Cisco DX シリーズ
ワイヤレス LAN 展開ガイド

Cisco DX シリーズは、企業の主要な事業所で働く従業員向けの業界初の次世代 IP エンドポイントです。魅力的かつ強力に統合され、常時接続でセキュア、ミッション クリティカルなユニファイド コミュニケーションと、HD ビデオおよびクラウドコンピューティング体験を含むコラボレーションを組み合わせ、そのインタラクティブで使いやすく、カスタマイズ可能なパーソナライゼーションとワークフローのオプションは、Android™ で設計されたエンタープライズグレードのプラットフォームから使用することができます。

Cisco DX シリーズは、従業員の生産性に新しい時代をひらきます。コラボレーション対応のビジネス プロセスとワークフローに新しい機会を生成し、ビジネス上の効果を促進します。
Cisco DX シリーズは、業界や地域、職場や家庭において現在および将来に新しく発生するニーズに対応します。

このガイドでは、ネットワーク管理者が無線 LAN 環境に Cisco DX シリーズを展開するのに役立つ情報と手引きを提供します。

マニュアルの変更履歴

日付	説明
13/05/24	10.0(1) リリース
13/08/20	10.0(2) リリース
14/04/19	10.1(1) リリース
14/09/18	10.2(2) リリース

目次

Cisco DX シリーズの概要

Cisco DX シリーズは企業内部のコラボレーションを支援するプラットフォームです。Cisco Unified Communication アプリケーションの機能を合わせて、無線および有線の Cisco Unified Communication デバイスの強固な基盤の上に構築します。CCX を利用したシスコ製品の 802.11 の実装では、音声やビデオなどの時間が重要なアプリケーションをキャンパス全体の無線 LAN（WLAN）環境で効率的に使用することが可能になりました。これらの拡張により、エンド ユーザがアクセス ポイント間をローミングするときのセキュリティは維持しながら、高速ローミング機能とほぼシームレスなマルチメディア トラフィックのフローが提供されます。

WLAN はライセンス不要のスペクトルを使用しているため、同じライセンス不要のスペクトルを使用する他のデバイスからの干渉が発生する可能性があることを理解する必要があります。また、Bluetooth ヘッドセットや電子レンジ、コードレス電話など、2.4 GHz スペクトルのデバイスは急増しており、2.4 GHz スペクトルは他のスペクトルよりも多くの輻輳が発生する可能性があります。5 GHz スペクトルは動作するデバイスがはるかに少数であり、使用可能な 802.11a/n データ レートを活用するためには、Cisco DX シリーズの運用において推奨されるスペクトルです。シスコでは、Cisco DX シリーズで最適化を実装していますが、ライセンス不要のスペクトルを使用する場合は中断のない通信は保証できず、マルチメディア カンバセーション中に最大で数秒間の音声またはビデオのギャップが発生する可能性があります。導入ガイドラインに従うことで、このような音声またはビデオのギャップが発生する可能性は低減されますが、完全になくなることはありません。ライセンス不要のスペクトルを使用していること、および WLAN デバイスへのメッセージ配信を保証できないことから、Cisco DX シリーズは医療機器としての使用を想定しておらず、臨床的な判断には使用できません。

Cisco DX シリーズの特徴

Cisco DX シリーズは、企業向けに構築されたコラボレーション デバイスです。

シスコ製品に期待されるようになったマルチメディア パフォーマンス レベルは、802.11n データ レートの導入と Cisco Compatible eXtensions（CCX）の採用により Cisco DX シリーズで維持されます。

- マルチタッチ カラー ディスプレイ
  - DX650 = 7 インチ
  - DX70 = 14 インチ
  - DX80 = 23 インチ
- Android™ OS 4.1.1
- 1.5 GHz デュアルコア プロセッサ
- 8 GB の eMMC フラッシュ メモリ
- 2 GB の LPDDR2 SDRAM
- IEEE 802.11 a/b/g/n Wi-Fi
- Bluetooth 3.0
- 2 ポート ギガビット イーサネット スイッチ
  - DX650 = クラス 3/4 Power over Ethernet（PoE）（電話ポート用）
- HDMI ポート
  - DX650 = 外部モニタ サポート用× 1
  - DX70 = ビデオ入力用× 1 と、ビデオ出力用× 1
  - DX80 = ビデオ入力用× 1 と、ビデオ出力用× 1
- タイプ A USB ポート
  - DX650 = USB 2.0 ポート× 2
  - DX70 = USB 2.0 ポート× 3
  - DX80 = USB 2.0 ポート× 3
- マイクロ タイプ B USB ポート× 1
- 3.5 mm ヘッドフォン ジャック

- microSD カードのサポート
- 全二重スピーカーフォンおよびワイドバンド オーディオ
- 前面カメラは HD 1080p 30-fps でビデオのエンコードおよびデコード可能
- Cisco TelePresence™ ソリューションやその他の H.264 ビデオ エンドポイントとの高解像度ビデオの相互運用性
- Cisco Collaboration および Unified Communication アプリケーションのすべての機能
  Cisco Quad、Cisco WebEx™、Cisco Unified Presence、インスタント メッセージ、電子メール、および Cisco Unified Communications Manager の音声およびビデオ テレフォニー機能
- 仮想デスクトップ クライアントの統合(VDI)およびクラウド コンピューティング
- Google Play™ へのアクセス
- ソフトウェア開発キット(SDK)を通じて Cisco Collaboration API をリンクする、ビジネス向けの拡張 Android アプリケーション

要件

Cisco DX600 シリーズは、音声、ビデオ、およびデータ通信を提供する IEEE 802.11a/b/g/n コラボレーション デバイスです。

ワイヤレス LAN の検証を行って、Cisco DX シリーズの展開に必要な要件が満たされているか確認する必要があります。

サイト調査

Cisco DX シリーズを実稼働環境に展開する前に、先進的なワイヤレス LAN を専門とするシスコ認定パートナーの手でサイト調査を実施する必要があります。サイト調査時に、RF(ラジオ周波数)スペクトルを分析して、目的の帯域(5 GHz または 2.4 GHz)内で使用可能なチャネルを決定できます。一般に、5 GHz 帯域では干渉が少なく、オーバーラップしないチャネルが多く存在します。そのため動作帯域は 5 GHz が推奨されています。特に Cisco DX シリーズを基幹業務で使用する場合は 5 GHz の使用が強く推奨されます。サイト調査には、その場所の対象カバレッジ プランを示すヒートマップも含まれます。さらにサイト調査では、その場所で使用するアクセス ポイント プラットフォーム タイプ、アンテナ タイプ、アクセス ポイント設定(チャネルと送信電力)も特定します。条件の厳しくない環境(オフィス、医療機関、教育、サービス業など)に対しては内蔵アンテナを持つアクセス ポイントを選択し、条件の厳しい環境(製造、倉庫、小売業など)に対しては外部アンテナを必要とするアクセス ポイント プラットフォームを選択することを推奨します。
詳細については、「音声用のワイヤレス LAN の設計」を参照してください。

その他の情報については、Steps to Success Web サイトを参照してください。
http://www.cisco.com/go/stepstosuccess

RF の確認

VoWLAN を展開できるか確認するために、環境を評価して、次の項目についてシスコのガイドラインが満たされることを確認します。

信号

セル エッジは、-67 dBm の信号レベルで隣接アクセス ポイントとの 20 ～ 30 % のオーバーラップが存在するように設計されている必要があります。

これにより、Cisco DX シリーズに対して常に十分な強さの信号が提供され、パケット損失のトリガーに対して信号ベースのトリガーが利用されている状況でシームレスにローミングするのに十分な 時間にわたって信号を保持できます。

また、Cisco DX シリーズからのアップストリーム信号が、送信データ レートに対するアクセス ポイントの受信感度に適合している必要があります。一般的に、アクセス ポイントの受信信号は、-67 dBm 以上になるようにしてください。

セル サイズは、Cisco DX シリーズが信号を 5 秒以上保持できるように設計することを推奨します。

チャネル使用率

チャネル使用率レベルは 40% 未満に維持される必要があります。

Cisco DX シリーズは、0 ～ 255 のスケール値をパーセンテージに変換するため、105 は Cisco DX シリーズの近接リスト メニューでは約 40% に相当します。

ノイズ

ノイズ レベルは -92 dBm を超過してはなりません。それにより、-67 dBm の信号が維持される場合に 25 dB の信号対雑音比（SNR）が実現されます。

また、Cisco DX シリーズからのアップストリーム信号が、送信データ レートに対するアクセス ポイントの信号対雑音比に適合している必要があります。

パケット損失/遅延

音声ガイドラインごとに、パケット損失が 1 % を超過してはなりません。超過すると、音声品質が大幅に低下する可能性があります。

ジッタは最小限（100 ms 未満）に抑える必要があります。

再試行

802.11 再送信は 20 % 未満である必要があります。

マルチパス

マルチパスは、null を生成し、信号レベルを低下させる可能性があるため、最小限に維持される必要があります。

展開が可能であることを確認するために、多様なツールとアプリケーションを使用してこれらの項目を評価できます。

- Unified Wireless LAN 管理用の Cisco Prime Network Control System（NCS）

  http://www.cisco.com/c/en/us/products/collateral/wireless/prime-network-control-system-series-appliances/data_sheet_c78-650051.html
- Unified Wireless LAN 管理用の Cisco Wireless Control System（WCS）

  http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd802570d0.html
- シスコ自律分散型ワイヤレス LAN 管理用の Cisco Wireless LAN Solution Engine（WLSE）

  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/ciscoworks-wireless-lan-solution-engine-software-2-13/product_data_sheet0900aecd80410b92.html
- Cisco Spectrum Expert

  http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert/product_data_sheet0900aecd807033c3.html
- Cisco Unified Operations Manager

  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-unified-operations-manager/data_sheet_c78-636705.html

呼制御

Cisco DX シリーズは、次の通信プラットフォームを使用したコール制御に Session Initiation Protocol（SIP）を利用します。

- Cisco Unified Communications Manager（CUCM）

  DX650
  最小 = 7.1(5)
  推奨 = 8.6(2)、9.1(2)、10.5(1)

  DX70
  最小 = 8.5(1)
  推奨 = 8.6(2)、9.1(2)、10.5(1)

  DX80
  最小 = 8.5(1)
  推奨 = 8.6(2)、9.1(2)、10.5(1)

Cisco Unified Communications Manager でのデバイス サポート

Cisco DX シリーズのデバイス サポートを有効にするためには、Cisco Unified Communications Manager でデバイス パッケージがインストールされているかサービス リリース アップデートが行われている必要があります。

Cisco Unified Communications Manager 用のデバイス パッケージは、次の場所から入手できます。
http://software.cisco.com/download/navigator.html?mdfid=278875240

プロトコル

次の音声およびワイヤレス LAN のプロトコルがサポートされています。

- Wi-Fi MultiMedia（WMM）
- Session Initiation Protocol（SIP）
- Real Time Protocol（RTP）
- AAC-LD、G.722、iSAC、G.711、iLBC、G.729
- H.264
- Real Time Control Protocol（RTCP）
- Cisco Discovery Protocol（CDP）

アクセス ポイント

Cisco DX シリーズは、次の Cisco Wireless LAN ソリューションでサポートされます。

- Cisco Unified Wireless LAN Controller

  最低 = 7.0.250.0

  推奨 = 7.4.121.0、7.6.130.0、8.0.100.0

- Cisco IOS アクセス ポイント（Autonomous）

  最低 = 12.4(21a)JY

  推奨 = 12.4(25d)JA2、15.2(4)JB6、15.3(3)JAB

サポートされているアクセス ポイントのモデルは、次に示すとおりです。

（注）Cisco DX シリーズは、内蔵の 802.11a/b/g/n 無線機が使用されている場合に Cisco AP3600 でサポートされますが、Cisco AP3600 用の 802.11ac モジュール（AIR-RM3000AC）が取り付けられている場合は Cisco Unified Wireless LAN Controller リリース 7.6.100.0 以降が必要です。

次の表に、シスコの各アクセス ポイントでサポートされるモードを示します。

Cisco AP シリーズ	802.11a	802.11b	802.11g	802.11n	802.11ac	Unified	Autonomous
600	Yes	Yes	Yes	Yes	No	Yes	No
700	Yes	Yes	Yes	Yes	No	Yes	No
1040	Yes	Yes	Yes	Yes	No	Yes	Yes
1130 AG	Yes	Yes	Yes	No	No	Yes	Yes
1140	Yes	Yes	Yes	Yes	No	Yes	Yes
1240 AG	Yes	Yes	Yes	No	No	Yes	Yes
1250	Yes	Yes	Yes	Yes	No	Yes	Yes
1260	Yes	Yes	Yes	Yes	No	Yes	Yes
1600	Yes	Yes	Yes	Yes	No	Yes	Yes

2600	Yes	Yes	Yes	Yes	No	Yes	Yes
3500	Yes	Yes	Yes	Yes	No	Yes	Yes
3600	Yes	Yes	Yes	Yes	Yes（AIR-RM3000AC モジュールを使用）	Yes	Yes
3700	Yes	Yes	Yes	Yes	Yes	Yes	Yes
890	Yes	Yes	Yes	Yes	No	Yes	Yes

（注）VoWLAN と屋外の MESH テクノロジー（1500 シリーズ）の間の連携は現在サポートされていません。

サードパーティ製アクセス ポイントに対して相互運用性テストを実施していないため、サードパーティ製アクセス ポイントのサポートは限定されています。

ただし、ユーザは Wi-Fi 対応アクセス ポイントに接続する場合の基本機能が必要です。

主な機能の一部を以下に示します。

- 5 GHz（802.11a/n）
- Wi-Fi Protected Access v2（WPA2+AES）
- Wi-Fi Multimedia（WMM）
- Diffserv コード ポイント（DSCP）
- サービス クラス（802.1p）
- QoS Basic Service Set（QBSS）

Cisco DX シリーズは、Cisco Client Extensions（CCX）対応のアクセス ポイントを使用できます。

主な機能の一部を以下に示します。

- Cisco Centralized Key Management（CCKM）
- ダイナミック伝送パワー コントロール（DTPC）

http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html

http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

アンテナ

一部の Cisco Access Point では、外部アンテナが必要であるか、使用可能です。

サポートされるアンテナのリストとそれらの外部アンテナの設置方法については、次の URL を参照してください。

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/product_data_sheet09186a008008883b.html

Distributed Antenna Systems（DAS）や Leaky Coaxial Systems などのサードパーティ製アンテナに対して相互運用性テストを実施していないため、サードパーティ製アンテナはサポートされません。

Distributed Antenna Systems 上での Cisco Wireless LAN の詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/positioning_statement_c07-565470.html

（注）Cisco 1040、1130、1140、1602i、2602i、3502i、3602i、および 3702i シリーズ アクセス ポイントは、全方向性アンテナを搭載していており、パッチ用には設計されていないため、天井に取り付ける必要があります。

モデル

次の Cisco DX シリーズ モデルを使用できます。

下記は、各モデルでサポートされるモード、周波数範囲とチャネルの概要です。

部品番号	ネットワーク モード	ピーク アンテナ ゲイン	周波数範囲	使用可能なチャネル	チャネル セット
CP-DX650-K9= CP-DX650-K9-W	Wi-Fi	2.4 GHz = 4 dBi 5 GHz = 4 dBi	2.412～2.472 GHz 5.180～5.240 GHz 5.260～5.320 GHz 5.500～5.700 GHz 5.745～5.825 GHz	13 4 4 11 5	1 ～ 13 36、40、44、48 52、56、60、64 100 ～ 140 149、153、157、161、165
CP-DX70-W-K9=	Wi-Fi	2.4 GHz = 2.6 dBi 5 GHz = 4 dBi	2.412～2.472 GHz 5.180～5.240 GHz 5.260～5.320 GHz 5.500～5.700 GHz 5.745～5.825 GHz	13 4 4 11 5	1 ～ 13 36、40、44、48 52、56、60、64 100 ～ 140 149、153、157、161、165
CP-DX80-K9=	Wi-Fi	2.4 GHz = 4.6 dBi 5 GHz = 7 dBi	2.412～2.472 GHz 5.180～5.240 GHz 5.260～5.320 GHz 5.500～5.700 GHz 5.745～5.825 GHz	13 4 4 11 5	1 ～ 13 36、40、44、48 52、56、60、64 100 ～ 140 149、153、157、161、165

Wi-Fi モードを使用している場合は、電源キューブ（Cisco DX650 には CP-PWR-CUBE-4=、DX70 および DX80 には CP-PWR-CUBE-5=）が必要です。

（注）チャネル 120、124、128 はアメリカ、ヨーロッパ、日本ではサポートされていませんが、他の地域ではサポートされている場合があります。

802.11j（チャネル 34、38、42、46）はサポートされていません。

日本用のチャネル 14 はサポートされません。

ワールド モード（802.11d）

ワールド モードでは、さまざまな領域でクライアントを使用できます。ローカル環境のアクセス ポイントによってアドバタイズされるチャネルと送信電力の使用に対してクライアントを適合させることができます。

Cisco DX シリーズは、使用するチャネルと送信電力を定義できる 802.11d 対応のアクセス ポイントが必要です。

アクセス ポイントが設置されている国に応じて、ワールド モード（802.11d）を有効にします。

一部の 5 GHz チャネルはレーダーのテクノロジーでも使用されているため、それらのレーダー周波数（DFS チャネル）を使用する場合、802.11 クライアントとアクセス ポイントは、802.11h に準拠している必要があります。802.11h では、802.11d を有効にする必要があります。

Cisco DX シリーズは、まず DFS チャネルをパッシブ スキャンしてから、それらのチャネルのアクティブ スキャンを実行します。

2.4 GHz（802.11b/g）を使用する場合、802.11d が有効でなければ、Cisco DX シリーズはチャネル 1 ～ 11 および低減された送信電力の使用を試みることができます。

（注）Cisco Unified Wireless LAN Controller の場合、ワールド モードは自動的に有効になります。

Cisco Autonomous Access Point の場合は、次のコマンドを使用してワールド モードを手動で有効にする必要があります。

```
Interface dot11radio X
world-mode dot11d country US both
```

サポートされる国

Cisco DX シリーズのサポート対象となる国とその 802.11d コードは次のとおりです。

アイスランド（IS）
アイルランド（IE）
アメリカ合衆国（US）
アラブ首長国連邦（AE）
アルゼンチン（AR）
イギリス（GB）
イスラエル（IL）
イタリア（IT）
インド（IN）
インドネシア（ID）
ウクライナ（UA）
ウルグアイ（UY）
エクアドル（EC）
エジプト（EG）
エストニア（EE）
オーストラリア（AU）
オーストリア（AT）
オマーン（OM）
オランダ（NL）
カナダ（CA）
キプロス（CY）
ギリシャ（GR）
クロアチア（HR）
コスタリカ（CR）
コロンビア（CO）
サウジアラビア（SA）
シンガポール（SG）
ジブラルタル（GI）
スイス（CH）
スウェーデン（SE）
スペイン（ES）
スロバキア（SK）
スロベニア（SI）
セルビア（RS）
タイ（TH）
チェコ共和国（CZ）
チリ（CL）
デンマーク（DK）
トルコ（TR）
ドイツ（DE）
ドミニカ共和国（DO）
ナイジェリア（NG）
ニュージーランド（NZ）
ノルウェー（NO）
ハンガリー（HU）
バーレーン（BH）
パナマ（PA）
パラグアイ（PY）
フィリピン（PH）
フィンランド（FI）
フランス（FR）
ブラジル（BR）
ブルガリア（BG）
プエルトリコ（PR）
ベトナム（VN）
ベネズエラ（VE）
ベルギー（BE）
ペルー（PE）
ポーランド（PL）
ポルトガル（PT）
マケドニア（MK）
マルタ（MT）
マレーシア（MY）
メキシコ（MX）
モナコ（MC）
モンテネグロ（ME）
ラトビア（LV）
リトアニア（LT）
リヒテンシュタイン（LI）
ルーマニア（RO）
ルクセンブルク（LU）
ロシア連邦（RU）
韓国（KR）
香港（HK）
台湾（TW）
中国（CN）
南アフリカ（ZA）
日本（JP）

（注）コンプライアンス情報は、次の URL にある Cisco Product Approval Status Web サイトで入手できます。

http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

無線特性

次の表は、Cisco DX シリーズのデータ レートと受信感度をまとめたものです。

5 GHz の仕様

5 GHz - 802.11a	データ レート	変調	受信感度
最大送信電力 = 16 dBm （モデルと地域によって異なる）	6 Mbps	OFDM - BPSK	-91 dBm
	9 Mbps	OFDM - BPSK	-91 dBm
	12 Mbps	OFDM - QPSK	-90 dBm
	18 Mbps	OFDM - QPSK	-88 dBm
	24 Mbps	OFDM - 16 QAM	-85 dBm
	36 Mbps	OFDM - 16 QAM	-81 dBm
	48 Mbps	OFDM - 64 QAM	-77 dBm
	54 Mbps	OFDM - 64 QAM	-76 dBm
5 GHz - 802.11n（20）	データ レート	変調	受信感度
最大送信電力 = 15 dBm （モデルと地域によって異なる）	7 Mbps（MCS 0）	OFDM - BPSK	-91 dBm
	14 Mbps（MCS 1）	OFDM - QPSK	-89 dBm
	21 Mbps（MCS 2）	OFDM - QPSK	-86 dBm
	29 Mbps（MCS 3）	OFDM - 16 QAM	-84 dBm
	43 Mbps（MCS 4）	OFDM - 16 QAM	-81 dBm
	58 Mbps（MCS 5）	OFDM - 64 QAM	-76 dBm
	65 Mbps（MCS 6）	OFDM - 64 QAM	-74 dBm
	72 Mbps（MCS 7）	OFDM - 64 QAM	-72 dBm
5 GHz - 802.11n（40）	データ レート	変調	受信感度
最大送信電力 = 15 dBm （モデルと地域によって異なる）	15 Mbps（MCS 0）	OFDM - BPSK	-90 dBm
	30 Mbps（MCS 1）	OFDM - QPSK	-87 dBm
	45 Mbps（MCS 2）	OFDM - QPSK	-85 dBm
	60 Mbps（MCS 3）	OFDM - 16 QAM	-81 dBm
	90 Mbps（MCS 4）	OFDM - 16 QAM	-78 dBm
	120 Mbps（MCS 5）	OFDM - 64 QAM	-74 dBm
	135 Mbps（MCS 6）	OFDM - 64 QAM	-72 dBm
	150 Mbps（MCS 7）	OFDM - 64 QAM	-70 dBm

2.4 GHz の仕様

2.4 GHz - 802.11b	データ レート	変調	受信感度
最大送信電力 = 16 dBm （モデルと地域によって異なる）	1 Mbps	DSSS - BPSK	-95 dBm
	2 Mbps	DSSS - QPSK	-93 dBm
	5.5 Mbps	DSSS - CCK	-90 dBm
	11 Mbps	DSSS - CCK	-86 dBm
2.4 GHz - 802.11g	**データ レート**	**変調**	**受信感度**
最大送信電力 = 16 dBm （モデルと地域によって異なる）	6 Mbps	OFDM - BPSK	-89 dBm
	9 Mbps	OFDM - BPSK	-89 dBm
	12 Mbps	OFDM - QPSK	-87 dBm
	18 Mbps	OFDM - QPSK	-85 dBm
	24 Mbps	OFDM - 16 QAM	-81 dBm
	36 Mbps	OFDM - 16 QAM	-78 dBm
	48 Mbps	OFDM - 64 QAM	-74 dBm
	54 Mbps	OFDM - 64 QAM	-72 dBm
2.4 GHz - 802.11n（20）	**データ レート**	**変調**	**受信感度**
最大送信電力 = 16 dBm （モデルと地域によって異なる）	7 Mbps（MCS 0）	OFDM - BPSK	-88 dBm
	14 Mbps（MCS 1）	OFDM - QPSK	-86 dBm
	21 Mbps（MCS 2）	OFDM - QPSK	-84 dBm
	29 Mbps（MCS 3）	OFDM - 16 QAM	-81 dBm
	43 Mbps（MCS 4）	OFDM - 16 QAM	-78 dBm
	58 Mbps（MCS 5）	OFDM - 64 QAM	-73 dBm
	65 Mbps（MCS 6）	OFDM - 64 QAM	-71 dBm
	72 Mbps（MCS 7）	OFDM - 64 QAM	-69 dBm

（注）受信感度は、特定のデータ レートでパケットをデコードするのに最低限必要な信号強度です。

上記の値は、純粋な無線仕様であって、一体型アンテナのゲインは考慮されていません。

802.11n 接続を実現するには、Cisco DX シリーズをアクセス ポイントから約 30 m（100 フィート）以内に配置することをお勧めします。

信号要件の詳細については、「音声用のワイヤレス LAN の設計」を参照してください。

言語サポート

Cisco DX シリーズは、次の言語をサポートしています。

ドイツ語	スロバキア語	ヘブライ語
韓国語	スロベニア語	ポーランド語
ノルウェー語	セルビア語	ポルトガル語
トルコ語	タイ語	ラトビア語
アラビア語	チェコ語	リトアニア語
イタリア語	デンマーク語	ルーマニア語
カタロニア語	ドイツ語	ロシア語
ギリシャ語	ハンガリー語	英語
クロアチア語	フィンランド語	中国語
スウェーデン語	フランス語	日本語
スペイン語	ブルガリア語	

各言語のサポートを有効にするには、対応するロケール パッケージをインストールする必要があります。Cisco DX シリーズのデフォルト言語は英語です。

ロケール パッケージは、次の URL にある [Localization] ページからダウンロードします。

http://software.cisco.com/download/navigator.html?mdfid=278875240

Bluetooth

Cisco DX シリーズは Bluetooth 3.0 テクノロジーをサポートしており、ワイヤレス ヘッドセット通信が可能です。

Bluetooth では、約 9 m（30 フィート）の範囲内であれば低帯域幅のワイヤレス接続が可能ですが、Bluetooth デバイスは常に Cisco DX シリーズから約 3 m（10 フィート）以内で使用することが推奨されます。

その Bluetooth プロファイルで接続済みのデバイスが優先されます。

Bluetooth デバイスは Cisco DX シリーズから直接見通せる場所にある必要はありませんが、壁や扉などの障害物がある場合は、通信の質に悪影響を生じることがあります。

Bluetooth は、802.11b/g/n や他の多くのデバイス（電子レンジ、コードレス電話機など）と同様に 2.4 GHz の周波数を使用します。そのため、Bluetooth の品質は、こうした免許申請の必要のない周波数の使用による干渉の影響を受ける可能性があります。

Bluetooth プロファイル

Cisco DX シリーズは、次の Bluetooth プロファイルをサポートしています。

ハンズフリー プロファイル（HFP）

Bluetooth ハンズフリー プロファイル（HFP）サポートでは、Bluetooth ヘッドセットでサポートされていれば、次の機能も利用できます。

- 呼出音
- コールへの応答
- コールの終了
- 録音の音量調節
- 最後の番号をリダイヤル
- コール待機
- 転送/拒否
- 三方向コール（保留して許可、リリースして許可）
- スピード ダイヤル

Advanced Audio Distribution プロファイル（A2DP）

Bluetooth Advanced Audio Distribution プロファイル（A2DP）は Bluetooth 対応のステレオ ヘッドセット、車の音声システムなどへの単方向品質ステレオ オーディオ ストリームの転送を行えます。

電話帳アクセス プロファイル（PBAP）

電話帳のアクセス プロファイル（PBAP）のサポートは、デバイス間の電話帳オブジェクトの交換を可能にします。

オブジェクトのプッシュ プロファイル（OPP）

オブジェクトのプッシュ プロファイル（OPP）のサポートは、デバイス間のファイル共有を可能にします。

共有オブジェクトは通常、送信者がファイル交換を開始する画像、名刺会議の詳細などです。

ヒューマン インターフェイス デバイス（HID）

ヒューマン インターフェイス デバイス（HID）は、Bluetooth 対応キーボードやマウスをサポートします。

詳細については、Bluetooth デバイスの製造業者が提供するマニュアルを参照してください。

共存（802.11b/g/n + Bluetooth）

802.11b/g/n と Bluetooth が同時に使用される共存を利用する場合、両方とも 2.4 GHz の周波数範囲を利用するので、いくつかの制限と展開要件を考慮する必要があります。

キャパシティ

共存（802.11b/g/n + Bluetooth）を使用する場合、コール キャパシティは、802.11b/g/n および Bluetooth 転送の両方で 2.4 GHz 帯が使用されるため低下します。

マルチキャスト オーディオ

共存を使用する場合、Push To Talk（PTT）、Multicast Music on Hold（MMOH）、および他のアプリケーションからのマルチキャスト オーディオはサポートされません。

音声品質

現在のデータ レート設定に応じて、共存の使用時に Bluetooth 転送を保護するために CTS を送信できます。
一部の環境では、6 Mbps を有効にしなければならない場合があります。

（注） 802.11b/g/n と Bluetooth は両方とも 2.4 GHz を利用するうえ、上記の制限もあるため、Bluetooth を使用する場合は 802.11a/n の使用を強く推奨します。

ビデオ コール

Cisco DX シリーズは、高解像度マルチタッチ カラー LCD と内蔵カメラによるビデオ コールをサポートしています。

Cisco Unified Communications Manager の**ビデオ コール機能**では、ビデオ コールに参加する場合、Cisco DX シリーズごとに有効にする必要があります。

Cisco DX シリーズは、他の Cisco DX シリーズ エンドポイント、Cisco TelePresence Systems、Cisco Unified IP Phone 8900 および 9900 シリーズ、およびその他のビデオ対応エンドポイントのビデオ コールを確立できます。

600p と HD 720p は、使用可能な他のエンドポイントと通信するときに、より高いグレードのビデオが必要ではない場合に使用される推奨ビデオ形式です。

600p（1024 x 600）は、DX650 エンドポイント間のビデオ コールに使用されるネイティブなデフォルト形式です。

リモート ユーザの場合は、Cisco Unified Communications Manager の Cisco DX シリーズ エンドポイント設定で有効にされる最大ビデオ解像度を 600p または HD 720p をにする必要があります。

ビデオ会議機能を実現するには、MCU でバージョン 5.7 以降が実行されているビデオ会議システムが必要です。

ビデオ コールは、Cisco AnyConnect VPN Client を使用しても VPN セッション経由で確立できます。

H.264 は 30 fps（フレーム/秒）がサポートされるビデオ ストリームに使用されるプロトコルです。

サポートするオーディオ コーデックの 1 つを使用する音声セッション用に別のストリームがあります。

Cisco DX シリーズは、現在のネットワーク接続が高いビデオ解像度をサポートできない場合、ビデオ ビット レートを必要に応じて調整可能な、ビデオ帯域幅適応をサポートしています。

次のビデオ形式がサポートされます:

- CIF（352 X 288）
- VGA（640 X 480）
- 240p（432 x 240）
- 360p（640 x 360）
- 480p（848 x 480）
- 600p（1024 x 600）
- HD 720p（1280 X 720）
- HD 1080p（1920 X 1080）

Cisco TelePresence の詳細については、次のマニュアルを参照してください。
http://www.cisco.com/c/en/us/products/collaboration-endpoints/index.html

Cisco Unified IP Phone 8900 および 9900 シリーズに関する詳細情報については、次の URL を参照してください:
http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8900-series/index.html
http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phones-9900-series/index.html

セキュリティ

ワイヤレス LAN を展開する場合、セキュリティが不可欠です。
Cisco DX シリーズは、次のワイヤレス セキュリティ機能をサポートしています。

WLAN 認証

- WPA2（802.1x 認証 + AES または TKIP 暗号化）
- WPA（802.1x 認証 + TKIP または AES 暗号化）
- WPA2-PSK（事前共有キー + AES 暗号化）
- WPA-PSK（事前共有キー + TKIP 暗号化）
- EAP-FAST（Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling）
- EAP-TLS（Extensible Authentication Protocol - Transport Layer Security）
- PEAP-MSCHAPv2（Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2）
- PEAP-GTC（Protected Extensible Authentication Protocol - Generic Token Card）
- Cisco Centralized Key Management（CCKM）
- なし

WLAN 暗号化

- AES（Advanced Encryption Standard）
- Temporal Key Integrity Protocol/Message Integrity Check（TKIP/MIC）
- WEP（Wired Equivalent Protocol）40/64 および 104/128 ビット

（注） 802.1x 認証を使用した動的 WEP および共有キー認証はサポートされません。

Cisco DX シリーズは次の追加のセキュリティ機能もサポートします。

- X.509 デジタル証明書
- イメージ認証
- デバイス認証
- ファイル認証

- シグナリング認証
- Secure Cisco Unified SRST
- メディア暗号化（SRTP）
- シグナリング暗号化（TLS）
- Certificate Authority Proxy Function（CAPF）
- セキュア プロファイル
- 暗号化された設定ファイル
- 画面ロック
- リモート ロック
- リモート ワイプ
- Cisco AnyConnect VPN Client

Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling（EAP-FAST）

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、アクセス ポイントと Cisco Access Control Server（ACS）や Cisco Identity Services Engine（ISE）などのリモート認証ダイヤルイン ユーザ サービス（RADIUS）サーバ間の Transport Level Security（TLS）トンネル内の EAP トランザクションを暗号化します。

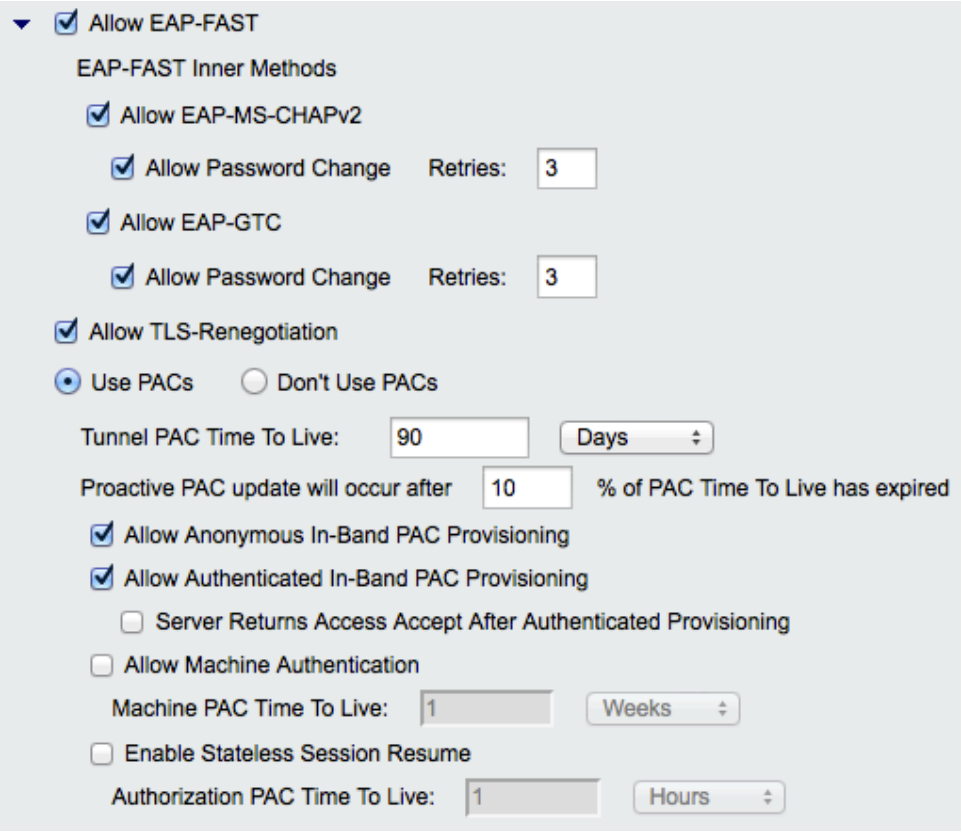
TLS トンネルでは、クライアント（Cisco DX シリーズ）と RADIUS サーバ間の認証に Protected Access Credential（PAC）が使用されます。サーバは Authority ID（AID）をクライアントに送信します。それを受けてクライアントは適切な PAC を選択します。クライアントは PAC-Opaque を RADIUS サーバに返します。サーバは、自分のマスターキーで PAC を復号します。これで両方のエンドポイントが同じ PAC キーを所有することになり、TLS トンネルが構築されます。EAP-FAST では、自動 PAC プロビジョニングがサポートされていますが、RADIUS サーバ上で有効にする必要があります。

EAP-FAST を有効にするには、RADIUS サーバに証明書をインストールする必要があります。

現在、Cisco DX シリーズでは、PAC の自動プロビジョニングに限ってサポートされています。そのため、次のように RADIUS サーバ上で [匿名インバンド PAC プロビジョニングを許可する（Allow anonymous in-band PAC provisioning）] を有効にしてください。

[匿名インバンド PAC プロビジョニングを許可する（Allow anonymous in-band PAC provisioning）] が有効な場合、EAP-GTC と EAP-MSCHAPv2 の両方を有効にする必要があります。

EAP-FAST では、認証サーバ上にユーザ アカウントを作成する必要があります。



実稼働ワイヤレス LAN 環境内で匿名 PAC プロビジョニングが許可されていない場合は、Cisco DX シリーズの初期 PAC プロビジョニング用として、ステージング RADIUS サーバをセットアップできます。

これには、ステージング RADIUS サーバをスレーブ EAP-FAST サーバとしてセットアップすることが必要であり、それにより、ユーザとグループのデータベースや EAP-FAST マスター キーとポリシー情報などの各コンポーネントが、実稼働マスター EAP-FAST サーバから複製されます。

EAP-FAST のマスター キーおよびポリシーがステージング スレーブ EAP-FAST RADIUS サーバへ送信されるように、実稼働マスター EAP-FAST RADIUS サーバがセットアップされていることを確認します。これにより、Cisco DX シリーズでは、[**匿名インバンド PAC プロビジョニングを許可する（Allow anonymous in-band PAC provisioning）**] が無効となっている実稼働環境内でも、プロビジョニングされた PAC を使用できるようになります。

PAC を更新するときは、認証済みのインバンド PAC プロビジョニングが使用されます。そのため、[**認証済みインバンド PAC プロビジョニングを許可する（Allow authenticated in-band PAC provisioning）**] が有効になっていることを確認します。

アクティブまたは期限切れのマスター キーで作成された既存の PAC を新しい PAC の発行に使用できる猶予期間中は、Cisco DX シリーズがネットワークに接続されているようにします。

ステージング ワイヤレス LAN がステージング RADIUS サーバだけをポイントするようにすること、およびステージング アクセス ポイント無線を未使用時に無効にすることを推奨します。

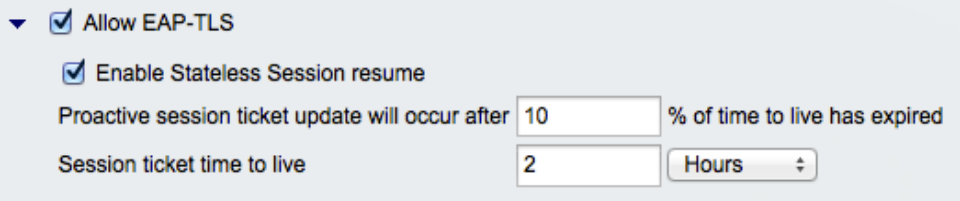
Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）は、TLS プロトコルを PKI と組み合わせて使用することで、認証サーバとの通信を保護しています。

TLS は、ユーザとサーバの両方の認証用およびダイナミック セッション キーの生成用に、証明書を使用する方法を提供します。

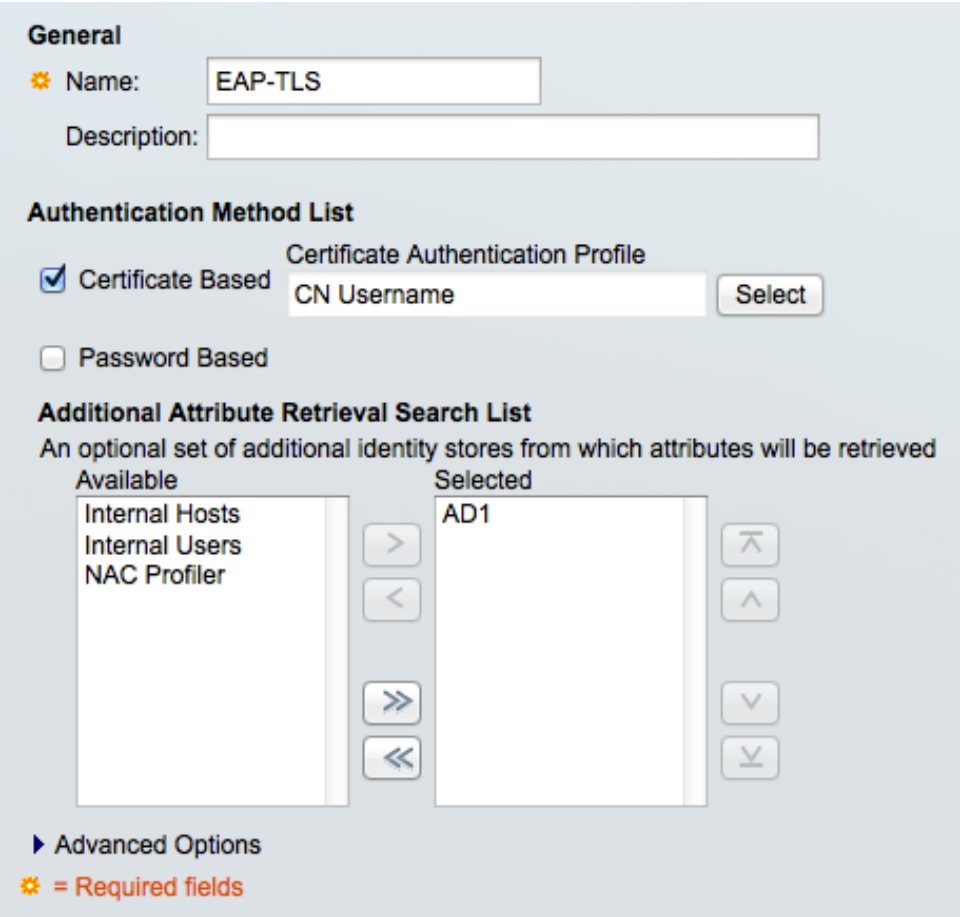
証明書をインストールする必要があります。

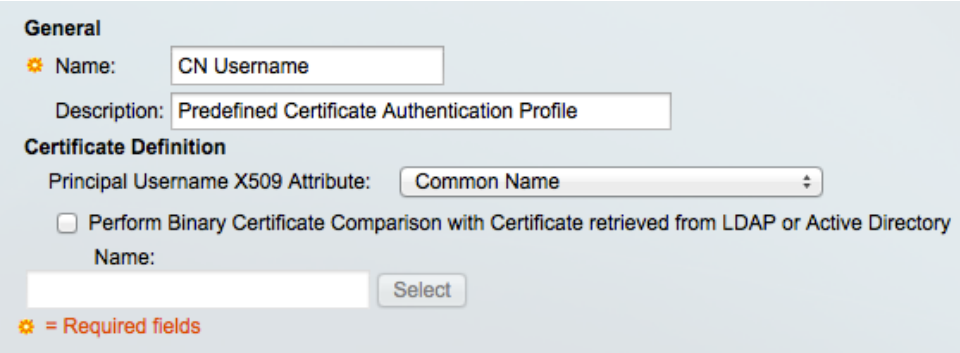
EAP-TLS は、高度なセキュリティを提供しますが、クライアント証明書の管理が必要となります。



EAP-TLS では、Cisco DX シリーズにインポートされた証明書の共通名と一致する認証サーバ上に、ユーザ アカウントが作成されていることが必要になる場合もあります。

このユーザ アカウントには複雑なパスワードを使用し、RADIUS サーバ上で有効にする EAP タイプは EAP-TLS のみにすることを推奨します。





詳細については、「証明書のインストール」を参照してください。

Protected Extensible Authentication Protocol（PEAP）

Protected Extensible Authentication Protocol（PEAP）は、サーバ側の公開キー証明書を使用してクライアントを認証するために、クライアントと認証サーバの間に暗号化された SSL/TLS トンネルを構築します。

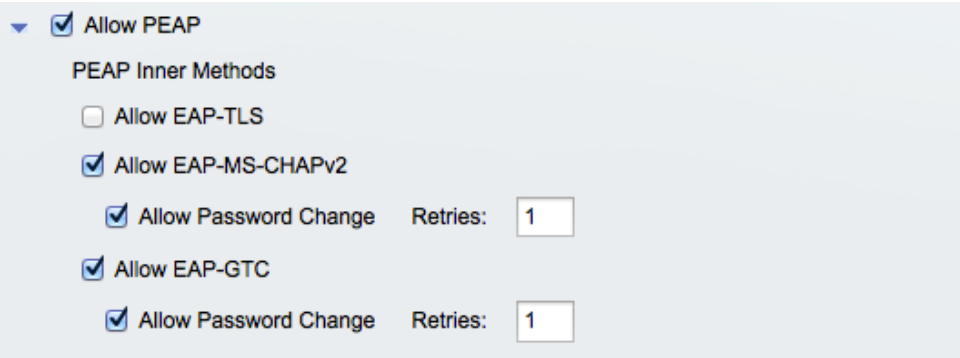
構築後の認証情報の交換は暗号化されるため、ユーザ クレデンシャルは盗聴から保護されます。

PEAP-MSCHAPv2 と PEAP-GTC はサポートされている内部認証プロトコルです。

PEAP では、認証サーバ上にユーザ アカウントを作成する必要があります。

認証サーバは、Cisco DX シリーズに証明書をインポートして検証されます。

詳細については、「証明書のインストール」を参照してください。



Cisco Secure Access Control System（ACS）と Cisco Identity Services Engine（ISE）の詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/products/security/secure-access-control-system/datasheet-listing.html

http://www.cisco.com/c/en/us/products/security/identity-services-engine/datasheet-listing.html

高速セキュア ローミング（FSR）

CCKM は、頻繁にローミングが発生するすべての環境で推奨される配置モデルです。

CCKM は、高速セキュア ローミングを可能にし、ネットワークに接続されていない時間を制限して、通話中のオーディオ ギャップを最小限に保ちます。

802.1x 認証は、CCKM を利用するために必要になります。

CCKM を使用しない 802.1x では、完全な再認証が必要になるため、ローミング時に遅延が発生する可能性があります。WPA と WPA2 では、一時的なキーが追加されるため、ローミング時間が長くなる可能性があります。

CCKM では、キー管理が集中化され、キー交換の回数が減少します。

CCKM を利用すると、ローミング時間を 400 ～ 500 ミリ秒から 100 ミリ秒未満に短縮できます。この場合、アクセス ポイント間の移行時間をユーザが体感することはなくなります。

Cisco DX シリーズは、CCKM と WPA2（AES または TKIP）の組み合わせまたは CCKM と WPA（TKIP または AES）の組み合わせをサポートしています。ここでは、WPA2（AES）と CCKM の組み合わせをお勧めします。

FSR タイプ	EAP タイプ	キー管理（Key Management）	暗号化（Encryption）
CCKM	EAP-FAST	WPA2、WPA	AES、TKIP
CCKM	EAP-TLS	WPA2、WPA	AES、TKIP
CCKM	PEAP-GTC	WPA2、WPA	AES、TKIP
CCKM	PEAP-MSCHAPv2	WPA2、WPA	AES、TKIP

EAP とユーザ データベースの互換性

次の表に、Cisco DX シリーズによりサポートされる EAP とデータベースの構成を示します。

データベース タイプ	EAP-FAST（フェーズ ゼロ）	EAP-TLS	PEAP-GTC	PEAP-MSCHAPv2
Cisco ACS	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	Yes	Yes
Windows AD	Yes	Yes	Yes	Yes
LDAP	No	Yes	Yes	No
ODBC（ACS for Windows のみ）	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS サーバ	Yes	No	Yes	Yes
すべてのトークン サーバ	No	No	No	No

電源管理

バッテリが内蔵されていないため、Cisco DX シリーズのワイヤレス LAN モードを有効にするには、電源が必要です。

Cisco DX650 は CP-PWR-CUBE-4= 電源を利用し、Cisco DX70 および DX80 は CP-PWR-CUBE-5= 電源を利用します。

ワイヤレス LAN は、イーサネットが接続されると自動的に無効になり、イーサネットが切断されたら、手動で再度有効にする必要があります。

Cisco DX シリーズは、主として、アイドル状態または着信時に、アクティブ モード（Wi-Fi 節電なし）を使用します。

電力節約なし（PS-NULL）フレームはオフチャネル スキャンで使用されます。

Delivery Traffic Indicator Message (DTIM)

DTIM 周期を **2**、ビーコン周期を **100 ミリ秒**に設定することを推奨します。

Cisco DX シリーズがアクティブ モードを使用するため、DTIM 周期は、ブロードキャストおよびマルチキャスト パケットおよびユニキャスト パケットの確認のための周期的な起動のスケジュールには使用されません。

アクセス ポイントに省電力対応のクライアントが関連付けられている場合、ブロードキャスト トラフィックとマルチキャスト トラフィックは、DTIM 周期になるまでキューイングされます。したがって、これらのパケットをクライアントにどれだけ早く届けられるかは DTIM によって決定されます。マルチキャスト アプリケーションを使用する場合は、より短い DTIM 周期を使用できます。

ワイヤレス LAN で複数のマルチキャスト ストリームが頻繁に発生する場合は、DTIM 周期を「**1**」に設定することを推奨します。

Quality of Service (QoS)

QoS により、キューイングで音声およびビデオ トラフィックに高いプライオリティを与えることができます。

音声、インタラクティブ ビデオ、およびコール制御トラフィック用に適切なキューイングを有効にするには、次のガイドラインに従ってください。

- アクセス ポイント上で **WMM** が有効になっていることを確認します。
- アクセス ポイント上で音声、インタラクティブ ビデオ、コール制御トラフィックにプライオリティを与える QoS ポリシーを作成します。

トラフィックのタイプ	DSCP	802.1p	WMM UP	ポート範囲
音声	EF（46）	5	6	UDP 16384 ～ 32767
ビデオ コールのインタラクティブ ビデオおよびオーディオ	AF41（34）	4	5	UDP 16384 ～ 32767
TelePresence コール（音声とビデオ）	CS4（32）	4	5	UDP 16384 ～ 32767
呼制御	CS3（24）	3	4	TCP 5060 - 5061

- 音声、インタラクティブ ビデオ、およびコール制御パケットが適切な QoS マーキングを持ち、他のプロトコルがそれと同じ QoS マーキングを使用していないことを確認します。
- Cisco Unified Wireless LAN Controller テクノロジーを使用する場合は WLAN 用の [**プラチナ（Platinum）**] QoS プロファイルを選択し、[802.1p タグ（802.1p tag）] を **5** に設定します。
- Cisco IOS スイッチ上で Differentiated Services Code Point（DSCP）の保護を有効にします。

（注） 音声やインタラクティブ ビデオ フレームは標準のビデオ コールでは DSCP AF41 および WMM UP 5 とマークされます。

Cisco Unified Communications Manager 10.0 リリースを含む Cisco DX シリーズの 10.1(1) リリース以降は、TelePresence コール用の音声フレームとビデオ フレームが DSCP CS4 と WMM UP 5 とマークされます。

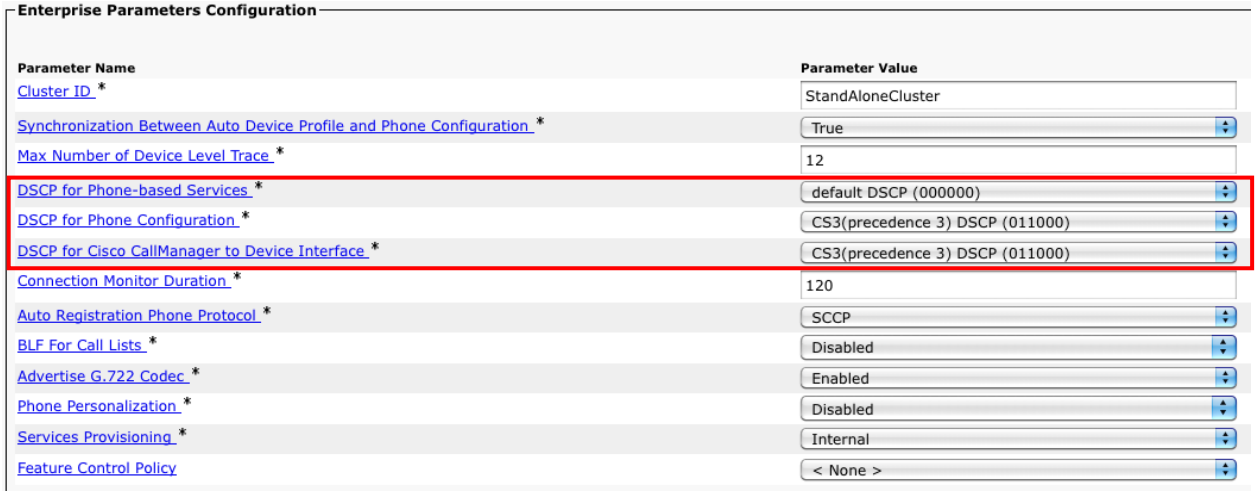
CAC（TSPEC）が音声またはビデオに対して有効になっている場合は、WMM UP マーキングがダウングレードする可能性があります。

Cisco DX シリーズと Cisco Unified Communications Manager で使用される TCP ポートと UDP ポートの詳細については、次の URL にある『Cisco Unified Communications Manager TCP and UDP Port Usage』を参照してください。

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_0_1/CUCM_BK_T537717B_00_tcp-port-usage-guide-100.html

Cisco Unified Communications Manager での QoS の設定

SIP DSCP 値は、Cisco Unified Communications Manager のエンタープライズ パラメータで設定されます。Cisco Unified Communications Manager では、デバイスに対して SIP パケットの DSCP マーキングを設定する際、[エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ページに示されているようなデフォルト値の CS3 が使用されます。



ネットワークの QoS ポリシーの設定

次のネットワーク デバイスに対して QoS ポリシーと設定を構成します。

Cisco スイッチ ポートの設定

Cisco Unified Wireless LAN Controller、シスコ製アクセス ポイントのスイッチ ポート、および任意のアップリンク スイッチ ポートを設定します。

信頼 COS に対して Cisco Unified Wireless LAN Controller を設定します。

Cisco Unified Wireless LAN Controller のスイッチ設定の例を次に示します。

```
mls qos
!
interface X
 mls qos trust cos
```

シスコのアクセス ポイントのスイッチ ポートとアップリンク ポートを信頼 DSCP に対して設定します。

アクセス ポイントのスイッチ設定の例を次に示します。

```
mls qos
!
interface X
 mls qos trust dscp
```

（注）Cisco Unified Wireless LAN Controller を使用する場合は、DSCP の信頼状態を実装するか、もしくは、QoS マーキングが正しく設定されるように、ワイヤレス パケットが通過するすべてのインターフェイス上で、Cisco Unified Wireless LAN Controller によって使用される UDP データ ポート（CAPWAP = 5246 および 5247）を信頼状態にします。

Cisco IOS アクセス ポイントの設定

Cisco IOS アクセス ポイント（AP）上で次の QoS ポリシーを使用して、CoS（UP）マッピングに対する DSCP を有効にします。これにより、正しくマーキングされている限り、パケットがアクセス ポイント レベルで受信されたときに音声キューに入れられます。

```
Class-map match-all Voice
 match ip dscp ef
class-map match-all Video
 match ip dscp af41
class-map match-all TelePresence
 match ip dscp cs4
class-map match-all CallControl
 match ip dscp cs3
!
policy-map DX
 class Voice
  set cos 6
class Video
  set cos 5
class TelePresence
  set cos 5
 class CallControl
  set cos 4
!
interface dot11radioX
 service-policy input DX
 service-policy output DX
```

Wired IP Phone のスイッチ ポートの設定

有線の Cisco IP Phone のスイッチ ポートを Cisco phone 信頼状態にします。

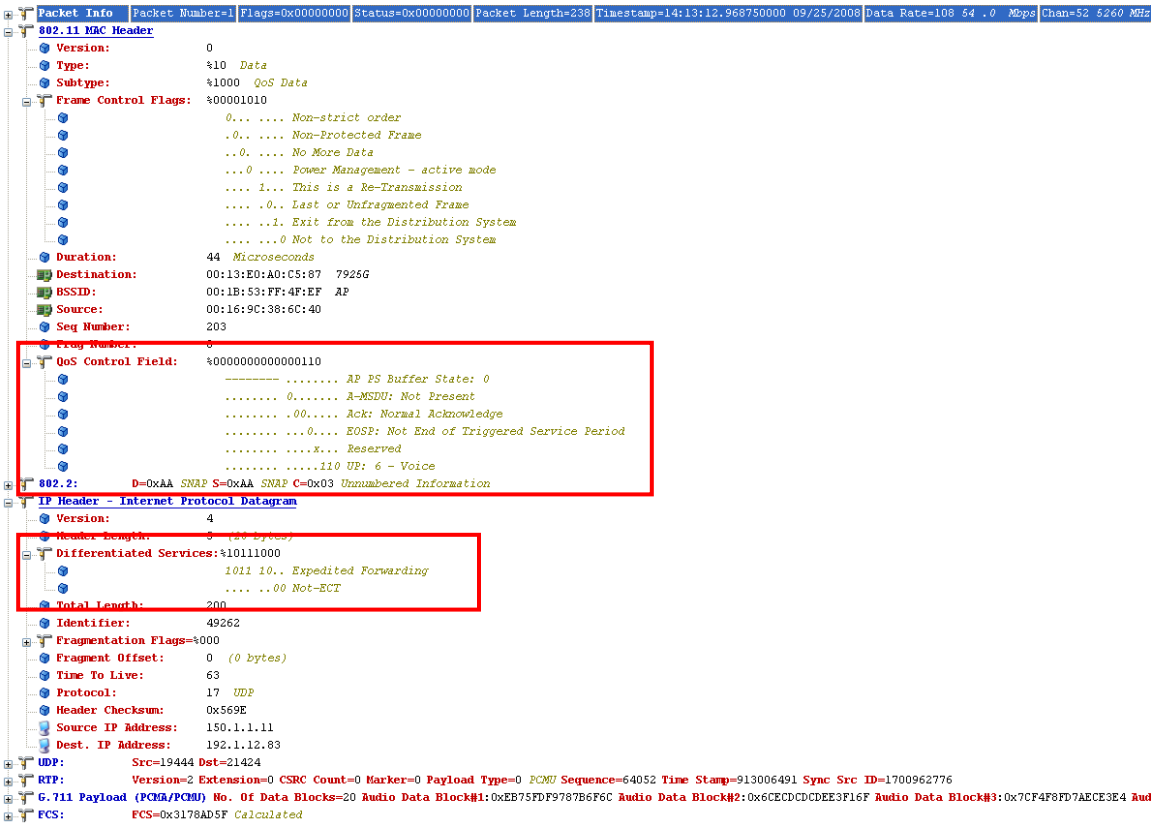
スイッチ設定の例を次に示します。

```
mls qos
!
Interface X
 mls qos trust device cisco-phone
 mls qos trust dscp
```

音声パケット キャプチャの例

次のパケット キャプチャは、ワイヤレスで Cisco DX シリーズ宛に送信された音声パケットが DSCP = EF および UP = 6 とマーキングされていることを示しています。

これには、アドミッション制御必須を音声に対し無効にする必要があります。そうしないと、Cisco DX シリーズが現在 TSPEC をサポートしないため、音声フレームが下位の User Priority(UP)にダウングレードされます。



