

FortiWLC (SD)

コマンドリファレンス



リリース 8.2.3

2016 年 8 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 © 2016 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 Sections 1 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	ii
本ガイドについて	37
対象読者	37
関連マニュアル	38
外部の参考資料	38
表記規則	39
構文表記	39
フォーティネットへのお問い合わせ	40
重要な概念	41
CLI の開始	41
CLI コマンド モード	42
ユーザ EXEC モード	42
特権 EXEC モード	42
グローバル設定モード	43
コマンド ラインのみのコマンド	43
コマンドの省略形	45
コマンドの no フォームと default フォームの使用	46
ヘルプの表示	47
コマンド ヒストリの使用	48
コマンド ヒストリ バッファのサイズのセット	48
コマンドの呼び出し	49

コマンド ヒストリ機能の無効化.....	49
show コマンドの出力における語句の検索	49
CLI プロンプトのカスタマイズ.....	50
デフォルトの CLI プロンプト.....	50
CLI プロンプトをカスタマイズするためのコマンド	50
端末特性の操作	50
端末設定の表示.....	50
端末画面の長さ と 幅のセット	51
セッションの終了	51
パスワードでのスペースの使用	51
ユーザ インターフェイス コマンド	53
?	54
disable	55
do	56
enable	57
end	58
exit	59
help	60
prompt	62
quit	63
show history.....	64
show terminal	65
terminal history	66
terminal history size.....	67

terminal length	68
terminal width	69
ファイル管理コマンド	71
cd	72
copy	73
copy running-config	75
delete	77
dir	79
downgrade	81
more	82
pwd	84
rename	85
run	86
show controller file systems	87
show flash	89
show running-config	90
show startup-config	91
show scripts	92
upgrade ap	93
upgrade controller	95
upgrade system	97
patch upgrade	99
システム管理コマンド	101
10gig-module	104

aeroscout	105
alarm	106
amconfig	109
audit period	110
bonding	111
calendar set	113
clear statistics interfaces	115
client-locator	116
controller-index	118
date	119
erase-guest-user	120
event	121
fastpath	124
fingerprint	125
guest-user	126
hostname	128
ip udp-broadcast downstream	129
ip udp-broadcast downstream-bridged	130
ip udp-broadcast upstream	131
ip udp-broadcast upstream-bridged	132
license	133
management wireless	135
nms-profile	136
nms-server	137

nms-vpn-server	138
ntp	139
passwd	141
ping	142
poweroff controller	143
proactive-spectrum-manager	144
proxy-arp-filtering	147
reload	148
reload-gui	150
reload-management	151
reload-security	152
reload-snmp	153
reload-vpn	154
reload-wapi	155
remove-license	156
roaming-domain	157
setup	160
show alarm	162
show ap-neighbor	164
show bonding	168
show calendar	170
show client-locator	171
show controller	172
show controller cpu-utilization	177

show controller file systems	178
show controller memory	180
show controller processes	182
show controller mobility-vars	184
show event	185
show fastpath	187
show features	189
show fingerprints	190
show flash	191
show guest-user	192
show interfaces accel	193
show hostname	194
show license	195
show ip udp-broadcast downstream all-ports	197
show ip udp-broadcast downstream-bridged all-ports	198
show ip udp-broadcast upstream all-ports	199
show ip udp-broadcast upstream-bridged all-ports	200
show license-file	201
show log	202
show nms-server	203
show ntp-server	204
show roaming-domain	205
show syslog-file	207
show syslog-host	209

show syslog-table	210
show sys-summary	212
show sys-summary ess	214
show sys-summary general	216
show sys-summary resources	218
show sys-summary stations	219
show sys-summary throughput	220
show system-id	221
show timezones	222
spectrum-band	223
start-ntp	224
statistics period	225
Sysconfig backup	226
Sysconfig restore	227
syslog-host	228
telnet	229
timezone	230
topo-update	233
traceroute	234
zeronet-packet	235
冗長化コマンド	237
nplus1 add	238
nplus1 delete	240
nplus1 disable	241

nplus1 enable	242
nplus1 period	243
nplus1 revert	244
nplus1 autorevert	245
nplus1 setdebugloglevel	246
nplus1 start master	247
nplus1 start slave	248
nplus1 stop	250
nplus1 takeover	251
nplus1 timeout	252
show nplus1	253
show nplus1 debugloglevel	257
インターフェイスおよび IP コマンド	259
gw	261
igmp-snoop	262
interface FastEthernet	264
ip address	267
ip address dhcp	269
ip default-gateway	270
ip dhcp-passthrough	272
ip dhcp-server	273
ip dns-server	274
ip domainname	276
ip ftp	277

ip scp	278
ip sftp	279
ip udp-broadcast	280
ipv6-neighbor-discovery-optimization	282
mac-address	283
port-profile	284
(config-port-profile) ap-vlan-tag	285
(config-port-profile) dataplane	286
(config-port-profile) disable	287
(config-port-profile) enable	288
(config-port-profile) multicast-enable	289
(config-port-profile) show	290
(config-port-profile) vlan	291
(config-port-profile) ip-prefix-validation-enable	292
show igmp-snoop	294
show interfaces FastEthernet ap	296
show interfaces FastEthernet controller	299
show interfaces FastEthernet statistics	302
show ip	304
show ipv6-neighbor	306
show second_interface_status	307
static-route	308
(config-static-route) interface	309
(config-static-route) ip	310

type	311
virtual-interface-profile	313
(config-vip) disable	314
(config-vip) enable	315
(config-vip) gateway	316
(config-vip) ip	317
(config-vip) show	318
VLAN コマンド	319
dhcp-server	321
(config-dhcp-server) disable	323
(config-dhcp-server) dns-server-primary	324
(config-dhcp-server) dns-server-secondary	325
(config-dhcp-server) domain-name	327
(config-dhcp-server) enable	328
(config-dhcp-server) ip-pool	329
(config-dhcp-server) lease-time	331
(config-dhcp-server) netbios-server-primary	332
(config-dhcp-server) netbios-server-secondary	334
(config-dhcp-server) option-43	336
(config-dhcp-server) show	338
(config-dhcp-server) vlan	339
(config-dhcp-server) virtual-interface-profile	341
gre	343
interface FastEthernet controller	345

ip remote-external-address	347
ip tunnel-ip-address	348
show dhcp-server	349
show gre	351
show dhcp-lease	352
show vlan.	353
test gre.	355
vlan	356
wapi-server	357
セキュリティ コマンド	359
8021x-network-initiation.	363
802.1x-termination.	364
access-list deny	365
access-list deny import	367
access-list permit.	369
access-list permit import	371
mac-filter-state.	373
administrator guest	374
allowed-l2-modes	375
app-visibility-policy	377
app-visibility-custom-application	379
sh service-summary Application-Visibility	380
authentication-mode	382
authentication-mode global	384

authentication-type	386
captive-portal	390
captive-portal-auth-method	392
cef	394
certmgmt delete-ca	397
certmgmt delete-csr	399
certmgmt delete-server	400
certmgmt export-ca	402
certmgmt export-csr	404
certmgmt export-server	406
certmgmt list-ca	408
certmgmt list-csr	410
certmgmt list-server	411
certmgmt view-ca	413
certmgmt view-csr	415
certmgmt view-server	416
change_mac_state	418
clear certificates	420
description	421
encryption-modes ccmp	422
encryption-modes ccmp-tkip	423
encryption-modes tkip	424
encryption-modes wep128	425
encryption-modes wep64	426

firewall-capability	427
firewall-filter-id	428
firewall-filter-id-flow	429
group-rekey interval	430
import	431
ip-address	432
key	433
key-rotation	434
local-admin	435
mac-delimiter	437
macfiltering	438
password	439
password-type	441
PMK-caching	442
pmk caching	443
port	444
primary-tacacs-ip	445
primary-tacacs-port	447
primary-tacacs-secret	449
privilege-level	451
psk key	454
radius-profile	456
radius-server primary	458
radius-server secondary	459

reauth	460
rekey period	461
secondary-tacacs-ip	462
secondary-tacacs-port	464
secondary-tacacs-secret	466
security-logging	468
security-profile	469
shared-authentication	472
show aaa statistics	473
show access-list deny	474
show access-list permit	475
show air-shield	476
show arp	477
show authentication-mode	479
show cef	480
show local-admins	481
show radius-profile	483
show security-profile	485
show ssl-server	488
show web	489
ssl-server accounting-radius-profile	491
ssl-server associate	493
ssl-server captive-portal	494
ssl-server captive-portal-external_URL	496

ssl-server port	498
ssl-server radius-profile	499
ssl-server cna-bypass	500
static-wep key	502
static-wep key-index	504
tunnel-termination	505
vpn client	506
(config-vpn-client) vpn-client-state.	507
(config-vpn-client) vpn-server-ip	508
(config-vpn-client) vpn-server-port.	509
vpn server	510
(config-vpn) encryption	511
(config-vpn) ip-pool	512
(config-vpn) port	513
(config-vpn) subnet-mask	514
(config-vpn) vpn-server-ip	515
(config-vpn) vpn-server-state.	516
web custom	517
web login-page	519
ESSID コマンド	521
accounting interim-interval.	523
accounting primary-radius	524
accounting secondary-radius.	526
ap-discovery join-ess.	528

ap-discovery join-virtual-ap	529
ap-vlan priority	531
ap-vlan-tag	532
apsd	533
band-steering-mode	535
band-steering-timeout	537
base-tx-rates	539
beacon dtim-period	541
beacon period	542
bssid	543
calls-per-bss	544
countermeasure	545
dataplane	546
edited-bssid	548
ess-ap	549
essid	550
gre name	551
l2bridge airf	552
l2bridge appletalk	553
l2bridge ipv6	554
multicast-enable	555
multicast-mac-transparency	556
overflowfrom-essprofile	557
publish-essid	559

security-profile	560
show ess-ap	561
show edited-bssid	562
show essid	563
ssid	566
supported-tx-rates	567
tunnel-type	569
virtual-port	570
vlan name	571
wireless-to-wireless-isolation	572
アクセス ポイントと無線コマンド	573
admin-mode	576
antenna-gain	577
antenna-property	578
antenna-selection	579
ap	580
ap-keepalive-timeout	582
ap-redirect	583
auto-ap-upgrade	584
autochannel	586
boot-script	587
building	588
channel	589
channel-width	591

connectivity	592
contact	594
controller domainname	595
controller hostname	596
controller ip	597
dataplane-encryption	598
description	599
fixed-channel	600
floor	601
hostname	602
interface Dot11Radio	603
led	605
link	606
link-probing-duration	607
keepalive-timeout	608
localpower	609
location	611
mac-address	612
mimo-mode	613
mode	615
model	616
n-only-mode	617
parent-ap	618
power-supply	620

preamble-short	622
protection-cts-mode	623
protection-mode	624
rfband	625
rf-mode	626
role	627
show ap	629
show ap-connectivity	632
show ap-discovered	634
show ap-redirect	636
show ap-swap	637
show ess-ap	638
show interfaces Dot11Radio	639
show interfaces Dot11Radio antenna-property	641
show interfaces Dot11Radio statistics	644
show regulatory-domain	649
show statistics ap300-diagnostics	650
show statistics station-per-ap	652
show statistics top10-ap-problem	653
show statistics top10-ap-talker	655
show topoap	657
show topoapap	658
swap ap	660
type	663

メッシュ コマンド.....	665
admin-mode.	666
descr	667
mesh-ap.	668
mesh-profile.	669
plugnplay	670
psk	671
不正 AP 検出コマンド.....	673
rogue-ap acl.	674
rogue-ap aging	675
rogue-ap assigned-aps	676
rogue-ap blocked.	677
rogue-ap detection.	679
rogue-ap min-rssi.	680
rogue-ap mitigation	681
rogue-ap mitigation-frames	682
rogue-ap operational-time	683
rogue-ap scanning-channels	684
rogue-ap scanning-time.	686
show rogue-ap acl	687
show rogue-ap blocked	688
show rogue-ap globals	689
show rogue-ap-list	690
サービス品質コマンド	691

action	693
avgpacketrates	694
dscp	695
dstip	696
dstip-flow	697
dstip-match	698
dstmask	699
dstport	700
dstport-flow	702
dstport-match	703
firewall-filter-id	704
firewall-filter-id-flow	706
firewall-filter-id-match	708
netprotocol-flow	710
netprotocol-match	711
packet max-length	712
packet min-length	713
packet-min-length-flow	714
packet-min-length-match	715
peakrate	716
priority	717

qoscodec	718
qosrule	722
qosrule-logging-frequency	725
qosrulelogging	726
qosvars admission	727
qosvars bwscaling	729
qosvars cac-deauth	730
qosvars calls-per-ap	731
qosvars calls-per-bssid	732
qosvars calls-per-interference	733
qosvars drop-policy	734
qosvars enable	735
qosvars intercell-periodicity	737
qosvars load-balance-overflow	738
qosvars max-stations-per-radio	739
qosvars max-stations-per-bssid	740
qosvars sip-idle-timeout	741
qosvars station-assign-age	742
qosvars tcpttl	743
qosvars ttl	744
qosvars udpttl	745
rspeccrate	746
rspecslack	747
srcip	748

srcmask	749
srcport	750
show phones	752
show phone-calls	753
show qoscodec	754
show qosflows	757
show qosrule	759
show qosstats	764
show qosvars	765
show statistics call-admission-control	767
tokenbucketrate	769
tokenbucketsize	771
trafficcontrol-enable	772
SNMP コマンド	773
reload-snmp	774
show snmp-community	775
show snmp-trap	776
show snmpv3-user	777
snmp-filter-config	778
snmpv3-user	779
snmpv3-user auth-key	780

snmpv3-user auth-protocol	781
snmpv3-user priv-key	782
snmpv3-user priv-protocol	783
snmpv3-user target ip-address	784
snmp start および snmp stop	785
snmp-server community	786
snmp-server contact	787
snmp-server description	788
snmp-server location	789
snmp-server trap	790
show snmp-filter-config	791
ステーション用コマンド	793
associated-station-max-idle-period	795
no station	796
show ap-assigned	797
show dot11 associations	799
show dot11 statistics client-traffic	801
show static-station	804
show station-log-config	805
show station commands	807
show station	809
show station 802.11	811
show station all	813
show station counter	815

show station details	817
show station general	822
show station mac-address	825
show station multiple-ip	827
show station network	828
show station security	831
show statistics station-per-ap	834
show statistics top10-station-problem	836
show statistics top10-station-talker	838
show topostaap	840
show topostation	841
static-station	843
station-aging-out-interval	844
station-log	847
(station-log) enable	850
(station-log) filelog	851
(station-log) syslog	852
(station-log) event id	853
(station-log) event severity	855
(station-log) show filters	857
station-log show	859

サービス コントロール コマンド	861
blocked-gateway	862
policy	863
service-type	865
service-control-config active-discovery	866
service-control-config essids	867
service-control-config gateways	868
service-control-config locations	869
service-control-config service-types	870
service-control-config state	871
service-control-config vlans	872
show service-control blocked-gateway	873
show service-control global-config	874
show service-control global-config-service	875
show service-control global-discovered-service	876
show service-control global-discovered-service-summary	877
show service-control location	878
show service-control policy	879
show service-control policy-config-service	880
show service-control policy-service	881
show service-control policy-service-summary	882
show service-control service-type	883
show service-control user-group	884
user-group	885

トラブルシューティング コマンド	887
analyze-capture	889
auto-report admin	890
auto-report send	892
capture-packets	894
debug captive-portal	901
debug connect	902
debug controller	903
debug eap	904
debug mac-filter	905
debug module	906
(diag-log) admin	910
(diag-log) config	912
(diag-log) restore	914
diagnostics	916
diagnostics-ap	918
diagnostics-controller	920
packet-capture-profile	922
(packet capture profile) ap-list	925
(packet capture profile) capture-sibling-frames	927
(packet-capture-profile) enable-profile	934

(packet capture profile) filter	936
(packet capture profile) interface list	937
(packet capture profile) mode	938
(packet capture profile) packet-truncation-length	940
(packet capture profile) rate-limiting	941
(packet capture profile) rate-limiting-mode	943
(packet capture profile) rxtx	944
(packet capture profile) token-bucket-rate	946
(packet capture profile) token-bucket-size	949
remote-log	952
show auto-report-config	953
show cef	955
show debug	956
show diag-log-config ap/controller/station	957
show packet-capture-profile	963
show statistics AP300-diagnostics	965

1 本ガイドについて

本ガイドでは、フォーティネット コントローラのコマンドライン インタフェース (CLI) で実行する FortiWLC (SD) コマンドについて詳しく説明します。このコマンド リファレンスの各章には、AP を管理する、あるいはシステムのセキュリティを設定するためのコマンドなどの関連コマンドのリストが含まれます。このガイドの最後には、FortiWLC (SD) で利用できるすべてのコマンドをアルファベット順に表示しています。このリストにあるコマンドのページ番号をクリックすると、そのコマンドの説明に移動できます。

このガイドは、各コマンドを使用するときに参照してください。各種のコマンドを組み合わせ使用して、ワイヤレス LAN のシステム セキュリティの設定や ESSID の設定などのシステム タスクを完了する方法を習得するために、『FortiWLC (SD) 設定ガイド』を合わせて参照してください。設定ガイドとコマンド リファレンスは同じ章構成になっており、詳細な参照情報、説明、そしてシステムの設定と保守タスクを実行するための手順を確認できます。



本ガイドで説明されていない機能やオプションはサポートされません。

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と、フォーティネット ワイヤレス LAN システム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

関連マニュアル

- 『FortiWLC (SD) リリース ノート』
- 『FortiWLC (SD) 設定ガイド』

外部の参考資料

- Stevens, W. R. 著、出版年 : 1994 年 『TCP/IP Illustrated, Volume 1, The Protocols』 Addison-Wesley, Reading, Mass.
- Gast, M.S. 著、出版年 : 2002 年 『802.11 Wireless Networks, The Definitive Guide』 O'Reilly and Associates, Sebastopol, Calif.

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。
<i>斜体</i>	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。
help	コマンドへの相互リンクを示します。リンクをクリックするとそのコマンドの説明が表示されます。
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。

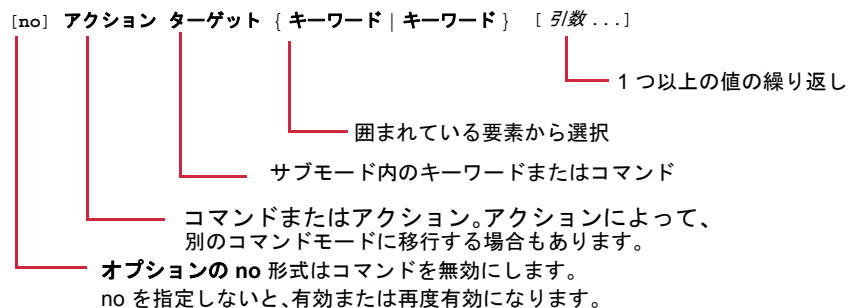
構文表記

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。
<i>斜体</i>	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。



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。

フォーティネットへのお問い合わせ

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。

<http://www.fortinet.com>

[Support] メニュー ボタンをクリックすると、フォーティネットのカスタマ サービス & サポートの情報をご覧いただけます。

2 重要な概念

本章では、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 \(41 ページ\)](#)
- [CLI コマンド モード \(42 ページ\)](#)
- [コマンドラインのみのコマンド \(43 ページ\)](#)
- [コマンドの省略形 \(45 ページ\)](#)
- [コマンドの no フォームと default フォームの使用 \(46 ページ\)](#)
- [ヘルプの表示 \(47 ページ\)](#)
- [コマンド ヒストリの使用 \(48 ページ\)](#)
- [show コマンドの出力における語句の検索 \(49 ページ\)](#)
- [CLI プロンプトのカスタマイズ \(50 ページ\)](#)
- [端末特性の操作 \(50 ページ\)](#)
- [セッションの終了 \(51 ページ\)](#)
- [パスワードでのスペースの使用 \(51 ページ\)](#)

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 アドレスを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、admin というユーザ ID が設定されていて、guest ユーザは無効です。

- 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` 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 ftp|scp|sftp *username*
- ip ftp|scp|sftp *password*
- 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
- packet-capture-profile
- poweroff
- show calendar
- show timezones
- show file systems
- show memory
- show controller cpu-utilization
- show processes
- show flash
- show high-availability
- show qosflows
- show scripts
- show station details
- show syslog-host
- show log
- autochannel
- high-availability
- 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。

```
controller# 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 :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index       : 1
Re-Key Period (seconds)    : 0
```

Captive Portal	: disabled
802.1X Network Initiation	: off
Shared Key Authentication	: off
Pre-shared Key (Alphanumeric/Hexadecimal)	: *****
Group Key Interval (Seconds)	: 0
PMK Caching	: disabled
Key Rotation	: disabled
Reauthentication	: off
MAC Filtering	: off
Firewall Capability	: none
Firewall Filter ID	:
Security Logging	: off

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	: 0
Re-Key Period (seconds)	: 0
Enable Multicast Re-Key	: off
Enable Captive Portal	: disabled
802.1X Network Initiation	: off
Enable Shared Key Authentication	: off
Pre-shared Key (Alphanumeric/Hexadecimal)	: *****
Enable Reauthentication	: off
MAC Filtering	: on

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。

- 特性あるいは機能を無効にする。
- コマンドをデフォルトにリセットする。
- コマンドのアクションを逆にする。
- **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。これらの条件については、コマンドのリファレンス ページで説明します。いくつかの例を下記に示します。

```
corpwifi# default history
corpwifi# default terminal length
corpwifi# default terminal width
```

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?	現在のモードで利用できる、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にまで省略できます。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 は履歴 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、履歴 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。

履歴 バッファの内容を表示するには、`default history` と入力します。

```
controller# default history
```

履歴 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
AP201	Local				None

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
prompt 文字列	CLI プロンプトをカスタマイズします。
no prompt	CLI プロンプトの表示を無効にします。
default prompt	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
```

端末画面の長さと幅のセット

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
```

端末の長さと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
```

パスワードでのスペースの使用

CLI インターフェイスでは制限があり、スペースを使用するパスワード フレーズを入力すると、ユーザに対して認証が要求される場合があります。しかし、これらのパスワードは Web UI では簡単に変更でき、スペースも明確に追加できます。ただし、パスワード フレーズを引用符で囲むと、CLI でもパスワードにスペースを追加できます。

```
default(15)# password "sample password"  
default(15)#
```

パスワードは引用符なしで入力するため、実際に設定されるパスワードは、上記では **sample password** の部分になります。

3 ユーザ インターフェイス コマンド

本章では、プロンプト (画面) の変更、端末の履歴、機能の表示などのユーザ インターフェイスの設定に関するコマンドについて説明します。また、ヘルプの表示や終了、各種のコマンド レベルに入るためのコマンドについて説明します。

- [?](#) (54 ページ)
- [disable](#) (55 ページ)
- [do](#) (56 ページ)
- [enable](#) (57 ページ)
- [end](#) (58 ページ)
- [exit](#) (59 ページ)
- [help](#) (60 ページ)
- [prompt](#) (62 ページ)
- [quit](#) (63 ページ)
- [show history](#) (64 ページ)
- [show terminal](#) (65 ページ)
- [terminal history](#) (66 ページ)
- [terminal history size](#) (67 ページ)
- [terminal length](#) (68 ページ)
- [terminal width](#) (69 ページ)

?

使用されるコマンド レベルに適用可能なサブコマンドのリストを表示します。

構文

?

コマンド モード

すべて

デフォルト

用途

CLI の各レベルで ? を入力するとヘルプが表示されます。各レベルで ? を使用すると、すべてのコマンドのリストが表示されます。各コマンドの後で ? を使用すると、適用可能なサブコマンドとオプションのリストが表示されます。

使用例

```
controller> ?
```

debug	Turns on debugging.
default	Reset to default values.
enable	Enables privileged mode.
exit	Exit the CLI.
help	Displays help information.
no	Disables various parameters.
prompt	Customizes the CLI prompt.
quit	Exit the CLI.
show	Displays various system parameters.
terminal	Displays or sets terminal characteristics.

関連コマンド

[help \(60 ページ\)](#)

disable

特権 EXEC モードを終了し、ユーザ EXEC モードを開始します。

構文

disable

コマンドモード

ユーザ EXEC

デフォルト

なし

用途

特権 EXEC モードで作業している際に、**disable** コマンドを使用してユーザ EXEC モードを開始します。プロンプトは、特権 EXEC モードの場合に # となり、ユーザ EXEC モードでは > に変わります。

使用例

以下のコマンドは、特権 EXEC モードを終了し、ユーザ EXEC モードを開始します。

```
controller# disable  
controller>
```

関連コマンド

[enable](#) (57 ページ)

do

任意のコマンド モードから CLI コマンドを実行します。

構文

do <command>

command 実行する CLI コマンド モード。

コマンド モード

すべての設定モード

デフォルト

なし

用途

do コマンドを使用して、グローバル設定モードあるいはいずれかの設定サブモードから EXEC レベルコマンド (**copy**、**default**、**show** など) を実行します。

使用例

以下のコマンドは、特権 EXEC モードに戻らずに、ファイル startup-config に現在の設定を保存します。

```
controller(config)# do copy running-config startup-config
```

以下のコマンドは、コントローラの IP 設定を表示します。

```
controller(config)# do show ip
Interface Number IP Address      NetMask      Gateway Address
Assignment Type Interface Mode
1                172.26.0.53   255.255.240.0 172.26.0.1    DHCP
active

          IP Addresses(1 entry)
controller#
controller(config)#
```

enable

特権 EXEC モードを開始します。

構文

enable

コマンドモード

ユーザ EXEC

デフォルト

なし

用途

ユーザ EXEC モードで **enable** コマンドを使用して、特権 EXEC モードを開始します。EXEC モードを開始します。プロンプトは、ユーザ EXEC モードの場合に > となり、特権 EXEC モードでは # に変わります。

使用例

ユーザ EXEC モードで実行される以下のコマンドは、管理パスワードの入力後、特権 EXEC モードを開始します。

```
controller> enable
Password:
controller#
```

関連コマンド

[disable](#) (55 ページ)

end

設定モードを終了し、特権 EXEC モードを開始します。

構文

end

コマンド モード

デフォルト

なし

用途

大半の設定モードでは **end** コマンドを使用して、設定モードを終了し、特権 EXEC モードを再度開始します。

使用例

以下のコマンドを使用すると、セキュリティ プロファイルおよびグローバル設定モードが終了し、特権 EXEC モードに入ります。

```
controller(config-security)# end  
controller#
```

関連コマンド

[exit \(59 ページ\)](#)

exit

設定モードを終了して次に高位のモードを開始します。あるいはユーザ EXEC モードで CLI を終了します。

構文

`exit`

コマンドモード

すべて

デフォルト

用途

`exit` コマンドは、現在どのコマンド モードで操作しているかによって動作が異なります。いずれかの設定モードの場合、`exit` コマンドを使用して、モードを終了して次に高いモードを開始します。ユーザあるいは特権 EXEC モードの場合、`exit` コマンドを使用して、CLI を終了します。

使用例

以下のコマンドは、セキュリティ プロファイル設定モードを終了し、次に高いモード (グローバル設定モード) を開始します。

```
controller(config-security)# exit
controller(config)#
```

関連コマンド

[quit \(63 ページ\)](#)

help

各コマンドのヘルプを表示します。

構文

```
help
help <command>
```

command 指定したコマンドに関するヘルプを表示します。

コマンドモード

すべて

デフォルト

現在のコマンド レベルで利用可能なコマンドを一覧表示します。

用途

help コマンドは、現在のコマンド モードのシステム コマンドを一覧表示します。**help** コマンドは、**?** コマンドとは異なり、コマンドとサブコマンドのリストを表示します。コマンドの前に **help** を入力すると、そのコマンドの説明が表示されます。

使用例

```
controller(config)# help radius-profile
radius-profile:
Manage RADIUS servers.
```

以下の例は、**radius-profile** コマンド サブモードで利用可能なコマンドを表示しています。

```
meru-wifi(config-radius)# help
default          Set RADIUS profile parameters to default value.
description      Specifies the RADIUS node.
do               Executes an IOSCLI command.
end              Save changes, and return to privileged EXEC mode.
exit             Save changes, and return to global configuration mode.
help             Displays help information.
ip-address       Configures the IP address.
key              Configures the secret key.
mac-delimiter    Configures the MAC Delimiter.
no               Disabling RADIUS profile parameters.
password-type    Configures the RADIUS Password Type.
```

[関連コマンド](#) [?](#) (54 ページ)

prompt

CLI プロンプトを変更します。

構文

```
prompt <prompt-name>  
no prompt
```

prompt-name 新しいプロンプトの名前。

コマンド モード

特権 EXEC

デフォルト

デフォルトのプロンプト名は、*default* です。

用途

このコマンドを使用して、CLI のプロンプト名を変更します。**no prompt** コマンドを使用して、セッションの端末プロンプトを無効にします。

使用例

以下のコマンドは、プロンプト名を **default** から **controller** に変更します。

```
default# prompt controller  
controller#
```


quit

CLI を終了します。

構文

`quit`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

`quit` コマンドを使用して、CLI を終了します。

使用例

以下のコマンドは、CLI を終了します。

```
default# quit
```

関連コマンド

[exit](#) (59 ページ)

show history

このセッションで最近使用されたコマンドのリストを表示します。

構文

`show history`

コマンドモード

ユーザおよび特権 EXEC モード

デフォルト

デフォルトのヒストリ サイズは 10 です。

用途

`show history` コマンドを使用して、最近入力したコマンドを表示します。ヒストリ バッファが表示するコマンドの数は、`terminal history size` コマンドによって決定されます。

使用例

以下のコマンドは、このセッションで入力された最新の 10 個のコマンドを表示します。

```
default> show history
 26 access-list permit import acl
 27 exit
 28 show access-list permit
 29 configure terminal
 30 access-list deny on
 31 exit
 32 show access-list deny
 33 disable
default>
```

関連コマンド

[*terminal history size*](#) (67 ページ)

show terminal

端末設定を表示します。

構文

`show terminal`

コマンドモード

ユーザおよび特権 EXEC モード

デフォルト

なし

用途

長さ、幅、バッファ サイズを含む、現在の端末の設定を表示します。

使用例

以下のコマンドは、端末設定を表示します。

```
controller# show terminal
Terminal Length:      50
Terminal Width:       80
History Buffer Size:   10
controller#
```

関連コマンド

- [terminal history \(66 ページ\)](#)
- [terminal history size \(67 ページ\)](#)

terminal history

入力されたコマンドの履歴を表示します。

構文

```
terminal history  
no terminal history
```

コマンド モード

ユーザおよび特権 EXEC モード

デフォルト

デフォルトの履歴 バッファ サイズは 10 です。

用途

この端末での最新の 10 個のコマンドを表示します。**no** フォームを使用すると、現在のセッションでこの機能が無効になります。

使用例

以下のコマンドを指定すると、この端末で最新使用された 10 個のコマンドが表示されます。

```
controller# terminal history  
15 prompt default  
16 show terminal  
17 show terminal  
18 terminal history  
19 show terminal  
20 terminal  
21 show terminal  
22 show terminal  
22 terminal history  
23 show terminal  
controller#
```

関連コマンド

- [show terminal \(65 ページ\)](#)
- [terminal history size \(67 ページ\)](#)

terminal history size

ヒストリ バッファに記録される行数を変更します。

構文

`terminal history size <historysize>`

`no terminal history`

historysize ヒストリ バッファに記録される行数。有効な値は 0 ～ 1,000 です。

コマンド モード

ユーザ EXEC

デフォルト

デフォルトのヒストリ サイズは 10 です。

用途

端末に表示する行数を変更します。ゼロ (0) を指定すると、表示されるヒストリ行数が「なし」になります。**no terminal history** コマンドを使用すると、ヒストリ機能が無効になります。

使用例

以下のコマンドを指定すると、ヒストリ バッファ サイズが変更され、最新の 33 個のコマンドが保存されます。

```
controller# terminal history size 33
controller#
controller# show terminal
Terminal Length:      10
Terminal Width:       80
History Buffer Size:   33
```

関連コマンド

- [show terminal](#) (65 ページ)
- [terminal history](#) (66 ページ)

terminal length

端末に表示する行数を調整します。

構文

`terminal length <length>`

length 端末に表示する行数。有効な範囲は 0 ～ 256 です。

コマンド モード

ユーザおよび特権 EXEC モード

デフォルト

ゼロ (0) 行。

用途

端末の行数を表示します。このパラメータを 0 に設定すると、1 行ずつ表示されます。0 より大きな数を設定すると、ブロックまたはグループ長で表示されます。

使用例

```
controller# terminal length 100
controller#
```

関連コマンド

[*terminal width*](#) (69 ページ)

terminal width

端末に表示するカラム数を調整します。

構文

```
terminal width <width>
```

width 端末に表示するカラム数。有効な範囲は 0 ～ 80 です。

コマンド モード

ユーザおよび特権 EXEC モード

デフォルト

ゼロ (0) 行。

用途

端末のカラム数を表示します。このパラメータを 0 に設定すると、1 カラムずつ表示されます。

使用例

```
controller# terminal width 60  
controller#
```

関連コマンド

[*terminal length*](#) (68 ページ)

4 ファイル管理コマンド

本章では、システム イメージおよびバックアップ設定ファイルなどのシステム ファイルの管理に使用するコマンドについて説明します。設定の保存、FortiWLC (SD) バージョンのアップグレードおよびダウングレード、設定を正しく理解して管理するための情報を表示する各コマンドについても説明します。

- [cd \(72 ページ\)](#)
- [copy \(73 ページ\)](#)
- [copy running-config \(75 ページ\)](#)
- [delete \(77 ページ\)](#)
- [dir \(79 ページ\)](#)
- [downgrade \(81 ページ\)](#)
- [more \(82 ページ\)](#)
- [pwd \(84 ページ\)](#)
- [rename \(85 ページ\)](#)
- [run \(86 ページ\)](#)
- [show controller file systems \(87 ページ\)](#)
- [show flash \(89 ページ\)](#)
- [show running-config \(90 ページ\)](#)
- [show startup-config \(91 ページ\)](#)
- [show scripts \(92 ページ\)](#)
- [upgrade ap \(93 ページ\)](#)
- [upgrade controller \(95 ページ\)](#)
- [upgrade system \(97 ページ\)](#)

cd

現在の作業ディレクトリを設定します。

構文

```
cd  
cd <directory>
```

<i>directory</i>	現在の作業ディレクトリとして設定するディレクトリの名前。
------------------	------------------------------

コマンドモード

特権 EXEC

デフォルト

デフォルトの作業ディレクトリは `images` です。

用途

`cd` を単独で入力すると、デフォルトの作業ディレクトリ (`images`) に変更します。また、ディレクトリ名を指定して `cd` を使用すると、現在の作業ディレクトリを次のいずれかのディレクトリに設定します。

<code>ATS/scripts</code>	AP ブート スクリプトが格納されているディレクトリ
<code>capture</code>	パケット捕捉ファイルを含むディレクトリ
<code>images</code>	アップグレード イメージを含むディレクトリ。

使用例

以下のコマンドは、`ATS/scripts` ディレクトリに移動して、変更を確認して、デフォルトの `images` ディレクトリに戻ります。

```
controller# cd ATS/scripts  
controller# pwd  
ATS/scripts  
controller# cd  
controller# pwd  
images
```

関連コマンド

- [dir \(79 ページ\)](#)
- [pwd \(84 ページ\)](#)

copy

ファイルをローカルおよびリモートでコピーします。

構文

```
copy filename ftp://<username>:<password>@server/filename ( ファイルをリモートにコピー )  
copy ftp://<username>:<password>@server/filename .( リモート ファイルをローカルにコピー )  
copy filename scp://<username>:<password>@server/directory/filename ( ファイルをリモートにコピー )  
copy sftp://<username>:<password>@server/filename .( リモート ファイルをローカルにコピー )  
copy filename tftp://server/filename ( ファイルをリモートにコピー )  
copy tftp://server/filename( リモート ファイルをローカルにコピー )
```

filename	リモートまたはローカル ファイルの名前。
ftp:// <username>:<password> @server	FTP を使用し、そのサーバで有効なユーザ名を使用して、コントローラとサーバ間でファイルを転送します。パスワードを指定できます。指定しないと、パスワードを入力するよう要求されます。
scp://username@server	SCP を使用し、そのサーバで有効なユーザ名を使用して、コントローラとサーバ間でファイルを転送します。
sftp:// <username>:<password> @server	SFTP を使用し、そのサーバで有効なユーザ名を使用して、コントローラとサーバ間でファイルを転送します。パスワードを指定できます。指定しないと、パスワードを入力するよう要求されます。
tftp://server/	TFTP を使用して、コントローラとサーバ間でファイルを送信します (ユーザ名は不要)。

コマンドモード

特権 EXEC

デフォルト

なし

用途

FTP あるいは SSH サーバが存在するリモート ファイル システムで、コントローラへ、またはコントローラからファイルをコピーします。

使用例

最初のコマンドにより FTP を使用して、user1@server1/home/backup/ にファイル dflt_backup.dbu がコピーされます 2 番目のコマンドにより、リモートバックアップファイルがローカルディレクトリにコピーされます。(ドット) は、コピーされるファイル名のショートカットです (dflt_backup.dbudflt_backup.dbu)。

```
controller# copy dflt_backup.dbu ftp://user1@server1/home/backup/  
dflt_backup.dbu
```

FTP password:

```
controller#
```

```
controller# copy ftp://user1@server1/home/backup/dflt_backup.dbu .
```

FTP password:

```
controller#
```

copy running-config

実行中の設定をローカル フラッシュあるいはリモート システムにコピーします。

構文

```
copy running-config startup-config
copy running-config ftp://username<:password>@server/directory/filename
copy running-config scp://username<:password>@server/directory/filename
copy running-config tftp://server/directory/filename
copy filename running-config
```

ftp://	FTP を使用し、そのサーバで有効なユーザ名を使用して、コ
username<:password>@s	ントローラとサーバ間でファイルを転送します。パスワードを
server	指定できます。指定しないと、パスワードを入力するよう要求
	されます。
scp://username@server	SCP を使用し、そのサーバで有効なユーザ名を使用して、コ
	ントローラとサーバ間でファイルを転送します。
tftp://server/	TFTP を使用して、コントローラとサーバ間でファイルを 送信
	します (ユーザ名は不要)。
startup-config	設定を開始します。
filename	running-config への出力あるいは入力として使用するファイル
	のファイル名。

コマンド モード

特権 EXEC

デフォルト

デフォルトは現在実行中の設定です。

用途

copy running-config コマンドを使用して、現在実行中の設定をシステムを起動する **startup-config** によって開始されるローカル フラッシュ設定ファイル、あるいはバックアップとして使用するリモート サーバにコピーします。リモート サーバをコピーに使用する場合、ファイルは FTP、SFTP、SCP あるいは TFTP を使用して転送できます。送信先のファイル名はユーザが選択可能です。

このコマンドは、入力ファイルのコマンドに対する実行中の設定を変更する、**running-config** への入力として、ファイル名を受け付けます。

リモート ロケーションからファイルを取り込むには、**copy** コマンドを使用します。

使用例

以下のコマンドは、いずれかの FTP を使用して、現在実行中の設定を user1@server1/home/backup/ にコピーします。

```
controller# copy running-config ftp://user1:mypwd@server1/home/backup/  
running-config
```

関連コマンド

[copy](#) (73 ページ)

delete

システムからファイルを削除するか、システムのイメージをアップグレードします。

構文

```
delete <filename>  
delete flash: <filename>
```

filename	削除するファイルの名前。
flash: filename	削除するアップグレード イメージの名前。

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、ファイルあるいはアップグレード イメージを削除します。このコマンドは、イメージ ディレクトリにダウンロードされている古く 不要になったイメージ ファイルを削除して、フラッシュ カードの容量を確保する場合に役立ちます。**dir** コマンドや **show flash** コマンドを使用して、イメージ ディレクトリに保存されているファイルを確認します。

使用例

以下のコマンド シーケンスは **capture** ディレクトリの内容を表示し、ファイル **my_capture_file** を削除し、再度ディレクトリの内容を表示します。

```
controller# cd capture  
controller# pwd  
/capture  
  
controller# dir  
dir  
total 1  
-rw-r--r--    1 root    root        28658 May 14 12:02 my_capture_file  
controller# delete my_capture_file  
controller# dir  
total 0
```

以下のコマンドはフラッシュ メモリからファイル 3.0-139 を削除します。

```
controller# delete flash: 3.0-139
controller#
```

関連コマンド

- [dir](#) (79 ページ)
- [pwd](#) (84 ページ)
- [show flash](#) (89 ページ)

dir

ディレクトリの内容を表示します。

構文

```
dir
dir <directory>
```

directory 表示するディレクトリの名前。

コマンド モード

特権 EXEC

デフォルト

現在の作業ディレクトリを表示します。

用途

dir を使用して、現在のディレクトリ内容の詳細なリストを表示します。オプションの *directory* 引数を使用して、その他のディレクトリを指定します。オプションのディレクトリには以下が含まれます。

```
ATS/scriptsThe directory containing the AP boot scripts.
backupThe directory containing the backup databases.
captureThe directory containing packet capture files.
imagesThe directory containing the system images.
scriptsThe directory containing the controller scripts.
```

使用例

以下のコマンドは現在のディレクトリ名およびその内容を表示します。

```
controller# dir
total 70
drwxr-xr-x   8 root      root          1024 Jan 30 19:00 meru-3.5-45
drwxrwxr-x   8 522      522          1024 Feb 21 19:34 meru-3.5-46
-rw-r--r--   1 root      root          3195 Feb 19 10:17 meru.user-
diagnostics.Dickens.2008-02-19.02-17-17.tar.gz
-rw-r--r--   1 root      root          3064 Feb 21 08:50 meru.user-
diagnostics.Dickens.2008-02-21.00-50-50.tar.gz
-rw-r--r--   1 root      root          2635 Feb 21 10:12 meru.user-
diagnostics.Dickens.2008-02-21.10-12-54.tar.gz
-rw-r--r--   1 root      root          3336 Mar  5 05:54 meru.user-
diagnostics.Dickens.2008-03-05.05-54-51.tar.gz
-rw-r--r--   1 root      root          2398 Feb 22 10:24 meru.user-
diagnostics.default.2008-02-22.10-24-42.tar.gz
```

```

lrwxrwxrwx    1 root    root      28 Feb 21 08:50 mibs.tar.gz -> meru-
3.5-46/mibs/mibs.tar.gz
-rw-r--r--    1 root    root     16778 Feb 21 08:50 pre-upgrade-config
-rw-r--r--    1 root    root     18588 Mar  6 02:56 script.log
-rw-r--r--    1 root    root     11172 Mar  5 05:59 startup-config
-rw-----    1 root    root      1915 Feb 21 08:50 upgrade.log
controller# dir scripts
total 2
-rw-r--r--    1 root    root     1239 Feb 21 19:16 create_rules.cli
controller#

```

関連コマンド [pwd \(84 ページ\)](#)

downgrade

システムをダウングレードします。

構文

`downgrade system version`

コマンド モード

特権 EXEC

デフォルト

なし

用途

システムに以前にインストールされていたイメージに戻す場合に、`downgrade system` コマンドを使用します。このダウングレードは、コントローラとすべての AP に影響を及ぼします。

`show flash` コマンドを使用してダウングレードできるシステム イメージのリストを表示します

使用例

以下のコマンドにより、システムがダウングレードされます。

```
controller# downgrade system 3.2-116
```

関連コマンド

- [show flash \(89 ページ\)](#)
- [upgrade system \(97 ページ\)](#)

more

詳細なファイルあるいはシステム情報を表示します。

構文

```
more running-config
more startup-config
more running-script
more file <pathname>
more log
```

コマンド モード

特権 EXEC

デフォルト

用途

このコマンドを使用して、running-config、startup-config、およびシステム ログ (syslogd.log) に含まれるようなシステム設定に関するさまざまな詳細情報を呼び出します。file キーワードを使用して、表示するファイルの完全なパス名を指定します。more running-config コマンドは、show running-config コマンドと 同義です。

コマンドを停止するには、Ctrl-C を押します。

使用例

次に示すのは running-config 出力の一部です。

```
default# more running-config
configure terminal
no ip dhcp-passthrough
audit period 60
auto-ap-upgrade enable
optimization none
hostname meru-wifi
ip dhcp-server 10.0.0.10
ip address 192.168.10.2 255.255.255.0
ip default-gateway 192.168.10.1
ip domainname 10.0.0.10
qosvars admission admitall
qosvars ttl 0
qosvars udpttl 0
```

```
qosvars tcpttl 0
qosvars enable
qosvars bwscaling 100
qosvars intercell-periodicity 30
qosvars drop-policy head
rogue-ap detection
rogue-ap acl 00:0c:e6:02:9e:6f
rogue-ap acl 00:0c:e6:03:5f:67
rogue-ap acl 00:0c:e6:04:5f:67
rogue-ap acl 00:0c:e6:05:b0:7a
rogue-ap acl 00:0c:e6:06:26:df
rogue-ap acl 00:0c:e6:07:17:d5
rogue-ap acl 00:0c:e6:08:e9:29
```

関連コマンド [show running-config \(90 ページ\)](#)

pwd

現在の作業ディレクトリを表示します。

構文

`pwd`

コマンド モード

特権 EXEC

デフォルト

現在の作業ディレクトリです。

用途

このコマンドを使用して、現在の作業ディレクトリのフルパス名を確認します。

使用例

```
controller# pwd
images
controller#
```

関連コマンド

[dir](#) (79 ページ)

rename

ローカル ファイルの名前を変更します。

構文

rename <source> <file_dst>

source

名前を変更する元のファイルの名前。

file_dst

変更先の名前、つまりファイル名の新しい名前。

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、ファイルの名前を変更します。

使用例

以下のコマンドは dflt_backup.mbu というファイル名を default_backup.mbu に変更します。

```
controller# rename dflt_backup.mbu default_backup.mbu
controller#
```

関連コマンド

[dir](#) (79 ページ)

run

指定されたスクリプトを実行します。

構文

run <script_file>

script_file 実行するスクリプトのフルパス名。

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、テストまたはその他の診断アプリケーションを実行し、画面にその結果を表示します。

使用例

```
controller# cd ATS/scripts
controller# dir
total 4
-rw-rw-r-- 1 root root 3922 Jan 13 10:05 jan01-config
controller# run jan01-config
```


show controller file systems

コントローラ ファイル システムに関する情報を表示します。

構文 `show controller file systems`

コマンド
モード 特権 EXEC

デフォルト なし

用途 このコマンドはシステム ディレクトリとファイル システムについての情報を表示します。以下の情報が提供されます。

表 3: *show controller file systems* の出力

パラメータ	説明
Filesystem	ファイル システムの名前を表示します。ディレクトリの場合、 none を表示します。
1K blocks	ファイル システムまたはディレクトリが使用するように設定されている 1K バイト ブロック数を表示します。
Used	ファイル システムまたはディレクトリが現在使用している 1K バイト ブロック数を表示します。
Available	ファイル システムまたはディレクトリが使用可能な 1K バイト ブロック数 (空きスペース) を表示します。
Use %	ファイル システムまたはディレクトリが現在使用している使用可能なブロックの割合 (%) を表示します。
Mounted on	ファイル システムがマウントされているマウント ポイントを表示するか、ディレクトリのパス名をリストします。

使用例 以下のコマンドはシステム ファイルに関する情報を表示します。

`controller# show controller file systems`

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/hda2	428972	230456	175630	57%	/
none	4880	40	4840	1%	/dev/shm
none	19528	6256	13272	33%	/opt/meru/var/run
none	9764	2944	6820	31%	/opt/meru/var/log
none	9764	896	8868	10%	/tmp
none	9764	0	9764	0%	/opt/meru/capture

controller#

関連コマンド

show flash

システム イメージ ファイル名をフラッシュ メモリに表示します。

構文

`show flash`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、フラッシュ イメージ ファイル名を表示します。

使用例

以下のコマンドはフラッシュ イメージ ファイル名を表示します。

```
controller# show flash
```

```
5.0-87
```

```
5.1-47
```

```
controller#
```

show running-config

現在のコントローラ設定を表示します。

構文

`show running-config`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、現在のシステム設定パラメータを表示します。

関連コマンド

[more \(82 ページ\)](#)

show startup-config

コントローラのスタートアップ設定を表示します。

構文

`show startup-config`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、コントローラのスタートアップ設定を表示します。この設定はコントローラが起動するときに使用されます。

関連コマンド

- [copy running-config \(75 ページ\)](#)
- [more \(82 ページ\)](#)

show scripts

有効な AP スクリプトを表示します。

構文

show scripts

コマンド モード

EXEC

デフォルト

なし

用途

このコマンドを使用して、有効な AP スクリプト (たとえば、AP を起動する起動スクリプト) の名前を表示します。以下の例は、スクリプトのコピーを記述し、さらにコピーが完了した後のスクリプトを示しています。

使用例

以下の例は、スクリプトのコピーを記述し、さらにコピーが完了した後のスクリプトを示しています。

```
controller# cd ATS/scripts
controller# copy scp://jsmith@server2/home/jsmith/default-ap .
SCP Password:
default-ap          100% |*****| 3          00:00
controller# show scripts
default-ap
controller#
```

upgrade ap

アクセス ポイントのシステム イメージをアップグレードします。

構文

```
upgrade ap <version>  
upgrade ap same <id>  
upgrade ap same <range>  
upgrade ap same all
```

version

アップグレード時に使用される FortiWLC (SD) システム イメージのバージョン。

same <id | range | all>

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。

- *id* - 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。
- *range* - 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。
- *all* - 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。

コマンド モード

特権 EXEC

デフォルト

なし

用途

アクセス ポイントのシステム イメージをアップグレードする前に、圧縮したイメージをコントローラの images ディレクトリに転送します。アップグレードする前に、イメージが images ディレクトリに存在している必要があります。**dir** コマンドを使用して、ディレクトリ内のイメージを確認します。

copy コマンドを使用して、新規のイメージ ファイルを転送します。たとえば、FTP を使用してファイルを転送するには、以下を入力します。

```
controller# copy ftp://jane@10.1.1.1/meru-3.2.tar .
```

ip ftp password コマンドを使用してデフォルト FTP パスワードの設定を完了していない場合は、パスワードの確認画面が表示されます。

ファイルが正常に送信されたことを確認するには、以下を入力します。

```
controller# show flash
3.2
```

範囲を指定することもできます。

使用例

以下のコマンドは、ID が 1、7、および 10 のアクセス ポイントをバージョン 3.3 にアップグレードします。

```
controller# upgrade ap 3.3 1,7,10
```

以下のコマンドは、ID が 4、7、10、12 ~ 20 までのアクセス ポイントをバージョン 3.3 にアップグレードします。

```
controller# upgrade ap 3.3 4-7,10,12-20
```

以下のコマンドは、すべてのアクセス ポイントを、コントローラが実行中のシステム イメージと同じバージョンにアップグレードします。

```
controller# upgrade ap same
```

```
This will overwrite all existing system images.Are you sure [y|n]? y
```

アップグレード プロセスが表示されます。アップグレードが成功すると、以下のようなメッセージが表示されます。

```
Upgrading APs
  1 AP-1          |=====| Success
controller#
```

関連コマンド

[upgrade system \(97 ページ\)](#)

upgrade controller

コントローラのシステム イメージをアップグレードします。

構文

```
upgrade controller <version>  
upgrade controller <version> force
```

<i>version</i>	アップグレード時に使用されるシステム イメージのバージョン。
<i>force</i>	アップグレードを強制します。適用パッチを戻す必要がある場合など現在実行中のバージョンにアップグレードする場合に必要です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

コントローラのシステム イメージをアップグレードする前に、コントローラの /images ディレクトリに圧縮バージョンを転送する必要があります。dir コマンドを使用して、現在のコントローラのディレクトリを確認します。

copy コマンドを使用して、新規のイメージ ファイルを転送します。たとえば、FTP を使用してファイルを転送するには、以下を入力します。

```
controller# copy ftp://jane@10.1.1.1/meru-5.1.tar .
```

ip ftp password コマンドを使用してデフォルト FTP パスワードの設定を完了していない場合は、パスワードの確認画面が表示されます。

ファイルが正常に送信されたことを確認するには、以下を入力します。

```
controller# show flash  
5.1
```

使用例

以下のコマンドはコントローラのシステム イメージをバージョン 5.1 にアップグレードします。

```
controller# upgrade controller 5.1-xx  
This will overwrite all existing system images.Are you sure [y|n]? y  
Upgrading Controller
```

```
Stopping FortiWLC (SD) services ...  
Upgrading the current configuration ...  
Upgrade complete.
```

```
Broadcast message from root (pts/0) (Fri Mar 10 14:51:59 2004):
```

```
Now rebooting system...  
The system is going down for reboot NOW!  
default#
```

関連コマンド

- [upgrade ap](#) (93 ページ)
- [upgrade system](#) (97 ページ)

upgrade system

コントローラおよびすべてのアクセス ポイントをアップグレードします。

構文

`upgrade system <version>`

version アップグレード時に使用されるシステム イメージのバージョン。

コマンド モード

グローバル設定

デフォルト

なし

用途

コントローラのシステム イメージをアップグレードする前に、コントローラの `/images` ディレクトリに圧縮バージョンを転送する必要があります。**dir** コマンドを使用して、現在のコントローラのディレクトリを確認します。

copy コマンドを使用して、新規のイメージ ファイルを転送します。たとえば、FTP を使用してファイルを転送するには、以下を入力します。

```
controller# copy ftp://jane@10.1.1.1/meru-5.1.tar .
```

ip ftp password コマンドを使用してデフォルト FTP パスワードの設定を完了していない場合は、パスワードの確認画面が表示されます。

ファイルが正常に送信されたことを確認するには、以下を入力します。

```
controller# show flash
5.1
```

使用例

以下のコマンドは、システム イメージ バージョン 5.1 を使用するように、コントローラとすべてのアクセス ポイントをアップグレードします。

```
controller# upgrade system 5.1
This will overwrite all existing system images.Are you sure [y|n]? y
Upgrading APs
  1 AP-1                      |                      | Success
Upgrading Controller
```

```
Stopping FortiWLC (SD) services ...  
Upgrading the current configuration ...  
Upgrade complete.
```

```
Broadcast message from root (pts/0) (Fri Mar 10 14:51:59 2004):
```

```
Now rebooting system...  
The system is going down for reboot NOW!  
controller#
```

関連コマンド

- [upgrade ap \(93 ページ\)](#)
- [upgrade controller \(95 ページ\)](#)


```
Upgrading Controller
Stopping FortiWLC (SD) services ...
Upgrading the current configuration ...
Upgrade complete.
```

```
Broadcast message from root (pts/0) (Fri Mar 10 14:51:59 2004):
```

```
Now rebooting system...
The system is going down for reboot NOW!
controller#
```

関連コマンド

- [upgrade ap \(93 ページ\)](#)
- [upgrade controller \(95 ページ\)](#)

5 システム管理コマンド

本章では、システム管理に使用するコマンドについて説明します。セットアップ スクリプトの実行、システム クロックやタイムゾーンの設定、およびシステムやネットワーク情報の収集などのタスクについて説明します。

- [10gig-module \(104 ページ\)](#)
- [aeroscout \(105 ページ\)](#)
- [alarm \(106 ページ\)](#)
- [amconfig \(109 ページ\)](#)
- [audit period \(110 ページ\)](#)
- [bonding \(111 ページ\)](#)
- [calendar set \(113 ページ\)](#)
- [clear statistics interfaces \(115 ページ\)](#)
- [client-locator \(116 ページ\)](#)
- [controller-index \(118 ページ\)](#)
- [date \(119 ページ\)](#)
- [erase-guest-user \(120 ページ\)](#)
- [event \(121 ページ\)](#)
- [fastpath \(124 ページ\)](#)
- [fingerprint \(125 ページ\)](#)
- [guest-user \(126 ページ\)](#)
- [hostname \(128 ページ\)](#)
- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [ip udp-broadcast upstream \(131 ページ\)](#)
- [ip udp-broadcast upstream-bridged \(132 ページ\)](#)
- [license \(133 ページ\)](#)
- [management wireless \(135 ページ\)](#)
- [nms-profile \(136 ページ\)](#)

- [nms-server](#) (137 ページ)
- [nms-vpn-server](#) (138 ページ)
- [ntp](#) (139 ページ)
- [passwd](#) (141 ページ)
- [ping](#) (142 ページ)
- [poweroff controller](#) (143 ページ)
- [proactive-spectrum-manager](#) (144 ページ)
- [proxy-arp-filtering](#) (147 ページ)
- [reload](#) (148 ページ)
- [reload-gui](#) (150 ページ)
- [reload-management](#) (151 ページ)
- [reload-security](#) (152 ページ)
- [reload-snmp](#) (153 ページ)
- [reload-vpn](#) (154 ページ)
- [reload-wapi](#) (155 ページ)
- [remove-license](#) (156 ページ)
- [roaming-domain](#) (157 ページ)
- [setup](#) (160 ページ)
- [setup](#) (160 ページ)
- [show alarm](#) (162 ページ)
- [show bonding](#) (168 ページ)
- [show calendar](#) (170 ページ)
- [show client-locator](#) (171 ページ)
- [show controller](#) (172 ページ)
- [show controller cpu-utilization](#) (177 ページ)
- [show controller file systems](#) (178 ページ)
- [show controller memory](#) (180 ページ)
- [show controller processes](#) (182 ページ)
- [show event](#) (185 ページ)
- [show fastpath](#) (187 ページ)
- [show features](#) (189 ページ)
- [show fingerprints](#) (190 ページ)
- [show flash](#) (191 ページ)
- [show guest-user](#) (192 ページ)

- [show hostname \(194 ページ\)](#)
- [show ip udp-broadcast downstream all-ports \(197 ページ\)](#)
- [show ip udp-broadcast downstream-bridged all-ports \(198 ページ\)](#)
- [show ip udp-broadcast upstream all-ports \(199 ページ\)](#)
- [show ip udp-broadcast upstream-bridged all-ports \(200 ページ\)](#)
- [show interfaces accel \(193 ページ\)](#)
- [show license \(195 ページ\)](#)
- [show license-file \(201 ページ\)](#)
- [show log \(202 ページ\)](#)
- [show nms-server \(203 ページ\)](#)
- [show ntp-server \(204 ページ\)](#)
- [show roaming-domain \(205 ページ\)](#)
- [show syslog-file \(207 ページ\)](#)
- [show syslog-host \(209 ページ\)](#)
- [show syslog-table \(210 ページ\)](#)
- [show sys-summary \(212 ページ\)](#)
- [show sys-summary ess \(214 ページ\)](#)
- [show sys-summary general \(216 ページ\)](#)
- [show sys-summary resources \(218 ページ\)](#)
- [show sys-summary stations \(219 ページ\)](#)
- [show sys-summary throughput \(220 ページ\)](#)
- [show system-id \(221 ページ\)](#)
- [show timezones \(222 ページ\)](#)
- [spectrum-band \(223 ページ\)](#)
- [start-ntp \(224 ページ\)](#)
- [statistics period \(225 ページ\)](#)
- [Sysconfig backup \(226 ページ\)](#)
- [Sysconfig restore \(227 ページ\)](#)
- [syslog-host \(228 ページ\)](#)
- [telnet \(229 ページ\)](#)
- [timezone \(230 ページ\)](#)
- [topo-update \(233 ページ\)](#)
- [traceroute \(234 ページ\)](#)
- [zeronet-packet \(235 ページ\)](#)

10gig-module

10 gig モジュールのステータスを有効または無効にします。

構文

`10gig-module <option>`

option

Enable または Disable

コマンド モード

グローバル設定

デフォルト

用途

使用例

```
controller# configure terminal
controller(config)# 10gig-module enable
```

aeroscout

Aeroscout 製品スイートのタグ トラッキングとの相互運用性を有効および無効にします。

構文

```
aeroscout enable  
aeroscout disable  
aeroscout ip-address  
aeroscout port
```

コマンド モード

グローバル設定

デフォルト

この機能はデフォルトで無効です。

用途

FortiWLC (SD) は、AeroScout のタグ (ただし、ラップトップではありません) プロトコルを実装することで、フォーティネットのインフラストラクチャ (コントローラおよびアクセス ポイント) と AeroScout のプラットフォームの相互運用を実現します。パラメータ **ip-address** と **port** を使用して、Aeroscout マシンが使用する IP とポートを指定します。

使用例

以下の例は、Aeroscout を有効にします。

```
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)# aeroscout enable
```

alarm

alarm-type (アラーム タイプ) を設定します。

構文

alarm <alarm-type>

二重引用符で囲んで次のアラーム タイプのいずれかを入力する必要があります。

- AP CPU Usage High (AP CPU 使用率高)
- AP Down (AP 停止)
- AP Memory Usage High (AP メモリ使用率高)
- AP Radio Card Failure (AP 無線カードの障害)
- AP Runtime Error (AP ランタイムエラー)
- AP Software Version Mismatch (AP ソフトウェアバージョンの不一致)
- AP Wireless Interface Down (AP ワイヤレス インターフェイス ダウン)
- AP Wireless Interface Station Capacity Full (AP ワイヤレス インターフェイス ステーションのキャパシティ限界)
- Admin Login Failure (管理者ログインのエラー)
- Alarm History Full (アラーム履歴が満杯)
- Alarm History Reaches Threshold (アラーム履歴がしきい値に達する)
- CAC limit reached (CAC の上限に到達)
- Certificate Error (証明書エラー)
- Certificate Installed (インストールされた証明書)
- Controller CPU Usage High (コントローラ CPU 使用率高)
- Controller IP Address Change (コントローラ IP アドレスの変更)
- Controller Memory Usage High (コントローラ メモリ使用率高)
- DFS Channel Update (DFS チャンネル更新)
- DHCP Address Pool Exhausted (DHCP アドレス プールの枯渇)
- Event Log Full (イベント ログが満杯)
- Event Log Reaches Threshold (イベント ログがしきい値に達する)
- Fan Module Failure (ファン モジュールの障害)
- High Channel Utilization (チャンネル利用率高)
- Interference Detected (干渉の検出)
- Link Down (リンク ダウン)
- Low Channel Quality (チャンネル品質低)

- MIC Counter Measure Activation (MIC カウンター測定の有効化)
- Master Down (マスタ ダウン)
- Power Module Failure (電源モジュールの障害)
- Radius Server Failed (Radius サーバの障害)
- Radius Server Restored Primary (リストアされたプライマリ Radius サーバ)
- Radius Server Switchover Failure Accounting (Radius サーバ スイッチオーバー障害アカウンティング)
- Radius Server Switchover (Radius サーバ スイッチオーバー)
- Rogue AP Detected (不正 AP の検出)
- Software License Expired (期限切れのソフトウェア ライセンス)
- Software License Violated (違反のあったソフトウェア ライセンス)
- System ID Changed (システム ID の変更)
- User 802.1x Authentication Failure (ユーザによる 802.1x 認証失敗)
- User TKIP Message Integrity Check Failure (ユーザによる TKIP メッセージ整合性チェックの失敗)
- Watchdog Failure (監視機能の障害)

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、アラーム タイプを使用してアラームを設定します。

使用例

```
MC3200(15)# configure terminal
MC3200(15)(config)# alarm "AP CPU Usage High"
MC3200(15)(config-alarm-configuration)#?
end (10) Save changes, and return to privileged EXEC mode.
exit (10) Save changes, and return to global configuration mode
reload-configuration (10) Reload Default Configuration of this alarm.
severity (10) Configures Severity of this alarm.
snmp (10) Enable/Disable Snmp for this alarm.
state (10) Enable/Disable this alarm.
syslog (10) Enable/Disable Syslog for this alarm.
threshold (10) Configures Threshold value for this alarm.
```

```
MC3200(15)(config-alarm-configuration)# snmp enable
MC3200(15)(config-alarm-configuration)# exit
MC3200(15)(config)#
```

関連コマンド [show alarm \(162 ページ\)](#)

amconfig

銅線または SFP のポートのいずれかをアクティブな MC5000 BLK1C2F2 インターフェイスとして選択します。

構文

```
amconfig copper  
amconfig sfp
```

copper	銅線ポートを使用します。
sfp	SFP ポートを使用します。

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドが必要なのは、銅線コネクタと SFP コネクタが MC5000 に混在する場合です。すべてのコネクタが一致している場合、このコマンドは必要ありません。

使用例

以下のコマンドは、銅線のポートを設定します。

```
controller# configure terminal  
controller(config)# amconfig copper  
controller(config)#
```

audit period

アクセス ポイントに関する情報をコントローラが収集する頻度を設定します。

構文

audit period <period>

period コントローラがアクセス ポイントに関する情報を収集する間隔。有効な値の範囲は 0、5 ～ 65,535 秒です。

コマンドモード

グローバル設定

デフォルト

デフォルトの監査間隔は 60 秒です。

用途

通常はこの監査間隔を変更する必要はありません。監査間隔は以下のコマンドにより収集されるデータに影響します。

- show ap-assigned
- show ap-siblings
- show ap-discovered
- show topoap

この監査間隔によって、不正 AP のアラームがクリアされる間隔も制御されます。

0 を設定すると、監査収集が無効になります。

使用例

以下のコマンドを指定すると、監査間隔が 120 秒に設定されます。

```
controller(config)# audit period 120
controller(config)#
```


bonding

サポートされるコントローラ プラットフォーム上のイーサネット ポート集約を有効 / 無効にします。

構文

```
bonding none  
bonding single  
bonding dual
```

コマンドモード

グローバル設定

デフォルト

bonding はデフォルトで **single** に設定されます。

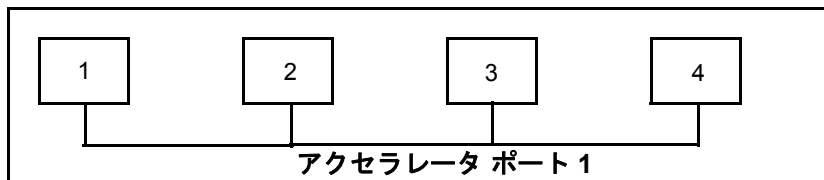
用途

bonding コマンドを使用すると、適用可能なイーサネット ポートがパラレル (並列) で使用され、スループットが増加します (ポート トランキング、またはリンク集約とも呼ばれます)。この機能は、AMC イーサネット ポート カードのある MC4100 と MC5000、および MC3200 と MC4200 コントローラでサポートされています。FastPath モード アクセラレーションと組み合わせると、スループットはさらに増加します。**show controller** コマンドで、ボンディングのステータスを確認します。

bonding single コマンドを使用すると、4 つすべてのポートを 1 つに組み合わせることができます。**bonding none** は、ボンディング設定を削除し、すべてのポートを個別に使用できるようにします。

コマンドを有効にするためには、コントローラが接続されるより前にスイッチのリンク集約がセットアップされている場合を除き、コントローラのリブートが必要です。このような状況は一般的ではないため、通常はリブートが必要になります。

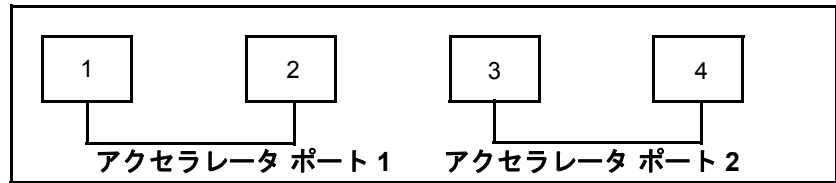
図 1: シングル ボンディング



bonding dual コマンドを使用すると、2 組のイーサネット ポートを 2 つのアクセラレータポートに組み合わせることができます。

Dual イーサネット モードには **bonding dual** 設定が必要です。

図 2: デュアル ボンディング



使用例

以下のコマンドは、MC4100 ポートすべてを 1 つに集約します。

```
mc4100(config)# bonding single
```

関連コマンド

- [fastpath \(124 ページ\)](#)
- [show bonding \(168 ページ\)](#)

calendar set

コントローラのハードウェア時計およびソフトウェア時計を設定します。

構文

```
calendar set <mm/dd/yyyy> <hh:mm:ss>
```

mm/dd/yyyy 月 / 日 / 年の形式で記述される日付 (たとえば、04/06/2008)。

hh:mm:ss 時 (24 時間式)、分、秒で記述される時刻。

コマンドモード

特権 EXEC

デフォルト

なし

用途

手動でシステムの日付と時刻を設定するには、**calendar set** コマンドを使用します。日付と時刻を設定すると、コントローラをリブートして、新たに設定した時刻にシステム クロックをリセットするかどうかの確認するメッセージが表示されます。プロンプトで **yes** と答えると、システム クロックが新しい時刻に設定されます。また、**running-config** を **startup-config** に保存することを求めるメッセージが表示されます。**show calendar** または **date** コマンドで、時刻設定を確認します。

使用例

以下のコマンドは、システムの日付とハードウェアの時計を 2008 年 3 月 6 日の 午後 1:00:00 に設定します。

```
controller# calendar set 03/06/2008 13:00:00
This command requires a controller reboot.Do you want to Proceed [yes/no]
yes
Thu Mar 6 13:00:02 UTC 2008
You will lose any unsaved configuration.Save to startup-config now [y|n]?
y
Configuration saved
```

Broadcast message from root (Thu Mar 6 13:00:29 2008):

The system is going down for reboot NOW!

関連コマンド

- [copy running-config](#) (75 ページ)
- [show calendar](#) (170 ページ)
- [date](#) (119 ページ)

clear statistics interfaces

インターフェイスの統計情報カウンタをリセットします。

構文

```
clear statistics interfaces Dot11Radio <ap_id>  
clear statistics interfaces FastEthernet controller  
clear statistics interfaces FastEthernet ap <ap_id>
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

clear statistics interfaces コマンドを使用して、Dot11Radio または FastEthernet インターフェイスの統計情報を消去します。Dot11Radio 統計情報を消去するときには、AP ID を指定する必要があります。FastEthernet 統計情報を消去するときは、コントローラ、すべての AP、または AP の ID を指定できます。

使用例

このコマンドを使用すると、すべての AP のすべての FastEthernet 統計情報が消去されます。

```
controller# clear statistics interfaces FastEthernet ap
```

このコマンドを使用すると、AP 5 のすべての FastEthernet 統計情報が消去されます。

```
controller# clear statistics interfaces FastEthernet ap 5
```

関連コマンド

- [show interfaces Dot11Radio statistics \(644 ページ\)](#)
- [show interfaces FastEthernet statistics \(302 ページ\)](#)

client-locator

クライアント ロケーション スクリプトを制御します。

構文

client-locator (クライアント ロケーション スクリプトを有効にする)
no client-locator (クライアント ロケーション スクリプトを無効にする)
show client-locator (クライアント ロケータ ユーティリティの状態を表示する)
client-locator add (OUI をロケータに追加する)
show client-locator ouis (ロケータに存在する OUI を表示する)

コマンド モード

特権 EXEC

デフォルト

無効

用途

この機能は、ICMP パケットをサイレント クライアントに送信することで、クライアントがスリープ状態に移行しないようにします。サイレント クライアントの OUI は、/opt/meru/bin フォルダに置かれている、ping_ouis という名前の予め定義されたスクリプトに入力されています。

ユーザも特定の OUI を追加でき、**add** および **show** コマンドで現在のリストを表示できます。

使用例

```
controller# client-locator
controller# sh client-locator
Client Locator utility is enabled
controller# no client-locator
controller# sh client-locator
Client Locator utility is disabled
controller#

controller# client-locator add 11:22:33
controller#

controller# show client-locator ouis
00:13:02
00:02:b3
```

00:03:47
00:04:23
00:07:e9
00:0c:f1
00:0e:0c
00:0e:35
00:11:11
00:12:f0
00:13:20
controller#

関連コマンド なし

controller-index

ステーションごとの BSSID 用のコントローラの識別子を設定します。

構文

controller-index <*identifier*>

identifier コントローラ固有の識別子 (ID)。 *Identifier* には、1 ～ 255 の値を設定できます。 *identifier* を 0 に設定すると、このオプションは無効になります。

コマンドモード

グローバル設定モード

デフォルト

無効 (0 に設定)。

用途

controller-index コマンドを使用して、仮想ポート機能で使用するコントローラを一意に識別します。ステーションごとに固有のリンクが割り当てられることで、仮想セル全体で一意的識別が可能になります。一意のコントローラ インデックスを、WLAN 内の各コントローラに適用する必要があります。

コントローラ インデックスは、一意の CSSID を作成するために使用されるシステム情報の一部です。仮想ポートを使用する ESS に対応するすべてのクライアントに、CSSID が割り当てられます。コントローラ インデックスが変更されると、CSSID の値も変更されるため、CSSID が割り当てられているすべてのクライアントの接続を解除して、再接続する必要があります。



同じネットワーク上の 2 台の異なるコントローラに同じインデックス番号を適用しないでください。

使用例

このコマンドでは、コントローラ インデックスを 1 に設定しています。

```
controller# configure terminal
controller(config)# controller-index 1
controller(config)# exit
```

関連コマンド

[virtual-port](#) (570 ページ)

date

現在の日付と時刻を表示します。

構文

date

コマンド モード

特権 EXEC

デフォルト

なし

用途

現在の日付と時刻を表示するには、**date** コマンドを使用します。システムの日付と時刻を設定するには、**calendar set** コマンドを使用します。

使用例

以下のコマンドを指定すると、システムの日付と時刻が表示されます。

```
controller# date  
Thu Mar 6 13:15:34 UTC 2008
```

関連コマンド

- [calendar set \(113 ページ\)](#)
- [show calendar \(170 ページ\)](#)

erase-guest-user

[guest-user \(126 ページ\)](#) コマンドで作成したゲスト ユーザ テーブルを消去します。

構文

erase-guest-user

コマンド モード

特権 EXEC

デフォルト

なし

用途

erase-guest-user コマンドを使用して、**guest-user** コマンドを使用して生成されたユーザ テーブルを消去します。

使用例

このコマンドは、ゲスト ユーザ テーブルを消去します。

```
controller# erase-guest-user
```

関連コマンド

[guest-user \(126 ページ\)](#)

event

event-type (イベント タイプ) を設定します。

構文

event <event-type>

二重引用符で囲んで次のイベント タイプのいずれかを入力する必要があります。

- AP CPU Usage High (AP CPU 使用率高)
- AP Down (AP 停止)
- AP Memory Usage High (AP メモリ使用率高)
- AP Radio Card Failure (AP 無線カードの障害)
- AP Runtime Error (AP ランタイムエラー)
- AP Software Version Mismatch (AP ソフトウェアバージョンの不一致)
- AP Wireless Interface Down (AP ワイヤレス インターフェイス ダウン)
- AP Wireless Interface Station Capacity Full (AP ワイヤレス インターフェイス ステーションのキャパシティ限界)
- Admin Login Failure (管理者ログインのエラー)
- Alarm History Full (アラーム履歴が満杯)
- Alarm History Reaches Threshold (アラーム履歴がしきい値に達する)
- CAC limit reached (CAC の上限に到達)
- Certificate Error (証明書エラー)
- Certificate Installed (インストールされた証明書)
- Controller CPU Usage High (コントローラ CPU 使用率高)
- Controller IP Address Change (コントローラ IP アドレスの変更)
- Controller Memory Usage High (コントローラ メモリ使用率高)
- DFS Channel Update (DFS チャンネル更新)
- DHCP Address Pool Exhausted (DHCP アドレス プールの枯渇)
- Event Log Full (イベント ログが満杯)
- Event Log Reaches Threshold (イベント ログがしきい値に達する)
- Fan Module Failure (ファン モジュールの障害)
- High Channel Utilization (チャンネル利用率高)
- Interference Detected (干渉の検出)
- Link Down (リンク ダウン)
- Low Channel Quality (チャンネル品質低)

- MIC Counter Measure Activation (MIC カウンター測定の有効化)
- Master Down (マスタ ダウン)
- Power Module Failure (電源モジュールの障害)
- Radius Server Failed (Radius サーバの障害)
- Radius Server Restored Primary (リストアされたプライマリ Radius サーバ)
- Radius Server Switchover Failure Accounting (Radius サーバ スイッチオーバー障害アカウンティング)
- Radius Server Switchover (Radius サーバ スイッチオーバー)
- Rogue AP Detected (不正 AP の検出)
- Software License Expired (期限切れのソフトウェア ライセンス)
- Software License Violated (違反のあったソフトウェア ライセンス)
- System ID Changed (システム ID の変更)
- User 802.1x Authentication Failure (ユーザによる 802.1x 認証失敗)
- User TKIP Message Integrity Check Failure (ユーザによる TKIP メッセージ整合性チェックの失敗)
- Watchdog Failure (監視機能の障害)

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、イベント タイプを使用してイベントを設定します。

使用例

```
MC3200(15)# configure terminal
MC3200(15)(config)# event "AP CPU Usage High"
MC3200(15)(config-event-configuration)#?
end (10) Save changes, and return to privileged EXEC mode.
exit (10) Save changes, and return to global configuration mode
reload-configuration (10) Reload Default Configuration of this alarm.
severity (10) Configures Severity of this alarm.
snmp (10) Enable/Disable Snmp for this alarm.
state (10) Enable/Disable this alarm.
syslog (10) Enable/Disable Syslog for this alarm.
threshold (10) Configures Threshold value for this alarm.
```

```
MC3200(15)(config-event-configuration)# snmp enable
MC3200(15)(config-event-configuration)# exit
MC3200(15)(config)#
```

関連コマンド [*show event*](#) (185 ページ)

fastpath

イーサネット ポート アクセラレータを有効および無効にします。

構文

```
fastpath on  
fastpath off
```

コマンド モード

グローバル設定

デフォルト

fastpath は有効です

制限事項

ユニキャスト IPv4 および UDP フローのみが **fastpath** により処理されます。

用途

fastpath ユーティリティは、イーサネット インターフェイスにおけるパケットの移動速度を、IP パケット ストリームの識別に基づいてアクセラレータします。**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。

使用例

以下では、fastpath アクセラレータを無効にします。

```
controller(config)# fastpath off  
controller#
```

関連コマンド

- [bonding \(111 ページ\)](#)
- [capture-packets \(894 ページ\)](#)

fingerprint

デバイスのフィンガープリントを使用すると、ネットワークに接続しているデバイスのさまざまな属性を収集できます。クライアントの OS、デバイス タイプ、使用されているブラウザなど、収集された属性に基づいて、個々のデバイスを完全または部分的に特定できます。以前のバージョンの FortiWLC (SD) では、ステーション情報にステーションの MAC アドレスおよびネットワーク アクティビティが含まれていました。デバイス フィンガープリントによってステーションに関する詳細が提供され、システム管理者は使用中のデバイス タイプを把握しやすくなり、必要な措置を講じることができます。[Monitor] > [Dashboard] を選択すると、デバイスの詳細情報を表示できます。fingerprint コマンドを使用するとデバイスを追加、削除、リストアでき、[show fingerprints \(190 ページ\)](#) では、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が表示されます。

構文 fingerprint [add/delete] ["description"] ["hexadecimal signature"]

コマンドモード グローバル設定

デフォルト なし

用途 デバイス フィンガープリントを使用すると、ステーションの OS とタイプを 16 進数のシグネチャをベースに検出して表示できます。fingerprint コマンドを使用して、システムにフィンガープリントを追加したり、システムからフィンガープリントを削除したりできます。

使用例

```
controller(config)# fingerprint add "devicetype" "34e514d"

controller#

controller(config)# fingerprint delete "devicetype" "34e514d"

controller#
```

関連コマンド [show fingerprints \(190 ページ\)](#)

guest-user

ゲスト ユーザ アカウントを作成し、ゲスト ユーザ サブモードに入ります。

構文

```
guest user <guestname>,<password>,<service start time>,<service end time>
```

guestname	name
password	password
service start time	アカウントを使用してユーザが開始できる時間。形式は “mm/dd/yyyy hh:mm:ss”
service end time	ユーザがアカウントにアクセスできない時間。形式は “mm/dd/yyyy hh:mm:ss”

コマンドモード

グローバル設定

デフォルト

なし

用途

guest-user コマンドを使用すると、ローカルの管理者は、ユーザの一時的なアクセスを提供するゲスト アカウントをキャプティブ ポータルに追加できるようになります。最大で 32 個のゲスト ユーザ アカウントを同時に作成できます。2 人以上のゲスト ユーザが同じユーザ アカウント名を使用できます。

The **guest-user** コマンドは、指定した *名前* でゲスト ユーザ アカウントを作成し、ゲスト ユーザ サブモードに入ります。このモードでは、パスワード、アカウント有効化の開始時間および終了時間など、残りのアカウント詳細を設定できます。

アカウントが作成され、ユーザがアカウント名を使用してキャプティブ ポータルにログインすると、正しいパスワードを提供し、設定済みアカウントの開始時間と終了時間の間でログインを試行し、ログインを成功させる必要があります。

同じ正確なコマンドを使用して既存のゲスト ユーザを編集します。

使用例

以下の例は、ゲスト ユーザを設定します。

```
MC3K-1(config)# guest-user ?
<guestname>          Enter the name of the guest user.
MC3K-1(config)# guest-user TempGuest ?
```



```

<password>          Enter the password of the guest user.
MC3K-1(config)# guest-user TempGuest XXXXX ?
<start-time>        Enter the service start-time (mm/dd/yyyy hh:mm:ss)
in double quotes.
MC3K-1(config)# guest-user TempGuest 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 TempGuest XXXXX "01/01/2010 00:00:00" "01/01/
2011 00:00:00" ?
<CR>
MC3K-1(config)# guest-user TempGuest XXXXX "01/01/2010 00:00:00" "01/01/
2011 00:00:00"
MC3K-1(config)# exit
MC3K-1# show guest-user

```

Guest User Name	Service
Start Time	Service End Time
TempGuest 00:00:00	01/01/2010 01/01/2011 00:00:00

Guest User Table(1 entry)

MC3K-1#

関連コマンド [show guest-user \(192 ページ\)](#)

hostname

コントローラのホスト名を指定します。

構文

hostname <name>

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用してホスト名をコントローラに割り当てます。

使用例

次のコマンドは、ホスト名 (デフォルト) を表示し、グローバル設定モードに入り、ラベル *mc1100* をコントローラに割り当てます。

```
default# show hostname
default
default(config)# configure terminal
default(config)# hostname 3200
mc3200(config)# exit
mc3200# show hostname
mc3200
```

ip udp-broadcast downstream

ブロードキャスト パススルーのすべての UDP ダウンストリーム ポートを設定します。

構文

```
ip udp-broadcast downstream all-ports on
ip udp-broadcast downstream all-ports selected
```

コマンド モード

端末設定

デフォルト

選択したポートはデフォルトでオンです。

用途

このコマンドを使用すると、パラメータ **on** を使用してパススルーのすべての UDP ダウンストリーム ポートを設定できます。パラメータ **selected** は、レガシー コマンド **ip udp-broadcast downstream <portNumber>** で指定された最大 8 つのポートがオンであることを意味します。このコマンドの **selected** バージョンがアクティブの場合にコマンド **show ip udp-broadcast downstream all-ports** を使用すると、最大 8 つのポートのリストが表示されます。このコマンドの **on** バージョンは、テストの目的でのみ使用することを推奨します。

```
default# configure terminal
default(config)# ip udp-broadcast downstream all-ports on
default(config)# end
default# show ip udp-broadcast downstream all-ports
Downstream UDP Broadcast All Ports

UDP All Ports : on
default#
```

関連コマンド

- [ip udp-broadcast upstream \(131 ページ\)](#)
- [ip udp-broadcast upstream-bridged \(132 ページ\)](#)
- [show ip udp-broadcast downstream all-ports \(197 ページ\)](#)
- [show ip udp-broadcast downstream-bridged all-ports \(198 ページ\)](#)
- [show ip udp-broadcast upstream all-ports \(199 ページ\)](#)
- [show ip udp-broadcast upstream-bridged all-ports \(200 ページ\)](#)

ip udp-broadcast downstream-bridged

ブロードキャスト ブリッジ パススルーのすべての UDP ダウンストリーム ポートを設定します。

構文

```
ip udp-broadcast downstream-bridged all-ports on
ip udp-broadcast downstream-bridged all-ports selected
```

コマンド モード

端末設定

デフォルト

選択したポートはデフォルトでオンです。

用途

このコマンドを使用すると、パラメータ **on** を使用してパススルーのすべての UDP ダウンストリーム ブリッジ ポートを設定できます。パラメータ **selected** は、レガシー コマンド **ip udp-broadcast downstream-bridged <portNumber>** で指定された最大 8 つのポートがオンであることを意味します。このコマンドの **selected** バージョンがアクティブの場合にコマンド **show ip udp-broadcast downstream-bridged all-ports** を使用すると、最大 8 つのポートのリストが表示されます。このコマンドの **on** バージョンは、テストの目的でのみ使用することを推奨します。

```
default# configure terminal
default(config)# ip udp-broadcast downstream-bridged all-ports on
default(config)# end
default# show ip udp-broadcast downstream-bridged all-ports
Downstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

関連コマンド

- [*ip udp-broadcast downstream-bridged* \(130 ページ\)](#)
- [*ip udp-broadcast upstream* \(131 ページ\)](#)
- [*show ip udp-broadcast downstream all-ports* \(197 ページ\)](#)
- [*show ip udp-broadcast downstream-bridged all-ports* \(198 ページ\)](#)
- [*show ip udp-broadcast upstream all-ports* \(199 ページ\)](#)
- [*show ip udp-broadcast upstream-bridged all-ports* \(200 ページ\)](#)

ip udp-broadcast upstream

ブロードキャスト パススルーのすべての UDP アップストリーム ポートを設定します。

構文

```
ip udp-broadcast upstream all-ports on
ip udp-broadcast upstream all-ports selected
```

コマンド モード

端末設定

デフォルト

selected

用途

このコマンドを使用すると、パラメータ **on** を使用してパススルーのすべての UDP アップストリーム ポートを設定できます。パラメータ **selected** は、レガシー コマンド **ip udp-broadcast upstream <portNumber>** で指定された最大 8 つのポートがオンであることを意味します。このコマンドの **selected** バージョンがアクティブの場合にコマンド **show ip udp-broadcast upstream all-ports** を使用すると、最大 8 つのポートのリストが表示されます。このコマンドの **on** バージョンは、テストの目的でのみ使用することを推奨します。

使用例

```
default# configure terminal
default(config)# ip udp-broadcast upstream all-ports selected
default(config)# end
default# show ip udp-broadcast upstream all-ports
Upstream UDP Broadcast All Ports

UDP All Ports : selected
default#
```

関連コマンド

- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [show ip udp-broadcast downstream all-ports \(197 ページ\)](#)
- [show ip udp-broadcast downstream-bridged all-ports \(198 ページ\)](#)
- [show ip udp-broadcast upstream all-ports \(199 ページ\)](#)
- [show ip udp-broadcast upstream-bridged all-ports \(200 ページ\)](#)

ip udp-broadcast upstream-bridged

ブロードキャストブリッジパススルーのすべてのUDPアップストリームポートを設定します。

構文

```
ip udp-broadcast upstream-bridged all-ports on  
ip udp-broadcast upstream-bridged all-ports selected
```

コマンドモード

端末設定

デフォルト

selected

用途

このコマンドを使用すると、パラメータ **on** を使用してパススルーのすべてのUDPアップストリームブリッジポートを設定できます。パラメータ **selected** は、レガシーコマンド **ip udp-broadcast upstream-bridged <portNumber>** で指定された最大8つのポートがオンであることを意味します。このコマンドの **selected** バージョンがアクティブの場合にコマンド **show ip udp-broadcast upstream-bridged all-ports** を使用すると、最大8つのポートのリストが表示されます。このコマンドの **on** バージョンは、テストの目的でのみ使用することを推奨します。

使用例

```
default# configure terminal  
default(config)# ip udp-broadcast upstream-bridged all-ports selected  
default(config)# end  
default# show ip udp-broadcast upstream-bridged all-ports  
Upstream UDP Broadcast All Ports  
  
UDP All Ports : selected  
default#
```

関連コマンド

- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [show ip udp-broadcast downstream all-ports \(197 ページ\)](#)
- [show ip udp-broadcast downstream-bridged all-ports \(198 ページ\)](#)
- [show ip udp-broadcast upstream all-ports \(199 ページ\)](#)
- [show ip udp-broadcast upstream-bridged all-ports \(200 ページ\)](#)

license

システムのライセンスを有効にします。

構文

```
license ftp://<host>/<filename>
```

host	ライセンス ファイルがあるホスト名を指定します。 <i>host</i> には、ホスト名または IP アドレスを指定できます。
filename	ライセンス ファイル名を指定します。

コマンドモード

グローバル設定モード

デフォルト

5 つの AP のライセンスと 1 つのコントローラ、および Enterprise Mesh AP が構成されています。

用途

このコマンドを使用して、システムのハードウェアと機能モジュールのライセンスを有効にします。ライセンス情報はコントローラのファームウェアに埋め込まれており、フォーティネットが生成するライセンス ファイルにより有効に設定されます。ライセンス ファイルはフォーティネットにより生成され、ユーザが購入したオプションに応じて、システム コンポーネントのライセンスを設定するために必要なキーが含まれます。

コンポーネントのライセンスには、マスタまたはスタンバイ コントローラのキーが含まれています。また、マスタまたはスタンバイ コントローラに関連付ける最大 AP 数 (コントローラのモデルが基準になります) も含まれます。

機能ライセンスでは以下がサポートされます。

- AP 数 (コントローラのモデルに応じてコントローラが使用する最大 AP 数)
- N+1 (複数のマスタ コントローラで 1 台のスタンバイ コントローラを使用する機能)
- ユーザごとのファイアウォール (ユーザごとにファイアウォール ポリシーを定義して適用する機能)
- GRE トンネル (ESS プロファイル設定を使用してトラフィックを選択してトンネルする機能)
- デュアル B/G (同じ周波数帯で AP208 の両方の無線を使用する機能)
- Enterprise Mesh

フォーティネットからライセンスキーを受け取ったら、キーを FTP ディレクトリ (FTP を使用している場合) または SCP の任意の場所に配置します。

no フォームを使用して、システムから特定の機能セットを削除できます。

使用例

以下のコマンドを使用すると、license17331.lic が FTP サーバ 192.168.1.10 から取得され、コントローラのライセンスが有効となります。

```
mc3000(config)# license ftp://admin:admin@192.168.1.10/license17331.lic
```

関連コマンド

- [show license \(195 ページ\)](#)
- [show license-file \(201 ページ\)](#)

management wireless

コントローラへのワイヤレス管理アクセスを有効または無効にします。

構文

```
management wireless  
no management wireless
```

コマンド モード

グローバル設定モード

デフォルト

コントローラのワイヤレス管理は有効になっています。

用途

management wireless コマンドを使用して、ワイヤレス ステーションがコントローラにアクセスして設定を変更できるようにします。サイトのセキュリティを保護する上でこの設定が問題となる場合は、**no management wireless** コマンドを使用してワイヤレスの管理アクセスを無効にすると、ワイヤレス クライアントから送信される VPN およびキャプティブポータル以外のすべてのパケットはブロックされます。

show controller コマンドを使用して、管理アクセスのステータスを確認できます。出力の最終行の Management by wireless stations: に、on または off の値が表示されます。

使用例

以下のコマンドにより、ワイヤレス ステーションからコントローラへの管理アクセスが無効になります。

```
controller# no management wireless
```

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

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

関連コマンド

[show controller \(172 ページ\)](#)

nms-profile

NMS プロファイルを有効または無効にします。

構文

```
nms-profile enable  
nms-profile disable
```

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して NMS プロファイル オプションを有効または無効にします。

使用例

以下のコマンドは、NMS プロファイルを有効にします。

```
controller# configure terminal  
controller(config)# nms-profile enable  
controller(config)#
```

nms-server

NMS サーバの登録または登録解除を行います。

構文

```
nms-server register  
nms-server unregister
```

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して NMS サーバの使用を制御します。HP OpenView などのネットワーク管理システム (NMS) であり、アラーム情報やトラップ情報を設定済みの管理ステーションに送信します。

使用例

次のコマンドは、NMS サーバを登録します。

```
controller# configure terminal  
controller(config)# nms-server register  
controller(config)#
```

nms-vpn-server

NMS VPN サーバの IP アドレスを設定します。

構文

nms-vpn-server <*ip address*>

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して NMS VPN サーバの IP アドレスを設定します。

使用例

```
controller# configure terminal
controller(config)# nms-vpn-server 172.27.172.61
controller(config)#
```

ntp

システム クロックと指定のネットワーク タイム プロトコル (NTP) サーバを同期化して、システムの時刻を更新します。

構文

```
ntp sync
ntp server <server>
```

server システム クロックとの同期化に使用する NTP サーバの IP アドレスまたはホスト名を指定します。

コマンドモード

特権 EXEC

デフォルト

なし

用途

ntp sync コマンドを使用して、**ntp server** コマンドで指定された NTP サーバとシステム クロックとを定期的に同期化できます。NTP を有効にしたり、NTP サーバを変更したりしても、システムをリブートするまで変更は有効になりません。一般用の NTP サーバに関する情報は、www.ntp.org を参照してください。

手動でシステム クロックを設定するには、**calendar set** コマンドを使用します。

システムの日付と時刻を確認するには、**date** コマンドを使用します。

show ntp-server コマンドを使用して、指定している NTP サーバの IP アドレスを確認できます。

使用例

以下のコマンドにより、NTP による同期化が実行され、IP アドレス 131.107.1.10 の NTP サーバが同期化に使用されます。

```
controller# ntp sync
controller# ntp server 131.107.1.10
Setting NTP Server to 131.107.1.10.Change will only take effect after
reboot.
```

関連コマンド

- [calendar set \(113 ページ\)](#)
- [date \(119 ページ\)](#)

- [show ntp-server](#) (204 ページ)

passwd

admin または guest パスワードを変更します。

構文

```
passwd admin  
passwd guest <password>
```

admin	管理 (administrative) パスワードを変更します。
guest	ゲスト (guest) パスワードを変更します。
password	administrative または guest パスワードを指定します。

コマンド モード

グローバル設定

デフォルト

デフォルトの admin パスワードは **admin** です。デフォルトの guest パスワードは **guest** です。

用途

初めてシステムにログインしたときは、管理パスワードを変更してください。パスワードを変更する際には、標準的な Linux ガイドラインに従ってください。

使用例

次の例では、admin のデフォルト パスワードを変更します。

```
MC5000-master# configure terminal  
MC5000-master(config)# passwd admin  
Changing password for user admin.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
MC5000-master(config)# end  
MC5000-master#
```

ping

ネットワーク接続をテストします。

構文

`ping <hostname>`

hostname ping を行うデバイスの IP アドレス。

コマンド モード

特権 EXEC

デフォルト

なし

用途

ping コマンドを使用して、デバイスへの基本的なネットワーク接続状態をテストします。

使用例

以下のコマンドを指定すると、コントローラ (10.3.1.2) から、IP アドレスが 10.3.4.5 のデバイスへの基本的な接続状態がテストされます。

```
controller# ping 10.3.4.5
PING 10.3.4.5 (10.3.4.5) from 10.3.1.2 : 56(84) bytes of data.
64 bytes from 10.3.4.5: icmp_seq=1 ttl=255 time=0.334 ms
64 bytes from 10.3.4.5: icmp_seq=2 ttl=255 time=0.294 ms
64 bytes from 10.3.4.5: icmp_seq=3 ttl=255 time=0.276 ms
64 bytes from 10.3.4.5: icmp_seq=4 ttl=255 time=0.234 ms
64 bytes from 10.3.4.5: icmp_seq=5 ttl=255 time=0.311 ms

--- 10.3.4.5 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 3996ms
rtt min/avg/max/mdev = 0.234/0.289/0.334/0.040 ms
controller#
```


poweroff controller

コントローラを安全にシャットダウンします。

構文

`poweroff controller`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`poweroff controller` コマンドを使用して、コントローラを安全にシャットダウンします。

コントローラを起動してから変更した設定を有効にする場合には、シャットダウンする前に `copy running-config startup-config` コマンドを使用してスタートアップ設定ファイルを保存するようにしてください。

使用例

以下のコマンドを指定すると、コントローラがシャットダウンします。

```
controller# poweroff controller
```

```
Are you sure you want to poweroff the controller [y|n]? y
```

```
Broadcast message from root (pts/0) (Fri May 14 21:51:31 2004):
```

```
The system is going down for system halt NOW!
```

コントローラがシャットダウンします。

関連コマンド

[*copy running-config*](#) (75 ページ)

proactive-spectrum-manager

操作のベスト チャンネルを監視し提案します。

構文

```
proactive-spectrum-manager evaluate
proactive-spectrum-manager stop
proactive-spectrum-manager view
```

evaluate	チャンネル使用を評価し、チャンネル変更を推奨または実行します。
stop	PSM をオフにします。
view	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。

コマンド モード

特権 EXEC

デフォルト

デフォルトで、View はすべてのチャンネル上で有効です。

用途

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。不正などのモード監視インターフェイスを表示するほか、チャンネル使用に関する GUI 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。

使用例

次のコマンドを使用すると、強制的にチャンネルの利点が即座にワンタイム評価されます。**Evaluation Time** がゼロ以外の場合、評価が x 分ごとに行われます。x は **Evaluation Time** で指定した数値です。x がゼロ以外の場合のみ、**stop** オプションを使用し、評価が繰り返されるのを停止する必要があります。この例では **adapt** を選択したため、既存のチャンネルおよび新しいチャンネルの差が **Adaptation Threshold** (デフォルトは 25%) の値よりも大きい場合、チャンネルは変更されます。

```
PSDMC1k# proactive-spectrum-manager
evaluate stop view
PSDMC1k# proactive-spectrum-manager evaluate
```

** Attention: Stations may be disconnected in this evaluation **

Are you absolutely sure [yes/No]? **yes**

Evaluation time [120s]?

View or Adapt [View/adapt]? **adapt**

Adaptation period [0] min (5-10080)? **5**

Adaptation threshold [25] %?

Interference detection for 120 s launched.

.....

Channel 1: goodness is N/A percent.

Channel 6: goodness is 100 percent.

Channel 11: goodness is N/A percent.

Channel 36: goodness is 0 percent.

Channel 40: goodness is N/A percent.

Channel 44: goodness is N/A percent.

Channel 48: goodness is N/A percent.

Channel 52: goodness is N/A percent.

Channel 56: goodness is N/A percent.

Channel 60: goodness is N/A percent.

Channel 64: goodness is N/A percent.

Channel 100: goodness is N/A percent.

Channel 104: goodness is N/A percent.

Channel 108: goodness is N/A percent.

Channel 112: goodness is N/A percent.

Channel 116: goodness is N/A percent.

Channel 120: goodness is N/A percent.

Channel 124: goodness is N/A percent.

Channel 128: goodness is N/A percent.

Channel 132: goodness is N/A percent.

Channel 136: goodness is N/A percent.

Channel 140: goodness is N/A percent.

Channel 149: goodness is N/A percent.

Channel 153: goodness is N/A percent.

Channel 157: goodness is N/A percent.

Channel 161: goodness is N/A percent.

Channel 165: goodness is N/A percent.

Channel pair 1,6: goodness is 100 percent.

Channel pair 6,11: goodness is 100 percent.

Channel pair 36,40: goodness is 0 percent.
 Channel pair 44,48: goodness is N/A percent.
 Channel pair 52,56: goodness is N/A percent.
 Channel pair 60,64: goodness is N/A percent.
 Channel pair 100,104: goodness is N/A percent.
 Channel pair 108,112: goodness is N/A percent.
 Channel pair 116,120: goodness is N/A percent.
 Channel pair 124,128: goodness is N/A percent.
 Channel pair 132,136: goodness is N/A percent.
 Channel pair 140,149: goodness is N/A percent.
 Channel pair 153,157: goodness is N/A percent.
 Channel pair 161,165: goodness is N/A percent.
 Recommended BG-channel of operation is 6.
 Recommended BG 40MHz channel of operation is 1,6.
 Recommended A-channel of operation is 36.
 Recommended A 40MHz channel of operation is 36,40.

*****check to see if channels changed*****

PSDMC1k# **show interfaces Dot11Radio**

AP ID	AP Name	IfIndex	AP Model	Admin	State	Op State	Channel	Oper Channel
Short Preamble	RF Band	AP Mode						

1	AP-1	2	AP320	Up	Enabled	36	36	off 802.11an	Normal
---	------	---	-------	----	---------	----	----	--------------	--------

1	AP-1	1	AP320	Up	Enabled	6	6	on 802.11bgn	Normal
---	------	---	-------	----	---------	---	---	--------------	--------

次のコマンドにより、Proactive Spectrum Manager の適応がトリガされます (チャンネルを評価し、チャンネル使用のワнтаム調整を行います)。

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**

proxy-arp-filtering

KDDI の電話がソフト ハンドオフ後にコントローラに認識されるようにします。

構文

