動設定の変更	61
システム ファイルの操作	61
ネットワーク サーバのファイルの操作	61

リモート ファイルの転送	62
リモート サーバへのファイルのコピー	62
リモート サーバのディレクトリ内容の表示	62
リモートのユーザ名とパスワードの設定	63
システム イメージのアップグレード	63
ファイル システム コマンドのまとめ	64
パッチのアップグレード	66
Web UI の使用	66
CLI の使用	69
システムの管理	73
セットアップ時のコントローラの基本パラメータの設定	73
Web UI からのコントローラ パラメータの設定	74
Web UI による UDP ブロードキャストの設定	75
CLI からのコントローラ パラメータの設定	75
システムとシステム パスワードの CLI からのリセット	75
ワイヤレス クライアントの CLI からのコントローラへのアクセスの制限	76
QoS ルールによる有線クライアントからコントローラへのアクセスの制限	77
CLI からの UDP ブロードキャストの設定	79
CLI からの時間サービスの設定	79
CLI コントローラ インデックスの設定	80
システム ライセンスの設定	80
CLI によるライセンスの設定	81
Web UI によるライセンスの設定	81
アクセス ポイントのサイト ライセンス	82
CLI コマンドの変更点	82

FortiWLM Location Manager の設定	82
CLI での設定	82
802.11n ビデオ サービス モジュール (ViSM)	83
ViSM の実装	84
AeroScout の使用	84
Location Feed の使用	85
AeroScout の設定	86
場所の精度	86
タグ プロトコルの実装	87
AeroScout と不正検出	88
AeroScout システム ログ エラー メッセージ	88
AeroScout モバイル装置	88
AeroScout の設定	90
AeroScout Engine からの AeroScout モバイル装置の設定	90
AeroScout 複合レポート	91
希薄化タイムアウト	91
一般 AP 通知	91
一般 AP 通知を受信するための AeroScout 統合ツールの設定	92
FortiPresence API の設定	92
仕組み	92
コントローラの設定	93
FortiWLC (SD) の通信ポート	94
コントローラ ベースの DHCP サーバの設定	95
DHCP サーバの作成	96
DHCP リースの表示	97
Fortinet Service Control の使用	98
Service Control のグローバル設定の変更	98
AP と コントローラを使用した有線サービス検出	99
サービスの追加または削除	100

場所の設定	101
ユーザ グループの作成	101
Service Control ポリシーの定義	103
IPv6 クライアントのサポート	103
基本的な IPv6 転送	104
動的 VLAN 環境での IPv6 転送	105
高パフォーマンス IPv6 転送	106
IPv6 セキュリティ	106
IPv6 マルチキャスト最適化	106
IPv6 優先順位設定	106
IPv6 ネットワーク管理の拡張	107
Spectrum Manager へのアクセス	107
Spectrum Manager ダッシュボード	107
イベント ログ	109
干渉イベントのクラスタリング	111
Spectrum Manager - チャネル可用性	112
Spectrum Manager - チャネル使用率	113
Spectrum Manager - Spectrogram	114
Spectrum Manager - イコライザ	115
Spectrum Manager - パーシステンス	116
コントロール パネル	118
Sensors Filter	118
Sensors Hierarchy	118
Group Information	118

Time Filter	119
Start Time	119
Stop Time	119
Advanced Filter	120
Interference	121
Display Settings	122
[Event Log] - [Display Settings]	122
[Channel Availability] - [Display Settings]	122
[Channel Utilization] - [Display Settings]	123
[Spectrogram] - [Display Settings]	124
[Equalizer] - [Display Settings]	126
[Persistence] - [Display Settings]	127
センサー	129
ソフトウェア センサー	129
ハードウェア センサー	129
RF 干渉の分類	130
干渉デバイスの無線周波数の特性	131
RF 干渉の検出	132
履歴スペクトラム ダッシュボード分析	134
イベント ログ	134
時間ベースの分析	134
Proactive Spectrum Manager	134
Web UI を使用した Proactive Dashboard Manager の設定	134
CLI を使用した Proactive Dashboard Manager の設定	136
デバイスのフィンガープリンティング	136
Web UI を使用した構成	136
新規のデバイス OS の追加	137
既存のデバイス OS の変更	137
デバイス OS の詳細をエクスポート	138
新規デバイス OS の詳細をインポート	138

CLI を使用した構成	138
ESS の設定	139
Web UI による ESS の追加	139
AP の仮想セルが実際にオンになるタイミング	147
CLI による ESS の追加	148
CLI による ESSID の割り当て	148
有効化と無効化	148
CLI 設定	149
ESS のセキュリティ プロファイル	151
CLI による ESSID AP の CAC の設定	151
CLI によるビーコン パラメータの設定	151
CLI による ESSID ブロードキャストの設定	152
CLI によるアクセス ポイントの ESSID 参加の設定	153
仮想化モードの設定	153
Web UI による AP400 の仮想セル サポートの設定	154
CLI による AP400 の仮想セル サポートの設定	155
プローブ応答しきい値の設定	157
SNRRange	157
GUI ページ:	158
CLI によるデータ転送速度の設定	158
CLI による VLAN の割り当て	160
サポートされる WMM 機能	161
U-APSD の設定	162

仮想セル オーバーフロー機能	162
仮想セル オーバーフローの使用	162
Web UI による仮想セル オーバーフローの設定	163
CLI による仮想セル オーバーフローの設定	163
ブリッジとトンネル	164
ブリッジ ESS プロファイルでサポートされている機能	164
ブリッジ AP 配備の例	165
ブリッジ プロファイルの設定	166
WAN のサバイバビリティ	167
ブリッジ AP とコントローラのコンタクトが失われた場合の処理	167
マルチキャスト	167
コントローラと AP の IGMP スヌーピングの設定	168
IGMP スヌーピングを設定するコマンド	169
マルチキャスト MAC 透過機能	169
Web UI からのマルチキャストの有効化	169
CLI によるマルチキャストの有効化	169
VLAN と ESS プロファイルのマッピングの表示	170
VLAN ごとのマルチキャストの制限	170
.....	170
GRE ESSID 機能	170
バンド ステアリング機能	170
Web UI によるバンド ステアリングの設定	171
CLI によるバンド ステアリングの設定	171
完全優先転送の上書き	174
[Expedited Forward Override] (完全優先転送の上書き) を設定する手順	174
Vport の SSID ブロードキャスト	176
Vport の SSID ブロードキャストの設定	176
複数の ESSID のマッピング	177
Web UI によるブリッジ モードの設定	179

CLI によるブリッジ モードの設定	180
単一 MAC での複数 IP の使用	180
時間ベースの ESS	181
タイマー プロファイルの作成	181
Web UI の使用	181
CLI の使用	183
冗長性の実装.....	185
N+1 の検出メカニズム	187
冗長イーサネット	187
CLI による冗長イーサネット フェイルオーバーの設定.....	188
冗長イーサネット フェイルオーバーからのリカバリ	188
N+1 冗長性	189
N+1 フォールバック	189
自動フォールバック	190
自動復帰.....	190
フェイルオーバーのシナリオ	191
ハートビートの周期およびハートビートのタイムアウトに関する推奨事項.....	191
ネットワークの準備	192
N+1 クラスタの設定.....	194
マスタ コントローラでの N+1 の開始	194
スレーブ コントローラでの N+1 の設定	195
N+1 インストールの監視	196

N+1 インストールの管理	198
実行設定の同期化	199
N+1 マスタ コントローラの無効化と削除	199
N+1 インストールの停止	199
マスタ コントローラの交換	200
N+1 システム ログの操作	200
アップグレード	202
N+1 フェイルオーバーからのリカバリ	203
デュアル イーサネット フェイルオーバーによる N+1 からのリカバリ	203
オプション 43	203
DHCP オプション 43 を使用した AP 対応冗長	204
DNS を使用した AP 対応冗長	204
ネットワーク インターフェイスの設定	205
インターフェイスの基本的なネットワーク設定	205
802.11d のサポート	206
デュアル イーサネットの操作	206
デュアル イーサネットの設定	206
冗長インターフェイスの設定	207
アクティブ インターフェイスの設定	207
FastEthernet インターフェイス情報の表示	207
インターフェイスおよびネットワーキング コマンド	208
ポート プロファイルの設定	208
ポート プロファイルの作成	209
特定のイーサネット ポートのポート プロファイルの有効化	211
802.1x 認証の有効化	212
CLI による有効化	212
Web UI による有効化	213
リンク アグリゲーション	214
事前設定	215

CLI による LACP の有効化	215
LACP ステータスの確認	215
Web UI による LACP の有効化	216
管理インターフェイスの設定	216
Physical Interfaces	217
物理インターフェイスの追加	217
VLAN Interfaces	218
管理 VLAN インターフェイスの追加	218
固定ルートの使用	220
固定ルートの追加	220
仮想インターフェイス	221
仮想インターフェイスの追加	221
セキュリティの設定	223
ワイヤレス LAN セキュリティの設定	223
Web UI によるセキュリティ プロファイルの設定	224
Wi-Fi 保護アクセス (WPA2)	228
暗号化サポート	229
CCMP-AES	229
WEP セキュリティ機能	229
WEP プロトコルの動作	230
WEP プロトコルの限界	231
GRE トンネルの設定	231
CLI によるセキュリティ プロファイルの設定	234

CLI での 802.1X RADIUS セキュリティの設定	235
802.1X RADIUS セキュリティ プロファイルの例	236
802.1X PTK キー変更	236
802.1X GTK キー変更	237
CLI での WPA2 の設定	239
WPA2 の設定例	239
WPA2-PSK の設定例	239
WPA の Opportunistic PMK キャッシュ	240
802.11 WEP 暗号化の設定	240
CLI 設定のチェック	242
Policy Enforcement Module (ポリシー適用モジュール)	243
CLI のファイアウォール ポリシーの設定	244
ユーザごとのファイアウォールのトラブルシューティング	245
RSA SecurID による認証	245
RSA SecurID 認証トークンおよびコード	245
RSA SecurID サーバ	245
RSA SecurID エージェント	246
RSA SecurID の設定	246
MAC フィルタリングの設定	246
MAC フィルタリングの動作	247
MAC フィルタリングの設定	249
拒否 MAC フィルタリング リストの設定	251
MAC フィルタリング用のリモート RADIUS サーバの設定	252
MAC フィルタ用のセキュリティ プロファイルの設定	253
セキュリティ証明書	253
ワイルドカード証明書の生成	255
証明書のインポート	255
サーバ証明書をアプリケーションに割り当てる	256

AP 証明書	257
AP CSR の生成	257
CSR のエクスポート	258
AP 証明書のインストール	259
証明書に関するトラブルシューティング	260
WAPI 設定	261
WAPI 認証モードの指定	261
WAPI 証明書のインポート	261
WAPI サーバの設定	262
Palo Alto Networks Firewall との統合	262
VPN 接続の設定	262
VPN 用にコントローラの証明書を有効化する	263
VPN の設定	263
VPN AP の追加	264
VPN クライアント接続の設定	266
認証	267
RADIUS 認証	267
RADIUS 認証の 802.1X の概念モデル	267
Web UI を使用したユーザのための RADIUS 認証の設定	268
CoA のサポート	269
Web UI を使用した管理者のための RADIUS 認証の設定	270
CLI を使用した管理者のための RADIUS 認証の設定	271
RADIUS に認証モードを設定する CLI の例	272
RADIUS 認証属性	272
802.1X の属性	272

クライアントの RADIUS アカウンティング	273
キャプティブ ポータルのための RADIUS アカウンティングの設定	277
RADIUS ベースの ESS プロファイル制限	277
リモート RADIUS サーバ	278
事前準備	279
仕組み	279
リレー AP について	279
Web UI を使用した設定	280
CLI を使用した設定	281
TACACS+ 認証	282
CLI を使用した TACACS+ 認証モードの設定	283
TACACS+ に認証モードを設定する CLI の例	283
Web UI を使用した TACACS+ 認証モードの設定	284
ローカル管理者認証	286
CLI を使用したローカル認証モードの管理者の設定	286
ローカル管理者を設定する CLI の例	286
Web UI を使用したローカル認証の設定と管理者の追加	287
802.1X 認証	287
802.1X の構成要素	288
EAP タイプについて	288
EAP-TLS	288
EAP-TTLS (Tunneled Transport Layer Security)	289
LEAP (Lightweight Extensible Authentication Protocol)	289
PEAP (Protected Extensible Authentication Protocol)	289
キャプティブ ポータル	291
フォーティネット キャプティブ ポータルの設定	291

HTML ページをカスタマイズして自社独自のページを使用する (オプション) . . .	292
カスタム ページの作成	293
CLI を使用した新しいカスタム HTML ファイルの実装	295
GUI を使用した新しいカスタム HTML ファイルの実装	296
CLI を使用したキャプティブ ポータルの設定	298
ローカルでのキャプティブ ポータル ゲスト ユーザ ID の作成	300
CLI の例 - ゲスト ユーザ ID の作成	300
キャプティブ ポータルの再認証の迂回の設定 (オプション)	303
Apple Captive Network Assistant (CNA) の迂回	303
N+1 構成のキャプティブ ポータル	304
キャプティブ ポータルのトラブルシューティング	305
キャプティブ ポータル プロファイル	305
有線クライアントのキャプティブ ポータル (CP) 認証	307
MAC 認証クライアントの CP の迂回	308
CLI を使用した設定	309
サードパーティのキャプティブ ポータル ソリューション	310
Web UI を使用したサードパーティ キャプティブ ポータルの設定	311
CLI を使用したサードパーティ キャプティブ ポータルの設定	311
キャプティブ ポータル認証のための RADIUS サーバの設定	312
Web UI でのキャプティブ ポータル認証のための RADIUS サーバの設定	312
CLI でのキャプティブ ポータル認証のための RADIUS サーバの設定	312
OAuth 認証のサポート	314
ソーシャル認証のサポート	314
キャプティブ ポータル除外プロファイルの作成	315
キャプティブ ポータル プロファイルでの Fortinet Presence の設定	316

セキュリティおよび ESS プロファイルでのキャプティブ ポータル プロファイルの有効化	318
不正 AP の検出と緩和.....	319
Web UI による不正 AP 緩和の設定	321
Web UI による許可対象 AP のリストの変更	321
Web UI によるブロック対象 AP のリストの変更.....	322
Web UI によるスキャンと緩和の設定	323
CLI を使用した不正 AP 検出の設定	325
スキャン リストへの AP の追加.....	325
スキャン リストからの AP の削除	326
CLI による AP アクセスとブロック リストの設定.....	326
不正緩和の例	327
CLI による検出と緩和の設定の変更	328
CLI による緩和 AP 数の変更	329
CLI によるスキャンと緩和の設定の変更	329
CLI による最小 RSSI の変更	330
不正緩和の例	330
CLI による不正検出と緩和の設定の変更	331
CLI による緩和 AP 数の変更	332
CLI によるスキャンと緩和の設定の変更.....	332
CLI による最小 RSSI の変更	333
Web UI による不正 AP 緩和の設定	333
Web UI による許可対象 AP のリストの変更.....	334
Web UI によるブロック対象 AP のリストの変更	334
Web UI によるスキャンと緩和の設定	335
不正緩和のトラブルシューティング.....	337
VLAN の設定.....	339
VLAN の設定とデプロイ	340
VLAN のブリッジ AP	341

ブリッジ モードでの有線ポート向け VLAN タギング	341
VLAN タギングの設定	342
CLI の使用	342
ブリッジ モードでの動的 VLAN のサポート	342
VLAN の削除	342
VLAN に関する詳細	343
VLAN プール	343
特長	343
設定	344
Web UI の使用	344
CLI の使用	344
アクセス ポイントの設定	347
AP 検出の仕組み	347
OAP832 および OAP433 の検出シーケンス	348
Web UI による AP の追加と設定	348
Web UI による AP の無線の設定	351
CLI による AP の追加と設定	354
CLI によるレイヤ 3 AP の設定	356
CLI による AP 電源、チャネル幅、MIMO モードの設定	357
CLI による AP の無線の設定	358
無線インターフェイス設定コマンドのまとめ	358
CLI による無線転送電力の設定	359
CLI による短いプリアンプルの有効化と無効化	360
CLI による不正 AP スキャンのための無線の設定	361
CLI による無線インターフェイスの有効化 / 無効化	361

CLI による 802.11n のみをサポートする無線の設定	361
AP の無線チャネルの設定	362
Sitesurvey	362
前提条件	363
Sitesurvey オプションの設定	363
CLI の使用	363
Sitesurvey の有効化	363
Sitesurvey の無効化	363
国コードとチャネルの設定	364
非アクティビティ時間の設定	364
IP アドレスの設定	364
SSID の設定	364
無線の有効化 / 無効化	365
Sitesurvey 更新レートの設定	366
転送電力の設定	366
Sitesurvey 設定の保存	366
GUI の使用	366
Sitesurvey 結果の表示	368
GUI の使用	368
接続パラメータ	369
パラメータのトラブルシューティング	369
ネットワーク パラメータ	369
Sitesurvey の無効化	370
CLI の使用	370
Sitesurvey 設定の表示	370
Sitesurvey 結果 (統計) の表示	371
出力例	371
無線リソースの自動プロビジョニング (ARRP)	372
Web UI を使用した設定	373

CLI を使用した設定	374
制限事項	375
802.11k/r の設定	376
制限事項	376
802.11K の有効化	376
Web UI の使用	376
CLI の使用	376
ローミング アクセス コントローラ (RAC)	377
ローミングのタイムアウト	377
RAC の設定に必要なステップ	378
Web UI を使用した設定	378
CLI を使用した設定	380
アクセス ポイントの交換	380
アクセス ポイントを交換する前の確認事項	380
アクセス ポイントの交換方法	381
AP 交換後の設定の更新	382
AP でサポートされている運用モード	382
セキュリティ モード	383
仮想化された環境での AP	384
外部アンテナのゲインの設定	384
自動 AP アップグレード	384
QoS (Quality of Service) の設定	389
Web UI による QoS ルールの設定	389
ブリッジ モード トラフィックの QoS ルール	393
[Match] チェックボックスと [Flow Class] チェックボックスについて	394

CLI による QoS ルールの設定	396
QoS ルール CLI 設定コマンド	396
CLI による QoS ルールの設定の例	398
VoIP の最適化	399
VoIP への QoS ルールの使用	400
標準外ポートのための QoS ルールの変更	401
グローバル QoS 設定	402
レート制限 QoS ルール	403
CLI によるレート制限	403
GUI によるレート制限 QoS ルール	405
レート制限の例	405
TCP の同じサブネットのクライアントにレート制限を設定	405
TCP の異なるサブネットのクライアントにレート制限を設定	406
コーデック ルールの設定	407
QoS 統計表示コマンド	410
電話 / コールのステータスの表示	410
コール アドミッション詳細の表示	411
QoS ルールのその他の例	411
特定のクライアントのレート制限の設定	412
ワイヤレス ピアツーピア QoS ルール	413
ピアツーピアの優先度の設定	413
ピアツーピアのブロック	414
802.11n ビデオ サービス モジュール (ViSM)	416
ViSM の実装	416
CLI による CAC (Call Admission Control) と負荷分散機能の設定	416
アプリケーション可視化 (DPI)	417
制限事項と推奨事項	418
アプリケーション可視化の有効化	419

ポリシーの作成.....	419
例	420
ポリシーのリスト.....	421
カスタム アプリケーション	422
カスタム アプリケーションの作成とそのポリシーへの割り当て	423
DPI ダッシュボード	426
CLI の使用.....	426
ポリシーの作成	426
ポリシーの監視	428
ブロックの統計情報	432
有線クライアントのサポート	433
ポリシー詳細の表示.....	434
帯域幅制限	434
制限事項 :.....	435
DSCP マーキング.....	435
有効な DSCP 値の文字列.....	437
CLI コマンド.....	438
ベスト プラクティス.....	439
仮想セルにおける AP のロード バランス.....	439
管理パケットの DSCP マーキング.....	441
DSCP 値の有効化.....	442
メッシュ ネットワーク	443
メッシュの制約.....	443

Enterprise Mesh の設計	444
ゲートウェイ AP	445
メッシュ AP	446
リーフ AP	446
有線クライアント	446
機器の要件	446
Enterprise Mesh システムのインストールと設定	447
アンテナの設置場所の決定	447
Fortinet Enterprise Mesh のインストール	447
フェーズ 1: イーサネット スイッチでコントローラと AP を接続する	448
フェーズ 2: メッシュ プロファイルを作成する	448
フェーズ 3: AP をメッシュに追加する	449
フェーズ 4: AP のメッシュ処理を設定する	450
フェーズ 5: ケーブルを外して AP を配備する	451
プラグ & プレイによるメッシュ AP の追加	451
メッシュでの VLAN の設定	453
VLAN トランクの有効化	453
CLI の使用	453
Enterprise Mesh のトラブルシューティング	454
メッシュ トポロジの表示	454
問題と解決方法の対応表	455
SNMP の設定	457
機能	458
SNMP アーキテクチャ	458
MIB テーブル	459
管理アプリケーションのための MIB テーブルのダウンロード	460
SNMP の設定	461
SNMP コミュニティ文字列	461
トラップ マネージャ	462

SNMP トラップ	463
SNMP/OID によってシステム ステータスを監視するオブジェクト	464
エージェントの連絡先と場所を設定するコマンド	465
CLI による FortiWLC の SNMP サービスの設定	466
Web UI による FortiWLC の SNMP サービスの設定	466
サードパーティ ベンダのセットアップ	467
SNMP の有効化、無効化、リロード	467
SNMP バージョン 3 のサポート	467
セキュリティ レベル	468
セキュリティ モデル	468
セキュリティ レベルとセキュリティ モデルの組み合わせ	469
SNMP バージョン 3 のコマンド	469
SNMP バージョン 3 のサポートの制限事項	469
トラブルシューティング	471
開始する場所	471
エラー メッセージ	472
システム ログ	473
ステーション ログ イベント	477
MAC フィルタリング ステーション ログ イベント	480
キー交換ステーション ログ イベント	481
認証ステーション ログ イベント	483
1X/WPA/WPA2 認証ステーション ログ イベント	486
DHCP ステーション ログ イベント	486
キャプティブ ポータル ステーション ログ イベント	488
システム診断	488

無線診断	488
ステーション診断	490
推論	490
ステーション推論メッセージ	492
保守性	494
ステーション ログ問題のフィルタ	495
問題 ID のリスト	497
診断イベントから確認できる他の情報	497
パケットの捕捉	498
パケット捕捉プロファイルの例 - WireShark	500
パケット捕捉結果で確認すること	501
検出ログで確認すること	501
FTP エラー コード	502
障害管理	505
アラーム	505
アラーム定義の変更	506
アラームのリスト	508
イベント	512
イベント定義の変更	513
???? ?? ??????	517
?????????	518
AP ????	527
802.11	530
???? ??????	531
?????? ????	532
QoS	534
?? AP	535
?????	536
N+1 ???	536

用語集.....	539
----------	-----

1 本ガイドについて

本ガイドでは、ワイヤレス LAN システムの設定で使用するさまざまなオプションを説明します。

対象読者

本ガイドは、ワイヤレス LAN システムを設定および保守するネットワーク管理者を対象としています。以下の概念を把握しておく、FortiWLAN を円滑に設定できます。

- ネットワーク管理に関する以下の概念
 - インターネット プロトコル (IP) アドレス設定とルーティング
 - Dynamic Host Configuration Protocol (DHCP)
 - レイヤ 2 およびレイヤ 3 スイッチの設定 (お使いになるスイッチで必要となる場合)
- IEEE 802.11 (Wi-Fi) に関する以下の概念
 - ESSID
 - WEP
- ネットワーク セキュリティ (オプション)
 - WPA
 - 802.1X
 - RADIUS
 - X.509 証明書

その他の関連情報

次の Web サイト、フォーティネット が提供するマニュアル、および外部の参考資料も利用できます。

Web リソース

FortiWLC を購入してから最初の 90 日間は、オンラインサポートを利用できます。サポート契約を締結されている場合には、契約期間中サポートを利用できます。次のような情報については、Web サイトをご覧ください。

- ナレッジベース (Q&A)
- ダウンロード
- サポートチケットを新規に発行するか、同じようなサポート内容が過去にないかどうかを確認してください。
- カスタマ ディスカッション フォーラム

URL : <http://support.fortinet.com>

フォーティネットのマニュアル

- 『FortiWLC (SD) リリース ノート』
- 『アクセス ポイントおよびレディオ スイッチ導入・設置ガイド』
- 『コントローラ導入・設置ガイド』
- 『FortiWLC (SD) コマンド リファレンス』
- 『FortiWLC (SD) 入門ガイド』

表記規則

本ガイドでは、情報をわかりやすく伝えるために、以下の表記規則を使用します。

太字	構文の説明の中で、そのまま入力するコマンドやキーワードを表します。
斜体	新しい用語、強調する内容、書籍名に使用します。構文の説明ではユーザが値を指定する引数にも使用します。
Courier フォント	ファイル名、フォルダ名、コンピュータ画面出力、およびユーザが入力すべき構文記述の文字列を示します。
Ctrl-	他のキーと一緒に Ctrl キーを使用する必要があることを示します。たとえば、Ctrl-D は、Ctrl を押した状態で D キーを押すことを意味します。キーは大文字で表記しますが、大文字 / 小文字の区別はされません。



そのトピックに対する追加情報、助言、ヒントです。



データの破損や損失、またはアプリケーションの予期しない動作を引き起こす可能性のある動作に関する重要な情報を示します。



装置の故障または身体に危険が及ぶ可能性のある動作に関する重大な情報を示します。

構文表記

サンプルのコマンド構文記述と入力例では、以下のテキスト要素と句読記号を使用して、コマンドに対するユーザの入力とコンピュータからの出力を示します。

太字	必須のコマンド、キーワード、区切り文字です。
斜体	値が代入される引数またはファイル名です。
no	その特性や機能を無効にすることを指示するためのオプションです。
[]	角括弧で囲まれる部分は、オプションの要素です。
{ }	中括弧は、囲まれた要素のいずれか 1 つを使用する必要があることを表します
	縦線で区切られた要素の中から選択します。
[{}]	オプションの要素内から 1 つを必ず選択します。
...	前の引数を繰り返すことができます。

以下の図は、構文表記のサンプルを表しています。

[no] アクション ターゲット { キーワード | キーワード } [引数 ...]

1 つ以上の値の繰り返し

囲まれている要素から選択

サブモード内のキーワードまたはコマンド

コマンドまたはアクション。アクションによって、別のコマンドモードに移行する場合があります。

オプションの no 形式はコマンドを無効にします。
no を指定しないと、有効または再度有効になります。



多くのコマンドには、コマンドのページの「デフォルト」の項に示したとおり、デフォルトの設定または値があります。

お問い合わせ

フォーティネットの Web サイトには、以下の URL でアクセスできます。

www.fortinet.com

カスタマ サービス & サポート

サポートが必要な場合には、フォーティネットのカスタマ サービス & サポート (24 時間対応、電話番号 : +1 408-542-7780) またはお近くの連絡先までお問い合わせください。サポートポータル (<https://support.fortinet.com/>) をご利用いただくこともできます。

フォーティネットのカスタマ サービス & サポートは、エンド ユーザと販売パートナーからの以下のお問い合わせに対応しています。

- テクニカル サポート
- ソフトウェア アップデート
- 部品交換サービス

2 CLI の概念

本章では、FortiWLC (SD) のコマンドライン インターフェイス (CLI) の使用に関するヒントを紹介します。各種のコマンド モードについて説明し、ヘルプ情報の入手、ヒストリ機能の使用、およびプロンプトと端末の特性のカスタマイズに関するヒントを紹介します。本章は以下の項で構成されています。

- [CLI の開始 \(33 ページ\)](#)
- [CLI コマンド モード \(34 ページ\)](#)
- [コマンドラインのみのコマンド \(35 ページ\)](#)
- [コマンドの省略形 \(37 ページ\)](#)
- [コマンドの no フォームと default フォームの使用 \(38 ページ\)](#)
- [ヘルプの表示 \(38 ページ\)](#)
- [コマンド ヒストリの使用 \(39 ページ\)](#)
- [show コマンドの出力における語句の検索 \(41 ページ\)](#)
- [CLI プロンプトのカスタマイズ \(41 ページ\)](#)
- [端末特性の操作 \(42 ページ\)](#)
- [セッションの終了 \(43 ページ\)](#)

CLI の開始

コマンドライン インターフェイスの使用を開始するには、次の手順を実行します。

1. コントローラに IP アドレスが割り当てられたら、シリアル コンソールまたはイーサネット ポートを使用するか、telnet または SSH2 をリモートで使用して、コントローラに接続します。
コントローラに IP アドレスに割り当てる方法については、『**FortiWLC (SD) 入門ガイド**』の「初期セットアップ」の章を参照してください。
2. ログイン プロンプトで、ユーザ ID とパスワードを入力します。デフォルトでは、guest と admin というユーザ ID が設定されています。
 - admin ユーザ、admin パスワードでログインすると、自動的に特権 EXEC モードに入ります。

- guest ユーザでログインすると、ユーザ EXEC モードに入ります。特権 EXEC モードに入るためには、ここで **enable** コマンドと、**admin** ユーザのパスワードを入力する必要があります。

3. コマンドの実行を開始します。

CLI コマンド モード

CLI はいくつかの異なるコマンド モードに分かれており、各モードには独自のコマンドセットがあり、いくつかのモードには 1 つ以上のサブモードがあります。システム プロンプトまたはコマンドの任意の場所にクエスチョン マーク (?) を入力すると、現在のモードで利用できるコマンドやオプションのリストが表示されます。

ユーザ EXEC モード

コントローラでセッションを開始すると、ユーザ モード (ユーザ EXEC モードとも呼びます) に入ります。ユーザ EXEC モードでは、コマンドの一部のみを使用できます。たとえば、多くのユーザ EXEC コマンドは、現在の設定情報を表示する **show** コマンドやカウンタやインターフェイスをクリアする **clear** コマンドのように、一時的に情報を表示するだけのコマンドです。コントローラのリブート時にユーザ EXEC コマンドは保存されません。

- アクセスする方法 : **guest** ユーザを使用して、コントローラのセッションを開始します。
- プロンプト : `default>`
- 終了方法 : **exit** または **quit** と入力します。
- まとめ : ユーザ EXEC モードは、コンソールの設定を変更する、システム設定を表示する、ネットワーク接続を確認するなどのシステム情報の確認のために使用します。

特権 EXEC モード

CLI のすべてのコマンドにアクセスするには、特権 EXEC モードに入る必要があります。**admin** でログインするか、ユーザ EXEC モードで **enable** コマンドを入力して、**admin** パスワードを指定すれば、特権 EXEC モードに入ることができます。このモードからは、すべての特権 EXEC コマンドを入力でき、グローバル設定モードに入ることもできます。

- アクセスする方法 : ユーザ EXEC モードで **enable** と入力するか、**admin** ユーザでログインします。
- プロンプト : `default#`
- 終了方法 : **disable** と入力します。
- まとめ : このモードを使用して、システム ファイルの管理といくつかのトラブルシューティングを実行します。このモードへのアクセスを保護するためには、(グローバル設定モードから) デフォルトのパスワードを変更してください。

グローバル設定モード

グローバル設定モードとそのサブモードを使用して、現行の設定を変更します。設定を保存すると、コントローラのリブート時にその設定は保存され、リスタートされます。

グローバル設定モードからは、さまざまなサブモード (分岐) に移行し、さらに限定的な設定機能を実行できます。設定サブモードの例としては、**security**、**qosrules**、**vlan** などがあります。

- 説明：コントローラ全体に適用されるパラメータを設定します。
- アクセスする方法：特権 EXEC モードの状態で、**configure terminal** と入力します。
- プロンプト：**controller(config)#**
- 終了方法：**exit**、**end** と入力するか、Ctrl-Z を押すと、特権 EXEC モード (1 つ前のレベル) に戻ります。
- まとめ：このモードは、いくつかのシステム設定に使用され、追加の設定サブモード (**security**、**qosrules**、**vlan**) に入ります。

コマンドラインのみのコマンド

多くの CLI コマンドについては、Web インターフェイスにも同等の機能があり、どちらのインターフェイスを使用しても同じ作業を行うことができます。以下のリストは、Web インターフェイスの機能にはないコマンドです。

EXEC モードのコマンド

- **configure terminal**
- **no history**
- **no prompt**
- **no terminal length |width**
- **help**
- **cd**
- **copy** (copy running-config startup-config、copy startup-config runningconfig、およびすべてのローカル / リモート copy を含む)
- **delete flash: image**
- **delete filename**
- **dir [dirname]**
- **debug**
- **disable**
- **enable**
- **exit**

- quit
- more (more running-config、more log log-file、more running-script を含む)
- prompt
- rename
- terminal history[size|length|width]
- traceroute
- show history
- show running-config
- show terminal

設定モードのコマンド

- do
- ip username ftp|scp|sftp
- ip password ftp|scp|sftp
- show context

アプリケーションまたはスクリプトを起動するコマンド

- calendar set
- timezone set|menu
- date
- capture-packets
- analyze-capture
- debug
- diagnostics[-controller]
- ping
- pwd
- shutdown controller force
- reload controller default
- run
- setup
- upgrade
- downgrade
- poweroff
- show calendar
- show timezones

- show file systems
- show memory
- show cpu-utilization
- show processes
- show flash
- show qosflows
- show scripts
- show station details
- show syslog-host
- show log
- autochannel
- rogue-ap log clear
- telnet
- syslog-host

コマンドの省略形

コマンドで CLI に対して必ず入力しなければならないのは、そのコマンドを特定するのに十分な部分だけです。次の例は、show security コマンドでは、コマンドを sh に省略できることを示しています。

```
Lab-mc3200# sh security-profile default
Security Profile Table

Security Profile Name : default
L2 Modes Allowed : clear
Data Encrypt : none
Primary RADIUS Profile Name :
Secondary RADIUS Profile Name :
WEK Key (Alphanumeric/Hexadecimal) : *****
Static WEK Key Index : 1
Re-Key Period (seconds) : 0
Captive Portal : disabled
802.1X Network Initiation : off
[Tunnel Termination] : PEAP, TTLS
Shared Key Authentication : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Group Keying Interval (seconds) : 0
Key Rotation : disabled
Reauthentication : off
```

```
MAC Filtering : off
Firewall Capability : none
Firewall Filter ID :
Security Logging : off
Allow mentioned IP/Subnet to pass through Captive portal : 0.0.0.0
Subnet Mask for allowed IP/Subnet to pass through Captive portal : 0.0.0.0
```

コマンドの no フォームと default フォームの使用

ほとんどすべての設定コマンドで no フォームを利用できます。一般的に、次の場合に no フォームを使用します。

1. 特性あるいは機能を無効にする。
2. コマンドをデフォルトにリセットする。
3. コマンドの動作を逆にする。
4. no フォームなしでコマンドを使用して、無効になっている機能を再度有効にするか、あるいは no コマンドのアクションを逆にします。

設定コマンドでは default フォームも使用できます。コマンドの default フォームによりコマンド設定がデフォルトの状態に戻ります。ほとんどのコマンドはデフォルトによって無効になるため、default フォームは no フォームと同じ機能になります。しかし、いくつかのコマンドはデフォルトによって有効になり、変数が特定のデフォルト値に設定されます。これらの場合、default コマンドはコマンドを有効にして、変数をデフォルト値に設定します。コマンドの参照ページでは、これらの条件を説明しています。

ヘルプの表示

システム プロンプトにクエスチョン マーク (?) を入力すると、各コマンド モードで利用できるコマンドのリストが表示されますコンテキスト センシティブ (文脈依存) ヘルプを使用する場合は、クエスチョン マーク (?) の前のスペース (あるいはスペースを入れないこと) が大きな意味をもちます。特定の文字シーケンスで始まるコマンドのリストを表示するには、クエスチョン マーク (?) の直後にその文字を入力します。スペースは入れません。この形式のヘルプは、あるワードの完全な形をユーザに提示することから、ワード ヘルプと呼ばれます。

キーワードまたは引数を表示するには、キーワードまたは引数の位置にクエスチョン マーク (?) を入力します。(?) の前にスペースを入れます。この形式のヘルプは、ユーザがすでに入

力したコマンド、キーワード、および引数に対して指定可能なキーワードまたは引数を提示することから、コマンド構文ヘルプと呼ばれます。

表 1: *Help* コマンドの例

コマンド	目的
(prompt)# help	ヘルプ システムの簡単な説明を表示します。
(prompt) # abbreviated-command?	現在のモードで使用できる、特定の文字列で始まるコマンドのリストを表示します。
(prompt)# abbreviated-command<Tab>	部分的なコマンド名を完全名に置き換えます。
(prompt)# ?	コマンド モードで利用できるすべてのコマンドを表示します。
(prompt)# command?	そのコマンドで利用できる構文オプション (引数とキーワード) のリストを表示します。
(prompt)# command keyword ?	このコマンドで次に利用できる構文のリストを表示します。

表示されるプロンプトは設定モードによって異なります。

コマンドとキーワードは、それぞれを個別に特定できる長さまでに省略できます。たとえば、configure terminal コマンドであれば、config t というように省略できます。

help コマンドを入力すると、ヘルプ システムの説明が表示されます。これは、どのコマンドモードでも利用できます。

コマンド ヒストリの使用

CLI は、セッション中に入力されたコマンドの履歴を保持する機能を備えています。この機能は、長いコマンドや複雑なコマンドを、パラメータを少しだけ変更して再入力する場合に便利です。コマンド ヒストリの機能を使用するには、以下の操作を実行します。

- コマンド ヒストリ バッファのサイズをセットする
- コマンドを呼び出す
- コマンド ヒストリ機能を無効にする

コマンド ヒストリ バッファのサイズのセット

デフォルトでは、CLI はヒストリ バッファに 10 個のコマンド行を記録します。現在のターミナル (端末) セッションでシステムが記録するコマンドの行数をセットし、コマンド ヒストリ機能を有効にするには、**terminal history** コマンドを使用します。

```
controller# terminal history [size n]
```

terminal no history size コマンドは、ヒストリ バッファに保存されている行数をリセットし、デフォルトである 10 行または size で指定した行数にします。

ヒストリ バッファのサイズをデフォルト (10) に戻すには、**default history** と入力します。

```
controller# default history
```

ヒストリ バッファの内容を表示するには、**terminal history** と入力します。

```
controller# terminal history
 7 interface Dot11Radio 1
 8 end
 9 interface Fast Ethernet controller 1 2
10 show interface Dot11Radio 1
11 end
12 show interfaces FastEthernet controller 1 2
13 sh alarm
14 sh sec
15 sh security
```

コマンドの呼び出し

ヒストリ バッファからコマンドを呼び出すには、以下のコマンド、またはキーの組み合わせを使用します。

- Ctrl-P または上向き矢印キー。これにより、ヒストリ バッファに保存されている最も新しいコマンドから順番に、コマンドが呼び出されます。このキー入力を繰り返すと、古いコマンドにさかのぼって呼び出されます。
- Ctrl-N または下向き矢印キー。ヒストリ バッファの中で、Ctrl-P または上向き矢印キーで呼び出したコマンドの後に新しいコマンドに戻ります。
- !number。ヒストリ リストの number のコマンドを実行します。terminal history コマンドまたは show history コマンドを使用して、ヒストリ バッファを一覧表示し、その後、このコマンドを使用して、そのシーケンス番号で表示されたコマンドを再実行します。
- ヒストリ バッファの内容を表示するには、show history コマンドを使用します。

```
controller# show history
```

コマンド ヒストリ機能の無効化

端末ヒストリ機能は、自動的に有効になっています。現行の端末セッションでこの機能を無効にするには、特権 EXEC モードまたは非特権 EXEC モードで **no terminal history** と入力します。

```
controller# no terminal history
```

show コマンドの出力における語句の検索

show コマンドの出力にある語句を素早く検索するには、以下のコマンドを使用します。

```
show argument | grep "string"
```

この機能を使用するには、単一の show コマンドしか grep への入力にできず、show コマンドには引数を指定できません (たとえば、show ap 54 のようなコマンド形式)。**"string"** には、リテラル文字を指定します。ここでは AP-54 のように大文字小文字は区別され、二重引用符で囲む必要があります。コマンド行につき 1 回の文字列検索のみを実行できます。

例として、show ap コマンドの出力で AP-54 という項目を検索して表示するには、以下のコマンドを入力します。

```
controller# show ap | grep "AP-54"
```

AP ID	AP Name	Serial Number	Op State	Availability	Runtime
	Connectivity	AP Model	AP Type		
54	AP-54	00:0c:e6:00:3e:a8	Disabled	Offline	3.1.4-25 None
AP332	Local				

AP Table(1 entry)

CLI プロンプトのカスタマイズ

デフォルトの CLI プロンプト

デフォルトでは、CLI プロンプトは、ユーザ EXEC モードの場合にはシステム名の後に大なり記号 (>)、特権 EXEC モードの場合にはシャープ記号 (#) になります。

CLI プロンプトをカスタマイズするためのコマンド

システムの CLI プロンプトをカスタマイズするには、グローバル設定モードで以下のいずれかのコマンドを使用します。

表 2: CLI プロンプトをカスタマイズするためのコマンド

コマンド	目的
<code>prompt 文字列</code>	CLI プロンプトをカスタマイズします。
<code>no prompt</code>	CLI プロンプトの表示を無効にします。
<code>default prompt</code>	プロンプトを、デフォルトであるホスト名にセットします。

端末特性の操作

端末設定の表示

画面の長さや幅を始めとする、現在の端末設定を表示するには、以下のように入力します。

```
controller> show terminal
Terminal Length:      0
Terminal Width:       80
History Buffer Size:  10
```

端末画面の長さや幅のセット

デフォルトでは、端末の長さは 0 行、幅は 80 列です。このデフォルト設定を上書きして、現行セッションでの現在の端末画面の行数あるいは文字列を設定するには、ユーザ EXEC モードで以下のコマンドを使用します。

```
controller> terminal length screen-length
controller> terminal width characters
```

端末の長さや幅をデフォルト値にリセットするには、`default` コマンドを使用します。

```
controller> default terminal length
controller> default terminal width
```

端末の長さをゼロ以外の値にすると、ページ毎の表示がオンになります。出力の長さが端末の長さを超えると、その出力は一時停止し、`---More---` と表示されます。

1. `---More---` プロンプトでスペース バーを押すと、その出力の次のページが表示されます。

2. ---More--- プロンプトで Enter キーを押すと、その出力の次の 1 行が表示されます。
3. ---More--- プロンプトでユーザがこれ以外の文字を押すと、その出力が終了し、コマンドプロンプトが表示されます。

セッションの終了

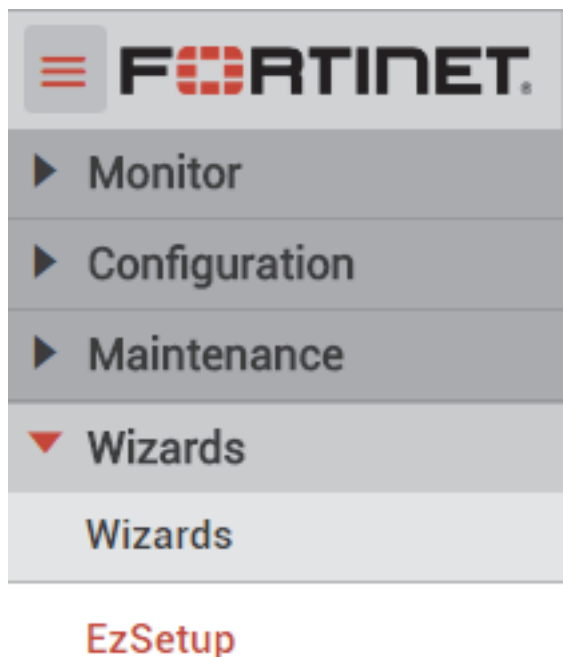
セッションを終了するには、ユーザ EXEC モードまたは特権 EXEC モードで以下のコマンドを使用します。

```
controller> exit
```


3 Web UI の概念

FortiWLC (SD) にアクセスするには、ブラウザにコントローラの IP アドレスを入力します (48 ページの「[ブラウザ](#)」を参照)。Web UI には、Monitor、Maintenance、Configuration、Wizards の 4 つのメニューが表示され、ここから操作を実行します。リストの項目をクリックすると、展開されて、その項目に含まれるオプションが表示されます。

図 1: Web UI のメニュー オプション



GUI と CLI コマンドの関係

FortiWLC (SD) のほとんどの作業は、CLI または GUI のどちらを使用しても実行できます。どちらか一方でないと実行できないコマンドもいくつかあります。下表にこのような例を記載します。前のページの図を参照するか、UI インターフェイスに指示されるリンクをクリックします。

確認したい内容	CLI を使用する場合	GUI を使用する場合
関連付けられているステーション	show station show phones	ステーション テーブル ([Monitor] > [Devices] > [All Stations])
検出可能なステーションと AP	show ap-discovered	ステーション テーブル ([Monitor] > [Devices] > [All Stations])
コントローラの設定	show controller	システム サマリ ([Monitor] > [Dashboard] > [System])
接続されている AP	show ap	ステーション テーブル ([Monitor] > [Devices] > [All Stations] をクリック)
AP の接続方法	show ap-connectivity ap-id	ステーション テーブル ([Monitor] > [Devices] > [All Stations] をクリック)
接続されているステーションの数	show station または show topostation	ステーション テーブル ([Monitor] > [Devices] > [All Stations])
特定の AP へのステーションの接続	show ap-assigned mac-address	ステーション テーブル ([Monitor] > [Devices] > [All Stations])
FTP を使用して新しいオペレーティングシステムバージョンをコントローラに追加する	copy ftp:// ftpuser:ftppasswd@ offbox-ip-address / meru-x.x-xxx-MODEL-rpm.tar. upgrade system x.x	なし
すべての AP の合計スループットを参照する	なし	システム ダッシュボード ([Monitor] > Dashboard > System)

確認したい内容	CLI を使用する場合	GUI を使用する場合
syslog メッセージのサマリ	show syslog-table でログ全体を表示する	システム ログ ファイル テーブル ([Maintenance] > [View Syslog]) で、時間を指定してログのセグメントを表示する
アラーム	show alarm	アラーム ([Monitor] > [Fault Management] > [Alarms])
検出された不正	show rogue-ap-list	不正 AP テーブル ([Monitor] > [Rogue Devices])
AP400 モデル	show ap	
スループットのボトルネック	show statistics top10 -ap -problem (損失 % を表示) analyze-capture start, analyze-capture stop, analyze-capture capture	システム ダッシュボード ([Monitor] > [Dashboard] > [System])
使用率が高いユーザ	show statistics top10-station-talker	ステーション ダッシュボード (click [Monitor] > [Dashboard] > [Station] をクリック)
ユーザの接続が失敗した理由	station-log/station add analyze-capture	ステーション診断 ([Monitor] > [Diagnostics] > [Station] をクリック)
活動していないスポット	show topoap	ステーション診断 ([Monitor] > [Diagnostics] > [All Station] > [Signal Strength Chart])
ステーションの再試行	show station	[Monitor] > [Dashboard] > [Station] > [Retries chart]
ユーザの場所	show station または show topostation	なし
過負荷の無線	show station show statistics top10-ap-problem	[Monitor] > [Dashboard] > [Radio] > [Retries chart] 無線ダッシュボード ([Monitor] > [Dashboard] > [Radio] > [Throughput Chart])

確認したい内容	CLI を使用する場合	GUI を使用する場合
高損失の無線	show station analyze-capture start, analyze-capture stop, analyze-capture snapshot	[Monitor] > [Dashboard] > [Radio] > [Loss % chart] コントローラ ダッシュボード ([Monitor] > [Controller] > [High-Loss Radio chart])
高ノイズの無線	なし	[Monitor] > [Diagnostics] > [Radio] コントローラ ダッシュボード ([Monitor] > [Controller] > [Noise Level chart])
無線管理のオーバーヘッド	show interfaces Dot11Radio statistics	[Monitor] > [Dashboard] > [Radio] > [Management Overhead Distribution chart]
ステーションの平均データ速度	show station 802.11 "802.11a" show station 802.11 "802.11b" show station 802.11 "802.11g" show station 802.11 "802.11g" show station 802.11 "802.11ab" show station 802.11 "802.11bg" show station 802.11 "802.11bgn"	[Monitor] > [Dashboard] > [Station] > [Average Rate charts]

ブラウザ

Web UI

- Internet Explorer 9、10 (Vista および Win XP)
- Mozilla Firefox 25 以上 (Vista および Win XP)
- Google Chrome 31 以上

Captive Portal (キャプティブ ポータル)

- Internet Explorer 6、7、8、9、10
- Apple Safari
- Google Chrome
- Mozilla Firefox 4.x およびそれ以前
- モバイル デバイス (Apple iPhone、BlackBerry など)

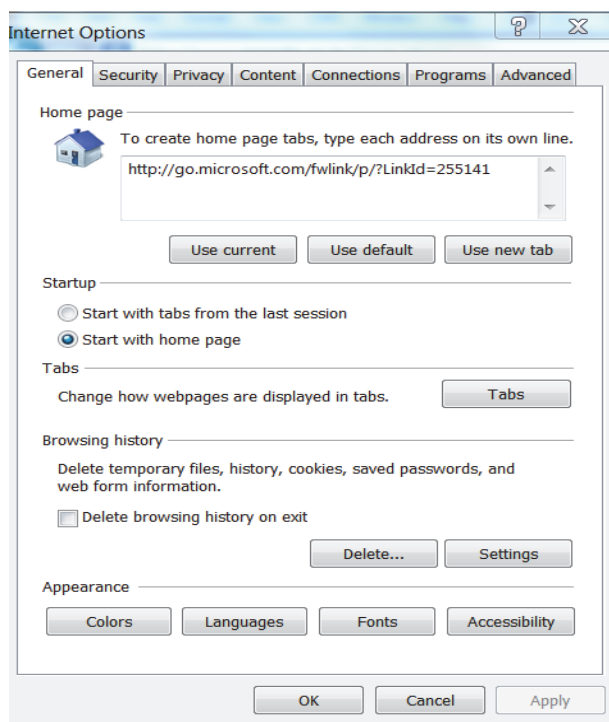
Internet Explorer のキャッシュ設定

Internet Explorer を使用するコンピュータでは、キャッシュ設定を必ずオフにしてください。ダッシュボードの更新がキャッシュ オン設定で無視されることが多いためです。Windows の Internet Explorer を設定するには、次の手順を実行します。

1. Internet Explorer を起動して、[ツール] > [インターネット オプション] をクリックして、[インターネット オプション] にアクセスします。

次のようなウィンドウが表示されます。

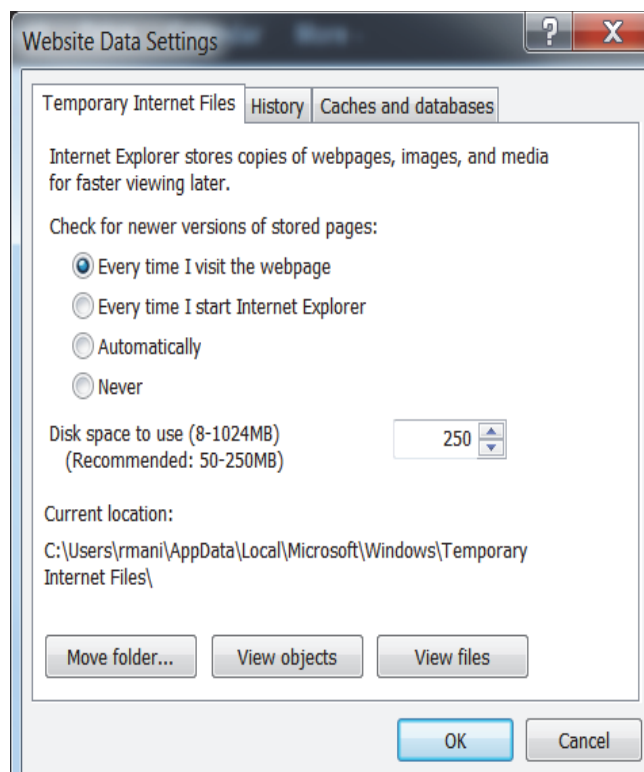
図 2: Microsoft Windows のインターネット オプション



2. [閲覧の履歴] で、[設定] をクリックします。

次のようなウィンドウが表示されます。

図 3: Web サイトのデータ設定



3. [Web サイトを表示するたびに確認する] オプションを選択します。

4. [OK] をクリックします。

これで、統計が変更されるたびにダッシュボードが更新されるようになります。

Mozilla Firefox では特別な設定は必要ありません。

Network Manager とは

Network Manager は、複数のコントローラを管理するフォーティネット製品です。

ESS、セキュリティ、VLAN、GRE、および RADIUS のプロファイルはすべて、Network Manager またはコントローラから設定できます。読み取り専用フィールドである Owner が NMS または controller のどちらであるかによって、プロファイルがどちらで設定されたのかを確認できます。プロファイルが Network Manager に属している場合、コントローラから変更や削除を行うことはできません。

プロファイルが Network Manager に属している場合は、Network Manager インターフェイスから変更 / 削除することを推奨します。何らかの理由で、コントローラから Network Manager にアクセスできない場合は、CLI の `nms-server unregister` コマンドを使用して Network Manager サーバからコントローラの登録を解除することを推奨します。

4 システム ファイルの管理

本章では、フォーティネット コントローラと共に利用できる全ファイルを管理するための単一インターフェイスを提供する、コントローラ ファイル システム (CFS) の使い方を説明します。本章は、以下の項で構成されています。

- [CFS について \(53 ページ\)](#)
- [Web UI によるファイルの管理 \(56 ページ\)](#)
- [設定ファイルの操作 \(60 ページ\)](#)
- [システム ファイルの操作 \(61 ページ\)](#)
- [システム イメージのアップグレード \(63 ページ\)](#)
- [ファイル システム コマンドのまとめ \(64 ページ\)](#)

CFS について

CFS を使用すると、コントローラのオペレーティング システムである FortiWLC (SD) とその設定ファイルを管理できます。

コントローラの操作に使用されるファイルは、コントローラのフラッシュ カード のディレクトリに置かれています。最初は、このフラッシュ カードには出荷時のオペレーティング システム (イメージと呼びます) が格納されていて、当然ながら、デフォルト設定にセットされています。通常の運用では、以下のような作業を実行する必要がでてくるでしょう。

- カスタム設定を設定し、設定ファイルにそれらの設定を保存する
- 設定ファイルをコントローラのバックアップ ディレクトリに保存する
- 設定ファイルをリモート ロケーションに保存して、より安全なバックアップを実現する、あるいは他のコントローラの設定の入力として活用する
- 既知の信頼できるバックアップ ファイルから設定をリストアする
- システムをデフォルト設定に戻す
- システムを新しいバージョンのオペレーティング システムにアップグレードする
- システムを前のバージョンのオペレーティング システムにダウングレードする
- 自動設定のためのスクリプトを実行する

これらの作業を行うには、CFS を使用してファイル进行操作します。CFS を使用すると、以下の作業が可能になります。

- ディレクトリ内のファイルに関する情報の表示
- ファイルの名前、サイズ、変更日などの情報を表示します。
- 異なるディレクトリへのナビゲーション
- 異なるディレクトリへの移動やディレクトリ内のファイルの表示が可能です。
- ファイルのコピー

CFS を使用すると、パス名によるコントローラ上のファイルのコピーや、リモート ファイルの操作が可能になります。URL (Uniform Resource Locator) を使用して、リモート ファイルの場所を指定します。URL は、WWW (World Wide Web) のファイルや場所の特定に広く使用されています。この URL 形式を使用して、リモート ファイル サーバのロケーションとの間でファイルのコピーや取得を実行できます。

- ファイルの削除

ローカル ディレクトリでの作業

コントローラのフラッシュ カードは、以下のディレクトリを使用して、システム ファイルを編成します。以下のローカル ディレクトリにアクセスできます。

ディレクトリ名	ディレクトリの内容
images	現行イメージが置かれているディレクトリであり、リモートで取得したアップグレード イメージを置いておくことができます
backup	バックアップの設定ファイルとデータベースが格納されているディレクトリ
ATS/scripts	AP ブートアップ スクリプトが格納されているディレクトリ
capture	パケット捕捉ファイルが格納されているディレクトリ

ディレクトリとファイルの情報の表示

pwd コマンドを使用すると、現在のディレクトリが表示されます。デフォルトでは、現行のワーキング ディレクトリは、以下の pwd コマンドで示すように、images です。

```
controller# pwd
images
```

ディレクトリの内容に関する詳しいリストを表示するには、dir コマンドを使用します。このコマンドは、オプションでディレクトリまたはファイル名を引数として受け付けます。

```
dir [[directory/]filename]
```

たとえば、images ディレクトリの内容を表示するには、以下のように入力します。

```
controller# dir
total 10
total 70
drwxr-xr-x   8 root    root      1024 Jan 30 11:00 meru-3.6-45
drwxrwxr-x   8 522    522      1024 Feb 21  2008 meru-3.6-46
-rw-r--r--   1 root    root      2233 Feb 19 02:07 meru.user-
diagnostics.Dickens.2008-02-19.02-07-17.tar.gz
-rw-r--r--   1 root    root      3195 Feb 19 02:17 meru.user-
diagnostics.Dickens.2008-02-19.02-17-17.tar.gz
-rw-r--r--   1 root    root      3064 Feb 21 00:50 meru.user-
diagnostics.Dickens.2008-02-21.00-50-50.tar.gz
lrwxrwxrwx   1 root    root        28 Feb 21 00:50 mibs.tar.gz -> meru-
3.6-46/mibs/mibs.tar.gz
-rw-r--r--   1 root    root     16778 Feb 21 0:50 pre-upgrade-config
-rw-r--r--   1 root    root     18549 Feb 21 00:53 script.log
-rw-r--r--   1 root    root     16427 Feb 21 00:53 startup-config
-rw-----   1 root    root      1915 Feb 21 0:50 upgrade.log
```

異なるディレクトリ内のファイルに関する情報を表示するには、ディレクトリ引数を以下のように使用します。

```
controller# dir ATS/scripts

total 4
-rwxr-xr-x   1 root    root        67 Feb 21  2008 dense-.scr
-rwxr-xr-x   1 root    root        25 Feb 21  2008 guard.scr
-rwxr-xr-x   1 root    root        82 Feb 21  2008 non-guard.scr
-rwxr-xr-x   1 root    root       126 Feb 21  2008 svp.scr
```

異なるディレクトリへの変更

cd コマンドを使用すると、コントローラの異なるディレクトリに移動します。

```
controller# cd backup
```

pwd コマンドを次のように使用して、現行のディレクトリの名前を表示します。

```
controller# pwd
backup
```

Web UI によるファイルの管理

ローカル ファイルは CLI でも管理できますが、FortiWLC (SD) Web UI では、[Maintenance] > [File Management] ボタンから便利な管理インターフェイスを利用できます。[File Management] ページには、以下のファイルのタイプごとのタブがあります。

- AP Init Script : AP ブートアップ スクリプトを管理する
- Diagnostics : 診断ファイルが含まれる
- SD Versions : コントローラに格納されているすべてのソフトウェア イメージ ファイル
- Syslog : システムの各種コンポーネントの保存された Syslog データ

それぞれのタブに関連する詳細については、以下の項を参照してください。






AP Init Script

ユーザが最初に File Management システムに移動したときに選択されるデフォルトのタブには、システムにインストールされているすべてのスクリプトが表示されますが、AP のブートアップ時に微調整できるように設計されています。以下の図 4 を参照してください。

図 4: [AP Init Script] テーブル

Software Image Library and Logs

AP Init Script
Diagnostics
SD versions
Patches
Syslog
Configuration

	Script Name	Last Modified Date	Size
			
	load-balance.scr	2016-05-23 17:36:10	79B
	trmtr.scr	2016-03-31 17:59:53	50B
	upgrade-SP.tar	2016-05-13 21:00:09	8MB

ブートスクリプトの横にあるラジオ ボタンをクリックし、画面の下にある以下に説明するボタンをクリックすると、そのブートスクリプトの操作を実行できます。

表 3: コマンド ボタン

ボタン	アクション
Refresh	表示されるスクリプトのリストを更新します。
New	[Add/Edit] ウィンドウを開きます。このウィンドウでは、新しいブート スクリプトを作成できます。
View	新しいウィンドウが開き、ブート スクリプトの内容が表示されます。
Edit	選択したスクリプトのコマンドやスクリプト名などを変更できます。
Delete	選択したスクリプトを削除します。
Import	ウィンドウが開き、ローカル ブート スクリプトを参照したり、それをコントローラにアップロードしたりできます。 注：アップロードできるのは、拡張子が “.txt” のファイルのみです。
Export	選択したスクリプトをローカル マシンにエクスポートします。

Diagnostics

[Diagnostics] タブには、コントローラによって生成されたすべての診断ファイルが表示されます。これらのファイルは圧縮形式であるため、ローカル マシンにダウンロードされたらファイルを解凍して、そのファイルに含まれるログを参照します。

図 5: [Diagnostics] タブ

Software Image Library and Logs ?

AP Init Script Diagnostics SD versions Patches Syslog Configuration			
<input type="checkbox"/>	Diagnostics File	Creation Date	Size
<input type="checkbox"/>			
<input type="checkbox"/>	forti-controller-diagnostics.CTET-Forti500D-Master.2016-05-06.20-33-38.tar.gz	2016-05-06 20:43:10	11MB
<input type="checkbox"/>	crash_channel_scan.pl.8.1-1-6_24May2016_11-35-22.tar.gz	2016-05-24 11:35:27	867KB

ファイルが解凍されたら、標準のテキスト エディタを使用して診断ログを参照できます。ログ ファイルをダウンロードするには、該当するファイルの隣のラジオ ボタンをクリックし、

[Export] をクリックします。下表に、画面のボタンによって実行される機能の説明を記載します。



表 4: コマンド ボタン

ボタン	アクション
Refresh	表示されるファイルのリストを更新します。
Export	選択したファイルをローカル マシンにエクスポートします。
Delete	選択したファイルを削除します。

Image

[Image] タブでは、コントローラに格納されている FortiWLC (SD) のイメージ ファイルを管理できます。これらのファイルはサイズがとて大きくなることがあるため、場合によっては、古いイメージを削除して、システム アップグレードを実行する必要があります。

図 6: [Image] タブ

Software Image Library and Logs 		
AP Init Script Diagnostics SD versions Patches Syslog Configuration		
<input type="checkbox"/>	Image Name	Size
		
<input type="checkbox"/>	8.1-1-6	189MB
<input type="checkbox"/>	8.1-1-4	189MB
<input type="checkbox"/>	8.1-1-5	197MB
<input type="checkbox"/>	8.1-1-7	189MB

下表に、システム ファイルの管理に使用できるボタンの詳細を記載します。

表 5: コマンド ボタン

ボタン	アクション
Refresh	表示されるファイルのリストを更新します。
Import	イメージ ファイルをローカル マシンからコントローラにアップロードできます。 注：コントローラのイメージ ファイルは、“tar” 形式である必要があります。
Delete	選択したファイルを削除します。

syslog

[Syslog] タブは、コントローラで生成され、格納された Syslog ファイルを簡単に表示および管理できるインターフェイスです。

図 7: [Syslog] タブ

Software Image Library and Logs ?

AP Init Script	Diagnostics	SD versions	Patches	Syslog	Configuration
----------------	-------------	-------------	---------	---------------	---------------

	Facility Name	Last Modified Date	Size(KB)
<input type="radio"/>	Security	05/24/2016 12:20:01	13
<input type="radio"/>	QoS	05/24/2016 11:48:48	1
<input type="radio"/>	System	05/24/2016 12:20:17	34
<input type="radio"/>	NMS	05/24/2016 12:00:01	1
<input type="radio"/>	Mobility	05/24/2016 11:48:48	1
<input type="radio"/>	Bulk Update	05/24/2016 11:48:48	1
<input type="radio"/>	Upgrade	05/24/2016 12:19:39	1
<input type="radio"/>	Per User Firewall	05/24/2016 11:55:15	1

Syslog ファイルは、“log” 形式で格納され、標準のテキスト エディタを使用して表示できます。いずれかのファイルをダウンロードして表示するには、該当するファイルの横にあるラジオ ボタンをクリックして、[Export] をクリックします。

表 6: コマンド ボタン

ボタン	アクション
Refresh	表示されるファイルのリストを更新します。
Export	選択したファイルをダウンロードおよび表示できます。

設定ファイルの操作

設定ファイルは、コントローラの機能を指示します。システムがデータベースからブートされるか、設定モードでユーザが CLI にコマンドを入力すると、設定ファイルの中のコマンドが CLI によって解釈されて、実行されます。CLI は、以下の 2 種類の設定ファイルを使用します。

- システム起動時に、起動データベース ファイル (startup-config) を実行する。
- 実行設定ファイル (running-config) に、ソフトウェアの現在の (実行中の) 設定を格納する。

起動設定ファイルが実行設定ファイルとは異なる場合があります。たとえば、設定を変更し、その変更をしばらくの間、評価してから、起動設定に保存する場合などがこれに当てはまります。

このような場合は、configure terminal コマンドを使用して設定を変更しますが、その設定を保存しないようにします。そして、その変更を永続的に組み込むと判断した段階で、copy running-config startup-config EXEC コマンドを使用 します。

現行の設定の変更

configure terminal EXEC コマンドを実行すると、実行設定を変更できます。コマンドはただちに実行されますが、保存はされません。変更を保存する方法については、「起動設定の変更」を参照してください。

表 7: 実行設定を変更する手順

コマンド	目的
controller# configure terminal	グローバル設定モードに入ります。
controller(config)#	実行設定に追加するコマンドを入力します。CLI はただちにこれらのコマンドを実行し、実行設定ファイルにも挿入します。

表 7: 実行設定を変更する手順

コマンド	目的
controller# copy running-config startup-config	実行設定ファイルを起動設定ファイルとして保存します。設定の変更をリブート後も持続させるには、実行設定を起動設定ファイルに保存する必要があります。
controller(config)# end または controller(config)# Ctrl-Z	設定セッションを終了し、EXEC モードを抜けます。注：Ctrl キーと Z キーを同時に押します。
controller(config)# Ctrl-C	すべての変更を取り消して、前のモードに戻ります。

起動設定の変更

設定の変更をリブート後も持続させるには、copy running-config startup-config EXEC コマンドを使用して、実行設定を起動設定にコピーします。

システム ファイルの操作

システム ファイルを操作するために、設定ファイルをリモート システムとの間でバックアップあるいは取得する必要がある場合もあるでしょう。リモート システムにアクセスするには、多くの場合、ユーザ名とパスワードが必要です。この項では、これらの作業を実行するためのコマンドの例をいくつか紹介します。

ネットワーク サーバのファイルの操作

ネットワーク サーバのファイルを指定するには、以下のいずれかの形式を使用します。

- ftp://<username>:<password>@server/filename
- scp://<username>:<password>@server/filename
- sftp://<username>:<password>@server/filename
- tftp://server/filename

server には、IP アドレスまたはホスト名を指定できます。username (ユーザ名) を指定すると、グローバル設定コマンド ip ftp username で指定したユーザ名より優先されます。password も、グローバル設定コマンド ip ftp password で指定したパスワードより優先されます。

指定した directory と filename は、ファイル転送の場合はディレクトリに対する相対形式、それ以外の場合は絶対形式になります。

以下の例では、セキュア FTP を使用して、ftp.fortinet.com という名前のサーバの meru-3.7-config という名前のファイルにアクセスしています。以下の例では、ユーザ名 admin、パスワード secret を使用して、このサーバにアクセスします。

```
controller# copy sftp://admin:secret@ftp.fortinet.com/meru-3.7-config<space>.
```

SCP (セキュア コピー) の場合は、sftp という接頭辞を scp に置き換えてください。

リモート ファイルの転送

FTP、SFTP、TFTP、SSH のいずれかのサーバのリモート ファイル システムで、以下の作業を実行できます。

- copy コマンドを使用して、コントローラとの間でファイルをコピーする
- dir コマンドを使用して、あるディレクトリのファイルのリストを表示する

リモート サーバへのファイルのコピー

たとえば、FTP を使用し、user1 というユーザで、images というローカル ディレクトリから server1 というサーバの /home/backup というリモート ディレクトリへ、jun01.backup.mbu というバックアップイメージをコピーするには、以下のように入力します。

```
controller# cd images
controller# dir
total 48
-rw-r--r-- 1 root root      15317 Jan  9 15:46 jun01.backup.mbu

controller# copy jun01.backup.mbu ftp://user1@server1/home/backup/.
FTP Password:
controller#
```

FTP の Password プロンプトに、user1 ユーザのパスワードを入力します。FTP の代わりに SCP を使用するには、次のように入力します。

```
controller# copy jun01.backup.mbu scp://user1@server1/home/backup/.
SCP Password:
```

リモート サーバのディレクトリ内容の表示

username に user1、password に userpass を使用し、server1 というサーバの /home/backup というリモート ディレクトリの内容を表示するには、以下のように入力します。

```
controller# dir ftp://user1:userpass@server1/home/backup
```

ユーザ名だけを指定してパスワードを指定しないと、パスワードを入力するための CLI プロンプトが表示されます。

```
controller# dir ftp://user1@server1/home/backup
FTP Password:
```

リモートのユーザ名とパスワードの設定

セキュアなリモート ファイル転送コマンドには、サーバに対する要求ごとにリモートのユーザ名とパスワードが必要です。CLI は、dir コマンドまたは copy コマンドで指定されたユーザ名とパスワードを使用して、リモート ファイル サーバの認証を行います。

セキュアなファイル転送コマンドのたびにユーザ名とパスワードを入力しなくてすむようにするには、ip ftp|sftp|scp コマンドを使用して、セッション中のこれらの値を設定できます。

たとえば、FTP ユーザ名を user1 に、FTP パスワードを userpass に設定するには、以下のように入力します。

```
controller# configure terminal
controller(config)# ip ftp username user1
controller(config)# ip ftp password userpass
controller(config)# ^Z
controller#
```

同様に、SCP ユーザ名を user1 に、SCP パスワードを userpass に設定するには、以下のように入力します。

```
controller# configure terminal
controller(config)# ip scp username user1
controller(config)# ip scp password userpass
controller(config)# ^Z
controller#
```

FTP のユーザ名とパスワードを前の例のように設定していれば、ここでは以下のように入力できます。

```
controller# dir ftp://server1/home/backup
```

システム イメージのアップグレード

コントローラは、FortiWLC (SD) の全ソフトウェアを含め、システム イメージがインストールされた状態で出荷されます。コントローラをブートすると、このイメージがロードされますが、新しいソフトウェア リリースが発表された場合などに、システム イメージのアップグレードを決断することもあるでしょう。

各リリースには、ドキュメント CD としてリリース ノート ファイルが付属し、異なるタイプのシステム設定を現行のリリースにアップグレードする方法が記載されています。システム

をアップグレードすることを選択した場合は、必ず、リリース ノートに記載されている最新の手順に従ってください。

ファイル システム コマンドのまとめ

以下のリストは、特権 EXEC モードで利用できる、ファイル システム コマンドです。

コマンド	目的
controller> cd [filesystem]	フラッシュ メモリ デバイスにデフォルト ディレクトリを設定します。ディレクトリ名を指定しないと、デフォルトのディレクトリは images に設定されます。指定可能なディレクトリは以下のとおりです。 images: アップグレード イメージを含むディレクトリ ATS/scripts: AP ブート スクリプトが格納されているディレクトリ backup: データベースのバックアップ イメージが格納されているディレクトリ
controller> pwd	現在の作業ディレクトリを表示します。
controller> dir [filesystem:][filename]	ファイル システムのファイルのリストを表示します。対象となるのは、cd コマンドで指定されたディレクトリ、または FTP の URL が参照するリモート ディレクトリのいずれかです。
controller# delete filename controller# delete directory:filename controller# delete flash: image	ファイル システムからファイルを削除するか、フラッシュ メモリからアップグレード イメージを削除します。directory パラメータを使用すると、異なるフォルダからファイルを削除できます。
controller# show flash	コントローラのフラッシュ メモリに格納されている各バージョンのイメージ ファイルを表示します。
controller# rename old new	ファイル名を old から new に変更します。
controller# show running-config	実行設定ファイルの内容を表示します。
controller# more running-config	実行設定ファイルの内容を表示します。show running-config のエイリアスですが、画面がいっぱいになると、キーを押して画面をスクロールするようユーザに通知されるという点が異なります。こうすることで、画面全体を 1 度にスクロールしなくても、1 度に 1 画面ずつ設定を表示できます。

コマンド	目的
controller# copy running-config ftp sftp scp:[[[//username:password]@location/directory]/filename]	<p>実行設定ファイルを FTP、SFTP、または SCP サーバに、たとえば次のようにコピーします。</p> <pre>controller# copy running-config ftp://user1:userpass@server1/jan01-config</pre> <pre>controller# copy running-config scp://user1:userpass@server1/jan01-config</pre>
controller# copy running-config startup-config	<p>実行設定を起動設定に保存することで、設定を永続的なものにします。一連の設定コマンドを実行し、その変更をリブート後も持続させたい場合には、必ずこのコマンドを実行してください。</p>
controller# reload ap [id] all controller default	<p>コントローラや指定した AP をリブートします。</p> <p>ap キーワードを指定するとすべての AP がリブートし、id を指定するとその id の AP がリブートします。</p> <p>all キーワードを指定すると、現行の起動設定を使用して フォーティネット コントローラとすべての AP がリブートされます。</p> <p>controller キーワードを指定すると、現在の起動設定を使用してコントローラがリブートされます。</p> <p>default キーワードを指定すると、出荷時のデフォルト起動設定を使用してコントローラとすべての AP がリブートされます。</p>
controller# upgrade feature <i>version</i>	<p>指定した機能でシステムをアップグレードします。</p>
controller# upgrade system <i>version</i>	<p>コントローラとすべての AP のシステム イメージを、version で指定されたバージョンにアップグレードします。</p>
controller# upgrade ap <i>version</i> same [id range all]	<p>コントローラが実行しているシステム ソフトウェアと同じバージョンに、アクセス ポイントのイメージをアップグレードします。</p> <p><i>id</i> : コントローラが実行されているシステム ソフトウェアと同じバージョンに、特定の ID のアクセス ポイントをアップグレードします。</p> <p><i>range</i> : リストで (カンマとハイフンを使用し、スペースやワイルドカードは使用しないで) 指定した範囲の AP をアップグレードします。AP ID は、昇順にリストに記述する必要があります。</p> <p><i>all</i> : コントローラが実行されているシステム ソフトウェアと同じバージョンに、すべてのアクセス ポイント イメージをアップグレードします。</p>

コマンド	目的
controller# downgrade system <i>version</i>	コントローラとすべての AP のシステム イメージを、version で指定されたバージョンにダウングレードします。このコマンドを実行すると、すべてのローカル ユーザとグループをシステムから削除するよう要求されます。
controller# run <i>script</i>	指定されたスクリプトを実行します。スクリプトが現行ディレクトリにある場合は、相対パス名を指定します。それ以外の場合は、フルパス名を指定する必要があります。スクリプトは、images、ATS/scripts、または backup のいずれかに置かれている必要があります。

パッチのアップグレード

パッチをインストール / アンインストールするオプションが追加され、さらにパッチの内容について詳細を表示することも、コントローラにインストールされているパッチの履歴を取得するのも容易になりました。これらの新しいオプションは、コントローラの Web UI と CLI から利用できます。

Web UI の使用

パッチ管理のオプションは、**[Maintenance] > [File Management] > [Patches]** タブで利用できます。コントローラにコピーされているパッチ ビルド ファイルがある場合は、このページのリストに表示されます。特定のオプションについては、パッチ ファイルを選択し、ページ下部のオプションをクリックします。

1. パッチのリスト

Software Image Library and Logs ?				
<div> AP Init Script Diagnostics SD versions Patches Syslog Configuration </div>				
<input type="checkbox"/>	Patch Name	Creation Date	Size	Currently Installed
<input type="checkbox"/>				
<input type="checkbox"/>	8.1-1-4-patch-coordCPUprofiling	2016-05-17 17:07:13	5.2MB	No

2. パッチの詳細

<input type="checkbox"/>	Patch Name	Creation Date	Size	Currently Instal
<input checked="" type="checkbox"/>	8.0-0dev-50-patch-bug1234_bug1236	2015-07-22 14:26:44	65KB	No
<input type="checkbox"/>	8.0-0dev-50-patch-bug1234	2015-07-22 14:12:21	65KB	No
<input type="checkbox"/>	8.0-0dev-50-patch-2015.07.22-17h.12m.09s	2015-07-22 20:59:51	7.1MB	No
<input type="checkbox"/>	8.0-0dev-50-patch-bug1234_bug1235	2015-07-22 16:31:48	65KB	No
<input type="checkbox"/>	8.0-0dev-51-patch-bug1234_bug1235	2015-07-24 02:53:49	Patch Content/Details Bug Number	
<input type="checkbox"/>	8.0-0dev-51-patch-bug1234	2015-07-24 15:52:32		

Patch Content/Details

Bug Number	Summary
37405	summary of bug 37405
37310	summary of bug 37310

File Path	Md5sum
/opt/meru/etc/coord.config	ed04e8b2dca901d1ce61f9160bfdb0a5

Close

Refresh

Details

History

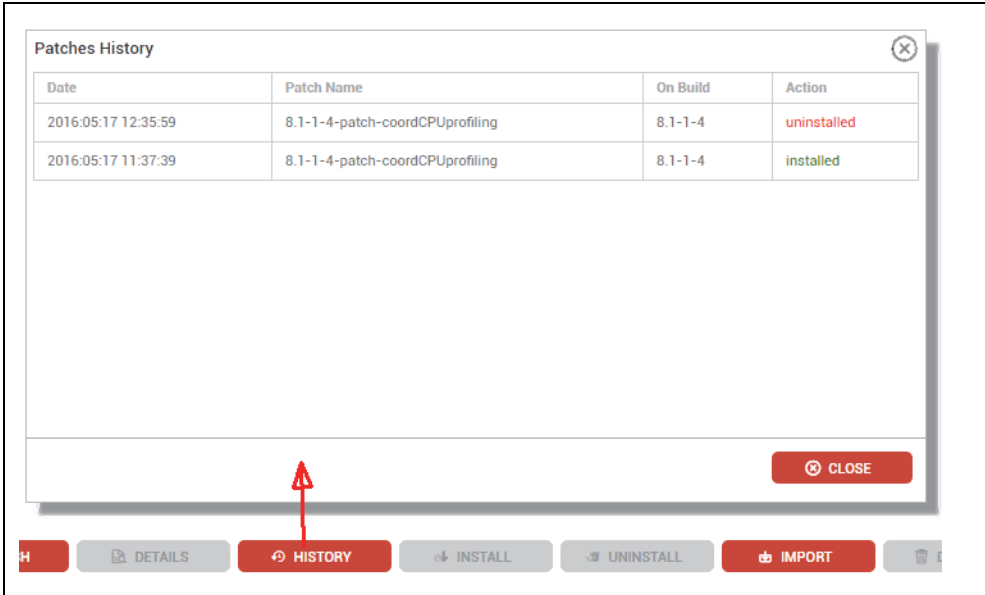
Install

Uninstall

Import

Delete

3. パッチの履歴



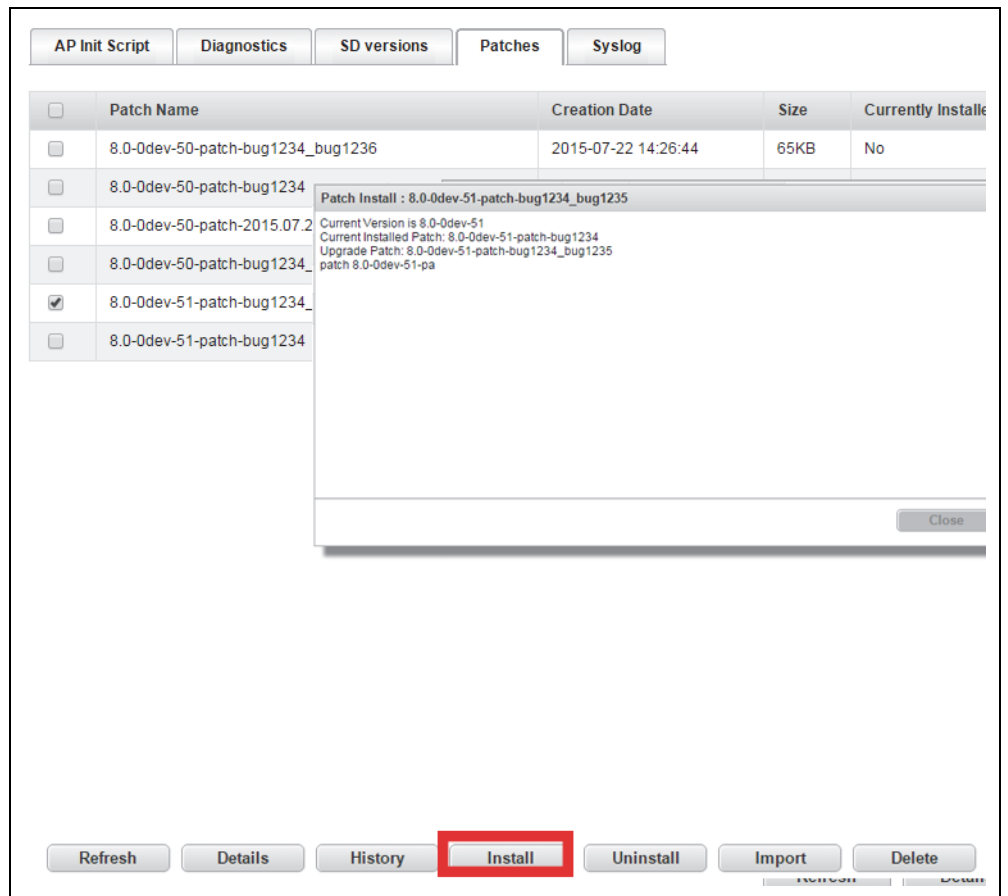
Patches History

Date	Patch Name	On Build	Action
2016.05.17 12:35:59	8.1-1-4-patch-coordCPUprofiling	8.1-1-4	uninstalled
2016.05.17 11:37:39	8.1-1-4-patch-coordCPUprofiling	8.1-1-4	installed

⊕ CLOSE

H **DETAILS** **HISTORY** **INSTALL** **UNINSTALL** **IMPORT** **🗑**

4. パッチのインストール



CLI の使用

1. show patches

コントローラにコピーされているパッチ ビルドのリストを表示します。

#show patches

8.0-0dev-51-patch-bug1234 [installed]

8.0-0dev-50-patch-bug1234_bug1236

8.0-0dev-50-patch-bug1234

8.0-0dev-50-patch-2015.07.22-17h.12m.09s

8.0-0dev-50-patch-bug1234_bug1235

```
8.0-0dev-51-patch-bug1234_bug1235
```

```
8.0-0dev-51-patch-bug1234
```

2. show patch installed

コントローラに現在インストールされているパッチを表示します。

```
controller(15)# show patch installed
```

```
8.0-0dev-51-patch-bug1234
```

3. show patch history

コントローラにインストールおよびアンインストールされた全パッチの履歴を表示します。

```
controller(15)# show patch history
```

```
2015:07:24 01:51:13: uninstalled 8.0-0dev-50-patch-bug1234 on build 8.0-0dev-51
```

```
2015:07:24 01:54:13: installed 8.0-0dev-51-patch-bug1234_bug1235 on build 8.0-0dev-51
```

```
2015:07:24 01:56:39: uninstalled 8.0-0dev-51-patch-bug1234_bug1235 on build 8.0-0dev-51
```

```
....<snipped>....
```

```
2015:07:24 14:54:50: uninstalled 8.0-0dev-51-patch-bug1234 on build 8.0-0dev-51
```

4. show patch details <パッチ名>

このパッチで提供されるバグ修正のリストを表示します。

```
controller(15)# show patch details 8.0-0dev-50-patch-bug1234
```

```
8.0-0dev-50-patch-bug1234
```

```
patch is revertable
```

```
bugs:
```

```
37405: summary of bug 37405
```

```
controller(15)#
```

5. show patch contents <パッチ名>

パッチビルドの MD5 チェックサムを表示します。

```
controller(15)# show patch contents 8.0-0dev-50-patch-bug1234
```

```
8.0-0dev-50-patch-bug1234
```

```
files:
```

```
/opt/meru/etc/coord.config: 3d4c720265e21a53dfafe2a484e8bf11
```

6. patch uninstall <パッチ名>

コントローラからパッチ ビルドをアンインストールするには、このコマンドを使用します。

```
controller(15)# patch uninstall
```

7. バックアップから元の状態に戻す

```
cp -f /data/.patch-backup//meru-8.0-0dev-51-patch-bug1234/coord.config /opt/  
meru/etc/coord.config
```

Reverting from backup done.

5 システムの管理

本章では、コントローラの設定とシステムの管理の手順を説明します。本章は、以下の項で構成されています。

- [セットアップ時のコントローラの基本パラメータの設定 \(73 ページ\)](#)
- [Web UI からのコントローラ パラメータの設定 \(74 ページ\)](#)
- [CLI からのコントローラ パラメータの設定 \(75 ページ\)](#)
- [システム ライセンスの設定 \(80 ページ\)](#)
- [FortiWLM Location Manager の設定 \(82 ページ\)](#)
- [802.11n ビデオ サービス モジュール \(ViSM\) \(83 ページ\)](#)
- [AeroScout の使用 \(84 ページ\)](#)
- [FortiWLC \(SD\) の通信ポート \(94 ページ\)](#)
- [コントローラ ベースの DHCP サーバの設定 \(95 ページ\)](#)
- [Fortinet Service Control の使用 \(98 ページ\)](#)
- [IPv6 クライアントのサポート \(103 ページ\)](#)
- [Spectrum Manager へのアクセス \(107 ページ\)](#)

セットアップ時のコントローラの基本パラメータの設定

コントローラの基本パラメータの設定は、レベル 15 の権限があるユーザが、対話型 setup スクリプトを使用して、新しいそれぞれのコントローラのセットアップを実行します。

- 国の設定
- コントローラ の場所
- ホスト名
- admin と guest のパスワード
- 動的 IP アドレスまたは固定 IP アドレスとネットマスク
- タイムゾーン
- DNS サーバ名

- ゲートウェイ サーバ名
- NTP (Network Time Protocol) サーバ

setup スクリプトを開始するには、特権 EXEC プロンプトから、「setup」と入力します。setup コマンドを使用するセッション例については、『*FortiWLC (SD) 入門ガイド*』の「初期セットアップ」の章を参照してください。

Web UI からのコントローラ パラメータの設定

既存のコントローラを設定するには、[Configuration] > [Devices] > [Controller] > [select a controller] > [Settings] をクリックします。以下のパラメータは、レベル 10 の権限で、Web UI から設定できます。

- Description (説明)、Location (場所)、Contact (連絡先) などのコントローラを認識し、追跡するための情報
- AP をコントローラが自動アップグレードするかどうか
- DHCP サーバのアドレスと DHCP リレー パススルー (パケットを DHCP サーバに実際に渡すかどうか)
- 統計ポーリング間隔と監査ポーリング間隔 (コントローラによるデータの更新に影響します)
- 他のスクリプトが指定されなかった場合に AP で実行する、デフォルトの AP 初期化スクリプト (bootscript)
- 識別に使用するコントローラのインデックス番号 (この ID を変更するとコントローラがリポートされます)
- コントローラが AeroScout ロケーション エンジンとやり取りして、関連する AP が AeroScout タグを提供することでリアルタイムのアセット追跡が提供されるかどうか
- FastPath モードを使用するかどうか。FastPath モードは、パケットがイーサネット インターフェイスを移動する速度を、IP パケット ストリームの識別に基づいてアクセラレートします。FastPath が有効な場合、IP パケット ストリームの先頭がコントローラによって処理され、同じストリームの後続のすべてのパケットは、コントローラでは処理されずに、最初のパケットの配列に従って転送されます。これによって、コントローラ処理の負荷が大幅に軽減されます。
- ボンディング モードは MC4200、MC5000、および MC6000 モデルに影響します。1 つのボンディングによって、すべてのイーサネット ポートが 1 つのポートに結合され、スループットが向上します。デュアル ボンディングでは、コントローラに 2 つのポートが設定されます。
- AP400 または AP1000 の仮想セルは、いずれのコントローラ設定でも決定されません。
- DFS (Dynamic Frequency Selection) が強制されるかどうか。米国のインストール環境では、DFS が強制されると、チャンネル 52 ~ 64 (5.25 ~ 5.35 GHz)、100 ~ 116 (5.47 ~

5.725 GHz)、および 136 ~ 140 (5.68 ~ 5.70 GHz) が DFS 規制に準拠するようになり、これらのチャンネルで干渉からレーダーが保護されます。

- ステーションがアクティブでない状態でクライアントがタイムアウトになるまでの分数を、Station Aging Out Period で設定します。

Web UI による UDP ブロードキャストの設定

Web UI コマンドで、一度にアップストリームとダウンストリームのトラフィックのすべての UDP ポートを有効にできます。大量のブロードキャストが発生してネットワーク停止につながる恐れがあるため、本番ネットワークでこの機能を有効にすることはお勧めしません。この機能は、テスト目的でのみ提供されます。

すべての UDP ブロードキャスト ポートを有効にする前に、それぞれの ESS (「ESS の設定」の章を参照) を特定の VLAN (「VLAN の設定」の章を参照) に割り当てる必要があります。デフォルトの VLAN に複数の ESS が存在し、すべての UDP ブロードキャスト ポートを有効にすると、動作しません。

すべてのポートの UDP ブロードキャスト アップストリーム/ダウンストリームを設定するには、次の手順を実行します。

1. [Configuration] > [Devices] > [System Settings] をクリックします。
2. [UDP Broadcast Ports] タブをクリックします。
3. 設定する UDP ブロードキャスト モードのタイプ (トンネル モードまたはブリッジ モード) を決定し、そのタブをクリックします。
4. [Add] をクリックします。
5. 設定する UDP ブロードキャスト ルールのタイプ、[Upstream] または [Downstream] をチェックします。
6. [UDP Port Number] を 1 ~ 65355 の範囲で指定し、[Save] をクリックします。
これで、[UDP Broadcast Port] リストにポート番号が表示されるようになります。

設定するすべてのポートについて、以上の手順を実行します。

CLI からのコントローラ パラメータの設定

システムとシステム パスワードの CLI からのリセット

システム ユーザ「admin」と「guest」のパスワードを、システム ブート時にリセットできません。コントローラ プロンプトの“accepting reset request”が表示されたら、「pass」と入力してパスワードをリセットします。

システム全体をデフォルト値にリセットするには、システム値をリセットするプロンプトに「reset」と入力します。

ワイヤレス クライアントの CLI からのコントローラへのアクセスの制限

ワイヤレス クライアントがコントローラ管理ユーティリティにアクセスしないようにするには、管理者が no management access コマンドを使用します。ワイヤレスの管理アクセスがブロックされていると、ワイヤレス クライアントからコントローラに送られるパケットは、キャプティブ ポータルに使用されるものを除くすべてがドロップされます。

コントローラへのワイヤレス アクセスを削除するには、次のコマンドを入力します。

```
controller(config)# no management wireless
```

管理ステータスをチェックするには、show controller コマンドを使用します。出力の最終行付近の Management by wireless stations: に、on または off の値が表示されます。

```
mc3200# show controller
Global Controller Parameters

Controller ID : 1
Description : controller
Host Name : MC3200
Uptime : 05d:17h:10m:59s
Location :
Contact :
Operational State : Enabled
Availability Status : Online
Alarm State : Major
Automatic AP Upgrade : on
Virtual IP Address : 172.29.0.137
Virtual Netmask : 255.255.192.0
Default Gateway : 172.29.0.1
DHCP Server : 10.0.0.240
Statistics Polling Period (seconds)/0 disable Polling : 60
Audit Polling Period (seconds)/0 disable Polling : 60
Software Version : 6.0.SR1-4
Network Device Id : 00:90:0b:23:2e:d3
System Id : 08659559054A
Default AP Init Script :
DHCP Relay Passthrough : on
Controller Model : MC3200
Region Setting : Unknown
Country Setting : United States Of America

Manufacturing Serial # : 4911MC32009025
Management by wireless stations : on
Controller Index : 0
```

```
FastPath Mode : on
Bonding Mode : single
Station Aging Out Period(minutes) : 2
Roaming Domain State : disable
Layer3 Routing Mode : off
```

ワイヤレス クライアントへのアクセスを再び有効にするには、management wireless コマンドを使用します。

```
controller(config)# management wireless
```

QoS ルールによる有線クライアントからコントローラへのアクセスの制限

有線ネットワーク デバイスからコントローラへのアクセスを制御するには、qosrules コマンドを使用して、ルール ベースの IP ACL リストを設定します。本項では、いくつかの種類の設定の qosrule の例を説明します。

以下の例は、192.168.1.7 のホスト以外のすべてのデバイスからのコントローラ (192.168.1.2) への管理アクセスをブロックします。srcip、dstip、srcport、dstport、netprotocol、または packet min-length がルールに対して設定されていると、マッチ タグが有効になります。

ホスト 192.168.1.7 からコントローラへの TCP/UDP によるアクセスを許可します。

```
controller(config)# qosrule 20 netprotocol 6 qosprotocol none
controller(config-qosrule)# netprotocol-match
controller(config-qosrule)# srcip 192.168.1.7
controller(config-qosrule)# srcip-match
controller(config-qosrule)# srcmask 255.255.255.255
controller(config-qosrule)# dstip 192.168.1.2
controller(config-qosrule)# dstip-match
controller(config-qosrule)# dstmask 255.255.255.255
controller(config-qosrule)# action forward
controller(config-qosrule)# end
controller(config)# qosrule 21 netprotocol 17 qosprotocol none
controller(config-qosrule)# netprotocol-match
controller(config-qosrule)# srcip 192.168.1.7
controller(config-qosrule)# srcip-match
controller(config-qosrule)# srcmask 255.255.255.255
controller(config-qosrule)# dstip 192.168.1.2
controller(config-qosrule)# dstip-match
controller(config-qosrule)# dstmask 255.255.255.255
controller(config-qosrule)# action forward
controller(config-qosrule)# end
```

以下の qosrule を指定すると、キャプティブ ポータル機能を使用している場合に、ワイヤレス クライアントが TCP ポート 8080/8081 でコントローラにアクセスできるようになります。

```
controller(config)# qosrule 22 netprotocol 6 qosprotocol none
controller(config-qosrule)# netprotocol-match
controller(config-qosrule)# srcip <subnet of wireless clients>
controller(config-qosrule)# srcip-match
controller(config-qosrule)# srcmask <netmask of wireless clients>
controller(config-qosrule)# dstport-match on
controller(config-qosrule)# dstip 192.168.1.2
controller(config-qosrule)# dstip-match
controller(config-qosrule)# dstmask 255.255.255.255
controller(config-qosrule)# dstport 8080
controller(config-qosrule)# action forward
controller(config-qosrule)# end
```

```
controller(config)# qosrule 23 netprotocol 6 qosprotocol none
controller(config-qosrule)# netprotocol-match
controller(config-qosrule)# srcip <subnet of wireless clients>
controller(config-qosrule)# srcmask <netmask of wireless clients>
controller(config-qosrule)# dstport-match on
controller(config-qosrule)# dstip 192.168.1.2
controller(config-qosrule)# dstip-match
controller(config-qosrule)# dstmask 255.255.255.255
controller(config-qosrule)# dstport 8081
controller(config-qosrule)# action forward
controller(config-qosrule)# end
```

以下の qosrule を指定すると、すべてのホストが TCP/UDP を使用してコントローラにアクセスできなくなります。

```
controller(config)# qosrule 24 netprotocol 6 qosprotocol none
controller(config-qosrule)# netprotocol-match
controller(config-qosrule)# dstip 192.168.1.2
controller(config-qosrule)# dstip-match
controller(config-qosrule)# dstmask 255.255.255.255
controller(config-qosrule)# action drop
controller(config-qosrule)# end
```

```
controller(config)# qosrule 25 netprotocol 17 qosprotocol none
controller(config-qosrule)# dstip 192.168.1.2
controller(config-qosrule)# dstip-match
controller(config-qosrule)# dstmask 255.255.255.255
controller(config-qosrule)# action drop
controller(config-qosrule)# end
```

CLI からの UDP ブロードキャストの設定

CLI コマンドで一度にアップストリームとダウンストリームのトラフィックのすべての UDP ポートを有効にできます。大量のブロードキャストが発生してネットワーク停止につながる恐れがあるため、本番ネットワークでこの機能を有効にすることはお勧めしません。この機能は、テスト目的でのみ提供されます。

すべての UDP ブロードキャスト ポートを有効にする前に、それぞれの ESS (「ESS の設定」の章を参照) を特定の VLAN (「VLAN の設定」の章を参照) に割り当てる必要があります。デフォルトの VLAN に複数の ESS が存在し、すべての UDP ブロードキャスト ポートを有効にすると、動作しません。

すべてのポートの UDP ブロードキャスト アップストリーム/ダウンストリームを設定するには、次の 2 つの CLI コマンドを使用します。

```
default# configure terminal
default(config)# ip udp-broadcast upstream all-ports selected
default(config)# ip udp-broadcast downstream all-ports on
default(config)# end
```

すべてのポートに設定されている UDP ブロードキャスト アップストリーム/ダウンストリームを表示するには、次の 2 つの CLI コマンドを使用します。

```
default# show ip udp-broadcast upstream all-ports
Upstream UDP Broadcast All Ports
UDP All Ports : on
default#
default# show ip udp-broadcast downstream all-ports
Downstream UDP Broadcast All Ports
UDP All Ports : selected
default#
```

アップストリームまたはダウンストリームのいずれかに現在設定されているブロードキャスト ポートを表示するには、show ip udp-broadcast [downstream/downstream-bridged/upstream/upstream-bridged] を使用します。

CLI からの時間サービスの設定

フォーティネットでは、NTP (Network Time Protocol) サーバを使用してシステム クロックを同期するようコントローラを設定することをお勧めします。そうすることで、システム時間の精度が保たれ、他のシステムと統一が図られます。システム時間が正確で統一されていることは、キー管理や存続時間の制御のパラメータとしてタイムスタンプを使用する、アラーム、トレース、システム ログ、および暗号化のようなアプリケーションにとって重要です。さらに、ネットワークの監視、測定、制御に加えて、侵入の検出、隔離、ロギングにも正確なクロックが必要です。

最初のシステム設定で、setup スクリプトから NTP サーバの IP アドレスの入力を求めるプロンプトが表示されます。そこで NTP サーバの IP アドレスを入力しなかった場合、または割り当てたサーバをその後に変更したい場合には、ntp server コマンドの後に、ntp sync コマンドを使用できます。

- 設定された NTP サーバに対して定期的に自動同期するには、start-ntp コマンドを使用します。

時間サーバとして指定できる NTP サーバがいくつか存在します。www.ntp.org サイトに、使用できるサーバのリストが記載されています。

いずれかのサーバを NTP サーバとして設定するには、以下のコマンドを使用します。

```
ntp server ip-address
```

ip-address は、クロック同期に使用する NTP サーバの IP アドレスです。



システムクロックの同期に NTP サーバを使用しない場合は、calendar set コマンドを使用して手動でシステム時間を設定できます。

CLI コントローラ インデックスの設定

コントローラ インデックスを CLI から設定するには、以下のコマンドを使用します。

```
ramecntrl(0)# configure terminal
ramecntrl(0)(config)# controller-index 22
ramecntrl(0)(config)# exit
```

インデックスを変更すると、コントローラがリブートされます。

システム ライセンスの設定

ライセンスはコントローラのファームウェアに組み込まれており、個々のコントローラに対応する、フォーティネットが生成したライセンスファイルを使用することで、有効になります。これらのライセンスファイルは、www.merunetworks.com/license から入手できます。



ユーザは GRE、MESH、PUF のライセンスを購入する必要はありません。

CLI によるライセンスの設定

CLI でライセンスを表示するには、以下のコマンドを使用します。

```
controller# show controller
controller# show license
controller# show license-file active
```

以下のいずれかのオプション機能を有効にする予定がある場合は、そのためのライセンスが必要です。

- 3 台以上の AP
- N+1 (3 台以上のコントローラ)
- ユーザごとのファイヤウォール
- GRE トンネル
- デュアル ABG
- メッシュ / ワイヤレス

Web UI によるライセンスの設定

GUI でライセンスを表示するには、[Maintenance] > [Licensing] > [View License] をクリックします。GUI を使用してライセンスをインポートするには、[Maintenance] > [Licensing] > [Import License] をクリックし、指示に従います。既存のライセンスを表示するには、[Maintenance] > [Licensing] > [View License] をクリックします。

以下の CLI コマンドは、192.168.1.10 の FTP サーバのライセンス ファイル 17331.lic をアクティブな mc3200 コントローラにインポートします。

```
controller# configure terminal
controller(config)# license ftp://admin:admin@192.168.1.10/license17331.lic
active
controller(config)# end
```

show license コマンドを使用して、システム ライセンスのステータスを表示します。

Feature Name	CtlrStatus	LicenseType	Expiry Date	TotalCount	InUse
controller	active	permanent	-	1	1
ap	active	permanent	-	30	2
DUAL_A_B_G	active	permanent	-	30	1
N_PLUS_1	active	permanent	-	5	0
PER_USER_FW	active	permanent	-	1	1
GRE_TUNNELS	active	permanent	-	1	1
11n_upgrade	active	trial	05/02/2010	1	1

License Table(7)

アクセス ポイントのサイト ライセンス

フォーティネットのアクセス ポイント ライセンスは、アクセス ポイントの追加ライセンスを購入しなくても、コントローラ全体にわたって使用できるようになりました。コントローラにライセンス ファイルをインポートすることで、コントローラ間でアクセス ポイントを移動させることができます。Fortinet FortiWLC (SD) 7.0 にアップグレードすると、この機能はフォーティネットのすべてのアクセス ポイントで自動的に有効になります。



このライセンス ポリシーは、FortiWLM、FortiConnect、Spectrum Manager では適用されません。

ライセンスに関するこの新しい機能拡張に伴い、次の CLI コマンドと GUI ページが変更されています。

CLI コマンドの変更点

- `show license-file <active|standby>` **変更後** -> `show license-file`
コントローラに含まれているライセンス ファイルをチェックする場合に使用するコマンドです。
- `license ftp://<ftp-server>/<license-file> <active|standby>` **変更後** -> `license ftp://<ftp-server>/<license-file>`
ライセンスをインポートする場合に使用するコマンドです。

FortiWLM Location Manager の設定

Location Manager は、リリース 3.7 以降でサポートされています。

CLI での設定

次の例では、Location on という名前の packet-capture-profile をコントローラに作成し、AP 16 から直接捕捉したパケットをポート #9177 の Location Manager に転送します。ポート 9177 は、L3 モードで到着するパケットを Location Manager がリスンするポートです。

```
MC3K-1#  
MC3K-1# configure terminal  
MC3K-1(config)# packet-capture-profile Location  
MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 9177  
MC3K-1(config-pcap)# ap-list 16  
MC3K-1(config-pcap)# exit
```



```
MC3K-1(config)# exit
MC3K-1# show packet-capture-profile Location
AP Packet Capture profiles
```

```
Packet Capture Profile Name      : Location
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3              : 13
Destination IP Address           : 1.1.1.1
UDP Destination Port             : 9177
Destination MAC for L2 mode      : 00:00:00:00:00:00
Rx only/Tx only/Both            : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                : 10
Token Bucket Size                : 10
AP Selection                     : 16
Extended Filter String           :
Interface List                   :
Packet Truncation Length         : 82
Rate Limiting                   : off
Capture frames sent by other APs in the network : on
MC3K-1#
```

packet-capture-profile コマンドの詳しい説明については、『*FortiWLC (SD) 設定ガイド*』のトラブルシューティングの章を参照してください。

802.11n ビデオ サービス モジュール (ViSM)

ビデオ ストリーミングには、遅延と損失が少なく、データのスループットが高いという要件が求められます。Fortinet Video Service Module™ (ViSM) は、オプションでライセンスが付与されるソフトウェア モジュールであり、遅延、レイテンシ、ジッタを最小限に抑えることで、802.11 に予測可能なビデオ パフォーマンスを提供します。混在トラフィックにおいても持続可能な優れたデータ速度に対応し、ビデオや音声の送受信の同期が可能です。

ViSM には、アプリケーション対応のスケジューリング、ビデオの同期化、クライアントのマルチキャスト グループ管理などのユニキャストおよびマルチキャストのビデオを最適化するメカニズムも追加されています。次のような機能を備えています。

- 安定性の高い優れたスループットにより、予測可能なパフォーマンスと安定したユーザ体験を提供します。
- アプリケーション対応の優先順位設定によって、ビデオ ストリームのビデオのコンポーネントを同期化し、アプリケーションの重要度に基づき、各フレームを配信します。
- マルチキャスト グループ管理では、クライアントがマルチキャスト グループのメンバーである仮想ポートのみへの配信を最適化します。

- ビデオ向けに最適化されたシームレスなハンドオフによって、マルチキャスト配信ツリーを再ルーティングすることで、アクセス ポイント間の送信時のビデオ フレームの損失を回避し、損失なしのモバイル ビデオを保証します。
- ユーザとロールに基づくポリシー強制によって、アプリケーション動作のきめ細かい制御を可能にします。
- 仮想化によって、どのクライアントがどのアプリケーションを実行しているのかが明確になります。

ViSM の実装

仮想ポートは既に、マルチキャストからユニキャストの転送に変更されています。ViSM によって、クライアントごとの IGMP スヌーピングが転送に追加されます。そのため、ViSM を実装するには、IGMP スヌーピングをオンにします。IGMP スヌーピングを制御する CLI コマンドについては、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。現段階で、ViSM ライセンスは強制されません。

AeroScout の使用

AeroScout System バージョン 3 (バージョン 2 ではありません) 製品は、FortiWLC と、AP400、A822、AP832、FAP-U421EV、FAP-U423EV、および AP1000 モデルで動作し、タグ付けされたアセットの特定と追跡が可能で、プロセスの自動化や盗用防止などの直接的なメリットがもたらされます。タグは、小型でバッテリーによって給電される、機器や個人に取り付けられるデバイスです。AeroScout で利用できる各種タグに関する詳細については、AeroScout の Web サイトを参照してください。

AeroScout タグは、アクセス ポイントには関連付けられず、代わりに、予め設定された間隔で、またはイベントがトリガされた時 (タグが動作する、ボタンが押されるなど) に、ビーコン シグナルが送信されます。AeroScout から送信されるメッセージをアクセス ポイントが受信し、RSSI 値やシグナル強度の測定値などの追加情報が付加されて、AeroScout Engine に転送されます。AeroScout Engine は、タグの正確な場所を計算します。

タグのレポートは、アクセス ポイントの通常の処理に影響せず、サポート対象のすべてのモード (802.11a/b/g 通信) で実行されます。AeroScout タグには IP アドレスもなく、送受信という観点からは単方向であり、標準の Wi-Fi メッセージを受け取りません。

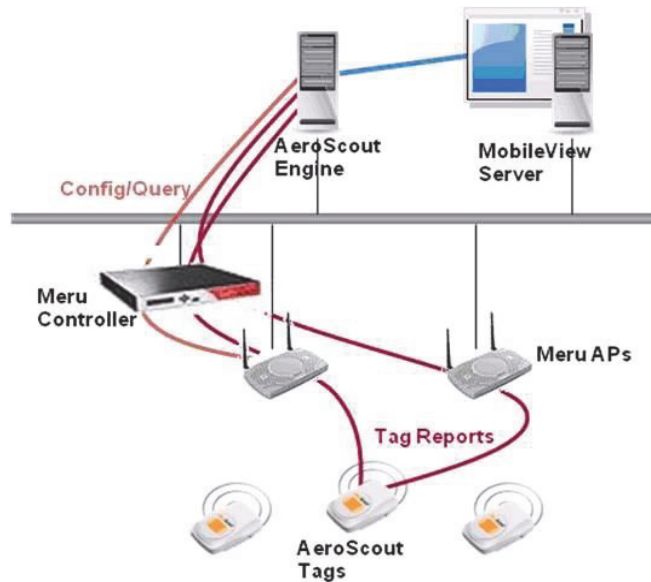
タグ シグナルを処理し、AeroScout Engine と通信する AP の場合、AeroScout Engine と IP のインターフェイス プロトコルがアクセス ポイントに実装されている必要があります。85 ページの [図 8](#) に、AeroScout ソリューションのアーキテクチャを図示します。AeroScout の実装で発生するハイレベルのプロセスは、以下のとおりです。

- AeroScout タグが、短いワイヤレス メッセージを定期的に送信します。

- このシグナルを、AeroScout ソフトウェアが動作する FortiWLC に接続されているアクセス ポイントが受信し、このシグナルは、測定されたシグナル強度と一緒に AeroScout Engine に送信されます。
- AeroScout Engine は、シグナル強度を使用して、報告された場所の座標を判断し、このデータを AeroScout MobileView に送信します。
- AeroScout MobileView は、場所データを使用して、マップを表示し、検索を有効にし、アラートを作成し、アセットを管理し、API を使用するサードパーティへのインターフェイスとしての役割を果たします。

Location Feed の使用

図 8: AeroScout ネットワーク図



フォーティネット標準 Wi-Fi インフラストラクチャに加えて、AeroScout Location Receiver と Exciter を、TDOA (Time-Different Of Arrival) とチョークポイントの目的で配備できます。

AeroScout の設定

タグの追跡は、FortiWLC と AP を使用し、AeroScout 製品から実行します。FortiWLC が AeroScout と連携して動作するように構成するには、aeroscout enable コマンドを使用します。

```
controller(config)# aeroscout ?
  disable          (10) Disabling AeroScout Feature.
  enable           (10) Enabling AeroScout Feature.
  ip-address       (10) The Aeroscout engine IP address.
  port             (10) The Aeroscout engine port.
controller(config)#
```

場所の精度

RSSI 値は、場所の計算の基本であるため、アクセス ポイントのチャンネルとタグの転送チャンネルを一致させ、アクセス ポイントのものではないチャンネルで転送されたタグ メッセージをドロップする必要があります。タグ レポートの各メッセージに転送チャンネルが含まれているため、このマッチングは実装されています。

以上の理由により、AeroScout のソリューション アーキテクチャとフォーティネットの仮想セルおよび Air Traffic Control™ テクノロジーの組み合わせによって、タグのロケーションの精度が向上します。つまり、フォーティネットの AP を仮想化された BSSID を使用して 1 つのチャンネルに配備できるため、タグ メッセージに多くの参照ポイントが提供され、ロケーションの精度が向上します。

タグのロケーションを正確に計算するには、3 つ以上のアクセス ポイントをタグが送信する Wi-Fi メッセージに報告する必要があります。メッセージを受信し、報告する AP が 3 つ未満の場合、精度の低いロケーションしか提供されず、多くの場合は、タグに最も近い AP のロケーションになります。タグのロケーションを参照するには、AeroScout を使用します。Fortinet CLI の show discovered-station コマンドや Fortinet CLI の他のどの場所にも、タグは表示されません。

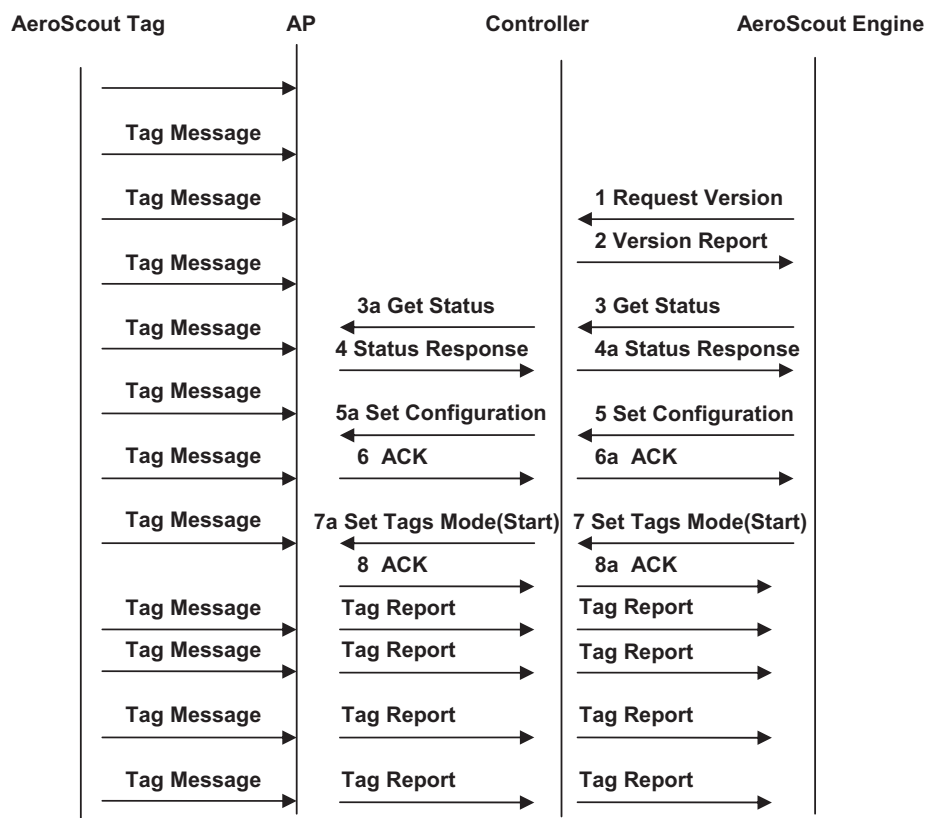
アセットがタグ付けされ、追跡される空間にできるだけ近い場所に AP を配置し、カバレッジエリアの中心のカバレッジ ホールを埋めるようにすることが重要です。追跡エリアを囲むように配置するとよいでしょう。AP の配置と AP 同士の距離を決定する際には、標準のフォーティネット Networks デプロイ ガイドラインも利用してください。すなわち、カバレッジと最適なデータ速度のプランニングを実施してください。AeroScout Exciter をチョークポイント ロケーションに使用する場合は、タグ メッセージを受け取る 1 つの AP だけで正確なロケーション レポートが提供されます。

タグ プロトコルの実装

タグ プロトコルは、アクセス ポイントと AeroScout Engine の間で動作します。フォーティ ネット AP は IBSS 形式のタグ フレームのみを受信し、処理しますが、フォーティ ネット AeroScout 実装は、IBSS (デフォルト) または WDS のいずれかのフレーム形式で送信される タグ (ラップトップではありません) メッセージをサポートします。

FortiWLC およびアクセス ポイントを現行バージョンにアップグレードすると、タグ プロトコルが自動的に有効になります。これ以外の設定の手順は必要ありません。AeroScout Tags、Engine、および MobileView アプリケーションの管理には、AeroScout プラットフォームを使用します。[87 ページの図 9](#) に、タグ プロトコルで使用される処理とメッセージを記載します。

図 9: AeroScout タグ プロトコル メッセージ



AeroScout と不正検出

AP インターフェイスが不正 AP 有効の専用スキャン モードになっていると、タグはどのチャネルについても転送されません。AP インターフェイスが不正 AP 有効の通常モードになっていると、タグはホーム チャネルでのみ転送されます。それ以外のチャネルのタグは転送されません。

AeroScout システム ログ エラー メッセージ

エラー条件	重大度	メッセージ
ATS AeroScout Manager メールボックスを作成できない	Critical	AeroScoutMgr mailbox creation failed
AeroScout モードをドライバに設定できない	Critical	Cannot set AeroScout mode to enable/disable
無効な AE メッセージ	warning	Unknown Message Code[0xXX]
		Data length error. rcvdLength[%d], expect at least [%d]
未知またはサポートしていないメールボックスからのメッセージ	miscellaneous	Msg from Unknown MailboxId[xx]
コントローラ メッセージを送信するためのメールボックス バッファを割り当てることができない	warning	AllocBuf failed reqID[0xXXXXX]
AeroScout カーネル モジュールへの IOCTL が失敗した	warning	reqID[0xXXXXX] IOCTL[xx] to AeroScout kernel module failed
ワイヤレス チャネルの構成情報を取得できない	warning	Could not get wireless interface config for interface[xx]

AeroScout モバイル装置

AeroScout は、RTLS (Real Time Location Service) のための Wi-Fi ベースのソリューションを提供しています。以下のデバイスは、AeroScout タグ ベースのロケーション管理をサポートしています。

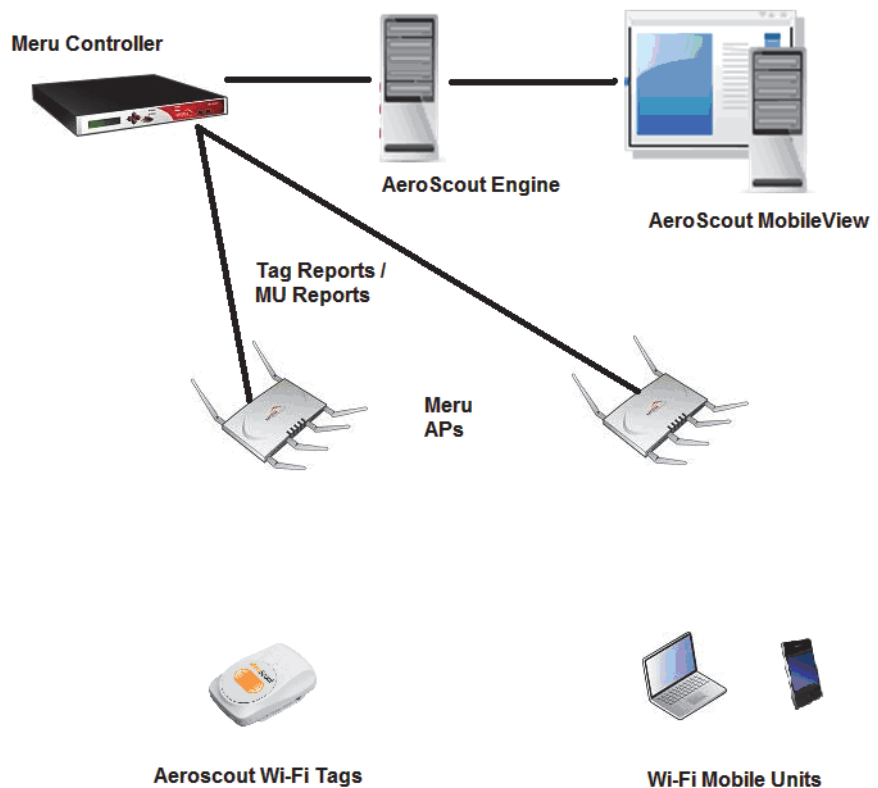
- AP400
- AP822
- AP832

- FAP-U421EV
- FAP-U423EV
- AP1000

AeroScout モバイル装置のアーキテクチャを 89 ページの図 10 に記載します。AeroScout の実装で発生するハイレベルのプロセスは、以下のとおりです。

- Wi-Fi モバイル装置がワイヤレス フレームを 1 つ以上の AP に送信します。
- AP は、(AP と AeroSpace Engine の間のトラフィックを制御する希薄メカニズムを使用して) 各 Wi-Fi モバイル装置のレポートを AeroScout Engine に送信します。
- AeroScout Engine は、座標を決定し、それを AeroScout MobileView に送信します。
- AeroScout MobileView は、ロケーション データを使用して、マップを表示し、検索を有効にし、アラートを作成し、アセットを管理し、サードパーティとのインターフェイスとしての役割を果たし、それ以外の多くの作業にもロケーション データを利用します。

図 10: Aeroscout モバイル装置



Wi-Fi モバイル装置 (MU) がいずれかのアクセス ポイントに関連付けられているか、ブロードキャストまたはユニキャスト メッセージを送信することで、場所の特定が可能になります。Wi-Fi モバイル装置から送信されたメッセージをアクセス ポイントが受信し、追加情報 (シグナル強度の測定値など) と一緒に、AeroScout 可視化システムのコア コンポーネントである AeroScout Engine に渡されます。AeroScout Engine は、Wi-Fi デバイスの正確な場所も計算します。モバイル装置の場所を特定するには、メッセージを受け取るアクセス ポイントが、各メッセージの RSSI 値を AeroScout Engine に渡す必要があります。アクセス ポイントは、関連付けられていない MU からのデータ メッセージも収集し、RSSI 値を AeroScout Engine に渡すことができます。

タグや Wi-Fi モバイル装置のレポートは、AP の通常の処理に影響しないため、AP は、通常の 802.11a/b/g 通信、監視、ブリッジ モードなどのサポートしているすべてのモードで実行されます。MU のトラフィックは多いため、AeroScout Engine に送信される MU メッセージを希薄化できます。

AeroScout の設定

タグの追跡は、FortiWLC と AP を使用し、AeroScout 製品から実行します。FortiWLC が AeroScout と連携して動作するように構成するには、以下のように `aeroscout enable` コマンドを使用します。

```
default# sh aeroscout
Aeroscout Parameters

Enable/Disable           : enable
Aeroscout Engine IP Address : 0.0.0.0
Aeroscout Engine Port     : 12092

default#
```

AeroScout Engine からの AeroScout モバイル装置の設定

以下の手順で、AeroScout Engine から AeroScout モバイル装置を設定します。

1. Aeroscout をコントローラで有効にします。
2. Aeroscout Engine を開きます。
3. Floor Map を Aeroscout Engine にロードします。
4. Aeroscout Engine に AP を追加します。
5. [Configuration] -> [system parameters] -> [Access Points] で、[Enable mobile-unit location with access Points] チェックボックスをオンにします。
6. AeroScout Engine の Mobile Unit Positioning オプションを開始するには、[Actions] メニューから [Start MU positioning] を選択します。

AeroScout 複合レポート

パフォーマンス向上の目的で、予め定義した期間内の複数の MU レポートを複合レポートにまとめることができます。フォーティネットのシステムでは、最大 18 MU のレポートを 1 つの複合レポートにまとめることができます。複合レポートに含まれるモバイル装置の数は、AeroScout 統合ツールで設定する [Compounded Message Timeout] によって異なります。[Compounded Message Timeout] は、AeroScout 統合ツールの [Set Configuration] で設定します。

希薄化タイムアウト

状況によっては、モバイル装置のトラフィックが多くなり、ロケーション解決に必要な時間がほとんどのモバイル装置のデータ速度よりもはるかに短くなることもあります。各 AP が個々の Wi-Fi フレームの AeroScout Engine へのレポートを開始すると、ネットワークに不要なデータ オーバーヘッドが発生し、必要とするよりはるかに高いレベルのリアルタイム ロケーションが提供されます。

AP が各モバイル装置からのメッセージを希薄化できるようにするために、AeroScout プロトコルに次の 2 つのパラメータが提供されています。

- Dilution Factor
- Dilution Timeout

フォーティネット モバイル装置は、Dilution Timeout のみをサポートし、実装しています。Dilution Timeout によって、特定のモバイル装置からのモバイル装置メッセージが発生しない期間の上限を設定できます。

たとえば、Dilution Timeout 値が 60 秒に設定された場合に、AP に対して 60 秒以上、メッセージをレポートしなかった MU からメッセージが到着すると、新しいメッセージは、Dilution Factor や Dilution Counter が初期化されるかどうかに関係なく、直ちに AE にレポートされます。AE に転送するためには、希釈化のパラメータに関係なく、MU によるコマンドのブロードキャストが必要です。

Dilution Timeout は、Aeroscout Engine で次のように設定できます。
[Configuration] -> [system parameters] -> [Access Points] -> [Dilution Time out]

一般 AP 通知

一般 AP 通知は、AeroScout 統合ツールにポート 12092 で送信される自主メッセージで、AP の接続状態 (AP がオンライン、オフラインになった、AeroScout パラメータの設定が変更された) が報告されます。AeroScout 統合ツールは、コントローラから送信されるすべての一般

AP 通知メッセージを認識します。一般 AP 通知のために、AeroScout Engine の IP アドレスをコントローラに設定する必要があります。



AeroScout モードが "enabled" から "disabled" に変更されると、一般 AP 通知は送信されません。
バージョン 1.0.1 の AP 統合ツールを必ず使用してください。

フォーティネット ソリューションでは、一般 AP 通知は、AP の接続状態の変更中や、コントローラでの AeroScout 設定の変更中に、コントローラから AeroScout Engine に送信されます。一般 AP 通知は通常、IP アドレスの変更やリブートからの "復帰"、あるいは AeroScout Engine との通信が必要になるエラー条件を伝達するために使用されます。

一般 AP 通知を受信するための AeroScout 統合ツールの設定

AeroScout 統合ツールを設定して一般 AP 通知を受信するようにするには、次の手順を実行します。

- コントローラの AeroScout を有効にし、コントローラの AeroScout 統合ツールの IP アドレスを設定します。
- AeroScout Integration Tool を開き、ポートをデフォルト値の '1122' から '12092' にします。
- AP がオンラインになってからオフラインになった場合には、コントローラの AeroScout 設定パラメータを変更します。コントローラのすべてについての AP の一般 AP 通知がコントローラから送信され、AeroScout 統合ツールは、それぞれの一般 AP 通知を認識します。

FortiPresence API の設定

FortiPresence API は、ワイヤレス小売分析ソリューションを拡張して、小売企業が分析レポートのデータを使用して、顧客の入店時間や滞在時間、新規顧客かリピーターかといった顧客の行動を理解できるようにします。



802.11ac AP でのみサポートされています。

仕組み

ロケーション サーバの機能がコントローラで有効になっていると、すべての 11ac AP から、検出されたリストの STA/AP の STA レポート、および割り当てられたリストの STA の STA レポートが指定間隔で送信されます。

STA レポートは、コントローラによってデータ分析サーバに転送され、そこでデータが分析され、情報がわかりやすい形でユーザに提供されます。

コントローラの設定

ロケーション サーバ機能は、次のコマンドを使用して、コントローラで有効にできます。レポートには、Legacy と FortiPresence の 2 種類の形式があります。標準の FortiPresence フィードは、サードパーティ パートナーが使用する必要があります。以下で必要とされる情報は、この機能が提供される FortiPresence ライセンスを購入すると取得できます。

1. ロケーションの サーバ IP アドレスを指定します。

```
(config)# location-server ip-address 1.1.1.1
```

2. ロケーション サーバ ポートを指定します。ポートとは、コントローラとロケーションサーバ間の通信に使用されるポートのことです。

```
(config)# location-server port 300
```

3. プロジェクト名を指定します。プロジェクト名は、パケットが属する顧客プロジェクトを示します。最大 16 の ASCII 文字を使用できます。

```
(config)# location-server project-name FortiStore
```

4. パスワードを指定します。シークレット (パスワード) は、信頼性と完全性を立証するために各パケットに署名する共有シークレットです。最大 16 の ASCII 文字を使用できます。

```
(config)# location-server secret fortisecret
```

5. レポート形式を指定します。標準の FortiPresence フィードを使用します。最大 16 の ASCII 文字を使用できます。

```
(config)# location-server report-format forti-presence
```

6. レポートのクエリが実行されるレポート間隔を指定します。ロケーション レポートの間隔 (秒数) であり、デフォルトは 5 秒です。

```
(config)# location-server report interval 30
```



間隔を 30 秒に設定することをお勧めします。

-
7. ロケーション サーバ ソースを指定します。

```
(config)# location-server source wifi
```

設定の詳細を表示するには、show location-server コマンドを使用します。

#show location-server

Location Server Configuration

ReportFormat : forti-presence

Project Name : FortiStore
Enable/Disable Location Server : enable
Secret : *****
Location Server Source : wifi
Location Server IP Address : 1.1.1.1
Location Server Port : 300
Location Report Interval (in Seconds) : 30

出力は、すべての AP がステーションの場所を特定するレポートを 30 秒ごとに送信し、コントローラが UDP ポート 300 で設定されているサーバ 1:1:1:1 にそれを転送することを示しています。

更新頻度は、クライアントに送信される更新の頻度を指定し、秒単位で測定されます。デフォルトは 5 秒です。クライアント デバイスは、MAC アドレスに基づき 5 秒にわたって展開されます。各クライアントで 5 秒ごとに更新が発生します。頻度を増やすと、ワイヤレス ネットワークが混雑して、ロケーション データに悪影響が及びます。



トラフィックは UDP として送信されます。

FortiWLC (SD) の通信ポート

AP とコントローラのためのトンネルには、以下の通信ポートを使用します。

トラフィック	ポート
AeroScout	UDP/6091
キャプティブ ポータル (http リダイレクト)	TCP/8080
キャプティブ ポータル (https リダイレクト)	TCP/8081
NM Location Manager - Web UI	TCP/443
NM Location Manager - Administrative Web UI (SSL)	TCP/8003
NM Location Manager - AP Communication (Capture Packets サブシステム)	UDP/9177 と UDP/37008
FTP	TCP/20 と TCP/21
H.323v1 フロー検出	TCP/1720
HTTP	TCP/8080

トラフィック	ポート
HTTPS	TCP/443
Fortinet L3 AP COMM	UDP/5000
ライセンス - ライセンスのみの目的での、コントローラを起点とする接続 (たとえば、wncagent -> merud)	TCP/32780
Fortinet L3 AP データ	UDP/9393
Fortinet L3 AP 検出 / キープアライブ	UDP/9292
NP1 アドバタイズ / 構成	UDP/9980
NTP	UDP/123
RADIUS アカウント	1813 / 1646
RADIUS 認証	1812 / 1645
SIP	UDP/TCP 5060
SSH	TCP/22
SNMP	UDP/161 と 162
syslog	UDP/514
TFTP	UDP/69
最大 5 のアップストリーム / ダウンストリームの UDP ブロードキャストを構成できる	UPD/xxx
TACACS+	TCP/49
Telnet	TCP/23
コントローラ パケット捕捉	UDP/9177
WIPS	UDP/9178
WireShark、OmniPeek、Newbury	UDP/9177
SAM (AP とサーバ)	EtherIP 97

コントローラ ベースの DHCP サーバの設定

FortiWLC (SD) リリース 5.1 以降では、コントローラから直接操作できる DHCP サーバをユーザが設定できます。この設定は、DHCP の作業を処理する独立したサーバを必要としない、比較的小規模の導入環境に適しています。この方法が特に有用なのは、(たとえば、guest ネットワークに使用する) VLAN のために別の DHCP サーバが必要ではあるものの、そのトラフィックが会社の DHCP サーバに影響しないようにしたい場合です。



コントローラ ベースの DHCP サーバでは、コントローラの (コントローラのグローバルパラメータの) [DHCP Relay Passthrough] オプションを [On] に設定する必要があります。このオプションを変更するには、Web UI にアクセスし、[Configuration] > [Devices] > [Controller] に移動します。

企業環境では、社内の DHCP サーバを使用しないことを推奨します。

DHCP サーバの作成

コントローラには、複数の異なる DHCP サーバをいつでも構成できます。DHCP サーバは、1つの VLAN にのみ関連付けることができます。LAN や仮想インターフェイス プロファイルに異なる DHCP サーバを設定するには、DHCP サーバごとに以下の手順を繰り返します。

DHCP サーバを作成するには、次の手順を実行します。

1. Web UI から、[Configuration] > [DHCP] に移動し、[DHCP Server] タブをクリックして、現在設定されている DHCP サーバを表示します。サーバが設定されていない場合、このページには何も表示されません。
2. [Add] をクリックして、DHCP サーバパラメータの設定を開始します。

図 11: DHCP サーバ設定

Internal DHCP server configuration - Add

DHCP Server Pool Name	<input type="text"/>	Enter 1-32 chars., Required
VLAN Name	<input type="button" value="No VLAN"/>	
State	<input type="button" value="Enable"/>	
Lease Time (in Seconds)	<input type="text" value="3600"/>	Valid range: [300-65535]
IP Pool start	<input type="text"/>	
IP Pool end	<input type="text"/>	
Domain Name	<input type="text"/>	Enter 0-256 chars.
Primary DNS Server	<input type="text"/>	
Secondary DNS Server	<input type="text"/>	
Primary Netbios Server	<input type="text"/>	
Secondary Netbios Server	<input type="text"/>	
DHCP Option 43	<input type="text"/>	Enter 0-32 chars.

