Webex Desk Series
ワイヤレス LAN 展開ガイド

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

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

このガイドでは、ネットワーク管理者がワイヤレス LAN 環境内でこの Webex Desk Series を展開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
07/14/21	10.5(1) リリース
10/19/21	10.8(1) リリース
01/17/22	10.11(1) リリース
03/25/22	10.13(1) リリース

目次

Webex Desk Series 概要

Webex Desk Series は、企業内のコラボレーションを提供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、音声やビデオといった、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、Webex Desk Series 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。

Webex Desk Series 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、マルチメディア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。Webex Desk Series 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。

製品モデル

次の Webex Desk Series モデルが利用可能です。

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	使用可能なチャネル	チャネル セット
CS-DESKPRO-K9	Webex Desk Pro	2.4 GHz = 4.13 dBi 5 GHz = 5.95 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	13 4 4 12 5	1 ~ 13 36、40、44、48 52、56、60、64 100 ~ 144 149、153、157、161、165
CS-DESK-LE-K9	Webex Desk Limited Edition	2.4 GHz = 4.13 dBi 5 GHz = 5.95 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	13 4 4 12 5	1 ~ 13 36、40、44、48 52、56、60、64 100 ~ 144 149、153、157、161、165

CS-DESK-K9	Webex Desk	2.4 GHz = 3.40 dBi 5 GHz = 6.10 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	13 4 4 12 5	1 ~ 13 36、40、44、48 52、56、60、64 100 ~ 144 149、153、157、161、165
CS-DESKMINI-K9	Webex Desk Mini	2.4 GHz = 5.00 dBi 5 GHz = 4.90 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	13 4 4 12 5	1 ~ 13 36、40、44、48 52、56、60、64 100 ~ 144 149、153、157、161、165
CD-DSKH-HUB-C-K9	Webex Desk Hub、カーボン	2.4 GHz = 3.55 dBi 5 GHz = 6.67 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	13 4 4 12 5	1 ~ 13 36、40、44、48 52、56、60、64 100 ~ 144 149、153、157、161、165
CD-DSKH-HUB-P-K9	Webex Desk Hub、プラチナ				

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。

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

日本用のチャネル 14 はサポートされていません。

要件

Webex Desk Series は、音声、ビデオ、およびデータ通信を提供する IEEE 802.11a/b/g/n/ac コラボレーション デバイスです。

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

サイト調査

Webex Desk Series を実稼働環境に展開する前に、先進的なワイヤレス LAN を専門とする Cisco 認定パートナーの手でサイト調査を実施する必要があります。サイト調査時に、RF 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 Webex Desk Series を基幹業務で使用する場合は 5 GHz の使用が強く推奨されます。サイト調査には、その場所の対象カバレッジ プランを示すヒートマップも含まれます。さらにサイト調査では、その場所で使用するアクセス ポイント プラットフォーム

タイプ、アンテナ タイプ、アクセス ポイント設定（チャネルと送信電力）も決定されます。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。

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

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、Webex Desk Series 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、Webex Desk Series 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、Webex Desk Series シリーズが信号を 5 秒以上保持できるように設計することを推奨します。

チャネルの使用率

チャネル使用率レベルは 40 % 未満に維持される必要があります。

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、Webex Desk Series 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もあります。

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

Webex Desk Series は、次の呼制御プラットフォームでサポートされています。

- **Webex Desk Pro**
  - Webex
  - Cisco Unified Communications Manager（CUCM）

    最小 = 10.5(2)

    推奨 = 11.5(1)、12.0(1)、12.5(1)、14.0(1) 以降
- **Webex Desk Limited Edition**
  - Webex
  - Cisco Unified Communications Manager（CUCM）

    最小 = 11.5(1)

    推奨 = 12.5(1)、14.0(1) 以降
- **Webex Desk**
  - Webex
  - Cisco Unified Communications Manager（CUCM）

    最小 = 11.5(1)

    推奨 = 12.5(1)、14.0(1) 以降
- **Webex Desk Mini**
  - Webex
  - Cisco Unified Communications Manager（CUCM）

    最小 = 11.5(1)

    推奨 = 12.5(1)、14.0(1) 以降
- **Webex Desk Hub**
  - Webex
  - Cisco Unified Communications Manager（CUCM）

    最小 = 11.5(1)

    推奨 = 12.5(1)、14.0(1) 以降

注：Cisco Unified Communications Manager では、Webex Desk Series デバイス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

Webex Desk Series は、次の Cisco 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、8.10.162.0
- Cisco IOS 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 = 16.12.7、17.3.5a、17.5.1、17.6.2
- 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、8.10.162.0
- Cisco Autonomous（自律）アクセス ポイント

  最小 = 15.2(4)JB6

  推奨 = 15.3(3)JPL
- Cisco Meraki アクセス ポイント

  最小 = MR 25.9、MX 13.33

  推奨 = MR 28.5、MX 16.16

アクセス ポイント

サポートされる Cisco 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。

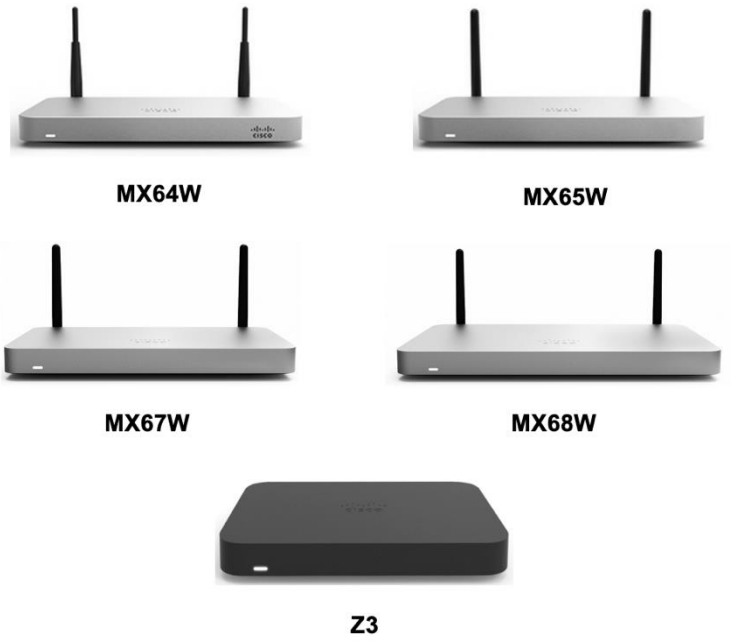
Webex Desk Series は、次の Cisco Aironet アクセス ポイント プラットフォームでサポートされています。

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
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
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

Webex Desk Series 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。



https://meraki.cisco.com/products/wireless#models [英語]

https://meraki.cisco.com/products/appliances#models [英語]

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
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
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 シリーズ屋外用アクセスポイントは、現在サポートされていません。

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、基本的な機能が必要です。

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）
- 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_jp/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、ac
- Wi-Fi マルチメディア（WMM）
- Session Initiation Protocol（SIP）
- Real Time Protocol（RTP）
    - AAC-LD、Opus、G.722、G.711、G.722.1、G.729
    - H.264、H.263
- Dynamic Host Configuration Protocol（DHCP）
- Trivial File Transfer Protocol（TFTP）
- Hypertext Transfer Protocol（HTTP）

Wi-Fi

次の表は、Webex Desk Series で使用される 802.11 モードごとの各データレートの最大 tx 電力と受信感度の情報を示しています。

Webex Desk Pro

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 = 20 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 = 19 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 = 18 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 = 19 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 = 18 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 = 18 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 = 19 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 = 19 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

Webex Desk Limited Edition

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 = 20 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 = 19 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 = 18 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 = 19 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 = 18 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 = 18 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 = 19 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 = 19 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

Webex Desk

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 = 19 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 = 19 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 = 18 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 = 19 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 = 18 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 = 22 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 = 21 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 = 20 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

Webex Desk Mini

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 = 19 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 = 19 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 = 18 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 = 19 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 = 18 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 = 22 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 = 21 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 = 20 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

Webex Desk Hub

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 = 20 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 = 20 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 = 19 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 = 20 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 = 19 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 = 19 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
5 GHz - 802.11ac (VHT160)	**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）	65 Mbps（MCS 0）	1	OFDM - BPSK
	130 Mbps（MCS 1）	1	OFDM - QPSK
	195 Mbps（MCS 2）	1	OFDM - QPSK
	260 Mbps（MCS 3）	1	OFDM - 16 QAM
	390 Mbps（MCS 4）	1	OFDM - 16 QAM
	520 Mbps（MCS 5）	1	OFDM - 64 QAM
	585 Mbps（MCS 6）	1	OFDM - 64 QAM
	650 Mbps（MCS 7）	1	OFDM - 64 QAM
	780 Mbps（MCS 8）	1	OFDM - 256 QAM
	867 Mbps（MCS 9）	1	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 = 25 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 = 20 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 = 20 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：受信感度は、特定のデータレートでパケットをデコードするのに最低限必要な信号強度です。

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

802.11n/ac 接続を実現するには、Webex Desk Series 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ドバタイズされるチャネルと送信電力の使用に対してクライアントを適合させることができます。

Webex Desk Series 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。

Webex Desk Series は、まず DFS チャンネルをパッシブスキャンしてから、それらのチャンネルのアクティブスキャンを実行します。

802.11d が有効になっていない場合、Webex Desk Series 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。

Webex Desk Series のサポート対象となる国とその 802.11d コードは次のとおりです。

オーストラリア(AU)
オーストリア(AT)
バーレーン(BH)
ベルギー(BE)
ブラジル(BR)
ブルガリア(BG)
カナダ(CA)
チリ(CL)
中国(CN)
コロンビア（CO）
コスタリカ（CR）
クロアチア（HR）
キプロス（CY）
チェコ共和国（CZ）
デンマーク（DK）
ドミニカ共和国（DO）
エクアドル（EC）
エジプト（EG）
ハンガリー(HU)
アイスランド(IS)
インド(IN)
アイルランド(IE)
イスラエル(IL)
イタリア（IT）
日本（JP）
韓国（KR）
ラトビア(LV)
リヒテンシュタイン(LI)
リトアニア(LT)
ルクセンブルク(LU)
マケドニア（MK）
マレーシア（MY）
マルタ（MT）
メキシコ（MX）
モナコ（MC）
モンテネグロ（ME）
フィリピン(PH)
ポーランド(PL)
ポルトガル(PT)
プエルトリコ(PR)
ルーマニア(RO)
ロシア連邦(RU)
サウジアラビア(SA)
セルビア(RS)
シンガポール（SG）
スロバキア（SK）
スロベニア（SI）
南アフリカ（ZA）
スペイン（ES）
スウェーデン（SE）
スイス（CH）
台湾（TW）
タイ（TH）
トルコ（TR）

エストニア（EE）
フィンランド（FI）
フランス（FR）
ドイツ（DE）
ジブラルタル（GI）
ギリシャ（GR）
香港(HK)
オランダ（NL）
ニュージーランド（NZ）
ナイジェリア（NG）
ノルウェー（NO）
パナマ(PA)
パラグアイ（PY）
ペルー(PE)
ウクライナ（UA）
アラブ首長国連邦（AE）
イギリス（GB）
アメリカ合衆国（US）
ウルグアイ（UY）
ベトナム（VN）

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/pdtcnc

Bluetooth

Webex Desk Series は Bluetooth テクノロジーをサポートしており、ワイヤレスヘッドセット通信が可能です。

Bluetooth では、30 フィートの範囲内であれば低帯域幅のワイヤレス接続が可能ですが、Bluetooth デバイスは常に Webex Desk Series から 10 フィート以内で使用することが推奨されます。

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

Webex Desk Series 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）
- オーディオ / ビデオリモート制御プロファイル（AVRCP）
- 汎用アクセスプロファイル（GAP）
- 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）

共存（802.11b/g/n + Bluetooth）モード

802.11b/g/n と Bluetooth が同時に使用される共存モードを利用する場合、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）モードを使用する場合、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 ツー 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

Webex Desk Series は、次の言語をサポートしています。

アラビア語	フランス語	ポーランド語
カタロニア語	ドイツ語	ポルトガル語
中国語	ヘブライ語	ロシア語
チェコ語	ハンガリー語	スペイン語
デンマーク語	イタリア語	スウェーデン語
オランダ語	日本語	トルコ語
英語	韓国語	
フィンランド語	ノルウェー語	

ビデオ コール

Webex Desk Series は、高解像度マルチタッチカラー LCD と内蔵カメラによるビデオコールをサポートしています。

Webex Desk Series は、他の Webex Desk Series エンドポイント、Cisco TelePresence Systems、および他のビデオ対応エンドポイントとのビデオ通話を確立できます。

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

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

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

次のビデオ形式がサポートされます：

- QnHD 180p（320 x 180）
- CIF 288p（512×288）
- nHD 360p（640 X 360）
- SD 448p（768×448）
- WSVGA 576p（1024 x 576）
- HD 720p（1280 X 720）
- HD 1080p（1920 X 1080）

デバイスの手入れ

Webex Desk Series をクリーニングするには、柔らかく湿った布を使用してデバイスを拭きます。

デバイスを損傷する可能性があるため、液体や粉末をデバイスに直接塗布しないでください。

デバイスの清掃に漂白剤などの腐食作用のある製品を使用しないでください。

デバイスを損傷する可能性があるため、デバイスのクリーニングに圧縮空気を使用しないでください。

詳細については、次の URL にある『Webex Desk Series ユーザーガイド』を参照してください。

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

無線 LAN の設計

Webex Desk Series 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

次のガイドラインを使用して、各ワイヤレス環境でのチャネル使用を計画します。

5 GHz（802.11a/n/ac）

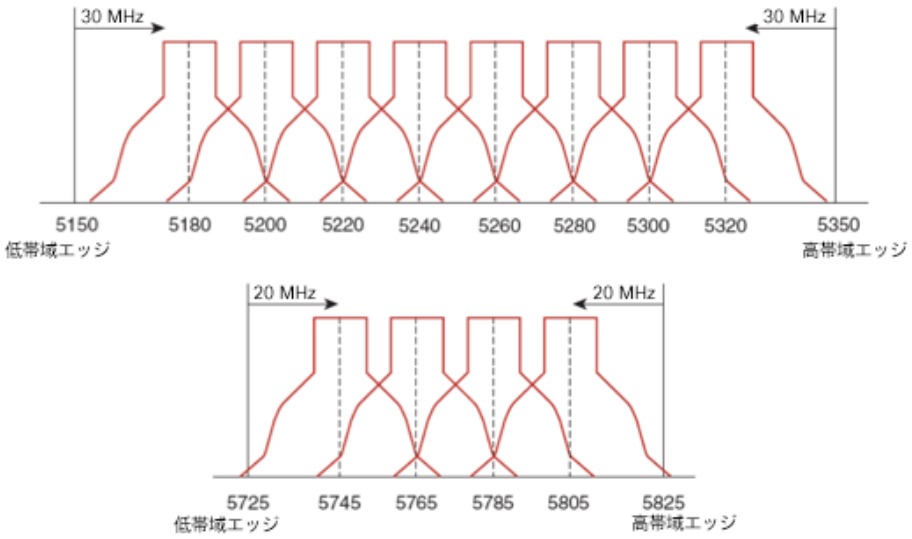
5 GHz は、Webex Desk Series の運用に使用するように推奨されている周波数帯域です。

通常は、アクセス ポイントに手動でチャ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 ポイントにチャネルを静的に割り当てる必要があります。

Webex Desk Series は、802.11h の動的周波数選択（DFS）と Transmit Power Control（TPC）をサポートしています。これらは、5.260 ~ 5.720 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 Webex Desk Series を展開する場合は、隣接チャンネルと 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、Webex Desk Series 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 台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。



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

Dynamic Frequency Selection（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。

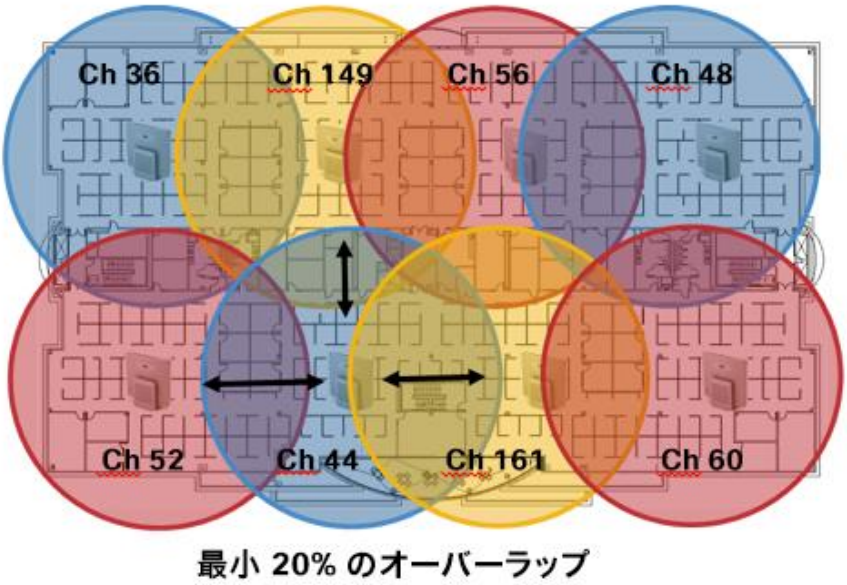
アクセス ポイントでレーダー イベントが繰り返し検出される場合（誤検出も含む）、レーダー信号が単一チャネル（ナローバンド）または複数のチャネル（ワイドバンド）に影響を与えているかどうかを特定し、ワイヤレス LAN における該当チャネルの使用を無効にします。

非 DFS チャネルにアクセス 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 チャネル（UNII-1）を使用するアクセス ポイントをエリアごとに少なくとも 1 つ設置します。これにより、新しい使用可能チャネルのスキャン中にアクセス ポイントの無線がホールドオフ期間になっているときもチャネルを使用できます。

UNII-3 チャネル（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 チャネル、欧州では 16 チャネル、日本では 19 チャネルを使用できます。

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

UNII-2 拡張チャネル（チャネル 100 ~ 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（チャネル 52 ~ 64）を無効にして、有効になるチャネルの数が多くなり過ぎないようにすることが推奨されます。

ワイヤレス LAN で多数の 5 GHz チャネルを有効にすると、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。

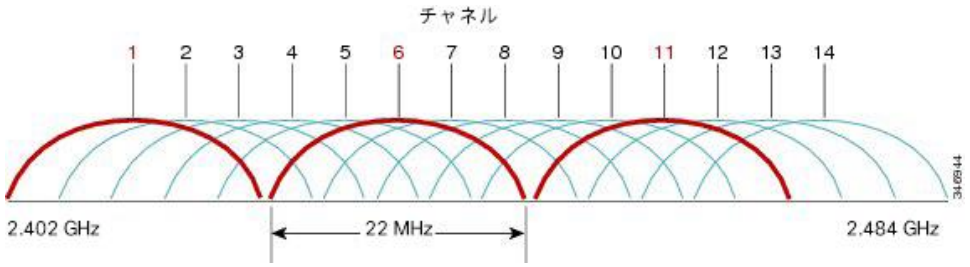
断続的な干渉源が存在する場合は、そのエリアにサービスを提供しているアクセス ポイントにチャネルを静的に割り当てる必要があります。

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ネルだけを利用する必要があります。オーバーラップのないチャネルには 22 MHz の間隔があり、少なくとも 5 チャネル離れています。

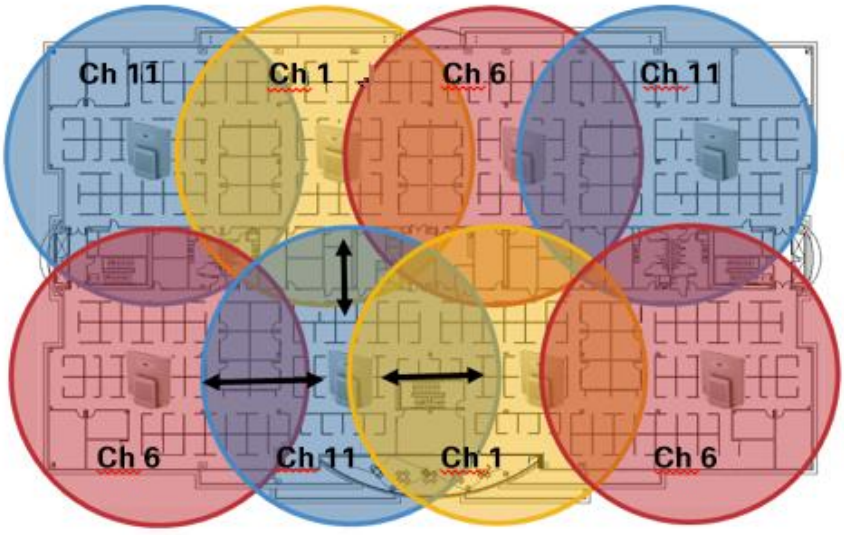
2.4 GHz 周波数範囲には、オーバーラップのないチャネルは 3 つしか存在しません（チャネル 1、6、11）。

802.11b/g/n 環境に Webex Desk Series を展開する場合は、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。



最小 20% のオーバーラップ

信号強度とカバレッジ

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

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

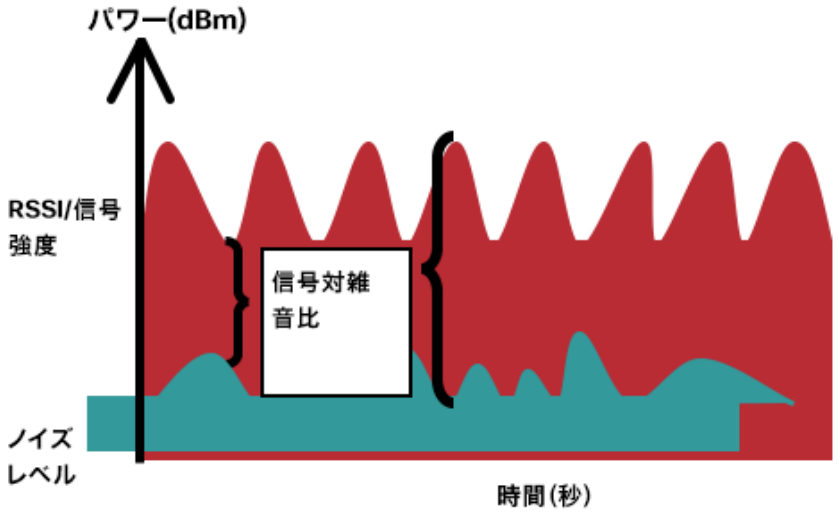
少なくとも 25 dB の信号対雑音比（SNR）、つまり -67 dBm の信号に対して -92 dBm のノイズ レベルを維持する必要があります。

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。

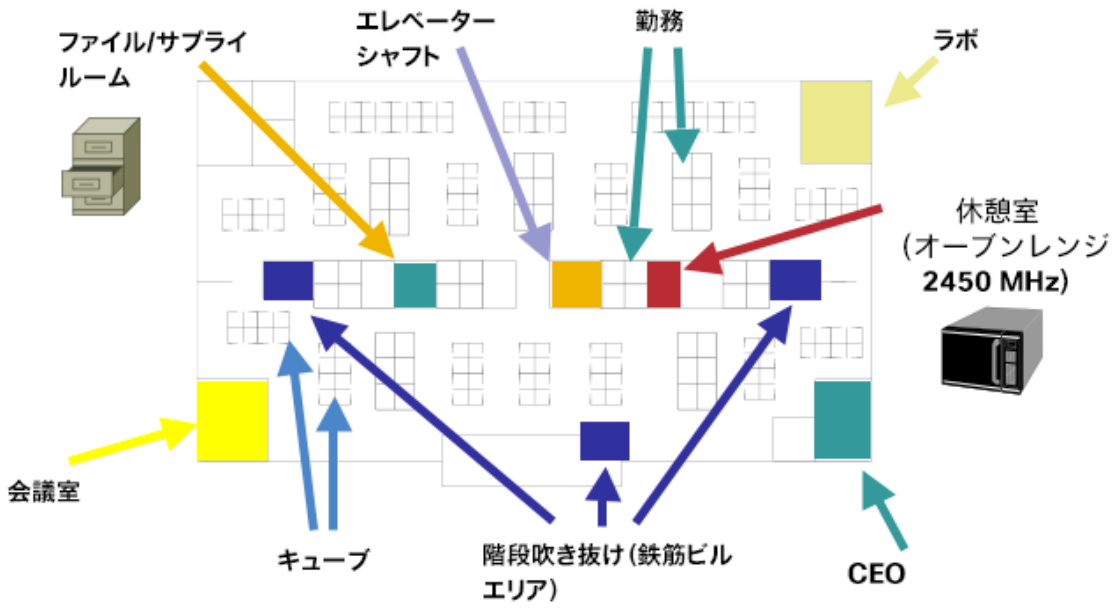
データ専用アプリケーションのための一般的なワイヤレス LAN 導入では、エレベータ、階段、屋外通路といった、VoWLAN サービスで必要とされる一部のエリアにはカバレッジが提供されません。

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、チャネル 11 に悪影響を及ぼす可能性があります。さらに一部の電子レンジは、周波数範囲全体（チャネル 1 ~ 11）に影響します。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。

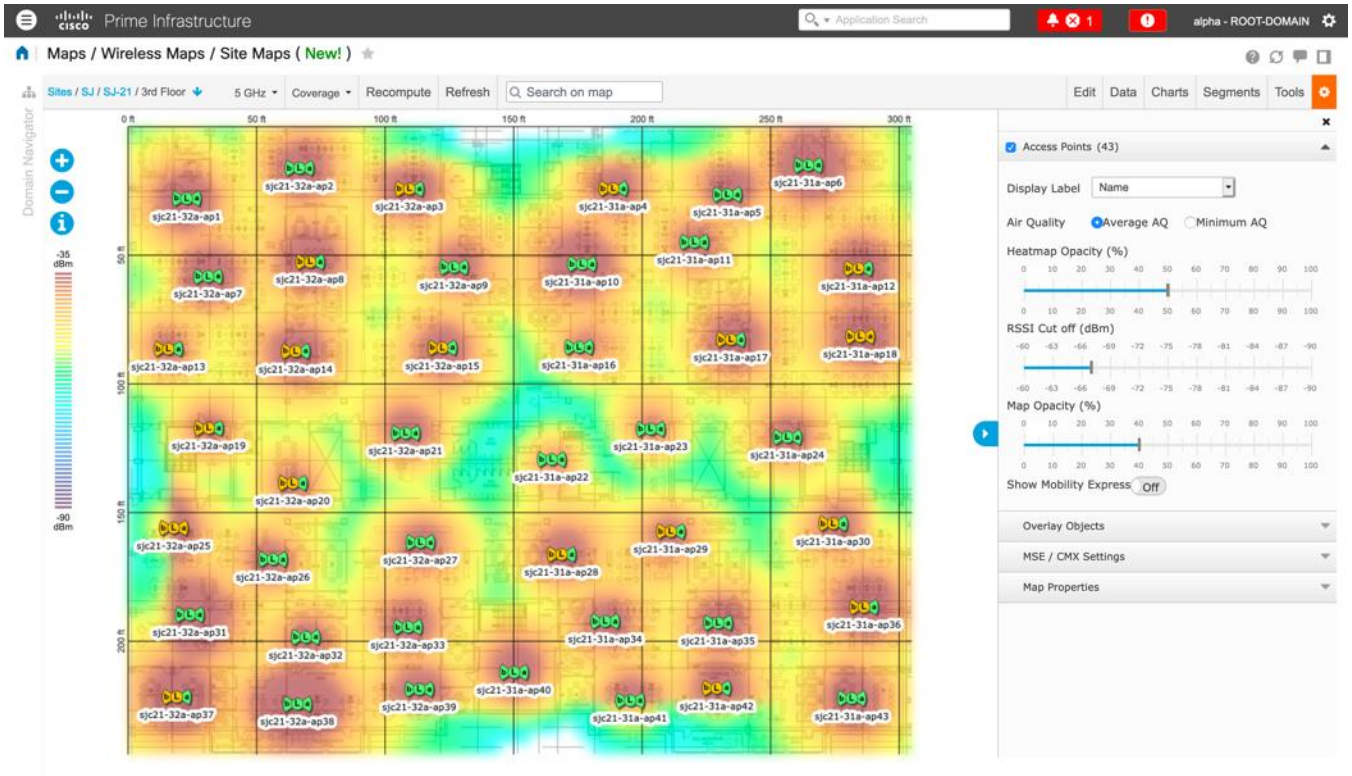
ただし、免許申請の必要のない 5 GHz 周波数を利用する製品も存在します（たとえば、5.8 GHz コードレス電話機も、UNII-3 チャネルに悪影響を及ぼす可能性があります）。



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。

Webex Desk Series には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、Webex Desk Series は最大 VHT80 MCS 9 2SS（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	サポートされる データ レート	無効な 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、	6、9 Mbps

		(VHT MCS 0 - MCS 9 3SS) 、(VHT MCS 0 - MCS 9 4SS)	
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

Webex Desk Series を条件の厳しい環境（製造、倉庫、小売業など）に展開する場合、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
Webex Desk Series 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 チャネル セットでは、8 または 12 チャネル計画のみを使用することを推奨します。可能な場合は、UNII-2 拡張チャネルを無効にします。

データ レート
マルチパスが高いレベルにある場合は、標準の推奨データ レート セットが適切に機能しない可能性があります。
そのため、低いデータ レート（6 Mbps など）を有効にしてこのような環境での運用を改善させることを推奨します。
音声専用に使用する場合は、24 Mbps を超えるデータ レートを無効にして最初の伝送成功率を上げることができます。同じ帯域をデータ、ビデオ、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 Webex Desk Series 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）。
Webex Desk Series 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、ビデオ、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

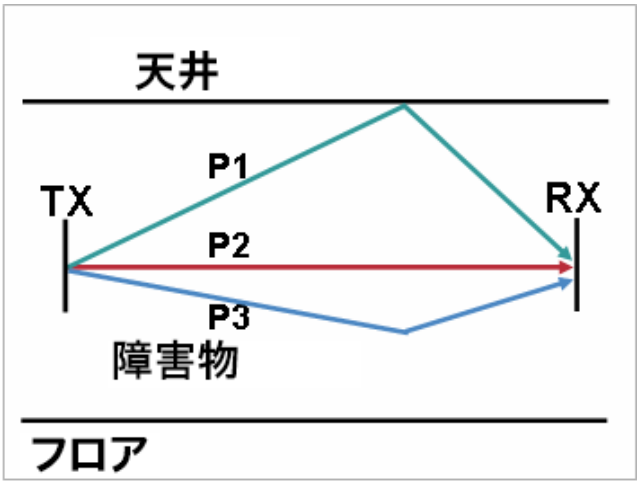
反射した波長が、メイン信号とちょうど位相がずれて到達し、メイン信号を完全に打ち消すような場合に発生します。

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て信号強度を増大させる場合に発生します。

信号振幅の減少

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



802.11a/n/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。

Webex Desk Series 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 および WPA（802.1x 認証）
- WPA2-PSK および WPA-PSK（事前共有キー）
- EAP-FAST（Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling）
- 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）
- なし

WLAN 暗号化

- AES（Advanced Encryption Standard）
- TKIP/MIC（Temporal Key Integrity Protocol/Message Integrity Check）

注：TKIP はブロードキャスト/マルチキャスト暗号としてしか使用できないため、アクセスポイントは AES（CCMP128）をサポートしている必要があります。

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。

Webex Desk Series 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
- 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 - Flexible Authentication via Secure Tunneling（EAP-FAST）

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

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

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

現在、Webex Desk Series では、PAC の自動プロビジョニングのみがサポートされています。そのため、RADIUS サーバー上で **[匿名インバンド PAC プロビジョニングを許可する（Allow anonymous in-band PAC provisioning）]** を有効にしてください。

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

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

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

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

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

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

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

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

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

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

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

証明書をインストールする必要があります。

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

EAP-TLS では、Webex Desk Series 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 では、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あります。

認証サーバーは、Webex Desk Series に証明書をインポートして検証されます。

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-NONE、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、Webex Desk Series に証明書をインポートして検証されます。

サービス品質（QoS）

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

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

- アクセスポイント上で **WMM** が有効になっていることを確認します。
- アクセスポイント上で音声、インタラクティブビデオ、呼制御トラフィックに優先順位を与える QoS ポリシーを作成します。

トラフィックのタイプ	DSCP	802.1p	WMM UP	ポート範囲
音声	EF（46）	5	6	UDP 16384 ~ 32767
TelePresence コール（音声とビデオ）	CS4（32）	4	5	UDP 16384 ~ 32767
コール制御	CS3（24）	3	4	TCP/UDP 5060 – 5061 または HTTPS 443

- 音声、インタラクティブビデオ、および呼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。

コール アドミッション制御（CAC）

Webex Desk Series は、現在、音声ストリームまたはビデオストリームのコール アドミッション コントロールをサポートしていません。

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

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 Deployment Guide（Cisco Meraki MS スイッチ 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]

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

Webex Desk Series は、両方の周波数セットを有効にします。これにより、Webex Desk Series は 5 GHz または 2.4 GHz 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（FT）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。WPA と WPA2 では、一時的なキーが追加されるため、ローミング時間が長くなる可能性があります。

802.11r（FT）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。

Webex Desk Series は現在、802.11r（FT）をサポートしていません。

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

Webex Desk Series 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。

帯域間のローミング

Webex Desk Series は両方の周波数セットを有効にし、インターバンドローミングを可能にし、現在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。

電源投入時に、Webex Desk Series は、2.4 GHz と 5 GHz のすべてのチャンネルをスキャンし、利用可能な場合は、設定されたネットワークのアクセスポイントへの関連付けを試行します。

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

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

イーサネットが Webex Desk Series に接続されたときにワイヤレス LAN が一時的に無効になりますが、ワイヤレス LAN が以前に有効化されていた場合はイーサネットが切断された時点で自動的に有効に復帰します。

Webex Desk Series は、主として、アイドル状態または着信時に、アクティブモード（Wi-Fi 節電なし）を使用します。

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

Delivery Traffic Indicator Message（DTIM）

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

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

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

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

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。

Cisco Access Point は、24 Mbps 以上のデータレートで 802.11a/n/ac と 802.11g/n の両方に対して最大 27 個の双方向音声ストリームをサポートします。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、チャネルの初期使用率、および環境によって異なります。

オーディオのみのコール

次に、アクセス ポイント/チャネルごとにサポートされるオーディオのみのコール（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

ビデオ コール

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

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

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

最大数ビデオコール	802.11 モード	オーディオ コーデック	オーディオ ビット レート	ビデオタイプ	ビデオ解像度	ビデオ ビット レート
2-11+	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	HD 720p	1,280 X 720	1000 kbps
1-7+	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	FHD 1080p	1920 X 1080	2500 Kbps

注：現在、コール アドミッション コントロールはサポートされていません。

マルチキャスト

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

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。

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

マルチキャストでは、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。

Webex Desk Series 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すことができます。

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

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

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）]** と **[CCKM]** が必須として構成されていないことを確認します
- **[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]** が **[無効（Disabled）]** になっていることを確認します
- **[802.11v]** が **[無効（Disabled）]** になっていることを確認します
- **[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
- [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
- **[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
- **[プラチナ（Platinum）]** QoS プロファイルで、**[802.1p タグ（802.1p Tag）]**を **[5]** に設定します

802.11 ネットワークの設定

Webex Desk Series 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。

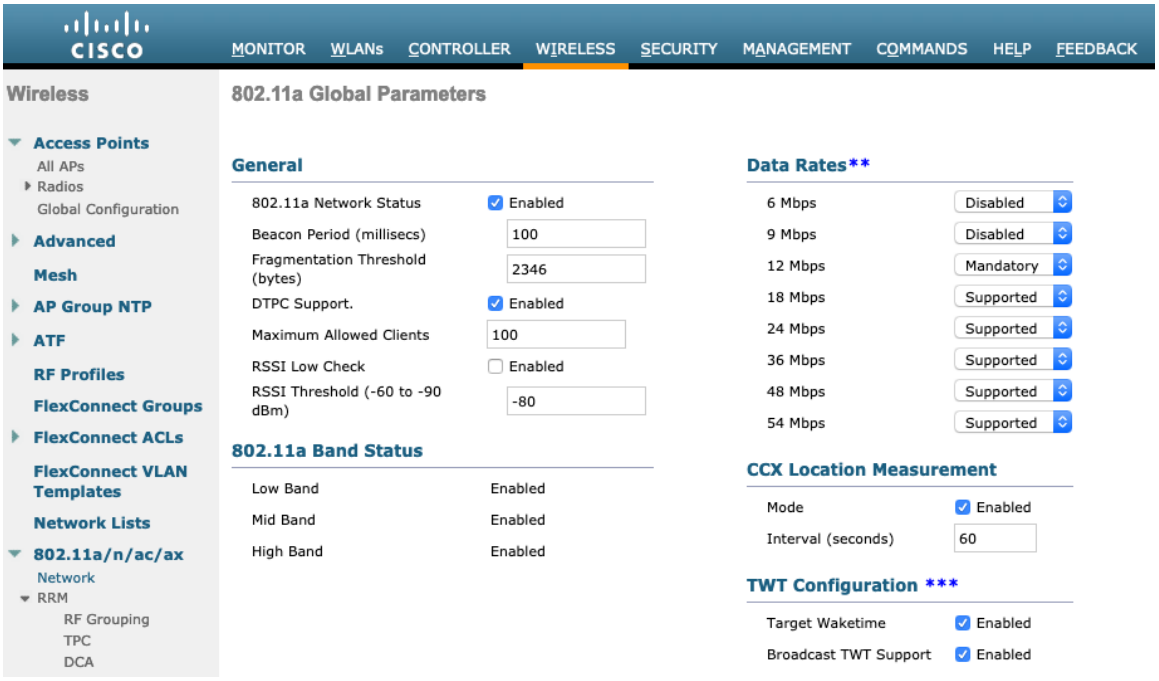
5 GHz を使用する場合は、802.11a/n/ac ネットワークのステータスが **[有効（Enabled）]** に設定されていることを確認します。

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

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。



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。

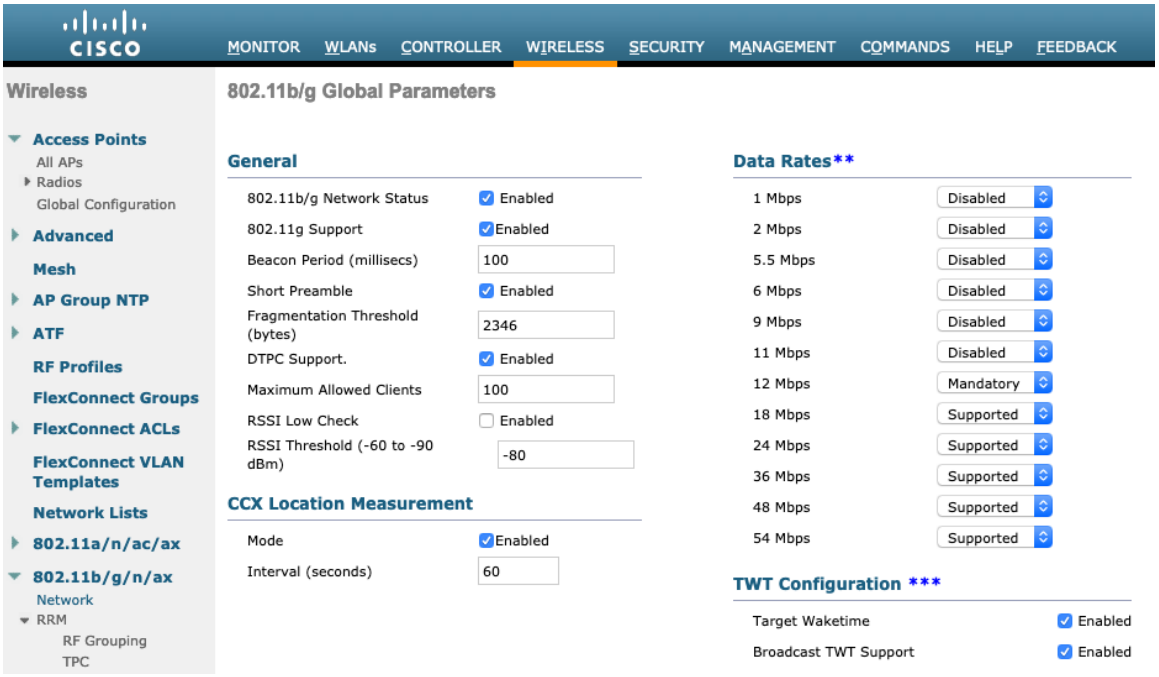
ロングプリアンブルを必要とするレガシークライアントがワイヤレス LAN に存在しない場合は、アクセスポイントの 2.4 GHz 無線設定で [ショートプリアンブル（Short Preamble）] **を [有効（Enabled）] に設定する必要があります。**ロング プリアンブルの代わりにショート プリアンブルを使用することによって、ワイヤレス ネットワークのパフォーマンスが向上します。

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。



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。

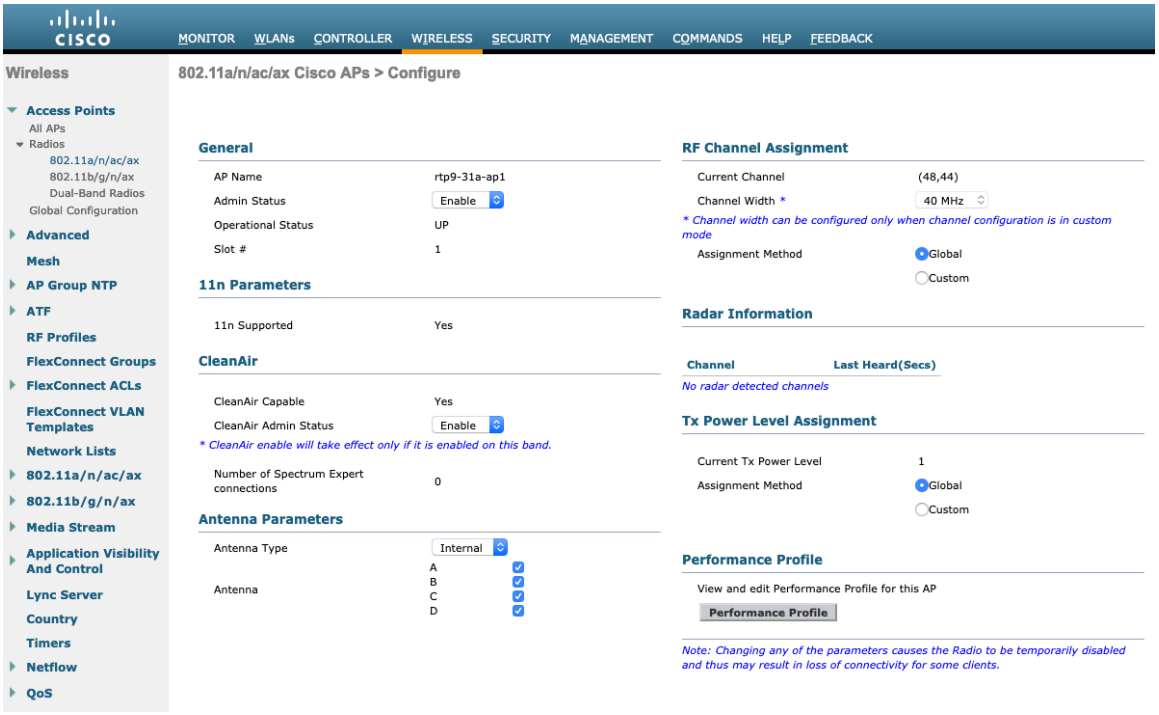
次のコマンドを使用して、すべてのアクセスポイントにグローバルに、または個別アクセスポイントからの無線ビームフォーミング機能を有効にします。

```
(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
```

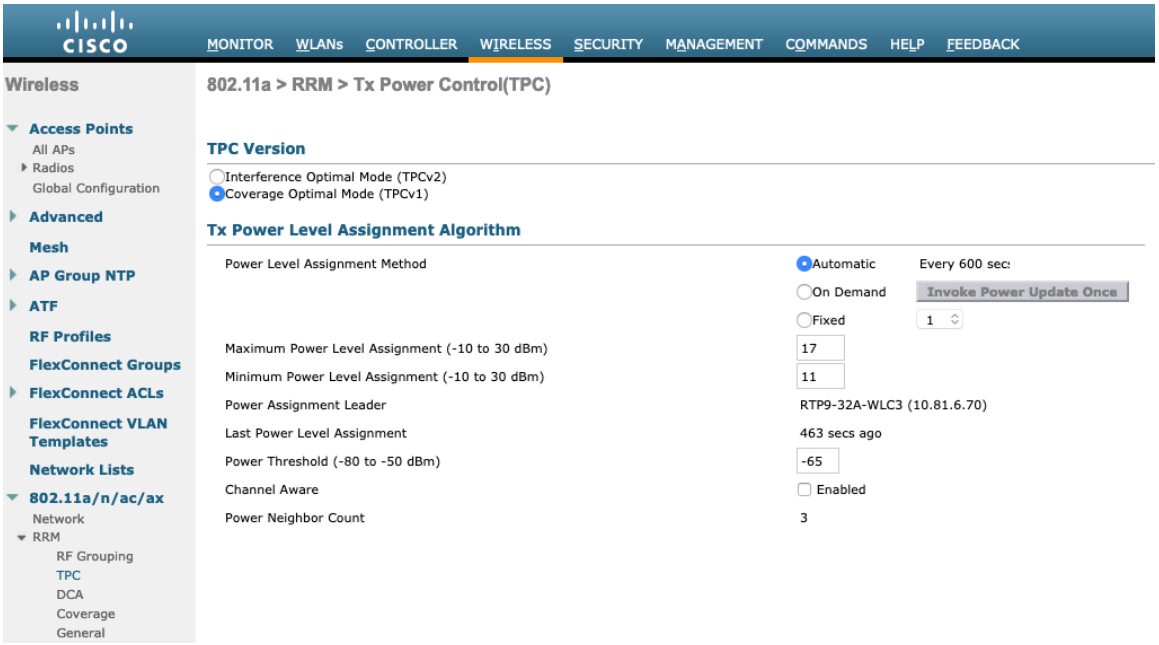


Auto RF（RRM）

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。

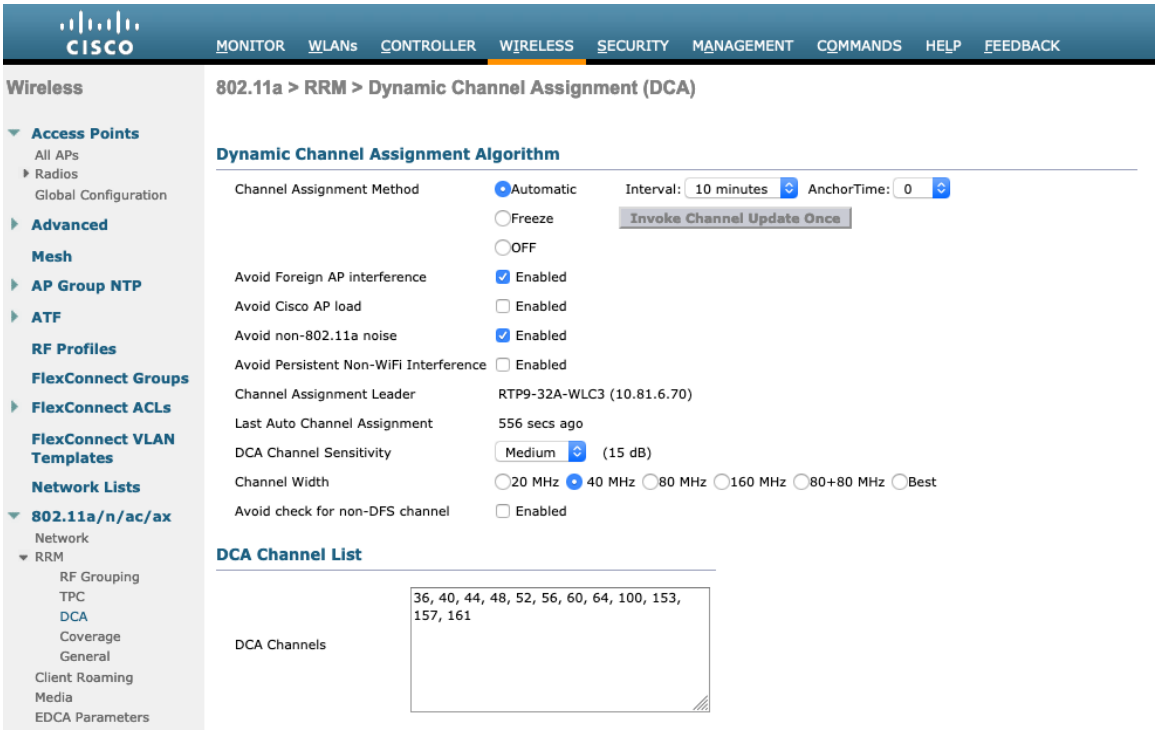
自動電力レベルの割り当てを使用する場合は、電力の最大レベルと最小レベルを指定できます。



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）。

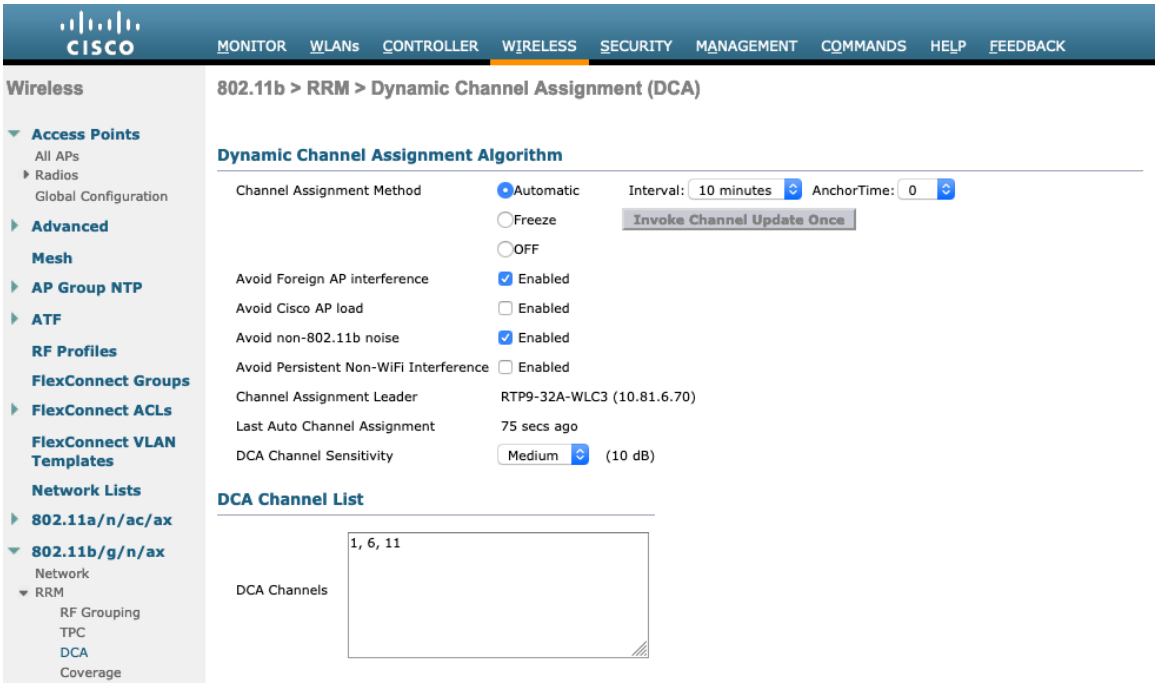
5 GHz チャネル幅は、Cisco 802.11n アクセスポイントを使用する場合は 20 MHz または 40 MHz、Cisco 802.11ac アクセスポイントを使用する場合は 20 MHz、40 MHz、または 80 MHz に設定できます。

すべてのアクセス ポイントで同じチャ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 リストではチャネル 1、6、および 11 だけを有効にします。

2.4 GHz 帯域で使用可能なチャネルの数が限られているために、40 MHz に対応した 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 チャネルを設定することを推奨します。



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。

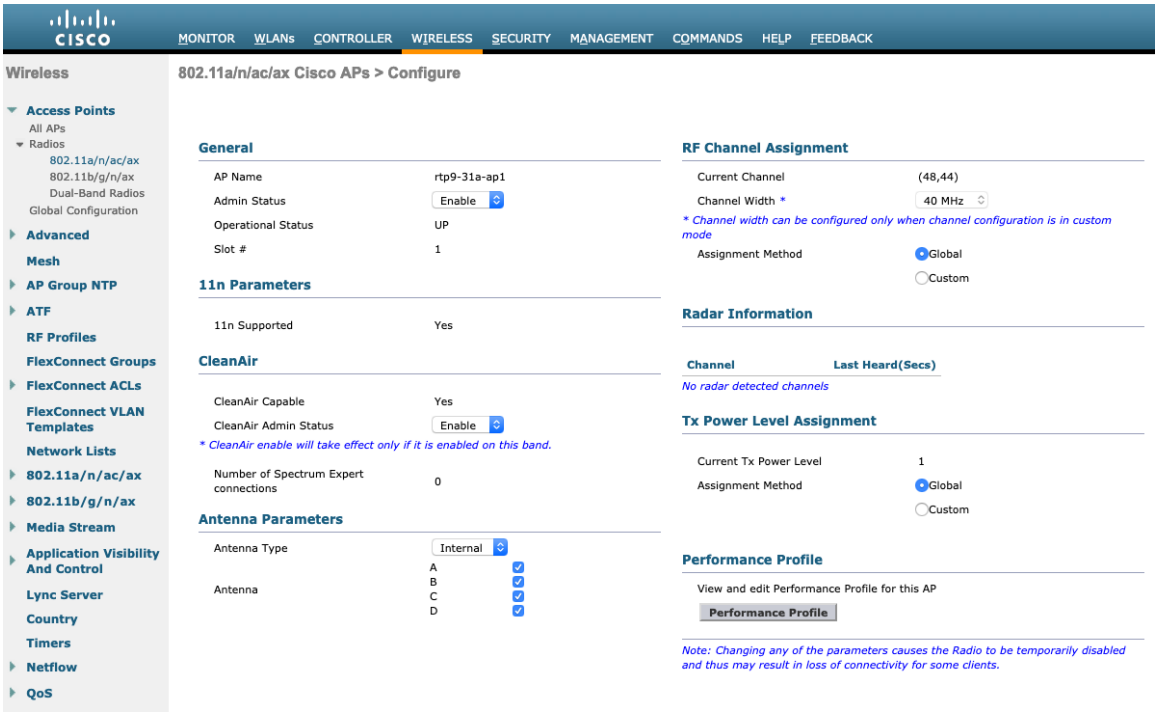
その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

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ネル幅を使用することを推奨します。



クライアントのローミング

Webex Desk Series は、Cisco 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。スキャニングとローミングはデバイス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。

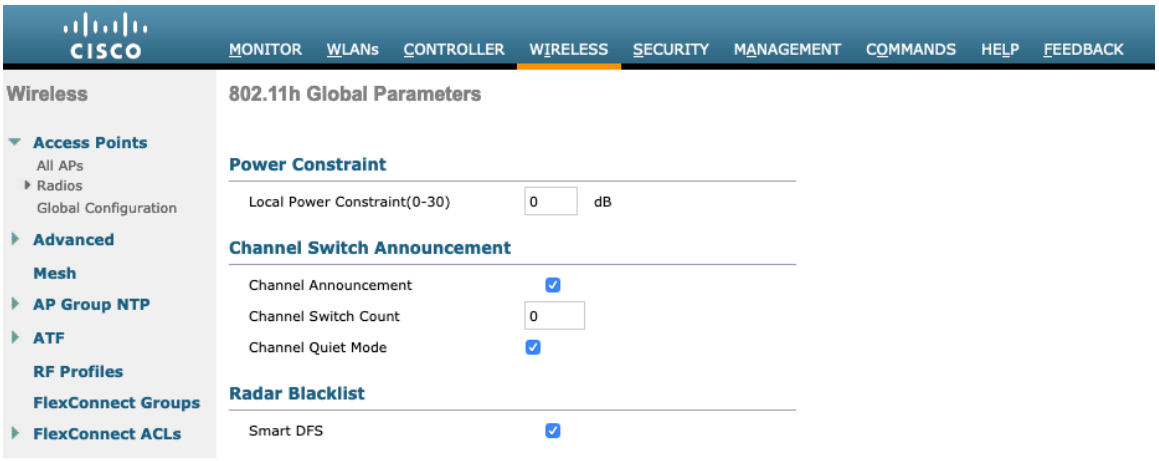
低遅延 MAC（LLM）を設定すると、アクセス ポイント プラットフォームによって 1 パケットあたりの再送信回数が 2 ~ 3 回に減るので、複数のデータ レートが有効である場合に問題が生じるおそれがあります。

