



Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド



Cisco Wireless Phone 840 および 860 は、ユーザーがタスクと通信を簡単に管理できるモバイル コラボレーション プラットフォームを提供します。Cisco Wireless Phone 840 および 860 は、セキュアなエンタープライズグレードのスマートフォンのパワーとパフォーマンスを提供しながら、シスコのコラボレーション ソリューションを通じて管理しやすいデバイスを提供します。Wi-Fi の柔軟性を備えた Cisco Wireless Phone 840 および 860 は、企業内のどこにいても、従業員の生産性を向上させます。Cisco Wireless Phone 840 は、IP65 等級の防塵、防滴、防湿性能があります。Cisco Wireless Phone 860 は、IP68 等級の完全な防塵性能を備えています。

このガイドでは、ネットワーク管理者がワイヤレス LAN 環境内で Cisco Wireless Phone 840 および 860 を導入するのに役立つ情報と手引きを提供します。

更新履歴

日付	コメント
01/08/21	1.1(0) リリース
03/30/21	1.2(0) リリース
08/30/21	1.3(0) リリース
10/29/21	1.4(0) リリース
04/15/22	1.5(0) リリース
07/26/22	1.6(0) リリース
10/04/22	1.7(0) リリース
04/21/23	1.8(0) リリース
07/23/23	1.9(0) リリース

目次

Cisco Wireless Phone 840 および 860 概要	7
電話機モデル	7
要件	8
サイト調査	8
コール制御	10
ワイヤレス LAN	10
プロトコル	17
Wi-Fi	18
規格	30
Bluetooth	31
言語	33
バッテリー寿命	33
840S および 860S バーコードスキャナ	35
電話機のお手入れ	36
アクセサリ	36
無線 LAN の設計	39
802.11 ネットワーク	39
5 GHz (802.11a/n/ac)	39
2.4 GHz (802.11b/g/n)	41
信号強度とカバレッジ	42
データ レート	45
条件の厳しい環境	47
セキュリティ	49
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	50
Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ)	51
Protected Extensible Authentication Protocol (PEAP)	51
Quality of Service (QoS)	51
コール アドミッション制御 (CAC)	52
有線 QoS	53
ローミング	54
高速セキュア ローミング (FSR)	55
帯域間のローミング	57
電源管理	57
コール キャパシティ	58

マルチキャスト.....	59
Cisco ワイヤレス LAN の設定	59
<i>Cisco AireOS</i> ワイヤレス LAN コントローラおよび <i>Lightweight</i> アクセスポイント	59
802.11 ネットワークの設定.....	61
WLAN の設定.....	72
コントローラの設定.....	82
コール アドミッション制御 (CAC)	84
RF プロファイル.....	88
FlexConnect グループ	91
マルチキャスト ダイレクト.....	92
QoS プロファイル.....	94
詳細設定	97
<i>Cisco Catalyst IOS XE</i> ワイヤレス LAN コントローラおよび <i>Lightweight</i> アクセスポイント	101
802.11 ネットワークの設定.....	103
WLAN の設定.....	111
コントローラの設定.....	127
モビリティ設定	128
コール アドミッション制御 (CAC)	129
マルチキャスト	130
詳細設定	132
設定例.....	134
<i>Cisco Mobility Express</i> および <i>Lightweight</i> アクセスポイント	143
コントローラの設定.....	143
802.11 ネットワークの設定.....	144
WLAN の設定.....	148
RF プロファイル.....	156
マルチキャスト ダイレクト.....	158
<i>Cisco Autonomous (自律) アクセス ポイント</i>	159
802.11 ネットワークの設定.....	159
WLAN の設定.....	164
コール アドミッション制御 (CAC)	176
QoS ポリシー	177
電源管理	180
設定例.....	181
<i>Cisco Meraki</i> アクセス ポイント	186
ワイヤレス ネットワークの作成.....	187
SSID の設定.....	189
無線の設定.....	194
ファイアウォール & トラフィック シェーピング.....	197
Cisco Call Control の設定	199
<i>Cisco Unified Communications Manager</i>	199

デバイスの有効化.....	199
製造元の認証局 (CA) 証明書.....	200
[デバイスプール (Device Pools)].....	201
電話ボタン テンプレート.....	202
セキュリティ プロファイル.....	202
SIP プロファイル.....	205
共通設定.....	208
QoS パラメータ.....	209
G.722 および Opus のアダプタイズメント.....	209
オーディオ ビット レート.....	209
製品固有の設定オプション.....	210
<i>Webex Calling</i>	215
個人的な使用.....	216
共同利用.....	218
デバイス設定.....	222
Cisco Wireless Phone 840 および 860.....	224
エンタープライズ モビリティ管理 (EMM).....	224
シスコワイヤレス電話機構成管理ツール.....	226
構成ファイルの作成.....	227
Cisco Unified Communications Manager の設定.....	251
Cisco Wireless Phone 840 および 860 の登録.....	254
手動設定.....	260
Wi-Fi プロファイルの設定.....	260
証明書管理.....	274
Cisco Phone アプリケーションの設定.....	281
Bluetooth 設定.....	285
ファームウェアのアップグレード.....	288
Cisco Unified Communications Manager.....	288
Webex Calling.....	289
Cisco Wireless Phone Upgrade ツール.....	289
Cisco Wireless Phone 840 および 860 の使用.....	296
アプリケーション.....	296
シスコの電話機.....	297
バーコード.....	303
バッテリー寿命.....	305
ボタン.....	307
通話品質設定.....	307
カスタム設定.....	309
緊急 (Emergency).....	312
ロギング.....	314
PTT.....	315

サウンドステージ	316
システムアップデート	322
Web API	322
アプリケーションストア	324
[IP Phone サービス (IP Phone Services)]	325
トラブルシューティング	326
問題レポート ツール	326
電話機の Web ページ	328
デバイス情報	328
ネットワーク情報	329
登録情報	330
デバイス ログ	332
WLAN 信号インジケータ	333
WLAN ネットワーク情報	334
初期化	335
電話機画面のスクリーンショットのキャプチャ	337
その他のマニュアル	338

Cisco Wireless Phone 840 および 860 概要

Cisco Wireless Phone 840 および 860 は、企業内のコラボレーションを実現するプラットフォームです。無線および有線の Cisco Unified Communication デバイスの強固な基盤として、Cisco Unified Communication アプリケーションの機能を統合します。

Cisco の 802.11 ソリューションにより、音声といった、時間に影響を受ける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できます。無線 LAN 環境の拡張により、アクセスポイント間のローミング時にセキュリティを維持しながら、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実現します。

WLAN はライセンス不要の周波数帯を使用しているため、ライセンス不要の同一周波数帯を使用する他のデバイスから干渉を受ける可能性があります。また、Bluetooth ヘッドセット、電子レンジやコードレス電話など、2.4 GHz 周波数帯を使用するデバイスは急増しており、2.4 GHz 周波数帯では他の周波数帯よりも多くの輻輳が発生する可能性もあります。5 GHz 周波数帯で動作するデバイスは非常に少数であるため、Cisco Wireless Phone 840 および 860 の運用において最大限の 802.11a/n/ac データレートを活用するにはこの周波数帯が推奨されます。

Cisco Wireless Phone 840 および 860 は最適化されていますが、ライセンスのない周波数帯を使用する場合、中断されない通信は保証できず、通話中に数秒の音声のギャップが生じる可能性があります。この導入ガイドラインに従うことで、このような音声のギャップが発生する可能性は低減されますが、完全には解消されません。

ライセンス不要の周波数帯を使用しており、WLAN デバイスへのメッセージの配信は保証されません。

Cisco Wireless Phone 840 および 860 は医療機器として使用されることを意図しておらず、医療診断用途では使用できません。

電話機モデル

次の Cisco Wireless Phone 840 および 860 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ピークアンテナゲイン、周波数範囲とチャンネルの概要です。

製品番号	説明	ピーク アンテナ ゲイン	周波数範囲	使用可能なチャンネル	チャンネル セット
CP-840	Cisco Wireless Phone 840	2.4 GHz = 1.7 dBi 5 GHz = 1.8 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz	13 4	1 ~ 13 36、40、44、48 52、56、60、64
CP-840S	Cisco Wireless Phone 840S (バーコードスキャナ付き)		5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	4 12 5	100 ~ 144 149、153、 157、161、165

CP-860	Cisco Wireless Phone 860	2.4 GHz = 0.6 dBi 5 GHz = 0.8 dBi	2.412 ~	13	1 ~ 13
			2.472 GHz	4	36、40、44、48
CP-860S	Cisco Wireless Phone 860S (バーコードスキャナ付き)		5.180 ~	4	52、56、60、64
			5.240 GHz	12	100 ~ 144
			5.260 ~	5	149、153、 157、161、165
			5.320 GHz		
			5.500 ~		
			5.720 GHz		
5.745 ~					
		5.825 GHz			

注：実際に使用されるチャンネルは、地域の規制によって異なります。

要件

Cisco Wireless Phone 840 および 860 は、音声通信を提供する IEEE 802.11a/b/g/n/ac デバイスです。

Cisco Wireless Phone 840 および 860 の導入に必要な要件が満たされていることを確認するには、環境の検証が必要です。

サイト調査

Cisco Wireless Phone 840 および 860 を実稼働環境に導入する前に、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によって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 周波数帯を分析して、対象帯域（5 GHz または 2.4 GHz）内で使用可能なチャン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ン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 Wireless Phone 840 および 860 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（チャンネルと送信電力）も決定されます。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推奨します。

Cisco Wireless Phone 840 および 860 の導入に必要な要件が満たされていることを確認するには、ワイヤレス LAN の検証が必要です。

電波状態表示

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間に 20 ~ 30 % のオーバーラップを維持する必要があります。

これにより、Cisco Wireless Phone 840 および 860 で十分な強さの信号が維持されます。パケット損失のトリガーではなく信号ベースのトリガーが利用されている環境では、シームレスにローミングするのに十分な時間信号を保持できます。

また、Cisco Wireless Phone 840 および 860 からのアップストリーム信号が、送信データレートに関するアクセスポイントの受信感度に適合している必要もあります。基本的な要件として、アクセスポイントの受信信号は -67 dBm 以上になるように設定してください。

セルサイズは、Cisco Wireless Phone 840 および 860 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。

チャンネルの使用率

チャン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。

ノイズ

ノイズレベルは -92 dBm を超過しないようにします。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) が実現します。

また、Cisco Wireless Phone 840 および 860 からのアップストリーム信号が、送信データレートに関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

音声ガイドラインによると、パケット損失は 1 % を超過しない必要があります。1 % を超過すると、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 (100 ms 未満) に維持される必要があります。

再試行回数

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、最小限に維持する必要があります。

コール制御

Cisco Wireless Phone 840 および 860 は、次のコール制御プラットフォームでサポートされています。

- Cisco Unified Communications Manager (CUCM)
最小 = 11.5(1)
推奨 = 12.5(1)、14.0(1) 以降
- Cisco Unified Survivable Remote Site Telephony (SRST)
最小 = 14.1
推奨 = 14.3 以降
- Webex Calling

注： Cisco Unified Communications Manager では、Cisco Wireless Phone 840 および 860 デバイスのサポートを有効にするために、デバイスパッケージまたはサービス リリース アップデートのインストールが必要です。

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。

<https://software.cisco.com/download/home/278875240>

ワイヤレス LAN

Cisco Wireless Phone 840 および 860 は、次のシスコ ワイヤレス LAN ソリューションでサポートされています。

- Cisco AireOS ワイヤレス LAN コントローラおよび Cisco Lightweight アクセスポイント
最小 = 8.3.143.0
推奨 = 8.3.150.0、8.5.182.0、8.8.130.0、8.10.183.0
- Cisco Catalyst IOS XE ワイヤレス LAN コントローラおよび Cisco Lightweight アクセスポイント
最小 = 16.12.1 秒
推奨 = 17.3.6、17.6.4、17.9.3、17.11.1
- Cisco Mobility Express および Cisco Lightweight アクセスポイント
最小 = 8.3.143.0
推奨 = 8.3.150.0、8.5.182.0、8.8.130.0、8.10.183.0
- Cisco Autonomous (自律) アクセス ポイント
最小 = 15.2(4)JB6
推奨 = 15.3(3)JPO

- Cisco Meraki アクセスポイント

最小 = MR 25.9、MX 13.33

推奨 = MR 29.5.1、MX 17.10.2

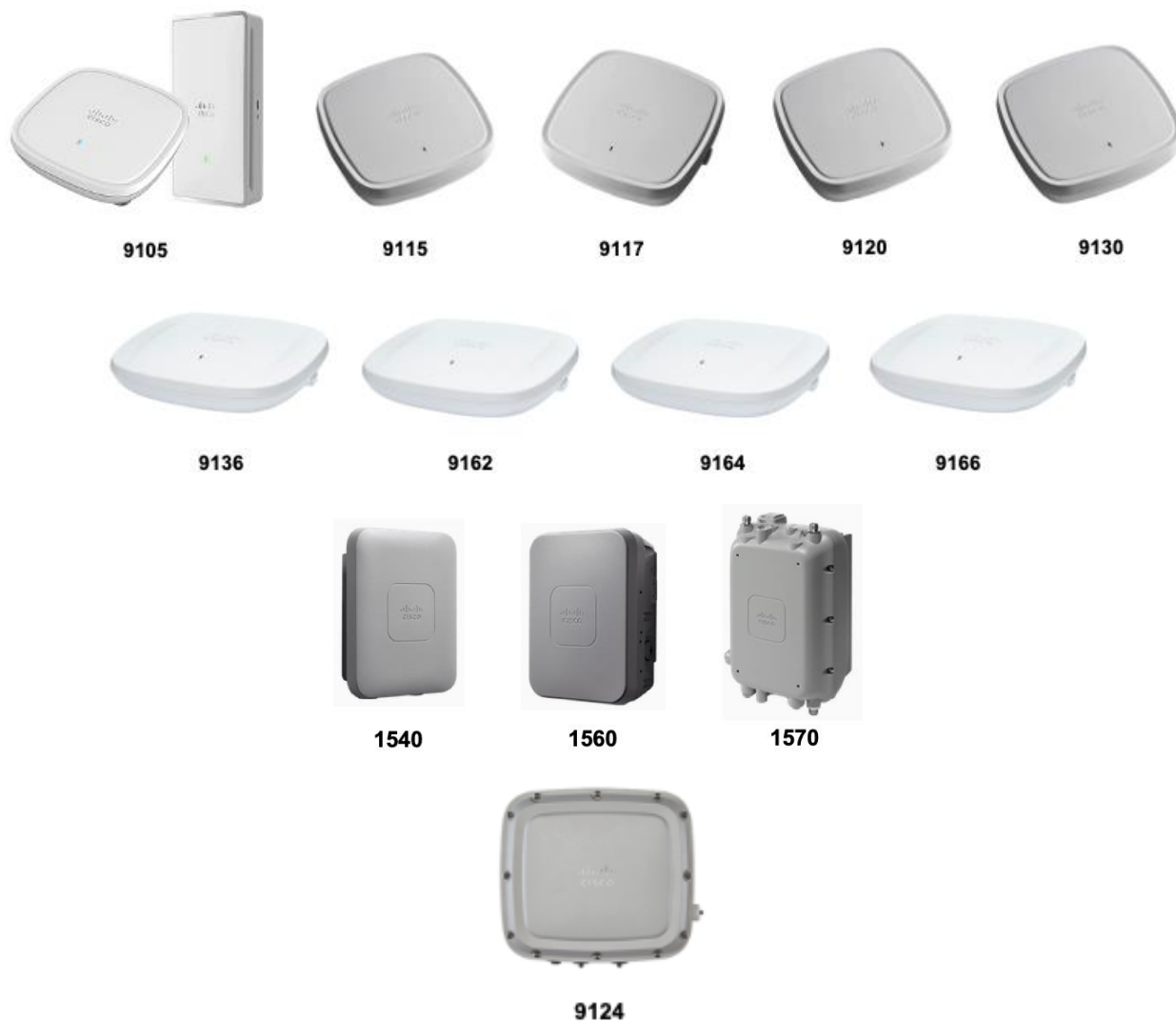
アクセスポイント

サポートされるシスコのアクセスポイントを以下に示します。

一覧にないアクセスポイントモデルはサポートされません。

Cisco Wireless Phone 840 および 860 は、次の Cisco Aironet アクセスポイント プラットフォームでサポートされます。





次の表に、各 Cisco Aironet 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	802.11ax	軽量	Mobility Express	自律型
1540	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1560	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1570	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
1700	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
1810	はい	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
1810W	はい	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ

1815	はい	はい	はい	はい	はい	いいえ	はい	はい (1815t ではありません)	いいえ
1830	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1840	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1850	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
2700	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
2800	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
3700	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
3800	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
4800	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
9105	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9115	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9117	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9120	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9124	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9130	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9136	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9162	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9164	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9166	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ

Cisco Wireless IP Phone 840 および 860 は、次の Cisco Meraki アクセス ポイント プラットフォームでサポートされます。



MR20



MR28



MR30H



MR32



MR33



MR34



MR36



MR36H



MR42



MR44



MR45



MR46



MR52



MR53



MR55



MR56



MR57



MR70



MR74



MR76



MR78



MR84



MR86



MX64W



MX65W



MX67W



MX68W



Z3

<https://meraki.cisco.com/products/wireless#models>

<https://meraki.cisco.com/products/appliances#models>

次の表に、各 Cisco Meraki アクセスポイントでサポートされるモードを示します。

Meraki AP シリーズ	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
MR20	はい	はい	はい	はい	はい	いいえ
MR28	はい	はい	はい	はい	はい	はい
MR30H	はい	はい	はい	はい	はい	いいえ
MR32	はい	はい	はい	はい	はい	いいえ
MR33	はい	はい	はい	はい	はい	いいえ
MR34	はい	はい	はい	はい	はい	いいえ
MR36	はい	はい	はい	はい	はい	はい
MR36H	はい	はい	はい	はい	はい	はい
MR42	はい	はい	はい	はい	はい	いいえ
MR44	はい	はい	はい	はい	はい	はい

MR45	はい	はい	はい	はい	はい	はい
MR46	はい	はい	はい	はい	はい	はい
MR52	はい	はい	はい	はい	はい	いいえ
MR53	はい	はい	はい	はい	はい	いいえ
MR55	はい	はい	はい	はい	はい	はい
MR56	はい	はい	はい	はい	はい	はい
MR57	はい	はい	はい	はい	はい	はい
MR70	はい	はい	はい	はい	はい	いいえ
MR74	はい	はい	はい	はい	はい	いいえ
MR76	はい	はい	はい	はい	はい	はい
MR78	はい	はい	はい	はい	はい	はい
MR84	はい	はい	はい	はい	はい	いいえ
MR86	はい	はい	はい	はい	はい	はい
MX64W	はい	はい	はい	はい	はい	いいえ
MX65W	はい	はい	はい	はい	はい	いいえ
MX67W	はい	はい	はい	はい	はい	いいえ
MX68W	はい	はい	はい	はい	はい	いいえ
Z3	はい	はい	はい	はい	はい	いいえ

注：上に明記されていないアクセスポイントモデルはサポートされません。

Cisco Aironet 1500 シリーズ屋外アクセスポイントのサポートは、ローカル アクセス ポイント モードのみに制限されています。

MESH モードで動作するアクセスポイントモデルはサポートされません。

サードパーティのアクセスポイントに対して相互運用性テストが実行されていないため、サードパーティのアクセスポイントとの相互運用性は保証できません。ただし、Wi-Fi 準拠のアクセスポイントに接続している場合は、基本的な機能が重要です。

主な機能の一部を以下に示します。

- 5 GHz (802.11a/n/ac)
- Wi-Fi Protected Access v2 (WPA2+AES)
- Wi-Fi マルチメディア (WMM)
- Traffic Specification (TSPEC)
- DiffServ コードポイント (DSCP)
- サービスクラス (CoS/802.1p)

アンテナシステム

一部の Cisco アクセスポイントでは、外部アンテナが必須または使用可能です。

Cisco Aironet アクセスポイントでサポートされる外部アンテナのリストとの設置方法については、次の URL を参照してください。

https://www.cisco.com/c/ja_ip/products/collateral/wireless/aironet-antennas-accessories/product_data_sheet09186a008008883b.html

注：一体型内部アンテナを搭載したアクセスポイント（壁取り付け用モデルを除く）は、無指向性アンテナを装備しており、壁面への設置を想定していないため、天井に取り付ける必要があります。

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。

- 802.11a, b, d, e, g, h, i, n, r, ac
- Wi-Fi マルチメディア (WMM)
- Traffic Specification (TSPEC)
- 不定期自動省電力配信 (UAPSD)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
 - Opus, G.722, G.711, G.729
- Dynamic Host Configuration Protocol (DHCP)
- HyperText Transfer Protocol (HTTP/HTTPS)

Wi-Fi

次の表に、Cisco Wireless Phone 840 および 860 で使用される 802.11 モードごとの最大送信電力とデータレートを示します。

Cisco Wireless Phone 840

5 GHz の仕様

5 GHz - 802.11a	データレート	空間スト リーム	変調
最大 Tx パワー = 16 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
5 GHz - 802.11n (HT20)	データレート	空間スト リーム	変調
最大 Tx パワー = 16 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM

	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbp (MCS 13)	2	OFDM - 64 QAM
	130 Mbp (MCS 14)	2	OFDM - 64 QAM
	144 Mbp (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 15 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	30 Mbps (MCS 8)	2	OFDM - BPSK
	60 Mbps (MCS 9)	2	OFDM - QPSK
	90 Mbps (MCS 10)	2	OFDM - QPSK
	120 Mbps (MCS 11)	2	OFDM - 16 QAM
	180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM
	270 Mbps (MCS 14)	2	OFDM - 64 QAM
	300 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11ac (VHT20)	データレート	空間ストリーム	変調
最大 Tx パワー = 16 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM

	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	87 Mbps (MCS 8)	1	OFDM - 256 QAM
	14 Mbps (MCS 0)	2	OFDM - BPSK
	28 Mbps (MCS 1)	2	OFDM - QPSK
	43 Mbps (MCS 2)	2	OFDM - QPSK
	58 Mbps (MCS 3)	2	OFDM - 16 QAM
	87 Mbps (MCS 4)	2	OFDM - 16 QAM
	116 Mbps (MCS 5)	2	OFDM - 64 QAM
	130 Mbps (MCS 6)	2	OFDM - 64 QAM
	144 Mbps (MCS 7)	2	OFDM - 64 QAM
	173 Mbps (MCS 8)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 15 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM
	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
300 Mbps (MCS 7)	2	OFDM - 64 QAM	

	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)	データレート	空間ストリーム	変調
最大 Tx パワー = 14 dBm (地域によって異なる)	33 Mbps (MCS 0)	1	OFDM - BPSK
	65 Mbps (MCS 1)	1	OFDM - QPSK
	98 Mbps (MCS 2)	1	OFDM - QPSK
	130 Mbps (MCS 3)	1	OFDM - 16 QAM
	195 Mbps (MCS 4)	1	OFDM - 16 QAM
	260 Mbps (MCS 5)	1	OFDM - 64 QAM
	293 Mbps (MCS 6)	1	OFDM - 64 QAM
	325 Mbps (MCS 7)	1	OFDM - 64 QAM
	390 Mbps (MCS 8)	1	OFDM - 256 QAM
	433 Mbps (MCS 9)	1	OFDM - 256 QAM
	65 Mbps (MCS 0)	2	OFDM - BPSK
	130 Mbps (MCS 1)	2	OFDM - QPSK
	195 Mbps (MCS 2)	2	OFDM - QPSK
	260 Mbps (MCS 3)	2	OFDM - 16 QAM
	390 Mbps (MCS 4)	2	OFDM - 16 QAM
	520 Mbps (MCS 5)	2	OFDM - 64 QAM
	585 Mbps (MCS 6)	2	OFDM - 64 QAM
	650 Mbps (MCS 7)	2	OFDM - 64 QAM
	780 Mbps (MCS 8)	2	OFDM - 256 QAM
	867 Mbps (MCS 9)	2	OFDM - 256 QAM

2.4 GHz の仕様

2.4 GHz - 802.11b	データレート	空間ストリーム	変調
最大 Tx パワー = 19 dBm (地域によって異なる)	1 Mbps	1	DSSS - BPSK
	2 Mbps	1	DSSS - QPSK
	5.5 Mbps	1	DSSS - CCK
	11 Mbps	1	DSSS - CCK
2.4 GHz - 802.11g	データレート	空間ストリーム	変調
最大 Tx パワー = 18 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
2.4 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
最大 Tx パワー = 18 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK

	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM

Cisco Wireless Phone 860

5 GHz の仕様

5 GHz - 802.11a	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
5 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK

	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM

	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	30 Mbps (MCS 8)	2	OFDM - BPSK
	60 Mbps (MCS 9)	2	OFDM - QPSK
	90 Mbps (MCS 10)	2	OFDM - QPSK
	120 Mbps (MCS 11)	2	OFDM - 16 QAM
	180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM
	270 Mbps (MCS 14)	2	OFDM - 64 QAM
	300 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11ac (VHT20)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM

	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	87 Mbps (MCS 8)	1	OFDM - 256 QAM
	14 Mbps (MCS 0)	2	OFDM - BPSK
	28 Mbps (MCS 1)	2	OFDM - QPSK
	43 Mbps (MCS 2)	2	OFDM - QPSK
	58 Mbps (MCS 3)	2	OFDM - 16 QAM
	87 Mbps (MCS 4)	2	OFDM - 16 QAM
	116 Mbps (MCS 5)	2	OFDM - 64 QAM
	130 Mbps (MCS 6)	2	OFDM - 64 QAM
	144 Mbps (MCS 7)	2	OFDM - 64 QAM
	173 Mbps (MCS 8)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM

	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM
	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
	300 Mbps (MCS 7)	2	OFDM - 64 QAM
	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	33 Mbps (MCS 0)	1	OFDM - BPSK
	65 Mbps (MCS 1)	1	OFDM - QPSK
	98 Mbps (MCS 2)	1	OFDM - QPSK
	130 Mbps (MCS 3)	1	OFDM - 16 QAM

	195 Mbps (MCS 4)	1	OFDM - 16 QAM
	260 Mbps (MCS 5)	1	OFDM - 64 QAM
	293 Mbps (MCS 6)	1	OFDM - 64 QAM
	325 Mbps (MCS 7)	1	OFDM - 64 QAM
	390 Mbps (MCS 8)	1	OFDM - 256 QAM
	433 Mbps (MCS 9)	1	OFDM - 256 QAM
	65 Mbps (MCS 0)	2	OFDM - BPSK
	130 Mbps (MCS 1)	2	OFDM - QPSK
	195 Mbps (MCS 2)	2	OFDM - QPSK
	260 Mbps (MCS 3)	2	OFDM - 16 QAM
	390 Mbps (MCS 4)	2	OFDM - 16 QAM
	520 Mbps (MCS 5)	2	OFDM - 64 QAM
	585 Mbps (MCS 6)	2	OFDM - 64 QAM
	650 Mbps (MCS 7)	2	OFDM - 64 QAM
	780 Mbps (MCS 8)	2	OFDM - 256 QAM
	867 Mbps (MCS 9)	2	OFDM - 256 QAM

2.4 GHz の仕様

2.4 GHz - 802.11b	データレート	空間ストリーム	変調
最大 Tx パワー = 19 dBm (地域によって異なる)	1 Mbps	1	DSSS - BPSK
	2 Mbps	1	DSSS - QPSK
	5.5 Mbps	1	DSSS - CCK
	11 Mbps	1	DSSS - CCK
2.4 GHz - 802.11g	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
2.4 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
最大 Tx パワー = 16 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK

	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM

注：802.11n/ac 接続を実現するには、Cisco Wireless Phone 840 および 860 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。

規格

ワールドモード (802.11d) 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ダプタイズされるチャン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 Wireless Phone 840 および 860 は、アクセスポイントが 802.11d に対応していて、地域ごとに使用するチャンネルと送信電力を決定できる場合に最適に動作します。

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 チャンネルはレーダー技術でも使用されており、該当レーダー周波数 (DFS チャンネル) を使用するには、802.11 クライアントとアクセスポイントが 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 Wireless Phone 840 および 860 は、まず DFS チャンネルをパッシブにスキャンし、その後でアクティブにスキャンします。

802.11d が有効になっていない場合、Cisco Wireless Phone 840 および 860 は、少ない送信電力でアクセスポイントへの接続を試みることができます。

次に、Cisco Wireless Phone 840 および 860 でサポートされる国とその 802.11d コードを示します。

オーストラリア (AU)	ギリシャ (GR)	ポーランド (PL)
オーストリア (AT)	ハンガリー (HU)	ポルトガル (PT)
ベルギー (BE)	アイスランド (IS)	ルーマニア (RO)
ブルガリア (BG)	アイルランド (IE)	スロバキア (SK)
カナダ (CA)	イタリア (IT)	スロベニア (SI)
クロアチア (HR)	ラトビア (LV)	スペイン (ES)
キプロス (CY)	リヒテンシュタイン (LI)	スウェーデン (SE)
チェコ共和国 (CZ)	リトアニア (LT)	スイス (CH)
デンマーク (DK)	ルクセンブルク (LU)	トルコ (TR)
エストニア (EE)	マルタ (MT)	イギリス (GB)
フィンランド (FI)	オランダ (NL)	アメリカ合衆国 (US)
フランス (FR)	ニュージーランド (NZ)	
ドイツ (DE)	ノルウェー (NO)	

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。

<https://cae-cnc-prd.cisco.com/pdtncc>

Bluetooth

Cisco Wireless Phone 840 および 860 は、ワイヤレスヘッドセット通信を可能にする Bluetooth テクノロジーをサポートします。

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。ただし、Bluetooth デバイスは、常に Cisco Wireless Phone 840 および 860 から約 3 m (10 フィート) 以内で使用することを推奨します。

Bluetooth デバイスは、電話機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と、品質に悪影響を及ぼす可能性があります。

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 Wireless Phone 840 および 860 は、次の Bluetooth プロファイルをサポートしています。

- 高度なオーディオ配信プロファイル (A2DP)
- 属性プロファイル (ATT)
- オーディオ / ビデオリモート制御プロファイル (AVRCP)
- デバイス ID プロファイル (DIP)
- 汎用アクセスプロファイル (GAP)
- 汎用属性プロファイル (GATT)
- 汎用オーディオ/ビデオ配信プロファイル (GAVDP)
- ハンズフリープロファイル (HFP)
- ヘッドセットプロファイル (HSP)
- ヒューマン インターフェイス デバイス プロファイル (HID)
- HID over GATT プロファイル (HOGP)
- メッセージ アクセス プロファイル (MAP)
- オブジェクト プッシュ プロファイル (OPP)
- パーソナル エリア ネットワーク プロファイル (PAN)
- 電話帳アクセス プロファイル (PBAP)
- スキャン パラメータ プロファイル (ScPP)
- シリアルポートプロファイル (SPP)
- サービス検出アプリケーション プロファイル (SDAP)

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、いくつかの制限と導入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、802.11g/n と Bluetooth の送受信を保護する CTS の利用により、コールキャパシティが減少します。

マルチキャストオーディオ

共存を使用する場合、プッシュトゥートーク (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、共存モードの使用時に 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 を有効にする必要があります。

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 を使用する場合には 802.11a/n/ac を使用することを推奨します。

言語

Cisco Wireless Phone 840 および 860 は現在、次の言語をサポートしています。

デンマーク語	ドイツ語	ロシア語
オランダ語	ハンガリー語	スロベニア語
英語	イタリア語	スペイン語
フィンランド語	ノルウェー語	スウェーデン語
フランス語	ポルトガル語	

バッテリー寿命

Cisco Wireless Phone 840 には 3040 mAh のバッテリーが搭載され、Cisco Wireless Phone 860 には 3000 mAh のバッテリーが搭載されています。

Cisco Wireless Phone 840 および 860 のバッテリー容量は、500 回のフル充電サイクル（空の状態からフル充電）後に 80% 以下になるため、Cisco Wireless Phone 840 および 860 のバッテリーは約 2 年ごとに交換することをお勧めします。

Cisco Wireless Phone 860 はホットスワップ可能なバッテリー機能をサポートしており、最大 60 秒でバッテリーを交換できます。Cisco Wireless Phone 840 にはホットスワップ可能なバッテリー機能は含まれていません。

次の表に、電話機のモデルごとの最大通話時間とアイドル時間を示します。

電話機のモデル	コール状態	バッテリー時間
840 / 840S	通話時	最大 17 時間
	アイドル	最大 168 時間
860 / 860S	通話時	最大 12 時間
	アイドル	最大 120 時間

実際のバッテリー持続時間には、さまざまな要因が影響します。

使用方法

Cisco Wireless Phone 840 または 860 のユーザーが通話中か、ローミング中か、ディスプレイをオンにしているか、Bluetooth やアプリケーションを使用しているか、メッセージを受信しているか、電話機のメニューを操作していると、バッテリー持続時間が短くなります。

カバレッジ

Cisco Wireless Phone 840 および 860 が適切な RF カバレッジエリア内にあり、通話サーバーへの常時接続を維持できることを確認してください。

Cisco Wireless Phone 840 および 860 のユーザーがカバレッジエリア外で長時間とどまっていると、バッテリー持続時間が短くなることがあります。

プロキシ ARP

アイドル時のバッテリー持続時間を最適化するために、プロキシ ARP 機能をサポートするアクセスポイントを使用することを推奨します。Cisco Wireless Phone 840 および 860 でプロキシ ARP を使用すると、DTIM 周期のたびに起動する必要がなくなり、サスペンドモードをより長く維持できるため、消費電力が低減されます。

アクセスポイントがプロキシ ARP をサポートしていない場合、Cisco Wireless Phone 840 および 860 では DTIM 周期のたびに起動が必要になります。これにより、バッテリー持続時間が最大 50 % 短くなります。

送信電力

Cisco Compatible Extensions (CCX) ダイナミック伝送パワーコントロール (DTPC) 機能をサポートするアクセスポイントを使用することを推奨します。DTPC が有効になっている場合、アクセスポイントはその送信電力をすべてのクライアントにアダプタイズします。これにより、Cisco Wireless Phone 840 および 860 は、接続先のアクセスポイントとの通信に最小限必要なレベルまで送信電力を調整できます。また、これによって他のエリアの不要なノイズも減少します。

マルチキャスト

Cisco Wireless Phone 840 または 860 がマルチキャストストリームにサブスクライブしている場合、Cisco Wireless Phone 840 または 860 は DTIM 周期のたびに起動し、マルチキャストフレームを受信する必要があります。このため、電力消費量が増大します。

省電力プロトコル

アクセスポイントは、通話時やアイドル時に使用される省電力プロトコルである U-APSD をサポートしている必要があります。

840S および 860S バーコードスキャナ

Cisco Wireless Phone 840S および 860S には、2D バーコードスキャナが搭載されています。スキャナを呼び出すには、Android アプリケーションが必要です。

Cisco Wireless Phone 840S および 860S は、次のバーコード記号をサポートしています。

- Aztec、CCA EAN-128、CCA EAN-13、CCA EAN-8、CCA GS1 DataBar Expanded、CCA GS1 DataBar Limited、CCA GS1 DataBar-14、CCA UPC-A、CCA UPC-E、CCB EAN-128、CCB EAN-13、CCB EAN-8、CCB GS1 DataBar Expanded、CCB GS1 DataBar Limited、CCB GS1 DataBar-14、CCB UPC-A、CCB UPC-E、CCC EAN-128、Codabar、Code 11、Code 128、Code 32、Code 39 Full ASCII、Code 39 Trioptic、Code 93、DataMatrix、Discrete (Standard) 2 of 5、EAN-128、EAN-13、EAN-13 + 2 Supplemental、EAN-13 + 5 supplemental、EAN-8、EAN-8 + 2 Supplemental、EAN-8 + 5 supplemental、GS1 DataBar Expanded、GS1 DataBar Limited、GS1 DataBar-14、Han Xin、Interleaved 2 of 5、ISBT-128、ISBT-128 Con、Macro Micro PDF、Macro PDF、Macro QR、Matrix 2 of 5、Micro PDF、Micro QR、MSI、PDF-417、QR Code、UPC-A、UPC-A + 2 Supplemental、UPC-A + 5 supplemental、UPC-E0、UPC-E0 + 2 Supplemental、UPC-E0 + 5 supplemental

詳細については、次の URL にある『**Cisco Wireless Phone 840 および 860 アドミニストレーションガイド**』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipp/800-series/adminguide/w800_b_wireless-800-administration-guide.html

電話機のお手入れ

Cisco Wireless Phone 840 は、IP65 等級の防塵、防滴、防湿性能があります。Cisco Wireless Phone 860 は、IP68 等級の完全な防塵性能を備えています。

通常の清掃の場合は、柔らかい湿った布で電話機を拭くだけでかまいません。

完全にクリーニングするには、過酸化水素水（最大 3%）またはイソプロピル アルコール溶液（最大 91%）を使用することを推奨します。

ブリーチ液（最大 10%）も使用できます。ただし、金属製の充電接点のクリーニングには使用しないでください。

これより多量の純粋なイソプロパノールや、代替となるアルコール ベースの液体が含まれるクリーニング液は、電話機を傷つける可能性があります。

キャリー ケースを使用すると、電話機の保護をさらに強化し、電話機を落とした場合にも保護されます。

詳細については、次の URL にある『Cisco Wireless Phone 840 および 860 ユーザーガイド』を参照してください。

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html

アクセサリ

Cisco Wireless Phone 840 および 860 では、次のアクセサリを使用できます。

- バッテリー
- 電話機の電源
- キャリーケース
- ベルトクリップ
- デスクトップチャージャー
- マルチ充電器
- ストラップ (840 のみ)
- スキャナハンドル (840S のみ)

840 充電器



860 充電器



詳細については、『Cisco Wireless Phone 840 および 860 アドミニストレーション ガイド』または『Cisco Wireless Phone 840 および 860 ユーザーガイド』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html

注：シスコでは、Cisco Wireless Phone 840 または 860 のサードパーティ製ケースまたはカバーを推奨、サポート、またはテストしていません。Cisco Wireless Phone 840 または 860 でサードパーティ製のケースまたはカバーを使用した場合、保証が無効となる場合があります。

無線 LAN の設計

Cisco Wireless Phone 840 および 860 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は、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。

802.11 ネットワーク

次のガイドラインに従ってワイヤレス LAN を導入し、設定します。

5 GHz (802.11a/n/ac)

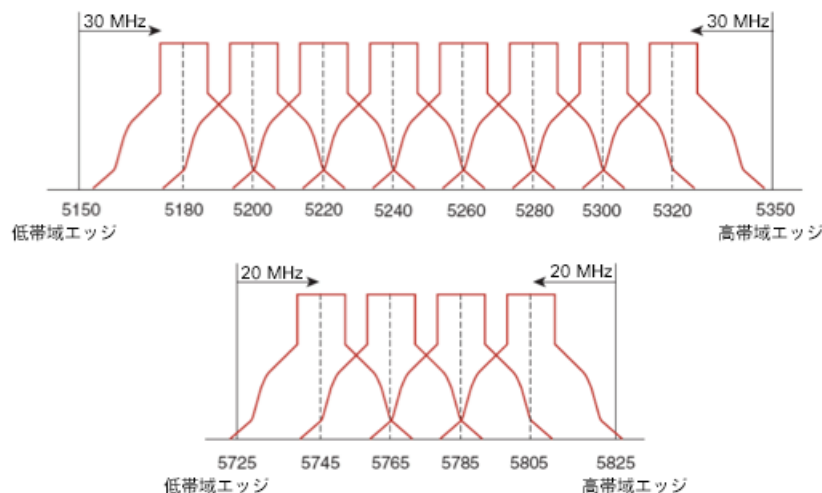
Cisco Wireless Phone 840 および 860 の運用では、5 GHz の周波数帯域を使用することを推奨します。

通常は、アクセスポイントに手動でチャンネルを割り当てる代わりに、アクセスポイントで自動チャンネル選択を使用することを推奨します。

断続的な干渉源が存在する場合は、そのエリアにサービスを提供しているアクセスポイントにチャンネルを静的に割り当てる必要があります。

Cisco Wireless Phone 840 および 860 は、802.11h の動的周波数選択 (DFS) と伝送パワーコントロール (TPC) をサポートします。これらは、5.260 ~ 5.720 GHz で動作するチャンネルを使用する場合に必要です。使用可能な 25 チャンネルのうち 16 チャンネルがこれに該当します。

802.11a/n/ac 環境に Cisco Wireless Phone 840 および 860 を導入する場合は、隣接するチャンネルと 20 % 以上オーバーラップさせる必要があります。これにより、シームレスなローミングが実現します。重要なエリアでは、Cisco Wireless Phone 840 および 860 がアクセスポイントの受信感度 (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 か所のアクセスポイントで -67 dBm 以上の信号レベルを確保できるように、オーバーラップを増やす (30% 以上) ことを推奨します。



チャンネル ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
中心周波数 MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805
帯域	UNII-1				UNII-2																UNII-3		

動的周波数選択 (DFS)

DFS は、レーダー信号を検出すると、トランスミッタに対して他のチャンネルにスイッチするように動的に指示します。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ン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るため、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、クライアントが隣接セルの干渉原になる可能性が低下するため、より密集したパフォーマンスの高いワイヤレス LAN を実現できます。

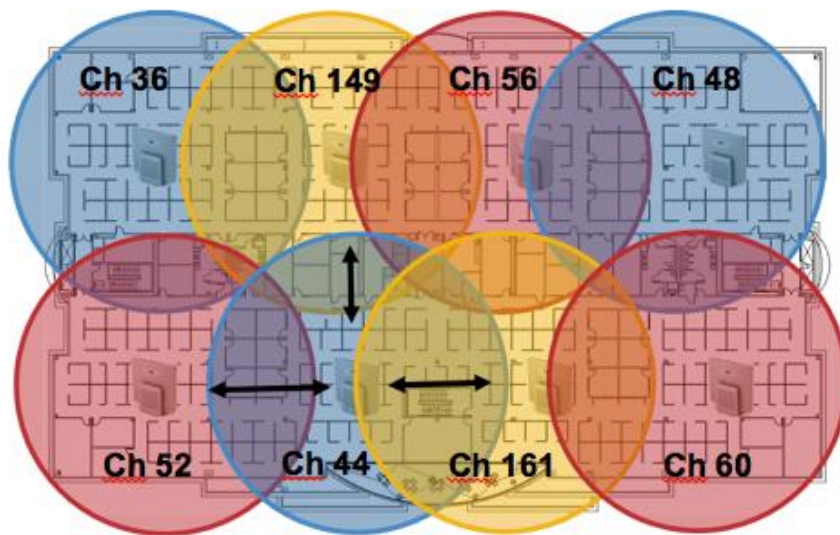
アクセスポイントでレーダーイベントが繰り返し検出される場合（誤検出も含む）、レーダー信号が単一チャンネル（ナローバンド）または複数のチャンネル（ワイドバンド）に影響を与えているかどうかを特定し、ワイヤレス LAN における該当チャンネルの使用を無効にします。

非 DFS チャンネルにアクセスポイントが存在する場合は、音声の中断を最小限に抑えられます。

レーダーアクティビティに備えて、非 DFS チャンネル（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ン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ンネルを使用できます。

UNII-3 チャンネル（5.745 ~ 5.825 GHz）は（利用可能であれば）任意で使用できます。

次に、5 GHz ワイヤレス LAN の導入例を示します。



最小 20% のオーバーラップ

5 GHz の場合、南・北・中央アメリカでは 25 チャンネル、欧州では 16 チャンネル、日本では 19 チャン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 を使用して 12 チャンネル セットを利用することが推奨されます。

UNII-2 拡張チャンネル（チャンネル 100 ~ 144）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（チャンネル 52 ~ 64）を無効にして、有効になるチャン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 チャンネルを有効にすると、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)

通常は、アクセス ポイントに手動でチャンネルを割り当てる代わりに、アクセス ポイントで自動チャンネル選択を使用することを推奨します。

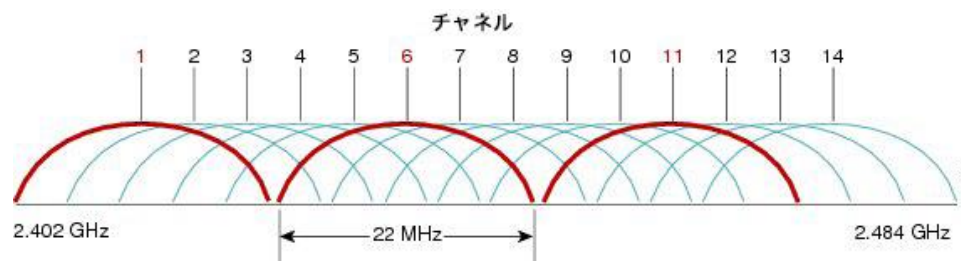
断続的な干渉源が存在する場合は、そのエリアにサービスを提供しているアクセス ポイントにチャンネルを静的に割り当てる必要があります。

2.4 GHz (802.11b/g/n) 環境では、VoWLAN を導入するとき、オーバーラップのないチャン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ンネルには 22 MHz の間隔があり、少なくとも 5 チャンネル離れています。

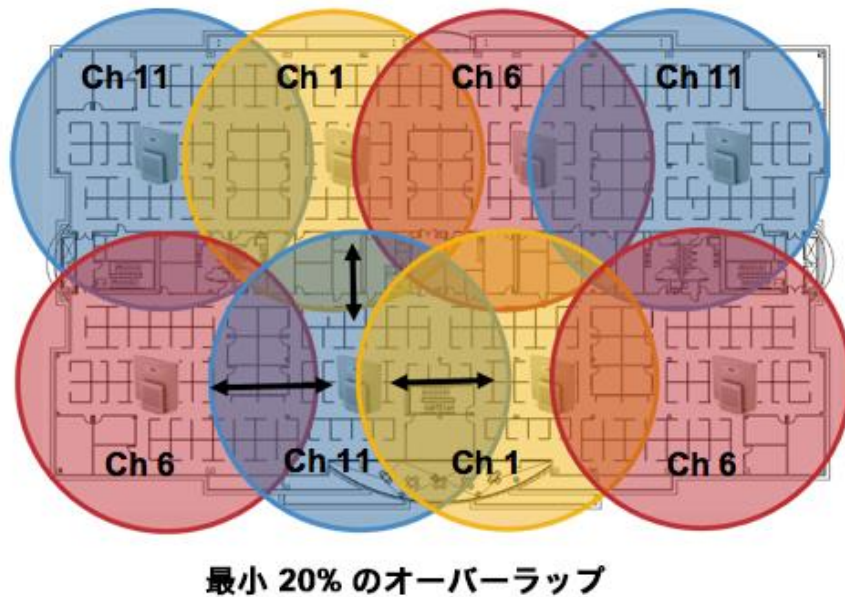
2.4 GHz 周波数範囲には、オーバーラップのないチャンネルは 3 つしか存在しません（チャンネル 1、6、11）。

802.11b/g/n 環境に Cisco Wireless Phone 840 および 860 を導入する場合は、オーバーラップのないチャンネルを使用する必要があり、隣接チャン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 チャンネル セットの使用は、サポートされていない設定です。



次に、2.4 GHz ワイヤレス LAN の導入例を示します。



信号強度とカバレッジ

Cisco Wireless Phone 840 および 860 で最低限の音声品質を確保するには、5 GHz または 2.4 GHz で常に -67 dBm 以上の信号レベルを保持する必要があります。アクセスポイントの受信感度については、送信データレートに対して要求される信号レベルも満たしている必要があります。

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

少なくとも 25 dB の信号対雑音比 (SNR) 、つまり -67 dBm の信号に対して -92 dBm のノイズレベルを維持する必要があります。

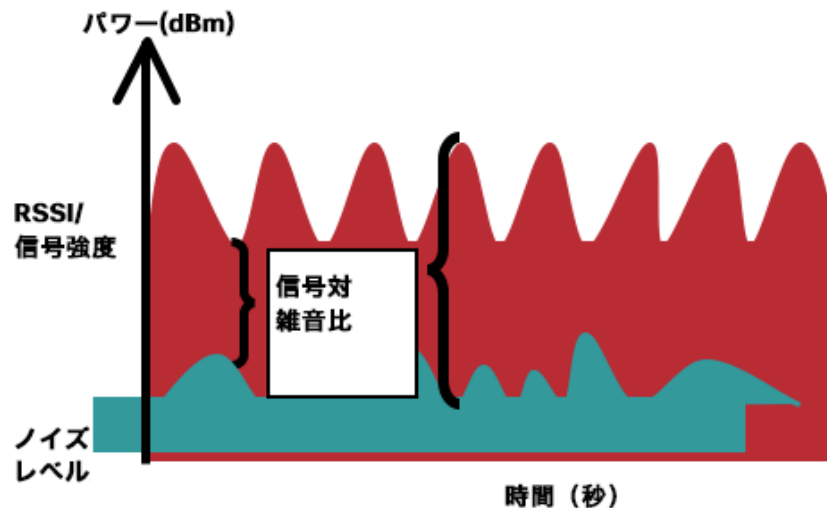
冗長性を持たせるために、オーバーラップのないチャンネル上に SNR が 25 dB の最低でも -67 dBm の信号を持つアクセスポイントを 2 つ以上設置することが推奨されます。

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を活用できる音声専用以外のアプリケーションに関して、そのような高いデータレートを任意で有効にすることもできます。

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、唯一の必須/基本レートとして設定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 を有効する必要があります。

上記の各要件を考慮すると、シングルチャンネル計画は導入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には、必ず、すべての重要エリアが適切にカバー（信号が到達）されるようにしてください。

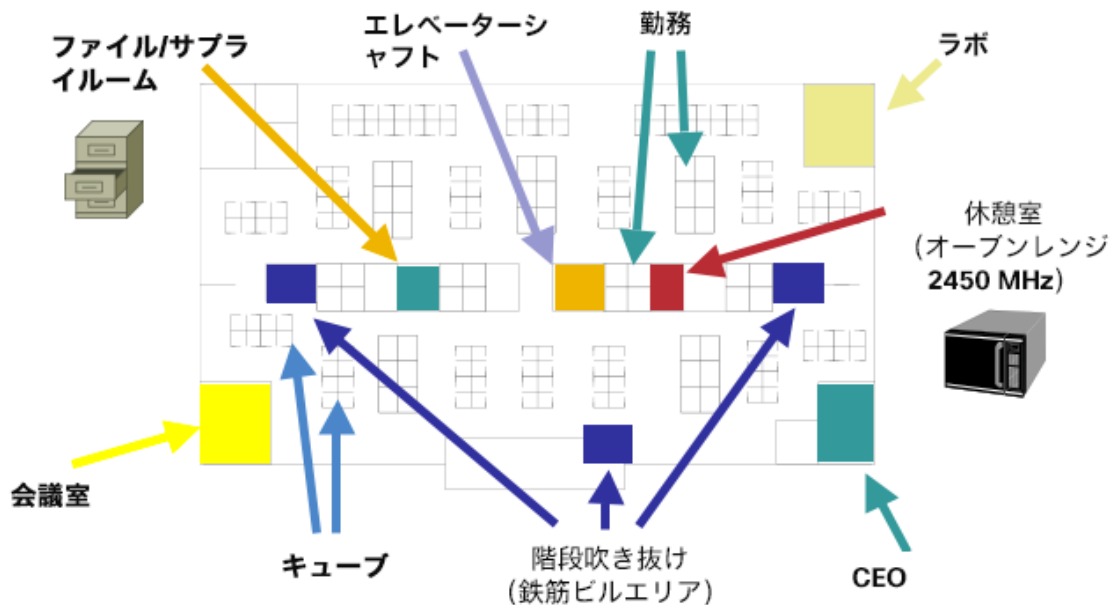
データ専用アプリケーションのための一般的なワイヤレス LAN 導入では、エレベータ、階段、屋外通路といった、VoWLAN サービスで必要とされる一部のエリアにはカバレッジが提供されません。

電子レンジ、2.4 GHz コードレス電話、Bluetooth デバイス、および 2.4 GHz 帯で動作する他の電子機器は、ワイヤレス LAN に干渉します。

電子レンジは、2450 MHz で動作します。これは、802.11b/g/n のチャンネル 8 と 9 の間に位置します。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、エネルギーの拡散が低減されています。電子レンジのエネルギーは、チャンネル 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（チャンネル 1 ~ 11）に影響します。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、チャンネル 1 を使用してください。

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 周波数に対しても同様の悪影響を与えることはありません。802.11a/n/ac テクノロジーでは、オーバーラップのないチャンネルが増えるため、通常はより低い初期 RF 使用率となります。音声導入の場合、音声には 802.11a/n/ac を使用し、データには 802.11b/g/n を使用することを推奨します。

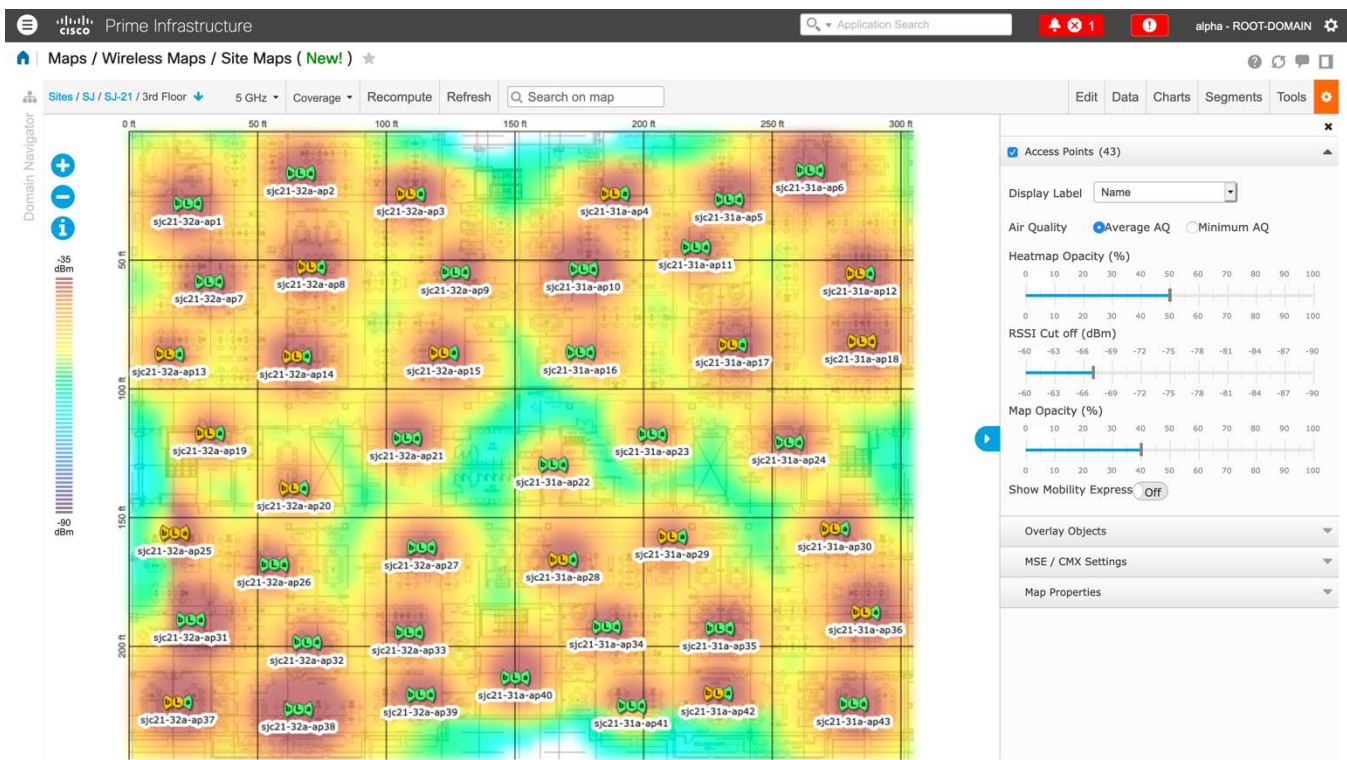
ただし、免許申請の必要のない 5 GHz 周波数を利用する製品も存在します（たとえば、5.8 GHz コードレス電話機も、UNII-3 チャンネルに悪影響を及ぼす可能性があります）。



下のチャートは、環境に存在する可能性のあるさまざまな物質の減衰レベルを示しています。

材料	Advertised Attenuation Level
ウッド	低
レンガ	中規模
具体的	High
金属	非常に高い

Cisco Prime Infrastructure 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

最良の結果を得るにはキャパシティと範囲が重要な要因となるため、5 GHz 導入の場合は 12 Mbps 未満のレートを、2.4 GHz 導入の場合は 12 Mbps 未満のレートを無効にすることをお勧めします。

Cisco Wireless Phone 840 および 860 には、両方ともデュアルアンテナがあるため、802.11n (最大 300 Mbps) の最大 MCS 15 データレートをサポートします。

802.11ac の場合、Cisco Wireless Phone 840 および 860 は、最大 VHT80 MCS 9 2SS データレート (最大 867 Mbps) をサポートします。

これより高い MCS レートを使用できる、同じ帯域周波数を使って 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/ac クライアント向けに、より高いレートを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/n 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ます。802.11b のレートのみを必須/基本レートとして設定できます。

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	必須データレート	サポートされているデータレート	無効化されたデータレート
802.11a/n/ac	12 Mbps	18 ~ 54 Mbps、 VHT MCS 0 - MCS 9 1SS、 VHT MCS 0 - MCS 9 2SS、 (VHT MCS 0 - MCS 9 3SS) 、 (VHT MCS 0 - MCS 9 4SS)	6、9 Mbps
802.11a/n	12 Mbps	18 ~ 54 Mbps、 HT MCS 0 - MCS 15、 (HT MCS 16 - MCS 31)	6、9 Mbps
802.11g/n	12 Mbps	18 ~ 54 Mbps、 HT MCS 0 - MCS 15、 (HT MCS 16 - MCS 31)	1、2、5.5、6、 9、11 Mbps
802.11b/g/n	11 Mbps	12 ~ 54 Mbps、 HT MCS 0 - MCS 15、 (HT MCS 16 - MCS 31)	1、2、5.5、6、 9 Mbps
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 レートを有効にも、無効にも選択できますが、キャパシティとスループットには影響しません。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え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、24 Mbps よりも高いデータ 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 レートを有効にしてください。

過度の再試行数が問題となる可能性がある環境への展開の場合、データレートの制限付きセットを使用できます。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、有効な最低データ レートだけを設定します。マルチキャスト パケットは、有効な最高必須/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。

条件の厳しい環境

Cisco Wireless Phone 840 および 860 を条件の厳しい環境（製造、倉庫、小売業など）に導入する場合、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 を導入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。条件の厳しい環境で適切に機能するアンテナ タイプを選択することも大切です。

アクセス ポイントの配置

Cisco Wireless Phone 840 または 860 とアクセスポイント間の障害物を最小限にし、アクセスポイントのアンテナからのラインオブサイトを確保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。

一部のエリアで一体型内部アンテナを搭載したアクセス ポイントを使用する場合は、アクセス ポイントを天井に取り付けることを推奨します。これらのアクセス ポイントは無指向性アンテナを装備しており、壁面への設置を想定していません。

周波数帯域

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

5 GHz チャンネル セットでは、8 または 12 チャン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 拡張チャン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。音声専用を使用する場合は、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、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

条件の厳しい環境ではマルチパスが高くなる可能性があることから、アクセスポイントと Cisco Wireless Phone 840 および 860 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 を導入しようとして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、アクセスポイント出力の過不足を防ぎます（5 GHz の場合、最低 11 dBm、最小 16 dBm）。

Cisco Wireless Phone 840 および 860 は、アクセスポイントの設定で DTPC が有効になっている場合、アクセスポイントの現在の送信電力設定を基に送信フレームの送信電力を決定します。

高速ローミング

高速ローミングには 802.11r/Fast Transition (FT) の使用が推奨されています。また 802.11r (FT) 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数も減少します。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確率が向上します。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。

Quality of Service (QoS)

音声およびコール制御フレームの WMM UP タグが正しく設定されるように、DSCP 値が有線ネットワーク全体で保持されることを確認する必要があります。

ビームフォーミング

Cisco 802.11n 対応アクセスポイントを使用している場合は、ビームフォーミング (ClientLink) を有効にする必要があります。これは、クライアントからの電波の受信に役立ちます。

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、信号品質が低下するため、受信機のデコード機能にも悪影響を与えます。

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

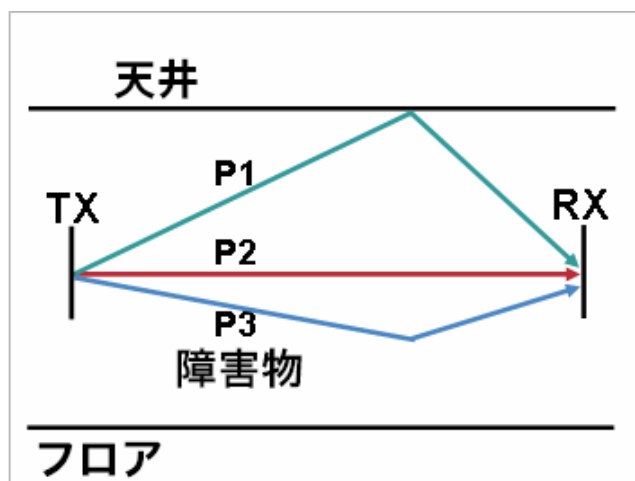
反射した波長が、メイン信号とちょうど位相がずれて到達し、メイン信号を完全に打ち消すような場合に発生します。

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/ac と 802.11g/n で使用される直交周波数分割多重方式 (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。

セキュリティ

ワイヤレス LAN を導入する場合、セキュリティが不可欠です。

Cisco Wireless Phone 840 および 860 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)
- WPA2-PSK (事前共有キー)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)
- PEAP (保護拡張認証プロトコル)

- 802.11r/Fast Transition (FT)
- CCKM (Cisco Centralized Key Management)
- なし

WLAN 暗号化

- AES (Advanced Encryption Standard)

注：WPA3 はサポートされていません。

802.1x-SHA2 キー管理はサポートされていません。

CCMP256、GCMP128、および GCMP256 暗号化方式はサポートされていません。

Cisco Wireless Phone 840 および 860 は、次の追加のセキュリティ機能もサポートしています。

- 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)
- 認証局プロキシ機能 (CAPF)
- セキュア プロファイル
- 暗号化された設定ファイル

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 Wireless Phone 840 または 860 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ー上に、ユーザーアカウントを作成する必要が生じることがあります。

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。

Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ)

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ) は、トランスポート層セキュリティ (TLS) を拡張する EAP プロトコルです。

EAP-TTLS-GTC、EAP-TTLS-MSCHAP、EAP-TTLS-MSCHAPv2、および EAP-TTLS-PAP は、サポートされている内部認証プロトコルです。

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

認証サーバーは、証明書を Cisco Wireless Phone 840 および 860 にインポートすることで検証できます。

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-GTC と PEAP-MSCHAPv2 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。

認証サーバーは、証明書を Cisco Wireless Phone 840 および 860 にインポートすることで検証できます。

Quality of Service (QoS)

Quality of Service により、キューイングで音声トラフィックを優先できます。

音声トラフィック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。
- QoS ポリシーを作成し、アクセス ポイント上で音声トラフィックとコール制御トラフィックを優先させます。

トラフィックタイプ	コールサーバ	DSCP	802.1p	WMM UP	プロトコル
音声	CUCM	EF (46)	5	6	RTP (UDP 16384 - 32767)
	Webex Calling	EF (46)	5	6	RTP (UDP 19560 ~ 65535)
コール制御	CUCM	CS3 (24)	3	4	SIP (TCP 5060 ~ 5061)
	Webex Calling	CS3 (24)	3	4	SIP (TCP 8934)

- 音声パケット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 IOS スイッチ上で Differentiated Services Code Point (DSCP) の保護を有効にします。

Cisco Wireless Phone 840 および 860 と Cisco Unified Communications Manager で使用される TCP ポートおよび 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。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_5_x/cucm_b_port-usage-cucm-105x/cucm_b_port-usage-cucm-105x_chapter_00.html

Webex Calling のネットワーク要件については、次の URL にある『**Port Reference Information for Webex Calling**』ドキュメントを参照してください。

<https://help.webex.com/en-US/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling>

コール アドミッション制御 (CAC)

アクセス ポイントでコール アドミッション制御を有効化できます。

- 音声用のコール アドミッション制御/Wi-Fi MultiMedia Traffic Specification (TSPEC) を有効にします。
- 音声トラフィック用に割り当てられる最大 RF 帯域幅を設定します (デフォルト = 75 %)。
- ローミング音声クライアント用に予約する帯域幅を設定します (デフォルト = 6 %)。

Pre-Call アドミッション制御

コール アドミッション コントロールがアクセスポイント上で有効な場合、Cisco Wireless Phone 840 および 860 は、Add Traffic Stream (ADDTS) をアクセスポイントに送信して、コールを発信または受信するための帯域幅を要求します。

AP が ADDTS 成功メッセージを送信すると、Cisco Wireless Phone 840 または 860 はコールを確立します。アクセスポイントがコールを拒否し、Cisco Wireless Phone 840 または 860 のローミング先となるアクセスポイントが他に存在しなければ、電話機に「ネットワークがビジーです (Network Busy)」と表示されます。インバウンドコールに対してアドミッションが拒否されても、コールを確立するために必要な帯域幅が不足していることを Cisco Wireless Phone 840 または 860 からリモートエンドポイントに通知することはありません。そのため、リモートユーザーがコールを終了するまで、コールが要求され続ける可能性があります。

ローミング アドミッション制御

通話中、Cisco Wireless Phone 840 および 860 は、現在のアクセスポイントおよび利用可能なすべてのアクセスポイントの Received Signal Strength Indicator (RSSI) と Packet Error Rate (PER) の値を測定して、ローミングに関する決定を行います。

コールが確立されていた元のアクセスポイントでコール アドミッション コントロールが有効になっていた場合、Cisco Wireless Phone 840 および 860 はローミング時に ADDTS 要求を新しいアクセスポイントに送信します。これは、再アソシエーション要求フレームに埋め込まれます。

有線 QoS

必要なネットワーク デバイスの QoS 設定と QoS ポリシーを設定します。

WLAN デバイスの Cisco スイッチ ポートの設定

Cisco ワイヤレス LAN コントローラ、Cisco 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。

Cisco IOS スイッチを使用する場合は、次のスイッチポート設定を使用します。

Cisco ワイヤレス LAN コントローラに対して COS 信頼状態を有効にする

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

Cisco 製アクセス ポイントに対して DSCP 信頼状態を有効にする

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

Cisco Meraki MS スイッチを使用する場合は、『Cisco Meraki MS Switch VoIP 導入ガイド』を参照してください。

https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf

注：Cisco Wireless LAN Controller を使用する場合は、DSCP 信頼状態を実装する必要があります。つまり、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 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）を信頼状態にする必要があります。

有線 IP フォンの Cisco スイッチ ポートの設定

Cisco 製の有線 IP フォンのスイッチ ポートで Cisco 製電話機の信頼状態を有効にします。

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
```

ローミング

Cisco Wireless Phone 840 および 860 では、802.11 モードがデフォルトで「自動」に設定されています。これにより、Cisco Wireless Phone 840 および 860 が 5 GHz または 2.4 GHz のいずれかに接続でき、インターバンド ローミングのサポートが有効になります。

802.11r/Fast Transition (FT) は、頻繁にローミングが発生するすべての種類の環境で推奨される導入モデルです。

CCKM を使用するには、802.1x 認証が必要です。

802.11r (FT) または 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、ローミング中に遅延が発生する可能性があります。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。

802.11r (FT) または CCKM を使用すると、ローミング時間を 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ーが体感することはありません。

Cisco Wireless Phone 840 および 860 では、WPA2 (AES) または WPA2-PSK (AES) を使用する 802.11r (FT) と WPA2 (AES) を使用する CCKM がサポートされます。

認証	ローミング時間
WPA2 パーソナル	150 ミリ秒
WPA2 エンタープライズ	300 ミリ秒
802.11r (FT)	100 ミリ秒未満
CCKM	100 ミリ秒未満

Cisco Wireless Phone 840 および 860 は、スキャンおよびローミングイベントを管理します。

大半のローミングは、現在の RSSI に基づく必須 RSSI 差分を満たしたことによってローミングがトリガーされている必要があります。これにより、シームレスなローミング（音声の中断なし）が実現します。

シームレスなローミングを実現するため、Cisco Wireless Phone 840 および 860 は、少なくとも 3 秒間アクセスポイントに関連付けられる必要があります。そうでない場合、パケット損失（最大 tx 回の再送信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する可能性があります。

高速セキュア ローミング (FSR)

802.11r/Fast Transition (FT) は、頻繁にローミングが発生するすべての種類の環境で推奨される導入モデルです。

Cisco Centralized Key Management (CCKM) もサポートされていますが、802.1x 認証が必要です。

802.11r (FT) と CCKM は、高速セキュア ローミングを可能にし、ネットワーク非接続時間を抑制して、通話中のオーディオギャップを最小限に抑えます。

802.11r (FT) を使用しない 802.1x または PSK と、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、ローミング中に遅延が発生する可能性があります。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。

802.11r (FT) と CCKM はキー管理を一元化して、キー交換の回数を減らします。

802.11r (FT) または CCKM を使用すると、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ーが体感することはありません。

802.11r (FT) ローミングには次の 2 つの方式があります。

Over the Air

クライアントは、FT 認証アルゴリズムによる 802.11 認証を使用して、ターゲット アクセス ポイントと直接通信します。

Over the Distribution

クライアントは、現在のアクセス ポイント経由でターゲット アクセス ポイントと通信します。クライアントとターゲット アクセス ポイントの間の通信は、WLAN コントローラを介してクライアントと現在のアクセス ポイントとの間で FT アクション フレームを介して伝送されます。

802.11r (FT) では、高速セキュア ローミング モデルとして、Over the Air 方式の使用が推奨されます。

802.11r (FT) と Over the Distribution 方式の組み合わせを使用する場合は、現在関連付けられているアクセス ポイントへの接続が必要になるため、現在のアクセス ポイントやターゲット アクセス ポイントと必ずしも通信できるとは限らない状況では適切に動作しない可能性があります。このような状況は、閉鎖環境においてローミング イベントが発生したときに、現在のアクセス ポイントとターゲット アクセス ポイントの両方へのライン オブ サイトを保持できない場合に発生する可能性があります。

Cisco Wireless Phone 840 および 860 では、WPA2-PSK または WPA2 を使用する 802.11r (FT) と、WPA2 または WPA を使用する CCKM がサポートされます。

FSR タイプ	認証	キーの管理	暗号化
802.11r (FT)	PSK	WPA2	AES
802.11r (FT)	EAP-TLS	WPA2	AES
802.11r (FT)	EAP-TTLS	WPA2	AES
802.11r (FT)	PEAP	WPA2	AES
CCKM	EAP-TLS	WPA2	AES
CCKM	EAP-TTLS	WPA2	AES
CCKM	PEAP	WPA2	AES

注：Cisco Wireless Phone 840 または 860 を導入する環境に他の Wi-Fi 電話機が存在し、それらの電話機が 802.11r (FT) をサポートしていない場合は、既存の同じ SSID を Cisco Wireless Phone 840 または 860 に使用できます。ただし（他の Wi-Fi 電話機が 802.11r (FT) を使用せず、802.11r (FT) 対応ネットワークで相互運用可能である限り）、他の既存のキー管理タイプ（802.1x、CCKM、802.1x + CCKM など）に加えて、Over the Air 方式を使用する 802.11r (FT) を有効にすることを推奨します。

帯域間のローミング

Cisco Wireless Phone 840 および 860 では、周波数帯域モードがデフォルトで「自動」に設定されています。自動モードではインターバンドローミングが有効になり、最も強い信号を優先します。電力レベルが同じである場合、一般的に信号強度のより強い 2.4 GHz が 5 GHz よりも優先されます。

電源オン時に Cisco Wireless Phone 840 および 860 が自動モードであれば、すべての 2.4 GHz チャンネルと 5 GHz チャンネルをスキャンした後、設定済みネットワーク用のアクセスポイント（使用可能な場合）への関連付けを試みます。

5 GHz のみまたは 2.4 GHz のみモードに設定されている場合、これらのチャンネルだけがスキャンされます。対象帯域を有効化して帯域間のローミングを実現するためにも、周波数帯分析を実施することが推奨されます。

電源管理

Cisco Wireless Phone 840 および 860 は、Wi-Fi Multimedia (WMM) がアクセスポイントの設定で有効であるかどうかに応じて、U-APSD の省電力方式を使用します。

アクセスポイントが プロキシ ARP をサポートしていない場合、アイドル時のバッテリー持続時間は最大 50 % 短くなります。

Cisco Wireless Phone 840 および 860 は、アイドル時または通話時に主に U-APSD 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)

Cisco Wireless Phone 840 および 860 は、ユニキャストパケット、ブロードキャストパケット、およびマルチキャストパケットをチェックする起動周期をスケジューリングするために、DTIM 周期を使用します。

プロキシ ARP が有効になっている場合、Cisco Wireless Phone 840 および 860 は DTIM 時に起動する必要はありません。

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。

DTIM 周期は、バッテリー持続時間とマルチキャスト パフォーマンスの間でトレードオフの関係になっています。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。

ダイナミック伝送パワー コントロール (DTPC)

Cisco Wireless Phone 840 または 860 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、ダイナミック伝送パワーコントロール (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方向のみに聞こえる場合に一方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 Wireless Phone 840 および 860 は、現在のチャン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。

アクセスポイントの無線送信電力は、Cisco Wireless Phone 840 および 860 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。

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 と 802.11g 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します。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、チャンネルの初期使用率、および環境によって異なります。

音声通話 (Audio Calls)

次に、アクセスポイント/チャンネルごとにサポートされる音声通話 (単一の双方向音声ストリーム) の最大数を示します。

音声通話の最大数	802.11 モード	オーディオコーデック	オーディオビットレート	データレート
13	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	6 Mbps
20	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	12 Mbps
27	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	24 Mbps 以上

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。

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、すべてのマルチキャスト パケットは、DTIM 周期までキューイングされます。

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

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 Wireless Phone 840 および 860 は、IGMP クエリ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せます。

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。

注：802.11b/g/n と Bluetooth が同時に使用される共存を使用する場合、マルチキャスト音声はサポートされません。

Cisco ワイヤレス LAN の設定

Cisco AireOS ワイヤレス LAN コントローラおよび Lightweight アクセスポイント

Cisco ワイヤレス LAN コントローラおよび Lightweight 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。

- **[802.11r (FT)]** または **[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 **[必須 (Required)]** に設定します
- **802.11k** を **[有効 (Enabled)]** に設定することを推奨
- **802.11v** を **有効** に設定することを推奨
- **[セッションタイムアウト (Session Timeout)]** が有効で、正しく設定されていることを確認します
- **[キーのブロードキャスト間隔 (Broadcast Key Interval)]** が有効になっていて、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) ブロッキング アクション (P2P (Peer to Peer) Blocking Action)]** 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。
- **[保護された管理フレーム (PMF) (Protected Management Frame (PMF)]** は、**[任意 (Optional)]** または **[無効 (Disabled)]** に設定する必要があります
- **[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 周期 (DTIM Period)]** を **[2]** に設定します
- **[クライアントの負荷分散 (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
- Cisco 802.11n 対応の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
- 必要に応じて **[自動 RF (Auto RF)]** を設定します
- **[ボイス (Voice)]** で、**[アドミッション制御必須 (Admission Control Mandatory)]** を **[有効 (Enabled)]** に設定します。
- **[ボイス (Voice)]** で **[ロードベース CAC (Load Based CAC)]** を **[有効 (Enabled)]** に設定します。
- **[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 **[音声の最適化 (Voice Optimized)]** または **[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。
- **[チャンネル通知 (Channel Announcement)]** および **[チャンネル静音モード (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 (Frame Aggregation)]** 設定を設定します
- CleanAir テクノロジーを搭載した Cisco 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
- Platinum QoS プロファイルの [プロトコルタイプ (Protocol Type)] を [なし (None)] に設定します。

802.11 ネットワークの設定

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域で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。

5 GHz を使用する場合は、802.11a/n/ac ネットワークのステータスが [有効 (Enabled)] に設定され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 対応の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。

必要に応じて、[許可される最大クライアント数 (Maximum Allowed Clients)] を設定できます。

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 以上をそれぞれ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ります。

The screenshot shows the Cisco Wireless configuration page for 802.11a Global Parameters. The left sidebar contains a navigation menu with options like Access Points, Radios, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, and 802.11a/n/ac/ax. The main content area is divided into several sections:

- General:**
 - 802.11a Network Status: Enabled
 - Beacon Period (milliseconds):
 - Fragmentation Threshold (bytes):
 - DTPC Support: Enabled
 - Maximum Allowed Clients:
 - RSSI Low Check: Enabled
 - RSSI Threshold (-60 to -90 dBm):
- 802.11a Band Status:**
 - Low Band: Enabled
 - Mid Band: Enabled
 - High Band: Enabled
- Data Rates**:**
 - 6 Mbps: Disabled
 - 9 Mbps: Disabled
 - 12 Mbps: Mandatory
 - 18 Mbps: Supported
 - 24 Mbps: Supported
 - 36 Mbps: Supported
 - 48 Mbps: Supported
 - 54 Mbps: Supported
- CCX Location Measurement:**
 - Mode: Enabled
 - Interval (seconds):
- TWT Configuration ***:**
 - Target Waketime: Enabled
 - Broadcast TWT Support: Enabled

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 が [有効 (Enabled)] に設定され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 対応の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。

必要に応じて、[許可される最大クライアント数 (Maximum Allowed Clients)] を設定できます。

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、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、サポート対象 (任意) レートとして 12 Mbps 以上をそれぞれ設定する必要があります。

The screenshot shows the Cisco Wireless configuration page for 802.11b/g Global Parameters. The interface is divided into three main sections: General, Data Rates, and CCX Location Measurement. The General section includes settings for 802.11b/g Network Status (Enabled), 802.11g Support (Enabled), Beacon Period (100), Short Preamble (Enabled), Fragmentation Threshold (2346), DTPC Support (Enabled), Maximum Allowed Clients (100), RSSI Low Check (Disabled), and RSSI Threshold (-80). The Data Rates section shows a list of rates from 1 Mbps to 54 Mbps, with 1 Mbps through 11 Mbps set to Disabled, 12 Mbps set to Mandatory, 18 Mbps through 36 Mbps set to Supported, and 48 Mbps and 54 Mbps also set to Supported. The CCX Location Measurement section shows Mode (Enabled) and Interval (60 seconds). The TWT Configuration section shows Target Waketime (Enabled) and Broadcast TWT Support (Enabled).

ビームフォーミング (ClientLink)

Cisco 802.11n 対応のアクセスポイントを、[クライアントリンク (ClientLink)] を有効にします。

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、または個別アクセスポイントからの無線ビームフォーミング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、ビームフォーミング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.....有効

Auto RF (RRM)

Cisco ワイヤレス LAN コントローラを使用する場合は、Auto RF を有効にし、チャンネルと送信電力の設定を管理することが推奨されます。

使用する周波数帯域 (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は、電力の最大レベルと最小レベルを指定できます。

Wireless

802.11a > RRM > Tx Power Control(TPC)

TPC Version

Interference Optimal Mode (TPCv2)
 Coverage Optimal Mode (TPCv1)

Tx Power Level Assignment Algorithm

Power Level Assignment Method: Automatic Every 600 sec
 On Demand
 Fixed 1

Maximum Power Level Assignment (-10 to 30 dBm): 17
 Minimum Power Level Assignment (-10 to 30 dBm): 11
 Power Assignment Leader: RTP9-32A-WLC3 (10.81.6.70)
 Last Power Level Assignment: 463 secs ago
 Power Threshold (-80 to -50 dBm): -65
 Channel Aware: Enabled
 Power Neighbor Count: 3

5 GHz を使用する場合は、多数のチャン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ためにチャンネルの数を制限できます（例：12 チャンネルのみ）。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

Wireless

802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method: Automatic Interval: 10 minutes AnchorTime: 0
 Freeze
 OFF

Avoid Foreign AP interference: Enabled
 Avoid Cisco AP load: Enabled
 Avoid non-802.11a noise: Enabled
 Avoid Persistent Non-WiFi Interference: Enabled
 Channel Assignment Leader: RTP9-32A-WLC3 (10.81.6.70)
 Last Auto Channel Assignment: 556 secs ago
 DCA Channel Sensitivity: Medium (15 dB)
 Channel Width: 20 MHz 40 MHz 80 MHz 160 MHz 80+80 MHz Best
 Avoid check for non-DFS channel: Enabled

DCA Channel List

DCA Channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 153, 157, 161

2.4 GHz を使用する場合、DCA リストではチャンネル 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ンネルの数が限られているために、40 MHz に対応した Cisco 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 チャンネルを設定することを推奨します。

The screenshot shows the Cisco Wireless configuration interface for Dynamic Channel Assignment (DCA). The left sidebar contains navigation options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'AP Group NTP', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'FlexConnect ACLs', 'FlexConnect VLAN Templates', 'Network Lists', and '802.11a/n/ac/ax'. The main content area is titled '802.11b > RRM > Dynamic Channel Assignment (DCA)'. Under 'Dynamic Channel Assignment Algorithm', the 'Channel Assignment Method' is set to 'Automatic' (selected), with 'Interval' at '10 minutes' and 'AnchorTime' at '0'. A button 'Invoke Channel Update Once' is visible. Other settings include 'Avoid Foreign AP interference' (Enabled), 'Avoid Cisco AP load' (Disabled), 'Avoid non-802.11b noise' (Enabled), 'Avoid Persistent Non-WiFi Interference' (Disabled), 'Channel Assignment Leader' (RTP9-32A-WLC3 (10.81.6.70)), 'Last Auto Channel Assignment' (75 secs ago), and 'DCA Channel Sensitivity' (Medium (10 dB)). Below this is the 'DCA Channel List' section, which contains a text box with the value '1, 6, 11'.

使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセス ポイントの設定をグローバル設定よりも優先させることができます。

その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

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。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセス ポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

チャンネル ボンディングは、5 GHz を使用する場合にのみ使用することをお勧めします。

すべてのアクセス ポイントで同じチャンネル幅を使用することを推奨します。

The screenshot shows the configuration page for a Cisco AP. The left sidebar lists navigation options like Access Points, Radios, and various profiles. The main content area is divided into several sections:

- General:** AP Name (rtp9-31a-ap1), Admin Status (Enable), Operational Status (UP), Slot # (1).
- 11n Parameters:** 11n Supported (Yes).
- CleanAir:** CleanAir Capable (Yes), CleanAir Admin Status (Enable), Number of Spectrum Expert connections (0).
- Antenna Parameters:** Antenna Type (Internal), Antenna (A, B, C, D) with checkboxes.
- RF Channel Assignment:** Current Channel (48,44), Channel Width (40 MHz), Assignment Method (Global).
- Radar Information:** Channel and Last Heard (Secs) table, currently empty.
- Tx Power Level Assignment:** Current Tx Power Level (1), Assignment Method (Global).
- Performance Profile:** View and edit Performance Profile for this AP.

クライアントのローミング

Cisco Wireless Phone 840 および 860 は、シスコ ワイヤレス LAN コントローラのクライアント ローミング セクションの RF パラメータを使用しません。スキャンングとローミングは電話機側が独立して管理します。

EDCA パラメータ

使用する周波数帯域に応じて 5 GHz または 2.4 GHz に対し、EDCA プロファイルを **[音声の最適化 (Voice Optimized)]** または **[音声とビデオの最適化 (Voice & Video Optimized)]** のいずれかに設定し、**[低遅延 MAC (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/ac アクセス ポイントでは LLM がサポートされません。

The screenshot shows the configuration page for EDCA Profile. The left sidebar is the same as the previous screenshot. The main content area shows:

- General:** EDCA Profile (Voice & Video Optimized), Enable Low Latency MAC (unchecked).

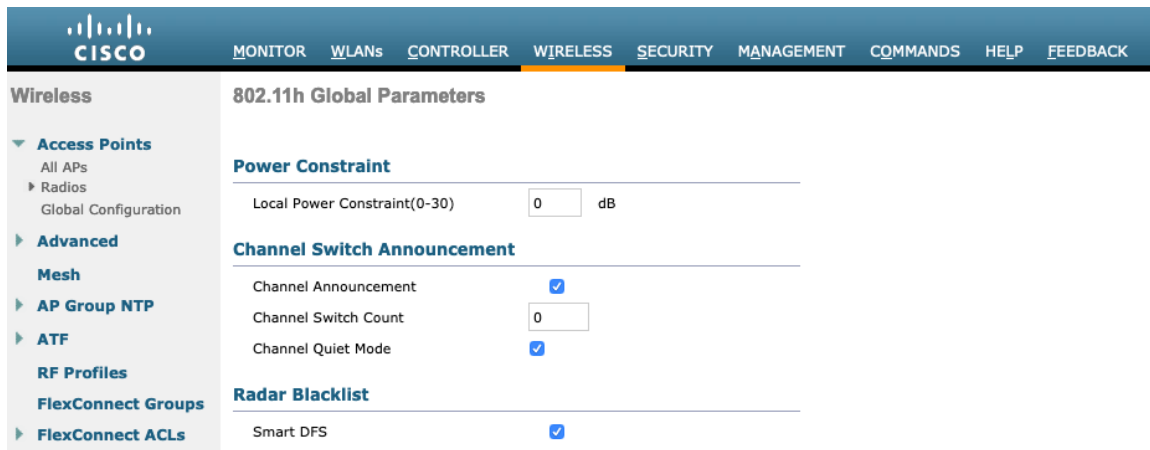
A note at the bottom states: "Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled."

DFS (802.11h)

Cisco Wireless Phone 840 および 860 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)]** を未設定のままにするか、0 dBm に設定します。

最新バージョンのシスコ ワイヤレス LAN コントローラでは、TPC (電力制限) とダイナミック伝送パワーコントロール (DTPC) の両方を同時に有効にすることはできません。

[チャンネル通知 (Channel Announcement)] および **[チャンネル静音モード (Channel Quiet Mode)]** を **[有効 (Enabled)]** にする必要があります。



The screenshot shows the Cisco Wireless configuration page for 802.11h Global Parameters. The left sidebar lists various configuration options under 'Wireless', including Access Points, Radios, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, and FlexConnect ACLs. The main content area is titled '802.11h Global Parameters' and contains three sections: 'Power Constraint' with a 'Local Power Constraint(0-30)' input field set to 0 dB; 'Channel Switch Announcement' with 'Channel Announcement' checked, 'Channel Switch Count' set to 0, and 'Channel Quiet Mode' checked; and 'Radar Blacklist' with 'Smart DFS' checked.

高スループット (802.11n/ac)

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。

802.11ac データ レートは 5 GHz にのみ適用できます。

[WMM] が有効になっていること、および **[WPA2 (AES)]** が 802.11n/ac 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 Wireless Phone 840 および 860 は、HT MCS 0 ~ MCS 15 と VHT MCS 0 ~ MCS 9 1SS および 2SS データレートのみをサポートしますが、MIMO アンテナテクノロジーを含む同じ帯域を利用する他の 802.11n/ac クライアントが存在するため、より高いレートが利用可能な場合には、オプションでより高い MCS レートを有効にできます。

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless 802.11n/ac/ax (5 GHz) Throughput

Access Points
 All APs
 Radios
 Global Configuration
Advanced
 Mesh
 AP Group NTP
 ATF
 RF Profiles
 FlexConnect Groups
 FlexConnect ACLs
 FlexConnect VLAN Templates
 Network Lists
802.11a/n/ac/ax
 Network
 RRM
 RF Grouping
 TPC
 DCA
 Coverage
 General
 Client Roaming
 Media
 EDCA Parameters
 DFS (802.11h)
 High Throughput (802.11n/ac/ax)
 CleanAir
 802.11b/g/n/ax
 Media Stream
 Application Visibility And Control
 Lync Server
 Country
 Timers
 Netflow
 QoS

General

11n Mode Enabled ²
 11ac Mode Enabled ²
 11ax Mode Enabled ²

VHT MCS Rates

SS1
 0-8 Enabled ⁴
 0-9 Enabled ⁴

SS2
 0-8 Enabled ⁴
 0-9 Enabled ⁴

SS3
 0-8 Enabled ⁴
 0-9 Enabled ⁴

SS4
 0-8 Enabled ⁴
 0-9 Enabled ⁴

HE MCS Rates

SS1
 0-7 Enabled
 0-9 Enabled
 0-11 Enabled

SS2
 0-7 Enabled
 0-9 Enabled
 0-11 Enabled

SS3
 0-7 Enabled
 0-9 Enabled
 0-11 Enabled

SS4
 0-7 Enabled
 0-9 Enabled
 0-11 Enabled

SS5
 0-7 Enabled

SS6
 0-7 Enabled

MCS (Data Rate ¹) Settings

0 (7 Mbps) Supported
 1 (14 Mbps) Supported
 2 (21 Mbps) Supported
 3 (29 Mbps) Supported
 4 (43 Mbps) Supported
 5 (58 Mbps) Supported
 6 (65 Mbps) Supported
 7 (72 Mbps) Supported
 8 (14 Mbps) Supported
 9 (29 Mbps) Supported
 10 (43 Mbps) Supported
 11 (58 Mbps) Supported
 12 (87 Mbps) Supported
 13 (116 Mbps) Supported
 14 (130 Mbps) Supported
 15 (144 Mbps) Supported
 16 (22 Mbps) Supported
 17 (43 Mbps) Supported
 18 (65 Mbps) Supported
 19 (87 Mbps) Supported
 20 (130 Mbps) Supported
 21 (173 Mbps) Supported
 22 (195 Mbps) Supported
 23 (217 Mbps) Supported
 24 (29 Mbps) Supported
 25 (58 Mbps) Supported
 26 (87 Mbps) Supported
 27 (116 Mbps) Supported
 28 (173 Mbps) Supported
 29 (231 Mbps) Supported
 30 (260 Mbps) Supported
 31 (289 Mbps) Supported

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、順スループットとキャパシティ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 Wireless Phone 840 および 860 の操作性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-MSDU

ユーザ プライオリティ 1、2 = 有効

ユーザ プライオリティ 0、3、4、5、6、7 = 無効

A-MPDU

ユーザ プライオリティ 0、3、4、5 = 有効

ユーザ プライオリティ 1、2、6、7 = 無効

Cisco Wireless Phone 840 および 860 の推奨事項に従って A-MPDU および A-MSDU 設定を設定するには、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-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
```

```
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
```