コール アドミッション制御

Cisco DX シリーズは、現在、音声ストリームまたはビデオ ストリームのコール アドミッション制御をサポートしていません。

アクセス ポイントで TSPEC が音声またはビデオに対して有効になっている場合は、音声フレームとビデオ フレームの優先順位が下がります。

TSPEC のサポートなしでは、TCLAS もサポートされません。

TSPEC は現時点ではサポートされていないため、SIP CAC およびメディア セッションのスヌーピングは Cisco Unified Wireless LAN Controller で選択オプションで有効にできます。

SIP CAC を有効にすることの長所と短所などの詳細については「Cisco Unified Wireless LAN Controller およびアクセス ポイントの設定」セクションを参照してください。

ローミング

Cisco DX シリーズは、デフォルトで、周波数帯域モードが自動に設定されるため、5 GHz と 2.4 GHz のどちらかに接続できます。

10.2(2) リリース以降の Cisco DX シリーズでは、自動周波数帯域に設定されている場合に、2.4 GHz よりも 5 GHz の方が優先されます。

電源オン時に、DX シリーズは、自動周波数帯域モードに設定されていれば、すべての 5 GHz チャネルと 2.4 GHz チャネルをスキャンしてから、ローカルに設定されたネットワーク設定を使用して信号が強い（-67 dBm 以上）使用可能な 5 GHz アクセス ポイントへのアソシエートを試みます。電源オン時に適切な信号を備えた 5 GHz AP を使用できない場合は、DX シリーズが最も強い RSSI を備えた使用可能なアクセス ポイントへのアソシエートを試みます。

自動周波数帯域に設定されている場合は、接続後に、その周波数帯域の範囲だけがスキャンされます（たとえば、5 GHz 経由で接続された場合は、5 GHz チャネルだけがスキャンされます）。その他の周波数帯域の範囲は、現在の接続が失われた場合にだけスキャンされます。

DX シリーズの周波数帯域が 5 GHz のみまたは 2.4 GHz のみに設定されている場合は、そのチャネルのみがスキャンされ、ネイバーが検出されます。

Cisco DX シリーズは、接続先のアクセス ポイントと同じ周波数帯域の範囲に含まれるすべてのネイバーを最も強い RSSI から最も弱い RSSI の順に列挙します。

Wi-Fi 設定メニューで自動周波数帯域に設定されている場合は、5 GHz と 2.4 GHz の両方の周波数帯域がスキャンされるため、使用可能なすべての WLAN を表示できます。

スペクトル分析を実施して、必要な帯域が使用可能かどうかを確認することをお勧めします。

CCKM は、頻繁にローミングが発生するすべての環境で推奨される配置モデルです。

802.1x 認証は、CCKM を利用するために必要になります。

CCKM を使用しない 802.1x では、完全な再認証が必要になるため、ローミング時に遅延が発生する可能性があります。WPA と WPA2 では、一時的なキーが追加されるため、ローミング時間が長くなる可能性があります。

CCKM を利用すると、ローミング時間を 400 ～ 500 ミリ秒から 100 ミリ秒未満に短縮できます。この場合、アクセス ポイント間の移行時間をユーザが体感することはなくなります。

Cisco DX シリーズは、CCKM と WPA2（AES または TKIP）の組み合わせまたは CCKM と WPA（TKIP または AES）の組み合わせをサポートしています。ここでは、WPA2（AES）と CCKM の組み合わせをお勧めします。

認証	ローミング時間
WPA/WPA2 Personal	150 ミリ秒
WPA/WPA2 Enterprise	300 ミリ秒
CCKM	100 ミリ秒未満

Cisco DX シリーズは、スキャン イベントとローミング イベントを管理します。

ローミングは、次のいずれかの理由でトリガーされます。

- RSSI 差分
- 最大 Tx 再送信（アクセス ポイントから 802.11 確認応答を受信していない）
- 欠落ビーコン
- AP 切断

大部分のローミングは、その時点の RSSI に基づいて必要な RSSI との差分に応じてトリガーされる必要があります。その結果、シームレスなローミング（音声またはビデオの中断がない）が実現します。

連続する 802.11 確認応答の欠落（最大 Tx 再送信）またはアクセス ポイントからのビーコンの欠落があると、予期しないローミングがトリガーされます。

シームレスなローミングを実現するため、Cisco DX シリーズは、少なくとも 3 秒間アクセス ポイントにアソシエートされている必要があります。そうでない場合、パケット損失（送信側の最大再送数またはビーコン受信の失敗数）の発生に基づいてローミングが発生します。

現在の信号が強い RSSI のしきい値を満たしている場合、RSSI に基づくローミングは発生しない場合があります。

（注） Cisco DX シリーズでは、スキャンおよびローミングは、電話機自体によって独立して管理されるため、Cisco Unified Wireless LAN Controller のクライアント ローミング セクションの RF パラメータを使用しません。

マルチキャスト

ワイヤレス LAN でマルチキャストを有効にする場合は、パフォーマンスおよびキャパシティに配慮する必要があります。

Cisco DX シリーズは、原則としてアクティブ モードを利用するクライアントですが、省電力モードのクライアントが関連付けられている場合は、DTIM 期間になるまですべてのマルチキャスト パケットがキューイングされることになります。

マルチキャストでは、そのパケットがクライアントによって受信される保障はありません。

マルチキャスト トラフィックは、アクセス ポイント上で使用可能な最高の必須/基本データ レートで送信されます。そのため、唯一の必須/基本レートとして最低の有効なレートだけを確実に設定することが必要になります。

クライアントは、マルチキャスト ストリームを受信するために、IGMP 加入要求を送信します。セッションを終了する場合、クライアントは、IGMP 脱退要求を送信します。

Cisco DX シリーズは、IGMP クエリー機能をサポートしています。この機能を使用すれば、ワイヤレス LAN 上のマルチキャスト トラフィックの量を必要に応じて減らすことができます。

すべてのスイッチ上で IGMP スヌーピングも有効になっていることを確認します。

Cisco Unified Wireless LAN Controller では、マルチキャスト ダイレクトを有効にすることが推奨されます。

（注） 802.11b/g/n と Bluetooth を併用する場合、マルチキャスト音声はサポートされません。

ワイヤレス LAN の設計

Cisco DX シリーズに対して十分なカバレッジ、コール キャパシティ、およびシームレスなローミングを実現するために、次のネットワーク設計ガイドラインに従う必要があります。

チャネル使用の計画

次のガイドラインを使用して、各ワイヤレス環境でのチャネル使用を計画します。

5 GHz (802.11a/n)

5 GHz は、Cisco DX シリーズの運用に使用するように推奨されている周波数帯域です。

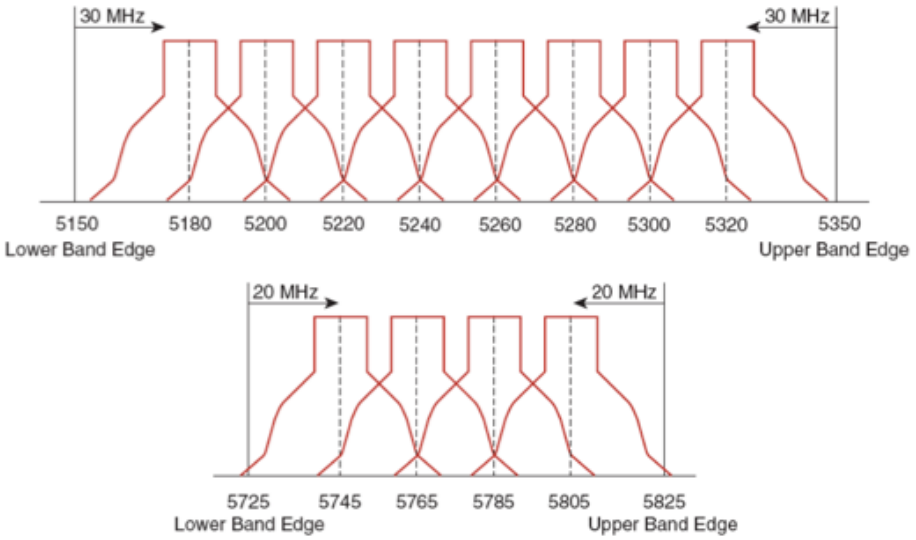
Cisco DX シリーズは、802.11h からの動的周波数選択（DFS）と Transmit Power Control（TPC）をサポートしています。これらは、5.260 ～ 5.700 GHz で動作するチャネルを使用する場合に必要です。使用可能な 24 チャネルのうち 15 チャネルがこれに該当します。

DFS では、レーダー信号が検出されると、トランスミッタは、他のチャネルにスイッチするように動的に指示されます。アクセス ポイントでレーダーが検出されると、アクセス ポイントが他の使用可能なチャネルのパッシブ スキャンを実行する間、そのアクセス ポイント上の無線は、少なくとも 60 秒間、保留状態になります。

TPC では、クライアントとアクセス ポイントが情報を交換できます。それにより、クライアントは、送信電力を動的に調整できます。クライアントは、アクセス ポイントとのアソシエーションを所定のデータ レートで維持するために、必要最低限のエネルギーを使用します。結果として、クライアントは、隣接セルの干渉の原因になりにくくなります。これにより、より密集して展開された、パフォーマンスの高いワイヤレス LAN を実現できます。

5 GHz チャネルは、それぞれの隣接チャネルとオーバーラップします。そのため、隣接アクセス ポイントに対して少なくとも 1 チャネル分の間隔が必要です。

802.11a/n 環境に Cisco DX シリーズを展開する場合は、隣接するチャネルと少なくとも 20 % のオーバーラップが存在する必要があります。これにより、シームレスなローミングが実現します。重要な領域では、Cisco DX シリーズがアクセス ポイントのレシーバ感度（現在のデータ レートに必要な信号レベル）を満たしながら、少なくとも 2 台のアクセス ポイントで -67 dBm 以上の信号を使用できるように、オーバーラップを増やす（30 % 以上）ことを推奨します。



Channel ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
Center Freq. MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805
Band	UNII-1				UNII-2															UNNII-3			

アクセス ポイント上での動的周波数選択（DFS）の使用方法

Cisco Autonomous Access Point の場合、動的周波数選択（DFS）を選択して、自動チャネル選択を使用します。

DFS が有効にされている場合、少なくとも 1 つの帯域（帯域 1 ～ 4）を有効にします。

Cisco Unified Access Point の場合、選択アクセス ポイントにチャネルが静的に割り当てられるエリア内で断続的な干渉が存在しなければ、Auto RF を有効にします。

アクセス ポイントでレーダー イベントが繰り返し検出される場合（正当なものまたは不適切なもの）、そのレーダー信号が 1 つのチャネル（ナローバンド）または複数のチャネル（ワイドバンド）に影響を与えているかどうかを特定し、ワイヤレス LAN におけるそのチャネルまたは複数のチャネルの使用を無効にします。

非 DFS チャネルに AP が存在する場合は、音声の中断を最小限に抑えることができます。

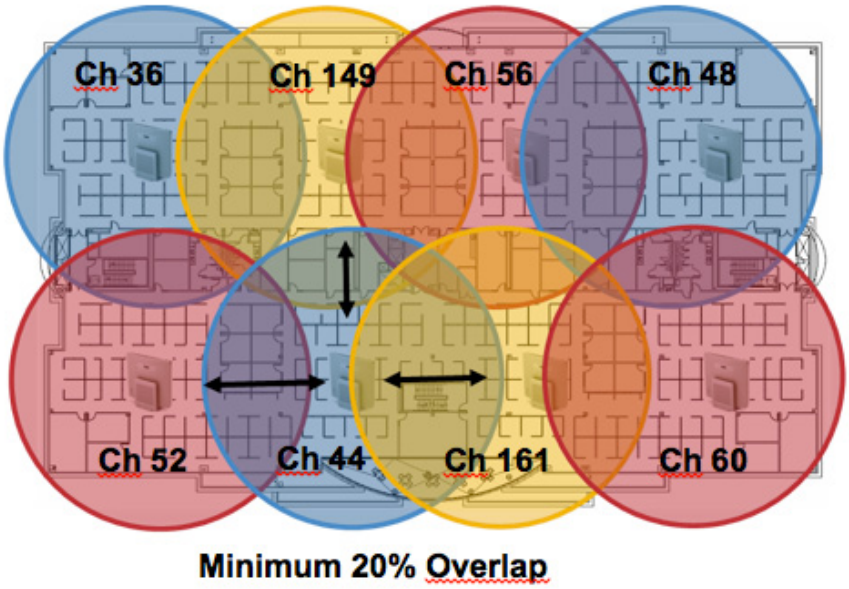
レーダー アクティビティに備えて、非 DFS チャネル（UNII-1）を使用するアクセス ポイントをエリアごとに少なくとも 1 つ設置します。これにより、新しい使用可能チャネルのスキャン中にアクセス ポイントの無線がホールドオフ期間になっているときも、チャネルを使用可能であることが保証されます。

Cisco Autonomous Access Point の場合、アクセス ポイントが UNII-1 チャネルだけを使用できる、帯域 1 のみを有効にします。

Cisco Unified Access Point の場合、任意のアクセス ポイントに UNII-1 チャネル（チャネル 36、40、44、48）を手動で選択できます。

UNII-3 チャネル（5.745 ～ 5.825 GHz）は、可能な場合に任意で使用できます。

次の図では、5 GHz セルが非 DFS チャネルを使用し、隣接する他のセルは DFS チャネルを使用することにより、いかなる状況でも最大のコール キャパシティを可能します。

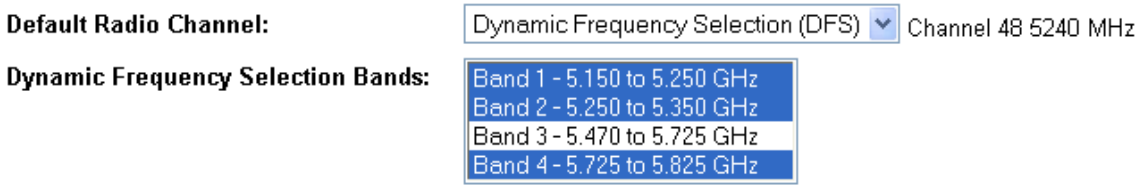


5 GHz の場合、南・北・中央アメリカでは 21 チャネル、欧州と日本では 16 チャネルを使用できます。

UNII-3 を使用可能な場所では、UNII-1、UNII-2、および UNII-3 だけを使用して 12 チャネル セットを利用することが推奨されます。

UNII-2 拡張チャネル（チャネル 100 ～ 140）の使用を予定している場合は、アクセス ポイント上で UNII-2（チャネル 52 ～ 64）を無効にして、有効になるチャネルの数が多くなり過ぎないようにすることが推奨されます。

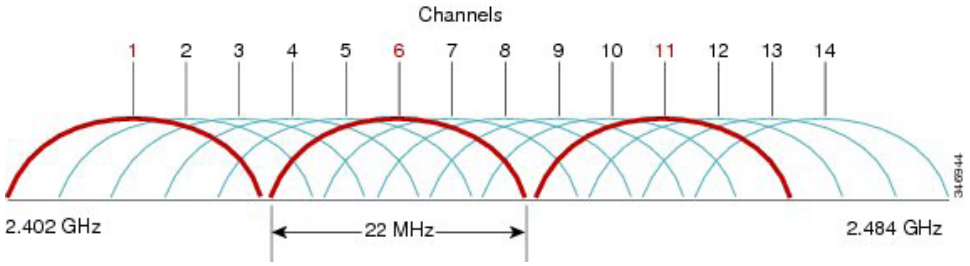
ワイヤレス LAN で多数の 5 GHz チャネルが有効にされると、新しいアクセス ポイントの検出が遅れる可能性があります。



2.4 GHz（802.11b/g/n）

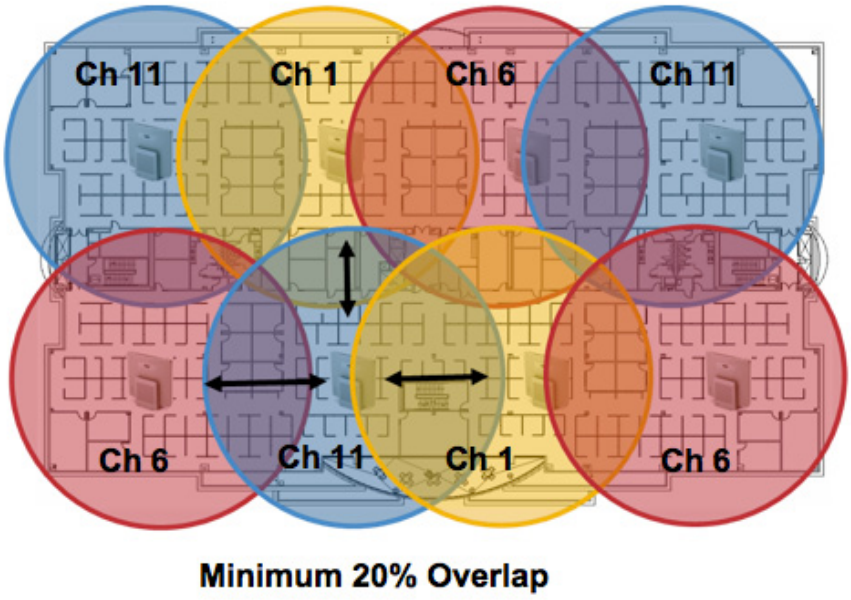
2.4 GHz（802.11b/g/n）環境では、VoWLAN を展開するとき、オーバーラップのないチャネルだけを利用する必要があります。オーバーラップのないチャネルには 22 MHz の間隔があり、少なくとも 5 チャネル離れています。

2.4 GHz 周波数範囲には、オーバーラップのないチャネルは 3 つしか存在しません（チャネル 1、6、11）。



802.11b/g/n 環境に Cisco DX シリーズを展開する場合、オーバーラップのないチャネルを使用する必要があり、隣接チャネルとのオーバーラップが少なくとも 20% 許容される必要があります。これにより、シームレスなローミングが実現します。

1、5、9、13 などのオーバーラップ チャネル セットの使用は、サポートされていない設定です。



信号強度とカバレッジ

許容可能な音声品質を保障するため、Cisco DX シリーズは 2.4 GHz または 5 GHz を使用する場合、-67 dBm 以上の信号を常に維持しつつ、アクセス ポイントのレシーバ感度で必要な送信されたデータ レートの信号レベルに対応しています。

Packet Error Rate（PER）が 1 % を超えていないことを確認してください。

25 dB の最小 Signal to Noise Ratio（SNR）が -67 dBm である信号に対して -92 dBm のノイズ レベルが維持される必要があります。

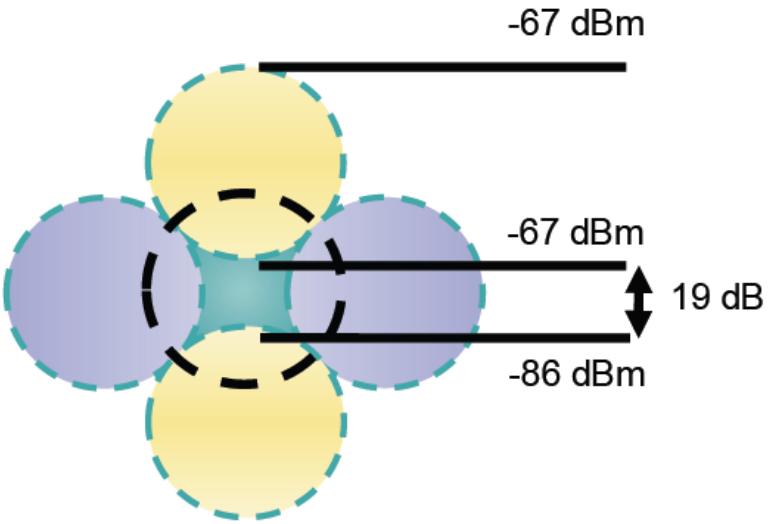
冗長性を持たせるために、オーバーラップのないチャネル上に SNR が 25 dB の最低でも -67 dBm の信号を持つアクセス ポイントを 2 つ以上設置することが推奨されます。

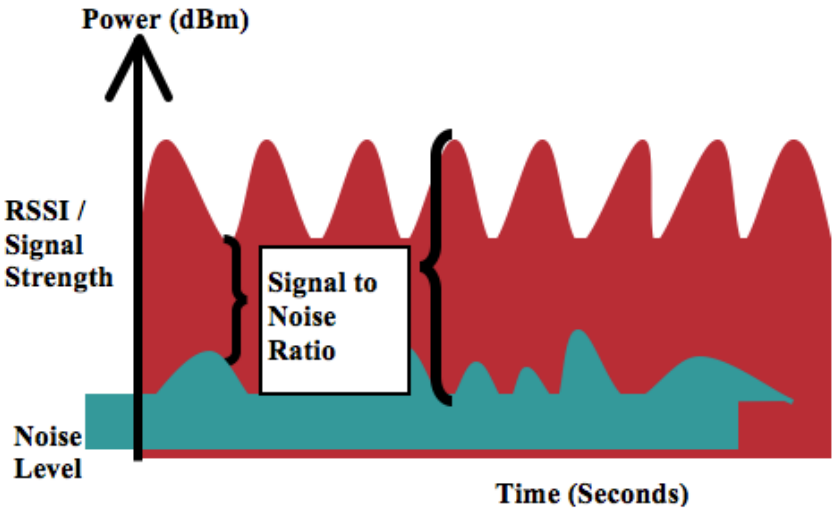
最大のキャパシティとスループットを実現するには、ワイヤレス LAN を 24 Mbps に設計する必要があります。それよりも高いデータ レートは、そのようなデータ レートを利用できる音声専用以外のアプリケーションに対して任意で有効にできます。

2.4 GHz の場合は最小データ レートを 11 Mbps または 12 Mbps に（802.11b クライアント サポート ポリシーに従う）、5 GHz の場合は最小データ レートを 12 Mbps に設定することが推奨されます。これは、必須/基本レートとして設定される唯一のレートにする必要もあります。

一部の環境では、必須/基本レートとして 6 Mbps を有効しなければならない場合があります。

上記の各要件を考慮すると、シングル チャネル計画は展開すべきではありません。





アクセス ポイントの設置を設計するときは、すべての重要エリアに適切なカバレッジ（信号）が必ず提供されるようにします。

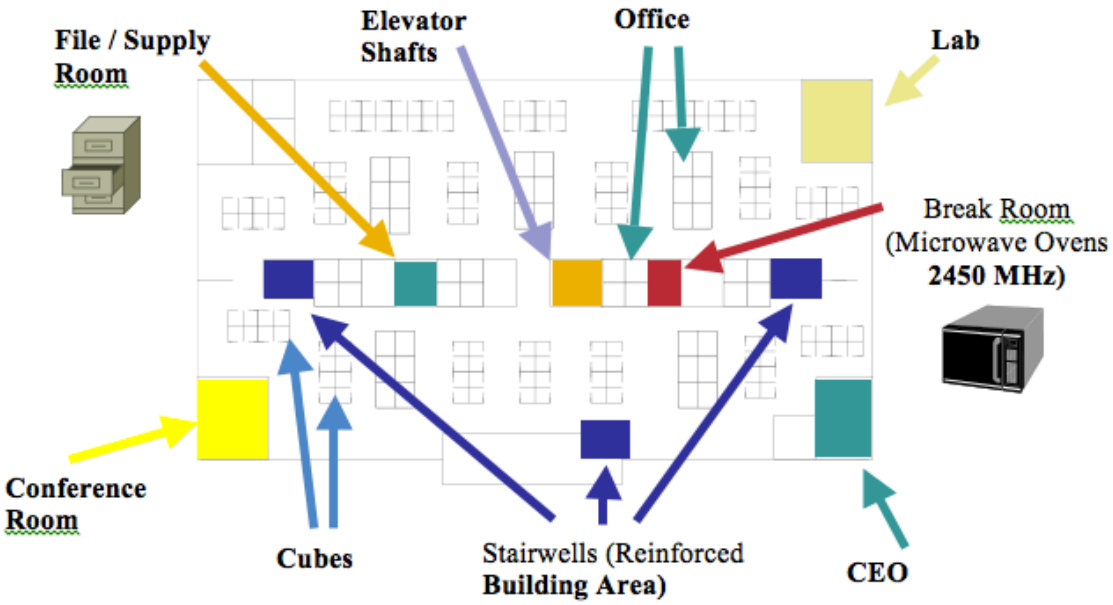
データ専用アプリケーションのための一般的なワイヤレス LAN 展開では、エレベータ、階段、屋外通路など、VoWLAN サービスで必要とされる一部のエリアにカバレッジが提供されません。

ワイヤレス LAN の干渉は、電子レンジ、2.4 GHz コードレス電話機、Bluetooth デバイス、または 2.4 GHz 帯域で動作するその他の電子製品によって発生します。

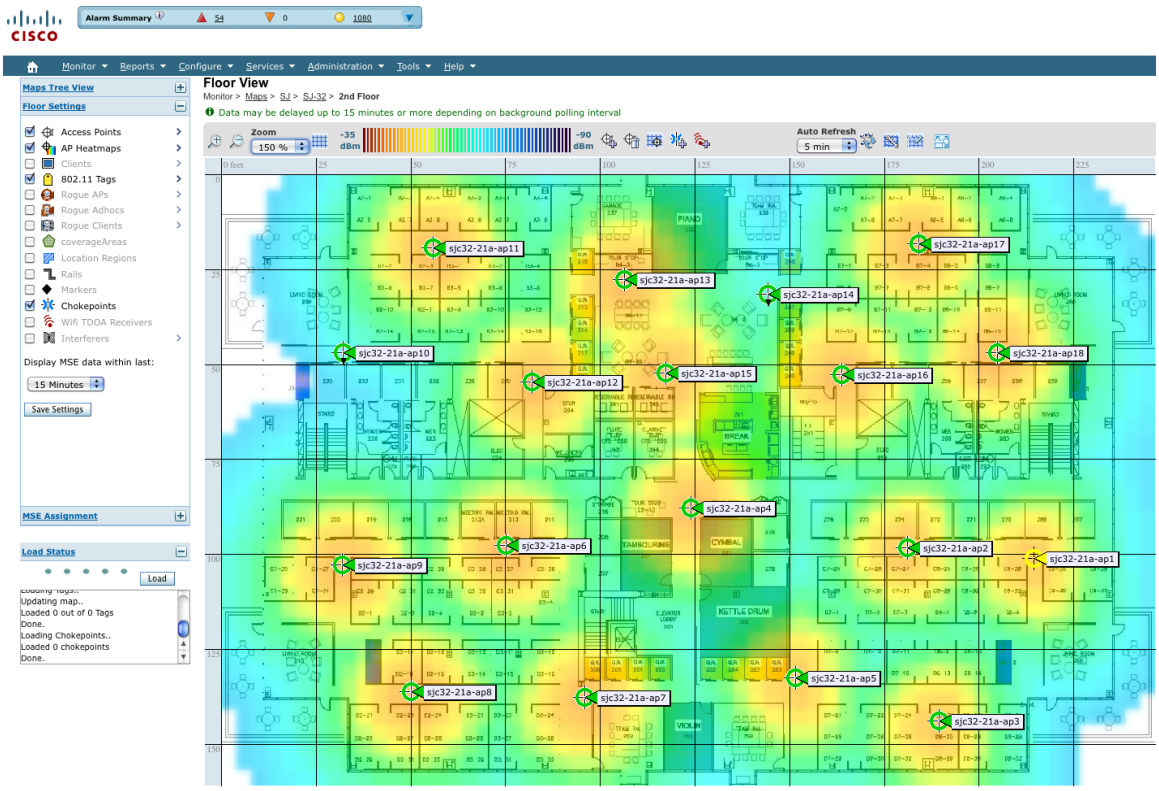
電子レンジは、2450 MHz で動作します。これは、802.11b/g/n のチャネル 8 と 9 の間にあります。一部の電子レンジは他のものよりもシールドが強化されており、そうしたシールドにより、エネルギーの拡散が減少します。電子レンジのエネルギーは、チャネル 11 に悪影響を及ぼす可能性があります。さらに一部の電子レンジは、周波数範囲全体（チャネル 1 ～ 11）に影響する可能性があります。電子レンジの干渉を回避するために、電子レンジの近くに配置されるアクセス ポイントでは、チャネル 1 を選択して使用します。

ほとんどの電子レンジ、Bluetooth、および周波数ホッピング デバイスは、5 GHz 周波数に対して同様の効果を与えることはありません。802.11a/n テクノロジーでは、オーバーラップのないチャネルがより多く提供され、通常はより低い初期 RF 使用率となります。音声展開の場合、音声には 802.11a/n を使用し、データには 802.11b/g/n を使用することが推奨されます。

ただし、免許申請の必要のない 5 GHz 周波数を利用する製品も存在します（たとえば、5.8 GHz コードレス電話機は、UNII-3 チャネルに悪影響を及ぼす可能性があります）。



Cisco Unified WCS または NCS を使用して、信号強度とカバレッジを確認できます。



データ レートの設定

キャパシティと範囲が最良の結果を得る重要な要因になるため、5 GHz 展開と 2.4 GHz 展開の 12 Mbps 未満のレートを無効にすることをお勧めします。

Cisco DX シリーズは単一アンテナのため、802.11n 接続に対して最大で MCS 7 データ レート(最大 50 Mbps)をサポートします。

より高い MCS レートは、同じ帯域周波数を利用して、これらのより高いレートを使用できる MIMO(複数入力/出力)アンテナ テクノロジーを利用する他の 802.11n クライアント向けに有効にしておくことができます。

ワイヤレス ネットワーク内で 802.11b クライアントが許可されない場合は、12 Mbps 未満のデータ レートを無効にすることが強く推奨されます。これにより、802.11b クライアントが OFDM フレームを検出できないために 802.11g 保護の CTS フレームを送信する必要性はなくなります。

802.11b クライアントがワイヤレス ネットワーク内に存在する場合は、802.11b のレートを有効にする必要があり、802.11b のレートだけが必須/基本レートとして設定できます。この場合、11 Mbps 以上のデータ レートを有効にすることが推奨されます。

推奨されるデータ レート設定は次のとおりです。

802.11 モード (802.11 Mode)	必須 データ レート	サポート済み データ レート	無効 データ レート
802.11a/n	12 Mbps	18 ～ 54 Mbps、 HT MCS 1 ～ MCS 7 (HT MCS 8 ～ MCS 23)	6、9 Mbps HT MCS 0
802.11g/n	12 Mbps	18 ～ 54 Mbps、 HT MCS 1 ～ MCS 7 (HT MCS 8 ～ MCS 23)	1、2、5.5、6、9、11 Mbps、 HT MCS 0

802.11b/g/n	11 Mbps	12 ～ 54 Mbps HT MCS 1 ～ MCS 7 （HT MCS 8 ～ MCS 23）	1、2、5.5、6、9 Mbps、 HT MCS 0
802.11a	12 Mbps	18 ～ 54 Mbps	6、9 Mbps
802.11g	12 Mbps	18 ～ 54 Mbps	1、2、5.5、6、9、11 Mbps
802.11b/g	11 Mbps	12 ～ 54 Mbps	1、2、5.5、6、9 Mbps
802.11b	11 Mbps	なし	1、2、5.5 Mbps

音声専用アプリケーションでは、24 Mbps よりも高いデータ レートは有効にも、無効にも選択できますが、キャパシティとスループットの観点において利点はありません。また、これらのレートを有効にすると、データ フレームの再試行回数が増加する可能性があります。

ビデオなどの他のアプリケーションでは、これらの高いデータ レートを有効にすると、恩恵が受けられる場合があります。

高いキャパシティとスループットを維持するには、24 Mbps 以上のデータ レートを有効にする必要があります。

過度の再試行数が問題となる可能性がある環境への導入の場合、データ レートの制限付きセットを使用できます（12、24、54、MCS 1、MCS 4、MCS 7）。この場合、最低の有効なレートは必須/基本レートです。

条件の厳しい環境または最大距離を必要とする配置では、必須/基本レートとして 6 Mbps を有効にすることが推奨されます。

（注）環境によっては、レガシー クライアント、環境要因、または最大範囲を使用する必要があるため、有効なデータ レートを下げる必要があります。

単一必須/基本レートとして、有効な最も低いデータ レートだけを設定します。マルチキャスト パケットは、有効な最も高い必須/基本データ レートで送信されます。

有効にするレートを下げると、キャパシティとスループットが減少することに注意してください。

コール キャパシティ

目的のコール キャパシティに対応するネットワークを設計します。

シスコのアクセス ポイントは、24 Mbps 以上のデータ レートで 802.11a/n と 802.11g/n の両方に対して最大 27 個の双方向音声ストリームをサポートできます。このキャパシティを実現するには、ワイヤレス LAN バックグラウンド トラフィックと初期無線周波数（RF）使用率を最小限にする必要があります。

コール数は、データ レート、チャネルの初期使用率、および環境によって異なります。

最大ストリーム数	オーディオ コーデック	オーディオ ビット レート	**802.11 モード（802.11 Mode）**	データ レート
13	G.722 / G.711	64 Kbps	802.11a/n または 802.11g/n + Bluetooth 無効	6 Mbps
20	G.722 / G.711	64 Kbps	802.11a/n または 802.11g/n + Bluetooth 無効	12 Mbps
27	G.722 / G.711	64 Kbps	802.11a/n または 802.11g/n + Bluetooth 無効	24 Mbps 以上

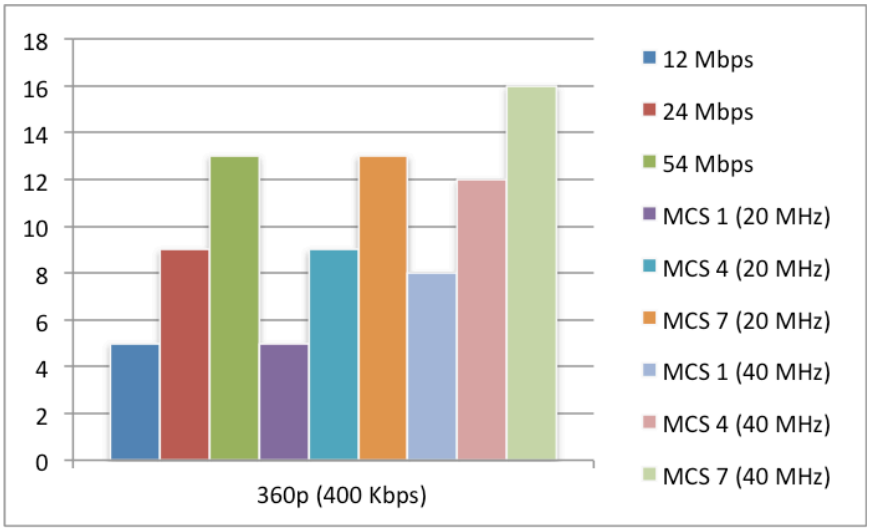
ビデオ コール

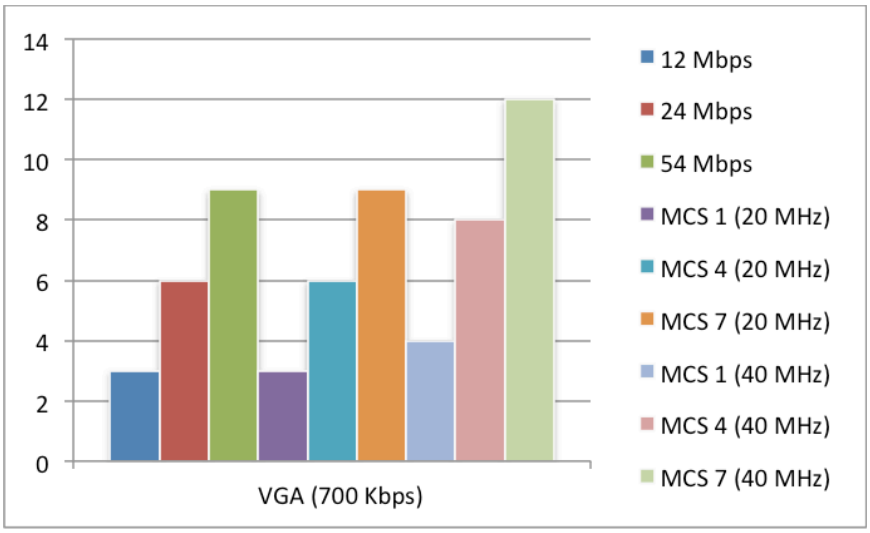
ワイヤレス LAN 上でビデオ コールを行うと、コール キャパシティが著しく低下します。

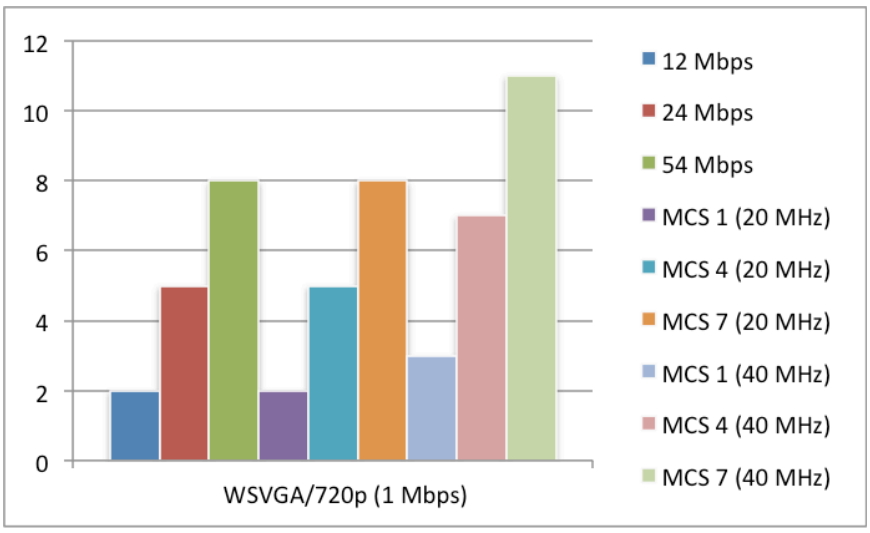
以下は、各ビデオ ビット レートでの、アクセス ポイント/チャネルごとにサポートされるビデオ コール（単一の双方向の音声およびビデオ ストリーム）の最大数のリストです。

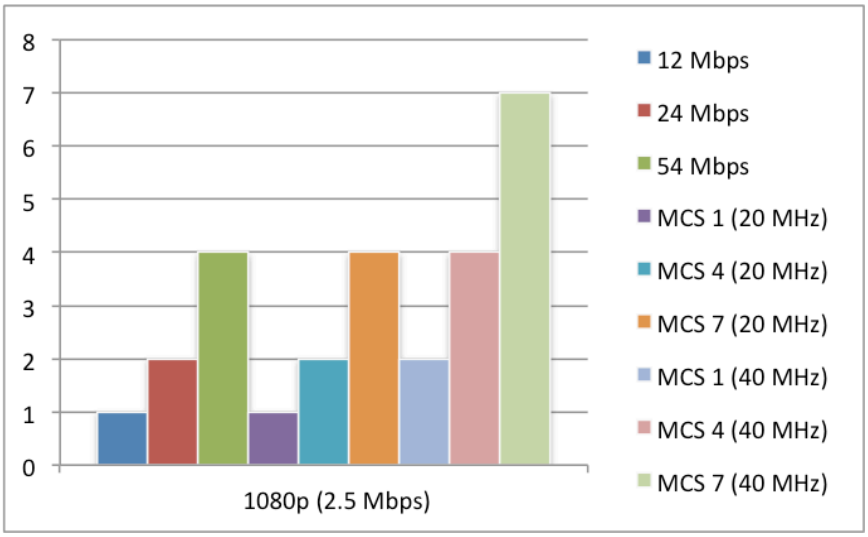
相互に通信する 2 台の Cisco DX シリーズのエンドポイントがある場合、2 つの双方向の音声およびビデオ ストリームになります。

最大数ビデオコール	802.11 モード	802.11 データレート	オーディオコーデック	オーディオビットレート	ビデオのタイプ	ビデオ解像度	ビデオビットレート
5 ～ 13	802.11a または 802.11g + Bluetooth 無効	12 ～ 54 Mbps	G.722 / G.711	64 Kbps	360p	640 x 360	400 kBps
5 ～ 13	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 20 個）	G.722 / G.711	64 Kbps	360p	640 x 360	400 kBps
8 ～ 16	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 40 個）	G.722 / G.711	64 Kbps	360p	640 x 360	400 kBps
3 ～ 9	802.11a または 802.11g + Bluetooth 無効	12 ～ 54 Mbps	G.722 / G.711	64 Kbps	VGA	640 X 480	700 kBps
3 ～ 9	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 20 個）	G.722 / G.711	64 Kbps	VGA	640 X 480	700 kBps
4 ～ 12	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 40 個）	G.722 / G.711	64 Kbps	VGA	640 X 480	700 kBps
2 ～ 8	802.11a または 802.11g + Bluetooth 無効	12 ～ 54 Mbps	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 kBps
2 ～ 8	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 20 個）	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 kBps
3 ～ 11	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 40 個）	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 kBps
1 ～ 4	802.11a または 802.11g + Bluetooth 無効	12 ～ 54 Mbps	G.722 / G.711	64 Kbps	1080p	1920 X 1080	2500 kBps
1 ～ 4	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 20 個）	G.722 / G.711	64 Kbps	1080p	1920 X 1080	2500 kBps
2 ～ 7	802.11a/n または 802.11g/n + Bluetooth 無効	MCS 1 ～ MCS 7（MHz チャネル 40 個）	G.722 / G.711	64 Kbps	1080p	1920 X 1080	2500 kBps


18
16
14
12
10
8
6
4
2
0
360p (400 Kbps)
12 Mbps
24 Mbps
54 Mbps
MCS 1 (20 MHz)
MCS 4 (20 MHz)
MCS 7 (20 MHz)
MCS 1 (40 MHz)
MCS 4 (40 MHz)
MCS 7 (40 MHz)


14
12
10
8
6
4
2
0
VGA (700 Kbps)
12 Mbps
24 Mbps
54 Mbps
MCS 1 (20 MHz)
MCS 4 (20 MHz)
MCS 7 (20 MHz)
MCS 1 (40 MHz)
MCS 4 (40 MHz)
MCS 7 (40 MHz)


12
10
8
6
4
2
0
WSVGA/720p (1 Mbps)
12 Mbps
24 Mbps
54 Mbps
MCS 1 (20 MHz)
MCS 4 (20 MHz)
MCS 7 (20 MHz)
MCS 1 (40 MHz)
MCS 4 (40 MHz)
MCS 7 (40 MHz)



(注)ビデオに対するコール アドミッション制御のサポートは現在ありません。

ダイナミック伝送パワー コントロール(DTPC)

Cisco DX シリーズとアクセス ポイント間で正常にパケットを交換するには、ダイナミック送信電力コントロール(DTPC)を有効にする必要があります。

DTPC により、RF トラフィックが一方向のみに聞こえる場合に一方向オーディオを防止できます。

アクセス ポイントで DTPC がサポートされていない場合、Cisco DX シリーズでは、現在のチャネルおよびデータ レートに応じて使用可能な最大送信電力を使用します。

DTPC をサポートするアクセス ポイントを使用する場合は、クライアントの電力がローカル アクセス ポイントの電力に一致するように設定します。

Cisco Autonomous Access Point では、クライアントの電力に対してデフォルトの**最大**電力設定を使用しないでください。デフォルトを使用すると、DTPC がクライアントにアドバタイズされません。

アクセス ポイントの無線送信電力は、Cisco DX シリーズがサポートできる送信電力を超えないようにしてください。

条件の厳しい環境

条件の厳しい環境(製造、倉庫、小売業)で Cisco DX シリーズを導入する場合、標準の推奨事項に追加の調整が必要となる場合があります。

条件の厳しい環境にワイヤレス LAN を展開する場合に注意する重要なポイントは次のとおりです。

アクセス ポイントおよびアンテナの選択
条件の厳しい環境では、外部アンテナ(Cisco 1602e、2602e、3502e、3602e、および 3702e シリーズ アクセス ポイントなど)が必要なアクセス ポイント プラットフォームを選択することを推奨します。条件の厳しい環境で適切に機能するアンテナ タイプが選択されることを確認することも大切です。

アクセス ポイントの配置

Cisco DX シリーズとアクセス ポイントとの間の障害物がなるべくないようにすることで、できる限り広い範囲からアクセス ポイントのアンテナが見通せるようにすることが重要です。アクセス ポイントまたはアンテナ、またはその両方が障害物の背後または金属面やガラス面の近くに配置されていないことを確認します。

統合アンテナを備えたアクセス ポイント（Cisco 1040、1130、1140、1602i、2602i、3502i、3602i、および 3702i シリーズ アクセス ポイントなど）が一部のエリアで使用される場合、アクセス ポイントは全方向性アンテナを搭載していており、パッチ用には設計されていないため、天井に取り付けることを推奨します。

周波数帯域

これまで通り、5 GHz の使用が推奨されます。802.11b レートが有効な場合は特に、2.4 GHz を使用すると、正常に機能しない場合があります。

5 GHz チャネル セットでは、8 または 12 チャネル計画のみを使用することを推奨します。可能な場合は、UNII-2 拡張チャネルを無効にします。

データ レート

マルチパスが高いレベルにある場合は、標準の推奨データ レート セットが適切に機能しない可能性があります。

そのため、低いデータ レート（6 Mbps など）を有効にしてこのような環境での運用を改善させることを推奨します。

音声専用に使用する場合は、24 Mbps を超えるデータ レートを無効にして最初の伝送成功率を上げることができます。

同じ帯域をデータ、ビデオ、またはその他のアプリケーションにも使用する場合は、より高いデータ レートを有効にすることをお勧めします。

送信電力

条件の厳しい環境における高マルチパスの可能性により、アクセス ポイントおよび Cisco DX シリーズの送信電力も制限する必要があります。これは、条件の厳しい環境に 2.4 GHz を展開しようと計画している場合にさらに重要です。

自動送信電力を使用する場合は、アクセス ポイントの送信電力が指定した範囲（最大および最小の電力レベル）を使用するように設定して、アクセス ポイントの送信の温度が上がり過ぎたり、脆弱になりすぎないようにします（5 GHz の場合、11 ～ 16 dBm）。

Cisco DX シリーズは、DTPC がアクセス ポイントの設定で有効になっている場合、送信されたフレームでどの送信電力を使用するかを指定するために、アクセス ポイントの現在の送信電力設定を使用します。

高速ローミング

高速ローミングに CCKM を使用することが推奨されます。CCKM を有効にすると、2 つのフレームのみにローミングする場合に、ハンドシェイクのフレームの数が減ります。ローミング中にフレーム数が減ると、ローミングが成功するチャンスが増えます。

802.1x 認証を使用している場合は、推奨された EAPOL キー設定を使用することが大切です。詳細については、「**Cisco Unified Wireless LAN Controller およびアクセス ポイントの設定**」の「**WLAN コントローラの高度な EAP 設定**」の項を参照してください。

Quality of Service（QoS）

Cisco Unified Wireless LAN Controller とアクセス ポイントが音声およびコール制御フレーム用に WMM UP タグを設定できるように、有線ネットワーク全体で DSCP 値が維持されていることを確認する必要があります。

ビーム形成

Cisco 802.11n アクセス ポイントを使用している場合は、ビーム形成（ClientLink）を有効にする必要があります。これは、クライアントの受信に役立ちます。

詳細については、「**Cisco Unified Wireless LAN Controller およびアクセス ポイントの設定**」の「**ビーム形成（ClientLink）**」の項を参照してください。

マルチパス

RF 信号が送信元から宛先まで複数の経路をたどると、マルチパスが発生します。

信号の一部が宛先に到達する一方、信号の別の部分は障害にぶつかり、その後に宛先に到達します。その結果、一部の信号では遅延が発生し、宛先までの経路が長くなるので、信号エネルギーが損失します。

異なる波形を組み合わせると、歪みが発生し、信号の質が下がるために受信機のデコード機能に影響します。

マルチパスは、反射面（金属やガラスなど）の存在する環境で発生する場合があります。このような反射面には、アクセス ポイントを取り付けないでください。

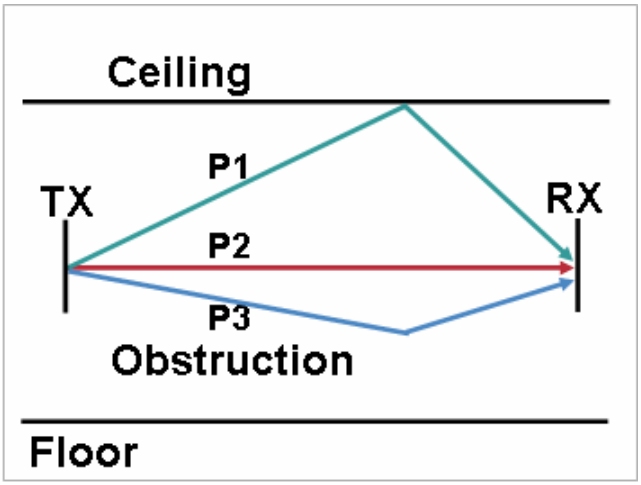
次に、マルチパスの影響を示します。

データ破損
マルチパスが非常に激しいために、送信された情報を受信機が検出できない場合に発生します。

信号の空白
反射した波長が、メイン信号とちょうど位相がずれて到達し、メイン信号を完全に打ち消すような場合に発生します。

信号振幅の増大
反射された波形が、メイン信号と位相が一致して到達し、メイン信号と重なり合って信号強度を増大させる場合に発生します。

信号振幅の減少
反射された電波が、ある程度メイン信号とずれた位相に到達し、そのためメイン信号の信号振幅が減少する場合に発生します。



802.11a/n および 802.11g/n で使用される直交周波数分割多重（OFDM）を使用することで、高マルチパス環境に見られる問題が軽減される場合があります。

高マルチパス環境で 802.11b を使用する場合、それらのエリアには低いデータ レートを使用してください（1 Mbps や 2 Mbps など）。

このような環境には、ダイバーシティ アンテナが役立つことがあります。

サイト調査ツールによる確認

次に示す多数のツールとアプリケーションは、カバレッジ、品質、および設定の確認に利用できます。

- Unified Wireless LAN 管理用の Cisco Prime Network Control System（NCS）

  http://www.cisco.com/c/en/us/products/collateral/wireless/prime-network-control-system-series-appliances/data_sheet_c78-650051.html
- Unified Wireless LAN 管理用の Cisco Wireless Control System（WCS）

  http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd802570d0.html
- シスコ自律分散型ワイヤレス LAN 管理用の Cisco Wireless LAN Solution Engine（WLSE）

  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/ciscoworks-wireless-lan-solution-engine-software-2-13/product_data_sheet0900aecd80410b92.html
- Cisco Spectrum Expert

  http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert/product_data_sheet0900aecd807033c3.html
- Cisco Unified Operations Manager

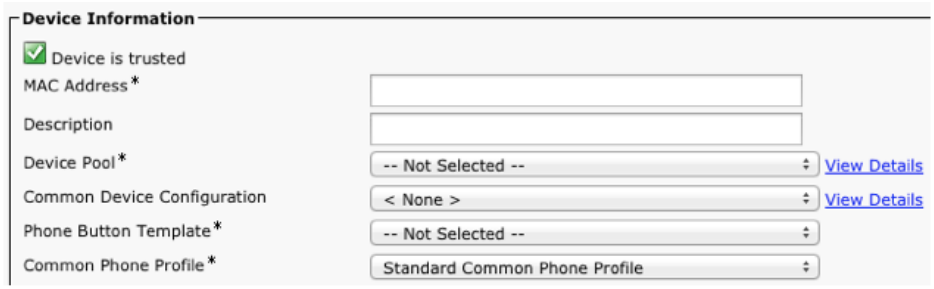
  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-unified-operations-manager/data_sheet_c78-636705.html

Cisco Unified Communications Manager の設定

Cisco Unified Communications Manager には、さまざまな製品、発呼機能、およびセキュリティ機能が搭載されています。

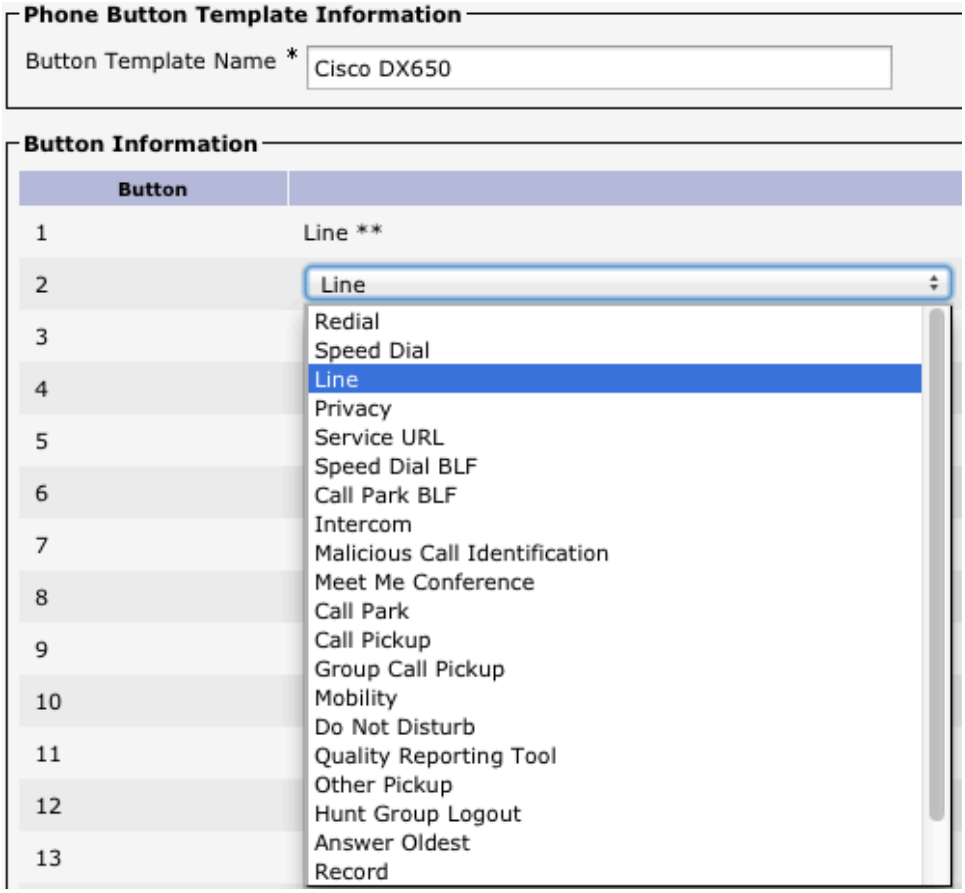
Cisco DX シリーズを Cisco Unified Communications Manager に追加する際、イーサネット MAC アドレスを使用して無線 LAN MAC を Wi-Fi 接続だけに使用するようにプロビジョニングする必要があります。

Cisco DX シリーズの **[設定（Settings）] > [デバイスについて（About Device）] > [ステータス（Status）]** に移動してイーサネット MAC アドレスを確認できます。



電話ボタン テンプレート

さまざまな機能に対するオプションを使用して、カスタムの電話ボタン テンプレートを作成できます。作成したテンプレートは、デバイスまたはグループ レベルで適用できます。

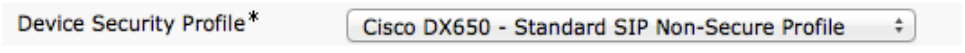


セキュリティ プロファイル

セキュリティ プロファイルを使用して、認証モードや、シグナリング、メディアおよびコンフィギュレーション ファイルが暗号化される暗号化モードを有効にできます。

セキュリティ プロファイルで Locally Signed Certificate（LSC）を使用にするには、Certificate Authority Proxy Function（CAPF）が動作している必要があります。

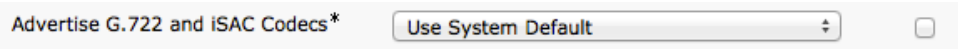
Cisco DX シリーズには、セキュリティ プロファイルも参照できる Manufacturing Installed Certificate（MIC）があります。



G.722 と iSAC のアドバタイズメント

Cisco Unified Communications Manager は、G.722 と iSAC をコーデック システム全体でサポートするかどうかを設定する機能をサポートしています。

G.722 コーデックと iSAC コーデックは、[**G.722 および iSAC コーデックのアドバタイズ（Advertise G.722 and iSAC Codecs）**] を [**無効（Disabled）**] に設定することで、会社の電話、共通の電話プロファイル、または個別の電話で無効にすることができます。



詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

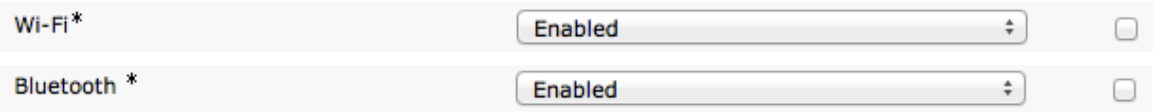
共通設定

ワイヤレス LAN および Bluetooth などの設定では、エンタープライズ電話、共通の電話プロファイル、または個々の電話レベルで設定できます。

ワイヤレス LAN および Bluetooth はデフォルトで有効です。

ワイヤレス LAN は、イーサネットが接続されると自動的に無効になり、イーサネットが切断されたら、手動で再度有効にする必要があります。

共通設定のオーバーライドは、いずれかの設定レベルで有効にできます。



オーディオおよびビデオのビット レート

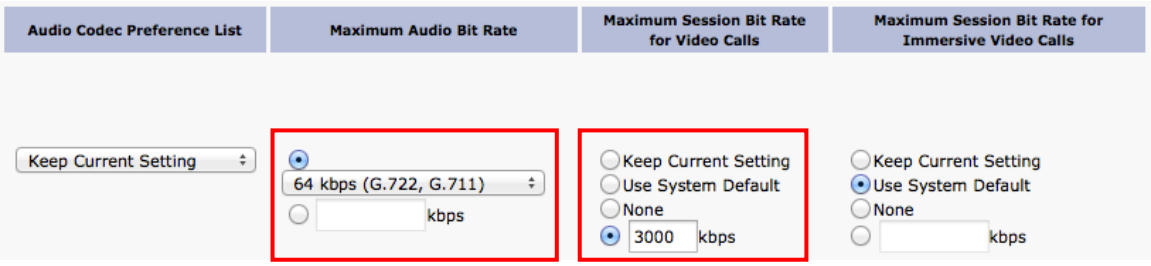
オーディオおよびビデオのビット レートを設定する場合は、Cisco Unified Communications Manager でリージョンを作成するか、既存のリージョンを編集します。

オーディオ コーデックには、G.722 または G.711 を選択することをお勧めします。

デフォルトでは、ビデオ コールのビット レートは 384 Kbps に設定されます。

標準的な展開では、ビデオ ストリームに 600p（1100 ～ 3000 kbps）または HD 720p（1000 ～ 1599 kbps）を使用することをお勧めします。

ビデオ品質を上げる場合は、HD 720p（G.722 オーディオを含めて全部で 1064 Kbps）を利用する場合はビデオ コール ビット レートを 1 Mbps に、HD 1080p（G.722 オーディオを含めて全部で 2064 Kbps）を利用する場合はビデオ コール ビット レートを 2 Mbps に設定します。