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。

DFS（802.11h）

[電力制限（Power Constraint）] **は未設定のままにするか、0 dB に設定する必要があります。**

[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（Enabled）] **にする必要があります。**



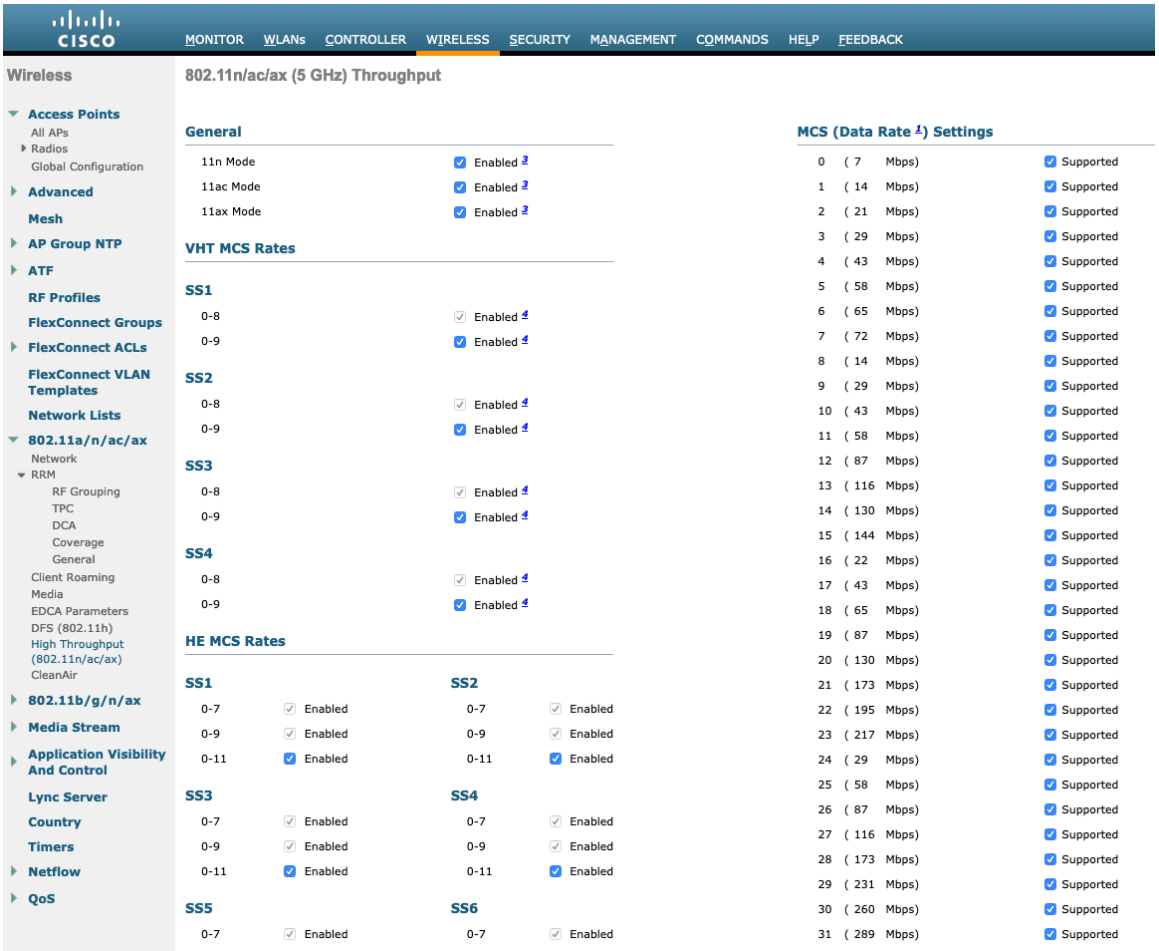
高スループット（802.11n/ac）

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。

Webex Desk Series 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。



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。

Webex Desk Series 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が必要です。

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

次のコマンドを使用して、Webex Desk Series の要件ごとに A-MPDU および A-MSDU 設定を行います。

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
```

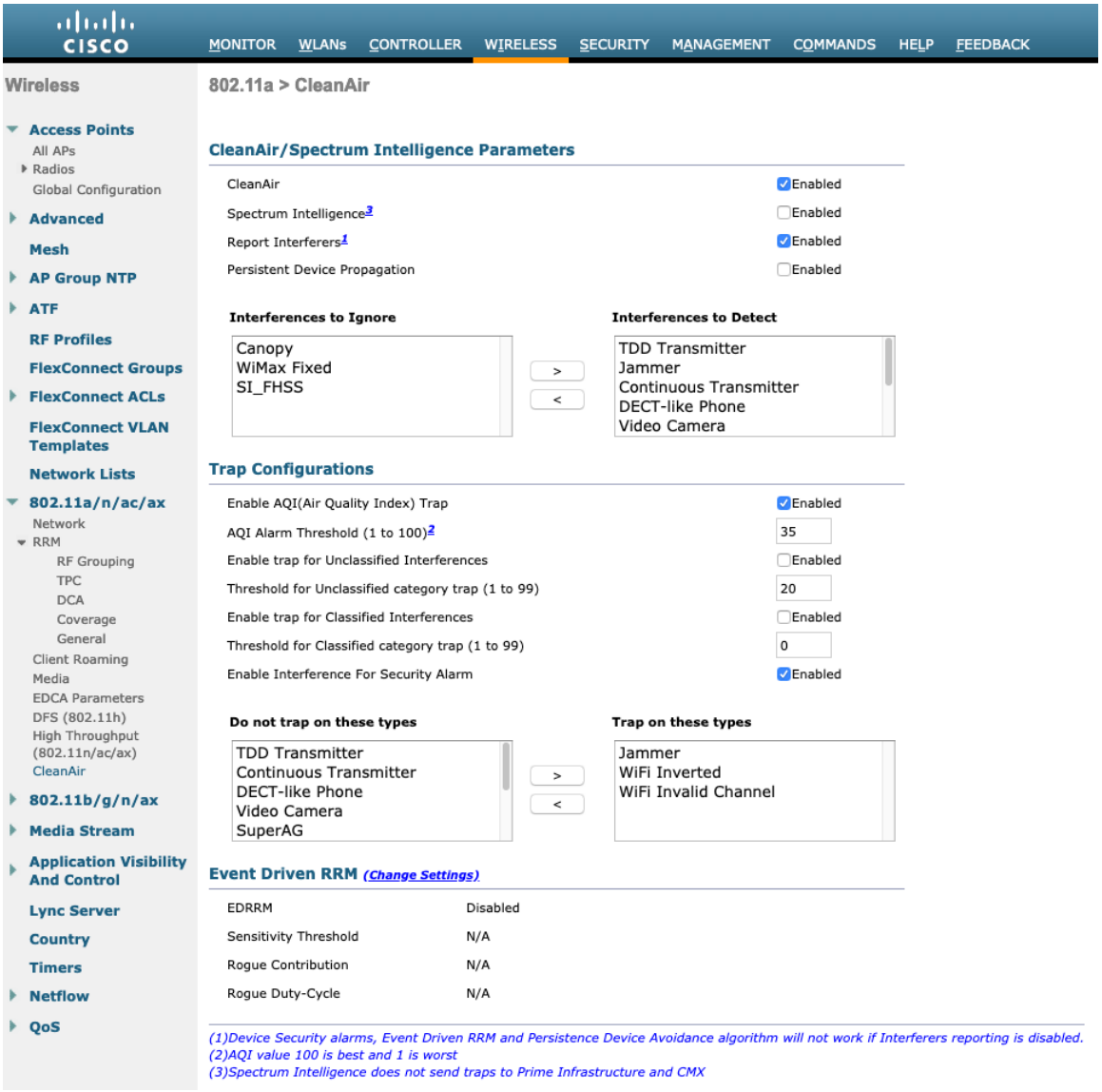
A-MPDU と A-MSDU と現在の設定を表示するには、5 GHz の場合は **show 802.11a**、2.4 GHz の場合は **show 802.11b** を入力します。

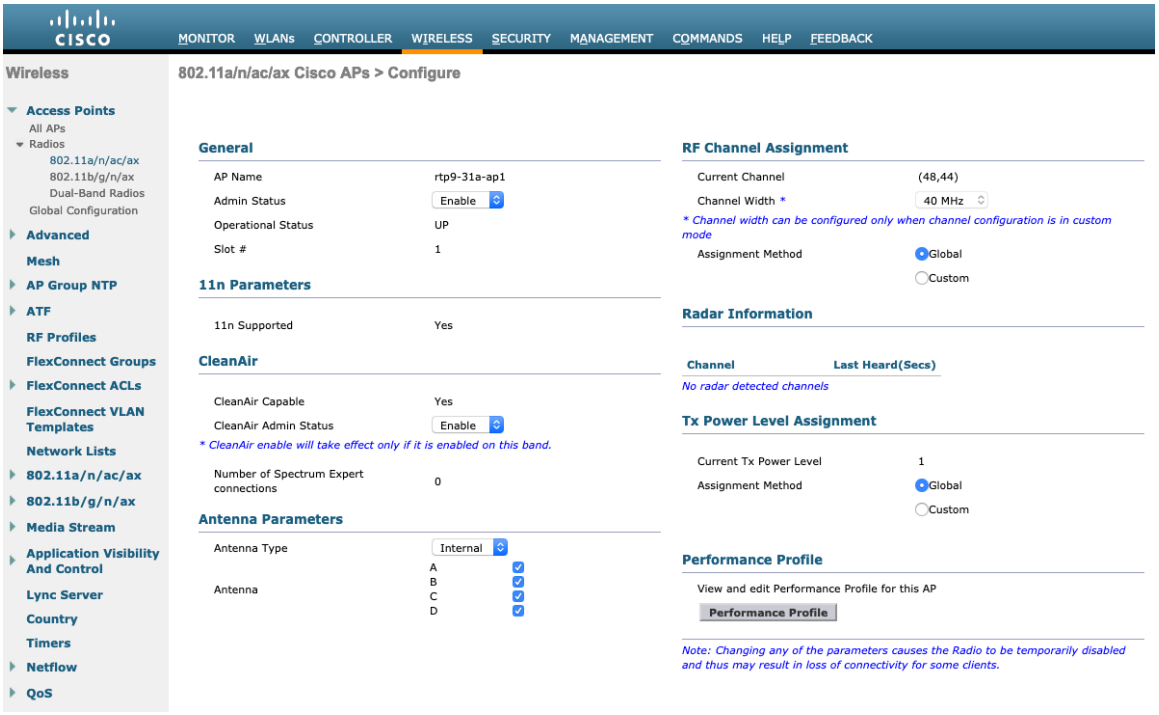
```
802.11n Status:
    A-MSDU Tx:
    Priority 0..................................... Disabled
```

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

CleanAir

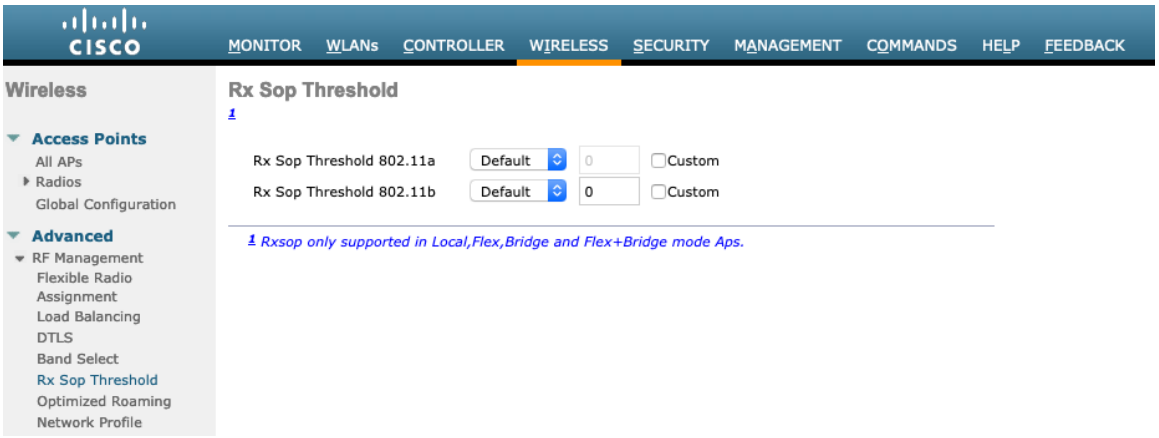
CleanAir テクノロジーを搭載したCisco 製のアクセスポイントを使用して既存の干渉を検出する場合は、**[CleanAir]** を **[有効（Enabled）]** にする必要があります。


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
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
802.11a > CleanAir
CleanAir/Spectrum Intelligence Parameters
CleanAir
Enabled
Spectrum Intelligence
Enabled
Report Interferers
Enabled
Persistent Device Propagation
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
Enabled
AQI Alarm Threshold (1 to 100)
35
Enable trap for Unclassified Interferences
Enabled
Threshold for Unclassified category trap (1 to 99)
20
Enable trap for Classified Interferences
Enabled
Threshold for Classified category trap (1 to 99)
0
Enable Interference For Security Alarm
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

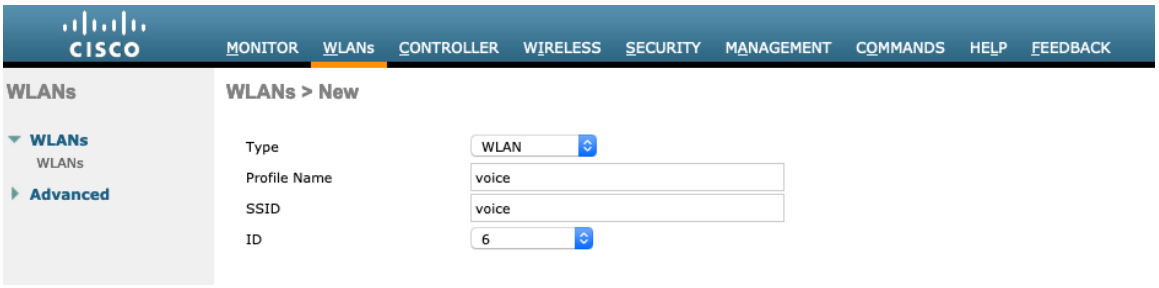
Webex Desk Series には別の SSID を使用することをお勧めします。

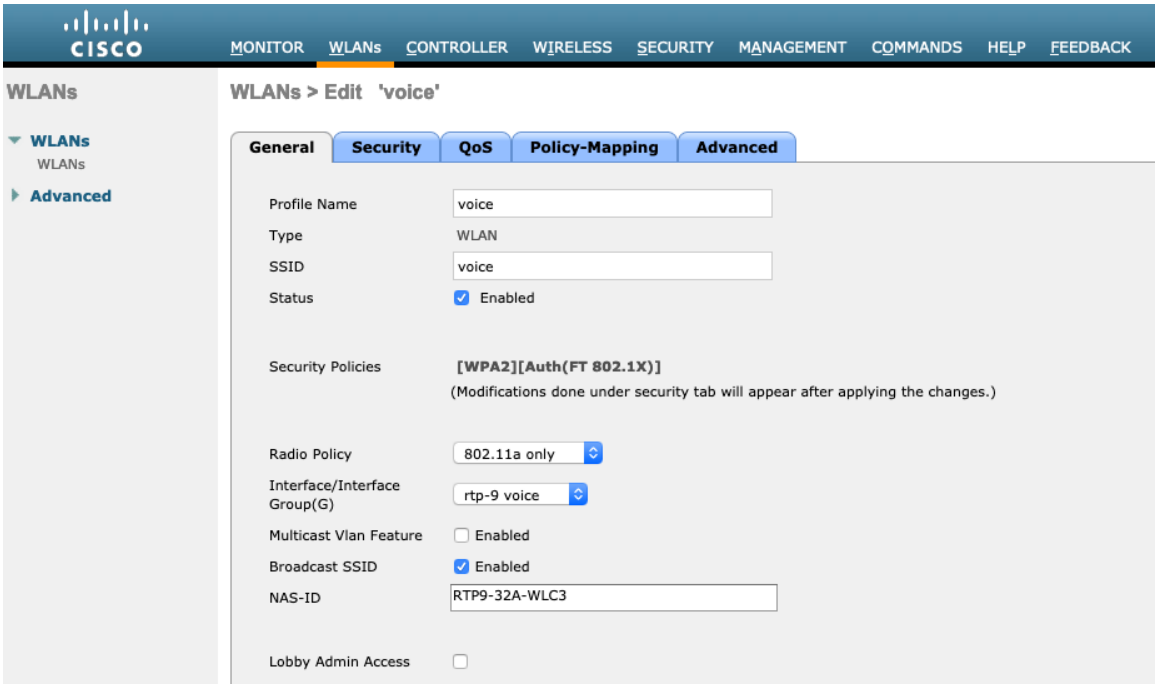
ただし、音声対応 Cisco Wireless LAN エンドポイントをサポートするように設定された既存の SSID がある場合、その WLAN を代わりに使用できます。

Webex Desk Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように設定できます（802.11a のみなど）。

Webex Desk Series 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。

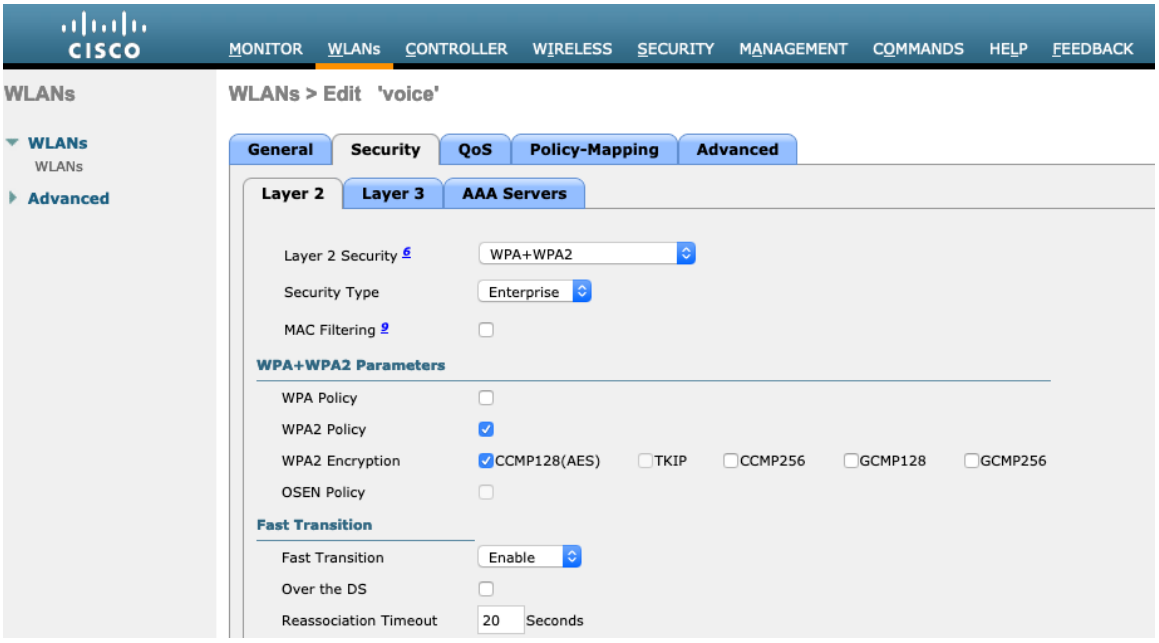
選択した SSID が他の LAN に使用されていないことを確認してください。使用されている場合で、特に異なるセキュリティ タイプを使用している場合は、電源の投入時またはローミング中に障害が発生する可能性があります。



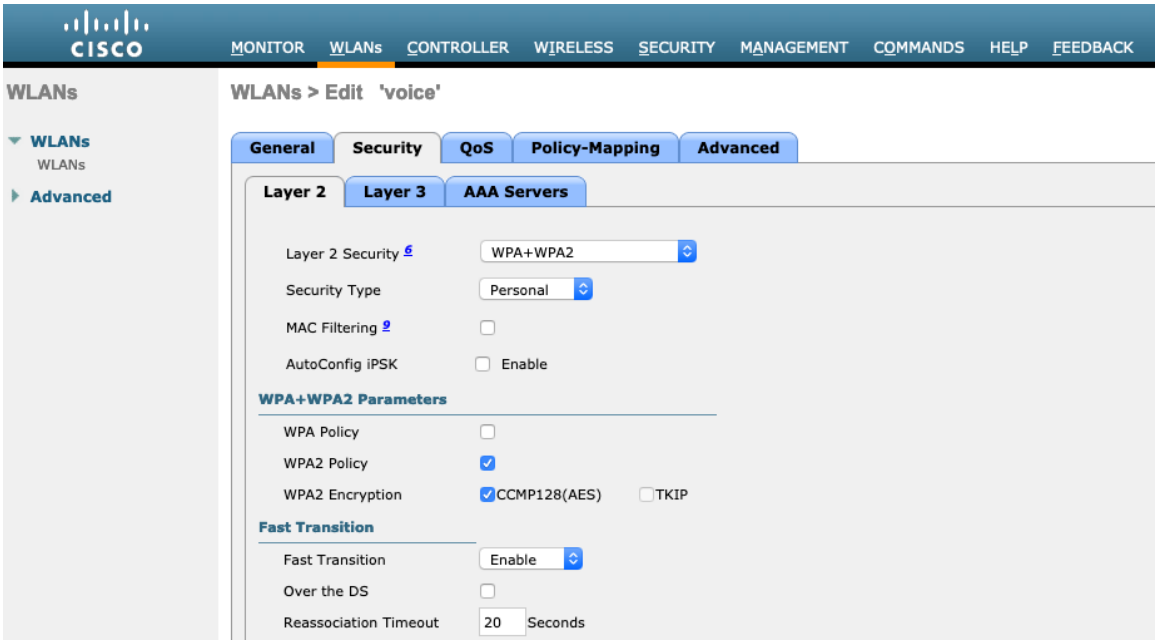


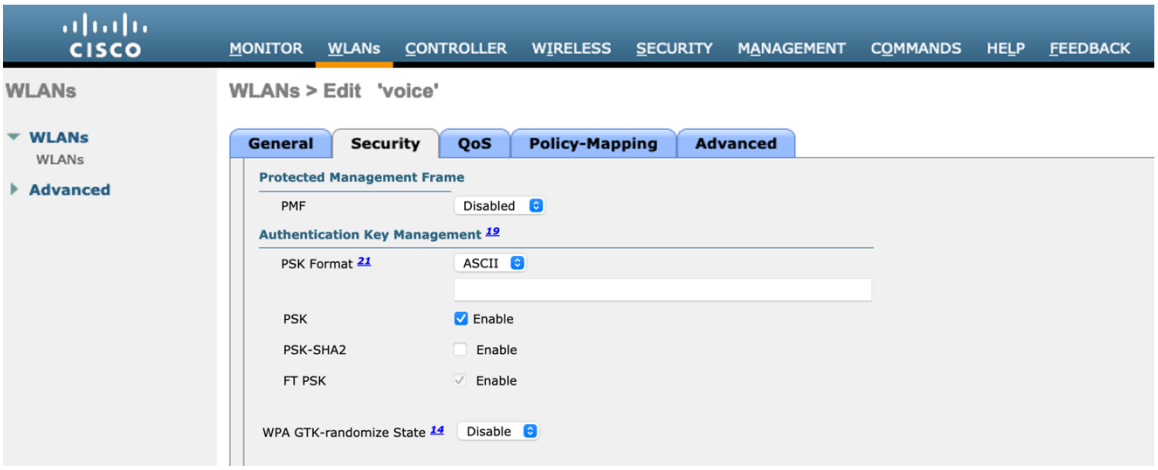
[保護された管理フレーム（PMF）（Protected Management Frame（PMF）] を **[任意（Optional）]** または **[無効（Disabled）]** に設定します。

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-SHA1 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 PSK のどちらかを有効にします。


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
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 9
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


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
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


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
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 9
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



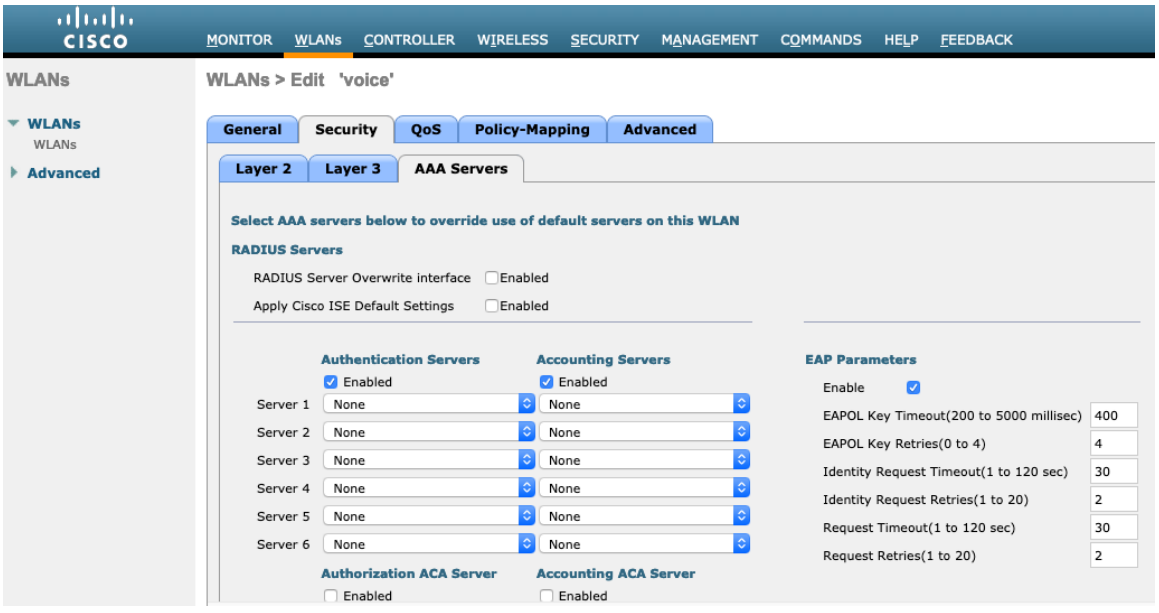
各種の音声クライアントに同じ SSID を使用する場合は、802.1x や PSK を使用するかどうかに応じて、802.11r（FT）、CCKM、PSK も有効にできます。

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、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。

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。

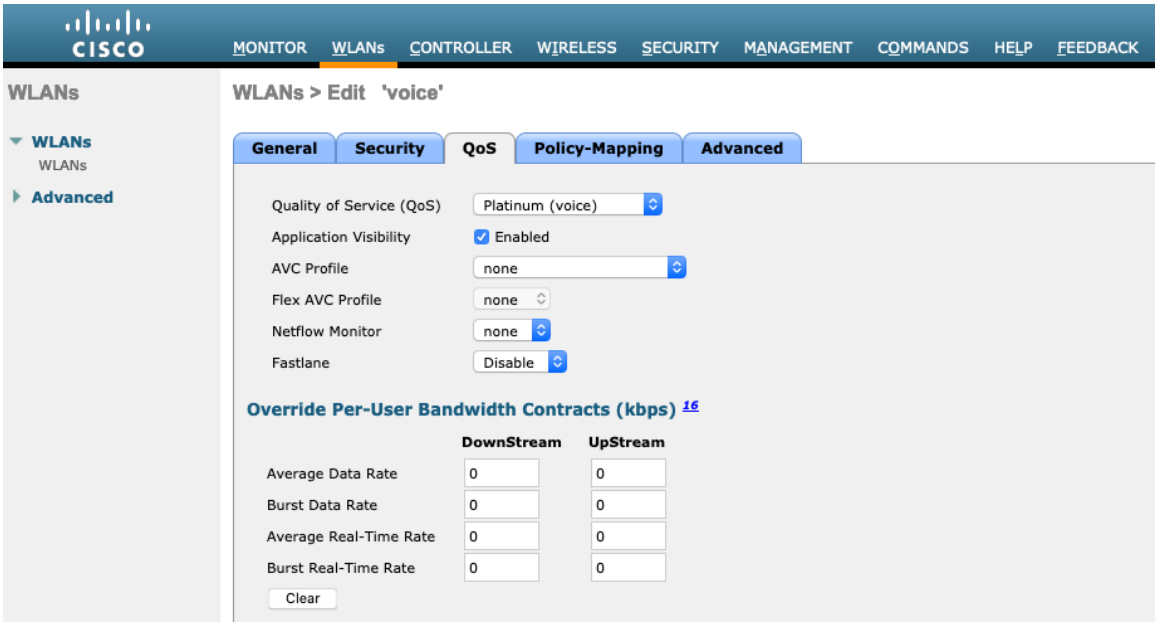


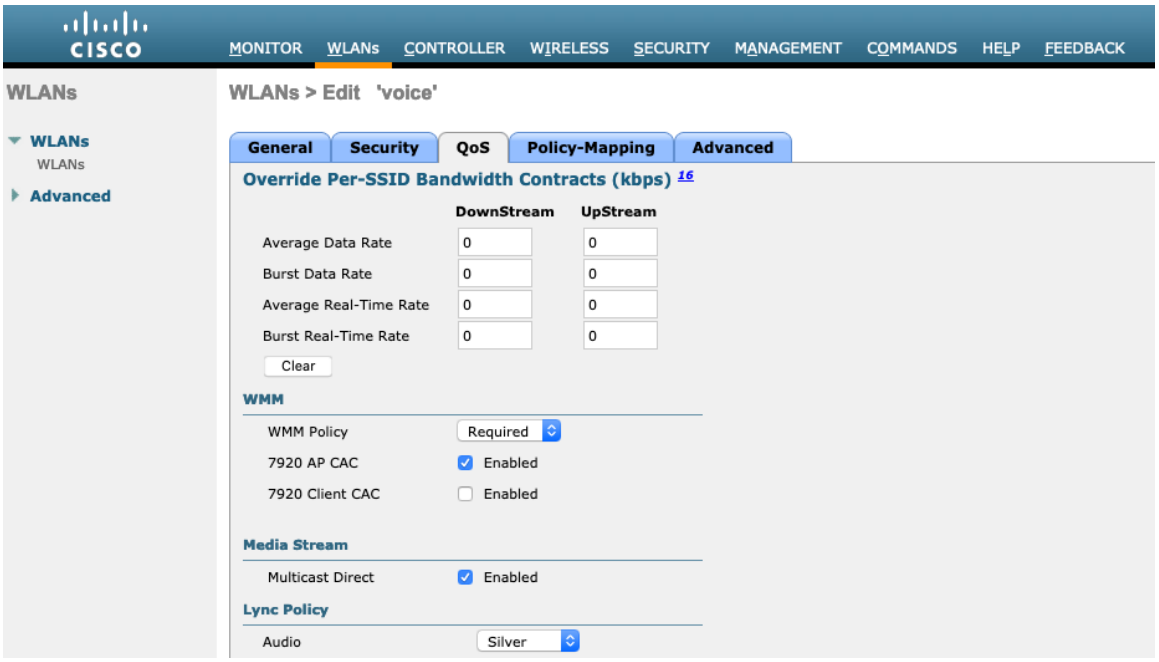
Webex Desk Series または他の WMM 対応電話機がこの SSID を使用する予定の場合にのみ、[WMM ポリシー（WMM Policy）] を **[必須（Required）]** に設定する必要があります。

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。

他の非 WMM クライアントが Webex Desk Series 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。





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。

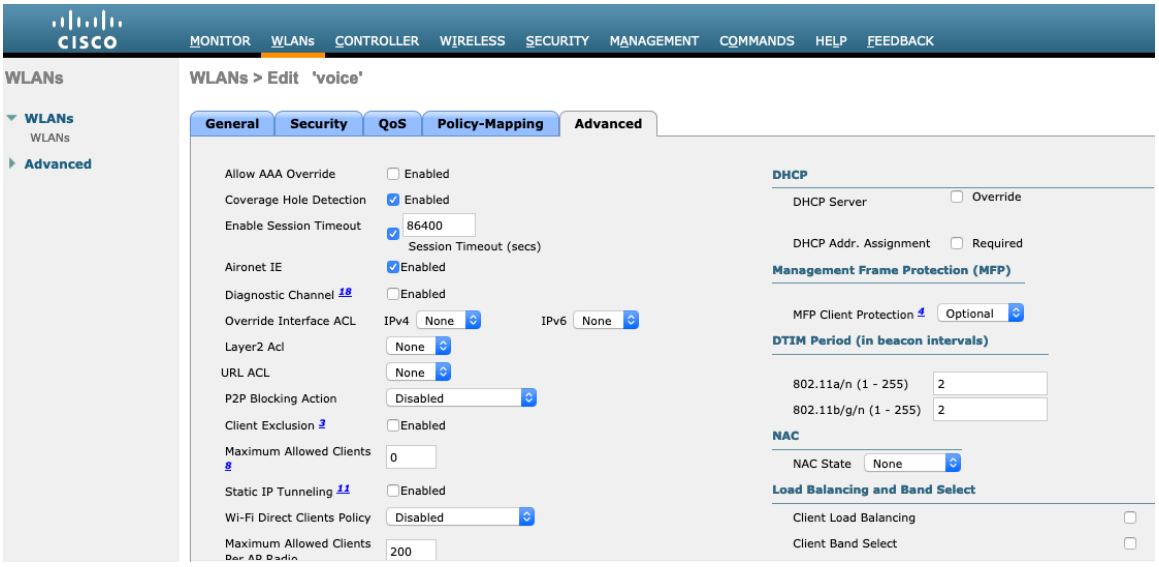
[管理フレーム保護（Management Frame Protection）] を **[任意（Optional）]** または **[無効（Disabled）]** に設定します。

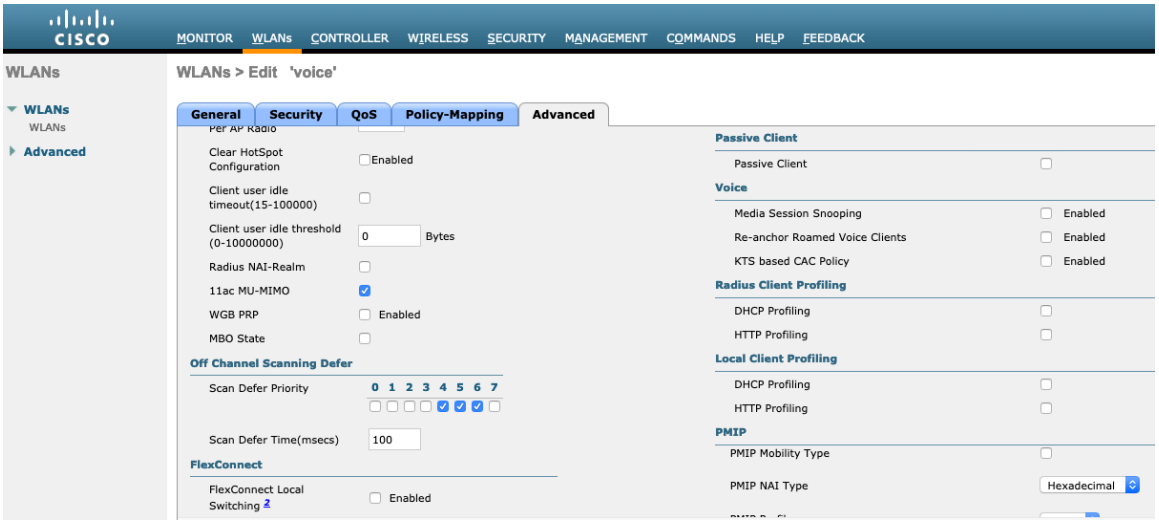
[DTIM 周期（DTIM Period）] を **[2]**に、ビーコン周期を **[100 ミリ秒]** に設定します。

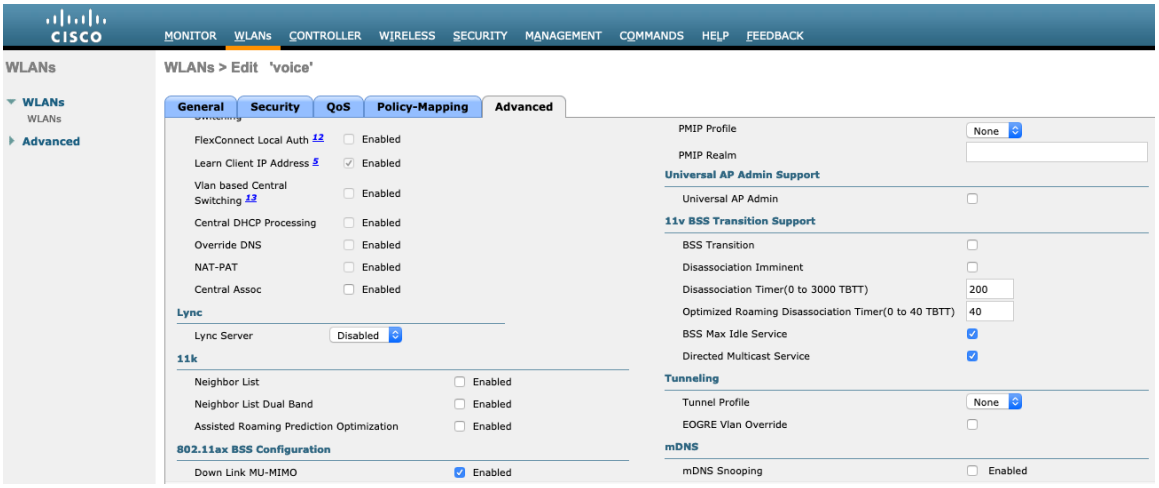
[クライアント ロード バランシング（Client Load Balancing）] と **[クライアントの帯域選択（Client Band Select）]** が無効になっていることを確認します。

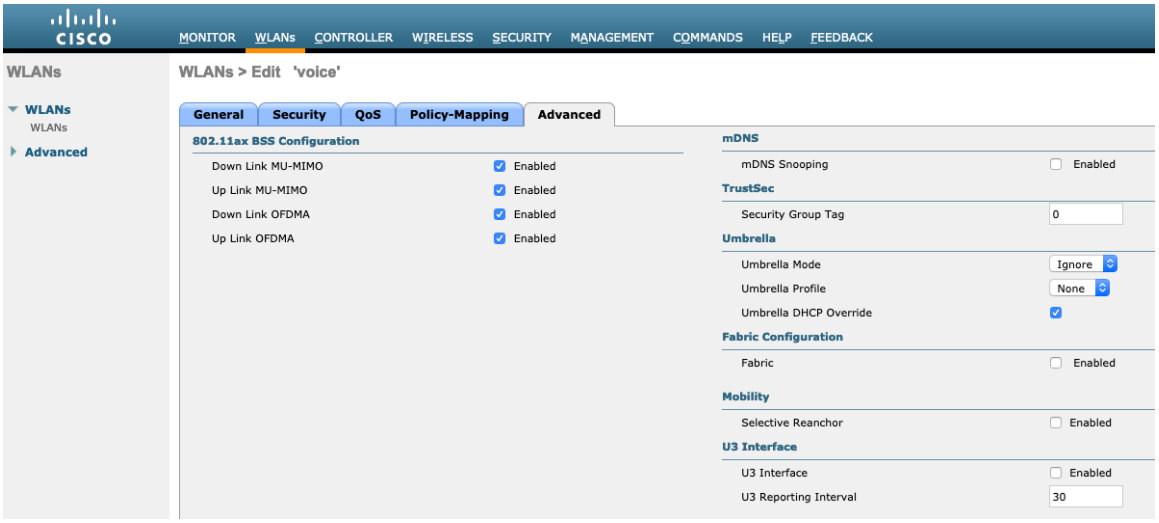
コールがコントローラ間ローミングを実行した後に終了すると、ワイヤレス LAN 接続が短時間中断されることがあるので、**[ローミングされた音声クライアントを再固定（Re-anchor Roamed Voice Clients）]** を無効にすることを推奨します。

802.11k と 802.11v はサポートされていないため、無効にする必要があります。



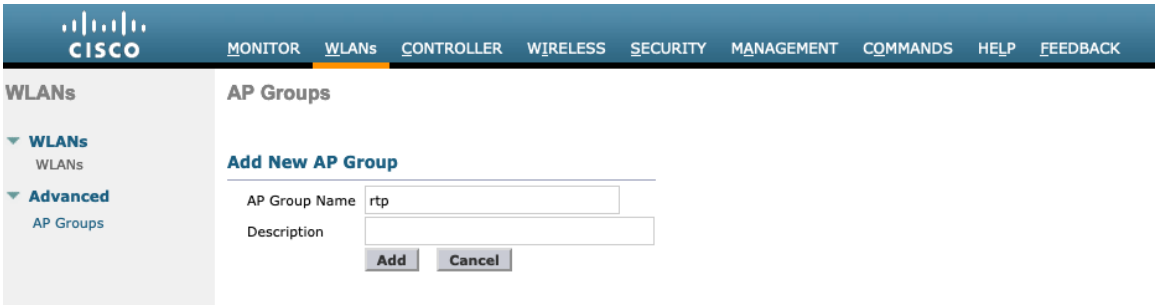

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
General Security QoS Policy-Mapping Advanced
Clear HotSpot Configuration
Enabled
Client user idle timeout(15-100000)
Client user idle threshold (0-10000000)
0
Bytes
Radius NAI-Realm
11ac MU-MIMO
WGB PRP
Enabled
MBO State
Off Channel Scanning Defer
Scan Defer Priority
0 1 2 3 4 5 6 7
Scan Defer Time(msecs)
100
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
Hexadecimal

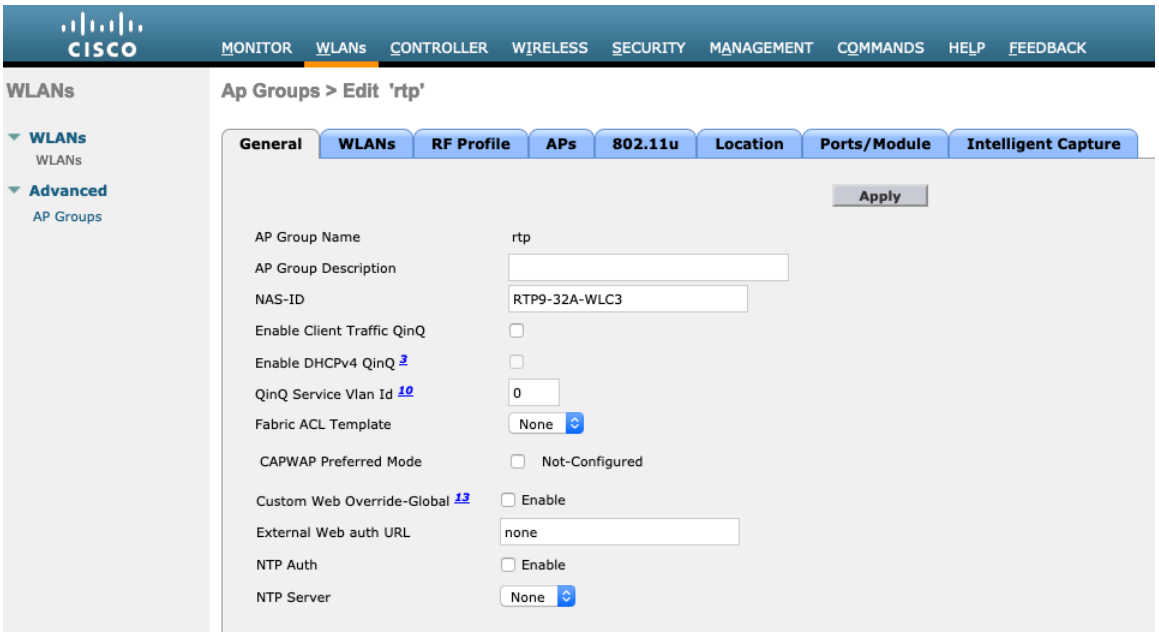

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
General Security QoS Policy-Mapping Advanced
FlexConnect Local Auth
Enabled
Learn Client IP Address
Enabled
Vlan based Central Switching
Enabled
Central DHCP Processing
Enabled
Override DNS
Enabled
NAT-PAT
Enabled
Central Assoc
Enabled
Lync
Lync Server
Disabled
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
None
PMIP Realm
Universal AP Admin Support
Universal AP Admin
11v BSS Transition Support
BSS Transition
Disassociation Imminent
Disassociation Timer(0 to 3000 TBTT)
200
Optimized Roaming Disassociation Timer(0 to 40 TBTT)
40
BSS Max Idle Service
Directed Multicast Service
Tunneling
Tunnel Profile
None
EOGRE Vlan Override
mDNS
mDNS Snooping
Enabled


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
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
0
Umbrella
Umbrella Mode
Ignore
Umbrella Profile
None
Umbrella DHCP Override
Fabric Configuration
Fabric
Enabled
Mobility
Selective Reanchor
Enabled
U3 Interface
U3 Interface
Enabled
U3 Reporting Interval
30

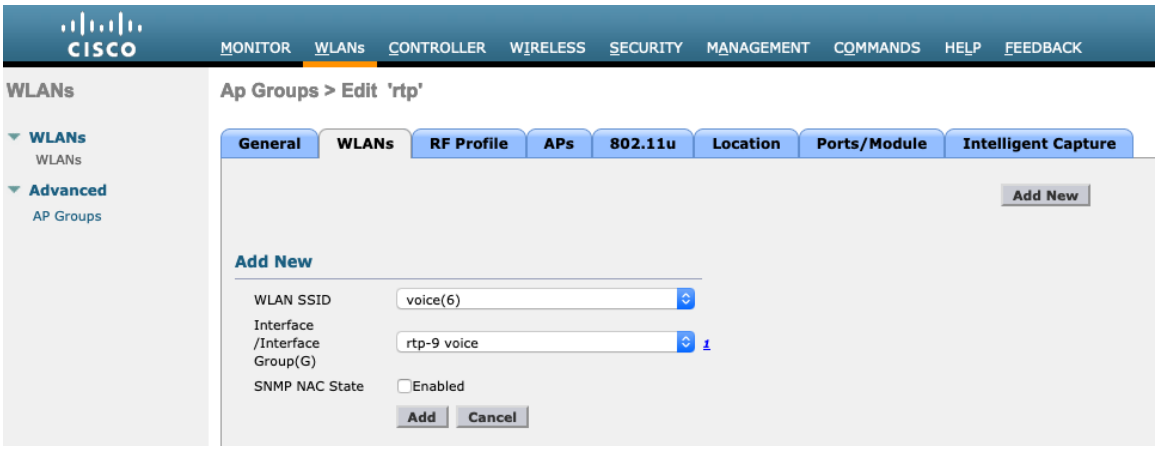
AP グループ

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。



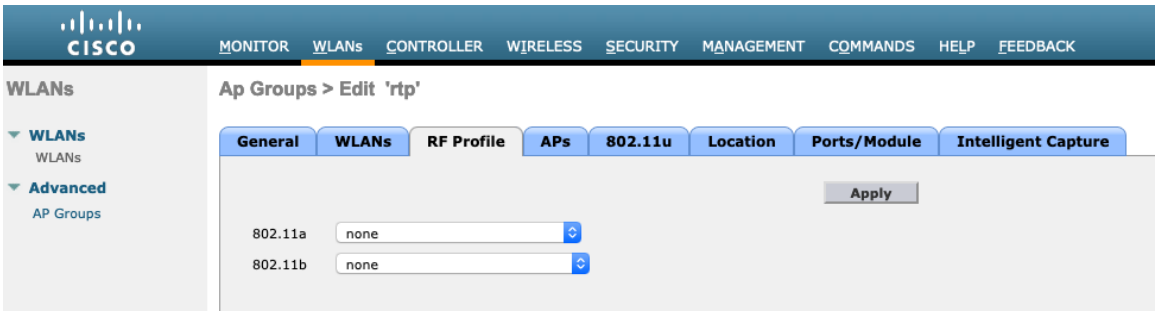


[WLAN（WLANs）] タブで、対象 SSID と、マッピングするインターフェイスを選択して、**[追加（Add）]** を押します。



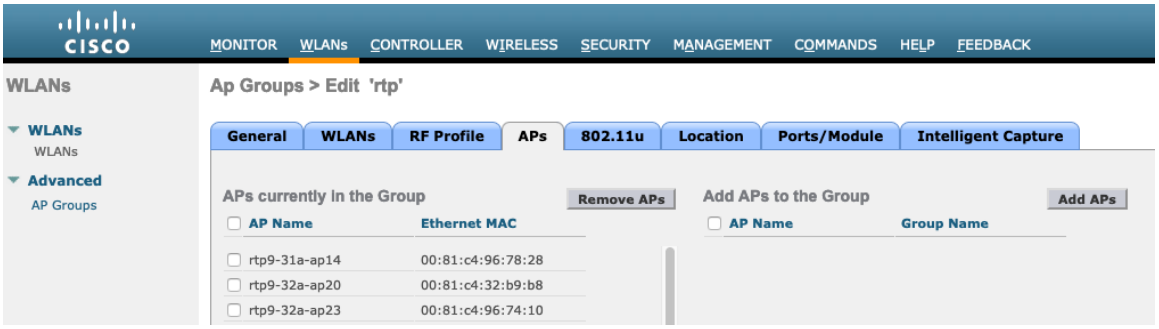
[RF プロファイル（RF Profile）] タブで、対象の 802.11a または 802.11b RF プロファイルを選択して、**[適用（Apply）]** を選択します。

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。

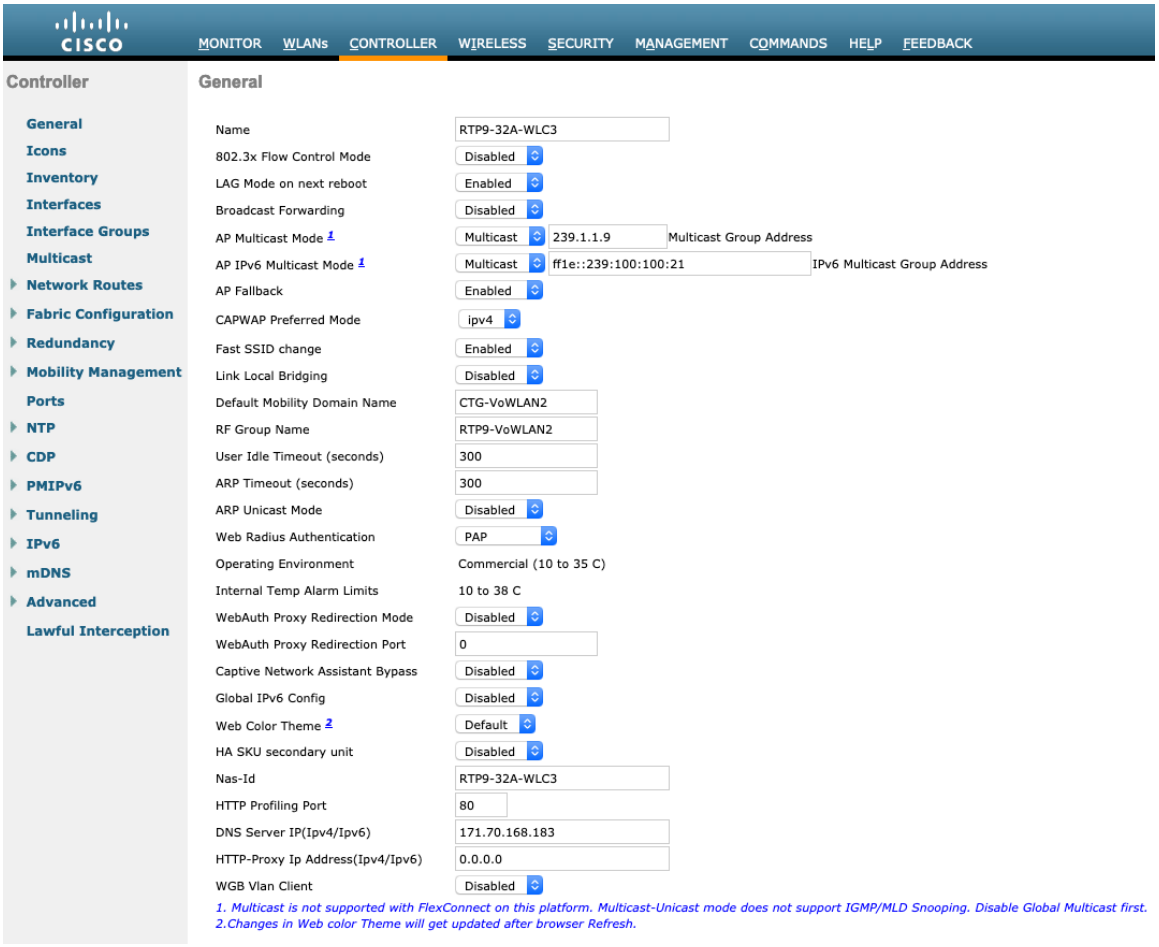


コントローラの設定

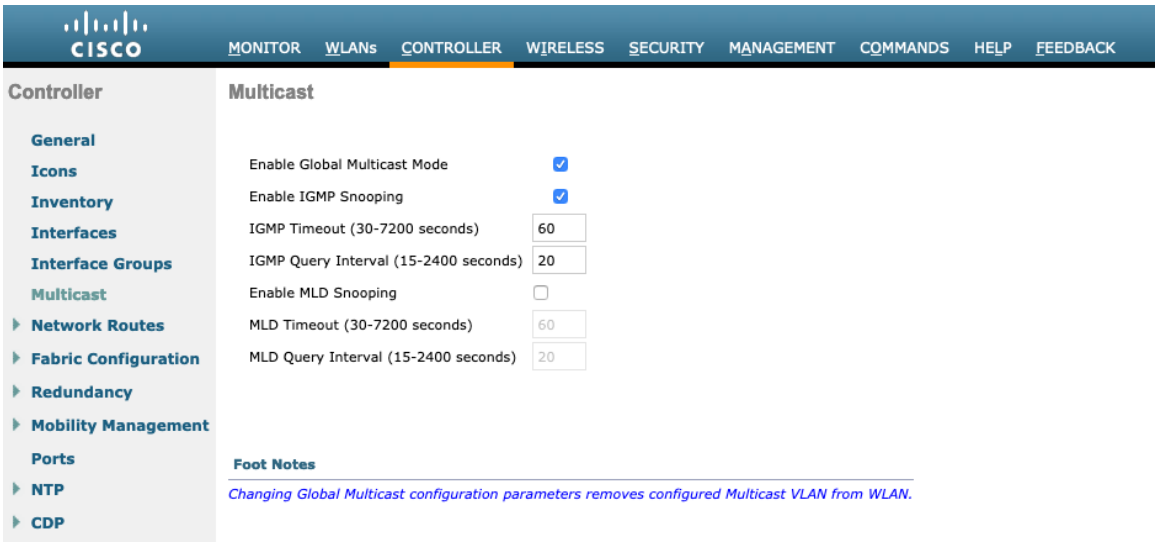
Cisco ワイヤレス LAN コントローラのホスト名が正しく設定されていることを確認します。

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。

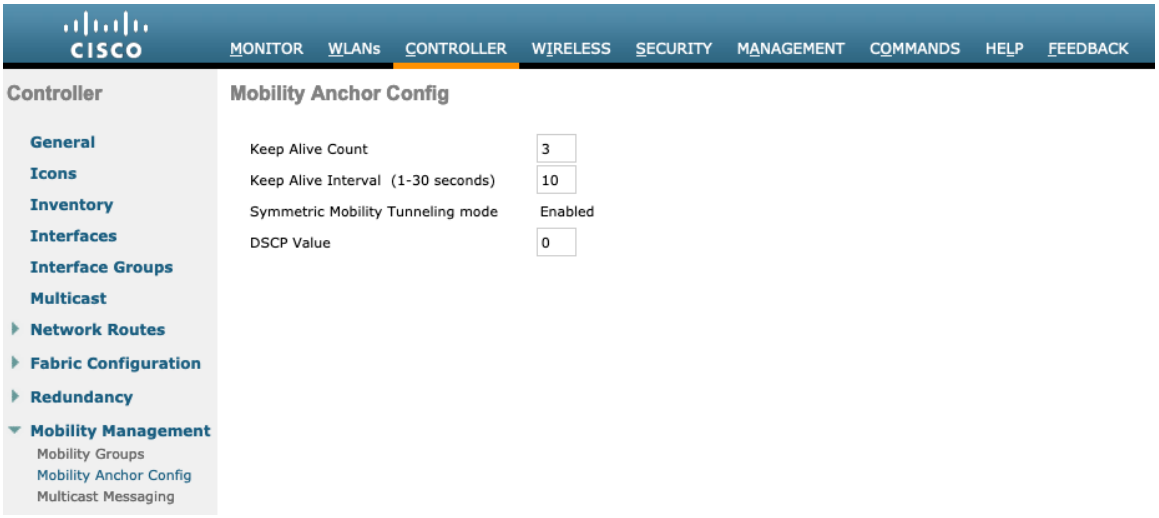
対象の AP マルチキャスト モードを設定します。



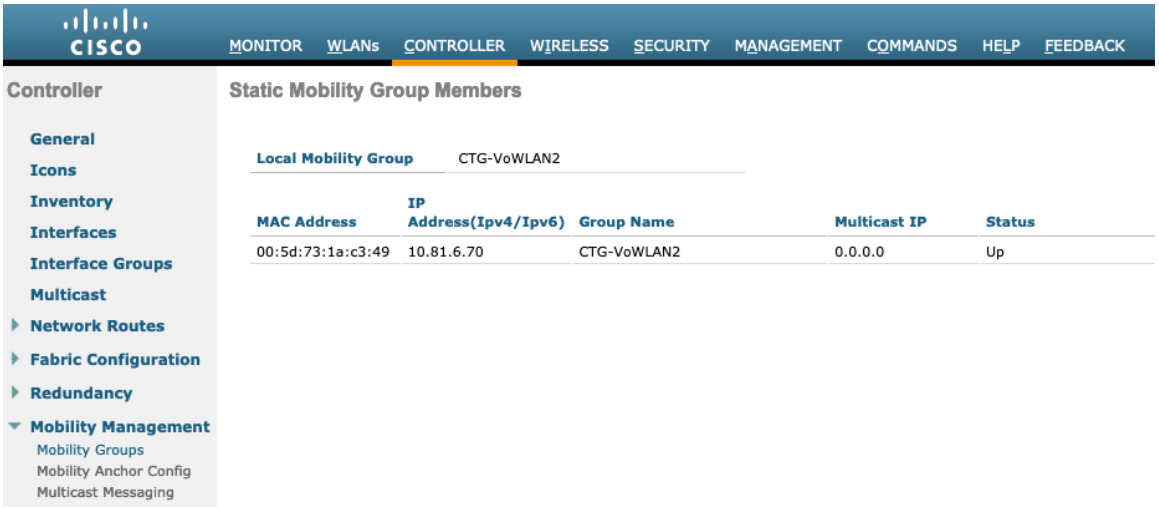
マルチキャストを使用する場合は、**[グローバル マルチキャスト モードの有効化（Enable Global Multicast Mode）]** および **[IGMP スヌーピングの有効化（Enable IGMP Snooping）]** を有効にする必要があります。



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。



コール アドミッション制御（CAC）

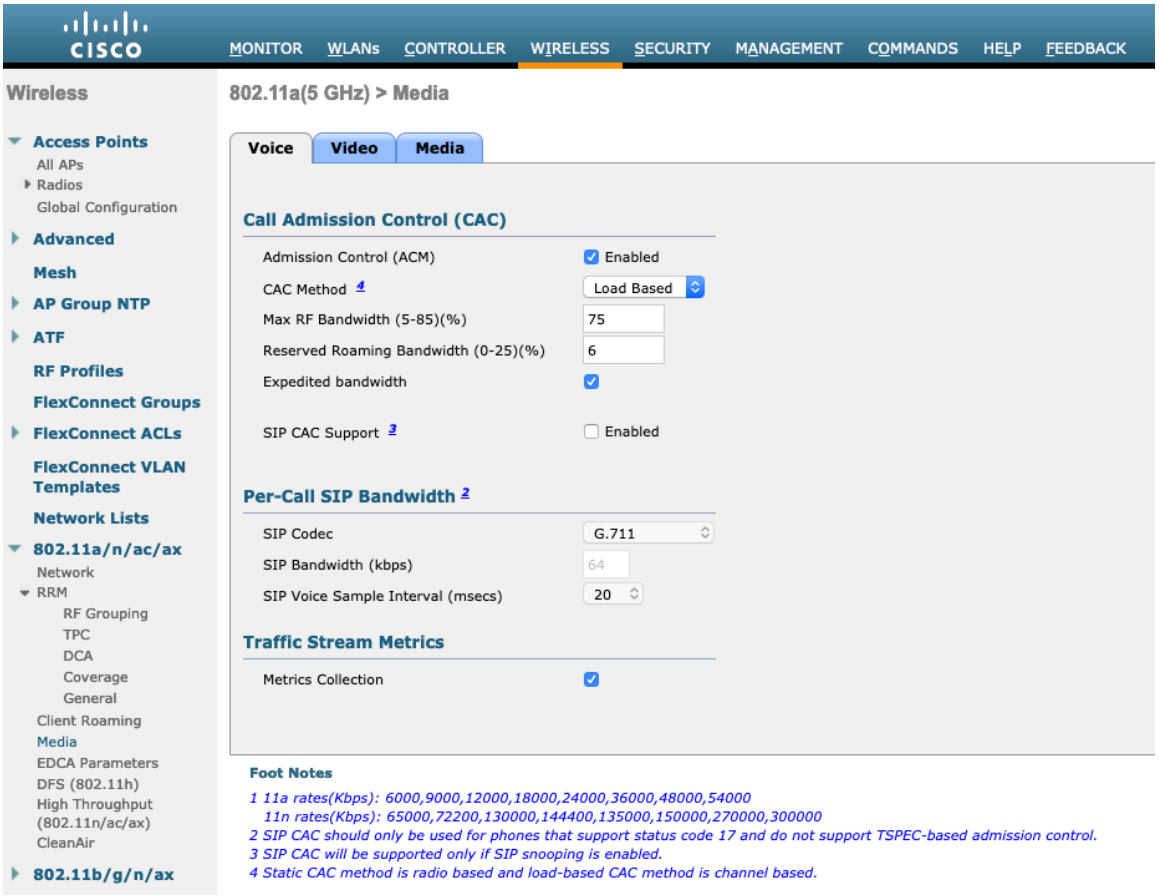
[音声（Voice）] で **[アドミッションコントロール必須（Admission Control Mandatory）]** を有効にして、使用する帯域（5 GHz または 2.4 GHz）に対して最大帯域幅および予約済みのローミング帯域幅の各割合を設定することを推奨します。

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。

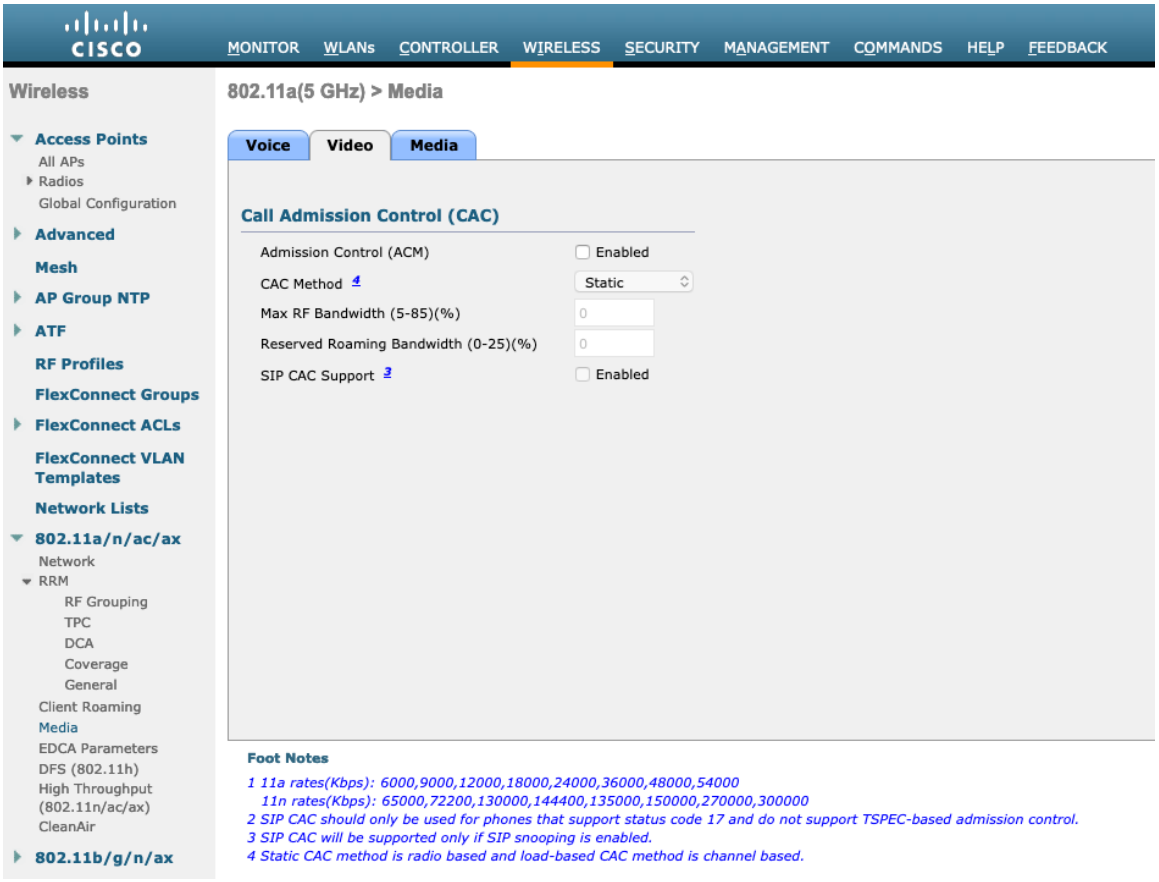
ローミング クライアントは予約済みのローミング帯域幅以外も使用できますが、その他の帯域幅がすべて使用されている場合に備え、ローミング クライアント向けに一定のローミング帯域幅が予約されます。

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。**



[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。



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）。

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

voice stream-size および voice max-streams の値は、必要に応じて次のコマンドを使用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..... Platinum (voice)
WMM..... 許可

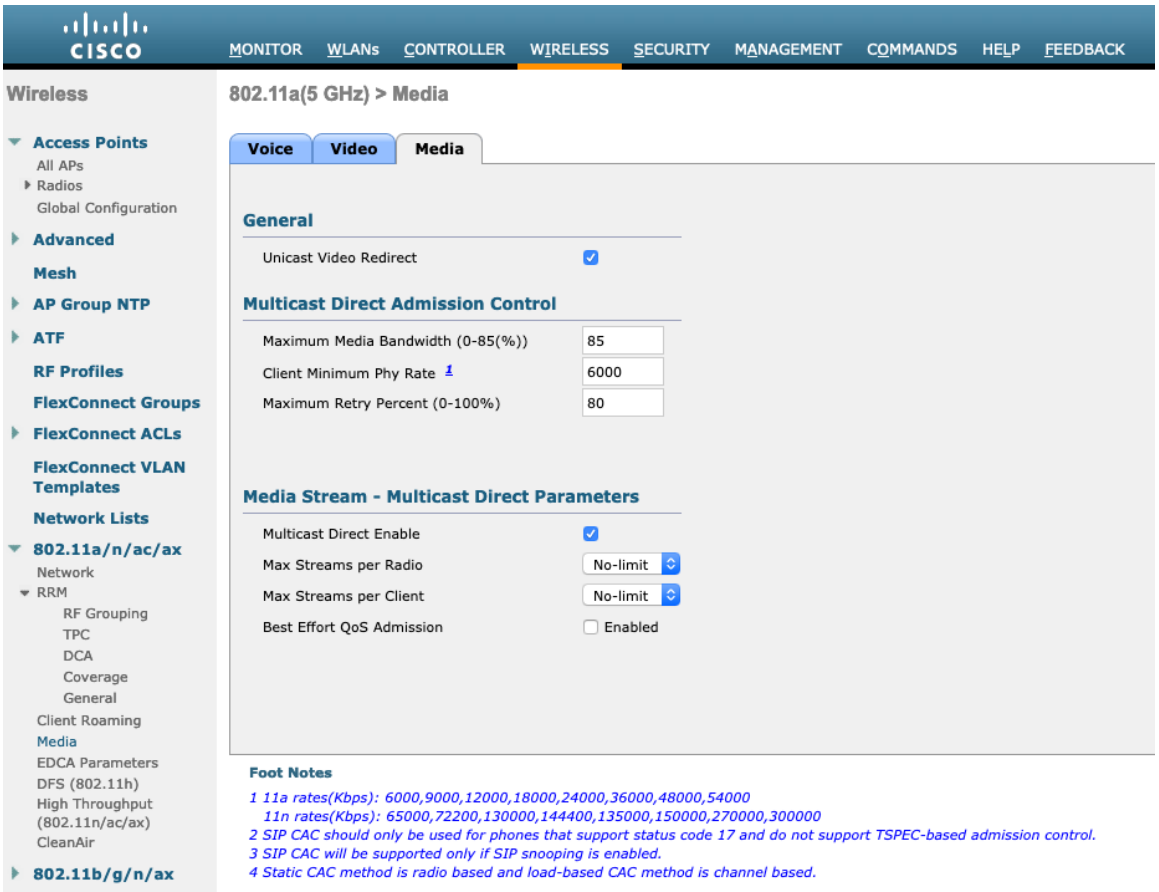
Dot11-Phone Mode (7920)..... ap-cac-limit
Wired Protocol..... 802.1P (Tag=5)

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。



RF プロファイル

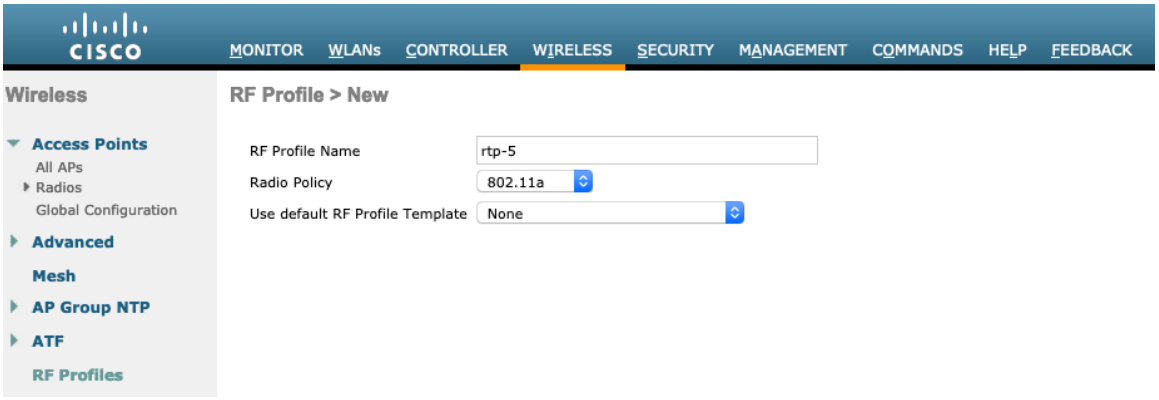
RF プロファイルを作成し、アクセス ポイントのグループが使用する必要がある周波数帯域、データ レート、RRM 設定などを指定できます。

Webex Desk Series 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。

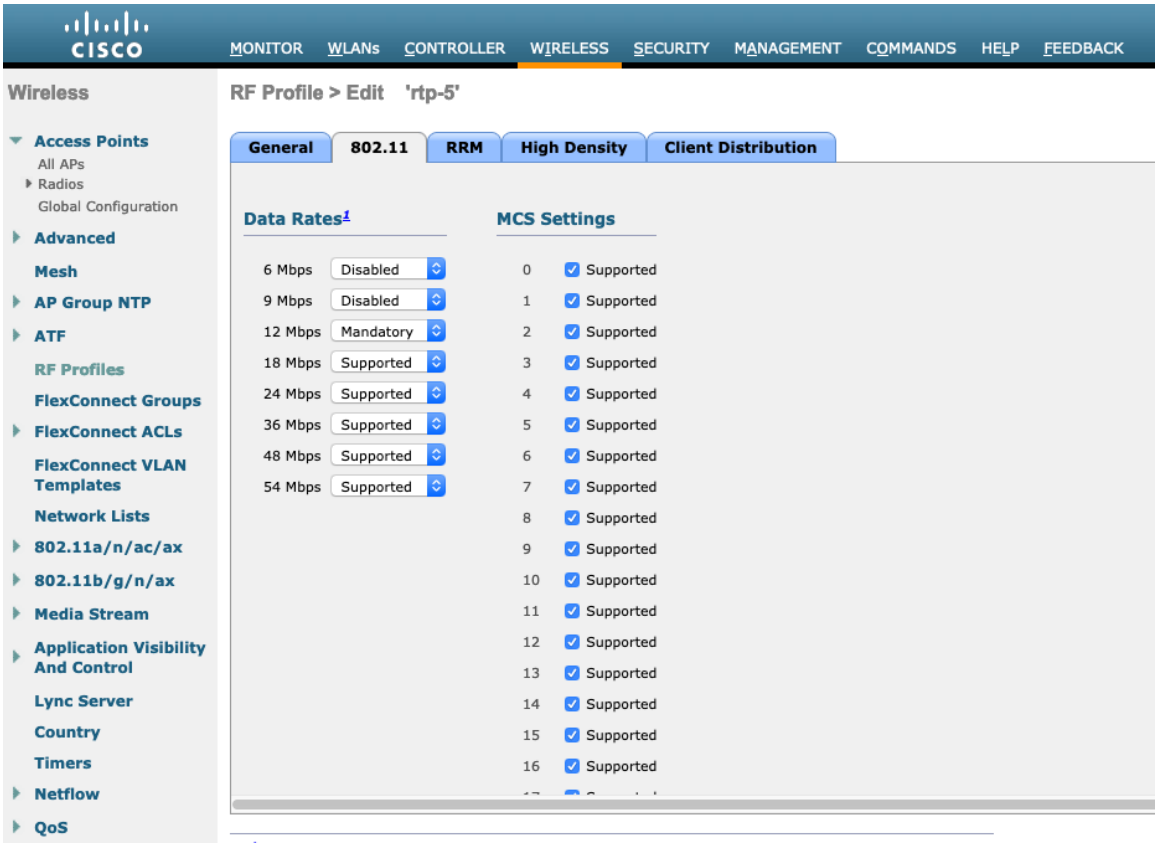
RF プロファイルを作成する場合、**[RF プロファイル名（RF Profile Name）]** と **[無線ポリシー（Radio Policy）]** を定義する必要があります。

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

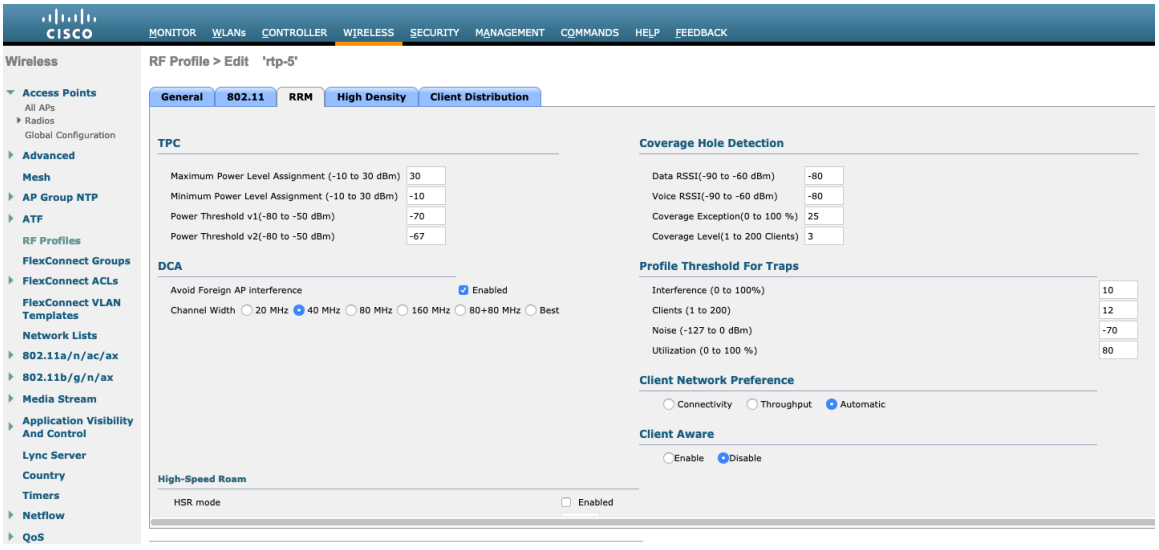


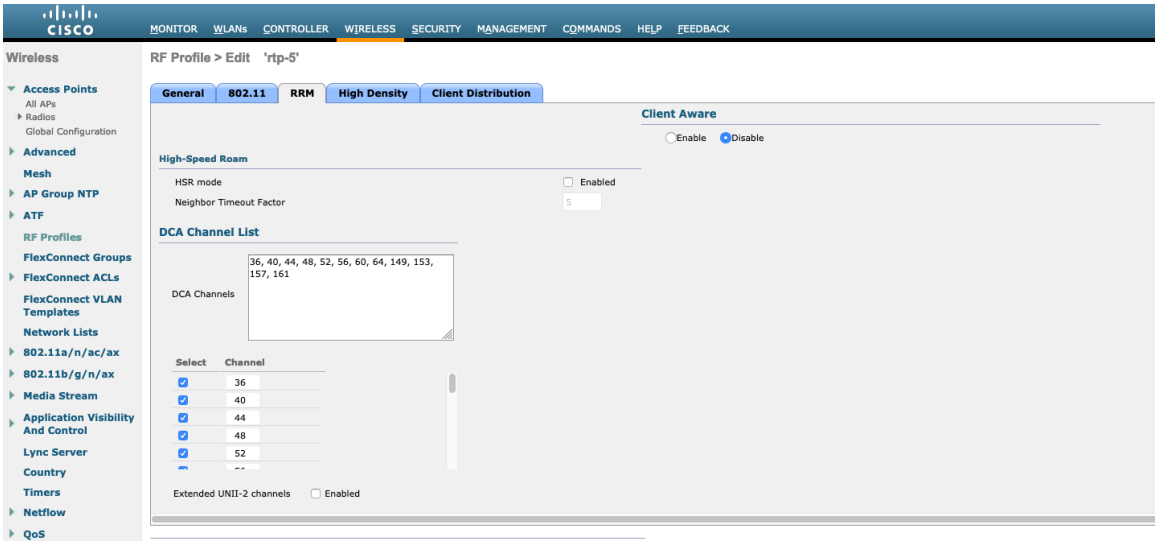
[802.11] タブで、必要に応じてデータレートを設定します。

[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。



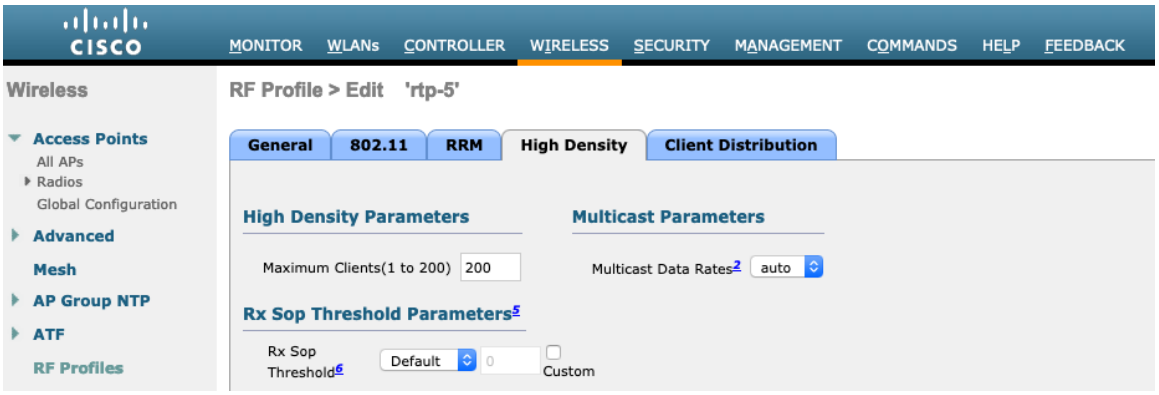
[RRM] タブでは、**[最大電力レベルの割り当て（Maximum Power Level Assignment）]** および **[最小電力レベルの割り当て（Minimum Power Level Assignment）]** 設定と、その他の **[DCA]**、**[TPC]**、および **[カバレッジホール検出（Coverage Hole Detection）]** 設定を設定できます。





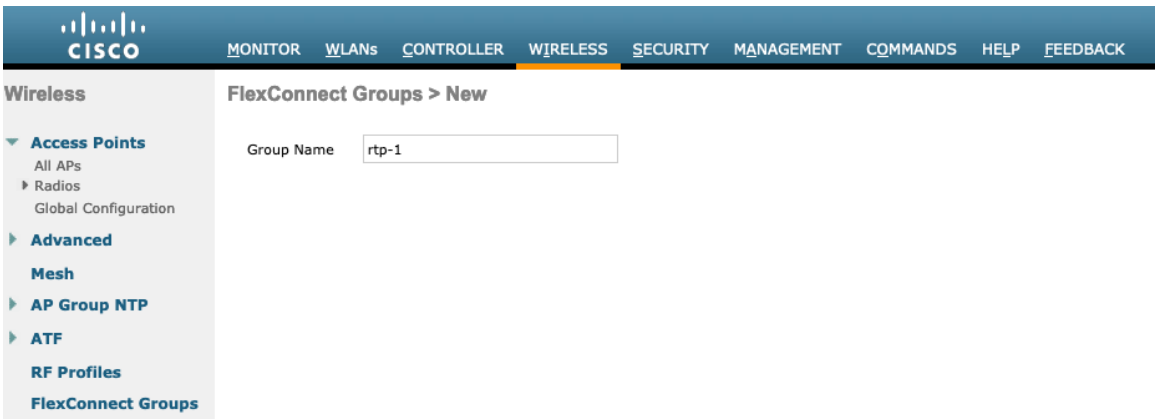
[高密度（High Density）] タブでは、**[最大クライアント数（Maximum Clients）]**、**[マルチキャストデータレート（Multicast Data Rates）]**、および **[Rx Sop のしきい値（Rx Sop Threshold）]** を設定できます。

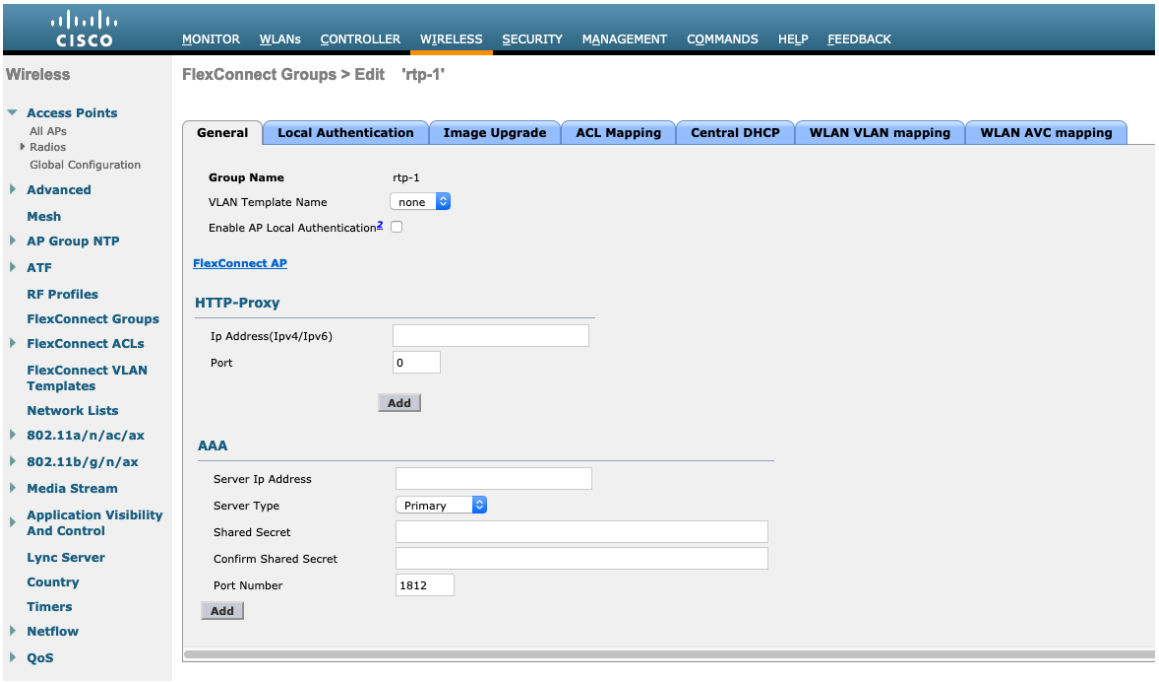
[Rx Sop のしきい値（Rx Sop Threshold）] にはデフォルト値を使用することを推奨します。



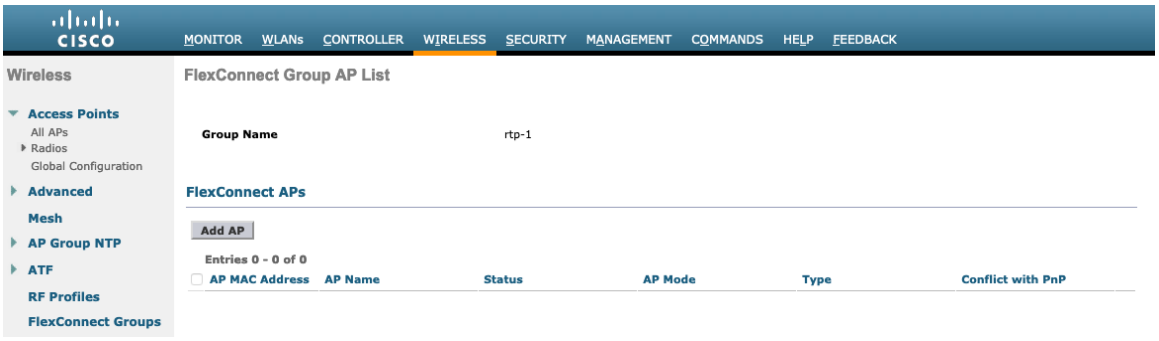
FlexConnect グループ

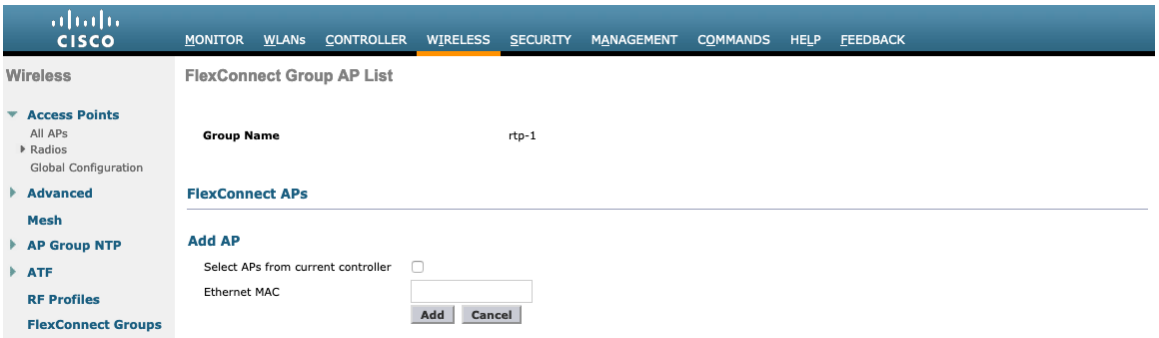
FlexConnect モード用に設定されたすべてのアクセス ポイントを FlexConnect グループに追加する必要があります。





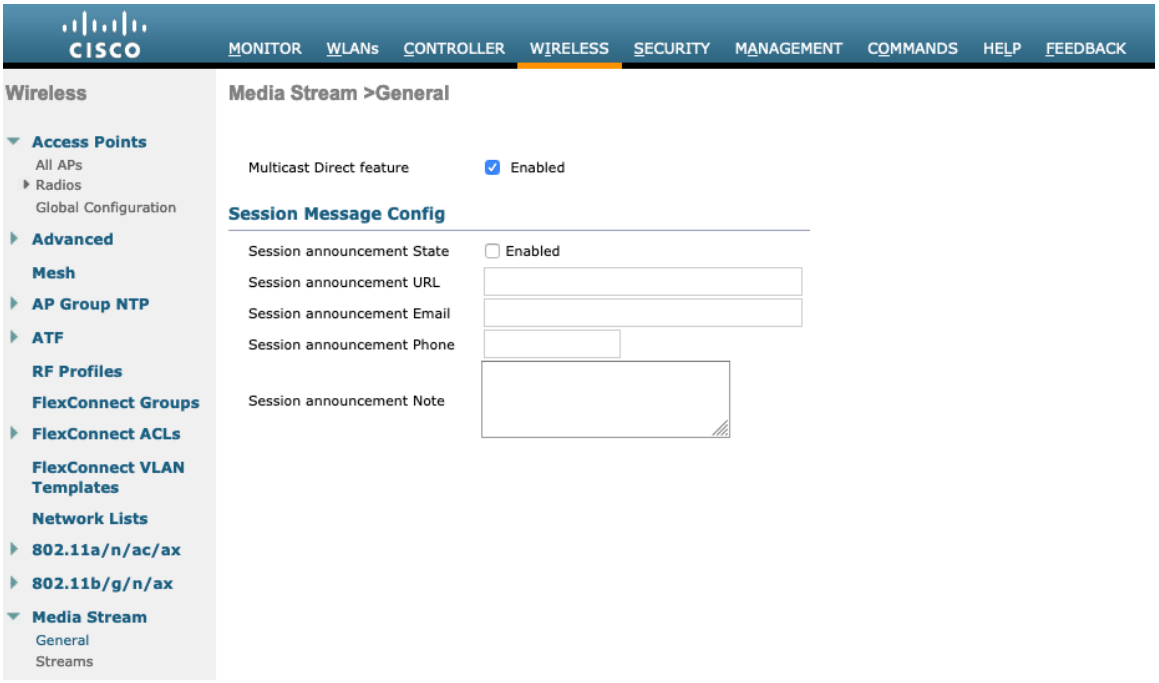
FlexConnect グループごとに許可されるアクセスポイントの最大数は制限されており、これは WLC モデル固有です。

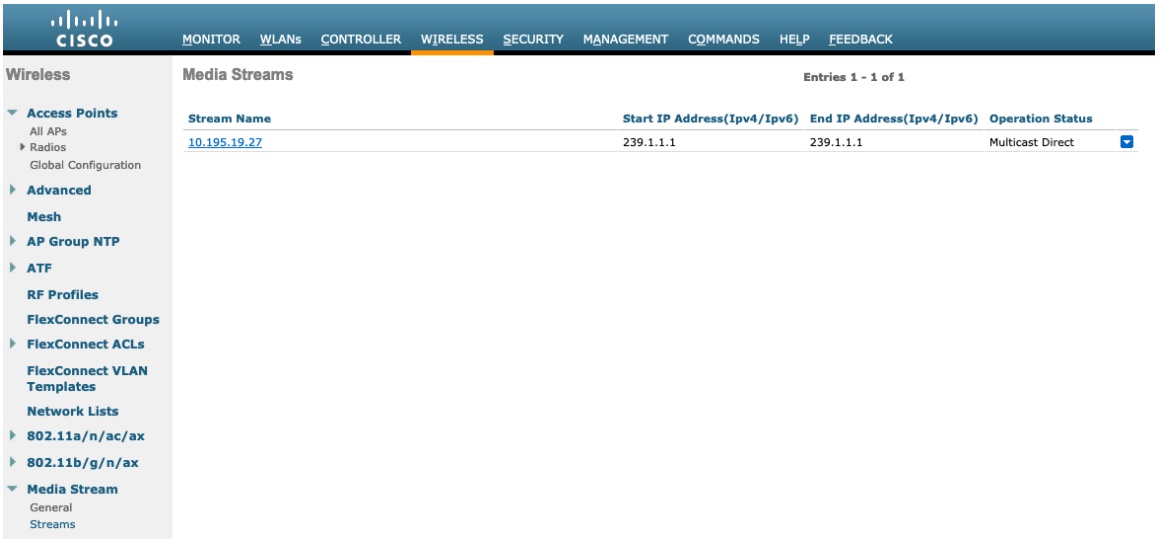




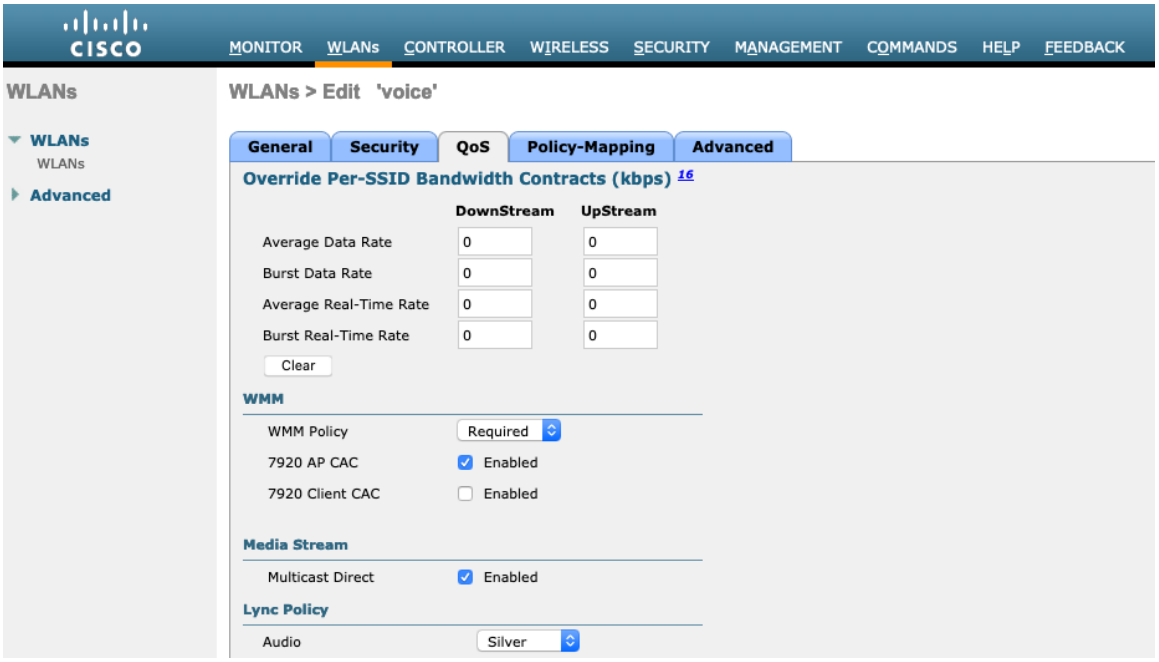
マルチキャスト ダイレクト

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





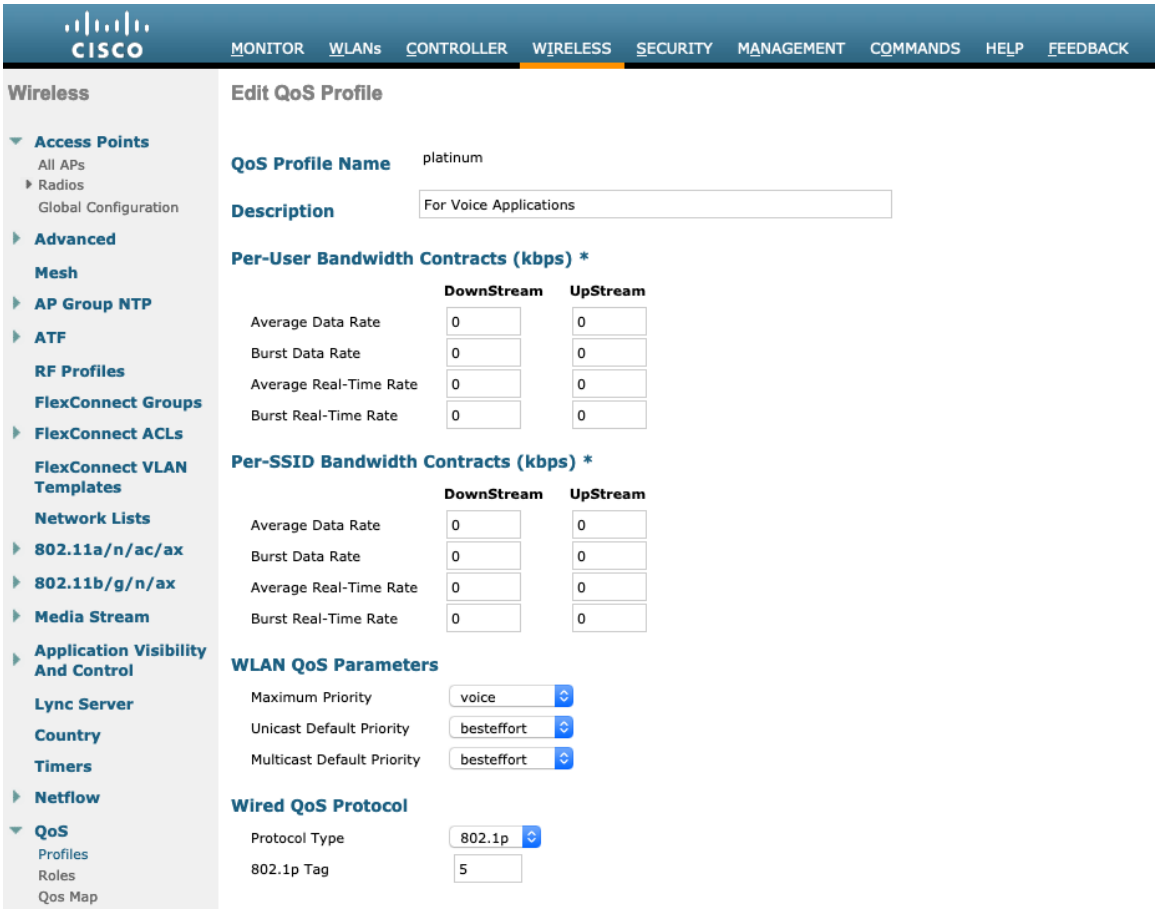
[マルチキャストダイレクト機能（Multicast Direct Feature）] を有効にすると、**[マルチキャストダイレクト（Multicast Direct）]** を有効化するオプションが WLAN 設定の [QoS] メニューに表示されます。

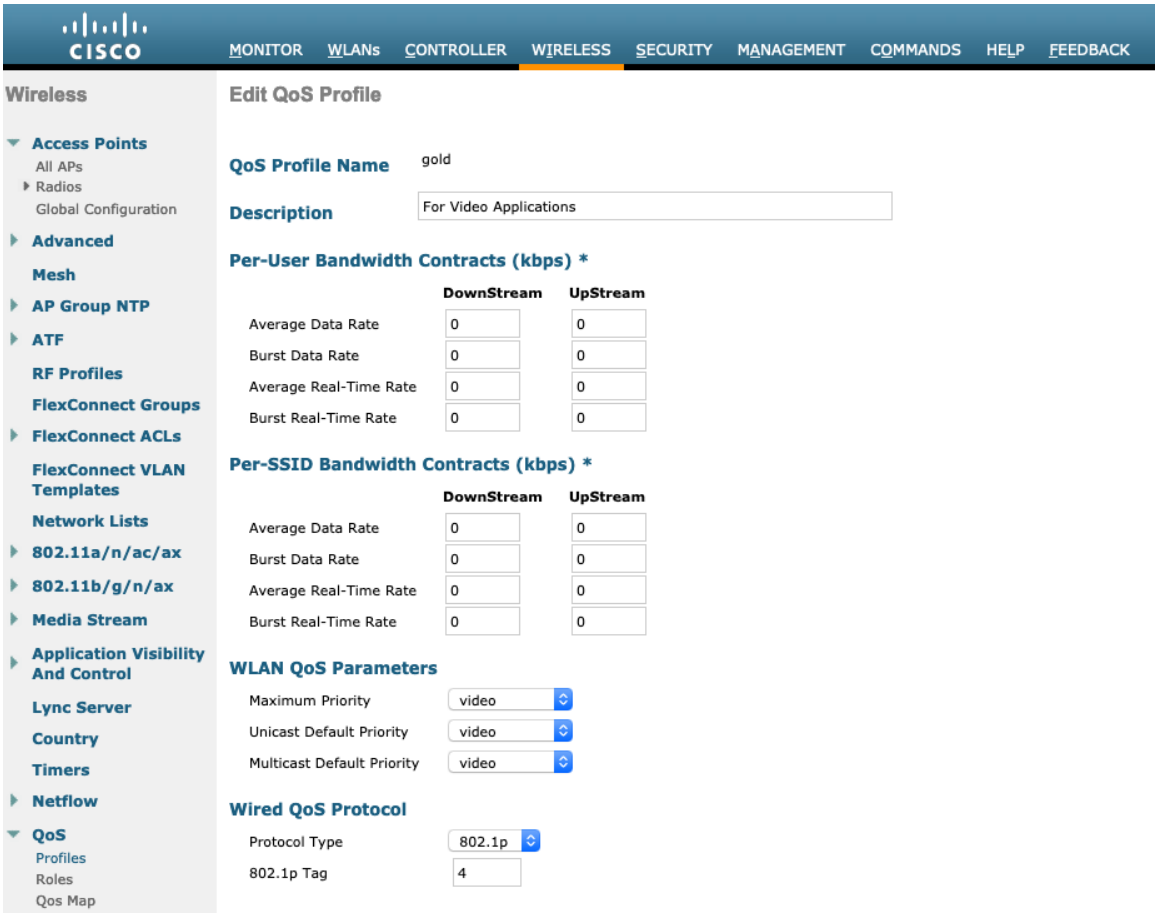


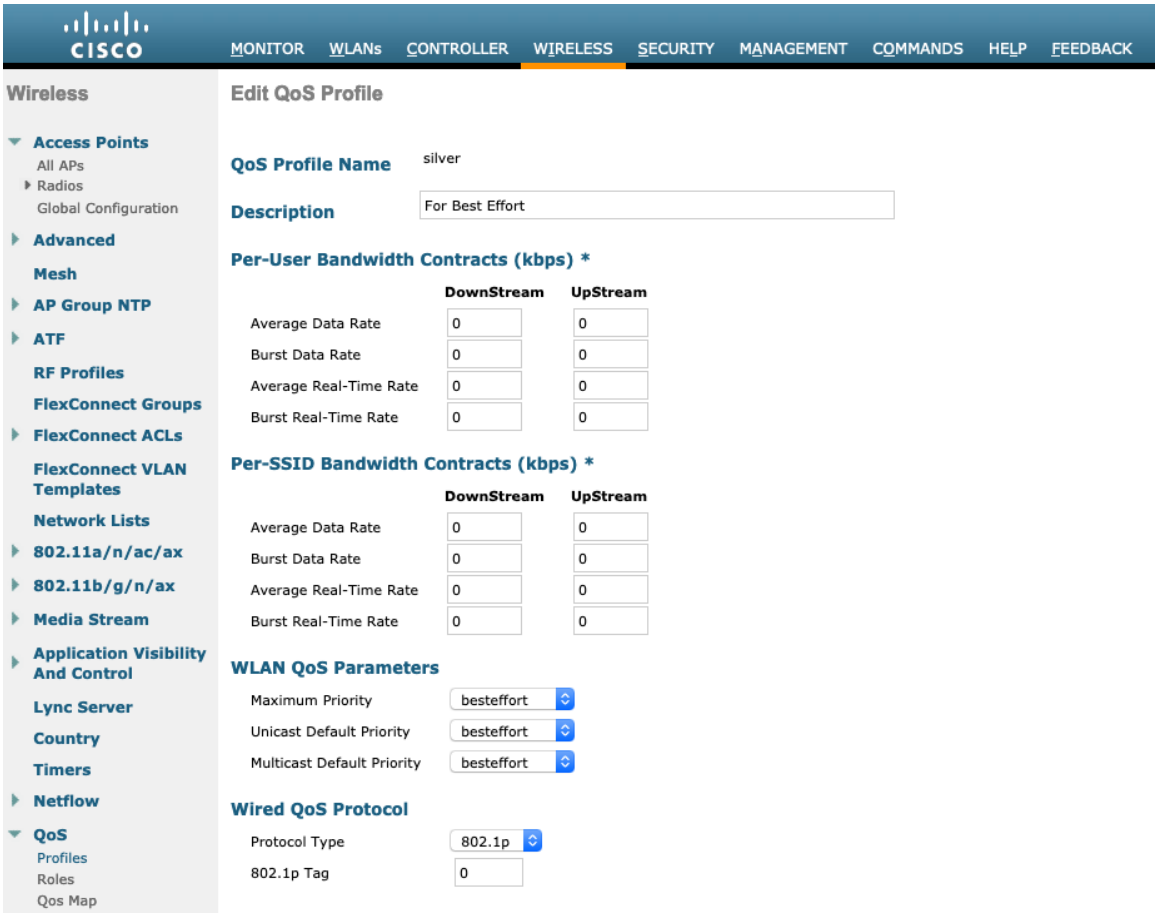
QoS プロファイル

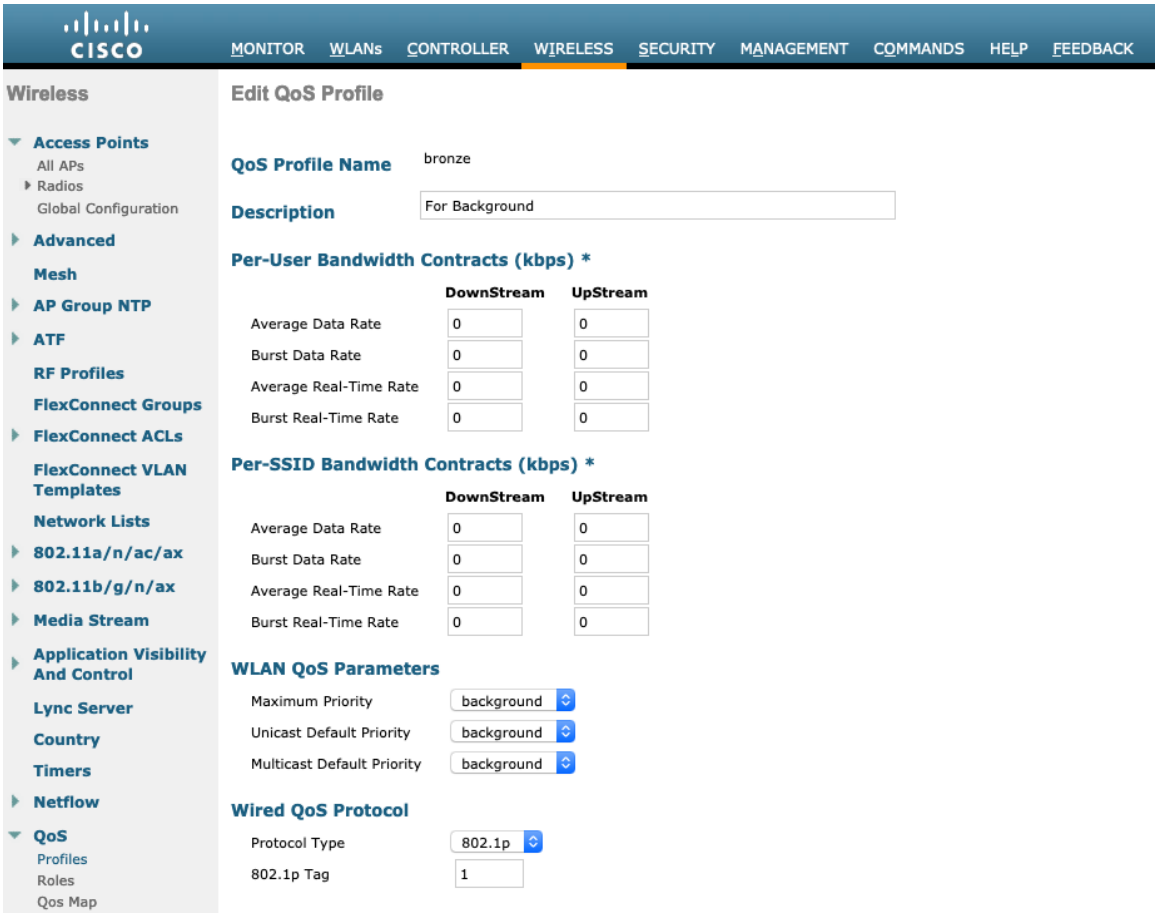
プロトコルタイプとして **[802.1p]** を選択することで、4 つの QoS プロファイル（Platinum、Gold、Silver、Bronze）を設定し、プロファイルごとに、**[802.1pタグ（802.1p Tag）]** を設定します。

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


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
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
platinum
Description
For Voice Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
voice
Unicast Default Priority
besteffort
Multicast Default Priority
besteffort
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
5


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
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
For Video Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
Unicast Default Priority