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-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
```

```
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
```

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-MSDU Tx:

```
優先度 0..... 無効
優先度 1..... 有効
優先度 2..... 有効
優先度 3..... 無効
優先度 4..... 無効
優先度 5..... 無効
優先度 6..... 無効
優先度 7..... 無効
```

A-MPDU Tx:

```
優先度 0..... 有効
優先度 1..... 無効
優先度 2..... 無効
優先度 3..... 有効
優先度 4..... 有効
優先度 5..... 有効
優先度 6..... 無効
優先度 7..... 無効
```

CleanAir

CleanAir テクノロジーを搭載したCisco 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。

802.11a > CleanAir

CleanAir/Spectrum Intelligence Parameters

CleanAir	<input checked="" type="checkbox"/> Enabled
Spectrum Intelligence ²	<input type="checkbox"/> Enabled
Report Interferers ¹	<input checked="" type="checkbox"/> Enabled
Persistent Device Propagation	<input type="checkbox"/> Enabled

Interferences to Ignore

- Canopy
- WiMax Fixed
- SI_FHSS

Interferences to Detect

- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT-like Phone
- Video Camera

Trap Configurations

Enable AQI(Air Quality Index) Trap	<input checked="" type="checkbox"/> Enabled
AQI Alarm Threshold (1 to 100) ²	35
Enable trap for Unclassified Interferences	<input type="checkbox"/> Enabled
Threshold for Unclassified category trap (1 to 99)	20
Enable trap for Classified Interferences	<input type="checkbox"/> Enabled
Threshold for Classified category trap (1 to 99)	0
Enable Interference For Security Alarm	<input checked="" type="checkbox"/> Enabled

Do not trap on these types

- TDD Transmitter
- Continuous Transmitter
- DECT-like Phone
- Video Camera
- SuperAG

Trap on these types

- Jammer
- WiFi Inverted
- WiFi Invalid Channel

Event Driven RRM [\(Change Settings\)](#)

EDRRM	Disabled
Sensitivity Threshold	N/A
Rogue Contribution	N/A
Rogue Duty-Cycle	N/A

(1) Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.
(2) AQI value 100 is best and 1 is worst
(3) Spectrum Intelligence does not send traps to Prime Infrastructure and CMX

Rx SOP しきい値

[Rx Sop のしきい値 (Rx Sop Threshold)]にはデフォルト値を使用することを推奨します。

WLAN の設定

Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

ただし、音声対応 Cisco Wireless LAN 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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ (たとえば 802.11a のみ) 適用するよう指定できます。

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

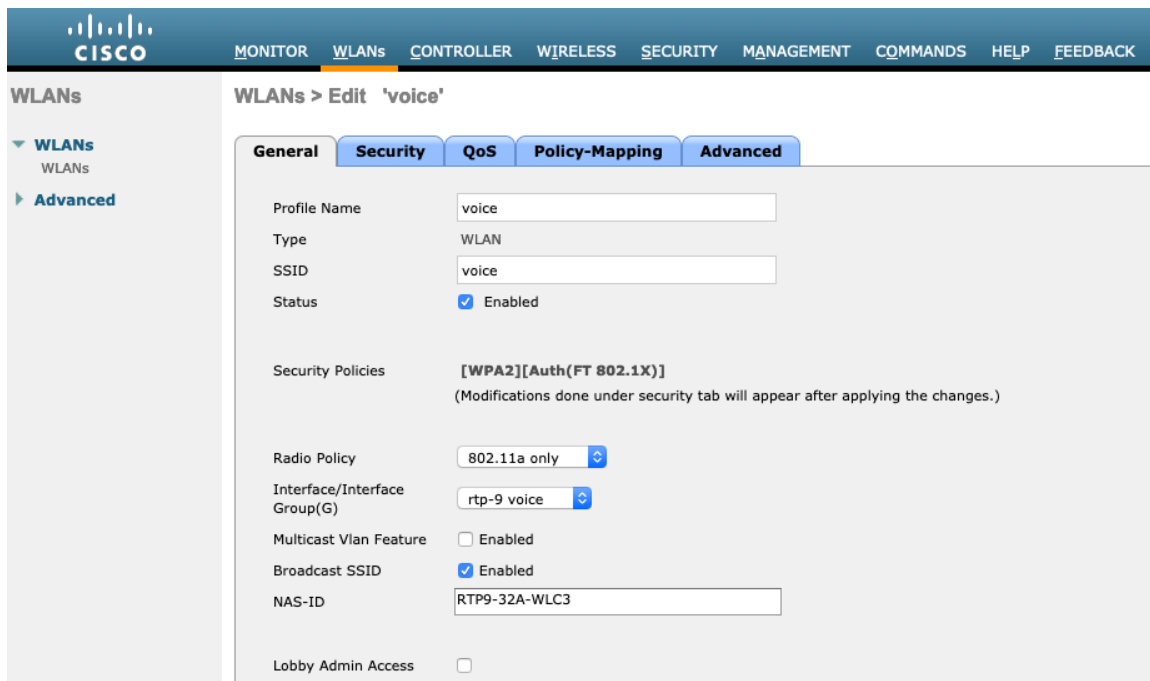
Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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。



The screenshot shows the Cisco WLAN configuration interface for creating a new WLAN. The top navigation bar includes MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows WLANs > Advanced. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	voice
SSID	voice
ID	6



The screenshot shows the Cisco WLAN configuration interface for editing an existing WLAN. The top navigation bar is the same as the previous screenshot. The left sidebar shows WLANs > Advanced. The main content area is titled 'WLANs > Edit 'voice'' and has tabs for General, Security, QoS, Policy-Mapping, and Advanced. The Security tab is selected, showing the following configuration:

Profile Name	voice
Type	WLAN
SSID	voice
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(FT 802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11a only
Interface/Interface Group(G)	rtp-9 voice
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	RTP9-32A-WLC3
Lobby Admin Access	<input type="checkbox"/>

高速セキュア ローミングに 802.11r (FT) を利用するには、Fast Transition を有効にするボックスをオンにします。

[Over the DS] をオフにして、Over the Distribution システム方式の代わりに Over the Air 方式を使用することを推奨します。

[保護された管理フレーム (PMF) (Protected Management Frame (PMF)] を **[任意 (Optional)]** または **[無効 (Disabled)]** に設定します。

AES 暗号化を使用した WPA2 ポリシーを有効にします。その後、802.1x と PSK のどちらを使用するかに応じて、認証キー管理タイプとして FT 802.1x と FT PSK のどちらかを有効にします。

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security **QoS** Policy-Mapping Advanced

Layer 2 **Layer 3** AAA Servers

Layer 2 Security [6](#) WPA+WPA2

Security Type Enterprise

MAC Filtering [2](#)

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption CCMP128(AES) TKIP CCMP256 GCMP128 GCMP256

OSEN Policy

Fast Transition

Fast Transition Enable

Over the DS

Reassociation Timeout 20 Seconds

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security **QoS** Policy-Mapping Advanced

Protected Management Frame

PMF Disabled

Authentication Key Management [19](#)

802.1X-SHA1 Enable

802.1X-SHA2 Enable

FT 802.1X Enable

CCKM Enable

WPA GTK-randomize State [14](#) Disable

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security **QoS** Policy-Mapping Advanced

Layer 2 **Layer 3** AAA Servers

Layer 2 Security [6](#) WPA+WPA2

Security Type Personal

MAC Filtering [2](#)

AutoConfig iPSK Enable

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

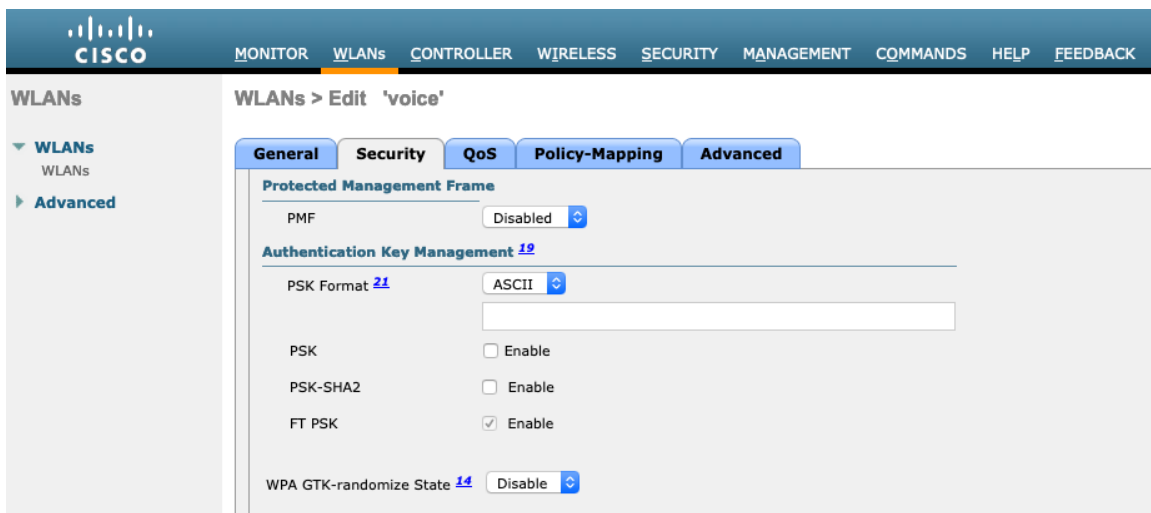
WPA2 Encryption CCMP128(AES) TKIP

Fast Transition

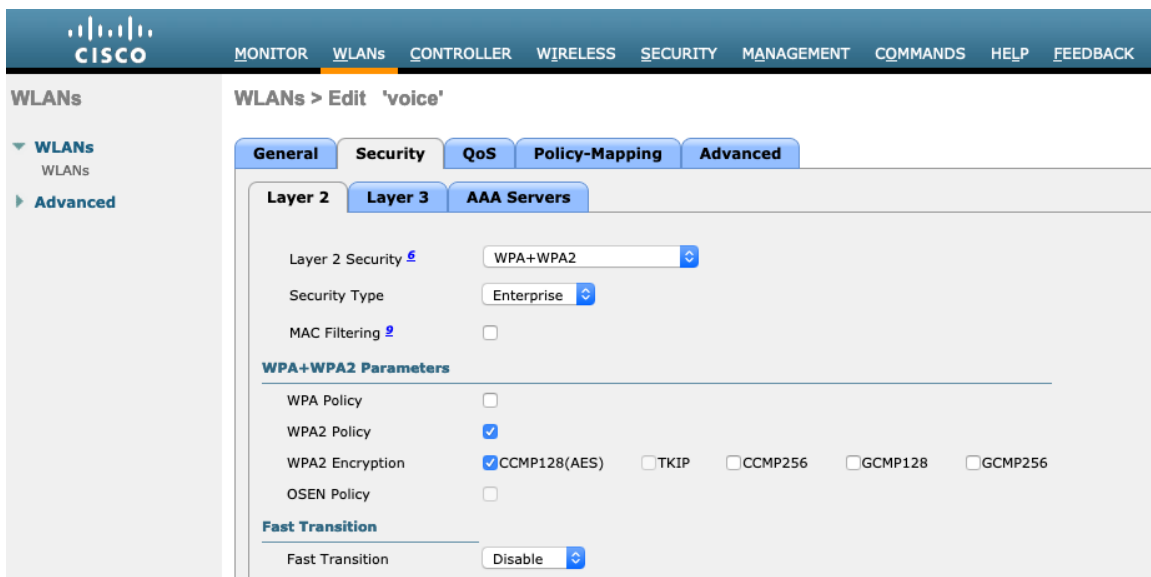
Fast Transition Enable

Over the DS

Reassociation Timeout 20 Seconds



高速セキュア ローミングに CCKM を利用するには、AES 暗号化を使用した WPA2 ポリシーと認証キー管理タイプ用の CCKM を有効にします。



各種の音声クライアントに同じ SSID を使用する場合は、802.1x、CCKM、PSK も有効にできます。802.1x や PSK を使用するかどうかに応じて、802.11r (FT) をサポートしない音声クライアントも含まれます。

RADIUS 認証およびアカウントサーバーは、SSID レベルごとに設定して、グローバルリストを上書きできます。

[有効 (Enabled)] で指定されていない場合 ([なし (None)]) に設定)、[セキュリティ (Security)] > [AAA] > [RADIUS] で定義された RADIUS サーバーのグローバルリストが使用されます。

グローバルレベルでのみ設定できる EAP ブロードキャストキー間隔を除き、EAP パラメータは SSID ごとまたはグローバルレベルで設定できます。

SSID ごとのレベルで EAP パラメータを設定する場合は、EAP パラメータセクションで [有効 (Enable)] をオンにして、必要な値を入力します。

The screenshot shows the Cisco WLAN configuration interface for the 'voice' SSID. The 'AAA Servers' section is active, showing options to override default servers. Under 'RADIUS Servers', there are checkboxes for 'RADIUS Server Overwrite interface' and 'Apply Cisco ISE Default Settings', both currently disabled. The 'Authentication Servers' and 'Accounting Servers' sections each have a table with 6 rows (Server 1 to Server 6). For Authentication Servers, the 'Enabled' checkbox is checked, and all server dropdowns are set to 'None'. For Accounting Servers, the 'Enabled' checkbox is checked, and all server dropdowns are set to 'None'. Below these are 'Authorization ACA Server' and 'Accounting ACA Server' checkboxes, both disabled. The 'EAP Parameters' section has an 'Enable' checkbox checked, followed by a table of parameters:

Parameter	Value
EAPOL Key Timeout(200 to 5000 millisec)	400
EAPOL Key Retries(0 to 4)	4
Identity Request Timeout(1 to 120 sec)	30
Identity Request Retries(1 to 20)	2
Request Timeout(1 to 120 sec)	30
Request Retries(1 to 20)	2

WMM ポリシーは、この SSID が Cisco Wireless Phone 840 および 860 などの WMM 対応電話機で使用されている場合にのみ、[必須 (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を別の WLAN に配置することを推奨します。

非 WMM クライアントが Cisco Wireless Phone 840 および 860 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。

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。

WLANs > Edit 'voice'

QoS

Quality of Service (QoS)

Application Visibility Enabled

AVC Profile

Flex AVC Profile

Netflow Monitor

Fastlane

Override Per-User Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLANs > Edit 'voice'

Security

Override Per-SSID Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WMM

WMM Policy

7920 AP CAC Enabled

7920 Client CAC Enabled

Media Stream

Multicast Direct Enabled

Lync Policy

Audio

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。86400 秒のセッションタイムアウトを有効にして、音声通話中に発生する可能性のある中断を回避することをお勧めします。また、クライアントのログイン情報を定期的に再検証して、クライアントが有効なログイン情報を使用していることを確認することもお勧めします。

[Aironet 拡張機能 (Aironet IE)] を有効にします。

[ピアツーピア (P2P) のブロッキングアクション (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。

必要に応じて、[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)] を設定できます。

[オフチャン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、または優先順位の高いアプリケーション (音声、呼制御など) の DSCP 値がアクセスポイントに保持されていない場合は、優先順位の高いキュー (4 ~ 6) と共に優先順位の低いキュー (0 ~ 3) を有効にしてオフチャンネルスキャンを待機させるとともに、場合によってはスキャンの待機時間を長くすることを推奨します。

EAP エラーが頻繁に発生する展開では、プライオリティキュー 7 を有効にして、EAP 交換中にオフチャンネルスキャンを延期することをお勧めします。

[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。

[DTIM 周期 (DTIM Period)] を [2] に、ビーコン周期を [100 ミリ秒] に設定します。

[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。

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。

802.11k および 802.11v を有効にすることを推奨します。

The screenshot shows the Cisco Wireless LAN Controller configuration interface for the 'voice' WLAN. The 'Advanced' tab is active, displaying various configuration options. The 'Client Exclusion' and 'Maximum Allowed Clients' settings are visible, along with the 'DHCP' and 'Management Frame Protection (MFP)' sections. The 'DTIM Period' is set to 2 for both 802.11a/n and 802.11b/g/n. The 'Client Load Balancing' and 'Client Band Select' options are disabled.

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

PER AP Radio

Clear HotSpot Configuration Enabled

Client user idle timeout(15-100000)

Client user idle threshold (0-10000000) Bytes

Radius NAI-Realm

11ac MU-MIMO

WGB PRP Enabled

MBO State

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching Enabled

Passive Client

Passive Client

Voice

Media Session Snooping Enabled

Re-anchor Roamed Voice Clients Enabled

KTS based CAC Policy Enabled

Radius Client Profiling

DHCP Profiling

HTTP Profiling

Local Client Profiling

DHCP Profiling

HTTP Profiling

PMIP

PMIP Mobility Type

PMIP NAI Type

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

FlexConnect Local Auth Enabled

Learn Client IP Address Enabled

Vlan based Central Switching Enabled

Central DHCP Processing Enabled

Override DNS Enabled

NAT-PAT Enabled

Central Assoc Enabled

Lync

Lync Server

11k

Neighbor List Enabled

Neighbor List Dual Band Enabled

Assisted Roaming Prediction Optimization Enabled

802.11ax BSS Configuration

Down Link MU-MIMO Enabled

PMIP Profile

PMIP Realm

Universal AP Admin Support

Universal AP Admin

11v BSS Transition Support

BSS Transition

Disassociation Imminent

Disassociation Timer(0 to 3000 TBTT)

Optimized Roaming Disassociation Timer(0 to 40 TBTT)

BSS Max Idle Service

Directed Multicast Service

Tunneling

Tunnel Profile

EOGRE Vlan Override

mDNS

mDNS Snooping Enabled

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

802.11ax BSS Configuration

Down Link MU-MIMO Enabled

Up Link MU-MIMO Enabled

Down Link OFDMA Enabled

Up Link OFDMA Enabled

mDNS

mDNS Snooping Enabled

TrustSec

Security Group Tag

Umbrella

Umbrella Mode

Umbrella Profile

Umbrella DHCP Override

Fabric Configuration

Fabric Enabled

Mobility

Selective Reanchor Enabled

U3 Interface

U3 Interface Enabled

U3 Reporting Interval

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。

The screenshot shows the Cisco AP Groups configuration page. The 'WLANs' tab is selected. The 'Add New AP Group' form is displayed with the following fields:

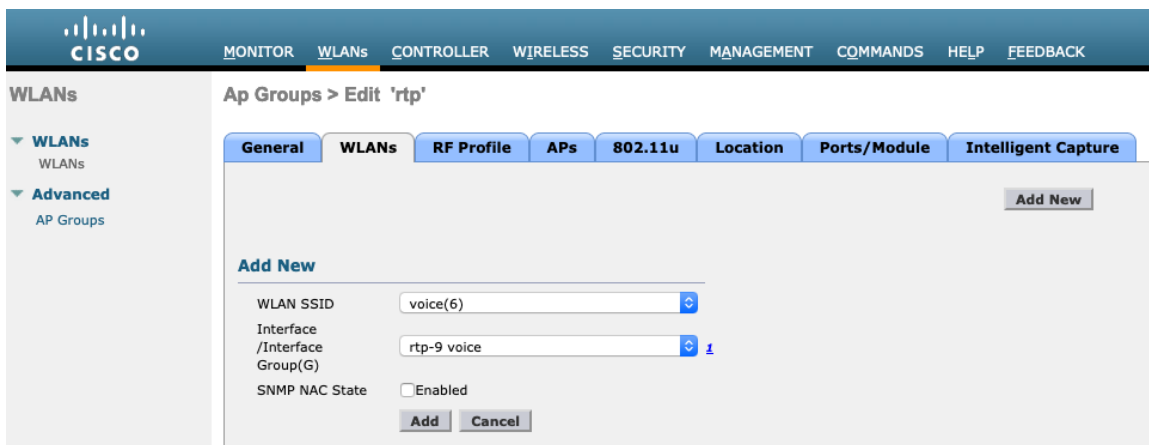
- AP Group Name: rtp
- Description: (empty)

Buttons: Add, Cancel

The screenshot shows the Cisco AP Groups configuration page for editing the 'rtp' group. The 'WLANs' tab is selected. The 'Edit' page has several tabs: General, WLANs, RF Profile, APs, 802.11u, Location, Ports/Module, and Intelligent Capture. The 'WLANs' tab is active, and the 'Apply' button is visible.

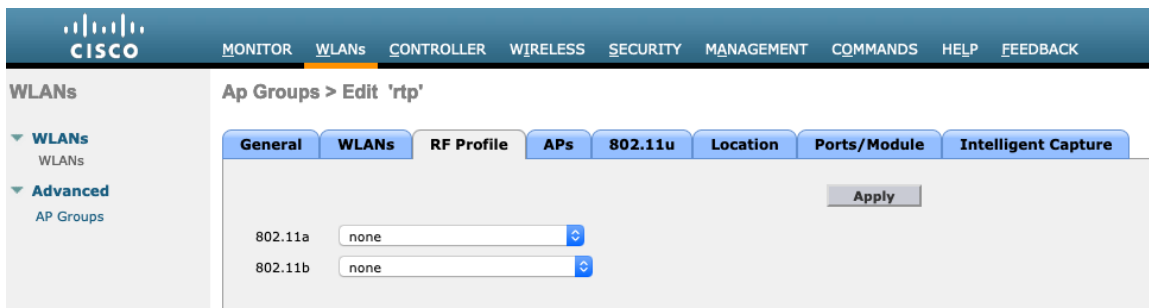
AP Group Name	rtp
AP Group Description	(empty)
NAS-ID	RTP9-32A-WLC3
Enable Client Traffic QinQ	<input type="checkbox"/>
Enable DHCPv4 QinQ	<input type="checkbox"/>
QinQ Service Vlan Id	0
Fabric ACL Template	None
CAPWAP Preferred Mode	<input type="checkbox"/> Not-Configured
Custom Web Override-Global	<input type="checkbox"/> Enable
External Web auth URL	none
NTP Auth	<input type="checkbox"/> Enable
NTP Server	None

[WLAN (WLANs)] タブで、対象 SSID と、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。



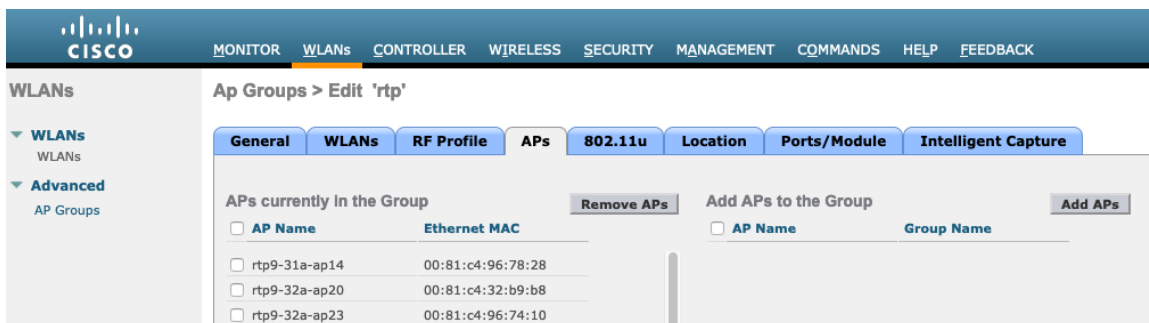
[RF プロファイル (RF Profile)] タブで、対象の 802.11a または 802.11b RF プロファイルを選択して、[適用 (Apply)] を選択します。

アクセス ポイントが AP グループに結合された後で変更が加えられた場合、変更の適用後にアクセス ポイントが再起動します。



[AP (APs)] タブで、対象アクセスポイントを選択して、[AP の追加 (Add APs)] を選択します。

その後、選択したアクセス ポイントが再起動します。



コントローラの設定

Cisco ワイヤレス LAN コントローラ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 ワイヤレス LAN コントローラ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。

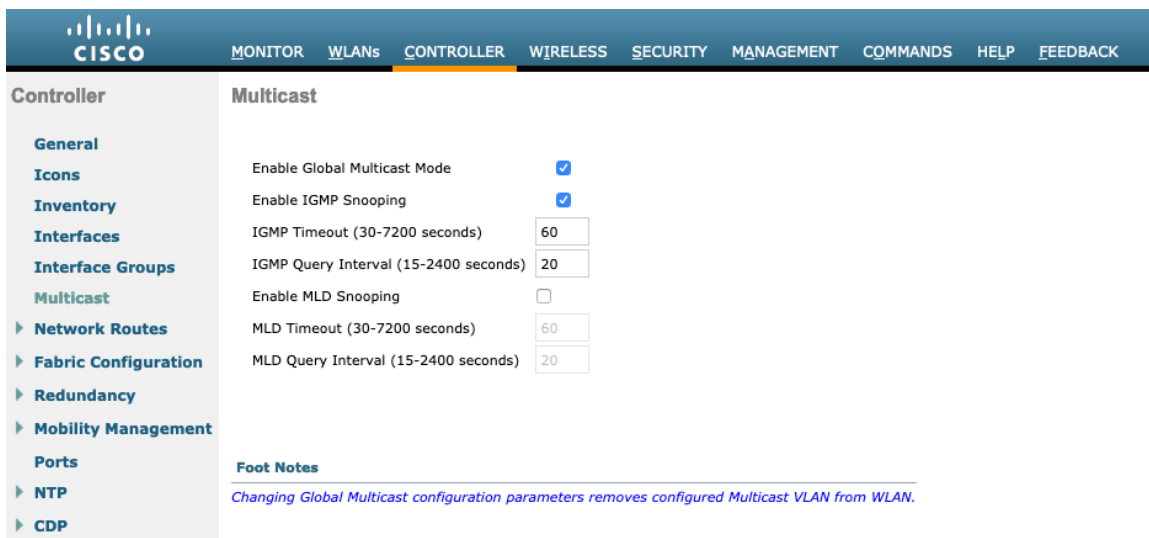
対象の AP マルチキャスト モードを設定します。

The screenshot shows the Cisco Controller configuration page for the General tab. The left sidebar lists various configuration categories, and the main area displays a list of settings for the controller. The settings include:

- Name: RTP9-32A-WLC3
- 802.3x Flow Control Mode: Disabled
- LAG Mode on next reboot: Enabled
- Broadcast Forwarding: Disabled
- AP Multicast Mode: Multicast (Multicast Group Address: 239.1.1.9)
- AP IPv6 Multicast Mode: Multicast (IPv6 Multicast Group Address: ff1e::239:100:100:21)
- AP Fallback: Enabled
- CAPWAP Preferred Mode: ipv4
- Fast SSID change: Enabled
- Link Local Bridging: Disabled
- Default Mobility Domain Name: CTG-VoWLAN2
- RF Group Name: RTP9-VoWLAN2
- User Idle Timeout (seconds): 300
- ARP Timeout (seconds): 300
- ARP Unicast Mode: Disabled
- Web Radius Authentication: PAP
- Operating Environment: Commercial (10 to 35 C)
- Internal Temp Alarm Limits: 10 to 38 C
- WebAuth Proxy Redirection Mode: Disabled
- WebAuth Proxy Redirection Port: 0
- Captive Network Assistant Bypass: Disabled
- Global IPv6 Config: Disabled
- Web Color Theme: Default
- HA SKU secondary unit: Disabled
- Nas-Id: RTP9-32A-WLC3
- HTTP Profiling Port: 80
- DNS Server IP (IPv4/IPv6): 171.70.168.183
- HTTP-Proxy Ip Address (IPv4/IPv6): 0.0.0.0
- WGB Vlan Client: Disabled

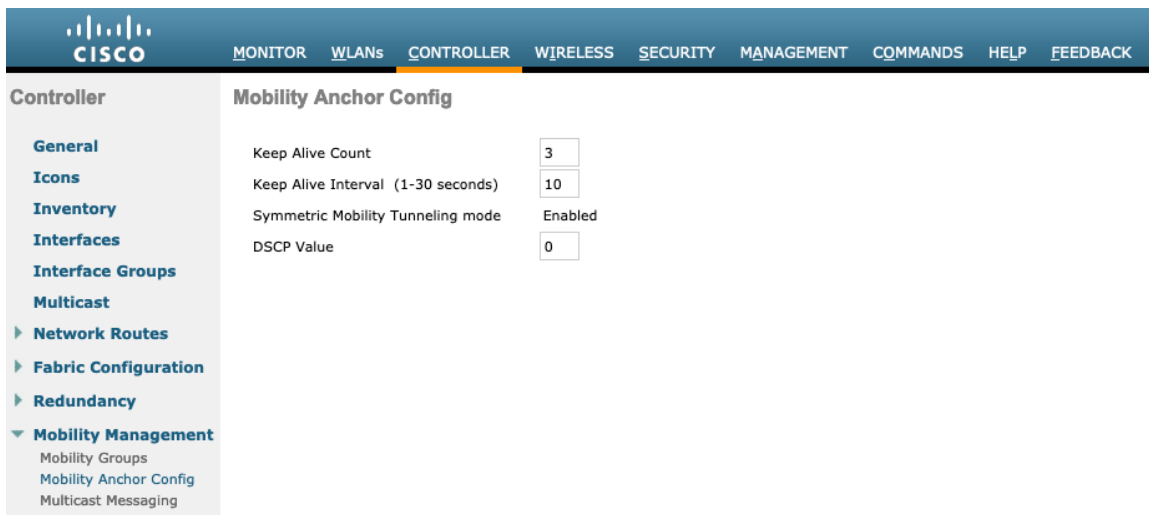
Footnote 1: Multicast is not supported with FlexConnect on this platform. Multicast-Unicast mode does not support IGMP/MLD Snooping. Disable Global Multicast first.
Footnote 2: Changes in Web color Theme will get updated after browser Refresh.

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。

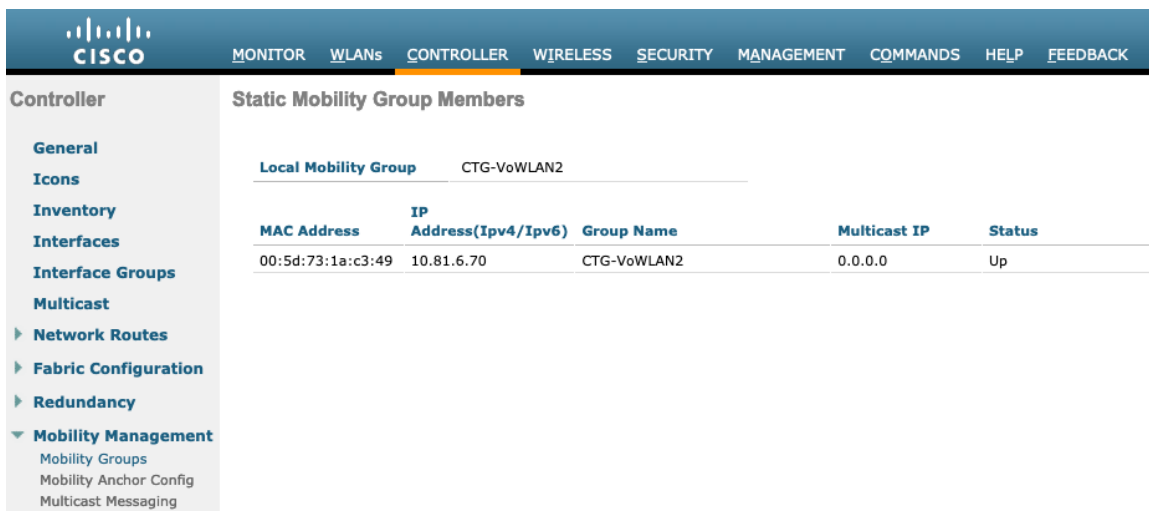


レイヤ 3 モビリティを使用している場合は、[シンメトリック モビリティ トンネリング (Symmetric Mobility Tunneling)] を [有効 (Enabled)] に設定する必要があります。

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 ワイヤレス LAN コントローラを同じモビリティ グループに設定する場合、各 Cisco ワイヤレス 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。



The screenshot shows the Cisco Controller web interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER (highlighted), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar shows a menu with categories like General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, and Mobility Management. The main content area is titled 'Static Mobility Group Members' and shows a table for the 'Local Mobility Group' 'CTG-VoWLAN2'.

MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
00:5d:73:1a:c3:49	10.81.6.70	CTG-VoWLAN2	0.0.0.0	Up

コール アドミッション制御 (CAC)

[音声 (Voice)] で **[アドミッションコントロール必須 (Admission Control Mandatory)]** を有効にして、使用する帯域 (5 GHz または 2.4 GHz) に対して最大帯域幅および予約済みのローミング帯域幅の各割合を設定することを推奨します。

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以外も使用できますが、その他の帯域幅がすべて使用されている場合に備え、ローミングクライアント向けに一定のローミング帯域幅が予約されます。

CAC を有効にする場合は、**[ロードベース CAC (Load Based CAC)]** が有効になっていることを確認します。

ロードベース CAC は、チャンネル上のすべての出力を考慮します。

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
 - Network
 - RRM
 - RF Grouping
 - TPC
 - DCA
 - Coverage
 - General
 - Client Roaming
 - Media
 - EDCA Parameters
 - DFS (802.11h)
 - High Throughput (802.11n/ac/ax)
 - CleanAir
- 802.11b/g/n/ax

802.11a(5 GHz) > Media

Voice Video Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method ⁴ Load Based ▾

Max RF Bandwidth (5-85)(%) 75

Reserved Roaming Bandwidth (0-25)(%) 6

Expedited bandwidth

SIP CAC Support ³ Enabled

Per-Call SIP Bandwidth ²

SIP Codec G.711 ▾

SIP Bandwidth (kbps) 64

SIP Voice Sample Interval (msecs) 20 ▾

Traffic Stream Metrics

Metrics Collection

Foot Notes

- ¹ 11a rates(Kbps): 6000,9000,12000,18000,24000,36000,48000,54000
11n rates(Kbps): 65000,72200,130000,144400,135000,150000,270000,300000
- ² SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- ³ SIP CAC will be supported only if SIP snooping is enabled.
- ⁴ Static CAC method is radio based and load-based CAC method is channel based.

[ビデオ (Video)] で [アドミッションコントロール必須 (Admission Control Mandatory)] を無効にする必要があります。

Wireless

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

802.11a(5 GHz) > Media

Voice Video **Media**

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method [4](#) Static

Max RF Bandwidth (5-85)(%)

Reserved Roaming Bandwidth (0-25)(%)

SIP CAC Support [3](#) Enabled

Foot Notes

1 11a rates(Kbps): 6000,9000,12000,18000,24000,36000,48000,54000
11n rates(Kbps): 65000,72200,130000,144400,135000,150000,270000,300000

2 SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.

3 SIP CAC will be supported only if SIP snooping is enabled.

4 Static CAC method is radio based and load-based CAC method is channel based.

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」で表示可能です）。

コールアドミッション制御 (CAC) 設定

Voice AC - Admission control (ACM).....有効

Voice max RF bandwidth..... 75

Voice reserved roaming bandwidth.....6

Voice load-based CAC mode.....有効

Voice tspec inactivity timeout..... 無効

Voice AC - Admission control (ACM).....[無効 (Disabled)]

Voice Stream-Size.....84000

Voice Max-Streams..... 2

Voice 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により調整できます。
SRTP を使用している場合は、音声 Stream-Size を増やす必要がある場合があります。

```
(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、次のコマンドを使って表示可能です。

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

```
Quality of Service..... プラチナ(音声)
WMM..... 必須
Dot11-Phone Mode (7920)..... ap-cac-limit
Wired Protocol..... なし
```

音声 TSPEC 非アクティブタイムアウトが無効になっていることを確認します。

```
(Cisco Controller) >config 802.11a cac voice tspec-inactivity-timeout ignore
```

```
(Cisco Controller) >config 802.11b cac voice tspec-inactivity-timeout ignore
```

メディアの設定で、[ユニキャスト ビデオ リダイレクト (Unicast Video Redirect)]と [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。

802.11a(5 GHz) > Media

General

Unicast Video Redirect

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%))	85
Client Minimum Phy Rate ¹	6000
Maximum Retry Percent (0-100%)	80

Media Stream - Multicast Direct Parameters

Multicast Direct Enable	<input checked="" type="checkbox"/>
Max Streams per Radio	No-limit
Max Streams per Client	No-limit
Best Effort QoS Admission	<input type="checkbox"/> Enabled

Foot Notes

¹ 11a rates(Kbps): 6000,9000,12000,18000,24000,36000,48000,54000
¹¹ⁿ rates(Kbps): 65000,72200,130000,144400,135000,150000,270000,300000
² SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
³ SIP CAC will be supported only if SIP snooping is enabled.
⁴ Static CAC method is radio based and load-based CAC method is channel based.

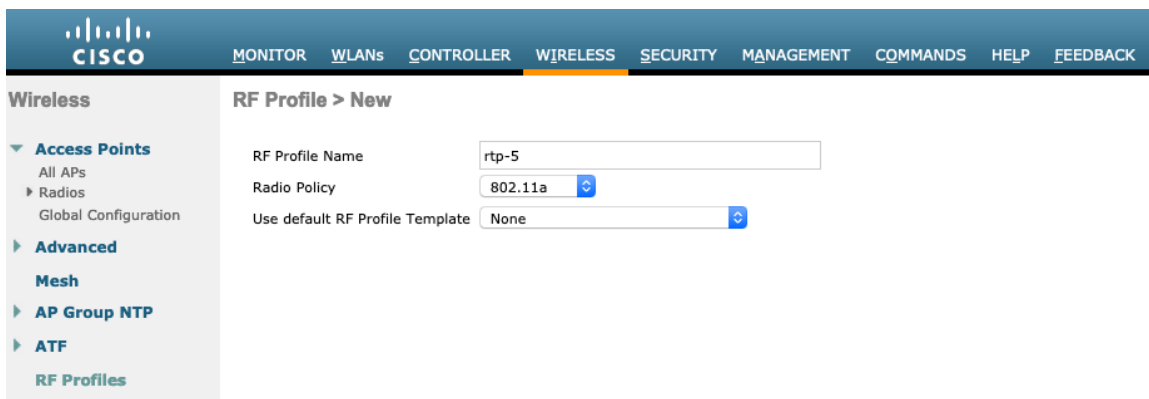
RF プロファイル

RF プロファイルを作成し、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 設定などを指定できます。

Cisco Wireless Phone 840 および 860 で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。作成した RF プロファイルは、AP グループに適用されます。

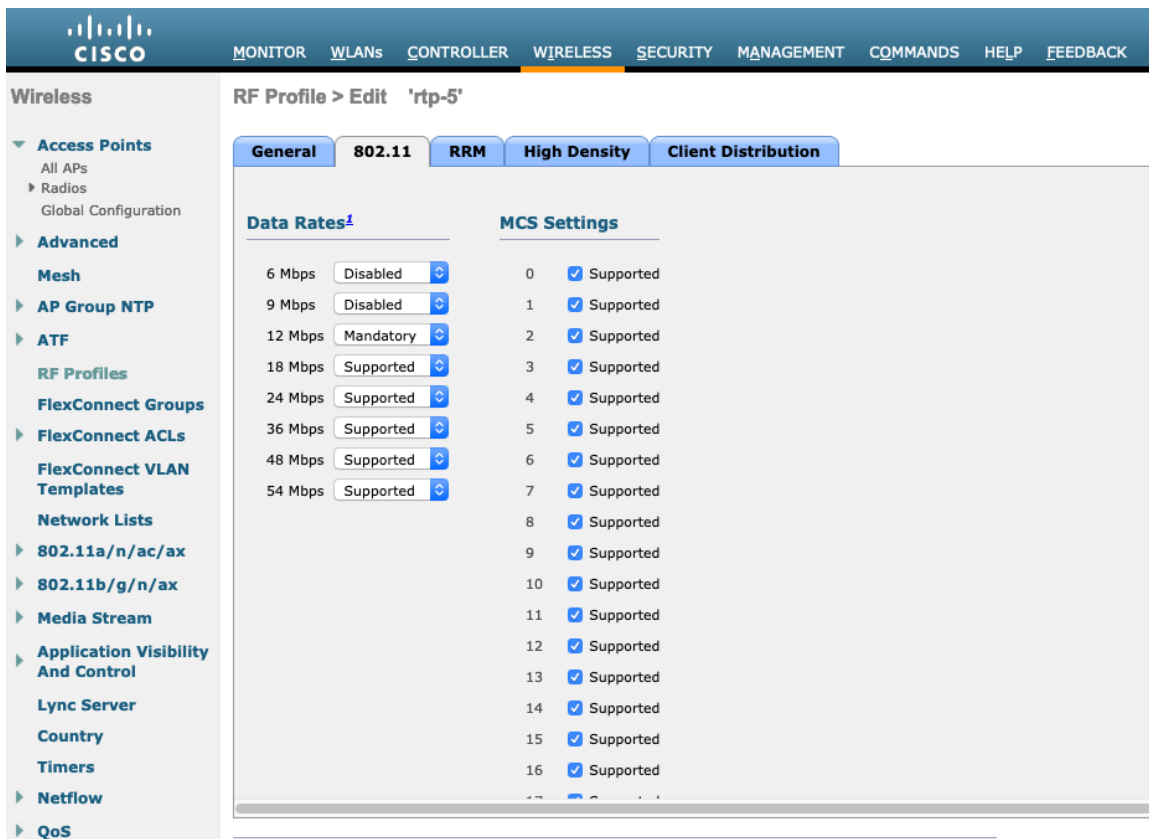
RF プロファイルを作成する場合、[RF プロファイル名 (RF Profile Name)] と [無線ポリシー (Radio Policy)] を定義する必要があります。

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



[802.11] タブで、必要に応じて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生じます。



[RRM] タブでは、[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)] 設定と、その他の [DCA]、[TPC]、および [カバレッジホール検出 (Coverage Hole Detection)] 設定を設定できます。

RF Profile > Edit 'rtp-5'

General 802.11 RRM High Density Client Distribution

TPC

Maximum Power Level Assignment (-10 to 30 dBm) 30
 Minimum Power Level Assignment (-10 to 30 dBm) -10
 Power Threshold v1(-80 to -50 dBm) -70
 Power Threshold v2(-80 to -50 dBm) -67

DCA

Avoid Foreign AP Interference Enabled
 Channel Width 20 MHz 40 MHz 80 MHz 160 MHz 80+80 MHz Best

Coverage Hole Detection

Data RSSI(-90 to -60 dBm) -80
 Voice RSSI(-90 to -60 dBm) -80
 Coverage Exception(0 to 100 %) 25
 Coverage Level(1 to 200 Clients) 3

Profile Threshold For Traps

Interference (0 to 100%) 10
 Clients (1 to 200) 12
 Noise (-127 to 0 dBm) -70
 Utilization (0 to 100 %) 80

Client Network Preference

Connectivity Throughput Automatic

Client Aware

Enable Disable

High-Speed Roam

HSR mode Enabled

RF Profile > Edit 'rtp-5'

General 802.11 RRM High Density Client Distribution

High-Speed Roam

HSR mode Enabled
 Neighbor Timeout Factor 5

DCA Channel List

DCA Channels
 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52

Extended UNII-2 channels Enabled

Client Aware

Enable Disable

[高密度 (High Density)] タブでは、[最大クライアント数 (Maximum Clients)]、[マルチキャストデータレート (Multicast Data Rates)]、および[Rx Sop のしきい値 (Rx Sop Threshold)]を設定できます。

[Rx Sop のしきい値 (Rx Sop Threshold)]にはデフォルト値を使用することを推奨します。

RF Profile > Edit 'rtp-5'

General 802.11 RRM High Density Client Distribution

High Density Parameters

Maximum Clients(1 to 200) 200

Multicast Parameters

Multicast Data Rates² auto

Rx Sop Threshold Parameters⁵

Rx Sop Threshold⁶ Default 0 Custom

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。

802.11r (FT) または 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のみ、シームレスなローミングを実現できます。

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar lists various configuration options under 'Wireless', with 'FlexConnect Groups' selected. The main content area is titled 'FlexConnect Groups > New' and contains a single text input field labeled 'Group Name' with the value 'rtp-1' entered.

The screenshot shows the Cisco Wireless configuration interface for editing a FlexConnect Group. The top navigation bar is the same as the previous screenshot. The left sidebar is also the same. The main content area is titled 'FlexConnect Groups > Edit 'rtp-1''. It features several tabs: 'General', 'Local Authentication', 'Image Upgrade', 'ACL Mapping', 'Central DHCP', 'WLAN VLAN mapping', and 'WLAN AVC mapping'. The 'General' tab is active and shows the following fields: 'Group Name' (rtp-1), 'VLAN Template Name' (none), and 'Enable AP Local Authentication' (checkbox). Below this is the 'FlexConnect AP' section, followed by the 'HTTP-Proxy' section with 'Ip Address(Ipv4/Ipv6)' and 'Port' fields, and an 'Add' button. The 'AAA' section includes 'Server Ip Address', 'Server Type' (Primary), 'Shared Secret', 'Confirm Shared Secret', and 'Port Number' (1812) fields, with an 'Add' button at the bottom.

FlexConnect グループごとに許可されるアクセスポイントの最大数は制限されており、これは WLC モデル固有です。

Wireless

FlexConnect Group AP List

Group Name rtp-1

FlexConnect APs

Add AP

Entries 0 - 0 of 0

AP MAC Address	AP Name	Status	AP Mode	Type	Conflict with PnP
----------------	---------	--------	---------	------	-------------------

Wireless

FlexConnect Group AP List

Group Name rtp-1

FlexConnect APs

Add AP

Select APs from current controller

Ethernet MAC

Add Cancel

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。

Wireless

Media Stream > General

Multicast Direct feature Enabled

Session Message Config

Session announcement State Enabled

Session announcement URL

Session announcement Email

Session announcement Phone

Session announcement Note

次に、ストリームを設定します。

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the configuration tree with 'Media Stream' selected under 'Wireless'. The main content area is titled 'Media Streams' and shows a table with one entry:

Stream Name	Start IP Address(Ipv4/Ipv6)	End IP Address(Ipv4/Ipv6)	Operation Status
10.195.19.27	239.1.1.1	239.1.1.1	Multicast Direct <input checked="" type="checkbox"/>

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

The screenshot shows the Cisco WLAN configuration interface for the 'voice' WLAN. The top navigation bar is the same as the previous screenshot. The left sidebar shows 'WLANs' selected. The main content area is titled 'WLANs > Edit 'voice'' and has tabs for General, Security, QoS, Policy-Mapping, and Advanced. The 'QoS' tab is active, showing the 'Override Per-SSID Bandwidth Contracts (kbps)' section with the following settings:

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Below this is a 'Clear' button. The 'WMM' section has the following settings:

WMM Policy	Required
7920 AP CAC	<input checked="" type="checkbox"/> Enabled
7920 Client CAC	<input type="checkbox"/> Enabled

The 'Media Stream' section has the following setting:

Multicast Direct	<input checked="" type="checkbox"/> Enabled
------------------	---

The 'Lync Policy' section has the following setting:

Audio	Silver
-------	--------

QoS プロファイル

次の 4 つの QoS プロファイルを設定します。

QoS プロファイル	プロトコルタイプ	802.1P タグ
Platinum	なし	なし
Gold	802.1p	4
Bronze	802.1p	1
Silver	802.1p	0

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), SECURITY, MANAGEMENT, COMMANDS, HELP. The left sidebar shows the 'Wireless' menu with various options like Access Points, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, 802.11a/n/ac/ax, 802.11b/g/n/ax, Media Stream, Application Visibility And Control, Lync Server, Country, Timers, Netflow, and QoS (Profiles, Roles, Qos Map). The main content area is titled 'Edit QoS Profile' and shows the configuration for the 'platinum' profile. The 'QoS Profile Name' is 'platinum' and the 'Description' is 'For Voice Applications'. There are two sections for bandwidth contracts: 'Per-User Bandwidth Contracts (kbps) *' and 'Per-SSID Bandwidth Contracts (kbps) *'. Each section has four rows for Average Data Rate, Burst Data Rate, Average Real-Time Rate, and Burst Real-Time Rate, with input fields for DownStream and UpStream values, all set to 0. There are also 'WLAN QoS Parameters' with dropdown menus for Maximum Priority (voice), Unicast Default Priority (besteffort), and Multicast Default Priority (besteffort). Finally, there is a 'Wired QoS Protocol' section with a dropdown menu for Protocol Type set to 'None'.

Wireless

- ▼ Access Points
 - All APs
 - ▶ Radios
 - Global Configuration
- ▶ Advanced
- Mesh
- ▶ AP Group NTP
- ▶ ATF
- RF Profiles
- FlexConnect Groups
- ▶ FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- ▶ 802.11a/n/ac/ax
- ▶ 802.11b/g/n/ax
- ▶ Media Stream
- ▶ Application Visibility And Control
- Lync Server
- Country
- Timers
- ▶ Netflow
- ▼ QoS
 - Profiles
 - Roles
 - Qos Map

Edit QoS Profile

QoS Profile Name gold

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority ▼

Unicast Default Priority ▼

Multicast Default Priority ▼

Wired QoS Protocol

Protocol Type ▼

802.1p Tag

Wireless

- ▼ **Access Points**
 - All APs
 - ▶ Radios
 - Global Configuration
- ▶ **Advanced**
- Mesh**
- ▶ **AP Group NTP**
- ▶ **ATF**
- RF Profiles**
- FlexConnect Groups**
- ▶ **FlexConnect ACLs**
- FlexConnect VLAN Templates**
- Network Lists**
- ▶ **802.11a/n/ac/ax**
- ▶ **802.11b/g/n/ax**
- ▶ **Media Stream**
- ▶ **Application Visibility And Control**
- Lync Server**
- Country**
- Timers**
- ▶ **Netflow**
- ▼ **QoS**
 - Profiles
 - Roles
 - Qos Map

Edit QoS Profile

QoS Profile Name bronze

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority	<input type="text" value="background"/>
Unicast Default Priority	<input type="text" value="background"/>
Multicast Default Priority	<input type="text" value="background"/>

Wired QoS Protocol

Protocol Type	<input type="text" value="802.1p"/>
802.1p Tag	<input type="text" value="1"/>

CISCO MONITOR WLANs CONTROLLER **WIRELESS** SECURITY MANAGEMENT COMMANDS HELP

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
 - Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
- 802.11b/g/n/ax
- Media Stream
- Application Visibility And Control
- Lync Server
- Country
- Timers
- Netflow
- QoS
 - Profiles
 - Roles
 - Qos Map

Edit QoS Profile

QoS Profile Name silver

Description For Best Effort

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority besteffort

Unicast Default Priority besteffort

Multicast Default Priority besteffort

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 0

詳細設定

EAP の詳細設定

グローバルレベルでのみ設定できる EAP ブロードキャストキー間隔を除き、すべての EAP パラメータは SSID ごとまたはグローバルレベルで設定できます。

EAP パラメータを表示または設定するには、[セキュリティ (Security)] > [高度な EAP (Advanced EAP)] を選択します。

The screenshot shows the Cisco configuration interface for Advanced EAP. On the left, there is a navigation menu with 'Security' expanded and 'Advanced EAP' selected. The main area displays several EAP parameters with their current values in input fields:

- Identity Request Timeout (in secs): 30
- Identity request Max Retries: 2
- Dynamic WEP Key Index: 0
- Request Timeout (in secs): 30
- Request Max Retries: 2
- Max-Login Ignore Identity Response: enable (dropdown menu)
- EAPOL-Key Timeout (in milliseconds): 400
- EAPOL-Key Max Retries: 4
- EAP-Broadcast Key Interval(in secs): 3600

コマンドラインを介して Cisco Wireless LAN Controller の EAP パラメータを表示するには、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
EAP-Broadcast Key Interval.....3,600
```

802.1x を使用する場合、Cisco ワイヤレス LAN コントローラの **[EAP 要求タイムアウト (EAP-Request Timeout)]** を少なくとも 20 秒に設定する必要があります。

Cisco ワイヤレス LAN コントローラソフトウェアの最近のバージョンでは、デフォルトの **[EAP 要求タイムアウト (EAP-Request Timeout)]** が 2 秒から 30 秒に変更されました。

EAP の失敗が頻繁に発生する展開では、**[EAP 要求タイムアウト (EAP-Request Timeout)]** を 30 秒未満に減らす必要があります。

Cisco ワイヤレス LAN コントローラに対する **[EAP 要求タイムアウト (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
```

PSK を使用する場合は、**[EAPOL キーのタイムアウト (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 キーの最大試行回数 (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。

802.1x を使用する場合は、**[EAPOL キーのタイムアウト (EAPOL-Key Timeout)]** および **[EAPOL キーの最大試行回数 (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 キーのタイムアウト (EAPOL-Key Timeout)] は、1000 ミリ秒 (1 秒) を超えないようにしてください。

Cisco ワイヤレス LAN コントローラに対する **[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 ワイヤレス LAN コントローラに対する **[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
```

[EAP-Broadcast Key Interval] が 3600 秒 (1 時間) 以上に設定されていることを確認します。

Cisco ワイヤレス LAN コントローラに対する **[EAP-Broadcast Key Interval]** 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 bcast-key-interval 3600
```

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 ワイヤレス LAN コントローラで Auto-Immune 機能を無効にすることを推奨します。

Cisco ワイヤレス LAN コントローラに対する 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.....[無効 (Disabled) ]
```

Client Exclusion Policy

Excessive 802.11-association failures..... 有効
Excessive 802.11-authentication failures..... 有効
Excessive 802.1x-authentication..... 有効
IP-theft..... 有効
Excessive Web authentication failure..... 有効

Signature Policy

Signature Processing..... 有効

Cisco ワイヤレス LAN コントローラに対する 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
```

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 Wireless Phone 840 および 860 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は 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><tolerance> Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds;  
Default tolerance 1000 msec
```

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>** と入力します。これにより、次のように表示されます。