```
proxy-arp-filtering enable
proxy-arp-filtering disable
```

コマンド モード

特権 EXEC

デフォルト

Proxy-arp-filtering はデフォルトで無効になります。

用途

このコマンドは、モバイル ステーションの ARP 要求に対するコントローラの ARP 応答の送信方法に影響します。このフラグが **enabled** の場合 (デフォルトでは **disabled**)、コントローラは、ターゲット IP がモバイル ステーションの VLAN のサブセットに属していない ARP 要求に応答しません。このコマンドによって、ハンドオフ後にコントローラが KDDI 電話を認識できるようになります。

使用例

```
default#
default# proxy-arp-filtering enable
default#
default#
default# proxy-arp-filtering disable
default#
```

関連コマンド

reload

コントローラとアクセス ポイントをリブートします。

構文

```
reload all
reload ap
reload ap <node-id>
reload controller
reload controller force
reload default
reload default factory
```

all	コントローラとすべてのアクセス ポイントをリブートします。
ap [node-id]	ノード ID が指定されない場合は、すべてのアクセス ポイントをリブートします。特定のアクセス ポイントをリブートするには、ノード ID を指定します。
controller [force]	コントローラのみをリブートします。 force オプションを指定すると、コントローラのリブート時に、最後に保存されたスタートアップ設定が強制的に適用されます。 force オプションはコントローラから応答がない場合にのみ使用してください。
default	コントローラをリブートして、パスワードとシステムの設定を工場出荷時の設定に戻します。さらに、AP スクリプト ファイル (ATS/scripts/*) も削除されます。 警告：このオプションの使用はできるだけ避けてください。システム操作に必要なファイルの一部が削除されることがあります。



N+1 ネットワークの場合、reload コマンドでフェイルオーバーは開始されません。
このコマンドは、アクティブ スレーブ コントローラで実行できません。

コマンドモード

特権 EXEC

デフォルト

なし

用途

高可用性環境で、**reload all** コマンドをリブート時に使用すると、マスタとバックアップ コントローラが同じ設定を使用できます。

使用例

以下のコマンドを指定すると、ノート ID が 2 であるアクセス ポイントがリブートされます。

```
controller# reload ap 2
```

関連コマンド

- [reload-gui \(150 ページ\)](#)
- [reload-management \(151 ページ\)](#)
- [reload-security \(152 ページ\)](#)
- [reload-snmp \(153 ページ\)](#)
- [reload-vpn \(154 ページ\)](#)
- [reload-wapi \(155 ページ\)](#)

reload-gui

Web UI プロセスをリセットします。

構文

`reload-gui`

コマンド モード

特権 EXEC

デフォルト

なし

用途

コマンド `reload-gui` を使用すると、Web UI プロセスがリセットされます。Web UI に関して次の問題が発生した場合に、このコマンドを使用します。

- Web UI にアクセスできない
- Web UI グラフのデータが更新されていない
- AP テーブルのページがフリーズした
- Web UI が不安定になった

使用例

以下のコマンドは、Web UI をリロードします。

```
controller# reload-gui
```

関連コマンド

- [reload \(148 ページ\)](#)
- [reload-management \(151 ページ\)](#)
- [reload-security \(152 ページ\)](#)
- [reload-snmp \(153 ページ\)](#)
- [reload-vpn \(154 ページ\)](#)
- [reload-wapi \(155 ページ\)](#)

reload-management

コントローラの管理プロセスをリセットします。

構文

reload-management

コマンド モード

特権 EXEC

デフォルト

なし

用途

「System Busy (システムがビジーです)」というメッセージが表示されシステムが応答しなくなったときに、このコマンドを使用してコントローラの管理プロセスをリセットします。このコマンドにより、システムが稼働モードに戻ります。

使用例

reload-management コマンドにより、「System Busy (システムがビジーです)」というエラー メッセージが表示された後の管理プロセスがリセットされます。

```
meru-wifi# show ap
The system is busy.Please try again.
meru-wifi#
meru-wifi# reload-management
```

関連コマンド

- [reload \(148 ページ\)](#)
- [reload-gui \(150 ページ\)](#)
- [reload-security \(152 ページ\)](#)
- [reload-snmp \(153 ページ\)](#)
- [reload-vpn \(154 ページ\)](#)
- [reload-wapi \(155 ページ\)](#)

reload-security

セキュリティ モジュールをリセットします。

構文

reload-security

コマンド モード

特権 EXEC

デフォルト

なし

用途

reload-security コマンドは、システムのすべてのセキュリティ関連プロセスをリスタートします。このコマンドを使用して、現在保存されているすべてのセキュリティ設定を再適用します。

使用例

以下のコマンドは、セキュリティ モジュールをリロードします。

```
controller# reload-security
```

関連コマンド

- [reload \(148 ページ\)](#)
- [reload-gui \(150 ページ\)](#)
- [reload-management \(151 ページ\)](#)
- [reload-snmp \(153 ページ\)](#)
- [reload-vpn \(154 ページ\)](#)
- [reload-wapi \(155 ページ\)](#)

reload-snmp

SNMP プロセスをリセットします。

構文

reload-snmp

コマンド モード

特権 EXEC

デフォルト

なし

用途

コマンド **reload-gui** を使用すると、Web UI プロセスがリセットされます。SNMP の問題が発生した場合に、このコマンドを使用します。

使用例

以下のコマンドは、SNMP モジュールをリロードします。

```
controller# reload-snmp
```

関連コマンド

- [reload \(148 ページ\)](#)
- [reload-gui \(150 ページ\)](#)
- [reload-management \(151 ページ\)](#)
- [reload-security \(152 ページ\)](#)
- [reload-vpn \(154 ページ\)](#)
- [reload-wapi \(155 ページ\)](#)

reload-vpn

VPN プロセスをリセットします。

構文

reload-vpn

コマンド モード

特権 EXEC

デフォルト

なし

用途

reload-vpn コマンドは、VPN 設定をリスタートします。VPN AP 経由の接続がうまくいかない場合に、このコマンドを使用します。

使用例

controller# **reload-vpn**

関連コマンド

- [reload](#) (148 ページ)
- [reload-gui](#) (150 ページ)
- [reload-management](#) (151 ページ)
- [reload-security](#) (152 ページ)
- [reload-snmp](#) (153 ページ)
- [reload-wapi](#) (155 ページ)
- [vpn server](#) (510 ページ)

reload-wapi

WAPI プロセスをリセットします。

構文

reload-wapi

コマンド モード

特権 EXEC

デフォルト

なし

用途

reload-wapi コマンドを使用すると、WAPI プロセスがリセットされます。WAPI サーバとの通信で問題が発生した場合に、このコマンドを使用します。

使用例

以下のコマンドは、WAPI 設定をリロードします。

```
controller# reload-wapi
```

関連コマンド

- [reload](#) (148 ページ)
- [reload-gui](#) (150 ページ)
- [reload-management](#) (151 ページ)
- [reload-security](#) (152 ページ)
- [reload-snmp](#) (153 ページ)
- [reload-vpn](#) (154 ページ)
- [wapi-server](#) (357 ページ)

remove-license

ライセンスを削除します。

構文

`remove-license`

コマンド モード

特権 EXEC モード

デフォルト

なし

用途

このコマンドを使用して、システム ハードウェアのライセンス、および `license` コマンドを使用して追加された機能モジュールを削除します。ライセンス情報はコントローラのファームウェアに埋め込まれており、フォーティネットが生成するライセンス ファイルにより有効に設定されます。

このコマンドを呼び出すと、コントローラがリブートします。

関連コマンド

[license \(133 ページ\)](#)

roaming-domain

クライアント ローミングを許可するコントローラのグループを設定します。

構文

```
roaming-domain create
roaming-domain start
roaming-domain stop
```

コマンド モード

グローバル設定

デフォルト

ローミング ドメインは存在しません。

用途

roaming-domain create コマンドを各コントローラに対して使用して、ローミング ドメインに参加中のコントローラのグループをセットアップします。その後に **roaming-domain start** コマンドを使用して各コントローラでサービスを開始します。サービスを無効にするには、**roaming-domain stop** コマンドを使用します。

この機能が使用されるのは、ローミング グループ内のメンバー コントローラが少なくとも 2 つの異なる IP サブネットに及び、コントローラ間でルート ネットワークを利用している環境に使用される場合のみです。最大 5 つのコントローラがローミング ドメインに参加できます。詳細については、『**FortiWLC (SD) 設定ガイド**』の「インターコントローラ ローミング」の章を参照してください。

ICR モードは 2 つあり、1 つは固定ホーム リンク用、もう 1 つは自動リンク用です。制限事項については、『**FortiWLC (SD) 設定ガイド**』の「インターコントローラ ローミング」を参照してください。

使用例

次の例は、最初のコントローラで ICR グループがどのように作成されるかを示しています。このセットアップを、ローミング ドメインにある他のすべてのコントローラで行う必要があります。

自動ホーム リンク設定の例

```
default(config)# roaming-domain create
Create Roaming Domain [y/n]?: y
```

```
-----
                Configure Roaming Domain
-----
```

```

When entering values, make sure they are identical in value and in
identical order
among all participating controllers! Remember to include the current
controller!
ESSID for this roaming domain, or q to quit:
IP address of a controller in roaming domain, or q to quit: 192.168.2.1
Is 192.168.2.1 correct [y/n]?: y
IP address of a controller in roaming domain is 192.168.2.1

Is this controller Static DHCP home for this roaming domain [y/n]? :n
IP address of a controller in roaming domain, or q to quit: 192.168.2.2

Is 192.168.2.2 correct [y/n]?: y
IP address of a controller in roaming domain is 192.168.2.2
Is this controller Static DHCP home for this roaming domain [y/n]? :n
IP address of a controller in roaming domain, or q to quit: q
-----
                Roaming Domain configured!
-----

```

固定ホーム リンク設定の例

```

default(config)# roaming-domain create
Create Roaming Domain [y/n]?: y
-----
                Configure Roaming Domain
-----

When entering values, make sure they are identical in value and in
identical order
among all participating controllers! Remember to include the current
controller!
ESSID for this roaming domain, or q to quit: fixed_home
Is homelink correct [y/n]?: y
ESSID for this roaming domain is homelink
IP address of a controller in roaming domain, or q to quit: 192.168.2.1
Is 192.168.2.1 correct [y/n]?: y
IP address of a controller in roaming domain is 192.168.2.1
Is this controller Static DHCP home for this roaming domain [y/n]? :y
IP address of a controller in roaming domain, or q to quit: 192.168.2.2

```



```
Is 192.168.2.2 correct [y/n]?: y
IP address of a controller in roaming domain is 192.168.2.2
IP address of a controller in roaming domain, or q to quit: q
-----
Roaming Domain configured!
-----
```

関連コマンド [show roaming-domain \(205 ページ\)](#)

setup

基本的なシステム設定セットアップ スクリプトを開始します。

構文

`setup`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`setup` スクリプトを使用して、システムの起動と実行に関する基本パラメータを設定します。スクリプトを実行すると、コントローラとの通信パラメータを確立するための情報を求めるメッセージが表示されます。

コントローラの IP アドレスを DHCP を使用して割り当てようとしている場合、以下の情報を提供する必要があります。

- コントローラのホスト名 (ホスト名は整数の集合として構成されるわけではありません)
- DHCP サーバの IP アドレス (コントローラの IP アドレスを割り当てるのに使用されません)
- コントローラの時刻を同期化するのに使用される NTP サーバ (オプション)

固定 IP アドレスを割り当てるには、以下の情報を提供する必要があります。

- コントローラのホスト名 (IP アドレスの形式ではありません)
- コントローラの IP アドレス
- コントローラのサブネット マスク
- コントローラのデフォルト ゲートウェイの IP アドレス
- ローカル DNS サーバの IP アドレス
- ローカル ドメインの名前
- コントローラの時刻を同期化するのに使用される NTP サーバ (オプション)

セットアップ スクリプトの詳細については、『*FortiWLC (SD) 入門ガイド*』を参照してください。

使用例

基本的なシステム設定を行うための初期設定スクリプトを実行するには、`setup` コマンドを使用します (一部のみを以下に示します)。

```
default# setup
```

```
Begin system configuration ...
```

```
Country code configuration for this machine.
```

```
The country code is currently set to US
```

```
Would you like to change it [yes/no/quit]?:
```

```
.
```

```
.
```

```
.
```

show alarm

コントローラで認識されているクリアされていないアラームを表示します。

構文 `show alarm`

コマンド
モード 特権 EXEC

デフォルト なし

用途 接続されているアクセス ポイントに関連するものも含め、コントローラで認識されている保留およびクリアされていないアラームを表示します。各アラームの日時、重要度、そしてアラームが発行されたノードが表示されます。

保留およびクリアされていないアラームが存在しない場合は、以下のメッセージが表示されます。

Alarms Table(No entries)

使用例 以下のコマンドにより、現在保留になっているアラームが表示されます。

controller# **show alarm**
Alarms Table

Alarm Type	Severity	Timestamp	Content
AP Down	Critical	2005/05/14 21:57:17	Access Point AP-1 (1)
AP Down	Critical	2005/05/14 21:57:14	Access Point AP-25 (25)

以下の表では、**show alarm** により出力されるフィールドについて説明しています。

情報	説明
Alarm Type	<p>アラーム タイプ。以下のいずれかになります。</p> <p>AP Down (AP 停止) : コントローラと access point の接続が失われています。イーサネット ケーブルが access point に接続されていないか、access point がダウンしています。</p> <p>Watchdog Failure (監視機能の障害) : watchdog プロセスがハングしています。この問題を解決するにはシステムをリブートする必要があります。</p> <p>Rogue AP Detected (不正 AP の検出) : 承認されていない AP (許可リストにない AP) が検出されました。</p> <p>Certificate expired (証明書期限切れ) : 証明書の有効期限が切れたか、証明書がまだ使用されていません。</p>
Severity	アラームの重要度 (常に Critical)
Timestamp	<p>UTC のアラームの日時 (<i>year/month/day hh:mm:ss</i>)</p> <p><i>year</i> = 年</p> <p><i>month</i> = 月を表す数 (01 ~ 12)</p> <p><i>day</i> = 日</p> <p><i>hh</i> = 時 (00 ~ 23)</p> <p><i>mm</i> = 分</p> <p><i>ss</i> = 秒</p>
Content	<p>アラームの詳細。不正なアクセス ポイントに関するアラームの場合には、Content フィールドには MAC アドレス、BSSID、およびステーションが使用するチャンネルが一覧表示されます。ダウンしたアクセス ポイントの場合は、Content フィールドには AP の名前と番号が一覧表示されます。</p>

関連コマンド [alarm](#) (106 ページ)

show ap-neighbor

近接する AP を表示します。

構文

```
show ap-neighbor
show ap-neighbor <AP ID> <InterfaceList>
show ap-neighbor details
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

特定エリアの密度範囲を確認するには、これらのコマンドで、近接する AP をチェックします。近接する AP のリストには、コントローラが同じであるかどうかに加えて、近接する AP に関する次の情報が表示されます。

- AP ID
- Controller Index
- AP MAC アドレス
- RSSI

使用例

次の例は、近接する AP の詳細を表示します。

```
Engg-wifi-Main# sh ap-neighbor details
```

AP ID Number	Interface Id ControllerIndex	Serial Number Current	Channel RSSI	Neighbor AP ID	Serial
8	1	00:0c:e6:04:fc:b5	11	10	
00:0c:e6:04:f0:b6	18		-54		
8	2	00:0c:e6:04:fc:b5	149	10	
00:0c:e6:04:f0:b6	18		-54		
8	1	00:0c:e6:04:fc:b5	11	11	
00:0c:e6:04:fc:b7	18		-66		
8	2	00:0c:e6:04:fc:b5	149	11	
00:0c:e6:04:fc:b7	18		-70		
8	1	00:0c:e6:04:fc:b5	11	5	
00:0c:e6:05:06:07	0		-76		

8	1	00:0c:e6:04:fc:b5	11	15
00:0c:e6:05:eb:7c	18		-76	
8	2	00:0c:e6:04:fc:b5	149	15
00:0c:e6:05:eb:7c	18		-86	
8	2	00:0c:e6:04:fc:b5	149	13
00:0c:e6:05:eb:7d	18		-63	
8	1	00:0c:e6:04:fc:b5	11	4
00:0c:e6:07:9e:9b	18		-72	
8	2	00:0c:e6:04:fc:b5	149	4
00:0c:e6:07:9e:9b	18		-86	
3	1	00:0c:e6:05:eb:11	11	0
00:00:00:00:00:00	0		-40	
3	2	00:0c:e6:05:eb:11	11	6
00:0c:e6:00:68:3f	0		-84	
3	1	00:0c:e6:05:eb:11	11	4
00:0c:e6:04:3c:8f	0		-70	
3	1	00:0c:e6:05:eb:11	11	22
00:0c:e6:04:99:79	0		-64	
3	2	00:0c:e6:05:eb:11	149	1
00:0c:e6:04:fc:c7	18		-62	
3	1	00:0c:e6:05:eb:11	11	1
00:0c:e6:04:fd:dd	0		-44	
3	1	00:0c:e6:05:eb:11	11	5
00:0c:e6:05:06:07	0		-73	

次の例は、近接する AP を表示します。

Engg-wifi-Main# sh ap-neighbor

AP ID	Interface	Id	Channel	Local APs	Remote APs	RSSI L1	RSSI
L2		RSSI L3	RSSI L4				
8	1	11	4	2	0	1	
5		0					
8	2	149	4	0	0	1	
2		1					
3	1	11	4	6	1	2	
7		0					
3	2	11	5	1	0	1	
4		0					
2	1	11	4	5	1	2	
6		0					

2	2		11	5	1	1	0
3		1					
5	1		11	5	7	2	3
6		1					
5	2		11	4	1	1	0
3		1					
1	1		11	7	6	1	8
4		0					
1	2		11	6	1	0	4
3		0					
4	1		11	6	5	2	4
5		0					
4	2		11	9	1	0	2
5		2					
13	1		11	5	3	1	3
4		0					
13	2		11	6	1	1	1
4		0					
10	1		11	4	5	1	2
5		1					
10	2		11	5	1	1	2
2		0					
11	1		11	5	7	0	4
7		0					
11	2		11	5	1	0	2
2		1					
15	1		11	7	6	1	5
7		0					
15	2		11	8	1	0	2
5		2					

AP Neighbors Consolidated List(20 entries)

次のコマンドは、特定のインターフェイスの特定の AP から見える近接する AP を表示します。

Engg-wifi-Main# **sh ap-neighbor 1 1**

AP ID	Interface	Id	Serial Number	Channel	Neighbor AP ID	Serial
Number		ControllerIndex	Current	RSSI		
1	1		00:0c:e6:04:fc:c7	11	0	
00:00:00:00:00:00		0		-79		
1	1		00:0c:e6:04:fc:c7	11	4	
00:0c:e6:04:3c:8f		0		-49		

1	1	00:0c:e6:04:fc:c7	11	11
00:0c:e6:04:fc:b7	18		-65	
1	1	00:0c:e6:04:fc:c7	11	1
00:0c:e6:04:fd:dd	0		-42	
1	1	00:0c:e6:04:fc:c7	11	5
00:0c:e6:05:06:07	0		-55	
1	1	00:0c:e6:04:fc:c7	11	8
00:0c:e6:05:ca:05	0		-56	
1	1	00:0c:e6:04:fc:c7	11	2
00:0c:e6:05:ea:e8	18		-63	
1	1	00:0c:e6:04:fc:c7	11	3
00:0c:e6:05:eb:11	18		-57	
1	1	00:0c:e6:04:fc:c7	11	15
00:0c:e6:05:eb:7c	18		-52	
1	1	00:0c:e6:04:fc:c7	11	4
00:0c:e6:07:9e:9b	18		-63	
1	1	00:0c:e6:04:fc:c7	11	5
00:0c:e6:07:9f:1d	18		-65	

AP Neighbors List(11 entries)

Engg-wifi-Main# sh ap-neighbor 1 2

AP ID	Interface Id	Serial Number	Channel	Neighbor AP ID	Serial
Number	ControllerIndex	Current	RSSI		
1	2	00:0c:e6:04:fc:c7	11	6	
00:0c:e6:00:68:3f	0		-64		
1	2	00:0c:e6:04:fc:c7	149	11	
00:0c:e6:04:fc:b7	18		-81		
1	2	00:0c:e6:04:fc:c7	149	2	
00:0c:e6:05:ea:e8	18		-72		
1	2	00:0c:e6:04:fc:c7	149	3	
00:0c:e6:05:eb:11	18		-61		
1	2	00:0c:e6:04:fc:c7	149	15	
00:0c:e6:05:eb:7c	18		-61		
1	2	00:0c:e6:04:fc:c7	149	4	
00:0c:e6:07:9e:9b	18		-63		
1	2	00:0c:e6:04:fc:c7	149	5	
00:0c:e6:07:9f:1d	18		-71		

AP Neighbors List(7 entries)

show bonding

イーサネット ポート ボンディング統計を表示します。

構文

```
show bonding
show bonding full
```

full オプションを追加すると、詳細のボンディング設定情報が表示されます。

コマンド モード

特権 EXEC

デフォルト

なし

用途

ボンディングでは、イーサネットを並列で使用することで、スループットが向上します (ポート トランキングやリンク集約とも呼ばれます)。この機能は、AMC イーサネット ポート カードを装備する MC4100 と MC5000 でサポートしています。FastPath モード アクセラレーションと組み合わせると、スループットはさらに増加します。

使用例

次のコマンドを使用すると、AMC アクセラレータ カードを装備する MC4100 と MC5000 のポート ボンディング統計が表示されます。

```
default# show bonding
Current bonding configuration = single
Master bonding interface 0:
  Master interface 0 num slave interfaces = 1
  Slave interface 0-0:
    Slave interface 0-0 link status = up
* Use 'show bonding full' to display more details.
default#
```

次の例では、デュアル ボンディング設定が表示されます。

```
default# show bonding
Current bonding configuration = dual
Master bonding interface 0:
  Master interface 0 num slave interfaces = 1
  Slave interface 0-0:
```

```
Slave interface 0-0 link status          = up
Master bonding interface 1:
  Master interface 1 num slave interfaces = 1
  Slave interface 1-0:
    Slave interface 1-0 link status      = down
* Use 'show bonding full' to display more details.
default#
```

関連コマンド [bonding \(111 ページ\)](#)

show calendar

ハードウェア クロックの現在の日付と時刻を表示します。

構文

show calendar

コマンド モード

特権 EXEC

デフォルト

なし

使用例

以下のコマンドを指定すると、ハードウェア クロックの現在の日時が表示されます。

```
controller# show calendar  
Thu Mar 6 14:00:12 UTC 2008  
controller#
```

関連コマンド

- [calendar set \(113 ページ\)](#)
- [date \(119 ページ\)](#)

show client-locator

ping パケットをフォーティネットのシステムに接続している特定の OUI に送信します。

構文

```
show client-locator  
no client-locator
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、ping パケットをフォーティネットのシステムに接続している特定の OUI に送信します。このコマンドは主に、サイレント モードのクライアントに使用します。

使用例

次の例では、クライアント ロケータを有効にし、無効にします。

```
corpwifi# client-locator  
corpwifi# sh client-locator  
Client Locator utility is enabled  
corpwifi# no client-locator  
corpwifi# sh client-locator  
Client Locator utility is disabled
```

関連コマンド

show controller

コントローラの設定情報を表示します。

構文 `show controller`

コマンド
モード 特権 EXEC

デフォルト なし

用途 `show controller` コマンドを使用して、コントローラのグローバル パラメータを表示します。以下のコントローラ情報が表示されます。

パラメータ	説明
Controller ID	コントローラの ID 番号。
Description	コントローラの説明 (オプション)。
Host Name	コントローラのホスト名。
Uptime	コントローラが起動してからの経過時間。
Location	コントローラの場所の説明 (オプション)。
Contact	コントローラに関して管理者からの支援が必要となった場合に連絡する担当者や担当部署の説明 (オプション)。
Operational State	コントローラの稼働状況。コントローラが稼働している場合の状態は enabled となり、稼働していない場合の状態は disabled となります。
Availability Status	コントローラの可用性。コントローラは、 online または offline になります。
Alarm State	アラーム状態として、 No Alarms になるか、 Critical などの状態を示します。

パラメータ	説明
Automatic AP Upgrade	On は、AP がコントローラに関連付けられる際に、AP をコントローラ上で稼働するソフトウェアのバージョンに自動的にアップグレードすることを示します。 Off は、この機能がアクティブではないことを示します。
Virtual IP Address	コントローラに割り当てられた仮想 IP アドレス。
Virtual Netmask	コントローラに割り当てられた仮想ネットマスク。
Default Gateway	デフォルト ゲートウェイの IP アドレス。
DHCP Server	動的なアドレス割り当てがコントローラに適用されている場合、DHCP 要求が転送されるサーバの IP アドレスが表示されます。
Statistics Polling Period (seconds)	渡されたパケット数やドロップしたパケット数などの統計情報をコントローラがポーリングする前に経過させる必要がある時間。
Audit Polling Period (seconds)	コントローラが監査情報を収集する前に経過させる必要がある時間。
Software Version	コントローラで実行中のソフトウェアのバージョン。
Network Device ID	コントローラのシリアル番号 (MAC アドレス)。
System ID	コントローラのシステム ID。
Default AP Init Script	デフォルトの初期化スクリプトの名前。このスクリプトは、スクリプトが明示的に指定されていないアクセス ポイントに対して実行されます。このスクリプトは、/ATS/scripts ディレクトリに存在する必要があります。
DHCP Relay Pass-Through	パススルー モードが DHCP リレー サーバで有効になっているかどうかを示します。
Encryption Module Status	任意の暗号化処理モジュールがコントローラ内に存在するかどうかを表示します。インストールされている場合、このパラメータは Online を表示します。インストールされていない場合、このパラメータは Not Installed を表示します。
Controller Model	コントローラのモデルを表示します。
Region Setting	コントローラが国際的モデルか米国限定モデルかを指定します (DFS の目的で使用)。

パラメータ	説明
Country Setting	コントローラが設置された国名を表示します。
Manufacturing Serial #	コントローラのシリアル番号。
Management by wireless stations	on に設定すると、コントローラへのワイヤレス管理アクセスが有効になります。 off に設定すると、ワイヤレスでは変更できません。
Controller Index	仮想セルが設定されている場合、仮想ポートがオフであれば 0、仮想ポートが設定 されていれば数値が表示されます。
Topology Information Update	トポロジ情報のアップデートは、トラブルシューティングやデバッグ情報の収集に役立ちます。トラブルシューティングやデバッグ情報の収集が必要な場合にのみ、この機能を有効にすることを推奨します。
AeroScout	Aeroscout が有効であると、タグのトラッキングが有効になります。AeroScout は、ラップトップのようなモバイル装置とはタグのメッセージが異なります。フォーティネットはタグのアセット トラッキングをサポートしています。
FastPath Mode	FastPath Mode が on の場合、スループットが高速になります。
Bonding Mode	Bonding Mode は、 single または dual です。ボンディングでは、イーサネットを並列で使用することで、スループットが向上します (ポート トランッキングやリンク集約とも呼ばれます)。この機能は、AMC イーサネット ポート カードを装備する MC4100 と MC5000 でサポートしています。FastPath モード アクセラレーションと組み合わせると、スループットはさらに増加します。
DFS	DFS が enabled であると、特定のフォルダをホストするすべてのサーバで同期データの複製が実行されます。
Station Aging Out Period (minutes)	

使用例

以下のコマンドは、コントローラ設定情報を表示します。

```
InteropLab# show controller
Global Controller Parameters
```


Controller ID	: 1
Description	: InteropLab
Host Name	: InteropLab
Uptime	: 47d:18h:55m:55s
Location	: DC Cabinet 6
Contact	: Network Group
Operational State	: Enabled
Availability Status	: Online
Alarm State	: No Alarm
Automatic AP Upgrade	: off
Virtual IP Address	: 172.26.96.11
Virtual Netmask	: 255.255.255.0
Default Gateway	: 172.26.96.1
DHCP Server	: 10.0.0.10
Statistics Polling Period (seconds)/0 disable Polling	: 60
Audit Polling Period (seconds)/0 disable Polling	: 60
Software Version	: 4.0-15
Network Device Id	: 00:90:0b:0e:a8:61
System Id	: 1FC4B274070D
Default AP Init Script	:
DHCP Relay Passthrough	: on
Controller Model	: MC1000
Country Setting America	: United States Of
Manufacturing Serial #	: 2008MC10001039
Management by wireless stations	: on
Controller Index	: 0
Topology Information Update	: off
AeroScout Enable/Disable	: disable
FastPath Mode	: on
Bonding Mode	: single
DFS	: disable
Station Aging Out Period(minutes)	: 0
InteropLab-MC1000#	

関連コマンド

- [show controller cpu-utilization \(177 ページ\)](#)

- [*show controller file systems*](#) (178 ページ)
- [*show controller memory*](#) (180 ページ)
- [*show controller processes*](#) (182 ページ)

show controller cpu-utilization

コントローラの CPU 使用率を表示します。

構文

`show controller cpu-utilization`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show controller cpu-utilization` コマンドを使用して、コントローラの CPU 使用率を表示します。実行中のプロセスのリストと同時に一般的な利用状況情報もリアルタイムで更新されながら表示されます。CTRL-C を使用すると、CLI プロンプトに戻ります。CPU 使用率は、使用した CPU 時間をプロセスの実行時間で除算したもので計算され、パーセントで表されます。すべてを加算しても 100% になることはほとんどありません。

使用例

以下のコマンドを指定すると、コントローラの CPU 使用率が表示されます。

```
controller# show controller cpu-utilization
```

関連コマンド

- [show controller \(172 ページ\)](#)
- [show controller file systems \(178 ページ\)](#)
- [show controller memory \(180 ページ\)](#)
- [show controller processes \(182 ページ\)](#)

show controller file systems

コントローラのファイル システム情報を表示します。

構文 `show controller file systems`

コマンド
モード 特権 EXEC

デフォルト なし

用途 このコマンドはシステム ディレクトリとファイル システムについての情報を表示します。
このコマンドにより次の情報が表示されます。

パラメータ	説明
Filesystem	ファイル システムの名前を表示します。ディレクトリの場合、 none を表示します。
1K blocks	ファイル システムまたはディレクトリが使用するように設定されている 1K バイト ブロック数を表示します。
Used	ファイル システムまたはディレクトリが現在使用している 1K バイト ブロック数を表示します。
Available	ファイル システムまたはディレクトリが使用可能な 1K バイト ブロック数 (空きスペース) を表示します。
Use %	ファイル システムまたはディレクトリが現在使用している使用可能なブロックの割合 (%) を表示します。
Mounted on	ファイル システムがマウントされているマウント ポイントを表示するか、ディレクトリのパス名をリストします。

使用例 以下のコマンドを指定すると、コントローラのファイル システム情報が表示されます。

controller# `show controller file systems`

Filesystem 1k-blocks Used Available Use% Mounted on

/dev/hdc	420453	145615	252426	37%	/
none	4880	40	4840	1%	/dev/shm
none	9764	4820	4944	50%	/var/run
none	9764	308	9456	4%	/var/log
none	9764	0	9764	0%	/tmp
none	9764	0	9764	0%	/capture

controller#

関連コマンド

- [show controller \(172 ページ\)](#)
- [show controller cpu-utilization \(177 ページ\)](#)
- [show controller memory \(180 ページ\)](#)
- [show controller processes \(182 ページ\)](#)

show controller memory

実行中のプロセスで使用されているメモリを表示します。

構文

```
show controller memory
show memory
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドはコントローラのメモリの利用状況を表示します。

使用例

```
controller# show controller memory
total:      used:      free:  shared: buffers:  cached:
Mem:  527548416 237649920 289898496          0 6414336 129626112
Swap:           0           0           0
MemTotal:           515184 kB
MemFree:            283104 kB
MemShared:           0 kB
Buffers:             6264 kB
Cached:             126588 kB
SwapCached:          0 kB
Active:             140332 kB
Inact_dirty:         19204 kB
Inact_clean:         28012 kB
Inact_target:        37508 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:            515184 kB
LowFree:             283104 kB
SwapTotal:           0 kB
SwapFree:            0 kB
Committed_AS:       656468 kB
controller#
```

関連コマンド

- [show controller \(172 ページ\)](#)
- [show controller cpu-utilization \(177 ページ\)](#)
- [show controller file systems \(178 ページ\)](#)
- [show controller processes \(182 ページ\)](#)

show controller processes

実行中のすべてのコントローラ プロセスに関する情報を表示します。

構文 `show controller processes`

コマンド
モード 特権 EXEC

デフォルト なし

用途 このコマンドはコントローラ プロセスのリストを表示します。各プロセスについて、以下の情報が表示されます。

パラメータ	説明
UID	(ユーザ ID) プロセスを所有するユーザ名を表示します。
PID	(プロセス ID) プロセスの ID 番号を表示します。
PPID	(親プロセス ID) このプロセスの親となるプロセスの番号を表示します。
C	
STIME	プロセスが開始したときのシステム時間を表示します。
TTY	プロセスが開始したときのターミナル情報を表示します。
TIME	プロセスの総実行時間を表示します。
CMD	プロセスの名前を表示します。

使用例 以下のサンプル コマンドでは、現在のシステム プロセスの一部が表示されます。

```
controller# show controller processes
UID      PID  PPID  C STIME TTY          TIME CMD
root      1    0  0 Oct14 ?        00:00:05 init
root      2    1  0 Oct14 ?        00:00:00 [keventd]
```


root	3	1	0	Oct14	?	00:00:04	[ksoftirqd_CPU0]
root	4	1	0	Oct14	?	00:00:00	[kswapd]
root	5	1	0	Oct14	?	00:00:00	[bdf flush]
root	6	1	0	Oct14	?	00:00:00	[kupdated]
root	223	1	0	Oct14	?	00:00:00	syslogd -m 0
root	228	1	0	Oct14	?	00:00:00	klogd -x
root	238	1	0	Oct14	?	00:00:01	/usr/sbin/sshd

関連コマンド

- [show controller \(172 ページ\)](#)
- [show controller cpu-utilization \(177 ページ\)](#)
- [show controller file systems \(178 ページ\)](#)
- [show controller memory \(180 ページ\)](#)

show controller mobility-vars

適切な RSSI 値についての情報を表示します。

構文 `show controller mobility-vars`

コマンドモード 特権 EXEC

デフォルト なし

用途 このコマンドは、現在の適切な RSSI 値を表示します。

パラメータ	説明
Topology Update	トポロジ情報のアップデートは、トラブルシューティングやデバッグ情報の収集に役立ちます。トラブルシューティングやデバッグ情報の収集が必要な場合にのみ、この機能を有効にすることを推奨します。以下のいずれかのオプションを選択します。 On : コントローラでトポロジ情報のアップデートを有効にします。 Off : トポロジ情報のアップデートを無効にします。これがデフォルト設定です。
AssocStationMaxIdle	関連付けられているステーションの最大アイドル時間。
Adequate RSSI	現在設定されている適切な RSSI 値。

使用例 以下の例は、現在の RSSI 値を示しています。

```
default (15)# show controller mobility-vars
Topology Update      AssocStationMaxIdle      Adequate RSSI
off                  2000                      -58
Controller Mobility Configuration Parameters(1 entry)
```

関連コマンド

- [show controller \(172 ページ\)](#)

show event

コントローラで認識されているクリアされていないイベントを表示します。

構文 `show event`

コマンド
モード 特権 EXEC

デフォルト なし

用途 接続されているアクセス ポイントに関連するものも含め、コントローラで認識されている保留およびクリアされていないイベントを表示します。各イベントの日時、重要度、そしてアラームが発行されたノードが表示されます。

保留およびクリアされていないイベントが存在しない場合は、以下のメッセージが表示されます。

Events Table(No entries)

使用例 以下のコマンドにより、現在保留になっているイベントが表示されます。

```
controller# show event
Events Table
```

Event Name	Severity	Source	FDN
Raised At	Detail Information		
User 802.1x Authentication Fail Major 00:23:1 07/26/2013 12:21:21 Acces		controller	SD-ST-3-DAbcWebAuth-
s Request rejected for User: <host/meru-it-THINK>, NAS IP: <172.29.0.137>, SSID: <DAbcWebAuth>, Calling Station ID: <00:23:14:ae:b9:28>, Called Station ID			
User 802.1x Authentication Fail Major 44:d8:8 07/26/2013 11:56:31 Acces		controller	SD-ST-3-DAbcWebAuth-
s Request rejected for User: <meru>, NAS IP: <172.29.0.137>, SSID: <DAbcWebAuth>, Calling Station ID: <44:d8:84:b6:42:6d>, Called Station ID: <00:90:0b:23			

以下の表では、`show event` により出力されるフィールドについて説明しています。

情報	説明
Event Type	<p>イベント タイプ。以下のいずれかになります。</p> <p>AP Down (AP 停止) : コントローラと access point の接続が失われています。イーサネット ケーブルが access point に接続されていないか、access point がダウンしています。</p> <p>Watchdog Failure (監視機能の障害) : watchdog プロセスがハングしています。この問題を解決するにはシステムをリブートする必要があります。</p> <p>Rogue AP Detected (不正 AP の検出) : 承認されていない AP (許可リストにない AP) が検出されました。</p> <p>Certificate expired (証明書期限切れ) : 証明書の有効期限が切れたか、証明書がまだ使用されていません。</p>
Severity	イベントの重要度 (常に Critical)
Timestamp	<p>UTC のイベントの日時 (<i>year/month/day hh:mm:ss</i>)</p> <p><i>year</i> = 年</p> <p><i>month</i> = 月を表す数 (01 ~ 12)</p> <p><i>day</i> = 日</p> <p><i>hh</i> = 時 (00 ~ 23)</p> <p><i>mm</i> = 分</p> <p><i>ss</i> = 秒</p>
Content	<p>イベントの詳細。不正なアクセス ポイントに関するアラームの場合には、Content フィールドには MAC アドレス、BSSID、およびステーションが使用するチャンネルが一覧表示されます。ダウンしたアクセス ポイントの場合は、Content フィールドには AP の名前と番号が一覧表示されます。</p>

関連コマンド [event \(121 ページ\)](#)

show fastpath

fastpath アクセラレータ統計を表示します。

構文

```
show fastpath
show fastpath cache
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

show fastpath コマンドを使用すると、fastpath 統計のほか、fastpath 状態、処理済みのパケット、キャッシュ ステータスなどが表示されます。

show fastpath cache コマンドを使用し、fastpath キャッシュ エントリを表示します。

使用例

次のコマンドを使用し、fastpath および fastpath キャッシュ統計を表示します。

```
MC500# show fastpath
```

```
Fastpath status:           On
Hardware acceleration:     Off
Number of accel engines:   1

Cache width:                32768
Cache depth:                8
Cache adds:                 0
Cache deletes:              0
Cache flushes:              22
Cache updates:              0
Cache replaces:             0
Cache active entries:       0
Cache collisions:           0
Total packets:              196049
Eligible packets:           186087
Downstream trials:          186097
```

```
Downstream hits:      0
Upstream trials:      0
Upstream hits:        0
Hits, 1st try:        0
Hits, 2nd try:        0
Hits, Nth try:        0
```

MC500# **show fastpath cache**

Upstream Cache Entries:

Buckt	E	D	Source IP	Port	Destination IP	Port	PR	Station MAC
Upstream			MAC	VLAN				

Downstream Cache Entries:

Buckt	E	D	Source IP	Port	Destination IP	Port	PR	Station MAC
Downstream			MAC	AP IP	Port			

関連コマンド [fastpath \(124 ページ\)](#)

show features

インストールされているパッチ機能を表示します。

show fingerprints

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します。

構文

show fingerprints

コマンドモード

特権 EXEC

デフォルト

なし

用途

デバイス フィンガープリントを使用すると、使用中のデバイスの OS およびタイプをシグネチャをベースに検出して表示できます。**show fingerprints** コマンドを使用して、現在設定されているデバイス フィンガープリントを表示します。

使用例

```
controller# show fingerprints
ID | Option 55 Description | Hexadecimal characters
1 Apple iOS 370103060f77fc
2 Apple Mac OSX 370103060f775ffc2c2e2f
3 Cisco VoIP Phone 370103060c0f1c2a429596
4 Google Android 2.x 3701792103
5 Google Android 2.1 370103061c21333a3b79
6 Google Android 2.3.x 3701792103061c333a3b
7 Google Android JellyBean 37012103060f1c333a3b
8 Google Android 2.3.6 3701792103060f1c333a3b77
9 Blackberry OS 370103060f
10 Nokia Maemo OS 370103060c0f111c28292a
11 Microsoft Windows7-Vista 37010f03062c2e2f1f2179f92b
12 Microsoft WindowsXP 37010f03062c2e2f1f21f92b
13 Microsoft Windows Phone 7 370103060f2c2e2f
14 Symbian OS 370c060f01031c78
15 Debian/Linux 2.6 generic 37011c02030f0677
16 Linux (unknown) 37011c02030f06770c2c2f1a792a
17 Ubuntu OS 37011c02030f06770c2c2f1a792a79f9fc2a
18 Palm OS 37011c02030f060c
```

関連コマンド

[fingerprint \(125 ページ\)](#)

show flash

システム イメージ ファイル名をフラッシュ メモリに表示します。

構文

show flash

コマンド モード

特権 EXEC

デフォルト

なし

用途

show flash コマンドを使用してフラッシュ メモリにあるシステム イメージのファイル名を表示します。

使用例

以下のコマンドを指定すると、フラッシュ メモリにあるシステム イメージの一覧が表示されます。

```
controller# show flash  
3.2-116  
3.1-139  
controller#
```

関連コマンド

[delete](#) (77 ページ)

show guest-user

キャプティブ ポータル ゲスト ユーザのアカウント情報を表示します。

構文

`show guest-user`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show guest-user` コマンドを使用して、ゲスト ユーザ アカウント情報を表示します。

各エントリにはアカウントの名前、アカウントがアクティブになる日付、およびアカウントが非アクティブになる日付が表示されます。

使用例

次のコマンドは、ゲスト ユーザ アカウントを表示します。

```
controller# show guest-user
Guest User Name      Service Start Time      Service End Time
frieda 05/30/2008 12:00:00      05/30/2008 15:00:00
      Guest User Table(1 entry)
```

関連コマンド

- [guest-user \(126 ページ\)](#)
- [ping \(142 ページ\)](#)

show interfaces accel

アクセラレート イーサネット ポート統計を表示します。

構文

```
show interfaces accel  
show interfaces accel <n>  
show interfaces accel <n> realtime
```

n 表示するアクセラレート インターフェイス (1、2 など)。

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、MC4100 にインストールされているアクセラレート イーサネット インターフェイス カード数を表示します。realtime オプションを使用すると、ステータスを連続して表示できます。

使用例

以下のコマンドは、MC4100 のアクセラレート カード統計を表示します。

```
mc4100# show interfaces accel
```

関連コマンド

show hostname

コントローラのホスト名を表示します。

構文

`show hostname`

コマンド モード

特権 EXEC

デフォルト

デフォルトのホスト名は *default* です。

用途

`show hostname` コマンドを使用して、コントローラのホスト名を表示します。ホスト名を変更しなかった場合、コントローラのホスト名は *default* です。

ホスト名は、`setup` または `hostname` コマンドで変更できます。

使用例

次のコマンドを使用すると、コントローラのホスト名 *controller* を表示します。

```
controller# show hostname
controller
controller#
```

関連コマンド

- [hostname \(128 ページ\)](#)
- [setup \(160 ページ\)](#)

show license

システムのライセンスを表示します。

構文

show license

コマンドモード

特権 EXEC

デフォルト

システムのライセンスを表示します。

用途

show license コマンドを使用して、すべての WLAN コントローラと AP のシステム ライセンスのステータスを表示します。このコマンドにより次の情報が表示されます。

パラメータ	説明
Feature Name	ライセンスを受けている機能の名前を表示します (コントローラまたは AP)。
CtrlStatus	高可用性設定となっている場合に、コントローラのステータス (アクティブまたはスタンバイ) を表示します。
LicenseType	使用中のライセンスのタイプとして、temporary (一時) または permanent (永久) を表示します。
Expiry Date	一時ライセンスが失効する日付を表示します。ライセンスが永久である場合、このフィールドには「-」が表示されます。
TotalCount	このライセンスの対象となっているエンティティの総数を表示します。
InUse	現在使用中となっているライセンスを受けているエンティティの数を表示します。

使用例

以下のコマンドを使用すると、システム ライセンス表 (サンプル) が表示されます。

```
meru-wifi# show license
```

Feature Name	CtlrStatus	LicenseType	Expiry Date	TotalCount	InUse
controller	active	permanent	-	1	1
ap	active	permanent	-	150	0
License Table(2)					

関連コマンド

- [copy \(73 ページ\)](#)
- [license \(133 ページ\)](#)
- [show license-file \(201 ページ\)](#)

show ip udp-broadcast downstream all-ports

ブロードキャスト ダウンストリーム ポートの状態を表示します。

構文

```
show ip udp-broadcast downstream all-ports
```

コマンドモード

EXEC モード

デフォルト

なし

用途

このコマンドを使用して、すべてのダウンストリーム udp-broadcast ストリームが **on** または **selected** のどちらであるかを表示します。このコマンドの **selected** バージョンがアクティブの場合にコマンド `show ip udp-broadcast downstream all-ports` を使用すると、レガシー コマンド `ip udp-broadcast downstream <portNumber>` で有効になった最大 8 つのポートのリストが表示されます。

使用例

このコマンドは、ダウンストリーム ブロードキャスト ポートの状態を表示します。

```
default# show ip udp-broadcast downstream all-ports
Downstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

関連コマンド

- [show ip udp-broadcast upstream all-ports \(199 ページ\)](#)
- [show ip udp-broadcast upstream-bridged all-ports \(200 ページ\)](#)
- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [ip udp-broadcast upstream \(131 ページ\)](#)
- [ip udp-broadcast upstream-bridged \(132 ページ\)](#)

show ip udp-broadcast downstream-bridged all-ports

ブロードキャスト ダウンストリーム ブリッジ ポートの状態を表示します。

構文

```
show ip udp-broadcast downstream-bridged all-ports
```

コマンドモード

EXEC モード

デフォルト

なし

用途

このコマンドを使用して、すべてのダウンストリーム ブリッジ udp-broadcast ストリームが **on** または **selected** のどちらであるかを表示します。このコマンドの **selected** バージョンがアクティブの場合にコマンド **show ip udp-broadcast downstream-bridged all-ports** を使用すると、レガシー コマンド **ip udp-broadcast downstream-bridged <portNumber>** で有効になった最大 8 つのポートのリストが表示されます。

使用例

このコマンドは、ダウンストリーム ブリッジ ブロードキャスト ポートの状態を表示します。

```
default# show ip udp-broadcast downstream-bridged all-ports
Downstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

関連コマンド

- [show ip udp-broadcast upstream all-ports \(199 ページ\)](#)
- [show ip udp-broadcast upstream-bridged all-ports \(200 ページ\)](#)
- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [ip udp-broadcast upstream \(131 ページ\)](#)
- [ip udp-broadcast upstream-bridged \(132 ページ\)](#)

show ip udp-broadcast upstream all-ports

ブロードキャスト アップストリーム ブロードキャスト ポートの状態を表示します。

構文

```
show ip udp-broadcast upstream all-ports
```

コマンドモード

EXEC モード

デフォルト

なし

用途

このコマンドを使用して、すべてのアップストリーム udp-broadcast ストリームが **on** または **selected** のどちらであるかを表示します。このコマンドの **selected** バージョンがアクティブの場合にコマンド `show ip udp-broadcast upstream all-ports` を使用すると、レガシー コマンド `ip udp-broadcast upstream <portNumber>` で有効になった最大 8 つのポートのリストが表示されます。

使用例

このコマンドは、すべてのポートのアップストリーム ブロードキャストの状態を表示します。

```
default# show ip udp-broadcast upstream all-ports
Upstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

関連コマンド

- [show ip udp-broadcast downstream all-ports \(197 ページ\)](#)
- [show ip udp-broadcast downstream-bridged all-ports \(198 ページ\)](#)
- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [ip udp-broadcast upstream \(131 ページ\)](#)
- [ip udp-broadcast upstream-bridged \(132 ページ\)](#)

show ip udp-broadcast upstream-bridged all-ports

ブロードキャスト アップストリーム ブロードキャスト ブリッジ ポートの状態を表示します。

構文

```
show ip udp-broadcast upstream-bridged all-ports
```

コマンドモード

EXEC モード

デフォルト

なし

用途

このコマンドを使用して、すべてのアップストリーム ブリッジ udp-broadcast ストリームが **on** または **selected** のどちらであるかを表示します。このコマンドの **selected** バージョンがアクティブの場合にコマンド `show ip udp-broadcast upstream-bridged all-ports` を使用すると、レガシー コマンド `ip udp-broadcast upstream-bridged <portNumber>` で有効になった最大 8 つのポートのリストが表示されます。

使用例

このコマンドは、すべてのポートのアップストリーム ブロードキャストの状態を表示します。

```
default# show ip udp-broadcast upstream-bridged all-ports
Upstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

関連コマンド

- [show ip udp-broadcast downstream all-ports \(197 ページ\)](#)
- [show ip udp-broadcast downstream-bridged all-ports \(198 ページ\)](#)
- [ip udp-broadcast downstream \(129 ページ\)](#)
- [ip udp-broadcast downstream-bridged \(130 ページ\)](#)
- [ip udp-broadcast upstream \(131 ページ\)](#)
- [ip udp-broadcast upstream-bridged \(132 ページ\)](#)

show license-file

システム ライセンス ファイルの内容を表示します。

構文

`show license-file`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show license-file` コマンドを使用して、アクティブまたはスタンバイ コントローラのライセンスの詳細な内容を表示します。出力にはライセンスされている機能も表示されます。

使用例

次の例は、アクティブ コントローラのライセンスの内容を示します。

```
slave# show license-file

----- STANDALONE LICENSE -----

SERVER this_host ANY
VENDOR Merud
USE_SERVER
INCREMENT controller merud 1.0 permanent 1 \
    HOSTID=COMPOSITE=2F402A47C8FE ISSUED=19-mar-2007 \
    START=16-jan-2007 SIGN="00E5 BBB3 2865 4C8C A6C0 57E9 B12F \
    1F00 4F91 ED66 12BB 7009 924B 8337 FD9C"
INCREMENT ap merud 1.0 permanent 150 HOSTID=COMPOSITE=2F402A47C8FE \
    ISSUED=19-mar-2007 START=16-jan-2007 SIGN="0082 37BB 8DB1 F8C3 \
    D379 5691 D6C3 2400 7C79 45EC BF94 427A 1507 FC9B A583"
```

関連コマンド

- [license \(133 ページ\)](#)
- [show license \(195 ページ\)](#)

show log

システム ログを表示します。

構文

`show log [running-config]`

コマンド モード

特権 EXEC

デフォルト

システム ログを表示します。

用途

`show log` コマンドを使用して、コントローラのシステム ログを表示します。オプションのキーワード **running-config** を使用すると、実行中の設定のみのログが表示されます。リリース 4.1 でこのコマンドが拡張され、設定の変更 (CLI または GUI)、主なコマンド、イベント、操作、およびエラーが表示されるようになりました。

使用例

次の例は、通常はとても長いコントローラのログの数行です。

```
meru-wifi# show log
```

```
Aug  8 09:46:19 meru-wifi ALARM: AP DOWN CRITICAL Access Point #10-1F-Mktg-208 (10) at location Near printer
```

```
Aug  8 09:46:19 meru-wifi ALARM: 11235195791 | system | info | ALR | AP DOWN CRITICAL Access Point #10-1F-Mktg-208 (10) at location Near printer
```

```
Aug  8 9:46:22 meru-wifi ALARM: AP UP Access Point #10-1F-Mktg-208 (10) is up
```

```
Aug  8 9:46:22 meru-wifi ALARM: 11235195821 | system | info | ALR | AP UP Access Point #10-1F-Mktg-208 (10) is up
```

```
Aug  8 13:42:34 meru-wifi ALARM: AP DOWN CRITICAL Access Point #10-1F-Mktg-208 (10) at location Near printer
```

関連コマンド

- [show running-config \(90 ページ\)](#)
- [syslog-host \(228 ページ\)](#)

show nms-server

コントローラの E(z)rf Network Manager Service Appliance の IP アドレスと、E(z)RF バージョン、接続のステータスを表示します。

構文

show nms-server

コマンドモード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、Network Manager のコントローラのサーバ ID、サーバ IP、コントローラ ID、サービス アプライアンスの Network Manager のバージョン、および Network Manager の接続ステータスを表示します。

使用例

次の例は、コントローラの Network Manager の情報を表示します。

```
corpwifi# sh nms-server
```

Server ID	Server IP	Controller ID	NmsAgent Version	Server connectivity status
1	192.168.34.210	5	2.1-4.0-A-98	connected

関連コマンド

show ntp-server

割り当てられているネットワーク タイム プロトコル (NTP) サーバを表示します。

構文

`show ntp-server`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show ntp-server` コマンドを使用して `ntp server` コマンドで指定されている NTP サーバを表示します。

使用例

以下のコマンドにより、NTP サーバが表示されます。

```
MC4200-1(15)# show ntp-server
NTP updates are enabled.
Server: asia.pool.ntp.org
```

関連コマンド

[ntp \(139 ページ\)](#)

show roaming-domain

ローミング ドメイン設定のステータスを表示します。

構文

```
show roaming-domain  
show roaming-domain all
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

show roaming-domain コマンドを使用して **roaming-domain** コマンドで指定された ICR ローミング ドメイン グループのステータスを表示します。all 引数を使用して、詳細を表示します。

使用例

以下のコマンドにより、ローミング ドメイン ステータスが表示されます。

```
MC500# show roaming-domain  
Roaming domain configuration:
```

```
Controller 192.168.1.100  
Controller 192.168.2.101
```

```
Roaming domain is active.
```

以下では、**all** 引数を使用し、詳細なバージョンを表示します。

```
MC500# show roaming-domain all  
Roaming domain configuration:
```

```
Controller 192.168.1.100  
Controller 192.168.2.101
```

```
Roaming domain is active.Running Status:
```

```
[05/23 07:48:042] Roaming state:
```

My Interface Addresses:

VLAN	IP	Netmask	MAC	Device	IP
0	192.168.1.30	255.255.255.0	00:02:b6:35:33:d2		native
	192.168.1.30				

Peer Controllers:

IP	Tunnel IP	VLAN
192.168.1.100	10.235.0.1	-1
192.168.2.101	10.235.0.2	-1

関連コマンド [roaming-domain \(157 ページ\)](#)

show syslog-file

外部システム ログ ファイルが存在する場合、それを表示します。

構文

```
show syslog-file
show syslog-file <facility>
```

facility オプションの facility パラメータは、出力をフィルタリングして、そのファシリティのみのエントリを表示します。facility には、次のようなエントリがあります。

```
802. モビリティ
バルクアップデート
nms
qos
security
system
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、外部のシステム ログ ファイルが存在する場合にその内容を表示します。デフォルトでは、外部ロギングは無効になっています。syslog-host コマンドを使用して、外部のシステム ログ ホストを設定できます。

使用例

以下のコマンドにより、syslog ファイル アップグレード モジュールが表示されます。

```
controller# show syslog-file upgrade
```

Line	Priority	Mnemonic	Time	Record
1	info	UPG	2008/01/17 00:43:12	Upgrade AP(s) from:3.6-6 to:3.6-6
2	info	UPG	2008/01/17 00:43:12	Upgrade AP 1 START
3	info	UPG	2008/01/17 00:43:12	Upgrade AP 2 START
4	info	UPG	2008/01/17 00:43:12	Upgrade AP 1 Upgrade Requested

5	info	UPG	2008/01/17 00:43:12	Upgrade AP 2 Upgrade Requested
6	info	UPG	2008/01/17 00:43:13	Upgrade AP 1 Reading File
7	info	UPG	2008/01/17 00:43:13	Upgrade AP 2 Reboot Requested
8	info	UPG	2008/01/17 00:43:15	Upgrade AP 1 Verifying Checksum
9	info	UPG	2008/01/17 00:43:16	Upgrade AP 1 Erasing Flash
10	info	UPG	2008/01/17 00:43:21	Upgrade AP 1 Writing Flash
11	info	UPG	2008/01/17 00:43:37	Upgrade AP 1 Success

SysLog(11 entries)

関連コマンド [syslog-host \(228 ページ\)](#)

show syslog-host

設定されている場合に、外部システム ログ用 (syslog) のホストを表示します。

構文

show syslog-host

コマンド モード

特権 EXEC

デフォルト

なし

用途

デフォルトでは、外部ロギングは無効になっています。**syslog-host** コマンドを使用して、外部のシステム ログ ホストを設定できます。

使用例

以下のコマンドを使用すると、システム ログ ホストが 10.1.2.3 であることが表示されます。

```
controller(config)# show syslog-host  
10.1.2.3  
controller(config)#
```

関連コマンド

- [syslog-host \(228 ページ\)](#)
- [show syslog-file \(207 ページ\)](#)
- [show syslog-table \(210 ページ\)](#)

show syslog-table

外部システム ログのファシリティ テーブルの表を表示します。

構文

```
show syslog-table
show syslog-table <facility>
```

facility オプションの facility パラメータは、出力をフィルタリングして、そのファシリティのみのエントリを表示します。facility には、次のようなエントリがあります。

802. モビリティ
バルクアップデート
nms
qos
security
system

コマンド モード

EXEC

デフォルト

なし

用途

このコマンドを使用すると、外部のシステム ログ テーブルが存在する場合は、その内容が表示されます。デフォルトでは、外部ロギングは無効になっています。syslog-host コマンドを使用して、外部のシステム ログ ホストを設定できます。

使用例

```
controller# show syslog-table
```

Description	Last Accessed	Size	# Lines	Last Record
Security	2008/03/06 14:21:55		2	0
QoS	2008/03/06 14:21:47		1	0
System WNC	2008/03/06 14:21:54		1	0
NMS	2008/03/06 14:21:47		1	0
Mobility	2008/03/06 14:21:47		1	0
Bulk Update	2008/03/06 14:21:47		1	0
Upgrade	2008/03/06 14:15:52		1	0
Per User Firewall	2008/03/06 14:22:02		1	0

以下のコマンドにより、syslog ファイルが存在するものの、ファイルの中にエントリが存在しないことが示されます。

```
controller(config)# show syslog-table security
```

Line	Priority	Mnemonic	Time	Record
31	info	WAU	2005/08/05 10:37:27	admin@10.0.220.25
logged in OK				
SysLog(1 entry)				

```
controller(config)#
```

関連コマンド

- [show syslog-file \(207 ページ\)](#)
- [show syslog-host \(209 ページ\)](#)

show sys-summary

指定されたパラメータによって、システム ステータスの各種統計が表示されます。

構文

```
show sys-summary <ess/general/resources/stations/throughput>
```

ess	ESS ごとに情報を表示します。
general	システム全般の詳細を表示します。
resources	システムの CPU、ファイルシステム、およびメモリの統計を表示します。
stations	現在接続されているステーションの数とタイプに関する統計を表示します。
throughput	コントローラのスループット統計を表示します。

コマンド モード

特権 EXEC

デフォルト

なし

用途

show sys-summary コマンドは、ワイヤレス環境とコントローラそのものに関する詳細統計を表示できます。指定するパラメータによって、異なる情報が表示されます。

使用例

以下の例は、**resources** パラメータの出力です。

```
default(15)# show sys-summary resources
System Resources Status
CPU Usage User[%] : 0
CPU Usage System[%] : 0
CPU Usage Idle[%] : 99
Memory Size Total[K] : 4008008
Memory Size Used[K] : 244100
Memory Size Free[K] : 3763908
Root File System Size Total[K] : 897363
Root File System Size Used[K] : 566296
Root File System Size Available[K] : 283190
Root File System Usage[%] : 67
```

```
default(15)#
```

関連コマンド

- [show sys-summary ess \(214 ページ\)](#)
- [show sys-summary general \(216 ページ\)](#)
- [show sys-summary resources \(218 ページ\)](#)
- [show sys-summary stations \(219 ページ\)](#)
- [show sys-summary throughput \(220 ページ\)](#)

show sys-summary ess

設定されているすべての ESSID または特定の ESS に関する各種統計を表示します。

構文

```
show sys-summary ess <ess>
```

ess 詳細を表示する ESS を指定します。

コマンド モード

特権 EXEC

デフォルト

なし

用途

show sys-summary コマンドのこのバージョンでは、2 つのオプションを使用できます。

- show sys-summary ess: すべての ESSID とその送信および受信の値の詳細を表示します。
- show sys-summary ess <ess>: 指定した ESS の詳細を表示します。

どちらのバージョンのコマンドでも、以下の詳細が表示されます。

- RF Band - ESS が動作するバンド。
- Radios - 各 ESS に割り当てられる無線の数。
- RX_TP - 受信スループット速度 (ビット/秒)。
- TX_TP - 送信スループット速度 (ビット/秒)。
- Total_TP - 全体スループット (ビット/秒の送信と受信の合計)。
- Stations - ESS の各バンドの無線の合計数。

使用例

以下の例は、このコマンドの一般と特定の両方のバージョンの出力を表示します。

```
Default(15)# show sys-summary ess
ESSID RFBAND RADIOS RX_TP[bps] TX_TP[bps] TOTAL_TP[bps] STATIONS
vcellclear 2.4GHz 4 0 0 0 1
vcellclear 5GHz 5 0 0 0 3
vcellmixedpsk 2.4GHz 4 0 0 0 0
vcellmixedpsk 5GHz 3 0 0 0 0
vcellwep64 2.4GHz 4 0 0 0 0
```



```

vcellwep64 5GHz 4 0 0 0 0
vcellwpa 2.4GHz 4 0 0 0 0
vcellwpa 5GHz 4 0 0 0 0
vcellwpa2 2.4GHz 3 0 0 0 0
vcellwpa2 5GHz 4 0 0 0 0
vcellwpa2psk 2.4GHz 5 0 0 0 4
vcellwpa2psk 5GHz 5 149 0 149 15
vcellwpapsk 2.4GHz 5 30 0 30 1
vcellwpapsk 5GHz 5 39 0 39 4
ESS Statistics Summary(14 entries)

default15)# show sys-summary ess vcellwpa2psk
RFBAND RADIOS RX_TP[bps] TX_TP[bps] TOTAL_TP[bps] STATIONS
2.4GHz 5 0 0 0 4
5GHz 5 149 0 149 15
ESS Statistics Summary(2 entries)
default(15)#

```

関連コマンド

- [show sys-summary \(212 ページ\)](#)
- [show sys-summary general \(216 ページ\)](#)
- [show sys-summary resources \(218 ページ\)](#)
- [show sys-summary stations \(219 ページ\)](#)
- [show sys-summary throughput \(220 ページ\)](#)

show sys-summary general

コントローラに関する一般的な詳細と FortiWLC (SD) のステータスを表示します。

構文

`show sys-summary general`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show sys-summary` コマンドのこのバージョンでは、コントローラの設定に関する詳細情報と、それがサービスするワイヤレス デバイスの一般的な統計を確認できます。次のような情報が表示されます。

- コントローラのホスト名
- コントローラのモデル
- ソフトウェアのバージョン
- インストールされている / 許可されている / オンライン / オフラインの AP の合計数
- 有線とワイヤレスのステーションの合計数
- 重大度ごとのアラームの合計数

コントローラのサポートによって、これ以外の詳細も表示されます。

使用例

```
default(15)# show sys-summary general
System General Information
Controller's Hostname : Engg-wifi-Main-4200
Controller's Model Name : MC4200
Controller's Version : 5.2-32
Controller's Uptime : 01d:23h:02m:49s
Access Point Limit : 500
Client(s) : 5000
Installed Access Point License Count : 150
In-Use Access Point License Count : 5
Online Access Point Count : 5
Offline Access Point Count : 1
```

Wireless Station Count : 24
2.4GHz Station Count : 6
5GHz Station Count : 18
Wired Station Count : 0
Alarm Count : 10
Critical Alarm Count : 5
Major Alarm Count : 0
Minor Alarm Count : 5
Rogue Access Point Count : 0
Rogue Station Count : 0
Unknown Rogue Device Count : 0
Clear ESS Profile Count : 1
Secure ESS Profile Count : 7
Captive Portal ESS Profile Count : 2
default(15)#

関連コマンド

- [*show sys-summary*](#) (212 ページ)
- [*show sys-summary ess*](#) (214 ページ)
- [*show sys-summary resources*](#) (218 ページ)
- [*show sys-summary stations*](#) (219 ページ)
- [*show sys-summary throughput*](#) (220 ページ)

show sys-summary resources

コントローラのリソース ステータスに関する統計を表示します。

構文

`show sys-summary resources`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show sys-summary` コマンドのこのバージョンでは、コントローラのリソースのステータスに関する詳細情報として、CPU 使用率、メモリ消費、および空きディスク領域などが表示されます。

使用例

```
default(15)# show sys-summary resources
System Resources Status
CPU Usage User[%] : 0
CPU Usage System[%] : 0
CPU Usage Idle[%] : 99
Memory Size Total[K] : 4008008
Memory Size Used[K] : 250704
Memory Size Free[K] : 3757304
Root File System Size Total[K] : 897363
Root File System Size Used[K] : 566296
Root File System Size Available[K] : 283190
Root File System Usage[%] : 67
default(15)#
```

関連コマンド

- [show sys-summary \(212 ページ\)](#)
- [show sys-summary ess \(214 ページ\)](#)
- [show sys-summary general \(216 ページ\)](#)
- [show sys-summary stations \(219 ページ\)](#)
- [show sys-summary throughput \(220 ページ\)](#)

show sys-summary stations

コントローラがアクティブにサービスしているステーションに関する統計を表示します。

構文

`show sys-summary stations`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show sys-summary` コマンドのこのバージョンでは、現在、ネットワークに存在するステーションの数やタイプに関する詳細情報が表示されます。これらの情報は、バンド、使用しているデータ ストリームの数、ステーションのタイプ (データまたは電話) ごとに分かれています。

使用例

```
default(15)# show sys-summary stations
System Stations Status
802.11a Station Count : 8
802.11an1stream Station Count : 0
802.11an2stream Station Count : 12
802.11an3stream Station Count : 0
802.11b Station Count : 0
802.11bg Station Count : 0
802.11gn1stream Station Count : 0
802.11gn2stream Station Count : 2
802.11gn3stream Station Count : 0
Associated Data Station Count : 20
Associated Phone Station Count : 1
default(15)#
```

関連コマンド

- [show sys-summary \(212 ページ\)](#)
- [show sys-summary ess \(214 ページ\)](#)
- [show sys-summary general \(216 ページ\)](#)
- [show sys-summary resources \(218 ページ\)](#)
- [show sys-summary throughput \(220 ページ\)](#)

show sys-summary throughput

ワイヤレス ネットワークのスループット レベルに関する統計を表示します。

構文

`show sys-summary throughput`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show sys-summary` コマンドのこのバージョンでは、現在のワイヤレス環境でのスループット レベルに関する詳細情報が表示されます。これらの詳細は、受信 (Rx) と送信 (Tx) のレベルごとに分かれており、ビット / 秒 (bps) 単位で表示されます。

使用例

```
default(15)# show sys-summary throughput
System Throughput Information
Controller Total Rx Bytes : 23858571
Controller Total Tx Bytes : 23833005
Controller Rx Throughput[bps] : 3181142
Controller Tx Throughput[bps] : 3177734
WLAN Total Rx Bytes : 896675
WLAN Total Tx Bytes : 34319495
WLAN Rx Throughput[bps] : 119556
WLAN Tx Throughput[bps] : 4575932
default(15)#
```

関連コマンド

- [show sys-summary \(212 ページ\)](#)
- [show sys-summary ess \(214 ページ\)](#)
- [show sys-summary general \(216 ページ\)](#)
- [show sys-summary resources \(218 ページ\)](#)
- [show sys-summary stations \(219 ページ\)](#)

show system-id

ライセンス生成に必要な、コントローラのシステム ID を表示します。

構文

`show system-id`

コマンド モード

特権 EXEC

デフォルト

なし

用途

使用例

以下のコマンドは、ライセンスに適用する必要があるコントローラ ID を表示します。

```
Master# show system-id
System Id : COMPOSITE=272FF2EEB5F8
Master#
```

関連コマンド

[license \(133 ページ\)](#)

show timezones

タイムゾーンと関連する都市を表示します。

構文

show timezones

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、タイムゾーンごとの主要都市が表示されます。

使用例

このコマンドによる出力 (一部) は以下のとおりです。

```
controller(config)# show timezones
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
.
.
.
```

関連コマンド

[*timezone*](#) (230 ページ)

spectrum-band

ワイヤレス環境の特定部分でのスペクトル スキャンを有効または無効にします。

構文

```
spectrum-band [band]  
no spectrum-band [band]
```

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、スペクトラム解析のためにスキャンされるワイヤレス スペクトラムの部分を調整します。コマンドの **no** フォームを使用すると、スペクトラム バンドが無効になります。コマンドを繰り返し使用して、スペクトラムの複数の部分でそれを有効にできます。また、単に **all** パラメータを使用してスペクトラム全体をスキャンすることも可能です。

使用例

```
controller(15)(config)# spectrum-band 2.4GHz
```

```
controller(15)(config)#
```

```
controller(15)(config)# no spectrum-band 2.4GHz
```

関連コマンド

start-ntp

指定のネットワーク タイム プロトコル (NTP) サーバとシステム クロックのシステム時刻の自動同期を開始します。

構文

start-ntp

コマンド モード

特権 EXEC

デフォルト

なし

用途

start-ntp コマンドを使用して、**ntp server** コマンドで指定した NTP サーバとシステムクロックの自動同期を有効にします。一般用の NTP サーバに関する情報は、www.ntp.org を参照してください。

使用例

NTP サーバの自動同期をセットアップするには、**start-ntp** コマンドを使用します。

```
controller# start-ntp
```

関連コマンド

[ntp \(139 ページ\)](#)

statistics period

コントローラが情報をポーリングする頻度を設定します。

構文

```
statistics period <period>
```

period コントローラが情報をポーリングするまでの時間。有効な値の範囲は 5 ～ 65,535 秒です。

コマンドモード

グローバル設定

デフォルト

デフォルトの統計期間は 60 秒です。

用途

statistics period コマンドを使用して、コントローラが情報をポーリングする頻度を変更します。たとえば、デフォルトでは、コントローラは渡されるパケット数やドロップしたパケット数などの情報を 60 秒間隔でポーリングします。ゼロ (0) を指定するとポーリングは無効になります。この頻度は、以下のコマンドで収集されるデータにも影響します。

- **show statistics station-per-ap** - AP ごとにステーション統計情報のリストを表示します。
- **show statistics top10-ap-problem** - 最も重大な問題がある AP のリストを表示します。
- **show statistics top10-ap-talker** - 最も重いトラフィック (最大 Tx+Rx フレーム) を処理している AP のリストを表示します。
- **show statistics top10-station-problem** - 最も重大な問題があるステーションのリストを表示します。
- **show statistics top10-station-talker** - 最も重いトラフィックを生成しているステーションのリストを表示します。

使用例

以下のコマンドを指定すると、統計情報を収集する頻度が 1,000 秒に設定されます。

```
controller(config)# statistics period 1000  
controller(config)#
```

Sysconfig backup

システム設定ファイルのバックアップを実行します。

構文

`Sysconfig backup`

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、システム設定ファイルをバックアップします。

使用例

```
MC3200(15)#  
MC3200(15)# configure terminal  
MC3200(15)(config)# Sysconfig backup
```

関連コマンド

[Sysconfig restore \(227 ページ\)](#)

Sysconfig restore

システム設定ファイルのリストアを実行します。

構文

`Sysconfig restore`

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、システム設定ファイルをリストアします。

使用例

```
MC3200(15)#  
MC3200(15)# configure terminal  
MC3200(15)(config)# Sysconfig restore
```

関連コマンド

[Sysconfig backup \(226 ページ\)](#)

syslog-host

外部のシステム ログ (syslog) ホストを設定します。

構文

```
syslog-host <hostname>  
no syslog-host
```

hostname 外部システム ログ ホストの名前または IP アドレス (ドット区切りの 10 進数表記)

コマンド モード

グローバル設定

デフォルト

デフォルトでは、ホストは指定されません。

用途

このコマンドは、システム ログのエラー ログ ファイルを保持する場所として指定するリモート サーバを設定します。デフォルトでは、ホストは指定されません。設定されているシステム ログ サーバを削除するには、**no syslog-host** コマンドを使用します。

使用例

以下のコマンドにより、システム ログ ホスト設定を確認し、ホスト 10.1.2.3 を外部システム ログ サーバに設定してから、変更を表示します。

```
controller(config)# do show syslog-host  
External logging is disabled  
controller(config)# syslog-host 10.1.2.3  
controller(config)# do show syslog-host  
10.1.2.3
```

以下のコマンドにより、システム ログ ホストの設定が削除され、変更が表示されます。

```
controller(config)# no syslog-host  
controller(config)# do show syslog-host  
External logging is disabled
```

関連コマンド

[show syslog-host \(209 ページ\)](#)

telnet

telnet 接続を設定します。

構文

```
telnet enable  
telnet disable
```

コマンド モード

グローバル設定モード

デフォルト

telnet アクセスは無効です。

用途

このコマンドは、telnet が有効な場合にコントローラに対する telnet のアクセスを無効にし、telnet が無効な場合に telnet アクセスを有効にします。

使用例

以下のコマンドを指定すると、telnet アクセスが無効になります。

```
controller(config)# telnet disable
```

timezone

タイムゾーンを設定します。

構文

```
timezone menu  
timezone set <zone>
```

zone 特定のタイムゾーンを直接設定します。

コマンド モード

特権 EXEC モード

デフォルト

なし

用途

このコマンドはコントローラのタイムゾーンを設定します。**menu** オプションを使用すると、メニューに location (地域 (大陸および海洋)) の番号付きリストが表示され、location を選択することでタイムゾーンを設定できます。選択の質問が終わると、タイムゾーンを設定するよう要求され、ゾーン設定が通知されます。**zone** 設定は、それ以降のタイムゾーンセッションで **set** オプションに対する引数として使用できます。タイムゾーンが変更されたら、コントローラをリブートする必要があります。

使用例

以下では、**menu** オプションを使用したタイムゾーンの設定方法を示します。

```
controller(config)# timezone menu  
Please identify a location so that time zone rules can be set correctly.  
Please select a continent or ocean.  
1) Africa  
2) Americas  
3) Antarctica  
4) Arctic Ocean  
5) Asia  
6) Atlantic Ocean  
7) Australia  
8) Europe  
9) Indian Ocean  
10) Pacific Ocean  
11) none - I want to specify the time zone using the Posix TZ format.
```


#? 10

Please select a country.

- | | |
|---------------------|-------------------------------|
| 1) Chile | 15) Northern Mariana Islands |
| 2) Cook Islands | 16) Palau |
| 3) Ecuador | 17) Papua New Guinea |
| 4) Fiji | 18) Pitcairn |
| 5) French Polynesia | 19) Samoa (American) |
| 6) Guam | 20) Samoa (Western) |
| 7) Kiribati | 21) Solomon Islands |
| 8) Marshall Islands | 22) Tokelau |
| 9) Micronesia | 23) Tonga |
| 10) Nauru | 24) Tuvalu |
| 11) New Caledonia | 25) US minor outlying islands |
| 12) New Zealand | 26) United States |
| 13) Niue | 27) Vanuatu |
| 14) Norfolk Island | 28) Wallis & Futuna |

#? 26

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Standard Time - Indiana - most locations
- 6) Eastern Standard Time - Indiana - Crawford County
- 7) Eastern Standard Time - Indiana - Starke County
- 8) Eastern Standard Time - Indiana - Switzerland County
- 9) Central Time
- 10) Central Time - Michigan - Wisconsin border
- 11) Central Time - North Dakota - Oliver County
- 12) Mountain Time
- 13) Mountain Time - south Idaho & east Oregon
- 14) Mountain Time - Navajo
- 15) Mountain Standard Time - Arizona
- 16) Pacific Time
- 17) Alaska Time
- 18) Alaska Time - Alaska panhandle
- 19) Alaska Time - Alaska panhandle neck

20) Alaska Time - west Alaska

21) Aleutian Islands

22) Hawaii

#? 16

The following information has been given:

United States

Pacific Time

The name of the time zone is 'America/Los_Angeles'.

Is the above information OK?

1) Yes

2) No

#? 1

The following command is the alternative way of selecting the same time zone

timezone set America/Los_Angeles

The time zone is successfully set

topo-update

トポロジ情報アップデート機能を有効または無効にします。

トポロジ情報のアップデートは、トラブルシューティングやデバッグ情報の収集に役立ちます。トラブルシューティングやデバッグ情報の収集が必要な場合にのみ、この機能を有効にすることを推奨します。

構文

```
topo-update enable  
topo-update disable
```

コマンド モード

グローバル設定

デフォルト

デフォルト設定は **disable** (無効) です。

用途

このコマンドは、トポロジ情報の情報アップデート機能が有効または無効のいずれかであることを確認します。有効な場合、コントローラは、トポロジ関連の **show** コマンド (**show topoap**, **show topoapap**, **show topostaap**, **show topostation**) に対して使用されるトラブルシューティング / デバッグ情報を収集します。

デフォルトでは、トポロジ情報の収集は無効です。

使用例

デフォルトでは、トポロジ情報の収集は無効です。トポロジ収集を有効にするには、次のコマンドを使用します。

```
barneveld# configure terminal  
barneveld(config)# topo-update enable  
barneveld(config)# exit
```

traceroute

ネットワーク接続をテストします。

構文

`traceroute <hostname>`

hostname 解決するホスト アドレスの名前と IP アドレス (ドット区切りの 10 進数表記)

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを指定すると、コントローラと特定のリモート デバイスとの間にあるすべてのルータの IP アドレスとステータスが表示されます。IP アドレスまたはホスト名の代わりに、ドメイン名を指定することもできます。

使用例

以下のコマンドを指定すると、Ourserver という名前のホストまでの経路に存在するルータが表示されます。

```
controller# traceroute Ourserver
traceroute to OurServer (10.0.13.1), 30 hops max, 38 byte packets
 1  mc3000 (10.19.1.1)  2997.354 ms !H  2999.525 ms !H  2999.944 ms !
```

関連コマンド

[ping \(142 ページ\)](#)

zeronet-packet

ソース / 宛先 IP アドレスが 0 (zeronet) で始まる、0.0.0.0 以外の IPv4 ユニキャスト パケットの転送を有効 / 無効にします。

構文

```
zeronet-packet enable  
zeronet-packet disable
```

コマンド モード

グローバル設定

デフォルト

無効

用途

この機能は、ソース / 宛先 IP アドレスが 0 (zeronet) で始まる、0.0.0.0 以外の IPv4 ユニキャスト パケットの転送を有効 / 無効にします。

使用例

```
amecntrl# configure terminal  
ramecntrl(config)# zeronet-packet ?  
<value>                               Enter Enable or Disable for Zeronet configuration  
      disable                          Disable  
      enable                           Enable  
ramecntrl(config)# zeronet-packet enable  
ramecntrl(config)# zeronet-packet disable  
ramecntrl(config)# exit
```


6 冗長化コマンド

本章では、システムの可用性を保護するために利用可能である N+1 冗長機能を設定するために使用されるコマンドについて説明します。ここで説明する **nplus1** コマンドを使用して 1 つまたは複数のマスタ コントローラにバックアップ スタンバイ コントローラを 1 台セットアップするか、Web UI から Option 43 を設定できます。

nplus1 コマンドには次が含まれます。

- [nplus1 add \(238 ページ\)](#)
- [nplus1 add \(238 ページ\)](#)
- [nplus1 delete \(240 ページ\)](#)
- [nplus1 disable \(241 ページ\)](#)
- [nplus1 enable \(242 ページ\)](#)
- [nplus1 revert \(244 ページ\)](#)
-
- [nplus1 setdebugloglevel \(246 ページ\)](#)
- [nplus1 start master \(247 ページ\)](#)
- [nplus1 start slave \(248 ページ\)](#)
- [nplus1 stop \(250 ページ\)](#)
- [nplus1 timeout \(252 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)
- [show nplus1 debugloglevel \(257 ページ\)](#)

nplus1 add

スレーブのクラスタ リストにマスタ コントローラを追加します。

構文

```
nplus1 add <master_hostname> <master_ip-address>
```

master_hostname マスタ コントローラのホスト名。

master_ip-address マスタ コントローラの IP アドレス。

コマンド モード

グローバル設定

デフォルト

なし

用途

nplus1 add コマンドは、スタンバイ スレーブ コントローラに対して使用します。このコマンドを使用して、スレーブが監視するマスタ コントローラを追加します。

N+1 設定を開始する前に、すべてのクラスタ コントローラで高可用性 (HA) サービスを無効にします (**high-availability stop** を使用)。また、このコマンドを使用する前に、このスレーブおよびすべてのマスタで N+1 を開始します (**nplus1 start slave** と **nplus1 start master** を使用)。

nplus1 add コマンドを使用して、最大で 5 台のマスタ コントローラを 1 台の バックアップ スレーブ コントローラに追加できます。その際にはマスタを 1 台ずつ追加します。クラスタにある各マスタ コントローラのホスト名 (たとえば、3000-1) 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。

nplus1 add master command コマンドを実行した後に、既存のコントローラを 交換している場合、**nplus1 access** コマンドを実行します。

使用例

次のコマンドでは、IP アドレスが 10.1.1.10 である 3000-1 という名前のマスタ コントローラを、バックアップ スレーブ コントローラ 3000-slave のクラスタ リストに追加した後に、その IP アドレス 10.1.1.10 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います。

```
3000-slave(config)# nplus1 add 3000-1 10.1.1.10
admin@10.1.1.10 Password: xxx
```



```
3000-slave(config)# nplus1 access 10.1.1.10
```

関連コマンド

- [nplus1 start master \(247 ページ\)](#)
- [nplus1 start slave \(248 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 delete

N+1 マスタ コントローラをクラスタから削除します。

構文

```
nplus1 delete <master_ip-address>
```

master_ip-address マスタ コントローラの IP アドレス。

コマンド モード

グローバル設定

デフォルト

なし

用途

N+1 マスタをスレーブのクラスタから削除するには、スレーブのコントローラから **nplus1 delete** コマンドを発行します。**nplus1 delete** は、スタンバイ スレーブ コントローラでのみ動作します。

使用例

次のコマンドは、IP アドレスが 10.1.1.10 であるマスタ コントローラをスレーブ コントローラ 3000-slave から削除しています。

```
3000-slave(config)# nplus1 delete 10.1.1.10
```

関連コマンド

[show nplus1 \(253 ページ\)](#)

nplus1 disable

マスタ コントローラで N+1 操作を無効にします。

構文

```
nplus1 disable <master_ip-address>
```

master_ip-address マスタ コントローラの IP アドレス。

コマンド モード

グローバル設定

デフォルト

なし

用途

マスタ コントローラで N+1 操作を無効にしながらも、クラスタにある設定を保持する場合は、**nplus1 disable** コマンドをスレーブ コントローラから実行します。**nplus1 disable** を発行するには、スレーブがスタンバイ状態にある必要があります。アクティブなスレーブに切り変わると (マスタ コントローラの交換) この操作はできません。

マスタ コントローラをリストアするには、スレーブ コントローラから **nplus1 enable** コマンドを実行します。

使用例

次の例は、IP アドレスが 10.1.1.10 であるマスタ コントローラを 3000-slave という名前のスレーブ コントローラで無効にしています。

```
3000-slave(config)# nplus1 disable 10.1.1.10
```

関連コマンド

- [nplus1 enable \(242 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 enable

nplus1 disable の後に、マスタ コントローラのステータスを有効に戻します。

構文

```
nplus1 enable <master_ip-address>
```

master_ip_address マスタ コントローラの IP アドレス。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、無効にされたマスタ コントローラで N+1 操作を有効にします。

新しく有効になったマスタ コントローラへのアクセスできるようにするには、スレーブ コントローラから **nplus1 access** コマンドを実行します。

使用例

次の例では、IP アドレスが 10.1.1.10 のマスタ コントローラを、3000-slave という名前のスレーブ コントローラから有効にしています。

```
3000-slave(config)# nplus1 enable 10.1.1.10
```

関連コマンド

- [nplus1 add \(238 ページ\)](#)
- [nplus1 disable \(241 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 period

スレーブ コントローラのハートビート間隔を変更します。

構文

```
nplus1 period <hb_period>
```

duration スレーブがマスタ コントローラにアドバタイズを送信する
間隔 (秒)。
値は、100 ~ 30000 になります。

コマンド モード

グローバル設定

デフォルト

1000 秒

用途

nplus1 period コマンドをスレーブ コントローラで使用して、マスタ コントローラにアドバタイズを送信するハートビート間隔を変更します。スレーブ コントローラがアドバタイズを受信しないと、自動フェイルオーバーが開始されます。

フェイルオーバーの後、マスタ (パッシブ) がアクティブなスレーブからのアドバタイズを監視します。マスタが指定された期間内にアドバタイズを受信しないと、自動フォールバックが開始されます。

使用例

この例では、ハートビート間隔を 2000 秒に設定しています。

```
NP1-MC4200-slave(15)(config)# nplus1 period 2000
nplus1 period set: 2000 millisecond
```

関連コマンド

nplus1 revert

スレーブのステータスをアクティブからスタンバイに変更します。

構文

nplus1 revert

コマンド モード

グローバル設定

デフォルト

なし

用途

nplus1 revert コマンドを使用して、スレーブ コントローラのステータスをアクティブからスタンバイに変更します (マスタ コントローラを 1 つ交換する場合)。障害のあったコントローラがしばらくオフラインになることが明らかであり、交換が必要な場合にこのコマンドを使用します。スレーブをアクティブからスタンバイに変更することで、クラスタの残りは引き続き監視されます。

非復帰モードが有効である場合、マスタ コントローラは、nplus1 がアップであり、アクティブ スレーブ コントローラでの動作に復帰する必要があります。

マスタ コントローラがダウンしていたり、**nplus1 revert** コマンドが実行されたりした場合、復帰は発生しません。

この状況で復帰させる必要がある場合は、

nplus1 revert force コマンドを使用して、アクティブ スレーブからパッシブへと状態を変更します。

例：

```
3000-slave# conf terminal
3000-slave(config)# nplus1 revert force
```

使用例

次の例では、スレーブ 3000-slave のステータスをアクティブからスタンバイに変更します。

```
3000-slave# nplus1 revert
```

関連コマンド

[show nplus1 \(253 ページ\)](#)

nplus1 autorevert

アクティブ スレーブ コントローラによって単独のフォールバックがトリガされます。

構文

`nplus1 autorevert`

コマンド モード

グローバル設定

デフォルト

なし

用途

マスタ コントローラがダウンすると、スレーブ コントローラがアクティブ スレーブ コントローラとして処理を引き継ぎます。これまで、ダウンしていたマスタ コントローラがアクティブになると、そのマスタ コントローラは `nplus1 revert` コマンドがアクティブ スレーブ コントローラで実行されるまでパッシブ コントローラであり続けていました。今回この動作が強化 (自動化) され、マスタ コントローラがオンラインになると自動復帰します。

使用例

次の例は、アクティブ スレーブ 3000-slave のフォールバックを自動トリガを有効にします。

```
3000-slave# nplus1 autorevert enable
```

関連コマンド

[show nplus1 \(253 ページ\)](#)

nplus1 setdebugloglevel

N+1 ログ メッセージの冗長レベルを設定します。

構文

```
nplus1 setdebugloglevel <number>
```

number 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。

コマンドモード

グローバル設定

デフォルト

デフォルトは 0 で、システム ログ メッセージは無効です。

用途

nplus1 setdebugloglevel コマンドを使用して、N+1 ログ メッセージの冗長レベルを設定します。。このコマンドはスレーブ コントローラでのみ使用できます。**show nplus1 debugloglevel** コマンドを使用してログ設定を確認します。

使用例

次の例では、スレーブ コントローラ 3000-slave のログの冗長レベルを 1 に設定しています。

```
3000-slave(config)# nplus1 setdebugloglevel 1
```

関連コマンド

- [show nplus1 \(253 ページ\)](#)
- [show nplus1 debugloglevel \(257 ページ\)](#)

nplus1 start master

Nplus1 マスタとしてコントローラを起動します。

構文

`nplus1 start master`

コマンド モード

グローバル設定

デフォルト

なし

用途

`nplus1 start slave` を使用してスレーブ コントローラを起動する前に、すべての マスタ コントローラで `nplus1 start master` を実行します。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。

使用例

次の例では、3000-master という名前のマスタ コントローラを開始しています。

```
3000-master(config)# nplus1 start master
```

関連コマンド

- [nplus1 start slave \(248 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 start slave

N+1 スレーブ コントローラを開始します。

構文

`nplus1 start slave`

コマンド モード

グローバル設定

デフォルト

なし

用途

`nplus1 start master` コマンドを使用してすべての N+1 マスタ コントローラが開始された後でのみ、`nplus1 start slave` コマンドを使用して N+1 スレーブ コントローラを起動します。この後、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。必要な間隔で UDP ポートを介してマスタによって送信されたアドバタイズメッセージを受け取ることで、クラスタにあるマスタの可用性を監視します。5 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 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。

- N+1 クラスタでは、スレーブおよびマスタ コントローラは同じモデルであり、FortiWLC (SD) ソフトウェアの同じバージョンを実行している必要があります。各マスタ コントローラがスレーブに割り当てられた後に、スレーブ コントローラにより、ハードウェア モデルと FortiWLC (SD) のバージョンが同一であることが確認されます。一致しない場合は、スレーブはこのマスタ用に切り替えられることは許可されず、ステータスがマスタ コントローラの [Status] 画面に表示されます。
- 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。

冗長からデュアル アクティブ設定へと変更するには、コントローラのリブートが必要です。

使用例

次の例では、3000-slave という名前のスレーブ コントローラを起動します。

```
3000-slave(config)# nplus1 start slave
Setting up this controller as a Passive Slave controller
3000-slave(config)#
```

関連コマンド

- [nplus1 start master \(247 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 stop

N+1 スレーブまたは N+1 マスタ コントローラを停止します。

構文

`nplus1 stop`

コマンド モード

グローバル設定

デフォルト

なし

用途

N+1 スレーブおよび N+1 マスタ コントローラは `nplus1 stop` を使用して別々に停止する必要があります。マスタ コントローラを停止する前に、スレーブに関連付けられているマスタ コントローラを無効にする必要があります。マスタを無効にしないと、スレーブが停止したマスタに対応してフェイルオーバーすることになります。また、スレーブ コントローラがアクティブではない (現在、マスタ コントローラを交換している) ときだけ、スレーブ コントローラで `nplus1 stop` を実行できます。

使用例

次の例では、3000-slave という名前のスレーブ コントローラで N+1 を停止しています。

```
3000-slave(config)# nplus1 stop
Making this a normal controller.
```

次の例では、3000-1 という名前のマスタ コントローラで N+1 を停止しています。

```
3000-1(config)# nplus1 stop
```

関連コマンド

- [nplus1 start master \(247 ページ\)](#)
- [nplus1 start slave \(248 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 takeover

マスタからスレーブ コントローラに手動でフェイルオーバーします。

構文

nplus1 takeover

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドはアクティブなマスタで実行します。

使用例

次の例では、3000-slave という名前のスレーブ コントローラで N+1 を停止しています。

```
3000-master(config)# nplus1 takeover
3000-master(config)#
```

関連コマンド

- [nplus1 start master \(247 ページ\)](#)
- [nplus1 start slave \(248 ページ\)](#)
- [show nplus1 \(253 ページ\)](#)

nplus1 timeout

スタンバイ スレーブをフェイルオーバーさせるトリガとなる未返信のキープアライブの数です。

構文

```
nplus1 timeout <number>
```

number 有効な範囲は 4 ～ 60 です (秒単位、秒あたり 1 回のキープアライブ)。

コマンド モード

グローバル設定

デフォルト

デフォルトは 4 です。

用途

nplus1 timeout は、スタンバイ スレーブ コントローラがマスタ コントローラの処理を引き継ぐトリガとなる未返信のキープアライブの数を示します。この数値に達すると、スタンバイ コントローラがアクティブ コントローラになり、障害のあるコントローラの IP アドレスを引き継ぎ、応答のないマスタの処理を引き継ぎます。

使用例

次の例では、3000-slave という名前のスレーブ コントローラでタイムアウトを 60 秒に設定します。

```
3000-slave(config)# nplus1 timeout 60
```

関連コマンド

- [nplus1 start master \(247 ページ\)](#)
- [nplus1 start slave \(248 ページ\)](#)

show nplus1

show nplus1 コマンドは、現在のコントローラの設定をチェックして、コントローラのステータスを表示します。

構文 show nplus1

コマンドモード 特権 EXEC

デフォルト なし

用途 show nplus1 コマンドを使用して、マスタまたはスレーブ コントローラのどちらでソフトウェアが開始しているかを確認します。また、show nplus1 コマンドを使用して、別のコマンドが実行されているかを確認できます。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 Enable - N+1 冗長化がマスタで有効になっています Disable - 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 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

フィールド	説明
Reason	<p>[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。</p> <p>Down - ユーザがマスタを無効にしています</p> <p>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)</p> <p>No Access - 設定のコピーを受信していないため、パッシブ スレーブはマスタにアクセスできません (コントローラを追加した直後に show nplus1 コマンドを実行すると表示されるメッセージですが、これが表示されることはほとんどありません)</p> <p>No Access - パッシブ スレーブはマスタ コントローラにアクセスできません (nplus1 access コマンドを使用し、交換したコントローラでマスタ コントローラへのアクセスが有効化されていない場合に主に発生します)。</p> <p>WTR Set - アクティブ スレーブのパッシブ スレーブへの移行において、この状態は、WTR タイマのカウントダウンで最初に行われるステップです。</p> <p>WTR <i>min</i> -WTR Set の制限に達したときに、このタイマがカウントダウンして、残り分数 (<i>min</i>) を表示します。</p>
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 5 でフェイルオーバーがトリガされず。
SW Version	コントローラの FortiWLC (SD) のソフトウェア バージョン。

使用例

次の例は、3000-1 という名前のマスタに関する基本的なマスタ コントローラ識別情報を表示しています。

```
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 <-- スレーブが開始していない場合は表示されません
Slave Status : Passive <-- レーブが開始していない場合は Unknown と表示されます
-----
```


次の例は、3000-slave という名前のスレーブ コントローラに関する基本的なスレーブ コントローラ識別情報を表示しています。

```
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
```

次の例では、アクティブ スレーブ の情報を表示しています。マスタ IP アドレスとホスト名が表示に追加されています。

```
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
```

関連コマンド

- [nplus1 add \(238 ページ\)](#)
- [nplus1 add \(238 ページ\)](#)
- [nplus1 delete \(240 ページ\)](#)
- [nplus1 disable \(241 ページ\)](#)
- [nplus1 revert \(244 ページ\)](#)
- [nplus1 setdebugloglevel \(246 ページ\)](#)

- [nplus1 start master \(247 ページ\)](#)
- [nplus1 start slave \(248 ページ\)](#)
- [nplus1 stop \(250 ページ\)](#)
- [nplus1 timeout \(252 ページ\)](#)

show nplus1 debugloglevel

N+1 ログ メッセージに設定された冗長レベルを表示します。

構文

`show nplus1 debugloglevel`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`show nplus1 debugloglevel` コマンドは、N+1 ログ メッセージに設定された冗長レベルを表示します。

使用例

```
3000-1# 3000-slave# show nplus1 debugloglevel
nplus1 Debug Logging Level: 0
3000-slave#
```

関連コマンド

[*nplus1 setdebugloglevel*](#) (246 ページ)

7 インターフェイスおよび IP コマンド

本章に含まれるコマンドは、ネットワーク インターフェイスを設定し、その関連情報を表示するために使用されます。

- [gw \(261 ページ\)](#)
- [igmp-snoop \(262 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dhcp-passthrough \(272 ページ\)](#)
- [ip dhcp-server \(273 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)
- [ip domainname \(276 ページ\)](#)
- [ip ftp \(277 ページ\)](#)
- [ip scp \(278 ページ\)](#)
- [ip sftp \(279 ページ\)](#)
- [ip udp-broadcast \(280 ページ\)](#)
- [ipv6-neighbor-discovery-optimization \(282 ページ\)](#)
- [mac-address \(283 ページ\)](#)
- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

- [show igmp-snoop \(294 ページ\)](#)
- [show interfaces FastEthernet ap \(296 ページ\)](#)
- [show interfaces FastEthernet controller \(299 ページ\)](#)
- [show interfaces FastEthernet statistics \(302 ページ\)](#)
- [show ip \(304 ページ\)](#)
- [show ipv6-neighbor \(306 ページ\)](#)
- [show second_interface_status \(307 ページ\)](#)
- [static-route \(308 ページ\)](#)
- [\(config-static-route\) interface \(309 ページ\)](#)
- [\(config-static-route\) ip \(310 ページ\)](#)
- [type \(311 ページ\)](#)
- [virtual-interface-profile \(313 ページ\)](#)
- [\(config-vip\) disable \(314 ページ\)](#)
- [\(config-vip\) enable \(315 ページ\)](#)
- [\(config-vip\) gateway \(316 ページ\)](#)
- [\(config-vip\) ip \(317 ページ\)](#)
- [\(config-vip\) show \(318 ページ\)](#)

gw

FastEthernet インターフェイスのゲートウェイ IP アドレスを設定します。

構文

gw <address>

address ゲートウェイの IP アドレスを設定します。

コマンド モード

FastEthernet インターフェイス設定モード

デフォルト

なし

用途

このコマンドを使用して、FastEthernet インターフェイスにより使用されるゲートウェイ IP アドレスを設定します。このインターフェイスがアクティブな操作用に設定されている場合 (つまり、FastEthernet インターフェイスの **type** が **active** として設定されている場合)、**gw** の設定は必須フィールドです。

使用例

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、インターフェイスの IP 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設定を指定し、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)# end
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [show interfaces FastEthernet controller \(299 ページ\)](#)
- [show second_interface_status \(307 ページ\)](#)
- [type \(311 ページ\)](#)

igmp-snoop

IGMP スヌーピングを設定します。

構文