オーディオ ビット レートを音声または音声 + ビデオ コールで使用するよう設定するには、次の情報を使用します。

オーディオ コーデック	オーディオ ビット レート
AAC-LD	128 Kbps
G.722 / G.711	64 Kbps
iSAC	32 kBps
iLBC	16 Kbps
G.729	8 Kbps

ビデオ コールで使用するビデオ ビット レートを設定するには、次の情報を使用します。

設定された値で Cisco DX シリーズから送信されたビデオ ストリームの解像度が決まります。

Cisco DX シリーズは、リージョン設定が考慮されたリモート デバイスの機能によって、最大 HD 1080p ビデオまで受信できます。

Cisco DX シリーズは、現在のネットワーク接続が高いビデオ解像度をサポートできない場合、ビデオ ビット レートを必要に応じて調整可能な、ビデオ帯域幅適応をサポートしています。

ビデオのタイプ	ビデオ解像度	フレーム/秒（fps）	ビデオ ビット レート範囲
240p	432 x 240	15 / 30	64 ～ 149 Kbps / 150 ～ 2999 Kbps
360p	640 x 360	30	300 ～ 649 Kbps
480p	848 x 480	30	650 ～ 999 Kbps
600p	1024 x 600	30	1100 ～ 3000 Kbps
HD 720p	1280 x 720	30	1000 ～ 1599 Kbps
HD 1080p	1920 X 1080	30	1600 ～ 4000 Kbps
CIF	352 x 288	30	64 ～ 159 Kbps
VGA	640 X 480	30	400 ～ 1500 Kbps

ビデオ通話機能

Cisco DX シリーズでビデオを送受信するには、その機能を Cisco Unified Communications Manager で有効にする必要があります。

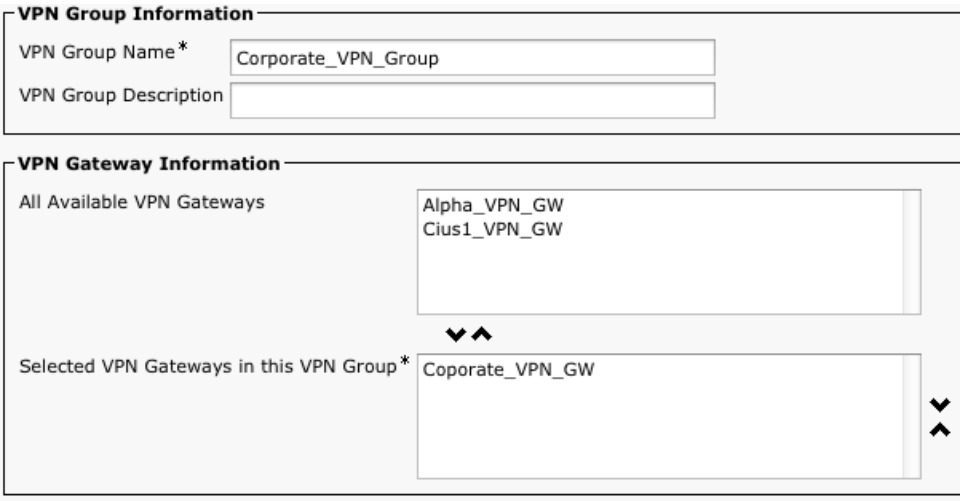
[プロダクト固有の設定（Product Specific Configuration Layout）] セクション内の電話機の設定で、[**ビデオ通話（Video Calling）**] オプションを [**有効（Enabled）**] に設定します。

VPN の設定

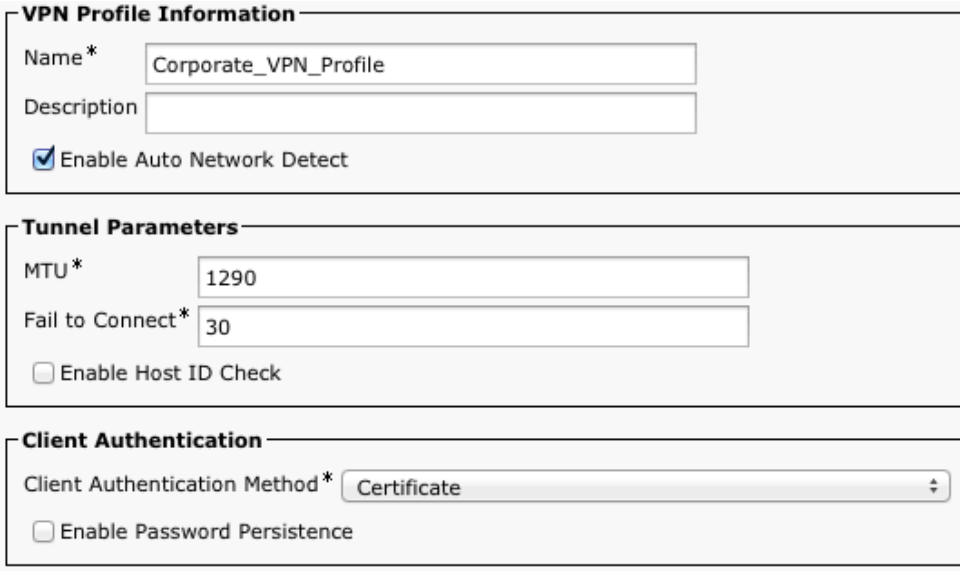
VPN 設定情報は、Cisco Unified Communications Manager によって管理者からプッシュ ダウンできます。

VPN ゲートウェイは名前と VPN ゲートウェイ URL が定義される場所に作成する必要があります。

VPN ゲートウェイが使用される情報を含む VPN グループも作成する必要があります。

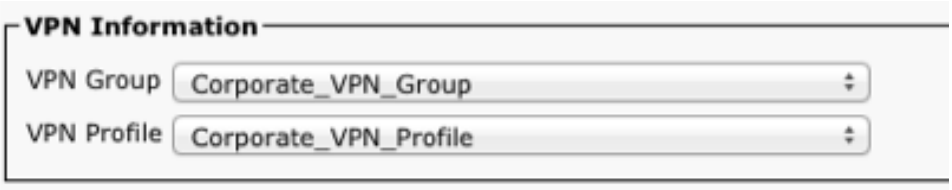


使用されるクライアント認証やその他のパラメータを指定する、VPN プロファイルを設定する必要があります。



VPN グループおよびプロファイルが設定されている場合は、共通の電話プロファイルに適用し、特定のデバイスに適用できます。

Cisco DX シリーズが現在ネットワークに接続され、Cisco Unified Communications Manager に接続できない場合は、VPN プロファイルが設定されていると VPN セッションが自動的に試行されます。

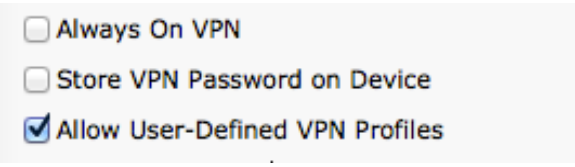


[常時 VPN（Always On VPN）]、**[デバイス上に VPN パスワードを保存（Store VPN Password On Device）]**、および [ユーザ定義 VPN プロファイルの許可（Allow User-Defined VPN Profiles）] は、エンタープライズ電話、共通の電話プロファイル、または個別の電話設定レベルで設定できます。

[常時 VPN（Always On VPN）] は、Cisco DX シリーズをセキュアなネットワーク上に維持し、Cisco Unified Communications Manager に常時接続します。

[デバイス上に VPN パスワードを保存（Store VPN Password On Device）] は、VPN パスワードをデバイス上に保存できるようにします。

[ユーザ定義 VPN プロファイルの許可（Allow User-Defined VPN Profiles）] は独自の VPN プロファイルを作成することができます。

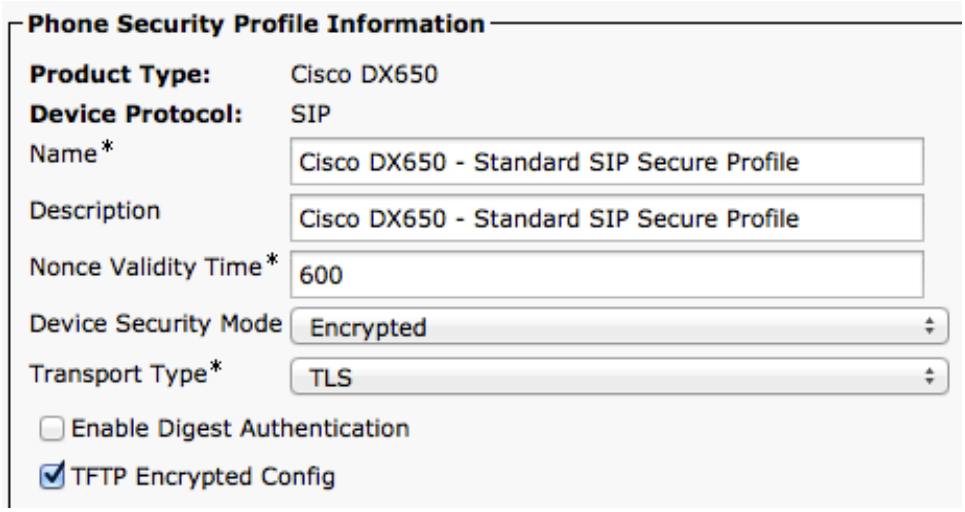


ワイヤレス LAN プロファイルの設定

Cisco Unified Communications Manager 10.0 リリースを含む Cisco DX シリーズの 10.1(1) リリース以降では、Cisco Unified Communications Manager 経由でワイヤレス LAN プロファイルを使用して Cisco DX シリーズをプロビジョニングできます。

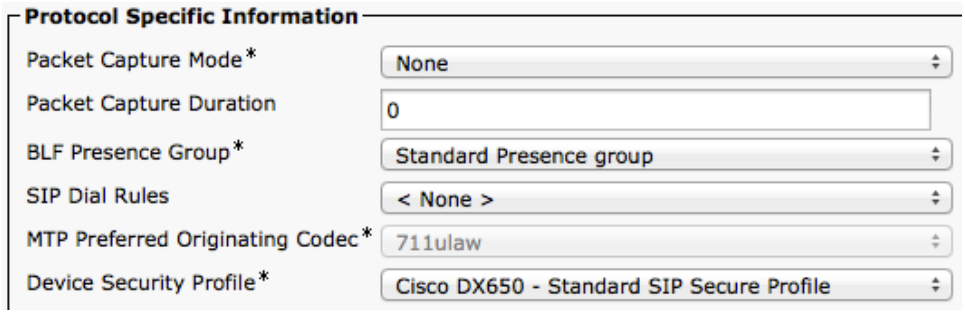
初めてプロビジョニングする場合は、Cisco DX シリーズをイーサネット経由でネットワークに接続することをお勧めします。

ワイヤレス LAN プロファイルを作成して、それを Cisco DX シリーズに関連付ける前に、ワイヤレス LAN プロファイル データが TFTP 経由のクリア テキストで Cisco DX シリーズに渡されないように、TFTP 暗号化が有効になっているセキュリティ プロファイルを使用するように Cisco DX シリーズを設定する必要があります。



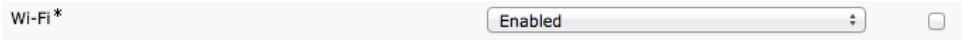
セキュリティ プロファイルを作成したら、それを Cisco DX シリーズに適用して、その Cisco DX シリーズのコンフィギュレーション ファイルに対して TFTP 暗号化を有効にする必要があります。

[デバイス セキュリティ プロファイル（Device Security Profile）] ドロップダウン メニューから設定済みのセキュリティ プロファイルを選択します。

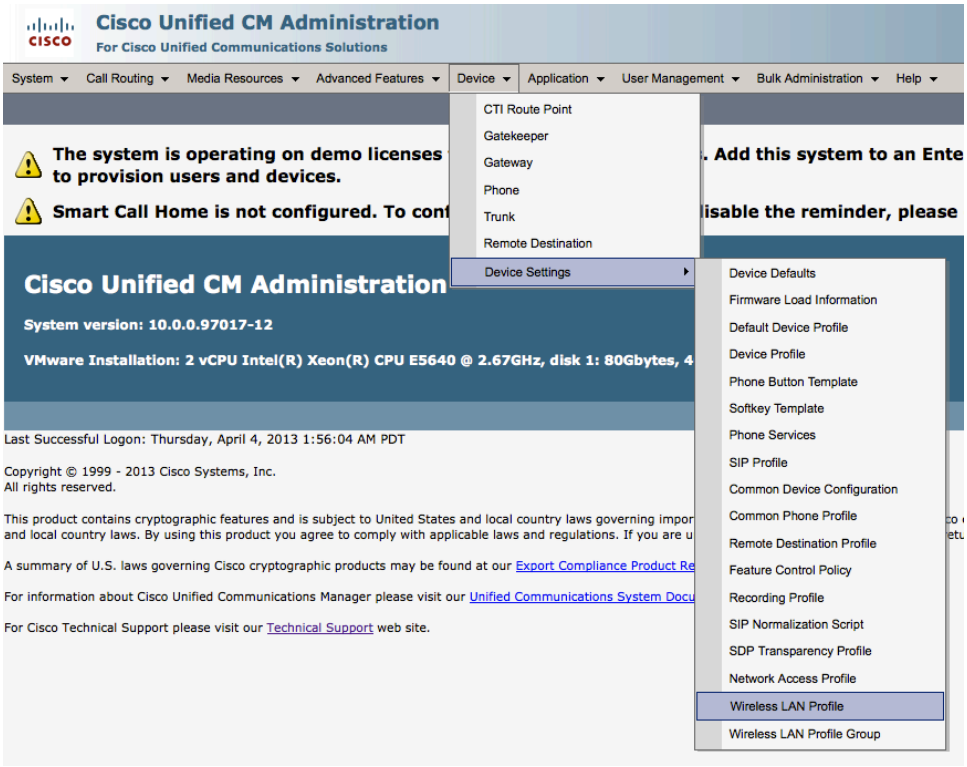


Cisco DX シリーズではデフォルトで **Wi-Fi** が有効になっていますが、Wi-Fi 機能は、エンタープライズ電話の設定、共通の電話プロファイル、または個別の電話レベルで管理できます。

ワイヤレス LAN プロファイル機能を使用している場合は、**Wi-Fi** を対応するデバイスに対して有効にする必要があります。そうしなかった場合は、デバイスをワイヤレス LAN に接続できなくなります。



ワイヤレス LAN プロファイルを作成するには、Cisco Unified Communications Manager の管理インタフェースで **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [ワイヤレス LAN プロファイル（Wireless LAN Profile）]** に移動します。

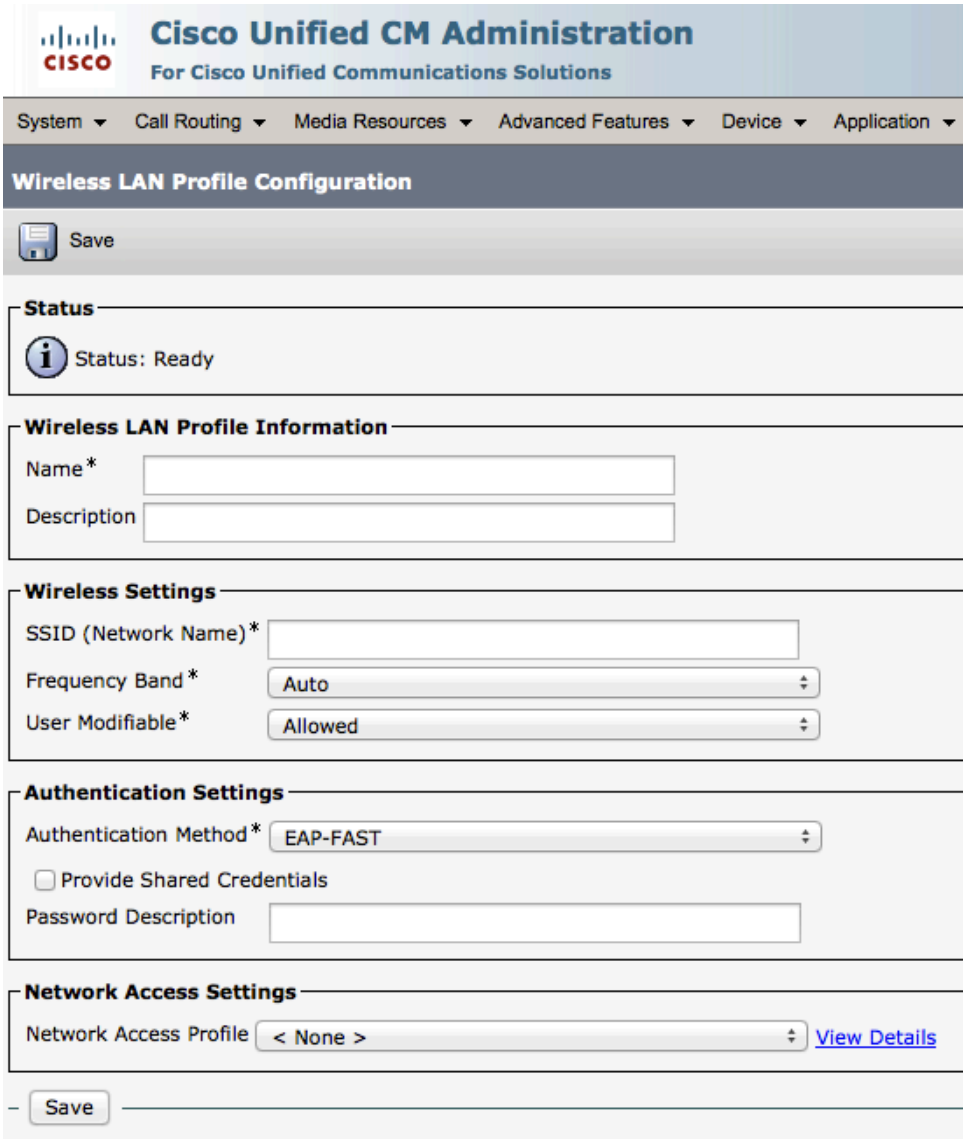


ワイヤレス LAN プロファイル ページで、**[新規追加（Add New）]** を選択します。

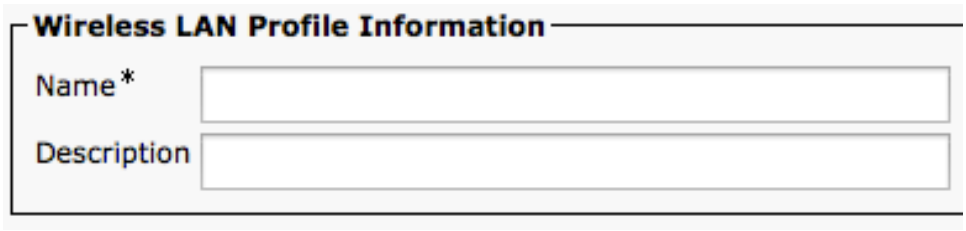
その後で、名前、説明、ワイヤレス設定（SSID、周波数帯域、ユーザが変更可能）、認証設定、およびネットワーク アクセス設定を指定してワイヤレス LAN プロファイルを作成できます。

ワイヤレス LAN プロファイルのデフォルト値は次のとおりです。

- **[周波数帯域（Frequency Band）]** = [自動（Auto）]
- **[ユーザが変更可能（User Modifiable）]** = [許可（Allowed）]
- **[認証方式（Authentication Method）]** = [EAP-FAST（EAP-FAST）]



最大 50 文字で構成されたワイヤレス LAN プロファイルの [**名前（Name）**] を入力します。
オプションで、最大 63 文字で構成された [**説明（Description）**] を設定できます。

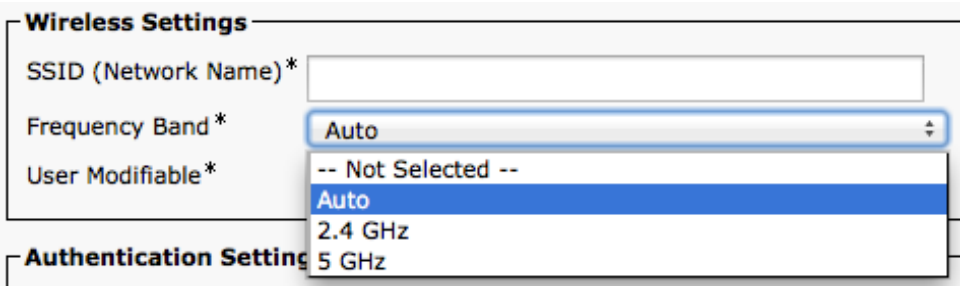


最大 32 文字の ASCII 文字で構成された [**SSID**] を入力します。

必要な [**周波数帯域（Frequency Band）**] オプションを選択します。

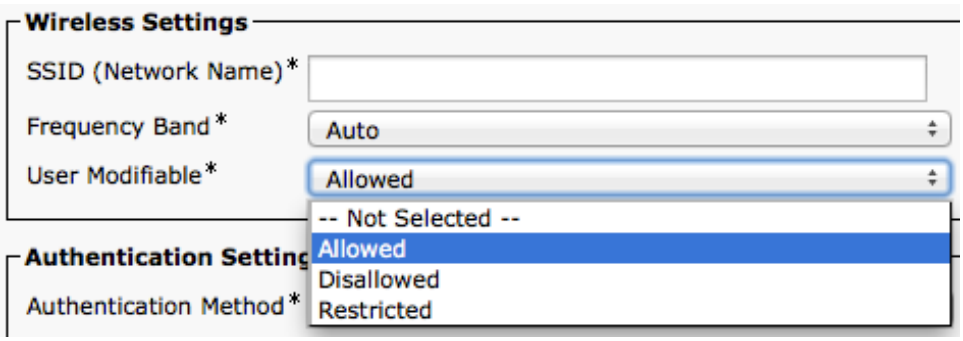
[**周波数帯域（Frequency Band）**] はデフォルトで [自動（Auto）] に設定されます。そのため、Cisco DX シリーズは 2.4 GHz と 5 GHz の両方の周波数を利用できます。

[自動（Auto）] が選択された場合は、5 GHz 周波数帯域が優先されます。

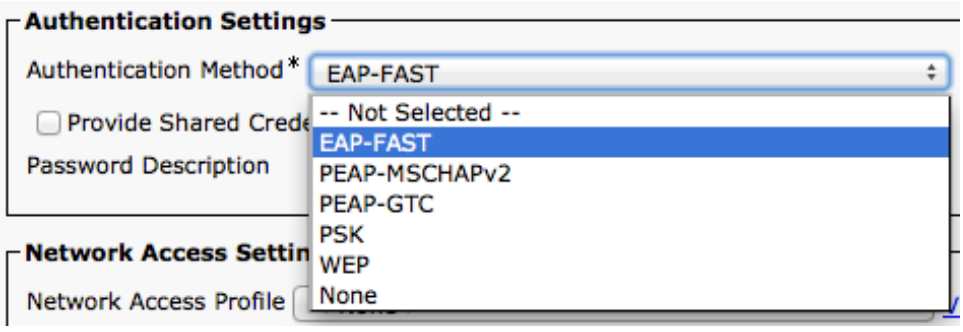


必要な [**ユーザが変更可能（User Modifiable）**] オプションを選択します。

- [**許可（Allocated）**]：ユーザはエンドポイント上の任意のワイヤレス LAN 設定（有効/無効、SSID、周波数帯域、認証方式、ユーザ名とパスワード、PSK パスフレーズ、WEP キーなど）をローカルで変更できます。
- [**拒否（Disallowed）**]：ユーザはワイヤレス LAN 設定を変更できません。
- [**制限（Restricted）**]：ユーザーは特定のワイヤレス LAN 設定（ユーザ名とパスワードなど）のみを変更できます。

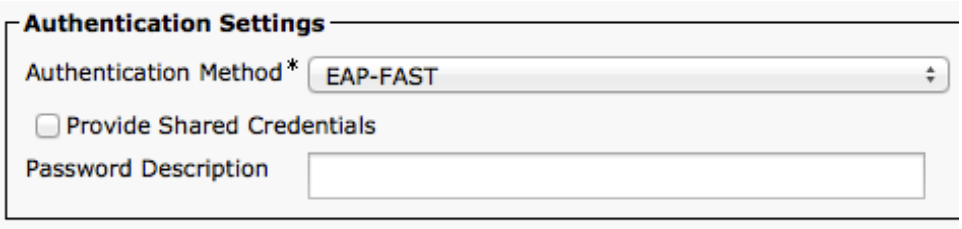


必要な [**認証方式（Authentication Method）**] オプションを選択します。



[**EAP-FAST（EAP-FAST）**]、[**PEAP-MSCHAPv2（PEAP-MSCHAPv2）**]、または [**PEAP-GTC（PEAP-GTC）**] が選択された場合は、共有クレデンシャル（ユーザー名とパスワード）を入力するオプションが有効になります。

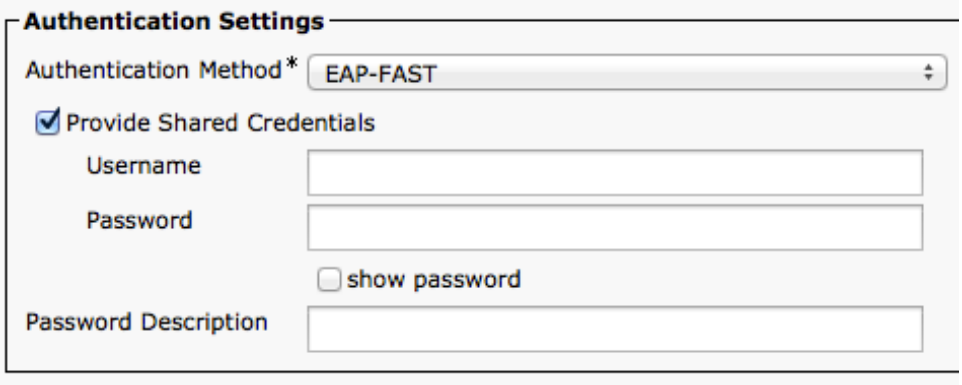
[**共有クレデンシャルの指定（Provide Shared Credentials）**] がオンになっていない場合は、管理者またはユーザが Cisco DX シリーズ上でユーザ名とパスワードをローカルで設定する必要があります。



[**共有クレデンシャルの指定（Provide Shared Credentials）**] がオンになっている場合は、このワイヤレス LAN プロファイルを使用するすべての Cisco DX シリーズで指定された [**ユーザ名（Username）**] と [**パスワード（Password）**] が使用されます。

ユーザ名とパスワードは最大 64 文字まで入力できます。

オプションで、[**パスワードの説明（Password Description）**] を入力できます。

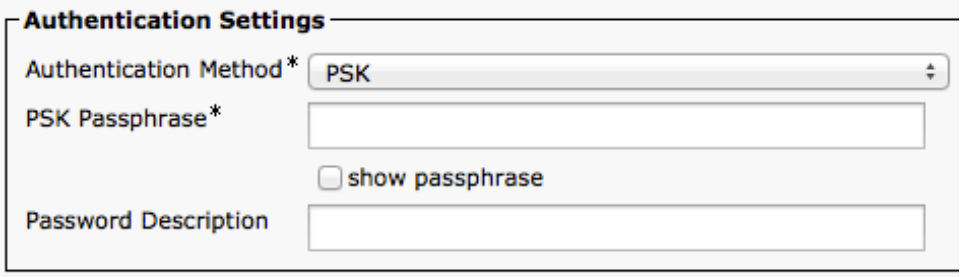


事前共有キー認証を使用するために [**PSK（PSK）**] が選択されている場合は、[**PSK パスフレーズ（PSK Passphrase）**] を入力する必要があります。

[**PSK パスフレーズ（PSK Passphrase）**] は、次の形式のいずれかにする必要があります。

- 8 ～ 63 文字の ASCII 文字列
- 64 文字の HEX 文字列

オプションで、[**パスワードの説明（Password Description）**] を入力できます。



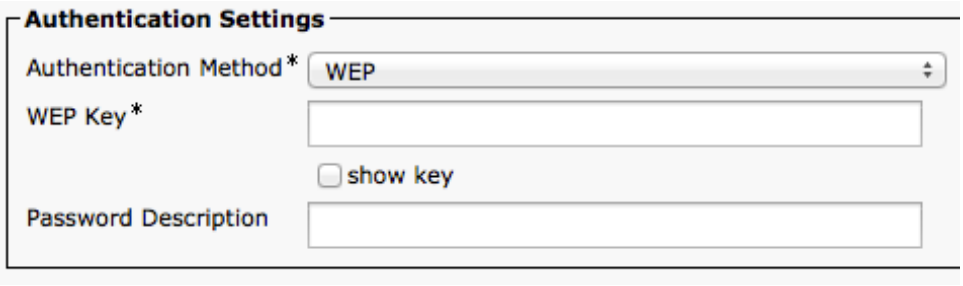
静的 WEP（有線と同等のプライバシー）認証を使用するために [**WEP（WEP）**] が選択された場合は、[**WEP キー（WEP Key）**] を入力する必要があります。

WEP キー 1 しかサポートされないため、入力したキーがアクセス ポイント側の送信キーと一致することを確認する必要があります。

[**WEP キー（WEP Key）**] は、次の形式のいずれかにする必要があります。

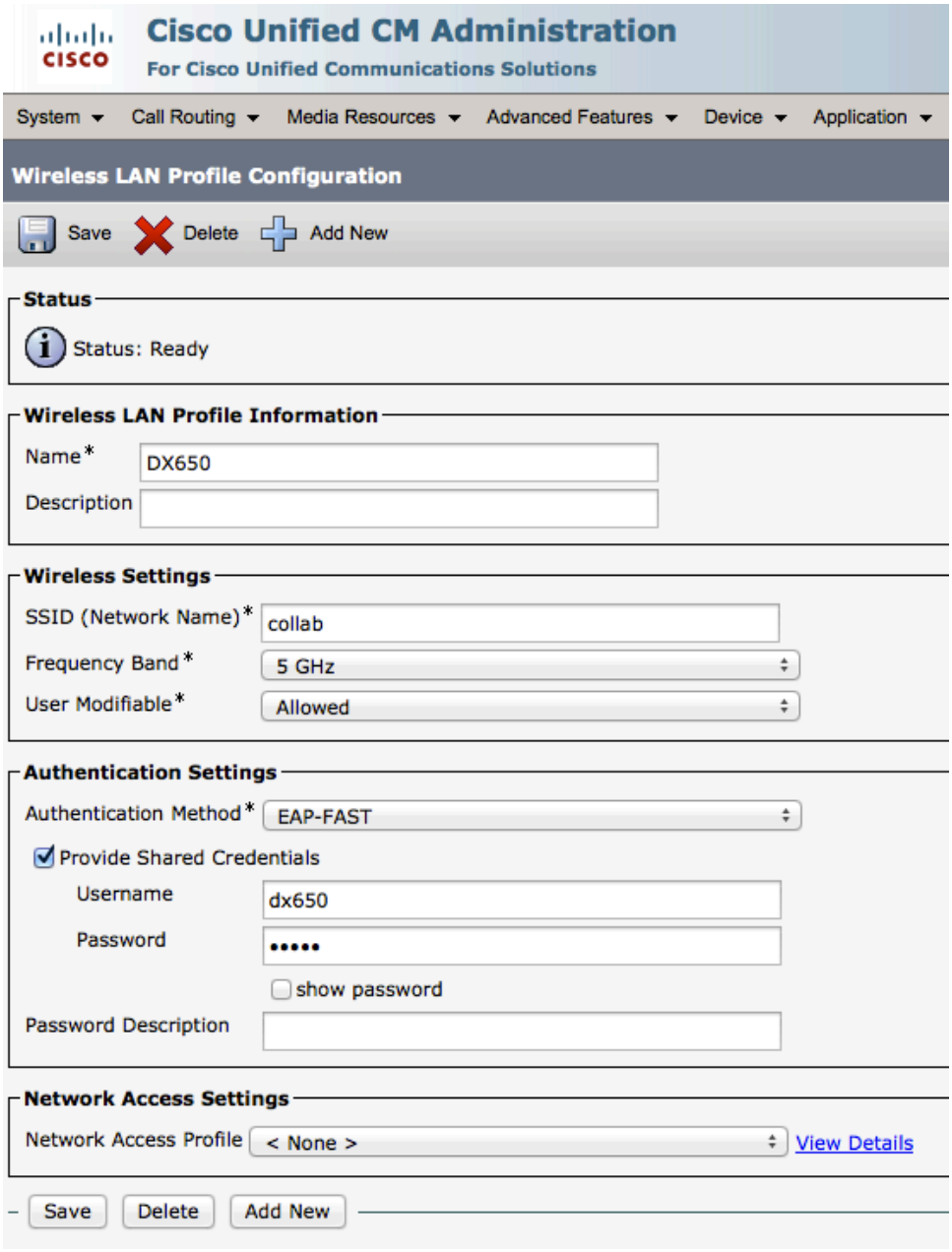
- **[40/64 ビット キー（40/64 Bit Key）]** = 5 桁の ASCII 文字列または 10 桁の HEX 文字列
- [**104/128 ビット キー（104/128 Bit Key）**] = 13 桁の ASCII 文字列または 26 桁の HEX 文字列

オプションで、[**パスワードの説明（Password Description）**] を入力できます。

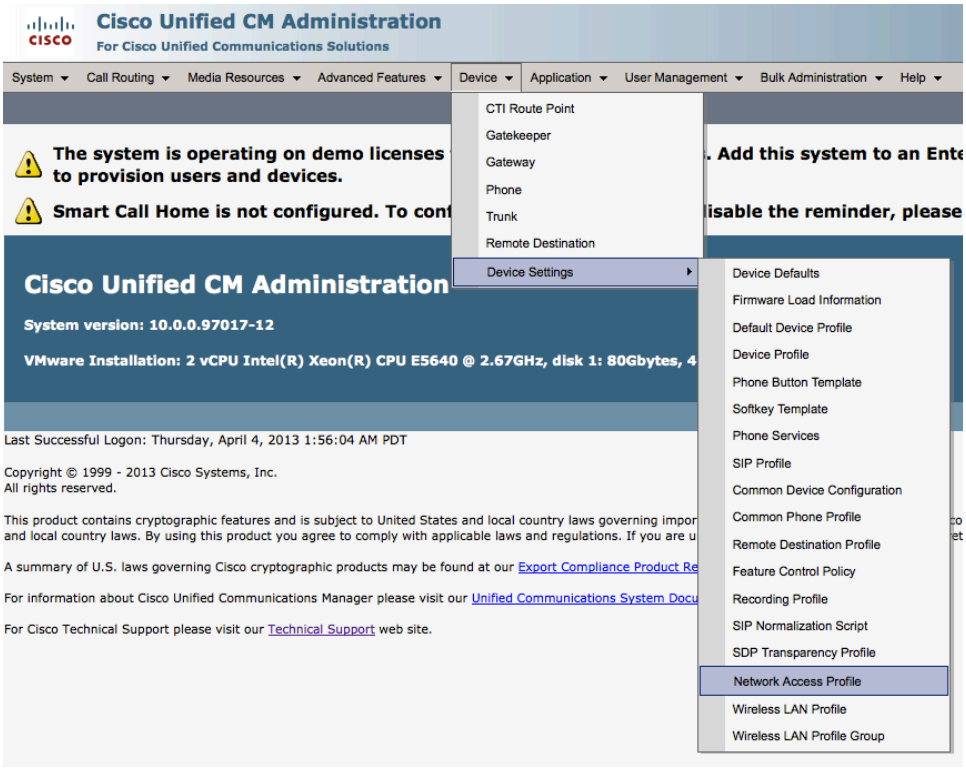


[**なし（None）**] が選択されている場合は、どの認証も必要なく、どの暗号化も使用されません。

ワイヤレス LAN プロファイルの設定が完了したら、[**保存（Save）**] を選択します。



ネットワーク アクセス プロファイルを作成するには、Cisco Unified Communications Manager の管理インタフェースで **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [ネットワーク アクセス プロファイル（Network Access Profile）]** に移動します。

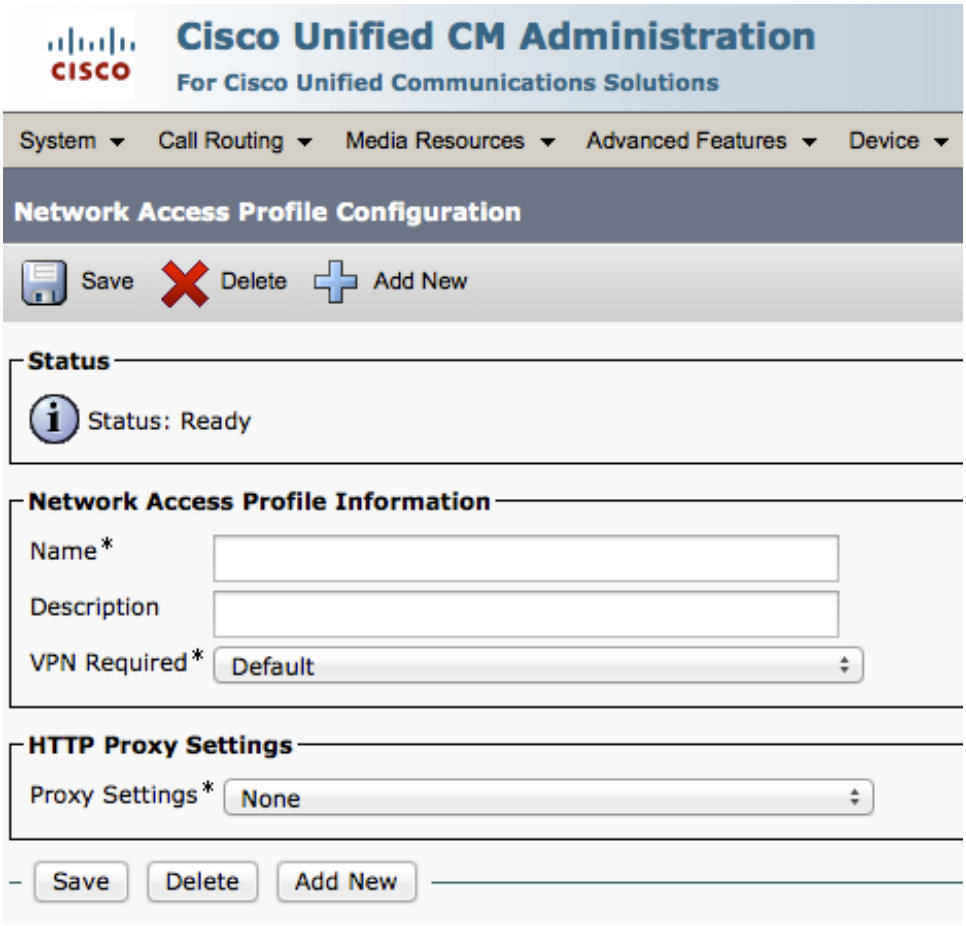


ネットワーク アクセス プロファイル ページで、[**新規追加（Add New）**] を選択します。

これにより、ネットワーク アクセス プロファイルが作成されるので、[名前（Name）]、[説明（Description）]、[VPN 必須（VPN Required）]、および [プロキシ設定（Proxy Settings）] を指定します。

ネットワーク アクセス プロファイルのデフォルト値は次のとおりです。

- [**VPN 必須（VPN Required）**] = [デフォルト（Default）]
- [**プロキシ設定（Proxy Settings）**] = [なし（None）]



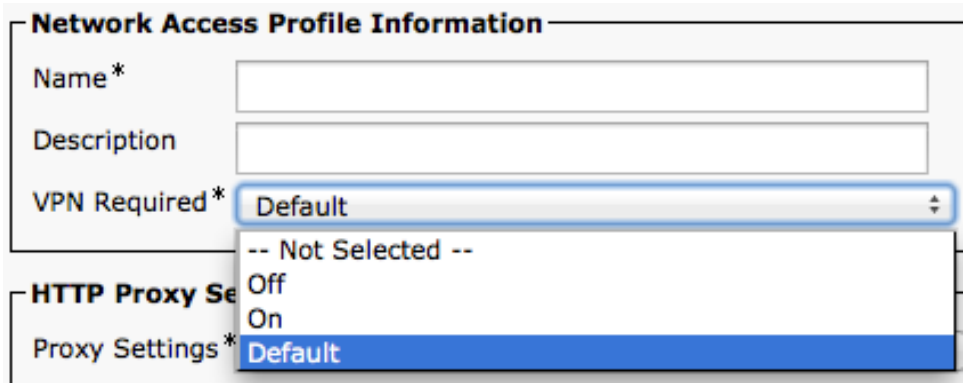
最大 50 文字で構成されたネットワーク アクセス プロファイルの [**名前（Name）**] を入力します。

オプションで、最大 63 文字で構成された [**説明（Description）**] を設定できます。

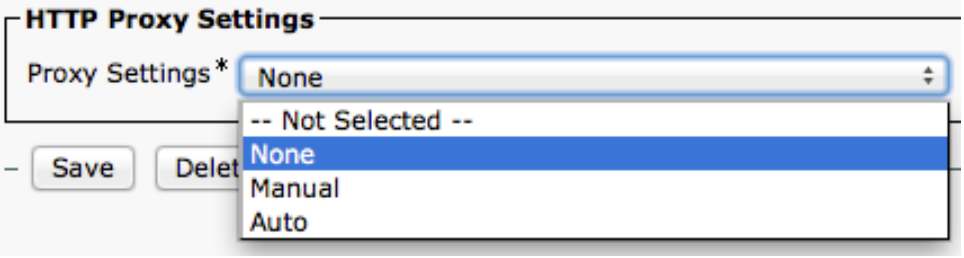
必要な [**VPN 必須（VPN Required）**] オプションを選択します。

[オン（On）] が選択された場合は、このネットワーク アクセス プロファイルが使用されるかぎり、常に、VPN が使用されます。

[デフォルト（Default）] が選択された場合は、システム デフォルトが使用されます。



必要な [**プロキシ設定（Proxy Settings）**] オプションを選択します。



[手動（Manual）] が選択された場合は、[**プロキシ ホスト名（Proxy Hostname）**] と [**プロキシ ポート（Proxy Port）**] を設定する必要があります。

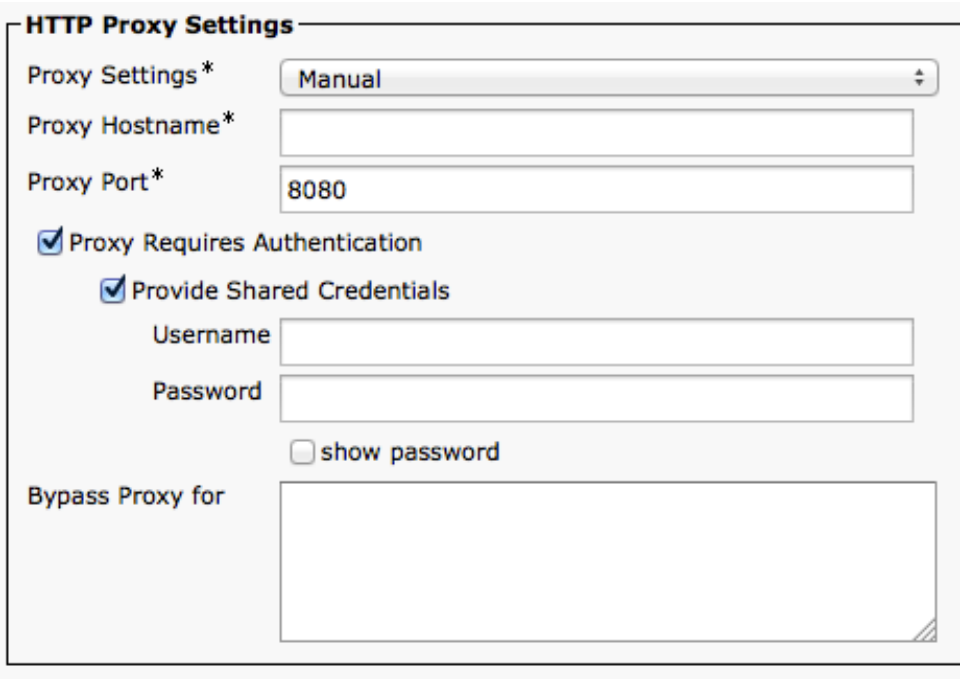
プロキシ ホスト名は最大 255 文字にすることができます。

プロキシ ポートはデフォルトで 8080 に設定されますが、1 ～ 65535 の範囲で設定できます。

オプションで、[**プロキシは認証が必須（Proxy Requires Authentication）**] を選択してから、[**共有クレデンシャルの指定（Provide Shared Credentials）**] を選択することにより、プロキシ認証を有効にすることができます。

ユーザ名とパスワードは最大 64 文字まで入力できます。

必要に応じて、[**次のプロキシをバイパス（Bypass Proxy for）**] ボックスにドメイン名を入力します。



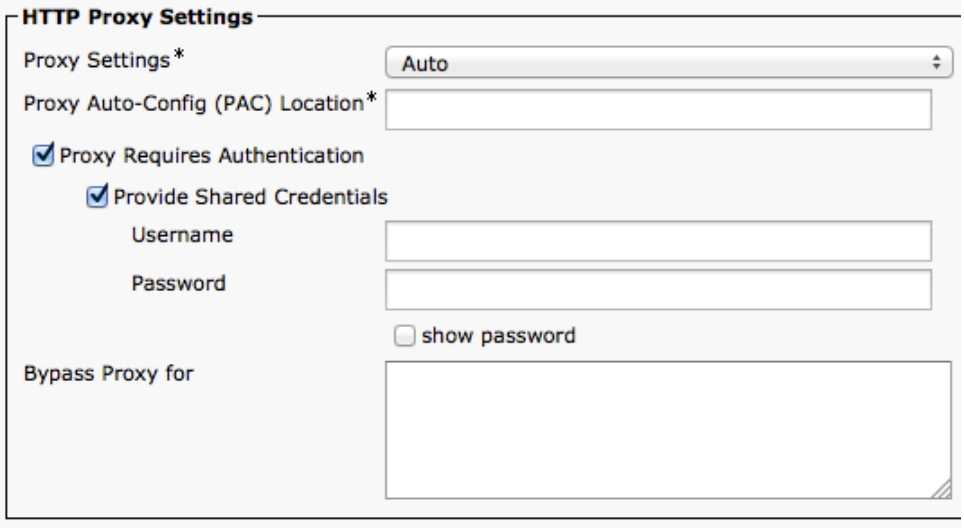
[自動（Auto）] が選択された場合は、[**プロキシ自動設定（PAC）のロケーション（Proxy Auto-Config (PAC) Location）**] を設定する必要があります。

プロキシ自動設定（PAC）のロケーションは、最大 255 文字にすることができます。

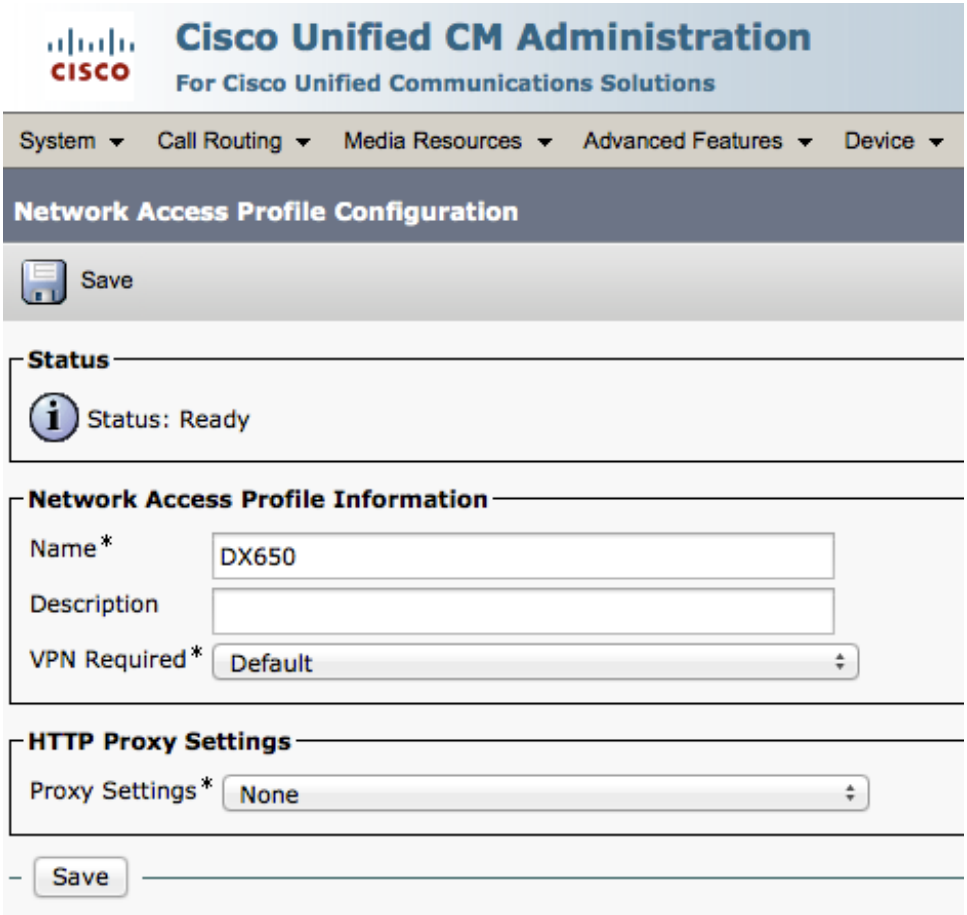
オプションで、[**プロキシは認証が必須（Proxy Requires Authentication）**] を選択してから、[**共有クレデンシャルの指定（Provide Shared Credentials）**] を選択することにより、プロキシ認証を有効にすることができます。

ユーザ名とパスワードは最大 64 文字まで入力できます。

必要に応じて、[**次のプロキシをバイパス（Bypass Proxy for）**] ボックスにドメイン名を入力します。

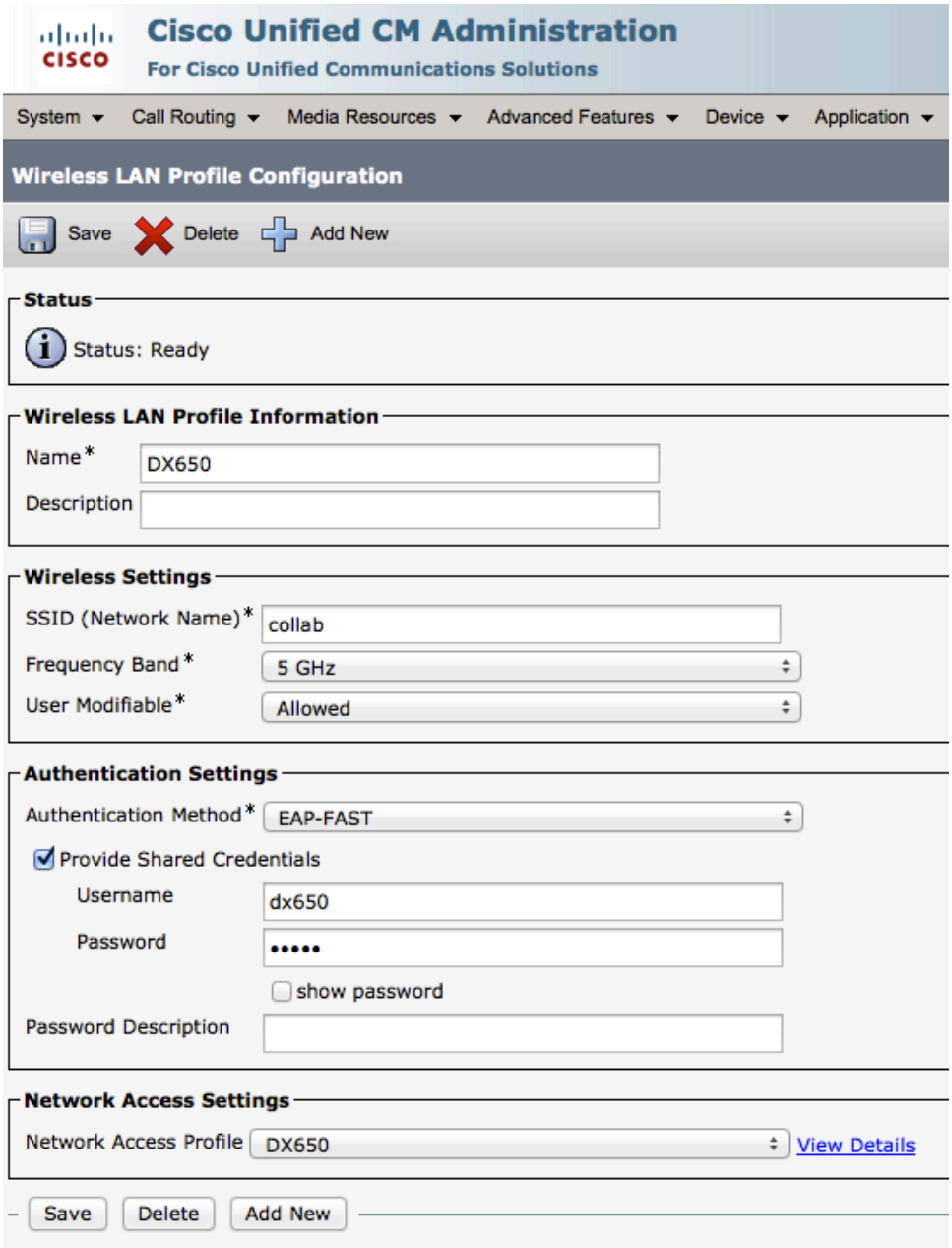


ネットワーク アクセス プロファイルの設定が完了したら、[**保存（Save）**] を選択します。

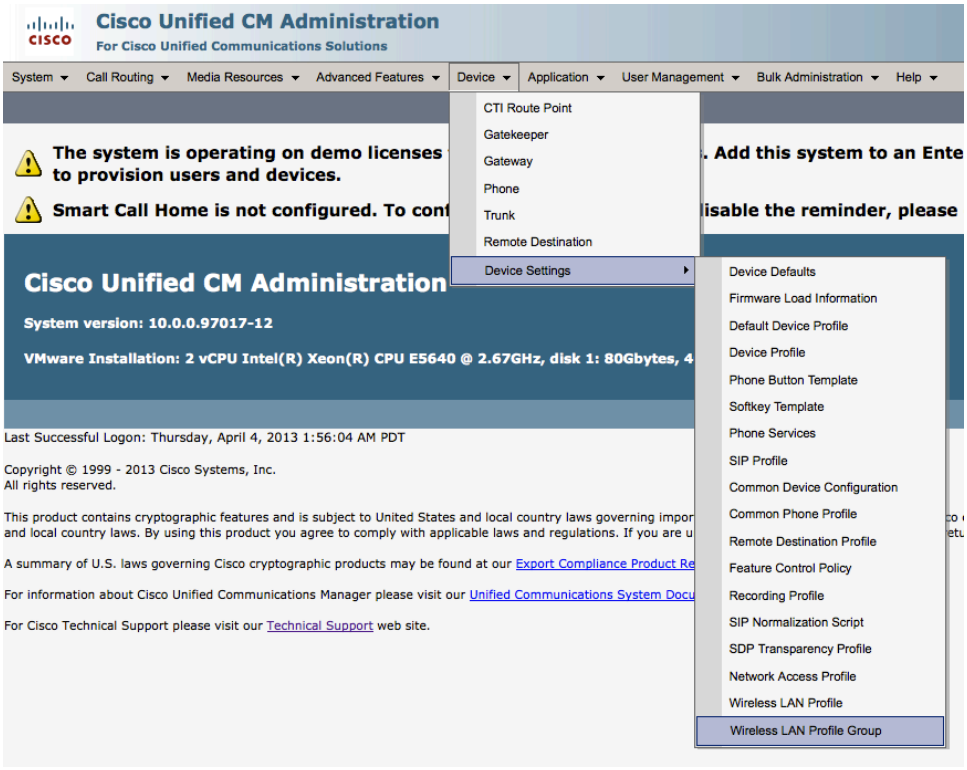


ネットワーク アクセス プロファイルを作成したら、それをワイヤレス LAN プロファイルに適用できます。

ネットワーク アクセス プロファイルをワイヤレス LAN プロファイルに適用したら、[**保存（Save）**] を選択します。



ワイヤレス LAN プロファイル グループを作成するには、Cisco Unified Communications Manager の管理インタフェースで **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [ワイヤレス LAN プロファイル グループ（Wireless LAN Profile Group）]** に移動します。