```
CCKM tsf Tolerance.....5000
```

不正ポリシー

[不正ロケーション検出プロトコル (Rogue Location Discovery Protocol)] にはデフォルト値 ([無効 (Disable)]) の使用を推奨します。

The screenshot displays the Cisco Catalyst IOS XE configuration page for 'Rogue Policies'. The left sidebar shows a navigation tree with 'Wireless Protection Policies' expanded to 'Rogue Policies'. The main configuration area is titled 'Rogue Policies' and includes a 'Rogue Detection Security Level' section with radio buttons for Low, High, Critical, and Custom (selected). Below this are various configuration options for Rogue Location Discovery Protocol, such as 'Rogue Location Discovery Protocol' (set to Disable), 'Expiration Timeout for Rogue AP and Rogue Client entries' (1200 Seconds), and 'Detect and report Ad-Hoc Networks' (checked). An 'Auto Contain' section is also visible with 'Auto Containment Level' set to 1.

Cisco Catalyst IOS XE ワイヤレス LAN コントローラおよび Lightweight アクセスポイント

Cisco ワイヤレス LAN コントローラおよび Lightweight 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。

- [802.11r (FT)] または [CCKM] が [有効 (Enabled)] になっていることを確認します。
- [Quality of Service (QoS) SSID ポリシー (Quality of Service (QoS) SSID Policy)] を [プラチナ (Platinum)] に設定します
- [WMM ポリシー (WMM Policy)] を [必須 (Required)] に設定します
- 802.11k を [有効 (Enabled)] に設定することを推奨
- 802.11v を [有効 (Enabled)] に設定することを推奨
- [セッションタイムアウト (Session Timeout)] が有効で、正しく設定されていることを確認します

- [キーのブロードキャスト間隔 (Broadcast Key Interval)] が有効になっていて、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) ブロッキング アクション (P2P (Peer to Peer) Blocking Action)] を無効にします。
- [クライアント除外タイムアウト (Client Exclusion Timeout)] が正しく設定されていることを確認します
- [DHCP が必要です (DHCP Required)] を無効にします
- [保護された管理フレーム (PMF) (Protected Management Frame (PMF)] は、[任意 (Optional)] または [無効 (Disabled)] に設定する必要があります
- [DTIM 周期 (DTIM Period)] を [2] に設定します
- [負荷分散 (Load Balance)] を [無効 (Disabled)] に設定します
- [帯域選択 (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。
- 必要に応じて [データレート (Data Rates)] を設定します
- 必要に応じて [RRM] を設定します
- [ボイス (Voice)] で、[アドミッション制御必須 (Admission Control Mandatory)] を [有効 (Enabled)] に設定します。
- [ボイス (Voice)] で [ロードベース CAC (Load Based CAC)] を [有効 (Enabled)] に設定します。
- [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。
- [EDCA プロファイル (EDCA Profile)] を [音声の最適化 (Voice Optimized)] または [音声およびビデオの最適化 (Voice and Video Optimized)] 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。
- [チャンネルスイッチステータス (Channel Switch Status)] と [スマート DFS (Smart DFS)] を有効にします
- [チャンネル スイッチ アナウンス モード (Channel Switch Announcement Mode)] を [待機 (Quiet)] に設定します
- 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
- [CleanAir] を有効にします
- [マルチキャストダイレクト対応 (Multicast Direct Enable)] を有効にします

802.11 ネットワークの設定

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域で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。

5 GHz を使用する場合は、5 GHz ネットワークのステータスが **[有効 (Enabled)]** に設定され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。

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 以上をそれぞれ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ります。

The screenshot shows the configuration page for the 5 GHz Network on a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "Configuration > Radio Configurations > Network". The "5 GHz Band" tab is selected. The "General" section is expanded, showing the following settings:

- 5 GHz Network Status:
- Beacon Interval*: 100
- Fragmentation Threshold(bytes)*: 2346
- DTPC Support:

There are two warning messages in yellow boxes:

- "Please disable 5 GHz Network Status to configure Beacon Interval, Fragmentation Threshold, DTPC Support."
- "Please disable 5 GHz Network Status to configure Data Rates"

The "Data Rates" section shows the following settings:

Rate	Status	Value	Requirement
6 Mbps	Disabled	9 Mbps	Mandatory
12 Mbps	Disabled	12 Mbps	Mandatory
18 Mbps	Supported	24 Mbps	Supported
36 Mbps	Supported	36 Mbps	Supported
48 Mbps	Supported	54 Mbps	Supported

2.4 GHz を使用する場合は、2.4 GHz ネットワークのステータスと 802.11g ネットワークのステータスが **[有効 (Enabled)]** に設定され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。

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、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、サポート対象 (任意) レートとして 12 Mbps 以上をそれぞれ設定する必要があります。

The screenshot shows the configuration page for the 2.4 GHz Band. The 'General' section includes the following settings:

- 2.4 GHz Network Status:
- 802.11g Network Status:
- Beacon Interval*: 100
- Short Preamble:
- Fragmentation Threshold(bytes)*: 2346
- DTPC Support:

The 'CCX Location Measurement' section includes:

- Mode:
- Interval*: 60

The 'Data Rates' section shows a table of data rates with dropdown menus for each rate:

Rate	Setting	Rate	Setting	Rate	Setting
1 Mbps	Disabled	2 Mbps	Disabled	5.5 Mbps	Disabled
6 Mbps	Disabled	9 Mbps	Disabled	11 Mbps	Disabled
12 Mbps	Mandatory	18 Mbps	Supported	24 Mbps	Supported
36 Mbps	Supported	48 Mbps	Supported	54 Mbps	Supported

高スループット (802.11n/ac)

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。

802.11ac データ レートは 5 GHz にのみ適用できます。

[WMM] が有効になっていること、および [WPA2 (AES)] が 802.11n/ac 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 Wireless Phone 840 および 860 は、HT MCS 0 ~ MCS 15 と VHT MCS 0 ~ MCS 9 1SS および 2SS データレートのみをサポートしますが、MIMO アンテナテクノロジーを含む同じ帯域を利用する他の 802.11n/ac クライアントが存在するため、より高いレートが利用可能な場合には、オプションでより高い MCS レートを有効にできます。

Configuration - > Radio Configurations - > High Throughput

5 GHz Band 2.4 GHz Band

Apply

11n

Enable 11n Select All

MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)
<input checked="" type="checkbox"/> 0/(7Mbps)	<input checked="" type="checkbox"/> 1/(14Mbps)	<input checked="" type="checkbox"/> 2/(21Mbps)	<input checked="" type="checkbox"/> 3/(29Mbps)
<input checked="" type="checkbox"/> 4/(43Mbps)	<input checked="" type="checkbox"/> 5/(58Mbps)	<input checked="" type="checkbox"/> 6/(65Mbps)	<input checked="" type="checkbox"/> 7/(72Mbps)
<input checked="" type="checkbox"/> 8/(14Mbps)	<input checked="" type="checkbox"/> 9/(29Mbps)	<input checked="" type="checkbox"/> 10/(43Mbps)	<input checked="" type="checkbox"/> 11/(58Mbps)
<input checked="" type="checkbox"/> 12/(87Mbps)	<input checked="" type="checkbox"/> 13/(116Mbps)	<input checked="" type="checkbox"/> 14/(130Mbps)	<input checked="" type="checkbox"/> 15/(144Mbps)
<input checked="" type="checkbox"/> 16/(22Mbps)	<input checked="" type="checkbox"/> 17/(43Mbps)	<input checked="" type="checkbox"/> 18/(65Mbps)	<input checked="" type="checkbox"/> 19/(87Mbps)
<input checked="" type="checkbox"/> 20/(130Mbps)	<input checked="" type="checkbox"/> 21/(173Mbps)	<input checked="" type="checkbox"/> 22/(195Mbps)	<input checked="" type="checkbox"/> 23/(217Mbps)
<input checked="" type="checkbox"/> 24/(29Mbps)	<input checked="" type="checkbox"/> 25/(58Mbps)	<input checked="" type="checkbox"/> 26/(87Mbps)	<input checked="" type="checkbox"/> 27/(116Mbps)
<input checked="" type="checkbox"/> 28/(173Mbps)	<input checked="" type="checkbox"/> 29/(231Mbps)	<input checked="" type="checkbox"/> 30/(260Mbps)	<input checked="" type="checkbox"/> 31/(289Mbps)

11ac

⚠ The Data rates are for 20MHz channels and Short Guard Interval

Enable 11ac Select All

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/8/(86.7Mbps)	<input checked="" type="checkbox"/> 1/9/(n/a)	<input checked="" type="checkbox"/> 2/8/(173.3Mbps)	<input checked="" type="checkbox"/> 2/9/(n/a)
<input checked="" type="checkbox"/> 3/8/(260.0Mbps)	<input checked="" type="checkbox"/> 3/9/(288.9Mbps)	<input checked="" type="checkbox"/> 4/8/(346.7Mbps)	<input checked="" type="checkbox"/> 4/9/(n/a)

11ax

Enable 11ax Select All

Multiple BSSIDs

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/7	<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 2/7
<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 3/7	<input checked="" type="checkbox"/> 3/9
<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 4/7	<input checked="" type="checkbox"/> 4/9	<input checked="" type="checkbox"/> 4/11
<input checked="" type="checkbox"/> 5/7	<input checked="" type="checkbox"/> 5/9	<input checked="" type="checkbox"/> 5/11	<input checked="" type="checkbox"/> 6/7
<input checked="" type="checkbox"/> 6/9	<input checked="" type="checkbox"/> 6/11	<input checked="" type="checkbox"/> 7/7	<input checked="" type="checkbox"/> 7/9
<input checked="" type="checkbox"/> 7/11	<input checked="" type="checkbox"/> 8/7	<input checked="" type="checkbox"/> 8/9	<input checked="" type="checkbox"/> 8/11

パラメータ

EDCA パラメータセクションで、使用する周波数帯域に応じて 5 GHz または 2.4 GHz の EDCA プロファイルを **[Optimized-voice]** または **[Optimized-video-voice]** に設定します。

DFS (802.11h) セクションで、Cisco Wireless Phone 840 および 860 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)]** を未設定のままにするか、0 dB に設定します。

[チャンネルスイッチステータス (Channel Switch Status)] と **[スマート DFS (Smart DFS)]** が有効になっている必要があります。

[チャンネル スイッチ アナウンス モード (Channel Switch Announcement Mode)] は **[待機 (Quiet)]** に設定する必要があります。

The screenshot shows the configuration page for a Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Radio Configurations > Parameters. The page is for the 5 GHz Band. The EDCA Parameters section shows the EDCA Profile set to 'optimized-video-v...'. The DFS (802.11h) section has a warning: 'DTPC Support is enabled. Please disable it at Network to configure Power Constraint'. Below this, the Power Constraint* is set to 0, Channel Switch Status is checked, Channel Switch Announcement Mode is set to Quiet, and Smart DFS is checked. An Apply button is visible in the top right of the configuration area.

RRM

チャンネルと送信電力設定を管理する自動割り当て方式を有効にすることをお勧めします。

使用する周波数帯域 (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は、電力の最大レベルと最小レベルを指定できます。

The screenshot shows the configuration page for RRM (Radio Resource Management) on a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "5 GHz Band" and "RRM". The "Power Assignment Method" is set to "Automatic". Other settings include:

- Power Assignment Leader: RCDN6-21A-WLC5 (10.201.81.9)
- Transmit Power Update Interval: 600 second(s)
- Last Run: 365 second(s) ago
- Power Neighbor Count: 3
- Max Power Level Assignment: 17
- Min Power Level Assignment: 11
- Power Threshold*: -70

5 GHz を使用する場合は、多数のチャン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ためにチャンネルの数を制限できます（例：12 チャンネルのみ）。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセス ポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

すべてのアクセス ポイントで同じチャンネル幅を使用することを推奨します。

Cisco Catalyst 9800-40 Wireless Controller | Welcome alpha | Search APs and Clients

Configuration > Radio Configurations > RRM

5 GHz Band | 2.4 GHz Band | FRA

General | Coverage | **DCA** | TPC | RF Grouping

Dynamic Channel Assignment Algorithm [Apply]

Channel Assignment Mode: Automatic Freeze Off

Interval: 10 minutes
 Anchortime: 0

Avoid Foreign AP Interference:
 Avoid Cisco AP load:
 Avoid Non 5 GHz Noise:
 Avoid Persistent Non-wifi Interference:

Channel Assignment Leader: RCDN6-21A-WLC5 (10.201.81.9)
 Last Auto Channel Assignment: 475 second(s) ago

DCA Channel Sensitivity: medium
 Channel Width: 20 MHz 40 MHz 80 MHz 160 MHz Best

Auto-RF Channel List

36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136

140 144 149 153 157 161 165

Event Driven RRM

EDRRM:

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

The screenshot displays the configuration interface for the Dynamic Channel Assignment Algorithm (DCA) on a Cisco Catalyst 9800-40 Wireless Controller. The configuration is for the 2.4 GHz Band. The 'Channel Assignment Mode' is set to 'Automatic', with options for 'Freeze' and 'Off'. The 'Interval' is set to 10 minutes, and the 'Anchortime' is 0. Several interference avoidance options are checked, including 'Avoid Foreign AP Interference' and 'Avoid Non 5 GHz Noise'. The 'Channel Assignment Leader' is identified as RCDN6-21A-WLC5 (10.201.81.9), and the last auto channel assignment occurred 531 seconds ago. The 'DCA Channel Sensitivity' is set to medium. The 'Auto-RF Channel List' shows channels 1 through 11, with checkboxes for each channel. The 'Event Driven RRM' section includes the 'EDRRM' option, which is currently unchecked.

使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセスポイントの設定をグローバル設定よりも優先させることができます。

その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

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。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

The screenshot shows the configuration page for a 5 GHz radio on a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "Edit Radios 5 GHz Band" and has two tabs: "Configure" (selected) and "Detail".

General

- AP Name: rcdn6-22a-ap1
- Admin Status: **ENABLED** (green indicator)
- CleanAir Admin Status: **ENABLED** (green indicator)

RF Channel Assignment

- Current Channel: 149
- Channel width: 40 MHz
- Assignment Method: Global

Antenna Parameters

- Antenna Type: Internal
- Antenna Mode: Omni
- Antenna A:
- Antenna B:
- Antenna C:
- Antenna D:
- Antenna Gain: 10

Tx Power Level Assignment

- Current Tx Power Level: 2
- Assignment Method: Global

Buttons: "Cancel" and "Update & Apply to Device".

CleanAir

CleanAir テクノロジーを搭載したCisco 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の有効化 (Enable CleanAir)]** を **[有効 (Enabled)]** にする必要があります。

The screenshot shows the "CleanAir" configuration page in the Cisco Catalyst 9800-40 Wireless Controller. The page is titled "CleanAir" and has two tabs: "General" (selected) and "Trap Configuration".

General

- Enable CleanAir:
- Enable SI:
- Report Interferers:
- Persistent Device Propagation:

Available Interference Types

Interference Types to detect

- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT-like Phone
- Video Camera

Buttons: "Apply".

WLAN の設定

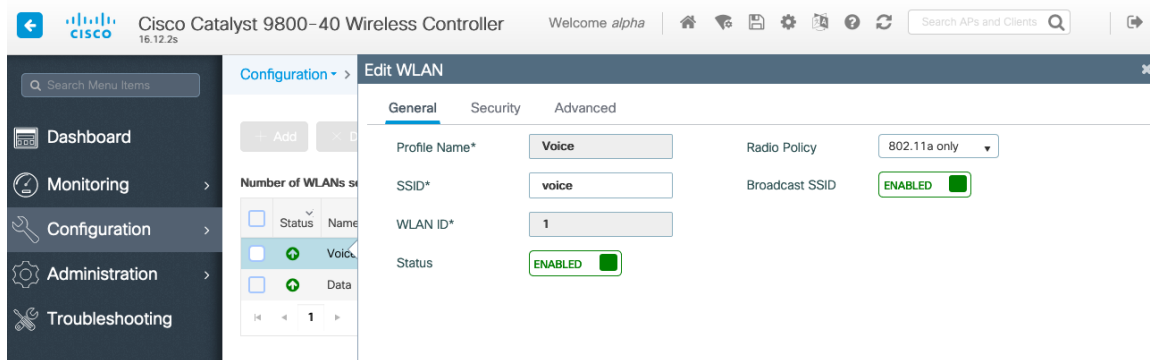
Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

ただし、音声対応 Cisco Wireless LAN 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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ（たとえば 802.11a のみ）適用するよう指定できます。

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャン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。

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 802.11r (FT) を利用するには、**[高速移行 (Fast Transition)]** を**[有効 (Enabled)]** にするボックスをオンにします。

[Over the DS] をオフにして、Over the Distribution システム方式の代わりに Over the Air 方式を使用することを推奨します。

[保護された管理フレーム (PMF) (Protected Management Frame (PMF))] を**[任意 (Optional)]** または**[無効 (Disabled)]** に設定します。

AES (CCMP128) 暗号化を使用した WPA2 ポリシーを有効にします。その後、802.1x と PSK のどちらを使用するかに応じて、認証キー管理タイプとして FT 802.1x と FT PSK のどちらかを有効にします。

Cisco Catalyst 9800-40 Wireless Controller

Welcome alpha

Search APs and Clients

Configuration > Tags & Profiles > Edit WLAN

Number of WLANs selected : 0

Status	Name	ID
<input checked="" type="checkbox"/>	Voice	1
<input checked="" type="checkbox"/>	Data	2

10 items

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode: WPA + WPA2

Fast Transition: Enabled

MAC Filtering:

Over the DS:

Reassociation Timeout: 20

Protected Management Frame

PMF: Disabled

WPA Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption:

- AES(CCMP128)
- CCMP256
- GCMP128
- GCMP256

MPSK:

Auth Key Mgmt:

- 802.1x
- PSK
- CCKM
- FT + 802.1x
- FT + PSK
- 802.1x-SHA256
- PSK-SHA256

Cancel Update & Apply to Device

Cisco Catalyst 9800-40 Wireless Controller

Welcome alpha

Search APs and Clients

Configuration > Tags & Profiles > Edit WLAN

Number of WLANs selected : 0

Status	Name	ID
<input checked="" type="checkbox"/>	Voice	1
<input checked="" type="checkbox"/>	Data	2

10 items

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode: WPA + WPA2

Fast Transition: Enabled

MAC Filtering:

Over the DS:

Reassociation Timeout: 20

Protected Management Frame

PMF: Disabled

WPA Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption:

- AES(CCMP128)
- CCMP256
- GCMP128
- GCMP256

MPSK:

Auth Key Mgmt:

- 802.1x
- PSK
- CCKM
- FT + 802.1x
- FT + PSK
- 802.1x-SHA256
- PSK-SHA256

PSK Format: ASCII

PSK Type: Unencrypted

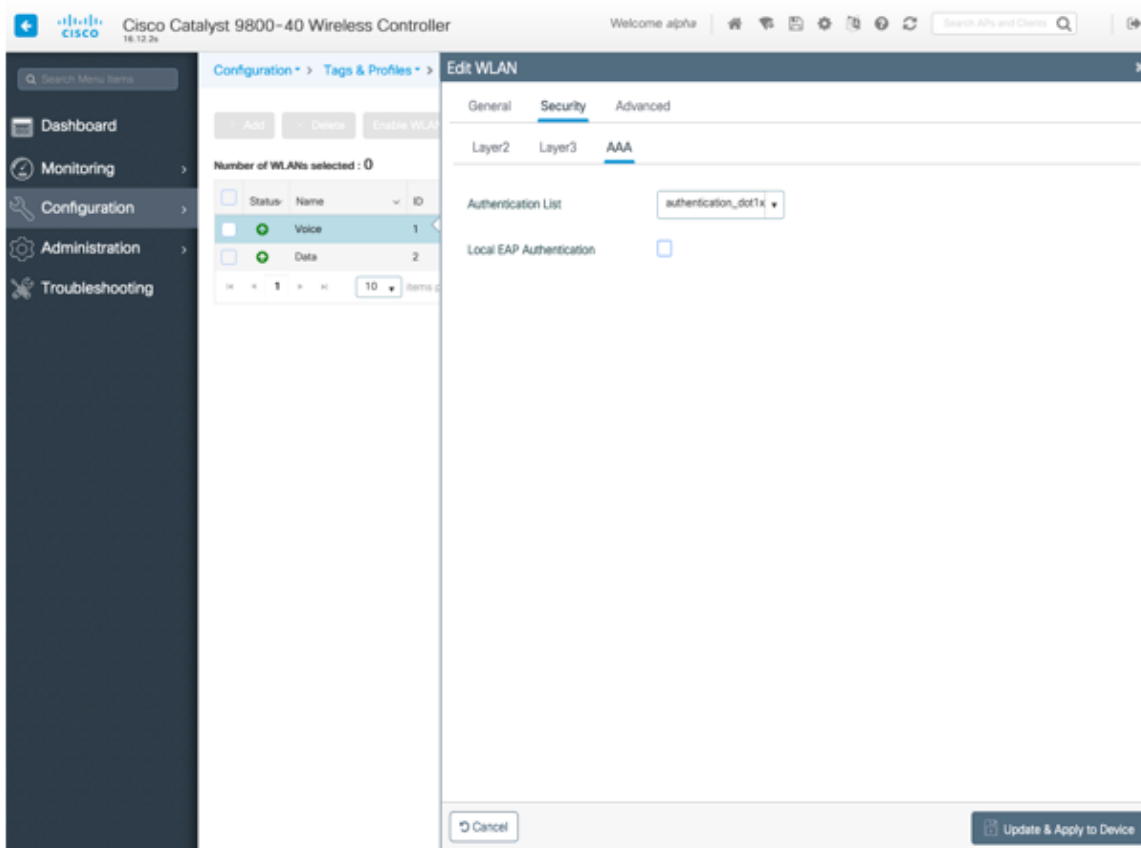
Cancel Update & Apply to Device

各種の音声クライアントに同じ SSID を使用する場合は、802.1x、CCKM、PSK も有効にできます。802.1x や PSK を使用するかどうかに応じて、802.11r (FT) をサポートしない音声クライアントも含まれます。

高速セキュア ローミングに CCKM を利用するには、AES 暗号化を使用した WPA2 ポリシーと認証キー管理タイプ用の 802.1x + CCKM を有効にします。

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 Wireless Phone 840 および 860 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** は 5000 ミリ秒に調整することをお勧めします。



[Aironet IE] は [有効 (Enabled)] にしないでください。

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

WMM ポリシーは、この SSID が Cisco Wireless Phone 840 および 860 などの WMM 対応電話機で使用されている場合にのみ、[必須 (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を別の WLAN に配置することを推奨します。

非 WMM クライアントが Cisco Wireless Phone 840 および 860 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。

WLAN ごと、AP ごと、WLAN ごと、または AP 無線ごとの WLAN ごとの最大クライアント接続は、必要に応じて構成できます。

[オフチャン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。

キュー 4 ~ 6 の遅延優先順位を有効にすることをお勧めします。

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、または優先順位の高いアプリケーション（音声、呼制御など）の DSCP 値がアクセスポイントに保持されていない場合は、優先順位の高いキュー（4 ~ 6）と共に優先順位の低いキュー（0 ~ 3）を有効にしてオフチャンネルスキャンを待機させるとともに、場合によってはスキャンの待機時間を長くすることを推奨します。

EAP エラーが頻繁に発生する展開では、プライオリティキュー 7 を有効にして、EAP 交換中にオフチャンネルスキャンを延期することをお勧めします。

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

[DTIM 周期 (DTIM Period)] を **[2]** に、ビーコン周期を **[100 ミリ秒]** に設定します。

802.11k および 802.11v を有効にすることを推奨します。

ポリシープロファイル

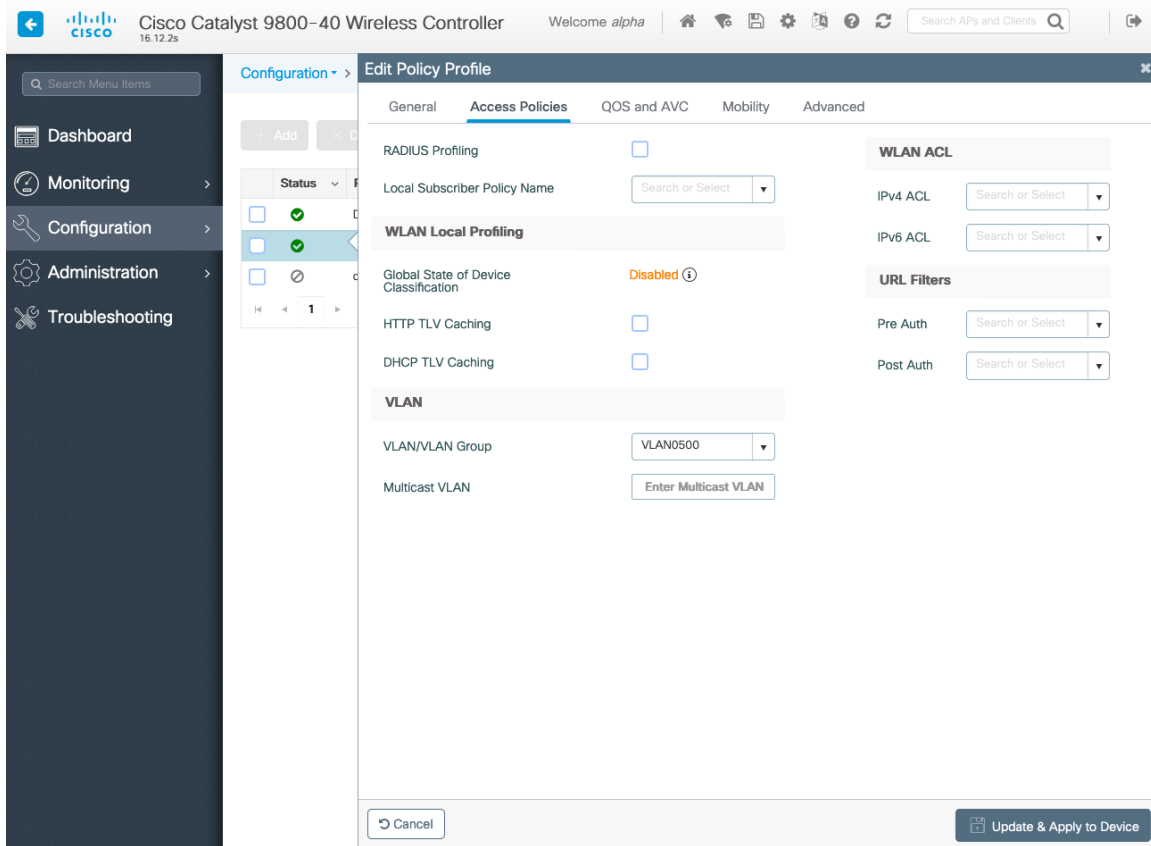
ポリシープロファイルは、アクセス、QoS、モビリティ、および詳細設定に関する追加設定を定義するために使用されます。

次に、ポリシープロファイルは、アクセスポイントに適用できるポリシータグを介して WLAN プロファイルにマッピングされます。

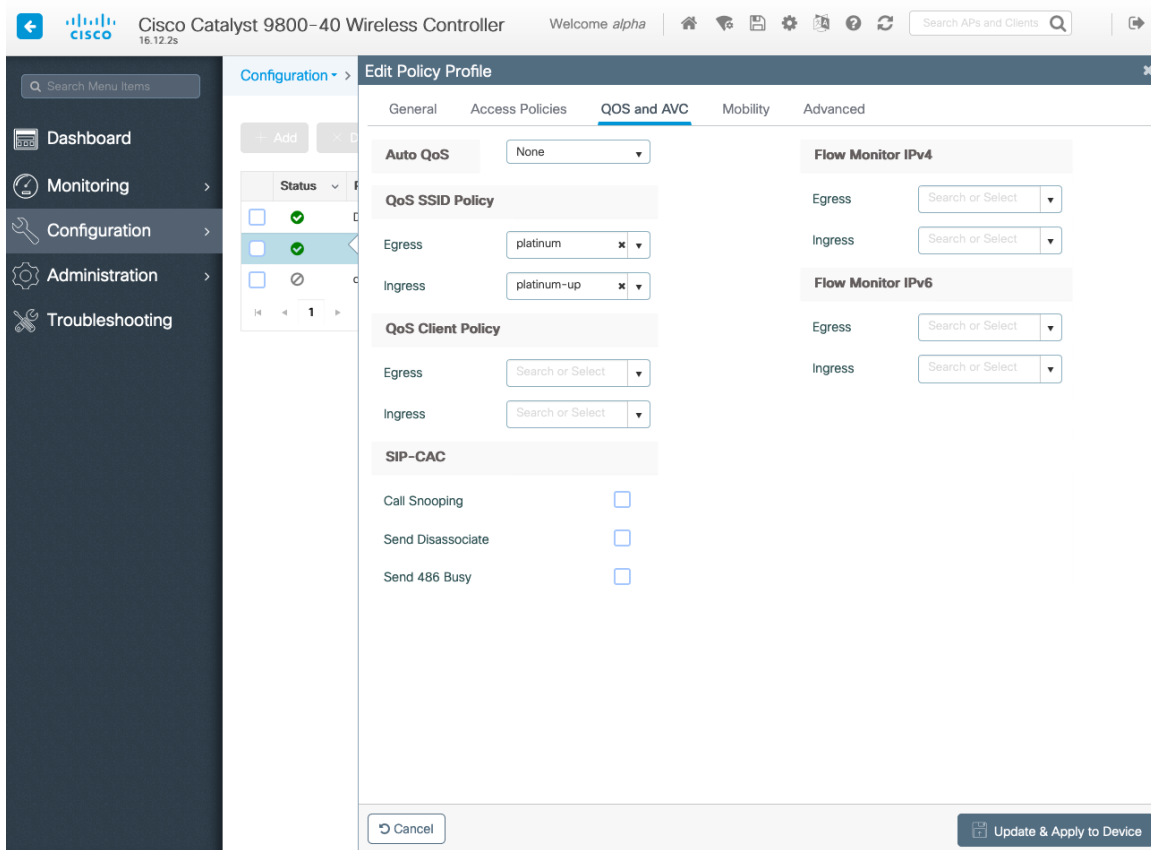
ポリシープロファイルの **[ステータス (Status)]** が **[有効 (Enabled)]** になっていることを確認します。

The screenshot displays the 'Edit Policy Profile' configuration page for a Cisco Catalyst 9800-40 Wireless Controller. The page is titled 'Edit Policy Profile' and has tabs for 'General', 'Access Policies', 'QoS and AVC', 'Mobility', and 'Advanced'. The 'General' tab is active. A warning message at the top states: 'Configuring in enabled state will result in loss of connectivity for clients associated with this profile.' The 'Name*' field is set to 'Voice'. The 'Description' field is empty. The 'Status' is set to 'ENABLED'. The 'Passive Client' and 'Encrypted Traffic Analytics' are set to 'DISABLED'. The 'CTS Policy' section includes 'Inline Tagging' (unchecked), 'SGACL Enforcement' (unchecked), and 'Default SGT' (set to 2-65519). The 'WLAN Switching Policy' section includes 'Central Switching', 'Central Authentication', 'Central DHCP', 'Central Association', and 'Flex NAT/PAT'. 'Central Switching', 'Central Authentication', 'Central DHCP', and 'Central Association' are all set to 'ENABLED', while 'Flex NAT/PAT' is set to 'DISABLED'. The interface includes a navigation menu on the left with options like Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The top bar shows 'Cisco Catalyst 9800-40 Wireless Controller' and 'Welcome alpha'.

ポリシープロファイルで使用する **[VLAN]** または **[VLAN グループ (VLAN Group)]** を選択します。



QoS SSID ポリシーが、出力の場合は [プラチナ (Platinum)] に、入力の場合は [プラチナアップ (Platinum-up)] に設定されていることを確認します。



必要に応じて [セッションタイムアウト (Session Timeout)] を設定します。86400 秒のセッションタイムアウトを有効にして、音声通話中に発生する可能性のある中断を回避することをお勧めします。また、クライアントのログイン情報を定期的に再検証して、クライアントが有効なログイン情報を使用していることを確認することもお勧めします。

必要に応じて [クライアント除外タイムアウト (Client Exclusion Timeout)] を設定します。

[IPv4 DHCP 必須 (IPv4 DHCP Required)] を無効にする必要があります。

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration interface. The main content area is titled 'Edit Policy Profile' and is divided into several sections:

- WLAN Timeout:** Session Timeout (sec) is 86400, Idle Timeout (sec) is 300, Idle Threshold (bytes) is 0, and Client Exclusion Timeout (sec) is checked and set to 60.
- DHCP:** IPv4 DHCP Required is unchecked, and DHCP Server IP Address is empty.
- AAA Policy:** Allow AAA Override and NAC State are unchecked. Policy Name is 'default-aaa-policy' and Accounting List is empty.
- WLAN Flex Policy:** WLAN Central Switching is unchecked. Split MAC ACL is empty.
- Air Time Fairness Policies:** 2.4 GHz Policy and 5 GHz Policy are both empty.

At the bottom of the configuration area, there are 'Cancel' and 'Update & Apply to Device' buttons.

RF プロファイル

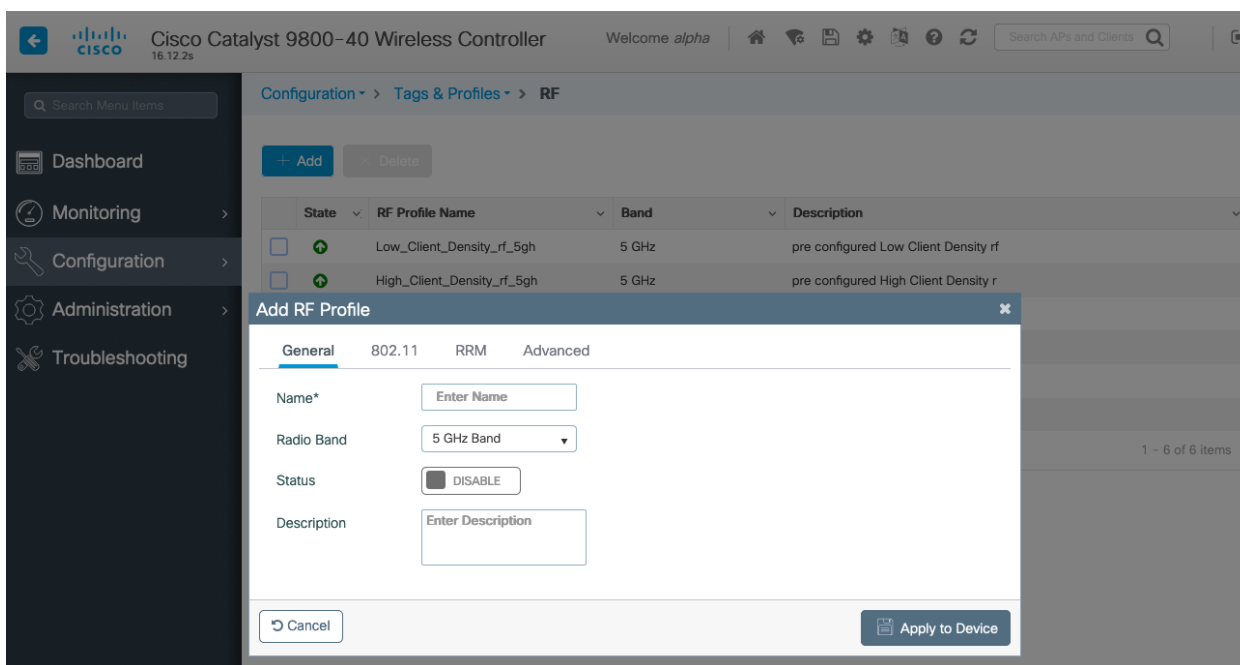
RF プロファイルを作成し、アクセスポイントのグループが使用する必要がある周波数帯域、データレート、RRM 設定、および詳細設定を指定できます。

Cisco Wireless Phone 840 および 860 で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。

RF プロファイルは RF タグに適用され、アクセスポイントに適用できます。

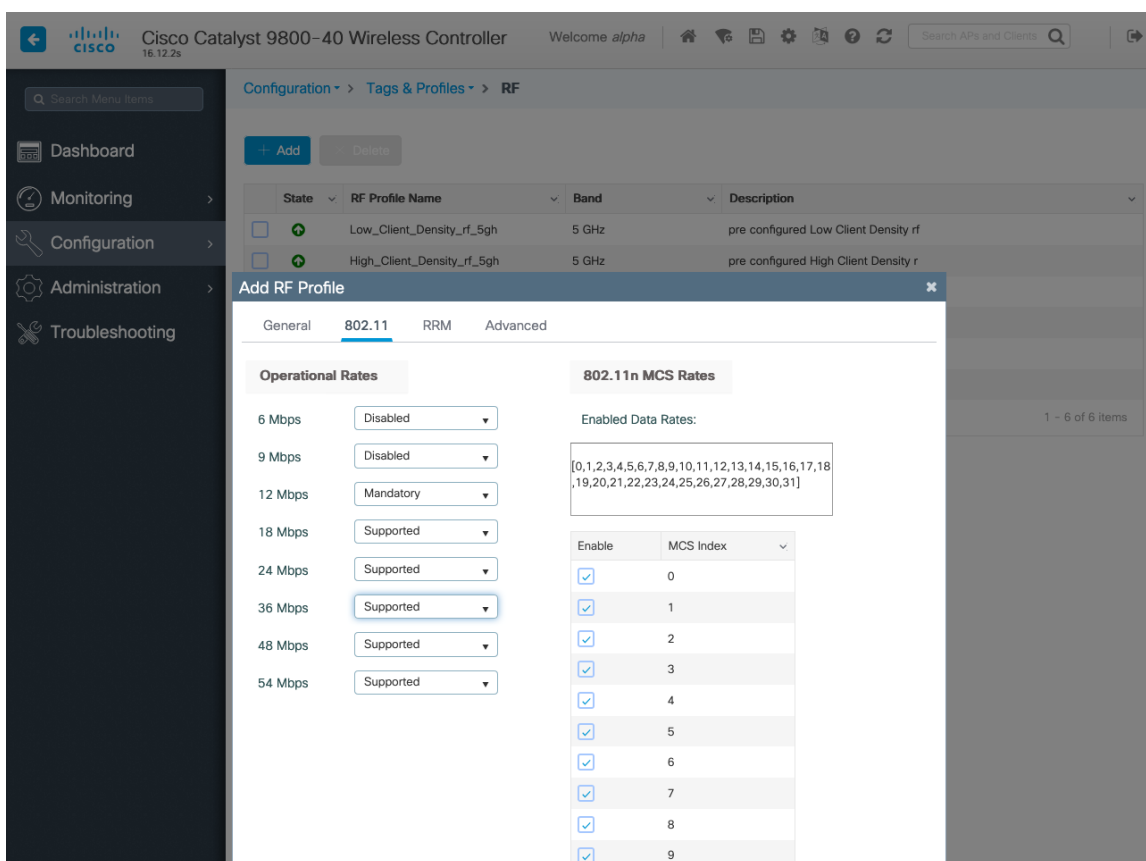
RF プロファイルを作成する場合、[名前 (Name)] と [無線ポリシー (Radio Policy)] を定義する必要があります。

[無線帯域 (Radio Band)] には、[5 GHz 帯域 (5 GHz Band)] または [2.4 GHz 帯域 (2.4 GHz Band)] を選択します。



[802.11] タブで、必要に応じて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生じます。



[RRM] タブでは、[最大電力レベル (Maximum Power Level)] および [最小電力レベル (Minimum Power Level)] 設定と、その他の [DCA]、[TPC]、および [カバレッジ (Coverage)] 設定を設定できます。

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration page. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > RF'. A table lists RF profiles:

State	RF Profile Name	Band	Description
<input type="checkbox"/>	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
<input type="checkbox"/>	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r

An 'Add RF Profile' dialog box is open, showing the 'RRM' tab selected. The dialog has tabs for General, Coverage, TPC, and DCA. The 'Coverage Hole Detection' section contains the following fields:

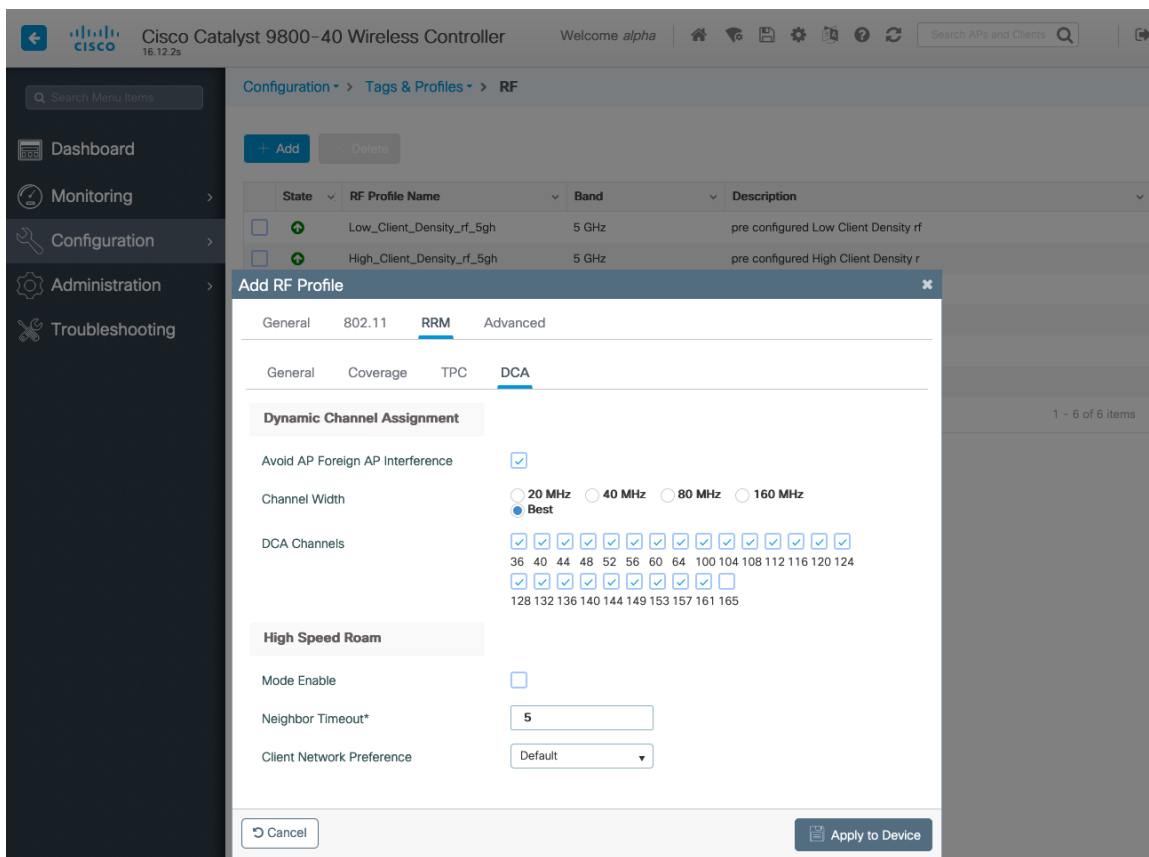
- Minimum Client Level (clients)*: 3
- Data RSSI Threshold (dBm)*: -80
- Voice RSSI Threshold (dBm)*: -80
- Exception Level(%)*: 25

Buttons for 'Cancel' and 'Apply to Device' are visible at the bottom of the dialog.

This screenshot is similar to the one above, showing the 'Add RF Profile' dialog box. In this instance, the 'TPC' tab is selected. The 'Transmit Power Control' section contains the following fields:

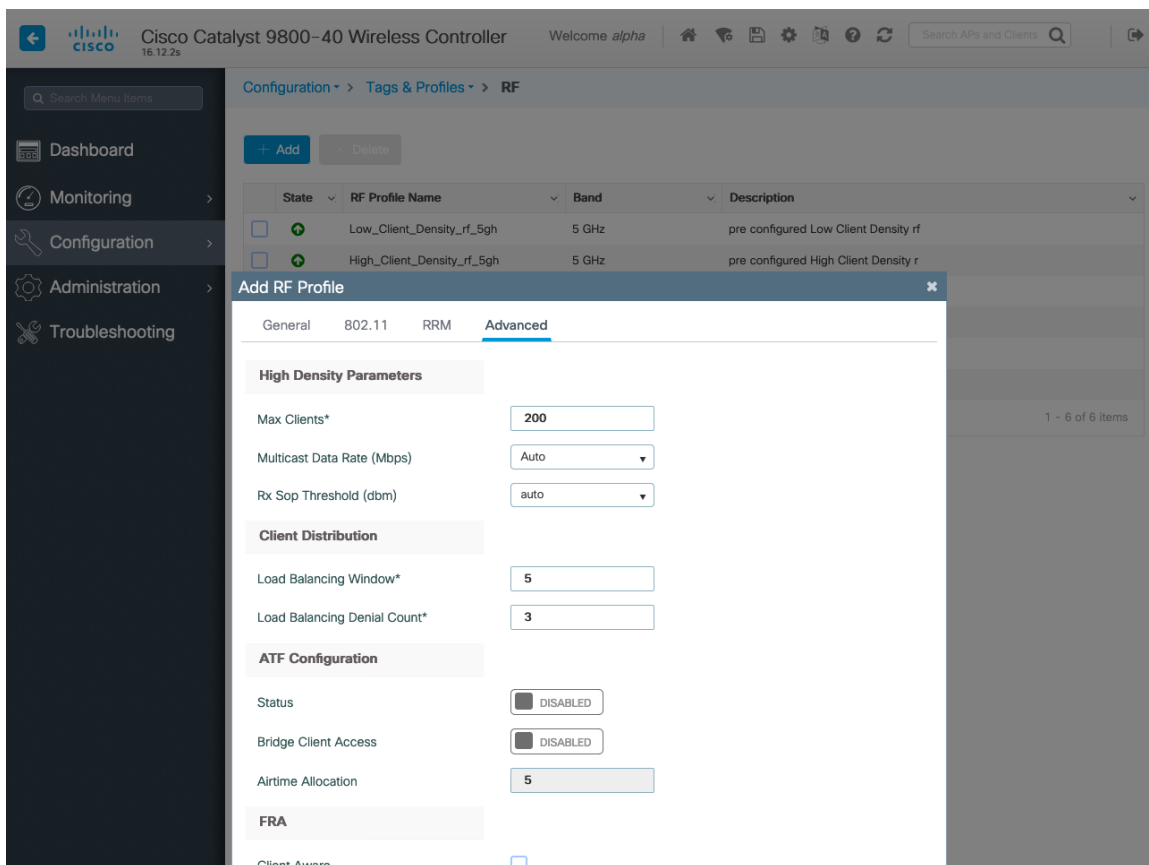
- Maximum Power Level(dBm)*: 30
- Minimum Power Level(dBm)*: -10
- Power Threshold V1(dBm)*: -70

The 'Cancel' and 'Apply to Device' buttons are also present at the bottom of the dialog.



[詳細設定 (Advanced)] タブでは、**[最大クライアント数 (Maximum Clients)]**、**[マルチキャストデータレート (Multicast Data Rates)]**、および**[Rx Sop のしきい値 (Rx Sop Threshold)]**を設定できます。

[Rx Sop のしきい値 (Rx Sop Threshold)]にはデフォルト値 (**[自動 (Auto)]**)を使用することを推奨します。



Flex プロファイル

Flex プロファイルは、アクセスポイントが Flexconnect モードで使用する必要がある設定を定義するために使用されます。

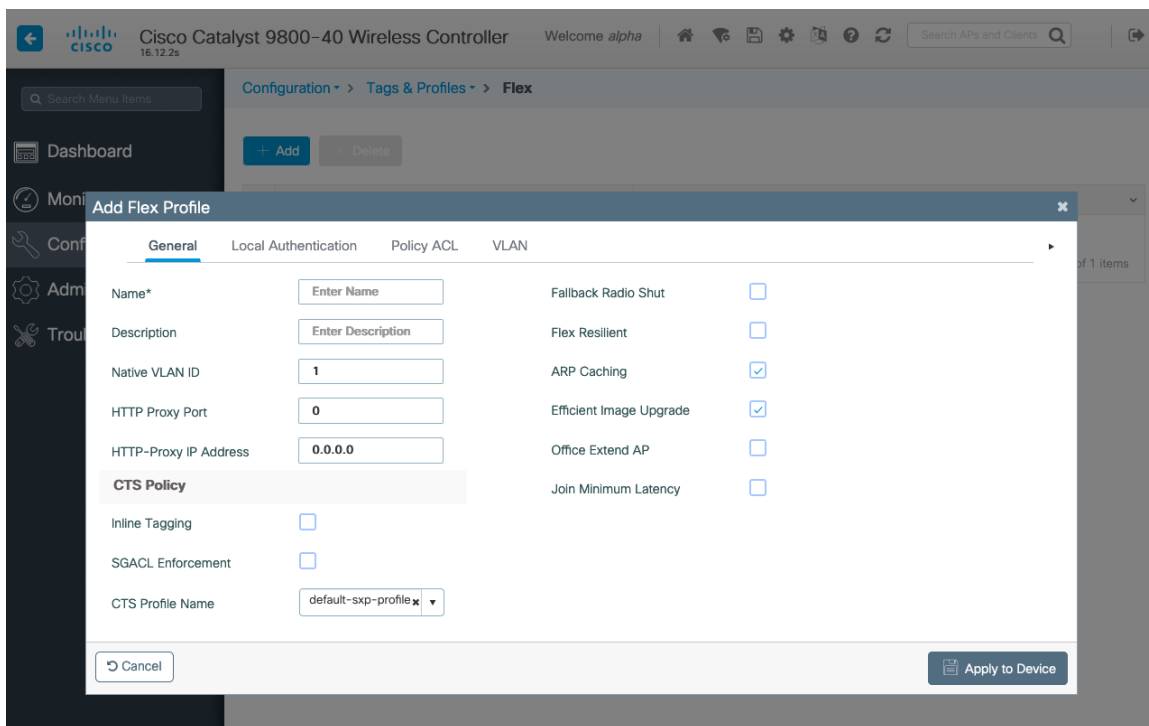
次に、Flex プロファイルはサイトタグに適用され、アクセスポイントに適用できます。

802.11r (FT) または CCKM を使用している場合は、同じ Flex プロファイル内のアクセスポイントにローミングするときのみ、シームレスなローミングを実現できます。

使用するアクセスポイントのネイティブ **VLAN ID** と、許可された VLAN を設定します。

[ARPキャッシング (ARP Caching)] が **[有効 (Enabled)]** になっていることを確認します。

必要に応じて、**[ローカル認証 (Local Authentication)]** を有効にします。



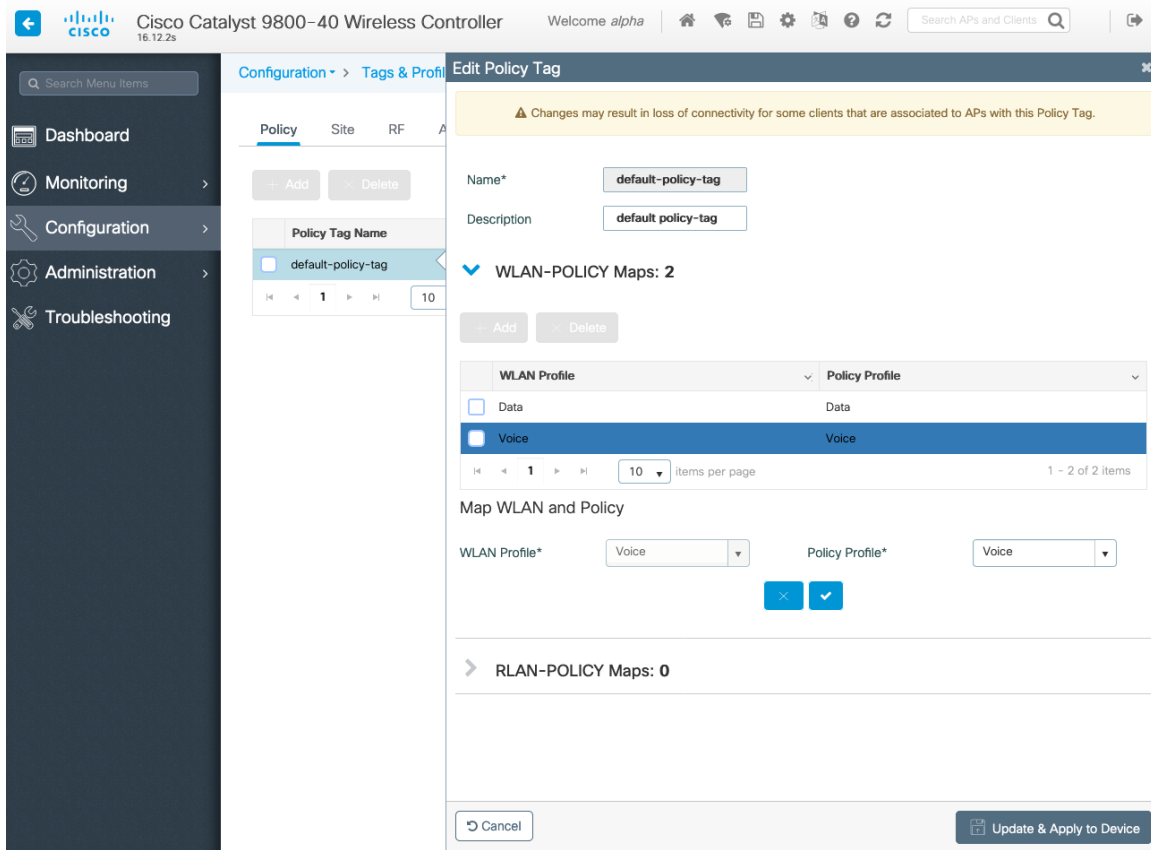
タグ

ポリシータグ

ポリシータグは、WLAN プロファイルとポリシープロファイルのマッピングを構成します。

次に、ポリシータグをアクセスポイントに適用して、有効にする WLAN と SSID、マッピングする必要のあるインターフェイス、使用する QoS およびその他の設定を指定します。

ポリシータグを作成するときは、**[追加 (Add)]** をクリックし、設定する WLAN プロファイルを選択してから、使用するポリシープロファイルを選択します。



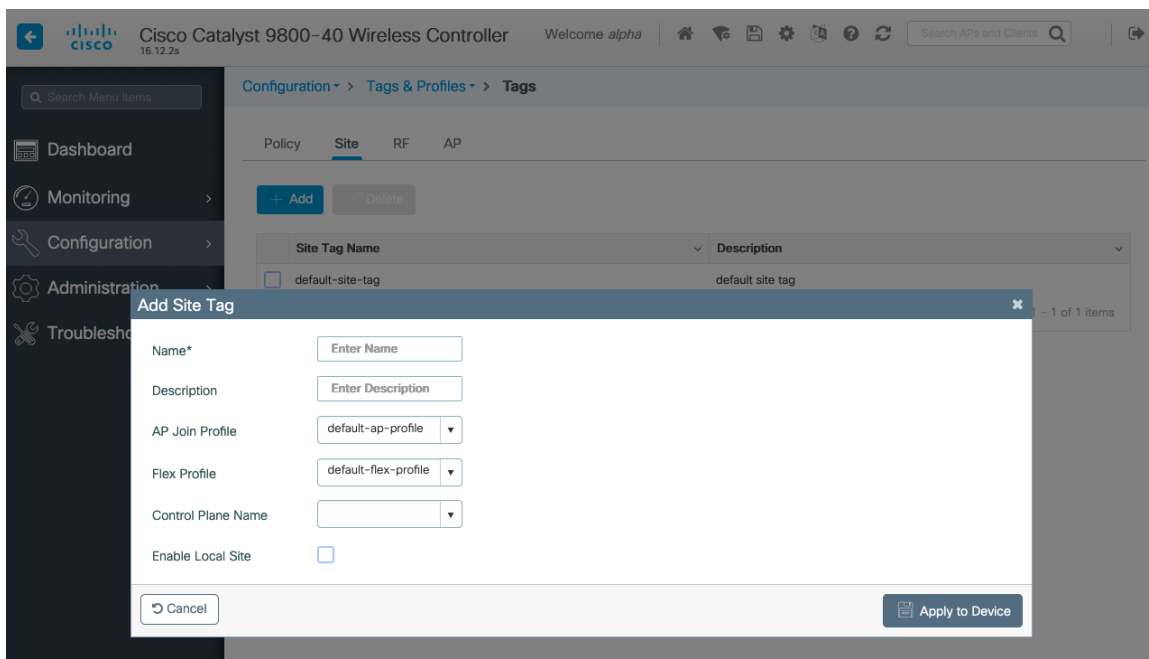
サイト タグ

サイトタグは、使用する AP 参加プロファイルとフレックスプロファイルを定義します。

次に、サイトタグがアクセスポイントに適用され、使用する AP 参加プロファイルおよびフレックス プロファイル パラメータを指定します。

サイトタグを作成するときは、**[追加 (Add)]** をクリックし、使用する **[AP 参加プロファイル (AP Join Profile)]** を選択します。

Flex プロファイルを含むサイトタグを作成する場合は、**[ローカルサイトの有効化 (Enable Local Site)]** がチェックされていないことを確認してから、必要な **[Flex プロファイル (Flex Profile)]** を選択します。

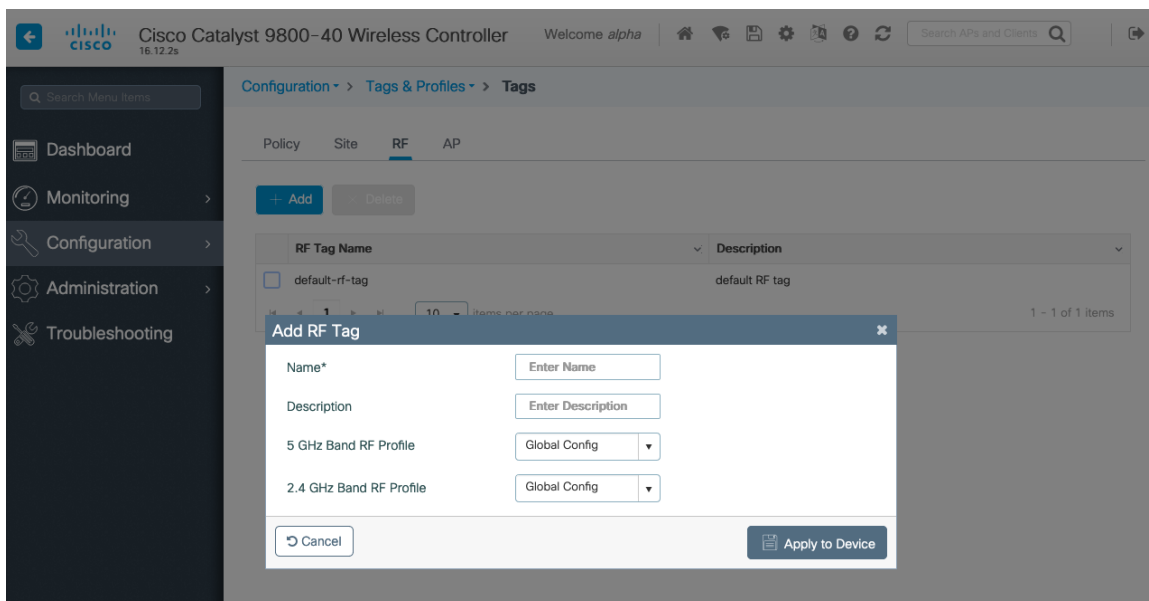


RF タグ

RF タグは、2.4 GHz および 5 GHz に使用する RF プロファイルを定義します。

次に、RF タグがアクセスポイントに適用され、使用する RF プロファイルパラメータを指定します。

RF タグを作成する場合は、使用する **[5 GHz 帯域 RF プロファイル (5 GHz Band RF Profile)]** と **[2.4 GHz 帯域 RF プロファイル (2.4 GHz Band RF Profile)]** を選択します。



タグを定義したら、アクセスポイントに適用できます。

The screenshot displays the 'Edit AP' configuration page in the Cisco Catalyst 9800-40 Wireless Controller interface. The 'General' tab is selected, showing various configuration parameters for the AP 'rcdn6-22a-ap1'. The 'AP Mode' is currently set to 'Local'. The 'Version' section shows the Primary Software Version as 16.12.2.132. The 'IP Config' section shows the DHCP IPv4 Address as 10.201.81.125. The 'Time Statistics' section shows the Up Time as 10 days 18 hrs 16 mins 54 secs.

設定されたフレックスプロファイルを含むサイトタグが適用されている場合、[AP モード (AP Mode)] は自動的に [フレックス (Flex)] に変更されます。

コントローラの設定

[デフォルトのモビリティドメイン (Default Mobility Domain)] が正しく設定されていることを確認します。

[AP LAG モード (AP LAG Mode)] を有効にします。

モビリティ設定

複数の Cisco ワイヤレス LAN コントローラを同じモビリティグループに設定する場合、各 Cisco ワイヤレス LAN コントローラの IP アドレスと MAC アドレスをモビリティピアの設定に追加する必要があります。

各 Cisco Wireless LAN Controller が同じ **[モビリティグループ名 (Mobility Group Name)]** で設定されていることを確認します。

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration page. The breadcrumb navigation is Configuration > Wireless > Mobility. The 'Global Configuration' tab is active. The configuration fields are as follows:

Mobility Group Name*	CTG-VoWLAN3	Apply
Multicast IPv4 Address	0.0.0.0	
Multicast IPv6 Address	::	
Keep Alive Interval (sec)*	10	
Mobility Keep Alive Count*	3	
Mobility DSCP Value*	48	
Mobility MAC Address*	706d.153d.b50b	

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration page. The breadcrumb navigation is Configuration > Wireless > Mobility. The 'Peer Configuration' tab is active. The 'Mobility Peer Configuration' section is expanded, showing a table of configured peers:

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Status	PMTU
706d.153d.b50b	10.201.81.9	N/A	CTG-VoWLAN3	0.0.0.0	N/A	N/A
6c31.0e7b.b8eb	10.201.81.10	10.201.81.10	CTG-VoWLAN3	0.0.0.0	Up	1385

Below the table, there are navigation controls: 10 items per page, and 1 - 2 of 2 items.

[モビリティ MAC アドレス (Mobility MAC Address)] がワイヤレス管理インターフェイスの MAC アドレスと一致していることを確認します。

Configuration > Interface > Wireless

Interface Name	Interface Type	Trustpoint Name	VLAN ID	IP Address	IP Netmask	MAC Address
<input type="checkbox"/> Vlan310	Management		310	10.201.81.9	255.255.255.240	70:6d:15:3d:b5:0b

10 items per page 1 - 1 of 1 items

コール アドミッション制御 (CAC)

[音声 (Voice)] で **[アドミッションコントロール必須 (Admission Control Mandatory)]** を有効にして、使用する帯域 (5 GHz または 2.4 GHz) に対して最大帯域幅および予約済みのローミング帯域幅の各割合を設定することを推奨します。

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以外にも使用できますが、その他の帯域幅がすべて使用されている場合に備え、ローミングクライアント向けに一定のローミング帯域幅が予約されます。

CAC を有効にする場合は、**[ロードベース CAC (Load Based CAC)]** が有効になっていることを確認します。

[ロードベース CAC (Load Based CAC)] は、チャンネル上のすべての出力を考慮します。

音声ストリームのサイズと音声ストリームの最大数の値は、必要に応じて調整できます。

S RTP を使用している場合は、音声ストリームのサイズを増やす必要がある場合があります。

[非アクティブタイムアウト (Inactivity Timeout)] が無効になっていることを確認します。

[ユニキャスト ビデオ リダイレクト (Unicast Video Redirect)] と **[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。

Cisco Catalyst 9800-40 Wireless Controller | Welcome alpha | Search APs and Clients

Configuration > Radio Configurations > Media Parameters

5 GHz Band | 2.4 GHz Band

Apply

Media

General

Unicast Video Redirect

Multicast Direct Admission Control

Media Stream Admission Control (ACM)

Maximum Media Stream RF bandwidth (%)*

Maximum Media Bandwidth (%)*

Client Minimum Phy Rate (kbps)

Maximum Retry Percent (%)*

Media Stream - Multicast Direct Parameters

Multicast Direct Enable

Max streams per Radio

Max streams per Client

Best Effort QOS Admission

Voice

Call Admission Control (CAC)

Admission Control (ACM)

Load Based CAC

Max RF Bandwidth (%)*

Reserved Roaming Bandwidth (%)*

Expedited Bandwidth

SIP CAC and Bandwidth

SIP CAC Support

Traffic Stream Metrics

Metrics Collection

Stream Size*

Max Streams*

Inactivity Timeout

マルチキャスト

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 (Global Multicast Mode)] および [IGMP スヌーピング (IGMP Snooping)] を有効にする必要があります。

Configuration > Services > Multicast

Global Wireless Multicast Mode: **ENABLED**

Wireless mDNS Bridging: **DISABLED**

Wireless Non-IP Multicast: **DISABLED**

Wireless Broadcast: **DISABLED**

AP Capwap Multicast: Unicast

MLD Snooping: **DISABLED**

IGMP Snooping Querier: **DISABLED**

IGMP Snooping: **ENABLED**

Last Member Querier Interval (milliseconds): 1000

IGMP Snooping

Disabled: No Vlan available

Enabled:

Status	VLAN ID	Name
+	1	default
+	310	VLAN0310
+	400	VLAN0400
+	500	VLAN0500

Wireless Broadcast and Wireless Non-IP Multicast

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の有効化 (Multicast Direct Enable)] を有効にする必要があります。

次に、ストリームを設定します。

Configuration > Wireless > Media Stream

General Streams

Multicast Direct Enable:

Session Message Config

Session Announcement State:

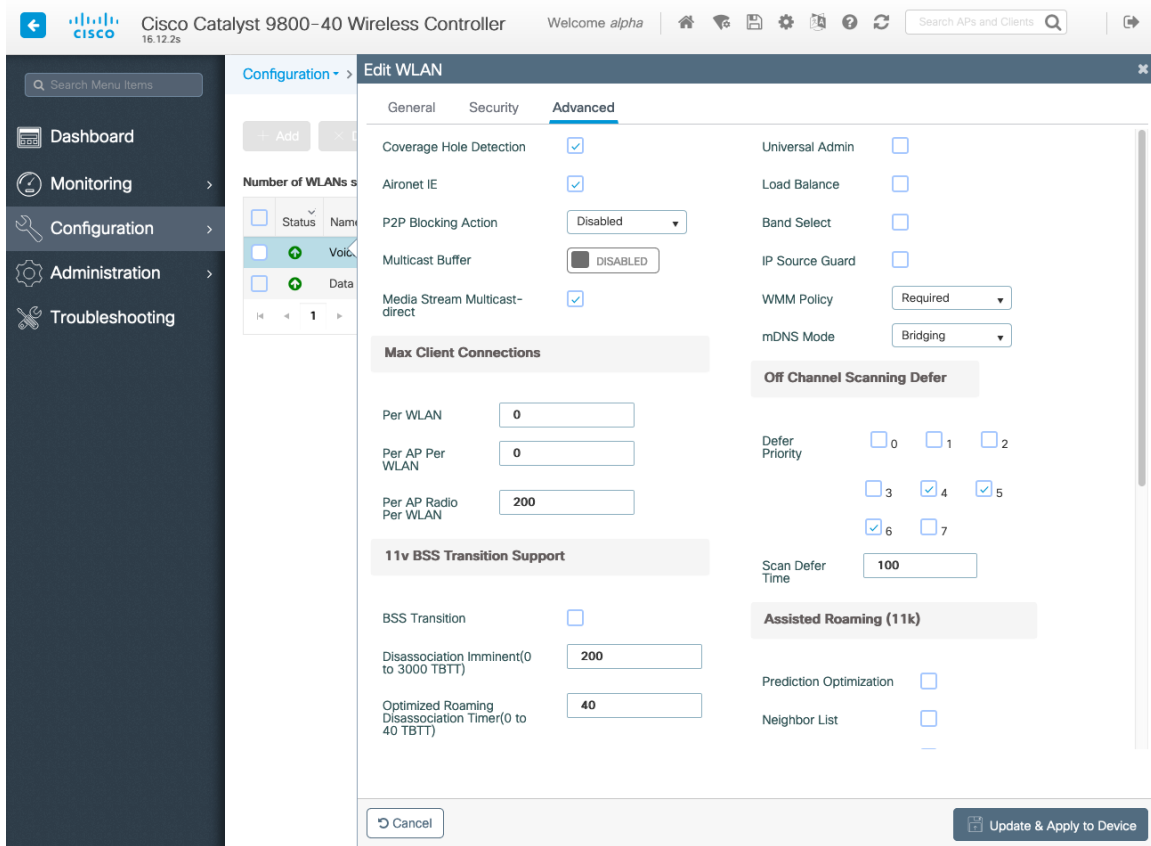
Session Announcement URL:

Session Announcement Email:

Session Announcement Phone:

Session Announcement Note:

また、WLAN 設定で [マルチキャストダイレクト (Multicast Direct)] を有効にします。



The screenshot shows the 'Edit WLAN' configuration page in the Cisco Catalyst 9800-40 Wireless Controller. The 'Advanced' tab is selected, displaying various configuration options:

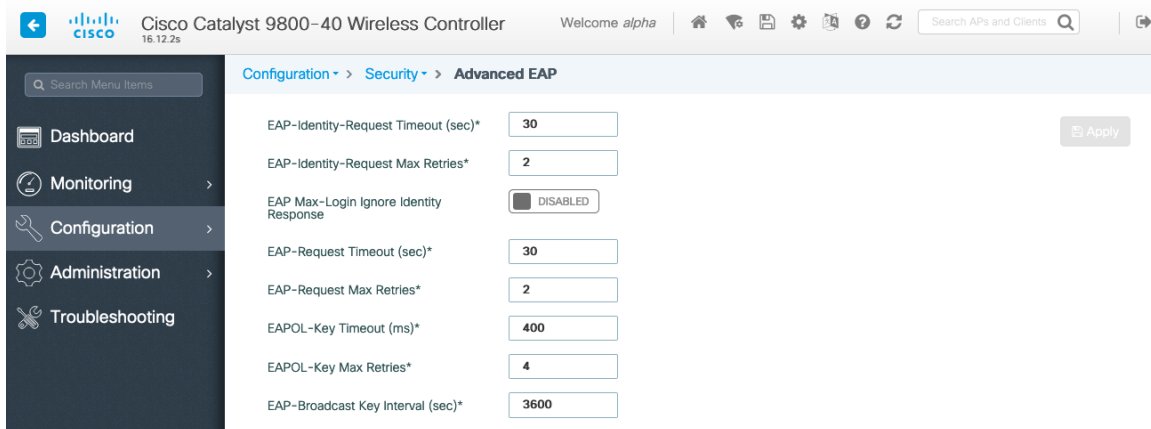
- Coverage Hole Detection:**
- Aironet IE:**
- P2P Blocking Action:** Disabled
- Multicast Buffer:** DISABLED
- Media Stream Multicast-direct:**
- Max Client Connections:**
 - Per WLAN: 0
 - Per AP Per WLAN: 0
 - Per AP Radio Per WLAN: 200
- 11v BSS Transition Support:**
 - BSS Transition:
 - Disassociation Imminent(0 to 3000 TBTT): 200
 - Optimized Roaming Disassociation Timer(0 to 40 TBTT): 40
- Off Channel Scanning Defer:**
 - Defer Priority: 0, 1, 2, 3, 4, 5, 6, 7
 - Scan Defer Time: 100
- Assisted Roaming (11k):**
 - Prediction Optimization:
 - Neighbor List:

Buttons at the bottom include 'Cancel' and 'Update & Apply to Device'.

詳細設定

EAP の詳細設定

EAP パラメータを表示または設定するには、[設定 (Configuration)] > [セキュリティ (Security)] > [高度な EAP (Advanced EAP)] を選択します。



The screenshot shows the 'Advanced EAP' configuration page under the 'Security' section. The following parameters are visible:

- EAP-Identity-Request Timeout (sec)*: 30
- EAP-Identity-Request Max Retries*: 2
- EAP Max-Login Ignore Identity Response: DISABLED
- EAP-Request Timeout (sec)*: 30
- EAP-Request Max Retries*: 2
- EAPOL-Key Timeout (ms)*: 400
- EAPOL-Key Max Retries*: 4
- EAP-Broadcast Key Interval (sec)*: 3600

An 'Apply' button is located at the top right of the configuration area.

802.1x を使用する場合、Cisco ワイヤレス LAN コントローラの [EAP 要求タイムアウト (EAP-Request Timeout)] を少なくとも 30 秒に設定する必要があります。

EAP の失敗が頻繁に発生する展開では、[EAP 要求タイムアウト (EAP-Request Timeout)] を 30 秒未満に減らす必要があります。

PSK を使用する場合は、[EAPOL キーのタイムアウト (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 キーの最大試行回数 (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。

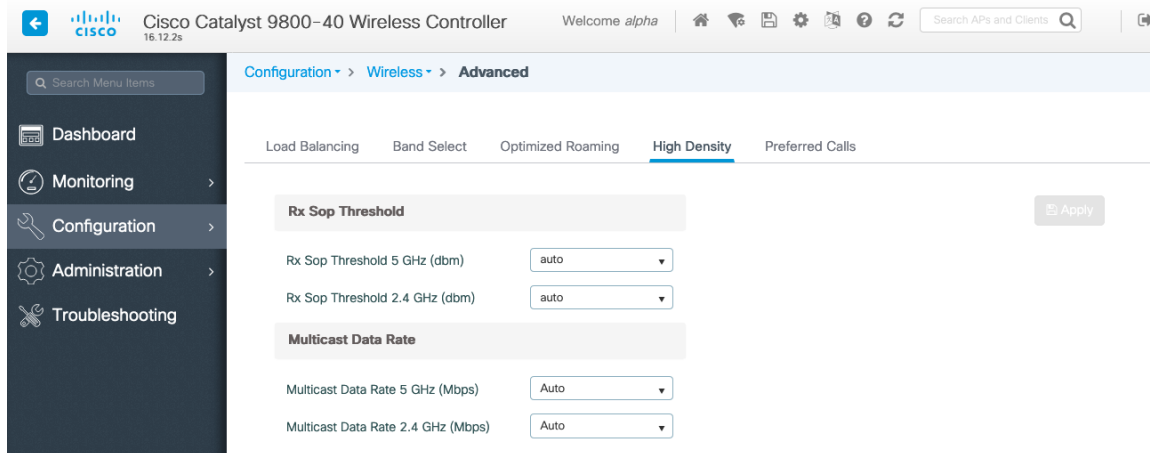
802.1x を使用する場合は、[EAPOL キーのタイムアウト (EAPOL-Key Timeout)] および [EAPOL キーの最大試行回数 (EAPOL-Key Max Retries)] のデフォルト値 (それぞれ 1000 ミリ秒および 2) を使用しても正しく動作しますが、それぞれ 400 および 4 に設定することを推奨します。

[EAPOL キーのタイムアウト (EAPOL-Key Timeout)] は、1000 ミリ秒 (1 秒) を超えないようにしてください。

[EAP-Broadcast Key Interval] が 3600 秒 (1 時間) 以上に設定されていることを確認します。

Rx SOP しきい値

[Rx Sop のしきい値 (Rx Sop Threshold)] にはデフォルト値 ([自動 (Auto)]) を使用することを推奨します。



The screenshot shows the configuration page for a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "Configuration > Wireless > Advanced". Under the "High Density" tab, there are two sections: "Rx Sop Threshold" and "Multicast Data Rate".

Section	Parameter	Value
Rx Sop Threshold	Rx Sop Threshold 5 GHz (dbm)	auto
	Rx Sop Threshold 2.4 GHz (dbm)	auto
Multicast Data Rate	Multicast Data Rate 5 GHz (Mbps)	Auto
	Multicast Data Rate 2.4 GHz (Mbps)	Auto

不正ポリシー

[不正ロケーション検出プロトコル (Rogue Location Discovery Protocol)] にはデフォルト値 ([無効 (Disable)]) の使用を推奨します。

Cisco Catalyst 9800-40 Wireless Controller 16.12.2s Welcome alpha

Configuration > Security > Wireless Protection Policies

Rogue Policies **RLDP** Rogue AP Rules Client Exclusion Policies

Rogue Location Discovery Protocol

Retry Count

Schedule RLDP

Day	Start Time	End Time
<input type="checkbox"/> Monday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Tuesday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Wednesday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Thursday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Friday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Saturday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Sunday	<input type="text"/>	<input type="text"/>

設定例

バージョン 16.12

```

service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname RCDN6-21A-WLC5
!
boot-start-marker
boot system flash bootflash:packages.conf
boot-end-marker
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
no logging console
!
aaa new-model
!
!

```

```

aaa group server radius RADIUS_SERVER_GROUP_DAY0
server name RADIUS_SERVER_DAY0_1
server name RADIUS_SERVER_DAY0_2
!
aaa authentication login default local
aaa authentication login authentication_login_day0 group RADIUS_SERVER_GROUP_DAY0
aaa authentication dot1x authentication_dot1x_day0 group RADIUS_SERVER_GROUP_DAY0
aaa authorization exec default local
aaa authorization network default local
!
aaa server radius dynamic-author
!
aaa session-id common
clock timezone CST -6 0
clock summer-time CDT recurring
call-home
! call-home の連絡先電子メールアドレスが sch-smart-licensing@cisco.com として設定されて
いる場合
! Cisco Smart License Portal で設定された電子メールアドレスは、SCH 通知を送信するための連
絡先電子メールアドレスとして使用されます。
Contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
no destination transport-method email
!
ip domain name cisco.com
!
login on-success log
!
subscriber templating
!
parameter-map type webauth global
virtual-ip ipv4 1.1.1.6
!
flow exporter wireless-local-exporter
destination local wlc
!
flow monitor wireless-avc-basic
exporter wireless-local-exporter
cache timeout active 60
record wireless avc basic
!
no device-tracking logging theft
access-session mac-move deny
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-3110682001
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3110682001
revocation-check none

```

rsa-keypair TP-self-signed-3110682001

!

crypto pki trustpoint SLA-TrustPoint

enrollment pkcs12

revocation-check crl

!

crypto pki certificate chain TP-self-signed-3110682001

certificate self-signed 01

```
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 33313130 36383230 3031301E 170D3139 30373130 30343236
35375A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31313036
38323030 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100B74F D6A0DE5D DFB2CDD2 5196AAB1 86C8BD48 3AAAF455 C4E7D559
41A10FE1 87EC742C C5014113 9A0FD83A F490EA64 DF68A513 AA6900C4 810A9FED
870309EA 781EB999 882F7374 EC79D592 DEC6C126 A5FB5666 905C24D8 B2064CD4
66823D6E 7E9A07F3 B043D632 EEDF4CAF D306C303 843493AA F44126E3 A07DE905
6B6C5B8E C8E6C9E6 45D79F62 B813FF8C B44FA7AC AEDB8A9E 55B75096 E4E76BC3
D5B90900 1A0C7CD0 910B6C63 920E9666 39EC3702 387757F1 C26F0BB5 89D4733D
FED71CF4 33002C77 0F721B21 5578C850 590BC846 7CB79469 A51CEBA5 96EA8672
DDB82A44 69EEDA13 DD83B0FA 3221A839 5F985C86 F2C57B78 8E6608B6 18A346D2
035D3B68 26BF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 141B4651 019E0AEC 8E64EB65 C0E023ED 60F6062C
0F301D06 03551D0E 04160414 1B465101 9E0AEC8E 64EB65C0 E023ED60 F6062C0F
300D0609 2A864886 F70D0101 05050003 82010100 3319F2A7 3E88539F 85C08F28
67553F93 408DCCC6 EFE2704E C142766C 5FFE0E97 0AFDE0EA 816CB4E2 60FFBC26
6E411C57 3F1AB3F8 2F1E9959 AED26C86 2C0B059D B692C72C B5859A15 999916F8
699587DC 94409E7C FF685698 2FB9ACEC 9315F1AA 357E3877 7AE1E37C F5CD7E46
EB3ADC44 3F22A9E0 EA35E6B8 E5508721 0E8754A1 6A6E3A6A C7FD8E64 6C3C722C
F90919C9 DE675E5C 301FF83A 0593ACE6 4A469209 CAAEC53F 5102FDD3 AE378090
46282E00 BCF65EB7 4C257EFD 57986F82 B6DD8336 CEA82E27 63B4C6C5 F92945E8
2AFE9A95 2AD21793 50FF7987 F4A79079 6FE92AE5 66DFC8B8 14021984 0B1E3F6E
45D57889 B04883C5 114D79AD FBB2CAFF 587ECF9D
```

quit

crypto pki certificate chain SLA-TrustPoint

certificate ca 01

```
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
```

```
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEB7C7F9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
```

quit

!

```
license udi pid C9800-40-K9 sn TTM231803A3
memory free low-watermark processor 375973
```

!

```
service-template webauth-global-inactive
  inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
  linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
  linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
diagnostic bootup level minimal
```

!

```
username <REMOVED> privilege 15 password 7 <REMOVED>
```

!

```
redundancy
  mode sso
```

!

```
vlan internal allocation policy ascending
```

!

```
class-map match-any AVC-Reanchor-Class
  match protocol cisco-jabber-audio
  match protocol cisco-jabber-video
  match protocol webex-media
  match protocol webex-app-sharing
  match protocol webex-control
  match protocol webex-meeting
  match protocol wifi-calling
```

!

```
interface Port-channel3
  switchport trunk native vlan 310
  switchport trunk allowed vlan 310,400,500
  switchport mode trunk
```

!

```
interface TenGigabitEthernet0/0/0
  switchport trunk native vlan 310
  switchport trunk allowed vlan 310,400,500
  switchport mode trunk
```

```

no negotiation auto
channel-group 3 mode active
!
interface TenGigabitEthernet0/0/1
switchport trunk native vlan 310
switchport trunk allowed vlan 310,400,500
switchport mode trunk
no negotiation auto
channel-group 3 mode active
!
interface TenGigabitEthernet0/0/2
switchport trunk native vlan 310
switchport trunk allowed vlan 310,400,500
switchport mode trunk
no negotiation auto
channel-group 3 mode active
!
interface TenGigabitEthernet0/0/3
switchport trunk native vlan 310
switchport trunk allowed vlan 310,400,500
switchport mode trunk
no negotiation auto
channel-group 3 mode active
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 10.201.81.25 255.255.255.240
negotiation auto
no cdp enable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan310
description Management
ip address 10.201.81.9 255.255.255.240
!
interface Vlan400
description Data
ip address 10.201.82.14 255.255.255.0
ip helper-address 72.163.42.112
ip helper-address 173.37.137.70
!
interface Vlan500
description Voice
ip address 10.201.83.14 255.255.255.0
ip helper-address 72.163.42.112
ip helper-address 173.37.137.70
!
ip default-gateway 10.201.81.1
ip forward-protocol nd

```

```

!
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ip tftp blocksize 8192
ip route 0.0.0.0 0.0.0.0 10.201.81.1
!
radius-server attribute wireless accounting mac-delimiter hyphen
radius-server attribute wireless accounting call-station-id macaddress
radius-server attribute wireless accounting callStationIdCase lower
radius-server attribute wireless authentication callStationIdCase lower
radius-server attribute wireless authentication mac-delimiter hyphen
radius-server attribute wireless authentication call-station-id ap-macaddress-ssid
radius-server load-balance method least-outstanding
!
radius server RADIUS_SERVER_DAY0_1
address ipv4 10.42.136.30 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
radius server RADIUS_SERVER_DAY0_2
address ipv4 10.42.3.31 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
control-plane
!
line con 0
exec-timeout 60 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
!
ntp server 10.81.254.202
ntp server 10.115.162.212
!
wireless mobility group member mac-address 6c31.0e7b.b8eb ip 10.201.81.10 public-ip
10.201.81.10 group CTG-VoWLAN3
wireless mobility group name CTG-VoWLAN3
wireless mobility mac-address 706d.153d.b50b
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile
wireless management interface Vlan310
wireless profile airtime-fairness default-atf-policy 0
wireless profile flex default-flex-profile
description "default flex profile"
wireless profile mesh default-mesh-profile
description "default mesh profile"
wireless profile policy Data

```

```
ipv4 flow monitor wireless-avc-basic input
ipv4 flow monitor wireless-avc-basic output
service-policy input silver-up
service-policy output silver
session-timeout 86400
vlan VLAN0400
no shutdown
wireless profile policy Voice
ipv4 flow monitor wireless-avc-basic input
ipv4 flow monitor wireless-avc-basic output
service-policy input platinum-up
service-policy output platinum
session-timeout 86400
vlan VLAN0500
no shutdown
wireless profile policy default-policy-profile
description "default policy profile"
vlan default
wireless tag site default-site-tag
description "default site tag"
wireless tag policy default-policy-tag
description "default policy-tag"
wlan Data policy Data
wlan Voice policy Voice
wireless tag rf default-rf-tag
description "default RF tag"
wireless rf-network RCDN6-VoWLAN3
wireless security dot1x eapol-key retries 4
wireless security dot1x eapol-key timeout 400
no wireless security dot1x max-login-ignore-identity-response
wireless fabric control-plane default-control-plane
wireless media-stream multicast-direct
wireless multicast
wlan Data 2 data
band-select
ccx aironet-iesupport
load-balance
security dot1x authentication-list authentication_dot1x_day0
no shutdown
wlan Voice 1 voice
no assisted-roaming neighbor-list
no bss-transition
ccx aironet-iesupport
channel-scan defer-priority 4
dtim dot11 24ghz 2
dtim dot11 5ghz 2
media-stream multicast-direct
radio dot11a
security ft
security wpa akm ft dot1x
security dot1x authentication-list authentication_dot1x_day0
wmm require
```


no shutdown
ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh
coverage data rssi threshold -90
coverage level 2
coverage voice rssi threshold -90
description "pre configured Low Client Density rfprofile for 2.4gh radio"
high-density rx-sop threshold low
tx-power v1 threshold -65
no shutdown
ap dot11 24ghz rf-profile High_Client_Density_rf_24gh
description "pre configured High Client Density rfprofile for 2.4gh radio"
high-density rx-sop threshold medium
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
tx-power min 7
no shutdown
ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh
description "pre configured Typical Client Density rfprofile for 2.4gh radio"
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
no shutdown
ap dot11 24ghz media-stream multicast-direct
ap dot11 24ghz media-stream video-redirect
no ap dot11 24ghz cac voice tspec-inactivity-timeout
ap dot11 24ghz cac voice tspec-inactivity-timeout ignore
ap dot11 24ghz cac voice acm
ap dot11 24ghz edca-parameters optimized-video-voice
ap dot11 24ghz exp-bwreq
ap dot11 24ghz tsm
ap dot11 24ghz rrm txpower max 14
ap dot11 24ghz rrm txpower min 5
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 5ghz rf-profile Low_Client_Density_rf_5gh
coverage data rssi threshold -90
coverage level 2
coverage voice rssi threshold -90
description "pre configured Low Client Density rfprofile for 5gh radio"
high-density rx-sop threshold low