```
igmp-snoop enable
iiigmp-snoop age-time <duration>
iiigmp-snoop disable
```

duration

IGMP グループにタイムアウトが実装される前の秒数を設定します。*duration* には、1 ～ 300 秒を設定できます。

最後の IGMP レポートの後で、タイムアウト間隔の前にレポートがでていない場合に、クライアントのマルチキャスト サブスクリプションは継続できなくなります。マルチキャスト グループの各 IGMP レポートについて、IGMP デーモンは特定のクライアントの ESS にあるマルチキャスト グループのタイムアウトをリセットします (クライアントのグループが明示的に離脱していない場合、グループ エントリを削除する必要がある時間のタイムアウト)。

コマンドモード

グローバル設定モード

制限事項

この機能では、動的 VLAN ではサポートされません。この機能は、IPv4 マルチキャスト以外ではサポートされません。

デフォルト

IGMP スヌーピングは無効です

用途

IGMP スヌーピングを使用すると、L2 デバイスは、IGMP プロトコル メッセージを傍受して、マルチキャスト転送テーブルを作成することでマルチキャスト転送についてスマートに判断できるようになります。そのため、ストリーミング メディアや帯域幅を多く消費する IP マルチキャスト アプリケーションのトラフィックを大幅に削減できます。IGMP バージョン v1 から v3 をサポートしています。

この機能が無効になっていると、コントローラは、サウスバウンド IP マルチキャスト トラフィックの受信時に、関連付けられているすべての AP に IP マルチキャスト パケットを転送します。この結果、IP マルチキャスト トラフィックをサブスクライブしていない AP へのトラフィックが大幅に増大します。

デフォルトでは、L2 スイッチ / ブリッジは、ブロードキャスト トラフィックと同じように、あるインターフェイスで受信したフレームをその他のすべてのインターフェイスに送信する方法で、IP マルチキャスト トラフィックを処理します。このため、ネットワークのトラフィックが増大し、ネットワークに接続しているホストのパフォーマンスが低下する恐れがあります。

IGMP プロトコルは、ステーションにより使用され、IP マルチキャスト グループ (アドレス) をサブスクライブまたはサブスクライブ解除します。特定の IP マルチキャスト グループに参加することを希望するステーションは、「グループ参加」メッセージを L3 デバイスに送信し、L3 デバイスは IP マルチキャスト グループ アドレスとインターフェイスをそのルーティング テーブルに記録します。L3 デバイスは、参加メッセージを受け取ったインターフェイスのみに関連する IP マルチキャスト アドレスにトラフィックを転送します。

L3 デバイスは、定期的にクエリーを送信し、ステーションが特定のグループへの IP マルチキャスト トラフィックを受信しているかどうかを判別します。そのように設定されているステーションが IGMP クエリーに応答します。ステーションからの応答に応じて、L3 デバイスは、ルーティング テーブルの不要な要素を削除します。

IGMP v2 および v3 には、ステーションが明示的な「グループからの離脱」メッセージを L3 デバイスに送信し、ステーションが特定の IP マルチキャスト グループのサブスクライブを解除できるようにできます。

これらの IGMP プロトコル メッセージは、L3 デバイスとステーション間の L2 デバイスをパススルーします。コントローラは、ネットワークで L2 デバイスのような動作をします。コントローラの IGMP スヌーピングは、トンネル マルチキャスト トラフィックのみに適用されます。

コントローラがサウスバンド IP トラフィックを受信すると、関連付けられているすべての AP に IP マルチキャスト パケットを転送します。この結果、IP マルチキャスト トラフィックをサブスクライブしていない AP へのトラフィックが大幅に増大します。コントローラに IGMP スヌーピング機能が必要なのは、このためです。

使用例

次のコマンドにより、IGMP スヌーピングが有効になり、タイムアウトが 240 秒に設定されます。

```
controller(config)# igmp-snoop enable
controller(config-if-FastEth)# igmp-snoop age-time 240
```

関連コマンド

[show igmp-snoop \(294 ページ\)](#)

interface FastEthernet

コントローラの FastEthernet インターフェイスを設定します。

構文

```
interface FastEthernet <interface_index>
```

interface_index 設定するインターフェイス ポート (1 または 2) を選択します。

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、設定する FastEthernet インターフェイスを選択し、FastEthernet 設定サブモードに入ります。

コントローラには 2 つの FastEthernet インターフェイスがあります。**setup** コマンドを使用してコントローラを最初に設定すると、1 つ目のインターフェイスが設定されます。このインターフェイスをその後に変更する場合や 2 つ目のインターフェイスを設定する場合に、このコマンドを使用します。次の例は、インターフェイス 1 を編集するコマンドを示します。また、FastEthernet 設定サブモードで利用可能なコマンドを示しています。

```
default(config)# interface FastEthernet 1
default(config-if-FastEth)# ?
do                                Executes an IOSCLI command.
end                                Save changes, and return to privileged EXEC mode.
exit                               Save changes, and return to global configuration mode.
gw                                Configure Gateway IP Address.
ip                                Configure IP Address and Netmask.
type                              Configure the type of the interface.
```

このサブモード コマンドには、インターフェイスの IP アドレスを設定する **ip address** コマンドが含まれています (VLAN および GRE トンネル設定のローカルエンドポイントとしても参照されます)。アドレスは、固定 IP アドレス (**ip address nnn.nnn.nnn.nnn**)、または DHCP (**ip address dhcp**) に設定できます。

gw コマンドは、インターフェイスが使用するゲートウェイ IP アドレスを設定します。

type コマンドは、インターフェイス 1 の **redundant** ポートとして使用するか、完全に機能するセカンダリの **active** ポートとして使用するかを決定します。

使用例

次のコマンドは、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。この設定を行うには、**type** オプションに **redundant** を指定します。タイプが **redundant** である場合は、IP アドレスを割り当てないでください。

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# type redundant
default(config-if-FastEth)# end
```

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設定を指定し、必須フィールドです。ゲートウェイは、VLAN または GRE トンネルのリモート エンドポイントの IP アドレスです。

```
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)# end
```



active 構成では、2 つ目のイーサネット インターフェイスは、プライマリ インターフェイスとして別の L2 ドメインに固定 IP アドレスを使用して設定する必要があります (DHCP は使用しません)。



冗長モードまたはアクティブ モードで 2 つ目のインターフェイスを設定する前に、ポート ボンディング モードを **dual** または **none** (コントローラ モードによる) に設定する必要があります。ボンディングの設定については、『FortiWLC (SD) 設定ガイド』を参照してください。

関連コマンド

- [gw \(261 ページ\)](#)
- [ip address \(267 ページ\)](#)

- [show interfaces FastEthernet controller](#) (299 ページ)
- [show second_interface_status](#) (307 ページ)
- [type](#) (311 ページ)

ip address

固定 IP アドレスの接続を設定します。

構文

```
ip address <ip-address> <ip-netmask>
```

ip-address *address* の IP アドレスを設定します。

ip-netmask *netmask* の IP アドレスを設定します。

コマンドモード

グローバル、FastEthernet、RADIUS プロファイル、AP 接続、および VLAN 設定モード

デフォルト

なし

用途

このコマンドは、設定モードでは実行できません。FastEthernet、AP、または VLAN 設定モードから実行する必要があります。このコマンドを使用して、コントローラ、RADIUS サーバ、アクセス ポイント、VLAN の IP アドレスおよびネットマスクを設定します (コマンドを起動したサブモードにより設定対象が異なります)。

AP の IP アドレスを設定する場合は、対象となる AP はリモート AP となり、固定の IP アドレスを設定することになります。**ip address dhcp** コマンドを使用して動的な IP アドレスを使用するように AP を設定することもできます。

VLAN サブモードで IP アドレスを設定する場合、VLAN に指定する IP アドレスは、クライアントに設定されているデフォルトのゲートウェイと一致する必要があります。

使用例

コントローラに固定 IP アドレスを割り当てるには、IP アドレスとサブネットの引数を指定して、**ip address** コマンドを以下のように使用します。

```
controller(config-ap)# ip address 10.0.0.19 255.0.0.0
```

リモート AP に固定 IP アドレスを割り当てるには、AP 接続サブモードに入り、**ip address** コマンドを使用して、IP アドレス 10.0.220.30 とネットマスク 255.255.255.0 をリモート AP に設定します。

```
controller(config)# ap 1
```

```
controller(config-ap)# 13-connectivity 13-preferred
```

```
controller(config-ap-connectivity)# ip address 10.0.220.30 255.255.255.0
```

```
controller(config-ap-connectivity)#
```

以下のコマンドにより、VLAN の IP アドレス 10.1.2.3 とネットマスク 255.0.0.0 が指定されます。

```
controller(config)# vlan qa tag 100
```

```
controller(config-vlan)# ip address 10.1.2.3 255.0.0.0
```

関連コマンド

- [gw \(261 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)
- [show ap-connectivity \(632 ページ\)](#)
- [show controller \(172 ページ\)](#)
- [type \(311 ページ\)](#)

ip address dhcp

DHCP 接続を設定します。

構文

ip address dhcp

コマンドモード

グローバルおよび AP 接続設定モード

デフォルト

なし

用途

このコマンドは、設定モードでは実行できません。FastEthernet、AP、または VLAN 設定モードから実行する必要があります。このコマンドを使用して、コントローラおよびアクセス ポイントの DHCP 接続を設定します (このコマンドを呼び出すサブモードによって設定対象が異なります)。

使用例

コントローラに動的な IP アドレスを割り当てるには、以下のように **ip address dhcp** コマンドを使用します。

```
controller(config-ap)# ip address dhcp
```

AP に動的な IP アドレスを割り当てるには、AP 接続サブモードに入り、**ip address dhcp** コマンドを使用して、動的に割り当てられる IP をリモート AP に 設定します。

```
controller(config)# ap 1  
controller(config-ap)# l3-connectivity l3-preferred  
controller(config-ap-connectivity)# ip address dhcp  
controller(config-ap-connectivity)#
```

関連コマンド

- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)
- [show controller \(172 ページ\)](#)

ip default-gateway

デフォルト ゲートウェイの接続を設定します。

構文

```
ip default-gateway <address>
```

address デフォルト ゲートウェイの IP アドレス。

コマンドモード

グローバル設定、AP 接続設定、および VLAN 設定モード

デフォルト

デフォルト ゲートウェイのデフォルトの IP アドレスは 0.0.0.0 です。

用途

このコマンドは、設定モードでは実行できません。FastEthernet、AP、または VLAN 設定モードから実行する必要があります。コントローラ、アクセス ポイント、VLAN のデフォルト ゲートウェイ接続を設定します (コマンドを呼び出すサブモードによって設定対象が異なります)。

VLAN のデフォルト ゲートウェイを設定する場合は、コントローラにより使用されるデフォルト ゲートウェイを使用して、VLAN を使用するワイヤレス クライアントから受信するトラフィックをルーティングします。

default フォームを使用して、デフォルト ゲートウェイの値をデフォルトに設定します。

使用例

コントローラにより使用されるデフォルト ゲートウェイの IP アドレスを割り当てるには、以下のように IP アドレスを指定して **ip default-gateway** コマンドを使用します。

```
controller(config-ap)# ip default-gateway 10.0.0.1
```

AP により使用されるデフォルト ゲートウェイの IP アドレスを割り当てるには、AP 接続サブモードに入り、**ip default-gateway** コマンドを使用して、リモート AP の IP アドレスを設定します。

```
controller(config)# ap 1
controller(config-ap)# 13-connectivity 13-preferred
controller(config-ap-connectivity)# ip default-gateway 10.0.0.1
```

VLAN により使用されるデフォルト ゲートウェイの IP アドレスを割り当てるには、以下のようコマンドを使用します。


```
controller(config)# vlan qa tag 100  
controller(config-vlan)# ip default-gateway 10.0.0.1
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)
- [show ap-connectivity \(632 ページ\)](#)
- [show controller \(172 ページ\)](#)

ip dhcp-passthrough

DHCP パススルーを有効 / 無効に設定します。

構文

```
ip dhcp-passthrough
no dhcp-passthrough
```

コマンドモード

グローバル設定および VLAN 設定モード

デフォルト

DHCP パススルーが有効になっています。

用途

このコマンドは、コントローラまたは VLAN の DHCP パススルー サービスを有効または無効 (**no** フォームを使用) にします (コマンドが呼び出されたサブモードにより設定対象が異なります)。有効に設定され、DHCP サーバの IP がデフォルトの 127.0.0.1 となっている場合は、DHCP パケットは、変更されずにパススルーします (ブリッジ)。パススルーにより、大半の実装環境において DHCP リレーが不要になります。これによりルータ上のリレー負荷が発生しますが、これは通常の動作です。

グローバル DHCP パススルーは、対応するモジュールの DHCP パススルー設定によってオーバーライドされます。

使用例

コントローラの DHCP パススルーを有効にするには、以下のように **ip dhcp-passthrough** コマンドを使用します。

```
controller(config)# ip dhcp-passthrough
```

VLAN の DHCP パススルーを有効にするには、以下のようにコマンドを使用します。

```
controller(config)# vlan qa tag 100
controller(config-vlan)# ip dhcp-passthrough
```

関連コマンド

- [ip dhcp-server \(273 ページ\)](#)
- [show controller \(172 ページ\)](#)

ip dhcp-server

DHCP リレー サーバを設定します。

構文

```
ip dhcp-server <ip-address>  
no ip dhcp-server
```

ip-address ドット区切り 10 進数値で表記される DHCP リレー サーバの IP アドレス (*n.n.n.n*)

コマンドモード

グローバル設定および VLAN 設定モード

デフォルト

DHCP リレー サーバのデフォルトの IP アドレスは、127.0.0.1 です。

用途

このコマンドは、コントローラと VLAN の DHCP リレーサーバを設定します (コマンドが呼び出されるサブモードにより設定対象が異なります)。

VLAN サブモードでこのコマンドが指定された場合、指定された DHCP サーバによりコントローラが割り当てる DHCP サーバの設定が上書きされます。相互運用のための設定用として、IP アドレス 255.255.255.255 が有効な DHCP リレー アドレスとして FortiWLC (SD) でサポートされます。

no フォームを使用して、DHCP リレー サーバを削除します。

使用例

コントローラの DHCP リレー サーバを設定するには、以下のように **ip dhcp-server** コマンドを使用します。

```
controller(config)# ip dhcp-server 10.0.1.20
```

VLAN の DHCP サーバを設定するには、以下のようにコマンドを使用します。

```
controller(config)# vlan qa tag 100  
controller(config-vlan)# ip dhcp-server 10.0.0.1
```

関連コマンド

- [ip dhcp-passthrough \(272 ページ\)](#)
- [show controller \(172 ページ\)](#)

ip dns-server

DNS サーバの IP アドレスを設定します。

構文

```
ip dns-server <ip_addr>  
ip dns-server primary <ip_addr>    (for AP connectivity sub-mode only)  
ip dns-server secondary} <ip_addr>  (for AP connectivity sub-mode only)  
no ip dns-server
```

ip_addr ドット区切り 10 進数値で表記される DNS サーバの IP アドレス
 (n.n.n.n)

コマンド モード

グローバル設定および AP 接続設定モード

デフォルト

デフォルトでは、DNS サーバは設定されません。

用途

このコマンドを使用して、IP アドレスを指定して DNS サーバを追加します。DNS サーバが追加されると、必要になった場合、システムは利用可能な最初の DNS サーバに接続します。システムは稼働している DNS サーバが見つかるまで DNS サーバに順次アクセスしていきます。

no フォームを使用して、DNS サーバを削除します。

使用例

コントローラにより使用される DNS サーバの IP アドレスを割り当てるには、以下のよう
に **ip dns-server** コマンドを IP アドレスを指定して使用します。

```
controller(config)# ip dns-server 10.0.200.1
```

AP により使用される DNS サーバの IP アドレスを割り当てるには、AP 接続サブ モードに
入り、**ip dns-server primary** または **ip dns-server secondary** コマンドを使用して、
リモート AP により使用される DNS サーバの IP アドレスを設定します。

```
controller(config)# ap 1  
controller(config-ap)# 13-connectivity 13-preferred  
controller(config-ap-connectivity)# ip dns-server primary 10.0.0.1
```

関連コマンド

- [ip address](#) (267 ページ)

- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)

ip domainname

DNS ドメイン名を設定します。

構文

```
ip domainname <name>  
no ip domainname
```

name 1 ～ 63 文字の範囲でドメイン名を指定します。

コマンドモード

グローバル設定

デフォルト

なし

用途

DNS で使用するドメイン名を設定します。**no** フォームを使用して、設定したドメイン名を削除します。

使用例

DNS で使用するドメイン名を割り当てるには、**configure terminal** と入力して グローバル設定モードに入り、以下のように名前を指定して **ip domainname** コマンドを使用します。

```
controller(config)# ip domainname fortinet.com
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)

ip ftp

FTP のユーザ名とパスワードを設定します。

構文

```
ip ftp username <username>  
ip ftp password <username> <password>
```

<i>username</i>	FTP のユーザ名を指定します。
<i>password</i>	FTP のパスワードを指定します。

コマンド モード

グローバル設定

デフォルト

なし

用途

FTP セッションのデフォルトのユーザ名とパスワードを設定します。

使用例

FTP のユーザ名をセッションで susanne に設定するには、以下のように指定します。

```
controller(config)# ip ftp username susanne
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)

ip scp

SCP のユーザ名とパスワードを設定します。

構文

```
ip scp username <username>  
ip scp password <username> <password>
```

<i>username</i>	SCP ユーザ名を指定します。名前に使用できる文字数は最大で 32 です。
<i>password</i>	SCP パスワードを指定します。パスワードに使用できる文字数は最大で 32 です。

コマンド モード

グローバル設定

デフォルト

用途

SCP セッションのデフォルトのユーザ名とパスワードを設定します。

使用例

SFTP のユーザ名をセッションで *suzanne* に設定するには、以下のように指定します。

```
controller(config)# ip scp username suzanne
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)

ip sftp

SFTP のユーザ名とパスワードを設定します。

構文

```
ip sftp username <username>  
ip sftp password <username> <password>
```

<i>username</i>	SFTP のユーザ名を指定します。
<i>password</i>	SFTP のパスワードを指定します。

コマンド モード

グローバル設定

デフォルト

なし

用途

SFTP セッションのデフォルトのユーザ名とパスワードを設定します。

使用例

SFTP のユーザ名をセッションで `suzann` に設定するには、以下のように指定します。

```
controller(config)# ip sftp username suzann
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)

ip udp-broadcast

UDP ブロードキャスト ポートを設定します。

構文

```
ip udp-broadcast upstream <port_number>
ip udp-broadcast upstream-bridged <port_number>
ip udp-broadcast downstream <port_number>
ip udp-broadcast downstream-bridged <port_number>
no ip udp-broadcast upstream <port_number>
no ip udp-broadcast upstream-bridged <port_number>
no ip udp-broadcast downstream <port_number>
no ip udp-broadcast downstream-bridged <port_number>
```

port_number アップストリームまたはダウンストリームのポート番号を指定します
(1 ~ 65535)。

コマンド モード

グローバル設定

デフォルト

ポートは設定されていません。

用途

このコマンドは、アプリケーションのブロードキャスト トラフィックを渡す場合に必要で、ブロードキャストの宛先アドレスで検査される UDP ポートのセットを設定し、有線インターフェイスのブロードキャストとしてアップストリームを送信するか、ワイヤレス インターフェイスでダウンストリームを送信します。設定可能なポートの最大数は各方向で 8 つです。**no** フォームを使用して UDP ブロードキャスト ポートを削除します。この機能は、ワイヤレス ステーション間の UDP ブロードキャストも設定します。

使用例

ワイヤレスをワイヤレス UDP ブロードキャストを設定するには、ポートのアップストリームおよびダウンストリーム ブロードキャストを有効にします。この例では、次の CLI コマンドによりポート 10000 でこの機能が有効になっています。

```
configure terminal
ip udp-broadcast upstream 10000
ip udp-broadcast downstream 10000
end
```

たとえば、ポート 5455 をワイヤレス クライアントの UDP ブロードキャスト用に使用する場合は、以下のコマンドを使用します。

```
controller(config)# ip udp-broadcast downstream 5455
```

たとえば、設定されているアップストリームのポート番号 3822 をキャンセルするには、以下のコマンドを使用します。

```
controller(config)# no ip udp-broadcast upstream 3822
```

関連コマンド

- [ip address \(267 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip default-gateway \(270 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)

ipv6-neighbor-discovery-optimization

IPv6 近接検出の最適化を有効または無効にします。

構文

`ipv6-neighbor-discovery-optimization`

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、ipv6 の近接検出の最適化機能を有効または無効にします。

使用例

```
MC3200(15)# configure terminal
MC3200(15)(config)# ipv6-neighbor-discovery-optimization enable
MC3200(15)(config)#
```

関連コマンド

[*show ipv6-neighbor*](#) (306 ページ)

mac-address

イーサネットインターフェイスの MAC アドレスを設定します。

構文

`mac-address <MAC-address>`

mac-address 16 進形式で指定する、イーサネット インターフェイスの MAC アドレス (xx:xx:xx:xx:xx:xx:xx:xx)。

コマンドモード

インターフェイス設定

デフォルト

なし

用途

MAC アドレスを入力して、イーサネット インターフェイスを設定します。

使用例

```
mc1100# (config)# ap 1
mc1100# (config-ap)# mac-address 00:12:F2:00:00:59
mc1100# (config-ap)#
```

関連コマンド

[show interfaces FastEthernet ap \(296 ページ\)](#)

port-profile

ポート プロファイルの作成および設定を許可します。

構文

port-profile <*profile*>

profile 変更または作成するプロファイルの名前。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、ポート プロファイルのプロパティをアクセスしたり、本章で説明する他のコマンドを使用して変更したりするのに使用します。ポート プロファイルをベースとするコマンドはすべて、ポート プロファイル設定モードで実行されます。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)#
```

関連コマンド

- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) ap-vlan-tag

現在のポート プロファイルの VLAN タグを指定できます。

構文

ap-vlan-tag <VLAN>

VLAN ポート プロファイルに割り当てる VLAN タグ。1 ～ 4094 の範囲で指定できます。

コマンド モード

ポート プロファイル設定

デフォルト

なし

用途

このコマンドは、現在のポート プロファイルに使用する VLAN タグを指定するのに使用します。VLAN タグは、ブリッジ モードでの操作でのみ使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# ap-vlan-tag 14
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) dataplane

ブリッジ モードとトンネル モードの間でポート プロファイルを切り替えることを許可します。

構文

`dataplane <mode>`

mode *bridged* または *tunneled* を指定します。

コマンド モード

ポート プロファイル設定

デフォルト

Tunneled

用途

このコマンドは、ポート プロファイルをブリッジまたはトンネルのどちらの操作で使用する必要があるかを指定するために使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# dataplane bridged
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) disable

現在のポート プロファイルを無効にします。

構文

disable

コマンド モード

ポート プロファイル設定

デフォルト

無効

用途

このコマンドは、アクティブなポート プロファイルを無効にするのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# disable
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) enable

現在のポート プロファイルを有効にします。

構文

enable

コマンド モード

ポート プロファイル設定

デフォルト

無効

用途

このコマンドは、アクティブなポート プロファイルを有効にするのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# enable
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) multicast-enable

このポート プロファイルを起点または終点とするマルチ フレームの送信を有効にします。

構文

```
multicast-enable  
no multicast-enable
```

コマンド モード

ポート プロファイル設定

デフォルト

オフ

用途

このコマンドは、ポート プロファイルの Allow Multicast フラグを設定するのに使用します。このポートでのマルチキャスト転送を有効にするには、**multicast-enable** コマンドを入力し、無効にするには、**no multicast-enable** を入力します。以下の例は、port1 プロファイルでのマルチキャストを有効にし、無効にします。

使用例

```
default(15)# configure terminal  
default(15)(config)# port-profile port1  
default(15)(config-port-profile)# multicast-enable  
default(15)(config-port-profile)#  
default(15)(config-port-profile)# multicast-disable  
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) show

変更する現在のポート プロファイルを表示できます。

構文

`show context`

コマンド モード

ポート プロファイル設定

デフォルト

なし

用途

このコマンドは、アクティブなポート プロファイルを表示するのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# show context
Port Profile Name: port1
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) vlan \(291 ページ\)](#)

(config-port-profile) vlan

ポート プロファイルがアクセスする VLAN の名前を指定します。

構文

vlan <name>

name VLAN の名前。

コマンド モード

ポート プロファイル設定

デフォルト

なし

用途

このコマンドは、設定されているポートがサービスする VLAN の名前を設定するのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# vlan v1
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)
- [\(config-port-profile\) show \(290 ページ\)](#)

(config-port-profile) ip-prefix-validation-enable

別のサブネットの IP アドレスがあるステーションがコントローラに接続する場合、動作の停止など、さまざまなネットワークの問題が発生する可能性があります。IP プレフィックス検証を有効にすると、異なるサブネットのステーションがコントローラに接続することを防止できます。デフォルトでは、IP プレフィックス検証はポート プロファイルでオフになっています。

構文

ip-prefix-validation-enable

name VLAN の名前。

コマンドモード

ポート プロファイル設定

デフォルト

なし

用途

このコマンドは、IP プレフィックス検証を有効または無効にするために使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# ip-prefix-validation-enable
default(15)(config-port-profile)#
```

関連コマンド

- [port-profile \(284 ページ\)](#)
- [\(config-port-profile\) ap-vlan-tag \(285 ページ\)](#)
- [\(config-port-profile\) dataplane \(286 ページ\)](#)
- [\(config-port-profile\) disable \(287 ページ\)](#)
- [\(config-port-profile\) enable \(288 ページ\)](#)
- [\(config-port-profile\) multicast-enable \(289 ページ\)](#)

[\(config-port-profile\) show](#) (290 ページ)

show igmp-snoop

IGMP スヌーピングに関連する情報を表示します。

構文

```
show igmp-snoop forwarding-table  
show igmp-snoop subscription-table]
```

コマンド モード

特権 EXEC モード

デフォルト

なし

用途

このコマンドは、IGMP スヌーピングが有効または無効であるか、また、有効である場合、デバイスが IGMP スヌープ グループからタイムアウトする秒数を表示します。

オプションの引数 **forwarding-table** を使用すると、参加している ESS ID のリスト、AP の MAC アドレス、マルチキャスト グループ名、およびフィルタモード情報が生成されます。

オプションの引数 **subscription-table** を使用すると、参加している ESS ID のリスト、AP の MAC アドレス、サブスクライブしているクライアントの MAC アドレス、マルチキャスト情報が生成されます。

使用例

```
controller# show igmp-snoop
```

```
IGMP Snoop
```

```
IGMP Snoop Enable/Disable          : enable
```

```
IGMP Snoop expiration timer period : 240
```

```
MC500# show igmp-snoop forwarding-table
```

```
Ess ID          AP MAC          Multicast Group  Filter Mode Source  
List
```

```
IGMP Snoop forward table(No entries)
```

```
MC500# show igmp-snoop subscription-table
```

```
<CR>
```

```
MC500# show igmp-snoop subscription-table
```


Ess ID	AP MAC	Client MAC	Multicast Group
Aging Time	Filter Mode	Source List	

IGMP Snoop subscription table (No entries)

関連コマンド [igmp-snoop \(262 ページ\)](#)

show interfaces FastEthernet ap

アクセス ポイントの FastEthernet 設定に関連する情報を表示します。

構文

show interfaces FastEthernet ap [ap-id] [interface index]

- ap-id

アクセス ポイントに固有の識別子を指定します。
- interface index

表示するインターフェイスを指定します。いくつかの AP モデルは、複数のインターフェイスがあるため、ユーザは使用するオプションを指定する必要があります。

コマンドモード

特権 EXEC モード

デフォルト

なし

用途

このコマンドは、すべての AP あるいは特定のアクセス ポイントの FastEthernet インターフェイス設定情報を表示します。以下の情報が提供されます。

パラメータ	説明
Type	ノード タイプ。たとえばアクセス ポイントです。
ID	各アクセス ポイント固有の識別子 (ID) です。
Name	アクセス ポイントの名前です。
Interface Index	このインターフェイスを識別するためのインデックスです。
MTU	インターフェイスの MTU (最大送信可能) です。
MAC Address	インターフェイスの MAC アドレスです。
Admin State	インターフェイスの管理状態です。状態は、 Up または Down になります。

パラメータ	説明
Operational State	インターフェイスの状態です。状態は、 Enabled または Disabled になります。
Last Changed	インターフェイスが最後に変更された日付です。
Uplink Type	インターフェイスがアップリンクまたはダウンリンク接続のいずれかに設定されているかを表示します。

使用例

以下のコマンドは、すべての AP の FastEthernet 設定を表示します。

```
controller# show interfaces FastEthernet ap
```

```
Type ID Name IfIndex MTU MAC Address Admin State Op State Last Change
Uplink Type
ap 170 AP-170 2 1500 00:0c:e6:0d:ef:87 Up Disabled 06/06/2013 09:09:34
Downlink
ap 170 AP-170 1 1500 00:0c:e6:0d:ef:87 Up Disabled 06/06/2013 09:09:34
Uplink
ap 169 AP-169 2 1500 00:0c:e6:0d:ef:71 Up Disabled 06/06/2013 09:09:34
Downlink
ap 169 AP-169 1 1500 00:0c:e6:0d:ef:71 Up Disabled 06/06/2013 09:09:34
Uplink
ap 167 AP-167 2 1500 00:0c:e6:0d:ee:aa Up Disabled 06/06/2013 09:09:34
Downlink
ap 167 AP-167 1 1500 00:0c:e6:0d:ee:a9 Up Enabled 06/06/2013 09:11:29
Uplink Interface Table(6)
```

The following command displays FastEthernet configuration information for AP 1:

```
controller# show interfaces FastEthernet ap 167
```

```
Type ID Name IfIndex MTU MAC Address Admin State Op State Last Change
Uplink Type
ap 167 AP-167 1 1500 00:0c:e6:0d:ee:a9 Up Enabled 06/06/2013 09:11:29
Uplink
ap 167 AP-167 2 1500 00:0c:e6:0d:ee:aa Up Disabled 06/06/2013 09:09:34
Downlink
Ethernet Table(2 entries)
```

以下のコマンドは、次の AP の特定のインターフェイスの FastEthernet 設定情報を表示しています。

```
controller# show interfaces FastEthernet ap 167 1
```

Ethernet Table
Node Type : ap
Node ID : 167
Node Name : AP-167
Interface Index : 1
Description : eth0-167-1
MTU : 1500
Interface Speed (Mbits/sec) : 1000
Duplex Mode : full-duplex
Physical Address : 00:0c:e6:0d:ee:a9
Administrative State : Up
Operational State : Enabled
Last Changed : 06/06/2013 09:11:29
Uplink Type : Uplink

関連コマンド [interface FastEthernet \(264 ページ\)](#)

show interfaces FastEthernet controller

コントローラの FastEthernet 設定に関連する情報を表示します。

構文

`show interfaces FastEthernet controller`

コマンドモード

特権 EXEC モード

デフォルト

なし

用途

このコマンドは、コントローラの FastEthernet インターフェイス設定情報を表示します。以下の情報が提供されます。

パラメータ	説明
Node Type	ノード タイプ。たとえばコントローラです。
Node ID	コントローラ固有の識別子 (ID) です。
Node Name	コントローラに割り当てられた名前です。
Interface Index	このインターフェイスを識別するためのインデックスです。
Description	インターフェイスの説明を表示します。
MTU	インターフェイスの MTU (最大送信可能) です。
Interface Speed (Mbits/sec)	インターフェイスの設定速度
Duplex Mode	インターフェイスが全二重と半二重のどちらのモードを使用しているかを示します。
Physical MAC Address	インターフェイスの MAC アドレスです。
Operational State	インターフェイスの状態です。状態は、 Enabled または Disabled になります。
Last Changed	インターフェイスが最後に変更された日付です。
In Octets	このインターフェイスが受信したオクテット数です。

パラメータ	説明
In Unicast Packets	このインターフェイスが受信したユニキャスト パケット数です。
In Non-Unicast Packets	このインターフェイスが受信した非ユニキャスト パケット数です。
In Discards	このインターフェイスによって破棄された着信パケット数です。
In Errors	このインターフェイス上でエラーとなった着信パケット数です。
In Unknown Protocols	このインターフェイスが受信した不明なプロトコルを持つパケット数です。
Out Octets	このインターフェイスが送信したオクテット数です。
Out Unicast Packets	このインターフェイスが送信したユニキャスト パケット数です。
Out Non-Unicast Packets	このインターフェイスが送信した非ユニキャスト パケット数です。
Out Discards	このインターフェイスによって破棄された送信パケット数です。
Out Errors	このインターフェイス上でエラーとなった送信パケット数です。
Out Queue Length	送信パケット キューのパケット数です。

使用例

以下のコマンドは、コントローラの FastEthernet 設定情報を表示します。

```
controller# show interfaces FastEthernet controller
```

```
Type          ID  Name          MTU      MAC Address      Op State  Last
Change
controller 1  controller    1500     00:90:0b:07:d0:82 Enabled   2008/
03/07 09:22:26
```

```
Interface Table(1 entry)
```

```
Interface Table
```

```
Node Type          : controller
```

```
Node ID            : 1
```

Node Name	: controller1
Interface Index	: 3
Description	: eth1
MTU	: 1500
Interface Speed (Mbits/sec)	: 100
Duplex Mode	: full-duplex
Physical Address	: 00:02:b3:e6:d7:12
Operational State	: Enabled
Last Changed	: -
Description	: eth1
In Octets	: 272189914
In Unicast Packets	: 1638979
In Non-Unicast Packets	: 0
In Discards	: 0
In Errors	: 0
In Unknown Protocols	: 0
Out Octets	: 1467641108
Out Unicast Packets	: 9827811
Out Non-Unicast Packets	: 0
Out Discards	: 0
Out Errors	: 0

関連コマンド [interface FastEthernet \(264 ページ\)](#)

show interfaces FastEthernet statistics

FastEthernet インターフェイスに関連する統計データを表示します。

構文

```
show interfaces FastEthernet statistics ap <ap_id>  
show interfaces FastEthernet statistics controller]
```

コマンド
モード

特権 EXEC モード

デフォルト

なし

用途

このコマンドは、FastEthernet AP またはコントローラの統計データを表示します。以下の情報が提供されます。

統計	説明
IfIndex	インターフェイスを識別するインデックスです。
Node ID	ノードに固有の識別子 (コントローラまたは AP) です。
Node Name	ノードに割り当てられた名前です。
Type	ノード タイプ。たとえばコントローラまたは AP です。
In Octets	このインターフェイスが受信したオクテット数です。
In Errors	このインターフェイスが受信したエラー数です。
Out Octets	このインターフェイスが送信したオクテット数です。
Out Errors	このインターフェイスが送信したエラー数です。

使用例

以下のコマンドは、コントローラおよび関連する AP についての FastEthernet 統計データを表示します。

```
controller# show interfaces FastEthernet statistics  
Ethernet Statistics
```


IfIndex	Node ID	Node Name	Type	In Octets	In Errors	Out
Octets	Out	Errors				
2	1	meru-wifi	controller	566589467	0	
192971219		0				
100	2	#2-2F-Sw-208	ap	665578131	0	
328290792		0				
100	3	#3-2F-Exec-201	ap	124603915	0	
84559243		0				
100	11	AP-11	ap	123112809	0	
545091756		0				
100	12	AP-12	ap	0	0	
0						

Ethernet Statistics(5 entries)

show ip

IP 設定情報を表示します。

構文

```
show ip
show ip default-gateway
show ip dhcp-server
show ip dns-server
show ip domainname
```

コマンドモード

特権 EXEC モード

デフォルト

コントローラの IP アドレス情報を表示します。

用途

このコマンドを使用して、コントローラに割り当てられている IP アドレス、デフォルトゲートウェイ、DHCP および DNS サーバ、およびドメイン名を確認します。

使用例

以下のコマンドは、各キーワードを使用して IP アドレスを表示しています。

```
controller# show ip
```

ID	IP Address	NetMask	Type
0	192.168.10.2	255.255.255.0	Static

IP Addresses(1 entry)

Interface Assignment	Number Type	IP Address Interface Mode	NetMask	Gateway Address
1 active		172.26.0.53	255.255.240.0	172.26.0.1 DHCP

IP Addresses(1 entry)

```
controller# show ip default-gateway
```

```
192.168.10.1
```

```
controller# show ip dhcp-server
```

```
10.0.0.10
```

```
controller# show ip dns-server
```

```
DNS Server
```

```
10.0.0.10
```

```
DNS Server Table(1 entry)
```

```
controller# show ip domainname
```

```
fortinet.com
```

show ipv6-neighbor

IPv6 近接テーブルを表示します。

構文

`show ipv6-neighbor`

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、IPv6 近接テーブルを表示します。

使用例

MC3200(15)# `show ipv6-neighbor`

関連コマンド

[*ipv6-neighbor-discovery-optimization*](#) (282 ページ)

show second_interface_status

FastEthernet インターフェイス 2 の冗長モード ステータスを表示します。

構文

`show second_interface_status`

コマンド モード

特権 EXEC モード

デフォルト

なし

用途

冗長モードとして構成されコントローラの第 1 インターフェイスのバックアップとして動作しているときの、第 2 FastEthernet インターフェイスのステータスを表示します。

関連コマンド

- [interface FastEthernet \(264 ページ\)](#)
- [type \(311 ページ\)](#)
- [show interfaces FastEthernet controller \(299 ページ\)](#)

static-route

固定ルートを作成・設定できます。

構文

`static-route <name>`

name 変更または作成するルートの名前。

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドは、固定ルートのプロファイルのプロパティをアクセスしたり、本章で説明する他のコマンドを使用して変更したりするのに使用します。固定ルートをベースとするコマンドはすべて、固定ルート設定モードで実行されます。

使用例

```
default(15)# configure terminal
default(15)(config)# static-route stat
default(15)(config-static-route)#
```

関連コマンド

- [\(config-static-route\) interface \(309 ページ\)](#)
- [\(config-static-route\) ip \(310 ページ\)](#)

(config-static-route) interface

ルートが使用するイーサネット インターフェイスを指定します。

構文

```
interface fastEthernet <interface>
```

interface **primary** または **secondary** インターフェイスを指定します。

コマンド モード

固定ルート設定

デフォルト

Primary

用途

このコマンドは、現在の固定ルートが使用するイーサネット インターフェイスを指定するのに使用します。primary または secondary のいずれかのインターフェイスを選択できます。

使用例

```
default(15)# configure terminal
default(15)(config)# static-route stat
default(15)(config-static-route)# interface fastEthernet secondary
default(15)(config-static-route)#
```

関連コマンド

- [static-route \(308 ページ\)](#)
- [\(config-static-route\) ip \(310 ページ\)](#)

(config-static-route) ip

ルートが使用する IP アドレスとサブネット マスクを指定します。

構文

```
ip address <ip> <subnet>
```

<i>ip</i>	255.255.255.255 表記の IP アドレス。
<i>subnet</i>	255.255.255.255 表記のサブネット マスク。

コマンド モード

固定ルート設定

デフォルト

なし

用途

このコマンドは、現在の固定ルートに使用する IP アドレスとサブネット マスクを指定するのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# static-route stat
default(15)(config-static-route)# ip address 192.168.14.0 255.255.255.0
default(15)(config-static-route)#
```

関連コマンド

- [static-route \(308 ページ\)](#)
- [\(config-static-route\) interface \(309 ページ\)](#)

type

FastEthernet インターフェイスの使用タイプを設定します。

構文

```
type active
type redundant
```

active	インターフェイスを完全な機能がある FastEthernet インターフェイスとして設定します。インターフェイス 1 または 2 に対して使用できます。
redundant	インターフェイスを FastEthernet インターフェイス 1 のバックアップとして設定します。これは、インターフェイス インデックス 2 に対してのみ使用できます。

コマンドモード

FastEthernet インターフェイス設定モード

デフォルト

なし

用途

このコマンドを使用して、FastEthernet インターフェイスの使用方法を決定します。**type** オプションは、**active** および **redundant** となります。用途は、設定されているポートに依存します。デフォルトのインターフェイス 1 は **active** として設定する必要がありますが、インターフェイス 2 は、**active** または **redundant** のいずれかに設定できます。



第 1 イーサネット インターフェイスは、デフォルトの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。

第 2 インターフェイスが **redundant** として設定される場合、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。この設定では、第 1 インターフェイスに固定 IP アドレスを設定する必要があります。

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)。

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。このような構成はスパニング ツリー ネットワーク セットアップで行います。



第 2 インターフェイスに割り当てられる IP アドレスを介してコントローラを検出するように AP を設定することはできません。冗長モードまたはアクティブ モードで第 2 インターフェイスを設定する前に、コントローラのボンディングモードを `dual` または `none` (コントローラ モードによる) に設定する必要があります。詳細については、『FortiWLC (SD) 設定ガイド』を参照してください。

使用例

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、インターフェイスの IP 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設定を指定し、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)# end
```

次のコマンドは、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。この設定を行うには、**type** オプションに **redundant** を指定します。

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# type redundant
default(config-if-FastEth)# end
```

関連コマンド

- [gw \(261 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip address \(267 ページ\)](#)
- [show interfaces FastEthernet controller \(299 ページ\)](#)
- [show second_interface_status \(307 ページ\)](#)

virtual-interface-profile

仮想インターフェイス プロファイルの作成・設定を許可します。

構文

`virtual-interface-profile <profile>`

profile 変更または作成するプロファイルの名前。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、仮想インターフェイス プロファイルのプロパティをアクセスしたり、本章で説明する他のコマンドを使用して変更したりするのに使用します。仮想インターフェイスをベースとするコマンドはすべて、仮想インターフェイス設定モードで実行されます。

使用例

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)#
```

関連コマンド

- [\(config-vip\) disable \(314 ページ\)](#)
- [\(config-vip\) enable \(315 ページ\)](#)
- [\(config-vip\) gateway \(316 ページ\)](#)
- [\(config-vip\) ip \(317 ページ\)](#)
- [\(config-vip\) show \(318 ページ\)](#)

(config-vip) disable

現在の仮想インターフェイス プロファイルを無効にします。

構文

disable

コマンド モード

仮想インターフェイス プロファイル設定

デフォルト

無効

用途

このコマンドは、アクティブな仮想インターフェイス プロファイルを無効にするのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# disable
default(15)(config-virtual-interface-profile)#
```

関連コマンド

- [virtual-interface-profile \(313 ページ\)](#)
- [\(config-vip\) enable \(315 ページ\)](#)
- [\(config-vip\) gateway \(316 ページ\)](#)
- [\(config-vip\) ip \(317 ページ\)](#)
- [\(config-vip\) show \(318 ページ\)](#)

(config-vip) enable

現在の仮想インターフェイス プロファイルを有効にします。

構文

enable

コマンドモード

仮想インターフェイス プロファイル設定

デフォルト

無効

用途

このコマンドは、アクティブな仮想インターフェイス プロファイルを有効にするのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# enable
default(15)(config-virtual-interface-profile)#
```

関連コマンド

- [virtual-interface-profile \(313 ページ\)](#)
- [\(config-vip\) disable \(314 ページ\)](#)
- [\(config-vip\) gateway \(316 ページ\)](#)
- [\(config-vip\) ip \(317 ページ\)](#)
- [\(config-vip\) show \(318 ページ\)](#)

(config-vip) gateway

現在の仮想インターフェイス プロファイルに使用するゲートウェイ アドレスを指定します。

構文

```
gateway <ip>
```

ip 255.255.255.255 表記の IP アドレス。

コマンド モード

仮想インターフェイス プロファイル設定

デフォルト

なし

用途

このコマンドは、アクティブな仮想インターフェイス プロファイルのゲートウェイ アドレスを設定するのに使用します。このアドレスは、標準 IP 表記 : 255.255.255.255 で入力する必要があります。

使用例

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# gateway 192.168.14.1
default(15)(config-virtual-interface-profile)#
```

関連コマンド

- [virtual-interface-profile \(313 ページ\)](#)
- [\(config-vip\) disable \(314 ページ\)](#)
- [\(config-vip\) enable \(315 ページ\)](#)
- [\(config-vip\) ip \(317 ページ\)](#)
- [\(config-vip\) show \(318 ページ\)](#)

(config-vip) ip

現在の仮想インターフェイス プロファイルに使用するサブネット IP アドレスとサブネット マスクを指定します。

構文

```
ip address <ip> <subnet>
```

<i>ip</i>	255.255.255.255 表記の IP アドレス。
<i>subnet</i>	255.255.255.255 表記のサブネット マスク。

コマンド モード

仮想インターフェイス プロファイル設定

デフォルト

なし

用途

このコマンドは、アクティブな仮想インターフェイス プロファイルのサブネット IP アドレスとサブネット マスクを設定するの に使用します。このアドレスは、標準 IP 表記：255.255.255.255 で入力する必要があります。

使用例

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# ip address 192.168.14.0
255.255.255.0
default(15)(config-virtual-interface-profile)#
```

関連コマンド

- [virtual-interface-profile \(313 ページ\)](#)
- [\(config-vip\) disable \(314 ページ\)](#)
- [\(config-vip\) enable \(315 ページ\)](#)
- [\(config-vip\) gateway \(316 ページ\)](#)
- [\(config-vip\) show \(318 ページ\)](#)

(config-vip) show

変更する現在の仮想インターフェイス プロファイルを表示できます。

構文

show context

コマンドモード

仮想インターフェイス プロファイル設定

デフォルト

なし

用途

このコマンドは、アクティブな仮想インターフェイス プロファイルを表示するのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# show context
Virtual Interface Profile Name: vip
default(15)(config-virtual-interface-profile)#
```

関連コマンド

- [virtual-interface-profile \(313 ページ\)](#)
- [\(config-vip\) disable \(314 ページ\)](#)
- [\(config-vip\) enable \(315 ページ\)](#)
- [\(config-vip\) gateway \(316 ページ\)](#)
- [\(config-vip\) ip \(317 ページ\)](#)

8 VLAN コマンド

FortiWLC (SD) では、仮想 LAN (VLAN) および Generic Routing Encapsulation (GRE) 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 および GRE 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。GRE トンネルと VLAN を作成して設定するコマンドは次のとおりです。

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)
- [gre \(343 ページ\)](#)
- [interface FastEthernet controller \(345 ページ\)](#)
- [ip remote-external-address \(347 ページ\)](#)
- [ip tunnel-ip-address \(348 ページ\)](#)
- [show dhcp-server \(349 ページ\)](#)
- [show gre \(351 ページ\)](#)

- [show dhcp-lease](#) (352 ページ)
- [show vlan](#) (353 ページ)
- [test gre](#) (355 ページ)
- [vlan](#) (356 ページ)
- [wapi-server](#) (357 ページ)

dhcp-server

コントローラをベースとする DHCP サーバの設定へのアクセスを提供します。

構文

`dhcp-server <name>`

name 変更または作成する DHCP サーバの名前。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、コントローラをベースとする DHCP サーバの設定モードへのアクセスに使用します。DHCP をベースとするコマンドはすべて、このモードで実行する必要があります。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)#
```

関連コマンド

- [show dhcp-server \(349 ページ\)](#)
- [show dhcp-lease \(352 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)

- [\(config-dhcp-server\) vlan](#) (339 ページ)
- [\(config-dhcp-server\) virtual-interface-profile](#) (341 ページ)

(config-dhcp-server) disable

現在の DHCP サーバを無効にします。

構文

disable

コマンドモード

DHCP サーバ設定

デフォルト

無効

用途

このコマンドは、アクティブな DHCP サーバを無効にするのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# disable
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) dns-server-primary

現在の DHCP サーバのプライマリ DNS サーバを設定します。

構文

`dns-server-primary <IP>`

IP 対象となる DNS サーバの IP。

コマンド モード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、プライマリ DNS サーバに DHCP サーバが使用する IP アドレスを入力します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# dns-server-primary 192.168.14.14
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) dns-server-secondary

現在の DHCP サーバのセカンダリ DNS サーバを設定します。

構文

`dns-server-secondary <IP>`

IP

対象となる DNS サーバの IP。

コマンドモード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、セカンダリ DNS サーバに DHCP サーバが使用する IP アドレスを入力します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# dns-server-secondary 192.168.17.17
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)

- [\(config-dhcp-server\) virtual-interface-profile](#) (341 ページ)

(config-dhcp-server) domain-name

現在の DHCP サーバが使用するドメイン名を設定します。

構文

`domain-name <name>`

name 設定するドメイン名。

コマンド モード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、DHCP サーバが使用するドメイン名を入力します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# domain-name sampledomain
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) enable

現在の DHCP サーバを有効にします。

構文

enable

コマンド モード

DHCP サーバ設定

デフォルト

無効

用途

このコマンドは、アクティブな DHCP サーバを無効にするのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# enable
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) ip-pool

DHCP サーバが割り当てることができる IP の範囲を指定します。

構文

`ip-pool <start-ip> <end-ip>`

start-ip 割り当てることができる最初の IP。

end-ip 割り当てることができる最後の IP。

コマンド モード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、現在の DHCP サーバが使用するために予約されている IP アドレスの範囲を設定します。コマンド ライン パラメータとして入力する 2 つの IP アドレスの間のすべての IP が使用できるようになります。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# ip-pool 192.168.15.100 192.168.15.150
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)

- [\(config-dhcp-server\) vlan](#) (339 ページ)
- [\(config-dhcp-server\) virtual-interface-profile](#) (341 ページ)

(config-dhcp-server) lease-time

DHCP サーバが割り当てることができるリースの時間を指定します。

構文

`lease-time <time>`

time リースの時間 (秒数)。300 ~ 65535 の範囲で指定できます。

コマンド モード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、現在のサーバが割り当てる DHCP リースの時間を設定します。
リース時間は秒単位で入力し、300 ~ 65535 の範囲で指定する必要があります。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# lease-time 3000
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) netbios-server-primary

現在の DHCP サーバのプライマリ NETBIOS サーバを設定します。

構文

`netbios-server-primary <IP>`

IP 対象となる NETBIOS サーバの IP。

コマンドモード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、プライマリ NETBIOS サーバに DHCP サーバが使用する IP アドレスを入力します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# netbios-server-primary 192.168.14.24
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)

- [\(config-dhcp-server\) virtual-interface-profile](#) (341 ページ)

```
(config-dhcp-server) netbios-server-secondary
```

現在の DHCP サーバのセカンダリ NETBIOS サーバを設定します。

構文

```
netbios-server-secondary <IP>
```

IP

対象となる NETBIOS サーバの IP。

コマンドモード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、セカンダリ NETBIOS サーバに DHCP サーバが使用する IP アドレスを入力します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# netbios-server-secondary 192.168.17.27
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)

- [\(config-dhcp-server\) virtual-interface-profile](#) (341 ページ)

(config-dhcp-server) option-43

DHCP サーバの DHCP オプション 43 設定を有効にします。

構文

option-43 <hostname1>,<hostname2>

hostname1 DHCP オプション 43 をサポートするコントローラのホスト名または IP アドレス。

hostname2 オプションで、DHCP オプション 43 をサポートする 2 つ目のコントローラを指定します。

コマンドモード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドを使用して、DHCP サーバの DHCP オプション 43 サポートを有効にします。この機能は、ベンダ固有の AP 操作に使用します。詳細については、AP のマニュアルを参照してください。最大で 2 つのコントローラをオプション 43 設定に指定できます。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# option-43 172.15.182.36,176.27.3.45
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)

- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) show

変更する現在の DHCP サーバを表示できます。

構文

`show context`

コマンドモード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドは、アクティブな DHCP サーバを表示するのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# show context
DHCP Server Pool Name: dhcp1
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) vlan \(339 ページ\)](#)
- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) vlan

DHCP サーバに割り当てる VLAN の名前を指定します。

構文

`vlan <name>`

name VLAN の名前。

コマンド モード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドは、DHCP サーバに割り当てる VLAN の名前を設定するのに使用します。コントローラが L2 ルーティング モードで動作している場合のみ、このオプションを使用できます。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# vlan v1
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)

- [\(config-dhcp-server\) virtual-interface-profile \(341 ページ\)](#)

(config-dhcp-server) virtual-interface-profile

DHCP サーバに割り当てる仮想インターフェイス プロファイルの名前を指定します。

構文

```
virtual-interface-profile <name>
```

name 仮想インターフェイス プロファイルに割り当てる名前。

コマンドモード

DHCP サーバ設定

デフォルト

なし

用途

このコマンドは、DHCP サーバに割り当てる仮想インターフェイス プロファイル の名前を設定するのに使用します。

使用例

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# virtual-interface-profile vint1
default(15)(config-dhcp-server)#
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [\(config-dhcp-server\) disable \(323 ページ\)](#)
- [\(config-dhcp-server\) dns-server-primary \(324 ページ\)](#)
- [\(config-dhcp-server\) dns-server-secondary \(325 ページ\)](#)
- [\(config-dhcp-server\) domain-name \(327 ページ\)](#)
- [\(config-dhcp-server\) enable \(328 ページ\)](#)
- [\(config-dhcp-server\) ip-pool \(329 ページ\)](#)
- [\(config-dhcp-server\) lease-time \(331 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-primary \(332 ページ\)](#)
- [\(config-dhcp-server\) netbios-server-secondary \(334 ページ\)](#)
- [\(config-dhcp-server\) option-43 \(336 ページ\)](#)
- [\(config-dhcp-server\) show \(338 ページ\)](#)

- [\(config-dhcp-server\) vlan](#) (339 ページ)

gre

GRE トンネル プロファイルを命名して、GRE 設定サブモードに入ります。

構文

`gre <name>`

name GRE トンネル プロファイルの名前。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、GRE トンネル プロファイルの名前を指定して、GRE 設定サブモードに入ります。GRE 設定サブモードでは、GRE トンネルの詳細なオプションを設定できます。このプロファイルの名前は、ESSID プロファイルの GRE プロファイルを指定する場合、この設定の他の部分でも使用されます。

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。

使用例

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場合にどのようにこのコマンドを使用するかを示しています。第 2 FastEthernet インターフェイスでは、トンネルのローカル エンドポイントの IP アドレスは 13.13.13.13 であり、リモート エンドポイントは 172.27.0.206 となっています。また、DHCP サーバは 10.0.0.12 にあります。

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
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
```

関連コマンド

- [essid \(550 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip dhcp-server \(273 ページ\)](#)
- [ip remote-external-address \(347 ページ\)](#)
- [show gre \(351 ページ\)](#)
- [test gre \(355 ページ\)](#)

interface FastEthernet controller

GRE トンネルで使用する設定済みの FastEthernet インターフェイスを選択します。

構文

```
interface FastEthernet controller <number>
```

number 設定するコントローラのインターフェイス番号。1 または 2 のいずれかになります。

コマンドモード

GRE 設定サブモード

デフォルト

なし

用途

このコマンドは、設定している GRE トンネルで使用するコントローラ インターフェイスを指定するために使用します。選択するインターフェイス (コントローラの FastEthernet インターフェイス 1 または 2) は、**setup** コマンドや **interface FastEthernet** コマンドを使用して構成されている必要があります。インターフェイスは、アクティブ モードに設定される必要があり、IP アドレスが割り当てられている必要があります。

使用例

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場合にどのようにこのコマンドを使用するかを示しています。第 2 FastEthernet インターフェイスでは、トンネルのローカル エンドポイントの IP アドレスは 13.13.13.13 であり、リモート エンドポイントは 172.27.0.206 となっています。また、DHCP サーバは 10.0.0.12 にあります。

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
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
```

関連コマンド

- [gre \(343 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)

- [ip dhcp-server \(273 ページ\)](#)
- [ip remote-external-address \(347 ページ\)](#)
- [show gre \(351 ページ\)](#)
- [test gre \(355 ページ\)](#)

ip remote-external-address

GRE トンネルのエンドポイントの IP アドレスを設定します。

構文

```
ip remote-external-address <address>
```

address GRE トンネルのリモート エンドポイントの IP アドレス。

コマンドモード

GRE 設定サブモード

デフォルト

用途

このコマンドを使用して、作成する GRE トンネルのリモート エンドポイントのアドレスを指定します。構成を正しく行うには、固有の IP アドレスを指定する必要があります。

使用例

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場合にどのようにこのコマンドを使用するかを示しています。第 2 FastEthernet インターフェイスでは、トンネルのローカル エンドポイントの IP アドレスは 13.13.13.13 であり、リモート エンドポイントは 172.27.0.206 となっています。また、DHCP サーバは 10.0.0.12 にあります。

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
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
```

関連コマンド

- [gre \(343 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip dhcp-server \(273 ページ\)](#)
- [ip tunnel-ip-address \(348 ページ\)](#)
- [show gre \(351 ページ\)](#)
- [test gre \(355 ページ\)](#)

ip tunnel-ip-address

GRE トンネルの IP アドレスを設定します。

構文

```
ip tunnel-ip-address <address>
```

address GRE トンネルの IP アドレス。

コマンドモード

GRE 設定サブモード

デフォルト

用途

このコマンドを使用して、作成する GRE トンネルのアドレスを指定します。構成を正しく行うには、固有の IP アドレスを指定する必要があります。

使用例

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場合にどのようにこのコマンドを使用するかを示しています。第 2 FastEthernet インターフェイスでは、トンネルのローカル エンドポイントの IP アドレスは 13.13.13.13 であり、リモート エンドポイントは 172.27.0.206 となっています。また、DHCP サーバは 10.0.0.12 にあります。

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
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
```

関連コマンド

- [gre \(343 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip dhcp-server \(273 ページ\)](#)
- [ip remote-external-address \(347 ページ\)](#)
- [show gre \(351 ページ\)](#)
- [test gre \(355 ページ\)](#)

show dhcp-server

コントローラをベースとする DHCP サーバの現在の設定を表示します。

構文

```
show dhcp-server
show dhcp-server <VLAN>
```

VLAN DHCP サーバが有効である特定の VLAN の ID。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを入力して、DHCP サーバに設定されているプロパティを表示します。

- 有効 / 無効
- サブネット
- クライアント IP 範囲
- サブネット マスク
- ブロードキャスト IP アドレス
- ゲートウェイ IP アドレス
- 最大リース時間
- DNS の IP (最大で 2)
- Netbios サーバの IP (最大で 2)

使用例

```
default(15)# show dhcp-server
```

Tag	State	Lease Time	DHCP IP	Subnet	DHCP Netmask	Gateway	IP
Pool	start	IP Pool end		Domain Name		DNS Server1	
102	enable	3600	192.168.102.0	255.255.255.0	192.168.102.1		
			192.168.102.25	192.168.102.50		0.0.0.0	

Internal DHCP server configuration(1 entry)

```
default(15)# show dhcp-server 102
```

Internal DHCP server configuration

```
Tag (0 for default)      : 102
State                    : enable
Lease Time (in Seconds)  : 3600
IP Subnet                : 192.168.102.0
Netmask                  : 255.255.255.0
Gateway                  : 192.168.102.1
IP Pool start            : 192.168.102.25
IP Pool end              : 192.168.102.50
Domain Name              :
DNS Server1              : 0.0.0.0
DNS Server2              : 0.0.0.0
Netbios Server1          : 0.0.0.0
Netbios Server2          : 0.0.0.0
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [show dhcp-lease \(352 ページ\)](#)

show gre

設定された GRE トンネル情報を表示します。

構文

`show gre <gre>`

`gre`

詳細な情報を表示する GRE トンネルの名前

コマンド モード

特権 EXEC

デフォルト

なし

用途

GRE トンネル設定に関する詳細を表示するには、**show gre** コマンドを使用します。

使用例

```
default# show gre
```

```
GRE NameRemote External AddressTunnel IP addressTunnel IP NetmaskLocal  
External
```

```
vlan1172.27.0.16212.12.12.12255.255.0.01
```

```
gre1172.27.0.20613.13.13.13255.255.0.02
```

```
GRE Configuration(2 entries)
```

関連コマンド

- [gre \(343 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip dhcp-server \(273 ページ\)](#)
- [ip remote-external-address \(347 ページ\)](#)
- [ip tunnel-ip-address \(348 ページ\)](#)
- [test gre \(355 ページ\)](#)

show dhcp-lease

コントローラをベースとする DHCP サーバの現在の DHCP リース情報を表示します。

構文

```
show dhcp-lease <option> <VLAN>
```

option	表示するパラメータ。統計 (<i>stats</i> パラメータを使用) または VLAN 情報 (<i>vlan</i> オプションを使用) を表示できます。
VLAN	DHCP サーバがアクティブである VLAN の ID。 <i>option</i> フィールドに <i>vlan</i> が指定されている場合のみ使用します。

コマンドモード

特権 EXEC

デフォルト

なし

用途

このコマンドを入力して、すべての DHCP クライアントのリストと割り当てられている IP アドレス、および割り当ての期間を表示します。

使用例

```
default(15)# show dhcp-lease vlan 102
```

関連コマンド

- [dhcp-server \(321 ページ\)](#)
- [show dhcp-server \(349 ページ\)](#)

show vlan

設定されている VLAN 情報を表示します。

構文

```
show vlan
show vlan <vlan>
show vlan ess-profile
```

vlan 詳細情報を表示する VLAN の名前。

コマンド モード

特権 EXEC

デフォルト

すべての設定されている VLAN が表示されます。

用途

特定の VLAN に関する詳細を確認するには、**show vlan** コマンドを使用して VLAN 名を指定します。VLAN と ESS プロファイルのマッピングを表示するには、**show vlan ess-profile** コマンドを使用します。この機能は、マルチキャストが有効である場合に使用します。

使用例

以下のコマンドは、すべての設定されている VLAN を表示します。

```
controller# show vlan
VLAN Configuration   VLAN Name Tag   IP Address      NetMask          Default
Gateway

my_vlan                3   0.0.0.0         0.0.0.0          0.0.0.0
guests                 1   0.0.0.0         0.0.0.0          0.0.0.0
```

以下のコマンドは、guests という VLAN の詳細な設定情報を示します。

```
controller# show vlan guests
VLAN Configuration

VLAN Name                : guests
Tag                       : 1
IP Address                : 0.0.0.0
```

```
Netmask : 0.0.0.0
IP Address of the Default Gateway : 0.0.0.0
Override Default DHCP Server Flag : off
DHCP Server IP Address : 0.0.0.0
DHCP Relay Pass-Through : on
controller#
```

以下のコマンドは使用中のそれぞれの VLAN と ESS のマルチキャスト機能を表示します。

```
controller# show vlan ess-profile
VLAN Name      VLAN Tag ESS Profile      Multicast IPv6  AirFortress
AppleTalk

-----
0      corp-mixed-peap  off      off  off      off
0      corp-mixed-psk   off      off  off      off
0      corp-wpa2peap    off      off  off      off
0      corp-wpa2psk     on       off  off      off
0      corp-wpapeap    off      off  off      off
0      corp-wpapsk     off      off  off      off
0      ph           off      on   off      off
Qa-Vlan-US     30      phone-meru    on      off  off      off
captive-portal-g 9      meru-guest    off     off  off      off
VLAN Ess Bonding(9)
```

関連コマンド [vlan \(356 ページ\)](#)

test gre

GRE トンネルをテストします。

構文

```
test gre <gre_name>  
test gre <gre_name> <ip_address>
```

gre_name	GRE プロファイル名
ip_address	(オプション) トンネルの背後で接続するマシンの IP アドレス。

コマンドモード

特権 EXEC

デフォルト

なし

用途

GRE トンネルのステータスを確認するには、**test gre** コマンドを使用します。このコマンドを実行すると、リモートエンドポイントの IP アドレスが Ping されます。

使用例

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 guest 13.13.13.13
```

関連コマンド

- [gre \(343 ページ\)](#)
- [interface FastEthernet \(264 ページ\)](#)
- [ip dhcp-server \(273 ページ\)](#)
- [ip remote-external-address \(347 ページ\)](#)
- [ip tunnel-ip-address \(348 ページ\)](#)
- [show gre \(351 ページ\)](#)

vlan

VLAN を作成し、VLAN 設定モードを開始します。

構文

```
vlan <name>  
vlan <name> <tag id>
```

name 英数字で 16 文字までの文字列。スペースは使用できません。

tag id VLAN のタグ番号。値は 1 ～ 4,094 になります。

コマンドモード

グローバル設定

デフォルト

なし

用途

FortiWLC (SD) には最大 512 の VLAN を作成できます。

使用例

以下のコマンドは、タグ番号 42 の VLAN に *engineering* という名前を割り当て、VLAN 設定サブモードのヘルプを表示します。

```
controller# vlan engineering tag 42  
controller(config-vlan)# ?  
default          Set various parameters to the default value.  
do               Executes an IOSCLI command.  
end              Save changes, and return to privileged EXEC mode.  
exit             Save changes, and return to global configuration  
mode.  
ip               Configure IP address, gateway, and DHCP server.  
no               Disabling various parameters.  
show             Displays various parameters.
```

関連コマンド

[show vlan \(353 ページ\)](#)

wapi-server

WLAN Authentication and Privacy Infrastructure に使用する IP アドレスを設定します。

構文

wapi-server <ip-address>

ip-address WAPI サーバーの IP アドレス。

コマンド モード

グローバル設定

デフォルト

なし

用途

WLAN Authentication and Privacy Infrastructure (WAPI) は、一部の国のワイヤレス LAN の国家標準です。WAPI 構成では、コントローラに中央認証サービス装置 (ASU) の IP が必要で、これによって、ワイヤレス通信が許可されます。

使用例

```
default(15)# configure terminal  
default(15)(config)# wapi-server 192.168.14.14  
default(15)(config-wapi-server)# end
```

関連コマンド

9 セキュリティ コマンド

セキュリティ コマンドは、WLAN のセキュリティ プロファイルの設定と保守に使用します。

- [8021x-network-initiation](#) (363 ページ)
- [access-list deny](#) (365 ページ)
- [access-list deny import](#) (367 ページ)
- [access-list permit](#) (369 ページ)
- [access-list permit import](#) (371 ページ)
- [administrator guest](#) (374 ページ)
- [allowed-l2-modes](#) (375 ページ)
- [app-visibility-policy](#) (377 ページ)
- [app-visibility-custom-application](#) (379 ページ)
- [sh service-summary Application-Visibility](#) (380 ページ)
- [authentication-mode](#) (382 ページ)
- [authentication-mode global](#) (384 ページ)
- [authentication-type](#) (386 ページ)
- [captive-portal](#) (390 ページ)
- [captive-portal-auth-method](#) (392 ページ)
- [cef](#) (394 ページ)
- [certmgmt delete-ca](#) (397 ページ)
- [certmgmt delete-csr](#) (399 ページ)
- [certmgmt delete-server](#) (400 ページ)
- [certmgmt export-ca](#) (402 ページ)
- [certmgmt export-csr](#) (404 ページ)
- [certmgmt export-server](#) (406 ページ)
- [certmgmt list-ca](#) (408 ページ)
- [certmgmt list-csr](#) (410 ページ)
- [certmgmt list-server](#) (411 ページ)

- [change_mac_state](#) (418 ページ)
- [change_mac_state](#) (418 ページ)
- [change_mac_state](#) (418 ページ)
- [change_mac_state](#) (418 ページ)
- [description](#) (421 ページ)
- [encryption-modes ccmp](#) (422 ページ)
- [encryption-modes ccmp-tkip](#) (423 ページ)
- [encryption-modes tkip](#) (424 ページ)
- [encryption-modes wep128](#) (425 ページ)
- [encryption-modes wep64](#) (426 ページ)
- [firewall-capability](#) (427 ページ)
- [firewall-filter-id](#) (428 ページ)
- [firewall-filter-id-flow](#) (429 ページ)
- [group-rekey interval](#) (430 ページ)
- [import](#) (431 ページ)
- [ip-address](#) (432 ページ)
- [key](#) (433 ページ)
- [key-rotation](#) (434 ページ)
- [local-admin](#) (435 ページ)
- [mac-delimiter](#) (437 ページ)
- [macfiltering](#) (438 ページ)
- [password](#) (439 ページ)
- [password-type](#) (441 ページ)
- [PMK-caching](#) (442 ページ)
- [pmkcaching](#) (443 ページ)
- [port](#) (444 ページ)
- [primary-tacacs-ip](#) (445 ページ)
- [primary-tacacs-port](#) (447 ページ)
- [primary-tacacs-secret](#) (449 ページ)
- [privilege-level](#) (451 ページ)
- [psk key](#) (454 ページ)
- [radius-profile](#) (456 ページ)
- [radius-server primary](#) (458 ページ)
- [radius-server secondary](#) (459 ページ)

- [reauth \(460 ページ\)](#)
- [rekey period \(461 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [secondary-tacacs-port \(464 ページ\)](#)
- [secondary-tacacs-secret \(466 ページ\)](#)
- [security-logging \(468 ページ\)](#)
- [security-profile \(469 ページ\)](#)
- [shared-authentication \(472 ページ\)](#)
- [show aaa statistics \(473 ページ\)](#)
- [show access-list deny \(474 ページ\)](#)
- [show access-list permit \(475 ページ\)](#)
- [show air-shield \(476 ページ\)](#)
- [show arp \(477 ページ\)](#)
- [show authentication-mode \(479 ページ\)](#)
- [show cef \(480 ページ\)](#)
- [show local-admins \(481 ページ\)](#)
- [show radius-profile \(483 ページ\)](#)
- [show security-profile \(485 ページ\)](#)
- [show ssl-server \(488 ページ\)](#)
- [show web \(489 ページ\)](#)
- [ssl-server associate \(493 ページ\)](#)
- [ssl-server captive-portal \(494 ページ\)](#)
- [ssl-server captive-portal-external_URL \(496 ページ\)](#)
- [ssl-server port \(498 ページ\)](#)
- [ssl-server radius-profile \(499 ページ\)](#)
- [static-wep key \(502 ページ\)](#)
- [static-wep key-index \(504 ページ\)](#)
- [tunnel-termination \(505 ページ\)](#)
- [vpn client \(506 ページ\)](#)
- [\(config-vpn-client\) vpn-client-state \(507 ページ\)](#)
- [\(config-vpn-client\) vpn-server-ip \(508 ページ\)](#)
- [\(config-vpn-client\) vpn-server-port \(509 ページ\)](#)
- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) encryption \(511 ページ\)](#)

- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)
- [web custom \(517 ページ\)](#)
- [web login-page \(519 ページ\)](#)

8021x-network-initiation

コントローラから 802.1X 認証が開始可能かどうかを設定します。

構文

```
8021x-network-initiation  
no 8021x-network-initiation
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

802.1X ネットワーク認証は有効になっています。

用途

802.1X ネットワーク認証により、コントローラが 802.1X 認証セッションを開始 できるようになっています。802.1X ネットワーク認証が無効の場合、コントローラはいかなる 802.1X ネットワーク認証も開始できません。

802.1X の初期化を有効にすると、認証側がプロアクティブに EAP-REQUEST パケットをクライアントに送信します。無効にすると、クライアントが EAP-START パケットを認証側 (コントローラ) に送信します。

使用例

以下のコマンドを指定すると、802.1X ネットワーク認証が無効になります。

```
controller(config-security)# no 8021x-network-initiation  
controller(config-security)#
```

関連コマンド

- [allowed-l2-modes \(375 ページ\)](#)
- [radius-profile \(456 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)

802.1x-termination

802.1x-Termination は、IOSCLI と 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。

構文

802.1x-termination
PEAP TTLS
802.1x-termination PEAP

コマンドモード

セキュリティ プロファイル設定

デフォルト

ターミネーションはオフです。

用途

802.1x ターミネーションによって、コントローラの PEAP/TTLS 外部セッションのターミネートが可能になります。内部 MSCHAPv2 802.1x は、バックエンド RADIUS サーバによって処理されます。これは、RADIUS サーバが PEAP または TTLS をサポートしていない場合に便利です。

使用例

以下のコマンドを指定すると、802.1X ターミネートが無効になります。

```
controller(config-security)# no 802.1x-termination (peap/ttls)
controller(config-security)#
```



以下の L2 モードは、PEAP または TTLS 認証プロトコルでのみ、サポートされています。

- 802.1x
 - WPA
 - WPA2
 - 混合
-

access-list deny

ステーションの MAC アドレスを拒否リストに追加し、ネットワークにアクセスするステーションを拒否します。ユーザが特定の MAC に短い説明を追加することもできます。

構文

```
access-list deny <MAC-address>  
(config-acl-deny)# descr <description up to 40 characters>  
(config-acl-deny)# exit  
no access-list deny <MAC-address>  
no access-list deny all
```

MAC-address	ネットワーク アクセスが拒否されるステーションの MAC アドレス。16 進形式 (nn:nn:nn:nn:nn:nn) でなければなりません。最大で 1000 のアドレスを使用できます。
all	all パラメータが指定されると、拒否リストで指定される MAC アドレスはすべて削除されます。

コマンドモード

グローバル設定

デフォルト

なし

用途

MAC アドレスのアクセス リスト フィルタリングは、アクセス リストまたは拒否リストに含まれる指定された 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、WLAN へのアクセスをコントロールします。拒否リストには、WLAN へのアクセスが拒否されるクライアント MAC アドレスのリストが含まれます。

Deny ACL は、RADIUS サーバで許可されているアクセスよりも優先的に適用されます。Deny ACL は、ステーションへのアクセスを即座に拒否するために使用します。管理者は、Deny ACL を使用して、特定のクライアントの振る舞いが異常な場合 (ウイルスに感染している、または他のデバイスを攻撃している) にこれらのクライアントを「ブラックリスト」に追加してそのアクセスを拒否できます。

許可リストあるいは拒否リストを作成する前に、MAC アドレスが許可または拒否される前に、**mac-filter-state** コマンドを使用して ACL を有効にする必要があります。有効にできるリストはいずれか 1 つのみです。許可リストと拒否リストを同時に有効にすることはできません。

no フォームを使用して、ネットワークへのステーション アクセスを拒否するリストにある、1 つあるいはすべてのエントリを削除します。

使用例

以下のコマンドは、MAC アドレス aa:11:aa:22:aa:33 を拒否リストに追加します。そして、DenyStation を MAC の説明として追加し、変更を表示します。

```
MC3200-5072(15)# configure terminal
MC3200-5072(15)(config)# access-list deny aa:11:aa:22:aa:33
MC3200-5072(15)(config-acl-deny)# descr DenyStation
MC3200-5072(15)(config-acl-deny)# end
MC3200-5072(15)# sh access-list deny
```

MAC Address	Description
aa:11:aa:22:aa:33	DenyStation

ACL Deny Access Configuration(1 entry)

```
MC3200-5072(15)#
```

関連コマンド

- [access-list permit \(369 ページ\)](#)
- [show access-list deny \(474 ページ\)](#)

access-list deny import

拒否リストに追加する MAC アドレスのテキスト ファイルをインポートします。

構文

```
access-list deny import <filename>
```

filename

拒否リストに追加する MAC アドレスを含むファイルの名前。ファイル名は UNIX ファイル命名規則に従う必要があります。

コマンドモード

グローバル設定

デフォルト

なし

用途

拒否リストに追加する MAC アドレスのリストがある場合は、すべての MAC アドレスをリストするテキスト ファイルを作成し、そのテキスト ファイルをインポートできます。MAC アドレスをリストしているファイルをインポートすることは、各 MAC アドレスで **access-list deny** コマンドを使うのと同じです。

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
00:0c:e6:bd:01:05
```

テキスト ファイルを作成したら、コントローラ ファイル システムに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、ファイルがコントローラ /images ディレクトリにあることを確認します。

使用例

以下のコマンドは *acl* という名前のテキスト ファイルをインポートし、ファイル内の MAC アドレスを拒否リストに追加します。

```
controller(config)# access-list deny 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  
controller(config)#
```

関連コマンド

- [copy \(73 ページ\)](#)
- [dir \(79 ページ\)](#)
- [show access-list deny \(474 ページ\)](#)

access-list permit

ステーションの MAC アドレスを許可リストに追加し、ネットワークにアクセスするステーションを許可します。ユーザが MAC に短い説明を指定することもできます。

構文

```
access-list permit <MAC-address>  
(config-acl-permit)# descr <description up to 40 characters>  
(config-acl-permit)# exit  
no access-list permit <MAC-address>  
no access-list permit all
```

MAC-address	ネットワーク アクセスが許可されるステーションの MAC アドレス。16 進形式 (nn:nn:nn:nn:nn:nn) でなければなりません。最大で 1000 のアドレスを使用できます。
all	all パラメータが指定されると、許可リストで指定される MAC アドレスはすべて削除されます。

コマンドモード

グローバル設定

デフォルト

なし

用途

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、WLAN へのアクセスをコントロールします。許可リストは、WLAN へのアクセスが許可される MAC アドレスのリストです。拒否リストは、WLAN へのアクセスが拒否される MAC アドレスのリストです。

許可リストあるいは拒否リストを作成する前に、MAC アドレスが許可または拒否される前に、**mac-filter-state** コマンドを使用して ACL を有効にする必要があります。有効にできるリストはいずれか 1 つのみです。許可リストと拒否リストを同時に有効にすることはできません。MAC フィルタリングを非アクティブにすることで、許可および拒否リストを作成し、これらを無効にできます。

no フォームを使用して、ネットワークへのステーション アクセスを許可するリストにある、1 つあるいはすべてのエントリを削除します。

使用例

以下のコマンドは、MAC アドレス 11:11:11:11:22:22:33 を許可リストに追加します。そして、その MAC の説明に「MyClient」を入力し、新しい情報を表示します。

```

MC3200-5072(15)# configure terminal
MC3200-5072(15)(config)# access-list permit 11:11:11:22:22:33
MC3200-5072(15)(config-acl-permit)# descr ?
    <Descr>                (10) Enter the Description to add.

MC3200-5072(15)(config-acl-permit)# descr MyClient
MC3200-5072(15)(config-acl-permit)# end
MC3200-5072(15)# sh access-list permit

MAC Address      Description
11:11:11:22:22:33  MyClient
ACL Allow Access Configuration(1 entry)

MC3200-5072(15)#

```

関連コマンド

- [access-list permit import \(371 ページ\)](#)
- [show access-list permit \(475 ページ\)](#)

access-list permit import

許可リストに追加する MAC アドレスのテキスト ファイルをインポートします。

構文

```
access-list permit import <filename>
```

filename 許可リストに追加する MAC アドレスを含むファイルの名前。ファイル名は UNIX ファイル命名規則に従う必要があります。

コマンドモード

グローバル設定

デフォルト

なし

用途

許可リストに追加する MAC アドレスのリストがある場合は、すべての MAC アドレスをリストするテキスト ファイルを作成し、そのテキスト ファイルをインポートできます。MAC アドレスをリストしているファイルをインポートすることは、各 MAC アドレスで **access-list permit** コマンドを使うのと同じです。

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
00:0c:e6:bd:01:05
```

テキスト ファイルを作成したら、コントローラ / images ディレクトリに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、ファイルがコントローラ ファイル システムにあることを確認します。

使用例

以下のコマンドは *permit_acl* という名前のテキスト ファイルをインポートし、ファイル内の MAC アドレスを許可リストに追加します。

```
controller(config)# access-list permit import permit_acl
00:30:ab:1f:d4:b6
00:40:96:52:27:52
00:04:75:bb:94:48
00:0c:e6:bd:4:05
00:40:05:c5:ca:02
00:04:23:4b:68:6c
00:05:3c:08:c5:9e
```

```
Successfully Added : 7
Duplicate Entries  : 0
Invalid Format      : 0
Entries Processed  : 7
controller(config)#
```

関連コマンド

- [copy \(73 ページ\)](#)
- [dir \(79 ページ\)](#)
- [show access-list permit \(475 ページ\)](#)

mac-filter-state

このコマンドを使用して、以下のいずれかの ACL 環境を選択します。

構文

```
mac-filter-state <acl-environment-state>
```

- deny Deny List Enabled
- disabled ACL Disabled
- permit Permit List Enabled

administrator guest

guest ユーザ アカウントを有効または無効にします。

構文

```
administrator guest enable  
administrator guest disable
```

コマンド モード

グローバル設定

デフォルト

4.0 では無効です。

用途

guest ユーザ アカウントは、4.0 リリースではデフォルトで無効になっています。以下の CLI コマンドを使用すると、有効または無効にできます。

使用例

```
ramecntrl# configure terminal  
ramecntrl(config)# administrator guest enable  
ramecntrl(config)# administrator guest disable  
ramecntrl(config)#
```

関連コマンド

- [captive-portal \(390 ページ\)](#)
- [password \(439 ページ\)](#)
- [password-type \(441 ページ\)](#)

allowed-l2-modes

許可されるレイヤ 2 認証モードを定義します。

構文

```
allowed-l2-modes 802.1x
allowed-l2-modes clear
allowed-l2-modes mixed
allowed-l2-modes mixed_psk
allowed-l2-modes wep
allowed-l2-modes wpa
allowed-l2-modes wpa-psk
allowed-l2-modes wpa2
allowed-l2-modes wpa2-psk}
```

802.1x	IEEE 802.1X 認証モードを許可します。
clear	認証モードを指定しません。
mixed	WPA モードと WPA2 モードの両方をサポートします。
mixed-psk	WPA-PSK モードと WPA2-PSK モードの両方をサポートします。
wep	静的な WEP 認証モードを許可します。
wpa2	Wi-Fi 保護アクセス 2 (WPA2) セキュリティ モードを許可します。
wpa2-psk	WPA2 事前共有キー (PSK) 確立手法を許可します。
wpa	Wi-Fi 保護アクセス (WPA) セキュリティ モードを許可します。
wpa-psk	WPA 事前共有キー (PSK) 確立手法を許可します。

コマンド モード

セキュリティ プロファイル設定

デフォルト

デフォルトで許可されるレイヤ 2 モードは **clear** です。この設定では、強制される認証はありません。

用途

このコマンドによって、セキュリティ プロファイルに割り当てるレイヤ 2 認証モードが決定されます。このコマンドを使用して 802.1X、WEP、WPA2、WPA2-PSK、WPA、または WPA-PSK 認証モードを追加します。



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。

802.1X RADIUS サーバを使用して WPA または WPA2 を実装できない場合、キーを確立する代替手段として WPA2-PSK または WPA-PSK を利用できます。WPA[2]-PSK 実装は、セキュリティ面では脆弱な点があり、小規模なサイトなどに適した方法です。

使用例

以下のコマンドを指定すると、許可される レイヤ 2 セキュリティ モードとして WPA2 が追加されます。

```
controller(config-security)# allowed-l2-modes wpa2  
controller(config-security)#
```

関連コマンド

- [encryption-modes tkip \(424 ページ\)](#)
- [encryption-modes wep128 \(425 ページ\)](#)
- [encryption-modes wep64 \(426 ページ\)](#)
- [radius-profile \(456 ページ\)](#)

app-visibility-policy

このコマンドを使用して、アプリケーション可視化ポリシーの作成を開始します。このコマンドを使用してポリシーを作成した後は、DPI 制御ルールを設定できます。

構文

app-visibility-policy <policy-name>

オプション

オプション	説明
advanced-detection	プロトコル / サブプロトコルの検出を有効化 / 無効化します。
apids	AP を設定します。 アクセス ポイントの追加: apids "<ap-id>: A" アクセス ポイント グループの追加: apids "<ap-group-name>: L"
appids	アプリケーション ID を設定します。 アプリケーションの追加: appids <application-ID>:<type>
description	ポリシー説明を設定します。
essids	ESSID を設定します。 ESS プロファイルの追加: essids <essid-name>
owner	プロファイルのオーナー。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。
policy-order	アプリケーション ポリシーの順序を設定します。ポリシーは、表示されている順序で実行されます。
state	このカスタム アプリケーションのエントリを有効化 / 無効化します。
version	プロファイルのバージョン

使用例

```
controller(15)# show application-visibility policy
```

Name	Enable	Applications	EssIds	AP Groups or APs
11	enable	2:A,3:B		apps1a
3:A				

```

123          enable      *                               appsla
143:A
1232454      enable      2:A,3:B,4:B,5:B,6:A,7:A,8:A,9:A appsla
145:A
ALL          enable      *                               appsla
145:A
a            enable      *                               appsla
123:L,143:A,145:A
rrer         enable      *                               appsla1
1234:L

```

Application Visibility Policy(6)
controller(15)#

凡例

凡例	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 として使用される場合、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。

app-visibility-custom-application

このコマンドを使用して、カスタム アプリケーションのポリシーを作成します。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。

構文

```
(config)# app-visibility-custom-application <policy-name>
(config-app-visibility-custom-application)# description <descriptive
text>
(config-app-visibility-custom-application)# url <app URL to block or
monitor>
```

使用例

```
(config)# app-visibility-custom-application CustomApp-BBC
(config-app-visibility-custom-application)# description "To Monitor BBC
traffic"
(config-app-visibility-custom-application)# url www.bbc.com
(config-app-visibility-custom-application)# exit
# sh application-visibility custom-application
```

Name	Description	ID
CustomApp-BBC	To Monitor BBC traffic	10001

sh service-summary Application-Visibility

使用例 すべてのポリシーを監視するには、このコマンドを使用します。

sh service-summary Application-Visibility

Feature	Type	Name	Value	ValueStr
Application-Visibility	Application	myspace	100	{"util":3006.76,"tx":6943001576,"rx":257651566}
Application-Visibility	Application	amazon_cloud	0	{"util":474.84,"tx":1093389603,"rx":43774451}
Application-Visibility	Application	facebook	0	{"util":184.00,"tx":421673492,"rx":18973696}
Application-Visibility	Application	twitter	0	{"util":164.58,"tx":358628579,"rx":35513363}
... <snipped> ...				
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	Essld	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)

トップ 10 アプリケーションの概要を表示するには、このコマンドを使用します。

mc1500(15)# sh application-visibility application-summary

APPID	Name	Station	Counts	AP	ESS	Tx
Bytes	Rx Bytes	TxRx Bytes		Counts	Counts	
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)

トラフィックのトレンドを表示するには、このコマンドを使用します。

mc1500(15)# sh service-summary-trend Application-Visibility

Feature Value	Type	Name	StartTime	EndTime
Application-Visibility 2009 02:00:00 370191907	Application	myspace	01/17/2009 01:00:00	01/17/2009 02:00:00
Application-Visibility 2009 02:00:00 523131985	Application	amazon_cloud	01/17/2009 01:00:00	01/17/2009 02:00:00
Application-Visibility 2009 02:00:00 221967525	Application	twitter	01/17/2009 01:00:00	01/17/2009 02:00:00
Application-Visibility 2009 02:00:00 220636588	Application	facebook	01/17/2009 01:00:00	01/17/2009 02:00:00
Application-Visibility 2009 02:00:00 113502079	Application	unknown	01/17/2009 01:00:00	01/17/2009 02:00:00
Application-Visibility 2009 02:00:00 106703142	Application	amazon_shop	01/17/2009 01:00:00	01/17/2009 02:00:00
Application-Visibility 2009 02:00:00 58696435	Application	linkedin	01/17/2009 01:00:00	01/17/2009 02:00:00

... .. <snipped>

Application-Visibility 2009 04:00:00 121917540	Application	linkedin	01/17/2009 03:00:00	01/17/2009 04:00:00
Application-Visibility 2009 04:00:00 3187860	Application	youtube	01/17/2009 03:00:00	01/17/2009 04:00:00

Service Data Summary Trend(24 entries)

authentication-mode

ユーザを設定するための認証コマンドのコマンド モード。

構文

```
authentication-mode authentication-type local
authentication-mode authentication-type radius
authentication-mode primary-radius <profile_name>
authentication-mode secondary-radius <profile_name>
authentication-mode no-primary-radius
authentication-mode no-secondary-radius}
```

local	ローカル コントローラがユーザ認証を実行します。キャプティブ ポータル認証の認証タイプがローカルである場合、ローカルの guest ユーザのみが有効になります。セッション タイムアウトとアクティビティ タイムアウトのコントローラ値が使用されます。ローカルがデフォルトで、それが失敗すると、RADIUS 認証がチェックされます。
radius	RADIUS サーバがユーザ認証を実行します。キャプティブ ポータル認証では、RADIUS サーバのユーザだけが有効になります。セッション タイムアウトとアクティビティ タイムアウトの RADIUS サーバ値が使用されます。セッション タイムアウト値が RADIUS サーバに設定されていない場合も、コントローラセッション タイムアウト値が使用されます。RADIUS が失敗すると、ローカル認証はチェックされません。
primary-radius	プライマリ RADIUS サーバ プロファイルの名前を指定します。
secondary-radius	セカンダリ RADIUS サーバ プロファイルの名前を指定します。
profile_name	プライマリまたはセカンダリ RADIUS サーバのプロファイル名です。
no-primary-radius	プライマリ RADIUS サーバの認証を実行しないようにします。
no-secondary-radius	セカンダリ RADIUS サーバの認証を実行しないようにします。

デフォルト

なし

用途

このコマンドを使用して、Web ユーザの認証が行われる場所を決定します。認証を実行するには、ローカルでコントローラを使用 (local 引数を使用) するか、プライマリおよびセカンダリ RADIUS サーバを使用 (radius 引数を使用) するか、両方を使用 (local と radius) します。

radius オプションを使用する場合は、プライマリの名前、オプションでセカンダリの名前、および RADIUS サーバ (profile_name 引数で指定) を使用します。これらのサーバのプロファイル名は、radius-profile コマンドで既に作成されている必要があります。radius オプションを指定する場合は、認証するユーザ ID ごとに、ユーザ名とパスワード、コントローラの IP アドレスを、外部 RADIUS サーバに作成する必要があります。

no-primary-radius または no-secondary-radius 引数を使用して、RADIUS サーバ認証設定を無効にします。

使用例

次のコマンドを使用すると、ローカル コントローラが有効になり、ユーザ認証が実行されます。

```
default(config)# authentication-mode local
```

次のコマンドを使用すると、プライマリ プロファイル名に設定されたプライマリ RADIUS サーバが有効になり、ユーザ認証が実行されます。

```
default(config)# authentication-mode radius
default(config)# authentication-mode radius-profile
default(config)# authentication-mode primary-radius Primary
```

次のコマンドを使用すると、プライマリ RADIUS サーバが無効となり、ユーザ認証を実行できなくなり、認証をローカル コントローラに返します。

```
default(config)# authentication-mode no-radius-profile
default(config)# authentication-mode local
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [show authentication-mode \(479 ページ\)](#)

authentication-mode global

管理者を設定するための認証コマンドのコマンドモード。

構文

authentication-mode global

コマンドモード

認証モード。これは、設定の下の別のコマンドモードです。

デフォルト

なし

用途

configure terminal を入力してから **authentication-mode global** を入力すると、(config-auth-mode) がプロンプトに追加され、[authentication-type \(386 ページ\)](#) コマンドを使用できるようになります。

使用例

次のコマンドは、プライマリとセカンダリの認証モードを RADIUS に設定し、RADIUS シークレットを提供します。

```
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-ip 172.18.1.3
ramcntrl(0)(config-auth-mode)# primary-radius-secret RadiusP
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)#
```

関連コマンド

- [authentication-type \(386 ページ\)](#)
- [show authentication-mode \(479 ページ\)](#)

authentication-type

コントローラ ユーザ ログインの認証タイプ (認証モードの) を設定します。

構文

```
authentication-type local
authentication-type radius
authentication-type primary-radius <profile_name>
authentication-type secondary-radius <profile_name>
authentication-type no-primary-radius
authentication-type no-secondary-radius}
```

local (default)	ローカル コントローラがユーザ認証を実行します。認証タイプがローカルである場合、ローカルの guest ユーザのみが有効になります。セッション タイムアウトとアクティビティ タイムアウトのコントローラ値が使用されます。ローカルがデフォルトで、それが失敗すると、RADIUS 認証がチェックされます。
radius	RADIUS サーバがユーザ認証を実行します。RADIUS サーバのユーザのみが有効になります。セッション タイムアウトとアクティビティ タイムアウトの RADIUS サーバ値が使用されます。セッション タイムアウト値が RADIUS サーバに設定されていない場合も、コントローラ セッション タイムアウト値が使用されます。RADIUS が失敗すると、ローカル認証はチェックされません。
primary-radius	プライマリ RADIUS サーバ プロファイルの名前を指定します。
secondary-radius	セカンダリ RADIUS サーバ プロファイルの名前を指定します。
profile_name	プライマリまたはセカンダリ RADIUS サーバのプロファイル名です。
no-primary-radius	プライマリ RADIUS サーバの認証を実行しないようにします。
no-secondary-radius	セカンダリ RADIUS サーバの認証を実行しないようにします。

コマンドモード

設定モード

デフォルト

なし

用途

このコマンドを使用し、Web ユーザの認証が行われる場所を決定します。認証を実行するには、ローカルでコントローラを使用 (local 引数を使用) するか、プライマリおよびセカン

ダリ RADIUS サーバを使用 (**radius** 引数を使用) するか、両方を使用 (**local** と **radius**) します。

radius オプションを使用する場合は、プライマリの名前、オプションでセカンダリの名前、および RADIUS サーバ (*profile_name* 引数で指定) を使用します。これらのサーバのプロファイル名は、**radius-profile** コマンドで既に作成されている必要があります。

radius オプションを指定する場合は、認証するユーザ ID ごとに、ユーザ名とパスワード、コントローラの IP アドレスを、外部 RADIUS サーバに作成する必要があります。

No-primary-radius-primary-radius または **no-secondary-radius** 引数を使用して、RADIUS サーバ認証設定を無効にします。

使用例

次のコマンドは、ローカル コントローラ認証を設定します。

```
default(config)# authentication-mode local
```

次のコマンドを使用すると、プライマリ プロファイル名に設定されたプライマリ RADIUS サーバが有効になり、ユーザ認証が実行されます。

```
default(config)# authentication-mode radius
default(config)# authentication-mode radius-profile
default(config)# authentication-mode primary-radius Primary
```

次のコマンドを使用すると、プライマリ RADIUS サーバが無効となり、ユーザ認証を実行できなくなり、認証をローカル コントローラに返します。

```
default(config)# authentication-mode no-radius-profile
default(config)# authentication-mode local
```

次のコマンドは、プライマリとセカンダリの認証モードを RADIUS に設定し、RADIUS シークレットを提供します。

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type radius
ramcntrl(0)(config-auth-mode)# primary-radiusprimary-
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-radiussecondary-
radius-ip secondary-radius-port secondary-radius-secret
```

8

(6-8)

Operator is the lowest authentication level and also the default. Operators can see statistics and results but cannot make any configuration changes.

5

(3-5)

Administrators can also do general configuration changes, but cannot upgrade APs or controllers, nor can they upgrade FortiWLC (SD) versions using

Telnet. They cannot configure an NMS server, NTP server, change the system password, date or time (all CLI). They cannot create local admins, a new feature in release 4.1, nor can they set the authentication mode for a controller (GUI and CLI). Administrators cannot add or remove licensing.

2

(0-2)

SuperUser administrators can perform all configurations on the controller.

They are the only ones who can upgrade APs or controllers and they can upgrade FortiWLC (SD) versions using Telnet. They can configure an NMS server, NTP server, system password, date and time (all CLI). They can also create other admins and set the authentication mode for a controller (GUI and

CLI). Superuser は、ライセンスを追加、削除できます。

Radius Authentication

© 2015 Fortinet, Inc. Authentication 141

4.1 Beta

```
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)#
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [show authentication-mode \(479 ページ\)](#)

captive-portal

キャプティブ ポータル機能を有効にします。

構文

```
captive-portal disabled
captive-portal webauth
no captive-portal
```

disabled キャプティブ ポータル機能を無効にします。

webauth キャプティブ ポータルで WebAuth を有効にします。

コマンドモード

セキュリティ プロファイル設定

デフォルト

キャプティブ ポータルは無効になっています。

用途

このコマンドを使用して、セキュリティ プロファイルにおけるキャプティブ ポータル Webauth を有効にします。キャプティブ ポータルが有効である場合、ステーションを ESS に関連付ける際に、ユーザは WebAuth ログイン ページ (キャプティブ ポータル) に移動します。

キャプティブ ポータルで Webauth が有効になっていると、クライアント ステーションの認証と承認が完了するまでは、HTTPS プロトコルと Secure Socket Layer (SSL) により、暗号化ログイン インターチェンジが提供されます。RADIUS 認証サーバは、ユーザ アクセスを決定するバックエンドとして使用されます。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、ステーションはキャプティブ ポータル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 ポータルから離れて、WLAN に入ることができます。

キャプティブ ポータル機能を無効にするには、**no captive-portal** または **captive-portal disabled** を使用します。

使用例

以下のコマンドを指定すると、セキュリティ プロファイルで WebAuth キャプティブ ポータルが有効になります。

```
default# configure terminal
default(config)# security-profile web_auth
```



```
default(config-security)# captive-portal webauth
default(config-security)# radius-server primary main-auth
default(config-security)# exit
default(config)# exit
```

関連コマンド

- [radius-server primary \(458 ページ\)](#)
- [ssl-server radius-profile \(499 ページ\)](#)
- [captive-portal-auth-method \(392 ページ\)](#)

captive-portal-auth-method

認証を、フォーティネットの内部 (デフォルト) またはサードパーティ ソリューションの外部に設定します。

構文

```
captive-portal-auth-method internal  
captive-portal-auth-method external
```

コマンド モード

設定モード、セキュリティ モード

デフォルト

フォーティネット キャプティブ ポータル

用途

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。CLI コマンド **captive-portal-auth-method** を使用して、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。CLI コマンド **ssl-server captive-portal-external-URL** を使用して、キャプティブ ポータル設定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。そして、コマンド **change_mac_state** で、キャプティブ ポータル ボックスの URL を指定します。

使用例

以下の例では、次の 2 つのタスクを完了することで、CLI でサードパーティのキャプティブ ポータルを設定します。

CLI コマンド **captive-portal-auth-method** を使用して、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。たとえば、次のように入力します。

```
controller1# configure terminal  
controller1(config)# security-profile CPExternal  
controller1(config-security)# captive-portal-auth-method  
external internal  
controller1(config-security)# captive-portal-auth-method ?  
<captivePortAuthMethod> Configure captive portal authentication method.
```

```
external external
internal internal
controller1(config-security)# captive-portal-auth-method external
```

CLI コマンド **ssl-server captive-portal-external-URL** を使用して、キャプティブ ポータル設定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。そして、コマンド **change_mac_state** で、キャプティブ ポータル ボックスの URL を指定します。たとえば、次のように入力します。

```
controller1# configure terminal
controller1(config)# ssl-server ca
captive-portal captive-portal-external-URL
controller1(config)# ssl-server captive-portal-external-URL
controller1(config)# exit
controller1# change_mac_state ?
<ip-address> Enter the Client IP Address.
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 on ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 on ftp_only
Configure a Radius Server for Captive Portal Authentication
© 2010 Fortinet, Inc. Captive Portals for Temporary Users 169
4.1 Beta
<CR>
controller1# change_mac_state 172.18.19.14 on ftp_only
controller1#
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 off ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 off
controller1
```