Multicast Default Priority
video
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
4


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
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
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
besteffort
Unicast Default Priority
Multicast Default Priority
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag

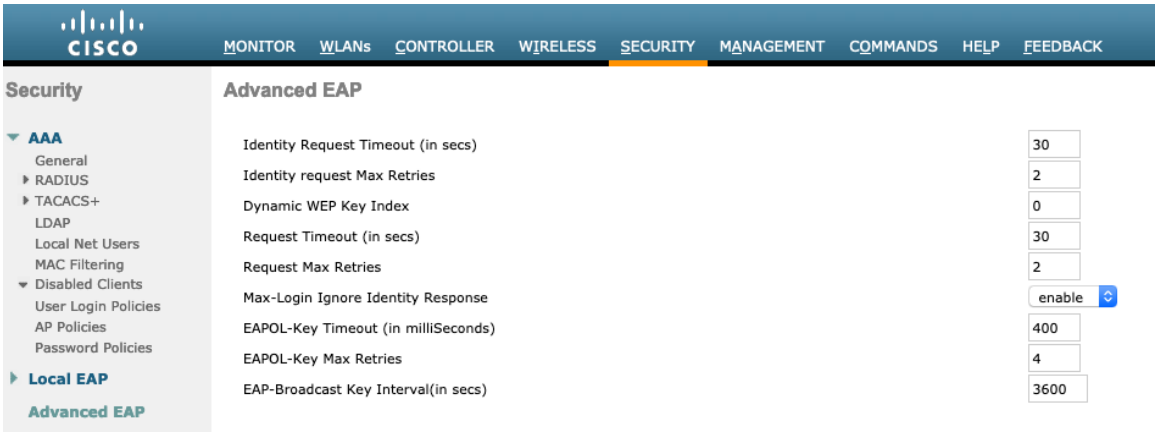


詳細設定

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。



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-Key Timeout]** をデフォルトの 1000 ミリ秒から 400 ミリ秒に減らし、**[EAPOL-Key Max Retries]** をデフォルトの 2 から 4 に設定することを推奨します。

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

[EAPOL-Key Timeout] は、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..... Enabled

Excessive 802.11-authentication failures..... Enabled

Excessive 802.1x-authentication..... Enabled

IP-theft..... Enabled

Excessive Web authentication failure..... Enabled

Signature Policy

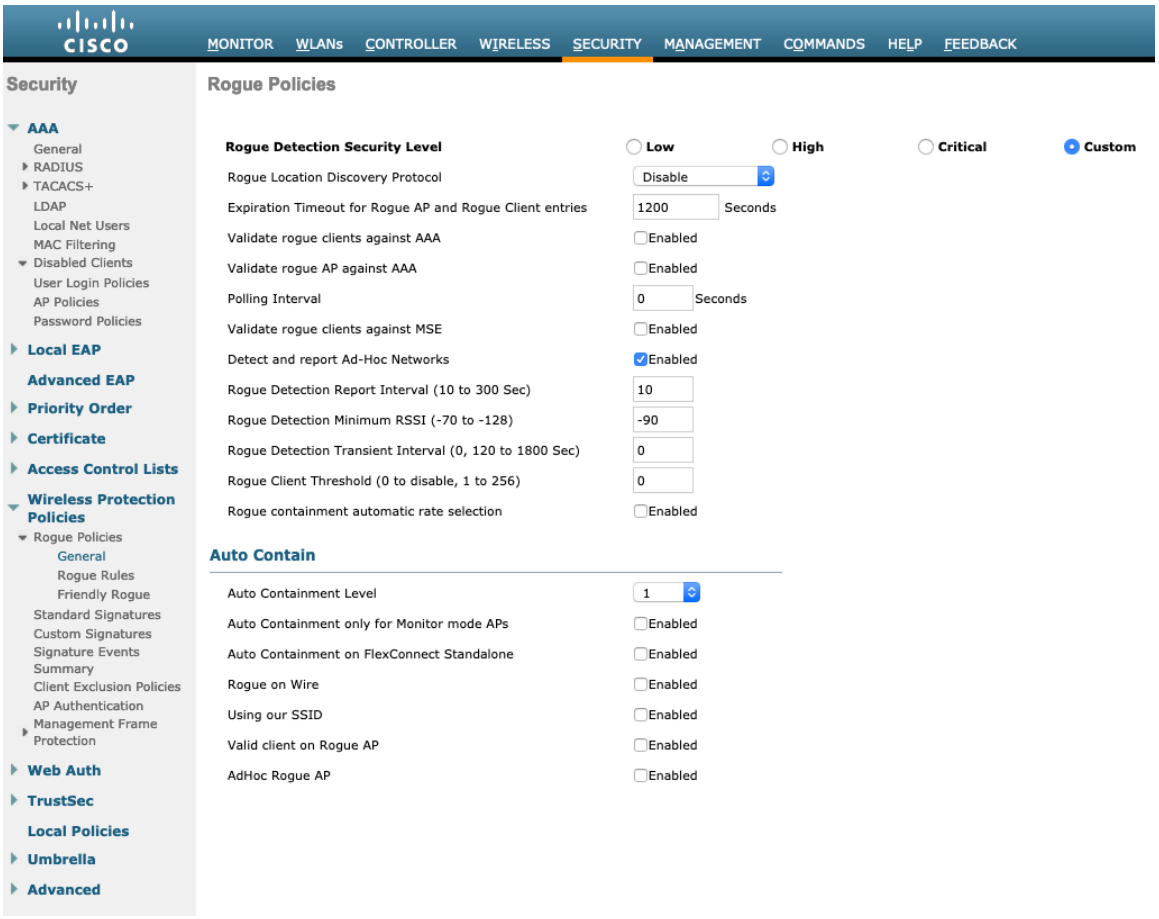
Signature Processing..... Enabled

Cisco 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

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 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）]** と **[CCKM]** が必須として構成されていないことを確認します
- **[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]** が **[無効（Disabled）]** になっていることを確認します
- **[802.11v]** が **[無効（Disabled）]** になっていることを確認します

- **[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
- **[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
- **[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

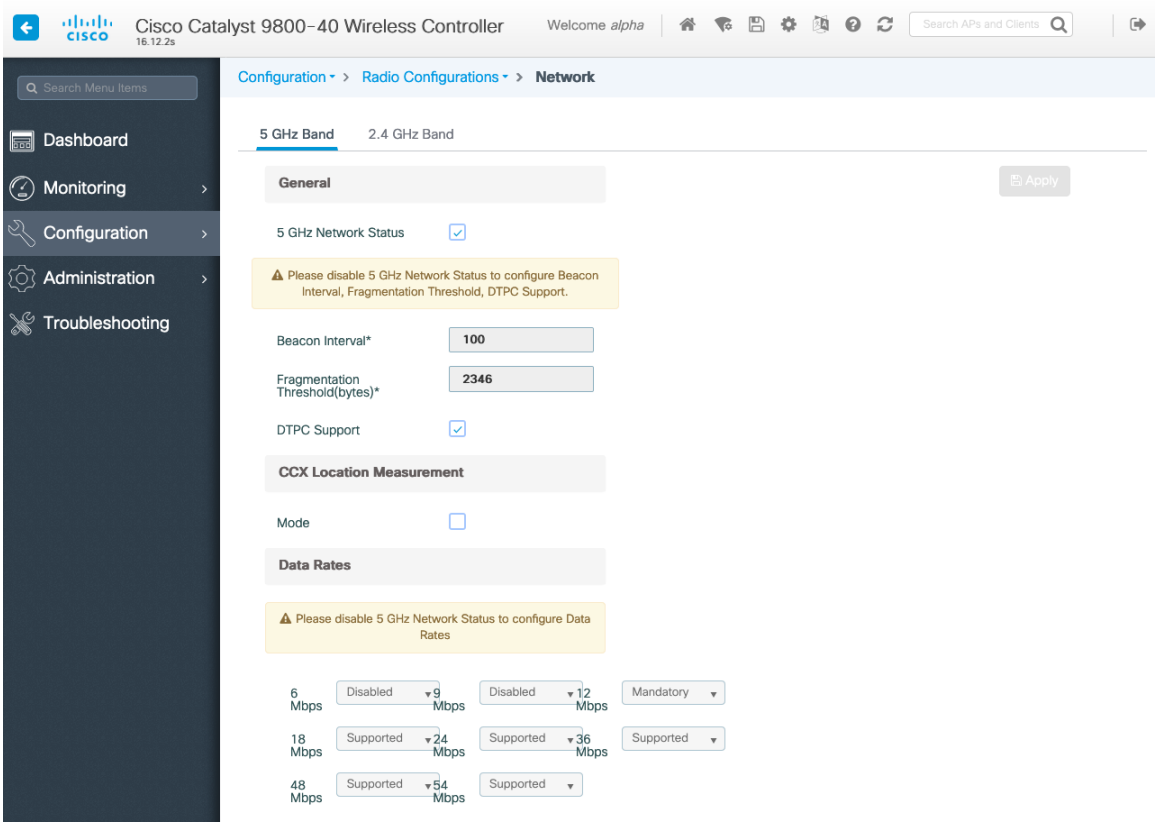
802.11 ネットワークの設定

Webex Desk Series 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。

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。

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。



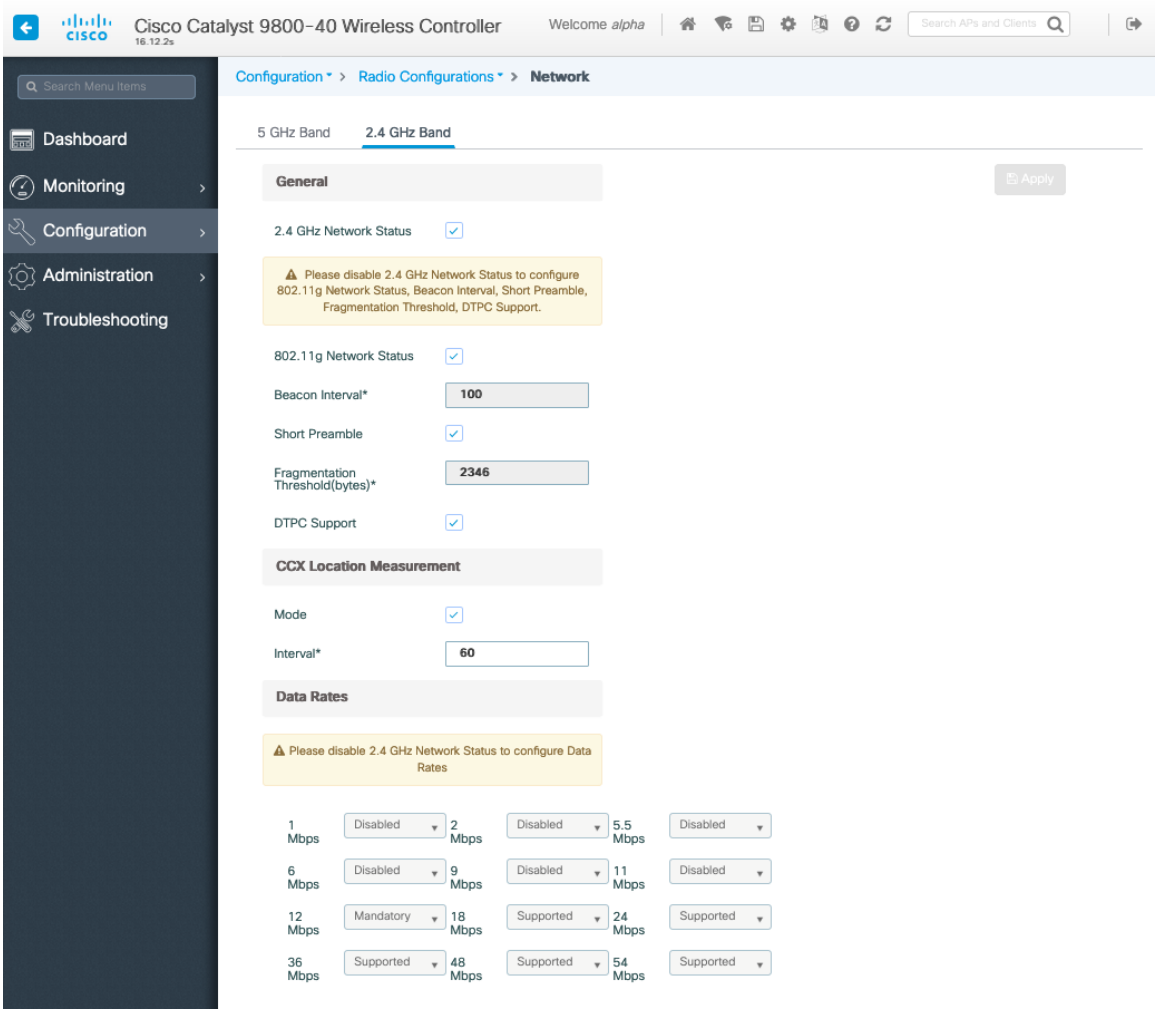
2.4 GHz を使用する場合は、2.4 GHz ネットワークのステータスと 802.11g ネットワークのステータスが **[有効（Enabled）]** に設定されていることを確認します。

[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。

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。



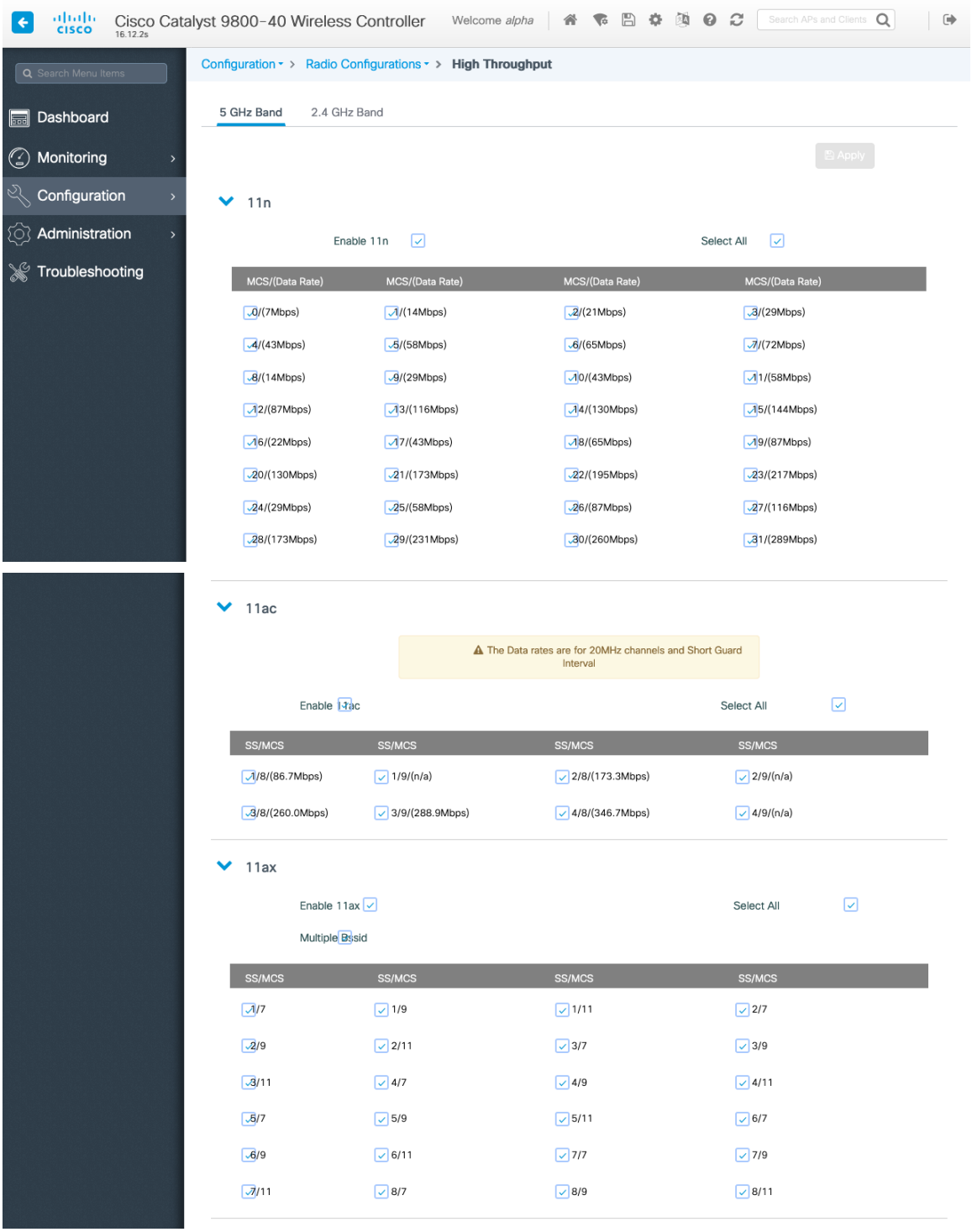
高スループット（802.11n/ac）

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。

Webex Desk Series 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。



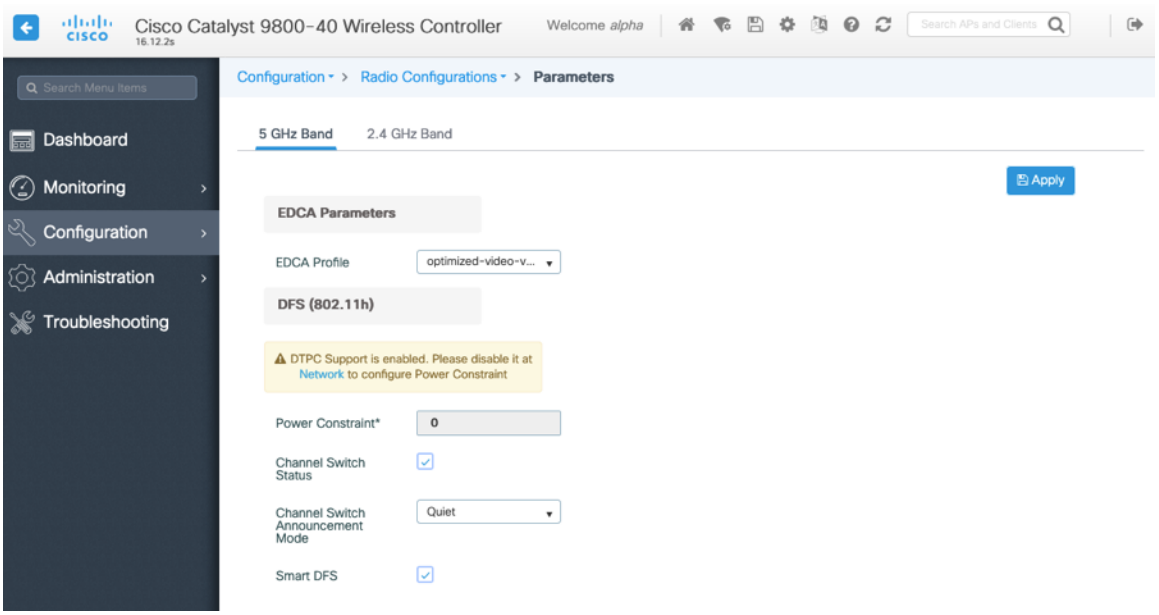
パラメータ

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、**[電力制限（Power Constraint）]** は未設定のままにするか、0 dB に設定する必要があります。

[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。**

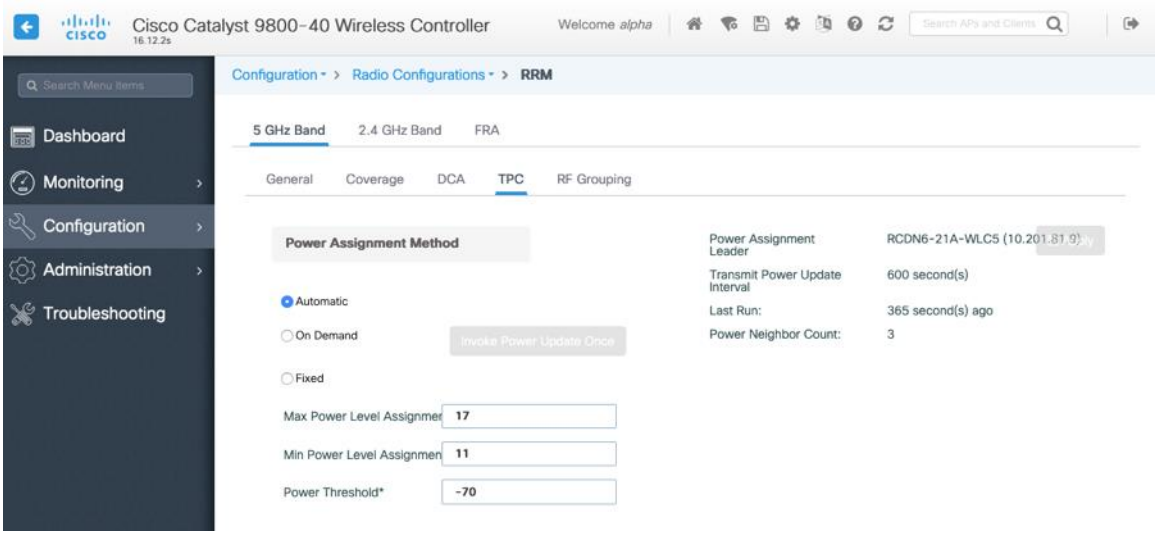


RRM

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。

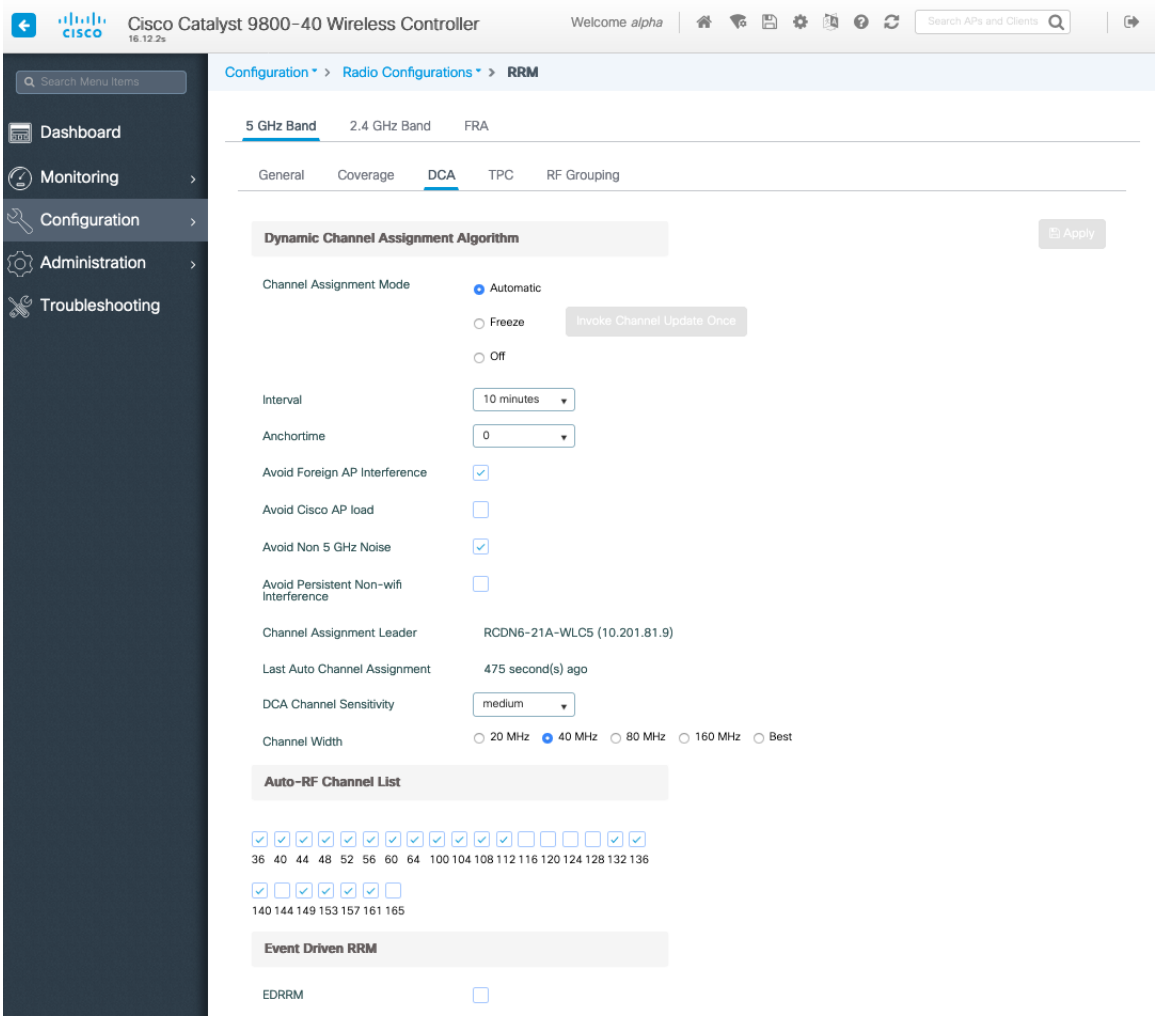
自動電力レベルの割り当てを使用する場合は、電力の最大レベルと最小レベルを指定できます。



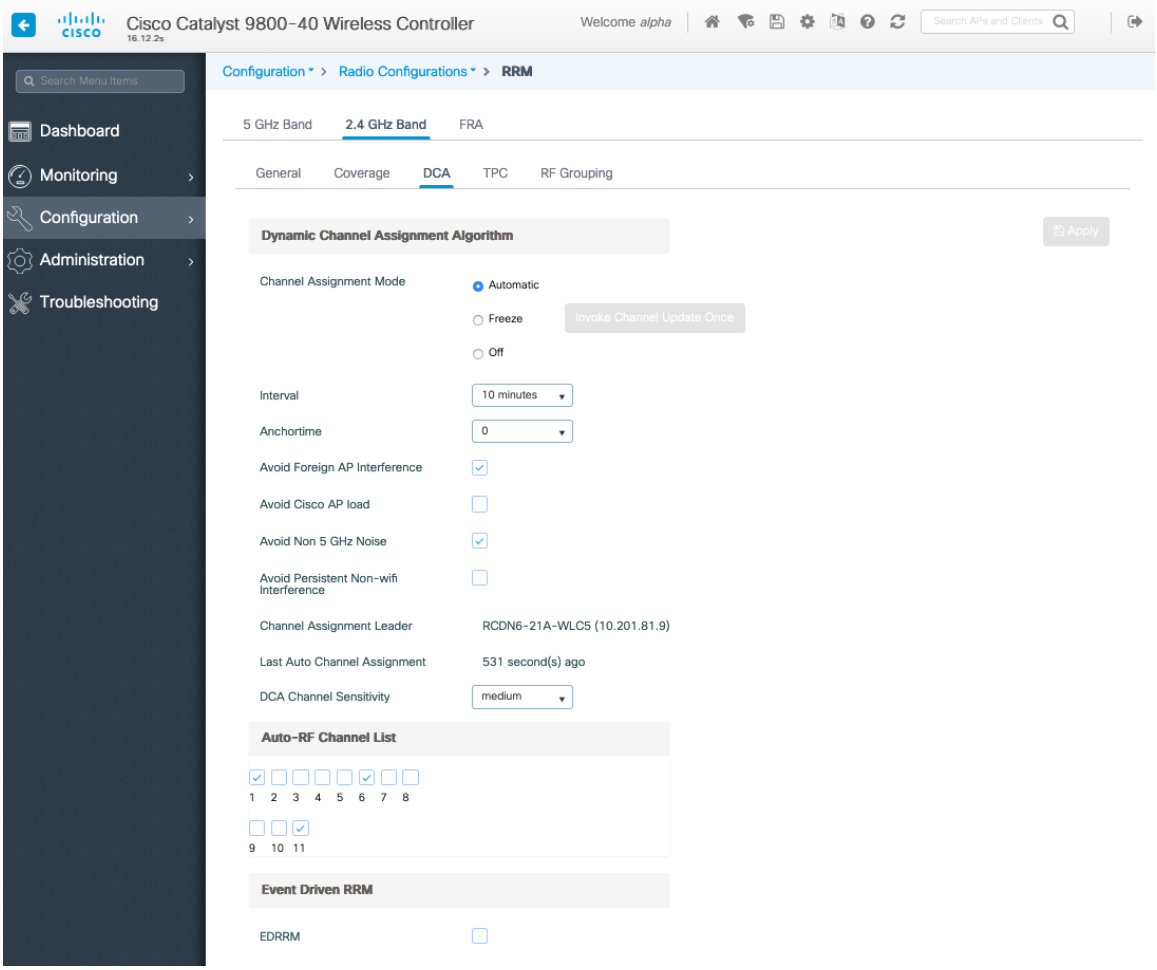
5 GHz を使用する場合は、多数のチャンネルをスキャンするために発生するアクセスポイント検出の遅延の可能性を回避するためにチャンネルの数を制限できます（例：12 チャンネルのみ）。

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、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。



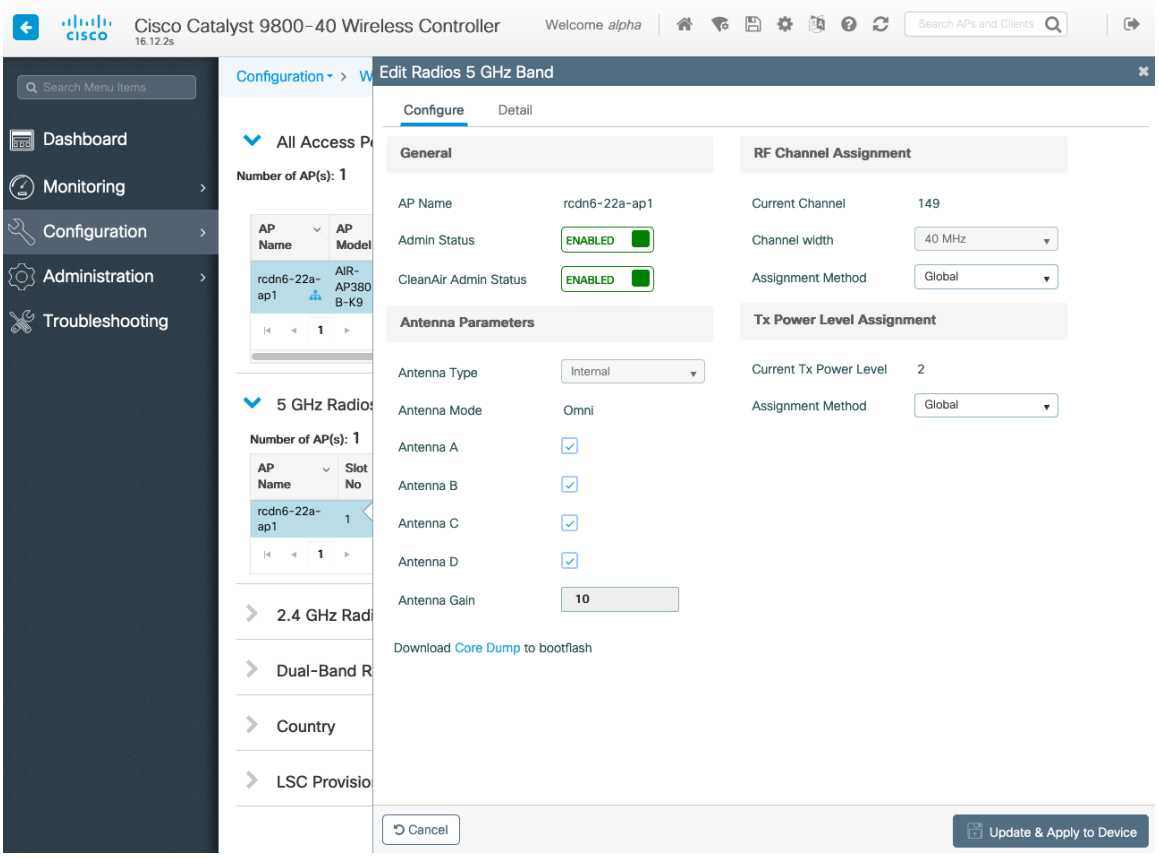
使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセス ポイントの設定をグローバル設定よりも優先させることができます。

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。

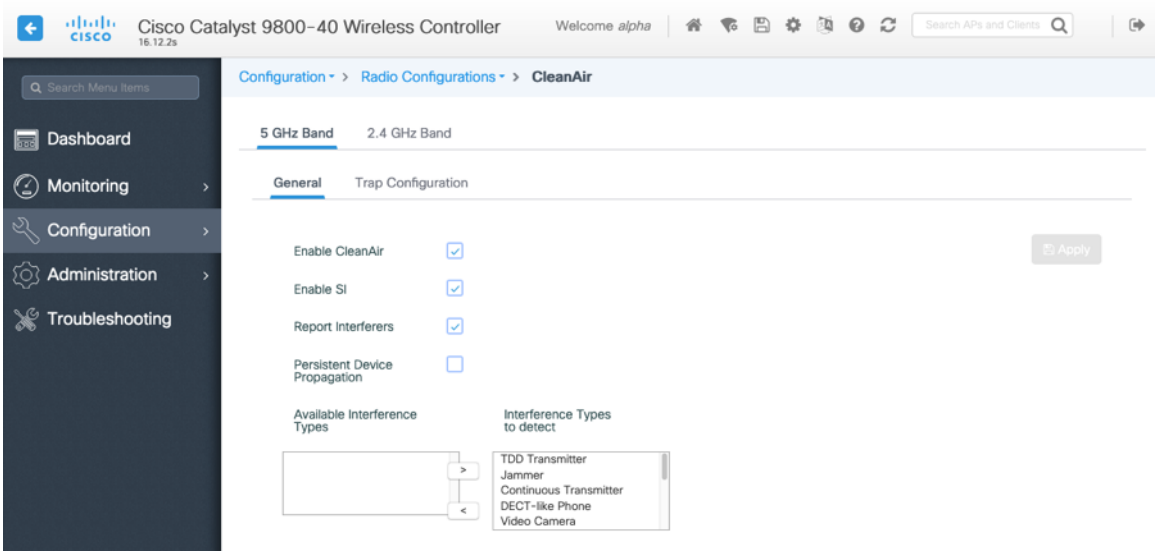
Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセス ポイントを使用している場合は 5 GHz チャネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。



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。



WLAN の設定

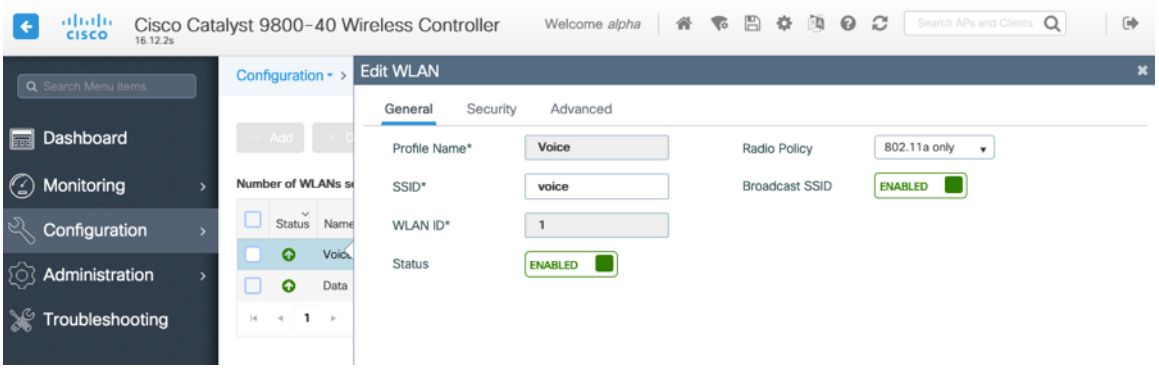
Webex Desk Series には別の SSID を使用することをお勧めします。

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。

Webex Desk Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように設定できます（802.11a のみなど）。

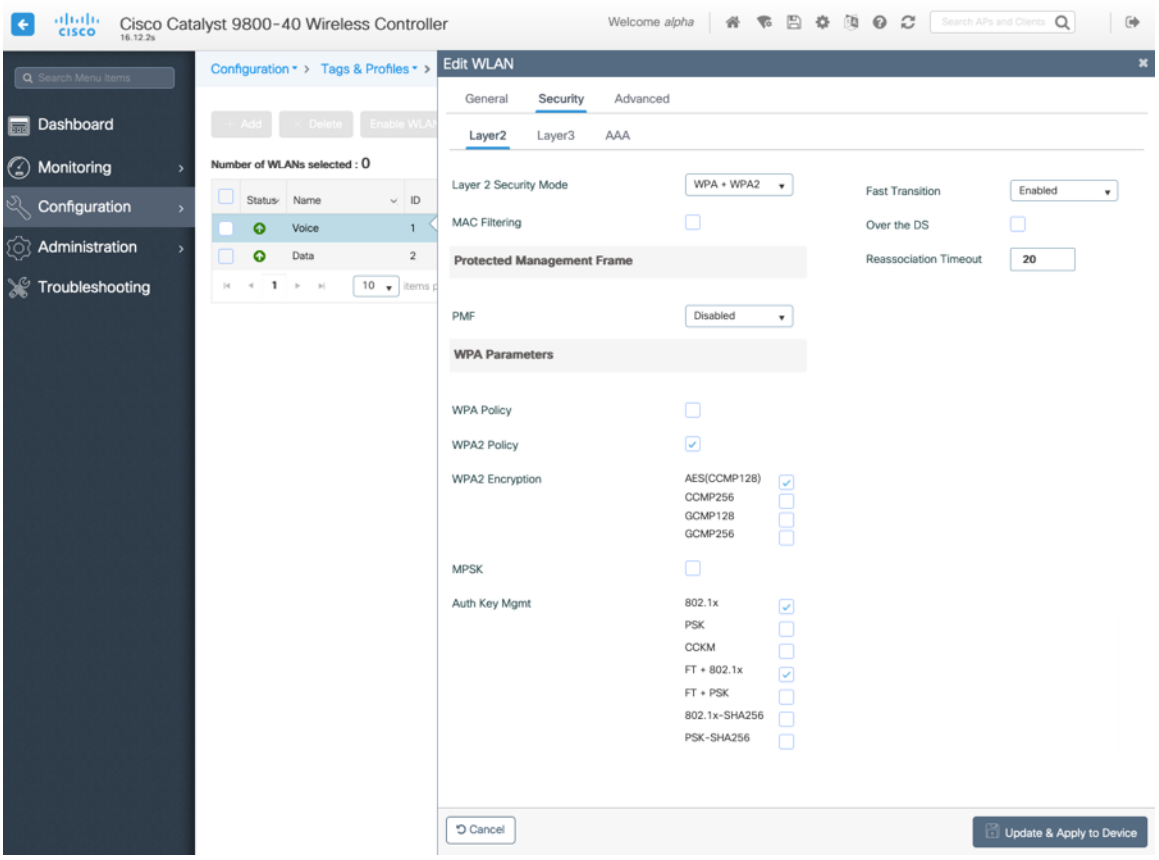
Webex Desk Series は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャンネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

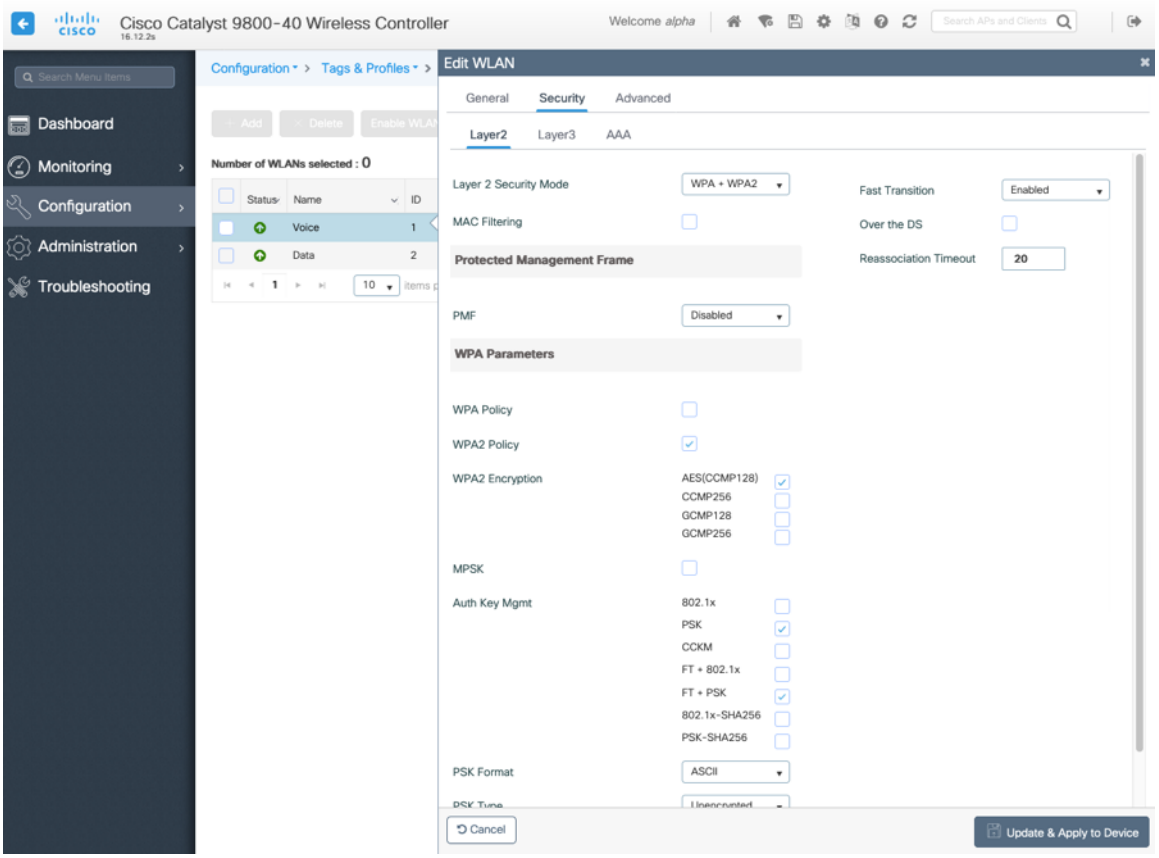
選択した SSID が他の LAN に使用されていないことを確認してください。使用されている場合で、特に異なるセキュリティ タイプを使用している場合は、電源の投入時またはローミング中に障害が発生する可能性があります。



[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。**

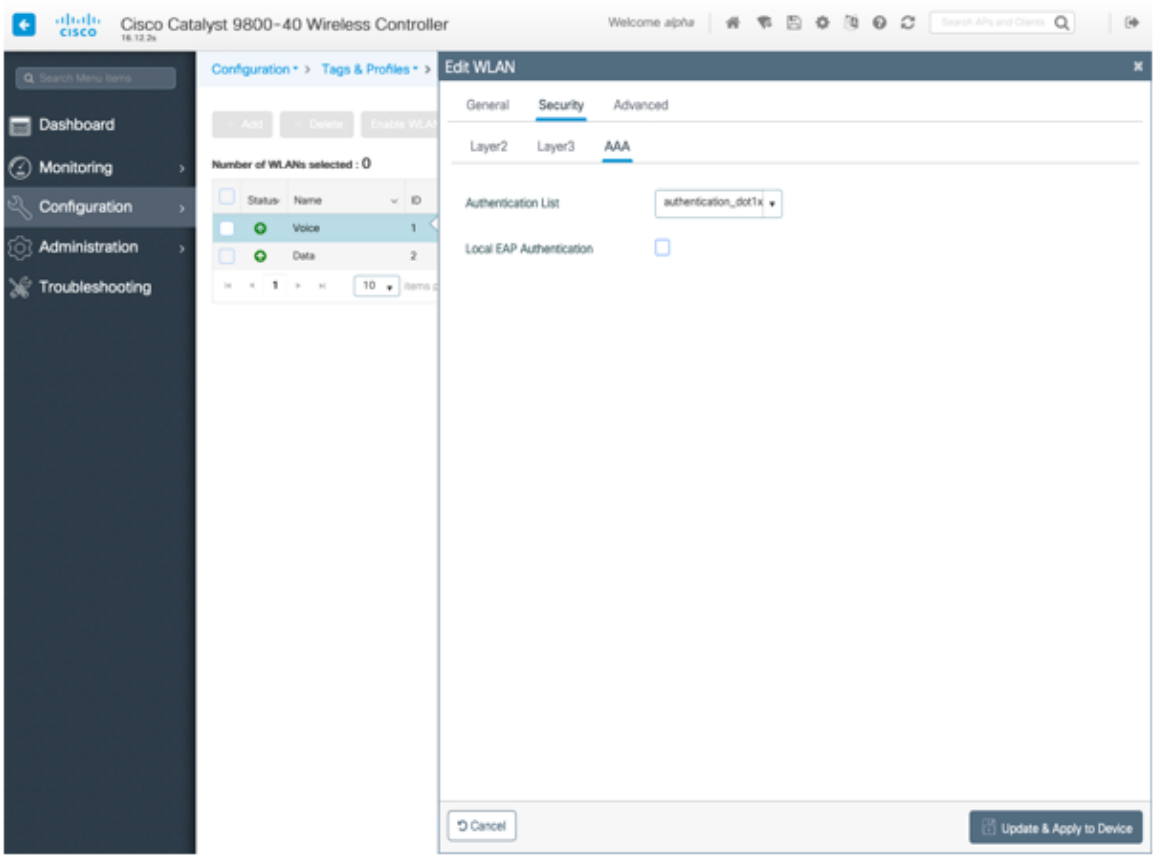
AES（CCMP128）暗号化を使用した WPA2 ポリシーを有効にします。その後、802.1x と PSK のどちらを使用するかに応じて、認証キー管理タイプとして 802.1x と PSK のどちらかを有効にします。


Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles >
Add
Delete
Number of WLANs selected : 0
Status
Name
ID
Voice
1
Data
2
10
Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
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
Fast Transition
Enabled
Over the DS
Reassociation Timeout
20
Cancel
Update & Apply to Device


Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles >
Add
Delete
Number of WLANs selected : 0
Status
Name
ID
Voice
1
Data
2
10
Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
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
Fast Transition
Enabled
Over the DS
Reassociation Timeout
20
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 や PSK を使用するかどうかに応じて、802.11r（FT）、CCKM、PSK も有効にできます。

802.1x を使用している場合は、RADIUS サーバーグループで定義された RADIUS サーバーにマップする AAA 認証リストを設定します。



[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（Disabled）] **にする必要があります。**

Webex Desk Series または他の WMM 対応電話機がこの SSID を使用する予定の場合にのみ、**[WMM ポリシー（WMM Policy）]** を **[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。

他の非 WMM クライアントが Webex Desk Series 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。

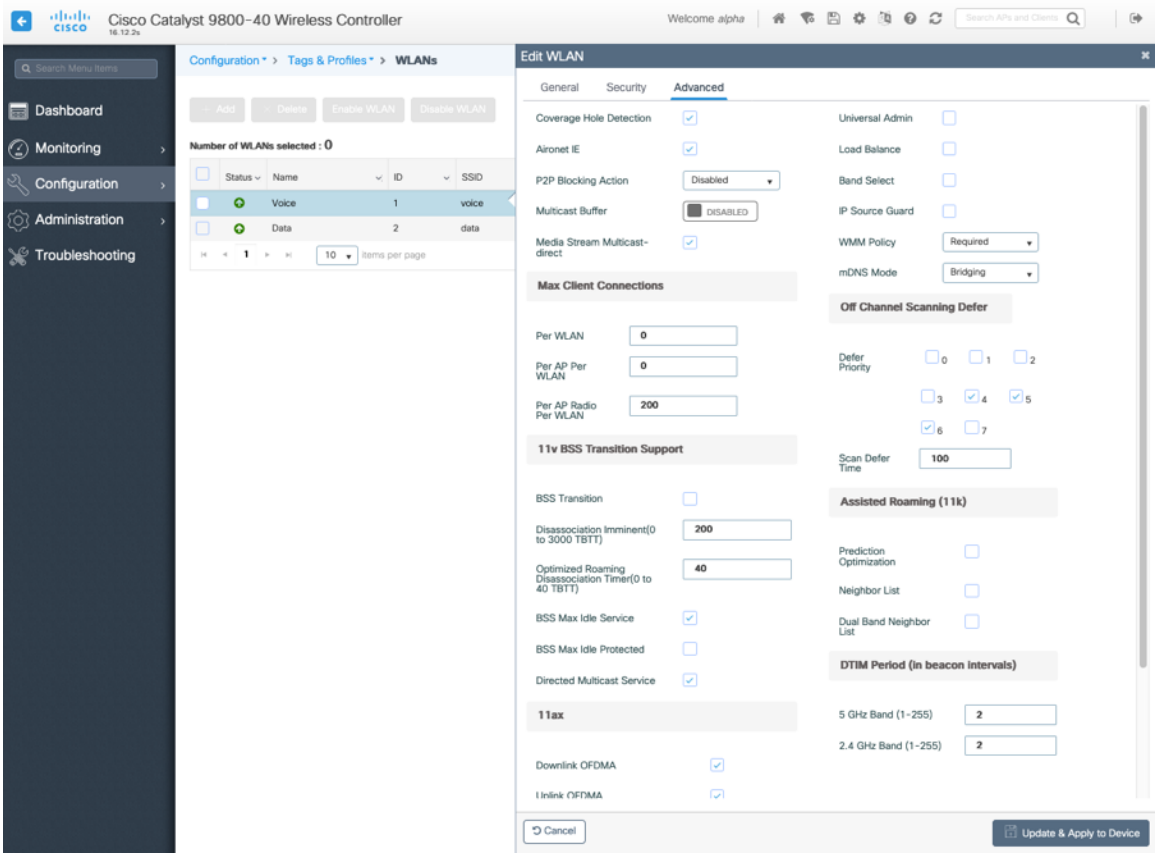
ベスト エフォート アプリケーションを頻繁に使用する場合、または優先順位の高いアプリケーション（音声、呼制御など）の DSCP 値がアクセスポイントに保持されていない場合は、優先順位の高いキュー（4 ~ 6）と共に優先順位の低いキュー（0 ~ 3）を有効にしてオフチャンネルスキャンを待機させるとともに、場合によってはスキャンの待機時間を長くすることを推奨します。

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 と 802.11v はサポートされていないため、無効にする必要があります。

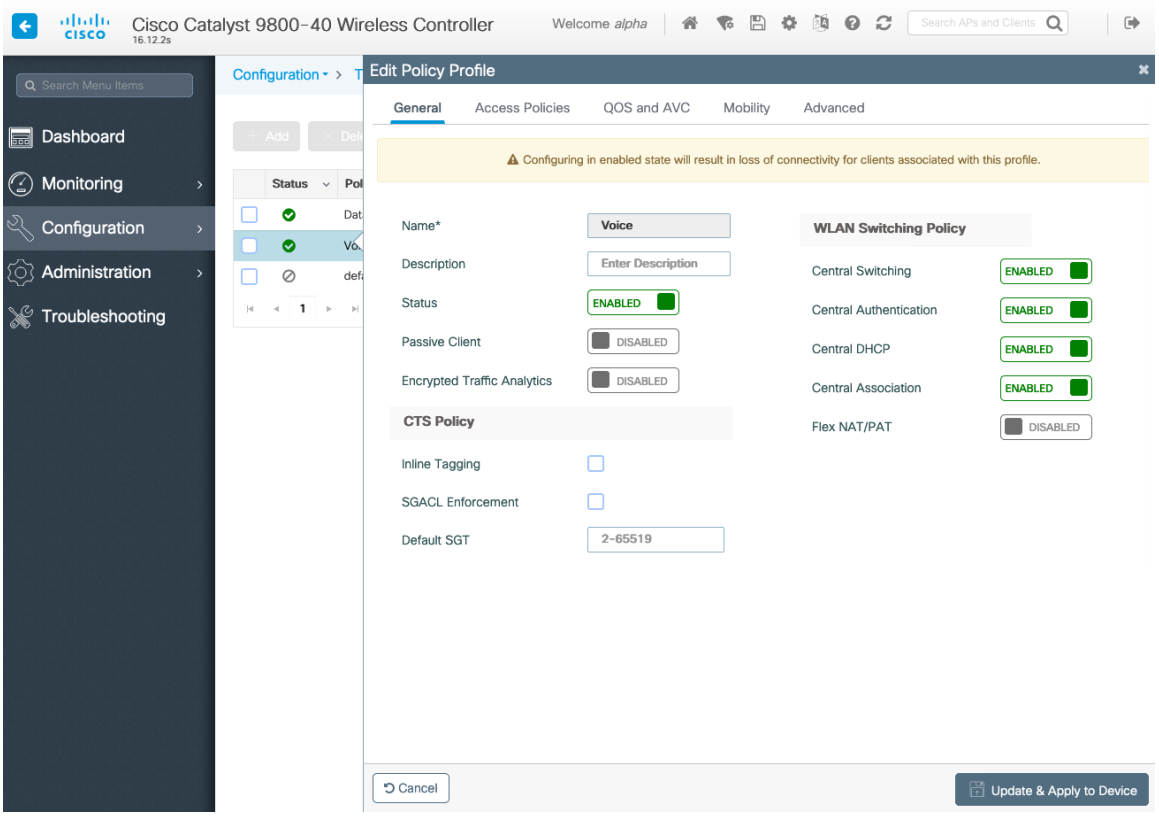


ポリシープロファイル

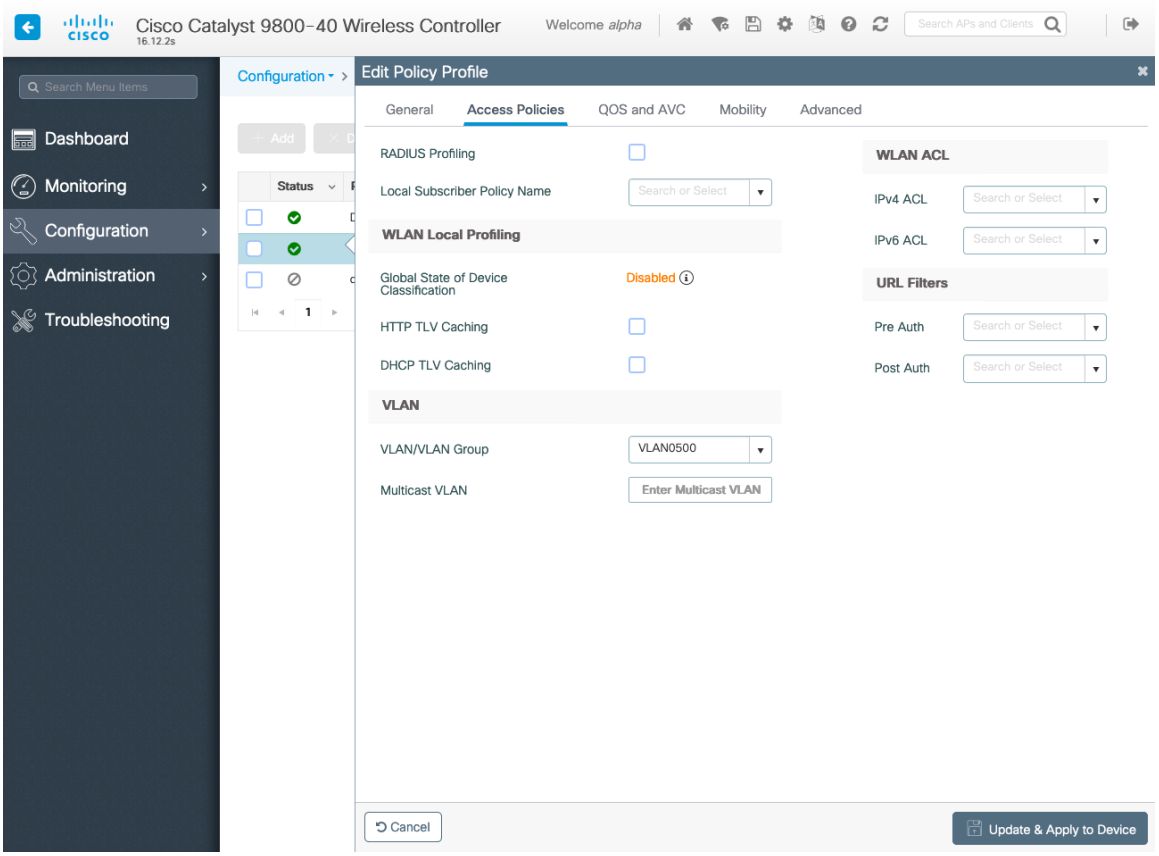
ポリシープロファイルは、アクセス、QoS、モビリティ、および詳細設定に関する追加設定を定義するために使用されます。

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。

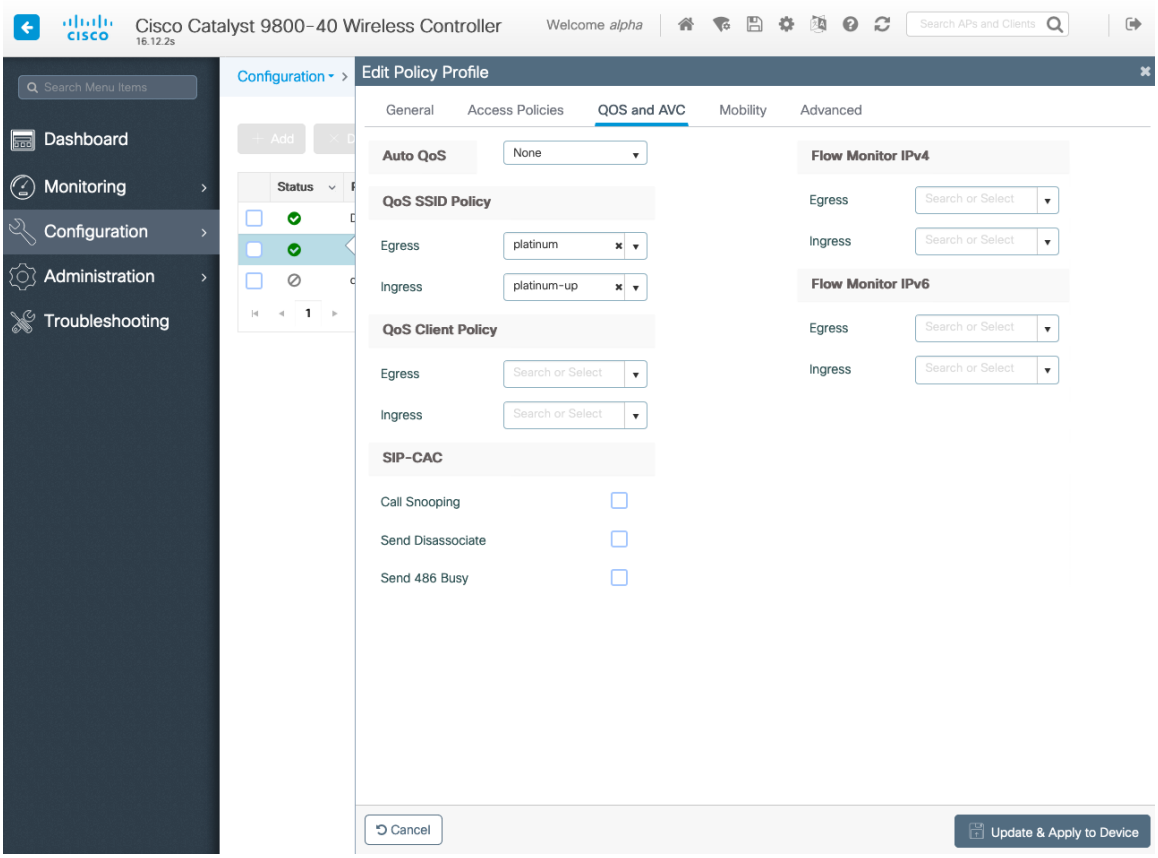
ポリシープロファイルの **[ステータス（Status）]** が **[有効（Enabled）]** になっていることを確認します。



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。



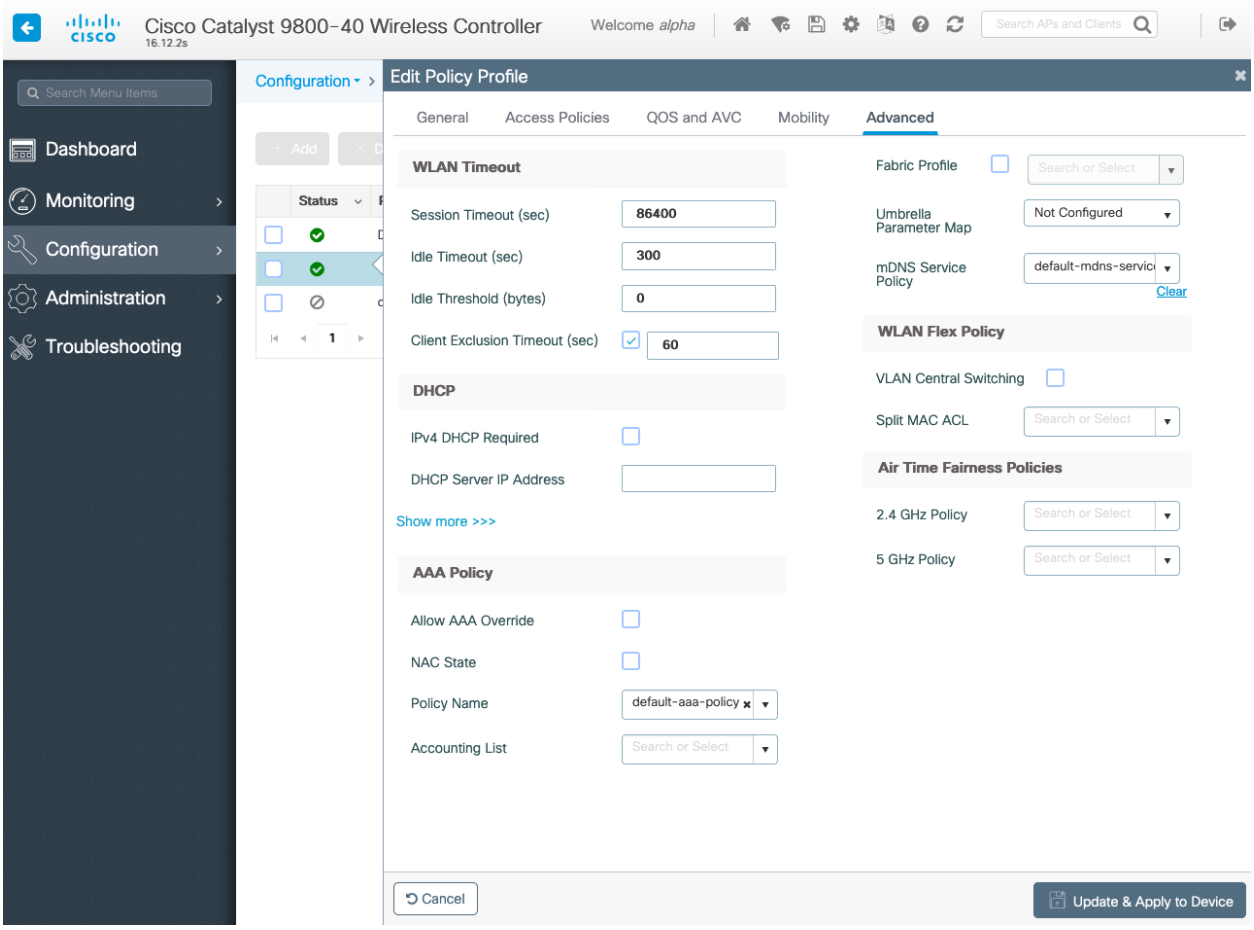
QoS SSID ポリシーが、出力の場合は **[プラチナ（Platinum）]** に、入力の場合は **[プラチナアップ（Platinum-up）]** に設定されていることを確認します。



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。**



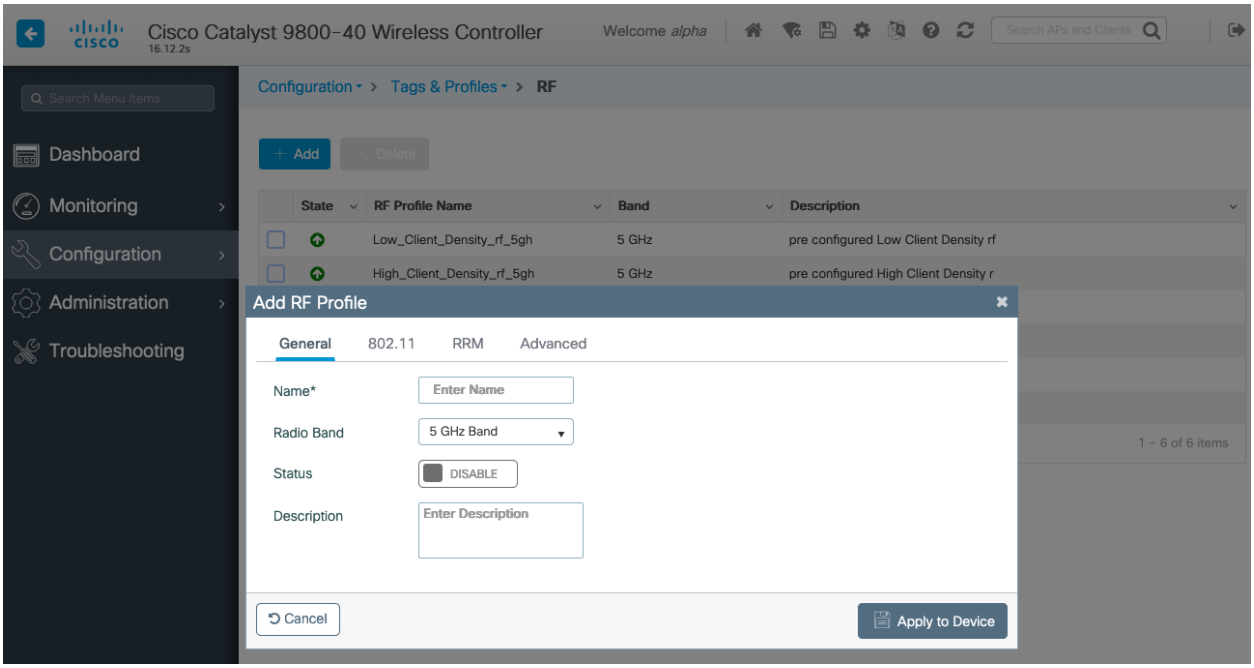
RF プロファイル

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。

Webex Desk Series 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。

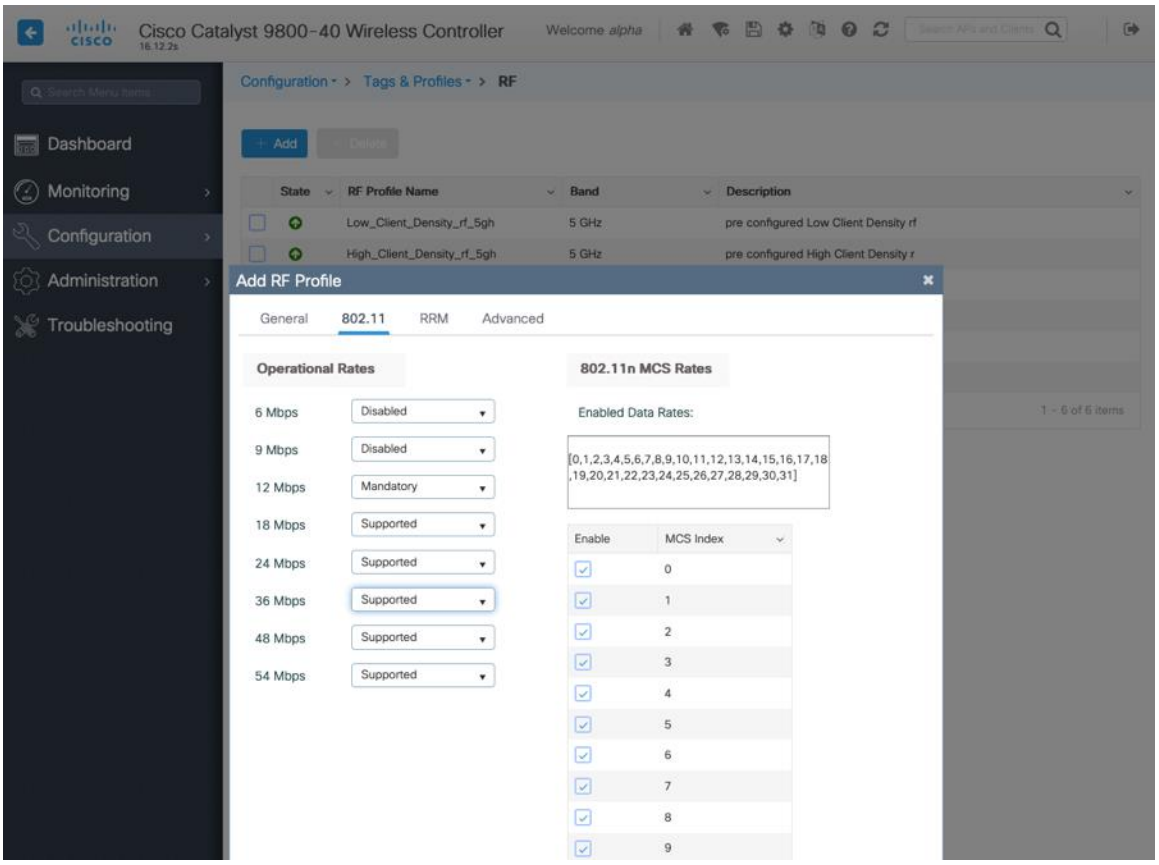
RF プロファイルは RF タグに適用され、アクセスポイントに適用できます。

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。

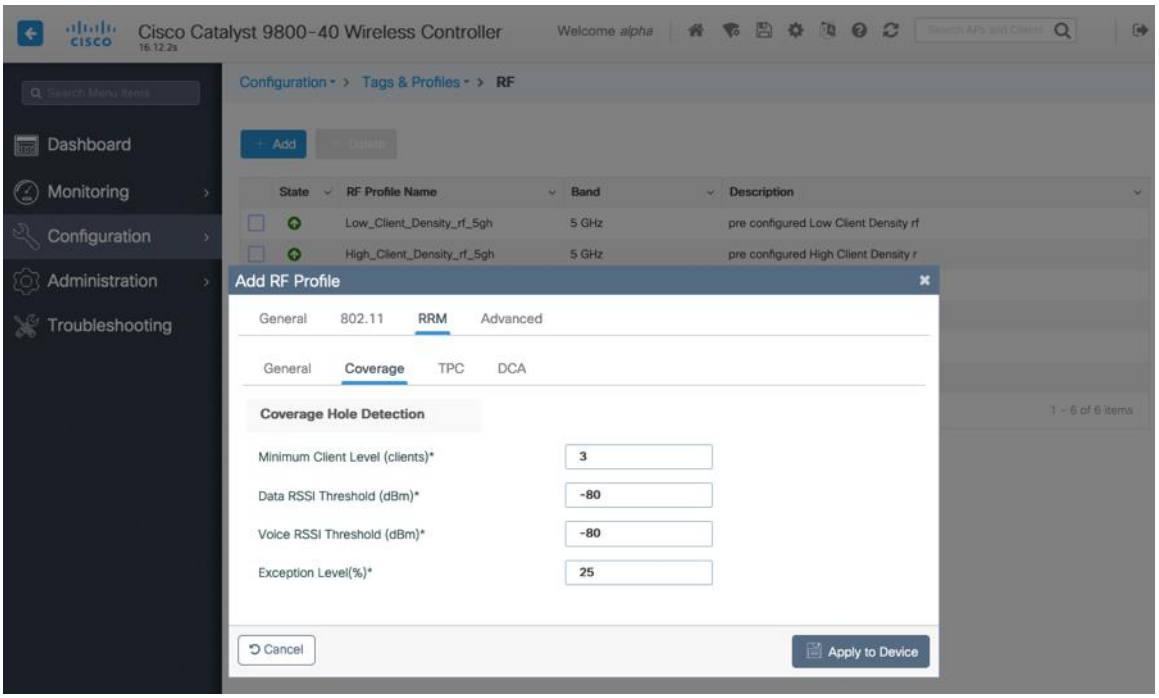


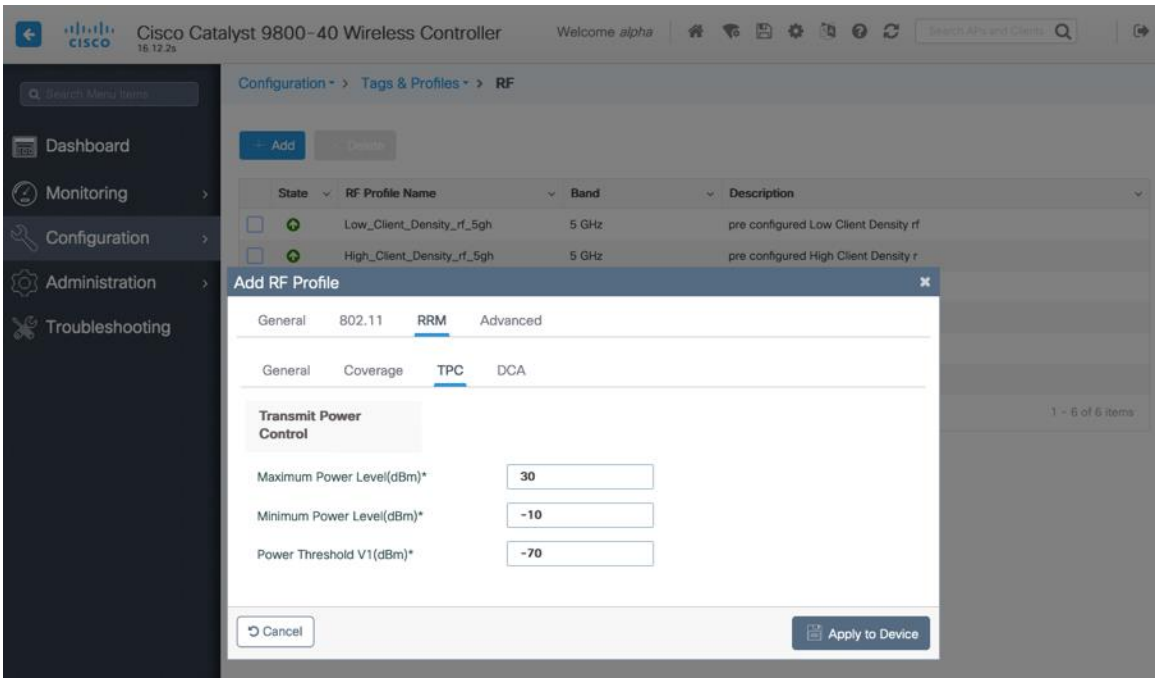
[802.11] タブで、必要に応じてデータレートを設定します。

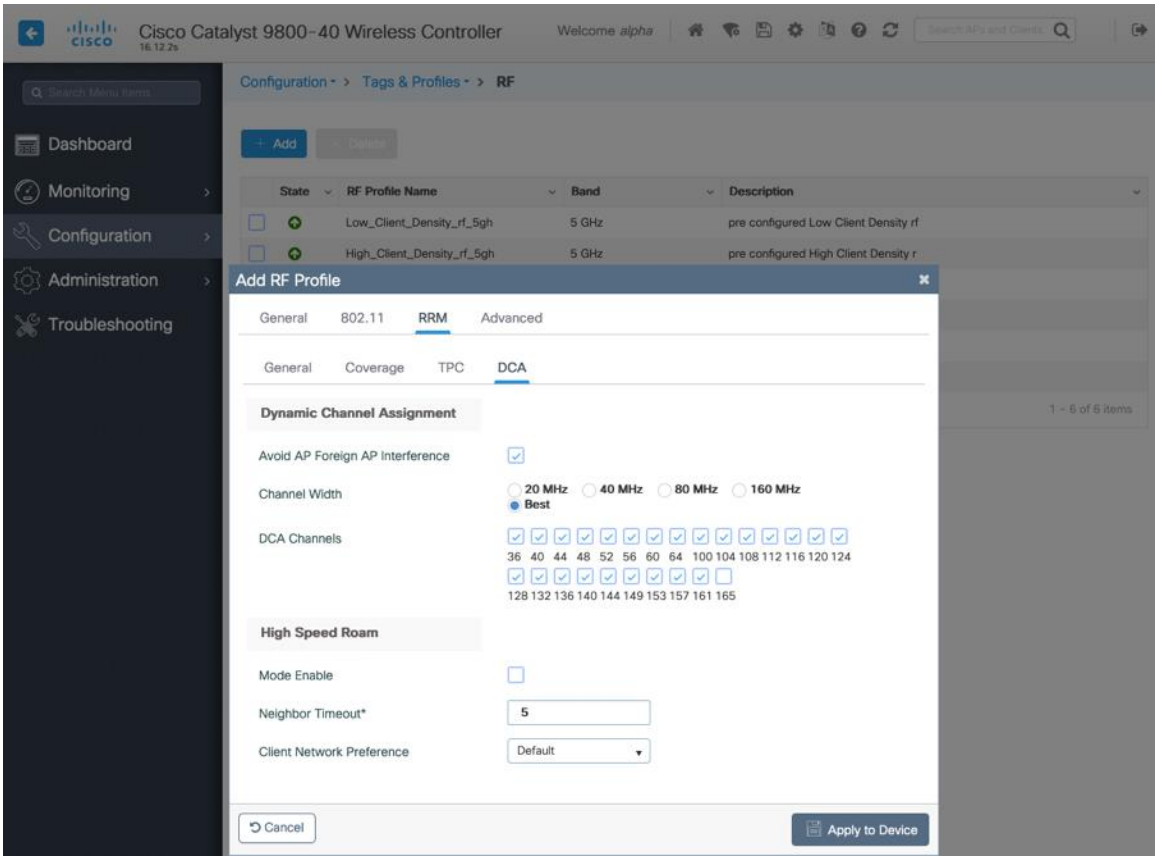
[必須（Mandatory）] として 12 Mbps を、**[サポート済み（Supported）]** として 18 Mbps 以上を有効にすることをお勧めします。ただし環境によっては、必須（基本）レートとして 6 Mbps を有効にする必要が生じます。



[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。

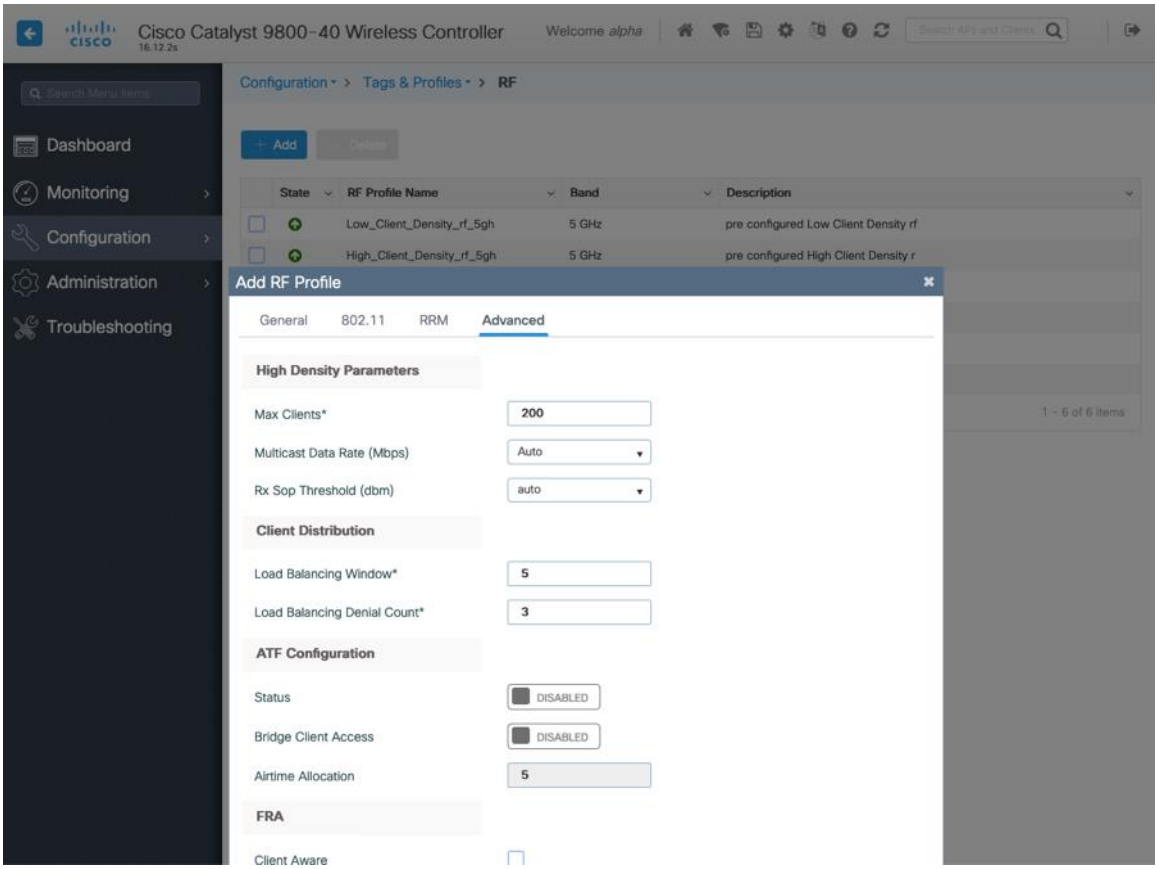






[詳細設定（Advanced）] **タブでは、**[最大クライアント数（Maximum Clients）] 、[マルチキャストデータレート（Multicast Data Rates）]、**および** [Rx Sop のしきい値（Rx Sop Threshold）] **を設定できます。**

[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

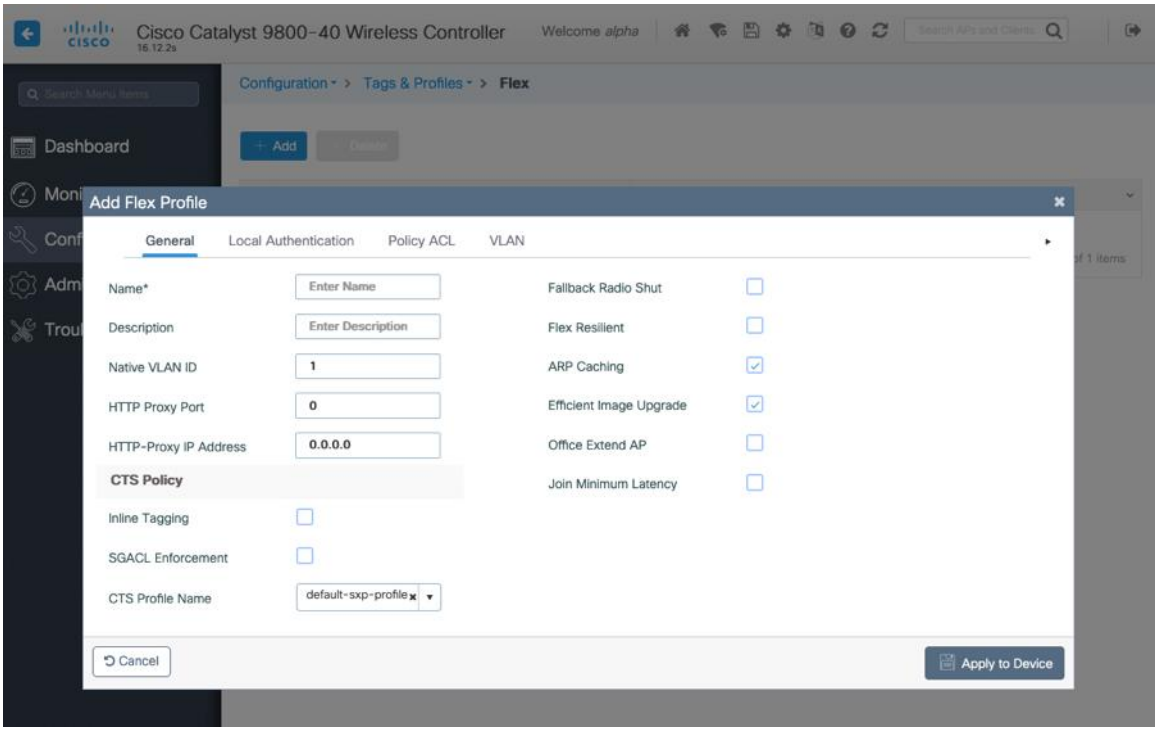
Flex プロファイルは、アクセスポイントが Flexconnect モードで使用する必要がある設定を定義するために使用されます。

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。

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。



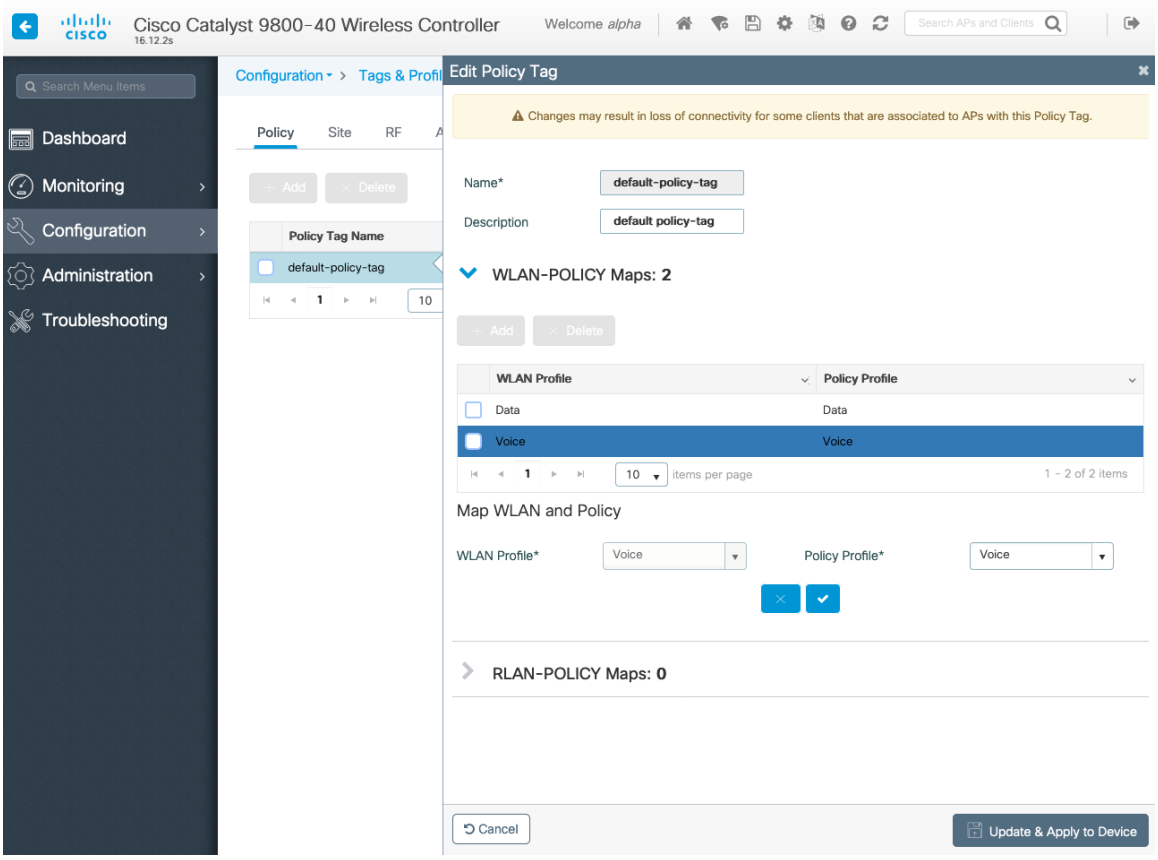
タグ

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。**



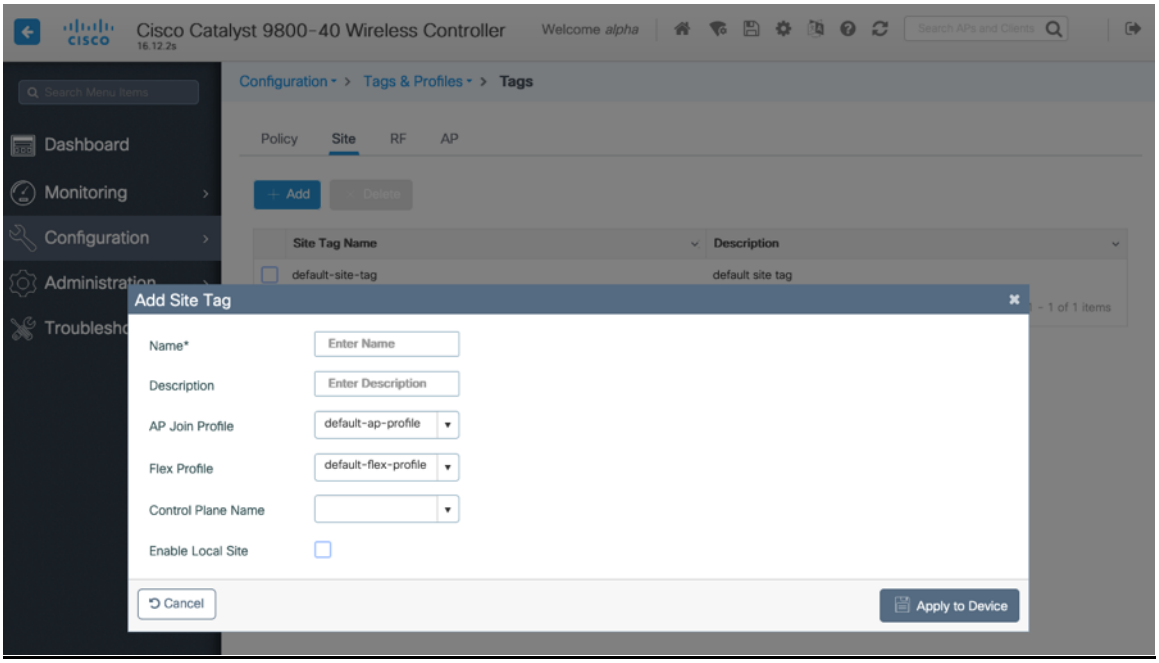
サイト タグ

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。

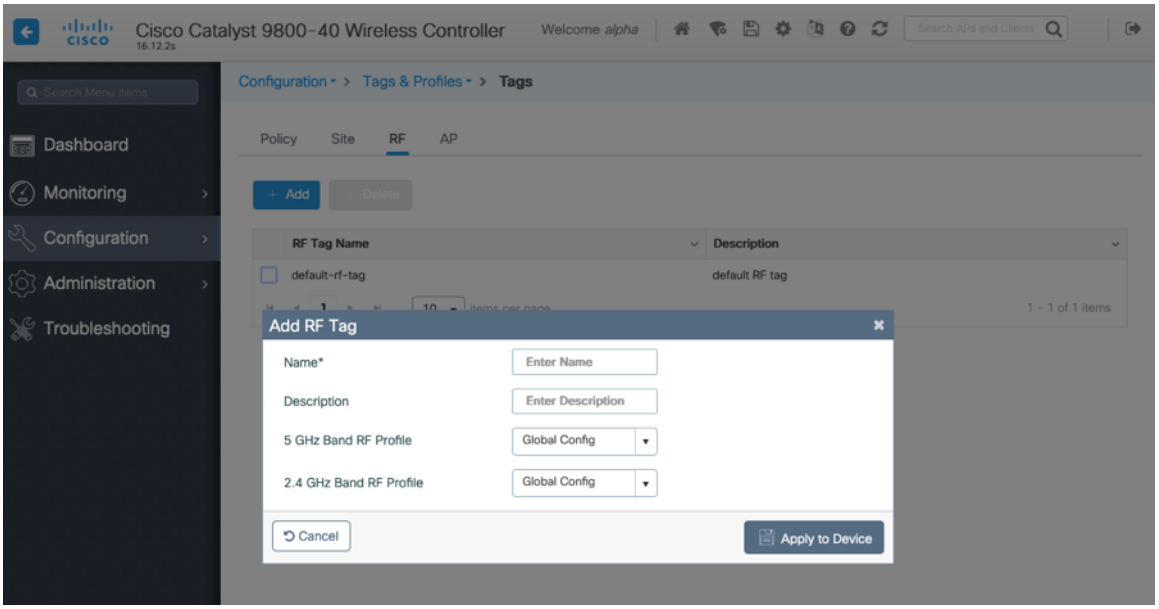


RF タグ

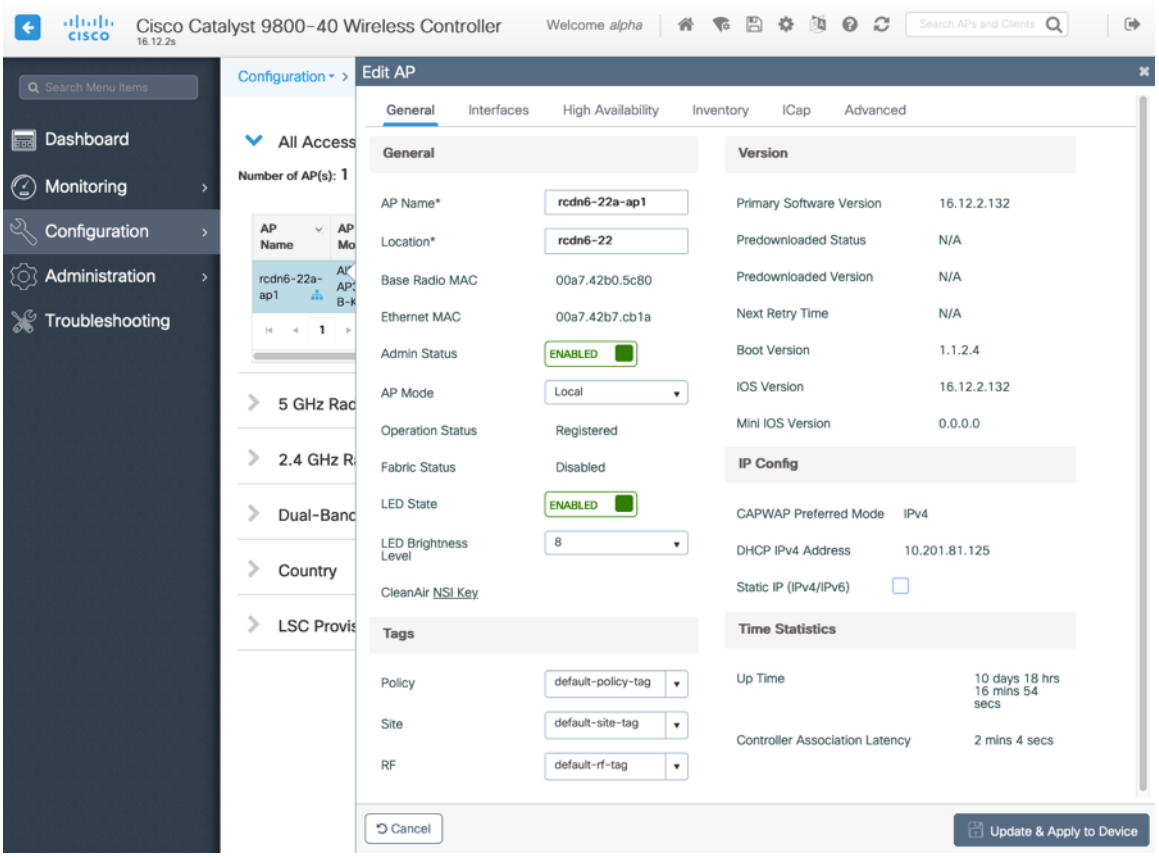
RF タグは、2.4 GHz および 5 GHz に使用する RF プロファイルを定義します。

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。

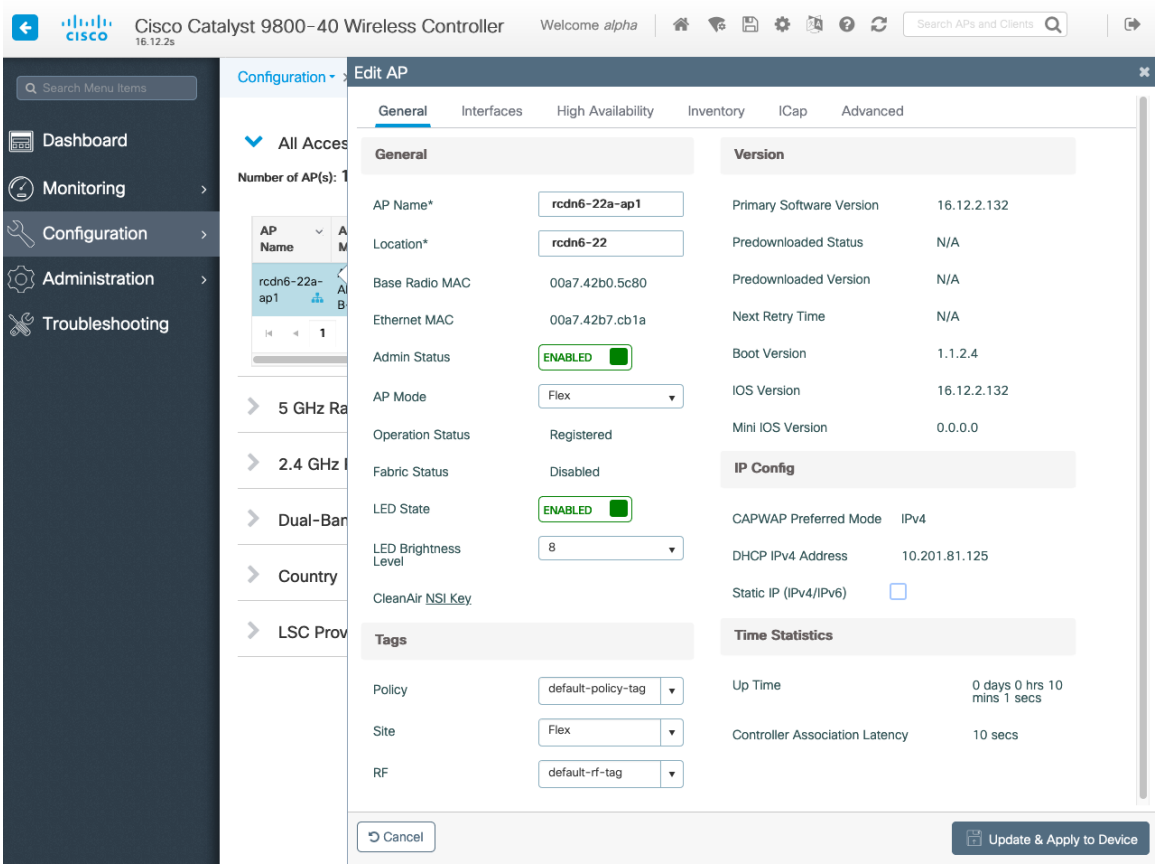
RF タグを作成する場合は、使用する **[5 GHz 帯域 RF プロファイル（5 GHz Band RF Profile）]** と **[2.4 GHz 帯域 RF プロファイル（2.4 GHz Band RF Profile）]** を選択します。



タグを定義したら、アクセスポイントに適用できます。



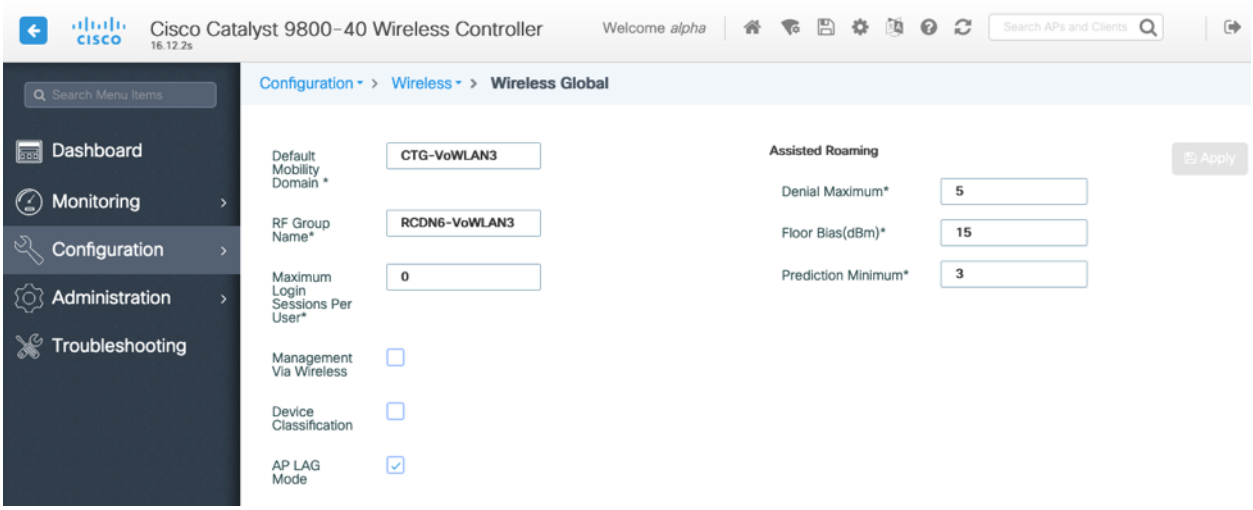
設定されたフレックスプロファイルを含むサイトタグが適用されている場合、**[AP モード（AP Mode）]** は自動的に **[フレックス（Flex）]**に変更されます。



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。

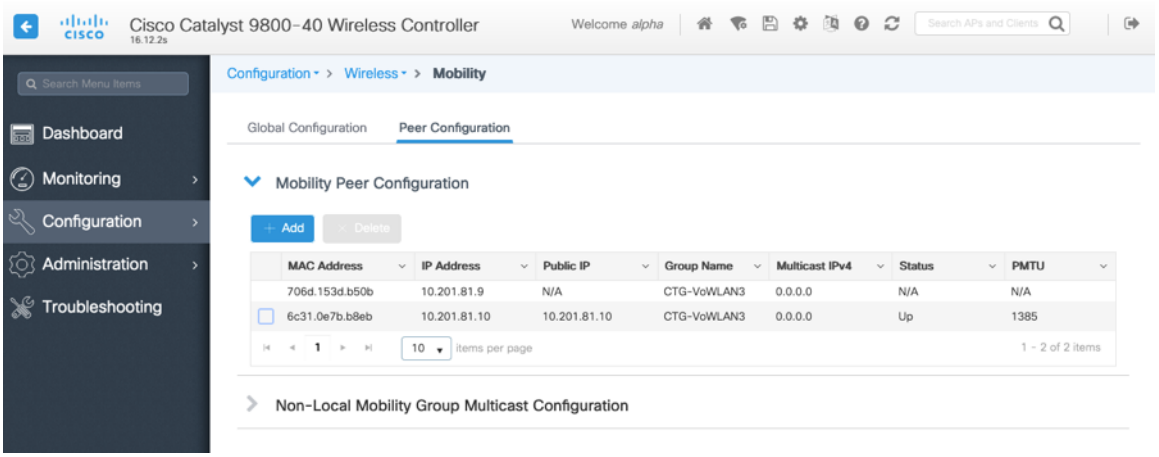
[AP LAG モード（AP LAG Mode）] を有効にします。



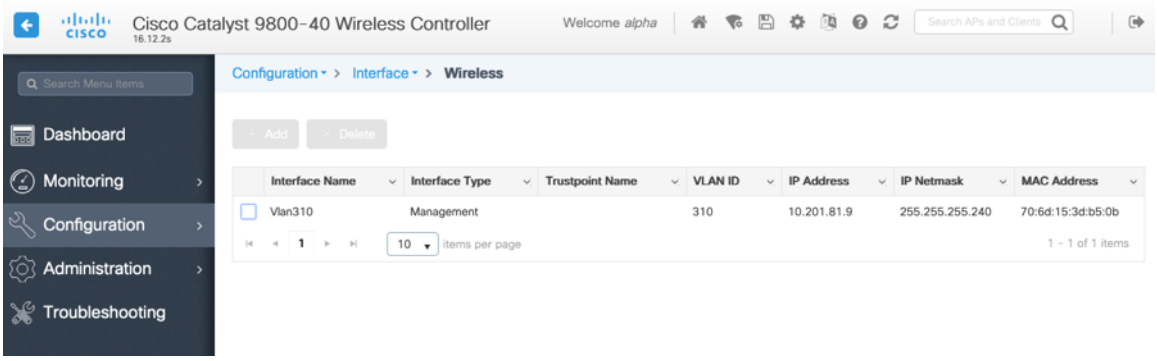
モビリティ設定

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。



[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。



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。

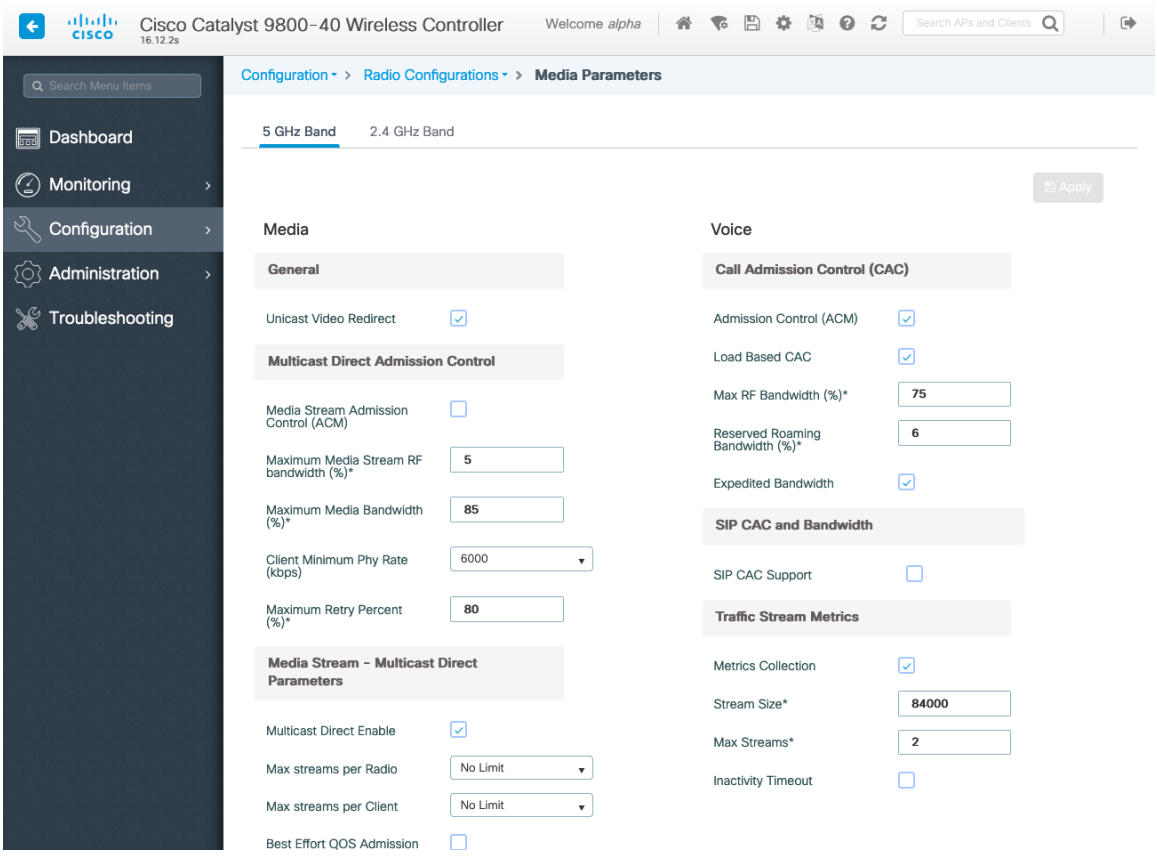
[ロードベース CAC（Load Based CAC）] **は、チャンネル上のすべての出力を考慮します。**

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。

SRTP 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。

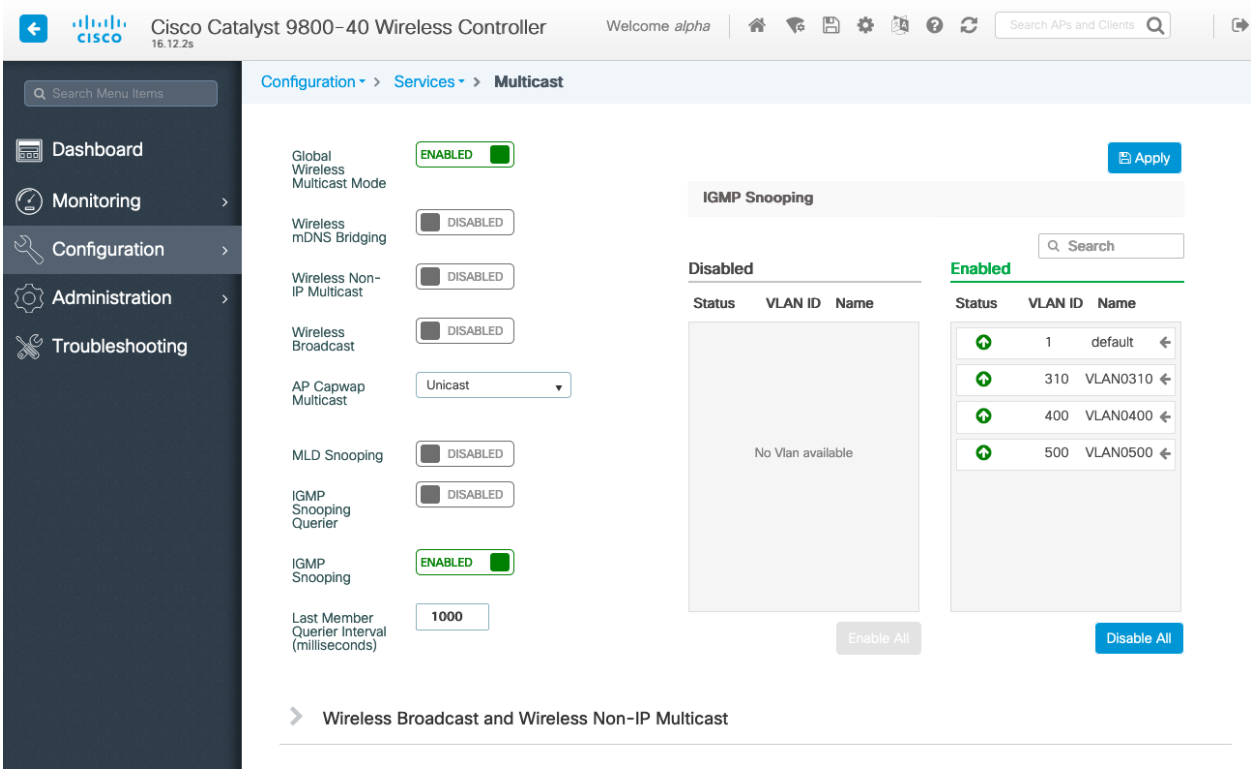
[非アクティブタイムアウト（Inactivity Timeout）] が無効になっていることを確認します。

[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。

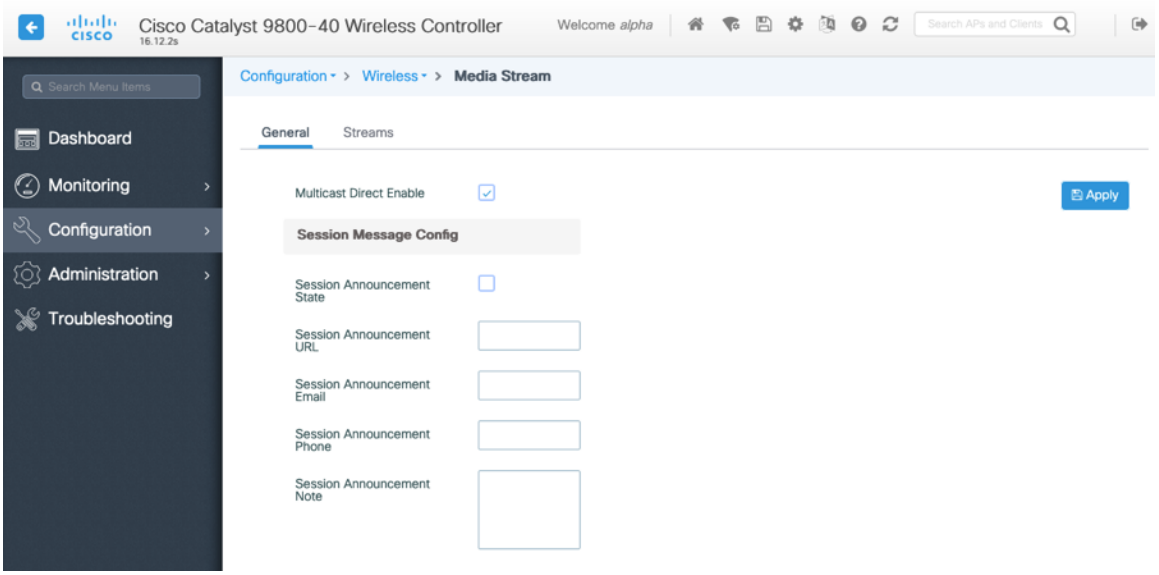


マルチキャスト

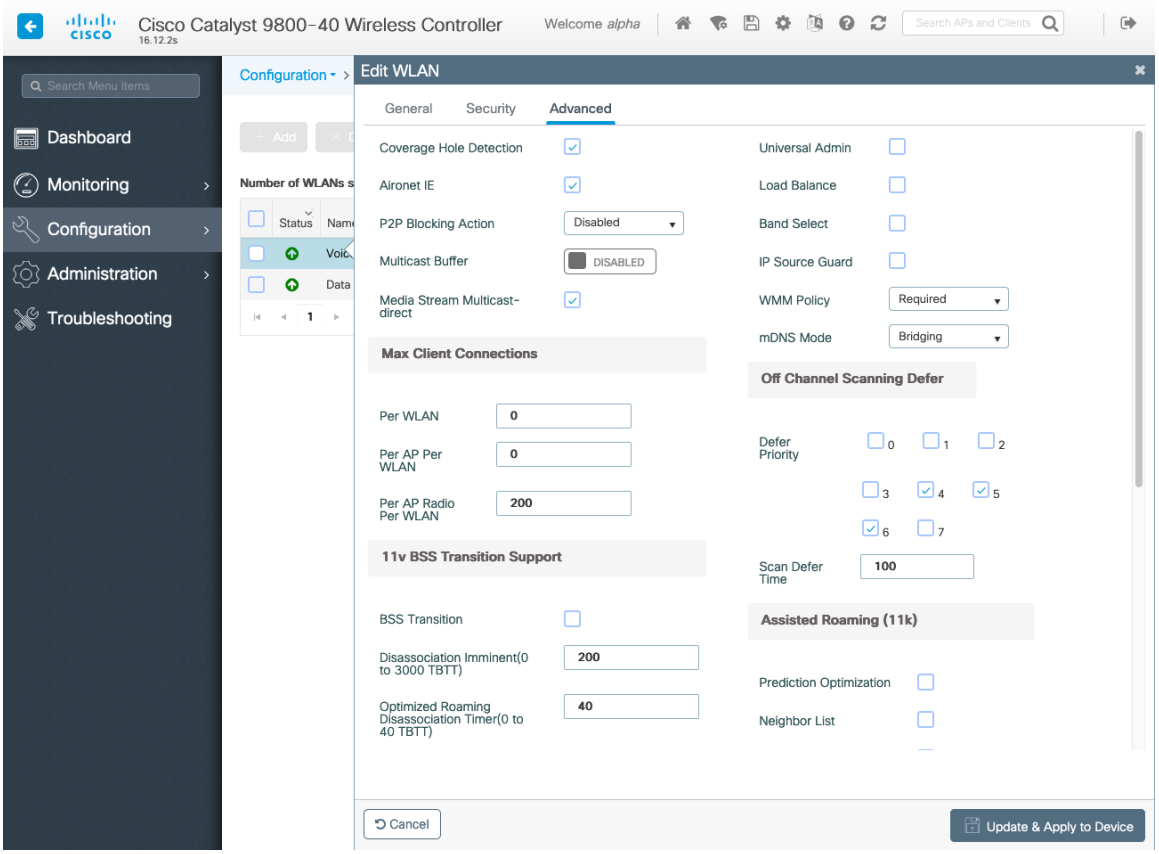
マルチキャストを使用する場合は、**[グローバル マルチキャスト モード（Global Multicast Mode）]** および **[IGMP スヌーピング（IGMP Snooping）]** を有効にする必要があります。



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。



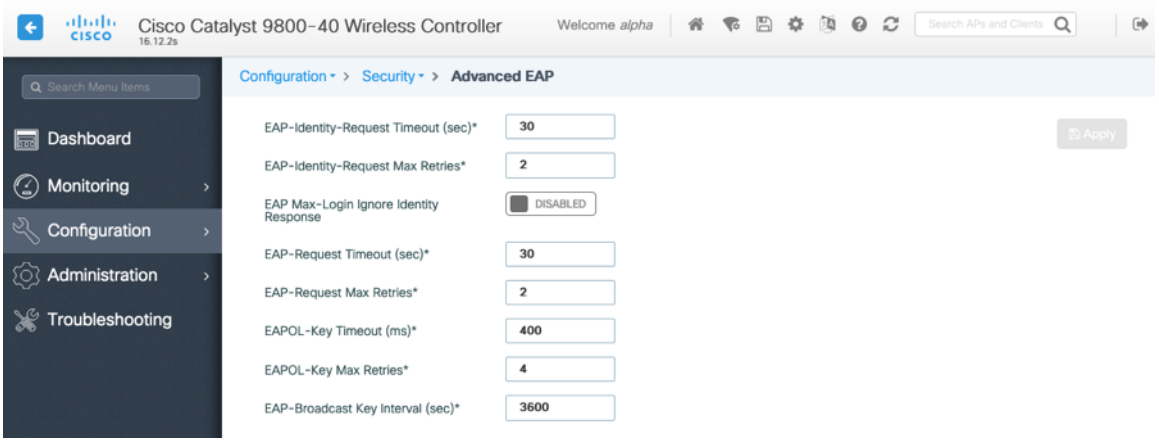
また、WLAN 設定で **[マルチキャストダイレクト（Multicast Direct）]** を有効にします。



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。**



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。

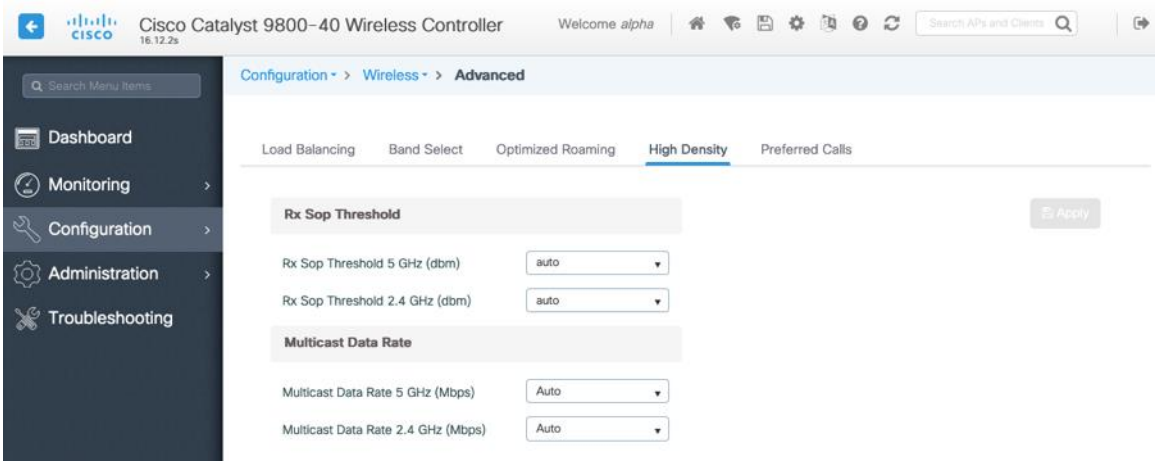
802.1x を使用する場合は、**[EAPOL キーのタイムアウト（EAPOL-Key Timeout）]** および **[EAPOL キーの最大試行回数（EAPOL-Key Max Retries）]** のデフォルト値（それぞれ 1000 ミリ秒および 2）を使用しても正しく動作しますが、それぞれ 400 および 4 に設定することを推奨します。

[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。

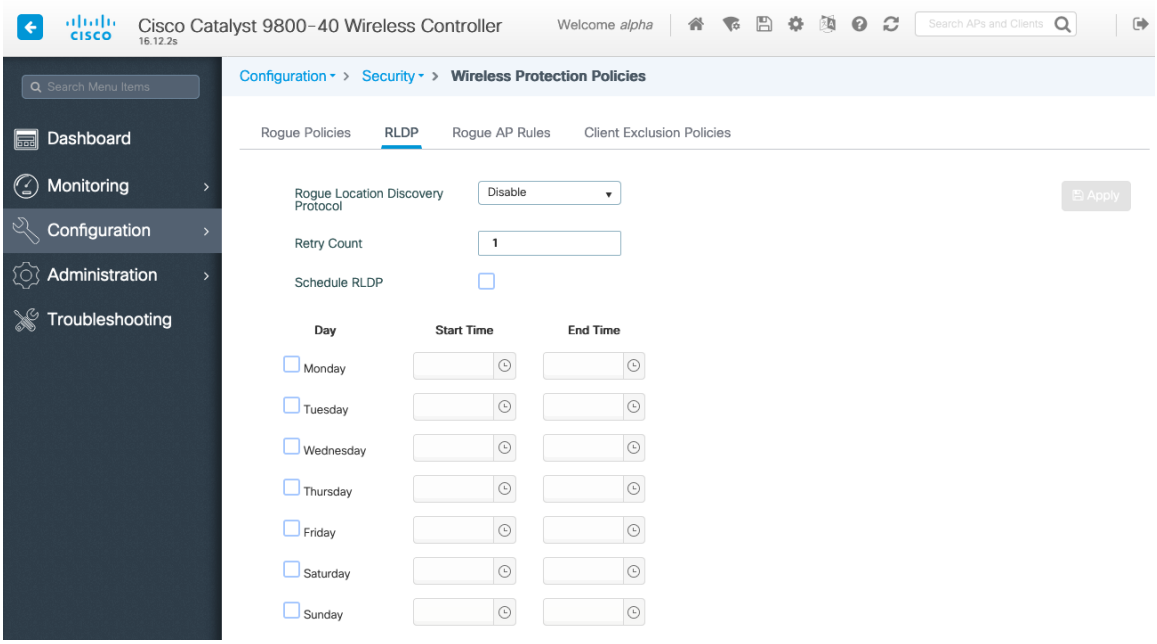
Rx SOP しきい値

[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。**



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。



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
 rsakeypair 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 EEBC7CF9 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

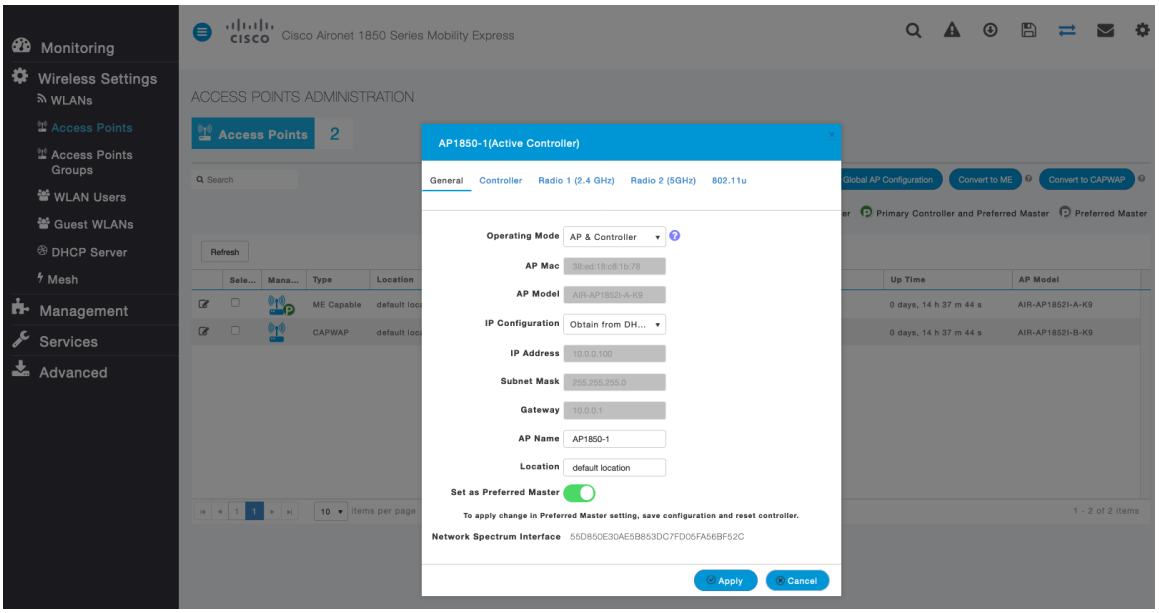
Cisco Mobility Express および Lightweight アクセスポイントを設定するときは、次のガイドラインを使用してください。

- **[802.11r（FT）]** と **[CCKM]** が必須として構成されていないことを確認します
- [Quality of Service（QoS）] **を** [プラチナ（Platinum）] **に設定します**
- **[802.11k]** が **[無効（Disabled）]** になっていることを確認します
- **[802.11v]** が **[無効（Disabled）]** になっていることを確認します
- [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

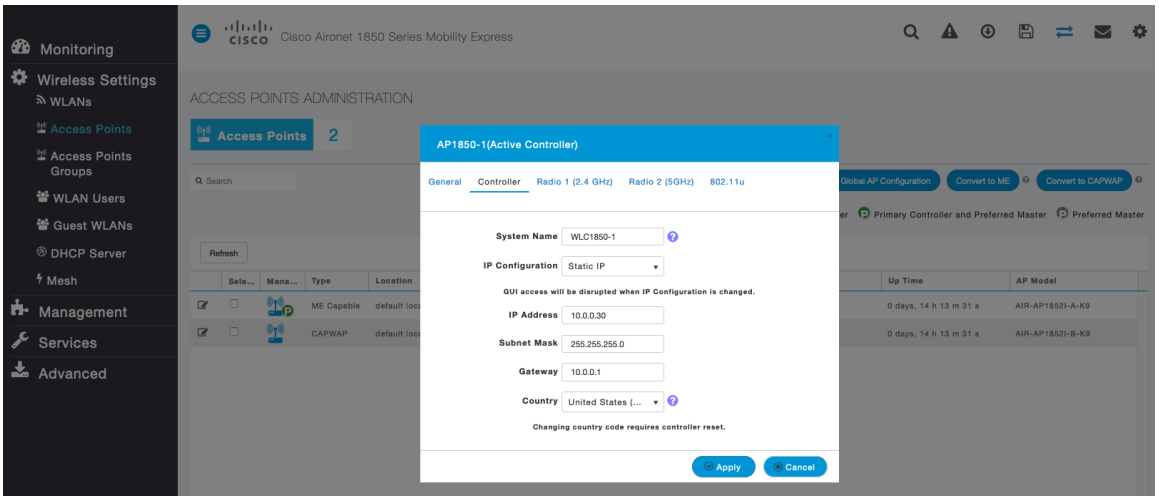
コントローラの設定

[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

Webex Desk Series 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。