```

tx-power v1 threshold -60
no shutdown
ap dot11 5ghz rf-profile High_Client_Density_rf_5gh
description "pre configured High Client Density rfprofile for 5gh radio"
high-density rx-sop threshold medium
rate RATE_6M disable
rate RATE_9M disable
tx-power min 7
tx-power v1 threshold -65
no shutdown
ap dot11 5ghz rf-profile Typical_Client_Density_rf_5gh
description "pre configured Typical Density rfprofile for 5gh radio"
no shutdown
ap dot11 5ghz media-stream multicast-direct
ap dot11 5ghz media-stream video-redirect
no ap dot11 5ghz cac voice tspec-inactivity-timeout
ap dot11 5ghz cac voice tspec-inactivity-timeout ignore
ap dot11 5ghz cac voice acm
ap dot11 5ghz exp-bwreq
ap dot11 5ghz tsm
ap dot11 5ghz edca-parameters optimized-video-voice
ap dot11 5ghz channelswitch quiet
ap dot11 5ghz rrm channel dca chan-width 40
ap dot11 5ghz rrm channel dca remove 116
ap dot11 5ghz rrm channel dca remove 120
ap dot11 5ghz rrm channel dca remove 124
ap dot11 5ghz rrm channel dca remove 128
ap dot11 5ghz rrm channel dca remove 144
ap dot11 5ghz rrm txpower max 17
ap dot11 5ghz rrm txpower min 11
ap dot11 5ghz rate RATE_24M supported
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap country US
ap lag support
ap tag-source-priority 2 source filter
ap tag-source-priority 3 source ap
ap profile default-ap-profile
capwap backup primary RCDN6-21A-WLC5 10.201.81.9
capwap backup secondary RCDN6-22A-WLC6 10.201.81.10
description "default ap profile"
hyperlocation ble-beacon 0
hyperlocation ble-beacon 1
hyperlocation ble-beacon 2
hyperlocation ble-beacon 3
hyperlocation ble-beacon 4
HyperLocation
lag
mgmtuser username <REMOVED> password 0 <REMOVED> secret 0 <REMOVED>
ntp ip 10.115.162.212
ssh
end

```

Cisco Mobility Express および Lightweight アクセスポイント

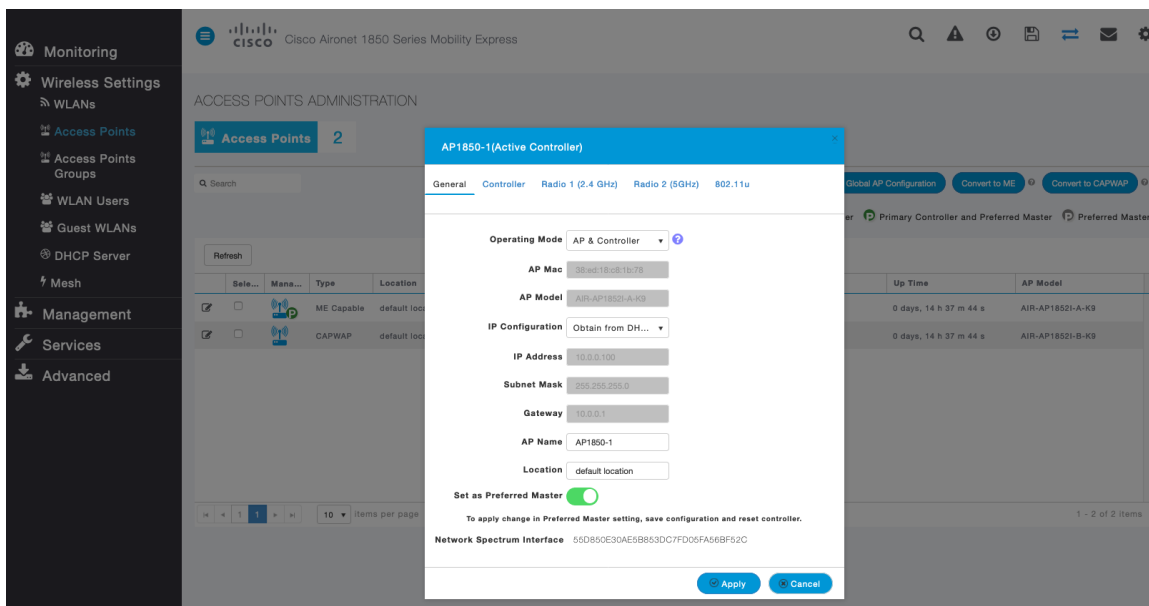
Cisco Mobility Express および Lightweight アクセスポイントを設定するときは、次のガイドラインを使用してください。

- [802.11r (FT)] または [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
- 802.11k を [有効 (Enabled)] に設定することを推奨
- 802.11v を有効に設定することを推奨
- [P2P (ピアツーピア) ブロッキングアクション (P2P (Peer to Peer) Blocking Action)] を無効にします
- [クライアントの帯域選択 (Client Band Select)] を [無効 (Disabled)] に設定します
- [クライアントの負荷分散 (Client Load Balancing)] を [無効 (Disabled)] に設定します
- 必要に応じて [データレート (Data Rates)] を設定します
- 必要に応じて [RF 最適化 (RF Optimization)] を設定します
- [トラフィックタイプ (Traffic Type)] を [音声とデータ (Voice and Data)] に設定します
- CleanAir テクノロジーを搭載した Cisco 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 (Multicast Direct)] を設定します

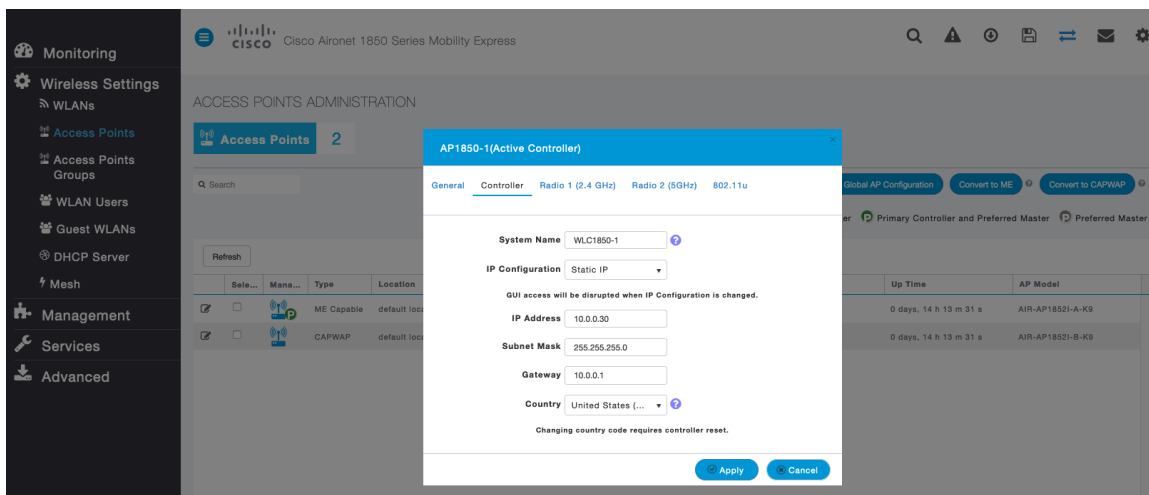
コントローラの設定

[コントローラ (Controller)] 機能を含むように、1 つ以上の Mobility Express 対応アクセスポイントの [動作モード (Operating Mode)] を設定します。

必要に応じて [AP 名 (AP Name)] と [IP 設定 (IP settings)] を設定します。



必要に応じて、Cisco ワイヤレス LAN コントローラの [システム名 (System Name)] と [IP 設定 (IP settings)] を設定します。



802.11 ネットワークの設定

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域で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。

5 GHz を使用する場合は、[5.0 GHz 帯域 (5.0 GHz Band)] が [有効 (Enabled)] になっていることを確認します。

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 以上をそれぞれ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ります。

2.4 GHz を使用する場合は、**[2.4 GHz 帯域 (2.4 GHz Band)]** が **[有効 (Enabled)]** になっていることを確認します。

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、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、サポート対象 (任意) レートとして 12 Mbps 以上をそれぞれ設定する必要があります。

5 GHz を使用する場合は、多数のチャン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ためにチャンネルの数を制限できます (例: 12 チャンネルのみ)。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

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

CleanAir テクノロジーを搭載したCisco 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 検出 (CleanAir detection)]** を **[有効 (Enabled)]** にする必要があります。

The screenshot displays the 'Advanced RF Parameters' configuration page. On the left is a navigation menu with options like Monitoring, Wireless Settings, Management, Services, Advanced, SNMP, Logging, RF Optimization, RF Profiles, Controller Tools, Security Settings, and CMX. The main content area includes the following settings:

- 2.4 GHz Band:
- 5.0 GHz Band:
- Automatic Flexible Radio Assignment:
- 2.4 GHz Optimized Roaming:
- 5 GHz Optimized Roaming:
- Event Driven RRM:
- CleanAir detection:
- 5.0 GHz Channel Width: 40 MHz (dropdown menu)
- 2.4 GHz Data Rates: A slider from 1 to 54 with a red bar indicating supported rates (1, 2, 5.5, 6, 9, 11, 12) and a red bar below indicating '802.11b devices not supported'.
- 5.0 GHz Data Rates: A slider from 6 to 54 with a red bar indicating supported rates (6, 9, 12, 18, 24, 36, 48, 54) and a red bar below indicating 'Some legacy devices not supported'.
- Select DCA Channels: A grid of checkboxes for 2.4 GHz (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) and 5.0 GHz (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165). Channel 6 is selected.

At least one Channel Number should be selected

Apply

RF 最適化

チャンネルと送信電力設定を管理するには、[RF 最適化 (RF Optimization)] を有効にすることをお勧めします。

[トラフィックタイプ (Traffic Type)] を [音声とデータ (Voice and Data)] に設定します。

The screenshot shows the Cisco Aironet 1850 Series Mobility Express web interface. The left sidebar contains navigation options: Monitoring, Wireless Settings, Management, Services, Advanced, SNMP, Logging, RF Optimization (highlighted), RF Profiles, Controller Tools, Security Settings, and CMX. The main content area is titled 'RF OPTIMIZATION' and shows a status bar for 'RF Optimization' set to 'Enabled'. Below this, there are three settings: 'RF Optimization' (dropdown menu set to 'Enabled'), 'Client Density' (slider set to 'Typical'), and 'Traffic Type' (dropdown menu set to 'Voice and Data'). An 'Apply' button is located at the bottom of the settings area.

使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセスポイントの設定をグローバル設定よりも優先させることができます。

その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

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。

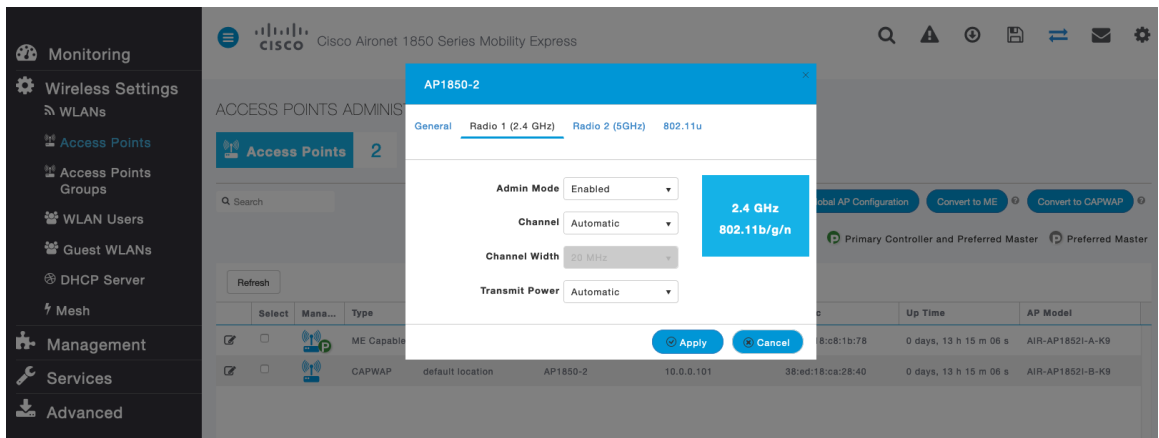
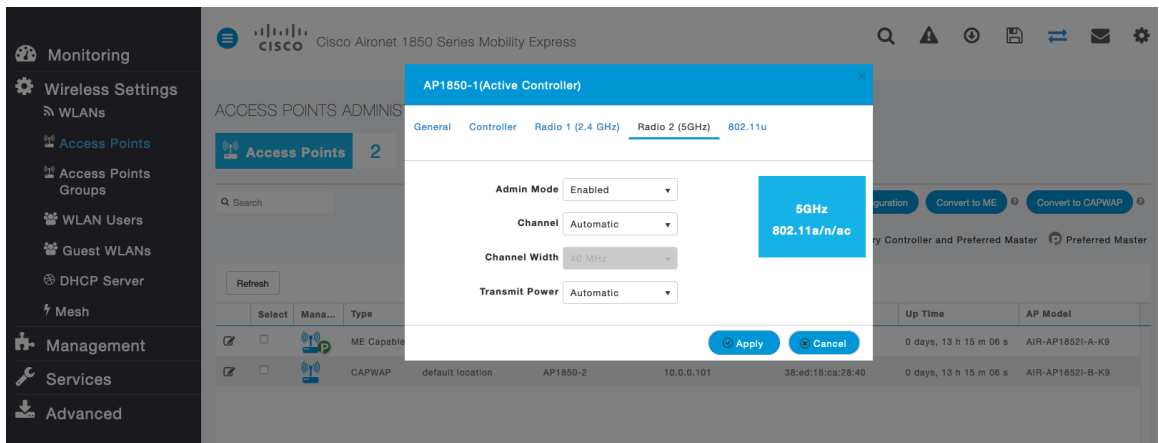
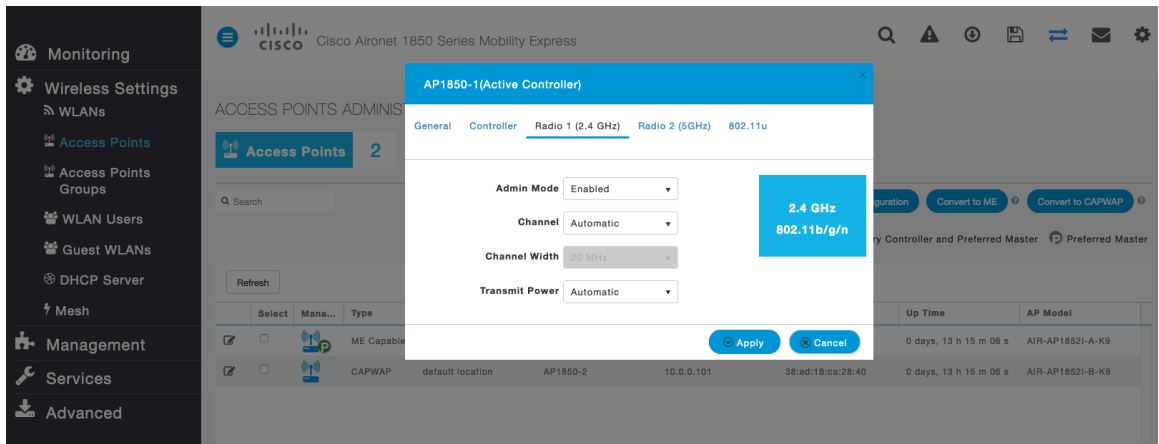
Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

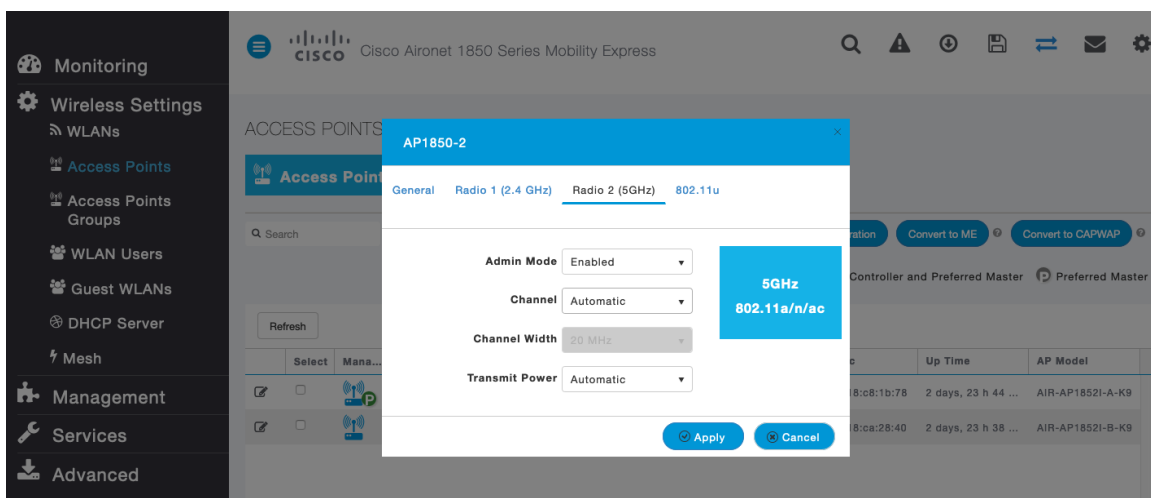
チャンネルボンディングは、5 GHz を使用する場合にのみ使用することをお勧めします。

すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

The screenshot shows the Cisco Aironet 1850 Series Mobility Express web interface for 'ACCESS POINTS ADMINISTRATION'. The left sidebar contains navigation options: Monitoring, Wireless Settings, WLANs, Access Points (highlighted), Access Points Groups, WLAN Users, Guest WLANs, DHCP Server, Mesh, Management, Services, and Advanced. The main content area shows 'Access Points' with a count of 2. There are buttons for 'Global AP Configuration', 'Convert to ME', and 'Convert to CAPWAP'. Below these are radio buttons for 'Primary Controller', 'Primary Controller and Preferred Master', and 'Preferred Master'. A table lists the access points:

	Sele...	Mana...	Type	Location	Name	IP Address	AP Mac	Up Time	AP Model
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ME Capable	default location	AP1850-1	10.0.0.100	38:ed:18:c8:1b:78	0 days, 14 h 37 m 44 s	AIR-AP1852I-A-K9
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CAPWAP	default location	AP1850-2	10.0.0.101	38:ed:18:ca:28:40	0 days, 14 h 37 m 44 s	AIR-AP1852I-B-K9





WLAN の設定

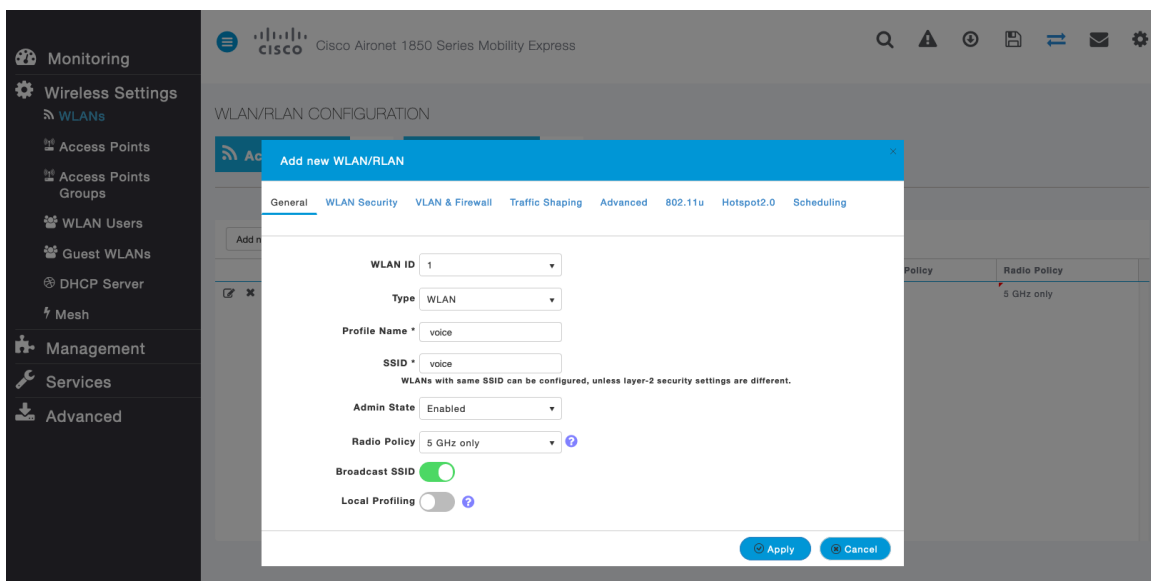
Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

ただし、音声対応 Cisco Wireless LAN 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。

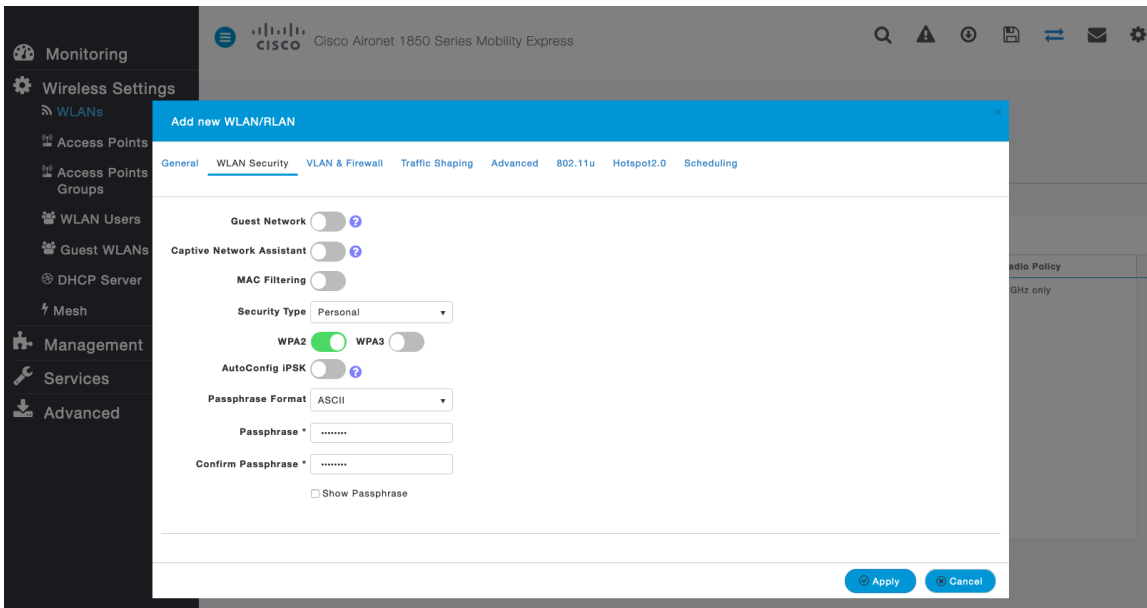
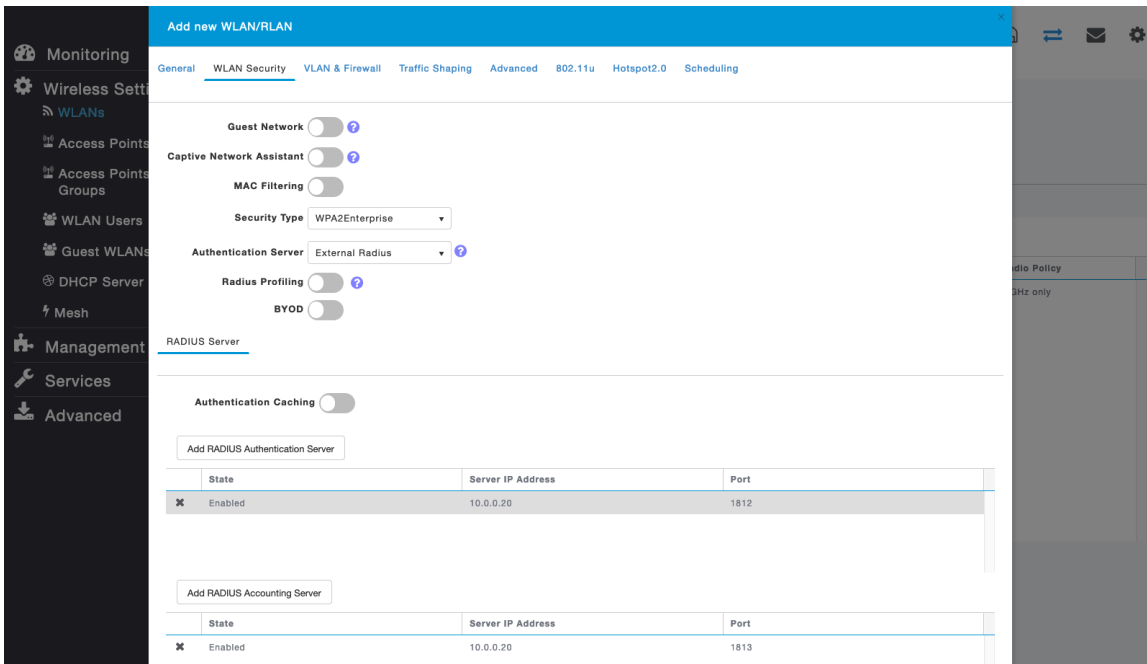
Cisco Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ（たとえば 5 GHz のみ）適用するよう指定できます。

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域で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。

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。



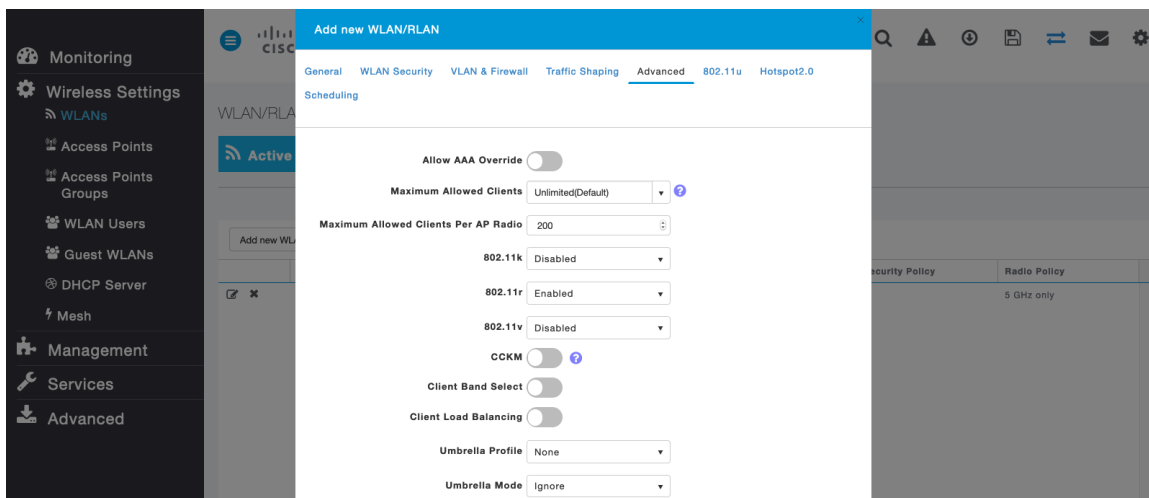
高速セキュア ローミング用に 802.11r (FT) を使用するには、802.1x または PSK のどちらを使用するかに応じて、[セキュリティタイプ (Security Type)] を [WPA2Enterprise] または [パーソナル (Personal)] に設定します。



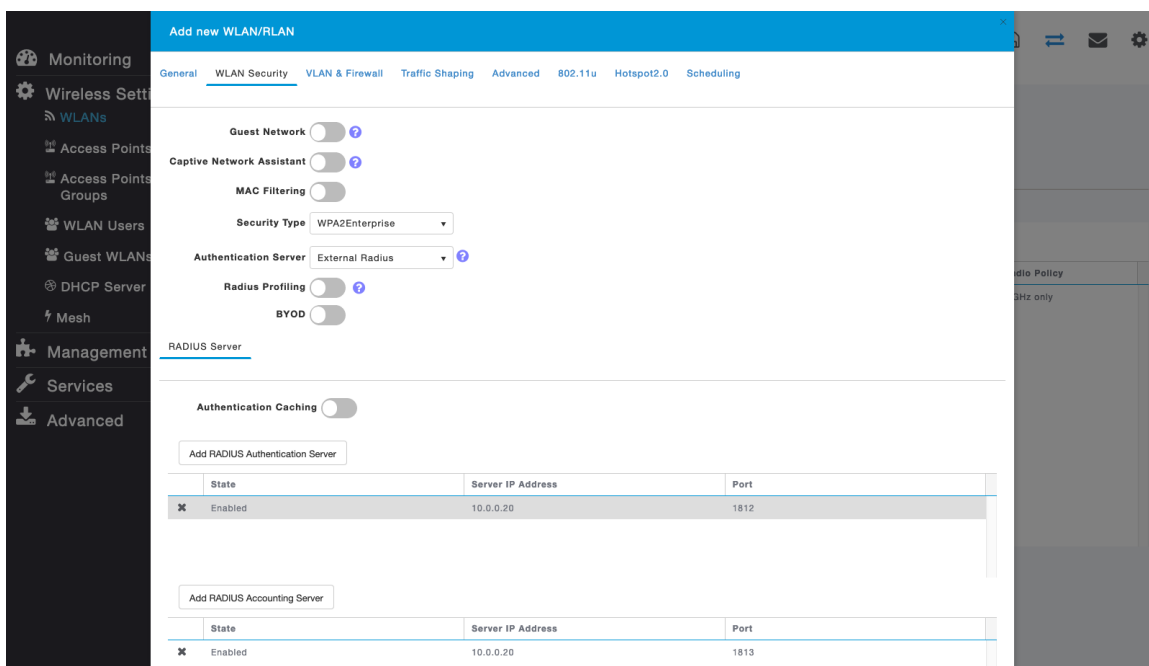
WLAN 設定の [詳細 (Advanced)] タブで、[802.11r] を [有効 (Enabled)] に設定します。

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

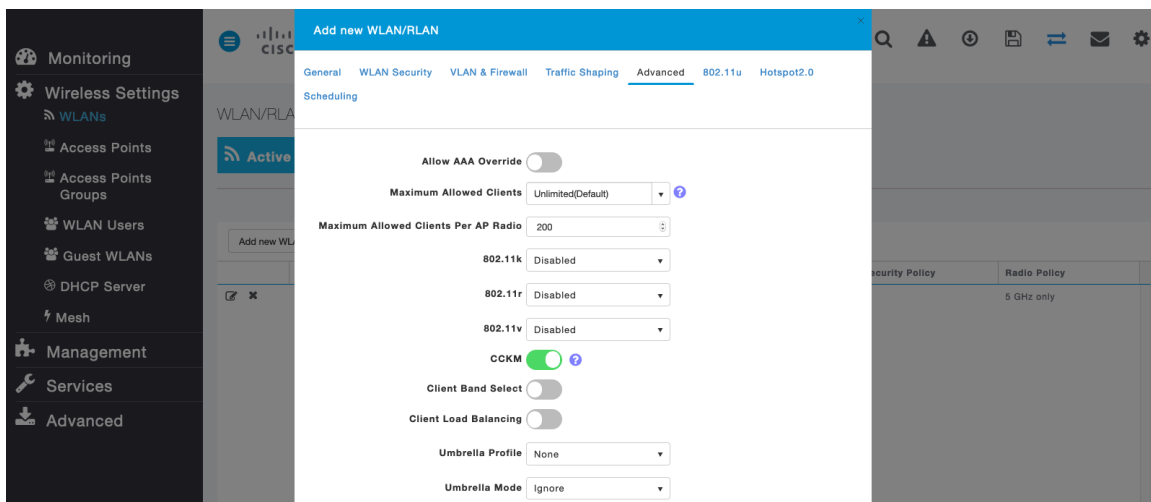
802.11k および 802.11v を有効にすることを推奨します。



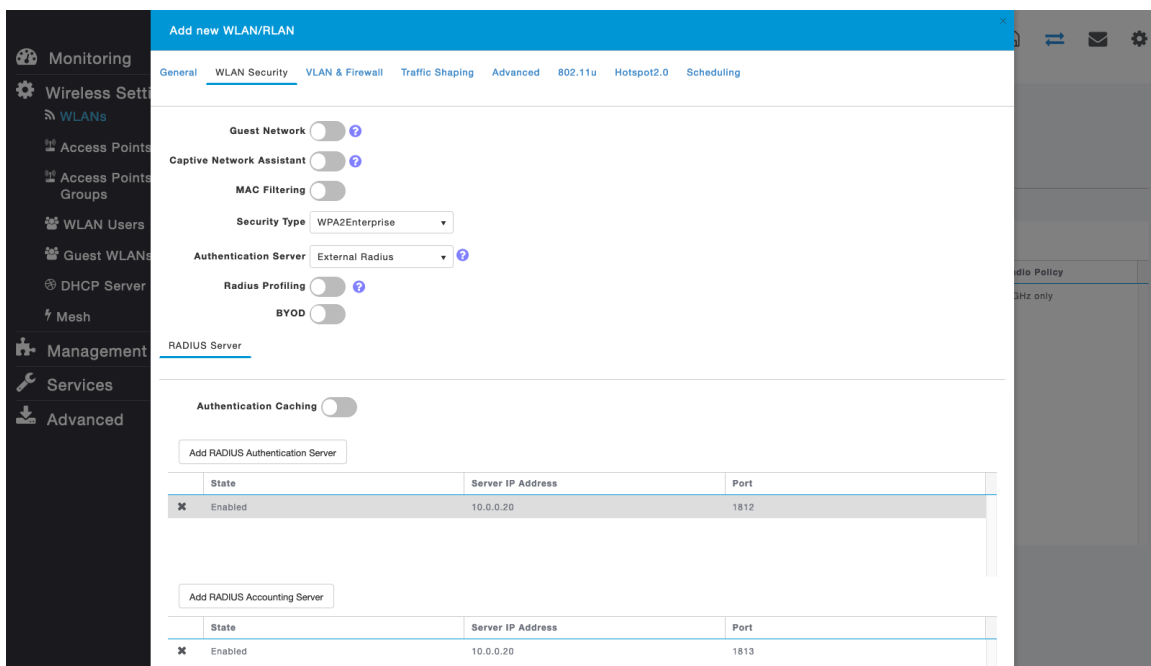
高速セキュアローミングに CCKM を使用するには、[セキュリティタイプ (Security Type)] を [WPA2Enterprise] に設定します。



WLAN 設定の [詳細 (Advanced)] タブで、[CCKM] を [有効 (Enabled)] に設定します。
 [クライアント帯域幅選択 (Client Band Select)] と [クライアントロードバランシング (Client Load Balancing)] が無効になっていることを確認します。
 802.11k および 802.11v を有効にすることを推奨します。



RADIUS 認証サーバーおよびアカウントサーバーは、WLAN レベルごとに設定して、グローバルリストを上書きできます。



ADMIN ACCOUNTS

Users 1

Management User Priority Order Local Admin Accounts TACACS+ **RADIUS** Auth Cached Users

Authentication Call Station ID Type: AP MAC Address:SSID

Authentication MAC Delimiter: Hyphen

Accounting Call Station ID Type: IP Address

Accounting MAC Delimiter: Hyphen

Fallback Mode: Passive

Username: cisco-probe

Interval: 300 Seconds

AP Events Accounting:

Apply

Add RADIUS Authentication Server

Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
<input checked="" type="checkbox"/> <input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.20	*****	1812

Add RADIUS Accounting Server

Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
<input checked="" type="checkbox"/> <input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.20	*****	1813

必要に応じて、WLAN の [ネイティブ VLAN ID (Native VLAN ID)] と [VLAN ID] を設定します。
[ピアツーピアブロック (Peer to Peer Block)] が無効になっていることを確認します。

Add new WLAN/RLAN

General WLAN Security **VLAN & Firewall** Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling

Client IP Management: Network(Default)

Peer to Peer Block:

Native VLAN ID: 1

Use VLAN Tagging: Yes

DHCP Scope: None VLAN ID: 3

No DHCP Scope associated with VLAN ID

Enable Firewall: No

VLAN ACL Map

VLAN Name	VLAN Id
data	2
voice	3

1 - 2 of 2 Items

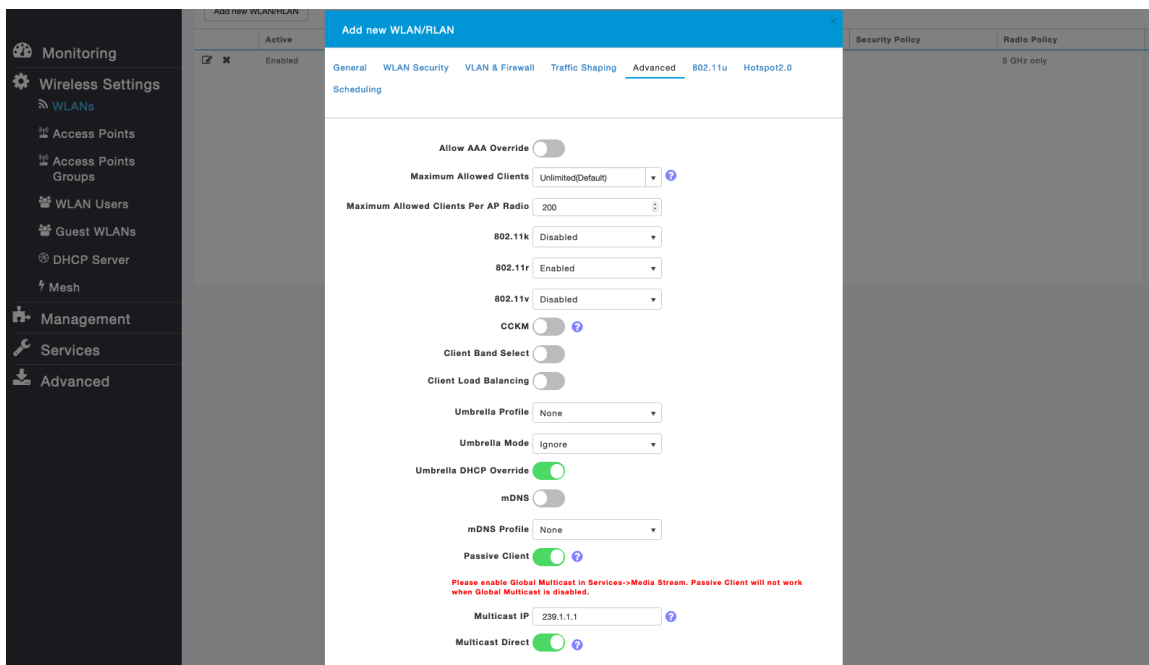
VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN

Apply Cancel

[QoS] に [プラチナ (音声) (Platinum (Voice))] が選択されていることを確認します。

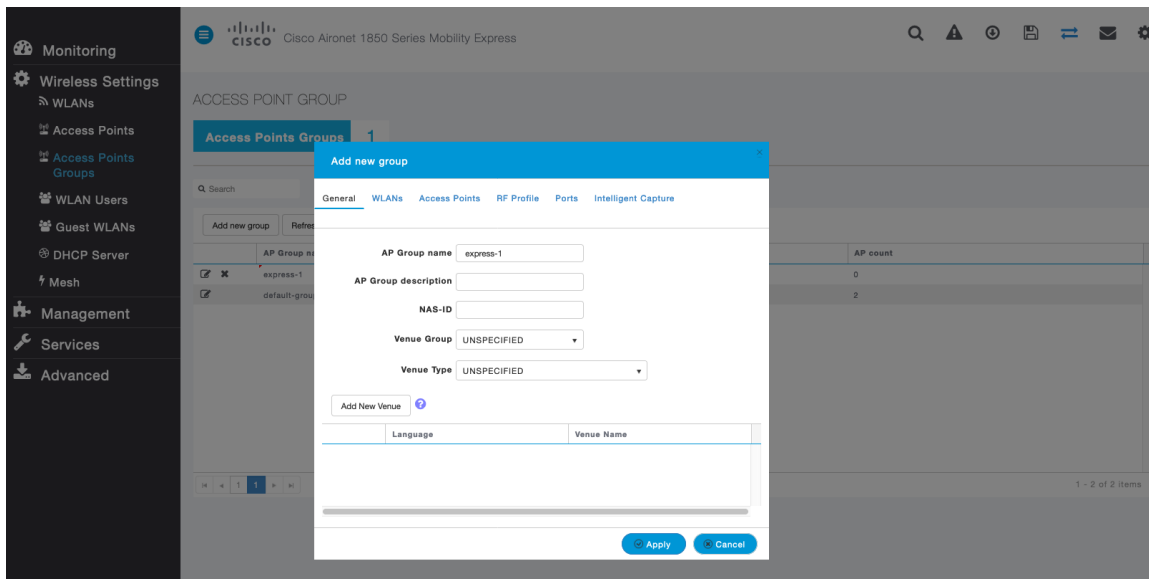
The screenshot displays the configuration page for a new WLAN/RLAN, specifically the 'Traffic Shaping' tab. The 'QoS' dropdown menu is set to 'Platinum (Voice)'. Below this, there are sections for 'Rate limits per client' and 'Rate limits per BSSID', each containing four fields for bandwidth limits (Average downstream, Average real-time downstream, Average upstream, and Average real-time upstream), all of which are currently set to 0 kbps. Further down, the 'Fastlane' option is set to 'Disabled', with a note indicating that enabling it would update the QoS value to platinum. The 'Application Visibility Control' is set to 'Enabled', and the 'AVC Profile' is set to 'voice'. At the bottom, there is an 'Add Rule' button and a table with columns for S..., Application, Action, Average Rate, and Burst Rate.

必要に応じて、[許可される最大クライアント数 (Maximum Allowed Clients)] と [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)] を設定できます。

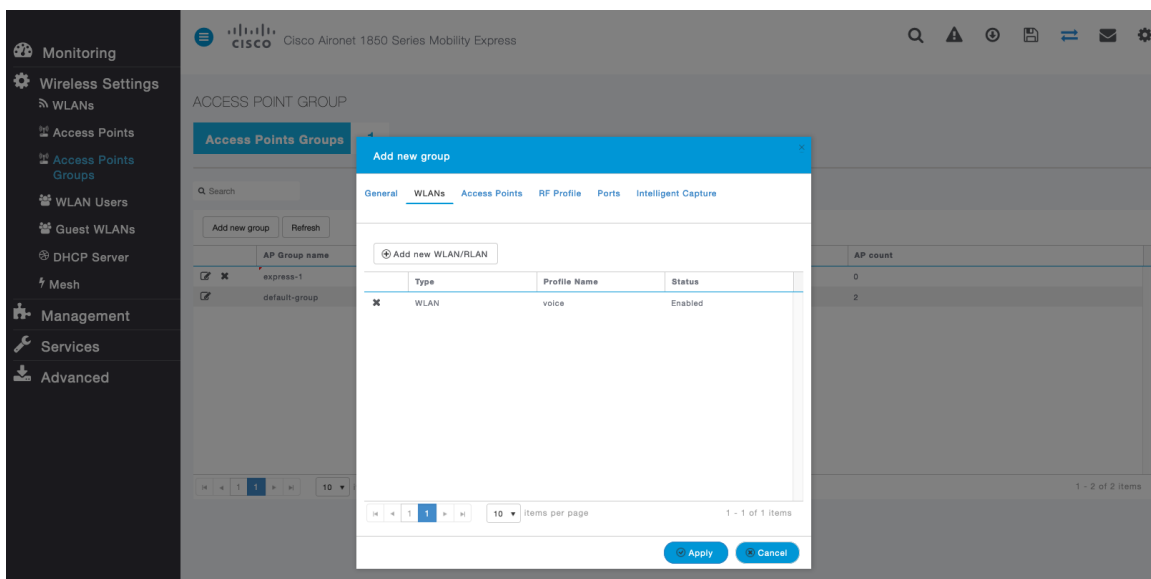
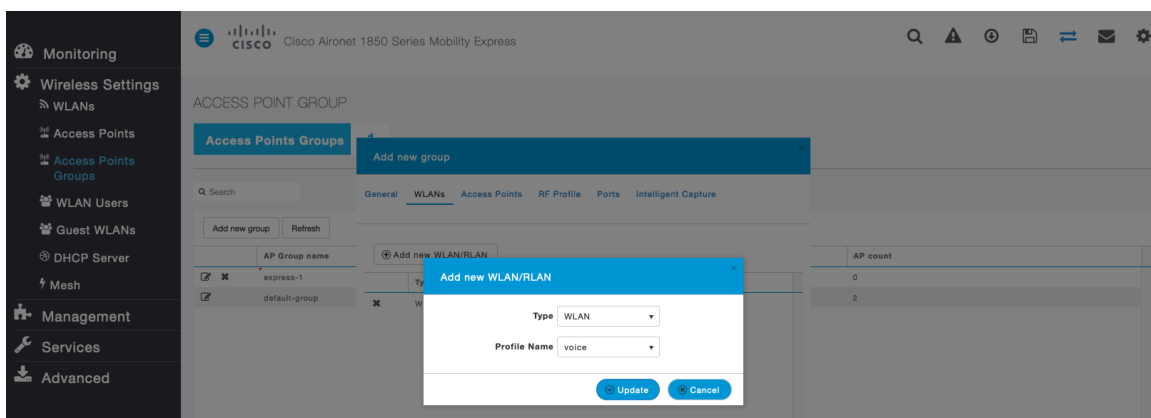


AP グループ

AP グループは、有効にする WLAN、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。

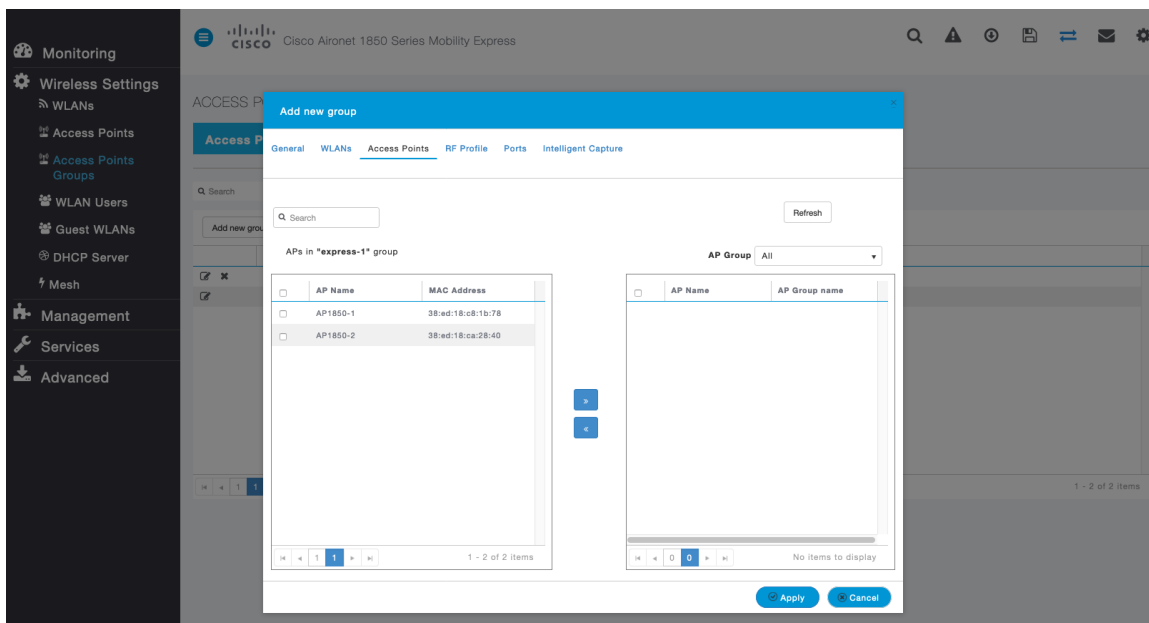


[WLAN (WLANS)] タブで、対象 WLAN と、マッピングするインターフェイスを選択して、[追加 (Add)] を選択します。

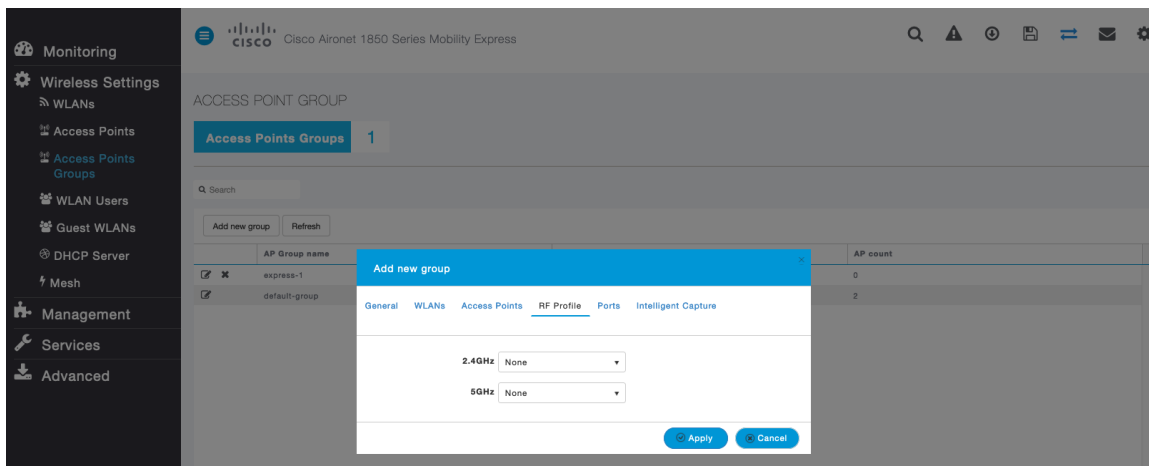


[アクセスポイント (Access Points)] タブで、対象アクセスポイントを選択して、[適用 (Apply)] を選択します。

その後、選択したアクセスポイントが再起動します。



[RF プロファイル (RF Profile)] タブで、対象の [2.4GHz] または [5GHz] プロファイルを選択して、[適用 (Apply)] を選択します。



RF プロファイル

RF プロファイルを作成し、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 設定などを指定できます。

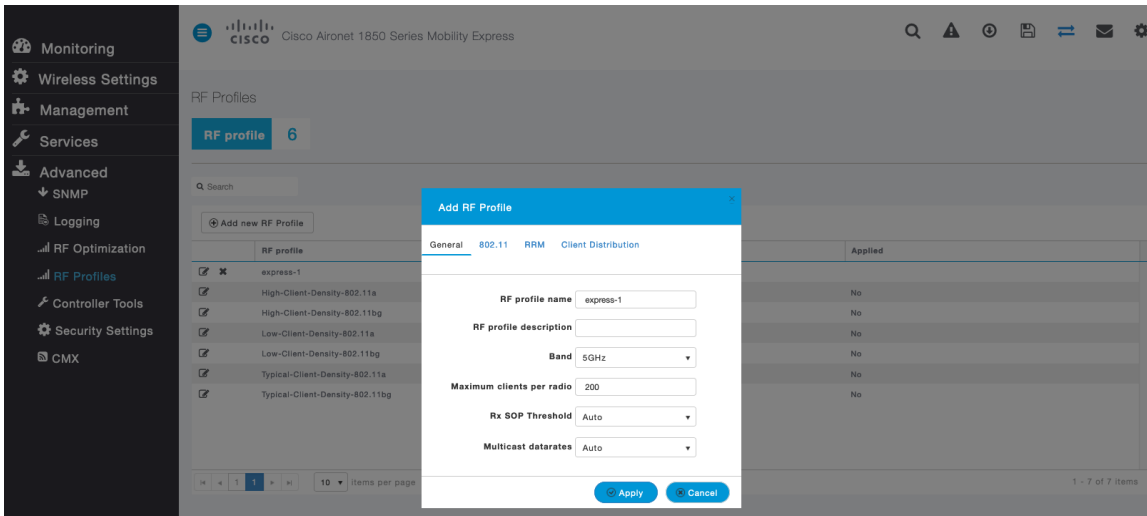
Cisco Wireless Phone 840 および 860 で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。作成した RF プロファイルは、AP グループに適用されます。

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 [5GHz] または [2.4GHz] を選択します。

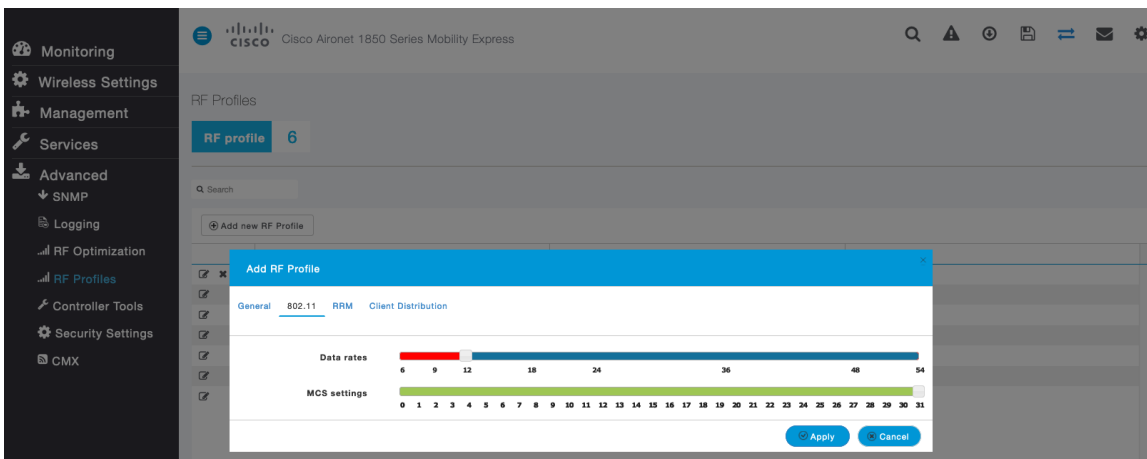
必要に応じて、[無線ごとの最大クライアント数 (Maximum clients per radio)]、[マルチキャストデータレート (Multicast Data Rates)]、および [Rx Sop のしきい値 (Rx Sop Threshold)] を設定できます。

[Rx Sop のしきい値 (Rx Sop Threshold)] にはデフォルト値 ([自動 (Auto)]) を使用することを推奨します。

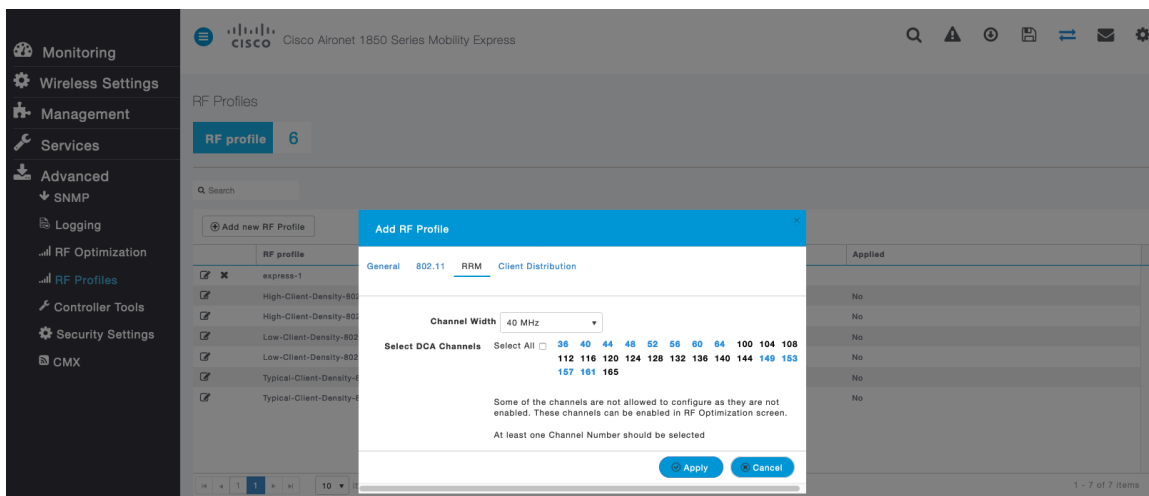


[802.11] タブで、必要に応じてデータレートを設定します。

[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生じます。



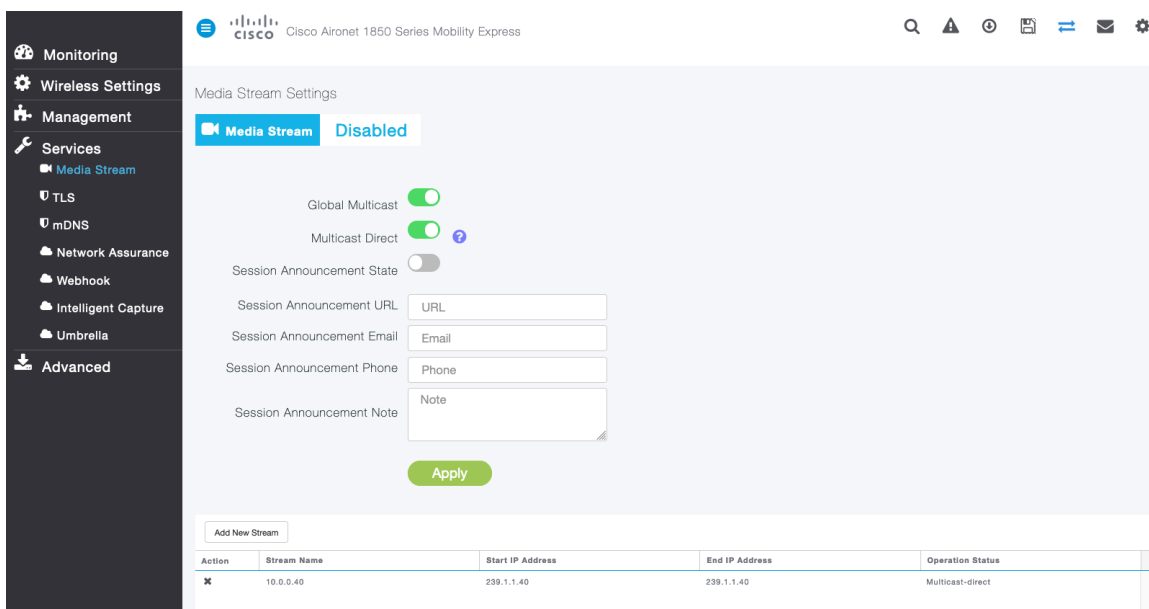
[RRM] タブでは、[チャンネル幅 (Channel Width)] 設定と [DCA チャンネル (DCA Channels)] を構成できます。



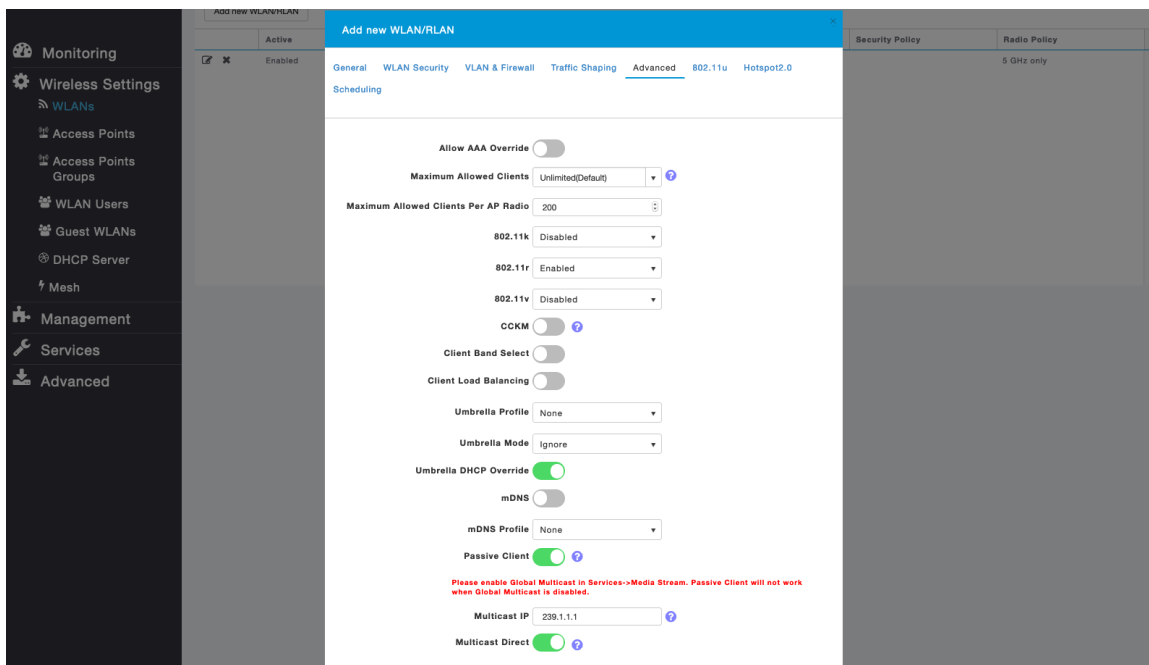
マルチキャスト ダイレクト

[メディアストリーム (Media Stream)] 設定で、[グローバルマルチキャスト (Global Multicast)] と [マルチキャストダイレクト (Multicast Direct)] を有効にします。

次に、ストリームを設定します。



[メディアストリーム (Media Stream)] 設定で [マルチキャストダイレクト (Multicast Direct)] を有効にすると、WLAN 設定の [詳細設定 (Advanced)] タブに [マルチキャストダイレクト (Multicast Direct)] を有効にするオプションが表示されます。



Cisco Autonomous (自律) アクセス ポイント

Cisco Autonomous 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。

- **[802.11r (FT)]** または **[CCKM]** が **[有効 (Enabled)]** になっていることを確認します。
- **802.11k** を **[有効 (Enabled)]** に設定することを推奨
- **802.11v** を有効に設定することを推奨
- 必要に応じて **[データレート (Data Rates)]** を設定します
- **[DTPC]** を有効にします。
- **[Quality of Service (QoS)]** を設定します。
- **[WMM ポリシー (WMM Policy)]** を **[必須 (Required)]** に設定します
- **[Aironet 拡張機能 (Aironet Extensions)]** が **[有効 (Enabled)]** になっていることを確認します。
- **[Public Secure Packet Forwarding (PSPF)]** を無効にします。
- **[IGMP スヌーピング (IGMP Snooping)]** を **[有効 (Enabled)]** に設定します。

802.11 ネットワークの設定

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域で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。

5 GHz を使用する場合は、802.11a/n/ac ネットワークのステータスが **[有効 (Enabled)]** に設定されていることを確認します。

Network Interfaces: Summary			
System Settings			
IP Address (Static)	10.9.0.9		
IP Subnet Mask	255.255.255.0		
Default Gateway	10.9.0.2		
MAC Address	18e7.281b.3f54		
Interface Status	GigabitEthernet	Radio0-802.11N 2.4GHz	Radio1-802.11AC 5GHz
Software Status	Enabled ↑	Disabled ↓	Enabled ↑
Hardware Status	Up ↑	Down ↓	Up ↑
Interface Resets	5	0	8

11r over Air を有効にして高速セキュア ローミングを有効にすることを推奨します。

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 以上をそれぞれ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ります。

5 GHz を使用する場合は、多数のチャン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ためにチャンネルの数を制限できます（例：12 チャンネルのみ）。

Cisco Autonomous アクセスポイントの場合、動的周波数選択（DFS）を選択して、自動チャン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。

帯域 1 は、UNII-1 チャンネル（チャンネル 36、40、44、または 48）を使用するアクセスポイントでのみ選択できます。

使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセスポイントの設定をグローバル設定よりも優先させることができます。

その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

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。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセスポイントを使用している場合は 5 GHz チャンネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

[クライアント電力 (Client Power)] が正しく設定されていることを確認します。Cisco Autonomous アクセスポイントでは、クライアント電力のデフォルト設定である **[最大 (Max)]** 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ダプタイズされません。

[ワールドモード (World Mode)] で [Dot11d] を有効にし、適切な [国コード (Country Code)] を設定します。

[Aironet 拡張機能 (Aironet Extensions)] 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、[DTIM] を「2」に設定します。

NETWORK

NETWORK MAP

Summary
Adjacent Nodes

NETWORK INTERFACE

Summary
IP Address
GigabitEthernet0
Radio0-802.11N 2.4GHz
Radio1-802.11AC 5GHz

RADIO1-802.11AC^{5GHz} STATUS DETAILED STATUS SETTINGS CARRIER BUSY TEST

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 56 minutes

Network Interfaces: Radio1-802.11AC^{5GHz} Settings

Enable Radio: Enable Disable

Current Status (Software/Hardware): Enabled ↑ Up ↑

Role in Radio Network:

- Access Point
- Access Point (Fallback to Radio Shutdown)
- Access Point (Fallback to Repeater)
- Repeater
- Root Bridge
- Non-Root Bridge
- Root Bridge with Wireless Clients
- Non-Root Bridge with Wireless Clients
- Workgroup Bridge
- Universal Workgroup Bridge Client MAC: (HHHH.HHHH.HHHH)
- Scanner
- Spectrum [Spectrum Information](#)

Max-Client: enable disable (1-255)

11r Configuration: enable disable
 over-air over-ds Reassociation-time: (20-1200 ms)

Data Rates:

6.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
9.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
12.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
18.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
24.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
36.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
48.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
54.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a0.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a1.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a2.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a3.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a4.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a5.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a6.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a7.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a8.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a9.1-4Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a0.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a1.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a2.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a3.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a4.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a5.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a6.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a7.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a8.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a9.2-4Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
a0.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a1.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a2.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a3.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a4.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a5.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a6.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a7.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

a8.3-2Mb/sec Require Enable Disable
a9.3-2Mb/sec Require Enable Disable

MCS Rates:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Enable	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Transmitter Power (dBm): 15 12 9 6 3 Max [Power Translation Table \(mW/dBm\)](#)

Client Power (dBm): Local 15 12 9 6 3 Max

DefaultRadio Channel: Channel 36 5180 MHz

Dynamic Frequency Selection Bands:
Band 1 - 5,150 to 5,250 GHz
Band 2 - 5,250 to 5,350 GHz
Band 3 - 5,470 to 5,725 GHz
Band 4 - 5,725 to 5,825 GHz

Channel Width: 20 MHz

World Mode Multi-Domain Operation: Disable Legacy Dot11d

Country Code: Indoor Outdoor

Radio Preamble: Short Long

Antenna: a-antenna ab-antenna abc-antenna abcd-antenna

Internal Antenna Configuration: Enable Disable
Antenna Gain(dBi): (-128 - 128)

Gratuitous Probe Response(GPR): Enable Disable
Period(Kusec): (10-255)
Transmission Speed:

Traffic Stream Metrics: Enable Disable

Aironet Extensions: Enable Disable

Ethernet Encapsulation Transform: RFC1042 802.1H

Reliable Multicast to WGB: Disable Enable

Public Secure Packet Forwarding: [PSPF must be set per VLAN. See VLAN page](#)

Beacon Privacy Guest-Mode: Enable Disable

Beacon Period: (20-4000 Kusec) Data Beacon Rate (DTIM): (1-100)

Max. Data Retries: (1-128) RTS Max. Retries: (1-128)

Fragmentation Threshold: (256-2346) RTS Threshold: (0-2347)

Root Parent Timeout: (0-65535 sec)

Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)

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 が有効に設定されていることを確認します。

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、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、サポート対象（任意）レートとして 12 Mbps 以上をそれぞれ設定する必要があります。

WLAN の設定

Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

ただし、音声対応 Cisco Wireless LAN 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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ（たとえば 802.11a のみ）適用するよう指定できます。

[WPA2] キー管理を有効にします。

[11r] または **[CCKM]** が有効になっていることを確認します。11r を推奨します。

Security

- [Admin Access](#)
- [Encryption Manager](#)
- [SSID Manager](#)
- [Dot11u Manager](#)
- [Server Manager](#)
- [AP Authentication](#)
- [Intrusion Detection](#)
- [Local RADIUS Server](#)
- [Advance Security](#)

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 33 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >

data

voice

SSID:

VLAN: [Define VLANs](#)

Backup 1:

Backup 2:

Backup 3:

Band-Select: Band Select

Universal Admin Mode: Universal Admin Mode

Interface: Radio0-802.11N^{2.4GHz}
 Radio1-802.11AC^{5GHz}

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

Open Authentication:

Web Authentication Web Pass

Shared Authentication:

Network EAP:

Server Priorities:

EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

Client Authenticated Key Management

Key Management: CCKM Enable WPA

WPA Pre-shared Key: ASCII Hexadecimal

11w Configuration:

11w Association-comeback: (1000-20000)

11w Saquery-retry: (100-500)

IDS Client MFP

Enable Client MFP on this SSID:

AP Authentication

Credentials: [Define Credentials](#)

Authentication Methods Profile: [Define Authentication Methods Profiles](#)

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

Rate Limit Parameters

Limit TCP:

Input: Rate: Burst-Size: (0-500000)

Output: Rate: Burst-Size: (0-500000)

Limit UDP:

Input: Rate: Burst-Size: (0-500000)

Output: Rate: Burst-Size: (0-500000)

General Settings

Advertise Extended Capabilites of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

Association Limit (optional): (1-255)

EAP Client (optional):
 Username: Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

Set DataBeacon Rate (DTIM): (1-100)

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

Radio1-802.11AC^{5GHz}:

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

ワイヤレス音声/データを別個の VLAN にセグメント化します。

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は、PSPF が無効になっていることを確認します。PSPF が有効になっている場合にクライアントが同じアクセス ポイントに関連付けられると、直接通信できません。PSPF を有効にすると、オーディオは無指向となります。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 48 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

Current VLAN List Create VLAN [Define SSIDs](#)

< NEW >

VLAN 2

VLAN 3

VLAN 10

Delete

VLAN ID: (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N^{2.4GHz}

Radio1-802.11AC^{5GHz}

Management VLAN (If non-native)

Apply Cancel

VLAN Information

View Information for: VLAN 2

	GigabitEthernet Packets	Radio0-802.11N ^{2.4GHz} Packets	Radio1-802.11AC ^{5GHz} Packets
Received	65884		65884
Transmitted	5462		5462

Refresh

暗号化タイプとして [AES] が選択されていることを確認します。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

Admin Access
Encryption Manager
SSID Manager
Dot11u Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 32 minutes

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 3 Define VLANs

Encryption Modes

None

WEP Encryption Optional

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

Cipher AES CCMP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit <input type="button" value="v"/>
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit <input type="button" value="v"/>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit <input type="button" value="v"/>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit <input type="button" value="v"/>

Global Properties

Broadcast Key Rotation Interval: Disable Rotation
 Enable Rotation with Interval: (10-10000000 sec)

WPA Group Key Update: Enable Group Key Update On Membership Termination
 Enable Group Key Update On Member's Capability Change

RADIUS サーバを認証およびアカウントングに使用できるように設定します。

Save Configuration Ping Logout Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

Admin Access
Encryption Manager
SSID Manager
Dot11u Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security

SERVER MANAGER GLOBAL PROPERTIES

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 42 minutes

Security: Server Manager

Backup RADIUS Server

IP Version: IPV4 IPV6

Backup RADIUS Server Name:

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

RADIUS

< NEW >
10.0.0.20
10.9.0.9

IP Version: IPV4 IPV6

Server Name: 10.0.0.20

Server: 10.0.0.20 (Hostname or IP Address)

Shared Secret:

Delete

Authentication Port (optional): 1812 (0-65535)

Accounting Port (optional): 1813 (0-65535)

Apply Cancel

Default Server Priorities

EAP Authentication

Priority 1: 10.0.0.20

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Accounting

Priority 1: 10.0.0.20

Priority 2: < NONE >

Priority 3: < NONE >

Admin Authentication (RADIUS)

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Admin Authentication (TACACS+)

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

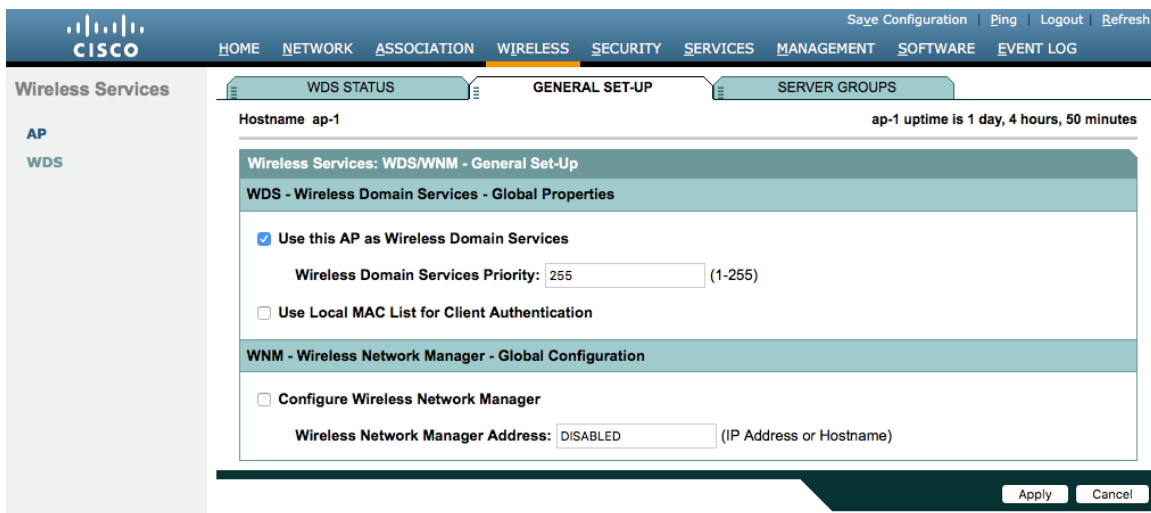
Apply Cancel

無線ドメイン サービス (WDS)

Cisco Autonomous アクセス ポイント環境では、無線ドメイン サービスを使用する必要があります。このサービスは高速セキュア ローミングにも必要です。

1 つのアクセス ポイントをプライマリ WDS サーバとして選択し、もう 1 つのアクセス ポイントをバックアップ WDS サーバとして選択します。

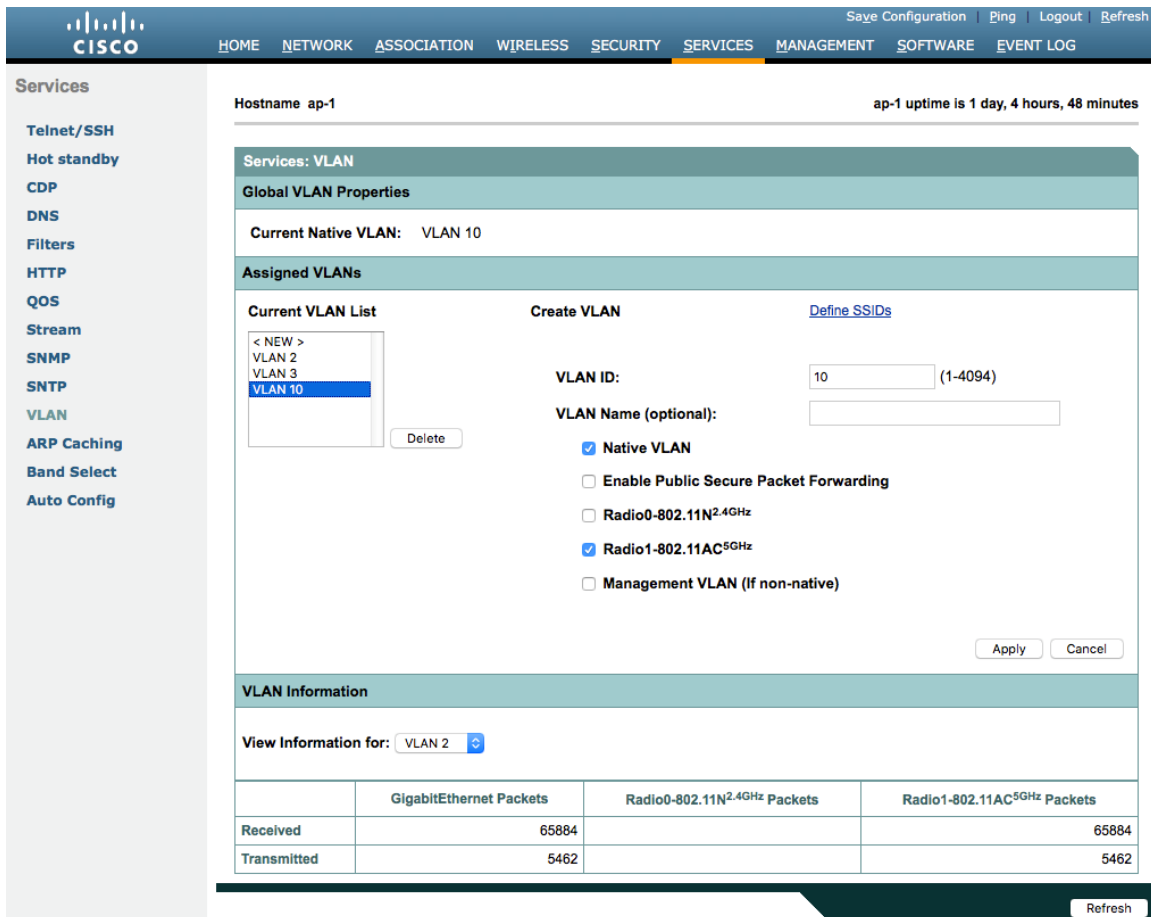
プライマリ WDS サーバに最も高い優先順位 (255 など) を設定し、バックアップ WDS サーバにそれよりも低い優先順位 (254 など) を設定します。



Cisco Autonomous アクセス ポイントはマルチキャスト プロトコルである Inter-Access Point Protocol (IAPP) を使用するため、専用のネイティブ VLAN を使用する必要があります。

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ためにも、VLAN 1 は使用しないことを推奨します。

Cisco Autonomous アクセス ポイントが直接接続しているスイッチ ポートでは、ポート セキュリティを無効にする必要があります。



無線ドメイン サービス用のサーバ グループを定義する必要があります。

最初に、インフラストラクチャ認証に使用するサーバ グループを定義します。

インフラストラクチャ認証にはローカル RADIUS を使用することを推奨します。

インフラストラクチャ認証にローカル RADIUS を使用しない場合は、無線ドメイン サービスが有効になっているすべてのアクセス ポイントが RADIUS サーバに設定されていることを確認する必要があります。

The screenshot shows the Cisco Wireless Services configuration interface for a WDS Server Group. The page title is "Wireless Services: WDS - Server Groups". The host is identified as "ap-1" with an uptime of "1 day, 4 hours, 51 minutes".

Server Group List: A list containing "< NEW >" and "WDS". A "Delete" button is next to the list.

Server Group Name: WDS

Group Server Priorities: [Define Servers](#)

- Priority 1: 10.9.0.9
- Priority 2: < NONE >
- Priority 3: < NONE >

Use Group For:

- Infrastructure Authentication
- Client Authentication

Authentication Settings:

- EAP Authentication
- LEAP Authentication
- MAC Authentication
- Default (Any) Authentication

SSID Settings:

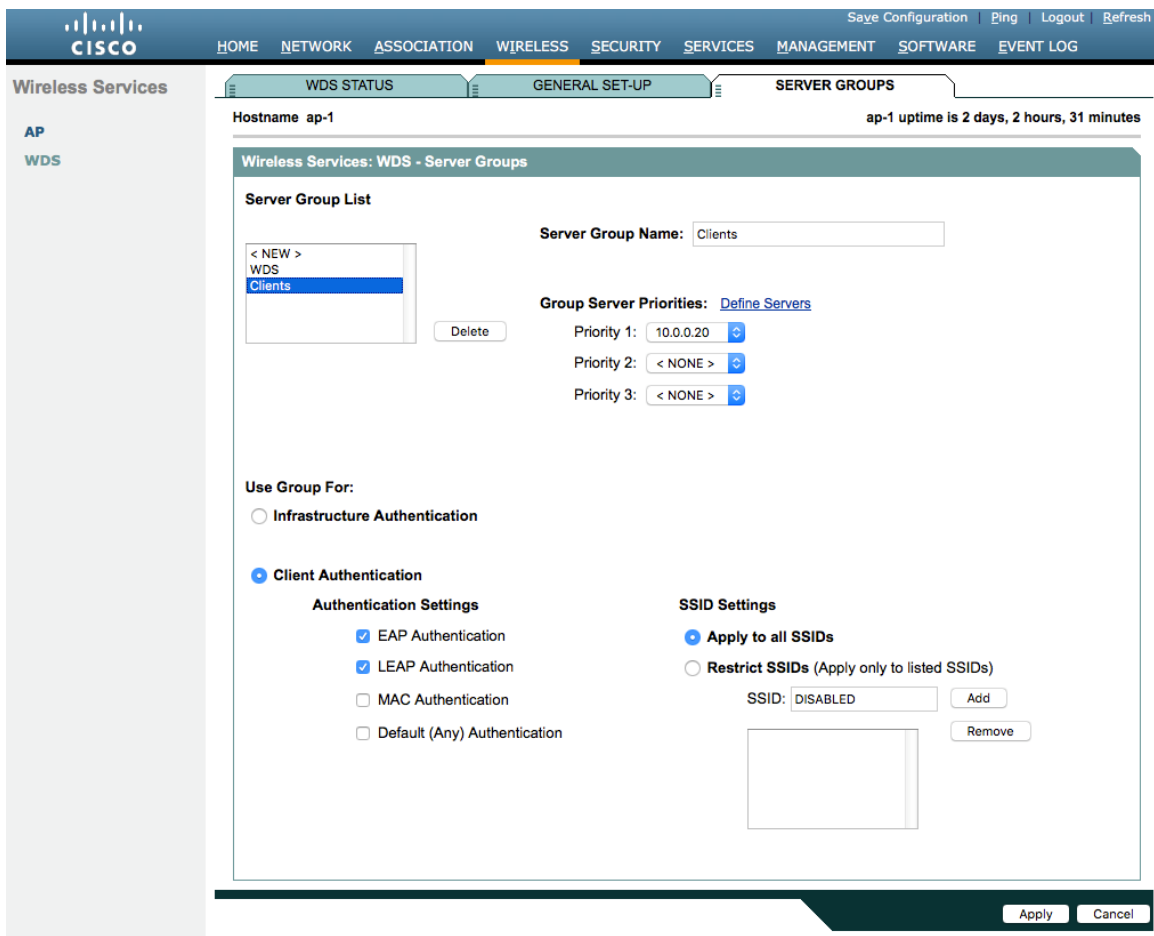
- Apply to all SSIDs
- Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED [Add] [Remove]

[Apply] [Cancel]

次に、クライアント認証に使用するサーバ グループを定義します。

無線ドメイン サービスが有効になっているすべてのアクセス ポイントが RADIUS サーバに設定されていることを確認する必要があります。



インフラストラクチャ認証にローカル RADIUS を使用する場合は、すべての認証プロトコルを有効にします。
 ローカルアクセスポイント用のネットワーク アクセス サーバー エントリを作成します。
 無線ドメイン サービスが有効になっているアクセス ポイントに対して認証を行うようにアクセス ポイントが設定されるユーザ アカウントを定義します。
 無線ドメイン サービスに参加する各アクセス ポイント上でローカル RADIUS を設定します。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

Admin Access
Encryption Manager
SSID Manager
Dot11u Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security

STATISTICS GENERAL SET-UP EAP-FAST SET-UP

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 43 minutes

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols: EAP FAST
 LEAP
 MAC

Apply Cancel

Network Access Servers (AAA Clients)

Current Network Access Servers

< NEW >
10.9.0.9

Delete

Network Access Server: 10.9.0.9 (IP Address)

Shared Secret:

Apply Cancel

Individual Users

Current Users

< NEW >
wds

Delete

Username: wds

Password: Text NT Hash

Confirm Password:

Group Name: < NONE >

MAC Authentication Only

Apply Cancel

User Groups

Current User Groups

< NEW >

Delete

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional): Infinite
 Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

..... Delete

Apply Cancel

無線ドメイン サービスが有効になるように必要なアクセス ポイントを正しく設定したら、WDS サーバとして機能するアクセス ポイントを含むすべてのアクセス ポイントを、WDS サーバに対して認証できるように設定する必要があります。

[SWAN インフラストラクチャに参加 (Participate in SWAN Infrastructure)] を有効にします。

単一の WDS サーバを使用する場合は、その WDS サーバの IP アドレスを指定できます。そうでない場合は、[自動検出 (Auto Discovery)] を有効にします。

WDS サーバに対する認証に使用する [ユーザー名 (Username)] と [パスワード (Password)] を入力します。

Wireless Services

AP

WDS

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 50 minutes

Wireless Services: AP

Participate in SWAN Infrastructure: Enable Disable

WDS Discovery: Auto Discovery Specified Discovery: (IP Address)

Username:

Password:

Confirm Password:

Authentication Methods Profile: [Define Authentication Methods Profiles](#)

アクセス ポイントを WDS サーバに対して認証できるように設定したら、[WDS ステータス (WDS Status)] から WDS サーバの状態と WDS サーバに登録されているアクセス ポイントの数を確認できます。

Wireless Services

AP

WDS

WDS STATUS

Hostname ap-1 ap-1 uptime is 1 day, 5 hours, 1 minute

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IPv4 Address	IPv6 Address	Priority	State
18e7.281b.3f54	10.9.0.9	::	255	Administratively StandAlone - ACTIVE

WDS Registration

APs: 1 Mobile Nodes: 0

AP Information

Hostname	MAC Address	IPv4 Address	IPv6 Address	CDP Neighbor	State
ap-1	18e7.281b.3f54	10.9.0.9	::	Switch-2.gil	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

Wireless Network Manager Information

IP Address	Authentication Status

コール アドミッション制御 (CAC)

Cisco Autonomous アクセス ポイントには、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 アクセス ポイントで CAC を有効にすることは推奨されません。

Cisco Autonomous アクセスポイントには、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)、サイレントモニタリング、コール録音は機能しません。

Cisco Autonomous アクセス ポイントで音声またはビデオのアドミッション制御を有効にする場合は、SSID でもアドミッションをブロック解除する必要があります。最近のリリースでは、アドミッションはデフォルトでブロック解除されています。

```
Dot11 ssid voice
vlan 3
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2 dot11r
admit-traffic
```

Save Configuration Ping Logout Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QoS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config

QoS POLICIES RADIO0-802.11N^{2.4GHZ} ACCESS CATEGORIES RADIO1-802.11AC^{5GHZ} ACCESS CATEGORIES ADVANCED

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 47 minutes

Services: QoS Policies - Access Category

Access Category Definition

Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2x-1; x can be 0-10)	AP	<input type="text" value="4"/>	<input type="text" value="4"/>	<input type="text" value="3"/>	<input type="text" value="2"/>
	Client	<input type="text" value="4"/>	<input type="text" value="4"/>	<input type="text" value="3"/>	<input type="text" value="2"/>
Max Contention Window (2x-1; x can be 0-10)	AP	<input type="text" value="10"/>	<input type="text" value="6"/>	<input type="text" value="4"/>	<input type="text" value="3"/>
	Client	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="4"/>	<input type="text" value="3"/>
Fixed Slot Time (0-20)	AP	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
	Client	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="2"/>
Transmit Opportunity (0-65535 μS)	AP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="3008"/>	<input type="text" value="1504"/>
	Client	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="3008"/>	<input type="text" value="1504"/>

Optimized Voice WFA Default Apply Cancel

Admission Control for Video and Voice

Video(CoS 4-5)
 Admission Control

Voice(CoS 6-7)
 Admission Control
Max Channel Capacity (%):
Roam Channel Capacity (%):

Apply Cancel

QoS ポリシー

Cisco Autonomous アクセス ポイントに次の QoS ポリシーを設定して、CoS (WMM UP) マッピングに対する DSCP を有効にします。

これにより、パケットは、正しくマーキングされている限り、アクセス ポイント レベルで受信されたときに適切なキューに入れられます。

Save Configuration Ping Logout Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QOS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config

QoS POLICIES RADIO0-802.11N^{2.4GHz} ACCESS CATEGORIES RADIO1-802.11AC^{5GHz} ACCESS CATEGORIES ADVANCED

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 44 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: Voice

Policy Name: Voice

Classifications: DSCP - COS Controlled Load (4)
DSCP - COS Video < 100ms Latency (5)
DSCP - COS Voice < 10ms Latency (6)

Delete Classification

Match Classifications: IP Precedence: Routine (0) IP DSCP: Best Effort (0-63) IP Protocol 119 Filter: No Filters defined. Define Filters. Default Classification for Packets on the VLAN: Best Effort (0)

Apply Class of Service: Best Effort (0) Add Best Effort (0) Add Best Effort (0) Add Best Effort (0) Add

Rate Limiting: Bits per Sec.: (8000-2000000000) Burst Rate (Bytes): (1000-512000000) Conform Action: Transmit Exceed Action: Drop Add

Apply Delete Cancel

Apply Policies to Interface/ VLANs

VLAN 2	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
Incoming		Data	Data
Outgoing		Data	Data
VLAN 3	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
Incoming		Voice	Voice
Outgoing		< NONE >	< NONE >
VLAN 10	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
Incoming		< NONE >	< NONE >
Outgoing		< NONE >	< NONE >

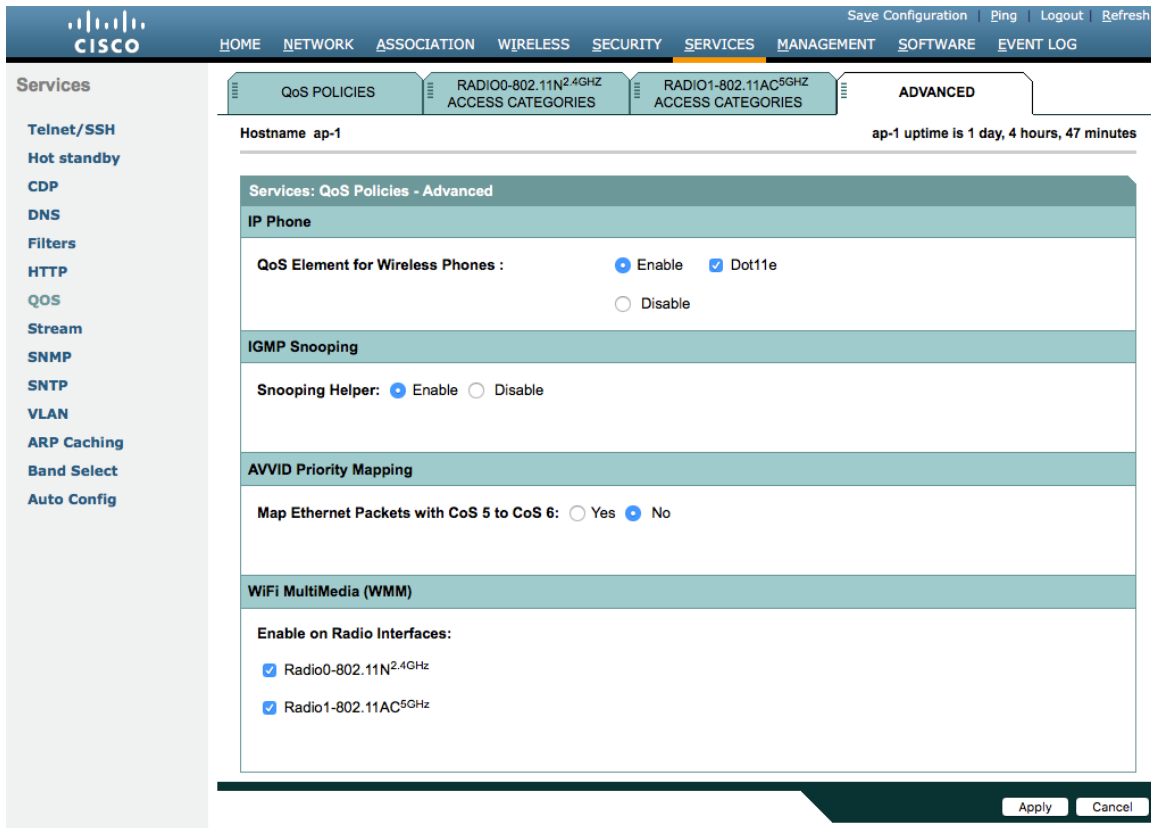
Apply Cancel

QBSS を有効にするには、[有効 (Enable)] を選択し、[Dot11e] をオンにします。

[Dot11e] をオンにすると、両方の CCA バージョン (802.11e および Cisco バージョン 2) が有効になります。

[IGMP スヌーピング (IGMP Snooping)] が有効になっていることを確認します。

[Wi-Fi マルチメディア (WMM) (Wi-Fi MultiMedia (WMM))] が有効になっていることを確認します。



[ストリーム (Stream)] 機能を直接、または QoS 設定セクションの無線アクセスカテゴリで **[最適化された音声 (Optimized Voice)]** を選択して有効にする場合は、デフォルト値を使用します。802.11b/g では 5.5、6、11、12、および 24 Mbps、802.11a では 6、12 および 24 Mbps、802.11n では 6.5、13 および 26 Mbps が通常のレートとしてデフォルトで有効化されます。

[ストリーム (Stream)] 機能を有効にする場合は、音声パケットのみが音声キューに追加されることを確認します。シグナリングパケットは、別個のキューに追加する必要があります。SIP を別個のキューに入れるには、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。

Services: Stream

Packet Handling per User Priority:

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Reliable	NO DISCARD (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

Low Latency Packet Rates:

- 6.0Mb/sec : Nominal Non-Nominal Disable
- 9.0Mb/sec : Nominal Non-Nominal Disable
- 12.0Mb/sec : Nominal Non-Nominal Disable
- 18.0Mb/sec : Nominal Non-Nominal Disable
- 24.0Mb/sec : Nominal Non-Nominal Disable
- 36.0Mb/sec : Nominal Non-Nominal Disable
- 48.0Mb/sec : Nominal Non-Nominal Disable
- 54.0Mb/sec : Nominal Non-Nominal Disable

Buttons: Apply, Cancel

電源管理

プロキシ ARP を有効にするには、[クライアントの ARP キャッシング (Client ARP Caching)] を [有効 (Enable)] に設定します。

また、[すべての IP アドレスが必ずしも既知でない場合に ARP 要求を無線インターフェイスに転送する (Forward ARP Requests to Radio Interfaces When Not All Client IP Addresses Are Known)] がオンになっていることを確認します。

Services: ARP Caching

Client ARP Caching: Enable Disable

Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known

Buttons: Apply, Cancel

設定例

バージョン 15.3

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap-1
!
logging rate-limit console 9
!
aaa new-model
!
aaa group server radius rad_eap
server name 10.0.0.20
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
server name 10.0.0.20
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius WDS
server name 10.9.0.9
!
aaa group server radius Clients
server name 10.0.0.20
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login method_WDS group WDS
aaa authentication login method_Clients group Clients
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
clock timezone -0500 -5 0
```

```

clock summer-time -0400 recurring
no ip source-route
no ip cef
ip domain name cisco.com
ip name-server 10.0.0.30
ip name-server 10.0.0.31
!
dot11 pause-time 100
dot11 syslog
!
dot11 ssid data
    vlan 2
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa version 2
!
dot11 ssid voice
    vlan 3
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa version 2 dot11r
!
dot11 arp-cache optional
dot11 phone dot11e
!
no ipv6 cef
!
crypto pki trustpoint TP-self-signed-672874324
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-672874324
    revocation-check none
    rsakeypair TP-self-signed-672874324
!
crypto pki certificate chain TP-self-signed-672874324
    certificate self-signed 01
    30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 36373238 37343332 34301E17 0D313630 38303332 33303533
    385A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
    532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3637 32383734
    33323430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
    CB155DD1 3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9
    5F5A1B75 7910F9F5 6E9EDEF4 730942C7 17DC4CBC E5AE3E49 0AF79419 0BEF34BC
    5DCEB4E2 FF2978CB C34D5AEE ED1DFB58 C7BF6592 61C1AD25 3EF87205 15EA58C2
    0A5E2B15 7F08FAEA 5DA2BFA7 95E56C60 22C229C7 024A91D7 A4FEB50B 5425357F
    02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
    23041830 168014FC 2FE6CF0E E0380A40 11381459 5D596E3E A684DA30 1D060355
    1D0E0416 0414FC2F E6CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
    4886F70D 01010505 00038181 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
    A8B174BC A46EB56A 857166C3 B9FD71DF 7264F5AF DC804A67 16BD35A2 4F39AFD7
    0BD24F71 BAF916AC E984343C A54B7395 E5D15237 8897D436 A150BFB2 DC23E8D3
    AFF0A51C B6253153 C4E2C022 66F1E361 B2EE49E2 763FCBC7 6381E7F7 61B6E14D

```

```

60CDF947 2C044617 37211E5F CE
quit
username <REMOVED> privilege 15 password 7 <REMOVED>
!
class-map match-all _class_Voice0
match ip dscp cs3
class-map match-all _class_Voice1
match ip dscp af41
class-map match-all _class_Voice2
match ip dscp cs4
class-map match-all _class_Voice3
match ip dscp ef
!
policy-map Voice
class _class_Voice0
set cos 4
class _class_Voice1
set cos 5
class _class_Voice2
set cos 5
class _class_Voice3
set cos 6
policy-map Data
class class-default
set cos 0
!
bridge irb
!
interface Dot11Radio0
no ip address
shutdown
antenna gain 0
traffic-metrics aggregate-report
stbc
mbssid
speed basic-12.0 18.0 24.0 36.0 48.0 54.0 m1. M2. M3. M4. M5. M6. M7. M8. M9. M10. M11. M12.
M13. M14. M15. M16. M17. M18. M19. M20. M21. M22. M23.
Power client local
channel 2412
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
!
encryption vlan 2 mode ciphers aes-ccm
!