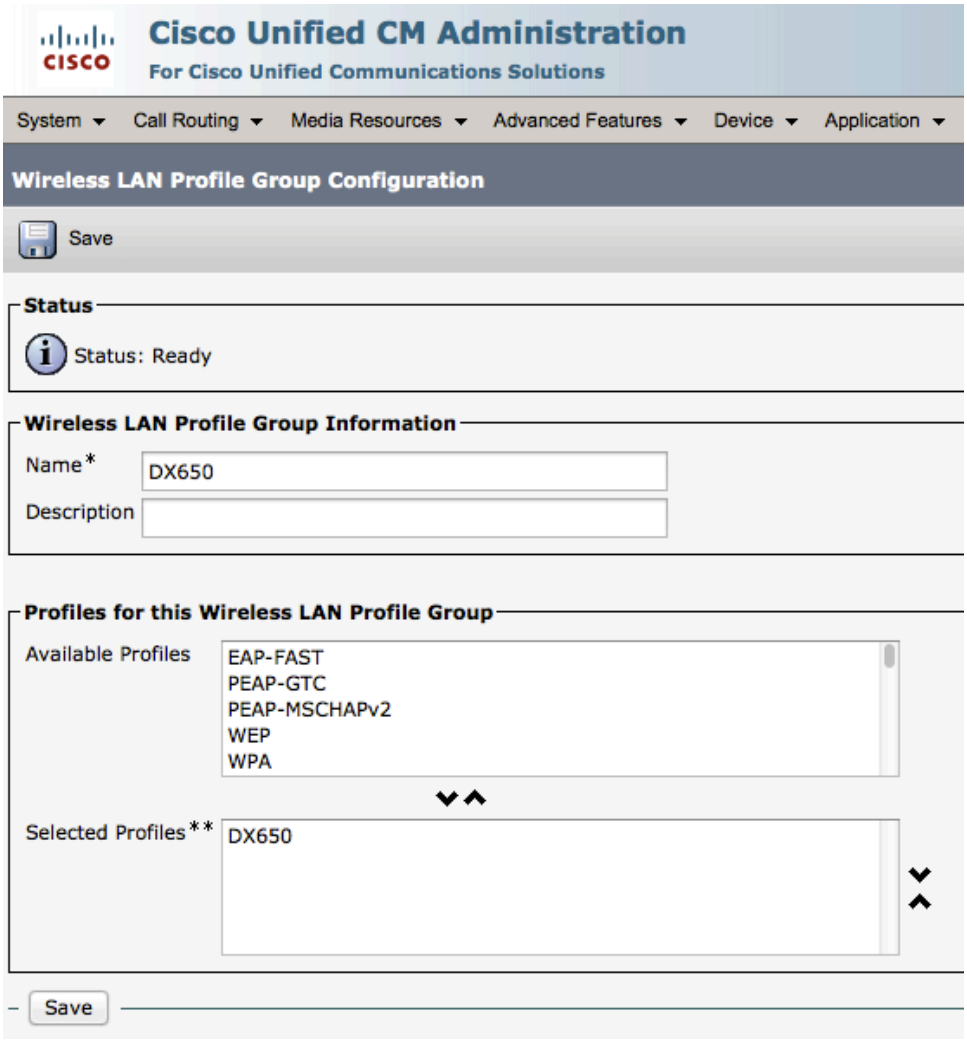


ワイヤレス LAN プロファイル グループ ページで、[**新規追加（Add New）**] を選択します。

その後で、名前、説明、およびワイヤレス LAN プロファイルを指定してワイヤレス LAN プロファイル グループを作成できます。

最大 **4** つのワイヤレス LAN プロファイルをワイヤレス LAN プロファイル グループに追加できます。

ワイヤレス LAN プロファイル グループの設定が完了したら、[**保存（Save）**] を選択します。



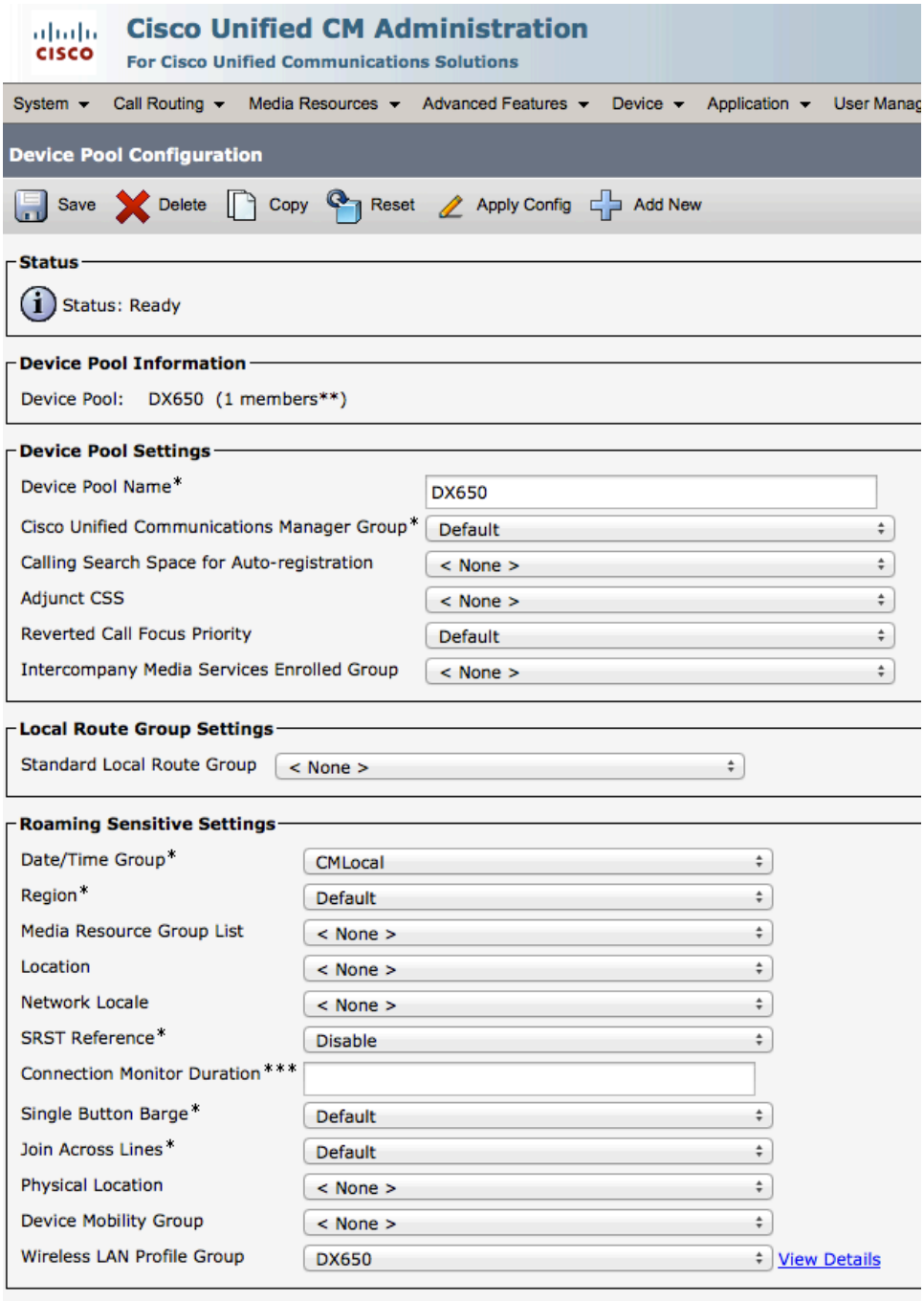
ワイヤレス LAN プロファイル グループを作成したら、それをデバイス プールまたは個別の Cisco DX シリーズに適用できます。

ワイヤレス LAN プロファイル グループをデバイス プールに適用するには、Cisco Unified Communications Manager の管理インタフェースで **[システム（System）] > [デバイス プール（Device Pool）]** に移動します。

必要に応じてデバイス プールを作成し、必要な Cisco DX シリーズをそのデバイス プールに配置します。

デバイス プールを作成したら、ワイヤレス LAN プロファイル グループを設定して、**[保存（Save）]** を選択します。

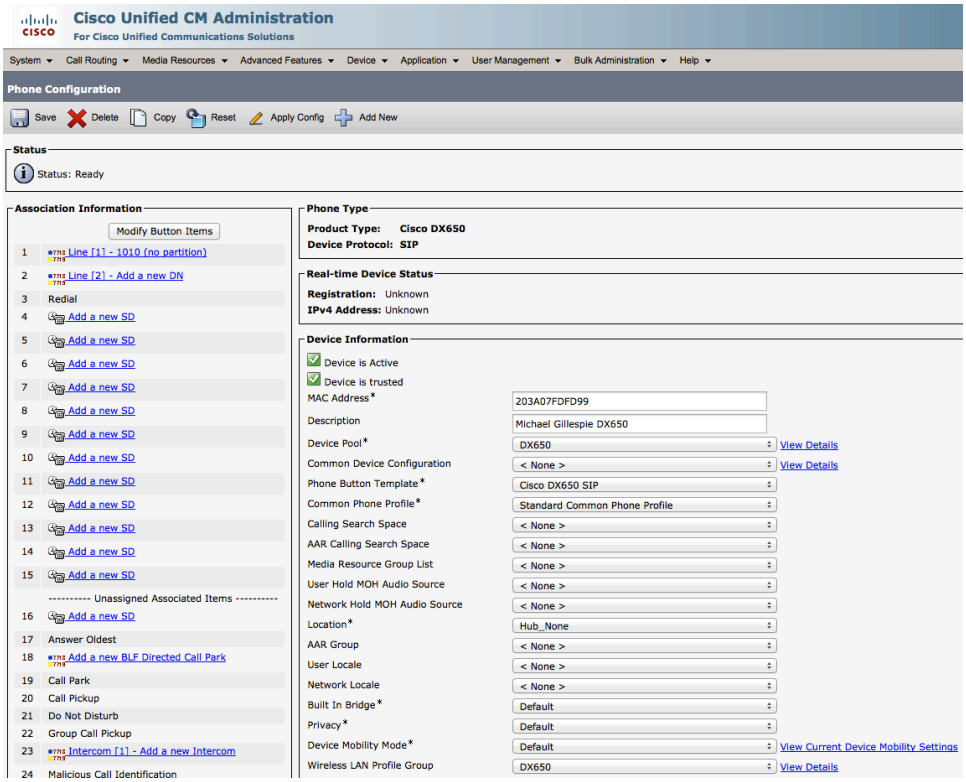
ワイヤレス LAN プロファイル グループをデバイス プールに適用したら、**[設定の適用（Apply Config）]** を選択して、Cisco DX シリーズがワイヤレス LAN プロファイル グループの設定をダウンロードできるようにします。



ワイヤレス LAN プロファイル グループを個別の DX シリーズに適用するには、Cisco Unified Communications Manager の管理インタフェースで **[デバイス(Device)] > [電話機(Phone)]** に移動します。

必要な Cisco DX シリーズに移動し、ワイヤレス LAN プロファイル グループを設定してから、**[保存(Save)]** を選択します。

ワイヤレス LAN プロファイル グループを個別の Cisco DX シリーズに適用したら、**[設定の適用(Apply Config)]** を選択して、Cisco DX シリーズがワイヤレス LAN プロファイル グループの設定をダウンロードできるようにします。



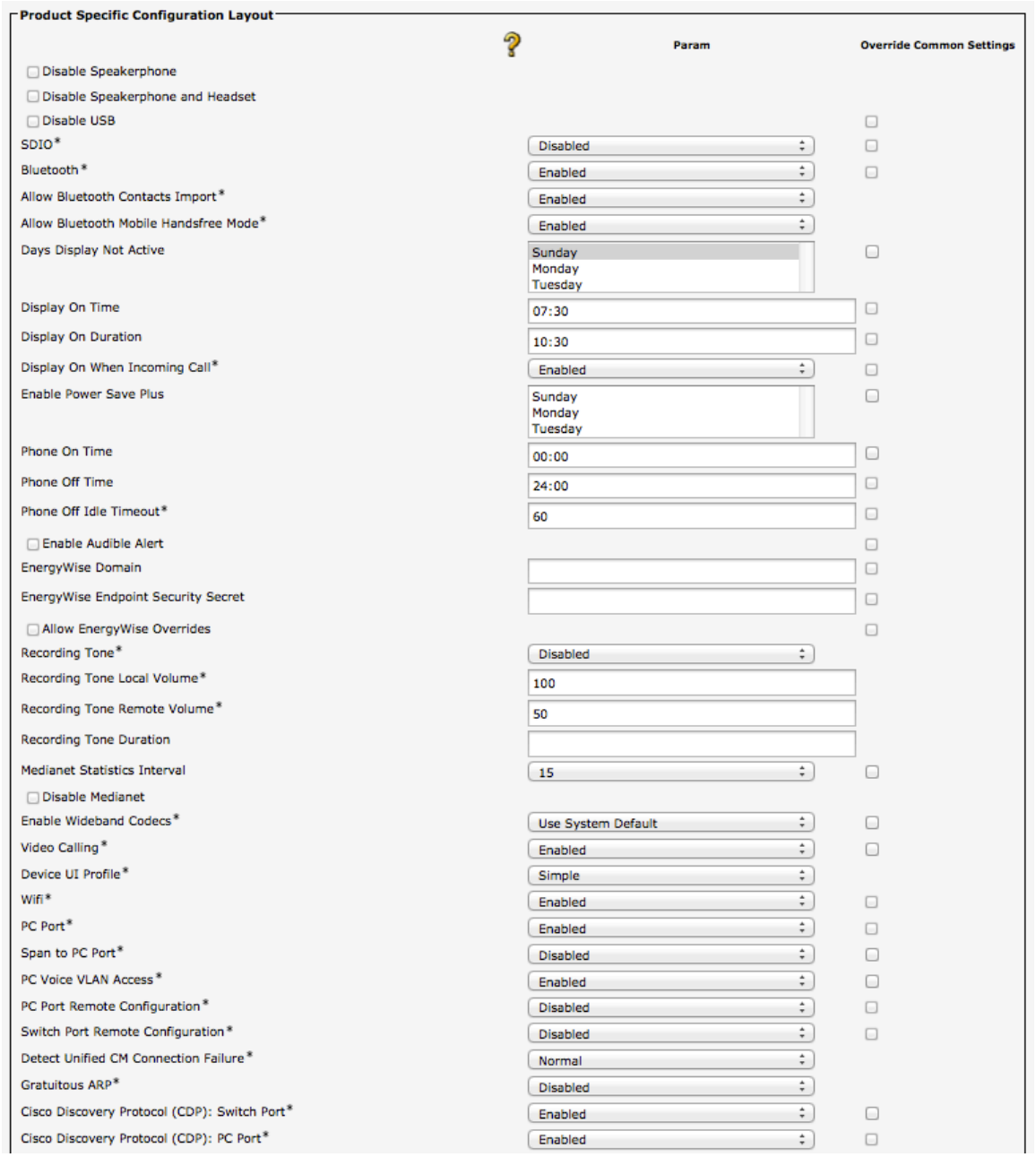
製品固有の設定オプション

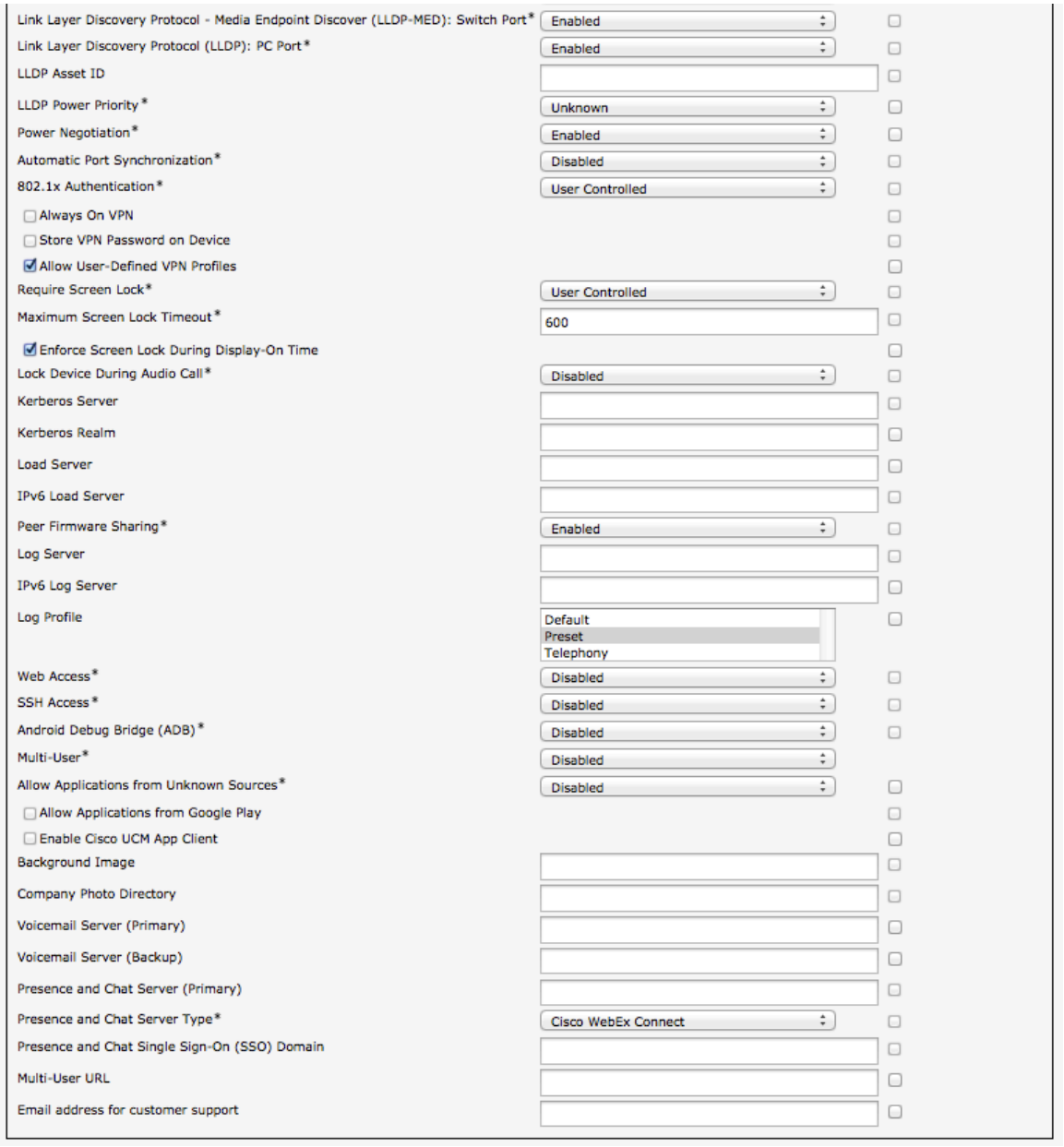
Cisco Unified Communications Manager Administration では、Cisco DX シリーズに対して次の設定オプションを使用できます。

これらのオプションの説明については、設定ページの上部の [?] をクリックしてください。

Cisco Unified Communications Manager では、一括管理ツールを使用して製品固有の設定オプションを一括で設定できます。

製品固有の設定オプションによっては、企業の電話機、共通電話プロファイル、または個々の電話機設定レベルで設定できるものもあります。


Product Specific Configuration Layout
Param
Override Common Settings
Disable Speakerphone
Disable Speakerphone and Headset
Disable USB
SDIO*
Disabled
Bluetooth*
Enabled
Allow Bluetooth Contacts Import*
Enabled
Allow Bluetooth Mobile Handsfree Mode*
Enabled
Days Display Not Active
Sunday
Monday
Tuesday
Display On Time
07:30
Display On Duration
10:30
Display On When Incoming Call*
Enabled
Enable Power Save Plus
Sunday
Monday
Tuesday
Phone On Time
00:00
Phone Off Time
24:00
Phone Off Idle Timeout*
60
Enable Audible Alert
EnergyWise Domain
EnergyWise Endpoint Security Secret
Allow EnergyWise Overrides
Recording Tone*
Disabled
Recording Tone Local Volume*
100
Recording Tone Remote Volume*
50
Recording Tone Duration
Medianet Statistics Interval
15
Disable Medianet
Enable Wideband Codecs*
Use System Default
Video Calling*
Enabled
Device UI Profile*
Simple
Wifi*
Enabled
PC Port*
Enabled
Span to PC Port*
Disabled
PC Voice VLAN Access*
Enabled
PC Port Remote Configuration*
Disabled
Switch Port Remote Configuration*
Disabled
Detect Unified CM Connection Failure*
Normal
Gratuitous ARP*
Disabled
Cisco Discovery Protocol (CDP): Switch Port*
Enabled
Cisco Discovery Protocol (CDP): PC Port*
Enabled



フィールド名	説明
スピーカーフォンを無効にする (Disable Speakerphone)	スピーカー フォン機能のみ無効になります。スピーカー フォン機能を無効にしても、ヘッドセットには影響しません。ハンドセットまたはヘッドセットで回線とスピード ダイヤルを使用できます。
スピーカーフォンとヘッドセットを無効にする(Disable Speakerphone and Headset)	すべてのスピーカーフォン機能およびヘッドセットのマイクを無効にします。
USB の無効化(Disable USB)	デバイスの USB ポートを無効にします。
SDIO	デバイス上の SDIO デバイスが有効になっているか無効になっているかを示します。

Bluetooth	電話機の Bluetooth デバイスが有効であるか、無効であるかを示します。
Bluetooth アドレス帳のインポートを許可（Allow Bluetooth Contacts Import）	このパラメータは、ユーザが Bluetooth デバイスからアドレス帳と通話履歴をインポートして同期できるようにします。
Bluetooth モバイル ハンズフリー モードを許可（Allow Bluetooth Mobile Handsfree Mode）	このパラメータは、ユーザが卓上電話機で携帯電話回線を利用できるようにします。
ディスプレイ非点灯日（Days Display Not Active）	このフィールドで、バックライトをデフォルトでオフのままにする日を指定します。通常これは、米国の企業顧客向けの場合土曜日と日曜日です。土曜日と日曜日がデフォルトです。リストには、曜日すべてが含まれます。土曜日と日曜日のバックライトをオフにするには、ユーザはコントロールを押したまま、[土曜日（Saturday）] と [日曜日（Sunday）] を選択します。
ディスプレイ点灯時刻（Display On Time）	このフィールドは、オフ スケジュールにリストされている日にディスプレイが自動的にオンになる時刻を示します。この値は 24 時間形式で指定する必要があります。ここで 0:00 は 1 日の始まりを表し、23:59 が 1 日の終わりを表します。このフィールドを空白にした場合はデフォルトの時刻にディスプレイがオンになります（たとえば、「7:30」）。ディスプレイを午前 7:00 にオンにするように設定するには、「07:00」と入力します（かっこは入力しません）。ディスプレイを午後 2:00 にオンにする場合は、「14:00」と入力します（かっこは入力しません）。
ディスプレイ点灯継続時間（Display On Duration）	このフィールドは、プログラムされた時刻にディスプレイがオンになった後、ディスプレイのアクティブな状態を保つ時間の長さを示します。このフィールドを空白のままにしておくと、電話機は「10:30」の既定のデフォルト値を使用します。最大値は 24 時間です。この値は、時間と分が自由形式です。「1:30」の場合、1 時間 30 分ディスプレイがオンになります。
着信コール時に点灯（Display On When Incoming Call）	デバイスがスクリーン セーブ モードの場合にこの機能を有効にすると、コールを着信した時点でディスプレイがオンになります。
音声アラートを有効にする（Enable Audio Alert）	このチェックボックスは、有効な場合、[電話機をオフにする時刻（Phone Off Time）] フィールドで指定された時刻の 10 分前に音声アラートを再生するように電話機に指示します。電話機の選択キーは、これからの電話機の状態の変化（Power Save Plus 機能によって電源がオフになる）をユーザに視覚的に警告するため素早く点滅します。また、音声でユーザに警告するには、このチェックボックスをオンにします。デフォルトではディセーブルになっています。このチェックボックスが表示されるのは、[Power Save Plus の有効化（Enable Power Save Plus）] リストボックスで 1 日以上が選択されている場合だけです。
EnergyWise ドメイン（EnergyWise Domain）	このフィールドでは、電話機が参加している EnergyWise ドメインを定義します。EnergyWise ドメインは、Power Save Plus 機能で必要となります。[Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで日数を選択した場合は、EnergyWise ドメインを用意する必要があります。デフォルトは空白です。
EnergyWise Endpoint Security Secret	このフィールドは、EnergyWise ドメイン内で通信するために使用するパスワード（共有秘密）を定義します。EnergyWise ドメインと秘密は、Power Save Plus 機能で必要となります。[Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで日数を選択した場合は、EnergyWise ドメインと秘密を用意する必要があります。デフォルトは空白です。

EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）	このチェックボックスにより、電話機に電源レベルの更新を送信するための EnergyWise ドメイン コントローラのポリシーを許可するかどうかを決定します。次の条件が適用されます。最初に、1 日以上、[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択する必要があります。[Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで日を選択しないと、EnergyWise からの電話機をオフにする指示は無視されます。第 2 に、Unified CM の管理での設定は、EnergyWise がオーバーライドを送信した場合でも、スケジュールどおりに有効になります。たとえば、[ディスプレイをオフにする時刻（Display Off Time）] が 22:00（午後 10 時）に設定されていると仮定すると、[ディスプレイをオンにする時刻（Display On Time）] フィールドの値は 06:00（午前 6 時）となり、[Power Save Plus の有効化（Enable Power Save Plus）] では 1 日以上が選択されています。EnergyWise が 20:00（午後 8 時）に電話機をオフにするように指示すると、この指示は、午前 6 時に設定された [電話機をオンにする時刻（Phone On Time）] まで有効となります（電話機ユーザによる介入が発生しないと仮定した場合）。午前 6 時になると、電話機はオンとなり、Unified CM の管理の設定による電力レベル変更の受信を再開します。電力レベルを電話機で再び変更するには、EnergyWise は電力レベル変更コマンドを新たに再発行する必要があります。また、EnergyWise が電話機の電源をオフにするよう指示した後でユーザが [選択（Select）] ソフトキーを押すと、ユーザとのインタラクションが有効になり、ユーザ操作の結果として電話機の電源がオンになります。デフォルトでは、オフになっています。
録音トーン(Recording Tone)	録音トーンが電話機で有効にするか無効にするかを設定するためにこれを使用できます。有効の場合、電話機は、すべてのコールの両方向に録音トーンを混合します。
録音トーンのローカル音量(Recording Tone Local Volume)	ローカル通話者が聞く録音トーンの音量を設定するために使用できます。この音量設定は再生に使用される実際のデバイス（ハンドセット、スピーカ フォン、ヘッドセット）に関係なく適用されます。音量設定は 0% ～ 100% の範囲内でなければなりません。0% ではトーンなし、100% では現在の音量設定と同じレベルになります。デフォルト値は 100% です。
録音トーンのリモート音量(Recording Tone Remote Volume)	リモート通話者が聞く録音トーンの音量を設定するために使用できます。音量設定は 0% ～ 100 % の範囲内でなければなりません。0% では -66dBM 未満、100% では -4dBM です。デフォルト値は -10dBM または 50% です。
録音トーンの長さ(Recording Tone Duration)	録音トーンがオーディオ ストリームに挿入される時間をミリ秒単位で指定します。このパラメータはデフォルトでこのフィールドのネットワーク ロケール ファイルの値に設定されます。このパラメータの有効な値の範囲は 1 ～ 3000 ミリ秒です。
Medianet 統計情報間隔（Medianet Statistics Interval）	Medianet 統計情報レポートはアクティブ メディア セッション中に定期的に更新されます。統計情報の収集間隔を秒単位で設定します。
メディアネットの無効化（Disable Medianet）	メタデータ、メディアトレース、パフォーマンス モニタリング、および通知を含むすべてのメディアネット オーディオ/ビデオ統計情報のレポート機能を無効にします。

高帯域コーデックの有効化（Enable Wideband Codecs）	電話アプリケーションが広帯域コーデックを Cisco Unified Communications Manager にアドバタイズするかどうかを指定します。コーデック ネゴシエーションには次の 2 段階の手順があります。最初に、電話アプリケーションが Cisco Unified Communications Manager でサポートされているコーデックをアドバタイズする必要があります（すべてのエンドポイントが同じセットのコーデックをサポートする訳ではありません）。2 番目に、Cisco Unified Communications Manager が、コール試行に関連するすべての電話機からサポートされるコーデックのリストを取得すると、リージョン ペア設定などのさまざまな要因に基づいて一般にサポートされるコーデックが選択されます。有効な値で [システム デフォルトの使用（Use System Default）]（この電話アプリケーションはエンタープライズ パラメータ、アドバタイズ G.722 コーデックで指定された設定により異なる）、[無効（Disabled）]（この電話アプリケーションが Cisco Unified Communications Manager にワイドバンドのコーデックをアドバタイズしない）、[有効（Enabled）]（この電話アプリケーションが Cisco Unified Communications Manager にワイドバンドのコーデックをアドバタイズする）のいずれかを指定します。
ビデオ コール（Video Calling）	有効になっている場合、デバイスがビデオ コールに参加することを示します。
デバイス UI プロファイル（Device UI Profile）	基本ビデオ発信者（[シンプル（Simple）]）、共有スペース電話（[パブリック（Public）]）、または一般コラボレーション ユーザ（[拡張（Enhanced）]）など、特定のユーザの個人情報に最適化するようにデバイスのユーザ インターフェイス特性を変更します。
Wifi	デバイス上の Wi-Fi が有効になっているか無効になっているかを示します。
PC ポート（PC Port）	デバイスの PC ポートが有効になっているか無効になっているかを示します。デバイス背面の「COMPUTER」というラベルのポートを通して、PC またはワーク ステーションとデバイスが接続されることにより、1 つのネットワーク接続を共有できます。
PC ポートへのスパン（Span to PC Port）	デバイスが、そのネットワーク ポート経由で送受信したパケットを PC ポートに転送するかどうかを示します。診断目的で使用されるモニタリングと記録用のアプリケーション（コール センター環境で共通）や、ネットワーク パケットキャプチャ ツールなど、デバイス トラフィックのモニタリングを必要とするアプリケーションが PC ポート上で実行されている場合は、[有効（Enabled）] を選択します。この機能を使用するには、PC Voice VLAN へのアクセスを有効にする必要があります。
PC Voice VLAN へのアクセス（PC Voice VLAN Access）	デバイス上の PC ポートに接続されたデバイスにボイス VLAN へのアクセスを許可するかどうかを示します。ボイス VLAN アクセスを無効にすると、接続されている PC でボイス VLAN 上のデータを送受信できなくなります。また、デバイスによって送受信されたデータを PC で受信することができなくなります。アプリケーションがデバイスのトラフィックをモニタリングする必要がある PC で実行されている場合は、この設定を [有効（Enabled）] に設定します。これらには、モニタリングおよび録音アプリケーションと、分析用のネットワーク モニタリング ソフトウェアの使用などが含まれます。
PC ポートのリモート設定（PC Port Remote Configuration）	デバイスの PC ポートの速度とデュプレックスのリモート設定を許可します。これは、デバイス上での手動設定よりも優先されます。
スイッチ ポートのリモート設定（Switch Port Remote Configuration）	デバイスのスイッチ ポートの速度とデュプレックスのリモート設定を許可します。これは、デバイス上での手動設定よりも優先されます。このポートを設定すると、デバイスのネットワーク接続が失われる可能性があることに注意してください。

Unified CM 接続障害の検出（Detect Unified CM Connection Failure）	このフィールドでは、Unified CM/SRST のバックアップへのデバイスのフェールオーバーが発生する前の最初のステップである、Cisco Unified Communications Manager（Unified CM）への接続障害を検出するための電話機の感度を決定します。有効な値は [標準（Normal）]（Unified CM 接続障害の標準システム レートで発生の検出）または [遅延（Delayed）]（Unified CM 接続のフェールオーバーの、通常よりも約 4 倍の遅延での発生の検出）を指定します。Unified CM 接続エラーの高速認識のためには、[標準（Normal）] を選択します。接続を再確立できるようするためにフェールオーバーを少し遅らせる場合は、[遅延（Delayed）] を選択します。[標準（Normal）] と [遅延（Delayed）] の接続エラー検出の正確な時間の差は、常に変化する多数の変数に応じて異なります。これは、有線イーサネット接続にだけ適用されます。デフォルト = 標準（Normal）
Gratuitous ARP	デバイスが Gratuitous ARP 応答から MAC アドレスを学習するかどうかを示します。Gratuitous ARP を受信するデバイス機能を無効にすると、この仕組みを使って音声ストリームのモニタリングおよび録音を行うアプリケーションが機能しなくなります。モニタリング機能が望ましくない場合は、この設定を無効に変更します。
Cisco Discovery Protocol（CDP）：スイッチ ポート（Cisco Discovery Protocol (CDP): Switch Port）	管理者がデバイスのスイッチ ポートの Cisco Discovery Protocol（CDP）を有効または無効にできるようにします。
Cisco Discovery Protocol（CDP）：PC ポート（Cisco Discovery Protocol (CDP): PC Port）	管理者がデバイスの PC ポートの Cisco Discovery Protocol（CDP）を有効または無効にできるようにします。
Link Layer Discovery Protocol - Media Endpoint Discover（LLDP-MED）：スイッチ ポート（Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port）	管理者がデバイスのスイッチ ポートのリンク層検出プロトコル（LLDP-MED）を有効または無効にできるようにします。
Link Layer Discovery Protocol（LLDP）：PC ポート（Link Layer Discovery Protocol - (LLDP): PC Port）	管理者がデバイスの PC ポートのリンク層検出プロトコル（LLDP）を有効または無効にできるようにします。
LLDP アセット ID	管理者は、リンク層検出プロトコル用のアセット ID を設定できます。
LLDP 電源優先度（LLDP Power Priority）	管理者は、リンク層検出プロトコル用の電源優先度を設定できます。
電力ネゴシエーション（Power Negotiation）	管理者は、電力ネゴシエーションを有効または無効にできます。電力ネゴシエーションをサポートしているスイッチにデバイスが接続されたときに、電力ネゴシエーション機能を有効にします。一方、スイッチが電力ネゴシエーションに対応していない場合は、アクセサリの電源を PoE で投入する前に、電力ネゴシエーション機能を無効にする必要があります。電力ネゴシエーション機能が無効の場合、デバイスのアクセサリの電源を最大 12.9W まで上げることができます。
自動ポート同期(Automatic Port Synchronization)	電話で PC ポートおよび SW ポートを同じ速度およびデュプレックスに同期することを有効にします。自動ネゴシエート用に設定されたポートだけが速度を変更します。

802.1X 認証（802.1x Authentication）	802.1x 認証機能のステータスを指定します。
常時 VPN（Always On VPN）	常にデバイスが VPN AnyConnect クライアントを起動し、Cisco Unified Communications Manager の設定済みの VPN プロファイルで接続を確立するかどうかを示します。
デバイス上に VPN パスワードを保存（Store VPN Password on Device）	このパラメータは VPN パスワードがデバイスに保存できるかどうかを制御します。この値はパスワード永続性が連携できるように設定されている場合にのみ使用されます。無効になっている場合は、ユーザの VPN パスワードがメモリに保存され、次の接続で自動的に再送信されます。ただし、デバイスの再起動時は、VPN パスワードを再入力する必要があります。有効になっている場合は、ユーザの VPN パスワードがデバイスに保存され、再起動後も保持されます。
ユーザ定義 VPN プロファイルの許可（Allow User-Defined VPN Profiles）	このパラメータは、ユーザが AnyConnect VPN Client を使用して VPN プロファイルを作成できるかどうかを制御します。無効にすると、ユーザは VPN プロファイルを作成できません。
画面ロックが必要（Require Screen Lock）	このパラメータは、デバイス上で画面ロックが必要かどうかを示します。[ユーザ制御（User Controlled）] が選択されている場合、デバイスはユーザ PIN またはパスワードの入力を促しません。[PIN] および [パスワード（Password）] オプションでは、画面のロックを解除するためのパスワードを入力する必要があります。[PIN] は数字のパスワードで、少なくとも 4 桁の長さが必要です。[パスワード（Password）] は英数字のパスワードで、少なくとも 4 文字で構成され、1 文字は数字以外、1 文字は大文字にする必要があります。
画面ロック タイムアウトの最大値（Maximum Screen Lock Timeout）	デバイスによって画面が自動的にロックされるまでの最大アイドル時間を秒単位で示します。画面がロックされると、画面のロックを解除する際にユーザ パスワードが要求されます。
ディスプレイがオンの時刻に画面ロックを強制（Enforce Screen Lock During Display-On Time）	このパラメータは、Cisco Unified Communications Manager で設定された期間後もデバイスがロックされないような、ユーザが業務時間全体でこれらのデバイスを自由に使用できる、消極的なロック ポリシーを提供します。作業後、デバイスはポリシーの定義に従ってロックし、権限のないユーザがアクセスすることを防ぎます。デバイスは、会議または昼休みのためのユーザ制御の手動ロック オプション（電源ボタン）を常にサポートしています。デバイスは、ユーザが次の使用時に PIN/パスワードを入力するまでロックされたままとなります。[オン（ON）]: デバイスは業務時間中またはディスプレイ点灯時刻の間はロックされます（デフォルト設定）。[オフ（OFF）]: デバイスは、ディスプレイ消灯時刻または業務時間後のみに、上に示されている日付/時刻設定に基づいてロックされます。
音声コール中のデバイスのロック（Lock Device During Audio Call）	音声コールがアクティブの間に、管理者は、音声コール中は画面をオンのままにするように画面ロック PIN 強制タイマーをオーバーライドできます。画面ロック タイマーは音声コールが完了し、タイマーの時間を超過すると有効になります。
Kerberos サーバ（Kerberos Server）	Web プロキシ Kerberos の認証サーバ。
Kerberos レルム(Kerberos Realm)	Web プロキシ Kerberos のレルム。

ロード サーバ(Load Server)	デバイスが、定義されている TFTP サーバではなく、代替サーバを使用して、ファームウェア ロードとアップグレードを取得することを示します。このオプションでは、ファームウェアのアップグレードに使用されるローカル サーバを指定して、特に WAN を介したアップグレードの場合に、インストール回数を減らすことができます。サーバのホスト名または IP アドレスを入力します(標準の IP アドレス形式を使用します)。指定されるサーバは TFTP サービスを実行している必要があり、TFTP パスにロード ファイルが必要です。ロード ファイルが見つからない場合、ロードがインストールされません。デバイスは TFTP サーバにリダイレクトされません。このフィールドが空白のままの場合、デバイスは指定された TFTP サーバを使用してロード ファイルおよびアップグレードを取得します。
IPv6 ロード サーバ(IPv6 Load Server)	電話機が、定義されている TFTP サーバではなく、代替 IPv6 サーバを使用して、ファームウェアのロードとアップグレードを取得することを示します。このオプションでは、ファームウェアのアップグレードに使用されるローカル IPv6 サーバを指定して、特に WAN を介したアップグレードの場合に、インストール回数を減らすことができます。サーバのホスト名または IPv6 アドレスを入力します(標準の IPv6 アドレス形式を使用します)。指定されるサーバは TFTP サービスを実行している必要があり、TFTP パスにロード ファイルが必要です。ロード ファイルが見つからない場合、ロードがインストールされません。電話機は TFTP サーバにリダイレクトされません。このフィールドが空白のままの場合、電話機は指定された TFTP サーバを使用してロード ファイルおよびアップグレードを取得します。
ピア ファームウェア共有(Peer Firmware Sharing)	PPID。サブネット内の単一のデバイスがイメージ ファームウェア ファイルを取得して、ピアに配信することができるよう、ピア ツー ピア イメージ配信を有効または無効にします。この結果、TFTP 帯域幅を削減し、ファームウェア アップグレードにかかる時間を低減します。
ログ サーバ(Log Server)	ログ メッセージの送信先となるリモート システムの IP アドレスとポートを指定します。
IPv6 ログ サーバ(IPv6 Log Server)	ログ メッセージの送信先となるリモート システムの IPv6 アドレスとポートを指定します。形式は [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:ppppp@@options です。options は base=x;pfs=y; という形式です。base 値の範囲は 0 ～ 7 で、pfs 値の範囲は 0 ～ 1 です。この 2 つのパラメータはオプションです。pfs または base を指定しなかった場合、pfs はデフォルト値の 0 に設定され、base はデフォルト値の 7 に設定されます。
ログのプロファイル(Log Profile)	事前定義されたデバッグ コマンドをリモートで実行します。
Web アクセス(Web Access)	このパラメータは、デバイスが Web ブラウザからの接続を許可するか、または別の HTTP クライアントからの接続を許可するかどうかを示します。デバイスの Web サーバ機能を無効にすると、デバイスの内部 Web ページへのアクセスがブロックされます。このページでは、統計情報および設定情報を提供します。QRT(Quality Report Tool)などの機能は、デバイスの Web ページにアクセスしないと、正しく動作しません。この設定は、Web アクセスに依存した、CiscoWorks 2000 などのサービスアビリティ アプリケーションにも影響します。
SSH アクセス(SSH Access)	このパラメータは、デバイスが SSH 接続を受け入れるかどうかを示します。デバイスの SSH サーバ機能を無効にすると、デバイスへのアクセスはブロックされます。

Android Debug Bridge (ADB)	このパラメータは、デバイス上で Android Debug Bridge（ADB）を有効または無効にします。
マルチユーザ（Multi-User）	このパラメータは、マルチユーザをデバイスで有効にするか、無効にするかを示します。
未知の提供元からのアプリケーションを許可（Allow Applications from Unknown Sources）	このパラメータは、URL から、あるいは電子メール、インスタント メッセージ（IM）、または Secure Digital（SD）カード経由で受け取った Android パッケージ（APK）から、ユーザが Android アプリケーションをデバイス上にインストールできるかどうかを制御します。
Google Play からのアプリケーションを許可（Allow Applications from Google Play）	このパラメータは、ユーザが Google の Android Market から Android アプリケーションをインストールできるかどうかを制御します。
Cisco UCM アプリケーション クライアントの有効化（Enable Cisco UCM App Client）	このパラメータは、アプリケーション クライアントがデバイス上で動作するかどうかを制御します。Application Client が有効の場合、Cisco Unified Communications Manager からインストールするアプリケーションを選択できます。
背景イメージ（Background Image）	このパラメータは、デフォルトの壁紙ファイルを指定します。このパラメータを有効にすると、管理者だけが、電話機の壁紙リストへのエンド ユーザ アクセスを無効にできます。
企業画像ディレクトリ（Company Photo Directory）	このパラメータは、デバイスがユーザを照会して、そのユーザに関連付けられた画像を取得するための URL を指定します。
ボイスメール サーバ（プライマリ）（Voicemail Server (Primary)）	プライマリ ビジュアル ボイスメール サーバのホスト名または IP アドレス。
ボイスメール サーバ（バックアップ）（Voicemail Server (Backup)）	バックアップ ビジュアル ボイスメール サーバのホスト名または IP アドレス。
プレゼンスとチャットのサーバ（プライマリ）（Presence and Chat Server (Primary)）	プライマリ プレゼンス サーバのホスト名または IP アドレス。
プレゼンスとチャットのサーバのタイプ（Presence and Chat Server Type）	このパラメータは、[プレゼンスとチャットのサーバ（Presence and Chat Server）] フィールドで指定されているサーバのタイプを示します。
プレゼンスとチャットのシングル サインオン（SSO）ドメイン（Presence and Chat Single Sign-On (SSO) Domain）	企業に対するシングルサインオン（SSO）認証を実施するために Cisco WebEx Connect Cloud で使用されるエンタープライズ ドメイン。
マルチ ユーザ URL（Multi-User URL）	このパラメータは、エクステンション モビリティ サーバの URL を指定します。
カスタマー サポートの電子メール アドレス（Email address for customer support）	ユーザがエンドポイント上の「問題レポート ツール」から問題レポート ファイルを送信する送信先電子メール アドレスを設定します。

DX650 固有のオプションは次のとおりです。

Power Save Plus の有効化（Enable Power Save Plus）	Power Save Plus 機能を有効にするには、スケジュールで、電話機の電源をオフにする日を選択します。Ctrl キーを押しながら日をクリックすると、Power Save Plus を実行する日を複数選択できます。デフォルトはディセーブル（選定日なし）。Power Save Plus モードでは 1 つのキーを点灯させるだけの電力が維持されます。電話機のその他の機能は、Power Save Plus モードではオフになります。Power Save Plus モードは、[電話機をオンにする時刻（Phone On Time）] と [電話機をオフにする時刻（Phone Off Time）] フィールドで指定された期間、電話機をオフにします。この期間は、通常、組織の通常の運用時間外です。点灯しているキーをユーザが押すと、電話機が完全にオンになります。点灯しているキーを押すと、電話機の電源が再投入され、完全に動作可能になる前に Unified CM に再登録されます。省電力モードはデフォルトで無効です。このフィールドの日を選択すると、次の、E911 の問題を示す通知が表示されます。Power Save Plus を有効にすることで、この通知で指定された条件に同意します。 Power Save Plus モード（「モード」）が有効である間は、モードに設定されたエンドポイントは、緊急コールでは無効で、インバウンド コールの受信ができません。このモードを選択することにより、次の条項に同意したものと見なされます。(I) モードが有効である間、緊急コールとコールの受信用の代替方法を責任を持って用意する必要があります。(II) シスコはこのモードの選択に関して何の責任を負いません。このモードを有効にすることは、お客様の責任で行っていただきます。(III) コール、発信、およびその他について、このモードを有効にした場合の影響をユーザにすべて通知する必要があります。
電話機をオンにする時刻（Phone On Time）	このフィールドでは、[Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで選択された日に自動的に電話機がオンになる時刻を指定します。時刻を 24 時間形式で入力します。00:00 は午前 0 時を表します。たとえば、午前 7:00（0700）に電話機を自動的にオンにするには、7:00 と入力します。電話機を午前 2:00 （1400）にオンにするには、14:00 と入力します。このフィールドがブランクの場合、電話機は 00:00 に自動的にオンになります。
電話機をオフにする時刻（Phone Off Time）	このフィールドは、[Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで選択された日に電話機がオフになる時刻を指定します。時:分の形式で時間を入力します。このフィールドがブランクの場合、電話機は午前 0 時（00:00）で自動的にオフになります。（注）[電話機をオンにする時刻（Phone On Time）] がブランク（または 00:00）の場合、もしくは [電話機をオフにする時刻（Phone Off Time）] がブランク（または 24:00）の場合、EnergyWise でオーバーライドを送信可能にしない限り、電話機では実質的に Power Save Plus 機能が無効なままの状態が継続されます。
電話機をオフにするアイドル タイムアウト（Phone Off Idle Timeout）	このフィールドは、デバイスの電源をオンにデバイスが給電側機器（PSE）を要求するまでにデバイスがアイドル状態になっている必要がある分数を表します。このフィールドの値は、次の場合に有効になります。デバイスがスケジュール通りに Power Save Plus モードにあり、電話機ユーザが Select キーを押して、Power Save Plus モードを解除した場合。[電話機をオフにする時刻（Phone Off Time）] を満たしているが、電話が使用中の場合。単位は分です。デフォルト値は 60 です。範囲は 20 ～ 1440 です。

これらの機能の詳細については、『Cisco DX Series Administration Guide』または『Cisco DX Series Release Notes』を参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

Cisco Unified Wireless LAN Controller およびアクセス ポイントの設定

Cisco Unified Wireless LAN Controller およびアクセス ポイントを設定するときは、次のガイドラインを使用してください。

- 802.1x 認証を使用する場合は、[**CCKM**] が [**有効（Enabled）**] になっていることを確認します。
- [**Quality of Service (QoS)**] を [**プラチナ（Platinum）**] に設定します。
- [**WMM ポリシー（WMM Policy）**] を [**必要条件（Required）**] に設定します。
- [**セッションのタイムアウト（Session Timeout）**] が有効で、正しく設定されていることを確認します。
- [**Aironet IE**] が [**有効（Enabled）**] になっていることを確認します。
- [**DTPC サポート（DTPC Support）**] を [**有効（Enabled）**] に設定します。
- [**P2P（ピアツーピア）のブロック アクション（P2P (Peer to Peer) Blocking Action）**] および [**パブリック セキュア パケット フォワーディング（PSPF）（Public Secure Packet Forwarding (PSPF)）**] を無効にします。
- [**クライアント除外（Client Exclusion）**] が正しく設定されていることを確認します。
- [**DHCP アドレス割り当て必須（DHCP Address Assignment Required）**] を無効にします。
- [**MFP クライアント保護（MFP Client Protection）**] を [**任意（Optional）**] または [**無効（Disabled）**] に設定します。
- [**DTIM 期間（DTIM Period）**] を「**2**」に設定します。
- [**クライアント ロード バランシング（Client Load Balancing）**] を [**無効（Disabled）**] に設定します。
- [**クライアントの帯域選択（Client Band Select）**] を [**無効（Disabled）**] に設定します。
- [**IGMP スヌーピング（IGMP Snooping）**] を [**有効（Enabled）**] に設定します。
- レイヤ 3 モビリティを使用している場合は、[**シンメトリック モバイル トンネリング モード（Symmetric Mobile Tunneling Mode）**] を有効にします。
- 2.4 GHz を使用している場合は、[**ショート プリアンブル（Short Preamble）**] を有効にします。
- Cisco 802.11n アクセス ポイントを使用している場合は、[**クライアント リンク（ClientLink）**] を有効にします。
- 必要に応じて [**データ レート（Data Rates）**] を設定します。
- [**CCX ロケーション測定（CCX Location Measurement）**] を有効にします。
- 必要に応じて [**Auto RF**] を設定します。
- 必要に応じて、[**ボイス（Voice）**] の [**SIP CAC サポート（SIP CAC Support）**] を設定します。
- [**ボイス（Voice）**] で [**トラフィック ストリーム メトリック（Traffic Stream Metrics）**] を有効にします。
- [**ビデオ（Video）**] で [**アドミッション制御必須（Admission Control Mandatory）**] を [**無効（Disabled）**] に設定します。
- [**EDCA プロファイル（EDCA Profile）**] を [**音声およびビデオの最適化（Voice and Video Optimized）**] に設定します。
- [**低遅延 MAC を有効にする（Enable Low Latency MAC）**] を [**無効（Disabled）**] に設定します。

- [**電力制限（Power Constraint）**] が [**無効（Disabled）**] になっていることを確認します。
- [**チャネル通知（Channel Announcement）**] および [**チャネル Quiet モード（Channel Quiet Mode）**] を有効にします。
- 必要に応じて [**高スループット データ レート（High Throughput Data Rates）**] を設定します。
- **フレームの集約**を設定します。
- CleanAir テクノロジーを搭載したシスコ製アクセス ポイントを使用している場合は、[**CleanAir**] を有効にします。
- 必要に応じて [**マルチキャスト ダイレクト機能（Multicast Direct Feature）**] を設定します。
- [**プラチナ（Platinum）**] QoS プロファイルで、[**802.1p タグ（802.1p Tag）**] を **5** に設定します。

（注） 他のリージョンからのクライアントが存在し、ワイヤレス LAN とのアソシエートが試みられる場合は、ワールド モード（802.11d）が有効であることを確認してください。

802.1x 認証を使用している場合は、高速セキュア ローミングを提供するため CCKM を実装することが推奨されます。

WLAN 設定

Cisco DX シリーズには、個別の SSID を割り当てることを推奨します。

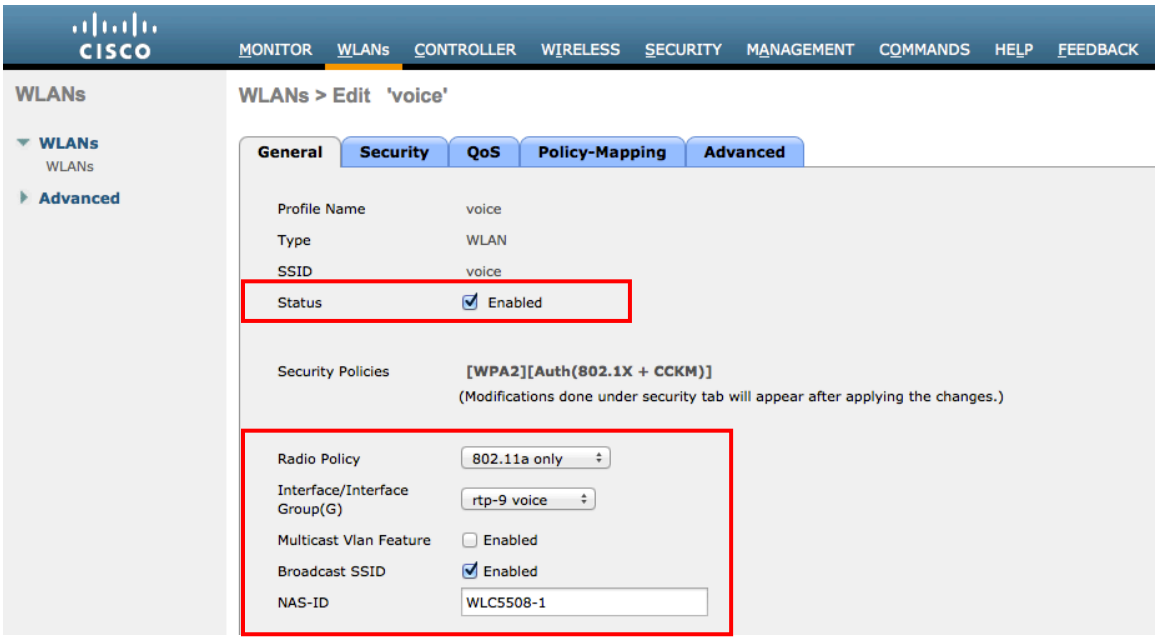
ただし、音声またはビデオ対応 Cisco Wireless LAN のエンドポイントをサポートするように設定された既存の SSID がある場合、その WLAN を代わりに使用できます。

Cisco DX シリーズで使用する SSID は、特定の 802.11 無線タイプにのみ適用するように設定できます（802.11a のみなど）。

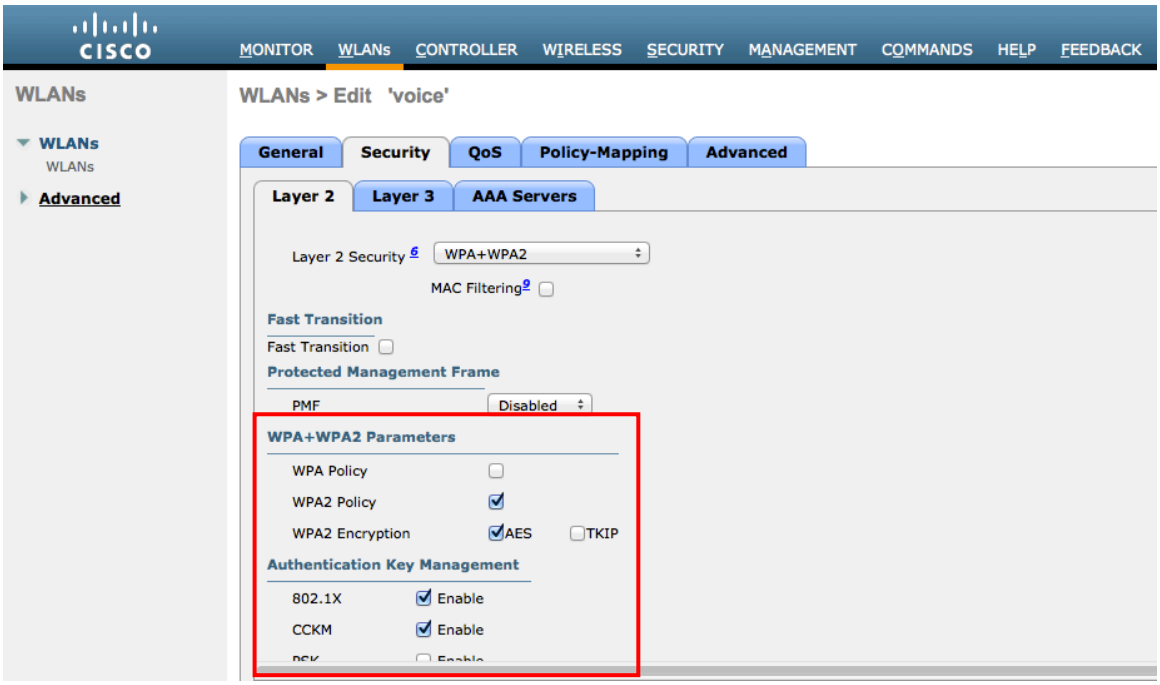
Cisco DX シリーズは 5 GHz 帯域でのみ動作させることを強くお勧めします。これは、多数のチャネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

[**ブロードキャスト SSID（Broadcast SSID）**] を有効にすると、ネットワークをただリストから選択し、追加パラメータ（セキュリティ クレデンシャル、周波数帯など）を、すべてのパラメータを手動で設定せずに設定できる Cisco DX シリーズの配置で役立ちます。

選択した SSID が他の LAN に使用されていないことを確認してください。使用されている場合で、特に異なるセキュリティ タイプを使用している場合は、電源の投入時またはローミング中に、障害が発生する可能性があります。



高速セキュア ローミングに CCKM を利用するには、[WPA2 ポリシー（WPA2 Policy）] を [AES] 暗号化と共に有効にし、認証キー管理タイプの [802.1x] と [CCKM] を有効にして、高速セキュア ローミングを有効にします。

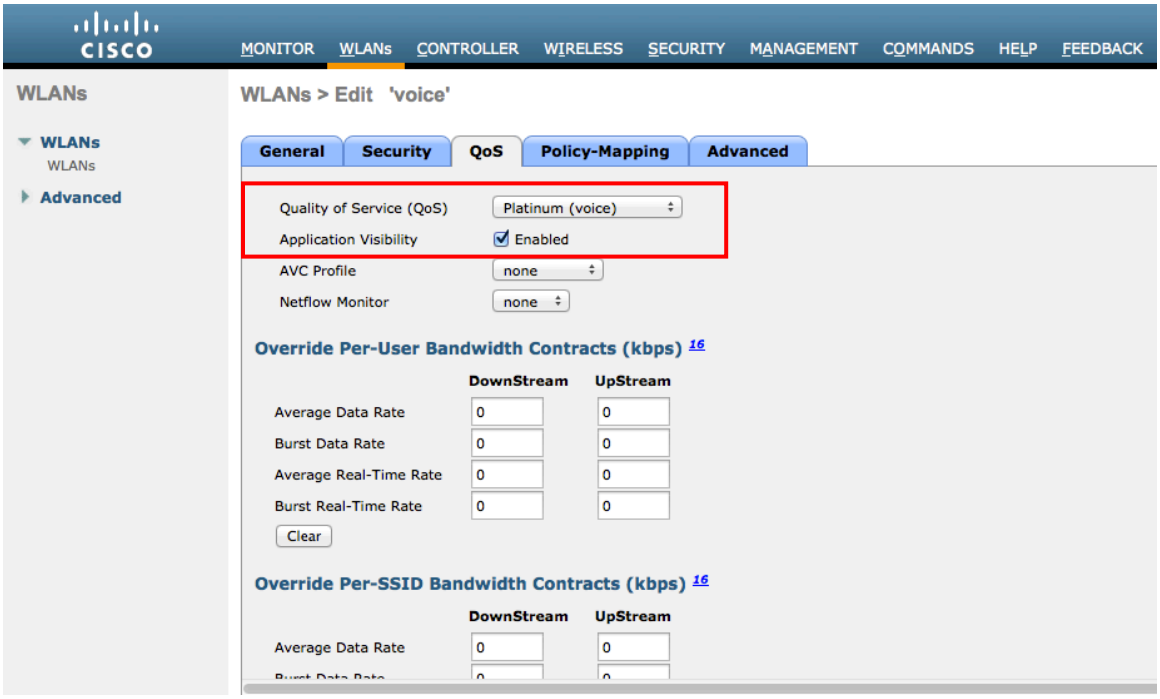


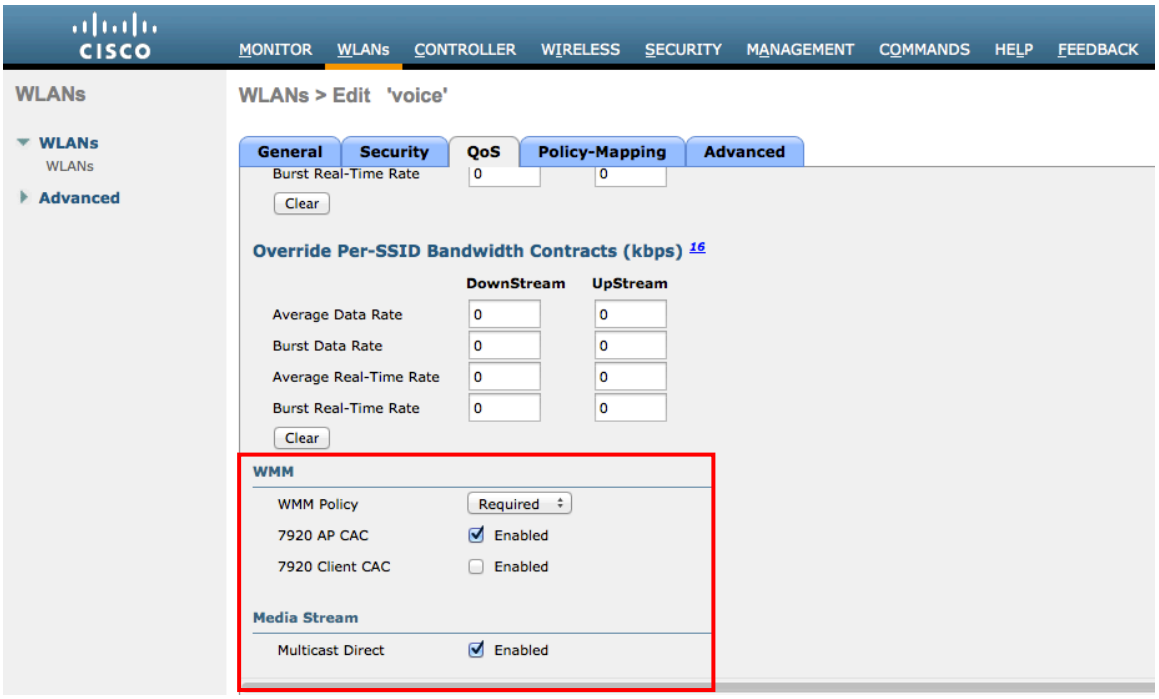
WMM ポリシーは、Cisco DX シリーズまたはその他の WMM 対応の音声およびビデオ対応エンドポイントがこの SSID を使用する場合にのみ、[**必要（Required）**] に設定する必要があります。