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。

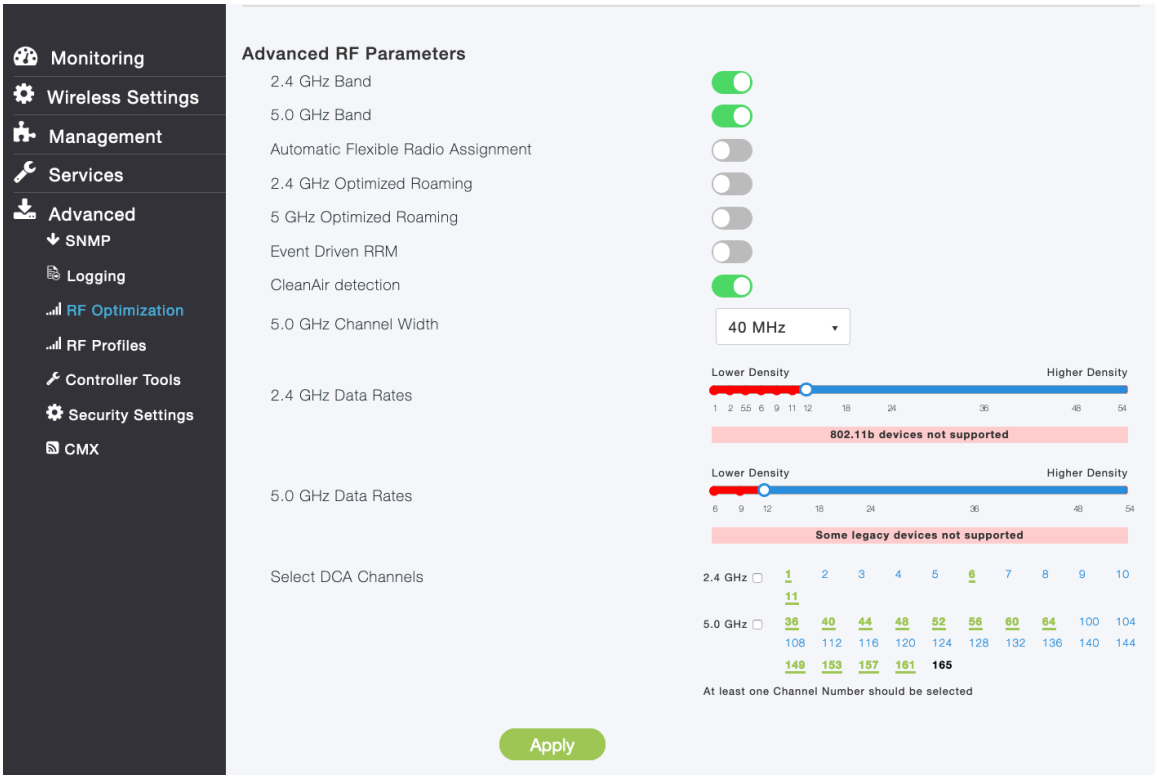
5 GHz を使用する場合は、多数のチャンネルをスキャンするために発生するアクセスポイント検出の遅延の可能性を回避するためにチャンネルの数を制限できます（例：12 チャンネルのみ）。

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。

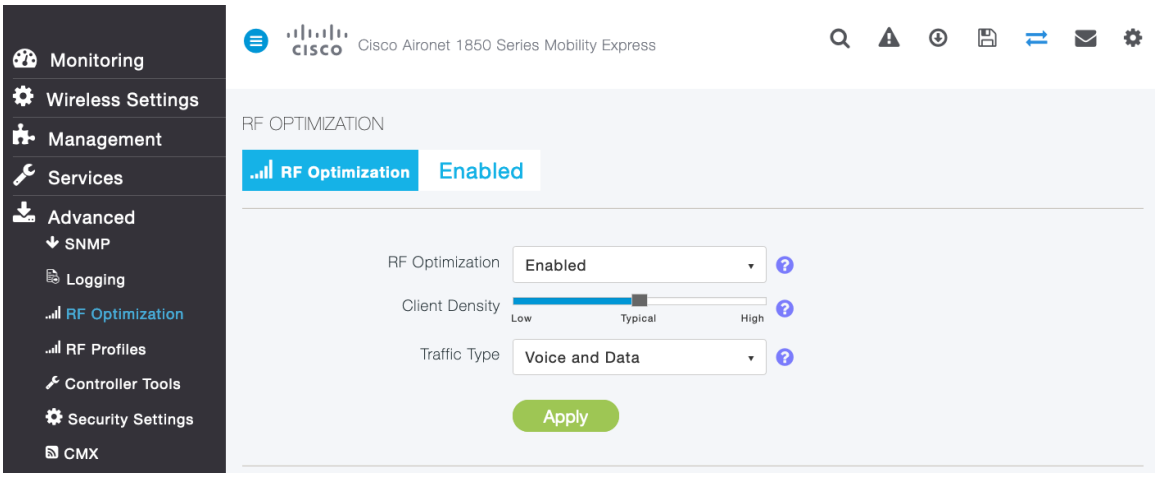
2.4 GHz を使用する場合、DCA リストではチャネル 1、6、および 11 だけを有効にします。

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。



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。



使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャ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。

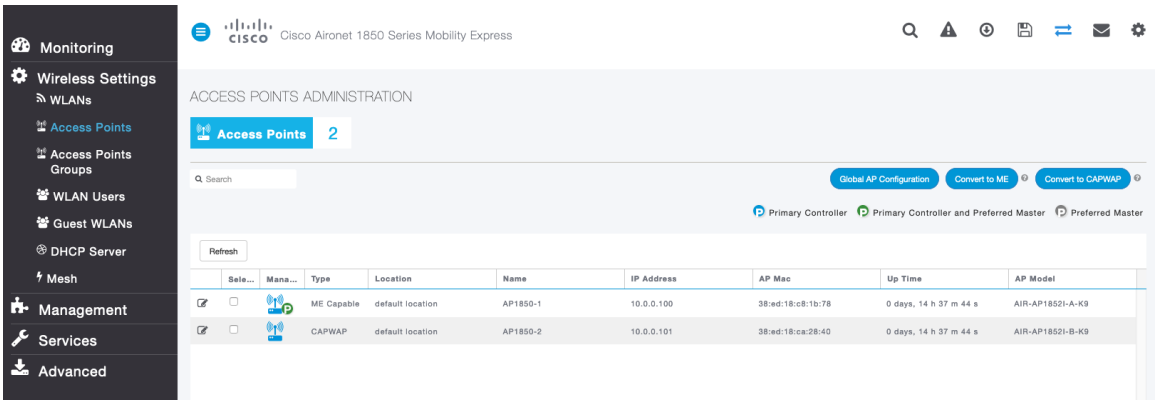
その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

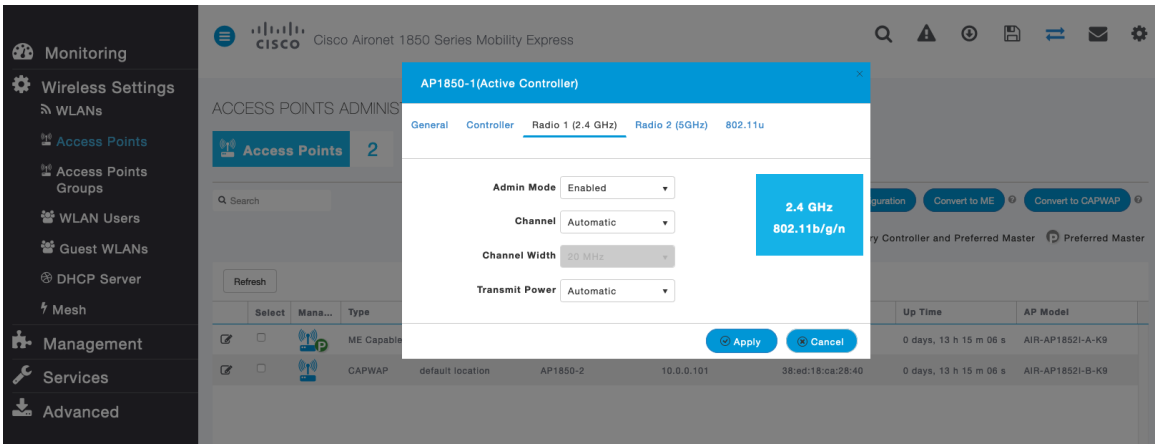
この設定は、エリア内に断続的な干渉が存在する場合に必要です。

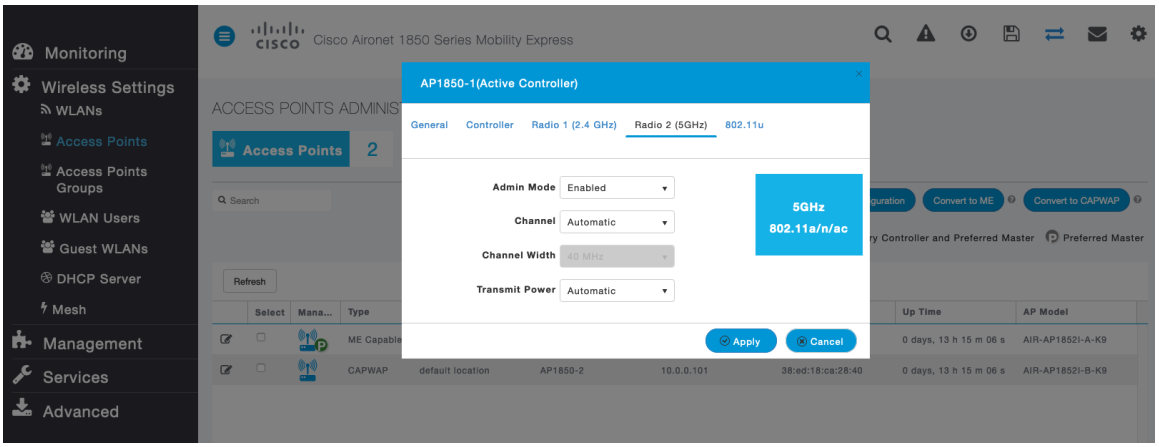
Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセス ポイントを使用している場合は 5 GHz チャネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

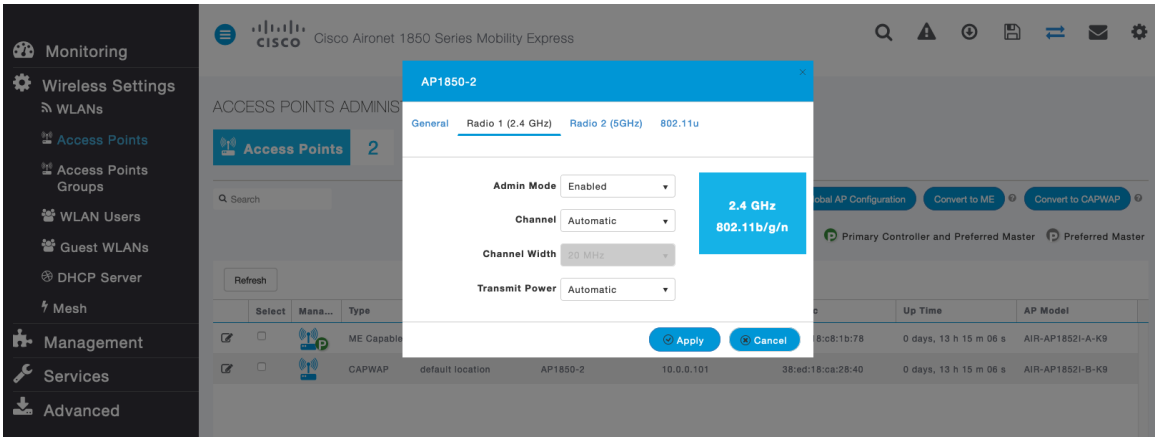
チャネル ボンディングは、5 GHz を使用する場合にのみ使用することをお勧めします。

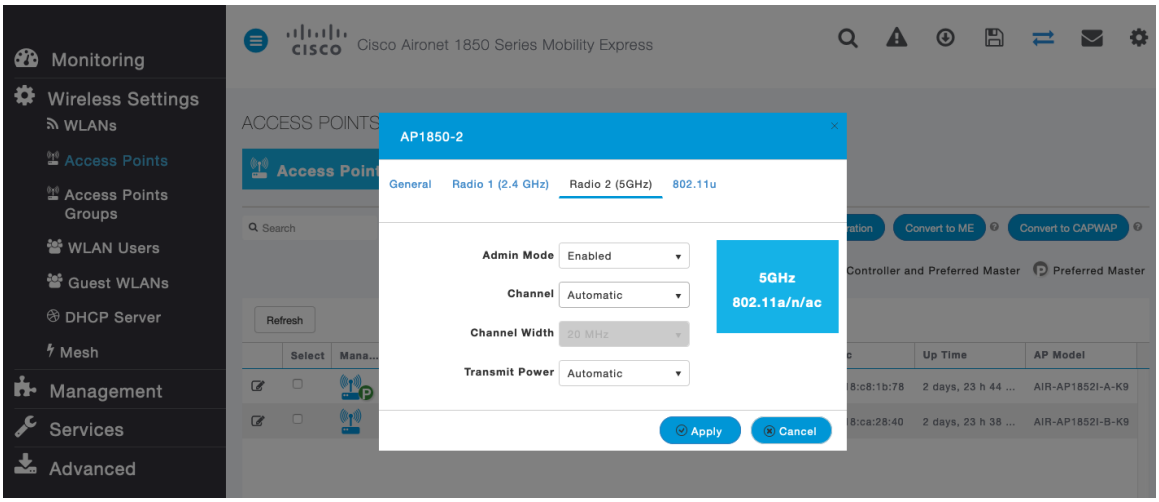
すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。











WLAN の設定

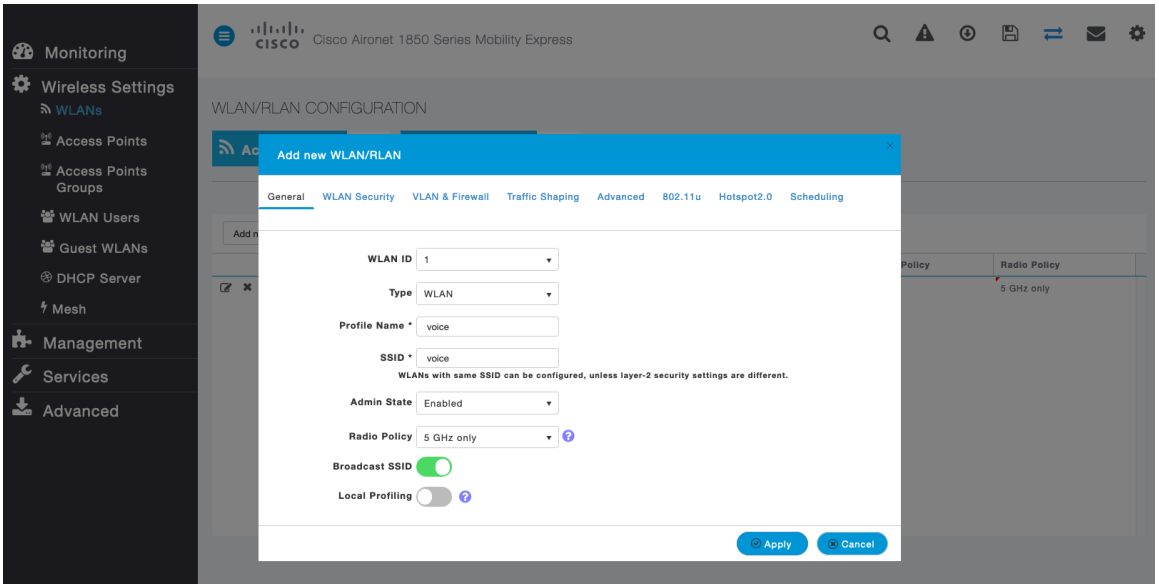
Webex Desk Series には別の SSID を使用することをお勧めします。

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。

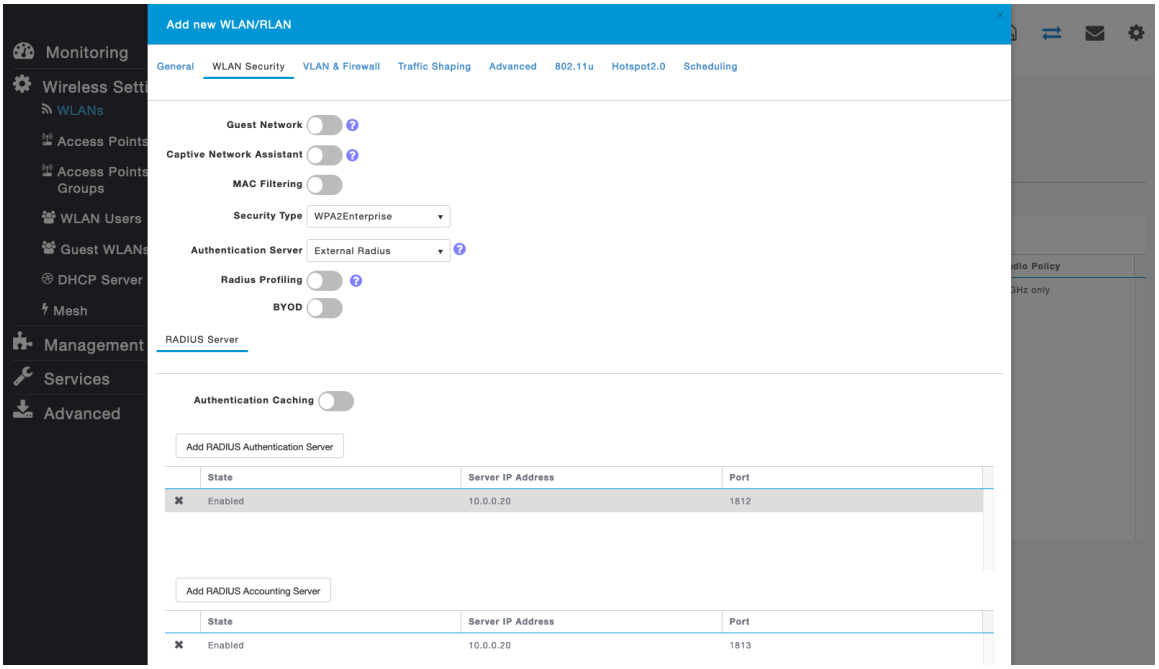
Webex Desk Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように設定できます（5 GHz のみなど）。

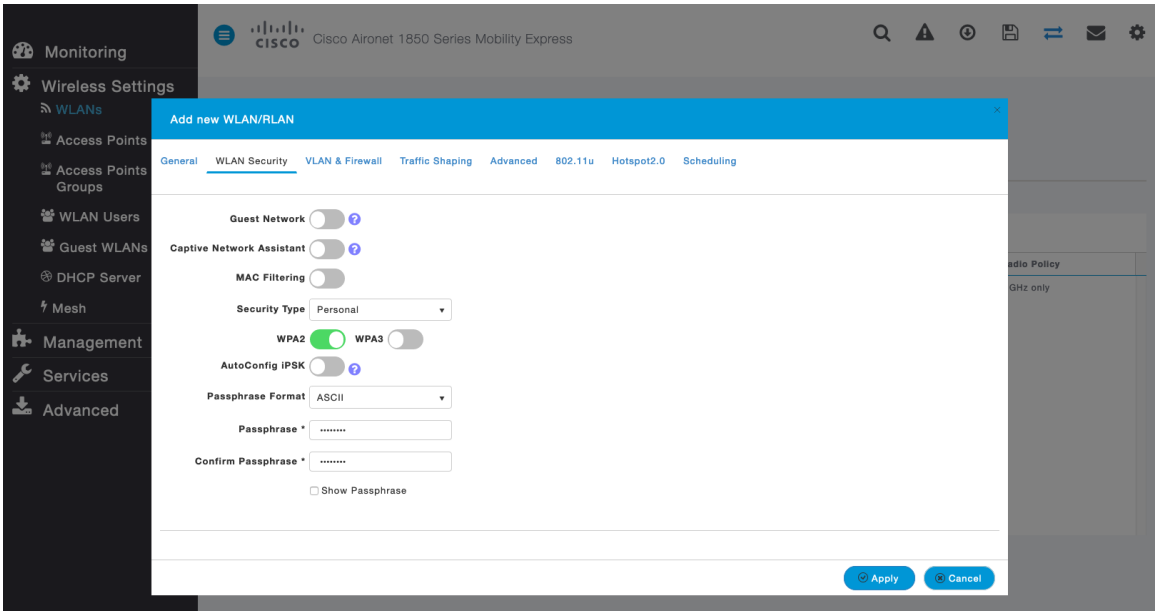
Webex Desk Series は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャンネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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。



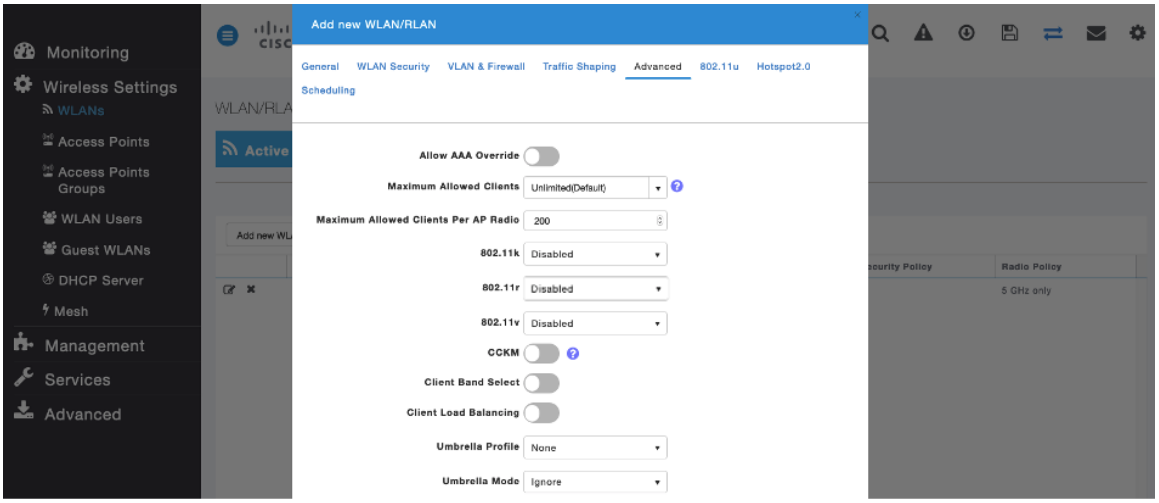
802.1x または PSK のどちらを使用するかに応じて、**[セキュリティタイプ（Security Type）]** を **[WPA2Enterprise]** または **[パーソナル（Personal）]** に設定します。



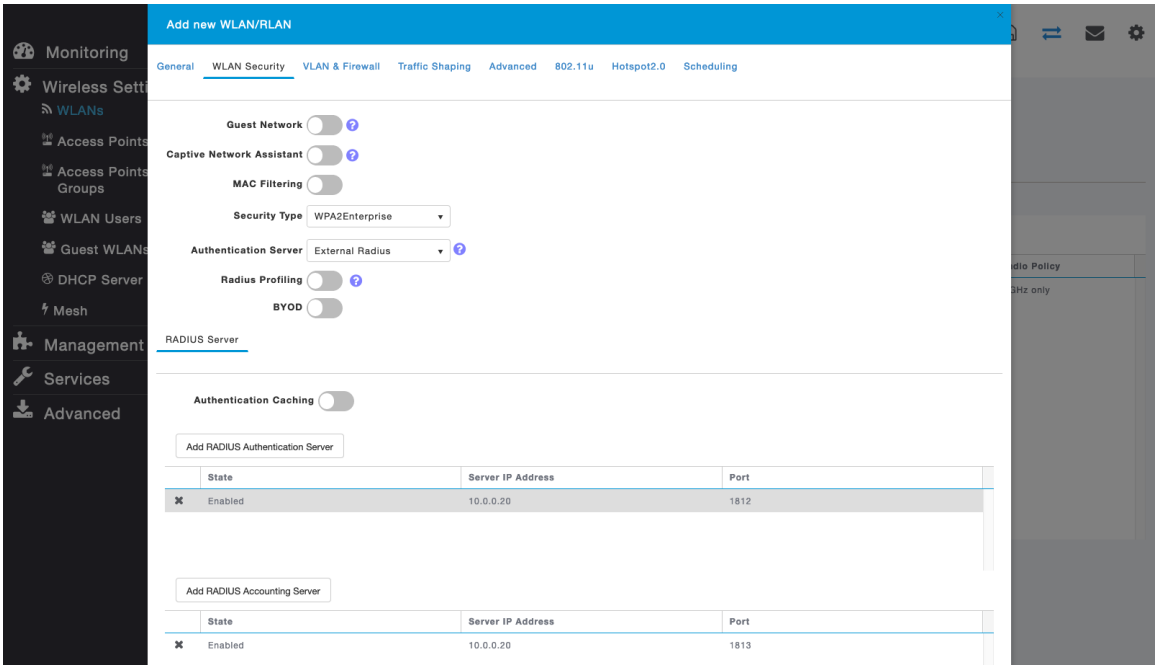


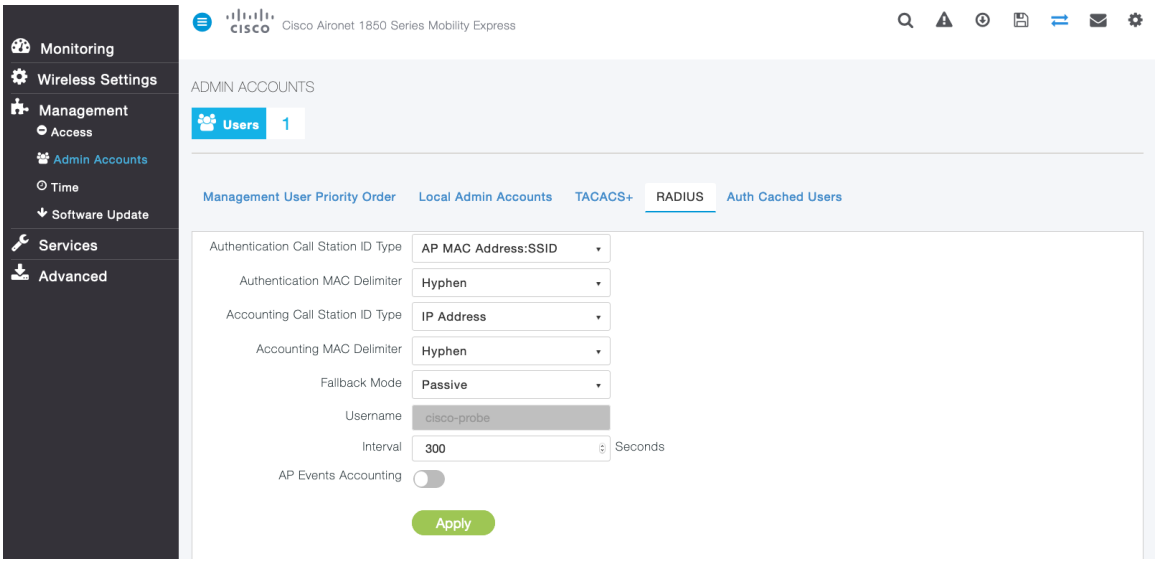
[クライアント帯域幅選択（Client Band Select）] と **[クライアント ロード バランシング（Client Load Balancing）]** が無効になっていることを確認します。

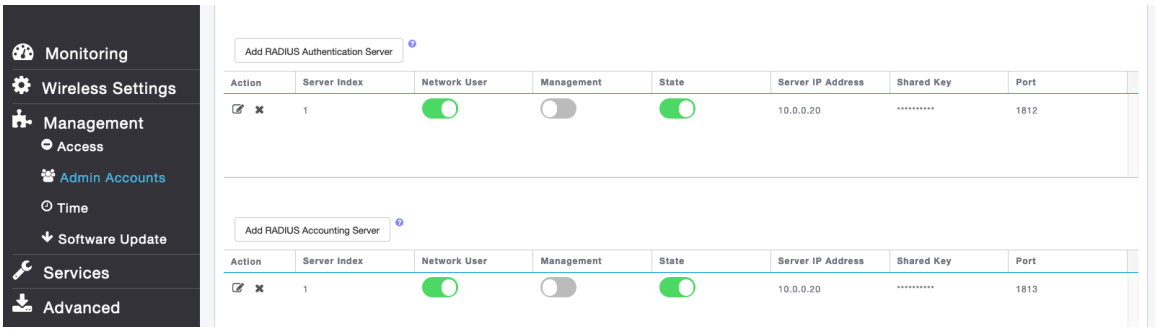
802.11k、802.11r、および 802.11v はサポートされていないため、無効にする必要があります。



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。**

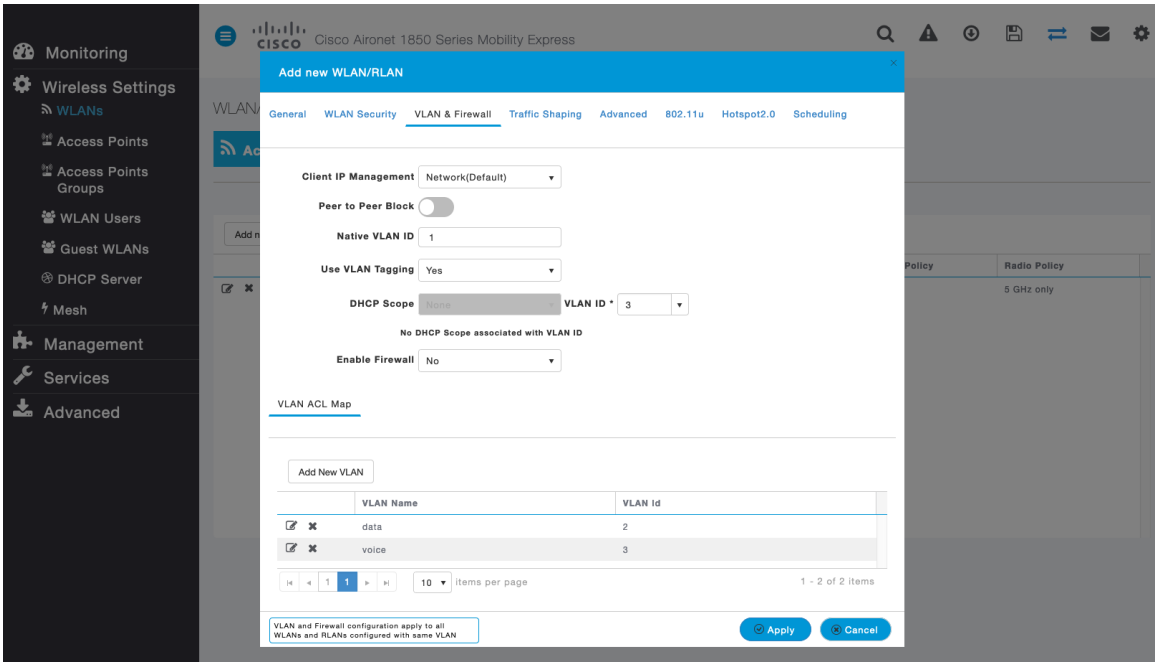




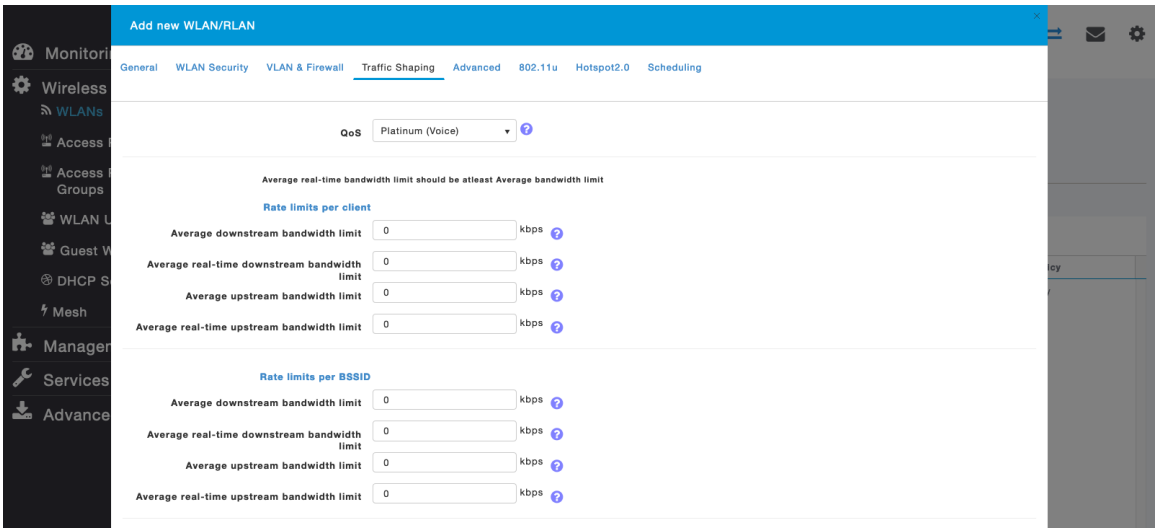


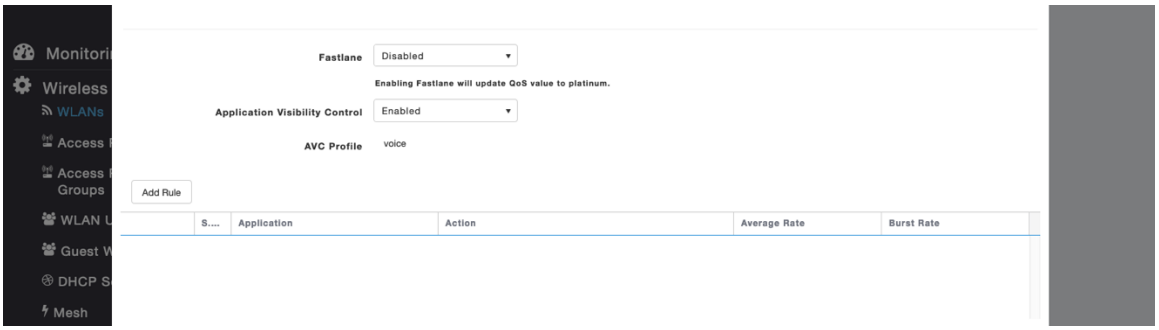
必要に応じて、WLAN の **[ネイティブ VLAN ID（Native VLAN ID）]** と **[VLAN ID]** を設定します。

[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。

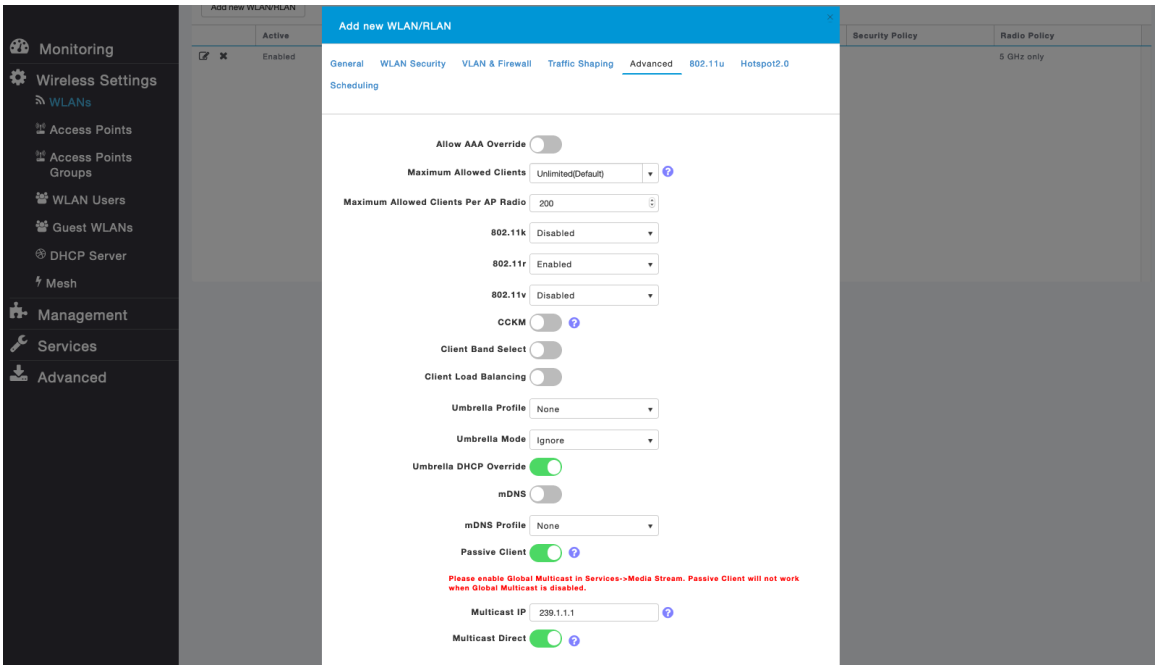


[QoS] に **[プラチナ（音声）（Platinum（Voice））]** が選択されていることを確認します。



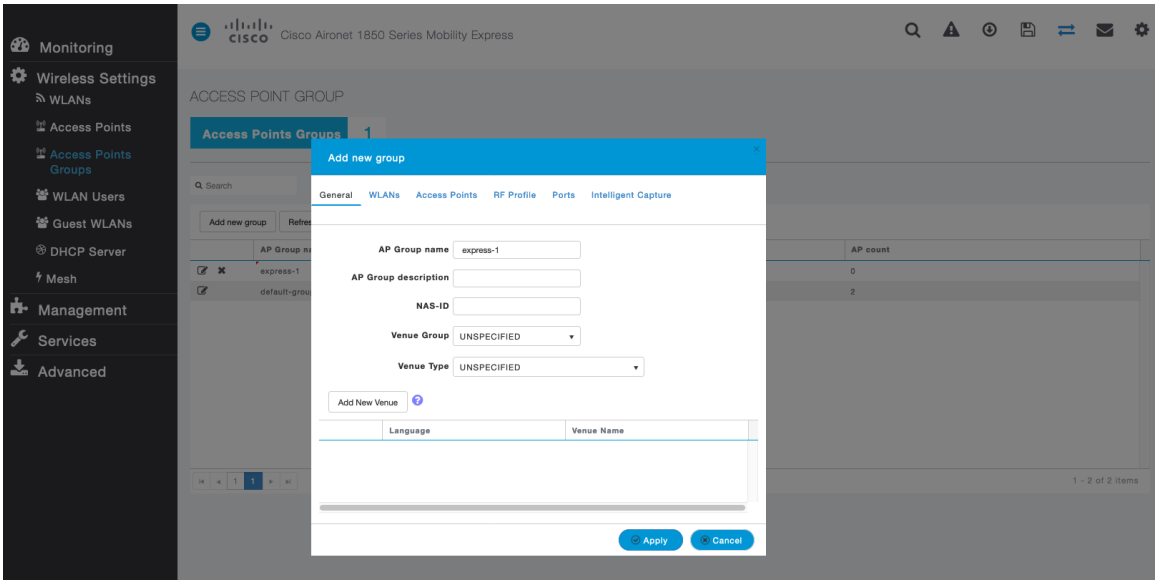


必要に応じて、**[許可される最大クライアント数（Maximum Allowed Clients）]** と **[AP 無線機ごとに許可される最大クライアント数（Maximum Allowed Clients Per AP Radio）]** を設定できます。

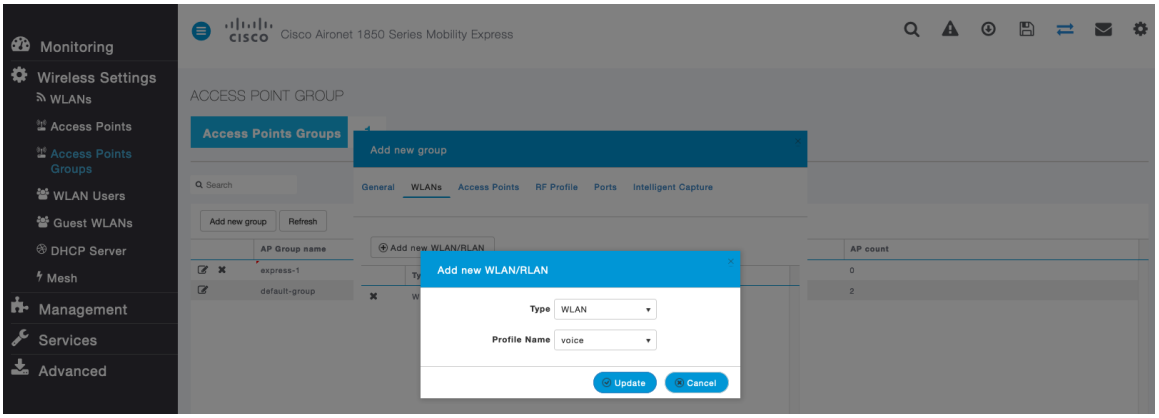


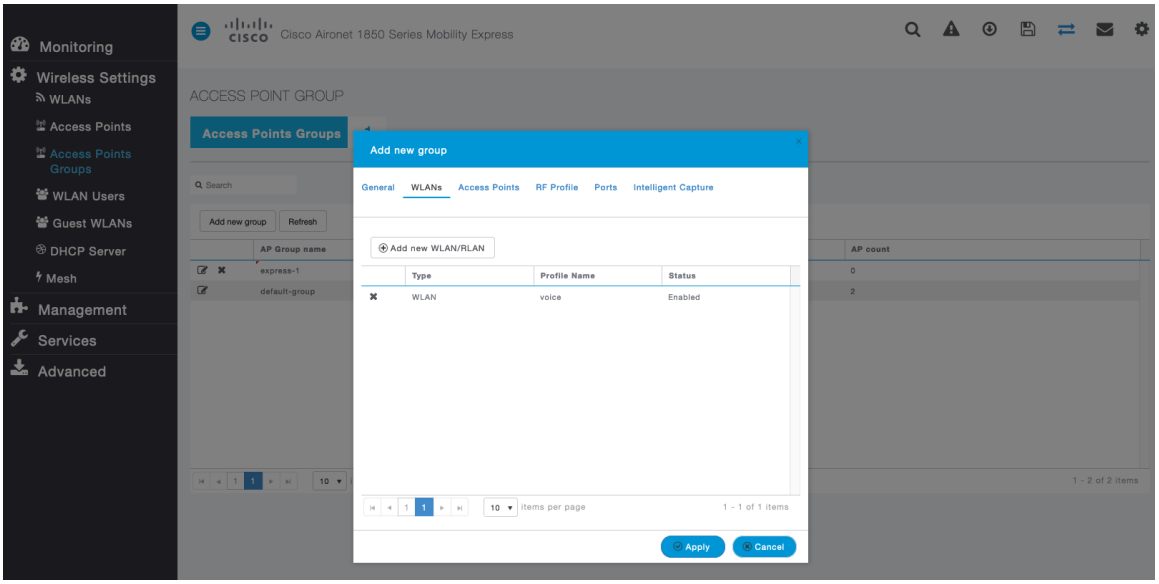
AP グループ

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。

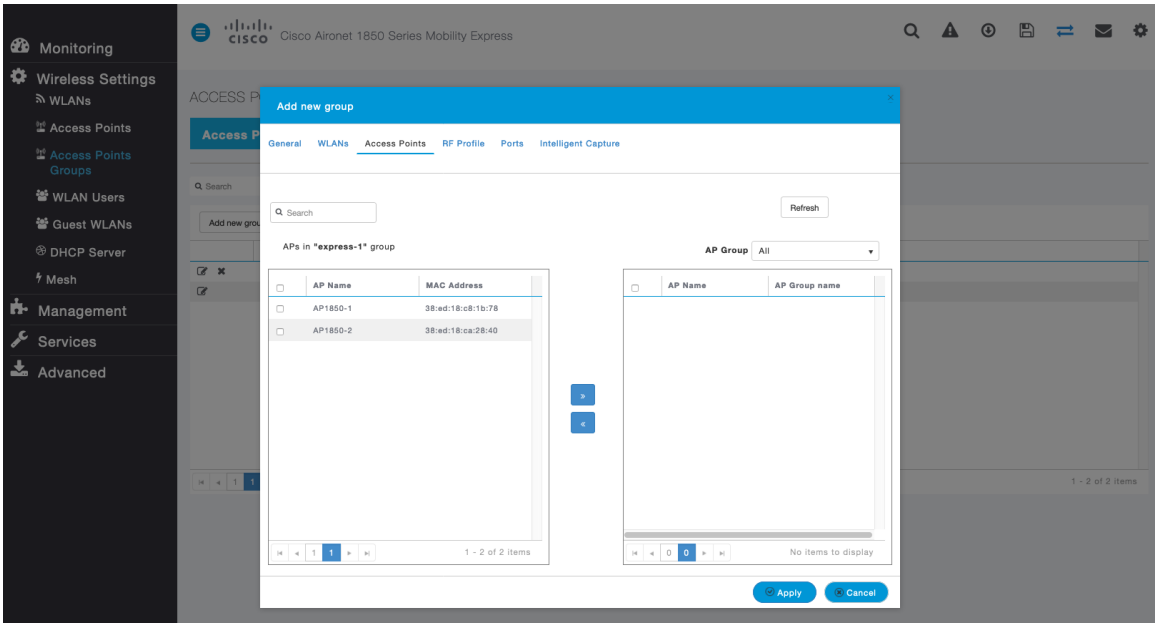


[WLAN（WLANs）] タブで、対象 WLAN と、マッピングするインターフェイスを選択して、**[追加（Add）]** を選択します。

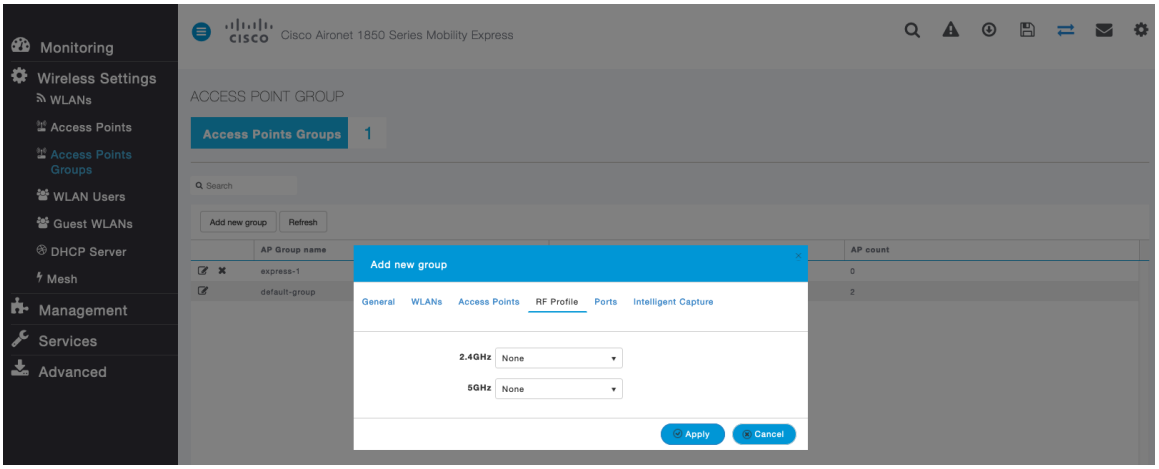




[アクセスポイント（Access Points）] タブで、対象アクセスポイントを選択して、**[適用（Apply）]** を選択します。その後、選択したアクセス ポイントが再起動します。



[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。

Webex Desk Series 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。

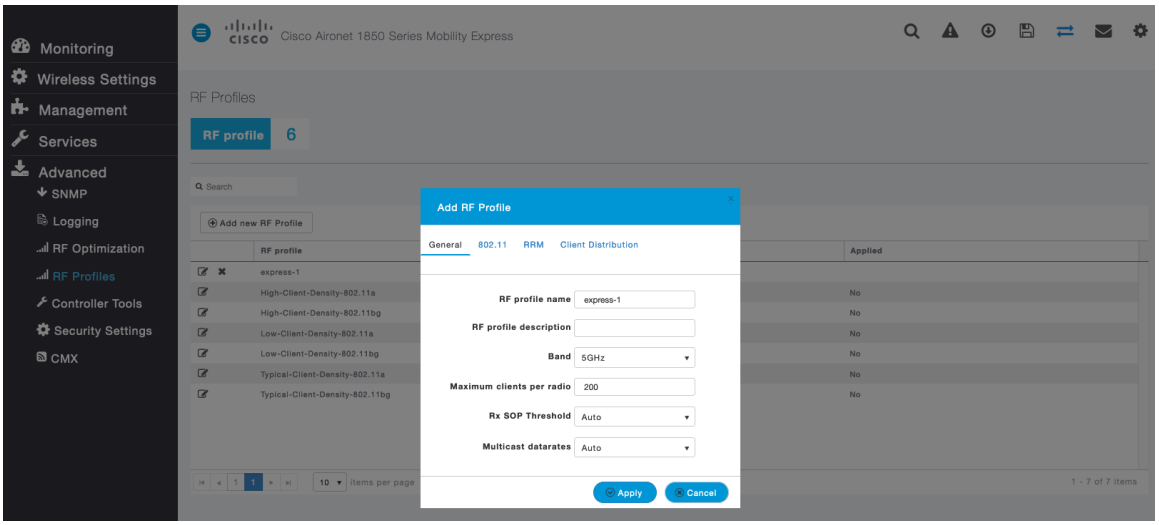
作成した RF プロファイルは、AP グループに適用されます。

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。

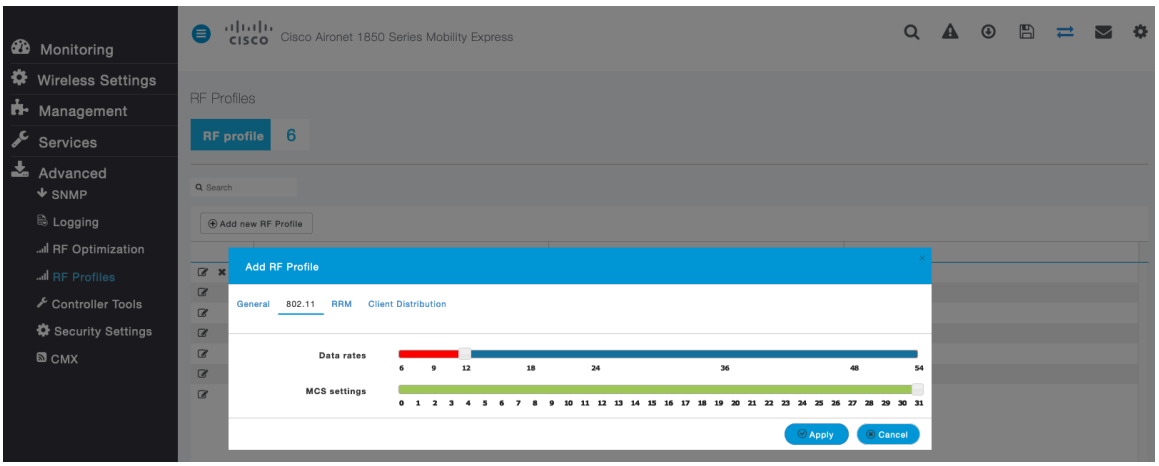
必要に応じて、[無線ごとの最大クライアント数（**Maximum clients per radio**）]、**[マルチキャストデータレート（Multicast Data Rates）]**、および **[Rx Sop のしきい値（Rx Sop Threshold）]** を設定できます。

[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。

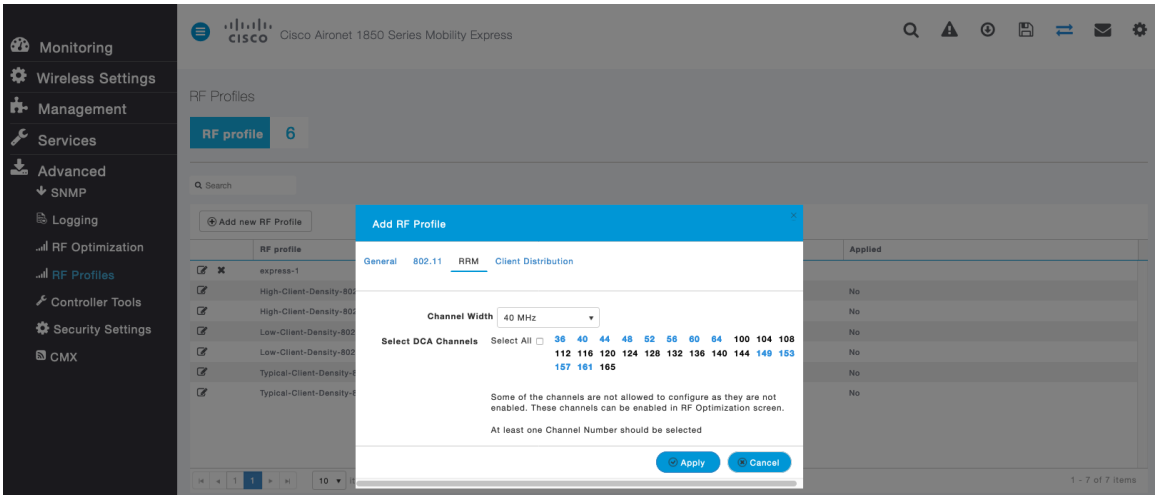


[802.11] タブで、必要に応じてデータレートを設定します。

[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。

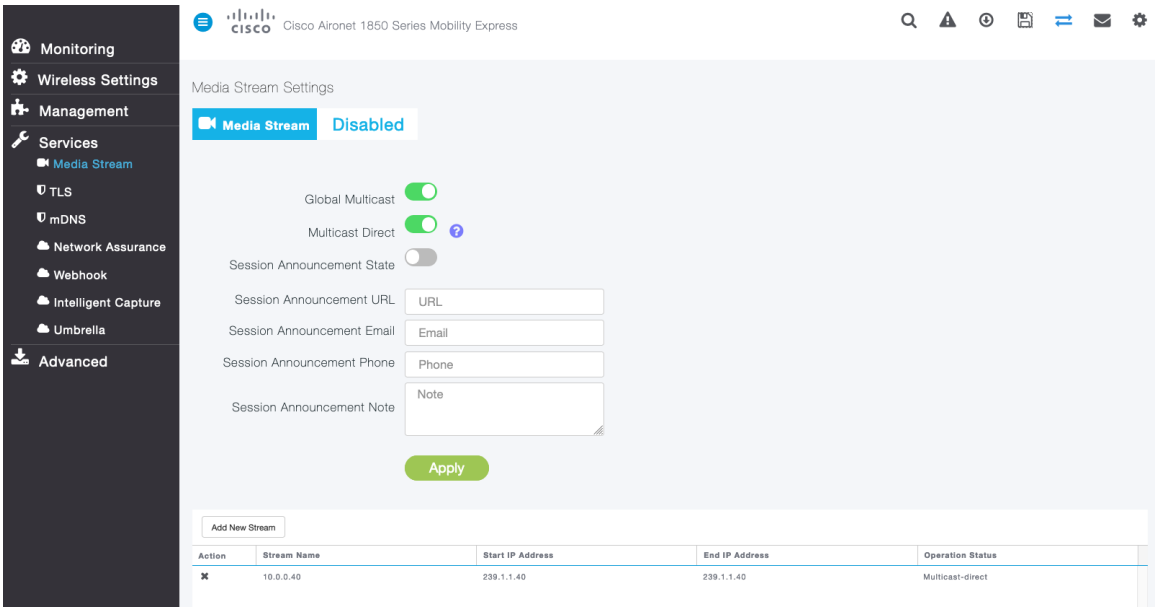


[RRM] タブでは、**[チャンネル幅（Channel Width）]** 設定と **[DCA チャンネル（DCA Channels）]** を構成できます。

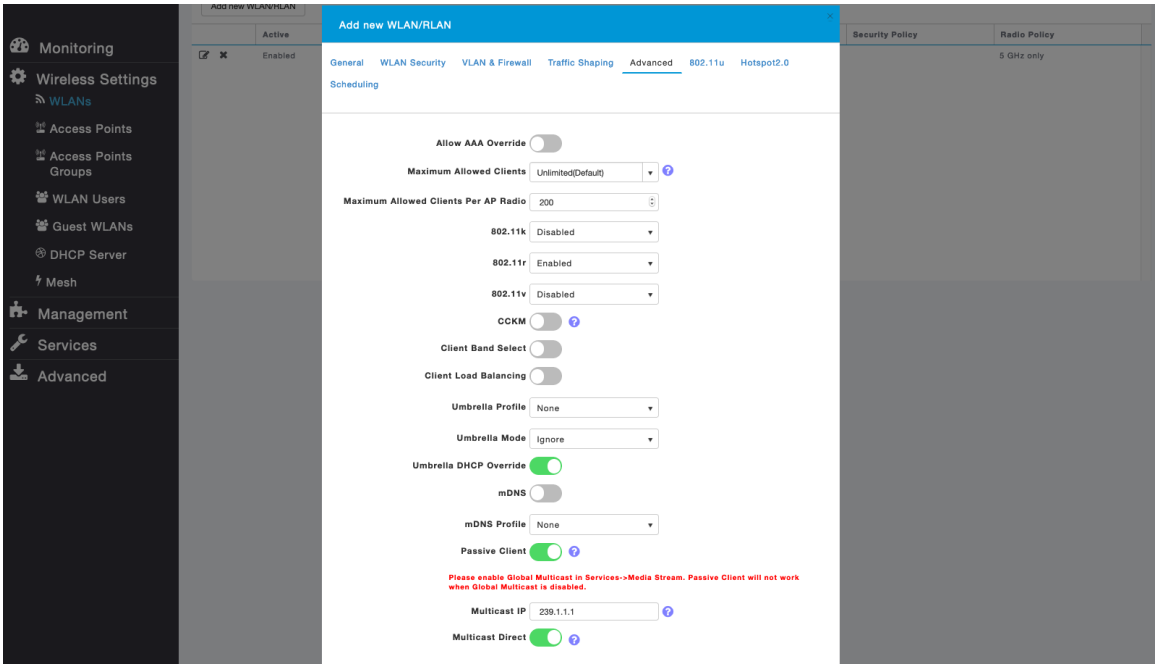


マルチキャスト ダイレクト

[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。



[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 Directture）]** 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 Directture）]** 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

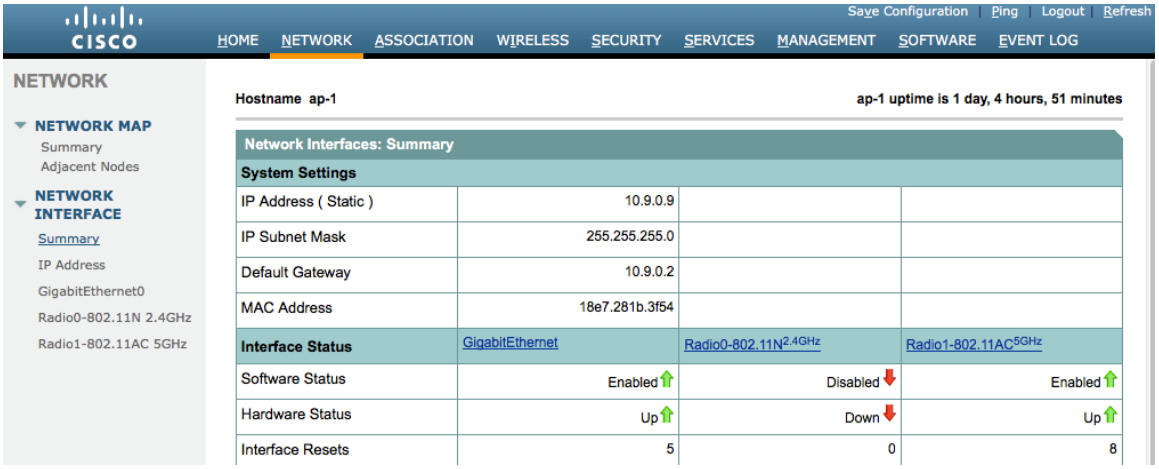
Cisco Autonomous アクセス ポイントを設定するときは、次のガイドラインを使用してください。

- **[802.11r（FT）]** と **[CCKM]** が必須として構成されていないことを確認します
- **[802.11k]** が **[無効（Disabled）]** になっていることを確認します
- **[802.11v]** が **[無効（Disabled）]** になっていることを確認します
- 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。
- **[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

Webex Desk Series 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。

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。



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 チャネル（チャネル 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。

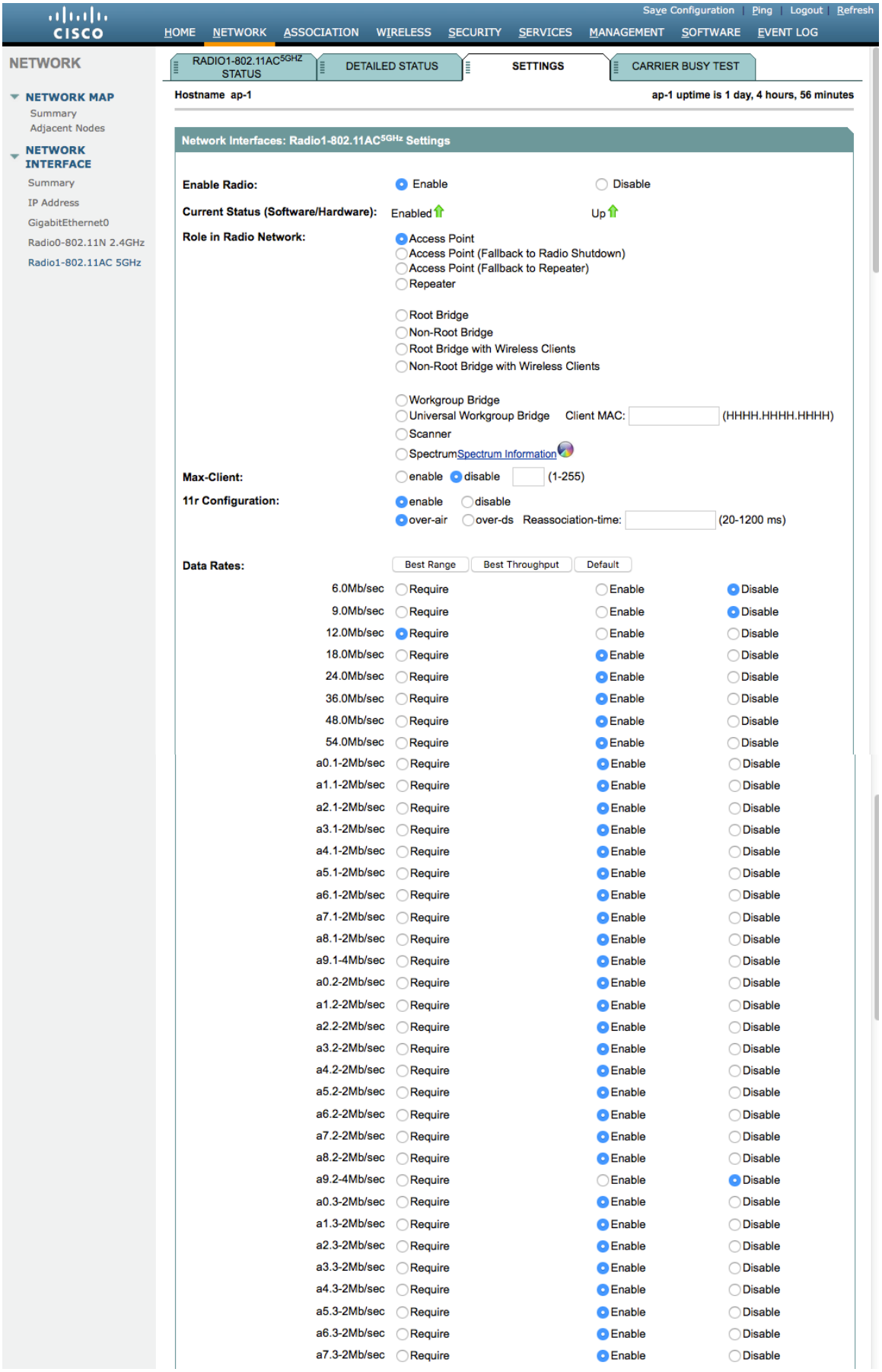
Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネル幅を 20 MHz または 40 MHz 用として設定でき、Cisco 802.11ac アクセス ポイントを使用している場合は 5 GHz チャネル幅を 20 MHz、40 MHz、または 80 MHz 用として設定できます。

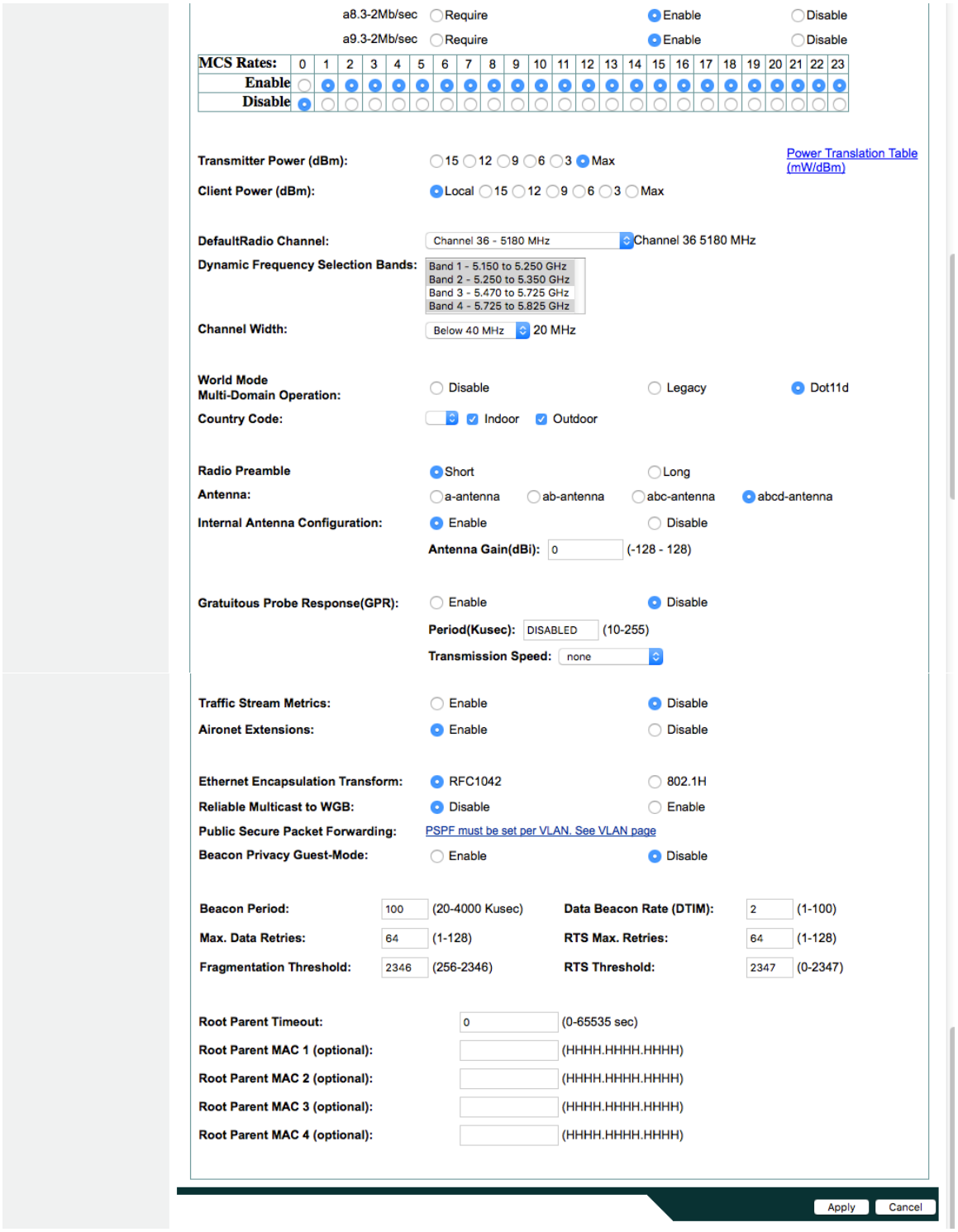
すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

[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。


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
NETWORK
NETWORK MAP
Summary
Adjacent Nodes
NETWORK INTERFACE
Summary
IP Address
GigabitEthernet0
Radio0-802.11N 2.4GHz
Radio1-802.11AC 5GHz
RADIO1-802.11AC5GHZ STATUS
DETAILED STATUS
SETTINGS
CARRIER BUSY TEST
Hostname ap-1
ap-1 uptime is 1 day, 4 hours, 56 minutes
Network Interfaces: Radio1-802.11AC5GHz 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
SpectrumSpectrum Information
Max-Client: enable disable (1-255)
11r Configuration: enable disable
over-air over-ds Reassociation-time: (20-1200 ms)
Data Rates: Best Range Best Throughput Default
6.0Mb/sec Require Enable Disable
9.0Mb/sec Require Enable Disable
12.0Mb/sec Require Enable Disable
18.0Mb/sec Require Enable Disable
24.0Mb/sec Require Enable Disable
36.0Mb/sec Require Enable Disable
48.0Mb/sec Require Enable Disable
54.0Mb/sec Require Enable Disable
a0.1-2Mb/sec Require Enable Disable
a1.1-2Mb/sec Require Enable Disable
a2.1-2Mb/sec Require Enable Disable
a3.1-2Mb/sec Require Enable Disable
a4.1-2Mb/sec Require Enable Disable
a5.1-2Mb/sec Require Enable Disable
a6.1-2Mb/sec Require Enable Disable
a7.1-2Mb/sec Require Enable Disable
a8.1-2Mb/sec Require Enable Disable
a9.1-4Mb/sec Require Enable Disable
a0.2-2Mb/sec Require Enable Disable
a1.2-2Mb/sec Require Enable Disable
a2.2-2Mb/sec Require Enable Disable
a3.2-2Mb/sec Require Enable Disable
a4.2-2Mb/sec Require Enable Disable
a5.2-2Mb/sec Require Enable Disable
a6.2-2Mb/sec Require Enable Disable
a7.2-2Mb/sec Require Enable Disable
a8.2-2Mb/sec Require Enable Disable
a9.2-4Mb/sec Require Enable Disable
a0.3-2Mb/sec Require Enable Disable
a1.3-2Mb/sec Require Enable Disable
a2.3-2Mb/sec Require Enable Disable
a3.3-2Mb/sec Require Enable Disable
a4.3-2Mb/sec Require Enable Disable
a5.3-2Mb/sec Require Enable Disable
a6.3-2Mb/sec Require Enable Disable
a7.3-2Mb/sec Require Enable Disable



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。

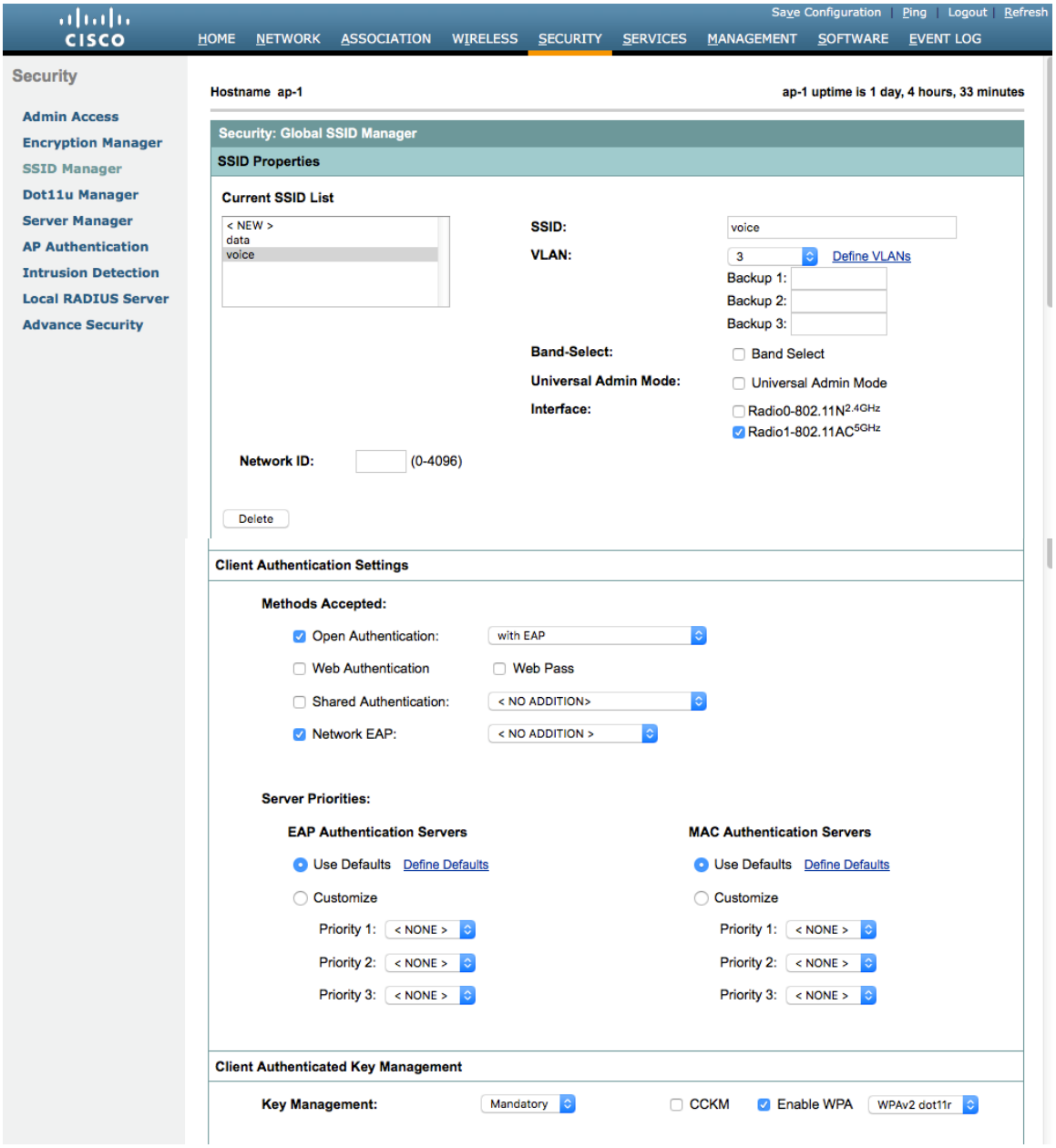
WLAN の設定

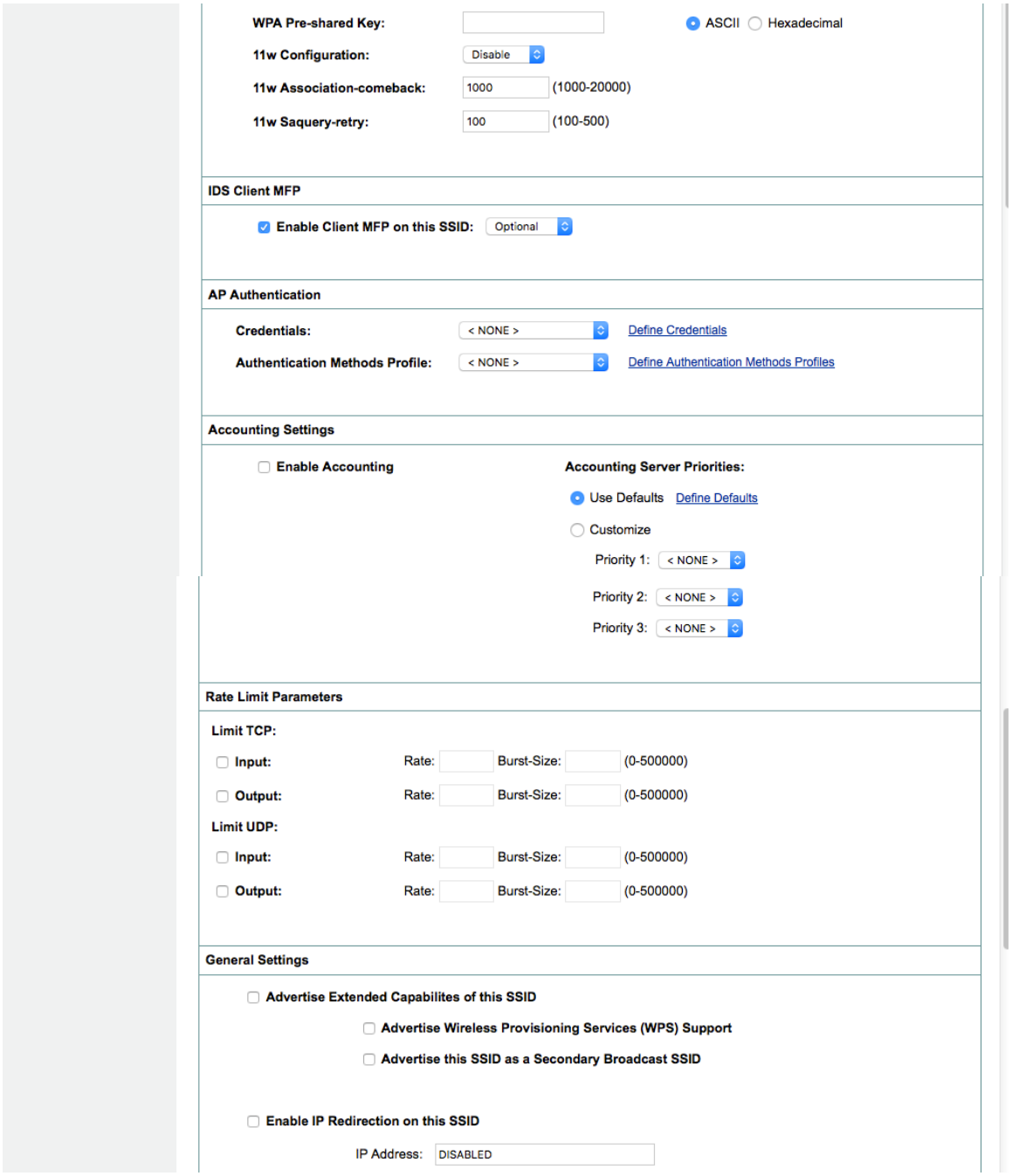
Webex Desk Series には別の SSID を使用することをお勧めします。

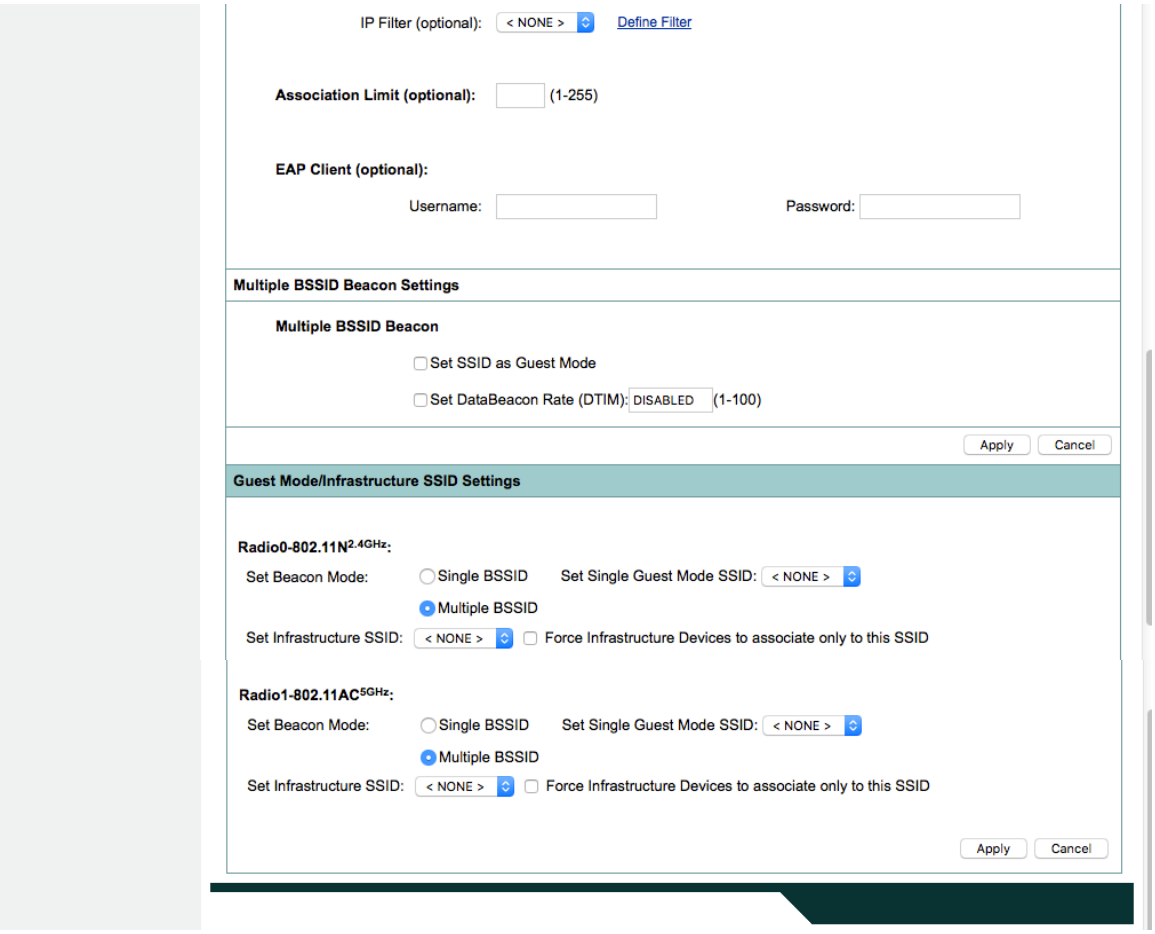
ただし、音声対応 Cisco Wireless LAN エンドポイントをサポートするように設定された既存の SSID がある場合、その WLAN を代わりに使用できます。

Webex Desk Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように設定できます（802.11a のみなど）。

[WPA2] キー管理を有効にします。

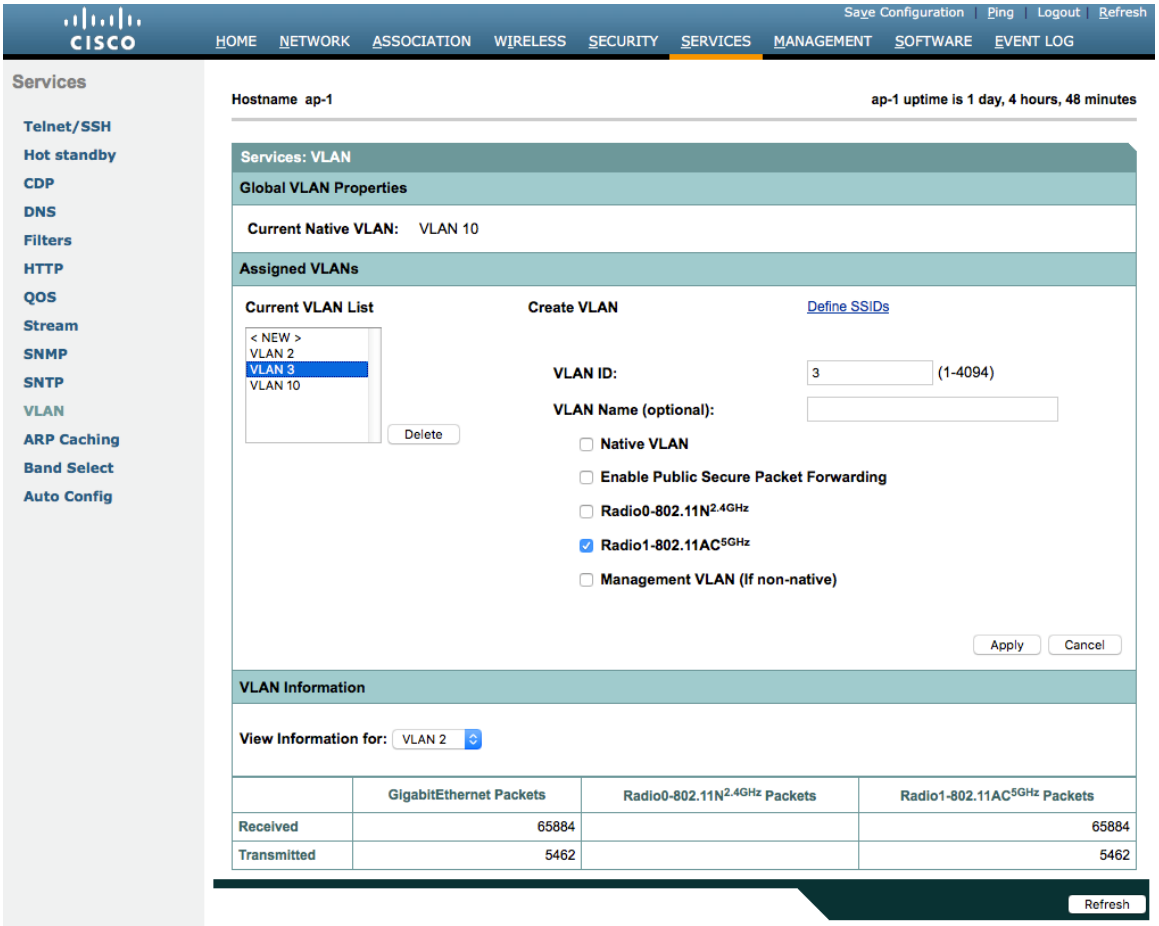



WPA Pre-shared Key:
ASCII
Hexadecimal
11w Configuration:
Disable
11w Association-comeback:
1000
(1000-20000)
11w Saquery-retry:
100
(100-500)
IDS Client MFP
Enable Client MFP on this SSID:
Optional
AP Authentication
Credentials:
< NONE >
Define Credentials
Authentication Methods Profile:
< NONE >
Define Authentication Methods Profiles
Accounting Settings
Enable Accounting
Accounting Server Priorities:
Use Defaults
Define Defaults
Customize
Priority 1:
< NONE >
Priority 2:
< NONE >
Priority 3:
< NONE >
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:
DISABLED

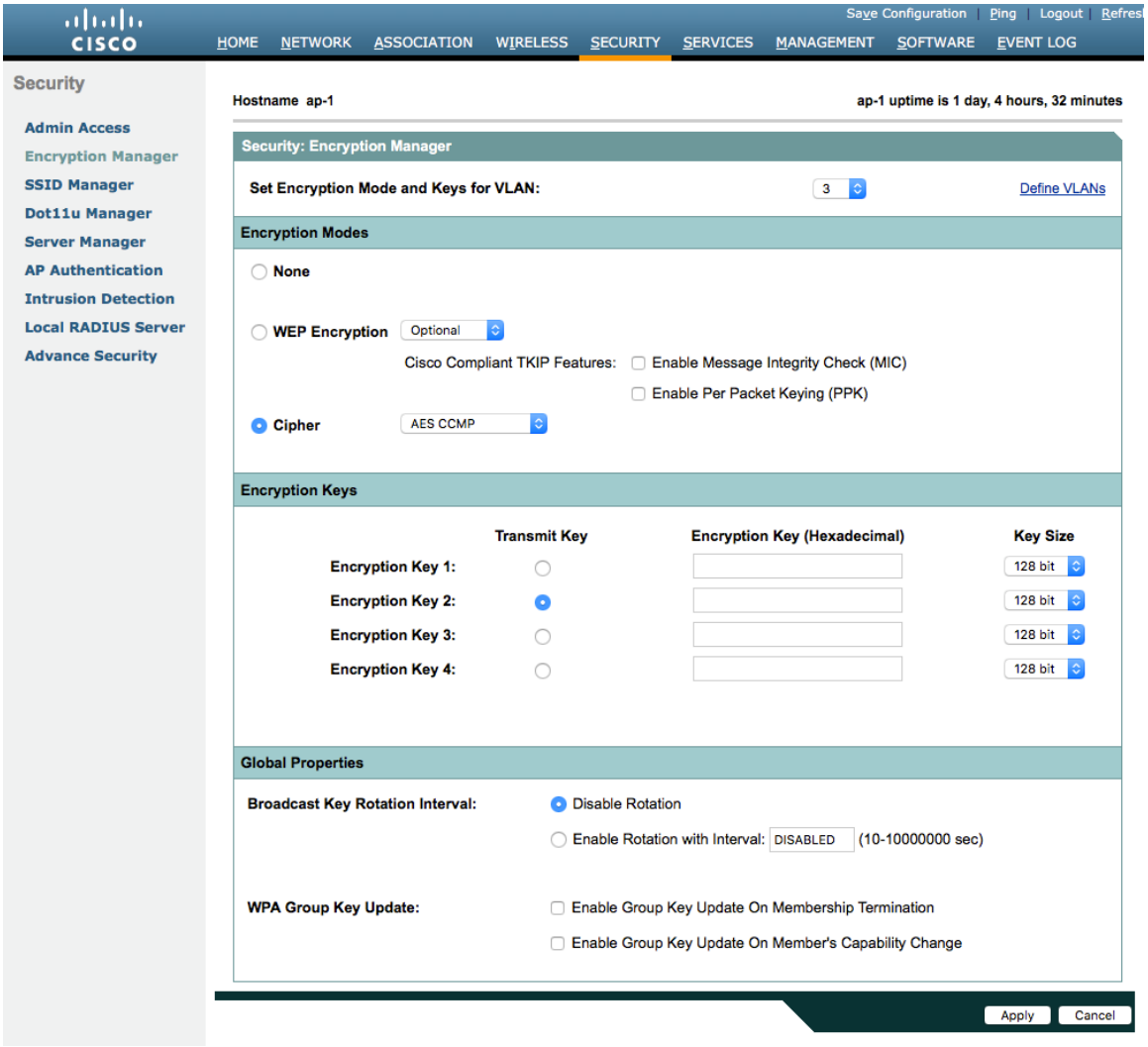


ワイヤレス音声/データを別個の VLAN にセグメント化します。

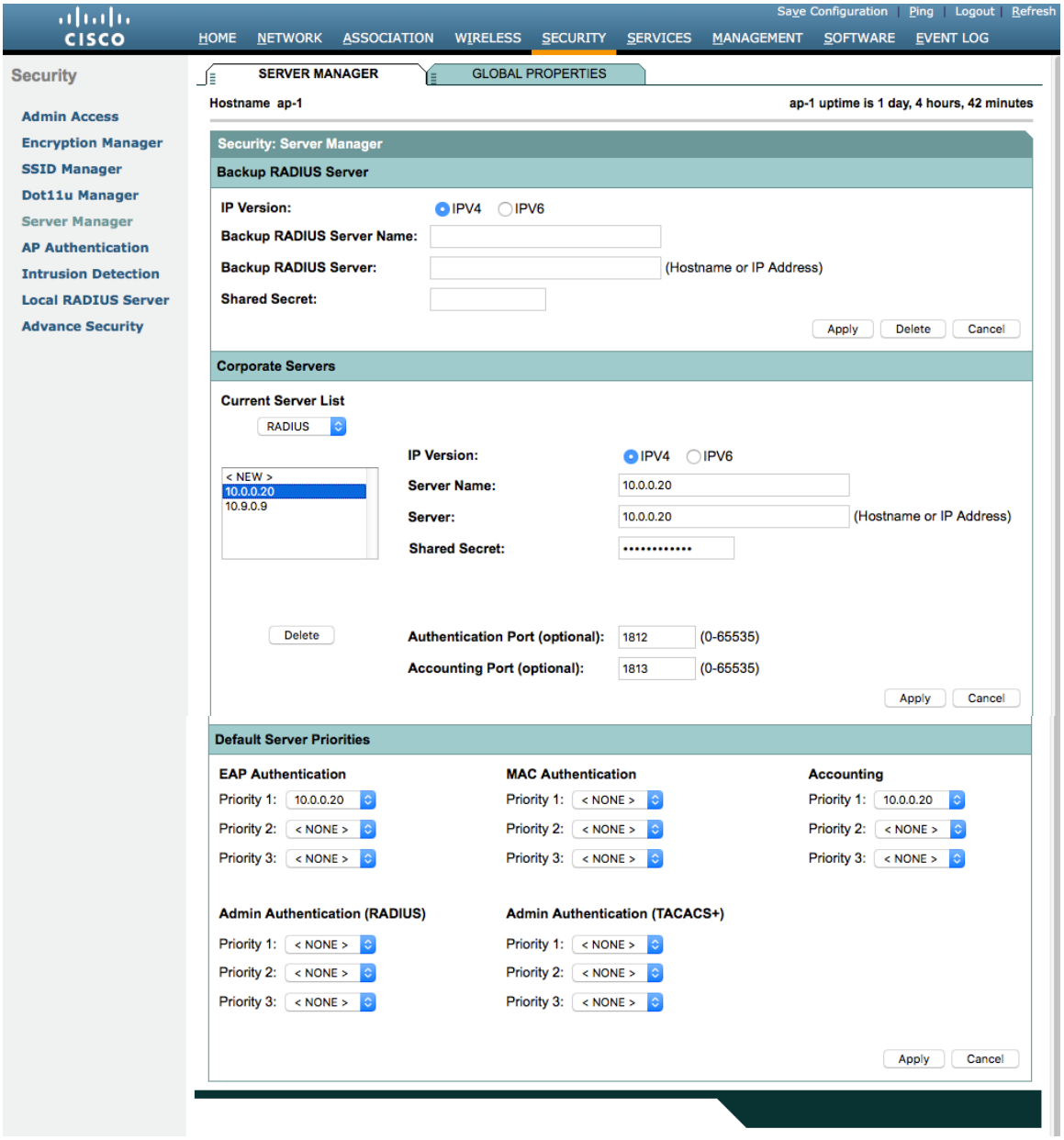
音声 VLAN に対して、パブリック セキュア パケット フォワーディング（PSPF）が有効になっている場合は、PSPF が無効になっていることを確認します。PSPF が有効になっている場合にクライアントが同じアクセス ポイントに関連付けられると、直接通信できません。PSPF を有効にすると、オーディオは無指向となります。



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。



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

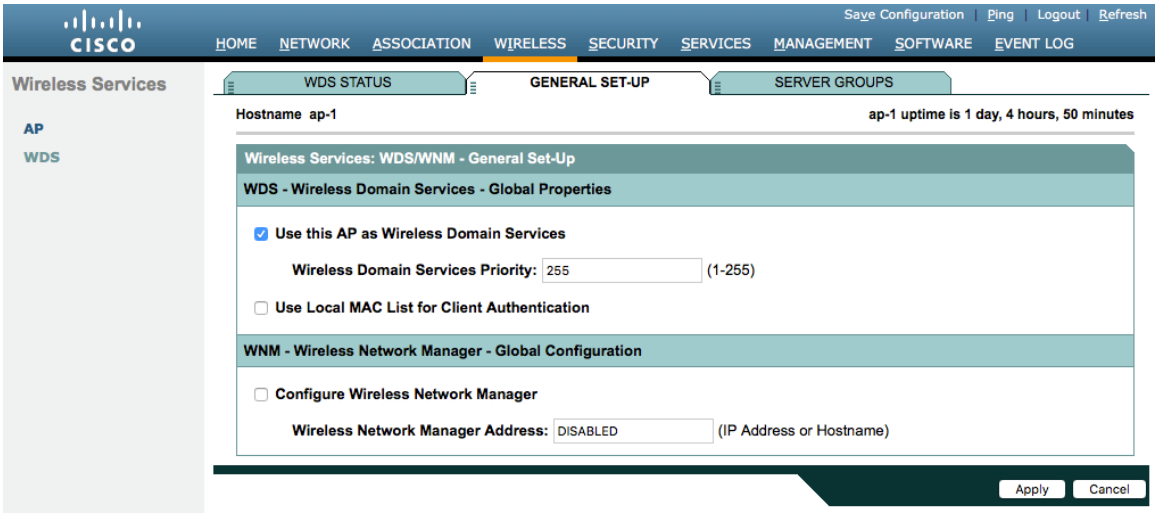


無線ドメイン サービス（WDS）

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。

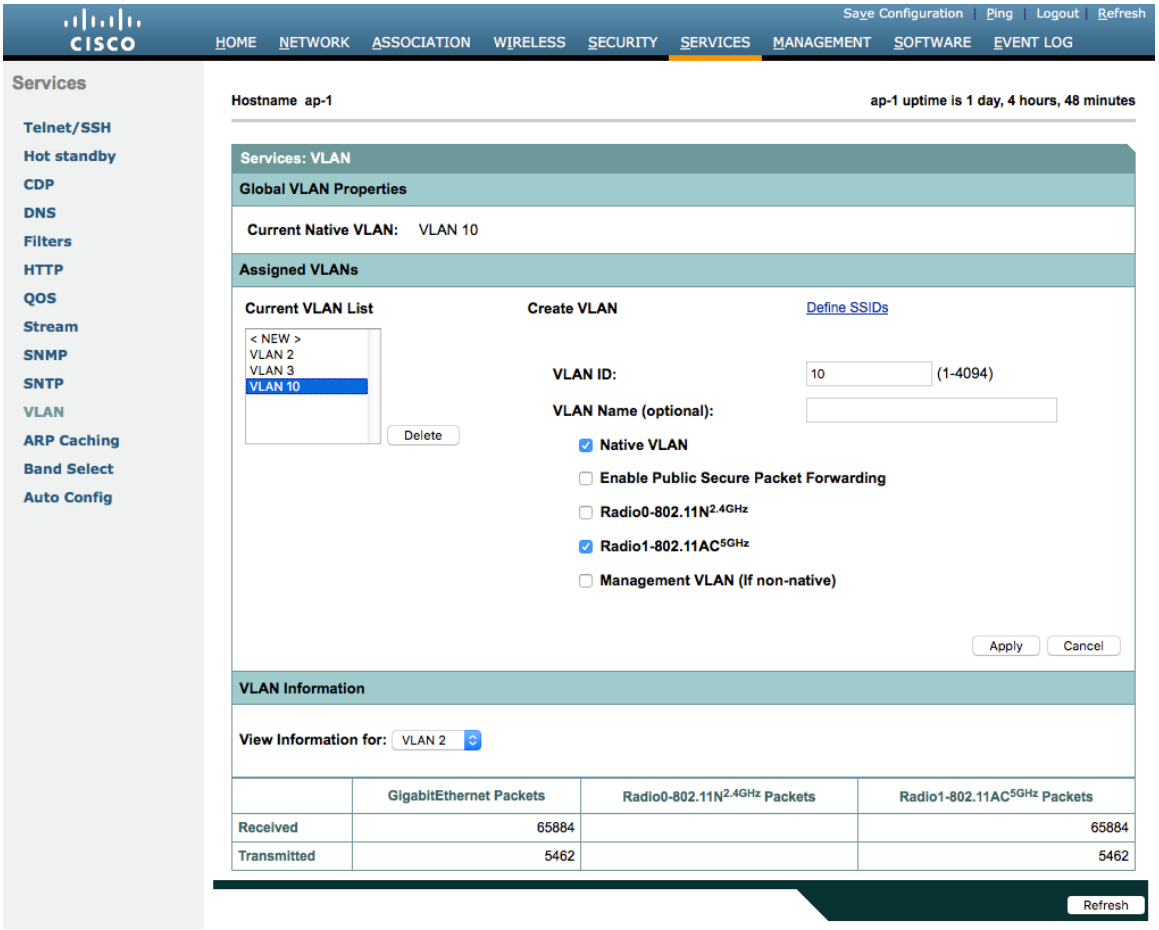
プライマリ WDS サーバに最も高い優先順位（255 など）を設定し、バックアップ WDS サーバにそれよりも低い優先順位（254 など）を設定します。



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。

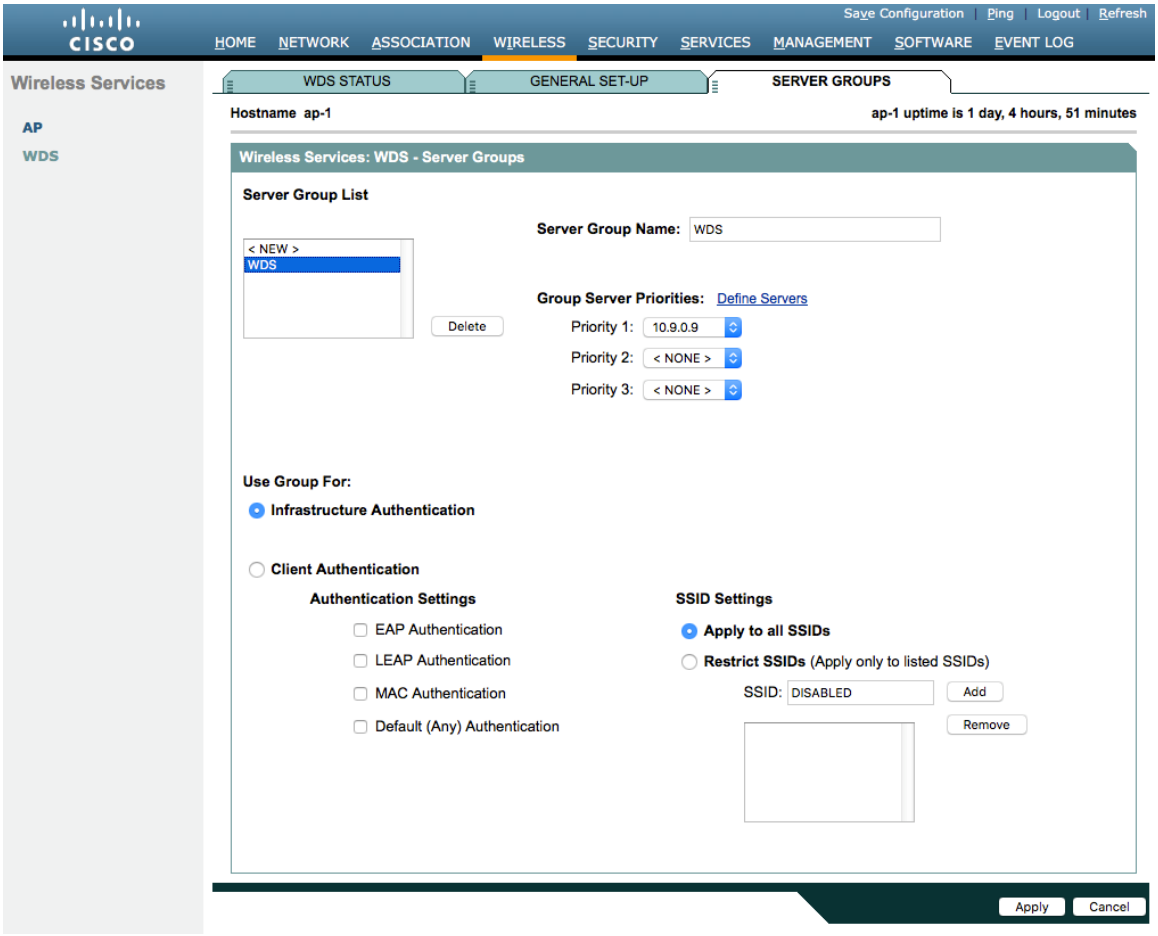


無線ドメイン サービス用のサーバ グループを定義する必要があります。

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。

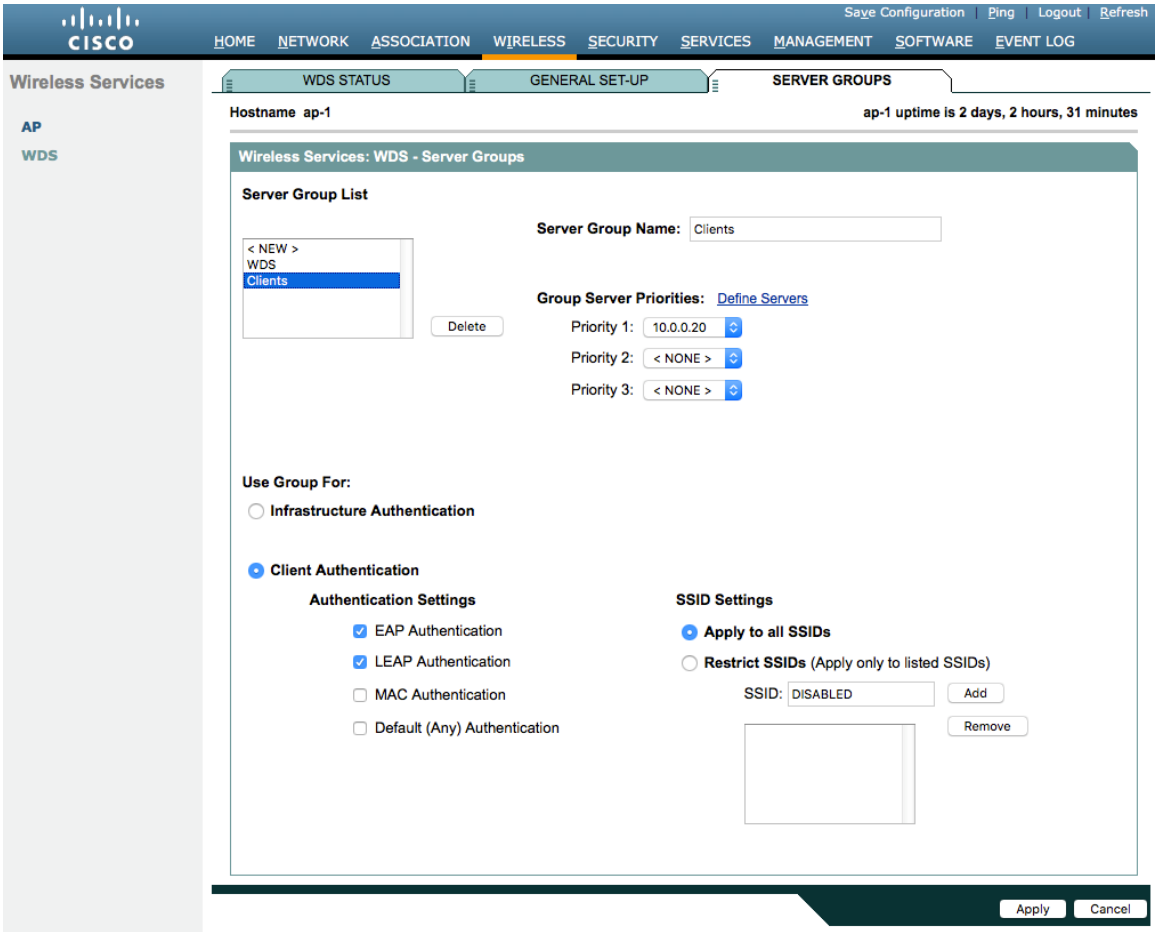
インフラストラクチャ認証にはローカル RADIUS を使用することを推奨します。

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。



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。

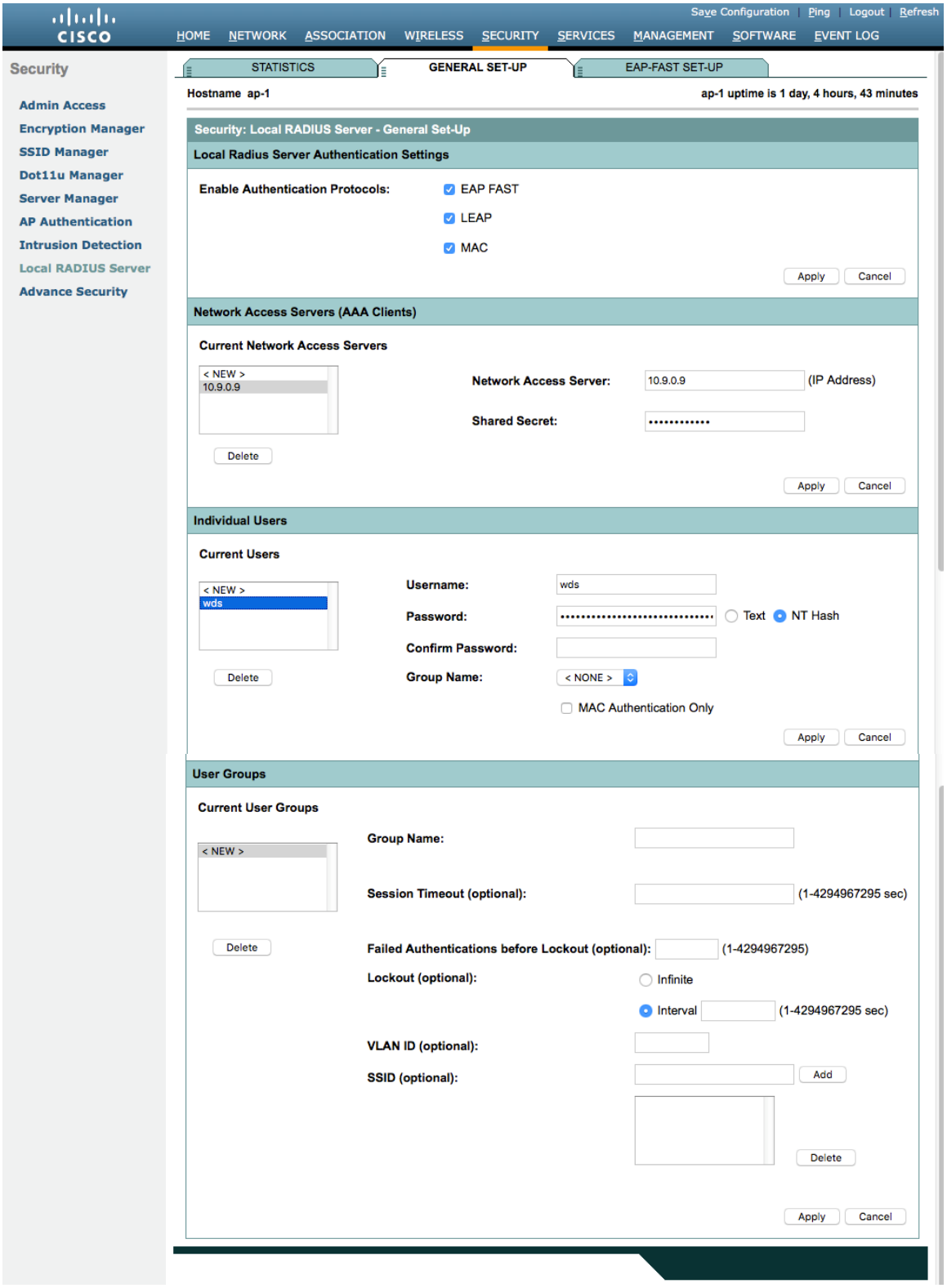


インフラストラクチャ認証にローカル RADIUS を使用する場合は、すべての認証プロトコルを有効にします。

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。

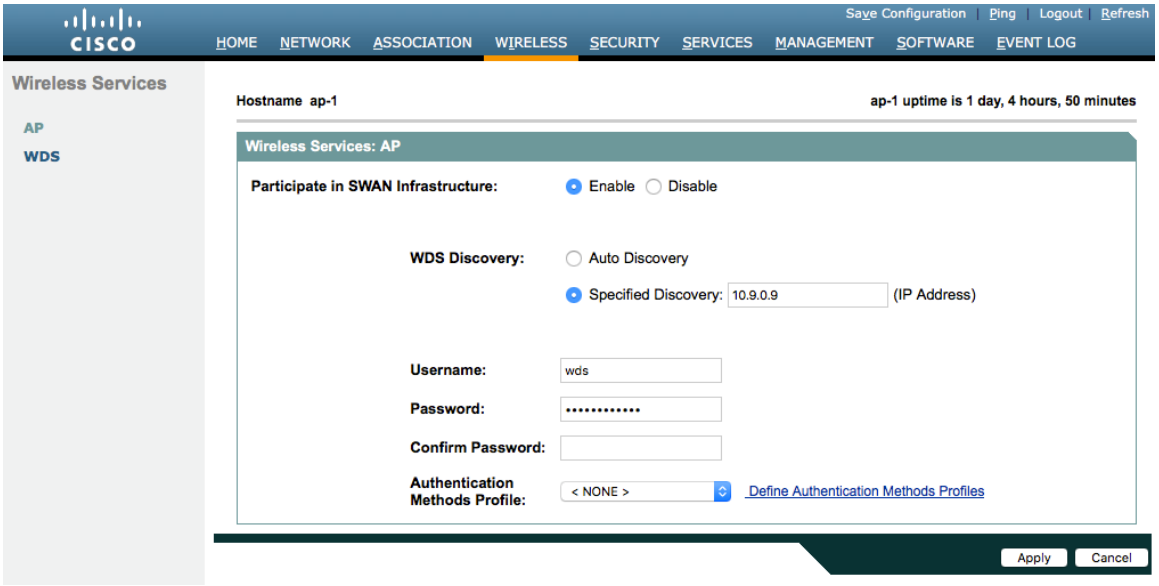


無線ドメイン サービスが有効になるように必要なアクセス ポイントを正しく設定したら、WDS サーバとして機能するアクセス ポイントを含むすべてのアクセス ポイントを、WDS サーバに対して認証できるように設定する必要があります。

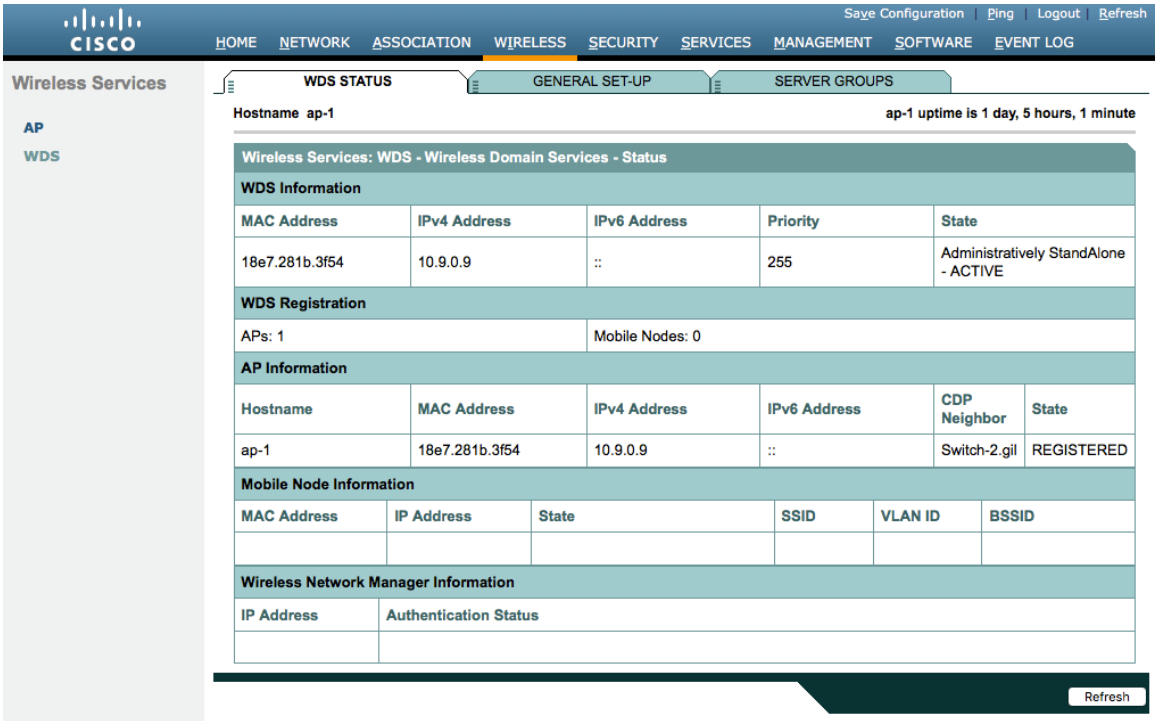
[SWAN インフラストラクチャに参加（Participate in SWAN Infrastructure）] を有効にします。

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 サーバー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。



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。



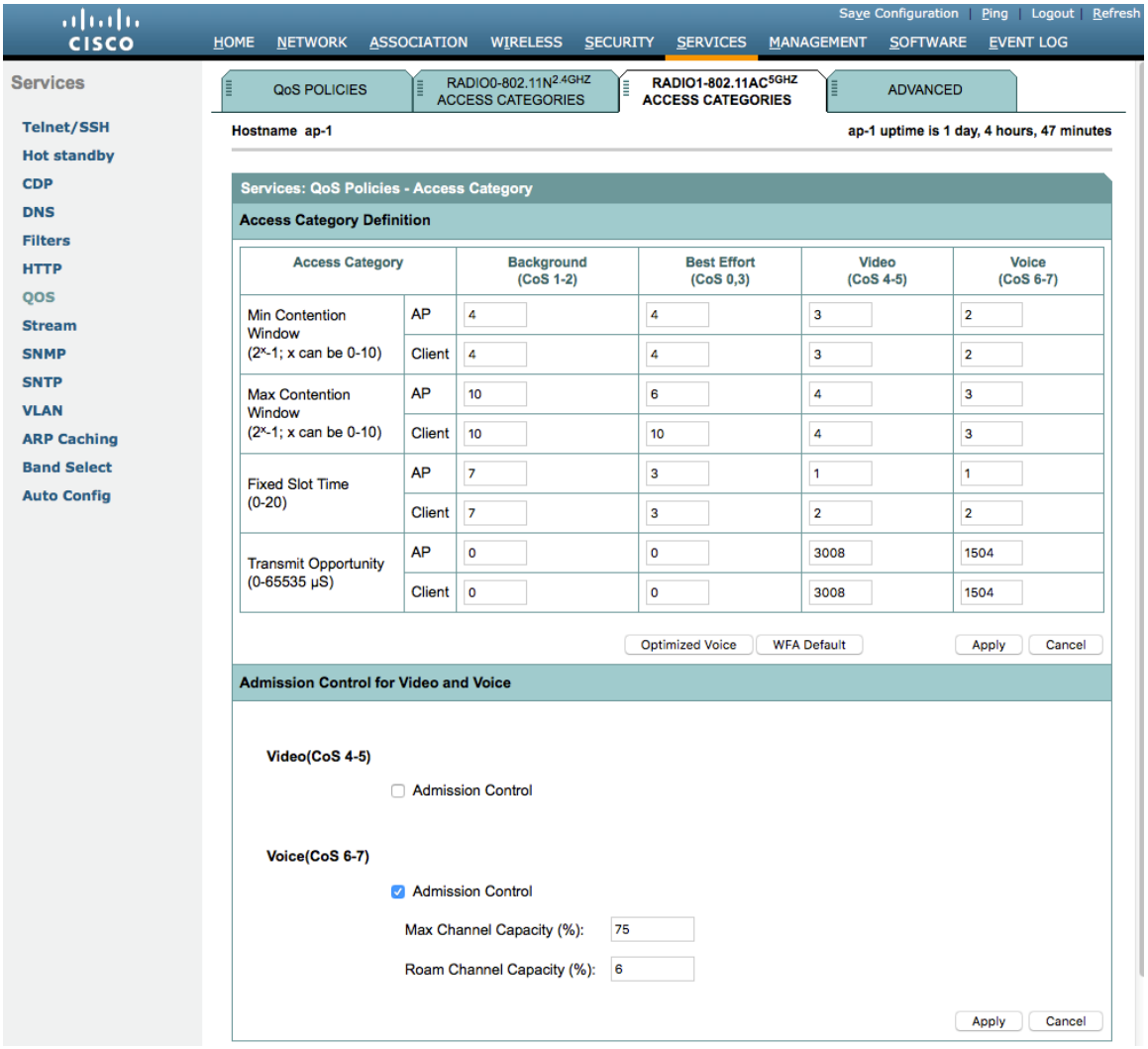
コール アドミッション制御（CAC）

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。

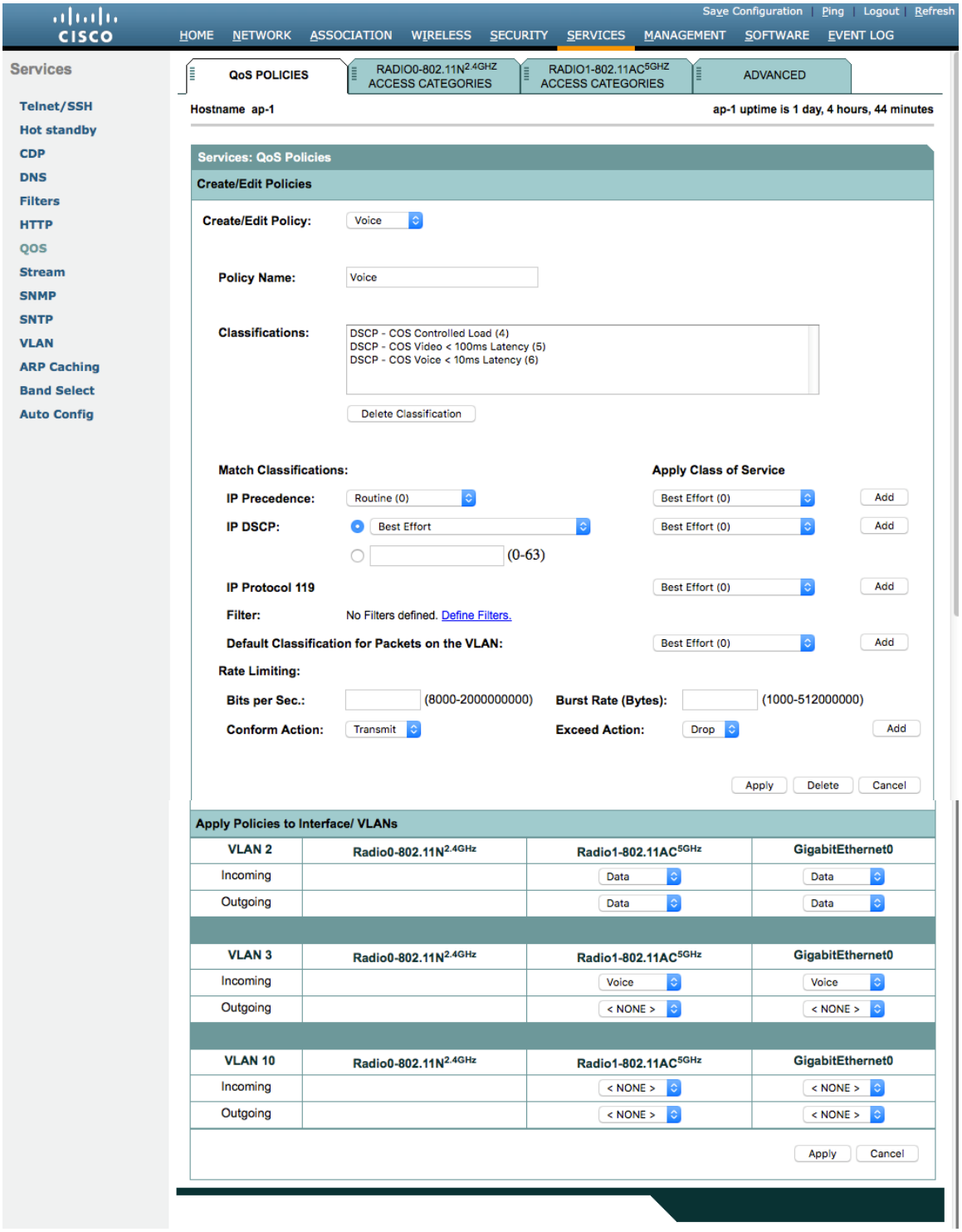
```
dot11 ssid voice
   vlan 3
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa version 2
   admit-traffic
```



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。

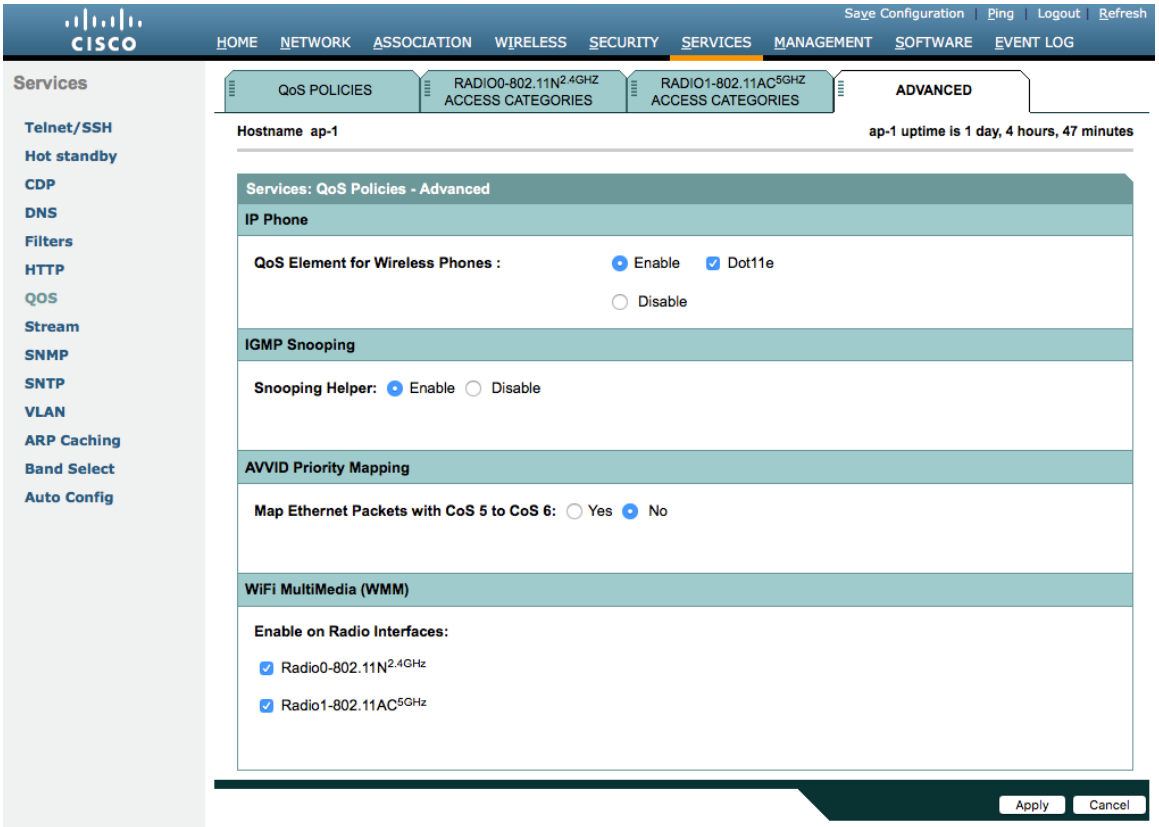


QBSS を有効にするには、**[有効（Enable）]** を選択し、**[Dot11e]** をオンにします。

[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。

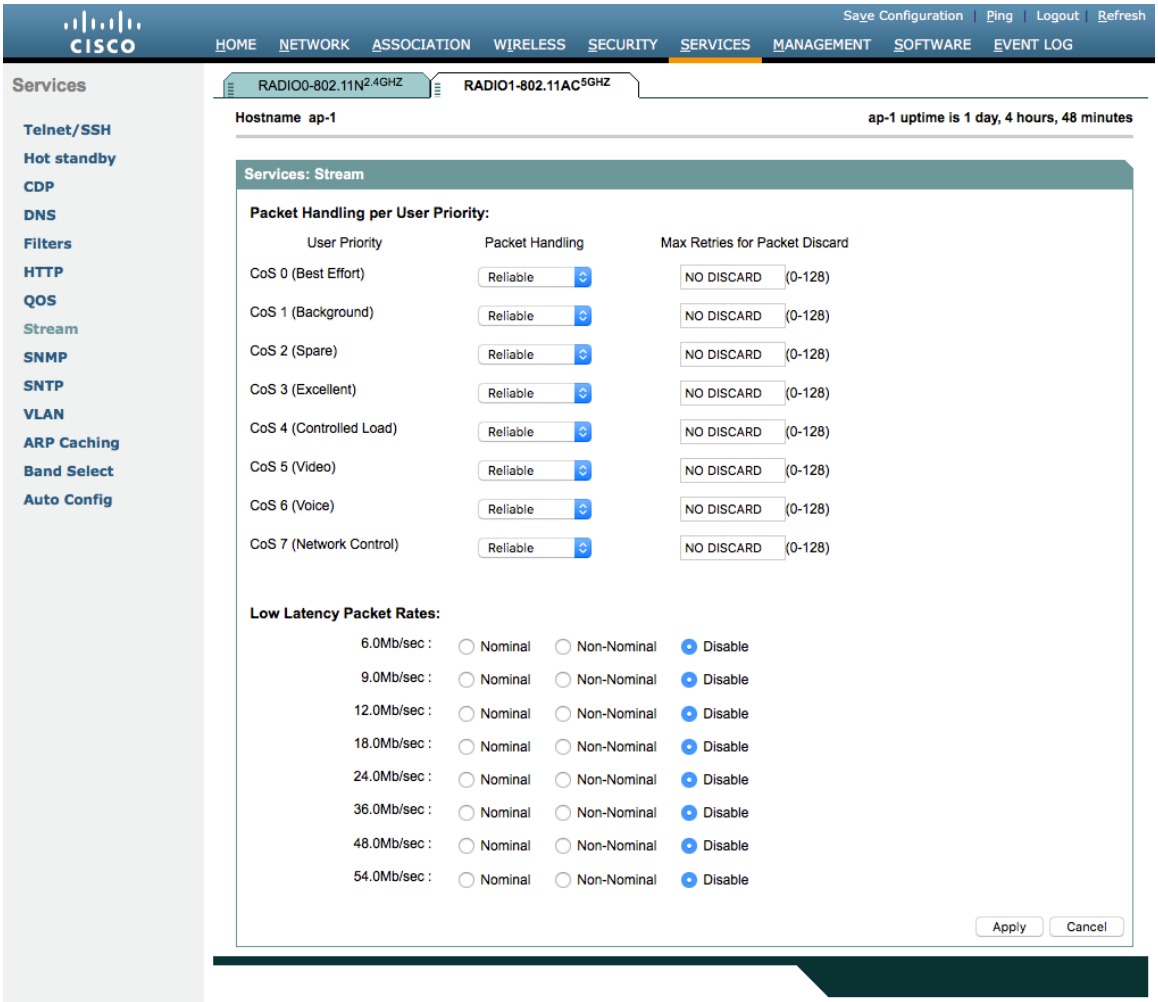
[IGMP スヌーピング（IGMP Snooping）] が有効になっていることを確認します。

[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。

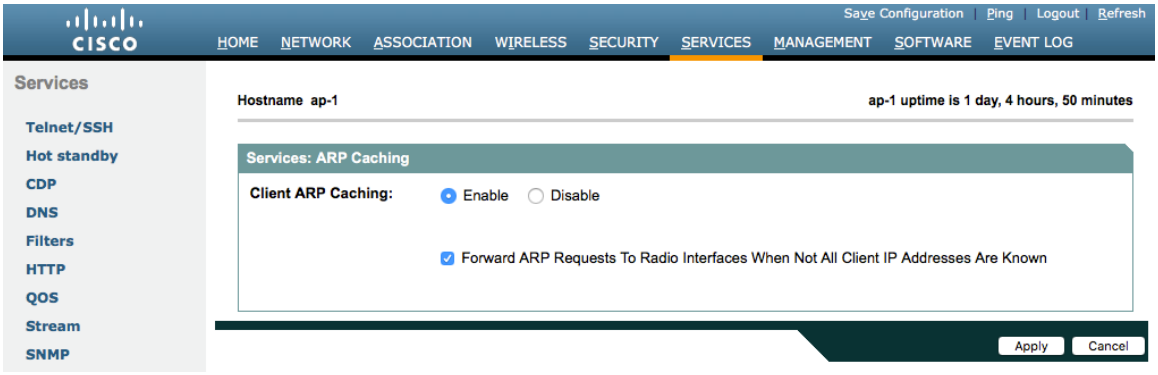


電源管理

プロキシ ARP は、デバイスに代わって ARP 要求に応答するのに役立ちます。

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。



設定例