3. 必要な情報を、表 8 の説明に従って入力します。

表 8: DHCP オプション

オプション	説明
DHCP Server Pool Name	DHCP サーバを説明する名前を入力します。
VLAN Name	このドロップダウン リストでは、サーバに適用する VLAN を選択できます。コントローラが L2 ルーティング モードで動作する場合のみ、このオプションを使用できます。
State	DHCP サーバを有効にするには [Enabled] に、無効にするには [Disabled] に設定します。
Lease Time	DHCP サーバが IP リースを割り当てる期間。この値は秒数で表示されます。
IP Pool Start/End	DHCP サーバが割り当てる IP プールの開始と終了の IP アドレス。
Domain Name	DHCP サーバがアクティブになるドメイン
Primary/Secondary DNS Server	DHCP サーバが使用するプライマリおよびセカンダリの DNS サーバ
Primary/Secondary Netbios Server	DHCP サーバが使用するプライマリおよびセカンダリの Netbios サーバ
DHCP Option 43	オプション 43 では、サーバが使用するプライマリとセカンダリのコントローラを手動で指定できます。プライマリとセカンダリのコントローラの IP アドレスを (カンマ区切りで) このフィールドに入力します。

4. [OK] をクリックしてサーバを保存します。

DHCP リースの表示

DHCP サーバが設定され、アクティブになると、クライアントへの IP アドレスの割り当てを開始できます。これらの割り当ては、DHCP リース テーブルに表示されます。このテーブルを表示するには、Web UI を開いて、[Configuration] > [DHCP] に移動します。DHCP リース テーブルが自動的に表示されます。

Fortinet Service Control の使用

Fortinet Service Control 機能は、会社のネットワーク内のクライアントによる、Bonjour などのプロトコルを使用してサービスをアドバタイズするデバイスへのアクセスや通信を可能にするよう設計されています。Bonjour 対応デバイスには、多くが小規模の使用向けに設計されているという制限がありますが、エンタープライズ レベルの環境で広く使用されるようになっています。サービスの特性によって、これらのプロトコルのワイヤレス トラフィック通信が異なるサブネット間でやり取りできないため、VLAN1 にいるユーザは (たとえば) VLAN2 で動作するデバイスにはアクセスできないというように、大規模の環境でのスケーラビリティに関するいくつかの課題があります。

Service Control は、異なるサブネットのクライアントと Bonjour 対応デバイスとのトラフィックをフォーティネットが受け渡しすることで、この問題を解決し、相互のシームレスな通信を可能にします。また、特定のユーザ、SSID、または VLAN が使用できるサービスをユーザが指定できるため、きめ細かい制御が可能になります。

Service Control を有効にするには、以下の手順を実行します。

1. [Configuration] > [Service Control] に移動します。デフォルトでは、Service Control Dashboard に移動しますが、現段階では何も情報は表示されません (サービスが無効になっているため)。
2. [Settings] タブをクリックして、[Global Settings] タブにアクセスします。
3. [Enable Service Control] のチェックをオンにします。ページが自動的に更新されます。

設定の手順については、以下の項を参照してください。

Service Control のグローバル設定の変更

Service Control が有効になると、[Settings] タブに 2 つのテーブル、Discovery Criteria と Advanced Options が表示されます。Discovery Criteria では、検出されるサービスのタイプをユーザが指定できます。デフォルトでは、すべての SSID と AP、およびコントローラのネイティブ VLAN で、システムに設定されている AirPlay と AirPrint のすべてのサービスが有線側のコントローラによって検出されるように設定されます。これを変更するには、[Services] 列の下 の鉛筆アイコンをクリックして、[Discovery Criteria] ダイアログにアクセスします。

図 12: [Discovery Criteria]

Discovery Criteria

Select Services

☒ All services

AppleTV
Chromecast
Printer

Select Wireless Network

☐ All ESSIDs

rfextcp
deskcsim
systemlab
vsta

☒ All APs

Jothi-desk

Select Wired Network

VLAN List 0 Example 1-3,5

Wired Gateway List 0

ADD

SAVE CANCEL

1. 上図に示すように [All Services] ボックスがチェックされていると、設定されているすべてのサービスが自動的にシステムによって検出されます。サービスのタイプを制限する場合は、このボックスのチェックをオフにして、検出されるようにするサービスを選択します。
2. [Select Wireless Network] セクションでは、サービスにアクセスできる SSID/AP (デフォルトでは、すべてがアクセス可能) をカスタマイズできます。これらのオプションによって、ワイヤレス デバイスによるサービスのアクセス方法が制御されます。
3. [Select Wired Network] セクションでは、有線デバイスによるサービスのアクセス方法を制御し、アクセスを許可する VLAN を入力します。有線ゲートウェイを追加するには、[Add] ボタンをクリックして、表示されるデバイスのリストから必要なオプションを指定します。
4. [Save] をクリックして、変更を保存します。

AP と コントローラを使用した有線サービス検出

以下の手順で、AP とコントローラを使用した有線サービス検出を実行します。

1. AP およびコントローラの有線インターフェイスを使用して、サービスを検出します。
AP またはコントローラを有線ゲートウェイ リストに追加します。

2. AP またはコントローラの有線インターフェイスがサービスを検出する必要がある VLAN にタグ付けされていて、その VLAN が VLAN リストに追加されることを確認します。



タグ付けされている VLAN (VLAN XX) のサービスを検出するコントローラの場合、そのコントローラの VLAN プロファイルが VLAN XX (設定した VLAN) になっている必要があります。AP の有線インターフェイスを特定の VLAN でのサービスの検出に使用する場合に、VLAN プロファイルをコントローラに作成する必要はありません。



AP やコントローラがネイティブ VLAN のサービスを検出するようにするには、VLAN リストを VLAN 0 を使用して更新する必要があります。

サービスの追加または削除

[Services] タブでは、Service Control で検出されるサービスをユーザーが変更できます。デフォルトでは、いくつかのサービスがシステムに事前に設定されていますが、[Add] ボタンをクリックして新しいサービスを作成することで、このリストにサービスを追加できます。

図 13: 新しいサービスの追加

The screenshot shows a web-based 'Add Service' dialog. It has three input fields: 'Name' (1-64 chars), 'Description' (0-64 chars), and 'Service Type' (1-512 chars). To the right of the 'Service Type' field is a red 'ADD' button. Below the inputs is a table with the title 'Added Service Types'. The table has one row with a checkbox and the text 'Service Types'. At the bottom of the dialog are three buttons: a red 'DELETE' button with a trash icon, a red 'SAVE' button with a floppy disk icon, and a red 'CANCEL' button with an 'X' icon.

以下の必須フィールドに入力します。

- [Name]: サービスの名前を入力します。
- [Description]: 短い説明を入力します。
- [Service Type]: サービスタイプの文字列を入力します。複数のエントリが必要な場合は、1 つずつ入力し、その後に [Add] をクリックします。追加したサービスは Added Service Types テーブルに表示されます。

注：追加したサービスを削除するには、隣にあるボックスのチェックをオンにして、[Delete] をクリックします。

[Save] をクリックして、新しいサービスを保存します。

場所の設定

[Locations] タブでは、サービスを検出してアドバタイズする場所を指定できます。デフォルトでは場所が設定されていないため、[Add] をクリックして追加します。

図 14: 場所の追加

The screenshot shows a web-based dialog titled "Add Location". It has two input fields: "Name" with a placeholder "Enter 1-32 chars. Required" and "Description" with a placeholder "Enter 1-255 chars.". Below these is a section titled "Add Member APs". Inside this section, there is a list box on the left labeled "Add APs" containing the items "AP-2", "AP-17", "AP-28", "AP-37", and "AP-39". To the right of this list box is a right-pointing arrow button ">>". Below the list box is a left-pointing arrow button "<<". To the right of the arrow buttons is an empty list box. At the bottom of the dialog are two buttons: "Save" and "Cancel".

場所は、3つの主要コンポーネント、すなわち、場所の名前、説明、およびメンバAPで構成されます。[Name] と [Description] に名前と説明を入力し、その場所のメンバにするAPをリストから選択します。右向き矢印ボタンをクリックして、選択したAPを新しい場所に追加します。

[Save] をクリックすると、新しい場所が Location テーブルに表示されます。これで、場所の定義で指定したAPでサービスにアクセスできるようになりました。

ユーザグループの作成

ユーザグループは、サブスクリイバとアドバタイザをグループ内で分離します。ユーザグループでは、どのユーザ/アドバタイザ(有線クライアントの場合はVLANによって、ワイヤレスクライアントではSSIDと場所によってグループ化されます)がアドバタイズされた

サービスにアクセスしたり、サービスをアドバタイズしたりできるかを定義します。デフォルトではグループは作成されないため、[Add] をクリックして作成します。

図 15: ユーザグループの作成

The screenshot shows the 'Add User Group' dialog box. At the top, there are three tabs: 'Services', 'AP Groups', and 'User Groups'. The 'User Groups' tab is selected. Below the tabs, the title 'Add User Group' is displayed with a red arrow pointing to it. The form contains the following fields and options:

- Name ***: A text input field with a placeholder 'Enter 1-32 chars.'
- Description**: A text input field with a placeholder 'Enter 0-64 chars.'
- Role**: Three radio buttons labeled 'Advertiser', 'Subscriber', and 'Both'. Below them is a note: 'Users in this group can be assigned the role of Advertiser and Subscriber in the Policies.'
- User Group Type**: Two radio buttons labeled 'Wireless' and 'Wired'.
- Select Wireless Users**: This section is active when 'Wireless' is selected. It contains two lists:
 - ESSIDs**: A list box containing 'rfextcp', 'deskcsim', 'systemlab', and 'vsta'.
 - AP Groups**: A list box containing 'Jothi-desk'. To its right is a checkbox labeled 'All APs'.

At the bottom of the dialog are two buttons: 'SAVE' and 'CANCEL'.

ユーザグループは、4つの主要コンポーネント、すなわち、グループの名前、説明、ロール、および有線ゲートウェイリストによるワイヤレス / 有線ユーザで構成されます。これらのフィールドを使用することで、定義されているサービスにアクセスできるユーザをカスタマイズできます。

1. [Name] と [Description] に名前と説明をそれぞれ入力します。
2. [Role] では、ユーザグループのロールを選択します。[Advertiser]、[Subscriber]、[Both] のいずれかのオプションを選択します。
3. [User Group Type] でユーザグループのタイプを選択します。[Wireless] または [Wired] のいずれかのオプションを選択します。
4. [User Group Type] で [Wireless] を選択すると、[Select Wireless Section] が表示されます。[Select Wireless Users] セクションで、アクセスを許可する SSID を選択します。複数のオプションを選択するには、クリックしてドラッグします。項目を1つずつ選択または選択解除するには、Ctrl を押しながらかlickします。
5. [User Group Type] で [Wired] を選択すると、[Select Wired Users] セクションが表示されます。アドバタイズされたサービスへのアクセスを許可する VLAN を入力します。
6. [Save] をクリックして、グループを作成します。これで、グループのパラメータに含まれるデバイスがアドバタイズされたサービスにアクセスできるようになりました。

Service Control ポリシーの定義

Service Control ポリシーは、特定のアドバタイズされたサービスにアクセスできるユーザグループを決定します。つまり、ポリシー テーブルを使用することで、サブスクリバ (サービスを使用するデバイス) とアドバタイザ (サービスを提供するデバイス) の間のルートを定義できます。

1. [Policies] タブで [Add] をクリックして、[Create Service Control Policy] ウィンドウにアクセスします。

図 16: ポリシーの作成

2. 作成するポリシーの名前を [Policy Name] に入力します。
3. ポリシーの説明を [Description] に入力します。
4. [Select Subscriber] ドロップダウンで、アクセスを許可するグループを指定します。
5. 該当するサービスを、[Choose Services] セクションのリストから選択します。すべてのサービスを選択する場合は、[All services] ボックスのチェックをオンにします。
6. 最後に、[Select Advertise] ドロップダウンで、サービスへのアクセスを提供するグループを選択します。
7. [Save] をクリックして、新しいポリシーを保存します。

IPv6 クライアントのサポート

FortiWLC (SD) は、フォーティネット アクセス ポイント (AP) に接続されたワイヤレスと有線のクライアントで、ブリッジとトンネルの両方のモードの ESS プロファイルをサポートしています。IPv6 クライアントのサポートでは、以下の機能が提供されます。

- [基本的な IPv6 転送 \(104 ページ\)](#)
- [動的 VLAN 環境での IPv6 転送 \(105 ページ\)](#)
- [高パフォーマンス IPv6 転送 \(106 ページ\)](#)

- [IPv6 セキュリティ \(106 ページ\)](#)
- [IPv6 マルチキャスト最適化 \(106 ページ\)](#)
- [IPv6 優先順位設定 \(106 ページ\)](#)
- [IPv6 ネットワーク管理の拡張 \(107 ページ\)](#)

基本的な IPv6 転送

FortiWLC (SD) は、トンネル モードおよびブリッジ モードで接続されている IPv6 クライアントの L2 スイッチとして動作します。IPv6 仕様 (RFC 2460) では、IPv6 モードの IPv6 ルータと IPv6 ホストのサブクラスが定義されています。コントローラと AP は IPv6 ホストとして動作し、IPv6 ルータとしてではなく、レイヤ 2 で IPv6 パケットを転送します。ESS プロファイルは、IPv4、デュアルスタック (IPv4 と IPv6)、および IPv6 のみのクライアントを同時にサポートします。クライアントの以下のモードの IPv6 アドレス設定がサポートされています。

- SLAAC (ステートレス アドレス自動設定)
- DHCPv6
- 固定 IPv6 設定 (手動)
- リンク ローカル アドレス

ワイヤレス クライアントの VLAN プロファイルでは、IPv4 アドレスが使用され、IPv6 は必要ありません。ESS の [Allow Multicast Flag] オプションは、ESS でマルチキャスト トラフィックを許可またはブロックするために使用されます。このオプションが Off に設定されていると、ルータ アドバタイズ、ルータ要請、近接検出メッセージ、および DHCPv6 パケット以外のすべての IPv6 マルチキャスト トラフィックがブロックされます。

ESS プロファイル設定では、[Bridging]、[Allow Multicast]、[Multi-To-Unicast] のフィールドを設定できます。詳細については、「ESS の設定」の章を参照してください。

AP に接続されている有線ネットワークの場合は、Port プロファイルの [Allow Multicast] と IPv6 ブリッジを設定します。詳細については、[208 ページの「ポート プロファイルの設定」](#)を参照してください。

IPv6 パラメータの [Neighbor Discovery Optimization] フィールドは、[Configuration] > [Devices] > [Controller] > [IPv6 Parameter] で設定できます。

IPv6 関連の CLI コマンドは、以下のとおりです。

- show station - このコマンドは、新しい列 [IP Mode] に IP アドレス タイプを表示します。この列の有効な値は、IPv4、IPv6、および IPv4v6 です。
- sh station multiple-ip - このコマンドは、ステーションの IPv4 アドレスごとに 1 行、IPv6 アドレスごとに 1 行を表示します。IPv6 アドレス タイプの列が追加され、アドレスが

IPv6 アドレスの場合は、Global Unicast、Global Unicast DHCP、Link Local、Temporary のいずれかの値が表示されます。

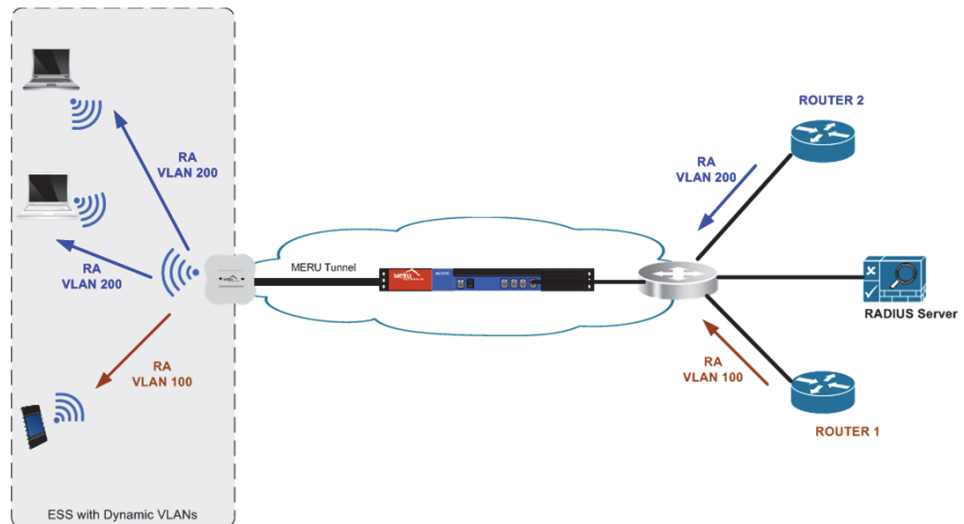
CLI コマンドの詳細については、『フォーティネット コマンド リファレンス ガイド』を参照してください。

動的 VLAN 環境での IPv6 転送

FortiWLC (SD) の過去のリリースの場合、動的 VLAN (1 つの ESS に複数の VLAN) の環境では、FortiWLC (SD) がマルチキャスト パケットを割り当てられている VLAN に関係なく、すべてのステーションに転送します。過去のリリースでは、この方法で IPv4 がサポートされていましたが、FortiWLC (SD) 6.0-2-0 以降では IPv6 がサポートされています。ルータ アドバタイズメントとは、ルータのプレフィックス情報を提供するメッセージであり、IPv6 ステーションはこれを使用して IPv6 アドレスを自動設定します。

下図に、ルータ アドバタイズメントのフィルタリングの動作の説明を記載します。

図 17: ルータ アドバタイズメントのフィルタリング



3 つのワイヤレス ステーションが、RADIUS で割り当てられた VLAN を使用して設定された ESS プロファイルに接続されています。2 つのステーションは VLAN 200 に、1 つのステーションは VLAN100 に属しています。VLAN 100 のルータによるルータ アドバタイズメントは、VLAN 200 に割り当てられているステーションには送信されません。

AP が動的 VLAN に設定されている ESS プロファイルでルータ アドバタイズメントを転送する場合、ある VLAN の RA は他の VLAN のステーションには送信されません。RA はユニキャスト パケットに変換されて、その VLAN に割り当てられているワイヤレス ステーションのみに送信されます。この動作はすべての RF 仮想化モードでサポートされており、マルチキャスト - ユニキャスト変換の設定よりも優先されます。

変換を有効にするには、ESS プロファイルで [Multicast-To-Unicast] フィールドを [Only Router Advertisement] (RA にのみ変換を実行する) に設定する必要があります。こうすることで、AP の RA パケットに対するマルチキャスト - ユニキャスト変換が実行されて、その VLAN ID に属しているステーションにのみパケットが送信されるようになります。

高パフォーマンス IPv6 転送

FastPath 機能がトンネル モードの IPv6 クライアントに対してサポートされています。この機能は、IPv4 と IPv6 の UDP と TCP のデータ フローでのみ、コントローラのスループットを向上させるために使用されます。コントローラの [FastPath] フィールドが [On] の場合は、スループットが向上します。

IPv6 セキュリティ

IPv6 セキュリティは、IPv6 リンク処理のセキュリティを確保するように設計されており、トンネルとブリッジの両方のモードに適用されます。IPv6 セキュリティは、以下のフィルタリング方法でサポートされています。

- RA ガード - これは、ネットワーク デバイス プラットフォームに到着する RA ガード メッセージをブロックまたは拒否するためにサポートされています。
- DHCPv6 ガード - これは、未承認の DHCP サーバとサーバからクライアントに DHCP パケットを転送するリレー エージェントを起点とする DHCP 応答メッセージとアドバタイズメント メッセージをブロックするためにサポートされています。

IPv6 マルチキャスト最適化

IPv6 マルチキャスト最適化は、近接の検出とルータ アドバタイズメントによって生成されるマルチキャスト トラフィックを少なくします。このサポートは、トンネル モードでのみ提供されます。

IPv6 優先順位設定

IPv6 QoS サポートは、IPv6 ヘッダのトラフィック クラス フィールドに基づいて IPv6 パケットの優先順位を設定することで提供されます。

IPv6 ネットワーク管理の拡張

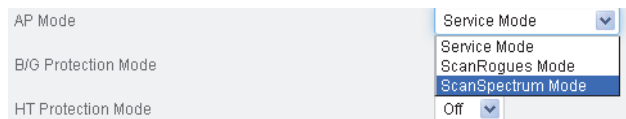
IPv6 クライアント サポート機能では、NMS が強化され、複数の IPv6 アドレスを格納できます。コントローラは、クライアントあたり最大 8 つの以下のアドレスをサポートします。

- グローバル ユニキャスト アドレス (DHCP と自動設定)
- リンク ローカル アドレス
- 一時アドレス

Spectrum Manager へのアクセス

- FortiWLC (SD) バージョン 6.0-2-0 以降では、スペクトラム スキャンニング モードで配備された AP を設定し、ソフトウェア ベースのスペクトラム監視デバイスとして動作するようにできます。この設定は、[Configuration] > [Wireless] > [Radio table] で実行します。スペクトラム スキャンニング モードで AP を設定するには、テーブルから該当するインターフェイスをクリックし、[AP Mode] ドロップダウンを使用して [ScanSpectrum Mode] を指定します。

図 18: [AP Mode] オプション



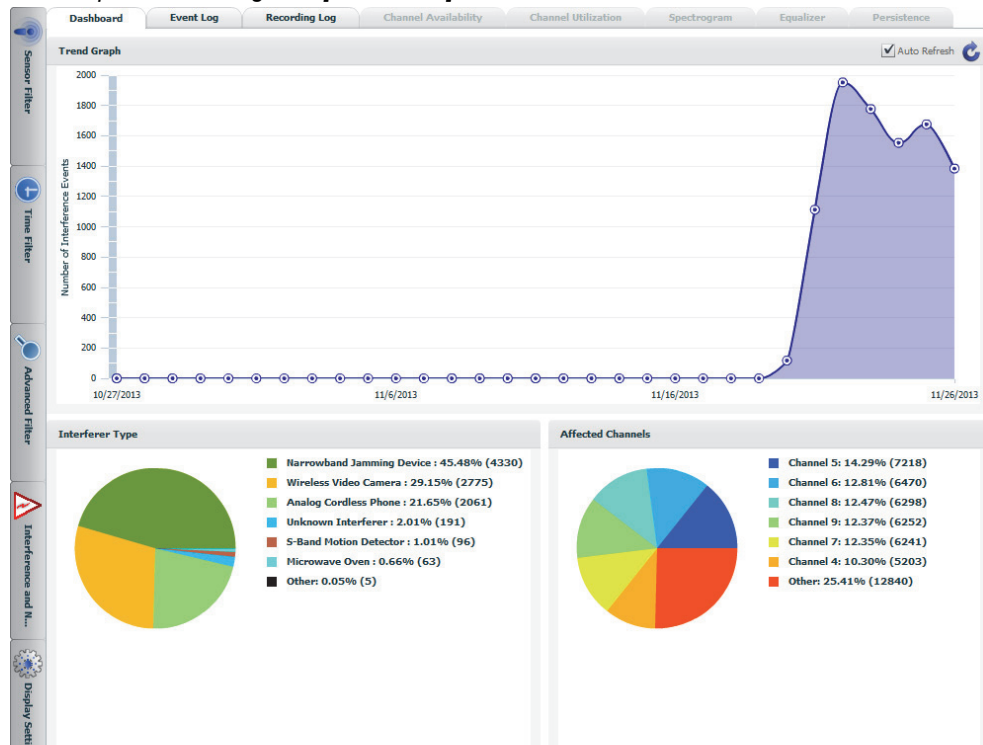
ScanSpectrum Mode で動作すると、選択したインターフェイスが通常のクライアントとしてサービスを実行できなくなります。

AP の設定が完了すると、ユーザは [Monitor] > [Spectrum Manager] > [Console] から Spectrum Manager にアクセスできるようになります。

Spectrum Manager ダッシュボード

Spectrum Manager の [Dashboard] 画面には、さまざまなセンサーから収集された干渉情報が表示されます。センサーについては、[129 ページの「センサー」](#) ([129 ページの「ソフトウェア センサー」](#) および [129 ページの「ハードウェア センサー」](#)) を参照してください。2.4Ghz および 5Ghz スペクトラムでの干渉デバイスのアクティビティがグラフで表示されます。[108 ページの図 19](#) は、Spectrum Manager の [Dashboard] 画面を示しています。

図 19: Spectrum Manager の [Dashboard]



以下の表は、[Dashboard] 画面で表示されるさまざまなセクションを示しています。

Trend Graph	[Trend Graph] は、長年にわたって確認された干渉イベント数をグラフ表示します。
Interferer Type	[Interferer Type] グラフは、設定された期間に確認された干渉タイプで分類された円グラフです。各項目は、設定された期間における干渉イベントの総数に対する、特定の干渉タイプからの個々の干渉イベント数の割合に比例します。
Affected Channels	<p>[Affected Channels] グラフは、干渉イベントによって特定のチャネルが影響を受けた回数を示す円グラフです。各項目は、イベントの総数に対し、特定のチャネルに影響を及ぼしたイベント数の割合に比例します。</p> <p>注：干渉イベントは複数のチャネルに同時に影響を及ぼします。</p>

[Dashboard] 画面には、データベースのフィルタリングや表示設定の変更を行うための拡張可能なさまざまな制御用パネルが表示されます。詳細については、[118 ページの「コントロールパネル」](#)のトピックを参照してください。

[Dashboard] 画面では、以下のタブにもアクセスできます。

1. [イベント ログ \(109 ページ\)](#)
2. [Spectrum Manager - チャネル可用性 \(112 ページ\)](#)
3. [Spectrum Manager - チャネル使用率 \(113 ページ\)](#)
4. [Spectrum Manager - Spectrogram \(114 ページ\)](#)
5. [Spectrum Manager - イコライザ \(115 ページ\)](#)
6. [Spectrum Manager - パースステンス \(116 ページ\)](#)



上記 2 ～ 6 のタブが有効なのは、[Event Log] 画面で [View live data from sensor] オプションを選択しているときだけです。また、センサーのページで、選択したセンサーの [Show Spectrum Display] から也表示できます。詳細については、[Spectrum Manager - \[Event Log\]](#) 画面を参照してください。

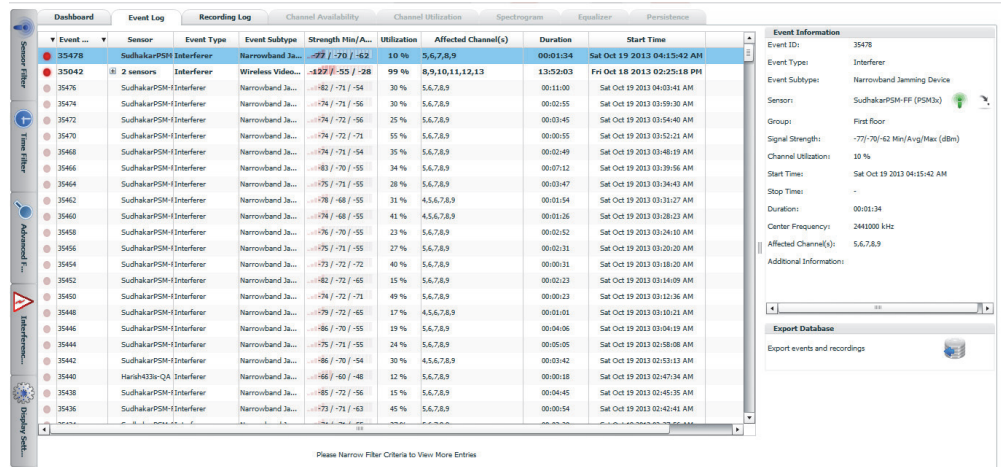
イベント ログ

[Spectrum Manager] > [Monitor] > [Dashboard] > [Event Log]

Spectrum Manager の [Event Log] 画面では、センサーの詳細なログ情報が表示されます。

[110 ページの図 20](#) は、Spectrum Manager の [Event Log] 画面を示しています。

図 20: Spectrum Manager - イベント ログ



以下の表は、[Event Log] 画面に表示される イベント情報を示しています。

フィールド	説明
Event ID	イベント ID が表示されます。
Event Type	イベントのタイプが表示されます。
Event Subtype	干渉ソース名が表示されます。

フィールド	説明
Sensor	<p>選択したセンサーの名前が表示されます。以下は選択可能なオプションです。</p> <ul style="list-style-type: none"> • [View live data from sensor] : このオプションを選択すると、センサーからのライブデータを読み取ることができますようになります。 <p>[View live data from sensor] オプションを選択すると、以下のタブが有効になります。</p> <ul style="list-style-type: none"> • [Channel Availability] • [Channel Utilization] • [Spectrogram] • [Equalizer] • [Persistence] <p>上記のタブでは、それぞれのタブで選択したセンサーのデータが表示されます。</p> <ul style="list-style-type: none"> • [Show interferer on map] : アイコンを選択します。 <p>[E(z)RF Map Management] 画面が表示され、フロア上の干渉デバイスの位置を示します。</p>
Group	センサーのグループが表示されます。
Signal Strength	干渉のシグナルの強度に加え、最小値、最大値、平均値 (dBm 単位) も表示されます。
Channel Utilization	干渉によって活用されるチャネルの割合が表示されます。
Start Time	センサーで検知された干渉の開始時刻が表示されます。
Stop Time	センサーで検知された干渉の終了時刻が表示されます。
Duration	センサーで検知された干渉の期間が表示されます。
Center Frequency	干渉の中心周波数が表示されます。
Affected Channel(s)	干渉によって影響を受けたチャネル数が表示されます。
Recording Id	記録しているイベント ID が表示されます。
Additional Information	アラートでトリガされたイベントの干渉タイプが表示されます。
Active	アクティブなイベントの数が太字と赤のドットでハイライト表示されます。

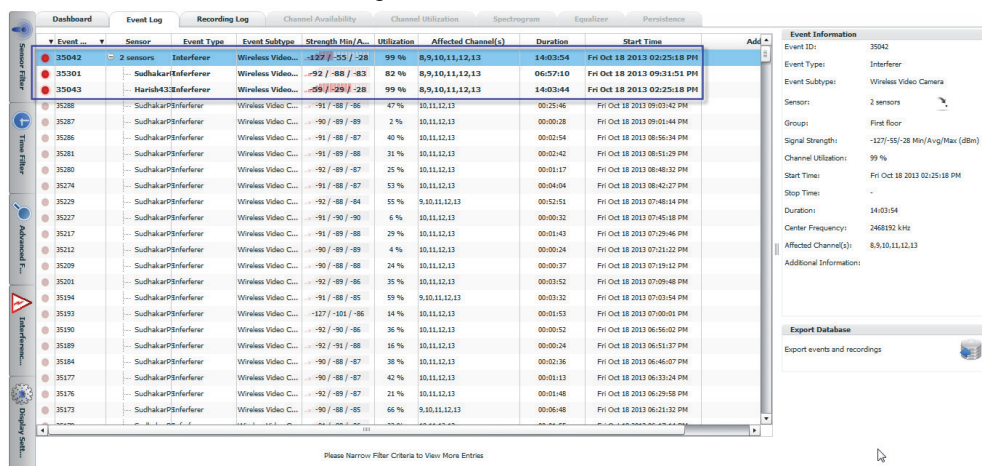
干渉イベントのクラスタリング

Spectrum Manager の [Event Log] 画面には、イベントのクラスタが表示されます。同一の干渉と干渉イベントに関連付けられている複数の干渉レポートは、同じクラスタ ID に割り当て

られます。複数のセンサーが同じ干渉イベントを報告する場合、その干渉イベントは、単一イベントとして報告されます。

112 ページの図 21 は、[Interference Event Clustering] 画面を示しています。

図 21: Interference Event Clustering



Spectrum Manager の [Event Log] 画面には、さまざまなコントロールパネルのタブが表示されます。詳細については、118 ページの「コントロールパネル」を参照してください。

Spectrum Manager - チャネル可用性

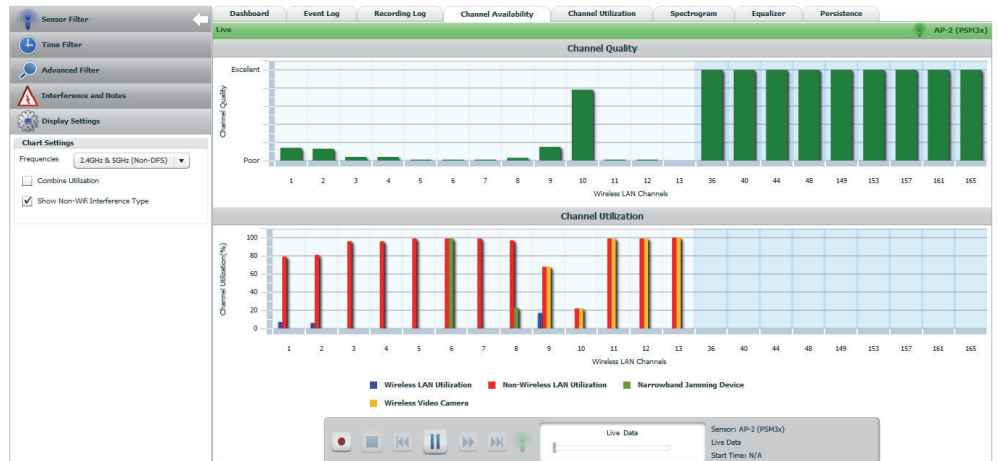
アクセス手順 : [Spectrum Manager] > [Monitor] > [Dashboard] > [Channel Availability]

1. [Channel Availability] タブを選択します。

[Channel Availability] 画面では、Channel Quality と Channel Utilization のグラフが表示されます。

113 ページの図 22 は、Spectrum Manager の [Channel Availability] 画面を示しています。

図 22: Spectrum Manager - チャネル可用性



2. Channel Quality と Channel Utilization のグラフは、Flash アプリケーションで表示されており、各 Wi-Fi チャネルについてリアルタイムで計算されたチャネル品質と、各チャネルで検出された干渉のレベルを表します。干渉は、802.11 の干渉と 802.11 以外の干渉とは異なります。Channel Utilization グラフでは、干渉ごとのチャネル使用率も表示されます。
3. 干渉はそれぞれ、干渉が使用されるチャネルのパーセンテージとして表示されます。



干渉ごとのチャネル使用率のタイプは、Channel Utilization グラフに表示されます。ただし、表示されるのは、[Display Settings] で [Show Non-Wifi Interference Type] オプションがチェックされている場合だけです。このオプションは、ハードウェア センサーについてのみ表示されます (129 ページの「ハードウェア センサー」を参照)。

4. [Channel Availability] 画面には、さまざまなコントロール パネルのタブが表示されます。詳細については、118 ページの「コントロール パネル」を参照してください。

Spectrum Manager - チャネル使用率

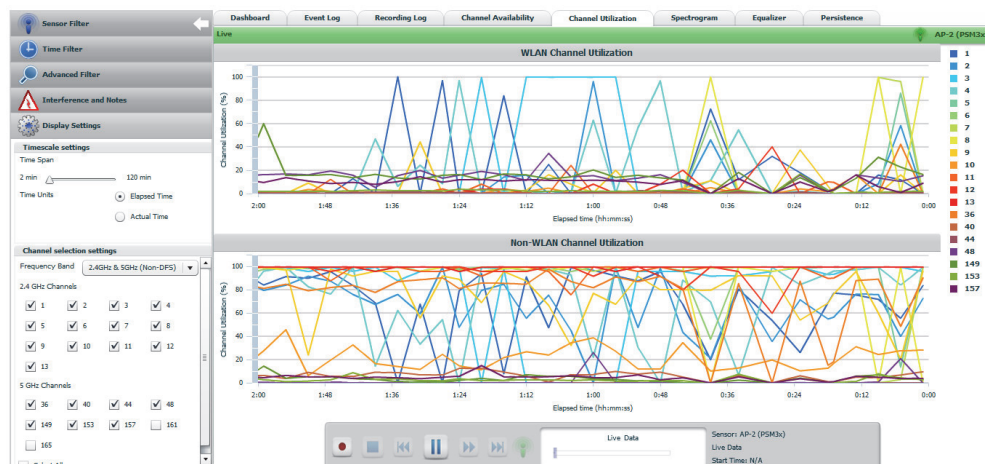
[Spectrum Manager] > [Monitor] > [Dashboard] > [Channel Utilization]

[Channel Utilization] タブを選択します。

114 ページの図 23 は、Spectrum Manager の [Channel Utilization] 画面を示しています。

[Channel Utilization] 画面には、WLAN Channel Utilization と Non-WLAN Channel Utilization のグラフが表示されます。このオプションは、ハードウェア センサーについてのみ表示されます (129 ページの「ハードウェア センサー」を参照)。

図 23: Spectrum Manager - チャネル使用率



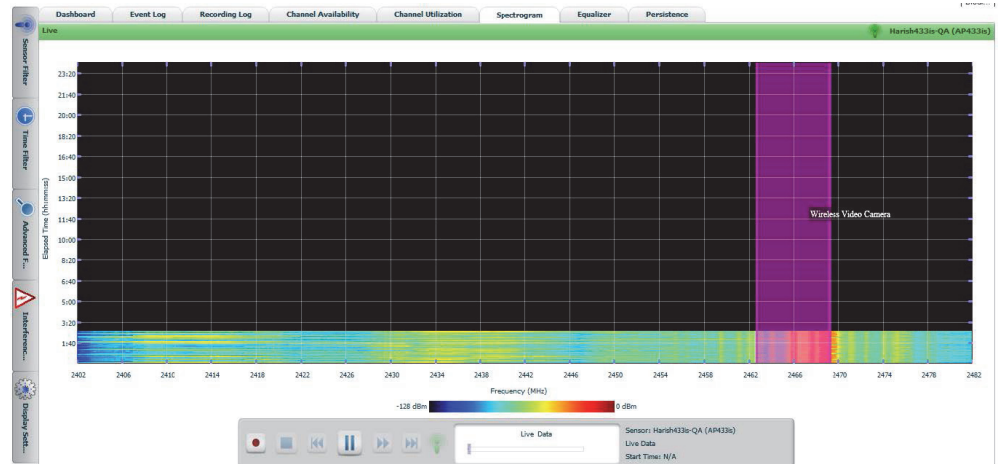
5. WLAN Channel Utilization と Non-WLAN Channel Utilization のグラフは、Flash アプリケーションで表示されており、各 WLAN と WLAN 以外のチャンネルについてリアルタイムで計算されたチャンネル使用率が示されます。
6. [Channel Utilization] 画面には、さまざまなコントロール パネルのタブが表示されます。詳細については、118 ページの「コントロール パネル」を参照してください。

Spectrum Manager - Spectrogram

アクセス手順 : [Spectrum] > [Monitor] > [Dashboard] > [Spectrogram]

1. [Spectrogram] タブを選択します。
115 ページの図 24 は、Spectrum Manager の [Spectrogram] 画面を示しています。
[Spectrogram] 画面では、干渉デバイスのスペクトラム動作が表示されます。

図 24: Spectrum Manager - Spectrogram



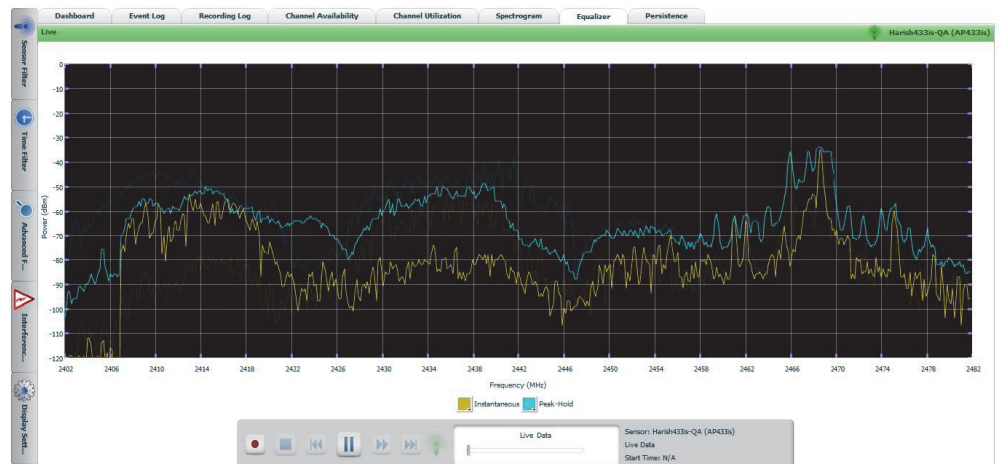
2. [Spectrogram] 画面をスクロールすると、以下の詳細情報が表示されます。
 - 時間の経過に伴って変化する RF エネルギーの周波数と振幅が表示されます。
 - X 軸には、周波数 (Mhz) または Wi-Fi チャンネル番号が表示されます。エネルギーの振幅は、即時データまたは最大ピーク ホールド振幅として示されます。振幅は、最弱の信号が青で表され、最強の信号が赤で表されます。
 - Y 軸には時間が表示されます。画面の下部に最新のデータが表示され、上部に向かってデータが示されます。
3. [Spectrogram] 画面には、さまざまなコントロール パネルのタブが表示されます。詳細については、118 ページの「コントロール パネル」を参照してください。

Spectrum Manager - イコライザ

[Spectrum] > [Monitor] > [Dashboard] > [Equalizer]

1. [Equalizer] タブを選択します。
116 ページの図 25 は、Spectrum Manager の [Equalizer] 画面を示しています。

図 25: Spectrum Manager - イコライザ



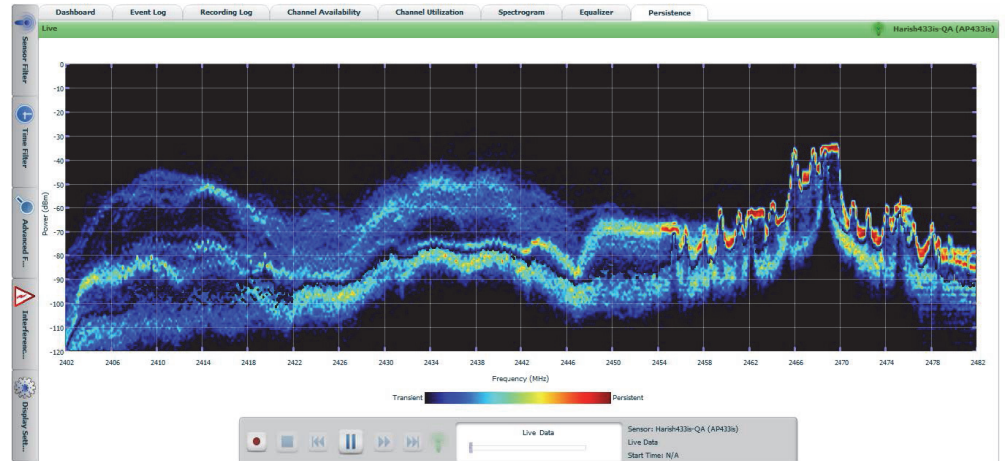
2. [Equalizer] 画面は、ブラウザにセンサーを起動する Flash アプリケーションで表示されます。[Equalizer] では、センサーでスキャンされた振幅と RF の周波数 (RF エネルギーまたは信号) を示します。センサーについては、**129 ページ**の「**センサー**」を参照してください。
3. [Spectrum Equalizer] には、振幅と、検出された RF エネルギーの周波数が示されます。X 軸の周波数の項目には、周波数 (MHz) か Wi-Fi チャンルのいずれかを表示できます。即時振幅 (スキャン期間中に収集された最新のデータ ポイント) と最大ピーク ホールド振幅 (スキャン期間中に収集された最高のデータ ポイント) が動的に示されます。即時データは黄で示され、ピーク ホールド データは青で示されます。色はユーザによる設定が可能です。
4. [Equalizer] 画面には、さまざまなコントロール パネルのタブが表示されます。詳細については、**118 ページ**の「**コントロール パネル**」を参照してください。

Spectrum Manager - パーシステンス

[Spectrum] > [Monitor] > [Dashboard] > [Persistence]

1. [Persistence] タブを選択します。
117 ページの図 26 は、Spectrum Manager の [Persistence] 画面を示しています。

図 26: Spectrum Manager - パーシステンス



2. [Persistence] 画面は Flash アプリケーションで表示されます。[Persistence] 画面では、干渉デバイスのスペクトラム アクティビティが示され、干渉イベントを表示するためのチャンネルのパーシステンス リンクを確認できます。
3. [Persistence] 画面には、**振幅**と、検出された RF エネルギーの**周波数**が示されます。即時振幅 (スキャン期間中に収集された最新のデータ ポイント) と最大ピーク ホールド振幅 (スキャン期間中に収集された最高のデータ ポイント) が動的に示されます。画面上のピクセルの色は、特定の周波数および振幅で検出されたエネルギーの回数を表しており、青は最新の周波数、赤は最高の周波数を示します。

[Persistence] 画面には、さまざまなコントロールパネルのタブが表示されます。詳細については、**118 ページの「コントロールパネル」**を参照してください。

コントロール パネル

コントロール パネルは、[Dashboard] 画面の左側に表示されます。

以下の項目では、[Monitor Console] 画面で利用可能なさまざまなコントロール パネルのタブについて説明しています。

- [Sensors Filter \(118 ページ\)](#)
- [Advanced Filter \(120 ページ\)](#)
- [Interference \(121 ページ\)](#)
- [Display Settings \(122 ページ\)](#)

Sensors Filter

Sensors Filter では、センサー階層下でセンサーを選択することで、画面に表示される情報をフィルタリングできます。次の手順を実行して、センサー フィルタを設定します。

- [Sensors Filter] タブを選択します。配備されているセンサーのリストが表示されます。
- [Sensor hierarchy] でセンサーを選択し、[Filter selected Group/sensor] をクリックします。以下の変更も生じます。
 - 選択したセンサーが [Dashboard] 画面の [Trend Graph]、[Interferer Type]、[Affected Channels] セクションに表示されます。
 - [Event Log] 画面では、選択したセンサーでイベント ログの詳細情報が更新されます。
- [Sensors Filter] タブには、以下の 2 つのセクションが表示されます。
 - [Sensors Hierarchy \(118 ページ\)](#)
 - [Group Information \(118 ページ\)](#)

Sensors Hierarchy

[Sensors Hierarchy] セクションには、コントローラに属しているセンサーの階層が表示されます。

Group Information

[Group Information] セクションには、選択した [Enterprise]、[Campus]、[Building]、[Floor]、[AP] の詳細が表示されます。

- 選択した [Enterprise]、[Campus]、[Building]、[Floor]、[AP] の以下の詳細情報が表示されます。
 - Name - センサーの名前が表示されます。
 - Description - センサーの MAC アドレスが表示されます。
 - IP Address - センサーの IP アドレスが表示されます。

- Status - センサーの接続ステータスが表示されます。
- 上部の [Sensors Hierarchy] セクションから [Enterprise]、[Campus]、[Building]、[Floor]、[AP] を選択します。
- [Filter Selected Group/Sensor] オプションを選択します。
- 選択したセンサーのグラフが [Dashboard] 画面の [Trend Graph]、[Interferer Type]、[Affected Channels] セクションに表示されます。

[Sensors Filter] タブは、以下のタブでのみ有効です。

- Dashboard
- Event Log

Time Filter

Time Filter では、画面を設定して、長期にわたる情報を表示できるようにします。これを実行するには、ページで [Start Time] と [Stop Time] パラメータを設定します。

次の操作を実行して、*Time Filter* を設定します。

- [Time Filter] タブを選択します。
- [Time Filter] タブには、以下の 2 つのセクションが表示されます。
 - [Start Time \(119 ページ\)](#)
 - [Stop Time \(119 ページ\)](#)

Start Time

- [Earliest Time Possible] オプションを選択します。最も早い時刻に利用できるデータがフェッチされます。
- [Start Time] を選択するには、[Earliest Time Possible] オプションのチェックをオフにします。
- [Time] オプションで、ドロップダウン・リストから時刻を選択します。表示形式は、*hh:mm:ss* です。
- [Date] オプションから、カレンダーのアイコンを選択し、*月*、*日*、*年*を選択します。表示形式は、*mm/dd/yyyy* です。

Stop Time

- [Use Current Time] オプションを選択します。現在の時刻が適用されます。
- [Stop Time] を選択するには、[Use Current Time] オプションのチェックをオフにします。
- [Time] オプションで、ドロップダウン・リストから時刻を選択します。表示形式は、*hh:mm:ss* です。
- [Date] オプションから、カレンダーのアイコンを選択し、*月*、*日*、*年*を選択します。表示形式は、*mm/dd/yyyy* です。

- [Apply Time Filter] オプションを選択します。
- [Time Filter] が [Dashboard] 画面の [Trend Graph]、[Interferer Type]、[Affected Channels] セクションに適用されます。

[Time Filter] タブは、以下のタブに適用され、有効になります。

- Dashboard
- Event Log

Advanced Filter

[Advanced Filter] オプションでは、利用可能な以下のフィルタを選択することで、画面に表示する情報を設定できます。

- チャンネル フィルタ
 - このフィルタは、利用可能なチャンネルに基づく情報のフィルタリングを可能にします。
 - [Channel] リストから目的のチャンネルを選択します。
 - [Apply Filter] を選択します。チャンネル フィルタは [Dashboard] 画面と [Event Log] 画面に適用されます。
- RSSI フィルタ
 - このフィルタは、干渉デバイスの信号強度を表します。
 - 目的の RSSI 値を [RSSI Filter] リストから選択します。表示される値の単位は、dBm です。
 - [Apply Filter] を選択します。RSSI フィルタは、[Dashboard] 画面と [Event Log] 画面に適用されます。
- 干渉タイプ
 - このフィルタは、干渉タイプを表します。
 - 干渉タイプ オプションのリストを使用して選択できます。
 - 目的の干渉タイプを選択します。
 - [Apply Filter] を選択します。干渉タイプフィルタは、[Dashboard] 画面に適用されます。



上記の [Advanced Filter] の干渉タイプ オプションは、[Dashboard] 画面でのみ有効です。

-
- イベント ログ タイプ
 - このフィルタは、イベント ログ タイプ (Alert Event または Interferer Log Event) を表します。

- [Interferer Log Events] と [Alert Event] のオプション リストは、[Event log] サブタイプで使用して選択できます。
- 目的のイベント ログ タイプを選択し、さらに目的のイベント サブタイプを選択します。
- [Apply Filter] を選択します。イベント ログ タイプ/ サブタイプのフィルタは、[Event Log] 画面に適用されます。



上記の [Advanced Filter] オプションは、[Event Log] 画面でのみ有効です。



[Advanced Filter] タブは、以下のタブでのみ有効です。

[Dashboard]

[Event Log]

Interference

[Interference] セクションには、以下の項目が表示されます。

- [Start Time]: 干渉および干渉タイプの開始時刻です。
- [Add Note]: Add Note アイコンを使用してメモを追加できます。



[Notes] セクションが有効なのは、手動での記録が完了したときです。[Notes] セクションには、以下の項目が表示されます。

[Delete Note] - [Delete Note] アイコンを使用してメモを削除できます。

[Timestamps] - [Timestamp] は、現在記録している再生時間をメモのタイムスタンプに合わせるために使用します。

[Interference and Notes] オプションは、以下のタブで表示されます。

- [Channel Availability]
- [Channel Utilization]
- [Spectrogram]
- [Equalizer]
- [Persistence]

Display Settings

[Display Settings] オプションでは、以下の画面に表示する情報を設定できます。



[Display Settings] タブは、以下のタブでのみ有効です。

- [Event Log]
- [Channel Availability]
- [Channel Utilization]
- [Spectrogram]
- [Equalizer]
- [Persistence]

[Event Log] - [Display Settings]

[Event Log] 画面に表示するカラムを選択するには、以下のアクションを実行します。

- [Event Log] タブを選択します。[Event Log] 画面が表示されます。
- [Display Settings] タブを選択します。
- 表示するカラムを選択します。
- 選択したカラムが [Event Log] 画面に表示されます。



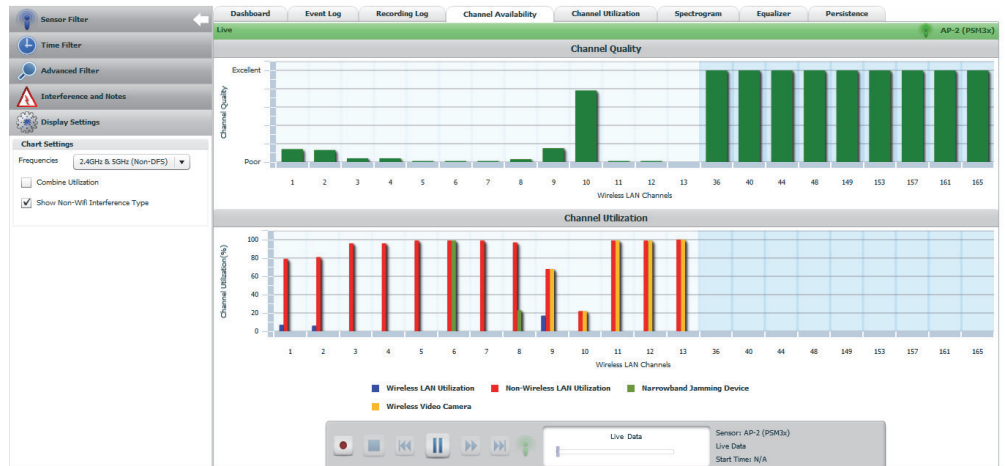
デフォルト カラムを表示するには、[Apply Default Column Setting] オプションを選択します。

[Channel Availability] - [Display Settings]

[Channel Availability] 画面のグラフ表示を変更するには、以下のアクションを実行します。

- [Channel Availability] タブを選択します。[Channel Availability] 画面が表示されます。
- [Display Settings] タブを選択します。(123 ページの [図 27](#) は、[Display Settings] の [Channel Availability] 画面を示しています)
- [Chart Settings] オプションが表示されます。

図 27: [Display Settings] - [Channel Availability]



- ドロップダウン リストから周波数を選択して、それぞれのチャンネルのチャンネル品質とチャンネル使用率を表示します。[Display Frequency] を設定して、2.4 GHz 周波数帯、5 GHz 周波数帯、または両方をスキャンできます。
- [Combine Utilization] オプションを選択します。これによって、Channel Utilization グラフ (Channel Quality 内) で 非ワイヤレス LAN 干渉とワイヤレス LAN 干渉を組み合わせることが可能になります。

[Channel Utilization] - [Display Settings]

[Channel Availability] 画面のグラフ表示を変更するには、以下のアクションを実行します。

- [Channel Utilization] タブを選択します。[Channel Utilization] 画面が表示されます。
- [Display Settings] タブを選択します。
- 以下のセクションが表示されます (124 ページの図 28 は、[Display Settings] の [Channel Utilization] 画面を示しています)。
 - [Timescale settings] (123 ページ)
 - [Channel selection settings] (123 ページ)

[Timescale settings]

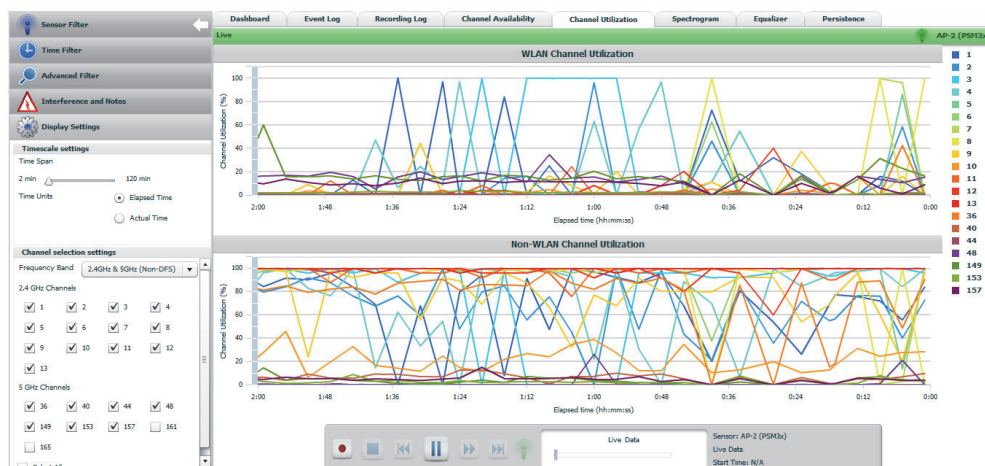
- [Time Span] で期間を選択します。有効な範囲は、2 分 ~ 120 分です。
- [Time Units] で時間単位を選択します。時間単位では、[Elapsed Time] (経過時間) または [Actual Time] (実時間) を選択できます。

[Channel selection settings]

[Frequency Band] のドロップダウン リストから周波数帯を選択します。

[Select All] オプションを選択すると、すべての WLAN チャンネル利用率が表示されます。

図 28: [Display Settings] - [Channel Utilization]



[Spectrogram] - [Display Settings]

[Spectrogram] - [Display Settings] を選択すると、以下のオプションが表示されます。

1. [Data]

- [Data] では、データのオプションを選択します。データのオプションとして、[Instantaneous] データまたは [Peak] データを選択できます。

2. [Time Span]

- [Time Span] では期間を選択します。期間の範囲は、[Long - Short] 間になります。

3. [Axis]

- [Axis] では軸のタイプを選択します。軸は、周波数と Wi-Fi チャンネルに基づいて構成されます。

[Frequency]: このオプションを選択すると、周波数に基づいてグラフが表示されます。

[Wi-Fi Channels]: このオプションを選択すると、Wi-Fi チャンネルに基づいてグラフが表示されます。[Wi-Fi Channels] オプションを選択すると、以下のパラメータが表示されます。

- [Highlight Channel]: [Highlight Channel] オプションのチェックボックスをオンにすると、X 軸のチャンネルにマウスカーソルを重ねたときにチャンネルがハイライト表示されます。

- [Wi-Fi Channel Width]: ドロップダウン リストから [Wi-Fi Channel Width] を選択します。これにより、表示するスペクトログラムのチャンネル幅が設定されます。ドロップダウン リ

ストからいずれかのオプションを選択します。オプションとしては、20Mhz、20Mhz+Upper 20 Mhz と 20Mhz+Lower 20 Mhz があります。



[Wi-Fi Channel Width] オプションが有効になるのは、選択した [Axis] が [Wi-Fi Channels] のときだけです。

4. [Band]

- [Band] リストからいずれかのオプションを選択します。
- 各帯のスペクトログラムは、ドロップダウン リストからいずれかのオプションを選択して設定できます。
- オプションには、2.4GHz、5GHz (低)、5GHz (高) があります。

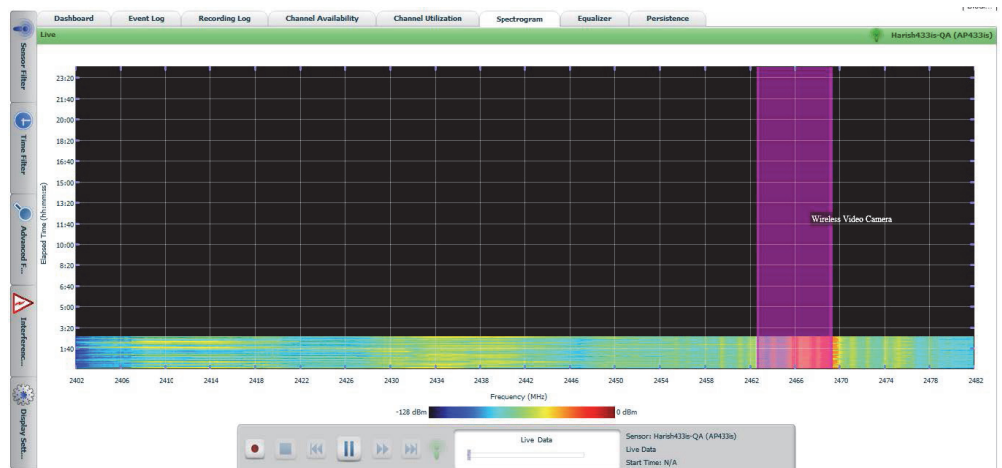


それに応じて、短期のスペクトログラム測定基準がグラデーションで表示されます。

5. [Overlay Interference] - このオプションを選択すると、特定の干渉のスペクトラム アクティビティがハイライト表示されます。

たとえば、目立つ干渉イベントが多いときに、特定の干渉を表示する場合には、その干渉デバイスのオーバーレイをチェックできます (125 ページの図 29 は、[Display Settings] の [Spectrogram] 画面を示しています)。

図 29: [Display Settings] - [Spectrogram]



マーカー

1. [Spectrogram] タブを選択します。[Spectrogram] 画面が表示されます。
2. [Display Settings] タブを選択します。

3. [Markers] セクションを選択します。
4. マーカーは、[Spectrogram] プロットの周波数に視覚的な印を付けるために使用できます。
5. [Markers] セクションでマーカーのチェックボックスをオンにします。マーカーが [Spectrogram] グラフに表示されます。
6. 画面でマーカーを選択し、それを目的の周波数まで移動し、視覚的な印を付けます。

[Equalizer] - [Display Settings]

[Equalizer] - [Display Settings] を選択すると、以下のオプションが表示されます。

1. [Persistence]

- [Persistence] ではパーシステンスの範囲を選択します。
- パーシステンスを設定すると、グラフで時間に基づくトレンドを学習できます。画面のパーシステンスを高めると、サンプルが保持および表示される時間が長くなり、時間の経過に伴う変化を確認できます。これは画面設定のバーで、ゼロから無限まで設定できます。
(127 ページの図 30 は、[Display Settings] の [Equalizer] 画面を示しています)。

2. [Axis]

- [Axis] では軸のタイプを選択します。軸は、周波数と Wi-Fi チャンネルに基づいて構成されます。
 - [Frequency]: このオプションを選択すると、周波数に基づいてグラフが表示されます。
 - [Wi-Fi Channels]: このオプションを選択すると、Wi-Fi チャンネルに基づいてグラフが表示されます。[Wi-Fi Channels] オプションを選択すると、以下のパラメータが表示されます。

- [Highlight Channel]: [Highlight Channel] オプションのチェックボックスをオンにすると、X 軸のチャンネルにマウスカーソルを重ねたときにチャンネルがハイライト表示されます。

- [Wi-Fi Channel Width]: ドロップダウン リストから [Wi-Fi Channel Width] を選択します。これにより、表示するスペクトログラムのチャンネル幅が設定されます。ドロップダウン リストからいずれかのオプションを選択します。オプションとしては、20Mhz、20Mhz+Upper 20 Mhz、20Mhz+Lower 20 Mhz があります。

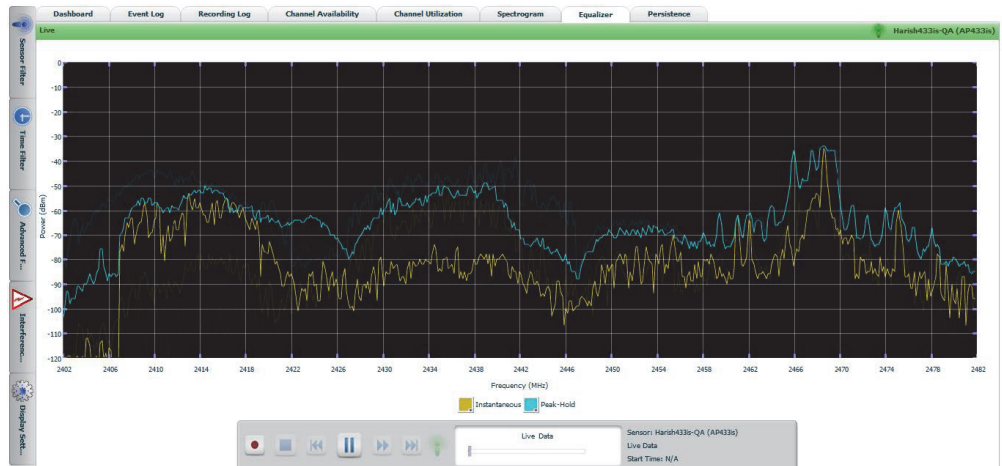


[Wi-Fi Channel Width] オプションが有効になるのは、選択した [Axis] が [Wi-Fi Channels] のときだけです。

1. [Band]

- [Band] リストからいずれかのオプションを選択します。
- 各帯の Equalizer は、ドロップダウン リストからいずれかのオプションを選択すると設定されます。
- オプションには、2.4GHz、5GHz (低)、5GHz (高) があります。

図 30: [Display Settings] - [Equalizer]



マーカー

1. [Equalizer] タブを選択します。[Equalizer] 画面が表示されます。
2. [Display Settings] タブを選択します。
3. [Markers] セクションを選択します。
4. マーカーは、[Equalizer] プロットの周波数に視覚的な印を付けるために使用できます。
5. [Markers] セクションでマーカーのチェックボックスをオンにします。マーカーが Equalizer グラフに表示されます。
6. 画面でマーカーを選択し、それを目的の周波数まで移動し、視覚的な印を付けます。

[Persistence] - [Display Settings]

[Persistence Settings] を選択すると、以下のオプションが表示されます。

1. [Persistence]
 - [Persistence] ではパースステンスの範囲を選択します。
 - パースステンスを設定すると、グラフで時間に基づくトレンドを学習できます。画面のパースステンスを高めると、サンプルが保持および表示される時間が長くなり、時間の経過に伴う変化を確認できます。これは画面設定のバーで、ゼロから無限まで設定できます。
- 128 ページの図 31 は、[Display Settings] の [Persistence] 画面を示しています。
2. [Axis]
 - [Axis] では軸のタイプを選択します。
 - 軸は、周波数 Wi-Fi チャンネルに基づいて構成されます。

- [Frequency]: このオプションを選択すると、周波数に基づいてグラフが表示されます。
- [Wi-Fi Channels]: このオプションを選択すると、Wi-Fi チャンネルに基づいてグラフが表示されます。[Wi-Fi Channels] オプションを選択すると、以下のパラメータが表示されます。

[Highlight Channel]: [Highlight Channel] オプションのチェックボックスをオンにすると、X 軸のチャンネルにマウスカーソルを重ねたときにチャンネルがハイライト表示されます。

[Wi-Fi Channel Width]: ドロップダウン リストから [Wi-Fi Channel Width] を選択します。これにより、表示するスペクトログラムのチャンネル幅が設定されます。ドロップダウン リストからいずれかのオプションを選択します。オプションとしては、20Mhz、20Mhz+Upper 20 Mhz、20Mhz+Lower 20 Mhz があります。

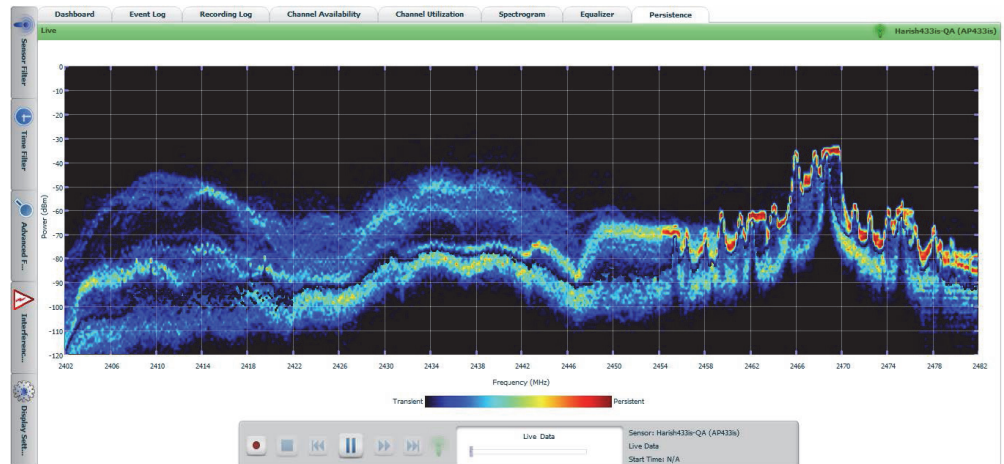


[Wi-Fi Channel Width] オプションが有効になるのは、選択した [Axis] が [Wi-Fi Channels] のときだけです。

1. [Band]:

- [Band] リストからいずれかのオプションを選択します。
- 各帯の Equalizer は、ドロップダウン リストからいずれかのオプションを選択すると設定されます。
- オプションには、2.4GHz、5GHz (低)、5GHz (高) があります。

図 31: [Display Settings] - [Persistence]



マーカー

1. [Persistence] タブを選択します。[Persistence] 画面が表示されます。
128 ページの図 31 は、[Display Settings] の [Persistence] 画面を示しています。

2. [Display Settings] タブを選択します。
3. [Markers] セクションを選択します。マーカーは、[Persistence] プロットの周波数に視覚的な印を付けるために使用できます。
4. [Markers] セクションでマーカーのチェックボックスをオンにします。マーカーが [Persistence] グラフに表示されます。
5. 画面でマーカーを選択し、それを目的の周波数まで移動し、視覚的な印を付けます。

センサー

センサーは、以下のように分類されます。

ソフトウェア センサー

ソフトウェア ベースのセンサーは、「スキャン スペクトラム」モードで無線が 1 つある標準 AP です。AP モードは「サービス モード」から「スキャン スペクトラム」モードに変更できます。



「サービス モード」から「スキャン スペクトラム」モードへの AP モードの変更は、[FortiWLC (SD)] でのみ実行されます。

ソフトウェア センサーには、以下のアクセス ポイントが含まれます。

- AP110、AP1014i
- AP1010i、AP1010e、AP1020i、AP1020e
- AP332i、AP332e
- AP832
- FAP-U421EV
- FAP-U423EV

ハードウェア センサー

ハードウェア ベースのセンサーは完全に、時間のエアウェーブの監視専用です。専用サブシステムがあるセンサーのため、無線から CPU リソースを取り上げることなく、ほぼ瞬時に干渉のタイプとソースについて分類およびレポートできます。ハードウェア センサーには、以下のアクセス ポイントが含まれます。

- PSM3x
- AP433is

RF 干渉の分類

Wi-Fi ネットワークが稼働するのは、ライセンスを受けていない 2.4 および 5 GHz 周波数帯であり、これはさまざまな他のデバイスとともに媒体を共有します。Bluetooth デバイスは例外ですが、それ以外のデバイスは Wi-Fi ネットワークと共存する構造になっていません。結果として、デバイスを干渉することで、通信向けに WLAN アクセス ポイントが使用されている WLAN チャンネルでエネルギーが放出され、AP のスループットに大きな影響が及ぶ可能性があります。

スペクトラムは、非 802.11 干渉デバイスをすべて検出します。特に、以下のリストに示されているデバイスが検出されます。

- 電子レンジ (従来型)
- 電子レンジ (インバータ式)
- Motorola Canopy Wireless
- 非 Wi-Fi ワイヤレス ブリッジ
- ワイヤレス ビデオ カメラ (デジタルとアナログ)
- アナログ コードレス フォン (2.4GHz と 5GHz)
- FHSS コードレス フォン (2.4GHz と 5GHz)
- DSSS コードレス フォン (2.4GHz と 5GHz)
- Bluetooth デバイス
- ワイヤレス ベビー モニタ
- ゲーム コントローラ
- RF ジャマー (狭帯域と広帯域の両方)
- ワイヤレス マウス
- Zigbee デバイス
- モーション ディテクター (S バンドおよびレーダーベース)

上記のデバイスに加え、RF Jamming デバイスも存在します。RF Jamming デバイスは、意図的にワイヤレス通信に干渉するために使用できます。ただし、これらのデバイスは米国などで違法であると考えられており、WLAN でのパフォーマンスとセキュリティの問題の原因となっています。

IEEE 802.11 規格をベースとするワイヤレス LAN は、ライセンスを受けていない 2.4 と 5 GHz の周波数帯で機能します。これらの帯域で無線周波数エネルギーを放出しているその他のデバイスは、WLAN 送信に干渉できます。[132 ページの「干渉デバイスの無線周波数の特性」](#)では、よくある RF 干渉とそれらの RF 特性の一部のリストを示しています。

干渉デバイスの無線周波数の特性

干渉デバイスの無線周波数の特性は、以下のリストのとおりです。

配備の観点からすると、スペクトラムのカバレッジはそのセンサー（受信機の感度）に依存するだけでなく、干渉デバイスの送信電力（または信号強度）にも依存します。離れた場所にはセンサーを配置できず、非常に低い信号強度の干渉デバイス パケットがセンサーに達すると考えられています。

理論上は、干渉デバイスの信号強度を下げるには、それらのデバイスを捉えるために多くのセンサーをパックする必要があります。

129 ページの「[センサー](#)」(129 ページの「[ソフトウェア センサー](#)」および 129 ページの「[ハードウェア センサー](#)」) は、利用する AP から少なくとも 6 フィート (1.8 メートル) 離れた場所にインストールする必要があります。それらを近づけると、干渉分類の精度に影響します。



利用する AP は、PSM3x の近くに設置しないようにしてください。AP の近くで放出される EMI (電磁干渉) が原因で誤イベント (アナログ コードレス フォンなど) が PSM3x センサーによって検出される可能性があります。

例：

Bluetooth には 2.2 dBm の送信電力があり、センサーでキャプチャするには、センサーを近くの特定期間サイトに配置する必要があります。このため、干渉デバイスの信号強度は、センサーのカバレッジ エリアに反比例します。

また、センサーのカバレッジ エリアは、受信機の感度に比例します。受信機の感度が高いと (高ゲインのアンテナで実現可能)、上記の例と比較して、もっと間隔を空けてセンサーを分散できます。

つまり、センサーのカバレッジ エリアは、検出される干渉デバイスの最小信号強度とセンサーの受信機の感度に依存します。干渉デバイスの信号強度と受信機の感度が高いほど、センサーのカバレッジは広くなり、逆に強度と感度が低いほど、範囲は狭くなります。上記の要素を

考慮すると、予測可能なカバレッジは、以下の表のように特定できます (一定の干渉送信電力がある場合)。これにより、管理者またはユーザの環境で、センサーの配備を予測できます。

表 9: 干渉デバイスの無線周波数の特性

干渉デバイス	周波数の範囲	送信電力	変調	サポートされている通信チャンネル数	幅	特徴
Bluetooth	2402 ~ 2480 MHz	2.2 dBm	GFSK、FHSS	79	1 MHz	パルス型、低電力
アナログコードレスフォン	2403 ~ 2480 MHz	なし	狭帯域 FM	40	300 kHz 未満	狭帯域 FM
DSSS デジタルコードレスフォン	2407.5 ~ 2472 MHz	20 dBm	DSSS	40	1.5 MHz	高電力、デューティ係数
FHSS デジタルコードレスフォン	2408.5 ~ 2472 MHz	21 dBm	FHSS	90	892 kHz	パルス型、高電力
従来式の電子レンジ	2.4 GHz	800 W	N/A	N/A	N/A	パルス型、広帯域
インバータ式電子レンジ	2.4 GHz	1300W	N/A	N/A	N/A	パルス型、広帯域
ワイヤレスビデオカメラ	2414 ~ 2468 MHz	10 dBm	周波数変調 (FM)	4	N/A	広帯域、高電力
デジタルビデオモニター	2402 ~ 2483 MHz	20 dBm	FHSS	27	2 MHz	高電力、周波数ホッピング
ゲームコントローラ	2402 ~ 2482 MHz	N/A	FHSS	40	500 kHz	パルス型、低電力、周波数ホッピング

RF 干渉の検出

音声通信や動画通信などの重要なアプリケーションをサポートしている WLAN により、RF 干渉の監視と管理はセキュリティ上、不可欠なものになっています。干渉の発生原因としては、RF ジャマーなどの意図的で悪意あるものから、近くで使用されているコードレスフォンといった意図しないものが考えられます。いずれの場合でも、それらのアプリケーションで

必要とされるリアルタイム通信をサポートする WLAN の機能は、RF 干渉によって深刻な侵害を受ける可能性があります。WLAN は、このようなセキュリティ問題を引き起こす干渉を RF 環境で継続的に検出し、ネットワーク管理者に対してアラートをトリガできる必要があります。

[Event Log] ページのリストに表示されるセンサーは、干渉イベント情報を示します。

133 ページの図 32 は、[Event Log] 画面で表示されるセンサー リストを示しています。

図 32: [Event Log] 画面で表示されるセンサー リスト

Dashboard

Event Log

Recording Log

Channel Availability

Channel Utilization

Spectrogram

Equalizer

Persistence

▼ Sensor Filter

Time Filter

Advanced Filter

Interference

Display Settings

Event ...	Sensor	Event Type	Event Subtype	Strength Hi/A...	Utilization	Affected Channel(s)	Duration	Start Time
▼ 35478	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-93 / -70 / -62	10 %	5,6,7,8,9	00:01:34	Sat Oct 19 2013 04:15:42 AM
● 35042	2 sensors	Interferer	Wireless Video...	-127 / -55 / -28	99 %	8,9,10,11,12,13	13:52:03	Fri Oct 18 2013 02:25:18 PM
35476	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-92 / -71 / -54	30 %	5,6,7,8,9	00:11:00	Sat Oct 19 2013 04:03:41 AM
35474	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-94 / -71 / -56	30 %	5,6,7,8,9	00:02:55	Sat Oct 19 2013 03:59:30 AM
35472	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-94 / -72 / -56	25 %	5,6,7,8,9	00:03:45	Sat Oct 19 2013 03:54:40 AM
35470	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-94 / -72 / -71	55 %	5,6,7,8,9	00:00:55	Sat Oct 19 2013 03:52:21 AM
35468	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-94 / -71 / -54	35 %	5,6,7,8,9	00:02:49	Sat Oct 19 2013 03:48:19 AM
35466	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-93 / -70 / -55	34 %	5,6,7,8,9	00:07:12	Sat Oct 19 2013 03:39:56 AM
35464	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-95 / -71 / -55	28 %	5,6,7,8,9	00:03:47	Sat Oct 19 2013 03:34:43 AM
35462	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-97 / -68 / -55	31 %	4,5,6,7,8,9	00:01:54	Sat Oct 19 2013 03:31:27 AM
35460	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-94 / -68 / -55	41 %	4,5,6,7,8,9	00:01:26	Sat Oct 19 2013 03:28:23 AM
35458	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-96 / -70 / -55	23 %	5,6,7,8,9	00:02:52	Sat Oct 19 2013 03:24:10 AM
35456	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-95 / -71 / -55	27 %	5,6,7,8,9	00:02:31	Sat Oct 19 2013 03:20:20 AM
35454	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-97 / -72 / -72	40 %	5,6,7,8,9	00:00:31	Sat Oct 19 2013 03:18:20 AM
35452	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-92 / -72 / -65	15 %	5,6,7,8,9	00:02:23	Sat Oct 19 2013 03:14:09 AM
35450	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-94 / -72 / -71	49 %	5,6,7,8,9	00:00:23	Sat Oct 19 2013 03:12:36 AM
35448	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-97 / -72 / -65	17 %	4,5,6,7,8,9	00:01:01	Sat Oct 19 2013 03:10:21 AM
35446	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-96 / -70 / -55	19 %	5,6,7,8,9	00:04:06	Sat Oct 19 2013 03:04:19 AM
35444	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-95 / -71 / -55	24 %	5,6,7,8,9	00:05:05	Sat Oct 19 2013 02:58:08 AM
35442	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-96 / -70 / -54	30 %	4,5,6,7,8,9	00:03:42	Sat Oct 19 2013 02:53:13 AM
35440	Harish433e-QA Interferer	Narrowband Jam...	Narrowband Jam...	-96 / -60 / -48	12 %	5,6,7,8,9	00:00:18	Sat Oct 19 2013 02:47:34 AM
35438	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-95 / -72 / -56	15 %	5,6,7,8,9	00:04:45	Sat Oct 19 2013 02:45:35 AM
35436	SudhakarPSM-Interferer	Narrowband Jam...	Narrowband Jam...	-97 / -71 / -63	45 %	5,6,7,8,9	00:00:54	Sat Oct 19 2013 02:42:41 AM

Event Information

Event ID: 35478

Event Type: Interferer

Event Subtype: Narrowband Jamming Device

Sensor: SudhakarPSM-HF (PSM43)

Group: First Floor

Signal Strength: -77/-70/-62 Mm [Avg]Max (dBm)

Channel Utilization: 10 %

Start Time: Sat Oct 19 2013 04:15:42 AM

Stop Time: -

Duration: 00:01:34

Center Frequency: 2441000 kHz

Affected Channel(s): 5,6,7,8,9

Additional Information:

Export Database

Export events and recordings

35

Please Narrow Filter Criteria to View More Entries

各干渉デバイス信号は、干渉イベントとして扱われ、以下のパラメータで検出されます。

- Event Subtype (干渉のタイプ)
- Signal Strength (現在 / 平均 / 最大) dBm
- Affected Channel(s) (影響を受けたチャネル)
- Center frequency (中心周波数)
- Duration (干渉イベントが確認された時間)
- Start Time (干渉イベントが開始した時刻)
- Stop Time (干渉イベントが終了した時刻)

アクティブな干渉イベントは、太字フォントと赤のドットでハイライト表示されます。

現時点で動作していないイベントは、グレー表示されます。

RF 干渉の分類は、以下のパラメータで検出されます。

- Channel
- Signal Strength

- Interferer

干渉は以下のように検出されます。

- 特定チャンネルでフィルタを選択する。
- - 10 dBm 以上 ~ -110 dBm 以上の範囲で信号強度をフィルタリングして検出される信号強度を変化させることで、2.4GHz と 5GHz スペクトラムに変動する干渉を検出できます。
- 干渉デバイスを特定する。
信号強度の範囲における全チャンネル、かつ全タイプの干渉デバイスでの干渉も「All」を選択することでフィルタリングできます。

履歴スペクトラム ダッシュボード分析

Spectrum Manager からは、分析用の履歴スペクトラム データが提供されます。干渉デバイスへの影響は、日時データを含む、利用可能な過去データで判断できます。干渉デバイスで引き起こされる干渉イベントは、*Spectrum Manager* データベースに保存され、将来の分析に使用されます。干渉イベントの履歴は 1 年間保持されます。

イベント ログ

特定のセンサーからトリガされたイベントは統合され、キャプチャされて [Event Log] 画面に表示されます。[Event Log] 画面は、133 ページの [図 32](#) に示されています。

時間ベースの分析

スペクトラム イベントは、時間ベースでトリガされるイベントであり、「開始時刻」と「終了時刻」は提供されません。現在の干渉アクティビティのダッシュボードが表示されます。ダッシュボードをリアルタイムで表示するには、[Earliest Time possible in Start time and Use current time in Stop time] のチェックボックスがオンになっていることを確認します。

Proactive Spectrum Manager

Proactive Spectrum Manager は、単一のチャンネル環境向けに設計されており、チャンネル スペクトラムの最上位のビューと、ネットワーク運用時の最良のチャンネルについての推奨事項を提示します。PSM ダッシュボードには、すべてのチャンネルの適合値とネットワーク運用時の推奨チャンネルが緑 (適合) と赤 (未使用) の棒グラフで表示されます。

Web UI を使用した Proactive Dashboard Manager の設定

ダッシュボードを使用して、スペクトラムに対するチャンネル適合と 2.4GHz および 5GHz の帯域の 20MHz またはチャンネル ボンド (40MHz) に使用できる最良のチャンネルを確認します。スペクトラムには、20MHz と 40MHz のすべてのチャンネルの適合値が棒グラフで表示されま

す。棒グラフが長いほど、チャンネルの状態が良いことを表します。棒グラフがグレーで表示される場合は、そのチャンネルで検知できないことを表します。

2 つの PSM オプション、View と Evaluate があります。

- デフォルトで、View はすべてのチャンネル上で有効です。View モードは、不正などの干渉を監視し、チャンネル使用についての推奨事項を表示します。図の各チャンネル上に緑色の帯が見える場合は、View のみが有効であるか、または、Evaluate も有効であり、どのチャンネルにも不正がありません。
- デフォルトでは、Evaluate はすべてのチャンネルで無効です。チャンネルで Evaluate モードを有効にすると、PSM は、指定した量の不正アクティビティを持つチャンネルからデバイスを移動し、これらのチャンネルの使用を管理します。Evaluate を有効にするには、以下の手順を実行します。

1. [Monitor] > [Spectrum Manager] > [PSM] をクリックします。
2. 画面の上部にある [Evaluate] をクリックします。

オプションで、[Evaluate] ドロップダウン リストからいずれかのオプションを選択します。

[View] では、不正検出がオンになり、ただちにスキャンが実行され、不正検出がオフになり、結果が表示されます。

[One Time Adapt] では、不正検出がオンになり、スキャンが実行され、不正検出がオフになり、ステーションがただちに推奨チャンネルへと移動します。

[Periodic Adapt] は、分単位の値で指定した間隔で繰り返します。指定した間隔 (分単位) で不正検出がオンになり、スキャンが実行され、不正検出がオフになり、ステーションがただちに推奨チャンネルへと移動します。

3. オプションで、[Evaluation Time] を 120 秒から 5 ~ 300 秒の範囲の値に変更します。Evaluation は不正スキャンに影響し ([Evaluation Time] の秒でオンになります)、オプションでチャンネルを変更します。
4. オプションで、[Threshold] を 25 から 1 ~ 100 の範囲の不正の数に変更します。[Threshold] は、チャンネルの変更のトリガとなる、現在のチャンネルと推奨チャンネルの間の適合値の差分を表します。ゼロ以外のしきい値は、Periodic Adapt (定期適応) に適用されます。
5. オプションで、[Adaption Interval] を 30 からゼロまたは 5 ~ 10080 秒の範囲の値に変更します。(値 1 ~ 4 秒はサポートされていません。)[Adaption Interval] は、このコントローラでチャンネルを自動変更できる頻度を決定します。
6. [Start Wizard] をクリックします。
7. [OK] を 2 回クリックして確認します。

[Graph Help] をクリックすると、グラフの色の意味が表示されます。図中の [Details] をクリックすると、図の緑の棒グラフに対応する数値が表示されます。不正スキャン パラメータのま

とめが、画面の下部に表示されます。また、いずれかの定期適応が実行中の場合は、定期適応の間隔が表示されます。このビューは、毎秒、自動更新されます。



不正検出がネットワークで有効になっていない場合は、評価モードが必要になった段階で PSM がオンにし、その後にオフに戻します。たとえば、[One Time Adapt] オプションを使用すると、PSM が不正検出をオンにし、スキャンを実行し、ステーションを推奨チャンネルにただちに移動します。これによって実行中の設定が上書きされ、AP がリブートします（保存して永続的に有効にします）。

チャンネルのブラックリスト化はどのような状況でも推奨されません。RS4000 とメッシュ無線はサポートされていません。フォーティネット以外の機器の数がチャンネルで多くなると、そのチャンネルを使用する機器の数の推奨値が少なくなります。マルチチャンネル設定でこの機能を使用しないでください。

CLI を使用した Proactive Dashboard Manager の設定

Proactive Dashboard Manager の CLI コマンドは、proactive-spectrum-manager evaluate です。たとえば、次のように使用します。

```
mg-mc2# proactive-spectrum-manager evaluate
** Attention: Stations may be disconnected in this evaluation **
Are you absolutely sure [yes/No]? yes
Evaluation time [120s]? 10
View or Adapt [View/adapt]? adapt
Adaptation period [0] min (5-10080)? 0
```

デバイスのフィンガープリンティング

デバイスのフィンガープリンティングにより、ネットワークに接続しているデバイスについてのさまざまな属性を収集できます。収集された属性によって、クライアント OS、デバイスタイプ、使用されているブラウザなど、個別デバイスの全部または一部を特定できます。

デバイスのフィンガープリンティングは、ステーションに関する多くの情報を提供し、システム管理者が使用中のデバイスのタイプを把握し、必要な措置を取ることができるようにします。デバイスの詳細は、[Monitor] > [Dashboard] で確認できます。フィンガープリントのコマンドを使用して、デバイスの追加、削除、リストアを行えます。また、show fingerprints コマンドでシステムに保存されているデバイス フィンガープリントを表示できます。CLI コマンドの詳細については、『コマンド リファレンス ガイド』を参照してください。

Web UI を使用した構成

[Configuration] > [Devices] > [Device Fingerprint]

このページにはデフォルトで、監視可能な構成済みデバイス OS タイプのリストが表示されます。

Device Fingerprint ⓘ

Fingerprints

<input type="checkbox"/>	Device Name (Option 55/60 Description)	Hexadecimal characters
🔍		
<input type="checkbox"/>	Apple Mac OS X 10.6-	370103060f775ffc2c2e2f
<input type="checkbox"/>	Apple Mac OS X 10.7+	370103060f775ffc2c2e
<input type="checkbox"/>	Apple iOS	370103060f77fc
<input type="checkbox"/>	Apple iOS 9.x	37017903060f77fc
<input type="checkbox"/>	Ascom 2.x Phone	370103060f2c2e2f4243
<input type="checkbox"/>	Ascom 4.x Phone	370103060f2a07642c2e
<input type="checkbox"/>	Ascom 5.x Phone	370103060f2a07642c2e2b
<input type="checkbox"/>	Ascom i62 Phone	370103060f2a07582c2e
<input type="checkbox"/>	Ascom-Myco-phone	37012103060f1c2b333a3b
<input type="checkbox"/>	Blackberry OS	370103060f
<input type="checkbox"/>	Chrome OS	3701792103060c0f1a1c33363a3b77fc
<input type="checkbox"/>	Cisco VoIP Phone	370103060c0f1c2a429596
<input type="checkbox"/>	Debian/Linux 2.6 generic	37011c02030f0677

REFRESH
ADD
EDIT
RESTORE
IMPORT
EXPORT
DELETE

新規のデバイス OS の追加

新規デバイス OS タイプを追加するには、[ADD] ボタンをクリックして、デバイス名と関連する 16 進数文字の特性を入力してから、[SAVE] をクリックします。このデバイスがリストに追加されます。

Add Fingerprint ⓘ

Device Name (Option 55/60 Description) *

Hexadecimal characters (Signature) *

SAVE
CANCEL

既存のデバイス OS の変更

既存のエントリを変更するには、そのエントリのチェックボックスをオンにし、[EDIT] ボタンをクリックします。ポップアップ ボックスで必要な変更を加えて [SAVE] ボタンをクリックします。

Edit Fingerprint ⓘ

Device Name (Option 55/60 Description) *

Hexadecimal characters (Signature) *

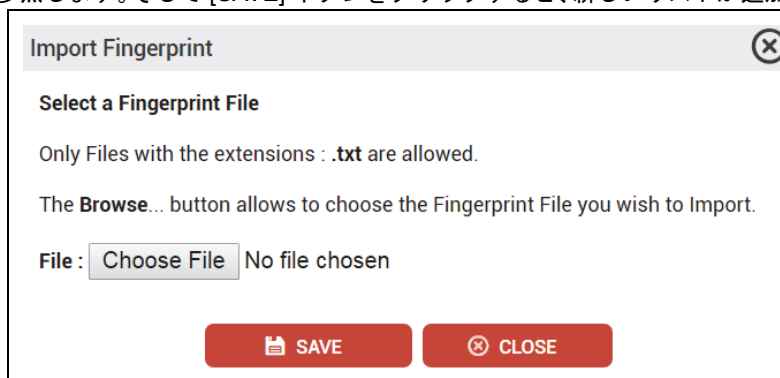
SAVE
CANCEL

デバイス OS の詳細をエクスポート

デバイスの既存リストを別のコントローラにエクスポートするには、列のヘッダでチェックボックスをオンにし、すべてのエントリを選択します。[EXPORT] ボタンをクリックすると、エントリのテキストファイルが作成されます。

新規デバイス OS の詳細をインポート

新しいエントリをインポートするには、[IMPORT] ボタンをクリックし、テキスト ファイルの場所を参照します。そして [SAVE] ボタンをクリックすると、新しいリストが追加されます。



CLI を使用した構成

CLI コマンドのフィンガープリントには以下のオプションがあります。

```
default(15)(config)# fingerprint ?
```

add	(10) Adds description and hexadecimal characters.
delete	(10) Deletes description and hexadecimal characters.
export	(10) Adds description and hexadecimal characters.
import	(10) Adds description and hexadecimal characters.
restore	(10) Restores configuration file.

- add - 新しいデバイスの OS タイプを追加する。
- delete - 既存デバイスの OS タイプを削除する。
- import - デバイスの OS タイプをインポートするファイル名を指定する。ファイルは通常、/opt/meru/images フォルダにある。
- export - デバイスの OS タイプの現在のリストをエクスポートする。エクスポートしたファイルは、txt ファイルとして、/opt/meru/images ディレクトリに保存されます。

6 ESS の設定

基本サービス セット (BSS) とは、IEEE 802.11 ワイヤレス LAN の基本ビルディング ブロックで、1つのアクセス ポイントと関連するすべてのクライアントをまとめて、BSS と呼びます。AP は、範囲内のクライアントが取得した名前 (SSID) をブロードキャストすることで、クライアントを取得します。クライアントがこれに応答することで、接続が確立されます。拡張サービス セット (ESS) の一部である同じネットワークへのアクセスが可能であれば、複数のアクセス ポイントが同じ SSID を共有できます。次のような異なる状況で、異なる種類の ESS を確立できます。

- 1つの ESSID に対して複数のアクセス ポイントをサポートする VLAN。
- 1つの物理アクセス ポイントに複数の異なる ESS。
- ESS ごとにネットワーク トラフィックが異なる ESS。VLAN を複数の ESS 間で共有するように指定することもできます。
- 特定の個人だけをサポートする ESSID。
- 支社などのリモート AP に使用する ESS。その AP がそれ以外にローカル トラフィックの ESS をサポートすることもできます。

ワイヤレス LAN システムでは、ESS ごとにビーコンをカスタマイズできるため、基本転送速度またはサポートされる転送速度、異なる BSS、異なるビーコン間隔、異なる DTIM 間隔などの、アクセス ポイントの異なる設定をサポートできます。このビーコンのカスタマイズによって、ESS ごとにサービスをカスタマイズでき、異なるクライアントやサービスも柔軟にサポートできます。

コントローラの ESS プロファイルは、E(z)RF Network Manager から設定できます。読み取り専用フィールド [Owner] をチェックすることで、ESS が設定された場所を確認できます。[Owner] は、[nms-server] または [controller] のいずれかです。AP1000 は、仮想セルを使用する ESS と仮想セルを使用しない別の ESS を同時にサポートできます。

Web UI による ESS の追加

ESS プロファイルは、E(z)RF Network Manager またはコントローラから設定できます。読み取り専用フィールドの Owner が nms-server または controller のどちらであるかによって、ESS プロファイルがどちらで設定されたのかを確認できます。AP400 は、仮想セル ESS ま

たは非仮想セル ESS のどちらかを使用するように設計されていますが、両方を同時に使用することはできません。AP1000 では、仮想セル ESS と非仮想セル ESS を同時に使用できません。コントローラの Web UI から ESS を追加するには、次の手順を実行します。

1. [Configuration] > [Wireless] > [ESS] > [Add] をクリックします。

[ESS Profile Add] 画面が表示されます。下図を参照してください。

図 33: ESS プロファイルの追加

ESS Profile - Add ?

ESS Profile *	<input type="text"/>	Enter 1-32 chars.
Enable/Disable	<input type="button" value="Enable"/>	
SSID *	<input type="text"/>	Enter 0-32 chars.
Security Profile	<input type="text" value="default"/>	
Essid Type	<input type="text" value="Regular"/>	
Backup ESS Profile	<input type="text" value="No Backup ESS"/>	
Timer Profile	<input type="text" value="No TIMER"/>	
Primary RADIUS Accounting Server	<input type="text" value="No RADIUS"/>	
Secondary RADIUS Accounting Server	<input type="text" value="No RADIUS"/>	
Accounting Interim Interval (seconds)	<input type="text" value="3600"/>	Valid range: [600-36000]
Reconnect Primary Server (minutes)	<input type="text" value="10"/>	Valid range: [5-60]
Bridging	<input type="checkbox"/> IPV6	
New AP's Join ESS	<input type="button" value="On"/>	
Tunnel Interface Type	<input type="text" value="No Tunnel"/>	
VLAN Name	<input type="text" value="No VLAN"/>	
VLAN Pool Name	<input type="text" value="No VLAN-POOL"/>	

2. [ESS Profile Name] フィールドに、拡張サービス セットの名前 (ID) を入力します。名前には最大で 32 文字の英数字を指定でき、スペースは使用できません。
3. [Enable/Disable] リストで、次のいずれかを選択します。
 - [Enable] : 作成された ESS プロファイルが有効になります。
 - [disable] : 作成された ESS プロファイルが無効になります。
4. [SSID] フィールドには、この ESS の SSID の 32 文字以下の名前を入力します。(仮想セル オーバーフローまたは非仮想セル ESS のいずれかを作成する場合、同じ ESSID の 2 つの ESS プロファイルを作成することになります。詳細については、[163 ページの「Web UI による仮想セル オーバーフローの設定」](#)を参照してください。)
5. [Security Profile Name] リストで、ESS プロファイルに関連付ける既存のセキュリティ プロファイルを選択します。デフォルトでは、ESS プロファイルに default という名前のセキュリティ プロファイルが関連付けられます。詳細については、[151 ページの「ESS の](#)

[セキュリティ プロファイル](#)」を参照してください。

6. [Primary RADIUS Accounting Server] リストで、事前に設定された RADIUS アカウンティング サーバ プロファイルの名前か [No RADIUS] オプションを選択します。[No RADIUS] オプションを選択すると、この ESSID プロファイルに接続するクライアントに RADIUS アカウント メッセージは送信されません。詳細については、認証の章の「[クライアントの RADIUS アカウンティング](#)」を参照してください。
7. [Secondary RADIUS Accounting Server] リストで、事前に設定された RADIUS アカウンティング サーバ プロファイルの名前か [No RADIUS] オプションを選択します。[No RADIUS] オプションを選択すると、この ESSID プロファイルに接続するクライアントに RADIUS アカウント メッセージが送信されません。詳細については、セキュリティの章の「[クライアントの RADIUS アカウンティング](#)」を参照してください。
8. [Accounting Interim Interval] フィールドに、RADIUS 認証のアカウントリング情報更新の間隔を秒単位で入力します。RADIUS アカウンティング サーバが有効な場合、コントローラは指定した間隔で一時的なアカウントリング レコードを RADIUS サーバに送信します。アカウントリング レコードは 802.1x を使用して認証を行うクライアントの RADIUS サーバにのみ送信されます。間隔は 600 ～ 36,000 秒 (10 分～ 10 時間) です。デフォルト値は、3,600 秒 (1 時間) です。詳細については、セキュリティの章の「[クライアントの RADIUS アカウンティング](#)」を参照してください。
9. [Beacon Interval] に、ビーコンが送信される間隔を設定します。ビーコン間隔に高い値を設定すると、アクセス ポイントがユニキャストとブロードキャストを送信する頻度が少なくなります。アクセス ポイントに接続されているクライアントの省電力機能が有効になっていると、ユニキャストとブロードキャストが送られる回数が少なくなることによってクライアントが省電力モードから " 復帰する " 回数が減り、クライアントのバッテリー寿命が長くなります。[Beacon Interval] フィールドに、ビーコンが送信される間隔 (ミリ秒) を入力します。ビーコン間隔は、20 ～ 1000 ミリ秒で指定します。AP400 および AP1000 の場合、ビーコン間隔は 20 の倍数 (20 ～ 1000 ミリ秒) です。WLAN のほとんどが Wi-Fi 電話で構成されていて、かつ、設定されている ESSID の数が少ない (たとえば、1 ～ 2 個) 場合は、ビーコン間隔を 100 に設定することを推奨します。
10. [SSID Broadcast] リストで、次のいずれかを選択します。
 - [On] : SSID が送信ビーコンに含まれます。
 - [Off] : SSID が送信ビーコンに含まれません。また、SSID が指定されないプローブ要求に対してプローブ応答が送信されません。
11. [Bridging] エリアで、次のいずれかのブリッジ オプションを選択します。
 - [AirFortress] : FortressTech レイヤ 2 のブリッジと Fortress Technology AirFortress ゲートウェイを使用した暗号化です。
 - [IPv6] : インターネットバージョン 6 アドレスのブリッジを設定します。トンネルモードによる IPv6 には、次のような制限があります。
 - 動的 VLAN なし

- 複数の ESSID の同じ VLAN へのマッピングなし
 - IPv6 フィルタリングのサポートなし
 - IPv6 IGMP スヌーピングなし
12. デフォルトでは、この ESS プロファイルに参加するアクセス ポイントは、仮想セルの同じチャンネルになります。[New APs Join ESS] プロファイル リストで、次のいずれかを選択します。
- [On] : (デフォルト) アクセス ポイントが自動的に ESS プロファイルに加わり、そのパラメータを使用して設定されるように指定します。
 - [Off] : アクセス ポイントが自動的に ESS プロファイルに加わらないようにします。これで、[ESS Profile] 画面にユーザが複数のインターフェイスを追加できるようになりました。以下の手順で、複数のインターフェイスを追加します。
 - [ESS Profile - Update] 画面で、[New APs Join ESS] プロファイルに [Off] を選択します。このオプションによって、AP が ESS プロファイルに自動的に参加しなくなります。
 - ESS プロファイルのチェックボックスをオンにし、[Settings] ボタンをクリックします。
 - [ESS Profile - Update] 画面が表示されます。
 - [ESS Profile - Update] 画面で、[ESS-AP Table] タブを選択します。
 - [ESS-AP Configuration] 画面が表示されます。[ESS-AP Configuration] 画面には、何も情報は表示されません。
 - [ESS-AP Configuration] 画面で、[Add] ボタンをクリックします。
 - [ESS-AP Configuration - Add] 画面が表示されます。これで、[ESS Profile] 画面にユーザが複数のインターフェイスを追加できるようになりました。
 - [OK] をクリックします。
 - これで、選択したインターフェイスが [ESS-AP Configuration] 画面に表示されます。
13. [Tunnel Interface Type] で、次のいずれかを選択します。
- [No Tunnel] : この ESS プロファイルにはトンネルが関連付けられません。
 - [Configured VLAN Only] : 次の [VLAN Name] リストに表示される設定済みの VLAN のみがこの ESS プロファイルに関連付けられます。このオプションを選択した場合は、手順 13 に進みます。
 - [RADIUS VLAN Only] : Radius 属性 [Tunnel Id] で、Radius によって VLAN が割り当てられます。802.1x/WPA/WPA2 または MAC フィルタリングでクライアントを認証する場合は、[Radius VLAN Only] を使用します。
 - [RADIUS and Configured VLAN] : 設定済み VLAN と Radius VLAN の両方がこの ESS プロファイルに関連付けられます。このオプションを選択した場合は、手順 15 に進みます。

- [GRE] : GRE トンネル設定を指定します。このオプションを選択した場合は、手順 14 に進みます。詳細については、セキュリティの章の「[GRE トンネルの設定](#)」を参照してください。
14. 手順 12 で [Configured VLAN Only] を選択した場合は、この ESS プロファイルに関連付ける VLAN をリストから選択します。
 15. [Tunnel Interface Type] に [GRE] を選択した場合は、[Configuration] > [Wired] > [GRE] エリアで前に設定した GRE トンネル プロファイルの名前を選択します。GRE が動作するには、DHCP リレーがローカルまたはグローバルで有効になっている必要があります。
 16. [Allow Multicast Flag] リストで、オプションでマルチキャストを有効 ([on]) にします。マルチキャストアプリケーションを使用する必要がある場合のみ、マルチキャストを有効にしてください。マルチキャストを有効にすると、無線側のすべてのマルチキャスト パケットが有線側に表示され、有線側のすべてのマルチキャスト パケットが無線側に表示されます。本章の **167 ページ**の「[マルチキャスト](#)」も参照してください。
 - [On] : マルチキャストを有効にします。マルチキャストアプリケーションを使用する必要がある場合のみ、マルチキャストを有効にしてください。マルチキャストを有効にすると、無線側のすべてのマルチキャスト パケットが有線側に表示され、有線側のすべてのマルチキャスト パケットが無線側に表示されます。
 - [Off] : マルチキャストを無効にします。
 17. ワイヤレスを分離して、同じ L2 ドメインで動作する 2 つのワイヤレス ステーションがワイヤレス トラフィックを使用して相互に直接通信しないようにします。これは、一般的な要件ではありませんが、一部のセキュリティ ポリシーで必要になる場合があります。ネットワークでこのような要件がある場合は、このオプションを [On] に設定します。



この機能は、ブリッジ プロファイルでのみ動作し、1 つの AP が使用する ESS プロファイルでのみ動作します。

18. [Multicast-to-Unicast Conversion] で、次のいずれかを選択します。
 - [On] : マルチキャスト / ユニキャスト間コンバージョンを有効にします。このコンバージョンによって、マルチキャスト パケットをユニキャスト パケットにコンバージョンし、すべてのクライアントにそれを配信できるようになります。
 - [Off] : マルチキャスト / ユニキャスト間コンバージョンを無効にします。マルチキャスト パケットはマルチキャスト パケットとしてクライアントに配信されます。
19. [ESS Configuration] ページの [RF Virtualization Mode] ドロップダウンでは、指定した ESS プロファイルが使用する仮想化の種類を指定できます。以下のオプションを選択します。
 - [Virtual Cell] : これは、AP400 以外のすべての AP モデルのデフォルト設定です。
 - [Virtual Port] : これは、AP400 モデルのデフォルト設定です。

- [Native Cell]: このオプションは、ESS で仮想化を無効にします。



仮想セル内の同じチャネルのすべての AP は、次の値が同じ設定である必要があります。

rf-mode
channel width
n-only-mode
channel と MIMO mode

20. AP が AP400 モデルである場合は、[Overflow for:] 設定に [Virtual ESS] を選択することで、この ESS を "オーバーフロー" ESS にできます。これは、指定された仮想セル ESS (前に作成されたもの) が上限に達すると、この非仮想セル ESS にオーバーフローすることを意味します。2 つの ESS プロファイルが 1 つの SSID を共有することで、必要に応じてクライアントをシームレスに相互に移動できるようにすることで、これが可能になります。詳細については、**162 ページの「仮想セル オーバーフロー機能」**を参照してください。
21. リリース 5.1 では、ESSID の WMM 設定に効果はありません。ただし、AP で APSD 機能を有効または無効にするには、WMM パラメータを [on] に設定する必要があります。詳細については、**161 ページの「サポートされる WMM 機能」**を参照してください。
22. APSD のサポートで、[on] または [off] を選択します。APSD は Advanced WMM Power Save という意味であり、AP400/AP1000 でサポートされています。詳細については、**161 ページの「サポートされる WMM 機能」**を参照してください。
[On]: 省電力モード クライアントのデータ パケットは、クライアントから渡されるトリガに基いてバッファされ、配信されます。この機能によって、省電力が推進され、従来の省電力モード (TIM 方式) よりもバッテリーの寿命が長くなります。これを動作させるには、WMM を [on] に設定する必要があります。前の手順を参照してください。
[Off]: APSD サポートなし。
23. DTIM は、省電力モードのクライアントに影響します。[DTIM Period] フィールドに、バッファに保存されたブロードキャスト フレームが送信されるまでのビーコン間隔の回数を入力します。この値は、ビーコン フレームの [DTIM Period] フィールドに送信されます。[DTIM Period] フィールドには 1 ~ 255 までの値を使用できます。デフォルトの DTIM 間隔は 1 です。DTIM 間隔に高い値を設定すると、アクセス ポイントによって送信されるブロードキャストの頻度が少なくなります。アクセス ポイントに接続されているクライアントで省電力が有効になっていると、ブロードキャストの送信数が少なければ、クライアントが省電力モードから "復帰する" 回数も少なくなり、クライアントのバッテリー寿命が長くなります。
現状で省電力モードになっているクライアントの動作のみが DTIM 間隔の値の影響を受けます。ブロードキャストは一般的に無線リソースを無駄に使用するため、Forti WLAN では、プロキシ サービス、またはユニキャストを少なくして効率化する方法のいずれかを使用してブロードキャストを緩和するメカニズムを採用しました。たとえば、有線側が受信する ARP レイヤ 2 ブロードキャストは、ワイヤレス クライアントにリレーされません。代わりに、FortiWLC が、すべてのワイヤレス クライアントに対する IP-MAC アド

レス マッピングのリストを管理し、クライアントに代わって、プロキシ ARP を使用して応答します。

24. [Dataplane Mode] リストで、AP/ コントローラ設定のタイプを選択します。

- [Tunneled] : (デフォルト) トンネル モードでは、コントローラと AP1000 がデータ トンネルで接続されるため、モバイル ステーションからのデータ パケットと制御パケットが AP からコントローラの間でトンネルされます。
- [Bridged] : ([Bridge] モードは、以前の [Remote AP] モードです。) ブリッジ モードでは、AP とコントローラの間でデータ パケットは渡されず、制御プレーン パケットのみが渡されます。ブリッジ モードに設定されていると、たとえば、サテライト オフィスなどのコントローラから離れた場所で、WAN や ISP が AP を導入し、管理できます。コントローラは、キープアライブ シグナルによってリモート AP を監視します。リモート AP は、認証やアカウントリングなどの情報をコントローラを介して交換できますが、データの交換はできません。ただし、リモート AP は、サブネット内の他の AP とはデータを交換できます。ブリッジ モードの ESSID は、コントローラを使用してデータプレーン トラフィック (DHCP を含む) を交換できないため、ブリッジ構成では FortiWLC のレート制限と QoS (および QoS 関連のすべての機能) の機能を使用できません。詳細については、本章の **164 ページの「ブリッジとトンネル」**を参照してください。

VLAN タグをブリッジ モード プロファイルに設定し (下記の手順 29 を参照)、その後、複数のプロファイルをその VLAN タグに関連付けることができます。下記の手順 26 で、AP VLAN 優先度を設定できます。

25. AP VLAN タグに 0 ~ 4094 を指定します。この VLAN タグ値はコントローラの VLAN プロファイルで設定され、802.1q VLAN を使用して ESSID のクライアント トラフィックをデータプレーン モードにタグ付けするために使用されます。このフィールドで、AP が到着する VLAN 802.1p データ パケットを WMM AC にマッピングする必要があるかどうかを指示します。ブリッジ ESS においては、デフォルトでこのフィールドが無効になり、AP は常に IPV4 パケットの DSCP フィールドによる到着パケットからいずれかの WMM AC へのマッピングを尊重します。この設定をオンにすると、AP は、パケットがいずれかの WMM AC にマッピングされている場合に、DSCP 優先度よりも VLAN 802.1p 優先度を尊重します。

26. VLAN 優先度を有効にするには、このフィールドを [On] に設定します。

- [On] : AP は、パケットの IP ヘッダにある DSCP 値を無視します。
- [Off] : AP は、パケットの IP ヘッダにある DSCP 値を尊重します。AP は、IP ヘッダの DSCP 値を適切な WMM キューに変換します。この機能は、ダウンストリーム パケットと、データプレーン モードが [Bridged] に設定されている ESSID に対してのみ作用します。

27. [Countermeasure] では、MIC 対策を有効または無効にする時期を選択します。

- [On] : (デフォルト) MIC 対策は、AP が 60 秒以内に同じクライアントで MIC エラーを 2 つ連続して検出した場合に役立ちます。AP は、エラーの原因となった ESSID から

すべてのクライアントの関連付けを解除し、どのクライアントも 60 秒間は接続できないようにします。これによって MIC 攻撃を回避します。

- [Off] : ネットワーク管理者が MIC エラーの原因を特定して解決する間のみ、MIC 対策を一時的にオフにしてください。

28. [Enable Multicast MAC Transparency] フィールドで、[on] または [off] を指定します。詳細については、本章の **169 ページ** の「[マルチキャスト MAC 透過機能](#)」を参照してください。

- [On] : すべてのダウンストリーム マルチキャスト パケットに、ストリーミングステーションの MAC アドレスが含まれます。
- [Off] : (デフォルト) すべてのダウンストリーム マルチキャスト パケットに、コントローラの MAC アドレスが含まれます。

29. バンド ステアリングは、機能によってクライアントにバンドを割り当てることで、AP1000 のマルチ バンド対応クライアントを調整します。ABGN トラフィックにバンドステアリングを使用するには、5GHz バンドへの A 機能があるデュアル モードクライアントに A ステアリングを使用するよう指示し、5GHz バンドへの AN 機能があるすべてのデュアル モードクライアントに N ステアリングを使用するよう指示します。バンドステアリングは、マルチキャスト トラフィックの振り分けにも便利です。追加されるクライアントにこのコマンドが動作するようにするには、[New APs Join ESS] フィールドも [on] に設定します。詳細については、本章の **170 ページ** の「[バンドステアリング機能](#)」を参照してください。以下のバンドステアリング モード オプションを指定できます。

- [Band Steering Disabled]
- [Band Steering to A band] : この ESS への接続時に、インフラストラクチャは、すべての A 対応ワイヤレス クライアントを 5GHz バンドにステアリングしようとします。
- [Band Steering to N band] : この ESS への接続時に、インフラストラクチャは、すべての A 対応でもある N 対応ワイヤレス クライアントを 5GHz バンドにステアリングしようとします。また、N 非対応ワイヤレス クライアントを 2.4GHz バンドにステアリングしようとします。

30. [Band Steering Timeout] は、関連付けられていない、禁止されているバンドへのステアリング対象クライアントの割り当てをブロックする秒数を設定します。このコマンドを動作させるには、Band Steering フィールドも A バンド または N バンドに設定します (上記参照)。[Band Steering Timeout] には、1 ~ 65535 の任意の整数を指定できます。

31. [Expedited Forward Override] オプションは、システムのデフォルト DSCP-WMM 優先度マッピングを上書きします。DSCP Expedited Forwarding (46) とマークされた IP ダイアグラムは、ダウンストリームの音声キュー (AC_VI) ではなく、AP の WMM 音声キュー (AC_VO) から (ステーションに) 送信されます。ESS プロファイルごとに設定でき、ブリッジとトンネルの両方の ESS プロファイルで動作します。設定については、本章の **174 ページ** の「[完全優先転送の上書き](#)」を参照してください。

32.[SSID Broadcast Preference] は、CISCO フォンの接続の問題を解決するためのもので、次の 3 つのオプションで構成されます。

- [disable] : このパラメータを "disable" に設定すると、AP はビーコンの SSID 文字列をアドバタイズしません。
- [always] : このパラメータを "always" に設定すると、AP によるビーコンの SSID のアドバタイズが常に有効になります。推奨された場合を除き、この設定にしないでください。
- [till-association] : これがデフォルトのオプションです。このパラメータを "till-association" に設定すると、クライアントのアソシエーション段階まではビーコンの SSID のアドバタイズが有効になり、接続のそれ以降の部分では SSID ブロードキャストが無効になります。このパラメータは、Vport ON で接続の問題を解決する、一部のバージョンの電話での設定よりも優先されます。ステーションのアソシエーションの後に、AP は SSID 文字列のブロードキャストを停止します。これで、AP CLI に加えて、ESS ごとのコントローラの GUI から、Vport パラメータの SSID ブロードキャストをユーザが設定できるようになりました。設定については、本章の **176 ページの「Vport の SSID ブロードキャスト」** を参照してください。デフォルトでは、このオプションが選択されています。

33.B、A、G、および BG の各モードのこれ以外のサポート速度と基本転送速度について、必要に応じて、有効または無効にします。

34.[OK] をクリックします。



Ascom i75 フォンを使用して VCell が有効な WPA2PSK プロファイルに接続されている場合は、BGN がサポートするすべての HT 転送速度のチェックボックスをオフにして ("なし" に設定して)、ESSID を作成します。

AP の仮想セルが実際にオンになるタイミング

AP400 を除くすべての AP は常に、仮想セルまたはネイティブセルを使用できる状態になっており、無線レベルでの設定は必要ありません。いずれかを有効にするには、各 ESS プロファイルの RF Virtualization モードを [Virtual Cell] または [Native Cell] に設定します。

AP400 では、RF Virtualization モードが無線インターフェイスでデフォルトで [Virtual Port] に設定されており、必要があれば変更できます。この設定は、ESS レベルの RF Virtualization モードの設定よりも優先されます。AP400 で動作するようにするには、無線と使用中の ESS の両方で、RF Virtualization モードが [Virtual Port] に設定されている必要があります。

下表に、AP400 仮想ポートで設定可能な 3 つの構成を記載します。

	無線設定	ESS 設定	ESSID
AP400	on	on	仮想化
	off	off	非仮想化
	off	on	非仮想化

CLI による ESS の追加

CLI による ESSID の割り当て

ESSID は、クライアントが WLAN への接続に使用する ESS 名です。ESSID は 32 文字以内の英数字で指定し、スペースや特殊文字は使用できません。

以下の例では、ESSID に **corp-users** という名前を付け、ESSID 設定モードに入ります。

```
controller# configure terminal
controller(config)# essid corp-users
controller(config-essid)#
```

有効化と無効化

[Enable and Disable] フィールドは、プロファイルのサービスのすべてが [Enabled] (有効)、[Disabled] (無効)であることを表します。特定の ESS プロファイルが [Disabled] になっていると、NMS は、その ESS プロファイルに属しているすべてのサービスを削除します。特定の ESS プロファイルが [Enabled] になっていると、NMS は、その ESS プロファイルに属しているすべてのサービスを作成します。状態が [Disabled] になっている ESSID プロファイルには、クライアントは関連付けられません。



"サービス" とは、クライアント接続のことです。ESSID の状態が無効であれば、BSSID が AP から削除され、クライアントが無線でその無効になっている SSID を認識できなくなります。

CLI 設定

```
MERUCNTRL# sh essid
```

ESS Profile Name Interface Type	Enable/Disable	SSID	Security Profile	Broadcast	Tunnel
meru	enable	meru	default	on	none
meruwpa	enable	meruwpa	meruwpa	on	none
meruwpa2psk	enable	meruwpa2psk	meruwpa2psk	on	none

ESS Profile(3)

```
MERUCNTRL# configure terminal
MERUCNTRL(config)# essid meru
MERUCNTRL(config-essid)# disable
MERUCNTRL(config-essid)# end
MERUCNTRL# sh essid
```

ESS Profile Name Interface Type	Enable/Disable	SSID	Security Profile	Broadcast	Tunnel
meru	disable	meru	default	on	none
meruwpa	enable	meruwpa	meruwpa	on	none
meruwpa2psk	enable	meruwpa2psk	meruwpa2psk	on	none

ESS Profile(3)

```
MERUCNTRL# sh essid meru
ESS Profile
```

```
ESS Profile                                : meru
Enable/Disable                             : enable
SSID                                        : meru
Security Profile                           : default
Primary RADIUS Accounting Server           :
Secondary RADIUS Accounting Server         :
Accounting Interim Interval (seconds)     : 3600
Beacon Interval (msec)                    : 100
SSID Broadcast                             : on
Bridging                                   : none

New AP's Join ESS                          : on
Tunnel Interface Type                      : none
```

```

VLAN Name :
Virtual Interface Profile Name :
GRE Tunnel Profile Name :
Allow Multicast Flag : off
Isolate Wireless To Wireless traffic : off
Multicast-to-Unicast Conversion : on
RF Virtualization Mode : VirtualPort
Overflow from :
APSD Support : on
DTIM Period (number of beacons) : 1
Dataplane Mode : tunneled
AP VLAN Tag : 0
AP VLAN Priority : off
Countermeasure : on
Multicast MAC Transparency : off
Band Steering Mode : disable
Band Steering Timeout(seconds) : 5
Expedited Forward Override : off
SSID Broadcast Preference : till-association
B Supported Transmit Rates (Mbps) : 1,2,5.5,11
B Base Transmit Rates (Mbps) : 11
A Supported Transmit Rates (Mbps) : 6,9,12,18,24,36,48,54
A Base Transmit Rates (Mbps) : 6,12,24
G Supported Transmit Rates (Mbps) : 6,9,12,18,24,36,48,54
G Base Transmit Rates (Mbps) : 6,9,12,18,24,36,48,54
BG Supported Transmit Rates (Mbps) :
1,2,5.5,11,6,9,12,18,24,36,48,54
BG Base Transmit Rates (Mbps) : 11
BGN Supported Transmit Rates (Mbps) :
1,2,5.5,11,6,9,12,18,24,36,48,54
BGN Base Transmit Rates (Mbps) : 11
BGN Supported HT Transmit Rates (MCS) :
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
BGN Base HT Transmit Rates (MCS) : none
AN Supported Transmit Rates (Mbps) : 6,9,12,18,24,36,48,54
AN Base Transmit Rates (Mbps) : 6,12,24
AN Supported HT Transmit Rates (MCS) :
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
AN Base HT Transmit Rates (MCS) : none
Owner : controller
1 Stream VHT Base MCS Set (MCS) : mcs0-9
2 Streams VHT Base MCS Set (MCS) : mcs0-9
3 Streams VHT Base MCS Set (MCS) : mcs0-9
1 Stream VHT Supported MCS Set (MCS) : mcs0-9
2 Streams VHT Supported MCS Set (MCS) : mcs0-9

```

```
3 Streams VHT Supported MCS Set (MCS)      : mcs0-9
MERUCNTRL#
```

ESS のセキュリティ プロファイル

ESS プロファイルとセキュリティ プロファイルは、E(z)RF Network Manager またはコントローラから設定できます。読み取り専用フィールドである Owner が nms-server または controller のどちらであるかによって、プロファイルがどちらで設定されたのかを確認できます。各 ESS にセキュリティ プロファイルを関連付ける必要があります。追加のセキュリティ プロファイルを作成しないと、ESS は、**default** という名前のデフォルトのセキュリティ プロファイルに自動的に関連付けられます。追加のセキュリティ プロファイルを使用するには、グローバル設定モードで、security-profile コマンドを使用して作成します（詳細については、本章の 139 ページの「[Web UI による ESS の追加](#)」、または第 9 章「[セキュリティの設定](#)」を参照してください）。ESS を作成する前に、セキュリティ プロファイルを作成します。E(z)RF Network Manager で作成したプロファイルをコントローラから変更することはできません。

以下の例では、corp-access という名前のセキュリティ プロファイルを関連付けます。

```
controller(config-ssid)# security-profile corp-access
controller(config-ssid)#
```

CLI による ESSID AP の CAC の設定

CAC (Call Admission Control) が実装されていると、qosvars calls-per-bssid コマンド (398 ページの「[CLI による QoS ルールの設定](#)」を参照) を使用することで、すべての BSSID に対する VoIP 通話の数が制限されます。ある ESSID の AP400 に対して特別な要件がある場合には、ssid/ess-ap 設定サブレベルから calls-per-bss コマンドを使用し、その AP に対して CAC の最大通話数の制限を設定できます。たとえば、ESSID のインターフェイス 1 で AP 1 に対する最大通話数を 10 に設定するには、以下のコマンドを使用します。

```
controller(config-ssid)# ess-ap 1 1
controller(config-ssid-essap)# calls-per-bss 10
controller(config-ssid-essap)# exit
```

CLI によるビーコン パラメータの設定

以下のビーコン パラメータを設定できます。

- ビーコン DTIM 間隔：DTIM は、省電力モードのクライアントに影響します。[DTIM Period] フィールドには、バッファに格納されたブロードキャスト フレームが送信されるまでのビーコン間隔数を入力します。この値は、ビーコン フレームの [DTIM Period] フィールドに送信されます。

[DTIM Period] フィールドには 1 ～ 255 までの値を使用できます。デフォルトの DTIM 間

隔は 1 です。DTIM 間隔に高い値を設定すると、アクセス ポイントによって送信されるブロードキャストの頻度が少なくなります。アクセス ポイントに接続されているクライアントで省電力が有効になっていると、ブロードキャストの送信数が少なければ、クライアントが省電力モードから " 復帰する " 回数も少なくなり、クライアントのバッテリー寿命が長くなります。

現状で省電力モードになっているクライアントの動作のみが DTIM 間隔の値の影響を受けます。ブロードキャストは一般的に無線リソースを無駄に使用するため、Forti WLAN では、プロキシ サービス、またはユニキャストを少なくして効率化する方法のいずれかを使用してブロードキャストを緩和するメカニズムを採用しました。たとえば、有線側が受信する ARP レイヤ 2 ブロードキャストは、ワイヤレス クライアントにリレーされません。代わりに、FortiWLC が、すべてのワイヤレス クライアントに対する IP-MAC アドレス マッピングのリストを管理し、クライアントに代わって、プロキシ ARP を使用して応答します。

- ビーコン間隔：ビーコンが送信される頻度を設定します。

ビーコン間隔設定は、ユニキャストとブロードキャストに影響します。ビーコン間隔は、20 ~ 1000 ミリ秒で指定します。AP1000 の場合、ビーコン間隔は 20 の倍数 (20 ~ 1000 ミリ秒) です。ビーコン間隔に高い値を設定すると、アクセス ポイントがユニキャストとブロードキャストを送信する頻度が少なくなります。アクセス ポイントに接続されているクライアントの省電力機能が有効になっていると、ユニキャストとブロードキャストが送られる回数が少なくなることでクライアントが省電力モードから " 復帰する " 回数が減り、クライアントのバッテリー寿命が長くなります。ビーコン間隔設定は、ユニキャストとブロードキャストに影響します。

WLAN のほとんどが Wi-Fi 電話で構成されていて、かつ、設定されている ESSID の数が少ない (たとえば、1 ~ 2 個) 場合、フォーティネットではビーコン間隔を 100 に設定することを推奨しています。

次の例では、ビーコン DTIM 間隔を 10 に、ビーコン間隔を 240 TU に設定しています。

```
controller(config-ssid)# beacon dtim-period 10
controller(config-ssid)# beacon period 240
```

CLI による ESSID ブロードキャストの設定

デフォルトでは、ESSID がブロードキャストされます。ESSID がブロードキャストされると、アドバタイズされるビーコンに ESSID が追加されます。パッシブ スキャンを使用するクライアントは、アクセス ポイントによって転送されるビーコンを受信します。ESSID のブロードキャストが無効な場合、ビーコンを受信するクライアントは、ESSID 情報を受信できません。

アクティブスキャンを使用するクライアントは、プローブ要求を送信し、アクセス ポイントからプローブ応答を待機します。ESSID のブロードキャストが無効な場合、プローブ要求に ESSID が含まれていない限り、アクセス ポイントはプローブ要求に応答しません。

ESSID がブロードキャストされないようにするには、no publish-ssid コマンドを使用します。

以下の例は、ESSID がブロードキャストされないようにします。

```
controller(config-ssid)# no publish-ssid
```

CLI によるアクセス ポイントの ESSID 参加の設定

デフォルトでは、新しいアクセス ポイントが WLAN に接続されると、検出時にアクセス ポイントが自動的に参加するよう設定されているすべての ESSID に参加し、BSSID が作成されます。

WLAN の設定が完成したら、この自動的に参加する機能を無効にすることで、設定がアクセス ポイントによって変更されないようにできます。限られたアクセス ポイントだけにアドバタイズする新しい ESS を追加する場合は、参加を無効にして、ESS-AP マッピングを手動で追加するほうが簡単です。

以下の例では、アクセス ポイントが自動的に ESSID に参加しないようにします。

```
controller(config-ssid)# no ap-discovery join-ess
```

自動的に参加しないようにした後は、BSSID を手動で割り当てる必要があります。



このコマンドのこのステータスが評価されるのは、新しい ESS-AP マッピングが作成された時だけです。ESS-AP マッピングは、**ess-ap** コマンドによって手動で作成されるか、新しい ESS が作成されるか新しいアクセス ポイントが検出されたときに自動的に作成されます。

仮想化モードの設定

[ESS Configuration] ページの [RF Virtualization Mode] ドロップダウンでは、指定した ESS プロファイルが使用する仮想化の種類を指定できます。このオプションには、次の 3 つの選択肢があります。

- Virtual Cell : AP400 を除くすべての AP モデルのデフォルト設定です。
- Virtual Port : AP400 モデルのデフォルト設定です。
- Native Cell : このオプションは、ESS で仮想化を無効にします。

フォーティネットのアクセス ポイントでは、仮想化がデフォルトでオンになります。仮想化の主な利点は、アクセス ポイント間のシームレスなローミングによる、インフラストラクチャ

主導によるハンドオフです。仮想ポートは、各クライアントに固有の仮想アクセス ポイントを割り当てるという点で仮想セルよりも利点があります。仮想ポートによって、クライアント同士がアクセスを共有するのではなく、クライアントごとの固有のアクセスが可能になります。クライアントごとに固有の仮想ポートが存在するため、クライアントのニーズに合わせてカスタマイズできます。たとえば、従業員が使用するアプリケーションに応じて異なる帯域幅を割り当てることができます。クライアントには、帯域幅の制限はあるものの高品質のサービスを提供し、ゲストには、低優先度の限定されたアクセスを割り当てることができます。

コントローラあたりの仮想ポート数に対し、次の 3 つの制限があります。

- コントローラがサポートするクライアントの数による制限。
- AP 無線の数による制限。AP400 における仮想ポートの理論上の最高数は、無線あたり 128 です。フォーティネットのベスト プラクティスでは、無線あたり 64 以下にすることを推奨します。
- 仮想セルによる制限。仮想セルあたりの仮想ポートが 2007 というハードウェアの制限があります。この数は、1 つの BSSID あたりの関連付けが 2007 以下という標準によって設定されているものです。フォーティネットの環境では、それぞれの BSSID が仮想セルになります。

AP400 の場合、他の仮想ポート構成と比べて次のような違いがあります。

- ESS プロファイル構成に加えて、仮想ポートを AP400 無線インターフェイスで有効にする必要があります。正しく動作するようにするには、無線と使用中の ESS の両方で、RF Virtualization モードを [Virtual Port] に設定する必要があります。AP400 では、仮想ポートがデフォルトで有効になります。
- 仮想ポートが有効な ESS プロファイルで一部の AP を仮想ポート用に設定し、それ以外を非仮想ポート用に設定すると、仮想ポート用に設定した AP だけが仮想ポートが有効な ESS によって認識されます。
- AP400 は、ステーションごとの仮想セルのみをサポートします。

Web UI による AP400 の仮想セル サポートの設定

次の 2 つの手順で仮想ポートを設定します。

1. [RF Virtualization Mode] を [Virtual Port] に設定して、ESS を作成します。
2. 次の手順で、仮想ポートのそれぞれの無線を設定します。
 - [Configure] > [Wireless] > [Radio] をクリックします。
 - 無線を選択します。
 - [RF Virtualization Mode] を [Virtual Port] に設定します。

- 設定を保存します。



複数の無線の設定には [Bulk Update] を使用します。

CLI による AP400 の仮想セル サポートの設定

AP 無線では、デフォルトで仮想ポートが有効です。

CLI の show interfaces Dot11Radio コマンドを使用すると、仮想ポート設定を表示できます。
たとえば、次のように入力します。

```
vcell122# show interfaces Dot11Radio 398 1 *****  
Wireless Interface Configuration
```

AP ID	: 398
AP Name	: AP-398
Interface Index	: 1
AP Model	: AP400
Interface Description	: ieee80211-398-1
Administrative Status	: Up
Operational Status	: Disabled
Last Change Time	: 08/01/2013 09:38:35
Radio Type	: RF6
MTU (bytes)	: 2346
Primary Channel	: 6
Operating Channel	: 6
Short Preamble	: on
RF Band Support	: 802.11abgn
RF Band Selection	: 802.11bgn
Transmit Power High(dBm)	: 24
AP Mode	: Service

```

Scanning Channels                : 1,2,3,4,5,6,7,8,9,10,11,12,
13,14,36,40,
44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,15
3,157,161,165
    G Protection Mode            : auto
HT Protection Mode                : off
Number of Antennas                : 1
Channel Width                     : 20-mhz
Channel Center Frequency Index    : 42
MIMO Mode                        : 2x2
802.11n only mode                : off
RF Virtualization Mode           : VirtualPort
Probe Response Threshold          : 15
Mesh Service Admin Status        : disable
Uplink Type                      : Downlink
Transmit Beamforming Support      : off
STBC Support                     : off

```

B/

仮想ポートをオフにするには、次のコマンドを使用します。

```

vcell122# configure terminal
vcell122(config)# interfaces Dot11Radio 398 1
vcell122(config-if-802)# rf-virtual-mode ?
<mode> (10) Enter RF Virtualization Mode.
NativeCell Native Cell Mode
VirtualPort Virtual Port Mode
vcell122(config-if-802)# rf-virtual-mode NativeCell

```



RF 仮想化での同じチャネルの AP はすべて、次の値が同じ設定である必要があります。

```

rf-mode
channel width
n-only-mode
channel と MIMO mode

```

プローブ応答しきい値の設定

Probe Response Threshold (プローブ応答しきい値) は、転送デバイスからの距離に基いて、要求に応答する AP を決定する方法を設定します。近くにあるステーションから送信された要求に AP が迅速に応答できるように設計されています。AP の CLI に加えて、GUI での設定もサポートしています。この機能は、AP ごとのインターフェイス レベルでのバルク更新でも設定できます。AP のデフォルトのプローブ応答しきい値は、15 です。

SNRRange

GUI には 0 ～ 100 の範囲の SNR 値を指定し、プローブ応答しきい値ゼロは、無効を表します。

GUI ページ:

図 34: [Wireless Interface Configuration - Update]

Wireless Interface Configuration - Update ?