関連コマンド [change_mac_state \(418 ページ\)](#)

cef

通常イベント フォーマット ログイング機能を設定します。

構文

```
cef server-ip<hostname> <port>
cef server-ip<IP address> <port>
cef server-ip<hostname>
cef server-ip<IP address>
cef enable
cef disable
```

- hostname リモート サーバの IP アドレスまたはホスト名です。
- ip address
- port 使用するサーバ ポートです。デフォルトでは、514 が使用されます。

コマンドモード

グローバル設定

デフォルト

無効がデフォルトです。

用途

このコマンドを使用し、システム ログ メッセージを通常イベント フォーマット ログイングに変換し、標準システム ログ フォーマットの他、ArcSight ログイング サーバとの相互運用性をサポートします。

この機能を有効にする前に、ログイングが実行される ArcSight サーバのホスト名または IP アドレスを設定します。

以下に、システム ログ メッセージをトリガするイベント、およびメッセージに含まれる情報を示します。

システム ログ メッセージをトリガするイベント	システム ログ メッセージ内に示される情報
ワイヤレスの関連付け	MAC アドレス、SSID、AP 番号、BSSID、およびタイム スタンプ
1x 認証試行	ユーザ名、MAC アドレス、および AP 番号
1x 認証失敗	ユーザ名、MAC アドレス、および AP 番号

システム ログ メッセージを トリガするイベント	システム ログ メッセージ内に示される情報
記録するように設定されている Qos およびファイアウォール ルールについては、ネットワーク トラフィックで実行されるアクションが許可または拒否されたか。	MAC アドレス、IP アドレス、および AP MAC アドレス
コントローラ管理インターフェイスへのすべてのアクセス	タイムスタンプ、IP アドレス
不正 AP の検出	不正 BSSID、AP 番号
コントローラの起動	タイムスタンプ
AP 停止	AP 番号、タイムスタンプ
AP 起動	AP 番号、タイムスタンプ
コントローラの状態のトランジション (マスタ、スレーブ)	

デバイス クラス イベント ID は以下のとおりです。

番号	イベント	DeviceEventClassId
1	ワイヤレスの関連付け	ワイヤレスの関連付け
2	1x 認証試行	802.1x 認証試行
3	1x 認証失敗	802.1x 認証失敗
4	記録するように設定されている Qos およびファイアウォール ルールについては、ネットワーク トラフィックで実行されるアクションが許可または拒否されたか。	ネットワーク トラフィック
5	コントローラ管理インターフェイスへのすべてのアクセス	コントローラ アクセス
6	不正 AP の検出	不正 AP の検出

番号	イベント	DeviceEventClassId
7	コントローラの起動	コントローラの起動
8	AP 起動	AP 起動
9	AP 停止	AP 停止
10	コントローラの状態のトランジション (マスタ、スレーブ)	コントローラ状態変更
11	他のすべてのログ メッセージ	通常のフォーティネット イベント

使用例

次は、cef ロギング サーバを 192.18.100.100 に設定し、cef を有効にします。

```
default(config)# cef server-ip 192.168.100.100 255.255.255.0
default(config)# cef enable
```

次の例は、CEF ロギング オプションを表示し、さらに、現在の CEF 設定を表示します。

```
WiFi36# configure terminal
WiFi36(config)# cef ?
disable                Disables Common Event Format Logging Feature.
enable                 Enables Common Event Format Logging Feature.
server-ip              Enter Server Details
WiFi36(config)# exit
WiFi36#
WiFi36# show cef
CEF Logging is disabled
CEF Logging Host is not configured
WiFi36#
```

関連コマンド

[show cef \(480 ページ\)](#)

certmgmt delete-ca

コントローラ Trusted Root CA 証明書を削除します。

構文

```
certmgmt delete-ca <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

`certmgmt delete-ca` コマンドを使用し、Trusted Root CA 証明書をコントローラの証明書リポジトリから削除します。

証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

Trusted Root CA 証明書は、信頼のあるサードパーティの証明書です。証明書をサポートする任意のクライアントまたはサーバソフトウェアは、信頼の置ける Root CA 証明書を保守します。これらの CA 証明書は、ソフトウェアが他のどの証明書を認証できるかを決定します。ソフトウェアは、コントローラの Trusted Root CA 証明書リポジトリにある CA のうち 1 つが発行した証明書のみを認証します。

使用例

次のコマンドは、ca1 という名前の Trusted Root CA 証明書を削除します。

```
controller# certmgmt delete-ca ca1
controller#
```

関連コマンド

- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)
- [certmgmt view-ca \(413 ページ\)](#)

- [certmgmt view-csr](#) (415 ページ)
- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt delete-csr

保留中の証明書署名要求 (CSR) を削除します。

構文

```
certmgmt delete-csr <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt delete-csr コマンドを使用し、Web UI を使用して作成された保留中の証明書署名要求 (CSR) を削除します。保留中の CSR は、署名および署名済み証明書取得のために CA に送信されたファイルです。署名済みの証明書が戻されるまでは、CSR のステータスは保留中だとみなされます。

使用例

次のコマンドは、ca1 という名前の証明書の保留中 CSR を削除します。

```
controller# certmgmt delete-csr ca1
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)
- [certmgmt view-ca \(413 ページ\)](#)
- [certmgmt view-csr \(415 ページ\)](#)
- [certmgmt view-server \(416 ページ\)](#)
- [change_mac_state \(418 ページ\)](#)

certmgmt delete-server

コントローラ サーバ証明書を削除します。

構文

```
certmgmt delete-server <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt delete-server コマンドを使用し、サーバ証明書をコントローラの証明書リポジトリから削除します。この CLI コマンドでサーバ証明書を削除できますが、サーバ証明書の作成とコントローラへのインポートは、Web UI からのみ可能です。

サーバ証明書は、PKI 目的のために様々なアプリケーションで使用されています。サーバ証明書のユーザは、プライベート キーおよび証明書要求を作成するプロセスを開始します。この証明書要求は署名のため CA/RA に送信されます。CA が証明書要求を処理すると、証明書はコントローラの証明書リポジトリに保存されます。

使用例

次のコマンドは、sc1 という名前のサーバ証明書を削除します。

```
controller# certmgmt delete-server sc1
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)

- [certmgmt view-ca](#) (413 ページ)
- [certmgmt view-csr](#) (415 ページ)
- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt export-ca

保留中のコントローラ Trusted Root CA 証明書をエクスポートします。

構文

```
certmgmt export-ca <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt export-ca コマンドを使用し、Trusted Root CA 証明書をコントローラの証明書リポジトリから別の場所へとエクスポートします。

証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

Trusted Root CA 証明書は、信頼のあるサードパーティの証明書です。証明書をサポートする任意のクライアントまたはサーバソフトウェアは、信頼の置ける Root CA 証明書を保守します。これらの CA 証明書は、ソフトウェアが他のどの証明書を認証できるかを決定します。ソフトウェアは、コントローラの Trusted Root CA 証明書リポジトリにある CA のうち 1 つが発行した証明書のみを認証します。この CLI コマンドでサーバ証明書をエクスポートできますが、サーバ証明書のコントローラへのインポートは、Web UI からのみ可能です。

使用例

次のコマンドは、ca1 という名前の Trusted Root CA 証明書をエクスポートします。

```
controller# certmgmt export-ca ca1
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)

- [certmgmt list-server](#) (411 ページ)
- [certmgmt view-ca](#) (413 ページ)
- [certmgmt view-csr](#) (415 ページ)
- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt export-csr

保留中の証明書署名要求 (CSR) をエクスポートします。

構文

```
certmgmt export-csr <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt export-csr コマンドを使用し、保留中の CSR を別の場所にエクスポートします。証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

保留中の CSR は、署名および署名済み証明書取得のために CA に送信されたファイルです。署名済みの証明書が戻されるまでは、CSR のステータスは保留中だとみなされます。

使用例

次のコマンドは、ca1 という名前の CSR をエクスポートします。

```
controller# certmgmt export-csr ca1
```

```
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)
- [certmgmt view-ca \(413 ページ\)](#)
- [certmgmt view-csr \(415 ページ\)](#)
- [certmgmt view-server \(416 ページ\)](#)

- [change_mac_state](#) (418 ページ)

certmgmt export-server

コントローラ サーバ証明書をエクスポートします。

構文

```
certmgmt export-server <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt export-server コマンドを使用し、サーバ証明書をコントローラの証明書リポジトリから別の場所へとエクスポートします。

サーバ証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

サーバ証明書は、PKI 目的のために様々なアプリケーションで使用されています。サーバ証明書のユーザは、プライベート キーおよび証明書要求を作成するプロセスを開始します。この証明書要求は署名のため CA/RA に送信されます。CA が証明書要求を処理すると、証明書はコントローラの証明書リポジトリに保存されます。

使用例

次のコマンドは、sc1 という名前のサーバ証明書をエクスポートします。

```
controller# certmgmt export-server sc1
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)

- [certmgmt list-server](#) (411 ページ)
- [certmgmt view-ca](#) (413 ページ)
- [certmgmt view-csr](#) (415 ページ)
- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt list-ca

コントローラの Trusted Root CA 証明書を一覧表示します。

構文

`certmgmt list-ca`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`certmgmt list-ca` コマンドを使用し、Trusted Root CA 証明書をコントローラの証明書リポジトリに一覧表示します。

証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

Trusted Root CA 証明書は、信頼のあるサードパーティの証明書です。証明書をサポートする任意のクライアントまたはサーバソフトウェアは、信頼の置ける Root CA 証明書を保守します。これらの CA 証明書は、ソフトウェアが他のどの証明書を認証できるかを決定します。ソフトウェアは、コントローラの Trusted Root CA 証明書リポジトリにある CA のうち 1 つが発行した証明書のみを認証します。

使用例

次のコマンドは、Trusted Root CA 証明書を一覧表示します。

```
controller# certmgmt list-ca
```

```
Trusted Root CA Certificates
```

```
-----
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)

- [certmgmt view-ca](#) (413 ページ)
- [certmgmt view-csr](#) (415 ページ)
- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt list-csr

保留中の証明書署名要求 (CSR) を一覧表示します。

構文

certmgmt list-csr

コマンドモード

特権 EXEC

デフォルト

なし

用途

certmgmt list-csr コマンドを使用し、保留中の CSR を一覧表示します。証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

保留中の CSR は、署名および署名済み証明書取得のために CA に送信されたファイルです。署名済みの証明書が戻されるまでは、CSR のステータスは保留中だとみなされます。

使用例

次のコマンドは、ca1 という名前の CSR をエクスポートします。

```
controller# certmgmt list-csr
Pending CSRs
-----
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)
- [certmgmt view-ca \(413 ページ\)](#)
- [certmgmt view-csr \(415 ページ\)](#)
- [certmgmt view-server \(416 ページ\)](#)
- [change_mac_state \(418 ページ\)](#)

certmgmt list-server

コントローラのサーバ証明書を一覧表示します。

構文

certmgmt list-server

コマンドモード

特権 EXEC

デフォルト

なし

用途

certmgmt list-server コマンドを使用して、コントローラの証明書リポジトリ内のコントローラのサーバ証明書 (GUI で作成され、インポートされたもの) を一覧表示します。

サーバ証明書は、PKI 目的のために様々なアプリケーションで使用されています。サーバ証明書のユーザは、プライベート キーおよび証明書要求を作成するプロセスを開始します。この証明書要求は署名のため CA/RA に送信されます。CA が証明書要求を処理すると、証明書はコントローラの証明書リポジトリに保存されます。

使用例

次のコマンドは、コントローラのサーバ証明書を一覧表示します。

```
controller# certmgmt list-server
```

```
Server Certificates
```

```
-----
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt view-ca \(413 ページ\)](#)
- [certmgmt view-csr \(415 ページ\)](#)

- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt view-ca

コントローラ Trusted Root CA 証明書を表示します。

構文

```
certmgmt view-ca <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt view-ca コマンドを使用し、Trusted Root CA 証明書の詳細を表示します。始めに Web UI を使用して証明書を作成しコントローラにインポートする必要があります。

Trusted Root CA 証明書は、信頼のあるサードパーティの証明書です。証明書をサポートする任意のクライアントまたはサーバソフトウェアは、信頼の置ける Root CA 証明書を保守します。これらの CA 証明書は、ソフトウェアが他のどの証明書を認証できるかを決定します。ソフトウェアは、コントローラの Trusted Root CA 証明書リポジトリにある CA のうち 1 つが発行した証明書のみを認証します。

使用例

次のコマンドは、ca1 という名前の Trusted Root CA 証明書を表示します。

```
controller# certmgmt view-ca ca1
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)
- [certmgmt view-csr \(415 ページ\)](#)

- [certmgmt view-server](#) (416 ページ)
- [change_mac_state](#) (418 ページ)

certmgmt view-csr

保留中の証明書署名要求 (CSR) を表示します。

構文

```
certmgmt view-csr <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt view-csr コマンドを使用し、Web UI を使用して作成された保留中の 証明書署名要求 (CSR) の詳細を表示します。保留中の CSR は、署名および署名済み証明書取得のために CA に送信されたファイルです。署名済みの証明書が戻されるまでは、CSR のステータスは保留中だとみなされます。

使用例

次のコマンドは、ca1 という名前の証明書の保留中 CSR を表示します。

```
controller# certmgmt view-csr ca1
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)
- [certmgmt list-csr \(410 ページ\)](#)
- [certmgmt list-server \(411 ページ\)](#)
- [certmgmt view-ca \(413 ページ\)](#)
- [certmgmt view-server \(416 ページ\)](#)
- [change_mac_state \(418 ページ\)](#)

certmgmt view-server

コントローラ サーバ証明書を表示します。

構文

```
certmgmt view-server <cert-alias>
```

cert-alias Web UI を使用して作成された証明書エイリアスの名前です。

コマンド モード

特権 EXEC

デフォルト

なし

用途

certmgmt view-server コマンドを使用し、コントローラの証明書リポジトリ内のサーバ証明書を表示します。

サーバ証明書は、Web UI を使用してのみ作成およびコントローラへのインポートが可能です。

サーバ証明書は、PKI 目的のために様々なアプリケーションで使用されています。サーバ証明書のユーザは、プライベート キーおよび証明書要求を作成するプロセスを開始します。この証明書要求は署名のため CA/RA に送信されます。CA が証明書要求を処理すると、証明書はコントローラの証明書リポジトリに保存されます。

使用例

次のコマンドは、sc1 と名付けられたサーバ証明書を表示します。

```
controller# certmgmt view-server sc1
controller#
```

関連コマンド

- [certmgmt delete-ca \(397 ページ\)](#)
- [certmgmt delete-csr \(399 ページ\)](#)
- [certmgmt delete-server \(400 ページ\)](#)
- [certmgmt export-ca \(402 ページ\)](#)
- [certmgmt export-csr \(404 ページ\)](#)
- [certmgmt export-server \(406 ページ\)](#)
- [certmgmt list-ca \(408 ページ\)](#)

- [certmgmt list-csr](#) (410 ページ)
- [certmgmt list-server](#) (411 ページ)
- [certmgmt view-ca](#) (413 ページ)
- [certmgmt view-csr](#) (415 ページ)
- [change_mac_state](#) (418 ページ)

change_mac_state

captive-portal-auth-method と併用することで、サードパーティのキャプティブ ポータル ソリューションの URL を指示します。

構文

```
change_mac_state <IP address> on <filter ID>
change_mac_state <IP address> off
```

コマンドモード

設定モード、セキュリティ モード

デフォルト

フォーティネット キャプティブ ポータル

用途

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。CLI コマンド **captive-portal-auth-method** を使用して、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。CLI コマンド **ssl-server captive-portal-external-URL** を使用して、キャプティブ ポータル設定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。そして、コマンド **change_mac_state** で、キャプティブ ポータル ボックスの URL を指定します。

使用例

以下の例では、次の 2 つのタスクを完了することで、CLI でサードパーティのキャプティブ ポータルを設定します。

CLI コマンド **captive-portal-auth-method** を使用して、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。たとえば、次のように入力します。

```
controller1# configure terminal
controller1(config)# security-profile CPExternal
controller1(config-security)# captive-portal-auth-method
external internal
controller1(config-security)# captive-portal-auth-method ?
<captivePortAuthMethod> Configure captive portal authentication method.
```

```
external external
internal internal
controller1(config-security)# captive-portal-auth-method external
```

CLI コマンド **ssl-server captive-portal-external-URL** を使用して、キャプティブ ポータル設定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。そして、コマンド **change_mac_state** で、キャプティブ ポータル ボックスの URL を指定します。たとえば、次のように入力します。

```
controller1# configure terminal
controller1(config)# ssl-server ca
captive-portal captive-portal-external-URL
controller1(config)# ssl-server captive-portal-external-URL
controller1(config)# exit
controller1# change_mac_state ?
<ip-address> Enter the Client IP Address.
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 on ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 on ftp_only
Configure a Radius Server for Captive Portal Authentication
© 2010 Fortinet, Inc. Captive Portals for Temporary Users 169
4.1 Beta
<CR>
controller1# change_mac_state 172.18.19.14 on ftp_only
controller1#
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 off ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 off
controller1
```

関連コマンド [captive-portal-auth-method \(392 ページ\)](#)

clear certificates

未割り当ての PEM および PFX 証明書ファイルを削除します。

構文

`clear certificates`

コマンド モード

特権 EXEC

デフォルト

なし

用途

`clear certificates` コマンドを使用して、使用されていない .pem および .pfx 証明書ファイルを削除します。これらは、Web UI を使用してシステムにインポートされた証明書ファイルですが、アプリケーションにはまだ割り当てられていません。

使用例

このコマンドは、使用されていない証明書をすべてクリアします。

```
controller# clear certificates
```

関連コマンド

[certmgmt delete-server \(400 ページ\)](#)

description

RADIUS プロファイル サーバについて説明します。

構文

description <text>

text RADIUS プロファイル サーバについて説明します。説明文の文字数は最大で 128 文字です。二重引用符で囲んで入力しなければなりません。

コマンドモード

RADIUS プロファイル設定

デフォルト

なし

用途

このコマンドを使用し、RADIUS プロファイルを説明する情報を指定します。説明文を二重引用符で囲んで入力します。使用可能な文字数は最大で 128 文字です。**show radius-profile** コマンドをプロファイル引数と一緒に使用して説明を表示します。

使用例

```
controller(config-radius)# description
"This server is located on the Second floor of building G in the NW server
area."
controller(config-radius)# do show radius-profile RAD1
RADIUS Profile Table
RADIUS Profile Name      :RAD1
Description               :This server is located on the Second floor of
building G in the NW server area.
RADIUS IP                 :192.168.100.1
RADIUS Secret             :*****
RADIUS Port               :1812
RADIUS VLAN Name          :
MAC Address Delimiter     :none
Password Type             : shared-secret
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [show radius-profile \(483 ページ\)](#)

encryption-modes ccmp

セキュリティ プロファイルの暗号スイートとして CCMP を設定します。

構文

```
encryption-modes ccmp  
no encryption-modes ccmp
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

暗号は設定されていません。

用途

このコマンドを使用して、WPA2 セキュリティ プロファイルの暗号スイートを CCMP に設定します。CCMP は、WPA2 設定で使用する暗号化標準です。

使用例

以下のコマンドにより、暗号化モードが CCMP に設定されます。

```
controller(config-security)# encryption-modes ccmp  
controller(config-security)#
```

関連コマンド

- [8021x-network-initiation \(363 ページ\)](#)
- [radius-profile \(456 ページ\)](#)

encryption-modes ccmp-tkip

セキュリティ プロファイルの暗号スイートとして CCMP および TKIP を設定します。

構文

```
encryption-modes ccmp-tkip  
no encryption-modes ccmp-tkip
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

暗号は設定されていません。

用途

このコマンドを使用して、CCMP および TKIP の両方を暗号化設定することにより、セキュリティ プロファイルでの WPA および WPA2 互換性の暗号スイートをセキュリティ プロファイル内に設定します。

使用例

以下のコマンドにより、暗号化モードが CCMP/TKIP に設定されます。

```
controller(config-security)# encryption-modes ccmp-tkip  
controller(config-security)#
```

関連コマンド

- [8021x-network-initiation \(363 ページ\)](#)
- [encryption-modes ccmp \(422 ページ\)](#)
- [encryption-modes tkip \(424 ページ\)](#)
- [radius-profile \(456 ページ\)](#)

encryption-modes tkip

セキュリティ プロファイルの暗号スイートとして TKIP を設定します。

構文

```
encryption-modes tkip  
no encryption-modes tkip
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

暗号は設定されていません。

用途

Temporal Key Integrity Check (TKIP) のセキュリティ プロファイル用の暗号スイートを設定するために、このコマンドを使用します。WEP の脆弱性を解消するための Wi-Fi Protection Access (WPA) ソリューションの一環として、TKIP では、暗号化キーのサイズが拡張され、使用するキーの数が増加しています。また、メッセージの整合性チェック機構も作成されています。ワイヤレス データ保護のために実装する必要がある WPA のその他のソリューションとして、アクセス コントロールと 802.1X により提供されているキー ローテーションがあります。これは、標準の拡張認証プロトコルタイプのいずれかを使用します (802.1X セットアップについては [radius-profile](#) を参照)。

TKIP は、128 ビットのキーと 64 ビットの Initialization Vector (IV) を使用するレイヤ 2 の暗号化アルゴリズムです。TKIP は、RC4 アルゴリズムを対称キーと一緒に使用して、暗号化テキストを生成します。対称キーは、テキストの暗号化と解読に使用され、802.1X EAP ソリューションも実装されている場合は、AP またはユーザのステーションに自動的に配信できます。TKIP では、メッセージ整合性チェック (MIC) が使用され、パケットの転送中に変更されていないことが確認されます。

使用例

以下のコマンドにより、暗号化モードが TKIP に設定されます。

```
controller(config-security)# encryption-modes tkip  
controller(config-security)#
```

関連コマンド

- [8021x-network-initiation \(363 ページ\)](#)
- [radius-profile \(456 ページ\)](#)

encryption-modes wep128

セキュリティ プロファイルの暗号スイートとして WEP-128 を設定します。

構文

```
encryption-modes wep128  
no encryption-modes wep128
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

暗号スイートは設定されていません。

用途

このコマンドを使用して、セキュリティ プロファイルの暗号スイートで WEP-128 (WEP2 とも呼ばれます) を使用するようにします。WEP-128 は、104 ビットキーと 24 ビットの Initialization Vector (IV) を使用するレイヤ 2 暗号化アルゴリズムです。WEP2 は、RC4 アルゴリズムを対称キーと一緒に使用して、暗号化テキストを生成します。対称キーはテキストの暗号化と解読のために使用されます。自動生成されますが、AP またはユーザ ステーションに手動で配信されます。生成されたキーは、管理者がキーを変更するまで使用されます。また、802.1X プロトコルも使用して、自動的にキーを生成する、WEP よりもさらにセキュアな「動的 WEP」環境にするようにセキュリティ プロファイルを設定できます。

使用例

以下のコマンドにより、暗号化モードが WEP-128 に設定されます。

```
controller(config-security)# encryption-modes wep128  
controller(config-security)#
```

関連コマンド

- [8021x-network-initiation \(363 ページ\)](#)
- [allowed-l2-modes \(375 ページ\)](#)
- [encryption-modes wep64 \(426 ページ\)](#)
- [rekey period \(461 ページ\)](#)
- [static-wep key \(502 ページ\)](#)

encryption-modes wep64

セキュリティ プロファイルの暗号スイートとして WEP-64 を設定します。

構文

```
encryption-modes wep64
no encryption-modes wep64
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

暗号スイートは設定されていません。

コマンド モード

このコマンドを使用すると、セキュリティ プロファイルの暗号スイートで、WEP-128 よりも暗号化レベルが低いフォームである WEP-64 を使用するように設定されます。WEP-64 (WEP または WEP40 と呼ばれます) は、40 ビットキーと 24 ビットの Initialization Vector (IV) を使用するレイヤ 2 暗号化アルゴリズムです。WEP は RC4 アルゴリズムと対称キーを使用して、暗号化されたテキストを作成します。対称キーはテキストの暗号化と解読のために使用されます。自動生成されますが、AP またはユーザ ステーションに手動で配信されます。生成されたキーは、管理者がキーを変更するまで使用されます。また、802.1X プロトコルも使用して、自動的にキーを生成する、WEP よりもさらにセキュアな「動的 WEP」環境にするようにセキュリティ プロファイルを設定できます。

使用例

以下のコマンドにより、暗号化モードが WEP-64 に設定されます。

```
controller(config-security)# encryption-modes wep64
controller(config-security)#
```

関連コマンド

- [8021x-network-initiation \(363 ページ\)](#)
- [allowed-l2-modes \(375 ページ\)](#)
- [encryption-modes wep128 \(425 ページ\)](#)
- [rekey period \(461 ページ\)](#)
- [static-wep key \(502 ページ\)](#)

firewall-capability

Selects the configuration source for per-user firewall.

構文

```
firewall-capability configured
firewall-capability none
firewall-capability radius-configured
```

コマンドモード

セキュリティ プロファイル設定

デフォルト

ファイアウォール機能は **none** に設定されています。

用途

ユーザごとのファイアウォールでは、ユーザ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、ユーザごとのネットワークの使用法を制御します。ユーザごとのファイアウォールのサポートは、RADIUS が返す *filter-id* 属性、またはユーザが ESS プロファイル設定の一部として設定する *firewall filter-id* パラメータを基準にして実装されます。

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* 属性は、ファイアウォール タグとして使用され、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 ポリシーを適用することで、アクションが実行されます。

RADIUS 設定がない場合には、ESS プロファイルで設定されているファイアウォール タグをアクション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。

使用例

次のコマンドは、ファイアウォール設定を RADIUS サーバ値に設定します。

```
meru-wifi # configure terminal
meru-wifi (config)# security-profile web_auth
meru-wifi(config-security)# firewall-capability radius-configured
```

関連コマンド

- [firewall-filter-id \(428 ページ\)](#)
- [show security-profile \(485 ページ\)](#)

firewall-filter-id

このコマンドも Quality of Service コマンドに適用され、その章に説明が記載されています。
[firewall-filter-id \(704 ページ\)](#) を参照してください。

firewall-filter-id-flow

このコマンドも Quality of Service コマンドに適用され、その章に説明が記載されています。
[firewall-filter-id-flow \(706 ページ\)](#) を参照してください。

group-rekey interval

wpa/802.1x プロファイルは、キー ローテーションが有効である場合のみ設定します。

構文

```
group-rekey interval <n>  
no group-rekey interval
```

n 再試行するまでの秒数。有効な範囲は 0 ～ 65535 です。

コマンド モード

セキュリティ プロファイル設定

デフォルト

デフォルトとしてゼロに設定されます。

用途

wpa/802.1x プロファイル (キー ローテーションが有効である場合のみ) を秒数で設定します。

無効にするには、コマンドの **no** フォームを使用します。

使用例

次の例では、WPA プロファイルに対してグループキー更新の間隔を 120 に設定します。

```
rao36vcell# configure terminal  
rao36vcell(config)# security-profile kddi  
rao36vcell(config-security)# allowed-l2-modes wpa  
rao36vcell(config-security)# encryption-modes tkip  
rao36vcell(config-security)# radius-server primary IAS  
rao36vcell(config-security)# key-rotation enabled  
rao36vcell(config-security)# group-rekey interval 120  
rao36vcell(config-security)# exit  
rao36vcell(config)# exit
```

関連コマンド

- [security-profile \(469 ページ\)](#)
- [8021x-network-initiation \(363 ページ\)](#)
- [allowed-l2-modes \(375 ページ\)](#)
- [encryption-modes tkip \(424 ページ\)](#)
- [psk key \(454 ページ\)](#)
- [show security-profile \(485 ページ\)](#)

import

このコマンドは廃止され、4.0 リリースでは使用できなくなりました。以前は、このコマンドを使用して、SCP 経由でリモート サイトからセキュリティ証明書をインポートしていました。証明書のインポートと管理には、GUI を使用してください。

ip-address

RADIUS プロファイルとして設定されているサーバの IP アドレスを設定します。

構文

`ip-address <address>`

address RADIUS プロファイルとして設定されているサーバの IP アドレスです。

コマンドモード

RADIUS サーバ プロファイル設定モード

デフォルト

なし

用途

このコマンドは、RADIUS プロファイルに設定されているサーバの IP アドレスを設定します。RADIUS サーバは、802.1X WLAN セキュリティの主要コンポーネントであり、アクセス リストをチェックしてユーザを認証することで、アクセス管理を提供します。

プライマリ サーバが利用できなくなった場合も認証サービスを引き続き利用できるようにするために、多くのサイトで、プライマリとセカンダリの RADIUS サーバが設定されます。

RADIUS サーバの IP アドレスとパス キーが設定に必要となります。

RADIUS サーバのプロファイルを設定したら、セキュリティ プロファイル内で **radius-server primary** と **radius-server secondary** コマンドを使用して、認証サービスを有効にします。

使用例

```
controller(config-radius)# ip-address 10.2.2.2
```

関連コマンド

- [key \(433 ページ\)](#)
- [mac-delimiter \(437 ページ\)](#)
- [radius-profile \(456 ページ\)](#)
- [port \(444 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)
- [show radius-profile \(483 ページ\)](#)

key

RADIUS プロファイルとして設定されているサーバの秘密キーを設定します。

構文

```
key <secret>  
no key
```

secret RADIUS サーバが使用する秘密キーを指定します。使用可能な文字数は最大で 64 文字です (! 文字は使用できません)。

コマンドモード

RADIUS サーバ プロファイル設定モード

デフォルト

キーは割り当てられていません。

用途

このコマンドを使用して、RADIUS サーバ プロファイルで設定されている RADIUS サーバの秘密キーを設定します。

使用例

以下のコマンドにより、RADIUS サーバ プロファイルで設定されている RADIUS サーバの秘密キーが **mysecret** に設定されます。

```
controller(config-radius)# key mysecret  
controller(config-radius)#
```

関連コマンド

[radius-profile \(456 ページ\)](#)

key-rotation

キー ローテーションの動きを設定します。

構文

```
key-rotation enabled  
key-rotation disabled
```

コマンド モード

セキュリティ プロファイル設定モード

デフォルト

なし

用途

このコマンドを使用して、秘密キーのローテーションを設定します。

使用例

以下のコマンドによりキー ローテーションが有効になります。

```
controller(config-security)# key-rotation enabled
```

local-admin

ローカル モード認証の管理者を設定し、指定されたローカル管理者の [password \(439 ページ\)](#) と [privilege-level \(451 ページ\)](#) を指定できるローカル管理設定モードに入ります。

構文

`local-admin <name>`

コマンドモード

設定モード。ローカル管理も、管理用のパスワードと特権レベルを設定するモードです。

デフォルト

なし

用途

リリース 4.1 で新しく追加された次のコマンドを使用して、ローカル管理者を設定します。

- [authentication-mode global \(384 ページ\)](#)
- [authentication-type \(386 ページ\)](#) (ローカル用)
- local-admin (このコマンド)
- password (ローカル管理モードでのみ動作)
- privilege-level (ローカル管理モードでのみ動作)
- [show local-admins \(481 ページ\)](#)

使用例

以下のコマンドで、ローカル管理を設定します。

```
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 JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
```

関連コマンド

- [password \(439 ページ\)](#)
- [privilege-level \(451 ページ\)](#)
- [show local-admins \(481 ページ\)](#)

mac-delimiter

RADIUS サーバ プロファイルの区切り文字を設定します。

構文

```
mac-delimiter colon
mac-delimiter hyphen
mac-delimiter none
mac-delimiter single hyphen
no mac-delimiter
```

colon	区切り文字をコロン (:) に指定します。
hyphen	区切り文字をハイフン (-) に指定します。
singlehyphen	各 3 オクテット (例、abcdef-abcdef) 間の区切り文字を単一のハイフン (-) に指定します。
none	区切り文字を使用しないように指定します (デフォルト)。

コマンドモード

RADIUS サーバ プロファイル設定モード

デフォルト

区切り文字は割り当てられません。

用途

このコマンドは、RADIUS サーバ プロファイルの区切り文字を設定します。サーバ データベース内のレコードを分割するために RADIUS サーバで使用される区切り文字を指定します。

使用例

```
controller(config-radius)# mac-delimiter colon
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [ip-address \(432 ページ\)](#)
- [key \(433 ページ\)](#)
- [port \(444 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)

macfiltering

セキュリティ プロファイルに MAC フィルタを設定します。

構文

```
macfiltering  
no macfiltering
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

MAC フィルタリングは無効です。

用途

このコマンドを使用すると、セキュリティ プロファイルで MAC フィルタを有効 / 無効にできます。このコマンドは、セキュリティ プロファイル内で `no macfiltering` コマンドを使用して ESS のグローバル MAC フィルタ設定を上書きする場合に有効です。

使用例

以下のコマンドを使用すると、セキュリティ プロファイルの MAC フィルタリングが無効になります。

```
controller(config-security)# no macfiltering
```

関連コマンド

[access-list permit \(369 ページ\)](#)

password

admin のローカル モード認証パスワードを設定します。

構文

`password <passwd>`

コマンド モード

設定モード > ローカル管理モード

デフォルト

なし

用途

リリース 4.1 で新しく追加された次のコマンドを使用して、ローカル管理者を設定します。

- [authentication-mode global \(384 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [local-admin \(435 ページ\)](#)
- password (ローカル管理モードでのみ動作)
- privilege-level (ローカル管理モードでのみ動作)
- [show local-admins \(481 ページ\)](#)

使用例

以下のコマンドで、ローカル管理を設定します。

```
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 JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
```

関連コマンド

- [local-admin \(435 ページ\)](#)
- [privilege-level \(451 ページ\)](#)

password-type

RADIUS プロファイルとして設定されているサーバのパスワード タイプを設定します。

構文

```
password-type shared-secret  
password-type mac-address  
no password-type
```

shared-secret	RADIUS サーバが使用する秘密キーをパスワードで使用するよう指定します。key コマンドを設定する必要があります。
mac-address	MAC フィルタリング設定の RADIUS に設定されているように、クライアントの MAC アドレスにパスワードを設定します。

コマンドモード

RADIUS サーバ プロファイル設定モード

デフォルト

共有シークレットが設定されています。

用途

このコマンドを使用し、クライアント アクセスに使用されるパスワードのタイプを設定します。デフォルトでは、RADIUS サーバ プロファイル内に key コマンドで設定されている RADIUS サーバの秘密キーが使用されます。mac-address タイプが選択されている場合、MAC フィルタリングの RADIUS 内にユーザとして設定されているクライアントのパスワードとして、クライアントの MAC アドレスが使用されます。

使用例

次のコマンドにより、RADIUS プロファイルとして設定されているサーバの MAC アドレスにパスワード タイプが設定されます。

```
controller(config-radius)# password-type mac-address  
controller(config-radius)#
```

関連コマンド

[radius-profile \(456 ページ\)](#)

PMK-caching

選択したセキュリティ プロファイルの PMK キャッシュを有効にします。この機能は、WPA2 と混合のセキュリティ プロファイルにのみ適用されます。

構文

```
pmk-caching  
no pmk-caching
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

デフォルトでは、PMK キャッシュが有効です。

用途

このコマンドは、アクティブなセキュリティ プロファイルの Pairwise Master Key (PMK) キャッシュの使用を有効または無効にします。PMK キャッシュによって、ワイヤレス クライアントと AP による認証結果がキャッシュされるため、前に認証されたことがあるクライアントから AP へのローミングで、高速のネットワーク アクセスが可能になります。

no pmk-caching コマンドを使用すると、PMK キャッシュが無効になります。

使用例

次のコマンドは、キーを 300 秒 (5 分) ごとに変更します。

```
MC3200-5072(15)# configure terminal  
MC3200-5072(15)(config)# security-profile Wpa2Test  
MC3200-5072(15)(config-security)# pmk-caching  
MC3200-5072(15)(config-security)# end
```

関連コマンド

pmk caching

このコマンドは、KDDI の電話の PMK キャッシュを有効または無効にします。

構文

`pmk caching [enabled | disabled]`

コマンド モード

セキュリティ プロファイル設定

デフォルト

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。

用途

セキュリティ プロファイル設定から、KDDI の電話の PMK キャッシュを有効または無効にします。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。

使用例

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以下の行を追加します。

```
default(config-security)# pmk caching 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)# pmk caching disabled
```

関連コマンド

- [security-profile \(469 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)
- [8021x-network-initiation \(363 ページ\)](#)
- [show security-profile \(485 ページ\)](#)

port

RADIUS サーバ プロファイルのポート番号を設定します。

構文

```
port port  
no port
```

port RADIUS 認証サーバ プロファイルで使用されるポートを指定します。有効なポート番号は 1024 ~ 65535 です、デフォルトでは、ポート 1812 が設定されます。ポート 1813 は、アカウントिंग RADIUS サーバに使用する必要があります。

コマンドモード

RADIUS サーバ プロファイル設定モード

デフォルト

ポート 1812 が割り当てられます。

用途

このコマンドにより、RADIUS サーバ プロファイルで使用されるポートが設定されます。通常、プロファイルが RADIUS アカウンティング サーバで使用されない限り、この設定を変更する必要はありません。RADIUS アカウンティング サーバで使用される場合は、1813 に変更する必要があります。

使用例

```
controller# config terminal  
controller(config)#  
controller(config-radius)# port 6600
```

関連コマンド

- [ip-address \(432 ページ\)](#)
- [key \(433 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)
- [radius-profile \(456 ページ\)](#)
- [port \(444 ページ\)](#)
- [show radius-profile \(483 ページ\)](#)

primary-tacacs-ip

プライマリ TACACS+ サーバの IP アドレスを指定します。

構文

primary-tacacs-ip <xx.xx.xx.xx>

コマンドモード

設定モード > 認証モード

デフォルト

なし

用途

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 \(384 ページ\)](#) (認証を TACACS に設定します)
- primary-tacacs-ip (このコマンド)
- [primary-tacacs-port \(447 ページ\)](#) (プライマリ TACACS サーバのポートを指定します)
- [primary-tacacs-secret \(449 ページ\)](#) (プライマリ TACACS サーバのパスワードを指定します)
- [authentication-type \(386 ページ\)](#) tacacs+
- [secondary-tacacs-ip \(462 ページ\)](#) (セカンダリ TACACS+ サーバの IP アドレスを指定します)
- [secondary-tacacs-port \(464 ページ\)](#) (セカンダリ TACACS サーバのポートを指定します)
- [secondary-tacacs-secret \(466 ページ\)](#) (セカンダリ TACACS サーバのパスワードを指定します)

使用例

次のコマンドは、TACACS+ サーバの認証を設定します。

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port      primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
Administrative User Management

AuthenticationType           : tacacs+
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   : 172.18.1.10
Primary TACACS+ Port         : 49
Primary TACACS+ Secret Key   : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port       : 49
Secondary TACACS+ Secret Key : *****
```

関連コマンド

- [authentication-mode global \(384 ページ\)](#)
- [primary-tacacs-port \(447 ページ\)](#)
- [primary-tacacs-secret \(449 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [secondary-tacacs-port \(464 ページ\)](#)
- [secondary-tacacs-secret \(466 ページ\)](#)

primary-tacacs-port

プライマリ TACACS+ サーバのポートを指定します。

構文

`primary-tacacs-port <xx>`

コマンドモード

設定モード > 認証モード

デフォルト

なし

用途

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 \(384 ページ\)](#) (認証を TACACS に設定します)
- [primary-tacacs-ip \(445 ページ\)](#) (プライマリ TACACS+ サーバの IP アドレスを指定します)
- [primary-tacacs-port \(447 ページ\)](#) (プライマリ TACACS サーバのポートを指定します)
- [primary-tacacs-secret \(449 ページ\)](#) (プライマリ TACACS サーバのパスワードを指定します)
- [authentication-type \(386 ページ\)](#) tacacs+
- [secondary-tacacs-ip \(462 ページ\)](#) (セカンダリ TACACS+ サーバの IP アドレスを指定します)
- [secondary-tacacs-port \(464 ページ\)](#) (セカンダリ TACACS サーバのポートを指定します)
- [secondary-tacacs-secret \(466 ページ\)](#) (セカンダリ TACACS サーバのパスワードを指定します)

使用例

次のコマンドは、TACACS+ サーバの認証を設定します。

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port      primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
Administrative User Management

AuthenticationType           : tacacs+
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   : 172.18.1.10
Primary TACACS+ Port         : 49
Primary TACACS+ Secret Key   : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port       : 49
Secondary TACACS+ Secret Key : *****
```

関連コマンド

- [authentication-mode global \(384 ページ\)](#)
- [primary-tacacs-ip \(445 ページ\)](#)
- [primary-tacacs-secret \(449 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [secondary-tacacs-port \(464 ページ\)](#)
- [secondary-tacacs-secret \(466 ページ\)](#)

primary-tacacs-secret

プライマリ TACACS+ サーバのパスワードを指定します。

構文

`primary-tacacs-ip <passwd>`

コマンドモード

設定モード > 認証モード

デフォルト

なし

用途

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 \(384 ページ\)](#) (認証を TACACS に設定します)
- [primary-tacacs-ip \(445 ページ\)](#) (プライマリ TACACS+ サーバの IP アドレスを指定します)
- [primary-tacacs-port \(447 ページ\)](#) (プライマリ TACACS サーバのポートを指定します)
- [primary-tacacs-secret \(449 ページ\)](#) (プライマリ TACACS サーバのパスワードを指定します)
- [authentication-type \(386 ページ\)](#) (for tacacs+)
- [secondary-tacacs-ip \(462 ページ\)](#) (セカンダリ TACACS+ サーバの IP アドレスを指定します)
- [secondary-tacacs-port \(464 ページ\)](#) (セカンダリ TACACS サーバのポートを指定します)
- [secondary-tacacs-secret \(466 ページ\)](#) (セカンダリ TACACS サーバのパスワードを指定します)

使用例

次のコマンドは、TACACS+ サーバの認証を設定します。

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
Administrative User Management

AuthenticationType           : tacacs+
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  : 172.18.1.10
Primary TACACS+ Port        : 49
Primary TACACS+ Secret Key  : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

関連コマンド

- [authentication-mode global \(384 ページ\)](#)
- [primary-tacacs-port \(447 ページ\)](#)
- [primary-tacacs-ip \(445 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [secondary-tacacs-port \(464 ページ\)](#)
- [secondary-tacacs-secret \(466 ページ\)](#)

privilege-level

admin のローカル モード認証権限レベルを設定します。

構文

privilege-level <0,1,2,3,4,5,6,7,8>

コマンドモード

設定モード > ローカル管理モード

デフォルト

なし

用途

次のコマンドを使用して、ローカル管理者を設定します。

- [authentication-mode global \(384 ページ\)](#)
- [authentication-type \(386 ページ\)](#) (ローカル用)
- [local-admin \(435 ページ\)](#)
- password (ローカル管理モードでのみ動作)
- privilege-level (ローカル管理モードでのみ動作し、2、5、および 8 の 3 つの数値のみ使用)
- [show local-admins \(481 ページ\)](#)

数値	マッピング先	名前と特権
8	8	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。
7	8	
6	8	
5	5	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)。リリース 4.1 の新機能であるローカル管理者の作成は実行できず、コントローラの認証モードも設定できません (GUI および CLI)。ライセンスの追加や削除も実行できません。
4	5	
3	5	

数値	マッピング先	名前と特権
2	2	SuperUser administrators 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)。リリース 4.1 の新機能であるローカル管理者の作成も実行でき、コントローラの認証モードも設定できます (GUI および CLI)。Superuser は、ライセンスを追加、削除できます。
1	2	
0	2	

使用例

以下のコマンドで、ローカル管理を設定します。

```
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 JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
```

```
ramcntrl(0)(config-local-admin)# password yosemite44  
ramcntrl(0)(config-local-admin)# exit  
ramcntrl(0)(config)# exit
```

関連コマンド

- [local-admin](#) (435 ページ)
- [password](#) (439 ページ)

psk key

WPA-Personal または WPA2-Personal Passphrase (「事前共有キー」) を設定します。

構文

```
psk key <key>  
no psk key
```

key

事前共有キー。

- 8 ～ 63 の ASCII 文字 (!\ " ? 文字はバックスラッシュ (\) 文字でエスケープする必要があります。例、!\ !?)
- 64 の 16 進数文字 (16 進数キーには、接頭辞 「0x」 を付ける必要があります。接頭辞なしではキーは動作しません)

コマンドモード

セキュリティ プロファイル設定モード

デフォルト

キーは設定されません。

用途

Wi-Fi-Protected Access (WPA および WPA2) 規格により、802.1X を使用してセキュリティ強度を向上させた認証方法などが提供され、システム環境がより安全になります。サイトで RADIUS サーバが実装されていない場合は、WEP64 および WEP128 共有キー実装を向上させるために、WPA/WPA2 Passphrase を利用できます。

WPA-Personal および WPA2-Personal では、WEP64 や WEP128 よりも長い共有秘密キー (256 ビット) を使用できるようになっています。このセキュリティ プロファイルを使用する ESSID 1 つにつき、1 PSK を割り当てます。このキーは、ESSID AP に配信されます。AP に参加するクライアントでは、割り当てを行う前に同じ共有キーが設定されている必要があります。

Passphrase はよりセキュリティが強化されていますが、キーの管理は自動ではありません。また、WLAN におけるすべてのクライアント ステーションと AP をパスワード変更時に更新する必要があるため、管理のために労力を費やす必要があります。パスワードは不正利用を防ぐために頻繁に変更してください。

WPA/WPA2 Passphrase では、以下を含むキーを使用できます。

- 64 の 16 進数文字 (つまり、0 ～ 9、a ～ f、A ～ F)。例：
0xa0a1a2a3a4a5a6a7a8a9aaabac や 0x12345678901234567890abcdef...

- 8 ～ 63 の ASCII 文字 (!\ " ? 文字はバックスラッシュ (\) 文字でエスケープする必要があります。例、!\ \?)。例 : m6o0secret79\?key

no psk key コマンドを使用して、固定 WPA/WPA2 Passphrase を無効にします。



16 進数キーを使用する場合、接頭辞 0x をキーの前に付ける必要があります。接頭辞 0x により、システムは 16 進数のキーが入力されることを認識します。

使用例

以下のコマンドにより、WPA/WPA2 Passphrase が作成されます。

```
controller(config-security)# psk key 012345678901234567890abcdef
```

関連コマンド

[allowed-l2-modes](#) (375 ページ)

radius-profile

RADIUS サーバのプロファイルを作成し、RADIUS サーバ設定モードに入ります。

構文

```
radius-profile <name>  
no radius-profile <name>
```

name RADIUS プロファイルとして設定されているサーバの名前。
 名前の長さは 1 ～ 16 文字です。

コマンド モード

グローバル設定モード

デフォルト

デフォルトはありません。

用途

このコマンドは、RADIUS サーバの設定プロファイルを作成します。RADIUS サーバは、802.1X WLAN セキュリティの主要コンポーネントであり、アクセス リストをチェックしてユーザを認証することで、アクセス管理を提供します。プライマリ サーバが利用できなくなった場合も認証サービスを引き続き利用できるようにするために、多くのサイトで、プライマリとセカンダリの RADIUS サーバが設定されます。コマンド **no radius-profile** を使用すると、プロファイルが削除されます。

プロファイル設定では、RADIUS サーバの IP アドレスとパスキーが必須であり、**ip-address** コマンドと **key** コマンドを使用して設定します。説明、ポート番号、およびレコードの区切り文字もオプションで指定でき、**description**、**port**、および **mac-delimiter c** コマンドを使用して指定します。また、秘密キーを使用する代わりに、クライアントの MAC アドレス (MAC フィルタリング設定の RADIUS 内に設定されている) を使用でき、**password-type** コマンドを使用して設定します。

RADIUS サーバのプロファイルを設定したら、**radius-server primary** または **radius-server secondary** コマンドを使用して、新たに設定されたプロファイルとセキュリティプロファイル設定との関係確立し、サーバのランク (プライマリまたはセカンダリ) を設定します。

RADIUS プロファイルは、RADIUS アカウンティング サーバ設定と MAC アドレスの ACL にも使用されます (「関連コマンド」セクションのリンクを参照)。

使用例

```
controller(config)# radius-profile main-auth  
controller(config-radius)# ?
```

called-station-id-type (10)	Configures the Called Station ID Type.
default	Set radius profile parameters to default value.
description	Specifies the radius node.
do	Executes an IOSCLI command.
end	Save changes, and return to privileged EXEC mode.
exit mode.	Save changes, and return to global configuration
ip-address	Configures the IP address.
key	Configures the secret key.
mac-delimiter	Configures the MAC Delimiter.
no	Disabling radius profile parameters.
password-type	Configures the RADIUS Password Type.
port	Configures port number.

関連コマンド

- [description \(421 ページ\)](#)
- [ip-address \(432 ページ\)](#)
- [key \(433 ページ\)](#)
- [mac-delimiter \(437 ページ\)](#)
- [port \(444 ページ\)](#)
- [password \(439 ページ\)](#)
- [accounting primary-radius \(524 ページ\)](#)
- [accounting secondary-radius \(526 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)

radius-server primary

プロファイルで指定されたプライマリ RADIUS サーバを割り当て、有効にします。

構文

```
radius-server primary <profile>  
no radius-server primary  
no radius-server all
```

profile **radius-profile** コマンドで作成された RADIUS サーバ プロファイルの名前を指定します。

コマンドモード

セキュリティ プロファイル設定

用途

このコマンドは、**radius-profile** コマンドで設定されたプロファイルで指定されたプライマリ RADIUS サーバを割り当て、有効にします。このコマンドを、RADIUS サーバ設定の最後のステップとして使用します。このコマンドで割り当てる前に、プロファイルが存在している必要があります。



RADIUS サーバ設定のプロファイルが適切なポート (1812: RADIUS 認証サーバのデフォルト ポート) を使用するようにします。

no radius-server all コマンドを使用して、プライマリおよびセカンダリ RADIUS サーバを無効にするか、**no radius-server primary** コマンドを使用してプライマリ RADIUS サーバを無効にします。

使用例

以下のコマンドは、プライマリ RADIUS サーバとしてプロファイル *main-auth* を割り当てます。

```
controller(config-security)# radius-server primary main-auth
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [radius-server secondary \(459 ページ\)](#)
- [show radius-profile \(483 ページ\)](#)

radius-server secondary

プロファイルで指定されたセカンダリ RADIUS サーバを割り当て、有効にします。

構文

```
radius-server secondary <profile>  
no radius-server secondary
```

profile **radius-profile** コマンドで作成された RADIUS サーバ プロファイルの名前を指定します。

コマンドモード

セキュリティ プロファイル設定

用途

このコマンドは、**radius-profile** コマンドで設定されたプロファイルで指定されたセカンダリ RADIUS サーバを割り当て、有効にします。このコマンドを、RADIUS サーバセットアップの最後のステップとして使用します。このコマンドで有効にする前に、プロファイルが存在している必要があります。

no radius-server secondary コマンドを使用すると、セカンダリ RADIUS サーバが無効になります。

使用例

以下のコマンドは、セカンダリ RADIUS サーバとして *backup-auth* プロファイルを割り当てます。

```
controller(config-security)# radius-server secondary backup-auth
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [radius-server primary \(458 ページ\)](#)
- [show radius-profile \(483 ページ\)](#)

reauth

再認証を有効にします。

構文

```
reauth  
no reauth
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

再認証は無効です。

用途

このコマンドを使用すると、コントローラが、RADIUS Access-Accept パケットにある「Session-timeout」RADIUS 属性を強制的に受け取るようになります。

Session-timeout 属性が使用され、ステーションが指定した期間にネットワーク (802.1X) への再認証を行う必要がある場合、このコマンドを使用します。「Session-timeout」が使用されない場合、セキュリティ プロファイル内の再認証を有効にする必要はありません。

使用例

以下のコマンドを使用すると、セキュリティ プロファイルの再認証が有効になります。

```
controller(config-security)# reauth
```

関連コマンド

rekey period

802.1X キーおよび WPA キー再生成の間隔を設定します。

構文

```
rekey period <seconds>  
no rekey period
```

seconds 802.1X キーが有効である時間を秒数で指定します。*seconds* の値は、0 ～ 65535 です。

コマンドモード

セキュリティ プロファイル設定

デフォルト

デフォルトのキー再生成間隔時間は 0 です。

用途

このコマンドは、802.1X キーが有効である時間の長さを定義します。*seconds* で指定した時間が経過すると、新しいキーが自動的に生成されます。セキュリティ違反を防ぐために、頻繁にキーを変更することを推奨します。

0 を指定すると、キー変更が無効となり、セッションの長さに関係なく、セッションが行われている間、キーは有効となります。

no rekey period コマンドを使用すると、キーの再生成が無効となります。

使用例

次のコマンドは、キーを 300 秒 (5 分) ごとに変更します。

```
controller(config-security)# rekey period 300
```

関連コマンド

[rekey period \(461 ページ\)](#)

secondary-tacacs-ip

セカンダリ TACACS+ サーバの IP アドレスを指定します。

構文

secondary-tacacs-ip <xx.xx.xx.xx>

コマンドモード

設定モード > 認証モード

デフォルト

なし

用途

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 \(384 ページ\)](#) (認証を TACACS に設定します)
- [primary-tacacs-ip \(445 ページ\)](#) (プライマリ TACACS+ サーバの IP アドレスを指定します)
- [primary-tacacs-port \(447 ページ\)](#) (プライマリ TACACS サーバのポートを指定します)
- [primary-tacacs-secret \(449 ページ\)](#) (プライマリ TACACS サーバのパスワードを指定します)
- [authentication-type \(386 ページ\)](#) (for tacacs+)
- [secondary-tacacs-ip \(462 ページ\)](#) (セカンダリ TACACS+ サーバの IP アドレスを指定します)
- [secondary-tacacs-port \(464 ページ\)](#) (セカンダリ TACACS サーバのポートを指定します)
- [secondary-tacacs-secret \(466 ページ\)](#) (セカンダリ TACACS サーバのパスワードを指定します)

使用例

次のコマンドは、TACACS+ サーバの認証を設定します。

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```



```
default(0)# show authentication-mode
Administrative User Management

AuthenticationType           : tacacs+
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   : 172.18.1.10
Primary TACACS+ Port         : 49
Primary TACACS+ Secret Key   : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port       : 49
Secondary TACACS+ Secret Key : *****
```

関連コマンド

- [authentication-mode global \(384 ページ\)](#)
- [primary-tacacs-port \(447 ページ\)](#)
- [primary-tacacs-secret \(449 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [secondary-tacacs-port \(464 ページ\)](#)
- [secondary-tacacs-secret \(466 ページ\)](#)

secondary-tacacs-port

セカンダリ TACACS+ サーバのポートを指定します。

構文

secondary-tacacs-port <xx>

コマンドモード

設定モード > 認証モード

デフォルト

なし

用途

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 \(384 ページ\)](#) (認証を TACACS に設定します)
- [primary-tacacs-ip \(445 ページ\)](#) (プライマリ TACACS+ サーバの IP アドレスを指定します)
- [primary-tacacs-port \(447 ページ\)](#) (プライマリ TACACS サーバのポートを指定します)
- [primary-tacacs-secret \(449 ページ\)](#) (プライマリ TACACS サーバのパスワードを指定します)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#) (セカンダリ TACACS+ サーバの IP アドレスを指定します)
- [secondary-tacacs-port \(464 ページ\)](#) (セカンダリ TACACS サーバのポートを指定します)
- [secondary-tacacs-secret \(466 ページ\)](#) (セカンダリ TACACS サーバのパスワードを指定します)

使用例

次のコマンドは、TACACS+ サーバの認証を設定します。

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port      primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
Administrative User Management

AuthenticationType           : tacacs+
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  : 172.18.1.10
Primary TACACS+ Port        : 49
Primary TACACS+ Secret Key  : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

関連コマンド

- [authentication-mode global \(384 ページ\)](#)
- [primary-tacacs-ip \(445 ページ\)](#)
- [primary-tacacs-secret \(449 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [primary-tacacs-port \(447 ページ\)](#)
- [secondary-tacacs-secret \(466 ページ\)](#)

secondary-tacacs-secret

セカンダリ TACACS+ サーバのパスワードを指定します。

構文

`primary-tacacs-ip <passwd>`

コマンドモード

設定モード > 認証モード

デフォルト

なし

用途

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 \(384 ページ\)](#) (認証を TACACS に設定します)
- [primary-tacacs-ip \(445 ページ\)](#) (プライマリ TACACS+ サーバの IP アドレスを指定します)
- [primary-tacacs-port \(447 ページ\)](#) (プライマリ TACACS サーバのポートを指定します)
- [primary-tacacs-secret \(449 ページ\)](#) (プライマリ TACACS サーバのパスワードを指定します)
- [authentication-type \(386 ページ\)](#) (for tacacs+)
- [secondary-tacacs-ip \(462 ページ\)](#) (セカンダリ TACACS+ サーバの IP アドレスを指定します)
- [secondary-tacacs-port \(464 ページ\)](#) (セカンダリ TACACS サーバのポートを指定します)
- [secondary-tacacs-secret \(466 ページ\)](#) (セカンダリ TACACS サーバのパスワードを指定します)

使用例

次のコマンドは、TACACS+ サーバの認証を設定します。

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
Administrative User Management

AuthenticationType          : tacacs+
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  : 172.18.1.10
Primary TACACS+ Port        : 49
Primary TACACS+ Secret Key  : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

関連コマンド

- [authentication-mode global \(384 ページ\)](#)
- [primary-tacacs-port \(447 ページ\)](#)
- [primary-tacacs-ip \(445 ページ\)](#)
- [authentication-type \(386 ページ\)](#)
- [secondary-tacacs-ip \(462 ページ\)](#)
- [secondary-tacacs-port \(464 ページ\)](#)
- [primary-tacacs-secret \(449 ページ\)](#)

security-logging

セキュリティ ログングをオンおよびオフにします。

構文

```
security-logging on
security-logging off
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

セキュリティ ログングは**オフ**です。

用途

セキュリティ ログングがオンの場合、syslog-host がコントローラに設定されていれば、ログがシステム ログに送信されます。

使用例

次のコマンドは、default という名前のコントローラでセキュリティ ログングをオンにしています。

```
default(config-security)# security-logging on
```

以下に、セキュリティ ログングが有効になった場合のシステム ログ エントリの一例を示します。

接続されたステーションは次のようにログされます。

```
*****
Feb 04 16:45:37 192.168.143.112 ALARM: 12022014871 | system | info | ALR |
New Station Connected : MacAddress : 00:40:96:a3:5d:34, UserName : , AP-Id
: 0, AP-Name : , BSSID : 00:12:F2:9b:02:01, ESSID : integ-mmode, Ip-Type :
dynamic dhcp, Ip-Address : 0.0.0.0, L2mode : wpa2, L3-mode : clear, Vlan-
Name : None, Vlan-Tag : 0
```

たとえば、ステーション切断メッセージは次のようになります。

```
*****
Feb 04 16:45:37 192.168.143.112 ALARM: 12022014871 | system | info | ALR |
Station Disconnected : MacAddress : 00:40:96:a3:5d:34
```

関連コマンド

- [firewall-filter-id \(428 ページ\)](#)
- [syslog-host \(228 ページ\)](#)

security-profile

セキュリティ プロファイルを作成し、セキュリティ プロファイル設定モードに入ります。

構文

```
security-profile <name>  
no security-profile <name>
```

name 最大 32 の英数字の文字列を指定します。スペースや特殊文字 を使用するには、二重引用符 (" ") で囲みます。

コマンドモード

グローバル設定

デフォルト

default セキュリティ プロファイルが提供されます。

用途

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。



同じ WEP キー インデックスは複数のセキュリティ プロファイルで使用できますが、各セキュリティ プロファイルで定義できるのは、レイヤ 2 メソッド 1 つだけです。

デフォルトでは、FortiWLC (SD) には、*default* という名前のセキュリティ プロファイルが付属しますが、このプロファイルでは認証が実施されず、すべてのワイヤレス クライアントがコントローラに接続できるオープン認証が使用されます。*default* プロファイルは、ESSID が作成される際に自動的に関連付けられます。

no フォームを使用して、セキュリティ プロファイルを削除します。ESSID により指定されない場合のみ、セキュリティ プロファイルを削除できます。*default* セキュリティ プロファイルを削除することはできません。

使用例

以下のコマンドを指定すると、*profile 1* というセキュリティ プロファイルを作成してセキュリティ プロファイル設定モードに入り、利用可能なコマンドが一覧表示されます。

```
controller(config)# security-profile "profile 1"
controller(config-security)#?
8021x-network-initiation (10) Enable 802.1x network initiation.
allowed-l2-modes          (10) Configure permitted L2 authentication modes.
captive-portal            (10) Enable captive portal.
captive-portal-auth-method (10) Configure captive portal authentication
method.
do                         (10) Executes an IOSCLI command.
encryption-modes          (10) Configure permitted cipher suites.
end                       (10) Save changes, and return to privileged EXEC
mode.
exit                      (10) Save changes, and return to global configuration
mod
e.
firewall-capability       (10) Configure Firewall Capability.
firewall-filter-id        (10) Configure Firewall Filter-ID.
group-rekey               (10) Configure the GroupRekey interval.
key-rotation              (10) Configure Key Rotation.
macfiltering              (10) Enable MAC Filtering.
no                        (10) Configure authentication parameters.
owner                     (10) Owner of the profile
passthrough-firewall-filter-id (10) Configure Passthrough Firewall Filter-
ID.
pmk-caching               (10) Enable PMK Caching.
psk                       (10) Configure the encryption WPA Pre-shared key
radius-server             (10) Configure RADIUS security.
reauth                   (10) Enable reauthentication.
rekey                     (10) Configure rekey period and related parameters.
security-logging          (10) Configure Security Profile Logging.
shared-authentication     (10) Enable shared authentication.
show                     (10) Displays various parameters.
static-wep                (10) Configure the static WEP key
tunnel-termination        (10) Configure Tunnel Termination.
```

関連コマンド

- [essid \(550 ページ\)](#)

- [security-profile](#) (469 ページ)
- [show security-profile](#) (485 ページ)

shared-authentication

共有認証の追加セキュリティを有効にします。

構文

```
shared-authentication enable  
no shared-authentication
```

コマンド モード

セキュリティ プロファイル設定

デフォルト

共有認証はオフです。

用途

このコマンドを使用して、共有認証を有効にします。

WiFi Protected Access (WPA) を使用しないネットワークでは、Wireless Encryption Protocol (WEP) 暗号を使用してオープン認証を使用できます。**no shared-authentication** コマンドを使用して、WEP による共有認証を無効にします。この設定によりセキュリティが強化され、ユーザのワイヤレス ネットワークに対する悪意のあるユーザからの侵入を防ぐ上で役立ちます。WEP 暗号化によるオープン認証の代わりに共有キーを使用すると、悪意のあるユーザが簡単に共有キーを解読し、ワイヤレス ネットワークにあるすべてのコンピュータにアクセスできてしまいます。

使用例

次の例は、共有認証を有効にします。

```
Controller# configure terminal  
Controller(config)# security-profile wep64  
Controller(config-security)# allowed-l2-modes wep  
Controller(config-security)# encryption-modes wep64  
Controller(config-security)# static-wep key 12345  
Controller(config-security)# static-wep key-index 1  
Controller(config-security)# shared-authentication ?  
enable                Enable shared authentication.  
Controller(config-security)# shared-authentication enable  
Controller(config-security)# exit  
Controller(config)# end  
Controller#
```

関連コマンド

[security-profile \(469 ページ\)](#)

show aaa statistics

認証統計の詳細情報を表示します。

構文

```
show aaa statistics
```

コマンドモード

EXEC

用途

このコマンドを使用して、802.1X パフォーマンスに関する統計情報を表示します。認証統計は、コントローラがリブートされるとリセットされます。

aaa 統計には以下の情報が含まれます。

統計	説明
802.1x Authentication Request Count	802.1x 認証要求の総数
802.1x Authentication Success Count	成功した認証要求の数
802.1x Authentication Failure Count	失敗した認証要求の数
802.1x Authentication Station Count	802.1x によって現在認証されているステーションの数

使用例

以下のコマンドは、802.1X 統計情報を表示します。

```
controller# show aaa statistics
```

```
Authentication Statistics
```

```
802.1x Authentication Request Count : 519
```

```
802.1x Authentication Success Count : 54
```

```
802.1x Authentication Failure Count : 465
```

```
802.1x Authentication Station Count : 481
```

show access-list deny

拒否 ACL の MAC アドレスのリストを表示します。

構文

show access-list deny

コマンド モード

EXEC

デフォルト

なし

用途

show access-list deny コマンドを使用して、WLAN へのアクセスが拒否されている MAC アドレスのリストが含まれる拒否リストを表示します。拒否リストの作成に加えて、MAC アドレスが拒否される前に有効にする必要があります。有効にできるリストはいずれか 1 つのみです。許可リストと拒否リストを同時に有効にすることはできません。MAC フィルタリングを非アクティブにすることで、許可および拒否リストを作成し、これらを無効にできます。

使用例

以下のコマンドは、拒否リストの MAC アドレスを表示します。

```
controller# show access-list deny
MAC Address

00:0c:e6:bd:01:05
00:0c:e6:12:07:41
00:0c:e6:09:46:64
00:0c:30:be:f8:19
00:07:e9:15:69:40
00:06:25:a7:e9:11
00:04:23:87:89:71
  Acl Deny Access Configuration (7 entries)
controller#
```

関連コマンド

- [access-list deny \(365 ページ\)](#)
- [access-list deny import \(367 ページ\)](#)

show access-list permit

許可 ACL の MAC アドレスのリストを表示します。

構文

`show access-list permit`

コマンド モード

EXEC

デフォルト

なし

用途

`show access-list permit` コマンドを使用して、WLAN へのアクセスが許可されている MAC アドレスのリストが含まれる許可リストを表示します。MAC アドレスが許可される前に、有効にする必要があります。同時に有効にできるのは 1 つの MAC フィルタリング リストのみであり、許可リストと拒否リストを同時に有効にすることはできません。MAC フィルタリングを非アクティブにすることで、許可および拒否リストを作成し、これらを無効にできます。

使用例

以下のコマンドは、許可リストの MAC アドレスのリストを表示します。

```
controller# show access-list permit
MAC Address
00:0c:e6:bd:01:05
00:0c:e6:12:07:41
00:0c:e6:09:46:64
00:0c:30:be:f8:19
00:07:e9:15:69:40
00:06:25:a7:e9:11
00:04:23:87:89:71
00:40:96:51:eb:2b
Acl Allow Access Configuration (8 entries)
controller#
```

関連コマンド

- [access-list permit \(369 ページ\)](#)
- [access-list permit import \(371 ページ\)](#)

show air-shield

Air-Shield 設定を表示します。

構文

`show air-shield`

コマンド モード

特権 EXEC

用途

このコマンドを使用すると、Air-Shield 機能の設定が表示されます。

使用例

次のコマンドは、Air-Shield のデフォルト設定を表示します。

```
controller# show air-shield
Air Shield

Air Firewall                : none
Allowed OUIs #1             : 00:00:00:00:00:00
Allowed OUIs #2             : 00:00:00:00:00:00
Allowed OUIs #3             : 00:00:00:00:00:00
Off-Hour Network Behaviour  : none
Time Interval Start         : 00:00
Time Interval End           : 00:00
```

関連コマンド

[access-list deny \(365 ページ\)](#)

show arp

コントローラの ARP 表と IP-MAC アドレス マッピングを表示します。

構文

`show arp`

コマンド モード

特権 EXEC

デフォルト

なし

用途

使用例

次の例は、コントローラの ARP 表と IP-MAC アドレス マッピングを表示します。

```
corpwifi# show arp
```

Address Iface	Hwtype	Hwaddress	Flags	Mask
192.168.34.188	ether	00:22:10:B9:39:0C	CM	ats
192.168.34.65	ether	00:21:5C:08:EC:C7	CM	ats
192.168.34.44	ether	00:09:EF:07:56:AF	CM	ats
192.168.34.190	ether	00:22:10:B9:39:03	CM	ats
192.168.34.146		(incomplete)		controller
192.168.34.43	ether	00:21:6B:3B:61:A8	CM	ats
192.168.34.1	ether	00:19:BB:B0:27:00	C	controller
192.168.37.11	ether	00:1E:2A:36:04:B1	CM	ats
192.168.34.96		(incomplete)		ats
192.168.34.41	ether	00:24:B2:EF:C2:2A	CM	ats
192.168.34.74	ether	00:0C:E6:07:9F:3F	C	controller
192.168.34.147	ether	00:21:29:67:BB:96	CM	ats
192.168.34.37	ether	00:1C:BF:25:67:76	CM	ats
192.168.34.72	ether	00:1C:BF:25:A6:11	CM	ats
192.168.34.70	ether	00:0C:E6:04:3C:E8	C	controller
192.168.34.210	ether	00:03:25:40:86:EA	C	controller
192.168.34.101	ether	00:0C:E6:05:EA:FA	C	controller
192.168.34.179	ether	00:90:7A:08:A9:15	CM	ats

192.168.34.76	ether	00:16:6F:C7:2F:78	CM	ats
192.168.34.151	ether	00:16:EA:60:3C:C0	CM	ats
192.168.34.178	ether	00:01:3E:10:30:8B	CM	ats
192.168.34.150	ether	00:22:68:A0:EF:8D	CM	ats
192.168.34.117	ether	00:01:3E:10:1D:F7	CM	ats
192.168.37.31	ether	00:1B:2F:C5:A5:6B	CM	ats
192.168.34.24	ether	00:22:10:B9:39:07	CM	ats
192.168.34.174	ether	00:22:68:A0:F0:3B	CM	ats
192.168.34.25	ether	00:22:10:B9:39:21	CM	ats
192.168.34.51	ether	00:0C:E6:07:9F:11	C	controller
192.168.34.121	ether	00:0C:E6:04:DF:79	C	controller
192.168.34.120	ether	00:0C:E6:04:FC:E9	C	controller
192.168.34.28	ether	00:22:10:B9:39:08	CM	ats
192.168.34.171	ether	00:16:6F:0D:47:81	CM	ats
192.168.34.197	ether	00:25:4B:95:92:5A	CM	ats
192.168.34.58	ether	00:01:3E:10:1A:1D	CM	ats
192.168.34.30	ether	00:22:10:B9:38:FF	CM	ats

関連コマンド

show authentication-mode

認証モード設定を表示します。

構文

show authentication-mode

コマンドモード

特権 EXEC

用途

このコマンドを使用すると、Web ユーザおよびキャプティブ ポータル ゲスト ユーザ認証が実行される場所を決定するために設定が表示されます。

使用例

次のコマンドを使用すると、プロファイル Primary 内で命名された RADIUS サーバがユーザ認証を実行中であることが示されます。

```
controller# show authentication-mode
auth_mode
```

```
AuthenticationType      : radius
Primary RADIUS Server    : Primary
Secondary RADIUS Server  :
```

次のコマンドを使用すると、コントローラがユーザ認証が実行中であることが示されます。

```
controller# show authentication-mode
auth_mode
```

```
AuthenticationType      : local
Primary RADIUS Server    :
Secondary RADIUS Server  :
```

関連コマンド

[authentication-mode \(382 ページ\)](#)

show cef

通常イベントフォーマット ログイング サーバ設定を表示します。

構文

show cef

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用すると、**cef** コマンドを使用して設定されている通常イベント フォーマット ログイング サーバの設定が表示されます。

使用例

以下に 192.18.100.100 のログイング サーバのステータスを示します。

```
default(config)# show cef
CEF Logging is disabled
Host      : 192.168.100.100
Port      : 514
```

関連コマンド

[cef](#) (394 ページ)

show local-admins

設定されているローカル管理者を表示します。

構文

`show local-admins`

コマンド モード

特権 EXEC

デフォルト

なし

用途

リリース 4.1 で新しく追加された次のコマンドを使用して、ローカル管理者を設定します。

- [authentication-mode global \(384 ページ\)](#)
- [authentication-type \(386 ページ\)](#) (ローカル用)
- `local-admin` (このコマンド)
- [password \(439 ページ\)](#) (ローカル管理モードでのみ動作)
- [privilege-level \(451 ページ\)](#) (ローカル管理モードでのみ動作)
- [show local-admins \(481 ページ\)](#)

使用例

以下のコマンドで、ローカル管理を設定します。

```
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 JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
```

関連コマンド

- [password \(439 ページ\)](#)
- [privilege-level \(451 ページ\)](#)
- [local-admin \(435 ページ\)](#)

show radius-profile

設定された RADIUS プロファイルを表示します。

構文

```
show radius-profile
show radius-profile <name>
```

name オプション。表示するプロファイルの名前を指定します。

コマンド モード

特権 EXEC

デフォルト

すべての RADIUS プロファイルのリストが表示されます。

用途

このコマンドは、**radius-profile** コマンド、または **<name>** の追加によって作成されたすべての RADIUS プロファイルを表示し、**name** プロファイルの詳細を表示します。

使用例

以下のコマンドは、設定されている RADIUS プロファイルを表示します。

```
controller# show radius-profile
```

Profile Name	RADIUS IP	Port	MAC Delimiter	Password	Type
MyRad	192.168.100.1	1812	none	shared-secret	

RADIUS Profile Table (1 entry)

以下のコマンドは、MyRad RADIUS プロファイルを表示します。

```
controller# show radius-profile MyRad
```

RADIUS Profile Table

RADIUS Profile Name	:MyRad
Description	:
RADIUS IP	:192.168.100.1
RADIUS Secret	:*****
RADIUS Port	:1812
MAC Address Delimiter	:none

Password Type : shared-secret

関連コマンド [radius-profile \(456 ページ\)](#)

show security-profile

設定されたセキュリティ プロファイルを表示します。

構文

show security-profile <name>

name オプション。表示するプロファイルの名前を指定します。

コマンド モード

特権 EXEC

デフォルト

すべてのセキュリティ プロファイルのリストが表示されます。

用途

このコマンドは、**security-profile** コマンドで作成されたすべてのセキュリティ プロファイルを一覧表示します。または、オプションで引数を指定すると、*name* で指定されたプロファイルの詳細が一覧表示されます。

使用例

以下のコマンドは、設定されているセキュリティ プロファイルを表示します。

```
controller# show security-profile
# show security-profile
```

Profile Name	L2 Mode	Data Encrypt	Firewall Filter
Clear-CP	clear	none	ab10
wpa-psk	wpa-psk	tkip	
wpa2peap	wpa2	ccmp	
wpa2psk	wpa2-psk	ccmp	
wpapeap	wpa	tkip	

Security Profile Table(5)

```
mc1000# show security-profile wpa-psk
Security Profile Table
```

Security Profile Name	: wpa-psk
-----------------------	-----------

```

L2 Modes Allowed           : wpa-psk
Data Encrypt               : tkip
Primary RADIUS Profile Name :
Secondary RADIUS Profile Name :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index       : 1
Re-Key Period (seconds)    : 0
Enable Multicast Re-Key    : off
Enable Captive Portal      : disabled
802.1X Network Initiation  : on
Enable Shared Key Authentication : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Enable Reauthentication    : off
MAC Filtering              : on

```

controller# show security-profile wpapeap

```

Security Profile Name      : wpapsk
L2 Modes Allowed          : wpa-psk
Data Encrypt               : tkip
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
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
Security Profile Table

```



```
Security Profile Name           : wpapeap
L2 Modes Allowed               : wpa
Data Encrypt                   : tkip
Primary RADIUS Profile Name    : snow_ias
Secondary RADIUS Profile Name  :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index          : 0
Re-Key Period (seconds)       : 0
Enable Multicast Re-Key       : off
Enable Captive Portal         : disabled
802.1X Network Initiation     : on
Enable Shared Key Authentication : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Enable Reauthentication       : off
MAC Filtering                 : on
```

関連コマンド [security-profile \(469 ページ\)](#)

show ssl-server

設定されている SSL サーバを表示します。

構文

show ssl-server

コマンド モード

特権 EXEC

デフォルト

すべての SSL サーバのリストが表示されます。

用途

このコマンドは、アクティブなすべての SSL サーバを一覧表示します。

使用例

以下のコマンドは、設定されている SSL サーバを一覧表示します。

```
controller# show ssl-server
SSL Server

Name                : cp-ssl
Server Port         : 10101
User Authentication Protocol : None
Server Lifetime     : 100
Server IP           : 192.168.10.2
Certificate          : controller.pem
RADIUS Profile Name : cp-IAS
Secondary RADIUS Profile Name :
CaptivePortalSessionTimeout : 0
CaptivePortalActivityTimeout : 0
Override RADIUS configurations : off
```

関連コマンド

- [ssl-server radius-profile \(499 ページ\)](#)
- [ssl-server port \(498 ページ\)](#)

show web

Web サーバ キャプティブ ポータル設定情報を表示します。

構文

```
show web custom
show web custom-area
show web login-page
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

show web custom コマンドを使用して、キャプティブ ポータル カスタム モードの IP 範囲を表示します。

show web custom-area コマンドを使用して、web-auth とキャプティブ ポータルのカスタマイズされたファイルを表示します。

show web login-page コマンドを使用して、キャプティブ ポータルと WebAuth でクライアント ログイン時に表示されるページのタイプを表示します。デフォルトのログイン ページが使用されている場合には、**default** という語がコマンドから返されます。

使用例

以下のコマンドを使用すると、使用中のデフォルトのキャプティブ ポータル /WebAuth のログイン ページが表示されます。

```
controller# show web login-page
default
```

次の例では、キャプティブ ポータルに対してカスタマイズされたページを使用するよう指示し、さらに、カスタム ログイン ページの場所を表示します。

```
MC3K-1(config)#
MC3K-1(config)# web custom ?
<attribute> Custom configuration for attribute in captive portal.
MC3K-1(config)# web custom Auth_IP subnet 1.1.1.0 mask 255.255.255.0
MC3K-1(config)# web custom Guest_IP subnet 2.2.2.0 mask 255.255.255.0
MC3K-1(config)# exit
MC3K-1# show web custom ?
<attribute> Displays values of attribute in custom captive
portal con
```

figuration.

MC3K-1# show web custom Auth_IP

1.1.1.0/24

MC3K-1# show web custom Guest_IP

2.2.2.0/24

関連コマンド [web login-page \(519 ページ\)](#)

ssl-server accounting-radius-profile

キャプティブ ポータル アカウントのプライマリとセカンダリの RADIUS サーバを指定します。

構文

```
ssl-server accounting-radius-profile primary <Radius server IP address>
ssl-server accounting-radius-profile secondary <Radius server IP address>
ssl-server no-primary-accounting-radius
ssl-server no-secondary accounting-radius
```

コマンド モード

特権 EXEC

デフォルト

プライマリやセカンダリの RADIUS プロファイルはありません

用途

このコマンドを使用して、キャプティブ ポータル アカウントに使用するプライマリとセカンダリの RADIUS サーバ アドレスを指定します。

使用例

次の例は、プライマリとセカンダリの両方の RADIUS アカウント プロファイルを割り当てた後に、両方の設定を削除します。

```
Master(config)#
Master(config)# ssl-server accounting-radius-profile primary IAS
Master(config)# ssl-server accounting-radius-profile secondary IAS
Master(config)# end
Master#
Master# sh ssl-server
SSL Server
```

Name	: Captive Portal
Server Port	: 10101
User Authentication Protocol	: None
Server Lifetime	: 100
Server IP	: 192.168.106.153
Certificate	:
Primary RADIUS Profile Name	:
Secondary RADIUS Profile Name	:

```
Primary Accounting Radius Server Profile Name : IAS
Secondary Accounting Radius Server Profile Name : IAS
Accounting Interim Interval (seconds) : 600
CaptivePortalSessionTimeout : 0
CaptivePortalActivityTimeout : 0
CaptivePortal Authentication Type : local-radius
Master# (config)
Master#(config)# ssl-server no-primary-accounting-radius
Master# (config)# ssl-server no-secondary-accounting-radius
```

関連コマンド [captive-portal \(390 ページ\)](#)

ssl-server associate

このコマンドは廃止されましたが、本リリースでブロックはされていません。設定されているどの証明書が SSL サーバに対応するのかを指定します。このコマンドを使用する代わりに、Web UI の [Management Server Certificate] ページを使用して、証明書をキャプティブポータル サービスに関連付けます。

構文

```
ssl-server associate pem <certificate>]
ssl-server associate pfx <certificate>]
```

certificate	PEM または PFX 証明書ファイル名を指定します (PEM はファイル拡張子 .pem を使用し、PFX は拡張子 .pfx を使用します)。
-------------	--

コマンドモード

グローバル設定

デフォルト

なし

用途

SSL サーバに使用する PEM または PFX 証明書を指定します。証明書をインポートしてキャプティブポータルで選択することで、Web UI からこれらの証明書を設定します。

使用例

関連コマンド

- [description](#) (421 ページ)
- [ssl-server captive-portal](#) (494 ページ)

CLI コマンド `ssl-server captive-portal-external-URL` を使用して、キャプティブポータル設定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。そして、コマンド `change_mac_state` で、キャプティブポータルボックスの URL を指定します。

ssl-server captive-portal

SSL サーバで使用するキャプティブ ポータル設定を指定します。

構文

```
ssl-server captive-portal activity-timeout <activity-timeout>
ssl-server captive-portal session-timeout <session-timeout>
ssl-server captive-portal authentication-type local
ssl-server captive-portal authentication-type radius override
```

activity-timeout	ユーザが自動的にログオフする前のユーザ セッションでの非アクティブ状態の分数 (0 ~ 60) です。デフォルトでは 0 が設定され、タイムアウトしません。
session-timeout	ステーションのアクティブなセッション用にタイムアウトが開始される前の分数 (0 ~ 1440) です。デフォルトでは 0 が設定され、タイムアウトしません。

コマンドモード

グローバル設定

用途

`ssl-server captive-portal authentication-type local` コマンドを使用すると、コントローラで設定されているタイムアウト値が使用されます (session-timeout と activity-timeout パラメータ)。キャプティブ ポータル認証では、ローカル guest ユーザのみが有効です。

これとは逆に、`ssl-server captive-portal authentication-type radius override` コマンドを使用すると、RADIUS サーバで設定されているタイムアウト値が使用されます (session-timeout と activity-timeout パラメータ)。キャプティブ ポータル認証では、RADIUS サーバ ユーザのみが有効です。

ローカルと RADIUS の両方の値が設定されている場合は、ローカルの値が使用されます。Radius サーバに値が設定されていない場合は、コントローラの値が自動的に使用されます。コントローラに値が設定されていない場合は、RADIUS サーバはチェックされません。

使用例

次の例では、ssl-server ページに 600 分のセッション タイムアウトを設定しています。

```
rao4038 # configure terminal
rao4038(config)# ssl-server captive-portal ?
activity-timeout    Configures activity-timeout for Captive Portal
```


authentication-type Configures authentication type for Radius configurations
session-timeout Configures session timeout period for Captive Portal
rao4038(config)# ssl-server captive-portal session-timeout 600
rao4038(config)#

関連コマンド

- [ssl-server associate \(493 ページ\)](#)
- [ssl-server port \(498 ページ\)](#)
- [ssl-server radius-profile \(499 ページ\)](#)

ssl-server captive-portal-external_URL

[captive-portal-auth-method \(392 ページ\)](#) と一緒に使用して、サードパーティのキャプティブ ポータル認証ソリューションを使用するよう指示します。

構文

`ssl-server captive-portal-external_URL`

コマンドモード

設定モード、セキュリティ モード

デフォルト

フォーティネット キャプティブ ポータル

用途

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。CLI コマンド `captive-portal-auth-method` を使用して、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。CLI コマンド `ssl-server captive-portal-external-URL` を使用して、キャプティブ ポータル設定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。そして、コマンド `change_mac_state` で、キャプティブ ポータル ボックスの URL を指定します。

使用例

以下の例では、次の 2 つのタスクを完了することで、CLI でサードパーティのキャプティブ ポータルを設定します。

CLI コマンド `captive-portal-auth-method` を使用して、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。たとえば、次のように入力します。

```
controller1# configure terminal
controller1(config)# security-profile CPExternal
controller1(config-security)# captive-portal-auth-method
external internal
controller1(config-security)# captive-portal-auth-method ?
<captivePortAuthMethod> Configure captive portal authentication method.
external external
```

```
internal internal
controller1(config-security)# captive-portal-auth-method external
```

CLI コマンド **ssl-server captive-portal-external-URL** を使用して、キャプティブポータル設定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。そして、コマンド **change_mac_state** で、キャプティブポータルボックスのURLを指定します。たとえば、次のように入力します。

```
controller1# configure terminal
controller1(config)# ssl-server ca
captive-portal captive-portal-external-URL
controller1(config)# ssl-server captive-portal-external-URL
controller1(config)# exit
controller1# change_mac_state ?
<ip-address> Enter the Client IP Address.
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 on ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 on ftp_only
Configure a Radius Server for Captive Portal Authentication
© 2010 Fortinet, Inc. Captive Portals for Temporary Users 169
4.1 Beta
<CR>
controller1# change_mac_state 172.18.19.14 on ftp_only
controller1#
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 off ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 off
controller1
```

関連コマンド

- [captive-portal-auth-method \(392 ページ\)](#)
- [change_mac_state \(418 ページ\)](#)

ssl-server port

SSL サーバの TCP ポート番号を指定します。

構文

`ssl-server port <port-number>`

port-number 1024 ~ 65,535 の範囲の TCP ポート番号。

コマンド モード

グローバル設定

デフォルト

SSL サーバのデフォルトのポート番号は 10101 です。

用途

SSL サーバの TCP ポート番号を指定します。

使用例

以下のコマンドを指定すると、SSL サーバのポート番号が 12345 と指定されます。

```
controller(config)# ssl-server port 12345
controller(config)#
```

関連コマンド

- [ssl-server associate \(493 ページ\)](#)
- [ssl-server captive-portal \(494 ページ\)](#)
- [ssl-server radius-profile \(499 ページ\)](#)

ssl-server radius-profile

RADIUS サーバ パラメータが設定されている RADIUS プロファイル名を設定します。

構文

```
ssl-server radius-profile primary <profile-name>
ssl-server radius-profile secondary <profile-name>
ssl-server no-1st-radius
ssl-server no-2nd-radius
```

profile-name RADIUS サーバの設定情報が含まれるファイルの名前。32 文字以下の英数字で、スペースは使用できません。

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドは、SSL サーバで使用されるプライマリまたはセカンダリ RADIUS サーバ パラメータを設定する RADIUS プロファイル名を指定します。

ssl-server no-1st-radius コマンドを使用すると、SSL サーバで使用する前に設定されたプライマリ RADIUS プロファイルが無効になります。

ssl-server no-2nd-radius コマンドを使用すると、SSL サーバで使用する前に設定されたセカンダリ RADIUS プロファイルが無効になります。

使用例

このコマンドを指定すると、プライマリ RADIUS サーバ設定プロファイル *main* を使用するように SSL サーバが設定されます。

```
controller(config)# ssl-server radius-profile primary main
controller(config)#
```

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [ssl-server associate \(493 ページ\)](#)
- [ssl-server captive-portal \(494 ページ\)](#)
- [ssl-server port \(498 ページ\)](#)

ssl-server cna-bypass

Apple の CNA のサポートを有効または無効にします。

構文 `ssl-server cna-bypass [on | off]`

**コマンド
モード** グローバル設定

デフォルト オフ (無効)

用途 有効にすると、Apple 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。

使用例 以下のコマンドは、Apple CNA バイパスを有効にします。

```
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
Configuring Fortinet Captive Portal 239
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

関連コマンド

- [radius-profile \(456 ページ\)](#)
- [ssl-server associate \(493 ページ\)](#)
- [ssl-server captive-portal \(494 ページ\)](#)
- [ssl-server port \(498 ページ\)](#)

static-wep key

固定の WEP キーを設定します。

構文

```
static-wep key <key>  
no static-wep key
```

key

- WEP64 では、キーは 5 つの ASCII 文字または 10 文字の 16 進数のキーになります。
- WEP128 では、キーは 13 の ASCII 文字または 26 文字の 16 進数となります。

コマンドモード

セキュリティ プロファイル設定

デフォルト

なし

用途

802.11 WEP (有線と同様のプライバシー) では、モバイル マシンとアクセス ポイント間のデータで MAC レベルの暗号化が利用されます。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。

WEP64 (WEP40 と呼ばれます) は、より広範に使用されており、以下を含むキーが使用されます。

- 10 の 16 進数文字 (つまり、0 ~ 9、a ~ f、A ~ F)。使用例 0x0123456789
- 5 の ASCII 文字 (すべてのキーボード文字)。使用例 01234 や mykey

WEP128 は広範には利用されていませんが、さらにセキュリティが強化されています。以下を含むキーが使用されます。

- 26 の 16 進数文字 (つまり、0 ~ 9、a ~ f、A ~ F)。使用例
0xa0a1a2a3a4a5a6a7a8a9aaabac や 0x12345678901234567890abcdef
- 13 の ASCII 文字 (すべてのキーボード文字)。例 : my-secret-key

`no static-wep key` コマンドを使用して、固定 WEP キーを無効にします。



16 進数キーを使用する場合、接頭辞 0x をキーの前に付ける必要があります。接頭辞 0x により、システムは 16 進数のキーが入力されることを認識します。

使用例

以下のコマンドは、`wpass` の WEP キーを指定します。

```
controller(config-security)# static-wep key wpass  
controller(config-security)#
```

関連コマンド

- [encryption-modes wep128 \(425 ページ\)](#)
- [encryption-modes wep64 \(426 ページ\)](#)
- [static-wep key-index \(504 ページ\)](#)

static-wep key-index

固定 WEP キーのインデックス位置を設定します。

構文

`static-wep key-index <position>`

position 固定 WEP キー インデックス位置。*position* は 1 ～ 4 の範囲になります。

コマンド モード

セキュリティ プロファイル設定

デフォルト

用途

このコマンドは、ユーザ ステーション キー管理プロファイルで設定できる 4 つの固定 WEP キーの内のいずれかを使用するように指定します。キー インデックス機能により、ユーザ プログラムで 4 つのキー設定が使用できる場合にも相互運用できるようになります。

使用例

以下のコマンドを指定すると、3 番目の WEP キーが使用されることになります。

```
controller(config-security)# static-wep key-index 3
controller(config-security)#
```

関連コマンド

- [static-wep key \(502 ページ\)](#)
- [encryption-modes wep128 \(425 ページ\)](#)
- [encryption-modes wep64 \(426 ページ\)](#)
- [security-profile \(469 ページ\)](#)

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。

構文

tunnel-termination <PEAP/TTLS>

コマンド モード

セキュリティ プロファイル設定

デフォルト

ターミネーションはオフです。

用途

トンネル ターミネーションによって、コントローラの PEAP/TTLS 外部セッションのターミネートが可能になります。内内部 MSCHAPv2 802.1x は、バックエンド RADIUS サーバによって処理されます。これは、RADIUS サーバが PEAP または TTLS をサポートしていない場合に便利です。

使用例

以下のコマンドは、トンネル ターミネーションを無効にします。

```
controller(config-security)# no tunnel-termination (peap/ttls)
controller(config-security)#
```



以下の L2 モードは、PEAP または TTLS 認証プロトコルでのみ、サポートされています。

- 802.1x
 - WPA
 - WPA2
 - 混合
-

vpn client

コントローラと Network Manager サーバの間の VPN 接続のプロパティを設定できます。

構文

vpn client

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、Network Manager アプライアンスに対する VPN 設定のプロパティを表示、設定します。この設定から、いくつかのサブコマンドが実行されます。

使用例

```
default(15)# configure terminal
default(15)(config)# vpn client
default(15)(config-vpn-client)# ?
do (10) Executes an IOSCLI command.
end (10) Save changes, and return to privileged EXEC mode.
exit (10) Save changes, and return to global configuration mode.
no (10) Disables various parameters.
vpn-client-state (10) Enables VPN Client.
vpn-server-ip (10) Configures the VPN Server IP address.
vpn-server-port (10) Configures the VPN Server port number.
default(15)(config-vpn-client)#
```

関連コマンド

- [\(config-vpn-client\) vpn-client-state \(507 ページ\)](#)
- [\(config-vpn-client\) vpn-server-ip \(508 ページ\)](#)
- [\(config-vpn-client\) vpn-server-port \(509 ページ\)](#)

(config-vpn-client) vpn-client-state

コントローラと Network Manager サーバの間の VPN 通信を有効または無効にできます。

構文

```
(config-vpn-client) vpn-client-state  
(config-vpn-client) no vpn-client-state
```

コマンド モード

VPN クライアント設定

デフォルト

無効

用途

このコマンドを使用して、Network Manager サーバの VPN 接続をアクティブまたは非アクティブにします。

使用例

以下の例は、VPN サーバを有効にし、その後に無効にします。

```
default(15)(config-vpn)# vpn-client-state  
default(15)(config-vpn)#  
default(15)(config-vpn)# no vpn-client-state  
default(15)(config-vpn)#
```

関連コマンド

- [vpn client \(506 ページ\)](#)
- [\(config-vpn-client\) vpn-server-ip \(508 ページ\)](#)
- [\(config-vpn-client\) vpn-server-port \(509 ページ\)](#)

(config-vpn-client) vpn-server-ip

VPN が有効な Network Manager サーバの IP アドレスを設定できます。

構文

(config-vpn-client) vpn-server-ip <IP>

IP IP を指定します (255.255.255.255 という形式)。

コマンド モード

VPN クライアント設定

デフォルト

なし

用途

このコマンドを使用して、VPN サーバの IP アドレスを指定します。

使用例

```
default(15)(config-vpn-client)# vpn-server-ip 10.9.8.7
default(15)(config-vpn-client)# end
```

関連コマンド

- [vpn client \(506 ページ\)](#)
- [\(config-vpn-client\) vpn-client-state \(507 ページ\)](#)
- [\(config-vpn-client\) vpn-server-port \(509 ページ\)](#)

(config-vpn-client) vpn-server-port

VPN サービスに使用するポートを指定できます。

構文

```
(config-vpn-client) vpn-server-port <port>
```

Port ポートを指定します (0 ～ 65535 の任意の整数)。

コマンド モード

VPN クライアント設定

デフォルト

1194

用途

このコマンドを使用して、VPN クライアント設定が使用するポートを指定します。

使用例

```
default(15)(config-vpn-client)# vpn-server-port 1194
default(15)(config-vpn-client)# end
```

関連コマンド

- [vpn client \(506 ページ\)](#)
- [\(config-vpn-client\) vpn-client-state \(507 ページ\)](#)
- [\(config-vpn-client\) vpn-server-ip \(508 ページ\)](#)

vpn server

VPN サーバのプロパティを設定できます。

構文

vpn server

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、コントローラでホスティングされる VPN 設定のプロパティを表示、設定します。この設定から、いくつかのサブコマンドが実行されます。

使用例

```
default(15)# configure terminal
default(15)(config)# vpn server
default(15)(config-vpn)# ?
    do (10) Executes an IOSCLI command.
    encryption (10) Enables Encryption.
    end (10) Save changes, and return to privileged EXEC mode.
    exit (10) Save changes, and return to global configuration mode.
    ip-pool (10) Configures the IP Pool address.
    no (10) Disables various parameters.
    port (10) Configures the VPN Server port number.
    subnet-mask (10) Configures the subnet mask.
    vpn-server-ip (10) Configures the VPN Server IP address.
    vpn-server-state (10) Enables VPN Server.
default(15)(config-vpn)#
```

関連コマンド

- [\(config-vpn\) encryption \(511 ページ\)](#)
- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)

(config-vpn) encryption

VPN 暗号化を有効または無効にできます。

構文

(config-vpn) encryption

コマンド モード

VPN 設定

デフォルト

無効

用途

このコマンドを使用して、コントローラの VPN 設定の暗号化をアクティブまたは非アクティブにします。

使用例

以下の例では、暗号化を有効にし、その後に無効にします。

```
default(15)(config-vpn)# encryption
default(15)(config-vpn)#
default(15)(config-vpn)# no encryption
default(15)(config-vpn)#
```

関連コマンド

- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)

(config-vpn) ip-pool

VPN サービスに使用する IP ポートを指定できます。

構文

```
(config-vpn) ip-pool <IP>
```

IP IP 範囲を指定します (255.255.255.255 という形式)。

コマンド モード

VPN 設定

デフォルト

192.168.0.0

用途

このコマンドを使用して、VPN 設定が使用できる IP の範囲を指定します。

使用例

```
default(15)(config-vpn)# ip-pool 192.168.100.0  
default(15)(config-vpn)# end
```

関連コマンド

- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) encryption \(511 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)

(config-vpn) port

VPN サービスに使用するポートを指定できます。

構文

(config-vpn) port <port>

Port ポートを指定します (0 ~ 65535 の任意の整数)。

コマンド モード

VPN 設定

デフォルト

1194

用途

このコマンドを使用して、VPN 設定が使用するポートを指定します。

使用例

```
default(15)(config-vpn)# port 1194
default(15)(config-vpn)# end
```

関連コマンド

- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) encryption \(511 ページ\)](#)
- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)

(config-vpn) subnet-mask

VPN サービスに使用するサブネット マスクを指定できます。

構文

```
(config-vpn) subnet-mask <netmask>
```

Netmask IP を指定します (255.255.255.255 という形式)。

コマンド モード

VPN 設定

デフォルト

255.255.0.0

用途

このコマンドを使用して、VPN 設定が使用するサブネット マスクを指定します。

使用例

```
default(15)(config-vpn)# subnet-mask 255.255.255.0
default(15)(config-vpn)# end
```

関連コマンド

- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) encryption \(511 ページ\)](#)
- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)

(config-vpn) vpn-server-ip

VPN サービスに使用する IP アドレスを設定できます。

構文

(config-vpn) vpn-server-ip <IP>

IP IP を指定します (255.255.255.255 という形式)。

コマンド モード

VPN 設定

デフォルト

なし

用途

このコマンドを使用して、VPN サーバの IP アドレスを指定します。

使用例

```
default(15)(config-vpn)# vpn-server-ip 10.9.8.7
default(15)(config-vpn)# end
```

関連コマンド

- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) encryption \(511 ページ\)](#)
- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-state \(516 ページ\)](#)

(config-vpn) vpn-server-state

VPN サービスを有効または無効にできます。

構文

```
(config-vpn) vpn-server-state  
(config-vpn) no vpn-server-state
```

コマンド モード

VPN 設定

デフォルト

無効

用途

このコマンドを使用して、コントローラの VPN サービスをアクティブまたは非アクティブにします。

使用例

以下の例は、VPN サーバを有効にし、その後に無効にします。

```
default(15)(config-vpn)# vpn-server-state  
default(15)(config-vpn)#  
default(15)(config-vpn)# no vpn-server-state  
default(15)(config-vpn)#
```

関連コマンド

- [vpn server \(510 ページ\)](#)
- [\(config-vpn\) encryption \(511 ページ\)](#)
- [\(config-vpn\) ip-pool \(512 ページ\)](#)
- [\(config-vpn\) port \(513 ページ\)](#)
- [\(config-vpn\) subnet-mask \(514 ページ\)](#)
- [\(config-vpn\) vpn-server-ip \(515 ページ\)](#)

web custom

キャプティブ ポータル カスタム モードを設定します。

構文