WLAN に非 WMM クライアントが存在する場合、それらのクライアントは別の WLAN に配置することを推奨します。

非 WMM クライアントが Cisco DX シリーズと同じ SSID を使用する必要がある場合は、WMM ポリシーが [**許可（Allowed）**] に設定されていることを確認します。

[**7920 AP CAC**] を有効にして、Qos Basic Service Set（QBSS）をクライアントにアドバタイズします。





必要に応じて [**セッション タイムアウトの有効化（Enable Session Timeout）**] を設定します。音声またはビデオ コール時に起こり得る障害を回避するため、セッション タイムアウトを無効にするか、タイムアウトを延長（24 時間/86400 秒など）することを推奨します。無効にすると、中断の発生は完全に回避されますが、セッション タイムアウトを有効にすると、クライアントのクレデンシャルを定期的に再検証し、クライアントが有効なクレデンシャルを使用していることを確認するのに役立ちます。

[Aironet 拡張機能（**Aironet IE**）]を有効にします。

[**ピアツーピア（P2P）のブロック アクション（Peer to Peer (P2P) Blocking Action**）] を無効にする必要があります。

必要に応じて [**クライアント除外（Client Exclusion**）] を設定します。

必要な場合は、[**AP 無線機ごとに許可される最大クライアント数（Maximum Allowed Clients Per AP Radio）**] を設定することもできます。

[**オフ チャネル スキャンの待機（Off Channel Scanning Defer）**] を調整することで、スキャンの待機時間だけでなく、特定のキューに対するスキャンを待機させることができます。

ベスト エフォート アプリケーションを頻繁に使用する場合（Web ブラウジング、VPN など）、または優先順位の高いアプリケーション（音声、ビデオ、コール制御など）の DSCP 値がアクセス ポイントに保持されていない場合は、優先順位の低いキュー（0 ～ 3）を、優先順位の高いキュー（4 ～ 6）に従って有効にしてオフ チャネル スキャンを保留することを推奨しますが、これにより潜在的にスキャンの保留時間が増加します。

[**DHCP アドレス割り当て必須（DHCP Address Assignment Required）**] を無効にする必要があります。

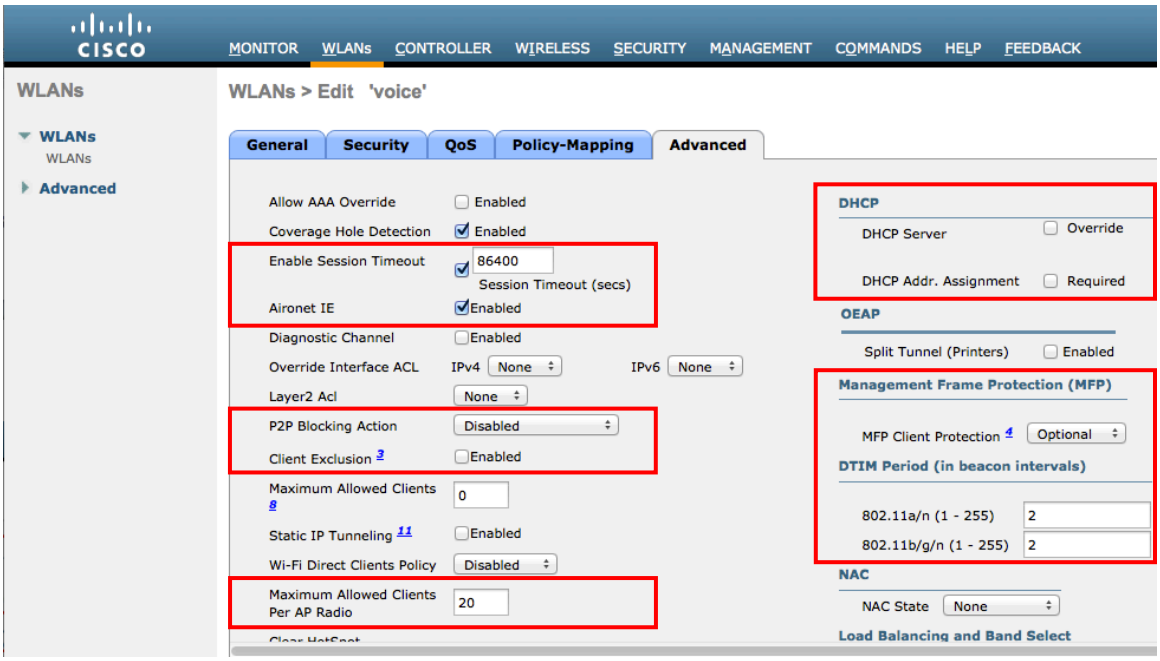
[**管理フレーム保護（Management Frame Protection）**] を [**任意（Optional）**] または [**無効（Disabled）**] に設定します。

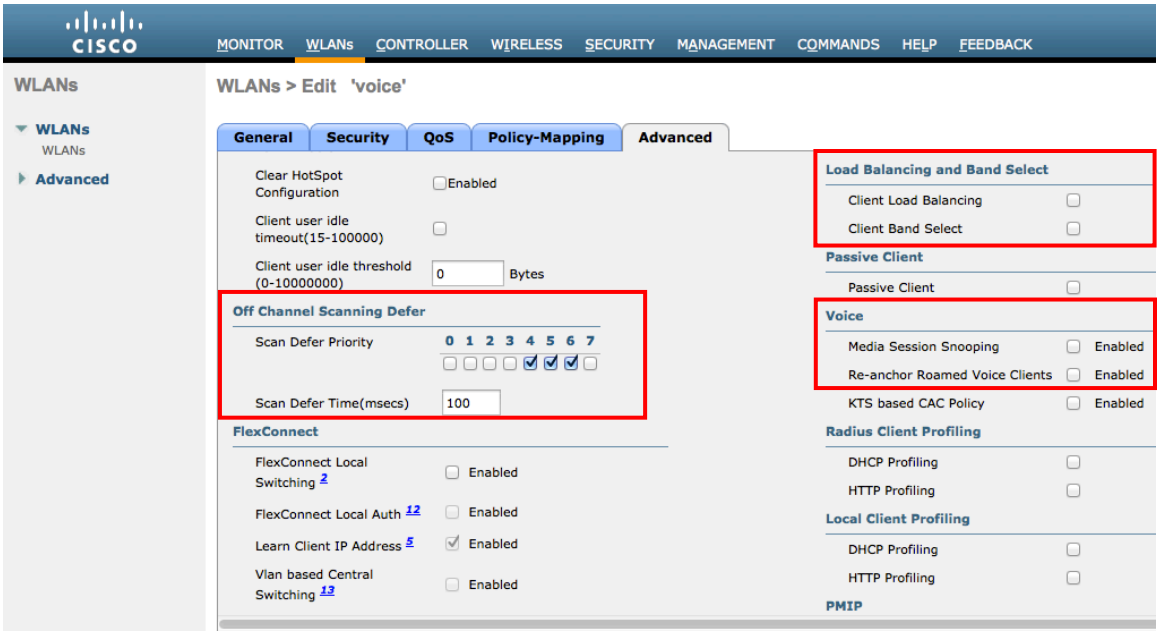
100 ミリ秒のビーコン周期で [**DTIM 期間（DTIM Period）**] を **2** で使用します。

[**クライアント ロード バランシング（Client Load Balancing）**] と [**クライアントの帯域選択（Client Band Select）**] が無効になっていることを確認します。

オプションで、[**メディア セッションのスヌーピング（Media Session Snooping）**] を有効にして SIP CAC を使用できるようにすることができます。

コールがコントローラ間ローミングを実行した後に終了すると、ワイヤレス LAN 接続が短時間中断されることがあるので、[**ローミングされた音声クライアントを再固定（Re-anchor Roamed Voice Clients）**] を無効にすることを推奨します。





Cisco Autonomous Access Point に対しては、802.1x 認証を使用する場合、SSID に open + eap および network-eap を設定します。

```
dot11 ssid voice
   vlan 21
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa cckm
   admit-traffic
```

Cisco Autonomous Access Point をワイヤレスドメイン サービス（WDS）サーバに登録する場合は、両方のタイプの認証が WDS の設定で有効になっていることを確認します。

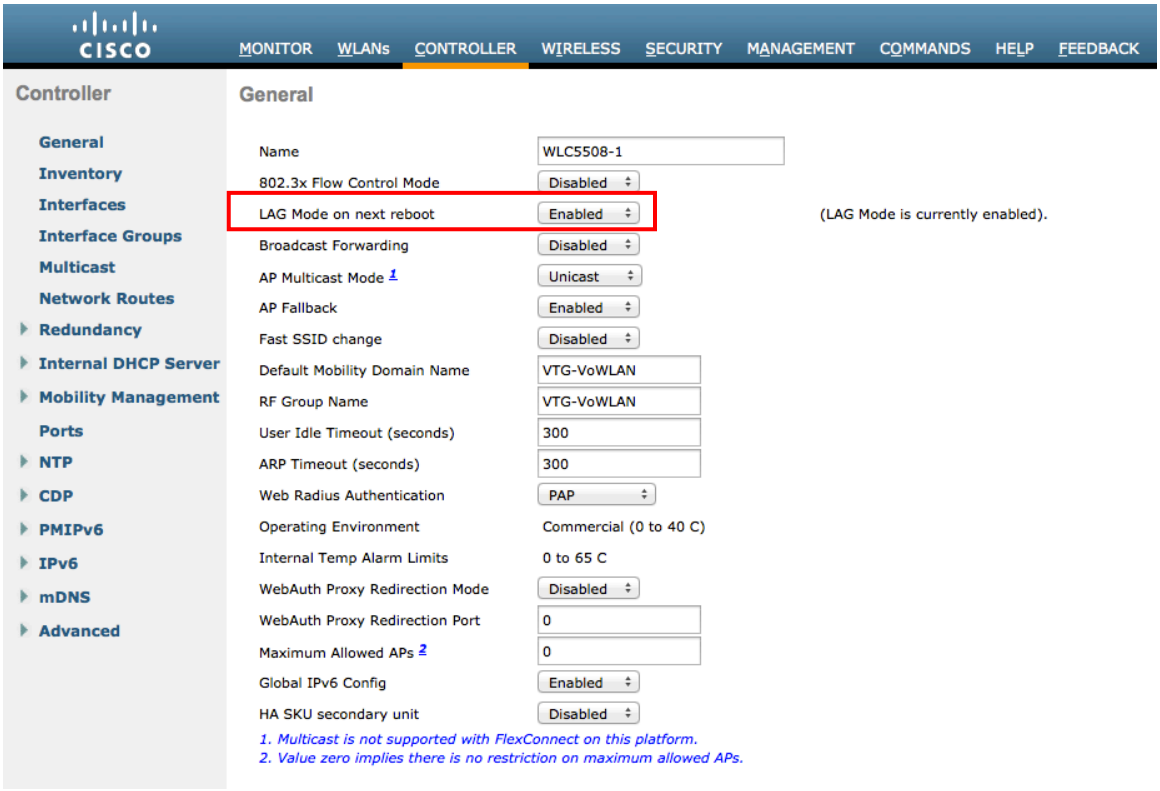
```
wlccp authentication-server infrastructure method_Infrastructure
wlccp authentication-server client mac method_Clients
wlccp authentication-server client eap method_Clients
wlccp authentication-server client leap method_Clients
wlccp wds priority 255 interface BVI1
```

コントローラの設定

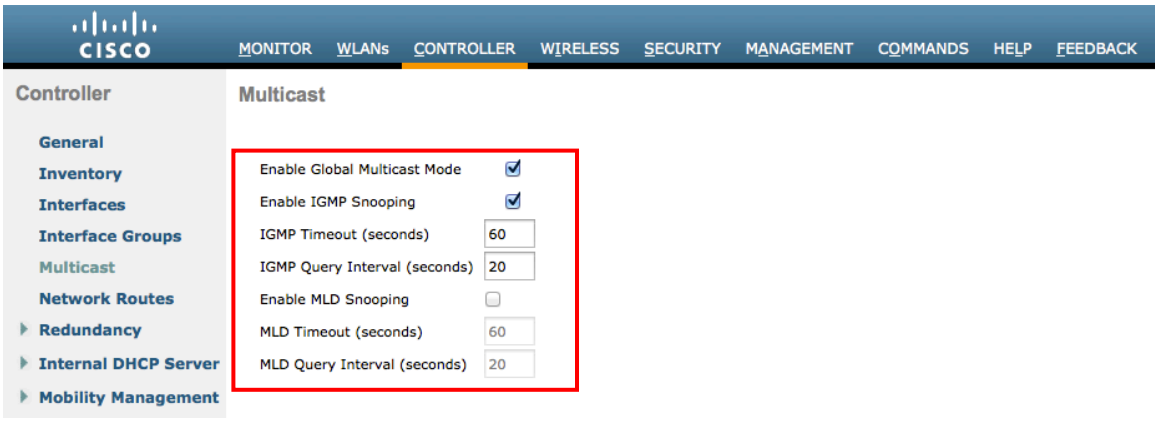
Cisco Unified Wireless LAN Controller のホスト名が正しく設定されていることを確認します。

Cisco Unified Wireless LAN Controller で複数のポートを使用している場合はリンク集約（LAG）を有効にします。

目的の AP マルチキャスト モードを設定します。

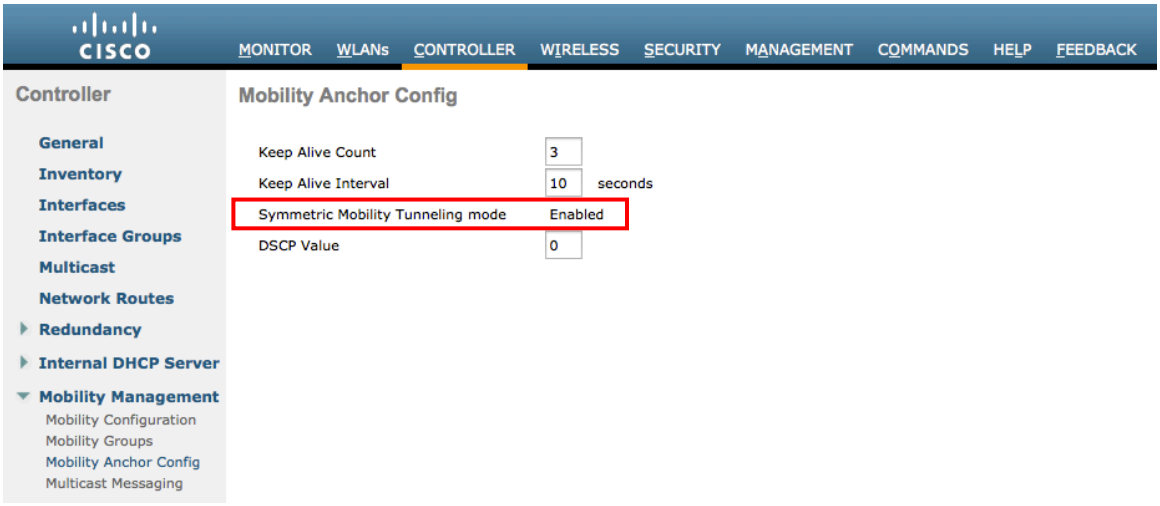


マルチキャストを使用する場合は、[**グローバル マルチキャスト モードの有効化（Enable Global Multicast Mode）**] および [**IGMP スヌーピングの有効化（Enable IGMP Snooping）**] を有効にする必要があります。

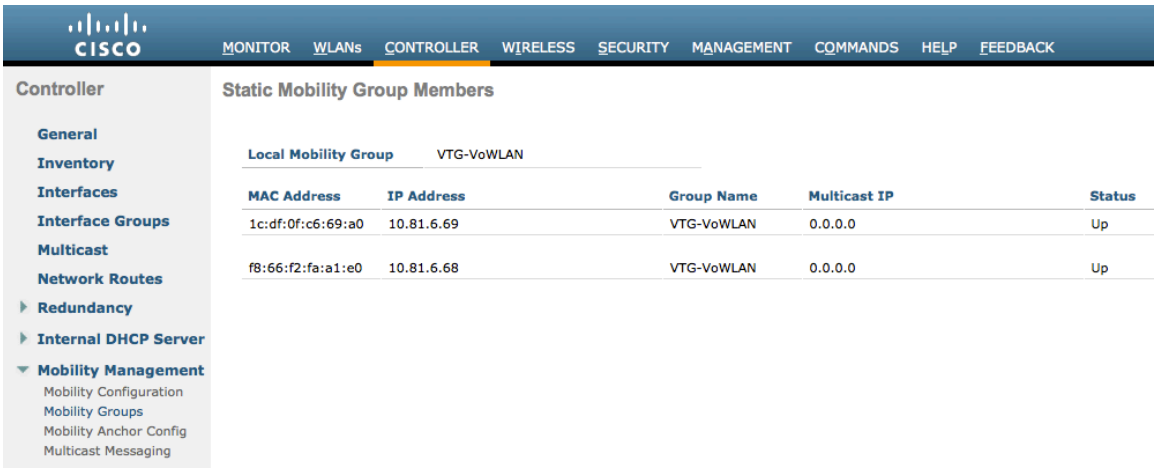


レイヤ 3 モビリティを使用している場合は、[**シンメトリック モビリティトンネリング（Symmetric Mobility Tunneling）**] を [**有効（Enabled）**] に設定する必要があります。

最新のバージョンでは、シンメトリック モビリティトンネリングがデフォルトで有効になり、設定することはできません。



複数の Cisco Unified Wireless LAN Controller を同じモビリティグループに設定する場合、各 Cisco Unified Wireless LAN コントローラの IP アドレスと MAC アドレスをスタティック モビリティグループ メンバの設定に追加する必要があります。



802.11 ネットワークの設定

5 GHz を使用する場合は、802.11a ネットワークのステータスが [**有効（Enabled）**] になっていることを確認します。

[**ビーコン周期（Beacon Period）**] を「**100 ms**」に設定します。

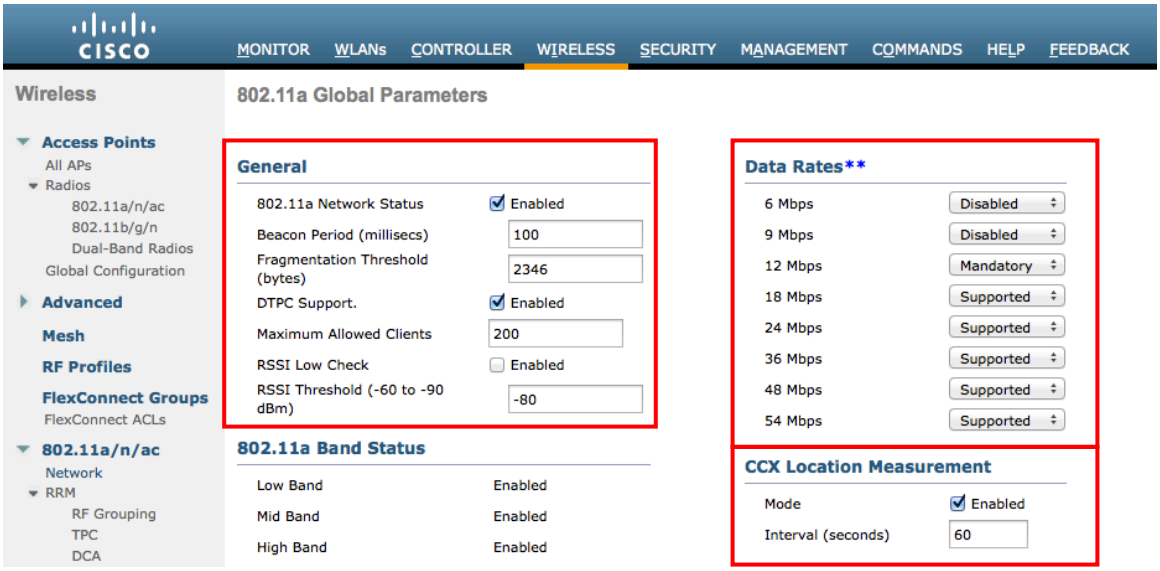
[**DTPC サポート（DTPC Support）**] が有効になっていることを確認します。

Cisco 802.11n アクセス ポイントを使用している場合は、[**クライアント リンク（ClientLink）**] が有効になっていることを確認します。

現在のリリースでは、[**許可される最大クライアント数（Maximum Allowed Clients）**] を設定することができます。

必須（基本）レートとして 12 Mbps を、サポート対象（任意）レートとして 18 Mbps 以上を設定することをお勧めします。ただし、環境によっては、6 Mbps を必須（基本）レートとして有効にする必要がある場合があります。

[**CCX ロケーション測定（CCX Location Measurement）**] を有効にします。



2.4 GHz を使用する場合は、802.11b/g/n ネットワークのステータスと 802.11g/n が有効になっていることを確認します。

[**ビーコン周期（Beacon Period）**] を「**100 ms**」に設定します。

ロング プリアンブルを必要とするレガシー クライアントがワイヤレス LAN に存在しない場合は、アクセス ポイントの 2.4 GHz 無線設定で [**ショート プリアンブル（Short Preamble）**] を [**有効（Enabled）**] に設定する必要があります。ロング プリアンブルの代わりにショート プリアンブルを使用することによって、ワイヤレス ネットワークのパフォーマンスが向上します。

[**DTPC サポート（DTPC Support）**] が有効になっていることを確認します。

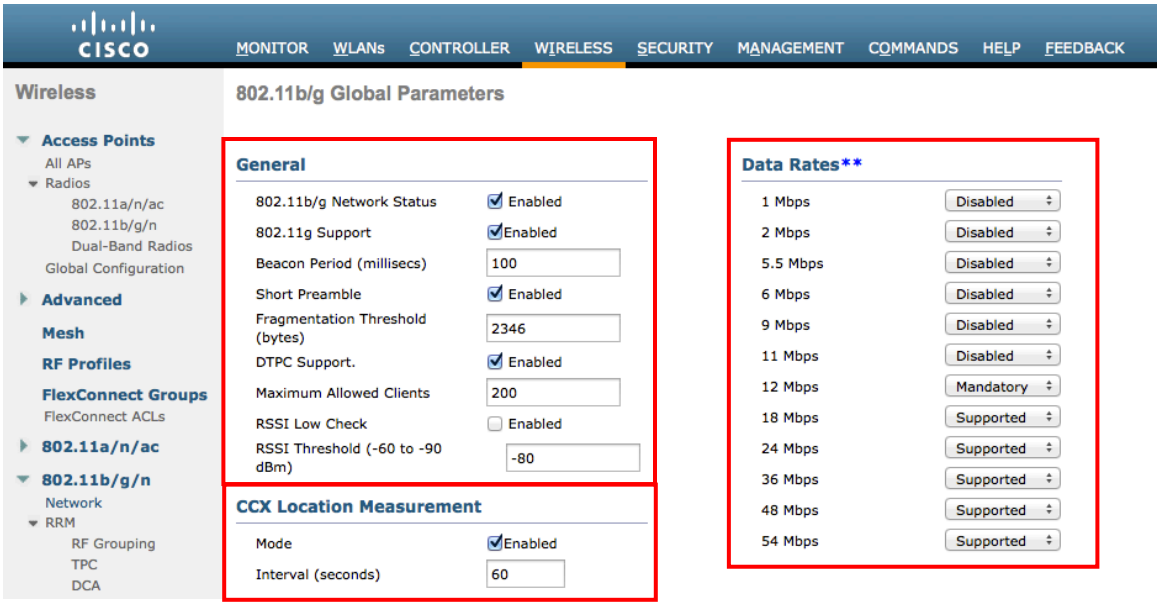
Cisco 802.11n アクセス ポイントを使用している場合は、[**クライアント リンク（ClientLink）**] が有効になっていることを確認します。

現在のリリースでは、[**許可される最大クライアント数（Maximum Allowed Clients）**] を設定することができます。

ワイヤレス LAN に接続する 802.11b のみのクライアントがない場合、必須（基本）レートとして 12 Mbps を、サポート対象（任意）レートとして 18 Mbps を設定することをお勧めします。ただし、環境によっては、6 Mbps を必須（基本）レートとして有効にする必要がある場合があります。

802.11b クライアントが存在する場合は、必須（基本）レートとして 11 Mbps を、サポート対象（任意）レートとして 12 Mbps 以上を設定する必要があります。

[**CCX ロケーション測定（CCX Location Measurement）**] を有効にします。



ビーム形成

Cisco 802.11n アクセス ポイントを使用している場合は、[**クライアント リンク（ClientLink）**] を有効にします。

ビーム形成は、1、2、5.5、および 11 Mbps のデータ レートではサポートされていません。

7.2.103.0 より前のリリースでは、[802.11 グローバル パラメータ（802.11 Global Parameters）] セクションを使用してグローバルに、またはアクセス ポイントの 802.11 無線設定ページを使用して個々のアクセス ポイントで、[**クライアント リンク（ClientLink）**] を有効にできます。

リリース 7.2.103.0 では、Cisco Unified Wireless LAN Controller の Web インターフェイスを使用して [**クライアント リンク（ClientLink）**] を設定することができなくなり、コマンドラインでのみ設定できます。

リリース 7.2.103.0 以降では、次のコマンドを使用して、すべてのアクセス ポイントにグローバルに、または個々のアクセス ポイント無線に対してビーム形成機能を有効にします。

（Cisco Controller）>config 802.11a beamforming global enable

（Cisco Controller）>config 802.11a beamforming ap <ap_name> enable

（Cisco Controller）>config 802.11b beamforming global enable

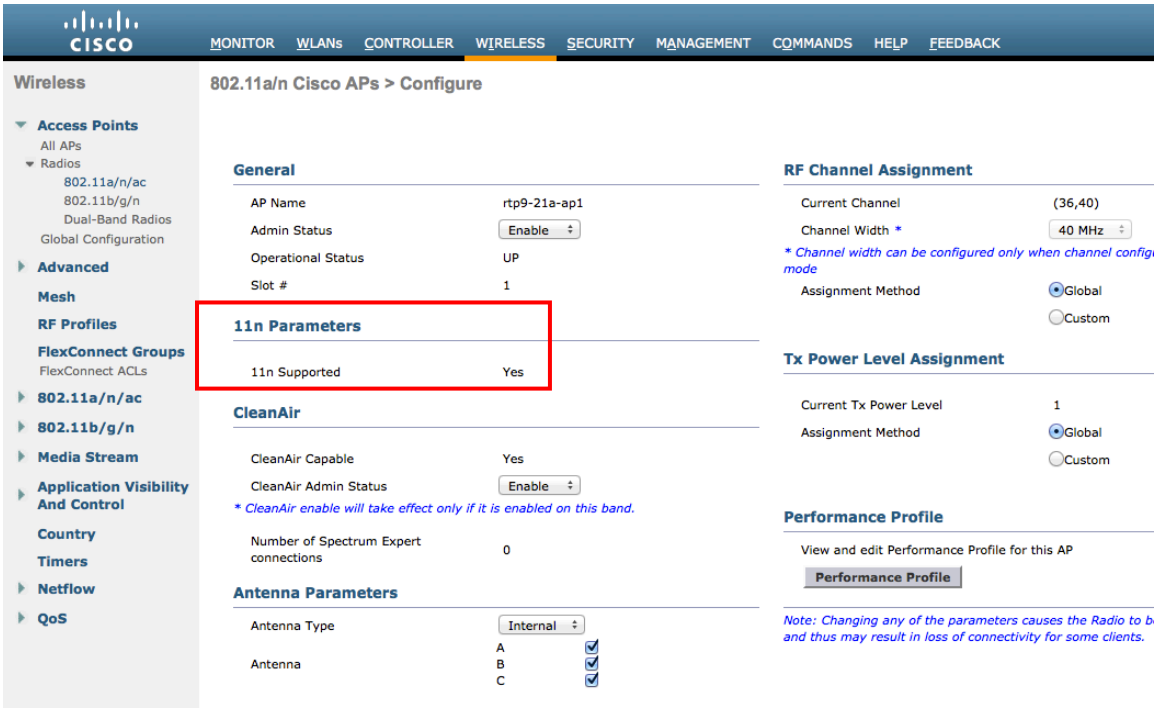
（Cisco Controller）>config 802.11b beamforming ap <ap_name> enable

次のコマンドを使用して、ビーム形成機能の現在のステータスを表示できます。

（Cisco Controller）>show 802.11a

（Cisco Controller）>show 802.11b

Legacy Tx Beamforming setting..... **Enabled**

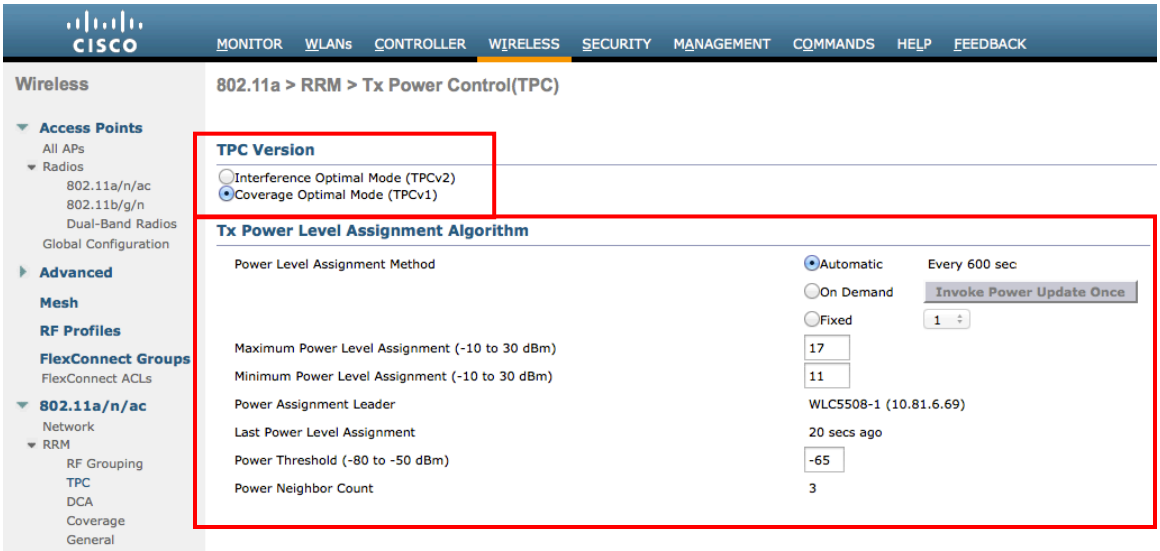


Auto RF（RRM）

Cisco Unified Wireless LAN Controller を使用する場合は、Auto RF でチャネルと送信電力の設定を管理できるようにすることが推奨されます。

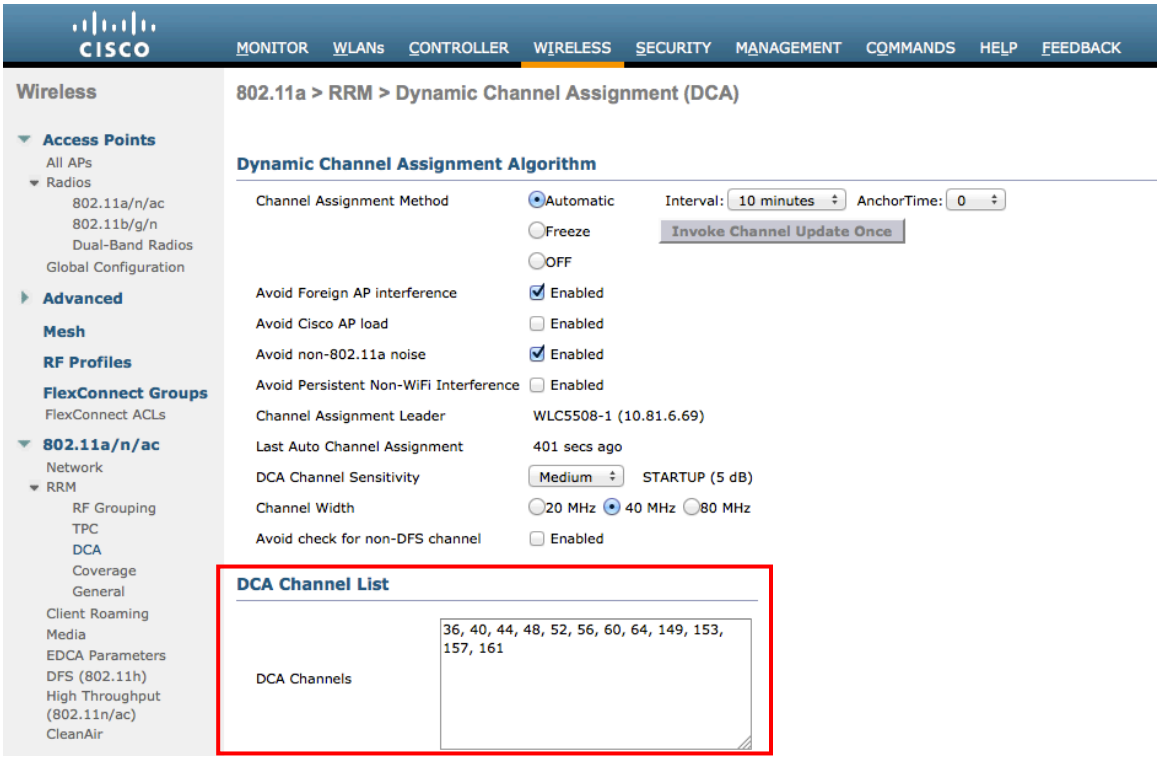
使用する帯域（5 GHz または 2.4 GHz ）に応じて、アクセス ポイントの送信電力レベルの割り当て方法を設定します。

自動電力レベルの割り当てを使用する場合、電力の最大レベルと最小レベルを指定できます。



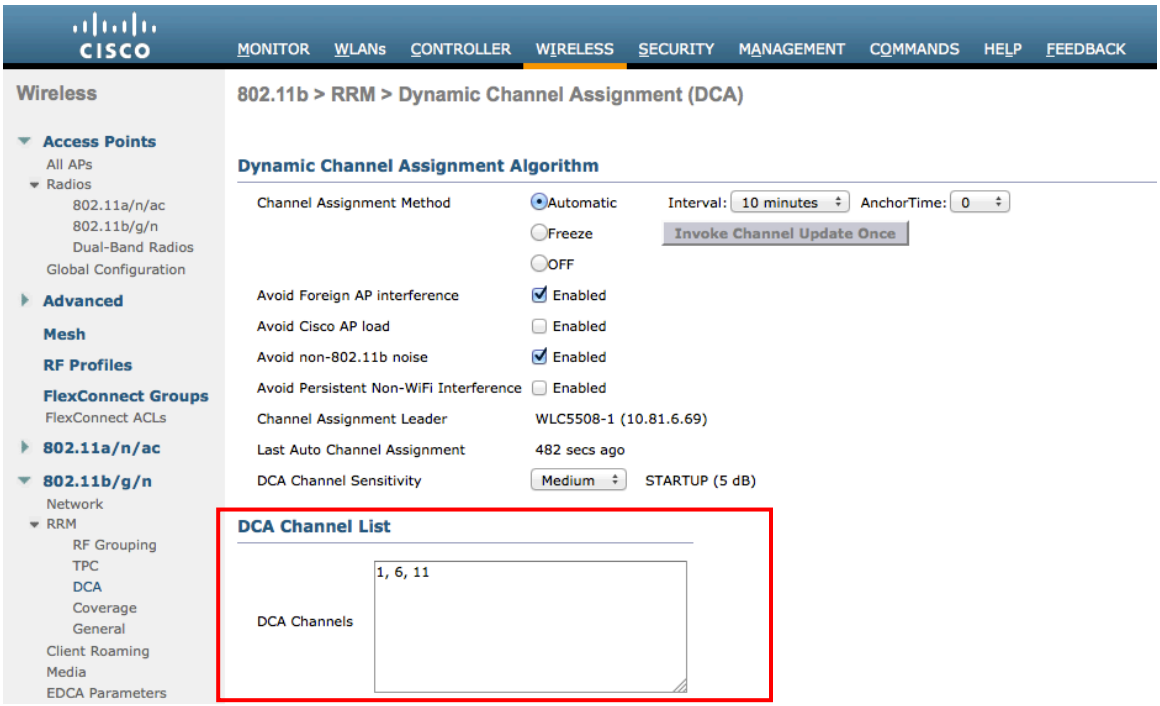
5 GHz を使用する場合は、有効にするチャネル数を最大で 12 チャネルに抑え、多数のチャネルをスキャンするために発生するアクセス ポイント検出の遅延の可能性を回避することを推奨します。

シスコ製の 802.11n アクセス ポイントを使用する場合、5 GHz チャネル幅は 20 MHz または 40 MHz に対して設定できます。



2.4 GHz を使用する場合、DCA リストではチャネル 1、6、および 11 だけを有効にします。

2.4 GHz 帯域で使用可能なチャネルの数が限られているために、40 MHz に対応したシスコ製の 802.11n アクセス ポイントを使用する場合でも、20 MHz には 2.4 GHz チャネルを設定することを推奨します。



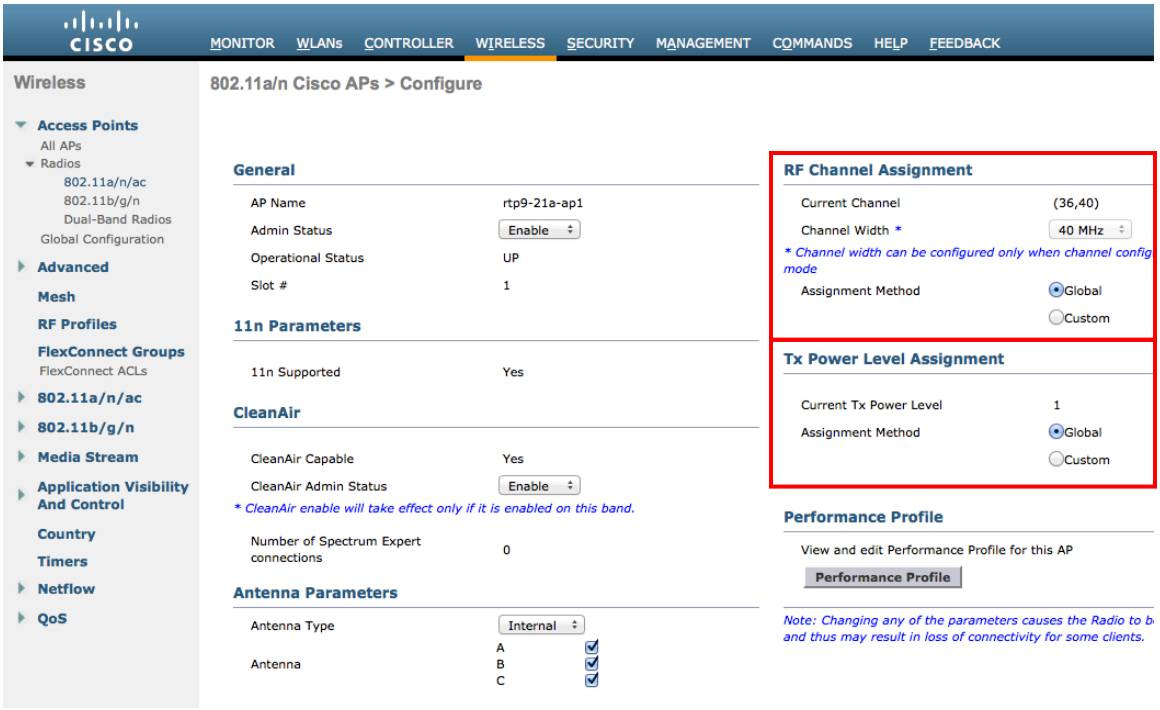
使用する帯域に応じて 5 GHz または 2.4 GHz にダイナミック チャネルおよび送信電力の割り当てを使用するため、グローバル設定よりも個々のアクセス ポイントが優先されるように設定できます。

有効なその他のアクセス ポイントを Auto RF に対して有効にして、静的に設定されているアクセス ポイントを回避できます。

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

シスコ製の 802.11n アクセス ポイントを使用する場合、5 GHz チャネル幅は 20 MHz または 40 MHz に対して設定できます。

チャネル ボンディングは 5 GHz を使用している場合にのみ使用することをお勧めします。



クライアント ローミング

Cisco DX シリーズでは、スキャンおよびローミングは、電話機自体によって独立して管理されるため、Cisco Unified Wireless LAN Controller のクライアント ローミング セクションの RF パラメータを使用しません。

コール アドミッション制御

Cisco DX シリーズは、現在、TSPEC(コール アドミッション制御)をサポートしていません。

音声用のコール アドミッション制御(TSPEC)は、他の TSPEC 対応クライアントが同じ帯域周波数を使用している場合にだけ有効にする必要があります。ビデオ用の TSPEC は有効にしないでください。

[音声(Voice)] に対して **[アドミッション制御必須(ACM)(Admission Control Mandatory (ACM))]** が有効になっている場合は、Cisco DX シリーズでオーディオ パケット送信アップストリームの優先順位を UP6(音声)からオーディオ専用コール用のより低い優先順位(UP5 ビデオ)に下げる必要があります。

音声のコール アドミッション制御が有効になっている場合、最大帯域幅を設定し、使用する帯域に応じて 5 または 2.4 GHz の予約ローミング帯域幅の割合を設定します。

音声に対する最大帯域幅のデフォルト設定は **75 %** で、このうち **6 %** はローミング クライアントに予約されています。

ローミング クライアントは予約済みのローミング帯域幅の使用に制限されませんが、その他の帯域幅がすべて使用されている場合に備え、ローミング帯域幅はローミング クライアント用にある程度の帯域幅を予約します。

CAC を有効にする場合は、[**負荷ベースの CAC（Load-based CAC）**] が有効であることを確認します。この機能は Cisco Unified Wireless LAN Controller で使用できますが、現在のところ、Cisco Autonomous Access Point プラットフォームでは使用できません。

負荷ベースの CAC は、チャネル上のすべてのエネルギーを考慮します。

TSPEC が現在サポートされていないため、**SIP CAC** が使用できますが、WLAN でメディア セッション スヌーピングを有効にする必要があります。

TSPEC をサポートしていないため**トラフィック ストリーム メトリック（TSM）**はサポートされていませんが、他の対応クライアントが同じ帯域周波数を使用している場合、この機能を有効にできます。

SIP CAC は、ダウンストリームの音声フレームが正しく順位付けされるようにします。

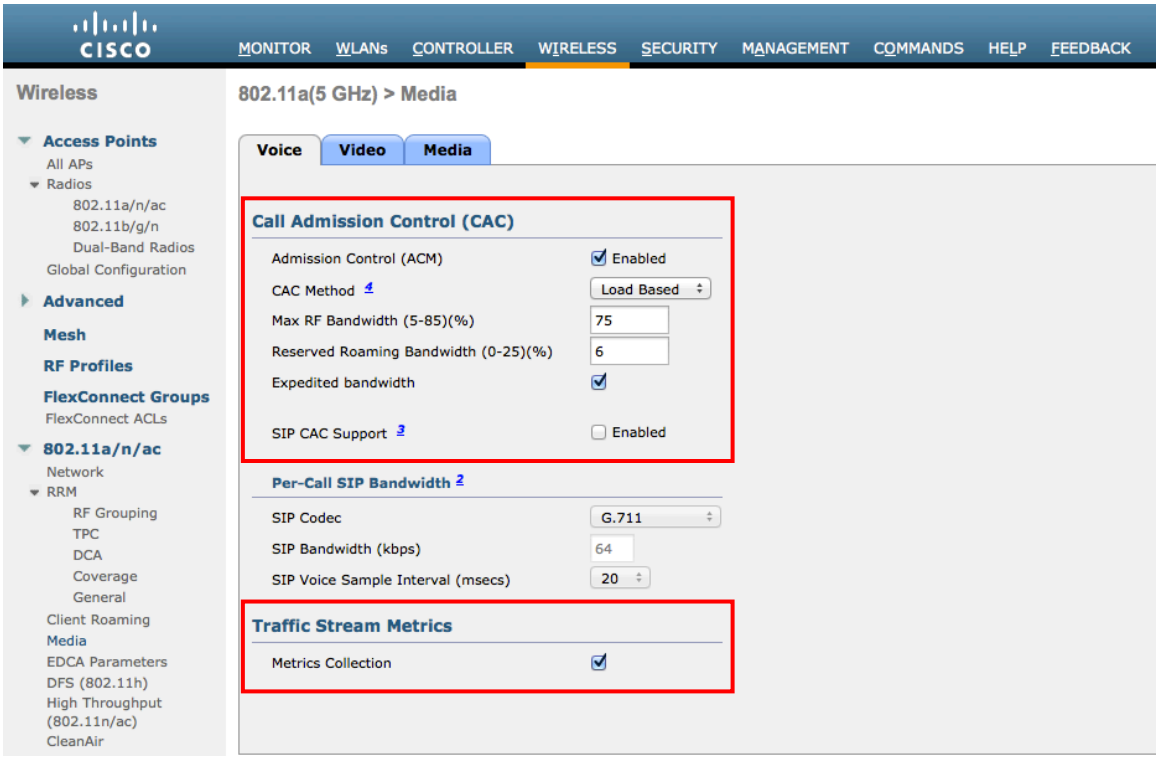
ロード ベース CAC を SIP CAC と使用し、すべてのチャネル 802.11 トラフィックとチャネルのエネルギーを考量して利用可能な帯域幅が設定されます。

クライアントが SIP 通信で TCP と UDP のどちらを使用するかによって、SIP CAC を使用する場合に、アクセス ポイントではコール アドミッション制御のためのさまざまな方法が使用されます。

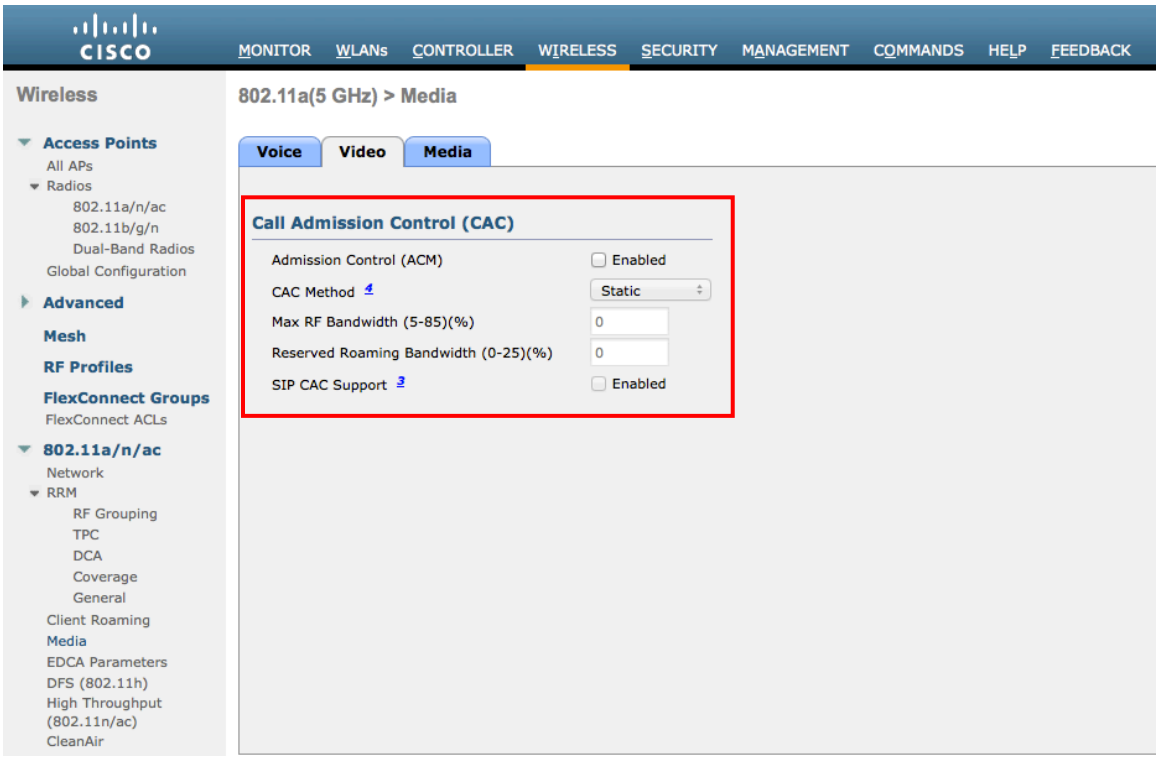
クライアントが SIP で TCP を使用している場合、アクセス ポイントはメディア セッションのスヌーピングが WLAN で有効な場合は SIP パケットをスヌーピングし、新しい音声ストリームに使用可能な帯域幅がない場合は SIP フレームをアップストリームまたはダウンストリームに転送しません。これは、Cisco Unified Communications Manager への登録の失敗が発生する可能性があります。

クライアントが SIP に UDP を使用している場合、アクセス ポイントは WLAN でメディア セッション スヌーピングが有効な場合、SIP パケットをスヌーピングし、486 ビジー メッセージをクライアントに送信します。このメッセージは「**ネットワークがビジーです（Network Busy）**」メッセージとして解釈され、クライアントが別のアクセス ポイントにローミングするか、またはそのセッションのコール セットアップを終了させます。

Cisco DX シリーズは SIP で TCP を使用しているため、別のコールを割り当てられない場合にチャネルがビジーである場合、Cisco DX シリーズの Cisco Unified Communications Manager への登録が失われる可能性があります。



[ビデオ（Video）] で [アドミッション制御必須（Admission Control Mandatory）] を無効にする必要があります。有効になっている場合は、ビデオ フレームの優先順位がベスト エフォートまで下げられます。



音声のコール アドミッション制御を有効にした場合は、次の設定を有効にする必要があります。この設定は、「**show run-config**」で表示できます。

```
Call Admission Control (CAC) configuration
Voice AC - Admission control (ACM)..... Enabled
Voice max RF bandwidth..... 75
Voice reserved roaming bandwidth..... 6
Voice load-based CAC mode..... Enabled
Voice tspec inactivity timeout..... Disabled
Video AC - Admission control (ACM)..... Disabled
Voice Stream-Size..... 84000
Voice Max-Streams..... 2
Video max RF bandwidth..... 25
Video reserved roaming bandwidth..... 6
```

voice stream-size および voice max-streams の値は、必要に応じて次のコマンドを使用して調整できます。

```
（Cisco Controller）>config 802.11a cac voice stream-size 84000 max-streams 2
```

WLAN 設定で QoS が正しくセットアップされていることを確認します。この設定は、次のコマンドを使用して表示できます。

```
（Cisco Controller）>show wlan <WLAN id>
```

```
Quality of Service..... Platinum (voice)
WMM..... Allowed
Dot11-Phone Mode (7920)..... ap-cac-limit
Wired Protocol..... 802.1P (Tag=5)
```

Cisco Autonomous Access Point でコール アドミッション制御を有効にした場合は、SSID でもアドミッションのブロックを解除する必要があります。

Cisco Autonomous Access Point には、負荷ベースの CAC と複数ストリームのサポートは存在しないので、Cisco Autonomous Access Point で CAC を有効にすることは推奨されません。

Cisco Autonomous Access Point は、1 ストリームのみに対応しており、ストリーム サイズはカスタマイズできないので、CAC が有効である場合に SRTP および barge（割り込み）は機能しません。

```
dot11 ssid voice
   vlan 21
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa cckm
   admit-traffic
```

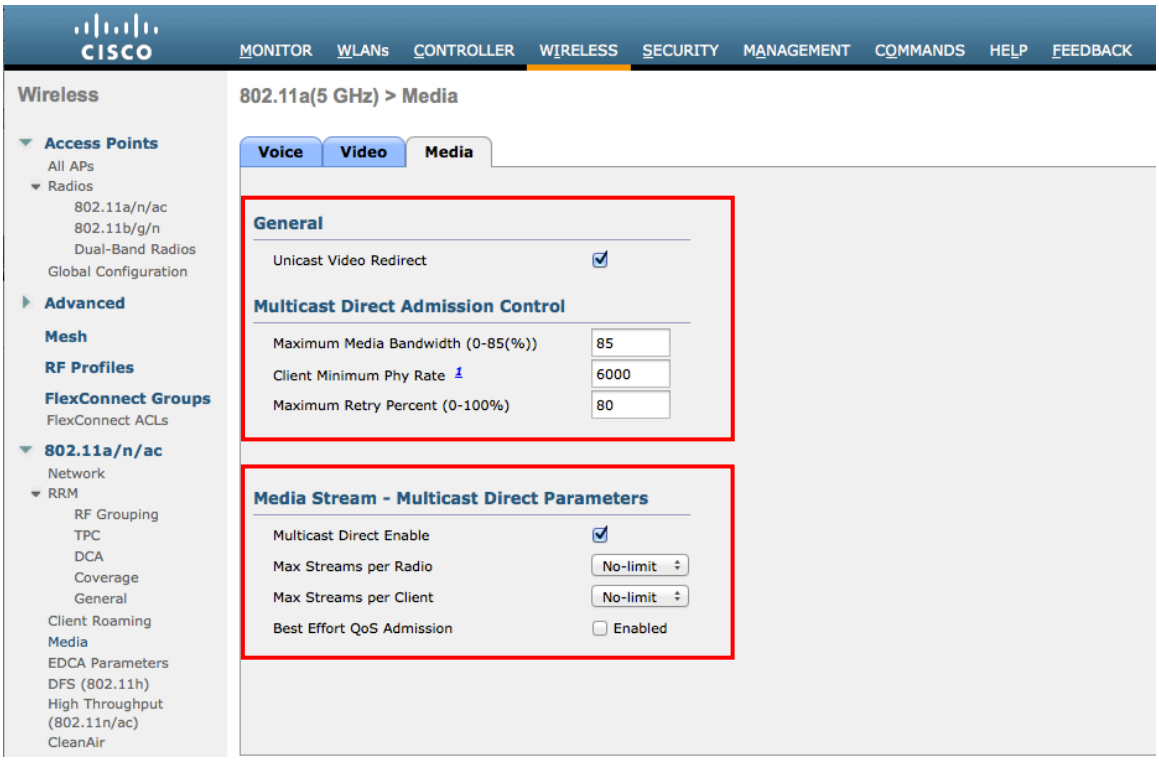
デフォルト値を使用することをお勧めします。この場合、5.5、6、11、12、および 24 Mbps が 802.11b/g 用の公称レートとして有効になり、6、12、および 24 Mbps が 802.11a 用として有効になり、6.5、13、および 26 Mbps が 802.11n 用として有効になります。

STREAM 機能を直接有効にするか、QoS の設定画面の無線アクセス カテゴリで [音声の最適化（Optimized Voice）] を選択することによって有効にする場合、音声パケットだけが音声キューに入っていることを確認します。シグナリング パケット（SIP）は、別個のキューに入れる必要があります。これを確実にするには、DSCP を適切なキューにマッピングする QoS ポリシーを設定します。

コール アドミッション制御と QoS の詳細については、次の URL にある『Cisco IOS Software Configuration Guide for Cisco Aironet Access Points』の「**Configuring QoS**」の章を参照してください。

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA.html

メディアの設定では、[**ユニキャスト ビデオ リダイレクト（Unicast Video Redirect）**] および [**マルチキャスト ダイレクトの有効化（Multicast Direct Enable）**] を有効にする必要があります。



EDCA パラメータ

使用する帯域に応じて 5 GHz または 2.4 GHz に対し、EDCA プロファイルを [**音声およびビデオの最適化（Voice and Video Optimized）**] に設定し、[**低遅延 MAC を有効にする（Enable Low Latency MAC）**] を無効にします。

低遅延 MAC（LLM）を設定すると、アクセス ポイント プラットフォームによって 1 パケットあたりの再送信回数が 2 ～ 3 回に減るので、複数のデータ レートが有効である場合に問題が生じるおそれがあります。

Cisco 802.11n アクセス ポイントでは、LLM はサポートされていません。

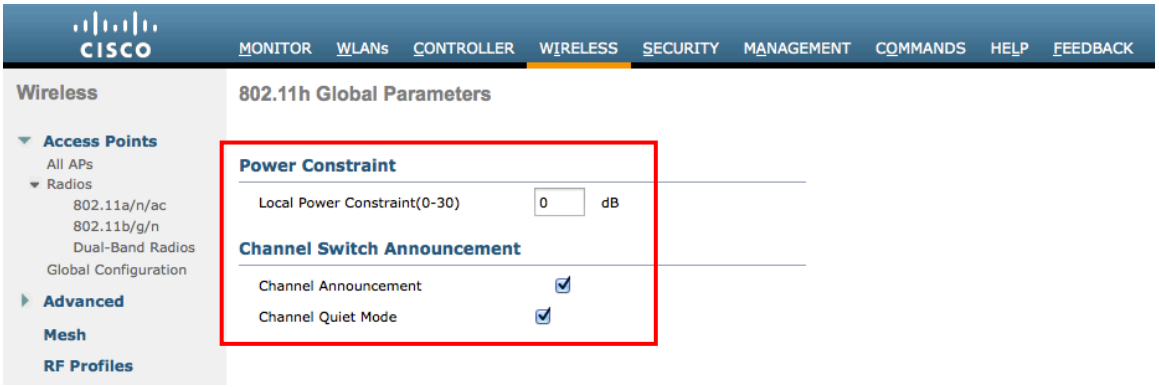
DFS（802.11h）

DFS（802.11h）の設定では、チャネル通知と Quiet モードを有効にします。

Cisco DX シリーズでは、送信電力の制御に DTPC が使用されるため、[**電力制限（Power Constraint）**] は未設定のままにするか、0 dBm に設定します。

Cisco Unified Wireless LAN Controller の最近のバージョンでは、TPC（電力制限）とダイナミック送信電力コントロール（DTPC）の両方を同時に有効にすることはできません。

[**チャネル通知（Channel Announcement）**] および [**チャネル Quiet モード（Channel Quiet Mode）**] を有効にする必要があります。