Wireless Interface

Wireless Statistics

Antenna Property

AP ID	1
IfIndex	2

Interface Description	<input type="text" value="ieee80211-1-2"/> Enter 0-256 chars.
Administrative Status	Down ▼
Primary Channel	36 ▼
Short Preamble	Off ▼
RF Band Selection	802.11ac ▼
Transmit Power(EIRP)	<input type="text" value="23"/>
AP Mode	Service Mode ▼
B/G Protection Mode	Auto ▼
HT Protection Mode	Off ▼
Channel Width	80 MHz ▼
MIMO Mode	3x3 ▼
802.11n only mode	Off ▼

CLI によるデータ転送速度の設定



各製品で使用されるデフォルト設定は以下のとおりです。

802.11b: Base (1、2、5.5、11)、Supported (1、2、5.5、11)

802.11bg: Base (1、2、5.5、11)、Supported (all)

802.11a: Base (all)、Supported (all)

データ転送速度とは、アクセス ポイントがデータの転送に使用するデータ速度です。次の 2 つのタイプのデータ速度があります。

- 基本データ転送速度

接続するすべてのクライアントがアクセス ポイントへの接続で必ずサポートしなければならない、必須の転送速度です。802.11AN/BGN では、データ速度は MCS インデックスを使用して選択します。実際のデータ速度は MCS インデックス、チャンネル幅、およびガード間隔に基づき計算されます。選択されたチャンネル幅が上述の 40MHz エクステンションである場合、クライアントのデータ速度は、関連のあるクライアント チャンネル幅およびガード間隔機能により異なります。有効な速度は以下のとおりです。

- 802.11b の有効な速度は 1、2、5.5、11 Mbps、または all (すべて)

- 802.11g の有効な速度は 6、9、12、18、24、36、48、54 Mbps、または all (すべて)
- 802.11bg の有効な速度は 1、2、5.5、11、6、9、12、18、24、36、48、54 Mbps、または all (すべて)
- 802.11bgn の有効な速度は 1、2、5.5、11、6、9、12、18、24、36、48、54 Mbps、または all (すべて)
- 802.11a の有効な速度は **6、9、12、18、24、36、48、54** Mbps、または all (すべて)
- 802.11an の有効な速度は 6、9、12、18、24、36、48、54、または all (すべて)
- 802.11an-mcs の有効な速度は MCS 0、MCS 1、MCS 2、MCS 3、MCS 4、MCS 5、MCS 6、MCS 7、MCS 8、MCS 9、MCS 10、MCS 11、MCS 12、MCS 13、MCS 14、MCS 15、または all (すべて)
- 802.11bgn-mcs の有効な速度は MCS 0、MCS 1、MCS 2、MCS 3、MCS 4、MCS 5、MCS 6、MCS 7、MCS 8、MCS 9、MCS 10、MCS 11、MCS 12、MCS 13、MCS 14、MCS 15、または all (すべて)
- サポートするデータ転送速度
クライアントが接続で使用するオプションの速度で、クライアントとアクセスポイントがサポートする速度です。有効な速度は以下のとおりです。
 - 802.11b の有効な速度は 1、2、5.5、11 Mbps、または all (すべて)
 - 802.11g の有効な速度は 6、9、12、18、24、36、48、および 54 Mbps、または all (すべて)
 - 802.11bg の有効な速度は 1、2、5.5、11、6、9、12、18、24、36、48、および 54 Mbps、または all (すべて)
 - 802.11bgn の有効な速度は 1、2、5.5、11、6、9、12、18、24、36、48、および 54 Mbps、または all (すべて)
 - 802.11a の有効な速度は **6、9、12、18、24、36、48、および 54** Mbps、または all (すべて)
 - 802.11an の有効な速度は **6、9、12、18、24、36、48、および 54** Mbps、または all (すべて)
 - 802.11an-mcs の有効な速度は MCS 0、MCS 1、MCS 2、MCS 3、MCS 4、MCS 5、MCS 6、MCS 7、MCS 8、MCS 9、MCS 10、MCS 11、MCS 12、MCS 13、MCS 14、MCS 15、または all (すべて)
 - 802.11bgn-mcs の有効な速度は MCS 0、MCS 1、MCS 2、MCS 3、MCS 4、MCS 5、MCS 6、MCS 7、MCS 8、MCS 9、MCS 10、MCS 11、MCS 12、MCS 13、MCS 14、MCS 15、または all (すべて)

すべての基本転送速度は、サポートされる転送速度として入力する必要があります。



基本速度を ESS プロファイルで変更すると、すべての ESSID にあるすべてのクライアントでこれが再度割り当てられます。

サポートされるデータ伝送速度とは、アクセス ポイントがサポートする伝送速度です。基本データ伝送速度は、サポートされる速度のサブセットです。アクセス ポイントは、まず、Basic (基本) で設定される最大データ伝送速度で送信します。この送信で問題が発生した場合、アクセス ポイントはデータ伝送が可能な最大速度に減速します。

基本データ転送速度の設定には、ESSID 設定モードで `base-tx-rates` コマンドを使用します。たとえば、802.11bg の場合には次のように指定します。

```
controller(config-ssid)# base-tx-rates 802.11bg
1|2|5.5|11|9|12|18|24|36|48|54|all
```

サポートする転送速度の設定には、ESSID 設定モードで `supported-tx-rates` コマンドを使用します。たとえば、802.11bg の場合は次のように指定します。

```
controller(config-ssid)# supported-tx-rates 802.11bg
1|2|5.5|11|9|12|18|24|36|48|54|all
```

基本転送速度を削除するには、`no base-tx-rates` コマンドでモードと速度の値を指定します。たとえば、802.11bg の場合は次のように指定します。

```
controller(config-ssid)# no base-tx-rates 802.11bg
1|2|5.5|11|9|12|18|24|36|48|54|all
```

サポートする転送速度を削除するには、`no supported-tx-rates` コマンドでモードと速度の値を指定します。たとえば、802.11bg の場合は次のように指定します。

```
controller(config-ssid)# no supported-tx-rates 802.11bg
1|2|5.5|11|9|12|18|24|36|48|54|all
```

無線のデータ速度を表示するには、`show ssid` コマンドを使用します。

CLI による VLAN の割り当て

ESSID を作成するときに、VLAN を ESSID に割り当てることができます。こうすることで、ネットワークの特定の部分に ESSID を分離できます。デフォルトでは、ESSID に VLAN は割り当てられません。VLAN を ESSID に割り当てる前に、`vlan` コマンドをグローバル設定モードで使用して VLAN を作成する必要があります。

以下の例では、VLAN に **corp** という名前を割り当てます。

```
controller(config-ssid)# vlan corp
controller(config-ssid)#
```

ESSID の VLAN の割り当てを削除するには、no vlan name コマンドを使用します。以下の例では、ESSID の VLAN 割り当てを削除しています。

```
controller(config-ssid)# no vlan corp
controller(config-ssid)#
```

サポートされる WMM 機能

一般的に WMM には、次の機能が含まれます。

- WMM (QoS 向け)
- WMM PS (U-APSD) - バッテリーの寿命

FortiWLC (SD) は、AP400 および AP1000 の QoS での WMM パケットのタグ付けを自動的にサポートしており (クライアントが WMM である場合)、この機能をオフにはできません。FortiWLC (SD) は、U-APSD を AP400/AP1000 でサポートしており、オンまたはオフにできます。

U-APSD は、バッテリーの寿命を延ばすために高度な省電力のメカニズムを必要とするモバイルデバイスや、遅延が増えることでユーザ体験が急速に悪化する VoIP のようなアプリケーションに最適です。WMM の省電力は、VoIP をサポートする携帯電話やコードレス電話向けに設計されたものです。WMM QoS と WMM APSD の両方のデフォルトと可能な設定を下記に記載します。

WMM-PS では、Wi-Fi ネットワークでサポートされている従来の省電力のメカニズムがさらに強化されています。デバイスが、消費電力が少なく、転送の遅延を最小限に抑えることでパフォーマンスの向上が可能になる、" 仮眠 " 状態にいる時間を長くできます。さらに、U-APSD では、個々のアプリケーションによる効率的かつ柔軟な無線転送と電力管理を推進することで、能力や遅延の要件を制御できます。



AP1000 モデルで WMM または WMM-APSD VoIP フォンを使用し、DSCP が完全優先転送に設定されている場合は、特別な QoS ルールを設定する必要があります。このルールでは、DSCP パラメータ値を CS6 または CS7 に設定することで、AP1000 がパケットを正しくキューイングし、最適な通話品質が確保されるようにする必要があります。

U-APSD 対応のステーションは、非定期のサービス期間 (SP) に AP400/AP1000 にフレームをダウンロードしてバッファするため、従来は発生していたビーコンの待ちは発生しません。U-APSD 対応ステーションでは、ステーションが省電力モードになっていると、AP が U-APSD をネゴシエーションし、U-APSD 用にネゴシエーションされた WMM アクセス カテゴリ

リ (優先度レベル) のデータを転送します。デバイスが省電力モードになると、アップリンクデータ フレームがトリガとなって、U-APSD 有効 WMM_AC キューにバッファされたフレームを AP400/AP1000 が送信するようになります。レガシー モードが保留になると、フレームは伝送されません。CLI の ESSID コマンドの apsd-support を使用して AP400/AP1000 U-APSD サポートを設定するか、Web UI から ESSID の APSD サポートを設定します ([Configuration] > [Wireless] > [ESSID] で [U-APSD] をオンにします)。

U-APSD の設定

APSD 設定は ESS ごとに設定し、APSD サポートはデフォルトでオンになりますが、この設定は、AP400/AP1000 にのみ作用します。Web UI から APSD を設定するには、[Configuration] > [Wireless] > [ESS] をクリックし、リストから ESS を選択して [APSD Support] を [on] に設定します。

CLI で APSD サポートをオン / オフにするには、次の例のように、ESSID に対して apsd-support コマンドを使用します。

```
default# configure terminal
default(config)# essid apsd
default(config-essid)# no apsd-support
default(config-essid)# end
```

仮想セル オーバーフロー機能

Vcell オーバーフローと呼ばれるこの機能は、仮想セル ESS と非仮想セル ESS のペアによって動作します。オーバーフロー ESS は、仮想セル ESS のパラメータ (仮想セルの設定を除く) を継承します。非仮想セル ESS は、仮想セル ESS 上限に達しない限り使用されず、上限に達した場合に、仮想セル ESS が必要に応じて他の ESS にオーバーフローします。2 つの ESS プロファイルが 1 つの SSID を共有することで、クライアントは、シームレスに両方を行き来します。オーバーフローは、しきい値を超えたビーコンに費やされた無線時間のパーセンテージに基いて判断され、パーセンテージが 50% に達すると、クライアントがオーバーフローを開始します。

仮想セル オーバーフローの使用

この機能は、高密度の環境向けに設計されており、ビーコンの転送に起因するボトルネックの解決策となります。仮想セル オーバーフローは、次のような場合に有効です。

- レガシー b デバイスによってビーコンのオーバーヘッドが極端に高くなった。
- 極めて高密度のネットワークがビーコンによって多くの無線時間を消費している。

仮想セル オーバーフローには、次のようなトレードオフがあります。

- モビリティとパフォーマンスのトレードオフ

- 密度とパフォーマンスのトレードオフ
- オーバーフロー クライアントで良好なパフォーマンスを確保するための解決策ではない

Web UI による仮想セル オーバーフローの設定

Web UI から仮想セル オーバーフローを設定するには、次の手順を実行します。

1. 139 ページの「[Web UI による ESS の追加](#)」の手順に従って、仮想セル ESS を作成します。仮想セルの設定を必ず [On] にします。
2. 139 ページの「[Web UI による ESS の追加](#)」の手順に従って、非仮想セル ESS を作成します。[RF Virtualization Mode] を必ず [Virtual Cell] 以外にします。これを、設定が [Overflow for] のオーバーフロー ESS にし、手順 1 で作成した ESS を選択します。このオーバーフロー ESS は、仮想セル ESS のこれ以外のパラメータを継承します。

CLI による仮想セル オーバーフローの設定

CLI の新しい `overflowfrom-essprofile` コマンドが、この目的のために追加されました。以下の例を参照してください。

```
default(15)# show essid
ESS Profile                                Enable/Disable SSID                        Secu-
rity Profile Broadcast Tunnel Interface Type
vcelloverflow                            enable                                vcelloverflow
default                                  on                                  none
ESS Profile(1)

default(15)# configure terminal
default(15)(config)#
default(15)(config)# essid vcelloveflowoss
default(15)(config-essid)# overflow-from vcelloveflow
default(15)(config-essid)# end

default(15)# show essid
ESS Profile                                Enable/Disable SSID                        Secu-
rity Profile Broadcast Tunnel Interface Type
vcelloverflow                            enable                                vcelloverflow
default                                  on                                  none
vcelloverflowoss                        enable                                vcelloverflow
default                                  on                                  none
ESS Profile(2)

default(15)# show essid vcelloverflowoss
Profile                                     ESS
ESS Profile                               : vcelloverflowoss
Enable/Disable                           : enable
SSID                                       : vcelloverflow
Security Profile                         : default
```

```

Primary RADIUS Accounting Server      :
Secondary RADIUS Accounting Server    :
Accounting Interim Interval (seconds) : 3600
Beacon Interval (msec)                : 100
SSID Broadcast                        : on
Bridging                             : none
New AP's Join ESS                     : on
Tunnel Interface Type                 : none
VLAN Name                            :
Virtual Interface Profile Name        :
GRE Tunnel Profile Name               :
Allow Multicast Flag                  : off
Isolate Wireless To Wireless traffic : off
Multicast-to-Unicast Conversion       : on
RF Virtualization Mode                : NativeCell
Overflow from                         : vcelloverflow
APSD Support                          : on
DTIM Period (number of beacons)       : 1
Dataplane Mode                       : tunneled
AP VLAN Tag                           : 0
AP VLAN Priority                      : off
Countermeasure                       : on
Multicast MAC Transparency            : off
Band Steering Mode                    : disable
Band Steering Timeout(seconds)        : 5

```

ブリッジとトンネル

ブリッジ AP 機能を使用すると、コントローラとは別の、たとえばサテライト オフィスのような場所に、WAN または ISP を使用して AP をインストールし、管理できます。ブリッジ接続で暗号化を有効にすると、ISP ベース接続にセキュリティが確立されます。

コントローラは、キーブアライブ シグナルを使用して、リモート AP を監視します。リモート AP は、認証やアカウンティングなどの制御情報をコントローラ経由で交換できますが、データは交換できません。(ただし、リモート ブリッジ AP は、サブネット内の他の AP とデータを交換できます。)

ブリッジ ESS プロファイルでサポートされている機能

ブリッジ ESS プロファイルでは、次の機能をサポートしています。

- WMM QoS AP400
- AP400 と AP1000 は、固定および動的 VLAN によるブリッジ ESS プロファイルをサポートします。
- Radius ベースの VLAN 割り当て

- 仮想セル / 仮想ポート (AP400、AP822、AP832、FAP-U421EV、FAP-U423EV、AP1000)
- 802.1X 認証 (動的 WEP、WPA、WPA2、または混在)
- 複数の ESSID
- キャプティブ ポータルを除くすべてのセキュリティ モード / オプション (固定キーと動的キーの両方)
- RADIUS 認証とアカウントリング ACL ベースおよび RADIUS ベースの MAC フィルタリング
- ACL ベースおよび Radius ベースの MAC フィルタリング
- IP DSCP または 802.1p と WMM アクセス カテゴリのマッピング (AP400)
- ブリッジ モードでのキャプティブ ポータルのサポート。
- QoS ルール
- L3 モビリティ

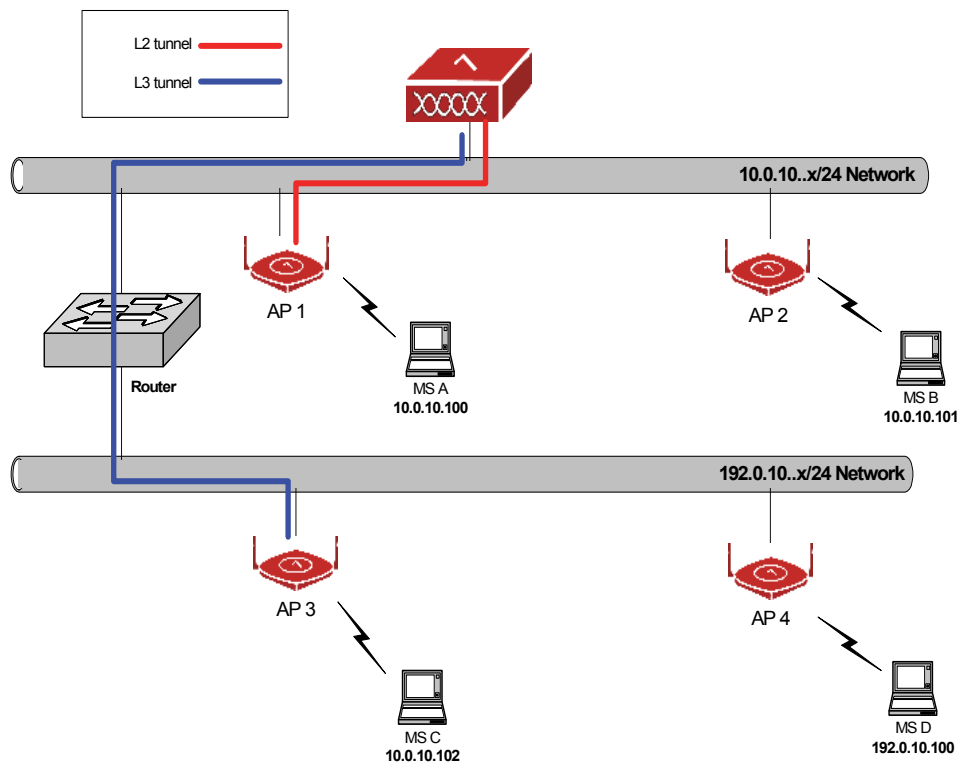
リモート AP はデータプレーン トラフィック (DHCP を含む) をコントローラと交換できないため、リモート AP 構成では、一部の フォーティネット ワイヤレス LAN 機能を使用できません。次の機能が含まれます。

- QoS ルールにファイアウォール フィルタ ID が含まれる場合、この QoS ルールはブリッジ モード ESS では無視されます。
- 動的フロー検出 (SIP/H.323 向け)
- DHCP リレー

ブリッジ AP 配備の例

下図は、リモート ブリッジ AP 配備の例です。AP1 は L2/ ローカル モードに、AP2 は L2/ リモート モードに、AP3 は L3/ ローカル モードに、AP4 は L3/ リモート AP モードにそれぞれ設定されています。コントローラ AP1 と AP2 は、同じ 10.0.10.x/24 サブネットに、AP3 と AP4 は異なるサブネット 192.0.10.x/24 に存在します。青と赤の線はそれぞれ、L2 と L3 のデータ トンネルを示します。また、MS A は D を介して AP 1 から 4 に関連付けられています。MS C と MS D は、同じ IP サブネット内の AP に割り当てられているものの、IP アドレスは異なります。その理由は、AP3 がローカル モードで設定されていて、レイヤ 3 のコントローラに再びトンネルされるためです。以下の例は、モバイル クライアントの IP ドメインが、データプレーンのブリッジまたはトンネルの設定によってどのように変更されるかを示します。

図 35: リモート AP トポロジの例



ブリッジ プロファイルの設定

UI の詳細な手順については、139 ページの「[Web UI による ESS の追加](#)」を参照するか、[Configuration] > [Wireless] > [ESS] をクリックして、編集する ESS を選択します。

CLI で、既存の ESSID にブリッジ AP を設定するには、以下の手順を実行します。

1. ESSID 設定モードに入り、データプレーン モードをブリッジに設定します。

```
controller# configure terminal
controller(config)# essid profile_name
controller(config-ap)# dataplane bridged
controller(config-ap)# exit
```

設定を変更したら、AP をハードリブートします。

2. コントローラとリモート AP の間にセキュア接続を確立するには、以下のコマンドを使用して、AP 接続のみを暗号化します。

```
controller# configure terminal
controller(config)# ap ap#
controller(config-ap)# dataplane-encryption on
controller(config-ap)# exit
```

リモート AP 機能を使用するには、会社のファイアウォール設定を更新して、特定のイーサネット ポートでのワイヤレス アクセスを許可する必要があります。該当するポートは以下のとおりです。

- L2 (イーサネット) L3 (UDP)
- Data 0x4000 9393
- Comm 0x4001 5000
- Discovery 0x4003 9292

WAN のサバイバビリティ

FortiWLC (SD) は、WAN 接続の停止中にブリッジおよびトンネル モードのデバイスで次のサポートを提供します。

ブリッジ AP とコントローラのコンタクトが失われた場合の処理

ブリッジ AP がホスト コントローラのコンタクトを失うと、デフォルト設定の 120 分間、またはコントローラのリンク プローブ設定 (1 ~ 32000 分) に指定された期間のアップタイムを提供します。この間に、既存のクライアントは正常に機能しますが、AP 間でのローミングはできません。この状況では、新しいクライアントはブリッジ AP に参加できません。

トンネル モードでは次のように動作します。

- ブリッジおよびトンネル モードでのバックアップ ESS を指定できます。このバックアップ プロファイルは、コントローラのリンクがダウンしているときに有効になります。
- 停止中に接続しようとする新しいデバイスは、クリアおよび PSK プロファイルを使用して接続します。

クライアントへのサービスはリンクがアップするまで継続され、停止中に接続したすべての新しいデバイスは、リンクがアップした後で再接続します。

マルチキャスト

マルチキャストは、ビデオなどのストリーミング メディアの配信で、複数の宛先に同時に配信するためによく使用される方法です。ストリームのコピーを各クライアントに送信する代

わりに、複数のクライアントが情報の 1 つのコピーを共有することで、ネットワークの負荷を軽減します。マルチキャストは高度な機能であり、ネットワークに多少の変化をもたらす可能性があります。デフォルトでは、マルチキャストは無効であり、特定の状況でのみ、有効にしてください。マルチキャストの用途としては、次のようなものがあります。

- ケーブルまたは衛星による IPTV のブロードキャスト (たとえば、Vbrick や Video Furnace)
- ブロードキャスト アプリケーション (たとえば、社長の全社員向けメッセージ)
- 遠隔学習 (ライブ講習)
- ビデオ監視
- ビデオ会議

マルチキャストが動作するには、次の 4 つの手順を実行する必要があります。

- AP400 で仮想セルと仮想ポートを有効にします (155 ページの「[CLI による AP400 の仮想セル サポートの設定](#)」と 157 ページの「[プローブ応答しきい値の設定](#)」の手順を参照してください)。
- コントローラの IGMP スヌーピングを有効にします (168 ページの「[コントローラと AP の IGMP スヌーピングの設定](#)」を参照してください)。
- 中間スイッチが含まれるネットワーク インフラストラクチャの IGMP スヌーピングを有効にします。これは、FortiWLC がソース マルチキャスト グループのメンバの問い合わせを実行しないために必要です。多くのコントローラと同様に、フォーティネットのコントローラも、この処理の実行をスイッチに依存しています。
- 仮想セルが有効な ESS をデフォルトの VLAN にマッピングします (160 ページの「[CLI による VLAN の割り当て](#)」を参照してください)。

コントローラと AP の IGMP スヌーピングの設定

マルチキャストは、IGMP スヌーピングを使用して実装されています。FortiWLC (SD) リリース 3.6 では、IGMP スヌーピングはコントローラのみで実行されていました。コントローラは、どのクライアントがどのマルチキャスト ストリームにサブスクライブされているかを認識し、サブスクライブされているマルチキャスト ストリームのみが、クライアントにサービスを提供している AP に送信されていました。AP は、どのクライアントがどのストリームにサブスクライブされているかを認識していないため、AP からサービスが提供されているすべてのクライアントにマルチキャスト ストリームが送信されていました。(仮想ポートでは、N 個のコピー (クライアントごとに 1 個) のコピーが存在していました。) このことで、無線時間が無駄に使用され、不要なトラフィックやコンテンションが発生していました。

リリース 4.0 以降では、仮想セルを使用する場合、IGMP スヌーピングは、コントローラだけでなく、AP400 (AP1000 を除く) でも実行されます。コントローラは、マルチキャスト ストリームのクライアント サブスクライブ リストを AP400 に渡すため、マルチキャスト ストリームがサブスクライブするクライアントだけに制限され、ワイヤレス トラフィックの削減

と時間の短縮につながります。(非仮想セル ESS プロファイルに接続しているステーションのマルチキャストの送信については、変更ありません。)

IGMP スヌーピングを設定するコマンド

以下のコマンドを使用して、コントローラおよび AP の IGMP スヌーピングを有効 / 無効にします。

```
igmp-snoop state [enable, disable]
```

igmp-snoop のステータスを表示するコマンド

```
show igmp-snoop
```

現在アクティブであるマルチキャスト グループを表示するコマンド

```
show igmp-snoop forwarding-table
```

マルチキャスト グループに参加しているステーションを表示するコマンド

```
show igmp-snoop subscription-table
```

マルチキャスト MAC 透過機能

この機能によって、一部のクライアントのマルチキャスト パケットの受信で必要になる、トンネル マルチキャストの MAC 透過が有効になります。マルチキャストは高度な機能であり、ネットワークに多少の変化をもたらす可能性があります。デフォルトでは、マルチキャストは無効です。マルチキャストを有効にするには、multicast-enable コマンド (下記の例を参照)、または Web UI の [Configuration] > [Wireless] > [ESS] > [Add] (下記の例を参照) を使用します。



マルチキャストは高度な機能です。マルチキャストを WLAN で有効にすると、ネットワークに若干の変化が発生する可能性があります。マルチキャストを有効にする前に、フォーティネット カスタマ サービスのテクニカル アシスタンス センタにお問い合わせください。

Web UI からのマルチキャストの有効化

マルチキャストを Web UI から有効にするには、ESS を追加または変更します。手順については、139 ページの「[Web UI による ESS の追加](#)」を参照してください。

CLI によるマルチキャストの有効化

以下の例では、CLI でマルチキャストを有効にします。

```
controller(config-essid)# multicast-enable
```

コマンドの詳細については、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。

VLAN と ESS プロファイルのマッピングの表示

以下のコマンドを使用して、現在マッピングされている VLAN と ESS プロファイルを表示します。

```
controller# show vlan ess-profile
```

コマンドの詳細については、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。

VLAN ごとのマルチキャストの制限

「マルチキャストからユニキャスト」への変換が有効になっているとき、マルチキャスト / ブロードキャスト パケットは該当する VLAN のみに限定されます。



この制限はワイヤレス クライアントのみに適用され、有線ポート プロファイルのクライアントには適用されません。

サポート対象 : AP110、AP122、AP332、AP822、AP832、OAP832、AP1020

GRE ESSID 機能

GRE トンネルのための ESSID 設定については、[第 13 章「VLAN の設定」](#)で説明しています。

バンド ステアリング機能

バンド ステアリングは、その能力を基準にクライアントにバンドを割り当てることで、マルチバンド対応クライアントを動作させます。バンド ステアリングを利用しないと、ABG クライアントは A または B/G のいずれかのチャンネルに関連付けられるため、特定のバンドに負荷が集中する恐れがあります。バンド ステアリングを利用すると、このトラフィックの一部を A バンドに送るように指示できます。バンド ステアリングを利用する別の例として、音声とデータ トラフィックの分離があります。すべての音声対応クライアントを（帯域幅が問題にならない）B/G チャンネルに置いたまま、データのためのクライアントを A バンドに移動できるため、高速のデータ転送が可能になります。ABGN トラフィックにバンド ステアリングを使用するには、5GHz バンドへの A 機能があるデュアル モードクライアントに A ステアリングを使用するよう指示し、5GHz バンドへの AN 機能があるすべてのデュアル モード クライ

ントに N ステアリングを使用するよう指示します。バンド ステアリングは、マルチキャスト
トラフィックの振り分けにも便利です。

Web UI によるバンド ステアリングの設定

バンド ステアリングは、ESS ごとに有効にします。ESS を作成または変更する際に、バンド
ステアリングを有効にできます。Web UI で有効にするには、[139 ページの「Web UI による
ESS の追加」](#)の指示に従って、[Enable Band Steering] フィールドを [On] に設定します。[Band
Steering Timeout] フィールドのデフォルトは 5 秒で、これは、関連付けられていない禁止さ
れているバンドへのステアリング対象クライアントの割り当てをブロックする秒数です。ク
ライアントが追加された段階でこのコマンドが動作するようにするために、ESS で [New APs
Join ESS] フィールドも [on] に設定します。

CLI によるバンド ステアリングの設定

バンド ステアリングに関する 2 つの CLI コマンドが追加されました。[bandsteering- mode]
は、ESS のバンド ステアリングを有効にします。[band-steeringtimeout] は、関連付けられて
いない状態で、ステアリングされたクライアントの割り当てを禁止されているバンドでブ
ロックする秒数です。band-steeringmode disable コマンドは、バンド ステアリングをオフに
します。バンド ステアリングを使用するには、以下の設定で ESS を作成します。

```
ESS Profile
ESS Profile                : bandsteering
Enable/Disable             : enable
SSID                       : bandsteering
Security Profile           : default
Primary RADIUS Accounting Server :
Secondary RADIUS Accounting Server :
Accounting Interim Interval (seconds) : 3600
Beacon Interval (msec)     : 100
SSID Broadcast             : on
Bridging                   : none
New AP's Join ESS          : on
Tunnel Interface Type      : none
VLAN Name                  :
Virtual Interface Profile Name :
GRE Tunnel Profile Name    :
Allow Multicast Flag       : off
Isolate Wireless To Wireless traffic : off
Multicast-to-Unicast Conversion : on
RF Virtualization Mode     : VirtualCell
Overflow from              :
APSD Support               : on
DTIM Period (number of beacons) : 1
```

```

Dataplane Mode           : tunneled
AP VLAN Tag              : 0
AP VLAN Priority          : off
Countermeasure           : on
Multicast MAC Transparency : off
Band Steering Mode        : a-steering
Band Steering Timeout(seconds) : 5

```

以下の例は、Bandsteeress という名前の既存の ESS で、バンド ステアリングを A チャネルに設定します。

```

default(15)# configure terminal
default(15)(config)# essid bandsteering
default(15)(config-essid)# dataplane bridged
default(15)(config-essid)# band-steering-mode a-steering
default(15)(config-essid)# end
default(15)#
default(15)# show essid bandsteering
ESS Profile
ESS Profile                : bandsteering
Enable/Disable             : enable
SSID                       : bandsteering
Security Profile           : default
Primary RADIUS Accounting Server :
Secondary RADIUS Accounting Server :
Accounting Interim Interval (seconds) : 3600
Beacon Interval (msec)      : 100
SSID Broadcast             : on
Bridging                   : none
New AP's Join ESS          : on
Tunnel Interface Type      : none
VLAN Name                  :
Virtual Interface Profile Name :
GRE Tunnel Profile Name    :
Allow Multicast Flag       : off
Isolate Wireless To Wireless traffic : off
Multicast-to-Unicast Conversion : on
RF Virtualization Mode     : VirtualPort
Overflow from              :
APSD Support               : on
DTIM Period (number of beacons) : 1
Dataplane Mode             : bridged
AP VLAN Tag                : 0
AP VLAN Priority           : off
Countermeasure             : on
Multicast MAC Transparency : off

```

```

Band Steering Mode                : a-steering
Band Steering Timeout(seconds)    : 5

```

以下の例は、バンド ステアリングを無効にします。

```

default(15)# configure terminal
default(15)(config)# essid bandsteering
default(15)(config-essid)# band-steering-mode disable
default(15)(config-essid)# end
default(15)#
default(15)# sh essid bandsteering
ESS Profile
ESS Profile                        : bandsteering
Enable/Disable                    : enable
SSID                              : bandsteering
Security Profile                  : default
Primary RADIUS Accounting Server  :
Secondary RADIUS Accounting Server :
Accounting Interim Interval (seconds) : 3600
Beacon Interval (msec)           : 100
SSID Broadcast                    : on
Bridging                         : none
New AP's Join ESS                 : on
Tunnel Interface Type             : none
VLAN Name                        :
Virtual Interface Profile Name    :
GRE Tunnel Profile Name          :
Allow Multicast Flag              : off
Isolate Wireless To Wireless traffic : off
Multicast-to-Unicast Conversion  : on
RF Virtualization Mode           : VirtualPort
Overflow from                     :
APSD Support                      : on
DTIM Period (number of beacons)  : 1
Dataplane Mode                   : bridged
AP VLAN Tag                      : 0
AP VLAN Priority                  : off
Countermeasure                   : on
Multicast MAC Transparency       : off
Band Steering Mode               : disable
Band Steering Timeout(seconds)    : 5

```

完全優先転送の上書き

[Expedited Forward Override] オプションは、システムのデフォルト DSCPWMM 優先度マッピングを上書きします。DSCP Expedited Forwarding (46) とマークされた IP ダイアグラムは、ダウンストリームの音声キュー (AC_VI) ではなく、AP の WMM 音声キュー (AC_VO) から (ステーションに) 送信されます。この機能は AP400 固有のものであり、デフォルトでは無効です。ESS プロファイルごとに設定でき、ブリッジとトンネルの両方の ESS プロファイルで動作します。

[Expedited Forward Override] (完全優先転送の上書き) を設定する手順

1. ESSID の完全優先転送機能を有効にする手順 :

```
default # config terminal
default(config)# essid meru
default(config-essid)# expedited-forward-override
default(config-essid)# end

default# show essid meru
ESS Profile
ESS Profile                               : meru
Enable/Disable                            : enable
SSID                                       : meru
Security Profile                          : default
Primary RADIUS Accounting Server          :
Secondary RADIUS Accounting Server        :
Accounting Interim Interval (seconds)    : 3600
Beacon Interval (msec)                   : 100
SSID Broadcast                            : on
Bridging                                  : none
New AP's Join ESS                         : on
Tunnel Interface Type                     : none
VLAN Name                                 :
Virtual Interface Profile Name            :
GRE Tunnel Profile Name                   :
Allow Multicast Flag                      : off
Isolate Wireless To Wireless traffic     : off
Multicast-to-Unicast Conversion           : on
RF Virtualization Mode                   : VirtualPort
Overflow from                             :
APSD Support                             : on
DTIM Period (number of beacons)          : 1
Dataplane Mode                           : tunneled
AP VLAN Tag                              : 0
AP VLAN Priority                          : off
Countermeasure                            : on
```

Multicast MAC Transparency	: off
Band Steering Mode	: disable
Band Steering Timeout(seconds)	: 5
Expedited Forward Override	: on
SSID Broadcast Preference	: till-association
B Supported Transmit Rates (Mbps)	: 1,2,5.5,11
B Base Transmit Rates (Mbps)	: 11

2. ESSID の完全優先転送機能を無効にする手順 :

```

Meru# config terminal
Meru(config)# essid meru
Meru (config-ssid)# no expedited-forward-override
Meru(config-ssid)# end
Meru # show essid meru
ESS Profile
ESS Profile                               : meru
Enable/Disable                           : enable
SSID                                     : meru
Security Profile                         : default
Primary RADIUS Accounting Server         :
Secondary RADIUS Accounting Server       :
Accounting Interim Interval (seconds)   : 3600
Beacon Interval (msec)                  : 100
SSID Broadcast                           : on
Bridging                                 : none
New AP's Join ESS                        : on
Tunnel Interface Type                    : none
VLAN Name                                :
Virtual Interface Profile Name           :
GRE Tunnel Profile Name                  :
Allow Multicast Flag                     : off
Isolate Wireless To Wireless traffic    : off
Multicast-to-Unicast Conversion          : on
RF Virtualization Mode                   : VirtualPort
Overflow from                            :
APSD Support                             : on
DTIM Period (number of beacons)         : 1
Dataplane Mode                           : tunneled
AP VLAN Tag                              : 0
AP VLAN Priority                          : off
Countermeasure                           : on
Multicast MAC Transparency               : off
Band Steering Mode                       : disable
Band Steering Timeout(seconds)          : 5
Expedited Forward Override               : off
SSID Broadcast Preference                 : till-association

```

B Supported Transmit Rates (Mbps)	: 1,2,5.5,11
B Base Transmit Rates (Mbps)	: 11

Vport の SSID ブロードキャスト

Vport の SSID ブロードキャスト機能は、Cisco フォンを使用する場合の接続性を向上するよう設計されています。

Vport の SSID ブロードキャストの設定

SSID Broadcast for Vport オプションは、ESSID 設定パラメータの同じオプションに似ています。ESSID 設定では、GUI または IOSCLI から、次の 3 つのパラメータを Vport の SSID ブロードキャストのオプションに設定できます。

1. [disable] : これが、ESSID プロファイル ページでのデフォルト設定です。このパラメータを "disable" に設定すると、AP はビーコンの SSID をアドバタイズしません。IOSCLI からこのオプションを "disable" に設定する例

```
default# configure terminal
default(config)# essid assign
default(config-essid)# publish-essid-vport disabled
default(config-essid)# exit
default(config)# exit
```

2. [always] : このパラメータを "always" に設定すると、AP によるビーコンの SSID のアドバタイズが常に有効になります。推奨された場合を除き、この設定にしないでください。IOSCLI からこのオプションを "always" に設定する例

```
default# conf terminal
default(config)# essid assign
default(config-essid)# publish-essid-vport always
default(config-essid)# end
```

3. [till-association] : このパラメータを "till-association" に設定すると、クライアントのアソシエーション段階までビーコンの SSID のアドバタイズが有効になり、接続のそれ以降は SSID ブロードキャストが無効になります。このパラメータは、Vport ON で接続の問題を解決する、一部のバージョンの電話での設定よりも優先されます。ステーションのアソシエーションの後に、AP は SSID 文字列のブロードキャストを停止します。これで、AP CLIに加えて、ESS ごとのコントローラの GUI から、Vport パラメータの SSID ブロード

キャストをユーザが設定できるようになりました。
IOSCLI からこのオプションを "till association" に設定する例

```
default# conf terminal
default(config)# essid assign
default(config-essid)# publish-essid-vport till-association
default(config-essid)# end
```

複数の ESSID のマッピング

以下の設定例では、3 つの ESSID を作成し、それらを 3 つの異なる VLAN にマッピングすることで、guest ユーザ、corporate ユーザ、および retail トラフィックに分離する方法を紹介します。

最初の ESSID である guest-users は、**guest** という名前の VLAN にマッピングされます。この ESSID は、認証方法や暗号化方法を必要としない、デフォルトのセキュリティ プロファイルを使用して設定されます。VLAN の IP アドレスは 10.1.1.2/24 で、デフォルト ゲートウェイは 10.1.1.1 です。DHCP サーバの IP アドレスは 10.1.1.254 です。この ESSID は、各アクセス ポイントに自動的に追加され、仮想 AP の一部になるようにも設定されます。(この ESSID をもつ同一チャンネル上のすべてのアクセス ポイントが、同じ BSSID を共有します。)

2 番目の ESSID である corp-users は、**corp** という名前の VLAN にマッピングされます。この ESSID は、corp-access という名前で認証 / 暗号化方法に 64 ビット WEP を必要とするセキュリティ プロファイルを使用するよう設定されます。固定 WEP は、**corp1** に設定されます。VLAN の IP アドレスは 10.1.2.2/24 で、デフォルト ゲートウェイは 10.1.2.1 です。DHCP サーバの IP アドレスは 10.1.2.254 です。この ESSID は、各アクセス ポイントに自動的に追加され、仮想 AP の一部になるようにも設定されます。

3 番目の ESSID である retail-users は、**retail** という名前の VLAN にマッピングされます。この ESSID は、retail-access という名前で認証方法に 802.1X を必要とするセキュリティ プロファイルを使用するよう設定されます。802.1X キーの変更期間は、1000 秒に設定されます。プライマリ RADIUS サーバの IP アドレスは 10.1.3.200 に、プライマリ RADIUS のポートは 1812 に、プライマリ RADIUS のシークレットは **secure-retail** に設定されます。VLAN の IP アドレスは 10.1.3.2/24 で、デフォルト ゲートウェイは 10.1.3.1 です。DHCP サーバの IP アドレスは 10.1.3.254 です。この ESSID は、ノード ID が 1 のアクセス ポイントにのみ追加されるように設定されます。また、アクセス ポイントからのビーコンでの ESSID 値のブロードキャストは無効で、この ESS には 00:0c:e6:02:7c:84 という BSSID が与えられます。

show vlan コマンドを使用して、VLAN 設定を確認します。

```
controller# show vlan
VLAN Configuration
```

VLAN Name	Tag	IP Address	NetMask	Default Gateway
guest	1	10.1.1.2	255.255.255.0	10.1.1.1
corp	2	10.1.2.2	255.255.255.0	10.1.2.1
retail	3	10.1.3.2	255.255.255.0	10.1.3.1

これで、VLAN とセキュリティ プロファイルが作成されたので、新しい ESSID を作成し、設定できます。

```

controller# configure terminal
controller(config)# essid guest-users
controller(config-essid)# security-profile default
controller(config-essid)# vlan guest
controller(config-essid)# exit
controller(config)# essid corp-users
controller(config-essid)# security-profile corp-access
controller(config-essid)# vlan corp
controller(config-essid)# exit
controller(config)# essid retail-users
controller(config-essid)# security-profile retail-access
controller(config-essid)# vlan retail
controller(config-essid)# no ap-discovery join-ess
controller(config-essid)# no publish-essid
controller(config-essid)# ess-ap 1 1
controller(config-essid-ess-ap)# bssid 00:0c:e6:03:f9:a4
controller(config-essid-ess-ap)# exit
controller(config-essid)# exit
controller(config)# exit
controller#

```

新しい ESSID が作成されたことを確認するには、show essid コマンドを使用します。

新しい ESSID の詳細設定を表示するには、show essid **essid-name** コマンドを使用します。

ESSID の *guest-users* と *corp-users* がコントローラに接続されている両方のアクセス ポイントに自動的に結合され、ESSID *retail-users* が AP 1 だけに結合されたことを確認するには、showess-ap ap **ap-node-id** コマンドまたは show ess-ap essid **essid-name** コマンドを使用します。

```

controller# show ess-ap ap 1
ESS-AP Configuration
AP ID: 1

```

ESSID	AP Name	Channel	BSSID
guest-users	AP-1	6	00:0c:e6:01:d5:c1
corp-users	AP-1	6	00:0c:e6:02:eb:b5
retail-users	AP-1	6	00:0c:e6:03:f9:a4

```

controller# show ess-ap ap 2
ESS-AP Configuration

```


AP ID	AP Name	Channel	BSSID
2			
ESSID	AP Name	Channel	BSSID
guest-users	AP-2	6	00:0c:e6:01:d5:c1
corp-users	AP-2	6	00:0c:e6:02:eb:b5

```
controller# show ess-ap essid retail-users
```

ESS-AP Configuration

ESSID: retail-users

AP ID	AP Name	Channel	BSSID
1	AP-1	6	00:0c:e6:03:f9:a4

```
controller# show ess-ap essid corp-users
```

ESS-AP Configuration

ESSID: corp-users

AP ID	AP Name	Channel	BSSID
1	AP-1	6	00:0c:e6:02:eb:b5
2	AP-2	6	00:0c:e6:02:eb:b5

リモート ロケーションのブリッジ AP300

ESSID でブリッジ モードが設定されると、その ESSID を使用する AP は、WAN または ISP によって、サテライト オフィスなどのコントローラから離れた場所で導入され、管理されます。コントローラは、keep-alive 信号でリモート AP を監視します。リモート AP は、認証およびアカウント情報などの制御情報をコントローラと交換できますが、データの交換はできません。リモート AP はサブネット内の他の AP とデータを交換できます。

リモート AP はデータプレーン トラフィック (DHCP を含む) をコントローラと交換できないため、リモート AP 構成では、一部の フォーティネット ワイヤレス LAN 機能を使用できません。次の機能が含まれます。

- QoS
- キャプティブポータル
- L3 モビリティ

次の機能を使用できます。

- VLAN
- 仮想セル
- 802.1X 認証
- 高ユーザ密度
- 複数の ESSID
- L3 トンネルのバックホールのデータプレーン暗号化

Web UI によるブリッジ モードの設定

Web UI で ESS を追加または変更する際にブリッジ モードを設定する手順については、[139 ページの「Web UI による ESS の追加」](#)を参照してください。

CLI によるブリッジ モードの設定

以下の例では、ESSID abcjk を作成し、モードをブリッジに設定し、タグを割り当て、最上位の優先度を abcjk に与えます。

```
test (config-ssid)#  
test# configure terminal  
test (config)# ssid abcjk  
test (config-ssid)# dataplane bridged  
test (config-ssid)# ap-vlan-tag 11  
test (config-ssid)# ap-vlan-priority  
test (config-ssid)# end
```

ここで使用しているコマンドの詳細については、『コマンド リファレンス ガイド』を参照してください。

単一 MAC での複数 IP の使用

現在の実装では、一般的なクライアント マシン (またはステーション) には、使用中のワイヤレス アダプタごとに 1 つの IP アドレスが与えられます。ただし、(VMware や Parallels などによって提供される) 仮想マシン モデルの利用が増加していることを考慮して、1 つのステーションで単一クライアントから複数のオペレーティング システムを実行できるようになっています。Fortinet FortiWLC (SD) の本バージョンでは、仮想マシンごとに個別の IP アドレスが与えられるため、パケット転送のトラブルシューティングが格段に容易になりました。

この機能をサポートするために、FortiWLC (SD) の [ESS Profile] 画面に、MIPS というラベルの新しい機能が追加されました。この機能は、デフォルトでは無効ですが、有効にすると、必要に応じて、" ホスト " (メイン) のオペレーティング システムから " ゲスト " (仮想) のシステムに、パケットがブリッジされます。以下の点に注意してください。

- クライアントから送信されるすべてのデータ パケットは、ソース アドレスのホスト OS MAC アドレスになります。
- クライアントに送信されるすべてのデータ パケットは、宛先アドレスのホスト OS MAC アドレスになります。
- OS ごとにクライアント ハードウェア アドレスが異なり、このアドレスは DHCP ペイロードの一部として送信されます。
- " ゲスト " OS ハードウェア デバイスには "00:0c:29" で始まる MAC アドレスが割り当てられますが、これは、VMware のグローバル標準 OUI です。DHCP サーバは、このハードウェア アドレスを使用することで、ゲスト OS を識別し、異なる IP アドレスの割り当てることができます。
- どの IP から送信される Grarp ARP パケットにも、対応する固有のクライアント ハードウェア アドレスが含まれます。

- ホスト OS が受信するすべてのブロードキャスト パケットは、ゲスト OS にも配信されます。
- ホスト OS が受信するすべてのユニキャスト パケットは、パケットの宛先 IP アドレスに基いてゲスト OS に配信されます。

この機能をサポートするためのコマンドが CLI に追加されました。

- `show station multiple-ip` : 個々のステーションから提供されるすべての IP アドレスと MAC アドレスを表示します (仮想デバイスの場合は 'vmac' というラベル)。ホスト デバイスの場合は、クライアント MAC と仮想 MAC が同じになります。



- IPv4 および IPv6 アドレス タイプのみがサポートされています。
- 1 つのステーションに属するすべての IP アドレスは、同じ VLAN の一部であると見なされます。
- 仮想 OS から提供される IP アドレスは常に動的アドレスであり、固定アドレスはサポートされていません。
- この機能が有効である場合、ICR はサポートされません。

時間ベースの ESS

ESS の提供は、事前定義済みの間隔でスケジューリングできます。デフォルトでは、ESS プロファイルは常にオンであり、クライアント / デバイスが使用可能です。タイマーを追加することで、事前定義された 1 日または数日の時間に基づいて ESS プロファイルの提供を制御できます。

時間ベースの ESS プロファイルを作成するには、最初にタイマー プロファイルを作成してから、タイマー プロファイルを ESS プロファイルに関連付けます。

タイマー プロファイルの作成

タイマー プロファイルは、Web UI または CLI を使用して作成できます。

Web UI の使用

[Configuration] > [Timer] に移動して、[Add] ボタンをクリックします。

[Add Timer Profile] ポップアップ ウィンドウで、[Timer Profile Name] に入力し、[Timer Type] を選択します。

Add Timer Profile

Timer Profile Name * Enter 1-32 chars.

Timer Type Absolute ▼

Absolute Timer

Service Start Time 1

Service End Time 1

Service Start Time 2

Service End Time 2

Service Start Time 3

Service End Time 3

SAVE CANCEL

- 絶対時刻タイマー プロファイルを使用して、複数の日にわたる時間の ESS の表示を有効 / 無効にできます。各タイマー プロファイルについて、最大 3 つの開始および終了時刻を設定できます。開始時刻または終了時刻を入力するには、日付選択ボックスをクリックします。下図を参照してください。
- 定期タイマー プロファイルは、1 週間の複数の曜日にわたって適用可能な開始タイムスタンプと終了タイムスタンプのセットです。定期タイマー プロファイルを作成するには、hh:mm の形式で時刻を入力します。hh は 2 桁の時間、mm は 2 桁の分です。図 2 は、日曜日、月曜日、火曜日、および木曜日の 08:10 a.m. または 14:45 (2.45 p.m) から適用されるタイマー プロファイルを示しています。

Periodic Timer

DaysOfTheWeek	<input type="checkbox"/> Sunday	<input type="checkbox"/> Monday	<input type="checkbox"/> Tuesday	<input type="checkbox"/> Wednesday
	<input type="checkbox"/> Thursday	<input type="checkbox"/> Friday	<input type="checkbox"/> Saturday	
Time Interval Start 1	<input type="text"/>	HH:MM		
Time Interval End 1	<input type="text"/>	HH:MM		
Time Interval Start 2	<input type="text"/>	HH:MM		
Time Interval End 2	<input type="text"/>	HH:MM		
Time Interval Start 3	<input type="text"/>	HH:MM		
Time Interval End 3	<input type="text"/>	HH:MM		

CLI の使用

新しい CLI コマンドで、さまざまなオプションを使用してタイマー プロファイルを作成できます。

構文

```
#(config-mode) timer-profile <profile-name>

#(timer-config-mode) <timer-type> <timer-slot> start-time <"mm/dd/yyyy hh:mm">
end-time <"mm/dd/yyyy hh:mm">
```

- timer-type は、絶対時刻タイマーまたは定期タイマーのいずれかになります。
- 絶対時刻タイマー プロファイルには、タイマーのスロットを 3 つ作成できます。
- 時刻は、mm/dd/yyyy<スペース>hh:mm の形式で二重引用符に囲んで指定する必要があります。

使用例：絶対時刻タイマー プロファイルの作成

```
default# configure terminal

default (config)# timer-profile monthly-access

default (config-timer)# absolute-timer time-slot-1 start-time "01/01/2014
10:10" end-time "02/02/2014 08:45"
```


7 冗長性の実装

次の 3 つのオプションを、コントローラの冗長性に使用できます。

- 冗長イーサネット: イーサネット リンクのこのレベルの冗長性では、イーサネット リンクがダウンすると、同じコントローラの別のイーサネット リンクが処理を引き継ぎます。
- N+1: コントローラのこのレベルの冗長性では、あるコントローラがダウンすると、指定されたスレーブ コントローラが障害が発生したマスタ コントローラを引き継ぎます。
- オプション 43: コントローラのこのレベルの冗長性では、AP がプライマリとセカンダリの両方のコントローラを認識します。プライマリ コントローラがダウンすると、AP が自動的にセカンダリ コントローラに切り替えます。プライマリ コントローラが復帰すると、プライマリ コントローラに切り替えます。

本章は、以下の項で構成されています。

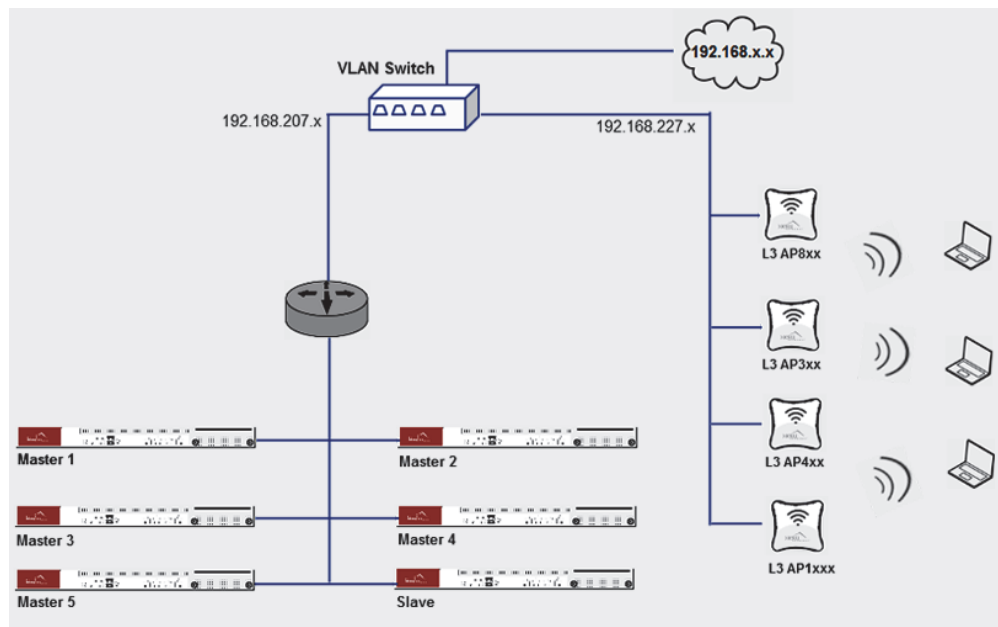
- [CLI による冗長イーサネット フェイルオーバーの設定](#)
- [N+1 冗長性](#)
- [オプション 43](#)

[illegible]

N+1 では、バックアップ コントローラがプライマリ コントローラと同じサブネットである必要があります。DHCP オプション 43 では、AP のプライマリとバックアップのコントローラを指定でき、この設定では、バックアップ コントローラがプライマリ コントローラと異なるサブネットであっても構いません。

N+1 の検出メカニズム

以下のフローチャートでは、N+1 のメカニズムを示しています。



冗長イーサネット

MC1500 を運用している場合は、以降の項で説明する手順に従うだけで、イーサネット冗長性をいつでも有効にできます。ただし、以下のコントローラ モデルでは、イーサネット冗長性をアクティブにする前に、デュアル ポート ボンディングを有効にする必要があります。

- MC3200
- MC4200
- MC5000 (アクセラレータ カード付き)
- MC6000



ボンディング モードがデュアルの場合は、g1 と g2 の両方のインターフェイスがマスタとスレーブの両方に接続している必要があります。

デュアル ボンディングを有効にするには、以下のコマンドを入力してコントローラを再起動します。

```
default# configure terminal
default(config)# bonding dual
default(config)# exit
default# copy running-config startup-config
```

CLI による冗長イーサネット フェイルオーバーの設定

次のコマンドは、コントローラのイーサネット インターフェイス 2 をイーサネット インターフェイス 1 のバックアップとして設定します。

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# type redundant
default(config-if-FastEth)# exit
default(config)# exit
default# copy running-config startup-config
```



冗長設定では、2 つ目のイーサネット インタフェースの IP アドレスを設定できません。フェイルオーバーが発生すると、プライマリ イーサネット インターフェイスの IP アドレスを受け取ります。

変更を有効にするには、システムをリブートする必要があります。ここでシステムをリブートし、show second_interface_status コマンドで 2 つ目の冗長インターフェイス設定を確認します

```
default# show second_interface_status
```

冗長イーサネット フェイルオーバーからのリカバリ

デュアル イーサネット 冗長モード設定が完了したら、コントローラをリブートする必要があります。上記の指示を参照してください。リブート後に、1 つ目のイーサネット インタフェース リンクがダウンすると、2 つ目のイーサネット インタフェースがコントローラ接続を引き継ぎます。冗長イーサネット フェイルオーバーは、LinkID に基づくものであり、スパンニング ツリー構成は必要ありません。LinkID が失われると、1 秒未満でフェイルオーバーが発生します。このフェイルオーバーは、アクセス ポイントからは透過的です。1 つ目のインタフェースが復帰したとしても、2 つ目のインターフェイスは引き続きアクティブのまま、すべての AP の処理を続行します。CLI コマンドの show second-interface-status で、これを確認できます。2

つ目のインターフェイスがダウンした場合のみ、1 つ目のインターフェイスが (アップしていれば) コントローラ接続を引き継ぎます。



ハードウェア コントローラでは、スイッチ ポートがダウンすると、インターフェイスのダウンとして検出され、リンク ダウンのアラームが生成されます。さらに、仮想コントローラでは、スイッチ ポートがダウンしても、インターフェイスのダウンとして検出されないため、リンク ダウンのアラームも生成されません。

VMWare クライアント ソフトウェアにおいて、マッピングされたインターフェイスが切断されたものとして設定されると、アラームが生成されます。

N+1 または L3 の冗長性も設定されている場合にコントローラ 1 で障害が発生すると、AP はコントローラ 2 に移動します。コントローラ 1 が再びオンラインになると、AP は即座にコントローラ 2 に戻り始めます。「[デュアル イーサネット フェイルオーバーによる N+1 からのリカバリ](#)」も参照してください。

N+1 冗長性

N+1 冗長性を実現するオプションのソフトウェア機能を実装した場合、同じサブネット内にあるスタンバイ N+1 スレーブ コントローラで、複数のマスタ コントローラの監視とシームレスなフェイルオーバーが可能になります。

複数のマスタ コントローラと 1 台のスタンバイ スレーブ コントローラが、固定 IP アドレス指定によって同一のサブネットに属するよう設定され、N+1 クラスタとして認識されます。スタンバイ スレーブは、クラスタにあるマスタ コントローラの可用性を監視しますが、これは、マスタが必要な間隔でウェルノウン UDP ポートを介して送信するアドバタイズ メッセージをスタンバイ スレーブが受信することで実現されます。4 つの連続するアドバタイズを受信しないと、スタンバイ スレーブは、アクティブ スレーブにステータスを変更し、障害のあったマスタの IP アドレスと操作を引き継ぎます。スタンバイ スレーブには、最後に保存されたマスタの設定のコピーがあるため、設定されているすべてのサービスは、スレーブがスタンバイからアクティブに切り替わる短い間だけ一時停止しますが、そのまま続行されます。

N+1 フォールバック

スレーブがアクティブ スレーブとしての役割を担う間、障害のあったマスタがクラスタに再度加わるまで、クラスタに対する監視活動は中断されます。アクティブ スレーブは、ARP を介したマスタのリスタートを検知します。アクティブ スレーブは、(アドバタイズ メッセージを介して) マスタが復帰したことを認識すると、引き続きアクティブ スレーブのままとなり、元のマスタはパッシブ状態に移行します。パッシブ状態となったマスタには、元のスレーブの IP アドレスが割り当てられます。パッシブ マスタをアクティブ マスタのステータスに移行するには、アクティブ スレーブで `nplus1 revert` コマンドを使用します。

```

NP-MC4200-master(15)(config)# nplus1 revert
NP-MC4200-master(15)(config)# end
NP-MC4200-master(15)# sh nplus1
-----

Current State : Active->Passive Slave
Heartbeat Period : 1000 milliseconds
Heartbeat Threshold : 4 threshold
Master IP : 172.19.215.31
Master Hostname : NP-MC4200-master
Slave IP : 172.19.215.32
Slave Hostname : NP1-MC4200-slave
License Type : Demo
License Usage (Used/Tot) : 1/1
-----

Master Controllers

-----

```

Hostname	IP Address	Admin	Status
NP-MC4200-master	172.19.215.31	Enable	Passive->Active

障害のあったマスタを長時間オフラインにする必要がある場合、管理者は手動でアクティブスレーブをスタンバイスレーブ設定に戻すことができます。この結果、スタンバイスレーブは必要に応じて再度、別のマスタをフェイルオーバーできるようになります。

自動フォールバック

フェイルオーバーが実行された後、パッシブマスタは、(nplus1 period コマンドを使用して指定された間隔で) アクティブスレーブからアドバタイズメントをリスンします。期限内にパッシブマスタがアクティブスレーブからアドバタイズメントを受信しなかった場合、パッシブマスタは自動フォールバックを開始します。

自動復帰

マスタコントローラが停止すると、スレーブコントローラがアクティブなスレーブコントローラとして引き継ぎます。停止していたマスタコントローラがアクティブになると、アクティブなスレーブコントローラで nplus1 revert コマンドが実行されるまでパッシブコントローラとしての状態を保持し続けます。自動復帰を有効にすることで、マスタコントローラがオンライン状態になった後に、最初のマスタコントローラとして引き継ぎます。

デフォルトでは、このオプションは無効になっています。自動復帰を有効にするには、nplus1 autorevert enable コマンドを使用します。自動復帰を有効にすることで、アクティブなスレーブコントローラは自らフォールバックをトリガします。

フェイルオーバーのシナリオ

シナリオ	説明
停電	マスタ コントローラでの停電時にフェイルオーバーが開始される。
スイッチ ポートの障害	スイッチでのポート障害時に、フェイルオーバーが開始される。
イーサネット ケーブルが抜き取られた	マスタ コントローラでイーサネット ケーブルが抜き取られると、スレーブ コントローラが引き継いで、アクティブ スレーブになる。
手動フェイルオーバー	マスタ コントローラで <code>nplus1 takeover</code> コマンドを実行すれば、フェイルオーバーが強制的に実行される。
np1adv プロセスの切断	np1 プロセスがマスタで切断されると、フェイルオーバーが開始される。
自動フェイルオーバー	<code>nplus1 period</code> コマンドで指定した時間内に、コントローラからのハートビートが受信されないと、自動フェイルオーバーが開始される。
“no reload” によるフェイルオーバー	<code>no reload</code> コマンドがフェイルオーバーをトリガする。このようなシナリオでは、マスタを手動で有効にする必要がある。 <code>reload</code> コマンドは、 <code>force</code> オプションに関する通知をスレーブに送信してマスタを有効にし、これによってマスタのステータスがスレーブで無効になる。

N+1 マスタのクラスタではほとんどの場合、AP はすべて L3 接続モードである必要がありますが、マスタとスレーブのユニットが 1 つずつしかない (N=1)、AP は L3 限定の接続モードになります。ただし、AP が L2 モードの場合は、フェイルオーバー後にリブートします。

ハートビートの周期およびハートビートのタイムアウトに関する推奨事項

ネットワーク環境においては、遅延を含むさまざまな要素が N+1 フェイルオーバーに影響することがあります。遅延が大きいネットワークでは、マスタとスレーブのコントロール間でハートビートが失われることで、N+1 フェイルオーバーが引き起こされる場合もあります。このため、ネットワークの遅延が大きい場合は、ハートビートの周期とハートビートのタイムアウトに大きい値を設定することを推奨しています。

デフォルトのハートビートの周期は 1000 ミリ秒、ハートビートのタイムアウトは 4 回です。大きい値を設定するには、以下のコマンドを使用します。

```
# nplus1 timeout 40
```

```
# nplus1 period 100
```

(フェイルオーバー開始までの) 障害検出時間は、ハートビートの周期 x ハートビートのタイムアウトで計算されます。

デフォルトのタイムアウトおよび周期：

- ハートビートの周期 (HP): デフォルトは 1000 ミリ秒、指定可能範囲は 100 ~ 30,000 (ミリ秒)
- ハートビートのタイムアウト (HT): 失われたハートビートのしきい値は、連続ハートビートパケットの数です。デフォルトは 4 タイムアウト、指定可能範囲は 4 ~ 60 (タイムアウト) です。
- 実際の障害検出時間 (AFDT) = HP (1000 ミリ秒) x HT (4) = 4000 ミリ秒 = 4 秒

ネットワークの準備

N+1 クラスタは一連のガイドラインの範囲内で設定し、前項に記載されているとおりに運用する必要があります。N+1 冗長性用にネットワークを設定するときには、次のガイドラインに従います。

- 以下の表は、N+1 クラスタにおいてサポートされているコントローラ モデルのペア (マスタとスレーブ) を示しています。

表 10: アクティブ/パッシブコントローラのペア

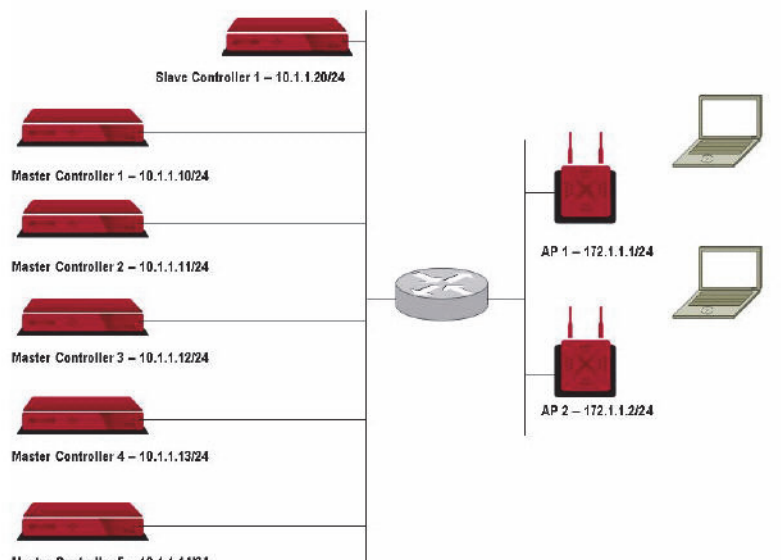
スレーブ ↓	マスタ →							
		1500-VE	1550	1550-VE	3200	3200-VE	4200	4200-VE
1500-VE		○	×	×	×	×	×	×
1550		×	○	×	×	×	×	×
1550-VE		○	○	○	×	×	×	×
3200		×	×	×	○	×	×	×
3200-VE		○	○	○	○	○	×	×
4200		×	×	×	×	×	○	×
4200-VE		○	○	○	○	○	○	○

- すべてのマスタおよびスレーブコントローラは固定 IP アドレスを使用して、N+1 クラスタ設定を一貫性をもって制御できるようにする必要があります。(DHCP アドレスは、N+1 クラスタに参加するコントローラではサポートされません)。
- マスタおよびスレーブコントローラは同じ IP サブネットに存在する必要があります。

- ネットワークにあるすべての AP は、コントローラとの接続でレイヤ 3 を使用するように設定する必要があります。
- スパニング ツリーは、コントローラが接続するスイッチ ポートでは無効にする必要があります。ポートでスパニング ツリーを無効する方法については、スイッチの設定マニュアルを参照してください。
- マスタおよびスレーブ コントローラには同じ日時を設定します。マスタおよびスレーブで日時が一致していないと、フェイルオーバー後の AP アップタイム情報が不正確なものになります。また、マスタで NTP を設定して、不正確な AP アップタイム情報にならないようにすることもできます。

N+1 クラスタの設定では、推奨される N+1 設定を簡略に示したネットワーク図を示します。

図 37: 冗長性ネットワーク デプロイの例



N+1 クラスタの設定

この設定には、CLI のみを使用でき、最大で 5 つのマスタと 1 つのスレーブを設定できます。N+1 設定に関連するコントローラすべてでパスワードが必要になります。N+1 の設定と開始の手順の概要は次のとおりです。

手順	コマンド	説明
1.	nplus1 start master	各マスタで N+1 冗長を開始します。
2.	nplus1 start slave	スレーブ コントローラで N+1 を開始します。
3.	nplus1 add master_hostname master_IP_address	マスタ コントローラのホスト名と IP アドレスをスレーブのクラスタ リストに追加します。

マスタ コントローラでの N+1 の開始

N+1 はまず、マスタ コントローラで開始する必要があります。

マスタ コントローラを設定するには、次の手順を実行します。

1. 各マスタ コントローラで設定モードに入り、N+1 ソフトウェアを開始します。

```
NP-MC4200-master(15)# configure terminal
NP-MC4200-master(15)(config)# nplus1 start master
```

2. 設定モードを終了し、N+1 ソフトウェアがマスタ コントローラで開始したことを確認します。

```
NP-MC4200-master(15)(config)# exit
NP-MC4200-master(15)# sh nplus1
-----
Master controller
Master IP : 172.19.215.31
Master Hostname : NP-MC4200-master
Master Status : Active
Slave IP : 172.19.215.32 <-- スレーブが起動していない場合は表示されません
Slave Status : Passive <-- スレーブが起動していない場合は Unknown と表示されます
-----
```


スレーブコントローラでの N+1 の設定

それぞれのマスタコントローラで N+1 を開始したら、スレーブコントローラでも N+1 を開始し、その後に、各マスタコントローラをスレーブコントローラに追加します。



スレーブコントローラは、N+1 を開始するクラスタの最後のコントローラである必要があります。スレーブコントローラで N+1 を開始する前に、すべてのマスタコントローラをクラスタに追加する必要があります。

スレーブコントローラで N+1 を設定するには、以下の手順を実行します。

1. 設定モードに入り、N+1 ソフトウェアを開始します。

```
NP1-MC4200-slave(15)# configure terminal
NP1-MC4200-slave(15)(config)# nplus1 start slave
Setting up this controller as a Passive Slave controller
```

2. show nplus1 コマンドを使用し、スレーブでソフトウェアが開始したことを確認します (マスタはマスタコントローラリストに表示されないことに注意してください)。

```
NP1-MC4200-slave(15)(config)# show nplus1
Current State : Passive
Heartbeat Period : 1000 milliseconds
Heartbeat Threshold : 4 threshold
Slave IP : 172.19.215.32
Slave Hostname : NP1-MC4200-slave
License Type : Demo
License Usage (Used/Tot) : 0/1
```

Master Controllers

Hostname	IP Address	Admin	Status	Switch	Reason	Missed Adverts	SW Version
----------	------------	-------	--------	--------	--------	----------------	------------

--

3. クラスタにある各マスタコントローラのホスト名と IP アドレスを指定します。この追加操作を完了するためにコントローラのパスワードを入力する必要があります。

```
NP1-MC4200-slave(15)# configure terminal
NP1-MC4200-slave(15)(config)# nplus1 add NP-MC4200-master 172.19.215.31
admin@172.19.215.31 Password:
```

4. 設定モードを終了し、マスタコントローラが有効になっていることをチェックします (Admin ステータスが有効になります)。

```
NP1-MC4200-slave(15)#sh nplus1
```

--

```

Current State : Passive
Heartbeat Period : 1000 milliseconds
Heartbeat Threshold : 4 threshold
Slave IP : 172.19.215.32
Slave Hostname : NP1-MC4200-slave
License Type : Demo
License Usage (Used/Tot) : 1/1

```

```

-----
--
Master Controllers

Hostname  IP Address  Admin  Status Switch  Reason  MissedAdverts  SW Version
-----
NP-MC4200-master 172.19.215.31  Enable  Active  Yes      -      0      6.1-2-15

```

N+1 インストールの監視

show nplus1 コマンドにより、現在のコントローラの設定をチェックし、コントローラのステータスを表示できます。さまざまなコントローラ ステータスで表示される情報を紹介するため、出力表示例をいくつか記載します。

- マスタの N+1 - 基本的なマスタとスレーブの両コントローラの識別情報を表示します。

```

NP-MC4200-master(15)# sh nplus1
-----
Master controller
Master IP : 172.19.215.31
Master Hostname : NP-MC4200-master
Master Status : Active
Slave IP : 172.19.215.32
Slave Status : Passive

```

- スタンバイ スレーブの N+1 - 基本的なスレーブ コントローラの識別情報に加え、クラスタ内のマスタ コントローラのステータスを表示します (以下の表に、ステータス フィールドの説明を記載します)。

```

NP1-MC4200-slave(15)#sh nplus1

```

```

-----
--
Current State : Passive
Heartbeat Period : 1000 milliseconds
Heartbeat Threshold : 4 threshold
Slave IP : 172.19.215.32

```

Slave Hostname : NP1-MC4200-slave
License Type : Demo
License Usage (Used/Tot) : 1/1

--							
Master Controllers							
Hostname	IP Address	Admin	Status	Switch	Reason	MissedAdverts	SW Version

NP-MC4200-master	172.19.215.31	Enable	Active	Yes	-	0	6.1-2-15

次の表で、各表示フィールドについて説明します。

フィールド	説明
Hostname	マスタ コントローラのホスト名。
IP Address	マスタ コントローラに割り当てられている固定 IP アドレス
Admin	マスタにおける N+1 冗長化のステータス <ul style="list-style-type: none">• Enable (有効) - N+1 冗長化がマスタで有効になっています• Disable (無効) - N+1 冗長化が無効になっています
Switch	マスタのアクティブ スレーブを担うスレーブの能力 <ul style="list-style-type: none">• Yes - スレーブおよびマスタ モデル /FortiWLC (SD) のバージョン番号が互換性があります• No - スレーブおよびマスタ モデル /FortiWLC (SD) のバージョン番号に互換性がなく、管理者がマスタで N+1 を無効にしました
Reason	[Switch] が [No] に設定されている場合、スイッチを作成できない理由を説明します。 <ul style="list-style-type: none">• Down: ユーザがマスタを無効にしています• SW Mismatch: FortiWLC (SD) ソフトウェアが同期化されていません (マスタ コントローラをアップデートします)• No Access: 設定のコピーを受け取らなかったため、パッシブ スレーブがマスタにアクセスできませんでした。これは、コントローラを追加した直後に show nplus1 が実行された場合に表示されるメッセージですが、表示されることはほとんどありません。

フィールド	説明
Missed Adverts	連続して欠落した（受信しなかった）アドバタイズの数 ([Switch] フィールドが [Yes] の場合、最大 4 でフェイルオーバーがトリガされます。
SW Version	コントローラの System Director のソフトウェア バージョン。

- アクティブ スレーブの N+1 - マスタ IP アドレス、ホスト名、ステータスが追加されて表示されます。ステータスがパッシブの場合は元のマスタが有効 (UP) であることを示し、ステータスが無効 (Down) の場合は元のマスタにアクセスできないことを示します。

```
NP-MC4200-master(15)# sh nplus1
```

```

-----
      Current State : Active Slave
      Heartbeat Period : 1000 milliseconds
      Heartbeat Threshold : 4 threshold
      Master IP : 172.19.215.31
      Master Hostname : NP-MC4200-master
      Slave IP : 172.19.215.32
      Slave Hostname : NP1-MC4200-slave
      License Type : Demo
      License Usage (Used/Tot) : 1/1
-----

      Master Controllers
      Hostname      IP Address  Admin    Status
-----
      NP-MC4200-master  172.19.215.31  Enable   Passive

```



スレーブの設定コマンドは、スレーブがアクティブである場合は機能しません。

N+1 インストールの管理

N+1 のインストールを管理するためのタスクには、以下があります。

- [実行設定の同期化](#)
- [N+1 マスタ コントローラの無効化と削除](#)
- [N+1 インストールの停止](#)
- [マスタ コントローラの交換](#)
- [N+1 システム ログの操作](#)

実行設定の同期化

マスタとスレーブの実行設定は、30 分ごとに自動的に同期化されます。

N+1 マスタ コントローラの無効化と削除

マスタ コントローラで N+1 操作を無効にしつつクラスタにある設定を保持するには、スレーブ コントローラから、無効にするコントローラの IP アドレスを指定して `nplus1 disable` コマンドを実行します。

```
NP1-MC4200-slave# configure terminal
NP1-MC4200-slave(config)# nplus1 disable 10.1.1.10
NP1-MC4200-slave(config)# end
```

N+1 マスタ コントローラをクラスタから削除するには、スレーブ コントローラから、削除するコントローラの IP アドレスを指定して `nplus1 delete` コマンドを実行します。

```
NP1-MC4200-slave# configure terminal
NP1-MC4200-slave(config)# nplus1 delete 10.1.1.10
NP1-MC4200-slave(config)# end
```

N+1 インストールの停止

N+1 スレーブ コントローラと N+1 マスタ コントローラは、別々に停止する必要があります。

N+1 スレーブ コントローラの停止

スレーブ コントローラで N+1 を停止するには、次のコマンドを使用します。

```
NP1-MC4200-slave# configure terminal
NP1-MC4200-slave(config)# nplus1 stop
Making this a normal controller.
NP1-MC4200-slave(config)# exit
NP1-MC4200-slave#
```

N+1 マスタ コントローラの停止

マスタ コントローラで N+1 を停止するには、次のコマンドを使用します。

```
3000-1# configure terminal
3000-1(config)# nplus1 stop
3000-1(config)# exit
```



以下のコマンドは、アクティブ スレーブ コントローラでは実行できません。これらのコマンドをアクティブ マスタで実行しても、フェイルオーバーはトリガされません。

- poweroff controller
- reload
- reload default
- reload default factory

マスタ コントローラの交換

新しいマスタ コントローラに交換するには、次の手順を実行します。

1. 元のマスタ コントローラの電源をオフにします。スレーブ コントローラがアクティブ コントローラになります。
2. 新しいコントローラに交換します。新しいコントローラのボンディング、インターフェイス モード、IP アドレスの設定が、元のマスタ コントローラと同じであることを確認します。
3. この新しいコントローラをマスタ コントローラにするために、新しいコントローラで "nplus1 start master" コマンドを実行します。
4. スレーブ コントローラを削除するために、新しいマスタ コントローラで "nplus1 slave <スレーブの IP アドレス >" コマンドを実行します。新しいマスタ コントローラがパッシブになります。
5. 新しいパッシブ マスタ コントローラで権限キーを生成するために、アクティブ スレーブ コントローラで "nplus1 access <スレーブの IP アドレス >" コマンドを実行します。
6. そして、アクティブ スレーブ コントローラで "nplus1 revert" コマンドを実行してから、新しいパッシブ マスタ コントローラに最新の実行設定をコピーします。

新しいアクティブ マスタ コントローラは自動的に、最新の実行設定で稼働するようになります。

N+1 システム ログの操作

show nplus1 debugloglevel コマンドは、N+1 ログ メッセージの冗長レベルを表示します。

```
NP1-MC4200-slave# sh nplus1 debugloglevel
nplus1 Debug Logging Level: 0
NP1-MC4200-slave#
```

システム ログのデバッグ レベルの設定

nplus1set debugloglevel コマンドは、N+1 ログ メッセージの冗長レベルを設定します。設定できるレベルの範囲は、0 ～ 3 です。レベル 1 にすると、ログ メッセージが最も簡易になります。デフォルト設定の 0 では、システム ログ メッセージが無効になります。

```
NP1-MC4200-slave(config)# nplus1 setdebugloglevel 1
```

N+1 システム ログ メッセージ

システム ログ メッセージが生成されると、syslog-host コマンドで設定されたシステム ログ サーバのログ ファイルに送信されます。エラー状態が発生すると、これらのメッセージがスタンダアロンの N+1 スレーブ コントローラによって送信されます。サンプルのシステム ログ メッセージは以下のとおりです。

```
Oct 26 14:02:45 slave nplus1_Slave: <エラー メッセージ>
```

システム ログ メッセージのリストを、以下に示します。

エラー メッセージ	説明 / 解決方法
IP address not assigned.Please run setup before using nplus1 (IP アドレスが割り当てられていません。nplus1 を使用する前に setup を実行してください)	nplus1 start slave コマンドが実行されましたが、コントローラの IP アドレスが存在しません。コントローラに対して setup コマンドを実行し、コントローラに固定 IP アドレスを割り当ててください。
ERROR: Could not get software version from file: <i>meru_sw_version_file</i> (エラー: <i>meru_sw_version_file</i> ファイルからソフトウェアバージョンを取得できませんでした)	FortiWLC (SD) ソフトウェアのバージョンを判断できませんでした。
Rejecting record number due to parsing issues (構文解析の問題により、レコード number を却下します)	設定されているマスタの永続レコードの読み取りエラー。マスタ コントローラを手動で再度追加してください。
Could not open socket for CLI server (CLI サーバのソケットを開けませんでした)	N+1 CLI の初期化に問題があります。

CLI server: Bind error for server ip: ip port: port (CLI サーバ : サーバ IP: <IP アドレス> ポー ト : <ポート番号> のバインド エラー)	N+1 CLI の初期化に問題があります。
ALERT: Software Mismatch: Master (master_ip): software_version Slave (slave_ip): software_version (ア ラート : ソフトウェアの不一 致 : マスタ (master_ip): software_version スレーブ (slave_ip): software_version)	マスタ コントローラのアドバタイズメントにより、ソフ トウェアの不一致が明確になりました。バージョン不一致 が発生していると、マスタ コントローラが冗長性を提供 できません。マスタ コントローラにスレーブ コントロー ラと同じバージョンのソフトウェアをインストールしてく ださい (または、スレーブ コントローラにマスタ コント ローラと同じバージョンのソフトウェアをインストールし てください)。
Copyback failed for master controller: master_ip (マスタ コ ントローラ master_ip のコピー バックが失敗しました)	スレーブがアクティブである状態でマスタ コントローラ の設定が変更され、コピーバックが失敗しました。マスタ コントローラに加えた新たな設定変更を削除してからマスタ コントローラをフェイルバックし、その後、必要な設定 変更を加えます。
For MC: master_ip State: SW Mismatch -> No Access - Saved Config does not exist (MC について : master_ip 状態 : SW 不一致 -> アクセスなし - 保 存された設定が存在しません)	ソフトウェアの不一致は解決されましたが、スレーブ コ ントローラからマスタ コントローラにアクセスできず、 冗長性を実現できません。nplus1 access master_ip コマ ンドを使用して、マスタ コントローラにアクセスできる ようにしてください。
Could not access host: master_ip.Setting No Access Count to: count (ホスト : master_ip にアクセスできませ ん。No Access Count を count に設定します)	マスタ コントローラにアクセスできませんでした。マスタ コントローラがアクセス可能になるまで、冗長性を実 現できません。count (デフォルトは 60 秒) 経過後にアク セスが再チェックされます。ゲートウェイ障害が原因であ る可能性があります。マスタ コントローラにアクセスで きるようにし、nplus1 access master_ip コマンドを使用 して確認します。

アップグレード

N+1 ネットワーク内のコントローラは、スタンドアロン環境のコントローラと同じようにアップグレードできます。ただし、アップグレードできるのは、アクティブ マスタとスタンバイ スレーブ コントローラだけです。フェイルオーバー モードのコントローラはアップグレードできません。

N+1 フェイルオーバーからのリカバリ

N+1 のマスタ コントローラがダウンすると、スレーブ コントローラがパッシブ スレーブからアクティブ スレーブへと移行 (フェイルオーバー) し、マスタ コントローラとしての動作を開始します。当初のマスタが復帰しても、アクティブ スレーブはアクティブ スレーブを継続し、復帰した当初のマスタはパッシブ マスタになります。AP (L2 モードの場合) はリブートします。

デュアル イーサネット フェイルオーバーによる N+1 からのリカバリ

マスタ コントローラで、1 つ目のイーサネット インターフェイスがダウンすると、コントローラは、同じコントローラの 2 つ目のインターフェイスにフェイルオーバーします。2 つ目のインターフェイスがダウンすると、Nplus1 フェイルオーバーが実行され、デュアル イーサネット冗長構成によって、N+1 パッシブ スレーブがアクティブ スレーブになります。

この段階で、アクティブ スレーブが制御下に置かれ、1 つ目のアクティブ スレーブ イーサネット インターフェイスがダウンすると、スレーブ コントローラが 2 つ目のイーサネット インターフェイスにフェイルオーバーします。

フェイルオーバーを復帰させるには、スレーブ コントローラの最初のインターフェイスが動作中であることを確認します。そして、当初のマスタ コントローラの 1 つ目のインターフェイスをアップします。N+1 アクティブ スレーブはアクティブ スレーブを継続し、当初の N+1 マスタがパッシブになります。

オプション 43

オプション 43 は、フォーティネット製品に含まれるものではなく、コントローラをマッピングする 1 つの方法です。DHCP オプション 43 を使用すると、AP のプライマリとバックアップのコントローラを指定できます。この設定では、バックアップ コントローラのサブネットワークをプライマリ コントローラとは異なるものに指定できます。オプション 43 では、AP に関連付けるコントローラ (プライマリとセカンダリ) を指定することで、冗長性を実装します。この機能は、すべてのアクセス ポイントでサポートされています。バックアップ コントローラは、DHCP または DNS のいずれかを使用して設定できます。

たとえば、オプション 43 を使用し、"wlan-controller" が P1 にマッピングされていて (P1 は P2 にリダイレクトされていて)、"wlan-controller-2" が S1 にマッピングされている (S1 は S2 にリダイレクトされている) 場合には、P1、P2、S1、S2 の順番に検出されます。コントローラで、DNS エントリとオプション 43 の両方が有効になっていると、AP は最初に、AP に設定されているホスト アドレスを使用します (デフォルト値 = wlan-controller)。ホスト アドレ

スが 0.0.0.0 に設定されている場合や、ホストが名前とその名前を DNS を使用して解決できない場合のみ、AP は DHCP オプション 43 の値を使用します。

オプション 43 の設定の具体的な方法については、サポート ポータルの How-To 4062-125 を参照してください。

DHCP オプション 43 を使用した AP 対応冗長

- L3 優先、コントローラ名 0.0.0.0 として AP を設定します。
- DHCP サーバで、オプション 43 の値を、プライマリとセカンダリのコントローラの IP やホスト名を使用して設定する必要があります。こうすることで、AP は、IP アドレスを取得するために DHCP サーバに接触した際に、DHCP サーバから、オプション 43 を使用して、プライマリとセカンダリのコントローラの IP 情報も取得します。

DNS を使用した AP 対応冗長

- AP を、L3 優先で、コントローラ名をコントローラのホスト名として設定します。
- DNS エントリを設定して、DNS サーバのプライマリ ホスト名を解決するようにします。
DNS エントリを設定して、DNS サーバのセカンダリ ホスト名を解決するようにします。
- AP のプライマリ コントローラのホスト名を、L3 優先モードで設定します。

8 ネットワーク インターフェイスの設定

setup プログラムを使用してコントローラをセットアップする場合に最初に実行すべき手順の 1 つは、『*FortiWLC (SD) 入門ガイド*』に説明したとおり、ネットワーキング パラメータを設定することでした。setup プログラムを実行しなかった場合や、setup スクリプトで設定した内容を変更する場合は、「[インターフェイスの基本的なネットワーク設定](#)」に記載されているコマンドを使用できます。

コントローラには 2 つの FastEthernet ポートが存在するため、2 つ目のポートを追加処理用に設定できます。2 つ目のポートは、冗長インターフェイスまたは 2 つ目のアクティブ FastEthernet インターフェイスとして使用できます。デュアル イーサネット機能を設定する際は、「[デュアル イーサネットの操作](#)」を参照してください。このような変更の後には、コントローラをリブートする必要があります。

インターフェイスの基本的なネットワーク設定

ネットワーク パラメータの設定には、必要に応じて以下のコマンドを使用します。

- FastEthernet ポートのパラメータを変更するには、interface FastEthernet コマンドを使用します。
- DHCP リレー サーバを使用してワイヤレス クライアントの動的 IP アドレス割り当てを設定するには、ip dhcp-server ip-address コマンドを使用します。
- コントローラの IP アドレスを設定するには、ip address ip-address netmask コマンドを使用します。
- デフォルト ゲートウェイを設定するには、ip default-gateway ip-address コマンドを使用します。
- ドメイン名を設定するには、ip domainname name コマンドを使用します。
- DNS ネーム サーバを追加するには、ip dns-server ip-address コマンドを使用します。

ネットワーク情報の設定に関する詳細については、『*FortiWLC (SD) 入門ガイド*』を参照してください。ここに記載されているコマンドに関する詳細については、『*FortiWLC (SD) コマンドリファレンス*』を参照してください。

802.11d のサポート

当初の 802.11 標準では、少数の規制ドメイン (国) のみでの処理が定義されていました。802.11d では、ビーコンで国コードをアドバタイズすることで、それ以外の多くの国でも 802.11 WLAN 機器を運用できるようになりました。デバイスが国コードを取り出して、それに従って通信を調整します。この機能を設定したり有効にしたりする必要はありません。フォーティネットの実装は現在、セットアップに表示されるすべての国で自動的に動作します。この機能を表示する show コマンドはありません。802.11 ビーコンの 802.11d、プローブ応答、国コード IE フィールドを検証します。

デュアル イーサネットの操作

デュアル イーサネットのサポートにより、コントローラの 2 つ目のイーサネット ポートが有効になり、冗長インターフェイスまたは第 2 アクティブ インターフェイスのいずれかとして動作させることができます。

第 2 インターフェイスが冗長として設定されると、スパンニング ツリー設定において第 1 インターフェイスのバックアップ インターフェイスとして動作します。この設定では、第 1 インターフェイスが稼働している場合には、第 2 インターフェイスはアイドル状態となり、第 1 インターフェイスに障害が発生すると、そのすべての機能を代行します。冗長設定では、第 1 インターフェイスは固定または DHCP の IP アドレスのいずれかです。

第 2 インターフェイスが active として設定される場合、その他の設定をサポート可能な別のインターフェイスとして設定できます (たとえば、第 1 インターフェイスを VLAN に設定しながら、GRE トンネルをサポートできます)。



第 1 イーサネット インターフェイスがデフォルト インターフェイスとして扱われます。デフォルトのインターフェイスの役割は、AP とコントローラ間でワイヤレス トンネル トラフィックを渡すことです。GRE と VLAN の一般的なサポートに加え、デフォルトのインターフェイスは、コントローラの管理インターフェイスにもなり、SSH および HTTPS を介した管理アクセス トラフィックをサポートします。

冗長モードの設定では、第 2 インターフェイスをデフォルトのイーサネット インターフェイスと同じ機能を実行可能なスイッチ ポートに接続することが必要となります。

冗長からデュアル アクティブ処理へと変更するには、コントローラのリブートが必要です。

デュアル イーサネットの設定

第 2 イーサネット インターフェイスは、冗長またはアクティブのいずれかとして設定できます。アクティブ インターフェイスは、VLAN または GRE (Generic Routing Encapsulation) ト

ンネルをサポートするために使用できます。冗長インターフェイスは、プライマリ インターフェイスに障害が発生した場合のバックアップ インターフェイスです。



アクティブまたは冗長として設定されるまで、イーサネット ケーブルを第 2 イーサネット ポートに差し込まないでください。

冗長インターフェイスの設定

「[冗長性の実装](#)」の章を参照してください。

アクティブ インターフェイスの設定

次のコマンドでは、VLAN または GRE (Generic Routing Encapsulation) トンネルをサポートするために使用可能なアクティブ (active) インターフェイスとしてイーサネット ポート 2 が設定されています。ip address は VLAN または GRE ローカル エンドポイントの IP アドレスと関連するネットマスクを指定します。gw コマンドは、ゲートウェイ アドレスを指定し、必須フィールドです。

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# ip address 172.26.16.200 255.0.0.0
default(config-if-FastEth)# gw 172.26.16.1
default(config-if-FastEth)# type active
default(config-if-FastEth)# exit
default(config)# exit
```



冗長からデュアル アクティブ処理へと変更するには、コントローラのリブートが必要です。

上記のインターフェイス設定が完了した後に、GRE トンネルを設定する場合は、セキュリティの章の「[GRE トンネルの設定](#)」を参照してください。

FastEthernet インターフェイス情報の表示

FastEthernet インターフェイス 1 の設定を表示するには、show interfaces FastEthernet controller コマンドまたは show interfaces FastEthernet ap コマンドを使用して、各インターフェイスのタイプの関連情報を表示します。

FastEthernet インターフェイス 2 の冗長設定を表示するには、show second_interface_status コマンドを使用します。

インターフェイスおよびネットワーキング コマンド

次のインターフェイスおよびネットワーキング設定コマンドを利用できます。

表 11: インターフェイスおよびネットワーキング コマンド

コマンド	目的
controller(config)# interface FastEthernet controller interface-index	コントローラ インターフェイスのインデックス (0 ~ 31) を指定し、FastEthernet インターフェイス設定サブモードに入ります。
controller(config)# ip address ip-address mask	コントローラの IP アドレスとサブネット マスクを指定します。DHCP を有効にしない場合は、このコマンドを使用して固定 IP アドレスを指定します。
controller(config)# gw ip-address	デフォルト ゲートウェイの IP アドレスを指定します。DHCP を使用しない場合は、このコマンドを使用してゲートウェイを指定します。
controller# setup	ホスト名およびその他のシステム パラメータやネットワーク設定パラメータをセットアップするために利用できる、会話型のスクリプトです。
controller# show interfaces FastEthernet statistics	コントローラと AP のイーサネット統計のサマリを表示します。
controller# show interfaces FastEthernet statistics controller	コントローラのイーサネット統計を表示します。
controller# show interfaces FastEthernet statistics ap id	指定したノード ID の AP のイーサネット統計を表示します。
controller# show second_interface_status	冗長モードで設定されている第 2 FastEthernet インターフェイスのステータスを表示します。

ポート プロファイルの設定

ポート プロファイル設定画面では、デプロイしたデバイスのプライマリ以外のイーサネットポートに適用するカスタム イーサネット プロファイルを作成できます。一部の AP モデルは、複数のイーサネット ポートを実装しており、そのうちの 1 つを常にワイヤレス サービスに使用し、残りを、ポート プロファイルを適用して設定できます。この機能が必要なければ、ポート プロファイル機能でポートを無効にすることもできます。

プライマリ以外のポートに（直接、またはポートに接続されたスイッチ経由で）接続されている各デバイスは、コントローラの Web UI ([Monitor] > [Devices] > [All Stations]) で、有線ステーションとして監視できます。インターフェイスがトンネル処理用に設定されていて、接続されているデバイスが SIP を利用する VoIP フォンである場合、その VoIP は、コントローラの電話データベースに SIP フォンとして記録されます。有線インターフェイスあたりのサポートされている有線ステーションの最大数は 128 です。

ポート プロファイルの設定と適用の手順については、以下の項を参照してください。

ポート プロファイルの作成

デフォルトでは、default ポート プロファイルがコントローラ インターフェイスに設定されます。既存のポート プロファイルを表示するには、Web UI を開き、[Configuration] > [Wired] > [Port] に移動します。図 38 を参照してください。

図 38: ポート テーブル

Port Table (1 entry)

<input type="checkbox"/>	Port Profile Name	Enable/Disable	Dataplane Mode	VLAN Name	Allow Multicast Flag	IPv6 Bridging
<input checked="" type="checkbox"/>	default	Disable	Tunneled		Off	Off

ポート プロファイルの一部として、いくつかのオプションを設定できます。

Port Table - Add ?

Port Profile Name *	<input type="text"/>	Enter 1-32 chars.
Enable/Disable	<input type="button" value="Disable"/> ▼	
VlanTrunk	<input type="button" value="Disable"/> ▼	
Dataplane Mode	<input type="button" value="Tunneled"/> ▼	
VLAN Name	<input type="button" value="No VLAN"/> ▼	
AP VLAN Policy	<input type="button" value="No VLAN"/> ▼	
AP VLAN Tag	<input type="text" value="0"/>	Valid range: [0-4094]
Security Profile Name	<input type="button" value="No Security Profile"/> ▼	
Primary RADIUS Accounting Server	<input type="button" value="No RADIUS"/> ▼	
Secondary RADIUS Accounting Server	<input type="button" value="No RADIUS"/> ▼	
Reconnect Primary Server (minutes)	<input type="text" value="10"/>	Valid range: [5-60]
Accounting Interim Interval (seconds)	<input type="text" value="3600"/>	Valid range: [600-36000]
Allow Multicast Flag	<input type="button" value="Off"/> ▼	
IPv6 Bridging	<input type="button" value="Off"/> ▼	
IP Prefix Validation	<input type="button" value="Off"/> ▼	

下表で、表示される各フィールドについて説明します。

表 12: ポート プロファイル オプション

フィールド	説明
Port Profile Name	プロファイル作成でポート プロファイルに指定した名前
Enable/Disable	現在、プロファイルの使用が有効になっているかどうかが表示されます。
Dataplane Mode	トンネルまたはブリッジのいずれかの構成にプロファイルを設定できます。
AP VLAN Tag	このフィールドは、プロファイルがブリッジ モードで動作する場合にのみ設定されます。VLAN タグは 0 ～ 4094 の整数で、AP が存在する VLAN を識別します。
VLAN Name	このフィールドは、プロファイルがトンネル モードで動作する場合にのみ使用されます。プロファイルを設定する VLAN を指定できます。
Allow Multicast Flag	このオプションでは、使用中のポート経由でのマルチキャスト転送を許可するかどうかを指定できます。
IPv6 Bridging	IPv6 デバイスのブリッジが On または Off のどちらであるかを指定します。

必要であれば、テーブルの隣にあるボックスをチェックして [Settings] をクリックすると、default プロファイルを変更できます。新しいプロファイルを追加するには、次の手順を実行します。

1. Web UI から、[Configuration] > [Wired] > [Port] に移動します。
2. [Add] をクリックします。画面が更新され、[Port Table - Add] ページが表示されます。
3. 希望するとおりに、プロファイルを設定します。設定オプションの説明については、[表 12](#) を参照してください。
4. 設定が完了したら、[OK] をクリックして新しいプロファイルを保存します。

プロファイルが作成されたら、ネットワーク デバイスの任意のポートにそのプロファイルを適用できます。手順については、以下の項を参照してください。

特定のイーサネット ポートのポート プロファイルの有効化

いずれかのイーサネット ポートにポート プロファイルを指定するには、[Port Profile Table] から該当するプロファイルを選択し、[Configuration] をクリックして、ポート AP テーブルにアクセスする必要があります。[Port AP Table] は、表示される画面の 2 つ目のタブです。

デフォルトでは、このポート AP テーブルは空白であり、必要なポートを手動で追加できません。ポートをプロファイルに追加するには、次の手順を実行します。

1. [Port AP Table] 画面で、[Add] をクリックします。このテーブルでは、ポート プロファイルが適用する AP とインターフェイス ID を選択できます。
2. ドロップダウン リストを使用して、AP とイーサネット ID を選択します。指定したイーサネット インターフェイス インデックスがアップリンク インターフェイスであると (すなわち、そのインターフェイスがネットワークへのプライマリ接続であると)、ポート プロファイルには設定できず、エラー メッセージが表示されます。
3. [OK] をクリックして、変更を保存します。

設定する各プロファイルに対して、これらの手順を繰り返します。

802.1x 認証の有効化

有線クライアントは、AP の有線インターフェイスに直接接続することも、L2 スイッチ経由で接続することもできます。複数の有線クライアントに使用する L2 スイッチの配備では、L2 スイッチを 802.1x パケットをパスする一層のように設定する必要があります。

有線クライアントの 802.1x 認証を有効にするには、次の手順を実行します。

1. RADIUS プロファイルとセキュリティ プロファイルを (Clear Encryption モードで 802.1x L2 認証メカニズムを使用して) 作成します。
2. セキュリティ プロファイルを対応するポート プロファイル設定に割り当てます。

CLI による有効化

RADIUS プロファイルの作成

```
default(15)(config)#
default(15)(config)# radius-profile dot1xport
default(15)(config-radius)# ip-address 10.10.10.10
default(15)(config-radius)# key meru2002
default(15)(config-radius)# port 1812
default(15)(config-radius)# exit
```

セキュリティ プロファイルの作成

```
default(15)# configure terminal
default(15)(config)# security-profile dotxportauth
default(15)(config-security)# allowed-l2-modes 802.1x
```

```
default(15)(config-security)# encryption-modes clear
default(15)(config-security)# radius-server primary dot1xport
default(15)(config-security)# exit
```

ポート プロファイルの作成

```
default(15)# configure terminal
default(15)(config)# port-profile dot1xauth
default(15)(config-port-profile)# enable
default(15)(config-port-profile)# dataplane tunnelled
default(15)(config-port-profile)# security-profile dot1xportauth
default(15)(config-port-profile)# exit
default(15)#
```

Web UI による有効化

RADIUS プロファイルの作成

RADIUS Profile Name	<input type="text" value="dot1xport"/>	Enter 1-16 chars.,
Description	<input type="text" value="Dot1x Auth on Port"/>	Enter 0-128 chars
RADIUS IP	<input type="text" value="172"/> . <input type="text" value="18"/> . <input type="text" value="1"/> . <input type="text" value="7"/>	
RADIUS Secret	<input type="password" value="....."/>	
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	
Called-Station-ID Type	<input type="text" value="Default"/>	
CCA	<input type="text" value="On"/>	

セキュリティ プロファイルの作成

Security Profile Name: dot1xportauth Enter 1-32 chars., F

L2 Modes Allowed: ☐ Clear ☒ 802.1x ☐ Static
☐ WPA2 ☐ WPA2 PSK ☐ MIXE
☐ MIXED_PSK ☐ WAI ☐ WAI f

Data Encrypt: ☐ WEP64 ☐ WEP128 ☐ CCM
☐ CCMP/TKIP ☐ WPI-SMS4 ☒ Clear

Primary RADIUS Profile Name: dot1xport ▼
No RADIUS
dot1xport

Secondary RADIUS Profile Name:
WEP Key (Alphanumeric/Hexadecimal)

ポート プロファイルの作成

Port Profile Name: dot1xauth Enter 1-32 chars., F

Enable/Disable: Disable ▼

Dataplane Mode: Tunneled ▼

VLAN Name: No VLAN ▼

Security Profile Name: No Security Profile ▼
No Security Profile
default
Secured
dot1xportauth
No RADIUS

Primary RADIUS Accounting Server:
Secondary RADIUS Accounting Server:
Accounting Interim Interval (seconds):

リンク アグリゲーション

リンク アグリゲーションによって、AP の両方のポートでデータ トラフィックが可能になり、結果として、スループットと冗長性が向上します。AP の第 2 インターフェイスにのみ、LACP を設定できます。LACP を AP の第 2 インターフェイスに構成する前に、AP をターミネートするスイッチでボンディングを有効にします。リンク アグリゲーションが設定されていると、AP の第 2 インターフェイスは第 1 インターフェイスのすべてのプロパティを継承します。有効にすると、両方のポートで LACP が動作します。

AP の第 2 インターフェイスは、デフォルトでは無効であり、有効になっている場合は、第 1 インターフェイスにボンディングされたペアとして動作します。第 2 インターフェイスをスタンドアロン モードで使用することはできません。ただし、LACP が有効になっている場合にどちらかのインターフェイスで障害が発生すると、第 2 インターフェイスが処理を引き継

いでトラフィックを渡します。フェイルオーバー時は、外部電源が供給されないか、PoE 経由だけでスイッチに給電される場合のみ、第 2 インターフェイスが動作します。



リンク アグリゲーションは、APAP832、AP822、FAP-U421、および FAP-U423 でのみ利用できます。AP をターミネートするスイッチが LACP をサポートしていないと、AP は非 LACP モードにフォールバックし、1つのインターフェイスだけがデータトラフィックを処理します。固定ボンディングはサポートしていません。

事前設定

LACP を AP で有効にする前に、以下の手順を必ず実行します。

- ポート AP エントリをその AP のポート プロファイルから削除する。
- AP をターミネートするスイッチのポートで LACP サポートを有効にする。
- AP には LACP をサポートする 802.3at 電力が必要である。

注：スイッチが LACP をサポートしていないと、AP は非 LACP モードで動作します。

CLI による LACP の有効化

AP のイーサネット インターフェイスで `lACP enable` コマンドを使用して、LACP を有効にします。

```
controller(15)# config terminal
controller(15)(config)# interface ap 108 2
controller(15)(config-if-WiredEth)# lACP enable
```

LACP ステータスの確認

`show interfaces ap <ap-id>` コマンドの Uplink Type and LACP カラムに、AP の LACP のステータスが表示されます。

```
Controller(15)# show interfaces Ethernet ap 108
```

Type	ID	Name	IfIndex	MTU	MAC Address	Admin	State	Op
State	Last	Change	Uplink	Type	LACP			
ap	108	AP-108	1	1500	00:0c:e6:13:01:a9		Up	
Disabled	05/19/2014	20:05:12	Uplink		disable			
ap	108	AP-108	2	1500	00:0c:e6:13:01:a9		Up	
Disabled	05/20/2014	23:51:48	Uplink-lACP		enable			

Ethernet Table(2 entries)

さらに診断が必要な場合は、show interfaces Ethernet statistics <ap-ID> コマンドを使用して、AP インターフェイスの Tx エラーと Rx エラーを確認できます。

```
Controller(15)# show interfaces Ethernet statistics ap 13
```

IfIndex Octets	Node ID Out Errors	Node Name	Type	In Octets	In Errors	Out
1 0	13	AP-13	ap	78217745	0	4637677
2 0	13	AP-13	ap	0	0	0
LACP 0	13	AP-13	ap	78217745	0	4638109

Ethernet Statistics(3 entries)

Web UI による LACP の有効化

1. [Configuration] > [Devices] > [AP] に移動して、AP を選択します。
2. [Ethernet Interface] タブに移動して第 2 イーサネット インターフェイスを選択し、[LACP] を [Enable] に設定します。

複数の AP の LACP をまとめて有効にするには、次の手順を実行します。

1. [Configuration] > [Wired] > [Ethernet] に移動し、すべての AP を選択して [Bulk Update] ボタンをクリックします。
2. [LACP] を [Enable] を設定します。



LACP の一括更新は、Web UI からのみ実行できます。

管理インターフェイスの設定

[Management Interfaces] テーブル ([Configuration] > [Devices] > [System Settings] > [Management Interfaces]) では、コントローラからワイヤレス ネットワークへのトラフィックの送信方法を制御できます。テーブル内のそれぞれのタブについては、以下の項を参照してください。

Physical Interfaces

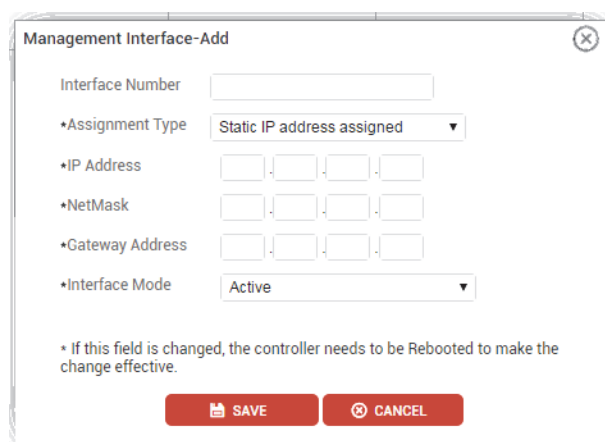
Physical Interfaces テーブルでは、コントローラの物理イーサネット ポートの IP 情報を設定します。設定できるポートの数は、購入したコントローラのモデルによって異なります。

物理インターフェイスの追加

新しい物理インターフェイスを設定するには、以下の手順を実行します。

1. Physical Interfaces テーブルで、[Add] をクリックします。[Management Interface-Add] ウィンドウが表示されます。

図 39: 物理インターフェイスの追加

A screenshot of the 'Management Interface-Add' dialog box. It contains the following fields: 'Interface Number' (text input), 'Assignment Type' (dropdown menu with 'Static IP address assigned' selected), 'IP Address' (four separate text input boxes for octets), 'NetMask' (four separate text input boxes for octets), 'Gateway Address' (four separate text input boxes for octets), and 'Interface Mode' (dropdown menu with 'Active' selected). At the bottom, there is a note: '* If this field is changed, the controller needs to be Rebooted to make the change effective.' and two buttons: 'SAVE' and 'CANCEL'.