```
web custom CaptivePortal1 landing-file-name<name.html> success-file-name
<name.html>
web custom CaptivePortal2 landing-file-name<name.html> success-file-name
<name.html>
```

コマンド モード

設定モード

デフォルト

なし

用途

web custom を使用して、最大 4 つのキャプティブ ポータル カスタム ファイル名を設定できます。

[web login-page \(519 ページ\)](#) コマンドを使用して、Web 認証とキャプティブ ポータルのデフォルトまたはカスタムのログイン ページを選択します。[web custom \(517 ページ\)](#) コマンドで、カスタム ページの名前を指定します。**show web custom** コマンドを使用して、キャプティブ ポータル /WebAuth 実装で使用されるファイルを表示します。デフォルトのログイン ページを使用している場合は、このコマンドで **empty.html** と **empty.gif** ファイルが表示されます。

使用例

以下のコマンドを使用すると、使用中のデフォルトのキャプティブ ポータル /WebAuth のログイン ページが表示されます。

```
controller# show web login-page
default
```

次の例では、キャプティブ ポータルに対してカスタマイズされたファイルを使用するよう指示し、さらに、カスタム ログイン ページの場所を表示します。

```
MC3K-1# configure terminal
MC3K-1(config)# web custom ?
CaptivePortal1      Custom configuration for captive portal 1
CaptivePortal2      Custom configuration for captive portal 2
MC3K-1(config)# web custom captiveportal2 ?
landing-file-name   subnet
```

```

MC3K-1(config)# web custom CaptivePortal2 landing-file-name landing.html
success-file-name success.html
MC3K-1 (config) web custom CaptivePortal2 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
capti
ve portal.
login-page            Displays the type of login page used for web-auth
and cap
tive portal.
MC3K-1# show web custom
Insufficient parameters for command
MC3K-1# show web custom-area
Html Files
total 16
-rw-rw-rw-   1 root    root        2607 Jul 13 16:26 page20K.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

```

関連コマンド [show web \(489 ページ\)](#)

web login-page

デフォルトまたはカスタムのいずれかのキャプティブ ポータル /WebAuth ログイン ページを選択します。

構文

```
web login-page default
web login-page custom
```

コマンドモード

グローバル設定モード

デフォルト

フォーティネット デフォルト ログイン ページ

用途

`web login-page` コマンドを使用して、Web 認証とキャプティブ ポータルのデフォルトまたはカスタムのログイン ページを選択します。[web custom \(517 ページ\)](#) コマンドで、カスタム ページの名前を指定します。`show web custom` コマンドを使用して、キャプティブ ポータル /WebAuth 実装で使用されるファイルを表示します。デフォルトのログイン ページを使用している場合は、このコマンドで `empty.html` と `empty.gif` ファイルが表示されます。



カスタム オプションを使用するには、Web UI を使用して一般ファイルをダウンロードして変更し、カスタマイズした .html と .gif ファイルをアップロードする必要があります。[Detailed] >

[Maintenance] > [Captive Portal] エリアで、[Customization] リンクと [Get Files] ボタンをクリックして、ファイルを取得します。一般ファイルを変更したら、[Import Files] リンクを使用してファイルをアップロードします。ページを有効にするには、`web login-page custom` コマンドを使用するか、[Customization] リンクで手順 2 に進み、モードを変更して [Customized] ラジオ ボタンを選択します。

`web login-page default` を使用して、デフォルトのログイン ページを変更します。

関連コマンド

- [web custom \(517 ページ\)](#)
- [show web \(489 ページ\)](#)

10 ESSID コマンド

本章では、ESS の作成や管理に使用するコマンドについて説明します。Radius アカウント、リモート AP、VLAN の作成などの機能を有効または無効にするコマンドについても説明します。また、独自の要件に対応するためにデフォルトのブロードキャスト設定を調整する多くのコマンドについても説明します E(z)RF Network Manager で作成されたプロファイルは、コントローラでは変更 / 削除できません。CLI コマンド **nms-server unregister** を使用すると、Network Manager からコントローラの登録を解除できます。設定の登録を解除すると、コントローラがプロファイルのコピーの所有者になり、Network Manager で作成されたプロファイルを編集または削除できるようになります。

- [accounting interim-interval \(523 ページ\)](#)
- [accounting primary-radius \(524 ページ\)](#)
- [accounting secondary-radius \(526 ページ\)](#)
- [ap-discovery join-ess \(528 ページ\)](#)
- [ap-discovery join-virtual-ap \(529 ページ\)](#)
- [apsd \(533 ページ\)](#)
- [band-steering-mode \(535 ページ\)](#)
- [band-steering-timeout \(537 ページ\)](#)
- [base-tx-rates \(539 ページ\)](#)
- [beacon dtim-period \(541 ページ\)](#)
- [beacon period \(542 ページ\)](#)
- [bssid \(543 ページ\)](#)
- [calls-per-bss \(544 ページ\)](#)
- [countermeasure \(545 ページ\)](#)
- [dataplane \(546 ページ\)](#)
- [edited-bssid \(548 ページ\)](#)
- [ess-ap \(549 ページ\)](#)
- [essid \(550 ページ\)](#)
- [gre name \(551 ページ\)](#)

- [l2bridge airf](#) (552 ページ)
- [l2bridge appletalk](#) (553 ページ)
- [l2bridge ipv6](#) (554 ページ)
- [multicast-enable](#) (555 ページ)
- [multicast-mac-transparency](#) (556 ページ)
- [overflowfrom-essprofile](#) (557 ページ)
- [publish-ssid](#) (559 ページ)
- [security-profile](#) (560 ページ)
- [show edited-bssid](#) (562 ページ)
- [show ess-ap](#) (561 ページ)
- [show ssid](#) (563 ページ)
- [ssid](#) (566 ページ)
- [supported-tx-rates](#) (567 ページ)
- [tunnel-type](#) (569 ページ)
- [virtual-port](#) (570 ページ)
- [vlan name](#) (571 ページ)
- [wireless-to-wireless-isolation](#) (572 ページ)

accounting interim-interval

コントローラが Interim-Update レコードを RADIUS アカウンティング サーバへ送信する前に経過する時間を指定します。

構文

`accounting interim-interval <value>`

value Interim-Update レコードが送信される前に経過する秒数。間隔は 600 ～ 3,600 秒 (10 分 ～ 10 時間) である必要があります。

コマンドモード

ESSID 設定

デフォルト

デフォルトの暫定的な送信間隔の値は 3,600 秒です。

用途

RADIUS アカウンティングが有効になっている場合、コントローラは Access-Accept 応答を RADIUS サーバから受信した後に、RADIUS アカウンティング サーバへ Accounting-Start レコードを送信します。クライアント セッションがタイムアウトするか、あるいはクライアントが分離されると、コントローラは RADIUS サーバへ Accounting-Stop レコードを送信します。Access-Accept 応答に Acct-Interim-Interval 属性が含まれていた場合、コントローラはクライアント セッションの間、`accounting interim-interval` コマンドで設定された間隔で Interim-Update レコードを送信します。

使用例

以下のコマンドは、アカウンティング サーバへの暫定的な送信間隔を 1,800 秒 (30 分) に設定します。

```
controller(config-ssid)# accounting interim-interval 1800
controller(config-ssid)#
```

関連コマンド

- [accounting primary-radius](#) (524 ページ)
- [accounting secondary-radius](#) (526 ページ)

accounting primary-radius

プライマリ RADIUS アカウンティング サーバを指定します。

構文

```
accounting primary-radius <profile>  
no accounting-radius all
```

profile RADIUS アカウンティング サーバ プロファイルの名前で、
radius-profile コマンドにより指定されます。

コマンド モード

ESSID 設定

デフォルト

コントローラとプライマリ RADIUS アカウンティング サーバとの間の通信は、デフォルトで無効に設定されています。

用途

accounting primary-radius コマンドを使用して、コントローラとプライマリ RADIUS アカウンティング サーバ間の通信を設定し有効にします。

RADIUS アカウンティングが有効になっている場合、コントローラは 802.1X の 使用を認証するクライアントの RADIUS アカウンティング サーバへ、アカウンティング レコードを送信します (トラッキングされるアカウンティング属性の一覧を表示するには、『**FortiWLC (SD) 設定ガイド**』の「RADIUS アカウンティングの設定」と「複数の ESSID の設定」を参照してください)。



この設定では、RADIUS 認証サーバを使用しないでください。RADIUS アカウンティング サーバは、ポート 1812 ではなく 1813 を使用するため、RADIUS 認証サーバは動作しません。

IP アドレス、ポート (1813 がアカウンティングの標準ポートです)、秘密キーなどの RADIUS アカウンティング サーバの設定情報は、**radius-profile** コマンドを使用して指定されます。

no accounting-radius all コマンドを使用して、プライマリ RADIUS アカウンティング サーバを無効にします。

使用例

以下のコマンドにより、プライマリ RADIUS アカウンティングサーバの *main-acct* プロファイルにサーバ情報が設定されます。

```
controller(config-ssid)# accounting primary-radius main-acct  
controller(config-ssid)#
```

関連コマンド

- [accounting interim-interval](#) (523 ページ)
- [radius-profile](#) (456 ページ)
- [accounting secondary-radius](#) (526 ページ)

accounting secondary-radius

セカンダリ RADIUS アカウンティング サーバを指定します。

構文

```
accounting secondary-radius <profile>  
no accounting-radius secondary  
no accounting-radius all
```

profile RADIUS サーバ プロファイルの名前で、radius-profile コマンドにより指定されます。

コマンドモード

ESSID 設定

デフォルト

コントローラとセカンダリ RADIUS アカウンティング サーバとの間の通信は、デフォルトで無効に設定されています。

用途

プライマリ RADIUS アカウンティング サーバがオフラインの場合に、コントローラがアカウンティング レコードを送信するセカンダリ RADIUS アカウンティング サーバを指定できます。accounting secondary-radius コマンドを使用して、セカンダリ RADIUS アカウンティング サーバとの通信を有効にします。

no accounting-radius secondary または no accounting-radius all を使用して、セカンダリ RADIUS アカウンティング サーバとの通信を無効にします。

RADIUS アカウンティングが有効になっている場合、コントローラは 802.1X を使用して認証するクライアントの RADIUS アカウンティング サーバへ、アカウンティング レコードを送信します (トラッキングされるアカウンティング属性の一覧を表示するには、『**FortiWLC (SD) 設定ガイド**』の「RADIUS アカウンティングの設定」と「複数の ESSID の設定」を参照してください)。

IP アドレス、ポート (1813 がアカウンティングの標準ポートです)、秘密キーなどの RADIUS アカウンティング サーバの設定情報は、radius-profile コマンドを使用して指定されます。

使用例

以下のコマンドにより、セカンダリ RADIUS アカウンティングサーバの backup-acct プロファイルにサーバ情報が設定されます。

```
controller# configure terminal  
controller(config) essid eng
```



```
controller(config-ssid)# accounting secondary-radius backup-acct  
controller(config-ssid)#
```

関連コマンド

- [accounting interim-interval](#) (523 ページ)
- [radius-profile](#) (456 ページ)
- [accounting primary-radius](#) (524 ページ)

ap-discovery join-ess

新しいアクセス ポイントが ESSID に自動的に参加し、その ESSID のパラメータを適用するのかを設定します。

構文

```
ap-discovery join-ess  
no ap-discovery join-ess
```

コマンド モード

ESSID 設定

デフォルト

無効

用途

デフォルト設定では、**join-ess-on-discovery** コマンドは有効になっています。つまり、アクセス ポイントは自動的に ESSID に参加し、BSS が自動的に作成されます。新しいアクセス ポイントが WLAN に接続されると、すべての ESSID を確認して、**ap-discovery join-ess** が有効になっているすべての ESSID に参加します。ESSID を作成すると、アクセス ポイントは新しい ESSID に参加します。

WLAN の設定が完了したら **ap-discovery join-ess** を無効にし、新しいアクセス ポイントが設定を変更しないようにします。アクセス ポイントの小規模なサブセットでのみ通知する新しい ESS を追加する場合は、**ap-discovery join-ess** を無効にして ESS を作成し、ESS-AP マッピングを手動で追加するほうが簡単です。

no フォームを使用して、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。**no** フォームが使用されている場合は、BSSID を手動で割り当てる必要があります。

使用例

以下のコマンドは、**ap-discovery join-ess** を無効にし、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# configure terminal  
controller(config) essid eng  
controller(config-essid)# no ap-discovery join-ess  
controller(config-essid)#
```

関連コマンド

- [ssid \(566 ページ\)](#)
- [show essid \(563 ページ\)](#)

ap-discovery join-virtual-ap

同一チャネルで検出されたアクセス ポイントが同じ BSSID を共有し、仮想セルを形成できるようにします。

構文 `ap-discovery join-virtual-ap`
 `no ap-discovery join-virtual-ap`

**コマンド
モード** ESSID 設定

デフォルト 無効

用途 デフォルトでは、ESSID を作成すると `ap-discovery join-virtual-ap` コマンドが有効になります。これによって、同じ BSSID を共有する同一チャネル上のアクセス ポイントのグループである、仮想セルを形成できます。`ap-discovery join-virtual-ap` コマンドが無効であると、同一チャネル上のアクセス ポイントは同じ BSSID を共有できず、仮想セルが形成されなくなります。`ap-discovery join-virtual-ap` コマンドが無効であると、各アクセス ポイントに固有の BSSID が割り当てられます。



このコマンドのステータスは、新しい ESS-AP マッピングが作成された場合にのみ評価されます。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。

`no` フォームを使用すると、同一チャネル上のアクセス ポイントによる BSSID の共有が無効になります。以下に、`ap-discovery join-virtual-ap` を無効にするいくつかの例を示します。

- 仮想セルを作成したくない場合 (つまり、各アクセス ポイントを固有の BSSID にする場合)。
- BSSID でアクセス ポイントを認識する必要がある場合。

使用例 以下のコマンドは、`ap-discovery join-virtual-ap` を無効にし、同一チャネル上のアクセス ポイントが同じ BSSID を共有しないようにします。

```
controller# configure terminal
controller(config) essid eng
controller(config-essid)# no ap-discovery join-virtual-ap
```

```
controller(config-ssid)#
```

関連コマンド

- [ess-ap \(549 ページ\)](#)
- [show ssid \(563 ページ\)](#)

ap-vlan priority

ブリッジ VLAN と一緒に使用することで、VLAN の最上位の優先度をタグ付けします。

構文

```
ap-vlan-priority  
no ap-vlan-priority
```

コマンド モード

ESSID 設定

デフォルト

なし

用途

ブリッジ モードの ESS プロファイルは、AP300、AP400、および AP1000 モデルでサポートされています。**dataplane** コマンドで、ESS プロファイルがブリッジされていることを指示します。次に、**ap-vlan-tag** コマンドでプロファイルに VLAN タグを設定し、さらに、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。**ap_vlan_priority** コマンドは、タグ付けされた VLAN の優先度を高めます。この設定によって、受信する VLAN 802.1p データ パケットを WMM AC にアクセス ポイントが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、デフォルトでこれが無効になり、AP は常に IPV4 パケットの DSCP による受信パケットからいずれかの WMM AC へのマッピングを適用します。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 の優先度を適用します。

使用例

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
```

関連コマンド

- [ap-vlan-tag \(532 ページ\)](#)
- [dataplane \(546 ページ\)](#)

ap-vlan-tag

ブリッジ VLAN にタグを割り当てます。

構文

```
ap-vlan-tag <number>  
no ap-vlan-tag <number>
```

コマンド モード

ESSID 設定

デフォルト

なし

用途

ブリッジ モードの ESS プロファイルは、AP300、AP400、および AP1000 モデルでサポートされています。**dataplane** コマンドで、ESS プロファイルがブリッジされていることを指示します。次に、**ap-vlan-tag** コマンドでプロファイルに VLAN タグを設定し、さらに、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。**ap-vlan priority** コマンドは、タグ付けされた VLAN の優先度を高めます。

使用例

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
```

関連コマンド

- [ap-vlan priority \(531 ページ\)](#)
- [dataplane \(546 ページ\)](#)

apsd

ESS で APSD がオンになっていると、AP は、デバイスが省電力を使用している間にフレームをバッファし、デバイスがオンラインに戻ったときにフレームを転送します。

構文

```
apsd-support  
no apsd-support
```

コマンド モード

ESSID 設定

デフォルト

ESS および APSD サポートごとに設定される APSD 設定は、デフォルトで**オン**になります。

用途

WMM は、これまでの省電力機能を拡張したもので、パフォーマンスの向上と転送のレイテンシの最小化し、省電力化を可能にします。そのために、U-APSD 対応のステーションは、非定期的サービス期間 (SP) に AP300 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 対応のステーションの場合、ステーションが省電力モードの場合には、AP300 が U-APSD とネゴシエーションし、U-APSD を使用してデータを転送します。デバイスが省電力モードから復帰すると、アップリンクデータ フレームによって、トリガ / 送信可能なキューにバッファされたフレーム を AP300 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。**show station** コマンドを実行して、APSD 設定を確認します。

使用例

以下の例では、APSD という名前の ESSID の WMM-APSD サポートをオフにします。

```
default# configure terminal  
default(config)# essid apsd  
default(config-essid)# no apsd-support  
default(config-essid)# end  
default(config)# end  
default# show station 802.11 mac-address 00:00:4c:5a:e9:94  
Station Database 802.11 Table  
MAC Address           : 00:00:4c:5a:e9:94  
AP ID                  : 56  
AP Name                : AP-56  
Interface Index        : 0
```

ESSID	: pk1
BSSID	: 00:0c:e6:f6:bf:d3
Virtual Port	: 06:0b:0d:5a:e9:94
RF Band	: 802.11g
Capabilities	: wmm,apsd
Last Associated time	: 11/11/2009 16:38:33
Last Handoff time	: 11/11/2009 16:33:08
Neighboring AP Count	: 0
Transmitted Throughput	: 530
Received Throughput	: 105
Current RSSI	: -43
Loss Percentage	: 76
Channel Utilization	: 0

band-steering-mode

デュアル バンド対応クライアントに対する ESS トラフィックを、バンド A またはバンド N に送信します。

構文

```
band-steering-mode a-steering  
band-steering-mode n-steering  
band-steering-mode disable
```

コマンド モード

設定 ESSID

デフォルト

デフォルトでは、バンド ステアリングは無効です。

用途

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のバランスを調整します。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、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、データのみクライアントを A バンドに移動できるため、高速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、5 GHz 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、5 GHz 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。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] フィールドを **on** に設定します ([essid \(550 ページ\)](#) コマンドを参照)。

使用例

以下の例では、バンド ステアリングを BandSteeringTest という名前の既存の ESS の A チャンネルに設定し、バンド ステアリングのタイムアウトを 7 秒に設定します ([band-steering-timeout \(537 ページ\)](#) を参照)。

```
DemoController# configure terminal  
DemoController(config)# essid bandSteeringTest  
DemoController(config-essid)# band-steering-mode a-steering  
DemoController(config-essid)# band-steering-timeout 7  
DemoController(config-essid)# end
```

関連コマンド

- [*band-steering-timeout*](#) (537 ページ)
- [*ssid*](#) (550 ページ)

band-steering-timeout

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。

構文 `band-steering-timeout <seconds>`

コマンドモード 設定 ESSID

デフォルト デフォルトは 5 秒です。

用途 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。

使用例 以下の例では、Bandsteeress という名前の ESS について、remote-ap-enable を設定し、バンドステアリングを A チャンネルに設定し、ステアリング タイムアウトを 10 秒に設定します。

```
default# configure terminal
default(config)# essid Bandsteeress
default(config-ssid)# dataplane
default(config-ssid)# remote-ap-enable
default(config-ssid)# band-steering-mode a-steering
default(config-ssid)# band-steering-timeout 10
default(config-ssid)# end
```

以下の例では、バンドステアリングを BandSteeringTest という名前の既存の ESS の A チャンネルに設定し ([band-steering-mode \(535 ページ\)](#) を参照)、バンドステアリングのタイムアウトを 7 秒に設定します。

```
DemoController# configure terminal
DemoController(config)# essid bandSteeringTest
DemoController(config-ssid)# band-steering-mode a-steering
DemoController(config-ssid)# band-steering-timeout 7
DemoController(config-ssid)# end
```

関連コマンド

- [band-steering-mode](#) (535 ページ)
- [essid](#) (550 ページ)

base-tx-rates

基本伝送速度 (Mbps) を設定します。

構文

```
base-tx-rates 802.11a all
base-tx-rates 802.11a <rate>
base-tx-rates 802.11b all
base-tx-rates 802.11b <rate>
base-tx-rates 802.11bg all
base-tx-rates 802.11bg <rate>
base-tx-rates 802.11g all
base-tx-rates 802.11g <rate>
base-tx-rates 802.11bg all
base-tx-rates 802.11bg <rate>
base-tx-rates 802.11bgn all
base-tx-rates 802.11bgn <rate>
base-tx-rates 802.11an all
base-tx-rates 802.11an <rate>
```

デフォルト値は以下のとおりです。

- B サポート対象伝送速度 (Mbps): 1,2,5,11
- B 基本伝送速度 (Mbps): 11
- A サポート対象伝送速度 (Mbps): 6,9,12,18,24,36,48,54
- A 基本伝送速度 (Mbps): 6,12,24
- G サポート対象伝送速度 (Mbps): 6,9,12,18,24,36,48,54
- G 基本伝送速度 (Mbps): 6,9,12,18,24,36,48,54
- BG サポート対象伝送速度 (Mbps): 1,2,5,11,6,9,12,18,24,36,48,54
- BG 基本伝送速度 (Mbps): 11
- BGN サポート対象伝送速度 (Mbps): 1,2,5,11,6,9,12,18,24,36,48,54
- BGN 基本伝送速度 (Mbps): 11
- BGN サポート対象 HT 伝送速度 (MCS): 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
- BGN 基本 HT 伝送速度 (MCS): なし
- AN サポート対象伝送速度 (Mbps): 6,9,12,18,24,36,48,54
- AN 基本伝送速度 (Mbps): 6,12,24
- AN サポート対象 HT 伝送速度 (MCS): 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
- AN 基本 HT 伝送速度 (MCS): なし

コマンド モード

ESS 設定

用途

基本速度を設定することで、アクセス ポイントに接続する際にすべてのクライアントがサポートしなければならない必須の速度が指定されます。引数 **all** が使用される場合を除いて、各基本伝送速度を変更（追加または削除）する場合は、個別のコマンドで実装される必要があります。つまり、単一のコマンドでいくつかの基本速度を設定することはできません（たとえば、**base-tx-rate 802.11bg 1 2 11** は無効です）。

コマンドの **no** フォームを使用して、指定した基本速度を無効にします。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。

使用例

以下のコマンドは、802.11bg の基本伝送速度を 11 Mbps に設定します。

```
controller# configure terminal
controller(config) essid eng
default(config-essid)# base-tx-rate 802.11bg 11
```

以下のコマンドは、802.11a の基本伝送速度をすべての速度（1、2、5.5、11、6、9、12、18、24、36、48、54 Mbps）をサポートするように設定します。

```
controller# configure terminal
controller(config) essid eng
default(config-essid)# base-tx-rate 802.11a all
```

関連コマンド

[*supported-tx-rates*](#) (567 ページ)

beacon dtim-period

ビーコンを送信する間隔を設定します。

構文

```
beacon dtim-period <period>
```

period

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に経過するビーコンの間隔。ビーコン間隔は、20 ～ 1000 ミリ秒で指定します。AP300 および AP208 の場合、ビーコン間隔は 20 の倍数 (20 ～ 1000 ミリ秒) です。OAP 180 の場合、ビーコン間隔は 100 の倍数 (100 ～ 500 ミリ秒) です。

コマンドモード

ESS 設定

デフォルト

デフォルトのビーコン DTIM 間隔は 1 です。

用途

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モード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。

一般的にブロードキャストはワイヤレスのリソースを浪費するため、FortiWLC (SD) はより効果的で限られたユニキャストにブロードキャストを置き換えます。したがって、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。

使用例

以下のコマンドは、ビーコン DTIM 間隔を 20 に変更します。

```
controller# configure terminal
controller(config) essid eng
default(config-essid)# beacon dtim-period 20
default(config-essid)#
```

関連コマンド

- [essid \(550 ページ\)](#)
- [show essid \(563 ページ\)](#)

beacon period

ビーコンを送信するレートを設定します。

構文

beacon period <period>

period

ビーコン間の TU 数 (1 TU=1.024 ms)。値は、20 ~ 1000 ミリ秒にする必要があります。AP300 モデルの場合は 20 の倍数です。

コマンドモード

ESSID 設定

デフォルト

デフォルトのビーコン間隔は 100 TU です。

用途

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で省電力モード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。

使用例

以下のコマンドは、ビーコン間隔を 200 TU に変更します。

```
controller# configure terminal
controller(config) essid eng
controller(config-essid)# beacon period 200
controller(config-essid)#
```

関連コマンド

[show essid \(563 ページ\)](#)

bssid

特定のアクセス ポイントの ESS に BSSID を設定します。

構文

bssid <bssid>

bssid 16 進数形式の固有の MAC アドレス (*nn:nn:nn:nn:nn:nn*)。

コマンド モード

ESS-AP 設定

デフォルト

なし

用途

デフォルトでは、FortiWLC (SD) のすべてのアクセス ポイントには、BSSID としてランダムな MAC アドレスが割り当てられます。各 BSSID が、WLAN 全体において固有の値である必要があります。さらに、同じチャネル上のすべてのアクセス ポイントには、デフォルトで同じ BSSID が割り当てられます。同じ BSSID が設定されたアクセス ポイントが自動的に連動して、その BSSID の仮想セルを形成します。各仮想セルは、クライアントからは 1 つのアクセス ポイントとして見なされるため、シームレスなハンドオフ、負荷分散、「行き来」のない最適なクライアント割り当てなどの利点が生まれます。

bssid コマンドを使用して、アクセス ポイントに割り当てられているデフォルトの BSSID を上書きします。BSSID を変更すると、上書きされた BSSID ではない、そのチャネル上のすべてのアクセス ポイントの BSSID が変更されます。

使用例

次のコマンドは、BSSID を 00:0c:e6:02:7c:84 に設定します。

```
controller# configure terminal
controller(config) essid eng
controller(config-essid-essap)# bssid 00:0c:e6:02:7c:84
controller(config-essid-essap)#
```

関連コマンド

- [show ess-ap \(561 ページ\)](#)
- [show edited-bssid \(562 ページ\)](#)

calls-per-bss

該当の BSSID に関する音声通話の最大数を設定します。

構文

calls-per-bss <calls>

calls 該当の BSSID に関する音声通話の最大数を設定します。通話数の許容範囲は 0 ～ 999 です。**calls** を 0 に設定すると、**qosvars calls-per-bssid** のグローバル設定の値が使用されるようになります。

コマンドモード

ESS-AP 設定

デフォルト

calls は 0 に設定されます。

用途

このコマンドは、グローバル QoS コマンドである **qosvars calls-per-bssid** に似ていますが、このコマンドでは、該当の BSSID のみに関する通話数の最大値を設定できます。これらの両方のコマンドが使用されている場合は、calls-per-bss の設定が優先的に適用されます。

このコマンドでデフォルトの 0 以外の引数を指定すると、当該の BSS の最大通話数のしきい値が設定されます。このコマンドにより Call Admission Control (CAC) 機能が実装され、許可される通話のしきい値を設定することで、一定レベルの音声の品質が保証されるようになります。設定されているしきい値に達する場合は、CAC により、メディア ストリームを効率的に処理できるだけの帯域幅が得られるまで、新規の SIP 接続が拒否されます。

該当の BSS の通話制限を超過すると、指定されたしきい値を通話数が下回るまで新しい通話は、486_BusyHere 応答 (通話中の応答) を受け取ります。

使用例

以下のコマンドを設定すると、この BSSID で許容される最大通話数は 14 に設定されます。

```
controller# configure terminal
controller(config) essid eng
controller (config-essid)ess-ap 3 1
controller(config-essid-essap)# calls-per-bss 14
```

関連コマンド

[qosvars calls-per-bssid \(732 ページ\)](#)

countermeasure

MIC 対策を有効または無効にします。

構文

```
countermeasure  
no countermeasure
```

コマンド モード

ESSID 設定

デフォルト

対策はデフォルトで有効になっています。

用途

countermeasure コマンドを使用すると、ESSID ごとに MIC 対策を有効または無効にできます。MIC 対策は、デフォルトではオンになっています。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場合にのみ、**no countermeasure** コマンドで MIC 対策を一時的にオフにする必要があります。

60 秒以内に AP が同じクライアントから連続して 2 つの MIC エラーを検出する場合に、MIC 対策が役に立ちます。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。

MIC 対策が無効になっていると、MIC エラーがあるパケットはドロップされますが、攻撃しているステーションが MIC エラーが検出された AP にパケットを送信し続けたとしても、クライアントの関連付けは解除されません。

使用例

以下の例では、ESSID jaypsk2 の MIC 対策を無効にし、その後に設定します。

```
Master# configure terminal  
Master(config)# essid jaypsk2  
Master(config-ssid)# no countermeasure  
Master(config-ssid)# countermeasure  
Master(config-ssid)# exit
```

dataplane

このコマンドを使用して、AP300 で VLAN とのブリッジをサポートします。このコマンドは、リリース 4.0 で、remote-ap-enable に代わるコマンドとして追加されました。

構文

`dataplane bridged`
`dataplane tunneled`

<code>bridged</code>	データ パケットがコントローラに渡されないようにします。コントロール プレーン パケットのみがコントローラに渡されます (リモート AP モード)。
<code>tunneled</code>	AP のデフォルトの動作を指定します。デフォルトでは、データおよびコントロール パケットがコントローラに渡されます。

コマンドモード

ESSID 設定

デフォルト

デフォルトは、tunneled です。

用途

このコマンドは、コントローラと AP の間で渡されるトラフィックのタイプを決定します。デフォルトでは、tunneled モードがアクティブになり、コントローラと AP がデータ トンネルで接続されて、モバイル ステーションからのデータが AP からコントローラにまたその逆にトンネルされます。

bridged モードが使用される場合、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リング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 構成では次の FortiWLC (SD) 機能を使用できません。仮想セル、VLAN、キャプティブ ポータル、L3 モビリティ、および QoS。

公共の場におけるブリッジ接続を安全にするには、AP 設定モードの dataplaneencryption on コマンドを使用します。

AP300 は、ブリッジ モード ESS プロファイルをサポートしています。dataplane コマンドで、ESS プロファイルがブリッジであることを指示します。次に、ap-vlan-tag コマンドでプロファイルに VLAN タグを設定し、さらに、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。ap_vlan_priority コマンドは、タグ付けされた VLAN の優先度を高めます。

使用例

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
```

関連コマンド

- [ap-vlan priority \(531 ページ\)](#)
- [ap-vlan-tag \(532 ページ\)](#)

edited-bssid

構文 edited-bssid <ap-id> <ifindex> <essid> <bssid>

**コマンド
モード** グローバル設定

デフォルト 無効

用途

使用例

```
default# configure terminal
default(config)# edited-bssid 11 1 Asvin_test 00:0c:e6:01:06:11
default(config)# edited-bssid 12 1 Asvin_test 00:0c:e6:1:06:12
default(config)# exit
default# show edited-bssid
```

AP	ID	IfIndex	ESS	Profile	BSSID
11		1		Asvin_test	00:0c:e6:01:06:11
12		1		Asvin_test	00:0c:e6:1:06:12

Edited BssID Entry(2 entries)

```
default#
```

関連コマンド [show edited-bssid \(562 ページ\)](#)

ess-ap

ESS にアクセス ポイントを割り当て、ESS-AP 設定モードに入ります。

構文

```
ess-ap <ap-id> <interface_index>
```

<i>ap-id</i>	ESS に関連付ける AP の ID 番号
<i>interface_index</i>	AP のワイヤレス インターフェイス インデックス。

コマンド モード

ESSID 設定

デフォルト

なし

用途

このコマンドを使用して、ESS にアクセス ポイントを割り当て、ESS-AP 設定モードに入ります。この設定モードでは、アクセス ポイントのチャネル用 BSSID と BSS ごとのコール数を割り当てることができます

使用例

以下のコマンドにより AP-3、インデックス 1 が設定されます。

```
controller# configure terminal
controller(config) essid eng
controller (config-essid)ess-ap 3 1
controller(config-essid-essap)#
```

関連コマンド

- [show ess-ap \(561 ページ\)](#)
- [bssid \(543 ページ\)](#)
- [calls-per-bss \(544 ページ\)](#)

ssid

拡張サービスセット識別子 (ESSID) を作成または削除します。

構文

```
ssid <ssid>  
no ssid <ssid>
```

ssid 英数字で 32 文字までの文字列。

コマンドモード

グローバル設定

デフォルト

なし

用途

ESSID とは WLAN の名前で、クライアントはこの ID を確認して接続します。デフォルトでは、ESS に参加するすべてのアクセス ポイントは、仮想セルの同一のチャンネルが関連付けられます。

FortiWLC (SD) に作成できる ESSID の最大数は 64 です。

デフォルトでは、すべての新しい ESSID は、*default* という名前のセキュリティ プロファイルを使用するよう、設定されています。他のセキュリティ プロファイルを使用するには、プロファイルを作成し、ESSID 設定モードで **security-profile** コマンドを使用して ESSID に割り当てます。

この値は、SSID 名に割り当てられている名前と同じである必要があります。

ESSID を削除するには、**no** フォームを使用します。

使用例

以下のコマンドは、*sj_engineering* という名前の ESSID を作成します。

```
controller# configure terminal  
controller(config)# ssid sj_engineering  
controller(config-ssid)#
```

関連コマンド

- [show ssid \(563 ページ\)](#)
- [ssid \(566 ページ\)](#)

gre name

GRE プロファイルを ESSID に割り当てます。

構文

```
gre name <name>
```

コマンド モード

ESSID 設定

デフォルト

なし

用途

ESSID を作成するときに、GRE を ESSID に割り当てることができます。これにより、ESSID で GRE トンネルを使用できるようになります。デフォルトでは、ESSID には、GRE トンネルが割り当てられていません。GRE 名を ESSID に割り当てる前に、グローバル設定モードで gre コマンドを使用して、GRE プロファイルを作成する必要があります。同様に、tunnel-type コマンドを使用して、GRE のトンネルタイプを ESSID に割り当てます。

使用例

次のコマンドは、corp という GRE を ESSID に割り当てています。

```
controller# configure terminal
controller(config) essid eng
controller(config-essid)# gre name corp
controller(config-essid)# tunnel-type GRE
```

関連コマンド

- [gre \(343 ページ\)](#)
- [tunnel-type \(569 ページ\)](#)

l2bridge airf

これらのコマンドを使用して、airf ブリッジを有効または無効にします。

構文

```
l2bridge airf  
no l2bridge airf
```

コマンド モード

ESSID 設定

デフォルト

デフォルトでは、airf ブリッジは無効、Air Fortress は無効になっています。

用途

FortressTech Layer 2 ブリッジおよび Fortress Technology AirFortress ゲートウェイの暗号を使用すると、管理者は FortressTech の暗号を ESSID (複数可) で指定できます。ssid 設定サブモードから **l2bridge airf** および **no l2bridge airf** コマンドを使用して、airf ブリッジをそれぞれ有効・無効にします。

使用例

次のコマンドを使用して、eng というコントローラで airf をオフにします。

```
eng(config)# configure terminal  
eng(config)# ssid sj_engineering  
eng(config-ssid)# no l2bridge airf
```

関連コマンド

[ssid](#) (550 ページ)

12bridge appletalk

AppleTalk ブリッジを有効または無効にします。

構文

```
12bridge appletalk  
no 12bridge appletalk
```

コマンド モード

ESSID 設定

デフォルト

Appletalk はデフォルトで無効です。

用途

12bridge appletalk および **no 12bridge appletalk** コマンドを使用して、AppleTalk ブリッジをそれぞれ有効または無効にします。複数の ESSID プロファイルがコントローラでアクティブになっていると、AppleTalk クライアントは、有効な AppleTalk プリンタを検出できません。アクティブな ESSID が 1 つだけの場合、この問題は発生しません。

使用例

次のコマンドは、eng というコントローラで AppleTalk をオフにします。

```
eng(config)# essid guest  
eng(config-essid)# no 12bridge appletalk
```

関連コマンド

[essid \(550 ページ\)](#)

12bridge ipv6

IPv6 トラフィックのプロトコルブリッジを有効にします。

構文

```
12bridge ipv6  
no 12bridge ipv6
```

コマンド モード

ESSID 設定

デフォルト

IPv6 ブリッジはデフォルトで無効になっています。

用途

ipv6 ブリッジでは、AP やコントローラは実際には IPv6/AppleTalk/AirF ネットワークに参加しません (実際のエンド ポイントではありません)。プロトコルはフォーティネットのインフラストラクチャを介して単にブリッジされるか、パススルーされ、これらのネットワークに対して透過になります。フォーティネットのデバイスは実際には IPv6/AppleTalk アドレスを取得せず、パケットも処理せずに、送信元から受信先へパケットを渡します。

使用例

次のコマンドは、eng というコントローラで IPv6 をオフにします。

```
eng # configure terminal  
eng(config)# essid guest  
eng(config-ssid)# no 12bridge ipv6
```

次のコマンドは、コントローラ eng の IPv6 をオンにします。

```
eng # configure terminal  
eng(config)# essid guest  
eng(config-ssid)# 12bridge ipv6
```

multicast-enable

ESSID のマルチキャストを有効にします。

構文

```
multicast-enable  
no multicast-enable
```

コマンド モード

ESSID 設定

デフォルト

マルチキャストは、デフォルトで無効です。

用途

ビデオなどの同じストリームを複数のステーションにブロードキャストする必要がある場合は、**multicast-enable** コマンドを使用します。マルチキャストを有効にすると、ワイヤレスのマルチキャスト 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 パケットがワイヤレスに表示されるようになります。

マルチキャストを無効にするには、**no** フォームを使用します。



マルチキャストは高度な機能です。WLAN でマルチキャストを有効にするとネットワークでわずかな変化が発生します。この機能を有効にする前に、ネットワーク管理者に必ず相談してください。

使用例

以下のコマンドは、マルチキャストを有効にします。

```
controller# configure terminal  
controller(config) essid eng  
controller(config-essid)# multicast-enable
```

関連コマンド

[show essid \(563 ページ\)](#)

multicast-mac-transparency

トンネル マルチキャストで MAC 透過を有効にします。

構文

```
multicast-mac-transparency  
no multicast-mac-transparency
```

コマンド モード

ESSID 設定

デフォルト

マルチキャストはデフォルトでは無効です。マルチキャスト透過はデフォルトでは無効です。

用途

multicast-mac-transparency コマンドを使用して、有線ステーションのソース MAC アドレスの表示をサポートします。有線ステーションのソース MAC アドレスは、マルチキャストパケットのソース MAC アドレス フィールドにあるワイヤレス クライアントに伝承されます。

使用例

次のコマンドは、マルチキャストを有効にして、multicast-mac-transparency を有効にします。

```
controller# configure terminal  
controller(config) essid eng  
controller(config-essid)# multicast-enable  
controller(config-essid)# multicast-mac-transparency
```

関連コマンド


[multicast-enable \(555 ページ\)](#)

overflowfrom-essprofile

使用例

```
default(0)# show essid
ESS Profile Name          SSID          Security
Profile                   Broadcast Tunnel Interface Type
vcelloverflow            vcelloverflow          default
on                        none
                        ESS Profile(1 entry)
default(0)# configure terminal
default(0)(config)# essid vcelloverflowoss
default(0)(config-essid)# overflowfrom-essprofile <ess profile name>
default(0)(config-essid)# end
default(0)# show essid
ESS Profile Name          SSID          Security
Profile                   Broadcast Tunnel Interface Type
vcelloverflow            vcelloverflow          default
on                        none
vcelloverflowoss         vcelloverflow          default
on                        none
                        ESS Profile(2)
default(0)# show essid vcelloverflowoss
ESS Profile

ESS Profile Name          : vcelloverflowoss
SSID                      : vcelloverflow
Security Profile Name     : 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                 :
GRE Tunnel Profile Name   :
```

Allow Multicast Flag	: off
Virtual Cell	: off (overflow ESS must not be VC)
Virtual Port	: off
ESS Profile Name for Overflow from	: vcellooverflow
	
APSD Support	: off
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

publish-essid

ESSID のブロードキャストを有効にします。

構文

```
publish-essid  
no publish-essid
```

コマンド モード

ESSID 設定

デフォルト

ESSID はデフォルトでブロードキャストされます。

用途

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。

no フォームを使用すると、ESSID をブロードキャストしなくなります。

使用例

次のコマンドによって、Eng という名前の ESSID のブロードキャストが無効になります。

```
controller# configure terminal  
controller(config)# ssid eng  
controller(config-ssid)# no publish-ssid  
controller(config-ssid)#
```

関連コマンド

[ssid](#) (550 ページ)

security-profile

セキュリティ パラメータを定義するセキュリティ プロファイルを、ESS に割り当てます。

構文

security-profile <name>

name ESS に割り当てる既存のセキュリティ プロファイルの名前。

コマンド モード

ESSID 設定

デフォルト

ESS に割り当てられるデフォルトのセキュリティ プロファイルは *default* です。

用途

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。ESSID を作成すると、*default* という名前のセキュリティ プロファイルが自動的に関連付けられます。このコマンドを使用して、異なるセキュリティ プロファイルを ESSID に割り当てます。

セキュリティ プロファイルを ESS に割り当てる前に、グローバル設定モードで **security-profile** コマンドを使用して、セキュリティ プロファイルを作成する必要があります。

使用例

以下のコマンドは、*nms-group* という名前のセキュリティ プロファイルを *eng* という名前の ESSID に割り当てます。

```
controller# configure terminal
controller(config)# essid eng
controller(config-essid)# security-profile nms-group
controller(config-essid)#
```

関連コマンド

- [essid \(550 ページ\)](#)
- [security-profile \(469 ページ\)](#)

show ess-ap

ESSID と関連付けられているアクセス ポイントを表示します。

構文

```
show ess-ap
show ess-ap <ap-id> <ssid> <Ifindex>
show ess-ap bssid <bssid>
show ess-ap channel <channel >
show ess-ap ssid <ssid> <ap-id> <Ifindex>
```

コマンドモード

特権 EXEC および ESSID 設定モード

デフォルト

なし

用途

show ess-ap コマンドの出力は、引数とコマンドが入力されるコマンド モードによって異なります。特権 EXEC モードでは、ESSID と関連するアクセス ポイントすべてが表示されます。ESSID 設定モードでは、設定されている ESSID について関連するアクセス ポイントが表示されます。

使用例

特権 EXEC モードの場合、以下のコマンドは ESSID および関連するアクセス ポイントをすべて表示します (以下は表示される内容の一部です)。

```
controller# show ess-ap
ESS Profile           AP ID AP Name           IfIndex Channel Max
Calls BSSID

mwf--1xtls           1    #1-2F-QA-208         2        161      0
00:0c:e6:69:4e:8c

mwf--1xtls           1    #1-2F-QA-208         1         1        0
00:0c:e6:14:40:f7

mwf--1xtls           2    #2-2F-Sw-208         2        161      0
00:0c:e6:69:4e:8c
controller#
```

関連コマンド

[ess-ap \(549 ページ\)](#)

show edited-bssid

BSSID テーブルを表示します。

構文 `show edited-bssid`

**コマンド
モード** 特権 EXEC

デフォルト 無効

用途 このコマンドを使用して、設定された edited-bssids のリストを表示します。

使用例

```
Asvin-test# show edited-bssid
AP ID IfIndex ESS Profile BSSID
11 1 Asvin_test 00:0c:e6:01:06:11
12 1 Asvin_test 00:0c:e6:1:06:12
Edited BssID Entry(2 entries)
Asvin-test#
```

関連コマンド [edited-bssid \(548 ページ\)](#)

show essid

ESSID の詳細情報を表示します。

構文

```
show essid <ssid>
```

ssid 詳細情報を表示する ESSID の名前。

コマンド モード

特権 EXEC

デフォルト

すべての ESSID のリストが表示されます。

使用例

最初のコマンドで、設定された ESSID を表示し、2 つ目のコマンドで、asc という名前の ESSID の情報を表示します。

```
InteropLab-MC1000# show essid ?
<EssId>                Display the detailed information for this ESSID.
    asc
    bradford
    polyspec
<CR>
InteropLab-MC1000# show essid asc
ESS Profile

ESS Profile                : default
Enable/Disable            : enable
SSID                      : sample
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  
InteropLab-MC1000#
```

関連コマンド [essid \(550 ページ\)](#)

ssid

ワイヤレスで公開される SSID を設定します。

構文

`ssid <ssid>`

ssid 1 ～ 32 文字の英数字の一意の SSID の名前。

コマンド モード

ESS 設定

デフォルト

なし

用途

このコマンドを使用して、ワイヤレスで公開される SSID を設定します。



SSID を指定しないと、ESS プロファイルと同じ名前がデフォルトになります。

使用例

関連コマンド

- [essid \(550 ページ\)](#)
- [show essid \(563 ページ\)](#)

supported-tx-rates

チャンネルでサポートする伝送速度を Mbps で設定します。

構文

```
supported-tx-rates 802.11a all
supported-tx-rates 802.11b all
supported-tx-rates 802.11g all
supported-tx-rates 802.11n all
supported-tx-rates 802.11bg all
supported-tx-rates 802.11bgn all
supported-tx-rates 802.11an all
supported-tx-rates 802.11an-mcs all
supported-tx-rates 802.11bgn-mcs all
supported-tx-rates 802.11a <Mbps rate>
supported-tx-rates 802.11b <Mbps rate>
supported-tx-rates 802.11g <Mbps rate>
supported-tx-rates 802.11n <Mbps rate>
supported-tx-rates 802.11bg <Mbps rate>
supported-tx-rates 802.11bgn <Mbps rate>
supported-tx-rates 802.11an <Mbps rate>
supported-tx-rates 802.11an-mcs <Mbps rate>
supported-tx-rates 802.11bgn-mcs <Mbps rate>
no supported-tx-rates ( 上記すべて )
```

802.11b <Mbps rate>	1 2 5.5 11
802.11g <Mbps rate>	6 9 12 18 24 36 48 54
802.11bg <Mbps rate>	1 2 5.5 11 6 9 12 18 24 36 48 54
802.11bgn <Mbps rate>	1 2 5.5 11 6 9 12 18 24 36 48 54
802.11a <Mbps rate>	6 9 12 18 24 36 48 54
802.11an <Mbps rate>	6 9 12 18 24 36 48 54
802.11an-mcs <Mbps rate>	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
802.11bgn-mcs <Mbps rate>	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

コマンドモード

ESS 設定

デフォルト

802.11a base - 6,12,24 Mbps
802.11b base - 11 Mbps

802.11g base - 6,9,12,18,24,36,48,54 Mbps
802.11an base - 6,12,24 Mbps
802.11bg base - 11 Mbps
802.11bgn base - 11 Mbps
802.11an base - 6,12,24 Mbps
802.11an-ht-mcs base - none
802.11bgn-ht-mcs base - none

用途

サポートされる速度を設定することで、クライアントが自由に接続できる速度を指定し、クライアントおよびアクセス ポイントがその速度をサポートすることになります。コマンドの **no** フォームを使用して、指定したサポートされる速度を 無効にします。

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。

使用例

以下のコマンドは、802.11bg でサポートされる伝送速度を 11 Mbps に設定します。

```
default(config-ssid)# supported-tx-rate 802.11bg 11
```

以下のコマンドは、802.11a のサポートされる伝送速度をすべての速度 (6、9、12、18、24、36、48、54 Mbps) をサポートするように設定します。

```
default(config-ssid)# supported-tx-rate 802.11a all
```

関連コマンド

[base-tx-rates \(539 ページ\)](#)

tunnel-type

ESSID に設定されるトンネルのタイプを設定します。

構文

```
tunnel-type GRE
tunnel-type configured-vlan-only
tunnel-type none
tunnel-type radius-and-configured-vlan
tunnel-type radius-only
```

コマンドモード

ESSID 設定サブモード

デフォルト

なし

用途

ESSID にトンネルを設定する場合は、このコマンドを使用して、トンネル タイプを指定します。VLAN および GRE のトンネル設定ではトンネルタイプを指定しますが、GRE 構成では常に GRE トンネルが指定され、VLAN ではそれ以外のオプションを指定できます (none 以外のタイプ)。

使用例

GRE ESSID (GRE プロファイルと同じ名前を使用) を設定するには、次の例のようにトンネル タイプに GRE を指定してセキュリティ プロファイルを指定します。

```
default# configure terminal
default(config)# essid guest
default(config-ssid)# tunnel-type GRE
default(config-ssid)# security-profile default
default(config)# exit
```

関連コマンド

- [gre \(343 ページ\)](#)
- [l2bridge appletalk \(553 ページ\)](#)
- [ssid \(550 ページ\)](#)
- [security-profile \(560 ページ\)](#)
- [vlan \(356 ページ\)](#)
- [vlan name \(571 ページ\)](#)

virtual-port

仮想ポートをオンにして、各クライアントの AP300 への固有の接続を可能にします。

構文

```
virtual-port  
no virtual-port
```

コマンド モード

設定モード

デフォルト

なし

用途

クライアントごとに固有の仮想ポートが存在すれば、クライアント同士がお互いのパフォーマンスに影響を与えることがなくなります。このコマンドは、仮想セル モードが有効である場合のみ適用されます。

使用例

以下の例は、仮想セルを有効にし、ESSID 5 の仮想ポートを有効にします。

```
Master1# config terminal  
Master1(config)# interface Dot11Radio 239 1  
Master1(config-if-802)# virtual-cell-mode  
Master1(config-if-802)# exit  
Master1(config)# essid 5  
Master1(config-ssid)# virtual-port  
Master1(config-ssid)# exit
```

関連コマンド

vlan name

VLAN を ESSID に割り当てます。

構文

```
vlan name <name>  
no vlan
```

コマンド モード

ESSID 設定

デフォルト

なし

用途

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 名を 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。同様に、**tunnel-type** コマンドを使用して、**configured vlan-only** または **radius-and-configured-vlan** のトンネルタイプを ESSID に割り当てます。

no vlan コマンドを使用すると、VLAN 割り当てが無効になります。

使用例

以下のコマンドは、*engineering* という VLAN を ESSID に割り当てます。

```
controller(config-ssid)# vlan name engineering  
controller(config-ssid)# tunnel-type configured-vlan-only
```

関連コマンド

- [tunnel-type \(569 ページ\)](#)
- [vlan \(356 ページ\)](#)

wireless-to-wireless-isolation

同じ AP に接続する個々のステーションのトラフィックを分離できるようにします。

構文

```
wireless-to-wireless-isolation  
no wireless-to-wireless-isolation
```

コマンド モード

ESSID 設定

デフォルト

無効

用途

一部のワイヤレス環境においては、同じ L2 ドメインに属している 2 台のワイヤレス ステーション同士が直接通信できないようにする必要がある場合があります。**wireless-to-wireless-isolation** を ESS で有効にすると、2 台のステーションが通信できなくなります。

no wireless-to-wireless-isolation コマンドを使用して、この機能を無効にします。

使用例

```
controller(config-ssid)# wireless-to-wireless-isolation  
controller(config-ssid)#
```

関連コマンド

11 アクセスポイントと無線コマンド

本章で説明するコマンドは、コントローラと AP 間の接続を設定・管理するため、そして AP 無線を設定するために使用されます。通常の設置サイトの場合は、デフォルトの無線設定でも問題はありませんが、サイトにおける特殊な要件に対応できるようにデフォルトの無線設定を調整するために、多くのコマンドを利用できるようになっています。

- [admin-mode \(576 ページ\)](#)
- [antenna-gain \(577 ページ\)](#)
- [antenna-property \(578 ページ\)](#)
- [antenna-selection \(579 ページ\)](#)
- [ap \(580 ページ\)](#)
- [ap-keepalive-timeout \(582 ページ\)](#)
- [ap-redirect \(583 ページ\)](#)
- [auto-ap-upgrade \(584 ページ\)](#)
- [autochannel \(586 ページ\)](#)
- [boot-script \(587 ページ\)](#)
- [building \(588 ページ\)](#)
- [channel \(589 ページ\)](#)
- [channel-width \(591 ページ\)](#)
- [connectivity \(592 ページ\)](#)
- [contact \(594 ページ\)](#)
- [controller domainname \(595 ページ\)](#)
- [controller hostname \(596 ページ\)](#)
- [controller ip \(597 ページ\)](#)
- [dataplane-encryption \(598 ページ\)](#)
- [description \(599 ページ\)](#)
- [fixed-channel \(600 ページ\)](#)
- [floor \(601 ページ\)](#)
- [hostname \(602 ページ\)](#)

- [interface Dot11Radio](#) (603 ページ)
- [keepalive-timeout](#) (608 ページ)
- [led](#) (605 ページ)
- [link](#) (606 ページ)
- [link-probing-duration](#) (607 ページ)
- [localpower](#) (609 ページ)
- [location](#) (611 ページ)
- [mac-address](#) (612 ページ)
- [mimo-mode](#) (613 ページ)
- [mode](#) (615 ページ)
- [model](#) (616 ページ)
- [n-only-mode](#) (617 ページ)
- [parent-ap](#) (618 ページ)
- [power-supply](#) (620 ページ)
- [preamble-short](#) (622 ページ)
- [protection-mode](#) (624 ページ)
- [protection-mode](#) (624 ページ)
- [rfband](#) (625 ページ)
- [rf-mode](#) (626 ページ)
- [role](#) (627 ページ)
- [show ap](#) (629 ページ)
- [show ap-connectivity](#) (632 ページ)
- [show ap-discovered](#) (634 ページ)
- [show ap-redirect](#) (636 ページ)
- [show ap-swap](#) (637 ページ)
- [show ess-ap](#) (638 ページ)
- [show interfaces Dot11Radio](#) (639 ページ)
- [show interfaces Dot11Radio antenna-property](#) (641 ページ)
- [show interfaces Dot11Radio statistics](#) (644 ページ)
- [show regulatory-domain](#) (649 ページ)
- [show statistics ap300-diagnostics](#) (650 ページ)
- [show statistics station-per-ap](#) (652 ページ)
- [show statistics top10-ap-problem](#) (653 ページ)
- [show statistics top10-ap-talker](#) (655 ページ)

- [show topoap](#) (657 ページ)
- [show topoapap](#) (658 ページ)
- [swap ap](#) (660 ページ)
- [type](#) (663 ページ)

admin-mode

無線インターフェイスを管理します。

構文

`admin-mode {Up | Down | Testing}`

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

このインターフェイスは、デフォルトでは Up (有効) になっています。

用途

このコマンドを使用して、インターフェイスを有効 (**Up**) または無効 (**Down**) にするかを制御します。インターフェイスを **Down** に設定すると、クライアント ステーションに無線で接続できなくなります。

デュアル無線 AP のスループットは、2 つの無線を管理する必要があるため、単一の無線 AP よりも若干低速となります。無線を使用していない場合は、このコマンドを使用して簡単に一時的に無効にして、パフォーマンスを向上できます。

使用例

```
controller(config-if-802)# admin-mode Down
```

関連コマンド

antenna-gain

アンテナ バンドを設定します。

構文

```
antenna-gain {2.4GHz gain | 5GHz gain}
```

gain *gain* (ゲイン) には 0 ～ 30 の整数を指定します。

コマンド モード

Dot11Radio インターフェイス設定

デフォルト

用途

このコマンドを使用して、アンテナ ゲインを `rfband` コマンドで使用する無線タイプに設定します。

使用例

```
default# configure terminal
default(config)# interface Dot11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# antenna-gain 2.4GHz 8
default(config-if-802-antenna)# end
default(config-if-802)# end
default(config)# end
```

関連コマンド

- [antenna-property \(578 ページ\)](#)
- [interface Dot11Radio \(603 ページ\)](#)

antenna-property

外部のアンテナ インターフェイスのプロパティを管理します。

構文

`antenna-property connector`

`connector` アンテナ コネクタの ID。1 (左アンテナ) または 2 (右アンテナ) のいずれかになります。

コマンド モード

Dot11Radio インターフェイス設定

デフォルト

用途

このコマンドにより、ゲイン、RF バンド (2.4GHz、5GHz、またはデュアル)、リンク タイプ (ポイントツーポイントまたはポイントツーマルチポイント) などのアンテナのプロパティを詳細に調節可能なサブコマンド モードに入ります。

使用例

```
controller(config-if-802)# antenna-property 1
```

関連コマンド

- [antenna-gain \(577 ページ\)](#)
- [antenna-selection \(579 ページ\)](#)
- [interface Dot11Radio \(603 ページ\)](#)
- [rfband \(625 ページ\)](#)
- [show interfaces Dot11Radio antenna-property \(641 ページ\)](#)
- [type \(663 ページ\)](#)

antenna-selection

左または右のアンテナを使用するようにアクセス ポイントを設定します。

構文

```
antenna-selection {left | right | diversity}
```

left	左のアンテナのみを使用するよう AP を設定します。
right	右のアンテナのみを使用するよう AP を設定します。
diversity	802.11b の AP201 が左右いずれかのアンテナのみを使用するのではなく、両方のアンテナを使用するように設定します。この機能を使用すると、アクセス ポイントは信号の強度が高い方のアンテナから受信できるようになります。 このコマンドを使用する前に、アンテナが「left」に設定 されている必要があります。 正しく動作させるには、「short-preamble」機能をオフ (デフォルト) にして、この複合 (diversity) モードを使用します。

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

デフォルトでは、システムが AP の左のアンテナを使用します。

用途

このコマンドは、すべてのアクセス ポイント モデルが右または左のアンテナを使用するように設定します。802.11b で接続する AP201 では、**diversity** モードを設定して、信号の強度が高い右または左のいずれかのアンテナから信号を受信するよう選択で きます。

使用例

```
controller(config-if_802)# antenna-selection right
controller(config-if_802)#
```

関連コマンド

[antenna-property](#) (578 ページ)

ap

アクセス ポイントの設定に入ります。

構文

```
ap id  
no ap id
```

id 各アクセス ポイント固有の識別子 (ID) です。

コマンド モード

グローバル設定

デフォルト

なし

用途

ap コマンドで識別番号を指定して、AP 設定サブモードに入り、指定したアクセス ポイントを設定します。**no ap id** コマンドを使用すると、コントローラと AP の間の割り当てが削除されます。

使用例

```
controller(config)# ap 1  
controller(config-ap)# ?  
boot-script          Configure boot script for this AP.  
building             Building location for this AP.  
connectivity         Manage AP connectivity.  
contact              Contact person for this AP.  
dataplane-mode       Determine whether the data packets go through the  
controller or not.  
default              Reset to default values  
description           Description of AP.  
do                   Executes an IOSCLI command.  
end                  Save changes, and return to privileged EXEC mode.  
exit                 Save changes, and return to global configuration  
mode.  
floor                Floor location for this AP.  
led                  Configure LED settings.  
link-probing-duration Duration AP waits before rebooting when controller  
link is down.
```

<code>location</code>	Location of this AP.
<code>mac-address</code>	Assign a new MAC address or pre-provision AP.
<code>model</code>	Assign AP HW type.
<code>no</code>	Disables various parameters.
<code>show</code>	Displays parameters related to this AP.

関連コマンド

- [boot-script \(587 ページ\)](#)
- [building \(588 ページ\)](#)
- [contact \(594 ページ\)](#)
- [connectivity \(592 ページ\)](#)
- [description \(599 ページ\)](#)
- [floor \(601 ページ\)](#)
- [hostname \(602 ページ\)](#)
- [led \(605 ページ\)](#)
- [link-probing-duration \(607 ページ\)](#)
- [location \(611 ページ\)](#)
- [mac-address \(612 ページ\)](#)

ap-keepalive-timeout

AP のキープアライブのタイムアウトを秒で設定します。

構文

ap-keepalive-timeout <value>

value AP のキープアライブのタイムアウトを秒 (1-1800) で入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

使用例

```
controller# configure terminal
controller(config)# ap-keepalive-timeout 10
```

関連コマンド

ap-redirect

AP を別のコントローラにリダイレクトします。

構文

```
ap-redirect ip-subnet <ip_addr subnet_addr> <controller_ip_addr>  
ap-redirect ip-subnet mac-address <MAC_addr> <controller_ip_addr>  
no ap-redirect
```

ip-subnet ip_addr subnet_addr	リダイレクトする 1 つ以上の AP の IP アドレスまたはサブ ネット アドレスを指定します。
mac-address mac_addr	リダイレクトする AP の MAC アドレスを指定します。
controller_ip_addr	AP をリダイレクトするコントローラのホスト名または IP ア ドレスを指定します。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用すると、他のコントローラ (ホスト名または IP アドレスで指定) にリダイレクトする AP を MAC アドレスまたは IP サブネット アドレスで指定できます。リダイレクトは、最初の検出の後に実行されます。各コントローラには、AP の MAC/IP サブネット アドレスをコントローラの IP アドレスまたはホスト名に関連付けるためのリダイレクトテーブルを設定できます。AP ごとに最大 5 ホップ (リダイレクト) が許可されます。

このコマンドの **no** フォームを使用すると、リダイレクトの割り当てを削除できます。

使用例

```
controller(config-ap)# ap-redirect mac-address 00:0c:e6:00:01:02  
172.10.10.5  
controller(config-ap)#
```

関連コマンド

[show ap-redirect \(636 ページ\)](#)

auto-ap-upgrade

コントローラによる AP ファームウェアの自動アップグレードを許可します。

構文

```
auto-ap-upgrade {enable | disable}
```

enable	AP 自動アップグレード機能をアクティブにします。これがデフォルト設定です。
disable	AP 自動アップグレード機能を無効にします。

コマンドモード

グローバル設定

デフォルト

AP 自動アップグレード機能はデフォルトで有効です。

用途

このコマンドは、AP が WLAN に参加したときに、コントローラによる AP の ファームウェアの自動アップグレードを許可します。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、AP を監視できなくなります (つまり、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、アップグレードを実行します。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。

この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。不一致があると (つまり、何らかの理由で AP がアップグレードできないと)、SNMP マネージャにアラームが発信されます。アップグレードが実行されると、AP/ コントローラのソフトウェア バージョン不一致を通知する、syslog と SNMP トラップが送信されます。アラームは手動でクリアする必要があります。

upgrade コマンドを使用するときに、この機能が通常の WLAN システム アップグレードを妨害することはありません。

使用例

```
controller(config)# auto-ap-upgrade enable
```

```
controller# show controller
```

Global Controller Parameters

Controller ID	: 1
Description	: 3dot4dot1 Controller
Host Name	: meru-ess
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	: on
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	: 3.7-48
Network Device Id	: 00:90:0b:07:9f:6a
System Id	: 245AA7436A21
Default AP Init Script	:
DHCP Relay Passthrough	: on
Controller Model	: MC3000
Country Setting	: United States Of
America	
Manufacturing Serial #	: N/A
Management by wireless stations	: on
Controller Index	: 0

autochannel

自動チャンネル設定を実行します。

構文

autochannel *channel_list*

channel_list スペース区切りの 802.11bg または 802.11a チャンネルのリスト。ワイヤレス インターフェイスのタイプに適したチャンネルが自動的に適用されます。

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドは、AP に自動的にチャンネルを割り当てます。

autochannel を実行すると、引数として指定されたチャンネルが AP に設定された国コードで有効であるかどうかを確認されます。チャンネルが無効である場合は、有効なチャンネルのリストを知らせるエラー メッセージが表示されます。そして、最適なチャンネルが選択され、指定された AP インターフェイスに設定されます (b/g または a などの、インターフェイスに設定されている RF バンドが基準となります)。このプロセスには 2 分程度かかり、この間、AP は動作しません。

自動チャンネル割り当てからあるインターフェイスを除外するには、**channel** および **fixed-channel** コマンドを使用します。

使用例

```
controller(config)# autochannel 2 3 4
Pre-initialization:
    out of 44 APs, 3 are enabled
```

関連コマンド

- [channel](#) (589 ページ)
- [fixed-channel](#) (600 ページ)

boot-script

アクセス ポイントの起動時に、指定されたスクリプトを実行します。

構文

```
boot-script script  
no boot-script
```

script 実行するスクリプトの名前。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、特定のスクリプトを使用してアクセス ポイントを起動します。
show ap scripts コマンドを *特権 EXEC* コマンド モードから実行すると、利用可能なスクリプトのリストを参照できます。

このコマンドの **no** フォームを使用すると、デフォルトの AP 起動スクリプトを無効にできます。

使用例

```
controller# show scripts  
default  
debug  
cli  
controller# configure terminal  
controller(config)# boot-script default  
controller(config)
```

関連コマンド

[boot-script \(587 ページ\)](#)

building

アクセス ポイントを配置するビル (建物) を指定します。

構文

building *building-name*

building-name アクセス ポイントを配置するビル (建物) の名前。ビルの名前には 64 文字以下の英数字を使用できます。名前にスペースを使用する場合は、二重引用符 (") で囲みます。

コマンドモード

アクセス ポイント設定

デフォルト

なし

用途

building コマンドの使用はオプションであり、情報提供の目的でのみ使用します。

使用例

次のコマンドは、ノード ID が「2」のアクセス ポイントが「building 1」に設置されていることを指定します。

```
controller# ap 2
controller(config-ap)# building "building 1"
controller(config-ap)# exit
```

関連コマンド

- [floor](#) (601 ページ)
- [location](#) (611 ページ)

channel

ワイヤレス インターフェイスに使用するチャンネル番号を設定します。

構文

channel *channel*

channel チャンネル ID

コマンド モード

Dot11Radio インターフェイス設定

デフォルト

なし

用途

ワイヤレス インターフェイスのチャンネルを設定します。**channel ?** と入力すると、使用中の無線タイプに使用できるチャンネルが表示されます。

autochannel コマンドの実行時にチャンネル設定が変更されないようにするには、**fixed-channel** コマンドを使用します。

使用例

```
controller(config-if_802)# channel ?
<channel>                      Enter the channel ID.
 1
10
11
149
153
157
161
165
 2
 3
36
 4
40
44
48
```

5
52
56
6
60
64
7
8

controller(config-if_802)# **channel 149**

関連コマンド

- [autochannel](#) (586 ページ)
- [fixed-channel](#) (600 ページ)

channel-width

AP300 チャンネル幅を変更します。

構文

`channel-width [20-mhz | 40-mhz-extension-channel-above | 40-mhz-extension-channel-below]`

20-mhz	チャンネル幅を 20 MHz に設定します。
40-mhz-extension-channel-above	上位の拡張チャンネルとのボンディングによって、チャンネル幅を 40 MHz に設定します。
40-mhz-extension-channel-below	下位の拡張チャンネルとのボンディングによって、チャンネル幅を 40 MHz に設定します。

コマンドモード

インターフェイス Dot11Radio 設定サブモード

デフォルト

20 MHz

用途

このコマンドを使用して、チャンネル幅を 20 MHz (デフォルト) から 40 MHz に 変更します (40-mhz-extension-channel-above または 0-mhz-extensionchannel- below 40) このコマンドによって、チャンネル ボンディングも設定され、40 MHz が作成されます。

使用例

次のコマンドは、上位チャンネルとのボンディングによって、AP のチャンネル幅 を 40 MHz に 増加させます。

```
default config terminal
default(config)interface Dot11Radio 1 1
default(config-if-802)# channel-width-above-40-MHz-Extension-channel
```

次のコマンドは、下位チャンネルとのボンディングによって、AP のチャンネル幅 を 40 MHz に 増加させます。

```
default config terminal
default(config)interface Dot11Radio 1 1
default(config-if-802)# channel-width below-40-MHz-Extension-channel
```

connectivity

AP 接続を管理し、**I2-preferred** または **I3-preferred** を使用している場合、AP 接続モードに入ります。

構文

```
connectivity { I2-only | I2-preferred | I3-preferred }
```

I2-only	AP 検出にレイヤ 2 のみを使用します。
I2-preferred	AP 検出の最初の試行でレイヤ 2 を使用します。16 秒以内にコントローラが見つからないと、レイヤ 3 の検出を試行します。
I3-preferred	AP 検出の最初の試行でレイヤ 3 を使用します。16 秒以内にコントローラが見つからないと、レイヤ 2 の検出を試行します。

コマンドモード

AP 設定

デフォルト

デフォルト接続では、レイヤ 2 が優先されます。

用途

このコマンドを使用して、コントローラへの AP の接続を管理します。AP とコントローラは、同じサブネットに存在することも、1 台以上のルータによって分離される異なるサブネットに存在することもできます。

AP が WLAN に参加すると、リンクするコントローラが検索されます。デフォルトでは、AP はレイヤ 2 の MAC アドレス ブロードキャスト検出パケットを使用して、コントローラに検出されるようにします。コントローラと AP が同じサブネットに存在する場合、AP はコントローラによって検出され、コントローラから AP に設定情報がダウンロードされます。

レイヤ 2 プロトコルではサブネットの外部の検出パケットが許可されないため、コントローラが AP と同じサブネットに存在しない場合は、レイヤ 3 ルーティングを確立する必要があります。デフォルトの接続では、コントローラが 16 秒以内に見つからないと、レイヤ 3 検出に切り替えられます。

サブネット間でルータを使用しており、AP がコントローラと異なるサブネットに存在している場合、**I3-preferred** オプションを使用して、コントローラへのレイヤ 3 接続を開始します。この構成で、DNS サーバにコントローラのデフォルト名である「wlan-controller」が含まれ、IP アドレスが「default」としてセットアップされていると、AP とコントローラの間の接続が自動的に確立され、AP がコントローラから設定情報を受信できます。

l2-preferred または **l3-preferred** を選択して、**ap-connectivity** モードに入ります。このモードでは、コントローラの IP アドレス、ホスト名、およびドメイン名を明示的に設定できます。



AP が L3 優先検出に設定されていて、コントローラの IP アドレスを変更 する場合は、すべての AP の設定でコントローラの新しい IP アドレスに更新する必要があります。更新しないと、リブート時に AP がコントローラを検出できません。AP がコントローラを検出できない場合は、AP をコントローラと同じ L2 サブネットに移動して再設定できます。L3 検出が失敗してから数分経過すると、L2 ブロードキャスト検出に復帰し、コントローラの IP を新しい値に再設定できます。

使用例

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。最初のコマンドで接続モードに入り、AP を 設定して DHCP から IP アドレスを取得するようにします (こうすることで、AP が DNS サーバに接続し、ホスト名「wlan-controller」に IP アドレスを問い合わせることができます)。

```
controller(config-ap)# connectivity l3-preferred
controller(config-ap-connectivity)#ip address dhcp
controller(config-ap-connectivity)#controller hostname wlan-controller
```

関連コマンド

- [controller domainname \(595 ページ\)](#)
- [controller hostname \(596 ページ\)](#)
- [controller ip \(597 ページ\)](#)
- [ip address dhcp \(269 ページ\)](#)
- [ip dns-server \(274 ページ\)](#)
- [show ap-connectivity \(632 ページ\)](#)

contact

アクセス ポイントの担当者を指定します。

構文

contact *contact*

contact 担当者の名前

コマンド モード

AP 設定

デフォルト

なし

用途

このコマンドで、アクセス ポイントの担当者を設定します。

使用例

```
controller(config-ap)# contact Bob  
controller(config-ap)#
```

関連コマンド

[location](#) (611 ページ)

controller domainname

アクセス ポイントを検出するコントローラ ドメイン名を設定します。

構文

`controller domainname`

コマンド モード

AP 接続設定

デフォルト

なし

用途

コントローラのドメイン名を設定します。

使用例

```
controller(config-ap-connectivity)# controller domainname acme  
controller(config-ap-connectivity)#
```

関連コマンド

- [controller hostname \(596 ページ\)](#)
- [controller ip \(597 ページ\)](#)

controller hostname

アクセス ポイントを検出するコントローラ ホスト名を設定します。

構文

`controller hostname hostname`

コマンド モード

AP 接続設定

デフォルト

なし

用途

コントローラの IP ホスト名を設定します。

使用例

```
controller(config-ap-connectivity)# controller hostname acmeCorp  
controller(config-ap-connectivity)#
```

関連コマンド

- [controller domainname \(595 ページ\)](#)
- [controller ip \(597 ページ\)](#)

controller ip

アクセス ポイントを検出するコントローラ IP を設定します。

構文

controller ip address

address コントローラの IP アドレスを設定します。

コマンド モード

AP 接続設定

デフォルト

なし

用途

コントローラの IP アドレスを設定します。

使用例

```
controller(config-ap-connectivity)# controller ip address 10.0.220.30
controller(config-ap)#
```

関連コマンド

- [controller domainname \(595 ページ\)](#)
- [controller hostname \(596 ページ\)](#)

dataplane-encryption

AP とコントローラの間データプレーン接続の暗号化を有効または無効にします。

構文

`dataplane-encryption {on | off}`

コマンド モード

AP 設定

デフォルト

データプレーン暗号化はオフです。

用途

このコマンドは、AP とコントローラの間データプレーン接続を暗号化します。メッシュおよびリモート AP で使用するよう設計されていますが、他の場所でも使用できます。この機能は、データ トンネル経由で送信されるデータ トラフィックが (エンドポイントの) AP とコントローラによって暗号化される IPsec のようなセキュリティ モードを提供します。暗号化アルゴリズムは 3DES.a です。この機能を有効にすると、暗号化 / 復号化がソフトウェアで実行されるため、パフォーマンスに影響します。

使用例

```
controller(config-ap)# dataplane-encryption on
controller(config-ap)#
```

関連コマンド

| description

アクセス ポイントを説明するテキスト。

構文

description *description*

description

アクセス ポイントの説明。説明の長さが 64 文字を超えると、Web インターフェイス ページが読みにくくなる場合があります。

コマンド モード

AP 設定

デフォルト

なし

用途

アクセス ポイントをテキストで説明します。

使用例

```
controller(config-ap)# description serves_QA+IT
controller(config-ap)#
```

関連コマンド

- [building](#) (588 ページ)
- [floor](#) (601 ページ)
- [location](#) (611 ページ)

fixed-channel

RF チャンネルを固定して、自動チャンネル設定で変更できないようにします。

構文

```
fixed-channel enable  
no fixed-channel
```

enable 固定チャンネル モードを有効にします。

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

no fixed-channel

用途

このコマンドを使用して、**autochannel** コマンドで自動チャンネル割り当てが実行されるのを回避します。**enable** キーワードを使用すると、固定チャンネル機能が有効になります。このコマンドでチャンネルを固定する前に、**channel** コマンドを使用してチャンネルを設定します

no fixed-channel コマンドを使用すると、自動チャンネル モードに戻ります。

使用例

```
controller(config-if_802)# fixed-channel enable  
controller(config-if_802)#
```

関連コマンド

- [autochannel](#) (586 ページ)
- [channel](#) (589 ページ)

floor

アクセス ポイントを配置するフロアを指定します。

構文

floor *floor-name*

floor-name アクセス ポイントを配置するフロアの名前。フロアの名前には 64 文字以下の英数字を使用できます。名前にスペースを使用する場合は、二重引用符 (" ") で囲みます。

コマンドモード

特権 EXEC

デフォルト

なし

用途

floor コマンドの使用はオプションであり、情報提供の目的でのみ使用します。

使用例

次のコマンドは、ノード ID が「2」のアクセス ポイントが「second floor (2 階)」に設置されていることを指定します。

```
controller# ap 2
controller(config-ap)# floor "second floor"
controller(config-ap)#
```

関連コマンド

- [building](#) (588 ページ)
- [location](#) (611 ページ)

hostname

アクセス ポイントのホスト名を設定します。

構文

`hostname hostname`

hostname 1 ～ 37 文字でホスト名を指定します。

コマンド モード

AP 接続設定

デフォルト

なし

用途

アクセス ポイントのホスト名を設定します。

使用例

```
controller(config-ap)# hostname acme  
controller(config-ap)#
```

interface Dot11Radio

設定の AP 無線インターフェイスを選択し、802.11 設定モードに入ります。

構文

```
interface Dot11Radio node-id interface_ID
```

<i>node-id</i>	設定するアクセス ポイントを選択します。
<i>interface_ID</i>	AP に無線が 2 つ存在する場合に、1 つ目または 2 つ目のどちらの無線インターフェイスであるかを指定します。 <i>interface_ID</i> は 1 または 2 です。

コマンドモード

グローバル設定

デフォルト

なし

用途

Dot11Radio モードに移動し、個々のアクセス ポイント インターフェイスを設定します。

使用例

```
controller(config)# interface Dot11Radio 1 1
controller(config-if-802)# ?
admin-mode           Administrative Mode.
antenna-property     Manage external wireless interface antennas.
antenna-selection    Antenna configuration.
channel              Configure the channel ID.
default              Set various parameters to the default value.
do                   Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
fixed-channel        Fix channel so it cannot be changed by auto-channel
configuration.
interop-mode         B/G protection mechanism.
mode                 AP mode configuration.
no                   Disables various parameters.
```

power example, 20,20,20.	Transmit power in the format low,medium,high.For
preamble-short	Enables short preamble.
protection-mode	bg protection mode.
rf-mode or bg).	Configure the Radio Frequency mode (802.11a, b, g,
scanning-channels	Configure the channels for scanning.
show interface.	Displays various parameters related to this wireless
tuning	Tune wireless interface.

関連コマンド

- [antenna-property](#) (578 ページ)
- [antenna-selection](#) (579 ページ)
- [channel](#) (589 ページ)
- [fixed-channel](#) (600 ページ)
- [protection-mode](#) (624 ページ)
- [preamble-short](#) (622 ページ)

led

LED モード ライトの点滅パターンを指定します。

構文

```
led {blink | NodeId | Normal}
```

blink	LED モードが 2 回短く点滅し、その後に 4 回短く点滅します。
NodeId	LED モード ライトの緑の短い点滅は、AP ID の末尾の数字を表します。緑の短い点滅の数は、AP ID のモジュロ 10 の数を表します。したがって、AP ID 4、14、24 の場合、NodeId モードは黄のライトが長く点滅した後に、緑のライトが短く 4 回点滅します。AP ID が 7、17、27 の場合、NodeId モードは黄のライトが長く点滅した後に、緑のライトが短く 7 回点滅します。このモードを使用することで、システムで特定の AP と他の AP を区別できます。
Normal	LED 点滅パターンは AP によって制御されます。

コマンド モード

AP 設定

デフォルト

デフォルトは **blink** (点滅) です。

用途

このコマンドを使用して、LED モード ライトの点滅パターンを指定します。いずれの場合にも、動作していなければ LED はオフになり、点灯しません。

使用例

次のコマンドは、点滅パターンを **Normal** に変更します。

```
controller(config-ap)# led normal
```

link

AP コネクタのリンク タイプを指定します。

構文

`link {Point-To-Point | Point-To-Multi-Point}`

コマンド モード

アンテナ プロパティ サブモード設定

デフォルト

Point-To-Multi-Point

用途

コネクタのリンク タイプを指定します。

使用例

`controller(config-ap)# link Point-To-Point`

関連コマンド

- [antenna-property \(578 ページ\)](#)
- [ap \(580 ページ\)](#)

link-probing-duration

コントローラのリンクが切断した場合の AP のリポートまでの待機時間を指定します。

構文

`link-probing-duration duration`

duration AP の待機時間を分単位で指定します。*duration* には 1 ～ 32000 を指定できます。

コマンド モード

AP 設定

デフォルト

なし

用途

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を (1 ～ 32000 分) 指定します。このコマンドをリモート 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。

使用例

```
controller(config-ap)# link-probing-duration 32000
```

関連コマンド

keepalive-timeout

AP へのリンクがダウンした場合であっても、コントローラから見て、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。

構文

```
controller(config-ap)# keepalive-timeout 1800
```

コマンドモード

AP 設定

デフォルト

なし

用途

AP へのリンクがダウンした場合であっても、コントローラから見て、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。

使用例

```
controller(config-ap)# keepalive-timeout 1800
```

関連コマンド

localpower

アンテナ ゲインを含む、AP 無線の最大転送電力を設定します。

構文

`localpower power-level`

- power-level* 無線の転送電力レベル (dBm)。このレベルは、使用している無線帯域や国コードによって異なります。米国では、*power-level* は、次の範囲の整数です。
- 802.11A 無線の場合は **5 ~ 最大 / チャンネル (下表参照)**
 - 802.11/Bg 無線の場合は **4 ~ 30**

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

802.11/Bg 無線の場合は 20、802.11a 無線の場合は 17

用途

フォーティネットの定義による転送電力は、アンテナでの EIRP1 (Effective Isotropic Radiated Power : 実効等方輻射電力) であり、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)。無線転送電力設定は、近接アクセス ポイント間でのコンテンツの管理に役立ちます。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 の場合にはチャンネル) に依存します。

米国におけるチャンネルと最大電力を下表に記載します。

チャンネル	米国における最大転送電力 (dBm)
36	23
40	23
44	23
48	23
52	30

チャンネル	米国における最大転送電力 (dBm)
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

使用例

次の例は、802.11/bg 無線の電力レベルを低くします。

```
controller(config-if_802)# localpower 17
controller(config-if_802)#
```

location

アクセス ポイントの場所。

構文

`location location`

location

アクセス ポイントの場所。

コマンド モード

AP 設定

デフォルト

なし

用途

アクセス ポイントの場所を説明します。

使用例

```
controller(config-ap)# location 10ft_from_west_window
```

関連コマンド

- [contact](#) (594 ページ)
- [description](#) (599 ページ)

mac-address

アクセス ポイントの MAC アドレス。

構文

`mac-address <MAC-address>`

mac-address 16 進表示のアクセス ポイントの MAC アドレス。

コマンド モード

AP 設定

デフォルト

なし

用途

アクセス ポイントの MAC アドレスを設定します。

使用例

```
controller(config-ap)# mac-address 00:E5:F0:B8:2A:3F00:12:F2:B8:2A:3F
controller(config-ap)#
```

関連コマンド

[ap \(580 ページ\)](#)

mimo-mode

AP300 の MIMO モードを設定します。

構文

mimo-mode [2x2 | 3x3]

2x2	2 つのデータ ストリームを送信し、この AP の 2 つのストリームでデータを受信します。
3x3	3 つのデータ ストリームを送信し、この AP の 3 つのストリームでデータを受信します。

コマンドモード

インターフェイス Dot11Radio 設定サブモード

デフォルト

2x2

用途

このコマンドを使用して、AP300 の MIMO モードを設定します。MIMO モードは、AP300 電源設定で調整する必要があります。MIMO モードと電源の関係は下記のとおりです。

電源	サポートする MIMO モード
802.3-af	デフォルトの電源。従来の 802.3-af PoE を使用する場合に選択します。この電源タイプは AP300 で 2x2 MIMO モードのみをサポートします。
802.3-at	高出力の次世代 PoE を使用する場合に選択します。この電源タイプは AP300 で 2x2 と 3x3 の両方の MIMO モードをサポートします。
5V-DC	オプションの ACC-AP300-PWR 電源を壁面コンセントに差し込む場合に選択します。この電源タイプは 2x2 と 3x3 の両方の MIMO モードをサポートします。
dual-802.3af	従来型の 2 つの 802.3-af PoE の電源の組み合わせによるドングルを使用する場合に選択します。この電源タイプは 2x2 と 3x3 の両方の MIMO モードをサポートします。

使用例

次の mimo-mode コマンドは、MIMO モードを 3x3 に設定します。

```
default config terminal
```

```
default(config)interface Dot11Radio 1 1
default(config-if-802)# mimo-mode 3x3
```

関連コマンド [*power-supply*](#) (620 ページ)

mode

AP 無線モードを、監視のみ、または通常のワイヤレス サービスの提供に設定します。

構文

```
mode {normal | scanning}
```

normal	AP 無線を通常のワイヤレス サービスを提供するよう設定します。
scanning	AP 無線を連続監視サービスのみを提供するよう設定します。

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

用途

指定したアクセス ポイントの無線を、指定したサービス タイプを提供するよう設定します。2 つの無線がインストールされている AP200 の場合には、それぞれの無線の機能モードを設定できます。

使用例

```
controller(config-if_802)# mode scanning
controller(config-if_802)#
```

model

AP モデル タイプを設定します。

構文

```
model {type}
```

type AP モデル タイプを設定します。

コマンド モード

AP 設定

デフォルト

用途

指定したアクセス ポイントのハードウェア モデル タイプを設定します。

使用例

```
controller(config-ap)# model AP320  
controller(config-ap)#
```

n-only-mode

802.1n をサポートする AP の無線の 802.11n-only を有効 / 無効にします。

構文

```
n-only-mode
no n-only-mode
```

コマンドモード

Dot11Radio サブモード

デフォルト

802.11n only モードは無効です。

制限事項

802.11n ではない AP ではサポートされません。

用途

802.11n をサポートする AP では、**n-only-mode** コマンドを使用して、無線で 802.11n プロトコルのみを有効にして、802.11n クライアントのみに関連付けを許可するようにします。802.11bg または 802.11a (周波数帯域による) のクライアントが無線を共有すると 802.11n のスループットが低下するため、このように設定することでパフォーマンスが向上します。

no n-only-mode コマンドを使用して、このモードを無効にし、802.11bg または 802.11a のユーザの関連付けを許可します。

使用例

この機能を無線で有効にします。

```
controller(config-if-802)# n-only-mode
```

この機能を無線で無効にします。

```
controller(config-if-802)# no n-only-mode
```

関連コマンド

[show interfaces Dot11Radio \(639 ページ\)](#)

parent-ap

エンタープライズ メッシュで、親 AP の ID を設定します。

構文

```
parent-ap AP_ID
```

ID 親 AP を示す整数。

コマンド モード

AP 設定

デフォルト

親 AP ID は 0 に設定されます。

用途

エンタープライズ メッシュ構成では、親 AP は、設定する AP の逆送接続を提供するよう指定されている AP です。親 AP はワイヤレス モードの AP に設定され、ゲートウェイ AP には設定されません。

エンタープライズ メッシュ構成では、第 1 層のみで、有線イーサネット接続経由でゲートウェイ AP が接続されます。メッシュのそれ以外の AP は、中間 AP またはリーフ AP のいずれかになり、親 AP との逆送ワイヤレス通信に 802.11a チャンネルを使用します。

設定手順などのこの機能の詳細については、『FortiWLC (SD) 設定ガイド』の「エンタープライズ メッシュ」の章を参照してください。

使用例

次の例は、AP 1 を AP 2 の親 AP に設定します。

```
controller(config-ap)# parent-ap 1
controller(config-ap)#
```

show ap コマンドで、親 AP の設定が表示されます。

```
controller(config-ap)# do show ap 2
AP Table
```

AP ID	: 2
AP Name	: AP-2
Serial Number	: 00:12:F2:00:00:24
Uptime	: 00d:00h:00m:00s

```
Location          :
Building          :
Floor             :
Contact           :
Operational State : Enabled
Availability Status : Online
Alarm State       : No Alarm
LED Mode          : Normal
AP Init Script    :
Boot Image Version : 3.9
FPGA Version      : wmac0:14.0
Runtime Image Version : 3.5-46
Connectivity Layer : None
Dataplane Encryption : off
AP Role           : wireless
Parent MAC Address : 00:12:F2:0:00:23
Parent AP ID      : 1
Link Probing Duration : 120
AP Model          : AP100
AP Label          : ATS1
Sensor AP ID      : 0
Hardware Revision : Rev 3
```

関連コマンド

- [ap \(580 ページ\)](#)
- [role \(627 ページ\)](#)
- [show ap \(629 ページ\)](#)

power-supply

指定したソースから給電するよう、AP300 に指示します。

構文

`power-supply [5V-DC | 802.3-af | 802.3-at | dual-802.3-af]`

電源	サポートする MIMO モード
802.3-af	デフォルトの電源。従来の 802.3-af PoE を使用する場合に選択します。この電源タイプは AP300 で 2x2 MIMO モードのみをサポートします。
802.3-at	高出力の次世代 PoE を使用する場合に選択します。この電源タイプは AP300 で 2x2 と 3x3 の両方の MIMO モードをサポートします。
5V-DC	オプションの ACC-AP300-PWR 電源を壁面コンセントに差し込む場合に選択します。この電源タイプは 2x2 と 3x3 の両方の MIMO モードをサポートします。
dual-802.3-af	従来型の 2 つの 802.3-af PoE の電源の組み合わせによるドングルを使用する場合に選択します。この電源タイプは 2x2 と 3x3 の両方の MIMO モードをサポートします。

コマンドモード

AP 設定サブモード

デフォルト

5V-DC

用途

このコマンドを使用して、AP300 の電源を設定します。

MIMO モードを 3x3 に変更する前に、電源設定を **DC power supply** または **802.3at PoE** のいずれかに必ず設定します。

使用例

次のコマンドは、壁面コンセントの電源から給電するよう AP300 に指示します。

```
default config terminal
default(config)ap 1
default (config-ap)# power-supply 5V DC
```

関連コマンド [mimo-mode](#) (613 ページ)

preamble-short

短いプリアンブルを使用するかどうかを指示します。

構文

```
preamble-short  
no preamble-short
```

コマンド モード

Dot11Radio インターフェイス設定

デフォルト

デフォルトで、短いプリアンブルが設定されます。

用途

このコマンドを使用して、プリアンブルを設定します。**no** 機能を使用すると、短いプリアンブルが無効になり、長いプリアンブルが使用されます。この機能は、オンまたはオフのいずれかです。

使用例

```
controller(config-if_802)# preamble-short  
controller(config-if_802)#
```

関連コマンド

protection-cts-mode

無線相互運用モードを設定します。

構文

protection-cts-mode {wmm-txop | 802.11-1999}

wmm-txop	802.11a フレームに WMM 方式の TXOP 保護を使用します。802.11b/802.11g が混在する環境で、一般的なスループットを上回る 802.11g クライアントのパフォーマンスが提供されます。
802.11-1999	802.11g フレームにワンフレーム保護を使用します。802.11b/802.11g が混在する環境で、標準の 802.11 パフォーマンスが提供されます。

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

デフォルトのモードは 802.11-1999 です。

用途

アクセス ポイントの相互運用モードを設定します。wmm-txop オプションでは、WMM TXOP 機能をインテリジェントな方法でデータに利用することで、パフォーマンスを向上できます。

使用例

```
controller(config-if_802)# protection-cts-mode wmm-txop
```

protection-mode

bg 保護モード設定を管理します。

構文

```
protection-mode {auto | off | on}  
no protection-mode
```

auto	使用中の無線のタイプで、デュアル スピード保護モードが自動的に有効になります。
off	デュアル スピード保護モードが常に無効になります。
on	デュアル スピード保護モードが常に有効になります。

コマンドモード

Dot11Radio インターフェイス設定

デフォルト

保護モードの **auto** 設定がデフォルトで有効になります。

用途

このコマンドを使用して、無線インターフェイスの bg 混在モード保護メカニズム モードを、**on**、**off**、または **auto** に設定します。**auto** を選択すると、使用中の無線のタイプで、802.11bg デュアル スピード保護メカニズムが有効になります。802.11Bg 無線では、802.11b が存在し、保護モードが有効 (**on** または **auto**) になっていると、802.11g クライアントで最適なパフォーマンスが得られます。このオプションは、802.11b のみや 802.11a 無線には影響しません。

使用例

自動保護モード設定を無効にするには、以下のように指定します。

```
controller(config-if_802)# protection-mode off
```

保護モード設定を有効にするには、以下のように指定します。

```
controller(config-if_802)# protection-mode on
```

保護モード設定を自動に戻すには、以下のように指定します。

```
controller(config-if_802)# protection-mode auto
```

関連コマンド

[rf-mode](#) (626 ページ)

rfband

アンテナ バンドを設定します。

構文

`rfband {2.4GHz | 5GHz | dual}`

コマンド モード

Dot11Radio インターフェイス設定

デフォルト

用途

デュアルバンドの無線処理を設定する場合に、**rfband** コマンドで、使用中の無線のタイプにアンテナ バンドを設定します。

使用例

```
default# configure terminal
default(config)# interface Dot11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# type External-dual-mode
default(config-if-802-antenna)# rfband dual
default(config-if-802-antenna)# end
default(config-if-802)# end
default(config)# end
```

関連コマンド

- [antenna-property](#) (578 ページ)
- [antenna-selection](#) (579 ページ)
- [interface Dot11Radio](#) (603 ページ)

rf-mode

無線周波数モードを設定します。

構文

`rf-mode mode`

mode

無線周波数を指定します。*mode* は次のいずれかです。

- **802.11a** - 802.11a 標準規格を指定します。
- **802.11b** - 802.11b 標準規格を指定します。
- **802.11bg** - 802.11b/g 相互運用モードを指定します。
- **802.11g** - 802.11g 標準規格を指定します。

コマンド モード

Dot11Radio インターフェイス設定

デフォルト

用途

アクセス ポイントの無線周波数モードを設定します。このコマンドで、無線バンドを選択できます。802.11bg モードを選択すると、独自の保護モードを設定でき、bg 混在環境での g クライアントのパフォーマンスが向上します。

使用例

AP 201 で、次のコマンドで 802.11bg 混在モードを使用するよう選択します。

```
controller(config-if_802)# rf-mode 802.11bg
controller(config-if_802)#
```

関連コマンド

[protection-mode \(624 ページ\)](#)

role

WLAN の AP の運用ロールを設定します。

構文

```
role { access | gateway | wireless }
```

access	非エンタープライズ メッシュ構成の AP のロール (デフォルト)。
gateway	エンタープライズ メッシュ構成で、イーサネット ポート経由で接続される AP。
wireless	エンタープライズ メッシュ構成で、ゲートウェイ AP ではない任意の AP。

コマンドモード

AP 設定

デフォルト

access モード

用途

AP は、access、gateway、または wireless の 3 つのモードのいずれかになります。エンタープライズ メッシュの一部ではない AP は、access モードになります。

エンタープライズ メッシュ構成では、1 つの AP がゲートウェイ AP に指定され、それ以外のすべての AP はワイヤレス モードになります。

エンタープライズ メッシュ構成では、第 1 層のみで、有線イーサネット接続経由でゲートウェイ AP が接続されます。メッシュのそれ以外の AP は、中間 AP またはリーフ AP であり、いずれもワイヤレスです。ワイヤレス AP は、802.11a チャネルを使用して、親 AP との逆送ワイヤレス通信を実行します。

設定手順などのこの機能の詳細については、『FortiWLC (SD) 設定ガイド』の「エンタープライズ メッシュ」の章を参照してください。

使用例

次の例は、AP 1 をゲートウェイ AP として設定します。

```
controller(config-ap)# role gateway
controller(config-ap)#
show ap コマンドで、親 AP の設定が表示されます。
controller(config-ap)# do show ap 1
```

AP Table

AP ID	: 1
AP Name	: AP-1
Serial Number	: 00:12:F2:0:00:23
Uptime	: 00d:00h:00m:00s
Location	:
Building	:
Floor	:
Contact	:
Operational State	: Disabled
Availability Status	: Offline
Alarm State	: No Alarm
LED Mode	: Normal
AP Init Script	:
Boot Image Version	: 3.9
FPGA Version	: wmac0:14.0
Runtime Image Version	: 3.5-46
Connectivity Layer	: None
Dataplane Encryption	: off
AP Role	: gateway
Parent MAC Address	: 00:00:00:00:00:00
Parent AP ID	: 0
Link Probing Duration	: 120
AP Model	: AP100
AP Label	: ATS1
Sensor AP ID	: 0
Hardware Revision	: Rev 3

関連コマンド

- [ap \(580 ページ\)](#)
- [parent-ap \(618 ページ\)](#)
- [show ap \(629 ページ\)](#)

show ap

アクセス ポイントの情報を表示します。

構文

show ap [*node-id*]

node-id オプション。アクセス ポイントの ID 番号。

コマンド モード

EXEC

デフォルト

なし

用途

アクセス ポイントの情報として、AP の ID と名前、MAC アドレス、動作状態、可用性ステータス、ランタイム イメージバージョン、接続レイヤ、モデル タイプ、リモート / ローカル配置などを表示します。オプションの ID を入力すると、そのアクセス ポイントの詳細情報が表示されます。現在、システムに存在するすべてのアクセス ポイントの概要情報を表示する場合は、ID を入力しないでください。

動作状態や可用性ステータスで、アクセス ポイントの状態を判断します。一般的なステータスの組み合わせとその意味は以下のとおりです。

- Enabled で On-line: アクセス ポイントは正しく動作している。
- Disabled で Off-line: コントローラがアクセス ポイントと通信できない。
- Disabled で On-line: アクセス ポイントまたはネットワークが正しく設定されていない。

機器が事前に設定されているか、検出されているか、または電源オフになっているか、可用性ステータスで監視します。ステータスの表すすべての値を、下表に記載します。

可用性ステータス	説明
Not Installed	ネットワーク エlementは事前プロビジョニングが完了していますが、検出されていません。
PowerOff	ネットワーク エlementはインストールされています (少なくとも 1 度は検出されています) が、現在は電源オンになっていません。

可用性ステータス	説明
Off-line	ネットワーク エlementは電源オンになっていますが、管理アクションによってオフラインになりました。
On-line	ネットワーク エlementは正しく動作しています。
Failed	ネットワーク エlementはインストールされ、電源がオンになっていますが、正しく動作していません。
In-test	ネットワーク エlementは現在、テストのための管理アクションを実行しているためにサービスを停止しています。

使用例

```
controller# show ap
```

AP ID	AP Name	Serial Number	Op State	Availability	Runtime
Connectivity	AP Model	AP Type			
1	#1-2F-QA-20	00:12:F2:00:2f:24	Disabled	Offline	3.2-1163.2.5-
7	None	AP208 Local			
2	#2-2F-Sw-20	00:12:F2:00:30:98	Enabled	Online	3.2-1163.2.5-
7	L3	AP208 Local			
3	#3-2F-Exec-	00:12:F2:00:17:94	Enabled	Online	3.2-1163.2.5-
7	L2	AP201 Local			
4	#4-2F-HW-20	00:12:F2:00:2f:3a	Disabled	Offline	None
	AP208 Local				
5	#5-1F-Front	00:12:F2:00:2e:c4	Disabled	Offline	None
	AP208 Local				