```
version 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
!
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 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
!
sntp server 10.0.0.2
sntp 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。

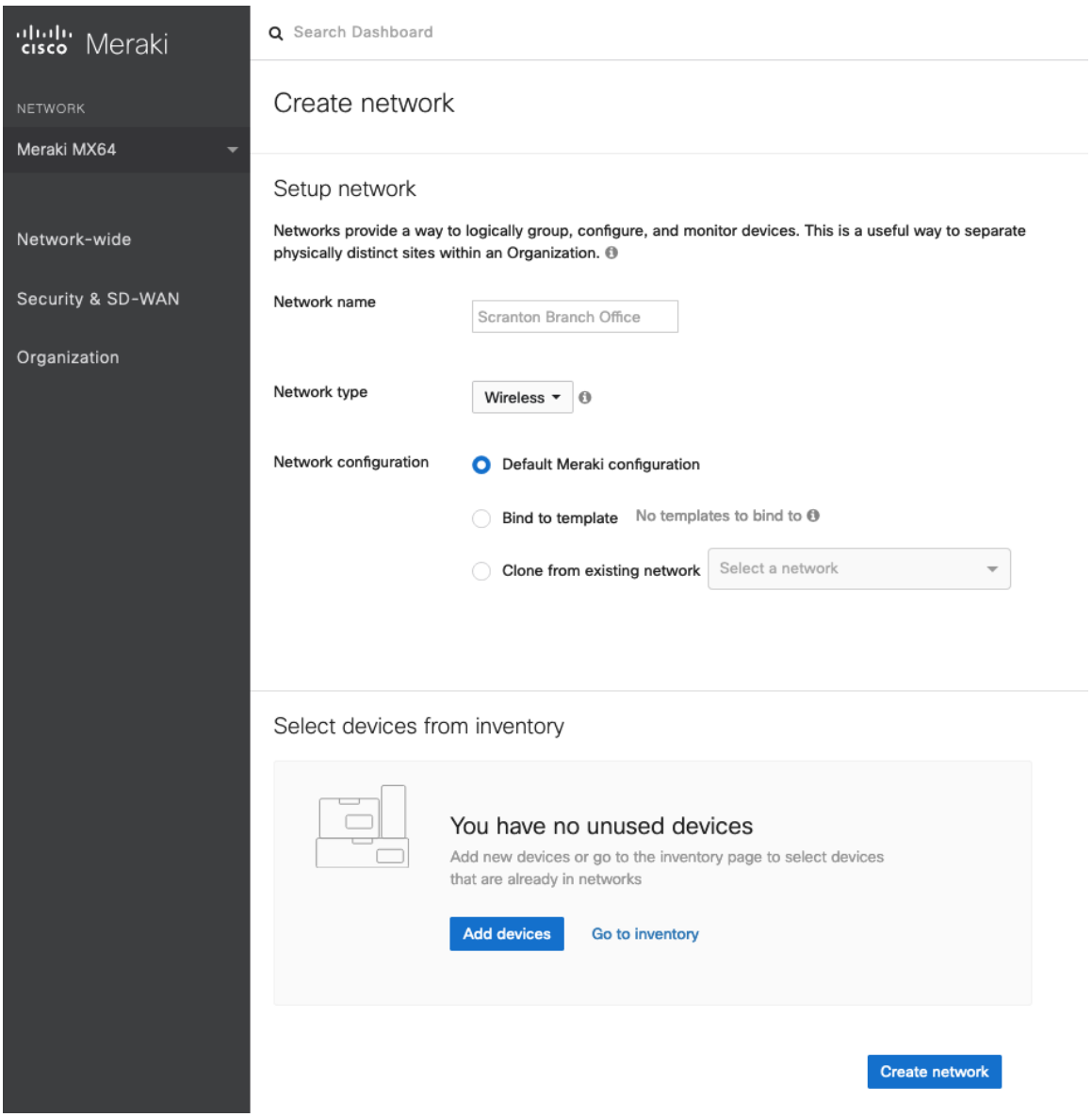
- **[スプラッシュページ（Splash page）]** を **[なし（None）]** に設定します。
- **[ブリッジモード（Bridge mode）]** を有効にします。
- **[VLAN タギング（VLAN tagging）]** を有効にします。
- **[帯域選択（Band selection）]** を **[5 GHz 帯域のみ（5 GHz band only）]** に設定します。
- 必要に応じて **[データレート（Data Rates）]** を設定します
- **[Quality of Service（QoS）]** を設定します。

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。

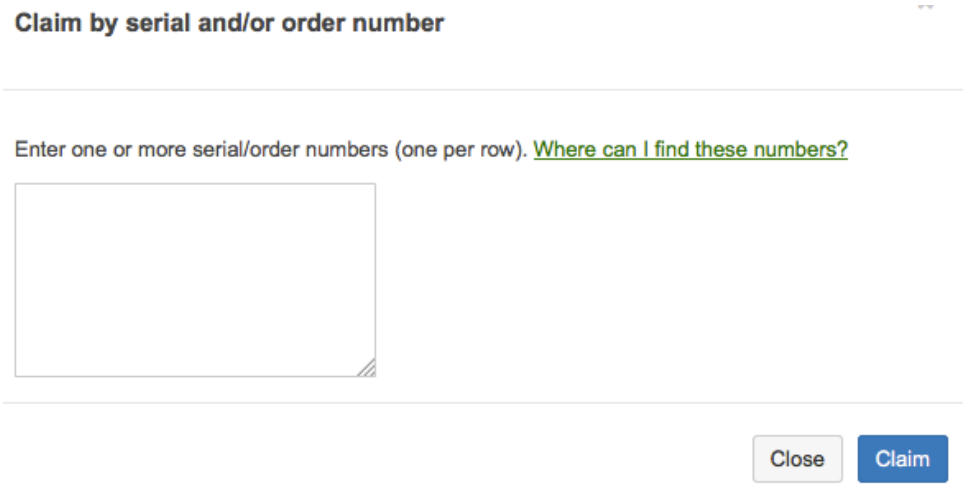


Cisco Meraki アクセス ポイントは、シリアル番号または注文番号を指定して要求できます。

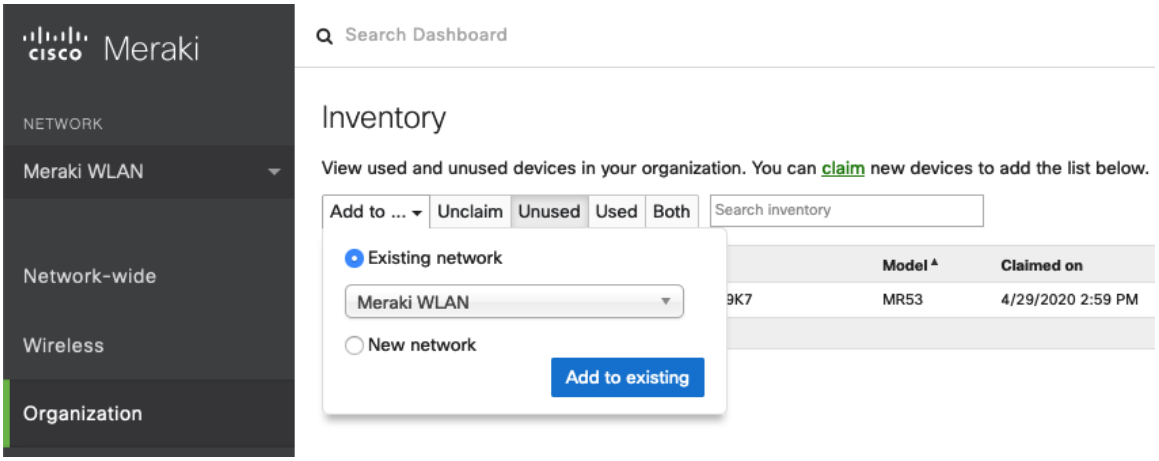
要求した Cisco Meraki アクセス ポイントは、使用可能なインベントリに表示されます。

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。

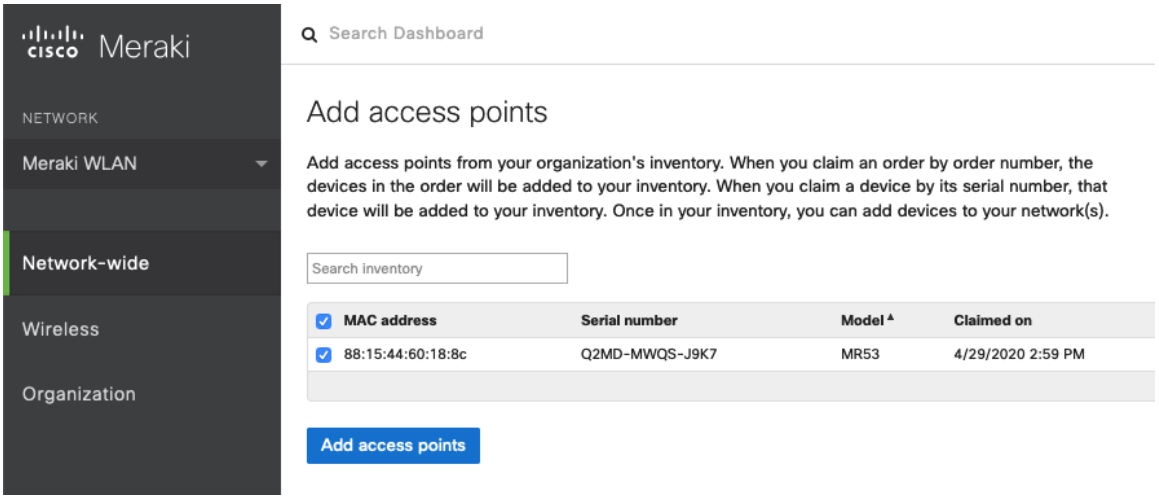
また、**[ワイヤレス（Wireless）] > [モニター（Monitor）] > [アクセスポイント（Access points）]** ページで **[AP の追加（Add AP）]** を選択し、**[要求（Claim）]** を選択して要求することもできます。



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。



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。



SSID の設定

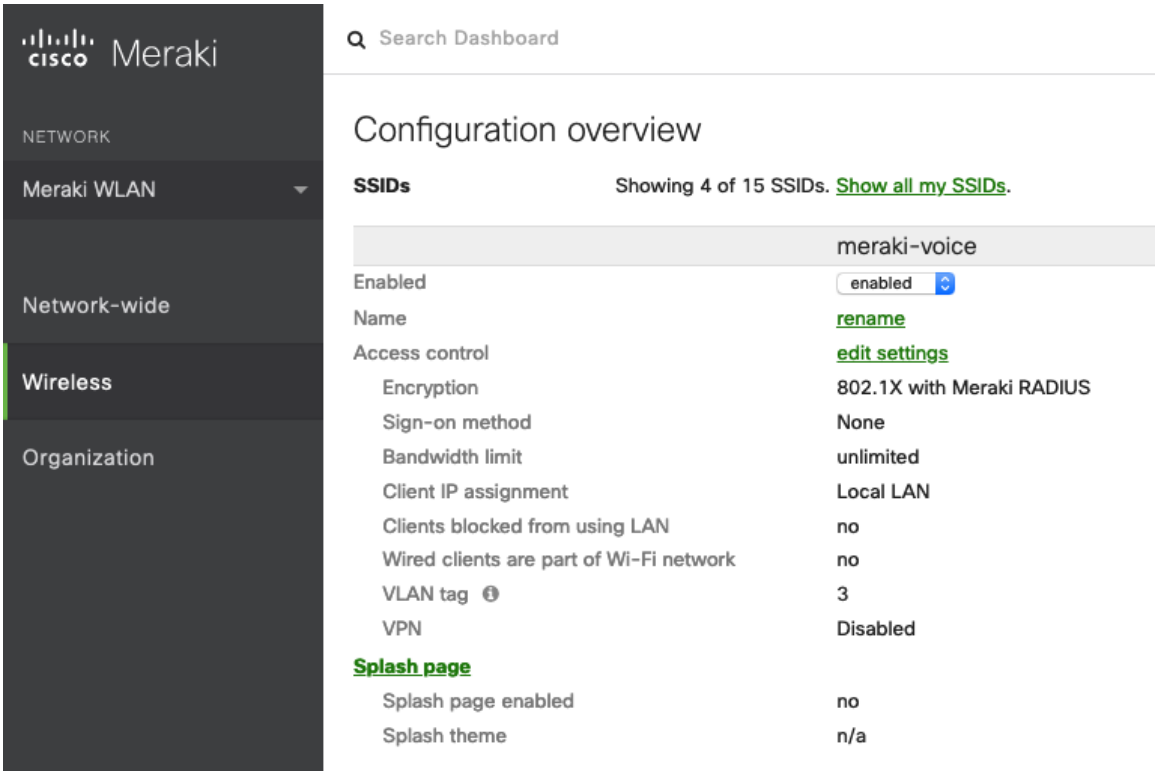
SSID を作成するには、ドロップダウン メニューから対象ネットワークを選択し、**[ワイヤレス（Wireless）] > [設定（Configure）] > [SSID（SSIDs）]** を選択します。

Webex Desk Series 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。



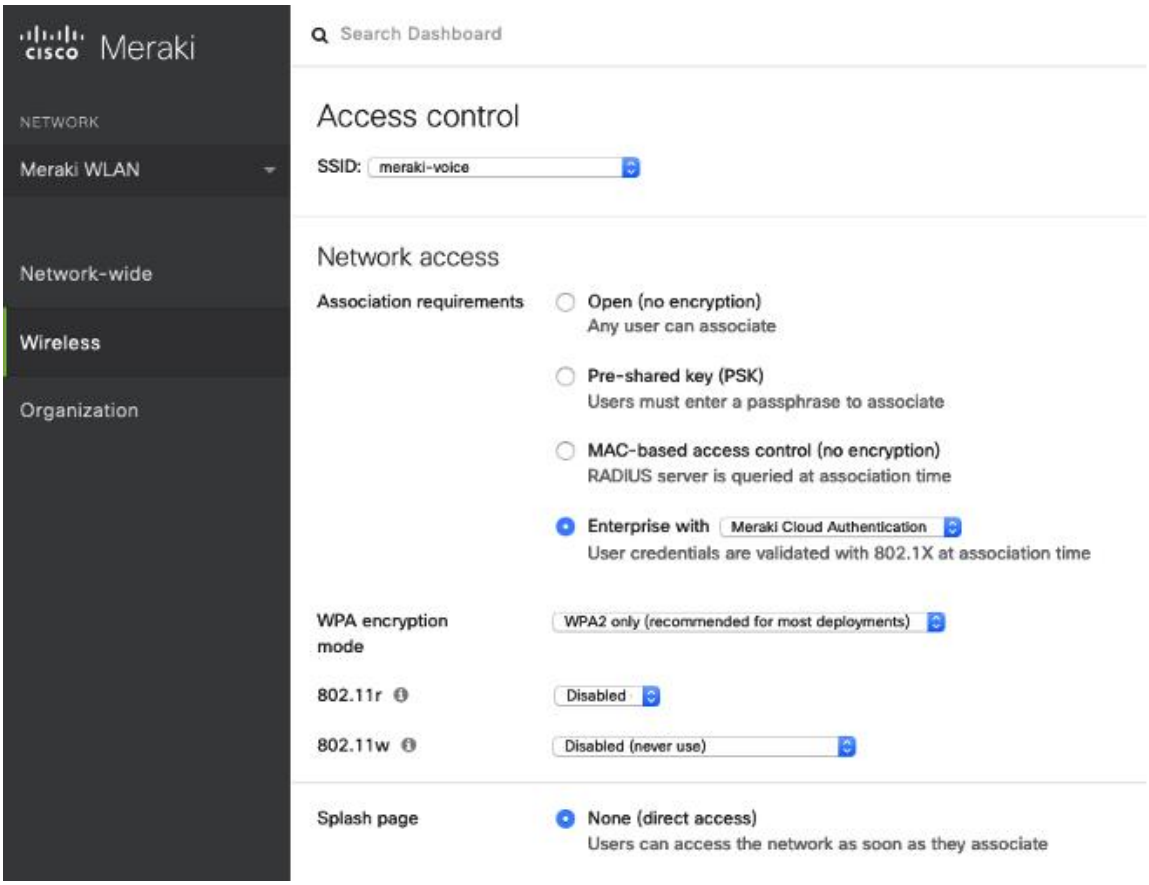
[ワイヤレス（Wireless）] > [設定（Configure）] > [アクセス制御（Access control）] ページで、**[WPA2-Enterprise]** を選択して 802.1x 認証を有効にします。

[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。

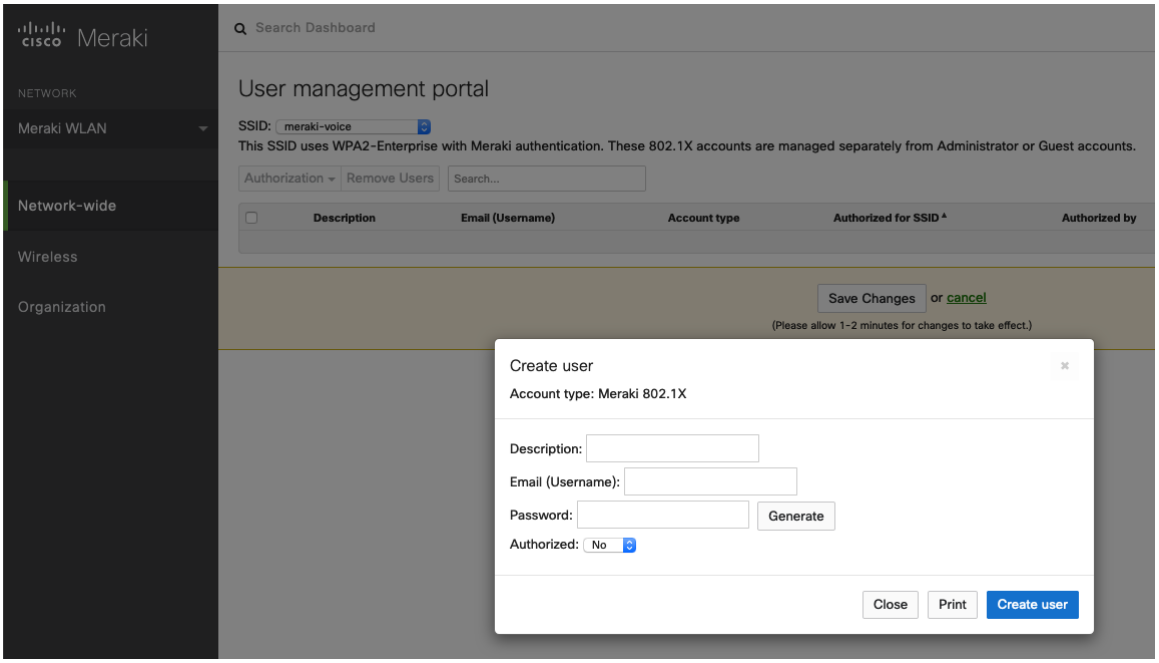
他の認証タイプ（事前共有キーなど）も使用できます。

[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。



[WPA2-Enterprise] が有効になっている環境で Cisco Meraki 認証サーバーを RADIUS サーバー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、Webex Desk Series が 802.1x 認証に認証サーバーを使用するように設定する必要があります。

注：Cisco Meraki アクセスポイントは EAP-FAST をサポートしません。



[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、Webex Desk Series は、呼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、Cisco Meraki 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。

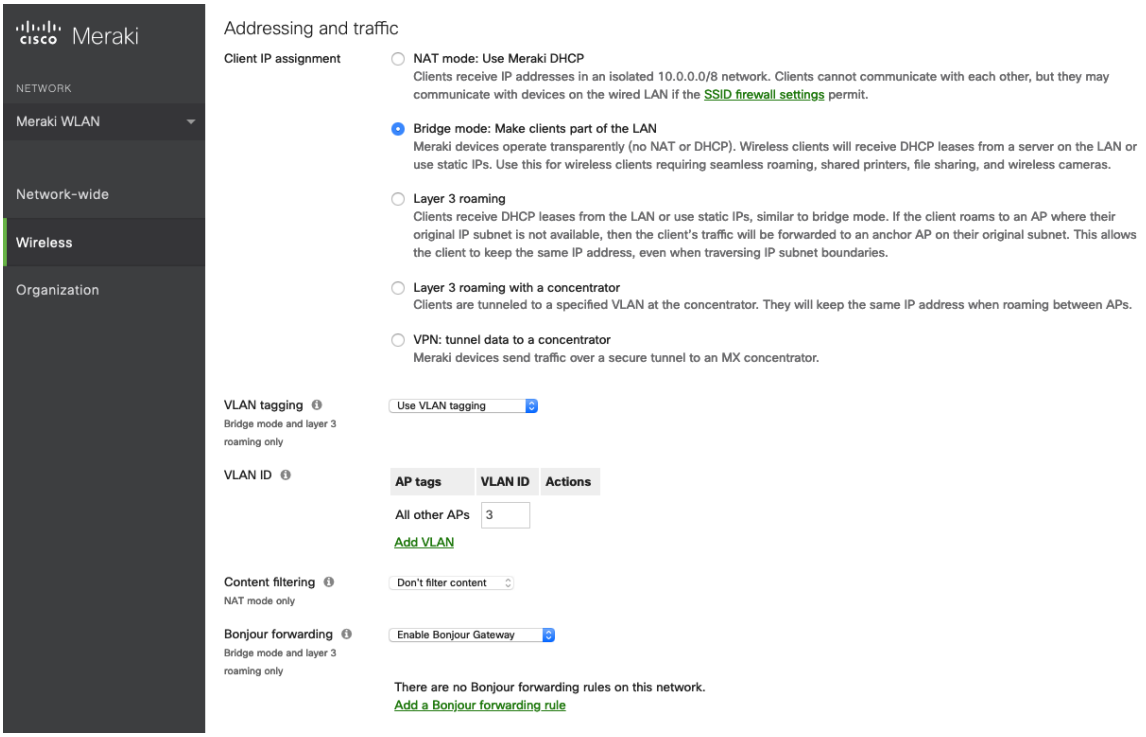
VLAN タギングを使用する場合は、VLAN を許可するトランク モードに設定されたスイッチ ポートに、Cisco Meraki アクセス ポイントが接続されることを確認します。