```

```

encryption vlan 3 mode ciphers aes-ccm
!
ssid data
!
ssid voice
!
antenna gain 0
peakdetect
dfs band 3 block
stbc
mbssid
speed basic-12.0 18.0 24.0 36.0 48.0 54.0 m0. M1. M2. M3. M4. M5. M6. M7. M8. M9. M10. M11.
M12. M13. M14. M15. M16. M17. M18. M19. M20. M21. M22. M23. A1ss9 a2ss8 a3ss9
power client local
channel width 40-below
channel 5180
station-role root
dot11 dot11r pre-authentication over-air
dot11 dot11r reassociation-time value 1000
dot11 qos class voice local
  admission-control
  admit-traffic narrowband max-channel 75 roam-channel 6
!
dot11 qos class voice cell
  admission-control
!
world-mode dot11d country-code US both
!
interface Dot11Radio1.2
encapsulation dot1Q 2
bridge-group 2
bridge-group 2 subscriber-loop-control
bridge-group 2 spanning-disabled
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
service-policy input Data
service-policy output Data
!
interface Dot11Radio1.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 subscriber-loop-control
bridge-group 3 spanning-disabled
bridge-group 3 block-unknown-source
no bridge-group 3 source-learning
no bridge-group 3 unicast-flooding
service-policy input Voice
!
interface Dot11Radio1.10
encapsulation dot1Q 10 native
bridge-group 1

```

```

bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0.2
encapsulation dot1Q 2
bridge-group 2
bridge-group 2 spanning-disabled
no bridge-group 2 source-learning
service-policy input Data
service-policy output Data
!
interface GigabitEthernet0.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 spanning-disabled
no bridge-group 3 source-learning
service-policy input Voice
!
interface GigabitEthernet0.10
encapsulation dot1Q 10 native
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
mac-address 18e7.281b.3f54
ip address 10.9.0.9 255.255.255.0
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip default-gateway 10.9.0.2
ip forward-protocol nd
no ip http server
ip http authentication aaa
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
nas 10.9.0.9 key 7 <REMOVED>
user wds nthash 7 <REMOVED>
!
radius-server attribute 32 include-in-access-req format %h

```

```

!
radius server 10.0.0.20
  address ipv4 10.0.0.20 auth-port 1812 acct-port 1813
  key 7 <REMOVED>
!
radius server 10.9.0.9
  address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
  key 7 <REMOVED>
!
access-list 111 permit tcp any any neq telnet
bridge 1 route ip
!
wlccp ap username wds password 7 <REMOVED>
wlccp ap wds ip address 10.9.0.9
wlccp authentication-server infrastructure method_WDS
wlccp authentication-server client eap method_Clients
wlccp authentication-server client leap method_Clients
wlccp wds priority 255 interface BVI1
!
line con 0
  access-class 111 in
line vty 0 4
  access-class 111 in
  transport input all
!
ntp server 10.0.0.2
ntp broadcast client
end

```

Cisco Meraki アクセス ポイント

Cisco Meraki 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。

- [WPA2-Enterprise] または [事前共有キー (Pre-shared key)] で [802.11r] を有効にします。
- [スプラッシュページ (Splash page)] を [なし (None)] に設定します。
- [ブリッジモード (Bridge mode)] を有効にします。
- [VLAN タギング (VLAN tagging)] を有効にします。
- [帯域選択 (Band selection)] を [5 GHz 帯域のみ (5 GHz band only)] に設定します。
- 必要に応じて [データレート (Data Rates)] を設定します
- [Quality of Service (QoS)] を設定します。

ワイヤレス ネットワークの作成

Cisco Meraki アクセス ポイントを追加して WLAN サービスを提供する前に、ワイヤレス ネットワークを作成する必要があります。

ドロップダウンメニューから **[新規ネットワークの作成 (Create a new network)]** を選択します。

ネットワークタイプで **[ワイヤレス (Wireless)]** を選択し、**[作成 (Create)]** をクリックします。

The screenshot shows the Cisco Meraki dashboard interface for creating a new network. On the left is a dark sidebar with the Meraki logo and navigation menu items: NETWORK, Meraki MX64, Network-wide, Security & SD-WAN, and Organization. The main content area has a search bar at the top. Below it, the 'Create network' section is active, showing 'Setup network' instructions. The form includes: 'Network name' (Scranton Branch Office), 'Network type' (Wireless), and 'Network configuration' (Default Meraki configuration). Below the configuration options is a 'Select devices from inventory' section with a message 'You have no unused devices' and buttons for 'Add devices' and 'Go to inventory'. A 'Create network' button is located at the bottom right of the form area.

Cisco Meraki アクセス ポイントは、シリアル番号または注文番号を指定して要求できます。

要求した Cisco Meraki アクセス ポイントは、使用可能なインベントリに表示されます。

Cisco Meraki アクセスポイントは、**[ネットワークの作成 (Create network)]** または **[組織 (Organization)]** > **[設定 (Configure)]** > **[インベントリ (Inventory)]** ページで **[デバイスの追加 (Add Devices)]** を選択して要求できます。

また、[ワイヤレス (Wireless)] > [モニター (Monitor)] > [アクセスポイント (Access points)] ページで [AP の追加 (Add AP)] を選択し、[要求 (Claim)] を選択して要求することもできます。

Claim by serial and/or order number

Enter one or more serial/order numbers (one per row). [Where can I find these numbers?](#)

Close

Claim

要求した Cisco Meraki アクセスポイントは、[組織 (Organization)] > [設定 (Configure)] > [インベントリ (Inventory)] ページで対象ワイヤレスネットワークに追加できます。

Search Dashboard

Inventory

View used and unused devices in your organization. You can [claim](#) new devices to add the list below.

Add to ... Unclaim Unused Used Both Search inventory

Existing network

Meraki WLAN

New network

Add to existing

	Model ^	Claimed on
9K7	MR53	4/29/2020 2:59 PM

要求したアクセスポイントは、[ワイヤレス (Wireless)] > [モニター (Monitor)] > [アクセスポイント (Access points)] ページで [AP の追加 (Add AP)] を選択して追加することもできます。

Q Search Dashboard

Add access points

Add access points from your organization's inventory. When you claim an order by order number, the devices in the order will be added to your inventory. When you claim a device by its serial number, that device will be added to your inventory. Once in your inventory, you can add devices to your network(s).

Search inventory

<input checked="" type="checkbox"/>	MAC address	Serial number	Model ^A	Claimed on
<input checked="" type="checkbox"/>	88:15:44:60:18:8c	Q2MD-MWQS-J9K7	MR53	4/29/2020 2:59 PM

[Add access points](#)

SSID の設定

SSID を作成するには、ドロップダウン メニューから対象ネットワークを選択し、**[ワイヤレス (Wireless)] > [設定 (Configure)] > [SSID (SSIDs)]** を選択します。

Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。データクライアントやその他のタイプのクライアントは、それぞれ異なる SSID と VLAN を使用する必要があります。

ただし、音声対応 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 がある場合は、その WLAN を使用できます。

SSID 名を設定するには、**[名前の変更 (Rename)]** を選択します。

SSID を有効にするには、ドロップダウンメニューから **[有効 (Enabled)]** を選択します。

Q Search Dashboard

Configuration overview

SSIDs Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)

meraki-voice	
Enabled	enabled <input type="button" value="v"/>
Name	rename
Access control	edit settings
Encryption	802.1X with Meraki RADIUS
Sign-on method	None
Bandwidth limit	unlimited
Client IP assignment	Local LAN
Clients blocked from using LAN	no
Wired clients are part of Wi-Fi network	no
VLAN tag ⓘ	3
VPN	Disabled
Splash page	
Splash page enabled	no
Splash theme	n/a

[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (Access control)] ページで、[WPA2-Enterprise] を選択して 802.1x 認証を有効にします。

[WPA2-Enterprise] を選択する際には、Cisco Meraki 認証サーバや外部の RADIUS サーバを使用できます。Cisco Meraki 認証サーバは PEAP 認証をサポートします。PEAP 認証では有効なメールアドレスが必要です。他の認証タイプ（事前共有キーなど）も使用できます。

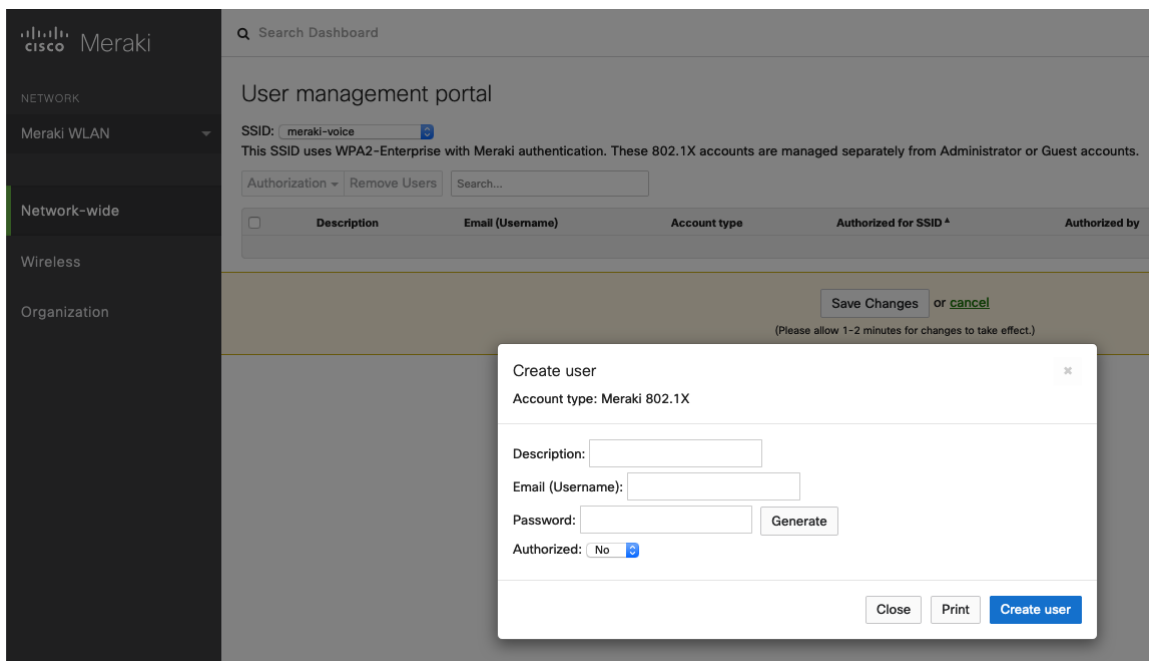
[802.11r] が有効になっていることを確認します。

[スプラッシュページ (Splash page)] が [なし (None)] に設定されていて、ダイレクトアクセスが有効になっていることを確認します。

The screenshot shows the Cisco Meraki dashboard interface. On the left is a dark sidebar with the Meraki logo and navigation menu items: NETWORK, Meraki WLAN, Network-wide, Wireless (highlighted), and Organization. The main content area is titled 'Access control' and includes a search bar at the top. Below the title, the SSID is set to 'meraki-voice'. The 'Network access' section contains 'Association requirements' with four radio button options: 'Open (no encryption)', 'Pre-shared key (PSK)', 'MAC-based access control (no encryption)', and 'Enterprise with Meraki Cloud Authentication' (which is selected). Below this is the 'WPA encryption mode' set to 'WPA2 only', '802.11r' set to 'Enabled', and '802.11w' set to 'Disabled'. The 'Splash page' section has 'None (direct access)' selected.

注：Cisco Meraki アクセスポイントは、802.11r (FT) による高速セキュアローミングをサポートしますが、Cisco Centralized Key Management (CCKM) はサポートしません。

[WPA2-Enterprise] が有効になっている環境で Cisco Meraki 認証サーバを RADIUS サーバとして使用する場合は、**[ネットワーク全体 (Network-wide)] > [設定 (Configure)] > [ユーザー (Users)]** ページでユーザーアカウントを作成し、Cisco Wireless Phone 840 および 860 が 802.1x 認証に認証サーバを使用するように設定する必要があります。



[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (Access control)] ページで、[ブリッジモード (Bridge mode)] を有効にすることを推奨します。この場合、Cisco Wireless Phone 840 および 860 は、コール制御やその他のエンドポイントがクラウドベースでない限り、ネットワークではなくローカルの LAN から DHCP を取得します。

[ブリッジモード (Bridge mode)] を有効にすると、VLAN タギングオプションが使用できるようになります。

SSID の [VLAN タギング (VLAN tagging)] を有効にすることを推奨します。

VLAN タギングを使用する場合は、VLAN を許可するトランク モードに設定されたスイッチ ポートに、Cisco Meraki アクセス ポイントが接続されることを確認します。

Cisco Meraki MS スイッチを使用する場合は、『Cisco Meraki MS Switch VoIP 導入ガイド』を参照してください。

https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf [英語]

Cisco IOS スイッチを使用する場合は、Cisco Meraki アクセス ポイントが接続するスイッチ ポートを次のように構成して、802.1q トランキングを有効にします。

```
Interface GigabitEthernet X
  switchport trunk encapsulation dot1q
  switchport mode trunk
  mls qos trust dscp
```

The screenshot shows the Meraki configuration interface for 'Addressing and traffic'. The left sidebar includes 'Meraki WLAN', 'Network-wide', 'Wireless', and 'Organization'. The main content area is titled 'Addressing and traffic' and contains the following sections:

- Client IP assignment:**
 - NAT mode: Use Meraki DHCP. Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.
 - Bridge mode: Make clients part of the LAN. Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras.
 - Layer 3 roaming. Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client roams to an AP where their original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.
 - Layer 3 roaming with a concentrator. Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
 - VPN: tunnel data to a concentrator. Meraki devices send traffic over a secure tunnel to an MX concentrator.
- VLAN tagging:** Use VLAN tagging. (Bridge mode and layer 3 roaming only)
- VLAN ID:**

AP tags	VLAN ID	Actions
All other APs	3	Add VLAN
- Content filtering:** Don't filter content. (NAT mode only)
- Bonjour forwarding:** Enable Bonjour Gateway. (Bridge mode and layer 3 roaming only). There are no Bonjour forwarding rules on this network. [Add a Bonjour forwarding rule](#).

[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (Access control)] ページでは、必要に応じて Cisco Wireless Phone 840 および 860 で使用する SSID の周波数帯域を設定できます。

Cisco Wireless Phone 840 および 860 は、**5 GHz 帯域のみ**での動作を推奨します。5 GHz 帯域で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。

距離が離れているために 2.4 GHz 帯域を使用する必要がある場合は、**[デュアルバンド運用 (2.4 GHz および 5 GHz) (Dual band operation (2.4 GHz and 5 GHz))]** を選択する必要があります。**[バンドステアリングを使用するデュアルバンド運用 (Dual band operation with Band Steering)]** オプションは使用しないでください。

従来の 2.4 GHz クライアントがワイヤレス LAN に接続できるようにする必要がある場合を除き、12 Mbps 未満のデータ レートは無効することを推奨します。

Cisco Meraki アクセスポイントは現在、DTIM 周期「1」、ビーコン周期「100 ミリ秒」を使用します。どちらも設定を変更することはできません。

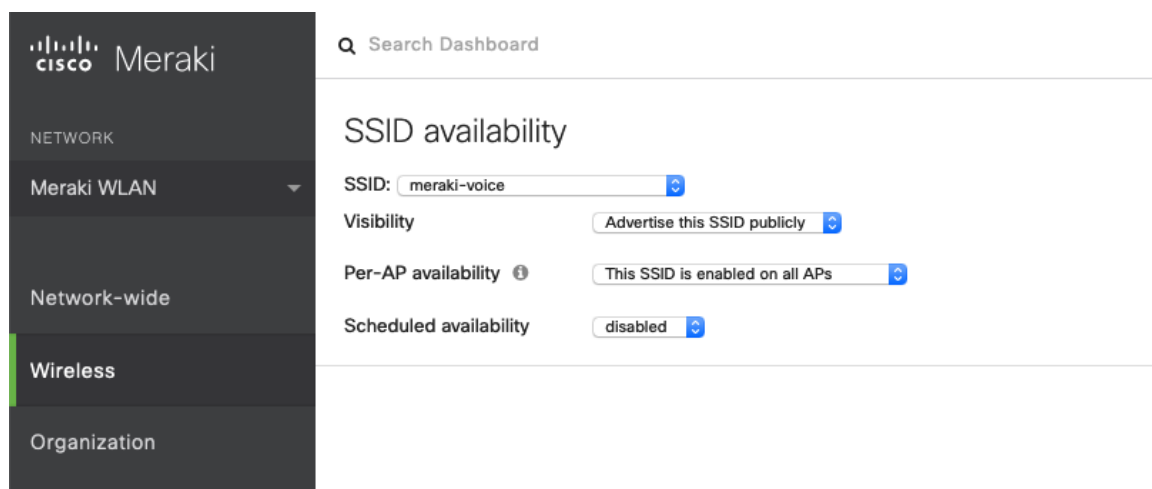
The screenshot shows the Meraki configuration interface for 'Wireless options'. The left sidebar includes 'Meraki WLAN', 'Network-wide', 'Wireless', and 'Organization'. The main content area is titled 'Wireless options' and contains the following sections:

- Band selection:**
 - Dual band operation (2.4 GHz and 5 GHz)
 - 5 GHz band only. 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.
 - Dual band operation with Band Steering. Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.
- Minimum bitrate (Mbps):** A slider ranging from 1 to 54 Mbps. The current setting is 12 Mbps. A yellow banner below the slider states: **802.11b devices not supported**.

[ワイヤレス (Wireless)] > [設定 (Configure)] > [SSID の可用性 (SSID availability)] ページでは、[可視性 (Visibility)] を [この SSID をパブリックにアドバタイズする (Advertise this SSID publicly)] に設定することで SSID をブローキャストできます。

[AP ごとの可用性 (Per-AP Availability)] は [この SSID をすべての AP で有効にする (This SSID is enabled on all APs)] に設定することを推奨します。

必要に応じて SSID の可用性をスケジュール設定できますが、[スケジュールされた可用性 (Scheduled Availability)] は [無効 (Disabled)] に設定することを推奨します。



無線の設定

[ワイヤレス (Wireless)] > [構成 (Configure)] > [無線設定 (Radio settings)] ページで、アクセスポイントを一括または個別に構成して、自動または手動のチャンネルと送信電力設定を定義できます。

Cisco Meraki アクセスポイントを使用する場合は、チャンネルおよび送信電力に [自動 (Auto)] を選択し、RF プロファイルで定義されているものを利用することを推奨します。

ただし、個々のアクセスポイントの 5 GHz または 2.4 GHz 無線のいずれかに、チャンネルと送信電力を静的に設定できます。これは、エリアに断続的な干渉源が存在する場合に必要なことがあります。一方で、他のアクセスポイントで [自動 (Auto)] を有効にし、静的チャンネルが割り当てられているチャンネルを回避できます。

Meraki Search Dashboard

Radio settings

Overview RF profiles

BAND: 5 CHANNEL: All AP TAG: MR53 RF PROFILE: All REGULATORY DOMAIN: FCC Edit

Search by AP name... Update auto channels Edit settings...

<input checked="" type="checkbox"/>	Status	AP name	Channel	Ch. Width (MHz)	Target power (dBm)	Transmit power (dBm)	RF Profile
<input checked="" type="checkbox"/>		MR53	36 (Auto)	20	8 - 30	8	Basic Indoor Profile

標準の **[基本屋内プロファイル (Basic Indoor Profile)]** を変更するか、**[バンド選択 (Band selection)]** を **[SSID ごと (Per SSID)]** に設定し、**[クライアントバランシング (Client balancing)]** を **[オフ (Off)]** に設定して新しい RF プロファイルを作成することをお勧めします。

Meraki Search Dashboard

RF PROFILES

Edit Basic Indoor Profile

General 2.4 GHz 5 GHz

General

Band selection

Per AP Per SSID

The Access Points configured to use this profile will follow the band selection set on the [Access Control page](#) for the respective SSID.

Minimum bitrate configuration

Per band
Set the minimum bitrates for the 2.4 & 5 GHz radios separately below.

Per SSID
The Access Points configured to use this profile will follow the minimum bitrate selection set on the [Access Control page](#) for the respective SSID. Per SSID minimum bitrate selection will be moved to RF profiles at a later date.

Client balancing

On Off

Client Balancing uses information about the state of the network and wireless client probes to steer the client to the best available access point during association. Read more about client balancing [here](#).

RF プロファイルでは、5 GHz 無線の **[チャンネル幅 (Channel width)]** は、20 MHz、40 MHz、または 80 MHz チャンネルを使用するように設定できます。

2.4 GHz 無線は 20 MHz チャンネルを使用し、他のチャンネル幅に設定することはできません。

すべてのアクセス ポイントで同じチャンネル幅を使用することを推奨します。

[AutoChannel] で使用される 5 GHz チャンネルも RF プロファイルで設定できます。

[AutoChannel] で使用される 2.4 GHz チャンネルは、チャンネル 1、6、および 11 のみに制限されています。

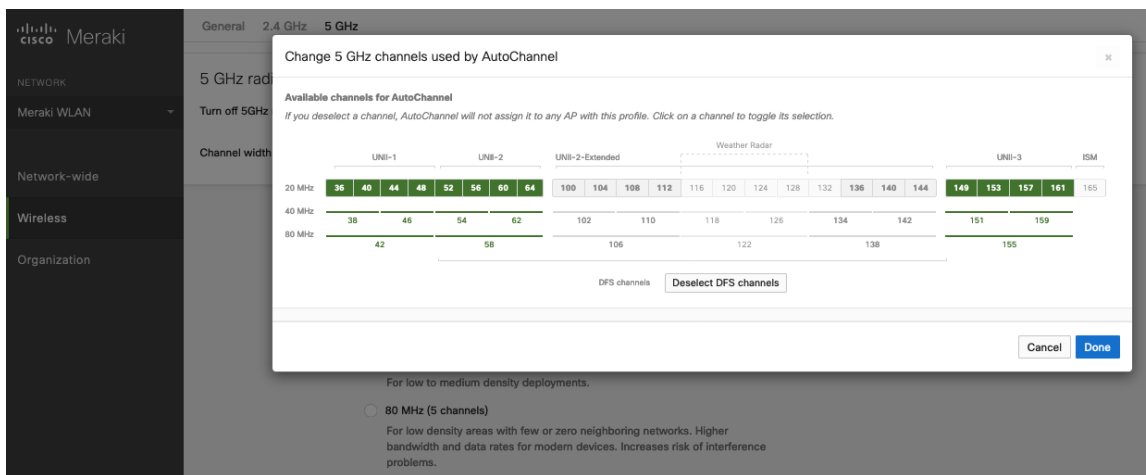
[無線送信電力範囲 (Radio transmit power range)] も RF プロファイルで設定されます。

[最小ビットレート構成 (Minimum bitrate configuration)] が [バンドごと (Per band)] に設定されている場合、SSID 構成で定義されている内容が上書きされます。

従来の 2.4 GHz クライアントがワイヤレス LAN に接続できるようにする必要がある場合を除き、12 Mbps 未満のデータレートは無効することを推奨します。

The screenshot displays the Cisco Meraki configuration interface for 5 GHz radio settings. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled '5 GHz radio settings' and includes the following sections:

- General:** 'Turn off 5GHz radio' (checked) and 'See band selection above.'
- Channel width:** 'Auto' and 'Manual' buttons, with 'Manual' selected.
- Manual 5 GHz channel width:** A section to 'Disable auto channel width by manually selecting a channel width for the APs in this profile.' It offers three radio button options:
 - 20 MHz (19 channels): Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.
 - 40 MHz (10 channels): For low to medium density deployments.
 - 80 MHz (5 channels): For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.
- Channel assignment method:** 'AutoChannel will assign radios to channels with low interference.' A link to 'Change channels used by AutoChannel...' is provided.
- Radio transmit power range (dBm):** A slider ranging from 2 to 30 dBm, with 'Transmit shorter distance' on the left and 'Transmit farther' on the right. The slider is currently set to 8 dBm.
- Set RX-SOP...** (link)
- Minimum bitrate:** A slider ranging from 6 to 54 Mbps, with 'Lower Density' on the left and 'Higher Density' on the right. The slider is currently set to 12 Mbps.



注：Cisco Meraki アクセス ポイントでは、ダイナミック伝送パワーコントロール（DTPC）がサポートされません。そのため、Cisco Wireless Phone 840 および 860 は、現在のチャンネルとデータレートでサポートされる最大送信電力を使用します。

ファイアウォール & トラフィック シェーピング

[ワイヤレス (Wireless)] > [設定 (Configure)] > [ファイアウォールとトラフィックシェーピング (Firewall & traffic shaping)] ページでは、トラフィック シェーピング ルールを定義できます。

ワイヤレスクライアントのローカル LAN アクセスを許可するように、[レイヤ 3 ファイアウォールルール (Layer 3 firewall rule)] が構成されていることを確認します。

トラフィック シェーピング ルールを定義できるようにするには、[トラフィックのシェープ (Shape traffic)] ドロップダウンメニューで [この SSID のトラフィックをシェープ (Shape traffic on this SSID)] を選択します。

[この SSID のトラフィックをシェープ (Shape traffic on this SSID)] を適用した後、[新しいルールを作成 (Create a new rule)] を選択して [トラフィック シェーピング ルール (Traffic shaping rules)] を定義します。

Cisco Meraki アクセス ポイントのデフォルトでは、DSCP EF (46) とマークされた音声フレームに WMM UP 6 ではなく WMM UP 5 のタグを、DSCP CS3 (24) とマークされたコール制御フレームに WMM UP 4 ではなく WMM UP 3 のタグを付けます。

Meraki

NETWORK

Meraki WLAN

Network-wide

Wireless

Organization

Search Dashboard

Firewall & traffic shaping

SSID: meraki-voice

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
	Allow	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules: There are no rules defined for this SSID.
[Add a layer 7 firewall rule](#)

Traffic shaping rules

Per-client bandwidth limit: unlimited [details](#) Enable SpeedBurst

Per-SSID bandwidth limit: unlimited [details](#)

Shape traffic: Shape traffic on this SSID

注：Cisco Meraki アクセスポイントでは、コールアドミッション制御/トラフィック仕様（TSPEC）をサポートしません。

Cisco Call Control の設定

Cisco Unified Communications Manager

Cisco Unified Communications Manager は、さまざまな電話機機能、発呼機能、およびセキュリティ機能を提供します。

デバイスの有効化

Cisco Unified Communications Manager で Cisco Wireless Phone 840 または 860 のデバイスタイプを有効にするには、対応するデバイスインネブラ (QED) の COP ファイルを、各 Cisco Unified Communications Manager サーバーの Cisco Unified Operating System Administration Web ページからインストールする必要があります。

デバイスインネブラ (QED) の COP ファイルのインストール後に、各 Cisco Unified Communication Manager ノードを再起動する必要がない場合があります。

Cisco Unified Communications Manager のバージョンに応じて、次を実行します。

11.5(1)SU4 以降

- すべての Cisco Unified Communications Manager ノードをリブートします。

11.5(1)SU5 以降または 12.5(1) 以降

- すべての Cisco Unified Communications Manager ノードで Cisco Tomcat サービスを再起動します。
- パブリッシャノードで Cisco CallManager サービスを実行している場合は、パブリッシャノードでのみサービスを再起動します。

注：サブスライバノードの Cisco CallManager サービスを再起動する必要はありません。

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 オペレーティングシステム アドミニストレーション ガイド**』を参照してください。

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

Cisco Wireless Phone 840 または 860 を Cisco Unified Communications Manager に追加する場合は、Wi-Fi MAC アドレスを使用してプロビジョニングする必要があります。

Cisco Wireless Phone 840 または 860 の Wi-Fi MAC アドレスは、**[設定 (Settings)] > [電話について (About phone)] > [Wi-Fi MAC アドレス (Wi-Fi MAC address)]** の順に選択して確認できます。

1.3(0) リリースの時点で、Cisco Wireless Phone 840 および 860 は、複数回線 (最大 6)、共有回線、およびプライバシーをサポートしています。

Cisco Wireless Phone 840 および 860 は自動登録をサポートしていません。

Device Information	
<input checked="" type="checkbox"/> Device is trusted	
MAC Address*	<input type="text"/>
Description	<input type="text"/>
Device Pool*	-- Not Selected -- View Details
Common Device Configuration	< None > View Details
Phone Button Template*	-- Not Selected --
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile View Details

注：Cisco Wireless Phone 840 および 860 は、直接コールにはコーリングサーチスペースを使用し、転送には再ルーティング コーリング サーチ スペースを使用するため、両方のオプションが正しく設定されていることを確認します。

Cisco Unified Communications Manager サーバーのホスト名と関連する証明書は、完全修飾ドメイン名 (FQDN) または IP アドレスを使用して一致する必要があります。

製造元の認証局 (CA) 証明書

Cisco Wireless Phone 840 および 860 には、新しい製造元の認証局 (CA) が使用されています。

新しいルート証明書と中間証明書が Cisco Unified Communications Manager にネイティブに含まれるまで、新しい製造元でインストールされた証明書 (MIC) を信頼するには、ルート証明書と中間証明書を証明書チェーンに手動で追加する追加の手順が必要です。

1. 外部で入手可能な Cisco PKI Web サイトから、不足しているルート証明書と中間証明書をダウンロードします。

<https://www.cisco.com/security/pki>

新しい MIC のルートを含む、信頼チェーンを完了するために不足している証明書は次のとおりです。

- [Cisco Manufacturing CA III \(cmca3\)](http://www.cisco.com/security/pki/certs/cmca3.pem) — 中間
- [Cisco Basic Assurance Root CA 2099 \(cbarc2099\)](http://www.cisco.com/security/pki/certs/cbarc2099.pem) — Cisco Manufacturing CA III のルート

2. Web ブラウザで、**Cisco Unified Operating System Administration** Web ページにログインします。
3. **[セキュリティ (Security)]** メニューで、**[証明書管理 (Certificate Management)]** を選択します。

4. **[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)]** を選択します。
5. **[証明書の目的 (Certificate Purpose)]** に対して **CallManager-trust** を選択し、証明書を参照し、**[アップロード (Upload)]** を選択します。

注：証明書は他のすべての Cisco Unified Communication Manager ノードに複製されるため、Cisco Unified Communication Manager パブリッシャのすべての証明書に対してこの手順を繰り返します。

6. **[証明書の目的 (Certificate Purpose)]** に対して **CAPF-trust** を選択し、証明書を参照し、**[アップロード (Upload)]** を選択します。

注：証明書は他のすべての Cisco Unified Communication Manager ノードに自動的に複製されないため、すべての Cisco Unified Communication Manager ノードのすべての証明書に対してこの手順を繰り返します。

[デバイスプール (Device Pools)]

Cisco Wireless Phone 840 または 860 を作成する場合は、**デバイスプール**を設定する必要があります。

デバイス プールでは、共通の設定 (Cisco Unified Communications Manager など)、ローミングに関連する設定 (日付/時刻グループ、地域など)、ローカル ルート グループ設定、デバイス モビリティに関連する情報の設定、およびその他のグループ設定を定義します。

デバイス プールを使用すると、デバイスを場所別、モデル タイプ別などにグループ化できます。

Device Pool Settings	
Device Pool Name*	Default
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >

Roaming Sensitive Settings	
Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	< None >
Location	< None >
Network Locale	< None >
SRST Reference*	Disable
Connection Monitor Duration***	
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	< None >
Device Mobility Group	< None >
Wireless LAN Profile Group	< None > View Details

電話ボタン テンプレート

新しい Cisco Wireless Phone 840 または 860 を作成する場合は、**電話ボタン テンプレート**を設定する必要があります。

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。

The image shows two screenshots of the Cisco configuration interface for Phone Button Template Information. The top screenshot is for 'Cisco 840' and the bottom is for 'Cisco 860'. Both show a table with 6 buttons and a dropdown menu for feature selection.

Button	Feature	Label
1	Line **	Line
2	Line	Line
3	Privacy	None
4	None	None
5	None	None
6	None	None

Buttons: Save, Delete, Copy, Reset, Apply Config, Add New

セキュリティ プロファイル

Cisco Wireless Phone 840 または 860 を作成する場合は、**デバイス セキュリティ プロファイル**を設定する必要があります。

セキュリティ プロファイルを使用すると、認証モードや暗号化モードを有効にできます。暗号化モードを有効にすると、シグナリング、メディア、および設定ファイルの暗号化が有効になります。

セキュリティ プロファイルで Locally Signed Certificate (LSC) を使用するには、認証局プロキシ機能 (CAPF) が動作している必要があります。

Cisco Wireless Phone 840 および 860 には、製造元でインストールされる証明書 (MIC) を備えています。この証明書もセキュリティプロファイルから使用できます。

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

SRTP Allowed - When this flag is checked, IPSec needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

BLF Presence Group*

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

Media Termination Point Required

Unattended Port

Require DTMF Reception

Early Offer support for voice and video calls (insert MTP if needed)

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

SRTP Allowed - When this flag is checked, IPSec needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

BLF Presence Group*

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

Media Termination Point Required

Unattended Port

Require DTMF Reception

Early Offer support for voice and video calls (insert MTP if needed)

デフォルトのデバイス セキュリティ プロファイルは、暗号化を使用しない、**Standard SIP Non-Secure Profile** です。

Phone Security Profile Information

Product Type: Cisco 840
Device Protocol: SIP
Name* Cisco 840 - Standard SIP Non-Secure Profile
Description Cisco 840 - Standard SIP Non-Secure Profile
Nonce Validity Time* 600
Device Security Mode Non Secure
Transport Type* TCP+UDP
 Enable Digest Authentication
 TFTP Encrypted Config

Phone Security Profile CAPF Information

Authentication Mode* By Null String
Key Order* RSA Only
RSA Key Size (Bits)* 2048
EC Key Size (Bits) < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5060

Phone Security Profile Information

Product Type: Cisco 860
Device Protocol: SIP
Name* Cisco 860 - Standard SIP Non-Secure Profile
Description Cisco 860 - Standard SIP Non-Secure Profile
Nonce Validity Time* 600
Device Security Mode Non Secure
Transport Type* TCP+UDP
 Enable Digest Authentication
 TFTP Encrypted Config

Phone Security Profile CAPF Information

Authentication Mode* By Null String
Key Order* RSA Only
RSA Key Size (Bits)* 2048
EC Key Size (Bits) < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5060

注：UDP はサポートされていないため、トランスポートタイプは TCP + UDP または TCP に設定する必要があります。

SIP プロファイル

Cisco Wireless Phone 840 または 860 を作成する場合は、**SIP プロファイル**を設定する必要があります。

Cisco Wireless Phone 840 および 860 のカスタム SIP プロファイルを作成することを推奨します（モバイルデバイスの**標準 SIP プロファイル**または**標準 SIP プロファイル**を使用しないでください）。

Protocol Specific Information
Packet Capture Mode*
Packet Capture Duration
 SRTP Allowed - When this flag is checked, IPSec needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
BLF Presence Group*
MTP Preferred Originating Codec*
Device Security Profile*
Rerouting Calling Search Space
SUBSCRIBE Calling Search Space
SIP Profile* [View Details](#)
Digest User
 Media Termination Point Required
 Unattended Port
 Require DTMF Reception
 Early Offer support for voice and video calls (insert MTP if needed)

Cisco Wireless Phone 840 および 860 の SIP プロファイルを作成するには、**標準 SIP プロファイル**を参照テンプレートとして使用します。

標準 SIP プロファイルをコピーし、次のパラメータを変更します。

[レジスタの再送間隔の調整値 (秒) (Timer Register Delta (seconds))] :

30 (デフォルトは 5) に設定。

[キープアライブのタイムアウト値 (秒) (Timer Keep Alive Expires (seconds))] :

300 (デフォルトは 120) に設定。

[サブスクライブのタイムアウト値 (秒) (Timer Subscribe Expires (seconds))] :

300 (デフォルトは 120) に設定。

[サブスクライブの再送間隔の調整値 (秒) (Timer Subscribe Delta (seconds))] :

15 (デフォルトは 5) に設定。

[システム (System)] > [Service Parameters (サービスパラメータ)] > [Cisco CallManager] で SIP ステーションのキープアライブインターバルが 120 秒間設定されたままになっていることを確認します。

カスタム SIP プロファイルの例

SIP Profile Information	
Name*	Custom 860 SIP Profile
Description	Custom 860 SIP Profile
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
User-Agent and Server header information*	Send Unified CM Version Information as User-Agent
Version in User Agent and Server Header*	Major And Minor
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, ar
Confidential Access Level Headers*	Disabled
<input type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Offer valid IP and Send/Receive mode only for T.38 Fax Relay	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
<input type="checkbox"/> Assured Services SIP conformance	
<input type="checkbox"/> Enable External QoS**	
SDP Information	
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
SDP Transparency Profile	Pass all unknown SDP attributes
Accept Audio Codec Preferences in Received Offer*	Default
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Allow RR/RS bandwidth modifier (RFC 3556)	
Parameters used in Phone	
Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	30
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Media Port Ranges	<input checked="" type="radio"/> Common Port Range for Audio and Video <input type="radio"/> Separate Port Ranges for Audio and Video
Start Media Port*	16384

Stop Media Port*	<input type="text" value="32766"/>
DSCP for Audio Calls	<input type="text" value="Use System Default"/> ▾
DSCP for Video Calls	<input type="text" value="Use System Default"/> ▾
DSCP for Audio Portion of Video Calls	<input type="text" value="Use System Default"/> ▾
DSCP for TelePresence Calls	<input type="text" value="Use System Default"/> ▾
DSCP for Audio Portion of TelePresence Calls	<input type="text" value="Use System Default"/> ▾
Call Pickup URI*	<input type="text" value="x-cisco-serviceuri-pickup"/>
Call Pickup Group Other URI*	<input type="text" value="x-cisco-serviceuri-opickup"/>
Call Pickup Group URI*	<input type="text" value="x-cisco-serviceuri-gpickup"/>
Meet Me Service URI*	<input type="text" value="x-cisco-serviceuri-meetme"/>
User Info*	<input type="text" value="None"/> ▾
DTMF DB Level*	<input type="text" value="Nominal"/> ▾
Call Hold Ring Back*	<input type="text" value="Off"/> ▾
Anonymous Call Block*	<input type="text" value="Off"/> ▾
Caller ID Blocking*	<input type="text" value="Off"/> ▾
Do Not Disturb Control*	<input type="text" value="User"/> ▾
Telnet Level for 7940 and 7960*	<input type="text" value="Disabled"/> ▾
Resource Priority Namespace	<input type="text" value="< None >"/> ▾
Timer Keep Alive Expires (seconds)*	<input type="text" value="300"/>
Timer Subscribe Expires (seconds)*	<input type="text" value="300"/>
Timer Subscribe Delta (seconds)*	<input type="text" value="15"/>
Maximum Redirections*	<input type="text" value="70"/>
Off Hook To First Digit Timer (milliseconds)*	<input type="text" value="15000"/>
Call Forward URI*	<input type="text" value="x-cisco-serviceuri-cfwdall"/>
Speed Dial (Abbreviated Dial) URI*	<input type="text" value="x-cisco-serviceuri-abbrdial"/>

Conference Join Enabled
 RFC 2543 Hold
 Semi Attended Transfer
 Enable VAD
 Stutter Message Waiting
 MLPP User Authorization

Normalization Script

Normalization Script ▾

<input type="checkbox"/> Enable Trace	
Parameter Name	Parameter Value
1	<input type="text"/> <input type="text"/> <input type="button" value="+"/> <input type="button" value="-"/>

Incoming Requests FROM URI Settings

Caller ID DN

Caller Name

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*

Resource Priority Namespace List

SIP Rel1XX Options*

Video Call Traffic Class*

Calling Line Identification Presentation*

Session Refresh Method*

Early Offer support for voice and video calls*

Enable ANAT

Deliver Conference Bridge Identifier

Allow Passthrough of Configured Line Device Caller Information

Reject Anonymous Incoming Calls

Reject Anonymous Outgoing Calls

Send ILS Learned Destination Route String

Connect Inbound Call before Playing Queuing Announcement

SIP OPTIONS Ping

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)*

Ping Interval for Out-of-service Trunks (seconds)*

Ping Retry Timer (milliseconds)*

Ping Retry Count*

SDP Information

Send send-receive SDP in mid-call INVITE

Allow Presentation Sharing using BFCP

Allow iX Application Media

Allow multiple codecs in answer SDP

共通設定

Web アクセスなどの一部の設定は、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。

Cisco Wireless Phone 840 および 860 では、**Web アクセス**はデフォルトで無効になっています。

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。

Web Access*

QoS パラメータ

SIP 通信、電話設定、および電話で使用される電話ベースのサービスに使用される DSCP 値は、Cisco Unified Communications Manager のエンタープライズ パラメータで定義されます。

SIP 通信および電話設定の DSCP 値は、デフォルトで CS3 に設定されます。

電話ベースのサービスは、デフォルトでベスト エフォート型トラフィックに設定されます。

Parameter Name	Parameter Value	Suggested Value
Cluster ID *	StandAloneCluster	StandAloneCluster
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
Auto Registration Legacy Mode *	False	False
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	Disabled	Disabled
Services Provisioning *	Internal	Internal
Feature Control Policy	< None >	
Wi-Fi Hotspot Profile	< None >	
IMS Inter Operator Id *	IMS Inter Operator Identification	IMS Inter Operator Identification
URI Lookup Policy *	Case Sensitive	Case Sensitive

G.722 および Opus のアドバタイズメント

Cisco Unified Communications Manager では、G.722 と Opus 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がサポートされています。

G.722 コーデックと Opus コーデックは、**[G.722 および Opus コーデックのアドバタイズ (Advertise G.722 and Opus 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、または個々の電話単位で無効化できます。

Advertise G.722 and OPUS Codecs*

オーディオ ビット レート

オーディオビット レートを設定するには、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。

Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Keep Current Setting	<input checked="" type="radio"/> 64 kbps (G.722, G.711) <input type="radio"/> kbps	<input type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input checked="" type="radio"/> 2000 kbps	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input type="radio"/> kbps

音声通話で使用するオーディオビットレートを設定するには、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
Opus	6 ~ 510 Kbps
G.722/G.711	64 Kbps
G.729	8 Kbps

製品固有の設定オプション

Cisco Unified Communications Manager の管理では、次の Cisco Wireless Phone 840 および 860 向け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。

一部の製品固有の設定オプションは、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。

Cisco Wireless Phone 840 および 860 設定オプション

Product Specific Configuration Layout

?

	Parameter Value	Override Enterprise/Common Phone Profile Settings
Web Access*	Disabled	<input type="checkbox"/>
Web Password	<input type="text"/>	
Reboot immediately after downloading software updates *	Disabled	
Emergency Numbers	<input type="text"/>	
Visual Voicemail Access*	Disabled	
Voicemail Server (Primary)	<input type="text"/>	<input type="checkbox"/>
Voicemail Server (Backup)	<input type="text"/>	<input type="checkbox"/>
Load Server	<input type="text"/>	<input type="checkbox"/>
Advertise G.722 and OPUS Codecs*	Use System Default	
Customer support upload URL	<input type="text"/>	<input type="checkbox"/>
Secondary SIP Server	<input type="text"/>	
Secondary SIP Server Port	<input type="text"/>	
Secondary SIP Transport*	UDP	
Secondary SIP Extension	<input type="text"/>	
Secondary SIP Username	<input type="text"/>	
Secondary SIP Password	<input type="text"/>	
Enterprise Mobility Management (EMM) Alternative Configuration	<input type="text"/>	
Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key	<input type="text"/>	
Recording Tone*	Disabled	
Announce Caller ID*	Disabled	
Mute SIP Registration Notifications*	Enabled	
Line 1 Ringtone	<input type="text"/>	
Line 2 Ringtone	<input type="text"/>	
Line 3 Ringtone	<input type="text"/>	
Line 4 Ringtone	<input type="text"/>	
Line 5 Ringtone	<input type="text"/>	
Line 6 Ringtone	<input type="text"/>	
Notification Sound	<input type="text"/>	
Alarm Sound	<input type="text"/>	
Wallpaper	<input type="text"/>	

フィールド名	説明
Web アクセス	電話機が Web ブラウザまたは他の HTTP クライアントからの接続を受け入れるかどうかを指定します。電話機の Web サーバ機能を無効にすると、電話機の内部 Web ページへのアクセスがブロックされます。これらのページは、統計情報と設定情報を提供します。
Web パスワード (Web Password)	このパラメータは、電話機の Web インターフェイスにアクセスするためのパスワードを指定します。8 ~ 127 文字のパスワードを入力します。
ソフトウェア アップデートをダウンロードした直後にリブートします。	このパラメータは、ソフトウェアアップデートをダウンロードした直後に電話機を再起動するか、手動で再起動するように電話機がユーザーに通知するかを指定します。ソフトウェアアップデートを適用するには、電話機を再起動する必要があります。

緊急電話番号	このパラメータは、電話機のキーパッドをロック解除せずにダイヤルできる緊急電話番号を指定します。たとえば日本では、電話機をロック解除せずにダイヤルできる緊急電話番号の有力な候補として 110 番が挙げられます。複数の番号を指定するには、カンマを区切り文字として使用します。たとえば、411、511、911 などを緊急電話番号として入力する場合は、フィールドに「411,511,911」とスペースなしで入力します。
ビジュアルボイスメールのアクセス	このパラメータは、ボイスメールへのアクセスを有効または無効にします。
ボイスメールサーバー (プライマリ)	このパラメータには、ビジュアルボイスメールのプライマリ Voicemail サーバーのアドレスが含まれています。
ボイスメールサーバー (バックアップ)	このパラメータには、ビジュアルボイスメールのバックアップ Voicemail サーバーのアドレスが含まれています。
ロード サーバー	電話機が、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ように指定します。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ます、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。
G.722 および Opus コーデックをアドバタイズする	このパラメータは、電話機が G.722 および Opus コーデックをアドバタイズするかどうかを指定します。コーデックのネゴシエーションでは、次の 2 つの手順が実行されます。まず、電話機が、サポートされるコーデックを Cisco Unified CallManager にアドバタイズします (すべてのエンドポイントが同じコーデックのセットをサポートしているわけではありません)。次に、Cisco Unified Communications Manager が、コール試行に関与するすべての電話機でサポートされるコーデックのリストを取得すると、現地のペアリング設定といった各要因を元に、一般にサポートされるコーデックを選択します。オプションは、[システムデフォルトの使用 (Use System Default)] (エンタープライズパラメータの [G.722 コーデックをアドバタイズ (Advertise G.722 Codecs)] で指定されている設定に従う)、[無効 (Disabled)] (G.722 または Opus サポートをアドバタイズしない)、および [有効 (Enabled)] (G.722 および Opus サポートをアドバタイズする) です。

カスタマー サポートのアップロード URL (Customer support upload URL)	この URL は、ユーザーがエンドポイントで「エラー レポート ツール」を実行したときに、問題レポートファイルのアップロードに使用されます。
セカンダリ SIP サーバー	このパラメータには、オプションの 2 番目の登録用のサーバーのアドレスが含まれています。
セカンダリ SIP サーバーポート	このパラメータには、オプションの 2 番目の登録用遠端ポート番号が含まれています。
セカンダリ SIP トランスポート	このパラメータには、オプションの 2 番目の登録用転送タイプが含まれています。
セカンダリ SIP 内線	このパラメータには、オプションの 2 番目の SIP 拡張機能が含まれています。
セカンダリ SIP ユーザー名	このパラメータには、オプションの 2 番目の SIP ユーザー名が含まれています。
セカンダリ SIP パスワード	このパラメータには、オプションの 2 番目の SIP パスワードが含まれています。
エンタープライズモビリティ管理 (EMM) 代替構成	このパラメータは、電話機がエンタープライズモビリティ管理 (EMM) ソリューションによって管理されていない場合に、ネイティブ シスコ アプリケーションを設定するためのファイルを指定します。
エンタープライズモビリティ管理 (EMM) 代替構成暗号化キー	このパラメータは、エンタープライズモビリティ管理 (EMM) 代替構成ファイルの生成に使用される暗号化キーを指定します。
[録音トーン (Recording Tone)]	電話機で録音トーンを有効にするかどうかを設定するために使用できます。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。
発信者番号を通知	このパラメータは、電話機が着信コールの発信者識別情報をアナウンスするかどうかを指定します。
SIP 登録通知のミュート	このパラメータは、SIP 登録イベントの通知をミュートするかどうかを指定します。
回線 1 の着信音	このパラメータは、回線 1 の呼び出し音を指定します。ダウンロードして回線 1 に使用する既存の着信音または着信音ファイルを指定できます。
回線 2 の着信音	このパラメータは、回線 2 の呼び出し音を指定します。ダウンロードして回線 2 に使用する既存の着信音または着信音ファイルを指定できます。

回線 3 の着信音	このパラメータは、回線 3 の呼び出し音を指定します。ダウンロードして回線 3 に使用する既存の着信音または着信音ファイルを指定できます。
回線 4 の着信音	このパラメータは、回線 4 の呼び出し音を指定します。ダウンロードして回線 4 に使用する既存の着信音または着信音ファイルを指定できます。
回線 5 の着信音	このパラメータは、回線 5 の呼び出し音を指定します。ダウンロードして回線 5 に使用する既存の着信音または着信音ファイルを指定できます。
回線 6 の着信音	このパラメータは、回線 6 の呼び出し音を指定します。ダウンロードして回線 6 に使用する既存の着信音または着信音ファイルを指定できます。
通知音	このパラメータは、ダウンロードする通知サウンドファイルを指定します。カンマ区切り形式を使用して複数のファイルを指定できます。ファイルがダウンロードされたら、カスタム設定アプリケーション、Android 設定、またはその他のアプリケーション設定で通知音を設定する必要があります。
アラーム音	このパラメータは、ダウンロードするアラームサウンドファイルを指定します。カンマ区切り形式を使用して複数のファイルを指定できます。ファイルをダウンロードしたら、カスタム設定アプリケーション、Android 設定、またはその他のアプリケーション設定でアラーム音を設定する必要があります。
Wallpaper	このパラメータは、ダウンロードする壁紙ファイルを指定します。カンマ区切り形式を使用して複数のファイルを指定できます。ファイルをダウンロードしたら、カスタム設定アプリケーションまたは Android 設定を使用して、ロック画面の壁紙とホーム画面の壁紙を設定する必要があります。

注：Web パスワードまたはセカンダリ SIP パスワードを長期間有効にしたままにする場合、またはエンタープライズ モビリティ管理 (EMM) 代替設定暗号キー オプションを使用する場合は、TFTP 暗号化が有効になっているセキュア プロファイルを使用する必要があります。

Cisco IP Phone 8861 および 8865 と Cisco Unified Communications Manager で使用される TCP ポートおよび 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。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_5_x/cucm_b_port-usage-cucm-105x/cucm_b_port-usage-cucm-105x_chapter_00.html

これらの機能の詳細については、『Cisco Wireless Phone 840 and 860 Administration Guide』または『Cisco Wireless Phone 840 and 860 Release Notes』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/webex-wireless-phone/products-release-notes-list.html>

Webex Calling

Webex はクラウド登録を有効にするため、Cisco Wireless Phone 840 または 860 に直接インターネット接続がある限り、VPN 接続は必要ありません。

Cisco Wireless Phone 840 および 860 は、Webex Calling に登録できるように、ファームウェアバージョン 1.6(0) 以降を実行している必要があります。

The screenshot displays the Webex Control Hub interface. The left sidebar contains navigation menus for Overview, MONITORING, MANAGEMENT, and SERVICES. The main content area is titled 'Overview' and includes several widgets: 'Getting Started Guide' (0 of 7 tasks completed), 'Updates' (Update your services to the new Webex experience), 'New offers' (Boost your users' collaboration experience for free with Basic Meetings), 'Webex services' (ALL ONLINE status for Webex, Calling, Meetings, Hybrid Services, Control Hub, Developer API, Room Devices, and Contact Center), 'Devices' (88 Total devices, with breakdowns for Online, Offline, Expired, Unknown, and Activating), 'Onboarding' (91 Total Users, with a donut chart showing 88% Not Verified, 12% Active, and 0% Inactive/Verified), and 'What's new' (webex + logo, The latest update is here!). A 'Quick links' section at the bottom right provides links for Admin capabilities, Manage subscriptions, Organization tasks, and Audit log.

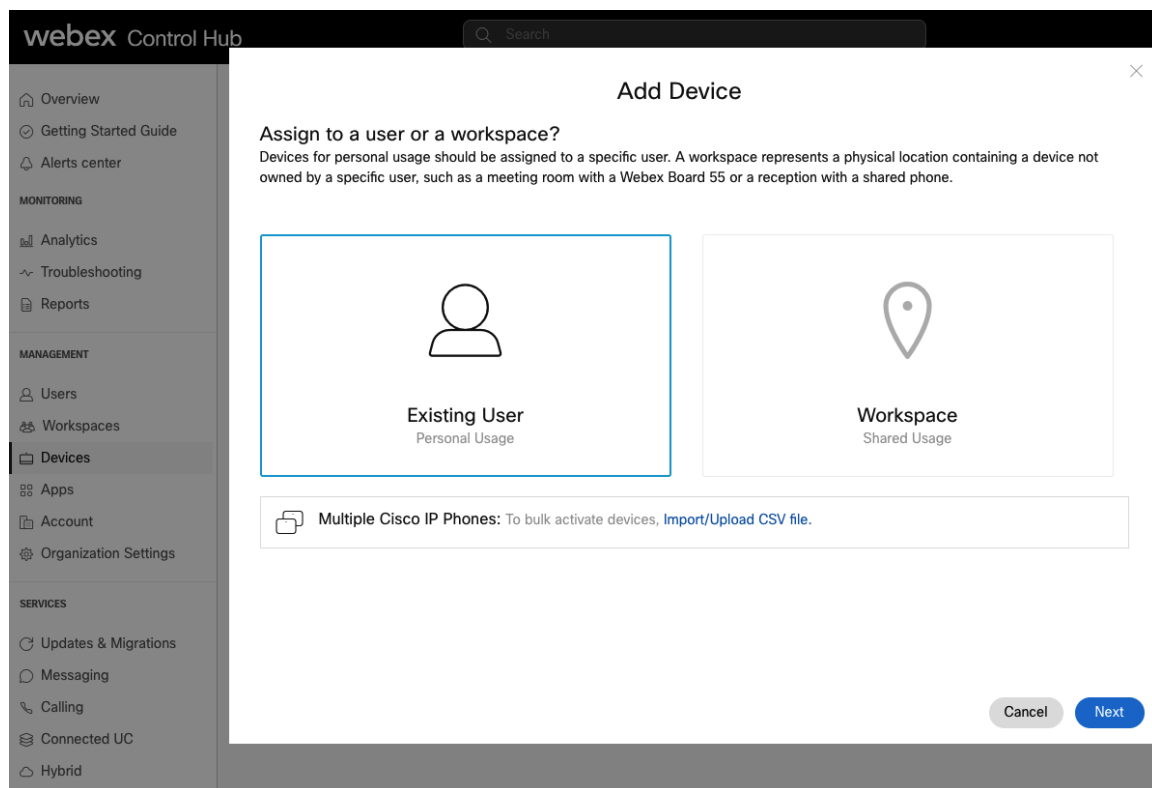
Cisco Wireless Phone 840 または 860 は、Webex Calling に追加して、個人使用または共有使用のワークスペースとしてユーザーに割り当てることができます。

個人的な使用

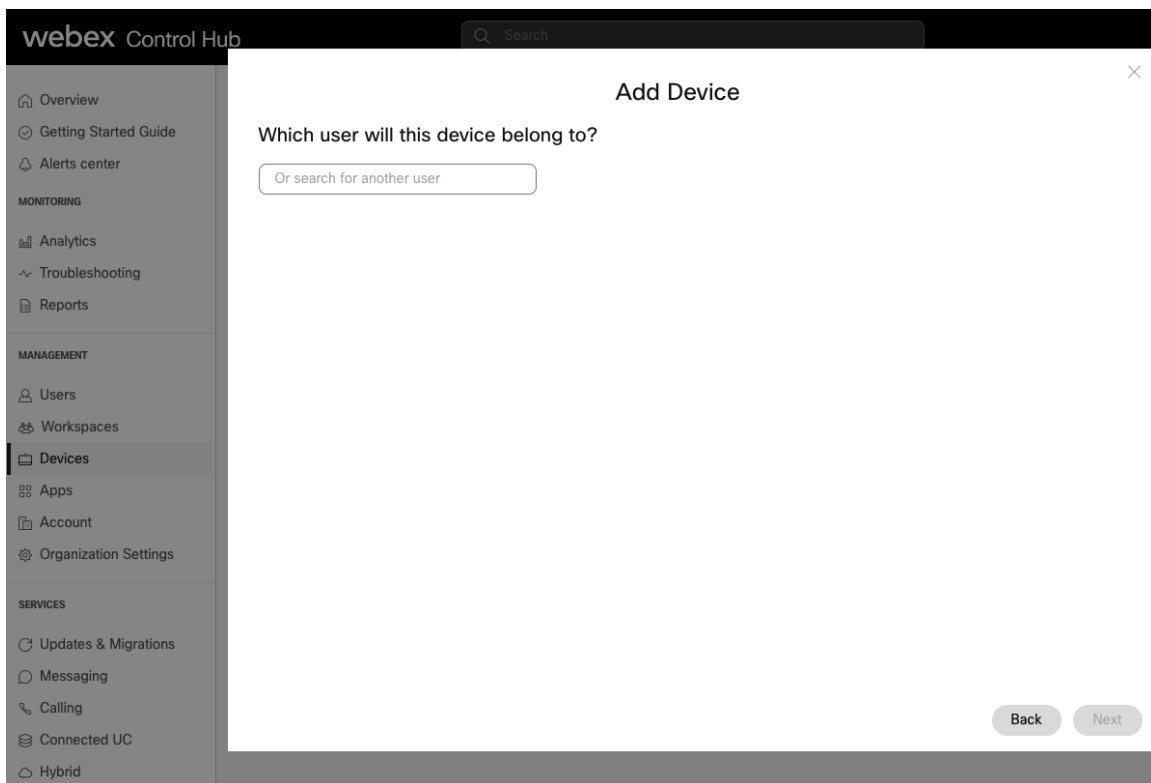
Cisco Wireless Phone 840 または 860 は、**[デバイス (Devices)]** を介してユーザが個人的に使用するよう設定できます。

ユーザーのデバイスを追加するには、**[デバイス (Devices)]** に移動し、**[デバイスの追加 (Add Device)]** を選択します。

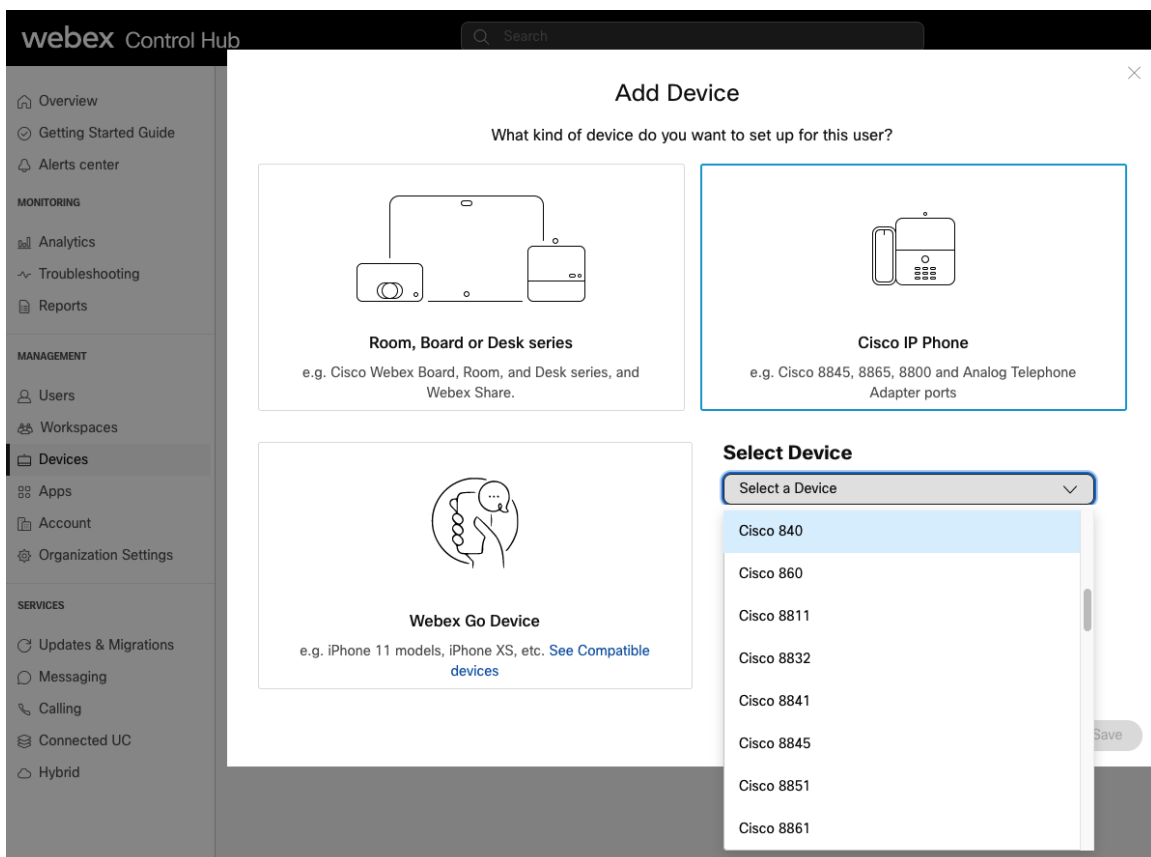
次の画面で、**[既存のユーザー (Existing User)]** を選択し、**[次へ (Next)]** をクリックします。



Cisco Wireless Phone 840 または 860 を割り当てるユーザを検索し、**[次へ (Next)]** をクリックします。



[Cisco IP 電話 (Cisco IP Phone)] を選択し、ドロップダウンリストから [Cisco 840] または [Cisco 860] を選択します。



Cisco Wireless Phone 840 または 860 の MAC アドレスを入力し、下のボックスをオンにして、**【保存 (Save)】** を選択します。

The screenshot shows the 'Add Device' interface in the Webex Control Hub. The left sidebar contains navigation options like Overview, Getting Started Guide, Alerts center, MONITORING (Analytics, Troubleshooting, Reports), MANAGEMENT (Users, Workspaces, Devices, Apps, Account, Organization Settings), and SERVICES (Updates & Migrations, Messaging, Calling, Connected UC, Hybrid). The main content area is titled 'Add Device' and asks 'What kind of device do you want to set up for this user?'. Three options are presented: 'Room, Board or Desk series' (e.g., Cisco Webex Board, Room, and Desk series, and Webex Share), 'Cisco IP Phone' (e.g., Cisco 8845, 8865, 8800 and Analog Telephone Adapter ports), and 'Webex Go Device' (e.g., iPhone 11 models, iPhone XS, etc. See Compatible devices). The 'Cisco IP Phone' option is highlighted with a blue border. Below the options, there is a 'Select Device' dropdown menu with 'Cisco 860' selected, and an 'Enter MAC Address' input field. A disclaimer is visible below the input field, and 'Back' and 'Save' buttons are at the bottom right.

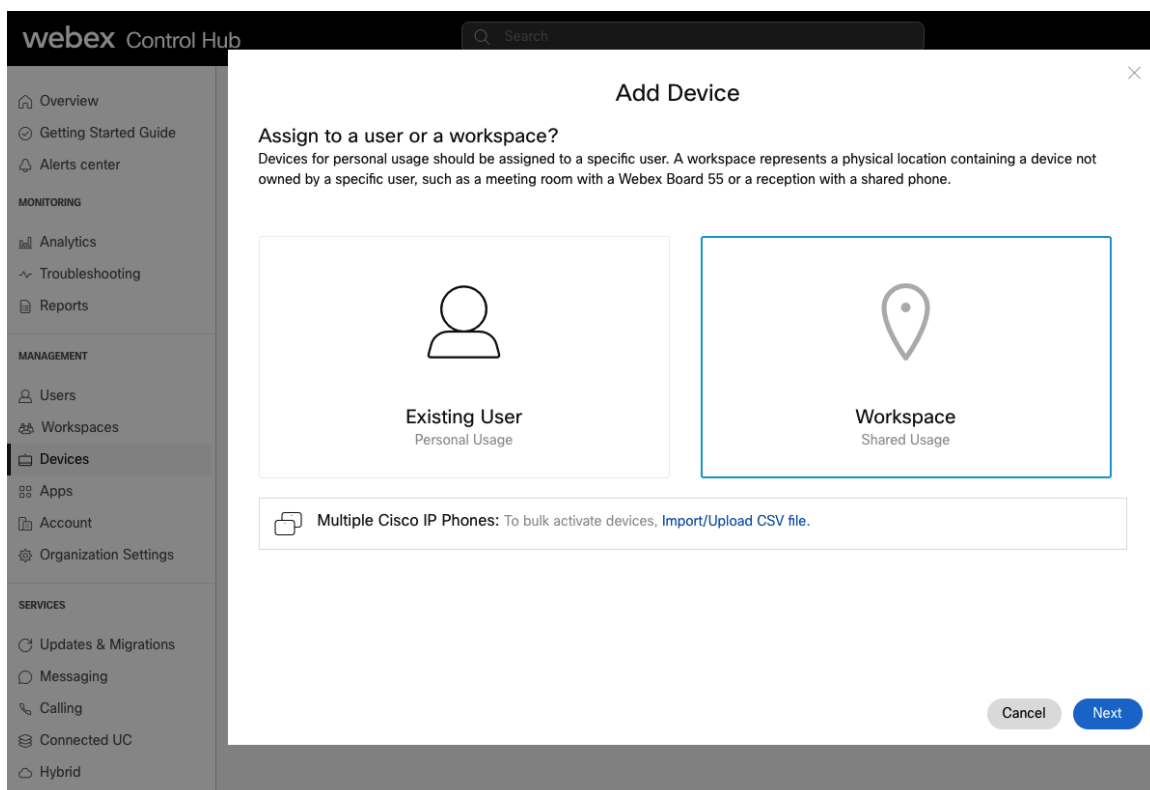
【ユーザー (Users)】 でユーザーを選択して、サービスを設定または変更します。

共同利用

Cisco Wireless Phone 840 または 860 は、**【デバイス (Devices)】** または **【ワークスペース (Workspaces)】** を使用してワークスペースとして設定できます。

【デバイス (Devices)】 を介してワークスペースを追加するには、**【デバイス (Devices)】** に移動し、**【デバイスの追加 (Add Device)】** を選択します。

次の画面で、**【ワークスペース (Workspace)】** を選択し、**【次へ (Next)】** をクリックします。



[既存のワークスペース (Existing Workspace)] または [新しいワークスペース (New Workspace)]
を選択します。


選択したオプションに応じて、ワークスペース名を検索または入力して、**[次へ (Next)]** をクリックします。

webex Control Hub


Search

Add Device

Assign to an existing workspace or a new workspace?
Select Existing Workspace to assign a device to an existing workspace. If you add multiple devices to the same workspace that are not designed to work together, there may be interference issues. Note that there can only be one Cisco IP Phone per workspace.



Existing Workspace



New Workspace


Which Workspace will the device be assigned to?
Workspaces containing Cisco IP Phones will not be shown, since you can only have one of these devices in a workspace.

webex Control Hub


Search

Add Device

Assign to an existing workspace or a new workspace?
Select Existing Workspace to assign a device to an existing workspace. If you add multiple devices to the same workspace that are not designed to work together, there may be interference issues. Note that there can only be one Cisco IP Phone per workspace.



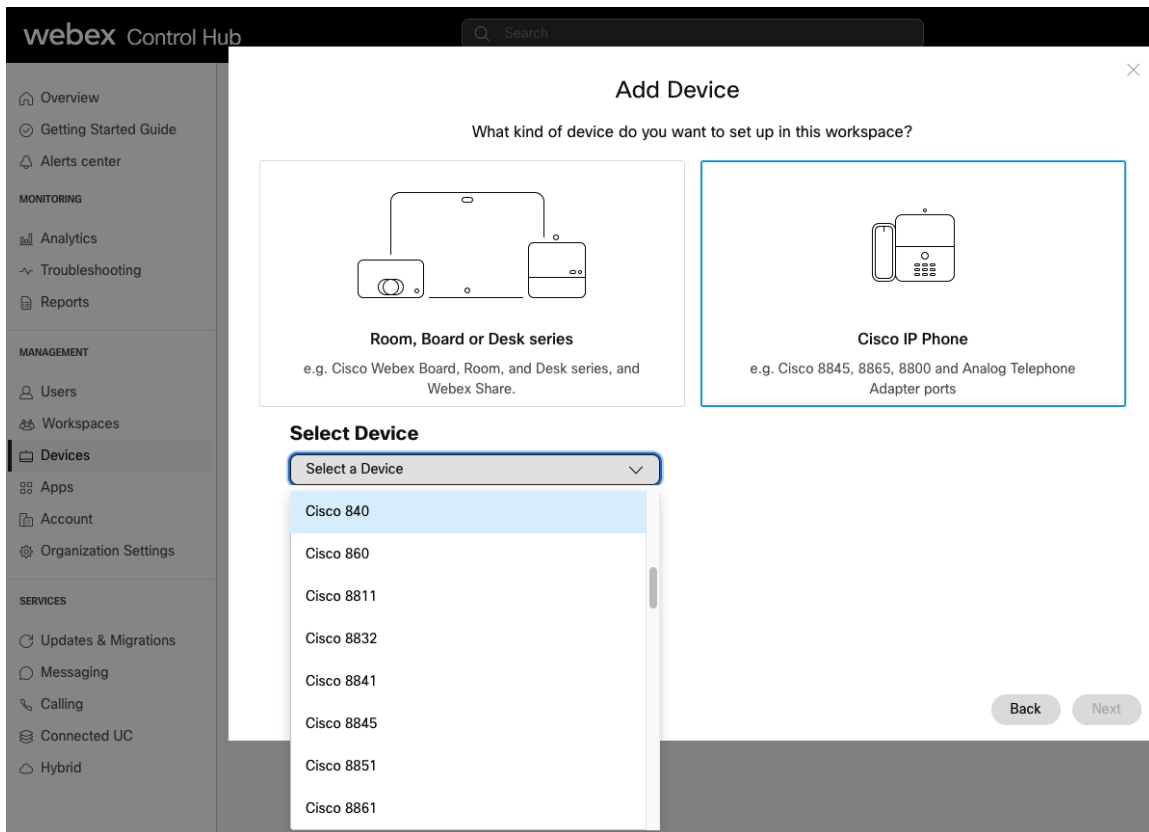
Existing Workspace



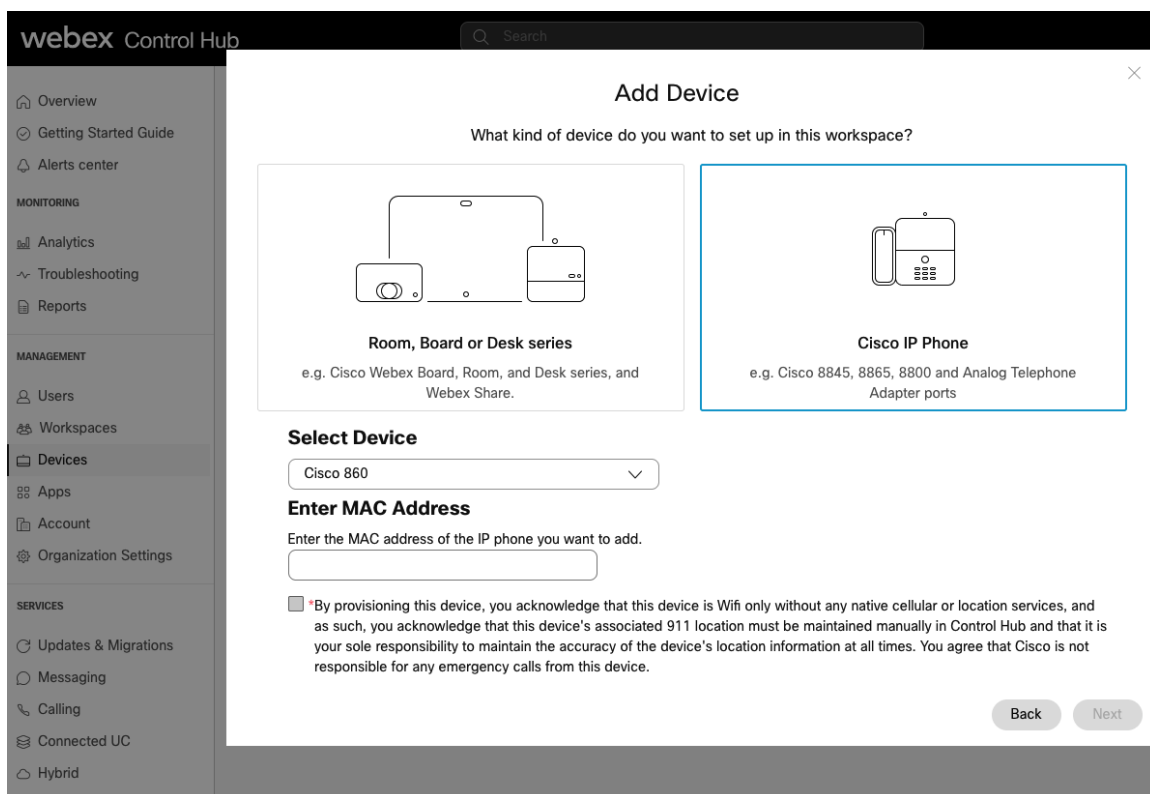
New Workspace

Where will this device be located?
What would you like to call the Workspace that this device will be assigned to?

[Cisco IP 電話 (Cisco IP Phone)] を選択し、ドロップダウンリストから [Cisco 840] または [Cisco 860] を選択します。



Cisco Wireless Phone 840 または 860 の MAC アドレスを入力し、下のボックスをオンにして、**[次へ (Next)]** を選択します。



次の画面でロケーション、電話番号、内線番号、および通話プランを設定し、[保存 (Save)] を選択します。

ワークスペースを介して既存の [ワークスペース (Workspaces)] を選択して、サービスを設定または変更します。

デバイス設定

Cisco Wireless Phone 840 および 860 では、次の設定オプションを使用できます。

Device Settings

Apply the location's default settings or customize the settings for this device. Then resync the device to apply these changes.

- Use the location settings
- Define custom device settings

🔍 Search

Audio Codec Priority ⓘ	<input checked="" type="checkbox"/>	Override regional defaults with custom values	
LDAP ⓘ	<input checked="" type="checkbox"/>		▼
Phone Security Password ⓘ			
Web Access ⓘ	<input checked="" type="checkbox"/>		▲
Set Password ⓘ			

Webex Calling のネットワーク要件については、次の URL にある『**Port Reference Information for Webex Calling**』ドキュメントを参照してください。

<https://help.webex.com/en-US/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling>

詳細については、次の URL にある『**Cisco Wireless Phone 840 and 860 Administration Guide**』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Cisco Wireless Phone 840 および 860

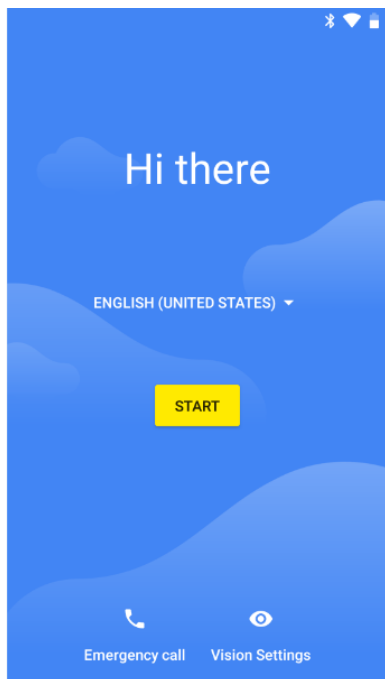
Cisco Wireless Phone 840 および 860 を設定するには、エンタープライズ モビリティ管理 (EMM) アプリケーションまたは Cisco Wireless Phone Configuration Management ユーティリティを使用して中央プロビジョニングを行うか、ローカル ユーザ インターフェイスを使用して手動で設定します。

エンタープライズ モビリティ管理 (EMM)

管理ツールを使用して Cisco Wireless Phone 840 および 860 の設定を管理し、サードパーティ製アプリケーションを許可する機能を使用する場合は、エンタープライズ モビリティ管理 (EMM) アプリケーションを活用する必要があります。

エンタープライズ モビリティ管理 (EMM) アプリケーションを介して Cisco Wireless Phone 840 および 860 を手動で設定するには、次のガイドラインを使用します。

起動画面で、ディスプレイをすばやく 6 回タップすると、QR コードをスキャンして、デバイス所有者方式で Cisco Wireless Phone 840 または 860 を EMM に登録できます。



次のアプリケーションは、デバイス所有者方式を使用して電話機を登録するときに、Cisco Wireless Phone 840 および 860 で使用できるように、許可されたアプリケーションとして追加する必要があります。これらのアプリケーションは Google Play ストアで使用できないためです。

- **Cisco Phone** = com.cisco.phone
- **Application URLs** = com.cisco.appurl
- **Diagnostics** = com.cisco.diagnostics
- **Logging** = com.cisco.logging
- **Port Manager** = com.cisco.portmanager
- **System Updater** = com.cisco.sysupdater
- **UCM Client** = com.cisco.ucmclient

The screenshot displays the Cisco Meraki Systems Manager interface. On the left, a sidebar lists various configuration categories under 'Systems Manager', with 'Android System Apps' highlighted. The main panel shows the configuration for a Cisco 860 device. A section titled 'Android System Apps' is active, showing a message: 'By default all system apps are disabled.' Below this, a 'List Type' dropdown is set to 'Allowlist'. A list of system apps is displayed, each with a green Android icon and a close button (X):

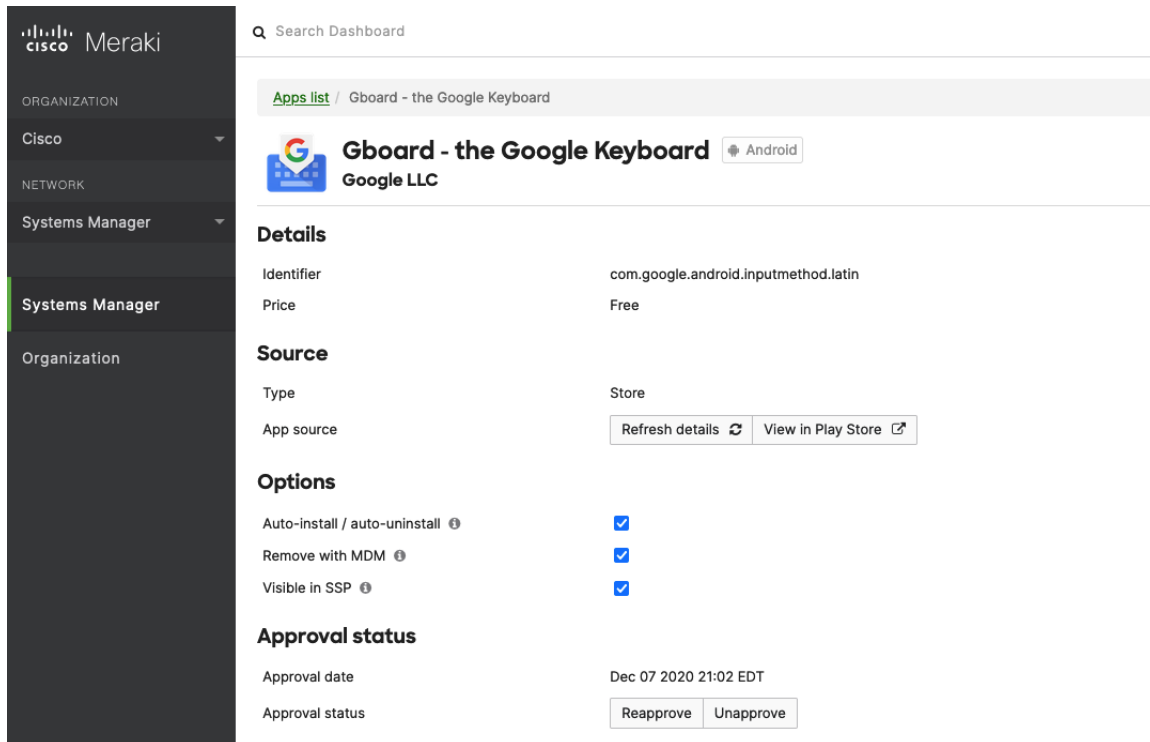
- com.cisco.phone
- com.cisco.appurl
- com.cisco.logging
- com.cisco.portmanager
- com.cisco.sysupdater
- com.cisco.ucmclient

以下は、Google Play ストアで入手可能で、デバイス所有者方式を使用して電話機を登録するときオプションで追加できる、Cisco Wireless Phone 840 および 860 に固有のシスコ アプリケーションのリストです。

- **Battery Life** = com.cisco.batterylife
- **Buttons** = com.cisco.buttons
- **Call Quality Settings** = com.cisco.callquality
- **Custom Settings** = com.cisco.customsettings
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- **Sound Stage** = com.cisco.soundstage
- **Web API** = com.cisco.webapi
- **Barcode** (840s and 860s models only) = com.cisco.barcode.service

必要に応じて、他のアプリケーションを許可できます。

使用する EMM プラットフォームによっては、デバイス所有者方式を使用して電話を登録するときに、**Gboard (Google キーボードアプリケーション)** も追加する必要がある場合があります)



The screenshot shows the Cisco Meraki Systems Manager interface. On the left is a dark sidebar with navigation options: ORGANIZATION, Cisco, NETWORK, Systems Manager, Systems Manager (highlighted), and Organization. The main content area has a search bar at the top. Below it, a breadcrumb trail reads 'Apps list / Gboard - the Google Keyboard'. The application card for 'Gboard - the Google Keyboard' by Google LLC is displayed, with an 'Android' platform tag. The card is divided into sections: 'Details' (Identifier: com.google.android.inputmethod.latin, Price: Free), 'Source' (Type: Store, App source: Refresh details, View in Play Store), 'Options' (Auto-install / auto-uninstall, Remove with MDM, Visible in SSP, all checked), and 'Approval status' (Approval date: Dec 07 2020 21:02 EDT, Reapprove, Unapprove buttons).