```
meru-wifi# show ap 1
```

AP Table

AP ID	: 1
AP Name	: #1-2F-QA-208
Serial Number	: 00:0c:e6:00:2f:24
Uptime	: 00d:00h:00m:00s
Location	: SunnyvaleSanta Clara
Building	: HQ
Floor	: 2nd floor
Contact	: Sam
Operational State	: Disabled

Availability Status	: Offline
Alarm State	: Critical
Enable High Density	: off
LED Mode	: Normal
AP Init Script	:
Boot Image Version	: 3.09.0003.9.01
FPGA Version	: 8.38.3wmac0:11.0 wmac1:11.0
Runtime Image Version	: 3.2-1163.2.5-71
Connectivity Layer	: None
Dataplane Mode	: tunneled
Link Probing Duration	: 120
AP Model	: AP208
AP Type	: Local

show ap-connectivity

アクセス ポイント接続を表示します。

構文 `show ap-connectivity`

コマンド
モード EXEC

デフォルト なし

用途 アクセス ポイントの接続情報として、設定のタイプ、使用された検出プロトコル、接続レ
イヤ、IP アドレスなどが表示されます。

使用例 次のコマンドは、すべての AP のアクセス ポイント接続情報を表示します。

default# `show ap-connectivity`

AP ID	AP Name	IP Configuration	Discovery Protocol	Connectivity	IP Address
1	#1-2F-QA-208	Static	L3-preferred	None	0.0.0.0
16	CustSup	Static	L3-preferred	L3	192.168.9.11
18	Mktg	Static	L3-preferred	L3	192.168.9.14
26	AP-26	DHCP	L2-preferred	L2	0.0.0.0
28	AP-28	Static	L3-preferred	L2	192.168.1.71
29	AP-29	Static	L2-preferred	L2	0.0.0.0
AP Network Connectivity configuration(6)					

次のコマンドは、AP 1 の詳細な接続情報を表示します。

default# `show ap-connectivity 1`
AP Network Connectivity configuration

AP ID : 1

AP Name : #1-2F-QA-208
IP Configuration : Static
Static IP Address : 192.168.10.21
Static IP Netmask : 255.255.255.0
Static Default Gateway : 192.168.10.1
Primary DNS Server : 10.0.0.10
Secondary DNS Server : 10.0.0.40
AP Host Name : Ap4-2F-QA
Discovery Protocol : L3-preferred
Controller Address : 192.168.10.2
Controller Host Name :
Controller Domain Name :
Connectivity Layer : None
Domain Name : localdomain
IP Address : 0.0.0.0
NetMask : 0.0.0.0
Gateway : 0.0.0.0
DNS Server 1 : 0.0.0.0
DNS Server 2 : 0.0.0.0
DNS Server 3 : 0.0.0.0
DNS Server 4 : 0.0.0.0
DNS Server 5 : 0.0.0.0
DNS Server 6 : 0.0.0.0
DNS Server 7 : 0.0.0.0
DNS Server 8 : 0.0.0.0

関連コマンド

- [show ap \(629 ページ\)](#)
- [show ap-discovered \(634 ページ\)](#)

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。

構文

show ap-discovered [*MAC_address*]

MAC_address オプション。この MAC アドレスの情報を表示します (ステーションまたは AP)。

コマンドモード

EXEC

デフォルト

なし

用途

システムで検出されたアクセス ポイントとステーションを表示します。

使用例

controller# **show ap-discovered**

ID BSSID	MAC Address Last	Type Previous	Channel Current	SSID Pkts Rx	RF Band	Name
16 00:0c:e6:07:32:c3 CustSup	00:02:2d:66:e1:b0 00d:00h:00m:20s 0	STATION	6 0	0	509	unknown
16 00:0f:f7:02:b7:4e CustSup	00:02:b3:d9:1f:54 00d:00h:00m:00s 14	STATION	6 14	13	8768	unknown
16 00:0f:8f:ef:9e:7f CustSup	00:02:b3:d9:1f:64 00d:00h:00m:18s 40	STATION	6 40	40	9	unknown
16 00:40:96:a3:72:22 CustSup	00:02:b3:e6:d7:12 00d:00h:00m:01s 17	STATION	6 17	23	1124	unknown
16 00:00:00:00:00:00 CustSup	00:03:2a:00:3c:58 00d:00h:00m:00s 0	STATION	6 0	0	3	802.11b
16 00:0c:e6:08:f0:8f CustSup	00:04:f2:00:3a:ae 00d:00h:00m:03s 13	STATION	6 13	13	6	unknown

```
16      00:06:25:09:21:0b STATION      6
00:0c:e6:06:ad:11 00d:00h:00m:01s 9      10      410      802.11b
CustSup

16      00:0c:85:76:35:ea STATION      6
00:0c:e6:02:5f:67 00d:00h:00m:00s 20     20      46298     unknown
CustSup

16      00:0c:e6:01:04:ff AP           6      qa-func
00:0c:e6:01:04:ff 00d:00h:00m:00s 4      4      178772     802.11g
CustSup

16      00:0c:e6:01:29:97 AP           6      meru-default
00:0c:e6:01:29:97 00d:00h:00m:00s 14     14      774781     802.11b
CustSup

16      00:0c:e6:01:3c:5f AP           6 meru-ess
00:0c:e6:01:3c:5f 00d:00h:00m:00s 24
```

関連コマンド

- [show ap \(629 ページ\)](#)
- [show ap-connectivity \(632 ページ\)](#)

show ap-redirect

AP とコントローラの割り当て設定を表示します。

構文

```
show ap-redirect ip-subnet <ip_subnet>  
show ap-redirect mac-address <mac_addr>
```

ip-subnet <ip_subnet> リダイレクトされるすべてのまたは指定した IP サブネット
アドレスを表示します。

mac-address <mac_addr> リダイレクトされるすべてのまたは指定した MAC アドレス
を表示します。

コマンド モード

特権 EXEC

デフォルト

なし

用途

アクセス ポイントのリダイレクト テーブルを表示します。

使用例

次の例は、MAC アドレスの AP リダイレクト テーブルを表示する方法を示します。

```
meru-wifi# show ap-redirect mac-address
```

```
AP MAC                      Destination Controller  
0:0c:e6:00:01:02    172.10.10.5  
                    Assignments of APs to controllers(1 entry)
```

関連コマンド

[ap-redirect](#) (583 ページ)

show ap-swap

アクセス ポイントの置換テーブルを表示します。

構文

show ap-swap

コマンド モード

EXEC

デフォルト

なし

用途

AP 置換テーブルのアクセス ポイント置換情報を表示します。AP のシリアル番号は AP の MAC アドレスであり、新規 AP シリアル番号として記載されている MAC アドレスに置換されます。

使用例

```
controller# show ap-swap
AP Serial Number      New AP Serial Number
00:0c:e6:00:05:02     00:0c:e6:00:30:98
      AP Replacement Table (1 entry)
controller#
```

関連コマンド

[swap ap \(660 ページ\)](#)

show ess-ap

アクセス ポイントの ESS-AP テーブルを表示します。

構文

`show ess-ap ap`

コマンド モード

AP 設定

デフォルト

なし

用途

ESSID、アクセス ポイント名、BSSID などの ESS-AP テーブルの情報を表示します。

使用例

controller# `show ess-ap ap 1`

ESS Profile	AP ID	AP Name	IfIndex	Channel	BSSID
meru-ess 16	CustSup	1	6		00:0c:e6:02:5f:67
meru-ess18	Mktg	1	6		00:0c:e6:02:5f:67
meru-ess26	AP-26	1	6		00:0c:e6:01:3c:5f
meru-ess28	AP-28	1	6		00:0c:e6:01:77:df
meru-ess29	AP-29	1	6		00:0c:e6:01:3c:5f

controller#

show interfaces Dot11Radio

AP ワイヤレス インターフェイスの設定を表示します。

構文

`show interfaces Dot11Radio [ap_id [if_index]]`

ap_id オプション。アクセス ポイントの ID。
if_index オプション。インターフェイスの ID。

コマンド モード

EXEC

デフォルト

なし

用途

すべての (または、オプションで指定した) AP ワイヤレス インターフェイスの設定を表示
します。ID 番号を入力して、特定のアクセス ポイントを指定します。

使用例

`controller# show interfaces Dot11Radio`

AP ID	AP Name	IfIndex	Op State	Channel	Short Preamble	AP Mode
16	CustSup	1	Enabled	6	on	Normal
18	Mktg	1	Enabled	6	on	Normal
26	AP-26	1	Enabled	6	on	Normal
28	AP-28	1	Enabled	6	on	Normal
29	AP-29	1	Enabled	6	on	Normal

Wireless Interface Configuration(5 entries)

`meru-wifi# show interfaces Dot11Radio 2`

AP ID	AP Name	IfIndex	AP Model	Admin State	Op State	Channel
Short Preamble	RF Band	AP Mode				

```
2      AP-2      1      AP100      Up      Disabled 6      on
802.11b      Normal
```

Wireless Interface Configuration(1 entry)

```
meru-wifi# show interfaces Dot11Radio 2 1
```

Wireless Interface Configuration

```
AP ID                : 2
AP Name              : AP-2
Interface Index      : 1
AP Model             : AP100
Description          : ieee80211-2-1
Administrative Status : Up
Operational Status   : Disabled
Last Change Time     : 2008/01/16 12:38:28
Radio Type           : RF1
MTU (bytes)          : 2346
Channel              : 6
Short Preamble       : on
RF Band Support      : 802.11b
RF Band Selection    : 802.11b
Antenna Selection    : None
Transmit Power High(dBm) : 21
AP Mode              : Normal
Fixed Channel        : off
Scanning Channels    : 1,2,3,4,5,6,7,8,9,10,11
Protection Mechanism : 802.11-1999
Protection Mode      : auto
Number of Antennas   : 1
Dual abg Support     : off
Fallback Channel     : 0
```

関連コマンド

show interfaces Dot11Radio antenna-property

AP アンテナのプロパティを表示します。

構文

```
show interfaces Dot11Radio antenna-property [[ap_ID] ifindex] connector
```

ap_ID	オプション。指定した AP のアンテナ制御情報を表示します。
ifindex	オプション。指定した AP ワイヤレス インターフェイスのアンテナ制御情報を表示します。
connector	オプション。指定したコネクタのアンテナ制御詳細情報を表示します。

コマンドモード

EXEC

デフォルト

なし

用途

このコマンドを使用して、アンテナのプロパティを表示します。引数を指定しないと、すべての AP のプロパティが表示されます。特定の AP、インターフェイス インデックス、またはコネクタの場所のプロパティを表示するよう指定できます。表示されるプロパティとしては、APID、インターフェイス インデックス、コネクタ番号 (左 =1、右 =2)、RF バンド、外部または内部のアンテナのタイプ、場所があります。

使用例

controller# show interfaces Dot11Radio antenna-property

AP ID	IfIndex	Connector	RF Band	Gain (dBm)	Type	Location
4	1	1	Dual	4	unknown	Left
4	1	2	Dual	0	unknown	Right
4	2	1	Dual	5	unknown	Left
4	2	2	Dual	0	unknown	Right
5	1	1	Dual	4	unknown	Left
5	1	2	Dual	0	unknown	Right
5	2	1	Dual	5	unknown	Left
5	2	2	Dual	0	unknown	Right

6	1	1	Dual	4	External	Left
6	1	2	Dual	4	External	Right
7	1	1	Dual	4	unknown	Left
7	1	2	Dual	0	unknown	Right
7	2	1	Dual	5	unknown	Left
7	2	2	Dual	0	unknown	Right
9	1	1	Dual	5	External	Left
9	1	2	Dual	5	External	Right
1	1	1	Dual	4	External	Left
1	2	1	Dual	5	External	Right
3	1	1	Dual	4	External	Left
10	1	1	Dual	4	External	Left
10	2	1	Dual	5	External	Right
8	1	1	Dual	4	External	Left
2	1	1	Dual	4	External	Left
2	2	1	Dual	5	External	Right

Antenna Property(24)

次のコマンドは、AP 5 のアンテナ プロパティを表示します。

controller# # show interfaces Dot11Radio antenna-property 5

AP ID	IfIndex	Connector	RF Band	Gain (dBm)	Type	Location
5	2	2	Dual	0	unknown	Right
5	2	1	Dual	5	unknown	Left
5	1	2	Dual	0	unknown	Right
5	1	1	Dual	4	unknown	Left

Antenna Property(4)

次のコマンドは、AP 5、インターフェイス 1 のアンテナ プロパティを表示します。

controller# show interfaces Dot11Radio antenna-property 5 1

AP ID	IfIndex	Connector	RF Band	Gain (dBm)	Type	Location
5	1	1	Dual	4	unknown	Left
5	1	2	Dual	0	unknown	Right

Antenna Property(2)

次のコマンドは、AP 5、インターフェイス 1、コネクタ 1 のアンテナ プロパティを表示します。

```
controller# show interfaces Dot11Radio antenna-property 5 1 1
Antenna Property
```

```
AP ID           : 5
Interface Index  : 1
Connector       : 1
RF Band         : Dual
Antenna Gain (dBi) : 4
Link Type       : Point-To-Multi-Point
Antenna Type    : unknown
Location        : Left
```

関連コマンド [antenna-property \(578 ページ\)](#)

show interfaces Dot11Radio statistics

無線の統計を表示します。

構文

show interfaces Dot11Radio statistics [[ap_ID] ifindex]

- ap_ID

オプション。指定した AP の統計を表示します。
- ifindex

オプション。指定した AP ワイヤレス インターフェイス の統計を表示します。

コマンドモード

EXEC

デフォルト

なし

用途

このコマンドを使用して、AP とそのインターフェイスの統計を表示します。引数を指定しないと、すべての AP のプロパティが表示されます。特定の AP やインターフェイス インデックスのプロパティを表示するよう指定できます。下表に、統計の説明を記載します。

統計	説明
Interface Index	ワイヤレス インターフェイスの固有の ID 番号
AP ID	アクセス ポイントの固有の数値 ID
AP Name	アクセス ポイントの名前
Channel	動作チャネル
Associations	無線に関連付けられているデバイスの合計数
Throughput	無線の合計スループット レベル
Channel Utilization	動作チャネルの全体使用レベル (パーセント単位)
Noise	ノイズ レベル (dBm 単位)
Loss Percentage	全体の損失パーセント
Management Percentage	管理トラフィック専用フレームの合計パーセント

統計	説明
Beacon Percentage	ビーコン専用トラフィックの合計パーセント
Probe Percentage	ワイヤレスのプロブ要求パーセント
Neighborhood	エリア内の他のデバイスの数
Retry Percentage	ワイヤレスの再試行フレームのパーセント

使用例

```
controller# show interfaces Dot11Radio statistics
```

```
IfIndex AP-ID AP-Name Ch Assoc Thruput Ch-Util Noise Loss% Mgmt% Beacon%
Probe% Neighborhood Retry%
1 102 AP-102-THOMAS-J 6 0 9 40 -64 1 16 6 10 0 2
2 102 AP-102-THOMAS-J 157 1 12 24 -79 99 3 3 0 0 0
1 103 AP-103-Harsh-JA 6 16 2795645 58 -60 13 22 8 14 0 30
2 103 AP-103-Harsh-JA 157 24 58153893 59 -80 0 1 1 0 0 48
1 104 AP-104-POPOV-JA 6 0 48 46 -68 0 18 7 11 0 3
2 104 AP-104-POPOV-JA 157 2 2000 23 -71 3 3 3 0 0 49
1 105 AP-105-KGUHA-JA 6 0 0 38 -73 0 16 6 9 0 0
2 105 AP-105-KGUHA-JA 157 0 0 16 -74 0 4 2 1 0 0
Wireless (802.11) Statistics(8 entries)
```

```
controller# show interfaces Dot11Radio statistics 10 1
Wireless (802.11) Statistics
```

```
Interface Index : 1
AP ID : 102
AP Name : AP-102-THOMAS-JADE
Channel : 6
Failed Count : 7445442
Retry Count : 0
Multiple Retry Count : 4215324
Frame Duplicate Count : 4836511
RTS Success Count : 152178695
RTS Failure Count : 5244008733372
ACK Failure Count : 68313813
```

WEP Undecryptable Count : 0
FCS Error Count : 54800443737
PLCP Error Count : 6010397952
Transmit Frame Count : 11082548
Multicast Transmit Frame Count : 0
Transmit Fragment Count : 11082548
Multicast Received Frame Count : 994077
Received Fragment Count : 69849074627
Received Retried frame Count : 47635890
Received Unicast frame Count : 707331523
Assigned Station Count : 0
Associated Station Count : 0
Discovered Station Count : 480
Average throughput : 0
Channel Utilization : 40
Qos Discarded Fragment Count : 0
Qos CF Polls Rx Count : 0
Qos CF Polls Unused Count : 0
Qos CF Polls Unusable Count : 0
Qos CF Polls Lost Count : 0
Transmit AMSDU Count : 0
Failed AMSDU Count : 0
Retry AMSDU Count : 0
Multiple Retry AMSDU Count : 0
Transmit Octets In AMSDU Count : 0
AMSDU Ack Failure Count : 0
Received AMSDU Count : 2442
Received Octets In AMSDU Count : 0
Transmit AMPDU Count : 5149202
Transmit MPDUs in AMPDU Count : 9082500
Transmit Octets In AMPDU Count : 4374061387
Received AMPDU Count : 0
MPDUs in Received AMPDU Count : 4303092
Received Octets In AMPDU Count : 0
AMPDU Delimiter CRC Error Count : 0
Implicit BAR Failure Count : 0
Explicit BAR Failure Count : 0

Channel Width Switch Count : 186733328
Frame 20 Mhz Transmit Count : 0
Frame 40 Mhz Transmit Count : 0
Frame 20 Mhz Received Count : 10035323
Frame 40 Mhz Received Count : 0
PSMP Success Count : 0
PSMP Failure Count : 0
Granted RDG Used Count : 0
Granted RDG Unused Count : 0
Transmit Frames in Granted RDG Count : 0
Transmit Octets in Granted RDG Count : 0
Beamforming Count : 0
Dual CTS Success Count : 0
Dual CTS Failure Count : 0
STBCCTS Success Count : 0
STBCCTS Failure Count : 0
Non STBCCTS Success Count : 0
Non STBCCTS Failure Count : 0
RTSLSIG Success Count : 0
RTSLSIG Failure Count : 0
Transmit Retry Limit Exceed Count Unaggr : 0
Transmit Retry Limit Exceed Count Aggr : 0
Transmit Retry Limit Exceed Count Subframe in Aggr : 0
Transmit Retry Limit Exceed Count BAR : 0
Transmit Multiple Retry Count Unaggr : 0
Transmit Multiple Retry Count Subframe in Aggr : 0
Transmit Multiple Retry Count BAR : 0
Number of bytes received : 0
Number of bytes transmitted : 0
Unicast Beacon Loss Threshold Exceeded : 0
Current Noise Level : -76
Loss Percentage : 0
Tx Failed Count by Hardware Retry Exceed : 0
Rx Data for Assigned Stations : 0
Rx Management Frames : 0
Total Rx Management Frames : 0
Total Rx Control Frames : 0

Management Frame Overhead : 17
Transmitted Unicast Frame Count : 0
Received All Data Frame Count : 0
Frames blocked by RF-barrier : 0
Beacon Overhead : 6
Probe Request and Response Overhead : 11
Neighborhood Counter : 0
Potential Beacon Collision Counter : 0
Profile of Beacon Data Rate : H H
Retry Percentage : 0

show regulatory-domain

国の規制情報を表示します。

構文

`show regulatory-domain`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、コントローラが設定されている国の規制情報を表示します。

使用例

```
controller# show regulatory-domain
```

```
RF Regulatory Domain
```

```
Country Code           : USA
Country Name           : United States Of America
Default B/G Channel    : 6
Default A Channel      : 40
```

show statistics ap300-diagnostics

インターフェイスごとの AP300 診断統計のリストを表示します。

構文 `show statistics ap300-diagnostics`

コマンドモード 特権 EXEC モード

デフォルト なし

用途

使用例 次の例は、`show statistics AP300-diagnostics` コマンドの結果を表示します。

Master1# `show statistics ap300-diagnostics`

AP-ID	IfIndex	AP-Name	Fatal	HW	INT	Tx	Underrun	INT	Tx	Timeout	INT
Carrier	Sense	Timeout	Rx	Overrun	INT	Rx	EOL	INT			
3	1	3-Guha	0	0		321		0			
48		0									
3	2	3-Guha	0	0		213		0			
306		0									
4	1	4-QA.Facing	0	0		3446		0			
0		0									
4	2	4-QA.Facing	0	0		6689		0			
0		0									
5	1	5-Popov	0	0		687		0			
251		0									
5	2	5-Popov	0	0		322		0			
788		0									
8	1	8-Amazon	0	0		374119		0			
0		0									
8	2	8-Amazon	0	0		14		0			
0		0									
96	1	AP-96	0	0		1775		0			
12		0									

96 0	2	AP-96 1	0	0	0	0
98 0	1	9-GrndConf 0	0	0	3764	0
98 0	2	9-GrndConf 0	0	0	0	0
103 24	1	103-carlos 0	0	0	467	0
103 412	2	103-carlos 1	0	0	356	0
239 0	1	AP-239 0	0	0	7492	0
239 2	2	AP-239 0	0	0	2	0

AP300 Diagnostic Statistics(16 entries)

Master1#

関連コマンド

show statistics station-per-ap

AP ごとのステーション統計のリストを表示します。

構文

`show statistics station-per-ap`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、各 AP のステーションの統計を表示します。

使用例

```
default# show statistics station-per-ap
AP  AP-Name  If  Station-MAC      Station-IP      SSID      Rx
Rate  Tx Rate  Rx-Pkts      Tx-Pkts      EncrypErr
2   AP-2      1   00:03:7f:bf:08:1e  0.0.0.0      abcjk      0
15          0           229          0
2   AP-2      2   00:40:96:a8:af:f3  172.27.0.70  abcjk      34
52          12881        7330         0
23  AP-23     1   00:16:6f:1a:c8:56  0.0.0.0      diag       0
52          312          765          0

Station Per AP Statistics(3 entries)
```

show statistics top10-ap-problem

問題がある上位のアクセス ポイントのリストを表示します。

構文 show statistics top10-ap-problem

コマンド
モード ユーザ EXEC

デフォルト なし

用途 show statistics top10-ap-problem コマンドを使用して、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。送受信の 20% を下限として、パケット再送数が上位 10 のアクセス ポイントが表示されます。マルチセルの WLAN 環境では、アップリンク パケット損失を正確に計算できないため、ダウンリンク パケット送信のみが対象となります。

使用例 次のコマンドは、問題がある上位 10 のアクセス ポイントを表示します。

```
controller# show statistics top10-ap-problem
AP  AP Name    If Tx Loss Percentage
```

```
2    #2-2F-Sw- 2    37
      Top 10 problem AP statistics(1 entry)
controller#
```

653 ページの表 4 に、show statistics top10-ap-problem 出力のフィールドについて説明します。

表 4: show statistics top10-ap-problem の出力

フィールド	説明
AP	アクセス ポイントの固有の ID 番号
AP Name	アクセス ポイントの名前

表 4: `show statistics top10-ap-problem` の出力

フィールド	説明
If	AP のインターフェイス番号
Tx Loss Percentage	送信中に損失したパケット (肯定応答なし) の割合

関連コマンド [show statistics top10-ap-talker](#) (655 ページ)

show statistics top10-ap-talker

直近のポーリング期間の毎分の送受信パケット率の合計に基づく、上位 10 のアクティブなアクセス ポイントを表示します。

構文 show statistics top10-ap-talker

コマンド
モード EXEC

デフォルト なし

用途 show statistics top10-ap-talker コマンドを使用して、直近のポーリング間隔の毎秒の送受信パケット率の合計に基づく、上位 10 のアクティブなアクセス ポイントを表示します。アクティブなアクセス ポイントのテーブルには、実際に送受信されたバイト数や通信時間ではなく、毎秒のフレーム数に基づくアクティビティが表示されます。

使用例 次のコマンドは、上位 10 のアクティブなアクセス ポイントが表示されます。

```
controller# show statistics top10-ap-talker
AP   AP Name    If Rx Frames/min  Tx Frames/min

2    #2-2F-Sw- 2  10625300          11452490
3    #3-2F-Exe 1  125023            1360549
6    #6-1F-CS- 1  195022            884976
2    #2-2F-Sw- 1  38201             909269
10   #10-1F-Mk 1  57274             714166
8    #8-1F-Dem 1  113896            325462
10   #10-1F-Mk 2  53540             383962
11   AP-11      2  9329              202435
11   AP-11      1  5860              201866
1    #1-2F-QA- 1  0                  0

      Top 10 talker AP statistics(10)
controller#
```

656 ページの表 5 に、show statistics top10-ap-talker 出力のフィールドの説明を記載します。

表 5: `show statistics top10-ap-talker` の出力

フィールド	説明
AP	アクセス ポイントの固有の ID 番号
AP Name	アクセス ポイントの名前
If	AP のインターフェイス番号
Rx Frames/min	直近のポーリング期間の受信フレーム数
Tx Frames/min	直近のポーリング期間の送信フレーム数

関連コマンド

[show statistics top10-ap-problem](#) (653 ページ)

show topoap

システムが認識している AP を表示します。

構文 `show topoap`

コマンド
モード 特権 EXEC

デフォルト なし

用途 アクセス ポイントに関する、割り当てられているリソース、近接 AP 数、接続数、割り当て数などの情報を表示します。

使用例

```
controller# show topoap
```

AP ID	AP Name	RsRq	RsAlloc	Neighbor	Attached
2	#2-2F-Sw-208	0	0	4	2
10	#10-1F-Mktg-208	0	0	5	11
3	#3-2F-Exec-201	0	0	5	7
11	AP-11	0	0	2	0
6	#6-1F-CS-AP201	0	0	4	6
8	#8-1F-DemoArea-	0	0	4	9

AP Wireless Resources(6 entries)

関連コマンド [show topoapap \(658 ページ\)](#)

show topoapap

システムの AP/AP エッジ レコードを表示します。

構文 show topoapap

コマンド
モード 特権 EXEC

デフォルト なし

用途 このコマンドは、show ap-siblings の出力情報と同様に、相互に認識できる AP を表示します。出力に表示される AP に関係なく、同じ BSSID のすべての AP が 調整されます。

使用例 controller# show topoapap
RSSI between APs

Detecting AP ID	Detecting AP Name	Sibling AP ID	Sibling AP Name
26	AP-26	16	CustSup
26	AP-26	18	Mktg
26	AP-26	28	AP-28
26	AP-26	29	AP-29
16	CustSup	26	AP-26
16	CustSup	18	Mktg
16	CustSup	28	AP-28
16	CustSup	29	AP-29
18	Mktg	26	AP-26
18	Mktg	16	CustSup
18	Mktg	28	AP-28
18	Mktg	29	AP-29
28	AP-28	26	AP-26
28	AP-28	16	CustSup
28	AP-28	18	Mktg
28	AP-28	29	AP-29
29	AP-29	26	AP-26

29	AP-29	16	CustSup
29	AP-29	18	Mktg
29	AP-29	28	AP-28
RSSI between APs(20)#			

関連コマンド

- [show topoap \(657 ページ\)](#)

swap ap

置換する AP の MAC アドレスを設定します。

構文

```
swap ap <old_mac_address> <new_mac_address>  
no swap ap <old_mac_address>
```

- old_mac_address 置換する古い AP の MAC アドレスを指定します。
- new_mac_address 置換する新しい AP の MAC アドレスを指定します。

コマンドモード

グローバル設定モード

デフォルト

なし

制限事項

AP を置換する場合は、同じモデルの AP にのみ置換できます (この目的の場合には、AP300 と AP300i は同じです)。

用途

このコマンドは、AP ID に関連付けられている設定を更新します。各 AP に、追跡に使用する ID とシリアル番号 (その MAC アドレス) があります。この コマンドによって、サイトで交換する AP のシリアル番号を新しい AP のシリアル番号が同じになります。置換テーブルの 2 つのシリアル番号を 1 つの AP ID にリンクすることで、システムが古い AP に設定されている機能で新しい AP を更新できるようになります。こうすることで、置換した新しい AP に設定を再入力する必要がなくなります。AP 設定、インターフェイス設定、ESS 設定の 3 つの設定 が AP に影響します。

このコマンドは当初、場所や建物などの、AP の機能には関係しない一般的な設定を保存する目的で設計されましたが、リリース 4.0 から、以下の AP 設定属性も保存されるようになりました。

属性	AP 設定への保存	インターフェイス 設定への保存	ESS 設定への保存
AP ID	○	○	X
AP Name	○	○	X

属性	AP 設定への保存	インターフェイス 設定への保存	ESS 設定への保存
Location	○		X
Building	○	X	X
Floor	○	X	X
Contact	○	X	X
LED Mode	○	X	X
Connectivity	○	X	X
Link probing duration	○	X	X
Channel	X	○	X
RF Band Selection	X	○	X
power	X	○	X
AP mode	X	○	X
Protection Mechanism	X	○	X
Protection Mode	X	○	X
Short preamble	X	○	X

このコマンドの **no** フォームを使用すると、AP 置換テーブルから AP エントリが削除されます。

このコマンドを実行し、AP を実際に置換してから、システムをリブートします。置換テーブルがチェックされ、変更が適用されます。新しい AP が更新されると、置換テーブルからエントリが削除されます。

使用例

```
controller(config)# swap ap 00:0c:e6:bc:61:4e 00:11:11:11:11:01
controller(config)##show ap-swap
```

```
AP Serial Number      New AP Serial Number
```

```
00:0c:e6:bc:61:4e    00:11:11:11:11:01
```

```
AP Replacement Table(1 entry)
```

関連コマンド [show ap-swap \(637 ページ\)](#)

type

アンテナ タイプの AP アンテナ コネクタを設定します。

構文

```
type {External| External-dual-mode | RS-Antenna}
```

コマンドモード

Dot11Radio アンテナ プロパティ設定

デフォルト

外部モード アンテナ

用途

このコマンドは、使用するアンテナ タイプの AP アンテナ コネクタ ポートを設定します。デフォルトでは、アクセス ポイントと一緒に出荷されるアンテナでは **External** が使用されるため、出荷時にインストールされている AP では変更は不要です。

AP Dual 11a または Dual 11bg を運用する場合は、**External-dual-mode** オプションを設定する必要があります。

External-dual-mode のアンテナを使用する場合には、次の制約があります。

- 11bg バンドでは、チャンネル 1 と 11 を使用します。
- 11a バンドでは、12 チャンネル以上の分離を推奨します (たとえば、チャンネル 44 や 56)。
- 正しく動作させるには、無線に 50db ~ 60db の分離が必要です。この分離は、チャンネル分離、アンテナ タイプ、アンテナ ゲイン、および取り付け時のアンテナ間の物理的な距離によって異なります。外部アンテナを AP208 Dual abg 機能で使用することを検討している場合は、フォーティネット サポートにお問い合わせください。
- アンテナ タイプの「外部デュアル モード」を選択する場合は、11b/g には 3dBi、11a には 5dBi のデフォルトのゲインが設定されます。ゲインは、使用する外部アンテナと RF バンドの特性と一致させる必要があります。

RS-antenna は、AP200 Dual a/b/g モードをサポートし、特別なケーブルを使用する、オプションの RS4000 アンテナのパラメータです。

RS アンテナを使用する場合には、次の制約があります。

- 11b/g バンドでは、チャンネル 1 と 11 を使用します。アンテナ タイプを RS アンテナに設定すると、アンテナ ゲインが自動的に設定されます (つまり、RS アンテナを選択すると、システムの各 RF バンドにデフォルト ゲインがプリセットされます)。

- 11a バンドでは、12 チャンネル以上の分離を推奨します (たとえば、チャンネル 44 や 56)。RS アンテナを設定すると、アンテナ ゲインが正しく設定されます (つまり、RS アンテナを選択すると、システムの各 RF バンドにデフォルト ゲインがプリセットされます)。
- RS アンテナとパッチ ケーブルを使用してください。

使用例

次の例は、外部デュアル モード アンテナを設定します。

```
default# configure terminal
default(config)# interface Dot11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# type External dual-mode
```

次の例は、RS アンテナを設定します。

```
default# configure terminal
default(config)# interface Dot11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# type RS-antenna
```

関連コマンド

- [antenna-property \(578 ページ\)](#)
- [rfband \(625 ページ\)](#)
- [interface Dot11Radio \(603 ページ\)](#)

12 メッシュ コマンド

FortiWLC (SD) 5.2 以降では、適切なライセンスが付与されていれば、一部の AP モデルでメッシュ サポートを利用できます。本章では、メッシュのサポートに使用する CLI コマンドについて説明します。これらのコマンドの対象となるアクションはすべて、Web UI から実行できます。

メッシュ ネットワークの設定に関する詳細については、『FortiWLC (SD) 設定ガイド』の「エンタープライズ メッシュによるワイヤレス バックボーン」の章を 参照してください。



メッシュ操作は現在、AP1000 シリーズと AP332e/i モデルでのみサポートされています。

- [admin-mode](#) (666 ページ)
- [descr](#) (667 ページ)
- [mesh-ap](#) (668 ページ)
- [mesh-profile](#) (669 ページ)
- [plugnplay](#) (670 ページ)
- [psk](#) (671 ページ)

admin-mode

メッシュを有効または無効にできます。

構文

`admin-mode <enable/disable>`

Enable/Disable メッシュを有効または無効のどちらにするかを指定します。

コマンド モード

メッシュ設定

デフォルト

無効

用途

このコマンドを使用して、現在のメッシュ ネットワークを有効にします。**admin-mode** が有効であれば、メッシュ ネットワークは有効になります。

使用例

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# admin-mode enable
default(15)(config-mesh)# end
```

関連コマンド

- [mesh-profile \(669 ページ\)](#)
- [plugnplay \(670 ページ\)](#)

descr

現在のメッシュ プロファイルの説明を入力します。

構文

descr <*description*>

description 選択したメッシュ プロファイルの簡単な (0 ~ 128 文字) 説明

コマンド モード

メッシュ設定

デフォルト

なし

用途

このコマンドを使用して、メッシュの説明を指定します。128 文字以下で説明を入力します。

使用例

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# descr "Sample mesh profile."
default(15)(config-mesh)# end
```

関連コマンド

- [mesh-profile \(669 ページ\)](#)
- [psk \(671 ページ\)](#)

mesh-ap

指定した AP を現在のメッシュ プロファイルに追加します。

構文

mesh-ap <*number*>

number AP ID 番号。

コマンド モード

メッシュ設定

デフォルト

なし

用途

このコマンドを使用して、新しい AP を現在のメッシュに追加します。

使用例

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# mesh-ap 2
default(15)(config-mesh)# end
```

関連コマンド

- [mesh-profile \(669 ページ\)](#)
- [descr \(667 ページ\)](#)
- [psk \(671 ページ\)](#)

mesh-profile

メッシュ設定モードに入ります。

構文

`mesh-profile <profile>`

profile 変更するメッシュ プロファイルの名前。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、メッシュのプロパティにアクセスしたり、本章に記載する他のコマンドを使用して変更したりするのに使用します。メッシュをベースとするコマンドはすべて、メッシュ設定モードで実行されます。

使用例

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)#
```

関連コマンド

- [admin-mode \(666 ページ\)](#)
- [descr \(667 ページ\)](#)
- [mesh-ap \(668 ページ\)](#)
- [plugnplay \(670 ページ\)](#)
- [psk \(671 ページ\)](#)

plugnplay

現在のメッシュの PlugNPlay 機能を有効または無効にします。

構文

`plugnplay <enable/disable>`

`enable/disable` PlugNPlay を有効または無効にします。

コマンド モード

メッシュ設定

デフォルト

無効

用途

PlugNPlay 機能を使用すると、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。メッシュ対応の AP は、最初に電源オンにした段階で、有効な PlugNPlay がある範囲内にメッシュを検索します。メッシュが見つかったら、メッシュ PSK と設定を最も近いメッシュ AP から自動的にダウンロードします。

メッシュ操作を可能にするには、この AP が ([mesh-ap \(668 ページ\)](#) コマンドを使用して) メッシュ AP テーブルに追加されている必要があります。

使用例

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# plugnplay enable
default(15)(config-mesh)# end
```

関連コマンド

- [admin-mode \(666 ページ\)](#)
- [descr \(667 ページ\)](#)
- [mesh-profile \(669 ページ\)](#)

psk

メッシュ暗号化に使用する事前共有キーを設定します。

構文

```
psk key <key>
```

key メッシュ通信の保護に使用する暗号化キー。

コマンドモード

メッシュ設定

デフォルト

なし

用途

このコマンドを使用して、メッシュ ノード間の通信で使用する、WPA 事前共有暗号化キーを指定します。このキーは、ノードのみが使用するものであり、メッシュへの接続時にエンドユーザが提供するものではありません。

使用例

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# psk key MySharedKey
default(15)(config-mesh)# end
```

関連コマンド

- [admin-mode \(666 ページ\)](#)
- [mesh-profile \(669 ページ\)](#)
- [plugnplay \(670 ページ\)](#)

13 不正 AP 検出コマンド

本章に含まれるコマンドは、不正 AP の検出に関する設定と情報を表示するために使用されます。

- [rogue-ap acl \(674 ページ\)](#)
- [rogue-ap aging \(675 ページ\)](#)
- [rogue-ap assigned-aps \(676 ページ\)](#)
- [rogue-ap blocked \(677 ページ\)](#)
- [rogue-ap detection \(679 ページ\)](#)
- [rogue-ap mitigation \(681 ページ\)](#)
- [rogue-ap mitigation \(681 ページ\)](#)
- [rogue-ap mitigation-frames \(682 ページ\)](#)
- [rogue-ap operational-time \(683 ページ\)](#)
- [rogue-ap scanning-channels \(684 ページ\)](#)
- [rogue-ap scanning-time \(686 ページ\)](#)
- [show rogue-ap acl \(687 ページ\)](#)
- [show rogue-ap blocked \(688 ページ\)](#)
- [show rogue-ap globals \(689 ページ\)](#)
- [show rogue-ap-list \(690 ページ\)](#)

rogue-ap acl

アクセス ポイントの BSSID を、認証される BSSID として、WLAN で許可されるアクセス コントロール リスト (ACL) に追加します。

構文

```
rogue-ap acl <bssid>  
no rogue-ap acl <bssid>
```

bssid 許可される BSSID としてアクセス コントロール リストに追加するアクセス ポイントの BSSID (ff:ff:ff:ff:ff:ff の形式で指定)。

コマンドモード

グローバル設定

デフォルト

なし

用途

rogue-ap acl コマンドを使用して、許可されるアクセス ポイントとして ACL に追加する、特定の BSSID が関連付けられたアクセス ポイントを指定できます。コントローラが把握しているすべての ESS は、ACL に自動的に追加されます。

BSSID は、認可される BSSID として ACL にリストすることも、ブロックされる BSSID のリストに入れることもできません。BSSID を許可されるリストに追加したい場合に、その BSSID が現在ブロックされるリスト (拒否リスト) にある場合は、最初にブロックされるリストからこの BSSID を削除してから (**no rogue-ap blocked** コマンドを使用)、許可されるリストに BSSID を追加する必要があります。

許可される BSSID エントリを ACL から削除するには、**no** フォームを使用します。

使用例

以下のコマンドを指定すると、BSSID 00:0e:cd:cb:0f:bc が許可される BSSID として ACL に追加されます。

```
controller(config)# rogue-ap acl 00:0e:cd:cb:0f:bc  
controller(config)#
```

関連コマンド

- [rogue-ap blocked \(677 ページ\)](#)
- [rogue-ap mitigation \(681 ページ\)](#)
- [show rogue-ap acl \(687 ページ\)](#)

rogue-ap aging

未検出の不正 AP アラームがアクティブなままになる時間を設定します。

構文

`rogue-ap aging <aging-time>`

aging-time 検出されなくなった不明またはブロックされる BSSID のアラームがアクティブなままになる時間。60 ～ 86,400 秒の範囲で値を指定します。

コマンドモード

グローバル設定

デフォルト

デフォルトの不正 AP アラームの有効期間は 60 秒です。

用途

このコマンドにより、検出されなくなった不明またはブロックされる BSSID のアラームが有効のままになる時間を設定します。この時間が経過すると、検出されなくなった不正 AP はアラームリストから自動的に削除され、アラームはクリアされます。

使用例

以下のコマンドは、不正 AP アラームの有効期間を 300 秒に設定します。

```
controller(config)# rogue-ap aging 300
controller(config)#
```

関連コマンド

[*rogue-ap mitigation*](#) (681 ページ)

rogue-ap assigned-aps

不正 AP 緩和を実行する AP の数を設定します。

構文

```
rogue-ap assigned-aps <number_aps>
```

number_aps 不正 AP 緩和に参加する AP の数を指定します。有効な値は 1 ～ 20 AP です。

コマンド モード

グローバル設定

デフォルト

緩和を実行する AP のデフォルトの数は 3 です。

用途

このコマンドは、不正 AP 緩和の実行を試行する AP の最大数を設定します。

WLAN では、AP のサブセットのみが緩和を実行します。これによって、ネットワーク スループット パフォーマンスを維持しつつ、電波として送信される緩和フレーム数を削減できます。不正 AP に最も近い AP が緩和フレームを送信します。

使用例

以下のコマンドにより、緩和を実行する AP 数が 5 に設定されます。

```
controller(config)# rogue-ap assigned-aps 5  
controller(config)#
```

関連コマンド

[rogue-ap mitigation \(681 ページ\)](#)

rogue-ap blocked

WLAN で承認しないアクセス ポイントとして指定されるアクセス ポイントの BSSID を指定します。

構文

```
rogue-ap blocked <bssid>  
no rogue-ap blocked <bssid>
```

bssid ACL でブロックされるように指定するアクセス ポイントの BSSID です。つまり、このアクセス ポイントは WLAN で許可されません。16 進数の形式 (xx:xx:xx:xx:xx:xx) で指定する必要があります。

コマンドモード

グローバル設定

デフォルト

なし

用途

rogue-ap blocked コマンドを指定して、特定の BSSID が関連付けられているアクセス ポイントを許可されないアクセス ポイントとして ACL に追加できます。

不正 AP 緩和モードが "selected" (**rogue-ap mitigation selected** コマンドを使用) の場合には、このリストにある BSSID に接続する不正なステーションだけが緩和されます。

BSSID は、認可される BSSID として ACL にリストすることも、ブロックされる BSSID のリストに入れることもできません。BSSID をブロックされるリストに追加する場合で、この BSSID が現在許可リストにある場合には、最初に許可リストからこの BSSID を削除して (**no rogue-ap acl** コマンドを使用)、ブロックされるリストに BSSID を追加します。

緩和のオプションが有線のクライアントをブロックするためのものである場合 (コマンド **rogue-ap mitigation wiredRogue** を使用している場合) や、有線にあるクライアントの BSSID がここに追加される場合、これらのクライアントは有線でのみブロックされます。

no フォームを使用して、ブロックされるリストから BSSID エントリを削除します。

使用例

以下のコマンドを指定すると、BSSID 00:02:2d:61:0a:2c がブロックされる BSSID として ACL に追加されます。

```
controller(config)# rogue-ap blocked 00:02:2d:61:0a:2c
```

```
controller(config)#
```

関連コマンド

- [rogue-ap acl \(674 ページ\)](#)
- [show rogue-ap blocked \(688 ページ\)](#)

rogue-ap detection

不正な AP の検出を有効にします。

構文

```
rogue-ap detection
no rogue-ap detection
```

コマンド モード

グローバル設定

デフォルト

不正な AP の検出はデフォルトでは無効になっています。

用途

不正 AP 検出を有効にすると、アクセス ポイントがスキャンされ検出されます。検出されたアクセス ポイントは、BSSID によってアクセス ポイントを一覧表示するアクセス コントロール リスト (ACL) と比較されます。ACL に記載されているアクセス ポイントは、許可またはブロックと指定され、許可されるアクセス ポイントは WLAN における動作が許可されるアクセス ポイントになり、ブロックされるアクセス ポイントは、WLAN での使用が許可されないアクセス ポイントになります。

不正な AP の検出を無効にするには、**no** フォームを使用します。

使用例

以下のコマンドを指定すると、不正な AP の検出が有効になります。

```
controller(config)# rogue-ap detection
controller(config)#
```

関連コマンド

- [rogue-ap acl \(674 ページ\)](#)
- [rogue-ap blocked \(677 ページ\)](#)

rogue-ap min-rssi

緩和の最小 RSSI しきい値レベルを設定します。

構文

rogue-ap min-rssi <level>

level 最小不正値 (dBm)

コマンド モード

グローバル設定

デフォルト

RSSI レベルはデフォルトでは -100 です。

用途

このコマンドは、緩和するステーションの最小 RSSI (受信信号強度) レベルを設定します。この値 (dBm) は、不正である AP/ ステーションを決定します。AP の RSSI 値が min-rssi level 以上であれば、不正になります。

使用例

次のコマンドは、最小 RSSI レベルを -80 に設定します。

```
controller # configure terminal
controller(config)# rogue-ap min-rssi -80
controller(config)#
```

関連コマンド

rogue-ap mitigation

不正 AP 緩和のレベルを設定します。

構文

```
rogue-ap mitigation all
rogue-ap mitigation none
rogue-ap mitigation selected
rogue-ap mitigation wiredRogue
```

all	不正 AP 緩和を有効にし、不正 AP の ACL で許可されていない検出されたすべての BSSID をブロックします。
none	不正 AP 緩和を無効にします。
selected	ブロックされるリストに記載されている BSSID の不正 AP 緩和を有効にします。
wiredRogue	AP の有線側で検出されたクライアントを緩和します。

コマンドモード

グローバル設定

デフォルト

不正な AP の緩和はデフォルトでは無効になっています。

用途

不正な AP 緩和は、不正な AP にステーションが関連付けられるのを防止します。不正 AP 緩和を有効にすると、フォーティネット アクセス ポイント を使用するクライアントが不正な AP 経由でネットワークにアクセスするのをブロックできます。

rogue-ap mitigation コマンドを使用して、許可されるアクセス ポイントとして以前は記載されていなかったすべての BSSID、またはブロックされる BSSID としてリストされている BSSID、または、AP の有線側で検出された不正クライアントを対象として不正 AP 緩和を有効にします。

使用例

以下のコマンドは、ブロックされるリストの BSSID の不正 AP 緩和を有効にします。

```
controller(config)# rogue-ap mitigation selected
controller(config)#
```

関連コマンド

[rogue-ap blocked](#) (677 ページ)

rogue-ap mitigation-frames

チャンネルごと、緩和間隔ごとに送出される不正 AP 緩和フレーム数を設定します。

構文

`rogue-ap mitigation-frames <number_frames>`

number_frames チャンネルごとの緩和フレームの最大数を設定します。有効な範囲は 1 ～ 50 で、デフォルトでは 10 に設定されています。

コマンドモード

グローバル設定

デフォルト

チャンネルごとに 10 緩和フレームがデフォルトで設定されます。

用途

不正な AP 緩和は、不正な AP にステーションが関連付けられるのを防止します。このコマンドにより各緩和間隔で送信される緩和フレーム数が設定されます。この数は、各チャンネルの不正ステーションの数と一致する必要はありません。

使用例

以下のコマンドにより、チャンネルごとの緩和フレーム数が 25 に設定されます。

```
controller(config)# rogue-ap mitigation-frames 25
controller(config)#
```

関連コマンド

[rogue-ap detection](#) (679 ページ)

rogue-ap operational-time

ホーム チャンネルで AP が操作モードで費やす時間を設定します。

構文

rogue-ap operational-time <operational-time>

operational-time ホーム チャンネルの操作時間をミリ秒で設定します。有効な範囲は、100 ～ 5000 ミリ秒で、デフォルト設定は 400 ミリ秒です。

コマンドモード

グローバル設定

デフォルト

デフォルトの設定では、操作時間は 400 ミリ秒になっています。

用途

スキャンが有効になっている場合、このコマンドによって、ホーム チャンネルで (通常のワイヤレス サービスを実行する) 操作モードに費やす時間がミリ秒数で設定されます。このコマンドは、**rogue-ap scanning-time** コマンドと関連しています。**rogue-ap scanning channels** コマンドによって、スキャンされるチャンネルが決定されます。

不正 AP のスキャン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を費やし、ホーム チャンネルでの通常の AP WLAN 操作に一定の時間を費やします。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。

ホーム以外のチャンネルのスキャンは、専用のスキャン AP (Dot11Radio インターフェイス設定サブモードの **mode** コマンドで設定されます) と、関連付けられているステーションがない AP によって、実行されます。

使用例

以下のコマンドを使用すると、操作時間が 2500 ミリ秒に設定されます。

```
controller(config)# rogue-ap operational-time 2500
controller(config)#
```

関連コマンド

[rogue-ap mitigation](#) (681 ページ)

rogue-ap scanning-channels

スキャン モードでスキャンされるチャンネルを設定します。

構文

```
rogue-ap scanning-channel <channel-list>
```

channel-list 不正 AP のスキャンを行う対象となるチャンネル セットのリスト。
0 ～ 256 文字までのカンマ区切りリストを使用します。

コマンド モード

グローバル設定

デフォルト

米国におけるデフォルト チャンネルの完全セットは、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。

用途

スキャンが有効になっている場合、このコマンドにより不正 AP をスキャンするチャンネル セットが指定されます。

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。AP201 モデルは、単一のインターフェイスにあるすべてのチャンネルをスキャンし、AP208 インターフェイス 1 は、802.11bg バンドにあるすべてのチャンネルをスキャンし、インターフェイス 2 は、802.11a バンドにあるすべてのチャンネルをスキャンします。

スキャンは、専用のスキャン AP (Dot11Radio インターフェイス設定サブモード の **mode** コマンドで設定されます) と関連付けられているステーションがない AP により実行されません。

不正 AP スキャンが一定時間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 (**rogue-ap scanning-time** コマンドにより決定されます) 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 (**rogue-ap operational-time** コマンドにより決定されます) 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。

使用例

以下のコマンドでは、スキャンするチャンネルが 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)#
```

関連コマンド

- [mode](#) (615 ページ)
- [rogue-ap detection](#) (679 ページ)
- [rogue-ap mitigation](#) (681 ページ)
- [rogue-ap operational-time](#) (683 ページ)
- [rogue-ap scanning-time](#) (686 ページ)

rogue-ap scanning-time

操作チャネル以外の各チャネルをスキャンするために AP が費やす時間を設定します。

構文

rogue-ap scanning-time <*scanning-time*>

scanning-time スキャン時間をミリ秒単位で設定します。有効な範囲 は、100 ～ 500 ミリ秒で、デフォルト設定は 100 ミリ秒です。

コマンド モード

グローバル設定

デフォルト

デフォルト設定では、スキャン時間は 100 ミリ秒です。

用途

スキャンが有効になっている場合、このコマンドによりチャネルの各グローバル リストのスキャンに費やすミリ秒数が設定されます。このコマンドは、**rogue-ap operational-time** コマンドと関連しています。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。

不正 AP スキャン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。

ホーム以外のチャネルのスキャンは、専用のスキャン AP (Dot11Radio インターフェイス設定サブモードの **mode** コマンドで設定されます) と、関連付けられているステーションがない AP によって、実行されます。

使用例

以下のコマンドにより、スキャン時間が 200 ミリ秒に設定されます。

```
controller(config)# rogue-ap scanning-time 200
controller(config)#
```

関連コマンド

- [rogue-ap detection \(679 ページ\)](#)
- [rogue-ap mitigation \(681 ページ\)](#)
- [rogue-ap operational-time \(683 ページ\)](#)
- [rogue-ap scanning-channels \(684 ページ\)](#)

show rogue-ap acl

不正 AP の ACL を表示します。

構文

show rogue-ap acl

コマンド モード

EXEC

デフォルト

なし

用途

使用例

以下のコマンドを使用すると、WLAN での動作が許可されているアクセス ポイント (BSSID で指定) のリストが表示されます。

```
controller# show rogue-ap acl
```

```
BSSID
```

```
f4:3c:00:1f:f2:d3
```

```
00:0c:e6:cd:cd:cd
```

```
00:0c:e6:c2:d5:b1
```

```
Allowed APs(3)
```

関連コマンド

[rogue-ap acl](#) (674 ページ)

show rogue-ap blocked

ブロックされた BSSID のリストを表示します。

構文

`show rogue-ap blocked`

コマンド モード

EXEC

デフォルト

なし

用途

使用例

以下のコマンドは、(BSSID で指定した) ブロックされるアクセス ポイントのリストを表示します。

```
controller# show rogue-ap blocked
```

BSSID	Creation Time	Last Reported Time
00:0c:e6:20:c1:48	2005/08/01 20:35:35	-

Blocked APs(1 entry)

関連コマンド

[rogue-ap acl \(674 ページ\)](#)

show rogue-ap globals

現在の不正 AP パラメータ設定を表示します。

構文

`show rogue-ap globals`

コマンド モード

EXEC

デフォルト

なし

用途

使用例

以下のコマンドは、現在の不正 AP のパラメータ設定を表示します。

```
controller> show rogue-ap globals
```

Global Settings

```
Detection                               : off
Mitigation                             : none
Rogue AP Aging (seconds)               : 60
Number of Mitigating APs               : 3
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,
56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165
RSSI Threshold for Mitigation          : -100
controller>
```

関連コマンド

- [rogue-ap aging \(675 ページ\)](#)
- [rogue-ap detection \(679 ページ\)](#)
- [rogue-ap mitigation \(681 ページ\)](#)

show rogue-ap-list

すべての不正な AP のリストを表示します。

構文 `show rogue-ap-list`

コマンド
モード 特権 EXEC

デフォルト なし

用途

使用例 以下のコマンドは、BSSID で指定される不正アクセス ポイントのリストを表示します。

controller# `show rogue-ap-list`

Rogue_AP_MAC	Type	Channel	SSID			BSSID	
Meru_AP1_ID	Last_AP1		RSSI_AP1	Meru_AP2_ID	Last_AP2		RSSI_AP2
Meru_AP3_ID	Last_AP3		RSSI_AP1	Inactive_audits			
00:00:4c:1a:84:9c	STATION	11					
00:0c:e6:96:37:81	4		00d:00h:00m:00s	-77	2		
00d:00h:00m:00s	-82	0	00d:00h:00m:00s	0	0		
00:03:2a:00:3d:be	STATION	11					
00:0c:e6:96:37:81	2		00d:00h:00m:11s	-75	4		
00d:00h:00m:11s	-86	0	00d:00h:00m:00s	0	0		
00:03:2a:00:6a:0e	STATION	11					
00:0c:e6:ae:a5:9d	2		00d:00h:00m:02s	-74	4		
00d:00h:00m:02s	-83	0	00d:00h:00m:00s	0	0		

関連コマンド [rogue-ap acl \(674 ページ\)](#)

14 サービス品質コマンド

本章に含まれるコマンドは、QoS (サービス品質) を設定し、その関連情報を表示するために使用されます。

- [action](#) (693 ページ)
- [avgpacketrates](#) (694 ページ)
- [dscp](#) (695 ページ)
- [dstip](#) (696 ページ)
- [dstip-flow](#) (697 ページ)
- [dstip-match](#) (698 ページ)
- [dstmask](#) (699 ページ)
- [dstport](#) (700 ページ)
- [dstport-flow](#) (702 ページ)
- [dstport-match](#) (703 ページ)
- [firewall-filter-id](#) (704 ページ)
- [firewall-filter-id-flow](#) (706 ページ)
- [firewall-filter-id-match](#) (708 ページ)
- [netprotocol-flow](#) (710 ページ)
- [netprotocol-match](#) (711 ページ)
- [packet max-length](#) (712 ページ)
- [packet min-length](#) (713 ページ)
- [packet-min-length-flow](#) (714 ページ)
- [packet-min-length-match](#) (715 ページ)
- [peakrate](#) (716 ページ)
- [priority](#) (717 ページ)
- [qoscodec](#) (718 ページ)
- [qosrule](#) (722 ページ)
- [qosrule-logging-frequency](#) (725 ページ)

- [qosrulelogging \(726 ページ\)](#)
- [qosvars admission \(727 ページ\)](#)
- [qosvars bwscaling \(729 ページ\)](#)
- [qosvars cac-deauth \(730 ページ\)](#)
- [qosvars calls-per-ap \(731 ページ\)](#)
- [qosvars calls-per-bssid \(732 ページ\)](#)
- [qosvars calls-per-interference \(733 ページ\)](#)
- [qosvars drop-policy \(734 ページ\)](#)
- [qosvars enable \(735 ページ\)](#)
- [qosvars intercell-periodicity \(737 ページ\)](#)
- [qosvars load-balance-overflow \(738 ページ\)](#)
- [qosvars max-stations-per-radio \(739 ページ\)](#)
- [qosvars max-stations-per-bssid \(740 ページ\)](#)
- [qosvars sip-idle-timeout \(741 ページ\)](#)
- [qosvars station-assign-age \(742 ページ\)](#)
- [qosvars tcpttl \(743 ページ\)](#)
- [qosvars ttl \(744 ページ\)](#)
- [qosvars udpttl \(745 ページ\)](#)
- [rspecrate \(746 ページ\)](#)
- [rspecslack \(747 ページ\)](#)
- [srcip \(748 ページ\)](#)
- [srcmask \(749 ページ\)](#)
- [srcport \(750 ページ\)](#)
- [show phones \(752 ページ\)](#)
- [show phone-calls \(753 ページ\)](#)
- [show qoscodec \(754 ページ\)](#)
- [show qosflows \(757 ページ\)](#)
- [show qosrule \(759 ページ\)](#)
- [show qosstats \(764 ページ\)](#)
- [show qosvars \(765 ページ\)](#)
- [show statistics call-admission-control \(767 ページ\)](#)
- [tokenbucketrate \(769 ページ\)](#)
- [tokenbucketsize \(771 ページ\)](#)
- [trafficcontrol-enable \(772 ページ\)](#)

action

QoS ルールがパケットに実行するアクションを指定します。

構文

```
action capture
action drop
action forward
```

capture	パケットを捕捉し、指定したポートに送信します。これがデフォルト設定です。
drop	ルール基準と一致するパケットをドロップします。
forward	パケットを転送します。

コマンドモード

Qosrule 設定

デフォルト

QoS ルールが一致する場合、デフォルトではパケットを捕捉するよう設定されています。

用途

このコマンドは、QoS 基準と一致するパケットに実行するアクションを指定します。

- 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: QoS プロトコル設定での指定に従って、QoS プロトコル検出が、明示的なリソース要求に対してフローを提供します。これは H323/SIP ベースの静的 QoS ルールに推奨されるアクションです。
- Drop: フローがドロップされます。

使用例

次のコマンドは、パケットに対して実行するアクションをドロップ (Drop) に設定します。

```
controller(config-qosrule)# action drop
```

関連コマンド

- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

avgbucketrate

QoS ルールの平均パケット レートを指定します。

構文

`avgbucketrate <avgbucketrate>`

avgbucketrate 平均パケット レートは、毎秒 0 ～ 200 パケットの範囲で指定します。

コマンド モード

Qosrule 設定

デフォルト

デフォルト設定はゼロです。

用途

このコマンドは、フローに平均パケット レートを設定します。レートが 0 以外で ある場合、トラフィック仕様 (TSpec) トークン バケット レートも 0 以外である必要があり、優先度 を 0 以外の値に設定することはできません。

使用例

次のコマンドは、平均パケット レート フローを毎秒 100 パケットに設定します。

```
controller(config-qosrule)# avgbucketrate 100
```

関連コマンド

- [priority \(717 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)
- [tokenbucketrate \(769 ページ\)](#)

dscp

DiffServ コードポイント クラスを指定します。

構文

dscp class

class コードポイント クラスを指定します。クラスは RFCs 2474、2475、および 2597 として指定する必要があります。

コマンドモード

Qosrule 設定

デフォルト

cs0 (best effort)

用途

このコマンドは、フロー内のパケットに対して、ホップごとの転送の動作を指定します。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。

使用例

次のコマンドは、DSCP を無効にします。

```
controller(config-qosrule)# dscp disabled
```

関連コマンド

- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

dstip

QoS ルールの宛先 IP アドレスを指定します。

構文

dstip <destination-ip-address>

destination-ip-address 宛先 IP アドレスを指定します。*nnn.nnn.nnn.nnn* の形式で指定する必要があります。

コマンドモード

Qosrule 設定

デフォルト

なし

用途

このコマンドは、QoS ルールの宛先 IP アドレスを指定します。宛先 IP アドレスを宛先サブネットマスクと一緒に使用して、一致する QoS ルールの基準を指定します。

使用例

次のコマンドは、宛先 IP アドレスを設定します。

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
controller(config-qosrule)# dstip 192.14.0.0
```

関連コマンド

- [dstmask \(699 ページ\)](#)
- [dstport-match \(703 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

dstip-flow

この qosrule の宛先 IP フローを有効にします。

構文

```
dstip-flow on  
dstip-flow off
```

on	dstip フローをオンにします。
off	dstip フローをオフにします。

コマンドモード

Qosrule 設定

デフォルト

デフォルトは、オフです。

用途

このコマンドは、QoS ルールの宛先 IP フローを有効にします。

使用例

次のコマンドは、宛先 IP フローをオンに設定します。

```
default# configure terminal  
default(config)# qosrule 200 netprotocol 6 qosprotocol none  
controller(config-qosrule)# dstip 192.14.0.0  
controller(config-qosrule)# dstip-flow on
```

関連コマンド

- [dstip-match \(698 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

dstip-match

現在の qosrule の宛先 IP マッチングを有効にします。

構文

```
dstip-match on  
dstip-match off
```

on	dstip マッチングをオンにします。
off	dstip マッチングをオフにします

コマンドモード

Qosrule 設定

デフォルト

オフ

用途

このコマンドは、QoS ルールの宛先 IP フローを有効にします。

使用例

このコマンドは、宛先 IP マッチングをオンにします。

```
default# configure terminal  
default(config)# qosrule 200 netprotocol 6 qosprotocol none  
controller(config-qosrule)# dstip 192.14.0.0  
controller(config-qosrule)# dstip-match on
```

関連コマンド

- [show qosrule \(759 ページ\)](#)
- [dstip-flow \(697 ページ\)](#)

dstmask

QoS ルールの宛先 IP アドレス ネットマスクを指定します。

構文

`dstmask <destination-netmask>`

destination-netmask 宛先 IP アドレスのサブネット マスクを指定します。
nnn.nnn.nnn.nnn の形式で指定する必要があります。

コマンド モード

Qosrule 設定

デフォルト

なし

用途

このコマンドは、QoS ルールの宛先 IP アドレスのサブネット マスクを指定します。宛先 IP アドレスを宛先サブネット マスクと一緒に使用して、一致する QoS ルールの基準を指定します。

使用例

次のコマンドは、宛先ネットマスクを設定します。

```
controller(config-qosrule)# dstmsk 255.0.0.0
```

関連コマンド

- [dstip \(696 ページ\)](#)
- [dstport-match \(703 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

dstport

QoS ルールの宛先 TCP または UDP ポートを指定します。

構文

dstport <destination-port>

destination-port 宛先 TCP または UDP ポートを指定します。0 ～ 65535 の範囲で指定します。

コマンドモード

Qosrule 設定

デフォルト

デフォルト ポートは 0 (すべてのポートを指定) です。

用途

このコマンドは、QoS ルールのマッチング基準として使用される宛先 TCP または UDP ポートを指定します (0 はすべてのポートを指定)。

コントローラは、通過するトラフィックを監視します。SIP または H.323 サービス用に予約されたポートでステーションからサーバに送信されるパケットを見つけると、そのシーケンスの後続の通信を追跡し、VoIP 通話に適したレベルのサービスを VoIP 通話に提供します。

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)
- H.323 サービス用の 1720 (TCP)
- Vocera サーバ用の 5200

これらは、それぞれのサービスの標準ポート番号です。VoIP デバイスがこれらのポートを使用してサーバと通信しているのであれば、システムで VoIP QoS ルールを設定する必要はありません。

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、コントローラの QoS ルールをシステムが使用しているポートに合わせて変更する必要があります。

使用例

次のコマンドは、宛先ポートを 1200 に設定します。

```
controller(config-qosrule)# dstport 1200
```

関連コマンド

- [dstport-match](#) (703 ページ)
- [dstport-flow](#) (702 ページ)
- [dstmask](#) (699 ページ)
- [qosrule](#) (722 ページ)
- [show qosrule](#) (759 ページ)

dstport-flow

QoS ルールの宛先ポート フローを有効にします。

構文

```
dstport-flow on  
dstport-flow off
```

on dstport フローをオンにします。

off dstport フローをオフにします。

コマンド モード

Qosrule 設定

デフォルト

デフォルトのポート フローはオフです。

用途

このコマンドは、QoS ルールの宛先ポート フローを有効にします。プロトコル番号に設定した値に一致させる場合は、このコマンドを使用します。トラフィック コントロールがオンの場合にのみ動作に相違が生じます。

使用例

次のコマンドは、QoS ルール 200 の宛先ポートを 1200 に設定します。

```
default# configure terminal  
default(config)# qosrule 200 netprotocol 6 qosprotocol none  
controller(config-qosrule)# dstport 1200  
controller(config-qosrule)# dstport-flow on
```

関連コマンド

- [dstport \(700 ページ\)](#)
- [dstport-match \(703 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

dstport-match

現在の QoS ルールの宛先 IP マッチングを有効にします。

構文

```
dstport-match on  
dstport-match off
```

on dstport-match をオンにします。

off dstport-match をオフにします。

コマンド モード

Qosrule 設定

デフォルト

デフォルトのポート フローはオフです。

用途

このコマンドは、QoS ルールの宛先ポート フローを有効にします。プロトコル番号に設定した値に一致させる場合は、このコマンドを使用します。

使用例

次のコマンドは、QoS ルール 200 の宛先ポートを 1200 に設定します。

```
default# configure terminal  
default(config)# qosrule 200 netprotocol 6 qosprotocol none  
controller(config-qosrule)# dstport 1200  
controller(config-qosrule)# dstport-match on
```

関連コマンド

- [dstport \(700 ページ\)](#)
- [dstport-flow \(702 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

firewall-filter-id

ユーザまたは ESS ごとに割り当てられたフィルタ ファイアウォール ID を QOS ルールに割り当てます

構文

`firewall-filter-id <filter id>`

filter id このセキュリティ プロファイルに割り当てられた filter-id を指定する英数字の値です。この値は、ファイアウォール機能が **configured** に設定された場合にコントローラで利用できるファイアウォール ポリシーを定義します。

コマンドモード

セキュリティ プロファイル設定および qosrule 設定

デフォルト

なし

用途

この値は、**ファイアウォール機能**が **configured** に設定された場合にのみコントローラで使用するファイアウォール ポリシーを定義します。ファイアウォール機能がセキュリティ プロファイルのファイアウォール フィルタ ID を使用して設定されている場合は、同じファイアウォール フィルタ ID を Qosrule に構成することで有効になります。

使用例

次のコマンドは、ファイアウォール フィルタ ID を 10 に設定します。

```
default(config)# security-profile abc
default(config-security)# firewall-capability configured
default(config-security)# firewall-filter-id 10
default(config-security)# exit
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
default(config-qosrule)# firewall-filter-id 10
default(config-qosrule)# firewall-filter-id-flow on
default(config-qosrule)# firewall-filter-id-match on
default(config-qosrule)# exit
```

関連コマンド

- [firewall-capability \(427 ページ\)](#)

- [firewall-filter-id \(704 ページ\)](#)
- [firewall-filter-id-flow \(706 ページ\)](#)
- [firewall-filter-id-match \(708 ページ\)](#)
- [security-logging \(468 ページ\)](#)
- [show security-profile \(485 ページ\)](#)
- [show qosrule \(759 ページ\)](#)
- [qosrulelogging \(726 ページ\)](#)
- [qosrule-logging-frequency \(725 ページ\)](#)

firewall-filter-id-flow

フィルタ ファイアウォール ID フローを QOS ルールに割り当てます。

構文

```
firewall-filter-id-flow on
firewall-filter-id-flow off
```

on	ファイアウォール フィルタ ID フローをオンにします。
off	ファイアウォール フィルタ ID フローをオフにします。

コマンドモード

セキュリティ プロファイル設定および qosrule 設定

デフォルト

ファイアウォール フィルタ ID フローのデフォルトはオフです。

用途

この値は、**ファイアウォール機能**が **configured** に設定された場合にのみコントローラで使用するファイアウォール ポリシーを定義します。ファイアウォール機能がセキュリティ プロファイルのファイアウォール フィルタ ID を使用して設定されている場合は、同じファイアウォール フィルタ ID を Qosrule に構成することで有効になります。

使用例

次のコマンドは、ファイアウォール フィルタ ID を 10 に設定します。

```
default(config)# security-profile abc
default(config-security)# firewall-capability configured
default(config-security)# firewall-filter-id 10
default(config-security)# exit
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
default(config-qosrule)# firewall-filter-id 10
default(config-qosrule)# firewall-filter-id-match on
default(config-qosrule)# exit
```

関連コマンド

- [firewall-capability \(427 ページ\)](#)
- [firewall-filter-id \(704 ページ\)](#)
- [firewall-filter-id-flow \(706 ページ\)](#)

- [firewall-filter-id-match](#) (708 ページ)
- [security-logging](#) (468 ページ)
- [show security-profile](#) (485 ページ)
- [show qosrule](#) (759 ページ)
- [qosrulelogging](#) (726 ページ)
- [qosrule-logging-frequency](#) (725 ページ)

firewall-filter-id-match

フィルタ ファイアウォール ID フローを QOS ルールに割り当てます。

構文

```
firewall-filter-id-match on  
firewall-filter-id-match off
```

on	ファイアウォール フィルタ ID マッチングをオンにします。
off	ファイアウォール フィルタ ID マッチングをオフにします。

コマンドモード

セキュリティ プロファイル設定および qosrule 設定

デフォルト

ファイアウォール フィルタ ID マッチングはデフォルトでオフです。

用途

この値は、**ファイアウォール機能**が **configured** に設定された場合にのみコントローラで使用するファイアウォール ポリシーを定義します。ファイアウォール機能がセキュリティ プロファイルのファイアウォール フィルタ ID を使用して設定されている場合は、同じファイアウォール フィルタ ID を Qosrule に構成することで有効になります。

使用例

次のコマンドは、ファイアウォール フィルタ ID を 10 に設定します。

```
default(config)# security-profile abc  
default(config-security)# firewall-capability configured  
default(config-security)# firewall-filter-id 10  
default(config-security)# exit  
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
default(config-qosrule)# firewall-filter-id 10  
default(config-qosrule)# firewall-filter-id-match on  
default(config-qosrule)# exit
```

関連コマンド

- [firewall-capability \(427 ページ\)](#)
- [firewall-filter-id \(704 ページ\)](#)
- [firewall-filter-id-flow \(706 ページ\)](#)

- [firewall-filter-id-match](#) (708 ページ)
- [security-logging](#) (468 ページ)
- [show security-profile](#) (485 ページ)
- [show qosrule](#) (759 ページ)
- [qosrulelogging](#) (726 ページ)
- [qosrule-logging-frequency](#) (725 ページ)

netprotocol-flow

QOS ルールの netprotocol フローを有効にします。

構文

```
netprotocol-flow on  
netprotocol-flow off
```

コマンド モード

QOS ルール設定モード

デフォルト

デフォルトはオフです。

用途

このコマンドは、QOS ルールの netprotocol フローを有効にします。

使用例

次のコマンドは、QoS ルール 3 の netprotocol フローを有効にします。

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# netprotocol-flow on  
controller(config-qosrule)# exit
```

関連コマンド

- [show qosrule \(759 ページ\)](#)
- [netprotocol-match \(711 ページ\)](#)

netprotocol-match

QoS ルール netprotocol マッチングを設定します。

構文

```
netprotocol-match on  
netprotocol-match off
```

コマンド モード

QOS ルール設定モード

デフォルト

netprotocol マッチングのデフォルトはオフです。

用途

このコマンドは、QOS ルールの netprotocol フローを有効にします。

使用例

次のコマンドは、QoS ルール 3 の netprotocol フローを有効にします。

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# netprotocol-match on  
controller(config-qosrule)# exit
```

関連コマンド

- [show qosrule \(759 ページ\)](#)
- [netprotocol-flow \(710 ページ\)](#)

packet max-length

QoS ルールの最大パケット長を設定します。

構文

`packet Max-length <number>`

number 0 ～ 1500 の数値

コマンド モード

QoS ルール設定モード

デフォルト

デフォルトは 0 (ゼロ) です。

用途

このコマンドは、QoS ルールの最大パケット長を設定します。

使用例

次のコマンドは、QoS ルール 3 の最大パケット長を 80 に設定します。

```
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
controller(config-qosrule)# packet max-length 80
```

関連コマンド

[show qosrule \(759 ページ\)](#)

packet min-length

QoS ルールの最小パケット長を設定します。

構文

`packet min-length <number>`

number 0 ～ 1500 の数値

コマンド モード

QoS ルール設定モード

デフォルト

デフォルトは 0 (ゼロ) です。

用途

このコマンドは、QoS ルールの最小パケット長を設定します。

使用例

次のコマンドは、QoS ルール 3 の最小パケット長を 80 に設定します。

```
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
controller(config-qosrule)# packet-min-length 100
controller(config-qosrule)# packet-min-length-flow on
controller(config-qosrule)# packet-min-length-match on
controller(config-qosrule)# end
```

関連コマンド

[show qosrule \(759 ページ\)](#)

packet-min-length-flow

QoS ルールの最小パケット長を設定します。

構文

`packet min-length <number>`

number 0 ～ 1500 の数値

コマンド モード

QoS ルール設定モード

デフォルト

デフォルトは 0 (ゼロ) です。

用途

このコマンドは、QoS ルールの最小パケット長を設定します。

使用例

次のコマンドは、QoS ルール 3 の最小パケット長を 80 に設定します。

```
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
controller(config-qosrule)# packet-min-length 100
controller(config-qosrule)# packet-min-length-flow on
controller(config-qosrule)# end
```

関連コマンド

[*show qosrule*](#) (759 ページ)

packet-min-length-match

QoS ルールの最小パケット長マッチングを有効にします。

構文

```
packet-min-length-match on  
packet-min-length-match off
```

コマンド モード

QoS ルール設定モード

デフォルト

パケット最小長マッチングのデフォルトはオフです。

用途

このコマンドは、QoS ルール マッチングの最小パケット長を有効にします。

使用例

次のコマンドは、QoS ルール 3 の最小パケット長マッチングを可能にします。

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# packet-min-length 100  
controller(config-qosrule)# packet-min-length-match on  
controller(config-qosrule)# end
```

関連コマンド

[show qosrule \(759 ページ\)](#)

peakrate

QoS コーデック ルールの Tspec ピーク レートを指定します。

構文

`peakrate <rate>`

rate トラフィック ピーク レート。有効な値の範囲は、0 ～ 1,000,000 バイト / 秒です。

コマンド モード

QoS コーデック 設定

デフォルト

デフォルトのトラフィック ピーク レートは 0 です。

用途

このコマンドは、QoS コーデック ルールの Tspec ピーク レートを指定します。

使用例

次のコマンドは、Tspec ピーク レートを 1000000 に設定します。

```
controller(config-qoscodec)# peakrate 1000000
```

関連コマンド

[show qoscodec \(754 ページ\)](#)

priority

QoS ルールのキューの優先度 レベルを指定します。

構文

priority <priority>

priority

ベストエフォートの優先度 キューを決定する数 (0 ～ 8) を指定します。デフォルトはゼロです。最高の優先度は 8 です。

コマンドモード

Qosrule 設定

デフォルト

デフォルトの優先度 レベルはゼロです。

用途

このコマンドは、QoS ルールの優先度 レベルを指定します。QoS には、予約されたトラフィックが適用され、AP パケット伝送の総帯域幅の最初の部分が割り当てられ、その次に各優先度 レベル (8 から 1)、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。

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。

使用例

次のコマンドは、優先度 レベルを 5 に設定します。

```
controller(config-qosrule)# priority 5
```

関連コマンド

- [avgpacketrates \(694 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)
- [tokenbucketrate \(769 ページ\)](#)

qoscodec

QoS コーデック エントリを指定し、QoS コーデック 設定モードに入ります。

構文

```
qoscodec id codec <codec> qosprotocol <qosproto> tokenbucketrate  
<tokenbucketrate> maxdatagramsize <maxdatagramsize> minpolicedunit  
<minpolicedunit> samplerate <samplerate>  
no qoscodec id
```


<i>id</i>	QoS コーデック ルールの固有の数値 ID。有効な値の範囲 は 0 ～ 6,000 です。
codec <i>codec</i>	<p><i>codec</i> の有効なエントリは以下のとおりです。</p> <p>1016 - 1016 音声：ペイロード タイプ 1、ビット レート 16 Kbps</p> <p>default - 未知のコーデックまたはコーデック 置換テーブルにエントリがないコーデック用のデフォルトの TSpec/RSpec を含む</p> <p>dv14 - DV14 音声：ペイロード タイプ 5、ビット レート 32 Kkbps</p> <p>dv14.2 - DV14.2 音声：ペイロード タイプ 6、ビット レート 64 Kbps</p> <p>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</p> <p>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</p> <p>g721 - G721 音声：ペイロード タイプ 2、ビット レート 32 Kbps</p> <p>g722 - 音声：ペイロード タイプ 9、ビット レート 64 Kbps、7 KHz</p> <p>g7221 - G7221 音声：ペイロード タイプ *、ビット レート 24 Kbps、16 KHz</p> <p>g7221-32 - G7221 音声：ペイロード タイプ *、ビット レート 32 Kbps、16 KHz</p> <p>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</p> <p>g728 - G728 音声：ペイロード タイプ 15、ビット レート 16 Kbps</p> <p>g729 - G729 音声：ペイロード タイプ 16、ビット レート 8 Kbps</p> <p>g7red - 独自 MSN コーデック音声：ペイロード タイプ *</p> <p>gsm - GSM 音声：ペイロード タイプ 3、ビット レート 13 Kbps</p> <p>h261 - H.261 ビデオ</p> <p>h263 - H.263 ビデオ</p> <p>lpc - IPC 音声：ペイロード タイプ 7、ビット レート 2.4Kkbps</p> <p>mpa - MPA 音声：ペイロード タイプ 14、ビット レート 32kbps</p> <p>siren - 独自 MSN 音声： ペイロード タイプ *、ビット レート 16 Kbps、16 KHz</p>

qosprotocol <i>qosprotocol</i>	次の QoS プロトコルを指定します。 h323 - H.323 (Microsoft NetMeeting で主に使用) none - その他すべてのプロトコル sip - SIP (Session Initiation Protocol)
tokenbucketrate <i>tokenbucketrate</i>	トークン バケット レート。有効な値の範囲は、0 ～ 1,000,000 バイト / 秒です。
maxdatagramsize <i>maxdatagramsize</i>	最大パケット サイズ。有効な値の範囲は 0 ～ 1,500 バイトです。
minpolicedunit <i>minpolicedunit</i>	規制単位の最小数。有効な値の範囲は 0 ～ 1,500 バイトです。有効な値の範囲は 0 ～ 1,500 バイトです。
samplerate <i>samplerate</i>	パケット レート。有効な値の範囲は 0 ～ 200 パケット / 秒です。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、QoS コーデック エントリを作成し、QoS コーデック設定モードに入ります。22 のコーデックが出荷時に提供され、*id* 番号を引数として使用してこのコマンドを使用することで、それぞれを編集できます。**no** フォームを使用すると、QoS コーデック テーブルからエントリを削除できます。提供されるコーデック エントリ は以下のとおりで、**show qoscodec** で参照できます。

ID	Codec	Qos Protocol
22	h263	sip
21	h261	sip
20	siren	sip
19	g729	sip
18	g7221-32	sip
17	g7221	sip
16	g711a	sip
15	g723.1	sip
14	gsm	sip
13	g711u	sip

```

12    default    sip
11    h263      h323
10    h261      h323
9     siren     h323
8     g729      h323
7     g7221-32  h323
6     g7221     h323
5     g711a     h323
4     g723.1    h323
3     gsm       h323
2     g711u     h323
1     default   h323
      QoS Codec Rules(22)

```

使用例

次のコマンドは、QoS コーデック ルール 4 を作成します。このルールでは、デフォルトの Codec、非 QoS プロトコル、トークン バケット レート 3333 バイト / 秒、最大データグラム サイズ 4 バイト、最小規制単位 45 バイト、サンプル レート 34 パケット / 秒を指定します。

```

controller(config)# qoscodec 4 codec default qosprotocol none
tokenbucketrate 3333 maxdatagramsize 4 minpolicedunit 45 samplerate 34
controller(config-qoscodec)#

```

関連コマンド

- [tokenbucketrate \(769 ページ\)](#)
- [show qoscodec \(754 ページ\)](#)

qosrule

QoS ルールを作成し、qosrule 設定モードに入ります。

構文

```
qosrule <id> netprotocol 6 qosprotocol h323
qosrule <id> netprotocol 6 qosprotocol none
qosrule <id> netprotocol 6 qosprotocol sip
qosrule <id> netprotocol 6 qosprotocol sccp
qosrule <id> netprotocol 6 qosprotocol <other>
qosrule <id> netprotocol 17 qosprotocol h323
qosrule <id> netprotocol 17 qosprotocol none
qosrule <id> netprotocol 17 qosprotocol sip
qosrule <id> netprotocol 17 qosprotocol sccp
qosrule <id> netprotocol 17 qosprotocol <other>
qosrule <id> netprotocol <other> qosprotocol h323
qosrule <id> netprotocol <other> qosprotocol none
qosrule <id> netprotocol <other> qosprotocol sip
qosrule <id> netprotocol <other> qosprotocol sccp
qosrule <id> netprotocol <other> qosprotocol <other>
no qosrule id
```

id

QoS ルールの ID を指定します。ID は固有の数値である必要があります。

netprotocol {6 | 17 | other}

QoS ルールのフロー プロトコルを指定します。プロトコルは、**6** (TCP)、**17** (UDP)、または *other* である必要があります。*other* は、Spectralink フォンで使用する SVP プロトコルの 119 などの任意の有効なプロトコル番号です。[全リストは、<http://www.iana.org/assignments/protocol-numbers> に記載されています。]

qosprotocol {h323 | none | sip | sccp | other}

ルールの QoS プロトコルを指定します。一般的に、ほとんどの環境で **none** が適当な設定です。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。

SIP

H.323

SCCP

other

none

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、QoS ルールを作成し、Qosrule 設定モードに入ります。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。ID、ネットワークと QoS プロトコルのパラメータ、およびポートなどのその他のパラメータを指定すると、平均パケット レートが自動的にルールに設定されます。このコマンドの **no** フォームを使用すると、QoS ルールを削除できます。

QoS ルールのその他のパラメータを修正する必要がある場合は、Qosrule モードに含まれるコマンドを使用して、それらの値を調整します。

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 または 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、次に各優先度 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。優先度に基づく QoS には、ルールで **priority** パラメータを使用して 8 レベルの優先度のいずれかを指定できます。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。

使用例

次のコマンドは、ネットワークおよび QoS プロトコルとしてそれぞれ UDP と SIP を使用して、ルール 3 を作成します。

```
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
```

次のコマンドで、設定した QoS ルールを表示します。

```
controller# show qosrule
```

ID	Dst IP	Dst Mask	DPort	Src IP	Src Mask
SPort	Prot	Firewall	Filter	Qos	Action
				Drop	

```

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      other forward head
8      0.0.0.0      0.0.0.0      0      0.0.0.0      0.0.0.0
5200 17      other forward head

```

QoS Rules(8)

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 トラフィックに優先度を指定します。次の 2 つの QoS ルールは、UDP 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。

関連コマンド

- [action \(693 ページ\)](#)
- [avgpacketrates \(694 ページ\)](#)
- [dstip \(696 ページ\)](#)
- [dstmask \(699 ページ\)](#)
- [dstport-match \(703 ページ\)](#)
- [priority \(717 ページ\)](#)
- [srcip \(748 ページ\)](#)
- [srcmask \(749 ページ\)](#)
- [srcport \(750 ページ\)](#)
- [show qosrule \(759 ページ\)](#)
- [tokenbucketrate \(769 ページ\)](#)
- [trafficcontrol-enable \(772 ページ\)](#)

qosrule-logging-frequency

ルールに関するログが更新される間隔を定義します。

構文

qosrule-logging-frequency <frequency>

frequency 間隔は 30 ～ 60 秒で、デフォルトの設定は 60 です。

コマンド モード

QoS プロファイル設定

デフォルト

頻度は 60 秒に設定されます。

用途

qosrule-logging-frequency コマンドは、このルールに関するログが更新される間隔を定義します。

使用例

次のコマンドは、ユーザごとのファイアウォール QoS ルールのこのパラメータの設定を表示します。

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
default(config-qosrule)# dstport 80
default(config-qosrule)# action drop
default(config-qosrule)# firewall-filter-id 1
default(config-qosrule)# qosrule-logging on
default(config-qosrule)# qosrule-logging-frequency 30
default(config-qosrule)# exit
default(config)# exit
default# sh qosrule
```

関連コマンド

[qosrulelogging \(726 ページ\)](#)

qosrulelogging

QoS ルールのログ (記録) をオンまたはオフに設定します。

構文

```
qosrulelogging on
qosrulelogging off
```

コマンドモード

QoS プロファイル設定

デフォルト

QoS ルールのログはオフになっています。

用途

QoS ルール syslog ログをオンまたはオフに設定します。オンになっていると、qosrule に影響するイベントが記録されます。

使用例

次のコマンドは、default というコントローラの QoS ルールのログを有効にします。

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
default(config-qosrule)# qosrulelogging on
```

関連コマンド

- [qosrule-logging-frequency \(725 ページ\)](#)

qosvars admission

QoS コール アドミッション ポリシーを指定します。

構文

```
qosvars admission admitall  
qosvars admission pending  
qosvars admission reject
```

admitall	すべての QoS フローを QoS トラフィック クラスで許可するよう指定します。予約された帯域幅の合計が利用可能な帯域幅を超えると、QoS トラフィック クラス全体の結果が悪化します。
pending	予約できる帯域幅がない場合に新しい QoS フローをベスト エフォートのトラフィック クラスに移動するよう指定します。他の QoS フローから十分な帯域幅が解放されると、ベストエフォートのトラフィック クラスに置かれたフローは、QoS トラフィック クラスにアップグレードされます。
reject	予約できる帯域幅がない場合にフローそのものではなくリソース要求を拒否するよう指示します。QoS フローが永久にベストエフォートのトラフィック クラスに移動されます。追加の帯域幅が後で利用可能になっても、これらの QoS フローは QoS トラフィック クラスに移動されません。

コマンドモード

グローバル設定

デフォルト

アドミッション コントロールはデフォルトで **pending** に設定されます。

用途

帯域幅の予約は SIP コール シグナル (SDP 本体で指定されているコーデック / ポート) に基づいて実行され、コールを受け取る AP で利用可能な帯域幅の大きさと、近接する AP で予約されたその他のアクティブな QoS フローが考慮されます。データ速度や各クライアントの距離によって、サポートするコール数が異なるため、コールにおけるクライアントの実データ転送速度 (1/2/5.5/11 Mbps) を考慮してその都度計算されます。

選択するキーワード (**admitall**、**pending**、または **reject**) で、その時点で利用できないワイヤレス リソースを要求する QoS フロー (たとえば、新しく確立した音声コール) に対する動作を指定します。

使用例

次のコマンドは、アドミッション コントロール ポリシーを変更して、帯域幅を利用できない場合にリソース要求を拒否するようにします。

```
controller(config)# qosvars admission reject
```

関連コマンド

[show qosvars \(765 ページ\)](#)

qosvars bwscaling

QoS フローの帯域幅スケールを指定します。

構文

qosvars bwscaling <value>

value スケールのパーセントを表す、1 ～ 100 までの値を指定します。

コマンド モード

グローバル設定

デフォルト

デフォルトの帯域幅スケールは 100% に設定されます。

用途

このコマンドは、帯域幅のスケール方法を指定します。値を 100% より低くすると、予約できるリソースの大きさが小さくなり、最大負荷の環境でのベストエフォート トラフィックにリソースを使用できるようになります。

使用例

次のコマンドは、帯域幅スケールを 40% に設定します。

```
controller(config)# qosvars bwscaling 40
```

関連コマンド

[show qosvars \(765 ページ\)](#)

qosvars cac-deauth

オプションの 802.11 認証解除を設定します。

構文

```
qosvars cac-deauth on  
qosvars cac-deauth off
```

コマンド モード

グローバル設定

デフォルト

このコマンドのデフォルト設定は **off** です。

用途

このコマンドは、コールの開始側が利用可能な CAC (Call Admission Control) リソースを超過した場合のシステムの動作を制御します。**on** に設定すると、システムは 802.11 認証解除フレームを送信し、クライアントを代替 BSS にプッシュします。**off** (デフォルト設定) に設定すると、システムは変更した INVITE メッセージを SIP サーバに送信します。CAC が有効になっている場合、AP や BSSID に設定したコール レベルしきい値に近づくと、管理者は上限に達した場合に発生するアクションとして、次のいずれかのアクションを設定できます。

- 一般的な SIP サーバの場合に、486_BusyHere メッセージを送信してコールを拒否する。
- 一定の必要な状況では、変更された INVITE メッセージを SIP サーバに送信する。
- それ以外の必要な状況では、変更した INVITE メッセージまたは 486_BusyHere メッセージを送信してコールを拒否する。これらのメッセージには、X-CallAdmission SIP 拡張ヘッダが含まれる。

使用例

次のコマンドは、CAC De-authentication 機能を有効にします。

```
controller(config)# qosvars cac-deauth on
```

関連コマンド

[show qosvars \(765 ページ\)](#)

qosvars calls-per-ap

AP あたりのコールの最大数を設定します。

構文

```
qosvars calls-per-ap <max_calls>
```

max_calls AP の最大同時コール数を指定します。有効な値は 0 ～ 256 です。デフォルトでは 0 が設定され、コールは許可されません。

コマンドモード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 0 です。

用途

このコマンドは、AP あたりの最大コール数のしきい値を設定します。このコマンドによって Call Admission Control (CAC) 機能が実装され、AP あたりの許可されるコールのしきい値を設定することで一定の音声の品質が保証されます。AP が設定したしきい値に近づくと、メディア ストリームを効率的に処理するのに十分な帯域幅を利用できるようになるまで、CAC は新しい SIP 接続を拒否します。

AP のコール制限を超えると、コールの数が指定されたしきい値より少なくなるまで、新しいすべてのコールが 486_BusyHere 応答を受け取ることになります。ある AP から別の AP へのハンドオフで、2 つ目の AP に利用可能なリソースがないと、必要なリソースを利用できるようになるまで、そのコールが保留中 / ベストエフォートとして分類されます。

使用例

次のコマンドは、AP あたりの最大コール数を 12 に設定します。

```
controller(config)# qosvars calls-per-ap 12
```

関連コマンド

- [qosvars cac-deauth \(730 ページ\)](#)
- [qosvars calls-per-bssid \(732 ページ\)](#)
- [show qosvars \(765 ページ\)](#)
- [show statistics call-admission-control \(767 ページ\)](#)

qosvars calls-per-bssid

BSSID あたりの最大コール数を設定します。

構文

qosvars calls-per-bssid <*max_calls*>

max_calls BSSID の最大同時コール数を指定します。指定できるコールの範囲は 0 ～ 1023 で、デフォルトでは 0 が設定され、すべてのコールが許可されます。

コマンドモード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 0 です。

用途

このコマンドで default (0) 以外の引数を指定すると、BSS あたりの最大コール数のしきい値が設定されます。このコマンドによって Call Admission Control (CAC) 機能が実装され、BSS あたりの許可されるコールのしきい値を設定することで一定の音声の品質が保証されます。BSS が設定したしきい値に近づくと、メディア ストリームを効率的に処理するのに十分な帯域幅を利用できるようになるまで、CAC は新しい SIP 接続を拒否します。

該当の BSS の通話制限を超過すると、指定されたしきい値を通話数が下回るまで新しい通話は、486_BusyHere 応答 (通話中の応答) を受け取ります。デフォルトでは *max_calls* が 0 に設定され、BSSID の制限がなくなり、AP あたりの制限が適用されることとなります。CAC の場合は、**qosvars calls-per-ap** と **qosvars calls-per-bssid** の両方が評価されます。

使用例

次のコマンドは、最大コール数を 14 に設定します。

```
controller(config)# qosvars calls-per-bssid 14
```

関連コマンド

- [qosvars cac-deauth](#) (730 ページ)
- [qosvars calls-per-ap](#) (731 ページ)
- [show qosvars](#) (765 ページ)
- [show statistics call-admission-control](#) (767 ページ)

qosvars calls-per-interference

干渉領域あたりの最大コール数を設定します。

構文

```
qosvars calls-per-interference <max_calls>
```

max_calls	干渉領域あたりの最大同時コール数を指定します。有効な値は 0 ～ 256 で、デフォルトでは 0 に設定されます。
-----------	---

コマンドモード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 0 です。

用途

このコマンドは、その領域を共有するアクセス ポイントの数に関係なく、干渉領域における最大コール数を設定します。どのような地理的な場所であっても、ワイヤレスの機能は決まっています。1つのアクセス ポイントがその領域に存在する場合は、そのアクセス ポイントがワイヤレス能力全体を利用することになり、複数のアクセス ポイントがその領域に存在する場合は、それらの AP が固定のワイヤレス能力を共有することになりますこの機能は、ある領域内、さらに、その領域を共有する AP の数に基いてコール数に上限を設定することで、固定数のコールが AP に分散されるようにします。

使用例

次のコマンドは、干渉領域あたりの最大コール数を 75 に設定します。

```
controller(config)# qosvars calls-per-interference 75
```

関連コマンド

- [qosvars cac-deauth \(730 ページ\)](#)
- [qosvars calls-per-bssid \(732 ページ\)](#)
- [show qosvars \(765 ページ\)](#)
- [show statistics call-admission-control \(767 ページ\)](#)

qosvars drop-policy

QoS グローバル ドロップ ポリシーを指定します。

構文

```
qosvars drop-policy head
qosvars drop-policy tail
```

head	キューの最大長に達した後に新しいパケットが到着した場合に、そのパケットをキューに入れることを許可し、キューの古い情報を新しい情報に置き換えることを許可するよう指定します。音声アプリケーションのような、一定速度のリアルタイム フローを使用するアプリケーションには、このオプションを選択します。一般的に、このようなアプリケーションでは、パケットの損失よりも遅延を最小化することの方が重要です。
tail	キューの最大長に達した後に新しいパケットが到着した場合に、そのパケットをドロップするよう指定します。フロー制御が組み込まれているアプリケーションを使用する場合は、このオプションを選択します。

コマンドモード

グローバル設定

デフォルト

ドロップ ポリシーは **tail** に設定されます。

用途

このコマンドは、パケットがキューからオーバーフローする場合に、パケットを QoS パケット キューの先頭または末尾のどちらからドロップするかを指定します。

使用例

次のコマンドは、ドロップ ポリシーを **head** に設定します。

```
controller(config)# qosvars drop-policy head
```

関連コマンド

[show qosvars \(765 ページ\)](#)

qosvars enable

QoS を有効にします。

構文

```
qosvars enable
qosvars no enable
```

コマンド モード

グローバル設定

デフォルト

QoS はデフォルトで有効です。

用途

このコマンドは、QoS 設定をグローバルで有効にします。

使用例

次のコマンドは、QoS 設定をグローバルで有効にします。

```
default(config)# qosvars enable
default(config)#
```

次のコマンドは、QoS を無効にします。

```
controller(config)# qosvars no enable
controller(config)#
```

関連コマンド

- [qosvars admission \(727 ページ\)](#)
- [qosvars bwscaling \(729 ページ\)](#)
- [qosvars cac-deauth \(730 ページ\)](#)
- [qosvars calls-per-ap \(731 ページ\)](#)
- [qosvars calls-per-bssid \(732 ページ\)](#)
- [qosvars drop-policy \(734 ページ\)](#)
- [qosvars load-balance-overflow \(738 ページ\)](#)
- [qosvars max-stations-per-radio \(739 ページ\)](#)
- [qosvars max-stations-per-bssid \(740 ページ\)](#)
- [qosvars tcpttl \(743 ページ\)](#)
- [qosvars ttl \(744 ページ\)](#)
- [qosvars udpttl \(745 ページ\)](#)

- [show qosvars](#) (765 ページ)

qosvars intercell-periodicity

このコマンドは、このリリースではサポートされません。

構文

`qosvars intercell-periodicity`

コマンド モード

グローバル設定

デフォルト

用途

このコマンドは CLI に表示されていますが、使用することはできず、サポートもされていません。

qosvars load-balance-overflow

AP および BSSID におけるクライアント ロード バランスを有効または無効にします。

構文

```
qosvars load-balance-overflow on  
qosvars load-balance-overflow off
```

コマンド モード

グローバル設定

デフォルト

このコマンドのデフォルト設定はオフ (無効) です。

用途

このコマンドは、BSSID および AP におけるクライアント ロード バランスを有効または無効にし、クライアント コール セッションの QoS レベルを保証します。このコマンドは、**qosvars max-stations-per-radio** および **qosvars max-stations-per-bssid** と一緒に使用します。ステーションの最大数に達すると、このコマンドが **on** に設定されている場合であっても、新しいコールの関連付けが ラウンドロビン方式で AS および BSSID に均等に分散されます。

使用例

次のコマンドは、クライアント ロード バランス オーバーフロー保護を有効にします。

```
controller(config)# qosvars load-balance-overflow on
```

関連コマンド

- [qosvars max-stations-per-radio \(739 ページ\)](#)
- [qosvars max-stations-per-bssid \(740 ページ\)](#)
- [show qosvars \(765 ページ\)](#)

qosvars max-stations-per-radio

ワイヤレス間のクライアント ロード バランスを設定します。

構文

qosvars max-stations-per-radio <max_stations>

max_stations ワイヤレスに関連付けることができるクライアント (ステーション) の最大数を指定します。デフォルトでは 128 に設定され、0 ~ 384 の範囲で指定できます。

コマンドモード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 128 です。

用途

このコマンドは、AP ワイヤレス間のクライアント ロード バランスを設定し、クライアント コール セッションの QoS レベルを保証します。このコマンドは、1 つのワイヤレスに割り当てることができるステーションの最大数を設定します。ステーションの最大数に達すると、**qosvars load-balance overflow** コマンドが **on** に設定されている場合であっても、新しいコールの関連付けがラウンドロビン方式でワイヤレスおよび BSSID に均等に分散されます。

使用例

次のコマンドは、ワイヤレスあたりの最大ステーション数を 15 に設定します。

```
controller(config)# qosvars max-stations-per-radio 15
```

関連コマンド

- [qosvars load-balance-overflow \(738 ページ\)](#)
- [qosvars max-stations-per-bssid \(740 ページ\)](#)
- [show qosvars \(765 ページ\)](#)

qosvars max-stations-per-bssid

BSSID 間のクライアント ロード バランスを設定します。

構文

```
qosvars max-stations-per-bssid <max_stations>
```

max_stations BSSID に関連付けることができるクライアント (ステーション) の最大数を指定します。デフォルトでは 0 に設定され、1023 以下の最大ステーション数を設定できます。

コマンドモード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 0 であり、基本的にはクライアント ロード バランスが無効になります。

用途

このコマンドは、BSSID 間のクライアント ロード バランスを設定し、クライアント コールセッションの QoS レベルを保証します。このコマンドは、1 つの BSSID に割り当てることのできるステーションの最大数を設定します。BSSID あたりの最大ステーション数に達すると、**qosvars load-balance overflow** コマンドが on に設定されている場合であっても、新しいコールの関連付けがラウンドロビン方式で BSSID 間に均等に分散されます。