Cisco Meraki MS スイッチを使用する場合は、『Cisco Meraki MS Switch VoIP Deployment Guide（Cisco Meraki MS スイッチ 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
```



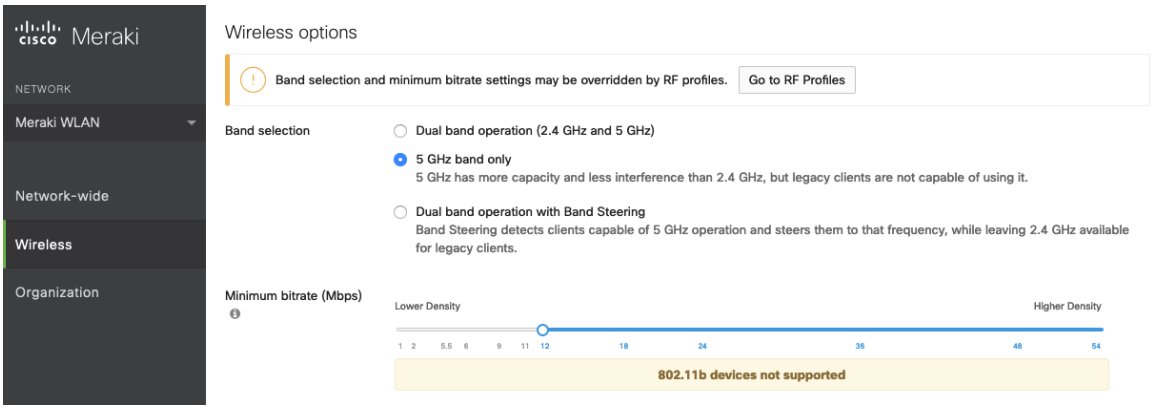
[ワイヤレス（Wireless）] > [設定（Configure）] > [アクセス制御（Access control）] ページでは、必要に応じて Webex Desk Series で使用する SSID の周波数帯域を設定できます。

Webex Desk Series は、5 GHz 帯域で動作させる場合は、**[5 GHz 帯域のみ（5 GHz band only）]** を選択することをお勧めします。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。

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。

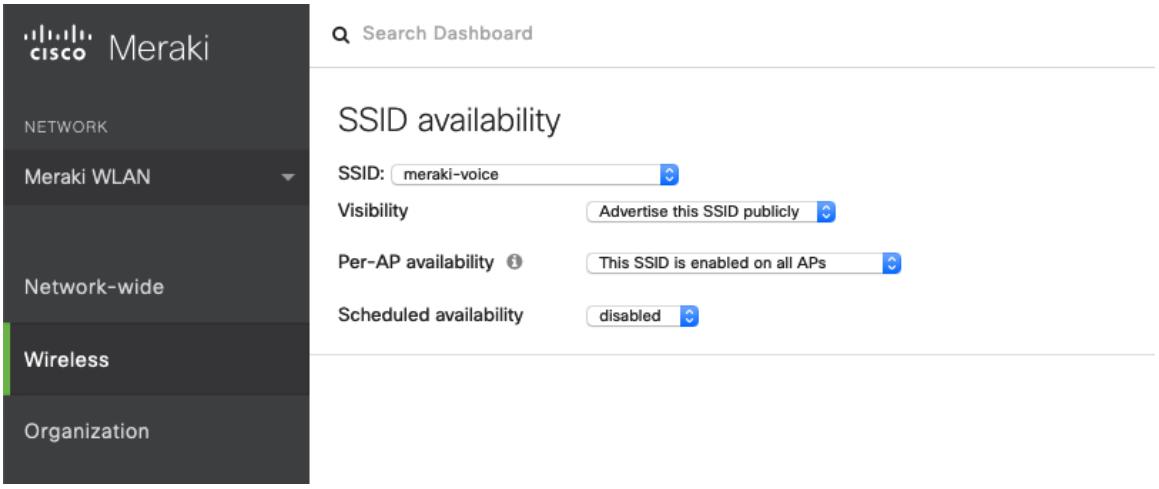
Cisco Meraki アクセスポイントは現在、DTIM 周期**「1」**、ビーコン周期**「100 ミリ秒」**を使用します。どちらも設定を変更することはできません。



[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 をブロードキャストできます。

[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。

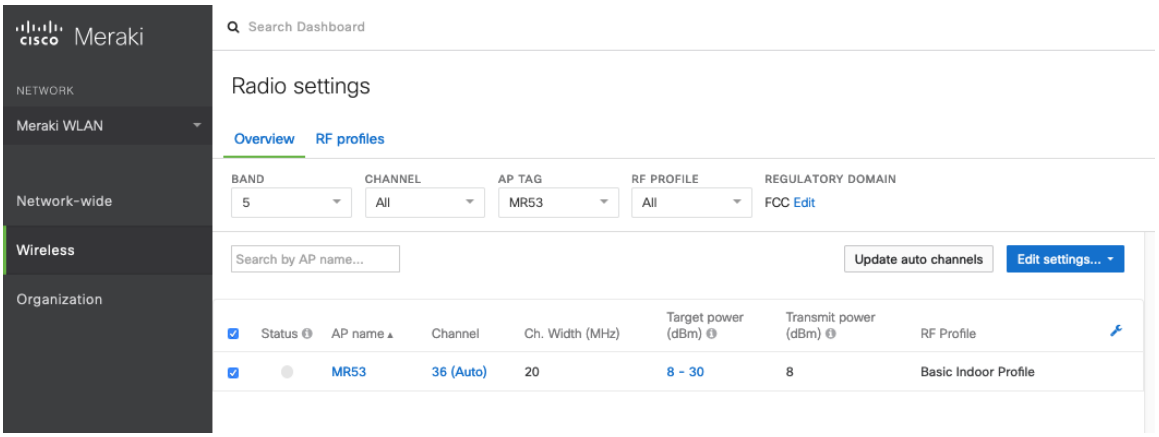


無線の設定

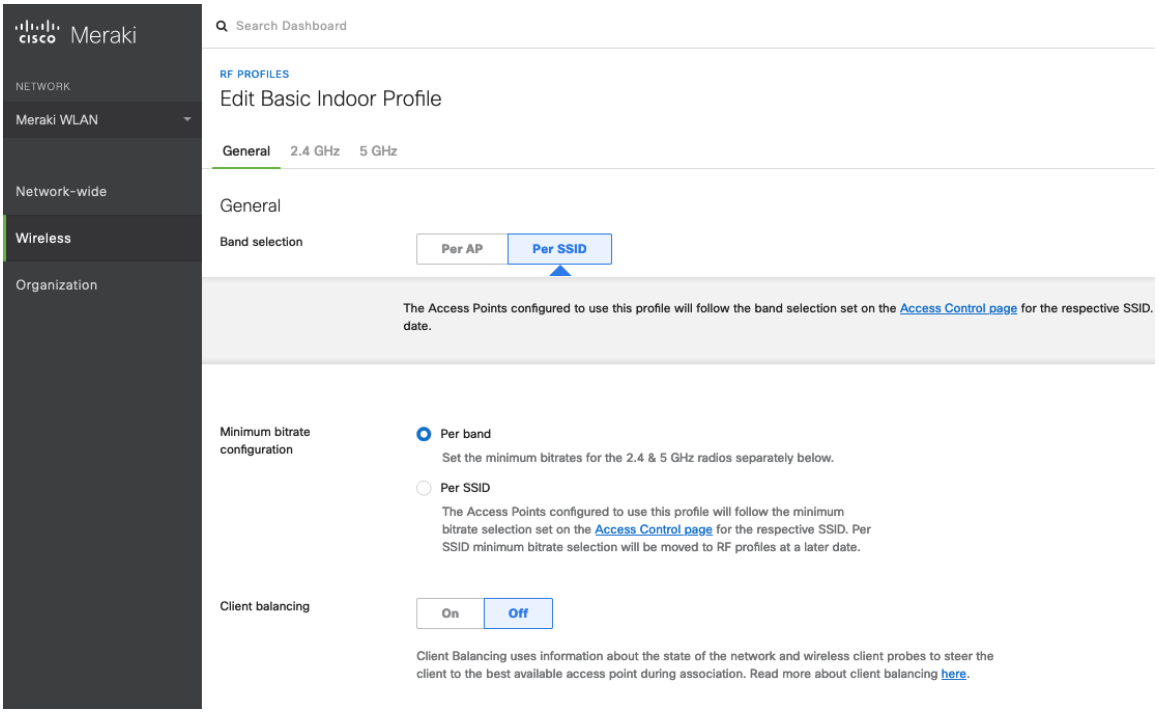
[ワイヤレス（Wireless）] > [構成（Configure）] > [無線設定（Radio settings）] ページで、アクセスポイントを一括または個別に構成して、自動または手動のチャンネルと送信電力設定を定義できます。

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になることがあります。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。



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。**



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。

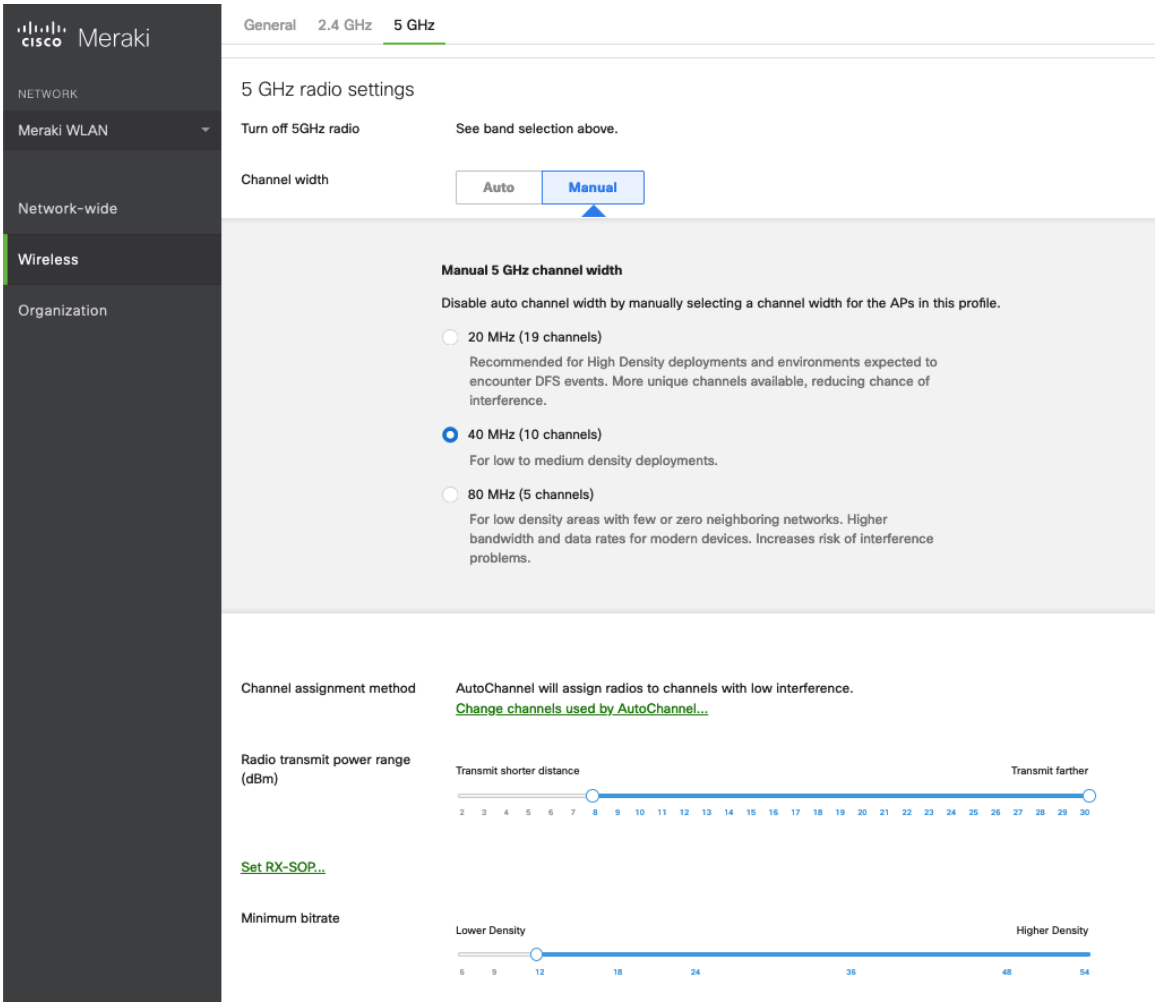
[AutoChannel] で使用される 5 GHz チャンネルも RF プロファイルで設定できます。

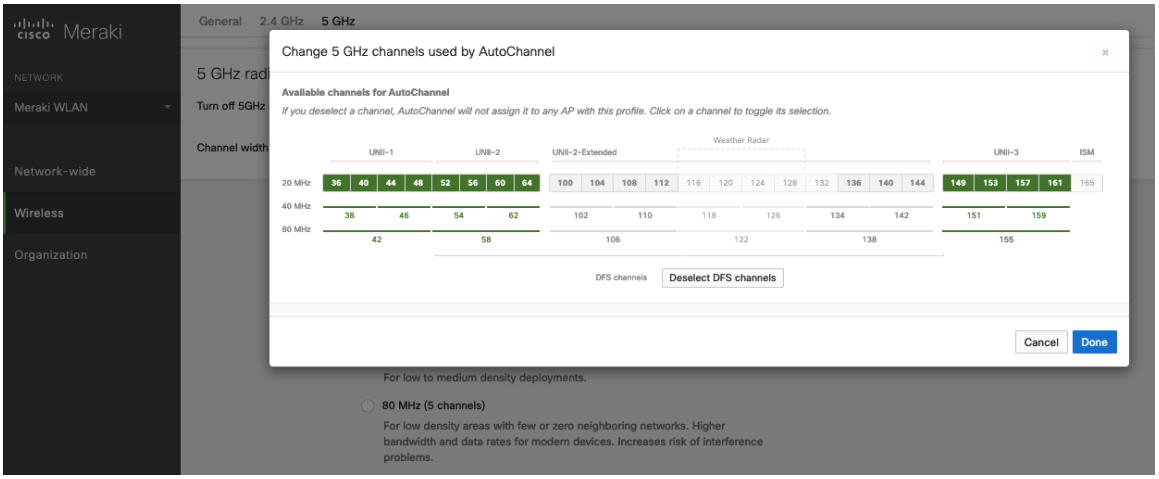
[AutoChannel] で使用される 2.4 GHz チャンネルは、チャンネル 1、6、および 11 のみに制限されています。

[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。





ファイアウォール & トラフィック シェーピング

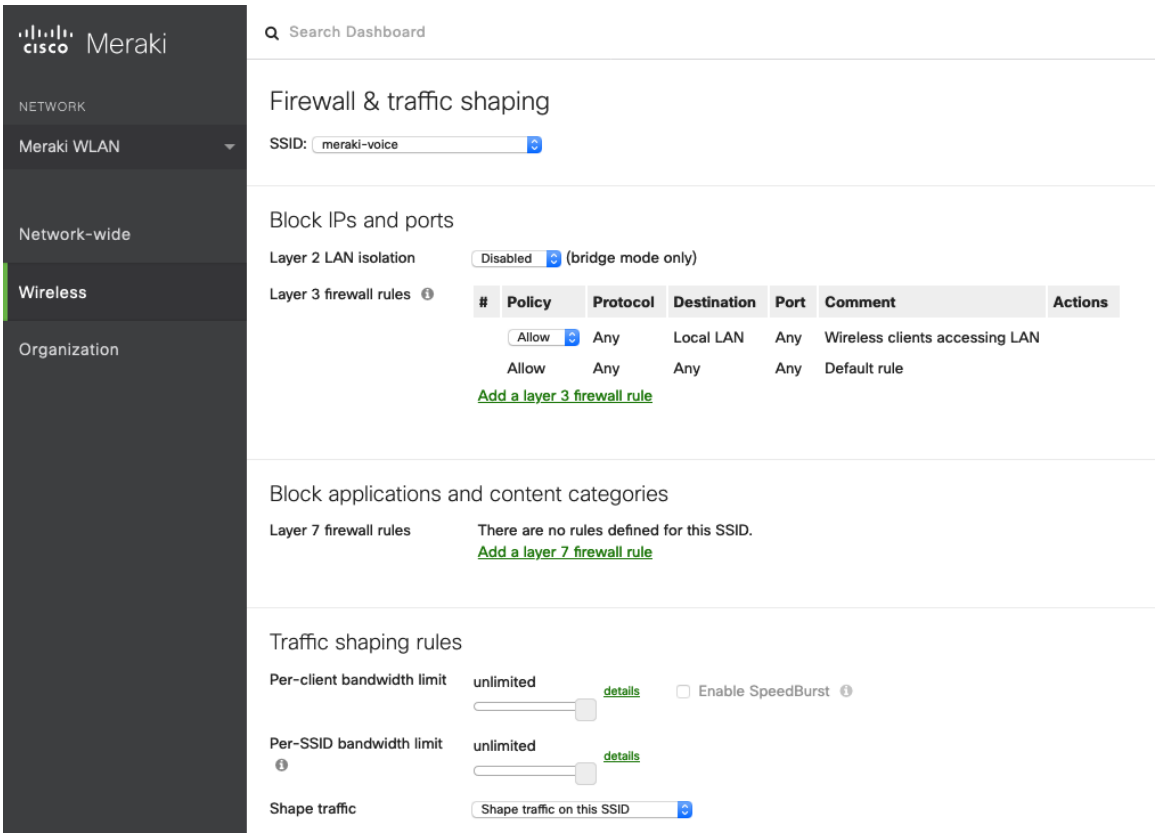
[ワイヤレス（Wireless）] > [設定（Configure）] > [ファイアウォールとトラフィックシェーピング（Firewall & traffic shaping）] ページでは、トラフィック シェーピング ルールを定義できます。

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。

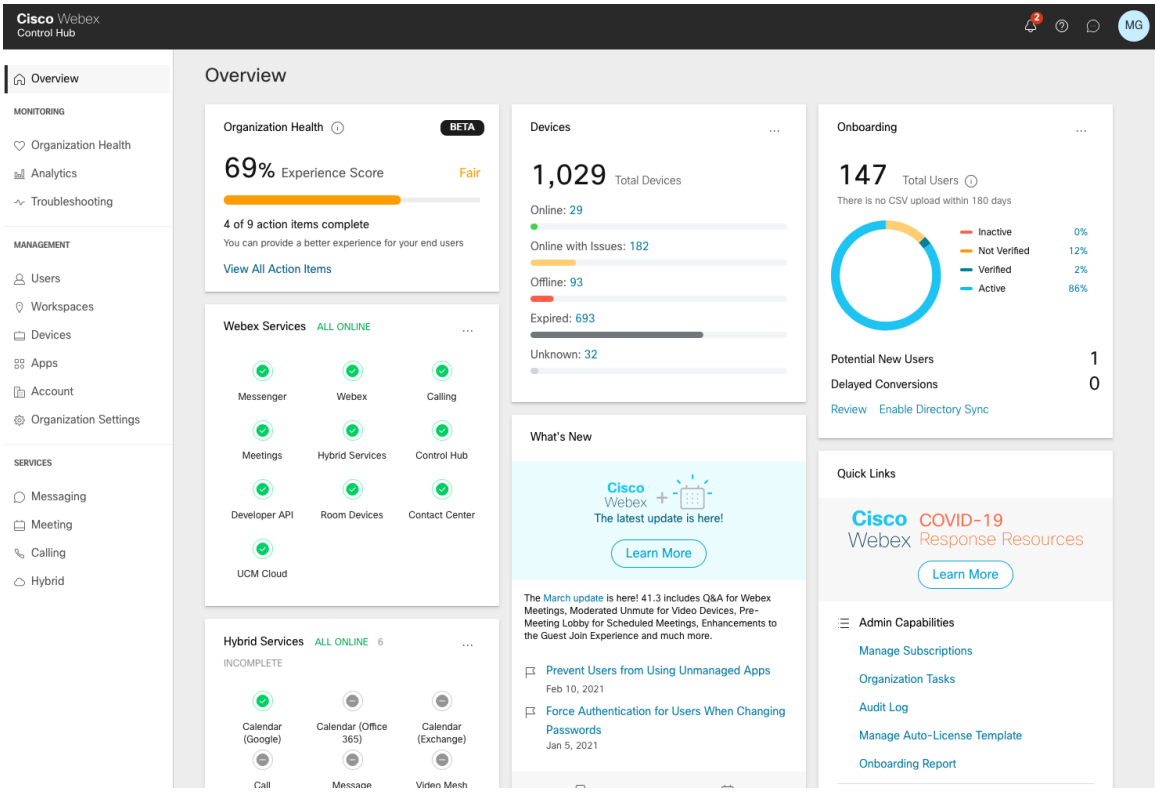


注：Cisco Meraki アクセスポイントでは、コールアドミッション制御/トラフィック仕様（TSPEC）をサポートしません。

Cisco Call Control の設定

Webex

Webex はクラウド登録を有効にするため、Webex Desk Series 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。



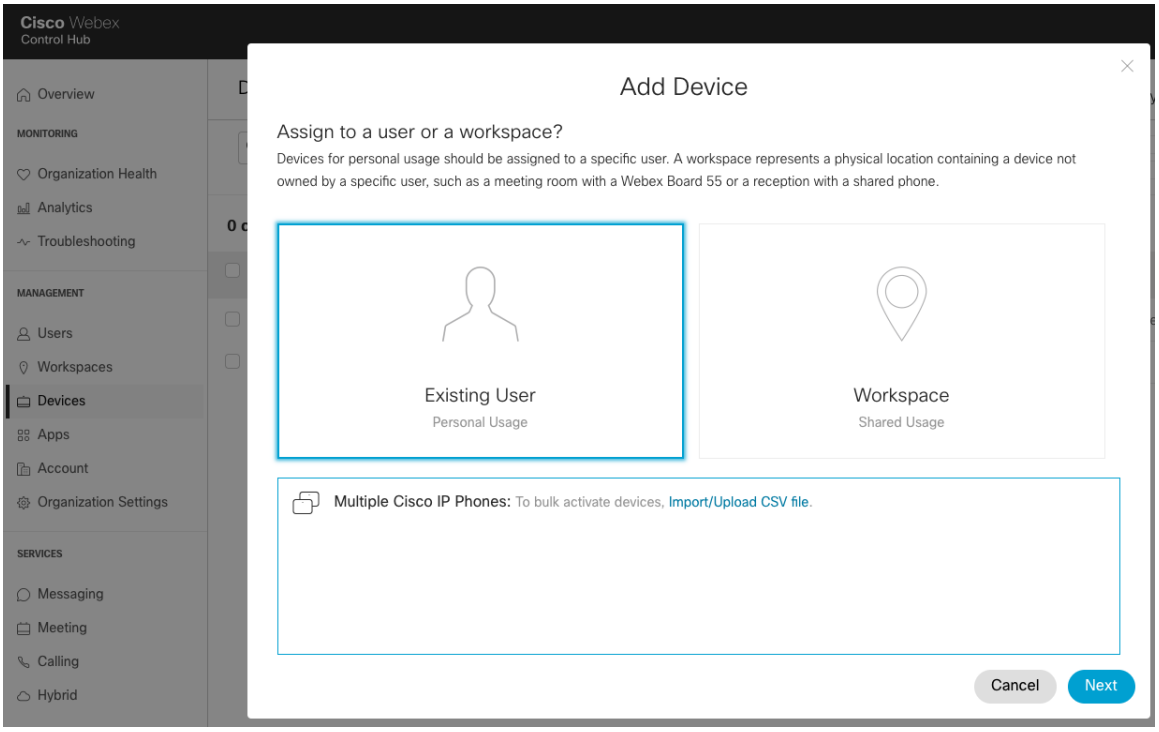
Webex Desk Series は、Webex に追加して、個人使用または共有使用のワークスペースとしてユーザーに割り当てることができます。

個人的な使用

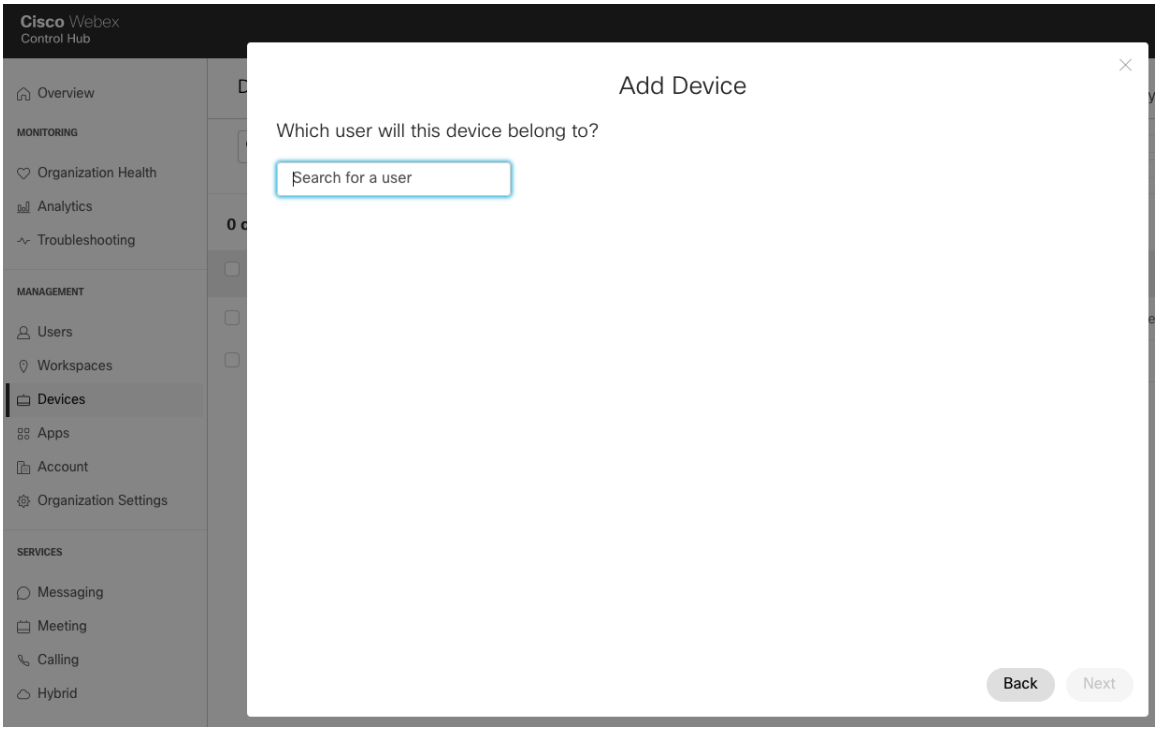
Webex Desk Series は、**[デバイス（Devices）]** 経由でユーザーが個人的に使用できるように構成できます。

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。



Webex Desk Series を割り当てるユーザーを検索し、**[次へ（Next）]** をクリックします。



Webex Desk Series に入力する **[アクティベーションコード（Activation Code）]** が表示されます。

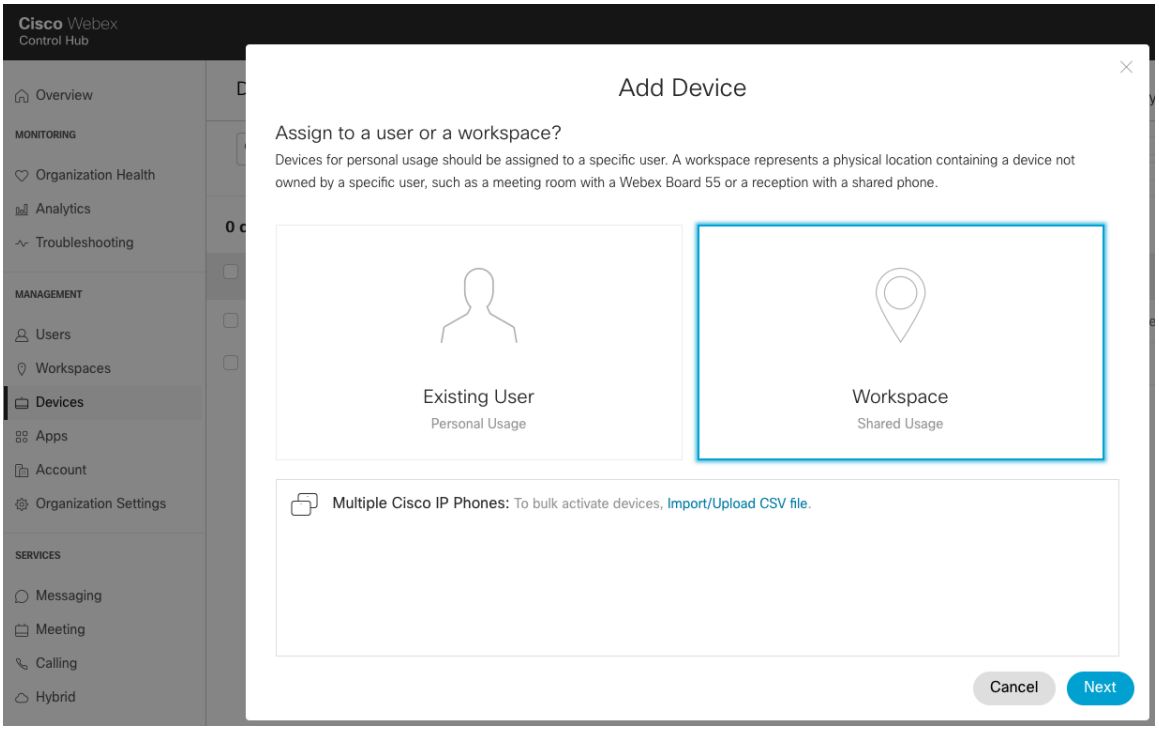
[ユーザー（Users）] でユーザーを選択して、サービスを設定または変更します。

共同利用

Webex Desk Series は、**[デバイス（Devices）]** または **[ワークスペース（Workspaces）]** を介してワークスペースとして設定できます。

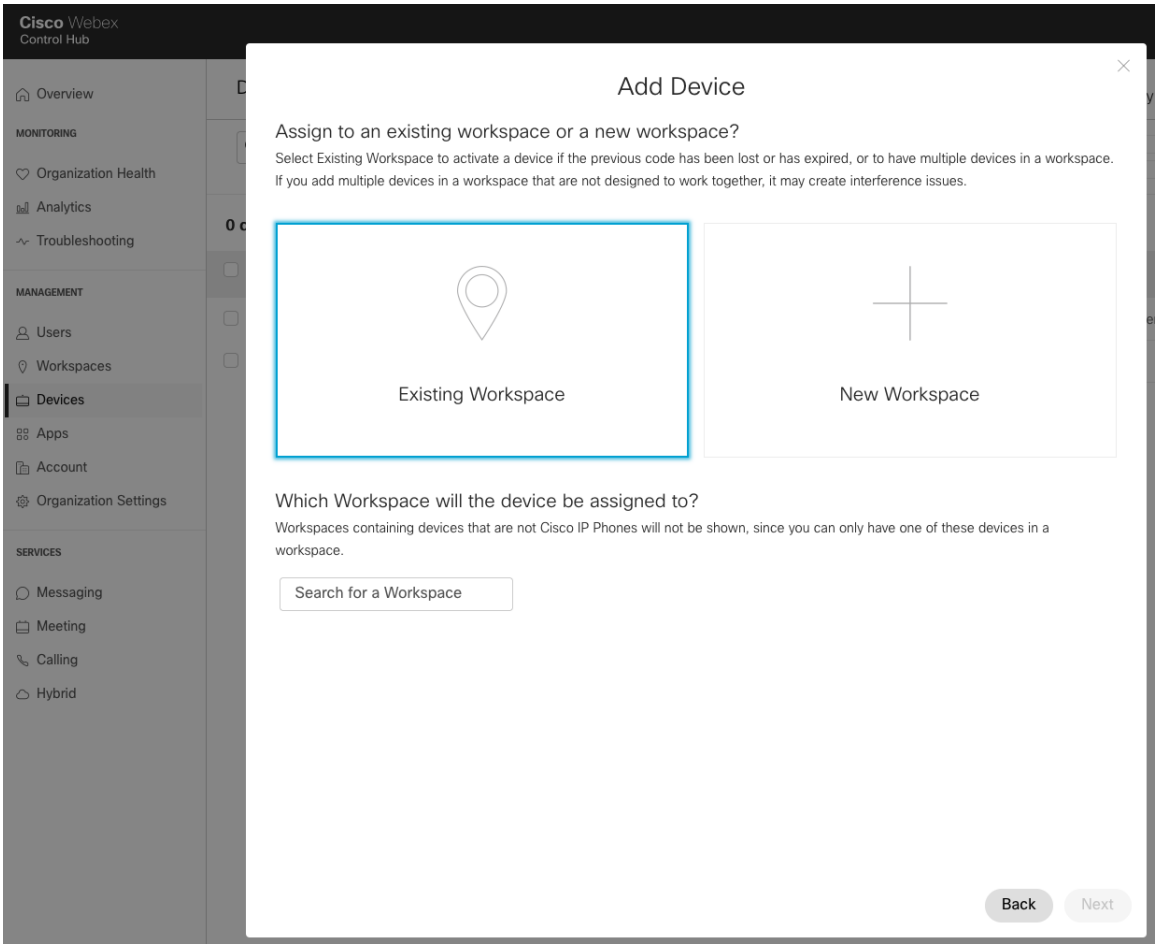
[デバイス（Devices）] を介してワークスペースを追加するには、**[デバイス（Devices）]** に移動し、**[デバイスの追加（Add Device）]** を選択します。

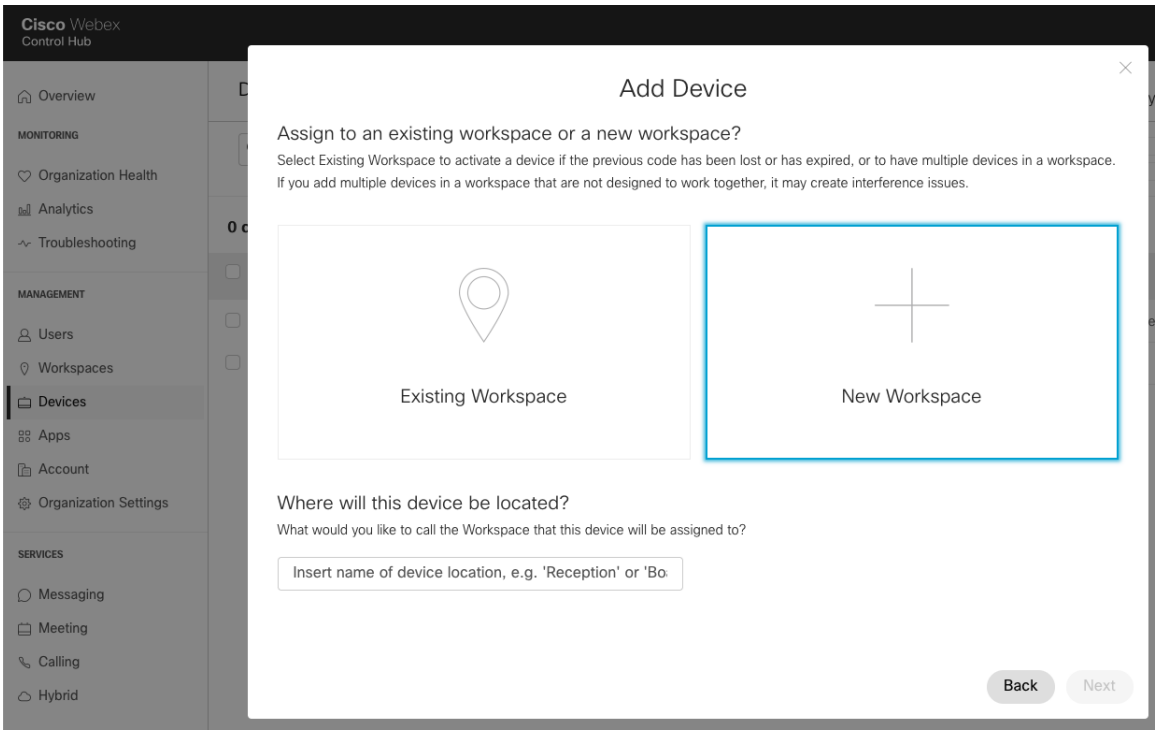
次の画面で、**[ワークスペース（Workspace）]** を選択し、**[次へ（Next）]** をクリックします。



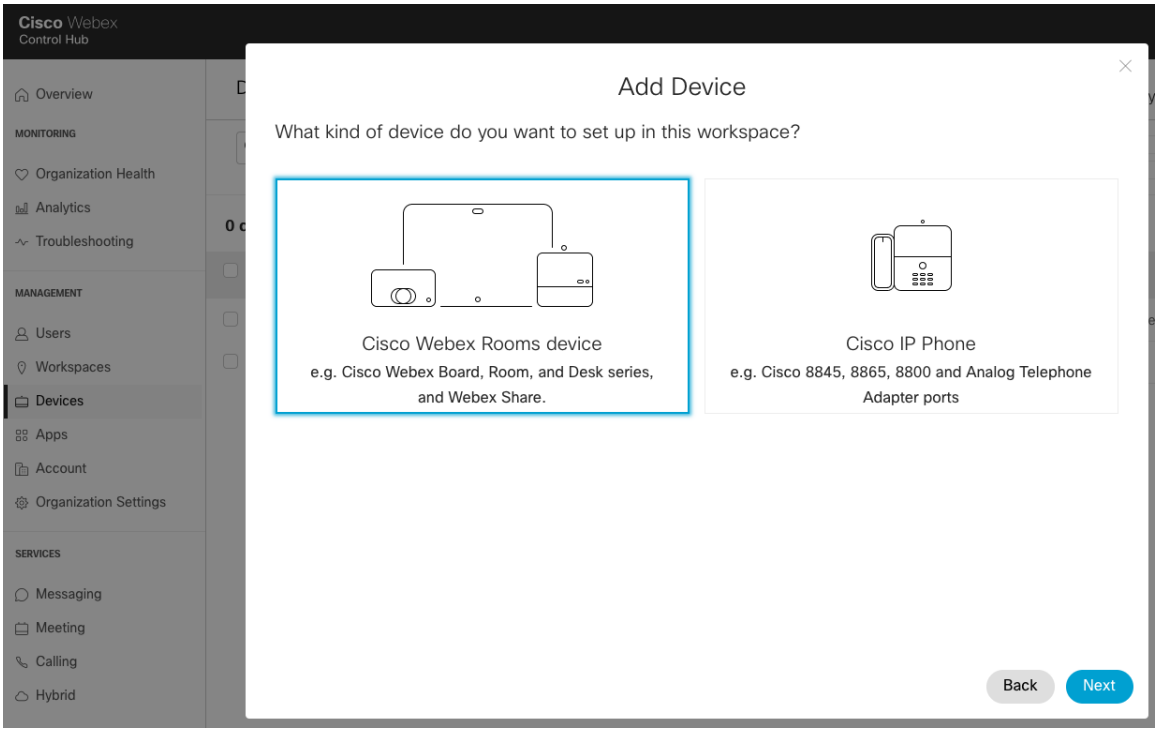
[既存のワークスペース（Existing Workspace）] **または** [新しいワークスペース（New Workspace）] **を選択します。**

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。

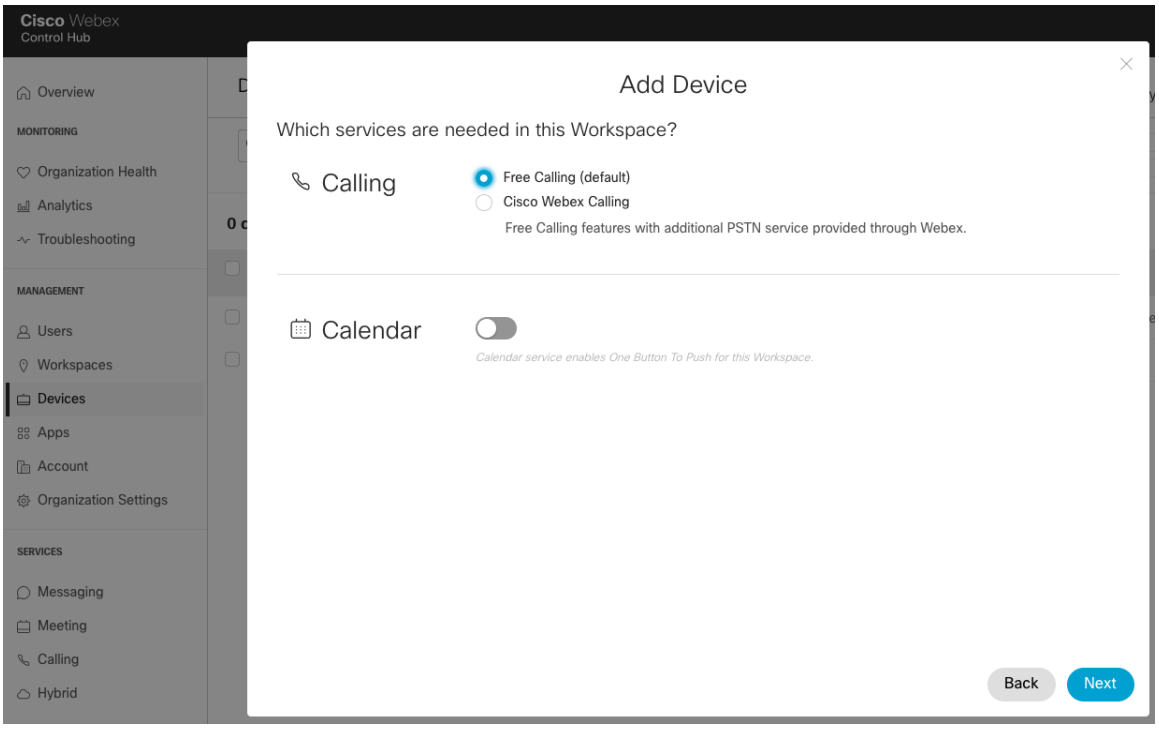




以前に **[新しいワークスペース（New Workspace）]** が選択されていた場合は、**[Webex ルームデバイス（Webex Rooms device）]** を選択し、**[次へ（Next）]** をクリックします。



さらに、**[新しいワークスペース（New Workspace）]** を選択した場合は、必要なサービスを設定してから、**[次へ（Next）]** をクリックします。



Webex Desk Series に入力する **[アクティベーションコード（Activation Code）]** が表示されます。

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。

Webex のネットワーク要件については、次の URL にある Webex Services ドキュメントのネットワーク要件を参照してください。

https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Services#id_135011

詳細については、『Webex Desk Series 管理者ガイド』を参照してください。

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

Cisco Unified Communications Manager

Cisco Unified Communications Manager は、さまざまな製品、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 Webex Desk Series のデバイスタイプを有効にするには、対応するデバイスパッケージの 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。

デバイスパッケージの 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。

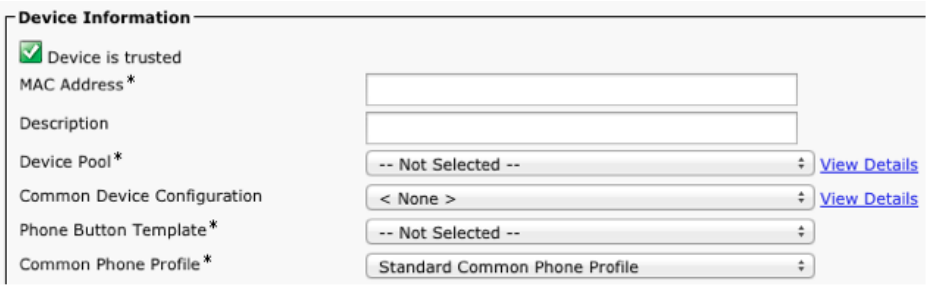
  注：サブスクライバノードの Cisco CallManager サービスを再起動する必要はありません。

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 Operating System Administration Guide（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

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

イーサネット MAC アドレスは、Webex Desk Series で **[バージョン情報（About）]** または **[設定（Settings）] > [このデバイスについて（About this device）]** に移動して見つけることができます。

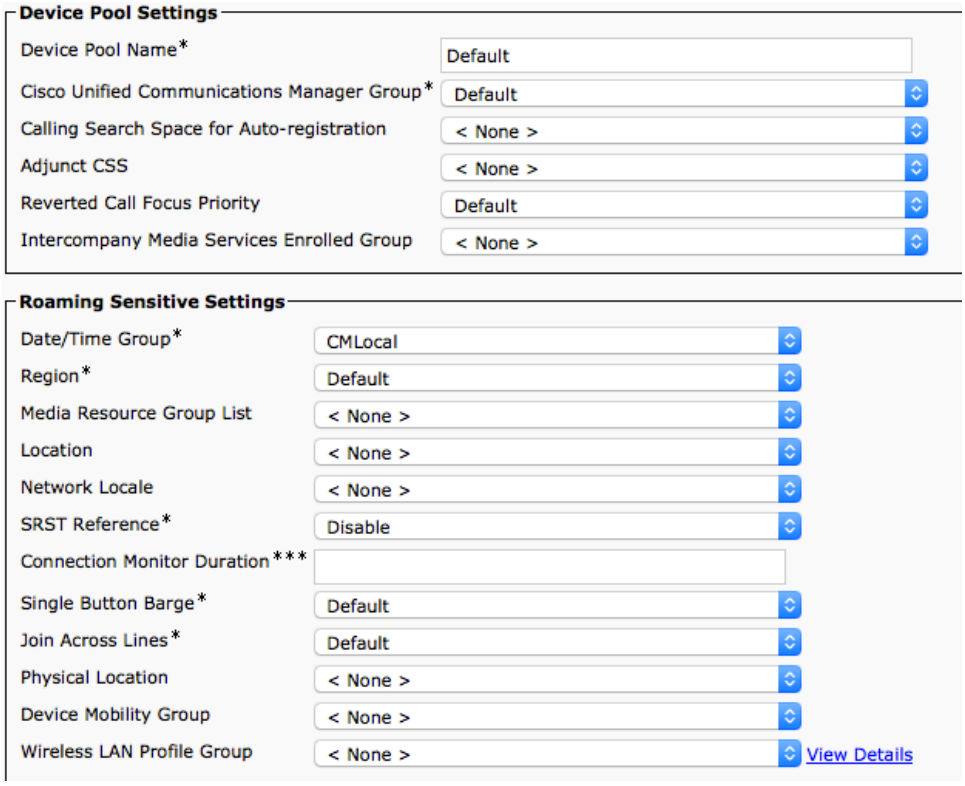


[デバイスプール（Device Pools）]

新しい Webex Desk Series を作成するときは、**[デバイスプール（Device Pool）]** 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。

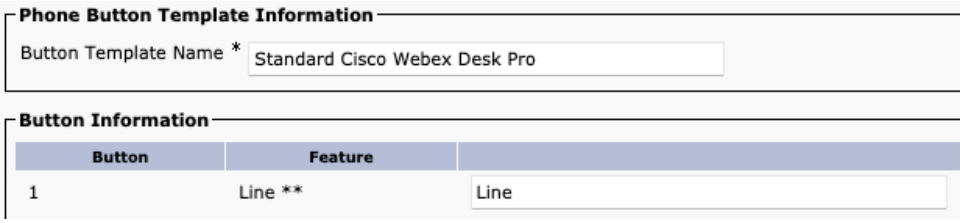
デバイス プールを使用すると、デバイスを場所別、モデル タイプ別などにグループ化できます。



電話ボタン テンプレート

新しい Webex Desk Series を作成するときは、**[電話ボタンテンプレート（Phone Button Template）]** を構成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。



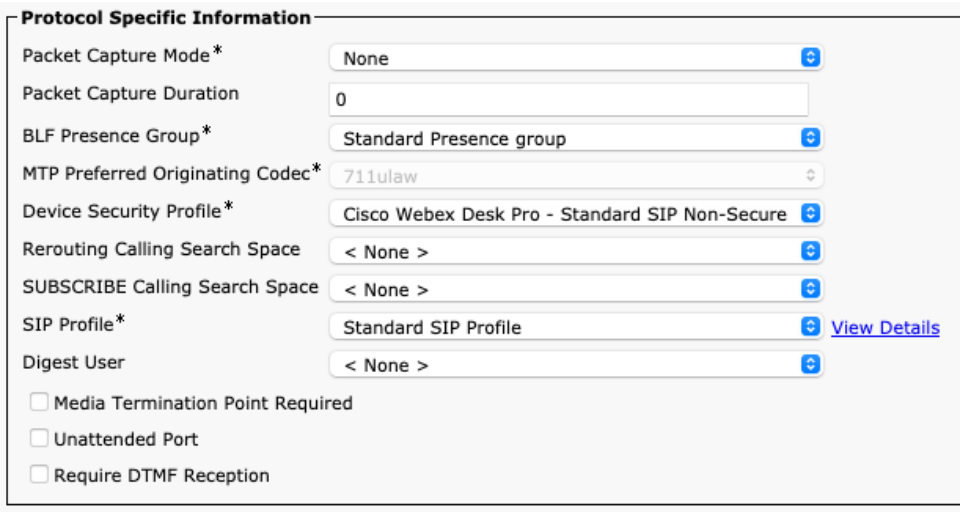
セキュリティ プロファイル

新しい Webex Desk Series を作成するときは、**[デバイス セキュリティ プロファイル（Device Security Profile）]** を設定する必要があります。

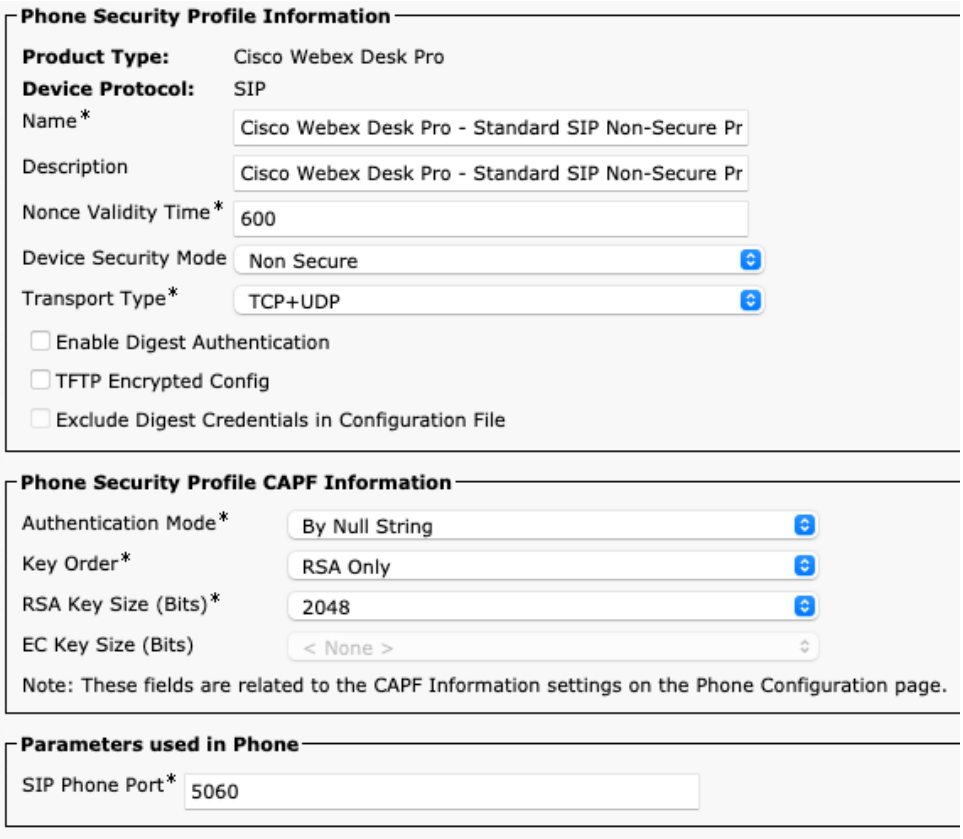
セキュリティ プロファイルを使用すると、認証モードや暗号化モードを有効にできます。暗号化モードを有効にすると、シグナリング、メディア、および設定ファイルの暗号化が有効になります。

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。

Webex Desk Series には、セキュリティプロファイルも参照できる Manufacturing Installed Certificate（MIC）があります。



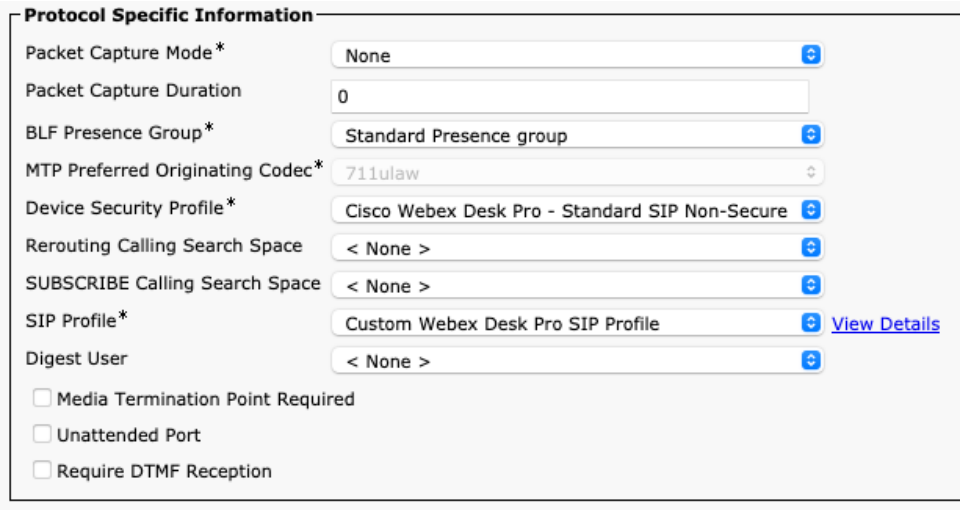
デフォルトのデバイス セキュリティ プロファイルは、暗号化を使用しない、**Standard SIP Non-Secure Profile** です。



SIP プロファイル

新しい Webex Desk Series を作成するときは、**[SIP プロファイル（SIP Profile）]** を設定する必要があります。

Webex Desk Series のカスタム SIP プロファイルを作成することをお勧めします（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）。



Webex Desk Series 用のカスタム 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。**

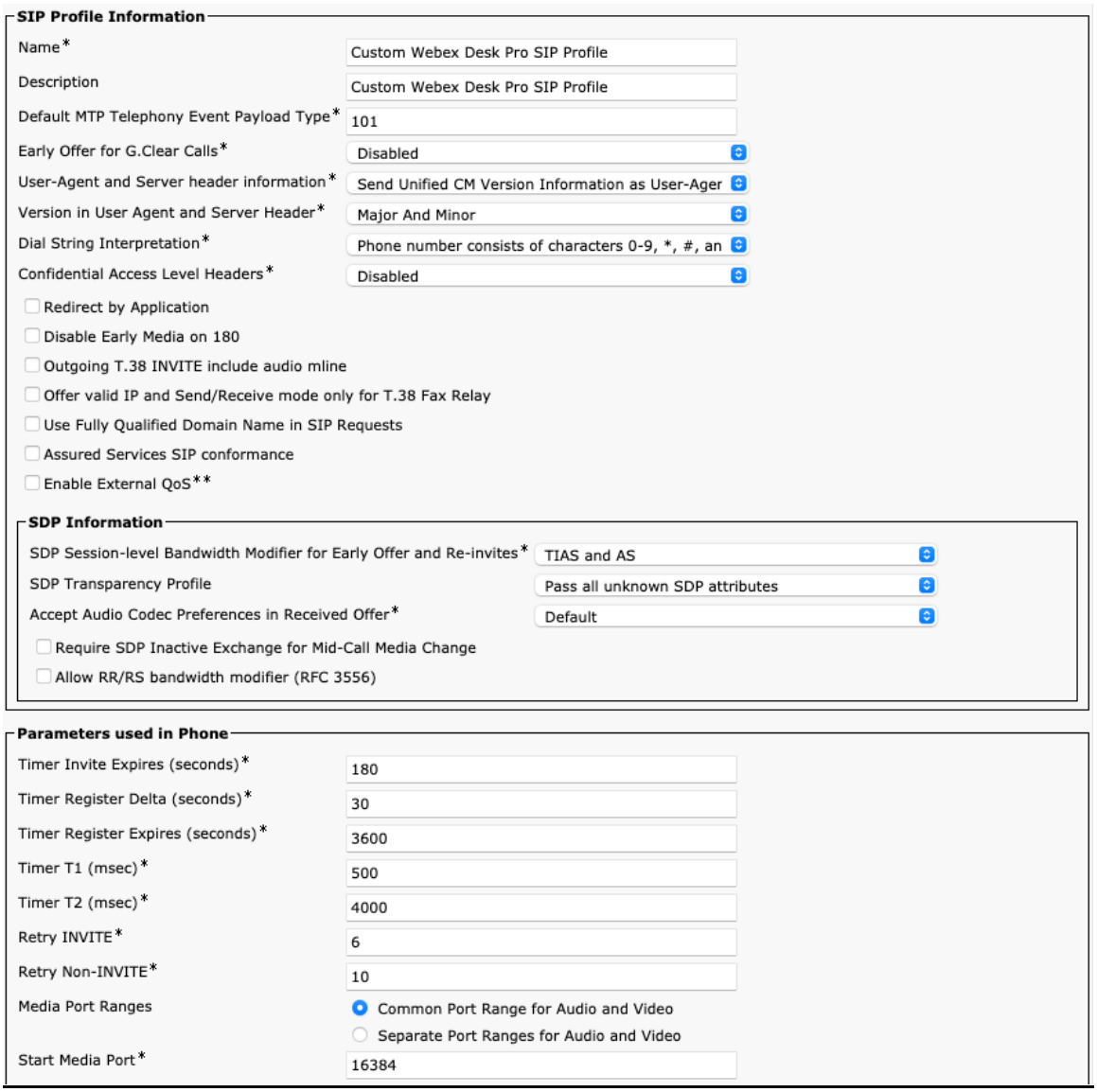
[キープアライブのタイムアウト値（秒）（Timer Keep Alive Expires（seconds））]：300**（デフォルトは 120）に設定。**

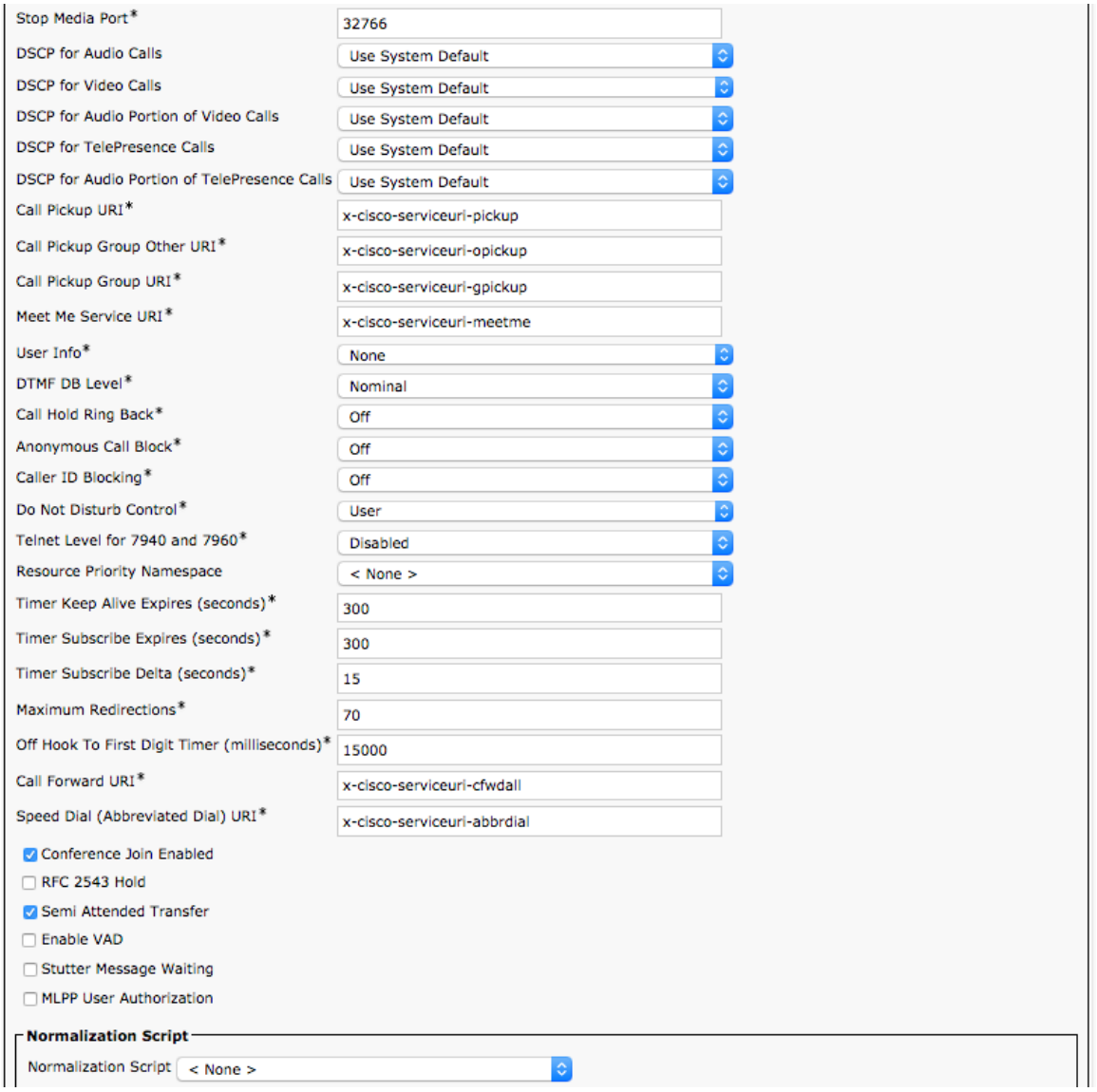
[サブスクライブのタイムアウト値（秒）（Timer Subscribe Expires（seconds））]：300**（デフォルトは 120）に設定。**

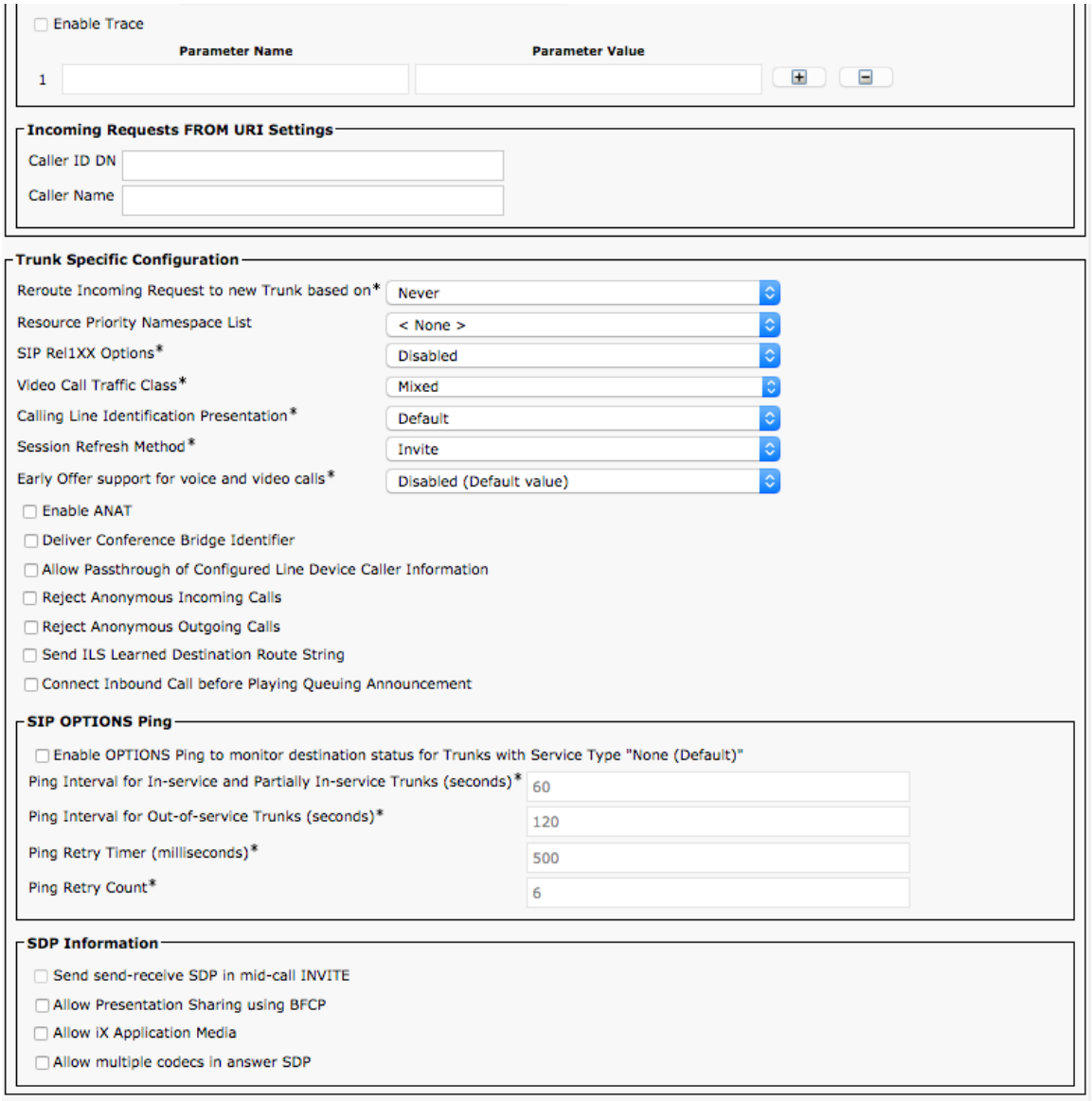
[サブスクライブの再送間隔の調整値（秒）（Timer Subscribe Delta（seconds））]：15**（デフォルトは 5）に設定。**

[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 Webex Desk Pro SIP Profile
Description
Custom Webex Desk Pro 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-Ager
Version in User Agent and Server Header*
Major And Minor
Dial String Interpretation*
Phone number consists of characters 0-9, *, #, an
Confidential Access Level Headers*
Disabled
Redirect by Application
Disable Early Media on 180
Outgoing T.38 INVITE include audio mline
Offer valid IP and Send/Receive mode only for T.38 Fax Relay
Use Fully Qualified Domain Name in SIP Requests
Assured Services SIP conformance
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
Require SDP Inactive Exchange for Mid-Call Media Change
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
Common Port Range for Audio and Video
Separate Port Ranges for Audio and Video
Start Media Port*
16384


Stop Media Port*
32766
DSCP for Audio Calls
Use System Default
DSCP for Video Calls
Use System Default
DSCP for Audio Portion of Video Calls
Use System Default
DSCP for TelePresence Calls
Use System Default
DSCP for Audio Portion of TelePresence Calls
Use System Default
Call Pickup URI*
x-cisco-serviceuri-pickup
Call Pickup Group Other URI*
x-cisco-serviceuri-opickup
Call Pickup Group URI*
x-cisco-serviceuri-gpickup
Meet Me Service URI*
x-cisco-serviceuri-meetme
User Info*
None
DTMF DB Level*
Nominal
Call Hold Ring Back*
Off
Anonymous Call Block*
Off
Caller ID Blocking*
Off
Do Not Disturb Control*
User
Telnet Level for 7940 and 7960*
Disabled
Resource Priority Namespace
< None >
Timer Keep Alive Expires (seconds)*
300
Timer Subscribe Expires (seconds)*
300
Timer Subscribe Delta (seconds)*
15
Maximum Redirections*
70
Off Hook To First Digit Timer (milliseconds)*
15000
Call Forward URI*
x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*
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
< None >

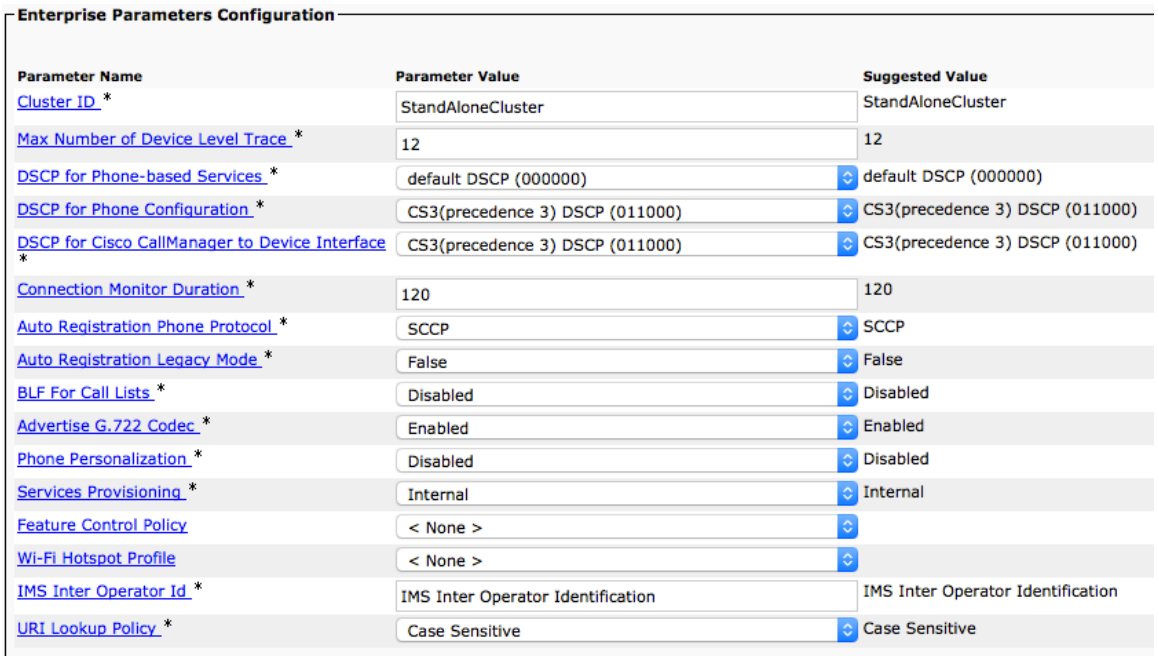


QoS パラメータ

SIP 通信、電話設定、およびデバイス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。



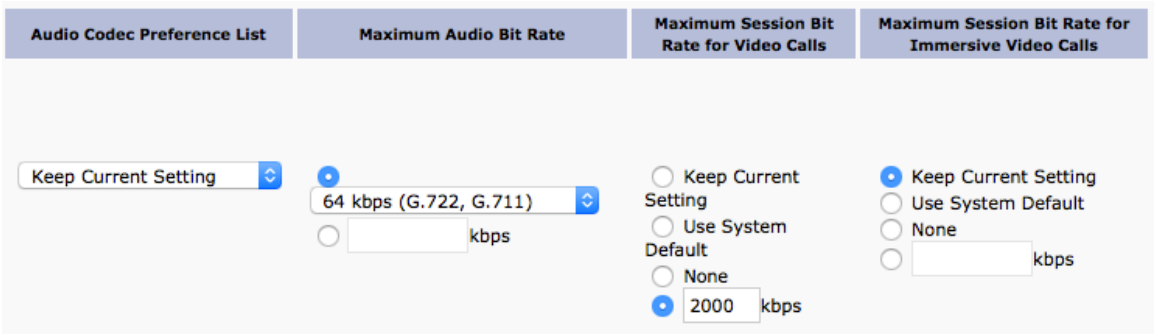
オーディオおよびビデオのビットレート

オーディオおよびビデオのビット レートを設定するには、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。

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

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

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



音声または音声 + ビデオ コール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
AAC-LD	128 ~ 256 Kbps
Opus	6 ~ 510 Kbps
G.722/G.711	64 Kbps
G.722.1	32 Kbps
G.729	8 Kbps

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

設定された値で Webex Desk Series から送信されたビデオストリームの解像度が決まります。

Webex Desk Series は、リージョン設定が考慮されたリモートデバイスの機能によって、最大 FHD 1080p ビデオまで受信できます。

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

ビデオタイプ	ビデオ解像度	フレーム/秒（FPS）	ビデオ ビット レート範囲
qnHD 180p	320 × 180	30	最大 128 Kbps
CIF 288p	512 x 288	30	129 ~ 256 Kbps
nHD 360p	640 x 360	30	257 ~ 384 Kbps
SD 448p	768 x 448	30	385 ~ 512 Kbps
WSVGA 576p	1024 X 576	30	513 ~ 768 Kbps
HD 720p	1280 X 720	30	769 ~ 1472 Kbps
FHD 1080p	1920 X 1080	30	1473 ~ 4000 Kbps

製品固有の設定オプション

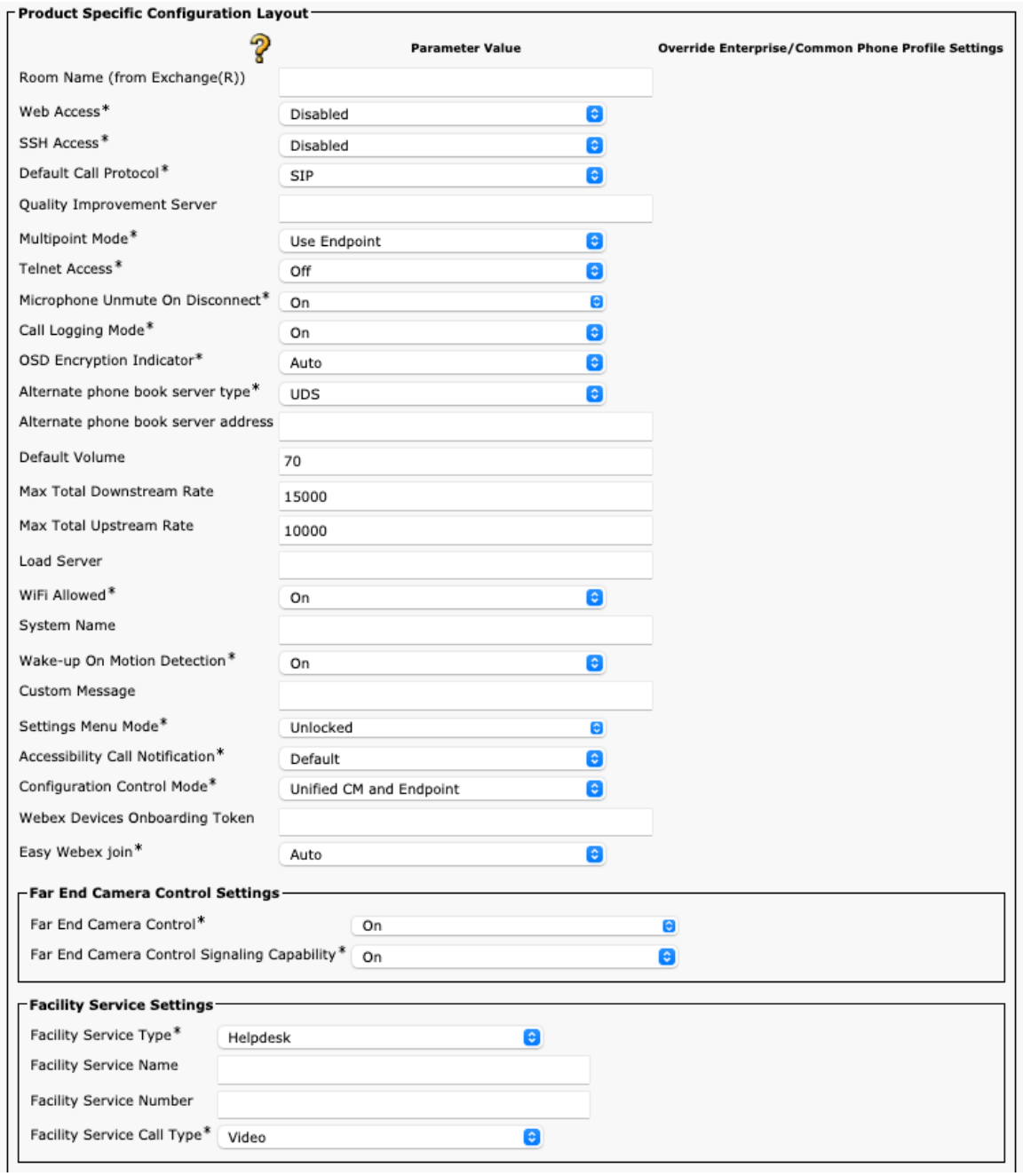
Cisco Unified Communications Manager Administration では、Webex Desk Series に対して次の設定オプションを使用できます。

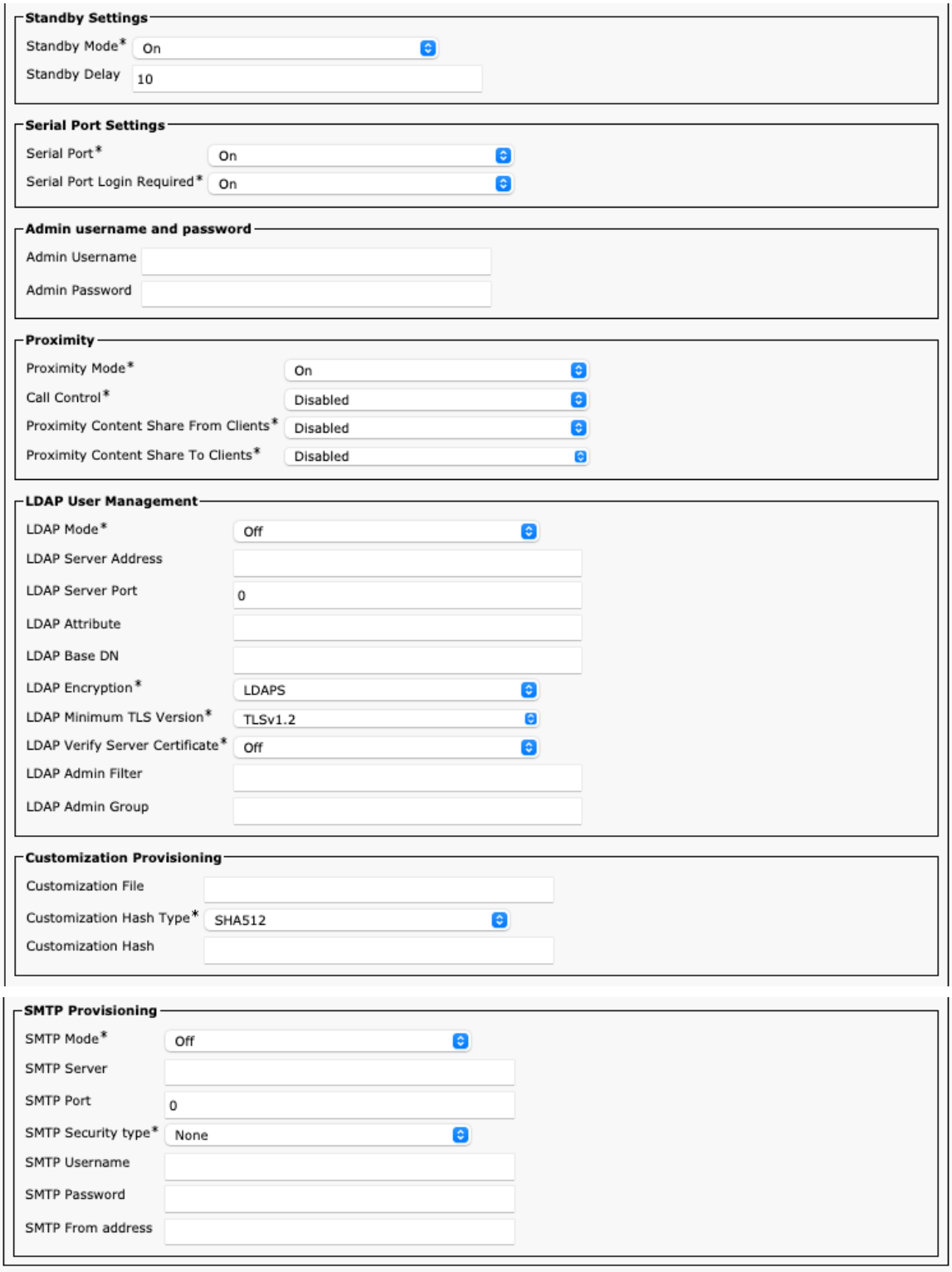
これらのオプションの説明については、設定ページの上部の **[?]** をクリックしてください。

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

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。

Webex Desk Series 設定オプション（バージョン 12.5 より前）





フィールド名	説明
会議室名（Exchange(R)）（Room Name (from Exchange(R)))	これは Exchange の会議室名です。この TelePresence システムが参加する会議をスケジュールするために使用します。（注: この設定は、Exchange で使用される名前と正確に一致する必要があります）

[Web アクセス（Web Access）]	このパラメータは、デバイスが Web ブラウザまたはその他の HTTP クライアントからの接続を受け入れるかどうかを示します。デバイスの Web サーバ機能をディセーブルにすると、電話の内部 Web ページや一部のサポート機能へのアクセスがブロックされますが、通常の動作には影響しません。このパラメータを有効にするには、デバイスのリセットが必要です。
SSH アクセス	このパラメータは、デバイスが ssh 接続を受け入れるかどうかを示します。デバイスの SSH サーバ機能をディセーブルにすると、ログ ファイルの収集などの特定のサポート機能がブロックされますが、通常の操作には影響しません。
[デフォルトコールプロトコル（Default Call Protocol）]	このパラメータでは、デバイスの標準通信プロトコルを設定します。Cisco Unified Communications Manager に登録する場合、このデバイスは SIP だけをサポートします。
[品質改善サーバ（Quality Improvement Server）]	デバイスから品質向上レポートを収集するリモート システムのホスト名または IP アドレスを指定します。
マルチポイントモード	このフィールドは、参加者がポイントツーポイントコールに追加されたときに、マルチポイントコールがどのように確立されるかを定義します。エンドポイントモードを使用すると、マルチポイントコールの機能が、マルチポイントコールを開始するエンドポイントの機能に制限されます。機能は、エンドポイントモデルと、マルチサイトなどのオプションの存在によって異なります。メディア リソース グループ リスト モードを使用すると、関連付けられたメディア リソース グループ リストを介してエンドポイントで使用できるリソースが利用されます。これには、音声会議やビデオ会議のリソースが含まれる場合があります。
Telnet アクセス	このパラメータは、デバイスが telnet 接続を受け入れるかどうかを示します。デバイスの telnet サーバー機能をディセーブルにすると、ログファイルの収集などの特定のサポート機能がブロックされますが、通常の操作には影響しません。
切断時のマイクのミュート解除	すべてのコールが切断されたときに、マイクを自動的にミュート解除するかどうかを定義します。会議室またはその他の共有リソースでは、このようにして次のユーザーのためにシステムを準備する場合があります。
コールロギングモード	システムが受信または送信するコールのコールロギングモードを設定します。コールログは、Web インターフェイスまたは xHistory コマンドを使用して表示できます。

OSD 暗号化インジケータ	暗号化インジケータ（鍵）が画面に表示される時間の長さを定義します。この設定は、暗号化されたコールと暗号化されていないコール、つまりセキュアな会議と非セキュアな会議の両方に適用されます。暗号化されたコールはロックされた鍵のアイコンで示され、暗号化されていないコールはバツ印の付いたロックされた鍵のアイコンで示されます。[自動（Auto）]：Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されている場合、暗号化インジケータがコールの最初の数秒間に表示されます。Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されていない場合、バツ印の付いた暗号化インジケータがコール全体にわたり表示されます。Conference Encryption Mode 設定が BestEffort に設定されていない場合、暗号化インジケータはまったく表示されません。AlwaysOn：暗号化インジケータはコール全体にわたり画面上に表示されます。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用されます。AlwaysOff：暗号化インジケータは画面上に表示されません。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用されます。
代替電話帳サーバのタイプ（Alternate phone book server type）	デフォルトで、エンドポイントは登録先の UCM 上の UDS サーバーを使用しますが、代替電話帳サーバーの使用を希望する場合は、このパラメータを代替電話帳のアドレスと組み合わせて、エンドポイントのデフォルト設定をオーバーライドします。UDS は代替電話帳タイプを UDS に設定し、TMS はタイプを TMS に設定します。
代替電話帳サーバのアドレス（Alternate phone book server address）	デフォルトで、エンドポイントは登録先の UCM 上の UDS サーバを使用しますが、代替電話帳サーバの使用を希望する場合は、このパラメータを代替電話帳のタイプと組み合わせて、エンドポイントのデフォルト設定をオーバーライドします。フィールドには電話帳サーバの完全な URL が必要です。UDS サーバーの URL の例: https://uds-host-name:8443/cucm-uds/users および TMS の例: https://tms-host-name/tms/public/external/phonebook/phonebookservice.asmx
デフォルトのボリューム	値は 0 から 100 の間で指定できます。1 ~ 100 の値は -34.5 dB ~ 15 dB（0.5 dB 刻み）の範囲に対応します。値 0 は、音声がオフになっていることを意味します。
ダウンストリーム速度合計の最大値	この構成は、許可される全体の最大受信ビットレートを指定します。ビットレートは任意の時点におけるすべてのアクティブコール間で均等に分割されます。値スペースの範囲は 64 ~ 10000 です。
アップストリーム速度合計の最大値	この構成は、許可される全体の最大送信ビットレートを指定します。ビットレートは任意の時点におけるすべてのアクティブコール間で均等に分割されます。値スペースの範囲は 64 ~ 10000 です。

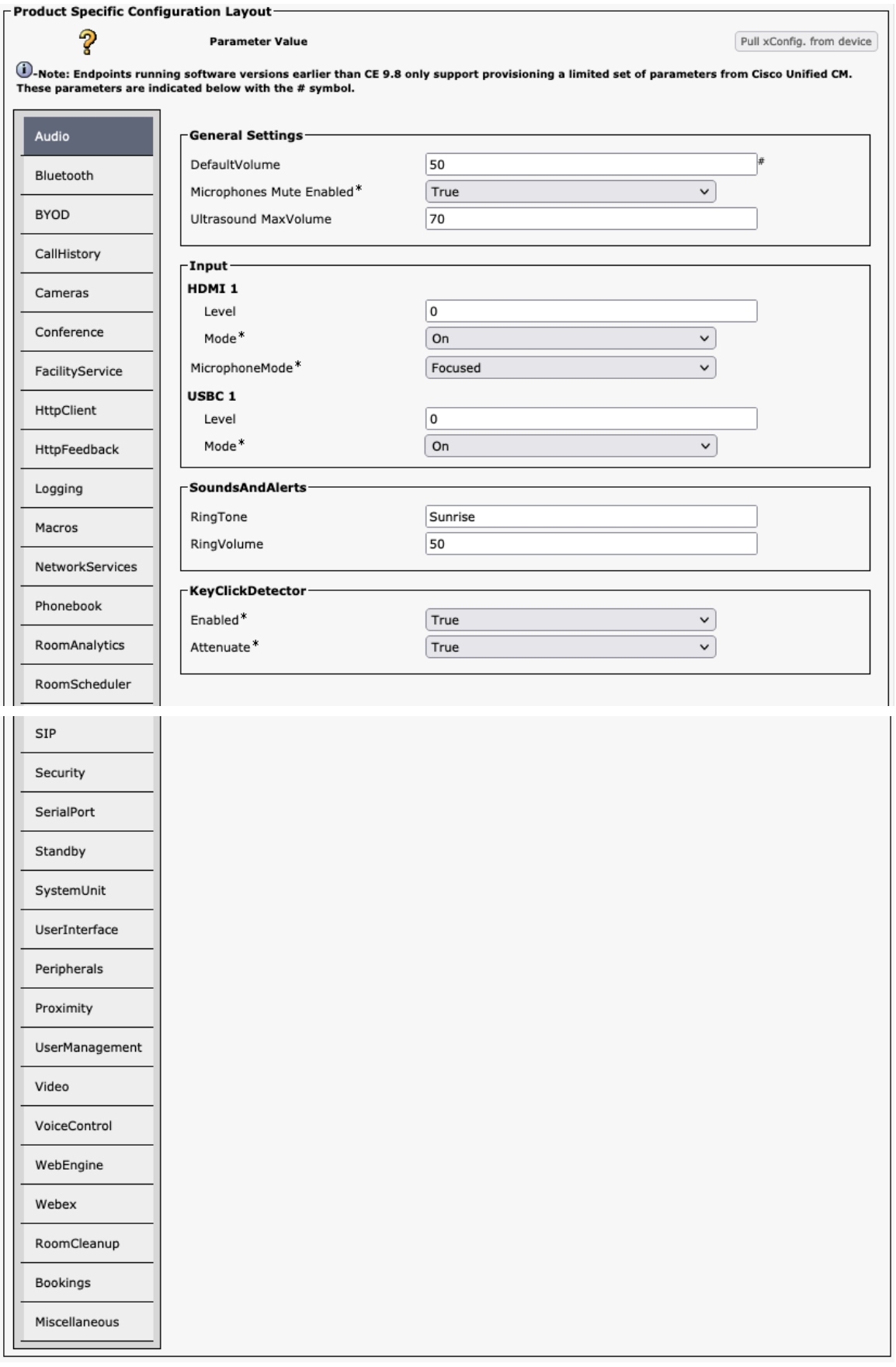
ロード サーバ（Load Server）	デバイスのファームウェアを含む代替サーバーのアドレス。フルパスとポートを指定してください。例: http://example.com/firmware
Wi-Fi が許可されています	エンドポイントで Wi-Fi の有効化を許可するかどうかを示す設定。
システム名（System Name）	システムの名前。デバイスのホスト名として使用できます。
モーション検知ウェイクアップ	部屋の動きを検出したときに、TelePresence エンドポイントがスタンバイモードを終了するかどうかを制御する設定。
カスタム メッセージ（Custom Message）	TelePresence エンドポイントのユーザーインターフェイスに表示されるカスタムメッセージの設定。
設定メニューモード	エンドポイント設定をロックするかどうかを指定する設定。つまり、パスワードによるユーザーログインを要求します。
ユーザー補助コール通知	エンドポイントが、聴覚障害のあるユーザーのユーザー補助設定として、着信通知に増幅されたビジュアルを使用する必要があるかどうかを示す設定。
構成制御モード	Xconfiguration 設定ソース。
Webex デバイスのオンボーディングトークン	Webex Cloud でデバイスを登録するために必要な 16 桁のワンタイムパスワード。
Webex に簡単に参加可能	Webex に簡単に参加可能機能を有効または非表示にします。
遠端カメラ制御設定	
遠端カメラ制御	リモート側（遠端）にこちら側のビデオ ソースの選択とローカル カメラの制御（パン、チルト、ズーム）を許可するかどうか決定できます。
遠端カメラ制御シグナリング機能	遠端制御（H.224）信号機能モードを設定します。
ファシリティサービス設定	
ファシリティサービスタイプ	この設定で、どのようなサービスかを選択できます。ファシリティサービスは、ファシリティ名とファシリティサービス番号が正しく設定されていないと利用できません。タッチコントローラでは、タイプが Helpdesk の FacilityService Service 1 だけを使用できます。ファシリティサービスは、リモートコントロールと画面上のメニューを使用する場合には使用できません。
ファシリティサービス名	各ファシリティサービスの名前を設定します。ファシリティサービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。タッチコントローラでは FacilityService Service 1 だけを使用でき、その名前がファシリ

	ティ サービス コール ボタンに使用されます。ファシリティサービスは、リモートコントロールと画面上のメニューを使用する場合には使用できません。
ファシリティサービス番号	各ファシリティサービスの番号を設定します。ファシリティサービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。タッチコントローラでは、FacilityService Service 1 だけを使用できます。ファシリティサービスは、リモートコントロールと画面上のメニューを使用する場合には使用できません。