詳細については、EMM アプリケーションのマニュアルを参照してください。

注： Cisco Wireless Phone 840 および 860 に証明書を一括で自動的に発行する場合は、EMM アプリケーションを使用する必要があります。

シスコワイヤレス電話構成管理ツール

管理ツールを使用して Cisco Wireless Phone 840 および 860 の設定を管理し、サードパーティ製アプリケーションを使用できない場合は、Cisco Wireless Phone Configuration Management ユーティリティを使用することをお勧めします。

1.5(0) リリースでは、Cisco Wireless Phone Configuration Management ユーティリティ (<https://configure.cisco.com>) が、Cisco Wireless Phone 840 および 860 電話管理の追加オプションになりました。

Cisco Wireless Phone Configuration Management ユーティリティにアクセスするには、Cisco.com アカウントが必要です。

注： Cisco Wireless Phone Configuration Management Utility は、Webex Calling に登録されている Cisco Wireless Phone 840 または 860 では現在サポートされていません。

構成ファイルの作成

Cisco Wireless Phone Configuration Management ユーティリティを使用してダウンロード可能な設定ファイルを作成するには、**[展開設定 (Deployment Configuration)]** タブに移動し、必要なアプリケーション パラメータを設定します。

[エクスポート (Export)] を選択して、ZIP 形式でエクスポートされる設定ファイルを保存します。


アプリケーション設定の構成

ドロップダウンリストから必要なアプリケーションを選択し、必要なパラメータを設定します。

バーコード

バーコード設定を構成するには、ドロップダウンリストから **[バーコード (Barcode)]** を選択します。

Choose Application

 Barcode ▼

Import

Export

Enable Barcode Scanner

False True



- > General 
- > Data Manipulation 
- > Custom Intent Settings 
- > Symbology Settings 
- > Replace Control Characters 
- > ScanFlex 

バッテリー寿命

[**バッテリー寿命 (Battery Life)**] を設定するには、ドロップダウンリストから [**バッテリー寿命 (Battery Life)**] を選択します。

Webex Wireless Phone Configuration Management

Deployment Configuration Initial Provisioning

Choose Application Battery Life

Import Export

Enable Battery Monitoring	False <input type="radio"/> True <input checked="" type="radio"/>	i
Low Battery Threshold	15%	i
Vibrate	False <input type="radio"/> True <input checked="" type="radio"/>	i
Sound	False <input type="radio"/> True <input checked="" type="radio"/>	i
Alarm Tone	Cesium	i
Snooze Time	2 min	i

ボタン

ボタン設定を構成するには、ドロップダウンリストから **[ボタン (Buttons)]** を選択します。

Webex Wireless Phone Configuration Management

Deployment Configuration Initial Provisioning

Choose Application Buttons

Import Export


- > Left Button [i](#)
- > Right Button [i](#)
- > Top Button [i](#)
- > Fingerprint Button [i](#)
- > Volume up Button [i](#)
- > Volume Down Button [i](#)



通話品質設定


[**コール品質設定 (Call Quality Settings)**] を設定するには、ドロップダウンリストから [**コール品質設定 (Call Quality Settings)**] を選択します。


Webex Wireless Phone Configuration Management




Deployment Configuration Initial Provisioning


Choose Application  Call Quality Settings ▼


Wi-Fi Low RSSI Threshold  -67 


▼ Channel Selection 

▼ Wi-Fi Band Selection 

Auto Band Selection	False <input checked="" type="checkbox"/> True 
2.4 GHz Wi-Fi Band	False <input checked="" type="checkbox"/> True 
5 GHz Wi-Fi Band	False <input checked="" type="checkbox"/> True 


> 2.4 GHz: Channels 1- 13 



> 5 GHz 


> Wi-Fi Preferences 


Webex Wireless Phone Configuration Management




Deployment Configuration Initial Provisioning

Choose Application  Call Quality Settings ▼

Wi-Fi Low RSSI Threshold  -67 

> Channel Selection 

▼ Wi-Fi Preferences 

FT	No	<input checked="" type="checkbox"/> Yes	
CCKM	No	<input checked="" type="checkbox"/> Yes	
CAC	No	<input type="checkbox"/> Yes	

注：1.8(0) リリースでは、**CAC**（コール アドミッション コントロール）を無効にするオプションが有効になっています。

1.9(0) リリースでは、**CAC**（コールアドミッション コントロール）はデフォルトで無効になっており、オプション機能になりました。

カスタム設定












[カスタム設定 (Custom Settings)] を設定するには、ドロップダウンリストから [カスタム設定 (Custom Settings)] を選択します。

Deployment Configuration Initial Provisioning

Choose Application  Custom Settings ▼

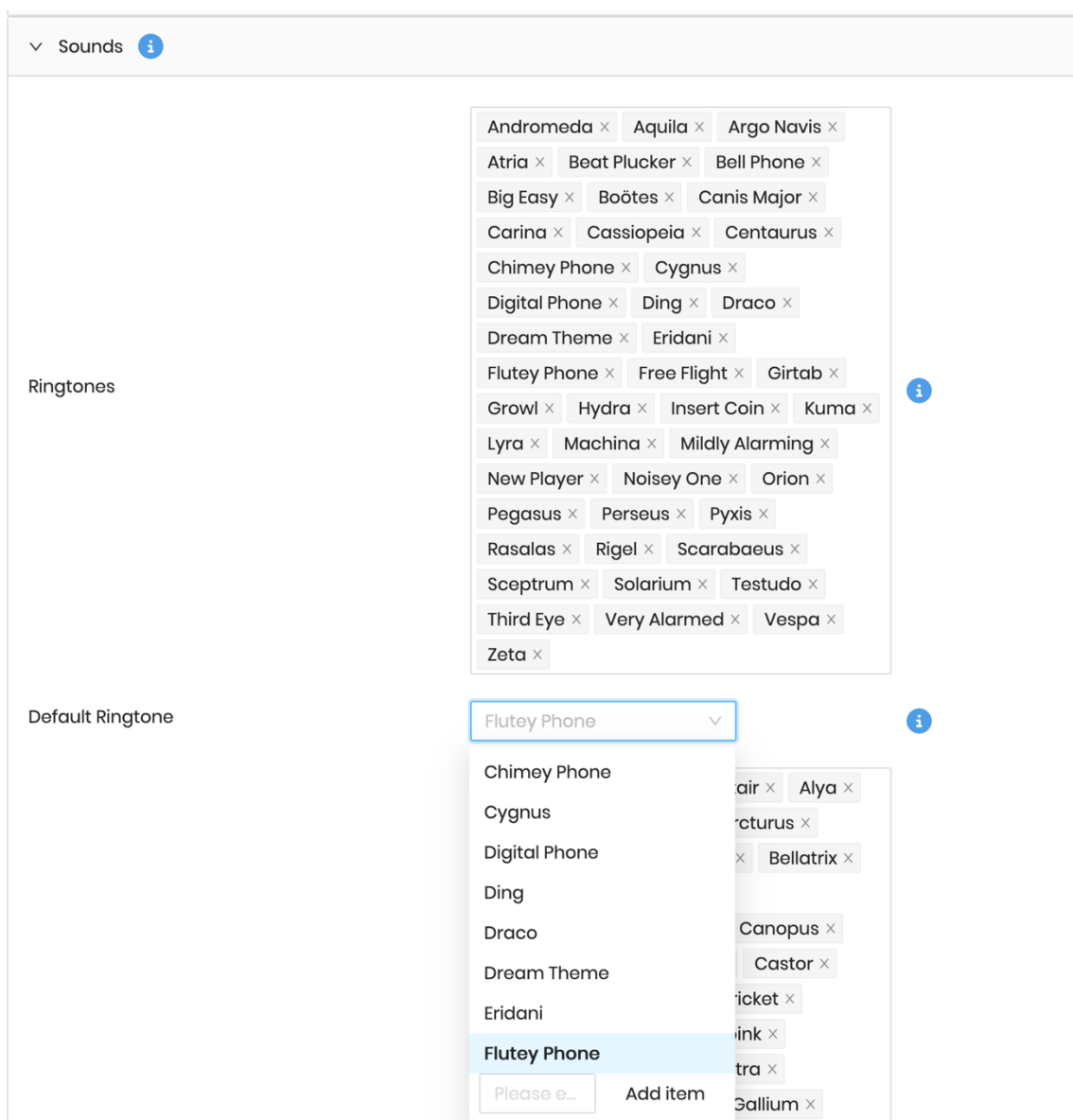
Import

Export

- > User Restrictions 
- > Time 
- > Edit Device Name 
- > Battery 
- > Keyboard 
- > Sleep 
- > Display 
- > Touch 
- > Sounds 
- > Camera 
- > Wallpaper 

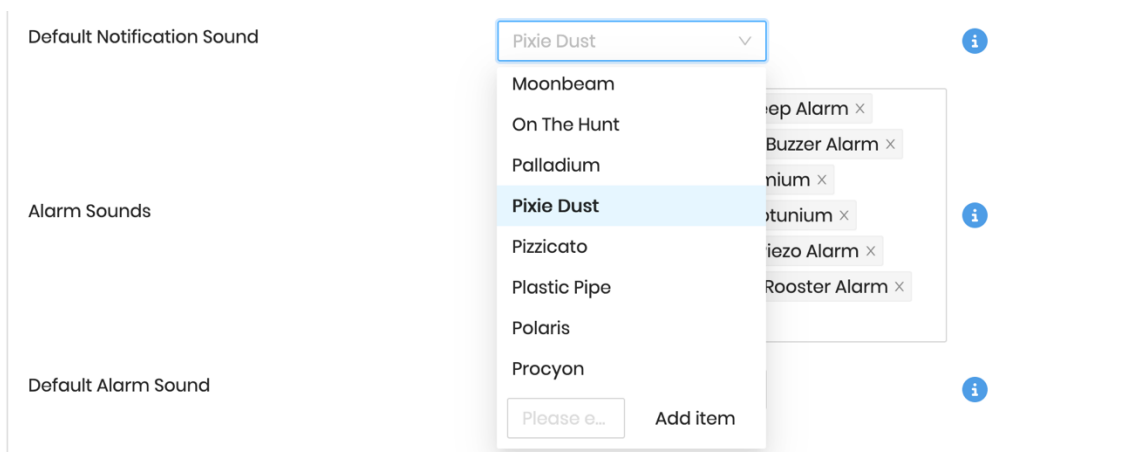
デフォルトの着信音は、**[サウンド (Sounds)]**メニューで管理できます。

カスタム着信音をデフォルトの着信音として設定する場合は、通知音の名前を入力し、**[項目の追加 (Add item)]**を選択します。



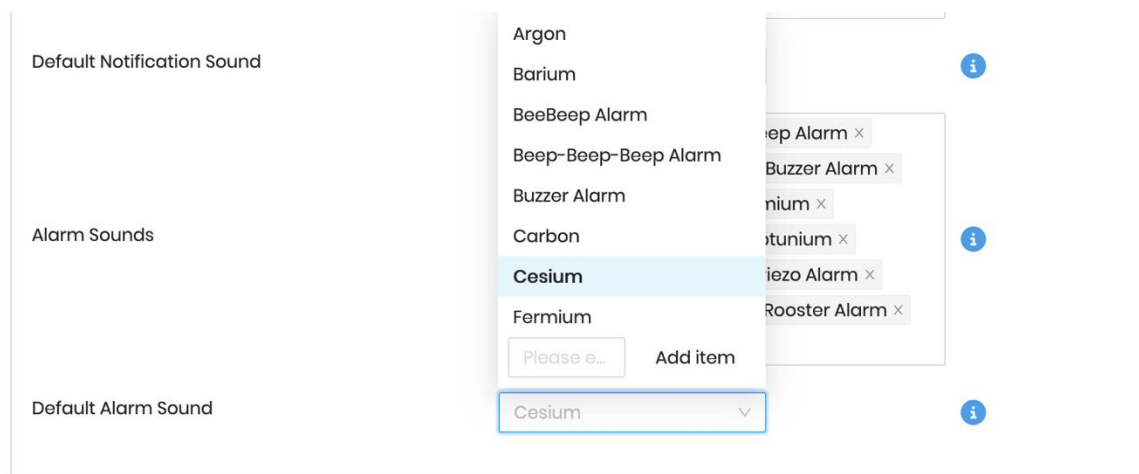
デフォルトの通知音は、**[サウンド (Sounds)]**メニュー内で管理できます。

カスタム通知音をデフォルトの通知音として設定する場合は、通知音の名前を入力し、**[項目の追加 (Add item)]**を選択します。

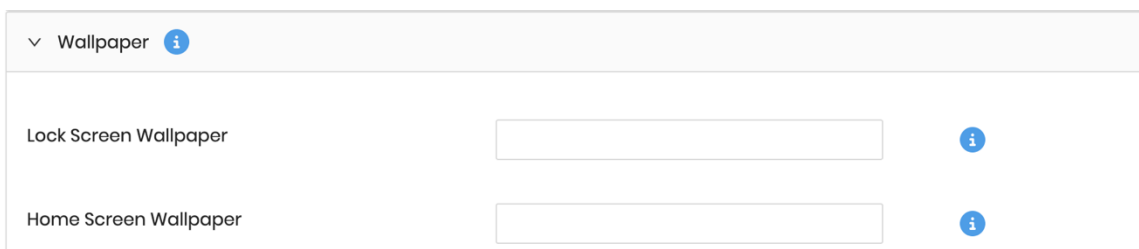


デフォルトのアラーム音は、**[サウンド (Sounds)]** メニューで管理できます。

カスタムアラーム音をデフォルトのアラーム音として設定する場合は、アラーム音の名前を入力し、**[項目の追加 (Add item)]** を選択します。



[ロック画面の壁紙 (Lock Screen Wallpaper)] と **[ホーム画面の壁紙 (Home Screen Wallpaper)]** は、**[壁紙 (Wallpaper)]** メニュー内で管理できます。



緊急 (Emergency)








緊急設定を構成するには、ドロップダウンリストから **[緊急 (Emergency)]** を選択します。

Webex Wireless Phone Configuration Management

Deployment Configuration Initial Provisioning

Choose Application

Enable Emergency Monitoring	False <input type="checkbox"/> True <input checked="" type="checkbox"/>	i
No Movement Sensitivity	<input type="text" value="Disabled"/>	i
No Movement Timeout (Seconds)	<input type="text" value="30"/>	i
Tilt Sensitivity	<input type="text" value="Disabled"/>	i
Tilt Timeout (Seconds)	<input type="text" value="10"/>	i
Running Sensitivity	<input type="text" value="Disabled"/>	i
Running Timeout (Seconds)	<input type="text" value="10"/>	i
Snooze Timeout (Seconds)	<input type="text" value="0"/>	i
Warning Timeout (Seconds)	<input type="text" value="10"/>	i
Panic Button	<input type="text" value="Disabled"/>	i

Panic Button Alarm Timeout (Seconds)	<input type="text" value="5"/>	
Panic Button Silent Alarm	False <input checked="" type="checkbox"/> True	
Emergency Call	False <input type="checkbox"/> True	
Emergency Dial Force Speaker	False <input checked="" type="checkbox"/> True	
Emergency Dial Number	<input type="text" value="911"/>	
Warning Tone	<input type="text" value="Pixie Dust"/>	
Alarm Tone	<input type="text" value="Cesium"/>	

PTT

PTT 設定を構成するには、ドロップダウンリストから **[PTT]** を選択します。

Deployment Configuration Initial Provisioning

Choose Application

Enable PTT	False <input checked="" type="checkbox"/> True	i
Allow PTT Transmission when Phone Is Locked	False <input checked="" type="checkbox"/> True	i
Username	<input type="text"/>	i
Multicast Address	<input type="text" value="224.0.1.116"/>	i
Codec	<input type="text" value="G.726"/>	i
Default Channel UI State	<input type="text" value="Enabled"/>	i
PTT Volume UI State	<input type="text" value="Enabled"/>	i
Channel 1	<input type="text" value="ALL"/>	i
Channel 1 Can Transmit	False <input checked="" type="checkbox"/> True	i
Channel 1 Can Subscribe	False <input checked="" type="checkbox"/> True	i

サウンドステージ

[サウンドステージ (Sound Stage)] を設定するには、ドロップダウンリストから [サウンドステージ (Sound Stage)] を選択します。

Deployment Configuration Initial Provisioning

Choose Application

Enable Sound Stage	False <input type="checkbox"/> True <input checked="" type="checkbox"/>	i
Enable Sound Profile Switch	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Enable Personal Profile	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Enable Normal Profile	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Enable Loud Profile	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Enable Soft Profile	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Enable Silent Profile	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Switch Profiles Silently	False <input type="checkbox"/> True <input checked="" type="checkbox"/>	i
Persist Active Profile Notification	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i
Enable NFC Beam	False <input checked="" type="checkbox"/> True <input type="checkbox"/>	i

事前設定されたプロファイル ([標準 (Normal)]、[大音量 (Loud)]、[ソフト (Soft)]、[サイレント (Silent)]) およびカスタムの個人プロファイルは、必要に応じて設定および調整できます。

Normal Profile Alarm Volume		20	
Normal Profile Alarm Minimum Volume		14	
Normal Profile Alarm Maximum Volume		75	
Normal Profile Ringer Volume		20	
Normal Profile Ringer Minimum Volume		14	
Normal Profile Ringer Maximum Volume		75	
Normal Profile Media Volume		20	
Normal Profile Media Minimum Volume		7	
Normal Profile Media Maximum Volume		75	
Normal Profile Call Volume		20	
Normal Profile Call Minimum Volume		20	
Normal Profile Call Maximum Volume		75	
Normal Profile Web API Volume		20	
Normal Profile Web API Minimum Volume		7	
Normal Profile Web API Maximum Volume		95	
Normal Profile PTT Volume		20	
Normal Profile PTT Minimum Volume		20	
Normal Profile PTT Maximum Volume		85	
Normal Profile Low Battery Alarm Volume		50	
Normal Profile Low Battery Alarm Minimum Volume		50	
Normal Profile Low Battery Alarm Maximum Volume		80	

その後、特定の条件が満たされたときにプロファイルに切り替えるようにルールを設定できます。

Apply Rule 1 False True i

Select Profile to Switch for Rule 1 Loud i

Type for Rule 1 Charging i

Apply Rule 2 False True i

Select Profile to Switch for Rule 2 Normal i

Type for Rule 2 Time i

Select Time Slot for Rule 2 08:00 AM i

Apply Rule 3 False True i

Select Profile to Switch for Rule 3 Soft i

Type for Rule 3 Time i

Select Time Slot for Rule 3 10:00 AM i

Apply Rule 4 False True i

Select Profile to Switch for Rule 4 Personal i

Type for Rule 4 Time i

Select Time Slot for Rule 4 08:00 PM i

Apply Rule 5 False True i

Select Profile to Switch for Rule 5 Silent i

Type for Rule 5 Time i

Select Time Slot for Rule 5 12:00 AM i

Web API

Web API 設定を構成するには、ドロップダウンリストから **[Web API]** を選択します。

Webex Wireless Phone Configuration Management

Deployment Configuration Initial Provisioning

Choose Application Web API

Import Export

Enable Web API False True i

Data Format XML i

Polling Username i

Polling Password i

Respond Mode Requester i

URL i

Push Username i

Push Password i

Push Alert Priority All i

Server Root URL i

Enable Notification Ringtone False True i

Web API Volume 50 i

Shortcut Title 1 i

Shortcut URL 1 i

Shortcut Title 2 i

Shortcut URL 2 i

Shortcut Title 3 i

Shortcut URL 3 i

Web API Event Label 1	<input type="text"/>	
Web API Event Url 1	<input type="text"/>	
All Web API Event 1	False <input type="checkbox"/> True	
State Change Web API Event 1	False <input type="checkbox"/> True	
Incoming Call Web API Event 1	False <input type="checkbox"/> True	
Registration Web API Event 1	False <input type="checkbox"/> True	
Unregistration Web API Event 1	False <input type="checkbox"/> True	
Outgoing Call Web API Event 1	False <input type="checkbox"/> True	
User Login/out Web API Event 1	False <input type="checkbox"/> True	
Emergency Alarm Web API Event 1	False <input type="checkbox"/> True	

Device Policy Controller アプリケーションの設定

Device Policy Controller は、Cisco Wireless Phone 840 および 860 が Cisco Wireless Phone で管理されている場合に、管理者がアプリケーション全体を無効にしたり、Wi-Fi プロファイルパラメータとオプションの電話ロック解除ピン/パスワードを定義したりできる新しいアプリケーションです。[設定管理ユーティリティ (Configuration Management Utility)]。

最大 5 つの Wi-Fi プロファイルを設定できます。

次のセキュリティ設定がサポートされています。

[セキュリティモード (Security Mode)]	EAP 方法	フェース 2 認証
なし	該当なし	なし
WPA2-Personal	該当なし	なし
WPA2-Enterprise	PEAP	GTC、MSCHAPV2
WPA2-Enterprise	TTLS	GTC、MSCHAP、MSCHAPV2、PAP

注：Cisco Wireless Phone Configuration Management Utility は、EAP-TLS (TLS) をサポートしていません。

オープン Wi-Fi ネットワークに接続するには、**SSID** を入力し、[セキュリティ (Security)] を [なし (None)] に設定します。

The screenshot shows the 'Webex Wireless Phone Configuration Management' interface. At the top, there are two tabs: 'Deployment Configuration' (selected) and 'Initial Provisioning'. Below the tabs, there is a 'Choose Application' dropdown menu set to 'Device Policy Controller'. There are 'Import' and 'Export' buttons. The main content area is titled 'Wi-Fi Profile' and contains a list of profiles. The first profile is selected and expanded, showing the following settings:

- Security:** A dropdown menu set to 'None'.
- * SSID:** An empty text input field.
- Hidden SSID:** A toggle switch set to 'False'.
- Phone Unlock Pin/password:** An empty text input field with a lock icon.

PSK 対応の Wi-Fi ネットワークに接続するには、**SSID** を入力し、[セキュリティ (Security)] を [WPA2-個人 (WPA2-Personal)] に設定してから、8-63 ASCII または 64 HEX パスワードを入力します。

Deployment Configuration Initial Provisioning

Choose Application Device Policy Controller

Import Export

Wi-Fi Profile i

Wi-Fi Profile i

1 ⊖ ⊕

Security WPA2-Personal i

* SSID i

* Password i

Hidden SSID False True i

Phone Unlock Pin/password i

EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [WPA2-EAP] に設定してから、[認証方式 (Authentication method)] を選択します。

PEAP または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、フェーズ 2 認証方式を選択し、必要に応じてヘッダーとフッターを除いた Base-64 (PEM) エンコーディング形式で CA 証明書を設定し、ID とパスワードを入力します。

Deployment Configuration Initial Provisioning

Choose Application Device Policy Controller

Import

Export

Wi-Fi Profile

Wi-Fi Profile

1

Security

WPA2-Enterprise

* SSID

* Password

Hidden SSID

False True

WPA2-Enterprise Parameters

EAP Method

PEAP

Phase 2 Authentication

MSCHAPV2

Domain

* Identity

Anonymous Identity

CA Certificate

Select CA Certificate

Phone Unlock Pin/password

注：ブロードキャストされていない Wi-Fi ネットワークは、**非表示の SSID** として設定する必要があります。それ以外の場合、Wi-Fi ネットワークは範囲内に表示されません。非ブロードキャスト Wi-Fi ネットワークに接続するには、**[非表示 SSID (Hidden SSID)]** を **[はい (True)]** に設定します。

設定された Wi-Fi ネットワークが Cisco Unified Communications Manager を指していることを確認します。それ以外の場合は、Cisco Wireless Phone 840 および 860 の電話アプリケーションで TFTP サーバーを手動で設定する必要があります。

ヘッダーとフッターが削除され、スペースや改行が含まれていない CA 証明書の形式が正しいことを確認します。

次のアプリケーションはデフォルトで許可されません。ただし、無効化されたアプリケーションのリストは、必要に応じてさらに設定できます。

- **Chrome** = com.android.chrome
- **Digital Wellbeing** = com.google.android.apps.wellbeing
- **Google** = com.google.android.googlequicksearchbox
- **Google TV** = com.google.android.videos
- **Maps** = com.google.android.apps.maps
- **Photos** = com.google.android.apps.photos
- **Play Store** = com.android.vending
- **Sound Recorder** = com.android.soundrecorder
- **YouTube** = com.google.android.youtube

Webex Wireless Phone Configuration Management

Deployment Configuration Initial Provisioning

Choose Application Device Policy Controller

Import Export

> Wi-Fi Profile i

Phone Unlock Pin/password

Disallow These Apps

- com.google.android.youtube x
- com.google.android.googlequicksearchbox x
- com.android.soundrecorder x
- com.google.android.apps.wellbeing x
- com.google.android.apps.maps x
- com.google.android.videos x
- com.google.android.apps.photos x
- com.android.vending x
- com.android.chrome x

+ New Tag

注：重要なアプリケーションが Device Policy Controller の設定で許可されていないことを確認してください。

- **Smart Launcher** = com.cisco.smartlauncher
- **Device Policy Controller** = com.cisco.devicepolicycontroller
- **Cisco Phone** = com.cisco.phone
- **Application URLs** = com.cisco.appurl
- **Logging** = com.cisco.logging
- **Port Manager** = com.cisco.portmanager
- **System Updater** = com.cisco.sysupdater
- **UCM Client** = com.cisco.ucmclient
- **Web API** = com.cisco.webapi
- **Settings** = com.android.settings

スマートランチャアプリケーションの設定

スマートランチャは、Cisco Wireless Phone 840 および 860 が Cisco Wireless Phone Configuration Management Utility によって管理されている場合に、エンドユーザがアクセスできるアプリケーションを制限する新しいアプリケーションです。

次のアプリケーションは、デフォルトでスマートランチャービューに表示されるようになっています。ただし、許可されたアプリケーションのリストは、必要に応じてさらに設定できます。

- **Cisco Phone** = com.cisco.phone
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- **Web API** = com.cisco.webapi
- **Webex** = com.cisco.wx2.android

Deployment Configuration Initial Provisioning

Choose Application

Set Allow-List of Applications

com.cisco.phone x com.cisco.ptt x
 com.cisco.emergency x com.cisco.webapi x
 com.cisco.wx2.android x + New Tag

Set Title of Launcher Application

以下は、Cisco Wireless Phone 840 および 860 にプレインストールされているアプリケーションのリストです。これらのアプリケーションを許可しない場合は、Device Policy Controller の設定に追加するか（**[設定 (Settings)]** アプリケーションを除く）、スマートランチャーの設定に追加して、スマートランチャービューからアクセスできるようにする必要があります。

シスコのプリインストールアプリケーション

- **Barcode** = com.cisco.barcode.service
- **Battery Life** = com.cisco.batterylife
- **Buttons** = com.cisco.buttons
- **Call Quality Settings** = com.cisco.callquality
- **Custom Settings** = com.cisco.customsettings
- **Diagnostics** = com.cisco.diagnostics
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- **Sound Stage** = com.cisco.soundstage
- **Web API** = com.cisco.webapi
- **Webex** = com.cisco.wx2.android

その他のプリインストールされたアプリケーション

- **Calculator** = com.google.android.calculator
- **Calendar** = com.google.android.calendar
- **Camera** = com.android.camera2
- **Chrome** = com.android.chrome
- **Clock** = com.android.deskclock
- **Contacts** = com.google.android.contacts

- **Digital Wellbeing** = com.google.android.apps.wellbeing
- **Drive** = com.google.android.apps.docs
- **Duo** = com.google.android.apps.tachyon
- **Files** = com.google.android.documentsui
- **Gmail** = com.google.android.gm
- **Google** = com.google.android.googlequicksearchbox
- **Google TV** = com.google.android.videos
- **Keep Notes** = com.google.android.keep
- **Maps** = com.google.android.apps.maps
- **Photos** = com.google.android.apps.photos
- **Play Store** = com.android.vending
- **Settings** = com.android.settings
- **Sound Recorder** = com.android.soundrecorder
- **YouTube** = com.google.android.youtube
- **YT Music** = com.google.android.apps.youtube.music

注：スマートランチャーは、Cisco Phone アプリケーションのみを許可することで、電話専用モードに設定できます。

設定アプリケーションとその他の重要なアプリケーションが Device Policy Controller の設定で許可されていないことを確認します。

コンフィギュレーションファイルのエクスポート

必要なアプリケーション設定の変更がすべて完了し、設定を保存する準備ができたなら、**[エクスポート (Export)]** を選択します。

変更内容を確認するための確認画面が表示されます。

ファイルを保護するには、**[エクスポート (Export)]** を選択する前に、**[設定の暗号化 (Encrypt Configuration)]** がオンになっていることを確認します (デフォルト設定)。

変更が確認されたら、**[エクスポート (Export)]** を選択します。



Device Policy Controller

Parameter	Prior Value	New Value
Wi-Fi Profile Length	0	1
Wi-Fi Profile 1-> Security	None	WPA2- Personal
Wi-Fi Profile 1-> SSID		cisco
Wi-Fi Profile 1-> Password		password

Copy Config

 Encrypt Configuration

Export

設定ファイルは、次のファイルを含む ZIP 形式 (CP8x0_config_6-8-2023.zip など) でエクスポートされます。

- **CP8x0_config_<MM-DD-YYYY>.json.enc**= Cisco Unified Communications Manager にアップロードされる暗号化された設定ファイル
- **CP8x0_key_<MM-DD-YYYY.txt**= Encryption key used to encrypt the config file

複数のファイルが Cisco Unified Communications Manager にアップロードされる場合は、必要に応じて **CP8x0_config_<MM-DD-YYYY>.json.enc** ファイルの名前を変更できます。

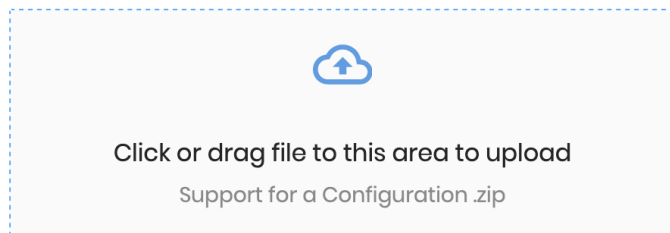
注：暗号化されていない設定オプションは、トラブルシューティング専用です。

Import Configuration Files

以前にエクスポートした ZIP ファイルを使用して追加の設定変更を行う場合は、**[インポート (Import)]** を選択します。

保存した ZIP ファイルを **[インポート設定 (Import Configuration)]** ウィンドウにドラッグし、**[インポート (Import)]** を選択します。

The Import Configuration upload allows you to upload a .zip file containing configuration parameters and values exported from this tool using the export functionality.



📎 CP8x0_config_6-8-2023.zip

Import

注： 以前に保存した ZIP ファイルが変更されていないことを確認します。

ZIP ファイルの名前は変更できますが、インポートが失敗するため、内部ファイルを変更することはできません。

Cisco Unified Communications Manager の設定

Cisco Wireless Phone Configuration Management ユーティリティを使用するように Cisco Unified Communications Manager を設定するには、次のガイドラインを使用します。

TFTP 暗号化を使用したセキュア プロファイルの作成

Cisco Wireless Phone Configuration Management ユーティリティからエクスポートされたファイルをホストするように Cisco Unified Communications Manager を設定する前に、TFTP 暗号化が有効になっているセキュア プロファイルを使用するように Cisco Wireless Phone 840 および 860 を設定する必要があります。Cisco 無線電話 840 および 860 をクリア テキストで入力します。

Phone Security Profile Information

Product Type: Cisco 840

Device Protocol: SIP

Name*

Description

Nonce Validity Time*

Device Security Mode ▼

Transport Type* ▼

Enable Digest Authentication

TFTP Encrypted Config

Phone Security Profile Information

Product Type: Cisco 860

Device Protocol: SIP

Name*

Description

Nonce Validity Time*

Device Security Mode ▼

Transport Type* ▼

Enable Digest Authentication

TFTP Encrypted Config

セキュリティ プロファイルを作成したら、そのプロファイルを Cisco Wireless Phone 840 および 860 に適用して、Cisco Wireless Phone 840 および 860 の設定ファイルの 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。

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

SRTP Allowed - When this flag is checked, IPSec needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

BLF Presence Group*

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

Media Termination Point Required

Unattended Port

Require DTMF Reception

Early Offer support for voice and video calls (insert MTP if needed)

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

SRTP Allowed - When this flag is checked, IPSec needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

BLF Presence Group*

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

Media Termination Point Required

Unattended Port

Require DTMF Reception

Early Offer support for voice and video calls (insert MTP if needed)

Upload Configuration Files

ダウンロードした暗号化 ZIP ファイルから **CP8x0_config_json.enc** ファイルを抽出し、[Cisco Unified OS の管理 (Cisco Unified OS Administration)] ページから TFTP サービスを実行しているすべての Cisco Unified Communications Manager ノードにファイルをアップロードします。<MM-DD-YYYY>次に、すべてのノードの TFTP サービスを再起動します。

必要に応じて、Cisco Unified Communications Manager の [サーバーのロード (Load Server)] オプションを使用して、設定ファイルをホストできます。

注： **CP8x0_config_<MM-DD-YYYY>.json.enc** ファイルは、複数のファイルが Cisco Unified Communications Manager にアップロードされる場合に備えて、必要に応じて名前を変更できます。

Cisco Wireless Phone 840 および 860 製品固有の設定オプションの設定

Cisco Wireless Phone 840 および 860 は、ダウンロードするファイルと、ファイルの復号に使用する暗号キーを通知するように設定する必要があります。

エンタープライズ モビリティ管理 (EMM) 代替設定製品固有の設定オプションを、抽出したファイルの名前 (例: CP8x0_config_<MM-DD-YYYY>.json.enc またはファイルの名前が変更された名前) を使用して設定します。

エンタープライズ モビリティ管理 (EMM) 代替構成暗号化キーの製品固有の設定オプションを、抽出したファイル (CP8x0_key_<MM-DD-YYYY.txt) を使用して設定します。

Enterprise Mobility Management (EMM) Alternative Configuration	<input type="text"/>
Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key	<input type="text"/>

電話ロック解除パスワードの設定

[電話ロック解除パスワード (Local Phone Unlock Password)] (デフォルト = **#) は、スマートランチャーを終了し、標準の Android インターフェイスにアクセスするために使用できます。[Device (デバイス)] > [Device Settings (デバイス設定)] > [Common Phone Profile (共通の電話プロファイル)] の [Common Phone Profile (共通の電話プロファイル)] で [電話ロック解除パスワード (Local Phone Unlock Password)] を設定し、Cisco Wireless Phone 840 および 860 に適用することをお勧めします。

Common Phone Profile Information	
Name *	<input type="text" value="Standard Common Phone Profile"/>
Description	<input type="text" value="Standard Common Phone Profile"/>
Local Phone Unlock Password	<input type="text"/>
DND Option *	<input type="text" value="Ringer Off"/>
DND Incoming Call Alert*	<input type="text" value="Beep Only"/>
Feature Control Policy	<input type="text" value="< None >"/>
Wi-Fi Hotspot Profile	<input type="text" value="< None >"/> View Details
<input checked="" type="checkbox"/> Enable End User Access to Phone Background Image Setting	

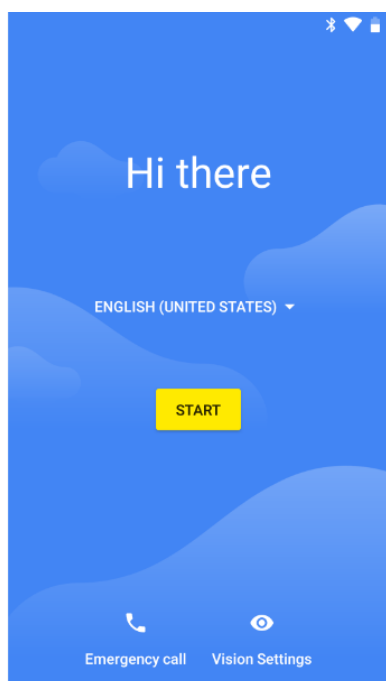
Cisco Wireless Phone 840 および 860 の登録

Cisco Wireless Phone Configuration Management ユーティリティを使用するには、最初に Cisco Wireless Phone 840 および 860 をファームウェア 1.5(0) 以降にアップグレードする必要があります。

Cisco Wireless Phone 840 および 860 を 1.5(0) 以降にアップグレードしたら、[設定 (Settings)]、[システム (System)]、[詳細 (Advanced)]、[オプションのリセット (Reset options)]、[すべてのデータの消去 (工場出荷時のリセット) (Erase all data (factory reset))] の順に選択して、工場出荷時の状態にリセットする必要があります。

注：Cisco Wireless Phone 840 および 860 が Cisco Wireless Phone Configuration Management ユーティリティに登録されると、は電話機を工場出荷時の状態にリセットすることなく、後続の更新をプッシュできます。

起動画面で、ディスプレイをすばやく 6 回タップすると、QR コードをスキャンして Cisco Wireless Phone 840 または 860 を Cisco Wireless Phone Configuration Management ユーティリティに登録するように求められます。



Cisco Wireless Phone Configuration Management ユーティリティの [初期プロビジョニング (Initial Provisioning)] タブで、初期プロビジョニングに使用する Wi-Fi ネットワーク パラメータとオプションの電話ロック解除ピン/パスワードを設定します。

次のセキュリティ設定がサポートされています。

[セキュリティモード (Security Mode)]	EAP 方法	フェース 2 認証
なし	該当なし	なし
WPA2-Personal	該当なし	なし
WPA2-Enterprise	PEAP	GTC、MSCHAPV2
WPA2-Enterprise	TTLS	GTC、MSCHAP、MSCHAPV2、PAP

注：Cisco Wireless Phone Configuration Management Utility は、EAP-TLS (TLS) をサポートしていません。

オープン Wi-Fi ネットワークに接続するには、**SSID** を入力し、[セキュリティ (Security)] を [なし (None)] に設定します。

Webex Wireless Phone Configuration Management

Deployment Configuration Initial Provisioning

Scan 'n' Go Provisioning

Wi-Fi Configuration

Security: None

* SSID:

Hidden SSID:

Security

Phone Unlock Pin/Password:

Generate

PSK 対応の Wi-Fi ネットワークに接続するには、**SSID** を入力し、[セキュリティ (Security)] を [WPA2-個人 (WPA2-Personal)] に設定してから、8-63 ASCII または 64 HEX パスワードを入力します。

Deployment Configuration Initial Provisioning

Scan 'n' Go Provisioning

Wi-Fi Configuration

Security: WPA2-Personal

* SSID:

* Password:

Hidden SSID:

Security

Phone Unlock Pin/Password:

EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [WPA2-EAP] に設定してから、[認証方式 (Authentication method)] を選択します。

PEAP または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、フェーズ 2 認証方式を選択し、必要に応じてヘッダーとフッターを除いた Base-64 (PEM) エンコーディング形式で CA 証明書を設定し、ID とパスワードを入力します。

Deployment Configuration Initial Provisioning

Scan 'n' Go Provisioning

Wi-Fi Configuration

Security: WPA2-Enterprise

* SSID:

* Password:

Hidden SSID:

Security

Phone Unlock Pin/Password:

EAP Configuration

EAP Method: PEAP

Phase 2 Authentication: MSCHAPV2

Domain:

* Identity:

Anonymous Identity:

CA Certificate:

注：ブロードキャストされていない Wi-Fi ネットワークは、**非表示の SSID** として設定する必要があります。それ以外の場合、Wi-Fi ネットワークは範囲内に表示されません。非ブロードキャスト Wi-Fi ネットワークに接続するには、**[非表示 SSID (Hidden SSID)]** を **[はい (True)]** に設定します。

設定された Wi-Fi ネットワークが、DHCP オプション 150 または DHCP オプション 66 を介して Cisco Unified Communications Manager を指していることを確認します。それ以外の場合は、Cisco Wireless Phone 840 および 860 の電話アプリケーションで TFTP サーバーを手動で設定する必要があります。

ヘッダーとフッターが削除され、スペースや改行が含まれていない CA 証明書の形式が正しいことを確認します。

[生成 (Generate)] を選択して QR コードを作成すると、QR コードが表示されます。

QR Code

Scan this QR code on your Webex wireless phone device by tapping six times on the "Hi there" text on the Welcome screen



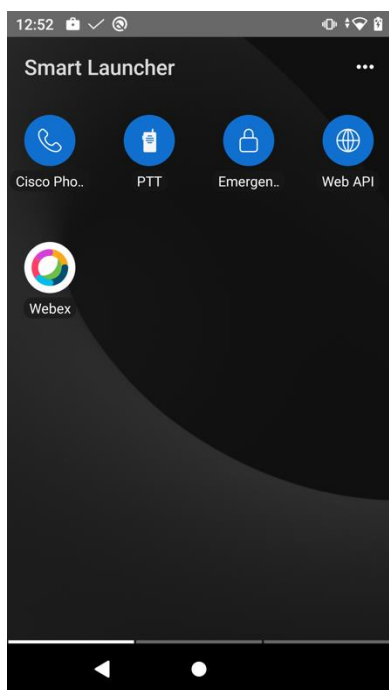
Done

注：QR コードを正常に生成するには、CA 証明書の文字を含む合計文字数が 2041 文字を超えないようにする必要があります。

Cisco Wireless Phone 840 または 860 で QR コードをスキャンします。

Cisco Wireless Phone 840 または 860 が近くにはない場合に備えて、QR コードを保存できます。その場合は、QR コードを PDF ファイルまたはスクリーンショットとして保存することをお勧めします。PNG ファイルとしてファイルを保存するとファイルが変更され、QR コードのスキャンが失敗します。

Cisco Wireless Phone 840 および 860 は、指定されたファイルを Cisco Unified Communications Manager からダウンロードし、それに応じてアプリケーションとその他の設定を更新しようとします。



注：Cisco Wireless Phone 840 および 860 は、設定された Wi-Fi ネットワークの範囲内にある必要があります。範囲内がない場合、セットアップは失敗します。

手動設定

ローカル ユーザ インターフェイスを介して Cisco Wireless Phone 840 および 860 を手動で設定するには、次のガイドラインを使用します。

Wi-Fi プロファイルの設定

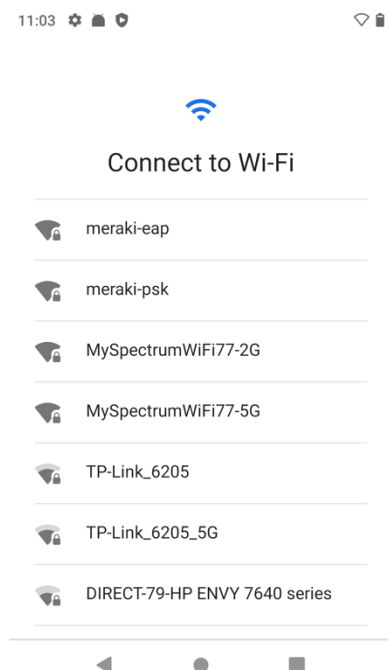
ローカル ユーザー インターフェイスを介して Wi-Fi ネットワークを手動で設定するには、次のガイドラインを使用します。

- ・ 初期状態の電話機または工場出荷時の状態にリセットされた電話機の場合は、スタートアップウィザードを使用して Wi-Fi ネットワークを構成するか、**[オフラインでセットアップ (Set up offline)]** を選択します。
- ・ 構成オプションは、ブロードキャストされた Wi-Fi ネットワークが構成されているか、Wi-Fi ネットワークが手動で構成されているかによって決まります。
- ・ 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。

[セキュリティモード (Security Mode)]	EAP 方法	キーの管理	暗号化
なし	該当なし	なし	なし
WPA2-Personal	該当なし	WPA2	AES
WPA2-Enterprise	PEAP	WPA2	AES
WPA2-Enterprise	TLS	WPA2	AES
WPA2-Enterprise	TTLS	WPA2	AES

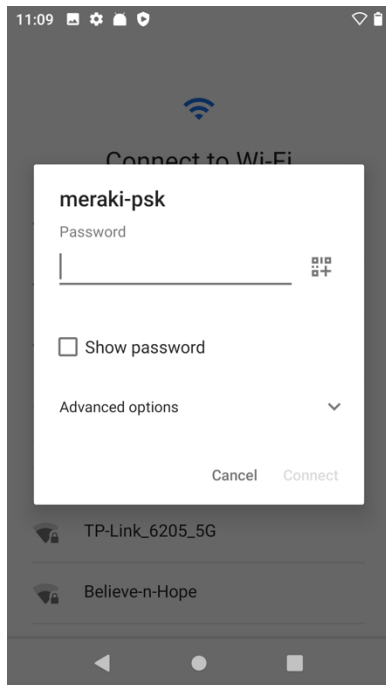
ブロードキャスト Wi-Fi ネットワークの設定

- ・ Wi-Fi ネットワークがブロードキャストされている場合は、スタートアップウィザード経由でリストから目的の Wi-Fi ネットワークを選択し、Wi-Fi ネットワークのセキュリティ設定に応じて必要なログイン情報を入力します。
- ・ ブロードキャスト Wi-Fi ネットワークを（スタートアップウィザードを使用せずに）オフラインで設定する場合は、電話機のディスプレイを下から上にスワイプして、インストールされているアプリケーションを表示し、**[設定 (Settings)] > [ネットワークとインターネット (Network and Internet)] > [Wi-Fi]** を選択して Wi-Fi ネットワークを設定します。。

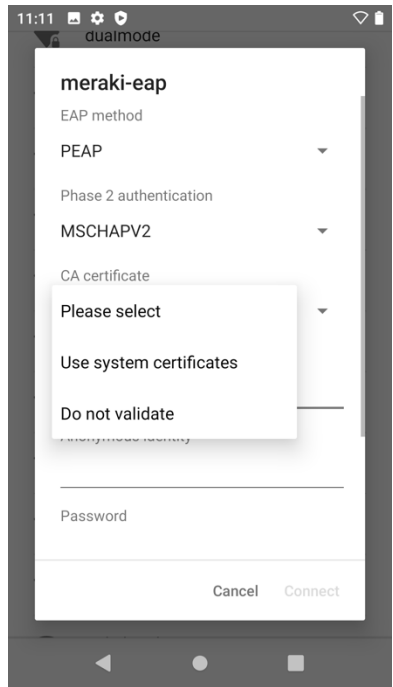
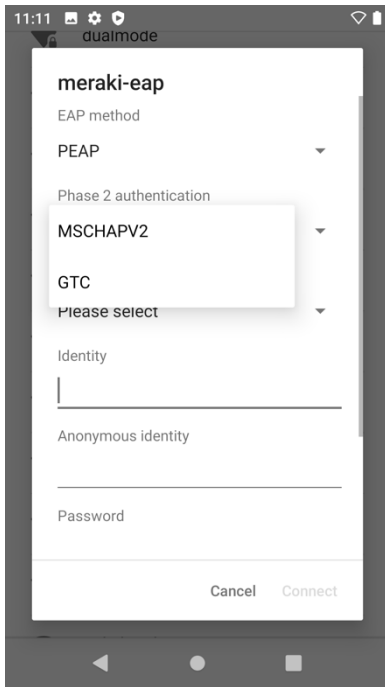
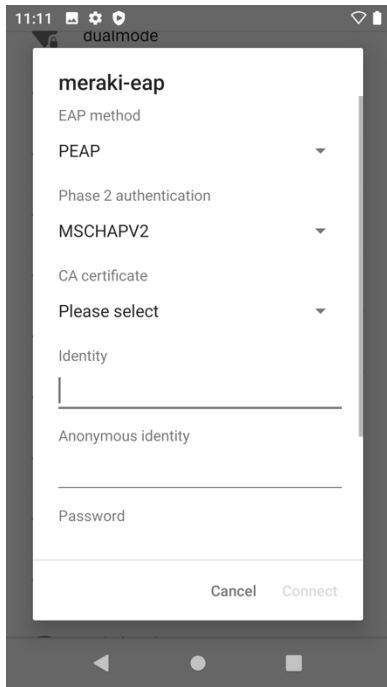
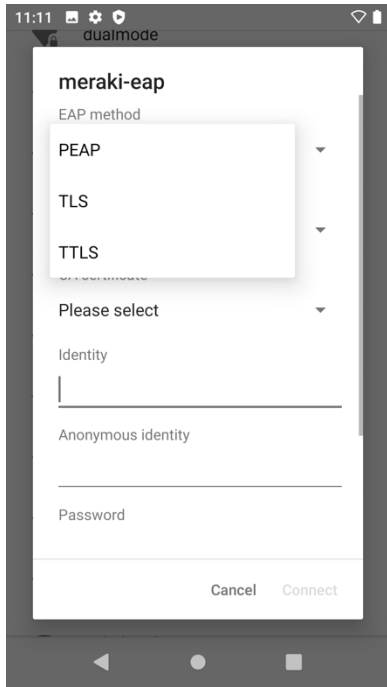


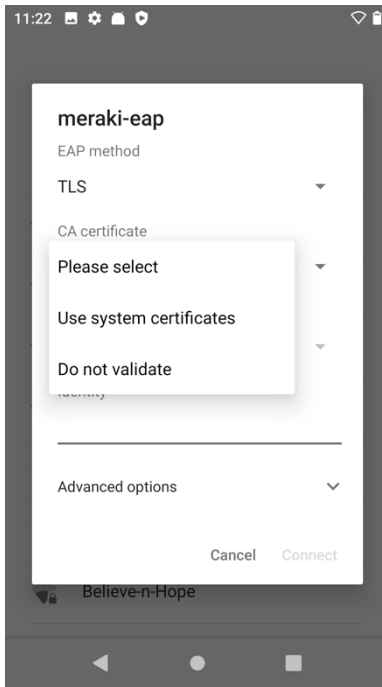
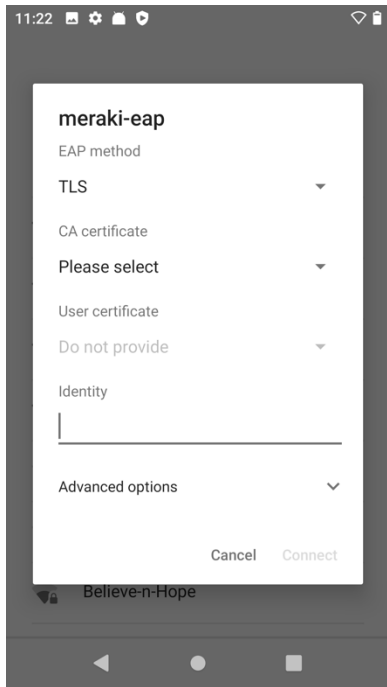
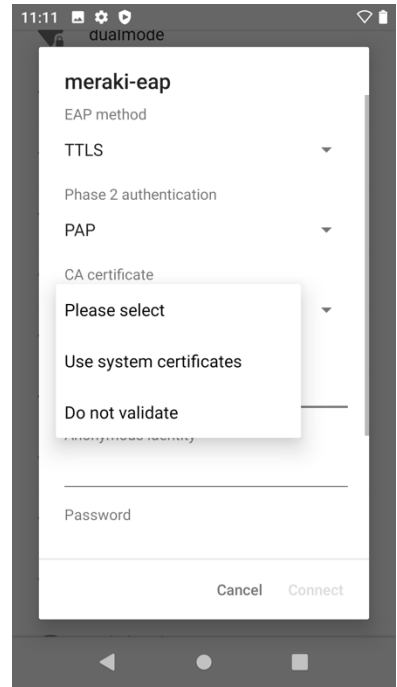
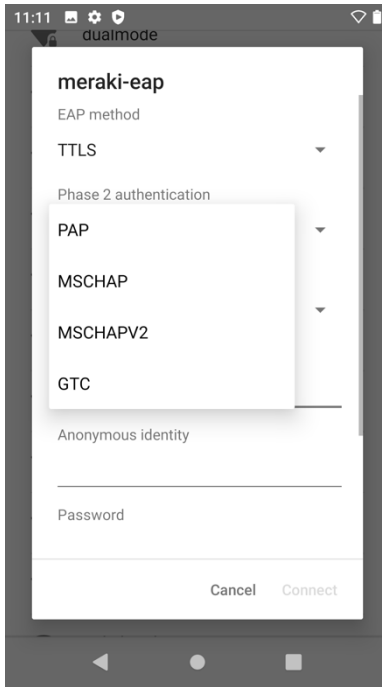
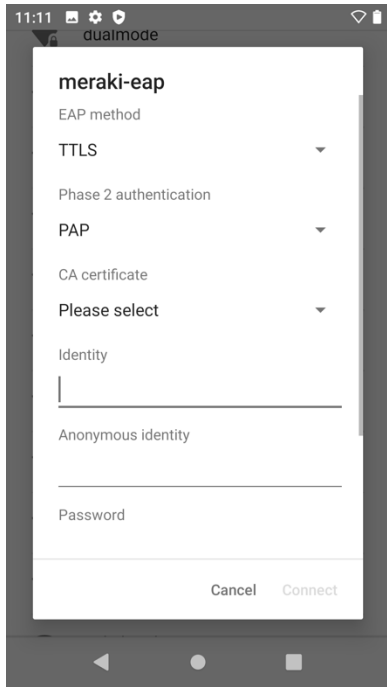
- ・ オープン Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックするだけです。

- ・ PSK 対応の Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックし、8-63 ASCII または 64 HEX パスワードを入力します。



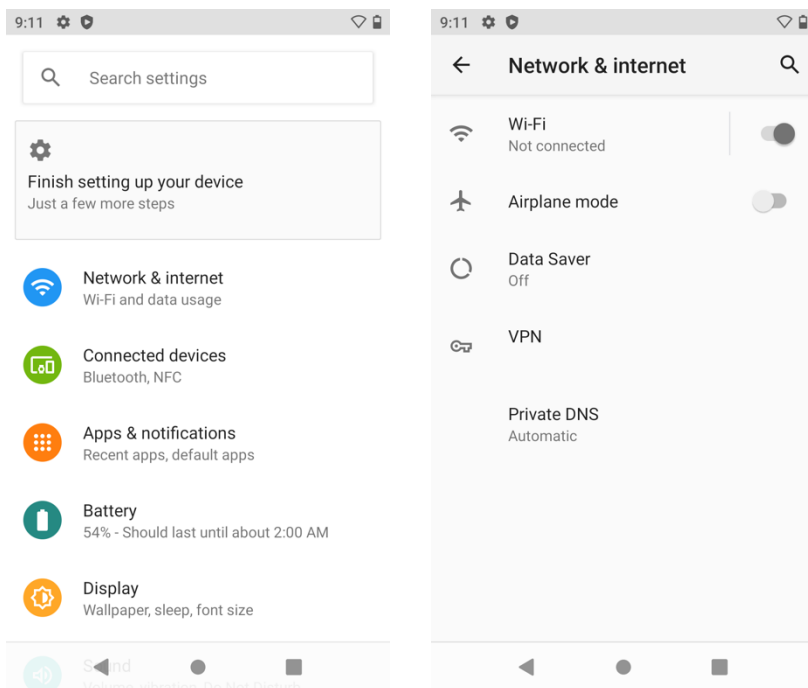
- ・ EAP 対応 Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックしてから、**[EAP 方式]** を選択します。
- ・ PEAP または EAP-TTLS (TTLS) の Wi-Fi ネットワークを設定する場合は、使用する**フェーズ 2 認証方式**と **CA 証明書**オプションを選択し、**ID** と**パスワード**を入力します。
- ・ EAP-TLS (TLS) Wi-Fi ネットワークを設定する場合は、使用する **[ユーザー証明書 (User certificate)]** および **[CA 証明書 (CA certificate)]** オプションを選択します。



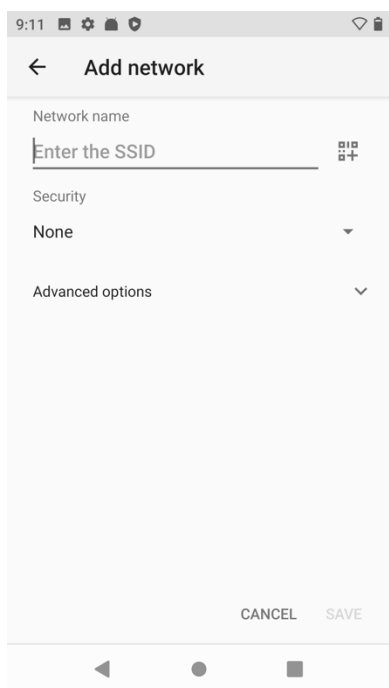


非ブロードキャスト Wi-Fi ネットワークの設定

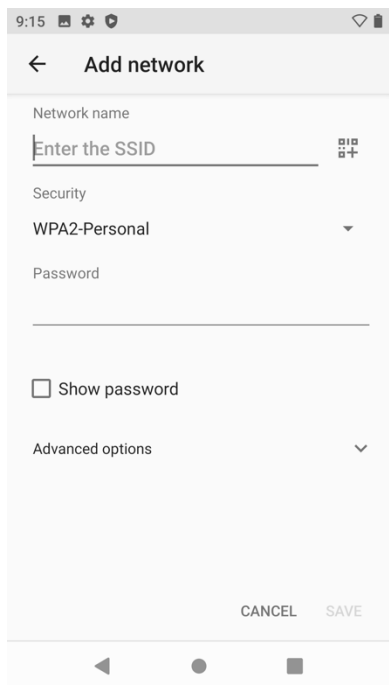
- ・ 非ブロードキャスト（非表示）Wi-Fi ネットワークを手動で設定する場合は、電話機のディスプレイを下から上にスワイプして、インストールされているアプリケーションを表示し、**[設定 (Settings)]** > **[ネットワークとインターネット (Network and Internet)]** > **[Wi-Fi]** を選択します。
- ・ Wi-Fi 設定の一番下で、**[ネットワークの追加 (Add Network)]** を選択し、ネットワーク名 (SSID)、セキュリティタイプを設定し、Wi-Fi ネットワークのセキュリティ設定に応じて必要なログイン情報を入力します。
- ・ ブロードキャストされていない Wi-Fi ネットワークは、Wi-Fi ネットワーク設定の**[詳細オプション (Advanced options)]** セクションで非表示ネットワークとしてマークする必要もあります。それ以外の場合、Wi-Fi ネットワークは範囲内にないと表示されます。



- ・ オープン Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、**[セキュリティ (Security)]** を **[なし (None)]** に設定します。

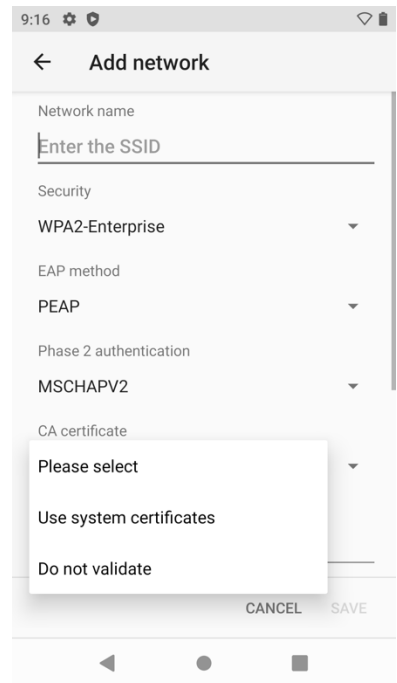
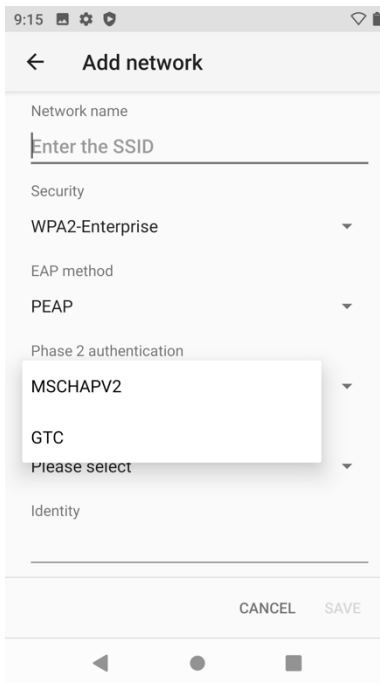
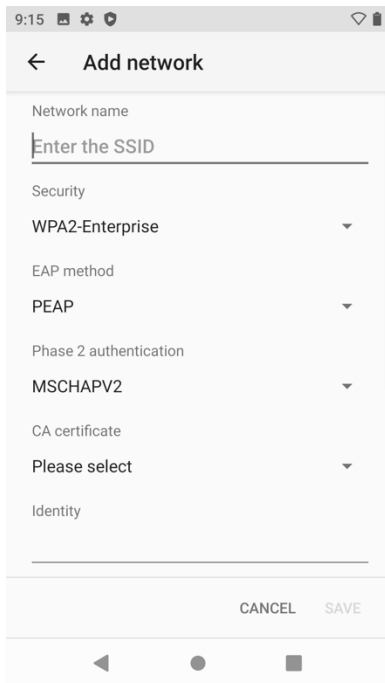
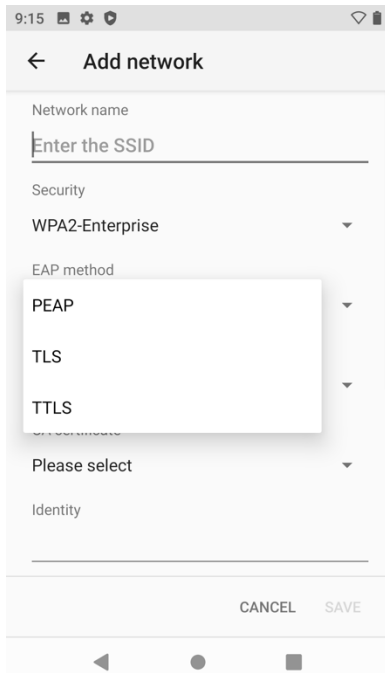


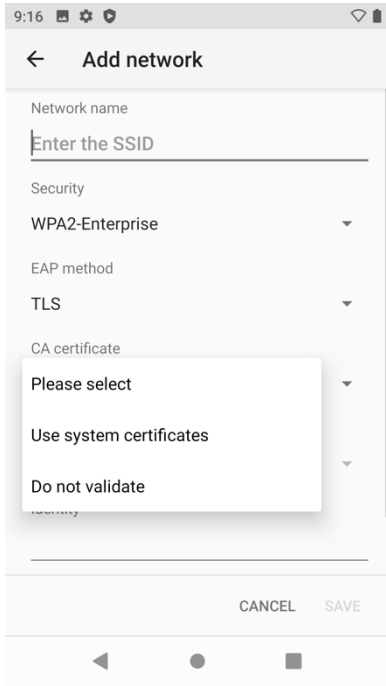
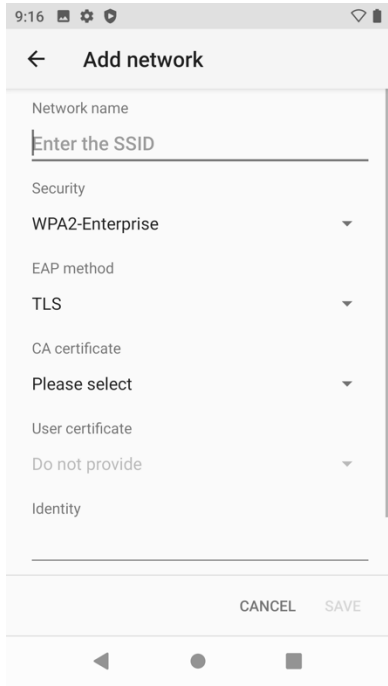
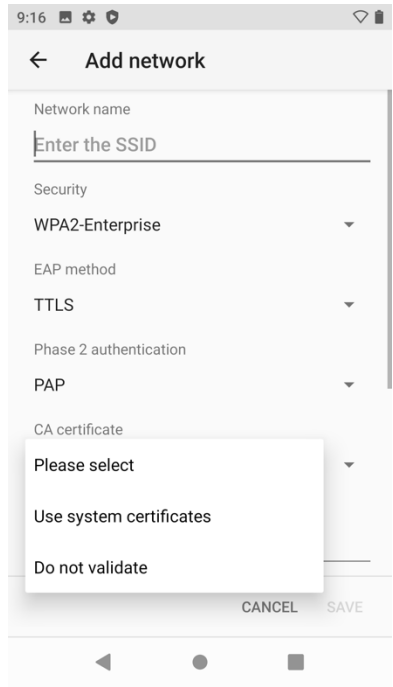
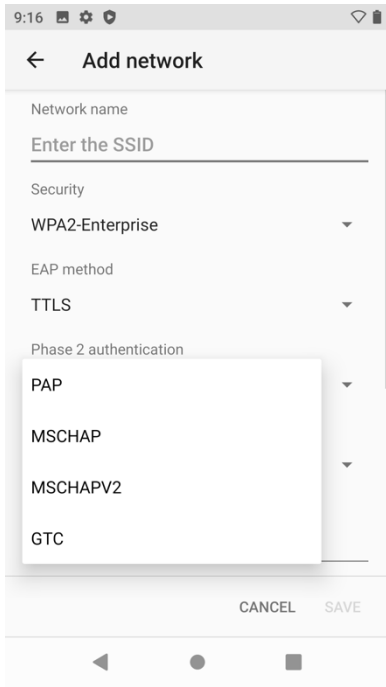
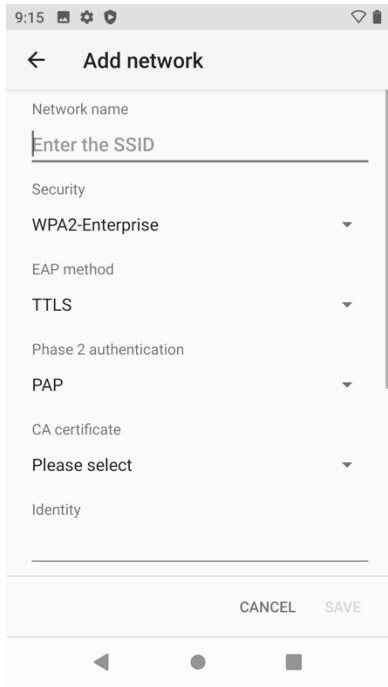
- ・ PSK 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [WPA2-個人 (WPA2-Personal)] に設定してから、8-63 ASCII または 64 HEX パスワードを入力します。



- ・ EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [WPA2-企業 (WPA2-Enterprise)] に設定してから、[EAP 方式 (EAP method)] を選択します。

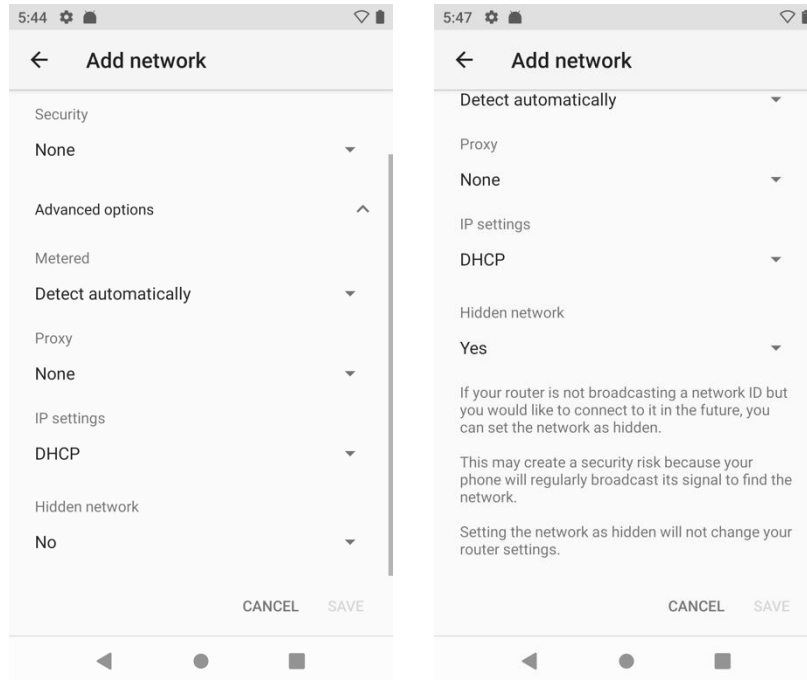
- PEAP または EAP-TTLS (TTLS) の Wi-Fi ネットワークを設定する場合は、使用するフェーズ 2 認証方式と CA 証明書オプションを選択し、ID とパスワードを入力します。
- EAP-TLS (TLS) Wi-Fi ネットワークを設定する場合は、使用する [ユーザー証明書 (User certificate)] および [CA 証明書 (CA certificate)] オプションを選択します。



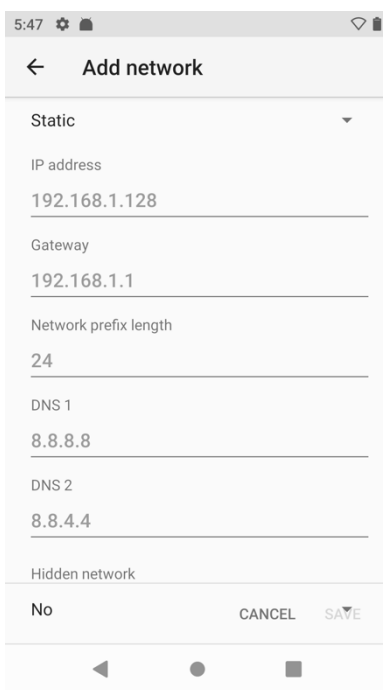
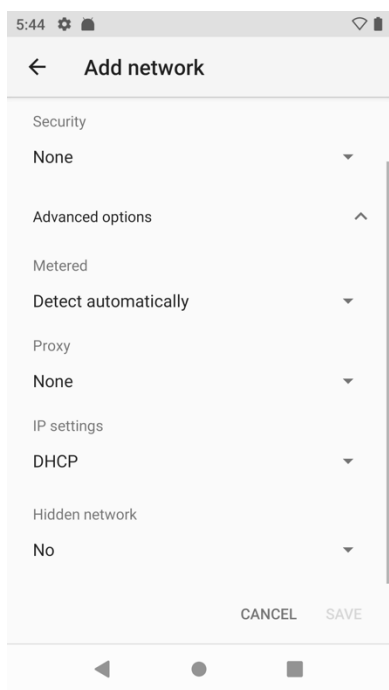


Wi-Fi ネットワークの詳細オプションの設定

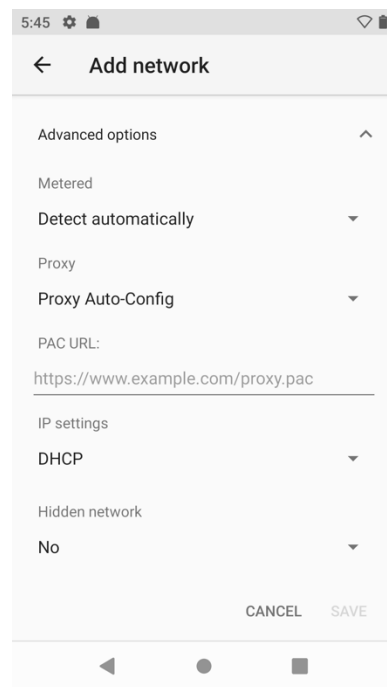
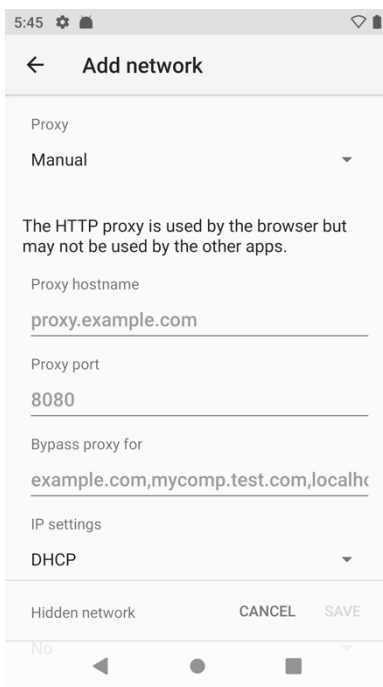
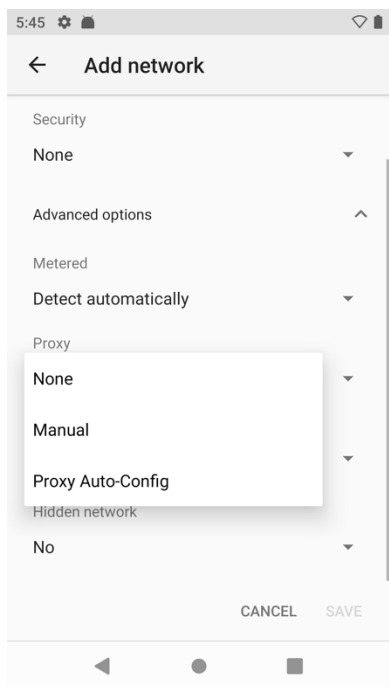
- ・ 非ブロードキャスト Wi-Fi ネットワークは、Wi-Fi ネットワーク設定の **【詳細オプション (Advanced options)】** セクションで非表示ネットワークとして設定する必要があります。それ以外の場合、Wi-Fi ネットワークは範囲内に表示されません。
- ・ 非ブロードキャスト Wi-Fi ネットワークに接続するには、**【非表示ネットワーク (Hidden network)】** を **【はい (Yes)】** に設定します。



- ・ IP 設定（静的または DHCP 設定）は、Wi-Fi ネットワーク設定の **【詳細オプション (Advanced options)】** セクションで設定できます。

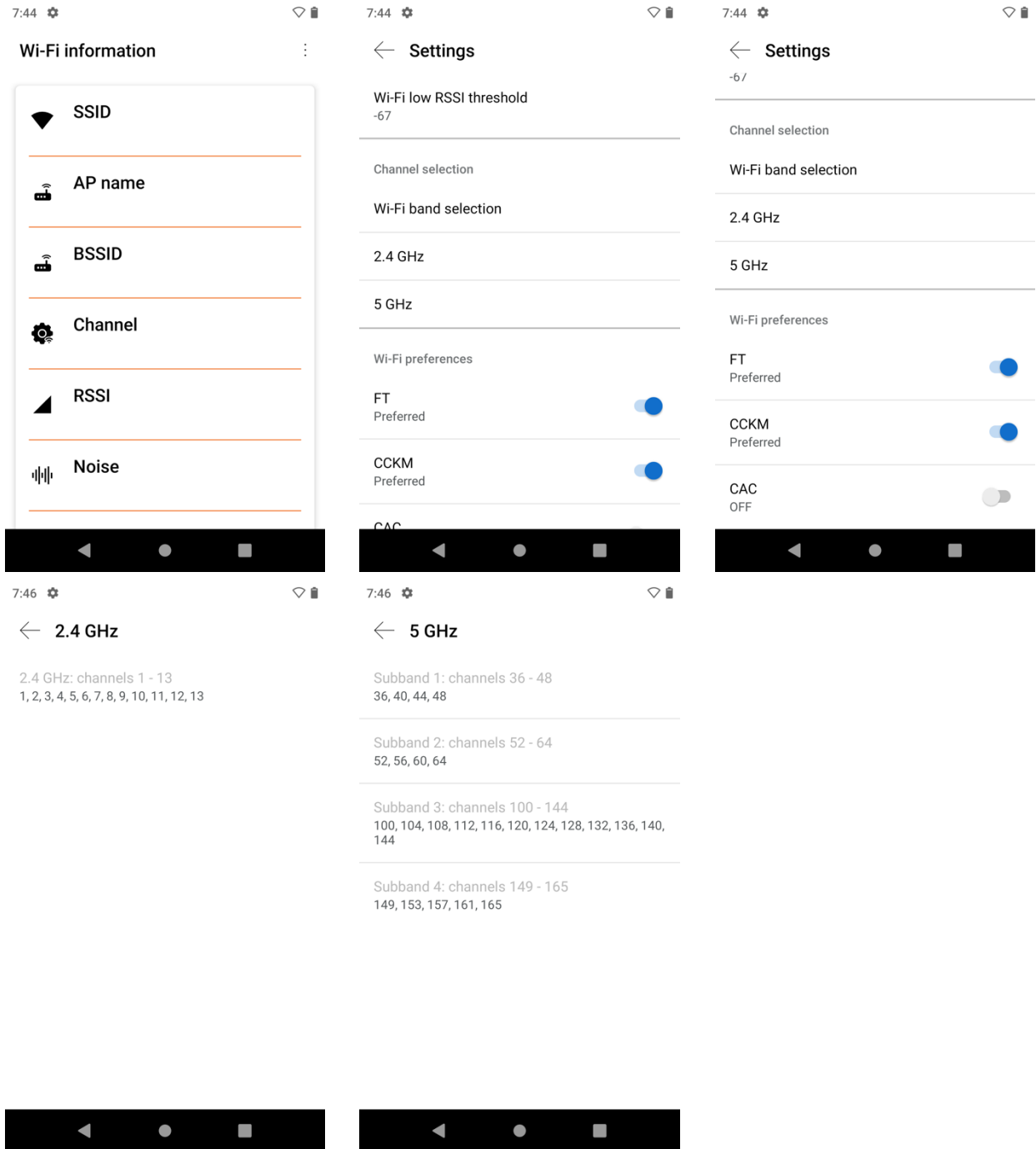


- ・ プロキシ設定は、Wi-Fi ネットワーク設定の **[詳細オプション (Advanced options)]** セクションで設定できます。

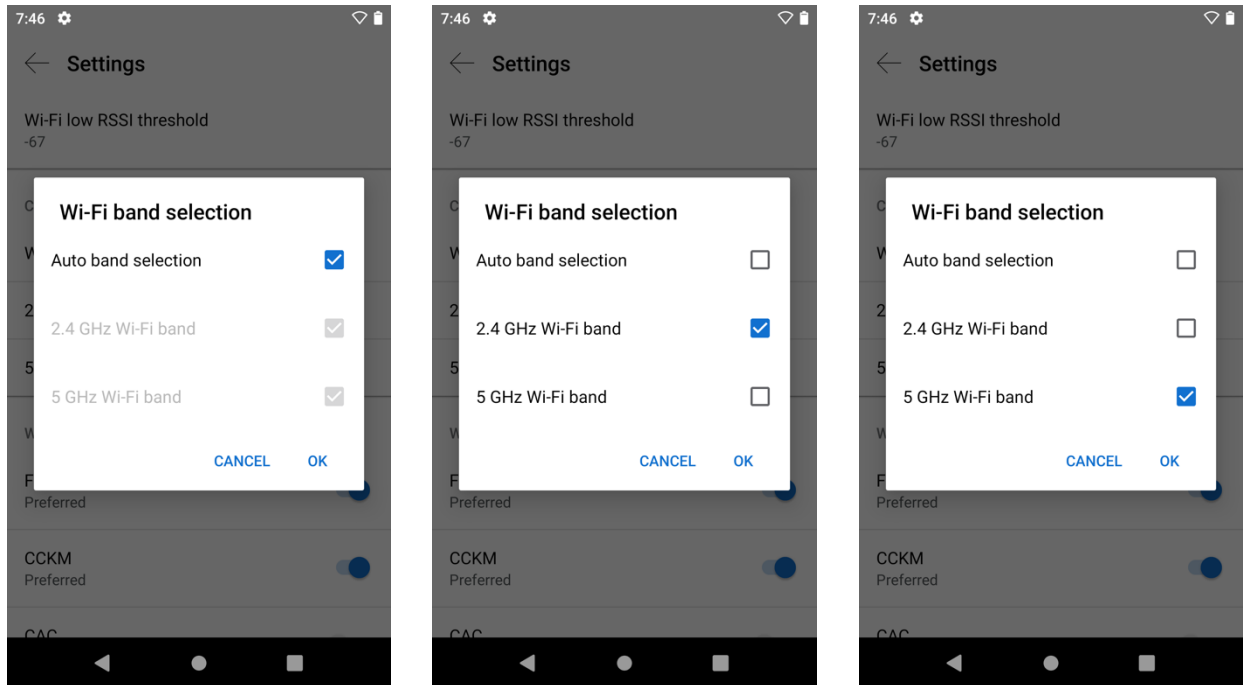


通話品質設定の設定

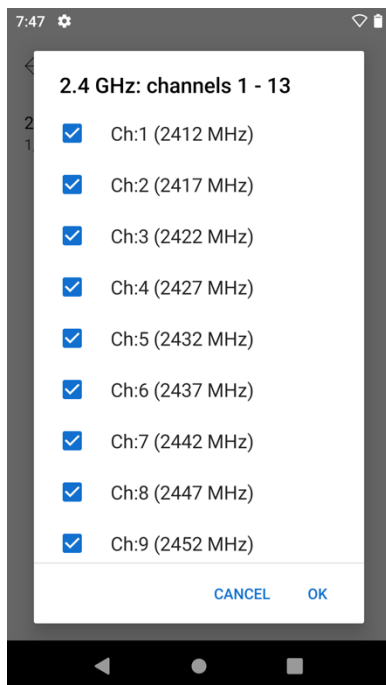
- 有効なチャネルを含む **Wi-Fi 帯域選択** (自動、2.4 GHz、5 GHz)、高速セキュア ローミング設定 (**FT** および **CCKM**)、および **Wi-Fi 低 RSSI しきい値**は、右上の 3 つの点を選択して設定できます。[**コール品質設定 (Call Quality Settings)**] アプリケーションで、[**設定 (Settings)**] を選択します。