仮想セル間でクライアント ロード バランスを実行したい場合は、**max-stations-per-bssid** を、ネットワーク内のデバイス数を仮想セル数 (または BSSID 数) で除算した数に設定することを推奨します。今後、ネットワークに参加するデバイスが増える可能性がある場合は、**qosvars load-balance overflow** を on にして、最大ステーション数に達した場合にラウンドロビン方式での新しいクライアント割り当てのロード バランスが実行されるようにしてください。

使用例

次のコマンドは、BSSID あたりの最大ステーション数を 30 に設定します。

```
controller(config)# qosvars max-stations-per-bssid 30
```

関連コマンド

- [qosvars max-stations-per-radio \(739 ページ\)](#)
- [qosvars load-balance-overflow \(738 ページ\)](#)
- [show qosvars \(765 ページ\)](#)

qosvars sip-idle-timeout

SIP コールのタイムアウト間隔を設定します。

構文

qosvars sip-idle-timeout <*seconds*>

seconds

コールがアイドル状態のままでいられる最大秒数を指定します。
interval には 5 ～ 3600 を指定でき、デフォルトは 150 秒です。

コマンド モード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 150 秒です。

用途

このコマンドを使用して、コールが応答するまでにアイドル状態でいられる時間を設定します (この設定は CAC の一部です)。有効な範囲は 5 ～ 3600 秒で、デフォルト設定は 120 秒です。

使用例

次のコマンドは、最大アイドル間隔を 1000 秒に設定します。

```
controller(config)# qosvars sip-idle-timeout 1000
```

関連コマンド

[show qosvars](#) (765 ページ)

qosvars station-assign-age

ステーションの関連付けに許可される秒数を設定します。

構文

`qosvars stations-assign-age <seconds>`

seconds ステーションの関連付けに許可される最大秒数を指定します。*interval* には 5 ～ 2000 を指定でき、デフォルトは 30 秒です。

コマンドモード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 30 秒です。

用途

このコマンドを使用して、BSS によるプローブまたは認証の要求 / 応答シーケンスの完了を待機する間に AP がクライアントの状態をキャッシュする時間を設定します。フォーティネット カスタマ サポートのテクニカル アシスタンス センタで推奨されていない限り、ほとんどのサイトでは、デフォルトである 30 秒が適当であり、変更しないでください。

使用例

次のコマンドは、最大関連付け間隔を 10 秒に設定します。

```
controller(config)# qosvars stations-assign-age 10
```

関連コマンド

[show qosvars \(765 ページ\)](#)

qosvars tcpttl

TCP QoS TTL (Time To Live) 値を指定します。

構文

qosvars tcpttl <value>

value 0 ～ 65,535 秒の値を指定できます。

コマンド モード

グローバル設定

デフォルト

デフォルトの TCP TTL は 0 秒です。

用途

このコマンドは、QoS TCP フローがベストエフォート クラスに移動されるまでにアクティブでない状態にいることができる秒数を指定します。

使用例

次のコマンドは、QoS TCP フロー TTL を 65535 に設定します。

```
controller(config)# qosvars tcpttl 65535
```

関連コマンド

[show qosvars](#) (765 ページ)

qosvars ttl

デフォルト QoS TTL (Time To Live) 値を指定します。

構文

qosvars ttl <value>

value 0 ～ 65,535 秒の値を指定できます。

コマンド モード

グローバル設定

デフォルト

デフォルト TTL 値は 0 です。

用途

このコマンドは、パケットのアクティビティが何もない継続中のフロー（たとえば、音声コール）をシステムが認識してリソースを保持する時間を指定します。

たとえば、デフォルト TTL 値が 300 秒に設定されていると、コールが何もパケットを交換しない状態が 5 分間続いてから、リソースが放棄されます。不連続送信を使用するアプリケーションでは、大きい TTL 値が必要になる可能性があります。

使用例

次のコマンドは、デフォルト QoS TTL 値を 300 秒 (5 分) に設定します。

```
controller(config)# qosvars ttl 300
```

関連コマンド

[show qosvars \(765 ページ\)](#)

qosvars udpttl

UDP QoS TTL (Time To Live) 値を指定します。

構文

qosvars udpttl <value>

value 0 ～ 65,535 秒の値を指定できます。

コマンド モード

グローバル設定

デフォルト

このコマンドのデフォルト設定は 0 です。

用途

このコマンドは、QoS UDP フローがベストエフォート クラスに移動されるまでにアクティブでない状態であることができる秒数を指定します。

使用例

次のコマンドは、QoS UDP フロー TTL を 65535 に設定します。

```
controller(config)# qosvars udpttl 65535
```

関連コマンド

[show qosvars \(765 ページ\)](#)

rspecrate

QoS コーデック ルールの予約スเปック レートを指定します。

構文

rspecrate <rate>

rate

予約スเปック レートを指定します。0 ～ 1,000,000 バイト / 秒です。

コマンドモード

QoS コーデック 設定

デフォルト

デフォルトの予約スเปック レートは 0 バイト / 秒です。

用途

このコマンドは、QoS コーデック ルールの Rspec レートを指定します。

使用例

次のコマンドは、Rspec レートを 1,000,000 バイト / 秒に設定します。

```
controller(config-qoscodec)# rspecrate 1000000
```

関連コマンド

[show qoscodec \(754 ページ\)](#)

rspecslack

QoS コーデック ルールの予約スเปック スラックを指定します。

構文

rspecslack <slack>

slack 予約スเปック スラックを指定します。0 ～ 1,000,000 バイト / 秒です。

コマンド モード

QoS コーデック 設定

デフォルト

デフォルトの予約スเปック スラックは 0 バイト / 秒です。

用途

このコマンドは、QoS コーデック ルールの予約スเปック (Rspec) スラックを指定します。

使用例

次のコマンドは、Rspec スラックを 1000000 に設定します。

```
controller(config-qoscodec)# rspecslack 1000000
```

関連コマンド

[show qoscodec \(754 ページ\)](#)

srcip

QoS ルールのソース IP アドレスを指定します。

構文

srcip <source-ip-address>

source-ip-address ソース IP アドレスを指定します。*nnn.nnn.nnn.nnn* の形式で指定する必要があります。

コマンドモード

Qosrule 設定

デフォルト

なし

用途

このコマンドは、QoS ルールのソース IP アドレスを指定します。ソース IP アドレスをソース サブネット マスクと一緒に、QoS ルールのマッチング基準として使用します。

使用例

次のコマンドは、ソース IP アドレスを設定します。

```
controller(config-qosrule)# srcip 192.20.0.0
```

関連コマンド

- [show qosrule \(759 ページ\)](#)
- [srcmask \(749 ページ\)](#)
- [srcport \(750 ページ\)](#)
- [qosrule \(722 ページ\)](#)

srcmask

QoS ルールのソース IP アドレス ネットマスクを指定します。

構文

srcmask <source-netmask>

source-netmask ソース IP アドレスのサブネット マスクを指定します。
nnn.nnn.nnn.nnn の形式で指定する必要があります。

コマンド モード

Qosrule 設定

デフォルト

なし

用途

このコマンドは、QoS ルールのソース IP アドレスのサブネット マスクを指定します。ソース IP アドレスをソース サブネット マスクと一緒に、QoS ルールのマッチング基準として使用します。

使用例

次のコマンドは、ソース ネットマスクを設定します。

```
controller(config-qosrule)# srcmsk 255.0.0.0
```

関連コマンド

- [srcip \(748 ページ\)](#)
- [srcport \(750 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

srcport

QoS ルールの TCP または UDP のソース ポートを指定します。

構文

srcport <source-port>

source-port TCP または UDP のソース ポートを指定します。0 ～ 65535 の範囲で指定します。

コマンドモード

Qosrule 設定

デフォルト

デフォルト ポートは 0 (すべてのポートを指定) です。

用途

このコマンドは、QoS ルールのマッチング基準として使用する、TCP または UDP のソース ポートを指定します (ゼロはすべてのポートを指定します)。

コントローラは、通過するトラフィックを監視します。SIP または H.323 サービス用に予約されたポートでステーションからサーバに送信されるパケットを見つけると、そのシーケンスの後続の通信を追跡し、VoIP 通話に適したレベルのサービスを VoIP 通話に提供します。

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)
- H.323 サービス用の 1720 (TCP)

これらは、それぞれのサービスの標準ポート番号です。VoIP デバイスがこれらのポートを使用してサーバと通信しているのであれば、システムで VoIP QoS ルールを設定する必要はありません。

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、コントローラの QoS ルールをシステムが使用しているポートに合わせて変更する必要があります。

使用例

次のコマンドは、ソース ポートを 1200 に設定します。

```
controller(config-qosrule)# srcport 1200
```


関連コマンド

- [srcip](#) (748 ページ)
- [srcmask](#) (749 ページ)
- [qosrule](#) (722 ページ)
- [show qosrule](#) (759 ページ)

show phones

登録されているすべての電話を表示します。

構文 `show phones`

コマンド
モード 特権 EXEC

デフォルト なし

用途 このコマンドは、システムに登録されているすべての電話を表示します。クライアント電話の MAC アドレスと IP アドレス、関連付けられている AP の名前、電話のタイプ、電話に関連付けられているユーザ名、コールを処理する SIP サーバなどの情報が表示されます。

WLAN との相互運用が可能な電話のリストについては、<http://www.merunetworks.com/partners/unplugged/voippartners/interoperablephones.php> を参照してください。

使用例 次のコマンドは、システムに登録されているすべての電話を表示します。

```
controller# show phones
```

MAC Server	IP	AP ID	AP Name	Type	Username
00:0f:86:12:1d:7c 10.6.6.103	10.0.220.119	1	AP-1	sip	5381

Phone Table(1 entry)

```
controller#
```

関連コマンド [show phone-calls \(753 ページ\)](#)

show phone-calls

アクティブなすべてのコールを表示します。

構文 `show phone-calls`

コマンド
モード 特権 EXEC

デフォルト なし

用途 このコマンドは、システムのすべてのアクティブなコールを表示します。

使用例 このコマンドは、システムのすべてのアクティブなコールを表示します。

controller# `show 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)

関連コマンド [show phones \(752 ページ\)](#)

show qoscodec

QoS コーデック ルールのサマリを表示します。

構文

```
show qoscodec <id>
```

id オプション。QoS コーデック ルールの番号を指定します。

コマンド モード

特権 EXEC

デフォルト

このコマンドのデフォルトでは、設定されているすべての QoS コーデック ルールが表示されます。

用途

このコマンドは、すべての QoS コーデック ルールを表示するか、オプションの引数を指定することで、特定の QoS コーデック ルールを表示します。

コーデック ルールの詳細には、次の情報が提供されます。

ID	QoS コーデック ルールの固有の数値 ID。
Codec	コーデック タイプを指定します。
Token Bucket Rate	トークン バケット レートを指定します。
Token Bucket Size	トークン バケットのサイズを指定します。
Peak Rate	Tspec (トラフィック仕様) ピーク レートを指定します。
Maximum Packet Size	最大パケット サイズを指定します。
Minimum Policed Unit	最小規制単位のサイズを指定します。
Reservation Rate	予約レートを指定します。
Reservation Slack	予約スラックを指定します。
Packet Rate	フロー パケット レートを指定します。
QoS Protocol	次の QoS プロトコルを指定します。 <ul style="list-style-type: none">• SIP• H.323

使用例

次のコマンドは、設定されているすべての QoS コーデック ルールを表示します。

```
controller> show qoscodec
```

ID	Codec	Qos Protocol
----	-------	--------------

22	h263	sip
21	h261	sip
20	siren	sip
19	g729	sip
18	g7221-32	sip
17	g7221	sip
16	g711a	sip
15	g723.1	sip
14	gsm	sip
13	g711u	sip
12	default	sip
11	h263	h323
10	h261	h323
9	siren	h323
8	g729	h323
7	g7221-32	h323
6	g7221	h323
5	g711a	h323
4	g723.1	h323
3	gsm	h323
2	g711u	h323
1	default	h323

QoS Codec Rules(22)

次のコマンドは、QoS コーデック ルール 4 を表示します。

```
controller> show qoscodec 4
```

QoS Codec Rules

ID	: 4
Codec	: g723.1
Token Bucket Rate (0-1,000,000 bytes/second)	: 2100

Token Bucket Size (0-16,000 bytes)	: 128
Peak Rate (0-1,000,000 bytes/second)	: 2500
Maximum Packet Size (0-1,500 bytes)	: 64
Minimum Policed Unit (0-1,500 bytes)	: 0
Reservation Rate (0-1,000,000 bytes/second)	: 2100
Reservation Slack (0-1,000,000 microseconds)	: 10000
Packet Rate (0-200 packets/second)	: 33
QoS Protocol	: h323

関連コマンド

- [peakrate](#) (716 ページ)
- [qoscodec](#) (718 ページ)
- [rspecrate](#) (746 ページ)
- [rspecslack](#) (747 ページ)
- [tokenbucketsize](#) (771 ページ)

show qosflows

すべての QoS フローを表示します。

構文 `show qosflows`

コマンド
モード 特権 EXEC

デフォルト なし

用途 `show qosflows` コマンドを使用して、アクティブおよびペンディングのすべての QoS フローを表示します。

使用例 次のコマンドは、QoS フローを表示します。

```
controller# show qosflows
ID      Source IP      Source Destination IP  Dest  Prot  Token Average
Status
                                Port          Port          BRate BRate
12      10.6.6.103      0      192.168.10.172      5060  17
16      10.6.6.103      0      192.168.10.161      5060  17
19      10.6.6.103      0      192.168.10.177      5060  17
24      10.6.6.103      0      192.168.10.157      5060  17
25      10.6.6.103      0      192.168.10.180      5060  17
26      10.6.6.103      0      192.168.10.150      5060  17
28      10.6.6.103      0      192.168.10.178      5060  17
13      10.6.6.103      0      192.168.10.143      5060  17
controller#
```

758 ページの表 6 に、show qosflows の出力のフィールドの説明を記載します。

表 6: show qosflows の出力

フィールド	説明
ID	QoS フローの固有の数値 ID
Source IP	ソース IP アドレス。宛先サブネット マスクと一緒に、QoS ルールのマッチング基準として使用されます。
Source Port	QoS ルールのマッチング基準として使用される TCP または UDP のソース ポート (ゼロはすべてのポートを指定)
Destination IP	宛先 IP アドレス。宛先サブネット マスクと一緒に、QoS ルールのマッチング基準として使用されます。
Destination Port	QoS ルールのマッチング基準として使用される TCP または UDP の宛先 ポート (ゼロはすべてのポートを指定)
Prot	Network protocol: フローが TCP (6)、UDP (17)、またはその他のいずれであるかを指定します。
Token BRate	トークン バケット レート (バイト / 秒)
Average BRate	平均バケット レート (バイト / 秒)
Status	予約ステータス

show qosrule

システムに設定されている QoS ルールを表示します。

構文

```
show qosrule
show qosrule <rule>
```

rule QoS ルールの ID を指定します。

コマンドモード

特権 EXEC

デフォルト

設定されているすべての QoS ルールを表示します。

用途

このコマンドは、すべての QoS ルールを表示するか、オプションの引数を指定することで、特定の QoS ルールを表示します。コマンドでルールを指定すると、ルールの優先度やトラフィック制御設定に関する追加情報が表示されます。

次の情報が表示されます。

ID	QoS ルールの固有の数値 ID
Dst IP (宛先 IP)	この IP アドレスは、宛先サブネット マスクと一緒に、QoS ルールのマッチング基準として使用されます。
Dst Mask (宛先ネットマスク)	宛先 IP アドレスのサブネット マスク
DPort (宛先ポート)	QoS ルールのマッチング基準として使用される、TCP または UDP の宛先ポート (ゼロはすべてのポートを指定)
Src IP (ソース IP)	ソース IP アドレス。ソース サブネット マスクと一緒に、QoS ルールのマッチング基準として使用されます。
Src Mask (ソース ネットマスク)	ソース IP アドレスのサブネット マスク
SPort (ソース ポート)	QoS ルールのマッチング基準として使用される TCP または UDP のソース ポート (ゼロはすべてのポートを指定)

Prot (ネットワーク プロトコル)	<p>フローが TCP (6)、UDP (17)、またはその他のいずれであるかを表します。QoS プロトコル検出を使用すると、ネットワーク プロトコルは以下のタイプの QoS プロトコルと一致します。</p> <p>UDP: SIP</p> <p>TCP: H.323</p> <p>TCP: SCCP</p>
Firewall Filter	このファイアウォール フィルタ qosrule に割り当てられている ID
Qos (QoS プロトコル)	<p>QoS プロトコルは、次のいずれかです。</p> <p>SIP</p> <p>H.323</p> <p>SCCP</p> <p>Other</p>
Average Packet Rate	平均フロー パケット レート
Action	<p>パケットに対するルールを指定します。</p> <p>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。</p> <p>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。</p> <p>Drop: フローがドロップされます。</p>
Drop (ポリシーのドロップ)	<p>キューが満杯である場合、受信パケットに対する処理を決定します。</p> <p>Head: キューが最大長に達した後に到着する新しいパケットを許可し、キューの古い情報を新しい情報に置換します。</p> <p>Tail: キューが最大長に達した後に到着する新しいパケットはドロップします。</p>
Token Bucket Rate	トークン パケット レート (バイト / 秒) を指定します。
Priority	キューに割り当てる優先度 レベルを指定します。
Traffic Control	<p>トラフィック制御を強制するかどうかを指定します。トラフィック制御は、次のいずれかです。</p> <p>On</p> <p>Off</p>
DiffServe Codepoint	DiffServ 設定が使用されているか識別します。また、設定が使用されていない場合、DiffServe を無効にします。

使用例

次のコマンドは、すべての QoS ルールを表示します。

```
controller> show qosrule
```

ID	Dst IP	Dst Mask	DPort	Src IP	Src Mask	
SPort	Prot	Firewall	Filter	Qos	Action	Drop
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		other	forward	head		
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	
5200	17	other	forward	head		
2001	10.0.0.10	255.255.255.255	53	192.168.37.0	255.255.255.0	
0	17 ab10	none	forward	head		
2002	10.0.0.40	255.255.255.255	53	192.168.37.0	255.255.255.0	
0	17 ab10	none	forward	head		
2003	192.168.37.4	255.255.255.255	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	forward	head		
4001	10.0.0.0	255.0.0.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	other	drop	head		
4002	192.168.0.0	255.255.224.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4003	192.168.64.0	255.255.192.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4004	192.168.128.0	255.255.128.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4005	192.168.48.0	255.255.240.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4006	192.168.40.0	255.255.248.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4007	192.168.32.0	255.255.252.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4008	192.168.38.0	255.255.254.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		

4009	192.168.36.0	255.255.255.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4010	192.168.37.0	255.255.255.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4011	172.16.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4012	172.17.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4013	172.18.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4014	172.26.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4015	172.27.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4016	0.0.0.0	0.0.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none forward	head	

QoS and Firewall Rules(25 entries)

次のコマンドは、QoS ルール 1 を表示します。

controller> **show qosrule 1**

QoS and Firewall Rules

ID	: 1
Id Class flow class	: none
Destination IP	: 0.0.0.0
Destination IP match	: none
Destination IP flow class	: none
Destination Netmask	: 0.0.0.0
Destination Port	: 1720
Destination Port match	: on
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	: 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	: h323
Average Packet Rate	: 0
Action	: capture
Drop Policy	: head
Token Bucket Rate	: 0
Priority	: 0
Traffic Control	: off
DiffServ Codepoint	: cs0
Qos Rule Logging	: off
Qos Rule Logging Frequency	: 60

関連コマンド

- [avgpacketrates \(694 ページ\)](#)
- [dstip \(696 ページ\)](#)
- [dstmask \(699 ページ\)](#)
- [dstport-match \(703 ページ\)](#)
- [priority \(717 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [srcip \(748 ページ\)](#)
- [srcmask \(749 ページ\)](#)
- [srcport \(750 ページ\)](#)
- [tokenbucketrate \(769 ページ\)](#)
- [trafficcontrol-enable \(772 ページ\)](#)

show qosstats

QoS 統計を表示します。

構文

`show qosstats`

コマンド モード

特権 EXEC

デフォルト

なし

用途

以下の QoS グローバル統計を表示します。

- H.323、SIP、および合計のセッション カウント
- H.323、SIP、および合計の拒否カウント
- H.323、SIP、および合計のペンディング カウント
- QoS アクティブ フロー カウント
- Qos ペンディング フロー カウント

使用例

```
controller> show qosstats
Global Quality-of-Service Statistics
Session Count           : 0
H.323 Session Count     : 0
SIP Session Count       : 0
Rejected Session Count   : 0
Rejected H.323 Session Count : 0
Rejected SIP Session Count : 0
Pending Session Count    : 0
Pending H.323 Session Count : 0
Pending SIP Session Count : 0
Active Flows             : 0
Pending Flows            : 0
```

Active Flows と Pending Flows には、H.323/SIP フローと、QoS ルールに設定されたすべてのフローが含まれます。

show qosvars

QoS グローバル パラメータを表示します。

構文

show qosvars

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、QoS グローバル パラメータ設定を表示します。「関連コマンド」セクションに記載されている **qosvars** コマンドを使用して、これらのパラメータを設定します。

使用例

次のコマンドは、QoS パラメータのデフォルト設定を表示します。

```
controller> show qosvars
```

Global Quality-of-Service Parameters

```
On/Off                        : on
Admission Control             : admitall
Drop Policy                   : head
Default Time-to-live (seconds) : 0
UDP Time-to-live (seconds)    : 0
TCP Time-to-live (seconds)    : 0
Bandwidth Scaling (percent)   : 100
Intercell Periodicity (ms)    : 30
Maximum Calls Per AP          : 0
Maximum Calls Per Interference Region : 0
Maximum Stations Per AP       : 128
Maximum Stations Per BSSID    : 0
Load Balance Overflow         : off
Maximum Calls Per BSSID       : 0
CAC Deauth                    : off
Station Assignment Age Time    : 30
```

SIP Idle Timeout (seconds) : 120

関連コマンド

- [qosvars admission \(727 ページ\)](#)
- [qosvars bwscaling \(729 ページ\)](#)
- [qosvars cac-deauth \(730 ページ\)](#)
- [qosvars calls-per-ap \(731 ページ\)](#)
- [qosvars calls-per-bssid \(732 ページ\)](#)
- [qosvars drop-policy \(734 ページ\)](#)
- [qosvars enable \(735 ページ\)](#)
- [qosvars load-balance-overflow \(738 ページ\)](#)
- [qosvars max-stations-per-radio \(739 ページ\)](#)
- [qosvars max-stations-per-bssid \(740 ページ\)](#)
- [qosvars tcpttl \(743 ページ\)](#)
- [qosvars ttl \(744 ページ\)](#)
- [qosvars udpttl \(745 ページ\)](#)

show statistics call-admission-control

CAC (Call Admission Control) 統計を表示します。

構文

```
show statistics call-admission-control ap
show statistics call-admission-control bss
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、AP または BSS ごとの CAC 統計を表示します。AP または BSS のいずれかの場合は、アクティブ コールの現在の数と、最大コール数の設定に達したために拒否されたコールの累積数が表示されます。BSS および AP あたりの拒否されたコールの累積数は、コントローラまたは AP のリブート時にリセットされます。下記の「関連コマンド」に記載されている **qosvars** コマンドを使用して、これらのパラメータを設定します。

使用例

次のコマンドは、AP の CAC 統計を表示します。

```
controller> show statistics call-admission-control ap
```

```
AP ID Current Calls Cumulative Rejected Calls
```

```
1      0              0
```

```
Call Admission Control AP Statistics(1 entry)
```

次のコマンドは、BSS の CAC 統計を表示します。

```
controller> show statistics call-admission-control bss
```

```
BSSID          Current Calls Cumulative Rejected Calls
```

```
00:12:f2:30:97:49 0          0
```

```
00:12:f2:4e:9b:ce 0          0
```

```
00:12:f2:de:ec:6f 0          0
```

```
Call Admission Control BSS Statistics(3 entries)
```

関連コマンド

- [qosvars calls-per-ap \(731 ページ\)](#)
- [qosvars calls-per-bssid \(732 ページ\)](#)

tokenbucketrate

QoS ルールのトークン バケット レートを指定します。

構文

`tokenbucketrate <tokenbucketrate>`

tokenbucketrate トークン バケット レートを指定します。レートには 0 ～ 1,000,000 バイト / 秒を指定できます。デフォルトは 0 です。

コマンド モード

Qosrule 設定

デフォルト

デフォルトのトークン バケット レートは 0 です。

用途

このコマンドは、トークンが仮想トークン バケットに入れられる速度を指定します。フローごとに専用のバケットが存在し、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。

優先度が有効になっていると、トークン バケット レートを指定できません。

トークン バケット レートと最大帯域幅の関係は、以下のとおりです。

<u>トークン バケット レート</u>	<u>最大帯域幅</u>
----------------------	--------------

1000	8Kbps
5000	40Kbps
12500	125Kbps
125000	1Mbps
625000	5Mbps
1000000	8Mbps (最大値)

トークン バケット レート = $x/8$ (x は優先最大帯域幅)

使用例

次のコマンドは、トークン バケット レートを 3333 に設定し、その後に 1,000,000 にリセットします。

```
controller # configure terminal
controller(config)# qoscodec 4 codec default qosprotocol none
tokenbucketrate 3333 maxdatagramsize 4 minpolicedunit 45 samplerate 34
controller(config-qosrule)# tokenbucketrate 1000000
```

関連コマンド

- [priority \(717 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)
- [tokenbucketsize \(771 ページ\)](#)

tokenbucketsize

トークン バケット サイズを指定します。

構文

`tokenbucketsize <size>`

size 0 ～ 16,000 バイトのトークン バケット サイズを指定します。

コマンドモード

QoS コーデック設定

デフォルト

デフォルトのトークン バケット サイズは 8K バイトです。

用途

このコマンドは、トークン バケットのサイズを指定します。

使用例

次のコマンドは、トークン バケット サイズを 10,000 バイトに設定します。

```
controller(config-qoscodec)# configure terminal
controller(config)# qoscodec 4 codec default qosprotocol none
tokenbucketrate 3333 maxdatagramsize 4 minpolicedunit 45 samplerate 34
controller(config-qoscodec)# tokenbucketsize 10000
```

関連コマンド

- [qoscodec \(718 ページ\)](#)
- [tokenbucketrate \(769 ページ\)](#)
- [show qoscodec \(754 ページ\)](#)

trafficcontrol-enable

QoS ルールのトラフィック制御ポリシーを有効にします。`no trafficcontrol` コマンドによって、トラフィック制御ポリシーが無効になります。

構文

```
trafficcontrol-enable  
no trafficcontrol
```

コマンド モード

Qosrule 設定

デフォルト

デフォルトでは、トラフィック制御が無効です。

用途

このコマンドを使用して、トラフィック制御を有効にします。トラフィック制御を有効にすると、[avgpacketrate \(694 ページ\)](#) コマンドで指定したレートにフロー (明示、検出済み、およびベストエフォート) 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。

使用例

次の例は、最初にトラフィック制御を有効にし、その後のコマンドでトラフィック制御を無効にしています。

```
controller(config-qosrule)# trafficcontrol-enable  
controller(config-qosrule)# no trafficcontrol
```

関連コマンド

- [avgpacketrate \(694 ページ\)](#)
- [qosrule \(722 ページ\)](#)
- [show qosrule \(759 ページ\)](#)

15 SNMP コマンド

本章で説明するコマンドは、システムの SNMP を設定してその内容を表示するために使用されます。SNMPv3 アーキテクチャは、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) の新しい記述、最新のメッセージ形式、およびエンティティに対するアクセスの設定に使用される標準 MIB を統合しています。SNMPv3 の新機能としては、メッセージ タイム スタンプと一緒にエンティティで共有される秘密鍵を使用するユーザ認証、暗号化によるデータのセキュリティ保護、および必要性に応じた MIB 情報に対するユーザアクセスの制御があります。

- [reload-snmp \(774 ページ\)](#)
- [show snmp-community \(775 ページ\)](#)
- [show snmp-trap \(776 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmp-filter-config \(778 ページ\)](#)
- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-key \(780 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)
- [snmp start および snmp stop \(785 ページ\)](#)
- [snmp-server community \(786 ページ\)](#)
- [snmp-server contact \(787 ページ\)](#)
- [snmp-server description \(788 ページ\)](#)
- [snmp-server location \(789 ページ\)](#)
- [snmp-server trap \(790 ページ\)](#)
- [show snmp-filter-config \(791 ページ\)](#)

reload-snmp

SNMP プロセスを再起動します。

構文

`reload-snmp`

コマンド モード

特権 EXEC

デフォルト

なし

用途

SNMP プロセスを再ロードするには、このコマンドを使用します。SNMP が SNMP の受信パケットに応答しない場合などに、このコマンドを使用できます。

使用例

`default# reload-snmp`

show snmp-community

コミュニティ内の IP アドレスおよび特権を表示します。

構文

`show snmp-community`

コマンド モード

特権 EXEC

デフォルト

なし

用途

IP アドレス、読み取り / 書き込み権限など、SNMP コミュニティに関する情報を表示するには、このコマンドを使用します。

使用例

`default# show snmp-community`

SNMP Community	Client IP	Privilege
public	0.0.0.0	read-only

SNMP Community Management(1 entry)

関連コマンド

[snmp-server community](#) (786 ページ)

show snmp-trap

SNMP トラップ コミュニティを表示します。

構文

`show snmp-trap`

コマンド モード

特権 EXEC

デフォルト

なし

用途

トラップ コミュニティ内の IP アドレスを表示するには、このコマンドを使用します。

使用例

```
controller# show snmp-trap
SNMP Trap Management
Trap Community          Destination IP
32                      10.10.1.1
      SNMP Trap Management(1 entry)
controller#
```

関連コマンド

[snmp-server trap](#) (790 ページ)

show snmpv3-user

SNMPv3 ユーザ情報を表示します。

構文

`show snmpv3 user`

コマンドモード

EXEC モード

デフォルト

なし

用途

このコマンドを使用すると、以下の情報が表示されます。

```
snmpv3# sh snmpv3-user
```

User Name Key	AuthProt	PrivProt	Target IP	Auth Key	Priv
NoAuthNoPriv	no-auth	no-priv	192.168.221.101		
MD5AuthNoPriv	md5-auth	no-priv	192.168.203.150	123456789	
SHAAuthNoPriv	sha-auth	no-priv	192.168.46.235	456789123	
MD5AuthDESPriv 456123987	md5-auth	des-priv	192.168.10.251	123456789	
SHAAuthDESPriv 741852963	sha-auth	des-priv	192.168.98.220	456789741	

SNMPv3 User Configuration(5)

関連コマンド

- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-key \(780 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)

snmp-filter-config

次のテーブルを基準として SNMP インターフェイス フィルタを設定します。

- Ap-Assigned (割り当て済み AP テーブル)
- AP-Discovered (検出済み AP テーブル)
- AP-Neighbor (AP 近接テーブル)
- AP-Neighbor detail (AP 近接詳細テーブル)

構文

`snmp-filter-config <parameters>`

パラメータは以下のとおりです。

- ap-assigned
- ap-discovered
- ap-neighbor
- ap-neighbor-detail

コマンド モード

グローバル設定

デフォルト

なし

用途

SNMP インターフェイスをフィルタリングするには、このコマンドを使用します。

```
MC3200(15)# configure terminal
MC3200(15)(config)# snmp-filter-config ap-discovered
MC3200(15)(config)#
```

関連コマンド

[show snmp-filter-config \(791 ページ\)](#)

snmpv3-user

新しい SNMPv3 ユーザ名を作成します。または、設定する既存の SNMPv3 ユーザ名を開きます。

構文

`snmpv3-user <name>`

コマンドモード

設定モード

デフォルト

なし

用途

このコマンドを使用して、SNMPv3 ユーザを設定するプロセスを開始します。「関連コマンド」に記載されているコマンドを使用して、さらにユーザを定義します。

使用例

以下の例では、SNMPv3 ユーザ MWP を作成します。

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)#
```

関連コマンド

- [snmpv3-user auth-key \(780 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)

snmpv3-user auth-key

SNMPv3 の秘密鍵を設定します。

構文

auth-key <authentication key>

コマンドモード

設定モード

デフォルト

なし

用途

このコマンドを使用する前に、以下の例に示すように、SNMPv3 ユーザを作成するか、既存のユーザを開く必要があります。

使用例

以下の例では、SNMPv3 ユーザ MWP を開き、認証鍵 8h8h8h を割り当てます。

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# auth-key 8h8h8h
```

関連コマンド

- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)

snmpv3-user auth-protocol

SNMPv3 USM ユーザの認証プロトコルを設定します。

構文

```
snmpv3-user auth-protocol md5-auth  
snmpv3-user auth-protocol no-auth  
snmpv3-user auth-protocol sha-auth
```

md5-auth	SNMPv3 USM ユーザの HMAC MD5 認証プロトコル
no-auth	SNMPv3 USM ユーザの認証プロトコルなし
sha-auth	SNMPv3 USM ユーザの HMAC SHA 認証プロトコル

コマンドモード

特権 EXEC モード

デフォルト

なし

用途

このコマンドを使用する前に、以下の例に示すように、SNMPv3 ユーザを作成するか、既存のユーザを開く必要があります。

使用例

以下の例では、SNMPv3 ユーザ MWP を開き、認証プロトコル sha-auth を割り当てます。

```
Master1 # configure terminal  
Master1(config)# snmpv3-user ?  
<Name>                Enter the SNMPv3 User name.  
Master1(config)# snmpv3-user MWP  
Master1(config-snmpv3-user)# auth-protocol sha-auth
```

関連コマンド

- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)

snmpv3-user priv-key

SNMPv3 の秘密鍵を設定します。

構文

`snmpv3-user <name>`

コマンド モード

設定モード

用途

このコマンドを使用する前に、以下の例に示すように、SNMPv3 ユーザを作成するか、既存のユーザを開く必要があります。

使用例

以下の例では、SNMPv3 ユーザ MWP を開き、秘密鍵 8h8h8h を割り当てます。

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                               Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# priv-key 8h8h8h
```

関連コマンド

- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)

snmpv3-user priv-protocol

SNMPv3 USM ユーザの秘密プロトコルを設定します。

構文

```
priv-protocol des-priv  
priv-protocol no-priv
```

des-priv	SNMPv3 USM ユーザの DES 秘密プロトコル
no-priv	SNMPv3 USM ユーザの秘密プロトコルなし

コマンドモード

設定モード

デフォルト

なし

用途

このコマンドを使用する前に、以下の例に示すように、SNMPv3 ユーザを作成するか、既存のユーザを開く必要があります。

使用例

以下の例では、SNMPv3 ユーザの MWP を開いてから、認証プロトコル sha-auth を割り当てます。

```
Master1 # configure terminal  
Master1(config)# snmpv3-user ?  
<Name> Enter the SNMPv3 User name.  
Master1(config)# snmpv3-user MWP  
Master1(config-snmpv3-user)# priv-protocol des-priv
```

関連コマンド

- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)

snmpv3-user target ip-address

snmpv3 ユーザの IP アドレスを設定します。

構文

`snmpv3-user target ip-address <XXX.XXX.XXX.XXX>`

コマンド モード

設定モード

デフォルト

なし

用途

このコマンドを使用する前に、以下の例に示すように、SNMPv3 ユーザを作成するか、既存のユーザを開く必要があります。

使用例

以下の例では、SNMPv3 ユーザの MWP を開き、IP アドレス 172.23.34.9 を割り当て ます。

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# target ip-address 172.23.34.9
```

関連コマンド

- [snmpv3-user \(779 ページ\)](#)
- [snmpv3-user auth-protocol \(781 ページ\)](#)
- [snmpv3-user priv-key \(782 ページ\)](#)
- [snmpv3-user priv-protocol \(783 ページ\)](#)
- [show snmpv3-user \(777 ページ\)](#)
- [snmpv3-user target ip-address \(784 ページ\)](#)

snmp start および snmp stop

SNMP を起動および停止します。SNMP ステータスを表示します。

構文

```
snmp start  
snmp stop  
snmp status
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

SNMP プロセスを起動および停止するには、このコマンドを使用します。SNMP が起動すると、SNMP イベント メッセージが生成され、サードパーティの SNMP ベースのプログラムとの相互通信を実行できます。

使用例

次のコマンドで、SNMP を起動します。

```
controller# snmp start
```

関連コマンド

snmp-server community

SNMP コミュニティを設定します。

構文

```
snmp-server community <community-string> <client_IP_address> ro
snmp-server community <community-string> <client_IP_address> rw
no snmp-server community <client_IP_address>
no snmp-server community 0.0.0.0
no snmp-server community <community-string>
no snmp-server community public <client_IP_address>
no snmp-server community public 0.0.0.0
no snmp-server community public <community-string>
```

<i>community-string</i>	32 文字以下の英数字で指定し、スペースや特殊記号は使用できません。
<i>client-ip-address</i>	SNMP の読み取り / 書き込みコミュニティに関連付けられている IP アドレスです。ワイルドカードを指定し、すべてのサーバへのアクセスを許可するには、0.0.0.0 を使用します。
ro rw	MIB への読み取り専用アクセスを許可するには、 ro と入力し、MIB への読み取り / 書き込みアクセスを許可するには、 rw と入力します。

コマンドモード

グローバル設定

デフォルト

なし

用途

SNMP コミュニティはパスワードとして機能し、SNMP サーバと SNMP クライアントの間で送信されるメッセージを認証します。SNMP コミュニティ スtring はテキストで送信されます。クライアントの IP アドレスまたはすべてのサーバ (0.0.0.0) を指定してコミュニティ スtring を削除するには、このコマンドの **no** フォームを使用します。

使用例

次のコマンドは文字列 **commstring1** をパスワードとして使用し、IP アドレスが **10.3.4.5** のサーバのみを許可して、読み取り専用のコミュニティを設定します。

```
controller(config)# snmp-server community commstring1 10.3.4.5 ro
```

関連コマンド

[show snmp-community \(775 ページ\)](#)

snmp-server contact

コントローラの担当者を設定します。

構文

`snmp-server contact <contact>`

contact 1 ～ 255 文字の担当者名です。

コマンド モード

グローバル設定

デフォルト

なし

用途

コントローラの担当者を識別するには、このコマンドを使用します。

使用例

```
controller(config)# snmp-server contact Joe
controller(config)#
```

関連コマンド

- [snmp-server description \(788 ページ\)](#)
- [snmp-server location \(789 ページ\)](#)

snmp-server description

コントローラの説明です。

構文

`snmp-server description <descr>`

descr 1 ～ 255 文字の SNMP サーバの説明です。

コマンド モード

グローバル設定

デフォルト

なし

用途

コントローラの説明を記述するには、このコマンドを使用します。

使用例

```
controller(config)# snmp-server description corp_manager
controller(config)#
```

関連コマンド

- [snmp-server location](#) (789 ページ)
- [snmp-server contact](#) (787 ページ)

snmp-server location

コントローラの場所の説明を設定します。

構文

`snmp-server location <location>`

location

コントローラの場所を記述する、1 ～ 255 文字の文字列です。

コマンドモード

グローバル設定

デフォルト

なし

用途

コントローラの場所を記述するには、このコマンドを使用します。

使用例

```
controller(config)# snmp-server location san_jose_california
controller(config)#
```

関連コマンド

- [snmp-server contact \(787 ページ\)](#)
- [snmp-server description \(788 ページ\)](#)

snmp-server trap

SNMP トラップ コミュニティを設定します。

構文

```
snmp-server trap <community-string> <client-ip-address>
```

<i>community-string</i>	SNMP コミュニティの名前です。32 文字以下の英数字で、スペースや特殊記号は使用できません。SNMP コミュニティはパスワードとして機能し、SNMP サーバと SNMP クライアントの間で送信されるメッセージを認証します。
<i>client-ip-address</i>	コントローラで生成された SNMP トラップをリスンする、SNMP トラップ レシーバの IP アドレスです。この機能を無効にし、すべてのサーバへのアクセスを許可するには、0.0.0.0 を使用します。

コマンドモード

グローバル設定

デフォルト

なし

用途

SNMP トラップ コミュニティを作成するには、**snmp-server trap** コマンドを使用します。コントローラおよび SNMP コミュニティで生成された SNMP トラップをリスンする、SNMP トラップ レシーバ (*client-IP-address* を使用) を指定します。SNMP コミュニティはテキストで送信されます。

SNMP サーバのトラップ コミュニティ スtring を削除するには、このコマンドの **no** フォームを使用します。

使用例

次のコマンドは、**commstring1** をコミュニティ スtring として使用し、**10.3.4.5** をトラップ レシーバとして指定して、SNMP トラップ コミュニティを設定します。

```
controller(config)# snmp-server trap commstring1 10.3.4.5
controller(config)#
```

関連コマンド

[show snmp-community \(775 ページ\)](#)

show snmp-filter-config

SNMP フィルタリングの設定パラメータを表示します。

構文

`show snmp-filter-config`

コマンド モード

グローバル設定

デフォルト

なし

用途

SNMP フィルタリング設定を表示するには、このコマンドを使用します。

```
MC3200(15)# show snmp-filter-config
```

SNMP フィルタリング パラメータ

AP-Discovered (検出済み AP テーブル) : on

Ap-Assigned (割り当て済み AP テーブル) : off

AP-Neighbor (AP 近接テーブル) : off

AP-Neighbor detail (AP 近接詳細テーブル) : off

```
MC3200(15)#
```

関連コマンド

[snmp-filter-config](#) (778 ページ)

16 ステーション用コマンド

本章では、ステーション (クライアント) との接続情報を表示するコマンドについて説明します。

- [associated-station-max-idle-period](#) (795 ページ)
- [no station](#) (796 ページ)
- [show ap-assigned](#) (797 ページ)
- [show dot11 associations](#) (799 ページ)
- [show dot11 statistics client-traffic](#) (801 ページ)
- [show static-station](#) (804 ページ)
- [show station-log-config](#) (805 ページ)
- [show station commands](#) (807 ページ)
- [show station 802.11](#) (811 ページ)
- [show station all](#) (813 ページ)
- [show station counter](#) (815 ページ)
- [show station details](#) (817 ページ)
- [show station general](#) (822 ページ)
- [show station mac-address](#) (825 ページ)
- [show station multiple-ip](#) (827 ページ)
- [show station network](#) (828 ページ)
- [show station security](#) (831 ページ)
- [show statistics station-per-ap](#) (834 ページ)
- [show statistics top10-station-problem](#) (836 ページ)
- [show statistics top10-station-talker](#) (838 ページ)
- [show topostaap](#) (840 ページ)
- [show topostation](#) (841 ページ)
- [station-aging-out-interval](#) (844 ページ)
- [station-aging-out-interval](#) (844 ページ)

- [station-log \(847 ページ\)](#)
- [\(station-log\) enable \(850 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)
- [\(station-log\) syslog \(852 ページ\)](#)
- [\(station-log\) event id \(853 ページ\)](#)
- [\(station-log\) event severity \(855 ページ\)](#)
- [\(station-log\) show filters \(857 ページ\)](#)
- [station-log show \(859 ページ\)](#)

associated-station-max-idle-period

関連付けられているステーションの最大アイドル時間を秒数で設定します。

構文

`associated-station-max-idle-period <value>`

value 関連付けられているステーションの最大アイドル時間を秒数 (30 ~ 86400) で入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

使用例

```
controller# configure terminal
controller(config)# associated-station-max-idle-period 10
```

関連コマンド

no station

アクセス ポイントに関連付けられているステーションの認証を解除 (削除) します。

構文

`no station [MAC_address]`

コマンド モード

グローバル設定モード

デフォルト

なし

用途

ステーションに de-auth メッセージを送信して ESS を強制的にオフにすることで、アクセス ポイントに関連付けられているステーションを削除します。このコマンドは、接続の問題をデバッグする場合に有用です。

使用例

以下のコマンドを使用すると、アクセス ポイントのステーション情報が削除されます。

```
controller# no station 00:40:96:a3:b2:95
```

関連コマンド

- [show station details \(817 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show ap-assigned

1 つ以上のアクセス ポイントに割り当てられているステーションの情報を表示します。

構文

show ap-assigned <MAC-address>

コマンド モード

EXEC

デフォルト

なし

用途

ID、MAC アドレス、ESSID などのアクセス ポイントのステーション情報を表示します。引数を指定しないでこのコマンドを実行すると、MAC アドレスのリストが表示されます。オプションの MAC アドレス引数を指定してこのコマンドを実行すると、そのステーションの詳細情報が表示されます。

使用例

以下のコマンドを使用すると、アクセス ポイントのステーション情報が表示されます。

```
controller# show ap-assigned
```

```
Assigned Stations(4 entries)
```

AP ID	Client	MAC	Type	SSID	State	Encrypt	Pkts Rx	Pkts Tx	Last
Prev	Curr	RF Band	AP Name						
2	00:02:6f:20:9a:00	STATION	mwf-wpapsk						ASSOCIATED
TKIP	34	19	00d:00h:02m:01s	188	188	802.11a	#2-2F-Sw-208		
2	00:02:6f:20:9a:01	STATION	mwf-wpapsk						ASSOCIATED
TKIP	34	19	00d:00h:02m:01s	188	188	802.11a	#2-2F-Sw-208		
2	00:02:6f:20:9a:02	STATION	mwf-wpapsk						ASSOCIATED
TKIP	35	17	00d:00h:02m:01s	188	188	802.11a	#2-2F-Sw-208		
2	00:02:6f:20:9a:03	STATION	mwf-wpapsk						ASSOCIATED
TKIP	34	17	00d:00h:02m:01s	188	188	802.11a	#2-2F-Sw-208		

```
Assigned Stations(4 entries)
```

以下のコマンドを指定すると、指定した MAC アドレスのステーション情報が表示されます。

```
meru-wifi# show ap-assigned 00:40:96:a3:b2:95
```

```
Assigned Stations
```

AP ID : 3
Client MAC : 00:40:96:a3:b2:95
Type : STATION
ESSID : meru-esspeap
Association State : ASSOCIATED
Key Type : none
Packets Received : 555
Packets Sent : 304
Last Activity : 0d:0h:0m:1s
Previous RSSI : 36
Current RSSI : 30
RF Band :802.11bg
AP Name : QA

関連コマンド

- [show dot11 associations](#) (799 ページ)
- [show dot11 statistics client-traffic](#) (801 ページ)
- [show station all](#) (813 ページ)
- [show station details](#) (817 ページ)
- [show station counter](#) (815 ページ)
- [show station general](#) (822 ページ)
- [show station network](#) (828 ページ)
- [show station security](#) (831 ページ)

show dot11 associations

システムから確認できるステーションを表示します。

構文

`show dot11 associations`

コマンド モード

EXEC

デフォルト

なし

用途

MAC アドレス、可用性、アクセス ポイント名、L2 および L3 ブロードキャスト情報を含む各種のステーション情報を表示します。

使用例

以下のコマンドを指定すると、システムから確認できるステーションが表示されます。

```
default# show dot11 associations
```

MAC Address	IP Type	AP Name	L2 Mode	L3 Mode	Authenticated
User Name	Tag	Client IP			

00:12:f0:54:a2:56	DHCP	11-Skim	wpa2-psk	clear	
0	192.168.34.21				

00:13:e8:83:27:3f	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.116				

00:16:6f:0d:59:4d	DHCP	9-Exit-Stairs-D	wpa-psk	clear	
0	192.168.34.89				

00:16:6f:0e:18:cd	DHCP	1-ops-Kshiomoto	wpa2-psk	clear	
0	192.168.34.42				

00:16:6f:24:7f:98	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.78				

00:18:de:bd:d0:04	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.43				

00:19:e3:06:2c:d3	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.86				

00:1a:6b:1d:9e:09	DHCP	1-ops-Kshiomoto	wpa2-psk	clear	
0	192.168.34.58				

00:1b:2f:c5:a5:24	DHCP	1-ops-Kshiomoto	clear	clear	
20	192.168.37.60				

00:1b:77:8d:75:13	DHCP	1-ops-Kshiomoto	wpa2-psk	clear	
0	192.168.34.103				

```

00:1b:77:95:94:79 DHCP      11-Skim      wpa2-psk clear
0      192.168.34.59
00:1b:77:95:a9:94 DHCP      29-Keith     wpa-psk  clear
0      192.168.34.44
00:1b:77:9a:63:4a DHCP      11-Skim      wpa2-psk clear
0      192.168.34.41
00:1c:bf:04:30:0e DHCP      11-Skim      wpa2-psk clear
0      192.168.34.77
00:1c:bf:25:73:6c DHCP      27-Ihab      wpa2-psk clear
0      192.168.34.54
00:40:96:a9:21:71 DHCP      10-Kaushik   wpa2-psk clear
0      192.168.34.106

```

Station Table(16 entries)

MAC Address	Availability	Client IP	IP Address Type	AP Name
L2 Mode L3 Mode		Authenticated User	Name Tag	
00:02:6f:20:00:00	Online	192.168.10.190	Discovered	#2-2F-Sw-
208 wpa-psk	clear		0	
00:02:6f:20:00:01	Online	192.168.10.191	Discovered	#2-2F-Sw-
208 wpa-psk	clear		0	
00:02:6f:20:00:02	Online	192.168.10.192	Discovered	#2-2F-Sw-
208 wpa-psk	clear			

Station Table(3 entries)

default#

関連コマンド

- [show ap-assigned \(797 ページ\)](#)
- [show dot11 statistics client-traffic \(801 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show dot11 statistics client-traffic

ステーションの統計情報を表示します。

構文

show dot11 statistics client-traffic <ap_MAC_address>

ap_MAC-address ステーションの MAC アドレスを指定して、クライアントトラフィックの統計情報を追加で表示します。

コマンドモード

EXEC

デフォルト

なし

使用例

次のコマンドは、ステーションの統計情報を表示します。

```
controller# show dot11 statistics client-traffic
Station Statistics
```

MAC Address	DHCP Req	AddrChg	VolHandoff	InvHandoff
00:0c:30:be:f7:c0 0		0	1	0
00:0c:85:76:35:ea 0		0	1	0
00:0c:85:e7:bf:20 0		0	4	0
00:20:a6:4c:40:1e 1		1	1	0
00:20:e0:98:10:92 0		1	2	0
00:40:96:40:ab:ae 0		1	4	0
00:40:96:49:40:ff 0		1	1	0
00:40:96:52:27:52 0		1	1	0

controller#

802 ページの表 7 に、**show dot11 statistics client-traffic** で出力されるフィールドの説明を記載します。

表 7: Output for show dot11 statistics client-traffic

フィールド	説明
MAC Address	ステーションの MAC アドレス
DHCP Request Count	フォーティネット WLAN に接続しているときにクライアントが IP アドレスを要求した回数
Address Change Count	クライアント IP アドレスが変更された回数
Voluntary Handoff Count	クライアントの接続を改善するために フォーティネット WLAN が AP アソシエーションを変更した回数
Involuntary Handoff Count	クライアントが異なる BSSID にアソシエーションを初期化した回数

以下のコマンドは、MAC アドレスが 00:0e:35:09:5d:5e であるステーションの統計情報が表示されます。

```
controller# show dot11 statistics client-traffic 00:0e:35:09:5d:5e
```

Station Statistics

```
MAC Address           : 00:0e:35:09:5d:5e
DHCP Request Count    : 1
Address Change Count  : 1
Voluntary Handoff Count : 12
Involuntary Handoff Count : 0
QoS Active Flow Count : 0
QoS Pending Flow Count : 0
SIP Video Reserved Bandwidth : 0
SIP Video Bandwidth   : 0
SIP Video Flow Count  : 0
SIP Audio Reserved Bandwidth : 0
SIP Audio Bandwidth   : 0
SIP Audio Flow Count  : 0
H.323 Video Reserved Bandwidth : 0
H.323 Video Bandwidth   : 0
H.323 Video Flow Count  : 0
H.323 Audio Reserved Bandwidth : 0
```

```
H.323 Audio Bandwidth      : 0
H.323 Audio Flow Count    : 0
SCCP Video Reserved Bandwidth : 0
SCCP Video Bandwidth      : 0
SCCP Video Flow Count     : 0
SCCP Audio Reserved Bandwidth : 0
SCCP Audio Bandwidth      : 0
SCCP Audio Flow Count     : 0
```

関連コマンド

- [show dot11 associations \(799 ページ\)](#)
- [show ap-assigned \(797 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)

show static-station

固定ステーションを表示します。

構文

`show static-station`

コマンドモード

特権 EXEC

デフォルト

なし

用途

ステーションが static-ip アドレスで接続し、アップストリーム パケットを送信しないと、コントローラのデータベースにはステーションの IP アドレス情報が存在しません。そのため、コントローラが、そのステーションにダウンストリーム パケットを送信できません。このような状況を回避するために、static-station コマンドを使用して、ステーションの IP 詳細を手動でコントローラに入力します。このコマンド ([station-aging-out-interval \(844 ページ\)](#)) は、そのようなステーションを表示します。このコマンド (show static-station) は、そのようなステーションを表示します。

使用例

```
namecntrl# configure terminal
namecntrl(config)# static-station 00:10:20:30:40:50
namecntrl(config-static-station)# ip-address 1.1.1.1
namecntrl# sh static-station
MAC Address      Client IP (V4)
00:10:20:30:40:50 1.1.1.1
Static Station Table(1 entry)
```

関連コマンド

[station-aging-out-interval \(844 ページ\)](#)

show station-log-config

ステーションの filelog および syslog の両方のステーション ログ設定を表示します。

構文

show station-log-config

コマンド モード

特権 EXEC

デフォルト

無効

用途

このコマンドを使用して、filelog と syslog の両方のステーション ログ設定を表示します。

使用例

```
ramecntrl# show station-log-config
syslog off
filelog off
ramecntrl# configure terminal
ramecntrl(config)# station-log
ramecntrl(config-station-log)# ?
do                               Executes an IOSCLI command.
end                               Save changes, and return to privileged EXEC mode.
exit                             Save changes, and return to global configuration
mode.
filelog                          Configure the filelog mode for the station log.
syslog                           Configure the syslog mode for the station log.
ramecntrl(config-station-log)# filelog on
ramecntrl(config-station-log)# syslog on
ramecntrl(config-station-log)# exit
ramecntrl(config)# exit
ramecntrl# sh station-log-config
syslog on
filelog on
ramecntrl#
station-log
filelog on
```

syslog on

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)

show station commands

[show station details \(817 ページ\)](#) コマンドは、以前は使用できましたが、現在は、さらにいくつかの show station コマンドが追加されています。

- [show station \(809 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station mac-address \(825 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

Disconnected Stations (切断されたステーション) が **show station all** コマンドの出力に追加されました。異なるバージョンの show station コマンドを使用すると、下表で説明するように異なる出力が表示されます。

確認したい内容	使用するコマンド
MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP、期限前に切断されたステーション	show station
802.11 ステーションの MAC アドレス、APID、AP 名、ESSID、BSSID、RF バンド、TxThx、RxThx、RSSI 損失 %、CH-Util、期限前に切断されたステーション	show station 802.11
すべてのステーション (60 秒前以降にドロップしたものも含む) : MAC アドレス、サービス状態、タイプ APID、AP 名、ESSID、BSSID、RF バンド、クライアント IP、IP タイプ、暗号化パケット、Tx、パケット数、Rx、期限前に切断されたステーション、切断されたステーション数	show station all
MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP	show station details

確認したい内容	使用するコマンド
MAC アドレス、MACFilterCnt、IPDiscCnt、Asso.Cnt SoftHOCnt、PwrSavingTrCnt、KeyExCnt、RadiusAuthCnt、 CPGuestUserCnt、Pkts Tx、Pkts Rx、TxByteCnt、 RxByteCnt、期限前に切断されたステーション	show station counter
MAC アドレス、期待される状態、サービス状態、タイプ、 開始時間、最終更新時、期限前に切断されたステーション	show station general
MAC アドレス、クライアント IP、IP タイプ、VLAN 名 (マッピングされた)、タグ、IGMP グループ、ホーム コントローラ、期限前に切断されたステーション	show station network
MAC アドレス、L2 モード、L3 モード、認証ユーザ名、暗号化、SessionTimeout、InactivityTimeout、フィルタ ID、期限前に切断されたステーション	show station security

show station

すべてのステーションのすべてのデータを表示します。

構文

`show station all`

コマンドモード

特権 EXEC

デフォルト

`show station all` コマンドは、MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP、および切断されたステーションを表示します。

用途

このバージョンのコマンドを使用すると、60 秒前以降にドロップしたものも含め、すべてのステーションの MAC アドレス、サービス状態、タイプ APID、AP 名、ESSID、BSSID、RF バンド、クライアント IP、IP タイプ、暗号化パケット、Tx、Pkts、Rx、切断されたステーションが表示されます。

使用例

```
controller# show station
```

Station Table

MAC Address	IP Type	AP Name	L2 Mode	L3 Mode	Authenticated
User Name	Tag	Client IP			
00:04:23:5a:b3:d0	DHCP	1-201-2F-SW	clear	clear	
0	192.168.10.122				
00:09:5b:c3:9f:32	Discovered	3-208-1F-Mktg	clear	clear	
0	192.168.10.121				
00:0d:93:7e:83:a7	DHCP	2-201-1F-CS	wpa-psk	clear	
0	fe80:0000:0000:0000:020d:93ff:fe7e:83a7				
00:0e:35:09:71:96	DHCP	9-208-2F-BoardR	wpa-psk	clear	
0	192.168.10.157				
00:0e:35:36:f1:f6	Discovered	3-208-1F-Mktg	clear	clear	
0	192.168.10.164				
00:0e:35:7f:1c:04	DHCP	1-201-2F-SW	wpa-psk	clear	
0	192.168.10.117				
00:0e:35:be:d9:dc	Unknown	6-208-2F-Hw-HiG	clear	clear	
0	0.0.0.0				

```

00:0e:9b:6f:4a:c0 DHCP 9-208-2F-BoardR wpa clear merunet\joe
0 192.168.10.101
00:0e:9b:9a:0e:c7 Unknown 3-208-1F-Mktg clear clear
0 0.0.0.0
00:0e:9b:9a:0f:7b DHCP 6-208-2F-Hw-HiG wpa-psk clear
0 192.168.10.115
00:0e:9b:b3:25:b7 DHCP 9-208-2F-BoardR wpa-psk clear
0 192.168.10.125
00:11:24:2c:e0:88 DHCP 2-201-1F-CS wpa-psk clear
0 fe80:0000:0000:0000:0211:24ff:fe2c:e088
00:11:24:96:6d:4b DHCP 2-201-1F-CS clear clear
0 fe80:0000:0000:0000:0211:24ff:fe96:6d4b
00:12:f0:54:a2:56 DHCP 3-208-1F-Mktg wpa-psk clear
0 192.168.10.126
00:12:f0:86:1b:d7 DHCP 1-201-2F-SW clear clear
0 192.168.10.160
00:13:ce:5d:12:31 DHCP 6-208-2F-Hw-HiG wpa clear rjones
0 192.168.10.133
00:14:a4:0a:e5:3e Discovered 2-201-1F-CS wpa-psk clear
0 192.168.10.143
00:40:96:a9:23:f0 DHCP 6-208-2F-Hw-HiG wpa2 clear ksampath
0 192.168.10.120
00:90:96:c5:26:a0 DHCP 2-201-1F-CS clear clear
0 192.168.10.112
Station Table(19 entries)

```

関連コマンド

- [show ap-assigned \(797 ページ\)](#)
- [show dot11 statistics client-traffic \(801 ページ\)](#)
- [show dot11 associations \(799 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show station 802.11

すべてのステーションの 802.11 データを表示します。

構文

`show station 802.11`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このバージョンのコマンドでは、802.11 ステーションの MAC アドレス、APID、AP 名、ESSID、BSSID、RF バンド、TxThx、RxThx、RSSI、損失 %、CH-Util が表示されます。このコマンドと show all コマンドとの違いは、以下の値が追加されるという点です。

- Tx スループット
- Rx スループット
- RSSI
- 損失 %
- CH-Util

使用例

次の例では、コマンドのヘルプを表示し、次に結果を表示します。

```
Master1# show station ?
802.11      Displays 802.11 data of the stations.
all         Displays all data of the stations.
counter     Displays counter data of the stations.
details     Displays station details, including statistics.
general     Displays general data of the stations.
mac-address Displays details of the station with the given MAC
address
s.
network     Displays network data of the stations.
security    Displays security data of the stations.
```

```
Master1# show station 802.11
```

```

MAC Address APID AP Name ESSID BSSID RF Band TxThru RxThru RSSI Loss ChUtl
RxR TxR Retr
00:03:2a:00:6a:0e 103 AP-103-Ha vcellclear 00:0c:e6:9a:5c:1c 802.11b 0 0 -
71 99 0 2 11 0
00:16:6f:b8:a4:61 103 AP-103-Ha vcellclear 00:0c:e6:9a:5c:1c 802.11bg 0 0
-56 0 0 0 0 0
00:16:6f:bb:4a:9c 103 AP-103-Ha vcellwpa2psk 00:0c:e6:9a:8e:ee 802.11bg
236767 7517 -45 0 1 39 45 20
00:16:ea:ed:be:14 103 AP-103-Ha vcellwpa2psk 00:0c:e6:9a:50:85
802.11an3s40 1419 627 -52 9 0 89 398 9
Master1#

```

関連コマンド

- [show ap-assigned \(797 ページ\)](#)
- [show dot11 statistics client-traffic \(801 ページ\)](#)
- [show dot11 associations \(799 ページ\)](#)
- [show station \(809 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show station all

すべてのステーションのすべてのデータを表示します。

構文

`show station all`

コマンドモード

特権 EXEC

デフォルト

`show station all` コマンドは、MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP、および切断されたステーションを表示します。

用途

このバージョンのコマンドを使用すると、60 秒前以降にドロップしたものも含め、すべてのステーションの MAC アドレス、サービス状態、タイプ APID、AP 名、ESSID、BSSID、RF バンド、クライアント IP、IP タイプ、暗号化パケット、Tx、Pkts、Rx、切断されたステーションが表示されます。

使用例

```
Master1# show station ?
802.11          Displays 802.11 data of the stations.
all             Displays all data of the stations.
counter        Displays counter data of the stations.
details        Displays station details, including statistics.
general        Displays general data of the stations.
mac-address    Displays details of the station with the given MAC
address.
network        Displays network data of the stations.
security       Displays security data of the stations.
Master1# show station all
```

```
MAC Address Service State Type APID AP Name ESSID BSSID RF Band Client IP
IP Type Encrypt Pkts Tx
Pkts Rx Dev Type
00:03:2a:00:6a:0e associated sip 103 AP-103-Ha vcellclea 00:0c:e6:9a:5c:1c
802.11b 192.168.148.107 DHCP none 44
44 wireless
```

```
00:16:6f:b8:a4:61 associated data 103 AP-103-Ha vcellclea
00:0c:e6:9a:5c:1c 802.11bg 192.168.148.106 DHCP none 6309
9925 wireless
00:16:6f:bb:4a:9c associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:8e:ee 802.11bg 192.168.108.106 DHCP CCMP 37912
20613 wireless
00:16:ea:ed:be:14 associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.148 Discovered CCMP 18285
9751 wireless
00:16:ea:ed:c1:7c associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.184 DHCP CCMP 518555
2630807 wireless
00:16:ea:ed:c3:12 associated data 103 AP-103-Ha vcellclea
00:0c:e6:9a:cb:17 802.11an3s40 192.168.148.102 Discovered none 14615
14208 wireless
00:16:ea:ed:c7:e6 associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.158 Discovered CCMP 18872
10178 wireless
00:16:ea:ed:cf:7c associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.128 Discovered CCMP 17728
11442 wireless
```

関連コマンド

- [*show station* \(809 ページ\)](#)
- [*show station 802.11* \(811 ページ\)](#)
- [*show station details* \(817 ページ\)](#)
- [*show station general* \(822 ページ\)](#)
- [*show station mac-address* \(825 ページ\)](#)
- [*show station network* \(828 ページ\)](#)
- [*show station security* \(831 ページ\)](#)

show station counter

すべてのステーションまたは指定した 1 つのステーションの診断推論に使用するカウンタデータを表示します。

構文

```
show station counter
show station counter mac-address <MAC address>
```

コマンドモード

特権 EXEC

デフォルト

show station counter mac-address コマンドは、MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP を表示します。

用途

このコマンドを使用して、ステーションの各種カウンタの詳細を表示します。詳細が表示されるカウンタは、MAC Filter ACL Count、IP Discovery Count、Association Count、Soft Handoff Count、Power Saving Transition Count、Key Exchange Count、Radius Authentication Count、Captive Portal Guest User Count、Packets Sent、Packets Received、Transmitted Byte Count、Received Byte Count、QoS Flow Count、Voice Call Count、MAC Filter ACL Fail Count、Radius Authentication Fail Count、Key Exchange Fail Count、Captive Portal Guest User Fail Count、Decrypt Fail Count、WEP Key Index Mismatch Count、MIC Fail Count、Assign Fail Count、Packet Loss Count、Power Save Poll Frames Received Count、SW Encryption Frames Count、SW Decryption Frames Count、LRU Swap Count および Tx Failed Count by Hardware Retry Exceed です。

使用例

```
ramecntrl# sh station counter
```

MAC Address	MacFilter	IPDisc	Asso.	SoftH0	PSTr	KeyEx	RadAuth	CPGuest
Pkts Tx	Pkts Rx	TxByteCnt	RxByteCnt					
00:40:96:ae:20:7a	1	1	1	0	0	1	2	0
154	229	51242	25604					

Station Database Counter Table(1 entry)

```
ramecntrl# sh station counter mac-address 00:40:96:ae:20:7a
```

Station Database Counter Table

MAC Address	: 00:40:96:ae:20:7a
MAC Filter ACL Count	: 1
IP Discovery Count	: 1

Association Count	: 1
Soft Handoff Count	: 0
Power Saving Transition Count	: 0
Key Exchange Count	: 1
Radius Authentication Count	: 2
Captive Portal Guest User Count	: 0
Packets Sent	: 154
Packets Received	: 229
Transmitted Byte Count	: 51242
Received Byte Count	: 25604
QoS Flow Count	: 0
Voice Call Count	: 0
MAC Filter ACL Fail Count	: 0
Radius Authentication Fail Count	: 0
Key Exchange Fail Count	: 0
Captive Portal Guest User Fail Count	: 0
Decrypt Fail Count	: 0
WEP Key Index Mismatch Count	: 0
MIC Fail Count	: 0
Assign Fail Count	: 0
Packet Loss Count	: 53
Power Save Poll Frames Received Count	: 0
SW Encryption Frames Count	: 0
SW Decryption Frames Count	: 0
LRU Swap Count	: 0
Tx Failed Count by Hardware Retry Exceed	: 0
namecntrl#	

関連コマンド

- [show station \(809 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station mac-address \(825 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show station details

すべてのステーションまたは指定した名前に関連付けられているステーションの詳細情報を表示します。このコマンドは、以前のリリースでもすでに使用されていま した。

構文

```
show station details ip-address <IP address>
show station details mac-address <MAC address>
show station details user <user>
```

コマンド
モード

特権 EXEC

デフォルト

なし

用途

show station details コマンドを使用して、IP アドレス、MAC アドレス、またはユーザに関連付けられているステーションのリストを表示します。

表 8: show station details コマンドの出力

フィールド	説明
MAC Address	ステーションの MAC アドレス
IP Type	ステーションの IP アドレスを割り当てる方法 Static IP address assigned: ステーションは固定 IP アドレスを使用します。IPv6 IP アドレスが表示されます。 Dynamic IP address assigned: ステーションは、送信されるトラフィックにより認識される固定 IP アドレスを使用します。 DHCP: ステーションは、DHCP により割り当てられる IP アドレスを使用します。
AP Name	アクセス ポイントの名前
L2 Mode	使用されるレイヤ 2 認証
L3 Mode	使用されるレイヤ 3 認証

表 8: show station details コマンドの出力

フィールド	説明
Authenticated User Name	ステーションに関連付けられている認証ユーザの名前 (使用されている場合)
Tag	ステーションに関連付けられている VLAN タグ (存在する場合)
Client IP	ステーションに割り当てられている IP アドレス。通常の 4 タブルの IP アドレスではなく、fe80:0000:0000:020d:93ff:fe7e:83a7 という形式の IP v 6 アドレスが表示されます。

show station コマンドでキーワードを使用すると、追加の情報と統計情報が表示されます。

mac-address というキーワードとステーションの MAC アドレスを使用すると、特定のステーションの情報が表示されます。この場合には、以下の情報が追加されます。

フィールド	説明
DHCP Req	コントローラがモバイル クライアントから DHCP 要求を受け取るたびに、このカウンタが加算されます。
AddrChg	モバイル クライアントの IP が A から B に変わったことをコントローラが認識するたびに、このカウンタが加算されます。
VolHandoff	コントローラがソフト ハンドオフを実行するたびに、このカウンタが加算されます。 Topology-updated が有効である必要があります。
InvHandoff	モバイル クライアントがハード ハンドオフを実行するたびに、このカウンタが加算されます。 Topology-updated が有効である必要があります。

次のような状況では、IP アドレスが 0.0.0.0 と表示されることがあります。

- 固定 IP アドレスのクライアント : アクセス ポイントにクライアントが関連付けられた後ではあるものの、クライアントが最初のパケットを送信する前の状態。最初のパケッ

トが送信された後は、クライアントの IP アドレスとアドレス タイプが、`show station` コマンドの出力に表示されます。

- DHCP によって IP アドレスが割り当てられるクライアント：クライアントが DHCP 要求を送信した後ではあるものの、DHCP サーバが応答する前の状態。DHCP サーバが応答した後は、クライアントの IP アドレスとアドレス タイプが、`show station` コマンドの出力に表示されます。

`details ip-address`、`details user`、および `mac-address` キーワードを使用すると、ステーション テーブルにあるステーションの詳細情報とステーションの統計情報が表示されます。

ステーションが 30 分間アクティブでない状態が続くと、WLAN から切断されます。

使用例

以下のコマンドを指定すると、対応するステーションの情報が表示されます。

```
controller# show station details mac-address 00:20:a6:4e:b5:9c
```

Station Table

MAC Address	IP Type	AP Name	L2 Mode	L3 Mode	Authenticated
User Name	Tag	Client IP			

00:40:96:a9:21:71	DHCP	10-Kaushik	wpa2-psk	clear	
0	192.168.34.106				

Station Statistics

MAC Address	DHCP Req	AddrChg	VolHandoff	InvHandoff
00:40:96:a9:21:71 0		0	1306	0

Assigned AP Table for MAC address 00:40:96:a9:21:71

AP ID	Client MAC	Type	SSID	State
Encrypt	Pkts Rx	Pkts Tx	Last	AP Name
Prev	Curr	RF Band		
10	00:40:96:a9:21:71	STATION	corp-wpa2psk	ASSOCIATED
CCMP	248810	111399	00d:00h:00m:05s	-71 -66 802.11abg 10-Kaushik

There are no QoS flows for MAC address 00:40:96:a9:21:71 (IP: 192.168.34.106)

Station Table

MAC Address	Availability	Client IP	IP Address	Type	AP Name
L2 Mode	L3 Mode	Authenticated User	Name	Tag	
00:20:a6:4e:b5:9c	Online	192.168.10.140	DHCP		#8-1F-
DemoArea-	wpa-psk	clear		0	

Station Statistics

MAC Address	DHCP Req	AddrChg	VolHandoff	InvHandoff
00:20:a6:4e:b5:9c	0	0	4	0

Assigned AP Table for MAC address 00:20:a6:4e:b5:9c

AP ID	Client MAC	Type	SSID	State	Encrypt	Pkts Rx	Pkts Tx	Last
Prev	Curr	RF Band	AP Name					
8	00:20:a6:4e:b5:9c	STATION	mwrf-wpapsk					ASSOCIATED
TKIP	4377	4566	00d:00h:00m:00s	205	204	802.11g	#8-1F-	
DemoArea-								

There are no QoS flows for MAC address 00:20:a6:4e:b5:9c (IP: 192.168.10.140)

関連コマンド

- [show station \(809 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station mac-address \(825 ページ\)](#)

- [show station network](#) (828 ページ)
- [show station security](#) (831 ページ)

show station general

すべてのステーション、または指定したステーションの一般データを表示します。

構文

```
show station general
show station general ip-address <IP address>
show station general mac-address <MAC address>
show station general user <username>
```

コマンド モード

特権 EXEC

デフォルト

show station コマンドは、MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP を表示します。

用途

このコマンドを使用して、ステーションの一般情報を表示します。

使用例

```
Master1# show station general
```

MAC Address Last Update time	Expected State	Service State	Type	Start time
00:03:2a:00:d7:c0 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:03:2a:00:e4:3f 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:11:24:92:40:4d 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:11:95:c2:29:1e 06:04:59 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:13:e8:06:cd:6b 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:16:6f:b8:d5:15 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:16:ea:88:1c:84 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009
00:17:9a:50:d8:23 06:03:52 06/16/2009 06:30:23	unknown	associated	data	06/16/2009

00:19:5b:03:44:93 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:19:7e:91:0a:7f unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:19:7e:91:0a:89 unknown	associated	data 06/16/2009
06:08:08 06/16/2009 06:30:23		
00:1a:c1:35:84:36 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1a:c1:35:86:96 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:2f:c5:a5:1e unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:2f:d0:5b:8c unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:2f:d0:5b:90 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:77:9a:61:4a unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1c:f0:9d:e3:fe unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1c:f0:9d:e4:0d unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1d:7e:0a:94:9c unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1f:e2:d8:39:92 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:20:a6:4e:c3:1b unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:00:41:50:ce unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:00:d7:f1:b6 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:00:d7:f2:b2 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:5c:08:ec:c7 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:5d:45:fa:12 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:22:68:a0:f0:3b unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
0:40:96:b4:12:c2 unknown	associated	data 06/16/2009 6:03:52
06/16/2009 06:30:23		

Station Database General Table(29 entries)

Master1#

関連コマンド

- [show station \(809 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station mac-address \(825 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show station mac-address

指定した MAC アドレスのステーションのすべてのデータを表示します。

構文

`show station <MAC address>`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドのバージョンは、この MAC アドレスのステーションのみを表示します。

使用例

```
Master1# show station ?
802.11          Displays 802.11 data of the stations.
all             Displays all data of the stations.
counter         Displays counter data of the stations.
details         Displays station details, including statistics.
general         Displays general data of the stations.
mac-address     Displays details of the station with the given MAC
address.
network         Displays network data of the stations.
security        Displays security data of the stations.
controller# show station mac-address 00:20:a6:4e:b5:9c
Station Table

MAC Address           : 00:20:a6:4e:b5:9c
IP Address Type       : DHCP
AP ID                 : 10
AP Name               : 10-Kaushik
L2 Security State     : wpa2-psk
L3 Security State     : clear
Authenticated User Name :
VLAN Name             :
```

Tag	: 0
RF Band	: unknown
Client IP	: 192.168.34.106
Availability Status	: Online
Description	:
Client IP	: 192.168.10.140
IP Address Type	: DHCP
AP ID	: 8
AP Name	: #8-1F-DemoArea-201
L2 Security State	: wpa-psk
L3 Security State	: clear
Authenticated User Name	:
VLAN Name	:
Tag	: 0
RF Band	: 802.11g

関連コマンド

- [show station \(809 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station mac-address \(825 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show station multiple-ip

1 つの MAC の複数の IP アドレスを使用するすべてのステーションを表示します。

構文

`show station multiple-ip`

コマンド モード

特権 EXEC

デフォルト

なし

用途

単一アダプタの仮想環境で実行中のステーションに使用されている IP アドレスを確認する場合は、このコマンドを使用します。

使用例

```
Master1# show station ?
802.11          Displays 802.11 data of the stations.
all             Displays all data of the stations.
counter         Displays counter data of the stations.
details         Displays station details, including statistics.
general         Displays general data of the stations.
mac-address    Displays details of the station with the given MAC
address.
multiple-ip     Displays multiple ip addresses of the stations.
network        Displays network data of the stations.
security       Displays security data of the stations.
```

show station network

すべてのステーション、または指定したステーションのネットワーク データを表示します。

構文

```
show station network
show station network ip-address <IP address>
show station network mac-address <MAC address>
show station network user <username>
```

コマンドモード

特権 EXEC

デフォルト

show station コマンドは、MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP を表示します。

用途

このコマンドを使用して、ステーション ネットワーク情報を表示します。

使用例

次の例は、ステーション ネットワークを表示します。

```
Master1# show station network
```

MAC Address Groups	Client IP Home Controller	IP Type	VLAN Name	Tag	IGMP
00:03:2a:00:d7:c0 0	192.168.106.139	DHCP	106	106	0
00:03:2a:00:e4:3f 0	192.168.106.140	DHCP	106	106	0
00:11:24:92:40:4d 0	192.168.106.137	DHCP	106	106	0
00:11:95:c2:29:1e 0	192.168.106.141	DHCP	106	106	0
00:13:e8:06:cd:6b 0	192.168.108.104	DHCP	108	108	0
00:16:6f:b8:d5:15 0	192.168.108.106	DHCP	108	108	0
00:16:ea:88:1c:84 0	192.168.108.116	DHCP	108	108	0
00:17:9a:50:d8:23 0	192.168.106.179	DHCP	106	106	0

00:19:5b:03:44:93	192.168.106.174	Discovered	106	106	0
00:19:7e:91:0a:7f	0.0.0.0	Unknown		0	0
00:19:7e:91:0a:89	192.168.108.108	DHCP	108	108	0
00:1a:c1:35:84:36	192.168.103.102	DHCP	VLAN103	103	0
00:1a:c1:35:86:96	192.168.103.100	DHCP	VLAN103	103	0
00:1b:2f:c5:a5:1e	192.168.106.181	DHCP	106	106	0
00:1b:2f:d0:5b:8c	192.168.77.100	Discovered		4096	0
00:1b:2f:d0:5b:90	192.168.108.123	DHCP	108	108	0
00:1b:77:9a:61:4a	0.0.0.0	Unknown	VLAN103	103	0
00:1c:f0:9d:e3:fe	192.168.103.104	DHCP	VLAN103	103	0
00:1c:f0:9d:e4:0d	10.101.66.6	DHCP		0	0
00:1d:7e:0a:94:9c	192.168.108.107	DHCP	108	108	0
00:1f:e2:d8:39:92	192.168.108.115	DHCP	108	108	0
00:20:a6:4e:c3:1b	192.168.106.195	DHCP	106	106	0
00:21:00:41:50:ce	192.168.108.103	Discovered	108	108	0
00:21:00:d7:f1:b6	192.168.106.123	Discovered	106	106	0
00:21:00:d7:f2:b2	0.0.0.0	Unknown		0	0
00:21:5c:08:ec:c7	0.0.0.0	Unknown	VLAN103	103	0
00:21:5d:45:fa:12	10.101.66.2	Discovered		0	0
00:22:68:a0:f0:3b	192.168.108.109	DHCP	108	108	0
0:40:96:b4:12:c2	192.168.108.105	DHCP	108	108	0

Station Database Network Table(29 entries)

関連コマンド

- [show ap-assigned](#) (797 ページ)
- [show dot11 statistics client-traffic](#) (801 ページ)
- [show station 802.11](#) (811 ページ)
- [show station all](#) (813 ページ)
- [show station details](#) (817 ページ)
- [show station counter](#) (815 ページ)
- [show station general](#) (822 ページ)
- [show station security](#) (831 ページ)

show station security

すべてのステーション、または指定したステーションのセキュリティ データを表示 します。

構文

```
show station security
show station security ip-address <IP address>
show station security mac-address <MAC address>
show station security user <username>
```

コマンドモード

特権 EXEC モード

デフォルト

show station コマンドは、MAC アドレス、IP タイプ、APID AP 名、L2 モード、L3 モード、認証されたユーザ名、タグ、RF バンド、クライアント IP を表示します。

用途

使用例

```
Master1# show station security
```

MAC Address	L2 Mode	L3 Mode	Auth.User Name
Encrypt SessionTimeout	InactivityTimeout	Filter ID	
00:03:2a:00:d7:c0	clear	clear	none
0	0		
00:03:2a:00:e4:3f	clear	clear	none
0	0		
00:11:24:92:40:4d	clear	clear	none
0	0		
00:11:95:c2:29:1e	clear	clear	none
0	0		
00:13:e8:06:cd:6b	wpa2-psk	clear	CCMP
0	0		
00:16:6f:b8:d5:15	wpa2-psk	clear	CCMP
0	0		
00:16:ea:88:1c:84	wpa2-psk	clear	CCMP
0	0		
00:17:9a:50:d8:23	clear	clear	none
0	0		

00:19:5b:03:44:93	clear	clear	none
0	0		
00:19:7e:91:0a:7f	wpa2-psk	clear	CCMP
0	0		
00:19:7e:91:0a:89	wpa2-psk	clear	CCMP
0	0		
00:1a:c1:35:84:36	wep	clear	WEP
0	0		
00:1a:c1:35:86:96	wep	clear	WEP
0	0		
00:1b:2f:c5:a5:1e	clear	clear	none
0	0		
00:1b:2f:d0:5b:8c	wpa2	clear	CCMP
0	0		
00:1b:2f:d0:5b:90	wpa2-psk	clear	CCMP
0	0		
00:1b:77:9a:61:4a	wep	clear	WEP
0	0		
00:1c:f0:9d:e3:fe	wpa-psk	clear	TKIP
0	0		
00:1c:f0:9d:e4:0d	wpa-psk	clear	TKIP
0	0		
00:1d:7e:0a:94:9c	wpa2-psk	clear	CCMP
0	0		
00:1f:e2:d8:39:92	wpa2-psk	clear	CCMP
0	0		
00:20:a6:4e:c3:1b	clear	clear	none
0	0		
00:21:00:41:50:ce	wpa2-psk	clear	CCMP
0	0		
00:21:00:d7:f1:b6	clear	clear	none
0	0		
00:21:00:d7:f2:b2	wpa-psk-in-progress	clear	
none	0	0	
00:21:5c:08:ec:c7	wep	clear	WEP
0	0		
00:21:5d:45:fa:12	wpa-psk	clear	TKIP
0	0		
00:22:68:a0:f0:3b	wpa2-psk-in-progress	clear	
CCMP	0	0	
00:40:96:b4:12:c2	wpa2-psk	clear	CCMP
0	0		

Station Database General Table(29 entries)

関連コマンド

- [show ap-assigned](#) (797 ページ)
- [show dot11 statistics client-traffic](#) (801 ページ)
- [show station 802.11](#) (811 ページ)
- [show station all](#) (813 ページ)
- [show station details](#) (817 ページ)
- [show station counter](#) (815 ページ)
- [show station general](#) (822 ページ)
- [show station network](#) (828 ページ)

show statistics station-per-ap

アクセス ポイントごとのステーション統計を表示します。

構文 `show statistics station-per-ap <ap-id>`

コマンド
モード EXEC

デフォルト なし

用途 `show statistics station-per-ap` コマンドを使用して、アクセス ポイントごとのステーション統計を表示します。デフォルトでは、すべてのアクセス ポイントのすべてのステーション統計が表示されます。1 つのアクセス ポイントのステーション統計を表示するには、コマンドの実行時にそのアクセス ポイントの ID 番号を指定します。

使用例 以下の短縮形のコマンドを指定すると、すべてのアクセス ポイントのステーション統計が表示されます。

```
controller# show statistics station-per-ap
AP  AP-Name  If  Station-MAC      Station-IP      SSID      Rx-
packets  Tx-packets  WEP-errorsEncryptionErr

2    #2-2F-Sw- 2    00:02:6f:20:00:33  0.0.0.0      mwf-wpapsk
1138      1134      0

2    #2-2F-Sw- 2    00:02:6f:20:00:32  0.0.0.0      mwf-wpapsk      996
988      0

2    #2-2F-Sw- 2    00:02:6f:20:00:31  0.0.0.0      mwf-wpapsk
1142      1132      0

controller#
```

表 9: `show statistic station-per-ap` の出力

フィールド	説明
AP	ステーションが現在通信しているアクセス ポイントの固有の ID 番号
AP-Name	ステーションが現在通信しているアクセス ポイントの名前
If	AP インターフェイス番号
Station-MAC	ステーションの MAC アドレス
Station-IP	ステーションの IP アドレス
SSID	ステーションに関連付けられている ESSID
Rx-packets	アクセス ポイントがステーションから受信した総パケット数
Tx-packets	アクセス ポイントからステーションに転送した総パケット数
WEP-errorsEncryptionErr	1 分間に発生した暗号化エラーの数。暗号化エラーは、ステーションがセッション開始時またはキー変更時に 802.1x プロトコルを正常に実行しなかった場合に発生する可能性が最も高くなります。

関連コマンド

- [show ap-assigned \(797 ページ\)](#)
- [show dot11 statistics client-traffic \(801 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

show statistics top10-station-problem

1 分間の WEP エラー数 (最小でも 10 個の WEP エラー) が最も多い上位 10 のステーションを表示します。

構文

`show statistics top10-station-problem`

コマンドモード

特権 EXEC

デフォルト

なし

用途

`show statistics top10-station-problem` コマンドを使用して、1 分間の WEP エラー数 (最小でも 10 個の WEP エラー) が最も多い上位 10 のステーションを表示します。WEP エラーは、ステーションがセッション開始時またはキー変更時に 802.1x プロトコルを正常に実行しなかった場合に発生する可能性が最も高くなります。

使用例

以下のコマンドを指定すると、1 分間の WEP エラー数 (最小でも 10 個の WEP エラー) が最も多い上位 10 のステーションが表示されます。

```
controller# show statistics top10-station-problem
```

AP	AP Name	If	Station MAC	Station IP	WEP Errors/min
11	11-Skim	1	00:1b:77:95:ab:81	0.0.0.0	105588
11	11-Skim	1	00:18:de:bd:d0:04	192.168.34.43	69757
1	1-ops-Ksh	1	00:1b:77:8d:75:13	192.168.34.103	58694
11	11-Skim	1	00:1c:bf:04:30:0e	192.168.34.77	51486
10	10-Kaushi	1	00:1b:77:50:b1:2a	0.0.0.0	33294
10	10-Kaushi	1	00:1c:bf:ae:4b:01	0.0.0.0	25154
29	29-Keith	1	00:1b:77:95:a9:94	192.168.34.44	18897
1	1-ops-Ksh	1	00:13:02:28:f4:9a	0.0.0.0	14929
11	11-Skim	1	00:1b:77:95:94:79	192.168.34.59	8140
9	9-Exit-St	1	00:13:02:88:6a:e2	0.0.0.0	7304

Top 10 station problem statistics(10)

837 ページの表 10 に、**show statistics top10-station-problem** コマンドのフィールドの説明を記載します。

表 10: *show statistics top10-station-problem* の出力

フィールド	説明
AP	アクセス ポイントの固有の ID 番号
AP Name	ステーションが関連付けられているアクセス ポイントの名前
If	AP のインターフェイス番号
Station MAC	ステーションの MAC アドレス
Station IP	ステーションの IP アドレス
WEP Errors/Minute	直前の 1 分間に発生した WEP エラーの累計数

I

関連コマンド [show statistics top10-station-talker \(838 ページ\)](#)

show statistics top10-station-talker

直近のポーリング期間の毎分の送受信パケット率の合計に基づく、上位 10 のアクティブなステーションを表示します。

構文 `show statistics top10-station-talker`

コマンド
モード 特権 EXEC

デフォルト なし

用途 `show statistics top10-station-talker` コマンドを使用して、最後にリセットしてから最後にポーリングを行ったときまでの間に検出された 1 分間の送信/受信パケット数の合計を基準に最もアクティブであると判断された 10 のステーションを表示します。アクティブなステーションのテーブルには、実際に送受信されたバイト数や通信時間ではなく、毎秒のフレーム数に基づくアクティビティが表示されます。

使用例 以下のコマンドを指定すると、最もアクティブなステーションが表示されます。

controller# `show statistics top10-station-talker`

AP	AP Name	If	Station MAC	Station IP	Rx Packets/min	Tx Packets/min
10	#10-1F-Mk	1	00:0e:35:09:5d:5e	192.168.10.125	370	400
8	#8-1F-Dem	1	00:05:4e:40:6f:46	192.168.10.141	357	347
6	#6-1F-CS-	1	00:0e:35:5f:f0:29	0.0.0.0	359	328
10	#10-1F-Mk	1	00:12:f0:0f:23:cd	0.0.0.0	259	304
10	#10-1F-Mk	1	00:0e:35:5f:f0:29	0.0.0.0	300	244
10	#10-1F-Mk	2	00:09:5b:a3:c2:fd	192.168.10.130	246	237
2	#2-2F-Sw-	2	00:02:6f:20:00:16	0.0.0.0	227	227
2	#2-2F-Sw-	2	00:02:6f:20:00:33	0.0.0.0	227	226
2	#2-2F-Sw-	2	00:02:6f:20:00:31	0.0.0.0	228	226
2	#2-2F-Sw-	2	00:02:6f:20:00:3a	0.0.0.0	227	226
Top 10 station talker statistics request(10)						
controller#						

839 ページの表 11 に、`show statistics top10-station-talker` の出力のフィールドの説明を記 載します。

表 11: `show statistics top10-station-talker` の出力

フィールド	説明
AP	アクセス ポイントの固有の ID 番号
AP Name	ステーションが現在通信しているアクセス ポイントの名前
If	AP のインターフェイス番号
Station MAC	ステーションの MAC アドレス
Station IP	ステーションの IP アドレス
Rx Packets/min	最後のリセットから最後のポーリングを行ったときまでに受信した パケット数
Tx packets/min	最後のリセットから最後のポーリングを行ったときまでに送信した パケット数

関連コマンド [show statistics top10-station-problem \(836 ページ\)](#)

show topostaap

システム内のステーション /AP エッジ レコードを表示します。

構文

show topostaap

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドは、システム内のステーション /AP エッジ レコードを表示します。

使用例

controller# **show topostaap**

Station MAC Address	AP ID	AP Name	Assigned	RSSI
00:0d:93:82:da:b3	1	AP-1	on	36
00:40:96:40:fa:eb	1	AP-1	on	28
00:40:96:51:c6:40	1	AP-1	on	0

関連コマンド

show topostation

アクセス ポイントに現在割り当てられているステーションの情報を表示します。

構文 show topostation

コマンド
モード 特権 EXEC

デフォルト なし

用途 show topostation コマンドを使用して、アクセス ポイントに現在割り当てられているステーションの情報を表示します (ステーションの観点から)。FortiWLC (SD) の一部であるステーションだけが表示されます。show ap-discovered コマンドを使用すると、それ以外のステーションが表示されます。

使用例 次のコマンドは、FortiWLC (SD) の一部であるステーションを表示します。

```
controller# show topostation
MAC Address      AP  AP Name      Last Handoff Time      State
BSSID            MSSID
00:12:f0:54:a2:56 11  11-Skim      2008/03/12 11:50:21    ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:83:27:3f 11  11-Skim      2008/03/12 11:29:53    ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:dd:17:57 8   8-Saro       2008/03/12 10:41:53    ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00

      Stations Topology(3 entries)
MAC Address      AP  AP Name      Last Handoff Time      State
BSSID            MSSID

00:12:f0:54:a2:56 11  11-Skim      2008/03/12 11:50:21    ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:83:27:3f 11  11-Skim      2008/03/12 11:29:53    ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:dd:17:57 8   8-Saro       2008/03/12 10:41:53    ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00

      Stations Topology(3 entries)
Last Handoff Time      State      MAC Address      AP  AP Name      BSSID
```

```
00:02:c7:34:48:90 8 #8-1F-DemoArea- 2005/08/09 08:47:19 ASSOCIATED
00:0c:e6:02:07:2f
00:03:2a:00:6a:80 3 #3-2F-Exec-201 2005/08/09 14:59:04 ASSOCIATED
00:0c:e6:44:08:eb
00:03:2a:00:6b:a6 8 #8-1F-DemoArea- 2005/08/09 15:48:26 ASSOCIATED
00:0c:e6:44:08:eb

Stations Topology(3 entries)
controller#
```

関連コマンド

- [show ap-discovered \(634 ページ\)](#)
- [show ap-assigned \(797 ページ\)](#)
- [show dot11 statistics client-traffic \(801 ページ\)](#)
- [show station 802.11 \(811 ページ\)](#)
- [show station all \(813 ページ\)](#)
- [show station details \(817 ページ\)](#)
- [show station counter \(815 ページ\)](#)
- [show station general \(822 ページ\)](#)
- [show station network \(828 ページ\)](#)
- [show station security \(831 ページ\)](#)

static-station

DHCP を使用できないステーションに固定 IP を設定します。

構文

```
static-station MAC_address  
    ip_address ip_address  
no static-station MAC_address
```

コマンド モード

グローバル設定モード

デフォルト

なし

用途

このコマンドを使用して、DHCP を使用できないためにアップストリーム パケットを転送しないステーションに固定 IP を設定します。これらのクライアントは、自動的に IP を認識して MAC アドレス マッピングをすることができません。このコマンドを使用すると、IP を手動で作成し、MAC マッピングすることができます。

ステーションの MAC アドレスを入力すると、config-static-station サブモードに入り、ここで ip-address コマンドを使用できます。

このコマンドの no フォームを使用すると、ステーションの IP アドレス マッピングから MAC アドレスが削除されます。

使用例

ここでは、IP アドレス 172.172.172.10 が MAC アドレス 00:00:04:23:55:15 のステーションに割り当てられます。

```
controller (config)# static-station 00:00:04:23:55:15  
controller(config-static-station)# ip-address 172.172.172.10
```

固定のステーション割り当てを削除するには、次の例のようにコマンドを使用します。

```
controller (config)# no static-station 00:00:04:23:55:15
```

station-aging-out-interval

ステーションがシステムから離れた後に、そのステーションのエントリを E(z)RF Network Manager のステーション テーブルに残しておく期間を設定します。

構文

`station-aging-out-interval <minutes>`

コマンドモード

グローバル設定モード

デフォルト

デフォルト値は 0 で、wncreg がエントリを削除するとすぐに、カウンタのそのステーションのエントリが削除されることを意味します。

用途

このコマンドは、リリース 3.6.1 で導入され、基本的には、(802.11、all、counter、details、general、network、security) といったステーション カウンタを表示するために使用されます。デフォルト値は 0 で、wncreg がエントリを削除するとすぐに、カウンタのそのステーションのエントリが削除されることを意味します。**station-aging -out-interval** ステーションがシステムから離れた後に、そのステーションのエントリを E(z)RF Network Manager のステーション テーブルに残しておく期間を設定します。このパラメータが存在する理由は、**show station** コマンドの出力には、デバッグやその他の目的に利用できる情報が含まれているためです。リリース 3.6.1 より前では、ステーションがシステムから離れるとすぐにそのステーションのエントリが削除されていました。そのため、ステーションがシステムから離れた後に問題が報告されても、そのステーションの問題をデバッグする手段がほとんどありませんでした。1 ~ 65535 の分数を指定します。0 (ゼロ) に設定すると、wncreg がエントリを削除するとすぐに、カウンタのそのステーションのエントリが削除されます。このゼロのデフォルト値は、このパラメータが存在しなかった、以前の FortiWLC (SD) バージョンで使用されていた設定と同じです。

この値は、" 分 " を表すため、値を 60 に設定すると、ステーションがネットワークから離れた後も 60 分間はステーションのカウンタの詳細 (すべてのカウンタ) が wncagent によって保持されることになります。このタイマーを、1 ~ 65535 の任意の値を設定します。**show controller** コマンドの出力には、ステーションがシステムを離れてからの時間が表示されません。

使用例

次の例は、ステーションがシステムから離れてからの時間を 60 に設定し、その設定を **show controller** コマンドで確認します。

```
InteropLab(config)# station-aging-out-interval ?
```

```

<0-65535>          Enter the station aging out interval(minute) between
1 and 65535, or 0 to disable.
InteropLab(config)# station-aging-out-interval 60
InteropLab(config)# exit
InteropLab # sh controller
Global Controller Parameters
Controller ID                : 1
Description                  : controller
Host Name                    : Engg-wifi-Main
Uptime                      : 01d:10h:44m:23s
Location                    :
Contact                     :
Operational State           : Enabled
Availability Status         : Online
Alarm State                 : Critical
Automatic AP Upgrade        : off
Virtual IP Address          : 10.101.64.100
Virtual Netmask             : 255.255.192.0
Default Gateway             : 10.101.64.1
DHCP Server                 : 192.168.101.250
Statistics Polling Period (seconds)/0 disable Polling : 60
Audit Polling Period (seconds)/0 disable Polling      : 60
Software Version            : 4.0-38
Network Device Id          : 00:00:50:51:e6:cc
System Id                   : DC89C8D202DA
Default AP Init Script      :
DHCP Relay Passthrough      : on
Controller Model            : MC5000
Country Setting             : United States Of
America
Manufacturing Serial #      : N/A
Management by wireless stations : on
Controller Index            : 10
Topology Information Update  : on
AeroScout Enable/Disable    : disable
FastPath Mode               : on
Bonding Mode                : dual

```

DFS	: disable
Station Aging Out Period(minutes)	: 60
Roaming Domain State	: disable

station-log

802.11 接続のデバッグ メッセージを有効にします。

構文

`station-log <station MAC address>`

コマンド モード

グローバル設定モード

デフォルト

なし

用途

このコマンドを使用して、指定したステーションの、802.11 Probe、Auth、Assoc、Deauth、Disassoc などの情報を収集します。

使用例

```
default# station-log ?
<CR>
<station_mac>          Specific station MAC you want to view.
show                    Display station log events.
default# station-log
Interactive Per-Station Event Logging Shell (enter "help" for help)
station-log> ?

Interactive Event Logging Shell Usage:
help, ?                This help message
exit, quit             Exit/Quit

station show           Show stations in the filter list
station add <AA:BB:CC:DD:EE:FF>
MAC                   Add a station to the filter list by
MAC
station del <AA:BB:CC:DD:EE:FF>
by MAC                Delete a station from the filter list
by MAC
station del <#>
by index              Delete a station from the filter list
by index
station del all
list                  Delete all stations from the filter
list
event show            Show the event filter list
```

```
event <event> <dispcnd>
<event>
```

Set the display condition for event

<event> may be: #ID of event, or "all"

<dispcnd> may be: "all" (!), "none"

(x) or "list" (?)

```
station-log> station show
```

The station filter list is empty!

```
station-log> event show ?
```

Event Filters

=====

Disp	ID#	Name
------	-----	------

?	1	IP Address Discovered
?	2	DHCP
?	3	Station Assign
?	4	802.11 State
?	5	CP User Authentication
?	6	1X Authentication
?	7	Encryption
?	8	Mac Filtering

```
station-log> event show all
```

Event Filters

=====

Disp	ID#	Name
------	-----	------

?	1	IP Address Discovered
?	2	DHCP
?	3	Station Assign
?	4	802.11 State
?	5	CP User Authentication
?	6	1X Authentication
?	7	Encryption
?	8	Mac Filtering

```
station-log> event all !
```

```
station-log> event show
```

```

Event Filters
=====
Disp | ID# | Name
-----
! | 1 | IP Address Discovered
! | 2 | DHCP
! | 3 | Station Assign
! | 4 | 802.11 State
! | 5 | CP User Authentication
! | 6 | 1X Authentication
! | 7 | Encryption
! | 8 | Mac Filtering
station-log> station add 00:40:96:AA:BB:CC
Added station 00:40:96:aa:bb:cc at position 0
station-log> station show
Station Filter List
=====
Index | MAC Address
-----
0 | 00:40:96:aa:bb:cc
station-log> station del all
The station filter list has been cleared
station-log>

```

関連コマンド

- [\(station-log\) filelog \(851 ページ\)](#)
- [station-log show \(859 ページ\)](#)

(station-log) enable

ステーションのログを有効にします。

構文

```
station-log> enable
station-log> disable
```

コマンド モード

ステーション ログ

デフォルト

オフ

用途

デフォルトでは、ステーション ログは無効です。このコマンドを使用して有効にします。

使用例

次のコマンドは、ステーション ログ モードに入り、ファイル ログをオンにします。

```
Meru01#configure terminal
Meru01(config)# station-log
Meru01(config-station-log)# enable
Meru01(config-station-log)# end
```

関連コマンド

- [station-log \(847 ページ\)](#)
- [station-log show \(859 ページ\)](#)

(station-log) filelog

システム ファイルへの推論イベント ログを有効にします。

構文

```
station-log> filelog on  
station-log> filelog off
```

コマンド モード

ステーション ログ

デフォルト

オフ

用途

推論イベントをログしない場合は、このコマンドを使用してオフにします。このログをオフにしても、オンになっている場合と比較してパフォーマンスにそれほど大きな差はありません。

使用例

次のコマンドは、ステーション ログ モードに入り、ファイル ログをオンにします。

```
Meru01#configure terminal  
Meru01(config)# station-log  
Meru01(config-station-log)# filelog on  
Meru01(config-station-log)# end  
Meru01# sh station-log-config  
syslog off  
filelog on
```

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) syslog \(852 ページ\)](#)
- [station-log show \(859 ページ\)](#)

(station-log) syslog

システム ファイルへのログを有効にします。

構文

```
station-log> syslog on  
station-log> syslog off
```

コマンド モード

ステーション ログ

デフォルト

オフ

用途

推論イベントをログしない場合は、このコマンドを使用してオフにします。このログをオフにしても、オンになっている場合と比較してパフォーマンスにそれほど大きな差はありません。

使用例

次のコマンドは、ステーション ログ モードに入り、ファイル ログをオンにします。

```
Meru01#configure terminal  
Meru01(config)# station-log  
Meru01(config-station-log)# syslog on  
Meru01(config-station-log)# end  
Meru01# sh station-log-config  
syslog on  
filelog on
```

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)
- [station-log show \(859 ページ\)](#)

(station-log) event id

イベント タイプごとのログを有効または無効にします。

構文

```
station-log> event id show
station-log> event id set <event-id>
station-log> event id remove <event-id>
```

コマンド モード

ステーション ログ

デフォルト

無効

用途

デフォルトでは、station-log によって、下記に示すすべてのイベントが表示され、ログされます。現在有効であるイベントを表示するには、**event id show** コマンドを使用します。

特定のイベント フィルタを有効にするには、**event id set <id>** コマンドを使用して、**event id show** コマンドで表示される該当する ID 番号を指定します。指定したイベントはフィルタされ、したがって、正常として表示され、ログされるようになります。

特定のイベント フィルタを無効にするには、**event id remove <id>** コマンドを使用して、**event id show** コマンドで表示される該当する ID 番号を指定します。フィルタは無効になり、イベント情報は表示されなくなります。



すべてのイベントのフィルタを有効または無効にするには、id フィールドに all と入力します (event id set all)。

使用例

```
station-log> event id show
```

Event ID Filters

=====

Enabled	ID#	Name
---------	-----	------

Yes	1	IP Address Discovered
Yes	2	DHCP
Yes	3	Station Assign

Yes		4		802.11 State
Yes		5		CP User Authentication
Yes		6		1X Authentication
Yes		7		Encryption
Yes		8		Mac Filtering
Yes		9		Diagnostics
Yes		10		Band Steering
Yes		11		SIP

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)
- [station-log show \(859 ページ\)](#)

(station-log) event severity

イベント タイプの重大度を指定します。

構文

```
station-log> event severity show
station-log> event severity set <event-id>
station-log> event severity remove <event-id>
```

コマンド モード

ステーション ログ

デフォルト

無効

用途

デフォルトでは、station-log によって、下記に示すすべてのイベント重大度が表示され、ログされます。現在有効である重大度を表示するには、**event severity show** コマンドを使用します。

特定のイベント フィルタを有効にするには、**event severity set <id>** コマンドを使用して、**event severity show** コマンドで表示される該当する ID 番号を指定します。フィルタは有効になり、重大度情報が表示されるようになります。

特定のイベント重大度を無効にするには、**event severity remove <id>** コマンドを使用して、**event severity show** コマンドで表示される該当する ID 番号を指定します。フィルタは無効になり、指定した重大度のイベントは表示されなくなります。



すべてのイベントのフィルタを有効または無効にするには、id フィールドに all と入力します (event id set all)。

使用例

```
station-log> event severity show
```

Event Severity Filters

=====

Enabled		Severity
---------	--	----------

Yes		Info
-----	--	------

Yes		Minor
-----	--	-------

Yes		Major
Yes		Critical

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)
- [station-log show \(859 ページ\)](#)
- [\(station-log\) event id \(853 ページ\)](#)

(station-log) show filters

ステーション ログのすべてのイベントと重大度のフィルタのステータスを表示します。

構文 station-log> show filters

コマンド
モード ステーション ログ

デフォルト なし

用途 すべてのステーション ログ フィルタの有効 / 無効のステータスをすばやく確認するには、station-log 端末にアクセスし、**show filters** コマンドを使用します。

使用例 station-log> show filters

```
Event ID Filters
=====
Enabled | ID# | Name
-----
Yes     | 1 | IP Address Discovered
Yes     | 2 | DHCP
Yes     | 3 | Station Assign
Yes     | 4 | 802.11 State
Yes     | 5 | CP User Authentication
Yes     | 6 | 1X Authentication
Yes     | 7 | Encryption
Yes     | 8 | Mac Filtering
Yes     | 9 | Diagnostics
Yes     | 10 | Band Steering
Yes     | 11 | SIP

Event Severity Filters
=====
Enabled | Severity
-----
```

Yes		Info
Yes		Minor
Yes		Major
Yes		Critical

The station filter list is empty!