ファシリティ サービス コール タイプ	各ファシリティサービスにコールタイプを設定します。ファシリティサービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。タッチコントローラでは、FacilityService Service 1 だけを使用できます。ファシリティサービスは、リモートコントロールと画面上のメニューを使用する場合には使用できません。
スタンバイ設定	
スタンバイ モード	このパラメータは、システムをスタンバイモードにするかどうかを決定します。
Standby Delay	スタンバイ モードに入る前に、システムがアイドル モードのまま経過する時間の長さ（分単位）を定義します。注：[スタンバイ制御（Standby Control）] が有効である必要があります。
シリアルポートの設定	
シリアルポート	このパラメータは、デバイスがシリアルポートを有効にするかどうかを示します。
シリアルポートログインが必要です	このパラメータは、シリアルポートに接続するときにログインが必要かどうかを定義します。
管理者のユーザ名とパスワード	
[Admin ユーザ名（Admin Username）]	管理者ユーザのユーザ ID を入力します。
[管理パスワード（Admin Password）]	管理者ユーザのパスワードを入力します。
プロキシミティ	
プロキシミティ モード	プロキシミティアプリがエンドポイントとペアリングできるようにします。

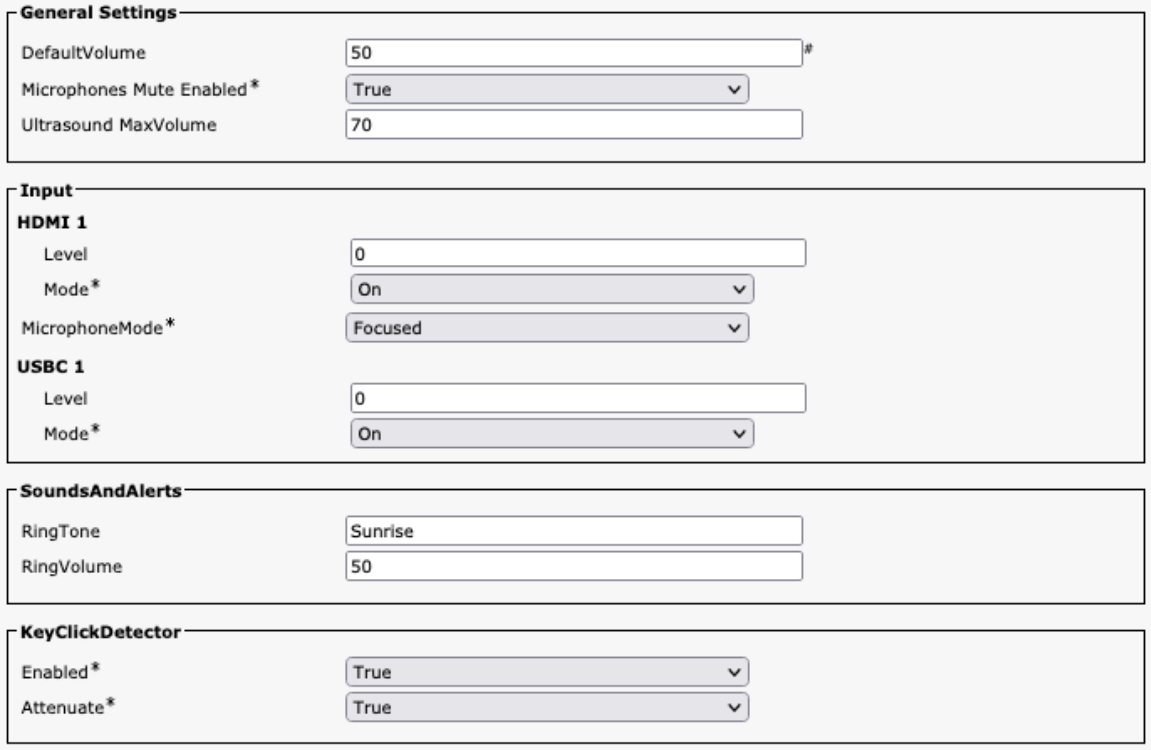
コール制御	プロキシミティアプリに呼制御を許可します。
プロキシミティクライアントからのコンテンツ共有	プロキシミティアプリによるコンテンツ共有を許可し、コンテンツをプレゼンテーションとしてデバイスから TelePresence エンドポイントに送信します。
プロキシミティクライアントへのコンテンツ共有	プロキシミティアプリが TelePresence エンドポイントからプレゼンテーションスライドを受信できるようにします。
LDAP ユーザー管理	
LDAP モード	ビデオ システムは、LDAP（Lightweight Directory Access Protocol）サーバを、ユーザ名とパスワードを一元的に保存および検証する場所として使用することをサポートします。この設定を使用して、LDAP 認証を使用するかどうか設定します。実装は、Microsoft Active Directory （AD）サービスでテスト済みです。
LDAP サーバーアドレス	LDAP サーバーの IP アドレスまたはホスト名を設定します。
LDAP Server Port	LDAP サーバーに接続するポートをオンに設定します。0 に設定した場合は、選択したプロトコルのデフォルトを使用します（「UserManagement LDAP Encryption」設定を参照）。
LDAP 属性	指定のユーザー名にマップするために使用する属性。設定しない場合、sAMAccountName が使用されます。
LDAP Base DN	検索を開始するエントリの識別名（ベース）。例："DC=company, DC=com"
LDAP 暗号化	ビデオ システムと LDAP サーバとの間の通信を保護する方法を定義します。ポート番号は、UserManagement LDAP Server Port 設定を使用してポート番号をオーバーライドできます。LDAPS：ポート 636 over TLS（Transport Layer Security）上の LDAP サーバに接続します。None：ポート 389 上の LDAP サーバに接続します（暗号化なし）。 STARTTLS：ポート 389 上の LDAP サーバに接続し、次に STARTTLS を送信して TLS 暗号化を有効にします。
LDAP の最小 TLS バージョン	許可する最低バージョンの TLS（Transport Layer Security）プロトコルを設定します。TLSv1.0：TLS バージョン 1.0 以上をサポートします。TLSv1.1：TLS バージョン 1.1 以上をサポートします。TLSv1.2：TLS バージョン 1.2 以上をサポートします。
LDAP 検証サーバー証明書	ビデオ システムを LDAP サーバに接続すると、サーバはビデオ システムに証明書を提示して身元を示します。この設定は、ビデオ システムがサーバの証明書を確認するかどうかを決定するために使用します。

LDAP 管理フィルタ	LDAP フィルタは、管理者権限が付与されるユーザを判別するために使用します。設定したら、この設定は UserManagement LDAP Admin Group 設定よりも優先されるようになります。例：（CN=adminuser）。構文の詳細については、LDAP 仕様を参照してください。
LDAP 管理グループ	この AD（Active Directory）グループのメンバーには、管理者権限が付与されます。この設定は、（memberOf:1.2.840.113556.1.4.1941:=）の短縮形です。UserManagement LDAP Admin Filter が設定されている場合、この設定は無視されます。例：CN=admin_group, OU=company groups, DC=company, DC=com
カスタマイズ プロビジョニング	
カスタマイズ ファイル	カスタマイズ プロビジョニング ファイルが保存されているアドレス。このフィールドには、カスタマイズ バンドル ファイルの完全な URL、または使用中の CUCM でホストされている場合はファイル名のみが必要です。
カスタマイズハッシュの型	使用するハッシュ関数の種類を設定します。
カスタマイズハッシュ	エンドポイントがファイルの整合性を確認できるように、カスタマイズ プロビジョニング ファイルから生成されたハッシュチェックサムを設定します。
SMTP プロビジョニング	
SMTP モード	この設定は、エンドポイントで SMTP を有効または無効にします。
SMTP サーバ	使用する SMTP サーバーのアドレスを設定します。
SMTP ポート（SMTP Port）	SMTP サーバーに使用するポート番号を指定します。
SMTP セキュリティタイプ	使用する SMTP セキュリティタイプを設定します。
SMTP Username	使用する SMTP ユーザー名を設定します。
SMTP Password	使用する SMTP ユーザー名を設定します。
SMTP 送信元アドレス	エンドポイントから SMTP 経由で電子メールを送信するときに使用する送信元アドレスを設定します。

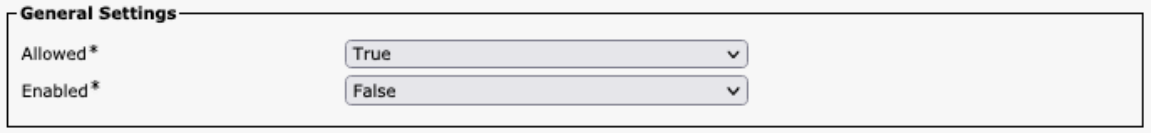
Webex Desk Pro 構成オプション（バージョン 12.5 以降）



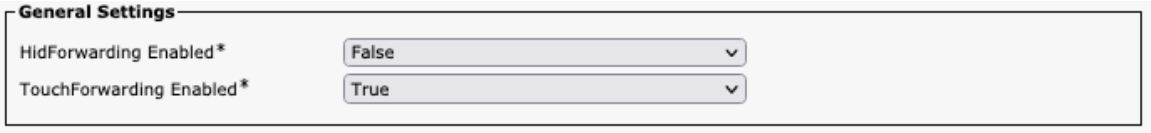
音声



Bluetooth

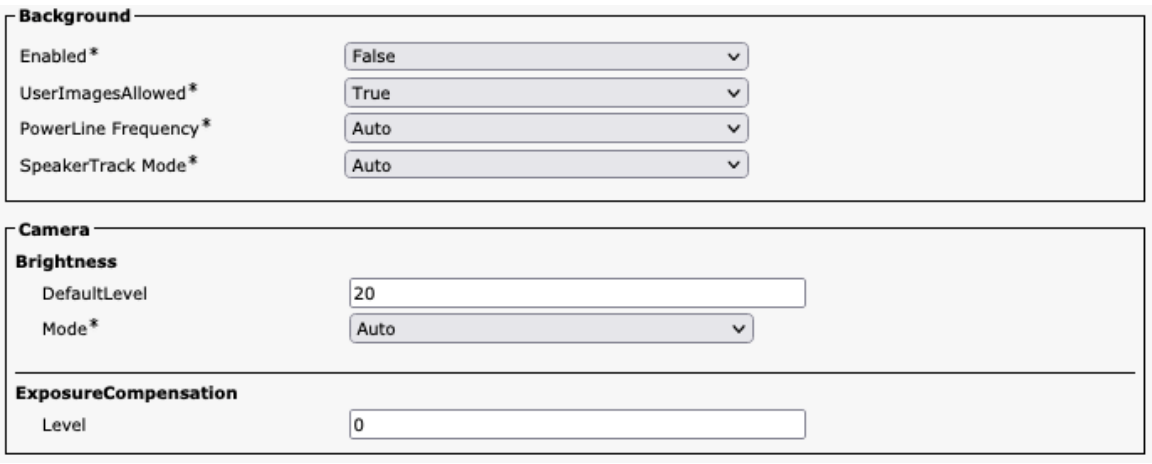


BYOD

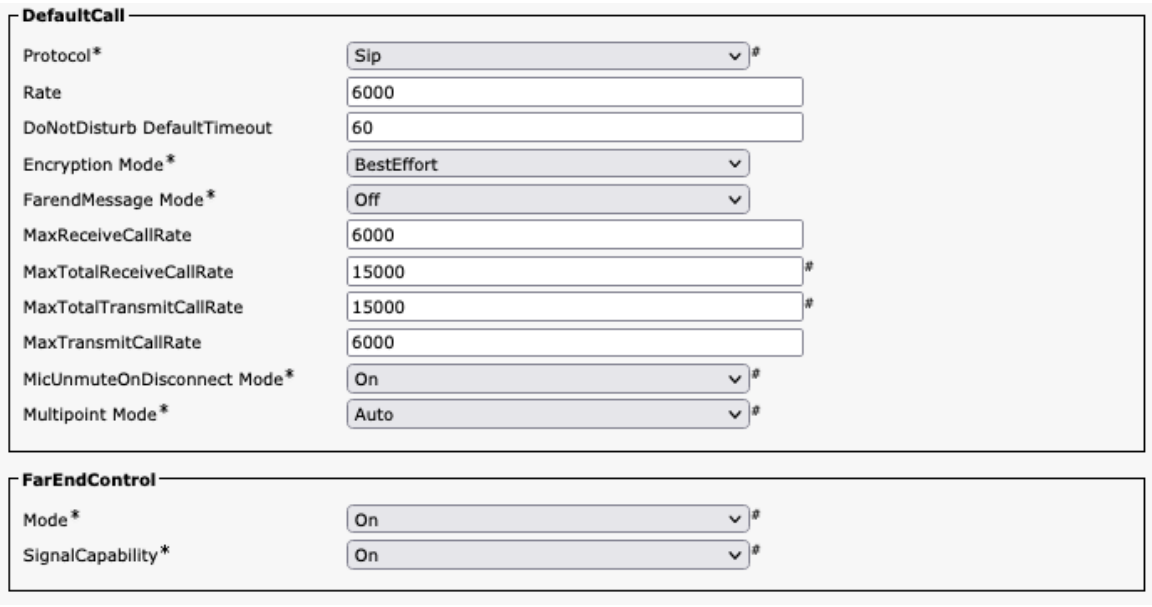


通話履歴

カメラ

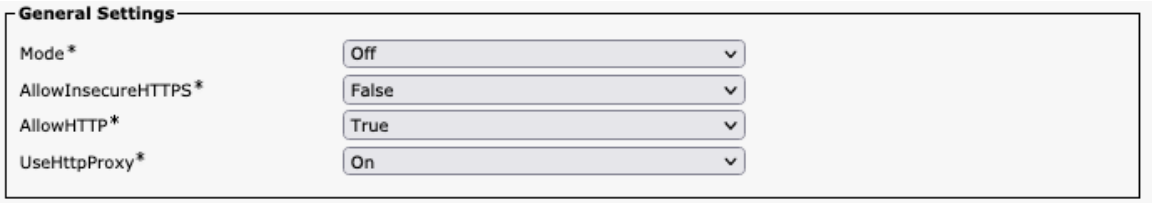

Background
Enabled*
False
UserImagesAllowed*
True
PowerLine Frequency*
Auto
SpeakerTrack Mode*
Auto
Camera
Brightness
DefaultLevel
20
Mode*
Auto
ExposureCompensation
Level
0

会議

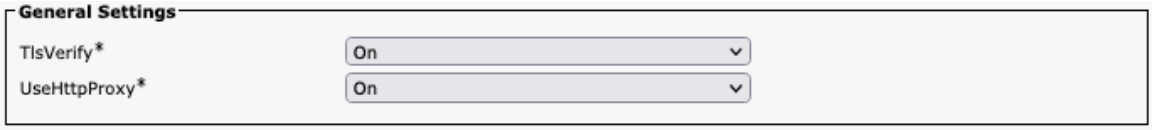

DefaultCall
Protocol*
Sip
Rate
6000
DoNotDisturb DefaultTimeout
60
Encryption Mode*
BestEffort
FarendMessage Mode*
Off
MaxReceiveCallRate
6000
MaxTotalReceiveCallRate
15000
MaxTotalTransmitCallRate
15000
MaxTransmitCallRate
6000
MicUnmuteOnDisconnect Mode*
On
Multipoint Mode*
Auto
FarEndControl
Mode*
On
SignalCapability*
On

ファシリティサービス

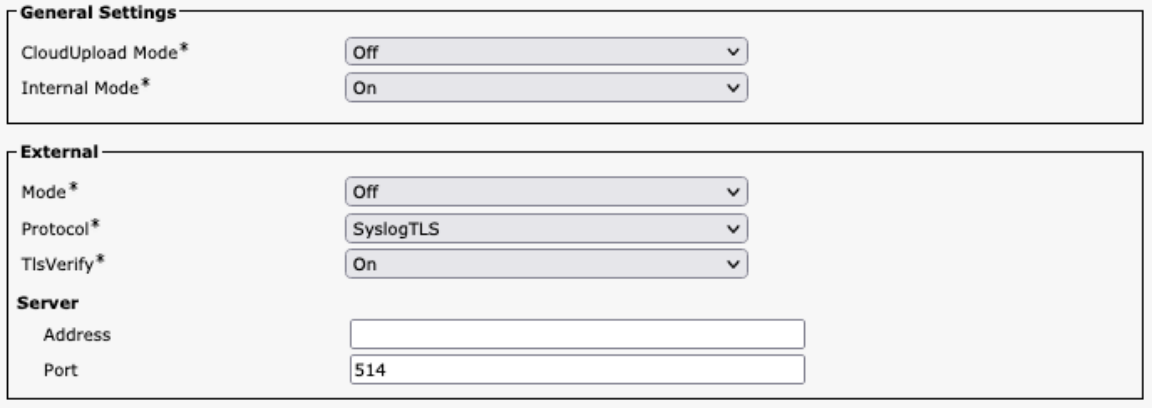
HTTP クライアント



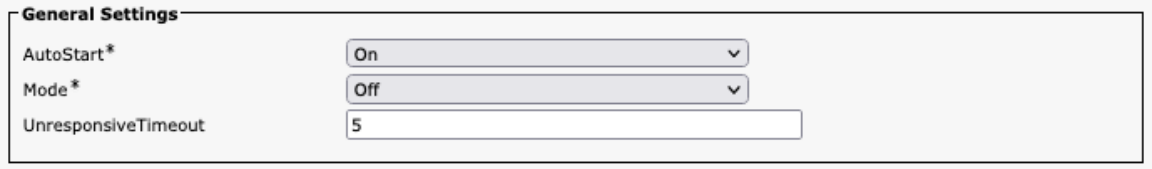
HTTP フィードバック



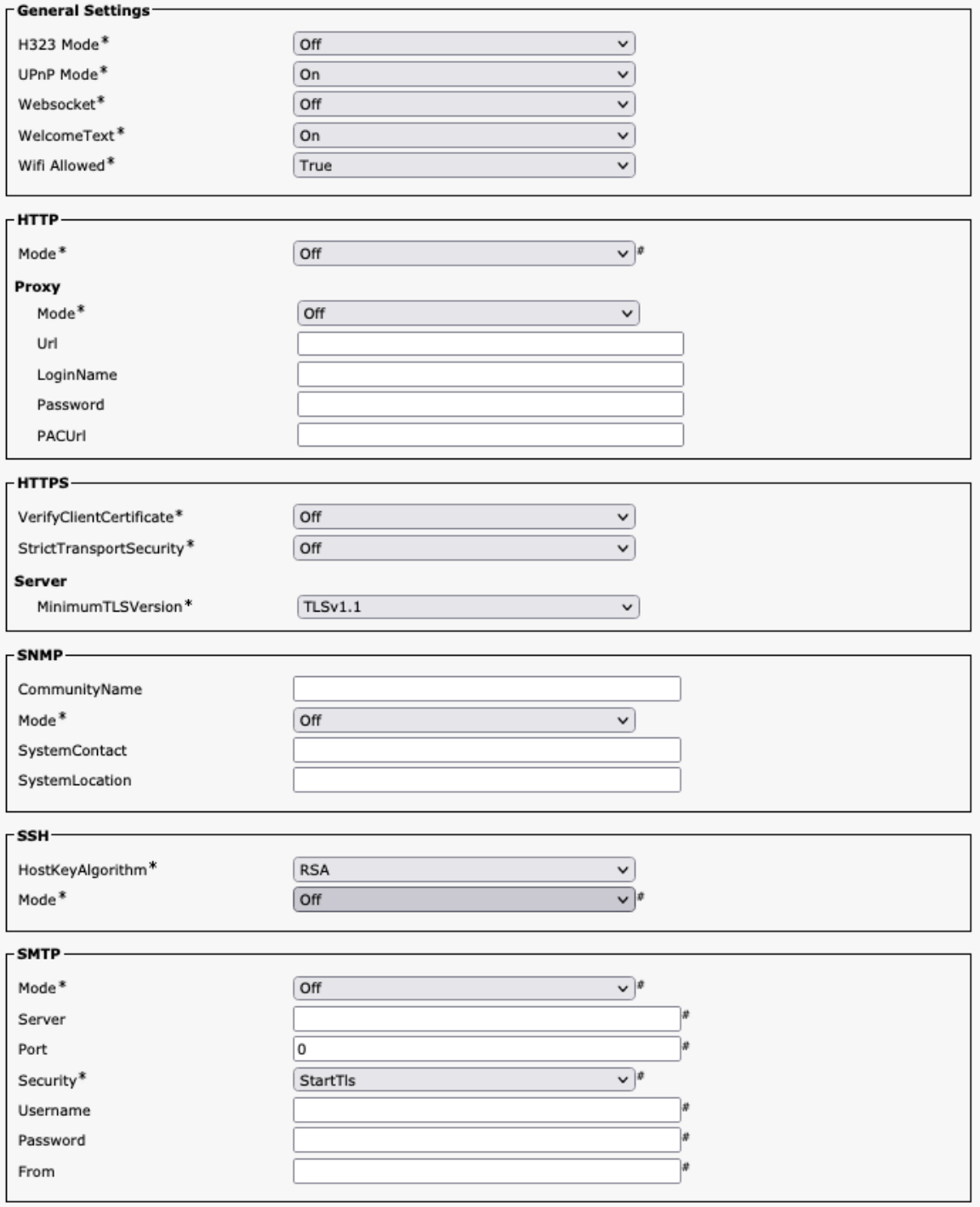
ロギング


General Settings
CloudUpload Mode*
Off
Internal Mode*
On
External
Mode*
Off
Protocol*
SyslogTLS
TlsVerify*
On
Server
Address
Port
514

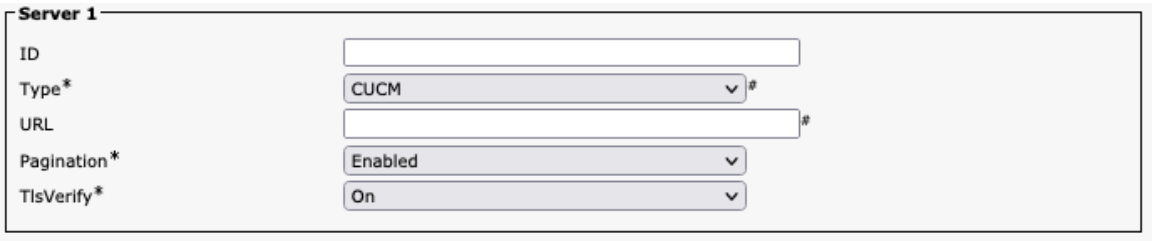
マクロ


General Settings
AutoStart*
On
Mode*
Off
UnresponsiveTimeout
5

ネットワーク サービス



電話帳（Phone Book）



Room 分析

General Settings

PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation

Mode*	Off
Interval	10

ルームスケジューラ

General Settings

Enabled*	False

SIP

General Settings

MinimumTLSVersion*	TLSv1.0

セキュリティ

Audit

Logging

Mode*	Internal

OnError

Action*	Ignore

Server

Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off

Session

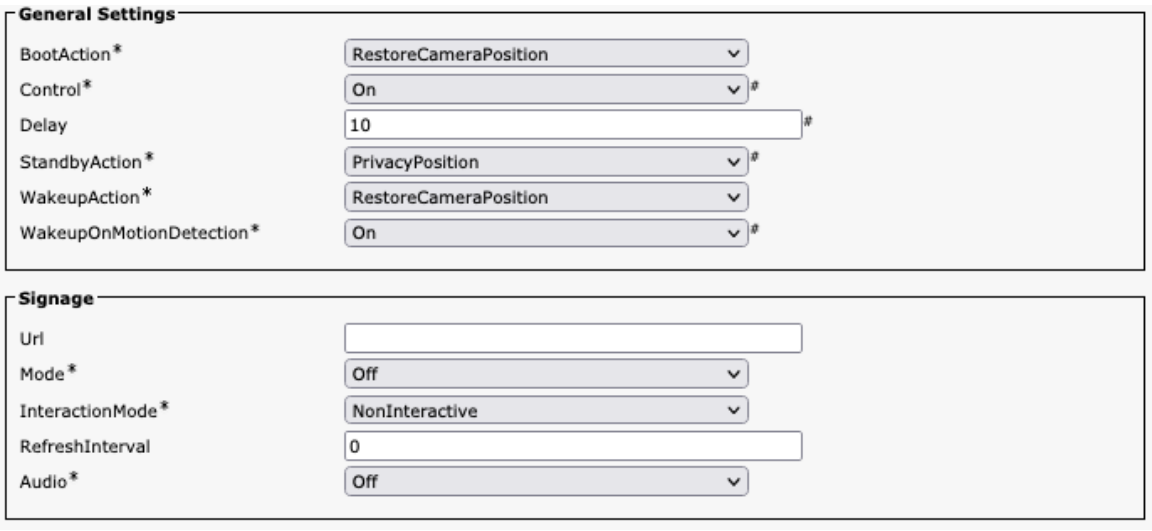
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

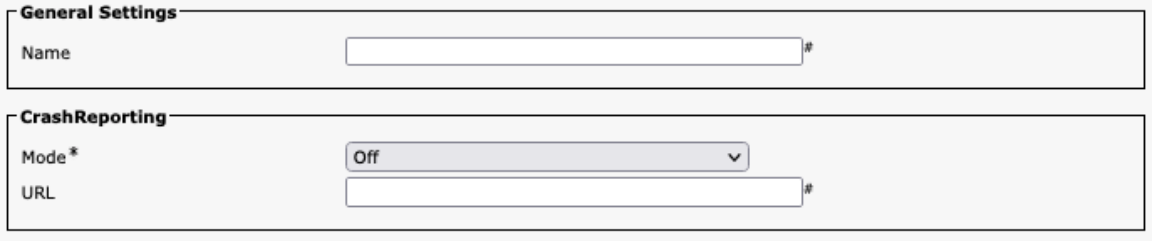
General Settings

BaudRate*	115200
LoginRequired*	On #
Mode*	On #

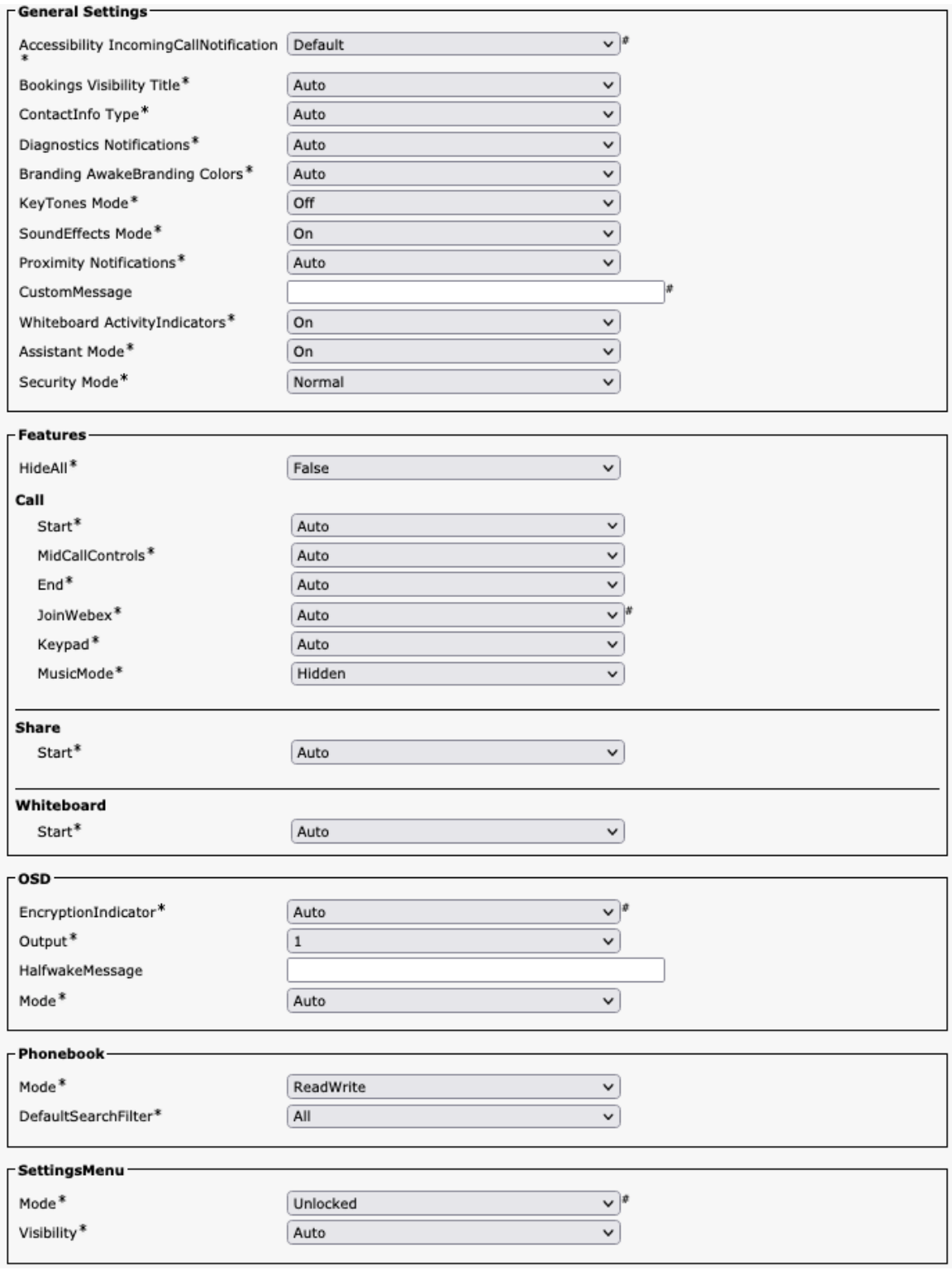
スタンバイ



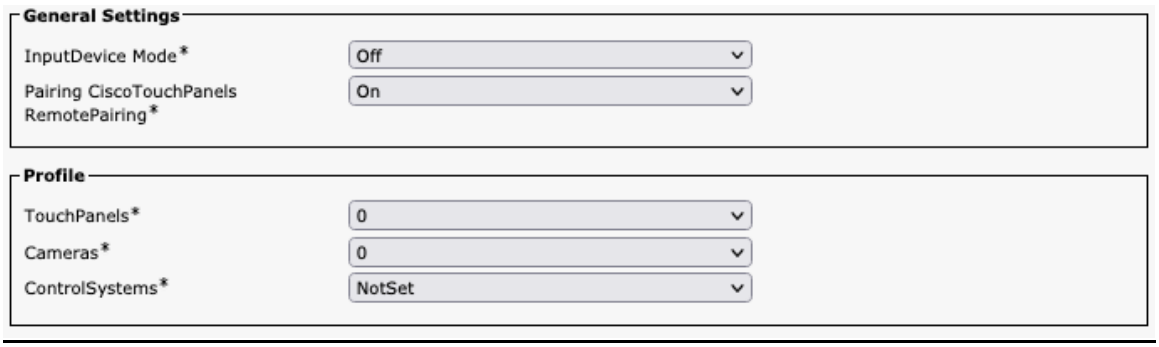
システム ユニット



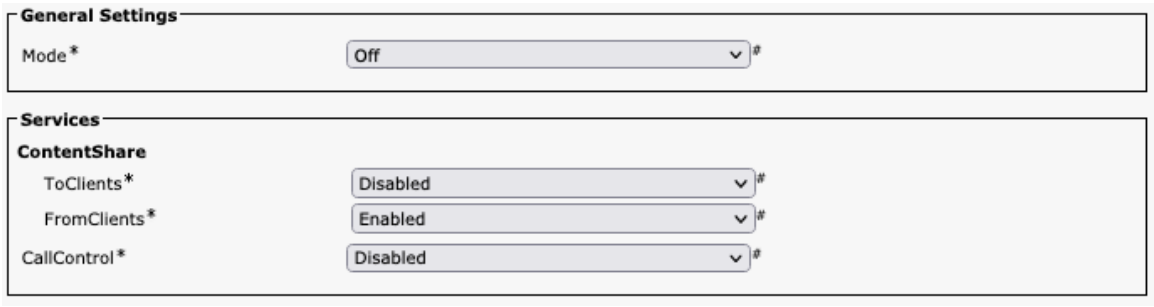
ユーザ インターフェイス



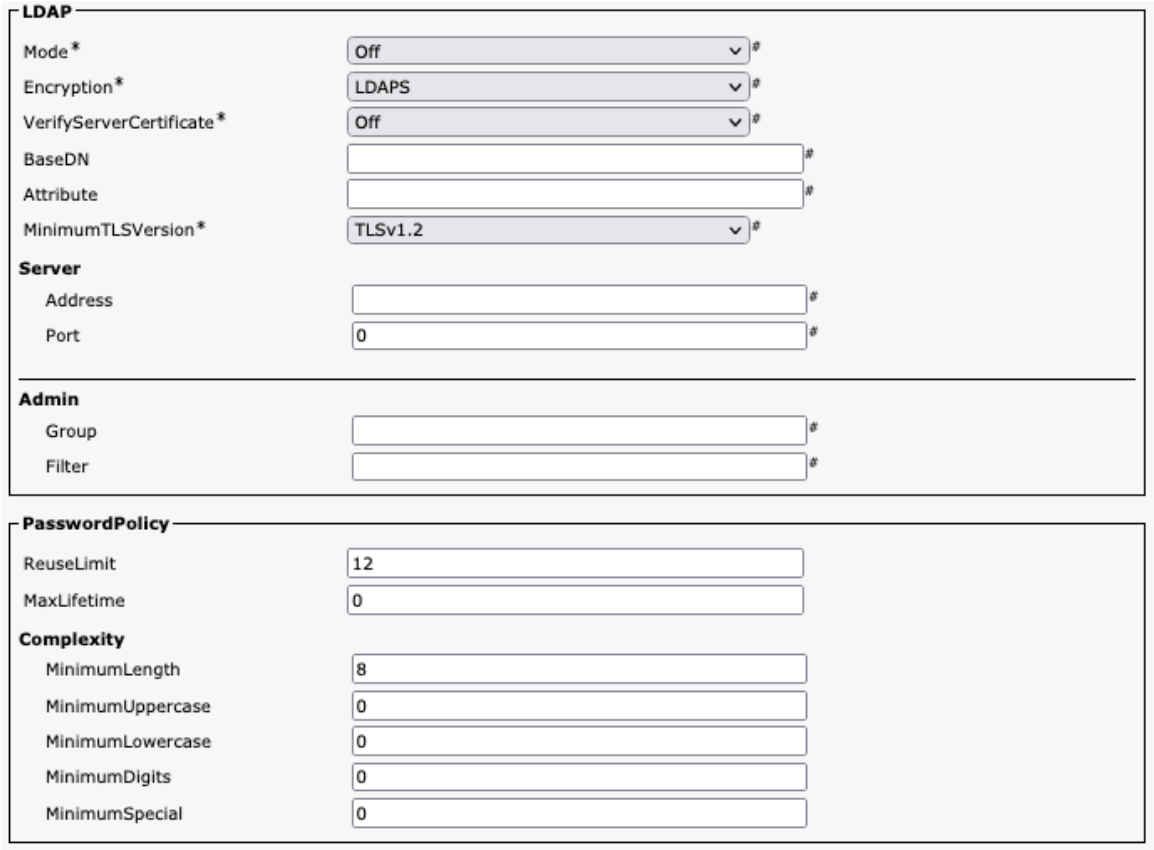
周辺機器



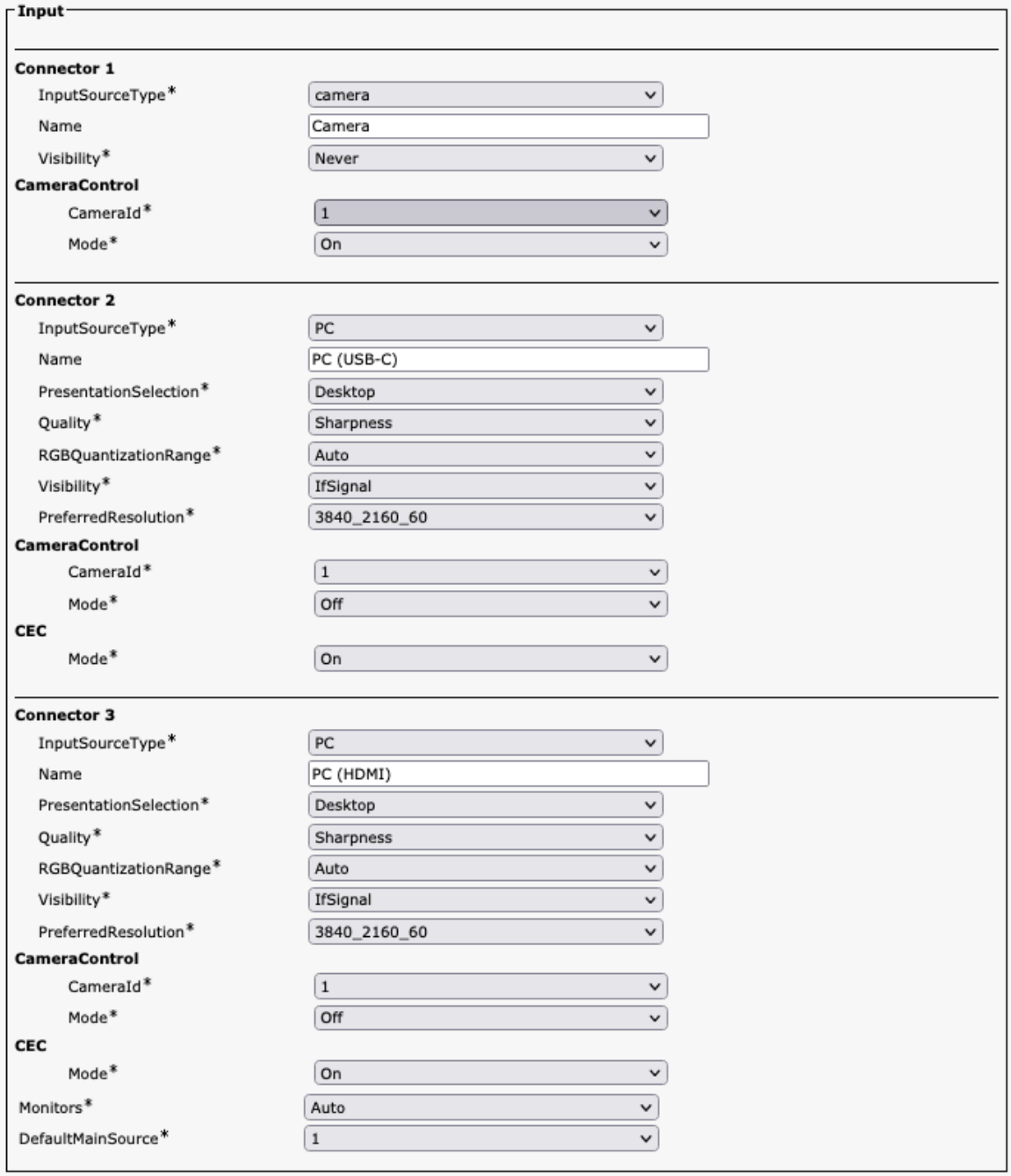
プロキシミティ

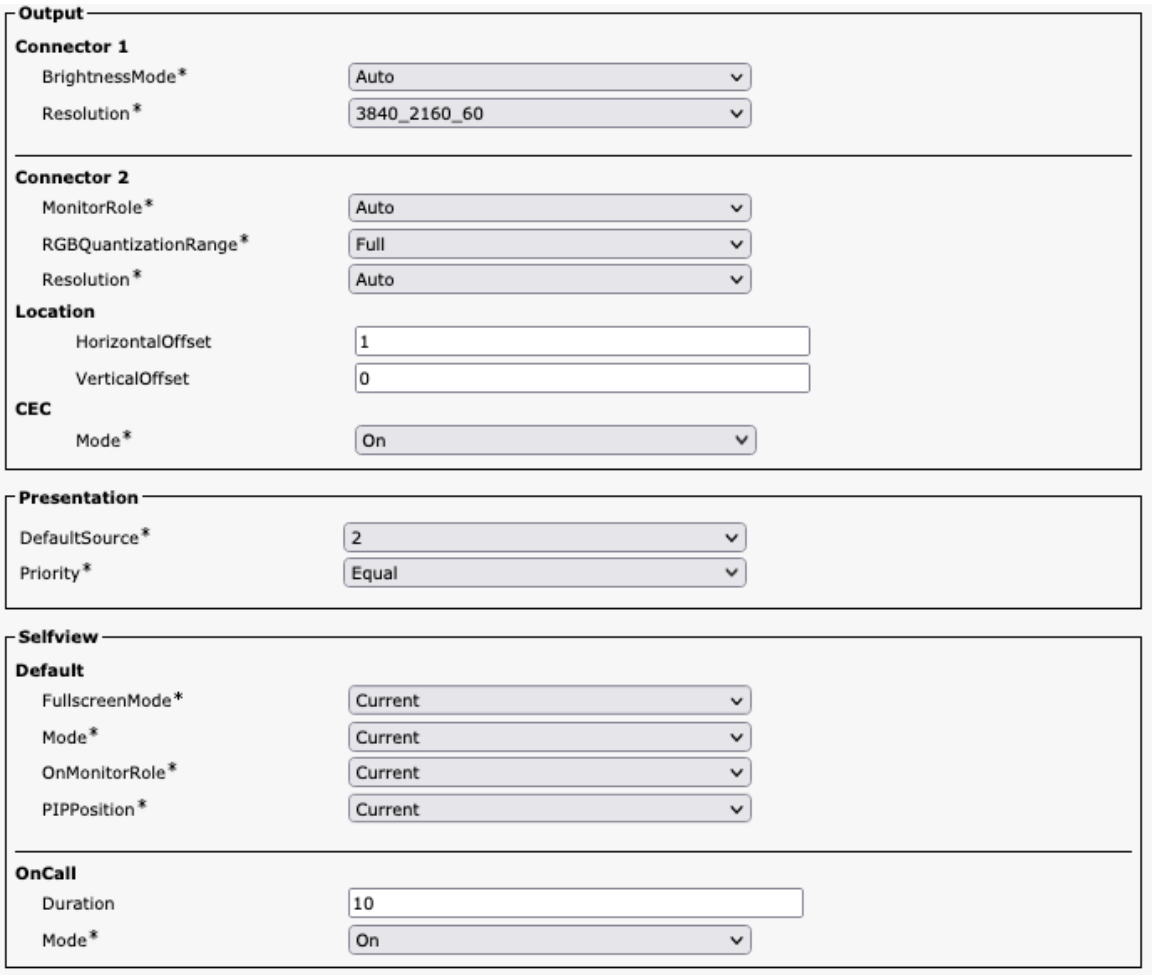


ユーザー管理

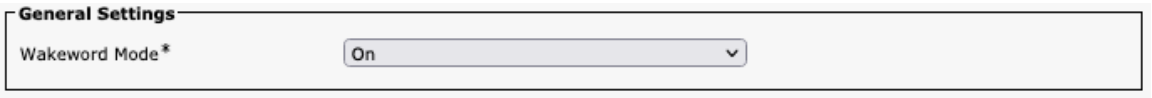


ビデオ


Input
Connector 1
InputSourceType*
camera
Name
Camera
Visibility*
Never
CameraControl
CameraId*
1
Mode*
On
Connector 2
InputSourceType*
PC
Name
PC (USB-C)
PresentationSelection*
Desktop
Quality*
Sharpness
RGBQuantizationRange*
Auto
Visibility*
IfSignal
PreferredResolution*
3840_2160_60
CameraControl
CameraId*
1
Mode*
Off
CEC
Mode*
On
Connector 3
InputSourceType*
PC
Name
PC (HDMI)
PresentationSelection*
Desktop
Quality*
Sharpness
RGBQuantizationRange*
Auto
Visibility*
IfSignal
PreferredResolution*
3840_2160_60
CameraControl
CameraId*
1
Mode*
Off
CEC
Mode*
On
Monitors*
Auto
DefaultMainSource*
1

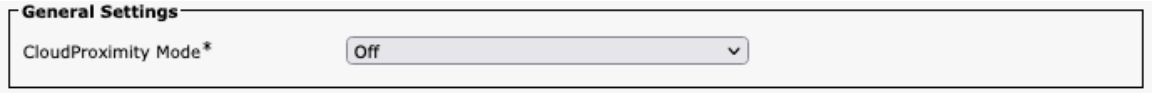


音声管理

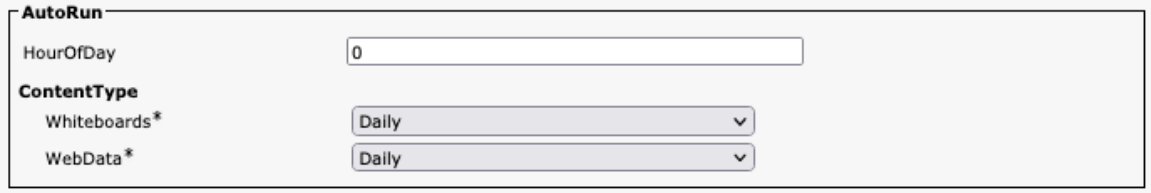


Web エンジン

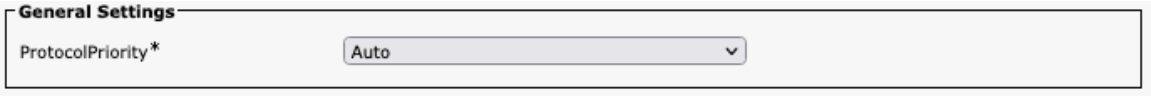
Webex



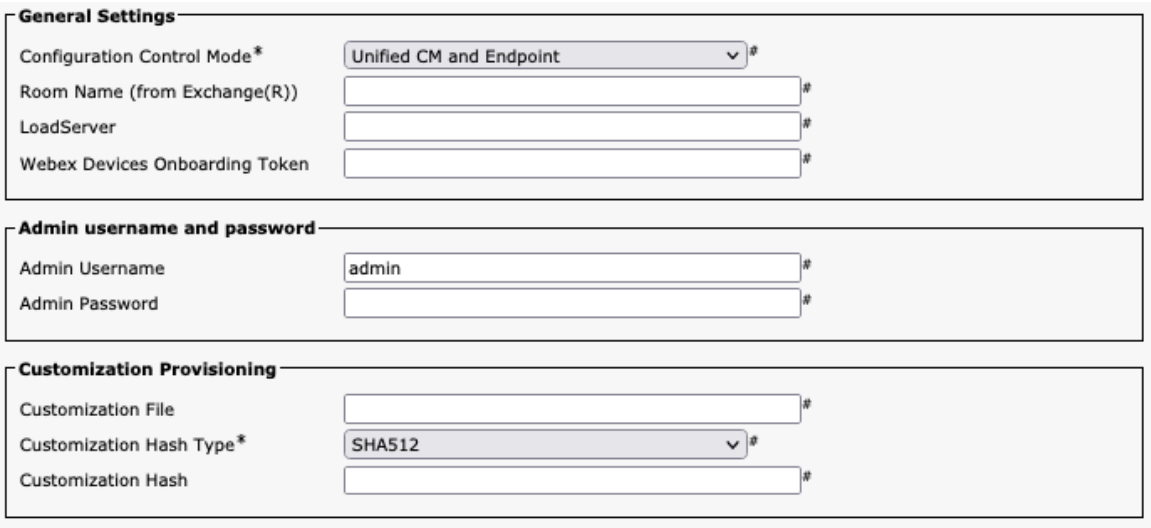
ルームクリーンアップ



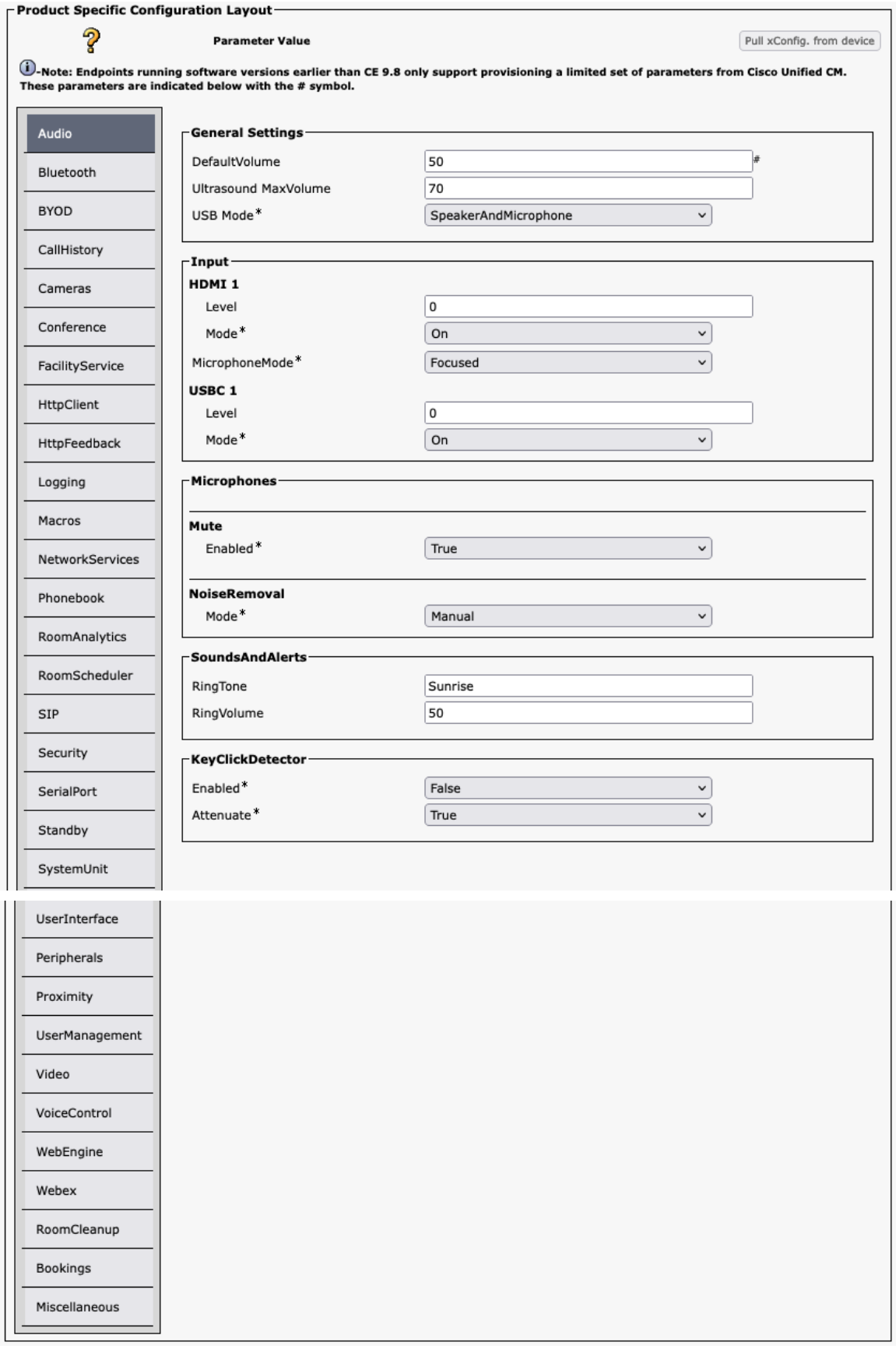
ブッキング



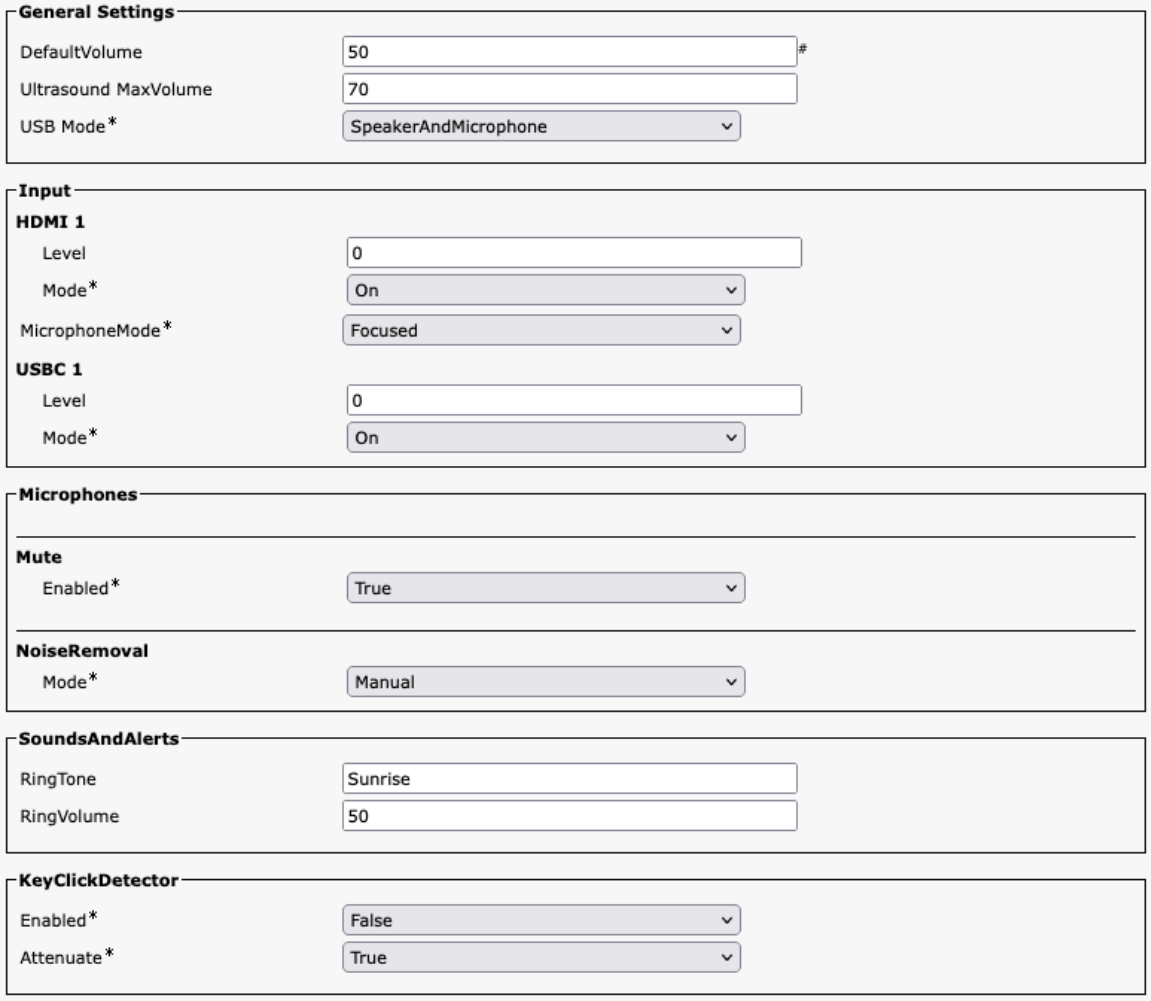
その他



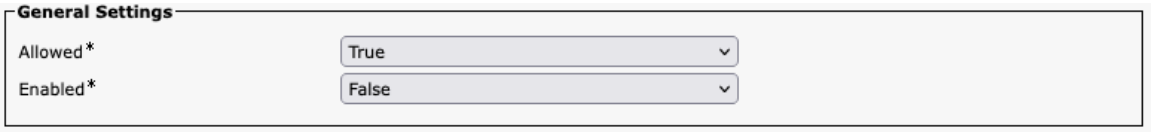
Webex Desk Limited Edition 構成オプション（バージョン 12.5 以降）



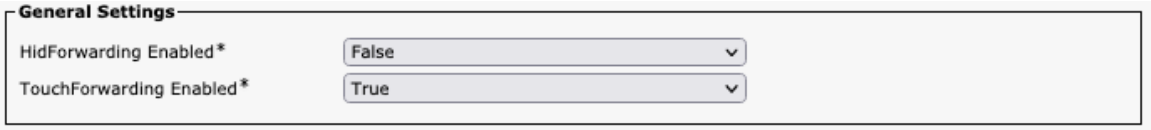
音声



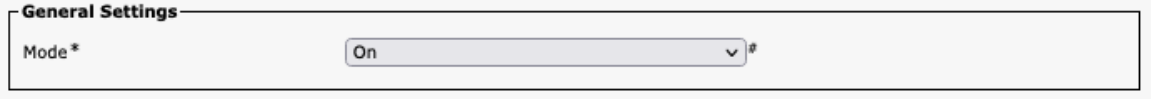
Bluetooth



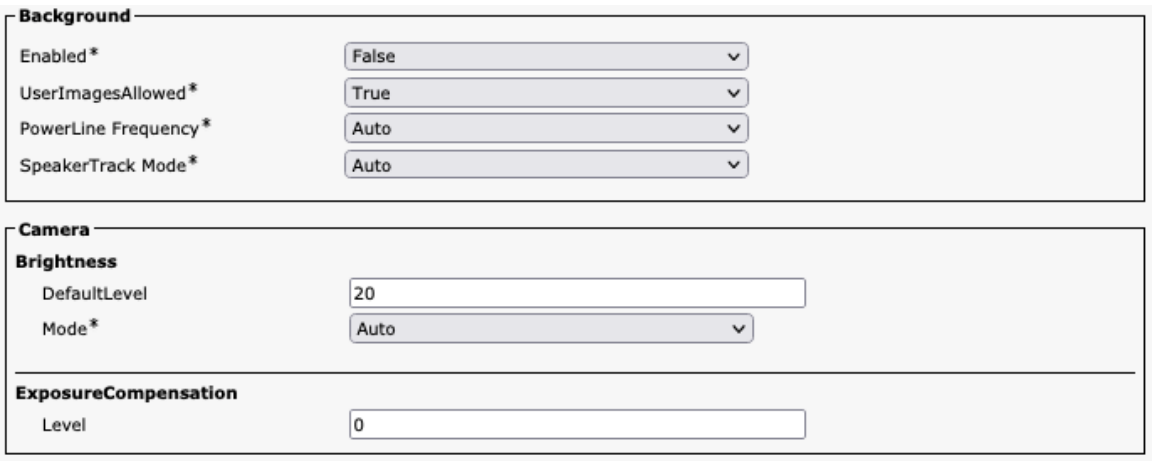
BYOD



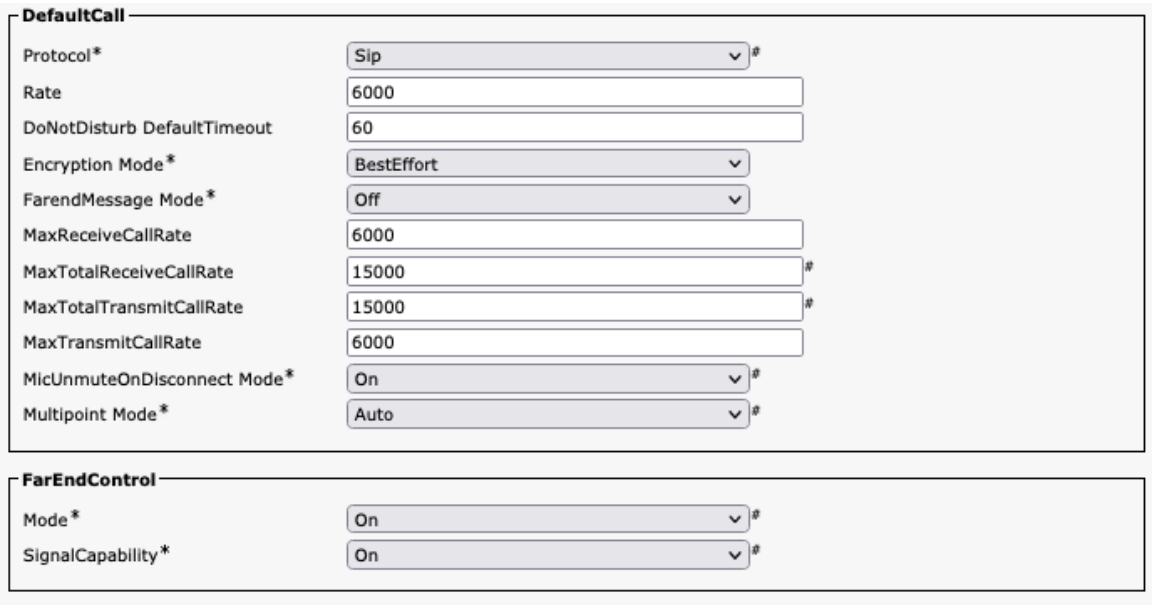
通話履歴



カメラ

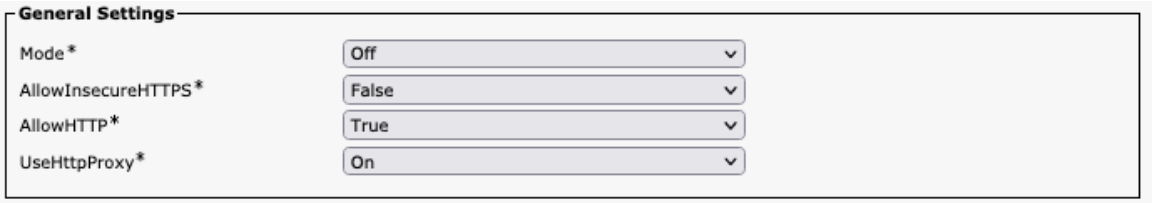

Background
Enabled*
False
UserImagesAllowed*
True
PowerLine Frequency*
Auto
SpeakerTrack Mode*
Auto
Camera
Brightness
DefaultLevel
20
Mode*
Auto
ExposureCompensation
Level
0

会議

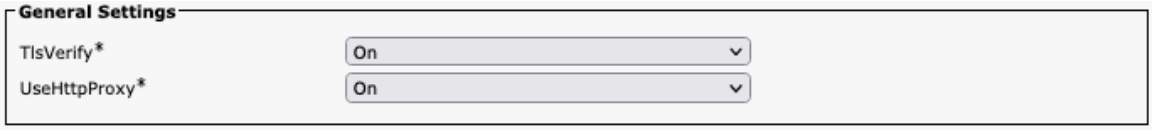

DefaultCall
Protocol*
Sip
Rate
6000
DoNotDisturb DefaultTimeout
60
Encryption Mode*
BestEffort
FarendMessage Mode*
Off
MaxReceiveCallRate
6000
MaxTotalReceiveCallRate
15000
MaxTotalTransmitCallRate
15000
MaxTransmitCallRate
6000
MicUnmuteOnDisconnect Mode*
On
Multipoint Mode*
Auto
FarEndControl
Mode*
On
SignalCapability*
On

ファシリティサービス

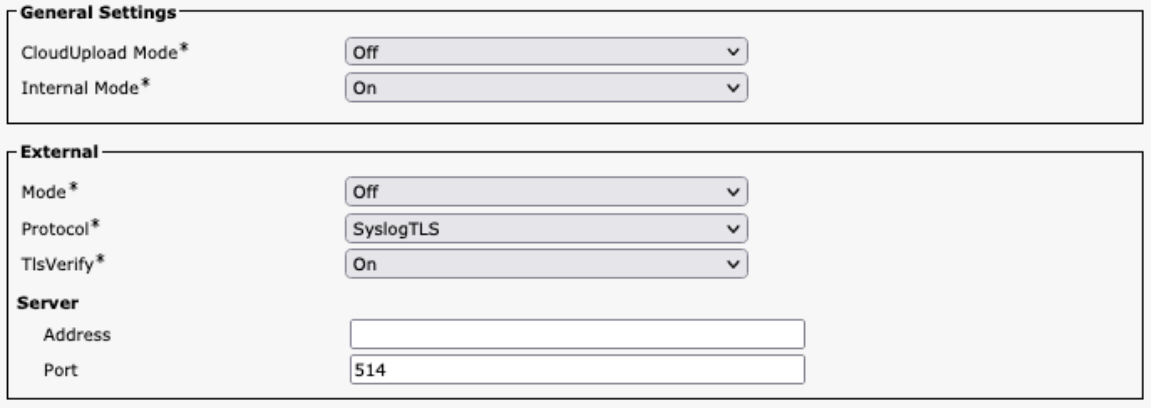
HTTP クライアント



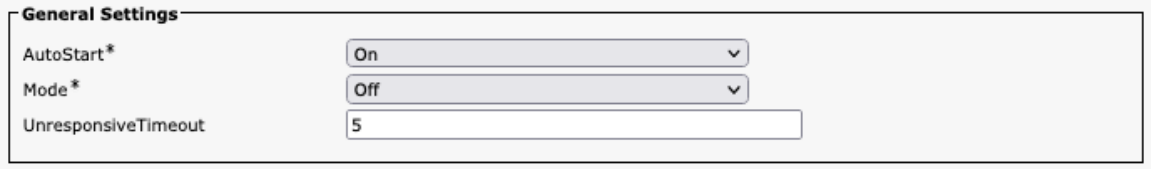
HTTP フィードバック



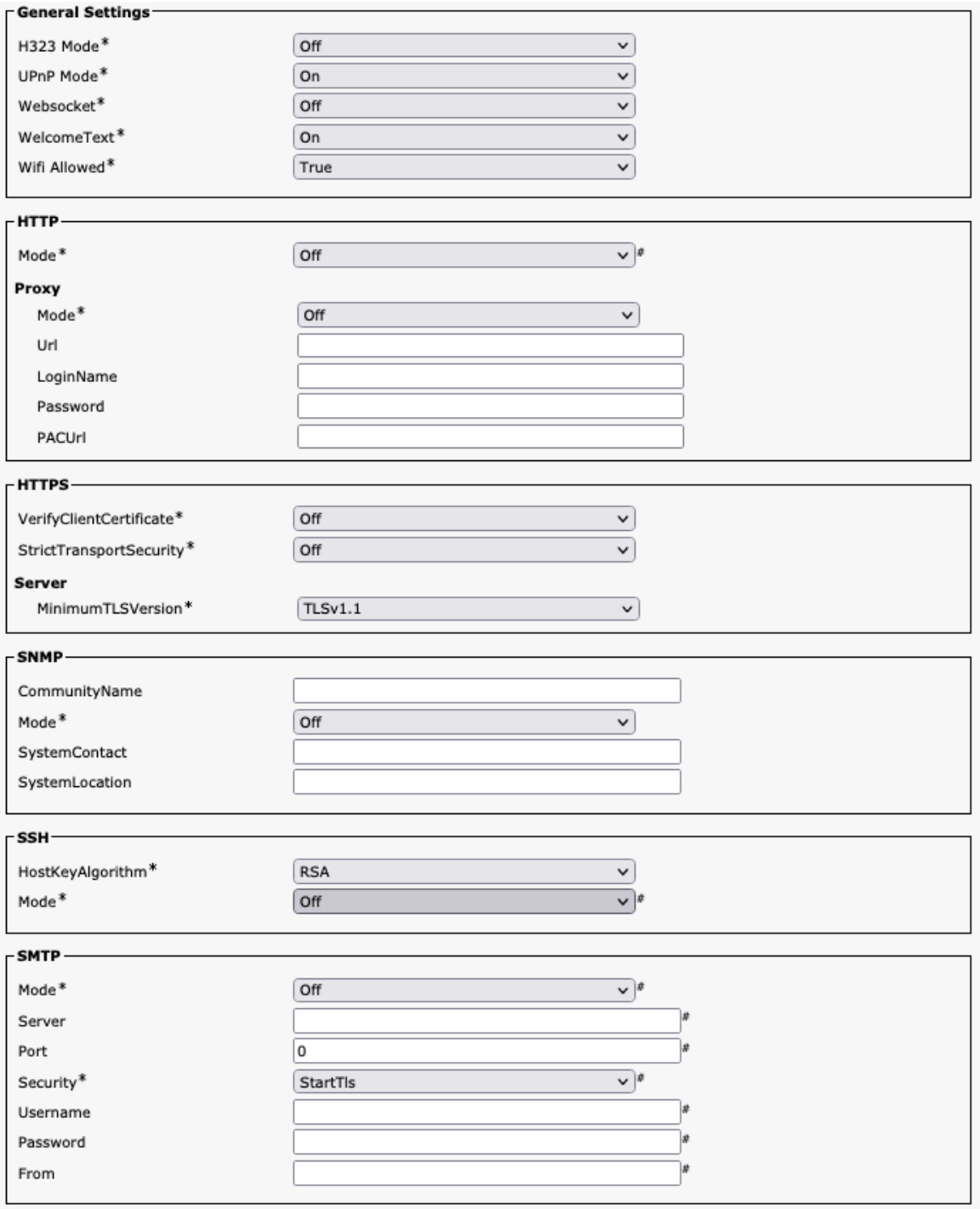
ロギング


General Settings
CloudUpload Mode*
Off
Internal Mode*
On
External
Mode*
Off
Protocol*
SyslogTLS
TlsVerify*
On
Server
Address
Port
514

マクロ


General Settings
AutoStart*
On
Mode*
Off
UnresponsiveTimeout
5

ネットワーク サービス



電話帳（Phone Book）

Room 分析

General Settings

PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation

Mode*	Off
Interval	10

ルームスケジューラ

General Settings

Enabled*	False

SIP

General Settings

MinimumTLSVersion*	TLSv1.0

セキュリティ

Audit

Logging

Mode*	Internal

OnError

Action*	Ignore

Server

Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off

Session

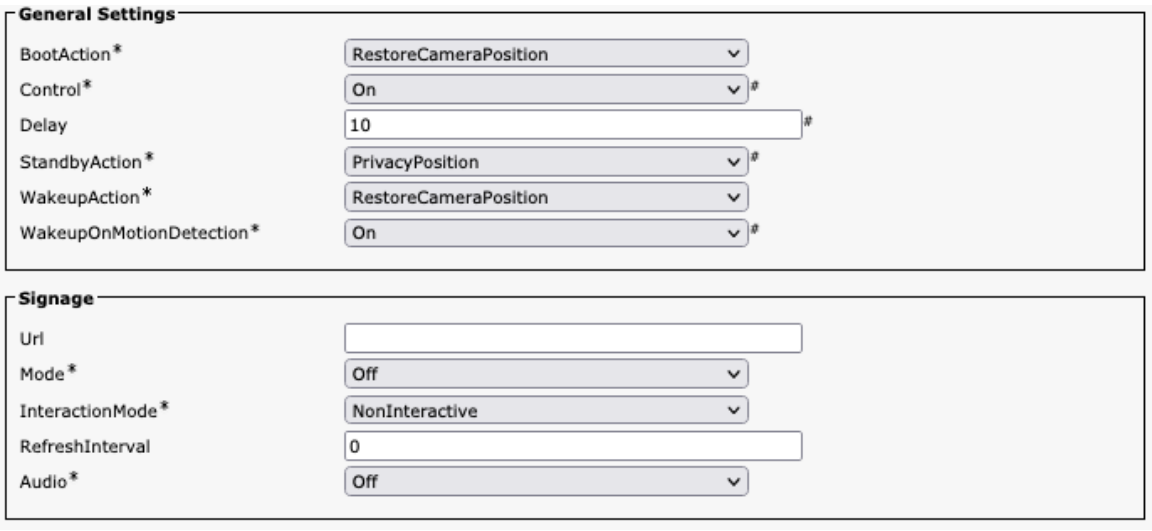
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

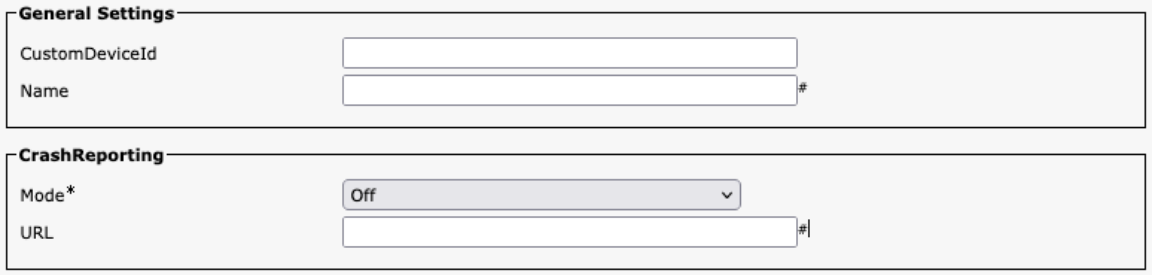
General Settings

BaudRate*	115200
LoginRequired*	On #
Mode*	On #

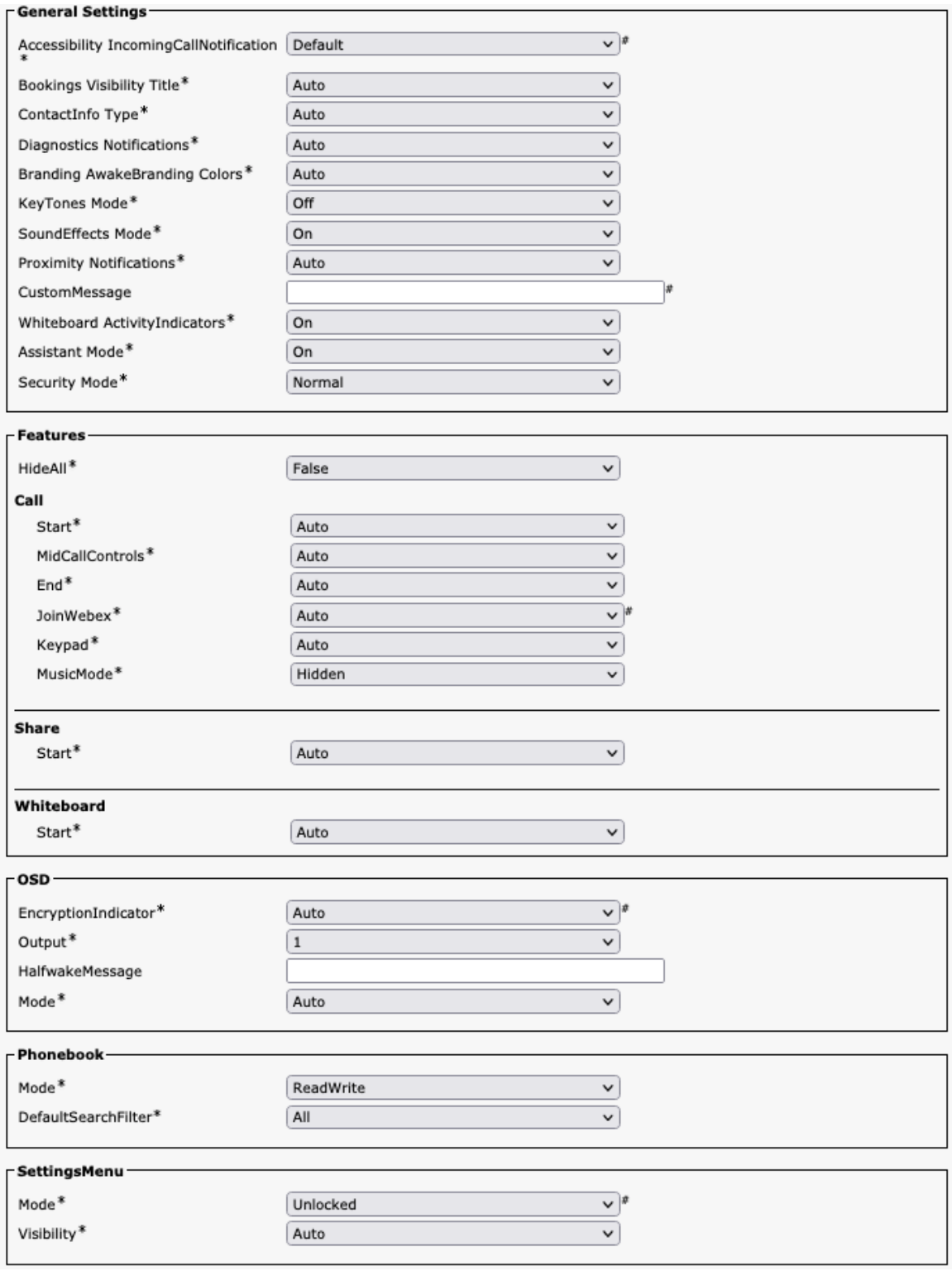
スタンバイ



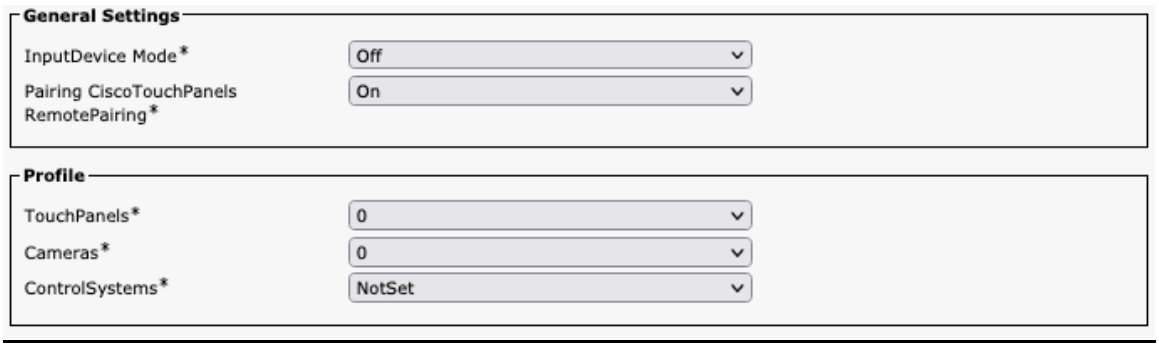
システム ユニット



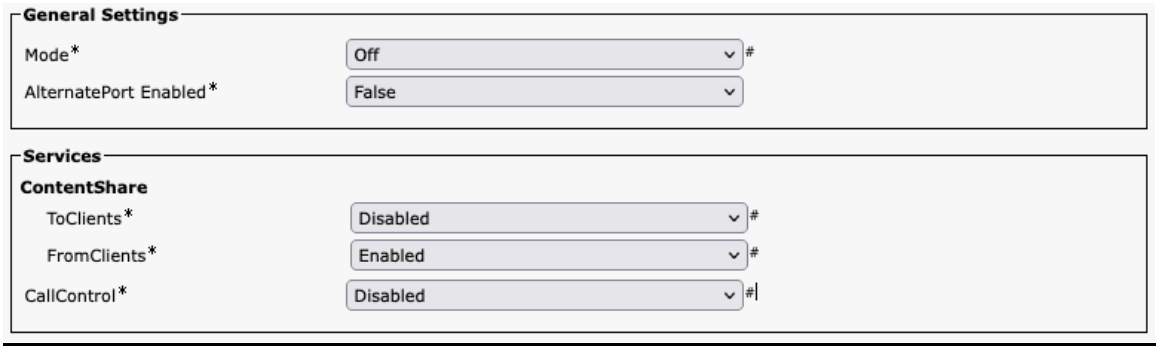
ユーザ インターフェイス



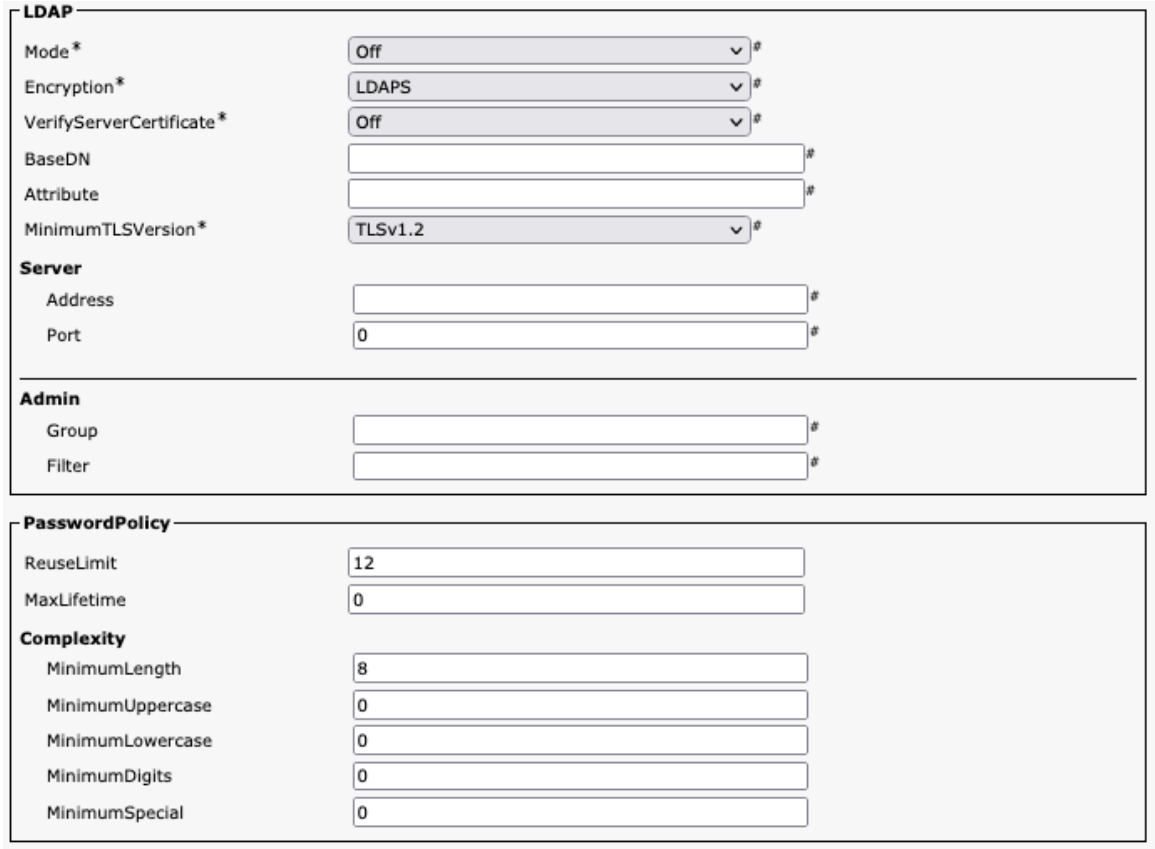
周辺機器



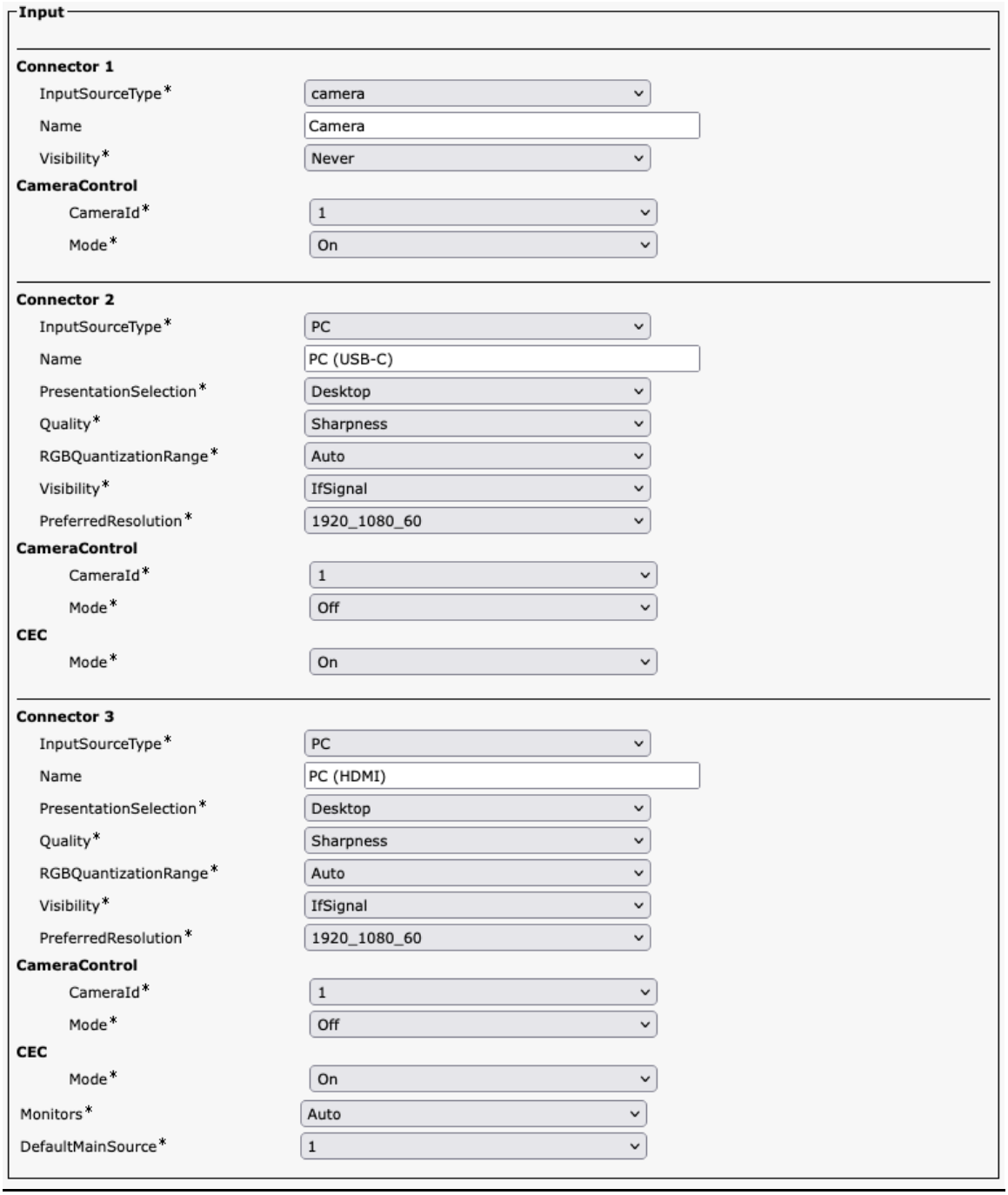
プロキシミティ

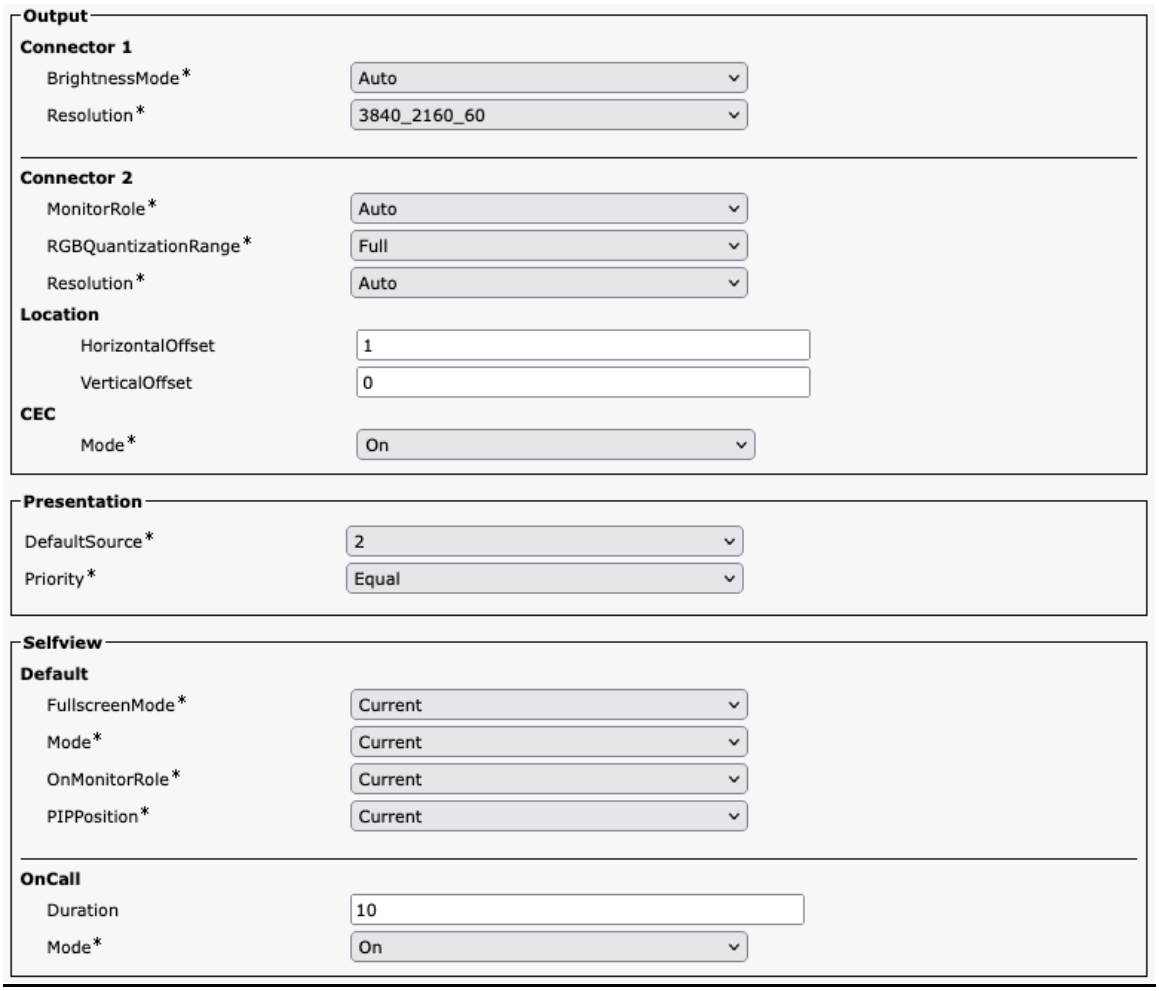


ユーザー管理

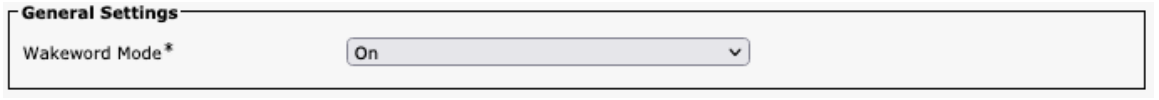


ビデオ


Input
Connector 1
InputSourceType* camera
Name Camera
Visibility* Never
CameraControl
CameraId* 1
Mode* On
Connector 2
InputSourceType* PC
Name PC (USB-C)
PresentationSelection* Desktop
Quality* Sharpness
RGBQuantizationRange* Auto
Visibility* IfSignal
PreferredResolution* 1920_1080_60
CameraControl
CameraId* 1
Mode* Off
CEC
Mode* On
Connector 3
InputSourceType* PC
Name PC (HDMI)
PresentationSelection* Desktop
Quality* Sharpness
RGBQuantizationRange* Auto
Visibility* IfSignal
PreferredResolution* 1920_1080_60
CameraControl
CameraId* 1
Mode* Off
CEC
Mode* On
Monitors* Auto
DefaultMainSource* 1

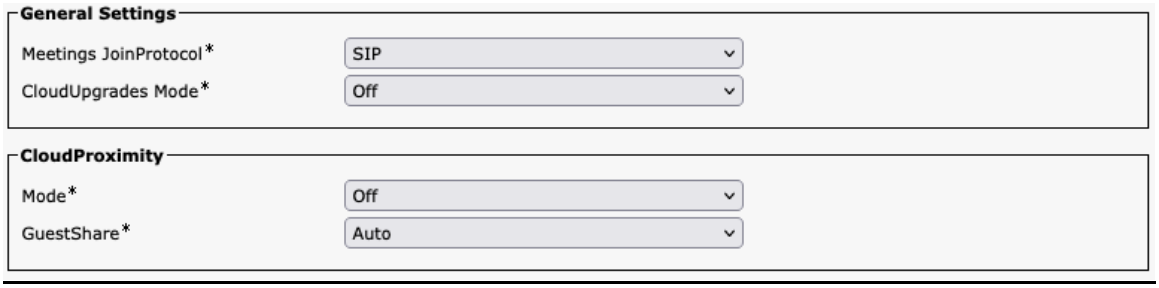


音声管理

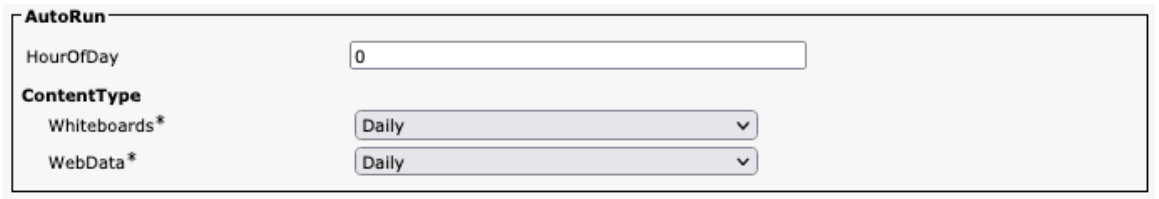


Web エンジン

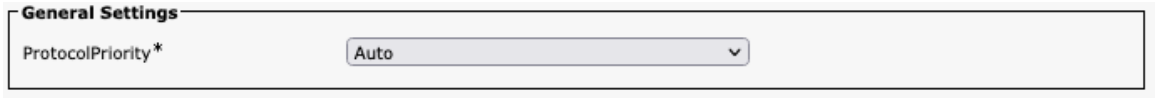
Webex



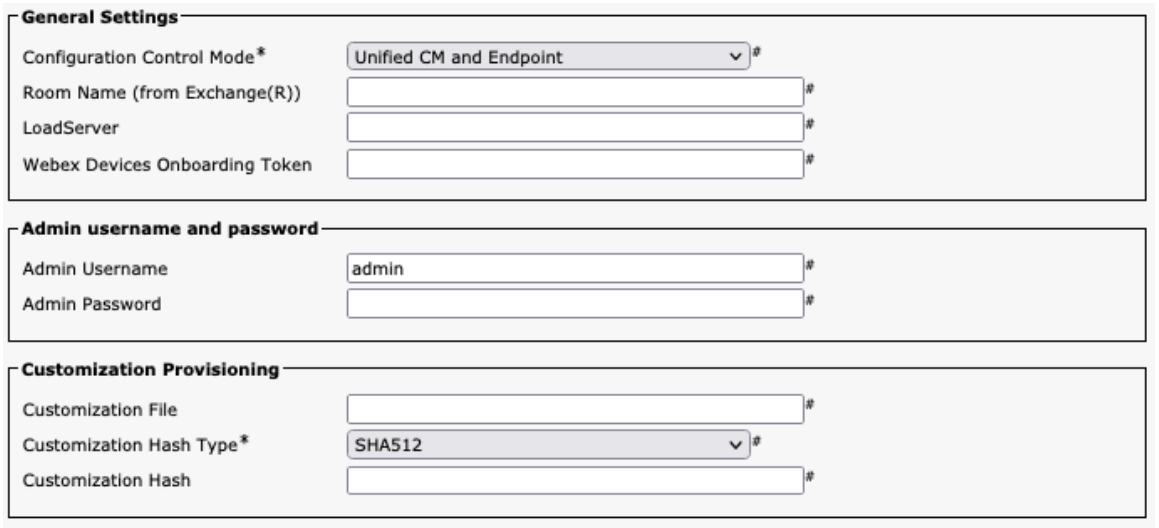
ルームクリーンアップ



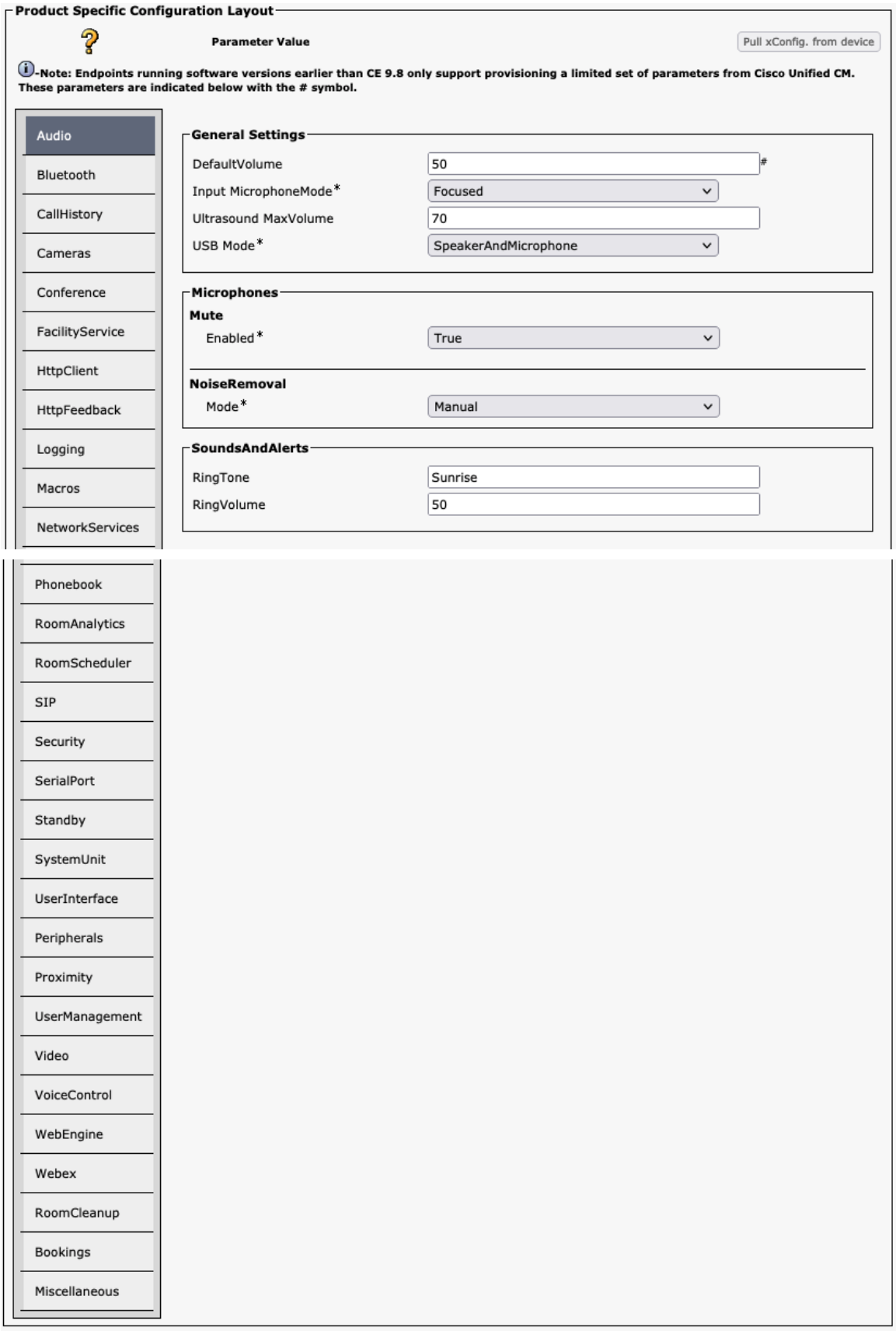
ブッキング



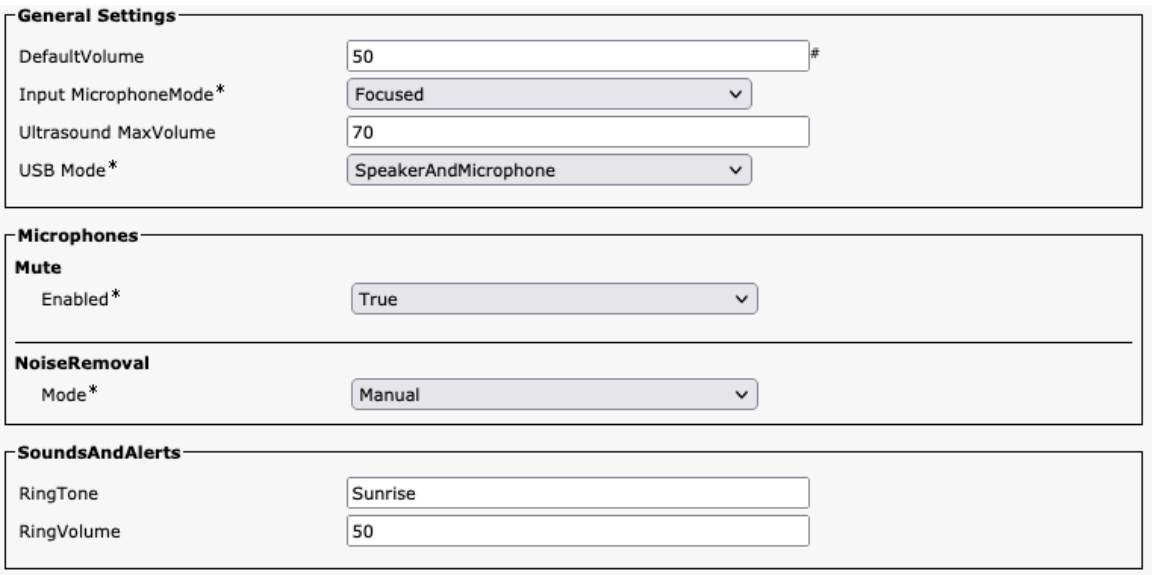
その他



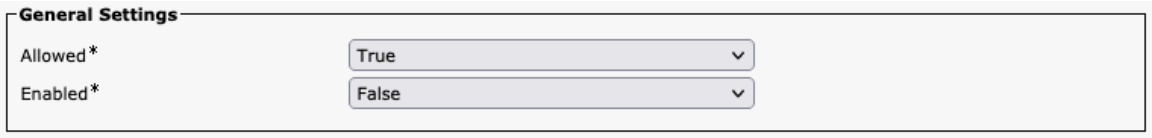
Webex Desk 構成オプション（バージョン 12.5 以降）



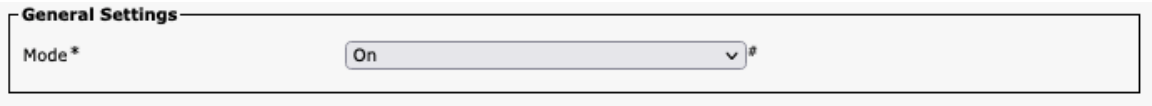
音声



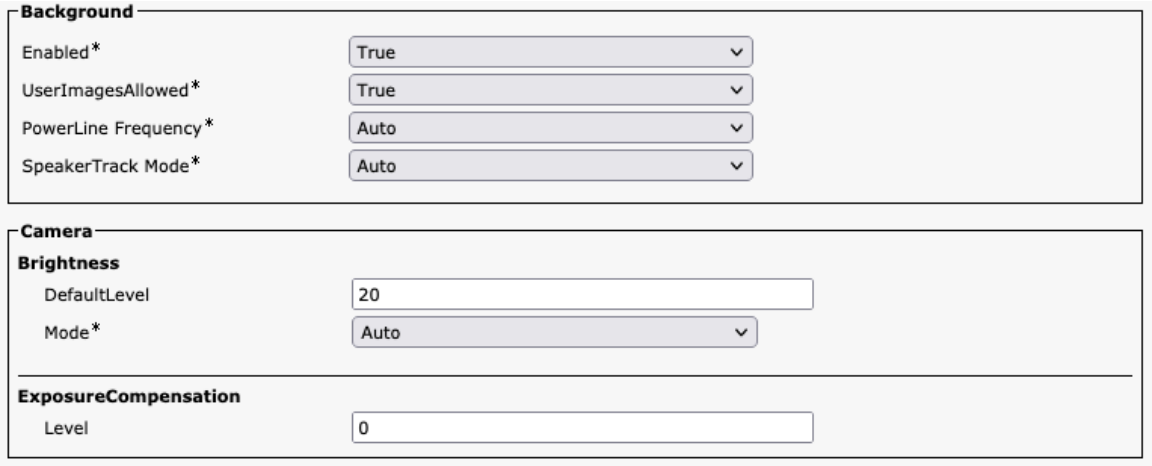
Bluetooth



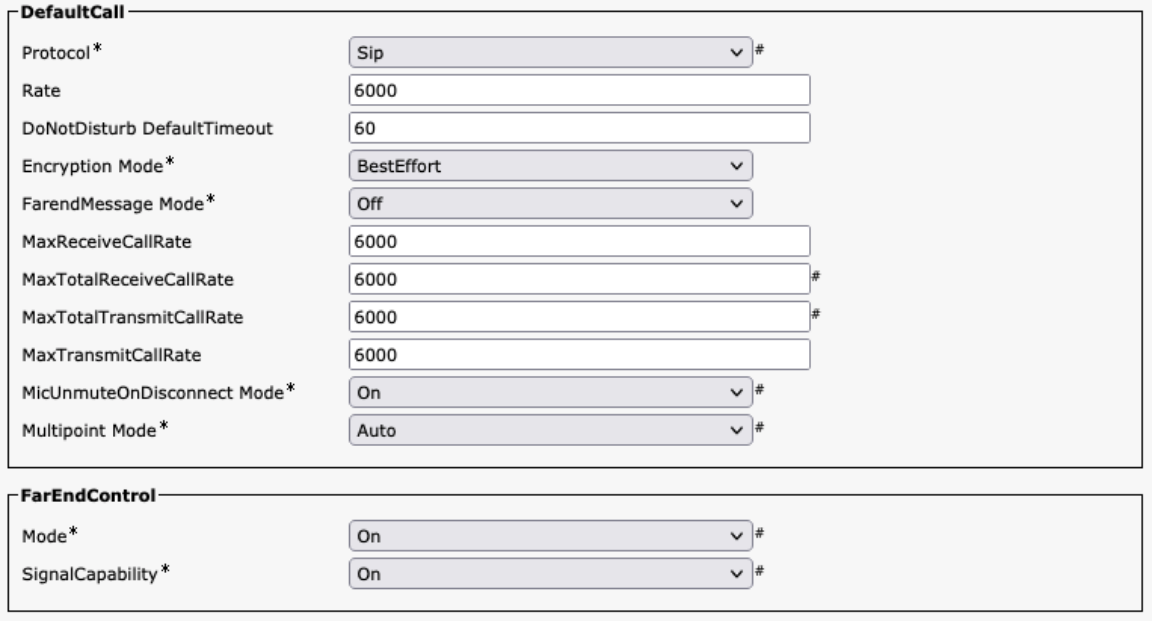
通話履歴



カメラ

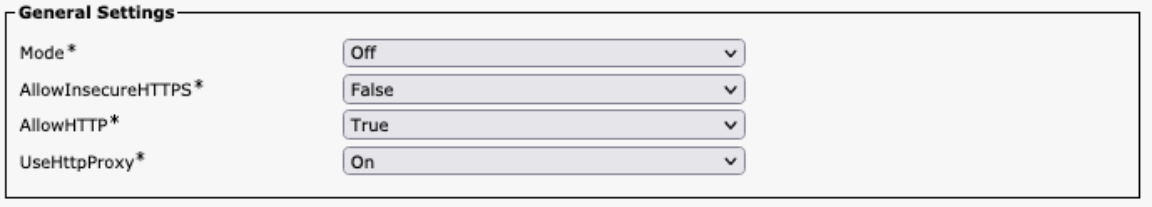


会議

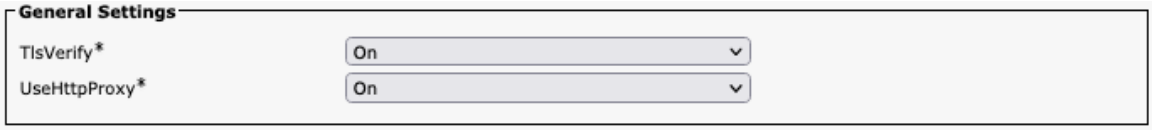


ファシリティサービス

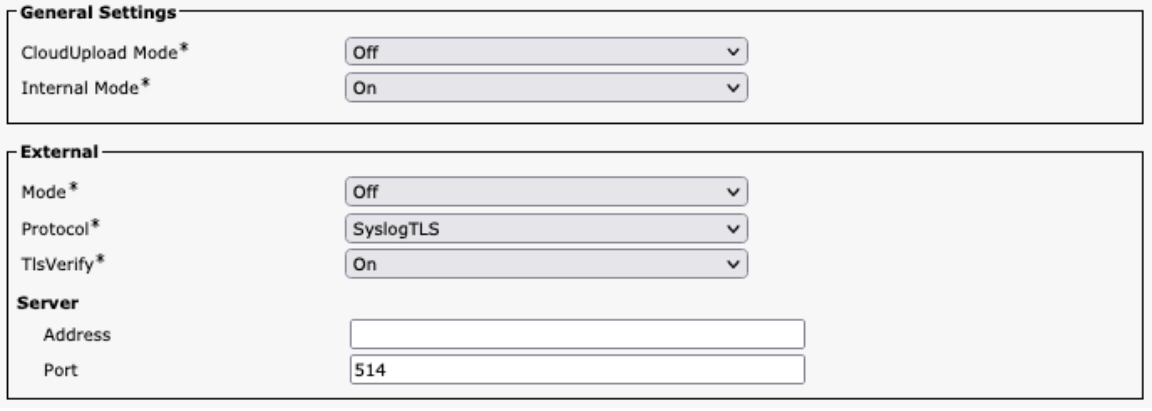
HTTP クライアント



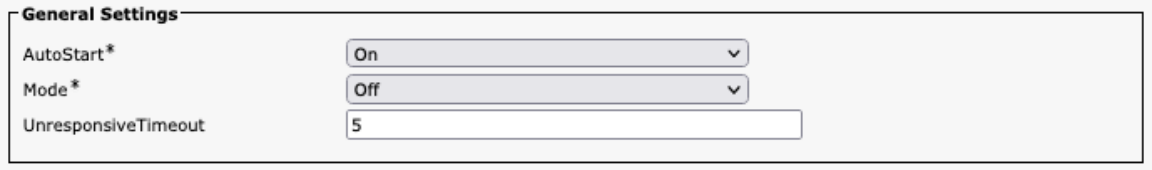
HTTP フィードバック



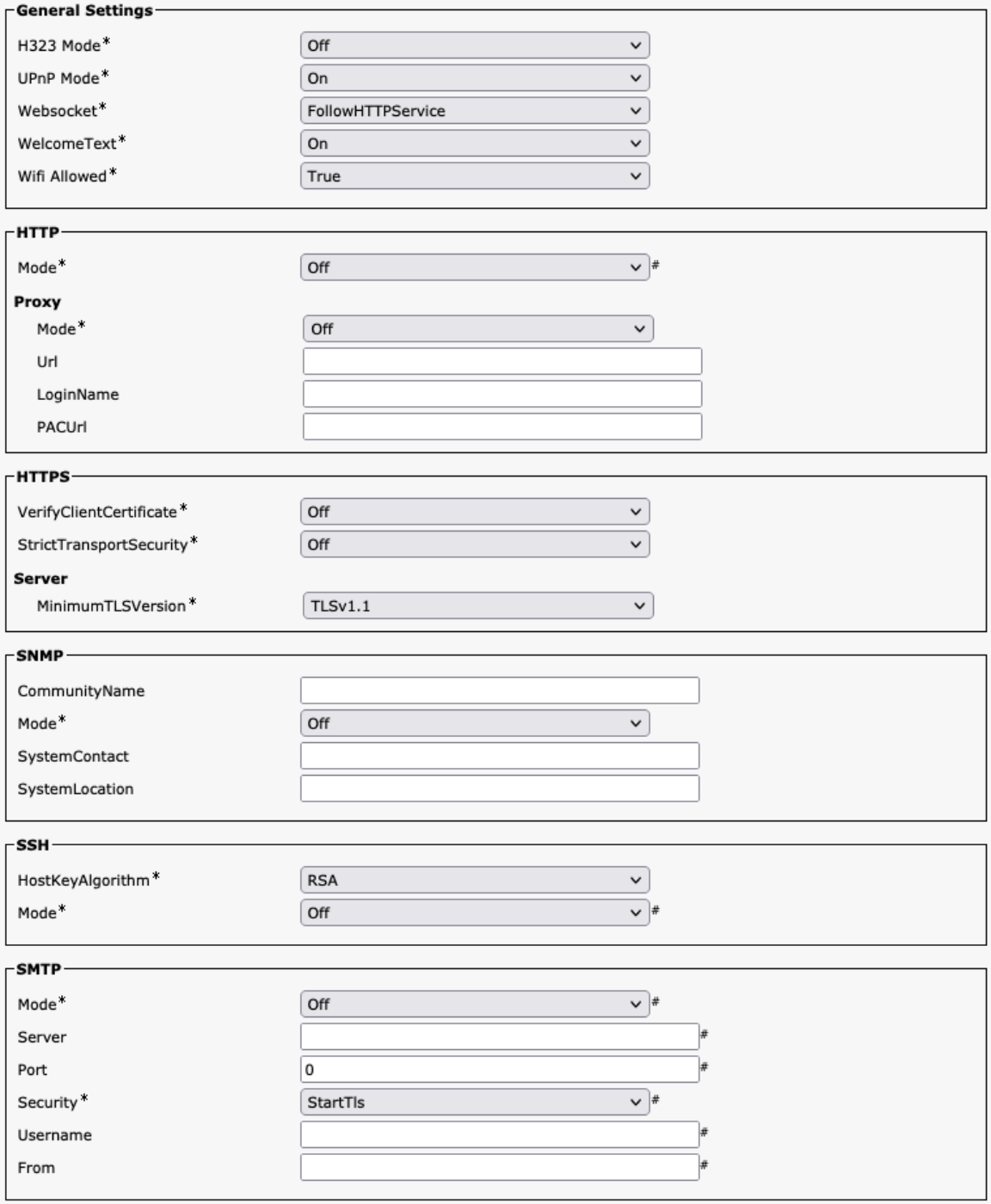
ロギング



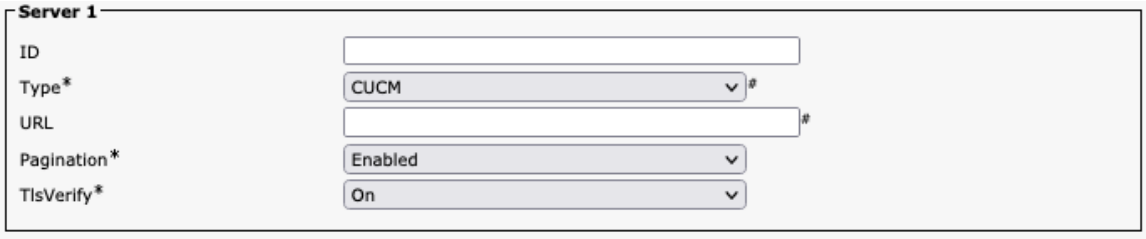
マクロ



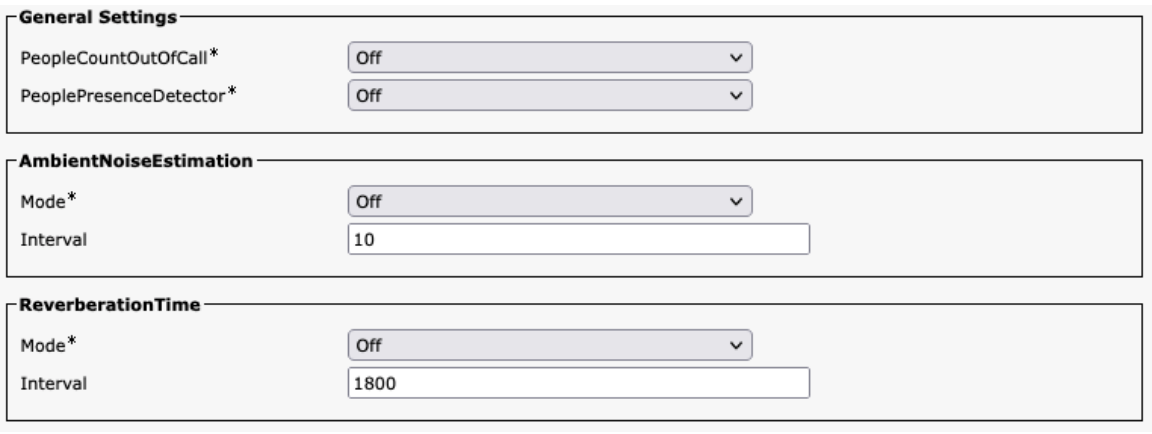
ネットワーク サービス



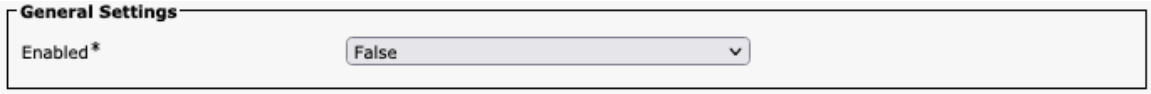
電話帳（Phone Book）



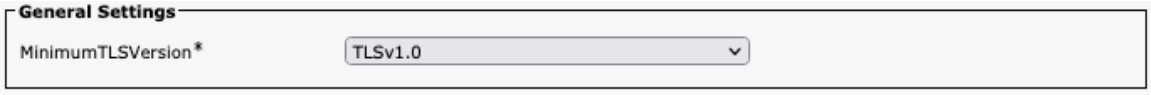
Room 分析



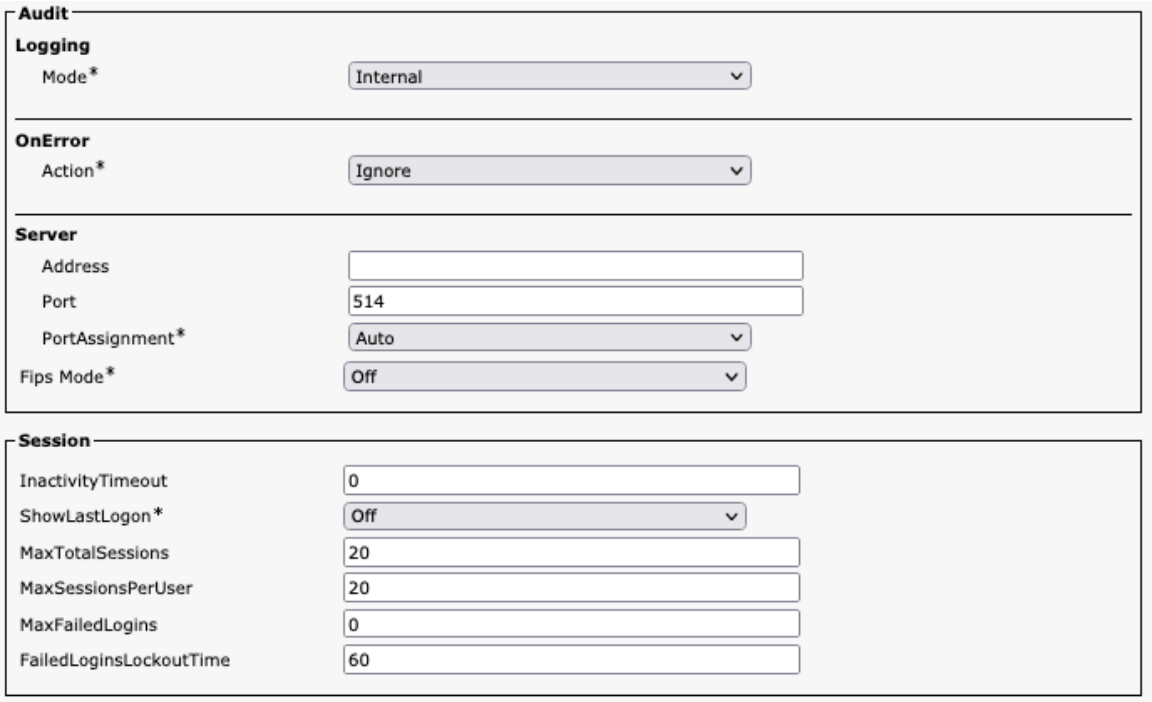
ルームスケジューラ



SIP

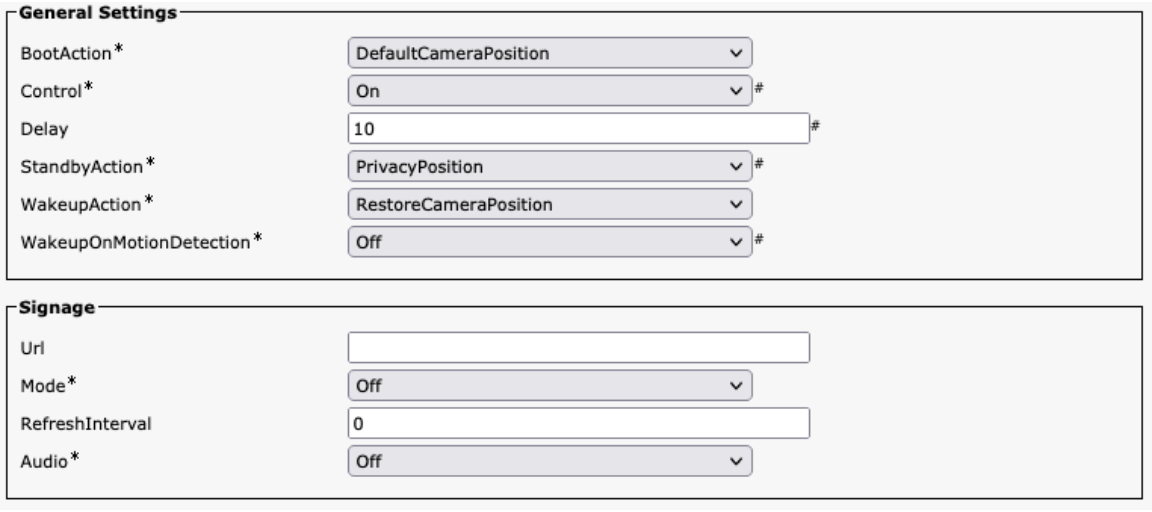


セキュリティ

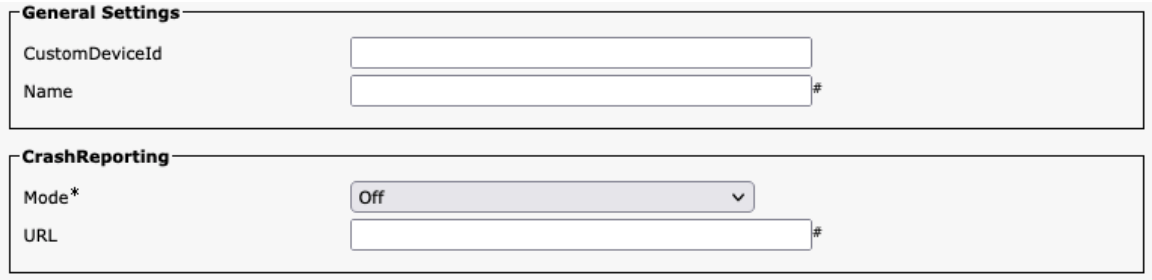


シリアルポート

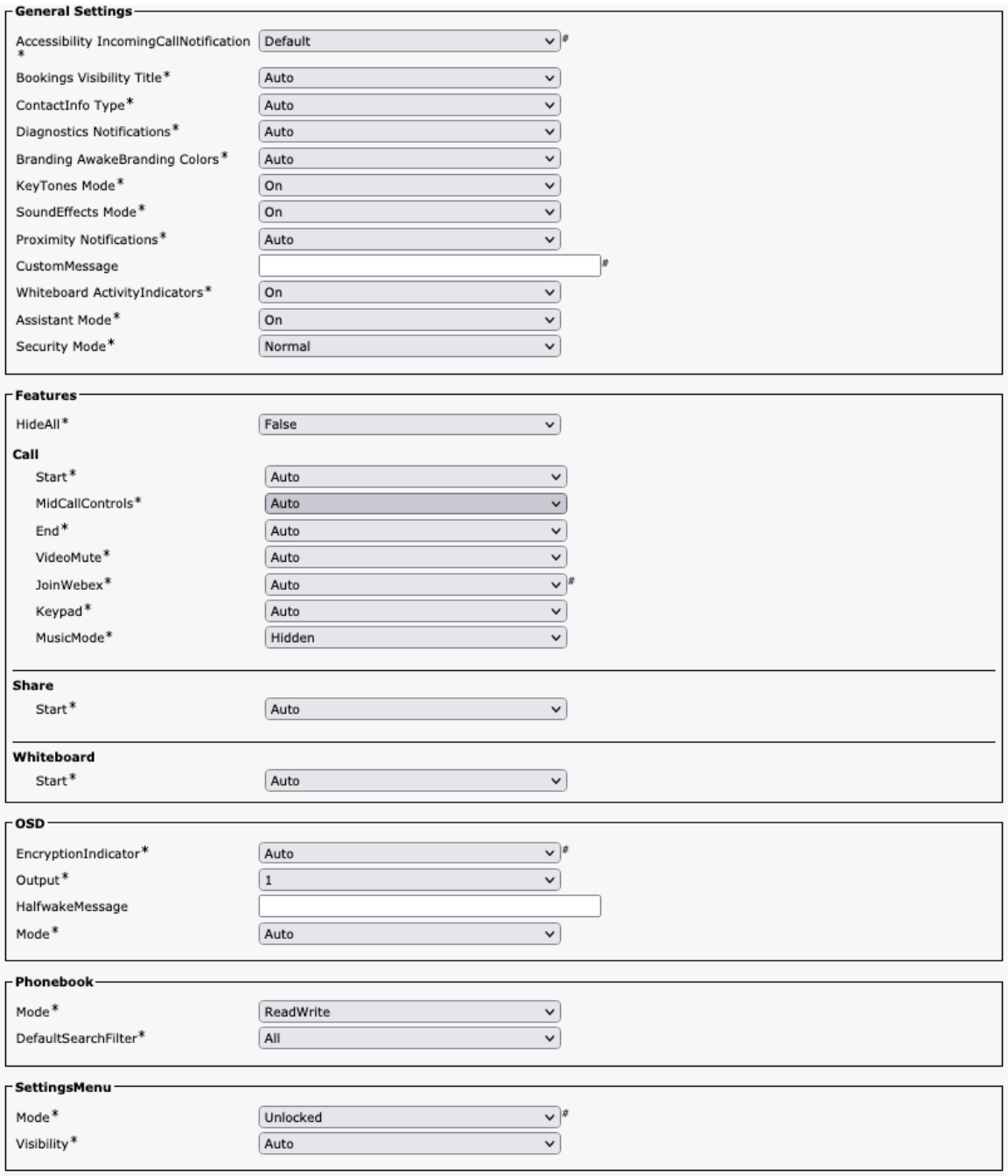
スタンバイ



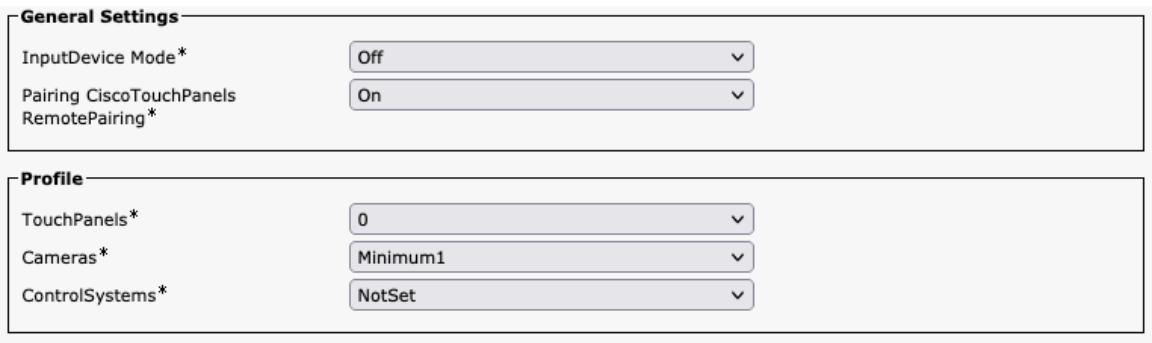
システム ユニット



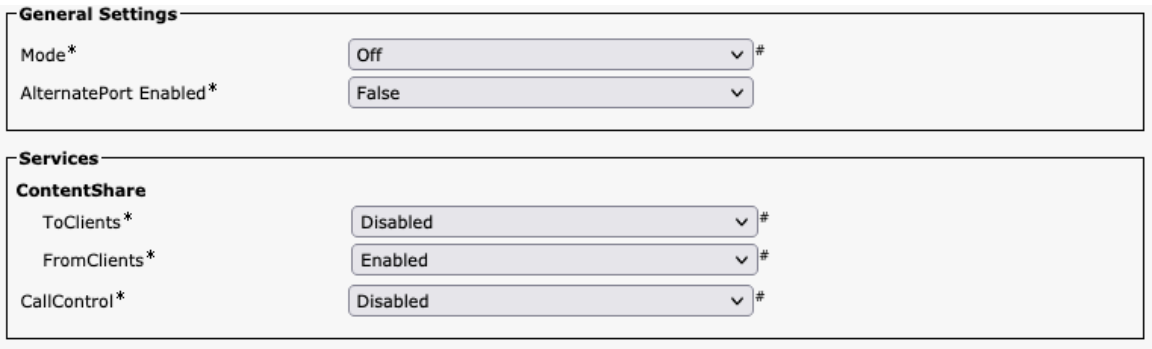
ユーザ インターフェイス



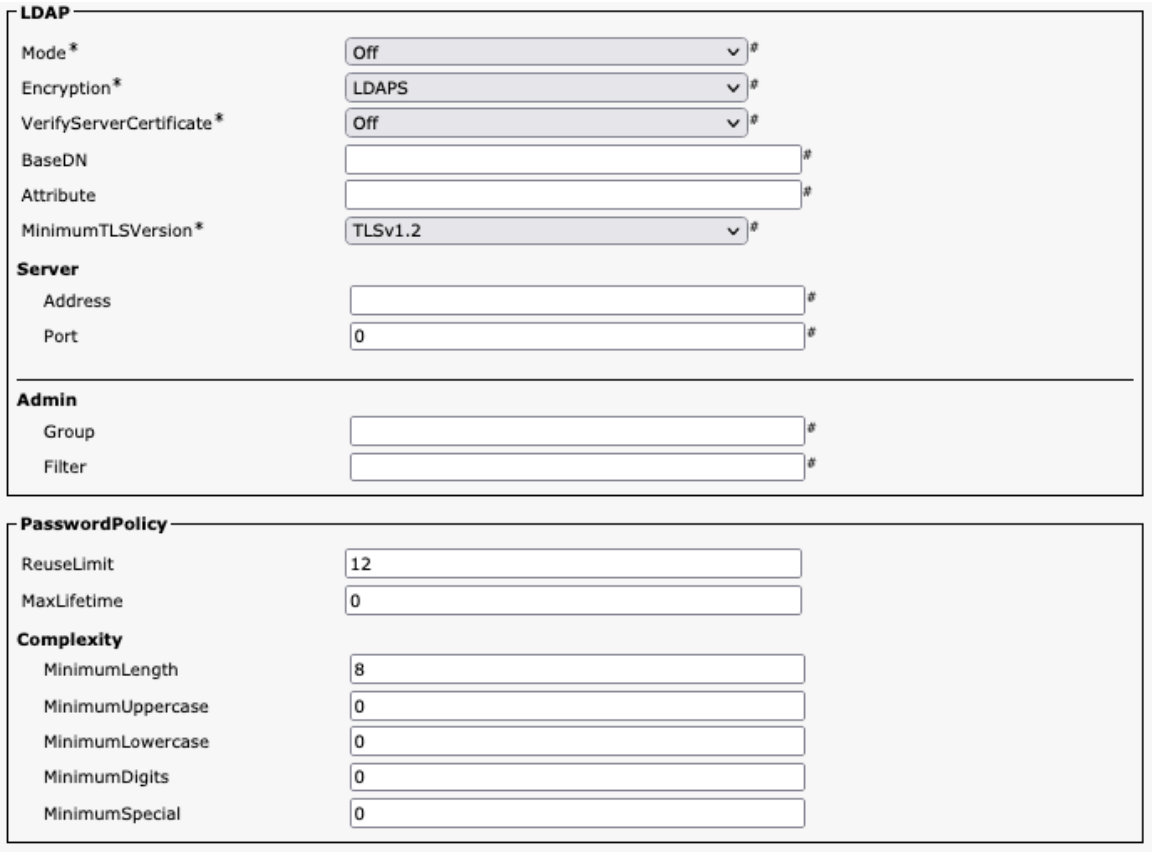
周辺機器



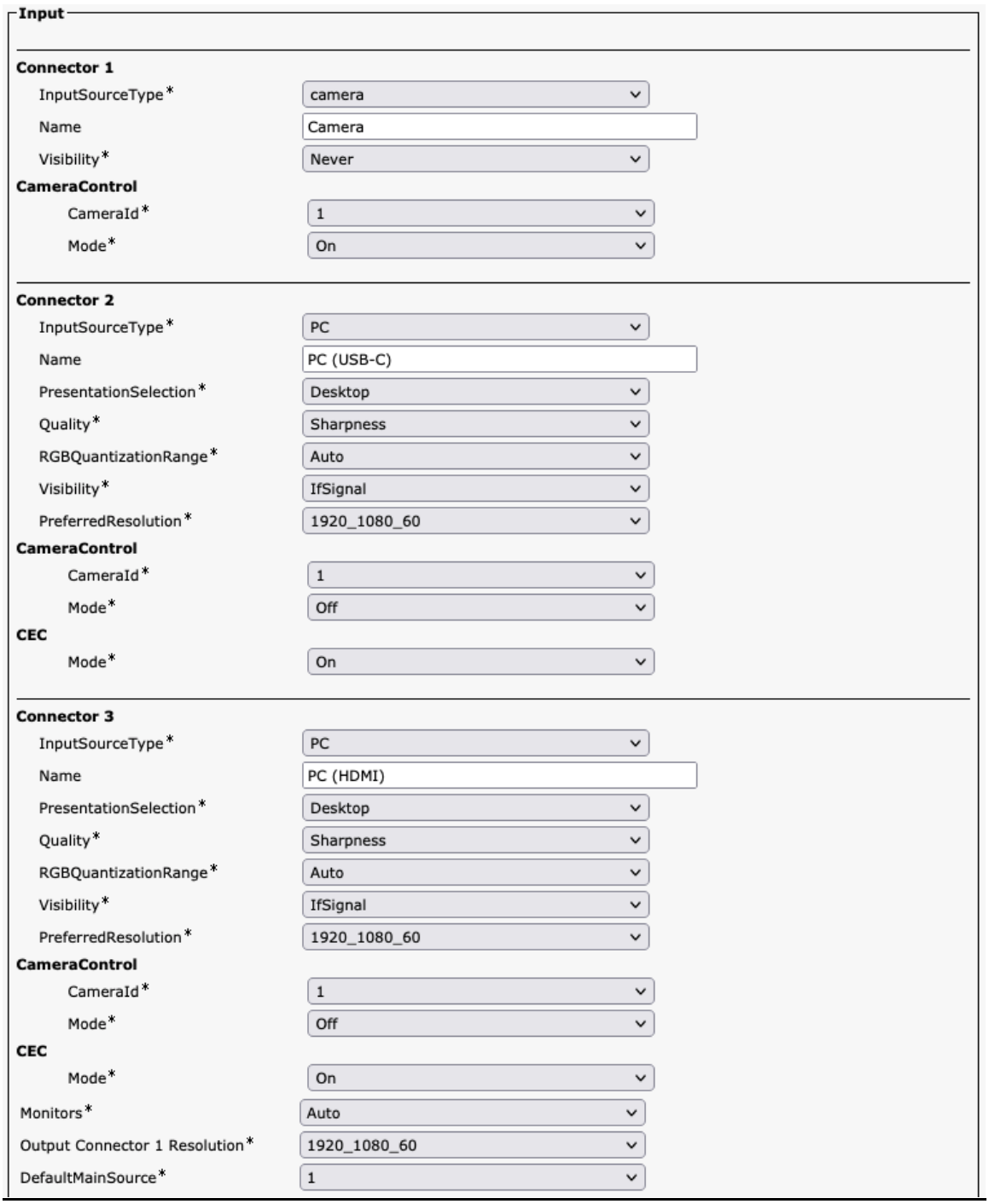
プロキシミティ

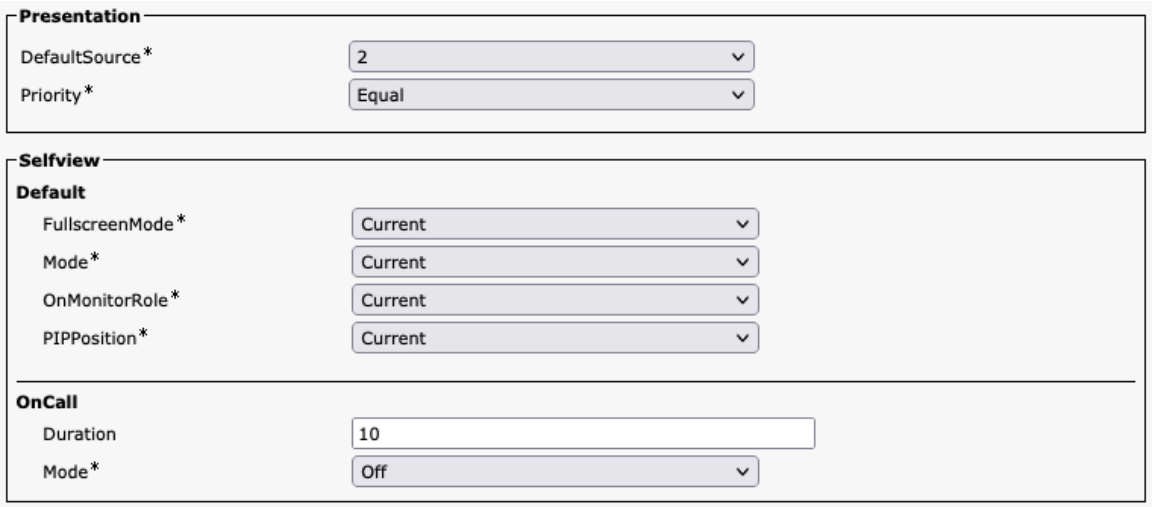


ユーザー管理

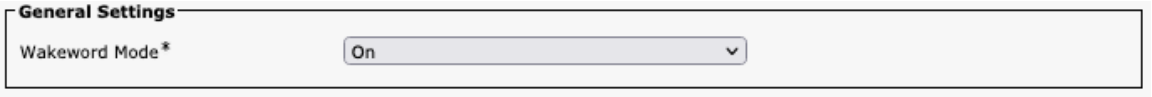


ビデオ

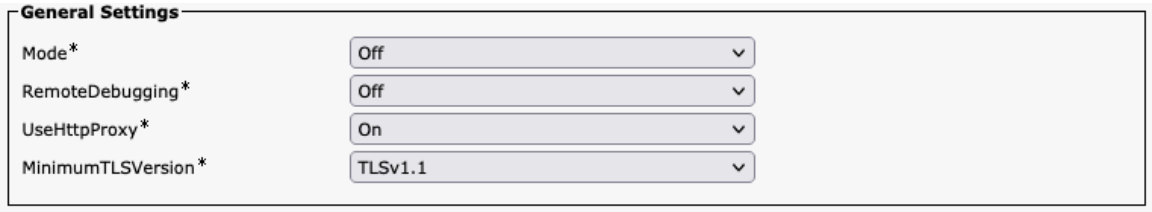

Input
Connector 1
InputSourceType* camera
Name Camera
Visibility* Never
CameraControl
CameraId* 1
Mode* On
Connector 2
InputSourceType* PC
Name PC (USB-C)
PresentationSelection* Desktop
Quality* Sharpness
RGBQuantizationRange* Auto
Visibility* IfSignal
PreferredResolution* 1920_1080_60
CameraControl
CameraId* 1
Mode* Off
CEC
Mode* On
Connector 3
InputSourceType* PC
Name PC (HDMI)
PresentationSelection* Desktop
Quality* Sharpness
RGBQuantizationRange* Auto
Visibility* IfSignal
PreferredResolution* 1920_1080_60
CameraControl
CameraId* 1
Mode* Off
CEC
Mode* On
Monitors* Auto
Output Connector 1 Resolution* 1920_1080_60
DefaultMainSource* 1



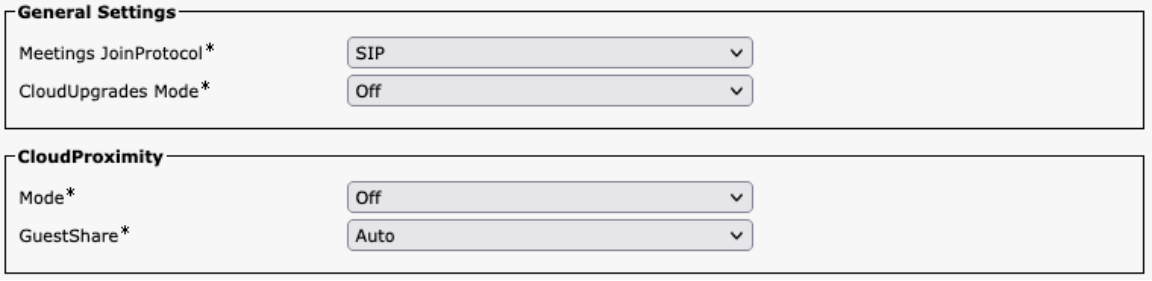
音声管理



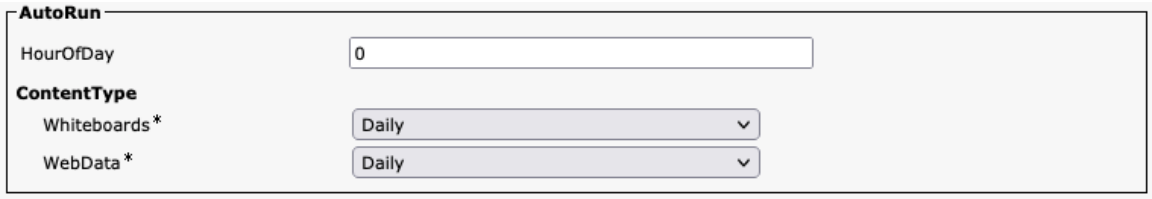
Web エンジン



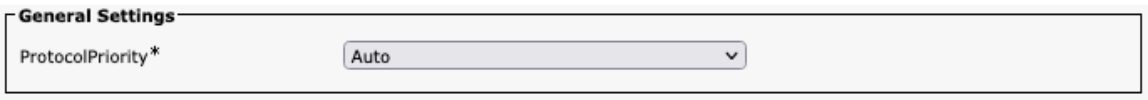
Webex



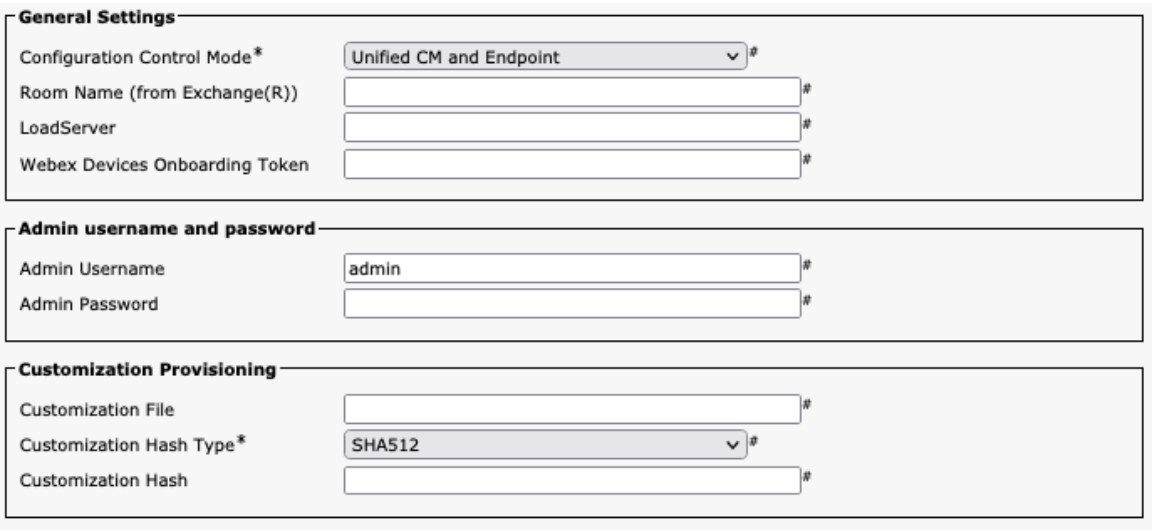
ルームクリーンアップ



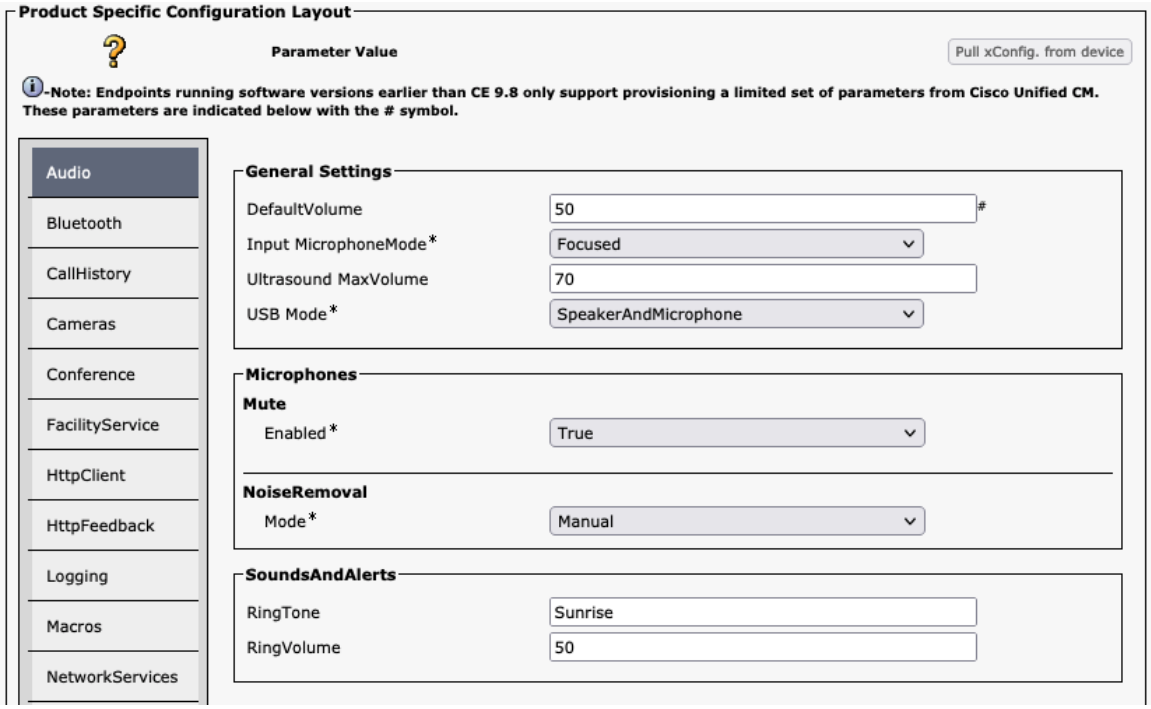
ブッキング

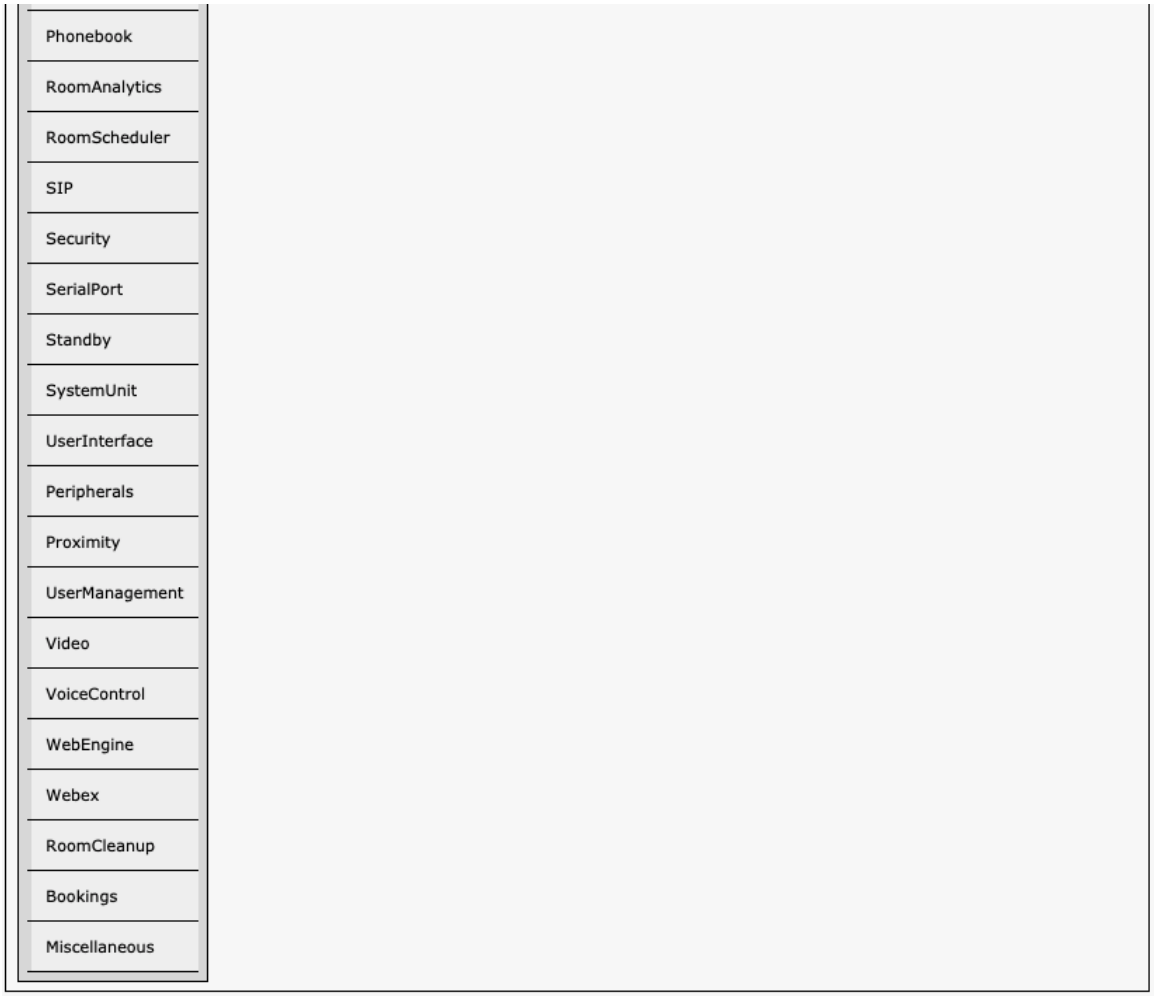


その他

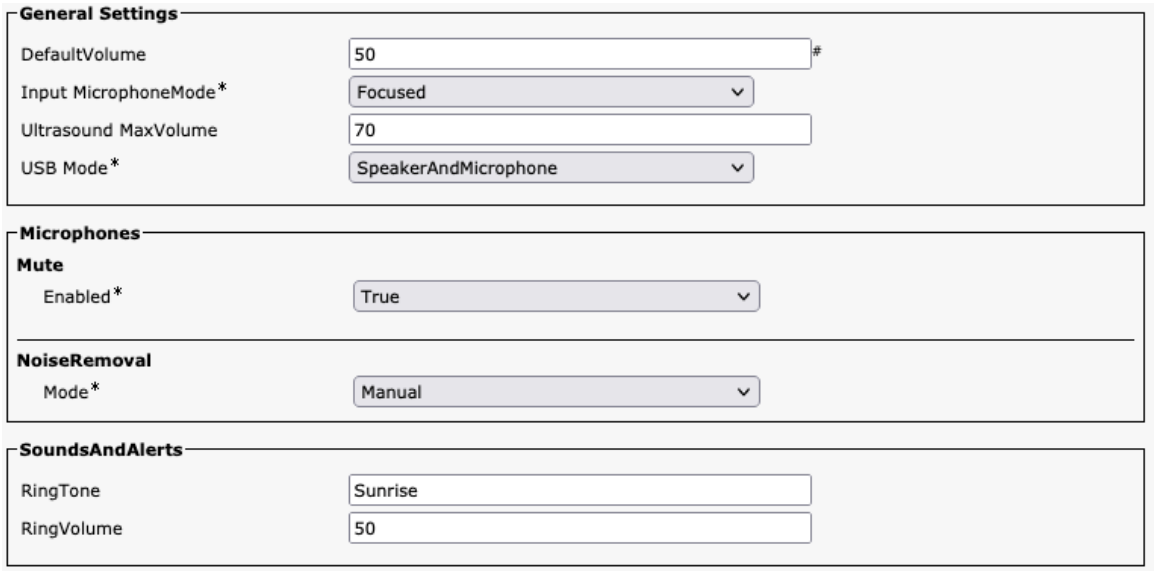


Webex Desk Mini 構成オプション（バージョン 12.5 以降）

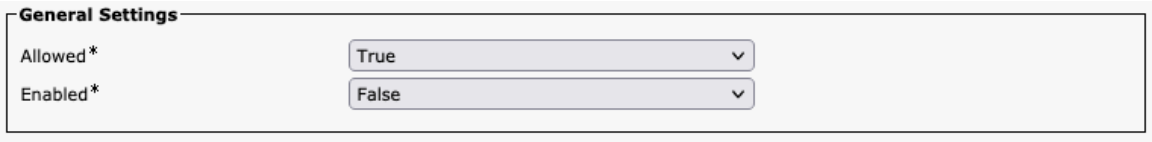



Phonebook
RoomAnalytics
RoomScheduler
SIP
Security
SerialPort
Standby
SystemUnit
UserInterface
Peripherals
Proximity
UserManagement
Video
VoiceControl
WebEngine
Webex
RoomCleanup
Bookings
Miscellaneous

音声

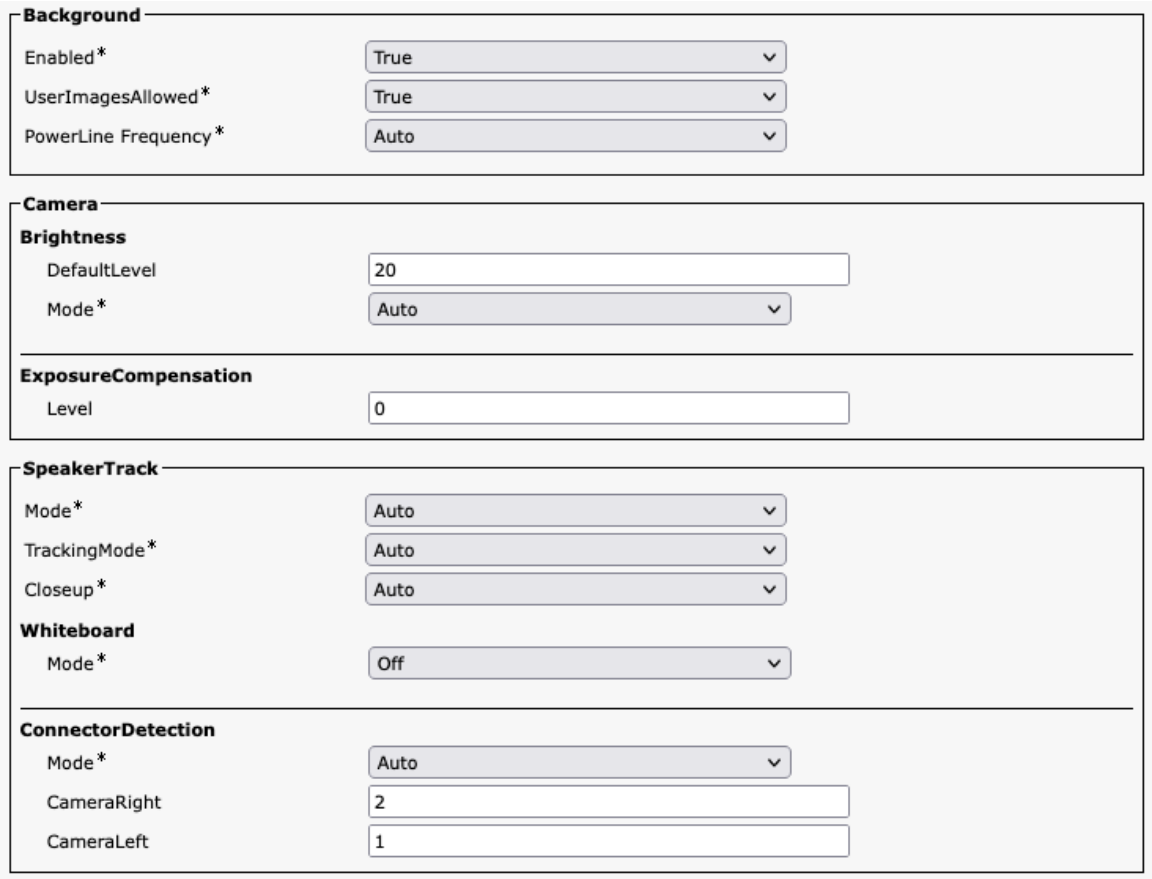

General Settings
DefaultVolume
50
#
Input MicrophoneMode*
Focused
Ultrasound MaxVolume
70
USB Mode*
SpeakerAndMicrophone
Microphones
Mute
Enabled*
True
NoiseRemoval
Mode*
Manual
SoundsAndAlerts
RingTone
Sunrise
RingVolume
50

Bluetooth

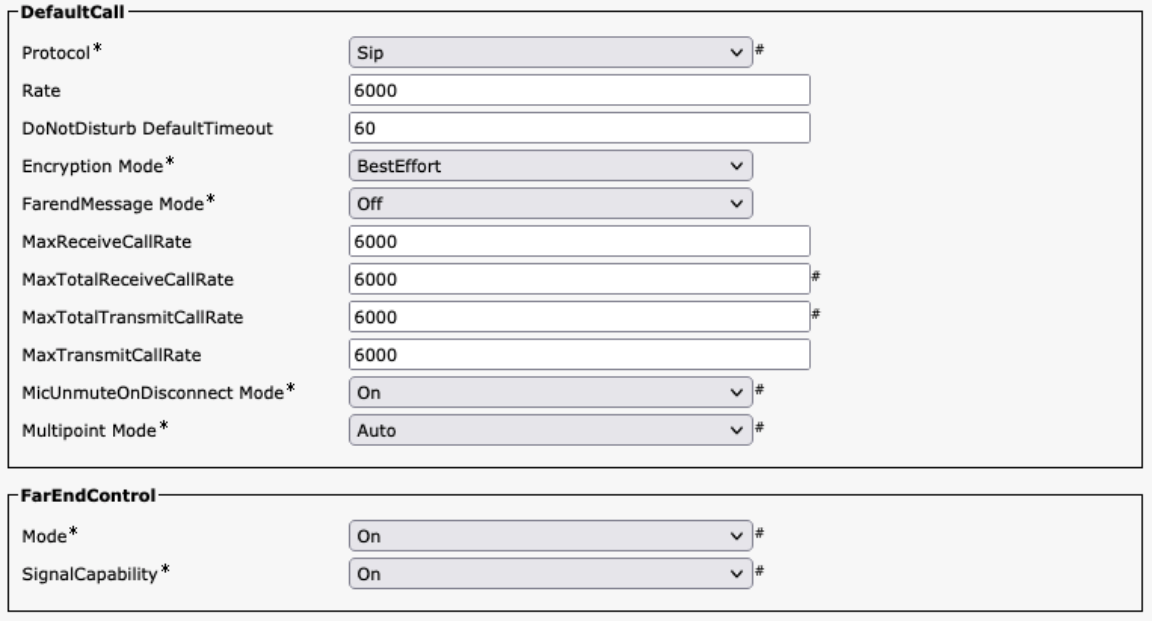


通話履歴

カメラ

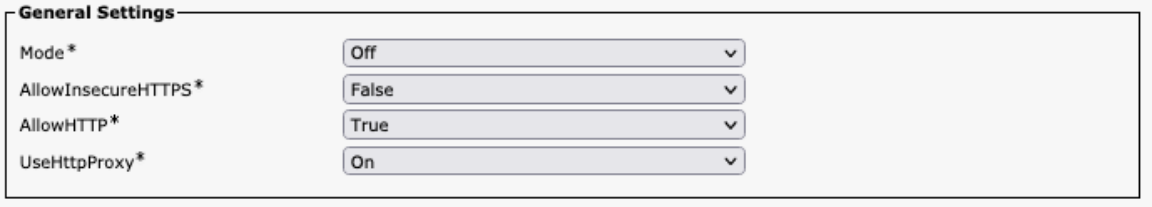


会議

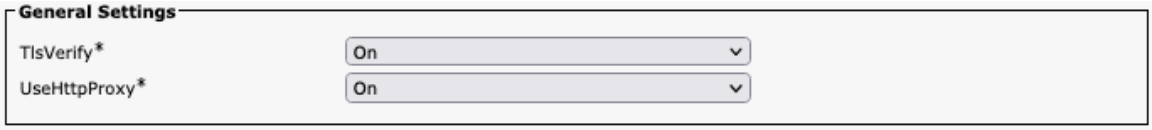


ファシリティサービス

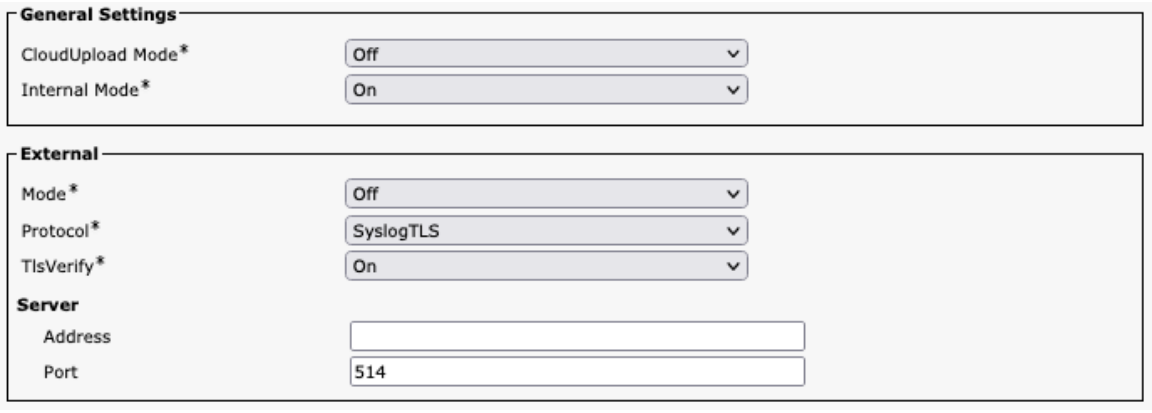
HTTP クライアント



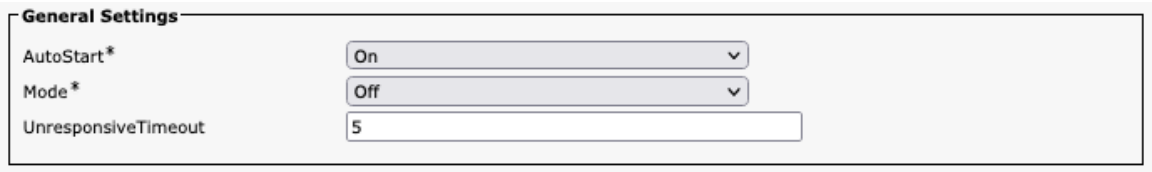
HTTP フィードバック



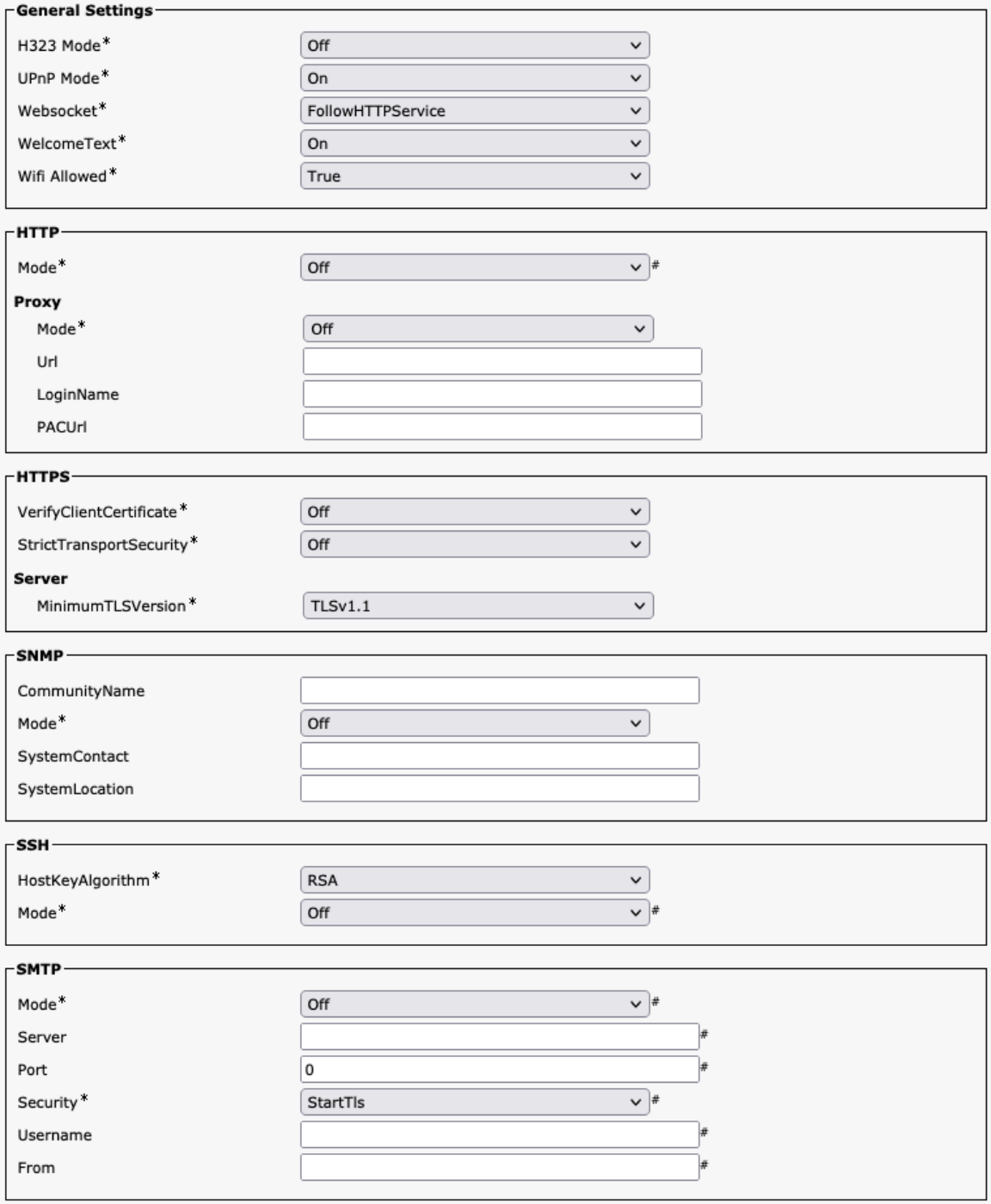
ロギング



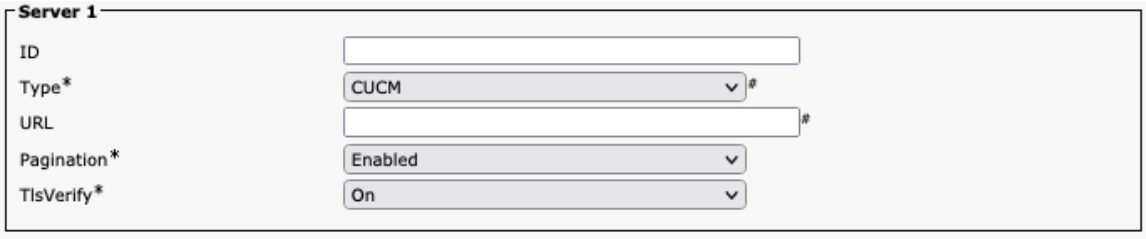
マクロ



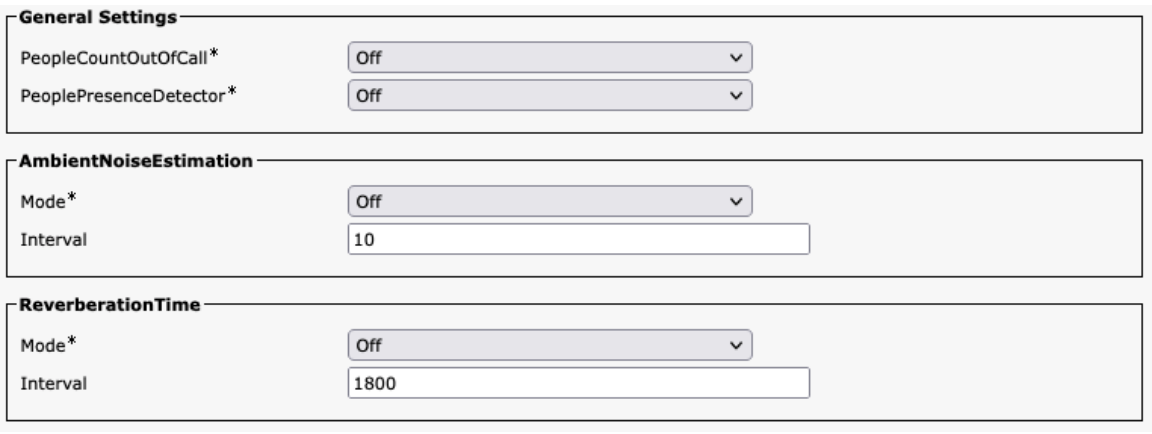
ネットワーク サービス



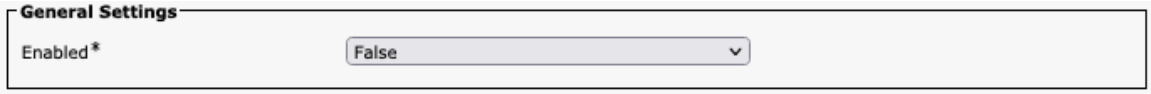
電話帳（Phone Book）



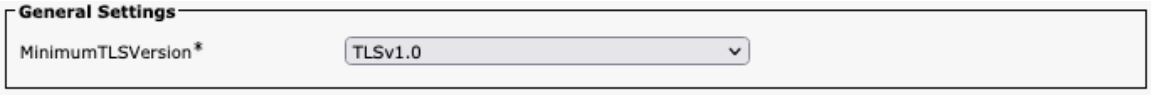
Room 分析



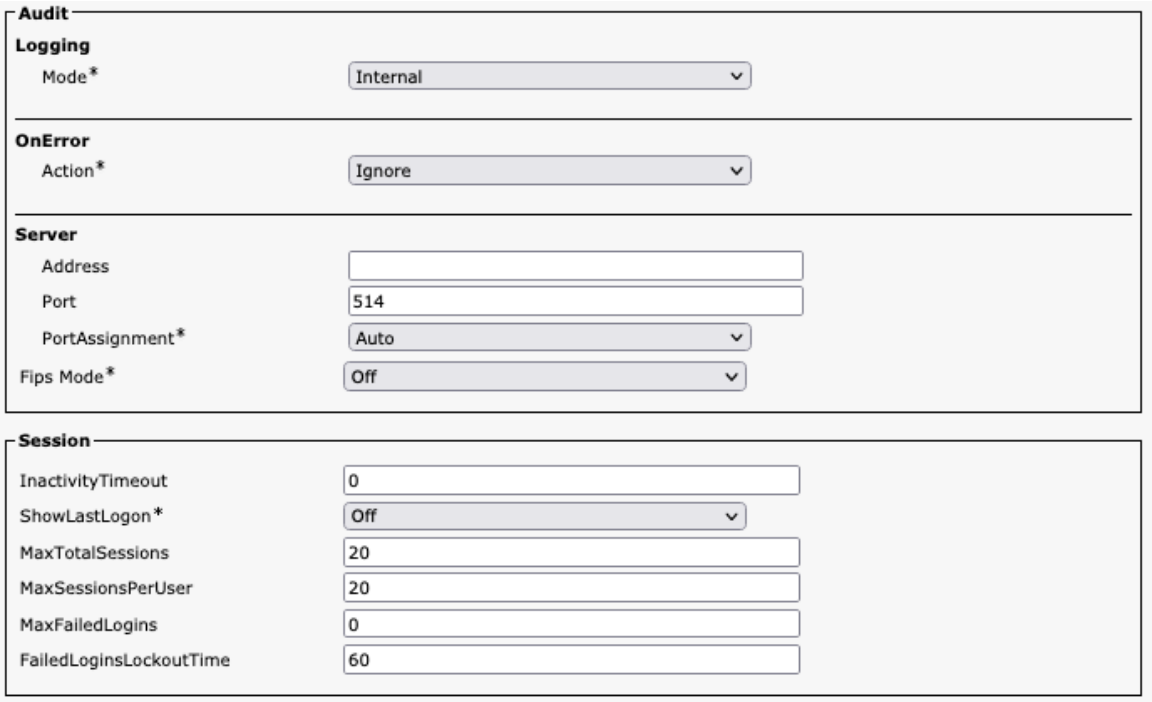
ルームスケジューラ



SIP

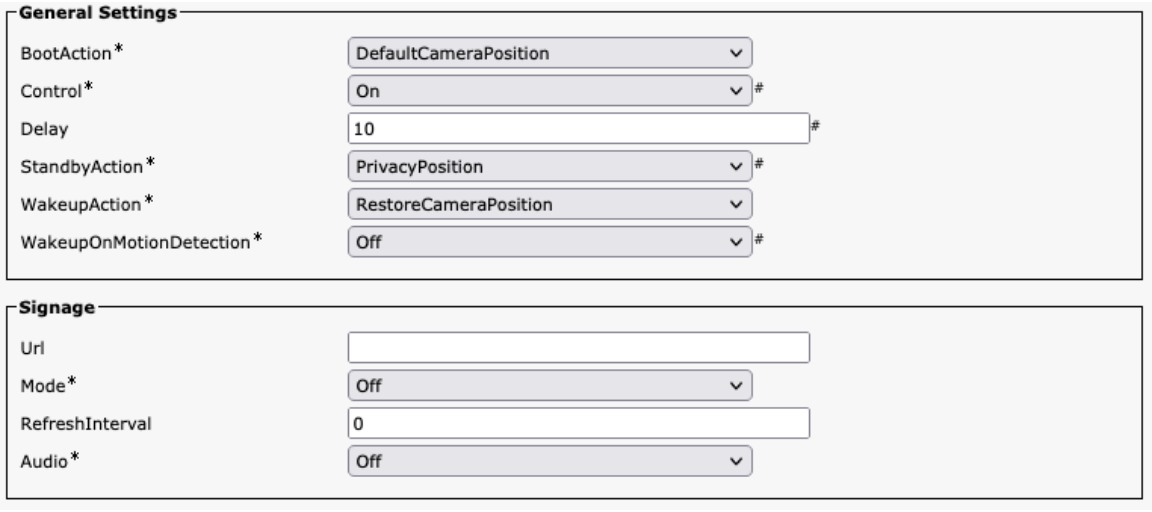


セキュリティ

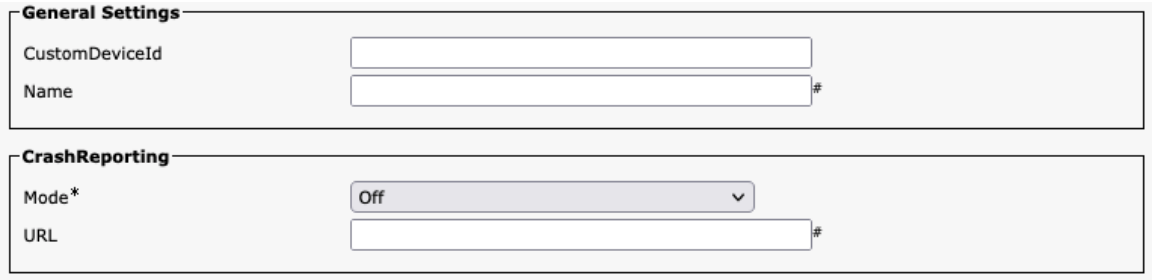


シリアルポート

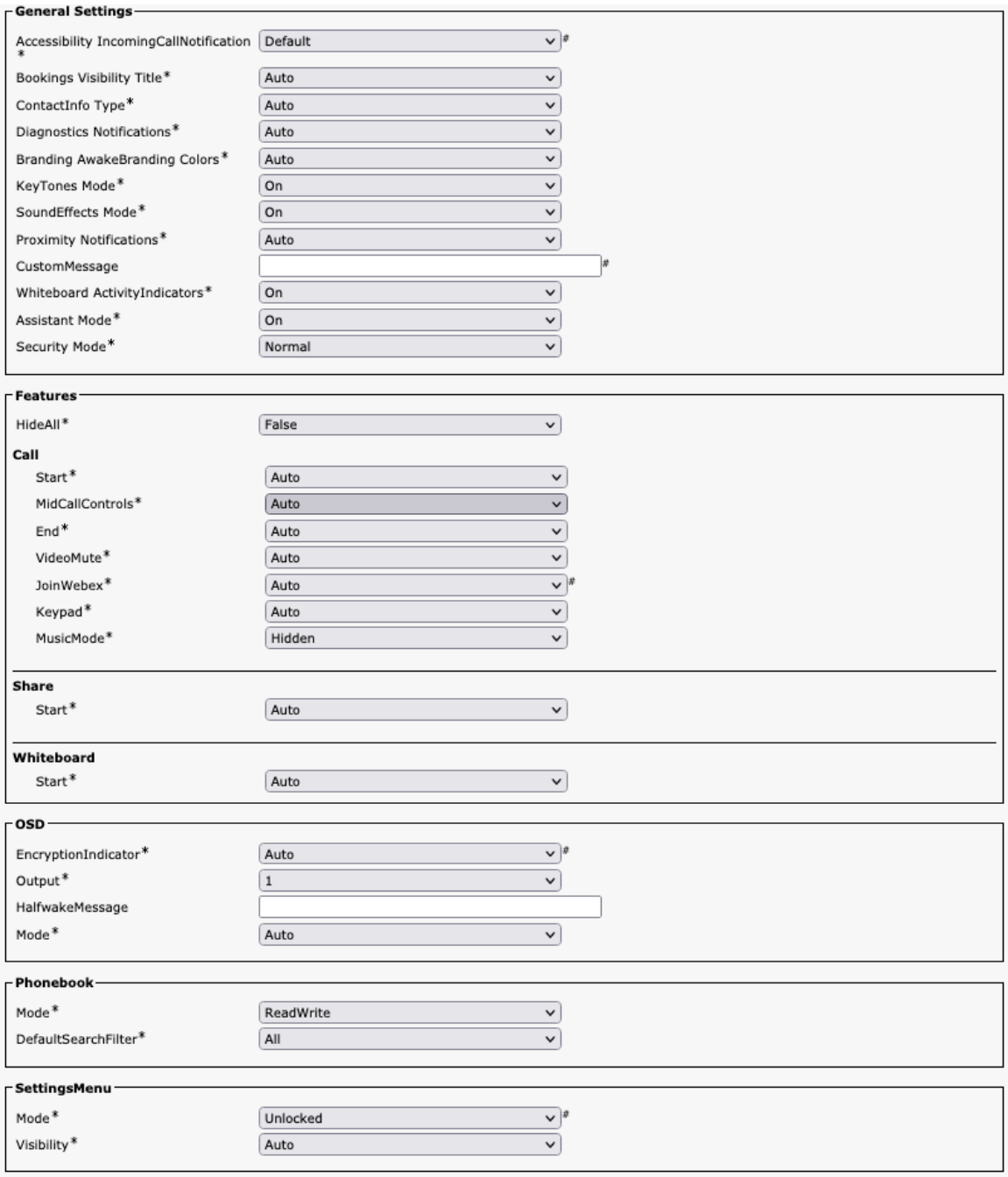
スタンバイ



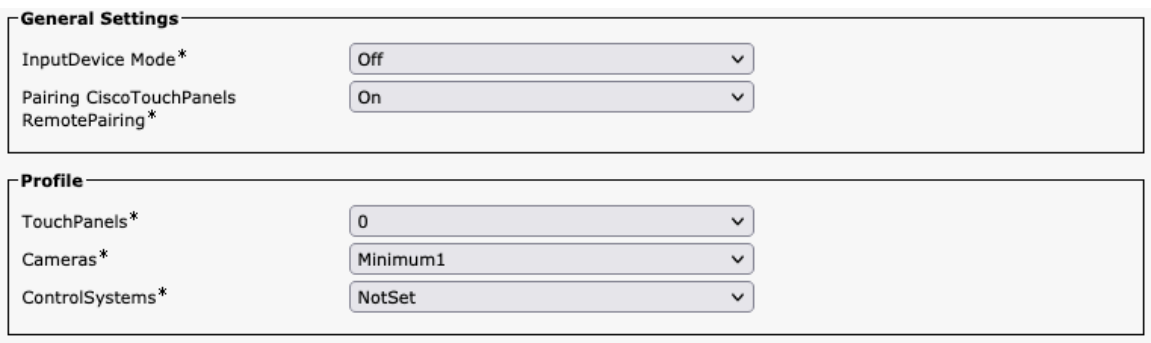
システム ユニット



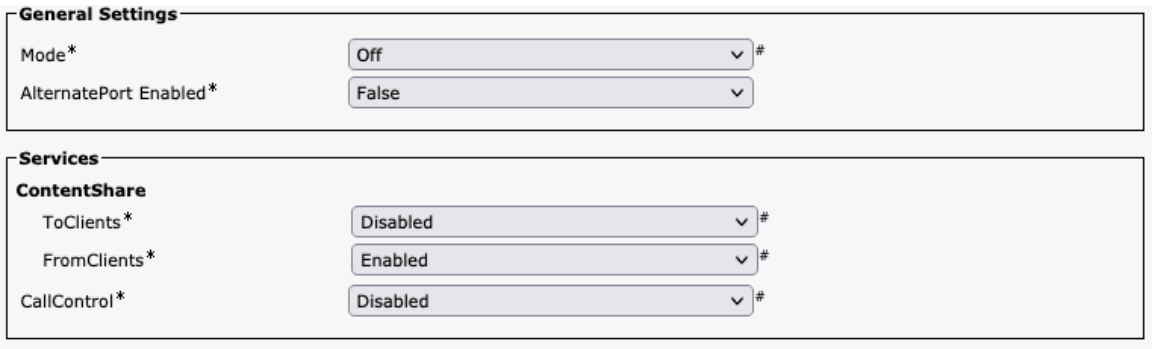
ユーザ インターフェイス



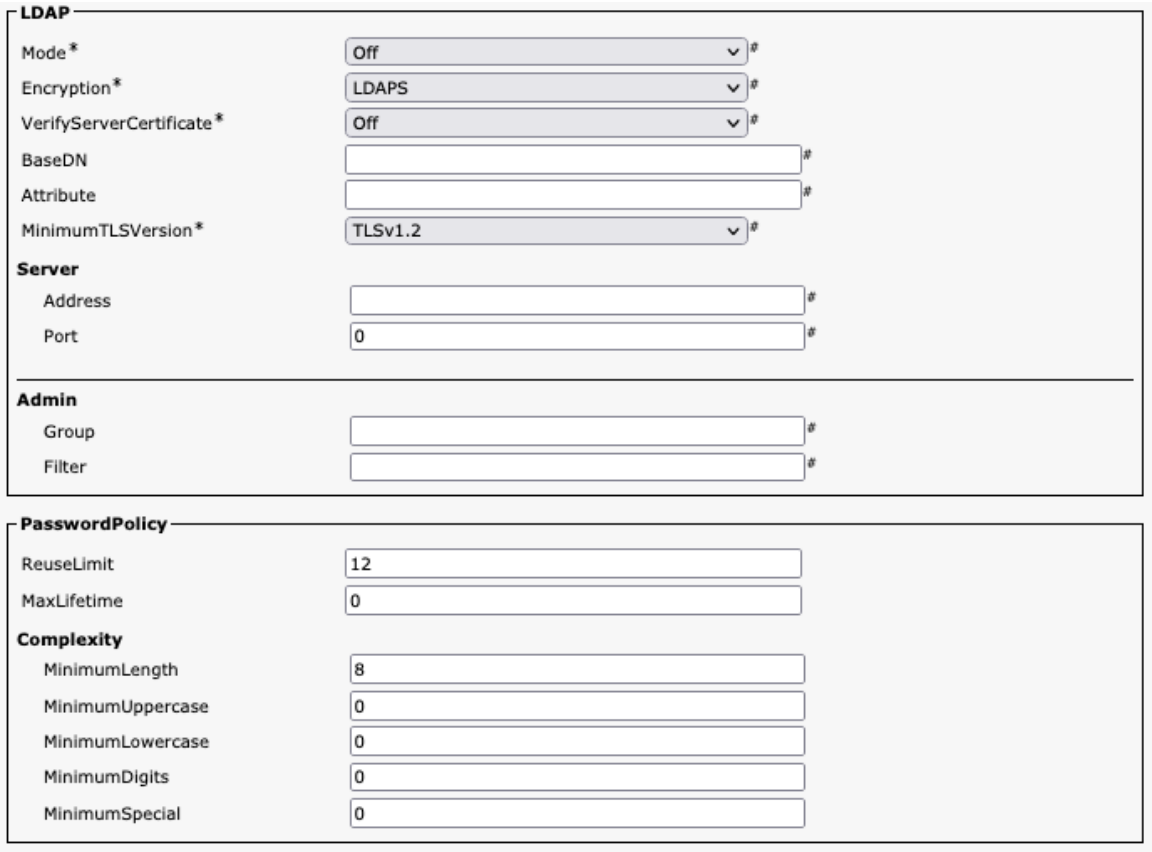
周辺機器



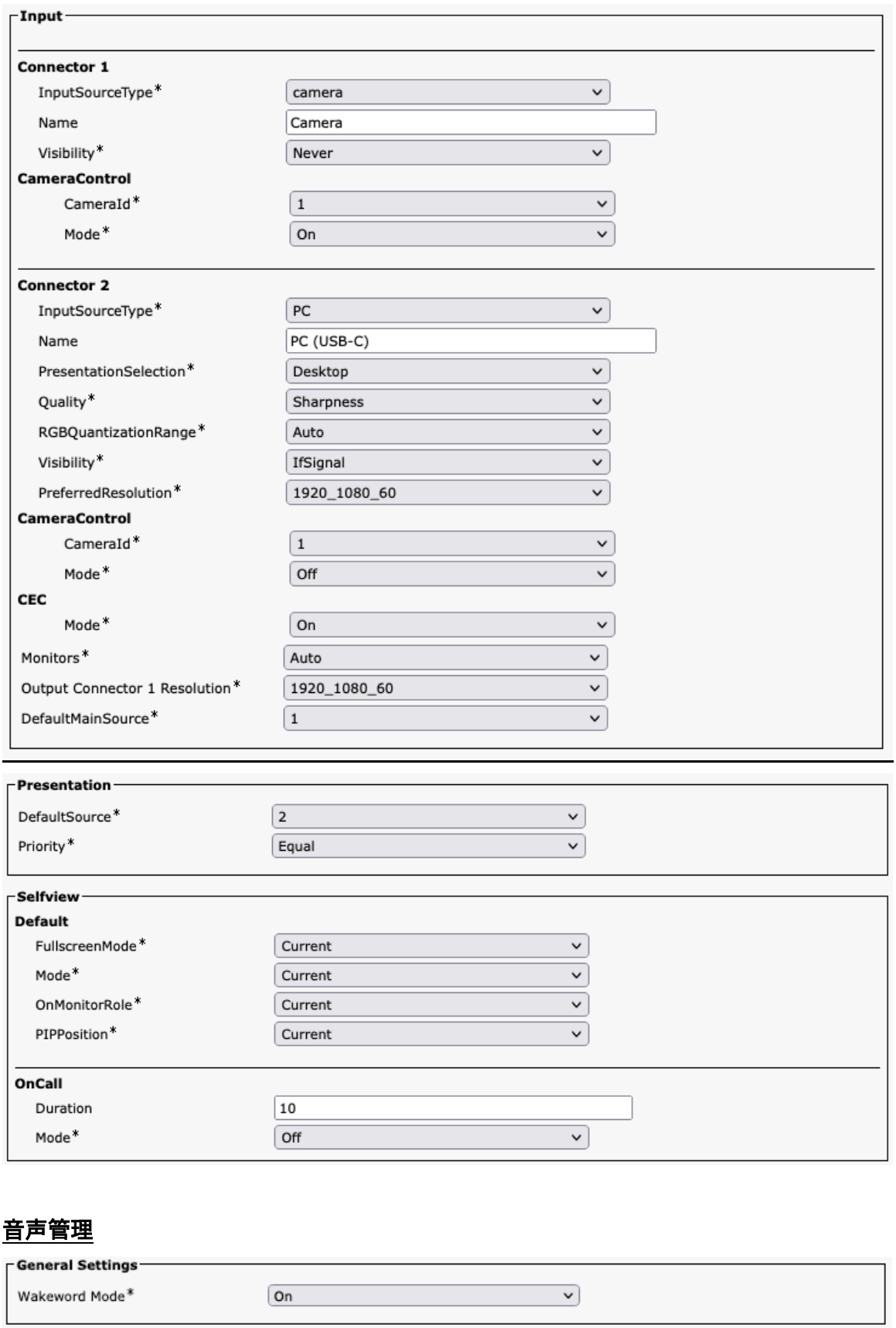
プロキシミティ



ユーザー管理



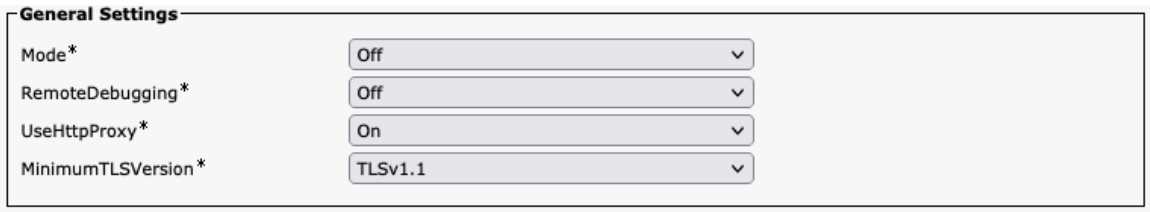
ビデオ


Input
Connector 1
InputSourceType*
camera
Name
Camera
Visibility*
Never
CameraControl
CameraId*
1
Mode*
On
Connector 2
InputSourceType*
PC
Name
PC (USB-C)
PresentationSelection*
Desktop
Quality*
Sharpness
RGBQuantizationRange*
Auto
Visibility*
IfSignal
PreferredResolution*
1920_1080_60
CameraControl
CameraId*
1
Mode*
Off
CEC
Mode*
On
Monitors*
Auto
Output Connector 1 Resolution*
1920_1080_60
DefaultMainSource*
1
Presentation
DefaultSource*
2
Priority*
Equal
Selfview
Default
FullscreenMode*
Current
Mode*
Current
OnMonitorRole*
Current
PIPPosition*
Current
OnCall
Duration
10
Mode*
Off

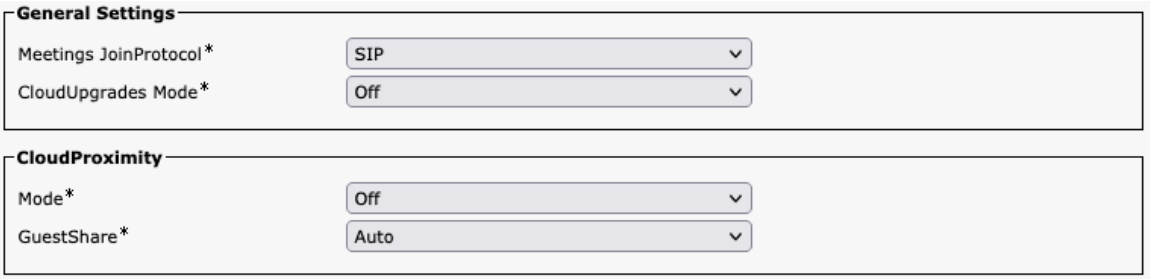
音声管理

General Settings
Wakeword Mode*
On

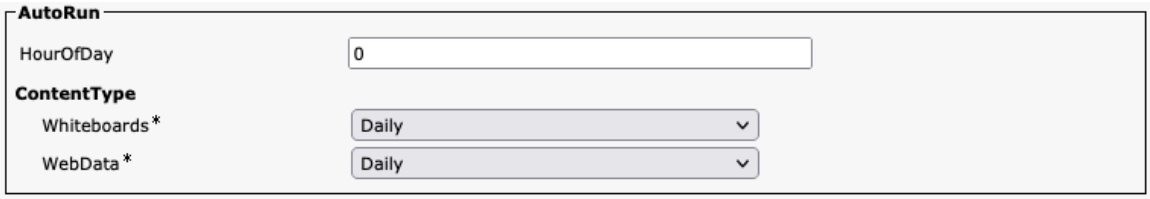