2. 下表に記載する方法で必要なデータに追加します。

フィールド	説明
Interface Number	必要とするインターフェイスの数。
Assignment Type	インターフェイスが固定または動的のどちらの IP アドレスを使用するかを指定します。
IP Address	固定 IP を使用する場合、インターフェイスが使用する IP アドレスを入力します。
NetMask	固定 IP を使用する場合、インターフェイスのネットマスクを入力します。

フィールド	説明
Gateway Address	固定 IP を使用する場合、インターフェイスのゲートウェイ アドレスを入力します。
Interface Mode	インターフェイスがアクティブ冗長になるかどうかを指定します。

3. [Save] をクリックして、インターフェイスを保存します。変更を適用するには、コントローラをリブートする必要があります。

VLAN Interfaces

VLAN Interfaces では、ネットワークで管理トラフィック専用で使用する VLAN を指定できます。管理トラフィックには、以下が含まれます。

- コントローラと AP、またはコントローラからコントローラへの通信
- Web UI または CLI へのアクセス
- SNMP トラフィック
- ネットワーク管理サーバおよび追加した任意のフォーティネット アプリケーション (SAM、Spectrum Manager など) への通信
- Syslog メッセージ
- 認証サーバ トラフィック (RADIUS、TACACS+ など)
- NTP 通信

この機能を使用すると、ユーザは、管理トラフィックをネットワークの他のトラフィックから分離し、専用の所定のデバイスにルーティングできます。本項の以下に記載する手順に従って、VLAN インターフェイスを作成します。

管理 VLAN インターフェイスの追加

1. VLAN Interfaces テーブルで、[Add] をクリックします。[Management Interface-Add] ウィンドウが表示されます。

図 40: VLAN インターフェイスの追加

Management Interface-Add

VLAN Name

Interface Number

1

Tag

IP Address

NetMask

Default Gateway

Assignment Type

Static IP address assigned

Interface Mode

Active

Save

Cancel

2. 下表に記載する方法で必要なデータを追加します。

フィールド	説明
VLAN Name	VLAN の名前を入力します。
Interface Number	使用する物理インターフェイス数を入力します。 注：管理 VLAN はインターフェイス番号 1 を使用する必要があるため、このフィールドは変更できません。
Tag	VLAN のタグを入力します。
IP Address	VLAN が使用する IP アドレスを入力します。
NetMask	VLAN のネットマスクを入力します。
Default Gateway	VLAN が使用するゲートウェイを入力します。
Assignment Type	管理 VLAN は固定 IP アドレスにのみ実装できるため、このフィールドは変更できません。
Interface Mode	管理 VLAN はアクティブ インターフェイスでのみ動作できるため、このフィールドは変更できません。

3. [Save] をクリックして、VLAN を保存します。新しい VLAN が VLAN Interfaces テーブルに表示されます。

固定ルートの使用

固定ルートを使用すると、設定されたサブネットへのアクセスを許可するアダプタをシステム管理者が手動で定義できます。これは、必要なルートが少ない小規模の環境や、特定のサブネットをお互いに分離する必要がある大規模の環境で使用されるものです。固定ルーティングには、(ネットワーク ルータがパケットの最良の配信パスを自動的に決定する) 動的ルートのような処理能力が必要でないというメリットもあります。

固定ルート テーブルを表示するには、Web UI にアクセスし、[Configuration] > [Devices] > [System Settings] > [Management Interfaces] > [Static Route] に移動します。

図 41: 固定ルート テーブル

Physical Interfaces		VLAN Interfaces		Static Route		
<input type="checkbox"/>	Static Route Name	IP Address/Subnet	Subnet Mask	FastEthernet	Interface Name	Default Gateway
	<input type="text"/>	<input type="text"/>	<input type="text"/>	ALL <input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>



少なくとも 1 つのルートが作成されるまで、このテーブルは空白です。

固定ルートの追加

新しい固定ルートを作成するには、固定ルート テーブルにアクセスし、[Add] をクリックします。[Static Route Configuration - Add] 画面が表示されます。

図 42: 固定ルートの作成

Static Route-Add

Static Route Name

IP Address/Subnet

Subnet Mask

Interface Name

Primary fastEthernet

Save

Cancel

下表に記載する方法で、必要な詳細情報を指定します。

表 13: 固定ルートのフィールド

フィールド	説明
Static Route Name	ルートを説明する名前を入力します。1 ～ 16 文字の長さで指定します。
IP Address/Subnet	ルートがアクセスを提供するサブネットを入力します。上記のように、一般的には xxx.xxx.xxx.0 の形式で指定します。
Subnet Mask	ルートのサブネット マスクを入力します。上記のように、一般的には 255.255.255.0 の形式で指定します。
FastEthernet	このドロップダウンを使用して、イーサネット アダプタが使用するルートを指定します。指定したアダプタは、設定されたサブネットにアクセスできるようになります。
Interface Name	ルートに使用するインターフェイスの名前。
Default Gateway	ルートのデフォルト ゲートウェイ。

フィールドに入力したら、[OK] をクリックしてルートを保存します。設定する各ルートについて、このプロセスを繰り返します。

仮想インターフェイス

L3 ルーティング モードで動作する場合、仮想インターフェイスを、デバイスの標準物理インターフェイスとほとんど同じ方法で動作するように設定できます。IP (または IP の範囲)、サブネット、およびゲートウェイを割り当てることができ、固有のプライベート IP 範囲にクライアントを分離するために使用できます。仮想インターフェイスを作成したら、クライアントの処理に使用するように、DHCP スコープ ([「コントローラベースの DHCP サーバの設定」](#)を参照) と ESS にマッピングできます。

仮想インターフェイス テーブルを参照するには、Web UI にアクセスし、[Configuration] > [Wired] > [Virtual Interface] に移動します。少なくとも 1 つのルートが作成されるまで、このテーブルは空白です。

仮想インターフェイスの追加

新しい仮想インターフェイスを作成するには、仮想インターフェイス テーブルにアクセスし、[Add] をクリックします。[Virtual Interface - Add] ウィンドウが表示されます。[図 43](#) を参照してください。

図 43: 仮想インターフェイスの作成

Virtual Interface - Add

Virtual Interface Profile Name

virt-int

Enter 1-32 chars., Required

Enable/Disable

Enable

Subnet IP Address

192

168

14

0

Subnet Mask

255

255

255

0

Gateway IP Address

192

168

14

1

下表に記載する方法で、必要な詳細情報を指定します。

表 14: 仮想インターフェイスのフィールド

フィールド	説明
Virtual Interface Profile Name	インターフェイスを説明する名前を入力します。1 ～ 32 文字の長さで指定します。
Enable/Disable	このドロップダウンを使用して、仮想インターフェイスを有効または無効にします。
Subnet IP Address	インターフェイスが使用するサブネットを入力します。上記のように、一般的には xxx.xxx.xxx.0 の形式で指定します。
Subnet Mask	インターフェイスのサブネット マスクを入力します。上記のように、一般的には 255.255.255.0 の形式で指定します。
Gateway IP Address	選択したサブネットのゲートウェイの IP アドレスを指定します。上記のように、一般的には xxx.xxx.xxx.1 の形式で指定します。

フィールドに入力したら、[OK] をクリックしてインターフェイスを保存します。設定する各インターフェイスについて、このプロセスを繰り返します。インターフェイスが作成されたら、DHCP スコープに割り当てることができます。詳しい手順については、「[コントローラベースの DHCP サーバの設定](#)」を参照してください。

9 セキュリティの設定

FortiWLC (SD) は、業界標準のセキュリティ オプションを提供しています。ESSID (および、設定されていれば、VLAN) の要件に従ってこれらの一連のオプションを設定することで、サイトのワイヤレス LAN と有線 LAN のインフラストラクチャを保護できます。

- [ワイヤレス LAN セキュリティの設定 \(223 ページ\)](#)
- [Web UI によるセキュリティ プロファイルの設定 \(224 ページ\)](#)
- [暗号化サポート \(229 ページ\)](#)
- [GRE トンネルの設定 \(231 ページ\)](#)
- [CLI によるセキュリティ プロファイルの設定 \(234 ページ\)](#)
- [Policy Enforcement Module \(ポリシー適用モジュール\) \(243 ページ\)](#)
- [RSA SecurID による認証 \(245 ページ\)](#)
- [MAC フィルタリングの設定 \(246 ページ\)](#)
- [セキュリティ証明書 \(253 ページ\)](#)
- [WAPI サーバの設定 \(262 ページ\)](#)
- [VPN 接続の設定 \(262 ページ\)](#)

セキュリティ関連の章、「[認証](#)」、「[キャプティブ ポータル](#)」、および「[不正 AP の検出と緩和](#)」も参照してください。

ワイヤレス LAN セキュリティの設定

ワイヤレス LAN システムにおいては、セキュリティ ポリシーを作成し、そのセキュリティ ポリシーを ESSID に割り当てると、レイヤ 2 とレイヤ 3 のセキュリティ オプションが適用されます。このように、セキュリティ ポリシーは、ESSID が提供するサービスと構造 (仮想ポート、仮想セルなど) に合わせてカスタマイズでき、関連付けられている AP に簡単に伝播できます。コントローラのセキュリティ プロファイルは、E(z)RF Network Manager から設定できます。読み取り専用のフィールド [Owner] を確認して、プロファイルが設定された場所を確認できます。[Owner] は、[E(z)RF] または [controller] のいずれかになります。一般的なセキュリティ設定作業は、以下のとおりです。

1. 各 SSID 内のクライアント トラフィックのセキュリティを維持し、他の SSID 内のクライアントから分離するために、VLAN を作成します。操作については、「[VLAN の設定](#)」の章を参照してください。
2. 認証サーバまたは RADIUS サーバを設定します (手順については、RADIUS サーバのドキュメントを参照してください)。
3. 必要とするセキュリティの種類に基づき、セキュリティ プロファイルを設定します (次の項に続きます)。
4. 1 つ以上の ESSID を設定し (手順については「[ESS の設定](#)」の章を参照してください)、それらに VLAN とセキュリティ プロファイルを割り当てます。

Web UI によるセキュリティ プロファイルの設定

Security Profile パラメータを設定するには、次の手順を実行します。

1. [Configuration] > [Security] > [Profile] をクリックします。
2. [Security Profile Name] ボックスで、セキュリティ プロファイルの名前を入力します。名前には最大で 32 文字の英数字を指定できます。スペースは使用できません。
3. [L2 Modes Allowed] 領域で、以下のいずれかのレイヤ 2 セキュリティ モードを選択します。
 - [Clear] : WLAN では、認証や暗号化が求められません。WLAN ではクライアント トラフィックの安全性が確保されません。これがデフォルト設定です。
 - [802.1X] : 802.1X 認証および WEP64 または WEP128 暗号化を提供できます。
 - [Static WEP keys] : ステーションで WEP キー を使用するよう求めます (手順 6 を参照)。
 - [WPA2] : EAP タイプのいずれかの 802.1X RADIUS サーバ認証を求めます (あらかじめ設定されている RADIUS サーバ プロファイルを選択するには、手順 4 を参照してください)。詳細については、[228 ページの「Wi-Fi 保護アクセス \(WPA2\)」](#)を参照してください。
 - [WPA2 PSK] : CCMP-AES 暗号プロトコルを使用して、事前共有キーを求めます (事前共有キーを入力するには手順 12 を参照してください)。
 - [WPA2-TKIP]
 - [MIXED] : 単一のセキュリティ プロファイルを使用して、WPA2 クライアントを許可します。
 - [MIXED PSK] : 事前共有キー クライアントが単一のセキュリティ プロファイルを使用することを許可します。
 - [WAI] : WPI-SMS4 暗号プロトコルを使用します。
 - [WAI PSK] : WPI-SMS4 暗号プロトコルを使用して、共有キーを求めます。

4. [Data Encrypt] 領域で、以下のいずれかを選択します (利用可能な選択肢は、選択した L2 モードによって異なります)。
- [Clear] : WLAN では暗号化を求めません。
 - [WEP64] : 64 ビットの WEP キーがパケットの暗号化に使用されます。詳細については、[229 ページの「WEP セキュリティ機能」](#)を参照してください。
 - [WEP128] : 128 ビットの WEP キーがパケットの暗号化に使用されます。詳細については、[229 ページの「WEP セキュリティ機能」](#)を参照してください。
 - [CCMP-AES] : 128 ビットのブロック キーが、WPA2 によるパケットの暗号化に使用されます。詳細については、[229 ページの「CCMP-AES」](#)を参照してください。
 - [WPI-SMS4] : WAI および WAI PSK で使用される暗号化アルゴリズムです。

WEP64 または WEP128 を使用する場合、手順 6 で説明しているように WEP キーを指定する必要があります。CCMP-AES for WPA2-PSK を指定する場合、手順 12 で説明しているように、事前共有キーを設定する必要があります。

5. [Primary RADIUS Profile Name] リストで、プライマリ サーバとして使用する設定済みの RADIUS サーバ プロファイルの 1 つを選択するか、[No RADIUS] オプションを選択します。設定されている RADIUS サーバ プロファイルがない場合には、選択可能なリストはなく、「No Data for Primary Radius Profile Name」というテキストが表示されます。RADIUS サーバ プロファイルを設定するには、[Configuration] > [Security] > [RADIUS] をクリックします。
6. [Secondary RADIUS Profile Name] リストで、セカンダリ サーバとして使用する設定済みの RADIUS サーバ プロファイルの 1 つを選択するか、[No RADIUS] オプションを選択します。設定されている RADIUS サーバ プロファイルがない場合には、選択可能なリストはなく、「No Data for Primary Radius Profile Name」というテキストが表示されます。RADIUS サーバ プロファイルを設定するには、[Configuration] > [Security] > [RADIUS] をクリックします。
7. [WEP Key] ボックスで、WEP キーを指定します。手順 2 で [WEP Keys] を選択した場合、16 進数またはテキスト文字列の形式で WEP キーを指定する必要があります。

WEP64 キーは 5 オクテット長である必要があります。これは 10 桁の 16 進数 (16 進数の文字列は 0x で始まる必要があります) または英数字 5 文字 (! 文字は使用できません) として指定できます。たとえば、0x619B947A3D は有効な 16 進数値で、**wpass** は有効な英数字の文字列です。

WEP128 キーは 13 オクテット長である必要があります。これは 26 桁の 16 進数 (16 進数の文字列は 0x で始まる必要があります) または英数字 13 文字 (! 文字は使用できません) として指定できます。たとえば、0xB58CE2C2C75D73B298A36CDA6A は有効な 16 進数値で、**mypass8Word71** は有効な英数字の文字列です。

8. [Static WEP Key Index] ボックスに、暗号化と復号化のための WEP キーで使用するインデックス番号を入力します。ステーションには、最大で 4 個の静的な WEP キーを関連付けることができます。静的な WEP キー インデックスは、1 から 4 までの整数である必要があります (0 から 3 の割り当てを使用するワイヤレス クライアントを処理するために内部マッピングが実行されます)。
9. [Re-Key Period] ボックスに、キーが有効である期間を入力します。0 から 65,535 秒の値を指定してください。鍵を変更するまでの時間のデフォルト値は、ゼロ (0) です。0 を指定すると、鍵の変更が無効になり、期間の長さに関わらずセッション中にキーは有効になります。
10. [BKSA Caching Period (seconds)] に、キーが有効である期間を入力します。0 から 65,535 秒の値を指定してください。デフォルト値は 43200 です。
11. [Captive Portal] リストで、次のいずれかを選択します。
 - [Disabled] : キャプティブ ポータルを無効にします。
 - [WebAuth] : WebAuth キャプティブ ポータルを有効にします。この機能は、すべての L2 モード選択で設定できます。
12. Bradford、Avenda、または CloudPath などの企業のサードパーティのキャプティブ ポータル ソリューションを使用する場合には、[Captive Portal Authentication Method] の値を [external] に変更します。詳細については、「[有線クライアントのキャプティブ ポータル \(CP\) 認証](#)」を参照してください。
13. 802.1X を使用するには、[802.1X Network Initiation] リストで次のいずれかを選択します。
 - [On] : コントローラは、EAP-REQUEST パケットをクライアントに送信して、802.1X 認証を開始します。デフォルトでは、この機能は有効化されています。
 - [Off] : クライアントは EAP-START パケットをコントローラに送信し、802.1X 認証を開始します。このオプションを選択すると、コントローラは 802.1X 認証を開始できません。
14. [Tunnel Termination] : tunnel-Termination は、IOSCLI および Controller GUI で提供されており、セキュリティ プロファイル単位ベースでの設定を実行します。[Tunnel Termination] リストから次のいずれかを選択します。
 - [PEAP] : PEAP (Protected Extensible Authentication Protocol) は、ワイヤレス ネットワークおよびポイントツーポイント接続で使用される認証プロトコルである EAP のバージョンです。802.1X ポート アクセス コントロールをサポートする 802.11 WLAN (ワイヤレス ローカル エリア ネットワーク) のための安全な認証を実現するために設計されています。公開キー証明書を使用してサーバを認証し、安全な Transport Layer Security (TLS) で認証を実行します。

- [TTLS] : TTLS (Tunneled Transport Layer Security) は、提案されているワイヤレス セキュリティ プロトコルです。



Tunnel Termination が有効な場合、フォーティネットのデフォルトの証明書が使用されます。この場合、認証を成功させるために、証明書はワイヤレス クライアント側で「信頼」される必要があります。証明書のインポート方法の詳細は、「[セキュリティ証明書](#)」を参照してください。



PEAP/TTLS が RADIUS サーバで設定されている場合、PEAP/TTLS ターミネーションを無効にする必要があります。

15. Static WEP Key モードが使用されている場合、[Shared Key Authentication] リストで、次のいずれかを選択します。
 - [On] : 802.1X 共有キー認証を有効にします。
 - [Off] : オープン認証を使用します。デフォルトでは、この機能はオフです。
16. 上記の手順 2 で PSK または WPA2-PSK を選択した場合は、[Pre-shared Key] テキストボックスに、キーを入力します。キーは、8 ～ 63 個の ASCII 文字または 64 個の 16 進数文字を指定できます。16 進数のキーの場合は、プレフィックス「0x」を使用してください。そうしないとキーが動作しません。
17. [Group Keying Interval] テキスト ボックスに、新しいグループキーを配信する間隔を秒数で入力します。
18. [PMK Caching] で、[On] または [Off] を選択します。
19. [Key Rotation] ドロップダウン リストで、この機能を有効にするか無効にするかを選択します。
20. [Backend Authentication Server Timeout] のタイムアウト値には、1 ～ 65535 秒を指定できます。
21. [Re-authentication] では、次のいずれかを選択します。
 - [On] : コントローラが、RADIUS Access-Accept パケットにある「Sessiontimeout」RADIUS 属性を強制的に受け取るようになります。一定期間が経過するとステーションがネットワーク (802.1X) を再認証するように求めるために Session-timeout 属性を使用する場合に、このオプションを使用します。「Session-timeout」が使用されていない場合、再認証を有効にする理由はありません。
 - [Off] : このセキュリティ プロファイルの再認証を無効にします。
22. [MAC Filtering] リストで、次のいずれかを選択します。
 - [On] : このセキュリティ プロファイルで MAC フィルタリングを有効にします。
 - [Off] : このセキュリティ プロファイルで MAC フィルタリングを無効にします。

23. [MAC Auth Primary RADIUS Profile Name] リストで、事前に設定された認証サーバ プロファイルの名前を選択します。
24. [MAC Auth Secondary RADIUS Profile Name] リストで、事前に設定された認証サーバ プロファイルの名前を選択します。
25. [MAC Accounting Primary RADIUS Profile Name] リストで、事前に設定された RADIUS アカウンティング サーバ プロファイルの名前か [No RADIUS] オプションを選択します。
26. [MAC Accounting Secondary RADIUS Profile Name] リストで、事前に設定された RADIUS アカウンティング サーバ プロファイルの名前か [No RADIUS] オプションを選択します。
27. [Firewall Capability] ドロップダウン リストで、次のいずれかを選択します。
- [Configured] : コントローラは、ファイアウォールのフィルタ ID の設定を通じてポリシーを定義します。
 - [RADIUS-configured] : RADIUS サーバは、ユーザの 802.1X 認証が成功した後に、このポリシーを提供します。このオプションを使用するには、RADIUS サーバでフィルタ ID が設定されている必要があります。フィルタ ID が設定されていない場合、ファイアウォールの機能は保証されません。
 - [None] : このセキュリティ プロファイルでファイアウォールの機能を無効にします。
28. [Firewall Filter ID] テキスト ボックスに、このセキュリティ プロファイルで使用するファイアウォールのフィルタ ID を入力します。フィルタ ID は、ファイアウォールの機能が設定されているときに、コントローラでファイアウォール ポリシーを定義する英数字の値になります。たとえば、1 になります。
29. [Security Logging] ドロップダウン リストで、次のいずれかを選択します。
- [On] : このセキュリティ プロファイルでセキュリティ関連のメッセージのログを有効にします。
 - [Off] : このセキュリティ プロファイルでセキュリティ関連のメッセージのログを無効にします。
30. [Passthrough Firewall Filter ID] テキスト ボックスに、[Configuration] > [QoS] > [System Settings] > [QoS and Firewall Rules] > [Add] を使用して作成したファイアウォール フィルタ ID を入力します。フィルタ ID は、認証がないキャプティブ ポータルが有効なクライアントのためのコントローラで使用するファイアウォール ポリシーを定義する英数字の値です。
31. [OK] をクリックします。

Wi-Fi 保護アクセス (WPA2)

802.11i 規格がリリースされるまでの間、WEP の既知の脆弱性を改善するという目的で Wi-Fi Alliance が提唱した、暫定的なセキュリティ規格である WPA2 および 802.1x プロトコルがフォーティネット ワイヤレス LAN システムでサポートされます。

WPA2 では、WPA Message Integrity Code (MIC) アルゴリズムがメッセージ認証コード (CCMP) により置き換えられています。CCMP は、完全に安全であると考えられ、RC4 暗号は、[229 ページの「CCMP-AES」](#)で説明されているように Advanced Encryption Standard (AES) により置き換えられています。

802.1X 認証を利用できない場合には (たとえば、SOHO などにおいて)、WPA2- Personal を代替手段として使用し、AP とクライアント間の手動でのキー配布を提供できます。

厳密にセキュアな WPA2 実装を実現するためには、「純粋な」実装、すなわち、すべての AP とクライアント デバイスで WPA2-Enterprise を稼働させる必要があります。ワイヤレス LAN システム環境においては、WPA2 を設定し、サイトの 802.1X ユーザ認証を活用し、TKIP または CCMP 暗号化が含まれているセキュリティ プロファイルを使用する ESS によって、このような実装を実現できます。このプロファイルの関連付けが終われば、ユーザと企業には極めて高いレベルのデータ保護が保証されます。

これらのセキュリティ オプションの設定については、[224 ページの「Web UI によるセキュリティ プロファイルの設定」](#)および [239 ページの「CLI での WPA2 の設定」](#)を参照してください。

暗号化サポート

ワイヤレス LAN システムは、CCMP-AES for WPA2 をサポートしています。WPA2 では暗号化の手法として CCMP/AES を使用します。これらのテクノロジーの説明については、この項を参照してください。フォーティネット は、WEP64 および WEP128 によるオリジナルの 802.11 暗号プロトコルもサポートしています。

サイトのクライアント ハードウェアが CCMP をサポートしていない場合には、セキュアな CCMP-AES 暗号化ソリューションを使用することをお奨めします。

CCMP-AES

AES は Advanced Encryption Standard の略であり、米国国防総省によって新しい暗号化規格として採用されています。このような経緯からもこれは極めて安全な暗号化手法となっています。AES はいくつかのモードで使用でき、CCMP は WPA2 で使用されるモードです。両方の用語は同じ意味を表します。

WEP セキュリティ機能

WEP64 および WEP128 (Wired Equivalent Privacy) は、IEEE Wi-Fi (Wireless Fidelity) 規格である 802.11 で規定されている、レイヤ 2 のセキュリティ プロトコルです。有線 LAN に一般的に求められるレベルのセキュリティとプライバシーをワイヤレス LAN にも提供するように設計されています。有線 LAN は、一般的にはビルへの立ち入りをコントロールするなどの物理的な方法で保護します。これは、物理的な環境をコントロールするためには効果的な方法

です。ところが、WLAN では、ネットワークが設置されている壁面の外まで無線波が届かないとも限らないため、このようなセキュリティ メカニズムは適用できません。WEP では、WLAN 内で転送されるデータを暗号化することで、有線ネットワークの物理的なセキュリティ対策と似た方法で保護することを目指しています。データの暗号化は、クライアントとアクセス ポイントの間の脆弱なリンクを保護します。この対策が講じられれば、認証、パスワードによる保護、エンドツーエンドの暗号化などの他の一般的な LAN セキュリティ メカニズムを導入して、プライバシーを保護できます。

WEP プロトコルでは、1 つのワイヤレス LAN 上のすべてのアクセス ポイントとクライアント無線 NIC が同じ暗号化キーを使用する必要があります。送信側の各ステーションは各フレームの本体を WEP キーを使って暗号化してから転送し、受け取り側のステーションは同じキーを使ってそれを復号化します。このような手順によって、それほど強い意図を持たない誰かが送受信を監視し、フレームに含まれている情報にアクセスするリスクを軽減します。

WEP 実装では、セキュリティ プロファイルの設定で、ユーザのステーション キー管理プログラムによって設定された 4 つの WEP キーのいずれかを指定するように設定できます。

WEP の設定については、240 ページの「[802.11 WEP 暗号化の設定](#)」の項を参照してください。

WEP プロトコルの動作

ユーザが WEP をアクティブにしていると、NIC は、RSA Security が提供する RC4 ストリーム暗号を使用して、各 802.11 フレームのペイロードを転送前に暗号化します。このペイロードは、フレーム本体と CRC (サイクリック リダンダンシ チェック) から構成されています。受け取り側ステーション (たとえば、アクセス ポイントやそれ以外の無線 NIC) は、そのフレームを受け取ると、復号化を実行します。結果として、802.11 WEP は 802.11 ステーション間のデータだけを暗号化します。フレームがネットワークの有線部分 (アクセス ポイント間など) に入ると、WEP は適用されなくなります。

暗号化の手順の中で、WEP は、送り側ステーションのユーザから渡される共有シークレットキーをランダムに生成された 24 ビットの初期化ベクトル (IV) と連結させることで、キー スケジュール (シード) を用意します。この IV によって、シークレット キーの寿命が長くなります。それは、ステーションはフレームの転送ごとにこの IV を変えることができるためです。WEP は、結果のシードを擬似乱数ジェネレータにかけて、フレームのペイロードに 32 ビットの ICV (Integrity Check Value) を加えた長さと同じになるキー ストリームを生成します。

ICV とは、受け取り側ステーションが後で再計算し、送り側ステーションから送られてきたものと比較することで、送られてきたデータが伝送中に何らかの形で改ざんされていないかどうかを判断するために使われるチェックサムです。不一致が発生した場合は、受け取り側ステーションは、そのフレームを拒絶するか、セキュリティ違反の可能性があると、そのユーザに警告を与えることができます。

WEP では、送り側と受け取り側のステーションが暗号化と復号化に同じキーを使用します。WEP では、データの暗号化と復号化のための 40 ビットあるいは 104 ビットのキーを指定します (これに 24 ビットの IV が追加されれば、それぞれ、FortiWLC (SD) の 64 ビット、128 ビットの WEP 仕様と一致します)。そのため、それぞれの無線 NIC とアクセス ポイントを、同じキーを使用して手動で設定する必要があります。

転送が行われる前に、WEP は、ビット XOR 処理を使ってキー ストリームをペイロードおよび ICV と結合して、暗号テキスト (暗号化されたデータ) を生成します。WEP には、フレーム本体の先頭の数ビットに、クリアな (暗号化されていない) IV が含まれています。受け取り側ステーションは、この IV と送り側ステーションのユーザから渡された共有シークレット キーを使って、フレーム本体のペイロード部分の復号化を行います。

WEP プロトコルの限界

WEP は比較的短い IV を使用し、キーが固定であるために、脆弱です。短時間の間、WEP は結果的に同じ IV を異なるデータ パケットのために使用します。大規模で使用率の高いネットワークでは、1 時間余りにわたって同じ IV が使用される可能性もあり、その結果として、同じようなキー ストリームのフレームが送受信されることになります。もしハッカーがこの同じ IV を使っているフレームを数多く収集すれば、そのハッカーはそれらのフレームに共通する値 (キー ストリームまたは共有シークレット キー) を特定できます。そうすれば、そのハッカーはどの 802.11 フレームでも解読できてしまいます。

802.11 規格の潜在的問題としてよく知られているのが、キーを変えるのが面倒であるという点です。802.11 規格では、ステーション間でのキーの交換をサポートする機能は提供されていません。異なるキーを使用するには、管理者が手動でアクセス ポイントと無線 NIC ごとに新しい共通キーを設定しなければなりません。WEP キーを定期的に変更しないと、権限のない人間が何らかのツールを使ってネットワークを監視し、暗号化されたフレームを解読できてしまうことになります。

このような弱点はありますが、最低レベルのセキュリティとして WEP を有効にしておくべきでしょう。多くのハッカーが、WEP を使用していないワイヤレス LAN を見つけ出し、さらには、ラップトップを使ってそのワイヤレス LAN のネットワーク上のリソースにアクセスできます。WEP を使用することで、少なくともこのようなことが起きる危険を最小限に抑えることができます。WEP は、大多数の善良な人を近づけないようにするためには効果的な手段だと言えるでしょう。

GRE トンネルの設定

GRE トンネルにより、ある終点から別の終点まで通過するパケットを分離できます。これは、IP トンネル内でパケットをカプセル化することで、ユーザ トラフィックが分割されています。

GRE トンネルは、図 44 に示す構成となります。ゲスト ESS にログインするゲスト ユーザには、「ゲスト」インターネット アクセス権限が付与され、企業キャンパス上にある一般的な共有リンク上でやりとりする企業ユーザのトラフィックから分離したトラフィックが関連付けられます。契約社員のユーザは、企業ユーザと同じような接続が設定されますが、ユーザファイアウォールポリシーによって特定のサイトへのアクセスが制限されます。

GRE トンネルを使用すると、ESS プロファイルを GRE プロファイルに関連付けて、ユーザトラフィックを分離することもできます。この方法はトラフィックを分離する方法として VLAN の代替となります。

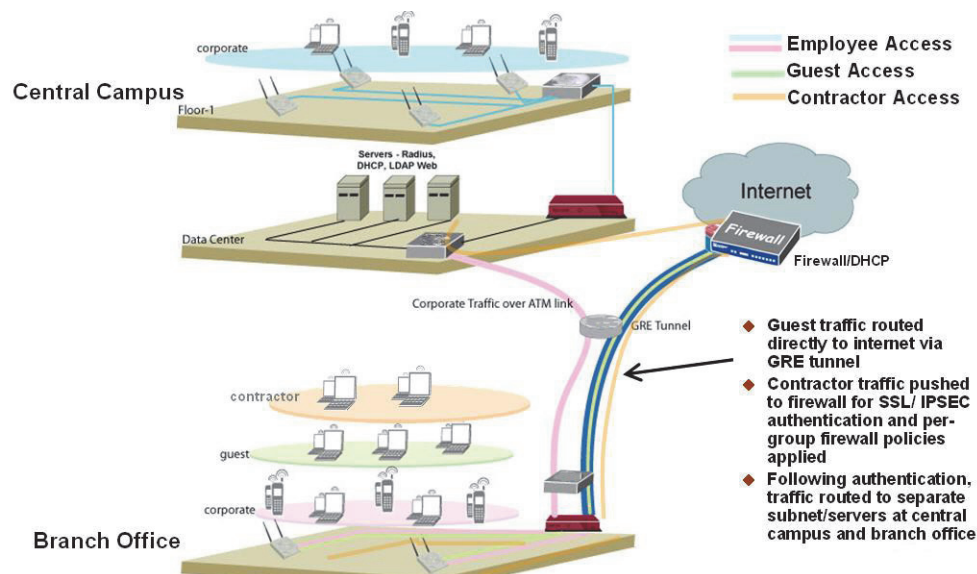


図 44: GRE トンネル構成の例

GRE トンネルを設定するには、GRE トンネル プロファイルと、GRE トンネルを指定してセキュリティ プロファイルも参照する ESSID を作成します。GRE は、E(z)RF Network Manager から設定できます。

トンネルに設定されるすべての IP アドレスは固有である必要があります。これらの IP アドレスによりトンネルの終点が定義されます。また、コントローラ FastEthernet IP アドレスはローカルの終点を定義し、ip remote-externaladdress コマンドはリモートの終点を指定します。ip tunnel-ip-address コマンドはトンネル ネットワークを定義します。



デュアルイーサネット設定の第 2 インターフェイスで GRE トンネルを設定する場合は、**207 ページの「アクティブインターフェイスの設定」**の手順に従って、第 2 イーサネット インターフェイスを設定してください。

次の例は、第 2 FastEthernet インターフェイスで GRE トンネル プロファイルを設定するコマンドを示しています。トンネルのローカル終点の IP アドレスとして 13.13.13.13、リモート終点の IP アドレスとして 172.27.0.206、そして DHCP サーバの IP アドレスに 10.0.0.12 が指定されています。

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.255.0
default(config-gre)# ip remote-external-address 172.27.0.206
default(config-gre)# ip dhcp-override
default(config-gre)# ip dhcp-server 10.0.0.12
default(config-gre)# end
```

GRE トンネルの設定を確認するには、show gre コマンドを使用します。

```
default# show gre
GRE Name      Remote External Address   Tunnel IP address   Tunnel IP Netmask
LocalExternal
vlan1        172.27.0.162              12.12.12.12         255.255.0.0
  1
gre1         172.27.0.206              13.13.13.13         255.255.0.0
  2
          GRE Configuration(2 entries)
```

GRE ESSID を設定するには、次の例のように、GRE プロファイル名、トンネル タイプとセキュリティ プロファイルを指定します。

```
default(config)# essid guest
default(config-essid)# gre name guest
default(config-essid)# tunnel-type gre
default(config-essid)# security-profile default
default(config)# exit
```

- GRE ESSID の名前は、GRE 設定手順で指定する GRE トンネル プロファイルの名前 (guest など) と同じである必要があります。GRE トンネル プロファイル名は gre name で指定されます。
- tunnel-type については、gre パラメータを GRE トンネル設定に指定する必要があります。
- security-profile コマンドを使用してセキュリティ プロファイル名を指定します。通常は default プロファイルを使用します。

GRE トンネルのステータスを確認するには、次のコマンドを使用します。

```
default# test gre gre_name ip_address
```

コマンドに含まれる各要素は次のとおりです。gre_name は、GRE プロファイルの名前です。ip_address は、トンネルの背後で接続されるマシンの IP アドレスです (オプション)。



デフォルトでは、このコマンドによりリモート終点が Ping されます。

GRE トンネルを設定する場合には次の点について注意する必要があります。

- DHCP リレー パススルーのフラグは GRE トンネルでは常にオフにします。これにより、DHCP リレーが確実に常時オンとなるため、DHCP 要求パケットが DHCP サーバ IP アドレスにより指定される DHCP サーバに転送されるようになります。
- GRE トンネルに接続するユーザに関連付けられている DHCP トラフィックは、関連付けられている GRE トンネルを経由してリモートにある設定済みの DHCP サーバにリレーされます。
- GRE トンネルでは IPv4 だけがサポートされます。

CLI によるセキュリティ プロファイルの設定

コントローラでは、必要とするセキュリティの種類に応じて複数のセキュリティ プロファイルを定義し、それらを異なるワイヤレス LAN の ESS (Extended Service Sets) に割り当てることができます。セキュリティ プロファイルとは、ESS 内でどのようにセキュリティ機能を扱うかを定義するパラメータのリストです。セキュリティ プロファイルでは、レイヤ 2 のセキュリティを定義でき、暗号スイート、プライマリやセカンダリ RADIUS サーバ、固定 WEP キー エントリやキー インデックス位置、およびその他のパラメータを指定できます。各種のセキュリティ プロファイルを作成しておく、同じ WLAN 内で複数の認証や暗号化方法を適用できるようになります。



レイヤ 2 メソッド 1 つだけを各セキュリティ プロファイルで定義できます。

コントローラは、認証がなく、どのワイヤレス クライアントもそのコントローラに接続できないことを表す、オープン認証の状態出荷されます。これらの設定は、**default** という名前のデフォルトのセキュリティ プロファイルに定義されています。

show security-profile default コマンドを使用すると、デフォルトのセキュリティ プロファイルを表示できます。


```

default# show security-profile default
Security Profile Table
Security Profile Name           : default
L2 Modes Allowed                : clear
Data Encrypt                    : none
Primary RADIUS Profile Name     :
Secondary RADIUS Profile Name   :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index            : 1
Re-Key Period (seconds)         : 0
Captive Portal                  : disabled
802.1X Network Initiation       : off
Tunnel Termination              : PEAP, TTLS
Shared Key Authentication       : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Group Keying Interval (seconds) : 0
PMK Caching                     : disabled
Key Rotation                    : disabled
Reauthentication                : off
MAC Filtering                   : off
Firewall Capability             : none
Firewall Filter ID              :
Security Logging                 : off
Passthrough Firewall Filter ID) :

```

default セキュリティ プロファイルは、認証方法、暗号化、あるいは暗号スイートを指定しない、「クリア」なレイヤ 2 アクセスができるよう、設定されています。

Tunnel Termination は、PEAP および TTLS で別々に設定されます。

CLI での 802.1X RADIUS セキュリティの設定

サイトの 802.1X への WLAN アクセスを承認されたユーザだけに限定するには、802.1X RADIUS 認証をセットアップします。手順は以下のとおりです。

- グローバル RADIUS サーバ プロファイルを作成し、ネットワーク上のプライマリ RADIUS サーバとの通信方法を指定します。オプションのセカンダリ RADIUS サーバを使用する場合には、別のプロファイルを作成し、同様に通信方法を指定します。
- 802.1X レイヤ 2 セキュリティを設定する ESS のためのセキュリティ プロファイルを作成し、プライマリ RADIUS プロファイルとオプションのセカンダリ RADIUS プロファイルを割り当てます。

使用するサイト用の種類の EAP プロトコルの設定の方法と、必要となる証明書があればそれをインストールするための手順については、使用する RADIUS サーバのドキュメントを参照

してください。RADIUS サーバの実際の設定については、ここでは説明しません。RADIUS サーバとコントローラの間の通信を可能にするための設定についてのみ説明します。

以下のコマンドでは、プライマリ RADIUS サーバのためのプロファイルである main-auth を作成し、このサーバの IP アドレスとシークレット キーを指定しています。それ以外のパラメータ (ポート番号 (1812) など) はすべてデフォルトを使用し、変更していません。

```
default# configure terminal
default(config)# radius-profile main-auth
default(config-radius)# ip-address 10.1.100.10
default(config-radius)# key secure-secret
default(config-radius)# exit
```

信頼性を強化するために、プライマリ サーバが利用できなくなった場合にバックアップとして動作するセカンダリ RADIUS サーバ プロファイルを設定します。

```
default# configure terminal
default(config)# radius-profile backup-auth
default(config-radius)# ip-address 10.1.100.2
default(config-radius)# key secure-secret2
default(config-radius)# exit
```

次に、802.1X を有効にし、RADIUS プライマリ サーバとセカンダリ サーバを記述しているプロファイルをポイントするセキュリティ プロファイルを作成します。

802.1X RADIUS セキュリティ プロファイルの例

以下の例では、**8021x-data** というプロファイルを作成します。このプロファイルは、802.1X 認証をサポートし、プライマリ RADIUS 認証サーバを有効にするために main-auth という RADIUS プロファイルを、セカンダリ RADIUS サーバを有効にするために backup-auth をそれぞれ使用します。

```
default(config)# security-profile 8021x-data
default(config-security)# allowed-l2-modes 802.1x
default(config-security)# radius-server primary main-auth
default(config-security)# radius-server secondary backup-auth
default(config-security)# exit
default(config)# exit
```

802.1X PTK キー変更

802.1X PTK キーの変更機能を使用すると、キーの変更期間が失効したときに、アクセス ポイントがユニキャスト キーおよびブロードキャスト キーをクライアントに送信します。これらの 2 つのキー パケットは暗号化されません。

802.1X PTK キー変更を有効にするには、セキュリティ プロファイル設定から次のコマンドを入力します (n には 0 から 65535 (60 分) の間の数値を秒で指定します)。

```
default(config-security)# rekey period n
```

802.1X PTK のキー変更を無効にするには、セキュリティ プロファイル設定から次のコマンドを入力します。

```
default(config-security)# rekey period 0
```

802.1X GTK キー変更

802.1X GTK キーの変更期間を設定するには、セキュリティ プロファイル設定から、次のコマンドを追加します (キー変更の期間は秒単位で指定します)。

```
default(config-security)# group-rekey interval n
```

802.1X GTK のキー変更を無効にするには、セキュリティ プロファイル設定から次のコマンドを入力します。

```
default(config-security)# no group-rekey interval
```

802.1X RADIUS サーバコマンドのまとめ

RADIUS サーバの設定に使用するコマンドは以下のとおりです。

表 15: 802.1X RADIUS サーバの設定に使用するコマンド

コマンド	目的
radius-profile name	指定した名前の RADIUS サーバ プロファイルを作成し、RADIUS プロファイル設定サブモードに入ります (最大 16 文字)。
description text	プロファイルの詳細を設定します (最大 128 文字)。
ip-address ip-address	RADIUS プロファイルの IP アドレスを設定します (必須パラメータ)。
key key	コントローラが RADIUS プロファイルに対して使用する共有シークレット テキスト文字列を指定します (パスワード タイプ (password-type) が共有シークレット (shared-secret) の場合には、必須パラメータです)。最大で 64 文字です。
password-type shared-secret mac-address	パスワード タイプが RADIUS key (共有シークレット) または、クライアントの MAC アドレスであるかどうかを指定します。MAC フィルタリング設定の RADIUS にあるクライアント セットアップにより決定されます。

表 15: 802.1X RADIUS サーバの設定に使用するコマンド

コマンド	目的
mac-delimiter colon hyphen singlehyphen none	オプション。RADIUS プロファイルの区切り文字を設定します。
port port	オプション。RADIUS プロファイル ポートを設定します (デフォルトポート 1812 がデフォルトで設定されています)。
vlan vlan	オプション。RADIUS サーバの VLAN を設定します。RADIUS サーバが VLAN 上にあるためにデフォルトのタグなしインターフェイスの代わりに VLAN インターフェイス に RADIUS 要求が送られる場合に、このコマンドを使用します。
pmkcatching pmkcatching disable	PMK キャッシュを有効または無効にします。
rekey period <i>n</i>	PTK のキー変更の期間を設定します。デフォルトでは、60 秒に設定されています。60 秒から 60 分の範囲で指定できます。
[no] group-rekey interval <i>n</i>	GTK グループのキー変更の期間を設定します。デフォルトでは、60 秒に設定されています。60 秒から 60 分の範囲で指定できます。

表 16: セキュリティ プロファイルの作成に使用するコマンド

コマンド	目的
allowed-l2-modes 802.1x	セキュリティ プロファイルの設定で、802.1X 認証を有効にします。
radius-server primary profile	セキュリティ プロファイルの設定で、プライマリ RADIUS サーバの設定パラメータを含む RADIUS プロファイルを指定します。
radius-server secondary profile	オプション。セキュリティ プロファイルの設定で、セカンダリ RADIUS サーバの設定パラメータを含む RADIUS プロファイルを指定します。

表 16: セキュリティ プロファイルの作成に使用するコマンド

rekey multicast-enable	オプション。セキュリティ プロファイルの設定で、マルチキャスト キー ブロードキャストを有効にします。
[no] 8021x-network-initiation	セキュリティ プロファイルの設定で、802.1X 初期化メソッドを決定します。有効 (デフォルト) の場合、AP が最初の EAP パケット (EAP ID 要求) をワイヤレス ステーションに送信し、ワイヤレス ステーションが 802.11 認証および 802.1X が有効な ESSID への割り当てを完了すると、802.1X を開始します。コマンド no 8021x-network-initiation を使用すると、ワイヤレス ステーションは EAPOL Start パケットを AP に送信し、802.1X 交換が開始されます。

CLI での WPA2 の設定

コントローラは、極めて安全であると考えられている CCMP 暗号化が取り入れられている WPA2 規格をサポートしています。WPA2 を実装すると、ワイヤレス LAN システムで最高のセキュリティ レベルを確保できます。

さらに、802.1X がサイトで実装されている場合には、自動キー交換が、RADIUS サーバで行われます。既存のプライマリおよびセカンダリ RADIUS サーバ プロファイルを既存の 802.1X 認証を活用するセキュリティ プロファイルで割り当てることができます。802.1X がサイトで実装されていない場合には、WPA2-PSK 設定を実装できます。

WPA2 の設定例

WPA2 セキュリティを設定するには、Web UI を使用し、[Configuration] > [Security] > [Profile] をクリックします。オプションの詳細については [Help] をクリックしてください。

次の CLI 例では、レイヤ 2 で WPA2 を有効にする **wpa2-ccmp** という名前のプロファイルを作成し、暗号化モードを CCMP-AES に設定しています。また、プライマリ RADIUS 認証サーバとして main-auth プロファイルでこの RADIUS サーバの名前を付けています。

```
default(config)# security-profile wpa2-ccmp
default(config-security)# allowed-l2-modes wpa2
default(config-security)# encryption-modes ccmp
default(config-security)# radius-server primary main-auth
default(config-security)# exit
default(config)# exit
```

WPA2-PSK の設定例

セキュリティを設定するには、Web UI を使用し、[Configuration] > [Security] > [Profile] をクリックします。オプションの詳細については [Help] をクリックしてください。

PSK キーを設定する場合、8 から 63 の ASCII 文字 (!\ " ? の文字はバックスラッシュ (\) でエスケープする必要があります。!!\? など) または 64 の 16 進数文字 (16 進数のキーには、"0x" という接頭辞を付ける必要があります。そうしないとキーは動作しません) をキーに使用します。

次の例では、レイヤ 2 で WPA2-PSK を有効にする *wpa2-psk* という名前のプロファイルを作成しています。また、暗号化モードを CCMP に設定しており、事前共有キーを theSecretKeyForNov28 に設定しています。

```
default(config)# security-profile wpa2-psk
default(config-security)# allowed-l2-modes wpa2-psk
default(config-security)# encryption-modes ccmp
default(config-security)# psk key theSecretKeyForNov28
default(config-security)# exit
default(config)# exit
```

WPA の Opportunistic PMK キャッシュ

Opportunistic PMK キャッシュを使用すると、コントローラを 802.1X 認証デバイスとして動作させることができます。完全な 802.1X 認証の結果をキャッシュし、コントローラに関連付けられている任意の AP にクライアントがローミングしている場合に、ワイヤレス クライアントは 4 ウェイハンドシェイクのみを実行し、新規のペアワイズ一時キーを決定できます。PMK キャッシュは、TKIP および 802.1X 認証と共に WPA を使用するときに、KDDI 電話でのみサポートされます。

システムは KDDI ベンダー ID を使用して KDDI の電話を自動検出し、使用可能であれば PMK キャッシュを適用します。

セキュリティ プロファイル設定から、KDDI 電話の PMK キャッシュを有効または無効にします。このオプションは、L2 暗号化に WPA が選択されている場合にのみ使用できます。

PMK キャッシュを有効にするには、WPA セキュリティ プロファイル設定に次の行を追加します。

```
default(config-security)# pmkcaching enabled
```

PMK キャッシュを無効にするには、WPA セキュリティ プロファイル設定で以下のコマンドを実行します。

```
default(config-security)# pmkcaching disabled
```

802.11 WEP 暗号化の設定

コントローラは、2 つの WEP 暗号スイート、WEP128 と WEP64 をサポートしています。

ほとんどのユーザ キー設定プログラムから、キー設定パラメータを使用して、相互に共有キーを設定し、キー スロット位置を 1 ～ 4 から選択できます。

802.11 WEP の設定例

次の例では、音声ユーザに対して固定の 128 ビットの WEP 暗号化をサポートする、`wep-` という名前のプロファイルを作成しています。固定の WEP キーが定義され、ユーザ ステーションの WEP キー定義の 3 つ目のキーインデックス位置を使用します。

```
default(config)# security-profile wep-
  default(config-security)# allowed-l2-modes wep
  default(config-security)# encryption-modes wep128
  default(config-security)# static-wep key
  default(config-security)# static-wep key-index 3
  default(config-security)# exit
default(config)# exit
default#
```

802.11 WEP コマンドのまとめ

802.11 WEP セキュリティの設定に使用するコマンドは以下のとおりです。

表 17: 802.11 WEP セキュリティの設定に使用するコマンド

コマンド	目的
encryption-modes wep128 wep64	暗号スイートをそれぞれ WEP128 または WEP64 に設定します。
static-wep key key	WEP キーを設定します。 <ul style="list-style-type: none">WEP64 (WEP あるいは WEP40 と呼びます) の場合は、キーは 5 文字の ASCII (たとえば、123de) または 10 文字の 16 進キー (たとえば、0x0123456789) です (接頭辞 0x を入力する必要があります)。WEP128 の場合は、キーは 13 文字の ASCII または 26 桁の 16 進数です (接頭辞 0x を入力する必要があります)。
static-wep key-index position	どの WEP キーが使用中であるかを設定します。position は 1 ～ 4 に設定できます。
allowed-l2-modes wep clear	802.11 WEP セキュリティを有効または無効にします。clear オプションはモードをオープンにします。

CLI 設定のチェック

現在設定されているすべてのセキュリティ プロファイルを確認するには、show security-profile コマンドを使用します。

```
# sh security-profile
Profile Name      L2 Mode      Data Encrypt Firewall Filter
default          clear        none
captive-portal   clear        none
wep              wep          wep64
802.1x           802.1x      wep128
wpa              wpa          tkip
wpapsk           wpa-psk     tkip
wpa2             wpa2        ccmp
wpa2psk          wpa2-psk    ccmp

Security Profile Table(8)
```

個々のセキュリティ プロファイルの詳細を確認するには、show security-profile *profile-name* コマンドを使用します。

```
default# show security-profile wpa-leap
Security Profile Table
Security Profile Name      : wpa-leap
L2 Modes Allowed          : 802.1x
Data Encrypt               : none
Primary RADIUS Profile Name : ACS-87-8#
Secondary RADIUS Profile Name :
WEP Key ASCII:(default) 13 chars / 0x:26 chars : *****
Static WEP Key Index      : 1
Re-Key Period (seconds)   : 0
Enable Multicast Re-Key   : off
Captive Portal            : disabled
802.1X Network Initiation : on
Tunnel Termination        : PEAP, TTLS
Shared Key Authentication : off
Pre-shared Key (Alphanumeric/Hexadecimal)      : *****
Group Keying Interval (seconds)                 : 0
PMK Caching                                       : disabled
Key Rotation                                     : disabled
Reauthentication                                 : off
MAC Filtering                                    : off
Firewall Capability                             : none
Firewall Filter ID                              :
Security Logging                                 : off
```

show web login-page と show web custom-area コマンドを使用すると、キャプティブ ポータルと WebAuth で使用する Web ページがどれであるか確認できます。

Policy Enforcement Module (ポリシー適用モジュール)

オプションの Policy Enforcement Module 機能を使用すると、ユーザ グループに関連付けられているファイアウォール タグに適用されるポリシーを基準として、トラフィックをドロップまたは許可することにより、ネットワーク コンテンツを制御できます。リリース 3.7 移行では、キャプティブ ポータル ユーザが含まれます。

フォーティネットのファイアウォールは汎用的であり、特定ポートまたはすべてのポートについて任意のサブネット間の通信を防ぐために使用できます。フィルタ ID を使用すると、任意の SSID からのユーザが特定のサブネットにアクセスするのを防ぐことができます。

ユーザごとのファイアウォール フィルタリングは、次のいずれかの方法で実装されます。

- RADIUS が返す filter-id 属性。この属性は RADIUS サーバで作成されユーザに関連付けられます。
- 設定されているファイアウォール filter-id パラメータ。セキュリティ プロファイル設定の一部であり、ESS に関連付けられているクライアントに適用されます。

RADIUS を用いたユーザごとのファイアウォールの場合には、Access-Accept (アクセス許可) メッセージの一部として返される filter-id 属性がファイアウォール タグとして使用されます。フィルタリング アクションは、このファイアウォール タグに設定されているファイアウォール ポリシーにより決定されます。

RADIUS 設定がない場合には、セキュリティ プロファイルで設定されているファイアウォール タグを、設定されているファイアウォール ポリシーを基準したフィルタリングの定義に使用できます。この場合、設定されているファイアウォールポリシーを適用します。ある ESS プロファイルに接続しているすべてのユーザには、このプロファイルに設定されているのと同じファイアウォール タグが割り当てられます。



RADIUS 設定を使用して正しく動作させるためには、RADIUS サーバで設定された *Filter-id* 属性がコントローラで使用されている属性と一致している必要があります。RADIUS サーバによっては、フィルタ ID を作成する必要があります。

トラフィックをフィルタリングするポリシーは、標準 QoS の qosrule 設定を使用して作成されます。また固有の優先度と設定パラメータは、本書の 15 章、および『*FortiWLC (SD) コマンド リファレンス*』の qosrule の項目を参照してください。

CLI のファイアウォール ポリシーの設定

ユーザごとのファイアウォール設定は、トラフィックを管理するための一連の qosrule ポリシーを設定することから開始します。

次の例は、qosrule 200 を Firewall filter-id 1 のポリシーとして作成しています。

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
default(config)# netprotocol-match
default(config-qosrule)# dstport 80
default(config-qosrule)# dstport-match on
default(config-qosrule)# action drop
default(config-qosrule)# firewall-filter-id 1
default(config-qosrule)# firewall-filter-id-match on
default(config-qosrule)# qosrule-logging on
default(config-qosrule)# qosrule-logging-frequency 30
default(config-qosrule)# exit
default(config)# exit
```

ポリシーの設定を確認するには、show qosrule コマンドを使用します。

```
default# show qosrule
```

ID	Dst IP	Dst Mask	DPort	Src IP	Src Mask	SPort
Prot	QoS	Action	Drop	Firewall	Filter	
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0
6	h323	capture	head			
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720
6	h323	capture	head			
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
17	sip	capture	head			
4	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5060
17	sip	capture	head			
7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0
17	none	forward	head			
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200
17	none	forward	head			
200	0.0.0.0	0.0.0.0	80	0.0.0.0	0.0.0.0	0
6	none	drop	tail 1			

QoS Rules(7 entries)

```
default#
```

次のコマンドは、例となるフィルタ ID 1 をセキュリティ プロファイルに適用するために必要です。

```
default(config-security)# firewall-capability configured
default(config-security)# firewall-filter-id 1
default(config-security)# security-logging off
```



ファイアウォールのルールを一度作成したら、ルールを変更してファイアウォールのログギングを有効 / 無効にすることはできません。回避策として、必須のオプションを使用してこのファイアウォールを作成するか、必須のオプションを使用して再度適用してください。

ユーザごとのファイアウォールのトラブルシューティング

- QoS ルールのページで利用可能な QoS ルール ログギング機能をオンにします。クライアント トラフィックがこのルールにヒットすると、同じ内容が syslog サーバに表示されます。また、CLI コマンド `show syslog-file firewall` でも表示されます。

コマンドの詳細については、『*FortiWLC (SD) 設定ガイド*』を参照してください。

RSA SecurID による認証

RSA SecurID は、2 要素認証メカニズムです。この認証メカニズムには主に次の 3 つのコンポーネントが含まれています。

- RSA SecurID 認証トークン (ハードウェア ベースまたはソフトウェア ベース)。ワンタイムの認証コードを生成します。
- RSA SecurID サーバ (認証マネージャ)
- RSA 認証エージェント

RSA SecurID 認証トークンおよびコード

各 RSA SecurID トークンには、工場出荷時にコード化される固有の「シード」が含まれます。トークンはこのシードを使用し、決められた間隔 (たとえば、60 秒) で認証コードを生成します。内蔵の時計および固有のシードにより、認証コードが定期的に変更されます。トークンの時計とサーバの時計は同期されています。サーバも、トークンと同じ間隔で認証コードを生成します。生成された認証コードは PIN 番号と組み合わせられ、こうしてセキュアな認証が可能となります。

RSA SecurID サーバ

ユーザ名とパスコードにより、ユーザは RSA SecurID サーバで認証されます。パスコードとは、トークンに表示される認証コードと PIN を組み合わせたものです (前述を参照)。

トークンを最初に使用する場合、新しい PIN を選択するように求められます。また、サーバは、定期的に、または、トークンとサーバが「ドリフト」すると、新しい時間同期 PIN を要求します。ドリフトが 3 分を超えると、サーバはユーザに対し、トークンが次に生成する認証コードを入力するように求め、トークンの所持を確認します。次の認証モードは、同じクロック ドリフトが使用されるため、サーバはトークンが有効であることを確認します。

RSA SecurID エージェント

この認証は、ユーザ名とパスコードを使用した標準の認証方式に似ていますが、パスコードは単純な文字ではありません。トークンの認証コードとユーザが知っている PIN とを組み合わせた数値です。

RSA SecurID は次の 2 つの方法で利用できます。

- EAP-RSA ベースの認証 - 現行で実装中
- ネイティブ SecurID 認証 - 今回は使用しません

RSA SecurID の設定

RSA サーバとコントローラ間の通信は、コントローラと他の RADIUS サーバ (IAS またはフリーの RADIUS) 間の通信と同じです。違うのは、RSA サーバに対するクライアント認証方法が 2 要素認証によるということです。フォーティネットはこの方式に対応しています。CLI コマンド radius-profile を使用し、コントローラ上の RSA サーバを設定します。たとえば、次のように入力します。

```
default# configure terminal
default(config)# radius-profile <RSA>
default(config-radius)# ip-address <IP of the RSA server>
default(config-radius)# key secure-secret
default(config-radius)# exit
```

MAC フィルタリングの設定

MAC フィルタリングは、指定の MAC アドレスに基づいてアクセスを許可あるいは拒否することで、ユーザステーションから WLAN へのアクセスを制御します。MAC アドレスは、IEEE 802 準拠のネットワークデバイスごとに固有です。802.11 ワイヤレス ネットワークでは、WLAN へのアクセスが試行された場合に特定のステーションのワイヤレス NIC カードに割り当てられている MAC アドレスを許可あるいは拒否することで、ネットワーク アクセスを制御できます。

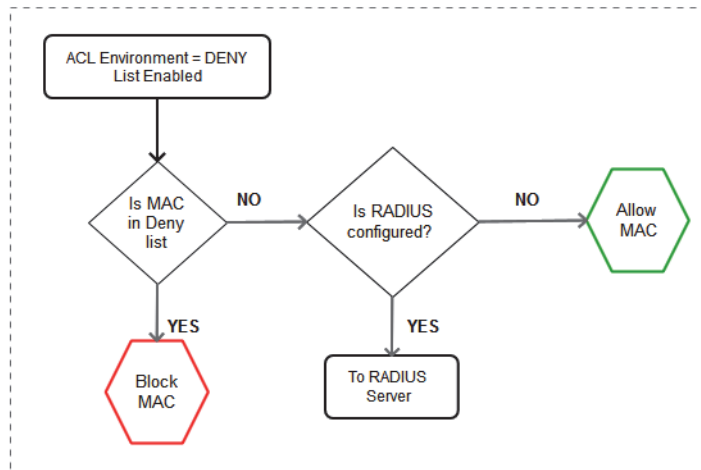
ワイヤレス LAN システムでは、以下の方法を使用した MAC フィルタリングが可能です。

- コントローラのローカルでフィルタリングする方法。MAC アドレスに基づいて特定のステーションに対してアクセスを許可または拒否するアクセスコントロール リスト (Access Control List: ACL) を管理することで、フィルタリングを実現します。MAC フィルタリングには、以下の 2 つの ACL を利用できます。
 - 許可 ACL。この許可リストに載っている MAC アドレスのみにアクセスを限定する。
 - 拒否 ACL。この拒否リストに載っているアドレス (クライアント) へのアクセスを却下する。

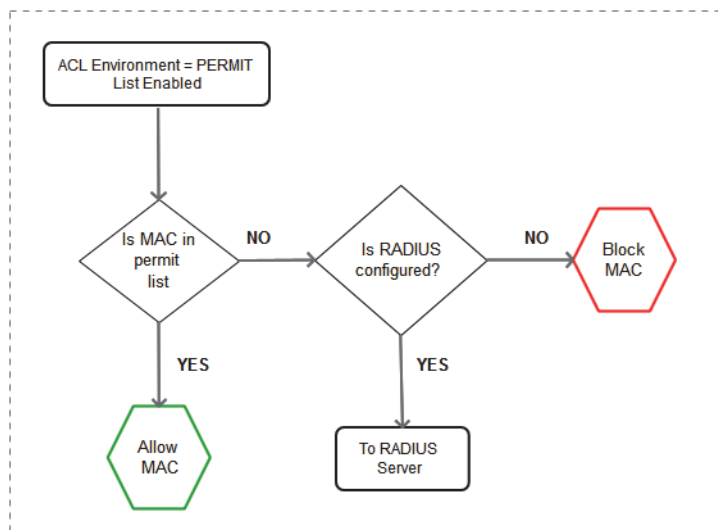
以下のフローチャートは、MAC フィルタリングの動作を示しています。

MAC フィルタリングの動作

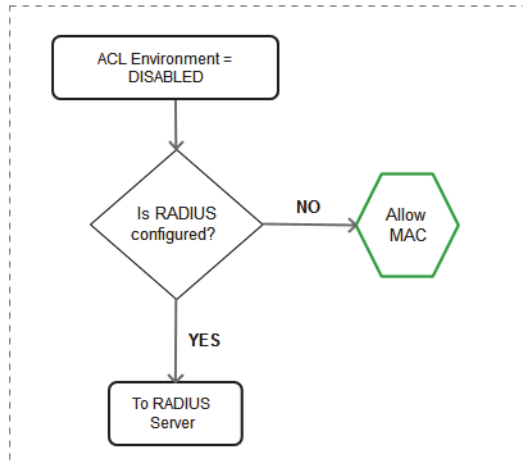
ACL 環境で拒否リストが有効になっている場合



ACL 環境で許可リストが有効になっている場合



ACL 環境が無効になっている場合



ローカルのアクセス / 拒否 ACL への変更は、リアルタイムで実装されます。

- リモートの、MAC アドレスを設定するためのアクセス権限が設定されている RADIUS サーバと連携したフィルタリング。ユーザ認証は「[RADIUS 認証](#)」に記載された手順で行われますが、ユーザの妥当性評価には MAC アドレスが使用されます。コントローラの拒否 ACL が有効になっていると、その拒否リストに載っているアドレス

は、RADIUS サーバの MAC アドレスよりも優先されます。RADIUS サーバ上の MAC アドレスへの変更は、リアルタイムでは実装されません。

- MAC フィルタを関連するセキュリティ プロファイルで有効または無効にできる ESS では、MAC フィルタ設定をコントローラまたは RADIUS サーバで無効にします。

MAC フィルタリング オプションに設定された状態によって、使用されるアクセスのタイプが決まり、また、ローカルの MAC フィルタリングが RADIUS サーバの状態よりも優先されます。

- コントローラの ACL 管理において有効な状態は、以下のとおりです。
 - disabled : (デフォルト) MAC アドレスが含まれている場合であっても、許可 ACL と拒否 ACL のどちらもアクティブではない状態
 - permit : 許可 ACL は有効で、拒否 ACL (存在する場合) は無効の状態
 - deny : 拒否 ACL は有効で、許可 ACL (存在する場合) は無効の状態
- リモート RADIUS サーバの管理において有効な状態は、以下のとおりです。
 - enabled
 - disabled

これらのコントローラと RADIUS サーバの設定を以下の表にまとめます。

	RADIUS Server Setting	
	disabled	enabled
MAC Filtering disabled	no MAC filtering	RADIUS MAC filtering only
Permit ACL enabled	allow client in Permit list only	check Permit list first; if not in Permit list, check RADIUS server
Deny ACL enabled	Deny list used only	if not in Deny list, check RADIUS server

MAC フィルタリングの設定

MAC フィルタリングは、コントローラおよび RADIUS サーバの両方で設定できます。デフォルトでは、MAC フィルタリングは無効になっています。MAC アドレスを追加する前に、MAC フィルタリングを有効にします。MAC フィルタリングは次の機能を提供します。

- セキュリティ プロファイル単位で適用する。

- 許可リストと拒否リストを同時に使用する。
- 許可リストと拒否リストの両方に同じ MAC アドレスを指定する。
- グローバルな許可リストと拒否リストと、ESS レベルごとの RADIUS ベースの MAC フィルタリングを同時に使用する。

MAC フィルタリングの状態を変更して許可リストを有効にするには、`mac-filter-state permit` コマンドを使用します。

許可 ACL リストにアドレスを追加するには、コマンドの引数としてアドレスを指定するか、準備しておいたリストからインポートします。1 つ以上の MAC アドレスを許可アクセス コントロール リストに追加するには、次のように入力します。

```
controller(config)# access-list permit 00:40:96:51:eb:2b 00:40:96:51:eb:22
controller(config-acl-permit)# descr MyClient
controller(config-acl-permit)# end
```

MAC アドレスのリストを許可 ACL にインポートするには、インポートするすべての MAC アドレスを列挙したテキスト ファイルを作成し、そのテキスト ファイルをインポートします。インポートされるテキスト ファイルを作成する場合は、1 行に 1 つだけの MAC アドレスを 16 進形式 (`xx:xx:xx:xx:xx:xx`) で記述します。たとえば、インポートするテキスト ファイルの内容は以下のようになります。

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
```

テキスト ファイルを作成したら、コントローラの `/images` ディレクトリにそのファイルを送信する必要があります。CLI からは、`copy` コマンドを使用してコントローラにファイルを送信します。`dir` コマンドを使用して、ファイルがコピーされたことを確認します。以下の例は、許可 ACL リストに MAC アドレスを追加する、`acl` という名前のテキスト ファイルをインポートするためのコマンドです。

```
controller(config)# access-list permit import acl

00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
00:0c:e6:bd:01:05
```



```
Successfully Added : 7
Duplicate Entries  : 0
Invalid Format     : 0
Entries Processed  : 7
```



FortiWLC (SD) 7.0-4-0 以降、次のコマンドは廃止されます。

- access-list state
- access-list radius-server

拒否 MAC フィルタリング リストの設定

拒否 ACL をセットアップするには、ACL 拒否状態を有効にしてから、拒否 ACL を設定するか、インポートします。

拒否 ACL は RADIUS アクセスより優先され、ステーションに対するアクセスを直ちに拒否したり、特定のクライアント (たとえば、ウィルスに感染している、あるいは他のデバイスを攻撃するクライアント) をブラックリストに載せることができます。

デフォルトでは、MAC フィルタリングは無効になっています。MAC フィルタリングの状態を変更して拒否リストを有効にするには、`mac-filter-state deny` コマンドを使用します。

拒否 ACL リストにクライアントのアドレスを追加するには、コマンドの引数として指定するか、準備しておいたリストからインポートします。このコマンドは、これらをコマンドの引数として指定し、簡単な説明を入力します。

```
controller(config)# access-list deny 00:40:96:51:eb:2b 00:40:96:51:eb:10
controller(config-acl-deny)# descr DenyStation
controller(config-acl-deny)# end
controller(config)#
```

拒否する MAC アドレスのリストをインポートするには、インポートするすべての MAC アドレスを列挙したテキスト ファイルを作成し、そのテキスト ファイルをインポートします。インポートされるテキスト ファイルを作成する場合は、1 行に 1 つだけの MAC アドレス を 16 進形式 (xx:xx:xx:xx:xx:xx) で記述します。たとえば、インポートするテキスト ファイルの内容は以下のようになります。

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
```

インポート用のテキスト ファイルを作成したら、CLI の copy コマンドを使用して、ファイルをコントローラの /images ディレクトリに送信します。dir コマンドを使用して、ファイルがコピーされたことを確認します。次に、ファイルをインポートします。

次の例では、MAC アドレスを拒否 ACL リストに追加する `denyacl` という名前のテキスト ファイルをインポートしています。

```
controller(config)# access-list deny import denyacl
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41

Successfully Added : 6
Duplicate Entries   : 0
Invalid Format      : 0
Entries Processed  : 6
```



ACL 環境が許可から拒否に変更された場合、アクティブな接続は切断されません。ただし、次の接続で MAC エントリは拒否または許可リストに対してフィルタされます。

MAC フィルタリング用のリモート RADIUS サーバの設定

RADIUS サーバの MAC フィルタリングが有効になると、ステーション MAC アドレスは、リモートの RADIUS サーバによって設定され管理されます。新しいステーションが WLAN にアクセスしようとする、コントローラは RADIUS サーバに MAC アドレスを問い合わせ、クライアントが許可されているかどうか判断します。RADIUS サーバから応答がない場合、あるいはクライアントは許可されていないと応答した場合、クライアントは WLAN への侵入を阻止されます。

CLI からの RADIUS サーバの設定には、セキュリティ プロファイルで `mac-filter-radius-server` コマンドを使用し、プライマリ (およびオプションでセカンダリ) RADIUS サーバ (IP アドレス、シークレット キー、ポート、認証テーブルの中での MAC アドレス間の区切り文字を含む) の設定プロファイルを指定します。

この RADIUS サーバは、次のいずれかの状況でのみ使用されます。

- ACL 環境で拒否リストが設定され、MAC エントリが拒否リストに含まれていない場合に、パケットが RADIUS サーバに転送される。
- ACL 環境で許可リストが設定され、MAC エントリが許可リストに含まれていない場合に、パケットが RADIUS サーバに転送される。

RADIUS プロファイルの設定に関する詳細は、235 ページの「[CLI での 802.1X RADIUS セキュリティの設定](#)」を参照してください。

MAC フィルタ用のセキュリティ プロファイルの設定

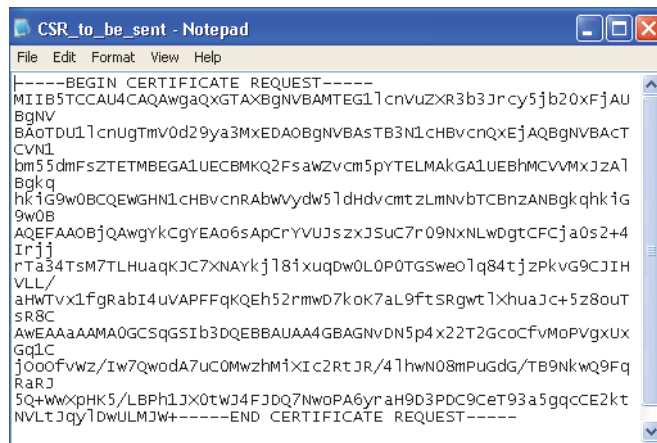
MAC フィルタリング設定をオフまたはオンにする設定により、セキュリティ プロファイルごとの制御が提供されます。たとえば、コントローラベースの MAC フィルタリングや RADIUS サーバの MAC フィルタリングが有効になっている場合は no macfiltering コマンドにより ESS のこれらの設定が無効になります。グローバル MAC フィルタを再度有効にするには、macfiltering コマンドを使用します。

セキュリティ証明書

証明書により、認証局 (CA) によって検証されたセキュリティ保証が提供されます。この章では、証明書の取得と利用のプロセスについて説明します。カスタム証明書を正しく動作させるには、証明書だけではなく、ルート CA までのすべての発行者の証明書の信頼チェーン全体をインポートする必要があります ([図 46](#) を参照)。

サーバ証明書は、特定の CSR を基準に生成されます ([図 45](#) を参照)。サーバ証明書と一緒に、信頼チェーン全体を取得する必要があります ([図 46](#) を参照)。

図 45: CA に送信される CSR の例



```
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIIB5TCCAUI4CAQAwgaQxGTAXBgNVBAMTEG1cnvuzXR3b3Jrcy5jb20xZjAu
BgnV
BA0TDU1lcuUgTmV0d29ya3MxEDA0BgNVBAStB3N1cHBvcnQxZjAQBgNVBAcT
CVN1
bm55dmFsZTETMBEGA1UECBMKQ2FsaWZvcml5pYELMAkGA1UEBhMCVVMxJzA1
Bgkq
hk1G9w0BCQEWGHN1cHBvcnRAbWVydW5ldHdvcm51dHdvcm51dHdvcm51dHdv
9w0B
AQEFAA0BjQAwGykCgYEAo6sApCrYVUJ5sZJSUC7r09NXLWdgtCFCfja0s2+4
Irjj
rTa34TSM7TLHuaqKJC7XNAYkj18ixuqDw0L0P0TGSwEo1q84tjzPkvG9CJ1H
VLL/
aHwTvx1fgRabI4uvAPFFqKQEH52rmwD7koK7aL9ftSRgtw1XhuaJc+5z8out
SR8C
AwEAAaAAMA0GCSqGSIb3DQEBBAAUAA4GBAGNVdN5p4x22T2GcoCfvm0PVgxUx
Gq1C
j0o0Fvwz/Iw7QwodA7uCOMwzhm1XiC2RtJR/41hwn08mpUGdG/TB9NkwQ9Fq
RaRJ
5Q+wwxpHK5/LBPh1JX0tWJ4FJDQ7Nw0PA6yrAH9D3PDC9CeT93a5gqcCE2kt
NVLTJqy1DwULMJW+-----END CERTIFICATE REQUEST-----
```

図 46: CA によって返される証明書の例 (サーバ、中間、およびルート)



証明書の署名要求 (CSR) は Web UI を使用してコントローラで直接生成してください。

コントローラでの CSR の生成

証明書要求を作成するには、証明書を必要とするコントローラで以下の手順を実行します。

1. [Configuration] > [Certificates] > [Controller Certificates] をクリックします。[Controller Certificate] ウィンドウが表示されます。
2. [Add] をクリックします。[Certificate Add] ウィンドウが表示されます。
3. このウィンドウで必要な情報を入力します。
4. [Apply] をクリックします。
5. CSR が生成され、ウィンドウに表示されます。
6. この証明書 PEM を、送信可能なフォームに張り付けるためにコピーするか、[Save] をクリックして、ファイルとして CSR を保存します。
7. [Close] をクリックします。
8. CSR を証明書の発行者に送信して処理します。CA によってオペレーティング システムのタイプを尋ねられたら、[Open SSL] (利用可能な場合) または [Other] を選択します。



証明書を要求する場合、ユーザ タイプは [admin] ではなく、[Web User] に設定する必要があります。間違ったユーザ タイプを指定すると、証明書を使用できなくなります。

証明書のエントリが [Server Certificates] ページの [Pending CSR] に表示されます。このエントリは、CA から送られインポートする証明書に一致します。これによって、証明書を要求したコントローラが唯一の証明書の使用者になるようにします。

ワイルドカード証明書の生成

SD では、トンネルおよびブリッジモードのキャプティブ ポータルの両方でワイルドカード証明書をサポートします。ワイルドカード証明書要求を作成するには、次の手順を実行します。

1. [Configuration] > [Certificates] > [Controller Certificates] をクリックします。[Controller Certificate] ウィンドウが表示されます。
2. [Add] をクリックします。[Certificate Add] ウィンドウが表示されます。
3. [General] セクションに詳細を入力します。
4. コモン ネームは、[Distinguished Name (DN)] セクションに「*.name」として入力します。たとえば、「*.merunetworks.com」と入力します。



これによって、ワイルドカード証明書が作成されます。「*」の部分は、システムによって、コントローラのホスト名と置き換わります。

5. [Apply] をクリックします。
6. CSR が生成され、ウィンドウに表示されます。
7. この証明書 PEM を、送信可能なフォームに張り付けるためにコピーするか、[Save] をクリックして、ファイルとして CSR を保存します。
8. [Close] をクリックします。
9. CSR を証明書の発行者に送信して処理します。CA によってオペレーティング システムのタイプを尋ねられたら、[Open SSL] (利用可能な場合) または [Other] を選択します。



証明書を要求する場合、ユーザ タイプは [admin] ではなく、[Web User] に設定する必要があります。間違ったユーザ タイプを指定すると、証明書を使用できなくなります。

証明書のエントリが [Server Certificates] ページの [Pending CSR] に表示されます。このエントリは、CA から送られインポートする証明書に一致します。これによって、証明書を要求したコントローラが唯一の証明書の使用者になるようにします。

証明書のインポート

署名済みのサーバ証明書をインストールする前に、必ず、トラスト チェーン内のルート証明書およびすべての中間証明書を追加する必要があります。この順番にインストールを実行しない場合、エラーが発生します。

信頼のあるルート CA および CA から受信したトラスト チェーン全体をインポートするには、次の手順に従います。

1. [Configuration] > [Certificates] > [Trusted Root CA] をクリックします。

2. [Import] をクリックします。
3. ルート CA ファイルに移動して、これを選択します。
4. [Open] をクリックして、証明書に適切なエイリアス名を付けます。
また、テキスト エディタで証明書を開いて、この証明書の PEM テキストをコピーして以下に示す「Certificate PEM」空白テキスト領域に貼り付けることもできます。
5. [Import] をクリックします。
インポートが完了したというメッセージが表示されます。
6. [OK] > [Close] をクリックします。
7. すべての証明書に対して、2 ～ 6 の手順を繰り返します。
これで、すべての証明書がコントローラにインポートされました。
8. [Configuration] > [Certificates] > [Controller Certificates] > [Pending CSR] > [Import] をクリックして、サーバ証明書をインポートします。
9. サーバ証明書へ移動して選択し、[Import] > [Open] > [Import] をクリックします。
10. [OK] > [Close] > [Close] をクリックします。
11. [Maintenance] > [Reboot System] に移動して、ウィンドウ上部にある [Reboot Controller] をオンにして、Web サーバを再起動します。[Reboot] をクリックして、アクションを実行します。

これで証明書のインポートが終了しました。

サーバ証明書をアプリケーションに割り当てる

証明書は、セキュリティ上の目的（つまり RADIUS の終了など）に加え、キャプティブ ポータルや Web 管理ツールで使用するために使用できます。サーバ証明書を割り当てるには、次の手順に従います。

1. [Controller Certificates] の表にある証明書を選択します。
2. [Applications] をクリックします。[Applications] ダイアログが表示されます。

図 47: 証明書を使用するアプリケーション

Application	Certificate
Web Administration & Management Application	--Default--
Captive Portal	--Default--
Security	--Default--
VPN	enggwifimain
WAPI	--Default--
VPN Client	--Default--

Save Cancel

3. ドロップダウン メニューを使用して、証明書を使用するアプリケーションを指定します。
4. [Apply] をクリックします。
5. [Close] をクリックします。
6. 証明書が適用され正しく有効化されていることを確認するには、システムの CLI から reload-security コマンドを使用します。

キャプティブ ポータルまたは管理アプリケーションで使用する証明書の割り当てを完了したら、Apache Web Server を再起動する必要があります。

AP 証明書

VPN アプリケーションでは、AP とコントローラ間の通信を安全にするために、セキュリティ証明書を AP とコントローラの両方にインストールする必要があります。次のセクションの指示に従って、AP で VPN 接続を正しくセットアップします。



一部の AP モデルでは、証明書があらかじめインストールされており、生成の必要がない場合があります。お使いの AP が VPN AP の表にすでに「Certificate Installed」と表示されている場合には (264 ページの「VPN AP の追加」を参照)、このプロセスを実施する必要はありません。

AP CSR の生成

AP 証明書をインストールする前に、その AP 用の証明書の署名要求 (CSR) を FortiWLC (SD) Web UI で生成する必要があります。次の手順を実行して、使用する AP 向けの CSR を作成して送信します。

1. Web UI から、[Configuration] > [Certificates] > [AP Certificates] に移動します。[AP Certificates] の表が表示されます。

図 48: AP 証明書の表

Certificate Management										
Trusted Root CA			Controller Certificates			AP Certificates				
	AP ID	AP Name	Serial Number	Operational State	Availability Status	AP Model	Certificate Status	User Req Status	CA	Validity (MM/DD/YYYY)
<input type="radio"/>	154	Jonky-AP-154	00:0c:e6:11:25:ed	Disabled	Offline	AP832e	---	None		-
<input type="radio"/>	156	Popov-AP-156	00:0c:e6:11:25:f5	Disabled	Offline	AP832e	---	None		-
<input type="radio"/>	160	Duy-AP-160	00:0c:e6:11:24:d1	Enabled	Online	AP832i	Not-Installed	None		-
<input type="radio"/>	163	KK-AP-163	00:0c:e6:11:26:59	Disabled	Offline	AP832e	---	None		-
<input type="radio"/>	167	AP-167	00:0c:e6:0d:ee:a9	Enabled	Online	AP332i	Not-Installed	None		-
<input type="radio"/>	169	AP-169	00:0c:e6:0d:ef:71	Disabled	Offline	AP332e	---	None		-
<input type="radio"/>	170	AP-170	00:0c:e6:0d:ef:87	Disabled	Offline	AP332e	---	None		-
<input type="radio"/>	172	AP-172	00:0c:e6:11:24:a7	Enabled	Online	AP832e	Not-Installed	None		-

2. AP の表で AP を選択して、[Create CSR] をクリックします。[CSR] ダイアログが表示されます。

図 49: CSR の設定

Certificate Signing Request - AP Certificate

Common Name: 00:0c:e6:11:24:d1 (AP MAC Address)

Validity: (1 - 3650 days)

Apply

Close

3. 表示されるダイアログの [Valid Till] フィールドでは、証明書の有効期間を指定します。証明書の有効期間の日数を入力して、[Apply] をクリックします。
AP の表は、CSR の生成が進行するときに、何度か更新されます。[User Req Status] 列に、「CSR Generation in Progress」から「CSR Generated」までの進捗が表示されます。列が更新されない場合は、[Refresh] をクリックします。
4. 「CSR Generated」が表示される場合、CSR をエクスポートする準備が整っており、認証局に送信できます。

CSR のエクスポート

CSR が生成されると、個々のファイルにエクスポートでき、検証用に認証局のサーバに提出できます。

1. AP 証明書の表で、選択していないのであれば、AP をクリックし、[Export] をクリックします。
2. ローカル マシンにエクスポートしたファイルをダウンロードします。
3. エクスポートしたファイルを認証局のサーバにアップロードします。サーバから次の 2 つのファイルが戻されます。

- CSR を使用して生成された AP 証明書
- ルート CA 証明書



証明書を要求する場合、ユーザタイプは `[admin]` ではなく、`[Web User]` に設定する必要があります。間違ったユーザタイプを指定すると、証明書を使用できなくなります。

認証局の信頼されるルート CA 証明書をシステムにインストールしてない場合は、この章の **255 ページ**の「[証明書のインポート](#)」で説明した手順に従ってインストールしてください。この操作は、AP に証明書をインストールする前に実行する必要があります。

AP 証明書のインストール

前のすべての手順を完了したら、AP に証明書をインストールする準備が整っています。

1. AP 証明書の表 ([Configuration] > [Certificates] > [AP Certificates]) で、AP を選択して、[Import] をクリックします。
2. 表示されるポップアップ ウィンドウで、証明書のエイリアス名を指定のフィールドに入力します。
3. [Choose File] をクリックして、認証局から提供された AP 証明書を参照します。
4. [Save] をクリックします。数秒後、「Certificate imported successfully」というメッセージが表示され、[Certificate Status] 列には、「Cert Installed」と表示されます。これらのメッセージが正しく表示されない場合は、[Refresh] をクリックして、表を更新します。

AP の証明書がインストールされ、使用できる状態になりました。



VPN を使用するように AP を設定および配備する前に、すべての AP に AP 証明書をインストールすることを推奨します。すべての証明書をインストールしたら、その後の手順は **263 ページ**の「[VPN の設定](#)」を参照してください。

証明書に関するトラブルシューティング

証明書のプロセスでは、以下のエラーが発生する可能性があります。

エラー メッセージ	原因	問題の解決方法
Certificate file is not a valid x.509 certificate (証明書ファイルは有効な x.509 証明書ではありません)	証明書ファイルが壊れているか、X.509 証明書 (PEM/DER) ファイルではありません。	有効な X.509 証明書ファイルへ移動します。
Certificate has expired or not yet valid (証明書の有効期限が切れているか、まだ有効ではありません)	証明書は、開始日 (Valid From) と 終了日 (Valid To) で示される特定の期間に有効となります。その証明書は、現時点で有効ではありません。	証明書の開始日 (Valid From) と 終了日 (Valid To) の範囲が正しいかどうか確認します。 証明書の開始日がまだ先の場合は、開始日が来てから証明書をインポートします。証明書の有効期限が切れている場合は、新しい証明書を CA から発行してもらいます。
Certificate alias name already exists (証明書のエイリアス名が既に存在します)	同一のエイリアス名を持つ別の証明書が既にインポートされています。	別のエイリアス名を使用します。
Certificate already exists (with either same alias name or different alias name) ([同一のエイリアス名を持つ、または、別のエイリアス名を持つ] 証明書が既に存在します)	証明書が既にインポートされています。	何も実行しません。
Certificate Public key verification failed (証明書の公開キーの検証に失敗しました)	証明書の CSR エイリアス名とは異なるエイリアス名を選択しました。	この証明書の CSR を作成する際に使用したエイリアス名を選択します。
Certificates Issuers verification failed (証明書発行者の検証に失敗しました)	信頼できるルート CA のリストにおいて、発行者の証明書 (トラスト チェーン式) を使用できません。最も一般的な原因として、最初に中間証明書またはサーバ証明書をインポートしようとしたことが挙げられます。	トラスト チェーンにある信頼できるルート CA の証明書を先にインポートします。 その後に、サーバ証明書をインポートします。

WAPI 設定

WLAN Authentication および Privacy Infrastructure (WAPI) は、WLAN の中国国家標準です。WAPI 機能で使用する認証モデルには、証明書ベースと PSK ベースの 2 つがあります。WAPI 証明書の構成では、コントローラに中央認証サービス装置 (ASU) の IP およびポート通信の詳細が必要であり、これによって、ワイヤレス通信を許可されます。

FortiWLC (SD) では、WAPI 設定をリリース 5.2 以降で実装しています。

WAPI 認証モードの指定

上記のように、ユーザは、導入環境で証明書ベースまたは PSK ベースの WAPI 承認を使用するかを指定できます。これはセキュリティ プロファイル設定から実行します。

1. Web UI で、[Configuration] > [Security] > [Profile] に移動します。
2. [Add] ボタンをクリックして、新しいプロファイルを作成します。
3. [L2 Modes Allowed] セクションで、WAPI オプションを指定します。
 - [WAI] : 証明書ベースのモデル
 - [WAI-PSK] : PSK のモデル



[Data Encrypt] フィールドの **[WPI-SMS4]** オプションは、いずれかの WAI オプションを使用して選択するときに、自動的に選択されます。

4. その他の選択項目に記入します。PSK オプションを使用している場合、[Pre-shared Key] フィールドに適切なエントリを設定してください。

導入環境で証明書ベースの WAI オプションを使用する場合、WAPI サーバを設定して、WAPI 証明書をインポートする必要があります。これらの詳細については、次のセクションに進んでください。

WAPI 証明書のインポート

WAPI 通信を適切に承認するために、証明書をシステムにインポートする必要があります。以下の手順に従ってください。

1. Web UI から、[Configuration] > [Certificates] > [Controller Certificates] に移動します。
2. [WAPI Cert Import] をクリックします。
3. WAPI 証明書の場所を確認して、[Import] をクリックします。一度に設定できる WAPI 証明書は 1 つです。
4. 証明書をインポートしたら、[WebTerm] リンクをクリックして、CLI コンソールを開きます。

5. コンソールにログインして、`reload-wapi` コマンドを実行して、WAPI サービスをリロードします。
6. 次のセクションに進んで、WAPI Authentication Service Unit との通信を設定します。

WAPI サーバの設定

WAPI サーバは、証明書ベースの WAI 認証を使用する場合にのみ、設定する必要があります。この設定は、WAPI 証明書がシステムにインポートされた後に、認証するために使用されます。

WAPI サーバを設定するには、次の手順に従います。

1. Web UI から、[Configuration] > [Security] > [WAPI Server] に移動します。
2. 次の情報を入力します。
 - WAPI Server IP : Authentication Service Unit の IP アドレス。
 - WAPI Server Port : WAPI 通信に使用するポート番号を入力します (デフォルト : 3810)。

Palo Alto Networks Firewall との統合

FortiWLC (SD) は、Palo Alto Networks Firewall ソリューションの User ID Agent ソリューションを Syslog ベースで組み込むことができます。これによって、Palo Alto Firewall でユーザがネットワークにログインするときのファイアウォール ルールをセットアップできます。

VPN 接続の設定

System Director のバージョン 5.2 以降では、ユーザは、サポートされている AP を設定して、VPN 接続を介して企業のコントローラに接続することができ、安全なリモート ワイヤレス信号を実現できます。これは、通信アプリケーションで使用できます。ユーザは、別のインターネットにアクセスできる場所への VPN アクセスが設定されている AP を使用して、企業ネットワークへの安全な回線を素早くセットアップできます。VPN 実装では、コントローラは TLS/SSL VPN サーバとして動作し、AP は TLS/SSL VPN クライアントとして動作します。

AP で VPN アクセスを設定するには、コントローラの AP テーブルに格納できるように、企業ネットワークに最初に接続する必要があります。AP の安全な VPN 接続では、セキュリティ証明書を使用する必要があります。一部の AP モデルでは、証明書があらかじめインストールされていますが、ユーザが自分で証明書をインストールする必要がある AP もあります。次の

セクションでは、VPN 接続を設定し、VPN アクセスのために AP を追加する方法について説明します。



VPN 機能は、現在 AP110、AP332e、AP332i、AP832、822、FAP-U421EV、FAP-U423EV、および AP1014i モデルで利用可能であり、すべての物理および仮想コントローラでサポートされています。

VPN 用にコントローラの証明書を有効化する

証明書がコントローラにインストールされている場合 (キャプティブ ポータルのアクセスについては [254 ページの「CA によって返される証明書の例 \(サーバ、中間、およびルート \) コントローラでの CSR の生成」](#) を参照)、同じ証明書を VPN アクセスに使用できますが、VPN 接続を許可する前に、使用できるように設定する必要があります。

VPN で使用できるように証明書を有効にするには、次の手順に従います。

3. Web UI から、[Configuration] > [Certificates] > [Controller Certificates] に移動します。
[Controller Certificates] の表が表示されます。
4. 証明書を選択して、[Used By...] をクリックします。アプリケーションのリストが表示されます。
5. [VPN] をクリックして、VPN で使用できるように証明書を有効にします。
6. 変更を反映するには、CLI からコマンドを実行する必要があるというメッセージが表示されます。次のようにコマンドを実行します。
 - Web UI の右上にある [WebTerm] リンクをクリックします。
 - コントローラの証明書を使用してログインします。
 - reload-vpn と入力して、Enter を押します。VPN サービスが再起動します。



これでコントローラの証明書が追加されました。必要なすべての AP セキュリティ証明書を追加してインストールすることを推奨します。次の順番で操作を実行すると、VPN を適切に導入できます。AP 証明書のインストール方法については、[257 ページの「AP 証明書」](#) を参照してください。

VPN の設定

特定の AP を設定する前に、システム管理者はコントローラで VPN 接続設定を最初に設定する必要があります。

VPN を設定するには、次の手順に従います。

1. Web UI から、[Configuration] > [Security] > [VPN Server] に移動します。[VPN Configuration] 画面が表示されます

図 50: VPN の設定

VPN Configuration

VPN Server

VPN APs

Status

☐ Enable ☒ Disable

VPN Server IP/Name

10.136.0.25

Controller's publicly reachable IP address or hostname (FQDN format)

VPN Server Port

1194

Valid range: [0-65535]

IP Pool

192

168

0

0

Netmask

255

255

0

0

(255.255.0.0 - 255.255.255.248)

2. VPN サーバの設定を入力します。詳細は次の表を参照してください。

フィールド	説明
[Status]	[Enable] または [Disable] に設定できます。[Enable] (有効) にすると、VPN サーバがアクティブになります。デフォルトでは無効です。
[VPN Server IP/Name]	VPN サーバで使用される IP アドレスや DNS 名を入力します。
[VPN Server Port]	VPN 通信で使用されるポートを入力します。デフォルトでは値は 1194 に設定されます。
[IP Pool]	VPN サーバで使用される IP 範囲 (標準の 255.255.255.255 の表記を使用) を入力します。 注: コントローラにアクセスしている IP (つまり、現在のマシンの IP アドレス) がこの範囲に含まれていないことを確認してください。含まれている場合は、VPN が有効化されると、ローカル接続が終了します。 注: IP アドレス 192.168.1.12 は、コントローラによって予約されており、指定された VPN 範囲には入りません。
[Netmask]	VPN サーバのネットマスクを入力します (標準の 255.255.255.255 の表記を使用)。

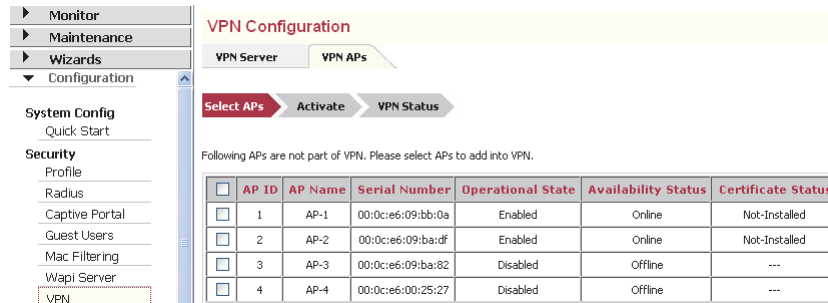
3. [OK] をクリックして、変更を保存します。コントローラは、VPN サービス向けに設定されました。

VPN AP の追加

VPN サーバを構成したら、AP を VPN アクセスに追加できます。この操作を実行するには、次の手順を実行します。

1. VPN の画面 ([Configuration] > [Security] > [VPN Server]) で、[VPN APs] タブをクリックします。画面が更新されます。図 51 を参照してください。

図 51: VPN AP の選択



	AP ID	AP Name	Serial Number	Operational State	Availability Status	Certificate Status
<input type="checkbox"/>	1	AP-1	00:0c:e6:09:bb:0a	Enabled	Online	Not-Installed
<input type="checkbox"/>	2	AP-2	00:0c:e6:09:ba:d9	Enabled	Online	Not-Installed
<input type="checkbox"/>	3	AP-3	00:0c:e6:09:ba:82	Disabled	Offline	---
<input type="checkbox"/>	4	AP-4	00:0c:e6:00:25:27	Disabled	Offline	---

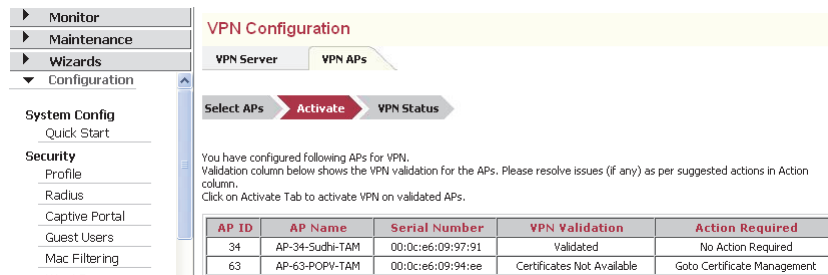
2. VPN アクセスの設定用の AP の横のボックスをオンにして、[Next] をクリックして、[Activate] タブに進みます。

新しいテーブルに、選択した AP の VPN の対応状況が表示されます。AP にすでにセキュリティ証明書がインストールされている場合、このテーブルは追加のアクションが必要がないことを示されます。しかし、選択した AP のいずれかで証明書のインストールが求められる場合、[Action Required] 列に、リンクが表示されます。このリンクから自動的に [Certificates] 画面に移動でき、証明書をインストールできます。図 52 には、2 台の AP が表示されており、1 台には証明書がすでに設定されており、もう 1 台には追加の手順が必要となっています。



AP 証明書のインストール手順については、この章の 257 ページの「AP 証明書」を参照してください。

図 52: 有効化テーブル



AP ID	AP Name	Serial Number	VPN Validation	Action Required
34	AP-34-Sudhi-TAM	00:0c:e6:09:97:91	Validated	No Action Required
63	AP-63-POPY-TAM	00:0c:e6:09:94:ee	Certificates Not Available	Goto Certificate Management

3. [Action Required] 列ですべての AP が「No Action Required」となったら、VPN デバイスを有効化できます。[Activate] をクリックして、[VPN Status] タブに進みます。AP は、自動的に表示され、配備できるようになります。



show vpn-ap CLI コマンドを使用して、VPN アクセスが現在設定されている AP を表示できます。このコマンドは、Web UI の右上にある WebTerm リンクから実行できます。

VPN クライアント接続の設定

VPN AP 接続を許可することに加えて、FortiWLC (SD) を設定して、同じように E(z)RF Network Manager に VPN 接続できます。この設定では、Network Manager アプライアンスが VPN サーバとして動作して、コントローラがクライアントとして動作します。完全な VPN 通信のためには、Network Manager アプライアンスで設定する必要があります。

VPN クライアント接続を設定するには、次の手順を実行します。

1. FortiWLC (SD) Web UI から、[Configuration] > [Security] > [VPN Client] に移動します。
2. [State] ドロップダウンを使用して、[Enable] を選択します。
3. [VPN Server IP] アドレス フィールドで、Network Manager アプライアンスの IP を入力します。VPN コントローラを関連付ける前に、Network Manager デバイスで VPN を設定する必要があります。
4. [VPN Server Port] フィールドに、VPN サービスで使用するポートを入力します。デフォルトでは 1194 です。
5. [OK] をクリックして、変更を保存します。

10 認証

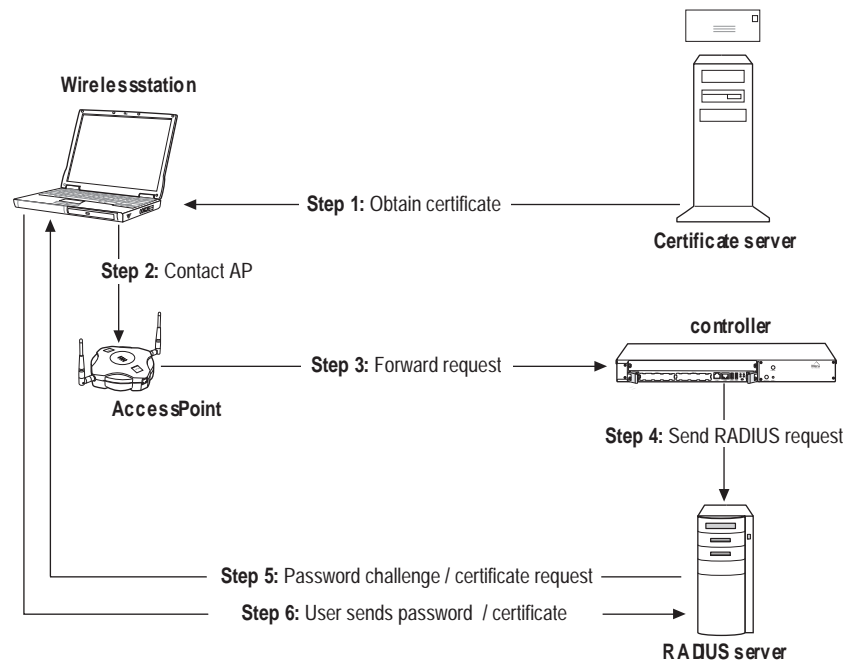
管理者が使用できる認証方法は 3 つあり、ユーザが使用できる認証方法は 2 つあります。管理者の認証には、RADIUS、TACACS+、またはローカル認証を使用します。ユーザの認証には、RADIUS またはローカル認証を使用します。

RADIUS 認証

RADIUS 認証の 802.1X の概念モデル

802.1X 認証の概念モデルは、次のようになります。

図 53: 802.1X RADIUS サーバ認証の概念モデル



00145

802.1X RADIUS 認証は、次のように機能します。

1. EAP タイプによっては、最初にユーザが証明書サーバからデジタル証明書を取得する必要があります。
2. エンドユーザとして EAP を使用し、認証を受けるために AP にコンタクトします。
3. AP がコントローラに要求を転送します。
4. コントローラが RADIUS クライアントとして動作して、RADIUS サーバに要求を送信します。
5. EAP タイプによって決まりますが、RADIUS サーバがエンドユーザにパスワードを要求するか、以前に証明書サーバから取得しておいたデジタル証明書をユーザが提示します。
6. RADIUS サーバがエンドユーザとアクセス ポイントを認証し、そのエンド ユーザからのデータを受け付けるためのポートをオープンします。

Web UI を使用したユーザのための RADIUS 認証の設定



注：RADIUS 認証にはレベル 10 のパーミッションが必要です。

ネットワーク上のゲストや従業員に RADIUS 認証を使用するには、以下の手順を実行します。

1. コントローラの IP アドレスと共有シークレットを RADIUS サーバに追加します。
2. RADIUS プロファイルを作成します (手順 1 と同じ共有シークレットを使用します)。
3. その RADIUS プロファイルをセキュリティ プロファイルに含めます。
4. セキュリティ プロファイルを ESS プロファイルに含めます。

管理者用に RADIUS 認証を設定するプロセスは、これとは異なり、もっと単純です。以下の手順に従い、RADIUS プロファイルを追加します。

1. [Configuration] > [Security] > [RADIUS] をクリックします。
2. 名前、説明、IP アドレス、秘密鍵、ポート番号 (1812 がデフォルトです) を入力します。
3. リストから MAC アドレスの区切り文字 ([Hyphen]、[Single Hyphen] または [Colon]) を選択します。
4. リストからパスワード タイプ ([Shared Key] または [MAC Address]) を選択します。
5. リストから Called Station ID タイプ (デフォルトでは、[MacAddress] または [MacAddress:SSID]) を選択します。
6. CoA ステータスを選択します。この RADIUS サーバからの CoA 要求を処理するには、これを [ON] に設定します。

7. [OK] をクリックします。



ポート 1700 での Cisco ISE からの CoA 要求は、自動的にサポートされます。

いつ RADIUS サーバを使用するのかを指定します。指定する方法は 2 つあります。1 つは、RADIUS プロファイルをコールするためのセキュリティ プロファイルを作成してから、そのセキュリティ プロファイルをコールするための ESS プロファイルを作成する 2 つの手順のプロセスです。このプロセスについては手順 6 と 7 で説明しています。

8. [Configuration] > [Security] > [Profile] をクリックします。このコントローラで作成されたすべてのセキュリティ プロファイルが表示されます。既存のセキュリティ プロファイルを変更して RADIUS サーバを使用するか、新しいセキュリティ プロファイルを追加できます。どちらの場合も、セキュリティ プロファイルには [Primary RADIUS Profile Name] と [Secondary RADIUS Profile Name] のドロップダウン リストが含まれています。設定済みの RADIUS サーバはすべてリストに表示されるため、リストから 1 つ選択できます。

セキュリティ プロファイルを使用する ESS プロファイルを指定します。

9. [Configuration] > [Wireless] > [ESS] をクリックします。このコントローラで作成されたすべての ESS プロファイルが表示されます。既存の ESS プロファイルを変更してセキュリティ プロファイルを使用するか、新しい ESS プロファイルを追加できます。どちらの場合も、[Security Profile Name] のドロップダウンリストが含まれています。そのため、設定済みのセキュリティ プロファイルはすべてリストに表示されるので、リストから 1 つ選択できます。

上記の手順 6 をスキップし、手順 7 の一部として ESS から直接 [Primary Radius Profile Name] と [Secondary Radius Profile Name] を選択することもできます。また、サーバのタイムアウトと再試行回数を設定できます。

- RADIUS サーバのタイムアウト：プライマリ RADIUS サーバで RADIUS 認証が再試行される間隔（秒単位）です。
- RADIUS サーバの再試行回数：プライマリ RADIUS サーバに到達するための試行回数です。再試行回数の上限に達すると、認証ワークフローはセカンダリ サーバに送信されます。すべての新しいクライアントは、セカンダリ RADIUS サーバを介して認証されます。

CoA のサポート

FortiWLC (SD) は、次の CoA (Change of Authorization) メッセージのサポートを提供します。

- 1x およびキャプティブ ポータルのユーザ セッションのみがサポートされます。

- プライマリ / セカンダリ RADIUS プロファイルの両方がサポートされます。
- コントローラは、UDP ポート 3799 で COA メッセージをリスンします。
- COA メッセージのユーザ セッションは、MAC アドレス とユーザ名のいずれか、または両方を使用して識別されます。
- 切断または CoA の要求は、コントローラに設定されているいずれの RADIUS サーバからでも送信できます。
- CoA の要求は UDP 1700 で実行され、これによって Cisco ISE の相互運用が可能になります。
- 切断メッセージについては、ステーション MAC アドレスのみが必要とされます。切断時に、クライアントはネットワークから完全に切断され、そのセッション データ、1x、PMK キャッシュも消去されます。キャプティブ ポータル セッションの場合は、セッション エージング タイマーも消去されます。切断後、クライアントは再接続するためにすべての認証シーケンスを経る必要があります。
- CoA メッセージの送信時は、FilterID の変更のみがサポートされます。

Web UI を使用した管理者のための RADIUS 認証の設定

すべての管理者の RADIUS 認証を設定するには、次の手順に従います。

1. [Configuration] > [User Management] をクリックします。
2. 画面上部の [Authentication Type] で [Radius] を選択します。[図 55](#) を参照してください。
3. 管理者の認証には 3 つのタブ ([RADIUS]、[Tacacs+]、[Local Admins]) があります。[Radius] タブがデフォルトで選択されています。

図 54: ユーザの RADIUS 認証の設定

Authentication Type: ☐ Radius ☒ Tacacs+ ☐ Local

Administrative User Management - Update

Primary RADIUS IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Primary RADIUS Port	<input type="text" value="1812"/> Valid range: [1024-65535]
Primary RADIUS Secret Key	<input type="text"/>
Secondary RADIUS IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Secondary RADIUS Port	<input type="text" value="1812"/> Valid range: [1024-65535]
Secondary RADIUS Secret Key	<input type="text"/>

4. プライマリ RADIUS サーバの IP アドレスを指定します。
5. プライマリ RADIUS ポート番号を指定します。デフォルトは 1812 です。
6. RADIUS サーバアクセスの秘密鍵を指定します。
7. オプションで、セカンダリ RADIUS サーバについて手順 4 ～ 6 を繰り返します。
8. [OK] をクリックします。
9. 次の 3 つのレベルを使用して、RADIUS サーバに管理者を追加します。

1	Operator は、最も低い、デフォルトでもある認証レベルです。Operator は、統計や結果を参照できますが、設定を変更することはできません。
10	Administrators は、一般的な設定の変更も可能ですが、AP やコントローラのアップグレードや Telnet を使用した FortiWLC (SD) バージョンのアップグレードは実行できません。NMS サーバや NTP サーバの設定、システムのパスワード、日付、時刻の変更は実行できません (いずれも、CLI を使用)。管理者を作成することも、コントローラの認証モードを設定することもできません (GUI および CLI)。ライセンスの追加や削除も実行できません。
15	SuperUser 管理者 は、コントローラのすべての設定を実行できます。AP やコントローラを唯一アップグレードでき、Telnet を使用して FortiWLC (SD) バージョンをアップグレードできます。NMS サーバや NTP サーバの設定、システムのパスワード、日付、時刻の変更を実行できます (いずれも、CLI を使用)。また、管理者を作成したり、コントローラの認証モードを設定したりできます (GUI および CLI)。Superuser は、ライセンスを追加、削除できます。

CLI を使用した管理者のための RADIUS 認証の設定

RADIUS 認証モードのすべてのコントローラ管理者を設定するためのコマンドは、次のとおりです。

- authentication mode global
- primary-radius-ip
- primary-radius-port
- primary-radius-secret
- authentication type radius
- secondary-radius-ip
- secondary-radius-port
- secondary-radius-secret

コマンドの詳細については、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。

RADIUS に認証モードを設定する CLI の例

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type radius
ramcntrl(0)(config-auth-mode)# primary-radius-
primary-radius-ip      primary-radius-port  primary-radius-secret
ramcntrl(0)(config-auth-mode)# primary-radius-ip 172.18.1.3
ramcntrl(0)(config-auth-mode)# primary-radius-secret RadiusP
ramcntrl(0)(config-auth-mode)# secondary-radius-
secondary-radius-ip    secondary-radius-port  secondary-radius-secret
ramcntrl(0)(config-auth-mode)# secondary-radius-ip 172.18.1.7
ramcntrl(0)(config-auth-mode)# secondary-radius-secret RadiusS
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit

ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType      : radius
Primary RADIUS IP Address : 172.18.1.3
Primary RADIUS Port : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 172.18.1.7
Secondary RADIUS Port : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
```

RADIUS 認証属性

802.1X の属性

RADIUS 802.1X メッセージ属性は以下のとおりです。

メッセージ : Access-Request

属性 :

- User-Name(1)
- NAS-IP-Adress(4)
- NAS-Port(5)
- Called-Station-Id(30) = <mac of Controller>:<ssid string>

- Calling-Station-Id(31)
- Framed-MTU(12)
- NAS-Port-Type(61) = Wireless-802.11(19)
- Connect-Info(77)
- Message-Authenticator(80)

オプション属性 (EAP タイプにより異なる) :

- EAP-Message(79)
- State(24)

オプション属性 (RADIUS ベースのユーザ管理により異なる)

- Service-Type(6) = Value:Login(1)
- User-Password(2) = Value:<password string>

メッセージ : Access-Accept

属性 :

- Framed-Protocol(7) = PPP(1)
- Service-Type(6) = Framed-User(2)
- Class(25)
- Message-Authenticator(80)

オプション属性 (EAP タイプにより異なる) :

- EAP-Message(79)

オプション属性 (RADIUS が割り当てられた VLAN に必須) :

- Tunnel-Medium-Type(65) = 802(6)
- Tunnel-Type(64) = VLAN(13)
- Tunnel-Private-Group-Id (81) = <the VLAN ID>

オプション属性 (RADIUS ベースのユーザ管理により異なる)

- Filter-Id(11) = Value:<Privilege Level>:<1-15>

クライアントの RADIUS アカウンティング

ネットワークに RADIUS アカウンティング サーバが存在する場合は、コントローラが RADIUS クライアントとして動作するように設定することで、コントローラがアカウンティング レコードを RADIUS アカウンティング サーバへ送信できるようになります。コントローラは、802.1X 認証ユーザとしてワイヤレス ネットワークに入ってきたクライアントに対し

て、あるいはキャプティブ ポータル認証されたクライアントに対して、アカウントینگ レコードを送信します。

RADIUS アカウンティングを使用するときは、RADIUS アカウンティング サーバ用に別の RADIUS プロファイルを設定し、ESS プロファイルをその RADIUS プロファイルに指し示します。たとえば、UDP ポート 1645 または 1812 (RADIUS 認証のための標準ポート) を使用する radiusprofile1 という RADIUS プロファイルが存在していて、セキュリティ プロファイルが radiusprofile1 を指し示しているとします。RADIUS アカウンティングをサポートするには、たとえ RADIUS アカウンティング サーバが RADIUS 認証サーバと同じであったとしても、新しい RADIUS プロファイル (radiusprofile1_acct など) を設定します。IP と鍵を適切に設定し、ポートを正しい RADIUS アカウンティング ポート (1646、1813 など) に設定します。次に、ESS プロファイルがこの新しい RADIUS プロファイル radiusprofile1_acct を指すように設定します。

セッション ID で識別されるクライアント セッションの期間中は、アカウントینگ レコードが送られます。プライマリ RADIUS アカウンティング サーバ用の RADIUS プロファイルと、プライマリ サーバがオフラインになった場合のバックアップとなるセカンダリ RADIUS アカウンティング サーバ用の別の RADIUS プロファイルを設定できます。バックアップの RADIUS サーバへの切り替えは、次のように実行されます。プライマリ RADIUS サーバへのアクセスが 30 秒間失敗すると、セカンダリ RADIUS サーバがデフォルトになります。切り替えのきっかけとなった試行は破棄され、次の RADIUS アクセスがセカンダリ RADIUS サーバに送られます。約 15 分後、アクセスはプライマリ RADIUS サーバに復帰します。

すべての RADIUS メッセージ (開始、暫定アップデート、停止) には、次の属性が含まれます。

表 18: RADIUS アカウンティング属性

RADIUS 属性	説明
Session-ID	Client IP Address-Current Time - RADIUS サーバから返されたセッション時間が優先されます。RADIUS サーバがセッション時間を返さない場合、設定済みの値が使用されます。
Status Type	Accounting Start/Accounting Stop/Interim-Update
Authentication	RADIUS 認証
User-Name	ユーザ名
User-Name	ステーション MAC アドレス (ステーション情報)
NAS-IP Address	コントローラ IP アドレス

表 18: RADIUS アカウンティング属性

RADIUS 属性	説明
NASPort	固有の値 (システムによって生成されます)
Called Station-ID	コントローラ MAC アドレス
Called Station-ID	コントローラ MAC アドレス : ESSID 名 (ステーションがどの ESS に接続できるのかを強制するのに使用されます)
Calling Station-ID	ステーションの MAC アドレス
Connect Info	ステーションの無線バンド
Class	クラス属性
NAS-Identifier	アクセス要求パケットの中のコントローラ (自身) を特定するための任意の文字列。最小値は 3 文字です。
Acct-Input-Octets*	このポート (インターフェイス) で受信し、アカウンティングのステータスタイプが STOP であるときに Accounting-Request で送信されるオクテットの数
Acct-Input-Packets*	このポート (インターフェイス) で受信し、アカウンティングのステータスタイプが STOP であるときに Accounting-Request で送信されるパケットの数
Acct-Output-Packets*	このポート (インターフェイス) で送信され、アカウンティングのステータスタイプが STOP であるときに Accounting-Request で送信されるパケットの数
Acct-Output-Octets*	このポート (インターフェイス) で送信され、アカウンティングのステータスタイプが STOP であるときに Accounting-Request で送信されるオクテットの数
Acct-Terminate-Cause	セッション終了の理由を取得するために使用され、アカウンティングのステータスタイプが STOP であるときに Accounting- Request で送信されます
Acct-Delay-Time	このレコードを送信するまでに待機した秒数を示すために送信されます
AP ID	ベンダ固有の情報 : クライアントの接続先の AP ID。アカウンティングが開始すると送信されます
AP ID	ベンダ固有の情報 : クライアントが接続を切断した AP ID。アカウンティングが停止すると送信されます

表 18: RADIUS アカウンティング属性

RADIUS 属性	説明
AP Name	ベンダ固有の情報クライアントの接続先の AP 名。アカウンティングが開始すると送信されます
AP Name	ベンダ固有の情報：クライアントが接続を切断した AP ID。アカウンティングが停止すると送信されます
Session-Time	セッションの開始から停止までの秒数

表 19: RADIUS 認証属性

RADIUS 属性	説明
User-Name	ユーザ名
NAS-IP-Address	コントローラ IP アドレス
NAS-Port	固有の値 = essid << 11 Sta AID
NAS-Port-Type	認証に使用される物理ポートのタイプ = 19
Called-Station-Id	自身の MAC アドレス : ESSID 名
Called-Station-Id	自身の MAC アドレス
Calling-Station-Id	STA MAC アドレス
Framed-MTU	最大 RADIUS MTU = 1250
Connect-Info	ステーションの無線バンド
VLAN ID	クライアントが接続を試みている先の ESS プロファイルの VLAN ID。802.1x クライアントでのみ有効であり、コントローラで設定されている場合にのみ送信されます
Service-Type	要求されたサービスのタイプを送信 = 8 (認証のみ)
Service-Type	要求されたサービスのタイプを送信 = 1 (ログイン)
User-Password	ユーザ パスワード

表 19: RADIUS 認証属性

RADIUS 属性	説明
Session-Timer	ユーザがネットワークに滞在することができる秒数
Class	RADIUS サーバによって返され、Accounting Request メッセージで送信されます
Vlan-Id	RADIUS サーバによって返される VLAN ID
Filter-Id	ユーザごとのファイアウォール機能 (PEM) と一緒に使用されます。RADIUS 応答ではフィルタ ID として送信される権限レベル (1、10、15)
Message-Authenticator	RADIUS サーバによって返されます
EAP Message	RADIUS サーバによって返されます
Tunnel-Medium-Type	ipv4、ipv6 などの伝送媒体を示します。CP では、VPN が設定されている場合に限り有効です。CP の場合には Access-Request でも送信されます。
Tunnel-Type	トンネルのタイプ。この場合は 13 などの VLAN となります。その他のものを受信した場合は、ACCESS-REJECT として扱います。CP では、VPN が設定されている場合に限り有効です。CP の場合には Access-Request でも送信されません。
Tunnel-Private-Group	この属性から VLAN ID を受信します (キャプティブ ポータルには適用されません)
Framed-Compression	現在使用されている圧縮プロトコルを示します。この場合は [NONE] です
Idle-Timeout	クライアントのアイドル時間を計算し、クライアントを停止するために使用します。

キャプティブ ポータルのための RADIUS アカウンティングの設定

277 ページの「[キャプティブ ポータルのための RADIUS アカウンティングの設定](#)」を参照してください。

RADIUS ベースの ESS プロファイル制限

この機能により、コントローラは RADIUS ベースの ESS プロファイルを介して接続を試みるワイヤレス クライアントを制限できるようになります。クライアントは、RADIUS Accept メッセージが戻されると、特定の SSID のみに接続できます。

このシステムでは、1 つの RADIUS サーバおよび複数の ESS プロファイルが存在し、802.1X セキュリティでこの RADIUS サーバが使用されます。RSSID 機能がない場合、RADIUS サーバ内でプロビジョニングされるすべてのワイヤレス クライアントは、すべての ESS プロファイル、そしてすべての関連付けられた VLAN に接続されます。SSID 制限により、RADIUS サーバをこれらの各ワイヤレス クライアントに対して設定できます。これらのワイヤレス クライアントは、接続可能な SSID を指定します。

ユーザは RADIUS サーバを使用し、SSID 接続を制限できます。制限には RADIUS Accept メッセージ内で VSA が使用されます。SSID の条件には以下の 3 つがあります。

RADIUS RADIUS サーバが送信	結果
受け入れ可能な SSID のリストはありません	接続が受け入れられます
ID を含む受け入れ可能な SSID のリスト	接続が受け入れられます
ID を含まない受け入れ可能な SSID のリスト	接続が受け入れられません

RADIUS サーバは、ペンダ コード 9 および属性番号 1 を Access-Accept (アクセス許可) メッセージに含んだ状態で、許可された SSID をペンダ固有の属性 (VSA) で戻す必要があります。属性値は文字列形式である必要があります。

文字列は ssid=<ssid-string> である必要があり、<ssid-string> は実際の SSID (ESSID と呼ばれます) に置き換えられます。

複数の許可された SSID が表示されたリストが使用された場合、各 SSID を、異なる属性インスタンスに置きます。属性の順序は問われません。ステーションが接続を試みている SSID が RADIUS サーバにより戻された SSID ではない場合、ステーションはアクセスを拒否されます。この機能には、関連付けられた CLI や Web UI コマンドはありません。RADIUS が、許可された SSID のリストを使用して応答した場合、リストを使用してユーザを処理し制限します。

リモート RADIUS サーバ

本社 (またはマスタ データセンター - DC) から物理的に離れたリモート サイトを含むネットワークの実装では、各リモート サイトでリモート RADIUS サーバを使用して、ローカルの認証を実行できます。

一般的なシナリオでは、RADIUS サーバは DC に共同配置されます。ローカル クライアントの認証に AAA サービスを必要とするリモート サイトは、DC の RADIUS サーバを使用します。これによって、リモート サイトと DC の間の遅延が大きくなるなどの問題が発生することがよくあります。リモート サイト内に RADIUS サーバを配備することで、この問題が緩和

され、リモート サイトやブランチは DC に依存せずにローカルの AAA サービス (RADIUS) を使用できます。

事前準備

リモート RADIUS サーバの配備を開始する前に、次の点に注意してください。

1. コントローラとサイトの AP 通信時間が RADIUS のタイムアウトよりも短いことを確認します。
2. リレー AP として設定可能な AP を少なくとも 1 つプロビジョニングする必要があります。
3. リレー AP として設定可能な AP は、L3 モードの Fortinet 11ac AP (AP122、AP822、AP832、および OAP832) だけです。
4. WAN のサバイバビリティについては、新しい 802.1x RADIUS クライアントは、リレー AP がコントローラを再検出するまで参加できません。

仕組み

この機能は、リモート サイトでセットアップされた RADIUS サーバを使用するローカル認証 (.1x、キャプティブ ポータル、および MAC フィルタリング) サービスを提供します。RADIUS サーバに加えて、リモート サイトは Fortinet 11ac AP をリレー AP として設定する必要もあります。リモート RADIUS プロファイルは、コントローラの WebUI ([Configuration] > [RADIUS]) または CLI を使用して ESS ごとに作成できます。リモート RADIUS プロファイルは通常のプロファイルと同様に機能し、プライマリおよびセカンダリの RADIUS 認証およびアカウンティングサーバとして使用できます。



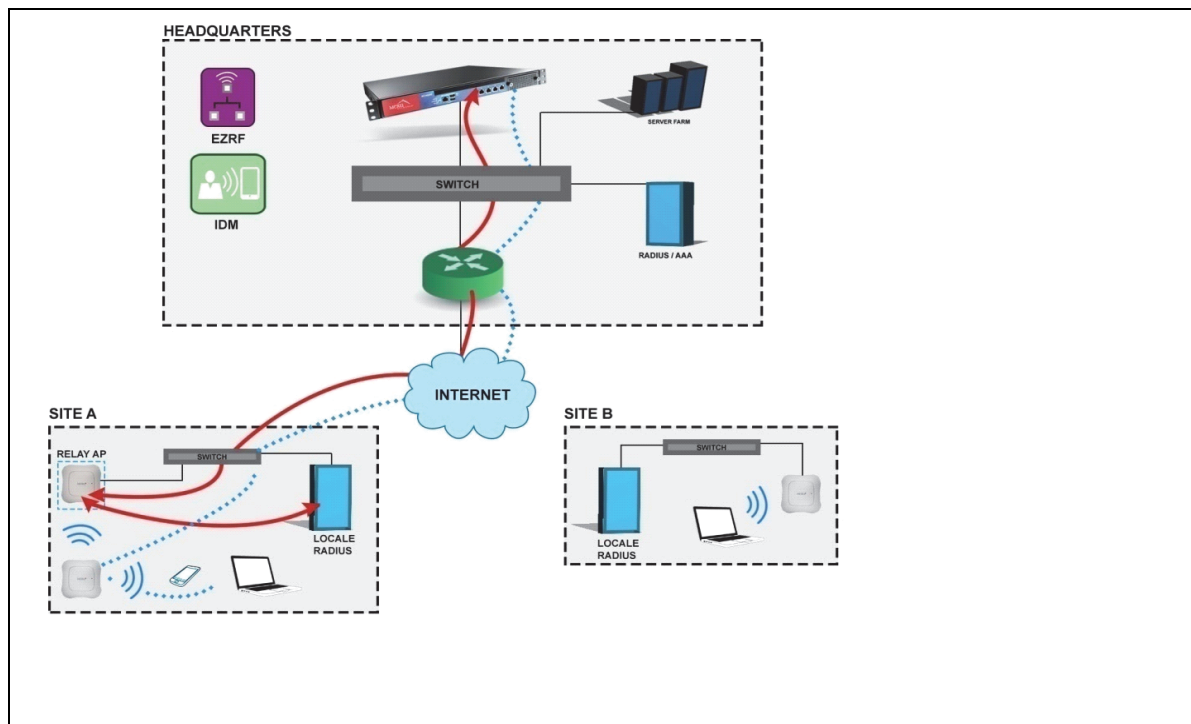
リモート サイトと DC の間の遅延が大きくなると、クライアントが切断されたり、ネットワークの動作が遅くなったりすることがあります。

リレー AP について

- リレー AP は、主として (リモート サイトの) RADIUS サーバと本社のコントローラの間で通信に使用されます。
- AP がリレー AP として設定されるのは、RAIDUS プロファイルで割り当てられた場合のみです。AP をリレー AP として指定した場合は、クライアント WLAN サービスによってリレー AP の負荷を増大させないようにしてください。負荷が大きくなると、リレー AP と DC の通信で問題が生じることがあります。通常クライアント WLAN サービスについては、別のフォーティネット アクセス ポイントを使用することをお勧めします。
- リモート RAIDUS プロファイルについては、セカンダリのリレー AP を設定することはできません。しかし、耐障害性を高めるため、代替 (バックアップ) の RADIUS プロファイルを設定し、このバックアップ RAIDUS プロファイルへのリレー AP として別の AP を

指定することをお勧めします。セキュリティ プロファイルで、この RADIUS プロファイル
をセカンダリ RADIUS サーバとして設定します。

次の図は、RADIUS をローカルで配備する単純なシナリオを示しています。



Web UI を使用した設定

Web UI を使用してリモート RADIUS を設定するには、次の手順を実行します。

[Configuration] > [RADIUS] > [RADIUS Configuration Table - ADD] ページに移動して、
[Remote Radius Server] を [ON] に設定します (下図の 1 を参照)。

リレー AP として使用する AP ([Remote Radius Relay ApId]) を選択します (下図の 2 を参照)。

CLI を使用した設定

```
# configure terminal
```

```
(config)# radius-profile RemoteRadius
```

```
(config-radius)# remote-radius-server on
```

```
(config-radius)# radius-relay-apid XXX
```

XXX は、リモート サイトでのリレー AP の AP ID です。