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)
- [station-log show \(859 ページ\)](#)
- [\(station-log\) event id \(853 ページ\)](#)
- [\(station-log\) event severity \(855 ページ\)](#)

station-log show

イベント ログ ヒストリと、802.11 probe、auth、assoc、deauth、disassoc などの情報を表示します。このコマンドは、会話型の station-log コマンドの代替バージョンです。

構文

```
station-log show
station-log show -mac=<station MAC address>
```

コマンドモード

グローバル設定モード

デフォルト

なし

用途

MAC アドレスが分からない場合や、現在までのすべてのイベント ログ ヒストリを表示したい場合は、**station-log show** を使用します。

MAC アドレス 11:22:33:44:55:66 のヒストリのみを表示する場合は、**station-log show=11:22:33:44:55:66** を使用します。

使用例

次の例は、ログされたすべてのステーションを表示します。

```
Master1# station-log show
2009-09-01 01:53:18.790 | 00:1c:f0:f9:02:bd | 802.11 State |
state change
<old=Unauthenticated><new=Authenticated><AP=00:0c:e6:05:eb:7d><BSSID=00:0c:e6:7a:29:0e>
2009-09-01 01:53:18.798 | 00:1c:f0:f9:02:bd | 802.11 State |
state change
<old=Authenticated><new=Associated><AP=00:0c:e6:05:eb:7d><BSSID=00:0c:e6:7a:29:0e>
2009-09-01 01:53:18.799 | 00:1c:f0:f9:02:bd | 1X Authentication | <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent
2009-09-01 01:53:19.368 | 00:20:a6:4e:c3:1b | Station Assign |
<AID=4> assigned to <AP_ID=5><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>
2009-09-01 01:53:19.978 | 00:20:a6:4e:c3:1b | Station Assign |
<AID=4> Assign Removed From
<AP_ID=5><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>
2009-09-01 01:53:19.978 | 00:20:a6:4e:c3:1b | Station Assign |
<AID=4> assigned to <AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>
```

```

2009-09-01 01:53:20.797 | 00:1c:f0:f9:02:bd | 1X Authentication |
<auth method=WPA2_EAP>:<pkt type=EAPOL_START> recvd <ESSID=client4>
<BSSID=00:0c:e6:7a:29:0e>

2009-09-01 1:53:20.797 | 00:1c:f0:f9:02:bd | 1X Authentication | <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent

2009-09-01 01:53:21.098 | 00:16:ea:ed:c3:12 | Station Assign |
<AID=4> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:3d:86:0c>

2009-09-01 01:53:21.098 | 00:16:ea:ed:c3:12 | Station Assign |
<AID=1> Assign Removed From
<AP_ID=553><ESSID=rxorn><BSSID=00:0c:e6:ba:48:20>

2009-09-01 01:53:21.098 | 00:16:ea:ed:be:30 | Station Assign |
<AID=2> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>

2009-09-01 01:53:21.098 | 00:16:ea:ed:cf:7c | Station Assign |
<AID=6> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:3d:86:0c>

2009-09-01 01:53:21.174 | 00:16:ea:ed:cf:7c | Station Assign |
<AID=6> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:3d:86:0c>

last 2653455

```

関連コマンド

- [station-log \(847 ページ\)](#)
- [\(station-log\) filelog \(851 ページ\)](#)
- [\(station-log\) syslog \(852 ページ\)](#)

17 サービス コントロール コマンド

本章では、サービス コントロールのグローバル設定に使用するコマンドについて説明します。

- [blocked-gateway \(862 ページ\)](#)
- [policy \(863 ページ\)](#)
- [service-type \(865 ページ\)](#)
- [service-control-config active-discovery \(866 ページ\)](#)
- [service-control-config essids \(867 ページ\)](#)
- [service-control-config gateways \(868 ページ\)](#)
- [service-control-config locations \(869 ページ\)](#)
- [service-control-config service-types \(870 ページ\)](#)
- [service-control-config state \(871 ページ\)](#)
- [service-control-config vlans \(872 ページ\)](#)
- [show service-control blocked-gateway \(873 ページ\)](#)
- [show service-control global-config \(874 ページ\)](#)
- [show service-control global-config-service \(875 ページ\)](#)
- [show service-control global-discovered-service \(876 ページ\)](#)
- [show service-control global-discovered-service-summary \(877 ページ\)](#)
- [show service-control location \(878 ページ\)](#)
- [show service-control policy \(879 ページ\)](#)
- [show service-control policy-config-service \(880 ページ\)](#)
- [show service-control policy-service \(881 ページ\)](#)
- [show service-control policy-service-summary \(882 ページ\)](#)
- [show service-control service-type \(883 ページ\)](#)
- [show service-control user-group \(884 ページ\)](#)
- [user-group \(885 ページ\)](#)

blocked-gateway

サービス コントロールの IP アドレスを使用して、ブロックされたゲートウェイを設定します。

構文

blocked-gateway <name>

コマンド モード

グローバル設定

デフォルト

なし

用途

サービス コントロールに対してブロックされる IP アドレスを設定するには、このコマンドを使用します。

使用例

```
controller# configure terminal
controller(config)# blocked-gateway meruip
controller(config)# exit
```

関連コマンド

[*show service-control blocked-gateway*](#) (873 ページ)

policy

サービス コントロール ポリシーを設定します。

構文

policy

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドは、ポリシーの一意の名前を設定します。ロールのタイプ (サブスクライバーまたはパブリッシャー)、ユーザ グループ、サービス タイプ、およびポリシーのオーナーを設定できます。

使用例

```
controller# configure terminal
controller(config)# policy merupolicy
MC3200(15)(config-policy)# description Fortinet Policy service control
controller(config)# exit
```

次の例は、コマンドのオプションを表示します。

```
controller# configure terminal
controller(config)# policy merupolicy
MC3200(15)(config-policy)# ?
description          (10) Specifies the Location.
end
mode.                (10) Save changes, and return to privileged EXEC
exit
mode.                (10) Save changes, and return to global configuration
owner                 (10) Owner of the profile
publisher-user-groups (10) Publisher User Groups.
service-types         (10) Service Types.
subscriber-user-groups (10) Subscriber User Groups.
```

関連コマンド

- [show service-control policy \(879 ページ\)](#)
- [show service-control policy-config-service \(880 ページ\)](#)

- [*show service-control policy-service*](#) (881 ページ)
- [*show service-control policy-service-summary*](#) (882 ページ)
- [*show service-control service-type*](#) (883 ページ)

service-type

サービス コントロールのサービス タイプを設定します。

構文

service-type

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、サービス タイプ、その説明、およびサービスタイプの値を設定します。

使用例

```
controller# configure terminal
controller(config)# service-type meruservicetype
MC3200(15)(config-service-type)# description Fortinet service type
controller(config)# exit
```

次の例は、コマンドのオプションを表示します。

```
controller# configure terminal
controller(config)# service-type meruservicetype
MC3200(15)(config-service-type)# ?
description          (10) Specifies the Service Type.
end
mode.                (10) Save changes, and return to privileged EXEC
exit
mode.                (10) Save changes, and return to global configuration
value                (10) Configure Value.
```

関連コマンド

[*show service-control service-type*](#) (883 ページ)

service-control-config active-discovery

このコマンドを使用すると、グローバル検出基準にもとづいた active-discovery がトリガされます。

構文

```
service-control-config active-discovery <id>/all/controller
```

<i>id</i>	AP ID を入力します
all	すべてのエンティティを設定します
controller	コントローラにサービス エージェントを設定します

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、検出対象のサービス タイプを指定します。デフォルトでは、すべての SSID のワイヤレス サービスと、コントローラの有線インターフェイス上の VLAN 0 のすべての AP と有線サービスが選択されています。

使用例

```
controller# configure terminal
controller(config)# service-control-config active-discovery all
controller(config)# exit
```

関連コマンド

- [show service-control global-discovered-service \(876 ページ\)](#)
- [show service-control global-discovered-service-summary \(877 ページ\)](#)

service-control-config essids

このコマンドを使用すると、グローバル検出基準に ESSID が追加されます。

構文

```
service-control-config essids <essids>
```

essids カンマで区切った ESSID プロファイル名を入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、この ESSID に接続しているパブリッシャーを検出します。

使用例

```
controller# configure terminal
controller(config)# service-control-config essids
controller(config)# exit
```

関連コマンド

- [show service-control global-config \(874 ページ\)](#)
- [show service-control global-config-service \(875 ページ\)](#)

service-control-config gateways

このコマンドは、サービス コントロールの有線ゲートウェイを設定します。

構文

service-control-config gateways <gateways>

gateways コントローラの AP ID または 0 (ゼロ) を入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、パブリッシャーを検出するための有線ゲートウェイのリストに AP やコントローラを追加します。

使用例

```
controller# configure terminal
controller(config)# service-control-config gateways
controller(config)# exit
```

関連コマンド

[*show service-control blocked-gateway*](#) (873 ページ)

service-control-config locations

このコマンドは、サービス コントロールの場所を設定します。

構文

`service-control-config locations <location name>`

location サービス コントロールをアクティブにする場所の名前を入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、ワイヤレスのサブスクライバー / パブリッシャーの場所を指定します。

使用例

```
controller# configure terminal
controller(config)# service-control-config locations
controller(config)# exit
```

関連コマンド

[show service-control location \(878 ページ\)](#)

service-control-config service-types

このコマンドは、サービス タイプを設定します。

構文

```
service-control-config service-types <service types>
```

service-types ネットワークで使用できるサービス タイプを入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、使用可能なサービスとそのサービス タイプを設定します。

使用例

```
controller# configure terminal
controller(config)# service-control-config service-types AppleTV
controller(config)# exit
```

関連コマンド

- [show service-control policy-service \(881 ページ\)](#)
- [show service-control policy-service-summary \(882 ページ\)](#)
- [show service-control service-type \(883 ページ\)](#)

service-control-config state

このコマンドは、サービス コントロールを有効または無効にします。

構文

`service-control-config state <enable/disable>`

<i>enable</i>	ネットワークでサービス コントロール機能を有効にします。
<i>disable</i>	ネットワークでサービス コントロール機能を無効にします。

コマンド モード

グローバル設定

デフォルト

なし

用途

使用例

```
controller# configure terminal
controller(config)# service-control-config state enable
controller(config)# exit
```

関連コマンド

[show service-control global-config \(874 ページ\)](#)

service-control-config vlans

このコマンドは、有線ゲートウェイのグローバル検出基準に VLAN を設定します。

構文

```
service-control-config vlan <vlans>
```

vlans VLAN ID の範囲をカンマで区切って入力します。

コマンド モード

グローバル設定

デフォルト

なし

用途

使用例

```
controller# configure terminal
controller(config)# service-control-config vlan 10
controller(config)# exit
```

関連コマンド

[show service-control global-config \(874 ページ\)](#)

show service-control blocked-gateway

ブロックされたゲートウェイ リストを表示します。

構文

```
show service-control blocked-gateway
```

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

このコマンドは、広告が無視されるブロックされた IP アドレスのリストを表示します。

使用例

```
controller# show service-control blocked-gateway
Name                IP Address
Fortinet            172.29.0.137
Servcie Connect Blocked Gateway(1 entry)
```

関連コマンド

- [blocked-gateway](#) (862 ページ)
- [service-control-config gateways](#) (868 ページ)

show service-control global-config

設定されているグローバル検出基準を表示します。

構文

`show service-control global-config`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

このコマンドを使用して、サービス タイプのリスト、VLAN、ESSID プロファイル、ロケーション リスト、有線ゲートウェイのリストなど、サービス コントロールのグローバル設定を表示します。

使用例

```
controller# show service-control global-config
service control Global Configuration
```

```
Enable Service      : enable
Service Type List   : *
VLANs                : 0
ESSIDs              : Dabcjk
Location List       : MeruEng
Wired Gateway List  : 0
```

関連コマンド

- [service-control-config active-discovery \(866 ページ\)](#)
- [service-control-config essids \(867 ページ\)](#)
- [service-control-config gateways \(868 ページ\)](#)
- [show service-control global-config-service \(875 ページ\)](#)

show service-control global-config-service

設定されているサービスのグローバル検出基準を表示します。

構文

`show service-control global-config-service`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

このコマンドは、使用可能なサービス コントロールのグローバル設定サービスを表示します。

使用例

controller# `show service-control global-config-service`

関連コマンド

- [service-control-config essids \(867 ページ\)](#)
- [service-control-config gateways \(868 ページ\)](#)
- [show service-control global-config \(874 ページ\)](#)

show service-control global-discovered-service

グローバルに検出されたサービス リストを表示します。

構文

`show service-control global-discovered-service`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

使用例

`controller# show service-control global-discovered-service`

関連コマンド

- [service-control-config active-discovery \(866 ページ\)](#)
- [show service-control global-discovered-service-summary \(877 ページ\)](#)

show service-control global-discovered-service-summary

グローバルに検出されたサービスのサマリを表示します。

構文

`show service-control global-discovered-service-summary`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

このコマンドは、検出されたサービスのタイプのサマリを表示します。

使用例

`controller# show service-control global-discovered-service-summary`

関連コマンド

- [service-control-config active-discovery \(866 ページ\)](#)
- [show service-control global-discovered-service \(876 ページ\)](#)

show service-control location

サービス コントロールの場所を表示します。

構文

```
show service-control location
```

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

使用例

```
controller# show service-control location
```

Name	AP ID	Description
FortiEng	10,6-9	Fortinet Engineering Area
FortiTest	1-5	Fortinet Test

Location(2)

関連コマンド

[service-control-config locations](#) (869 ページ)

show service-control policy

サービス コントロール ポリシーを表示します。

構文

`show service-control policy`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

使用例

```
controller# show service-control policy
Name          Subscriber User Group  Service Type  Publisher User Group
MeruPolicy    MeruUSER                      *             MeruUSER
              service control Policy(1 entry)
```

関連コマンド

- [policy \(863 ページ\)](#)
- [show service-control policy-config-service \(880 ページ\)](#)
- [show service-control policy-service \(881 ページ\)](#)
- [show service-control policy-service-summary \(882 ページ\)](#)

show service-control policy-config-service

ポリシーとその設定を表示します。

構文 `show service-control policy-config-service`

コマンド
モード ユーザ EXEC

デフォルト なし

用途

使用例

```
controller# show service-control policy-config-service
Policy  Service Type List      Sub APs      Sub VLANs      Sub ESSIDs
Sub Cont  Pub APs      Pub VLANs      Pub ESSIDs      Pub Cont
1         _airplay._tcp.local.,_r 6-10      1
enable    6-10      1      enable
Policy Configuration Service(1 entry)
```

- 関連コマンド
- [policy \(863 ページ\)](#)
 - [show service-control policy \(879 ページ\)](#)
 - [show service-control policy-service \(881 ページ\)](#)
 - [show service-control policy-service-summary \(882 ページ\)](#)

show service-control policy-service

サービスのフィルタリング後のリストとサブスクライバーが使用できるサービス タイプを表示します。

構文

`show service-control policy-service <name>`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

使用例

controller# `show service-control policy-service merupolicysrv`

関連コマンド

- [policy \(863 ページ\)](#)
- [show service-control policy \(879 ページ\)](#)
- [show service-control policy-config-service \(880 ページ\)](#)
- [show service-control policy-service-summary \(882 ページ\)](#)

show service-control policy-service-summary

サービスのサマリ リストを表示します。

構文

`show service-control policy-config-service-summary <name>`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

このコマンドを使用すると、設定されているポリシー サービスのサマリが表示されます。

使用例

`controller# show service-control policy-service-summary merupolicy`

関連コマンド

- [policy \(863 ページ\)](#)
- [show service-control policy \(879 ページ\)](#)
- [show service-control policy-config-service \(880 ページ\)](#)
- [show service-control policy-service \(881 ページ\)](#)

show service-control service-type

サービス タイプのリストを表示します。

構文

`show service-control service-type`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

使用例

```
controller# show service-control service-type
```

Name	Description	Service Type
AppleTV	Apple TV	_airplay._tcp.local.,_raop._tcp.local.
Printer	Printer	_ipp._tcp.local.,_ipps._tcp.local.,_uni

Service Type(2)

関連コマンド

[service-type](#) (865 ページ)

show service-control user-group

サービス コントロールのユーザ グループを表示します。

構文

`show service-control user-group`

コマンド モード

ユーザ EXEC

デフォルト

なし

用途

使用例

```
controller# show service-control user-group
Name          VLAN          ESSIDs        Locations
MeruUSER      Dabcjk        MeruEng
User Group(1 entry)
```

関連コマンド

[user-group](#) (885 ページ)

user-group

サービス コントロールのユーザ グループを設定します。

構文

user-group

コマンド モード

グローバル設定

デフォルト

なし

用途

このコマンドを使用して、ユーザ グループの一意の名前を設定します。ユーザ グループの
ロール タイプ (サブスクライバーまたはパブリッシャー)、ESSID リスト、ロケーション、
および VLAN リストを設定できます。

使用例

```
controller# configure terminal
controller(config)# user-group
MC3200(15)(config-user-group)# description Fortinet User Group
MC3200(15)(config-user-group)# enable-pub-role on
controller(config)# exit
```

次の例は、コマンドのオプションを表示します。

```
controller# configure terminal
controller(config)# user-group
MC3200(15)(config-user-group)# ?
description                (10) Specifies the User Group.
enable-pub-role             (10) Configure Publisher Role.
enable-sub-role             (10) Configure Subscriber Role.
end                          (10) Save changes, and return to privileged EXEC mode
essids                      (10) Configure ESSID list.
exit                         (10) Save changes, and return to global configuration
mode.
locations                   (10) Configure Location list.
vlans                       (10) Configure VLAN list.
```

関連コマンド

[show service-control user-group \(884 ページ\)](#)

18 トラブルシューティング コマンド

本章では、WLAN のトラブルシューティングに役立つコマンドについて説明します。

- [analyze-capture \(889 ページ\)](#)
- [auto-report admin \(890 ページ\)](#)
- [auto-report send \(892 ページ\)](#)
- [capture-packets \(894 ページ\)](#)
- [debug captive-portal \(901 ページ\)](#)
- [debug connect \(902 ページ\)](#)
- [debug controller \(903 ページ\)](#)
- [debug eap \(904 ページ\)](#)
- [debug mac-filter \(905 ページ\)](#)
- [debug module \(906 ページ\)](#)
- [\(diag-log\) admin \(910 ページ\)](#)
- [\(diag-log\) config \(912 ページ\)](#)
- [\(diag-log\) restore \(914 ページ\)](#)
- [diagnostics \(916 ページ\)](#)
- [diagnostics-ap \(918 ページ\)](#)
- [diagnostics-controller \(920 ページ\)](#)
- [\(packet-capture-profile\) enable-profile \(934 ページ\)](#)
- [\(packet capture profile\) mode \(938 ページ\)](#)
- [packet-capture-profile \(922 ページ\)](#)
- [\(packet capture profile\) ap-list \(925 ページ\)](#)
- [\(packet capture profile\) capture-sibling-frames \(927 ページ\)](#)
- [\(packet-capture-profile\) enable-profile \(934 ページ\)](#)
- [\(packet capture profile\) filter \(936 ページ\)](#)
- [\(packet capture profile\) interface list \(937 ページ\)](#)
- [\(packet capture profile\) mode \(938 ページ\)](#)

- [\(packet capture profile\) packet-truncation-length](#) (940 ページ)
- [\(packet capture profile\) rate-limiting](#) (941 ページ)
- [\(packet capture profile\) rate-limiting-mode](#) (943 ページ)
- [\(packet capture profile\) rxtx](#) (944 ページ)
- [\(packet capture profile\) token-bucket-rate](#) (946 ページ)
- [\(packet capture profile\) token-bucket-size](#) (949 ページ)
- [remote-log](#) (952 ページ)
- [show auto-report-config](#) (953 ページ)
- [show cef](#) (955 ページ)
- [show debug](#) (956 ページ)
- [show diag-log-config ap/controller/station](#) (957 ページ)
- [show packet-capture-profile](#) (963 ページ)
- [show statistics AP300-diagnostics](#) (965 ページ)

analyze-capture

ワイヤレス トラフィックを分析します。

構文

```
analyze-capture snapshot  
analyze-capture start <filename> ap <ap-list> bssid <bssid-list>  
analyze-capture stop
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

analyze-capture コマンドは、指定した AP および BSSID のいずれかを使用しているすべてのクライアントについて、802.11 管理と TCP セッション状態の統計情報を捕捉します。収集される情報のタイプは、クライアントの再認証と再連結、および TCP セッションの統計情報です。

このコマンドを起動して長時間実行しても、ディスク スペースを消費しません。**snapshot** または **stop** キーワードを指定するまで、出力は生成されません。

AP または BSSID の文字列をグループ化するには、二重引用符を使用する必要があります。

使用例

たとえば、次のコマンドでは、check.txt ファイルに、AP 1 ～ 3 と BSSID 00:0c:e6:32:22:01 および 00:0c:e6:30:11:22 に関する捕捉が生成されます。

```
controller# analyze-capture start check.txt ap "1 2 3" bssid  
"00:0c:e6:32:22:01 00:0c:e6:30:11:22"  
controller#
```

関連コマンド

[packet-capture-profile](#) (922 ページ)

auto-report admin

フォーティネット サポートと一緒に作業する場合のみ、このコマンドを使用してください。このコマンドは、自動レポートをオン / オフにして、診断情報をフォーティネット サポートに送信できるようにします。

構文

```
auto-report admin on
auto-report admin off
```

コマンド モード

設定モード

デフォルト

オフ

用途

このコマンドは、**auto-report send** コマンドと一緒に使用します。**auto-report send** で間隔を指定すると、**auto-report admin** が **on** に設定されている間、そのスケジュールでレポートが送信されます。

使用例

以下の例では、`cwon:cwon@172.27.0.79/diagagent.conf` に 1 時間ごとにレポートを送信します。

```
Meru01#configure terminal
Meru01(config)# auto-report
Meru01(config-auto-report)# ?
```

```
admin    Configures administration mode for auto-reporting
do       Executes an IOSCLI command
end      Saves changes and returns to privileged exec mode
exit     Saves changes and returns to global configuration mode
send     Uploads log files to named URL once or periodically
```

```
Meru01(config-auto-report)# send ftp://cwon:cwon@172.27.0.79/
diagagent.conf 1
Meru01(config-auto-report)# admin on
Meru01(config-auto-report)# show auto-report-config
```

```
Administration Status      on
```

Auto-reporting Interval	every hour
Auto-reporting URL	cwon:cwon@172.27.0.79

関連コマンド

- [auto-report send \(892 ページ\)](#)
- [\(diag-log\) admin \(910 ページ\)](#)
- [\(diag-log\) config \(912 ページ\)](#)
- [\(diag-log\) restore \(914 ページ\)](#)
- [show auto-report-config \(953 ページ\)](#)

auto-report send

この機能は、カスタマ サポートと一緒に作業する場合のみ使用してください。このコマンドは診断ログ ファイルの情報を暗号化されたレポートに変換し、FTP を使用してレポートを送信してから、ログ ファイルをクリアします。

構文

```
auto report send <username:password> <URL Location><interval>
```

<i>username</i>	FTP ユーザ名 - 必須
<i>password</i>	FTP パスワード - 必須
<i>URL location</i>	アップロードの IP アドレス
<i>interval</i>	レポートを送信する頻度 (単位: 時)。24 と指定すると、1 日に 1 度。

コマンドモード

グローバル設定

デフォルト

なし

用途

このコマンドは診断ログ ファイルの情報を暗号化されたレポートに変換し、レポートを送信してから、ログ ファイルをクリアします。間隔を指定すると、**auto-report admin** が on に設定されている間、そのスケジュールでレポートが送信されます。URL でパスワードを使用する必要があります。ログイン名がない場合は、anonymous とパスワード anonymous を使用します。パスワード フィールドが空の状態であると、ファイルを解凍できません。

使用例

以下の例では、anonymous:anonymous@192.168.105.75 に 1 時間ごとにレポートを送信します。

```
Meru01#configure terminal
Meru01(config)# auto-report
Meru01(config-auto-report)# ?
```

admin	Configures administration mode for auto-reporting
do	Executes an IOSCLI command
end	Saves changes and returns to privileged exec mode
exit	Saves changes and returns to global configuration mode

send Uploads log files to named URL once or periodically

```
default(config-auto-report)# send ftp://anonymous:anonymous@192.168.105.75  
1
```

```
default# sh auto-report-config
```

```
Administration Status on
```

```
Auto-Reporting Interval every 1 hour
```

```
Auto-Reporting Url ftp://anonymous:anonymous@192.168.105.75
```

```
Administration Status                on
```

```
Auto-reporting Interval               every hour
```

```
Auto-reporting URL                    cwon:cwon@172.27.0.79
```

関連コマンド

- [auto-report admin \(890 ページ\)](#)
- [\(diag-log\) admin \(910 ページ\)](#)
- [\(diag-log\) config \(912 ページ\)](#)
- [\(diag-log\) restore \(914 ページ\)](#)
- [show auto-report-config \(953 ページ\)](#)

capture-packets

このコマンドは、AP150 パケット捕捉に使用します。AP300 および AP200 の場合、[packet-capture-profile \(922 ページ\)](#) モードの新しい強力な FortiWLC (SD) コマンドを使用できません。**capture-packets** コマンドも引き続きサポートされており、このコマンドを使用するどのスクリプトも以前のリリースとまったく同じように実行でき、AP150 では、これが唯一のオプションです。

Ethereal でコントローラのインターフェイス上またはアクセス ポイントの無線上のパケットを捕捉します。

構文

```
capture-packets [-c count][-i ap_id1[, ap_id2, ...]]{m,n,t}[-r infile] [-R filter]r|a|ad|d [-V] [-v frame] [-w savefile -a stop-condition] [-x]
```

-a stop-condition	停止条件 (-a filesize:1000 など) です。
-c count	実際のデータを捕捉する場合に読み取るパケットのデフォルトの個数を指定します。
-f capture-filter	フィルタ式です。
-F file-format	捕捉ファイルの形式 (-F netmon1 など) です。
-i ap_id1[, ap_id2, ...]	AP (番号で指定) からパケット、および追加の AP のリスト (オプション) を捕捉します。
-n	ネットワーク オブジェクトの名前解決 (ホスト名、TCP ポート名、UDP ポート名など) を無効にします。
-N {m,n,t}	特定のタイプのアドレスおよびポート番号の名前解決を有効にし、他のタイプのアドレスおよびポート番号の名前解決を無効にします。MAC アドレスの解決を有効にするには m 、ネットワーク アドレスの解決を有効にするには n 、トランスポート層のポート番号の解決を有効にするには t を引数のオプションとして指定します。 -N と -n の両方を指定すると、 -n は無効になります。
-p	インターフェイスの不規則モードを無効にします。
-q	捕捉したパケットのカウントを表示しません。
-r infile	1 列目に追加のフィールド (フレーム番号) を含む捕捉済みのファイルの概要を表示します。

-R <i>'display-filter'</i>	捕捉を表示する前に、カスタム フィルタまたは Ethereal フィルタを適用します。フィルタ名を単一引用符 (") で囲み、式演算子で連結して、複雑なフィルタを作成します。== などの演算子を使用する複雑なフィルタでは、スペースを使用しないでください。この引数で利用できるカスタム フィルタのリストについては、以下の表を参照してください。Ethereal フィルタの詳細については、 http://www.ethereal.com/docs/man-pages/ethereal-filter.4.html を参照してください。
-S <i>Record</i>	フレーム番号で記録 / 要約して再生できるようにします。
-s <i>snaplen</i>	<i>snaplen</i> は、実際のデータのスナップショットのデフォルトの長さを定義します。
-t <i>r a ad d</i>	パケット リスト ウィンドウに表示するパケット タイム スタンプの形式を定義します。この形式には、 r (相対時間)、 a (絶対時間)、 ad (日付付き絶対時間)、または d (デルタ時間) があります。相対時間は最初のパケットから現在のパケットまでの経過時間です。絶対時間はパケットが捕捉された実際の時間であり、日付が表示されません。日付付き絶対時間はパケットが捕捉された時間です。デルタ時間は前のパケットが捕捉されてからの経過時間です。デフォルト値は相対時間です。
-V	プロトコル ツリーを表示します。
-v <i>frame</i>	フレーム番号で再生します。
-w <i>savefile</i> -a <i>stop-condition</i>	ファイルに捕捉情報を書き込み、ファイル サイズを制限します。フォーティネットは、 -w および -a 引数を併用することを推奨しています。この場合は、 <i>stop-condition</i> パラメータに filesize:5000 を設定し、ファイル サイズを 5 MB に制限します。
-x	16 進形式でパケット捕捉を表示します。
-S <i>record</i>	フレーム番号で記録 / 要約して再生できるようにします。
-v <i>playback</i>	「フレーム番号」をフレーム再生します。

コマンド モード

グローバル設定

デフォルト

なし

用途

AP150 ネットワーク トラフィックを捕捉するには、**capture-packets** コマンドを使用します。コントローラのインターフェイスでパケットを捕捉するには、引数なしで **capture-packets** コマンドを使用します。また、最初に **debug ap** コマンドを実行した場合は、**capture-packets** コマンドでアクセス ポイントからのパケットを捕捉できます。アクセス ポイントで捕捉されたパケットのみを表示するように、パケットをフィルタリングできます。デフォルトでは、アクセス ポイントおよびコントローラのローカル インターフェイスからのパケットが表示されます。捕捉をリアルタイムで表示することも、ファイルに保存して後でオフラインで分析することもできます。SSH でコントローラにアクセスしている場合は、SSH トラフィックをフィルタリングして捕捉および表示する情報の量を削減することを検討します (例については、626 ページの「使用例」を参照してください)。インターフェイス フィルタまたは MAC アドレス フィルタが設定されている場合のみ、AP150 に **capture-packets** を使用します。これらのフィルタが設定されていないと、AP150 が大量のデータを受け取ることになり、最終的にはコントローラにアクセスできなくなります。

リアルタイムのパケット捕捉を停止するには、**Ctrl-C** を押します。

アクセス ポイントで捕捉されるパケットには、不明なアクセス ポイントからのトラフィックおよびアクセス ポイント間のトラフィックがあります。**-R** 引数で、捕捉したパケットをフィルタリングします (カスタム フィルタのリストについては、次の表を参照してください)。

WEP 暗号化フレームは、無線で捕捉されると、暗号化されます。暗号化されていないデータ フレームを捕捉するには、コントローラのローカル インターフェイスから捕捉します。固定 WEP キーを使用する場合、Windows バージョンの Ethereal とフォーティネット プラグインを併用することでフレームを複合化できます。

次の点で、アクセス ポイントから送信されるパケットは、アクセス ポイントで受信されるパケットと異なります。

- アクセス ポイントで受信されるパケットは再送信ごとに 1 個存在します。再送信ビットは無線で受信されるものとして設定されます。再送信の回数に関わらず、送信されたフレームは 1 回のみ表示されます。controller.cap.tx.flags.retries フィールドを使用して、フレームが再試行された回数を確認します。送信されたフレームの 802.11 MAC ヘッダーの再送信ビットには、常にゼロが設定されます。
- 受信されたフレームについては、TSF フィールドは最初のビットが受信された時間と同じです。送信されたフレームについては、TSF フィールドは最後の送信の直後の時間です。
- 受信された 802.11 肯定応答は捕捉されますが、送信された肯定応答は捕捉されません。

イーサネット MTU を超える捕捉されたフレームは断片化されます。捕捉エントリを参照すると、断片化されたフレームの 2 つ目のエントリは、概要として “M-Cap 802.11 Continuation Controller ATS Capture Fragment Continuation” と表示されます。

次の表に、**capture-packets** コマンドの **-R** 引数で利用できるフィルタを記載します。

controller.cap	アクセス ポイントで捕捉したパケットのみに制限し、コントローラのローカル インターフェイスからのパケットを除外します。
controller.cap.version	トンネルのバージョン
controller.cap.outer.fraglen	フラグメントの長さ
controller.cap.frag	断片化フィールド
controller.cap.outer.fragmented	断片化されています。
controller.cap.outer.morefrags	追加のフラグメント
controller.cap.outer.fragnumber	断片化番号
controller.cap.outer.seq	捕捉されたフレームの方向 (送信または受信)
controller.cap.rx.flags	受信フラグ
controller.cap.rx.flags.diversity	アンテナ ダイバーシティで受信
controller.cap.rx.flags.antenna_select	フレームを受信したアンテナ
controller.cap.rx.flags.shortpreamble	短いプリアンプル
controller.cap.rx.flags.assigned	送信側がこの AP に割り当てられているかどうか
controller.cap.rx.flags.fcs_failure	チェックサムが有効であるかどうか
controller.cap.rx.flags.frame_too_late	キャリアから受信したフレームの遅延が無意味であるほどに大きすぎるかどうか
controller.cap.rx.silence	パケット受信直前の信号強度
controller.cap.rx.signal	パケット受信中の信号強度
controller.cap.rx.left_rssi	左アンテナからの RSSI
controller.cap.rx.right_rssi	右アンテナからの RSSI
controller.cap.rx.rate	802.11 パケット速度 (100 Kbps 単位)
controller.cap.rx.cca_dclk	CCA high から最初のデータ ビットまでの時間 (ミリ秒単位)
controller.cap.rx.length	受信 802.11 フレームの長さ
controller.cap.rx.time	フレームを受信した低 TSF 時間
controller.cap.rx.channel	フレームを受信したチャンネル
controller.cap.rx.crc	802.11 FCS

<code>controller.cap.tx.flags</code>	送信フラグ
<code>controller.cap.tx.flags.success</code>	802.11 肯定応答を受信したかどうか
<code>controller.cap.tx.flags.initcts</code>	RTS が最初の送信時に送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry1cts</code>	RTS が最初の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry2cts</code>	RTS が 2 回目の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry3cts</code>	RTS が 3 回目の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry4cts</code>	RTS が 4 回目の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry5cts</code>	RTS が 5 回目の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry6cts</code>	RTS が 6 回目の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.retry7cts</code>	RTS が 7 回目の再送信で送信された場合、CTS を受信したかどうかを表します
<code>controller.cap.tx.flags.ackps</code>	肯定応答の PS ビット (存在する場合)
<code>controller.cap.tx.flags.ackrssi</code>	肯定応答の RSSI (存在する場合)
<code>controller.cap.tx.flags.retries</code>	再送信の試行回数 (フレームが 1 回だけ送信された場合はゼロ)
<code>controller.cap.tx.flags.antenna</code>	フレームを送信したアンテナ
<code>controller.cap.tx.flags.preamble</code>	フレーム (または、再試行した場合は最終フレーム) の送信に使用された短いプリアンプル
<code>controller.cap.tx.time</code>	フレーム (または再試行した場合は最終フレーム) が送信された低 TSF 時間
<code>controller.cap.tx.length</code>	802.11 フレームの長さ
<code>controller.cap.tx.rate</code>	フレーム (または再試行の場合には最終フレーム) の送信に使用された速度
<code>controller.cap.tx.channel</code>	フレームを送信したチャンネル

使用例

次のコマンドは、ICMP パケットのみを捕捉します。

```
controller# capture-packets -R icmp
```

Capturing on controller

```
30.434804 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
30.435000 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
31.433751 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
31.433866 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
32.432920 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
32.433042 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
33.432088 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
33.432203 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
34.431320 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
34.431434 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
35.430419 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
35.430523 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
36.429761 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
36.429860 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
```

次のコマンドは、SSH トラフィックをフィルタリングします。

```
controller# capture-packets -R 'tcp.srcport!=22&&tcp.dstport!=22'
```

次のコマンドは、最大サイズが 5 MB の **capture-file** ファイルにパケットを捕捉します。

```
controller# capture-packets -w capture-file -a filesize:5000
```

Capturing on controller

559

controller#

次のコマンドは、IP アドレス 10.1.225.42 で送受信される RADIUS フレームのみを捕捉します。

```
controller# capture-packets -w capture_file -a filesize:5000 -R
'ip.addr==10.1.225.42&&radius'
```

次のコマンドは、capture_file ファイルに保存される DHCP フレームをフィルタリングし、捕捉されたファイルを表示します。

```
controller# debug ap 1
```

```
controller# capture-packets -w capture_file -a filesize:5000 -R bootp.dhcp
```

```
controller# capture-packets -r capture_file
```

```
1  0.000000  10.0.220.49 -> 10.0.0.10    DHCP DHCP Request  -  
Transaction ID 0x9a5e380e  
2  0.002390    10.0.0.10 -> 10.0.220.49  DHCP DHCP ACK      -  
Transaction ID 0x9a5e380e
```

次のコマンドは、BSS 00:0c:e6:01:00:0d 上のすべてのトラフィック、クライアント 00:07:40:01:02:03 で送受信されるすべてのトラフィック、およびすべての EAPOL トラフィックをフィルタリングします。

```
controller# capture-packets -R 'wlan.bssid==00:0c:e6:01:00:0d'  
controller# capture-packets -R 'wlan.addr==00:07:40:01:02:03'  
controller# capture-packets -R eapol
```

関連コマンド [packet-capture-profile](#) (922 ページ)

debug captive-portal

キャプティブ ポータルのデバッグ メッセージを有効にします。

構文

```
debug captive portal  
no debug captive portal
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

キャプティブ ポータルの認証を検証するには、このデバッグ モジュールを使用します。このデバッグ情報は、ワイヤレス クライアントと認証サーバの間のエンドツーエンドのパケット転送の詳細です。複数のキャプティブ ポータル ログイン ページが存在できますが、キャプティブ ポータルは 1 つだけです。

使用例

次の例は、キャプティブ ポータルのデバッグを有効にし、その後に無効にします。

```
demo# debug captive-portal  
OK!  
demo# no debug captive-portal  
demo#
```

関連コマンド

[captive-portal \(390 ページ\)](#)

debug connect

802.11 接続のデバッグ メッセージを有効にします。

構文

```
debug connect  
no debug all
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

このデバッグ モジュールは、ワイヤレス クライアントから実行された 802.11 プロセスに関する情報、特に 802.11 のプローブ、認証、連結、認証解除、連結解除などを表示します。このデバッグには、このコマンドより新しい [station-log \(847 ページ\)](#) コマンドの使用を推奨します。

使用例

次の例は、802.11 接続のデバッグを有効にします。

```
demo# debug connect  
OK!  
demo# no debug connect
```

関連コマンド

[station-log \(847 ページ\)](#)

debug controller

コントローラのリアルタイム トレースを有効にします。

構文

```
debug controller
no debug controller
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

debug module コマンドでトレース ファシリティを指定した後に、**debug controller** コマンドでコントローラのトレースを有効にします。すべてのトレース情報はコントローラのコンソール ウィンドウに表示されます。

トレースを無効にするには、**no** フォームを使用します。**no** フォームでは、入力済みのデバッグ モジュール コマンドがすべて無効になります。

使用例

次のコマンドは、コントローラのトレースを有効にし、簡潔なデバッグ メッセージ リストを表示します。

```
controller# debug controller
Real-time trace display enabled for severity >= 0.
controller# [08/05 14:29:06.190] QOS: RsrcTopoMsgProcessor: topo-rm msg
type = 0, len= 52.

[08/05 14:29:24.230] QOS: RsrcTopoMsgProcessor: topo-rm msg type = 0, len=
52.
[08/05 14:29:27.047] SEC: ieee802_1x_receive: Set NAS-port to <2051>
[08/05 14:29:27.048] SEC: Received EAPOL-START frame from client
(00:0e:35:09:5d:5e).
[08/05 14:29:27.048] SEC: Sending EAPOL-EAP Request-Identity to client
(00:0e:35:09:5d:5e), ID (1).
```

関連コマンド

[debug module](#) (906 ページ)

debug eap

拡張認証プロトコルのデバッグ メッセージの表示を有効にします。

構文

```
debug eap  
no debug all
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

拡張認証プロトコルは、特定の認証機能ではなく、認証フレームワークです。EAP は共通の機能を実装し、認証機能のネゴシエーションを実行します。このような機能は、EAP メソッドと呼ばれ、現在は約 40 個のメソッドが存在します。EAP が、802.11 a/b/g ワイヤレス アクセス ポイントなど、802.1X 対応の NAS (ネットワーク アクセス サーバ) デバイスで起動されると、EAP メソッドは安全な認証機能を実装し、クライアントと NAS の間で安全な PMK (Pair-wise Master Key) をネゴシエーションできます。PMK は、TKIP または CCMP (AES ベース) による暗号化を使用するワイヤレスの暗号化セッションに使用できます。

使用例

次の例は、EAP のデバッグを有効にし、その後に無効にします。

```
demo# debug eap  
OK!  
# no debug all
```

関連コマンド

debug mac-filter

MAC フィルタリングのデバッグ メッセージの表示を有効にします。

構文

```
debug mac filter
no debug all
```

コマンド モード

特権 EXEC

デフォルト

なし

用途

使用例

次の例は、MAC フィルタのデバッグを有効にし、その後に無効にします。

```
demo# debug mac-filter
OK!
demo# no debug all
```

関連コマンド

[macfiltering](#) (438 ページ)

debug module

特定のファシリティのトレースを有効にします。

構文

```
debug module ip
debug module coord
debug modulesec
no debug module
```

ip	DHCP トレース ファシリティを指定します。
coord	クライアント アクセス ポイントの割り当てトレース ファシリティを指定します。
sec	セキュリティ トレース ファシリティを指定します。

コマンドモード

特権 EXEC

デフォルト

なし

用途

トレースを指定するには、**debug module** コマンドを使用します。**debug module** コマンドは、異なるキーワードで複数回実行できます。トレース ファシリティを指定したら、**debug controller** コマンドでコントローラのトレースを有効にして、コントローラのコンソールにトレース情報を送信します。**debug module coord** コマンドを実行した後に、マスクのパラメータを指定する必要があります。このため、コマンドは **debug module <xxx> mask <hex value>** です。

使用例

次のコマンドは、セキュリティおよび DHCP をトレース ファシリティとして指定します。

```
demo# debug module sec
OK!
demo# debug controller
Real-time trace display enabled for severity >= 0.
demo# [04/13 20:21:19.201] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:19.201] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:19.201] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
```

```

[04/13 20:21:25.211] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:25.211] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:25.211] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:31.231] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:31.231] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:31.231] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:37.242] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:37.242] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:37.242] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:43.261] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:43.262] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
demo# no debug controller
OK!
demo# no debug module sec
OK!
demo# debug module ip
OK!
demo# no debug module ip
OK!
demo#

```

このコマンドは、クライアント アクセス ポイントの割り当てトレース ファシリティを指定します。

```

default# sup-cli
default] tr coord
On? FlagValue Description
-----
00000001 Assign Manager
00000002 Beacon Manager
00000004 Configuration
00000008 Dispatcher

```

```

00000010 Handoff Manager
00000020 InterCell Manager
00000040 Main Thread
00000080 Nms Agent
00000100 Resource Manager
00000200 Time Estimator
00000400 Timer Scheduler
00000800 Topology Graph
00001000 Topology Manager
00004000 Memory Usage
00008000 Message Stats
00010000 Assign Manager Detail
00020000 Beacon Manager Detail
00040000 Configuration Detail
00080000 Dispatcher Detail
00100000 Handoff Manager Detail
00200000 InterCell Manager Detail
00400000 Main Thread Detail
00800000 Nms Agent Detail
01000000 Resource Manager Detail
02000000 Time Estimator Detail
04000000 Timer Scheduler Detail
08000000 Topology Graph Detail
10000000 Topology Manager Detail
20000000 General
40000000 Test
80000000 Customer
-----
00000000 = Current Mask
default]
default] exit
default# debug module coord mask 0000FFFF
OK!
default# sup-cli
default] tr coord
On? FlagValue Description
-----

```

```

* 00000001 Assign Manager
* 00000002 Beacon Manager
* 00000004 Configuration
* 00000008 Dispatcher
* 00000010 Handoff Manager
* 00000020 InterCell Manager
* 00000040 Main Thread
* 00000080 Nms Agent
* 00000100 Resource Manager
* 00000200 Time Estimator
* 00000400 Timer Scheduler
* 00000800 Topology Graph
* 00001000 Topology Manager
* 00004000 Memory Usage
* 00008000 Message Stats
00010000 Assign Manager Detail
00020000 Beacon Manager Detail
00040000 Configuration Detail
00080000 Dispatcher Detail
00100000 Handoff Manager Detail
00200000 InterCell Manager Detail
00400000 Main Thread Detail
00800000 Nms Agent Detail
01000000 Resource Manager Detail
02000000 Time Estimator Detail
04000000 Timer Scheduler Detail
08000000 Topology Graph Detail
10000000 Topology Manager Detail
20000000 General
40000000 Test
80000000 Customer
-----
0000ffff = Current Mask
default]

```

関連コマンド [debug controller \(903 ページ\)](#)

(diag-log) admin

この機能は、カスタマ サポートと一緒に作業する場合のみ使用してください。コントローラ、AP、ステーションの診断管理ステータスをオンまたはオフにします。

構文

```
admin station on
admin controller on
admin ap on
admin station on
admin station off
admin controller off
admin ap off
```

コマンド モード

configure terminal > diag-log

デフォルト

なし

用途

診断推論をオンにすると、**[Monitor] > [Diagnostics] > [Inferences]** の Web UI インターフェイス、または CLI コマンドの **show station counter** を使用して結果を確認できます。

使用例

以下のコマンドは、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
Meru01(config-diag-log)# admin ap on
Meru01(config-diag-log)# admin station on
```

次の例は、コマンドのオプションを表示します。

```
corpwifi# configure terminal
corpwifi(config)# diag-log
corpwifi(config-diag-log)# ?
admin          Manages diagnostics admin status.
config         Download diagnostics configuration file from url.
do             Executes an IOSCLI command.
end            Save changes, and return to privileged EXEC mode.
```


exit	Save changes, and return to global configuration
mode.	
restore	Restores to default diagnostics configuration file.

```
corpwifi(config-diag-log)# admin ?
ap                Configure admin mode for AP diagnostics.
controller        Configure admin mode for controller diagnostics.
station           Configure admin mode for station diagnostics.
corpwifi(config-diag-log)# admin ap ?
off               Turn off AP diagnostics.
on                Turn on AP diagnostics.
corpwifi(config-diag-log)# exit
```

関連コマンド

- [auto-report admin \(890 ページ\)](#)
- [auto-report send \(892 ページ\)](#)
- [\(diag-log\) config \(912 ページ\)](#)
- [\(diag-log\) restore \(914 ページ\)](#)
- [show auto-report-config \(953 ページ\)](#)

(diag-log) config

この機能は、カスタマ サポートと一緒に作業する場合のみ使用してください。URL から診断設定ファイルをダウンロードします。

構文

config <url>

コマンドモード

configure terminal > diag-log

デフォルト

なし

用途

診断設定の変更は、フォーティネット サポートのみが実行できます。フォーティネット サポートが診断設定ファイルを変更したら、**config** コマンドでユーザがそのファイルを実装できます。[\(diag-log\) restore \(914 ページ\)](#) コマンドでデフォルト設定に戻すことができます。

使用例

次の例は、cwon:cwon@182.27.0.79 から設定ファイルをダウンロードします。

```
Meru01# configure terminal
Meru01(config)# diag-log
Meru01(config-diag-log)# config cwon:cwon@182.27.0.79
```

次の例は、コマンドのオプションを表示します。

```
corpwifi# configure terminal
corpwifi(config)# diag-log
corpwifi(config-diag-log)# ?
admin                Manages diagnostics admin status.
config               Download diagnostics configuration file from url.
do                  Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
restore              Restores to default diagnostics configuration file.
corpwifi(config-diag-log)# config ?
<url>                The url of downloading diagnostics configuration
file.
```

```
corpwifi(config-diag-log)# config
```

関連コマンド

- [auto-report admin](#) (890 ページ)
- [auto-report send](#) (892 ページ)
- [\(diag-log\) admin](#) (910 ページ)
- [\(diag-log\) restore](#) (914 ページ)
- [show auto-report-config](#) (953 ページ)

(diag-log) restore

この機能は、カスタマ サポートと一緒に作業する場合のみ使用してください。デフォルトの診断設定ファイルに戻します。

構文

restore <filename>

コマンド モード

configure terminal > diag-log

デフォルト

なし

用途

診断設定の変更は、フォーティネット サポートのみが実行できます。フォーティネット サポートが診断設定ファイルを変更してユーザに送信し、[\(diag-log\) config \(912 ページ\)](#) コマンドでそのファイルをユーザが実装した場合は、**restore** コマンドを使用することで、デフォルト設定に戻すことができます。

使用例

次の例は、デフォルト ファイル diag-controller.conf に戻します。

```
default# configure terminal
default (config)# diag-log
default (config-diag-log)# restore diag-controller.conf
diag-log restoring diag-controller configuration now...
done
```

次の例は、コマンドのオプションを表示します。

```
corpwifi# configure terminal
corpwifi(config)# diag-log
corpwifi(config-diag-log)# ?
admin                Manages diagnostics admin status.
config               Download diagnostics configuration file from url.
do                   Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
restore              Restores to default diagnostics configuration file.
corpwifi(config-diag-log)# restore ?
```

<file-name> The file name of restoring default configuration.

関連コマンド

- [auto-report admin](#) (890 ページ)
- [auto-report send](#) (892 ページ)
- [\(diag-log\) admin](#) (910 ページ)
- [\(diag-log\) config](#) (912 ページ)
- [show auto-report-config](#) (953 ページ)

diagnostics

システム診断データを収集し、圧縮ログ ファイルに出力します。

構文

diagnostics

コマンド モード

特権 EXEC

デフォルト

なし

用途

diagnostics コマンドは、WLAN 内のコントローラおよびすべての AP からシステム情報を収集し、圧縮および保存されたログ ファイルにデータを出力します。サポートにこのファイルを送信して、システムの問題をデバッグできます。100 台以上の AP を含む WLAN では、このコマンドが完了するまでに、10 分以上かかる可能性があります。

圧縮ファイルの名前は、*year.month.day.hour.minutes* (meru-gather-2007.09.24.20.59.tar.gz) を含む日付スタンプを統合しており、images ディレクトリに保存されます。後で、**copy ftp** コマンドを使用して、サポートにファイルを送信できるサーバにファイルを移動できます。

使用例

```
controller# diagnostics
Cleaning up previous gather data
Getting process information ...
Getting system log information ...
Getting kernel information ...
Getting network information ...
Getting software information ...
Getting version information ...
Getting disk information ...
Getting Meru data ...
Getting high availability information ...
Data gathering phase complete
```

```
images/meru-gather-2007.09.24.20.59.tar.gz created
Use the ftp option of the cli command to move this file off the machine
```

関連コマンド

- [diagnostics-ap \(918 ページ\)](#)
- [diagnostics-controller \(920 ページ\)](#)

diagnostics-ap

指定した AP の診断データを収集し、圧縮ログ ファイルに出力します。

構文

```
diagnostics-ap all
diagnostics-ap <ap-id>
```

ip-id AP 番号

コマンド モード

特権 EXEC

デフォルト

なし

用途

diagnostics-ap コマンドは、コントローラから情報を収集し、保存される前の圧縮されたログ ファイルにデータを出力します。サポートに圧縮ログ ファイルを送信して、システムの問題をデバッグできます。

圧縮ファイルの名前は、*year.month.day.hour.minutes* (meru-gather-2007.09.24.20.57.tar.gz) を含む日付スタンプを統合しており、images ディレクトリに保存されます。後で、**copy ftp** コマンドを使用して、サポートにファイルを送信できるサーバにファイルを移動できます。

このコマンドは **diagnostics** コマンドに似ていますが、AP のみの情報を収集します。したがって、**diagnostics** コマンドより短時間で完了します。

使用例

```
controller# diagnostics-ap
Getting process information ...
Getting system log information ...
Getting kernel information ...
Getting network information ...
Getting software information ...
Getting version information ...
Getting disk information ...
Getting Meru data ...
Getting high availability information ...
Data gathering phase complete
```


images/meru-gather-2007.09.24.20.57.tar.gz created

Use the ftp option of the cli command to move this file off the machine

関連コマンド

- [diagnostics](#) (916 ページ)
- [diagnostics-controller](#) (920 ページ)

diagnostics-controller

現在のコントローラの診断データを収集し、圧縮ログ ファイルに出力します。

構文

`diagnostics-controller`

コマンド モード

特権 EXEC

デフォルト

なし

用途

diagnostics-controller コマンドは、コントローラから情報を収集し、圧縮および保存されたログ ファイルにデータを出力します。サポートにこのファイルを送信して、システムの問題をデバッグできます。

圧縮ファイルの名前は、*year.month.day.hour.minutes* (meru-gather-2007.09.24.20.57.tar.gz) を含む日付スタンプを統合しており、*images* ディレクトリに保存されます。後で、**copy ftp** コマンドを使用して、サポートにファイルを送信できるサーバにファイルを移動できます。

このコマンドは **diagnostics** コマンドに似ていますが、コントローラのための情報を収集するため、短時間で完了します。

使用例

```
controller# diagnostics-controller
Getting process information ...
Getting system log information ...
Getting kernel information ...
Getting network information ...
Getting software information ...
Getting version information ...
Getting disk information ...
Getting Meru data ...
Getting high availability information ...
Data gathering phase complete
```

```
images/meru-gather-2007.09.24.20.57.tar.gz created
Use the ftp option of the cli command to move this file off the machine
```

関連コマンド

- [diagnostics](#) (916 ページ)
- [diagnostics-ap](#) (918 ページ)

packet-capture-profile

このパケット捕捉コマンドは、既存のプロファイルを更新するか、新しいプロファイルを作成し、その後に pcap モードに入ります。

構文

```
packet-capture-profile <profile name>  
no packet capture profile
```

コマンドモード

configure terminal > packet-capture-profile

デフォルト

なし

用途

このコマンドは、既存のパケット捕捉プロファイルを更新するか、新しいプロファイルを作成します。同時に、pcap モードを起動します。pcap モードでは、次のパケット捕捉コマンドを使用できます。

- [\(packet capture profile\) ap-list \(925 ページ\)](#) コマンドで、パケットを送信する AP のリストを設定します。
- [\(packet-capture-profile\) enable-profile \(934 ページ\)](#) コマンドで、プロファイル (packet-capture-profile コマンドで作成) を有効にします。
- [\(packet capture profile\) rate-limiting \(941 ページ\)](#) コマンドで、ap-list の AP で実行されるパケット トランケーションの長さを設定します。
- [\(packet capture profile\) rate-limiting \(941 ページ\)](#) コマンドで、ap-list の AP で実行されるレート制限を設定します。
- [show auto-report-config \(953 ページ\)](#) コマンドで、情報が流れる方向に基づいて、送信されるパケットを指定します。現在は、rx のみを使用できます。
- [\(packet capture profile\) token-bucket-rate \(946 ページ\)](#) コマンドで、トークン バケット レートを設定します。
- [\(packet capture profile\) token-bucket-size \(949 ページ\)](#) コマンドで、トークン バケット サイズを設定します。
- [\(packet capture profile\) mode \(938 ページ\)](#) コマンドで、パケットの宛先を設定します。
- [packet-capture-profile \(922 ページ\)](#) コマンドで、フィルタを適用します。
- [\(packet capture profile\) interface list \(937 ページ\)](#) コマンドで、インターフェイス リストを適用します。

上記のコマンドで生成されたプロファイルは、コントローラから AP にダウンロードされる NMS の残りの設定と一緒に、AP にダウンロードされます。また、AP は設定に従って転送

を開始します。Wireshark を使用する場合は、フォーティネットのヘッダを認識するフォーティネットのカスタム バージョンをサポートからオプションで入手できます。

使用例

次の例は、すべてのコマンド オプションを表示し、プロファイル LM を作成し、転送モードを I3 に設定し、ap-list を 16 に設定します。

```
MC3K-1# configure terminal
MC3K-1(config)# packet-capture-profile ?
ap-list                Set the AP list seperated by commas or all APs.
capture-sibling-frames Enable Capture frames sent by other APs in the
network.
enable-profile          Enable this packet capture profile.
end                     Save changes, and return to privileged EXEC mode.
exit mode.              Save changes, and return to global configuration
filter                  Set the filter string.
interface-list          Set the interface list.
mode                    Set the transmit mode to layer2 or layer3.
no                       Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting           Enable RateLimiting.
rate-limiting-mode      Set the rate limit per station or cumulative.
rxtx                    Set the traffic snort to tx or rx or both.
token-bucket-rate       Set the token-bucket-rate.
MC3K-1(config)# packet-capture-profile LM
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)# enable-profile
MC3K-1(config-pcap)# exit
MC3K-1(config)# exit
MC3K-1# show packet-capture-profile LM
AP Packet Capture profiles

Packet Capture Profile Name      : LM
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3              : l3
```

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

関連コマンド

- [\(packet capture profile\) ap-list \(925 ページ\)](#)
- [\(packet-capture-profile\) enable-profile \(934 ページ\)](#)
- [\(packet capture profile\) mode \(938 ページ\)](#)
- [\(packet capture profile\) rate-limiting \(941 ページ\)](#)
- [\(packet capture profile\) rate-limiting \(941 ページ\)](#)
- [\(packet capture profile\) token-bucket-rate \(946 ページ\)](#)
- [\(packet capture profile\) token-bucket-size \(949 ページ\)](#)

(packet capture profile) ap-list

パケット捕捉のために、パケットの転送元の AP のリストを設定します。

構文

```
ap-list <apid>,<apid>,<apid>  
no ap list
```

apid パケットの転送元の AP ID のカンマ区切りリスト
 です。

コマンド モード

configure terminal > packet-capture-profile

デフォルト

なし

用途

このコマンドは、[\(packet capture profile\) mode \(938 ページ\)](#) コマンドで指定する、L2/L3 モードで宛先ハードウェアにパケットを転送する AP ID の入力に使用されます。これは、[packet-capture-profile \(922 ページ\)](#) モードのサブセット コマンドです。

使用例

次の例は、LM プロファイルを作成し、AP 16 にパケットの転送を指示します。

```
MC3K-1#  
MC3K-1# configure terminal  
MC3K-1(config)# packet-capture-profile LM  
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 LM  
AP Packet Capture profiles  
  
Packet Capture Profile Name               : LM  
Packet Capture profile Enable/Disable    : off  
Modes Allowed L2/L3                       : l3  
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
```

関連コマンド

- [packet-capture-profile \(922 ページ\)](#)
- [\(packet capture profile\) mode \(938 ページ\)](#)

(packet capture profile) capture-sibling-frames

このパケット捕捉コマンドを使用すると、ネットワークの他の AP300/AP200 から送信されるフレームを捕捉できます。

構文

```
capture-sibling-frames
no capture-sibling-frames
```

コマンドモード

configuration > packet capture

デフォルト

オフ

用途

capture-sibling-frames コマンドを使用すると、AP300/AP200 が他の AP から送信されたフレームを捕捉できます。たとえば、ラップトップを持っておらず、どのパケットを AP が受信するかを把握したい場合は、シブリングに送信されるパケットをリスンするよう、2 つ目の AP に指示します。Location Manager などのアプリケーションのシブリング データをオフにする (またはフィルタする) こともでき、パフォーマンス向上につながります。このコマンドは、仮想セルあり / なし、仮想ポートあり / なしで動作し、AP200 と AP300 の両方に利用できます。

使用例

次の例は、シブリング フレームの捕捉を無効にし、その後有効にします。

```
default(config)# exit
default# sh packet-capture-profile test
AP Packet Capture profiles
Packet Capture Profile Name           : test
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : l3
Destination IP Address                 : 0.0.0.0
UDP Destination Port                   : 0
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 :
Extended Filter String :
Interface List :
Packet Truncation Length : 82
Rate Limiting : off
Capture frames sent by other APs in the network : on

```

```

default# configure terminal
default(config)# packet-capture-profile test
default(config-pcap)# no capture-sibling-frames
default(config-pcap)# end
default# sh packet-capture-profile test
AP Packet Capture profiles
Packet Capture Profile Name : test
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3 : 13
Destination IP Address : 0.0.0.0
UDP Destination Port : 0
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 :
Extended Filter String :
Interface List :
Packet Truncation Length : 82
Rate Limiting : off
Capture frames sent by other APs in the network : off

```

次の例では、**test** という名前のプロファイルを作成し、シブリング フレームの捕捉を有効にし、Location Manager の捕捉を設定します。プロファイルはまだ有効になっていません。

```

default# configure terminal
default(config)# packet-capture-profile test
default(config-pcap)# capture-sibling-frames
default(config-pcap)# end
default# sh packet-capture-profile test

```

```

AP Packet Capture profiles
Packet Capture Profile Name           : test
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : 13
Destination IP Address                 : 0.0.0.0
UDP Destination Port                   : 0
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                           :
Extended Filter String                 :
Interface List                         :
Packet Truncation Length               : 82
Rate Limiting                          : off
Capture frames sent by other APs in the network : on

```

Configuration of Capture Sibling frames field in Packet Capture:

Configuring packet capture profile:

```

-----
Default# configure terminal
Default(config)# packet-capture-profile LM1
Default(config-pcap)# mode 13 destination-ip 172.18.81.11 port 17777
Default(config-pcap)# ap-list 2,3,4,5,6
Default(config-pcap)# enable-profile
Default(config-pcap)# end

```

Controller Output:

```

-----
Default# sh packet-capture-profile LM1
AP Packet Capture profiles

Packet Capture Profile Name           : LM1
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3                   : 13

```

```

Destination IP Address           : 172.18.81.11
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                     : 2,3,4,5,6
Extended Filter String           :
Interface List                   :
Packet Truncation Length         : 82
Rate Limiting                    : off
Capture frames sent by other APs in the network : on
Default#

```

AP Output:

ap 2> sniff profile show LM1

```

=====
Name           : LM1
Enabled        : enable
Current State = : Rx
mode           : L3
L2: Destination MAC (L2) : 00:00:00:00:00:00
L3: IP address   : 172.18.81.11
L3: IP port     : 17777
Format         : PPI
Maximum length, truncated: 82
Token bucket rate      : 10
Token bucket size     : 10
Token bucket interval  : 100000
Rate limit            : off
Rate limit mode       : station
Filter              : All packets pass
=====
Radio mode          : 1

```

=====

ap 2>

コントローラ出力の “capture frames sent by other APs in the network” は、シブリング フレーム (フォーティネット OUI フレーム) の捕捉を開始または停止するオプションです。AP のフィルタ オプションと同様に、送信されるパケットとフィルタされるオプションが表示されます。

次の例では、シブリング フレーム捕捉オプションをオフにし、プロファイルを有効にします。

```
Default# configure terminal
Default(config)# packet-capture-profile LM1
Default(config-pcap)# ?
ap-list                Set the AP list seperated by commas.
capture-sibling-frames Enable Capture frames sent by other APs in the
network.
enable-profile          Enable this packet capture profile.
end                     Save changes, and return to privileged EXEC mode.
exit mode.              Save changes, and return to global configuration
filter                  Set the filter string.
interface-list          Set the interface list.
mode                    Set the transmit mode to layer2 or layer3.
no                       Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting           Enable RateLimiting.
rate-limiting-mode      Set the rate limit per station or cumulative.
rxtx                    Set the traffic snort to tx or rx or both.
token-bucket-rate       Set the token-bucket-rate.
token-bucket-size       Set the token-bucket-size.
Default(config-pcap)# no capture-sibling-frames
Default(config-pcap)# enable-profile
Default(config-pcap)# end
```

Controller output:

```

-----
Default# sh packet-capture-profile LM1
AP Packet Capture profiles

Packet Capture Profile Name           : LM1
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3                   : L3
Destination IP Address                 : 172.18.81.11
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                           : 2,3,4,5,6
Extended Filter String                 :
Interface List                         :
Packet Truncation Length               : 82
Rate Limiting                         : off
Capture frames sent by other APs in the network : off
Default#

```

AP Output:

```

-----
ap 2> sniff profile show LM1

```

```

=====
Name           : LM1
Enabled        : enable
Current State = : Rx
mode           : L3
L2: Destination MAC (L2) : 00:00:00:00:00:00
L3: IP address   : 172.18.81.11
L3: IP port     : 17777
Format         : PPI
Maximum length, truncated: 82
Token bucket rate      : 10

```

```

Token bucket size      : 10
Token bucket interval  : 100000
Rate limit             : off
Rate limit mode        : station
Filter :
    OUI [ 0: c:e6]
=====

=====

Radio mode             : 1
=====

ap 2>

```

このオプションを OFF にすると、ソース アドレス 00:0c:e6 (meru) / 00:12:f2 (foundry) と Per Station BSSID のパケットが AP によって設定されたサーバに転送されなくなります。

関連コマンド

- [packet-capture-profile \(922 ページ\)](#)
- [\(packet capture profile\) rate-limiting \(941 ページ\)](#)
- [show packet-capture-profile \(963 ページ\)](#)

(packet-capture-profile) enable-profile

現在のパケット捕捉プロファイルを有効にします。

構文

```
enable-profile  
no enable-profile
```

コマンド モード

configure terminal > packet-capture-profile <name>

デフォルト

なし

用途

packet-capture-profile を有効または無効にするには、このコマンドを使用します。このコマンドは、[\(packet capture profile\) mode \(938 ページ\)](#) のサブセットコマンドです。

使用例

次の例では、シブリング フレーム捕捉オプションをオフにし、その後でプロファイルを有効にします。

```
Default# configure terminal  
Default(config)# packet-capture-profile LM1  
Default(config-pcap)# ?  
ap-list                Set the AP list seperated by commas.  
capture-sibling-frames Enable Capture frames sent by other APs in the  
network.  
enable-profile          Enable this packet capture profile.  
end                     Save changes, and return to privileged EXEC mode.  
exit mode.             Save changes, and return to global configuration  
filter                  Set the filter string.  
interface-list          Set the interface list.  
mode                    Set the transmit mode to layer2 or layer3.  
no                      Delete/reset Pcap profile parameters.  
packet-truncation-length Set the packet-truncation-length.  
rate-limiting           Enable RateLimiting.  
rate-limiting-mode      Set the rate limit per station or cumulative.  
rxtx                    Set the traffic snort to tx or rx or both.
```



```
token-bucket-rate      Set the token-bucket-rate.  
token-bucket-size      Set the token-bucket-size.  
Default(config-pcap)# no capture-sibling-frames  
Default(config-pcap)# enable-profile  
Default(config-pcap)# end
```

関連コマンド

- [\(packet capture profile\) ap-list \(925 ページ\)](#)
- [packet-capture-profile \(922 ページ\)](#)

(packet capture profile) filter

捕捉する MAC アドレス フィルタを設定するパケット捕捉コマンドです。このコマンドは現在、使用できません。

(packet capture profile) interface list

捕捉するインターフェイス リストを設定するパケット捕捉コマンドです。このコマンドは現在、使用できません。

(packet capture profile) mode

AP300 および AP200 の現在のパケット捕捉プロファイルの伝送モードをレイヤ 2 またはレイヤ 3 に設定するパケット捕捉コマンドです。

構文

```
mode 12 destination-mac xx:xx:xx:xx:xx:xx
mode 13 destination-ip x.x.x.x port <port number>
```

コマンドモード

```
configure terminal > packet-capture-profile
```

デフォルト

なし

用途

パケット捕捉には、L2 および L3 の 2 つのモードを使用できます。これらの情報は、指定された L2 または L3 のいずれかのモードを使用してパケットを宛先に転送する場合に、AP によって使用されます。これは、[\(packet capture profile\) mode \(938 ページ\)](#) のサブセットコマンドです。

使用例

次の例は、プロファイル LM を作成し、伝送モードを L3 に設定します。

```
MC3K-1# configure terminal
MC3K-1(config)# packet-capture-profile LM
MC3K-1(config-pcap)# mode 13 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 LM
AP Packet Capture profiles
```

```
Packet Capture Profile Name           : LM
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

関連コマンド [packet-capture-profile \(922 ページ\)](#)

(packet capture profile) packet-truncation-length

AP がハードウェア デバイスに転送するパケットの長さを設定します。

構文

`packet-truncation-length <number>`

`number` バイト単位のパケットの長さ

コマンドモード

`configure terminal > packet-capture-profile`

デフォルト

なし

用途

このコマンドは、AP がハードウェア デバイスに転送するパケットの長さを設定します。AP は、宛先ハードウェアにパケットを転送する前に、すべてのパケットの長さをこの値に減らします。Location Manager が動作するには、パケットの長さが 82 バイト以上である必要があります。これは、([packet capture profile](#)) *mode* (938 ページ) のサブセット コマンドです。

使用例

次のコマンドは、パケット トランケーションの長さを 83 に設定します。

```
demo# configure terminal
demo(config)# packet-capture-profile MWP
demo(config-pcap)# packet-truncation-length 83
```

関連コマンド

[packet-capture-profile](#) (922 ページ)

(packet capture profile) rate-limiting

現在のパケット捕捉プロファイルの速度制限をオン / オフにするパケット捕捉コマンドです。

構文

```
rate-limiting
no rate-limiting
```

コマンドモード

configure terminal > packet-capture-profile

デフォルト

なし

用途

このコマンドを使用して、速度制限をオンにします。速度制限を **on** にすると、[\(packet capture profile\) token-bucket-rate \(946 ページ\)](#) コマンドの速度を使用して、パケットが転送されます。[\(packet capture profile\) ap-list \(925 ページ\)](#) コマンドで指定された各 AP が、トークン パケット速度で設定された最大パケットを毎秒転送します。これは、[packet-capture-profile \(922 ページ\)](#) モードのサブセット コマンドです。

使用例

次の例では、**show** コマンドでパケット捕捉プロファイルの速度制限が **on** になっていることを確認し、その後に速度制限を **off** にします。

```
default# show packet-capture-profile
Profile Name          L2/L3 Mode      Destination IP  Destination
MAC   Rx/Tx/Both      Rate Limiting  AP Selection
testing                    13              0.0.0.0
00:00:00:00:00:00 rx      station
AP Packet Capture profiles(1 entry)
default# configure terminal
default(config)# no packet-capture-profile testing
default(config)# exit
```

関連コマンド

- [\(packet capture profile\) token-bucket-rate \(946 ページ\)](#)
- [\(packet capture profile\) ap-list \(925 ページ\)](#)
- [packet-capture-profile \(922 ページ\)](#)
- [\(packet capture profile\) token-bucket-rate \(946 ページ\)](#)

- [\(packet capture profile\) rate-limiting-mode \(943 ページ\)](#)

(packet capture profile) rate-limiting-mode

現在のパケット捕捉プロファイルの速度制限に、station (ステーション単位) または cumulative を設定します。本リリースでは、ステーション単位が唯一のオプションです。

構文

rate-limiting station
rate-limiting cumulative (リリース 4.0 では実装されていません)

station	速度制限モードをステーション単位に設定します
cumulative	ベータ テストでは機能しません

コマンドモード

グローバル設定

デフォルト

なし

用途

現在、**station** のみが実装されています。速度制限のコマンドを使用して、パケット捕捉プロファイルの速度制限を有効にできます。速度制限モードによって、モード設定に基づき、ステーションまたは AP あたりのどちらで制限するかが決定します。**station** に設定するとステーションあたりの速度制限になり、**AP** に設定すると AP あたりの速度制限になります。制限は Token Bucket Rate と Token Bucket Size に基づき、速度によって転送できるパケットの数が決定し、メモリによってキャッシュできるパケットの数が決定します。

使用例

次の例は、Test という名前のパケット捕捉プロファイルをステーションあたりの速度制限モードに設定します。

```
ramecntrl(config)# packet-capture-profile Test
ramecntrl(config-pcap)# rate-limiting-mode station
ramecntrl(config-pcap)# exit
ramecntrl(config)# exit
```

関連コマンド

- [\(packet capture profile\) rate-limiting \(941 ページ\)](#)
- [show packet-capture-profile \(963 ページ\)](#)

(packet capture profile) rxtx

現在のパケット捕捉プロファイルのトラフィック侵入検出を、受信、送信、または送受信に設定します。

構文

```
rxtx rx-only  
rxtx tx-only  
rxtx both
```

rx-only	受信トラフィックのみ - 現在はこの設定のみが有効です。
tx-only	送信トラフィックのみ - ベータ テストでは現在、この設定は動作しません。
both	送信 / 受信トラフィック - ベータ テストでは現在、この設定は動作しません。

コマンド モード

設定

デフォルト

rx-only

用途

現段階では、トラフィック侵入検出を受信トラフィックの監視 (rx-only) に設定します。これは、[\(packet capture profile\) mode \(938 ページ\)](#) のサブセット コマンドです。

使用例

次のコマンドは、MWP という名前のパケット捕捉プロファイルのトラフィック侵入検出を rx-only に設定します。

```
demo# configure terminal  
demo(config)# packet-capture-profile MWP  
default(config-pcap)# ?  
ap-list          Set the AP list seperated by commas.  
capture-sibling-frames Enable Capture frames sent by other APs in the  
network.  
enable-profile   Enable this packet capture profile.  
end              Save changes, and return to privileged EXEC mode.  
exit             Save changes, and return to global configuration  
mode.  
filter           Set the filter string.
```

<code>interface-list</code>	Set the interface list.
<code>mode</code>	Set the transmit mode to layer2 or layer3.
<code>no</code>	Delete/reset Pcap profile parameters.
<code>packet-truncation-length</code>	Set the packet-truncation-length.
<code>rate-limiting</code>	Enable RateLimiting.
<code>rate-limiting-mode</code>	Set the rate limit per station or cumulative.
<code>rxtx</code>	Set the traffic snort to tx or rx or both.
<code>token-bucket-rate</code>	Set the token-bucket-rate.
<code>token-bucket-size</code>	Set the token-bucket-size.
<code>default(config-pcap)# rxtx ?</code>	
<code>both</code>	Both Rx and Tx
<code>rx-only</code>	Rx only
<code>tx-only</code>	Tx only
<code>demo(config-pcap)# rxtx rx-only</code>	

関連コマンド [packet-capture-profile \(922 ページ\)](#)

(packet capture profile) token-bucket-rate

現在のパケット捕捉プロファイルのトークン バケット レートを設定します。

構文

```
token-bucket-rate <rate>  
no token-bucket-rate
```

rate 秒あたりの宛先に転送されるパケットの数。ゼロ以外の値です。

コマンドモード

configure terminal > packet-capture-profile

デフォルト

なし

用途

token-bucket-rate は、[\(packet capture profile\) rate-limiting \(941 ページ\)](#) が on に設定されている場合に宛先に毎秒転送されるパケット数 (ゼロ以外) を制限し、token-bucket-rate 値は、転送できる毎秒の最大パケット数を AP に指示します。token-bucket-rate は常に、[\(packet capture profile\) token-bucket-size \(949 ページ\)](#) よりも低い値である必要があります。[\(packet capture profile\) rate-limiting \(941 ページ\)](#) を on にすると、AP から転送されるパケットの数が token-bucket-rate で設定されたパケットの数に制限されます。

使用例

次の例は、LM という名前のパケット捕捉プロファイルに、使用可能なすべてのパラメータを設定します。トークン バケット レートは 1000 に設定されます。

```
MC3K-1(config-pcap)#  
MC3K-1(config)# packet-capture-profile LM  
MC3K-1(config-pcap)# ?  
ap-list                      Set the AP list seperated by commas.  
capture-sibling-frames      Enable Capture frames sent by other APs in the  
network.  
enable-profile               Enable this packet capture profile.  
end                           Save changes, and return to privileged EXEC mode.  
exit                         Save changes, and return to global configuration  
mode.  
filter                       Set the filter string.  
interface-list               Set the interface list.
```

```

mode                Set the transmit mode to layer2 or layer3.
no                  Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting       Enable RateLimiting.
rate-limiting-mode   Set the rate limit per station or cumulative.
rxtx                Set the traffic snort to tx or rx or both.
token-bucket-rate    Set the token-bucket-rate.
token-bucket-size    Set the token-bucket-size.
MC3K-1(config-pcap)#
MC3K-1(config-pcap)# tok
token-bucket-rate token-bucket-size
MC3K-1(config-pcap)# token-bucket-rate 1000
MC3K-1(config-pcap)# tok
token-bucket-rate token-bucket-size
MC3K-1(config-pcap)# token-bucket-size 10000
MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 17777
MC3K-1(config-pcap)# rate-limiting
MC3K-1(config-pcap)# exit
MC3K-1(config)# exit
MC3K-1# show packet-capture-profile LM
AP Packet Capture profiles
Packet Capture Profile Name           : LM
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                    : 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                       : 1000
Token Bucket Size                       : 10000
AP Selection                           : 16
Extended Filter String                  :
Interface List                          :
Packet Truncation Length                : 82
Rate Limiting                           : on
Capture frames sent by other APs in the network : on

```

MC3K-1#

関連コマンド

- [\(packet capture profile\) rate-limiting \(941 ページ\)](#)
- [\(packet capture profile\) token-bucket-size \(949 ページ\)](#)

(packet capture profile) token-bucket-size

ワイヤレス パケットが格納された後に宛先に転送されるバケットの深さを設定します。

構文

```
token-bucket-size <size>  
no token-bucket-size
```

size	ワイヤレス パケットが格納された後に宛先に転送されるバケットの深さです。token-bucket-rate より大きいゼロ以外の値を指定します。
------	--

コマンドモード

configuration mode > packet-capture-profile

デフォルト

なし

用途

ワイヤレス パケットが格納された後に宛先に転送されるバケットの深さを設定します。[\(packet capture profile\) token-bucket-rate \(946 ページ\)](#) の値は常に、token-bucket-size よりも小さい値である必要があります。[\(packet capture profile\) rate-limiting \(941 ページ\)](#) が on の場合、AP から転送されるパケット数は、[\(packet capture profile\) token-bucket-rate \(946 ページ\)](#) で設定されたパケット数に制限されます。

使用例

次の例は、LM という名前のパケット捕捉プロファイルに、使用可能なすべてのパラメータを設定します。トークンバケットサイズは 10000 に設定されます。

```
MC3K-1(config-pcap)#  
MC3K-1(config)# packet-capture-profile LM  
MC3K-1(config-pcap)# ?  
ap-list                Set the AP list seperated by commas.  
capture-sibling-frames Enable Capture frames sent by other APs in the  
network.  
enable-profile          Enable this packet capture profile.  
end                    Save changes, and return to privileged EXEC mode.  
exit                   Save changes, and return to global configuration  
mode.  
filter                 Set the filter string.
```

```

interface-list      Set the interface list.
mode                Set the transmit mode to layer2 or layer3.
no                  Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting       Enable RateLimiting.
rate-limiting-mode  Set the rate limit per station or cumulative.
rxtx                Set the traffic snort to tx or rx or both.
token-bucket-rate   Set the token-bucket-rate.
token-bucket-size   Set the token-bucket-size.
MC3K-1(config-pcap)#
MC3K-1(config-pcap)# tok
token-bucket-rate token-bucket-size
MC3K-1(config-pcap)# token-bucket-rate 1000
MC3K-1(config-pcap)# tok
token-bucket-rate token-bucket-size
MC3K-1(config-pcap)# token-bucket-size 10000
MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 17777
MC3K-1(config-pcap)# rate-limiting
MC3K-1(config-pcap)# exit
MC3K-1(config)# exit
MC3K-1# show packet-capture-profile LM
AP Packet Capture profiles
Packet Capture Profile Name           : LM
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : 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                      : 1000
Token Bucket Size                      : 10000
AP Selection                           : 16
Extended Filter String                 :
Interface List                         :
Packet Truncation Length               : 82
Rate Limiting                          : on

```


Capture frames sent by other APs in the network : on
MC3K-1#

関連コマンド

- [\(packet capture profile\) rate-limiting \(941 ページ\)](#)
- [\(packet capture profile\) token-bucket-rate \(946 ページ\)](#)

remote-log

ログを置いておくリモート サイトを設定します。

構文

```
remote-log start smb <mount-point> <workgroup> <username>  
remote-log stop smb <mount-point> <workgroup> <username>
```

<i>mount-point</i>	リモート ディスクのマウント ポイント (<i>//hostname/sharename</i>) を指定します。
<i>workgroup</i>	ユーザにリモート ログの設定を作成する権限が付与されているワークグループを指定します。
<i>username</i>	リモート ログの設定を作成するユーザの名前を指定します。

コマンド モード

特権 EXEC

デフォルト

なし

用途

remote-log コマンドは、ネットワーク共有ディスクにすべてのシステム ログをコピーできます。デフォルトでは、ログ エントリはコントローラのフラッシュ カードに保存されますが、容量が限られます。結果的に、一定の容量に達すると、新しいエントリの保存容量を確保するために、ログ エントリが消去されることになります。ネットワーク共有を指定することで、ログされたエントリ of 全履歴を保存できます。

リモート ログを設定するには、**remote-log start smb** コマンドを使用し、オプションで、ネットワーク マウント ポイント、ワークグループ、およびユーザ名を追加します。ユーザ名のパスワードを入力するよう要求されます。リモート ログを停止してネットワーク共有をアンマウントするには、同じコマンド パラメータを使用しますが、**start** ではなく、**stop** キーワードを使用します。

ネットワーク共有に正しく接続されていることを確認します。コマンド ラインに指定しないと、ワークグループとユーザ名を入力するよう要求されます。

使用例

次のコマンドは、engineering ワークグループの admin ユーザに、共有ディスク IT を使用してサーバ maple にリモート ログを作成することを許可します。

```
controller# remote-log start smb //maple/IT engineering admin  
controller#
```

show auto-report-config

auto-report コマンド **send** と **admin** で作成した auto-report (自動レポート) 設定を表示します。

構文

show auto-report-config

コマンドモード

設定モード > auto-report モード

デフォルト

なし

用途

このコマンドを使用して、auto-report で使用される設定済みの値を表示します。

使用例

以下の例では、`cwon:cwon@172.27.0.79/diagagent.conf` に 1 時間ごとにレポートを送信します。最後のコマンドが **show auto-report-config** コマンドです。

```
Meru01#configure terminal
Meru01(config)# auto-report
Meru01(config-auto-report)# ?
```

```
adminConfigures administration mode for auto-reporting
do Executes an IOSCLI command
endSaves changes and returns to privileged exec mode
exitSaves changes and returns to global configuration mode
sendUploads log files to named URL once or periodically
```

```
Meru01(config-auto-report)# send ftp://cwon:cwon@172.27.0.79/
diagagent.conf 1
Meru01(config-auto-report)# admin on
Meru01(config-auto-report)# show auto-report-config
```

```
Administration Statuson
Auto-reporting Intervalevery hour
Auto-reporting URLcwon:cwon@172.27.0.79
```

関連コマンド

- [auto-report admin](#) (890 ページ)
- [auto-report send](#) (892 ページ)
- [\(diag-log\) admin](#) (910 ページ)
- [\(diag-log\) config](#) (912 ページ)
- [\(diag-log\) restore](#) (914 ページ)

show cef

ArcSight の Common Event Format (CEF) ログを表示します。

構文

show auto-report config

コマンド モード

EXEC モード

デフォルト

なし

用途

このコマンドを使用して、CEF ログに使用される設定済みの値を表示します。

使用例

次の例は、CEF ロギング オプションを表示し、さらに、現在の CEF 設定を表示します。

```
BangWiFi36# configure terminal
BangWiFi36(config)# cef ?
disable          Disables Common Event Format Logging Feature.
enable           Enables Common Event Format Logging Feature.
server-ip        Enter Server Details
BangWiFi36(config)# exit
BangWiFi36#
BangWiFi36# show cef
CEF Logging is disabled
CEF Logging Host is not configured
BangWiFi36#
```

show debug

デバッグ情報を表示します。

構文

`show debug`

コマンド モード

特権 EXEC

デフォルト

なし

用途

このコマンドを使用して、デバッグ情報を表示します。

使用例

```
ramecntrl# show debug
Current trace status:
  Current log entries      : 920 (Out of 10000 max.)
  Log frozen?              : NO
  Auto-freeze severity    : -1 (Disabled)
  Real-time display severity : -1 (Disabled)
ramecntrl#
```

show diag-log-config ap/controller/station

AP、コントローラ、およびステーションの診断ログ設定を表示します。

構文

show diag-log-config ap
show diag-log-config controller
show diag-log-config station

コマンド
モード

特権 EXEC

デフォルト

無効

用途

このコマンドを使用して、コントローラ、AP、およびステーションの管理ステータスとDiagnostics Logging 設定を表示します。このイベント パラメータは、リリース 4.0 で **show diag-log-config station** に追加されました。

使用例

次の例は、診断インターフェイスのすべてのコントローラしきい値を表示します。

```
ramecntrl# sh diag-log-config ap
```

```
AP Diagnostics                               Disabled
AP Diag Stats Monitoring Interval            240 seconds
AP interface Stats Monitoring Interval       300 seconds
```

Diagnostics Type	SubType	Debug	Infor	Minor	Major
Critical					
Fatal Hw Error Interrupts	diag stats	-	-	-	1
2					
Rx Overrun Interrupts	diag stats	-	-	-	1
2					
Rx eol Interrupts	diag stats	-	-	-	1
2					
Tx Underrun Interrupts	diag stats	-	-	-	1
2					

Tx Timeout Interrupts 1260	diag stats	-	-	-	1200
Carrier Sense Timeout Int 1260	diag stats	-	-	-	1200
Tx Failed(No Tx Buff) 2	diag stats	-	-	-	1
Tx Failed(Fifo Underrun) 2	diag stats	-	-	-	1
No SkBuff for Beacon 2	diag stats	-	-	-	1
Aggregate Desc Conf Err 2	diag stats	-	-	-	1
Data Underrun Aggregate 2	diag stats	-	-	-	1
Delimiter Underrun Aggregate 2	diag stats	-	-	-	1
Rx pkts with Bad Version 2	diag stats	-	-	-	1
Beacon Misscount -	diag stats	-	-	-	-
Beacon buff Null Cnt 2	diag stats	-	-	-	1
Radio Reset(Beacon Stuck) 21	diag stats	-	-	-	20
Radio Reset(TP Scale) 2	diag stats	-	-	-	1
Radio Reset(Fatal Tasklet) 2	diag stats	-	-	-	1
Radio Reset(Rx Overrun Tasklet) 2	diag stats	-	-	-	1
Radio Reset(Calibrate) 2	diag stats	-	-	-	1
Radio Reset(Tx Ant Switch) 2	diag stats	-	-	-	1
Radio Reset(Rx Chain) 2	diag stats	-	-	-	1
Radio Reset(No Tx Frames) 2	diag stats	-	-	-	1
Radio Reset(Total) 2	diag stats	-	-	-	1
Tid Reset Count 2	diag stats	-	-	-	1

Slam Tx No Ack Addr	diag stats	-	-	-	3000
-					
Tx Failed(Too Many Retries)	if stats	-	-	-	120000
-					
Tx Excessive Retries Aggre	if stats	-	-	-	120000
-					
Rx Data for Assigned sta	if stats	-	-	-	-
-					
All Tx Frames	if stats	-	-	-	-
-					
Rx Mgmt for Assigned sta	if stats	-	-	-	12000
-					
Rx All Data Frames	if stats	-	-	-	-
-					
Rx All Mgmt Frames	if stats	-	-	-	120000
-					
Rx All Cntl Frames	if stats	-	-	-	240000
-					
Mgmt Frames Overhead in Airtime	if stats	-	-	-	30
-					
Association Count	if stats	-	-	-	40
-					
Retry Percentage	if stats	-	-	-	40
-					
Noise Floor	if stats	-	-	-	-75
-					

namecntrl# sh diag-log-config controller

Controller Diagnostics	Disabled
Monitoring Interval	60 second(s)

Diagnostics Type	SubType	Object-ID	Debug	Infor	Minor
Major	Critical				
process-restart	crash	-	-	-	-
ON					
process-resource	mem-usage(%)	-	-	50	70
90					
process-resource	cpu-usage(%)	-	-	50	70
90					

keepalive-timeout 9	all(N)		-	-	5	7
cpu-usage 90	process(%)		-	-	50	70
file-system 90	all(%)		-	-	50	70
file-system -	partition(%)	0	-	-	-	-
partition 1000	access(N/sec)		-	-	100	500
mem-usage 200	free-mem(MB)		-	-	-	-
mailbox ON	all		-	-	-	-
mailbox -	mailbox	0	-	-	-	-
wncreg-table -	state		-	ON	-	-
ats-table ON	state		-	-	-	-
interface 100	error(N)		-	-	10	50
client-density 100	all(%)		-	-	80	90
ip-conflict ON	all		-	-	-	-
ip-unassigned -	all		-	-	-	-
gateway-unreach ON	error		-	-	-	-
radius-svr-unreach ON	error		-	-	-	-
dhcp-svr-unreach ON	error		-	-	-	-

```
ramecntrl# sh diag-log-config station
```

Station Diagnostics	Disabled
Station Diagnostics Data Collection Interval	60 second(s)
State Diagnostics Inference Interval	300 second(s)

Inference Threshold Table

Station Counter	ID#	Low	High
MAC Filter ACL Success	1	-	5
MAC Filter ACL Failure	2	-	5
Radius Auth Success	3	-	5
Radius Auth Failure	4	-	5
Assignment Failure	5	-	5
Association Success	6	-	5
Key Exchange Success	7	-	5
Key Exchange Failure	8	-	5
MIC Failure	9	-	5
IP Address Update	10	-	10
Data Decryption Failure	11	-	5
CP Guest User Success	12	-	5
CP Guest User Failure	13	-	5
Soft Handoff	14	-	15

Inference Rule Table

Id#	Inference Description	Severity	Operational Counter ID#
1	MAC Filtering ACL Failure	Critical	2
2	Radius Authentication Failure	Critical	4
3	Assignment Failure	Critical	5
4	Association Success	Infor	6
5	802.1x Key Exchange Failure	Critical	8
6	MIC Failure	Critical	9
7	IP Address Update	Infor	10
8	Data Decryption Failure	Critical	11
9	CP Guest User Failure	Critical	13
10	Soft-Handoff	Infor	14
11	Hard-Handoff	Infor	6 & 10

namecntrl#

関連コマンド

- [\(diag-log\) admin \(910 ページ\)](#)
- [\(diag-log\) config \(912 ページ\)](#)
- [\(diag-log\) restore \(914 ページ\)](#)
- admin ap on
- admin controller on
- admin station on

show packet-capture-profile

すべてのパケット捕捉プロファイルとその状態およびモードを表示します。オプションで、指定した 1 つのパケット捕捉プロファイルを表示します。

構文

```
show packet-capture-profile
show packet-capture-profile <profile name>
```

profile name コマンドを変更して、指定したプロファイルだけを表示するようにします。

コマンドモード

EXEC モード

デフォルト

すべてのパケット捕捉プロファイル

用途

profile name を指定せずにコマンドを実行すると、すべてのパケット捕捉プロファイルとその状態 (有効 / 無効) およびモード (レイヤ 2 / レイヤ 3) が表示されます。次のコマンドでは、指定した 1 つのパケット捕捉プロファイルの情報が表示されます。

使用例

次の例は、プロファイル LM が表示されますが、このプロファイルは現在、無効です。

```
MMC3K-1# show packet-capture-profile LM
AP Packet Capture profiles
Packet Capture Profile Name           : LM
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : L3
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
次の例は、Test という名前のプロファイルのステータスを表示します。
corporatewifi# show packet-capture-profile test
AP Packet Capture profiles:
Packet Capture Profile Name       : test
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3               : L3
Destination IP Address            : 192.168.34.210
UDP Destination Port              : 9178
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                      : all
Extended Filter String            :
Interface List                    :
Packet Truncation Length          : 0
Rate Limiting                     : off
Capture frames sent by other APs in the network : on

```

関連コマンド [packet-capture-profile \(922 ページ\)](#)

show statistics AP300-diagnostics

インターフェイスごとの AP300 診断統計のリストを表示します。

構文 `show statistics ap300-diagnostics`

コマンド
モード 特権 EXEC モード

デフォルト なし

用途

使用例 次の例は、`show statistics AP300-diagnostics` コマンドの結果を表示します。

Master1# `show statistics ap300-diagnostics`

AP-ID	IfIndex	AP-Name	Fatal	HW	INT	Tx	Underrun	INT	Tx	Timeout	INT
Carrier	Sense	Timeout	Rx	Overrun	INT	Rx	EOL	INT			
3	1	3-Guha	0	0		321		0			
48		0									
3	2	3-Guha	0	0		213		0			
306		0									
4	1	4-QA.Facing	0	0		3446		0			
0		0									
4	2	4-QA.Facing	0	0		6689		0			
0		0									
5	1	5-Popov	0	0		687		0			
251		0									
5	2	5-Popov	0	0		322		0			
788		0									
8	1	8-Amazon	0	0		374119		0			
0		0									
8	2	8-Amazon	0	0		14		0			
0		0									
96	1	AP-96	0	0		1775		0			
12		0									

96	2	AP-96	0	0	0	0
0		1				
98	1	9-GrndConf	0	0	3764	0
0		0				
98	2	9-GrndConf	0	0	0	0
0		0				
103	1	103-carlos	0	0	467	0
24		0				
103	2	103-carlos	0	0	356	0
412		1				
239	1	AP-239	0	0	7492	0
0		0				
239	2	AP-239	0	0	2	0
2		0				

AP300 Diagnostic Statistics(16 entries)

Master1#

関連コマンド [diagnostics \(916 ページ\)](#)