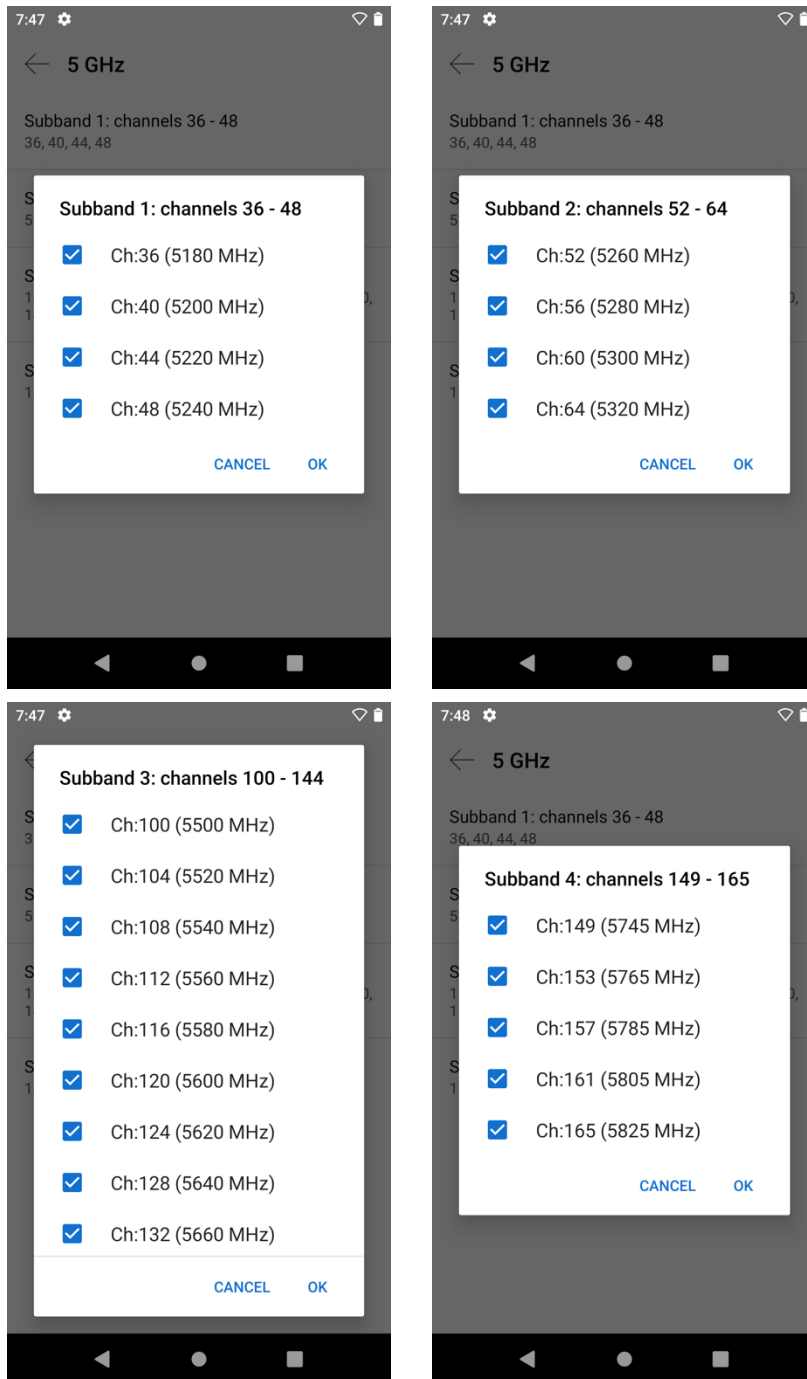


- 単一の Wi-Fi 周波数帯域を使用する場合、または Wi-Fi 周波数帯域ごとに有効にするチャンネルを制限する場合は、**[Wi-Fi 帯域選択 (Wi-Fi Band Selection)]** を選択し、**[自動 (Auto)]** をオフにして、2.4 GHz Wi-Fi 帯域のみ、5 GHz Wi-Fi 帯域のみ、または 2.4 GHz と 5 GHz の両方を使用する場合は両方。

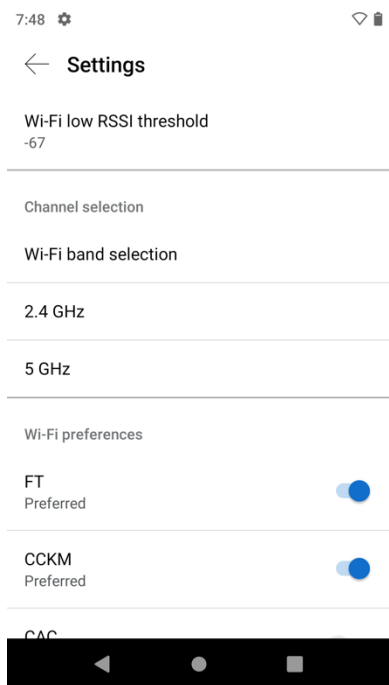


- [自動 (Auto)]** がオフの場合、目的のチャンネルセットをクリックするだけで、Wi-Fi 周波数帯域ごとに有効にするチャンネルを設定できます。





- ・ 高速セキュア ローミングに 802.11r (FT) を使用する場合は、**FT** のスライダが右側にある **【優先 (Preferred)】** に設定されていることを確認します。
- ・ 高速セキュア ローミングに CCKM を使用する場合は、**CCKM** のスライダが **【優先 (Preferred)】** に設定されていることを確認します。
- ・ **FT** と **CCKM** の両方が **【優先 (Preferred)】** に設定されている場合、802.11r (FT) が CCKM よりも優先されます。



注：EAP-TLS、EAP-TTLS、または PEAP を使用し、802.11r (FT) を優先に設定している場合は、アクセスポイントで有効になっている 802.11r (FT) または CCKM がネゴシエートされます。

1.8(0) リリースでは、**CAC** (コール アドミッション コントロール) を無効にするオプションが有効になっています。

1.9(0) リリースでは、**CAC** (コールアドミッション コントロール) はデフォルトで無効になっており、オプション機能になりました。

WPA3 はサポートされていません。

802.1x-SHA2 キー管理はサポートされていません。

CCMP256、GCMP128、および GCMP256 暗号化方式はサポートされていません。

詳細については、次の URL にある『**Cisco Wireless Phone 840 および 860 アドミニストレーション ガイド**』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

証明書管理

Cisco Wireless Phone 840 および 860 では、**EAP-TLS** に X.509 デジタル証明書を使用できます。**EAP-TTLS** または **PEAP** を使用する場合は、X.509 デジタル証明書を使用してサーバ検証を有効にできます。

EAP-TLS を使用する場合は、日付と時刻が正しく設定されていることを確認する必要があります。

クライアントおよびサーバ証明書では、DER と Base-64 (PEM) の両方のエンコーディングが使用できます。キー サイズが 1024、2048、および 4096 の証明書がサポートされます。

クライアントおよびサーバ証明書が 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。

Microsoft® 認証局 (CA) サーバを使用することを推奨します。他の CA サーバタイプは、Cisco Wireless Phone 840 および 860 との完全な相互運用性がない場合があります。

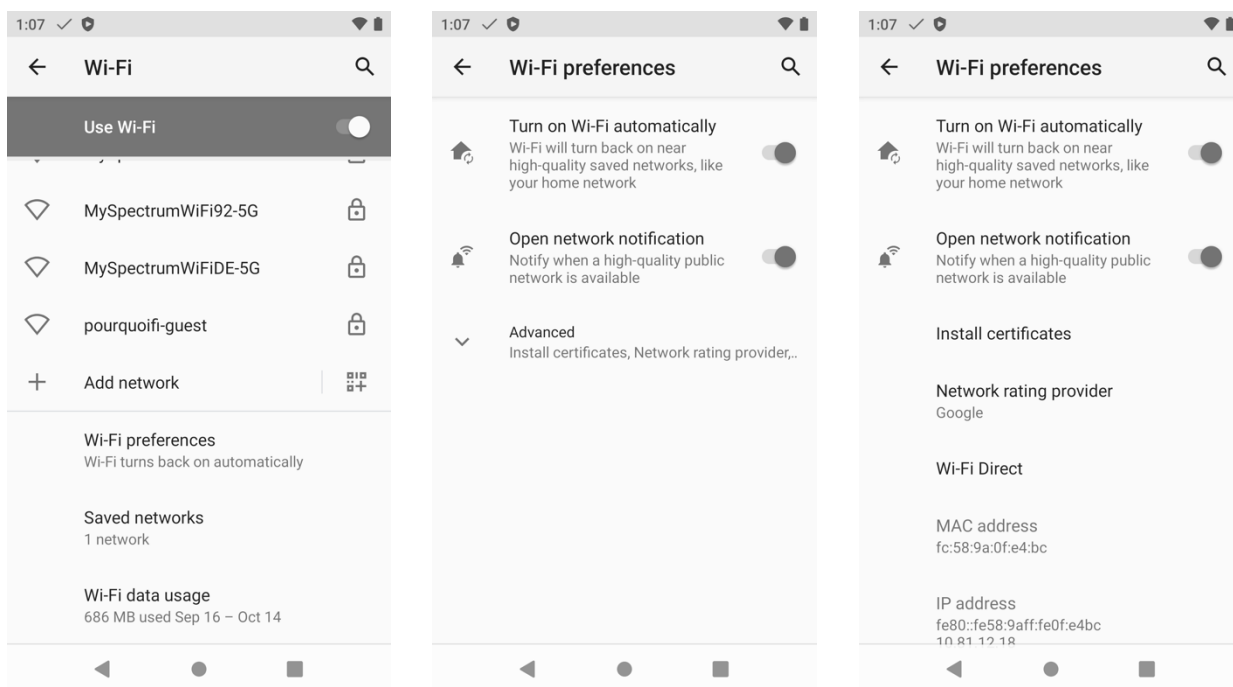
証明書のインストール

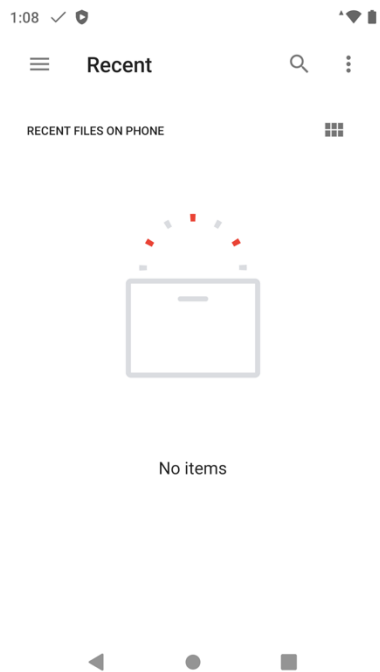
証明書は、EMM でサポートされている場合、エンタープライズ モビリティ管理 (EMM) アプリケーションを介して自動的にインストールできます。詳細は、EMM ドキュメントを参照してください。

証明書は、Wi-Fi 設定またはセキュリティ設定で手動でインストールすることもできます。

Wi-Fi 設定を使用して証明書を手動でインストールするには、[設定 (Settings)]、[ネットワークとインターネット (Network and Internet)]、[Wi-Fi]、[Wi-Fi 設定 (Wi-Fi Preferences)]、[詳細 (Advanced)] の順に選択し、[証明書のインストール (Install certificates)] を選択します。

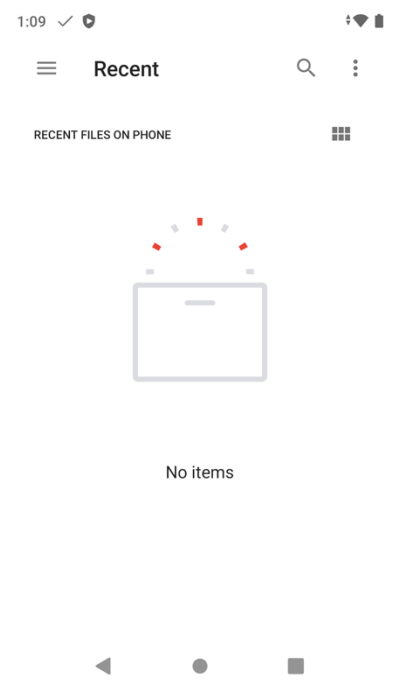
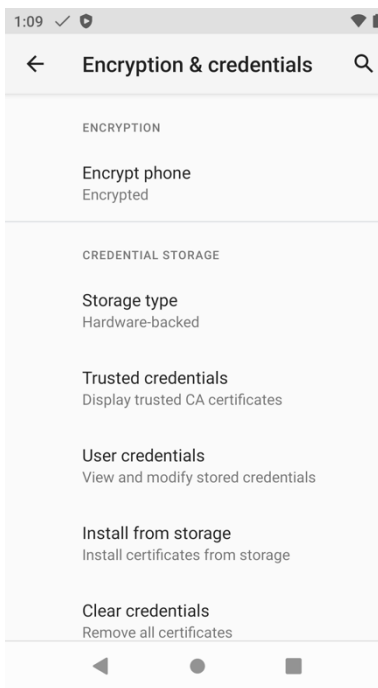
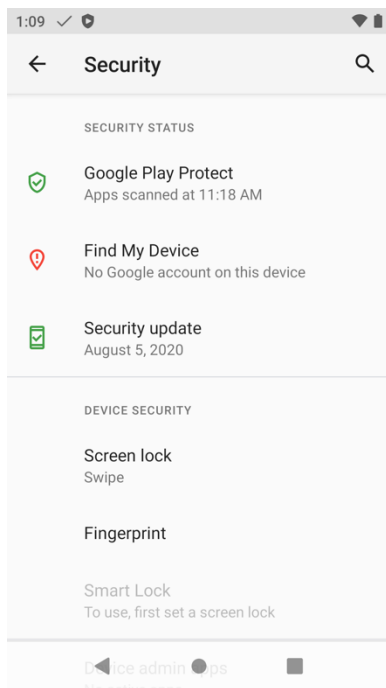
事前に電話機のストレージにダウンロードまたはコピーされた証明書を選択してインストールできます。





[セキュリティ (Security)] 設定を使用して証明書をインストールするには、[設定 (Settings)]、[セキュリティ (Security)]、[暗号化とログイン情報 (Encryption and credentials)] の順に選択し、[ストレージからインストール (Install from storage)] を選択します。

事前に電話機のストレージにダウンロードまたはコピーされた証明書を選択してインストールできます。

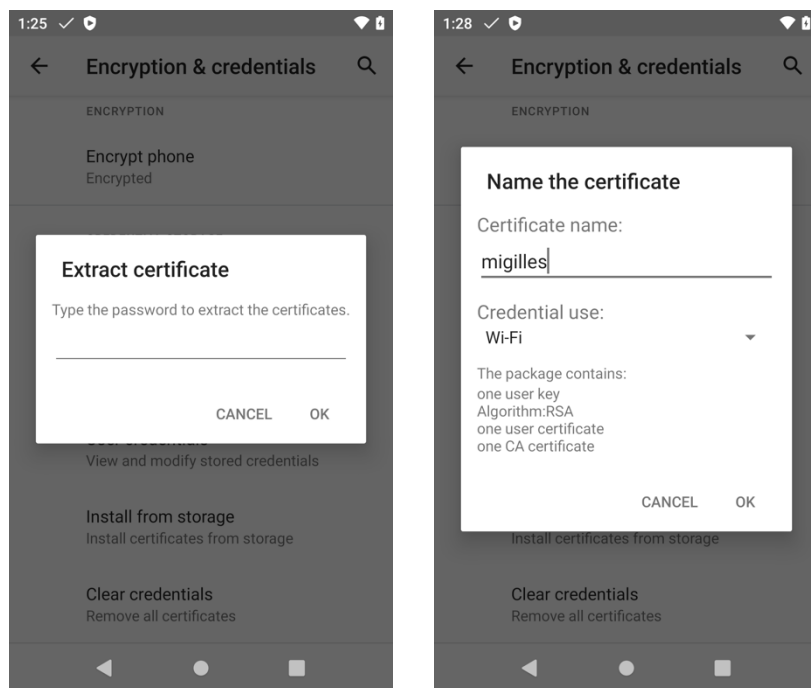


EAP-TLS を利用するには、ユーザー証明書をインストールする必要があります。

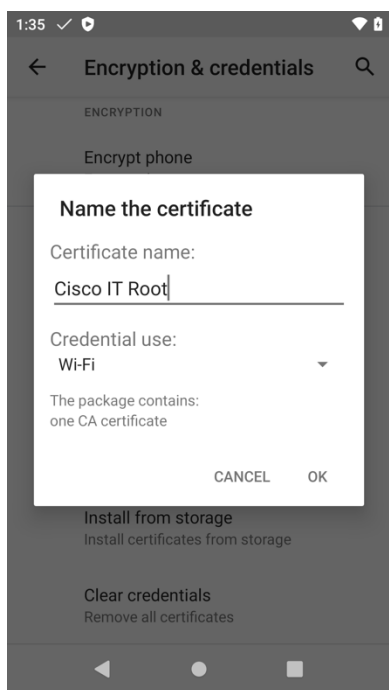
証明書とキーを抽出するには、パスワードの入力が必要になる場合があります。

証明書名を入力できます。

ユーザ証明書を発行した CA チェーンが RADIUS サーバの信頼リストに追加されたことを確認します。



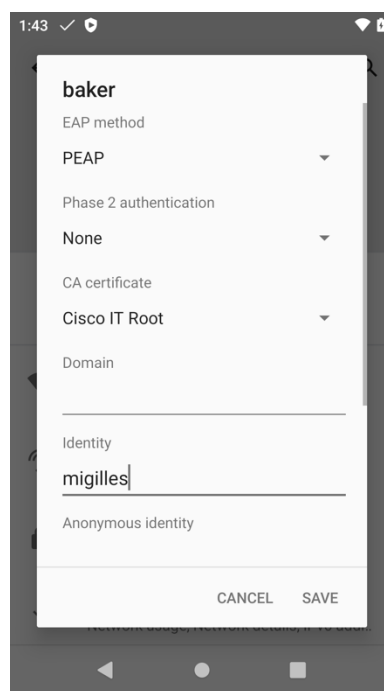
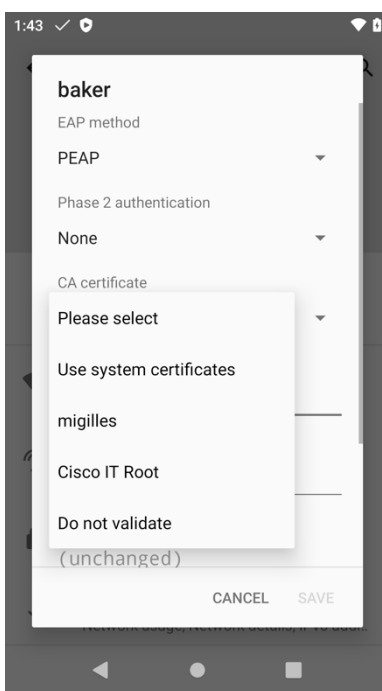
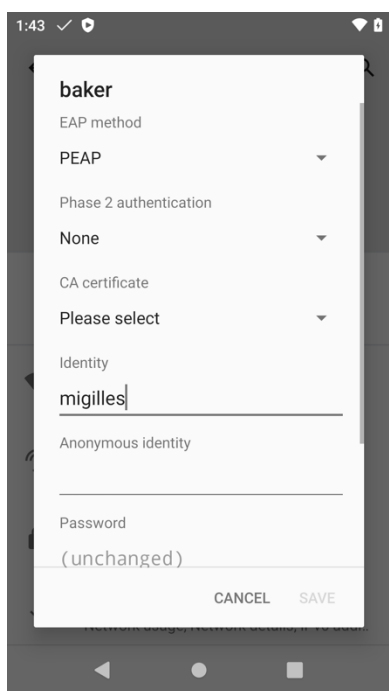
RADIUS サーバの証明書を発行したルート CA の証明書は、**EAP-TLS**、**EAP-TTLS**、または **PEAP** サーバ検証を有効にするためにインストールする必要があります。



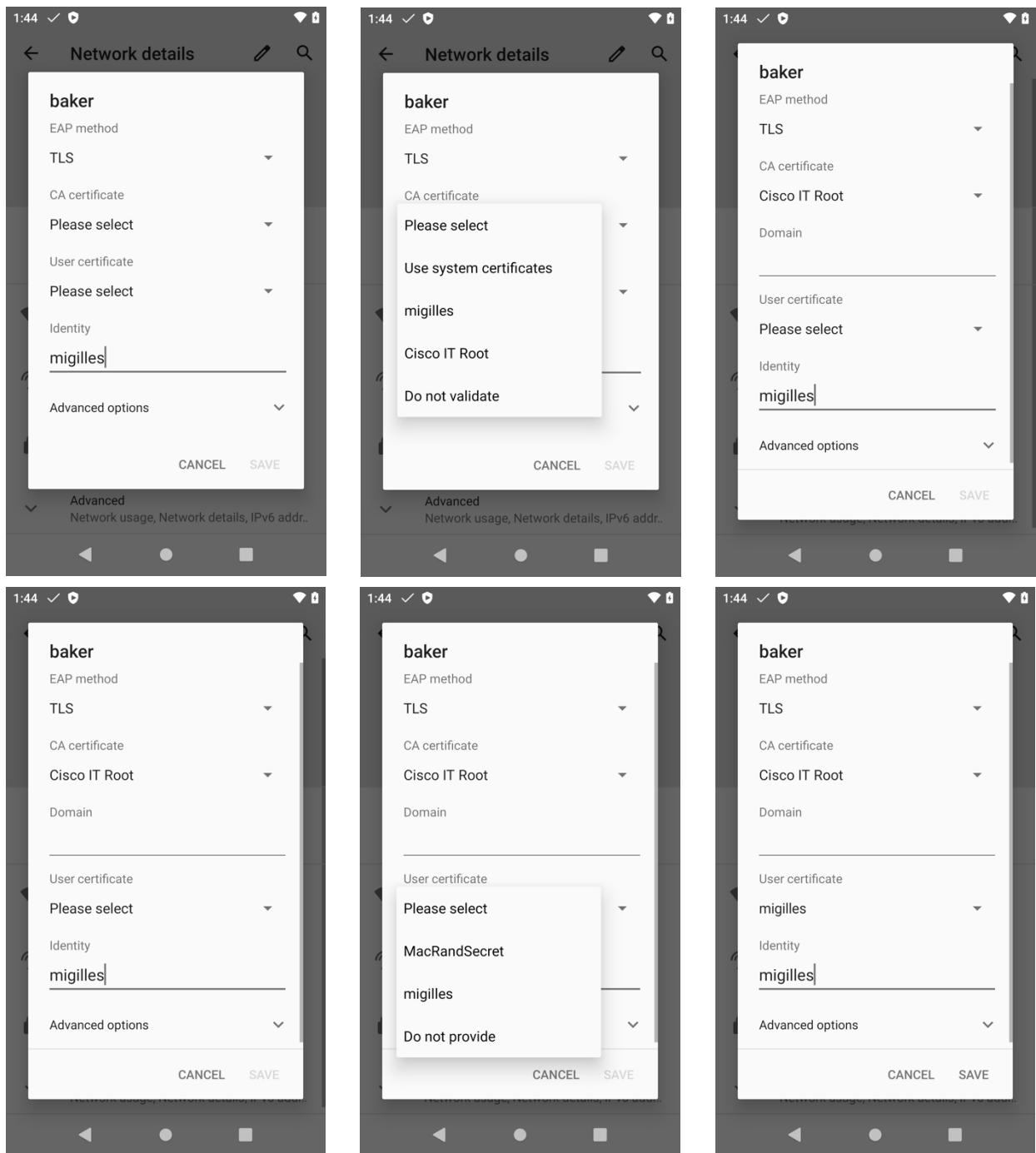
証明書の設定

証明書がインストールされると、Wi-Fi プロファイル設定で使用する証明書を選択できます。

PEAP および **EAP-TTLS** の場合、サーバー検証を有効にするように **CA 証明書** をオプションで設定できます。



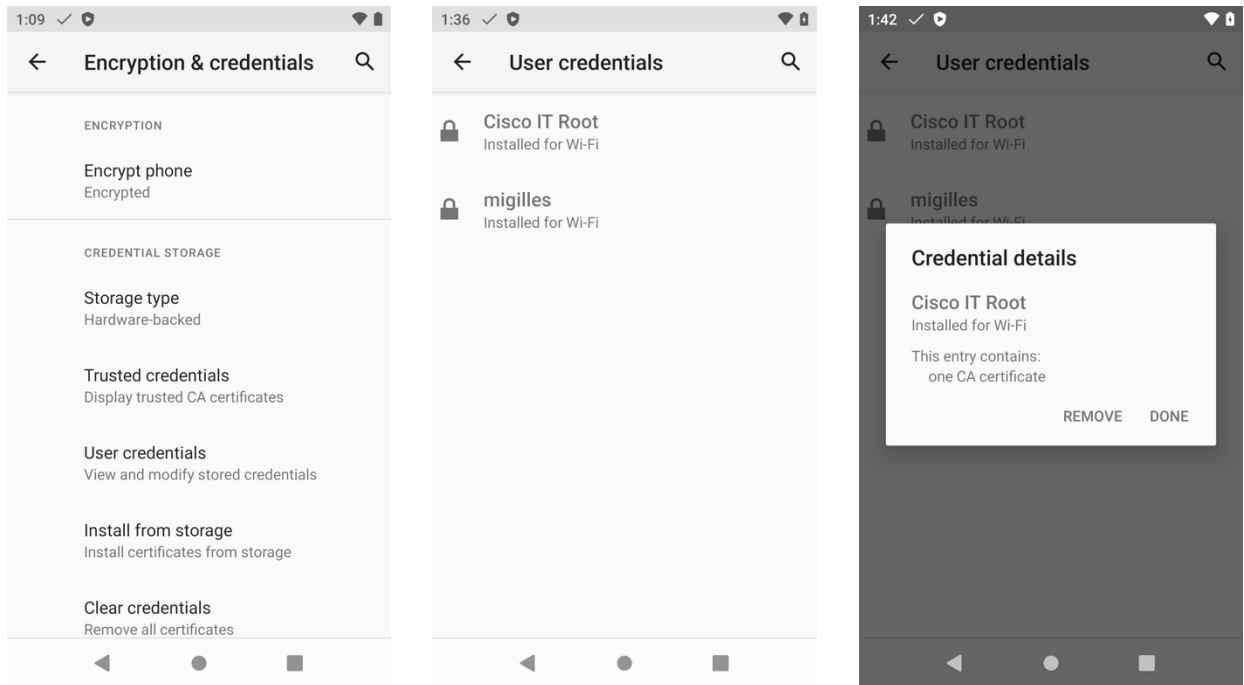
EAP-TLS の場合、**ユーザー証明書**を設定する必要があり、オプションでサーバー検証を有効にするように **CA 証明書**を設定できます。



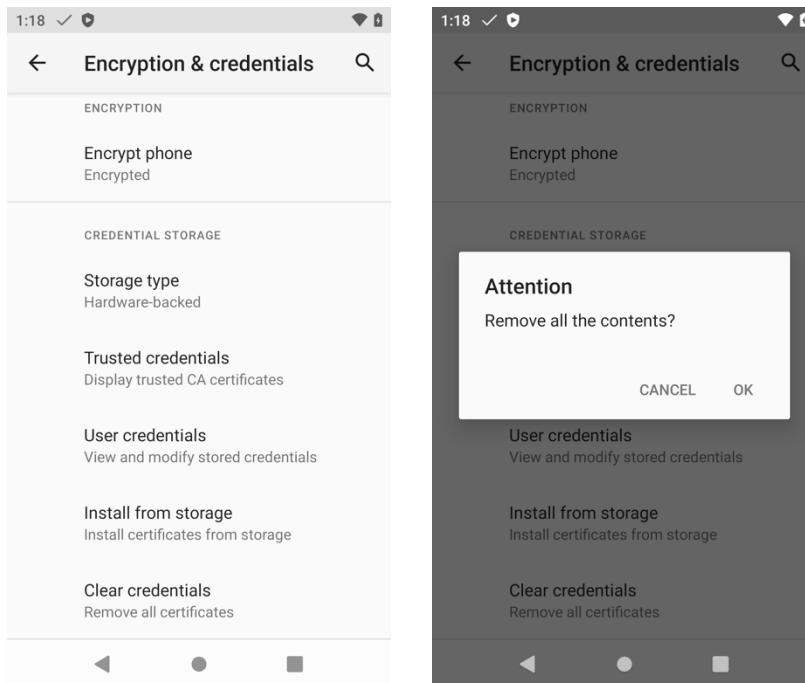
証明書の削除

証明書は個別またはまとめて削除できます。

個々の証明書を削除するには、[設定 (Settings)]、[セキュリティ (Security)]、[暗号化とクレデンシャル (Encryption and credentials)]、[ユーザクレデンシャル (User credentials)] の順に選択し、[削除 (Remove)] を選択します。



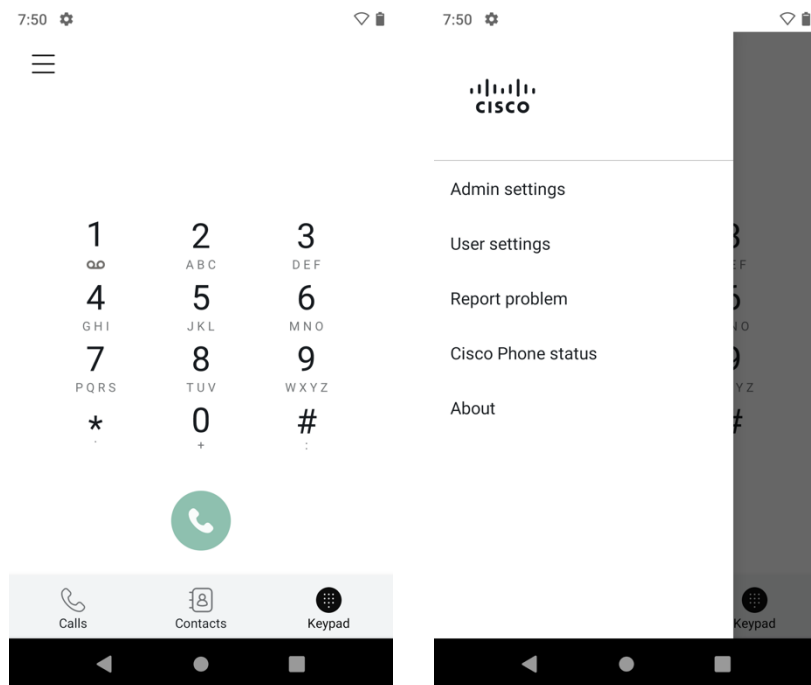
すべての証明書を削除するには、[設定 (Settings)]、[セキュリティ (Security)]、[暗号化とログイン情報 (Encryption and credentials)] の順に選択し、[OK] を選択して削除を確認します。



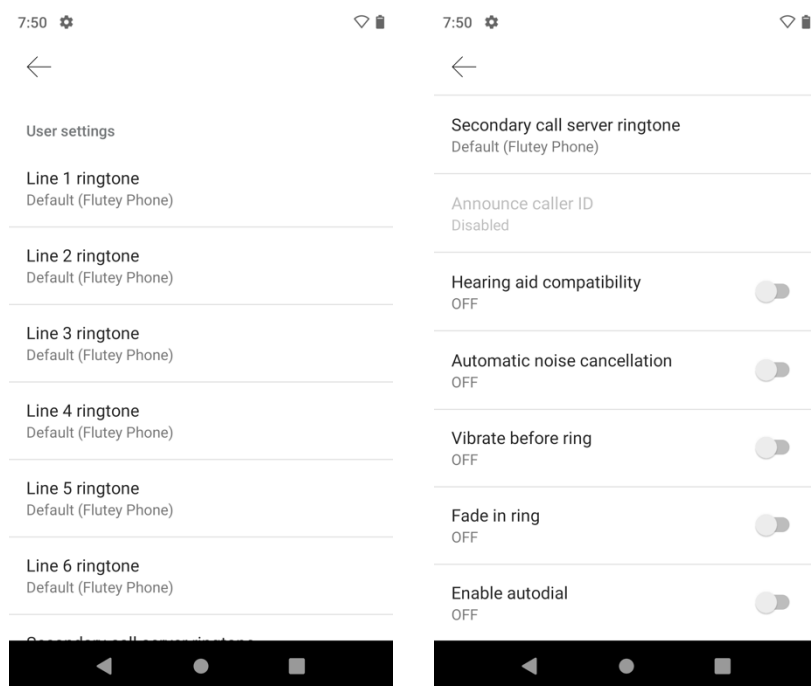
Cisco Phone アプリケーションの設定

Cisco Phone アプリケーションを設定するには、次のガイドラインを使用します。

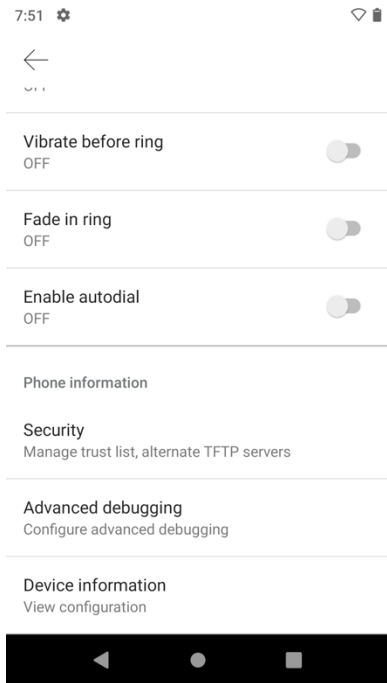
- Cisco Phone の設定は、Cisco Phone アプリケーションで左上隅にある 3 本の線を選択して設定できます。



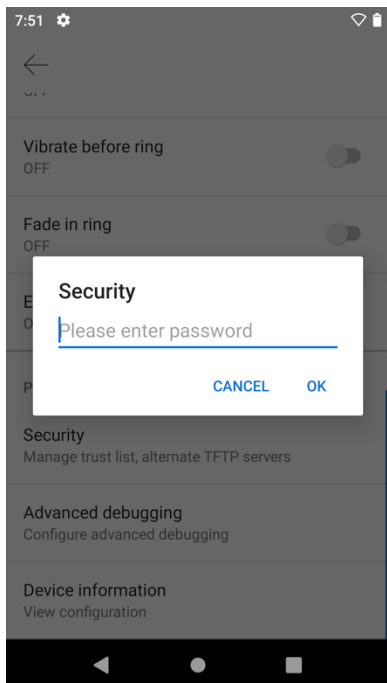
- 着信音などのユーザ設定は、必要に応じて設定できます。



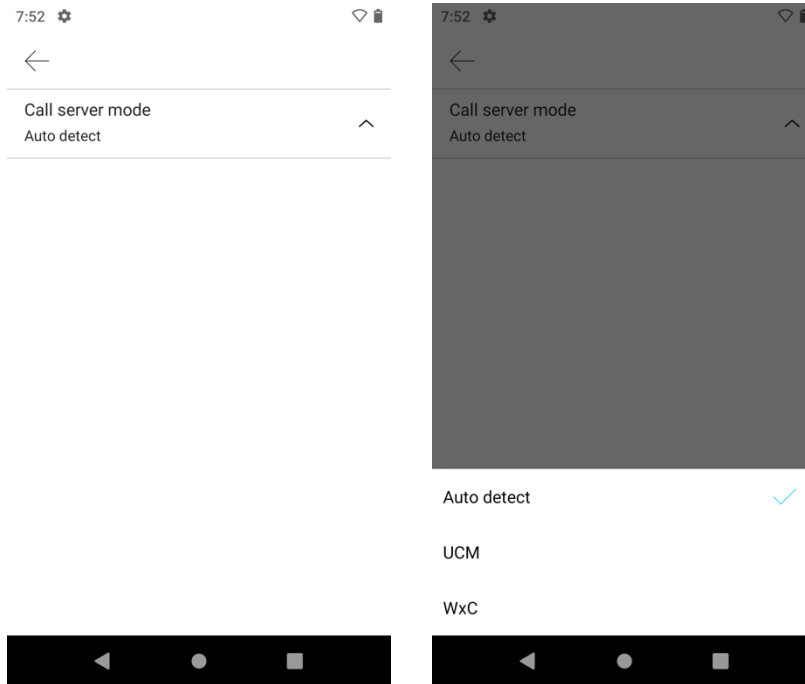
- ・ 信頼リストと TFTP サーバーは、[電話情報 (Phone information)] > [セキュリティ (Security)] の順に選択して管理できます。



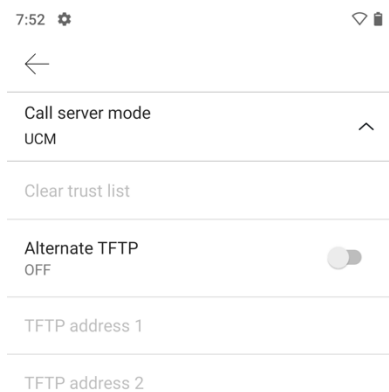
- ・ [電話情報 (Phone information)] > [セキュリティ (Security)] を選択したら、[ローカル電話ロック解除パスワード (Local Phone Unlock Password)] を入力する必要があります (デフォルト = **#)。



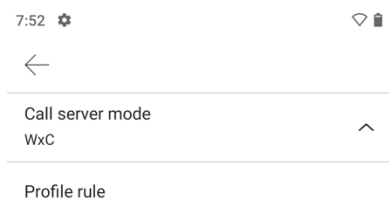
- 1.6(0) リリースでは、コール サーバー モードは [自動検出 (Auto detect)] に設定されます。この場合、ネットワークが DHCP オプション 150 または DHCP オプション 66 を提供し、Cisco Wireless Phone 840 または 860 は Cisco Unified Communications Manager で設定されます。それ以外の場合は、Webex Calling に登録しようとします。



- Cisco Unified Communications Manager に登録する必要があり、登録先の Cisco Unified Communications Manager にネットワークが DHCP オプション 150 または DHCP オプション 66 を提供していないため、TFTP サーバーを手動で設定する必要がある場合は、コールサーバーモードを UCM に設定します。[Alternate TFTP] を有効にしてから、TFTP サーバーのアドレスを入力します。
- Cisco Wireless Phone 840 または 860 が以前に Cisco Unified Communications Manager に登録されていて、別の Cisco Unified Communications Manager クラスタに登録する場合は、[信頼リストのクリア (Clear trust list)] を選択します。



- Webex Calling に登録し、手動で設定を構成する必要がある場合は、コールサーバーモードを WxC に設定し、[プロファイルルール (Profile rule)] を選択して、プロファイルルール情報を入力します。



- 左上隅にある戻る矢印を 2 回選択して [設定 (Settings)] メニューを終了し、設定を保存します。

詳細については、次の URL にある『Cisco Wireless Phone 840 および 860 アドミニストレーション ガイド』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

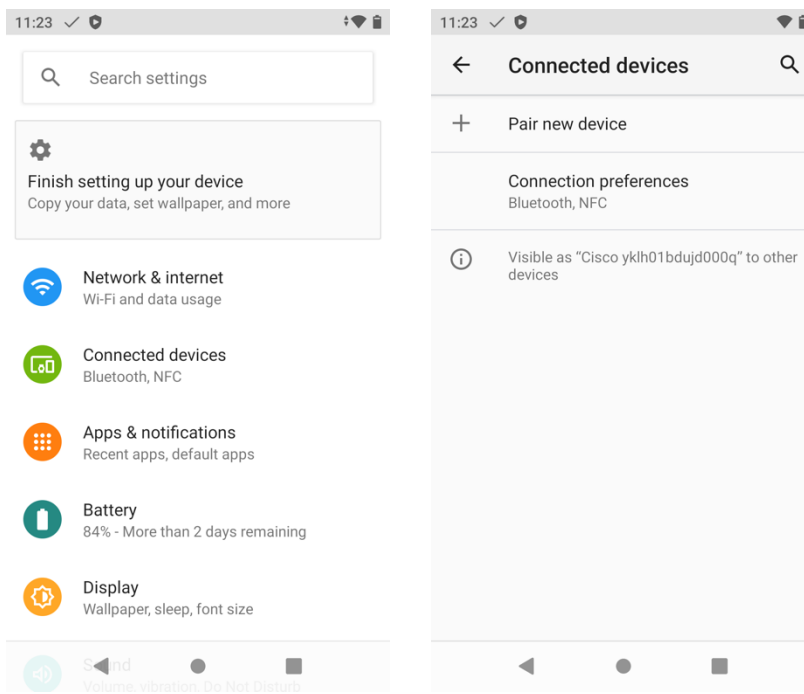
注：DHCP オプション 66 は、1.2(0) リリースでサポートされています。

Bluetooth 設定

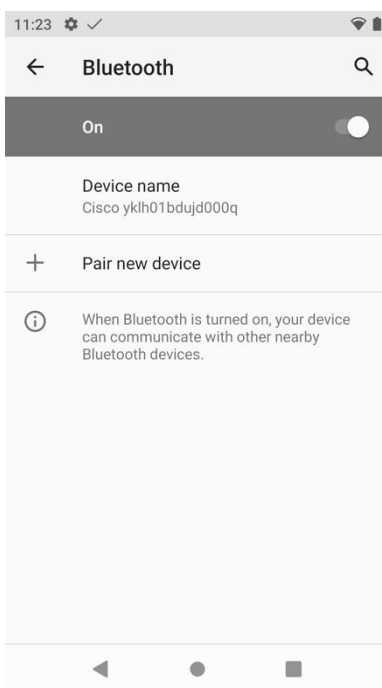
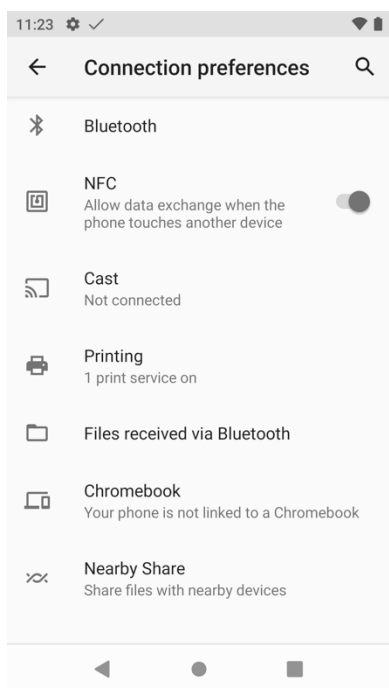
Cisco Wireless Phone 840 および 860 では、ハンズフリー通信を可能にする Bluetooth がサポートされます。

Bluetooth ヘッドセットと Cisco Wireless Phone 840 および 860 をペアリングする手順は次のとおりです。

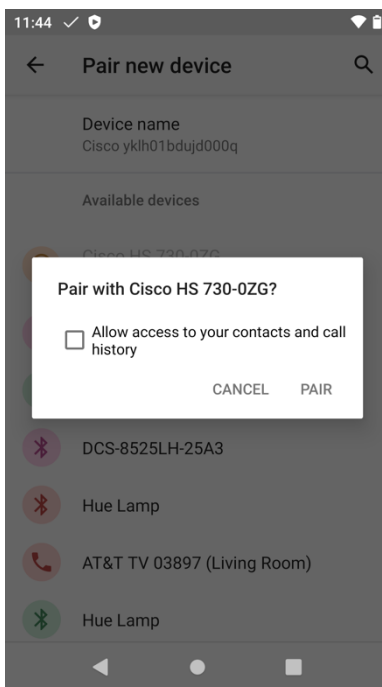
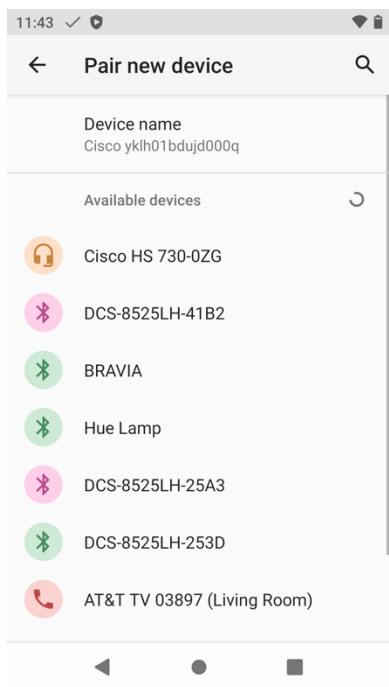
- **[設定 (Settings)] > [接続済みデバイス (Connected devices)]** の順に選択します。



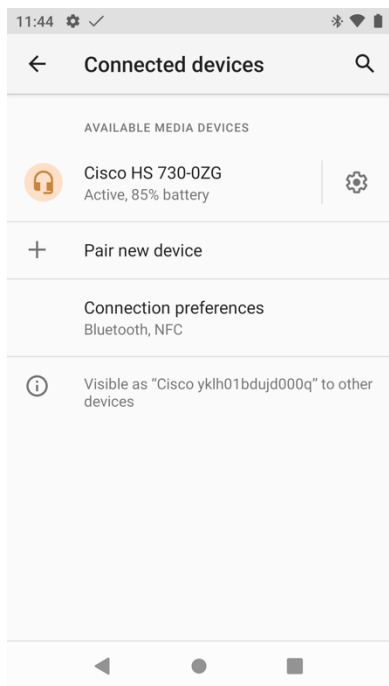
- **[設定 (Settings)]**、**[接続済みデバイス (Connected devices)]**、**[接続設定 (Connection Preferences)]**、**[Bluetooth]** の順に選択して、Bluetooth が **[オン (On)]** に設定されていることを確認します。
- Bluetooth デバイス名は、必要に応じて変更することもできます。



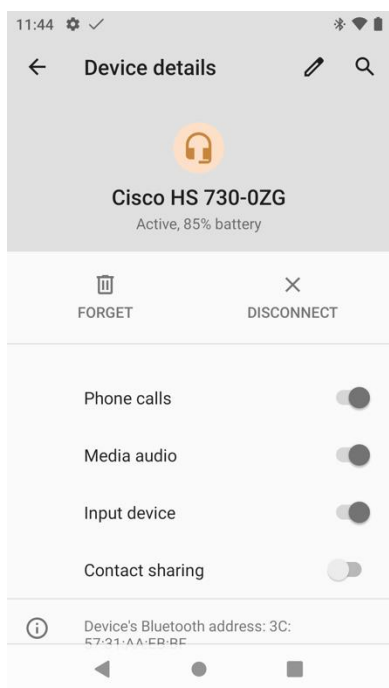
- Bluetooth デバイスがペアリングモードになっていることを確認し、**[新しいデバイスをペアリング (Pair new device)]** を選択します。
- Bluetooth デバイスがリストに表示されたら、それを選択します。
- Cisco Wireless Phone 840 および 860 は、Bluetooth デバイスと自動的にペアリングしようとしています。失敗した場合、プロンプトが表示されたら PIN コードを入力します。



- ペアリングに成功すると、Cisco Wireless Phone 840 および 860 は Bluetooth デバイスへの接続を試みます。

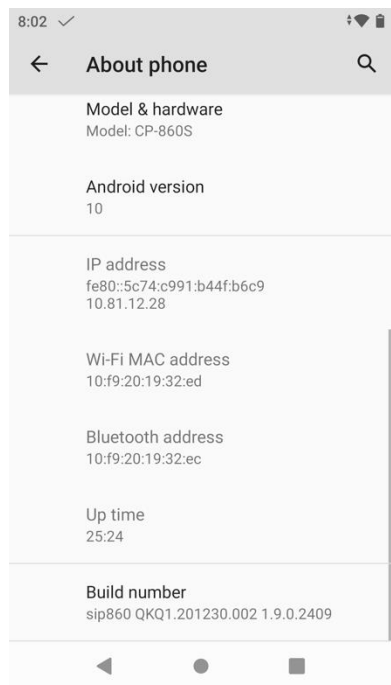


- Bluetooth デバイス名は、デバイスの詳細で変更できます。
- Bluetooth デバイスを選択してから [切断 (Disconnect)] を選択すると、現在接続されている Bluetooth デバイスが切断されます。
- 選択した Bluetooth デバイスのペアリングを解除するには [切断 (Forget)] を選択します。



ファームウェアのアップグレード

現在のビルド番号は、[設定 (Settings)] > [電話情報 (About phone)] > [ビルド番号 (Build number)] で確認できます。



Cisco Unified Communications Manager

ファームウェアをアップグレードするには、Cisco Unified Communications Manager の署名済み COP ファイルをインストールしてから、Cisco TFTP サービスを実行しているすべてのノードで Cisco TFTP サービスを再起動します。

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 オペレーティング システム アドミニストレーション ガイド**』を参照してください。

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

ダウンロードされた電話機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。Cisco Wireless Phone 840 または 860 は、指定されたイメージを実行していない場合、ファームウェア ファイルをフラッシュメモリにダウンロードします。

ロード サーバを、ファームウェア ファイルを取得する代替 TFTP サーバとして指定できます。この設定オプションは、TCP ポート 6970 の HTTP (UDP ポート 69 の TFTP がサポートされていないため) 経由で、Cisco Unified Communications Manager Administration 内の Cisco Wireless IP Phone 8821/8821-EX の製品固有の設定セクションにあります。ファームウェアを ZIP ファイル形式でダウンロードし、内容を抽出してから、それらのファイルをロード サーバにコピーします。

コールサーバで [ソフトウェア更新のダウンロード後すぐに再起動する (Reboot successfully after download software updates)] オプションが有効になっていない場合、ユーザーは再起動して新しいファームウェアを適用することを確認するプロンプトが表示されます。

注： Cisco Unified Communications Manager のバージョンが 14 SU1 より前の場合は、TCP ポート 6970 で動作する外部 HTTP ロード サーバを展開して使用することをお勧めします。14 SU1 より前のバージョンには HTTP 範囲ヘッダーのサポートが含まれていないため、ファームウェアのダウンロード中にネットワークが中断された場合、ダウンロードは中断したところから再開するのではなく、再開する必要があります。

Webex Calling

Cisco Wireless Phone 840 および 860 にインストールされるファームウェアバージョンは、Webex Control Hub (安定版、ベータ版、最新版) で構成されたソフトウェア アップグレード チャンネルによって決定され、そのソフトウェア アップグレード チャンネルで新しいファームウェアが利用可能になると、自動的にプッシュダウンされます。

Cisco Wireless Phone Upgrade ツール

Cisco Wireless Phone Upgrade Tool (<https://webexphoneupgrade.cisco.com>) は、Cisco Wireless Phone 840 または 860 を 1.6(0) リリースにアップグレードできるクラウドベースのツールです。

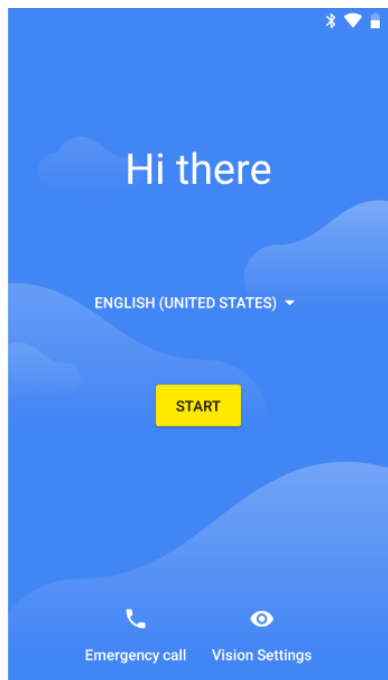
新しいクラウドベースのツールを使用すると、Wi-Fi プロファイル設定とロードサーバ情報を含む生成された QR コードをスキャンすることで、Cisco Wireless Phone 840 および 860 ファームウェアを 1.6(0) リリースに簡単にアップグレードできます。

1.6(0) リリースには Webex Calling のサポートが含まれているため、このアップグレード方法は、Cisco Wireless Phone 840 または 860 を使用しており、Webex Calling に登録したいが、Cisco Wireless Phone 840 または 860 ファームウェア。

Cisco Wireless Phone Configuration Management ユーティリティにアクセスするには、Cisco.com アカウントが必要です。

Cisco Wireless Phone 840 または 860 が新品でない場合は、[設定 (Settings)]、[システム (System)]、[詳細 (Advanced)]、[オプションのリセット (Reset options)]、[すべてのデータの消去 (工場出荷時の状態へのリセット) (Erase all data (factory reset))]の順に選択して、初期設定にリセットする必要があります。

起動画面で、ディスプレイをすばやく 6 回タップすると、QR コードをスキャンして Cisco Wireless Phone 840 または 860 ファームウェアをアップグレードするように求められます。



Wi-Fi 設定とロードサーバーパラメータを設定します。

次のセキュリティ設定がサポートされています。

[セキュリティモード (Security Mode)]	EAP 方法	フェース 2 認証
なし	該当なし	なし
WPA2-Personal	該当なし	なし
WPA2-Enterprise	PEAP	GTC、MSCHAPV2
WPA2-Enterprise	TTLS	GTC、MSCHAP、MSCHAPV2、PAP

注： Cisco Wireless Phone Upgrade Tool は EAP-TLS (TLS) をサポートしていません。

オープン Wi-Fi ネットワークに接続するには、**SSID** を入力し、[セキュリティ (Security)] を [なし (None)] に設定します。

Webex Wireless Phone Upgrade Tool

Initial Provisioning

Wi-Fi Configuration

Security:

* SSID:

Hidden SSID:

Load Server

Network Protocol: ⓘ

Server Address: ⓘ

Server Port: ⓘ

Relative Path on Server: ⓘ

PSK 対応の Wi-Fi ネットワークに接続するには、**SSID** を入力し、[セキュリティ (Security)] を [WPA2-個人 (WPA2-Personal)] に設定してから、8-63 ASCII または 64 HEX パスワードを入力します。

Webex Wireless Phone Upgrade Tool

Initial Provisioning

Wi-Fi Configuration

Security: WPA2-Personal

* SSID:

* Password:

Show:

Hidden SSID:

Load Server

Network Protocol: HTTP ⓘ

Server Address: wxcmppupgrade.bcl.d.webex.com ⓘ

Server Port: 80 ⓘ

Relative Path on Server: cp_840_860 ⓘ

EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [WPA2-EAP] に設定してから、[認証方式 (Authentication method)] を選択します。

PEAP または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、フェーズ 2 認証方式を選択し、必要に応じてヘッダーとフッターを除いた Base-64 (PEM) エンコーディング形式で CA 証明書を設定し、ID とパスワードを入力します。

Webex Wireless Phone Upgrade Tool

Initial Provisioning

Wi-Fi Configuration

Security: WPA2-Enterprise

* SSID:

* Password:

Show:

Hidden SSID:

Load Server

Network Protocol: HTTP 

Server Address: wxcmpupgrade.bclid.webex.com 

Server Port: 80 

Relative Path on Server: cp_840_860 

EAP Configuration

EAP Method: PEAP

Phase 2 Authentication: MSCHAPV2

Domain:

* Identity:

Anonymous Identity:

CA Certificate:

Select CA Certificate

Generate

注：ブロードキャストされていない Wi-Fi ネットワークは、非表示の **SSID** として設定する必要があります。それ以外の場合、Wi-Fi ネットワークは範囲内に表示されません。非ブロードキャスト Wi-Fi ネットワークに接続するには、[非表示 SSID (Hidden SSID)] を [はい (True)] に設定します。

ヘッダーとフッターが削除され、スペースや改行が含まれていない CA 証明書の形式が正しいことを確認します。

Cisco Wireless Phone 840 および 860 ファームウェア ファイルは、ファームウェア アップグレードにシスコが管理するロード サーバーを使用する代わりに、代替のロード サーバーにダウンロードしてホストすることもできます。

次のファイルをダウンロードして、代替 HTTP または HTTPS ロードサーバーにアップロードする必要があります。

- http://wxcmppupgrade.bclid.webex.com/cp_840_860/UpgradeDPC.apk
- http://wxcmppupgrade.bclid.webex.com/cp_840_860/sip840-ota_update-signed-1.6.0.1409.zip
- http://wxcmppupgrade.bclid.webex.com/cp_840_860/sip860-ota_update-signed-1.6.0.1852.zip

注：HTTPS 方式を使用するには、Android の証明書信頼ストアに含まれる信頼できる CA から証明書が HTTPS サーバーに発行されていることを確認する必要があります。

デフォルトのロードサーバー (**wxcmppupgrade.bclid.webex.com**) の証明書は、Android の証明書信頼ストアに含まれる信頼できる CA から発行されません。したがって、HTTPS は使用せず、デフォルトの HTTP TCP ポート 80 設定を使用する必要があります。

設定が完了したら、[生成 (Generate)] を選択して QR コードを作成すると、QR コードが表示されます。

QR Code

×

Scan this QR code on your Webex wireless phone device by tapping seven times on the "Hi there" text on the Welcome screen



Done

Cisco Wireless Phone 840 または 860 で QR コードをスキャンします。

Cisco Wireless Phone 840 または 860 が近くにいる場合に備えて、QR コードを保存できます。その場合は、QR コードを PDF ファイルまたはスクリーンショットとして保存することをお勧めします。PNG ファイルとしてファイルを保存するとファイルが変更され、QR コードのスキャンが失敗します。

Cisco 無線電話 840 および 860 は、設定された Wi-Fi ネットワークへの接続を試み、ロード サーバーからファームウェア ファイルをダウンロードします。

Cisco Wireless Phone 840 および 860 は、自動的に初期設定にリセットされます。

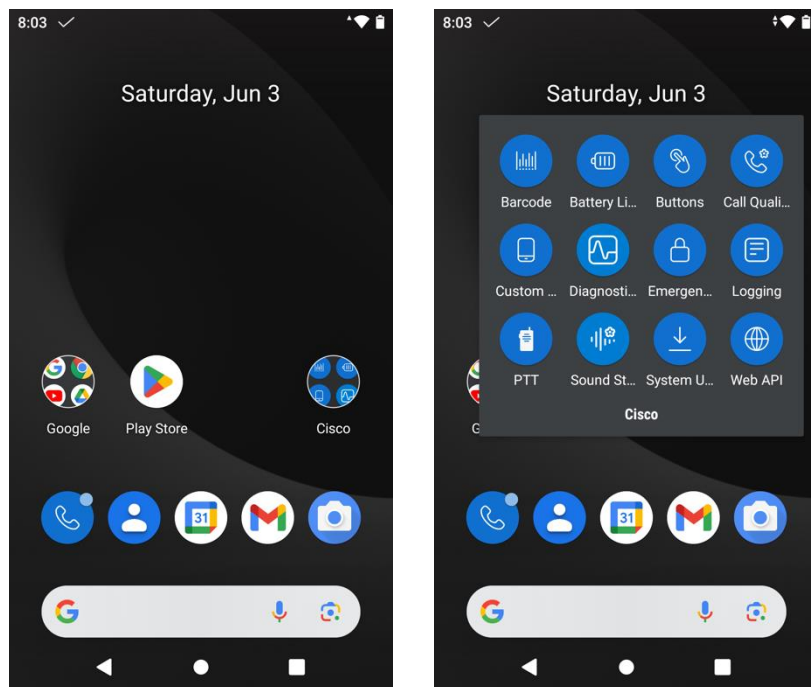
注： Cisco Wireless Phone 840 および 860 は、設定された Wi-Fi ネットワークの範囲内にある必要があります。範囲内がない場合、ファームウェアのアップグレードは失敗します。

Cisco Wireless Phone 840 および 860 の使用

アプリケーション

Cisco Wireless Phone 840 および 860 には、次のカスタム アプリケーションがプリインストールされています。

- **Cisco Phone** - 音声コールとビデオ コール
- **バッテリー寿命** - バッテリー モニタリング
- **ボタン** : ボタンのカスタマイズ
- **通話品質設定** - Wi-Fi のカスタマイズ
- **カスタム設定** : ユーザー制限とデバイス設定
- **診断** - ハードウェアのトラブルシューティング
- **緊急** - パニック ボタン機能
- **ロギング** - 高度なデバッグ
- **PTT** : プッシュツートーク機能
- **システム アップデータ** - ファームウェア更新通知
- **Web API** - Web API の設定
- **バーコード** : バーコードスキャン機能 (840 および 860 モデルのみ)

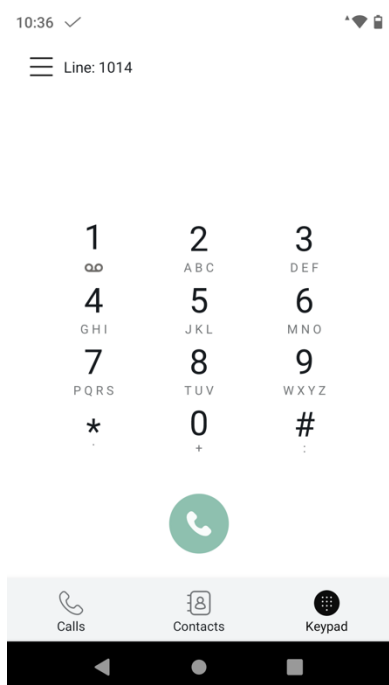


シスコの電話機

電話アプリケーションを起動するには、メイン ページまたはアプリケーション メニューから **[Cisco Phone]** アイコンを選択します。

Cisco Wireless Phone 840 および 860 は、電源投入後に Cisco Unified Communications Manager または Webex Calling への登録を試行するため、コールを発信または受信するためにアプリケーションを手動で起動する必要はありません。

通知ステータスバーにチェックマークアイコンがあり、内線番号が Cisco Phone アプリケーションに表示されている場合、Cisco Wireless Phone 840 および 860 は Cisco Unified Communications Manager または Webex Calling に登録されています。

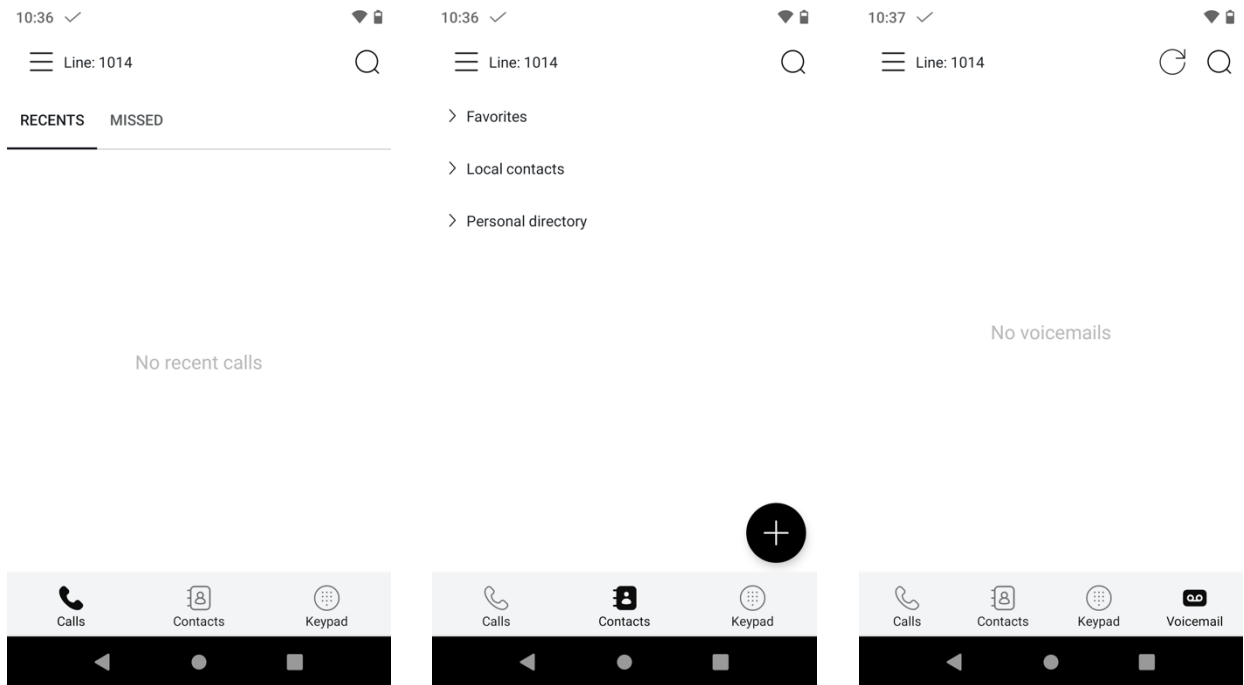


通話履歴には、**[通話 (Calls)]** タブからアクセスできます。

連絡先とお気に入りには、**[連絡先 (Contacts)]** タブからアクセスできます。連絡先を追加するには、**[+]** アイコンを選択し、連絡先を追加するディレクトリを選択します。その連絡先リストを表示または管理するには、パーソナルディレクトリにログインする必要があります。

手動コールは、**[キーパッド (Keypad)]** タブを使用して発信できます。

コールサーバーで **[ビジュアルボイスメールアクセス (Visual Voicemail Access)]** が有効になっている場合は、**[ボイスメール (Voicemail)]** タブからボイスメールにアクセスできます。

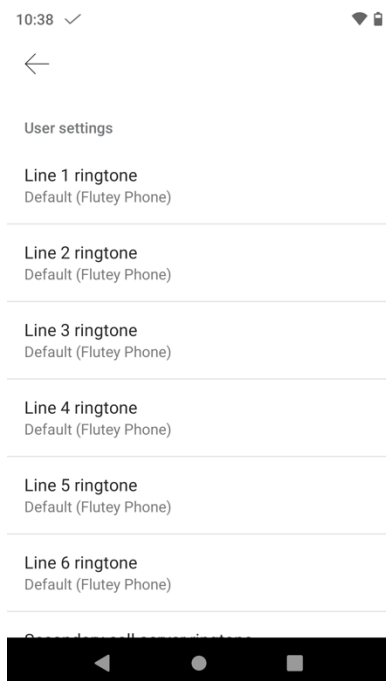


着信音を設定するには、左上隅にある 3 本の線を選択し、[ユーザー設定 (User settings)] を選択します。

1.7(0) リリースでは、着信音は回線ごとに設定できますが、以前のリリースでは 1 つの着信音しか設定できませんでした。

1.8(0) リリースでは、事前にインストールされている着信音を Cisco Unified Communications Manager 内の回線ごとに設定および管理できます。

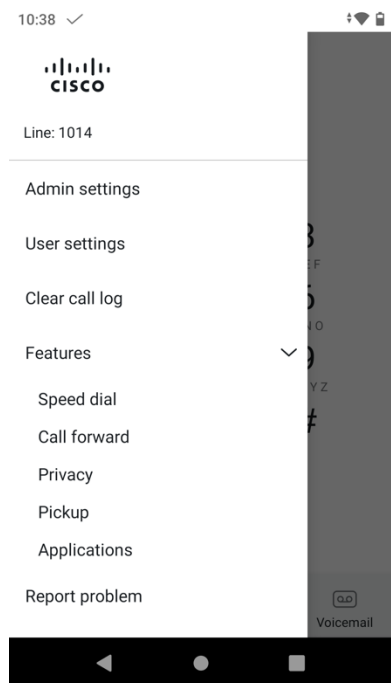
1.9(0) リリースでは、Cisco Unified Communications Manager 内で回線ごとにカスタム着信音を設定および管理し、電話機にダウンロードできます。



Cisco Unified Communications Manager 内の [回線 1 ~ 6 の着信音 (Line 1-6 Ringtone)] オプションに設定できる、事前にインストールされている着信音を以下に示します。

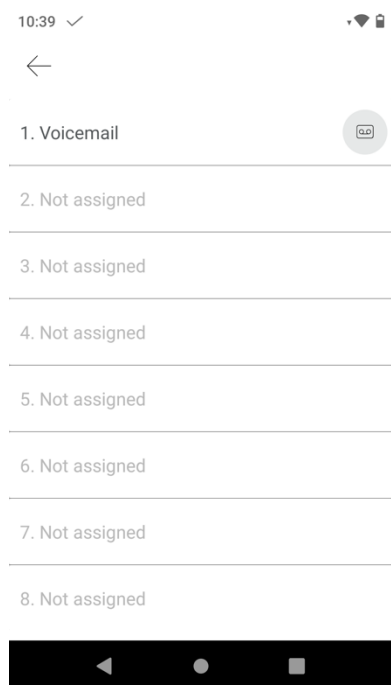
- Andromeda
- Aquila
- Argo Navis
- Atria
- Beat Plucker
- Bell Phone
- Big Easy
- Bootes
- Canis Major
- Carina
- Cassiopeia
- Centaurus
- Chimey Phone
- Cygnus
- Digital Phone
- Ding
- Draco
- Dream Theme
- Eridani
- Flutey Phone
- Free Flight
- Girtab
- Growl
- Hydra
- Insert Coin
- Kuma
- Lyra
- Machina
- Mildly Alarming
- New Player
- Noisy One
- Orion
- Pegasus
- Perseus
- Pyxis
- Rasalas
- Rigel
- Scarabaeus
- Sceptum
- Solarium
- Testudo
- Third Eye
- Very Alarmed
- Vespa
- Zeta

短縮ダイヤル、コール転送、プライバシー（有効な場合）、ピックアップ、アプリケーション（設定されている場合）などの機能にアクセスするには、左上隅にある 3 本の線を選択し、**[機能 (Features)]** を選択します。



短縮ダイヤルを設定するには、**[機能 (Features)]**、**[短縮ダイヤル (Speed dial)]** の順に選択します。

既存のローカル連絡先の番号にマッピングして短縮ダイヤルを設定したら、**[キーパッド (Keypad)]** タブで、関連付けられた番号を押し続けます。

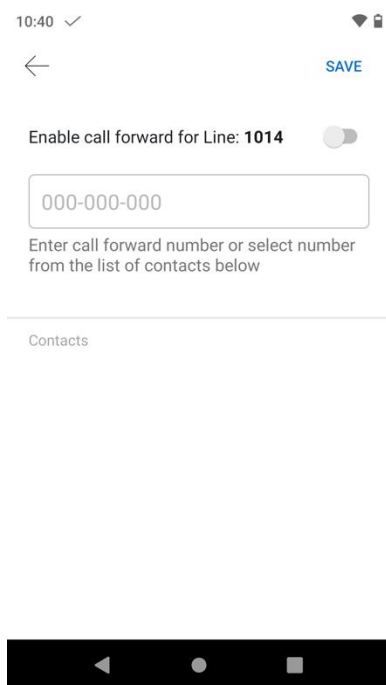


Cisco Wireless Phone 840 および 860 が Cisco Unified Communications Manager に登録されている場合にコール転送を有効にするには、**[機能 (Features)]**、**[コール転送 (Call forward)]** の順に選択し、スライダをタップしてスライダを右に移動し、すべてのコールを転送する宛先番号を入力します。

Cisco Wireless Phone 840 および 860 が Webex Calling に登録されている場合にコール転送を有効にするには、**[機能 (Features)]**、**[常にコール転送 (Call forward always)]**、または**[機能 (Features)]**、**[話中の場合のコール転送 (Call Forward when busy)]** を選択し、スライダをタップして右に移動し、すべてのコールを転送する宛先番号を入力します。に設定します。

コール転送を無効にするには、スライダをタップして左に移動します。

右上隅の**[保存 (SAVE)]** を選択して設定を保存します。

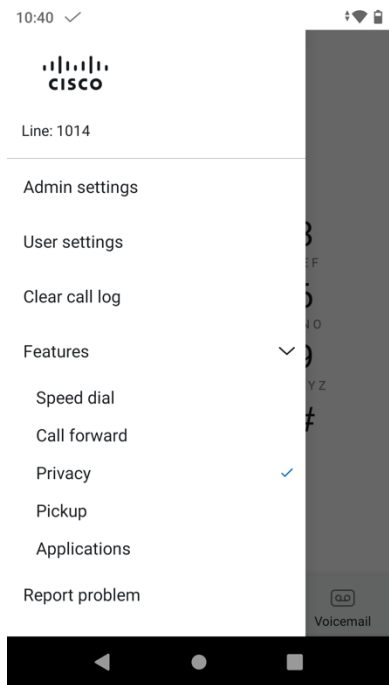


1.3(0) リリースでは、プライバシー機能がサポートされるようになりました。

プライバシー機能を使用するには、回線の 1 つを共有回線にし、ボタンの 1 つに**プライバシー**が設定されたカスタム電話ボタン テンプレートを作成し、電話機に適用する必要があります。

次に、プライバシーを有効にするには、**[機能 (Features)]**、**[プライバシー (Privacy)]** の順に選択します。

[プライバシー (Privacy)] の右側にチェックマークが表示され、この機能が有効になっているかどうかが表示されます。

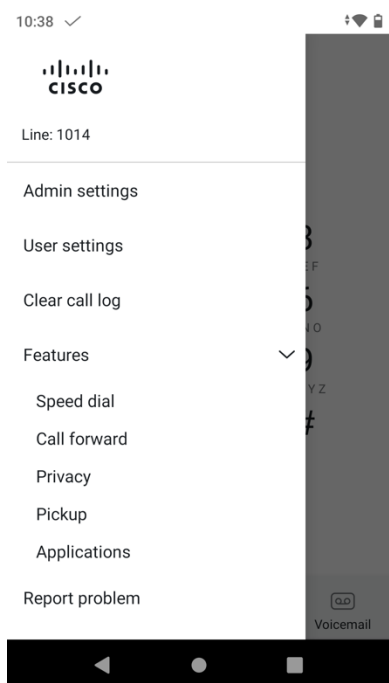


注： Webex Calling に登録されている場合、プライバシーは Cisco Wireless Phone 840 および 860 ではサポートされません。

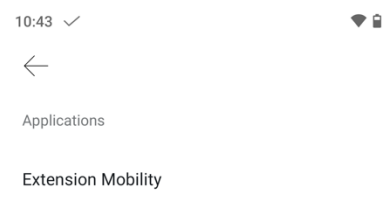
1.9(0) リリースでは、コール **ピックアップ**機能がサポートされるようになりました。

Cisco Unified Communications Manager 内の Cisco Wireless Phone 840 および 860 の回線に対してコール **ピックアップグループ**が設定されていることを確認します。

コール **ピックアップ**機能を使用するには、[**機能 (Features)**]、[**ピックアップ (Pickup)**] の順に選択します。



設定済みのアプリケーションにアクセスするには、**[機能 (Features)] > [アプリケーション (Applications)]**の順に選択します。

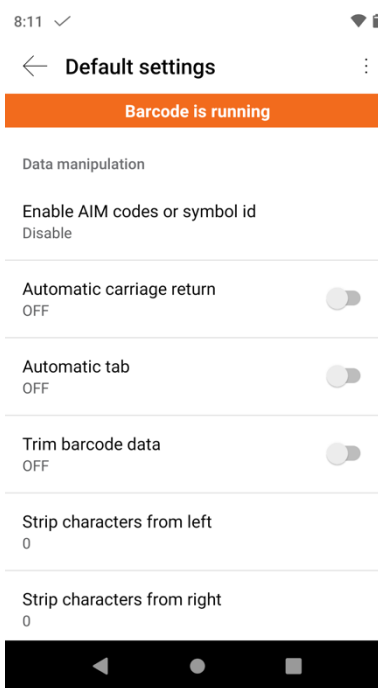
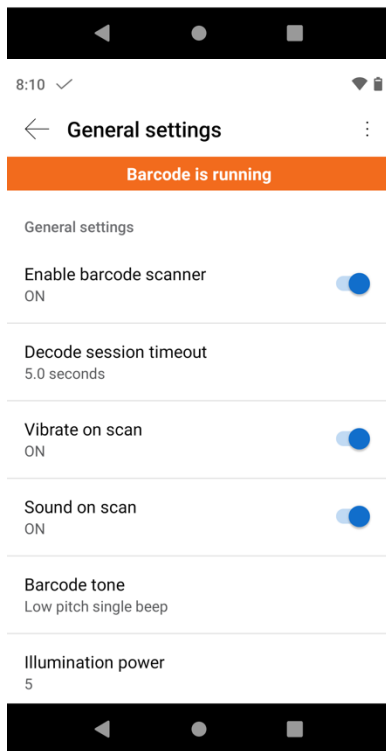
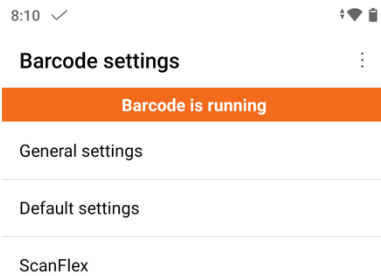


注：Webex Calling に登録されている場合、アプリケーションは Cisco Wireless Phone 840 および 860 ではサポートされません。

バーコード

バーコードスキャナは、Cisco 無線電話 840S および 860S モデルでのみ使用できます。

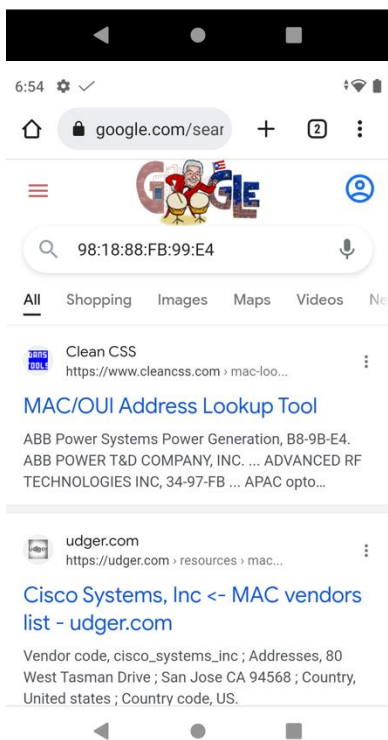
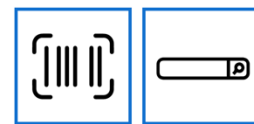
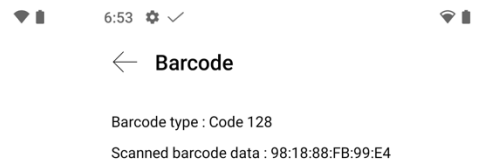
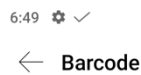
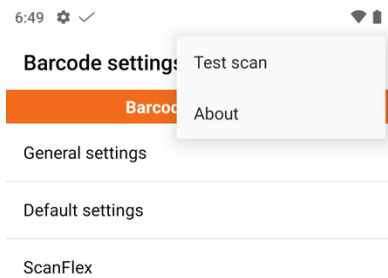
バーコードスキャナの設定は、バーコードアプリケーションでカスタム設定できます。