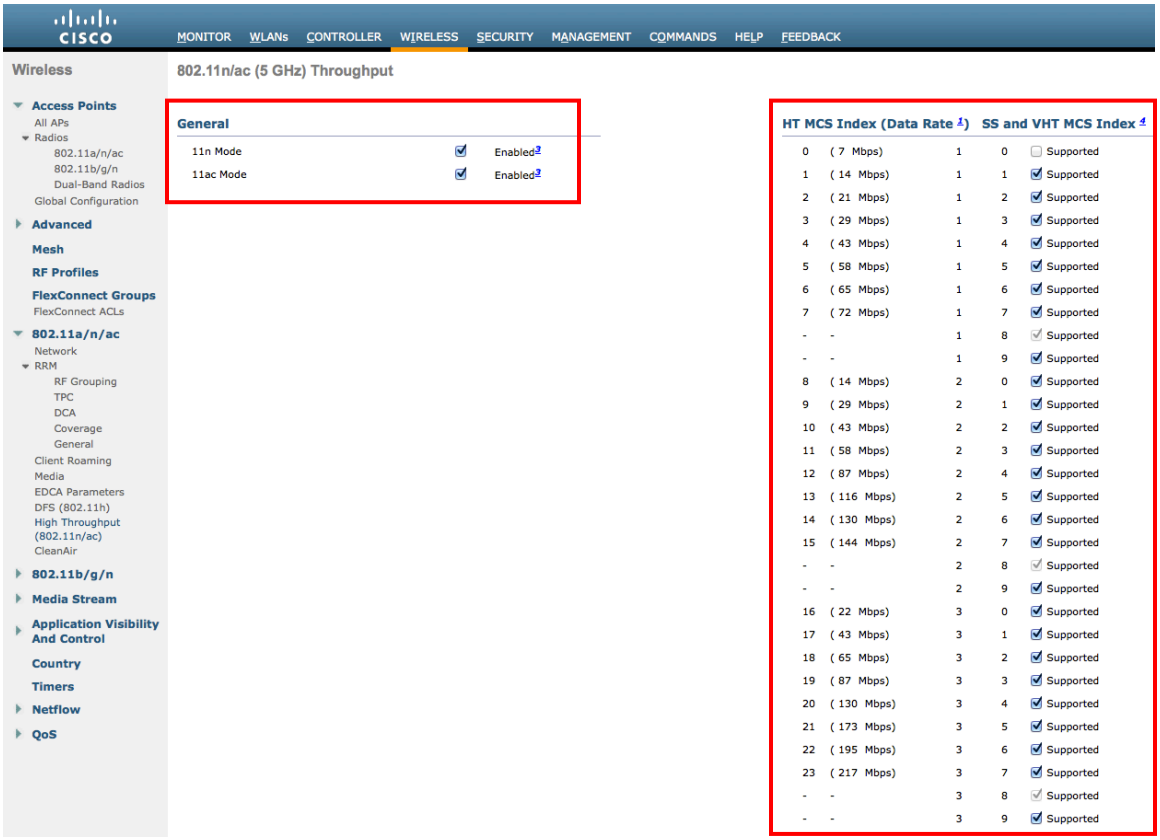
高スループット（802.11n）

802.11n データ レートは無線（2.4 GHz および 5 GHz）ごとに設定できます。

WMM が有効化されており **WPA2（AES）**が、802.11n データ レートを使用するように設定されていることを確認します。

Cisco DX シリーズは MCS 0 ～ MCS 7 データ レートのみをサポートしていますが、それより高い MCS レートは、MIMO アンテナ テクノロジーを含む同じ帯域周波数を使用している他の 802.11 クライアントが存在する場合にオプションで有効にすることで利用できるようになります。

MCS 0 を無効にすることを推奨します。



フレームの集約

フレームの集約は複数の MAC プロトコル データ ユニット（MPDU）または MAC サービス データ ユニット（MSDU）を一緒にパッケージングして、順スループットと容量が最適になる点でオーバーヘッドを低減するためのプロセスです。
MAC プロトコル データ ユニット（A-MPDU）の集約にはブロックの確認応答を使用する必要があります。

Cisco DX シリーズの使用体験を最適化するために、A-MPDU と A-MSDU の設定を次のように調整することをお勧めします。

A-MPDU
ユーザ プライオリティ 0、3、4、5 = イネーブル
ユーザ プライオリティ 1、2、6、7 = ディセーブル

A-MSDU
ユーザ プライオリティ 1、2 = イネーブル
ユーザ プライオリティ 0、3、4、5、6、7 = ディセーブル

Cisco Unified Wireless LAN Controller の 7.0.116.0 リリースでは、デフォルト A-MPDU および A-MSDU の設定は、次のとおりです。

A-MPDU
ユーザ プライオリティ 0、4、5 = イネーブル
ユーザ プライオリティ 1、2、3、6、7 = ディセーブル

A-MSDU
ユーザ プライオリティ 0、1、2、3、4、5 = イネーブル
ユーザ プライオリティ 6、7 = ディセーブル

Cisco DX シリーズの推奨事項に基づいて A-MPDU と A-MSDU の設定を構成するには、次のコマンドを使用します。

5 GHz の設定を設定するには、802.11a ネットワークを最初に無効にし、変更が完了したら再び有効にする必要があります。

```
config 802.11a 11nSupport a-mpdu tx priority 0 enable
config 802.11a 11nSupport a-mpdu tx priority 3 enable
config 802.11a 11nSupport a-mpdu tx priority 4 enable
config 802.11a 11nSupport a-mpdu tx priority 5 enable
config 802.11a 11nSupport a-mpdu tx priority 1 disable
config 802.11a 11nSupport a-mpdu tx priority 2 disable
config 802.11a 11nSupport a-mpdu tx priority 6 disable
config 802.11a 11nSupport a-mpdu tx priority 7 disable
config 802.11a 11nSupport a-msdu tx priority 1 enable
config 802.11a 11nSupport a-msdu tx priority 2 enable
config 802.11a 11nSupport a-msdu tx priority 0 disable
config 802.11a 11nSupport a-msdu tx priority 3 disable
config 802.11a 11nSupport a-msdu tx priority 4 disable
config 802.11a 11nSupport a-msdu tx priority 5 disable
config 802.11a 11nSupport a-msdu tx priority 6 disable
config 802.11a 11nSupport a-msdu tx priority 7 disable
```

2.4 GHz の設定を設定するには、802.11b/g ネットワークを最初に無効にし、変更が完了したら再び有効にする必要があります。

```
config 802.11b 11nSupport a-mpdu tx priority 0 enable
config 802.11b 11nSupport a-mpdu tx priority 3 enable
config 802.11b 11nSupport a-mpdu tx priority 4 enable
config 802.11b 11nSupport a-mpdu tx priority 5 enable
config 802.11b 11nSupport a-mpdu tx priority 1 disable
config 802.11b 11nSupport a-mpdu tx priority 2 disable
config 802.11b 11nSupport a-mpdu tx priority 6 disable
config 802.11b 11nSupport a-mpdu tx priority 7 disable
config 802.11b 11nSupport a-msdu tx priority 1 enable
config 802.11b 11nSupport a-msdu tx priority 2 enable
config 802.11b 11nSupport a-msdu tx priority 0 disable
config 802.11b 11nSupport a-msdu tx priority 3 disable
config 802.11b 11nSupport a-msdu tx priority 4 disable
config 802.11b 11nSupport a-msdu tx priority 5 disable
config 802.11b 11nSupport a-msdu tx priority 6 disable
config 802.11b 11nSupport a-msdu tx priority 7 disable
```

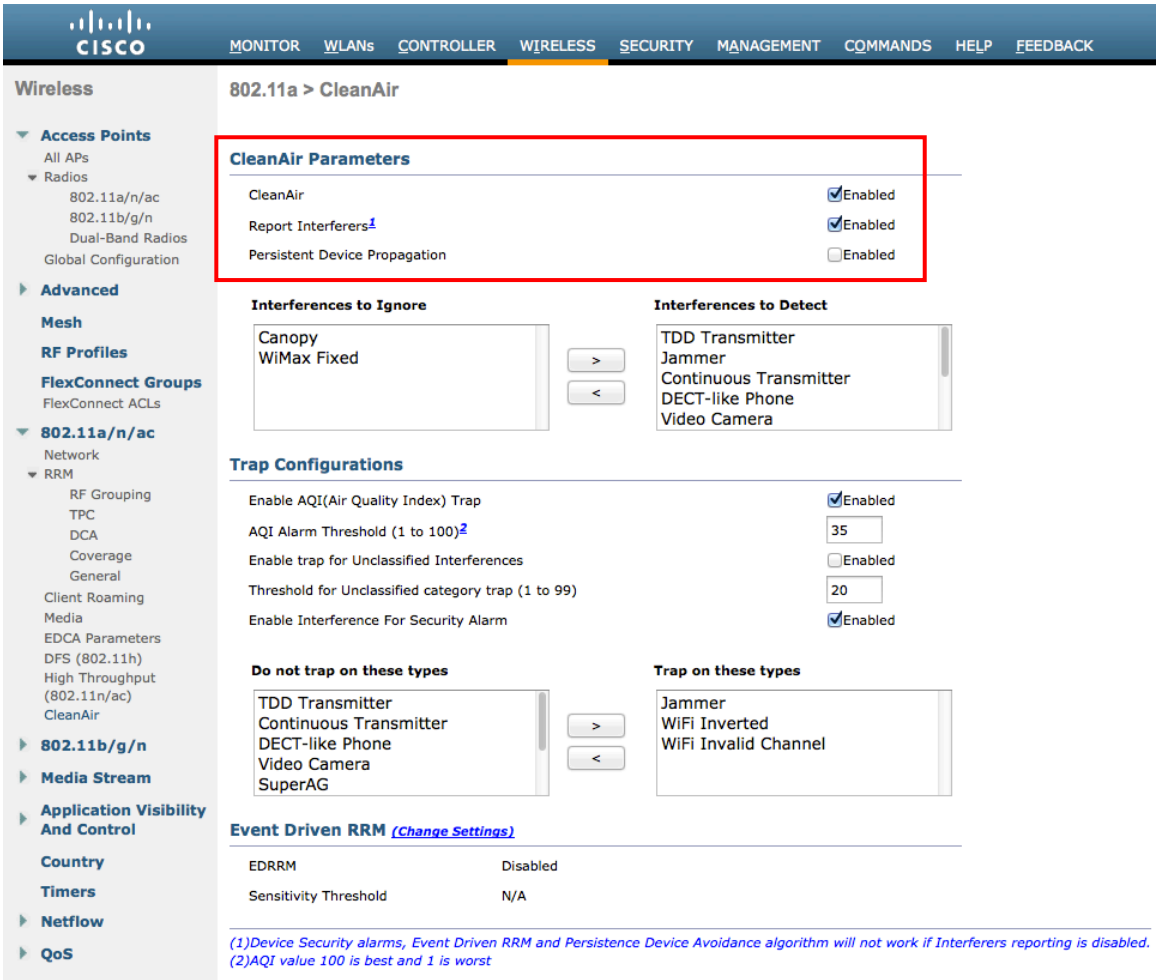
A-MPDU と A-MSDU と現在の設定を表示するには、5 GHz の場合は show 802.11a、2.4 GHz の場合は show 802.11b を入力します。

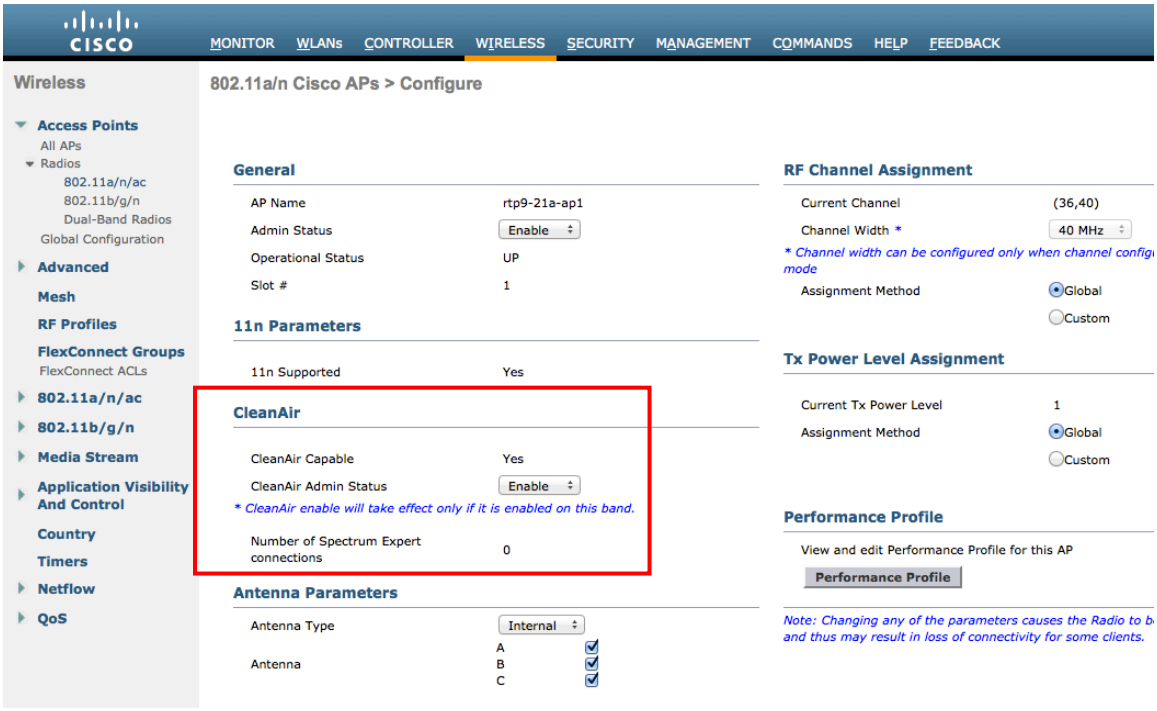
```
802.11n Status:
  A-MPDU Tx:
    Priority 0..... Enabled
    Priority 1..... Disabled
    Priority 2..... Disabled
    Priority 3..... Enabled
    Priority 4..... Enabled
    Priority 5..... Enabled
```

Priority 6..... Disabled
Priority 7..... Disabled
A-MSDU Tx:
Priority 0..... Disabled
Priority 1..... Enabled
Priority 2..... Enabled
Priority 3..... Disabled
Priority 4..... Disabled
Priority 5..... Disabled
Priority 6..... Disabled
Priority 7..... Disabled

CleanAir

CleanAir テクノロジーを搭載したシスコ製のアクセス ポイントを使用して既存の干渉を検出する場合は、[**CleanAir**] を [**有効（Enabled）**] にする必要があります。

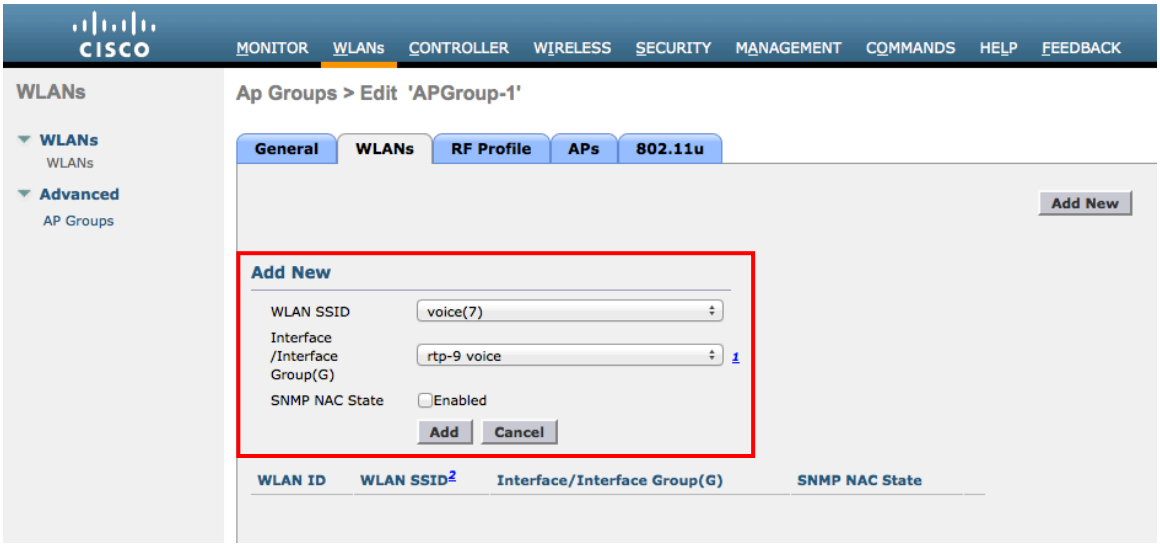




AP グループ

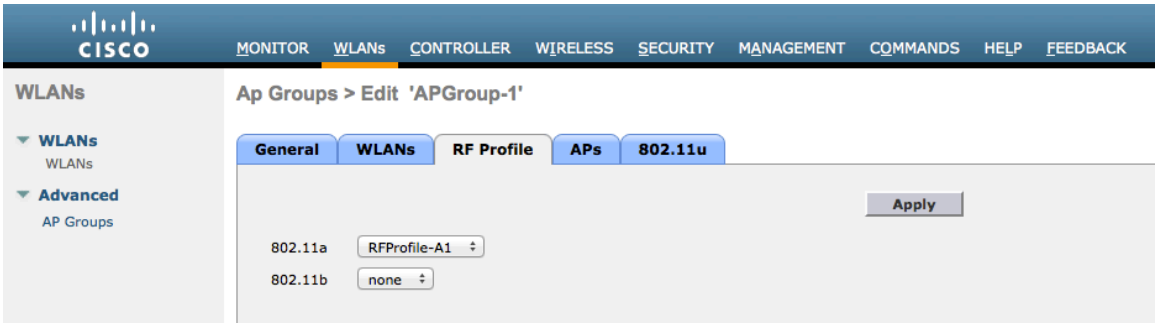
AP グループは、有効にする WLAN/SSID、マッピングする必要があるインターフェイスのほか、AP グループに割り当てられたアクセス ポイントに使用する必要がある RF プロファイル パラメータを指定するために作成できます。

[**WLANs**] タブでは、目的の SSID およびマッピングするインターフェイスを選択して、[**追加（Add）**] を押します。



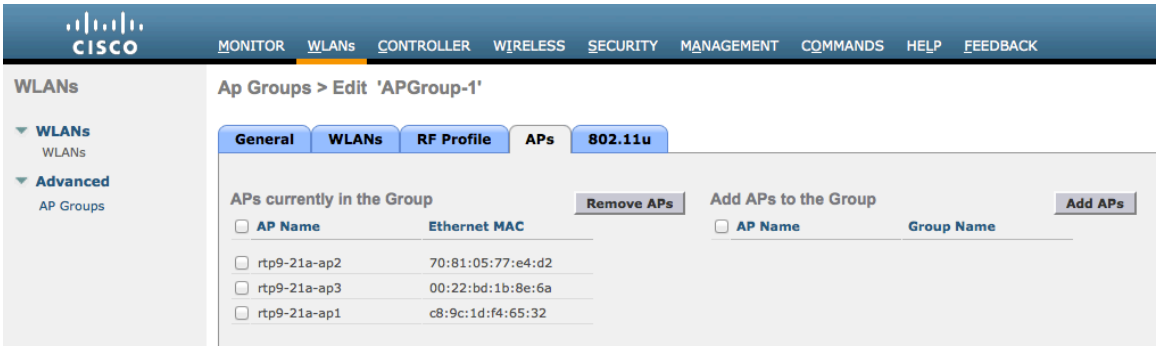
[**RF プロファイル（RF Profile）**] タブでは、目的の 802.11a または 802.11b RF プロファイルを選択して、[**適用（Apply）**] を押します。

アクセス ポイントが AP グループに結合されてから変更が加えられた場合、変更の適用後、アクセス ポイントがリブートします。



[**APs**] タブでは、目的のアクセス ポイントを選択して、[**AP の追加（Add APs）**] を押します。

その後、選択したアクセス ポイントがリブートします。



RF プロファイル

RF プロファイルは、アクセス ポイントのグループが使用する必要がある周波数帯域、データ レート、RRM 設定などを指定するために作成できます。

Cisco DX シリーズで使用される SSID を 5 GHz 無線にのみ適用できるようにすることを強くお勧めします。

作成された RF プロファイルは、AP グループに適用されます。AP グループ設定の詳細については、「AP グループ」を参照してください。

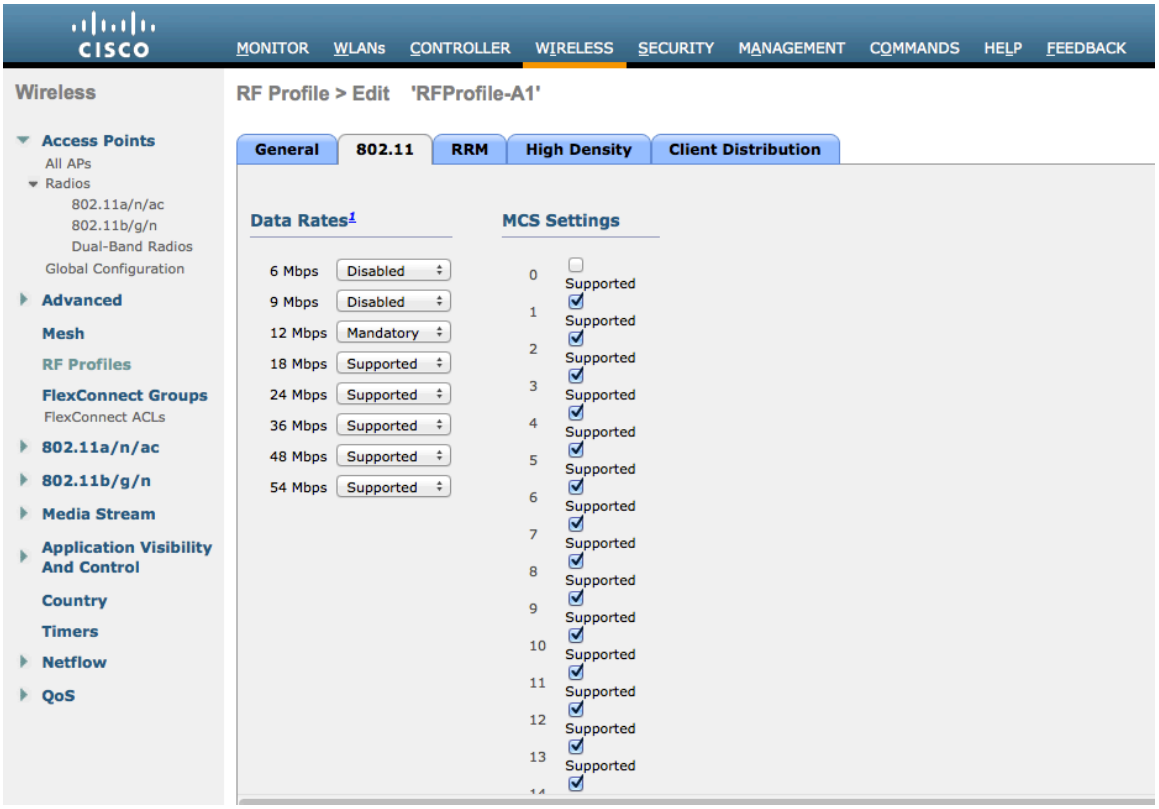
RF プロファイルを作成する場合、[**RF プロファイル名（RF Profile Name）**] と [**無線ポリシー（Radio Policy）**] を定義する必要があります。

[**無線ポリシー（Radio Policy）**] に対して、802.11a または 802.11b/g を選択します。

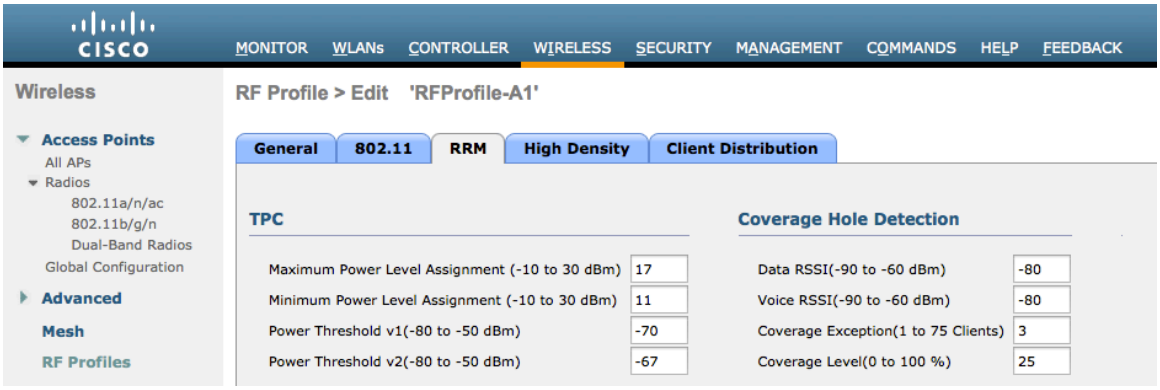
[**802.11**] タブでは、目的のデータ レートを設定します。

[**必須（Mandatory）**] として 12 Mbps を、[**サポート済み（Supported）**] として 18 Mbps 以上を有効にすることをお勧めします。ただし、環境によっては、必須（基本）レートとして 6 Mbps を有効にする必要がある場合があります。

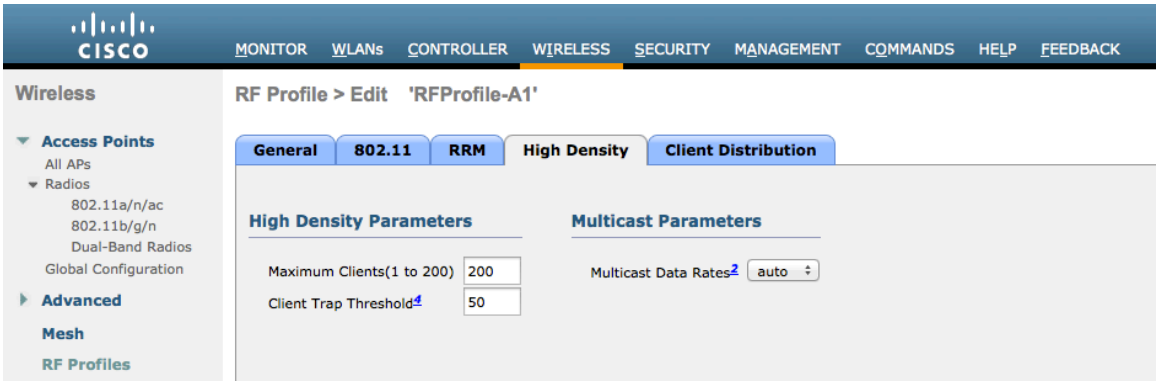
MCS 0 は 6 MbPS が有効でない場合、無効にする必要があります。



[RRM] タブで、[**最大電力レベルの割り当て（Maximum Power Level Assignment）**] および [**最小電力レベルの割り当て（Minimum Power Level Assignment）**] のほか、他の [**TPC**] および [**カバレッジ ホールの検出（Coverage Hole Detection）**] を設定できます。



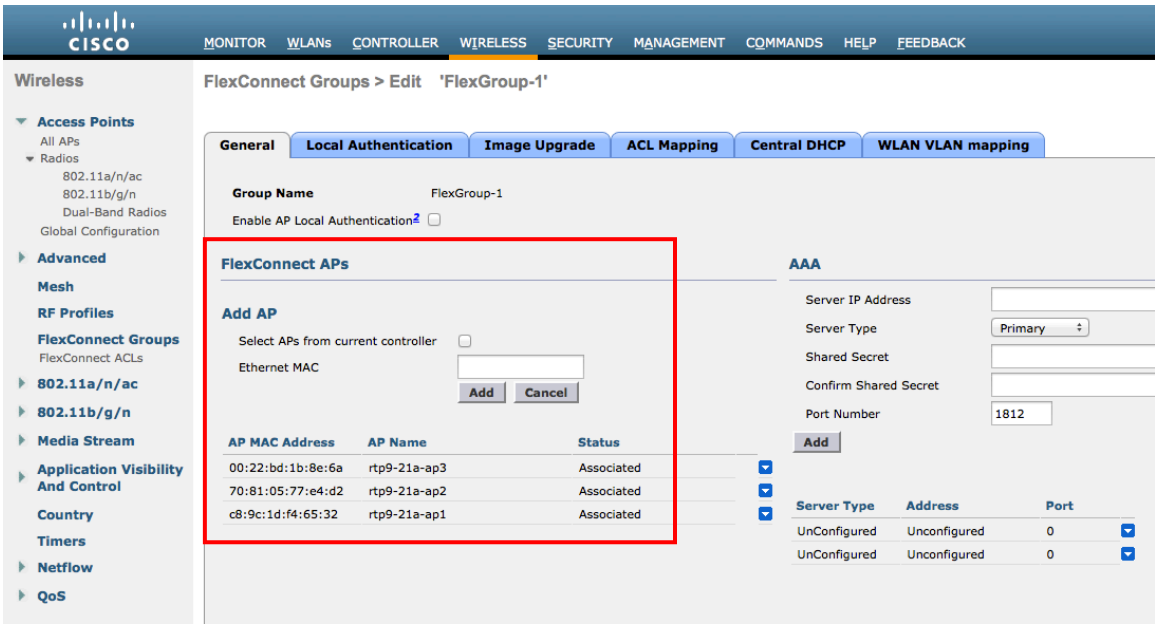
[高密度（High Density）] タブでは、[最大クライアント数（Maximum Clients）] および [マルチキャスト データ レート（Multicast Data Rates）] を設定することもできます。



FlexConnect グループ

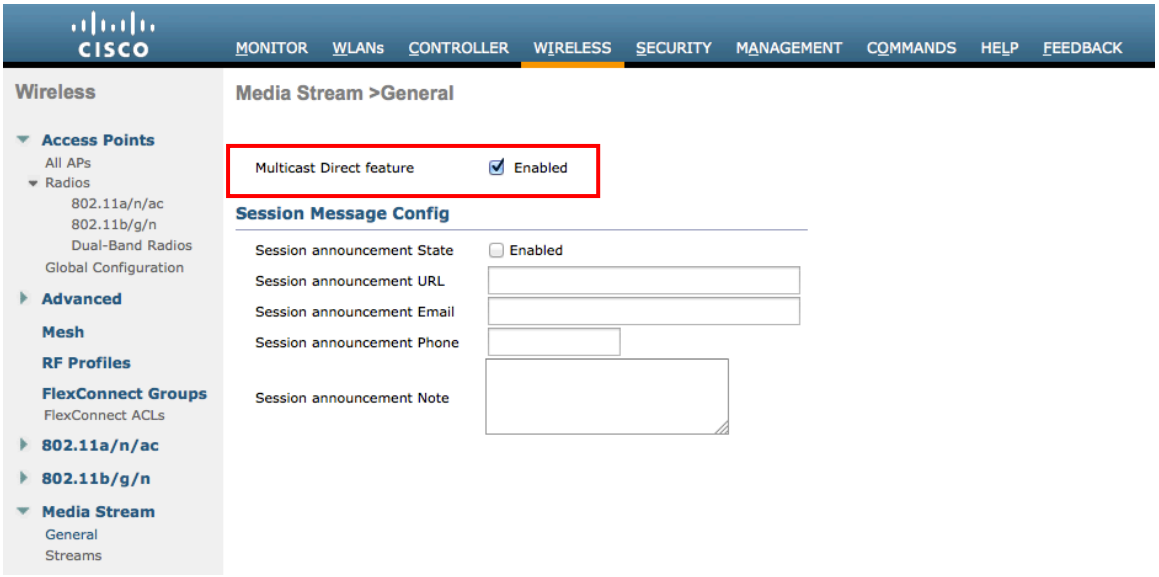
FlexConnect モード用に設定されたすべてのアクセス ポイントを FlexConnect グループに追加する必要があります。

CCKM を使用している場合は、同じ FlexConnect グループ内のアクセス ポイントにローミングするときにのみシームレスなローミングを実行できます。

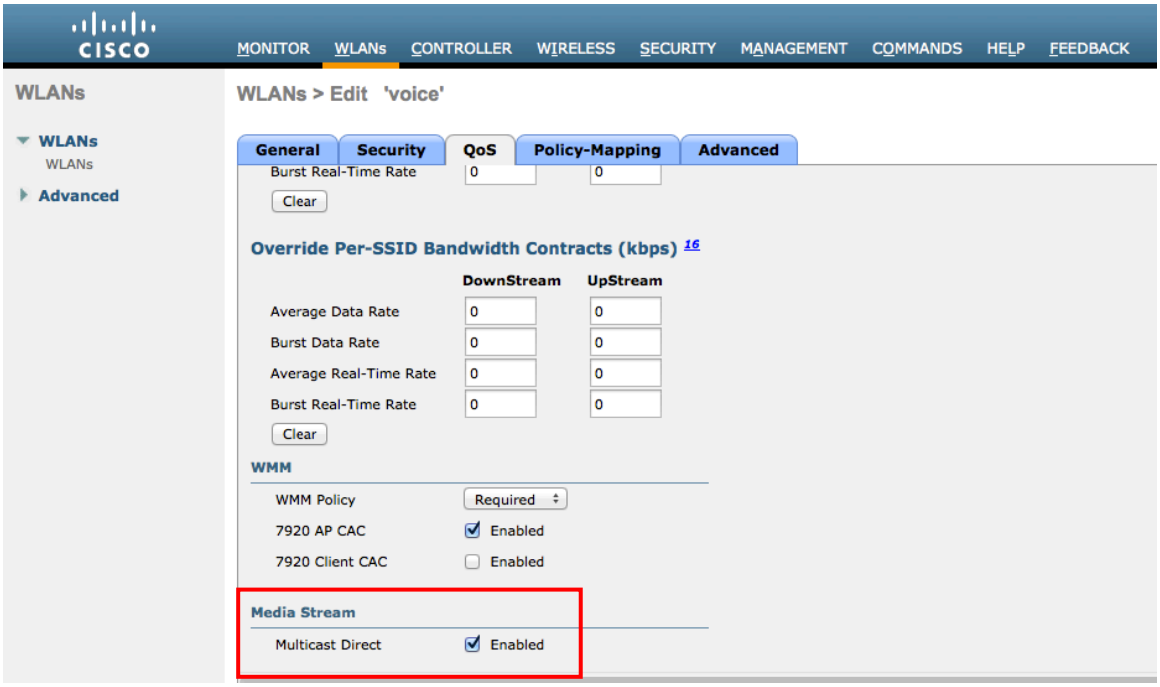


マルチキャスト ダイレクト

メディア ストリームの設定で、[マルチキャスト ダイレクト機能（Multicast Direct Feature）] を有効にする必要があります。



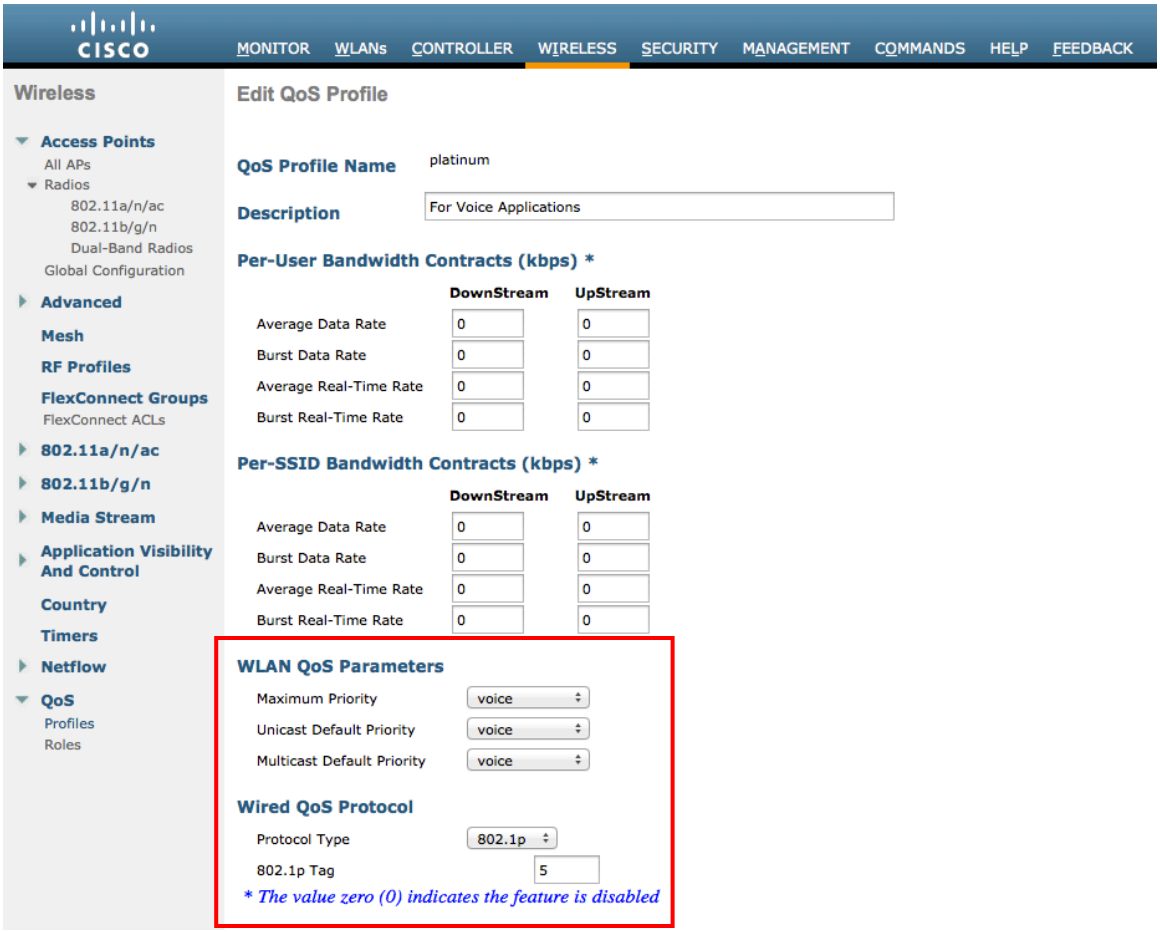
[**マルチキャスト ダイレクト機能（Multicast Direct Feature）**] を有効にすると、WLAN 設定の **Multicast Direct** を有効化するオプションが [QoS] メニューに表示されます。

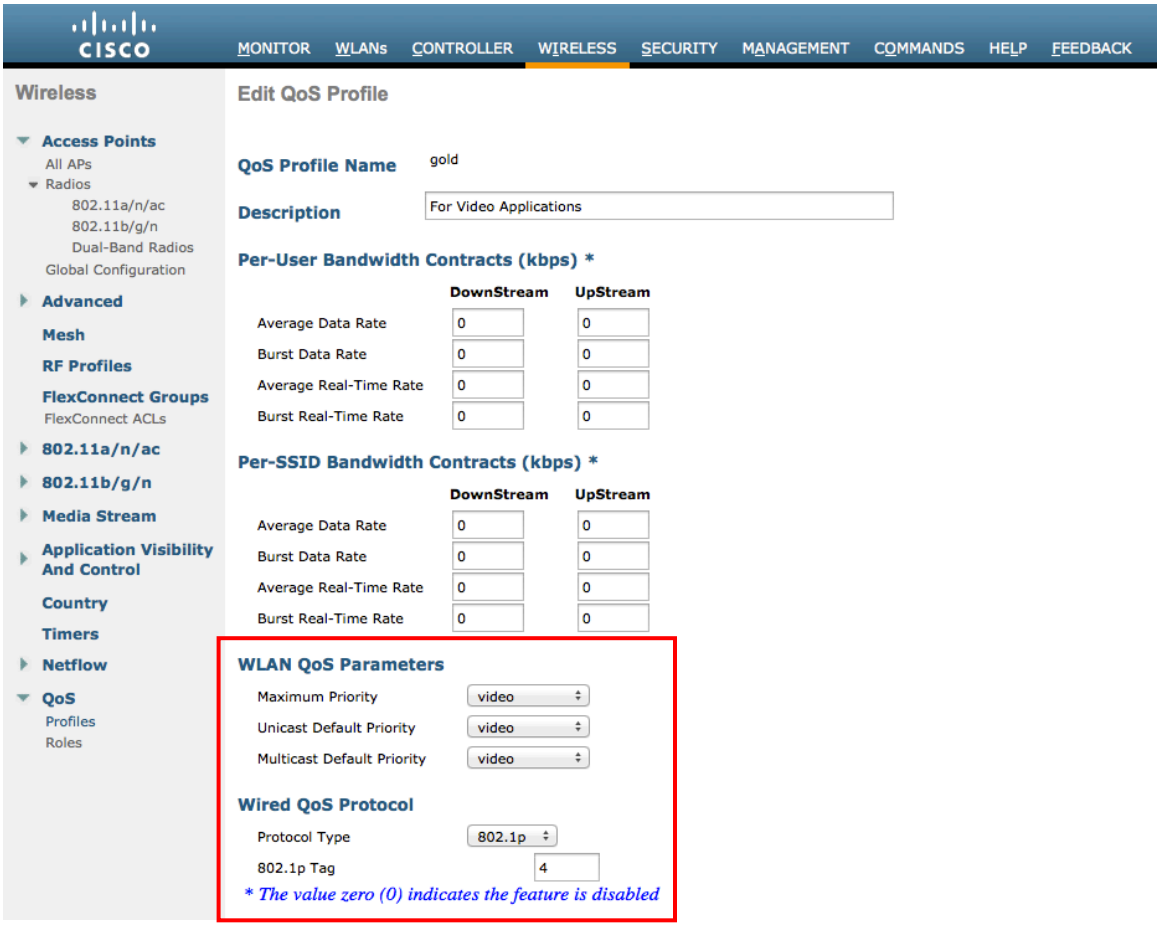


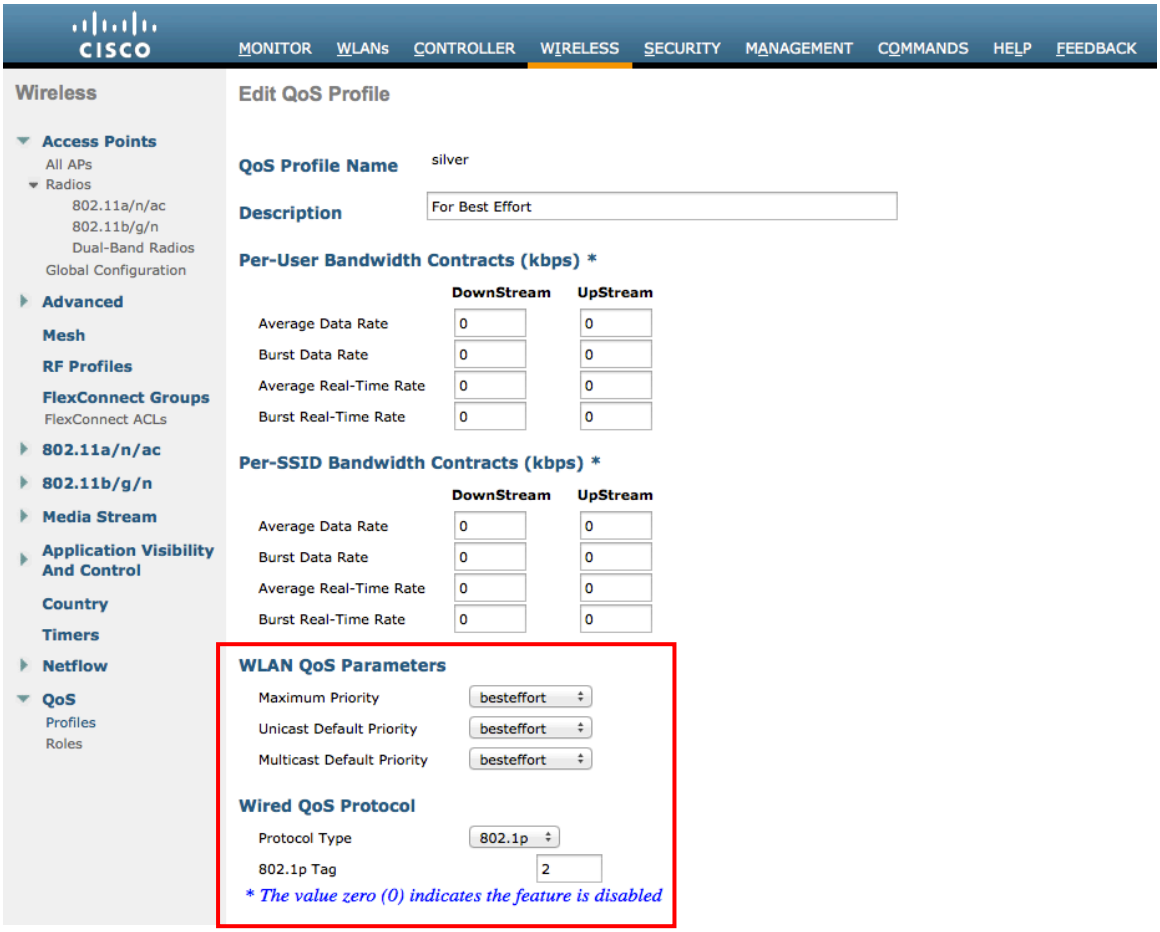
QoS プロファイル

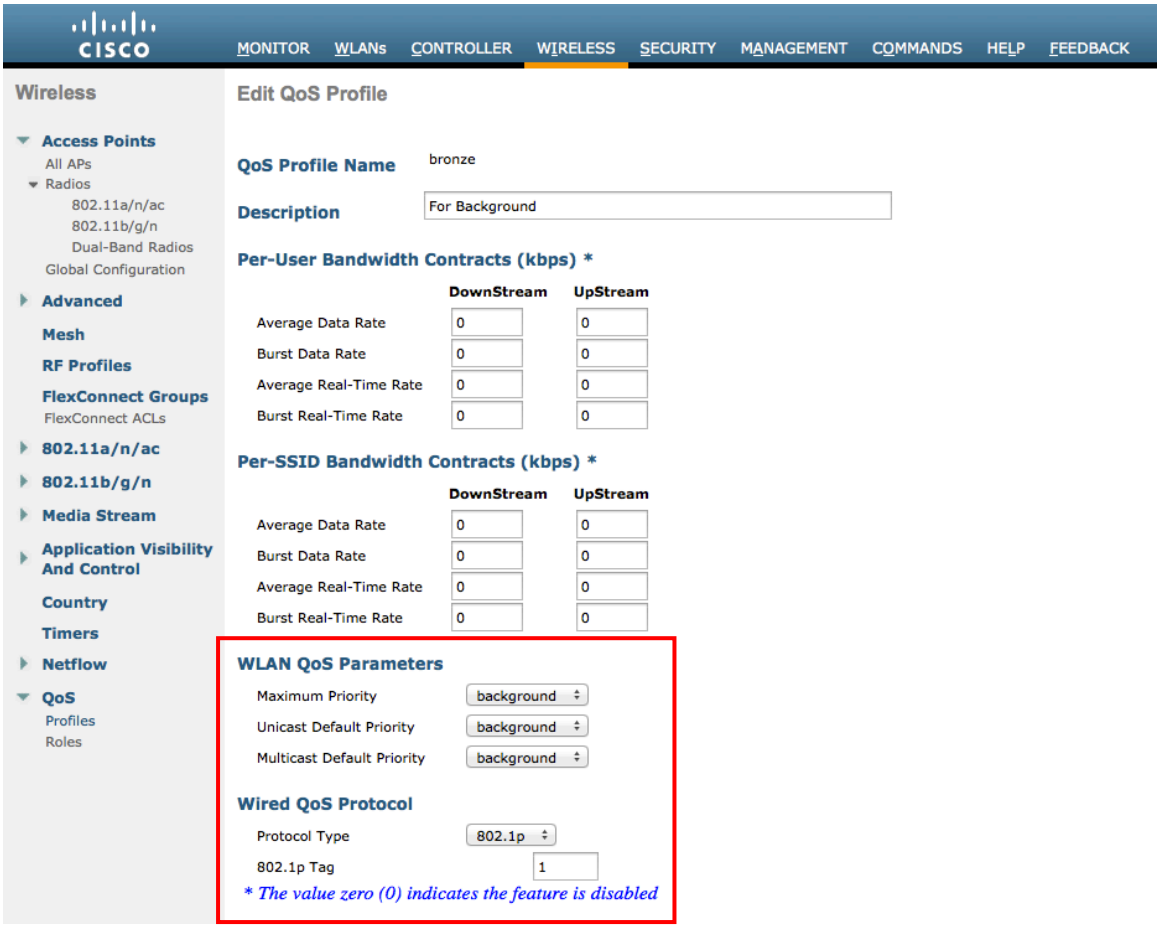
プロトコル タイプとして [**802.1p**] を選択することで、4 つの QoS プロファイル（Platinum、Gold、Silver、Bronze）を設定し、プロファイルごとに、[**802.1p タグ（802.1p Tag）**] を設定します。

- Platinum = 5
- Gold = 4
- Silver = 2
- Bronze = 1




MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
Profiles
Roles
Edit QoS Profile
QoS Profile Name
gold
Description
For Video Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
video
Unicast Default Priority
Multicast Default Priority
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
4
* The value zero (0) indicates the feature is disabled


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
Profiles
Roles
Edit QoS Profile
QoS Profile Name
silver
Description
For Best Effort
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
besteffort
Unicast Default Priority
Multicast Default Priority
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
2
* The value zero (0) indicates the feature is disabled



(注) 7.5.102.0 リリースで 802.1p タグ マッピングが変更されました。

7.5.102.0 リリースより前は、Platinum = 6、Gold = 5、Silver = 3、Bronze = 1 でした。

QoS Basic Service Set（QBSS）

Cisco DX シリーズがサポートする QoS Basic Service Set（QBSS）には、3 つのバージョンがあります。

シスコが最初に提供したバージョンは 0 ～ 100 のスケールで、クリア チャネル アセスメント（CCA）には基づいていないため、チャネル使用率は計上されず、個々のアクセス ポイントの無線を送信する 802.11 トラフィックだけが計上されます。そのため、同じ周波数を使用する他の 802.11 エネルギーまたは干渉は計上されません。最大しきい値はクライアント側で定義され、45 に設定されます。

QBSS は 802.11e にも含まれており、0 ～ 255 のスケールで、CCA に基づいています。そのため、チャネルの使用状況を正確に表すことができます。最大しきい値はクライアント側で定義され、105 に設定されます。

Cisco DX シリーズは QBSS をパーセント形式（0 ～ 255 を 0 ～ 100% に）変換します。近接リスト メニューに、チャネル使用率の値として表示されます。

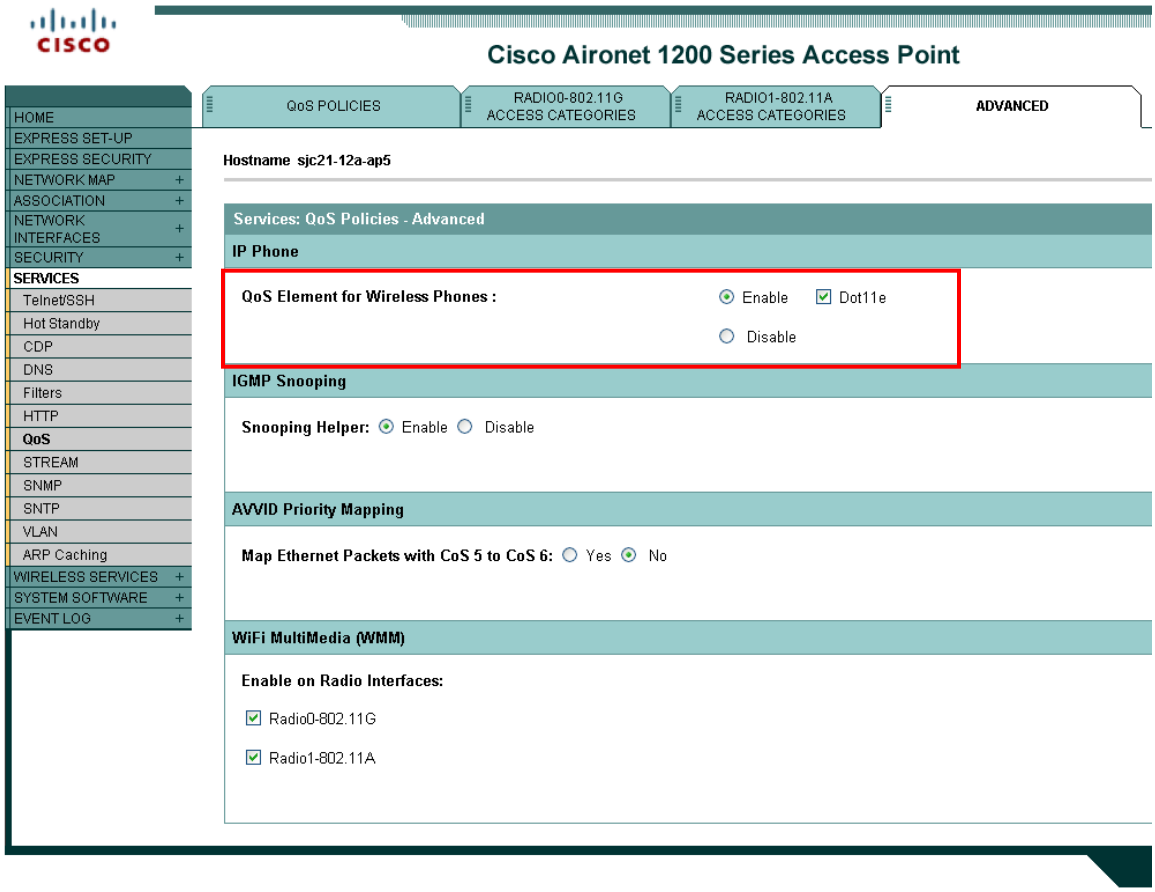
シスコが提供する 2 番めのバージョンは 802.11e バージョンに基づいていますが、デフォルトの最大しきい値 105 を任意で設定できます。

QBSS の各バージョンは、アクセス ポイントに対して任意で設定できます。

Cisco Unified Wireless LAN Controller に対して WMM を有効にすると、802.11e バージョンの QBSS が有効になります。また、[**7920 クライアント CAC（7920 Client CAC）**] オプションと [**7920 AP CAC**] オプションも用意されており、[**7920 クライアント CAC（7920 Client CAC）**] を選択するとシスコのバージョン 1 が有効になり、[**7920 AP CAC**] を選択するとシスコのバージョン 2 が有効になります。詳細については、「WLAN QoS の設定」を参照してください。

Cisco Autonomous Access Point では、「**dot11 phone**」または「**dot11 phone dot11e**」によって QBSS が有効になります。

「**dot11 phone**」を使用すると、2 つのシスコ バージョンが有効になり、「**dot11 phone dot11e**」を使用すると、両方の CCA バージョン（802.11e およびシスコ バージョン 2）が有効になります。「**dot11 phone dot11e**」を有効にすることを推奨します。



CCKM タイムスタンプの許容値

デフォルトの CCKM タイムスタンプ許容値は 1000 ミリ秒に設定されます。

Cisco DX シリーズのローミング エクスペリエンスを最適化するために、CCKM タイムスタンプ許容値を 5000 ミリ秒に調整することをお勧めします。

```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?
<tolerance> Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msecs
```

シスコの推奨事項に従って CCKM タイムスタンプの許容値を設定するには、次のコマンドを使用します。

（Cisco Controller）>config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >

変更を確認するには、**show wlan <WLAN id>** を入力します。これにより、次のように表示されます。

CCKM tsf Tolerance..... **5000**

Auto-Immune

Auto-Immune（自己免疫）機能は、サービス拒否（DoS）攻撃に対する保護のために任意選択で有効にできます。

この機能を有効にしても、Voice over Wireless LAN によって中断が引き起こされる可能性があります。そのため、Cisco Unified Wireless LAN Controller で Auto-Immune 機能を無効にすることを推奨します。

Cisco Unified Wireless LAN Controller に対する Auto-Immune 設定を表示するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

（Cisco Controller）>show wps summary

Auto-Immune
Auto-Immune..... **Disabled**

Client Exclusion Policy
Excessive 802.11-association failures..... Enabled
Excessive 802.11-authentication failures..... Enabled
Excessive 802.1x-authentication..... Enabled
IP-theft..... Enabled
Excessive Web authentication failure..... Enabled

Signature Policy
Signature Processing..... Enabled

Cisco Unified Wireless LAN Controller に対する Auto-Immune 機能を無効にするには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

（Cisco Controller）>config wps auto-immune disable

WLAN コントローラの高度な EAP 設定

Cisco Unified Wireless LAN Controller の高度な EAP 設定が、次の情報に従って設定されていることを確認する必要があります。

Cisco Unified Wireless LAN Controller に対する EAP 設定を表示するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

```
(Cisco Controller) >show advanced eap
EAP-Identity-Request Timeout (seconds)..... 30
EAP-Identity-Request Max Retries..... 2
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 30
EAP-Request Max Retries..... 2
EAPOL-Key Timeout (milliseconds)..... 400
EAPOL-Key Max Retries..... 4
```

802.1x または WPA/WPA2 を使用する場合、Cisco Unified Wireless LAN Controller の EAP-Request Timeout を少なくとも 20 秒に設定する必要があります。

Cisco Unified Wireless LAN Controller ソフトウェアの最近のバージョンでは、デフォルトの EAP-Request Timeout が 2 ～ 30 秒に変更されました。

Cisco Unified Wireless LAN Controller に対する EAP-Request Timeout を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

```
(Cisco Controller) >config advanced eap request-timeout 30
```

WPA/WPA2 PSK を使用する場合は、EAPOL-Key Timeout をデフォルトの 1000 ミリ秒から 400 ミリ秒に減らし、EAPOL-Key Max Retries をデフォルトの 2 から 4 に設定することを推奨します。

WPA/WPA2 を使用する場合は、EAPOL-Key Timeout および EAPOL-Key Max Retries のデフォルト値（それぞれ 1000 ミリ秒および 2）を使用しても正しく動作しますが、それぞれ 400 および 4 に設定することを推奨します。

EAPOL-Key Timeout は、1 秒（1000 ミリ秒）を超えないようにしてください。

Cisco Unified Wireless LAN Controller に対する EAPOL-Key Timeout を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

```
(Cisco Controller) >config advanced eap eapol-key-timeout 400
```

Cisco Unified Wireless LAN Controller に対する EAPOL-Key Max Retries Timeout を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

```
(Cisco Controller) >config advanced eap eapol-key-retries 4
```

TKIP カウンターメジャー ホールドオフ時間

TKIP カウンターメジャー モードは、アクセス ポイントが 60 秒以内にメッセージ整合性チェック（MIC）エラーを 2 回受信すると開始されます。このモードが開始されると、アクセス ポイントはその 802.11 無線に関連付けられたすべての TKIP クライアントの認証を解除し、カウンターメジャー ホールドオフ時間（デフォルトは 60 秒）の間、クライアントをホールドオフにします。

Cisco Unified Wireless LAN Controller に対する TKIP カウンターメジャー ホールドオフ時間を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

（Cisco Controller）>config wlan security tkip hold-down <nseconds> <WLAN id>

変更を確認するには、**show wlan <WLAN id>** を入力します。これにより、次のように表示されます。

Tkip MIC Countermeasure Hold-down Timer..... 60

Cisco Autonomous Access Point に対して、TKIP カウンターメジャー イベントが発生した場合にクライアントをホールドオフにする秒数を入力します。

Interface dot11radio X
countermeasure tkip hold-time <nseconds>

VLAN および Cisco Autonomous Access Point

ワイヤレス音声およびデータを別個の VLAN にセグメント化します。

ワイヤレス クライアントのサブネットは 1,000 ホストを超えてはなりません。

Cisco Autonomous Access Point を使用する場合は、専用のネイティブ VLAN を使用します。Cisco Autonomous Access Point では、マルチキャスト プロトコルである Inter-Access Point Protocol（IAPP）が使用されます。

ネイティブ VLAN については、IAPP パケットが正常に交換されることを確実にするために、VLAN 1 は使用しないことを推奨します。

音声 VLAN に対して、パブリック セキュア パケット フォワーディング（PSPF）が有効になっている場合、クライアントが同じアクセス ポイントに関連付けられたときに直接通信できないため、PSPF が無効になっていることを確認します。PSPF を有効にすると、オーディオは無方向となります。

ポート セキュリティは、Cisco Autonomous Access Point が直接接続しているスイッチ ポートで無効にする必要があります。

レイヤ 3 モビリティが有効であり、Wireless LAN Services Module（WLSM）が展開されている場合に限り、Cisco Autonomous Access Point の SSID 設定でネットワーク ID を無効にします。