```
# configure terminal
```

```
(config)# radius-profile RemoteRadius
```

```
(config-radius)# no remote-radius-server
```

```
# show radius-profile <remoteRadius-profile-name>
```

例

```
# show radius-profile site-a
```

RADIUS Configuration Table

RADIUS Profile Name : site-a

Description : Remote radius profile for Site-A

RADIUS IP : 172.18.1.8

RADIUS Secret : *****

RADIUS Port : 1812

Remote Radius Server : on
Remote Radius Relay ApId : 2
MAC Address Delimiter : hyphen
Password Type : shared-secret
Called-Station-ID Type : default
Owner : controller
COA : on

TACACS+ 認証

Terminal Access Controller Access-Control System Plus (TACACS+) は、ネットワーク上の TACACS+ サーバで実行されるリモート認証プロトコルであり、RADIUS 認証に似ています。ただし、この 2 つの認証には違いがいくつかあります。RADIUS は認証と承認を 1 つのユーザ プロファイルで組み合わせますが、TACACS+ は認証と承認の操作を切り離します。もう 1 つの違いは、TACACS+ は TCP ポート 49 を使用し、RADIUS は UDP ポート 1812 を使用する点です。FortiWLC (SD) は TACACS+ 認証をサポートしますが、アカウントिंगはサポートしません。FortiWLC (SD) は RADIUS 認証とアカウントिंगの両方をサポートします。TACACS+ 認証では Cisco ACS サーバのみがサポートされています。

現在の GUI ウィンドウでのアクティビティに必要な TACACS+ レベル (15 (superuser)、10 (admin)、1 (user)) は、ヘルプに一覧表示されます。FortiWLC (SD) の任意の GUI ウィンドウで [Help] をクリックします。CLI の場合、すべてのコマンド リストには必要な認証レベルも含まれています。この認証レベルは、リリース 5.1 から RADIUS 認証とローカル管理者認証の両方で使用されるようになっています。TACACS+ は実際には 8 つのレベルを提供していますが、フォーティネットでは本書で説明している 3 つの認証レベルのみを使用しています。使用する 3 つのレベルは次のとおりです。

- | | |
|---|---|
| 1 | Operator は、最も低い、デフォルトでもある認証レベルです。Operator は、統計や結果を参照できますが、設定を変更することはできません。 |
|---|---|

10	Administrators は、一般的な設定の変更も可能ですが、AP やコントローラのアップグレードや Telnet を使用した FortiWLC (SD) バージョンのアップグレードは実行できません。NMS サーバや NTP サーバの設定、システムのパスワード、日付、時刻の変更は実行できません (いずれも、CLI を使用)。管理アカウントを作成することも、コントローラの認証モードを設定することもできません (GUI および CLI)。ライセンスの追加や削除も実行できません。
15	SuperUser 管理者 は、コントローラのすべての設定を実行できます。AP やコントローラを唯一アップグレードでき、Telnet を使用して FortiWLC (SD) バージョンをアップグレードできます。NMS サーバや NTP サーバの設定、システムのパスワード、日付、時刻の変更を実行できます (いずれも、CLI を使用)。また、管理者を作成したり、コントローラの認証モードを設定したりできます (GUI および CLI)。Superuser は、ライセンスを追加、削除できます。

CLI を使用した TACACS+ 認証モードの設定

FortiWLC (SD) 4.1 では、Cisco ACS サーバのすべての管理者の TACACS+ 認証モードを設定する新しいコマンドが追加されました。

- authentication mode global
- primary-tacacs-ip
- primary-tacacs-port
- primary-tacacs-secret
- authentication type tacacs+
- secondary-tacacs-ip
- secondary-tacacs-port
- secondary-tacacs-secret

コマンドの詳細については、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。

TACACS+ に認証モードを設定する CLI の例

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type tacacs+
ramcntrl(0)(config-auth-mode)# primary-tacacs-
primary-tacacs-ip      primary-tacacs-port      primary-tacacs-secret
ramcntrl(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.5
ramcntrl(0)(config-auth-mode)# primary-tacacs-secret TacacsP
ramcntrl(0)(config-auth-mode)# secondary-tacacs-
secondary-tacacs-ip      secondary-tacacs-port      secondary-tacacs-secret
ramcntrl(0)(config-auth-mode)# secondary-tacacs-ip 172.18.1.10
```

```

ramcntrl(0)(config-auth-mode)# secondary-tacacs-secret TacacsS
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType          : tacacs+
Primary RADIUS IP Address  : 172.18.1.3
Primary RADIUS Port        : 1812
Primary RADIUS Secret Key  : *****
Secondary RADIUS IP Address : 172.18.1.7
Secondary RADIUS Port       : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address  : 172.18.1.5
Primary TACACS+ Port        : 49
Primary TACACS+ Secret Key  : *****
Secondary TACACS+ IP Address : 172.18.1.10
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#

```

コマンドの詳細については、『*FortiWLC (SD) コマンドリファレンス*』を参照してください。

Web UI を使用した TACACS+ 認証モードの設定

Cisco ACS サーバですべての管理者の TACACS+ 認証を設定するには、次の手順を実行します。

1. [Configuration] > [User Management] をクリックします。
2. 画面上部の [Authentication Type] で [Tacacs+] を選択します。
3. 管理者の認証 ([図 55](#) を参照) には 3 つのタブ ([RADIUS]、[Tacacs+]、[Local Admins]) があります。[Tacacs+] タブをクリックします。

図 55: 管理者の認証の設定

Authentication Type: ☐ Radius ☒ Tacacs+ ☐ Local

Administrative User Management - Update

Primary TACACS+ IP Address

192

168

101

247

Primary TACACS+ Port

49

Valid range: [0-65535]

Primary TACACS+ Secret Key

●●●●●●●●

Secondary TACACS+ IP Address

0

0

0

0

Secondary TACACS+ Port

49

Valid range: [0-65535]

Secondary TACACS+ Secret Key

4. プライマリ TACACS+ サーバの IP アドレスを指定します。
5. プライマリ TACACS+ ポート番号を指定します。デフォルトは 49 です。
6. TACACS+ サーバ アクセスの秘密鍵を指定します。
7. オプションで、セカンダリ TACACS+ サーバについて手順 4 ～ 6 を繰り返します。
8. [OK] をクリックします。
9. 次の 3 つのレベルを使用して、TACACS+ サーバに管理者を追加します。

1	Operator は、最も低い、デフォルトでもある認証レベルです。Operator は、統計や結果を参照できますが、設定を変更することはできません。
10	Admininstrators は、一般的な設定の変更も可能ですが、AP やコントローラのアップグレードや Telnet を使用した FortiWLC (SD) バージョンのアップグレードは実行できません。NMS サーバや NTP サーバの設定、システムのパスワード、日付、時刻の変更は実行できません (いずれも、CLI を使用)。管理者を作成することも、コントローラの認証モードを設定することもできません (GUI および CLI)。ライセンスの追加や削除も実行できません。
15	SuperUser 管理者は、コントローラのすべての設定を実行できます。AP やコントローラを唯一アップグレードでき、Telnet を使用して FortiWLC (SD) バージョンをアップグレードできます。NMS サーバや NTP サーバの設定、システムのパスワード、日付、時刻の変更を実行できます (いずれも、CLI を使用)。また、管理者を作成したり、コントローラの認証モードを設定したりできます (GUI および CLI)。Superuser は、ライセンスを追加、削除できます。

ローカル管理者認証

ローカル管理者の認証はコントローラ上で実行され、RADIUS や TACACS+ と同じ 3 つの権限レベル (15 (superuser)、10 (admin)、1 (user)) が使用されます。管理者がローカル認証を使用している場合には、RADIUS および TACACS+ は使用できません。

CLI を使用したローカル認証モードの管理者の設定

リリース 4.1 で新しく追加された次のコマンドを CLI で使用して、ローカル管理者を設定します。

- authentication-mode global
- authentication-type local
- local-admin
- password
- privilege-level
- show local admins

コマンドの詳細については、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。

ローカル管理者を設定する CLI の例

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type local
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType           : local
Primary RADIUS IP Address   : 0.0.0.0
Primary RADIUS Port         : 1812
Primary RADIUS Secret Key   : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port       : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address  : 0.0.0.0
Primary TACACS+ Port        : 49
Primary TACACS+ Secret Key  : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
ramcntrl(0)(config)# local-admin LocalUser
ramcntrl(0)(config-local-admin)# privilege-level 15
```

```
ramcntrl(0)(config-local-admin)# password LocalUser
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)
```

Web UI を使用したローカル認証の設定と管理者の追加

管理者のローカル認証を設定し、オプションでローカル管理者を追加するには、次の手順を実行します。

1. [Configuration] > [User Management] をクリックします。
2. 画面上部の [Local] ラジオ ボタンを選択します。

実際にローカル管理者を追加するには、手順 3 に進みます。

3. 管理者の認証 (図 55 を参照) には 3 つのタブ ([RADIUS]、[Tacacs+]、[Local Admins]) があります。[Local Admin] タブをクリックします。
4. [Add] をクリックします。[Local Admins - Add] ウィンドウが表示されます (図 56 を参照)。

図 56: 管理者のローカル認証の設定

Authentication Type : ☐ Radius ☐ 'Tacacs+' ☒ Local

Local Admins (empty)

Radius	Tacacs+	Local Admins
--------	---------	--------------

User Name	Privilege Level
-----------	-----------------

5. ローカル管理者のユーザ名を入力します。
6. 同じローカル管理者のパスワードを入力します。
7. 権限レベル (15 (Superuser)、10 (Admin)、または 1 (Operator)) を入力します。各レベルについては、以下で説明しています。
8. [OK] をクリックします。

802.1X 認証

802.11 規格における認証では、ユーザやステーションの識別よりも、ワイヤレス LAN の接続に重点が置かれています。ユーザ数が数百から数千程度の企業のワイヤレス環境のセキュリティにおいては、802.11 で規定された WEP タイプに加えて、あるいは、TKIP/CCMP-AES と 802.1X 認証が組み込まれている WPA/WPA2 を使用することで、集中化されたユーザ認証の強制的な使用をサポートする認証フレームワークを使用する必要があります。

IEEE 802.1X の使用は、保護されたネットワークへのユーザ トラフィックを認証し、制御するための効果的なフレームワークとなると共に、WPA/WPA2 が設定されている場合であれば、動的な異なる暗号化キーを提供します。802.1X は、EAP (Extensible Authentication Protocol: 拡張認証プロトコル) と呼ばれるプロトコルを有線とワイヤレスの両方の LAN のメディアに結び付け、トークンカード、Kerberos、ワンタイム パスワード、証明書、公開キー認証などの複数の認証方法をサポートします。

802.1X の構成要素

802.1X 認証には、以下の 3 つの基本要素が関係しています。

1. サプリカント - ワイヤレス ステーション上で稼動するソフトウェア クライアント
2. 認証機器 - アクセス ポイントとコントローラ
3. 認証サーバ - 認証データベース。通常は、Cisco ACS、Steel-Belted RADIUS サーバ (Juniper)、または Microsoft IAS のような RADIUS サーバ

EAP (拡張認証プロトコル) は、サプリカント (ワイヤレス ステーション) と認証サーバ (RADIUS、MS IAS など) との間で認証情報を渡すために使用されます。実際の認証は、EAP タイプによって定義され、処理されます。アクセス ポイント (および、そのアクセス ポイントの設定内のコントローラ) が、認証機器として動作します。認証機器はサーバのクライアントで、サプリカントと認証サーバに通信の許可を与えます。

EAP タイプについて

選択する EAP タイプと、認証を導入するかどうかについては、必要とするセキュリティのレベルによって異なります。最も一般的に導入されているいくつかの EAP 認証タイプを以下に示します。コントローラは、これらすべてをサポートしています。

- EAP-TLS
- EAP-PEAP
- EAP-TTLS
- Cisco LEAP

EAP-TLS

EAP-TLS (Transport Layer Security) は、クライアントとネットワークの間の、証明書ベースの双方向認証を提供します。認証には、クライアントとサーバの証明書を使用します。また、ユーザ ベース、セッション ベースの暗号化キーを動的に生成して、WLAN クライアントとアクセス ポイントの間の後続の通信のセキュリティを確保するために使用することもできます。この種の認証メカニズムでは、ユーザとコンピュータの証明書を保管し、配布するために、管理者が証明書サーバをインストールする必要があります。ワイヤレス クライアントが

WLAN を使用しようとする前に、各クライアントに証明書がダウンロードされ、インストールされる必要があります。規模が大きい WLAN 環境では、これは厄介な作業です。

EAP-TTLS (Tunneled Transport Layer Security)

EAP-TTLS (Tunneled Transport Layer Security) は、EAP-TLS の拡張機能として、Funk Software と Certicom によって開発されました。この方法は、暗号化されたチャネル (すなわちトンネル) を使用して、証明書ベースの、クライアントとネットワークの双方向認証を提供します。また、ユーザベース、セッションベースの暗号化キーを動的に生成するための手段も提供します。EAP-TLS とは異なり、EAP-TTLS はサーバ側の証明書のみを必要とします。

LEAP (Lightweight Extensible Authentication Protocol)

LEAP (Lightweight Extensible Authentication Protocol) は、主に Cisco Aironet WLAN で使用される EAP 認証タイプです。動的に生成した WEB キーを使ってデータ転送を暗号化し、双方向認証をサポートしています。Cisco は最近になって LEAP のライセンスを多くの会社に許可するようになったため、Cisco 以外でも LEAP を利用できるようになりました。

PEAP (Protected Extensible Authentication Protocol)

PEAP (Protected Extensible Authentication Protocol) は、802.11 ワイヤレス ネットワーク経由で、認証データを安全に転送する方法を提供します。これには、パスワードベースの旧式のプロトコルも含まれます。PEAP では、PEAP クライアントと認証サーバとの間のトンネリングを使用して、これを実現しています。競合する TTLS (Tunneled Transport Layer Security) と同様、PEAP は、サーバ側の証明書だけを使用してワイヤレス LAN クライアントを認証するため、セキュアなワイヤレス LAN の導入と管理が簡素化されます。Microsoft、Cisco、RSA Security が PEAP を開発しました。最近になって、Cisco の LEAP 認証サーバである ACS に PEAP のサポートが追加されました。

802.1X EAP タイプ 特徴 / 利点	MD5	TLS	TTLS	PEAP	LEAP
クライアント証明書が必要か	X	○	X	X	X
サーバ証明書が必要か	X	○	○	○	X
WEP キー管理	X	○	○	○	○
提供元	Microsoft	Microsoft	Funk	MS	Cisco
認証属性	一方向	双方向	双方向	双方向	双方向
導入の難易	低	高	中	中	中
ワイヤレス セキュリティ	最低	最高	高	高	高

上記の認証メカニズムに関する注意点を以下に示します。

1. MD5 は、一般的には一方向認証のみを提供するために使用されることはありません。MD5 は WEP キーの自動配布とローテーションをサポートしていないため、手動での WEP キーのメンテナンス作業の解消には役立ちません。
2. TLS は極めて高いセキュリティを提供していますが、管理者が各ワイヤレス ステーションにクライアント証明書をインストールする必要があります。ネットワーク管理者からみれば、PKI インフラのメンテナンスのための時間と作業が増えることになります。
3. TTLS では TLS のトンネリングによって証明書の問題が解決されるため、クライアント側に証明書を置く必要がなくなります。TTLS が選択される理由として多いのが、この点です。TTLS は Funk Software が強く推進している方式で、サブリカントと認証サーバソフトウェアに対する使用料が発生します。
4. LEAP には最も長い歴史があります。以前は Cisco 独自の仕様でしたが、現在は Cisco がこのソフトウェアのライセンスを供与しているため、他のベンダのワイヤレス LAN アダプタも LEAP をサポートするようになってきています。
5. 最近の PEAP は、クライアント側に証明書が必要ないという点で、EAPTTLS と同じように動作します。Cisco と Microsoft が PEAP を支持し、Microsoft からは追加費用なしで入手できます。LEAP から PEAP へ移行したい場合には、Cisco の ACS 認証サーバが両方をサポートしています。

11 キャプティブ ポータル

あるユーザ グループに制限付きのワイヤレス アクセスを提供する場合には、キャプティブ ポータルを使用します。キャプティブ ポータルとは、ネットワークでテンポラリ ユーザを隔離するための機能であり、企業におけるゲストや、図書館を利用する生徒などのテンポラリ ユーザに対応するための機能です。キャプティブ ポータルが有効な場合は、Secure Socket Layer (SSL、HTTPS と呼ばれます) の HTTP プロトコルによって、ユーザが認証および承認されるまで RADIUS サーバで暗号化されたログイン インターチェンジが提供されます。このインターチェンジでは、DHCP、ARP、および DNS パケットを除くクライアントからのすべてのトラフィックは、アクセスが許可されるまでドロップされます。アクセスが許可されない場合は、ユーザはキャプティブ ポータルのログイン ページから離れることはできません。アクセスが許可されると、ユーザはキャプティブポータル ページから WLAN に入ることができます。本項では、キャプティブ ポータルを実装する方法、およびフォーティネット キャプティブ ポータルの GUI ページをカスタマイズする方法について説明します。ゲストのログインは、デフォルトでは無効化されており、権限レベル 1 (最低レベル) が必要です。291 ページの「[フォーティネット キャプティブ ポータルの設定](#)」を行うことも、307 ページの「[有線クライアントのキャプティブ ポータル \(CP\) 認証](#)」を使用することもできます。

ブリッジ モードのキャプティブ ポータルの詳細については、[フォーティネットのサポートポータル](#)に掲載されている「CP bridged_2013-04_v2」を参照してください。



動的 VLAN の割り当ての RADIUS 属性 (Tunnel-Type、Tunnel- s Medium-Type、および Tunnel-Private-Group-ID、コマンド `vlan support` を参照) は、サポートされておらず、RADIUS 交換の一部として戻される場合は、無視されます。

パススルーを実行する前に、セキュリティ ログギングをオンにする必要があります。また、新しい設定を有効にするためには、セキュリティ ログギングを一度オフにして再びオンにする必要があります。

フォーティネット キャプティブ ポータルの設定

キャプティブ ポータル機能を組み込んで実装するには、次のタスクを実行します。

- [CLI を使用したキャプティブ ポータルの設定](#) (298 ページ)

- 認証について： [キャプティブ ポータル認証のための RADIUS サーバの設定 \(312 ページ\)](#)、
または [ローカルでのキャプティブ ポータル ゲスト ユーザ ID の作成 \(300 ページ\)](#)
- [HTML ページをカスタマイズして自社独自のページを使用する \(オプション\) \(292 ページ\)](#)
- [キャプティブ ポータルの再認証の迂回の設定 \(オプション\) \(303 ページ\)](#)

HTML ページをカスタマイズして自社独自のページを使用する (オプション)

自社のロゴや証明書を使用して、独自のキャプティブ ポータルのログインおよびログイン成功ページを作成する場合は、本項の手順を実行します。フォーティネット Networks が提供しているデフォルトのすべてのキャプティブ ポータル ページを使用する場合には、この操作は不要です (292 ページの [図 57](#) のログイン例を参照)。カスタムの HTML ページを作成する場合には、最大で 4 セットのキャプティブ ポータルのカスタム ログイン ページを作成できます。これらは、Captive Portal 1 から 4 として参照されます。各セットには、6 ファイルが含まれますが、メインのログイン ページと認証成功のページだけをカスタマイズできます。その他の残りの 4 つの HTML ページは、常にデフォルトのページになります。複数のカスタム ファイルを作成する場合、最大で 300 人のローカル ユーザで同じ認証 (RADIUS またはローカル) を使用する必要があります (ユーザは各カスタム ポータルで異なる場合があります)。

図 57: デフォルトのキャプティブ ポータル ログイン ページ



Meru Networks, Inc.

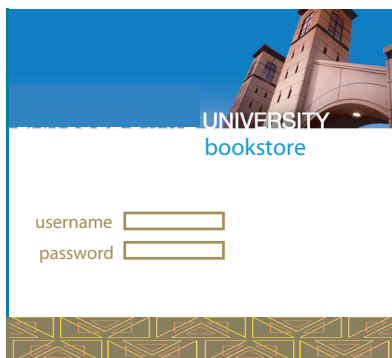
User ID

Password

Login

Copyright © 2004, Meru Networks, Inc. All rights reserved.

図 58: カスタマイズされたキャプティブ ポータル ログイン ページ



デフォルト ページおよび作成したカスタム ポータルの 2 ページ (最大 4 セット) のすべてのカスタム ポータル ページ (HTML、CSS、JS、およびグラフィック) は、同じフォルダにすべて配置されます。そのため、各カスタム ファイルには、一意の名前を必ず指定する必要があります。また、このため、CP1 および CP2 のカスタム ページで使用する CSS ファイルなどのファイルは共有できます。カスタマイズできないすべてのページが、デフォルトの HTML ファイルを使用するのはこのためです。カスタム Web ポータル ファイルの場所は以下のとおりです。

/opt/meru/etc/ws/html.vpn.custom

/opt/meru/etc/ws/Styles.vpn.custom

/opt/meru/etc/ws/Images.vpn.custom

カスタム ページの作成

独自のカスタム ページを作成する最も簡単な方法は、フォーティネット のデフォルト ファイルをダウンロードして、テンプレートとして 2 つのカスタマイズ可能なファイル (ログイン ページと認証成功ページ) を使用し、これらの変更した 2 つの HTML ページに新しい名前を付けることです。以下の手順に従ってください。

1. テンプレート ファイルを入手します。[Maintenance] > [Captive Portal] > [Customization] > [Get Files] をクリックします。

zip.tar.gz という名前の zip ファイルが、コンピュータにダウンロードされます。

zip.tar.gz file を解凍すると、以下のデフォルトの 6 ファイルを含む html.vpn フォルダを確認できます。

- カスタマイズ可能なログイン ページ (デフォルトのファイル名は loginformWebAuth.html)
- カスタマイズ可能なログイン成功ページ (デフォルトのファイル名は auth_web_ok.html)
- ログインが失敗し、再試行が必要であることを伝えるページ (デフォルトのファイル名は loginformWebAuthRetry.html)

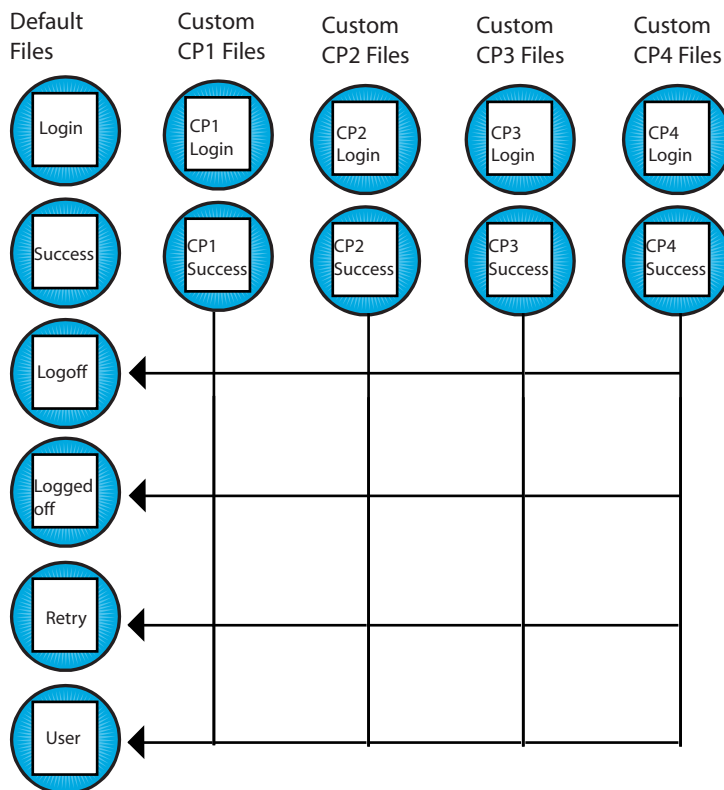
- Web 認証に成功し、ログオフするかどうかを確認するページ (デフォルトのファイル名は logoff User.html)
 - ログオフしたことを伝えるページ (デフォルトのファイル名は loggedoff.html)
 - ログオフが失敗し、再試行が必要であることを伝えるページ (デフォルトのファイル名は logoffUserFailed.html)
2. キャプティブ ポータル インターフェイス 1 つにつき作成できるのは、ログイン ページ loginformWebAuth.html とログイン成功ページ auth_web_ok.html の代替となる 2 つのカスタム ファイルのみです。2 つのカスタマイズ可能な HTML ファイルの場所を確認し、テンプレートとして使用して、カスタム HTML ファイルを作成します。メモ帳などのプログラムを使用して、変更を行い、一意の名前を付けてファイルを保存します。
- CSS、JavaScript、および HTML がサポートされます。
 - .html、.gif、.jpg、.png、.bmp、.css、.js の形式のファイルで最大 50K のグラフィックをアップロードできます。
最初のフォーティネットのロゴのグラフィックを交換するには、次の行を検索してください。
src="Images.vpn/img_merulogo.gif" width=133 border=0></TD>
"Images.vpn/img_merulogo.gif" を "Images.vpn.custom/your_image.gif" に変更します (.gif ファイルの新しいディレクトリには Images.vpn.custom を指定します)。
次の山のグラフィックを交換するには、次の行を検索してください。
src="Images.vpn/img_aboutmeru.jpg" width=326 border=0></TD></TR>
"Images.vpn/img_aboutmeru.jpg" を "Images.vpn.custom/your_image2.gif" に変更します (.gif ファイルの新しいディレクトリには Images.vpn.custom を指定します)。
その他にも、ロゴ、テキスト、フォーマットを編集できます。変更できない行は、loginformWebAuth.html ファイルにあるコントローラと RADIUS サーバ間のログイン通信プロセスです。
3. コントローラに 1 つずつ新しいキャプティブ ポータルのファイル (HTML、CSS、JS、およびグラフィック) をインポートします。[Maintenance] > [Captive Portal] > [Import File] をクリックして、テキスト ボックス [Import File] に場所とファイルを入力します。ファイルの名前が一意であること、同じディレクトリにすべて保存されていることを確認してください。
カスタム ページを使用することをコントローラで指定します。[Configuration] > [Captive Portal] をクリックして、[Customization] ラジオ ボタンをオンにします。

カスタマイズした HTML、CSS、JS、およびグラフィック ファイルがコントローラに配置されました。

4. フォーティネット (Fortinet) という用語を削除したり、残りの 4 つのファイル loginformWebAuthRetry.html、logoff User.html、loggedoff.html、logoffUserFailed.html にその他の変更をする場合、手順 1 でダウンロードしたデフォルトのファイルを変更して手順 3 と同じようにインポートします。ポータル ページの 5 セットすべて (デフォルト、CP1、CP2、CP3、CP4) で、変更したデフォルトのファイルが使用されます。これ

らの 4 つのファイルには、1 つのバージョンしかありません。図 59 を参照してください。

図 59: キャプティブ ポータル HTML ページ (最大)



次に、FortiWLC (SD) でどの状況でカスタム ファイルを使用するかを指定します。「**CLI を使用した新しいカスタム HTML ファイルの実装**」または「**GUI を使用した新しいカスタム HTML ファイルの実装**」を実行します。

CLI を使用した新しいカスタム HTML ファイルの実装

ユーザのどのサブセットに新しいログインおよびログイン成功ページを表示するかを指定し、CLI を使用してカスタム キャプティブ ポータル ページを実装します。このサブネットのユーザがログインすると、対応するカスタム ページが表示されます。一度に最大で 2 セットのキャプティブ ポータル ページを実装できます。たとえば、図書館の学生には、Custom Captive Portal 1 のログインおよびログイン成功ページを表示し、フットボール スタジアムの来訪者には、Custom Captive Portal 2 のログインおよびログイン成功ページを表示することができます。図 59 を参照してください。

どのユーザにどのページを表示するかを決定します。CLI コマンド web custom CaptivePortal[1|2] landing-file-name <landing.html> success-file-name <success.html> を使用して、2つのキャプティブ ポータル ページを指定します。次に、web custom CaptivePortal[1|2] subnet <x.x.x.x> mask <x.x.x.x> を使用して、カスタム キャプティブ ポータル ページを表示するネットワークまたはサブネットを指定します。たとえば、次のように入力します。

```
MC3K-1# configure terminal
MC3K-1(config)# web custom ?
CaptivePortal1      Custom configuration for captive portal 1
CaptivePortal2      (10) Custom configurations for captive portal2.
CaptivePortal3      (10) Custom configurations for captive portal3.
CaptivePortal4      (10) Custom configurations for captive portal4.MC3K-
1(config)# web custom captiveportal2 ?
landing-file-name subnet
MC3K-1(config)# web custom CaptivePortal1 landing-file-name landing.html
success-file-name success.html
MC3K-1 (config) web custom CaptivePortal1 subnet 1.1.1.0 mask 255.255.255.0
MC3K-1(config)# exit
MC3K-1# show web ?
custom              Displays IP range for captive portal custom mode.
custom-area         Lists the files in the custom area for web-auth and
captive portal.
login-page          Displays the type of login page used for web-auth and
captive portal.
MC3K-1# show web custom-area
Html Files
total 16
-rw-rw-rw-   1 root    root      2607 Jul 13 16:26 page2OK.html
-rw-rw-rw-   1 root    root      4412 Jul 13 16:26 page2LOGIN.html
-rwx-----   1 root    root      2607 Jul 13 16:04 auth_web_ok.html
-rw-rw-rw-   1 root    root      4412 Jul 13 16:04 loginformWebAuth.html
-rwx-----   1 root    root         0 Jun 30 00:31 empty.html
Image Files
total 9
-rwx-----   1 root    root         0 Jun 30 00:31 empty.gif
-rw-rw-rw-   1 root    root      8574 Oct 29 2008 Sample.jpg
MC3K-1# show web login-page
custom
```

GUI を使用した新しいカスタム HTML ファイルの実装

最初にキャプティブ ポータルでカスタム HTML ファイルを使用することを指定し、Web UI を使用してカスタム キャプティブ ポータル ページを実装します。これらの HTML ファイルでは、インポートされた CSS、JS およびグラフィック ファイルが参照されます。次に、サブネットとマスクを指定して、新しいログインおよびログイン成功ページを表示する必要がありますユーザのサブセットを指定します。このサブネットのユーザがログインすると、対応す

るカスタム ページが表示されます。たとえば、図書館の学生には、Custom Captive Portal 1 のログイン ページを表示し、フットボール スタジアムの来訪者には、Custom Captive Portal 2 のログイン ページを表示することができます。

次の手順でキャプティブ ポータルでカスタム HTML ファイルを使用することを指定します。

1. [Maintenance] > [Customization] をクリックし、コントローラを選択して [Change Mode] をクリックします。
2. 下方にスクロールして、[Customized] を選択します。

次の手順で、カスタム ページを表示するユーザのサブセットを指定します。

1. [Configuration] > [Security] > [Profile] をクリックして、リストからセキュリティ プロファイルを選択して、必ずセキュリティ ロギングをオンにします。セキュリティ ロギング設定は、セキュリティ プロファイル テーブルの下部付近で行います。キャプティブ ポータル設定を稼働するには、この設定をオンにする必要があります。
2. [Maintenance] > [Captive Portal] > [Custom CP] をクリックします。
[Custom Captive Portal] ページが表示されます。

図 60: [Custom Captive Portal] ページ

Custom Captive Portal

Captive Portal 1:

Login Page

Success Page

Configured Subnets		Add	Delete
	Subnet	Network Mask	

Captive Portal 2:

Login Page

Success Page

Configured Subnets		Add	Delete
	Subnet	Network Mask	

3. CP1 の新しい HTML ログイン ページおよびログイン成功ページの名前を指定します。これらは、現在コントローラにあるため、場所を指定する必要はありません。[Save Page Info] をクリックします。
4. [Add] をクリックし、サブネット IP とネットワーク マスクを指定して、少なくとも 1 つのサブネットを指定し、[OK] をクリックします。このサブネットからユーザがログインすると、これらのカスタム ページが表示されます。
5. [Configuration] > [Security] > [Profile] > [Add] をクリックして、このポータルの対応するセキュリティ プロファイルを作成します。このプロファイルでキャプティブ ポータルの設定を必ず webauth にしてから、保存します。
6. [Configuration] > [Security] > [Captive Portal] をクリックします。このウィンドウで、RADIUS サーバを識別し、セッション、およびアイドル タイムアウトを調整するかどうかを指定します。セッション タイムアウトおよびアイドル タイムアウトは、分で指定します。



[L3 User Session Timeout] フィールドは、スリープ モードに入るときに認証が解除される問題がある特定のクライアントに対して使用されます。このフィールドでは、これらのクライアントがキャプティブ ポータルで認証されている状況からドロップするまで、指定された時間 (分) をメモリに保持することを指定します。

7. [OK] をクリックします。

カスタム HTML ファイルがこれで設定されました。Captive Portal 1、Captive Portal 2、Captive Portal 3、Captive Portal 4 の最大で 4 セットのカスタム ファイルを設定できます。また、デフォルトのファイルを使用することもできます。図 59 を参照してください。

CLI を使用したキャプティブ ポータルの設定

- radius-profile で、プライマリとセカンダリのキャプティブ ポータル認証サーバを定義します。
- accounting-radius-profile で、プライマリとセカンダリのキャプティブ ポータル アカウンティング サーバを定義します。
- captive-portal > activity-timeout で、タイムアウト値を決定します。クライアントが、この時間 (分) を超えてアイドル状態になっている場合、クライアントには再認証が求められます。
- captive-portal > session-timeout で、タイムアウト値を決定します。クライアント セッションがこの時間 (分) を超過すると、クライアントには再認証が求められます。
- change_mac_state
- ssl-server captive-portal-external-URL で、キャプティブ ポータルは指定された URL にあるサードパーティ ソリューションを使用するようになります。
- captive-portal-auth-method で、認証を internal (フォーティネットのデフォルト) または external (サードパーティ ソリューション) に設定します。

キャプティブ ポータル CLI の例

以下の例では、次のタスクを完了することで、CLI でキャプティブ ポータルを設定します。

- ゲスト ユーザ ID (ゲスト) とパスワードを作成します。
- サービスの開始時刻を入力します (01/01/2010 00:00:00)。
- サービスの終了時刻を入力します (01/01/2011 00:00:00)。
- キャプティブ ポータルを表示します。

```
MC3K-1(config)# guest-user ?
<guestname> Enter the name of the guest user.
MC3K-1(config)# guest-user Guest ?
<password> Enter the password of the guest user.
MC3K-1(config)# guest-user Guest XXXXX ?
<start-time> Enter the service start-time (mm/dd/yyyy hh:mm:ss) in double
quotes.
MC3K-1(config)# guest-user Guest XXXXX "01/01/2010 00:00:00" ?
<end-time> Enter service end-time (mm/dd/yyyy hh:mm:ss) in double quotes.
MC3K-1(config)# guest-user Guest XXXXX "01/01/2010 00:00:00" "01/01/2011
00:00:00" ?
<CR>
MC3K-1(config)# guest-user Guest XXXXX "01/01/2010 00:00:00" "01/01/2011
00:00:00"
MC3K-1(config)# exit
MC3K-1#
MC3K-1# show guest-user
Guest User Name Service Start Time          Service End Time
Guest 01/01/2010 00:00:00          01/01/2011 00:00:00
          Guest User Table(1 entry)
```

この項のコマンドは、キャプティブ ポータルの設定方法を示しています。RADIUS サーバ ユーザの設定は、別途実行します。また、これはベンダーによって異なります (利用可能なアプリケーションの情報については、カスタマ サービス Web サイトを確認してください)。クライアント アプリケーションでは、Microsoft Internet Explorer および Netscape 7 ブラウザの両方がサポートされます。

1. WebAuth キャプティブ ポータルのセキュリティ プロファイルを作成します。

```
default# configure terminal
default(config)# security-profile web_auth
default(config-security)# captive-portal webauth
default(config-security)# exit
default(config)# exit
```

2. web_auth Security Profile を ESSID にバインドします。

```
default# configure terminal
default(config)# essid WebAuth-meru-WIFI
```

```
default(config-essid)# security-profile web_auth
default(config-essid)# exit
```

3. プライマリの RADIUS 認証サーバ プロファイルを使用するように SSL サーバを設定します。

```
default(config)# ssl-server radius-profile primary main-auth
default(config)# end
```

4. 設定を保存します。

```
default(config)# copy running-config startup-config
```

ユーザが認証されると、会社の VLAN に移動でき、セッションに QoSRules を適用できます。各ユーザのセッションには、デフォルトでタイムアウト値が設定されています。特に指定しない場合、デフォルトは 33 分になっています。ユーザが接続を解除して、60 秒以内に同じコントローラの同じ SSID に戻って接続する場合は、再認証は要求されません。RADIUS サーバから戻されるセッション時間が優先されます。RADIUS サーバがセッション時間を返さない場合は、設定値が使用されます。

ローカルでのキャプティブ ポータル ゲスト ユーザ ID の作成

RADIUS 認証を使用する代わりに、認証目的でゲスト ユーザ ID をセットアップできます (これは、RADIUS 認証のバックアップになります。RADIUS 認証が失敗すると、このリストが使用されます)。リリース 3.6 以降で、ユーザ ID がサポートされます。ゲスト ID を使用する場合は、[Captive Portal Authentication] フィールドが [Local] に設定されていることを確認してください ([Configuration] > [Security] > [Captive Portal] をクリックします)。

両方のリリースでのゲスト ユーザの機能は以下のとおりです。

ゲスト ユーザの機能	サポート
ユーザ数	300
ユーザの追加 / 削除	○
ユーザ パスワードの変更	○
ログインできる時間	○
ログインできる日	○
ローカル管理者への割り当て	○

CLI の例 - ゲスト ユーザ ID の作成

次の CLI では、Guest という名前のゲスト ユーザを作成しています。

```

MC3K-1 configure terminal
MC3K-1(config)# guest-user ?
<guestname>          Enter the name of the guest user.
MC3K-1(config)# guest-user Guest ?
<password>           Enter the password of the guest user.
MC3K-1(config)# guest-user Guest XXXXX ?
<start-time>         Enter the service start-time (mm/dd/yyyy hh:mm:ss) in
double quotes.
MC3K-1(config)# guest-user Guest XXXXX "01/01/2010 00:00:00" ?
<end-time>           Enter service end-time (mm/dd/yyyy hh:mm:ss) in double
quotes.
MC3K-1(config)# guest-user Guest XXXXX "01/01/2010 00:00:00" "01/01/2011
00:00:00" ?
<CR>
MC3K-1(config)# guest-user Guest XXXXX "01/01/2010 00:00:00" "01/01/2011
00:00:00"
MC3K-1(config)# exit
MC3K-1#
MC3K-1# show guest-user
Guest User Name Service Start TimeService End Time

Guest 01/01/2010 00:00:00 01/01/2011 00:00:00

      Guest User Table(1 entry)
MC3K-1#

```

これは、キャプティブ ポータル ユーザのローカル認証が失敗したときに RADIUS 認証が自動的にチェックされるため、ローカル認証の別のオプションとなります。このオプションは、[Local and RADIUS] と呼ばれます。Web UI で、[Configuration] > [Security] > [Captive Portal] をクリックして、これを設定します。

図 61: ローカルのキャプティブポータル認証には2つのオプションがあります。

▼ Internal Portal Settings

Portal URL

Protocol

☒ https
☐ http

Certificate

--Default--

* Please make sure DNS server has the above redirection URL entry mapped to the Controller's IP address

User Authentication

Authentication Type

radius

Radius Authentication

Primary Profile

NO RADIUS

Secondary Profile

NO RADIUS

Radius Accounting

Primary Profile

NO RADIUS

Secondary Profile

NO RADIUS

*Accounting Interim Interval

600

[600-36000] seconds

User Session

*Session Timeout

0

[0-1440] minutes

*Activity Timeout

0

[0-60] minutes

*Session Caching Time

1

[1-1440] minutes

▼ External Portal Settings

External Portal URL

[0-255] chars

External Portal IP

172

19

241

230

▼ Advanced Settings

Apple Captive Network Assistant (CNA) Bypass

On

これに対応する CLI コマンド `ssl-server captive-portal authentication-type` は、ローカルおよび RADIUS 認証の両方を使用するようにコントローラを設定します。

```

Controller(config)# ssl-server captive-portal authentication-type ?
  local                Set Authentication Type to local.
  local-radius         Set Authentication Type to Local and RADIUS.
  
```

キャプティブ ポータルの再認証の迂回の設定 (オプション)

すべてのユーザやトラフィック タイプをキャプティブ ポータルで認証および承認する必要があります。VPN ソフトウェアのユーザは、認証なしでポータルをパススルーできます。このパススルー ファイアウォール フィルタ ID を有効にするには、次の手順を実行します。

1. [Configuration] > [Security] > [Profile] をクリックします。
2. [Passthrough Firewall Filter ID] に名前を入力します。
3. [Configuration] > [QoS] > [System Settings] をクリックして、[Configuration] メニューの [QosRule] セクションを表示します (パススルー ルールを入力するには PPF ライセンスが必要です)。
4. ルールを追加します。ルールは、入力された順番で保存され、入力されると変更はできません。
5. 画面の下部で、[QoS Filter ID] を入力します。
フィルタの最後のエントリは、その他のすべてのトラフィックをドロップするルールになります。これにより、パススルー以外のトラフィックが、認証なしでキャプティブ ポータルをトラバースすることを禁止できます。

Apple Captive Network Assistant (CNA) の迂回

CNA を迂回または無効化できます。有効にすると、Apple デバイスまたは Android 5.0 以降を実行する Android デバイスを使用したキャプティブ ポータル認証 (トンネル モード) において自動ログインのポップアップが表示されなくなります。

GUI の使用

CNA の迂回を有効にするには、**[Configuration] > [Captive Portal] > [Advanced Settings]** に移動し、[Bypass Apple CNA] で [ON] を選択します。

CLI の使用

ssl-server コマンドで cna-bypass オプションを使用して、CNA の迂回を有効または無効にします。

```
mc3200(15)# configure terminal
master(15)(config)# ssl-server cna-bypass on
master(15)(config)# exit
master(15)# sh ssl-server
```

Captive Portal

Name	: Captive Portal
Server Port	: 10101
User Authentication Protocol	: None
Server Lifetime	: 100
Server IP	: 172.18.34.177
Certificate	:
Authentication Type	: radius
Primary Profile	:
Secondary Profile	:
Primary Profile	:
Secondary Profile	:
Accounting Interim Interval (seconds)	: 600
CaptivePortalSessionTimeout	: 0
CaptivePortalActivityTimeout	: 0
Protocol	: https
Portal URL	:
CaptivePortal External URL	:
CaptivePortal External IP	: 172.18.34.177
L3 User Session Timeout(mins)	: 1
Apple Captive Network Assistant (CNA) Bypass	: on

N+1 構成のキャプティブ ポータル

キャプティブ ポータルの変更は、N + 1 の環境では以下のように反映されます。スレーブがマスタの代わりに稼働するときに、マスタのキャプティブ ポータル ページを使用します。アクティブなスレーブで変更が行われると、変更はマスタには自動的に反映されません。

キャプティブ ポータルのトラブルシューティング

- CaptivePortal1 と CaptivePortal2 には同じサブネットを入力しないでください。このようにすると、CaptivePortal1 で設定されているスプラッシュ ページだけが表示されます。
- カスタム ページは、この機能を使用する前に正しくインポートする必要があります。292 ページの「[HTML ページをカスタマイズして自社独自のページを使用する \(オプション\)](#)」を参照してください。
- コントローラにページと画像が正しくインポートされていることをチェックするには、show web custom-area コマンドを使用します。
- インポートしたページが正しく表示されることを確認するには、CLI `https://<controller ip>/vpn/<page Name>` を使用します。
- キャプティブ ポータル認証が実行されていることを確認するには、キャプティブ ポータル認証時に RADIUS サーバの access-accept メッセージを確認します。
- カスタム キャプティブ ポータル ページを使用しているときでも、デフォルトの 4 つの HTML ファイルが使用されます。カスタマイズできるのは 2 ファイルのみです。これを変更する唯一の方法は、CP1 と CP2 の両方で使用されている 4 つのデフォルト ファイルを変更することです。

キャプティブ ポータル プロファイル

キャプティブ ポータル プロファイル機能を使用すると、異なる設定を持つ個別のキャプティブ ポータル プロファイルを作成できます。このようなキャプティブ ポータル プロファイルをセキュリティ プロファイルにマッピングすることによって、キャプティブ ポータル ユーザのアクセスをより細かく制御できます。

キャプティブ ポータル プロファイルを作成するには、**[Configuration] > [Security] > [Captive Portal]** ページに移動します。**[Captive Portal Profile]** タブを使用して、キャプティブ ポータル プロファイル設定を指定します。作成したキャプティブ プロファイルは、セキュリティ プロファイルで有効にすることができます。次のスクリーンショットは、キャプティブ プロファイルを作成して割り当てるプロセスを示しています。



最大 8 つのキャプティブ プロファイルを作成できます。

1. キャプティブ ポータル プロファイルの作成

Maintenance

Wizards

Configuration

System Config

Quick Start

Security

Profile

RADIUS

Captive Portal

Guest Users

MAC Filtering

WAPI Server

VPN Client

VPN Server

Rogue APs

Wired

VLAN

VLANPOOL

GRE

Ethernet

Port

Wireless

Radio

ESS

Mesh

ServiceControl

Timer

QoS Settings

Devices

System Settings

Controller

APs

AP Group

Antennas

Redirect

Application

DHCP

SNMP

Certificates

Global Settings

Captive Portal Profiles

Search :

No Data

Add Captive Portal Profile

CP Name

Enter 1-32 chars.

User Authentication

Authentication Type

radius

Radius Authentication

Primary Profile

No Radius

Secondary Profile

No Radius

Radius Accounting

Primary Accounting

No Radius

Secondary Accounting

No Radius

Accounting Interim Interval

600

Valid range: [600-36000].

External Portal Settings

External Portal URL

Enter 0-255 chars.

External Portal IP

172.16.10.39

Advanced Settings

Session Timeout

0

Valid range: [0-1440].

Activity Timeout

0

Valid range: [0-60].

Session Caching Time

1

Valid range: [1-1440].

CNA bypass

Off

2. キャプティブ ポータル プロファイルのセキュリティ プロファイルへの指定

Configuration	Profile Name	GP-print
System Config Quick Start Security Profile RADIUS Captive Portal Guest Users MAC Filtering WAPI Server VPN Client VPN Server Rogue APs Wired VLAN VLANPOOL GRE Ethernet Port Wireless Radio RSS	L2 Modes Allowed <input type="checkbox"/> Clear <input type="checkbox"/> WPA2 <input checked="" type="checkbox"/> MIXED_PSK Data Encrypt <input type="checkbox"/> WEP64 <input checked="" type="checkbox"/> CCMP/TKIP Primary RADIUS Profile Name No RADIUS ▼ Secondary RADIUS Profile Name No RADIUS ▼ WEP Key (Alphanumeric/Hexadecimal) Static WEP Key Index 1 Valid range: [1-4] Re-Key Period (seconds) 0 Valid range: [0-65535] BKSA Caching Period (seconds) 43200 Valid range: [0-65535]	<input type="checkbox"/> 802.1x <input type="checkbox"/> WPA2 PSK <input type="checkbox"/> WAI <input type="checkbox"/> WEP128 <input type="checkbox"/> WPI-SMS4 <input type="checkbox"/> Static WE <input type="checkbox"/> MIXED <input type="checkbox"/> WAI PSK <input type="checkbox"/> CCMP-A <input type="checkbox"/> Clear
	Captive Portal WebAuth ▼ Captive Portal profile CP-Guest ▼	

有線クライアントのキャプティブ ポータル (CP) 認証

ポート プロファイル (トンネルおよびブリッジ) により接続する有線クライアントは、外部トラフィックを渡すために CP 認証を必要とします。有線クライアントの CP 認証には、L2 モードに Clear プロファイルが設定されたセキュリティ プロファイル、または L2 モードに 802.1X Clear プロファイルが設定されたセキュリティ プロファイルを使用できます。

サポートされているアクセス ポイント : AP122、AP822v2、AP822、OAP832、AP832、AP332 (メッシュ構成の G1/G2 ポートのみをサポート)、AP433 (メッシュ構成の G1 ポートのみをサポート)、FAP-U421EV、および FAP-U423EV

有線クライアントが外部トラフィックを渡すように設定するには、次の手順を実行します。

1. キャプティブ ポータル (CP) プロファイルを作成します。
2. セキュリティ プロファイルで、CP プロファイルをセキュリティ プロファイルにマッピングします。セキュリティ プロファイルで、少なくとも 1 つのセキュリティ オプション (802.1x、WebAuth、MAC 認証、または CP の迂回) を有効にします。
3. ポート プロファイルで、セキュリティ プロファイルをポート プロファイルにマッピングします。

注 :

- CP 認証は、VLAN トランクが無効になっている場合にのみ使用できます。
- 動的 VLAN はサポートされません。
- リーフ AP に接続する有線クライアントのポート プロファイルは、ブリッジ モードに設定されている必要があります。
- 有線クライアントのポートからイーサネット ケーブルの接続が一度切断され、再接続された場合は、再認証が失敗します。

有線クライアントのステーション ログ

```
2015-Dec-2 14:31:55.075109 | 08:9e:01:28:64:25 | Station Assign | wired
Assigned to <AP_ID=2>(v0)
```

MAC 認証クライアントの CP の迂回

MAC アドレス (MAC フィルタリング) による認証が成功した有線クライアントとワイヤレスクライアントは、キャプティブ ポータル認証クライアントとみなされます。CP の迂回では、RADIUS ベースの MAC フィルタリングとローカルの MAC フィルタリングの両方がサポートされます。ただし、意図的に任意のクライアントをブロックする場合は、そのクライアントの MAC アドレスをローカルの ACL 拒否リストだけに追加します。

CP 認証を迂回するには、セキュリティ プロファイルで次の手順を実行します。

1. 同じセキュリティ プロファイルで、キャプティブ ポータルと MAC フィルタリングを有効にします。
2. MAC 認証クライアントの CP の迂回を有効にします。
3. このセキュリティ プロファイルを ESSID に使用します。

注：

- キャプティブ ポータルを有効にする必要があります。
- MAC フィルタリングの認証が失敗した場合、クライアントは Web 認証にリダイレクトされます。

Captive Portal	WebAuth ▼
Captive Portal profile	local ▼
Captive Portal Authentication Method	internal ▼
802.1X Network Initiation	Off ▼
Tunnel Termination	<input type="checkbox"/> PEAP <input type="checkbox"/> TTLS
Shared Key Authentication	Off ▼
Pre-shared Key (Alphanumeric/Hexadecimal)	<input type="text"/>
Group Keying Interval (seconds)	0 Valid range: [0-65535]
PMK Caching	Off ▼
Key Rotation	Disabled ▼
Reauthentication	Off ▼
MAC Filtering	On ▼
ACL Environment State	Permit List Enabled ▼
MAC Auth Primary RADIUS Profile Name	radius34 ▼
MAC Auth Secondary RADIUS Profile Name	radius37 ▼
MAC Accounting Primary RADIUS Profile Name	radius34AC ▼
MAC Accounting Secondary RADIUS Profile Name	IDAU1721826200 ▼
Firewall Capability	none ▼
Captive Portal Bypass For MAC Authentication	On ▼

CLI を使用した設定

この機能を有効にしたり無効にしたりするには、`captive-portal-bypass-mac` コマンドを使用します。

次のステーション ログは、クライアント ステータスの情報を提供します。

ワイヤレス ステーション: MAC フィルタリングは成功、CP は迂回

```
2016-May- 1 04:24:53.030415 | 00:73:8d:b9:e6:bf | Mac Filtering | Mac in
permit list - accept client
```

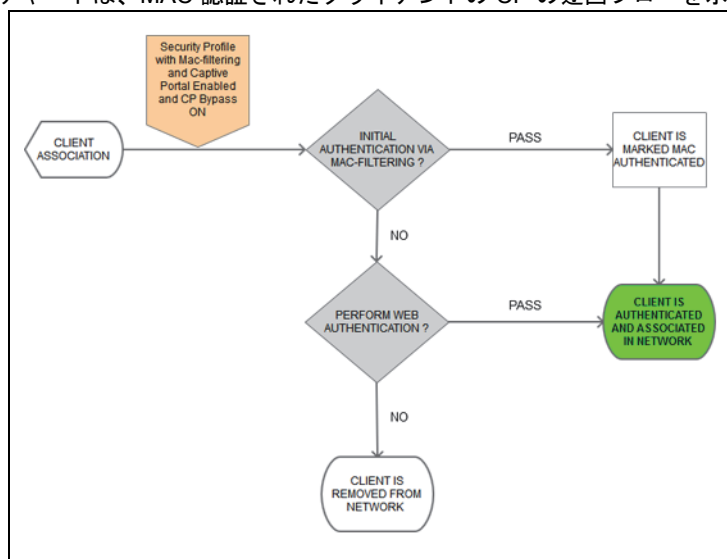
2016-May- 1 04:24:53.030895 | 00:73:8d:b9:e6:bf | Mac Filtering | Mac-Filtering is Success and Captive Portal is Bypassed for Wireless Client <00:73:8d:b9:e6:bf>

有線ステーション: MAC フィルタリングは成功、CP は迂回

2016-May- 1 04:38:06.888828 | f0:1f:af:33:cd:4e | Mac Filtering | Mac in permit list - accept client

2016-May- 1 04:38:06.890213 | f0:1f:af:33:cd:4e | Mac Filtering | Mac-Filtering is Success and Captive Portal is Bypassed for Wired Client <f0:1f:af:33:cd:4e>

次のフローチャートは、MAC 認証されたクライアントの CP の迂回フローを示しています。



サードパーティのキャプティブ ポータル ソリューション

フォーティネット キャプティブ ポータル ソリューションの代わりに、サードパーティ ソリューションを使用できます。ただし、両方は使用できません。Bradford、Avenda、CloudPath などの会社はすべて、FortiWLC (SD) 4.1 以降で動作するキャプティブ ポータル ソリューションを提供しています。対応するセキュリティ プロファイルとキャプティブ ポータル設定の 2 か所に、サードパーティのキャプティブ ポータル ソリューションを指示する必要があります。

Web UI を使用したサードパーティ キャプティブ ポータルの設定

キャプティブ ポータル認証方法を [external] に設定して、セキュリティ プロファイルでサードパーティのキャプティブ ポータル ソリューションを使用するよう指示します。詳細な手順は、「[Web UI によるセキュリティ プロファイルの設定](#)」を参照してください。

キャプティブ ポータルの外部 URL を [Captive Portal] ボックスの URL に設定して、キャプティブ ポータル設定で使用するサードパーティのキャプティブ ポータル ソリューションを使用することを指定します。

1. [Configuration] > [Security] > [Captive Portal] をクリックします。
2. キャプティブ ポータルの外部 URL の値を [third-party] ボックスの URL に変更します。
3. [OK] をクリックします。

CLI を使用したサードパーティ キャプティブ ポータルの設定

セキュリティ プロファイルでサードパーティのキャプティブ ポータル ソリューションを設定する前に、SSL サーバを設定します。たとえば、以下のように SSL サーバを設定します。

```
controller1# show ssl-server
Captive Portal

Name                                     : Captive Portal
Server Port                             : 10101
User Authentication Protocol             : None
Server Lifetime                          : 100
Server IP                               : 172.18.37.223
Certificate                              :
Authentication Type                      : radius
Primary Profile                          : IDAU1721946201
Secondary Profile                        :
Primary Profile                          : IDAC1721946201
Secondary Profile                        :

Accounting Interim Interval (seconds)    : 600
CaptivePortalSessionTimeout              : 0
CaptivePortalActivityTimeout              : 0
Protocol                                 : https
Portal URL                               :
CaptivePortal External URL                : https://172.19.46.201/portal/
172.18.37.223?meruInitialRedirect
CaptivePortal External IP                 : 172.18.37.223
L3 User Session Timeout(mins)             : 1
Apple Captive Network Assistant (CNA) Bypass : on
```

外部のキャプティブ ポータルを使用して SSID を設定する例は、以下のとおりです。

```
controller1# configure terminal
controller1(config)# security-profile CPEExternal
controller1(config-security)# captive-portal-auth-method external
controller1(config-security)# passthrough-firewall-filter-id IDMAUTH
controller1(config)# essid CaptivePortal-External
controller1(config-essid)# security-profile CaptivePortal-External
controller1(config-essid)# end
```

キャプティブ ポータル認証のための RADIUS サーバの設定

Web UI でのキャプティブ ポータル認証のための RADIUS サーバの設定

認証のために、RADIUS サーバのアイデンティティとシークレットをセットアップできます。これは、設定されているすべてのユーザ ID よりも優先されますが、RADIUS アカウンティングがフェイルオーバーすると、ローカル認証ゲスト ユーザ ID が使用されます。以下の手順に従ってください。

1. [Configuration] > [Security] > [RADIUS] をクリックして、RADIUS プロファイル テーブルにアクセスします。
2. [Add] をクリックします。
3. RADIUS サーバの情報を指定します。
4. [OK] をクリックして設定を保存します。
5. [Configuration] > [Security] > [RADIUS] > [Add] をクリックして、キャプティブ ポータル ログイン ページで使用するセキュリティ プロファイルを有効にします。
6. RADIUS プロファイルの名前など必須情報を指定します。キャプティブ ポータルを使用するには L2MODE が [clear] になっている必要があります。キャプティブ ポータルを [WebAuth] に設定して、必要に応じてその他のパラメータを調整します。

これで、アイデンティティとシークレットが設定されました。

CLI でのキャプティブ ポータル認証のための RADIUS サーバの設定

CLI コマンド `ssl-server captive-portal authentication-type` によって、コントローラがローカル認証、RADIUS 認証またはその両方を使用するように設定できます。両方を選択するとローカル認証が最初に試行され、認証できない場合は RADIUS 認証が試行されます。

```
Controller(config)# ssl-server captive-portal authentication-type ?
local                Set Authentication Type to local.
```

local-radius	Set Authentication Type to Local and RADIUS.
radius	Set Authentication Type to RADIUS.

次の例では、radius-auth-pri という名前の RADIUS 認証プロファイルを設定しています。

```
/* RADIUS PROFILE FOR AUTHENTICATION */
default# configure terminal
default(config)# radius-profile radius-auth-pri
default(config-radius)# ip-address 172.27.172.3
default(config-radius)# key sept20002
default(config-radius)# mac-delimiter hyphen
default(config-radius)# password-type shared-secret
default(config-radius)# port 1812
default(config-radius)# end
default#
default# sh radius-profile radius-auth-pri
RADIUS Profile Table
RADIUS Profile Name   : radius-auth-pri
Description           :
RADIUS IP             : 172.27.172.3
RADIUS Secret         : *****
RADIUS Port           : 1812
MAC Address Delimiter : hyphen
Password Type         : shared-secret
```

次の例では、radius-auth-sec という名前の RADIUS セキュリティ プロファイルを設定しています。

```
default# configure terminal
default(config)# radius-profile radius-auth-sec
default(config-radius)# ip-address 172.27.172.4
default(config-radius)# key sept20002
default(config-radius)# mac-delimiter hyphen
default(config-radius)# password-type shared-secret
default(config-radius)# port 1812
default(config-radius)# end
default#
default# sh radius-profile radius-auth-sec
RADIUS Profile Table
RADIUS Profile Name   : radius-auth-pri
Description           :
RADIUS IP             : 172.27.172.4
RADIUS Secret         : *****
RADIUS Port           : 1812
MAC Address Delimiter : hyphen
Password Type         : shared-secret
```

OAuth 認証のサポート

FortiWLC (SD) で Fortinet Connect (MCT) 14.10.0.2 を使用する場合は、キャプティブ ポータル ユーザ向けに OAuth 認証がサポートされます。一般的なシナリオで、外部の Web サイトにアクセスしようとするユーザ (ホテルのゲストなど) は、認証のためにキャプティブ ポータル ページにリダイレクトされます。キャプティブ ポータル ページで、ユーザはユーザ名、パスワード、電子メールなどの情報を登録し、ホテルのキャプティブ ポータルから確認を受け取って認証プロセスを完了します。



- Fortinet Connect で OAuth が有効にされている必要があります。
- SSL3 が有効 (HTTPS) なサイトにアクセスするワイヤレス クライアントのみが、この機能を使用できます。
- ワイヤレス クライアントが有線ネットワークに配置されたプロキシ サーバを使用する場合、クライアントはログイン タイムアウトの期限が切れるまでインターネットにアクセスできます。
- トンネル モードでは ESS プロファイルについてのみサポートされます。
- IPv4 クライアントについてのみサポートされます。

OAuth を有効にすることで、ユーザはキャプティブ ポータル認証で OAuth をサポートする任意のソーシャル メディア (Facebook、Google、Twitter、OpenID など) のログイン認証情報を使用できます。この機能により、ユーザは登録に時間を費やしたり、繰り返し認証するためにパスワードを覚えたりする必要がなくなります。



MCT での OAuth の設定、および OAuth サービス プロバイダへの登録の詳細については、Fortinet Connect 14.10.0.2 のリリース ノートを参照してください。

ソーシャル認証のサポート

キャプティブ ポータル認証プロセスで、Fortinet Presence が外部 CP 認証サーバとしてサポートされるようになりました。これにより、ユーザは Facebook や Gmail の OAuth のようなソーシャル メディア アカウントを使用して認証できます。

サポートされる AP : AP122、AP822、AP832、OAP832、FAP-U421EV、および FAP-U423EV



設定前に、次の点に注意してください。

- コントローラでロケーション サービスを有効にします (詳細は 92 ページの「[FortiPresence API の設定](#)」を参照)。
- データ分析ストアで AP を指定します。
- 「ブリッジ モード」ではサポートされません。

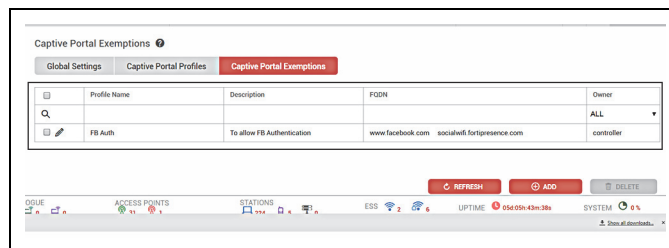
ソーシャル認証のサポートを有効にするには、次の手順を実行します。

1. キャプティブ ポータル除外プロファイルを作成します。
2. キャプティブ ポータル プロファイルで Fortinet Presence を使用するよう設定します。
3. このキャプティブ ポータル プロファイルをセキュリティ プロファイルで有効にし、このセキュリティ プロファイルを ESS プロファイルに追加します。

キャプティブ ポータル除外プロファイルの作成

ソーシャル ログインを有効にするには、除外 URL のリストを含むプロファイルを作成し、キャプティブ ポータル プロファイルで FortiPresence を外部認証サーバとして選択します。

1. [Configuration] > [Security] > [Captive Portal] > [Captive Portal Exemptions] に移動します。



2. [Add] ボタンをクリックして、ソーシャル認証が許可される URL のリストを含むプロファイルを作成します。プロフィールに複数の URL を追加するには、各 URL エントリの後にスペースを入力します。最大 32 の URL を追加できます。

Captive Portal Profiles | Captive Portal Exemptions

Add Captive Portal Exemptions

Profile Name * Enter 1-32 characters

Description Enter 0-128 characters

FQDN Enter 1-256 characters

+ ADD

Added FQDN

<input type="checkbox"/>	FQDN
<input type="checkbox"/>	www.facebook.com, socialwifi.fortipresence.com

DELETE

SAVE CANCEL



各プロフィールには、FQDN リストの一部として必ず socialwifi.fortipresence.com を追加してください (設定可能な URL の数は、これを含めて最大 32 です)。これは、クライアントがソーシャル Wi-Fi ログイン ページにアクセスするために必要です。

キャプティブ ポータル プロファイルでの Fortinet Presence の設定

1. [Configuration] > [Security] > [Captive Portal] > [Captive Portal Profiles] に移動します。
2. 認証タイプがローカルまたは RADIUS のキャプティブ ポータル プロファイルを作成します。
 - 認証タイプがローカルの場合は、次の認証情報を使用するゲスト ユーザを作成します。
 - ユーザ名 : gooduser
 - パスワード : good

- 認証タイプが RADIUS の場合は、RADIUS サーバで次の認証情報を使用するユーザを作成します。
 - ユーザ名 : gooduser
 - パスワード : good

3. [External Portal Settings] を次のように変更します。

Edit Captive Portal Profile

CP Name

FBAuth

User Authentication

Authentication Type

local

External Portal Settings

External Server

Fortinet-Presence

Captive Portal Exemption Profile

FB Auth

External Portal URL

socialwifi.fortipresence.com

Enter 0-255 chars.

Advanced Settings

Session Timeout

0

Valid range; [0-1440].

Activity Timeout

0

Valid range; [0-60].

Session Caching Time

1

Valid range; [1-1440].

CNA bypass

Off

SAVE

CANCEL

1. 外部サーバ (1) として [Fortinet-Presence] を選択します。
2. 除外 URL を含めて作成したプロファイル (2) を選択します。
3. 外部ポータル URL (3) として <http://socialwifi.fortipresence.com/wifi.html?login> を入力します。

Fortinet Presence のサーバ設定およびアカウントについては、『FortiPresence 設定ガイド』を参照してください (<http://docs.fortinet.com/d/fortipresence-analytics-configuration-guide>)。

セキュリティおよび ESS プロファイルでのキャプティブ ポータル プロファイルの有効化

このキャプティブ ポータル プロファイルをセキュリティ プロファイルで有効にし、このセキュリティ プロファイルを ESS プロファイルにマッピングします。セキュリティ プロファイルで、[CAPTIVE PORTAL SETTINGS] セクションを次のように変更します。

Security Configuration Table - Add ?

Security Profile Name * Enter 1-32 chars.

SECURITY SETTINGS

Security Mode *

CAPTIVE PORTAL SETTINGS

Captive Portal ❶

Captive Portal profile ❷

Captive Portal Authentication Method ❸

Passthrough Firewall Filter ID Enter 0-16 chars.

MAC FILTERING SETTINGS

MAC Filtering

FIREWALL SETTINGS

0 0 2 0 0 0 0 1 01d:03h:51m:48s 1%

1. [Captive Portal] を [WebAuth] に設定します。
2. ソーシャル Wi-Fi ログイン用に作成したキャプティブ ポータル プロファイルを選択します。
3. [Captive Portal Authentication Method] を [external] に設定します。



ESS プロファイルで、データプレーン モードをトンネルに設定します。

12 不正 AP の検出と緩和

不正 AP とは、許可されていないワイヤレス アクセス ポイントのことです。これらの不正 AP は、有線ネットワークに接続されているか、近接するネットワークのビルの外側にあるか、ハッカーが駐車している車の中にある可能性もあります。不正 AP によって企業ネットワークにセキュリティ リスクが生じる恐れがあるため、有効なネットワーク ユーザが不正 AP に接続することがないようにする必要があります。不正 AP は、WLAN テクノロジーがどのように動作するかをユーザが実験するという悪意のない理由や、セキュア ネットワークに対する悪意ある攻撃のような危険性を伴う理由で、企業ネットワークで発生するものです。VPN テクノロジーとファイアウォール テクノロジーが正しく適用された有線ネットワークに対しては、ビルの物理的なセキュリティでも十分に対処できますが、WLAN の場合、それだけでは不十分です。WLAN 内での RF の伝播継承によって、ターゲットになる WLAN の近く（たとえば、駐車場）にいる未承認のユーザが、たとえ建物の中にいない場合であっても、ネットワークへのアクセスが可能になってしまいます。

表 20: フォーティネット の不正の検出と緩和のサポート

	不正検出	不正緩和
AP1000	4.1 以降	4.1 以降
AP400	5.0 以降	5.0 以降

どのような理由で存在するかに関係なく、不正 AP は WLAN のそれ以外の部分のセキュリティ ポリシーに反するものであり、セキュリティ アーキテクチャ全体の中の脆弱箇所です。たとえ不正 AP を持ち込んだ当人には悪意がなかったとしても、結果としては悪意ある行為が発生する可能性があります。そのような悪意ある行為としては、承認されたアクセス ポイントの振りをしてセキュリティ情報を収集し、それがさらにネットワークを悪用するために使われる可能性があるという例が挙げられます。通常、ネットワーク セキュリティのメカニズムは、ネットワークを未承認のユーザから保護するものですが、ネットワークそのものの正当性を確認する手段をユーザに提供するものではありません。この種のセキュリティ侵害は、個人情報の収集、保護されているファイルへのアクセス、ネットワークのパフォーマンス低下を招く攻撃、ネットワークの管理に対する攻撃などにつながる可能性があります。

許可されていない AP がネットワークにアクセスできないようにするために、不正 AP の存在のスキャンと不正 AP からのクライアント トラフィックの緩和の両方を有効にします。これ

らの機能は、CLI と Web UI のいずれかから、コントローラで許可対象とブロック対象の WLAN BSSID のリストを管理し、不正 AP が検出されたときに緩和を実行する AP セット (緩和 AP) を調整することで、グローバルに設定します。

チャネル スキャンの結果として、不正 AP のリストが蓄積され、コントローラによってそのリストが不正 AP の近くにある多くの緩和 AP に送信されます。緩和 AP は、緩和 (deauth) フレームをクライアントが関連付けられている不正 AP に送信して、これらのクライアントをネットワークから削除します。不正 AP が存在すると、Web UI 監視ダッシュボードおよびシステムログ警告メッセージに警告が表示されるため、管理者は状況を把握して、危険な AP を削除して設定リストを更新できます。

不正スキャンを設定して、デュアル無線 AP の 1 つの無線の専用にする 것도、同じ無線でクライアントのサービスも一定時間は実行するようにすることもできます。不正 AP スキャン (検出) が一定時間有効になっていると、AP はチャネルのスキャンに一定の時間を使い、ホーム チャネルでの通常の AP WLAN 操作に一定の時間を使います。スキャンと通常のこの処理サイクルは、ステーションが割り当てられていない、指定した AP または AP インターフェイスで発生するので、ネットワーク処理タスクのパフォーマンスが大きく低下することはありません。

AP400 と AP1000 では、各無線がデュアルバンド (2.4GHz と 5.0GHz の両方をサポート) であり、スキャン専用の無線として設定されている場合に、すべてのチャネルとすべてのバンドでスキャンを実行できます。アクセスポイントが検出されると、BSSID が BSSID の AP アクセス制御リストと比較されます。アクセス ポイントは、アクセス制御リスト (ACL) においては、「known」、「blocked」、または「nonexistent」の状態になります。「known」(既知) の AP は、システム管理者によってその AP の BSSID が ACL に登録されていたために、承認されていると判断されたものです。「selected」(選択) の AP は、未承認 AP としてワイヤレス LAN システムがブロックしたものです。フォーティネット WLAN は、ACL に登録されていないこれ以外の AP もレポートします。これらの AP が ACL で「known」あるいは「selected」と指定されるまで、アラートが管理コンソールに送られます。たとえば、ACL に追加されていない限り、サードパーティの BBS は不正として検出されます。

フォーティネット AP は、不正に関連しているアクセス ポイントまたはワイヤレス ステーションからのトラフィックを監視することでも、不正 AP を検出します。そのため、不正が範囲外にある場合であっても、その不正に関連付けられているワイヤレス ステーションが範囲内にあるのであれば、不正 AP を検出できます。

本章では、以下の内容を説明します。

- [Web UI による不正 AP 緩和の設定 \(321 ページ\)](#)
- [CLI を使用した不正 AP 検出の設定 \(325 ページ\)](#)
- [CLI による検出と緩和の設定の変更 \(328 ページ\)](#)
- [不正緩和のトラブルシューティング \(337 ページ\)](#)

Web UI による不正 AP 緩和の設定

許可されていない AP がネットワークにアクセスできないようにするために、不正 AP の存在のスキャンと不正 AP からのクライアント トラフィックの緩和の両方を有効にします。これらの機能は、コントローラで許可対象とブロック対象の WLAN BSSID のリストを管理し、不正 AP が検出されたときに緩和を実行する AP セット (緩和 AP) を調整することで、グローバルに設定します。

不正検出を実行する AP のホワイトリストを作成できます。このホワイトリストに追加されていない AP は、不正 AP/ クライアントかどうかのスキャンを行いません。

不正 AP スキャン (検出) が一定時間有効になっていると、AP はチャネルのスキャンに一定の時間 (スキャン時間をミリ秒で設定) を使い、ホーム チャネルでの通常の AP WLAN 操作に一定の時間 (処理時間をミリ秒で設定) を使います。このスキャンと操作の繰り返しは極めて短い間隔で繰り返されるため、ネットワーク処理の低下に気付くことなく、両方のタスクが実行されます。

特定の AP でスキャンされるチャネルは AP のモデルにより決定されます。チャネル スキャンの結果として、不正 AP のリストが蓄積され、コントローラによってそのリストが不正 AP の近くにある多くの緩和 AP に送信されます。緩和 AP は、緩和 (deauth) フレームをクライアントが関連付けられている不正 AP に送信して、これらのクライアントをネットワークから削除します。不正 AP が存在すると、Web UI 監視ダッシュボードおよびシステムログ警告メッセージに警告が表示されるため、管理者は状況を把握して、危険な AP を削除して設定リストを更新できます。

また、AP の有線インターフェイスで不正デバイスが検出されたり、ステーションの AP の検出リストにデバイスが追加されていたりすると、有線不正通知が、Web UI 監視ダッシュボードとシステム ログ アラーム メッセージを介して送信されます。不正クライアントが AP に関連付けられると、そのクライアントは不正に分類されます。

Web UI による許可対象 AP のリストの変更

許可対象 AP のリストを変更するには、次の手順を実行します。

1. Web UI から、[Configuration] > [Security] > [Rogue APs] > [Global Settings] ページにアクセスして、不正検出を有効にします。

Update ?

APs Blocked APs

Off ▼

No mitigation ▼

600 Valid range: [60-86400]

3 Valid range: [1-20]

100 Valid range: [100-500]

400 Valid range: [100-5000]

channel 10 Valid range: [1-50]

1,2,3,4,5,6,7,8,9,10,11,12,13, Enter 0-256 chars.

-100 Valid range: [-100-0]

ADD DELETE

AP を追加して不正をスキャンするには、[Add] ボタンをクリックし、リストから AP を選択します。

Add APs

<input type="checkbox"/>	AP ID	AP Name	Operational State	Availability Status	AP Model	Location
<input type="checkbox"/>						
<input type="checkbox"/>	3	RF-Chamber-1	Enabled	Online	AP832i	
<input type="checkbox"/>	4	RF-Chamber-2	Enabled	Online	AP832i	
<input type="checkbox"/>	6	RF-Chamber-3	Enabled	Online	AP832i	
<input type="checkbox"/>	13	PM-Desk-1020	Disabled	Offline	AP1020	
<input type="checkbox"/>	17	AP-17	Enabled	Online	AP822i	
<input type="checkbox"/>	19	AP-19	Disabled	Offline	AP122	
<input type="checkbox"/>	20	Spectrum-AP	Enabled	Online	AP332e	
<input type="checkbox"/>	22	Kartik-RF-Chamber-4	Enabled	Online	AP832e	

ADD CLOSE

Web UI によるブロック対象 AP のリストの変更

許可対象 AP のリストを変更するには、次の手順を実行します。

1. Web UI から、[Configuration] > [Rogue APs] > [Blocked APs] をクリックします。ブロック対象 BSSID としてアクセス制御リスト (ACL) に登録されているアクセス ポイントに関する情報が表に表示されます。
2. WLAN のブロック対象 AP の最新リストを表示するには、[Refresh] をクリックします。
3. ブロック対象リストに AP を追加するには、[Add] をクリックします。
 - [BSSID] ボックスに、アクセス ポイントの BSSID を 16 進数形式で入力します。
 - [OK] をクリックして、BSSID を ACL に追加します。
4. ブロックされた BSSID がリストに表示され、以下の情報が表示されます。
 - [BSSID]: アクセス ポイントの BSSID。
 - [Creation Time]: ブロックされた AP エントリが作成された時のタイムスタンプ。
 - [Last Reported Time]: AP が最後に検出された時刻。このフィールドが空白の場合、AP はまだ検出されていません。
5. ブロック対象 BSSID を ACL から削除するには、削除するブロック対象 AP のチェックボックスを選択し、[Delete] をクリックしてから、[OK] をクリックします。

Web UI によるスキャンと緩和の設定

不正 AP のスキャンと緩和を設定するには、以下の手順を実行します。

1. Web UI から、[Configuration] > [Wireless IDS/IPS] > [Rogue APs] をクリックします。[Rogue AP] 画面が、[Global Settings] タブが選択された状態で表示されます。図 62 を参照してください。

図 62: Web UI の不正 AP グローバル設定

RogueAP Global Settings - Update

Global Settings Allowed APs Blocked APs

Detection	On	
Mitigation	Block only BSSIDs in blocked list	
Rogue AP Aging (seconds)	60	Valid range: [60-86400]
Number of Mitigating APs	3	Valid range: [1-20]
Scanning time in ms	100	Valid range: [100-500]
Operational time in ms	400	Valid range: [100-5000]
Max mitigation frames sent per channel	10	Valid range: [1-50]
Scanning Channels	1,2,3,4,5,6,7,8,9,10,11,12	Enter 0-256 chars.
RSSI Threshold for Mitigation	-100	Valid range: [-100-0]

- [Detection] リストで、次のいずれかを選択します。
 - [On] : 不正 AP のスキャンを有効にします。
 - [Off] : 不正検出を無効にします。
- [Mitigation] リストで、次のいずれかを選択します。
 - [No mitigation] : 不正 AP 緩和は実行されません。
 - [Block all BSSIDs that are not in the ACL] : [Allowed APs] リストで承認されている AP として指定されていない、検出されたすべての BSSID の不正 AP 緩和を有効にします。
 - [Block only BSSIDs in blocked list] : [Blocked APs] リストに登録されている BSSID に対してのみ、不正 AP 緩和を有効にします。
 - [Block Clients seen on the wire] : AP の有線側で検出されたすべての不正ステーションの不正検出を有効にします (多くの場合は、会社のネットワーク)。[Block clients seen on the wire] を選択すると、会社のネットワークで認識されたクライアントが緩和の対象になります。[Block clients seen on the wire] を選択し、有線不正クライアントの BSSID がブロック対象リスト (322 ページの「[Web UI によるブロック対象 AP のリストの変更](#)」を参照) に入力されていると、リストに指定されているクライアントだけが緩和されます。
- [Rogue AP Aging] ボックスには、コントローラが不正を検出しなくなった場合に不正 AP アラームをクリアするまでの経過時間を入力します。60 ~ 86,400 秒の値を指定できます。

5. [Number of Mitigating APs] テキストボックスには、不正 AP のスキャンと緩和を実行する AP の数 (1 ~ 20) を入力します。
6. [Scanning time in ms] テキストボックスには、緩和 AP が不正 AP のスキャン チャンネルをスキャンする時間を入力します。100 ~ 500 ミリ秒を指定できます。
7. [Operational time in ms] テキストボックスには、緩和 AP がホーム チャンネルの運用モードに費やす時間を入力します。100 ~ 5000 ミリ秒を指定できます。
8. [Max mitigation frames sent per channel] テキストボックスには、検出された不正 AP に送信される緩和フレームの最大数を入力します。1 ~ 50 deauth フレームを指定できます。
9. [Scanning Channels] テキストボックスには、不正 AP がスキャンされるチャンネルのリストを入力します。0 ~ 256 文字までのカンマ区切りリストを使用します。デフォルトの全チャンネル セットは、1、2、3、4、5、6、7、8、9、10、11、36、40、44、48、52、56、60、64、149、153、157、161、165 です。
10. [RSSI Threshold for Mitigation] テキストボックスには、ステーションを緩和する最小しきい値レベルを入力します。有効な値の範囲は、-100 ~ 0 です。
11. [OK] をクリックします。

CLI を使用した不正 AP 検出の設定

これらの CLI コマンドは、不正検出を設定します。コマンドの詳細については『*FortiWLC (SD) コマンド リファレンス*』を参照してください。

スキャン リストへの AP の追加

```
default(15)# configure terminal
default(15)(config)# rogue-ap detection-ap 1
default(15)(config)# rogue-ap detection-ap 3
default(15)(config)# exit
```

Show Output

```
default(15)# sh rogue-ap detection-ap-list
AP ID
1
3
```

Rogue Device Detecting APs(2)

スキャン リストからの AP の削除

```
default(15)# configure terminal
default(15)(config)# no rogue-ap detection-ap 1
default(15)(config)# no rogue-ap detection-ap 3
default(15)(config)# end
```

Show Output

```
default(15)# show rogue-ap detection-ap-list
AP ID
```

Rogue Device Detecting APs(No entries)

CLI による AP アクセスとブロック リストの設定

この機能では、許可対象 BSSID のリストとブロック対象 BSSID のリストが含まれるアクセス制御リスト (ACL) を使用します。デフォルトでは、WLAN のすべてのフォーティネット ESS BSSID が自動的に許可対象 ACL に含まれます。同じ BSSID を両方のリストに指定することはできません。

BSSID が 00:0e:cd:cb:cb:cb アクセス ポイントを許可対象アクセス ポイントとしてアクセス制御リストに追加するには、次のコマンドを入力します。

```
controller (config)# rogue-ap acl 00:0e:cd:cb:cb:cb
controller (config)#
```

許可対象リストのすべての BSSID のリストを表示するには、次のコマンドを入力します。

```
controller# show rogue-ap acl
Allowed APs
BSSID
00:0c:e6:cd:cd:cd
00:0e:cd:cb:cb:cb
```

1 つの BSSID を不正 AP 検出のブロック対象リストとアクセス リストの両方に同時に指定することはできません。たとえば、00:0c:e6:cd:cd:cd をブロック対象リストに指定するとします。この BSSID が許可対象リストにすでに指定されている場合は、この BSSID を許可対象リストから削除し、その後でブロック対象リストに追加する必要があります。次のようにコマンドを入力します。

```
controller (config)# no rogue-ap acl 00:0c:e6:cd:cd:cd
controller (config)#
controller (config)# rogue-ap blocked 00:0c:e6:cd:cd:cd
```

```

controller (config)# exit
controller# show rogue-ap acl
Allowed APs
BSSID
00:0e:cd:cb:cb:cb
controller# show rogue-ap blocked
BssId          Creation Date    Last Reported
-----
00:0c:e6:cd:cd:cd  11/02 01:05:54    11/02 01:06:20

```

不正 AP 検出の状態を有効にし、確認するには、次のコマンドを入力します。

```

controller (config)# rogue-ap detection
controller# show rogue-ap globals
Global Settings
Detection                               : on
Mitigation                             : none
Rogue AP Aging (seconds)                : 60
Number of Candidate APs                 : 3
Number of Mitigating APs               : 5
Scanning time in ms                    : 100
Operational time in ms                  : 400
Max mitigation frames sent per channel : 10
Scanning Channels                       :
1,2,3,4,5,6,7,8,9,10,11,36,40,44,48,52,56,60,64,149,153,157,161,165
RSSI Threshold for Mitigation           : -100

```

CLI コマンド show rogue-ap-list を使用すると、ネットワークのすべての不正クライアントと AP が表示されます。

不正緩和の例

ブロック対象リストの AP に対する不正 AP 緩和を有効にし、確認するには、次のコマンドを入力します。

```

controller# configure terminal
controller (config)# rogue-ap detection
controller (config)# rogue-ap mitigation selected
controller (config)# exit
controller# show rogue-ap globals
Global Settings
Detection                               : on
Mitigation                             : selected
Rogue AP Aging (seconds)                : 60
Number of Candidate APs                 : 3
Number of Mitigating APs               : 5
Scanning time in ms                    : 100
Operational time in ms                  : 400

```

```

Max mitigation frames sent per channel : 10
Scanning Channels                      :
1,2,3,4,5,6,7,8,9,10,11,36,40,44,48,52,56,60,64,149,153,157,161,165
RSSI Threshold for Mitigation          : -100

```

CLI による検出と緩和の設定の変更

不正 AP の検出と緩和の機能に設定されているデフォルト値は、ほとんどの場合に十分な効果を発揮しますが、ネットワークの要件によって、スキャンや緩和のサービスを緩和したり強化したりする必要がある場合は、デフォルト設定を変更することもできます。以下の `rogue-ap` コマンドを使用します。

```

controller (config)# rogue-ap ?
acl                Add a new rogue AP ACL entry.
aging              Sets the aging of alarms for rogue APs.
assigned-aps       Number of APs assigned for mitigation.
blocked            Add a new rogue AP blocked entry.
detection          Turn on rogue AP detection.
min-rssi           Sets RSSI Threshold for Mitigation.
mitigation         Set the rogue AP mitigation parameters.
mitigation-frames  Sets the maximum number of mitigation frames sent out
per channel.
operational-time   Sets the APs time on the home channel during scanning.
scanning-channels  Sets the global Rogue AP scanning channels.
scanning-time      Sets the APs per channel scanning time

```

一般的なルールとして、AP が専用スキャン モードとなっていない限り、スキャンと緩和に費やされる時間が多くなるほど、AP の通常の WLAN サービスに費やされる時間は短くなります。サービスの提供方法については、いくつかのルールが存在します。

- コントローラが、スキャンと緩和を実行する AP を選択します。緩和を実行する AP は、不正 AP からの距離と、設定されている緩和 AP 数によって決定されます。
- 運用パフォーマンスを維持するために、クライアントが関連付けられている場合は、ホーム チャンネルでのみ緩和を実行します。
- 設定はグローバルに管理されます。特定の AP が緩和を実行するよう設定する方法はありません。
- 緩和は、不正 AP に関連付けられているクライアントに対してのみ実行されます。不正 AP そのものは緩和されません。ネットワークから不正 AP を削除する作業は、ネットワーク管理者の責任です。
- AP 緩和フレームには、QoS フレームよりも低く、ベストエフォート フレームよりも高い優先度が設定されます。
- ネットワーク トラフィックを少なくするために、ホーム チャンネルだけが含まれるスキャン チャンネル リストを設定することもできます。

CLI による緩和 AP 数の変更

デフォルトでは、3 つの緩和 AP がコントローラによって選択され、スキャンと緩和が実行されます。この数を、ネットワークのニーズに応じて、最大で 20 AP、最小で 1 AP に設定できます。緩和 AP 数を 5 に変更するには、次のコマンドを実行します。

```
controller (config)# rogue-ap assigned-aps 5
```

CLI によるスキャンと緩和の設定の変更

不正 AP スキャンが有効になっていると、AP はチャネルのスキャンに一定の時間を使い、ホーム チャネルでの通常の AP WLAN 操作に一定の時間を使います。このスキャンと操作の繰り返しは極めて短い間隔で繰り返されるため、ネットワーク処理の低下に気付くことなく、両方のタスクが実行されます。

スキャンが有効になっている場合、rogue-ap operational-time コマンドを使用して、ホームチャネルでの通常のワイヤレス サービスに費やすミリ秒数を指定します。このコマンドは、rogue-ap scanning-time コマンドに関連しています。スキャンされるチャネルは、rogue-ap scanning channels コマンドにより決定されます。デフォルトの全チャネルセットは、1、2、3、4、5、6、7、8、9、10、11、36、40、44、48、52、56、60、64、149、153、157、161、165 です。

以下のコマンドは、処理時間をデフォルトの 400 から 2500 ミリ秒に変更します。

```
controller (config)# rogue-ap operational-time 2500
```

以下のコマンドは、スキャン時間をデフォルトの 100 から 200 ミリ秒に変更します。

```
controller (config)# rogue-ap scanning-time 200
```

以下のコマンドでは、スキャンするチャネルが 1、6、11、36、44、52、60 に設定されます。

```
controller (config)# rogue-ap scanning-channels 1,6,11,36,44,52,60
controller (config)# exit
```

変更されたことを確認するには、show rogue-ap globals コマンドを実行します。

```
controller# show rogue-ap globals
Global Settings
Detection                : on
Mitigation                : selected
Rogue AP Aging (seconds) : 60
Number of Candidate APs  : 5
Number of Mitigating APs : 5
Scanning time in ms      : 200
Operational time in ms   : 2500
Max mitigation frames sent per channel : 10
```

Scanning Channels	: 1,6,11,36,44,52,60
RSSI Threshold for Mitigation	: -100

CLI による最小 RSSI の変更

RSSI は、AP が不正の緩和を試行するしきい値です。シグナルがとても弱いと (AP が離れていると)、AP は緩和を試行しません。

緩和するステーションの最小 RSSI (受信信号強度) レベルを変更するには、rogue-ap min-rssi コマンドを使用します。0 ~ -100 の範囲をサポートしており、デフォルト設定は -100 です。

次のコマンドは、最小 RSSI レベルを -80 に設定します。

```
controller (config)# rogue-ap min-rssi -80
controller (config)#
```

表 21: 不正緩和の CLI コマンド

不正緩和コマンド	アクション
rogue-ap mitigation all	アクセス制御リストにないすべての不正 AP に緩和を設定します。
rogue-ap mitigation selected	ブロック対象リストにあるすべての不正 AP に緩和を設定します。
rogue-ap mitigation wiredrogue	すべての有線側不正 AP に緩和を設定します。有線側の不正クライアントがブロック対象 ACL リストに追加されていると、リストにある有線側不正クライアントだけがブロックされます。
show rogue-ap globals	現在の不正データを表示します。
rogue-ap mitigation none	不正緩和をオフにします。

不正緩和の例

ブロック対象リストの AP に対する不正 AP 緩和を有効にし、確認するには、次のコマンドを入力します。

```
controller# configure terminal
controller(config)# rogue-ap detection
controller(config)# rogue-ap mitigation selected
controller(config)# exit
controller# show rogue-ap globals
Global Settings
Detection                : on
Mitigation                : selected
Rogue AP Aging (seconds) : 60
Number of Candidate APs   : 3
Number of Mitigating APs  : 5
```



```

Scanning time in ms           : 100
Operational time in ms       : 400
Max mitigation frames sent per channel : 10
Scanning Channels             :
1,2,3,4,5,6,7,8,9,10,11,36,40,44,48,52,56,60,64,149,153,157,161,165
RSSI Threshold for Mitigation : -100

```

CLI による不正検出と緩和の設定の変更

不正 AP の検出と緩和の機能に設定されているデフォルト値は、ほとんどの場合に十分な効果を発揮しますが、ネットワークの要件によって、スキャンや緩和のサービスを緩和したり強化したりする必要がある場合は、デフォルト設定を変更することもできます。以下の `rogue-ap` コマンドを使用します。

```

controller(config)# rogue-ap ?
acl                Add a new rogue AP ACL entry.
aging              Sets the aging of alarms for rogue APs.
assigned-aps       Number of APs assigned for mitigation.
blocked            Add a new rogue AP blocked entry.
detection           Turn on rogue AP detection.
min-rssi           Sets RSSI Threshold for Mitigation.
mitigation          Set the rogue AP mitigation parameters.
mitigation-frames  Sets the maximum number of mitigation frames sent out
per channel.
operational-time    Sets the APs time on the home channel during scanning.
scanning-channels  Sets the global Rogue AP scanning channels.
scanning-time       Sets the APs per channel scanning time

```

一般的なルールとして、AP が専用スキャン モードとなっていない限り、スキャンと緩和に費やされる時間が多くなるほど、AP の通常の WLAN サービスに費やされる時間は短くなります。サービスの提供方法については、いくつかのルールが存在します。

- コントローラが、スキャンと緩和を実行する AP を選択します。緩和を実行する AP は、不正 AP からの距離と、設定されている緩和 AP 数によって決定されます。
- 運用パフォーマンスを維持するために、クライアントが関連付けられている場合は、ホーム チャネルでのみ緩和を実行します。
- 設定はグローバルに管理されます。特定の AP が緩和を実行するよう設定する方法はありません。
- 緩和は、不正 AP に関連付けられているクライアントに対してのみ実行されます。不正 AP そのものは緩和されません。ネットワークから不正 AP を削除する作業は、ネットワーク管理者の責任です。
- AP 緩和フレームには、QoS フレームよりも低く、ベストエフォート フレームよりも高い優先度が設定されます。
- ネットワーク トラフィックを少なくするために、ホーム チャネルだけが含まれるスキャン チャネル リストを設定することもできます。

CLI による緩和 AP 数の変更

デフォルトでは、3 つの緩和 AP がコントローラによって選択され、スキャンと緩和が実行されます。この数は、ネットワークのニーズに応じて、最大で 20 AP、最小で 1 AP に設定できますが、相互の不正緩和を干渉する可能性があるため、緩和 AP の数を多くしないことを推奨します。緩和 AP 数を 5 に変更するには、次のコマンドを実行します。

```
controller(config)# rogue-ap assigned-aps 5
```

CLI によるスキャンと緩和の設定の変更

不正 AP スキャンが有効になっていると、AP はチャネルのスキャンに一定の時間を使い、ホーム チャネルでの通常の AP WLAN 操作に一定の時間を使います。このスキャンと操作の繰り返しは極めて短い間隔で繰り返されるため、ネットワーク処理の低下に気付くことなく、両方のタスクが実行されます。

スキャンが有効になっている場合、rogue-ap operational-time コマンドを使用して、ホーム チャネルでの通常のワイヤレス サービスに費やすミリ秒数を指定します。このコマンドは、rogue-ap scanning-time コマンドに関連しています。スキャンされるチャネルは、rogue-ap scanning channels コマンドにより決定されます。デフォルトの全チャネル セットは、1、2、3、4、5、6、7、8、9、10、11、36、40、44、48、52、56、60、64、149、153、157、161、165 です。

以下のコマンドは、処理時間をデフォルトの 400 から 2500 ミリ秒に変更します。

```
controller(config)# rogue-ap operational-time 2500
```

以下のコマンドは、スキャン時間をデフォルトの 100 から 200 ミリ秒に変更します。

```
controller(config)# rogue-ap scanning-time 200
```

以下のコマンドでは、スキャンするチャネルが 1、6、11、36、44、52、60 に設定されます。

```
controller(config)# rogue-ap scanning-channels 1,6,11,36,44,52,60
controller(config)# exit
```

変更されたことを確認するには、show rogue-ap globals コマンドを実行します。

```
controller# show rogue-ap globals
Global Settings
Detection                : on
Mitigation                : selected
Rogue AP Aging (seconds) : 60
Number of Candidate APs  : 5
Number of Mitigating APs : 5
Scanning time in ms      : 200
Operational time in ms   : 2500
Max mitigation frames sent per channel : 10
```

Scanning Channels	: 1,6,11,36,44,52,60
RSSI Threshold for Mitigation	: -100

CLI による最小 RSSI の変更

RSSI は、AP が不正の緩和を試行するしきい値です。シグナルがとても弱いと (AP が離れていると)、AP は緩和を試行しません。

緩和するステーションの最小 RSSI (受信信号強度) レベルを変更するには、`rogue-ap min-rssi` コマンドを使用します。0 ~ -100 の範囲をサポートしており、デフォルト設定は -100 です。

次のコマンドは、最小 RSSI レベルを -80 に設定します。

```
controller(config)# rogue-ap min-rssi -80
controller(config)#
```

Web UI による不正 AP 緩和の設定

許可されていない AP がネットワークにアクセスできないようにするために、不正 AP の存在のスキャンと不正 AP からのクライアント トラフィックの緩和の両方を有効にします。これらの機能は、コントローラで許可対象とブロック対象の WLAN BSSID のリストを管理し、不正 AP が検出されたときに緩和を実行する AP セット (緩和 AP) を調整することで、グローバルに設定します。

不正 AP スキャン (検出) が有効になっていると、AP はチャンネルのスキャンに一定の時間 (スキャン時間をミリ秒で設定) を使い、ホーム チャンネルでの通常の AP WLAN 操作に一定の時間 (処理時間をミリ秒で設定) を使います。このスキャンと操作の繰り返しは極めて短い間隔で繰り返されるため、ネットワーク処理の低下に気付くことなく、両方のタスクが実行されます。

特定の AP でスキャンされるチャンネルは AP のモデルにより決定されます。チャンネル スキャンの結果として、不正 AP のリストが蓄積され、コントローラによってそのリストが不正 AP の近くにある多くの緩和 AP に送信されます。緩和 AP は、緩和 (deauth) フレームをクライアントが関連付けられている不正 AP に送信して、これらのクライアントをネットワークから削除します。不正 AP が存在すると、Web UI 監視ダッシュボードおよびシステムログ警告メッセージに警告が表示されるため、管理者は状況を把握して、危険な AP を削除して設定リストを更新できます。

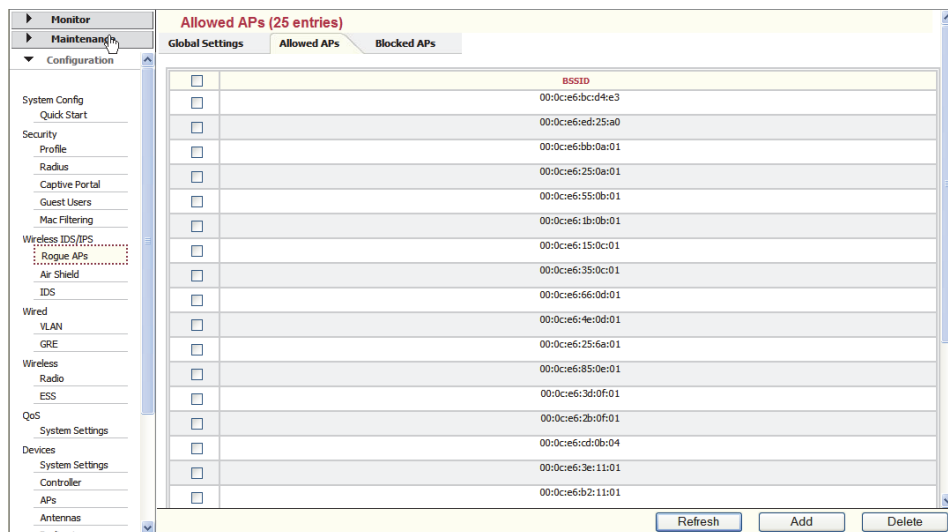
また、AP の有線インターフェイスで不正デバイスが検出されたり、ステーションの AP の検出リストにデバイスが追加されていたりすると、有線不正通知が、Web UI 監視ダッシュボードとシステム ログ アラーム メッセージを介して送信されます。不正クライアントが AP に関連付けられると、そのクライアントは不正に分類されます。

Web UI による許可対象 AP のリストの変更

許可対象 AP のリストを変更するには、次の手順を実行します。

1. Web UI から、[Configuration] > [Wireless IDS/IPS] > [Rogue APs] > [Allowed APs] をクリックします。
[Allowed APs] 画面が表示されます。図 63 を参照してください。

図 63: Web UI の [Allowed APs] リスト



2. BSSID をリストに追加するには、[Add] をクリックします。
 - [BSSID] ボックスに、許可対象アクセス ポイントの BSSID を、16 進数形式で入力します。
 - BSSID を ACL に追加するには、[OK] をクリックします。
3. BSSID をリストから削除するには、削除する BSSID を選択し、[Delete] をクリックしてから、[OK] をクリックします。

Web UI によるブロック対象 AP のリストの変更

許可対象 AP のリストを変更するには、次の手順を実行します。

1. Web UI から、[Configuration] > [Wireless IDS/IPS] > [Rogue APs] > [Blocked APs] をクリックします。ブロック対象 BSSID としてアクセス制御リスト (ACL) に登録されているアクセス ポイントに関する情報が表に表示されます。
2. WLAN のブロック対象 AP の最新リストを表示するには、[Refresh] をクリックします。

3. ブロック対象リストに AP を追加するには、[Add] をクリックします。
 - [BSSID] ボックスに、アクセス ポイントの BSSID を 16 進数形式で入力します。
 - [OK] をクリックして、BSSID を ACL に追加します。
4. ブロックされた BSSID がリストに表示され、以下の情報が表示されます。
 - [BSSID]: アクセス ポイントの BSSID。
 - [Creation Time]: ブロックされた AP エントリが作成された時のタイムスタンプ。
 - [Last Reported Time]: AP が最後に検出された時刻。このフィールドが空白の場合、AP はまだ検出されていません。
5. ブロック対象 BSSID を ACL から削除するには、削除するブロック対象 AP のチェックボックスを選択し、[Delete] をクリックしてから、[OK] をクリックします。

Web UI によるスキャンと緩和の設定

不正 AP のスキャンと緩和を設定するには、以下の手順を実行します。

1. Web UI から、[Configuration] > [Wireless IDS/IPS] > [Rogue APs] をクリックします。
[Rogue AP] 画面が、[Global Settings] タブが選択された状態で表示されます。図 62 を参照してください。

図 64: Web UI の不正 AP グローバル設定

RogueAP Global Settings - Update

Global Settings	Allowed APs	Blocked APs
Detection	On	
Mitigation	Block only BSSIDs in blocked list	
Rogue AP Aging (seconds)	60	Valid range: [60-86400]
Number of Mitigating APs	3	Valid range: [1-20]
Scanning time in ms	100	Valid range: [100-500]
Operational time in ms	400	Valid range: [100-5000]
Max mitigation frames sent per channel	10	Valid range: [1-50]
Scanning Channels	1,2,3,4,5,6,7,8,9,10,11,12	Enter 0-256 chars.
RSSI Threshold for Mitigation	-100	Valid range: [-100-0]

2. [Detection] リストで、次のいずれかを選択します。
 - On: 不正 AP のスキャンを有効にします。

- Off: 不正検出を無効にします。
3. [Mitigation] リストで、次のいずれかを選択します。
 - [No mitigation]: 不正 AP 緩和は実行されません。
 - [Block all BSSIDs that are not in the ACL]: [Allowed APs] リストで承認されている AP として指定されていない、検出されたすべての BSSID の不正 AP 緩和を有効にします。
 - [Block only BSSIDs in blocked list]: [Blocked APs] リストに登録されている BSSID に対してのみ、不正 AP 緩和を有効にします。
 - [Block Clients seen on the wire]: AP の有線側で検出されたすべての不正ステーションの不正検出を有効にします (多くの場合は、会社のネットワーク)。[Block clients seen on the wire] を選択すると、会社のネットワークで認識されたクライアントが緩和の対象になります。[Block clients seen on the wire] を選択し、有線不正クライアントの BSSID がブロック対象リスト (322 ページの「[Web UI によるブロック対象 AP のリストの変更](#)」を参照) に入力されていると、リストに指定されているクライアントだけが緩和されます。
 4. [Rogue AP Aging] ボックスには、コントローラが不正を検出しなくなった場合に不正 AP アラームをクリアするまでの経過時間を入力します。60 ~ 86,400 秒の値を指定できます。
 5. [Number of Mitigating APs] テキストボックスには、不正 AP のスキャンと緩和を実行する AP の数 (1 ~ 20) を入力します。
 6. [Scanning time in ms] テキストボックスには、緩和 AP が不正 AP のスキャン チャネルをスキャンする時間を入力します。100 ~ 500 ミリ秒を指定できます。
 7. [Operational time in ms] テキストボックスには、緩和 AP がホーム チャネルの運用モードに費やす時間を入力します。100 ~ 5000 ミリ秒を指定できます。
 8. [Max mitigation frames sent per channel] テキストボックスには、検出された不正 AP に送信される緩和フレームの最大数を入力します。1 ~ 50 deauth フレームを指定できます。
 9. [Scanning Channels] テキストボックスには、不正 AP がスキャンされるチャネルのリストを入力します。0 ~ 256 文字までのカンマ区切りリストを使用します。デフォルトの全チャネル セットは、1、2、3、4、5、6、7、8、9、10、11、36、40、44、48、52、56、60、64、149、153、157、161、165 です。
 10. [RSSI Threshold for Mitigation] テキストボックスには、ステーションを緩和する最小しきい値レベルを入力します。有効な値の範囲は、-100 ~ 0 です。

11.[OK] をクリックします。



検出ステーション データベースにすでに存在しているステーションが AP 有線インターフェイスの DHCP ブロードキャストでも検出された場合、そのステーションは AP と同じ物理有線ネットワークに接続されていることになります。そのようなステーションは、不正デバイスである可能性があり、コントローラによって、不正が AP と同じ有線ネットワークに存在することを示す、有線不正というフラグが設定されます。有線不正の緩和が有効になっていると、緩和アクションがその不正デバイスに対して実行されます。

不正緩和のトラブルシューティング

AP のステーションの検出リスト、またはコントローラの不正リストに不正 AP が表示されていないかどうかをチェックします。

不正の検出に時間がかかり過ぎる場合は、スキャンするチャネルの数を減らしてください。

13 VLAN の設定

仮想ローカル エリア ネットワーク (VLAN) は、有線あるいは無線の複数の LAN セグメントにまたがるブロードキャスト ドメインです。各 VLAN は、個別の論理ネットワークです。組織や機能ごとに、論理的にトラフィックをセグメント化することで、1つのネットワークに複数の VLAN が共存できます。この方法を利用すると、ある部署で使用するすべてのシステムを、物理的な場所に関係なく、相互接続できます。これによって、ブロードキャスト ドメインを制限してセキュリティを向上できます。VLAN をソフトウェアで構成すると、柔軟性が高まります。VLAN は、データ リンク層 (OSI 第 2 層) で動作しますが、しばしば、ネットワーク層 (OSI 第 3 層) で IP ネットワークやサブネットに直接マッピングするよう構成されます。最大 512 の VLAN を作成できます。

IEEE 802.1Q は、VLAN 識別子でトラフィックをタグ付けするのに使用する一般プロトコルです。VLAN1 は、デフォルトまたはネイティブの VLAN と呼ばれ、削除することはできず、すべてのトラフィックがタグ付けされていません。トランク ポートは、複数の VLAN やタグを集約するネットワーク接続であり、一般的には、2つのスイッチやスイッチとルータの間で使用されます。VLAN メンバは、ポート ベース、MAC ベース、プロトコル ベース、または 802.1x プロトコルと組み合わせて使用する認証ベースで設定できます。VLAN では、複数の ESSID と組み合わせて使用し、ESSID と VLAN を 1 対 1 にマッピングするか、複数の ESSID を 1つの VLAN にマッピングすることで、単一のアクセス ポイントで複数のワイヤレス ネットワークをサポートします。セキュリティ プロファイルを VLAN に割り当てると、セキュリティ要件を VLAN の用途に基づき微調整できるため、有線と同等以上のセキュリティをワイヤレス ネットワークで実現できます。

VLAN の割り当ては、RADIUS ベースの MAC フィルタリングや認証の目的で行われます。VLAN の割り当ては、キャプティブ ポータル認証では、いずれの戻り属性によっても実行されません。VLAN は、リモート スイッチに依存しており、リモート スイッチがトランキングをサポートするよう設定されている必要があります。詳細については、フォーティネット Wi-Fi テクノロジー ノート WF107 の「VLAN の 設定とデプロイ」を参照してください。このドキュ

メントには、スイッチで推奨される設定と VLAN 設定とデプロイに関する包括的な説明が記載されています。



AP122 および AP822 をブリッジ モードで配備する場合は、1 から 4 までの固定 /RADIUS VLAN を作成しないことを推奨します。

VLAN の設定とデプロイ

VLAN は、E(z)RF Network Manager またはコントローラのいずれかで設定 / 所有できます。読み取り専用フィールドである Owner が nms-server または controller のどちらであるかによって、プロファイルがどちらで設定されたのかを確認できます。

ESSID を VLAN にマッピングするには、VLAN を最初に設定する必要があります。VLAN を CLI から作成するには、vlan *name* tag *id* コマンドを使用します。name は 16 文字以下の英数字で、tag *id* は 1 ~ 4,094 の間で指定できます。

たとえば、guest という名前の VLAN を、タグ番号 1 で作成するには、グローバル設定モードで以下のように入力します。

```
controller (config)# vlan guest tag 1
controller (config-vlan)#
```

上記でプロンプトが変更されたことで分かるように、VLAN 設定モードに入り、VLAN インターフェイスの IP アドレス、デフォルト ゲートウェイ、DHCP パススルーまたはオプションで DHCP サーバを割り当てることができます (指定すると、この DHCP サーバが、コントローラの DHCP サーバの設定より優先されます)。

以下の例では、次のパラメータが設定されます。

- VLAN インターネットの IP アドレス : 10.1.1.2 でサブネット マスクが 255.255.255.0
- デフォルト ゲートウェイ : 10.1.1.1
- DHCP サーバ : 10.1.1.254

```
controller (config-vlan)# ip address 10.1.1.2 255.255.255.0
controller (config-vlan)# ip default-gateway 10.1.1.1
controller (config-vlan)# ip dhcp-server 10.1.1.254
controller (config-vlan)# exit
controller (config)#
```

VLAN を GUI から作成するには、[Config] > [Wired] > [VLAN] > [Add] をクリックします。

VLAN のブリッジ AP

ESS の作成時に、AP400/AP822/AP832、FAP-U421EV、FAP-U423EV、AP1000 を、トラフィックをイーサネット インターネットにブリッジするよう設定できます。この方法を、ブリッジ VLAN データプレーン モード (ESSID ごと) と呼び、リモート AP モードと呼ぶこともあります。これら 2 つの AP モデルでは、ポートの出口で 802.1Q VLAN タグを使用してイーサネット フレームをタグ付けでき、802.1p 優先度ビットを設定できます。ブリッジは、ESS プロファイルの Dataplane Mode パラメータを Bridged (デフォルトは Tunneled) に設定することで構成します。

トンネル モードでは、ESS のすべてのトラフィックが AP からコントローラに送信され、そこからさらに転送されます。この設定は、ESS プロファイルごとに実行します。ブリッジ モードでは、クライアント トラフィックはローカル スイッチに送信されます。フォーティネットの制御と調整のトラフィックは、この場合にも、AP とコントローラの間で送信されます。

リモート AP400 は、FortiWLC (SD) 4.0 以降で VLAN を使用できます。ESS の設定時に、Dataplane Mode 設定で、AP/ コントローラ設定のタイプを選択します。

ブリッジ VLAN でサポートされているもの：

- 非仮想セル
- 仮想ポート
- MAC フィルタリング /1x/WPA/WPA2 の RADIUS プロファイル
- WMM に定義されている標準 DSCP/802.1q の AC マッピング
- MAC フィルタリング /1x/WPA/WPA2 の RADIUS プロファイル
- RADIUS によって割り当てられた VLAN (802.1x の場合にも)
- QoS ルール

ESSID の設定については、本書の ESSID の章を参照してください。

ブリッジ モードでの有線ポート向け VLAN タギング

ブリッジ モードで有線ポート向けの VLAN タギングを有効にできます。有線ポートの VLAN タギングでは、4 つの VLAN ポリシーが提供されます。

- VLAN なし

- 固定 VLAN: VLAN タグは、0 ～ 4094 の有効な範囲内で設定します。



AP110/1014 ではサポートされていません。

VLAN タギングの設定

CLI の使用

Port プロファイル設定で、以下のコマンドを使用してポリシーと VLAN タグを指定します。

- default (config-port-profile)# port-ap-vlan-policy
- default(config-port-profile)# port-ap-vlan-tag

ブリッジ モードでの動的 VLAN のサポート

AP がトンネルおよびブリッジ モードのときに、RADIUS サーバで VLAN を動的に割り当てることで、ステーションで IP を動的に受け取ることができます。



- 動的 VLAN はキャプティブ ポータルではサポートされません。
- AP が接続しているスイッチ ポートには、適切な VLAN をタグ付けする必要があります。

VLAN の削除

VLAN が ESSID に割り当てられている場合は (139 ページの第 6 章「ESS の設定」を参照)、その VLAN を削除できません。E(z)RF Network Server で作成された VLAN は削除できません。Network Server から実行する必要があります。コントローラに作成された VLAN を削除するには、グローバル設定モードで以下のコマンドを使用します。

```
no vlan name
```

たとえば、vlan1 という名前の VLAN を削除するには、以下のように入力します。

```
controller (config)# no vlan vlan1  
controller (config)#
```

VLAN に関する詳細

FortiWLC (SD) では、仮想 LAN (VLAN) および GRE (Generic Routing Encapsulation) トンネルの両方を構成して物理的な制約ではなく論理的な制約を加えることで、トラフィックを分割するためのコマンドが利用できます。VLAN の代わりとして、GRE トンネルをいずれかのイーサネット インターフェイスで設定できます (セキュリティの章の「[GRE トンネルの設定](#)」を参照)。VLAN と GRE のトンネルをネットワーク内で共存させ、部署や機能ごとにトラフィックを論理的にセグメント化できます。この方法を利用すると、ある部署で使用するすべてのシステムを、物理的な場所に関わらず、相互接続できます。これによって、ブロードキャスト ドメインを制限してセキュリティを向上できます。

VLAN を複数の ESSID と一緒に使用すると (第 6 章「[ESS の設定](#)」を参照)、単一のアクセス ポイントで複数のワイヤレス ネットワークをサポートできます。ESSID と VLAN の 1 対 1 マッピングを作成することも、複数の ESSID を単一の VLAN にマッピングすることもできます。

VLAN によるセキュリティ設定のカスタマイズもサポートされています。VLAN にセキュリティ プロファイルを割り当てることで、VLAN の使用を基準とするセキュリティ要件を調整できます (詳細は、第 9 章「[セキュリティの設定](#)」を参照してください)。

VLAN プール

大規模なブロードキャストの削減や、アドレス空間が枯渇するリスクの軽減のために、ESS プロファイルで VLAN プールを有効にできるようになりました。

VLAN プールによって基本的に、管理者は VLAN のサブセットを使用して名前の付いたエエリアスを作成し、アドレスのプールを作成できます。VLAN プールを有効にすることで、クライアント / デバイスを特定の VLAN に関連付けることができます。これによって、適切なまたは個別の VLAN プールを監視することで、効果的にネットワークを管理できます。

特長

- 最大 16 の VLAN をプールに関連付けることができます。
- 最大 64 の VLAN プールを作成できます。
- VLAN に関連付けられるクライアントの最大数を指定できます。
- プール内の VLAN に関連付けられたクライアント / デバイスの動作は変わりません。
- VLAN が VLAN プールから削除されても、VLAN に接続されているクライアント / デバイスは、引き続き VLAN に関連付けられます。ただし、クライアントが切断されて再接続すると、VLAN は変わります。

設定

Web UI の使用

1. VLAN タグを作成します。

VLAN Configuration (8 entries)

<input type="checkbox"/>	VLAN Name	Tag	Ethernet Interface Index	IP Address	Netmask
<input type="checkbox"/>	WMHS-Private	20	1	172.20.0.30	255.255.0.0
<input type="checkbox"/>	NGES_Private	17	1	172.17.0.30	255.255.0.0
<input type="checkbox"/>	Primary-School	18	1	172.18.0.30	255.255.0.0
<input type="checkbox"/>	GCPS-Public	25	1	172.25.0.2	255.255.0.0
<input type="checkbox"/>	GCPS-BYOD	10	1	10.10.0.2	255.255.0.0
<input type="checkbox"/>	vlan112	112	1	172.18.112.222	255.255.0.0
<input checked="" type="checkbox"/>	Guest-BYOD-1	120	1	10.11.120.2	255.255.0.0
<input checked="" type="checkbox"/>	Guest-BYOD-2	122	1	10.17.100.2	255.255.0.0

2. VLAN プールを作成し、1つまたは複数の VLAN タグを割り当てます。これらの VLAN タグは別のプロファイルで使用されていないことを確認してください。

VLAN Pool Configuration - Add

VLAN Pool Name: BYOD-Pool (Enter 1-64 chars., Required)

Vlan Pool Tag List: 120,122 (Enter the tags using comma separator)

3. VLAN プールのリストを確認します。

VLAN Pool Configuration (1 entry)

<input type="checkbox"/>	VLAN Pool Name	Vlan Pool Tag List
<input checked="" type="checkbox"/>	BYOD-Pool	120,122

CLI の使用

1. VLAN を設定します。

```
default(config)# vlan vlan10 tag 10
```

```
default(config-vlan)# ip address 10.0.0.222 255.255.255.0
```

```
default(config-vlan)# ip default-gateway 10.0.0.1
```

```

default(config-vlan)# exit
default(config)# exit
default# sh vlan vlan10

VLAN Configuration

VLAN Name                : vlan10
Tag                       : 10
Ethernet Interface Index  : 1
IP Address                : 10.0.0.222
Netmask                   : 255.255.255.0
IP Address of the Default Gateway : 10.0.0.1
Override Default DHCP Server Flag : off
DHCP Server IP Address    : 0.0.0.0
DHCP Relay Pass-Through   : on
Owner                    : controller
Maximum number of clients : 253

```

2. VLAN プールを設定します。

```

default(config)# vlan-pool vlangroup
default(config-vpool)# tag-list 10,36
default(config-vpool)# exit
default(config)# exit
default# sh vlan-pool

VLAN Pool Name      Vlan Pool Tag List
vlangroup           10,36
VLAN Pool Configuration(1 entry)

```


14 アクセス ポイントの設定

本章では、以下の手順を説明します。

- [AP 検出の仕組み \(347 ページ\)](#)
- [Web UI による AP の追加と設定 \(348 ページ\)](#)
- [Web UI による AP の無線の設定 \(351 ページ\)](#)
- [CLI による AP の追加と設定 \(354 ページ\)](#)
- [CLI による AP の無線の設定 \(358 ページ\)](#)
- [AP の無線チャネルの設定 \(362 ページ\)](#)
- [Sitesurvey \(362 ページ\)](#)
- [AP でサポートされている運用モード \(382 ページ\)](#)
- [外部アンテナのゲインの設定 \(384 ページ\)](#)
- [自動 AP アップグレード \(384 ページ\)](#)

AP 検出の仕組み

アクセス ポイントの検出には、以下の 3 種類があります。

- レイヤ 2 のみ - アクセス ポイントはコントローラと同じサブネットです。
- レイヤ 2 優先 - アクセス ポイントはブロードキャストを送り、まず、レイヤ 2 の検出を試行することでコントローラを探します。応答がなかった場合には、アクセス ポイントはレイヤ 3 の検出を試行します。
- レイヤ 3 優先 - アクセス ポイントはレイヤ 3 の検出を最初に試行することで、検出メッセージをコントローラに送ります。応答がなかった場合には、アクセス ポイントはレイヤ 2 の検出を試行します。
- レイヤ 3 のみ - アクセス ポイントはレイヤ 3 のみを試行することで、検出メッセージをコントローラに送ります。

レイヤ 2 とレイヤ 3 の検出では、アクセス ポイントは、コントローラが見つかるまで、レイヤ 2、レイヤ 3、およびメッシュ (メッシュが有効である場合) を交互に繰り返します。



それぞれの検出サイクルで、AP は、2 秒間隔で 5 回のブローブ要求を送信します。

アクセス ポイントは、DHCP から固有の IP アドレスを取得することも (デフォルトの方法)、ユーザが固定 IP アドレスを割り当てることもできます。アクセス ポイントは、自身の IP アドレスを取得した後に、コントローラの IP アドレスを探す必要があります。デフォルトでは、レイヤ 3 の検出を使用すると、アクセス ポイントは DNS を使用し、ホスト名を問い合わせることで、コントローラの IP アドレスを取得します。デフォルトのホスト名は「wlan-controller」です。ここでは、DNS サーバがコントローラがあるドメインの名前を認識していると仮定しています。ドメイン名は AP の設定から入力することも、DHCP サーバから取得することもできますが、ドメイン名がないと、レイヤ 3 設定の AP は、コントローラを見つけることができません。また、AP を設定して、コントローラの IP を直接指定することもできます (コントローラの固定 IP が設定されている場合)。

アクセス ポイントは、コントローラの IP アドレス取得後に、UDP ポート 9393 を使用して検出メッセージを送信します。コントローラがこのメッセージを認識すると、AP とコントローラの間にリンクが形成されます。

OAP832 および OAP433 の検出シーケンス

OAP832 と OAP433 がたとえ L3 のみのモードで設定されていても、アクセス ポイントは L3 優先モードを使用してコントローラを検出します。L3 優先モードが失敗すると、L2 モードにフォールバックします。

Web UI による AP の追加と設定

AP をコントローラに追加する場合は、次の特性を設定できます。

- AP ID
- AP 名
- シリアル番号
- 場所、建物、フロア
- 連絡先
- LED モード
- ブートスクリプト (AP 初期化スクリプト)

- データプレーン暗号化
- AP ロール
- 親 AP ID
- リンク プローブ期間
- 電源タイプ
- AP 屋内 / 屋外タイプ

フォーティネット アクセス ポイントは、レイヤ 2 ネットワークまたはレイヤ 3 ネットワーク 経由でコントローラに接続できます。AP を追加し、設定するには、次の手順を実行します。

1. [Configuration] > [Devices] > [APs] > [Add] をクリックします。
[AP Table Add] ウィンドウが表示されます。

図 65: AP をネットワークに追加する

AP Table - Add

AP ID	<input type="text"/>	Valid range: [0-9999], Required
AP Name	<input type="text"/>	Enter 1-63 chars., Required
Serial Number	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Location	<input type="text"/>	Enter 0-64 chars.
Building	<input type="text"/>	Enter 0-64 chars.
Floor	<input type="text"/>	Enter 0-64 chars.
Contact	<input type="text"/>	Enter 0-64 chars.
LED Mode	Normal <input type="button" value="v"/>	
AP Init Script	<input type="text"/>	Enter 0-64 chars.
Dataplane Encryption	On <input type="button" value="v"/>	
Parent AP ID	<input type="text"/>	Valid range: [0-9999]
Link Probing Duration	120 <input type="text"/>	Valid range: [1-32000]
Power Supply Type	802.3-af <input type="button" value="v"/>	
AP Indoor/Outdoor type	Indoor AP <input type="button" value="v"/>	
KeepAlive Timeout(seconds)	25 <input type="text"/>	Valid range: [1-1800]

2. 以下の値を指定し、[OK] をクリックします。

フィールド	説明
AP ID (必須)	最大 9999 文字の固有の AP 数字 ID。
AP Name (必須)	アクセス ポイントの識別子として割り当てる、64 文字以下の英数字。AP を説明する、ビル内の設置場所などを表す分かりやすい名前を指定するといいいでしょう。
Serial Number (オプション)	これらのボックスは、AP の底部にある、長いパーツ番号の一部である MAC アドレスを記録するためのものです。MAC アドレスは、末尾 12 桁の数字です。
Location (オプション)	64 文字以下の英数字
Building (オプション)	64 文字以下の英数字
Floor (オプション)	64 文字以下の英数字
Contact (オプション)	64 文字以下の英数字
LED Mode (オプション)	<p>AP332/AP400 および AP1000 の LED 表示を設定します。</p> <p>Normal: LED についての説明は、『アクセス ポイント インストール ガイド』に記載されています。</p> <p>Node ID: リリース 5.1 ではサポートしていません</p> <p>Blink: すべての LED が点滅するよう設定します。これは、1 つの AP を特定するのに便利です。点滅の順番は、AP モデルによって異なります。</p> <p>Dark: 電源以外のすべての LED をオフにします。</p>
AP Init Script (オプション)	ブート時にアクセス ポイントが実行する初期化スクリプトの名前。
Dataplane Encryption (オプション)	<p>メッシュ構成で、AP とコントローラのデータ パケットの受け渡し方法を選択します。</p> <p>On: AP とコントローラのリンクが暗号化されます</p> <p>Off: AP とコントローラのリンクが暗号化されません (デフォルト)</p>
AP Role (オプション)	<p>メッシュ構成で、AP のメッシュにおける役割を決定します。</p> <p>access: アクセス ポイントは、標準の AP として動作します。</p> <p>wireless: アクセス ポイントは、エンタープライズ メッシュ構成の一部であり、802.11/bg クライアントに対するワイヤレス アクセス サービスと、802.11/a リンクのバックホール サービスを提供します。</p> <p>gateway: アクセス ポイントは、エンタープライズ メッシュ構成の一部であり、有線とワイヤレスのサービス間のリンクを提供します。</p>

フィールド	説明
Parent AP ID (オプション)	メッシュ構成で、ワイヤレス AP に親 AP からのシグナルを検出するよう指示することで、バックホール接続によるワイヤレス AP を提供します。複数の AP を同じ親 AP ID に割り当てることができます。
Link Probing Duration (オプション)	コントローラのリンクが切断した場合のブリッジ AP のリポートまでの待機時間 (1 ~ 32000 分)。この設定をリモート AP 設定で使用することで、リモート コントローラへの接続が切断した場合の AP のリポートを回避できます。デフォルトは 120 です。
KeepAlive Timeout (seconds)	KeepAlive Timeout (seconds) には、AP へのリンクがダウンした場合であっても、コントローラの観点から、リモート AP がオンライン状態であり続ける時間 (1 ~ 1800 秒) を指定します。コントローラから AP への検出メッセージは、[Link Probing Duration] ボックスと [KeepAlive Timeout (seconds)] で指定した時間によって変更されます。デフォルトは 25 です。
AP Indoor/ Outdoor AP (オプション)	屋内と屋外の AP では、チャネルや電力レベルの規制設定が異なります。この設定で、それらの値を調整します。

Web UI による AP の無線の設定

348 ページの「[Web UI による AP の追加と設定](#)」が終了すると、AP の無線が FortiWLC (SD) に表示されるようになります。以下の手順に従って、無線を設定します。

1. [Configuration] > [Wireless] > [Radio] をクリックします。
2. 1 つ目の列の鉛筆のアイコンをクリックして、いずれかの無線を選択します。多くの AP には、無線が 2 つあるので注意してください。その場合には、両方の無線を設定します。
3. 無線の設定には、[Wireless Interface]、[Wireless Statistics]、[Antenna Property] の 3 つのタブを使用します。[Wireless Interface] がデフォルトのタブです。無線の既存のインターフェイス設定がここに表示されます。グレー表示されている設定は変更できません。以下のチャートに従って変更し、[OK] をクリックします。

フィールド	説明
Interface Description	256 文字以下の英数字を使用でき、スペースも使用できます (たとえば、Lobby AP interface 1)。デフォルトでは、ieee80211-ap_id-index_ID という説明が設定されます。
Administrative Status	インターフェイスを使用するかどうかを表します。 Up: インターフェイスを有効にします Down: インターフェイスを無効にします

フィールド	説明
Primary Channel	ドロップダウン リストから、使用するワイヤレス インターフェイスのチャンネル番号を選択します。表示されるチャンネル番号は、[RF Band Selection] と各国の規制ドメインによって異なります。たとえば、米国の 802.11b にはチャンネル 1 ～ 11 が表示され、802.11a にはチャンネル 36、40、44 などが表示されます。2 つのアクセス ポイントが同じチャンネルにある場合のみ、同じ仮想 AP に属することができます。したがって、異なるチャンネルにある 2 つの近接するアクセス ポイントは、シームレス ハンドオフ (0 ms) を実行できません。
Short Preamble	短いプリアンプルは、無線において効率性が高いですが、すべてのクライアントでサポートされているわけではありません。 On Off
RF Band Selection	このインターフェイスが使用する RF バンドを選択します。利用可能な選択肢は、AP モデルとインストールされている無線カード (たとえば、802.11an)、および有効なライセンスによって異なります。
Transmit Power (EIRP)	フォーティネット AP の無線は、デフォルトでは、最大電力レベルで動作します。電力レベルが高ければ、クライアント ステーションが受信するフレームのシグナル強度が高くなり、クライアント ステーションが高速でフレームをデコードできるようになり、カバレッジ エリアが広がります。フォーティネットは仮想セル テクノロジを使用しているため、このことで、干渉が最小限に抑えられ、再アソシエーションなしにより良い AP へとクライアントを移動できるようになります。極めて稀な状況では、同一チャンネル干渉のために、AP の電力レベルを下げることを推奨します。サポートに連絡して、問題が間違いなく同一チャンネル干渉によるものであることを確認してください。転送能力を変更するには、[Transmit Power High (dBm)] フィールドの値を変更します。最大レベルは、国コードや使用する RF バンドによって異なります。
AP Mode	インターフェイスの無線が Normal Mode (クライアントのサービスを最初に実行し、バックグラウンドでスキャンを実行する) または Scanning Mode (不正 AP の監視専用) のいずれであるかを選択します。
B/G Protection Mode	802.11b/g 相互運用モードを設定します。この設定のデフォルトは auto であり、変更する場合は、必ずフォーティネット サポートに相談してください。
HT Protection Mode	HT 保護はデフォルトで Off に設定されます。オプションは以下のとおりです。 On Off Auto

フィールド	説明
channel width	<p>以下を設定できます。</p> <p>20 MHz</p> <p>40MHz Extension Channel Above</p> <p>40MHz Extension Channel Below</p> <p>1 つの仮想セル内のすべての AP が同じチャネル幅である必要があります。</p>
MIMO Mode	<p>次のいずれかを選択します。</p> <p>2x2 AP1000 で、802.3af PoE を使用する場合</p> <p>3x3 AP400 の場合 (無線と電源の構成によって異なります)</p>
802.11n Only Mode	<p>802.11n Only Mode は、N 対応の AP400/AP1000 に使用します。次のいずれかを選択します。</p> <p>On: 802.11n のみをサポートします</p> <p>Off : (デフォルト) 802.11an または 802.11bn をサポートします</p>
RF Virtualization Mode	<p>このフィールドは、基底となる AP が AP400 モデルである場合のみ表示されます。基底となる AP がこれ以外の AP である場合、このフィールドは GUI にグレー表示されます。RF Virtualization Mode のデフォルト値は Virtual Port です。オプションは、Virtual Port、Virtual Cell、および Native Cell です。</p>
Probe Response Threshold	<p>プローブ応答しきい値を入力します。有効な範囲は 0 ~ 100 です。</p>
Mesh Service Admin Status	<p>メッシュ サービス管理ステータスを有効 (Enable) または無効 (Disable) にします。</p>
Transmit Beamforming Support	<p>送信ビームフォーミング サポートを選択します。</p> <ul style="list-style-type: none"> • Disabled • SU-MIMO • MU-MIMO (802.11ac Wave 2 対応クライアントをサポートする場合) <p>AP832、AP822、FAP-U421EV、FAP-U423EV でのみサポートしています。</p>
STBC Support	<p>STBC サポートを選択します。</p> <p>On</p> <p>Off</p>

フィールド	説明
DFS Fallback Option	<p>レーダー検出時に AP の異なるチャンネルへのフォールバックを許可する場合に選択します。AP1xx、AP433、AP 8xx、AP1xxx、AP332、FAP-U421EV、FAP-U423EV でのみサポートしています。</p> <p>DFS Fallback Option を有効にすると、以下ようになります。</p> <ul style="list-style-type: none"> DFS Fallback Channel に 52 が選択されます。 DFS Channel Revertive に 45 分が設定されます。 レーダーが検出されると、フォールバック チャンネル 52 が 60 秒間チェックされ、レーダーが検出されない場合はチャンネル 52 に切り替わります。 45 分経過すると、元の動作チャンネルに戻ります (チャンネル有効テストにパスし、チャンネルが利用可能な場合)。 <p>DFS Fallback Option を無効にすると、以下ようになります。</p> <ul style="list-style-type: none"> レーダーが検出されると、システムによってフォールバック チャンネルが選択されます。 30 分経過すると、元のチャンネルに戻ります (チャンネルを 60 秒間監視して、チャンネル有効テストにパスした場合)。
DFS Fallback Channel	フォールバック チャンネルを選択します。
DFS Channel Revertive (minutes)	AP が元のチャンネルに戻る時間を選択します。



AP1000 無線は常に仮想セルが有効ですが、AP1000 を非想セル モードで使用方法もあります。
「[CLI による ESS の追加](#)」を参照してください。

CLI による AP の追加と設定

CLI で AP を設定するには、最初に AP 設定モードに入り (以下に示す最初のコマンド)、それ以外の AP 設定コマンドを使用します。

コマンド	目的
configure terminal	グローバル設定モードに入ります。
ap ap-id	指定した AP の AP 設定を入力します。show ap コマンドを使用して、AP のリストを取得します。

コマンド	目的
... commands ...	次のチャートに記載されている AP 設定コマンドをここに入力します。
boot-script string	ブート時にアクセス ポイントが実行する初期化スクリプトの名前。ここで何も設定しないと、AP はデフォルトのブート スクリプトを使用します。
building string	ビルを識別する説明を入力します。
contact string	AP の連絡先情報を入力します。
connectivity l2-only l2-preferred l3-preferred	この設定で、コントローラへのレイヤ 2 またはレイヤ 3 接続を設定します。l3-preferred または l2-preferred のいずれかを使用すると、接続設定が追加された場合に、AP 接続モードが呼び出されます。
dataplane-encryption {on off}	メッシュ構成で、AP とコントローラのデータ パケットの受け渡し方法を選択します。 On: AP とコントローラのリンクが暗号化されます。 Off: AP とコントローラのリンクが暗号化されません (デフォルト)。
description string	AP の説明を入力します。これが GUI に表示される AP 名になります。
floor string	AP のフロアを入力します。
led {normal blink NodeId Normal}	AP400 および AP1000 の LED 表示を設定します。 Normal: AP400 および AP1000 の LED は、『フォーティネット アクセス ポイント インストール ガイド』に記載されているとおりに表示されます。 Blink: すべての LED が点滅するよう設定します。これは、1 つの AP を特定するのに便利です。 Dark: すべての LED をオフにします。
link-probing duration minutes	リモート AP の場合は、キープアライブ シグナルの間隔を分数で設定します。1 ~ 3200 の間の分数を指定できます。
location string	AP の場所情報を入力します。
mac-address ff:ff:ff:ff:ff:ff	AP を事前に設定する場合に、MAC アドレスを設定します。
model string	AP を事前に設定する場合に、AP のモデル タイプを入力します。

コマンド	目的
no boot-script	ブートスクリプトを無効にします。
end	特権 EXEC モードに戻ります。

CLI によるレイヤ 3 AP の設定

以下のコマンドを使用すると、コントローラと同じサブネットにない AP のレイヤ 3 設定をセットアップできます。AP が DHCP から自分自身の IP アドレスを取得できるように指定することで、IP アドレスの取得に DNS サーバを使用できるようになります。ネットワーク管理者が「wlan-controller」というホスト名のコントローラの IP アドレスを DNS サーバに追加していれば、DNS はその「wlan-controller」というホスト名をもつコントローラの IP アドレスを返すことができます。