バーコードスキャナをテストするには、バーコードアプリケーションで右上隅にある 3 つのドットを選択し、**[スキャンのテスト (Test scan)]** を選択します。

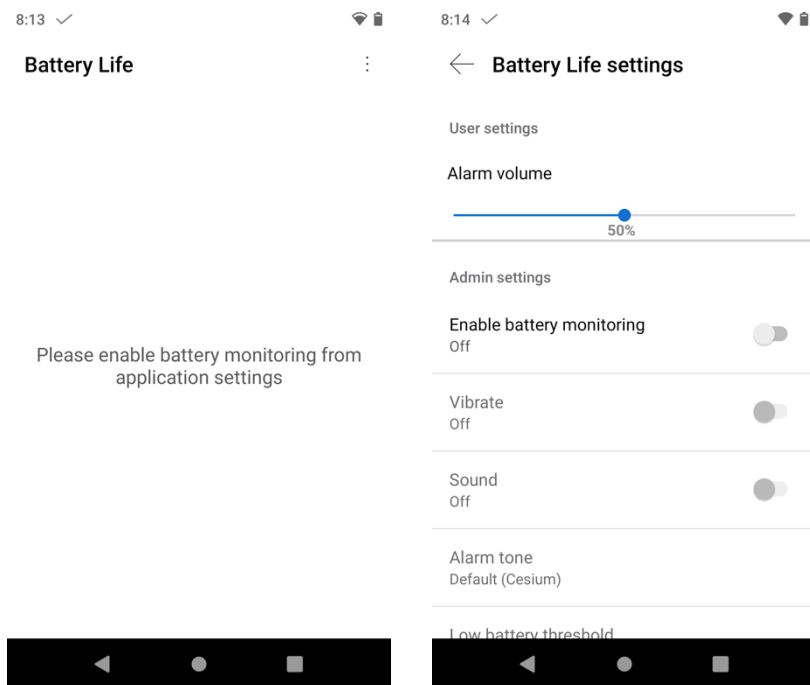
下のバーコードアイコンを押して、バーコードスキャンを開始します。

バーコードがスキャンされると、検索アイコンを選択して検索を実行できます。



バッテリー寿命

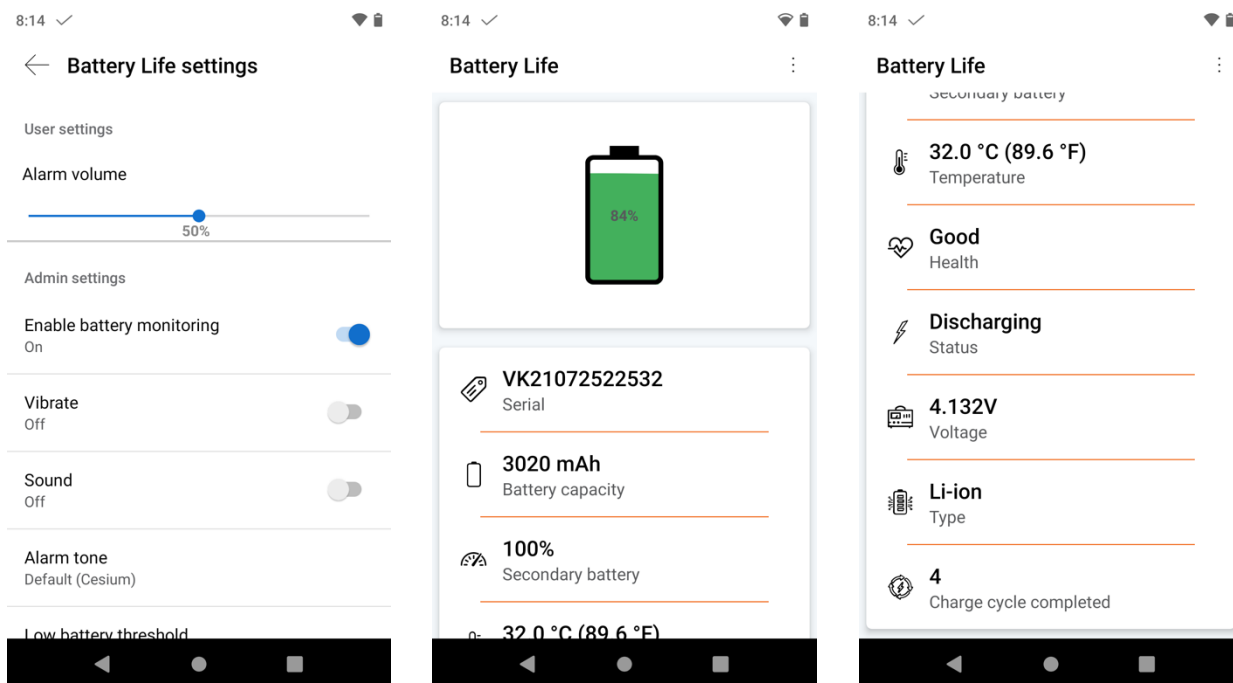
バッテリー寿命のモニタリングを有効にするには、**[バッテリー寿命 (Battery Life)]** アプリケーションで右上隅にある3つのドットを選択し、**[設定 (Settings)]** を選択します。



バッテリー寿命のモニタリングを有効にするには、**[バッテリーのモニタリングを有効にする (Enable backup monitoring)]** スライダーが右側にある**[オン (On)]** に設定されていることを確認します。

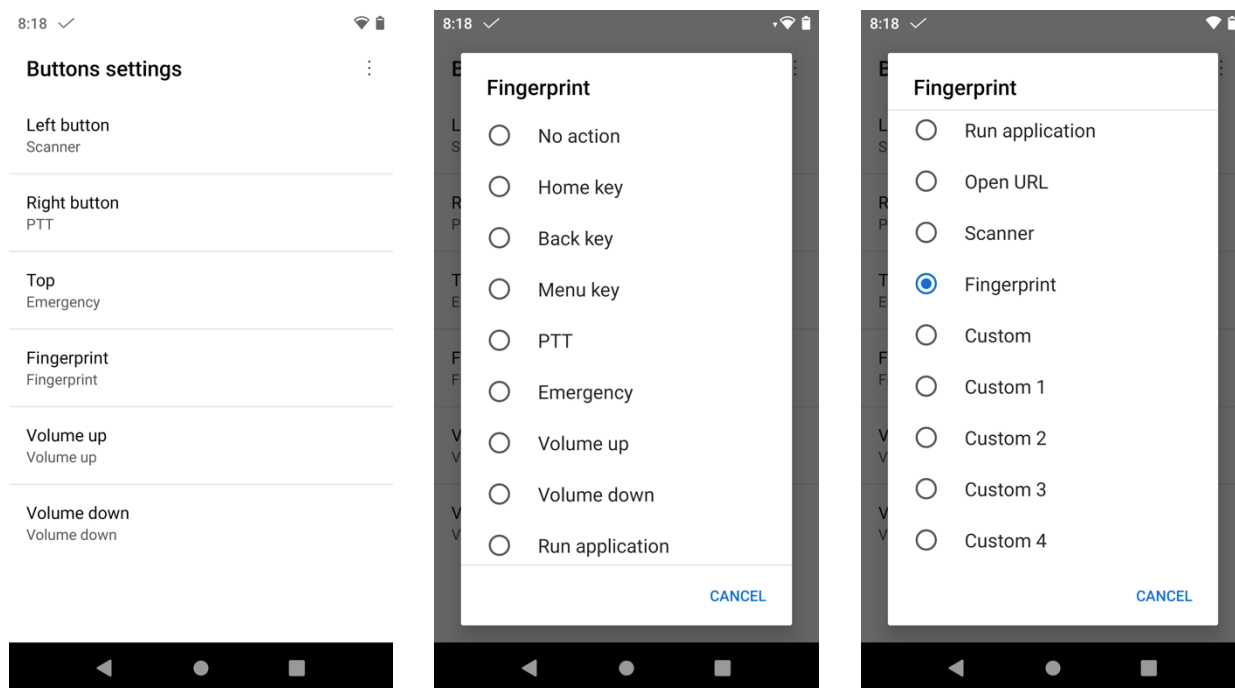
フル充電サイクルの数も表示できます。

充電サイクルの数が **500** に達すると、通知が表示され、バッテリーを交換する必要があります。



ボタン

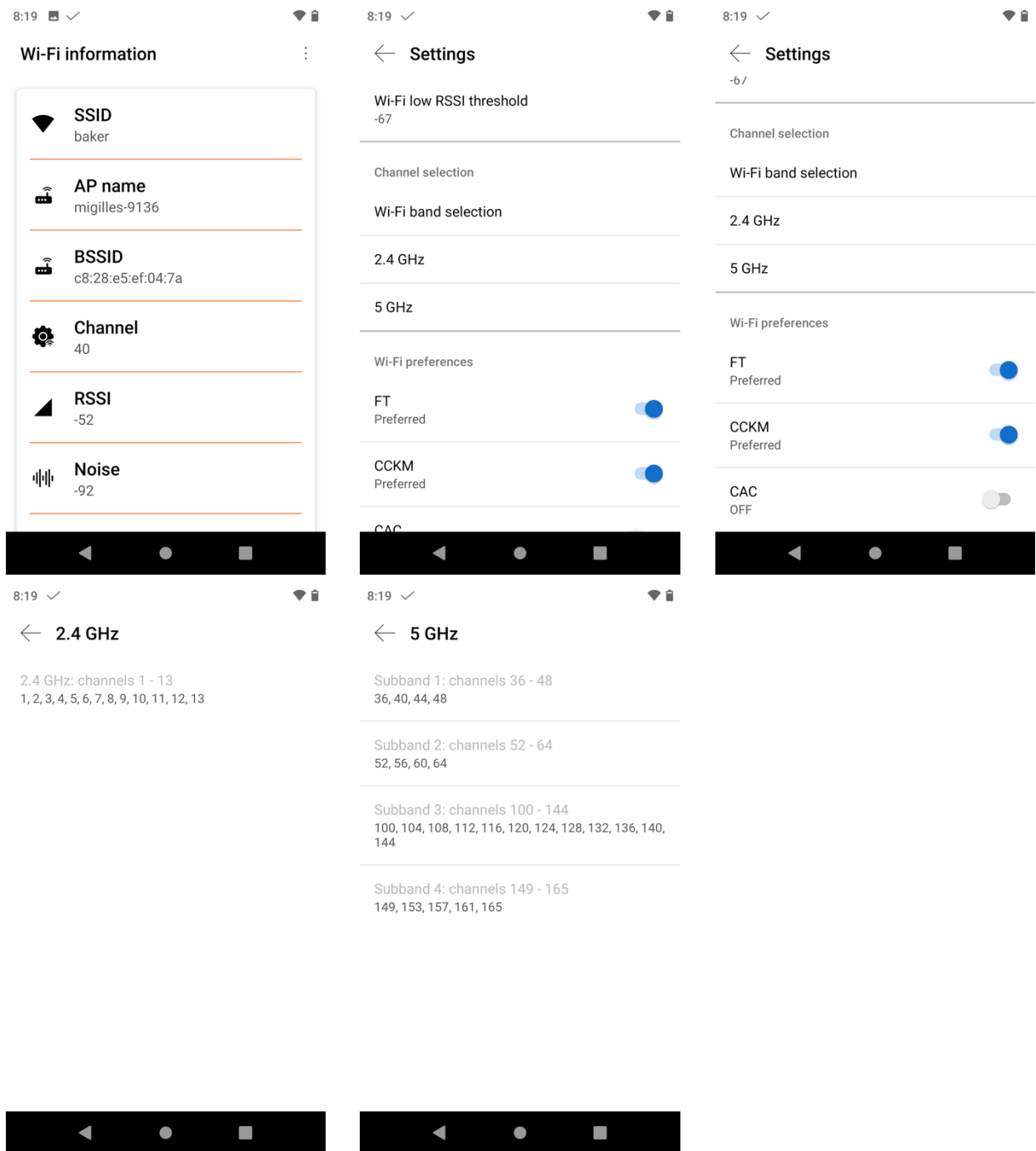
Cisco 無線電話 840 および 860 のハード ボタンは、**ボタン アプリケーション**でカスタム設定できます。



注：[フィンガープリント (Fingerprint)] ボタンは、Cisco ワイヤレス 電話 860 でのみ使用できます。

通話品質設定

有効なチャンネルを含む **Wi-Fi 帯域選択** (自動、2.4 GHz、5 GHz)、高速セキュア ローミング設定 (**FT** および **CCKM**)、および **Wi-Fi 低 RSSI しきい値**は、右上の 3 つの点を選択して設定できます。[**コール品質設定 (Call Quality Settings)**] アプリケーションで、[**設定 (Settings)**] を選択します。

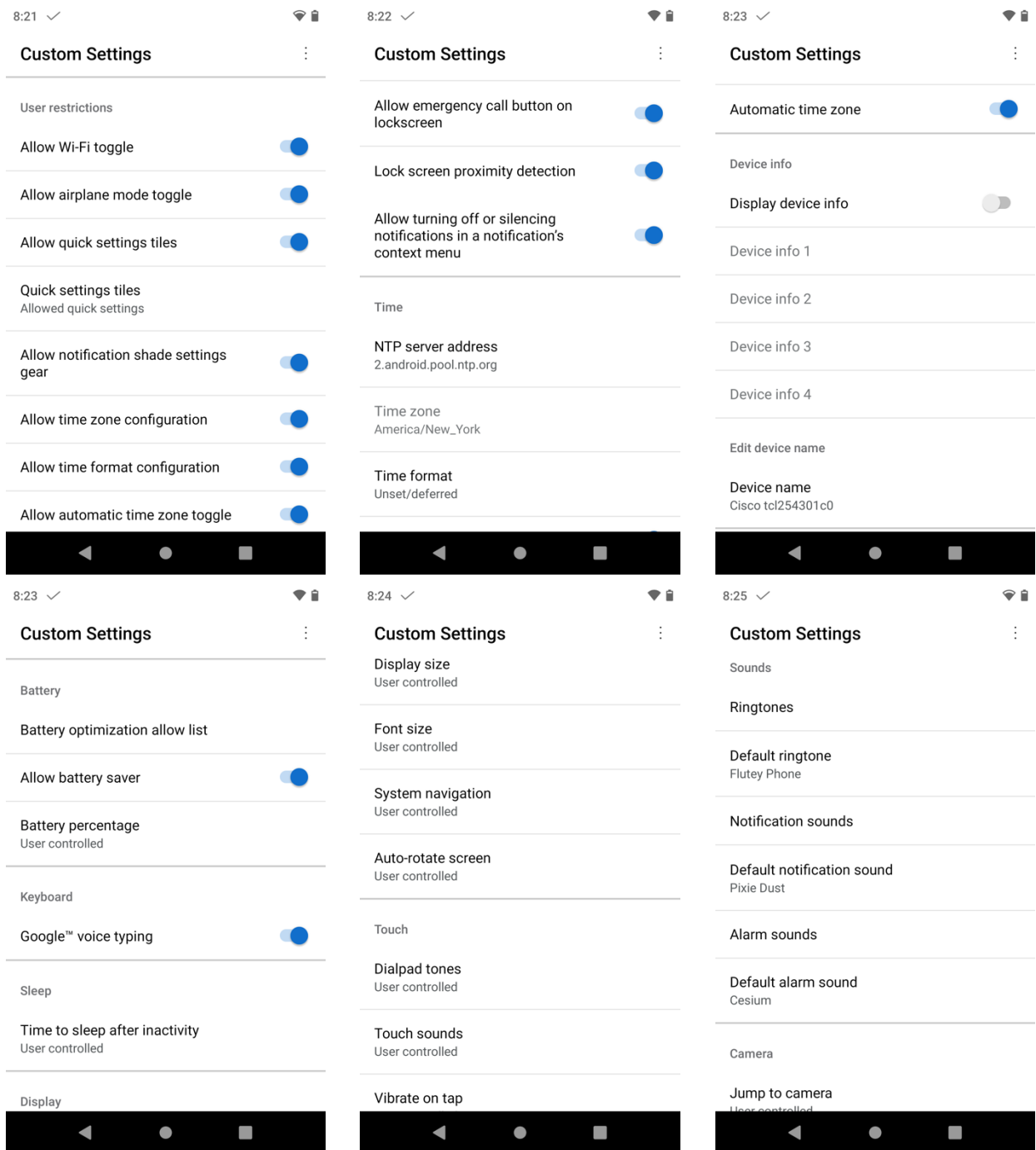


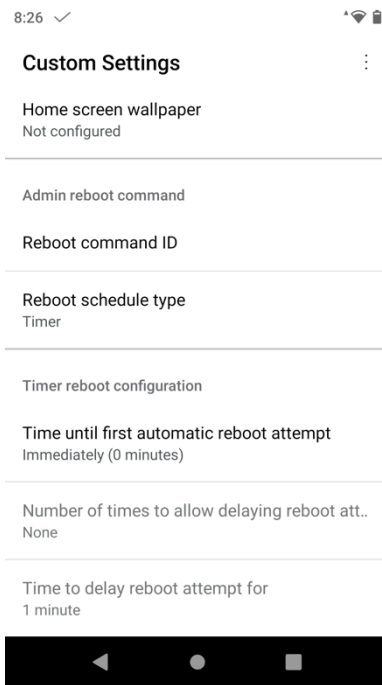
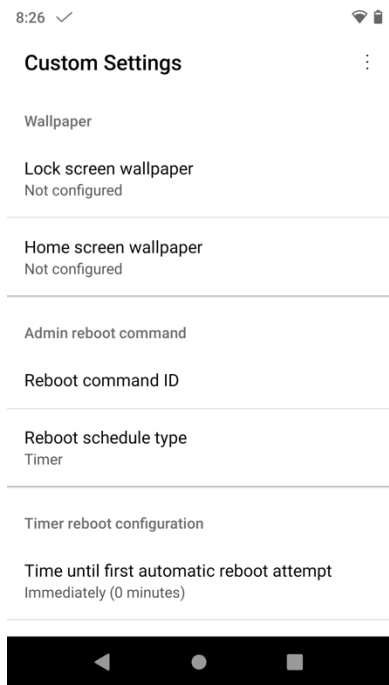
注：1.8(0) リリースでは、**CAC**（コール アドミッション コントロール）を無効にするオプションが有効になっています。

1.9(0) リリースでは、**CAC**（コールアドミッション コントロール）はデフォルトで無効になっており、オプション機能になりました。

カスタム設定

ユーザー制限、時間設定などのさまざまな設定は、**カスタム設定アプリケーション**でカスタム設定できます。





通知音を表示および管理するには、[サウンド (Sounds)]、[通知音 (Notifications)]の順に選択します。

アラーム音を表示および管理するには、[サウンド (Sounds)] > [アラーム音 (Alarm サウンド)]を選択します。

デフォルトの通知音とデフォルトのアラーム音は、[サウンド (Sounds)]メニューでも管理できます。

1.9(0) リリースでは、カスタム通知音とアラーム音を Cisco Unified Communications Manager 内で設定および管理し、電話機にダウンロードできます。

以下は、デフォルトの通知音として設定できるプレインストールされた通知音です。

- Adara
- Aldebaran
- Altair
- Alya
- Antares
- Antimony
- Arcturus
- Argon
- Beat Box Android
- Bellatrix
- Beryllium
- Betelgeuse
- Caffeinated Rattlesnake
- Canopus
- Capella
- Captain's Log
- Castor
- Ceti Alpha

- Cobalt
- Cricket
- Dear Deer
- Deneb
- Doink
- Don't Panic
- Drip
- Electra
- Fluorine
- Fomalhaut
- Gallium
- Heaven
- Helium
- Highwire
- Hojus
- Iridium
- Krypton
- Kzurb Sonar
- Lalande
- Look At Me
- Merope
- Mira
- Missed It
- Moonbeam
- On The Hunt
- Palladium
- Pixie Dust
- Pizzicato
- Plastic Pipe
- Polaris
- Procyon
- Proxima
- Radon
- Regulus
- Selenium
- Shaula
- Sirius
- Sirrah
- Space Seed
- Spica
- Strontium
- Syrma
- Ta Da
- Talitha
- Tejat
- Thallium
- Tinkerbell
- Tweeters
- Upsilon
- Vega
- Voila
- Xenon
- Zirconium

以下は、デフォルトのアラーム音として設定できるプレインストールされたアラーム音です。

- Argon
- Barium
- BeeBeep Alarm
- Beep-Beep-Beep Alarm
- Buzzer Alarm
- Carbon
- Cesium
- Fermium
- Hassium
- Helium
- Neptunium
- Nobelium
- Osmium
- Piezo Alarm
- Platinum
- Plutonium
- Rooster Alarm
- Scandium

注：1.5(0) リリースでは、インターネット上のデフォルトの NTP サーバーにアクセスできない場合に備えて、DHCP オプション 42 を NTP サーバーの設定に使用できるようになりました。

緊急 (Emergency)

モーションセンサー、パニックボタン、緊急コール、トーンの設定などの緊急設定は、**緊急アプリケーション**で右上隅にある 3 つのドットを選択し、**[設定 (Settings)]** を選択することで設定できます。

10:42

Emergency



Panic button feature is disabled

When activated:

- Alarm will not sound
- Emergency call will not be placed

10:43

Emergency



Long press to trigger panic alarm

When activated:

- Alarm will not sound
- Emergency call will not be placed



10:42

← Emergency settings

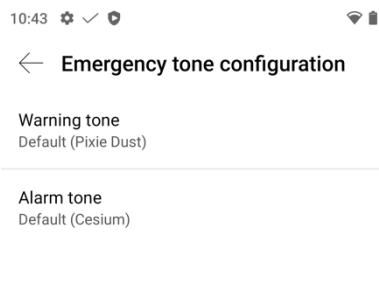
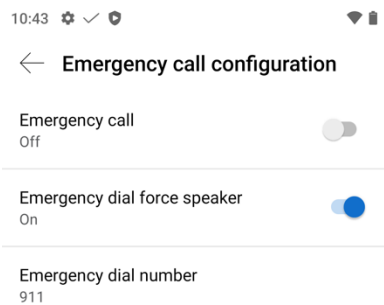
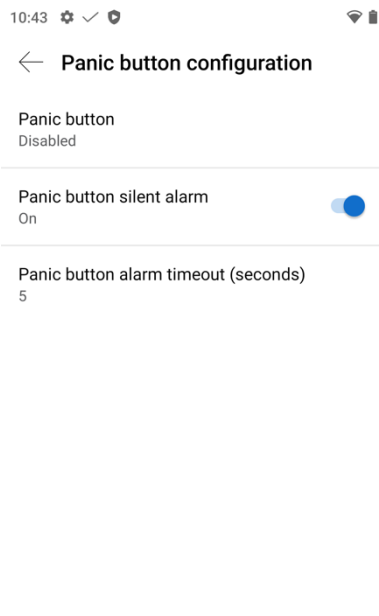
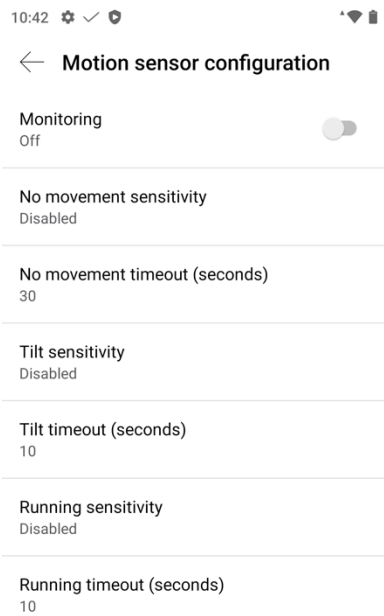
Motion sensor configuration
Motion sensor configuration

Panic button configuration
Button behavior and silent alarm

Emergency call configuration
Emergency call behavior

Emergency tone configuration
Emergency tone selection



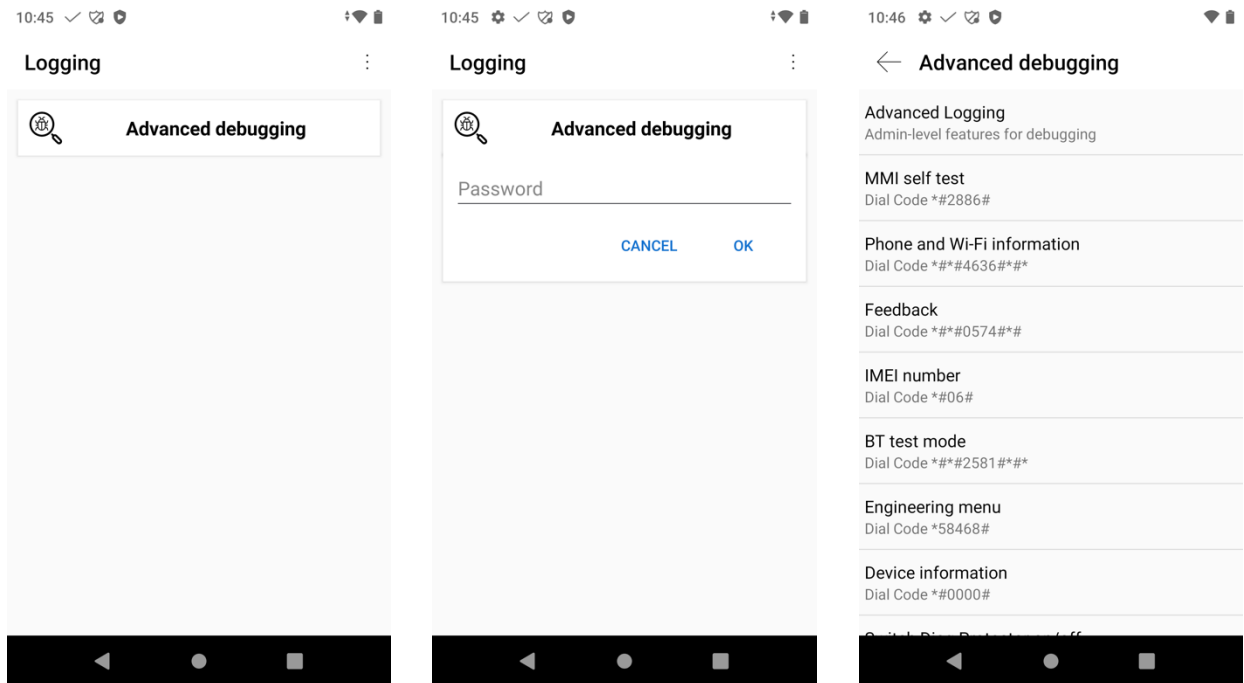


注：Cisco Wireless Phone 840 および Cisco Wireless Phone 860 の右上には、緊急ボタン（赤色のボタン）があります。

ロギング

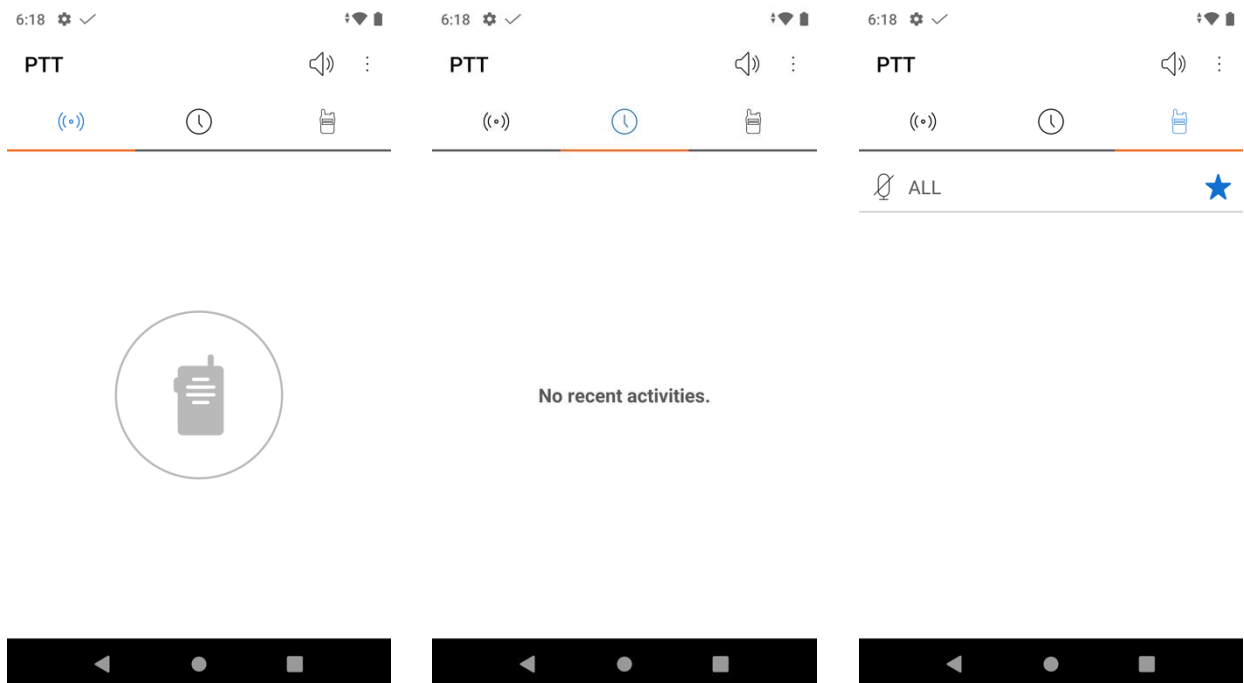
ロギング アプリケーションでは、さまざまなデバッグ オプションを使用できます。

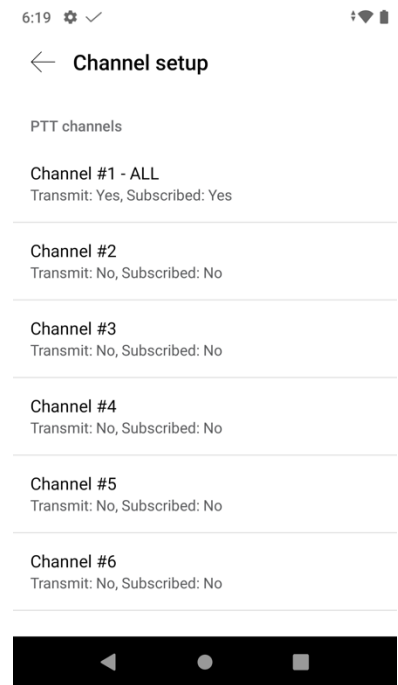
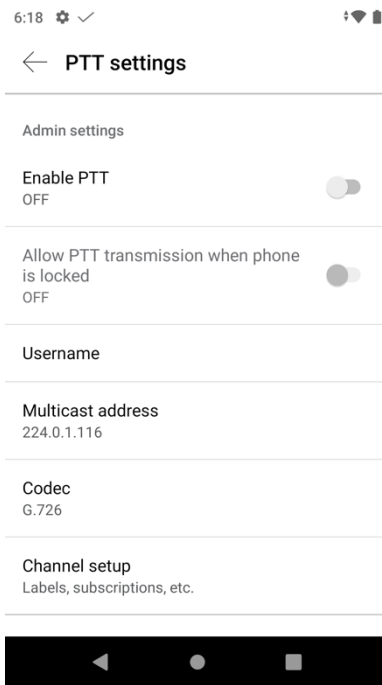
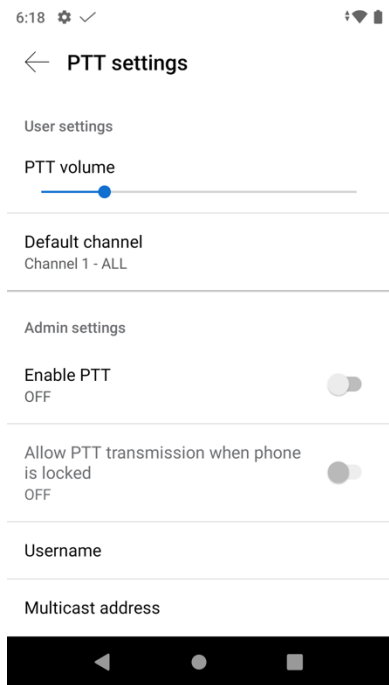
入力画面で、ローカル電話機ロック解除パスワードを入力します（デフォルト = **#）。



PTT

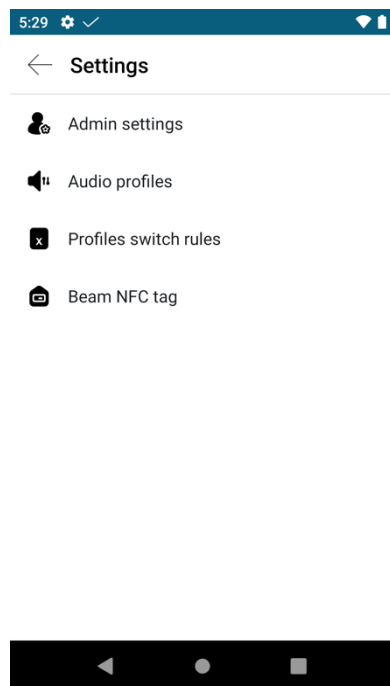
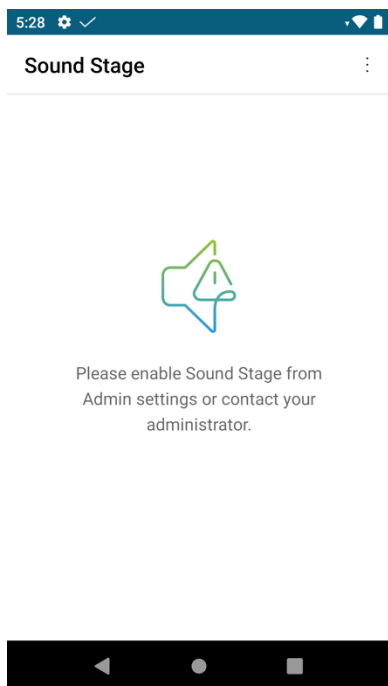
プッシュ ツーク (PTT) 設定は、PTT アプリケーションで右上隅にある 3 つのドットを選択し、**[設定 (Settings)]** を選択することで設定できます。



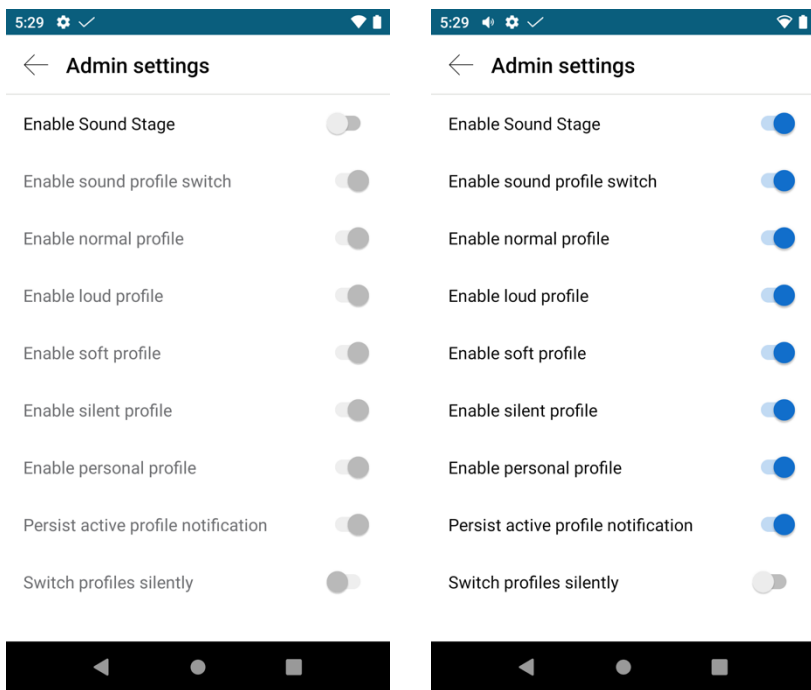


サウンドステージ

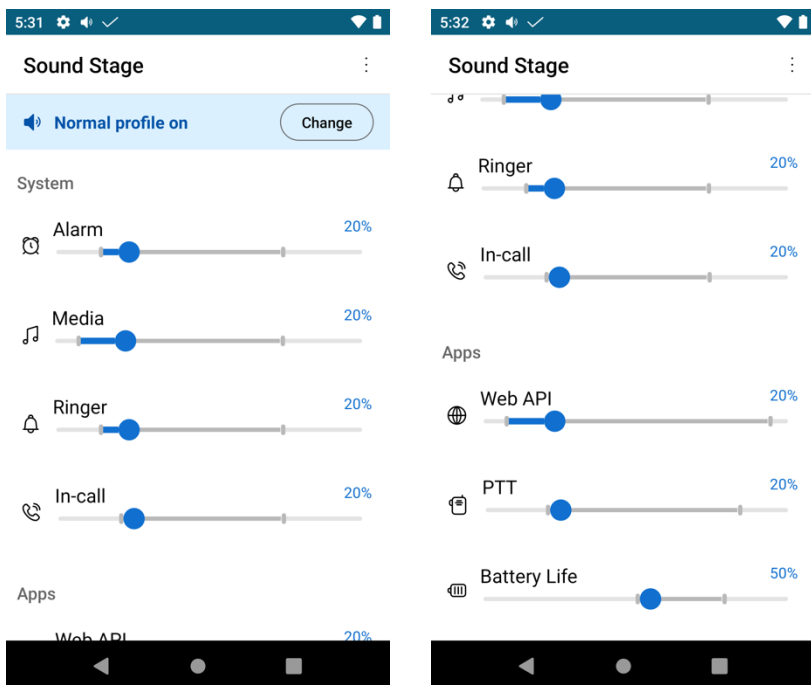
サウンドステージの設定を構成するには、サウンドステージアプリケーションで右上隅にある3つのドットを選択し、**【設定 (Settings)】**を選択します。



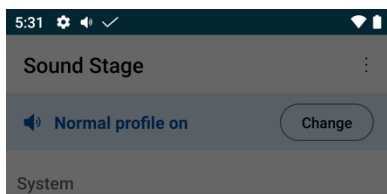
サウンドステージを有効にするには、**【管理設定 (Admin settings)】**を選択し、**【サウンドステージの有効化 (Enable Sound Stage)】**のスライダーが右側にあることを確認します。



[サウンドステージの有効化 (Enable Sound Stage)] を有効にすると、デフォルトで [標準 (Normal)] プロファイルが選択されます。



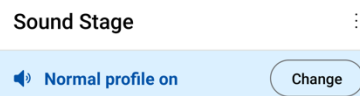
現在のオーディオプロファイルは、メインの [サウンドステージ (Sound Stage)] 画面で [変更 (Change)] を選択して変更できます。



CHANGE AUDIO PROFILE

- Normal
- Loud
- Soft
- Silent
- Personal

The audio profile could also be changed by scanning a programmed NFC tag without the phone open.

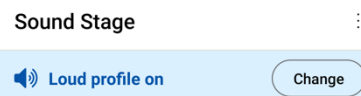


System

- Alarm 20%
- Media 20%
- Ringer 20%
- In-call 20%

Apps

Web API 20%



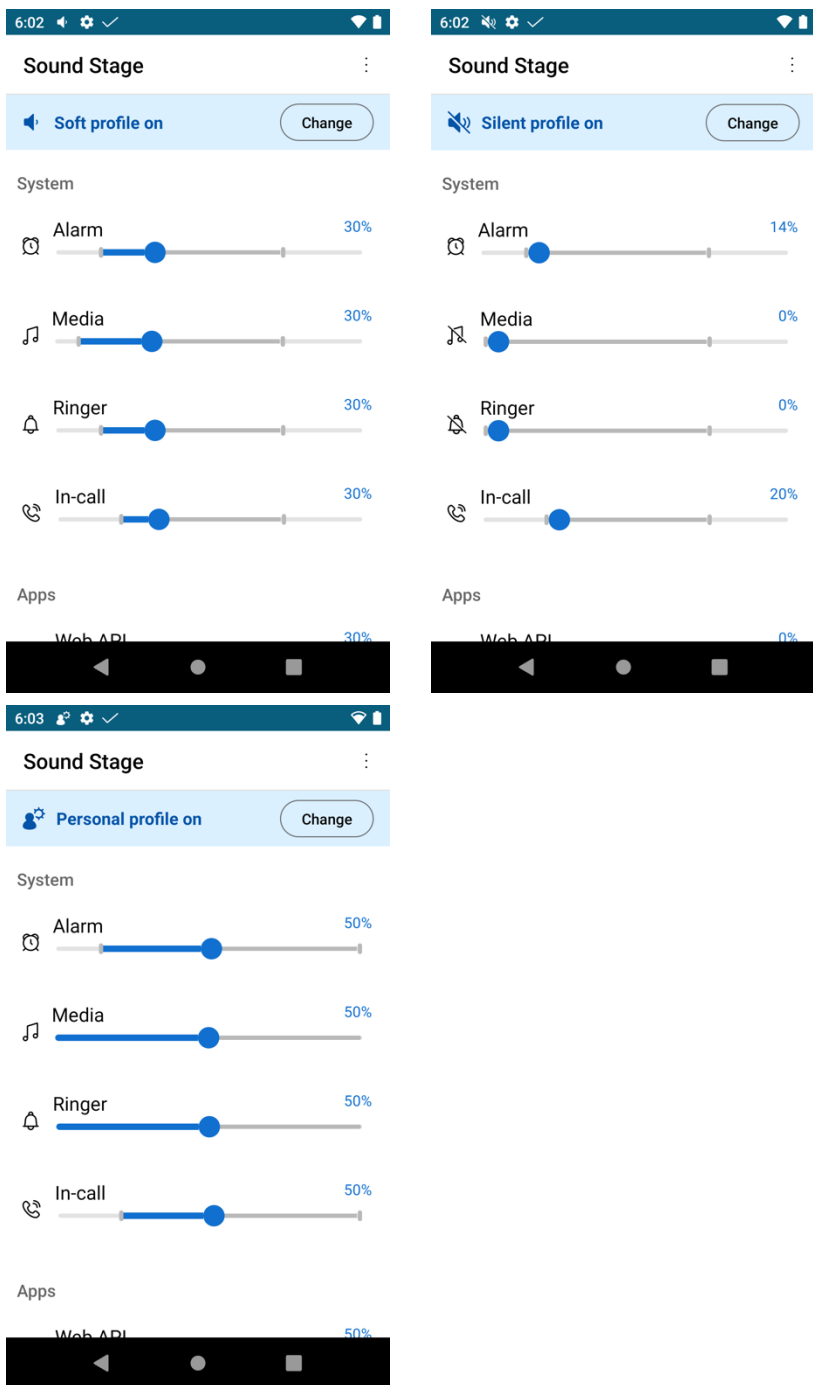
System

- Alarm 75%
- Media 75%
- Ringer 75%
- In-call 75%

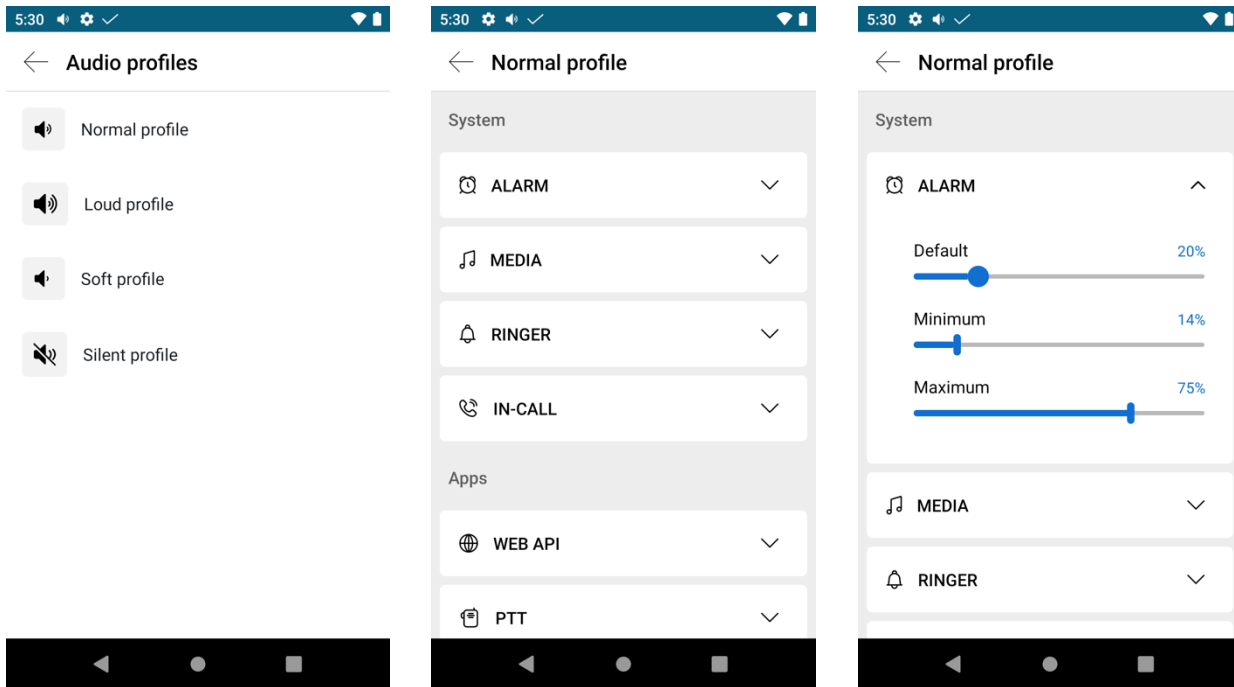
Apps

Web API 75%

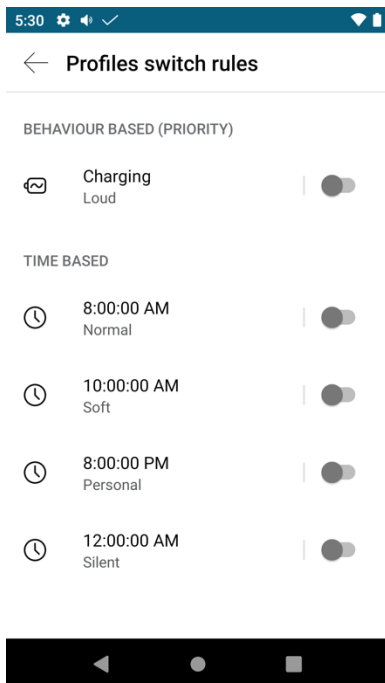




オーディオプロファイルを設定するには、[オーディオプロファイル (Audio profiles)] を選択します。システムとアプリケーションのデフォルト、最小、および最大音量は、オーディオプロファイルごとに設定できます。

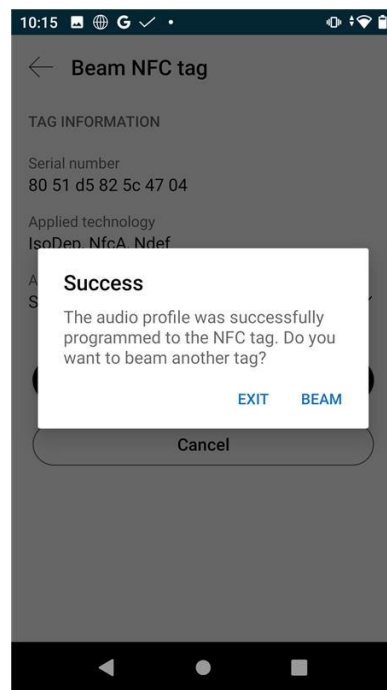
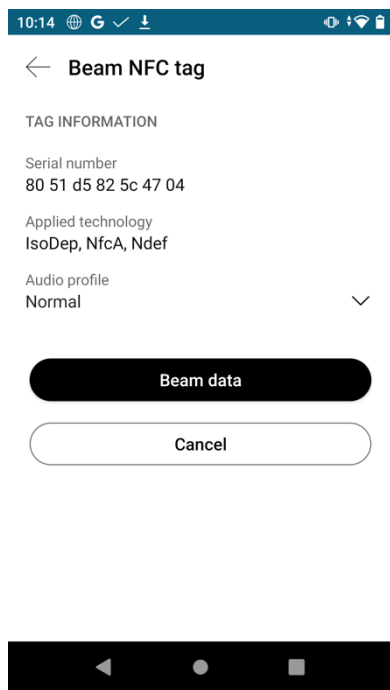
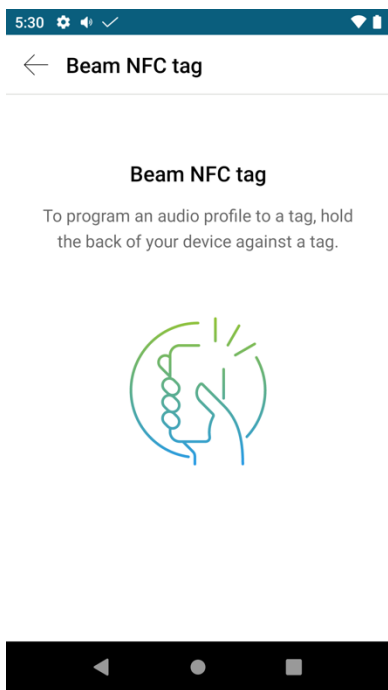


プロファイル切り替えルールを設定するには、[プロファイル切り替えルール (Profiles switch rules)] を選択します。

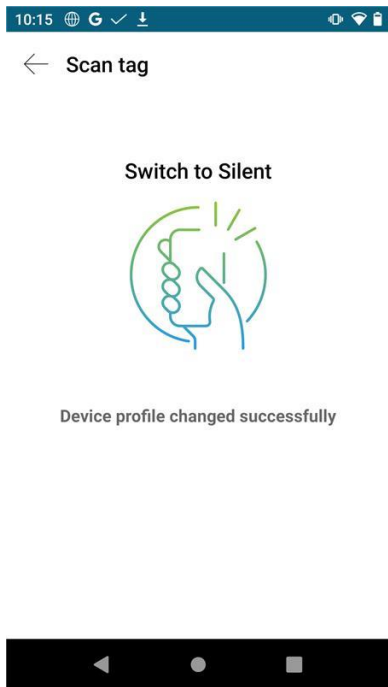


[NFC タグをビーム (Beam NFC tag)] を選択することで、特定のオーディオプロファイルに対して NFC タグをプログラムできます。

これは、ユーザーがある環境から別の環境に移動する際に、より少ないボリュームまたはより大きなボリュームを必要とする場合に役立ちます。

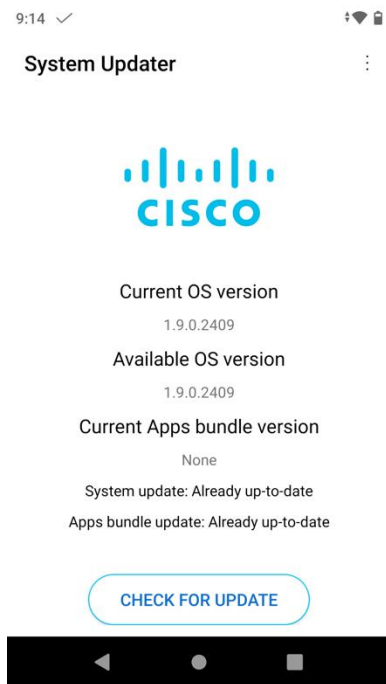


NFC タグがスキャンされ、音声プロファイルが設定されると、確認画面が表示されます。



システムアップデート

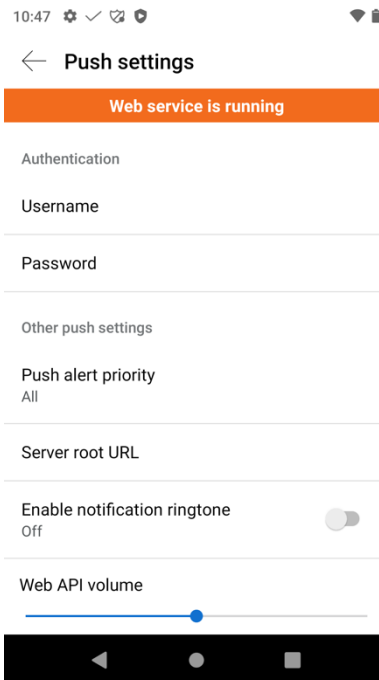
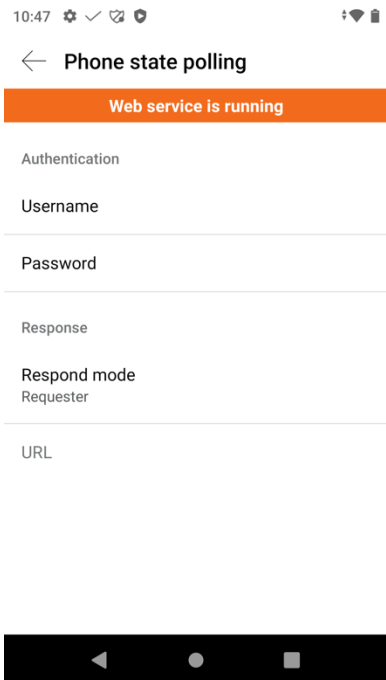
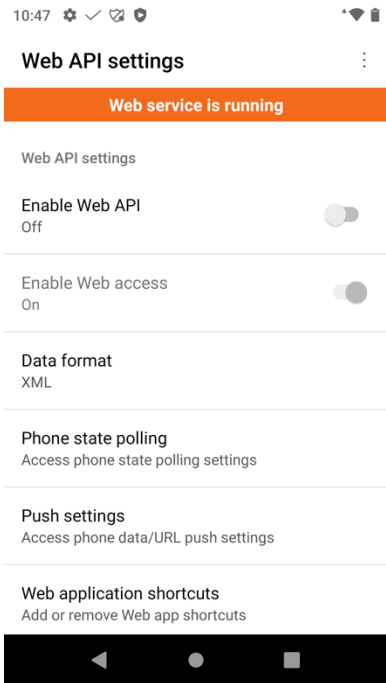
管理者は、ファームウェアの更新を管理し、Cisco 無線電話 840 および 860 にプッシュダウンします。コールサーバーで [ソフトウェア アップデートのダウンロード後すぐに再起動する (Reboot successfully after download software updates)] オプションが有効になっていない限り、ユーザーは再起動して新しいファームウェアを適用することを確認するように求められます。

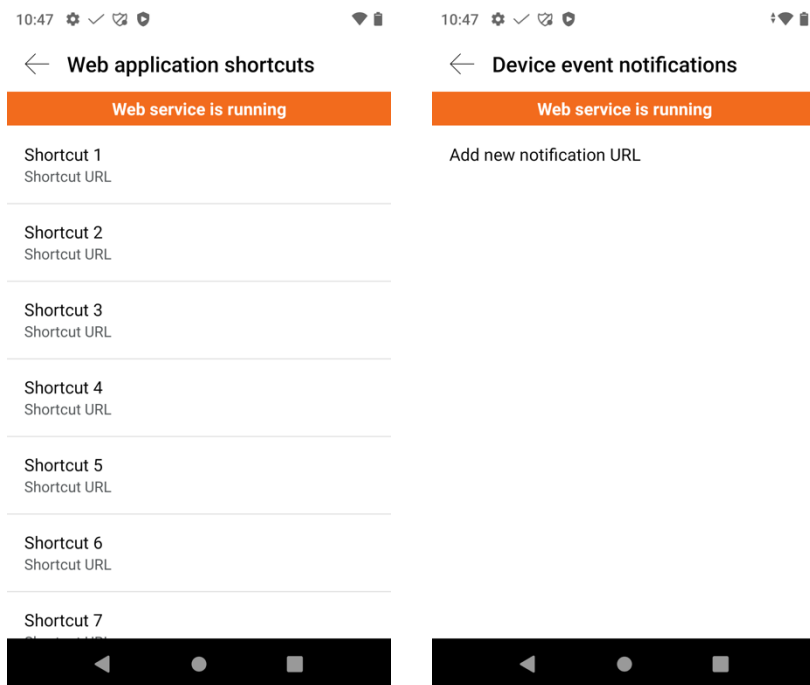


注：システム アップデータ アプリケーションは、ファームウェアの更新に直接使用しないでください。

Web API

Web API 設定は、**Web API** アプリケーションでカスタム設定できます。





注：詳細については、『Cisco Wireless Phone 800 Series Developer's Guide』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

アプリケーションストア

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 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>

IP Phone サービス (IP Phone Services)

次のドキュメントには、アプリケーション開発者が Cisco Wireless Phone 840 および 860 用の IP 電話サービスを作成および展開するために必要な情報が記載されています。

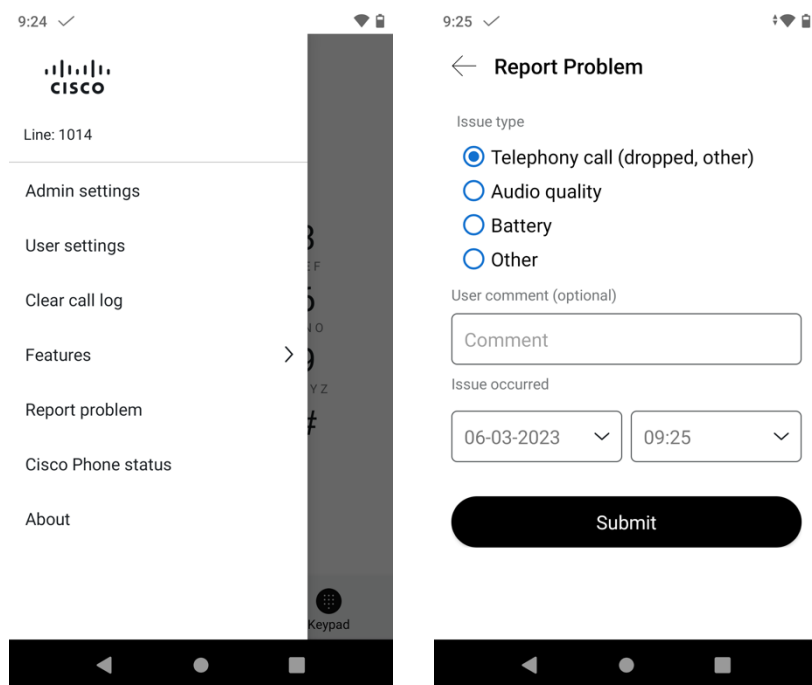
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

トラブルシューティング

問題レポート ツール

問題レポートを作成するには、**Cisco Phone** アプリケーションで左上隅にある 3 本の線を選択し、**[問題の報告 (Report problem)]** を選択します。

Cisco Unified Communications Manager の**カスタマー サポート アップロード URL** オプションは、電話機ごとに設定して、ログを自動的に取得するか、**[デバイスログ (Device Logs)]** の下にある電話機の Web ページからログを手動でダウンロードできます。



カスタマー サポート アップロード URL の設定

サーバでアップロード スクリプトを使用して PRT ファイルを受信する必要があります。PRT は、HTTP POST メカニズムを使用し、次のパラメータをアップロード（マルチパート MIME エンコーディングを使用）に含めます。

- devicename (例 : "SEP001122334455")
- serialNo (例 : "FCH12345ABC")
- username (Cisco Unified Communications Manager で設定される、デバイス所有者のユーザ名)
- prt_file (例 : "probrep-20141021-162840.tar.gz")

サンプル スクリプト

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "\\");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "\\");

$username = $_POST['username'];
$username = trim($username, "\\");

// where to put the file
$fullfilename = "/var/prtuploads/" . $filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}

?>
```

電話機の Web ページ

電話機の Web ページ インターフェイスにアクセスすると、Cisco Wireless Phone 840 および 860 の情報をリモートから収集できます。

Web ページインターフェイス (<https://x.x.x.x>) には、デバイス情報、ネットワーク情報、登録情報、およびデバイスログに関する読み取り専用の情報が含まれています。Web ページインターフェイスにアクセスするには、コールサーバーで **Web アクセス** を有効にする必要があります。

デバイス情報


Cisco Wireless Phone 840 および 860 のデバイス情報が提供されます。ここでは、MAC アドレス、およびバージョン情報が表示されます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<https://x.x.x.x>) にアクセスし、[デバイス情報 (Device information)] を選択します。

Cisco Unified Communications Manager

		Device information	
		Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)	
Device information	Device Serial No	tcl254301c0	
Network information	Device name	SEP10F9201932ed	
Registration information	Product ID	CP-860S	
Device logs	Version ID	V01	
	Model number	CP-860S	
	Time	Sat Jun 03 21:58:46 EDT 2023	
	Time zone	America/New_York	
	Platform version	sip860 QKQ1.201230.002 1.9.0.2409	
	APK bundle version	None	
	Cisco Dialer version	21.5.65593	
	Emergency version	21.3.64939-cisco	
	WebAPI version	21.3.64946-cisco	
	Load ID	sip860-1.9.0.2409-65593	
	Device admin app		
	Certificate Trust List (CTL) download		
	Status	Downloader file not found	
	URI	http://10.195.19.43:6970/CTLSEP10F9201932ED.tlv	
	Time	Sat Jun 03 19:57:56 EDT 2023	
	MD5 hash		
	Initial Trust List (ITL) download		
	Status	Download successful	
	URI	http://10.195.19.43:6970/ITLSEP10F9201932ED.tlv	
	Time	Sat Jun 03 19:57:57 EDT 2023	
	MD5 hash	a7af30890e5ce7c5b2f957cc959eca23	

Webex Calling

	Device information Cisco Webex Wireless Phone CP-860 (10F920194A8D)	
Device information Network information Registration information Device logs	Device Serial No	tcl254400ds
	Device name	10f920194a8d
	Product ID	CP-860
	Version ID	V01
	Model number	CP-860
	Time	Mon Jun 05 16:24:19 EDT 2023
	Time zone	America/New_York
	Platform version	sip860 QKQ1.201230.002 1.9.0.2409
	APK bundle version	None
	Cisco Dialer version	21.5.65593
	Emergency version	21.3.64939-cisco
	WebAPI version	22.1.68093-cisco
	Load ID	sip860-1.8.0.2136-55928
	Profile Rule	https://cisco-int.bcl.d.webex.com/dms/CP860/860.xml Download successful Mon Jun 05 15:51:07 EDT 2023
	Profile Rule B	https://cisco-int.bcl.d.webex.com/dms/CP860/10f920194a8d.xml Download successful Mon Jun 05 15:51:11 EDT 2023
	Profile Rule C	
	Profile Rule D	
	Upgrade Rule	https://binaries.webex.com/cisco-860-stable/20221201164830/sip860-1.8.0.2136-55928.iosads Download successful Mon Jun 05 15:51:12 EDT 2023

ネットワーク情報

Cisco Wireless Phone 840 および 860 はネットワーク情報を提供し、無線 LAN とネットワークの情報が表示されます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<https://x.x.x.x>) にアクセスし、[ネットワーク情報 (Network information)] を選択します。



Network information

Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)

[Device information](#)

[Network information](#)

[Registration information](#)

[Device logs](#)

Active network interface	WLAN
MAC address	10:f9:20:19:32:ed
Bluetooth address	10:f9:20:19:32:ec
SSID	baker
BSSID	c8:28:e5:ef:04:7a
Frequency	5GHz
DHCP server	64.101.49.191
DHCP	Yes
IP address	10.81.12.28
Subnet mask	255.255.255.0
Gateway	10.81.12.1
DNS server 1	64.102.6.247
DNS server 2	171.70.168.183
NTP server address	2.android.pool.ntp.org

登録情報

Cisco Wireless Phone 840 および 860 は登録情報を提供し、電話機の DN と登録ステータス情報が表示されます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<https://x.x.x.x>) にアクセスし、[登録情報 (Registration information)] を選択します。

Cisco Unified Communications Manager



Registration information

Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)

[Device information](#)
[Network information](#)
[Registration information](#)
[Device logs](#)

UCM

Phone DN	Shared Line	Auto Answer	Call Forward	Forwarded Address	Status
1014	True	Disabled	Disabled		Registered


SECONDARY REGISTRATION

Phone DN	
SIP Server	
Server Port	
Protocol	
SIP Code	
Status	

CALL SERVER FEATURES

Hunt Group	Enabled
Hunt Group Status	Logged out
Visual Voicemail	Enabled
Privacy	Enabled

Webex Calling



Registration information

Cisco Webex Wireless Phone CP-860 (10F920194A8D)

[Device information](#)
[Network information](#)
[Registration information](#)
[Device logs](#)

WEBEX

Line Number	Line Name	Shared Line	Call Forward	Forwarded Address	Status
2675	bbqfx45w29	True	Disabled		Registered

ACCOUNT INFO

SIP Server	199.19.196.177
Server Port	8934
Protocol	TLS

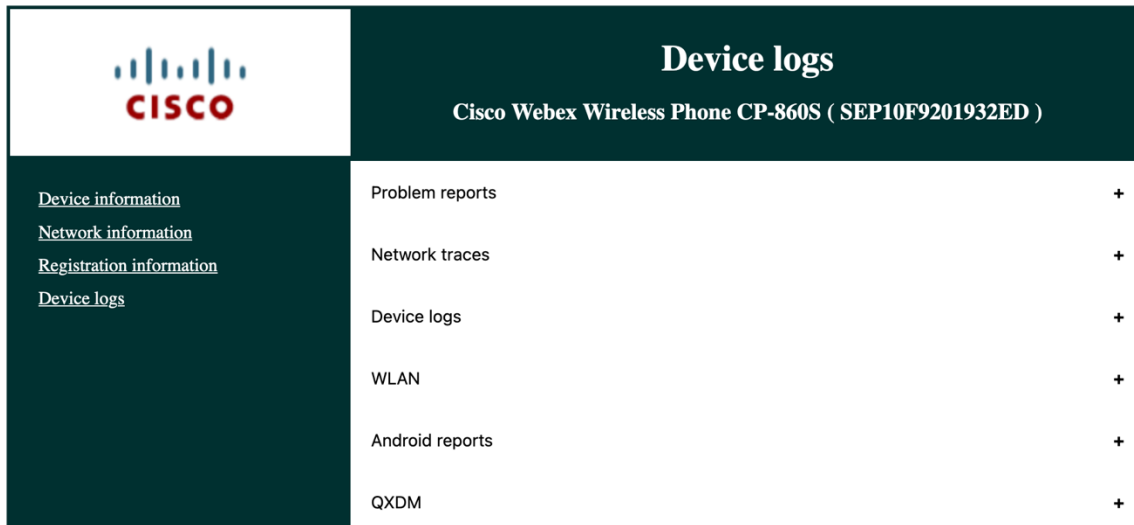
CALL SERVER FEATURES

Voicemail	Disabled
-----------	----------

デバイス ログ

トラブルシューティング用のデバイスログは、Cisco Wireless Phone 840 または 860 の Web インターフェイスから入手できます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<https://x.x.x.x>) にアクセスし、[デバイスログ (Device logs)] を選択します。



Device logs	
Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)	
Device information	Problem reports +
Network information	Network traces +
Registration information	Device logs +
Device logs	WLAN +
	Android reports +
	QXDM +

ログファイルタイプ ([**問題レポート (Problem reports)**]、[**ネットワークトレース (Network Traces)**]、[**デバイスログ (Device logs)**]、[**WLAN**]、[**Android レポート (Android reports)**]、[**QXDM**]) の右側にある [+] 記号をクリックすると、これらのログ ファイルが一覧表示され、ダウンロードできます。

1.6(0) リリースでは、Cisco Wireless Phone 840 および 860 を介して問題レポートとネットワークトレースをキャプチャできます。

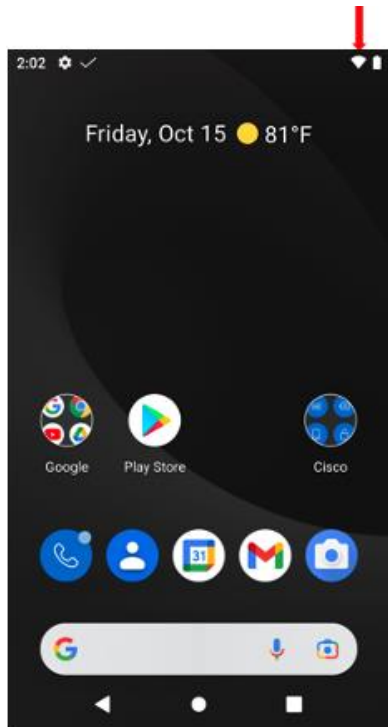
問題レポートを生成するには、[**問題レポート (Problem reports)**] の [**PRT の生成 (Generate PRT)**] を選択します。

ネットワークトレースをキャプチャするには、[**Network traces**] で [**Start Packet Capture**] を選択します。パケットのキャプチャを停止するには、[**パケットキャプチャの停止 (Stop Packet Capture)**] を選択します。

WLAN 信号インジケータ

Cisco Wireless Phone 840 および 860 の WLAN 信号インジケータは、ディスプレイの右上隅に表示されます。

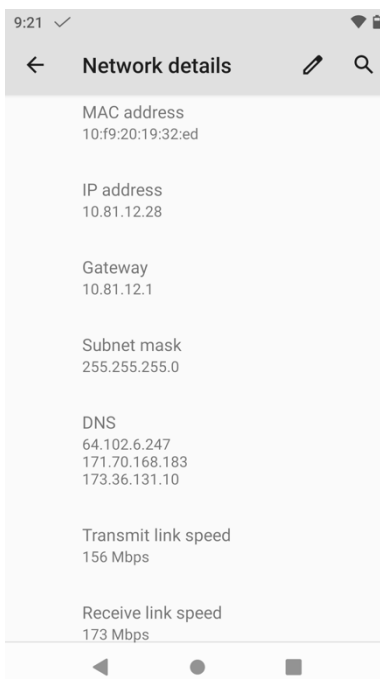
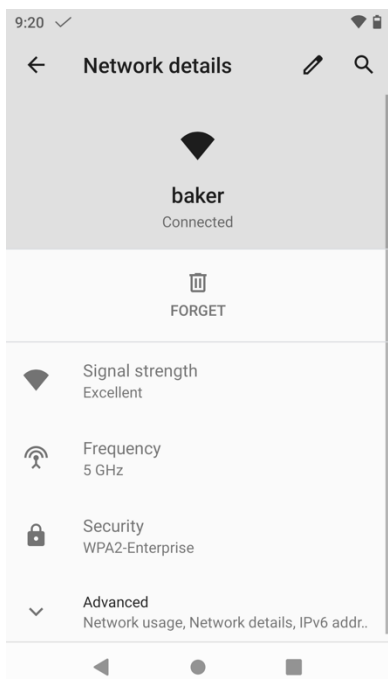
Cisco Wireless Phone 840 および 860 がアクセスポイントに接続されると、次のようにアイコンがグレーになります。



WLAN ネットワーク情報

Cisco Wireless Phone 840 および 860 の現在の WLAN ネットワーク情報を表示するには、**[設定 (Settings)]**、**[ネットワークとインターネット (Network and Internet)]**、**[Wi-Fi]** の順に選択し、接続されている Wi-Fi ネットワークを選択します。

設定済みの Wi-Fi ネットワークは、**[削除 (Forget)]** を選択して削除できます。



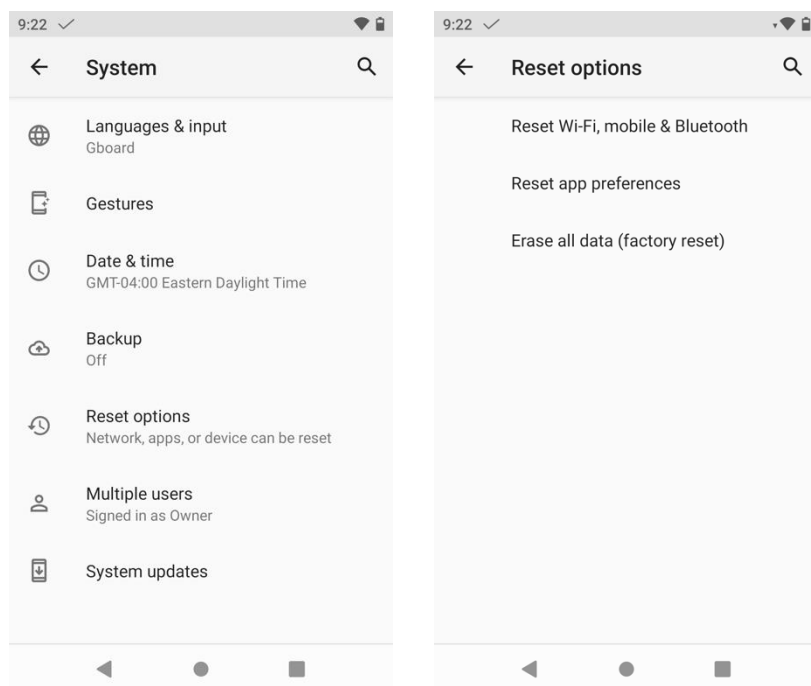
初期化

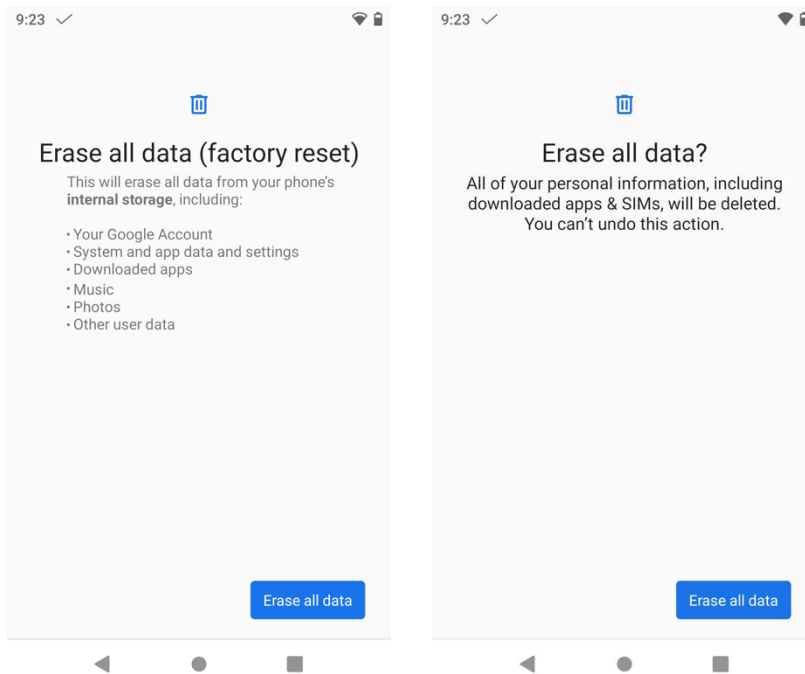
Cisco Wireless Phone 840 および 860 の設定を工場出荷時のデフォルトにリセットするには、**[Settings]**、**[System]**、**[Advanced]**、**[Reset options]**、**[Erase all data (factory reset)]** の順に選択します。

消去されるすべてのデータを示す情報画面が表示されます。初期設定へのリセットを続行するには、**[すべてのデータを消去 (Erase all data)]** を選択する必要があります。

確認画面が表示されたら、**[すべてのデータを消去 (Erase all data)]** を選択して、データを初期化します。

電話機が再起動し、工場出荷時の設定が復元された状態で起動します。





Cisco Wireless Phone 840 または 860 を正しく起動できない場合は、次の手順でも初期化を開始できます。

- 電源ボタン (Cisco ワイヤレス電話 840 の場合は左上のボタン、Cisco ワイヤレス電話 860 の場合は右側の上から 2 番目のボタン) を押して電話機の電源をオフにし、**【電源オフ (Power off)】** を選択します。
- **緊急ボタン** (Cisco Wireless Phone 840 および Cisco Wireless Phone 860 の右上にある赤いボタン) を押したままにして、電話機の電源をオンにします。
- 赤い**緊急ボタン**を押したまま、電話機が振動するまで**電源ボタン**を押したままにしてから、**電源ボタン**を放します。
- **【ブートローダー (Bootloader)】**画面が表示されたら、赤い**緊急ボタン**を放します。
- リカバリモードが表示されるまで音量小ボタンを押し、電源ボタンを押してそのオプションを選択します。
- 電話機が再起動し、Android アイコンを表示された新しい画面に戻ります。
- この画面で電源ボタンを押したまま、**【音量を上げる (Volume up)】**ボタンをすばやく押し放し、**【リカバリメニュー (Recovery Menu)】**画面に入力します。
- **【リカバリメニュー (Recovery Menu)】**が表示されたら、**電源ボタン**を放します。
- 音量小ボタンを押して**【データの消去/初期設定へのリセット (Wipe data/factory reset)】**を強調表示し、電源ボタンを押してそのオプションを選択します。
- 音量小ボタンを押して**【データの初期化 (Factory data reset)】**を強調表示し、電源ボタンを押してそのオプションを選択します。
- **Reboot system now** が強調表示されたら、**電源ボタン**を再度押します。
- Cisco Wireless Phone 840 または 860 が再起動し、工場出荷時の設定に復元されます。

注： Cisco Wireless Phone 840 または 860 が Google アカウントにサインインしている場合、電話機は工場出荷時のワイプ保護が有効になっています。この保護は、設定された Google アカウントが削除されるまで有効のままです。

工場出荷時設定へのリセット方法を使用する場合、デフォルト設定を復元した後は工場出荷時のワイプ保護をバイパスすることはできません。

したがって、設定済みの Google アカウントを正常に削除するには、電話機の Android ユーザ インターフェイスを使用して Cisco Wireless Phone 840 または 860 を初期設定にリセットする必要があります。

ログイン情報が不明で、電話機の Android ユーザーインターフェイスにアクセスして電話機を初期設定にリセットできない Google アカウントが設定されている場合、電話機は回復不能であり、保証の下で交換することはできません。

電話機画面のスクリーンショットのキャプチャ

Cisco Wireless Phone 840 または 860 の現在の表示は、電源ボタンを押して **[スクリーンショット (Screenshot)]** を選択することでキャプチャできます。

その他のマニュアル

Cisco Wireless Phone 840 および 860 データシート

<https://www.cisco.com/c/en/us/products/se/2020/11/Collateral/datasheet-c78-744461.html>

Cisco Wireless Phone 840 および 860 ユーザーガイド

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Cisco Wireless Phone 840 および 860 ユーザーガイド

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html

Cisco Wireless Phone 840 および 860 クイックリファレンスガイド

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/800-series/grg/webex_wireless_phone_840_grg.pdf

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/800-series/grg/webex_wireless_phone_860_grg.pdf

Cisco Wireless Phone 840 および 860

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/webex-wireless-phone/products-release-notes-list.html>

Cisco Wireless Phone 840 および 860

<https://software.cisco.com/download/home/286327931>

Cisco Unified Communications Manager

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/series.html>

Webex Calling

<https://help.webex.com>

Cisco Voice ソフトウェア

<https://software.cisco.com/download/home/278875240>

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

Cisco Wireless Phone 800 Series 開発者向けガイド

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

Real-Time Traffic over Wireless LAN

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rto wlan-srnd.html

Cisco Unified Communications 設計ガイド

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html>

Cisco AireOS ワイヤレス LAN コントローラに関するドキュメント

<https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

Cisco Catalyst IOS XE ワイヤレス LAN コントローラに関するドキュメント

https://www.cisco.com/c/ja_ip/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html

Cisco Mobility Express に関するドキュメント

<https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-and-configuration-guides-list.html>

Cisco Autonomous アクセス ポイントに関するドキュメント

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/atnms-ap-8x/configuration/guide/cg-book.html

Cisco Meraki ワイヤレス LAN に関するドキュメント

<https://documentation.meraki.com>

CCDE、CCENT、Cisco Eos、Cisco Lumin、Cisco Nexus、Cisco StadiumVision、Cisco TelePresence、WebEX、Cisco ロゴ、DCE、および Welcome to the Human Network は商標です。Changing the Way We Work, Live, Play, and Learn および Cisco Store はサービスマークです。Access Registrar、Aironet、AsyncOS、Bringing the Meeting To You、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、CCSP、CCVP、Cisco、Cisco Certified Internetwork Expert ロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems ロゴ、Cisco Unity、Collaboration Without Limitation、EtherFast、EtherSwitch、Event Center、Fast Step、Follow Me Browsing、FormShare、GigaDrive、HomeLink、Internet Quotient、IOS、iPhone、iQuick Study、IronPort、IronPort ロゴ、LightStream、Linksys、MediaTone、MeetingPlace、MeetingPlace Chime Sound、MGX、Networkers、Networking Academy、Network Registrar、PCNow、PIX、PowerPanels、ProConnect、ScriptShare、SenderBase、SMARTnet、Spectrum Expert、StackWise、The Fastest Way to Increase Your Internet Quotient、TransPath、Webex、および Webex ロゴは、Cisco またはその関連会社の米国およびその他の国における登録商標です。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧は、http://www.cisco.com/web/JP/trademark_statement.html でご確認いただけます。Third-party trademarks mentioned are the property of their respective owners。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)。

本ドキュメントまたは Web サイトに掲載されているその他の商標はそれぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(0809R)。



Bluetooth の用語マークとロゴは、Bluetooth SIG, Inc. が所有する登録商標であり、かかる商標の Cisco Systems, Inc.による使用はライセンスに基づいています。

© 2023 Cisco Systems, Inc. All rights reserved.