Cisco DX シリーズの設定

Cisco DX シリーズ上で Wi-Fi 設定を構成するには、キー パッドとタッチ スクリーンを使用して、**[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [Wi-Fi 設定（Wi-Fi settings）]** に移動します。

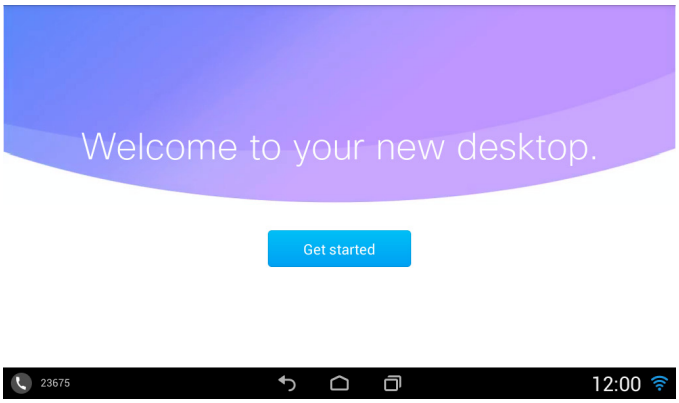
Cisco DX シリーズをワイヤレス LAN モードに対して有効にするには、電源が必要です。

セットアップ アシスタント

Cisco DX シリーズの電源を初めてオンにすると、ユーザのセットアップ プロセスを誘導するセットアップ アシスタントが起動します。

設定プロセスを開始するサービスを選択します。

- WebEx
- Jabber
- ボイスメール
- E メール
- 連絡先
- カレンダー

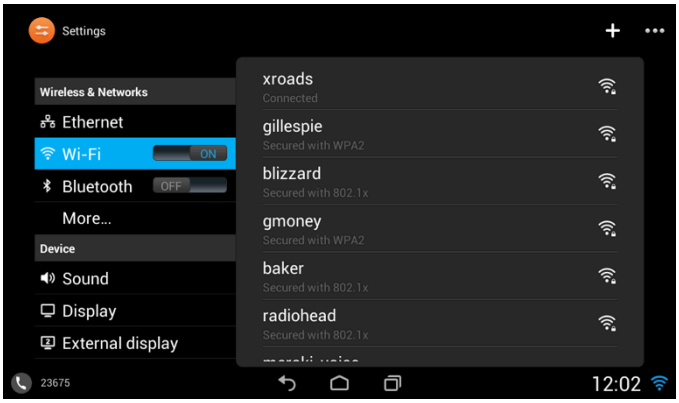


ワイヤレス LAN の設定

無線 LAN のプロファイルを設定するには、次のガイドラインを使用します。

- **[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [Wi-Fi]** に移動します。
- **[Wi-Fi]** が **[オン（On）]** に設定されていることを確認します。

  Wi-Fi が Cisco Unified Communications Manager で有効になっていることを確認します。そうでない場合はオプションが設定メニューに表示されません。
  アクティブなイーサネット接続がある場合、**[Wi-Fi]** は無効になり、**[Wi-Fi]** を有効にする前に、イーサネットを切断する必要があります。
- ブロードキャストされた Wi-Fi ネットワークをリストから選択するか、または Wi-Fi ネットワークを手動で追加します。
- Wi-Fi ネットワークを手動で追加する場合、[ネットワークを追加（Add network）] を選択し、**SSID** を入力します（大文字と小文字が区別されます）。

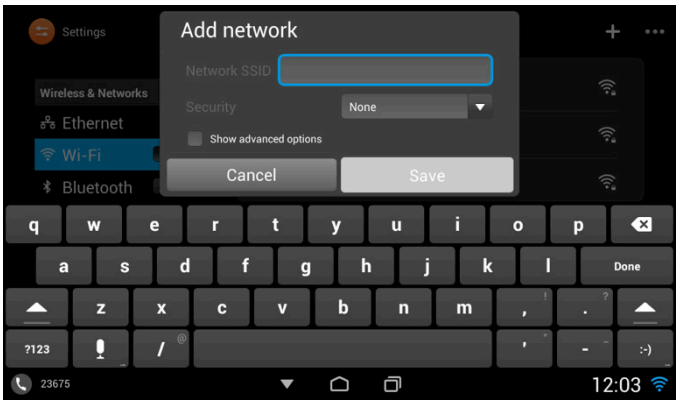


- 次に、サポートされる利用可能なセキュリティ モードと、各モードで使用できるキー管理および暗号化タイプを示します。

  キー管理および暗号化タイプ（暗号化方式）は、アクセス ポイントの現在の設定に基づいて自動設定されます。有効になっている最も強力なキー管理タイプ（WPA2 など）がまず優先され、次に有効になっている最も強力な暗号化方式（AES など）が優先されます。

セキュリティ モード（Security Mode）	802.1x タイプ（802.1x Type）	キー管理（Key Management）	暗号化（Encryption）
なし	該当なし	なし	なし
WEP	該当なし	静的	WEP（40/64 または 104/128 ビット）
WPA/WPA2 PSK	該当なし	WPA-PSK、WPA2-PSK	TKIP、AES
802.1x EAP	EAP-FAST、PEAP-MSCHAPv2、PEAP-GTC、TLS	WPA、WPA2	TKIP、AES

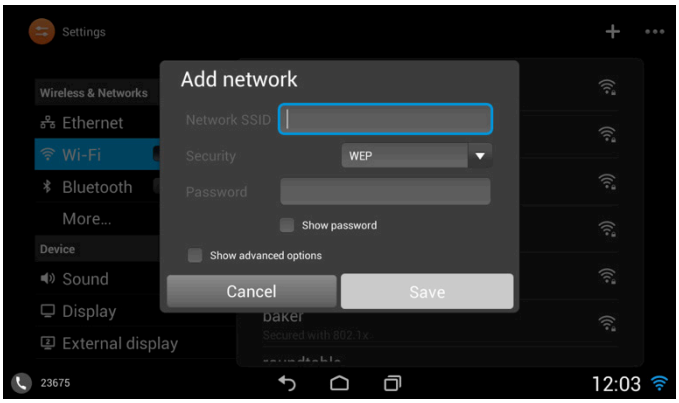
- セキュリティなし（オープン セキュリティ）でワイヤレス ネットワーク プロファイルを設定する場合は、[SSID] を入力し、[セキュリティ タイプ（Security Type）] に [**なし（None）**] を選択します。



- **WEP** セキュリティ モードは、静的 WEP キー（パスワード）を入力する必要があります。

  キー インデックス 1 のみがサポートされます。したがって、キー インデックス 1 だけがアクセス ポイントに設定されていることを確認することができます。

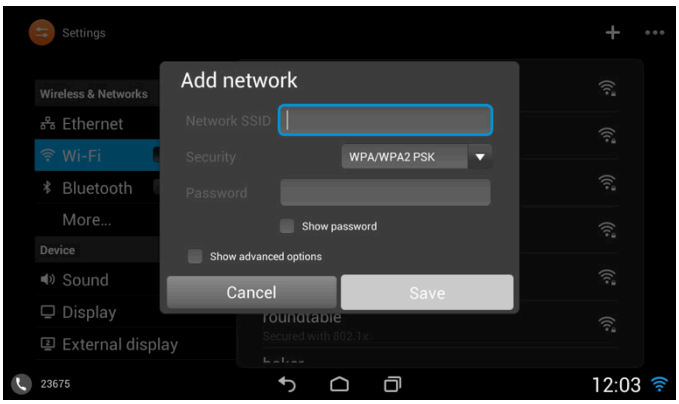
キー スタイル	キー サイズ	文字
ASCII	40/64 ビット	5
ASCII	104/128 ビット	13
16 進数	40/64 ビット	10（0 ～ 9、A ～ F）
16 進数	104/128 ビット	26（0 ～ 9、A ～ F）



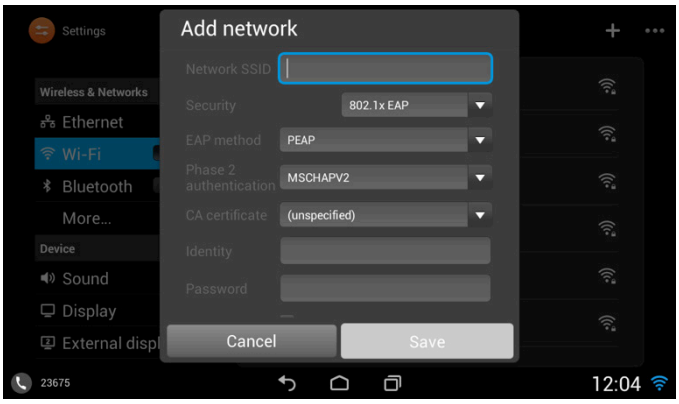
- **[WPA/WPA2 PSK]** をセキュリティ モードとして選択する場合、事前共有キー（パスワード）を設定する必要があります。

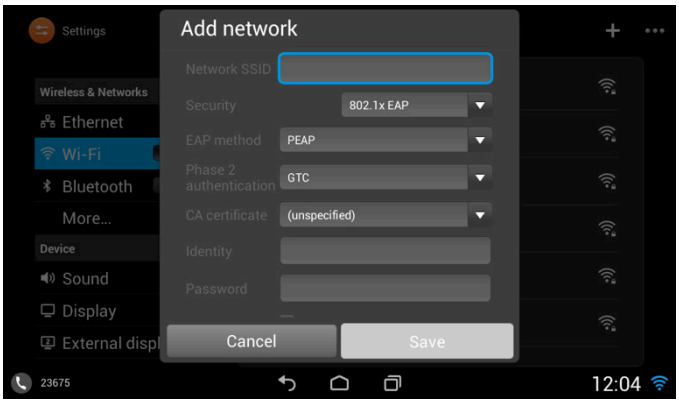
  ASCII または 16 進数形式のパスワードを入力します。

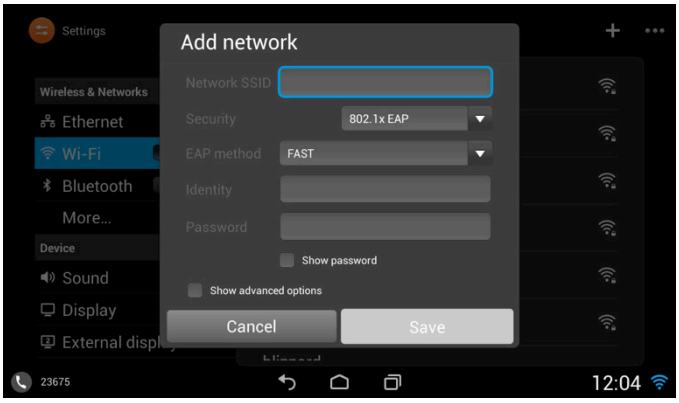
キー スタイル	文字
ASCII	8 ～ 63
16 進数	64（0 ～ 9、A ～ F）

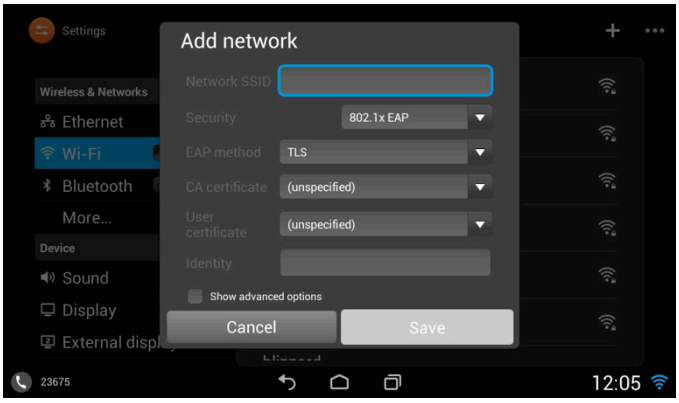


- **[802.1x EAP]** をセキュリティ モードとして選択した場合、EAP-FAST（FAST）または PEAP を使用している場合はユーザ名（ID）とパスワードを設定する必要があります。
- [PEAP] を選択する場合は、フェーズ 2 の認証タイプ（MSCHAPv2 や GTC）を指定する必要があります。
- サーバ検証で PEAP を使用する場合、CA 証明書をオプションでインポートおよび設定できます。
- EAP-TLS（TLS）を使用する場合は、ユーザ証明書と CA 証明書がインポートされ、設定する必要があります。

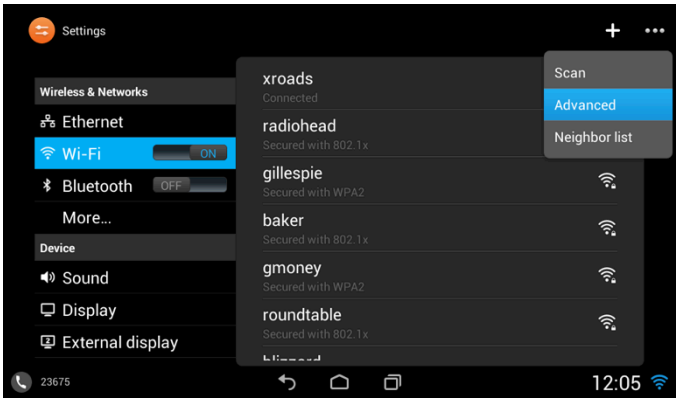


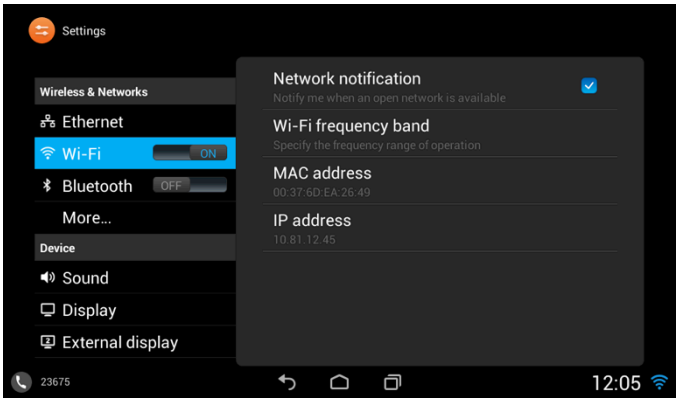






- 使用する周波数帯域をセットするには、**[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [Wi-Fi] > [詳細設定（Advanced）]** で **[Wi-Fi の周波数帯（Wi-Fi frequency band）]** を選択します。**[詳細設定（Advanced）]** メニューを表示するには、右上にある [...] を選択します。



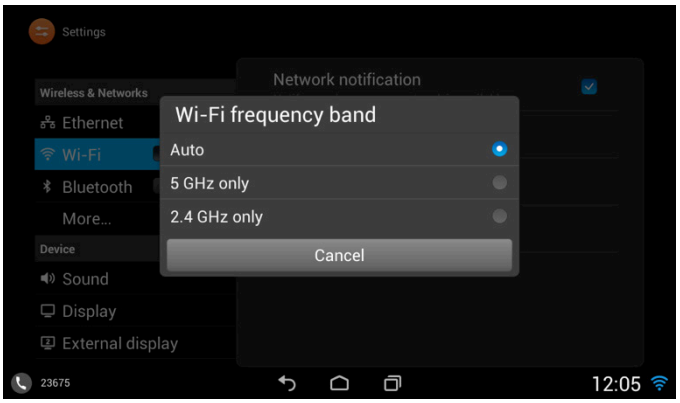


- 周波数帯域を設定するには、次の 802.11 モードの 1 つを選択します。
    - Auto
    - 5 GHz
    - 2.4 GHz

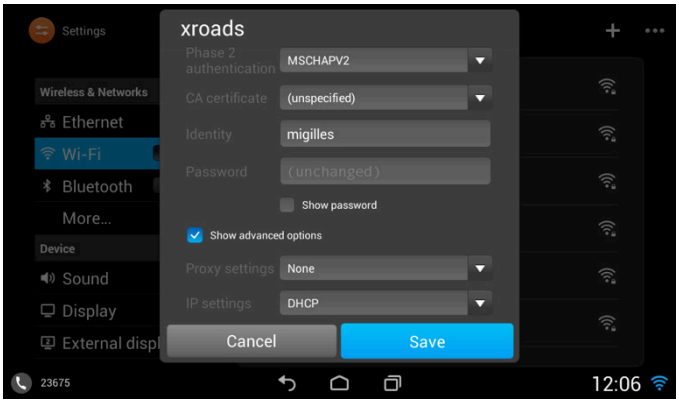
    [自動(Auto)] モードは、電源オン時または切断時に 5 GHz と 2.4 GHz の両方のチャネルをスキャンしてから、信号が強い(-67 dBm 以上)使用可能な 5 GHz アクセス ポイントへのアソシエートを試みます。そうでない場合は、RSSI が最も強い使用可能なアクセス ポイントへのアソシエートを試みます。
    [5 GHz のみ(5 GHz Only)] モードは、5 GHz チャネルだけをスキャンしてから、使用可能な 5 GHz アクセス ポイントへのアソシエートを試みます。

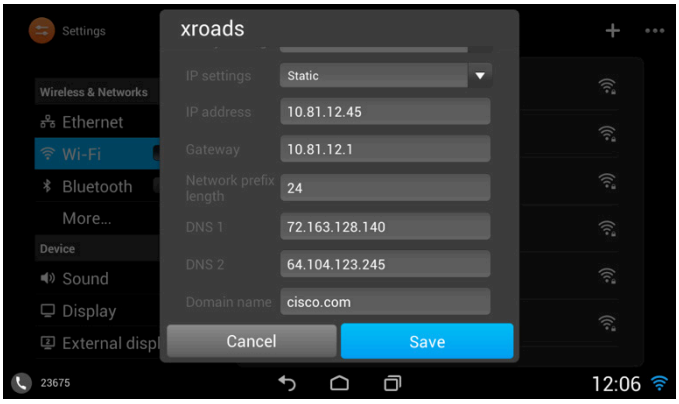
    [2.4 GHz のみ(2.4 GHz Only)] モードは、2.4 GHz チャネルだけをスキャンしてから、使用可能な 2.4 GHz アクセス ポイントへのアソシエートを試みます。

    5 GHz 周波数帯域のみを使用する場合は Cisco DX シリーズ上の周波数帯域を 5 GHz のみに設定することを強くお勧めします。そうすれば、2.4 GHz 周波数帯域へのスキャンと潜在的なローミングを回避できます。

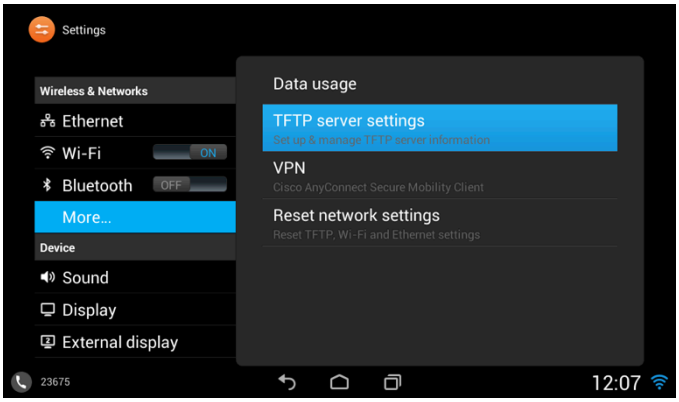


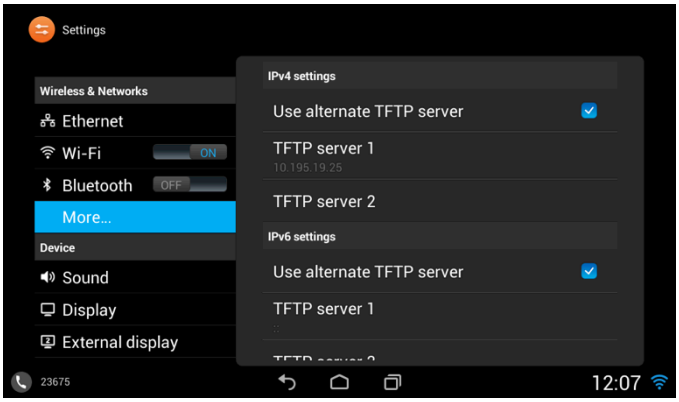
- ダイナミック ホスト コンフィギュレーション プロトコル(DHCP)またはスタティック IP 設定は、**[詳細オプションを表示(Show advanced options)]** にチェックを入れた後、無線 LAN のプロファイル設定の **[IP 設定(IP settings)]** オプションによって設定できます。



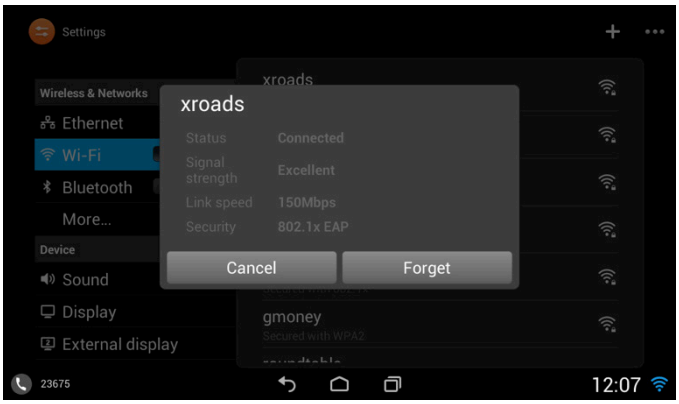


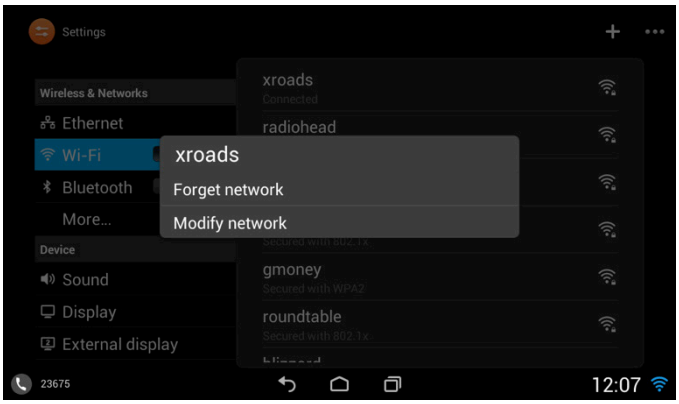
- ネットワークの DHCP スコープを使用して TFTP サーバに IP アドレスを提供するよう、DHCP オプション 150 または 66 が設定されていない場合は、**[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [詳細（More...）] > [TFTP サーバの設定（TFTP server settings）]** に移動し、[**代替 TFTP サーバの使用（Use alternate TFTP server**）] を有効にして TFTP サーバの IP アドレスを入力します。





- ネットワーク プロファイルは、選択したワイヤレス LAN をタップして [**切断（Forget）**] を選択するか、もしくは、無線 LAN を選択したまま [**ネットワークから切断（Forget network）**] を表示することで削除できます。
- ワイヤレス LAN プロファイル パラメータはワイヤレス LAN を選択したままにして [**ネットワークを変更（Modify network）**] を選択すると変更できます。





（注）CCKM は、EAP-FAST、EAP-TLS、または PEAP を使用するときに、アクセス ポイントで有効な場合ネゴシエーションされます。

WEP128 は Cisco Unified Wireless LAN Controller では WEP104 として一覧表示されます。

共有キー認証および 802.1x + 動的 WEP はサポートされません。

Cisco DX シリーズは、最大 8 つのワイヤレス LAN プロファイルを記憶することができます。

ネットワークを追加することができない場合は、ワイヤレス LAN プロファイルの最大数にすでに達しているかどうかを確認します。ワイヤレス LAN プロファイルの 1 個を、新しいネットワークを追加するため手動で削除する必要がある場合があります。

詳細については、次の URL にある『Cisco DX Series Administration Guide』を参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

証明書のインストール

Cisco DX シリーズは、EAP-TLS で使用可能な、または、PEAP 使用時の認証サーバ検証に使用可能な X.509 デジタル証明書をサポートしています。

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）は、TLS プロトコルを PKI と組み合わせて使用することで、認証サーバとの通信を保護しています。

TLS は、ユーザとサーバの両方の認証用およびダイナミック セッション キーの生成用に、証明書を使用する方法を提供します。

EAP-TLS は、高度なセキュリティを提供しますが、クライアント証明書の管理が必要となります。

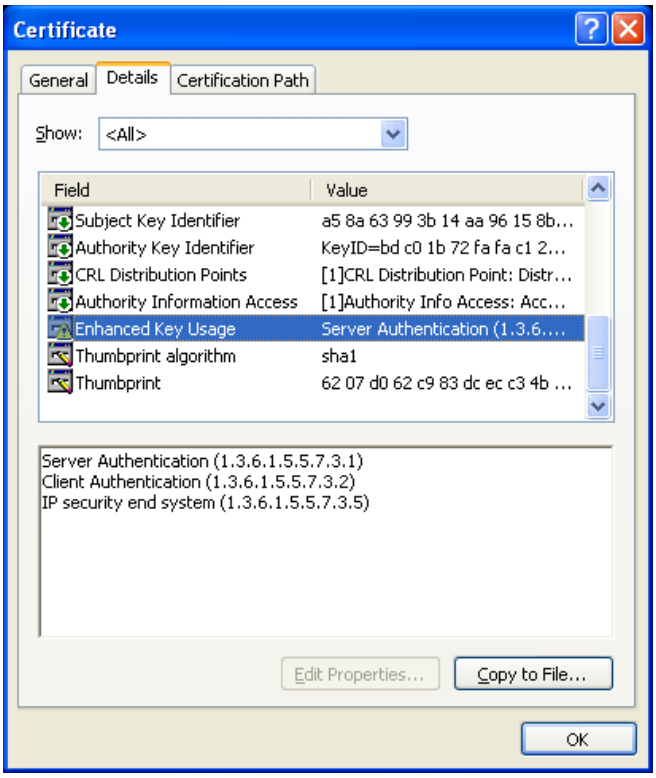
Microsoft® 認証局（CA）サーバが推奨されます（これらの CA タイプとの相互運用性しか認定されていません）。他の CA サーバ タイプは Cisco DX シリーズとの完全な相互運用性がない場合があります。

DER および Base-64 形式はクライアントおよびサーバの証明書を使用できます。

キー サイズが 1024、2048、および 4096 の証明書だけがサポートされます。

クライアントおよびサーバの証明書が SHA-1 または SHA-2 アルゴリズムのいずれかを使用して署名されていることを確認してください。SHA-3 署名アルゴリズムはサポートされていません。

ユーザ証明書詳細の [拡張キー使用（Enhanced Key Usage）] セクションの一覧にクライアント認証が表示されていることを確認します。



X.509 デジタル証明書はサーバ検証で EAP-TLS または PEAP を WLAN 認証に使用する場合にインストールする必要があります。

ユーザ証明書は、**PKCS #12** 形式（**.p12** または **.pfx** 拡張子）で、証明書および秘密キーを含む必要があります。

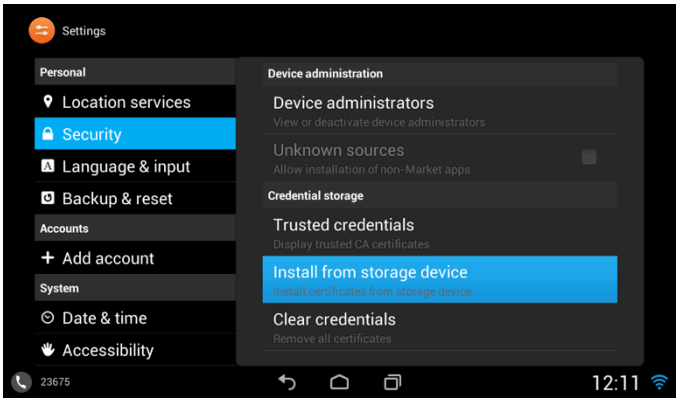
CA 証明書は **DER** または **Base-64** 形式（.cer 形式がサポートされていないため、拡張子は **.crt**）にする必要があります。

一度証明書がインストールされると、セキュア デバイスとみなされ、PEAP を使用する場合は、CA 証明書が要求されます。

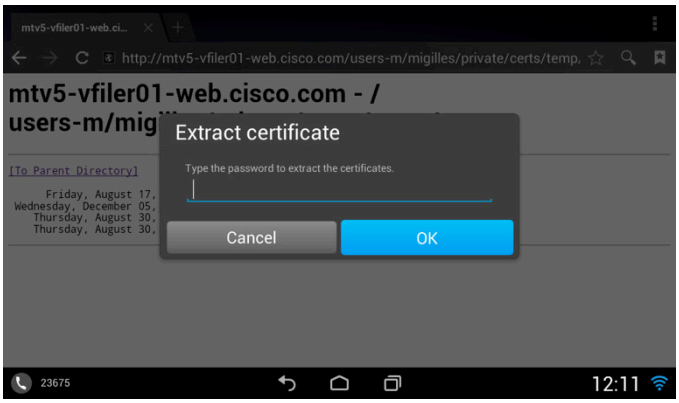
証明書は、Web ブラウザのダウンロードや ADB プッシュ（**adb push *cert_name* /sdcard/*cert_name***）でインストールすることができます。

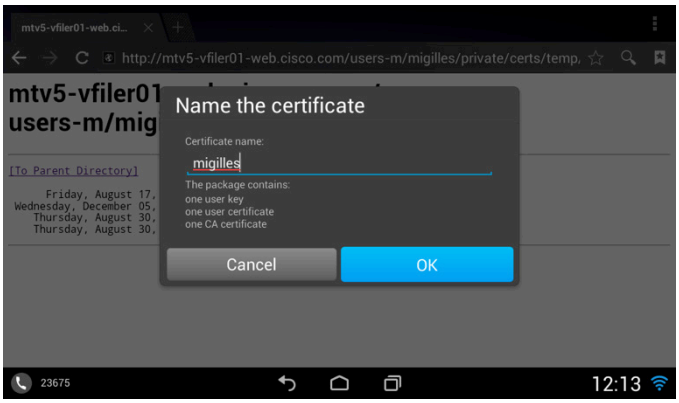
Cisco DX シリーズに証明書をインストールするには、次のガイドラインを使用します。

- Web ブラウザを使用して証明書をインストールするには、証明書に移動して選択します。
- ADB プッシュ経由で Cisco DX シリーズに証明書をコピーする場合、[**ストレージ デバイスからインストール（Install from storage device）**] オプションを選択します。

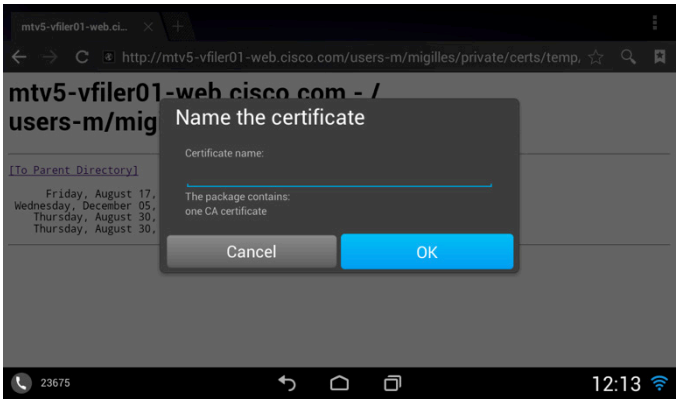


- ユーザ証明書のインストールでは、インポートされた PKCS #12 ファイルから証明書とキーを抽出するためにパスワードを入力する必要があります。
- パスワードを入力した後で、証明書に名前を付けるようプロンプトが表示されます。

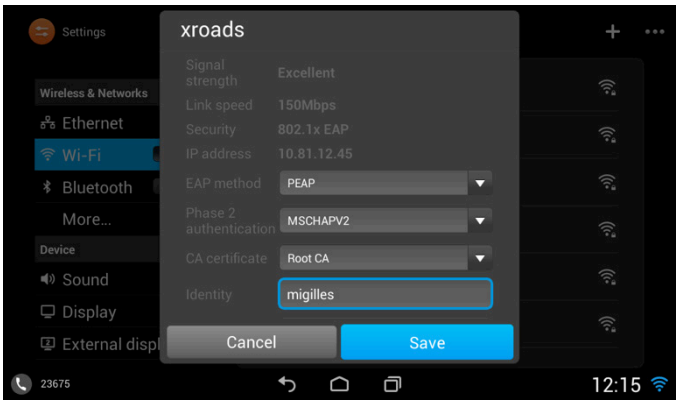


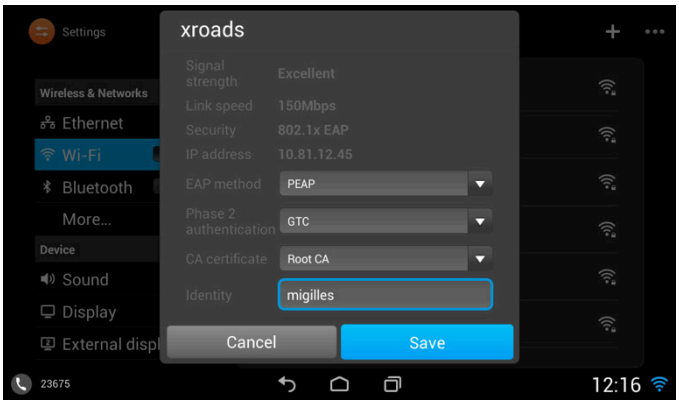


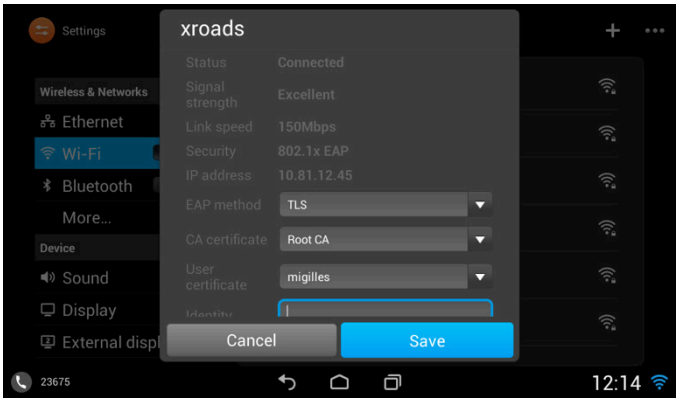
- CA 証明書の場合、証明書を指定します。



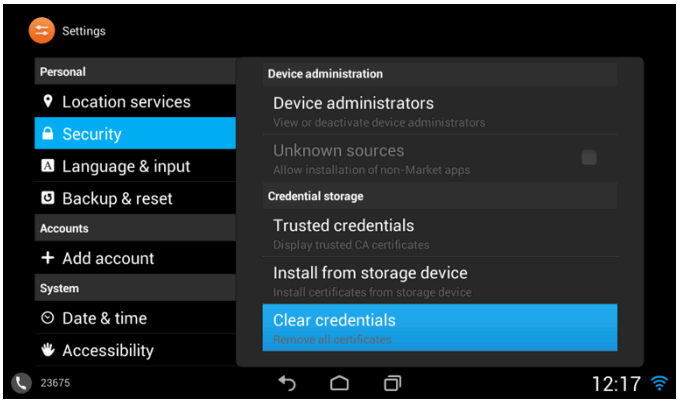
- 証明書をインストールすると、PEAP でのサーバ検証または EAP-TLS に利用できるようになります。
- PEAP でサーバの検証を行う場合、[**CA 証明書（CA certificate）**] を設定する必要があります。
- EAP-TLS では、[**ユーザ証明書（User certificate）**] と [**CA 証明書（CA certificate）**] を設定する必要があります。

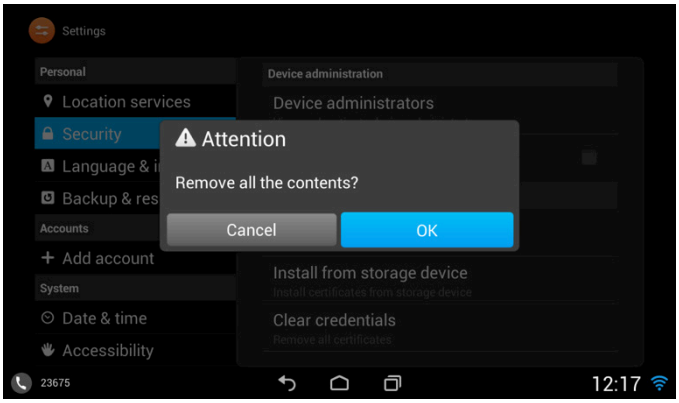






- すべての証明書を削除するには、[セキュリティ（Security）] メニューの [**認証ストレージの消去（Clear credentials）**] を選択します。





Bluetooth の設定

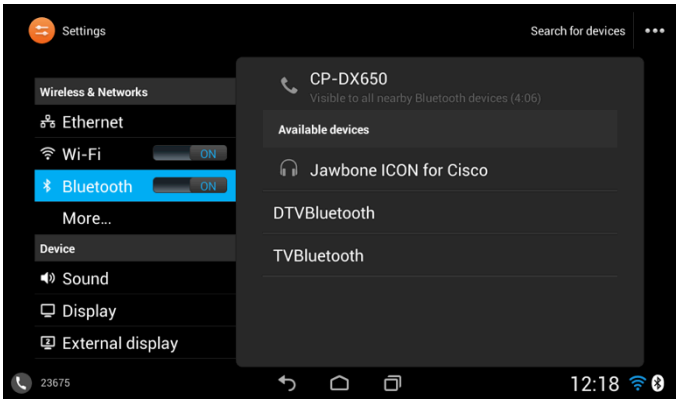
Cisco DX シリーズ は Bluetooth 3.0 をサポートしており、ハンズフリー コミュニケーションが可能です。

Cisco DX シリーズの Bluetooth デバイスをペアにするには、以下の手順に従ってください。

- **[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [Bluetooth]** に移動します。
- [**Bluetooth**] が [**オン（On）**] に設定されていることを確認します。

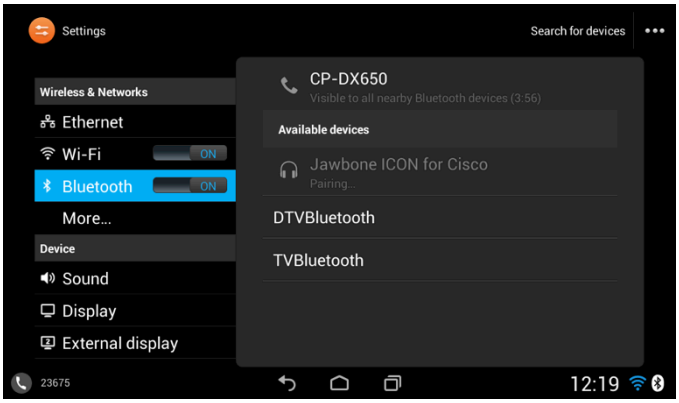
  Bluetooth が Cisco Unified Communications Manager で有効になっていることを確認します。そうでない場合は、このオプションが設定メニューに表示されません。
- [**デバイスの検索（Search for devices）**] を選択します。

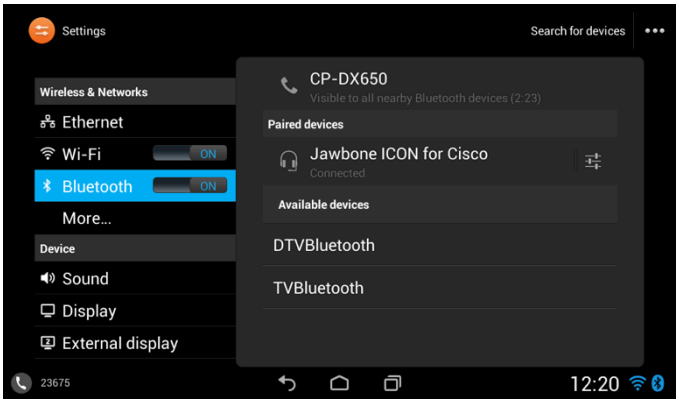
  Bluetooth デバイスがペアリング モードになっていることを確認します。
- Bluetooth デバイスがリストに表示されたら、それを選択します。
- 右上隅にある [...] を選択し、[**デバイスの名前を変更（Rename Device）**] を選択することにより、Cisco DX シリーズでの Bluetooth デバイス名を必要に応じて設定します。
- Bluetooth を使用した Cisco DX シリーズの可視性は任意に一時的に有効にできます（最大 2 分）。

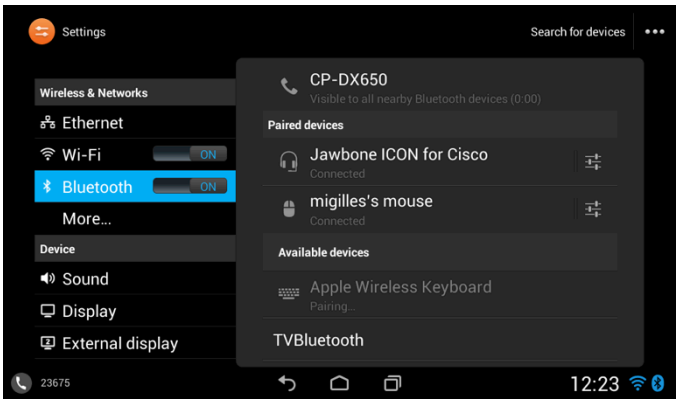


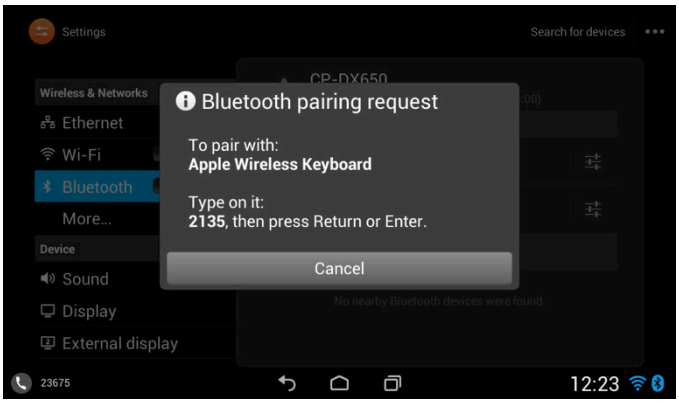
- Cisco DX シリーズは、PIN コード **0000** を使用するためペアリングを試みます。

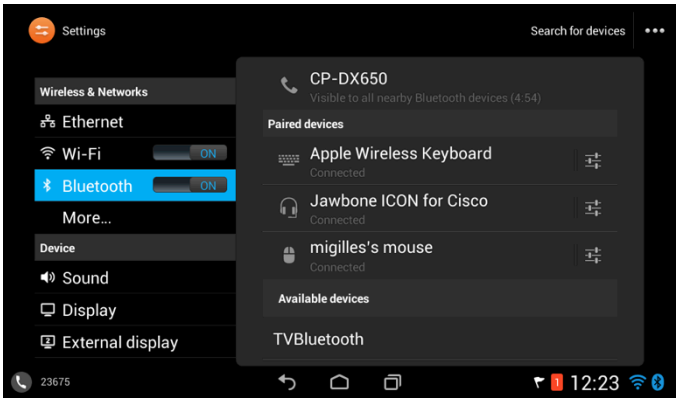
  失敗した場合、プロンプトが表示されたら PIN コードを入力します。
- ペア化されると、Cisco DX シリーズは、Bluetooth デバイスへの接続を試みます。



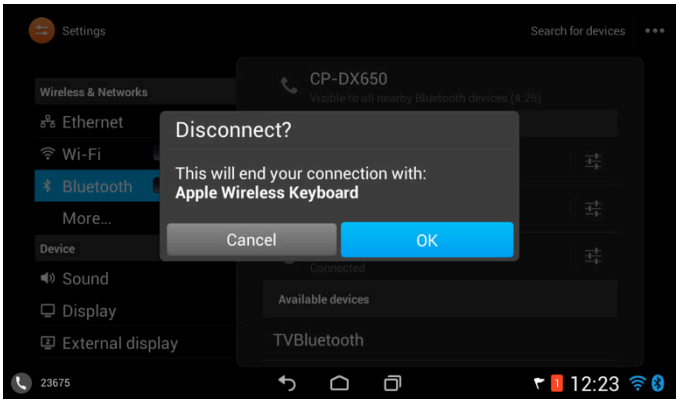




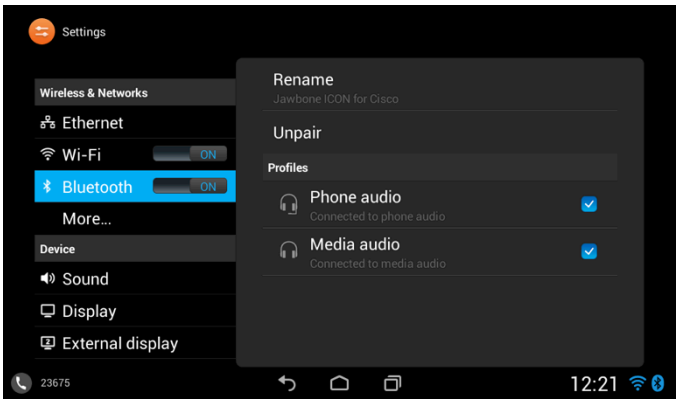


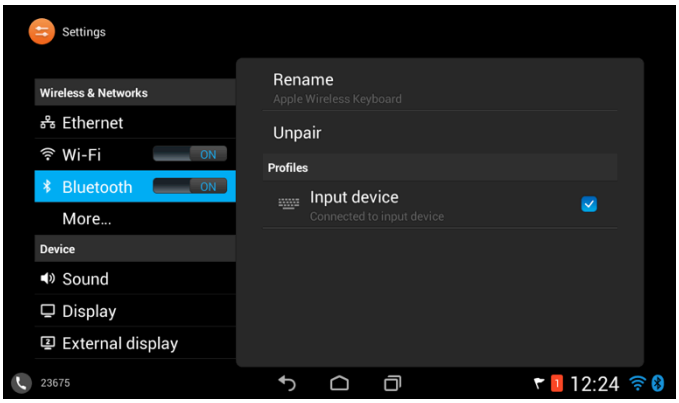


- Bluetooth デバイスの選択をして **[OK]** を選択すると、現在接続されている Bluetooth デバイスの接続が解除されます。

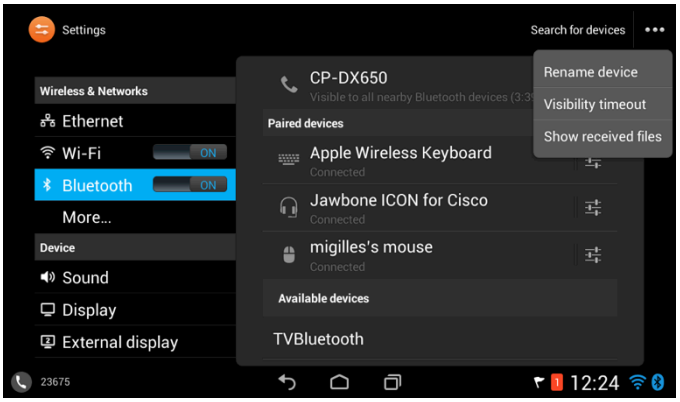


- Bluetooth デバイス名は、相手側デバイスに関連付けられた設定アイコンを選択して [**名前を変更（Rename）**] を選択することで、必要に応じて名前を変更できます。
- [**ペアを解除（Unpair）**] を選択すると、選択されている Bluetooth デバイスをペア解除します。





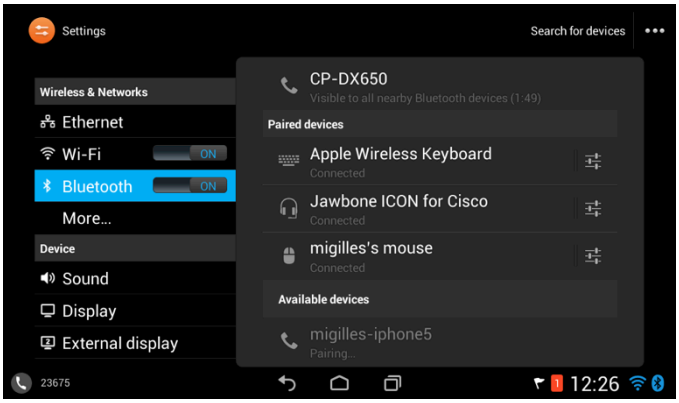
- その他の Bluetooth 設定とメニューにアクセスするには、右上にある [...] を選択します。

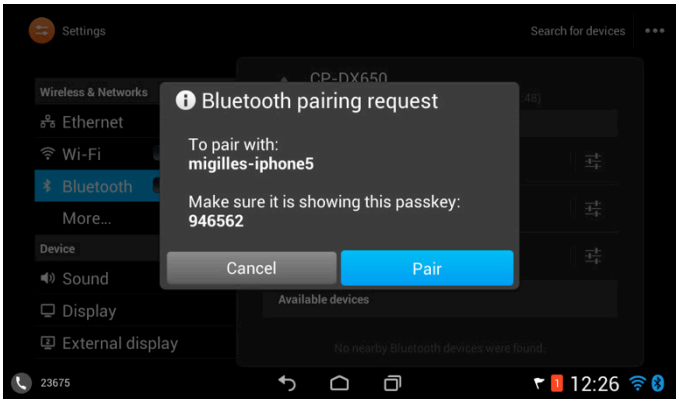


携帯電話共有

Cisco DX シリーズの 10.1(1) リリース以降では、携帯電話と Cisco DX シリーズをペア化して携帯電話共有を有効にすることができます。

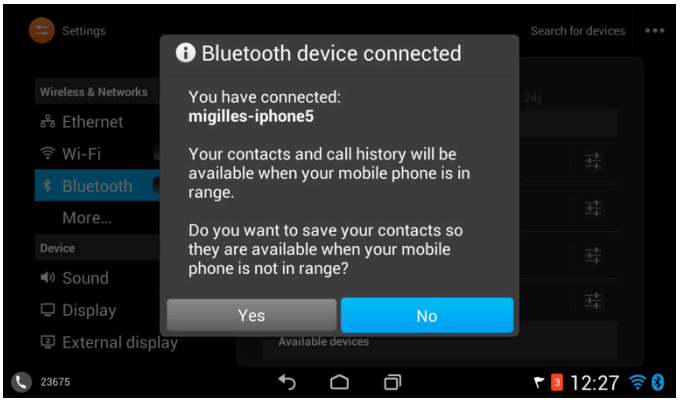
- Bluetooth 対応携帯電話がペアリング モードになっていることを確認してから、リストからデバイスを選択します。
- その後で、ペアリングを承認して開始するためのセキュリティ プロンプトが表示されます。
- パスキーが確認されたら [**ペア（Pair）**] を選択します。



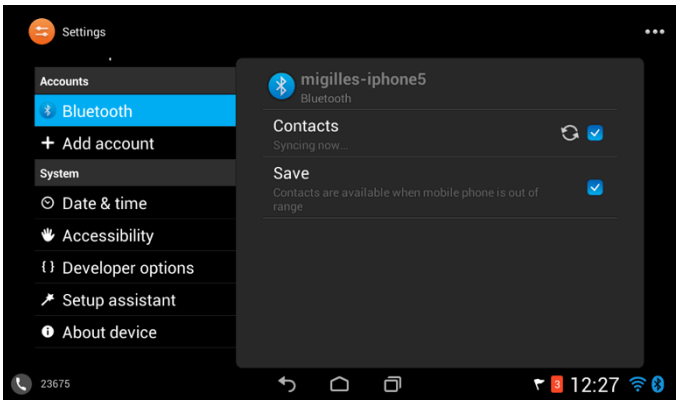


- ペア化されると、Cisco DX シリーズは、Bluetooth 対応携帯電話への接続を試みます。
- その後で、Bluetooth 対応携帯電話からのアドレス帳と通話履歴を常時使用可能にするか、Bluetooth 対応携帯電話が接続されているときにだけ使用可能にするかを選択するためのプロンプトが表示されます。

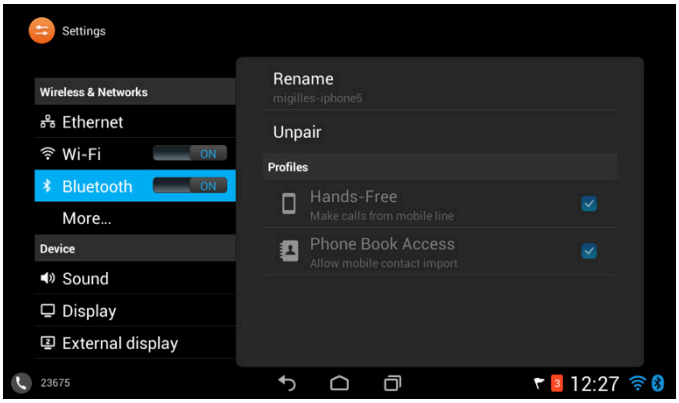
  Cisco Unified Communications Manager で [**Bluetooth アドレス帳のインポートを許可（Allow Bluetooth Contacts Import）**] が有効になっていることを確認する必要があります。



- ペア化された Bluetooth 対応携帯電話用の Bluetooth アカウントが作成されます。

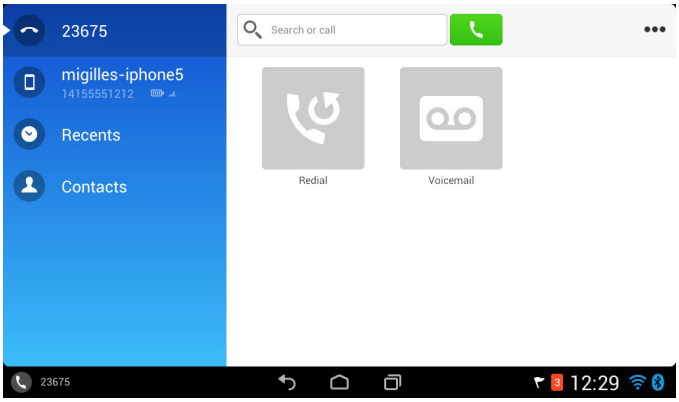


- その他の Bluetooth デバイス オプションは Bluetooth デバイス設定で構成できます。

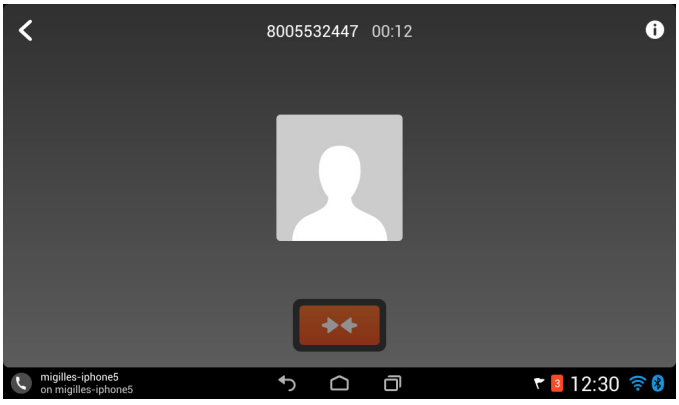


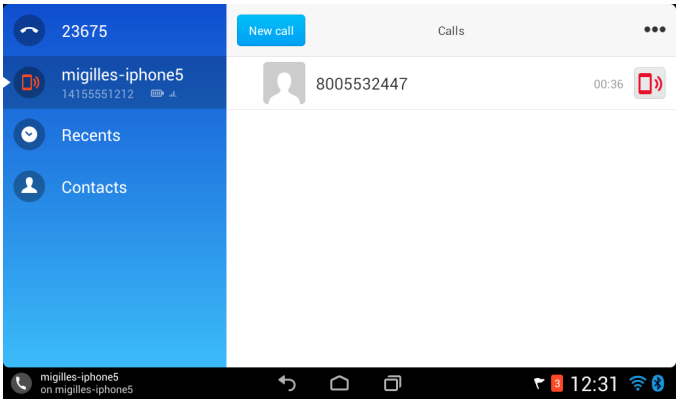
- Cisco DX シリーズは、Bluetooth 対応携帯電話宛てのコールに応答し、携帯電話の回線を利用して発信できます。

  Cisco Unified Communications Manager で [**Bluetooth モバイル ハンズフリー モードを許可（Allow Bluetooth Mobile Handsfree Mode）**] が有効になっていることを確認する必要があります。

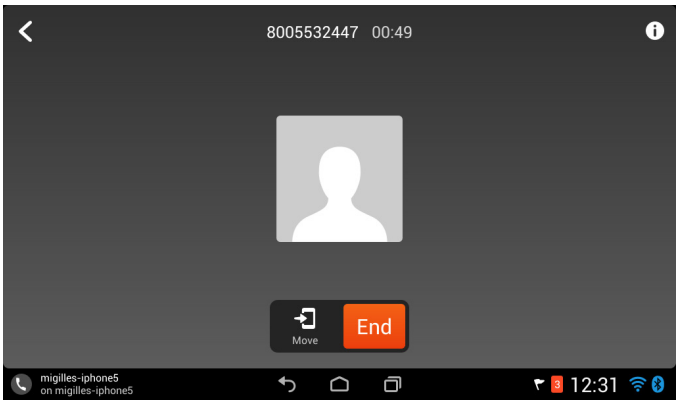


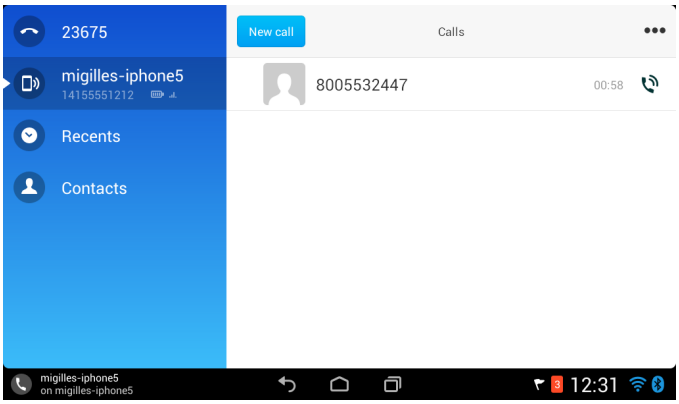
- コールは Cisco DX シリーズと Bluetooth 対応携帯電話の間で簡単に移動できます。
- Bluetooth 対応携帯電話から Cisco DX シリーズにコールを移動するには、オレンジ色のボタンまたはメイン電話画面上の赤色の携帯電話アイコンを押すだけです。





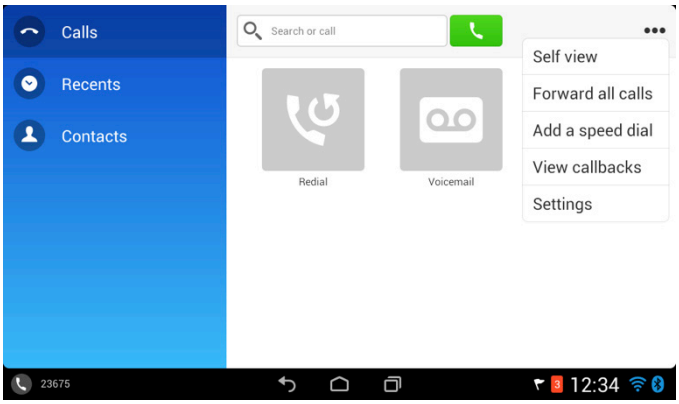
- そうすれば、コールが Bluetooth 対応携帯電話を経由して Cisco DX シリーズに転送されます。
- Bluetooth 対応携帯電話にコールを戻すには [**移動（Move）**] を選択します。