```
default# configure terminal
default(config)# ap 1
default(config-ap)# connectivity l3-preferred
default(config-ap-connectivity)# ip address dhcp
default(config-ap-connectivity)# controller hostname wlan-controller
default(config-ap-connectivity)# end
default#
```

以下の表は、ap-connectivity モードで利用できるコマンドです。

表 22: 接続モードコマンドのまとめ

コマンド	目的
controller {domainname name hostname name ip <ip-address>}	コントローラの IP 情報を設定します。 domainname name は、1 ～ 63 文字の文字で指定します。 hostname name は、1 ～ 63 文字の文字で指定します。 IP アドレスを nnn.nnn.nnn.nnn という形式で指定するか、dhcp と指定して動的に AP IP アドレスを取得します。
hostname name	AP ホスト名を設定します。名前は、1 ～ 63 文字の文字で指定します。
ip address {ip-address dhcp}	AP の IP アドレス設定を指定します。 ip-address を使用すると、AP に固定アドレスを割り当てます。 dhcp を使用すると、動的に AP の IP アドレスを取得します。

表 22: 接続モードコマンドのまとめ

コマンド	目的
ip default-gateway gateway	デフォルト ゲートウェイの IP アドレスを、nnn.nnn.nnn.nnn という形式で追加します。
ip dns-server {primary <DNS ip-address> secondary <DNS ip-address>}	固定 IP のエントリを DNS サーバに追加します。 primary ip-address は、固定 IP に対するプライマリ DNS サーバを設定します。 secondary ip-address は、固定 IP に対するセカンダリ DNS サーバを設定します。

CLI による AP 電源、チャネル幅、MIMO モードの設定

以下の手順で、電源タイプ、チャネル幅、MIMO モードを設定します。

1. コントローラのターミナル セッションを開きます。
2. CLI プロンプトで、terminal configuration コマンドを使用して、設定モードに入ります。
3. ap # コマンドを使用して AP を選択します。以下の例では AP1 を選択します。

```
default(config)# ap 1
```

4. CLI コマンド power-supply を使用して、AP Power、802.3af Power Over Ethernet、802.3-at Power Over Ethernet、または dual-802.3-af Power Over Ethernet の 5V-DC に値を設定します。

```
default(config-ap)# power-supply 5V-DC
```

5. ap 設定モードを終了します。

```
default(config-ap) # exit
```

6. interface Dot11Radio **node-id interface_ID** コマンドを使用して、無線設定サブモードに入ります。たとえば、AP1 に対してはインターフェイス 1 を使用します。

```
default(config)# interface Dot11Radio 1 1
```

7. channel-width コマンドを使用して、チャネル幅を 20 MHz (デフォルト) から、40 MHz (40-mhz-extension-channel-above または 0-mhz-extensionchannel- below 40) に変更します。このコマンドで、チャネル ボンディングも設定されます。

```
default(config-if-802)# channel-width above 40 MHz Extension channel
```

8. mimo-mode 3x3 コマンドを使用して MIMO Mode を 2x2 (デフォルト) から 3x3 に変更し、終了します。

```
default(config-if-802)# mimo-mode 3x3
default(config-if-802)# end
```

これで、AP が設定されました。

CLI による AP の無線の設定

無線のいずれかを設定するには、無線インターフェイス設定モードに入る必要があります。以下の手順に従ってください。

表 23: 無線インターフェイス設定モードに入る

コマンド	目的
configure terminal	グローバル設定モードに入ります。
interface Dot11Radio <ap-id> <Interface ID>	特定の AP および無線インターフェイスのためのインターフェイスの設定に入ります。無線インターフェイスのリストを取得するには、show interfaces Dot11Radio を使用します。 AP800 の場合は、第 2 インターフェイスが 802.11ac サポートを提供します。
... commands ...	802.11 設定コマンドをここに入力します。
end	特権 EXEC モードに戻ります。
copy running-config startup-config	これは、エントリを設定ファイルに保存するためのオプションの手順です。

無線インターフェイス設定コマンドのまとめ

無線インターフェイス設定モードで利用できるコマンドは、以下のとおりです。

表 24: 無線インターフェイス設定モードで使用できるコマンド

コマンド	目的
admin-mode	無線インターフェイスを有効または無効にします。
antenna-property	外部ワイヤレス インターフェイス アンテナを管理します。
channel	チャネル ID を設定します。
localpower	すべての AP の AP 転送電力レベルを設定します。

表 24: 無線インターフェイス設定モードで使用できるコマンド

コマンド	目的
mode	AP モード設定
n-only-mode	パフォーマンス向上の目的で、無線で 802.11n クライアントのみをサポートします。
preamble-short	短いプリアンプルを有効または無効にします。
protection-mode	802.11b/g 相互運用モードを設定します。この設定のデフォルトは auto であり、変更する場合は、必ずフォーティネット サポートに相談してください。
rf-mode	無線周波数モード (802.11a、b、g、bg、bgn、または an) を設定します。仮想セル内の同じチャネルのすべての AP は、rf-mode が同じ設定である必要があります。
scanning channels	チャネルのスキャンを設定します。
tuning	ワイヤレス インターフェイスをチューニングします。

CLI による無線転送電力の設定

無線転送電力は、AP のカバレッジ エリアを変更し、この設定によって、近接するアクセス ポイント間のコンテンションを容易に管理できるようになります。フォーティネット AP での転送電力は、アンテナでの EIRP1 (Effective Isotropic Radiated Power : 実効等方輻射電力) として定義され、アンテナ ゲインが含まれます。(この点を覚えておくことが重要で、転送電力はコネクタでの電力ではありません)。電力レベル設定は、国コードや使用する無線バンド (および、802.11a の場合にはチャネル) に依存します。

たとえば、転送電力を localpower で 20 dBm2 に設定し、アンテナ ゲインを 3 から 2 dBm に設定すると、コネクタの実転送電力は 18 dBm になります。

8dBi (isotropic) ゲインの外部アンテナを使用する場合は、ゲイン値を同じ値、8 に調整します。アンテナの後の希望する EIRP が同じである場合は、転送電力を同じ値である 20 のままにします。EIRP 値を高くしたり低くしたりするには、転送電力を希望する値に調整します。

最大電力設定は、802.11/bg 無線の場合で、4 ~ 30dBm の整数です。

802.11a の最大転送電力は、使用中のチャネルによって異なります。詳細を、下表に記載します。ここに記載されているのは、米国の電力レベルです。

802.11a チャネル	米国における最大転送電力 (dBm)
36	17
40	23
44	23

802.11a チャンネル	米国における最大転送電力 (dBm)
48	23
52	30
56	30
60	30
64	30
100	30
104	30
108	30
112	30
116	30
120	30
124	30
128	30
132	30
136	30
140	30
149	36
153	36
157	36
161	36
165	36

Dot11 無線インターフェイス設定モードで `localpower` コマンドを使用すると、最大電力レベルを設定できます。

```
localpower max-level
```

たとえば、802.11a の無線最大電力を 15 に設定するには、以下のように入力します。

```
localpower 15
```

CLI による短いプリアンプルの有効化と無効化

無線プリアンプル (ヘッダとも呼びます) は、パケットの先頭にあるデータ区分で、ここには、パケットの送受信でアクセス ポイントとクライアント デバイスが必要とする情報が格納されています。デフォルトでは、短いプリアンプルに設定されますが、長い無線プリアンプルにすることも、短い無線プリアンプルにすることもできます。

- プリアンプルを短くすると、スループットのパフォーマンスが向上します。
- プリアンプルを長くすると、アクセス ポイントと旧式のワイヤレス LAN カードとの互換性が保証されます。旧式のワイヤレス LAN カードを使用していない場合は、短いプリアンプルを使用してください。

短いプリアンプルを無効にする、すなわち長いプリアンプルを使用するには、以下のように入力します。

```
no preamble-short
```

短いプリアンプルを有効にするには、以下のように入力します。

```
preamble-short
```

CLI による不正 AP スキャンのための無線の設定

不正 AP のスキャン処理を定期的に行うように無線を設定するには、Dot11 無線インターフェイス設定モードで、以下のコマンドを使用します。

```
mode scanning
```

無線のクライアント サービスを復帰するには、以下のコマンドを使用します。

```
mode normal
```

CLI による無線インターフェイスの有効化 / 無効化

無線インターフェイスを一時的に無効にするには、Dot11Radio インターフェイス設定モードで、以下のコマンドを使用します。

```
admin-mode Down
```

後で、オフラインのインターフェイスを有効にするには、以下のコマンドを使用します。

```
admin-mode Up
```

CLI による 802.11n のみをサポートする無線の設定

AP 無線インターフェイスを設定して、802.11n クライアントのみをサポートし、スループットを向上させるようにするには、Dot11 無線インターフェイス設定モードで以下のコマンドを使用します。

```
n-only-mode
```

802.11n のみのサポートを無効にするには、以下のコマンドを使用します。

```
no n-only-mode
```

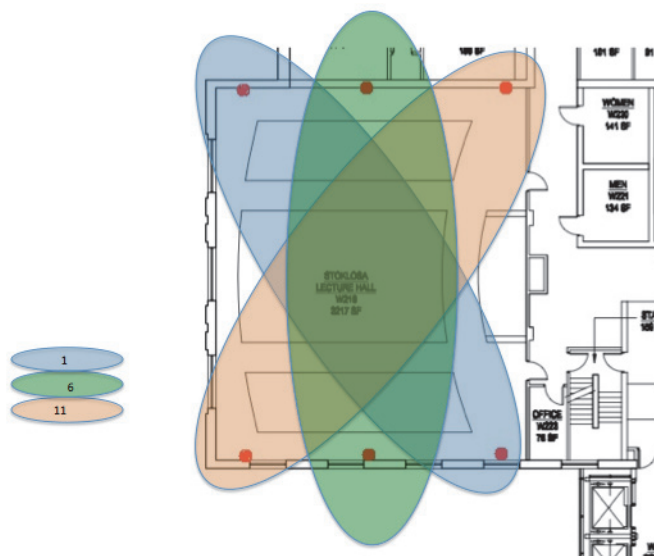
仮想セル内の同じチャネルのすべての AP は、n-only が同じ設定である必要があります。

AP の無線チャネルの設定

AP チャネルの設定は、米国内での導入においては、11 のオーバーラップ チャネルで構成される 802.11bg に対して設定できます。802.11a に対するチャネルの設定は、802.11a スペクトラム内でオーバーラップするチャネルがないため、発生しません。

802.11b/g 規格には、14 個のチャネルがあります。FCC の規則の結果として 11 個のチャネルがあり、米国では 1 ~ 11 までのチャネルを使用します。それ以外の国では、チャネル 12、13、14 も使用している可能性があります。これらのチャネルは、ワイヤレス伝送波の中心周波数を表します。実際には、802.11bg ではある一定のエリアの 3 つの運用周波数だけを設定でき、多くの環境では、それぞれにオーバーラップがない、チャネル 1、6、11 を使用します。

図 66: チャネル 1、6、11



チャネルを割り当てるには、Dot11Radio インターフェイス コマンドの channel を使用します。Web UI では、[Configuration] > [Wireless] > [Radio] をクリックしてチャネルを設定し、ドロップダウン リストから [Channel] を選択します。

Sitesurvey

フォーティネットの Sitesurvey は、ネットワークのプランニングを支援する簡単なツールで、クライアントが高いスループットで受信でき、優れたカバレッジを保证するための AP の正し

い位置（設置場所）を探すのに役立ちます。AP の正しい位置を探すには、Wi-Fi クライアントを sitesurvey モードの AP に接続し、設置しようとする場所の周辺を移動して、Wi-Fi クライアントへの接続が良好な状態になるエリアを (Sitesurvey ツールからの結果に基づいて) 特定します。Sitesurvey の結果を見ながら、AP の位置を調整できます。

前提条件

- Sitesurvey は、AP832、AP822、FAP-U421、FAP-U423 でのみサポートしています。
- AP で FortiWLC (SD) 6.1-2 以上が動作している必要があり、Open Clear モードでのみ接続できます。

Sitesurvey オプションの設定

Sitesurvey の設定と監視のオプションは、CLI (AP ブート コンソール) と GUI から使用できます。Sitesurvey のオプションにアクセスするには、コンソールから AP CLI に接続するか、シリアル ポートを使用します。

CLI の使用

通常の AP ブート プロセスの後に、AP ブート プロンプトに sitesurvey enable コマンドを入力して、AP を Sitesurvey モードで再起動します。Sitesurvey モードでは、AP に sitesurvey プロンプト (ss) が表示されます。

Sitesurvey のコマンドはすべて、sitesurvey キーワードで開始しますが、sitesurvey キーワードの代わりに ss (別名) を使用することもできます。Sitesurvey では、Sitesurvey の機能を設定および監視するための以下の追加コマンドを使用できます。

Sitesurvey の有効化

```
sitesurvey enable
```

このコマンドで、sitesurvey モードが有効になります。AP が sitesurvey モードでリブートし、Sitesurvey のプロンプトが表示されます。

```
ss > _
```

Sitesurvey の無効化

```
sitesurvey disable
```

このコマンドで、sitesurvey モードが無効になります。AP が通常の動作モードでリブートします。

国コードとチャネルの設定

```
sitesurvey countrycode set <country code>
```

デフォルトでは、国コードは US に設定されます。国コードを設定する場合、その国コードの最初の有効なチャネルと無線 0 および無線 1 の最大サポート Tx 電力は自動的に設定されます。国コードのデフォルト チャネルを上書きするには、以下のコマンドを入力します。

```
sitesurvey channel set <radio_index> <channel>
```

次のように設定します。

- radio_index は、AP 無線を指定します。
- 無線 1 (2.4 Ghz) の場合は「1」を入力します。
- 無線 2 (5 Ghz) の場合は「2」を入力します。

サポートしている国コードのリストを取得するには、`ss countrycode help` コマンドを使用します。

非アクティビティ時間の設定

```
sitesurvey inactivitytime <itime>
```

このコマンドは、クライアントと関連付けられる前に AP が Sitesurvey モードのままである時間 (単位: 秒) を設定します。時間は秒単位で指定し、デフォルトでは、AP が 3600 秒間、Sitesurvey モードのままになります。非アクティビティ時間が経過すると、AP は通常の AP モードにリポートします。



GUI を使用している場合、非アクティビティの状態が 3600 秒間続くと、非アクティビティ時間の設定に関係なく、ブラウザ ウィンドウがリセットされます。ブラウザの再読み込み時間は変更できません。

IP アドレスの設定

```
sitesurvey ipconfig <ip_address> <netmask>
```

このコマンドは、Sitesurvey AP に IP アドレスを設定します。この IP アドレスを使用すると、ブラウザから Sitesurvey の GUI にアクセスできます。デフォルトでは、IP アドレスとネットマスクはそれぞれ、192.168.0.1 と 255.255.255.0 に設定されます。

SSID の設定

```
sitesurvey ssid <radio_index> [<ssid>]
```

次のように設定します。

- radio_index は 0、1、または 3
- 無線 0 (2.4 Ghz) の場合は「1」を入力します
- 無線 1 (5 Ghz) の場合は「2」を入力します
- 両方の無線の SSID を指定する場合は「3」を入力します

このコマンドは、指定した無線の SSID を設定します。デフォルトでは、無線 1 (2.4Ghz) の SSID は Meru_Site_Survey_2.4 に、無線 2 (5 Ghz) の SSID は Meru_Site_Survey_5 に設定されます。

例

```
ss > sitesurvey ssid 3
```

MERU_SITE_SURVEY SSID 無線 1 と無線 2 の両方に対し、MERU_SITE_SURVEY という MERU_SITE_SURVEY SSID が割り当てられる

```
ss > sitesurvey ssid 1 <-- SSID を指定しない場合、デフォルトでは無線 1 には  
MERU_SITE_SURVEY_2.4 という SSID が割り当てられる
```

```
ss > sitesurvey ssid 2 <-- SSID を指定しない場合、デフォルトでは無線 2 には  
MERU_SITE_SURVEY_5 という SSID が割り当てられる
```

```
ss > sitesurvey ssid 3 <-- SSID を指定しない場合、無線 1 には MERU_SITE_SURVEY_2.4  
が SSID として割り当てられる
```

無線 2 には MERU_SITE_SURVEY_5 が SSID として割り当てられる

SSID を AP 無線に設定した後に、以下のコマンドを使用して、SSID のブロードキャストを無線ごとに有効または無効にできます。

```
sitesurvey publishssid <radio_index> [on|off]
```

デフォルトでは、両方の無線の SSID がブロードキャストされます。

無線の有効化 / 無効化

```
sitesurvey {radio | r} <radio_index> [on|off]
```

次のように設定します。

- radio_index は 0、1、または 3
- 無線 1 (2.4 Ghz) の場合は「0」を入力します。
- 無線 2 (5 Ghz) の場合は「1」を入力します。
- 両方の無線の場合は「3」を入力します。

このコマンドは、AP 無線を有効または無効にします。Sitesurvey AP に接続する Wi-Fi クライアントは、AP で有効になっているのと同じ無線を使用する必要があります。デフォルトでは、両方の無線が有効です。

Sitesurvey 更新レートの設定

```
sitesurvey statsrefrate [<rate>]
```

このコマンドは、AP が Sitesurvey の結果を収集して送信 (表示) する間隔 (ミリ秒で指定) を設定します。デフォルトでは、更新レートは 1000 ミリ秒に設定されます。Sitesurvey の結果は、Sitesurvey の GUI ページまたは CLI から参照できます。

転送電力の設定

```
sitesurvey txpwr set <radio_index> [<tx_power>]
```

次のように設定します。

- radio_index は 0、1、または 3
- 無線 1 (2.4 Ghz) の場合は「0」を入力します
- 無線 2 (5 Ghz) の場合は「1」を入力します
- 両方の無線の場合は「3」を入力します

このコマンドを使用して、いずれかの AP 無線の転送電力を設定します。デフォルトでは、転送電力は、国コード、チャンネル、およびハードウェアの機能に基づく最大可能転送電力に設定されます。sitesurvey txpwr set 3 コマンド (転送電力値なし) は、両方の無線を選択した国でサポートしている最大転送電力に設定します。

Sitesurvey 設定の保存

```
sitesurvey save
```

すべての Sitesurvey オプションを設定したら、このコマンドを入力して Sitesurvey の設定を保存します。このコマンドは、設定したすべてのパラメータを使用して ESSID を作成します。これで、Wi-Fi を ESSID を使用してこの AP に関連付けることができます。

GUI の使用

Sitesurvey の GUI ページにアクセスするには、AP の IP アドレスを入力します。設定していない場合は、AP のデフォルト IP アドレス (192.168.0.1) を入力します。デフォルトでは、GUI ページに Sitesurvey の結果ページが表示されます。[Configure] ボタンをクリックして、Sitesurvey 設定オプションにアクセスします。

図 67: Sitesurvey 設定オプション:

The screenshot shows the 'Site Survey' configuration window for Meru Networks. The window is titled 'Site Survey' and features the Meru Networks logo. The configuration is organized into two columns for Radio 0 and Radio 1. The settings include:

- SSID Radio 0:** MERU_SITE_SURVEY_2.4
- SSID Radio 1:** MERU_SITE_SURVEY_5
- Country:** UNITED STATES (dropdown menu)
- Radio 2.4 Ghz:** ON (dropdown menu)
- Radio 5 Ghz:** ON (dropdown menu)
- TX Power Radio 0:** 25 dBm (5 to 25 dBm)
- TX Power Radio 1:** 23 dBm (7 to 23 dBm)
- 2.4 Ghz Channels:** 6 (dropdown menu)
- 5 Ghz Channels:** 36 (dropdown menu)
- Publish SSID Radio 0:** ON (dropdown menu)
- Publish SSID Radio 1:** ON (dropdown menu)
- Stats Refresh Rate:** 1000 msec
- Inactivity timeout period:** 3600 sec

At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

表 25: GUI を使用する Sitesurvey 設定パラメータ

パラメータ	説明
SSID Radio 0 SSID Radio 1	Wi-Fi クライアントの接続でブロードキャストする値を入力します。デフォルト値は、Radio 0 の場合は Meru_Site_Survey_2.4、Radio 1 の場合は Meru_Site_Survey_5 です。
Country	このリストから国を選択します。この選択によって、それぞれの無線の最初の有効チャンネルが自動的に設定されますが、異なるチャンネル番号を選択することで選択を上書きできます。
Radio 2.4 Ghz Radio 5 Ghz	ON または OFF を選択して、無線を有効または無効にします。
Tx Power Radio 0 Tx Power Radio 1	それぞれの無線の転送電力を入力します。Radio 0 (2.4 Ghz) の最大値と Radio 1 (5 Ghz) の最大値は、選択した国とチャンネルによって異なります。
2.4 Ghz Channels 5 Ghz Channels	有効なチャンネルを選択します。デフォルトでは、選択した国の最初の有効チャンネルに自動的に設定されます。
Publish SSID Radio 0 Publish SSID Radio 1	SSID のブロードキャストを ON または OFF のどちらにするかを選択します。

表 25: GUI を使用する Sitesurvey 設定パラメータ

パラメータ	説明
Stats Refresh Rate	Sitesurvey の結果を収集して送信 (表示) する間隔 (ミリ秒) を入力します。
Inactivity timeout period	AP がクライアントの接続を待機する間隔 (ミリ秒) を入力します。非アクティビティ時間が経過すると、AP は通常の AP モードにリブートします。

上記のパラメータを設定したら、[Apply] ボタンをクリックして設定を保存します。

Sitesurvey 結果の表示

Sitesurvey 結果は、CLI や GUI で参照できます。

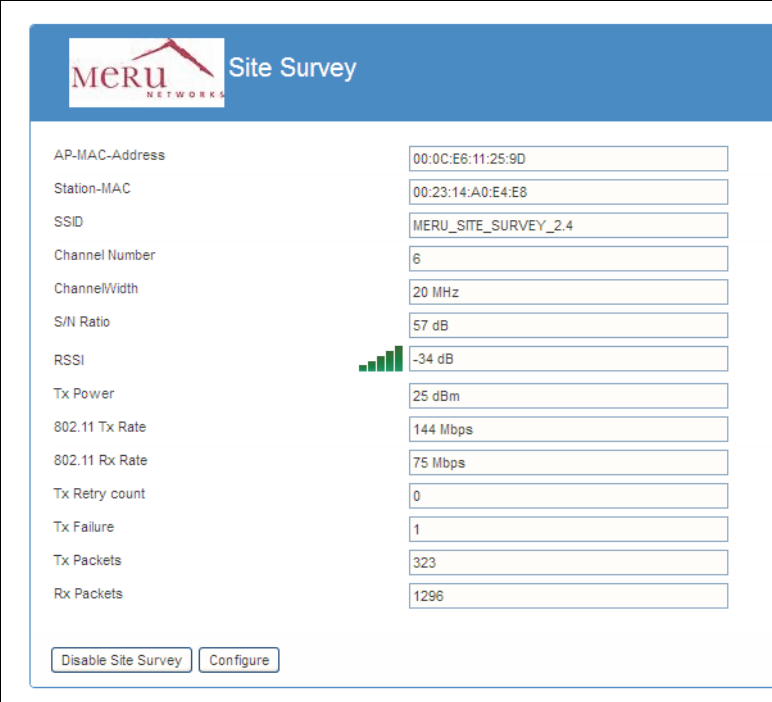
GUI の使用

デフォルトでは、ブラウザで AP に接続すると、Sitesurvey ページ (下図) が表示されます。Sitesurvey ページには、Wi-Fi クライアントの接続に関する重要な情報や、設定されている値が表示されます。



GUI ページには、AP に接続されている 1 つのクライアントのみの Sitesurvey 結果が表示されます。接続されているすべてのクライアントの Sitesurvey 結果を表示するには、CLI のオプションを使用します。

図 68: Sitesurvey 結果の表示



The screenshot displays the Meru Networks Site Survey web interface. At the top, there is a blue header with the Meru Networks logo and the text "Site Survey". Below the header, a list of network parameters is shown on the left, with their corresponding values in input fields on the right. The parameters include AP-MAC-Address, Station-MAC, SSID, Channel Number, Channel Width, S/N Ratio, RSSI, Tx Power, 802.11 Tx Rate, 802.11 Rx Rate, Tx Retry count, Tx Failure, Tx Packets, and Rx Packets. The RSSI field includes a green signal strength indicator. At the bottom, there are two buttons: "Disable Site Survey" and "Configure".

Parameter	Value
AP-MAC-Address	00:0C:E6:11:25:9D
Station-MAC	00:23:14:A0:E4:E8
SSID	MERU_SITE_SURVEY_2.4
Channel Number	6
Channel Width	20 MHz
S/N Ratio	57 dB
RSSI	-34 dB
Tx Power	25 dBm
802.11 Tx Rate	144 Mbps
802.11 Rx Rate	75 Mbps
Tx Retry count	0
Tx Failure	1
Tx Packets	323
Rx Packets	1296

Buttons: [Disable Site Survey](#) [Configure](#)

接続パラメータ

Sitesurvey の RSSI、S/N Ratio、Tx Power、802.11 Tx Rate、802.11 Rx Rate などのパラメータは、ある場所における Wi-Fi クライアントの接続を表します。

パラメータのトラブルシューティング

Tx Retry count パラメータと Tx Failure パラメータは、ある場所での Wi-Fi クライアントと AP の接続で発生した問題やエラーを表します。

ネットワーク パラメータ

Tx Packets と Rx Packets は、AP と Wi-Fi クライアントの間のネットワーク データ トラフィックを表します。

注：Wi-Fi クライアントを持ってユーザが移動すると、設定されている更新レートごとに Sitesurvey 結果が更新されます。

Sitesurvey の無効化

AP の Sitesurvey を無効にするには、[Disable Sitesurvey] ボタンをクリックします。このボタンによって、AP が通常の AP モードでリブートします。

CLI の使用

Sitesurvey 設定の表示

```
sitesurvey showconfig
```

このコマンドで、現在の Sitesurvey 設定が表示されます。

出力例

```
ss > sitesurvey showconfig

Site Survey                : 1
Country Code               : US
AP IP address              : 192.168.0.1
AP Netmask                  : 255.255.255.0
SSID for radio0            : MERU_SITE_SURVEY_2.4
SSID for radio1            : MERU_SITE_SURVEY_5
Broadcast SSID for radio0  : 1
Broadcast SSID for radio1  : 1
radio0 <2.4G>              : 1
radio1 <5G>                : 1
Channel for radio0         : 6
Channel for radio1         : 36
Tx Power for radio0       : 25
Tx Power for radio1       : 23
Basic Tx Rate for radio0  : 1 2 5.5 11
Basic Tx Rate for radio1  : 1 2 5.5 11
Stats Refresh Rate        : 1000
```


Inactivity Timeout : 3600

ss >

Sitesurvey 結果 (統計) の表示

sitesurvey showstatistics

このコマンドで、AP に接続されているすべての Wi-Fi クライアントの Sitesurvey 結果が表示されます。

出力例

ss > sitesurvey showstatistics

ss >

AP MAC			STATION MAC			ESSID		Ch	ChWd	SNR
RSSI	TxPwr	TxRate	RxRate	TxRetry	TxFail	TxPkts	RxPkts			

- - - - -										
00:0c:e6:12:28:1f	6c:88:14:f3:a8:04						survey51	36	20	42
-45	23	144	130	0	1	65	68 ss stats			

ss >

AP MAC			STATION MAC			ESSID		Ch	ChWd	SNR
RSSI	TxPwr	TxRate	RxRate	TxRetry	TxFail	TxPkts	RxPkts			

- - - - -										
00:0c:e6:12:28:1f	6c:88:14:f3:a8:04						survey51	36	20	42
-45	23	144	130	0	1	66	68 ss stats			

ss >

AP MAC			STATION MAC			ESSID		Ch	ChWd	SNR
RSSI	TxPwr	TxRate	RxRate	TxRetry	TxFail	TxPkts	RxPkts			

- - - - -										
00:0c:e6:12:28:1f	6c:88:14:f3:a8:04						survey51	36	20	42
-45	23	144	123	0	1	68	68 ss stats			

ss >

AP MAC		STATION MAC			ESSID		Ch	ChWd	SNR
RSSI	TxPwr	TxRate	RxRate	TxRetry	TxFail	TxPkts	RxPkts		

- -----									
00:0c:e6:12:28:1f	6c:88:14:f3:a8:04	survey51					36	20	42
-45	23	144	104	0	1	69	691		

ss >

無線リソースの自動プロビジョニング (ARRP)

ARRP 機能を使用することによって、各 AP はすべてのチャンネルをスキャンし、コントローラにスキャンの詳細情報を提供します。コントローラでは、この情報を使用して、使用できる最良のチャンネルを無線ごとに選択して割り当てます。デフォルトでは、この機能は無効になっています。

- 11ac AP でのみサポートされています。
- 有効にすると、仮想セルが 11ac AP で利用できなくなります。
- 11ac AP 以外の AP は設定どおりに機能し続け、自動チャンネル機能による影響を受けません。
- AP は、初期計画と動的チャンネルの両方の変更後に、新たに割り当てられたチャンネルにリブートします。
- ARRP を無効にすると、11ac AP はすべてデフォルトのチャンネルにリブートします。

Web UI を使用した設定

この機能を有効にするには、[Configuration] > [Wireless] > [ARRP] に移動し、[Configuration] タブで [Auto Channel] オプションを有効にします。

Automatic Radio Resource Provisioning ?

ConfigurationAP - Radio Interfaces

Auto Channel

☒

Radio 1 Planning Channel

1

20 MHz

Radio 2 Planning Channel

149

40 MHz Extension channel above

Auto Power

☐

Freeze

☐

Timer State

☐

Timer (min)

15

Valid range: [15-3600]

DFS

☐

- Planning Channel: 有効にすると、全 AP の各無線は、無線 1 と無線 2 に選択されたチャンネルに設定されます。上掲のスクリーンショットでは、[Radio 1 Planning Channel] には 1 /20MHz が設定され、[Radio 2 Planning Channel] には 149/40MHz が設定されています。全 AP で受信したレポートに基づき、コントローラは最適なチャンネルを割り当てます。DFS チャンネルは、Planning Channel として設定するために利用することはできません。
- Auto Power: Auto Power オプションをいつ有効にしたかに関係なく、Auto Power 機能が適用されるのは、必ずチャンネルの割り当て後になります。有効にすると、コントローラは (チャンネルごとに) 近接する 11ac AP 間で最適な電力レベルを判断します。ARRP 機能が有効なときにのみ、Auto Power オプションを有効にし、適用できます。
- Freeze: このオプションは、初期計画フェーズの後に適用されます。このオプションを無効にすると、11ac AP は、割り当てられているチャンネルで定期的なスキャンを (1 分経つごとに) 実行します。これは、チャンネルの品質を判断するために使用されます。(3 連続スキャンに基づき) チャンネルの品質がしきい値の上限を超えると、チャンネルの変更要求が送信されます。有効にすると、チャンネル品質に関係なく、定期的なスキャンが無効になり、11ac AP は割り当てられたチャンネルのままになります。
- このオプションを無効にすると、無線インターフェイス設定は変更できなくなります。
- Timer State と Timer: このオプションは、Freeze オプションが無効のときのみ利用できます。頻繁なチャンネル変更を回避するために、チャンネル スキャンが 15 分ごとに行われるように間隔を設定できます。デフォルトでは Timer の間隔には 15 分が設定されており、

3600 分まで指定できます。有効にすると、AP は 15 分経過するたびにチャンネル品質スキャンを開始し、10 分間に 1 分ごとのスキャンを継続します。この期間に収集されたデータに基づき、チャンネルの変更が発生する場合があります。スキャンの 10 分が終了すると、次の 15 分間はチャンネルのスキャンが無効になります。

- DFS: デフォルトでは、計画フェーズでの DFS チャンネルのスキャンと割り当ては無効になっています。有効にすると、AP は DFS チャンネルをスキャンできるようになります。また、AP には DFS チャンネルを割り当てることができるようになります。
- DFS オプションは、ARRP が有効になっているときに選択する必要があります。Auto RF を有効にしてから DFS を有効にすると、すべての AP へのチャンネル割り当て再計画が必要になります。
- REPLAN: このオプションは、初期計画が完了した後に、新しい AP がネットワークに追加された場合に使用されます。

[AP-Radio Interfaces] タブには、すべての AP が表示されます。また、各 AP の動作周波数と転送電力も表示されます。

CLI を使用した設定

- 現在の設定を表示するには、`show arrp-config` コマンドを使用します。

```
MC-4200-AC-MCA(15)# show arrp-config
```

```
MCA Global Settings
```

```
Enable/Disable Auto Channel : enable
```

```
Radio 1 Channel              : 11
```

```
Radio 1 Channel Width       : 20-mhz
```

```
Radio 2 Channel              : 48
```

```
Radio 2 Channel Width       : 20-mhz
```

```
Auto Power on/off           : off
```

```
Freeze yes/no                : No
```

```
Timer State on/off          : on
```

```
Timer                        : 15
```

```
Dfs on/off                   : on
```

- AP のリストと、それらの動作周波数と電力の値を表示するには、`show arrp-ap-radio-interface` コマンドを使用します。

```
MC-4200-AC-ARRP(15)# show arrp-ap-radio-interface
```

AP ID	AP Name	Radio1 oper ch	Radio2 oper ch	Radio1 Transmit Power (dBm)	Radio2 Transmit Power (dBm)
3	AP-3	6	36	24	23
4	AP-4	1	36	24	23
6	AP-6	6	40	24	23
13	AP-13	1	36	24	23
17	AP-17	1	36	24	23
19	AP-19	6	36	10	13
20	AP-20	6	36	24	23

ARRP radio interfaces(7 entries)

- ARRP 機能を設定および使用するには、`arrp global` コマンドに続けて、以下のいずれかのオプションを使用します。

-auto-power - To enable or disable auto allocation of transmit power

-dfs - To enable or disable the use of DFS channels in planning

-disable - To disable ARRP

-Enable - To enable ARRP

-Freeze- To enable or disable dynamic channel scanning

-radio1-channel-planning- To specify channel for initial planning

-radio2-channel-planning- To specify channel for initial planning

-replan- To perform re-planning if a new AP has joined network

-timer-state- Enable or disable to avoid frequent channel change

-timer-value- To specify the time interval for the dynamic channel scan

制限事項

- 無効にすると、自動チャネル機能が有効になる前に AP が vCell プロファイルの一部であったかどうかに関係なく、既存の vCell プロファイルはすべての 11ac AP にプッシュされます。ネイティブ セルのプロファイルは変更されません。
- 自動電力機能の一部として、電力レベルが高いと報告されていた近接の AP の電力レベルが低下した場合、AP での Tx 電力レベルはデフォルトの高い値には戻りません。

802.11k/r の設定

コントローラ ドメイン内で利用可能な最良のアクセス ポイント間で高速ローミングを実現する 802.11r の実装から、デバイスに関するメリットを得られます。また、802.11k 仕様の実装により、802.11k ネイバーと無線測定レポートを計算できるようになります。

高速ローミング機能と 802.11k は、ESS プロファイルで設定できます。

サポートされているアクセス ポイント : AP122、AP822、AP832、OAP832

制限事項

- 802.11K/v/r 仕様に準拠しているクライアントのみにサポートされています。
- 高速ローミングはインターコントローラ ローミングでは利用できません。

802.11K の有効化

Web UI の使用

- [Configuration] > [Wireless] > [ESS] に移動し、[ESS Profile] タブで以下を変更します。
 - [802.11R] で、[On] を選択します。
 - [802.11r Mobility Domain] で、整数値を入力します。
 - [802.11k] で、[On] を選択して無線測定を実行します。

802.11r	On ▼
802.11r Mobility Domain	7 Valid range: [1-65535]
802.11k	Off ▼

CLI の使用

```
default(15)# configure terminal
default(15)(config)# essid fastroam-1
default(15)(config-essid)# 802.11r on
default(15)(config-essid)# 802.11k on
default(15)(config-essid)# 802.11r-mobility-domain-id 100
```

ローミング アクセス コントローラ (RAC)

クライアントは、同一サブネットでも異なるサブネットでも、2つの異なるコントローラに接続されたアクセス ポイント間でローミングできます。FortiWLC (SD) では、固定ローミングまたは動的ローミングを指定できます。

RAC を有効にするにあたり、以下の点を考慮してください。

- RAC を有効にした ESS プロファイルで IP プレフィックス検証をオフにする必要があります。
- RAC は複数の ESSID で有効にできます。
- ESSID プロファイルのいずれかのパラメータが変更されたら、RAC を停止し、ローミング ドメイン内のすべてのコントローラに対し、ESSID に加えられた変更を更新する必要があります。
- コントローラ IP の IP アドレスをローミング ドメインに追加する前に、その IP にアクセスできることを確認します。
- show roaming-domain all コマンドの出力において、VLAN カラムの -1 の値は、ローミング ドメイン内の別のコントローラにトンネリングしていることを示します。

[static DHCP home configuration] では、ホーム コントローラとして (ローミング ドメイン内の) いずれかのコントローラを指定します。ローミング ドメイン内のいずれかのコントローラと関連付いているクライアントは、このホーム コントローラから IP アドレスを受信します。コントローラがホーム コントローラに設定されると、ESS プロファイルに設定されている「Tunnel Interface Type」のとおり、そのコントローラのすべてのネイティブ VLAN、設定済みの VLAN、動的な VLAN 設定に適用されます。

[dynamic DHCP home configuration] では、初めてコントローラに関連付けられたクライアントは、そのコントローラから継続して IP アドレスを受信し、ホーム コントローラのクライアントになります。動的なローミングを許可するには、ホーム コントローラの IP アドレスに 0.0.0.0 を設定します。

ローミングのタイムアウト

動的なローミング シナリオにおいて、クライアントがカバレッジ エリアから離れ、設定されているタイムアウト値を超えた間隔で戻ると、関連付けが新たに発生し、クライアントはホーム コントローラとは異なるコントローラと関連付けられる場合があります。クライアントのローミングのタイムアウト値 (分) は CLI で設定できます。

```
default(15)(config)# roaming-domain roam-time-out 70
```

デフォルトかつ最小のタイムアウト値は 60 分であり、240 分まで指定できます。ローミングのタイムアウトのカウントダウンは、クライアントがカバレッジ エリアから離れるとすぐに開始されます。

注 : RCA が停止すると、既存のクライアントはすべて強制的に認証が解除され、再接続が必要になります。クライアントでローミングが使用されているかどうかに関係なく、このプロセスはローミング ドメイン内のすべてのクライアントに適用されます。

RAC の設定に必要なステップ

固定ローミング

1. ローミング ドメインの ESSID を指定します。
2. メンバコントローラとして、コントローラの IP アドレスを追加します。
3. ホームコントローラとして、コントローラの IP アドレスを追加します。
4. ピアコントローラを追加したら、上記の手順を繰り返します。ESSID 名とホームコントローラの IP アドレスは変更しないようにします。

動的なローミング

1. ローミング ドメインの ESSID を指定します。
2. メンバコントローラとして、コントローラの IP アドレスを追加します。
3. ホームコントローラの IP アドレスとして、0.0.0.0 を追加します。
4. ピアコントローラを追加したら、上記の手順を繰り返します。ESSID 名とホームコントローラ IP アドレス (0.0.0.0) は変更しないようにします。

Web UI を使用した設定

1. [Configuration] > [Wired] > [RAC] に移動します。
2. [Peer Controllers] タブで以下を追加します。
 - ESSID: これは、ローミング ドメイン内のすべてのコントローラで完全に一致させる必要があります。
 - ピアコントローラの IP アドレス

- ホーム DHCP コントローラの IP アドレスローミング ドメイン内のホーム コントローラの IP アドレス。アクセスしているクライアントからの DHCP パケットはすべてホーム コントローラに転送され、ホーム コントローラでローカルに配信されます。

- [Roaming Domain State] で [Enable] を選択します。

CLI を使用した設定

RAC を設定するための新しい CLI コマンド `roaming-domain` と以下のオプションが利用できます。

- `ssid` - ローミング ドメイン内の 6 つすべてのコントローラで利用可能な共通の ESSID を指定します。
- `start` - RAC を開始します。
- `stop` - RAC を停止します。
- `peer-controller` - ローミング ドメイン内でピア コントローラの IP アドレスを指定します。
- `homedhcp-controller` - ローミング ドメイン内のホーム コントローラを指定します。

例

```
default(15)(config)# roaming-domain start

default(15)(config)# roaming-domain ssid Roaming1 peer-controller 10.10.1.20
                        homedhcp-controller 10.10.12.100
```

動的な DHCP ホーム

```
default(15)(config)# roaming-domain ssid Roaming1 peer-controller 10.10.1.20
                        homedhcp-controller 0.0.0.0.
```

アクセス ポイントの交換

以下のような場合、AP を交換できます。

- AP に障害がある場合。障害のある AP と同じモデルの新しい AP と交換できます。
- 旧 AP モデルから新 AP モデルに移行する場合。

アクセス ポイントを交換する前の確認事項

アクセス ポイントを交換するにあたり、以下の重要ポイントを覚えておく必要があります。

- ある AP モデルを別のモデルに交換しても、一般的には、当初の設定が保持されます。新しい AP に、古い AP にはない設定があると、それらの設定はデフォルトに設定されます。
- AP を交換しても一部の設定や構成は引き継がれますが、AP400 を異なるモデル (AP1000 など) に単純に交換できるというわけではありません。これら 2 つのモデルの機能や構成の仕様は大きく異なり、同じではないと考えるべきです。

アクセス ポイントの交換方法

既存の AP を新しい AP モデルに交換する場合は、ap-swap コマンドを使用すると、サイトの AP 設定の更新が容易になります。ap-swap コマンドを使用するには、新旧の AP の MAC アドレスが必要です。MAC アドレスは、2 つの方法で確認できます。show ap コマンドで、交換する AP の MAC アドレスを確認できます。また、AP の背面でも MAC アドレスを確認できます。ラベルのバーコードの下にシリアル番号が記載されており、このシリアル番号の末尾 12 桁が AP の MAC アドレスです。

ap-swap コマンドを使用すると、交換する AP の MAC アドレスを新しい AP の MAC アドレスに置換できます。2 つの番号を置換テーブル内の AP ID にリンクさせることで、システムは古い AP の設定済みの設定を新しい AP に割り当てることができます。記録される設定としては、チャンネル番号、プリアンプル、および電源の設定があります。入れ替えのための情報を入力したら、show ap-swap コマンドを使用して、AP を物理的に交換する前に AP の MAC 設定をもう一度確認します。

MAC アドレスの再確認が終わったら、古い AP をシステムから外してオフラインにします。AP を交換します。AP が検出されると、置換テーブルがチェックされ、その変更内容が新しい AP に適用されます。新しい AP が更新されると、その AP のエントリが置換テーブルから削除されます。

AP を交換する手順をまとめると、次のようになります。

```
meru-wifi (config)# show ap ( 交換する AP のシリアル番号を取得する )
meru-wifi (config)# swap ap 00:0c:e6:00:00:66 00:CE:60:00:17:BD
meru-wifi (config)# exit
meru-wifi# show ap-swap
  AP Serial Number      New AP Serial Number
00:0c:e6:00:00:66      00:ce:60:00:17:bd
AP Replacement Table(1 entry)
meru-wifi# show ap
```

AP を交換するためのコマンドを完了したら、古い AP を取り外して、ステータスが Disconnect/offline と表示されているのを確認し、古い AP を新しい AP に交換します。

AP 交換後の設定の更新

表 26: AP 交換後の設定の更新

AP タイプ	設定の変更	その他
どちらの AP (新しい AP と交換した古い AP) も同じ	以下の設定が保持される : <ul style="list-style-type: none"> • ATS-Entry: AP name、location、Contact、Descr、KeepAlive • 802.11 Entry: RFTYPE、Channel、Tx Power、Channel-Width、VCell Mode • ESS-AP Entry: BSSID、Channel 	通常、障害のある AP を交換する場合に使用される。
AP モードが異なる	以下の AP 設定のみが保持される <ul style="list-style-type: none"> • ATS-Entry: AP 名、ロケーション、連絡先、説明、KeepAlive 以下の無線 /BSSID 設定は、新しい AP モデルのデフォルト設定に変更される。 <ul style="list-style-type: none"> • 802.11 Entry: RFTYPE、Channel、Tx Power、Channel-Width、VCell Mode • ESS-AP Entry: BSSID、Channel 	通常、古い AP モデルから新しい AP モデルに移行する際に実行される。 例 : AP1020/AP1010 から AP822 への移行

AP でサポートされている運用モード

2 つの無線を搭載する AP332/AP400/AP832 と AP1000 は、どちらも 5.0 GHz になるように設定できますが、両方の無線を 2.4 GHz に設定することはできません。両方の無線を 2.4 GHz で使用する場合は、無線を別々のチャンネルにします。

AP1000 の無線は、デフォルトで以下のバンドに設定されます。

AP モデル	無線 1	無線 2	無線 3
AP122	BGN	AC	-
AP332	BGN	AN	-
AP1010	BGN		-
AP1020	BGN	AN	-

AP モデル	無線 1	無線 2	無線 3
AP400	BGN	AN	両方のバンドをスキャン (AP433is)
AP822	BGN	AC	
AP832	BGN	AC	-
FAP-U421EV	BGN	AC	-
FAP-U423EV	BGN	AC	-

セキュリティ モード

AP400/AP1000 は、802.11i セキュリティ標準でサポートされているすべてのセキュリティ モデル (WEP、WPA、WPA2、および混在モード) をサポートしていますが、802.11n は、平文と WPA2 セキュリティのみをサポートしています。802.11n をどのセキュリティ モードにも設定できますが、WPA2 または平文を使用する場合のみ、11n のメリットが生まれます。そのため、WEP または WPA に設定した SSID に接続するどの 11n クライアントも、レガシー ABG クライアントと同じように動作します。WEP または WPA のいずれかに設定した 802.11n ESSID には、その ESSID に対応する 802.11n 速度がありません。ESSID を混在モードに設定すると、WPA2 クライアントでのみ 802.11n 速度が有効になり、WPA クライアントはレガシー ABG クライアントのように動作します。詳細については、下表を参照してください。

ESSID セキュリティ	AP400/AP1000 で実現する 11n のメリット
平文および WPA2	すべての 11n のメリットが実現します。
WEP と WPA	11n のメリットは実現しません。クライアントはレガシー ABG クライアントと同じように動作します。
混在モード	混在モードに設定された ESS の 11n パフォーマンスは、ネットワークで使用するアプリケーションの種類によって異なります。混在モードに接続する WPA2 クライアントのみに、11n のメリットが生かされます。WPA クライアントは、レガシー ABG クライアントと同じように動作します。

仮想化された環境での AP

仮想化された環境での同じチャネルの AP はすべて、次の値が同じ設定である必要があります。

- rf-mode
- channel width
- n-only-mode
- channel と MIMO mode

外部アンテナのゲインの設定

AP で生成される総電力が 30dbi を超えることはできません。この数値には、すべてのアンテナ ゲインが含まれます。したがって、アンテナで 2dbi が生成される場合、無線は 28dbi を生成できます。FortiWLC (SD) は、自動的にアンテナ ゲインを設定します。AP400 の場合には、アンテナが 5dbi と仮定されるため、AP400 は 25dbi に設定されます。アンテナによっては、この数値が正しいことも、正しくないこともあります。

アンテナ ゲインを確認し、変更するには、FortiWLC (SD) から以下の手順を実行します。

1. [Devices] の下で [Configuration] > [AP] をクリックします。
2. AP ID を選択します。
3. [Antenna Property] タブをクリックします。
4. [Interface] (1/2) を選択します。
5. 必要であれば、ゲインを変更します。
6. [OK] をクリックします。



アンテナ ゲインが、Dot 11 物理設定で設定された無線のローカル電力を超えることはできません。

自動 AP アップグレード

AP 自動アップグレード機能はデフォルトで有効です。これにより、AP が WLAN に参加すると、コントローラが AP のファームウェアを自動的にアップグレードできるようになります。AP のファームウェアがコントローラのファームウェアと異なるレベルである場合、サービスを提供できなくなります (すなわち、WLAN の一部でなくなります)。

AP が検出段階を開始すると、コントローラがファームウェアのバージョンをチェックし、コントローラのバージョンと同じレベルでない場合は、アップグレードが開始します。この機能によって、AP のグループを既存の WLAN に追加するプロセスが容易になります。

自動 AP アップグレード機能が有効になっていれば、AP とコントローラのソフトウェアバージョンが一致していないことを警告する syslog メッセージや SNMP トラップを介して、影響を受ける AP のアップグレードステータスを確認できます。不一致が存在すると、アラームが SNMP マネージャにディスパッチされます。ファームウェアの AP へのダウンロードが終わると、AP がブートし、検出が試行され、チェックされ、アップグレードの後に、新しいソフトウェアバージョンが実行されます。一致していることが確認されると、AP とコントローラのソフトウェアのバージョンが一致していることを通知する一連の syslog メッセージと SNMP トラップが送信され、アラームがクリアされます。

この機能を無効にする手順は以下のとおりです。

```
default# auto-ap-upgrade disable
default# show controller
Global Controller Parameters
Controller ID                               : 1
Description                                : 3dot4dot1 Controller
Host Name                                   : DC9
Uptime                                      : 03d:01h:17m:33s
Location                                   : Qa scale testbed near
IT room
Contact                                    : Raju
Operational State                          : Enabled
Availability Status                        : Online
Alarm State                               : No Alarm
Automatic AP Upgrade                      : off
Virtual IP Address                        : 192.168.9.3
Virtual Netmask                           : 255.255.255.0
Default Gateway                           : 192.168.9.1
DHCP Server                               : 10.0.0.10
Statistics Polling Period (seconds)/0 disable Polling : 60
Audit Polling Period (seconds)/0 disable Polling      : 60
Software Version                             : 3.7-49
Network Device Id                           : 00:90:0b:07:9f:6a
System Id                                    : 245AA7436A21
Default AP Init Script                      :
DHCP Relay Passthrough                     : on
Controller Model                            : mc3200
Country Setting                             : United States Of America
Manufacturing Serial #                     : N/A
Management by wireless stations            : on
Controller Index                           : 0
Topology Information Update                : off
AP ステータスの表示
```

Web UI で、[Monitor] > [Dashboard] > [Radio] または [Monitor] > [Diagnostics] > [Radio] をクリックして、AP 無線のステータスを表示します。[Help] をクリックするとチャートの説明が表示されます。すべての画面の下のアイコンに、緑の AP (有効) と赤の AP (無効) が表示されます。[Monitor] > [Dashboard] > [System] でも同じ情報を確認できます。

CLI のいくつかのコマンドに、AP ステータスが表示されます。

表 27: システム ステータスを表示するコマンド

コマンド	目的
show ap [index]	シリアル番号、アップタイム、動作ステータス、可用性、アラーム状態、セキュリティ モード、プライバシー ビット、ブートスクリプト、AP モデル、FPGA バージョンなどの AP のステータスを表示します。AP インデックスを指定しないと、AP ステータスの概要が表示されます。
show antenna-property	アンテナのプロパティを表示します。
show ap-connectivity	アクセス ポイント接続を表示します。
show ap-discovered	検出されたアクセス ポイントとステーションのリストを表示します。
show ap-limit	このコントローラにライセンスされている AP 数を表示します。
show ap-siblings	AP シブリング テーブルを表示します。同じチャンネルで動作し、相互にやり取りできる AP のことを、AP シブリングと呼びます。AP は、-80 ~ -85dbm の低い RSSI でビーコンを認識できますが、これより低い RSSI 値は認識できません。
show ap-swap	アクセス ポイントの置換テーブルを表示します。
show ess-ap	アクセス ポイントの ESS-AP テーブルを表示します。
show interfaces Dot11radio	ワイヤレス インターフェイスの設定を表示します。
show interfaces Dot11Radio statistics	ワイヤレス インターフェイスに関連する統計を表示します。
show regulatory-domain	国の規制情報を表示します。
show statistics top10-ap-problem	問題がある上位 10 のアクセス ポイントのリストを表示します。
show statistics top10-ap-talker	最もアクティブな上位 10 のアクセス ポイントのリストを表示します。

表 27: システム ステータスを表示するコマンド

コマンド	目的
show topoap	コーディネータから見た全アクセス ポイントのトポロジを表示します。
show topoapap	AP のすべての組み合わせの間の受信信号強度表示 (Signal Strength Indicator : RSSI) を表示します。

15 QoS (Quality of Service) の設定

QoS ルールは、ネットワーク トラフィック タイプを評価し、優先順位を付けます。たとえば、通話 (VoIP) や、会社の特定の部署 (グループ、VLAN) からのトラフィックを優先させることができます。本章では、ワイヤレス LAN システムの QoS 設定について説明します。

- [Web UI による QoS ルールの設定 \(389 ページ\)](#)
- [CLI による QoS ルールの設定 \(396 ページ\)](#)
- [VoIP の最適化 \(399 ページ\)](#)
- [グローバル QoS 設定 \(402 ページ\)](#)
- [レート制限 QoS ルール \(403 ページ\)](#)
- [コーデック ルールの設定 \(407 ページ\)](#)
- [QoS 統計表示コマンド \(410 ページ\)](#)
- [QoS ルールのその他の例 \(411 ページ\)](#)

Web UI による QoS ルールの設定

GUI から QoS ルールを設定するには、以下の手順を実行します。

1. [Configuration] > [QoS Settings] > [QoS and Firewall Rules] タブをクリックします。
2. [Add] をクリックします。以下の画面が表示されます。

図 69: QoS ルールの追加

3. [ID] フィールドに、QoS ルールの固有数値識別子を入力します。有効な範囲は、0 ～ 6000 です。
4. [Destination IP] フィールドに、QoS ルールの一致基準として使用する宛先 IP アドレスを入力します。宛先 IP アドレスは宛先サブネット マスクと一緒に使用され、一致を決定します。
5. [Destination Netmask] フィールドに、宛先 IP アドレスのサブネット マスクを入力します。
6. [Destination Port] フィールドに、QoS ルールの一致基準として使用する TCP または UDP ポートを入力します。任意のポートを指定するには、0 (ゼロ) を入力します。
7. [Source IP] フィールドに、QoS ルールの一致基準として使用するソース IP アドレスを入力します。ソース IP アドレスはソース サブネット マスクと一緒に使用され、一致を決定します。
8. [Source Netmask] フィールドに、ソース IP アドレスのサブネット マスクを入力します。
9. [Source Port] フィールドに、QoS ルールの一致基準として使用する TCP または UDP ポートを入力します。任意のポートを指定するには、0 (ゼロ) を入力します。
10. [Network Protocol] フィールドに、QoS ルールのフロー プロトコルのプロトコル番号を入力します。プロトコル番号は 0 ～ 255 です。TCP のプロトコル番号は 6、UDP のプロトコル番号は 17 です。プロトコル番号のリストについては、<http://www.iana.org/assignments/protocol-numbers> を参照してください。

QoS プロトコル検出を併用している場合は、ネットワーク プロトコルを QoS プロトコル タイプに一致させる必要があります。以下のネットワーク プロトコルと QoS プロトコルを使用します。

- UDP: SIP
 - TCP: H.323 または SIP
11. ポリシー適用モジュール設定が有効な場合 (オプション機能) は、[Firewall Filter ID] フィールドに、使用するフィルタ ID を入力します (ユーザごと、または ESS ごと)。この ID は 1 ～ 16 文字の英数字にする必要があります。
12. [Packet minimum length] フィールドに、ルールに一致する最小パケット長のサイズを指定します (有効な範囲 : 0 ～ 1500)。
13. [Packet maximum length] フィールドに、ルールに一致する最大パケット長のサイズを指定します (有効な範囲 : 0 ～ 1500)。
14. [QoS Protocol] ドロップダウン リストで、次のいずれかを選択します。
- SIP
 - H.323
 - Other
 - None
- キャプチャ ルールでは、QoS プロトコルがどの QoS プロトコル ディテクタがフローに必要なリソースを自動的に (暗黙的に) 導出するのかを決定します。一致するフローのリソース要件を明示的に指定する場合は、[Other] を選択します。QoS プロトコル値はキャプチャ以外のルールでは無視されます。
15. [Average Packet rate] ボックスに、フローの平均パケット レートを入力します。レート の範囲は 0 ～ 200 パケット / 秒です。
16. [Action] リストで、ルールが指定するアクションを選択します。
- Forward: QoS プロトコル検出を無視し、QoS プロトコル指定の有無にかかわらず、明示的なリソース要求に対してフローを提供します。
 - Capture: システムは、QoS プロトコル検出を使用して、フローのリソース要件を分析します。
 - Drop: フローがドロップされます。
17. [Token Bucket Rate] ボックスに、トークンが架空のトークン バケットに置かれるレート (Kbps または Mbps で指定し、チェックしたオプションによって異なります) を入力します。フローごとに専用のパケットが存在し、一定の速度でそこにトークンが追加 されます。パケットを送信するには、パケットのサイズと等しい数のトークンをバケットから削除する必要があります。十分な数のトークンがないと、バケットに十分な数のトークンが入るまで、システムは待機します。
18. [Priority] ボックスに、フローがベストエフォート キューに置かれる優先度を入力します。優先度が高いベストエフォート キューにあるパケットは、優先度が低いキューのパケットよりも先にアクセス ポイントから伝送されます。ただし、伝送されるのは、予約済みのフローのパケットの後です。
- 優先度の値の範囲は 0 ～ 8 で、0 の優先度が最低、8 の優先度が最高です。デフォルト値

は 0 です。優先度を有効に (0 以外を指定) した場合は、平均パケット レートやトークンパケット レートは指定できません。

19. [Traffic Control] リストで、次のいずれかを選択します。

- On
- Off

すべてのタイプのフロー (明示、検出済み、およびベストエフォート) で、トラフィック制御で [On] を選択すると、ユーザが指定したレートへのフローが制限されます。そのレートより多いパケットはドロップされます。

20. [DiffServ Codepoint] リストで、適用可能な場合は、適切な DiffServ 設定を選択します。

21. [QoS Rule Logging] リストで、この QoS ルールに対するロギング アクティビティを有効にするか無効にするかを選択します。

- On
- Off

22. QoS ロギングが有効な場合、[QoS Rule Logging Frequency] フィールドで、このルールに関連するパケットをログするデフォルト収集間隔を変更します。間隔は 30 ~ 60 (秒) である必要があります。

23. [Match] チェックボックス：対応する [Match] チェックボックスが選択されているフィールドでは、[ACTION] フィールドで示されているアクションが、一致するパケットで実行されます。[Match] チェックボックスが選択されていない場合、フィールドのデータに関係なく、任意の値のパケットが一致し、[ACTION] フィールドで示されているアクションはパケットで実行されません。394 ページの「[\[Match\] チェックボックスと \[Flow Class\] チェックボックスについて](#)」も参照してください。

24. [Flow Class] チェックボックス：[Flow Class] オプションは、フロー制御ルール ([Traffic Control] が有効であり、[Token Bucket Rate] が指定されたルール) およびファイアウォール ルールのみに関連します。一般的にこれは、レート制限です。フィールドの [Flow Class] のチェックがオンになっている場合、パケットがルール (フロー制御またはファイアウォール タイプ) に一致すると、これらのフィールドは [Flow Class] エントリに保存されます。[Flow Class] エントリは 1 組のフローの集約のためにシステムにより使用され、フローが同じような動作を行うようになり、パケットをドロップしたり、または、パケット制限を測定したりできます。

たとえば、ルールに Src IP アドレス 0.0.0.0 が含まれ、[Flow Class] チェックボックスがオンになっていて、[Token Bucket Rate] が 10 キロバイト / 秒に設定されている場合、システムを通過するすべてのパケットはこのルールに一致し、各フローでは最大スループットである 10000 バイト / 秒が可能となります。ルールに Src IP アドレス 10.0.0.10 が含まれ、[Flow Class] チェックボックスがオンになっていて、[Token Bucket Rate] が 10 キロバイト / 秒に設定されている場合は、IP アドレス 10.0.0.10 のマシンから伝送されるすべてのパケットはこのルールに一致する必要があるため、このマシンで許可される累積スルー

ブットはわずか 10000 バイト / 秒にしかありません。[394 ページの「\[Match\] チェックボックスと \[Flow Class\] チェックボックスについて」](#) も参照してください。

25. QoS ルールを追加するには、[OK] をクリックします。

ブリッジ モード トラフィックの QoS ルール

QoS ルールはブリッジ モード トラフィックをサポートします (IPv4)。ブリッジ モード トラフィックでは、以下の条件項目が転送パケットかドロップパケットのいずれかと一致します。

- Destination IP (宛先 IP)
- Destination Port (宛先ポート)
- Source IP (ソース IP)
- Source Port (ソースポート)
- Network Protocol (ネットワーク プロトコル): ブリッジ モード トラフィックの QoS ルールでは、宛先ポートまたはソースポートが指定された場合、ネットワーク プロトコルを強制的に含める必要があります。

ブリッジ モード トラフィックの QoS ルールを作成する際に考慮すべきポイントを以下に示します。

- ポート指定をサポートしているプロトコルのポートのみを指定できます。ポート指定のないプロトコル (ICMP など) は、AP で無視されます。
- ファイアウォールのフィルタ ID が使用されている QoS ルールは無視されます。
- 照合値が「0」に設定されているルールはすべてワイルドカードと見なされ、すべてのトラフィックが一致します。
- ブリッジ モード トラフィックの QoS ルールは、捕捉アクションを含む他の条件項目をサポートしません。
- アプリケーション可視化が有効になっている場合にパケットがドロップされるのは、アプリケーション可視化プロファイルと QoS ルールの両方にドロップアクション / ルールがある場合のみです。

注:

- コントローラと AP 間のトラフィックをブロックするルールを作成すると、AP とコントローラの接続が切断されるため、そのようなルールは作成しないようにしてください。
- QoS ルール数が 50 を超えると、システム パフォーマンス全体に影響する場合があります。

[Match] チェックボックスと [Flow Class] チェックボックスについて

2つのチェックボックス、[Match] と [Flow Class] は、互いに独立して動作し、2つの異なる機能を実行します。[Match] はほぼ必ず使用しますが、これは、左側の設定が一致する必要があることを示すチェックボックスであるためです。これによって、QoS ルールの一致基準が設定されます。複数の一致基準をチェックできます。一致とは、QoS ルールの最初のフェーズの実行であり、これについては、[図 70](#) の緑のボックスを参照してください。

基準が一致すると、QoS ルールのアクション フェーズが実行されます。このフェーズは、[図 70](#) でオレンジのボックスで囲まれた部分です。ここでは、フェーズ 1 の Matching で一致したパケットをどのように処理するかを記述します。たとえば、ルールによって、指定したソースからのパケットを捕捉し、それをドロップできます。アクションとは、QoS のフェーズ 2 の実行のことです。

[Flow Class] 列は、レート制限に関する記述です。ルールにレート制限が含まれている場合、[Traffic Control] と [Token Bucket Rate] がオンになっている必要があります。QoS ルールがトラフィック制御を実行すると、[Flow Class] 列のチェックマークが参照されます。チェックマークが何もオンになっていないと、レート制限がすべてに適用されます。[Destination]、[Source]、または [Network Protocol] の [Flow Class] のチェックがオンになっていると、次のように処理されます。

- [Destination] の [Flow Class] - それぞれの宛先フローにレート制限が適用されます。
- [Source] の [Flow Class] - すべてのソース フローの合計がレート以下である必要があります。
- [Network] の [Protocol Flow Class] - このプロトコルを使用して転送されるすべてのデータにレート制限が適用されます。

図 70: QoS ルールの動作 -- 変更

QoS and Firewall Rules - Update

Summary Selection		Match	Flow Class
ID			On
1. MATCH CRITERIA			
Destination IP	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
Destination Port	1720 Valid range: [0-65535]	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Source IP	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
Source Port	0 Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	6 Valid range: [0-255]	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0 Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0 Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
2. Take Action			
QoS Protocol	H.323		
Average Packet Rate	0 Valid range: [0-200]		
Action	CAPTURE		
Drop Policy	Head		
Token Bucket Rate	0 Valid range: [0-1000000]		
Priority	0 Valid range: [0-8]		
Traffic Control	300		
DiffServ Codepoint	DiffServ Disabled		
Qos Rule Logging	Off		
Qos Rule Logging Frequency	60 Valid range: [30-60]		
3. Rate Limit			



QoS ルールの作成時に、1 つ以上の [Match Flow] フラグを選択する必要があります。選択しないと、先の処理に進めません。

CLI による QoS ルールの設定

QoS ルールを CLI で設定するには、QoS ルール設定モードに入る必要があります。configure terminal と入力し、qosrule <rule-id> コマンドで QoS ルールを指定します。これら 2 つのコマンドのオプションについては、次の表を参照してください。

コマンド	目的
configure terminal	グローバル設定モードに入ります。
qosrule rule-id netprotocol {6 17 <i>protocolnumber</i> } qosprotocol {H323 sip none other sccp}	指定したルール ID の QoS ルール設定に入ります。show qosrules を使用して、ルール ID のリストを取得します。必須パラメータは、以下のとおりです。 netprotocol: ネットワーク プロトコル。TCP であれば 6、UDP であれば 17 などの標準ネットワーク プロトコル番号になります。SVP プロトコル (Spectralink フォンで使用) であれば 119 などの、任意の有効なプロトコル番号になります (全リストは、 http://www.iana.org/assignments/protocol-numbers に記載されています)。 qosprotocol: QoS プロトコル。次のいずれかになります。 H.323 sip (SIP - Session Initiation Protocol) none (上記以外のすべてのプロトコル)
... commands ...	QoS ルール設定コマンドをここで入力します (下表参照)。
end	特権 EXEC モードに戻ります。
copy running-config startup-config	これは、エントリを設定ファイルに保存するためのオプションの手順です。

QoS ルール CLI 設定コマンド

QoS ルール設定モードに入ると (上記の手順を参照)、以下の QoS ルール設定コマンドを実行できます。

コマンド	目的
dstip ip	255.255.255.255 という形式の宛先 IP。
dstmask ipmask	255.255.255.255 という形式の宛先ネットマスク。
dstport port	0 ～ 65535 の宛先ポート番号。
srcip ip	255.255.255.255 という形式のソース IP。
srcmask ipmask	255.255.255.255 という形式のソース ネットマスク。
srcport port	0 ～ 65535 のソース ポート番号。
action {forward capture drop}	<p>ルールに一致するパケットに対して実行するアクション。次のいずれかになります。</p> <p>forward - フローは、QoS プロトコル検出を迂回し、QoS プロトコルが指定されているかどうかに関係なく、明示的なリソース要求に渡されます。</p> <p>capture - フローは、QoS プロトコル検出をパスし、指定された QoS プロトコルを使用します。H.323/SIP ベースの固定 QoS ルールには、このアクションをお奨めします。</p> <p>drop - フローはドロップされます。</p>
dscp class	DiffServ コードポイントのクラス。この設定により、フロー内のパケットに対するホップ転送ごとの動作を選択できます。RFC 2475 および 2597 に精通している方がこれらの値を変更することを推奨します。
priority rate	ベストエフォートの優先度キューを指定する数値 (0 ～ 8) で、0 (ベストエフォート) がデフォルト、8 が最高の優先度です。優先度をオン (ゼロ以外) にするか、平均パケット速度と TSpec トークン パケット速度を指定できますが、両方を設定することはできません。デフォルトは 0 です。
avgpacketrates rate	平均パケット速度 : 0 ～ 200 パケット / 秒。ゼロ以外の値を指定した場合は、TSpec トークン パケット速度にもゼロ以外の値を指定します。その場合、優先度にはゼロ以外の値を指定できません。デフォルトは 0 です。
tokenbucketrate rate	TSpec トークン パケット速度 : 0 ～ 1,000,000 バイト / 秒で、チェックボックスがオンかどうかで異なります。ゼロ以外の値を指定した場合は、平均パケット速度にもゼロ以外の値を指定します。その場合、優先度にはゼロ以外の値を指定できません。デフォルトは 0 です。

コマンド	目的
trafficcontrol-enable	トラフィック制御の規制をオンにします。トラフィック制御をオンにすると、優先度が割り当てられているトラフィックは割り当てられた速度で送受信され、それより速くなることはありません。
no trafficcontrol	トラフィック制御の規制をオフにします。これがデフォルト設定です。

CLI による QoS ルールの設定の例

以下のコマンドは、IP 電話に QoS ルール 10 を設定します (IP 電話のサーバの IP アドレスは 10.8.1.1)。

```
controller (config)# qosrule 10 netprotocol 17 qosprotocol none
controller (config-qosrule)# srcip 10.8.1.1
controller (config-qosrule)# srcmask 255.255.255.0
controller (config-qosrule)# srcport 0
controller (config-qosrule)# dstip 10.8.1.1
controller (config-qosrule)# dstmask 255.255.255.0
controller (config-qosrule)# dstport 0
controller (config-qosrule)# action forward
controller (config-qosrule)# tokenbucketrate 9400
controller (config-qosrule)# avgpaketrate 35
controller (config-qosrule)# end
```

SCCP 電話を使用する場合には、別の VLAN を SCCP 電話用に作成し、次の qosrule を G.711 (20ms) コーデック用に作成して qosflow トラフィックを処理することを推奨します。

```
controller (config)# qosrule 123 netprotocol 17 qosprotocol none
controller (config-qosrule)# srcmask subnet_mask (for example, 255.255.192.0)
controller (config-qosrule)# srcip subnet_IP_addr (for example, 172.27.128.0)
controller (config-qosrule)# action forward
controller (config-qosrule)# avgpaketrate 50
controller (config-qosrule)# tokenbucketrate 10000
controller (config-qosrule)# exit
controller (config)# qosrule 124 netprotocol 17 qosprotocol none
controller (config-qosrule)# dstip subnet_IP_addr (for example, 172.27.128.0)
controller (config-qosrule)# dstmask subnet_mask (for example, 255.255.192.0)
controller (config-qosrule)# action forward
controller (config-qosrule)# avgpaketrate 50
controller (config-qosrule)# tokenbucketrate 10000
controller (config-qosrule)# exit
```

以下の例では、UDP トランスポート経由で Windows Media Server 9 から CBR エンコードされたビデオを 1 Mbps でストリーミングする場合の QoS ルールを設定します。

この例の設定パラメータは以下のとおりです。

- Rule ID: 11
- Network protocol: 17 (UDP)
- QoS protocol: なし
- Source IP address: 0.0.0.0
- Source subnet mask: 0.0.0.0
- Source port: 0
- Destination IP address: 10.10.43.100 (これは、ビデオ ストリームを受け取るワイヤレス シーモンの IP アドレスです)
- Destination subnet mask: 255.255.255.255
- Destination port: 5004
- Action to take if packets match rule: Forward
- Drop policy: Head
- Token bucket rate: 128 kbytes/second
- Average packet rate: 10 packets/second

以下のコマンドで、UDP トランスポート経由の Windows Media Server 9 からの ビデオ ストリーミングに対する QoS ルールを設定します。

```
controller (config)# qosrule 11 netprotocol 17 qosprotocol none
controller (config-qosrule)# srcip 0.0.0.0
controller (config-qosrule)# srcmask 0.0.0.0
controller (config-qosrule)# srcport 0
controller (config-qosrule)# dstip 10.10.43.100
controller (config-qosrule)# dstmask 255.255.255.255
controller (config-qosrule)# dstport 0
controller (config-qosrule)# action forward
controller (config-qosrule)# tokenbucketrate 128000
controller (config-qosrule)# avgpaketrate 10
controller (config-qosrule)# end
```

VoIP の最適化

VoIP (Voice over IP) 接続の転送も、多くの点では他のどのネットワーク アプリケーションと変わりません。ある IP と別の IP との間でパケットが送受信されます。音声データが、一方でバイナリ データにエンコードされ、他方でデコードされます。ある意味、音声も 1 つのデータの形態にすぎません。ただし、音声特有の問題もいくつか存在します。

以下のように、高品質音声トラフィックに対する要件は多くのデータトラフィックに対する要件とまったく同じというわけではありません。

- データパケットが 1 秒遅れて届いたとしても、一般的には問題は発生しません。データは、遅れてくるパケットを受け取るまでバッファされます。音声パケットが 1 秒遅れて届いた場合には、それは使えないと判断され、使われなくなってしまうかもしれません。
- データパケットが 1/3 秒かかって宛先に届く場合、一般的には十分に速いと考えられます。音声パケットが定期的に 1/3 秒かかって届いている場合には、ユーザは相手の会話を遮らないようにするために文と文の間に長い休止を入れるようになるでしょう。

高品質の VoIP 電話では、コンスタントかつ迅速にデータを届ける必要があります。VoIP データの要件を満たすには、データ経路全体に渡って豊富な帯域幅が確保された接続、あるいは電話の長さに見合った QoS (Quality of Service) を確実に提供する手段が必要になります。

帯域幅が十分に確保されている場合であっても、通話のセットアップには困難な作業を伴う可能性があります。通話が開始されるとき、その通話の宛先は、公共スイッチネットワーク (PSTN) に接続されている標準的な電話機か、特定の IP 番号の IP デバイスカ、あるいは複数のコンピュータの中の 1 台 (自宅やオフィスのコンピュータなど) である場合もあるでしょう。宛先のデバイスが公共ネットワーク上の電話である場合、開始プロトコルは、インターネットと電話のネットワークの間のゲートウェイを特定する必要があります。宛先デバイスがローカルネットワークにある場合、開始プロトコルは、その通話に使用するコンピュータあるいはデバイスを特定する必要があります。

宛先のデバイスが特定されたら、開始側デバイスと宛先デバイスは、データのコード/デコード方法のネゴシエーションを行う必要があります。宛先デバイスを探して、通話の通信手段を確立するこのプロセスは、**セッション開始 (session initiation)** と呼ばれます。

セッション開始には、主に以下の 2 つの規格が使用されます。

- Session Initiation Protocol (SIP)。大部分の VoIP 通話に使用されています。
- H.323。Microsoft NetMeeting などのマルチメディア通信で使用されています。

どちらの場合も、開始側デバイスはサーバに問い合わせで宛先デバイスを見つけ出し、通信方法を確立します。

双方のデバイスがマッチングされて通信規格が選択されれば、通話が確立されます。サーバの設定に応じて、VoIP サーバは通信ループにそのまま残るか、ループから抜けます。

VoIP への QoS ルールの使用

ワイヤレス LAN システムは、音声通話に適したレベルの QoS で自動的に音声トラフィックを提供するように設計されています。受信トラフィックは、事前に定義済みの QoS ルールと照合され、その一致内容に応じて適切な優先度が割り当てられます。

受信トラフィックで監視されるポート番号は以下のとおりです。

- SIP サービス用の 5060 (UDP または TCP)
- H.323 サービス用の 1720 (TCP)
- Vocera 用の 5200 (UDP)

VoIP デバイスとサーバが異なるポートを使用するように設定されている場合は、システムが使用しているポートに合わせて、コントローラの QoS ルールを変更します。Web UI または CLI のいずれかで、QoS ルールを変更します。

標準外ポートのための QoS ルールの変更

コントローラは、SIP または H.323 コールの帯域幅要求を検知し、かつ帯域幅を予約するようあらかじめ設定されています。Web UI または CLI のいずれかで、QoS ルールを変更します。出荷時に、以下のデフォルトの QoS ルールが設定されています。

```
default(15)# show qosrule
```

ID	Dst IP Prot Firewall	Dst Mask Filter Qos	DPort Action	Src IP	Src Mask	SPort
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0
6		h323	capture			
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720
6		h323	capture			
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
17		sip	capture			
5	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
6		sip	capture			
7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0
17		other	forward			
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200
17		other	forward			
9	0.0.0.0	0.0.0.0	80	0.0.0.0	0.0.0.0	0
17		other	capture			
10	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5060
6		other	capture			

QoS and Firewall Rules(8 entries)

最初の 2 つの事前に設定されている QoS ルールは、TCP ポート 1720 との間で送信される H.323 トラフィックにプライオリティを指定します。次の 2 つの QoS ルールは、UDP/TCP ポート 5060 との間で送信される SIP トラフィックに優先度を指定します。ルール 7 と 8 は Vocera バッジ用で、UDP のポート 5200 を使用します。

たとえば次のような特別な要件がない限り、一般的に、コントローラに QoS ルールを設定する必要はありません。たとえば、次のように入力します。

- 特定のポートあるいは IP アドレスからの着信パケットをドロップしたい。
- H.323 および SIP トラフィック以外のトラフィックに優先度を与えるよう、コントローラを設定したい。

ルールを設定して、優先度に基づいた QoS を実現したり、QoS を予約したりできます。QoS には、予約されたトラフィックが適用され、総帯域幅の最初の部分が割り当てられ、次に固定の優先度レベル、最後にベストエフォート (デフォルト) のトラフィック クラスが続きます。トラフィック仕様 (IETF IntServ RFC では TSpec とも呼ばれます) として平均パケットレート パラメータとトークン バケット レート パラメータを併用することで、新規アプリケーション用に予約する QoS を設定できます。

グローバル QoS 設定

グローバル QoS パラメータによって、グローバル レベルでの通話の品質を決定する設定を指定できます。これらの設定により、CAC (Call Admission Control)、クライアントの負荷分散機能、帯域幅のスケール設定、および TTL (Time To Live) の設定などの微調整が可能です。

以下のグローバル QoS パラメータの設定が可能です。

表 28: グローバル QoS パラメータ

コマンド	目的
<code>qosvars admission { admitall pending reject }</code>	アドミSSION制御。有効な値は、admitall、pending、reject です。
<code>qosvars ttl ttl-value</code>	TCP および UDP のほか、他のすべてのプロトコルに対するデフォルトの有効期間 (秒) です。
<code>qosvars tcpttl ttl-value</code>	TCP プロトコルの有効期間 (秒) です。
<code>qosvars udpttl ttl-value</code>	UDP プロトコルの有効期間 (秒) です。
<code>qosvars bwscaling value</code>	Tspec 帯域幅のスケール要素 (パーセント) です。範囲は 1 ~ 100% で、一般的には 100% です。
<code>qosvars cac-deauth {on off}</code>	オプションの 802.11 認証解除動作を設定します。
<code>qosvars calls-per-ap max</code>	AP あたりの最大コール数を設定します。
<code>qosvars calls-per-bssid max</code>	BSSID あたりの最大コール数を設定します。

表 28: グローバル QoS パラメータ

コマンド	目的
qosvars drop-policy {head tail}	ドロップ ポリシーを設定します。有効な値はそれぞれ head または tail です。
qosvars load-balance overflow {on off}	BSSID 間の負荷分散を有効または無効にします。
qosvars max-stations-per-radio max	1 つの無線と連携できる最大ステーション数を設定します (0 ~ 128)。デフォルトは 128 です。仮想ポートを使用したり、クライアントとして電話を使用したりする予定がある場合は、AP400 無線 (またはインターフェイス リージョンあたり) で約 50 のクライアントを推奨します。データのためのインストール環境で、無線あたり最大 128 のクライアントを予定している場合、AP400 では 256 ということになります。AP1000 は、無線あたり最大 20 のデータ クライアントをサポートします。
qosvars max-stations-per-bssid max	1 つの BSSID と連携できる最大ステーション数を指定します (0 ~ 1023)。
qosvars no enable	QoS をオフにします。
SIP Idle Timeout	SIP 接続がタイムアウトになるまでの時間を設定します。
Station Assignment Aging Time (s)	ステーションのエージングが開始するまでの時間を設定します。
Maximum Calls Per Interference Region	任意の干渉エリアで許可されるコール数を指定します。

レート制限 QoS ルール

レート制限は、ネットワーク インターフェイスでの送受信の全体的なトラフィック スループットを制御します。ネットワークやデバイスに対して特定の帯域幅制限を設定でき、実際のトラフィックがそのポリシーに違反すると、何らかの方法でトラフィックがシェーピングされます。この実装では、一定のキューイング (パケット送信の遅延) を適用することで、トラフィックがポリシーに適合するようになるまで、パケットがドロップします。

CLI によるレート制限

トラフィック制御をオンにし、トークン バケット レートをトークン バケットの制限として使用することで、トラフィックにレート制限を設定できます。以下の手順に従って、クライア

ント 10.11.31.115 に約 3Mbps のレート制限を設定し、この機能を確認するための簡単なテストを実行します。

1. トークン バケット レートから、設定すべきレート制限を決定します。以下の例では、レート制限を 3Mbps (3Mbps = 3000000bps、3000000/8=46875) に設定します。
2. クライアントにレート制限を設定する qosrule を作成します。

```
Controller1# sh qosrule 23
QoS and Firewall Rules
```

```
ID : 23
Id Class flow class : on
Destination IP : 10.11.31.115 (this is the client to be rate limited)
Destination IP match : on
Destination IP flow class : on
Destination Netmask : 255.255.255.255
Destination Port : 0
Destination Port match : none
Destination Port flow class : none
Source IP : 0.0.0.0
Source IP match : none
Source IP flow class : none
Source Netmask : 0.0.0.0
Source Port : 0
Source Port match : none
Source Port flow class : none
Network Protocol : 6
Network Protocol match : on
Network Protocol flow class : on
Firewall Filter ID :
Filter Id match : none
Filter Id Flow Class : none
Packet minimum length : 0
Packet Length match : none
Packet Length flow class : none
Packet maximum length : 0
QoS Protocol : other
Average Packet Rate : 0
Action : forward
Drop Policy : head
Token Bucket Rate : 46875
Priority : 0
Traffic Control : on
DiffServ Codepoint : disabled
Qos Rule Logging : on
Qos Rule Logging Frequency : 31
```

GUI によるレート制限 QoS ルール

トラフィック制御をオンにし、トークン バケット レートをトークン バケットの制限として使用することで、1 人のユーザのトラフィックにレート制限を設定できます。以下の手順に従って、トラフィックにレート制限を設定します。

1. [Configure] > [QoS Settings] > [QoS and Firewall rules] タブ > [Add] をクリックします。
[QoS and Firewall rules Add] ウィンドウが表示されます。
2. 下スクロールして、[QoS and Firewall rules Add] ウィンドウの下半分に移動します。
3. [Traffic Control] を [On] に設定します。
4. トークン バケット レートから、設定すべきレート制限を設定します。これは、配備環境のニーズによって、Kbps (0 ~ 1000) または Mbps (0 ~ 64) のいずれかで入力します。
5. [OK] をクリックします。

これで、レート制限が設定されました。

レート制限の例

TCP の同じサブネットのクライアントにレート制限を設定

サブネット 10.11.31.0 のクライアントにレート制限を設定するには、以下の手順を実行します。

1. トークン バケット レートから、設定すべきレート制限を決定します。以下の例では、レート制限を 3Mbps (3Mbps = 3000000bps、3000000/8/8=46875) に設定します。
2. 特定のサブネットからのクライアントをレート制限するために、以下の qosrule を作成します。

```
Controller1# sh qosrule 23
QoS and Firewall Rules
ID: 23
ID Class flow class : on
Destination : 10.11.31.0 (this is the subnet to be rate limited)
Destination IP match : on
Destination IP flow class : on
Destination Netmask : 255.255.255.0
Destination Port : 0
Destination Port match : none
Destination Port flow class : none
Source IP : 0.0.0.0
Source Netmask : 0.0.0.0
Source Port : 0
Source Port match : none
Source Port flow class : none
Network Protocol : 6
```

```
Network Protocol match : on
Network Protocol flow class : on
Firewall Filter ID :
Filter Id match : none
Filter Id Flow Class : none
Packet minimum length : 0
Packet Length match : none
Packet Length flow class : none
Packet maximum length : 0
QoS Protocol : other
Average Packet Rate : 0
Action : forward
Drop Policy : head
Token Bucket Rate : 46875
Priority : 0
Traffic Control : on
DiffServ Codepoint : disabled
QoS Rule Logging : on
QoS Rule Logging Frequency : 60
```

3. throughput スクリプトを使用して、クライアント 10.11.31.115 に Chariot が送信する TCP ダウンストリームを設定します。Chariot でのスループットが平均で約 3Mbps になります。

この QoS ルールの結果として、10.11.31.xxx ネットワークの各クライアントが、同じサブネットの個々のソースから約 3 mbps を取得するようになります。

TCP の異なるサブネットのクライアントにレート制限を設定

クライアントが使用中のサブネット以外にクライアントのレート制限を設定するには、次の手順を実行します。

1. トークン バケット レートから、設定すべきレート制限を決定します。以下の例では、レート制限を 3Mbps (3Mbps = 3000000bps、3000000/8/8=46875) に設定します。
2. 特定のサブネットからのクライアントをレート制限するために、以下の qosrule を作成します。

```
Controller1# sh qosrule 23
QoS and Firewall Rules
ID : 23
Id Class flow class : on
Destination IP : 10.11.31.0 (this is the subnet to be rate limited)
Destination IP match : on
Destination IP flow class : none
Destination Netmask : 255.255.255.0
Destination Port : 0
Destination Port match : none
Destination Port flow class : none
```

Source IP : 0.0.0.0
Source Netmask : 0.0.0.0
Source Port : 0
Source Port match : none
Source Port flow class : none
Network Protocol : 6
Network Protocol match : on
Network Protocol flow class : on
Firewall Filter ID :
Filter Id match : none
Filter Id Flow Class : none
Packet minimum length : 0
Packet Length match : none
Packet Length flow class : none
Packet maximum length : 0
QoS Protocol : other
Average Packet Rate : 0
Action : forward
Drop Policy : head
Token Bucket Rate : 46875
Priority : 0
Traffic Control : on
DiffServ Codepoint : disabled
Qos Rule Logging : on
Qos Rule Logging Frequency : 60

- throughput スクリプトを使用して、10.11.31.xxx の異なるクライアントに Chariot が送信する TCP ダウンストリームを設定します。

10.11.31.xxx ネットワークのすべてのクライアントが、個々のソースから 3 Mbps を共有するようになります。

コーデック ルールの設定

この項では、設定が可能で、コマンドで指定できるコーデック ルールについて説明します。



使用する SIP 電話が "ptime" をサポートしていれば、コーデック ルールを設定する必要はまったくありません。サポートしていない場合には、QoS ルールを設定し、電話が使用するパケット化 / サンプル速度に基づいてそのルールが設定されていることを確認してください。

SIP の ptime 属性は、SIP 仕様のオプション部分です。この属性により、SIP メディア デバイスに対して RTP メディア ストリームのパケット化速度をミリ秒単位で通知できます。たとえば、ptime の値が「20」に設定されていると、SIP デバイスは 20 ミリ秒ごとに他者に 1 RTP パケットを送信します。この仕様に従って、ワイヤレス LAN システムは、コーデックとパケット化の速度に基づき、正確に QoS 帯域幅を確保できます。

SDP メディア属性の一部として含まれている "ptime" 属性の例を以下に示します。

```
m=audio 62986 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=ptime:20
```

SDP デバイスと SIP デバイスの間でのメディアのネゴシエーションにおいて ptime 属性が存在しないと、ワイヤレス LAN システムは、qoscodec コマンドで指定されている codec type のデフォルト値を使用します。



正規のパケット化速度は、実際のメディア トラフィックと一致するように設定する必要があり、そのように設定されていないと、QoS の確保が正確ではなくなります。カスタマ サポートの FTP サイトに掲載されているスプレッドシート、qoscodec_parameters.xls を使用すると、関連するパラメータの適切な値の判断が容易になります。詳細とアクセス方法については、カスタマ サポートまでお問い合わせください。

QoS コーデック ルールを設定するには、QoS コーデック設定モードに入る必要があります。以下の手順に従ってください。

コマンド	目的
configure terminal	グローバル設定モードに入ります。
qoscodec rule-id codec <codec-type> qosprotocol {H323v1 sip} tokenbucketrate tbr maxdatagramsize maxdg minpolicedunit minpol samplerate sr	<p>指定したルール ID の QoS コーデック設定に入ります。</p> <p>show qoscodec を使用して、ルール ID のリストを取得します。必須パラメータは以下のとおりです。</p> <p>codec : codec というキーワードの後に、コーデック タイプを入力します。指定できるコーデック タイプは以下のとおりです。</p> <p>qosprotocol.QoS プロトコル。次のいずれかになります。 H323 (H.323); sip (SIP - Session Initiation Protocol)</p> <p>tokenbucketrate : トークン バケット速度 : 0 ~ 1,000,000 バイト / 秒で、チェックボックスがオンかどうかで異なります。</p> <p>maxdatagramsize : 最大データグラム サイズ。0 ~ 1,500 バイトです。</p> <p>minpolicedunit : 最小規制単位。0 ~ 1,500 バイトです。</p> <p>samplerate. サンプル速度。0 ~ 200 パケット / 秒。</p>
... commands ...	QoS コーデック設定コマンドをここに入力します。

コマンド	目的
end	特権 EXEC モードに戻ります。
copy running-config startup-config	これは、エントリを設定ファイルに保存するためのオプションの手順です。

コーデック タイプは以下のいずれかです。

表 29: QoS コーデック タイプ

タイプ	説明
1016	1016 音声 : ペイロード タイプ 1、ビット レート 16 Kbps
default	未知のコーデック、またはコーデック変換テーブルにエントリがないコーデックのためのデフォルト TSpec/RSPEC が含まれています
dv14	DV14 音声 : ペイロード タイプ 5、ビット レート 32 Kbps
dv14.2	DV14.2 音声 : ペイロード タイプ 6、ビット レート 64 kbps
g711a	G711 音声 : ペイロード タイプ 8、G.711、A-law 、ビット レート 64 Kbps
g711u	G711 音声 : ペイロード タイプ 0、G.711、U-law 、ビット レート 64 Kbps
g721	G721 音声 : ペイロード タイプ 2、ビット レート 32 Kbps
g722	音声 : ペイロード タイプ 9、ビット レート 64 Kbps、7 KHz
g7221	G7221 音声 : ペイロード タイプ *、ビット レート 24 Kbps、16 KHz
g7221-32	G7221 音声 : ペイロード タイプ *、ビット レート 32 Kbps、16 KHz
g723.1	G7231 音声 : ペイロード タイプ 4、G.723.1、ビット レート 6.3 Kbps
g728	G728 音声 : ペイロード タイプ 15、ビット レート 16 Kbps
g729	G729 音声 : ペイロード タイプ 16、ビット レート 8 Kbps
g7red	MSN 独自のコーデック音声 : ペイロード タイプ *
gsm	GSM 音声 : ペイロード タイプ 3、ビット レート 13 kbps
h261	H.261 ビデオ

表 29: QoS コーデック タイプ

タイプ	説明
h263	H.263 ビデオ
lpc	IPC 音声 : ペイロード タイプ 7、ビット レート 2.4 Kbps
mpa	MPA 音声 : ペイロード タイプ 14、ビット レート 32 Kbps
siren	MSN 独自の音声 : ペイロード タイプ *、ビット レート 16 Kbps、16 KHz

以下のコマンドは、QoS CODEC 設定モードで使します。

表 30: QoS CODEC 設定モードのコマンド

コマンド	目的
tokenbucketsize size	トークン バケットのサイズ (バイト数)。0 ~ 16,000 バイト。デフォルトは 8。
peakrate rate	トラフィックのスペック ピーク レート。0 ~ 1,000,000 バイト / 秒。デフォルトは 0。
rspecrate rate	予約スペック速度。0 ~ 1,000,000 バイト / 秒。デフォルトは 0。
rspecslack slack	予約スペック スラック。0 ~ 1,000,000 ミリ秒。デフォルトは 0。

QoS 統計表示コマンド

電話 / コールのステータスの表示

SIP サーバに登録されているアクティブな SIP フォンを表示するには、show phones コマンドを使します。

```

Controller(15)# show phones
      MAC          IP          AP ID AP Name          Type Username
      Server      Transport
00:01:3e:12:24:b5  172.18.122.21   3    QoS-Lab          sip  100
172.18.122.122    udp
      Phone Table(1 entry)

```



```

Controller(15)#
  To display the active SIP phone calls, use the show phone-calls command.
controller# sh phone-calls
  From MAC           From IP           From AP From AP Name   From Username
  From Flow Pending  To MAC           To IP           To AP   To AP Name
  To Username        To Flow   Pending   Type State
00:0f:86:12:1d:7c  10.0.220.119      1             AP-1           5381
100      off      00:00:00:00:00:00  10.0.220.241    0
69        101      off      sip  connected

      Phone Call Table(1 entry)
controller#

```

コール アドミッション詳細の表示

AP が現在サポートしているコールを表示するには、show statistics call-admission-control ap コマンドを使用します。

```

controller# show statistics call-admission-control ap
  AP ID Current Calls Cumulative Rejected Calls
  6      0              0
Call Admission Control AP Statistics(1 entry)

```

特定の BSSID に関連するコールを表示するには、show statistics call-admission control bss コマンドを使用します。

```

controller# show statistics call-admission-control bss
  BSSID              Current Calls Cumulative Rejected Calls
00:0c:e6:13:00:da 0
00:0c:e6:52:b3:4b 0
00:0c:e6:f7:42:60 0

Call Admission Control BSS Statistics(3 entries)

```

QoS ルールのその他の例

本章のこれまでの例 (398 ページの「[CLI による QoS ルールの設定の例](#)」および 405 ページの「[レート制限の例](#)」) 以外のものを以下に記載します。

- [特定のクライアントのレート制限の設定 \(412 ページ\)](#)
- [ワイヤレス ピアツーピア QoS ルール \(413 ページ\)](#)

特定のクライアントのレート制限の設定

任意のソースのクライアント 10.11.31.115 にレート制限を設定するには、以下の手順を実行します。

1. トークン バケット レートから、設定すべきレート制限を決定します。以下の例では、レート制限を 3Mbps (3Mbps = 3000000bps、3000000/8/8=46875) に設定します。
2. いずれかのソースからの特定のクライアントをレート制限するために、以下の qosrule を作成します。

```
Controller1# sh qosrule 23
QoS and Firewall Rules
ID : 23
ID Class flow class : on
Destination IP : 10.11.31.115 (this is the client to be rate limited)
Destination IP match : on
Destination IP flow class : on
Destination Netmask : 255.255.255.255
Destination Port : 0
Destination Port match : none
Destination Port flow class : none
Source IP : 0.0.0.0
Source Netmask : 0.0.0.0
Source Port : 0
Source Port match : none
Source Port flow class : none
Network Protocol : 6
Network Protocol match : on
Network Protocol flow class : on
Firewall Filter ID :
Filter Id match : none
Filter Id Flow Class : none
Packet minimum length : 0
Packet Length match : none
Packet Length flow class : none
Packet maximum length : 0
QoS Protocol : other
Average Packet Rate : 0
Action : forward
Drop Policy : head
Token Bucket Rate : 46875
Priority : 0
Traffic Control : on
DiffServ Codepoint : disabled
Qos Rule Logging : on
Qos Rule Logging Frequency : 60
```

- throughput スクリプトを使用して、クライアント (10.11.31.115) に Chariot が送信する TCP ダウンストリームを設定します。

Chariot でのスループットが平均で約 3 Mbps になります。この QoS ルールの結果として、クライアント 10.11.31.115 がトラフィックを受け取る場合に、約 3mbps のレート制限が適用されます。

ワイヤレス ピアツーピア QoS ルール

一般的に、2 つの IP アドレス間の特定のプロトコルに優先度 QoS ルールを作成するには、ネットワーク プロトコルを指定し、そのプロトコルに一致するフローを選択します。こうすることで、IP 間の特定のプロトコルに QoS 優先度が作成されます。

ピアツーピアの優先度の設定

この IP ベースの QoS ルールは、ソースが 172.18.85.11 で宛先が 172.18.85.12 のピアツーピア トラフィックに優先度を設定します。

```
Testing# show qosrule 11
QoS and Firewall Rules
ID : 11
Id Class flow class : on
Destination IP : 172.18.85.12
Destination IP match : on
Destination IP flow class : none
Destination Netmask : 255.255.255.255
Destination Port : 0
Destination Port match : none
Destination Port flow class : none
Source IP : 172.18.85.11
Source Netmask : 255.255.255.255
Source IP match : on
Source IP flow class : none
Source Port : 0
Source Port match : none
Source Port flow class : none
Network Protocol : 0
Network Protocol match : none
Network Protocol flow class : none
Firewall Filter ID :
Filter Id match : none
Filter Id Flow Class : none
Packet minimum length : 0
Packet Length match : none
Packet Length flow class : none
Packet maximum length : 0
QoS Protocol : none
```

```

Average Packet Rate : 100
Action : forward
Drop Policy : head
Token Bucket Rate : 1000000
Priority : 0
Traffic Control : off
DiffServ Codepoint : disabled
Qos Rule Logging : on
Qos Rule Logging Frequency : 31

```

ピアツーピアのブロック

このピアツーピアのブロックの例では、ルール 60 と 61 を、DNS サーバが実際にそのネットワークにあるゲスト インターネット アクセスの分離された WLAN に適用されます。ルール 60 と 61 は、ワイヤレス クライアントがクライアントと同じサブネットにある場合のみ必要になります。

ID	Dst IP	Dst Mask	DPort	Src IP	Src Mask	SPort
Prot	Firewall	Filter	Qos	Action	Drop	
60	0.0.0.0	0.0.0.0	53	0.0.0.0	0.0.0.0	0
0		none	forward	tail		
61	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	53
0		none	forward	tail		
100	192.168.2.0	255.255.255.0	0	192.168.2.0	255.255.255.0	0
0		none	drop	tail		

```

qosrule 60 netprotocol 0 qosprotocol none
firewall-filter-id ""
id-flow on
dstip 0.0.0.0
dstmask 0.0.0.0
dstport 53
dstport-match on
dstport-flow on
srcip 0.0.0.0
srcmask 0.0.0.0
srcport 0
action forward
droppolicy tail
priority 0
avgpacketrates 0
tokenbucketrate 0
dscp disabled
qosrulelogging off
qosrule-logging-frequency 60
packet-min-length 0
packet-max-length 0
no trafficcontrol

```

```

exit
qosrule 61 netprotocol 0 qosprotocol none
firewall-filter-id ""
id-flow on
dstip 0.0.0.0
dstmask 0.0.0.0
dstport 0
srcip 0.0.0.0
srcmask 0.0.0.0
srcport 53
srcport-match on
srcport-flow on
action forward
droppolicy tail
priority 0
avgpacketrates 0
tokenbucketrate 0
dscp disabled
qosrulelogging off
qosrule-logging-frequency 60
packet-min-length 0
packet-max-length 0
no trafficcontrol
exit
qosrule 100 netprotocol 0 qosprotocol none
firewall-filter-id ""
id-flow on
dstip 192.168.2.0
dstip-match on
dstip-flow on
dstmask 255.255.255.0
dstport 0
srcip 192.168.2.0
srcip-match on
srcip-flow on
srcmask 255.255.255.0
srcport 0
action drop
droppolicy tail
priority 0
avgpacketrates 0
tokenbucketrate 0
dscp disabled
qosrulelogging off
qosrule-logging-frequency 60
packet-min-length 0
packet-max-length 0
no trafficcontrol

```

802.11n ビデオ サービス モジュール (ViSM)

ビデオ ストリーミングには、遅延と損失が少なく、データのスループットが高いという要件が求められます。フォーティネット Video Service Module™ (ViSM) は、オプションでライセンスが付与されるソフトウェア モジュールであり、遅延、レイテンシ、ジッタを最小限に抑えることで、802.11 に予測可能なビデオ パフォーマンスを提供します。混在トラフィックにおいても持続可能な優れたデータ速度に対応し、ビデオや音声の送受信の同期が可能です。

ViSM には、アプリケーション対応のスケジューリング、ビデオの同期化、クライアントのマルチキャスト グループ管理などのユニキャストおよびマルチキャストのビデオを最適化するメカニズムも追加されています。次のような機能を備えています。

- 安定性の高い優れたスループットにより、予測可能なパフォーマンスと安定したユーザ体験を提供します。
- アプリケーション対応の優先順位設定によって、ビデオ ストリームのビデオのコンポーネントを同期化し、アプリケーションの重要度に基づき、各フレームを配信します。
- マルチキャスト グループ管理では、クライアントがマルチキャスト グループのメンバーである仮想ポートのみへの配信を最適化します。
- ビデオ向けに最適化されたシームレスなハンドオフによって、マルチキャスト配信ツリーを再ルーティングすることで、アクセス ポイント間の送信時のビデオ フレームの損失を回避し、損失なしのモバイル ビデオを保証します。
- ユーザとロールに基づくポリシー強制によって、アプリケーション動作のきめ細かい制御を可能にします。
- 仮想化によって、どのクライアントがどのアプリケーションを実行しているのかが明確になります。

ViSM の実装

仮想ポートはすでに、マルチキャストからユニキャストの転送へと変更されています (U-APSD 以外のクライアント用)。ViSM によって、クライアントごとの IGMP スヌーピングが転送に追加されます。そのため、ViSM を実装するには、IGMP スヌーピングをオンにします。IGMP スヌーピングを制御する CLI コマンドについては、『*FortiWLC (SD) コマンド リファレンス*』を参照してください。現段階で、ViSM ライセンスは強制されません。ViSM は、AP1000 のアクセス ポイントには推奨されていません。

CLI による CAC (Call Admission Control) と負荷分散機能の設定

通話とトラフィックのグローバルな QoS を形成するためには、CAC (Call Admission Control) とクライアントの負荷分散機能を AP あるいは BSSID ごとに設定できます。

CAC コマンドを使用すると、AP あるいは BSSID ごとに存在できる新しい SIP 接続 (通話) の数のしきい値レベルを設定し、利用可能な帯域幅のグローバルな量を確定できます。結果

として、新しい通話が一時的に拒否される場合であっても、既存の通話は安定したレベルのサービスを確保できます。CAC が有効になっていると、AP あるいは BSSID に対して通話レベルのしきい値に近づいた場合に発生させる動作を管理者が設定できます。設定する動作としては、たとえば、486_BusyHere という応答、ipPathfinder への変更した INVITE メッセージ、あるいは 802.11 De-authentication メッセージをシステムが通話元を送るといった動作を設定できます。既存の通話が十分な帯域幅をもたない別の AP に移ると、その通話は、必要なリソースが利用できるようになるまでの間、保留 / ベストエフォートとして分類されます。



ESSID に対して固有の CAC 値を設定できます。ESSID レベルでの CAC の設定は、この項に記載されているグローバル設定よりも優先されます。ESSID に対する CAC の設定については、**151 ページ**の「[CLI による ESSID AP の CAC の設定](#)」を参照してください。

クライアントの負荷分散機能を有効にすると、AP または BSSID に対するクライアントの連携のラウンドロビンの負荷分散機能が実装されます。ステーションの最大数が関連付けられると、新しいステーションはラウンドロビン方式に参加できるようになります。

以下のコマンドでは、CAC を有効にし、AP ごとの通話数の上限を 12 に設定します。

```
controller (config)# qosvars cac-deauth on
controller (config)# qosvars calls-per-ap 12
```

以下のコマンドでは、クライアントの負荷分散機能のオーバーフロー保護を有効にし、AP ごとの通話数の上限を 15 に設定します。

```
controller (config)# qosvars load-balance-overflow on
controller (config)# qosvars max-stations-per-radio 15
```

以下のコマンドでは、BSSID ごとの通話数の上限を 14、BSSID ごとの最大ステーション数を 30 に設定します。

```
controller (config)# qosvars calls-per-bssid 14
controller (config)# qosvars max-stations-per-bssid 30
```

アプリケーション可視化 (DPI)

お使いのネットワークで、特定のアプリケーション トラフィックの監視やブロックを行えます。FortiWLC (SD) では、アプリケーション / サービスへのアクセスを監視および制限できま

す。アプリケーション / サービスのリストは、[Configuration] > [Access Control] > [Application] で確認できます。



- 11ac アクセス ポイントでのみサポートされます。
- カスタム アプリケーションで定義されているプロパティは、ブロックおよび監視用に設定されているシステム定義のアプリケーションよりも優先されます。

制限事項と推奨事項

- DPI ステータスを FortiWLM サーバにエクスポートするには、エクスポート先のポートとして 4739 を設定する必要があります。
- コントローラにおける ESS プロファイルの総数と AP の総数が上限に達すると、ポリシーは作成できません。各ポリシーを設定する場合は以下のようになります。
 - 適用可能な ESS の総数は 64 です。**ヒント:** この最大数をサポートするには、ESS 名が 15 文字以下になるようにします。
 - 適用可能な AP の総数は 186 です。この最大数をサポートするには、AP ID が 1 ~ 500 AP ID の範囲に収まるようにする必要があります。**ヒント:** AP のカバレッジを最大にするために、個々の AP を指定するのではなく、AP グループを作成して使用できます。
- BitTorrent ダウンロードは、監視は可能ですが、ブロックはできません。
- カスタム アプリでは、BitTorrent トラフィックの監視もブロックもできません。
- サブプロトコル トラフィックの高度な検出は、大量のリソースを使用するタスクであるため、適度な利用を推奨します。
- カスタム アプリケーション ([Application] で [Settings] > [Custom Applications] タブを選択) は削除しないことを推奨します。カスタム アプリケーションを削除すると、ダッシュボードのトップ 10 アプリケーションに不正確なステータスが表示される可能性があります。
- カスタム アプリケーションは、ポリシーにマッピングされていない場合でもデフォルトで監視されます。ブロックしない場合は、ポリシーに追加する必要があります。
- アプリケーションの監視またはブロックを設定するには、DPI を有効にし、適切なポリシーを作成する必要があります。

アプリケーション監視を設定して使用するには、以下のように操作します。

1. アプリケーション可視化を有効にします。
2. ポリシーを作成します。
3. システム定義アプリケーションやカスタム アプリケーションをポリシーに関連付けます。

アプリケーション可視化の有効化

DPI を有効にするには、**[Configuration] > [Applications] > [Settings]** タブに移動します。

Applications ?

Dashboard Settings Policies

Global Settings System Defined Applications Custom Applications

Enable Application Classification ON ▼

Export Interval 90 Seconds

Enable Netflow Export ☐

Export Destination 0.0.0.0

Destination Port 4739

DPI Version 16.04.08

1. [Enable Application Classification] で **[ON]** を選択します。これはグローバル設定であり、すべての AP で DPI を有効にします。
2. [Export Interval] は設定不可フィールドであり、90 秒に設定されます。
3. [Export Destination] : 適切な Network Manager サーバの IP アドレスを指定または変更 (*Network Manager* によって自動的にプッシュされる場合) します。これは、Network Manager サーバに状態をエクスポートするために使用されます。
4. Fortinet Network Manager に値をエクスポートするには、**[Enable Netflow Export]** を選択し、Fortinet Network Manager サーバの IP (エクスポート先) を指定します。

ポリシーの作成

1 つまたは複数のアプリケーション トラフィックを監視およびブロックするためのポリシーを作成できます。これは、以下のいずれかに対して実行できます。

- すべての ESS プロファイル
- ESS プロファイルごと
- すべての AP
- AP ごと
- AP グループごと

- ESS と AP の組み合わせ

例

以下のスクリーン ショットは、**AP-3** 経由で **sdpi-832-t** ESS プロファイルに接続するクライアントで **Yelp** トラフィックをブロックするポリシーを作成する手順を示しています。

The screenshot shows two overlapping windows from a network management interface.

Add Policy Window:

- Name:** Yelp (with a note: Enter 1-32 chars. ,Required)
- Policy:** Enable (dropdown)
- Description:** To monitor YELP traffic (with a note: Enter 1-256 chars)
- Advanced Detection:** Disable (dropdown)
- Select ESS. Or select AP/AP Group. Or select ESS and AP/AP Group.™**
 - ESSID Table:**

ESSID
<input type="checkbox"/> appsla
<input checked="" type="checkbox"/> sdpi-832-t
<input type="checkbox"/> sdpi-832-b
<input type="checkbox"/> sdpi-122-t
<input type="checkbox"/> sdpi-122-b
 - AP Group or AP Table:**

AP Group or AP
<input type="checkbox"/> allaps
<input type="checkbox"/> AP-1
<input checked="" type="checkbox"/> AP-3
<input type="checkbox"/> AP-4
<input type="checkbox"/> AP-5
- Select applications to detect and collect statistics. Select applications to block**

Application Name	Action
All Application	<input checked="" type="checkbox"/> Detect <input type="checkbox"/> Block

Add Application Dialog:

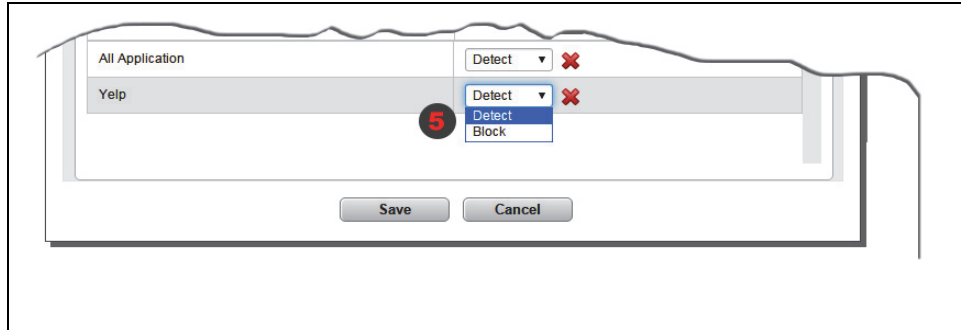
- Application Name Table:**

Application Name	Application Category
<input checked="" type="checkbox"/> Yelp	Social Networking
<input type="checkbox"/> Amazon_shop	Business
<input type="checkbox"/> Youporn	Streaming
<input checked="" type="checkbox"/> Ebay	Business
<input type="checkbox"/> Pornhub	Streaming

Red circles and arrows indicate the steps: 1. Select 'sdpi-832-t' in the ESSID table. 2. Select 'AP-3' in the AP Group or AP table. 3. Click the 'Add...' button in the 'All Application' row. 4. Select 'Yelp' in the 'Add Application' dialog.

1. ESSID テーブルから ESS プロファイルを選択します。
2. AP グループまたは AP テーブルから AP を選択します。
3. [ADD] ボタンをクリックしてアプリケーション リストを表示します。
4. リストからアプリケーションを選択し、[ADD] ボタンをクリックします。

5. ドロップダウン リストから **[Block]** を選択し、**[Save]** ボタンをクリックします。



ポリシーのリスト

デフォルトでは [Policies] タブに以下の内容が表示されます。

Applications <small>Help</small>							
<div>Dashboard Settings Policies</div>							
<input type="checkbox"/>	Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Owner
Search : ▶	<input type="text"/>	ALL ▼	ALL ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	A2	Enable	Enable	All Application, Facebook, Twitter, BBC, M_Controller	sdpi-832-b, sdpi-822v2-b	APs: AP-1, AP-19, AP-30	controller
<input type="checkbox"/>	Yelp	Enable	Disable	All Application, Facebook, Myspace, Twitter, Youtube, Ebay, BBC, Yelp	sdpi-832-t, sdpi-822v2-t	APs: AP-3, AP-19, AP-30, AP-39	controller
<input type="checkbox"/>	B3	Enable	Disable	All Application, Facebook, Ebay	sdpi-822v2-t, sdpi-822v2-b	APs:	controller

- **[Policy Name]** : ポリシーを特定する名前。
- **[Policy]** : ポリシーのステータス。
- **[Advanced Detection]** : システム定義アプリケーションのサブプロトコル、およびプロトコルを表示するには、[Enable] を選択します。
- **[Application ID List]** : ポリシーでブロックまたは監視されているシステム定義アプリケーションやカスタム アプリケーションのリスト。ブロックされているアプリケーションは赤色で表示され、監視のみされているアプリケーションは緑色で表示されます。
- **[ESSID List]** : このポリシーに設定されている ESS プロファイルの名前。クライアントは、この ESSID プロファイルを使用して接続し、監視対象のアプリケーションにアクセスしています。
- **[AP Groups or APs]** : このポリシーに設定されている AP のリスト。クライアントは、これらの AP または AP グループを経由して接続し、監視対象のアプリケーションにアクセスしています。

- **[Owner]** : オーナーはコントローラか NMS のいずれかになります。コントローラでポリシーが作成されると、オーナーはコントローラとしてリストに表示されます。
- **[Search]** : 名前、AP、ESS、オーナーのいずれかで個別のポリシーを特定するには、検索ボックスにキーワードを入力し、Enter キーを押します。キーワードに一致する列がハイライト表示されます。ステータスに基づいて表示をフィルタリングするには、ステータスを (ドロップダウンから) 選択し、対応する列をハイライト表示します。
- **[Policy Reordering]** : ポリシーは、表示されている順序で実行されます。ポリシーの優先順位を並び替えるには、[Reorder] ボタンをクリックし、[Action] 列の矢印を使用してリストの表示順を上下させます。並び順の変更を有効にするには、これを保存する必要があります。

Reorder Policy						
Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Action
Corporate - 1	Enable	Disable	All Application, Facebook	mts	APs: AP-8	▼
Corporate - 2	Enable	Disable	Facebook , All Application	mts	APs: AP-8, AP-10	▲



ESS と AP の組み合わせが複数のポリシーに表示される場合には、順序の上位にあるポリシーがトリガされます。

下図では、ESSID MTS と APID AP-8 が Corporate-1 と Corporate-2 の両方のポリシーに表示されています。Corporate-1 ポリシーは Facebook トラフィックを許可し、Corporate-2 ポリシーは Facebook トラフィックをブロックします。Corporate-1 は Corporate-2 よりも上位にあるため、Facebook トラフィックは許可され、ブロックされません。ただし、AP-10 の Facebook トラフィックは Corporate-2 ポリシーによりブロックされます。

Reorder Policy						
Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Action
Corporate - 1	Enable	Disable	All Application, Facebook	mts	APs: AP-8	▼
Corporate - 2	Enable	Disable	Facebook , All Application	mts	APs: AP-8, AP-10	▲

カスタム アプリケーション

カスタム アプリケーションは、システム定義アプリケーションに含まれない、ユーザ定義アプリケーションです。コントローラに最大 32 個のアプリケーションを追加し、Network Manager でも最大 32 個のアプリケーションを追加できます。



カスタム アプリケーションのプロトコル / サブプロトコルの検出 / サポートは利用できません。

カスタム アプリケーションは、以下の要素を 1 つまたは複数組み合わせたものです。

- 事前定義された L4 および L7 プロトコル
- ソース ポートや宛先ポート
- ユーザ エージェント
- 任意の HTTP/HTTPS URL
- 宛先 IP



ポリシーで監視またはブロックされるカスタム アプリケーションの場合、そのプロパティのすべてがトラフィックと一致している必要があります。

カスタム アプリケーションの作成とそのポリシーへの割り当て

1. カスタム アプリケーションを作成するには、[Application] > [Settings] > [Custom Applications] に移動し、[Add] ボタンをクリックします。

The screenshot shows the 'Custom Applications' tab in a settings window. Below a table with columns 'Name', 'Description', and 'ID', there is an 'Add Custom Application' dialog box. The dialog contains the following fields:

- Name: Text input field with a hint 'Enter 1-32 chars.'
- Description: Text input field with a hint 'Enter 0-64 chars.'
- L4 Protocol: Dropdown menu with 'None' selected.
- L7 Protocol: Dropdown menu with 'None' selected.
- Source Ports: Text input field with a hint 'Valid range: [1-65535]'.
- Destination Ports: Text input field with a hint 'Valid range: [1-65535]'.
- User Agent: Text input field with a hint 'Enter 1-256 chars.'
- HTTP/HTTPS URL: Text input field with a hint 'Enter 1-256 chars.'
- Destination IPs: Text input field with a hint 'Valid IP Address'.

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

2. カスタム アプリケーションのプロパティを入力し、[Save] をクリックします。以下の例では、www.bbc.com からのトラフィックが監視されます。

Add Custom Application

Name	<input type="text" value="CustomApp-BBC"/>	Enter 1-32 chars.
Description	<input type="text" value="To monitor BBC traffic"/>	Enter 0-64 chars.
L4 Protocol	<input type="text" value="None"/>	
L7 Protocol	<input type="text" value="None"/>	
Source Ports	<input type="text"/>	Valid range: [1-65535]
Destination Ports	<input type="text"/>	Valid range: [1-65535]
User Agent	<input type="text"/>	Enter 1-256 chars.
HTTP/HTTPS URL	<input type="text" value="www.bbc.com"/>	Enter 1-256 chars.
Destination IPs	<input type="text"/>	Valid IP Address

3. カスタム アプリケーションのリストを表示します。

Global Settings		System Defined Applications		Custom Applications	
<input type="checkbox"/>	Name	Description	ID	Owner	
Search : ▶		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	CustomApp-BBC	To monitor BBC traffic	10001	controller	

4. カスタム アプリケーションをポリシーに追加します。[420 ページの「例」](#)で説明している手順を使用します。ただし、図の手順 4 では、カスタム アプリケーションの一番下まで

スクロールします。カスタム アプリケーションを選択してから、ポリシー設定を選択します。

Add Application

<input type="checkbox"/>	Application Name	Application Category
Search : <input type="text"/>		
<input type="checkbox"/>	Apple-Music	Streaming
<input type="checkbox"/>	Naver	Web
<input type="checkbox"/>	Booking-Com	Web
<input type="checkbox"/>	Cnn	Web
<input checked="" type="checkbox"/>	CustomApp-BBC	Custom Application

Add

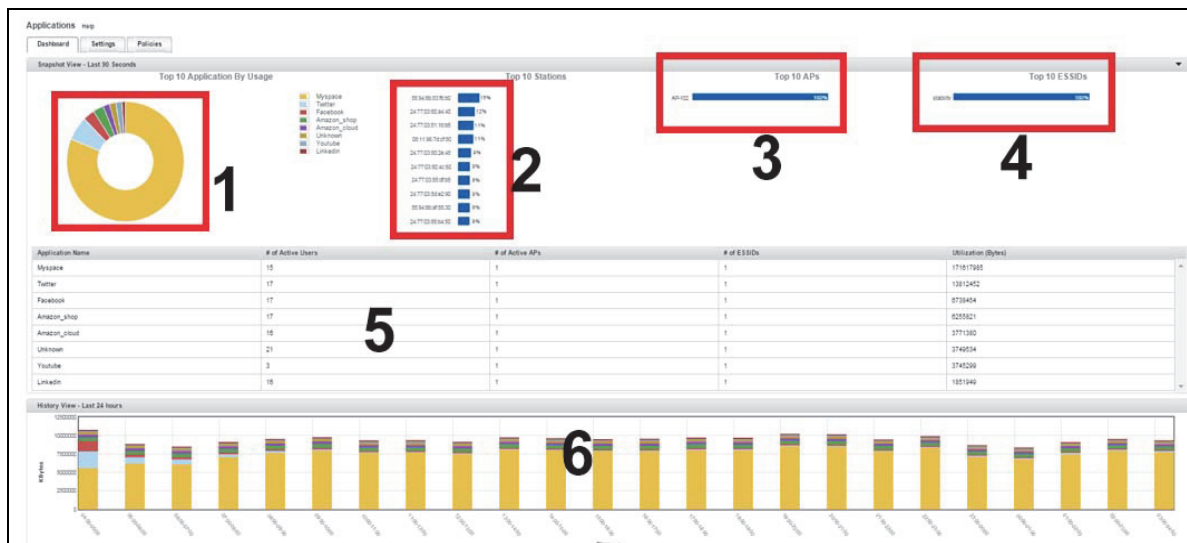
Cancel

5. カスタム アプリケーションがポリシーのリストに表示されるようになります。

<input type="checkbox"/>	Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Owner
Search : <input type="text"/>							
<input type="checkbox"/>	Corporate - 1	Enable	Disable	All Application, Facebook	mts	APs: AP-8	controller
<input type="checkbox"/>	Corporate - 2	Enable	Disable	All Application, Facebook CustomApp-BBC	mts	APs: AP-8, AP-10	controller

DPI ダッシュボード

DPI ダッシュボードには、監視 (検出) のみに設定されているアプリケーションが表示されます。ブロックされているアプリケーションは、AP でドロップされるため、ダッシュボードに表示されません。



1. 使用率トップ 10 の監視対象アプリケーションを使用して作成された円グラフが表示されます。
2. トップ 10 アプリケーションの 1 つまたは複数に接続されているトップ 10 ステーションのリスト。これは、ステーションごとの特定のアプリケーションの使用率を示すものではありません。
3. トップ 10 アプリケーションの 1 つまたは複数にトラフィックを送信している AP のリスト。
4. トップ 10 アプリケーションの 1 つまたは複数にトラフィックを送信している ESS プロファイルのリスト。
5. この表には、トップ 10 アプリケーションと、ステーション数、ESS プロファイル、AP、トラフィック サイズ (バイト) についての統計情報 (整数) が表示されます。
6. 表示されるのは、過去 24 時間のアプリケーション トラフィックの履歴データです。

CLI の使用

ポリシーの作成

1. config モードで、**app-visibility-policy <policy-name>** コマンドを使用します。
2. **state enable** コマンドを使用して、ステータスを有効にします。

3. **appids** <application-ID>:<type> を使用してアプリケーション ID とポリシー タイプを指定します。
 - トラフィックの使用を許可して監視するには、**A** を使用します。
 - トラフィックをブロックするには、**B** を使用します。
4. 1 つのポリシーに、アプリケーション トラフィックを監視およびブロックするルールを追加できます。

```
mc1500(15)(config)# app-visibility-policy CorpNet
mc1500(15)(config-app-visibility-policy)# description ""
mc1500(15)(config-app-visibility-policy)# state enable
mc1500(15)(config-app-visibility-policy)# appids 6:B
mc1500(15)(config-app-visibility-policy)# essids stability
mc1500(15)(config-app-visibility-policy)# apids "5:A"
mc1500(15)(config-app-visibility-policy)# owner controller
mc1500(15)(config-app-visibility-policy)# version 0
mc1500(15)(config-app-visibility-policy)# exit
```

特定の AP 用に設定されたポリシーとタイプのリストを表示するには、**show application-visibility policy-config-service <app-id>** コマンドを使用します。

```
mc1500(15)# show application-visibility policy-config-service 5
```

AP	ESSID	APPID	Action
5	1	2	Allow
5	1	5	Allow
5	1	6	Block
5	1	8	Allow
5	1	24	Allow
5	1	32	Allow
5	1	41	Allow
5	1	70	Allow

Application Visibility Policy Service(8)

凡例

図 71: DPI Config オプションの凡例

ラベル	説明
A	アプリケーションに使用する場合、アプリケーション トラフィックを許可、検出、監視することを意味します。
B	アプリケーション トラフィックを検出してブロックする場合に使用します。
A	AP-ID として使用する場合、個別の AP を追加することを示します。
L	ap-group をポリシーに追加する場合に使用します。

ポリシーの監視

```
mc1500(15)# sh service-summary Application-Visibility
```

Feature	Type	Name	Value	ValueStr
Application-Visibility	Application	myspace {"util":3006.76,"tx":6943001576,"rx":257651566}	100	
Application-Visibility	Application	amazon_cloud {"util":474.84,"tx":1093389603,"rx":43774451}	0	
Application-Visibility	Application	facebook {"util":184.00,"tx":421673492,"rx":18973696}	0	
Application-Visibility	Application	twitter {"util":164.58,"tx":358628579,"rx":35513363}	0	
Application-Visibility	Application	unknown {"util":97.92,"tx":221291109,"rx":13202213}	0	
Application-Visibility	Application	amazon_shop {"util":77.81,"tx":162324404,"rx":24026568}	0	
Application-Visibility	Application	linkedin {"util":48.60,"tx":109814218,"rx":6565367}	0	
Application-Visibility	Application	youtube 1.34,"tx":2910287,"rx":292302}	0	{"util":
Application-Visibility	Station	58:94:6b:b5:ca:c4 {"util":591.86,"tx":1364192275,"rx":53208638}	100	
Application-Visibility	Station	00:27:10:cb:90:40 {"util":571.51,"tx":1317000065,"rx":51657115}	0	
Application-Visibility	Station	10:0b:a9:44:f6:ac {"util":297.04,"tx":681777356,"rx":29579769}	0	

```

Application-Visibility Station      24:77:03:80:4c:60      0
{"util":294.30,"tx":676177538,"rx":28620457}

Application-Visibility Station      84:3a:4b:48:1e:c0      0
{"util":291.67,"tx":668985331,"rx":29513381}

Application-Visibility Station      24:77:03:80:2e:48      0
{"util":287.46,"tx":660217415,"rx":28188180}

Application-Visibility Station      08:11:96:7d:cf:80      0
{"util":286.78,"tx":657504303,"rx":29271859}

Application-Visibility Station      24:77:03:80:a4:40      0
{"util":281.94,"tx":646183947,"rx":29009375}

Application-Visibility Station      24:77:03:80:5f:54      0
{"util":280.23,"tx":645624714,"rx":25475052}

Application-Visibility Station      24:77:03:85:b4:50      0
{"util":279.89,"tx":641592459,"rx":28689908}

Application-Visibility EssId        stability          100
{"util":4055.84,"tx":9313033268,"rx":399999526}

Application-Visibility AP            AP-109            100
{"util":4055.84,"tx":9313033268,"rx":399999526}

```

Service Data Summary(20 entries)

```
mc1500(15)# sh ap
```

```

ap          ap-certificate      ap-discovered      ap-online-
  history    ap-reboot-event      ap-redirect        application-
  visibility

ap-assigned  ap-connectivity      ap-neighbor        ap-reboot-
  count      ap-reboot-top10      ap-swap

mc1500(15)# sh application-visibility application-summary

```

APPID	Name	Station Counts	AP Counts	ESS Counts
Tx Bytes	Rx Bytes	TxRx Bytes		
5	myspace	12	1	1
7274981850	269918317	7544900167		
24	amazon_cloud	13	1	1
1149026229	45994062	1195020291		

2	facebook	13	1	1
443832821	19962877	463795698		
8	twitter	13	1	1
375850987	37259491	413110478		
0	unknown	20	1	1
233565871	13899667	247465538		
70	amazon_shop	13	1	1
170637983	25318821	195956804		
41	linkedin	12	1	1
115430025	6896689	122326714		
32	youtube	13	1	1
3022484	304784	3327268		

Application Visibility Statistics Summary(8)

mc1500(15)#

mc1500(15)# sh service-summary-trend Application-Visibility

Feature	Type	Name	StartTime
EndTime	Value	ValueStr	
Application-Visibility	Application	myspace	01/17/2009
01:00:00 01/17/2009 02:00:00	370191907		
	{"util":254501.59,"tx":3561906268,"rx":140012805}		
Application-Visibility	Application	amazon_cloud	01/17/2009
01:00:00 01/17/2009 02:00:00	523131985		
	{"util":35964.57,"tx":502700232,"rx":20431753}		
Application-Visibility	Application	twitter	01/17/2009
01:00:00 01/17/2009 02:00:00	221967525		
	{"util":15259.95,"tx":202733592,"rx":19233933}		
Application-Visibility	Application	facebook	01/17/2009
01:00:00 01/17/2009 02:00:00	220636588		
	{"util":15168.45,"tx":210304218,"rx":10332370}		
Application-Visibility	Application	unknown	01/17/2009
01:00:00 01/17/2009 02:00:00	113502079		
	{"util":7803.10,"tx":106412520,"rx":7089559}		

Application-Visibility	Application	amazon_shop	01/17/2009
01:00:00	01/17/2009	02:00:00 106703142	
{ "util":7335.69, "tx":93322094, "rx":13381048 }			
Application-Visibility	Application	linkedin	01/17/2009
01:00:00	01/17/2009	02:00:00 58696435	
{ "util":4035.30, "tx":55165018, "rx":3531417 }			
Application-Visibility	Application	youtube	01/17/2009
01:00:00	01/17/2009	02:00:00 1454576	
{ "util":100.00, "tx":1315107, "rx":139469 }			
Application-Visibility	Application	myspace	01/17/2009
02:00:00	01/17/2009	03:00:00 781850640	
{ "util":264335.11, "tx":7508697893, "rx":309808509 }			
Application-Visibility	Application	amazon_cloud	01/17/2009
02:00:00	01/17/2009	03:00:00 112454581	
{ "util":38019.66, "tx":1078606475, "rx":45939338 }			
Application-Visibility	Application	facebook	01/17/2009
02:00:00	01/17/2009	03:00:00 472612999	
{ "util":15978.53, "tx":448955762, "rx":23657237 }			
Application-Visibility	Application	twitter	01/17/2009
02:00:00	01/17/2009	03:00:00 442033093	
{ "util":14944.65, "tx":401239344, "rx":40793749 }			
Application-Visibility	Application	amazon_shop	01/17/2009
02:00:00	01/17/2009	03:00:00 229558452	
{ "util":7761.12, "tx":202329371, "rx":27229081 }			
Application-Visibility	Application	unknown	01/17/2009
02:00:00	01/17/2009	03:00:00 215482783	
{ "util":7285.24, "tx":200402948, "rx":15079835 }			
Application-Visibility	Application	linkedin	01/17/2009
02:00:00	01/17/2009	03:00:00 125984872	
{ "util":4259.41, "tx":118235346, "rx":7749526 }			
Application-Visibility	Application	youtube	01/17/2009
02:00:00	01/17/2009	03:00:00 2957801	
{ "util":100.00, "tx":2659330, "rx":298471 }			
Application-Visibility	Application	myspace	01/17/2009
03:00:00	01/17/2009	04:00:00 859492100	
{ "util":269614.13, "tx":8269499897, "rx":325421104 }			
Application-Visibility	Application	amazon_cloud	01/17/2009
03:00:00	01/17/2009	04:00:00 116518953	
{ "util":36550.84, "tx":1119128571, "rx":46060960 }			

Application-Visibility	Application	facebook	01/17/2009
03:00:00	01/17/2009	04:00:00	461844358
{ "util":14487.60,"tx":440897736,"rx":20946622 }			
Application-Visibility	Application	twitter	01/17/2009
03:00:00	01/17/2009	04:00:00	408573605
{ "util":12816.55,"tx":369504893,"rx":39068712 }			
Application-Visibility	Application	unknown	01/17/2009
03:00:00	01/17/2009	04:00:00	237048541
{ "util":7435.98,"tx":221824322,"rx":15224219 }			
Application-Visibility	Application	amazon_shop	01/17/2009
03:00:00	01/17/2009	04:00:00	204090068
{ "util":6402.10,"tx":178965615,"rx":25124453 }			
Application-Visibility	Application	linkedin	01/17/2009
03:00:00	01/17/2009	04:00:00	121917540
{ "util":3824.43,"tx":114827231,"rx":7090309 }			
Application-Visibility	Application	youtube	01/17/2009
03:00:00	01/17/2009	04:00:00	3187860
{ "util":100.00,"tx":2879796,"rx":308064 }			

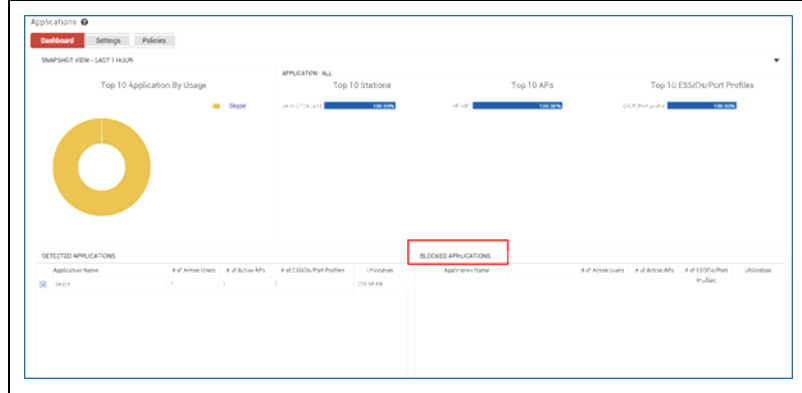
Service Data Summary Trend(24 entries)

アプリケーション可視化における機能としては、他にも以下のものがあります。

- ブロックされたトラフィックの統計情報
- ポート プロファイルを使用しての有線クライアントのサポート
- 帯域幅制限
- DSCP マーキング

ブロックの統計情報

ダッシュボードには、ブロックされたトラフィックについての詳細な統計情報が表示されます。



[BLOCKED APPLICATIONS] セクションには以下の統計情報が表示されます。

- [Application Name] : ブロックするように設定されているアプリケーションのトラフィック。
- [# of Active Users] : アプリケーションへのアクセスを要求しているユーザ数。
- [# of Active APs] : トラフィックをブロックしている AP 数。
- [# of ESSIDs / Port] : ワイヤレス クライアントおよび有線クライアントに接続されている ESSID/ ポート プロファイル数。
- [Utilization] : ブロックされているトラフィックの量。

有線クライアントのサポート

トラフィックの検出、ブロック、帯域幅制御を行う有線クライアントの追加を有効にするために、ポート プロファイルを追加できます。新しいポリシー ページが更新され、コントローラで作成されたポート プロファイルのリストが表示されます。ESSID とポート プロファイルの両方の組み合わせ、ESS プロファイルのみ、ポート プロファイルのみのいずれかを使用して、ポリシーを作成できます。以下に示す例では、CLI を使用して有線ポートのポリシーを作成し、ポリシーの詳細を表示しています。

```
default(15)# configure terminal
default(15)(config)#
default(15)(config)# app-visibility-policy wiredPorts
default(15)(config-app-visibility-policy)#
default(15)(config-app-visibility-policy)# port-profiles wired-profile
default(15)(config-app-visibility-policy)# state enable
default(15)(config-app-visibility-policy)# appids *
```

```
default(15)(config-app-visibility-policy)# advanced-detection enable
```

カンマ区切りの値を使用して、複数のポート プロファイルを追加できます。

```
例： default(15)(config-app-visibility-policy)# port-profiles wired-  
profile,default
```

ポリシー詳細の表示

```
default(15)# sh application-visibility policy wiredPorts
```

Application Visibility Policy

Policy Name : wiredPorts

Policy Order : 2

Description :

Policy : enable

Advanced Detection : enable

Bandwidth Limiting : disable

Application ID List : *

ESSID List :

AP Groups or APs :

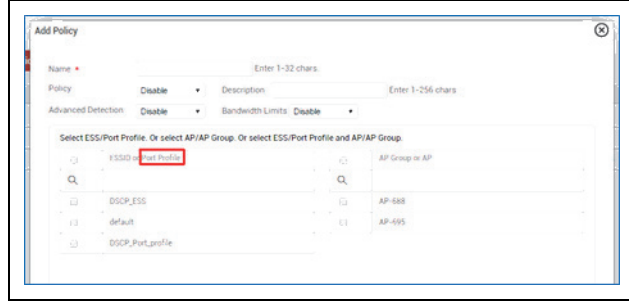
Owner : controller

Port Profile List : wired-profile

```
default(15)#
```

帯域幅制限

選択したアプリケーションで帯域使用量の制限を適用できます。



1. 帯域幅制限を有効にするには、ポリシーを作成し、[Enable option for Bandwidth Limits] を選択します。
2. [ESSID] または [Port Profile] を選択します。
3. クライアントおよび SSID/ ポート向けの最大帯域幅の制限を指定します。

	最小	最大
クライアント	150 kbps	1 Gbps
ESSID/ ポート プロファイル	150 kbps	12 Gbps

制限事項：

- 帯域幅制限は、最大 10 個のアプリケーションに実装できます (個別に実装することも、ポリシーにわたって累積的に実装することも可能)。
- 有効にすると、帯域幅制限ポリシーはすべての AP に適用可能になります。AP と AP グループの選択はできません。
- クライアントでの使用向けに設定されている最大帯域幅の値は、ESSID またはポート トラフィックの使用で設定されている値以下または同等でなければなりません。
- トンネル プロファイルが使用されているクライアント トラフィックのみサポートされています。

DSCP マーキング

DSCP の値を アプリケーション トラフィック (アップストリーム：AP からコントローラへ、およびダウストリーム：AP からステーションへ) に追加して、その優先度を変更できます。選択したアプリケーションの DSCP 値は、検出されたアプリケーション トラフィックを (ワイヤレスまたは有線 STA に) マーキングするために使用されます。

DSCP 値がアプリケーション トラフィックに適用される場合、この値と関連優先度は、トラフィックの次のノードまで保持されます。DSCP 値を有するトラフィックが QoS 対応スイッチに流れると、DSCP 値は、スイッチで指定されている QoS 値で上書きされる場合があります。

ダウンストリーム トラフィックでは、コントローラによって DSCP 値が適用されてから、AP に転送されます。これがサポートされているのは、トンネル モードの ESSID だけです。

注：DSCP マーキングは、最大 10 個のアプリケーション (すべてのポリシーを含む) に追加できます。

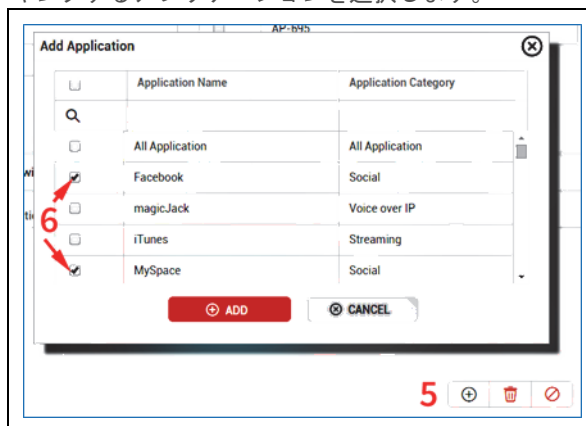
DSCP 値をアプリケーション トラフィックに割り当てるには、次の手順を実行します。

1. [Configuration] > [Access Control] > [Application] > [Policies] タブに移動します。
2. [Add] ボタンをクリックして、新しいポリシーを追加します。

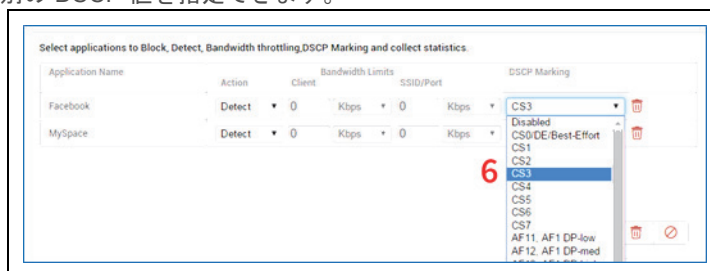
新しいポリシーについて、以下の詳細を設定します。

1. ポリシーの名前を入力します。
2. [Enable] を選択してポリシーを有効にします。
3. ESS プロファイルを選択します。
4. AP または AP グループを選択します。
5. 追加アイコンをクリックして、アプリケーションのリストを表示します。

6. DSCP 値でマーキングするアプリケーションを選択します。



7. リスト表示されたアプリケーションについて、[DSCP Marking] カラムのドロップダウンから、個別の DSCP 値を指定できます。



有効な DSCP 値の文字列

- af11
- af12
- af13
- af21
- af22
- af23
- af31
- af32
- af33
- af41
- af42
- af43

- cs0
- cs1
- cs2
- cs3
- cs4
- cs5
- cs6
- cs7
- X
- ef

DSCP 値の詳細については、次の Web サイトを参照してください。<https://tools.ietf.org/html/rfc4594>

CLI コマンド

ダウンストリーム トラフィックの DSCP マーキングを有効にするには、以下のコマンドを使用します。

```
default(15)(config)# app-visibility-config controller-dscp-marking-state enable
```

以下のコマンド形式は、DSCP マーキングを設定し、帯域幅の制限を指定します。

```
<app-id>:A or B|C:<per-client-bw-value>:<bw-unit>|E:<per-ess-bw-value>:<bw-unit>|D:<dscp-string>
```

- アプリケーション ID - <app-id>
- ルール タイプ (A- 許可、B - ブロック) - < A または B>
- クライアントの帯域幅制限ごと - C:<bw-value>:<bw-unit> [サポートされているユニット K、M、G]
- ESSID の帯域幅制限ごと - E:<bw-value>:<bw-unit> [サポートされているユニット K、M、G]
- DSCP 値 - D:<dscp-value-string> [サポートされている値]

例 :

```
2:A|C:150:K|E:1:M|D:af11
```

上掲のコマンドは、ID 2 のアプリケーションへのトラフィックを許可し、このアプリケーション トラフィックにアクセスしているクライアントの帯域幅と ESS プロファイルをそれぞれ 150 キロビットと 1 メガビットに制限し、アップストリーム トラフィックの DSCP を af11 に設定します。

ベスト プラクティス

アプリケーション可視化ポリシーを作成する場合の推奨ベスト プラクティスは以下のとおりです。

- 検出、ブロック、または帯域幅制限の適用が可能な単一ポリシーを作成できる場合は、検出、ブロック、または帯域幅制限の適用を単独で行うポリシーを個別に作成することをお勧めします。
- ポリシーは、以下の順序で優先順位付けされます。
 - ブロック
 - 帯域幅制限
 - 検出 (全般)

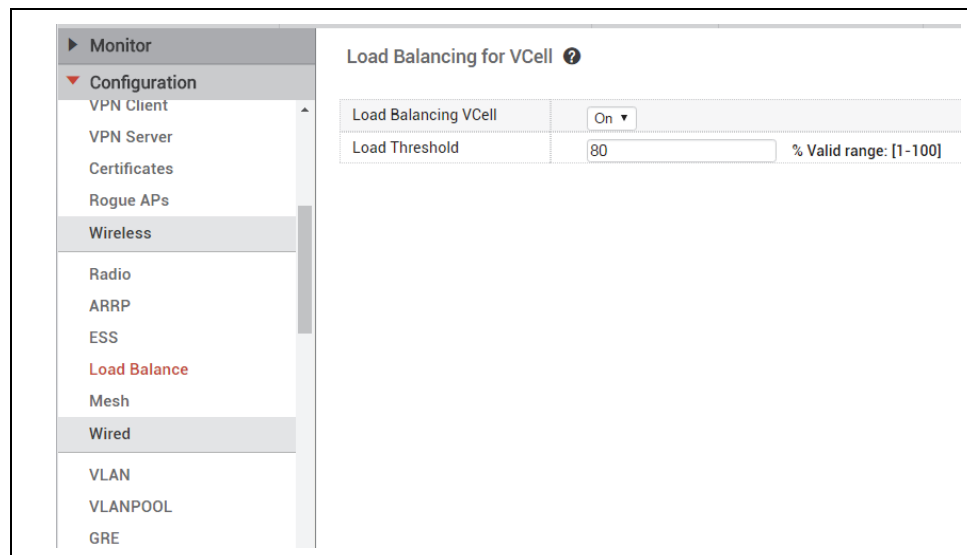
仮想セルにおける AP のロード バランス

ロード バランスを設定することで、ワイヤレス クライアントを代替アクセス ポイントに効果的に分散できます。ロード バランスは、「AP の現在のロード」と「クライアントの RSSI 値」の 2 つの要素に基づき、コントローラによって実行されます。

- AP の現在のロード - 現在のロードは、AP に割り当てられているクライアント数を示します。
- クライアントの RSSI 値 - クライアントの RSSI 値は、コントローラが受信します。

新規クライアントがネットワークに加わると、コントローラによって、「最大ロードしきい値を下回って動作し、かつ最高の RSSI 値を提供している AP」にそのクライアントが接続されます。

ロード バランスを有効にするには、アクセス ポイントのロードしきい値を設定します。
[Configuration] > [Wireless] > [Load Balance] に移動します。



1. [Load Balancing vCell] : [On] を選択してこの機能を有効にします。
2. [Load Threshold] : ロードしきい値を指定します。この値は、AP に接続可能なクライアント数をパーセンテージで示すものです。たとえば、AP の最適な容量が 80 クライアントの場合に、しきい値として 90% を設定すると、最大 72 クライアントが接続可能ということになります。
3. RSSI しきい値は、CLI (`load-balance-vcell rssi-threshold <rssi-value>`) で設定できます。最高および代替 AP の RSSI 値を指定します。ロード バランスは、設定された RSSI 値を下回る値の場合に有効になります。デフォルト値は -65dbm であり、設定可能な範囲は -75dbm ~ -45dbm です。以下の表は、さまざまなモードおよびチャネル帯域幅の場合に推奨される RSSI しきい値を示しています。

	20 MHz	40 MHz	80 MHz	160 Mhz / 80+80 Mhz
802.11b	-76 dbm	なし	なし	なし
802.11a/g	-65 dbm	なし	なし	なし
802.11n	-64 dbm	-61 dbm	-58 dbm	なし
802.11ac	-57 dbm	-54 dbm	-51 dbm	-48 dbm

nPlus1 のサポート : ロード バランス機能により、nplus1 起動時のローミング中に利用可能な最良のアクセス ポイントにクライアントを接続できます。

以下の表では、2 つの AP (AP1 と AP2) 間におけるさまざまなロード バランス シナリオと、クライアントがネットワークに参加しようとする場合に予想される結果を示しています。:

- L1 は AP1 におけるロードを示し、L2 は AP2 におけるロードを示します。値「1」は、AP1 がそのロードしきい値に達していることを示します。
- R1 は AP1 における RSSI 値を示し、R2 は AP2 における RSSI 値を示します。値「1」は、RSSI 値が設定値を上回っていることを示します。

シナリオ	予想される結果
L1=1、L2=0、R1=0、R2=0	AP1 が最大容量で動作しているため、クライアントは AP2 に割り当てられます。
<ul style="list-style-type: none"> • L1=0、L2=0、R1=0、R2=0 • L1=0、L2=0、R1=-1、R2=-1 • L1=1、L2=1、R1=1、R2=1 	これらのシナリオでは、コントローラがデフォルトの連携機能を使用して、クライアントを AP に割り当てます。
<ul style="list-style-type: none"> • L1=0、L2=1、R1=1、R2=0 • L1=1、L2=0、R1=1、R2=0 • L1=1、L2=0、R1=1、R2=1 • L1=1、L2=1、R1=1、R2=0 	これらのシナリオでは、クライアントは AP2 に割り当てられます。
L1 =1 または L2 =1 のその他の場合	クライアントは現在の AP (AP1 など) と関連付けられたままです。

管理パケットの DSCP マーキング

DSCP (Differentiated Services Code Point) の値を管理およびアプリケーション トラフィックに適用できます ([Application Visibility Enhancements] セクションを参照)。DSCP 値は選択可能なフィールドであり、さまざまな優先レベルをネットワーク トラフィックに割り当てるために使用できます。

デフォルトでは、トラフィック パケットに EF 値が含まれていましたが、この機能が搭載されたことで、EF から、要件を満たす適切な DSCP 値へと優先度ビットを変更できます。

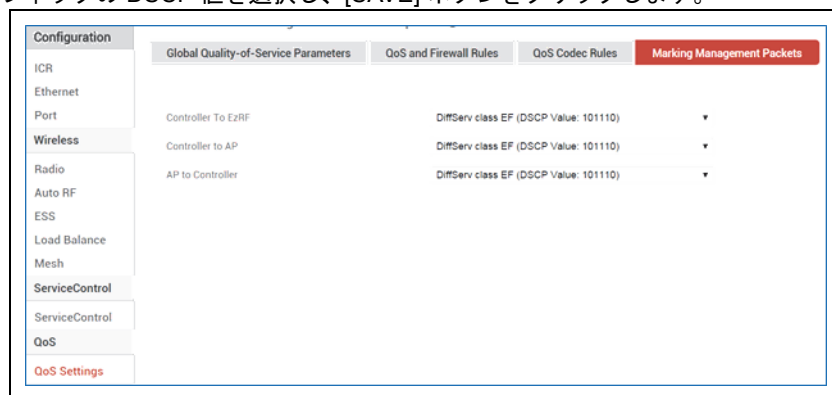
以下の項目間の管理トラフィックには、DSCP 値を割り当てることができます。

- AP からコントローラまで
- コントローラから AP まで
- コントローラから Network Manager まで

DSCP 値の有効化

Web UI から DSCP を設定するには、[Configuration] > [Policies] > [QoS Settings] > [Marking Management Packets] タブに移動します。

各トラフィックの DSCP 値を選択し、[SAVE] ボタンをクリックします。



Configuration	Global Quality-of-Service Parameters	QoS and Firewall Rules	QoS Codec Rules	Marking Management Packets
ICR				
Ethernet				
Port	Controller To EzRF			DiffServ class EF (DSCP Value: 101110) ▼
Wireless	Controller to AP			DiffServ class EF (DSCP Value: 101110) ▼
Radio	AP to Controller			DiffServ class EF (DSCP Value: 101110) ▼
Auto RF				
ESS				
Load Balance				
Mesh				
ServiceControl				
ServiceControl				
QoS				
QoS Settings				

16 メッシュ ネットワーク

Enterprise Mesh は、AP をコントローラに接続するイーサネット リンクの代替オプションの無線製品です。Enterprise Mesh システムを配備することで、有線のスイッチド バックボーンを完全なワイヤレス 802.11 バックボーンに置き換え、同等のスループット、QoS、およびサービスが実現します。

Enterprise Mesh の機能は次のとおりです。

- 階層型帯域幅アーキテクチャ
- RF スペクトラムの動的な割り当てと負荷分散
- 全 2 重機能
- バックボーンよりも拡張された仮想セル、QoS、および RF 調整
- ワイヤレス WDS による Enterprise Mesh トラフィックのカプセル化
- データプレーン暗号化 (暗号化 / 復号化がソフトウェアに置かれるため、パフォーマンスに影響します)

メッシュ配備は、次のような環境では使用しないことを推奨します。

- 大都市圏または公共の Wi-Fi ネットワーク
- 高いスループット、密度、または品質が求められるビデオ / 音声アプリケーション

メッシュの制約

フォーティネットのメッシュ ネットワークの設計と実装では、次のような制限があります。

- Enterprise Mesh AP には、コントローラに対する L3 接続が必要です。
- SAM 経由のバックホール リンクの監視はサポートされていません。
- メッシュにアクティブに使用されない無線は、SAM の目的に使用できません。
- Enterprise Mesh では、ワイヤレス クライアント向けのブリッジ モードはサポートされていません。トンネル モードのみがサポートされています。
- ゲートウェイとメッシュ AP は、最大 4 のバックホール リンクをサポートしています。
- ゲートウェイ (すなわち、ネットワークに物理接続されている AP) からは、クラウドあたり 16 以下の AP で、最大 3 ホップがサポートされています。
- メッシュ クラウドで同時にアクティブにできるステーションは最大 500 です。

- 最小チャンネル分離のガイドラインに従って、非オーバーラップチャンネルを使用してください。
- DFS チャンネルでのメッシュ処理は推奨されません。
- 複数のアップリンク接続の集約はサポートされていません。
- 1 つの AP を複数のメッシュクラウドに割り当てることはできません。
- 1 つのコントローラで最大 64 のメッシュプロファイルを作成できます。メッシュプロファイルごとに最大 16 の AP を含めることができます。
- OAP832 には 5Ghz の無線 1 しかないため、その無線でのみメッシュを確立できます。

Enterprise Mesh の設計

Enterprise Mesh は一般的に、ハブ & スポーク構成 ([図 72](#))、チェーン構成 ([図 73](#))、またはこれらのバリエーションで構成されます。

高密度ネットワークでは、衝突が発生する可能性があります、ハブ & スポーク (すべての AP がゲートウェイをポイント) が最適なトポロジです。

- 最適なパフォーマンスを実現するには、チャンネルごとにクラウドを作成することで、隣接する小さいクラウド間の衝突を回避します。クラウドは、バックホールのトポロジパスでゲートウェイ AP と通信する AP の集まりとして定義されます。

図 72: Enterprise Mesh ネットワーク - ハブ & スポーク設計

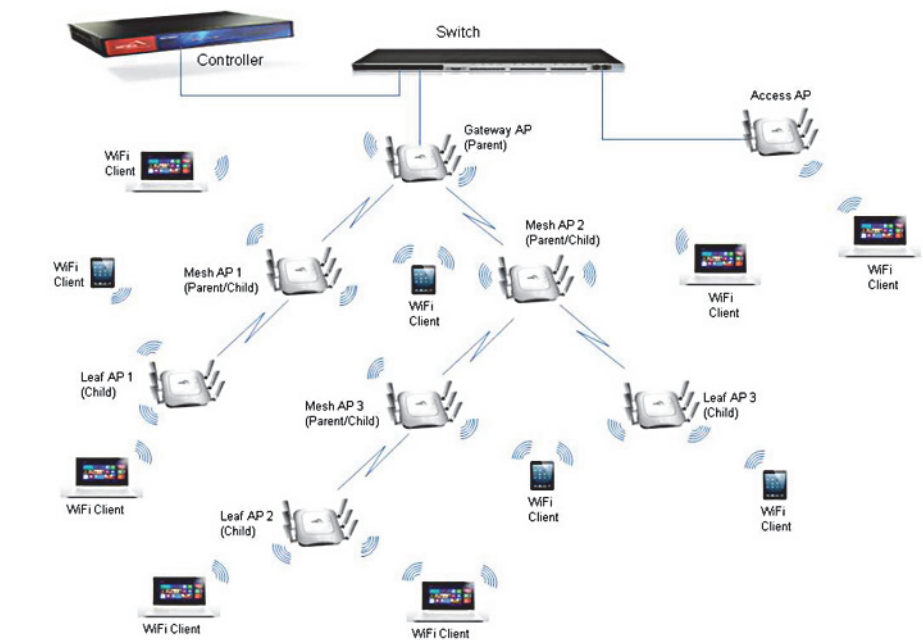
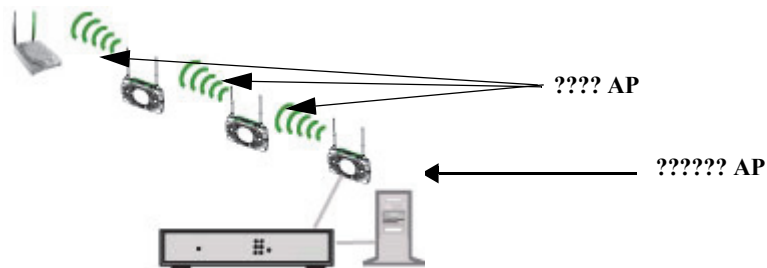


図 73: 3 ホップの Enterprise Mesh - チェーン設計



ゲートウェイ AP

ゲートウェイ AP は、Enterprise Mesh ネットワークの有線エッジに配置され、有線とワイヤレスのサービス間をリンクします。ゲートウェイ AP は、ネットワークに有線接続する唯一の AP です。

メッシュ AP

メッシュ AP とは、ゲートウェイ AP として動作していないすべての AP のことです。メッシュ AP は、他のメッシュ AP 間の中間サービスを提供したり、メッシュ チェーンのエンドポイントとして使用されたりします (図 73)。メッシュ AP は、ネットワークに有線接続できます。



メッシュ AP の未使用のイーサネット ポートは、イーサネット スイッチの有線ポートと同じ方法で構成し、使用できます。したがって、ユーザは、他の有線デバイスでハブ / スイッチを接続し、会社のネットワークにアクセスできます。ポートを使用するには、ポート プロファイルを設定する必要があります。詳細については、「[ポート プロファイルの設定](#)」を参照してください。

リーフ AP

ワイヤレス バックホール接続を介してコントローラに接続されるが、別のノードにはワイヤレス バックホール サービスを提供できない AP。

有線クライアント

メッシュ AP として構成される AP400 の未使用のイーサネット ポート (インターフェイス 1) は、最大 512 の有線クライアントへの接続に使用できます。

機器の要件

どのコントローラ モデルもメッシュ環境に使用できます。現段階でメッシュ処理をサポートしている AP モデルを以下に記載します。

- AP1000 シリーズ
- AP332e/i
- AP832、AP800
- AP433
- FAP-U421EV
- FAP-U423EV

Enterprise Mesh システムのインストールと設定

アンテナの設置場所の決定

Enterprise Mesh は、AP を (リピータとして) 使用することで、ワイヤレスの受信範囲を拡張します。Enterprise Mesh 内の AP は、親 AP からの信号を検索するよう指示されます。このため、アンテナの設置場所と受信状態はシステム パフォーマンスの最適化にとって重要です。

無線経路に障害物があると、無線信号の品質と強度が低下します。経路上の障害物からの最大距離を計算することが重要であり、アンテナの設置場所と高さを決定する際に考慮する必要があります。また、無線信号が容易に損失される可能性がある長距離リンクにおいては特に重要です。

ワイヤレス ホップの無線経路を設計する場合は、次の点を考慮します。

- ノード間の経路に隣接している、または、経路の障害物になる可能性がある、ツリーや他のリーフに注意します。
- 建物からの距離が十分にあり、建物の構造が経路の障害になる可能性がないことを確認します。
- 地図、航空写真、または衛星画像データを使用して、アンテナ間の地形のトポロジをチェックします (地域ごとの情報が含まれるソフトウェア パッケージを利用できます)。
- 自動車、列車、または航空機の移動が一時的な障害物になる可能性がある経路を避けます。

Fortinet Enterprise Mesh のインストール

Enterprise Mesh の AP は、5 つのフェーズで設定されます。



これらの手順は、プラグ & プレイの機能を使用しないで設定することを前提としています。詳細については、[451 ページの「プラグ & プレイによるメッシュ AP の追加」](#)を参照してください。

- **フェーズ 1: イーサネット スイッチでコントローラと AP を接続する**
- **フェーズ 2: メッシュ プロファイルを作成する**
- **フェーズ 3: AP をメッシュに追加する**
- **フェーズ 4: AP のメッシュ処理を設定する**
- **フェーズ 5: ケーブルを外して AP を配備する**

フェーズ 1: イーサネット スイッチでコントローラと AP を接続する

標準のメッシュの初期セットアップでは、ユーザが、希望するすべてのメッシュ AP を、ローカル スイッチによる有線接続経由で 1 度に設定できます (この設定は、リモート配備の前に実行することを想定しています)。ローカルで設定する前に AP をリモートで配備できる代替方法については、「[プラグ & プレイによるメッシュ AP の追加](#)」を参照してください。

1. スイッチまたはハブ経由で、すべての AP をコントローラに直接接続します。
2. コントローラの電源をオンにします。
3. 別々の電源または PoE (Power over Ethernet) 接続を使用して、AP を電源に接続します。
4. コントローラに IP アドレスが割り当てられていない場合は、次の設定を実行し、割り当てられている場合は、手順 5 に進みます。
 - シリアル ケーブルでコンピュータをコントローラに接続します。
 - 115200 ボー、8 ビット、パリティなしに設定した PC 端末プログラムを使用してコントローラにアクセスし、デフォルトのユーザ / パスワード (admin/admin) でログインします。
 - setup コマンドを使用してコントローラに IP アドレスを割り当てます。
 - コントローラをリブートし、admin として再ログインします。
5. admin アカウントで、コントローラの CLI にログインします (ログインしていない場合)。
6. Enterprise Mesh に接続される AP がコントローラに接続されている (有効でオンラインである) ことを確認し、AP のランタイム バージョンがコントローラの FortiWLC (SD) と同じバージョンであることを確認します。
 - show controller コマンドで、FortiWLC (SD) のバージョンを確認します。
 - show ap コマンドで、AP を確認します。

フェーズ 2: メッシュ プロファイルを作成する

必要に応じて、1 つのコントローラで複数の異なるメッシュを管理できます。以下の手順に従って、メッシュ プロファイルを作成します。

1. Web UI (インターネット ブラウザを開き、コントローラの IP アドレスを入力してアクセスします) から、[Configuration] > [Wireless] > [Mesh] に移動します。[Mesh Configuration] 画面が表示されます (メッシュ プロファイルが既に存在していない限り、この画面には何も表示されません)。
2. [Add] をクリックします。
3. [Mesh Configuration - Add] 画面に、以下の詳細を入力します。
 - Name: メッシュ プロファイルの名前を入力します。
 - Description: プロファイルの短い説明 (場所など) を入力します。

- Pre-shared Key: メッシュ通信の暗号化キーを入力します。このキーは、メッシュ プロファイルに追加された AP 間で自動的に共有されるため、後で手動で入力する必要はありません。このキーは、8 ～ 63 文字である必要があります。
 - Admin Mode: このフィールドを [Enable] に設定すると、メッシュ プロファイルが有効になります。何らかの理由でプロファイルが無効にする必要がある場合は、このフィールドを [Disable] に設定します。
 - PlugNPlay Status: このオプションを使用すると、メッシュ AP をワイヤレスでメッシュに追加できるため、メッシュの設定で AP を接続する必要がなくなります。詳細については、「[プラグ & プレイによるメッシュ AP の追加](#)」を参照してください。
4. すべてのフィールドを設定したら、[OK] をクリックします。新しいメッシュ プロファイルがメッシュ テーブルに表示されます。

フェーズ 3 : AP をメッシュに追加する

ここまでの手順でメッシュが作成されたので、次に、AP をメッシュに 追加できます。以下の手順に従ってください。



メッシュ AP をメッシュに追加するには、そのメッシュ AP がコントローラの AP テーブルに存在する必要があります (メッシュ AP は手動で追加するか、前の手順で実行したようにコントローラに接続されている必要があります)。

1. [Configuration] > [Wireless] > [Mesh] 画面で、変更するメッシュ プロファイルの隣にあるチェックボックスをオンにし、[Settings] をクリックします。メッシュの設定がまとめて表示されます。

図 74: メッシュの変更

Mesh Configuration - Update

Name		Mesh832
Description	<input type="text" value="prat"/>	Enter 0-128 chars.
Pre-shared Key (Alphanumeric/Hexadecimal)	<input type="text" value="....."/>	
Admin Mode	<input type="button" value="Enable"/> ▼	
PlugNPlay Status	<input type="button" value="Disable"/> ▼	

2. [Mesh AP Table] タブをクリックします。AP がまだ追加されていないので、このテーブルは空白です。
3. [Add] をクリックします。
4. 表示されるページで、[AP ID] ドロップダウンを使用して、該当する AP を指定します。
5. [OK] をクリックして AP を追加します。AP がメッシュ AP テーブルに表示されます。

追加するすべての AP について、以上の手順を繰り返します。すべての AP が追加されたら、メッシュ処理を使用するよう設定できます。

フェーズ 4 : AP のメッシュ処理を設定する

AP は実際にメッシュ プロファイルに追加されましたが、さらに、メッシュ処理を使用するよう設定する必要があります。以下の手順に従ってください。

1. Web UI から、[Configuration] > [Devices] > [APs] に移動します。
2. いずれかのメッシュ AP の隣のチェックボックスをオンにし、鉛筆アイコンをクリックします。
3. [Wireless Interface] タブをクリックして、AP で利用できるワイヤレス インターネットを表示します。
4. いずれかのインターフェイスの隣のチェックボックスをオンにし、[Settings] をクリックします。いずれかのインターフェイスを選択できますが、現段階では、デュアル インターフェイス メッシュはサポートされていません。
5. [Wireless Interface] タブで、[Mesh Service Admin Status] のドロップダウン ボックスをクリックし、[Enable] を選択します。

図 75: メッシュ サービスの有効化

The screenshot shows a configuration page for a mesh service. It includes the following elements:

- Virtual Cell:** A dropdown menu currently set to "Off".
- Probe Response Threshold:** A text input field containing the value "15". To its right, it says "Valid range: [0-100]".
- Mesh Service Admin Status:** A dropdown menu with three options: "Disable", "Disable", and "Enable". The "Enable" option is highlighted in blue.
- Show Detail Info...**: A link to view more details.

6. [OK] をクリックして、設定の変更を保存します。

メッシュの一部であるすべての AP について、以上の手順を繰り返します。図 76 に示すように、メッシュ AP メンバ テーブルにすべての AP が表示されているのを確認します。

図 76: メッシュ AP メンバテーブル

Mesh Profile Mesh AP Table Mesh Topology											
<input type="checkbox"/>	Mesh Name	AP ID	AP Name	AP Mac Address	Available State	Parent AP ID	Parent AP Mac Address	Uplink Interface Index	Uplink Channel	Downlink Interface Index	Downlink Channel
<input type="checkbox"/>	Mesh832	149	AP-149	00:0c:e5:11:25:cd	Online	0	00:00:00:00:00:00	0	0	2	157
<input type="checkbox"/>	Mesh832	124	AP-124	00:0c:e5:13:04:8f	Offline	0	00:00:00:00:00:00	0	0	0	0
<input type="checkbox"/>	Mesh832	141	AP-141	00:0c:e5:11:25:1b	Online	130	00:0c:e5:13:14:9b	2	157	2	157
<input type="checkbox"/>	Mesh832	132	Sudhodesh-AP822	00:0c:e5:14:7f:19	Offline	0	00:00:00:00:00:00	0	0	0	0
<input type="checkbox"/>	Mesh832	139	.join	00:0c:e5:11:25:a5	Offline	0	00:00:00:00:00:00	0	0	0	0
<input type="checkbox"/>	Mesh832	130	AP-130	00:0c:e5:13:14:9b	Online	149	00:0c:e5:11:25:cd	2	157	2	157
<input type="checkbox"/>	Mesh832	125	AP-125	00:0c:e5:11:25:8f	Offline	0	00:00:00:00:00:00	0	0	0	0
<input type="checkbox"/>	Mesh832	125	AP-125	00:0c:e5:14:7f:3f	Offline	0	00:00:00:00:00:00	0	0	0	0

フェーズ 5: ケーブルを外して AP を配備する

フェーズ 5 では、ケーブルを外し、AP を最終設置場所に配置し、オンにします。そうすることで、コントローラが AP をワイヤレス AP として認識します。

AP を配備するには、以下の手順に従ってください。

1. 各 AP に電源が用意されていることを確認し、PoE を使用する場合は、メッシュ ノードの電源アダプタを用意してからアクティブにします。
2. AP を外し、最終設置場所に置きます。
3. AP の電源を順番にオンにします (ゲートウェイ AP の電源を最初にオンにしてから、ゲートウェイに直接接続するメッシュ ノードの電源をオンにするなど)。次の AP の電源をオンにする前に、前の AP がオンラインになったことを確認します。
4. コントローラの CLI から、copy running-config startup-config コマンドを使用して、構成を保存します。
5. クライアントの ESSID を作成し、クライアントを接続します。ping や参照などのクライアントに対して試行します。

配備が完了すると、AP が自動的に、バックホール アクセスの提供に適切な親構成を判断します。設計したとおりに AP が正しい場所に設置されれば、AP は自動的にオンラインになり、それ以上の設定は必要ありません。これで、インストールは完了です。

プラグ & プレイによるメッシュ AP の追加

448 ページの「[フェーズ 2: メッシュ プロファイルを作成する](#)」で説明したように、PlugNPlay オプションを使用すると、メッシュ ノードをワイヤレスで既存のメッシュに接続でき、コントローラに最初に直接有線で接続する必要がなくなります。この機能はデフォルトで無効になっています。

既存のメッシュで PlugNPlay が有効になっていると、メッシュ対応の AP を所定の場所に配備することで、AP が範囲内のメッシュを自動的に探し出し、AP 自身をコントローラに追加できます。これで、(本章の前述の手順に従って) メッシュサービス用に設定された AP が 1

つだけあるメッシュ プロファイルをセットアップできるようになり、メッシュ対応 AP を所定の場所にインストールできるようになります。電源がオンになると、新しい AP が以前に設定したメッシュ AP とリンクされ、コントローラの AP データベースに追加されます。



これは、新しい AP がメッシュ処理を自動的に実行するというものではありません。PlugNPlay によって、データベースに直接追加されますが、コントローラのメッシュ AP テーブルへの追加やメッシュ処理の設定がさらに必要です。PlugNPlay は単に、物理的に接続することなく、AP がコントローラと同期できるというものです。

以下の手順に従って、PlugNPlay のメカニズムを使用して新しい AP をインストールします。このシナリオでは、**448 ページの「フェーズ2: メッシュ プロファイルを作成する」と 449 ページの「フェーズ3: AP をメッシュに追加する」**に記載されている手順に従って、メッシュ プロファイルが既に作成されており、1 つ以上のアクティブなメッシュ AP が追加されていることを前提としています。

1. 新しいメッシュ対応 AP を開梱し、既存のメッシュ ノードの範囲内に設置します。
2. 電源を接続して、オンラインになるのを待ちます。コントローラに自動的に接続され、新しいファームウェアと設定のダウンロードにある程度の時間がかかります。
3. コンピュータを使用して、コントローラの Web UI にアクセスします。
4. Web ブラウザから、[Configuration] > [Wireless] > [Mesh] に移動します。
5. 既存のメッシュの隣のチェックボックスをオンにし、[Settings] をクリックします。
6. [Mesh AP Table] タブをクリックします。
7. [Add] をクリックし、新しく追加された AP をドロップダウン リストから選択します。接続されたばかりであるため、リストには最も新しい (大きい) AP ID 番号で表示されている可能性が高くなります。
8. [OK] をクリックして、新しい AP をテーブルに追加します。

これで、AP がメッシュの一部となったため、以下の手順に従って、メッシュ サービスを有効にできます。

1. [Configuration] > [Devices] > [APs] に移動します。
2. 新しいメッシュ AP の隣のチェックボックスをオンにし、[Settings] をクリックします。
3. [Wireless Interface] タブをクリックして、AP で利用できるワイヤレス インターネットを表示します。
4. いずれかのインターフェイスの隣のチェックボックスをオンにし、[Settings] をクリックします。いずれかのインターフェイスを選択できますが、現段階では、デュアル インターフェイス メッシュはサポートされていません。
5. **図 75** に示すように、[Wireless Interface Configuration - Update] 画面で、[Mesh Service Admin Status] のドロップダウン ボックスをクリックし、[Enable] を選択します。
6. [OK] をクリックして、設定の変更を保存します。

設定する必要がある新しいメッシュ ノードそれぞれに、これらの手順を繰り返します。すべてのノードを追加したら、ノードの追加が必要になるまで、メッシュの PlugNPlay を無効にすることを推奨します。

メッシュでの VLAN の設定

メッシュ AP は VLAN トランキングをサポートするようになりました。

メッシュ ネットワークで VLAN トランキングを有効にする前に、以下の推奨事項に従ってください。

- セカンダリ冗長性ネットワークはサポートされていないため、メッシュ再検出を使用して冗長性を持たせます。
- VLAN メッシュにおけるゲートウェイ AP では、プロファイルに VLAN タグが含まれている場合、トンネル モードで ESS とポート プロファイルを使用する必要があります。

VLAN トランクの有効化

CLI の使用

```
controller(15)# configure terminal
controller(15)(config)# port-profile vlantrunk
controller(15)(config-port-profile)# enable
controller(15)(config-port-profile)# vlantrunk enable
controller(15)(config-port-profile)# multicast-enable
controller(15)(config-port-profile)# end
controller(15)(config)# mesh vlantest
controller(15)(config-mesh)# admin-mode enable
controller(15)(config-mesh)# psk key 12345678
controller(15)(config-mesh)# meshvlantrunk enable
controller(15)(config-mesh)# end
controller(15)#
controller(15)# sh mesh-profile
```

Name	Description	Admin Mode	PlugNPlay Status	VLAN Trunking
St				

vlantrunk	enable	disable	enable
testvlan	enable	disable	enable
vlantest	enable	disable	enable

Mesh Configuration(3)

```

controller(15)# configure terminal
controller(15)(config)# mesh-profile vlantest
controller(15)(config-mesh)# mesh-ap 65
controller(15)(config-mesh-mesh-ap)# end
controller(15)#
controller(15)# sh port-profile

```

Profile Name		Enable/Disable	VlanTrunk	Dataplane Mode
VLAN Name	Security Profile	Allow Multicast	IPv6 Bridging	
default		enable		bridged
on	off		enable	
vlantrunk		enable		bridged
off	off		enable	

Port Table(2)

Enterprise Mesh のトラブルシューティング

メッシュ トポロジの表示

Web UI の Mesh Topology ビューで、現在のメッシュ環境を迅速に評価できます。アクセスするには、[Configuration] > [Wireless] > [Mesh] > (メッシュを選択) > [Mesh Topology] に移動します。

[Mesh Topology] タブで、表示されているメッシュ ノードをクリックして、ツリーを展開し、ノード間の接続を確認できます。

問題と解決方法の対応表

問題	考えられる原因と解決方法
指定した親 AP にワイヤレス AP が接続されない。	ワイヤレスまたはゲートウェイ AP で、ESSID ごとのブリッジが有効になっていないことを確認してください。
AP が、作成した構成とは異なるものを取得してしまう。	AP が、以前に使用していた AP の古い構成を取得している可能性があります。CLI コマンド reload ap id default (for one AP) または reload all default で、すべての AP を出荷時のデフォルトにリセットしてみてください。その後に、 447 ページの「Enterprise Mesh システムのインストールと設定」 に記載されているセットアップの指示に従ってください。
AP がリブートする。	チャネルの状態が悪い可能性があります。ワイヤレス スニファを使用して、バックホール チャネルの状態を確認してください。

17 SNMP の設定

SNMP エージェントを使用するとネットワーク管理者は、統計情報を収集して異常なイベントをトラップにより通知することで、パフォーマンス管理および障害管理の機能を利用できるようになります。

ここに記載する情報は、すべてのコントローラ モデルと以下の AP シリーズに適用されます。

- AP400
- AP1000

ワイヤレス LAN システムの SNMP エージェントは、HP OpenView のような他社のネットワーク管理システム (Network Management System : NMS) と連携して、アラームやトラップの情報を、設定済みの管理ステーションに渡すことができます。

フォーティネット FortiWLC (SD) は、SNMP プロトコルの複数のバージョンをサポートしています。フォーティネット ソフトウェアでは、インターネット標準管理フレームワークのすべてのバージョン (SNMPv1、SNMPv2c、および SNMPv3) が同じ基本構造とコンポーネントを共有します。さらに、インターネット標準管理フレームワークのすべてのバージョンの仕様で、同じアーキテクチャを採用しています。

番号	機能	RFC
1	SNMPv1	RFC-1155、RFC-1157
2	SNMPv2c	RFC-1901、RFC-1905、RFC-1906
3	SNMPv3	RFC-1905、RFC-1906、RFC-2571、RFC-2574、RFC-2575
4	MIB-II	RFC-1213
5	Fortinet Private MIB	フォーティネット ワイヤレス LAN 独自 MIB

フォーティネット FortiWLC (SD) は、SNMP による書き込み処理をサポートしていません。CLI または Web UI を使用して、必要な設定をプロビジョンする必要があります。

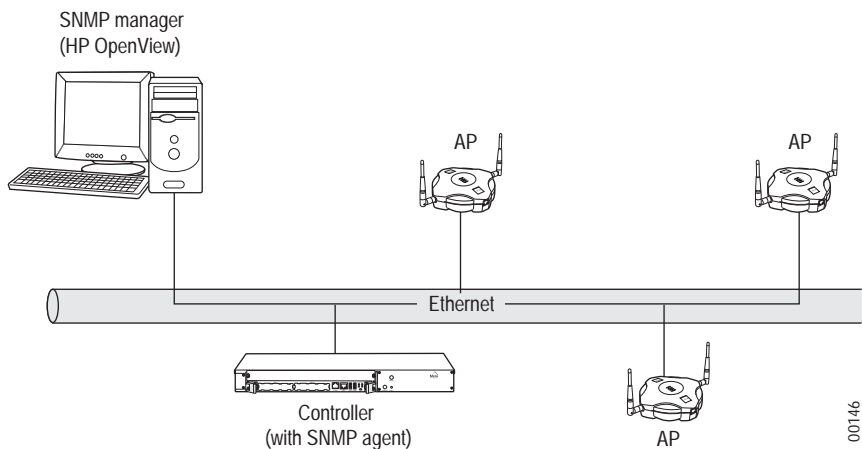
機能

以下のプロトコルについて、読み取り機能のみをサポートしています (書き込みはサポートされていません)。

- RFC-1214
- SNMPv1/v2c/v3
- フォーティネット WLAN システム

SNMP アーキテクチャ

図 77: SNMP ネットワーク管理アーキテクチャ



ワイヤレス LAN システムの SNMP ネットワーク管理アーキテクチャは、図に示したようなクライアント / サーバアーキテクチャを採用しています。管理対象ネットワークの SNMP モデルは、以下の要素で構成されます。

- 1 つ以上の管理対象ノード。上の図では、コントローラも SNMP ベースの管理対象ネットワークの中の管理対象ノードの 1 つです。SNMP エージェントは、管理対象ノードに置かれていて、アクセス ポイントからの統計を収集し、結合してから、MIB 変数を介して SNMP マネージャに送ります。SNMP 経由で設定された設定情報も、SNMP エージェントによってアクセス ポイントに伝播されます。
- 管理アプリケーションがインストールされている 1 台以上の管理ステーション。
- 設定、状態、統計、および管理対象ノードのアクションの制御が記述されている、各管理対象ノードの管理情報。

- マネージャとエージェントが管理メッセージの交換に使用する、管理プロトコル。SNMP 管理対象ネットワークでは、管理プロトコルは SNMP (Simple Network Management Protocol) です。これが、マネージャとエージェントの間でやり取りされるメッセージのフォーマットと意味を定義します。フォーティネット ワイヤレス LAN システムでは、trap、get、および MIB walk の各関数のみに対するサポートを提供しています。

読み取りと書き込みのどちらの特権も、SNMP マネージャに対してコミュニティ文字列へのアクセスを与えるものではありません。コントローラの読み取りおよび読み取り / 書き込みのコミュニティ文字列の数の制限はありません。

MIB テーブル

ワイヤレス LAN システムの SNMP 実装によりサポートされる MIB テーブルは、コントローラからダウンロードでき、外部にコピーできます。MIB テーブルはフォーティネットの Web サイトからも入手できます。ワイヤレス LAN システムの MIB Enterprise テーブルのサマリは以下のとおりです。

mwstatistics.1	mwTop10ApStationProblemTable.1
mwGlobalStatistics.1 *	mwTop10ApStationProblemEntry.1
mwIf80211StatsTable.1	mwTop10Statistics.2
mwGlobalStatistics.2 *	mwTop10ApStationRxtxTable.1
mwIfStatsTable.1	mwTop10ApStationRxtxEntry.1
mwIfStatsEntry.1	mwTop10Statistics.3
mwGlobalStatistics.6 *	mwTop10ApProblemTable.1
mwStationStatsTable.1	mwTop10ApProblemEntry.1
mwStationStatsEntry.1	mwGlobalStatistics.4
mwGlobalStatistics.7 *	mwTop10ApRxtxTable.1
mwApStationStatsTable.1	mwTop10ApRxtxEntry.1
mwApStationStatsEntry.1	mwStatistics.1
mwGlobalStatistics.8 *	mwPhoneTable.1
mwCacApStatsTable.1	mwPhoneEntry.1
mwCacApStatsEntry.1	mwStatistics.2
mwGlobalStatistics.9 *	mwPhoneCallTable.1
mwCacBssStatsTable.1	mwPhoneCallEntry.1
mwCacBssStatsEntry.1	mwStatistics.3
mwStatistics.2 *	mwStatusTable.1
mwTop10Statistics.1	mwStatusEntry.1

FortiWLC (SD) 4.0 以降のグローバル統計は、64 ビット カウンタを使用します。

管理アプリケーションのための MIB テーブルのダウンロード

サードパーティの SNMP ベースのネットワーク管理プログラムを使用している場合、管理プログラムがコントローラと AP を管理できるようにするための フォーティネット ワイヤレス LAN システム独自の MIB テーブルを統合する必要があります。MIB テーブルは、圧縮ファイル (zip) として利用可能であり、コントローラから外部にコピーできます。

mibs.tar.gz というファイルに含まれ、images ディレクトリにある Enterprise MIB テーブルをダウンロードするには、次の CLI コマンドを使用します。

```
controller# cd image
controller# copy mibs.tar.gz off-box_location
```

Web UI を使用して Enterprise MIB テーブルをダウンロードするには、次の手順を実行します。

1. Web ブラウザ (IE または Firefox) を開き、システム IP アドレス (https://172.29.0.133 など) を入力してから、ユーザ名とパスワード (出荷時のデフォルトのユーザ名 / パスワードは admin/admin) を入力します。
2. [Configuration] > [SNMP] > [Setup] > [Download MIB Files] > [Download MIBs] をクリックします。
3. ダウンロードが完了すると、[Downloads] リストにファイルが表示されます。
4. mibs(x).tar.gz ファイルを保存します。

SNMP の設定

コントローラの SNMP エージェントは、以下のように正しく設定されている必要があります。

1. 読み取りのコミュニティ文字列が設定されていないと、Web UI を使用してコントローラのどのコンポーネントも表示できず、同様に、書き込みのコミュニティ文字列が設定されていないと更新ができません。
2. トラップを正しい SNMP マネージャに送るためには、トラップ マネージャの設定が必要です。
3. 連絡先と場所の情報を正しく設定しておく、問題が発生した場合に SNMP マネージャがそれらの情報にアクセスし、誰に連絡すればよいのかを知ることができます。

SNMP コミュニティ文字列

SNMP コミュニティ文字列は、MIB オブジェクトへのアクセスを認証します。SNMP マネージャが特定の MIB に対する読み取り / 書き込みのいずれかあるいは両方のアクセスが可能であるかどうかを決定します。SNMP マネージャがコントローラにアクセスするためには、事前にコントローラの少なくとも 1 つのコミュニティ文字列と一致するコミュニティ文字列を、同じアクセス権限で渡しておく必要があります。

コミュニティ文字列の属性は、以下のいずれかになります。

- read-only (読み取り専用)。このコミュニティ文字列の管理ステーションは、MIB の全オブジェクトを参照できますが、変更できません。
- read-write (読み取り - 書き込み)。このコミュニティ文字列の管理ステーションは、MIB の全オブジェクトに対して読み取りと書き込みのアクセスが可能です。

コミュニティ文字列の設定には、特権 EXEC モードに入って、以下の手順を実行します。

表 31: SNMP コミュニティ文字列の設定

コマンド	目的
configure terminal	グローバル設定モードに入ります。
snmp-server community string host {ro rw}	指定したホストと特権で、新しい SNMP コミュニティ文字列を作成します。ホストは、ホスト名、または 255.255.255.255 という形式の IP アドレスのどちらでも構いません。アクセス特権は、read-only (ro) または read-write (rw) のどちらかです。
end	特権 EXEC モードに戻ります。
show running-config	エントリを確認します。
copy running-config startup-config	(オプション) 設定ファイルにエントリを保存します。

トラップ マネージャ

トラップ マネージャとは、トラップを受け取って処理する管理ステーションのことです。コントローラのトラップ マネージャの数に制限はありません。トラップ マネージャは、コミュニティにグループ分けされます。1 つのコミュニティには、IP アドレスで指定された 1 つ以上のホストが所属します。

表 32: SNMP トラップ マネージャの設定

コマンド	目的
configure terminal	グローバル設定モードに入ります。
snmp-server trap community-string hostIP	トラップ メッセージの受け取りに関する、以下の情報を指定します。 community-string には、通知処理と一緒に送る文字列を指定します。 hostIP には、ホスト (宛先となる受け取り側) の名前またはアドレスを指定します。
end	特権 EXEC モードに戻ります。

表 32: SNMP トラップ マネージャの設定

コマンド	目的
show running-config	エントリを確認します。
copy running-config startup-config	(オプション) 設定ファイルにエントリを保存します。

SNMP トラップ

ワイヤレス LAN システムの重要なトラップは以下のとおりです。

番号	ケース	トラップ ID	シナリオ
1	コントローラ停止	SNMP Poll	コントローラが停止したり IP 接続が失われたりすると、SNMP マネージャが、SNMP ポーリング メカニズムによってコントローラ停止を検出します。
2	コントローラの起動	Cold Start trap	コントローラが起動すると、SNMP エージェントによって SNMP サーバの <Cold Start> トラップが生成されます。
3	NPlus1 マスタ停止	meru-wlanmib.my の mwlMasterDown	NPlus1 のマスタ コントローラが停止すると、SNMP によって MasterDown トラップが生成されます。
4	NPlus1 マスタ起動	meru-wlanmib.my の mwlMasterUp	NPlus1 のマスタ コントローラが起動すると、SNMP によって MasterUp トラップが生成されます。
5	AP 停止	meru-wlanmib.my の mwlAtsDown	AP が停止すると、SNMP によって AP_DOWN トラップが生成されます。
6	AP 起動	meru-wlanmib.my の mwlAtsUp	AP が起動すると、SNMP によって AP_UP トラップが生成されます。
7	不正 AP の検出	meru-wlanmib.my の mwlRogueApDetected	システムが不正デバイスを検出すると、SNMP によって <RogueAPDetected> トラップが生成されます。
8	不正 AP の削除	meru-wlanmib.my の mwlRogueApRemoved	システムが不正デバイスがネットワークから失くなったことを検出すると、SNMP によって <RogueAPRemoved> トラップが生成されます。

以下のリストは、ワイヤレス LAN システムに存在するすべてのトラップです。

mwlRogueApDetected	3.6 の新規 :
mwlRogueApRemoved	mwlCacLimitReached
mwlAtsDown	mwlRadarDetected
mwlAtsUp	mwlMasterDown
mwlWatchdogFailure	mwlMasterUp
mwlWatchdogUp	mwlSoftwareLicenseExpired
mwlCertificateError	mwlSoftwareLicenseInstalled
mwlCertificateInstalled	mwlTopoStaAtsAdd
mwlApSoftwareVersionMismatch	mwlAtsNeighborLoss
mwlApSoftwareVersionMatch	mwlAtsNeighborLossCleared
mwlApInitFailure	mwlHandoffFail
mwlApInitFailureCleared	mwlHandoffFailCleared
mwlApRadioCardFailure	mwlResourceThresholdExceed
mwlApRadioCardFailureCleared	mwlResourceThresholdExceedCleared
mwlAuthFailure	mwlSystemFailure
mwlRadiusServerSwitchover	mwlSystemFailureCleared
mwlRadiusServerSwitchoverFailure	mwlApBootimageVersionMismatch
mwlRadiusServerRestored	mwlApBootimageVersionMatch
mwlAcctRadiusServerSwitchover	mwlMacFilterDeny
mwlAcctRadiusServerSwitchoverFailure	mwlMacFilterDenyCleared
mwlMicFailure	mwlApTemperature
mwlMicCounterMeasureActivated	mwlApTemperatureCleared
mwlHardwareDiagnostic	
mwlHardwareDiagnosticCleared	
mwlCacLimitReached	
mwlRadarDetected	
mwlOperationalChannelChange	

SNMP/OID によってシステム ステータスを監視するオブジェクト

SNMP の get 処理を使用して、これらのオブジェクトを監視します。

番号	ケース	OID	表示される内容
1	システムのアップタイム	mwConfigController.my の mwWncVarsUpTime	システムのアップタイム
2	システム運用 ステータス	mwConfigController.my の mwWncVarsOperationalS tate	システムの現在の運用ステータス
3	システム 可用性ステータス	mwConfigController.my の mwWncVarsAvailabilityStatus	システムの現在の可用性ステータス
4	AP アップタイム	mwConfigAp.my の mwApUpTime	AP のアップタイム
5	AP 運用 ステータス	mwConfigAp.my の mwApOperationalState	AP の現在の運用ステータス
6	AP 可用性 ステータス	mwConfigAp.my の mwApAvailabilityStatus	AP の現在の可用性ステータス

エージェントの連絡先と場所を設定するコマンド

システムの説明、SNMP エージェントの連絡先と場所を設定するには、以下のコマンドを使用します。

表 33: SNMP の説明、連絡先、場所の設定

コマンド	目的
configure terminal	グローバル設定モードに入ります。
snmp-server contact text	システムの連絡先を設定します。 例 : snmp-server contact support@fortinet.com
snmp-server location text	システムの場所を設定します。 例 : snmp-server location Tower Building, IT Department
snmp-server description text	システムの説明を設定します。 例 : snmp-server description main controller

表 33: SNMP の説明、連絡先、場所の設定

コマンド	目的
end	特権 EXEC モードに戻ります。
show running-config	エントリを確認します。
copy running-config startup-config	(オプション) 設定ファイルにエントリを保存します。

CLI による FortiWLC の SNMP サービスの設定

特定の IP アドレスの SNMP サーバ コミュニティを設定するには、以下のコマンドを使用します。

```
default# configure terminal
default(config)#
default(config)# snmp-server community public 0.0.0.0 rw
default(config)# end
default# show snmp-community
SNMP Community Client IP Privilege
public 0.0.0.0 read-write
SNMP Community Management(1 entry)
default#
```

特定の IP アドレスのトラップ コミュニティを設定するには、以下のコマンドを使用します。

```
default# configure terminal
default(config)# snmp-server trap public 10.0.220.30
default(config)# end
default# show snmp-trap
Trap Community Destination IP
public 10.0.220.30
SNMP Trap Management(1 entry)
```

Web UI による FortiWLC の SNMP サービスの設定

特定の IP アドレスの SNMP サーバ コミュニティを設定するには、以下の手順を実行します。

1. Web ブラウザ (IE または Firefox) を開き、システム IP アドレス (<https://172.29.0.133> など) を入力してから、ユーザ名とパスワード (出荷時のデフォルトのユーザ名 / パスワードは admin/admin) を入力します。
2. [Configuration] > [SNMP] > [Setup] > [SNMP Community Management] > [Add] をクリックします。
3. SNMP コミュニティ名とクライアント IP アドレスを入力し、read-write などの特権レベルを選択します。

4. [OK] をクリックします。

特定の IP アドレスのトラップ コミュニティを設定するには、以下のコマンドを使用します。

5. [Configuration] > [SNMP] > [Setup] > [SNMP Trap Management] > [Add] をクリックします。
6. トラップ コミュニティとトラップ宛先 IP アドレスを入力します。
7. [OK] をクリックします。

サードパーティ ベンダのセットアップ

フォーティネット MIB ファイルをコンパイルし、SNMP マネージャにロードして、FortiWLC で使用できるようにします。SNMP マネージャにはフォーティネット MIB ファイルが必要であり、コンパイルして SNMP から フォーティネット OID にアクセスできるようにする必要があります。フォーティネット MIB をコントローラからダウンロードするには、次の手順を実行します。

1. MIB コンパイラを開きます。すべての MIB をロードしてコンパイルします。
2. Web UI から FortiWLC にアクセスします。
3. MIB ツリー ブラウザから、ios -> org -> dod -> internet -> private -> enterprise -> meru -> meru-wlan -> mwConfiguration -> mwWncVars> を展開します。
4. walk 処理をアクティブにします。これで、mwWncVars ツリーの下すべての OID を照会します。

SNMP の有効化、無効化、リロード

SNMP 設定が完了したら、以下の snmp start コマンドで有効にします。

```
controller# snmp start
```

SNMP メッセージをオフにするには、snmp stop コマンドを使用します。

```
controller# snmp stop
```

SNMP モジュールをリロードするには、reload-snmp コマンドを使用します。

```
controller# reload-snmp
```

SNMP バージョン 3 のサポート

FortiWLC (SD) 4.0 以降でサポートされている SNMPv3 アーキテクチャでは、SNMP エンティティ (マネージャ、エージェント、プロキシ フォワーダ) に新しい説明が組み込まれ、メッセージ形式と、エンティティへのアクセスの設定に使用する標準 MIB が更新されました。

FortiWLC の SNMP エージェントはマルチリンガルであり、SNMPv1/v2X に使用する snmp-community や SNMP v3 の SNMPv3-user の設定が正しければ、SNMPv1/v2c/v3 を同時にサポートします。次のような新しい機能があります。

- エンティティ共有秘密キーを使用する、ユーザ認証のセキュリティ レベル
- メッセージ タイムスタンプ
- 暗号化を使用するデータ機密
- 知る必要があるかどうかに基づく、MIB 情報へのユーザ アクセスの制御

セキュリティ レベル

SNMPv3 は、セキュリティ レベルとセキュリティ モデルの両方を提供します。セキュリティ レベルは、セキュリティ モデル内のセキュリティの許可レベルです。セキュリティ レベルとセキュリティ モデルの組み合わせで、SNMP パケットの処理時に使用するセキュリティ メカニズムが決定します (本書の「[セキュリティ レベルとセキュリティ モデルの組み合わせ](#)」を参照してください)。SNMPv3 メッセージは、次の 3 つのセキュリティ レベルのいずれかに送信できます。

- 認証なし、暗号化なし。noAuth/noPriv と呼ばれます。Priv はプライバシーのことです。このセキュリティでは、データのアクセスやトラップの送信には、有効なユーザ名だけが必要です。
- 認証あり、暗号化なし。Auth/noPriv と呼ばれます。このセキュリティでは、メッセージを受け取るためには、有効なユーザとして認証される必要があります。秘密キーを共有し、そのキーを使用して各メッセージと一緒に送信するメッセージ ハッシュ認証コードを生成することで、認証されます。
- 認証あり、暗号化あり。Auth/Priv と呼ばれます。このセキュリティでは、2 つ目の共有秘密キーを使用してユーザが認証され、データ ペイロードが暗号化されます。

セキュリティ モデル

SNMPv3 は、セキュリティ レベルとセキュリティ モデルの両方を提供します。セキュリティ モデルとは、ユーザが存在するグループをセットアップする認証戦略のことです。次の 3 つのセキュリティ モデルを使用できます。

- SNMPv1
- SNMPv2c
- SNMPv3

セキュリティ モデルとセキュリティ レベルの組み合わせで、SNMP パケットの処理時に使用するセキュリティ メカニズムが決定します (本書の「[セキュリティ レベルとセキュリティ モデルの組み合わせ](#)」を参照してください)。

セキュリティ レベルとセキュリティ モデルの組み合わせ

以下の表に、セキュリティ モデルとセキュリティ レベルの組み合わせを記載し、それぞれの組み合わせでのセキュリティを説明します。

モデル	レベル	認証	暗号化	動作
v1	noAuthNoPriv	コミュニティ文字列	なし	コミュニティ文字列を使用して認証をマッチングする。
v2c	noAuthNoPriv	コミュニティ文字列	なし	コミュニティ文字列を使用して認証をマッチングする。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名を使用して認証をマッチングする。
v3	authNoPriv	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA のアルゴリズムに基づく認証を提供する。
v3	authPriv	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA のアルゴリズムに基づく認証を提供する。CBC-DES (DES-56) 規格に基づく認証に加えて、DES 56 ビット暗号化を提供する。

SNMP バージョン 3 のコマンド

これらのコマンドの詳しい説明は、『*FortiWLC (SD) コマンド リファレンス*』に記載されています。

- snmpv3-user
- snmpv3-user auth-key
- snmpv3-user auth-protocol
- snmpv3-user priv-key
- snmpv3-user priv-protocol
- snmpv3-user target ip-address

SNMP バージョン 3 のサポートの制限事項

現段階で、フォーティネットは以下の SNMP v3 機能についてはサポートしていません。

- FortiWLC は、SNMP MIBS での書き込みアクセスをサポートしていないため、全ユーザは読み取り参照制御テーブルに属し、グループ内の読み取り参照として内部で処理されます。参照アクセス制御モデル (VACM) で、特定のグループに属しているユーザが管理エンティティに対するアクセス (読み取り、書き込み、通知) が可能であるかどうかを判断し

ます。グループ内の対応する読み取り、書き込み、または通知ビューに関連付けることで、アクセス ポリシーが定義されます。

- SNMPv3 通知: フォーティネットは、SNMPv3 trap/inform をサポートしていません。サポートしている SNMPv3 機能 (読み取りのみ)に加えて、フォーティネットのネットワーク コントローラは、既存の snmp-community テーブルを使用した SNMPv1/v2c アクセスと snmp-trap コミュニティ テーブルを使用した SNMPv1 トラップの両方を引き続き提供します。

18 トラブルシューティング

- 開始する場所
- エラー メッセージ
- システム ログ
- システム診断
- パケットの捕捉
- FTP エラー コード

開始する場所

トラブルシューティングは以下のように開始することを推奨します。

Web UI または CLI ?	問題がある場所は ?	解決策
Web UI	ステーション	[Monitor] > [Diagnostics] > [Station] をクリックして、ステーションログの履歴を表示します。
Web UI	無線	[Monitor] > [Diagnostics] > [Radio] をクリックして、無線ログの履歴を表示します。

Web UI または CLI ?	問題がある場所は？	解決策
CLI	ステーション	<p>次のいずれかのコマンドを使用してステーション ログの履歴を表示します。</p> <p>station-log show-mac=< 影響を受ける MAC アドレス ></p> <p>station-log show (MAC が不明の場合)</p> <p>この問題が再現可能または継続的に発生する場合には、ターミナルセッションを記録して、station-log インターフェイスに入り、station add <MAC> コマンドを使用して影響を受ける MAC アドレスを追加します。MAC アドレスを把握していない場合は、event all all を入力して、すべての MAC アドレスのすべてのイベントをキャプチャします。</p>
CLI	コントローラ	<p>diagnostics-controller コマンドを使用して controller-log の履歴を表示します。</p> <p>この問題が再現可能または継続的に発生する場合には、ターミナルセッションを記録して、station-log コマンドを使用して station-log インターフェイスに入り、station add <MAC> コマンドを使用して影響を受ける MAC アドレスを追加します。MAC アドレスを把握していない場合は、event all all を入力して、すべての MAC アドレスのすべてのイベントをキャプチャします。</p>

エラー メッセージ

コントローラまたは AP のいずれかで発生する可能性がある一般的なエラー メッセージを次に示します。

メッセージ テキスト	説明
[07/20 13:02:11.122] 1m[35m**Warning**[0m WMAC: Wif(0):SetTsf() TSF[00000000:000006e3] -> [00000033:77491cfd]thr[0000 0000:03938700]	<p>完全な診断を実行した後に AP コマンド ラインまたは AP のトレース ログ出力に表示される場合があります。</p> <p>SetTsf() メッセージは、AP が TSF (TSF は、時間同期機能であり、AP のクロックです) を、特定のしきい値 (しきい値は 5 秒) 以上調整した (進めた) ことを示しています。上記の特定ケースは、AP が起動したばかりであり、TSF の値を近接の AP の TSF 値に合わせて調整しています。</p> <p>現在の TSF が低い値であるため (つまり、6e3 マイクロ秒)、AP が起動したばかりであることが分かります。初期化中に、近隣の AP がこの AP と同じように BSSID をサポートしている場合には、AP は自分の TSF を近隣の TSF と同期化します。これは、仮想セルをサポートするための要件です。</p>
[07/31 14:01:33.506] *****ERROR***** QOS: FlowMgr failed while processing flow request, reason= 5, srcMac[00:23:33:41:ed:27], dstMac[00:00:00:00:00:00].	<p>コントローラの CLI インターフェイスで表示される場合があります。</p> <p>通話を開始したステーションで AP フローをセットアップまたは削除しようとすると、このエラーが発生します。"reason=5" は、フローのセットアップや削除が試行された AP にこのステーションが割り当てられていないことを意味します。</p> <p>推測される影響として、MAC アドレスの代わりに QoS フローが確立されないため、ステーション (おそらく電話) の通話品質が通常よりも低くなることが考えられます。</p>
Received non-local pkt on AP!	<p>このメッセージは、コントローラのシリアル コンソールまたはコントローラの診断に含まれる dmesg.txt 出力に表示される場合があります。このメッセージは、イーサネット タイプ 0x4001 または UDP ポート 5000 パケット (それぞれ L2 および L3 COMM) がコントローラのイーサネットから受信されたが、実際にはコントローラの MAC または IP アドレスに向けたものではなかったことを示しています。</p>

システム ログ

システム ログは、以下の情報を記録します。

- 設定変更 (CLI または GUI)
- 主要なコマンド
- イベントと操作
- エラー

CLI コマンド show log を使用すると、ログ全体を表示できます。Web UI から システム ログ ファイルを表示するには、[Maintenance] > [Syslog] > [View Syslog Files] をクリックします。

図 78: Syslog ファイル テーブル

Facility Name	Last Accessed	Size (KB)	#Lines	Last Record
Security	08/04/2010 13:26:59	27	16	Controller Access User admin@192.168.105.78 login to controller at time Wed Aug 4 10:14:43 2010 is OK
QoS	07/30/2010 17:06:33	1	0	
System WNC	08/04/2010 14:22:42	421	1995	ROGUE AP REMOVED. CONTROLLER (1:20040) ROGUE AP DETECTED. Station mac=00:1c:f0:f9:02:8f bss=00:12:cf:4f:b1:fc cch= 0 ess=
NMS	08/04/2010 10:27:44	7	55	[MODIFY:Administrative User Management]
Mobility	07/30/2010 17:06:33	1	0	
Bulk Update	07/30/2010 17:06:33	1	0	
Upgrade	07/30/2010 17:05:28	2	16	Upgrade complete Meru rpms installed:
Per User Firewall	07/30/2010 17:06:33	1	0	

[Facility Name] には、次の 8 つの情報ソースのいずれかが表示されます。

ファシリティ	メッセージの内容
Security	ユーザ ログインおよびキャプティブ ポータル アクティビティを含むセキュリティ設定の作成と違反
QoS	このコントローラで作成された Quality of Service ルールの作成と違反の両方に関する QoS メッセージ
System WNC	不正 AP syslog メッセージ
NMS	Network Manager Server の syslog メッセージ
Mobility	ハンドオフまたはリダイレクト メッセージ

ファシリティ	メッセージの内容
Bulk Update	GUI から利用可能な一括アップデート (Bulk Update) コマンドの使用が、ここに記録されます。[AP Configuration]、[Wireless Interfaces Configuration]、[Antenna Property] ページからアクセスする一括アップデート (Bulk Update) 機能によって、選択した AP グループが更新されます。これらの各領域で一括アップデートは同じように動作しますが、更新される項目は、一括アップデートが開始されたページによって異なります。
Upgrade	CLI コマンド upgrade の使用
Per-user Firewall	ユーザごとのファイアウォールの作成と違反

上記のチャートにある Facility のいずれかを選択してから [View Syslog] をクリックして、これらの詳細を表示します。

図 79: セキュリティ システム ログの詳細

Syslog facility: Security (16 entries)				
Line	Priority	Mnemonic	Time	Record
6	info	WAU	07/30/2010 17:13:21	Controller Access User admin@192.168.106.99 login to controller at time Fri Jul 30 17:13:21 2010 is OK
10	info	WAU	07/30/2010 17:13:43	Controller Access User admin@192.168.105.78 login to controller at time Fri Jul 30 17:13:43 2010 is OK
11	info	WAU	07/30/2010 17:13:58	Controller Access User admin@192.168.105.78 login to controller at time Fri Jul 30 17:13:58 2010 is OK
12	info	WAU	07/30/2010 17:14:01	Controller Access User admin@192.168.102.108 login to controller at time Fri Jul 30 17:14:01 2010 is OK
13	info	WAU	07/30/2010 17:14:04	Controller Access User admin@192.168.102.108 login to controller at time Fri Jul 30 17:14:04 2010 is OK
74	info	WAU	08/02/2010 09:09:48	Controller Access User admin@172.26.0.52 login to controller at time Mon Aug 2 09:09:48 2010 is OK
126	info	WAU	08/02/2010 17:04:56	Controller Access User admin@192.168.157.105 login to controller at time Mon Aug 2 17:04:56 2010 is FAILED
127	info	WAU	08/02/2010 17:04:58	Controller Access User admin@192.168.157.105 login to controller at time Mon Aug 2 17:04:58 2010 is OK
180	info	WAU	08/03/2010 01:03:04	Controller Access User admin@192.168.102.108 login to controller at time Tue Aug 3 01:03:04 2010 is OK

エントリ	意味
Line	エントリがある syslog ファイルの行番号
Priority	エントリの重大度。優先度として、debug、info、notice、warning、error、err、crit、alert、emerg、panic があります。
Mnemonic	エントリに割り当てられる 3 文字のニーモニック。 CAP = キャプティブ ポータル RED = リダイレクト FOR = 転送 WAU = WebAuth ユーザ認証 WST = Web サーバ イベント WPW = Web UI ユーザ パスワード管理
Time	エントリが記録された日時
Record	syslog イベントの詳細、メッセージのカテゴリによって異なります。 Security: ユーザ ログイン、キャプティブ ポータルのアクティビティ QoS: QoS ルールの作成と違反 System WNC: 不正なアクティビティ NMS: このコントローラが Network Manager の一部である場合、Network Manager Server によって開始されたすべてのアクティビティ Mobility: これは主に RED (リダイレクト) メッセージで構成される Bulk Update: グループで完了した AP アップデート Upgrade: FortiWLC (SD) のアップグレード Per-User Firewall: ファイアウォールの作成と違反

図 79 の 1 つのように [Facility] 画面の列の情報を検索するには、次の操作を実行します。列の上部にあるボックス ([Line]、[Priority]、[Mnemonic]、[Time]、[Record]) に、検索データを入力してメッセージをフィルタします。フィルタにヒットするメッセージだけが表示されます。[Priority] については、選択した優先度レベル以上のメッセージが表示されます。たとえば、debug を検索すると、debug は最も低い優先度レベルであるため、すべてのメッセージが表示されます。info を検索すると、info 以上のメッセージである、notice、warning、error、err、crit、alert emerg、panic (最も高い優先度) が表示されます。

[Time] 列の上にあるカレンダー アイコンをクリックして、特定の日または時刻を入力して、このカテゴリの syslog メッセージをフィルタできます。

ステーション ログ イベント

ステーション ログ イベント メッセージは、次の形式で表示されます。

[object name, field name <old value: new value>, field name <old value: new value> ...]"

Log Category : "nms", Priority : 'info', Mnemonic : "CONFIG"

次の表は、一般的なステーション ログ イベントについて説明しています。

イベント	イベントが発生させた状況	説明
00:0f:8f:9d:d3:23 Station Assign <AID=1> assigned to <AP_ID=31><ESSID=swhan- essid><BSSID=00:0c:e6:9d:4f:be >	モバイル ステーションが AP::ESSID::BSSID に割り当て られました。	モバイル ステーションが BSSID に 割 り当てられています。モバイル ステ ーションが AP::ESSID::BSSID に割り当 てられると、モバイルは次のステー ジである 802.11 認証とアソシエーシ ョンに進みます。802.11 認証とアソシ エーションに進むと、AID 値がステー ションに割り当てられます。
00:0f:8f:9d:d3:23 Station Assign <AID=1> Assign Removed From <AP_ID=31><ESSID=swhan- essid><BSSID=00:0c:e6:9d:4f:be >	モバイル ステーションの割り当て 状態が AP::ESSID::BSSID から削 除されました。	モバイル ステーションは、次のステー ジである割り当てに進むことができま せん。最もよくある原因は、モバイル ステーションが、ステーションの割り 当て時間内に 802.11 認証またはアソ シエーションに進むことができなかった ことです。
00:16:6f:3b:17:a9 IP Address Discovered <Old IP discovery Method=none><Old IP=0.0.0.0<New IP discovery Method=dynamic><New IP=10.101.66.25>	モバイル ステーションの検出方法 または IP アドレスが変更され、 システムが新しい IP アドレスを 受け入れました。	新しい IP フィールドには、ステー ションによって使用されている IP ア ドレスが示されます。

イベント	イベントを発生させた状況	説明
00:16:6f:3b:17:a9 IP Address Discovered <IP = 10.101.64.100> fails due to one of local IPs	モバイルステーションは、検出され、コントローラの IP アドレスを使用しようとしています。	システムは、この IP アドレスを使用するステーションの IP トラフィックをブロックします。
00:16:6f:3b:17:a9 IP Address Discovered ip update not performed.<Client IP=10.101.64.1> is used by a wired station <00:0e:84:85:33:00>	モバイルステーションは、検出され、MAC アドレスが表示されている有線ステーションによって使用されている IP アドレスを使用しています。	システムは、この IP アドレスを使用するステーションの IP トラフィックをブロックします。

Syslog メッセージ	説明
AP DOWN CLEAR Access Point <ap-id> is up	アクセス ポイント ap-id が WLAN に追加されました。 カバレッジが拡大します。 対策：なし
AP DOWN CRITICAL Access Point <ap-id> is down	アクセス ポイント ap-id が WLAN から削除されました。 サービス対象外となるエリアができることが予想されます。 対策：このイベントが予想外のものであった場合は、アクセス ポイントとコントローラ間のネットワーク接続を確認してください。
AP rebooted by admin	アクセス ポイントが手動でリブートされました。 対策：なし
AP Software Version Mismatch	AP 上のソフトウェア バージョンがコントローラ上のものと一致しません。このメッセージが生成されるのは、自動 AP アップグレード機能が無効になっている場合だけです。 対策：この状態を解決するには、upgrade ap コマンドを使用して手動で AP をアップグレードし、動作が継続していることを確認する必要があります。
CAP <user>@<a.b.c.d> logged in <OK FAILED>	指定されたキャプティブ ポータルのユーザのログインが成功 (OK) したか、ログインが拒否されました (FAILED)。

Syslog メッセージ	説明
Controller rebooted by admin	コントローラが手動でリブートされました。
AP Boot Image Version Mismatch	AP 上のブート イメージのバージョンが、AP ソフトウェアのバージョンに必要となるものと一致しません。 対策：AP ソフトウェアのバージョンをアップグレードする前に、ブート イメージのオプション付きの upgrade ap コマンドを使用して、ブート イメージをアップグレードする必要があります。
AP Initialization Failure	AP を正しく初期化できませんでした。 対策：AP ネットワーク ケーブルが正しく接続されているかどうかをチェックします。AP のブート イメージのバージョンが AP ソフトウェアのバージョンと一致しているか、また、AP ソフトウェアのバージョンがコントローラのソフトウェア バージョンと一致しているかどうかをチェックします。これらをチェックした後も AP の初期化が失敗する場合は、フォーティネット カスタマ サポートに連絡してください。
AP Temperature	AP の温度が最大しきい値を超えています。
Hardware Diagnostic	AP のハードウェア診断チェックが失敗しました。 対策：フォーティネット カスタマ サポートに連絡してください。
ROGUE AP DETECTED CLEAR STATION mac=<mac-address> bss=<bssid> ch=<channel-id> reported by AP <ap-id>	前に不正として報告されたステーションが、どのアクセス ポイントからも検出されなくなりました。
ROGUE AP DETECTED CRITICAL STATION mac=<mac-address> bss=<bssid> ch=<channel-id> reported by AP <ap-id>	未知の BSSID を使用しているステーションが検出されました。 対策：bssid が他の有効な WLAN に属していないかどうかを調べてください。属していなければ、不正 AP 緩和機能をオフにすることも考えられます。
Radio Card Failure	AP 無線カードの障害。 フォーティネット カスタマ サポートに連絡してください。

Syslog メッセージ	説明
WLAN services started on controller	コントローラ上で FortiWLC (SD) プロセスが開始しました。
WLAN services stopped on controller	FortiWLC (SD) プロセスが停止しました。
WST:WS Serving...	Web サーバの新しいイベント メッセージ。
WPW :<user>@<a.b.c.d> changed password <OK FAILED>	指定された FortiWLC (SD) ユーザのパスワード変更が成功 (OK) または失敗 (FAILED) しました。

MAC フィルタリング ステーション ログ イベント

MAC フィルタリング ログ イベントでは、7 つのイベントが定義されています。

イベント	イベントが発生させた状況	説明
00:66:77:c2:03:01 Mac Filtering Mac in permit list - accept client	ステーション、00:66:77:c2:03:01 は、「ACL Allow Access List」にあり、「Permit List Enabled」がオンになっています。	モバイル ステーションは、次のステージまたは割り当てに進みます。
00:66:77:c2:04:01 Mac Filtering Mac not in permit list - reject client	ステーション、00:66:77:c2:04:01 は、「ACL Allow Access List」になく、「Permit List Enabled」がオンになっています。Radius 認証は、無効になっています。	モバイル ステーションは、次のステージまたは割り当てに進むことができません。
00:66:77:c2:03:01 Mac Filtering Mac not in deny list - accept client	ステーション、00:66:77:c2:03:01 は、「ACL Deny Access List」になく、「Deny List Enabled」がオンになっています。Radius 認証は、無効になっています。	モバイル ステーションは、次のステージまたは割り当てに進みます。
00:66:77:c2:04:01 Mac Filtering Mac in deny list - reject client	ステーション、00:66:77:c2:04:01 は、「ACL Deny Access List」にあり、「Deny List Enabled」がオンになっています。Radius 認証は、無効になっています。	モバイル ステーションは、次のステージまたは割り当てに進むことができません。
00:66:77:c2:03:01 Mac Filtering Sent RADIUS request	Radius 認証が有効であり、Radius 認証要求が送信されています。	Radius 要求メッセージが認証に送信されました。

イベント	イベントが発生させた状況	説明
00:66:77:c2:02:01 Mac Filtering RADIUS authentication succeeded (vlan 0)	Radius 認証が有効であり、Radius 受け入れ応答メッセージが受信されました。	モバイル ステーションは、次のステージまたは割り当てに進みます。
00:66:77:c2:02:06 Mac Filtering RADIUS authentication failed	Radius 認証が有効であり、Radius 拒否応答メッセージが受信されました。	モバイル ステーションは、次のステージまたは割り当てに進むことができません。

キー交換ステーション ログ イベント

キー交換は、暗号キーがユーザ間で交換されるセキュアな方法です。WPA、WPA2、WPA PSK、WPA2 PSK、MIXED または MIXED_PSK のいずれかが有効である場合、ステーションはこの接続ステージを通過します。

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 1X Authentication M1 <msg type=EAPOL_KEY> PTK sent	システムは、最初のキー交換メッセージを送信します。	これは、WPA、WPA2、WPA PSK、WPA2 PSK、MIXED または MIXED_PSK で共通です。システムは、4 回送信を試行します。そして、802.11 認証解除を送信して M2 メッセージを受信しない場合、キー交換処理を中止します。
M2 <pkt type=EAPOL_KEY> MIC Verified	システムは、キー交換メッセージ、M2 をステーションから受信し、MIC が正しく検証されました。	これは、WPA、WPA2、WPA PSK、WPA2 PSK、MIXED または MIXED_PSK で共通です。
00:16:6f:3b:17:a9 1X Authentication M3 <msg type=EAPOL_KEY> WPA PTK Negotiation sent	システムは、WPA または WPA-PSK モードの第 3 キー交換メッセージを送信します。	システムは、4 回送信を試行します。そして、802.11 認証解除を送信して M2 メッセージを受信しない場合、キー交換処理を中止します。
00:16:6f:3b:17:a9 1X Authentication M4 <pkt type=EAPOL_KEY> <key type=Unicast Key> Key Pairwise	システムは、WPA または WPA-PSK モードの第 4 キー交換メッセージをステーションから受け取ります。	システムは、4 回送信を試行します。そして、802.11 認証解除を送信して M2 メッセージを受信しない場合、キー交換処理を中止します。

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 1X Authentication M5 <msg type=EAPOL_KEY> WPA GTK Rekey Negotiation sent	システムは、WPA または WPA-PSK モードの第 5 キー交換メッセージを送信します。	
00:16:6f:3b:17:a9 1X Authentication M6 <pkt type=EAPOL_KEY> <key type=Group Key>	システムは、WPA または WPA-PSK モードの第 6 キー交換メッセージをステーションから受け取ります。	これは、WPA または WPA-PSK のキー交換の最後のメッセージです。これはキー交換が成功したことを示します。ステーションは次のステージに進むことができます。
00:16:6f:3b:17:a9 1X Authentication M3 <msg type=EAPOL_KEY> WPA2 PTK Negotiation sent	システムは、WPA2 または WPA2-PSK モードの第 3 キー交換メッセージを送信します。	システムは、4 回送信を試行します。そして、802.11 認証解除を送信して M2 メッセージを受信しない場合、キー交換処理を中止します。
00:16:6f:3b:17:a9 1X Authentication M4 <pkt type=EAPOL_KEY> <key type=Unicast Key> Key Pairwise	システムは、WPA2 または WPA2-PSK モードの第 4 キー交換メッセージをステーションから受け取ります。	これは、WPA2 または WPA2-PSK のキー交換の最後のメッセージです。これはキー交換が成功したことを示します。ステーションは次のステージに進むことができます。
00:16:6f:3b:17:a9 1X Authentication Sending Station Disconnect, Reason : MIC Failure, Auth Type 802.1X	ステーションから送信されたメッセージが、MIC のエラーになりました。	WPA-PSK または WPA2-PSK では、不正なパスフレーズやパスワードによって、このエラーが発生します。MIC エラーが発生すると、システムは 802.11 認証解除をステーションに送信します。
00:16:6f:3b:17:a9 1X Authentication Sending Station Disconnect, Reason : 4-way Handshake Timeout, Auth Type 802.1X	クライアントからの応答がないため、キー交換を中止しました。	システムは 1 秒間隔で 6 回キー交換メッセージを送信しようとします。ステーションが応答しない場合、キー交換を中止します。

認証ステーション ログ イベント

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 802.11 State state change <old=Unauthenticated><new=Aut henticated><AP=00:0c:e6:04:fc:a d><BSSID=00:0c:e6:0a:ca:6e>	ステーションが 802.11 認証フェーズを AP::BSSID で正しく完了しました。	
00:16:6f:3b:17:a9 802.11 State state change <old=Unauthenticated><new=Aut henticated><AP=00:0c:e6:04:fc:a d><BSSID=00:0c:e6:0a:ca:6e>	ステーションが 802.11 アソシエーション フェーズを AP::BSSID で正しく完了しました。	

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 802.11 State state change <old=Associated><new=Unauthenticated><AP=00:0c:e6:04:fc:c0> <BSSID=00:0c:e6:d8:84:14>	ステーションの 802.11 のステータスが、Associated から Unauthenticated に変更しました。	<p>次の理由で、Associated から Unauthenticated にステータスが変更します。</p> <p>ステーションがタイムアウトしました。デフォルトのタイムアウト期間は、30 分です。802.11 が設定されたステーションのタイムアウト期間が、割り当てられたステーションのタイムアウト期間と異なります。</p> <p>ステーションは、802.11 認証解除フレームを送信し、関連付けられている BSSID から自発的に離れました。</p> <p>ステーションは、BSSIDOLD から BSSIDNEW に移動しました。BSSIDOLD のアソシエーションのステータスは、自動的にクリアされません。</p> <p>マルチコントローラ環境では、ステーションは ControllerOLD から ControllerNEW に移動し、2 台のコントローラが同じサブネットに存在します。ControllerOLD のアソシエーションステータスは、自動的にクリアされます。</p> <p>Radius 拒否、メッセージ タイムアウト、または不明な理由のために、1x/WPA/WPA2 認証が失敗しました。</p> <p>タイムアウトまたは MIC エラーのために、キー交換が失敗しました。</p>

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 802.11 State <AID=1> handoff <OLD_AP_ID=3><NEW_AP_ID=4><BSSID=00:0c:e6:30:47:17>	ステーションが AP 間で切り替わりました (ハンドオフ)。	仮想セルまたは仮想ポートの ESS にモバイルステーションが関連付けられている場合にのみ、このイベントが生成されます。略語の意味は以下のとおりです。 AID: アソシエーション ID OLD_AP_ID: ハンドオフ前にステーションを利用していた AP NEW_AP_ID: ハンドオフ後にステーションを利用していた AP BSSID: 仮想セルまたは仮想ポートの親 BSSID
00:16:6f:3b:17:a9 802.11 State Received Deauth frame from station <Deauth reason: authentication leave><deauth packet RSSI = 62><AID=3><BSSID=00:0c:e6:f9:01:01>	ステーションが 802.11 認証解除フレームを送信しました。	ステーションは、ESS/BSS から離れることを決定しました。これは、AP400 でのみサポートされます。
00:16:6f:3b:17:a9 802.11 State Received Disassoc frame from station <Disassoc reason: association leave><deauth packet RSSI = 57><AID=3><BSSID=00:0c:e6:f9:01:01>	ステーションが 802.11 アソシエーション解除フレームを送信しました。	ステーションがアソシエーションを解除することを決定しました。これは、AP400 でのみサポートされます。

1X/WPA/WPA2 認証ステーション ログ イベント

DHCP ステーション ログ イベント

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 1X Authentication <auth method=WPA2_EAP>:<pkt type=EAPOL_START> recvd <ESSID=vcellwpa2> <BSSID=22:01:0f:3b:17:a9>	システムが、ESSID::BSSID ペアに関連付けられているステーションから EAPOL_START メッセージを受信しました。	2 つの認証方法 WAP2_EAP または WPA_EAP があります。この標準は、メッセージがオプションであるとしています。
00:16:6f:3b:17:a9 1X Authentication <EAP code=request> <EAP ID=1> <EAP type=Identity> sent	システムが、EAP アイデンティティ要求をステーションに送信しました。	システムは、1 秒間隔で最大 4 回このメッセージを試行しました。認証が進むと、EAP ID が 1 つ増えます。
00:16:6f:3b:17:a9 1X Authentication <pkt type=EAP_PACKET> <EAP code=response><EAP ID=1>	システムは、ステーションから EAP 応答メッセージを受信しました。	応答の EAP ID は、要求の EAP ID と一致する必要があります。
00:16:6f:3b:17:a9 1X Authentication RADIUS <msg code=access_request><msg ID=178> sent <ip=192.168.101.17>:<port=1812>	システムは、ステーションの要求を Radius サーバ IP:: ポートに転送しました。	認証が進むと、メッセージ ID が 1 つ増えます。
00:16:6f:3b:17:a9 1X Authentication <pkt type=EAP_PACKET> <EAP code=request><EAP ID=2> <info=relay eap-request from RADIUS> sent	システムが、Radius サーバの要求をステーションに転送しました。	
00:16:6f:3b:17:a9 1X Authentication <pkt type=EAP_PACKET> <EAP code=success><EAP ID=13> <info=relay eap-request from RADIUS> sent	システムが Radius Accept メッセージを受信し、EAP SUCCESS メッセージをモバイルに送信しました。	これは、認証の最後のメッセージです。WAP または WAP2 が使用されている場合、キー交換のステージが直ぐに続きます。
00:16:6f:3b:17:a9 1X Authentication Backend Authentication Timeout	Radius サーバに送信されたメッセージがタイムアウトしました。	

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 1X Authentication Sending EAP Failure to station, (identifier 1)	EAP エラー メッセージがステーションに送信されました。	このイベントが発生するケースは以下の 3 つです。 Radius メッセージがタイムアウトする。 ステーションへの EAP メッセージがタイムアウトする。 Radius サーバが拒否メッセージを送信する。
00:16:6f:3b:17:a9 1X Authentication RADIUS Access-Reject received	システムが、Radius サーバから Radius Reject メッセージを受信しました。	
00:16:6f:3b:17:a9 1X Authentication Backend Authentication Failure	システムが、Radius サーバから Radius Reject メッセージを受信しました。	

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 DHCP <msg_type=DISCOVER><server_ip=255.255.255.255><server_mac=ff:ff:ff:ff:ff:ff><client_ip=0.0.0.0	システムは、ステーションから DHCP メッセージを受信しました。	メッセージには、サーバの IP および MAC、およびクライアント IP が表示されます。 表示される DHCP メッセージ タイプは、DISCOVER、REQUEST、または RELEASE です。
00:16:6f:3b:17:a9 DHCP <msg_type=OFFER><server_ip=10.101.64.1><server_mac=00:0e:84:85:33:00><offered_ip=10.101.66.25>	システムは、DHCP サーバから DHCP メッセージを受信しました。	メッセージには、サーバの IP および MAC、およびクライアントの IP が表示されます。 表示される DHCP メッセージ タイプは、OFFER、ACK、NACK または INFORM です。

キャプティブ ポータル ステーション ログ イベント

イベント	イベントが発生させた状況	説明
00:16:6f:3b:17:a9 CP User Authentication <User=vijay> authenticated <ipaddr=10.101.66.25>	システムが、Radius Accept メッセージを受信しました。	ユーザが正しく認証されました。

システム診断

コントローラには次の 4 つの診断があります。

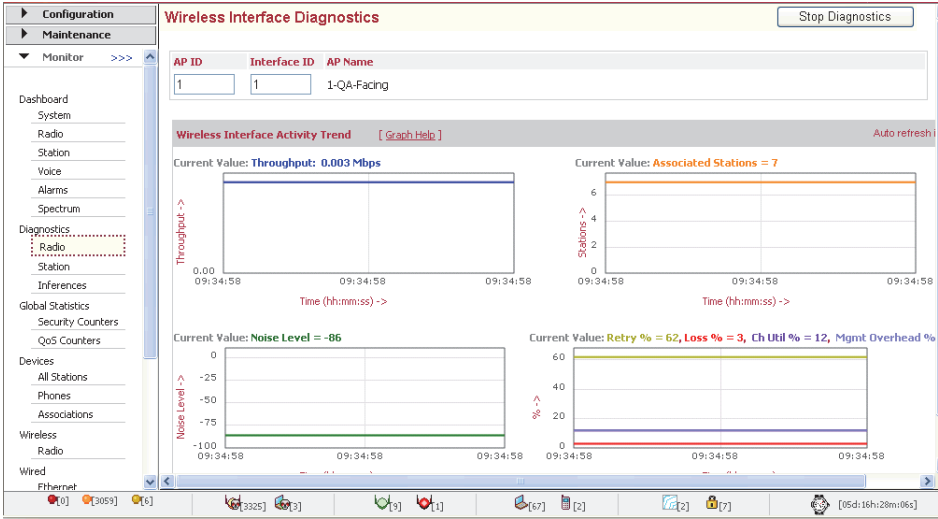
- 無線診断
- ステーション診断
- 推論
- ステーション接続診断 (保守性)

無線診断

各 AP には、1 つまたは 2 つの無線があり、それぞれを設定できます ([Configuration] > [Wireless] > [Radio])。診断情報を確認して、これらの無線のワイヤレス アクティビティの傾向をチェックできます。

1. [Monitor] > [Diagnostics] > [Radio] をクリックします。
2. AP の番号およびインターフェイス ID (Radio 1 または 2) を指定します。
3. 画面の右上隅にある [Start Diagnostics] をクリックします。

図 80: 無線診断



1. これらの無線の傾向については、4 つのチャートをチェックします。

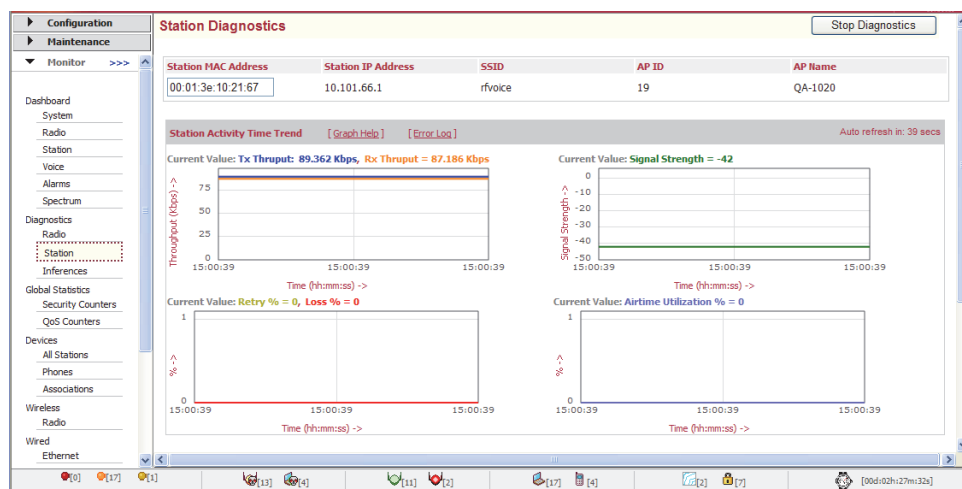
チャート	表示される情報	この情報を確認する理由
Throughput	無線のアップストリームおよびダウンストリーム トラフィックの合計	この AP のカバレッジ エリアで応答が低速になっています。
Noise Level	受信した無線信号にどのぐらいの不要なノイズがあるか。	接続の問題が発生している、またはこの AP のカバレッジ エリアで転送速度が低下しています。
Associated Stations	この AP を使用しているクライアント数	別の AP を追加する必要があるかどうかを確認できます (AP の導入に関する推奨は、リセラーにお問い合わせください)
Current Value	パケット再試行数、損失率、チャネルの利用率、および無線の管理オーバーヘッド。	この AP のカバレッジ エリアで応答が低速になっています。

ステーション診断

ステーションの診断情報を確認することで、AP の各クライアントの詳細を確認できます。

1. [Monitor] > [Diagnostics] > [Station] をクリックします。
2. クライアントの MAC アドレスを指定します。Windows XP でクライアントの MAC アドレスを確認する方法の 1 つは、[プログラム]>[アクセサリ]>[コマンド プロンプト] をクリックしてコマンド プロンプトを開き、コマンド ipconfig /all を入力します。これにより、ワイヤレス接続の物理アドレスが表示されます。
3. 画面の右上隅にある [Start Diagnostics] をクリックします。

図 81: ステーション診断



1. これらのステーションの傾向については、4 つのチャートをチェックします。
 - スループット
 - 損失 %
 - シグナルの強度
 - 利用時間
2. チャートの説明については、[Help] をクリックします。

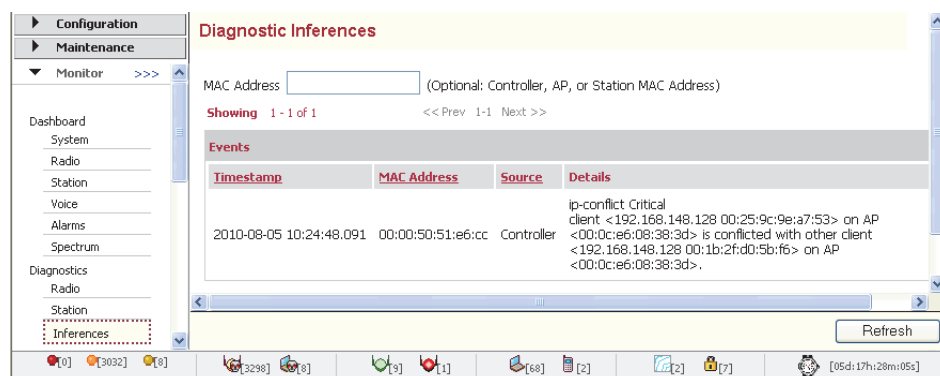
推論

推論とは、ワイヤレス ネットワークの問題の原因についての最も有力な説です。診断推論を確認して、コントローラ、AP、およびステーションをチェックします。

1. [Monitor] > [Diagnostics] > [Inferences] をクリックします。

- オプションで、コントローラ、AP、またはステーションの MAC アドレスを指定して、リストを絞り込みます。
最近のイベントのリストが、詳細と一緒に表示されます。

図 82: 診断推論



このメッセージの最初の部分は、問題と重大度レベルです。上記の例では、IP の競合が発生しています。これはクリティカルな問題です。[Station Entry] の情報が、以下に表示されています。これを読み取るか、MAC アドレスを [Station Diagnostics] ウィンドウにカット アンドペーストします。

図 83: [Station Entry] の読み取り

Sample Station Entry

Inference Rule #8 matched : IP Address Update 32 times within 360 seconds.
 [IP 172.27.0.198] [dhcp] [data] [AP-3 AP-3] [BSSID 00:0c:e6:3d:0b:45] [ESSID rcomm_diag]
 [Vlan Tag 0] [L2 State clear] [L3 State clear] [First Seen @ UTC Jun 9 13:50:22]

Inference Rule #12 matched : Soft Handoff 21 times within 360 seconds.
 [IP 172.27.0.198] [dhcp] [data] [AP-2 AP-2] [BSSID 00:0c:e6:3d:0b:45] [ESSID rcomm_diag]
 [Vlan Tag 0] [L2 State clear] [L3 State clear] [First Seen @ UTC Jun 9 13:50:22]

Information Provided

- Rule that triggered entry
- Latest IP address of station
- DHCP used
- Type of traffic (data or SIP)
- AP updated
- BSSID of Station
- ESSID of Station
- VLAN tag number
- Authentication used on L2
- Authentication used on L3
- Date problem was first seen

ステーション推論メッセージ

可能性のあるステーション ルールおよびメッセージは以下のとおりです。

#	ステーション メッセージ	備考
1	MAC Filter ACL Success	ステーションが、MAC フィルタリング ACL 認証を実行しました。
2	MAC Filter ACL Failure	ステーションは、MAC フィルタリング ACL 認証試行のしきい値を超過しました。
3	MAC Filter RADIUS Success	ステーションが、MAC フィルタリング Radius 認証を実行しました。
4	MAC Filter RADIUS Failure	ステーションは、MAC フィルタリング Radius 認証試行のしきい値を超過しました。
5	Assignment Failure	<p>ステーションは、802.11 割り当て試行のしきい値を超過しました。これが発生する原因は以下のとおりです。</p> <p>関連付けられている AP が AP テーブルに見つからない。</p> <p>ステーションの最大数 (AP モデルによって異なる) を超過した。</p> <p>ライセンス付与されているステーションの最大数を超過した。</p> <p>コントローラは、AP の設定を受け取っていない。</p> <p>割り当てられるクライアントの BSSID が BSS テーブルに見つからない。</p> <p>AP にステーションの空きスロットがない。</p> <p>RSSI がこのステーションに不適切である。</p>
6	WEP-key Index Mismatch	<p>WEP キー インデックスの不一致カウントを監視してください。</p> <p>(まだ実装されていません)</p>
7	Association Success	ステーションが 802.11 アソシエーションを実行しました。
8	Key Exchange Success	ステーションが 802.1x キー交換を実施しました。

#	ステーション メッセージ	備考
9	Key Exchange Failure	<p>ステーションが 802.1x キー交換試行回数のしきい値を超過しました。AP が、AP とクライアント間の 1X 認証エラーの以下のいずれかの状態を検出しました。</p> <p>EAPoL ハンドシェーク エラー</p> <p>EAPoL ハンドシェイクのタイムアウト</p> <p>その他の原因としては、Hostapd が、1X 認証および 802.1x キー交換エラーの以下の状態のいずれかを検出したことが考えられます。</p> <p>無効な Radius VLAN タグが検出された。</p> <p>EAP パケットがステーションに到達しなかった。</p> <p>MIC エラーが発生し、MIC エラーと 802.1x キー交換エラーの回数が増加した。</p> <p>4 ウェイ ハンドシェイクがタイムアウトした。</p> <p>グループ キーの更新がタイムアウトした。</p> <p>EAP キー再生カウンタが一致しない。</p>
10	MIC Failure	ステーションが 802.1x MIC 試行回数のしきい値を超過しました。
11	802.1x RADIUS Success	ステーションが 802.1x Radius 認証を実施しました。
12	802.1x RADIUS Failure	ステーションが 802.1x Radius 認証試行回数のしきい値を超過しました。
13	IP Address Update	IP アドレスが有効なものから 0 に、0 から有効なものに、または有効なものから有効なものに変更されました。
14	Data Decryption Failure	<p>RX パケットのデータ復号化エラーが発生しました (試行回数のしきい値を超過しました)。Hostapd は、</p> <p>Ess.MicCountermeasureData.MicCounter が</p> <p>MIC_COUNTERMEASURE_PERIOD (60 秒) 内で 1 を超過したことを検出しました。これが発生すると、Hostapd は、AP がこのステーションからの通信の受け入れを停止し、ステーションの関連付けを解除することを通知します。</p>
15	CP Guest User Success	ステーションが、キャプティブ ポータルのゲストを認証しました。
16	CP Guest User Failure	ステーションが、キャプティブ ポータルのゲストの認証試行回数のしきい値を超過しました。
17	CP RADIUS User Success	ステーションが、Radius を使用してキャプティブ ポータル ユーザを認証しました。
18	CP RADIUS User Failure	ステーションが、キャプティブ ポータルの Radius ユーザ認証試行回数のしきい値を超過しました。
19	Soft-Handoff	ステーションが、ソフトハンドオフを実行しました。

可能性のあるコントローラ推論メッセージは以下のとおりです。

コントローラ メッセージ	表示される情報
DHCP server reached	IP アドレスの割り当てに必要な DHCP サーバに到達できました。
DHCP server unreachable	IP アドレスの割り当てに必要な DHCP サーバに到達できませんでした。
Gateway reached	クライアント サブネットワークのデフォルト ゲートウェイに到達できました。
Gateway unreachable	クライアント サブネットワークのデフォルト ゲートウェイに到達できませんでした。
RADIUS server reached	クライアント認証に必要な Radius サーバに到達できました。
RADIUS server unreachable	クライアント認証に必要な Radius サーバに到達できませんでした。
VLAN gateway reached	クライアント通信のパスにある VLAN ゲートウェイに到達できました。
VLAN gateway unreachable	クライアント通信のパスにある VLAN ゲートウェイに到達できませんでした。
IP Address conflict between wireless clients or between wired and wireless clients or between wireless client and controller	少なくとも、2 つのワイヤレス クライアントまたはコントローラに同じ IP アドレスが割り当て (指定) されており、ネットワークで障害が発生しています。
IP un-assignment of client by failure of DHCP IP assignment	DHCP サーバが割り当てできなかったため、IP アドレスがクライアントから削除されました。

保守性

ステーションの接続問題をトラブルシューティングするための既存の 2 つの診断ツールに加え、station-log issues コマンドを使用することで、ステーションの接続に関してより明確な理由を把握できます。station-log issues コマンドを使用すると追加表示される 2 つの列 (Issue Observed と Reason) には、問題および妥当と思われる原因の具体的な詳細が示されます。

```
default(15)# station-log issues
```

```
Time stamp          | Client MAC address | AP MAC address    | Issue observed
  | Reason
```

2014-03-14 07:15:13.342 | 00:00:00:00:00:00 | 00:0c:e6:0e:00:21 | AP radio
reset | Reset of radio interface 0

2014-03-14 07:17:58.851 | a8:86:dd:db:6a:c9 | 00:0c:e6:0e:00:21 | Handoff retry
failure | Handoff retry failed for BSSID 00:0c:e6:02:4c:45

問題の事前定義リストは以下のとおりです。

表 34: 接続の問題

問題	説明
関連付けられている AP が頻繁に変更される	この問題は、現在の AP と以前関連付けられていた AP を比較すると確認できます (3 分間に 3 回異なる AP に関連付け)。
AP 無線がリセットされる	AP 無線がリセットされるたびに AP で確認できます。
キューで長い遅延が発生する	この問題は、クライアントに送信されたパケットが予想時間 (5 秒) よりも長くキューにとどまった場合に、AP キューマネージャで確認できます。
距離がある AP に接続している	クライアントが、RSSI 値の高い最も近い AP ではなく、RSSI 値の低い遠くの AP に接続している場合に確認される問題です。
RSSI 値は適切だが、データ転送速度が低い	これは、関連付けられている AP の RSSI 値が適切だと見なされる (-70 を上回っている) が、ワイヤレスのデータ転送速度が期待される性能を下回っている場合に見られる問題です。
AP スループットは高いが、再試行の回数が多い	AP スループットは高いが再試行の割合も高い場合に確認される問題です。
関連付けと関連付けの解除が頻繁に実行される	同じ AP に対して継続的にクライアントの関連付けと関連付けの解除が行われる場合に確認される問題です (3 分間に 3 回同一の AP に関連付け)。
ハンドオフが行ったり来たりする	2 つの AP 間で 12 秒間にハンドオフの肯定応答メッセージを 3 つ受信した場合に確認できる問題です (AP1 から AP2、そして AP1 に戻る)。
ハンドオフの再試行エラー	開始されたハンドオフが 5 回繰り返し失敗した場合に確認される問題です。

ステーション ログ問題のフィルタ

デフォルトでは、station-log issues コマンドを使用するとすべての問題が画面に表示されます。以下のフィルタ オプションを使用すると、特定の問題を表示させることができます。

- MAC アドレス別：

特定の MAC アドレスに固有の問題を表示するには、`-mac` フィルタを使用します。

```
default(15)# station-log issues -mac a8:86:dd:db:6a:c9
```

- AP MAC アドレス別：

特定の AP に関連する問題を表示するには、`-apmac` フィルタを使用します。

```
default(15)# station-log issues -apmac 00:0c:e6:0e:00:21
```

- 問題 ID:

画面に出力された問題のリストから特定の問題だけを表示するには、`-is <IssueID1>,<IssueID2>` を使用します。次の例では、問題 ID が 2 および 9 の問題が表示されます。

```
default(15)# station-log issues -is 2,9
```

- 最後のエントリ：

最後の問題を表示するには、`-last <x>` フィルタを使用します。このとき、`x` には整数を指定します。

```
default(15)# station-log issues -last 2
```

- 検索パターンを使用

テキスト パターンに一致する問題を表示するには、`-search "text"` オプションを使用します。

```
station-log issues -search "Reset of radio"
```

- ヘルプ

使用可能なすべてのオプションを表示するには、`help` キーワードを使用します。

```
default(15)# station-log issues help
```

Usage: station-log issues <Arguments>

<Arguments>

help Display this help and exit

all Display all logs

-is <Issue ID>[,<Issue ID>] Display issues matching issue ID

(Example) -is 2,3 : filtering for AP radio reset and Long queuing delay

-mac <MAC> Display issues for this client MAC address

(Example) -mac 00:90:0b:23:2e:b7 : filtering '00:90:0b:23:2e:b7'

-apmac <MAC> Display issues for this AP MAC address

(Example) -apmac 00:90:0b:23:2e:b7 : filtering '00:90:0b:23:2e:b7'

-search "<PATTERN>" Display issues matching this pattern.PATTERN is case-sensitive

(Example) -search "Reset of radio" : filtering matching string 'Reset of radio'

```
-last <NUM> Display the last <NUM> issues.NUM should be greater than 0  
(Example) -last 5: print the last 5 issues
```

問題 ID のリスト

表 35: ステーション ログの問題 ID のリスト

問題 ID	説明
1	関連付けられている AP が頻繁に変更される
2	AP 無線がリセットされる
3	キューで長い遅延が発生する
4	距離がある AP に接続している
5	RSSI 値は適切だが、データ転送速度が低い
6	AP スループットは高いが、再試行の回数が多い
7	関連付けと関連付けの解除が頻繁に実行される
8	ハンドオフが行ったり来たりする
9	ハンドオフの再試行エラー

診断イベントから確認できる他の情報

CLI でコントローラの診断推論を表示するには、diag-log コマンド admin controller on を使用して、コントローラの診断推論をオンにします。

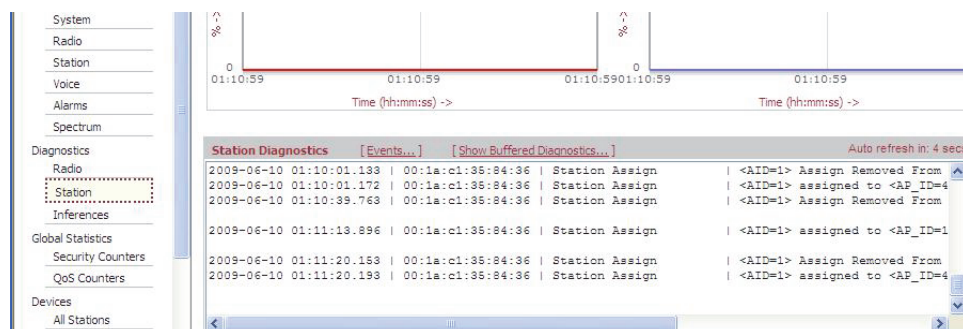
```
Meru01# configure terminal  
Meru01(config)# diag-log  
Meru01(config-diag-log)# admin controller on
```

diag-log コマンド admin station on を使用して、コントローラの診断推論をオンにします