ビデオ コール設定

ビデオ コール設定は、電話アプリケーションの右上隅にある [...] を選択してから [**設定（Settings）**] を選択することで設定できます。



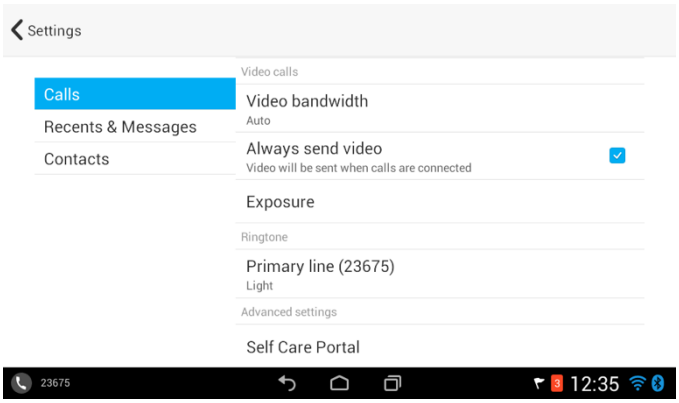
オーディオのミュート ソフトキーを押すと、送信された音声を停止します。

ビデオのミュート ソフトキーを押すと、送信されたビデオを停止します。

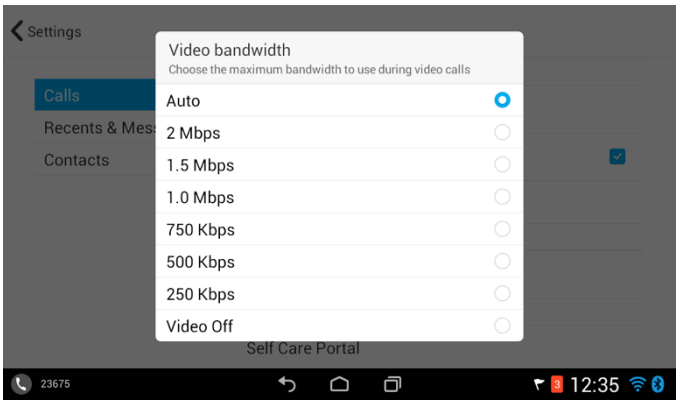
ビデオ コールでは、ローカル ビデオを、リモート エンドポイントのビデオとともに表示することが可能です。

[**送信中のビデオ（Always send video）**] は、遠端デバイスにビデオ機能があることを想定して、Cisco DX シリーズがコールの開始後すぐにビデオのストリーミングを開始するかどうかを指定します。無効化されている場合、いつでもビデオのミュートを解除して、ビデオのストリーミングを開始することができます。この設定はデフォルトで有効になっています。

明るさは、電話機の設定内の [露出（Exposure）] を使用して、現在の作業環境に合わせて設定できます。



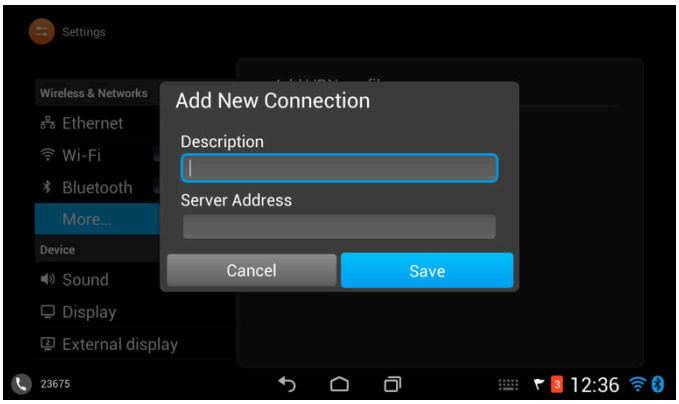
ビデオ帯域幅は現在の作業環境のニーズに合わせて設定することができます。これは、デフォルトで [**自動（Auto）**] に設定され、ビデオ帯域幅適応を可能にします。



VPN 設定

VPN 接続は、管理者が許可していれば、設定できます。

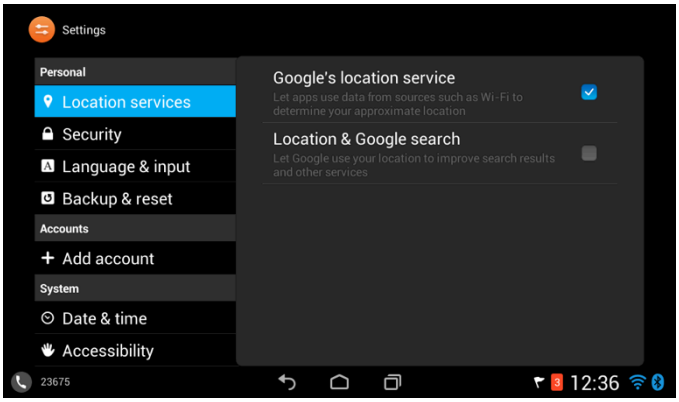
接続の説明およびサーバ アドレスを入力します。



ロケーション設定

ロケーションは、現在の Wi-Fi 接続により、より良好に決定でき、情報がアプリケーション間で共有できるようになります。

位置サービスで [**Google の位置サービス（Google's location service）**] を選択します。

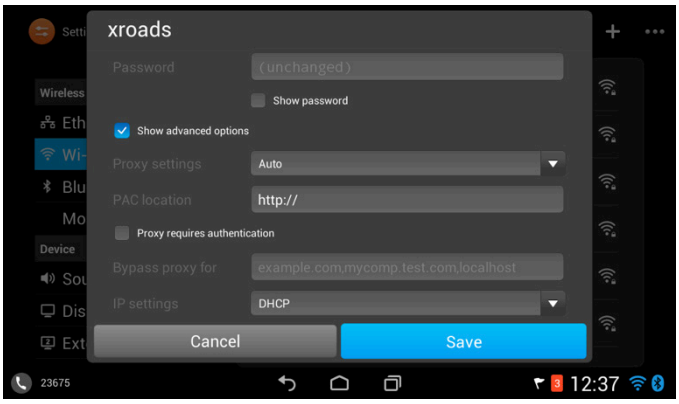


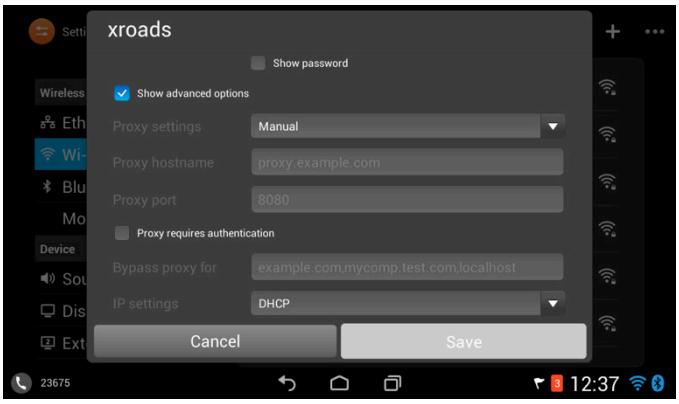
プロキシの設定

プロキシ設定は、[**詳細オプションを表示（Show advanced options）**] にチェックを入れた後、無線 LAN のプロファイル設定の [**プロキシ設定（Proxy settings）**] オプションによって設定できます。

プロキシは、デフォルトでは何も設定されません。

[自動（Auto）] または [手動（Manual）] プロキシ モードをオプションで有効化し、設定できます。





デバイス UI プロファイル

Cisco DX シリーズは、**シンプル** モード（電話機のみ）、**拡張**モード、または**パブリック** モードに設定できます。

シンプル モードは、基本的なビデオ通話機能を提供しますが、電子メール、カレンダー、Webex、Jabber IM、Google Play などのコラボレーション アプリケーションへのアクセスを禁止します。

シンプル モードを有効にするには、Cisco Unified Communications Manager で [**デバイス UI プロファイル（Device UI Profile）**] を [**シンプル（Simple）**] に設定します。

シンプル モードでは、次のような機能も使用できます。

- 表示によるボイスメール
- デュアル独立ディスプレイ
- VPN 経由の登録
- 携帯電話共有
- 問題レポート ツール

拡張モードは、すべてのコラボレーション機能を有効にします。

パブリック モードは、コミュニティ向けの電話に使用されます。

ファームウェアのアップグレード

ファームウェアをアップグレードするには、Cisco Unified Communications Manager の署名付き COP ファイルをインストールします。

COP ファイルのインストール方法については、次の URL にある『Cisco Unified Communications Manager Operating System Administrator Guide』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

TFTP サーバのダウンロード時に、設定ファイルが解析され、デバイスのロードが識別されます。その後で、Cisco DX シリーズは、指定されたイメージがまだ実行されていなければ、ファームウェア ファイルをフラッシュにダウンロードします。

ロード サーバを代替 TFTP サーバとして指定してファームウェア ファイルを取得できます。このファイルは Cisco Unified Communications Manager Administration 内の Cisco DX シリーズの製品固有の設定セクションにあります。

Cisco DX シリーズの使用方法

アプリケーション市場

さまざまなアプリケーションを Google Play からダウンロードして入手できます。

Google Play は、Google™ によって開発された Android OS 用アプリケーション市場です。**Play Store** アプリケーションで、ユーザは、サードパーティの開発者が公開したアプリケーションを参照し、ダウンロードすることができます。

Google Play は書籍と参考書、ビジネス、コミック、通信、教育、エンターテインメント、金融、ゲーム、健康/フィットネス、ライブラリ/デモ、ライフスタイル、ライブ壁紙、メディア/ビデオ、医療、音楽/オーディオ、ニュース/雑誌、パーソナライゼーション、写真、生産性、ショッピング、社会、スポーツ、ツール、輸送、旅行/地域、天気およびウィジェットなどのアプリケーションを提供します。

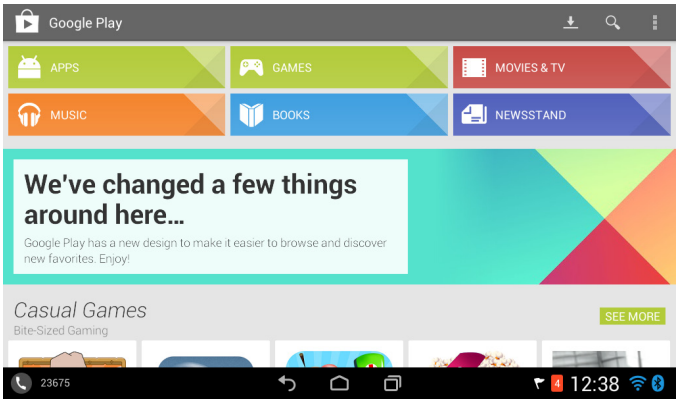
Play Store アプリケーションは [**Google Play からのアプリケーションを許可（Allow Applications from Google Play）**] が Cisco Unified Communications Manager のシステム管理者によって有効にされている場合だけ表示されます。

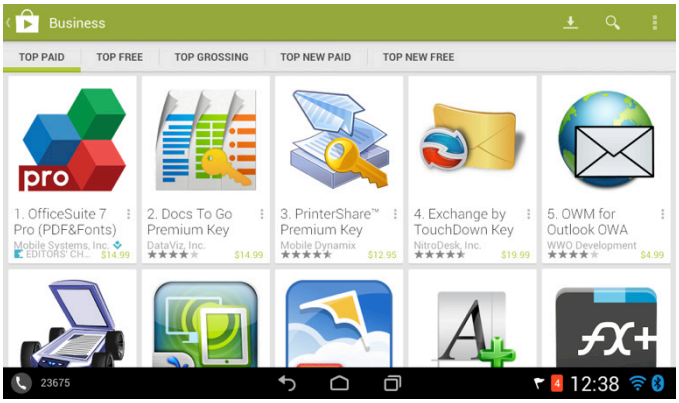
Google のアカウントはアプリケーションをダウンロードするために必要です。

最初に Google Play を起動した時、まだアカウントを持っていない場合はクレデンシャルを使用してサインインまたは登録するようプロンプトが表示されます。

Google Play は、次の URL でもアクセスできます。

https://play.google.com/store



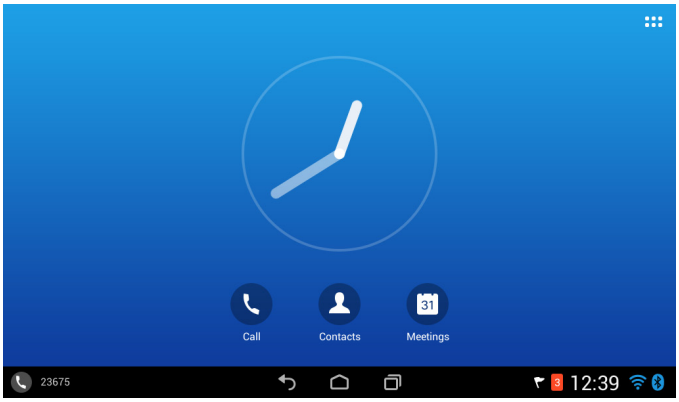


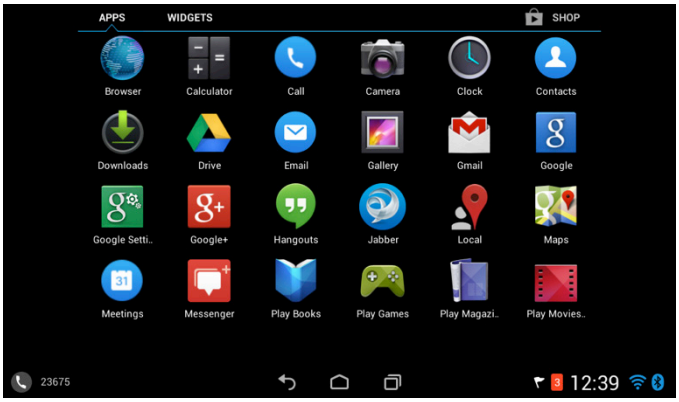
アプリケーション

Google Play によって提供されるアプリケーション以外に、音声およびビデオ通話用の Cisco Unified Communications Manager の電話クライアント、Cisco Jabber IM、Cisco Unified Presence、Cisco WebEx、電子メール、カレンダー、連絡先などのアプリケーションがプレインストールされています。

電話アプリケーション

電話アプリケーションを起動するには、タスク バーで、アプリケーション メニューまたはメイン ページで作成されたショートカットから電話アイコンを選択します。





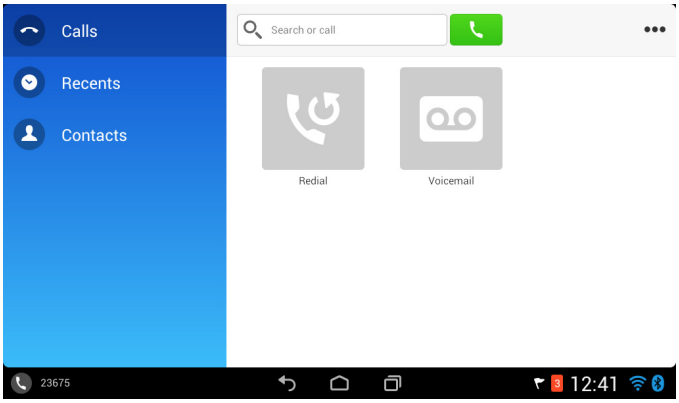
電話アプリケーションの起動後、電話ボタン テンプレートで設定された回線、短縮ダイヤルやその他のオプションが、[**通話（Calls）**] メニューに表示されます。

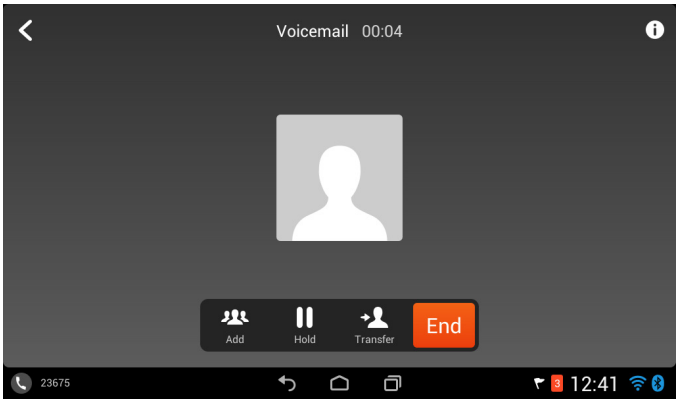
通話履歴、メッセージは [**新着（Recents）**] メニューにあります。

連絡先およびお気に入りが、右上隅にある接続のアイコンでアクセスできます。

Cisco DX シリーズは電源投入後に Cisco Unified Communications Manager に登録しようとするため、アプリケーションを手動で起動する必要はありません。

名前や内線番号付きの電話アイコンが表示されていれば、Cisco DX シリーズが Cisco Unified Communications Manager に登録されています。

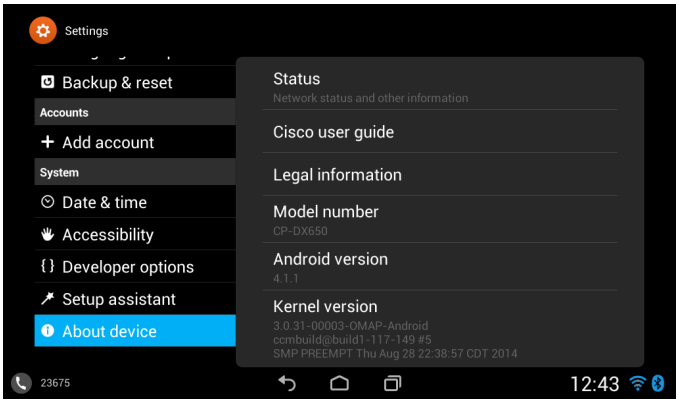


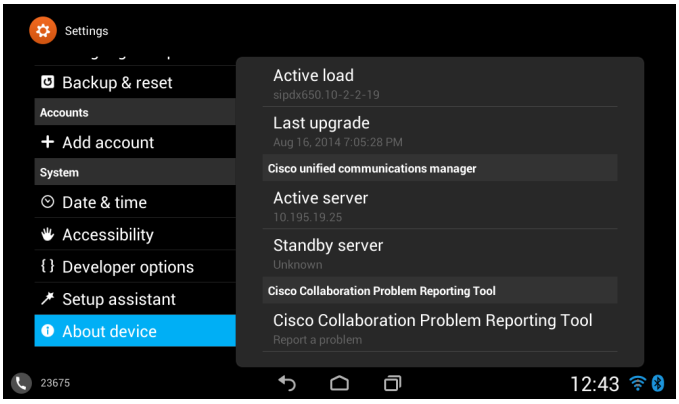


トラブルシューティング

デバイスについて

状態とバージョン情報は [設定（Settings）] メニューの [**端末について（About Device）**] に表示されます。

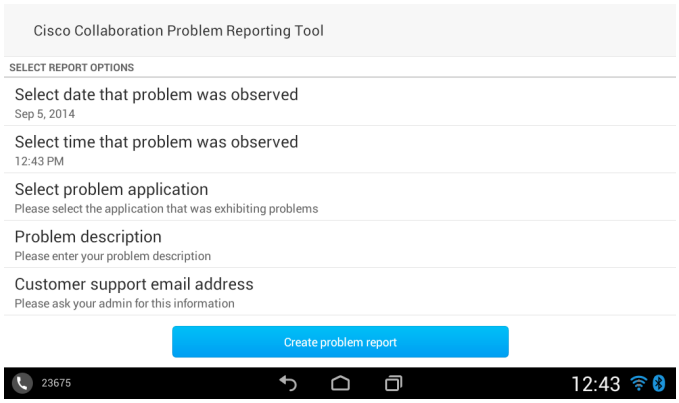




Cisco Collaboration Problem Reporting Tool

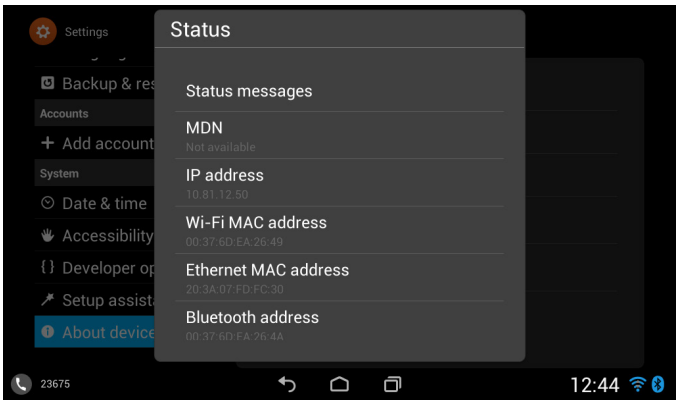
問題についてのレポートは、[端末について（About Device）] メニューにある Cisco Collaboration Problem Reporting Tool で作成できます。

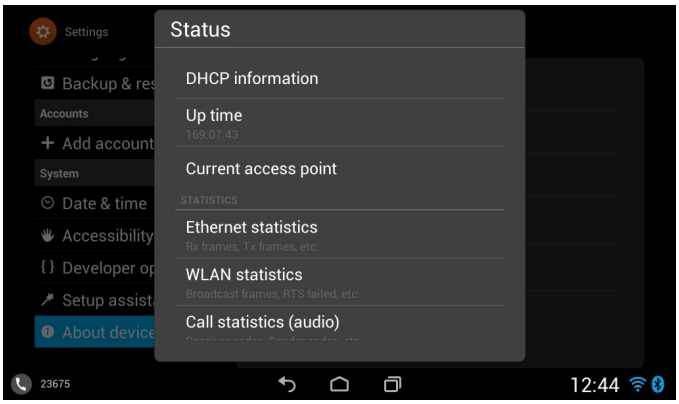
日時、問題となるアプリケーション、問題の説明とカスタマー サポートの電子メール アドレスを定義できます。



ステータス

ステータス メッセージ、IP アドレス、MAC アドレス、DHCP 情報、アップ タイム、現在のアクセス ポイントと統計情報が **[端末について（About Device）] > [ステータス（Status）]** を選択して表示できます。

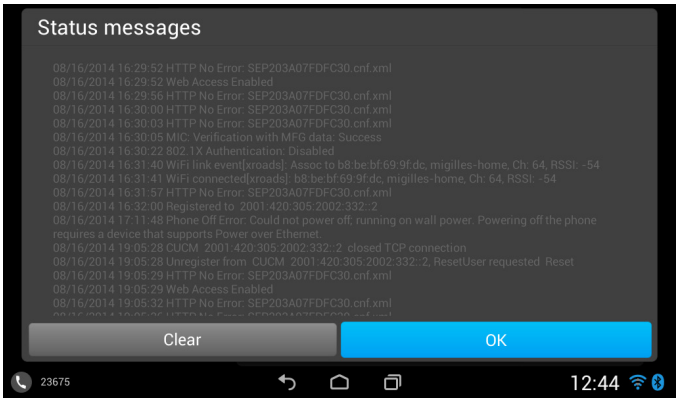




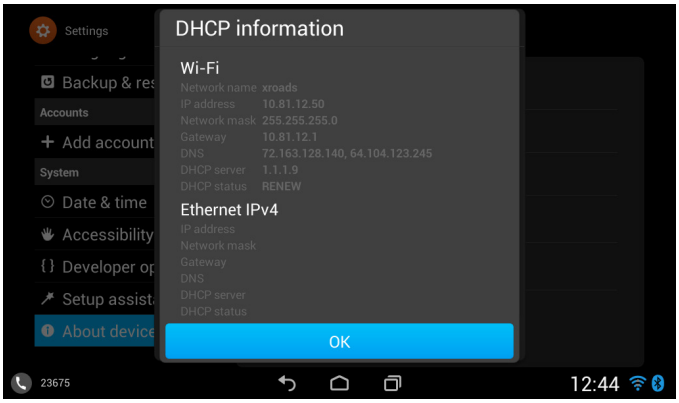
ステータス メッセージ

[ステータス メッセージ（Status messages）] を選択してメッセージ ログを表示します。

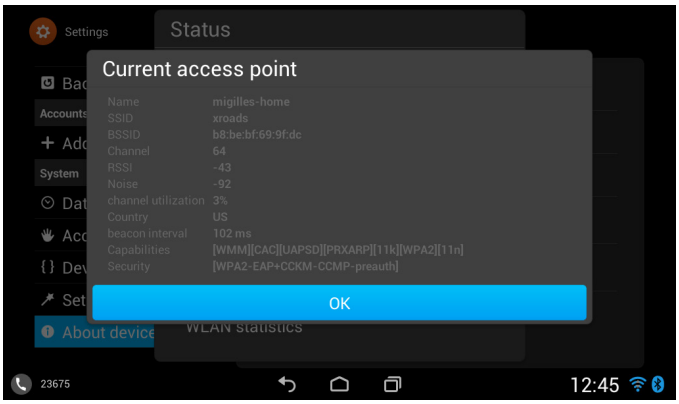
メッセージ ログをリセットするには、**[クリア（Clear）]** を選択します。



[**DHCP 情報（DHCP information）**] を選択して Wi-Fi およびイーサネット インターフェイス用の DHCP 情報を表示します。

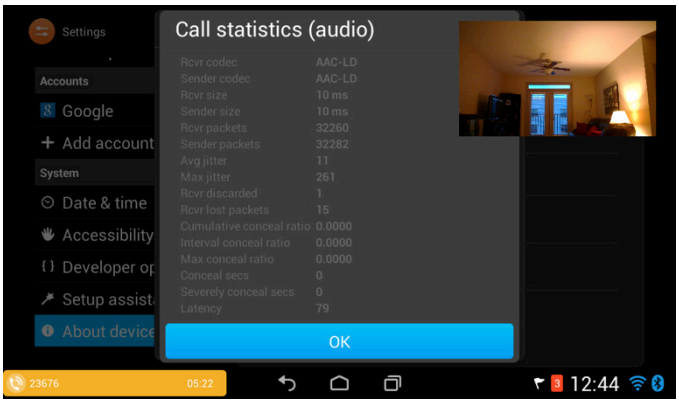


現在のアクセス ポイントの接続の詳細を表示するには、アクセス ポイントを [**現在のアクセス ポイント（Current access point）**] を選択します。

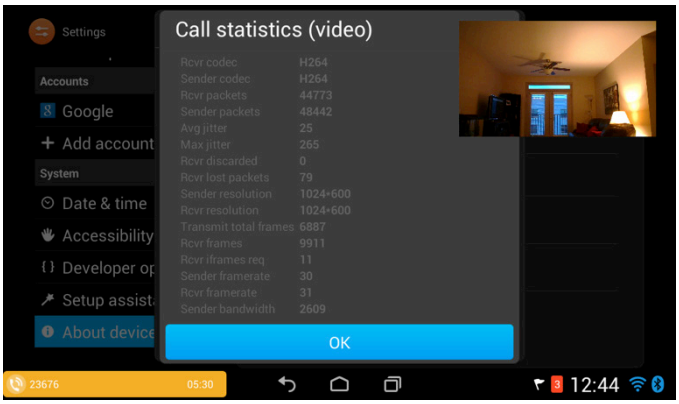


送信および受信されたバイト、パケット、廃棄されたパケット、パケット エラー、再試行カウンタ、および ACK 障害情報を表示するには、[**WLAN 統計（WLAN statistics）**] を選択します。

現在または最後の音声ストリームに関する情報を表示するには、[**コール統計（オーディオ）（Call statistics (audio)）**] を選択します。



現在または最後の音声ストリームに関する情報を表示するには、[**コール統計（ビデオ）（Call statistics (video)）**] を選択します。



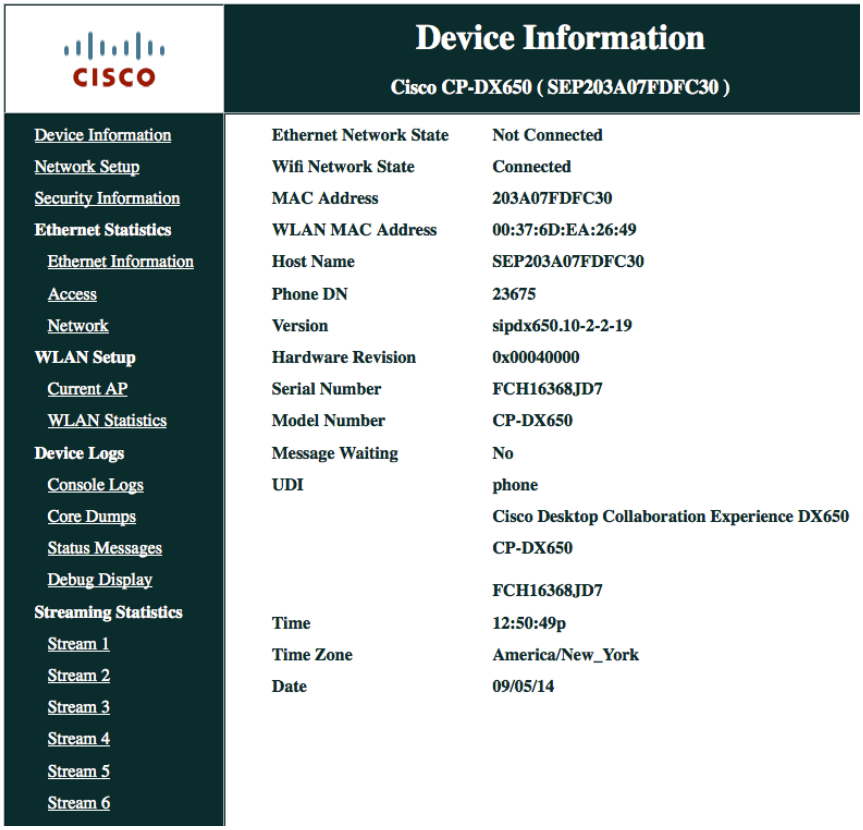
デバイスの Web ページ

Cisco DX シリーズの Web ページで、デバイス情報、ネットワーク設定、WLAN 設定、ストリーミング、およびその他の統計情報を表示したり、デバイス ログへアクセスできます。

デバイス情報

Cisco DX シリーズはネットワーク ステータス、MAC アドレスとバージョン情報が表示されるデバイス情報を提供します。

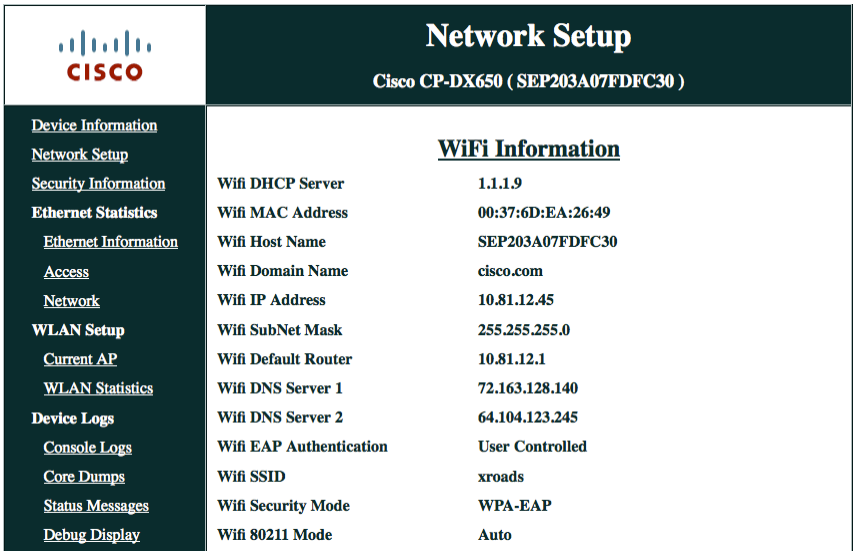
Cisco DX シリーズの Web インターフェイス（http://x.x.x.x）を参照して、[**デバイス情報（Device Information）**] を選択してこの情報を確認します。



ネットワークのセットアップ

Cisco DX シリーズは、Wi-Fi、イーサネット、および Cisco Unified Communications Manager の情報を示すネットワーク セットアップ情報を表示できます。

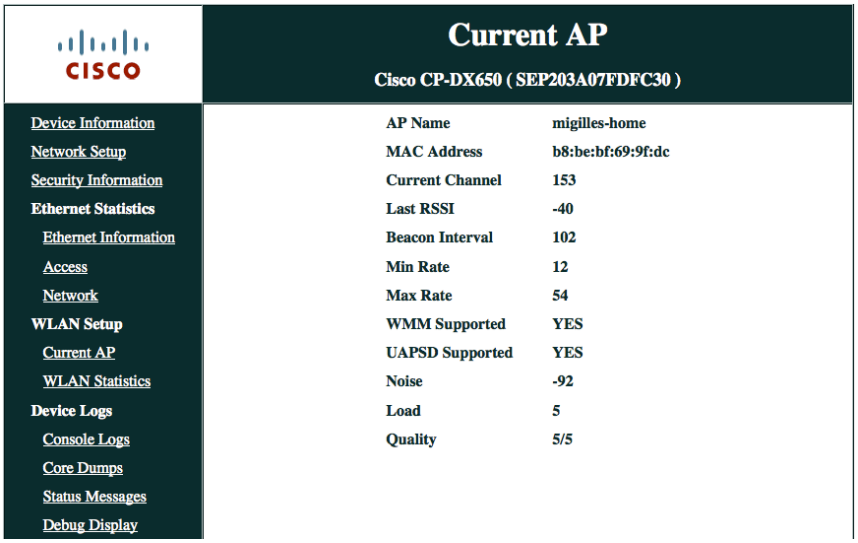
Cisco DX シリーズの Web インターフェイス(http://x.x.x.x)を参照して、[**ネットワークのセットアップ(Network Setup)**] を選択してこの情報を確認します。



現在のアクセス ポイント

現在のアクセス ポイントに関する詳細は、Cisco DX シリーズの Web インターフェイスでも表示できます。

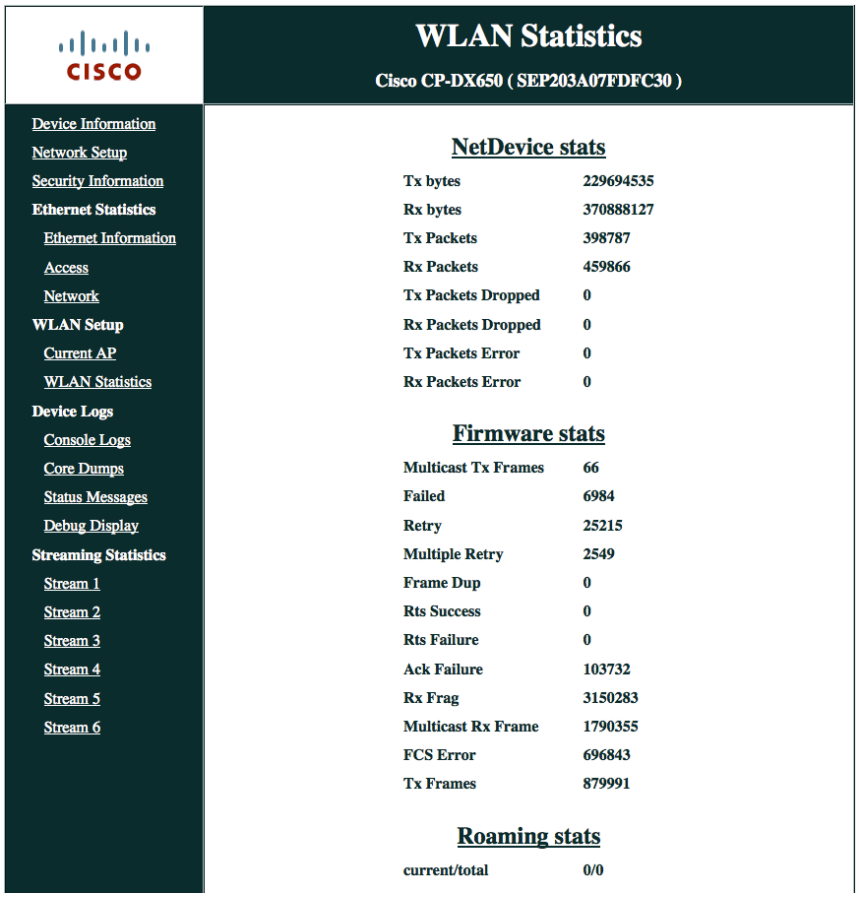
Cisco DX シリーズの Web インターフェイス（http://x.x.x.x）を参照して、[**現在の AP（Current AP）**] を選択し、この情報を確認します。



WLAN 統計情報

Cisco DX シリーズはパケットとカウンタが表示された WLAN 統計情報も提供します。

Cisco DX シリーズの Web インターフェイス（http://x.x.x.x）を参照して、[**WLAN 統計（WLAN Statistics）**] を選択し、この情報を確認します。

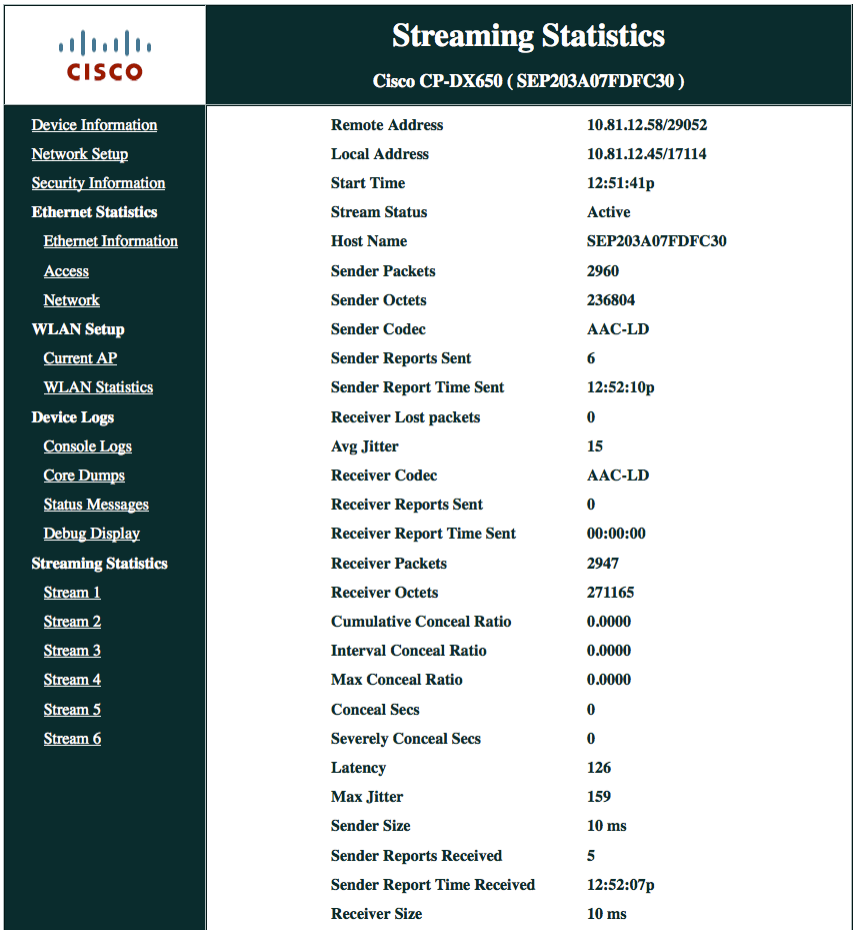


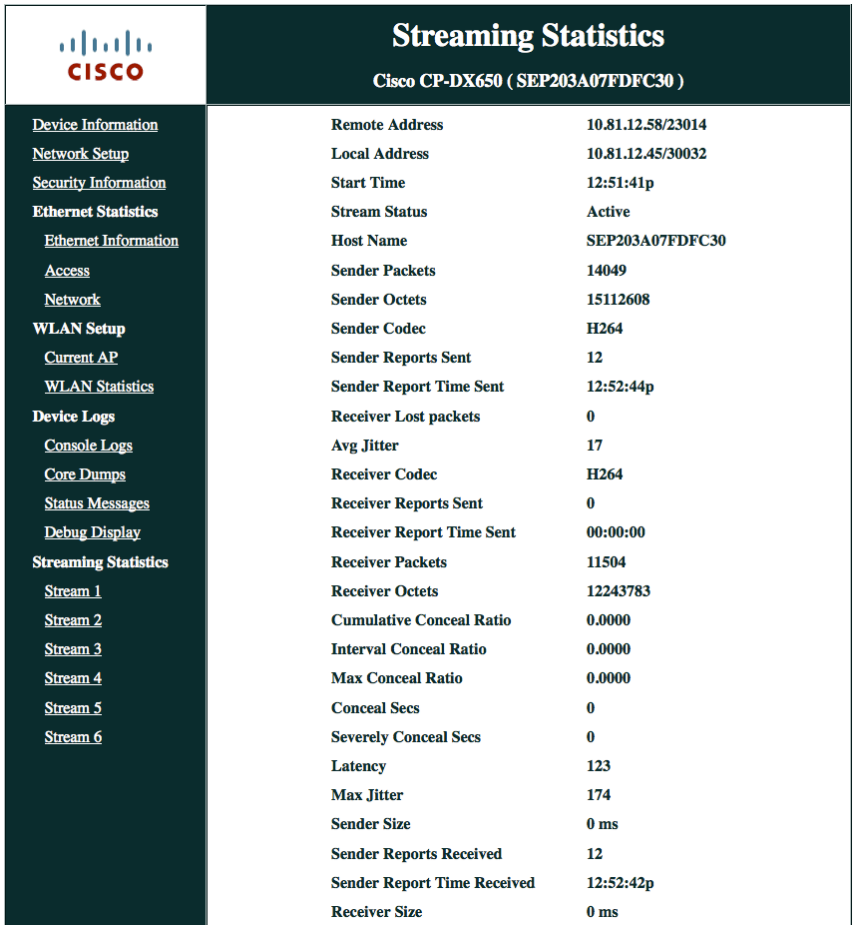
ストリームの統計

Cisco DX シリーズでは、MOS、ジッタ、パケット カウンタなど、コールに関する統計情報を表示できます。

Cisco DX シリーズの Web インターフェイス（http://x.x.x.x）を参照して、[**ストリームの統計（Streaming Statistics）**] を選択し、この情報を確認します。

Cisco DX シリーズでは、音声やビデオの MOS（コール品質）統計情報を表示しません。


Streaming Statistics
Cisco CP-DX650 (SEP203A07FDFC30)
Device Information
Network Setup
Security Information
Ethernet Statistics
Ethernet Information
Access
Network
WLAN Setup
Current AP
WLAN Statistics
Device Logs
Console Logs
Core Dumps
Status Messages
Debug Display
Streaming Statistics
Stream 1
Stream 2
Stream 3
Stream 4
Stream 5
Stream 6
Remote Address 10.81.12.58/29052
Local Address 10.81.12.45/17114
Start Time 12:51:41p
Stream Status Active
Host Name SEP203A07FDFC30
Sender Packets 2960
Sender Octets 236804
Sender Codec AAC-LD
Sender Reports Sent 6
Sender Report Time Sent 12:52:10p
Receiver Lost packets 0
Avg Jitter 15
Receiver Codec AAC-LD
Receiver Reports Sent 0
Receiver Report Time Sent 00:00:00
Receiver Packets 2947
Receiver Octets 271165
Cumulative Conceal Ratio 0.0000
Interval Conceal Ratio 0.0000
Max Conceal Ratio 0.0000
Conceal Secs 0
Severely Conceal Secs 0
Latency 126
Max Jitter 159
Sender Size 10 ms
Sender Reports Received 5
Sender Report Time Received 12:52:07p
Receiver Size 10 ms



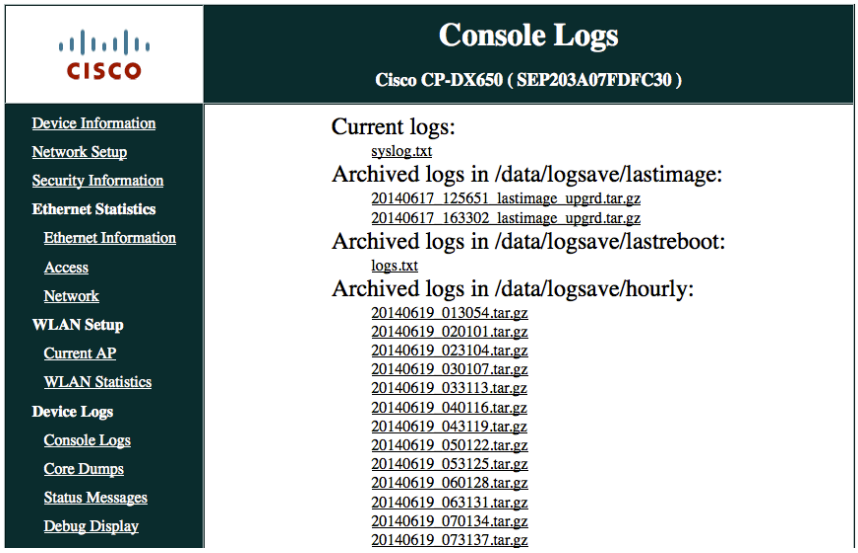
詳細については、次の URL にある『Cisco DX Series Administration Guide』を参照してください。

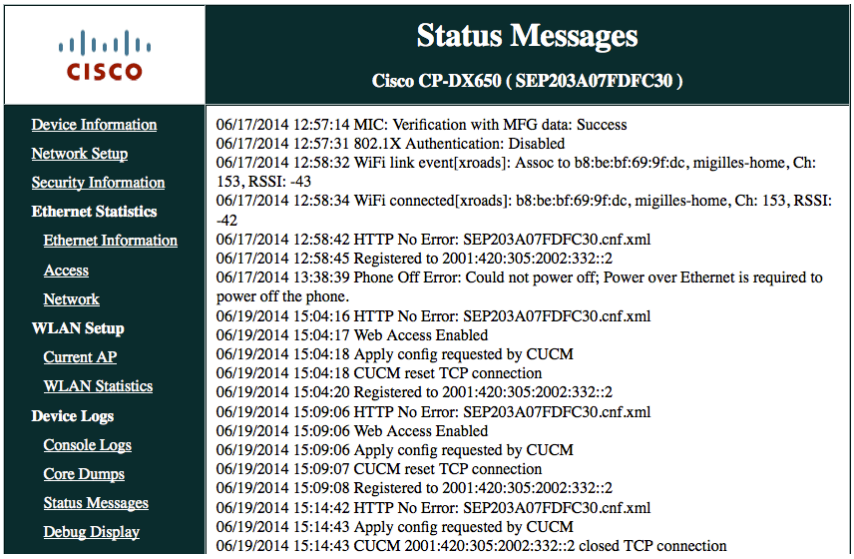
http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

デバイス ログ

コンソール ログ、コア ダンプ、ステータス メッセージが Cisco DX シリーズの Web インターフェイスからトラブルシューティング目的で取得できます。

Cisco DX シリーズの Web インターフェイス（http://x.x.x.x）を参照して、[**デバイス ログ（Device Logs）**] を選択し、この情報を確認します。



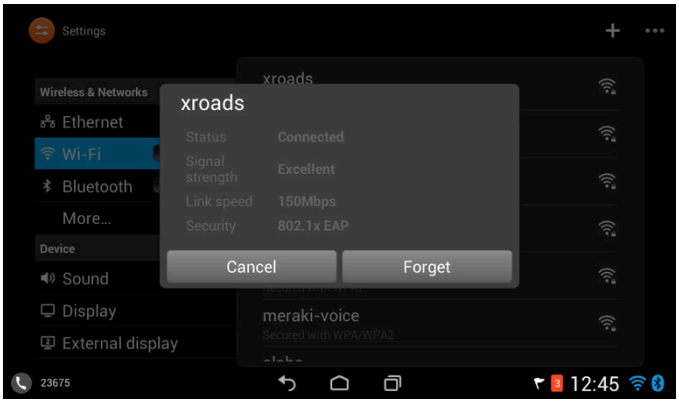


WLAN 情報

接続ステータス、WLAN 信号インジケータ、および近接リスト情報は Cisco DX シリーズ上でローカルに表示できます。

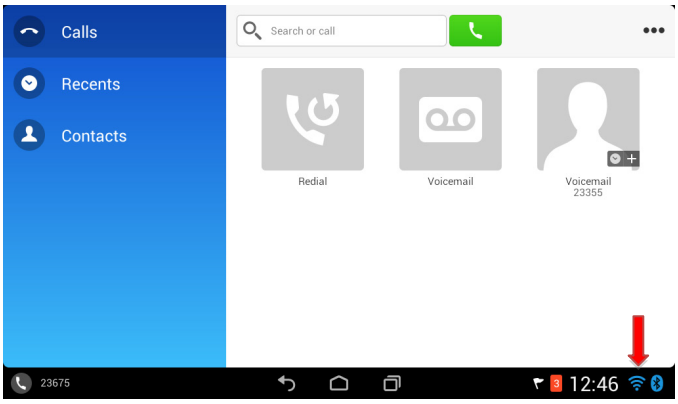
接続状況

状態、セキュリティ タイプ、信号強度、リンク速度および IP アドレスに関連する現在の接続情報が現在接続されているネットワークをタップすると表示できます。



WLAN 信号インジケータ

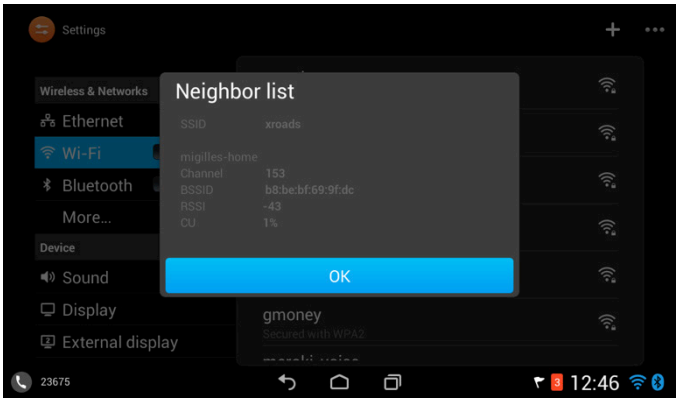
WLAN 信号インジケータは右下隅に常に表示されます。



近接リスト

Cisco DX シリーズの近接リスト メニューに現在のネイバーが表示されます。

近接リストを表示するには、**[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [Wi-Fi]** の右上隅にある [...] を選択し、**[近接リスト（Neighbor list）]** を選択します。

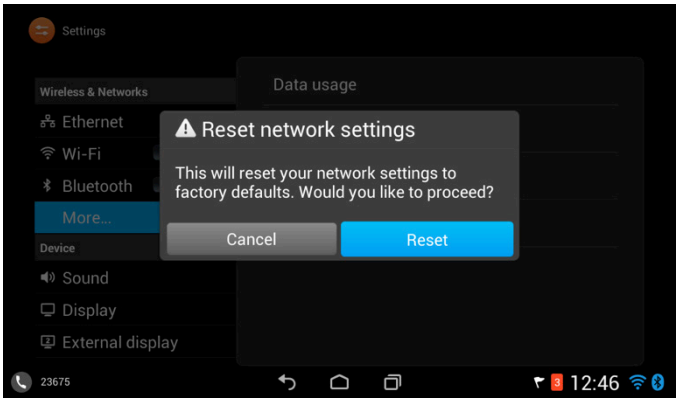


詳細については、次の URL にある『Cisco DX Series Administration Guide』を参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

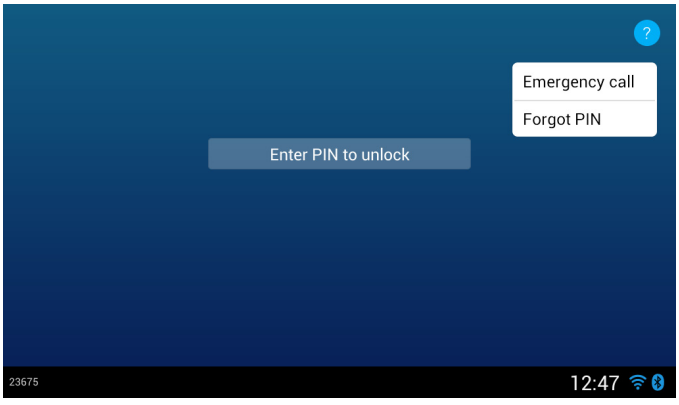
ネットワーク設定のリセット

ネットワーク設定は、**[設定（Settings）] > [無線とネットワーク（Wireless & networks）] > [詳細...（More...）]** から**[ネットワーク設定をリセット（Reset network settings）]** を選択することによって、リセットできます。



忘れた PIN のリセット

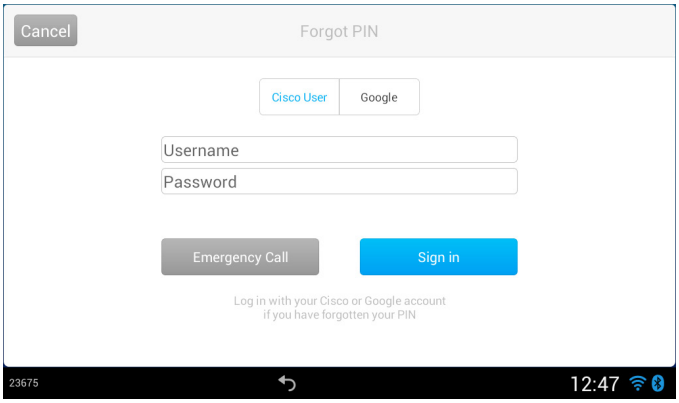
PIN を忘れた場合は、ロック解除画面で [?] を選択してから、**[PIN を忘れた場合（Forgot PIN）]** を選択することにより、PIN をリセットできます。



[PIN を忘れた場合（Forgot PIN）] を選択すると、次のアカウントの 1 つで認証する画面が表示されます。

- シスコ ユーザ
- Google

認証が成功すると、PIN をリセットできます。



リモート ロックとワイプ

Cisco Unified Communications Manager の管理者は、任意の Cisco DX シリーズをリモートでロックまたはワイプすることができます。

Cisco DX シリーズをリモートでロックする場合は、電話の設定ページで [**ロック（Lock）**] オプションを選択します。そうすると、Cisco DX シリーズ にアクセスするための PIN の入力が要求されます。

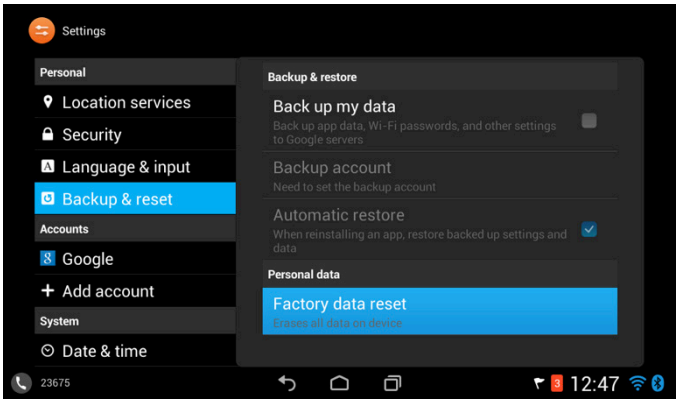
Cisco DX シリーズ上のデータをすべて消去する場合は、電話の設定ページで [**ワイプ（Wipe）**] オプションを選択します。

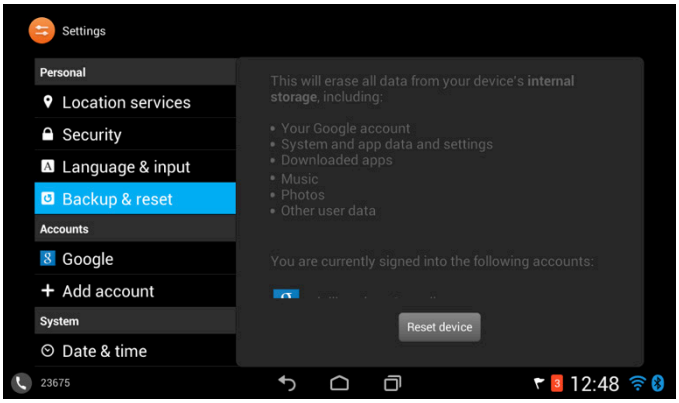
[**常時 VPN（Always On VPN）**] を有効にすると、デバイスをロックまたはワイプするため Cisco DX シリーズを常時オンラインにしておくことができます。

ファクトリ設定の復元

すべてのデータは Cisco DX シリーズから、[設定（Settings）] の **[データの初期化（Factory data reset）] > [バックアップとリセット（Backup & reset）]** を選択して、消去できます。

工場出荷時のデータへのリセットを進めるために [**デバイスのリセット（Reset Device）**] を選択する必要がある場所では、確認画面が表示されます。





Cisco DX シリーズが適切に起動できない場合、出荷時の状態へのリセットは、次の手順で開始できます:

- 電源を切断して、デバイスをオフにします。
- # キーを押し続け、電源を接続します。
- メッセージ LED が点灯するまで # キーを押したままにします。
- メッセージ LED が点灯したら、# キーを放します。
- 1 2 3 4 5 6 7 8 9 * 0 # を押します。
- メッセージ LED が 3 回点滅し、工場出荷時の状態にリセットする手順が受け入れられたことを示します。
- Cisco DX シリーズで、通常の起動プロセスが続行され、工場出荷時の設定がリストアされます。

別のイメージを起動するには、次の手順を実行します。

- 電源を切断して、デバイスをオフにします。
- * キーを押し、電源を接続します。
- メッセージ LED が点灯するまで * キーを押したままにします。
- メッセージ LED が 3 回点滅したら、* キーを放します。
- Cisco DX シリーズは代替イメージを使用して起動します。

デバイスのデバッグ

デバイスのデバッグは Cisco DX シリーズに SSH または Android Debug Bridge（ADB）シェルによってアクセスすることによりオプションで有効にできます。

ADB を使用する場合は、Cisco Unified Communications Manager で Cisco DX シリーズの設定が有効になっていることを確認します。
次の場所から ADB を含む Android SDK をダウンロードします。

http://developer.android.com/sdk

SSH を使用する場合は、ユーザ名とパスワードを Cisco Unified Communications Manager 内の Cisco DX シリーズの [SSH] セクションで設定されていることを確認します。
ローカル ログイン = cisco でパスワード = default です。

デバイス画面のスクリーンショットのキャプチャ

現在の画面は、http://x.x.x.x/CGI/Screenshot にアクセスするとキャプチャできます（**x.x.x.x** は、Cisco DX シリーズの IP アドレスです）。プロンプトで、Cisco Unified Communications Manager で Cisco DX シリーズに関連付けられたアカウントのユーザ名とパスワードを入力します。

ヘルスケア環境

この製品は、医療機器ではありません。他の装置または機器からの干渉を受けやすい、ライセンスのない周波数帯域を使用します。

アクセサリ

Cisco DX シリーズ では、次のアクセサリを使用できます。

サードパーティのアクセサリ

- Bluetooth ヘッドセット
  - www.plantronics.com
  - www.jabra.com
  - www.jawbone.com
  - www.vxicorp.com
  - www.motorola.com

その他の資料

Cisco DX シリーズ データシート

http://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/datasheet-listing.html

Cisco DX シリーズ管理ガイド

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

Cisco DX シリーズ ユーザ ガイド

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html

Cisco DX シリーズ リリース ノート

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

Cisco DX シリーズ ソフトウェア

http://software.cisco.com/download/navigator.html?mdfid=284711383

Cisco Unified Communications Manager

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Voice ソフトウェア

http://software.cisco.com/download/navigator.html?mdfid=278875240

Real-Time Traffic over Wireless LAN SRND

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

Cisco Unified Communications SRND

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html

Cisco Unified Wireless LAN Controller に関するマニュアル

http://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html

Cisco Autonomous Access Point に関するマニュアル

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA.html