```
Meru01# configure terminal  
Meru01(config)# diag-log  
Meru01(config-diag-log)# admin station on
```

特定のイベントの詳細を確認するには、[図 82](#) のように Web UI 画面から MAC アドレスをコピーし、[Station Diagnostics] ウィンドウ ([Monitor] > [Diagnostics] > [Station]) にペーストし、[Start Diagnostics] をクリックします。

図 84: MAC アドレスを [Station Diagnostics] ウィンドウにペーストした結果



画面の下方にスクロールして、[Show Buffered Diagnostics] をクリックします。

パケットの捕捉

packet-capture-profile コマンドを使用すると、コントローラのローカル インターフェイスでのパケット捕捉、またはアクセス ポイントからの送信の傍受による捕捉が可能です。パケットが捕捉されると、3 つのオプションでそれらパケットを使用できます。リアルタイムでのパケット捕捉の確認、将来的なオフライン分析のためのファイルへの保存、または IDS プログラムやデバイスへの送信が可能です。

CLI コマンド packet-capture-profile では、最大で 10Mb のファイルを捕捉できます。packet-capture-profile を使用する前に、captive ディレクトリが空であることを確認してください。packet-capture-profile コマンドを使用すると、コントローラにローカルにパケットを保存せずに、外部デバイスに AP から直接捕捉したパケットを転送できます。これにより、パケット捕捉のファイル サイズ (コントローラのメモリにより制限されることはありません) に対する制限がなくなります。また、捕捉ファイルを外部に保存およびアーカイブできるようになります。以下の CLI コマンドを使用して、捕捉されたパケットを AP からハードウェア デバ

イスまたはプログラムに送信します。このコマンドでは、Location Manager を使用する必要があります。

操作	使用するコマンド
pcap モードに入り、パケット捕捉プロファイルを作成します。	packet-capture-profile は、既存プロファイルを更新するか、新規プロファイルを作成し、pcap モードに入ります。このモードでは、残りのコマンドが使用されます。
パケットを送信する AP を決定します。	ap-list は、パケットを送信する AP を決定します。AP 名は、1 つずつカンマで区切って入力する必要があります。この時点では、all オプションや範囲指定は利用できません。このリストは、バッファスペースによって制限されます。1、2、3、... 90 を制限を超過せずに入力できます。メモ帳などのアプリケーションでリストを作成して、コマンドに張り付けることを推奨します。バッファサイズを超過すると、コマンドが失敗して、AP のリスト全体の再入力が必要になります。AP のリストがバッファサイズを超過する場合、別のプロファイルを作成して、残りの AP に対応させることができます。
パケットの送信先を示します。 使用するポートを示します。	mode によって、転送モードを layer2 または layer3 に設定し、宛先 IP と、使用するポートを指定します。ポート 9177 は、Location Manager のために使用され、17777 はデバッグに使用されます。
AP が送信する最大のパケット サイズを決定します。	packet-truncation-length は、パケット捕捉のトランケーション長を設定します。デフォルトは 0 であり、トラブルシューティングと WIPS での操作です。82 は、Location Manager 用に使用されます。
パケットを送信するレートを制限するかどうかを決定します。	rate-limiting は、パケット捕捉レート制限を、ステーションごとまたは累積に設定します。 ! 注：現在、レート制限が on の場合、パケットはステーションごとにのみ制限されます。
AP に送信される、または AP から受信する、またはその両方のパケットを捕捉するかどうかを決定します。	rttx は、トラフィック侵入の検出を、受信トラフィック、送信トラフィック、またはその両方に対して設定します。
使用する帯域幅を制限します。	token-bucket-rate は、トークン バケット レートを設定します。
使用する帯域幅を制限します。	token-bucket-size は、トークン バケット サイズを設定します。
設定を AP にダウンロードして、パケットの捕捉を開始します。	enable-profile は、パケット捕捉プロファイルをオンにします。

すべてのパケット捕捉コマンドの詳しい説明については、『*FortiWLC (SD) コマンド リファレンス*』のトラブルシューティングの章を参照してください。

パケット捕捉プロファイルの例 - WireShark

ここでは、WireShark を実行する外部システムが必要です。この例では、Sniffer という名前の packet-capture-profile をコントローラで作成し、AP-5 からポート 17777 の WireShark にレイヤ 3 モードで捕捉したパケットを転送しています。ポート 17777 は、WireShark が受信パケットを L3 モードで IP アドレス 1.1.1.1 のリモートマシンでリスンする PPI カプセル化ポートです。

```
MC3200(15)# configure terminal
MC3200(15)(config)# packet-capture-profile sniffer
MC3200(15)(config-pcap)# mode l3 destination-ip 1.1.1.1 port 17777
MC3200(15)(config-pcap)# ap-list 5
MC3200(15)(config-pcap)# enable
MC3200(15)(config-pcap)# packet-truncation-length 0
MC3200(15)(config-pcap)# exit
MC3200(15)(config)# end
MC3200(15)# sh packet-capture-profile sniffer
AP Packet Capture
Profile Name                : sniffer
Enable/Disable              : enable
Encapsulation               : ppi
L2/L3 Mode                  : l3
Destination IP Address      : 1.1.1.1
UDP Destination Port        : 17777
Destination MAC for L2 Mode : 00:00:00:00:00:00
Rx only/Tx only/Both       : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate           : 10
Token Bucket Size           : 10
AP Selection (ID)           : 5
Extended Filter String      :
Interface Index             :
Packet Truncation Length    : 0
Rate Limiting               : off
Capture Sibling Frames      : on
MC3200(15)#
MC3200(15)#
```

packet-capture-profile コマンドの詳しい説明については、『*FortiWLC (SD) コマンド リファレンス*』のトラブルシューティングの章を参照してください。

パケット捕捉結果で確認すること

検出が L3 経由の場合、capture-packet の結果は、AP からコントローラへの UDP ポート 9292 のパケットの後に、コントローラから AP へのセカンド UDP 9292 パケットが続きます。

これらの 2 つの UDP パケットの後には、約 9 つの UDP ポート 5000 パケットがあります。パケット間の時間デルタをチェックします。パケット間には 10 分の数秒のみしかありません。通常 5 番目の UDP 5000 パケットは、AP からコントローラへのものであり、最初のパケットには、認証に使用された証明書が含まれます。証明書パケットの後に続くのは、証明書を含む UDP ポート 5000 を使用するコントローラから AP へのパケットです。

検出ログで確認すること

成功した検出メッセージの中の主要なメッセージは、以下のとおりです。

```
COMM: CSDS_REQUEST_DISCOVERY message
COMM: Discovery request from <AP MAC address>/<AP IP Address> received
[skip unimportant messages]
COMM: Searching redirect entry for ipAddr 192.168.10.53
[skip unimportant messages]
COMM: Trying to check-out <n> licenses for feature "ap".
COMM: lc_checkout OK for feature "ap".Now, <n> licenses have been checked out
COMM: Response msg to ATS <AP MAC address>/<AP IP Address>
[skip unimportant messages]
COMM: Starting ATS script as: /opt/meru/bin/meru-wnc-ats start 3 8 1 1
Result: Registered virtual device '<AP MAC address>'
COMM: State file /opt/meru/var/run/discovery.state successfully written.
[skip unimportant messages]
COMM: authentication message 0 with payload type 0 from --- 3:8:37
COMM: /CN=meru AP/ST=California/C=US/Email=support@merunetworks.com - OK
[skip unimportant messages]
COMM: AuthMgr::ProcessAccept: 3:8 new key 8f 8e eb ...
One example of the messages you would see when discovery failed because of a
licensing issue is:
COMM: Trying to check-out 1 licenses for feature "ap".
COMM: Checking out one more license for AP failed.FlexRetCode = -9
COMM: lc_checkout FAIL
COMM: AP-1 00:0C:E6:00:2C:96 failed licensing
```

検出ログでは以下も確認してください。

- sh license コマンドの出力が、AP 数と同じまたはそれ以上のライセンス数を示しているか？
- show license-file active コマンドの出力が、sh controller コマンドで出力されるシステム ID と一致する HOSTID=COMPOSITE=<controller system id> のようなシステム ID を示しているか？

FTP エラー コード

この項では、FTP のダウンロードで発生する可能性があるエラー コードのリストを示します。ここで示すコードは、業界標準のレポート用コードです。

- 100 番台のコード：要求されたアクションが実行されます。新しいコマンドに進む前に応答を要求しています。
 - 110 マーカー応答の再始動。この場合、MARK yyyy = mmmm という形でテキストが表示され、特定の実装による違いはありません。yyyy の部分はユーザ プロセスのデータ ストリーム マーカーで、mmmm はサーバの同等のマーカーです (マーカーと "=" の間にスペースが入っています)。
 - 120 サービスがあと (n) 分で作動します。
 - 125 データ接続はオープン済み、転送を開始します。
 - 150 ファイルのステータスは正常、データ接続をオープンします。
 - 150 ファイルのステータスは正常、データ接続をオープンします。
- 200 番台のコード：要求されたアクションは正常に完了しました。
 - 200 コマンドで問題は発生しませんでした。
 - 202 コマンドはこのサイトには実装されていないか、無用です。
 - 211 システムのステータス、またはシステム ヘルプの応答。
 - 212 ディレクトリのステータス。
 - 213 ファイルのステータス。
 - 214 ヘルプ メッセージ。サーバの使用方法、または特定の非標準コマンドの意味に関するヘルプです。この応答は、ユーザが人である場合にのみ有用です。
 - 215 NAME システムのタイプ。NAME は、Assigned Numbers (割り当て済みの番号) ドキュメントのリストに記載されている正式なシステム名です。
 - 220 新しいユーザがサービスを利用できます。
 - 221 サービスはコントロール接続をクローズします。必要があった場合は、ログアウトされています。
 - 225 データ接続はオープンしています。進行中の転送はありません。
 - 226 データ接続をクローズします。要求されたファイルに対するアクションは成功しました (たとえば、ファイルの転送やファイルのアポート)。
 - 227 パッシブ モードに入ります (h1、h2、h3、h4、p1、p2)。
 - 230 ユーザはログインされました。処理を続行してください。
 - 250 要求されたファイルに対するアクションは問題なく、完了しました。
 - 257 "PATHNAME" が作成されました。
- 300 番台のコード：コマンドは受け付けられましたが、要求されたアクションは、さらなる情報を受け取るために保留になっています。
 - 331 ユーザ名は問題ありませんが、パスワードが必要です。
 - 332 ログイン用のアカウントが必要です。
 - 350 要求されたファイルに対するアクションは、さらなる情報を受け取るために保留になっています。

- 400 番台のコード：コマンドは受け付けられておらず、要求されたアクションは実行されませんでした。このエラー条件は一時的なものです、アクションをもう一度要求する場合もあります。
 - 421 サービスを利用できません。コントロール接続をクローズします。(何らかのコマンドによって、サービスをシャットダウンしなければならないと分かった場合の結果である可能性もあります。)
 - 425 データ接続をオープンできません。
 - 426 接続はクローズしました。転送はアボートしました。
 - 450 要求されたファイルに対するアクションは実行されませんでした。ファイルを使用できませんでした(ファイルが使用中だったなど)。
 - 451 要求されたアクションがアボートしました(処理中のローカル エラー)。
 - 452 要求されたアクションは実行されませんでした。システムに十分なストレージ領域がありません。
- 500 番台のコード：コマンドは受け付けられておらず、要求されたアクションは実行されませんでした。500 構文エラー、コマンドを認識できませんでした。コマンド行が長すぎるといったエラーが含まれている可能性があります。
 - 501 パラメータまたは引数の構文エラー。
 - 502 コマンドが実装されていません。
 - 503 コマンドの順序が正しくありません。
 - 504 そのパラメータに対してコマンドが実装されていません。
 - 530 ユーザはログインしていません。
 - 532 ファイルを格納するためにはアカウントが必要です。
 - 550 要求されたアクションは実行されませんでした。ファイルを使用できませんでした(ファイルが見つからない、アクセスできないなど)。
 - 551 要求されたアクションがアボートしました。未知のページ タイプです。
 - 552 要求されたアクションがアボートしました。ストレージの割り当てを超えました(現行のディレクトリまたはデータセットに対して)。
 - 553 要求されたアクションは実行されませんでした。ファイル名が正しくありません。

19 障害管理

アラームとイベントの情報は、[Monitor] > [Fault Management] ページで確認できます。デフォルトでは、[Active Alarms] テーブルが表示され、最近トリガされたすべてのアラームが示されます。

図 85: [Fault Management] テーブル

Fault Management							
<div>Alarms Events Storage Info</div>							
<div>Active Alarms Alarm History Definition</div>							
<input type="checkbox"/>	Alarm Name	Severity	Source	FDN	Raised At	Detail	UserAcknowledged
<input type="checkbox"/>		ALL	ALL				ALL
<input type="checkbox"/>	AP Down	Critical	Access point	SD-AP-37	05/23/2013 17:07:18	AP [MAC address=00:0c:e6:11:25:cb> IP<172.18.114.35>] is down	No
<input type="checkbox"/>	AP Down	Critical	Access point	SD-AP-39	05/22/2013 12:50:13	AP [MAC address=00:0c:e6:0a:59:28> IP<172.18.13.22>] is down	No

[Fault Management] ページには、FortiWLC (SD) において主要な 2 つのイベント タイプである「アラーム」と「イベント」に関する情報が表示されます。詳細については、以下のそれぞれの項を参照してください。

アラーム

アラームが生成されると、ユーザはそれに対して [Acknowledge] または [Clear] を選択できます。選択するには、対象アラームの隣にあるボックスをチェックし、ウィンドウの下部に向かって適切なボタンをクリックします。

- Clear - [Active Alarms] テーブルから [Alarm History] テーブルにアラームを移動させます。
- Acknowledge - [UserAcknowledged] 列で確認済みとしてアラームをマークします。

上図で示されているように、[Active Alarms] テーブルには、複数の列が表示されています。

表 36: [Active Alarm] 列

列	説明
Alarm Name	トリガされるアラームの名前。
Severity	重大度レベルは、Information (情報)、Minor (少し重要)、Major (重要)、Critical (極めて重要) のいずれかになります。
Source	アラームをトリガしたデバイスのタイプ (コントローラ、AP)。
FDN	アラームをトリガしたデバイスの名前。
Raised At	アラームがトリガされた日時。
Detail	デバイス詳細情報の識別を含む、アラームに関する詳細な情報。
UserAcknowledged	アラームが Acknowledged としてフラグが立てられているかどうかを示します。

アラーム定義の変更





FortiWLC (SD) では、事前設定済みのアラームのリストが提供されますが、ユーザは [Alarms] > [Definition] タブを使用して、環境のニーズに合わせてアラームをカスタマイズすることも可能です。

図 86: アラーム定義

Fault Management

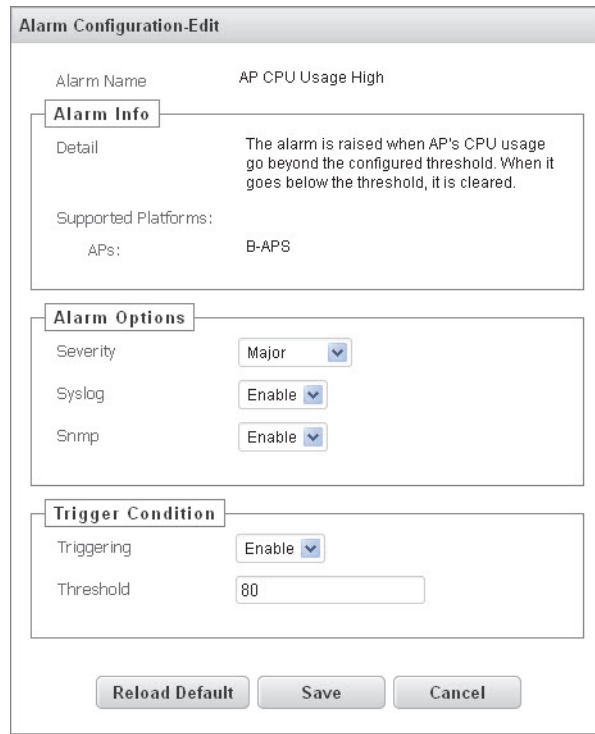
Alarms Events Storage Info

Active Alarms Alarm History Definition

Alarm Name	Severity	Triggering Condition	Threshold	Syslog	Snmp
<input type="text"/>	ALL <input type="button" value="v"/>	ALL <input type="button" value="v"/>	<input type="text"/>	ALL <input type="button" value="v"/>	ALL <input type="button" value="v"/>
 AP CPU Usage High	Major	Enable	80	Enable	Enable
 AP Down	Critical	Enable	0	Enable	Enable
 AP Memory Usage High	Major	Enable	70	Enable	Enable
 AP Radio Card Failure	Critical	Enable	0	Enable	Enable

上図に示されているように、各アラームには重大度レベル、トリガー条件、しきい値が事前に設定されています。これらの値を変更するには、対象アラームの隣にある小さな鉛筆アイコンをクリックします。507 ページの図 87 のように、[Event Configuration] ウィンドウがポップアップで表示されます。

図 87: アラームの編集



The image shows a dialog box titled "Alarm Configuration-Edit". It contains three main sections: "Alarm Info", "Alarm Options", and "Trigger Condition".

- Alarm Info:** The "Alarm Name" is "AP CPU Usage High". The "Detail" text states: "The alarm is raised when AP's CPU usage go beyond the configured threshold. When it goes below the threshold, it is cleared." The "Supported Platforms:" section lists "APs: B-APS".
- Alarm Options:** Contains three dropdown menus: "Severity" set to "Major", "Syslog" set to "Enable", and "Snmp" set to "Enable".
- Trigger Condition:** Contains two fields: "Triggering" set to "Enable" and "Threshold" set to "80".

At the bottom of the dialog are three buttons: "Reload Default", "Save", and "Cancel".

ウィンドウに表示されるドロップダウンを使用して、環境のニーズに合わせてアラームをカスタマイズし、終了したら [Save] をクリックします。必要に応じて、ユーザは [Reload Default] をクリックすれば、アラームの設定を元の値にリセットできます。



[Threshold] フィールドのユニットは、選択したアラームに応じて異なります。たとえば、[AP Memory Usage High] を変更すると、しきい値はシステム メモリ全体に対するパーセンテージで計測されます (デフォルト 70%)。ただし、Link Down などのアラームでは、バイナリ アラームのため、しきい値が必要ありません (つまり、AP へのリンクがダウンしたときにトリガされるものであるため、パーセンテージでは表されません)。

アラームのリスト

番号	アラーム	重大度	ソース	説明
1.	Alarm link up	Information	全コントローラ モデル	コントローラの物理リンクがアップしました。
2.	Alarm link down	Critical	全コントローラ モデル	コントローラの物理リンクがダウンしました。接続を確認してください。
3.	Alarm auth fail	Information	コントローラ モデル	認証が失敗したため、管理者が GUI へのログインに失敗しました。
4.	AP down	Critical	全 AP モデル	AP がダウンしました。理由としては、AP のリブート、AP のクラッシュ、またはコントローラからのイーサネット ケーブルがダウンしていることが考えられます。また、AP が別のコントローラに接続されている可能性もあります。
5.	Radio Failure	Critical	全 AP モデル	初期ブートアップ時に無線が動作しようとして失敗すると、アラームが生成されます。これは、AP 無線のハードウェアに何らかの問題があるために発生します。
6.	Rogue AP detected	Critical	全コントローラ モデル	不正 AP がネットワークで検出されました。次のようなメッセージが表示されます。 Rogue AP Detected Critical 06/04/2010 10:04:51 CONTROLLER (1:24194) ROGUE AP DETECTED.Station mac=0c:60:76:2d:fe:d9 bss=00:02:6f:3a:fd:89 by AP Ben-Cubei (18) 「不正 AP の検出と緩和」 の章を参照してください。
7.	AP software version mismatch	Critical	全 AP モデル	AP のソフトウェア バージョンがコントローラのソフトウェア バージョンと一致しません。自動 AP アップグレードがオンになっている必要があります。CLI コマンド upgrade ap same <ap id> force または upgrade ap same all force で、コントローラから AP をアップデートしてください。CLI コマンド auto-apupgrade enable で自動アップグレードをオンに戻すこともできます。
8.	AP init failure	Major	全 AP モデル	AP の初期化が失敗しました。

番号	アラーム	重大度	ソース	説明
9.	Software license expired	Major	全コントローラ モデル	コントローラ ソフトウェアのライセンスが満了しました。追加ライセンスの取得については、 www.merunetworks.com/license を参照してください。
10.	802.1X auth failure	Major、Minor、Information	全コントローラ モデル	RADIUS サーバの認証が失敗しました。原因を調べるには、RADIUS サーバのログでエラー メッセージを確認し、ステーションのログもチェックしてください。このアラームが稀にしか発生しない場合は、無視しても構いません。ただし、このメッセージが繰り返し発生する場合は、認証が失敗したためにステーションがネットワークに入れない可能性があります。その場合には、RADIUS サーバをチェックして、クライアントとサーバの認証情報が同じであることを確認してください。
11.	MIC failure AP	Major	全コントローラ モデル	ネットワークが TKIP を使用してデータを暗号化する場合には、グループ キー ハンドシェイクで提供される Michael MIC Authenticator Tx/Rx キーのみが使用されます。パケットの Michael MIC の失敗は通常、WPA WPSK パスワードが正しくないことを表します。
12.	MIC countermeasure activation	Major	全コントローラ モデル	MIC 障害が 2 回続けて発生しました (前述参照)。

番号	アラーム	重大度	ソース	説明
13.	RADIUS Server Switchover	Major	全コントローラ モデル	<p>プライマリ認証 RADIUS サーバからセカンダリ認証 RADIUS サーバへの切り替えが発生しました。このメッセージが発生した場合、プライマリ RADIUS サーバが設定されているもののアクセスできず、セカンダリ RADIUS サーバは設定もされてアクセスもできます。</p> <p>このメッセージは、802.1x の切り替えでのみ生成され、キャプティブ ポータルの切り替えでは生成されません。</p> <p>たとえば、次のようなメッセージが生成されます。 RADIUS Server Switchover Major 06/07/2010 14:09:57 RADIUS Server switches over from Primary <172.18.1.7> to Secondary <172.18.1.3> for Profile <wpa></p>
14.	RADIUS Server Switchover Failed	Major	全コントローラ モデル	<p>セカンダリ RADIUS サーバが設定されていないため、プライマリ認証 RADIUS サーバからセカンダリ認証 RADIUS サーバへの切り替えが失敗しました。このメッセージが発生した場合、プライマリ RADIUS サーバが設定されているもののアクセスできず、セカンダリ RADIUS サーバが設定されていません。</p> <p>このメッセージは、802.1x の切り替え失敗でのみ生成され、キャプティブ ポータルの切り替え失敗では生成されません。</p> <p>たとえば、次のようなメッセージが生成されます。 RADIUS Server Switchover Failed Major 06/07/2010 14:02:47 Primary RADIUS Server <172.18.1.7> failed.No valid Secondary RADIUS Server present.Switchover FAILED for Profile <wpa> Alarms Table(1 entry)</p>

番号	アラーム	重大度	ソース	説明
15.	Restore Primary RADIUS Server	Major	全コントローラ モデル	<p>セカンダリ認証 RADIUS サーバからプライマリ認証 RADIUS サーバへの切り替えが発生しました。This alarm was generated while doing RADIUS fail back to the primary server after 15 minutes.</p> <p>このメッセージは、802.1x のプライマリ RADIUS の復帰でのみ生成され、キャプティブ ポータルの復帰では生成されません。</p> <p>たとえば、次のようなメッセージが生成されます。</p> <p>Restore Primary RADIUS Server Major 06/07/2010 15:54:10 Security Profile <wpa> restored back to the Primary RADIUS server <172.18.1.7></p>
16.	Acct RADIUS server switchover	Major	全コントローラ モデル	<p>いずれかのアカウントリング RADIUS サーバ (プライマリまたはセカンダリ) から他方への切り替えが発生しました。このメッセージは、802.1x の切り替えでのみ生成され、キャプティブ ポータルの切り替えでは生成されません。</p> <p>たとえば、プライマリからセカンダリへの切り替えが発生すると、次のようなメッセージが生成されます。</p> <p>Accounting RADIUS Server Switch Major 06/07/2010 14:39:00 Accounting RADIUS Server switches over from Primary <172.18.1.7> to Secondary <172.18.1.3> for Profile <wpa></p>

番号	アラーム	重大度	ソース	説明
17.	Acct RADIUS server switchover failed	Major	全コントローラ モデル	<p>あるアカウントリング RADIUS サーバから他方のサーバへの切り替えが失敗しました。このメッセージが発生した場合、プライマリ アカウントリング RADIUS サーバが設定されているもののアクセスできず、セカンダリ アカウントリング RADIUS サーバが設定されていません。</p> <p>このメッセージは、802.1x の切り替え失敗でのみ生成され、キャプティブ ポータルの切り替え失敗では生成されません。</p> <p>たとえば、次のようなメッセージが生成されます。 Accounting RADIUS Server Switch Major 06/07/2010 14:22:26 Primary Accounting RADIUS Server <172.18.1.7> failed.No valid Secondary Accounting RADIUS Server present.Switchover FAILED for Profile <wpa></p>
18.	Master down	Critical	全コントローラ モデル	N+1 のマスタ コントローラがダウンし、制御できなくなりました。スレーブ コントローラが引き継ぎます。
19.	Master up	Critical	全コントローラ モデル	N+1 のマスタ コントローラがアップし、動作を開始しました。このコントローラがスレーブ コントローラから制御を引き継ぎます。
20.	CAC limit reached (CAC の上限に到達)	Major	全コントローラ モデル	ATM ネットワークのアドミッション制御のことを CAC (Connection Admission Control) と呼び、このプロセスで、ネットワークへの進入を許可するトラフィックを決定します。このメッセージが発生すると、トラフィックの総量がネットワークで現在発生しており、それ以上は受け付けられない状態です。

イベント

特定の処理が行われたことを示すという点で、「イベント」は「アラーム」と類似しています。ただし、通常「アラーム」では問題を解決するためにユーザによる何らかの介入が必要になるのに対し、「イベント」では変更が加えられたことを示すにとどまります。つまり、[Events] タブにはシステムにおける処理に関する参照情報が示されます。

図 88: [Events] テーブル

Fault Management

Alarms

Events

Storage Info

Event View

Definition

Events Table 1-10 of 274						
<input type="checkbox"/>	Event Name	Severity	Source	FDN	Raised At	Detail Information
<input type="checkbox"/>		ALL	ALL			
<input type="checkbox"/>	Admin Login Failure	Critical	Controller	SD-Usr-admin	05/20/2013 11:41:00	An admin user admin from client <172.27.0.61> failed login 2 times.
<input type="checkbox"/>	Admin Login Failure	Critical	Controller	SD-Usr-admin	05/20/2013 11:40:54	An admin user admin from client <172.27.0.61> failed login 1 times.
<input type="checkbox"/>	User 802.1x Authentication Failure	Major	Access point	SD-ST4-ga-vcellwpa2psk-5c:ac:4c:28:62:04	05/08/2013 19:45:11	Access Request rejected for Calling Station ID: <5c:ac:4c:28:62:04>, Authentication Type: <802.1x>, Reason: <Four Way Handshake Timeout>
<input type="checkbox"/>	User 802.1x Authentication Failure	Major	Access point	SD-ST4-ga-vcellwpa2psk-00:16:8f:af:78:b5	05/08/2013 19:45:04	Access Request rejected for Calling Station ID: <00:16:8f:af:78:b5>, Authentication Type: <802.1x>, Reason: <Four Way Handshake Timeout>
<input type="checkbox"/>	User 802.1x Authentication Failure	Major	Access point	SD-ST4-ga-vcellwpa2psk-5c:ac:4c:28:62:04	05/08/2013 19:45:02	Access Request rejected for Calling Station ID: <5c:ac:4c:28:62:04>, Authentication Type: <802.1x>, Reason: <Four Way Handshake Timeout>

以下の表では、[Events] テーブルに表示される列の概要を示しています。

表 37: [Events] テーブルの列

列	説明
Event Name	トリガされるイベントの名前。
Severity	重大度レベルは、Information (情報)、Minor (少し重要)、Major (重要)、Critical (極めて重要) のいずれかになります。
Source	イベントをトリガしたデバイスのタイプ (コントローラ、AP)。
FDN	イベントをトリガしたデバイスの名前。
Raised At	イベントがトリガされた日時。
Detail	デバイス詳細情報の識別を含む、イベントに関する詳細な情報。

イベント定義の変更

FortiWLC (SD) では、事前設定済みのイベントのリストが提供されますが、ユーザは [Events] > [Definition] タブを使用して、環境のニーズに合わせてイベントをカスタマイズすることも可能です。

図 89: イベントの定義

Fault Management

Alarms Events Storage Info

Event View Definition

	Event Name	Severity	State	Threshold Limit	Syslog	Snmp
		ALL ▾	ALL ▾		ALL ▾	ALL ▾
✎	Admin Login Failure	Critical	Enable	1	Enable	Enable
✎	Alarm History Reaches Threshold	Major	Enable	90	Enable	Enable
✎	CAC limit reached	Major	Enable	0	Enable	Enable
✎	Certificate Error	Information	Enable	0	Enable	Enable
✎	Certificate Installed	Information	Enable	0	Enable	Enable
✎	Controller IP Address Change	Major	Enable	0	Enable	Enable

上図に示されているように、各イベントには重大度レベル、トリガー条件、しきい値が事前に設定されています。これらの値を変更するには、対象イベントの隣にある小さな鉛筆アイコンをクリックします。507 ページの図 87 のように、[Event Configuration] ウィンドウがポップアップで表示されます。

図 90: イベントの編集

Event Configuration-Edit

Event Name Alarm History Reaches Threshold

Event Info

Detail The event is generated when history alarm table is 90% full.

Supported Platforms: All Platforms

Event Options

Severity Major ▾

Syslog Enable ▾

Snmp Enable ▾

Trigger Condition

State Enable ▾

Threshold Limit 90

Reload Default Save Cancel

ウィンドウに表示されるドロップダウンを使用して、環境のニーズに合わせてイベントをカスタマイズし、終了したら [Save] をクリックします。必要に応じて、ユーザは [Reload Default] をクリックすれば、イベントの設定を元の値にリセットできます。



[Threshold] フィールドのユニットは、選択したイベントに応じて異なります。たとえば、[Alarm History Reaches Threshold] を変更すると、しきい値はアラーム テーブル履歴全体に対するパーセンテージで計測されます (デフォルト 90%)。ただし、RADIUS Server Switchover などのイベントでは、バイナリ アラームのため、しきい値がありません (つまり、RADIUS サーバの切り替えのときにトリガされるものであるため、パーセンテージでは表されません)。

A システム ログ メッセージ

この付録には、FortiWLC (SD) に現在実装されているすべてのシステム ログ メッセージの簡単な説明を記載します。

- [コントローラ管理](#) (518 ページ)
- [AP システム](#) (527 ページ)
- [802.11](#) (530 ページ)
- [システム セキュリティ](#) (531 ページ)
- [キャプティブポータル](#) (532 ページ)
- [QoS](#) (534 ページ)
- [不正 AP](#) (535 ページ)
- [ライセンス](#) (536 ページ)
- [N+1 冗長性](#) (536 ページ)

コントローラ管理

イベント	システム ログの例	説明	アクション
CONTROLLER REBOOT	Oct 13 11:11:32 172.18.37.201 ALARM: 1255432836 system notice NOT Controller administrative reboot requested	コントローラのリブートが要求されました。	

イベント	システム ログの例	説明	アクション
CONTROLLER BOOT	Oct 13 11:12:55 172.18.37.201 syslog: syslogd startup succeeded	異なるプロセス と WLAN サー ビスが開始した ことを示すコン トローラ ブー ト シーケンス。	
PROCESS START	Oct 13 11:12:55 172.18.37.201 syslog: klogd startup succeeded		
	Oct 13 11:12:58 172.18.37.201 sysctl: net.ipv4.ip_forward = 1		
	Oct 13 11:12:58 172.18.37.201 sysctl: net.ipv4.conf.default.rp_filter = 1		
	Oct 13 11:12:58 172.18.37.201 sysctl: kernel.sysrq = 0		
	Oct 13 11:12:58 172.18.37.201 sysctl: kernel.core_uses_pid = 1		
	Oct 13 11:12:58 172.18.37.201 network: Setting network parameters: succeeded		
	Oct 13 11:12:58 172.18.37.201 network: Bringing up loopback interface: succeeded		
	Oct 13 11:12:58 172.18.37.201 crond: crond startup succeeded		
	Oct 13 11:12:58 172.18.37.201 sshd: succeeded		
	Oct 13 11:12:58 172.18.37.201 sshd[303]: Server listening on 0.0.0.0 port 22.		
	Oct 13 11:12:58 172.18.37.201 network: Bringing up interface eth0: succeeded		
	Oct 13 11:12:59 172.18.37.201 xinetd: xinetd startup succeeded		
	Oct 13 11:12:59 172.18.37.201 root: Start WLAN Services ...		
	Oct 13 11:13:01 172.18.37.201 meru: /etc/init.d/ceflog: / opt/meru/var/run/running-db/ceflog.conf: No such file or directory		
	Oct 13 11:13:01 172.18.37.201 meru: Setting up swapspace version 0, size = 43446272 bytes		
	Oct 13 11:13:01 172.18.37.201 meru: Using /lib/modules/ 2.4.18-3-meruenabled/kernel/drivers/dump/dump.o		
	Oct 13 11:13:01 172.18.37.201 meru: Kernel data gathering phase complete		
	Oct 13 11:13:05 172.18.37.201 meru: Warning: loading / opt/meru/kernel/ipt_vlan_routing.mod will taint the kernel: non-GPL license - Proprietary		
	Oct 13 11:13:37 172.18.37.201 meru: Process RemoteUpgrade did not come up.Will retry again		
	Oct 13 11:13:37 172.18.37.201 root: Controller Up on Tue		

イベント	システム ログの例	説明	アクション
CONTROLLER SHUTDOWN	Oct 13 11:11:33 172.18.37.201 root: Stop WLAN Services ...	異なるプロセスと WLAN サービスが停止したことを示すコントローラ シャットダウン シーケンス。	
PROCESS STOP	Oct 13 11:11:33 172.18.37.201 meru: icrd stopped. Oct 13 11:11:33 172.18.37.201 meru: Rlos stopped. Oct 13 11:11:37 172.18.37.201 meru: discovery stopped. Oct 13 11:11:37 172.18.37.201 meru: WncDhcpRelay stopped. Oct 13 11:11:37 172.18.37.201 meru: nmsagent stopped. Oct 13 11:11:38 172.18.37.201 meru: melfd stopped. Oct 13 11:11:38 172.18.37.201 meru: igmp-snoop-daemon stopped. Oct 13 11:11:44 172.18.37.201 meru: dfstd stopped. Oct 13 11:11:45 172.18.37.201 meru: aeroscoutd stopped. Oct 13 11:11:45 172.18.37.201 meru: snmp stopped. Oct 13 11:11:46 172.18.37.201 meru: cmdstd stopped. Oct 13 11:11:47 172.18.37.201 meru: rfsmgr stopped. Oct 13 11:11:49 172.18.37.201 meru: wncclid stopped. Oct 13 11:11:50 172.18.37.201 meru: sipfd stopped. Oct 13 11:11:51 172.18.37.201 meru: rulefd stopped. Oct 13 11:11:52 172.18.37.201 meru: watchdog stopped. Oct 13 11:11:52 172.18.37.201 meru: oct_watchdog stopped. Oct 13 11:11:52 172.18.37.201 meru: h323fd stopped. Oct 13 11:11:53 172.18.37.201 meru: sccpfd stopped. Oct 13 11:11:54 172.18.37.201 meru: coordinator stopped. Oct 13 11:11:54 172.18.37.201 meru: security-mm stopped. Oct 13 11:11:56 172.18.37.201 meru: hostapd stopped. Oct 13 11:11:57 172.18.37.201 meru: rogueapd stopped. Oct 13 11:11:58 172.18.37.201 meru: xems stopped. Oct 13 11:11:58 172.18.37.201 meru: apache stopped. Oct 13 11:12:01 172.18.37.201 meru: xclid stopped. Oct 13 11:12:07 172.18.37.201 meru: wncagent stopped. Oct 13 11:12:07 172.18.37.201 meru: Removed VLAN - :vlan133:- Oct 13 11:12:08 172.18.37.201 meru: vlan stopped		
コントローラ管理			

イベント	システム ログの例	説明	アクション
	<p>Oct 13 11:12:15 172.18.37.201 meru:</p> <p>Oct 13 11:12:18 172.18.37.201 root: WLAN Services stopped</p> <p>Oct 13 11:12:18 172.18.37.201 rc: Stopping meru: succeeded</p> <p>Oct 13 11:12:18 172.18.37.201 sshd[317]: Received signal 15; terminating.</p> <p>Oct 13 11:12:18 172.18.37.201 sshd: sshd -TERM succeeded</p> <p>Oct 13 11:12:18 172.18.37.201 xinetd: xinetd shutdown succeeded</p> <p>Oct 13 11:12:18 172.18.37.201 crond: crond shutdown succeeded</p> <p>Oct 13 11:12:19 172.18.37.201 syslog: klogd shutdown succeeded</p>		

イベント	システム ログの例	説明	アクション
SSH LOGIN SESSION	<p>Oct 13 11:13:58 172.18.37.201 sshd[4874]: PAM _pam_init_handlers: no default config /etc/pam.d/other</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4874]: PAM _pam_init_handlers: no default config /etc/pam.d/other</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4874]: Accepted password for admin from 172.18.37.12 port 1891 ssh2</p> <p>Oct 13 11:14:00 172.18.37.201 sshd(pam_unix)[4876]: session opened for user admin by (uid=0)</p> <p>Oct 13 11:14:00 172.18.37.201 PAM-env[4876]: Unable to open config file: No such file or directory</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4876]: lastlog_perform_login: Couldn't stat /var/log/lastlog: No such file or directory</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4876]: lastlog_openseek: /var/log/lastlog is not a file or directory!</p> <p>Apr 09 12:00:22 172.18.49.14 -- admin[19814]: LOGIN ON pts/3 BY admin FROM xp.merunetworks.com</p> <p>Apr 09 15:23:07 172.18.37.203 sshd(pam_unix)[23750]: session closed for user admin</p> <p>Apr 09 15:07:53 172.18.37.203 su(pam_unix)[28060]: session opened for user root by admin(uid=0)</p> <p>Apr 09 15:08:09 172.18.37.203 su(pam_unix)[28060]: session closed for user root</p> <p>Apr 09 17:48:48 172.18.37.203 sshd[28588]: Received disconnect from 172.18.37.15: 11: Disconnect requested by Windows SSH Client.</p>	<p>コントローラのユーザが SSH 接続を使用してログインしました。</p>	
WEB ADMIN LOGIN	<p>Oct 13 11:15:07 172.18.37.201 xems: 1255433051 security info WAU Controller Access User admin@172.18.37.12 login to controller at time Tue Oct 13 11:24:11 2009 is OK</p>	<p>admin がコントローラ GUI にログインしました。</p>	

イベント	システム ログの例	説明	アクション
NTP SERVER NOT ACCESSIBLE	Apr 12 18:01:10 172.18.49.14 root: NTP server time.windows.com did not respond.	NTP サーバにアクセスできません。	NTP サーバがダウンしていないかどうかを確認するか、コントローラに NTP サーバが正しく設定されているかどうかを確認してください。設定が正しくない場合は、“Setup” コマンドを使用して設定を修正してください。
User Management: RADIUS request sent	Mar 29 13:43:40 172.18.86.229 SecurityMM: 1269866620 security info RBAC Sending RADIUS Access-Request message for user : pat	RADIUS ベースのコントローラユーザ管理で、RADIUS アクセス要求が RADIUS サーバに送信されます。	
User Management: Group ID not available	Mar 29 13:46:32 172.18.86.229 xems: 1269866791 security info RBAC Group Id not available for Group Num 700 and User Id pat	コントローラユーザに設定されたグループ ID を使用できません。	このグループ ID でグループを作成するか、このユーザのグループ ID を変更してください。
User Management: RADIUS Success	Mar 29 13:49:18 172.18.86.229 SecurityMM: 1269866959 security info RBAC RADIUS Access succeed for user <pat>	RADIUS ベースのコントローラユーザ管理で、RADIUS 認証が成功しました。	

イベント	システム ログの例	説明	アクション
User Management: Group Number received from RADIUS	Mar 29 13:49:18 172.18.86.229 SecurityMM: 1269866959I security info RBAC Group Num <700> received from RADIUS server for user <pat>	RADIUS サーバから、ログインしたユーザのグループ番号が返されました。	
User Management: User Login Success	Mar 29 13:49:18 172.18.86.229 xems: 1269866959I security info WAU Controller Access User pat@172.18.45.17 login to controller at time Mon Mar 29 18:19:19 2010 is OK	コントローラユーザがログインしました。	
User Management: RADIUS Failure	Mar 29 13:50:42 172.18.86.229 SecurityMM: 1269867043I security info RBAC RADIUS Access failed for user <local1234>	コントローラユーザの RADIUS 認証が失敗しました。	
User Management: User Login Failure	Mar 29 13:50:43 172.18.86.229 xems: 1269867043I security info WAU Controller Access User local1234@172.18.45.17 login to controller at time Mon Mar 29 18:20:43 2010 is FAILED	コントローラユーザのログインが失敗しました。	
DUAL ETHERNET	info NOT 10/08/2009 00:12:42 <00:90:0b:0a:81:b0> 1st interface link up.	コントローラの1つ目のインターフェイスリンクがアップしました。	
DUAL ETHERNET	info NOT 10/08/2009 00:16:14 <00:90:0b:0a:81:b0> 1st interface link down.	コントローラの1つ目のインターフェイスリンクがダウンしました。	
DUAL ETHERNET	info NOT 10/08/2009 00:25:55 <00:90:0b:0a:81:af> 2nd interface link up.	コントローラの2つ目のインターフェイスリンクがアップしました。	

イベント	システム ログの例	説明	アクション
DUAL ETHERNET	info NOT 10/08/2009 00:26:16 <00:90:0b:0a:81:af> 2nd interface link down.	コントローラの2つ目のインターフェイスリンクがダウンしました。	
DUAL ETHERNET	info NOT 10/08/2009 00:25:56 <00:90:0b:0a:81:af> switch to 2nd interface done.	コントローラがデュアルイーサネットの冗長モードで構成されています。1つ目のインターフェイスがダウンしたため、2つ目のインターフェイスが引き継ぎました。	
DUAL ETHERNET	info NOT 10/08/2009 00:26:19 <00:90:0b:0a:81:af> switch to 1st interface done.	コントローラがデュアルイーサネットの冗長モードで構成されています。2つ目のインターフェイスがダウンしたため、1つ目のインターフェイスが引き継ぎました。	
DUAL ETHERNET: STANDALONE MODE EXAMPLE	info NOT 10/08/2009 00:12:42 <00:90:0b:0a:81:b0> 1st interface link up. info NOT 10/08/2009 00:16:14 <00:90:0b:0a:81:b0> 1st interface link down.	コントローラがスタンドアロンモードで構成されていて、1つ目のインターフェイスがダウンした場合のシーケンス。	1つ目のインターフェイスリンクダウンのメッセージが表示された場合は、1つ目のインターフェイスへの接続をチェックしてください。

イベント	システム ログの例	説明	アクション
DUAL ETHERNET: REDUNDANT MODE EXAMPLE	info NOT 10/08/2009 0:24:26 <00:90:0b:0a:81:af> 1st interface link up. info NOT 10/08/2009 00:25:52 <00:90:0b:0a:81:af> 1st interface link down. info NOT 10/08/2009 0:25:55 <00:90:0b:0a:81:af> 2nd interface link up. info NOT 10/08/2009 0:25:56 <00:90:0b:0a:81:af> switch to 2nd interface done. info NOT 10/08/2009 0:26:16 <00:90:0b:0a:81:af> 2nd interface link down. info NOT 10/08/2009 0:26:19 <00:90:0b:0a:81:af> 1st interface link up. info NOT 10/08/2009 0:26:19 <00:90:0b:0a:81:af> switch to 1st interface done.	コントローラが 冗長モードで設 定されているこ とを示すシーケ ンス。1 つ目の インターフェイ スがダウンする と、2 つ目のイン ターフェイス が引き継ぎま す。	ダウンしたイン ターフェイスの 接続をチェック してください。
DUAL ETHERNET: ACTIVE MODE EXAMPLE	info NOT 10/08/2009 0:37:29 <00:90:0b:0a:81:b0> 1st interface link up. info NOT 10/08/2009 0:37:29 <00:90:0b:0a:81:af> 2nd interface link up. info NOT 10/08/2009 0:38:34 <00:90:0b:0a:81:af> 2nd interface link down. info NOT 10/08/2009 0:38:39 <00:90:0b:0a:81:b0> 1st interface link down. info NOT 10/08/2009 0:38:43 <00:90:0b:0a:81:b0> 1st interface link up. info NOT 10/08/2009 0:38:45 <00:90:0b:0a:81:af> 2nd interface link up.	コントローラが アクティブ モー ドで設定されて いることを示す シーケンス。	ダウンしたイン ターフェイスの 接続をチェック してください。

AP システム

イベント	システム ログの例	説明	アクション
AP Down	Mar 21 12:56:51 172.18.65.202 ALARM: 1206084411I system info ALR AP DOWN CRITICAL Access Point Pat-AP300 (2) at time Fri Mar 21 07:26:51 2008	<p>このメッセージは、コントローラが AP Down イベントを検出した場合に生成されます。</p> <p>AP Down イベントは次のようないくつかの理由で報告される可能性があります。</p> <p>AP のアップグレード 電源障害 ネットワーク障害、AP にアクセスできない AP のクラッシュ</p>	未知の問題で AP クラッシュが発生した場合は、カスタマ サポートにご連絡ください。
AP Up	Mar 21 12:57:20 172.18.65.202 ALARM: 1206084440I system info ALR AP UP Access Point Pat-AP300 (2) is up at time Fri Mar 21 07:27:20 2008	このメッセージは、コントローラが AP Up イベントを検出した場合に生成されます。	

イベント	システム ログの例	説明	アクション
AP Software Version Mismatch	Mar 21 15:19:05 172.18.65.202 ALARM: 1206092945I system info ALR AP SOFTWARE VERSION MISMATCH CRITICAL AP Pat-AP300 (2) - Software Version Mismatch : AP version is 3.4.SR3m-10 and Controller version is 3.6-40	このメッセージは、AP のソフトウェア バージョンがコントローラのソフトウェア バージョンと一致しない場合に生成されます。	AP 自動アップグレードが有効になっていると、コントローラが自動的に AP ソフトウェアを同じバージョンにアップグレードします。 有効になっていない場合は、手で AP ソフトウェアをコントローラと同じバージョンにアップグレードしてください。
AP Upgrade	Apr 09 12:41:18 172.18.37.203 ALARM: 1270817859I system notice NOT Software version of AP 4 is being changed from 4.0-86 to 4.0-89	AP ソフトウェアがアップグレードされます。	
Boot Image Version Mismatch	Apr 28 14:03:35 172.18.65.202 ALARM: 1209371615I system info ALR AP BOOTIMAGE VERSION MISMATCH CRITICAL BootImage_Version_MisMatch_for_AP1	このメッセージは、AP に非互換ブート イメージが存在する場合に生成されます。	
Boot Image Match	Apr 28 14:03:51 172.18.65.202 ALARM: 1209371631I system info ALR AP BOOTIMAGE VERSION MISMATCH CLEAR BootImage_Version_Match_for_AP1	このメッセージは、AP の非互換ブート イメージが互換ブート イメージに置換された場合に生成されます。	

イベント	システム ログの例	説明	アクション
AP Neighbor Loss	Apr 28 14:01:12 172.18.65.202 ALARM: 1209371472I system info ALR AP NEIGHBOR LOSS CRITICAL Neighbor_Loss_for_AP1	このメッセージは、AP の近接 AP が失われた場合に生成されます。	
AP Neighbor Loss Cleared	Apr 28 14:01:18 172.18.65.202 ALARM: 1209371478I system info ALR AP NEIGHBOR LOSS CLEAR Neighbor_Loss_for_AP1	このメッセージは、AP Neighbor Loss アラームがクリアされた場合に生成されます。	
Hardware Diagnostics Error	Mar 21 13:49:53 172.18.65.202 ALARM: 1206087593I system info ALR AP HARDWARE DIAGNOSTIC ERROR CRITICAL HardwareDiagnostics	このメッセージは、AP に非互換 FPGA バージョンが存在する場合に生成されます。	
Hardware Diagnostics Error Cleared	Mar 21 13:49:47 172.18.65.202 ALARM: 1206087587I system info ALR AP HARDWARE DIAGNOSTIC ERROR CLEAR HardwareDiagnostics	このメッセージは、AP の非互換 FPGA バージョンが互換バージョンに置換された場合に生成されます。	
Handoff Fail	Apr 28 14:02:04 172.18.65.202 ALARM: 1209371524I system info ALR HAND OFF FAIL CRITICAL HandOff_Fail_for_AP1	このメッセージは、ハンドオフが失敗した場合に生成されます。	
Handoff Fail Cleared	Apr 28 14:02:21 172.18.65.202 ALARM: 1209371541I system info ALR HAND OFF FAIL CLEAR HandOff_Fail_Cleared_for_AP1	このメッセージは、ハンドオフ失敗アラームがクリアされた場合に生成されます。	

イベント	システム ログの例	説明	アクション
Resource Threshold Exceeded	Mar 21 13:56:27 172.18.65.202 ALARM: 1206087987I system info ALR RESOURCE THRESHOLD EXCEED CRITICAL ResourceThreshold	このメッセージは、リソース (CPU およびメモリ) のしきい値を超えた場合に生成されます。	
Resource Threshold Exceed Cleared	Mar 21 13:57:17 172.18.65.202 ALARM: 1206088037I system info ALR RESOURCE THRESHOLD EXCEED CLEAR ResourceThreshold	このメッセージは、リソースしきい値超過アラームがクリアされた場合に生成されます。	
System Failure	Mar 21 14:18:29 172.18.65.202 ALARM: 1206089309I system info ALR SYSTEM FAILURE CRITICAL SystemFailure	このメッセージは、システム障害が発生した場合に生成されます。	
System Failure Cleared	Mar 21 14:19:04 172.18.65.202 ALARM: 1206089344I system info ALR SYSTEM FAILURE CLEAR SystemFailure	このメッセージは、システム障害アラームがクリアされた場合に生成されます。	
Watchdog Failure	Mar 21 14:27:28 172.18.65.202 ALARM: 1206089848I system info ALR WATCHDOG FAILURE CRITICAL WatchDog_Failure	このメッセージは、Watchdog プロセスが停止した場合に生成されます。	
Watchdog Failure Cleared	Mar 21 14:27:59 172.18.65.202 ALARM: 1206089879I system info ALR WATCHDOG FAILURE CLEAR WatchDog_Failure	このメッセージは、Watchdog プロセスが再開した場合に生成されます。	

イベント	システム ログの例	説明	アクション
Certificate Error	Mar 21 15:04:10 172.18.65.202 ALARM: 1206092050I system info ALR CERTIFICATE ERROR CRITICAL Certificate_Error	このメッセージは、認証エラーが発生した場合に生成されます。	
Certificate Error Cleared	Mar 21 15:04:38 172.18.65.202 ALARM: 1206092078I system info ALR CERTIFICATE ERROR CLEAR Certificate_Error	このメッセージは、認証エラーアラームがクリアされた場合に生成されます。	
AP Init Failure	Apr 28 12:55:58 172.18.65.202 ALARM: 1209367557I system info ALR AP INIT FAILURE CRITICAL Init_Failure_for_AP1	このメッセージは、AP の初期化が失敗した場合に生成されます。	
AP Init Failure Cleared	Apr 28 12:55:45 172.18.65.202 ALARM: 1209367545I system info ALR AP INIT FAILURE CLEAR Init_Failure_for_AP1	このメッセージは、AP 初期化失敗アラームがクリアされた場合に生成されます。	
AP Radio Card Failure	Apr 28 13:01:00 172.18.65.202 ALARM: 1209367860I system info ALR AP RADIO CARD FAILURE CRITICAL Radio_Card_Failure_for_AP1	このメッセージは、AP 無線カードが動作しなくなった場合に生成されます。	
AP Radio Card Failure Cleared	Apr 28 13:01:08 172.18.65.202 ALARM: 1209367868I system info ALR AP RADIO CARD FAILURE CLEAR Radio_Card_Failure_for_AP1	このメッセージは、AP 無線カード障害アラームがクリアされた場合に生成されます。	

イベント	システム ログの例	説明	アクション
Primary RADIUS Server Restored	Mar 21 15:50:53 172.18.65.202 ALARM: 1206094852I system info ALR PRIMARY RADIUS SERVER RESTORED CRITICAL RADIUS_Server_Restored	このメッセージは、ダウンしたプライマリ RADIUS サーバが復旧した場合に生成されます。	
RADAR Detected	Mar 21 15:12:08 172.18.65.202 ALARM: 1206092528I system info ALR RADAR DETECTED CRITICAL Radar Detected	このメッセージは、DFS Manager がレーダーを検出した場合に生成されます。	
MIC Counter Measure Activation	Apr 28 13:57:36 172.18.65.202 ALARM: 1209371256I system info ALR MIC COUNTERMEASURE ACTIVATION CRITICAL MIC_CounterMeasure_Activation_for_AP1	このメッセージは、2 回続けて MIC 障害が発生した場合に生成されます。	
AP MIC Failure	Apr 28 13:13:12 172.18.65.202 ALARM: 1209368592I system info ALR AP MIC FAILURE CRITICAL MIC_Failure_for_AP1	このメッセージは、MIC 障害が発生している場合に生成されます。	

802.11

イベント	システム ログの例	説明	アクション
Station Unassociated	Apr 09 13:25:28 172.18.37.203 coordinator: Wireless Associations, Unassociated for STA 00:1f:3b:6c:62:e7 in BSSID 00:0c:e6:56:dd:3b ESS 4088clear AP_ID 1 at Time Fri Apr 9 13:41:49 2010	802.11 ステーションのアソシエーション解除。	
Station Associated	<p>Apr 09 14:05:04 172.18.37.203 coordinator: Wireless Associations, Associated for STA 00:1f:3b:6c:62:e7 in BSSID 00:0c:e6:56:dd:3b ESS 4088clear AP_ID 1 at Time Fri Apr 9 14:21:25 2010</p> <p>Mar 22 13:23:34 172.18.65.202 ALARM: 1206127090I system info ALR Station Info Update : MacAddress : 00:40:96:ae:20:7a, UserName : pat, AP-Id : 1, AP-Name : AP-1, BSSID : 00:0c:e6:8f:01:01, ESSID : pat, Ip-Type : dynamic dhcp, Ip-Address : 172.18.65.11, L2mode : clear, L3-mode : clear, Vlan-Name : VLAN-111, Vlan-Tag : 111</p> <p>Apr 06 11:59:24 172.18.65.202 ALARM: 1270535364I system info ALR Station Disconnected : MacAddress : 00:40:96:ae:20:7a</p>	<p>802.11 ステーションのアソシエーション。</p> <p>ステーションの接続。</p> <p>ステーションの切断。</p>	

システム セキュリティ

イベント	システム ログの例	説明	アクション
RADIUS ACCESS REQUEST	Mar 29 13:14:06 172.18.98.221 RADIUSInfo: RADIUS Access-Request Message sent for Client (00:1e:37:0e:98:3e).	RADIUS 要求 メッセージが RADIUS サーバ に送信されまし た。	
RADIUS ACCESS ACCEPT	Mar 29 13:14:06 172.18.98.221 RADIUSInfo: RADIUS Access-Accept message received for Client (00:1e:37:0e:98:3e).	RADIUS サーバ が RADIUS 要求 に対して Access-Accept メッセージを応 答しました (成 功した場合のシ ナリオ)。	
802.1X RADIUS ACCESS REQUEST	Apr 09 15:05:58 172.18.37.203 ALARM: 1270826539I system info ALR 802.1x Authentication Attempt INFO RADIUS Access Attempt by station with MAC address 00:1f:3b:6c:62:e7 and user is NULL , AP Id: <1>	802.1X 認証の 一部として、 RADIUS 要求 メッセージがコ ントローラから RADIUS サーバ に送信されまし た。	

イベント	システム ログの例	説明	アクション
802.1X RADIUS ACCESS REJECT WITH BAD USERNAME	Apr 13 19:48:23 172.18.48.151 ALARM: 1271169441 system info ALR 802.1X AUTHENTICATION FAILURE INFO Access Request rejected for User: <harsh>, NAS IP: <172.18.48.151>, SSID: <wpa2h>, Calling Station ID: <00:1f:3b:83:21:13>, Called Station ID: <00:90:0b:0a:82:48>, Authentication Type: <802.1X>, Reason: <Bad Username or Password>, AP Id: <1>	802.1X 認証の一部として、RADIUS サーバが、「ユーザ名またはパスワードが正しくない」という理由で Access-Reject メッセージを応答しました (失敗した場合のシナリオ)。(Failure scenario).	ユーザ名またはパスワードが正しいかどうかを確認してください。
RADIUS SWITCHOVER FAILURE	Apr 09 15:07:54 172.18.37.203 ALARM: 1270826655 system info ALR RADIUS SERVER SWITCHOVER FAILED MAJOR Primary RADIUS Server <172.18.1.3> failed.No valid Secondary RADIUS Server present.Switchover FAILED for Profile <4089wpa2>	RADIUS 認証時に、プライマリ RADIUS サーバにアクセスできませんでした。セカンダリ RADIUS サーバは設定されていません。	コントローラからプライマリ RADIUS サーバへの接続をチェックしてください。 他の RADIUS サーバを使用できる場合は、そのサーバをセカンダリ サーバとして設定してください。
ACCOUNTING RADIUS SWITCHOVER	Mar 22 16:38:19 172.18.65.202 ALARM: 1206061018 system info ALR ACCOUNT RADIUS SERVER SWITCHOVER MAJOR Accounting RADIUS Server switches over from Primary <1.1.1.1> to Secondary <2.2.2.2> for Profile <WPA2>	アカウントの確認で、プライマリ RADIUS サーバにアクセスできず、セカンダリ RADIUS サーバへの切り替えが試行されました。	プライマリ RADIUS サーバとコントローラの間の接続をチェックしてください。

イベント	システム ログの例	説明	アクション
ACCOUNTING RADIUS SWITCHOVER FAILURE	Mar 22 16:41:51 172.18.65.202 ALARM: 1206061230I system info ALR ACCOUNT RADIUS SERVER SWITCHOVER FAILED MAJOR Primary Accounting RADIUS Server <1.1.1.1> failed.No valid Secondary Accounting RADIUS Server present.Switchover FAILED for Profile <WPA2>	アカウントの確認で、プライマリ RADIUS サーバにアクセスできず、切り替え用のセカンダリ RADIUS サーバが設定されていません。	コントローラからプライマリ RADIUS サーバへの接続をチェックしてください。 他の RADIUS サーバを使用できる場合は、そのサーバをセカンダリ サーバとして設定してください。
MAC FILTERING: RADIUS SWITCHOVER	Mar 21 16:38:57 172.18.65.202 ALARM: 1206097736I system info ALR RADIUS SERVER SWITCHOVER MAJOR RADIUS Server switched over from Primary < 1.1.1.1 > to Secondary < 172.18.1.7 > for Mac Filtering	MAC フィルタリングで、プライマリ RADIUS サーバにアクセスできず、セカンダリ RADIUS サーバへの切り替えが試行されました。	設定されているプライマリ RADIUS サーバとコントローラの間の接続をチェックしてください。

キャプティブ ポータル

イベント	システム ログの例	説明	アクション
Captive Portal Login Request	Mar 29 14:11:53 172.18.98.221 xems: 1269867812l security info CAP Captive Portal User(pat@172.18.98.41) login Request Received.	キャプティブ ポータル ユーザへのログイン要求を受け取りました。	
Captive Portal: RADIUS Login Success	Mar 29 14:11:53 172.18.98.221 SecurityMM: 1269867812l security info CAP pat@172.18.98.41 StationMac[00:1b:77:af:dc:6e] RADIUS User logged in OK	キャプティブ ポータル RADIUS ユーザのログインが成功しました。	
Captive Portal: Redirection	Mar 29 13:39:16 172.18.86.229 xems: 1269866356l security info CAP Captive Portal User(172.18.86.14) Redirected.Sending login (https://secsol:8081/vpn/loginformWebAuth.html)	キャプティブ ポータルのログイン完了。	

イベント	システム ログの例	説明	アクション
Captive Portal: Login Sequence	<p>Mar 22 13:23:47 172.18.65.202 httpd: 1206127103I 802.mobility info CAP 172.18.111.11:8080 1 http://www.google.com/webhp?complete=1&hl=en</p> <p>Mar 22 13:23:47 172.18.65.202 xems: 1206127103I 802.mobility info RED 172.18.111.11:8080 1</p> <p>Mar 22 13:23:47 172.18.65.202 xems: 1206127103I 802.mobility info RED 172.18.111.11:8080 2</p> <p>Mar 22 13:23:47 172.18.65.202 httpd: 1206127103I 802.mobility info CAP 172.18.111.11:8080 2</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 1 http://172.18.111.211:8081/vpn/loginformWebAuth.html</p> <p>Mar 22 13:23:49 172.18.65.202 xems: 1206127105I 802.mobility info CNT 172.18.111.11:8081 1</p> <p>Mar 22 13:23:49 172.18.65.202 xems: 1206127105I 802.mobility info CNT 172.18.111.11:8081 2</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 2</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 1 http://172.18.111.211:8081/vpn/Images.vpn/newlogo.gif</p> <p>Mar 22 13:23:49 172.18.65.202 xems: 1206127105I 802.mobility info CNT 172.18.111.11:8081 1</p> <p>Mar 22 13:23:49 172.18.65.202 xems: 1206127105I 802.mobility info CNT 172.18.111.11:8081 2</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 2</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 1 http://172.18.111.211:8081/favicon.ico</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 2</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 1</p> <p>http://172.18.111.211:8081/favicon.ico</p> <p>Mar 22 13:23:49 172.18.65.202 httpd: 1206127105I 802.mobility info CAP 172.18.111.11:8081 2</p>		

イベント	システム ログの例	説明	アクション
	<p>Mar 22 13:23:55 172.18.65.202 httpd: 1206127110I 802.mobility info CAP 172.18.111.11:8081 1 http://172.18.111.211:8081/vpn/loginUser</p> <p>Mar 22 13:23:55 172.18.65.202 xems: 1206127110I 802.mobility info LOG 172.18.111.11:8081 1</p> <p>Mar 22 13:23:55 172.18.65.202 xems: 1206127110I security info CAP ramesh@172.18.111.11 logged in OK</p> <p>Mar 22 13:23:55 172.18.65.202 xems: 1206127110I 802.mobility info LOG 172.18.111.11:8081 2</p> <p>Mar 22 13:23:55 172.18.65.202 httpd: 1206127110I 802.mobility info CAP 172.18.111.11:8081 2</p>		

QoS

イベント	システム ログの例	説明	アクション
QoS: Action Drop	Apr 13 18:14:23 172.18.117.217 kernel: 1271193480 system info ALR Network Traffic, Flow of Traffic MAC: 00:40:96:ad:49:b0->MAC: 00:90:0b:0a:81:ae src_ip:172.18.117.27-> dst_ip:69.147.125.65:[dst_port:0], rule id: 23, action: Drop.AP MAC Address : 00:0c:e6:05:c5:14	このメッセージは、設定されているパケットパラメータに基づく QoS ルールに一致するパケットがドロップした場合に生成されます。	
QoS: Action Forward	Apr 13 18:21:54 172.18.117.217 kernel: 1271193932 system info ALR Network Traffic, Flow of Traffic MAC: 00:14:a8:59:c8:80->MAC: 00:90:0b:0a:81:ae src_ip:172.18.117.1-> dst_ip:172.18.117.217:[dst_port:0], rule id: 23, action: Forward.AP MAC Address : 00:00:00:00:00:00	このメッセージは、設定されているパケットパラメータに基づく QoS ルールにパケットが一致する場合に生成されます。設定されている QoS ルールに一致するパケットは、その先の処理へと進みます。	

イベント	システム ログの例	説明	アクション
QoS: Action Capture	Apr 13 18:30:47 172.18.117.217 kernel: 1271194465 system info ALR Network Traffic, Flow of Traffic MAC: 00:40:96:ad:49:b0->MAC: 00:90:0b:0a:81:ae src_ip:172.18.117.27-> dst_ip:172.18.122.122:[dst_port:5060], rule id: 3, action: Capture.AP MAC Address : 00:0c:e6:07:5d:71	このメッセージは、設定されているパケットパラメータに基づく QoS ルールにパケットが一致する場合に生成されます。パケットは捕捉され、対応するフロー ディテクタに送信されて、その先の処理へと進みます。	
CAC Per BSSID > CAC Per AP	info ALR 05/04/2010 13:39:20 CAC LIMIT REACHED MAJOR CAC/Global Bssid Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e] in BSSID [00:0c:e6:de:a2:ef]	このメッセージは、(BSSID に基づく) CAC 制限に達した場合に生成されます。コールは却下されます。	
CAC Per AP > CAC Per BSSID	info ALR 05/04/2010 14:42:39 CAC LIMIT REACHED MAJOR CAC/AP Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e]	このメッセージは、(AP に基づく) CAC 制限に達した場合に生成されます。コールは却下されます。	

イベント	システム ログの例	説明	アクション
CAC Per AP = CAC Per BSSID	info ALR 05/04/2010 15:03:22 CAC LIMIT REACHED MAJOR CAC/AP Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e]	このメッセージ は、(AP=BSSID に基づく) CAC 制限に達した場 合に生成されま す。コールは却 下されます。	
CAC PER Interference	info ALR 05/04/2010 15:09:01 CAC LIMIT REACHED MAJOR CAC/Interference Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e]	このメッセージ は、(インター フェイス リー ジョンあたりの CAC に基づく) CAC 制限に達 した場合に生成 されます。コー ルは却下されま す。	

不正 AP

イベント	システム ログの例	説明	アクション
ROGUE AP DETECTED	Oct 13 11:11:31 172.18.37.201 ALARM: 1255432835I system info ALR ROGUE AP DETECTED CRITICAL CONTROLLER (1:13) ROGUE AP DETECTED.AP mac=00:1f:28:57:fa:b7 bss=00:1f:28:57:fa:b7 cch= 6 ess=Integral by AP AP-204 (204)	不正 AP が検出 されました。	
ROGUE AP REMOVED	Mar 29 13:12:43 172.18.86.229 ALARM: 1269864763I system info ALR ROGUE AP REMOVED CONTROLLER (1:24490) ROGUE AP DETECTED.AP mac=00:12:f2:00:17:63 bss=00:12:f2:00:17:63 cch=161 ess=rogue-35	不正 AP が削除 されました。	

ライセンス

イベント	システム ログの例	説明	アクション
LICENSE EXPIRE WARNING	Mar 22 15:27:42 172.18.65.202 ALARM: 1205970893I system notice NOT controller license expires in 1 day	ライセンスが 1 日後に満了することの通知。	ソフトウェアのライセンスをインストールしてください。
LICENSE EXPIRE WARNING	Mar 22 15:33:46 172.18.65.202 ALARM: 1205971257I system notice NOT controller license expires tonight at midnight.	ライセンスが午前 0 時に満了することの通知。	ソフトウェアのライセンスをインストールしてください。
LICENSE EXPIRED	Mar 22 15:42:17 172.18.65.202 ALARM: 1206057655I system info ALR SOFTWARE LICENSE EXPIRED MAJOR controller license has already expired.	ライセンスが満了しました。	ソフトウェアのライセンスをインストールしてください。
LICENSE EXPIRED ALARM CLEAR	Mar 22 15:52:23 172.18.65.202 ALARM: 1206058262I system info ALR SOFTWARE LICENSE EXPIRED CLEAR controller	ライセンスアラームがクリアされました。	

N+1 冗長性

イベント	システム ログの例	説明	アクション
MASTER CONTROLLER DOWN	Apr 19 14:24:26 172.18.253.203 nplus1_Slave: ALERT: Master Controller has timed out: Regression1 172.18.253.201	マスタ コント ローラにアクセ スできないこと がスレーブで検 出されました。 スレーブがアク ティブ状態に移 行します。	マスタ コント ローラを診断し てください。
PASSIVE TO ACTIVE SLAVE STATE TRANSITION	Apr 19 14:24:26 172.18.253.203 nplus1_Slave: Slave State: Passive->Active	パッシブ スレー ブがアクティブ スレーブへと移 行します。	
ACTIVE SLAVE	May 15 16:07:49 172.18.32.201 nplus1_Slave: Slave State: Active	スレーブがアク ティブ状態で す。	
ACTIVE TO PASSIVE SLAVE TRANSITION	May 15 16:07:59 172.18.32.201 nplus1_Slave: Slave State: Active->Passive	マスタ コント ローラにアクセ スできることが スレーブで検出 されたため、ス レーブが再び パッシブになり ます。	
ACTIVE TO PASSIVE SLAVE TRANSITION	Apr 19 14:40:21 172.18.253.203 nplus1_Slave: NOTICE: Active Slave Controller (Regression1 172.18.253.201) -> Passive Slave (RegressionSlave 172.18.253.203)	マスタ コント ローラにアクセ スできることが スレーブで検出 されたため、ス レーブが再び パッシブになり ます。	
PASSIVE SLAVE	Apr 19 14:40:21 172.18.253.203 nplus1_Slave: Slave State: Passive	スレーブがパッシ ブ状態です。	

イベント	システム ログの例	説明	アクション
MASTER CONTROLLER DOWN ALARM	May 15 16:07:49 172.18.32.201 ALARM: 1210847902I system info ALR MASTER CONTROLER DOWN INFO	マスタ コントローラ ダウン アラーム。	
MASTER CONTROLLER UP ALARM	May 15 16:07:59 172.18.32.201 ALARM: 1210847912I system info ALR MASTER CONTROLER UP INFO	マスタ コントローラ アップ アラーム。	
SLAVE CONFIG SYNC	Apr 19 14:51:07 172.18.253.201 sshd[7465]: PAM _pam_init_handlers: no default config /etc/pam.d/other Apr 19 14:51:07 172.18.253.201 sshd[7465]: PAM _pam_init_handlers: no default config /etc/pam.d/other Apr 19 14:51:07 172.18.253.201 sshd[7465]: Accepted publickey for root from 172.18.253.203 port 34674 ssh2 Apr 19 14:51:07 172.18.253.201 PAM-env[7465]: Unable to open config file: No such file or directory	スレーブが scp を使用してマスタ コントローラ と設定ファイルを同期中であると、SSH システム ログ メッセージが表示されます。	

B 用語集

本書で使用する用語と略語をこの用語集にまとめました。

A B C D E F G H I J K L M N O P Q R S T U V W X Y

数字

10BaseT	IEEE 規格 (802.3) の 1 つで、ツイスト ペア ケーブルを使用し、ベースバンド伝送方式で 10 Mbps (メガビット / 秒) のイーサネット ネットワーク (LAN) を運用するための仕様。
100baseT	FastEthernet 規格 (802.3u) の 1 つで、 CSMA/CD LAN アクセス方式を使用した最大 100 Mbps の転送が可能です。
3DES	トリプル DES。DES (Data Encryption Standard) の 1 つで、3 個の 64 ビット キーを使用するため、DES が使用するキーの 3 倍の長さになります。
802.11	802.11 (IEEE 802.11) は、ワイヤレス ローカル エリア ネットワーク (WLAN) に使用される無線テクノロジー仕様です。802.11 では、802.11 MAC (Media Access Control) インターフェイスと PHY (物理) インターフェイスを含む、モバイル (ワイヤレス) ネットワーク アクセス リンク レイヤを定義しています。2 つのワイヤレス クライアント同士、およびワイヤレス クライアントとベース ステーションの間の通信プロトコルを定義しています。 Wi-Fi と呼ばれるこの 802.11仕様は、異なる無線周波数で動作するいくつかの規格から構成されており、その中には、2.4 GHz (802.11 b/g) および 5 GHz (802.11a) の免許なしに使用できる周波数のための規格も含まれています。新たなワイヤレス ネットワーキング形態が生まれれば、802.11仕様にもそれに対応する新たな規格が追加されます。
802.11a	802.11 の規格の 1 つで、5 GHz 帯で最大 54 Mbps のデータ転送速度の通信を行います。802.11a仕様では 802.11b よりも多くの無線チャネルを利用でき、 OFDM を使用します。これらの追加チャネルによって無線とマイクロ波の干渉が抑えられます。
802.11b	2.4 GHz 帯 (2.4 GHz ~ 2.4835 GHz) のワイヤレス ネットワーキングのための国際規格で、最大 11 Mbps のスループットをもたらします。この周波数は、電子レンジ、コードレス電話、医療機器、実験機器、および Bluetooth デバイスにも使われています。
802.11e	802.11 WLAN で Quality of Service (QoS) を提供するための IEEE の仕様です。802.11e は、IEEE 802.11を補完するものであり、802.11 MAC layer supplying a Time Division Multiple Access (TDMA) 構造体と、

音声およびビデオなどの遅延が許容されないアプリケーションを支援するためのエラー修正機構を提供する 802.11 MAC レイヤーの機能強化を提供します。

802.11g	802.11b と同様、この規格も 2.4 GHz 帯で動作しますが、 OFDM を使用して、最大 54 Mbps のスループットを提供します。
802.11i	128 ビットの Advanced Encryption Standard (AES) および Temporal Key Integrity Protocol (TKIP) を 802.1X 認証でサポートし、キー管理機能をサポートし、WLAN セキュリティ機能を向上します。
802.11j	現在の 802.11 規格の機能を強化して、日本での 4.9GHz ~ 5GHz の帯域幅をサポートします。
802.11k	2005 年の批准のため、802.11k Radio Resource Management 規格が、ワイヤレス LAN の効率的な運用のために、アクセス ポイントとスイッチの測定情報を提供します。
802.11n	ワイヤレス環境で 100 Mbps 以上のスループットを提供することを目的とした新しい規格。
802.11r	ワイヤレス ネットワーク間でローミングするためのワイヤレス クライアントの機能を向上させる開発中の仕様。
802.16	ポイントツーマルチポイント アーキテクチャを使用する固定の広帯域のワイヤレス MAN (メトロポリタン アクセス ネットワーク) のための仕様。この規格は、ライセンスを受けた 10GHz と 66GHz の帯域幅の使用と、2GHz と 11GHz (ライセンスを受けた、およびライセンスを受けていない) 周波数範囲の帯域幅の使用を定義します。802.16 は、約 30 マイルの距離での極めて高いビット レートをサポートします。
802.1X	ワイヤレス LAN のセキュリティ実装。オペレーティング システムとネットワーク アクセス デバイスの間でのポート ベースの認証を使用するため、RADIUS、EAP (Extensible Authentication Protocol)、LDAP を使用するユーザ認証のセキュリティを強化します。

A

AAA	認証 (authentication)、承認 (authorization)、アカウンティング (accounting) の頭文字 (トリプル A)。セキュアなネットワークをユーザに保証するためのサービスを提供する、IP ベースのシステム。これらのサービスを強制するには、RADIUS サーバのようなサーバが必要となります。
アクセス ポイント (Access Point)	コントローラ (controller) が管理するデバイスの 1 つで、携帯電話やラップトップのような ステーション (station) とワイヤレス LAN システムとのワイヤレスでの通信を可能にします。
アカウンティング (accounting)	ユーザ セッションが使用したリソース、たとえば、ログオン時間、データ転送、リソースなどをトラッキングするサービス。通常、アカウンティング サービスは、課金、監査、分析などに使用されます。
ACL	Access Control List (アクセス コントロール リスト) の略。ステーションから WLAN へのアクセスを制限するためにコントローラが使用するリストです。ACL には、許可 ACL、拒否 ACL、ステーション内の NIC デバイスの MAC アドレスが記録されている RADIUS サーバ リストがあります。設定によって、ACL を有効あるいは無効のどちらかに設定できます。
AES	Advanced Encryption Standard の略。暗号化規格の 1 つで、対称暗号化アルゴリズム (Rijndael) を使用しています。AES は、米国商務省標準技術局 (National Information and Standards Institute: NIST) によって連邦情報処理標準 (Federal Information Processing Standard: FIPS) として採用されました。

エアトラフィックコントロール (Air Traffic Control)	ワイヤレス ネットワーク内のすべての転送を詳細に管理するフォーティネットのテクノロジー。他のベンダーが提供しているテクノロジーとは異なり、Air Traffic Control テクノロジーは、コチャネルの影響と近隣チャネルの干渉を排除し、ネットワークのすべてのアクセス ポイントが単一の無線チャネルを共有できる方法で単一の 802.11 チャネルでのアップリンクおよびダウンリンク転送を調整します。Channel Layering を使用するときには、チャネル全体でトラフィックのロードバランスを行います。
ATS	Access Transaction Station の略。アクセス ポイント (Access Point) の別の呼び方。
減衰 (attenuation)	RF 信号の減衰は、壁や人のような障害物が存在することで強くなります。特定の物体によって生じる減衰量は、その物体の材質によって異なります。
認証 (authentication)	ユーザを特定するプロセスのこと。一般的にはユーザ名とパスワードが使用されますが、MAC アドレスが使用される場合もあります。
承認 (authorization)	ユーザ名とパスワードを使って認証されたユーザに対して、ネットワーク リソースへのアクセスを許可、または却下するプロセスのこと。

B

バックボーン (backbone)	大規模ネットワークの中心的な要素です。2 つ以上のサブネットワークをリンクし、大規模の企業や組織におけるデータ転送の主要パスとなります。ネットワークのバックボーンは、有線かワイヤレスのどちらかです。
帯域幅 (bandwidth)	ネットワーク上で同時に利用できる総転送容量。利用可能な帯域幅は、ネットワークに接続されたデバイス間でのデータ転送速度、ネットワークのオーバーヘッド、ユーザ数、PC をネットワークに接続するために使用するデバイスの種類などの可変要素によって変動します。これは、サイズによって容量が決まる水道管と似ています。パイプが太ければそれだけ多くの水が流れることができます。ネットワークの帯域幅が大きければそれだけ多くのデータがそこを通過できます。規格 802.11b は 11 Mbps、802.11a と 802.11g は 54 Mbps の帯域幅を提供します。これらは、ネットワークの仕様上の能力です。プロトコルのオーバーヘッド、衝突、実装に起因する制約などの多くの要因によって、実際にはこれらの値は低くなります。
ベースステーション (base station)	セルラー ネットワーキングの用語で、ある範囲内 (通常はセル サイト) での携帯無線電話との通信を維持する無線トランスミッター / レシーバーを指します。
bps	bits per second (ビット / 秒) のこと。1 秒間に送信あるいは受信できるビット数を基準にして、通信回線のデータ転送速度を表す単位。bps (ビット / 秒) は、しばしば Bps (バイト / 秒) と混同されます。8 ビットが 1 バイトに相当するため、ワイヤレス ネットワークの速度が 11 Mbps (11 メガビット / 秒) であれば、毎秒 1.375 MBps (1.375 メガバイト / 秒) のデータが送られることになります。
ブリッジ (bridge)	あるローカル エリア ネットワーク (Local Area Network: LAN) を他の LAN に接続するための製品で、接続には同じプロトコル (たとえば、ワイヤレス、イーサネット、トークンリング) を使用します。同じ敷地内のビルをつなぐ場合は、一般的にはワイヤレス ブリッジが使われます。
BSC	Base Station Controller の略。無線リソースを管理し、セル間のハンドオフを制御します。セルラー ネットワークと公共交換電話網 (Public Switched Telephone Network: PSTN) との間で音声の圧縮 / 解凍を行うためのトランスコーダーが含まれている場合もあります。

BSSID Basic Service Set ID (基本サービス セット識別子) の略。**アクセス ポイント (Access Point)** を特定するための手段で、通常は、人間ではなく機器を特定するために使われます。48 ビットのイーサネット MAC アドレスは、802.11 ワイヤレス サービスを特定するために使用されます。仮想セルでは、すべての同じチャンネルの AP が同じ BSSID を持つように見えます。このように、クライアント側からネットワークが仮想化されます。仮想ポートを使用する場合、各クライアントには異なる BSSID が関連付けられ、独自のプライベート AP があるように見えます。**ESSID** も参照してください。

C

コチャネル干渉 (Co-channel Interference) 2 台のトランスミッタが緊密に同期化されずに同じ周波数を使用するときに、無線干渉が発生します。レガシーのワイヤレス システムは、このような同期を実行できないため、1 つのチャンネル上で転送するアクセス ポイントまたはセル タワーは、離れて配置する必要があります。この結果、カバレッジのギャップが生じ、別のチャンネルに切り替えた無線でこのギャップを埋める必要があります。そのため、非効率で複雑なマイクロセル アーキテクチャになります。Air Traffic Control テクノロジーによって、アクセス ポイントの転送を緊密に同期化でき、コチャネル干渉を回避でき、近隣の AP が同じチャンネルを使用できるようになります。

チャンネル ボンディング (Channel Bonding) 2 つの重複しない 20 MHz のチャンネルを単一の 40 MHz チャンネルに統合します。これにより、同時に 2 倍のデータ量を転送できますが、利用可能なチャンネル数は、半分になります。MIMO と共に、802.11n 規格における重要なイノベーションの 1 つです。

チャンネル レイヤリング (Channel Layering) 複数の仮想セルが同じ物理空間に配置されるものの、重複しないチャンネルで利用可能なキャパシティを倍増するワイヤレス LAN アーキテクチャ。追加されたキャパシティは、冗長性のために使用したり、より高いデータ転送レートやユーザ密度をサポートするために使用されます。1 台の AP の複数の無線を介して、または複数の近隣の AP を使用して有効にできます。総キャパシティは、利用可能な重複していないチャンネル数によってのみ制限されます。

チャンネルの再利用 (Channel Reuse) 異なる AP が同じチャンネルを使用できるパターン。マイクロセル ネットワークでは、このような AP は、コチャネル干渉を避けるために話して配置する必要があります。つまり、連続するカバレッジを実現するには、複数のチャンネルが必要となります。Air Traffic Control テクノロジーを使用するネットワークでは、同じチャンネルをネットワーク全体で再利用できるため、1 つのチャンネルのみが必要であり、他のチャンネルを別の目的に残しておくことができます。

CHAP Challenge Handshake Authentication Protocol (チャレンジ ハンドシェイク 認証プロトコル) の略。この認証プロトコルは、ユーザを認証するための 3 方向のハンドシェイクを定義しています。CHAP は、MD5 ハッシュ アルゴリズムを使って、チャレンジに対する応答を生成します。認証機器は、この応答をチェックできます。

CLI Command-line interpreter (コマンドライン インタープリタ) の略。コマンド シェルと似た方法で、**コントローラ (controller)** に対して命令を発行します。

クライアント (client) ネットワークに接続され、そのネットワーク上の他のメンバに対してサービス (ファイル、プリント機能) を要求するものの総称。

クライアント デバイス (client device) クライアントとは、エンド ユーザのことです。Wi-Fi クライアント デバイスとしては、ラップトップ コンピュータに差し込む PC カード、ラップトップ コンピュータに内蔵されている mini-PCI モジュール、携帯コンピューティング デバイスに差し込む PC カード、USB 無線、PCI/ISA バス Wi-Fi 無線などがある。

	ります。アクセスポイントやゲートウェイと同様、クライアント デバイスは通常、ハブ デバイスと通信します。
衝突回避 (collision avoidance)	ネットワーク ノードの特性の 1 つで、衝突のリスクなく信号を転送できるタイミングをプロアクティブに検出します。
コントローラ (controller)	ワイヤレス LAN において、 アクセス ポイント (Access Point) の設定と統合を行うデバイス。
CSMA-CA	IEEE 802.11 WLAN に採用されているメディア アクセス方式。「送る前に確認する」方式で、複数の無線の同時伝送に起因する衝突を最小限に抑えます (ただし、解決するものではありません)。IEEE 802.11 規格では、衝突の検出ではなく、衝突の回避を使用する必要があると規定していますが、これは、この規格では転送に半二重の無線同士での送信または受信を採用していて、両方が同時に行われることがないためです。
CSMA/CD	イーサネット ネットワーク上のトラフィックを管理し、ノイズを減らすための方式の 1 つ。ネットワーク デバイスは、チャンネルが利用できることを検知してから、データを伝送します。ただし、2 つのデバイスが同時にデータを転送した場合は、送り側デバイスが衝突を検出し、しばらく経ってから再送します。
D	
dBm	1 ミリワット (mW) に対する相対電力 (デシベル) の単位。
サービス拒否 (Denial of Service : DoS)	意図的にユーザがネットワーク リソースを使用できないようにされている状態。
DES	Data Encryption Standard (データ暗号化標準) の略。対称暗号化アルゴリズムの 1 つで、56 ビットのキーを常に使用します。後継である 3DES への移行が急速に進んでいます。
DHCP	サーバへの動的な IP アドレスの割り当てを可能にするユーティリティ。割り当てには、予め定義されたリストと予め定義された時間を使用し、割り当てた IP アドレスの使用時間を制限して、再割り当てを行います。DHCP を使用しない場合は、ネットワーク上のすべてのコンピュータに手動で IP アドレスを割り当てることになります。DHCP を使用すると、コンピュータがネットワークにログインするたびに、自動的に IP アドレスが割り当てられます。
DNS	インターネット上の多数のサーバに保存されているデータベースにアクセスすることで、URL を IP アドレスに変換するプログラム。Web へのアクセスの背後では、このプログラムがアルファベットのアドレスから数字のアドレスへの変換を行っています。DNS サーバは、mywebsite.com というような名前を 107.22.55.26 というような数字の集まりに変換します。すべての Web サイトには、インターネット上で固有の固定 IP アドレスが割り当てられています。
DSL	普通のツイスト ペア銅線の POTS (Plain Old Telephone Service) 電話線を使って高速のデータ、音声、ビデオの転送を行うためのテクノロジー プロトコルであり、いくつかの種類があります。

E

EAP	Extensible Authentication Protocol (拡張認証プロトコル) の略。PPP の拡張仕様。EAP は、トークンカード、Kerberos、ワンタイム パスワード、証明書、公開キー認証、スマート カードなどの複数の認証方法をサポートします。IEEE 802.1x では、EAP を LAN カプセル内にどのようにカプセル化するかを規定しています。
EAP-TLS	Extensible Authentication Protocol with Transport Layer Security の略。EAP-TLS は、デジタル証明書を使用した双方向認証をサポートしています。クライアントからのアクセス要求が発生すると、認証サーバはサーバ証明書を返します。クライアントは自身の証明書を返し、送られてきたサーバ証明書の正当性の評価も行います。これらの証明書の値を使ってセッションの暗号化キーが生成されます。
EAP-TTLS	Extensible Authentication Protocol with Tunneled Transport Layer Security の略。EAP-TTLS は、証明書とパスワード チャレンジの組み合わせを使用して 802.1X 環境での認証を行います。TTLS は、EAP が定義した認証方式に加えて、旧式の CHAP (Challenge Handshake Authentication Protocol)、PAP (Password Authentication Protocol)、MS-CHAP (Microsoft CHAP)、MS-CHAPV2 もサポートしています。
暗号化キー (encryption key)	データの暗号化とその後の復号化を可能にする一連の英数字 (文字列と数字の組み合わせ) で、1 つのネットワークのメンバ間で安全に共有できます。WEP では、暗号化キーを使用して、送られるワイヤレスデータを自動的に暗号化しています。受け取り側では、コンピュータが同じ暗号化キーを使って自動的に復号化し、データを読み取ることができます。
エンタープライズ (enterprise)	大規模な企業や事業体を指す言葉としてよく使われます。エンタープライズ市場は、オフィス ビル、工場、倉庫、研究所、さらには大規模な大学などを対象にしています。
ESSID	Extended Service Set Identifier (拡張サービス セット識別子) の略。32 文字以内の文字で表される 802.11 ワイヤレスネットワークの識別名で、人間が利用することを想定しています。クライアントのセットアップで ESSID を指定すると、範囲内にある他のネットワークではなく、その ESSID のワイヤレスネットワークへ確実に接続できます。 複数のアクセス ポイント (Access Point) で 1 つの ESSID を共有できます。このように設定しておくと、 ステーション (station) は同じ ESSID をもつ複数のアクセス ポイント (Access Point) の間でローミングできます。
イーサネット (Ethernet)	有線環境における国際標準ネットワークング テクノロジー。ベーシックな規格である 10BaseT のネットワークでの帯域幅は、約 10 Mbps です。最近では、Fast Ethernet (100 Mbps) と Gigabit Ethernet (1000 Mbps) の方が優勢です。

F

FCC	Federal Communications Commission (米国連邦通信委員会) の略。米国の通信関係の法律の管理機関。
ファイアウォール (firewall)	ネットワークを保護し、認証されていないユーザからのアクセスを防ぐシステム。ソフトウェア、ハードウェア、またはこれら 2 つの組み合わせによってファイアウォールを構築します。ネットワークへの無制限のアクセスを防ぎ、ネットワークの外へデータが流出するのを制限します。
第 4 世代 (Fourth Generation)	仮想セルを利用するシステムなど、コントローラがハンドオフを管理するワイヤレス LAN システムを説明するために調査会社 Gartner 社が使用した用語。コントローラは、アクセス ポイントの管理にのみを担当し、クライアントはハンドオフを開始するタイミングを自分で決定する必要がある第 3 世代の (マイ

クロセル アーキテクチャ) システムと比較されます。第 2 世代のシステムはコントローラがなく、スタンドアロンの運用向けに設計されており、第 1 世代では独自の 802.11 以外のシステムが使用されていました。

G

- ゲイン (gain)** アンプの出力と入力電力の比率を dB で表したものです。ゲインは、アンプの直線的な作動範囲で表され、入力が 1 dB 上昇すると出力も 1dB 上昇します。
- ゲートウェイ (gateway)** ワイヤレスの世界では、ゲートウェイとは、NAT や DHCP の提供を始めとする追加ソフトウェア機能をもつアクセス ポイントのことです。ゲートウェイが VPN サポート、ローミング、ファイアウォール、多様なレベルのセキュリティなどの機能を備えている場合もあります。

H

- ハンドオフ (Handoff)** クライアントがネットワークを移動するときに、アクセス ポイント間でリンクを転送すること。レガシーのマイクロセル ネットワークでは、Wi-Fi クライアントは、ハンドオフに責任を持ちます。つまり、リンクの品質と全体的なネットワーク パフォーマンスは、クライアントが 802.11 ローミング アルゴリズムの実装に依存しています。仮想セルおよび仮想ポート ネットワークでは、クライアントが単一の仮想 AP に接続した状態で、ネットワーク自身がハンドオフを管理します。
- ハブ (hub)** イーサネット経由または WiFi 経由で PC をネットワークに接続するために使用する、マルチポートのデバイス。有線のハブにはいくつものポートが装備されていて、毎秒 10 メガビットから数ギガビットの範囲の速度でデータを転送できます。ハブは、受け取ったパケットを接続されているすべてのポートに送ります。4 台程度のコンピュータを接続できる小型のハブや、48 台以上の接続が可能な大型のハブもあります。ワイヤレス ハブには、数百台の接続が可能です。
- Hz (ヘルツ)** 周波数を表す国際単位で、旧式の単位であるサイクル / 秒と同等です。1 メガヘルツ (MHz) は 100 万 ヘルツ、1 ギガヘルツ (GHz) は 10 億ヘルツです。米国の標準周波数は 60 Hz、AM ラジオ放送の周波帯は 535 ~ 1605 kHz、FM ラジオ放送の周波帯は 88-108 MHz、ワイヤレス 802.11b LAN は 2.4 GHz を使用します。

I

- IP 番号 (IP number)** IP アドレスとも呼ばれます。インターネット上のトラフィックの送り側と受け取り側を特定するための 32 ビットの 2 進数。一般的には *nnn.nnn.nnn.nnn* という形式で表現され、*nnn* は 0 ~ 256 です。
- ID ベース ネットワーキング (identity-based networking)** 物理的な場所ではなく、ワイヤレス クライアントの ID をベースに WLAN ポリシーが割り当てられ、適用されるという概念。ID ネットワーキングでは、ワイヤレス デバイスは WLAN システムに対して 1 度だけ認証が必要です。コンテキスト情報はローミングによってデバイスに渡され、シームレスなモビリティ環境が実現します。
- IEEE** Institute of Electrical and Electronics Engineers (電気電子学会) の略 (www.ieee.org)。電気および関連分野のエンジニア、科学者、学生が会員となっている団体。30 万人以上の会員を有し、コンピュータおよび通信の標準規格を策定しています。

IEEE 802.11	電気電子学会 (IEEE) の LAN の標準規格群。大多数の有線ネットワークは、CSMA/CD ベースのイーサネット ネットワーク用の仕様である 802.3、またはトークンリング ネットワーク用の仕様である 802.5 のどちらかに準拠しています。802.11 はワイヤレス LAN の標準規格を規定していて、互換性のない (相互運用性のない) 3 つのテクノロジー、すなわち、周波数ホッピング方式 FHSS (Frequency Hopping Spread Spectrum)、直接拡散方式 DSSS (Direct Sequence Spread Spectrum: DSSS)、赤外線を含みます。WECA は、ワイヤレス ネットワーク用の 11 Mbps の高速 DSSS 規格である 802.11b にフォーカスしています。
インフラ モード (infrastructure mode)	AP への接続を提供するための、クライアントの設定。アドホック モードでは PC 同士が直接通信するのに対して、インフラ モードにセットされたクライアントは中央の AP 経由でデータを渡します。AP は、近接しているワイヤレス ネットワークのトラフィックを仲介するだけでなく、有線ネットワークとの通信も提供します。「アドホック (Ad-Hoc)」と「AP」も参照のこと。
IP	Internet Protocol (インターネット プロトコル) の略。メッセージの送信と受信をインターネット アドレスのレベルで行うための一連の取り決め。
IP テレフォニー (IP telephony)	IP ベースでの LAN、WAN、およびインターネットを介した、音声、データ、ビデオの転送をサポートするテレフォニー。VoIP (Voice over IP) は IP テレフォニーの一例です。
IP アドレス (IP address)	インターネット経由で送られる情報の送り側と受け取り側を特定する 32 ビットの数値。1 つの IP アドレスは、インターネット上の特定のネットワークを特定する識別子と、そのネットワークの中で特定のデバイス (サーバやワークステーションである場合もあります) を特定する識別子の 2 つの部分に分かれます。
IPSec	IETF (Internet Engineering Task Force) が規定した、認証と暗号化を提供するセキュリティ プロトコル。レイヤ 3 で動作する IPSec は、VPN ユーザやワイヤレス ユーザにセキュリティを提供するために広く利用されています。Airespace を始めとする一部のベンダは、IPSec セッションでのクライアントのローミングにセキュア モビリティを実現する特別な WLAN 機能を提供しています。
ISDN	ブロードバンド インターネット接続の一種で、ユーザの自宅からダイヤルアップ回線ネットワークまでのデジタル サービスを提供します。ISDN は、標準的な POTS 銅線を使って、音声、データ、あるいはビデオを送信します。
ISO ネットワーク モデル (ISO network model)	<p>国際標準化機構 (International Standards Organization: ISO) が開発したネットワーク モデルで、7 つの異なるレベル、すなわちレイヤで構成されています。これらのレイヤと相互のインターフェイスが規格化されているため、あるプロトコルのいくつかの部分を修正あるいは変更すればテクノロジーの進化やシステム要件の変更に対応できます。以下の 7 つのレイヤで構成されます。</p> <ul style="list-style-type: none"> ● 物理 ● データリンク ● ネットワーク ● トランスポート ● セッション ● プレゼンテーション ● アプリケーション <p>IEEE 802.11 は、物理レイヤ (PHY) と、データリンク レイヤの下位の部分までを対象とした規格です。データリンク レイヤのこの下位の部分は、MAC (Medium Access Controller) サブレイヤと呼ばれています。</p>

J

K

L

LAN	Local Area Network (ローカル エリア ネットワーク) の略。物理的に近い場所にある PC やその他のデバイスを接続し、インターネット接続、プリンター、ファイル、ドライブといったリソースを共有接続するシステム。デバイスの接続に Wi-Fi を使用している場合には、ワイヤレス LAN (WLAN) と呼ばれます。
LDAP	Lightweight Directory Access Protocol の略。情報ディレクトリへのアクセスのためのプロトコルで、X.500 規格に準拠しています。
LWAPP	Lightweight Access Point Protocol の略。IETF (International Engineering Task Force) に提案された、アクセス ポイントと WLAN システム デバイス (スイッチ、アプライアンス、ルータなど) の間の通信プロトコルを標準化するために作成された仕様。最初にこの仕様の策定を開始した企業としては、Airespace や NTT DoCoMo が挙げられます。「CAPWAP」を参照してください。

M

MAC	Medium Access Control (メディア アクセス制御) の略。ネットワーク コントローラの機能で、誰にいつ転送させるかを決定します。各ネットワーク アダプタを特定するため、802.11 の各デバイスには、固有の MAC がハードコーディングされています。この識別子をワイヤレス ネットワークのセキュリティのために使用できます。ネットワークの MAC テーブルに追加されている MAC アドレスを持つ 802.11 無線だけが、そのネットワークにアクセスできます。
中間者攻撃 (Man in Middle)	Man in Middle (MiM)。攻撃の一種で、通信する二者の間 (たとえば、ワイヤレス クライアントとアクセス ポイントの間) で送受信されるトラフィックの傍受あるいは改ざんを試みます。システムが正規の受け取り側と傍受しようとする攻撃者の通信を区別できないと、MIM が成功します。
Mbps	Million bits per second (メガビット / 秒) の略。
MIC	Message Integrity Check (メッセージ整合性チェック) の略。MIC は、IEEE 802.11i 作業グループが策定したドラフト規格の一部です。802.11 (Wi-Fi) フレームのデータ部分と 4 バイトの ICV (Integrity Check Value) の間に 8 バイトのこのフィールドを追加することで、ペイロードとヘッダーの両方を保護します。MIC を実装するアルゴリズムは、Michael と呼ばれています。
マイクロセル (Microcell)	コチャネル干渉を緩和するために隣接する AP を異なる重複しないチャネルに調整する必要があるワイヤレス アーキテクチャ。このアーキテクチャでは、ネットワークを構築する前、およびネットワークが変更されるときに両方で複雑なチャネルの計画が必要となります。また、スペクトルが非効率に使用されているため、コチャネル干渉がそれでも発生することがあります。特に 2.4 GHz では発生しやすくなります。マイクロセル アーキテクチャは、2G セル電話システムやレガシーのワイヤレス LAN システムで一般的に使用されていました。3G セル ネットワークや Air Traffic Control を使用するワイヤレス LAN システムでは使用されないため、すべてのアクセス ポイントが単一のチャネルを共有できます。

モバイル プロ
フェッショナル
(mobile
professional)

セールスマンや出張が多いビジネスマンで、移動時間が長いために、インターネット経由で会社のネットワークに定期的にアクセスして、ファイル / データ / 電子メールの送受信をする必要がある人のこと。

マルチパス
(multipath)

送り側から出された電波が反射、屈折、拡散したために、受け取り側が複数の経路 (マルチパス) からその電波を受け取ってしまう過程あるいは状態のこと。

N

NAT

Network Address Translation の略。1 つのネットワーク上で使われている IP 番号を別のネットワークで使われている IP 番号に変換するシステム。通常は、一方のネットワークが内部ネットワーク、もう一方のネットワークが外部ネットワークです。一般的には内部 IP 番号は比較的大きな IP 番号セットであるため、外部ネットワーク用に小さな IP 番号セットに圧縮する必要があります。

ネットワーク名
(network
name)

すべての共有コンポーネントの中からワイヤレス ネットワークを識別します。ほとんどのワイヤレス ネットワークでは、インストール段階でネットワーク名または SSID を入力する必要があります。個々のコンピュータ、有線ネットワーク、ワークグループのセットアップで、異なるネットワーク名を使用します。

NIC

Network Interface Card (ネットワーク インターフェイス カード) の略。PC アダプタ カードの一種で、ワイヤレス (Wi-Fi) で、あるいはネットワーク ケーブルにつなげて使用することでコンピュータとネットワーク デバイス (ハブ、スイッチなど) との間の双方向通信を可能にします。オフィスで使用されている有線 NIC のほとんどは、10 Mbps (イーサネット)、100 Mbps (FastEthernet)、10/100 Mbps デュアル スピードのいずれかで動作します。高速の Gigabit NIC や 10 Gigabit NIC もあります。「*PC カード*」を参照してください。

O

OFDM

Orthogonal Frequency Division Multiplexing (直交周波数分割多重) の略。大量のデジタル データを電波経由で伝送するための変調方式。OFDM は、無線信号を異なる周波数で並列で受信側へ伝送される複数の小さな信号に分割します。OFDM は、信号伝送でのクロストーク (漏話) を減らします。802.11a は OFDM を使用しています。

オーバーレイ
ネットワーク
(Overlay
Network)

アクセス ポイントと似ていますが、クライアントに対応しない無線センサーの専用ネットワークであり、セキュリティと管理上の問題について常時エアウェーブをスキャンします。無線は、スキャンとクライアント アクセス間で再配備できないため、AP ベースのスキャンの柔軟性が、オーバーレイ ネットワークにはありません。また、リアルタイムの管理と侵入防止に必要なメインのワイヤレス ネットワークと緊密に統合できません。

P

パーティショニ
ング
(Partitioning)

単一のリソースを仮想リソースに分割して、特定のアプリケーション専用にする仮想化の手法。サーバ仮想化の仮想マシン、SAN での仮想ディスク ドライブ、フォーティネットの無線 LAN 仮想化における仮想ポートなどがこの例になります。パーティショニングの主な利点は、管理と分離です。各アプリケーションとユーザは、必要なリソースを正確に使用できるようになり、他のユーザやアプリケーションから保護

できます。また、割り当てられた共有リソース以上が消費されることがなくなります。ワイヤレスのコンテキストでは、スイッチドイーサネットポートのようにワイヤレス LAN が動作するようになります。

**プーリング
(Pooling)**

複数の物理リソースが、単一の仮想リソースに統合される仮想化の手法。仮想ストレージ アレイにおけるマルチ ディスク ドライブ、最新のサーバにおけるマルチ CPU、およびフォーティネットの仮想セルにおけるマルチ アクセス ポイントなどがこの例になります。プーリングの主な利点は、俊敏性の向上、管理の合理化、およびスケール メリットです。リソースは、アプリケーション間でオンデマンドで移動でき、オーバープロビジョニングを回避でき、制限のあるインフラストラクチャでアプリケーションとユーザを解放できます。

**PC カード (PC
card)**

主に PC、ポータブル コンピュータ、PDA、ラップトップで使われている取り外し可能なクレジット カードサイズのメモリまたは I/O デバイスで、タイプ 2 PCMCIA 規格のスロットに差し込むことができます。PC カードの例としては、Wi-Fi カード、メモリ カード、モデム、NIC、ハード ドライブなどがあります。

PCI

高パフォーマンスの I/O コンピュータ バスで、大部分のコンピュータの内部で使用されています。これ以外のバスのタイプとしては、ISA や AGP があります。PCI および他のコンピュータ バスによって、マザーボードや他のコネクタがサポートしていないサービスや機能を提供する内部カードを追加できます。

PDA

ラップトップ コンピュータより小型で、コンピュータとしての機能や通信機能については多くの点で同等の能力をもつもの。PDA には、さまざまなサイズ、複雑さ、機能のものががあります。PDA では、内蔵の Wi-Fi カード無線、差し込み型の PC カード無線、またはコンパクト フラッシュの Wi-Fi 無線を使ったワイヤレス接続が可能です。

PEAP

Protected Extensible Authentication Protocol の略。Microsoft が開発した EAP-TLS (Extensible Authentication Protocol with Transport Layer Security) の拡張仕様です。PEAP Part 1 では TLS を使用してサーバのみの認証を行うため、各クライアントヘユーザ証明書が送られることはありません。PEAP Part 2 は、EAP クライアントとサーバの間の双方向認証を行います。

**ピアツーピア
ネットワーク
(peer-to-peer
network)**

サーバや中央のハブあるいはルータを使用しない、ワイヤレスまたは有線のコンピュータ ネットワーク。ネットワーク上のすべての PC は、ネットワークのサーバまたはクライアントとして平等に動作し、各クライアント コンピュータは、アクセス ポイントやハブを介さずに他のワイヤレス コンピュータと会話できます。ただし、トラフィックの監視やインターネット アクセスの提供を行う中央のベースステーションがないため、さまざまな信号がお互いに衝突し、全体的なパフォーマンスが低下する場合があります。

PHY

OSI ネットワーク モデルで最下位のレイヤ。主として、物理的な (PHYsical) 伝送媒体経由での生のビットストリーム伝送を処理します。ワイヤレス LAN の場合は、伝送媒体は空間です。PHY では、データ速度、変調方式、および信号処理に関するパラメータ、トランスミッタ / レシーバーの同期方式などを定義します。実際の無線環境では、PHY は無線のフロントエンドとベースバンド信号の処理部分にあたります。

**プレナム
(plenum)**

天井プレナムとは、天井タイルの裏側から上部の建物の鋼材までの空間のことです。通常、天井プレナムには、HVAC ダクト、電気配線、水道管、断熱材など設置されています。天井プレナムにネットワーク装置を設置する場合は、その装置がプレナム認定のものである必要があります。

PoE

Power over Ethernet の略。電源コードの代わりにツイストペアのイーサネット データ ケーブルを使って電力を供給するためのテクノロジーで、IEEE 802.3af 規格で定義されています。電源のデータ ケーブルから入ってデバイス側に流れる電流はデータ信号とは分離されるため、干渉し合うことはありません。

POTS

Plain Old Telephone Service の略。標準のアナログ電話サービスのこと (Plain Old Telephone Service の略)。

プロキシ サーバ (proxy server) プロキシ サーバは、大きな会社や組織でネットワークの操作とセキュリティを強化するために使用されるもので、2 つ以上のネットワーク間でダイレクトに通信が行われるのを回避できます。プロキシ サーバは、正当なデータ要求をリモート サーバに転送するか、場合によっては保存しておいたりリモート サーバのデータをデータ要求に直接返します。

PSTN Public Switched Telephone Network (公衆交換電話網) の略。20 世紀後期の通話の一般的な方法で、回線とスイッチを使用することを前提に設計されています。21 世紀には VoIP に移行するものと考えられます。

Q

QoS Quality of Service の略。インターネット帯域幅を管理し、割り当てるためのテクノロジー群。アプリケーション、ユーザ グループ、トラフィック フローなどの要素に固有のパフォーマンス要件を満たすために必要となるサービス レベルを実現するために使用されます。サービス レベルに定義されているのは、ネットワークの可用性 (稼働時間)、レイテンシ、パケット ロスなどのネットワーク サービス測定基準です。

R

RADIUS Remote Authentication Dial-In User Service の略。ユーザの接続を認証し、要求されたシステムまたはサービスへのアクセスを許可するサービス。Microsoft ISA サーバは、RADIUS サーバの一例です。

レンジ (range) ワイヤレス ネットワークの受信範囲。大部分の Wi-Fi システムのレンジは、100 フィート (約 30 メートル) かそれ以上です。環境と使用するアンテナのタイプによって異なりますが、Wi-Fi 信号のレンジは最大 1 マイル (約 1.6 キロメートル) 程度です。

RC4 アルゴリズム (RC4 algorithm) RC4 アルゴリズムは、IV (初期化ベクトル) と秘密キー使って、周期性の高い擬似乱数ストリームを生成します。RSA Security 社が開発した RC4 は、SSL を始めとする多くの転送プロトコルや WEP で使用されています。

RF Radio Frequency (無線周波数) の略。ワイヤレス LAN アクセス ポイントとワイヤレス クライアント (ラップトップ、PDA、電話など) との間の伝送に使用する周波数の種類。ワイヤレス LAN は、2.4 GHz (IEEE 802.11b または IEEE 802.11g) か 5 GHz (IEEE 802.11G) のどちらかの RF スペクトラムを使用できます。

RFID Radio Frequency ID の略。無線周波数を使用して、リーダーとの間で信号の送受信を行うデバイス。箱に貼られたスマートラベル、支払いに使用されるスマートカードやキーチェーン、停車せずに支払いができるようにするために車のフロントガラスに取り付ける箱などのさまざまな形のタグがあります。最近では、従来のパッシブ型デバイスより広い範囲でのより正確なトラッキングを可能にするために、アクティブ型の 802.11 RFID タグがエンタープライズ環境に導入されています。

RF フィンガープリンティング (RF fingerprinting) エンタープライズ WLAN 環境において RF フィンガープリンティングとは、壁や設計に関する特性、たとえば減衰やマルチパスなどを考慮してビルの RF 特性の青写真を作成することをいいます。この情報を場所のトラッキングのために AP が収集したリアルタイムの情報と比較することで、802.11 デバイスの位置をトラッキングします。RF の特性を考慮に入れることによって、RF フィンガープリンティングは現在利用できる最も精度の高いワイヤレス デバイスのトラッキング方法になっています。

RF 予測 (RF prediction) 建物に関する取り込んだデータやサンプルの WLAN 設計設定を基にして、スループットやカバレッジ エリアなどの WLAN の特性を予測するプロセス。

RF 三点測定 (RF triangulation)	802.11 デバイスのトラッキングに広く利用されている方法で、3 つ以上のアクセス ポイントが RSSI 情報を比較することで、あるデバイスの位置の三点測定を行います。RF 三点測定は、導入は簡単ですが、マルチパスや減衰を始めとする、受信感度に影響する RF 特性を考慮しないために RF フィンガープリンティングと比較すると精度が落ちます。
ローミング (roaming)	異なる AP のカバレッジ エリア間でクライアントが移動するときに、ハンドオフを必要とするプロセス。マイクロセル Wi-Fi ネットワークでは、ローミングは、接続がドロップしたり、ネットワークのパフォーマンスが低下するリスクがある複雑な処理となる場合があります。クライアントは、AP から切断し、別の AP を検索する決定を自身が行う必要があります。仮想セルおよび仮想ポート テクノロジを使用するネットワークでは、インフラストラクチャがローミングを制御し、自動的にクライアントを最適な AP に接続します。
不正なアクセス ポイント (rogue Access Point)	ワイヤレス ネットワーク内で動作することが認められていないアクセス ポイントのこと。物理的に近い場所にいるワイヤレス ユーザ (クライアント) によるチャレンジを必要としないアクセスを許してしまう可能性があることから、不正な AP はエンタープライズ ネットワークのセキュリティを脅かすものです。
RJ-45	イーサネット ネットワークで使用する標準コネクタ。標準の RJ-11 電話コネクタにとてもよく似ていますが、電話コネクタでは 4 本しか回線を使用できないのに対して、RJ-45 コネクタでは最大 8 本の回線を使用できます。
ローミング (roaming)	ある AP カバレッジエリアから別の AP カバレッジエリアへ接続のロスなくシームレスに移動すること。
ルータ (router)	あるローカル エリア ネットワーク (LAN) またはワイド エリア ネットワーク (WAN) から別の LAN または WAN ヘッダー パケットを転送するデバイスのこと。ルータは、ルーティング テーブルとルーティング プロトコルを基に転送される各フレームの中のネットワーク アドレスを読み取り、トラフィック負荷、回線コスト、速度、接続状態などを基に最も効率が良いルートでどのようにフレームを送るのかを決定します。
RSA	公開キー アルゴリズムの 1 つで、1977 年に開発され、Rivest、Shamir、Adleman という開発者の名前から命名されました。現在は RSA Data Security 社が所有権をもち、暗号化、デジタル署名、キー交換に使用されています。
RSN	Robust Security Network の略。IEEE 802.11i の中の新しい規格で、802.11 ワイヤレス ネットワークにおけるセキュリティとプライバシーのメカニズムを提供します。RSN は、EAP (Extensible Authentication Protocol) による 802.1x 認証を活用し、暗号化には AES を使用しています。
RSSI	Received Signal Strength Indication (受信信号強度表示) の略。受信信号の強さの測定値。

S

スキャン (scanning)	不正なアクセス ポイントや攻撃者からの不正なエアウェーブをチェックするプロセス。多くの AP は、スキャンとトラフィックの提供を同時には実行できないため、AP のスキャンは、オーバーレイ ネットワークとして通常実装されます。フォーティネットの AP は、エアウェーブのスキャンとクライアントの処理を同時に実行でき、オーバーレイが不要になっています。フォーティネットのシングルチャネル アーキテクチャでは、すべての AP が、すべてのクライアントの信号を検出できるため、不正侵入のスキャンの正確性が向上しています。
--------------------	--

サーバ (server)	<p>ネットワーク上の他のコンピュータやデバイスにリソースを提供するコンピュータのこと。プリントサーバ、インターネットサーバ、データサーバなどの種類があります。サーバは、ハブやルータに結合されている場合もあります。</p> <p>シングルチャネル</p> <p>仮想セルテクノロジーを使用するネットワークなど、同じチャネル上ですべてのアクセスポイントが動作するネットワークを説明するときに使用される用語。シングルチャネルの運用は、マイクロセルアーキテクチャと比較して格段に効率的であり、仮想セルおよびネットワークからハンドオフを制御する場合には、必須となります。シングルチャネルでは、すべてのAPが自動的に範囲内のすべてのクライアントから信号を受け取るため、侵入検知が容易でセキュリティが向上しており、場所の追跡が正確になっています。1つのチャネルのみを外部アクセスからブロックする必要があるため、最小で1つの無線でRFバリアを機能させることができます。</p>
SIP	Session Initiation Protocol (セッション開始プロトコル) の略。SIPは、ユーザ(通常は人)を探し、ユーザ間でのマルチメディア通信(たとえばVoIP通話)をセットアップするためのプロトコルです。
サイト調査 (site survey)	<p>ワイヤレスネットワークを設置する人が、ワイヤレスネットワークを設置する場所を調査する作業のこと。サイト調査は、ある施設の無線とクライアントの使用に関する属性を特定し、最も効果的に動作できる設置環境にアクセスポイントを設置するために行われるものです。ワイヤレスLANシステム(WLAN)は、必ずしもサイト調査を行わなくても効果的に動作するよう設計されています。</p>
スペクトラルの 効率性 (spectral efficiency)	無線スペクトラル使用のデータ転送率。仮想セルが1つのみで提供できるカバレッジをマイクロセルが提供するには、3つの重複しないチャネルが少なくとも必要となるため、仮想セルは、マイクロセルアーキテクチャよりも格段に効率的です。
SSID	WLAN経由で送られるパケットのヘッダに添付されている32文字の識別子であり、モバイルデバイスがあるBBSへ接続しようとするときの名前となります(ESSIDと呼ぶこともあります)。SSIDによって、あるWLANと別のWLANを区別できるため、ある特定のWLANに接続しようとするすべてのアクセスポイントとデバイスは同じSSIDを使用することになります。SSIDを指定しない限り、デバイスがそのBSSに加わることはできません。パケットの中の平文からSSIDを読み取ることができるため、ネットワークに対していかなるセキュリティも提供しません。基本的にはワイヤレスネットワークを特定する名前であるということから、SSIDはネットワーク名とも呼ばれます。
ssh	Secure Shell (セキュアシェル) の略。ユーザがリモートデバイスにログオンし、コマンドを実行するための端末エミュレーションプログラム。クライアントとホストの間のトラフィックは暗号化されます。
SSL	Secure Socket Layer (セキュアソケットレイヤ) の略。多くのオンラインショッピングやバンキングサイトで広く利用されている暗号化スキームで、取引の整合性を保護します。SSLセッションが開始すると、サーバはブラウザに対して公開キーを送ります。その後、ブラウザはそのセッションで交換する秘密キーを取得するために、ランダムに生成した秘密キーを送り返します。
ステーション (station)	MeruワイヤレスLANシステムとのワイヤレスでの通信を アクセスポイント (Access Point) 経由で行う必要がある、たとえば携帯電話やラップトップのようなデバイス。
サブネットワーク / サブネット (subnetwork/ subnet)	1つの大規模ネットワーク内の小さな複数のネットワークのこと。多数のコンピュータ間でのアドレッシングを簡素化するために使用されます。サブネットは、ルータ、ハブ、またはゲートウェイを通して中央ネットワークに接続されます。ワイヤレスLANがローカルコンピュータと会話する場合にも、通常はサブネットを使用します。

サブネット モビリティ (subnet mobility)	ワイヤレス ユーザが単一の IP アドレスを使用して異なるサブネットに配置されている複数のアクセスポイント間でローミングできること。
サブリカント (supplicant)	ネットワークへのアクセスを要求するワイヤレス クライアント。
スイッチ (switch)	ハブの一種で、複数のデバイスによる同じネットワークの使用を効率的に制御することで最適なネットワーク パフォーマンスを実現します。スイッチは、ネットワーク トラフィックを取り締まります。すなわち、ハブは受け取ったすべてのパケットをすべてのポートに送りますが、これに対して、スイッチは受け取り側のポートだけにパケットを転送します。

T

TCP	Transmission Control Protocol の略。インターネット プロトコル (IP) と一緒に使用されるプロトコルであり、インターネット経由のコンピュータ間でのデータ送信をパケットと呼ばれる単位で行います。データの実際の配達の部分を担当するのが IP で、パケットのトラッキングを担当するのが TCP です。1 つのメッセージをパケットに分割することで、インターネット経由での効率的なルーティングを実現しています。たとえば、ある Web ページを Web サーバからダウンロードする場合は、そのサーバの TCP プログラム レイヤがそのファイルをパケットに分割し、各パケットに番号を振ってから、パケットを 1 つずつ IP プログラム レイヤに渡します。すべてのパケットの宛先 IP アドレスは同じですが、各パケットはネットワークの異なるルートで送られる可能性もあります。受け取り側では、TCP は個々のパケットを受け取り、すべてのパケットが送られてきたら、それらを元の 1 つのファイルの形に組み立てなおします。
TCP/IP	TCP/IP は、インターネット、および 1 つのネットワーク上のコンピュータ同士の通信の基底となるテクノロジーです。最初のパートである TCP は、伝送の役割を果たします。送信側と受信側でメッセージのサイズをマッチングすることで、受け取ったメッセージが正しいことを保証します。次のパートである IP は、ユーザのコンピュータのネットワーク上でのアドレスです。TCP/IP ネットワーク上の各コンピュータには、それぞれの IP アドレスが割り当てられています。IP アドレスは起動時に動的に割り当てられるか、固有で割り当てられます。すべての TCP/IP メッセージには、宛先ネットワークのアドレスと宛先ステーションのアドレスが含まれています。そのため、TCP/IP メッセージを 1 つの組織内あるいは全世界の中の複数のネットワーク (サブネット) へ転送できるのです。
TKIP	Temporal Key Integrity Protocol の略。WEP を強化した暗号化テクニック。セッション キーをローテーションする一連のアルゴリズムを使用して保護機能を高めています。TKIP には RC4 暗号化アルゴリズムが使用されていますが、128 ビットの暗号化キー、48 ビットの IV (初期化ベクトル)、新しい MIC (メッセージ整合性コード)、および IV シーケンス処理ルールといった機能が追加されています。

U

USB	PC と周辺装置間の高速双方向シリアル接続で、12 ギガビット / 秒の速度でデータを転送します。データ速度は、標準の USB で 12 Mbps、新仕様の USB 2.0 で最大 480 Mbps です。1394、ファイアウォール、iLink の帯域幅はすべて最大 400 Mbps です。
UTC	Universal Time (協定世界時) の略。グリニッジ標準時とも呼ばれます。タイムゾーンや夏時間のための調整はされません。

V

仮想セル (Virtual Cell)

複数のアクセス ポイントが単一の仮想リソースにプールされる独自のワイヤレス LAN アーキテクチャ。すべての AP が同じ BSSID と無線チャネルを使用するため、クライアントでは、AP を区別できません。クライアントがネットワークを移動するときでも、同じ仮想 AP に接続したままになるため、クライアント側から開始されるハンドオフは不要です。その代わりに、ネットワークが、すべての無線接続を最も適切な AP に自動的にルーティングします。これにより帯域幅が最大化され、ネットワークの管理が合理化されます。また、スケーラビリティと冗長性のために無線スペクトラムを保持できます。

仮想ポート (Virtual Port)

仮想ポートネットワークをパーティション化して、各クライアント デバイスが独自の BSSID で自身のプライベート ネットワークを持つことができる仮想セル アーキテクチャに関する機能強化。クライアント側からは、ネットワークをどこに移動しても、必ず接続したままになる自身の専用 AP を得るような状況になります。スイッチドイーサネット ポートのように、仮想ポートでは各ポートに 1 つのクライアントしかないため、レイテンシが排除され、帯域幅のジッタやコンテンションを削除できます。イーサネットポートとは異なり、各ユーザやデバイスに合わせてカスタマイズでき、独自のクライアント側のソフトウェアや機能拡張を追加しなくても、クライアントの動作をネットワークで管理できます。

VoFi (Voice over Wi-Fi) または VoWLAN (Voice over Wireless LAN)

ワイヤレス ネットワークで動作する Voice over IP リンク。VoIP は、通常高いデータ転送率は不要ですが、低レイテンシとスムーズなハンドオフが求められ、ワイヤレス ネットワークにストレスを与えます。さらに、多くのハンドセットは小さすぎて波長を別々の距離で配置する MIMO のマルチ アンテナを収容できないため、802.11n 電話はまだ利用できません。つまり、VoFi を実行する 802.11n ネットワークは、802.11b/g クライアントを処理する方法が求められています

VLAN

仮想 LAN (Virtual LAN)。デバイスを論理的なグループに分けることで、別々のネットワーク上のユーザが同一ネットワーク上にいるかのような形で通信し合うことを可能にする方法です。

VPN

Virtual Private Network の略。インターネット経由の情報転送のセキュリティを高めるように設計されたテクノロジーの呼称です。VPN には、有線ネットワーク、ワイヤレス ネットワーク、POTS 経由のダイヤルアップ接続といった形態があります。VPN は、エンド ユーザのコンピュータ、ローカルのワイヤレス ネットワークやインターネット全体、企業のサーバやデータベースへ至るすべての経路に渡って、暗号化された専用のトンネルを形成します。

W

WAN

Wide Area Network (ワイド エリア ネットワーク) の略。ある程度の広さをもつ地区、地域、国、あるいは海外までを含めた地理的なエリアをカバーする、PC を始めとする接続コンピューティング デバイスの通信システム。電話ベースのデータネットワークと Wi-Fi を区別するための用語として使われる場合もあります。電話ネットワークは WAN、WiFi ネットワークはワイヤレス ローカル エリア ネットワーク (WLAN) とみなされます。

WEP

Wired Equivalent Privacy の略。Wi-Fi が提供するベーシックなワイヤレス セキュリティ。ホーム ユーザや小規模ビジネスのユーザがワイヤレス データを保護するのであれば、WEP でも十分であるかもしれませんが。WEP には、40 ビット (64 ビットとも呼ばれます) と 104 ビット (128 ビットとも呼ばれます) の 2 種類の暗号化モードがあります。104 ビットの暗号化ではより長いキーが生成されるために解読に長い時間がかかることから、40 ビット (64 ビット) の暗号化に比べてより高いセキュリティが提供されます。

Wi-Fi	各種の 802.11 仕様にに基づくワイヤレス LAN のブランド名。Wi-Fi のロゴが付くすべての製品は、主要な 802.11 クライアントおよびインフラストラクチャベンダから構成される業界団体である Wi-Fi Alliance によって、その相互運用性がテストされています。
WLAN	Wireless LAN (ワイヤレス LAN) の略。LAN とみなされる場合もあります。ローカルエリアネットワークの一種で、ノード間の通信に有線ではなく高い周波数の電波を使用します。
WME	Wireless Multimedia Extension の略。QoS のための Wi-Fi Alliance 規格で、IEEE 802.11e 仕様の一部。EDCF (Enhanced Distribution Coordination Function) をベースにしています。
WNC	Wireless Network Controller (ワイヤレス ネットワーク コントローラ) の略。 コントローラ (controller) の別の呼び方。
WSM	Wi-Fi Scheduled Media の略。802.11e 規格の HCF 部分をベースにした、QoS のための Wi-Fi Alliance の新しい規格で、特定のデータタイプに対する帯域幅セグメント専用。WSM は、同等の役割を果たす WME と比べると、エンタープライズ環境では使われなくなってきました。
WPA	Wi-Fi 保護アクセス Wi-Fi Alliance は、802.11 ワイヤレス LAN 用のデータ暗号化方式として WPA をまとめました。WPA は、TKIP (Temporal Key Integrity) を活用している 802.11i の標準規格化前のバージョンで、業界の支持を受けています。2003 年の第 3 四半期に 802.11i 規格が正式承認されるまでの間は、代替りの規格として WPA を使用することになっています。

X

X.509	国際電気通信連合の電気通信標準化部門 (International Telecommunications Union Telecommunication Standardization Sector: ITU-T) が作成し、最も広く使用されている、デジタル証明書を定義するための規格。
--------------	---