Web エンジン



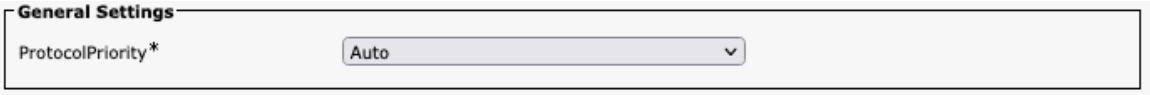
Webex



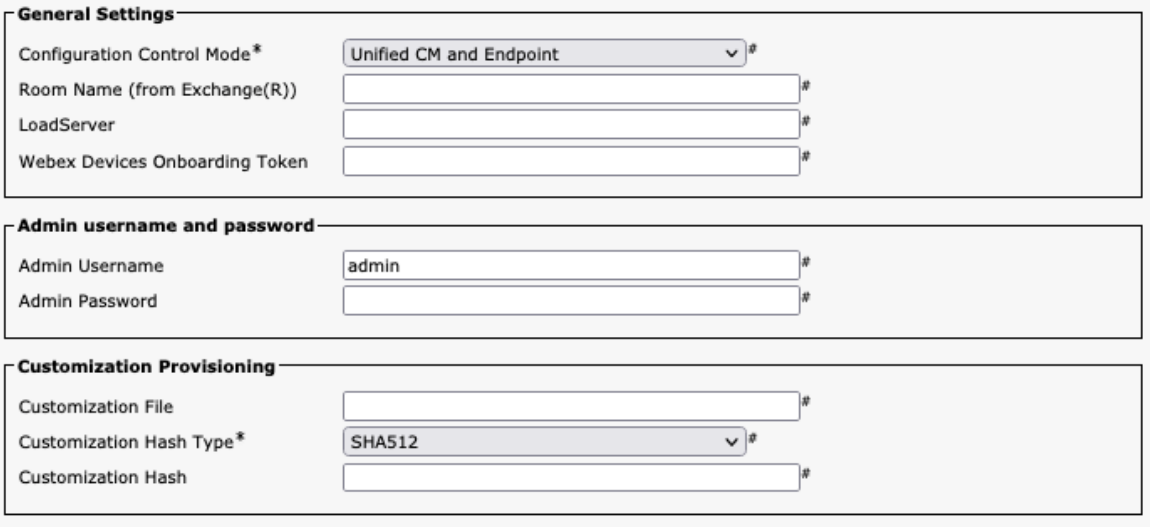
ルームクリーンアップ



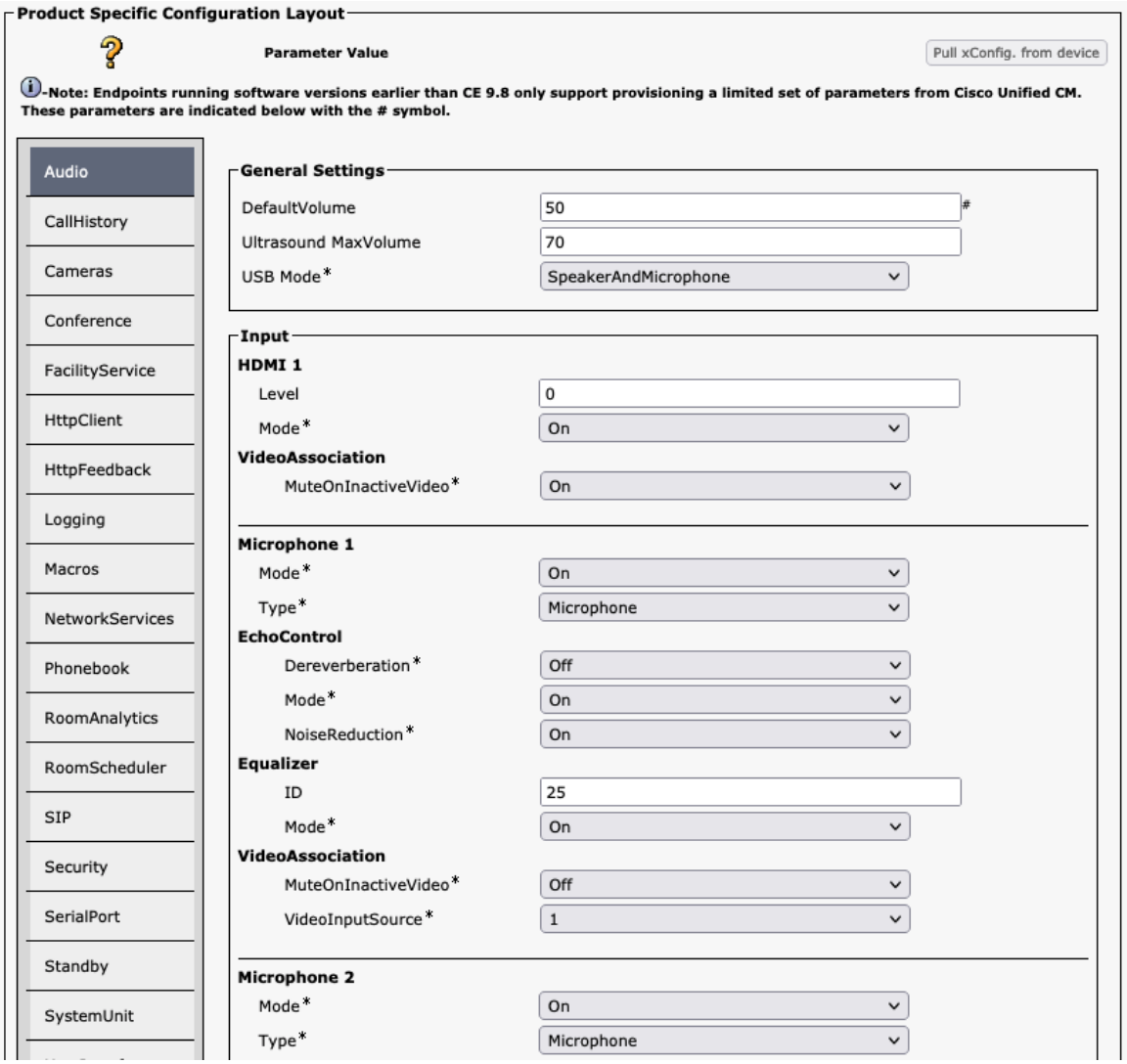
ブッキング

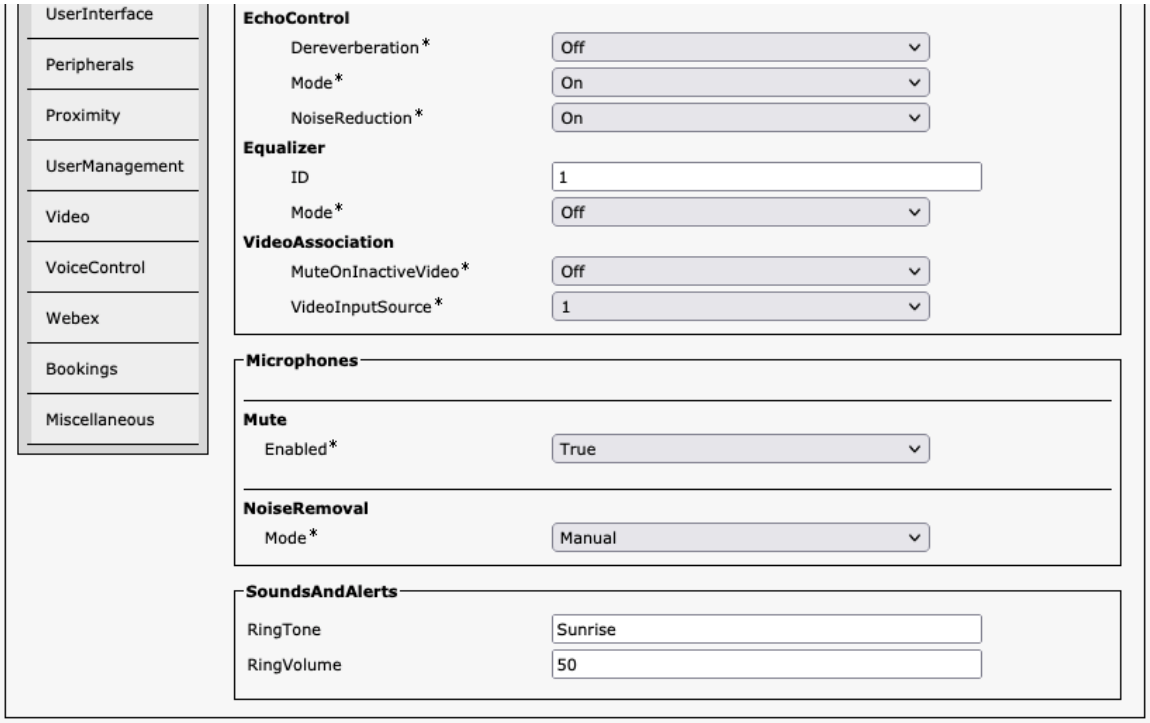


その他

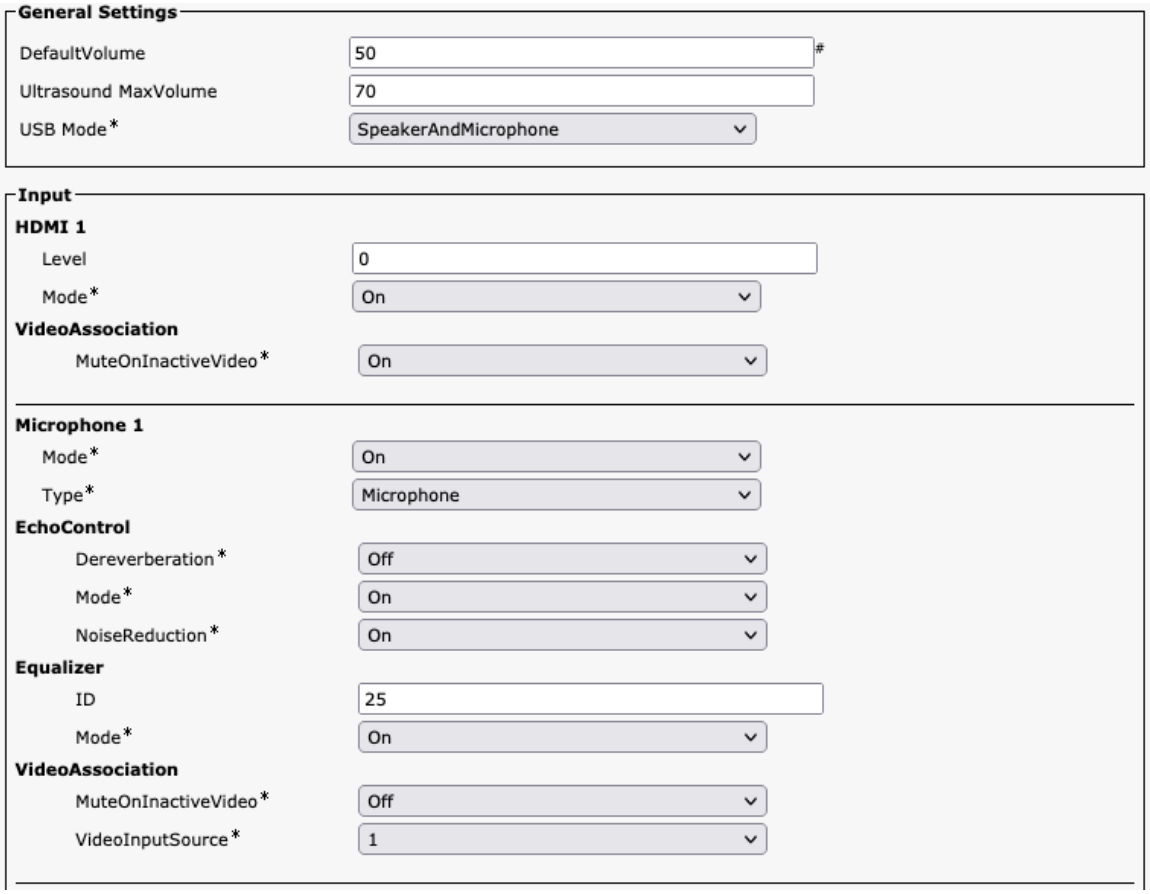


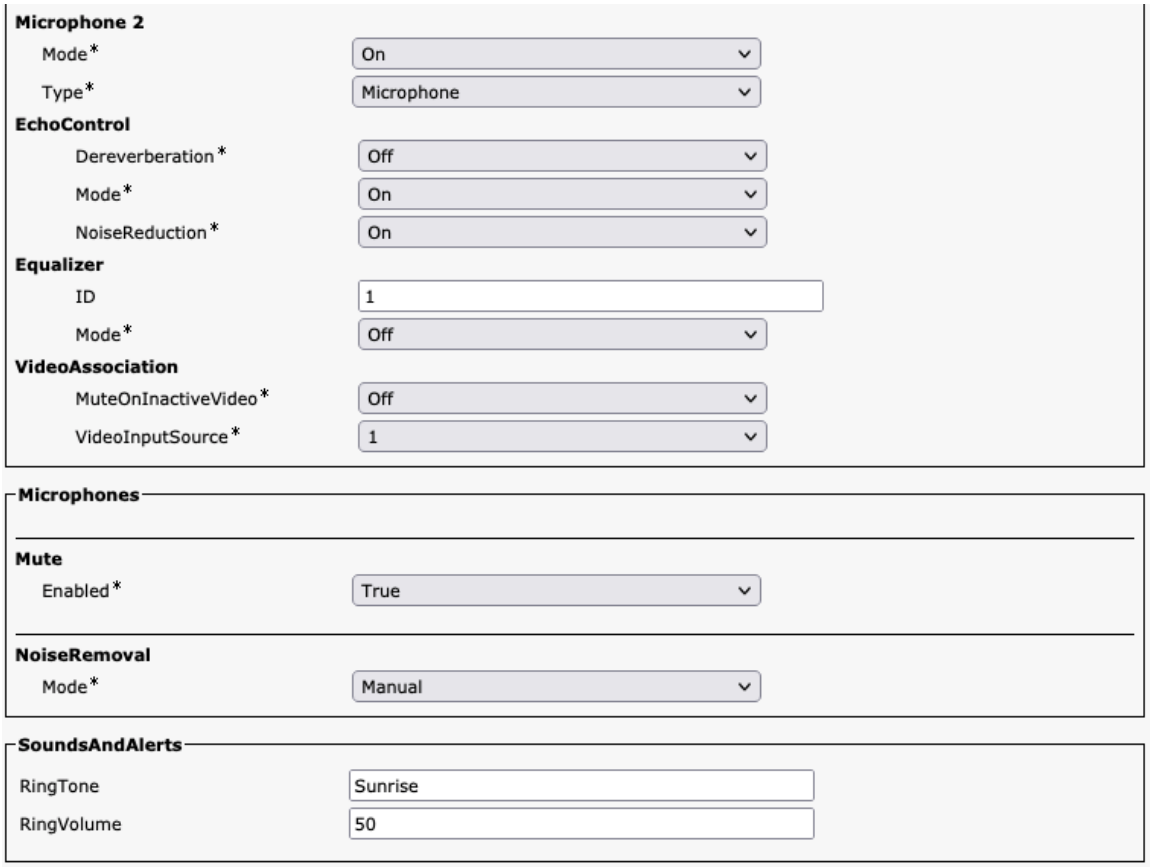
Webex Desk Hub 構成オプション（バージョン 12.5 以降）



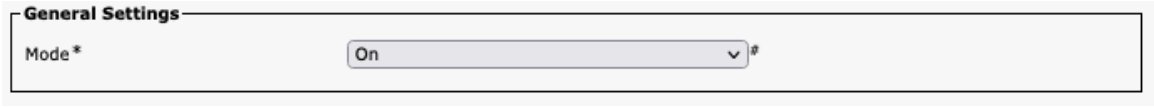

UserInterface
Peripherals
Proximity
UserManagement
Video
VoiceControl
Webex
Bookings
Miscellaneous
EchoControl
Dereverberation*
Off
Mode*
On
NoiseReduction*
On
Equalizer
ID
1
Mode*
Off
VideoAssociation
MuteOnInactiveVideo*
Off
VideoInputSource*
1
Microphones
Mute
Enabled*
True
NoiseRemoval
Mode*
Manual
SoundsAndAlerts
RingTone
Sunrise
RingVolume
50

音声

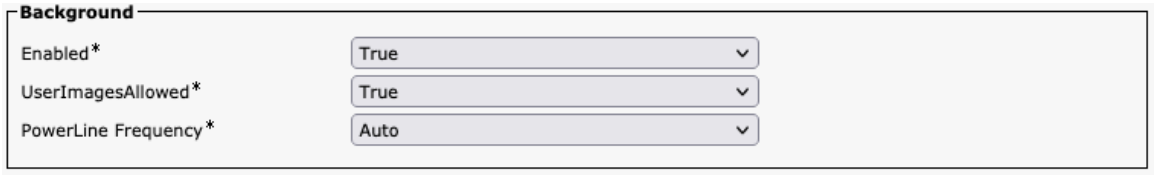

General Settings
DefaultVolume
50
Ultrasound MaxVolume
70
USB Mode*
SpeakerAndMicrophone
Input
HDMI 1
Level
0
Mode*
On
VideoAssociation
MuteOnInactiveVideo*
On
Microphone 1
Mode*
On
Type*
Microphone
EchoControl
Dereverberation*
Off
Mode*
On
NoiseReduction*
On
Equalizer
ID
25
Mode*
On
VideoAssociation
MuteOnInactiveVideo*
Off
VideoInputSource*
1


Microphone 2
Mode*
On
Type*
Microphone
EchoControl
Dereverberation*
Off
Mode*
On
NoiseReduction*
On
Equalizer
ID
1
Mode*
Off
VideoAssociation
MuteOnInactiveVideo*
Off
VideoInputSource*
1
Microphones
Mute
Enabled*
True
NoiseRemoval
Mode*
Manual
SoundsAndAlerts
RingTone
Sunrise
RingVolume
50

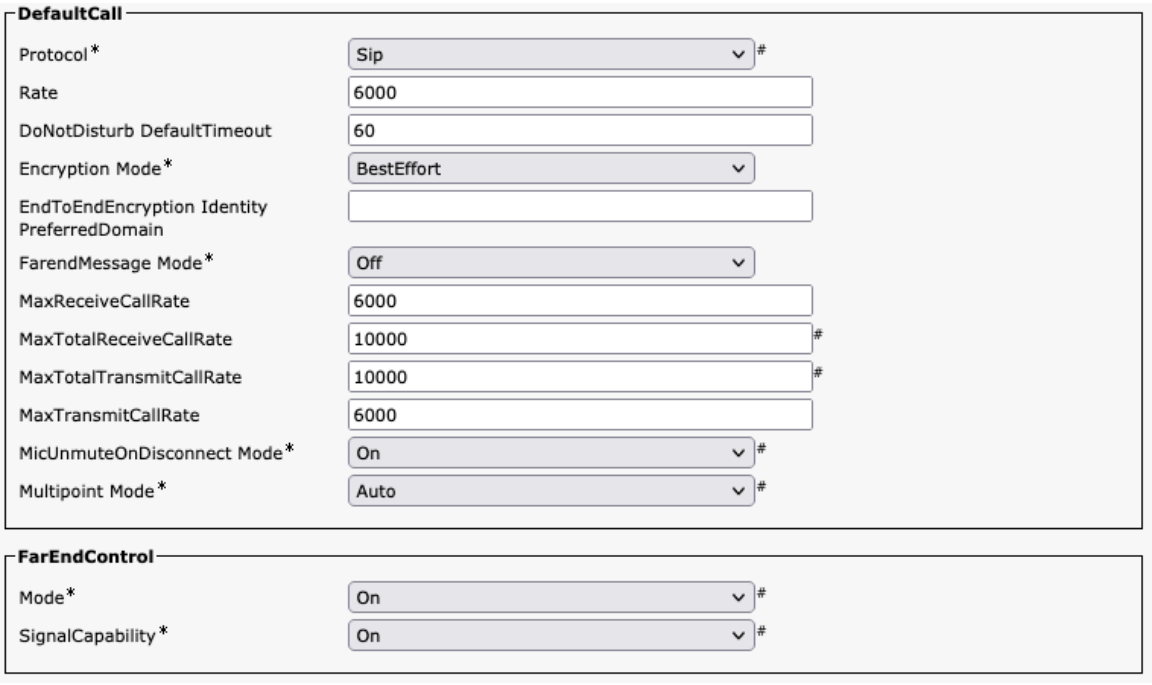
通話履歴


General Settings
Mode*
On

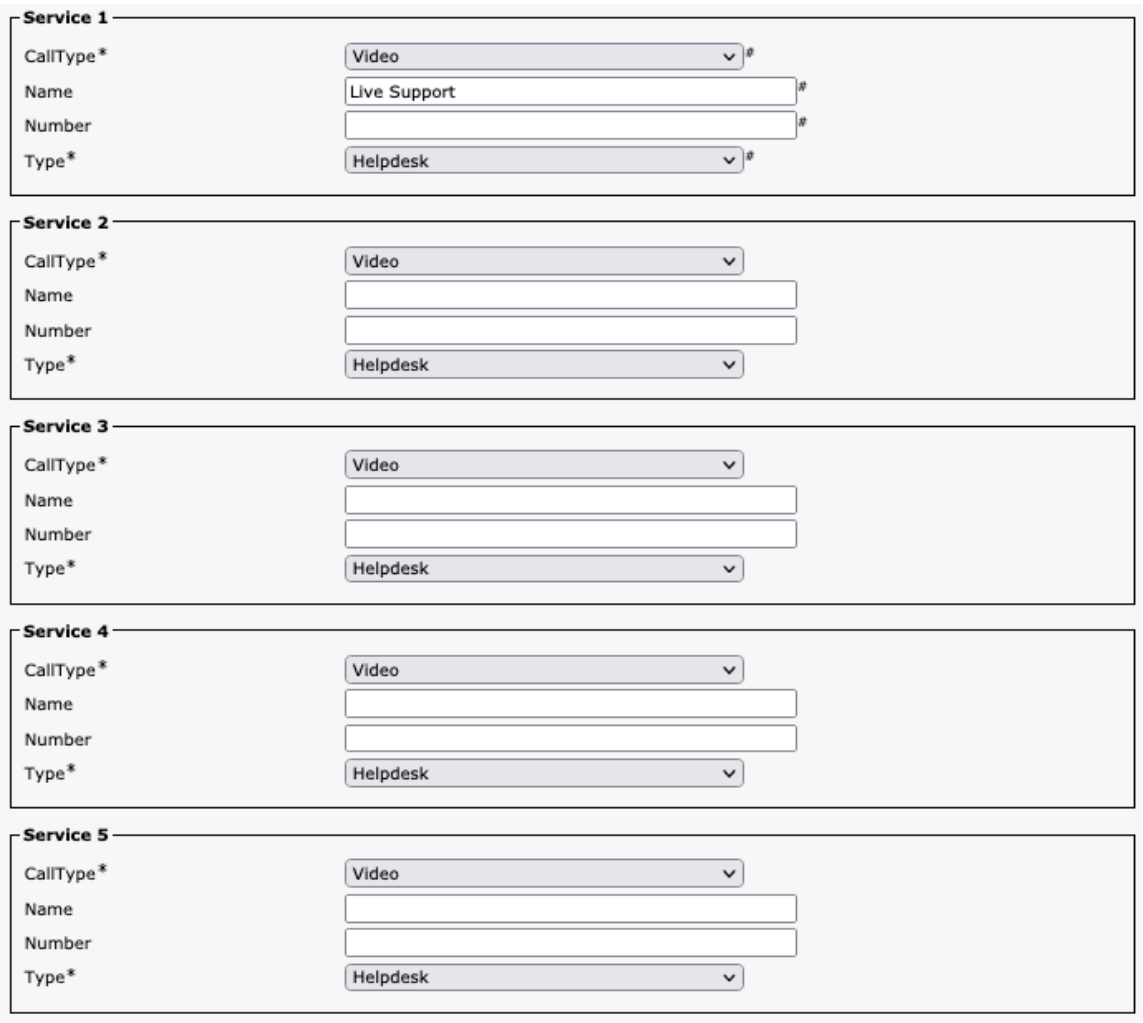
カメラ


Background
Enabled*
True
UserImagesAllowed*
True
PowerLine Frequency*
Auto

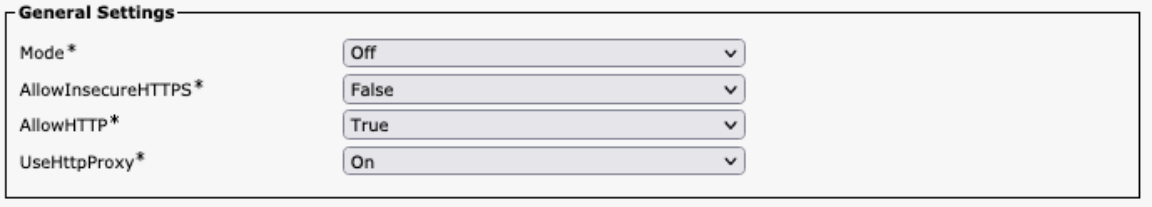
会議



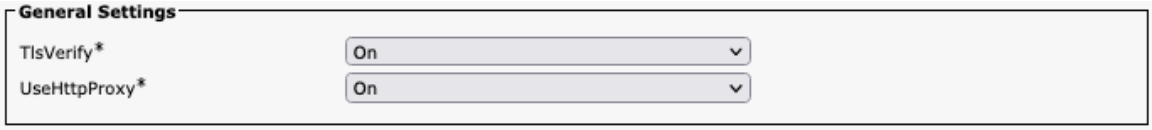
ファシリティサービス



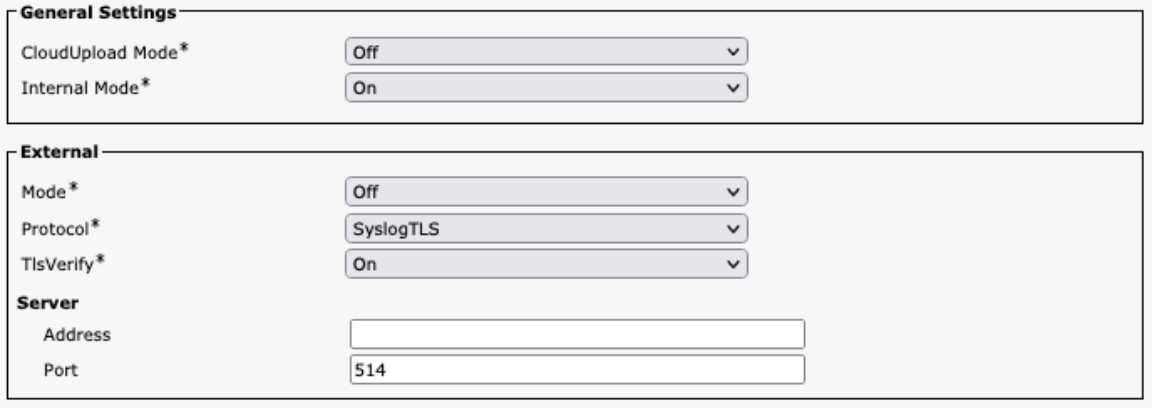
HTTP クライアント



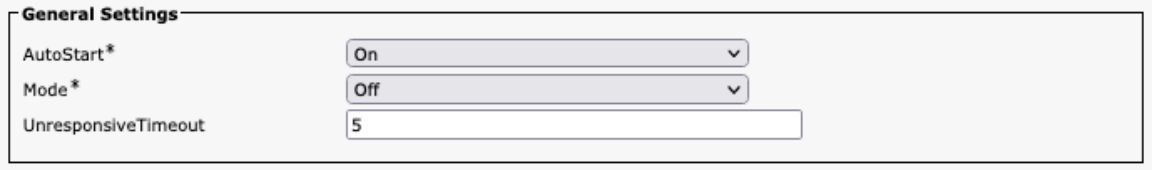
HTTP フィードバック



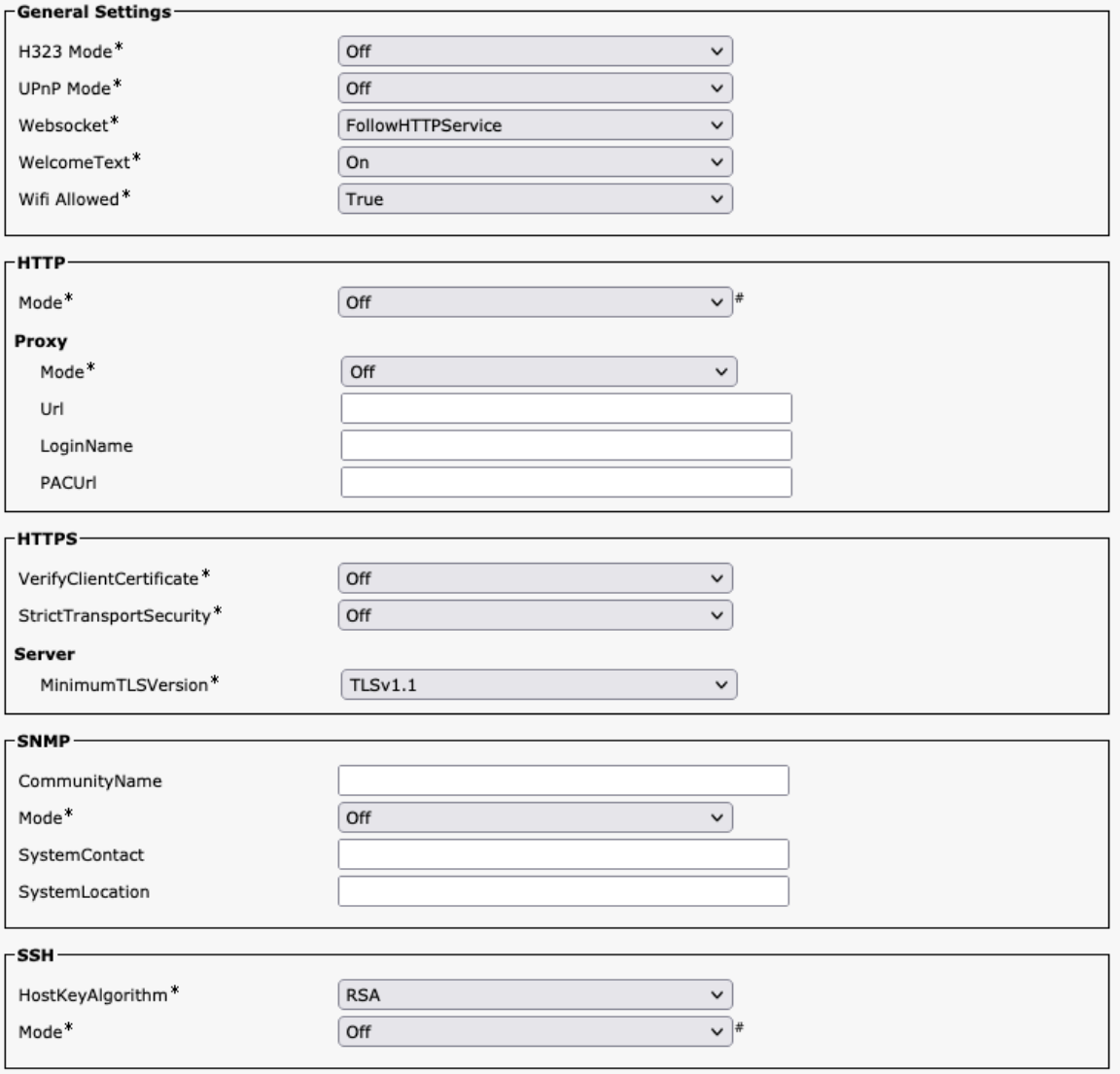
ロギング



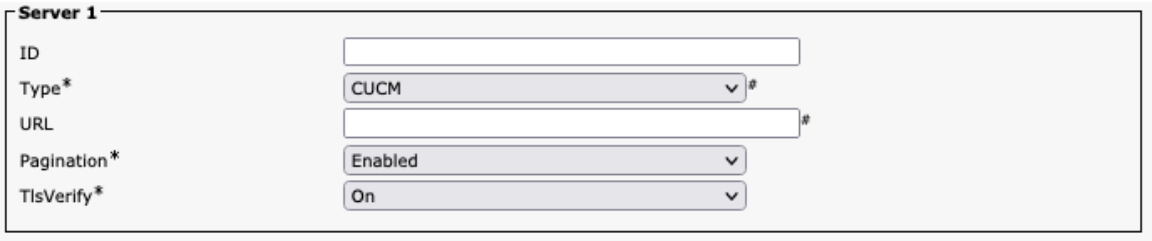
マクロ



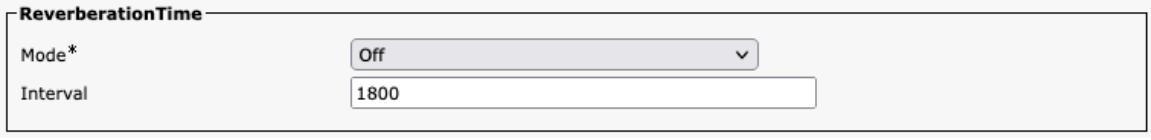
ネットワーク サービス



電話帳（Phone Book）



Room 分析



ルームスケジューラ

General Settings

Enabled*	False

SIP

General Settings

MinimumTLSVersion*	TLSv1.0

セキュリティ

Audit

Logging

Mode*	Internal

OnError

Action*	Ignore

Server

Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off

Session

InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

General Settings

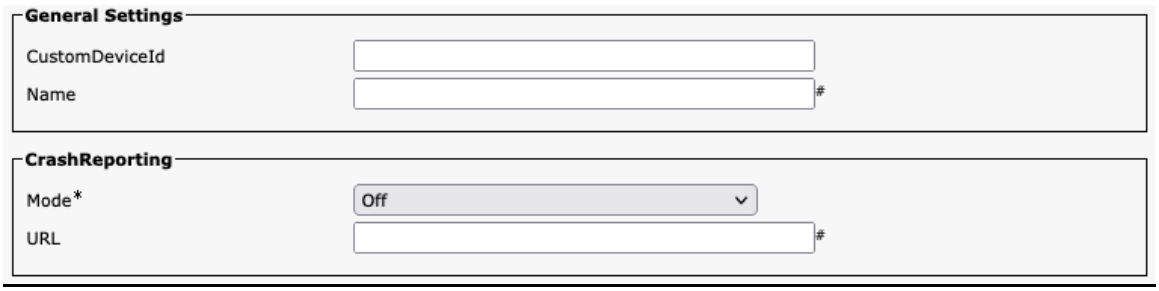
BaudRate*	115200
LoginRequired*	On #
Mode*	On #

スタンバイ

General Settings

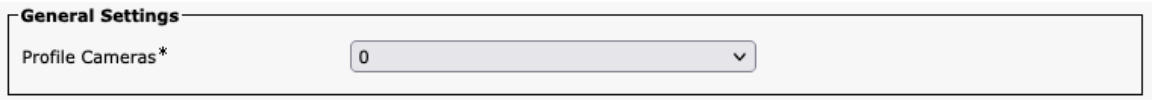
BootAction*	DefaultCameraPosition
Control*	On #
Delay	10 #
StandbyAction*	PrivacyPosition #
WakeupAction*	RestoreCameraPosition
WakeupOnMotionDetection*	Off #
Halfwake Mode*	Auto

システム ユニット

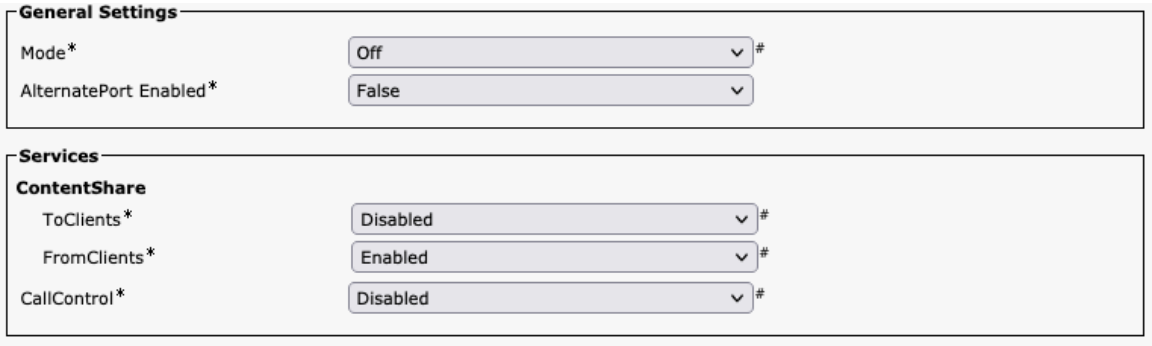


ユーザ インターフェイス

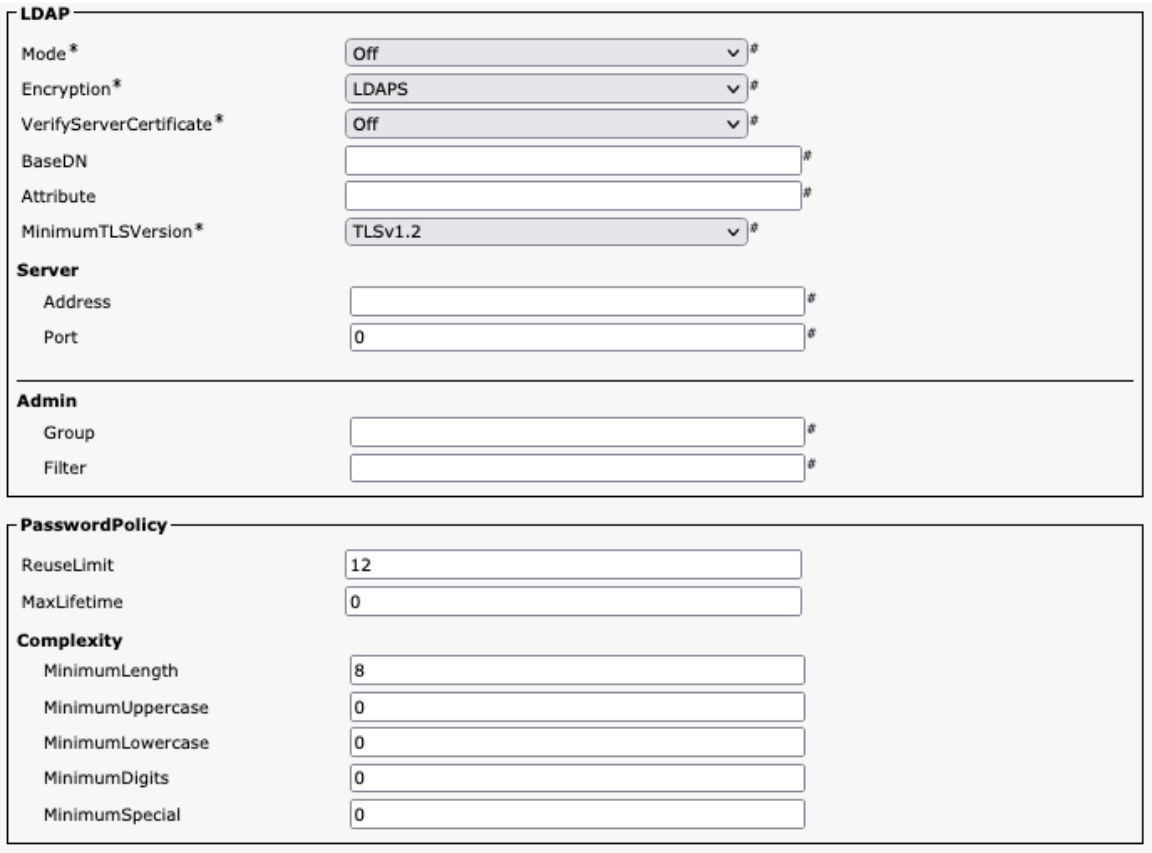
周辺機器



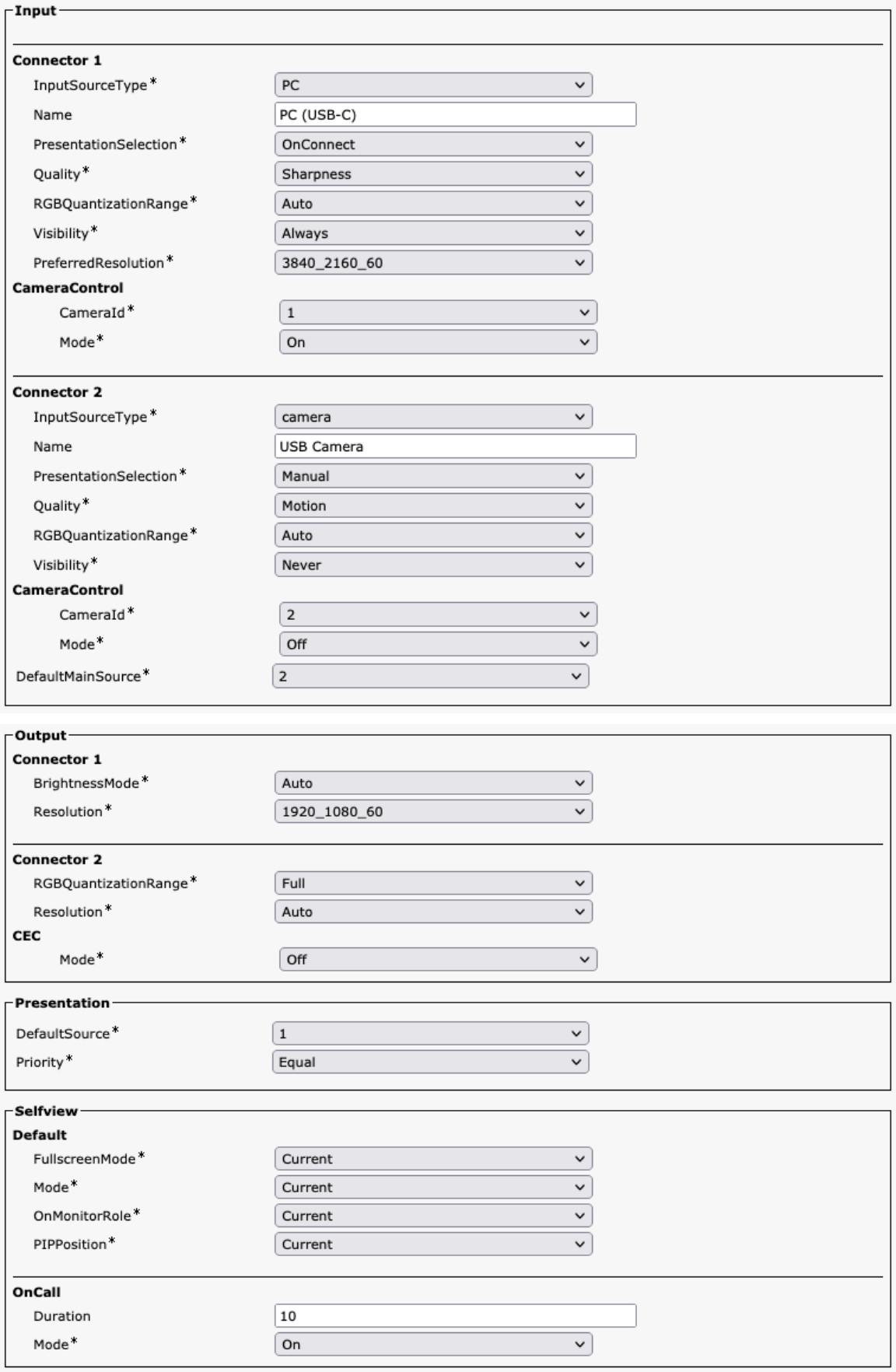
プロキシミティ



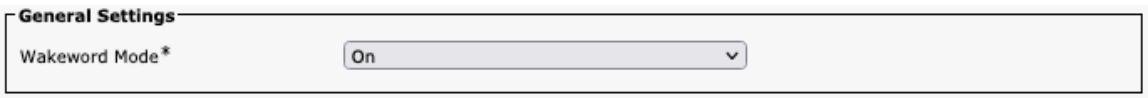
ユーザー管理



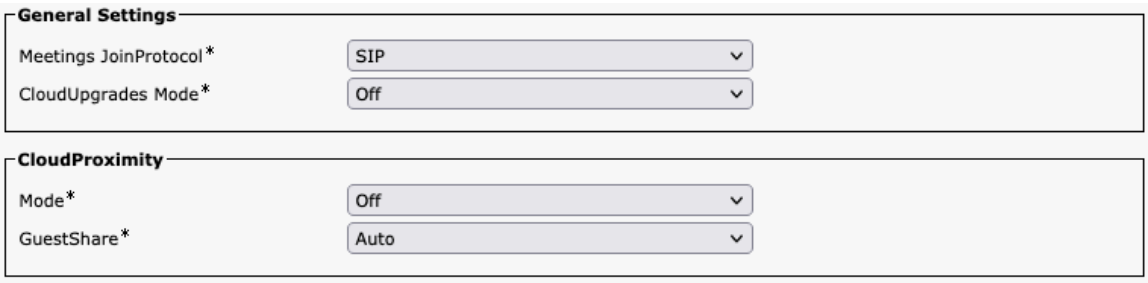
ビデオ


Input
Connector 1
InputSourceType* PC
Name PC (USB-C)
PresentationSelection* OnConnect
Quality* Sharpness
RGBQuantizationRange* Auto
Visibility* Always
PreferredResolution* 3840_2160_60
CameraControl
CameraId* 1
Mode* On
Connector 2
InputSourceType* camera
Name USB Camera
PresentationSelection* Manual
Quality* Motion
RGBQuantizationRange* Auto
Visibility* Never
CameraControl
CameraId* 2
Mode* Off
DefaultMainSource* 2
Output
Connector 1
BrightnessMode* Auto
Resolution* 1920_1080_60
Connector 2
RGBQuantizationRange* Full
Resolution* Auto
CEC
Mode* Off
Presentation
DefaultSource* 1
Priority* Equal
Selfview
Default
FullscreenMode* Current
Mode* Current
OnMonitorRole* Current
PIPPosition* Current
OnCall
Duration 10
Mode* On

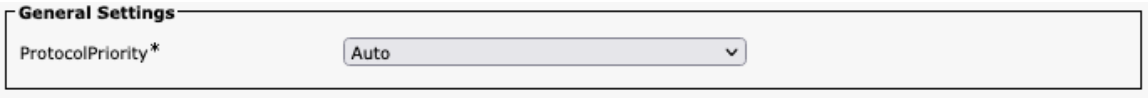
音声管理



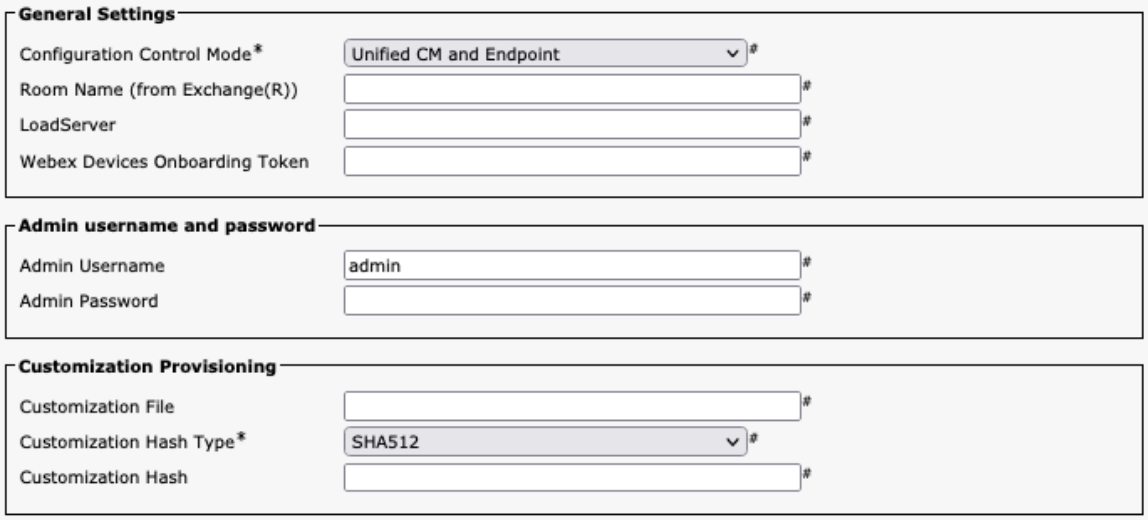
Webex



ブッキング



その他



注： 管理者のユーザー名とパスワード、または SMTP パスワードを有効にする場合は、TFTP 暗号化が有効になっている安全なプロファイルを使用する必要があります。

Webex Desk Series および 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

詳細については、『Webex Desk Series 管理者ガイド』を参照してください。

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

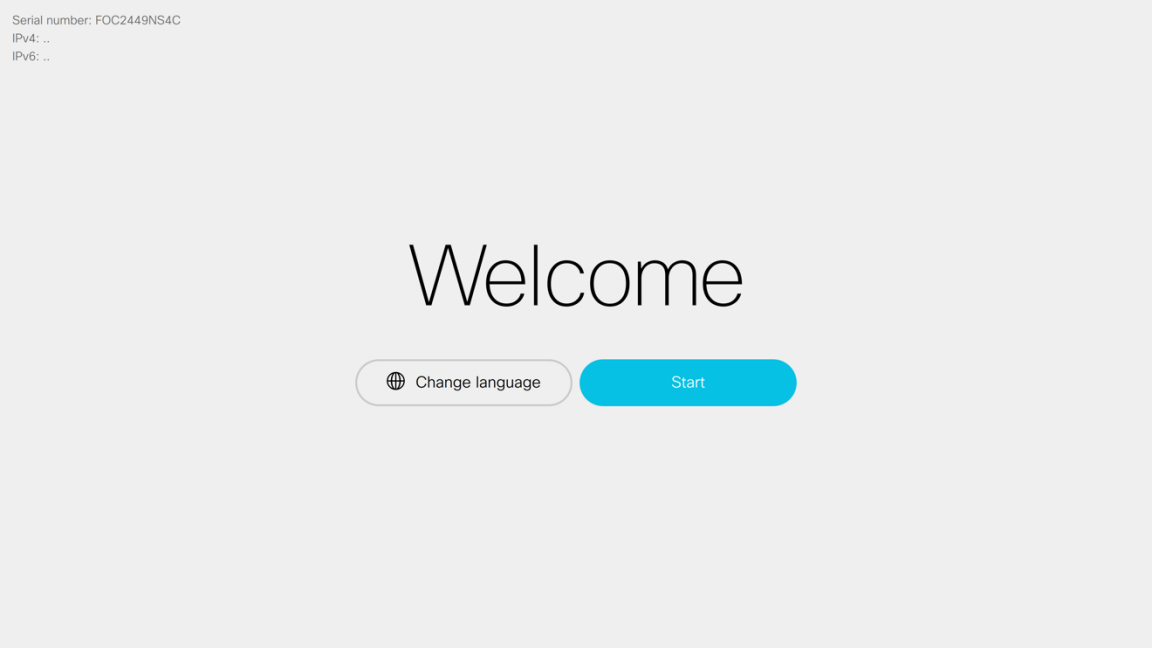
Webex Desk Series の設定

Webex Desk Series を設定するには、ローカル ユーザー インターフェイスを使用します。

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。

- すぐに使用できる（工場出荷時の状態にリセットされた）Webex Desk Series の場合、スタートアップウィザードを使用して Wi-Fi ネットワークを設定します。



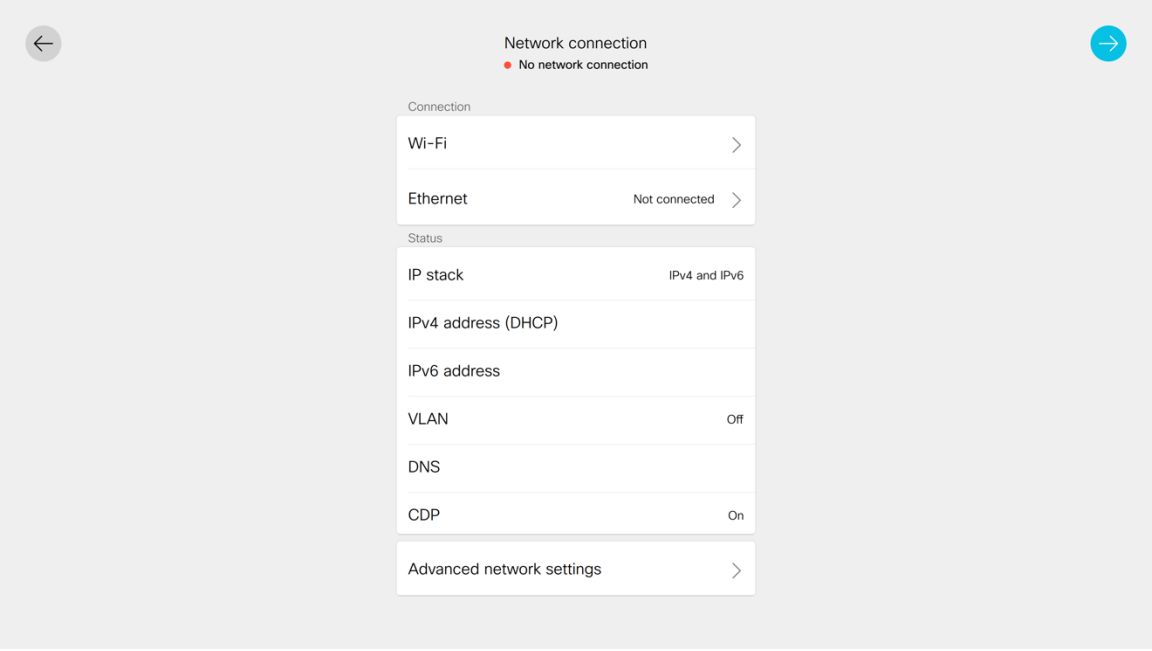
- 構成オプションは、ブロードキャストされた Wi-Fi ネットワークが構成されているか、Wi-Fi ネットワークが手動で構成されているかによって決まります。

- 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。

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

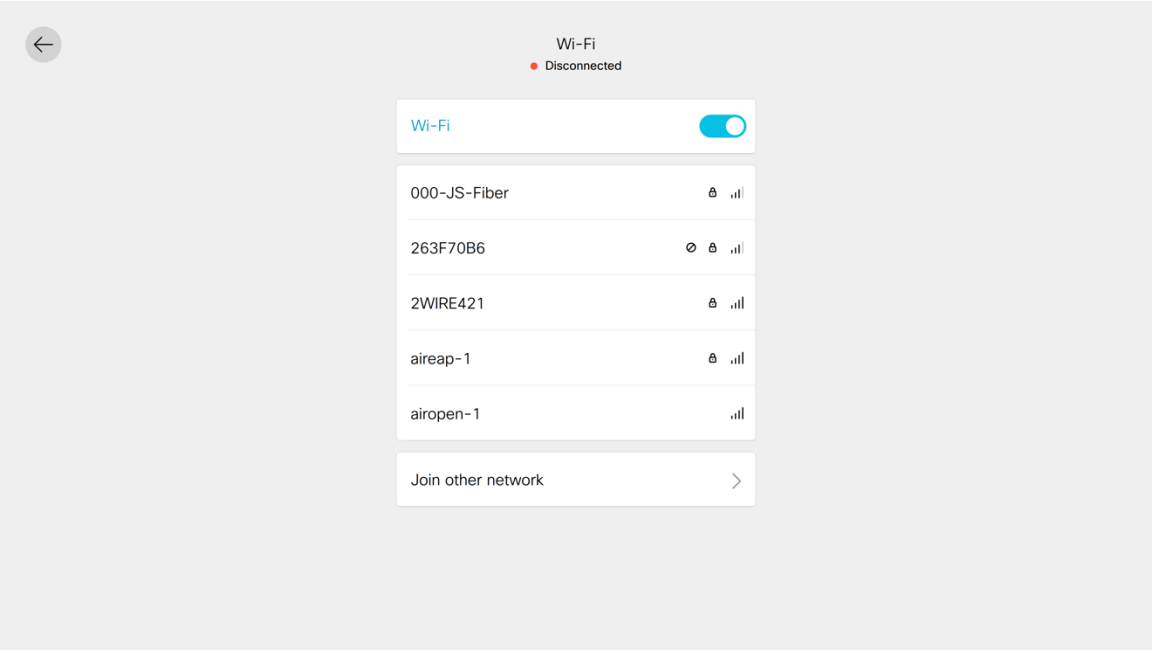
[セキュリティモード（Security Mode）]	EAP 方法	キーの管理	暗号化
オープン（Open）	該当なし	なし	なし
PSK	該当なし	WPA2、WPA	AES、TKIP
EAP	FAST	WPA2、WPA	AES、TKIP
	PEAP	WPA2、WPA	AES、TKIP
	TLS	WPA2、WPA	AES、TKIP
	TTLS	WPA2、WPA	AES、TKIP

- **[Wi-Fi]** を選択して Wi-Fi ネットワークを構成します。

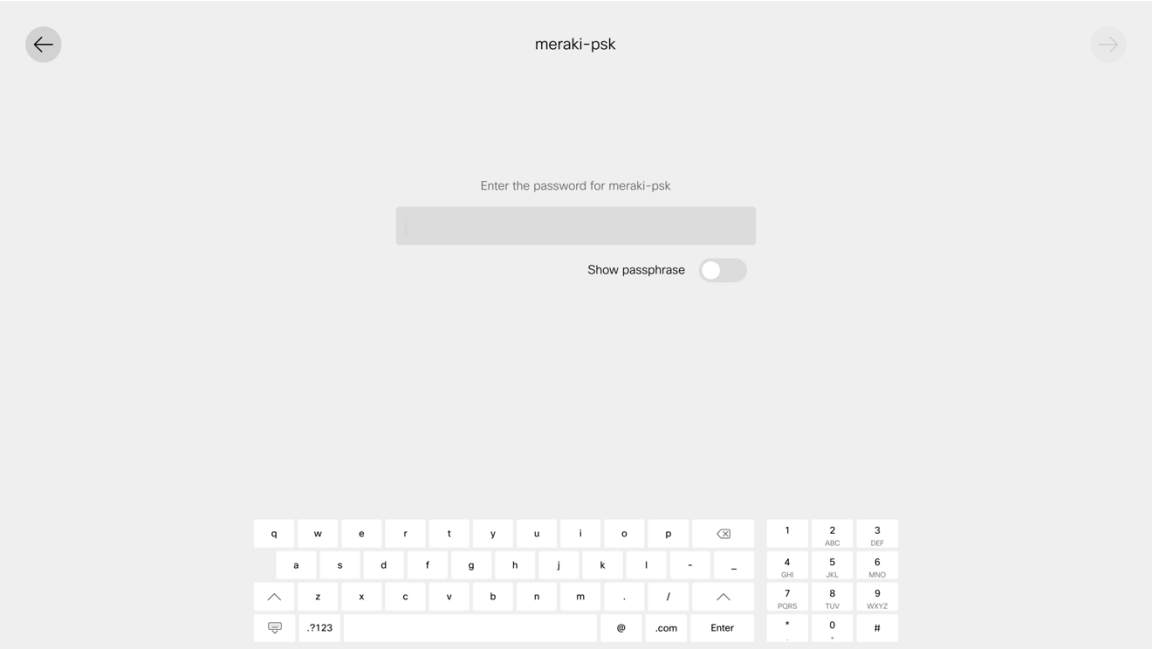


ブロードキャスト Wi-Fi ネットワークの設定

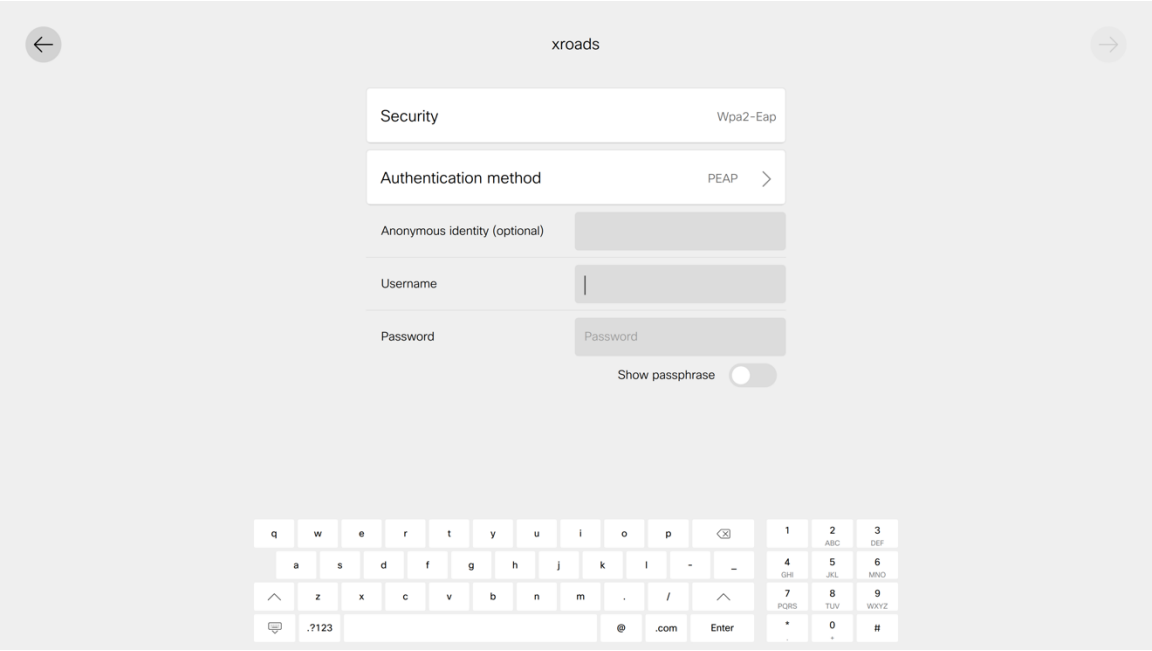
- Wi-Fi ネットワークがブロードキャストされている場合は、リストから目的の Wi-Fi ネットワークを選択し、Wi-Fi ネットワークのセキュリティ設定に応じて必要なログイン情報を入力します。

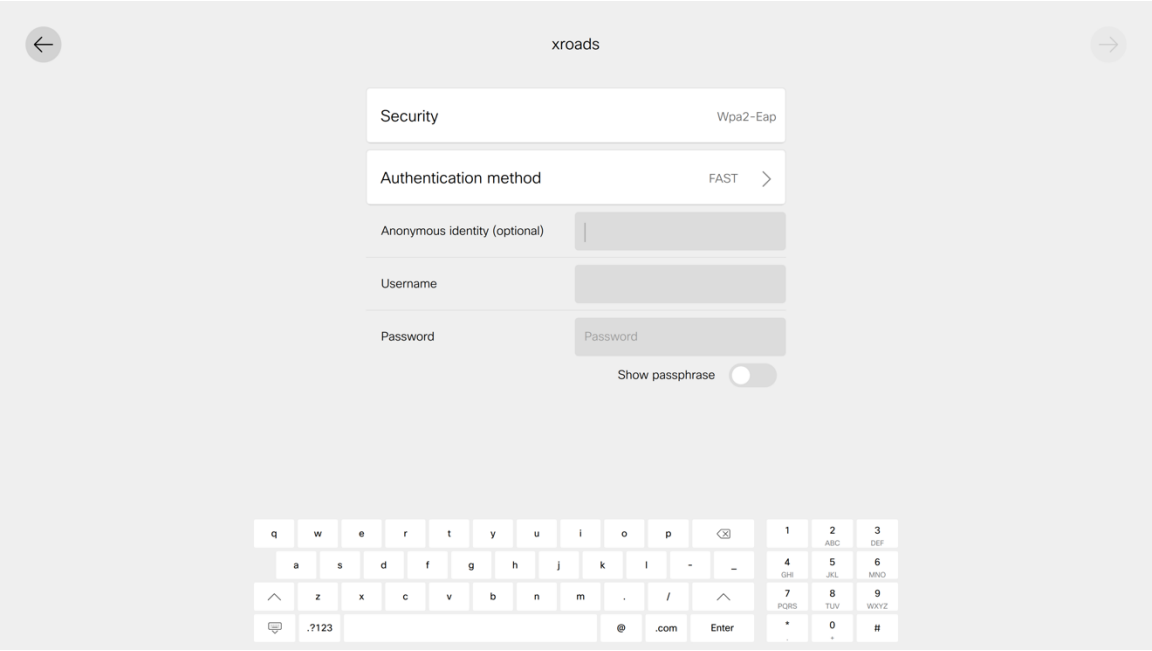


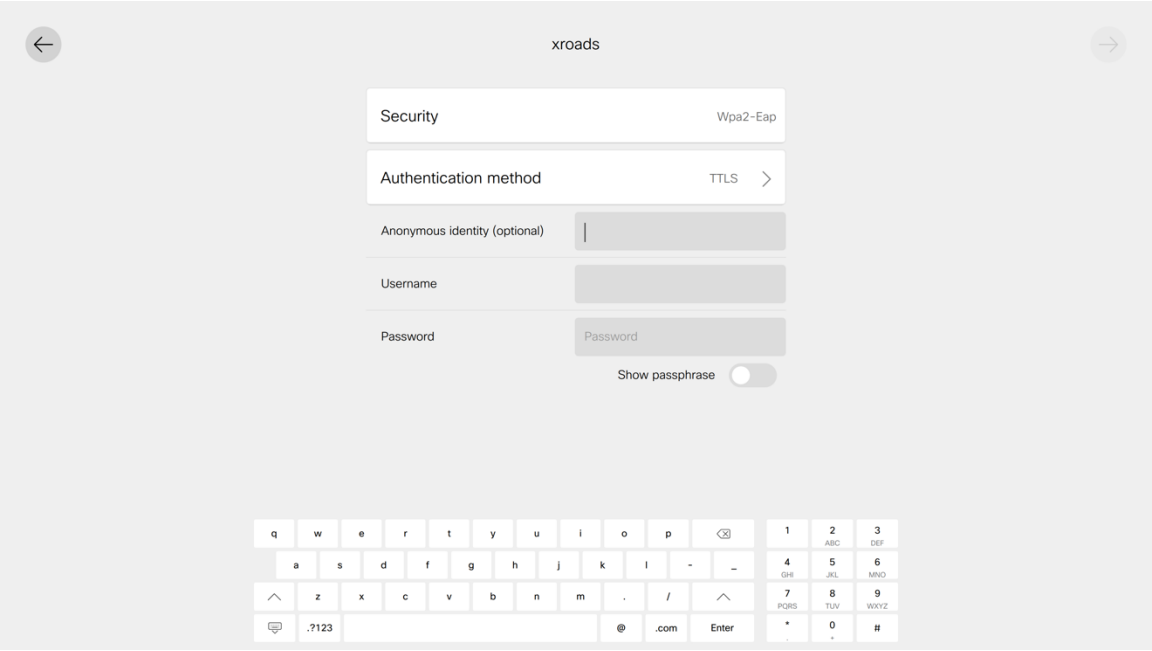
- オープン Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックするだけです。
- PSK 対応の Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックし、8-63 ASCII または 64 HEX **パスワード**を入力します。



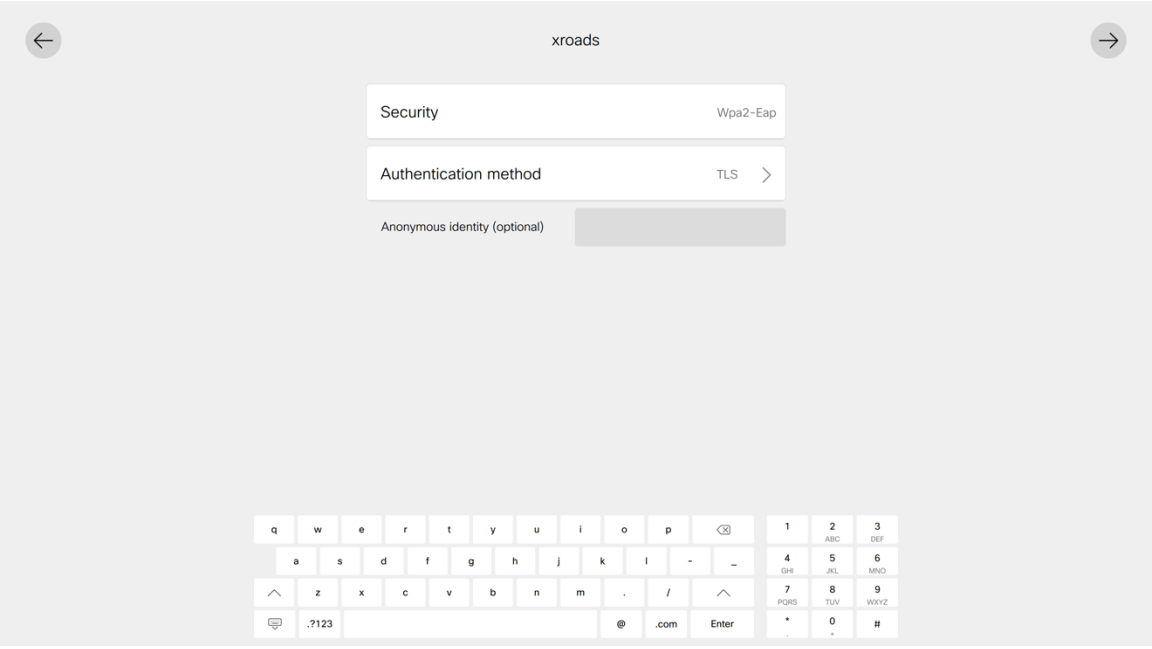
- EAP 対応 Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックしてから、**[認証方式（Authentication method）]** を選択します。
- PEAP、EAP-FAST（FAST）、または EAP-TTLS（TTLS）Wi-Fi ネットワークを設定する場合は、**[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。


xroads
Security
Wpa2-Eap
Authentication method
PEAP
Anonymous identity (optional)
Username
Password
Password
Show passphrase


xroads
Security
Wpa2-Eap
Authentication method
FAST
Anonymous identity (optional)
Username
Password
Password
Show passphrase

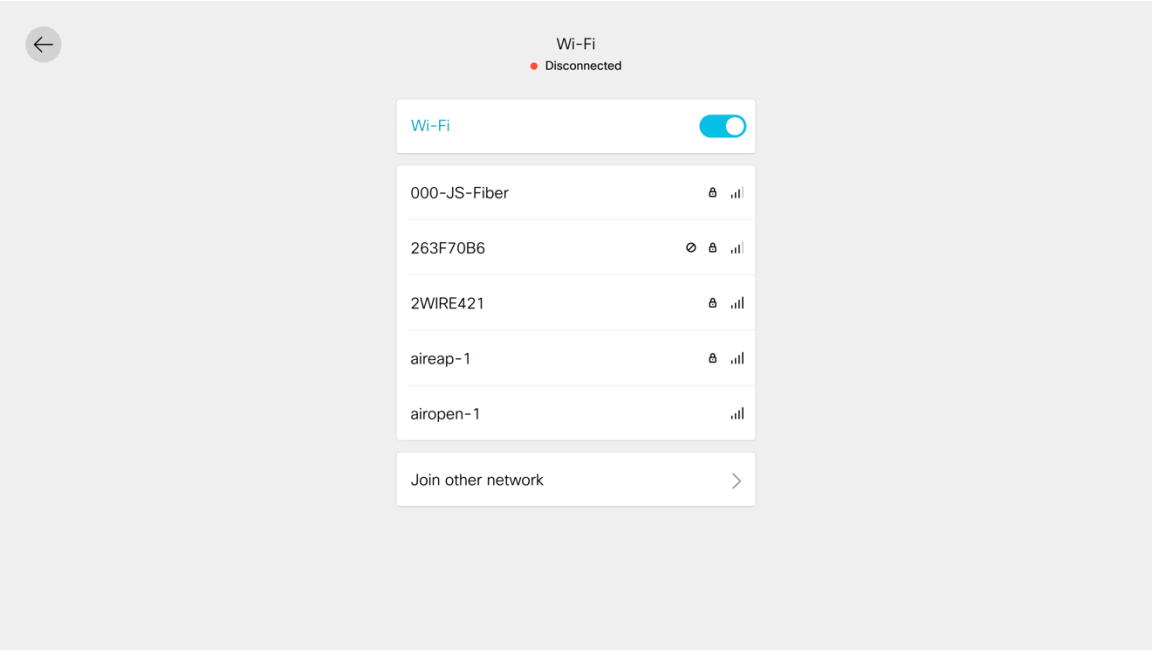


- EAP-TLS（TLS）Wi-Fi ネットワークを構成する場合は、デバイスの Web ページから適切なユーザー証明書と CA 証明書がインストールされていることを確認する必要があります。

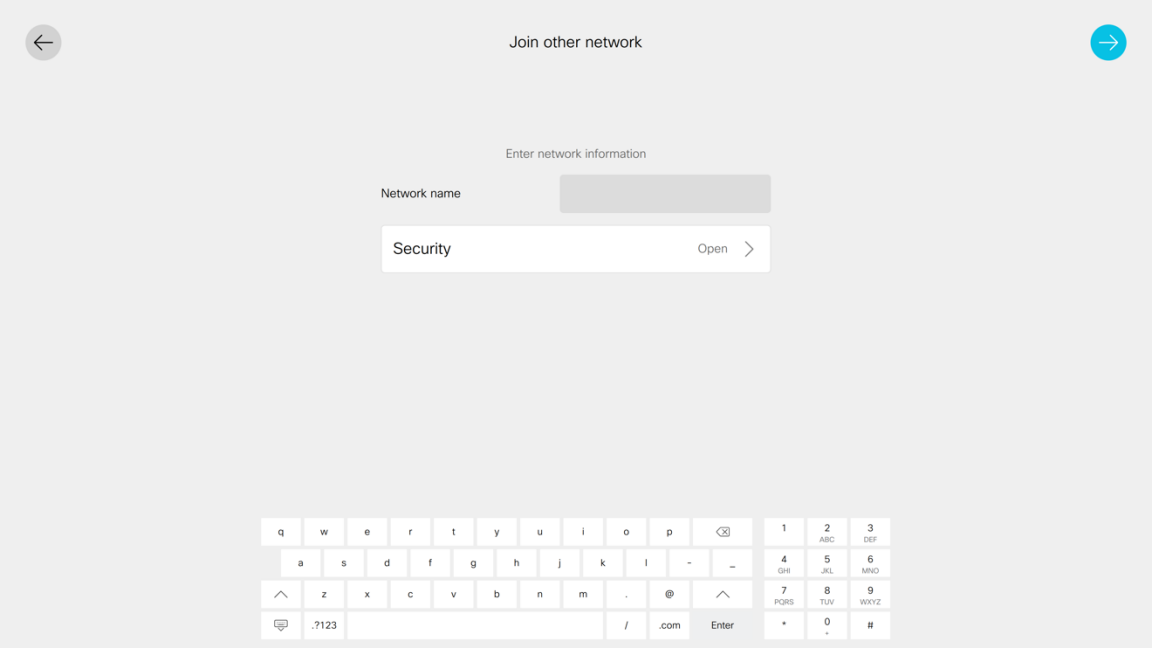


非ブロードキャスト Wi-Fi ネットワークの設定

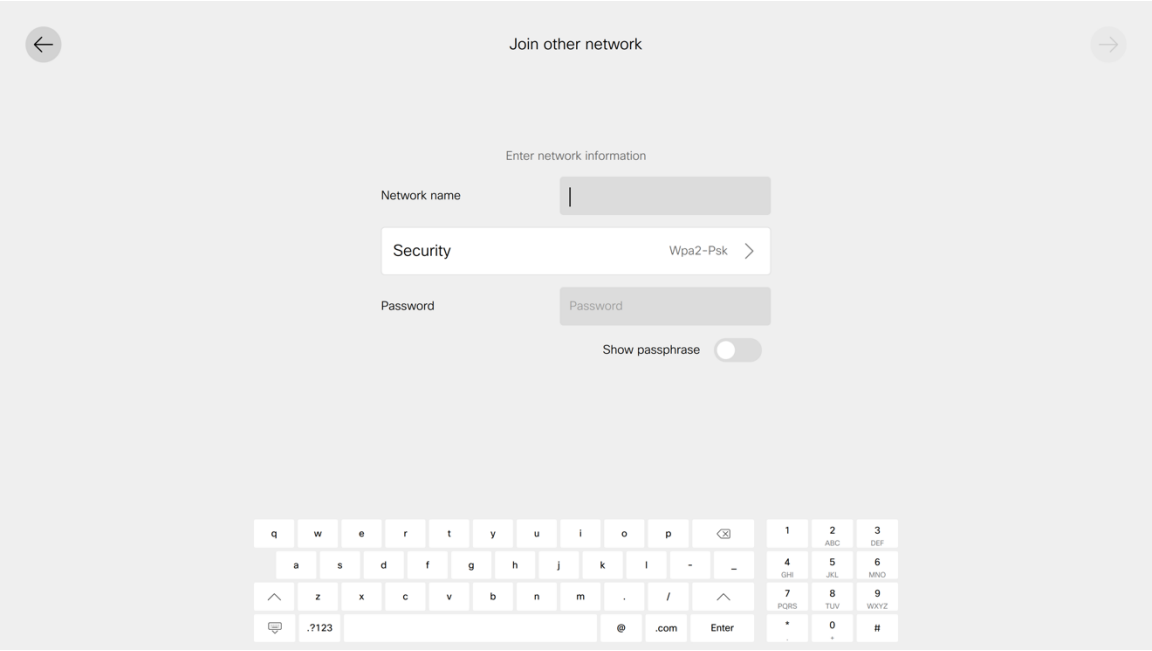
- 非ブロードキャスト（非表示）Wi-Fi ネットワークを手動で構成する場合は、**[他のネットワークに参加]** を選択します。
- 次に、**ネットワーク名（SSID）**、**セキュリティ**タイプを設定し、Wi-Fi ネットワークのセキュリティ設定に応じて必要なログイン情報を入力します。



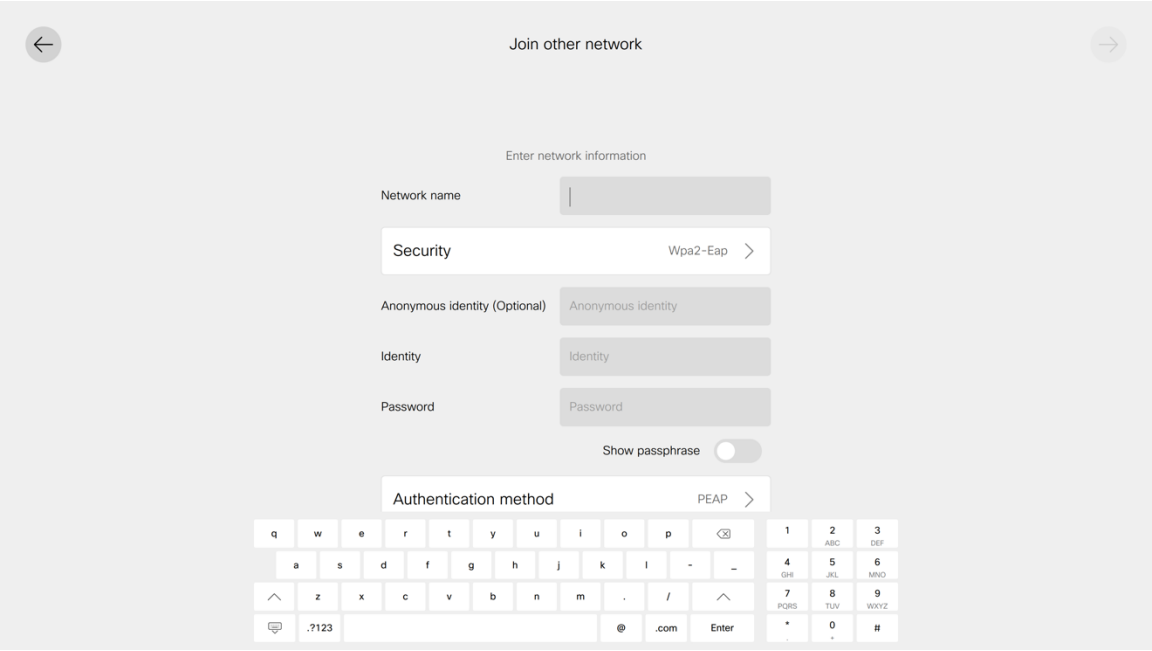
- オープン Wi-Fi ネットワークに接続するには、**ネットワーク名**を入力し、**[セキュリティ（Security）]** を **[オープン（Open）]** に設定します。

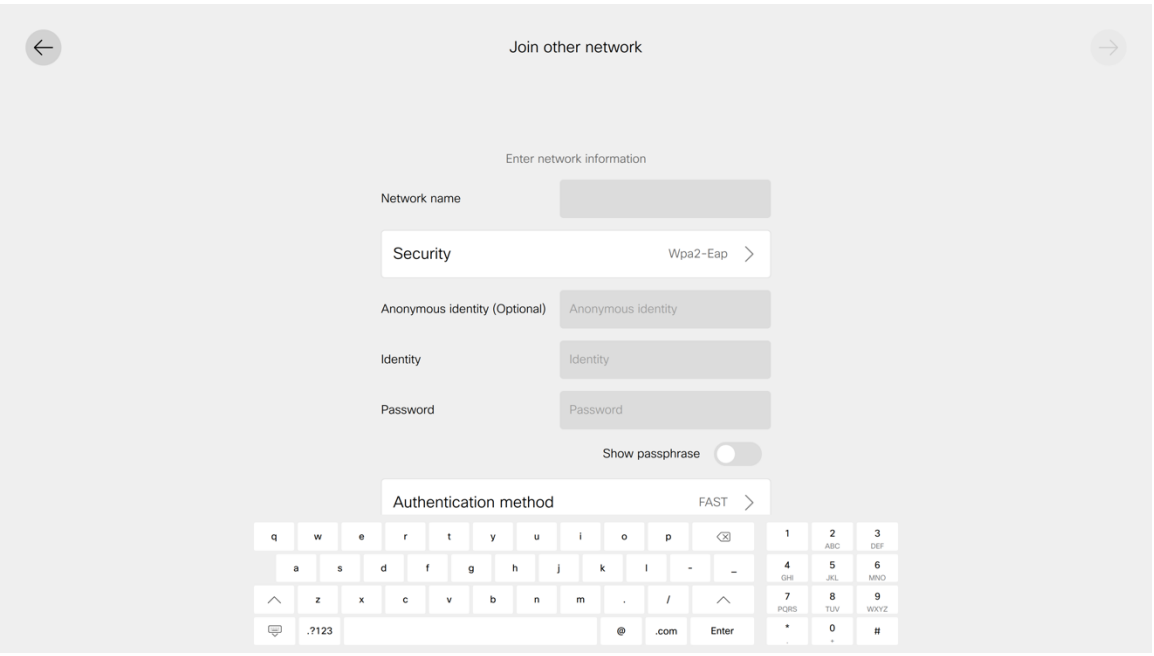


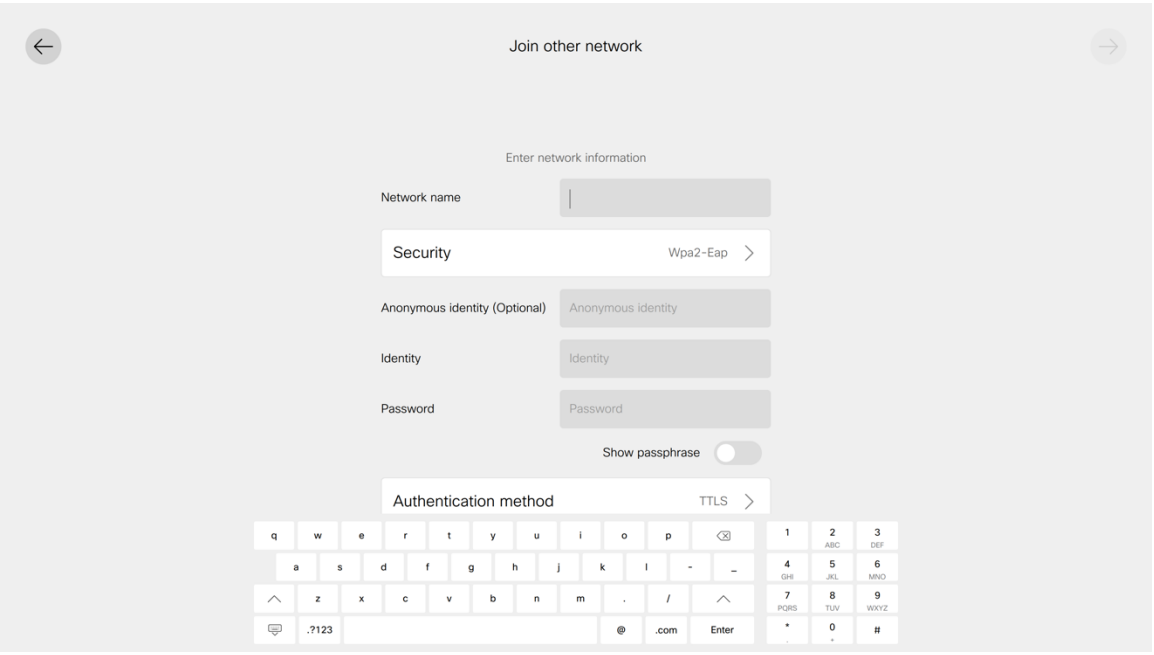
- PSK 対応の Wi-Fi ネットワークに接続するには、**ネットワーク名**を入力し、**[セキュリティ（Security）]** を **[WPA2-PSK]** に設定してから、8-63 ASCII または 64 HEX **パスワード**を入力します。



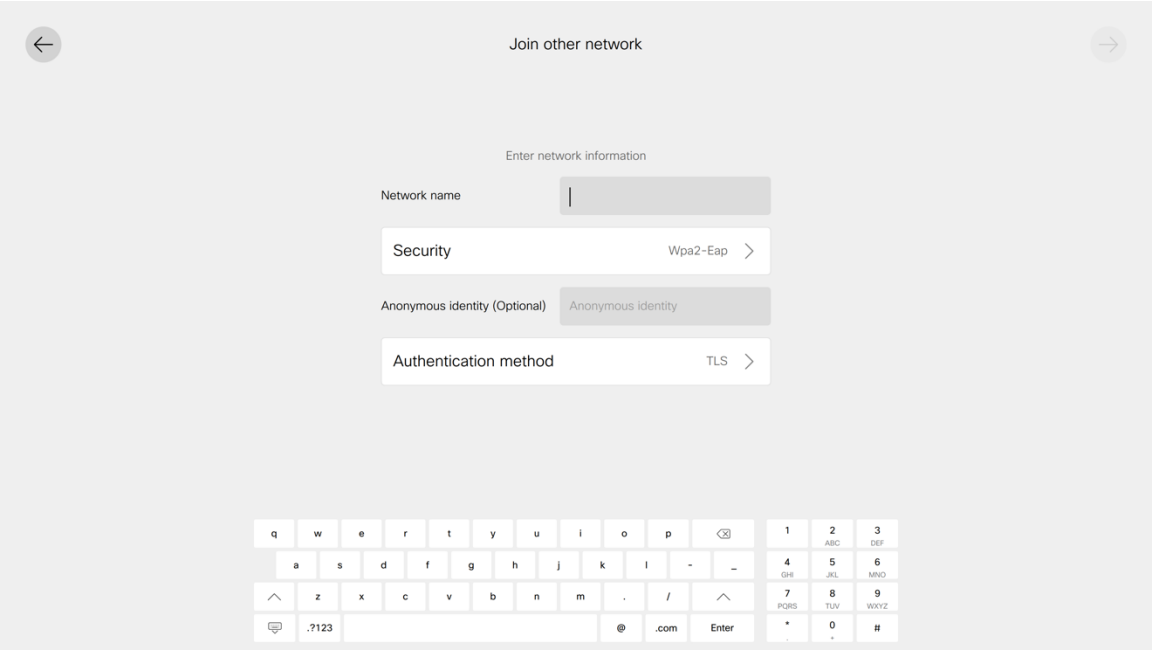
- EAP 対応の Wi-Fi ネットワークに接続するには、**ネットワーク名**を入力し、**[セキュリティ（Security）]** を **[WPA2-EAP]** に設定してから、**[認証方式（Authentication method）]** を選択します。
- PEAP、EAP-FAST（FAST）、または EAP-TTLS（TTLS）Wi-Fi ネットワークを設定する場合は、**[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。





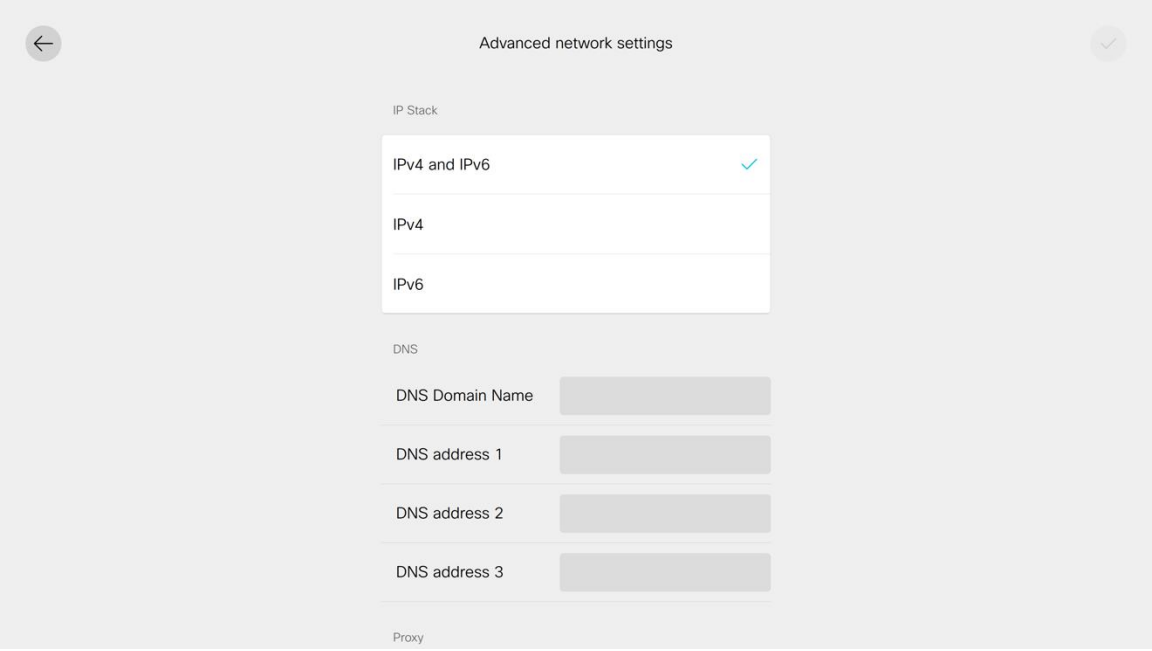


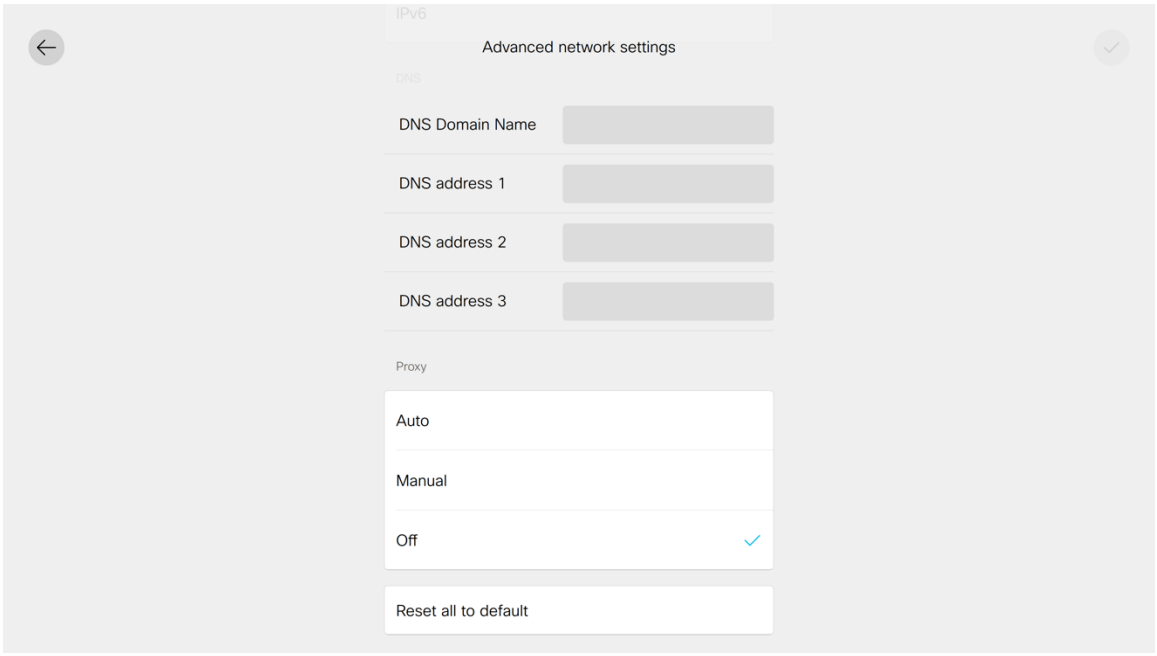
- EAP-TLS（TLS）Wi-Fi ネットワークを構成する場合は、デバイスの Web ページから適切なユーザー証明書と CA 証明書がインストールされていることを確認する必要があります。

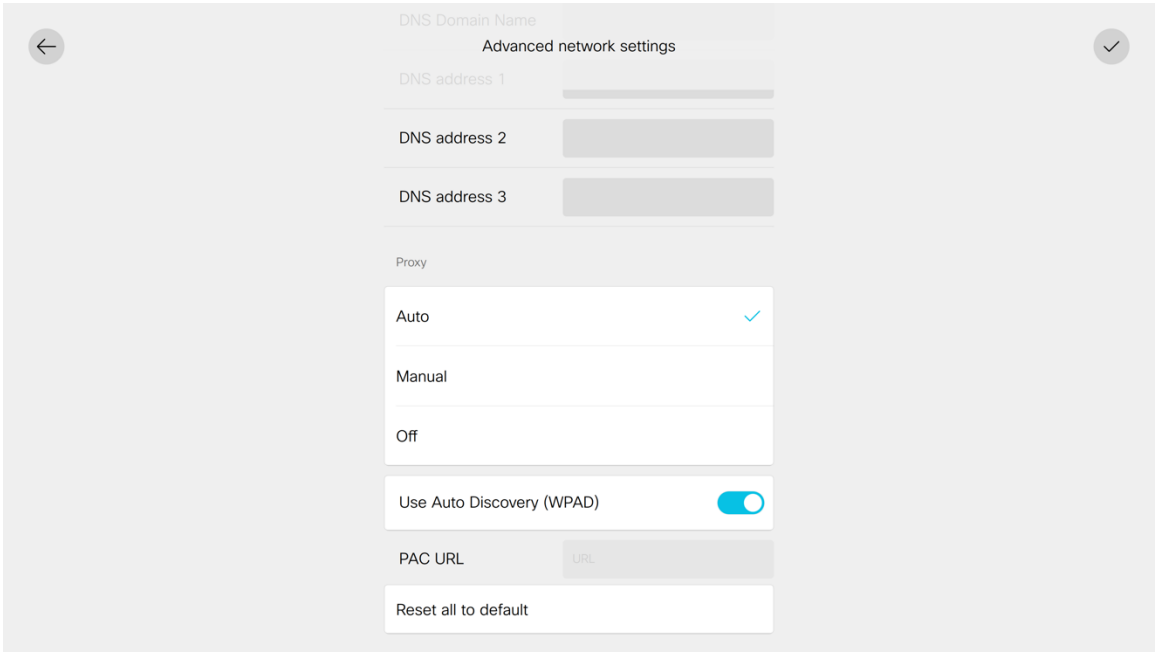


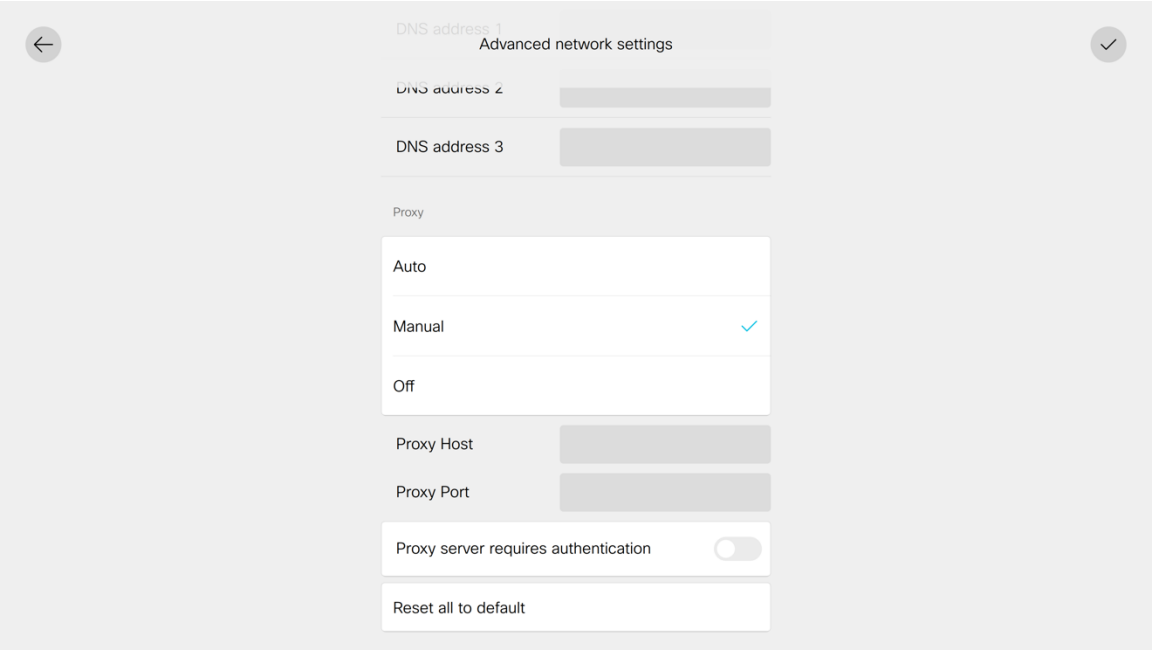
Wi-Fi ネットワークの詳細オプションの設定

- **プロキシ設定は、**[ネットワーク接続設定（Network connection）] **の** [詳細ネットワーク設定（Advanced network settings）] **セクションで構成できます。**




IPv6
Advanced network settings
DNS
DNS Domain Name
DNS address 1
DNS address 2
DNS address 3
Proxy
Auto
Manual
Off
Reset all to default


DNS Domain Name
Advanced network settings
DNS address 1
DNS address 2
DNS address 3
Proxy
Auto
Manual
Off
Use Auto Discovery (WPAD)
PAC URL
URL
Reset all to default



注：TKIP はブロードキャスト/マルチキャスト暗号としてしか使用できないため、アクセスポイントは AES（CCMP128）をサポートしている必要があります。

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『Webex Desk Series 管理者ガイド』を参照してください。

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

証明書管理

Webex Desk Series は、**EAP-TLS** に X.509 デジタル証明書を利用したり、**PEAP**、**EAP-FAST**、または **EAP-TTLS** を使用するときにサーバー検証を有効にしたりすることができます。

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。

クライアント証明書とサーバー証明書には、Base-64（PEM）エンコードのみを使用できます（DER エンコードはサポートされていません）。

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ー証明書が 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。

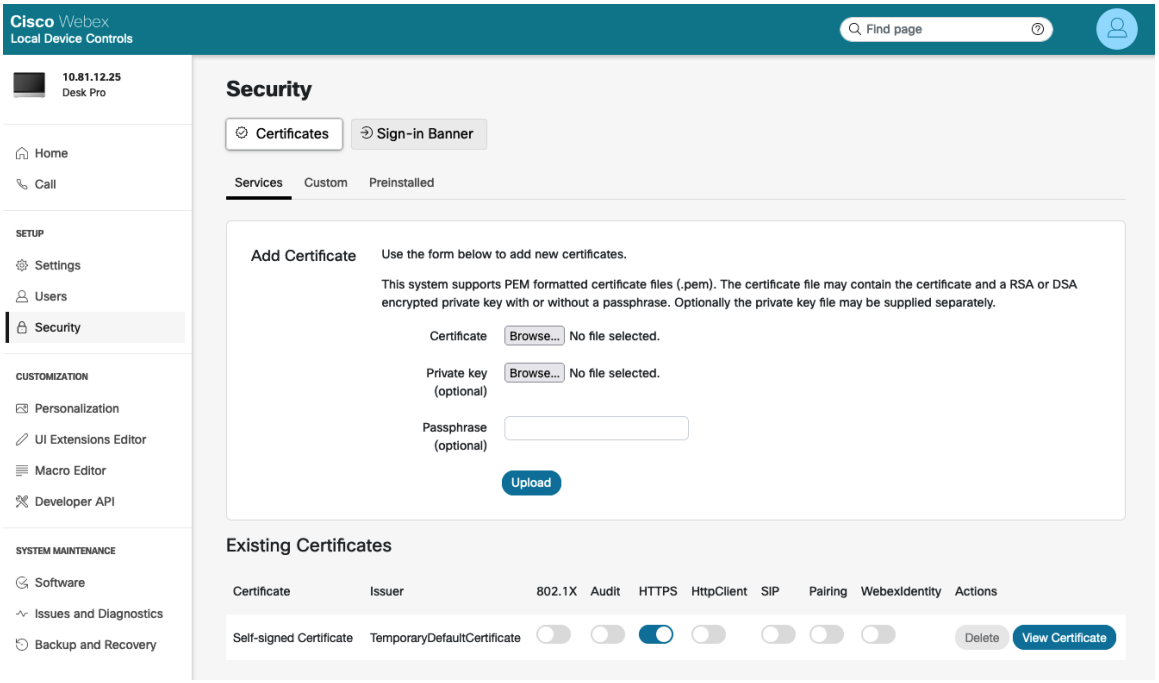
Microsoft® 認証局（CA）サーバを使用することを推奨します。他の CA サーバータイプは Webex Desk Series との完全な相互運用性がない場合があります。

証明書のインストール

証明書は、Webex Desk Series の Web ページからインストールできます。

自動証明書の登録は現在サポートされていません。

Webex Desk Series の Web ページから証明書をインストールするには、**[セキュリティ（Security）] > [証明書（Certificates）]** を選択し、ユーザー証明書またはサーバー証明書（ルート CA）のどちらをインストールするかに応じて、**[サービス（Servives）]** または **[カスタム（Custom）]** を選択します。



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。

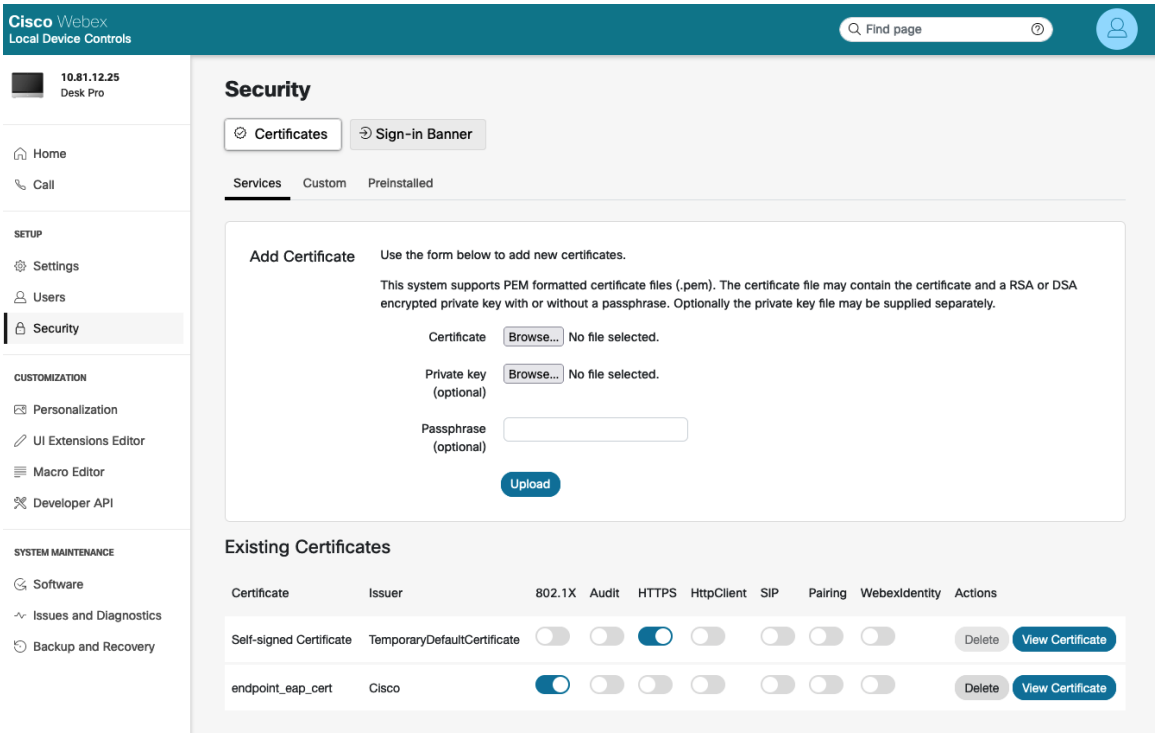
必要に応じて、秘密キーを証明書と一緒にアップロードできます。

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。

802.1X が正常にインストールされたら、ユーザー証明書が有効になっていることを確認します。

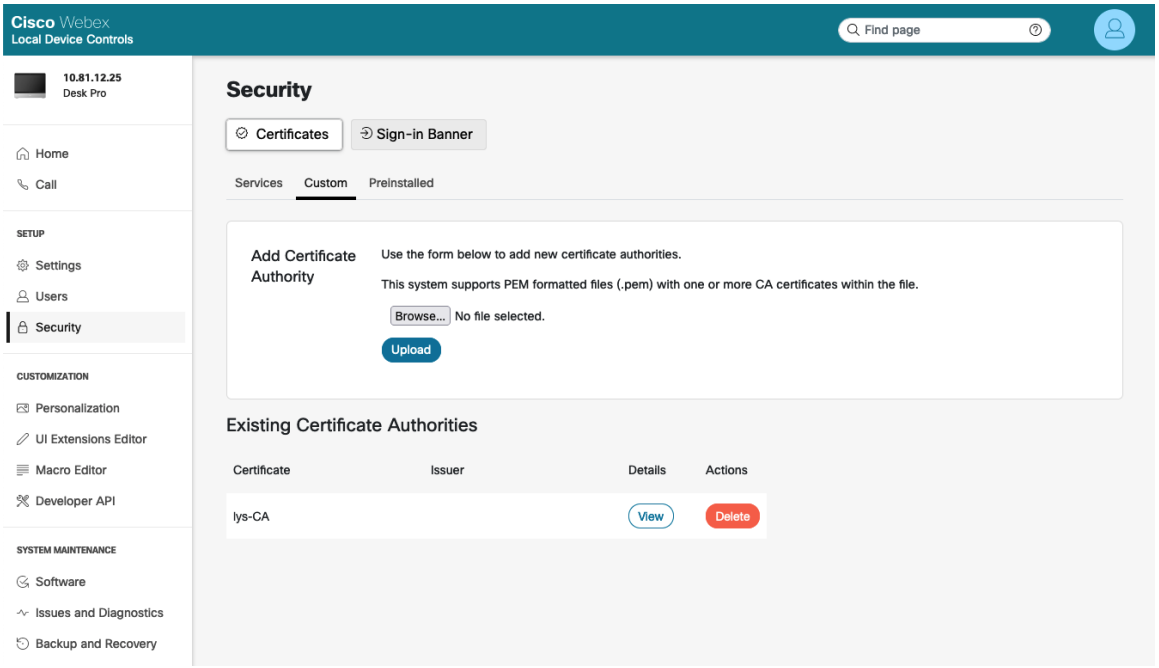
802.1X で有効にできるユーザー証明書は 1 つだけです。したがって、その証明書は EAP-TLS ユーザー証明書として自動的に使用され、追加の Wi-Fi プロファイルの構成は必要ありません。

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 サーバーの証明書を発行したルート CA の証明書は、**EAP-FAST**、**EAP-TLS**、**EAP-TTLS**、または **PEAP** サーバー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。

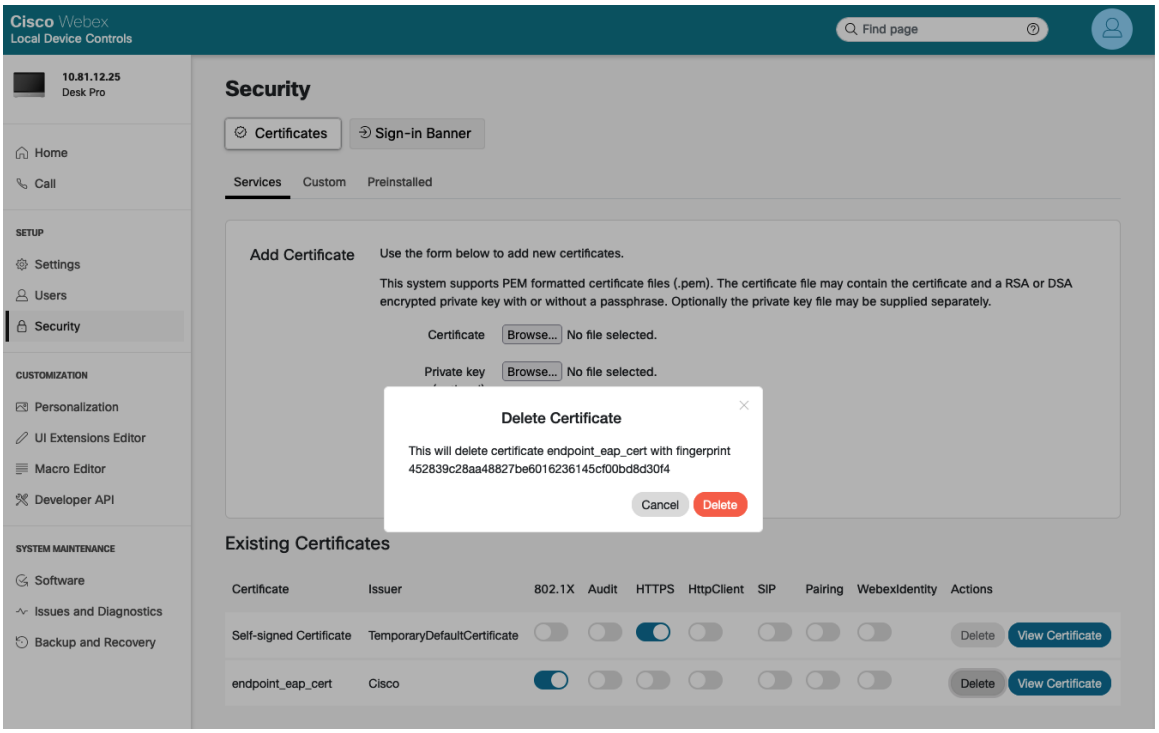
インストールすると、サーバー検証が自動的に有効になり、追加の Wi-Fi プロファイルの構成は必要ありません。



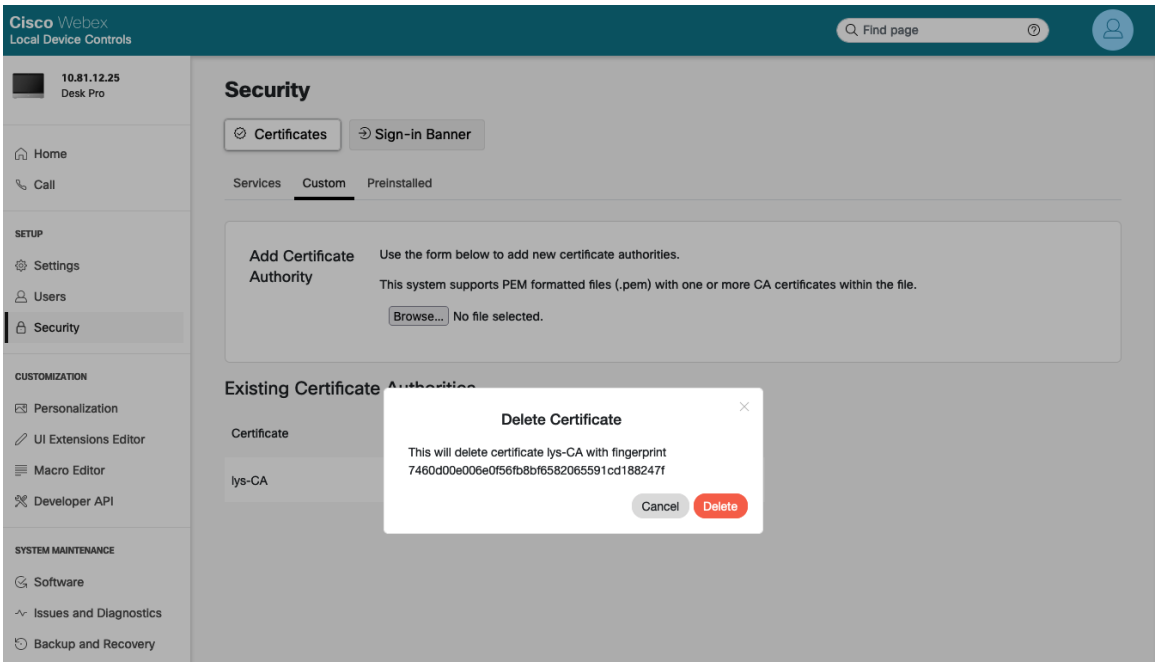
証明書の削除

証明書は個別に削除できます。

個々のユーザー証明書を削除するには、**[セキュリティ（Security）] > [証明書（Certificates）] > [サービス（Services）]** を選択し、**[削除（Delete）]** を選択します。



個々のユーザー証明書を削除するには、**[セキュリティ（Security）] > [証明書（Certificates] > [カスタム（Custom）]** を選択し、**[削除（Delete）]** を選択します。



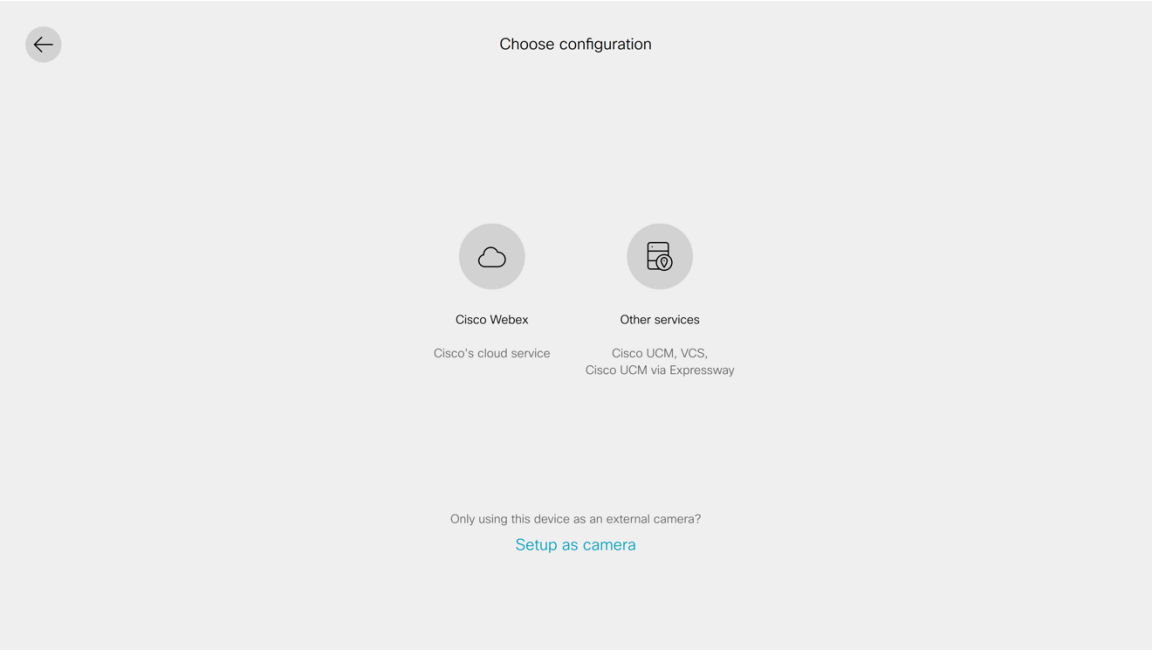
詳細については、次の URL にある『Webex Desk Series 管理者ガイド』を参照してください。

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

呼制御の構成

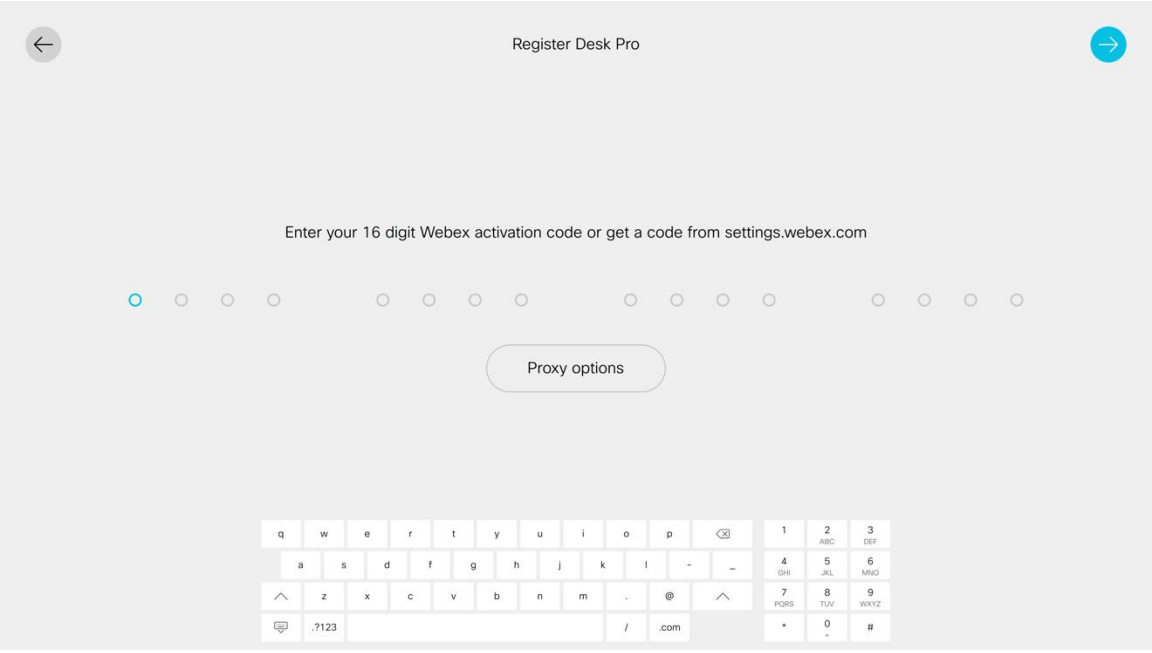
Webex Desk Series は、さまざまな呼制御システムに登録できます。

スタートアップウィザードを使用して、目的の呼制御システムを選択します。



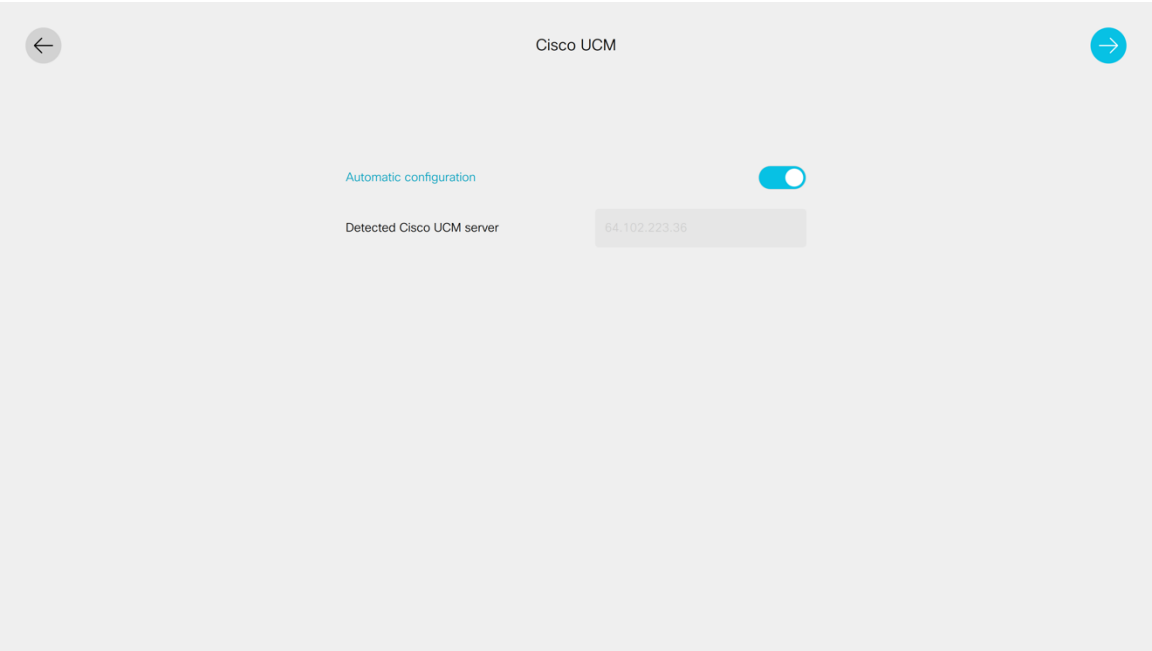
Webex

Webex が選択されている場合は、16 桁のアクティベーションコードを入力し、必要に応じてプロキシオプションを設定します。



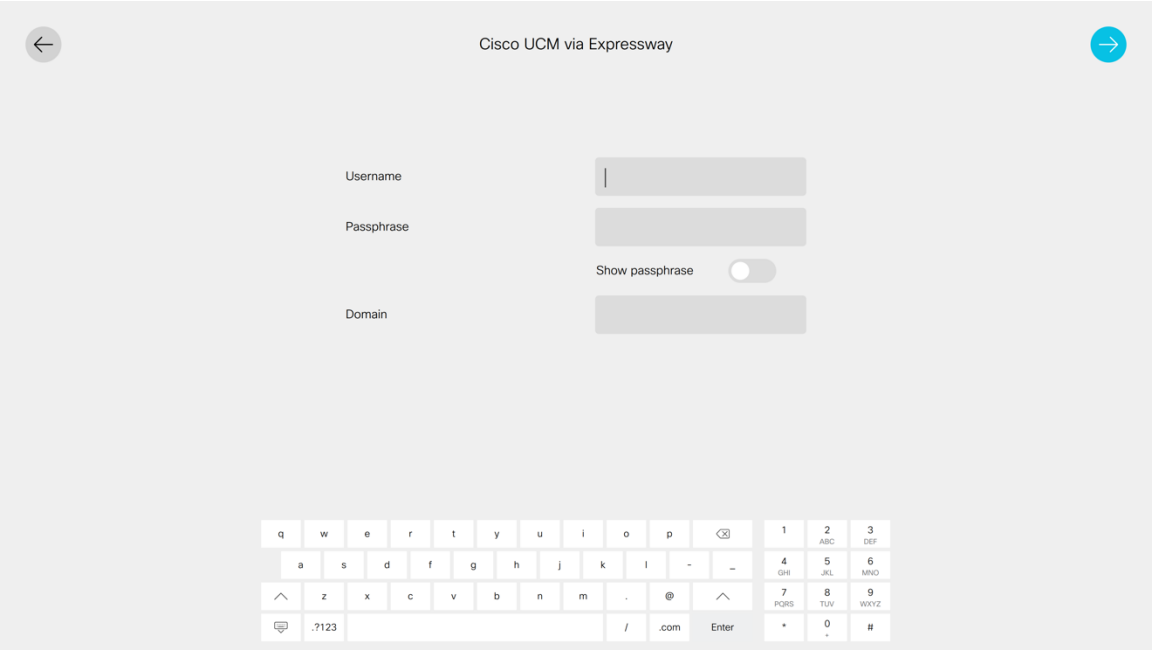
Cisco Unified Communications Manager（UCM）

Cisco UCM が選択されている場合は、自動構成選択を使用してネットワーク経由で提供される **Cisco UCM** サーバーアドレスを使用するか、**Cisco UCM** サーバーを手動で入力します。



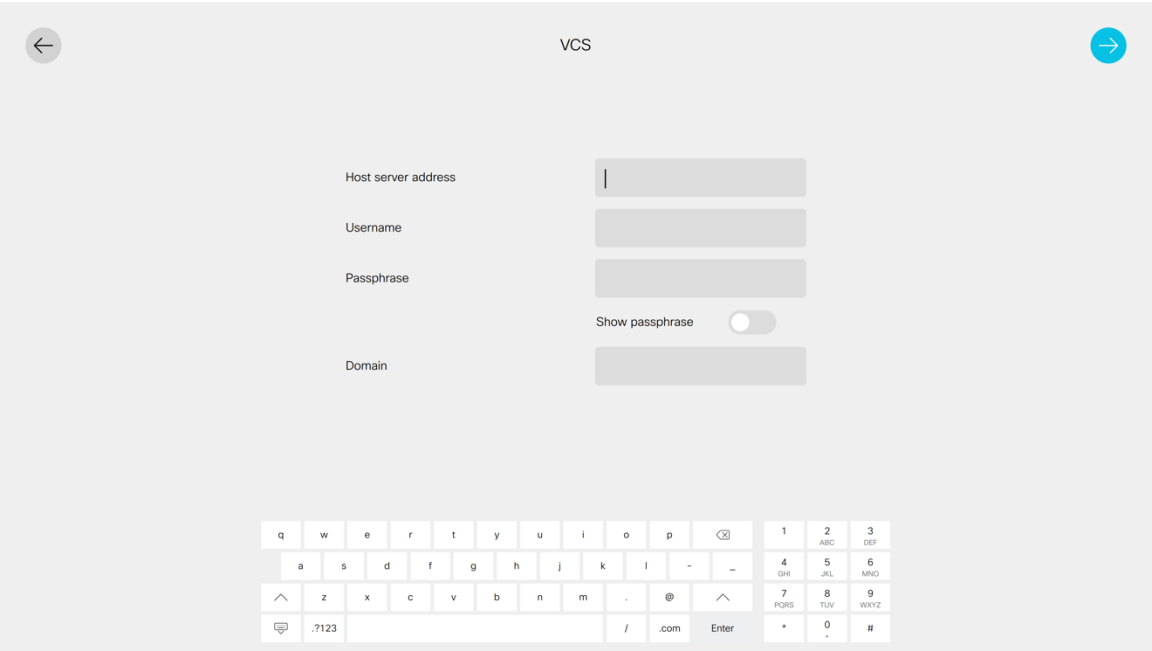
Express 経由の Cisco Unified Communications Manager

Expressway 経由の Cisco UCM **が選択されている場合は、**ユーザー名、パスフレーズ、**および**ドメイン情報**を入力します。**



Cisco Video Communication Server（VCS）

VCS が選択されている場合は、**ホストサーバーアドレス**、**ユーザー名**、**パスフレーズ**、および**ドメイン情報**を入力します。

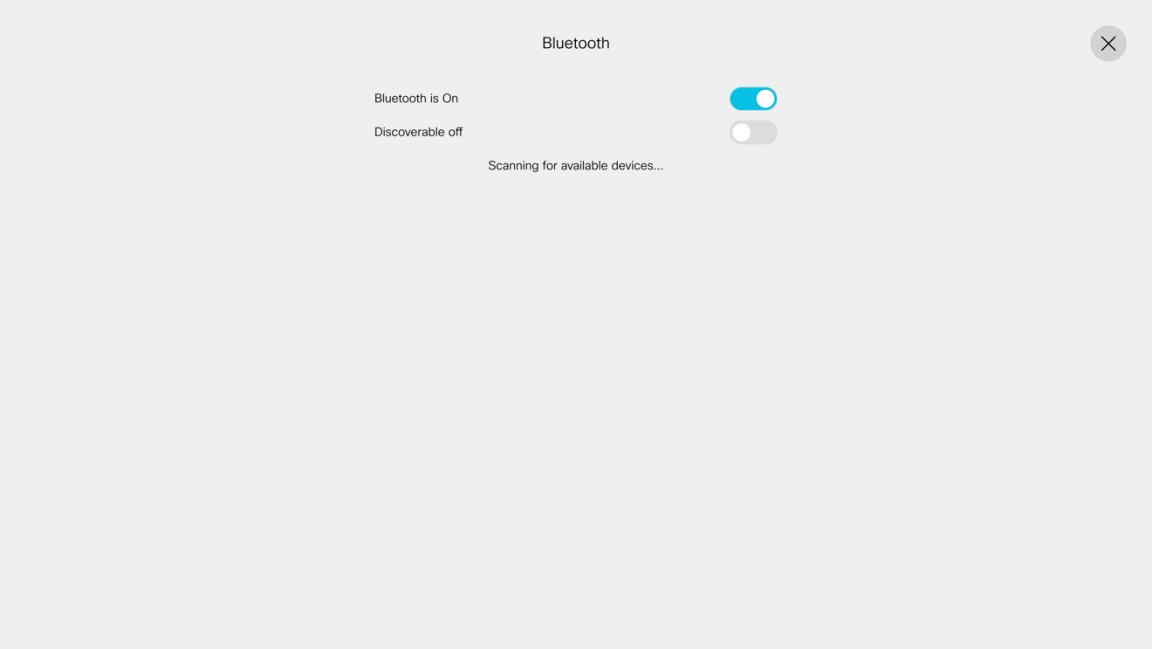


Bluetooth 設定

Webex Desk Series には、ハンズフリー通信を可能にする Bluetooth サポートが含まれています。

Bluetooth ヘッドセットと Webex Desk Series をペアリングする手順は次のとおりです。

- [設定（Settings）] > [Bluetooth] に移動します。
- **[Bluetooth]** が **[オン（On）]** に設定されていることを確認します。



- Bluetooth デバイスがペアリングモードになっていることを確認します。
- Bluetooth デバイスがリストに表示されたら、それを選択します。
- その後、Webex Desk Series は Bluetooth デバイスと自動的にペアリングを試みます。
  失敗した場合、プロンプトが表示されたら PIN コードを入力します。
- ペアリングされると、Webex Desk Series は Bluetooth デバイスへの接続を試みます。
- Bluetooth デバイスを切断するには、そのデバイスをタップします。もう一度タップして接続します。
- **[ペアリング解除（Unpair）]** を選択して、ペアリングされた Bluetooth デバイスを削除します。

ファームウェアのアップグレード

Webex

Webex Desk Series 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 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 の署名付き COP ファイルをインストールします。

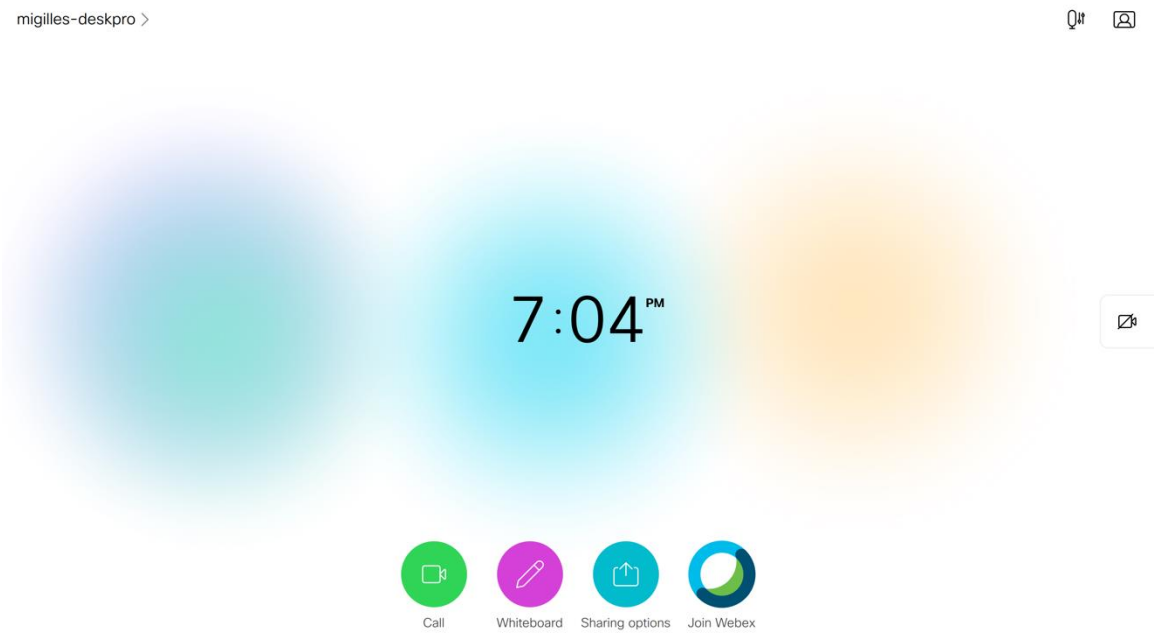
COP ファイルのインストール方法については、次の URL にある『Cisco Unified Communications Manager Operating System Administration Guide（Cisco Unified Communications Manager オペレーティング システム アドミニストレーション ガイド）』を参照してください。

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

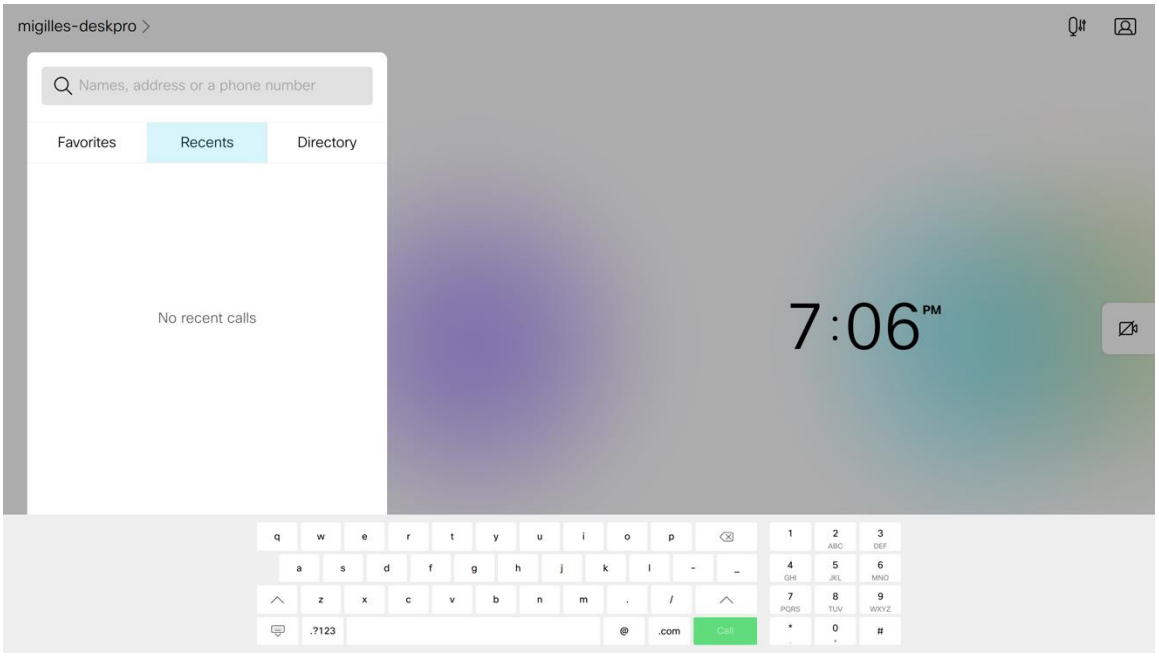
ダウンロードされたデバイス構成ファイルが解析され、デバイスのロードが識別されます。その後、Webex Desk Series はファームウェアファイルをフラッシュにダウンロードします（指定されたイメージがまだ実行されていない場合）。

Webex Desk Series の使用

Webex Desk Series は、ローカルまたはミーティング経由での通話やコンテンツの共有など、さまざまなコラボレーションオプションを提供します。



[通話（Call）] オプションを選択して電話をかけ、名前、ビデオアドレス、または電話番号を入力します。

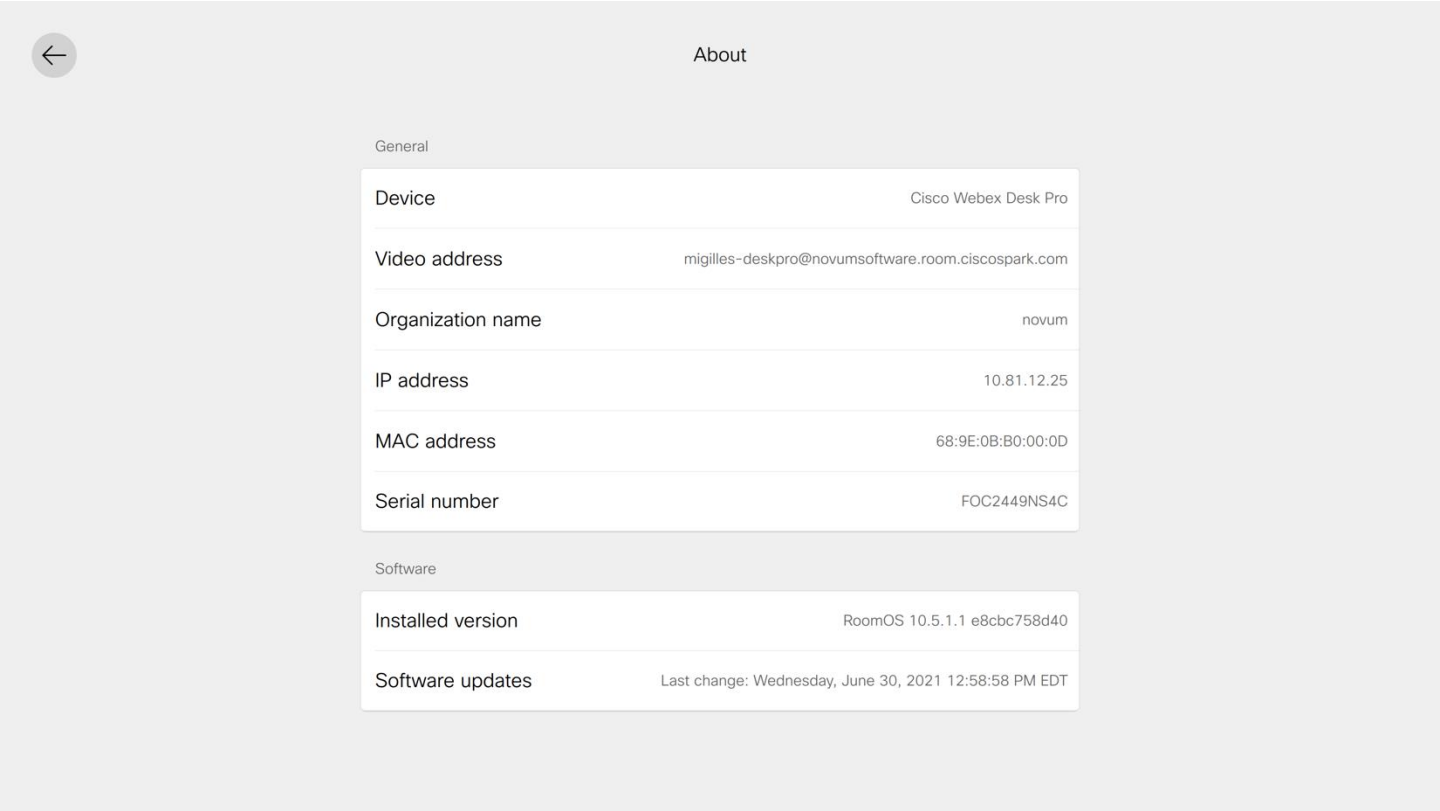


トラブルシューティング

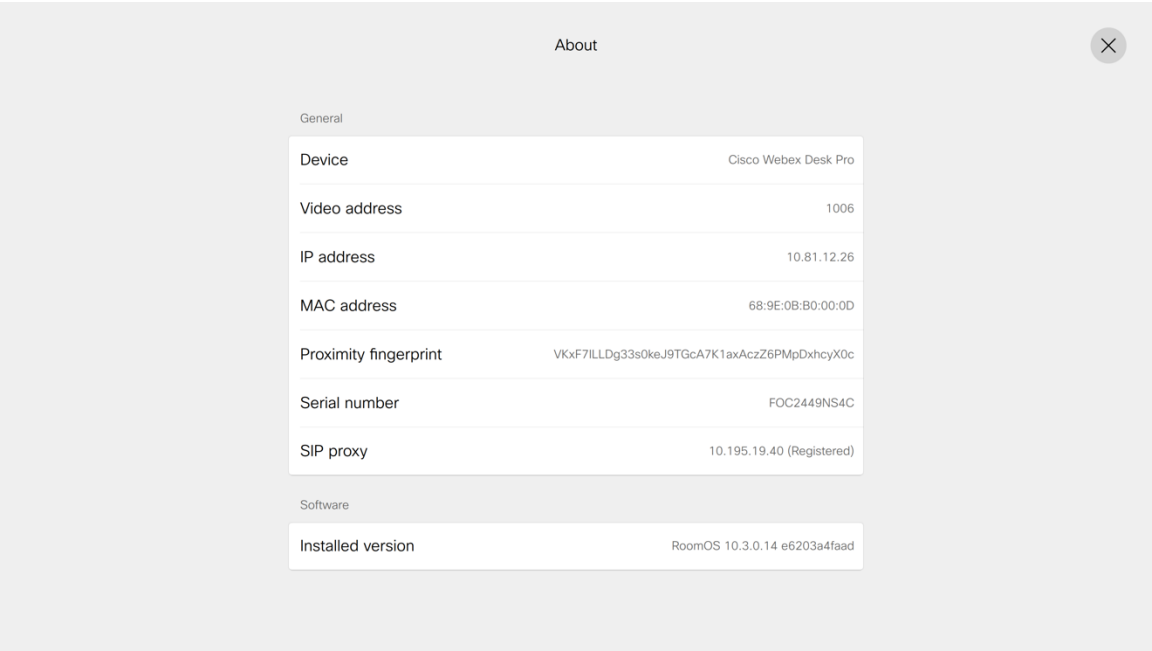
デバイスについて

ビデオアドレス、IP アドレス、MAC アドレス、シリアル番号、およびバージョン情報は、**[設定（Settings）]** > **[このデバイスについて（About this device）]** に表示されます。

Webex

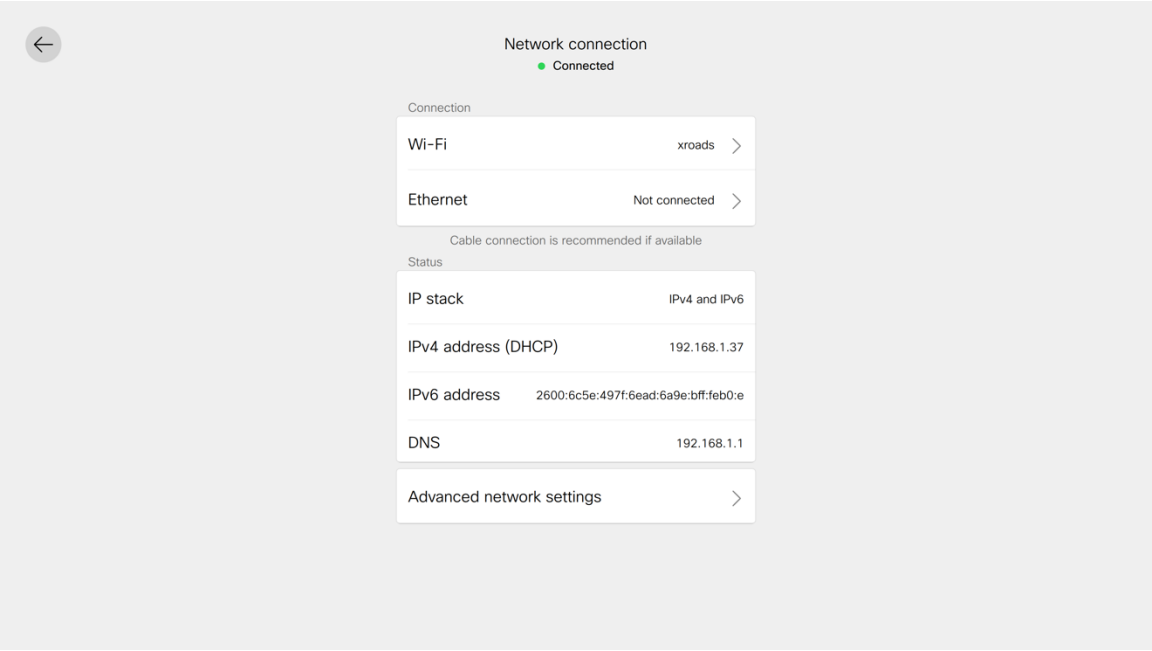


Cisco Unified Communications Manager



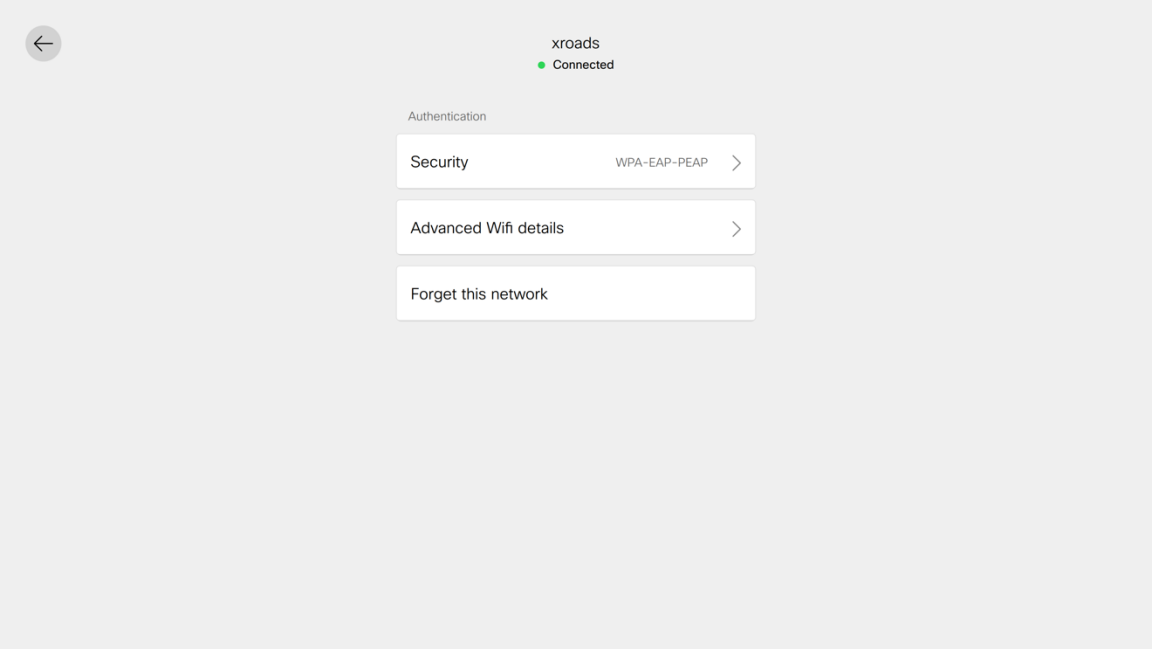
ネットワーク接続ステータス

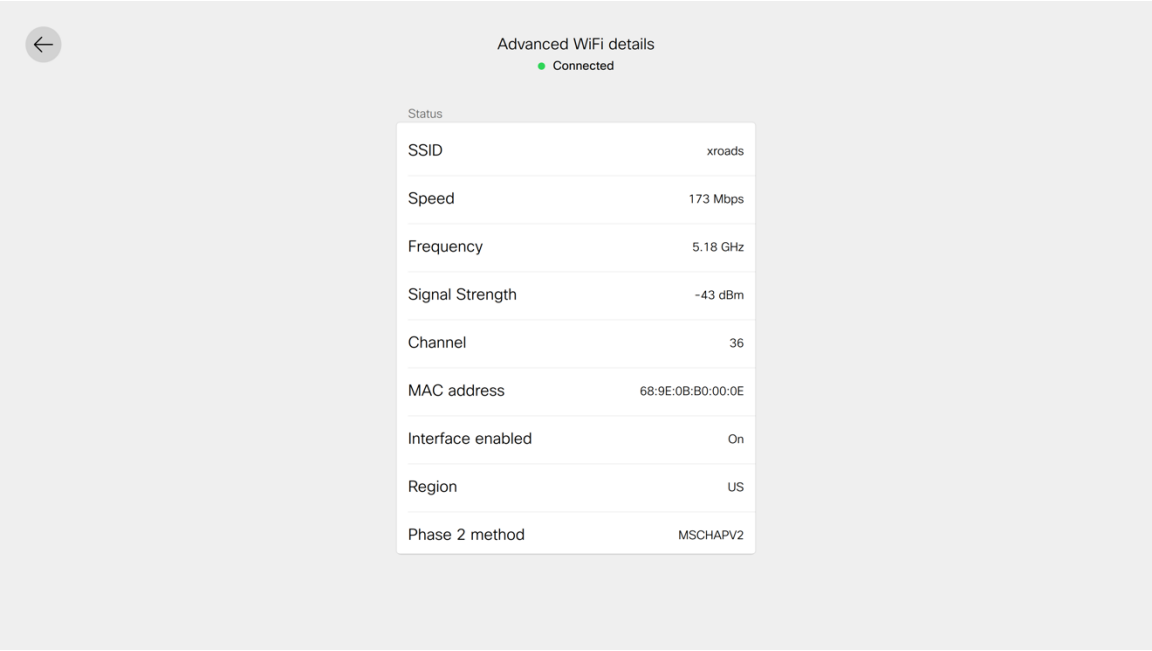
現在のネットワーク接続ステータスと IP アドレス情報は、**[設定（Settings）] > [ネットワーク接続（Network connection）]** に表示されます。



高度な Wi-Fi の詳細

SSID、速度/データレート、周波数/チャンネル、信号強度、WLAN MAC アドレスなどを含む詳細な Wi-Fi 接続は、**[設定（Settings）] > [ネットワーク接続（Network connection）] > [Wi-Fi]** で接続された Wi-Fi ネットワークを選択し、**[高度な Wi-Fi の詳細（Advanced Wifi details）]** を選択すると表示されます。





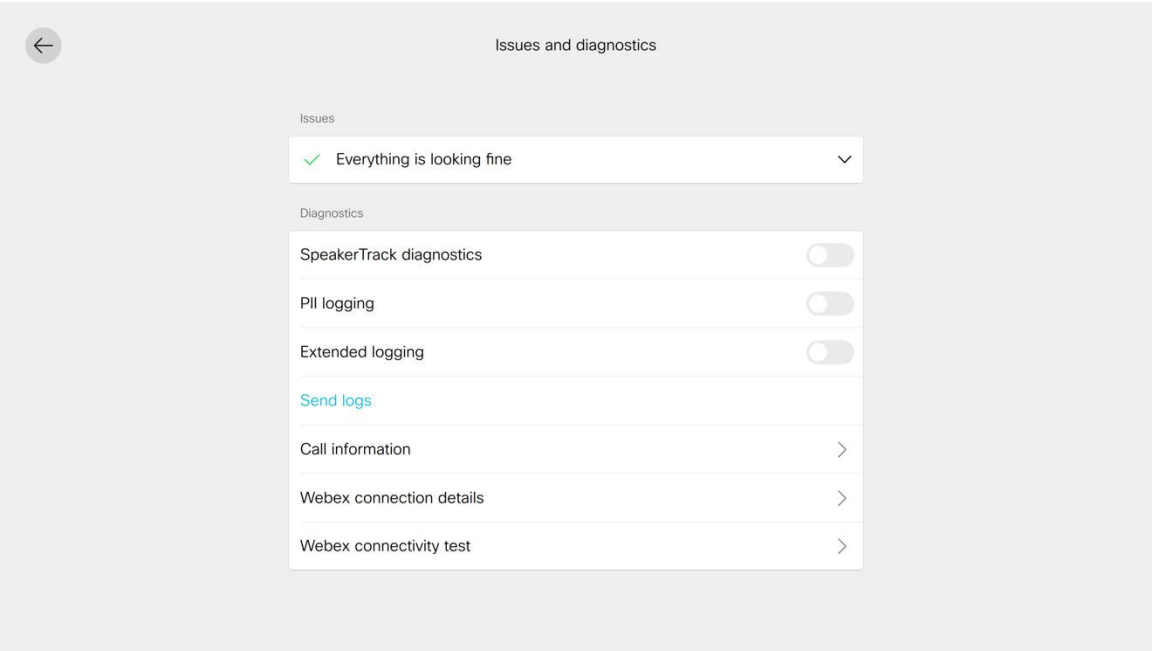
問題と診断

[設定（Settings）] > [問題と診断（Issues and Diagnostics）] を選択すると、現在の問題と診断オプションが表示されます。

Webex

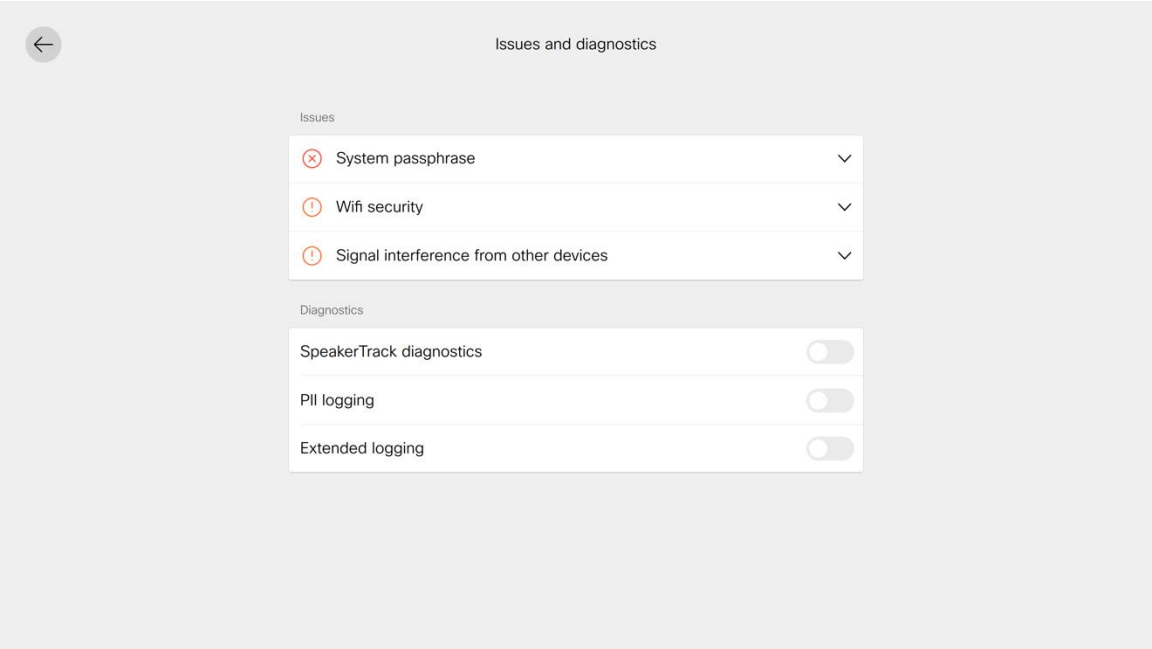
Webex に登録すると、デバイスログを Webex Control Hub から要求するか、**[問題と診断（Issues and Diagnostics）]**メニューから送信できます。デバイスログは、Webex Control Hub または Webex Series Web ページの **[システムメンテナンス] > [問題と診断（Issues and Diagnostics）] > [システムログ（System Logs）]** からダウンロードできます。

Webex 接続テストは、**[問題と診断（Issues and diagnostics）]** メニューから開始することもできます。



Cisco Unified Communications Manager

Cisco Unified Communications Manager に登録すると、デバイスログは、**[システムメンテナンス（System Maintenance）] > [問題と診断（Issues and Diagnostics）] > [システムログ（System Logs）]** の Webex Desk Series Web ページからダウンロードできます。



デバイスの Web ページ

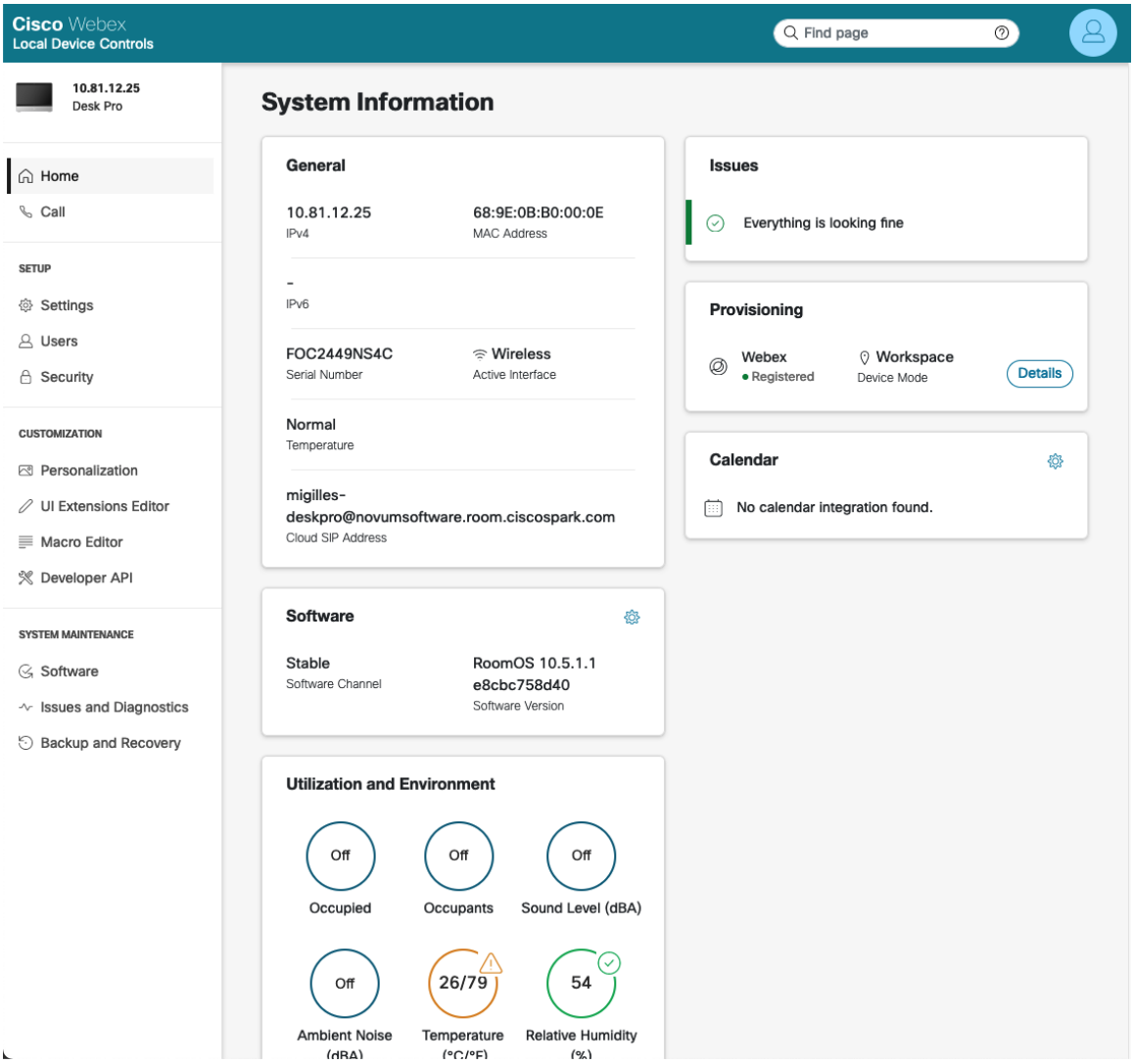
Webex Desk Series の Web ページには、システム情報、セットアップ、カスタマイズ、およびシステム メンテナンス オプションが用意されています。

Web ページにアクセスするには、Webex Desk Series の Web ページで設定された有効な管理者アカウントのログイン情報でログインします。

システム情報

Webex Desk Series は、ネットワークステータス、IP アドレス、MAC アドレス、シリアル番号、バージョン情報などのシステム情報を提供します。

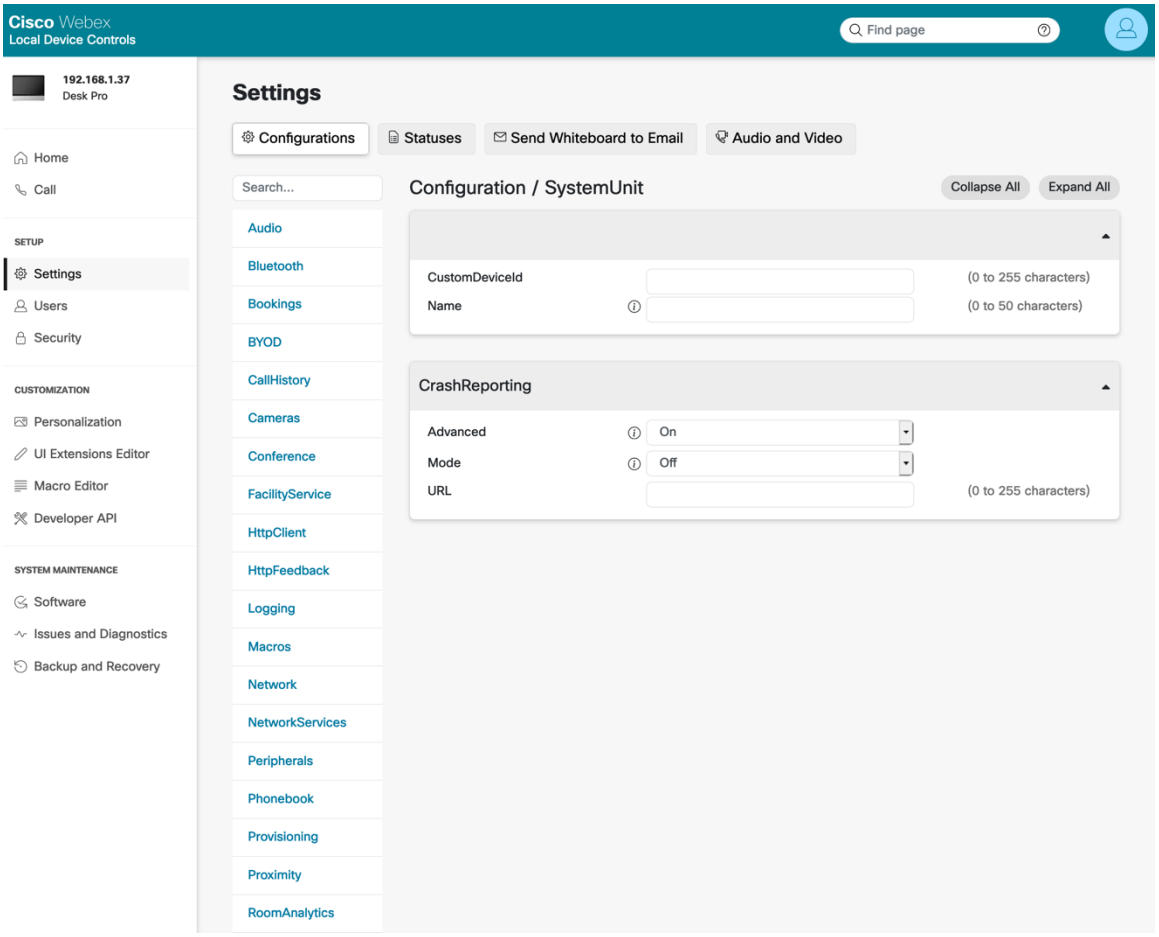
Webex Desk Series の Web インターフェイス（https://x.x.x.x）を参照し、**[ホーム（Home）]** を選択してこの情報を表示します。

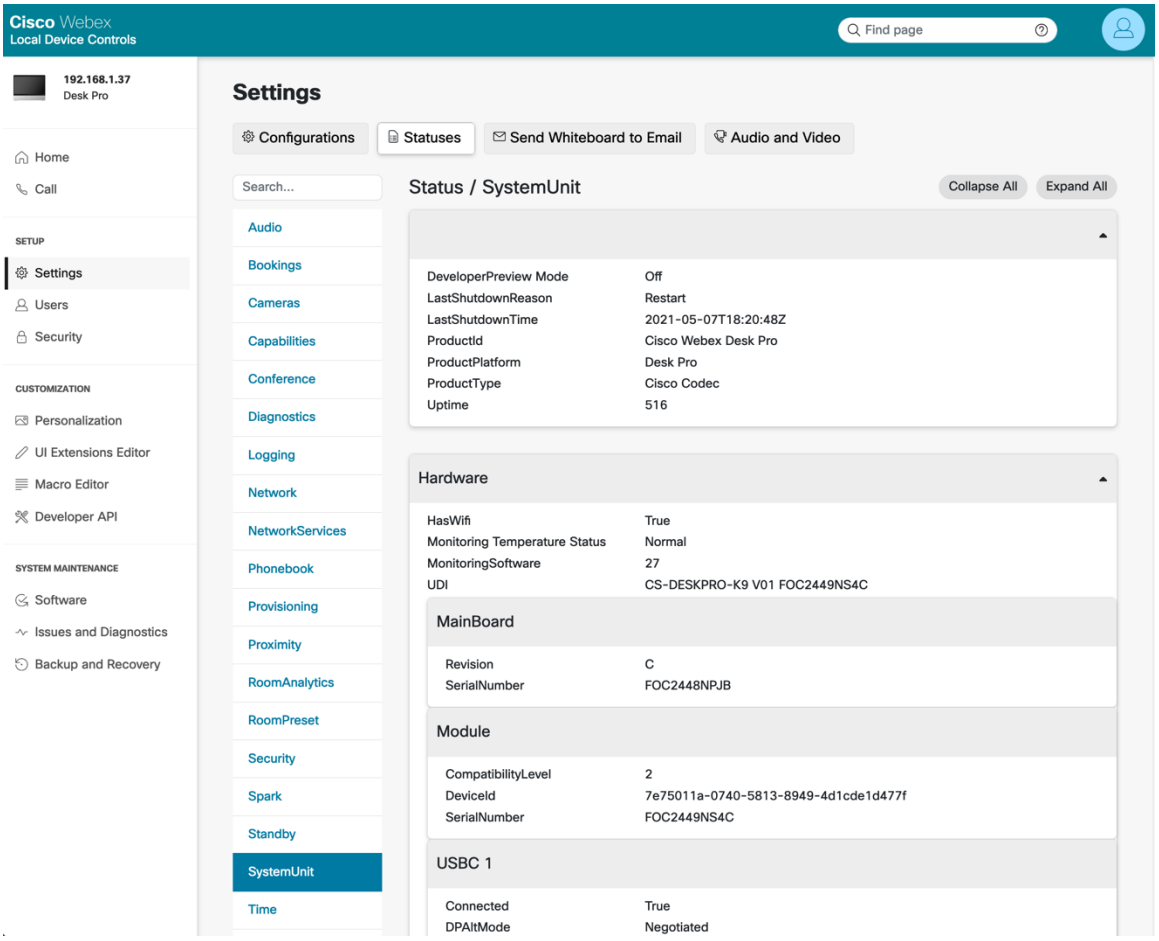


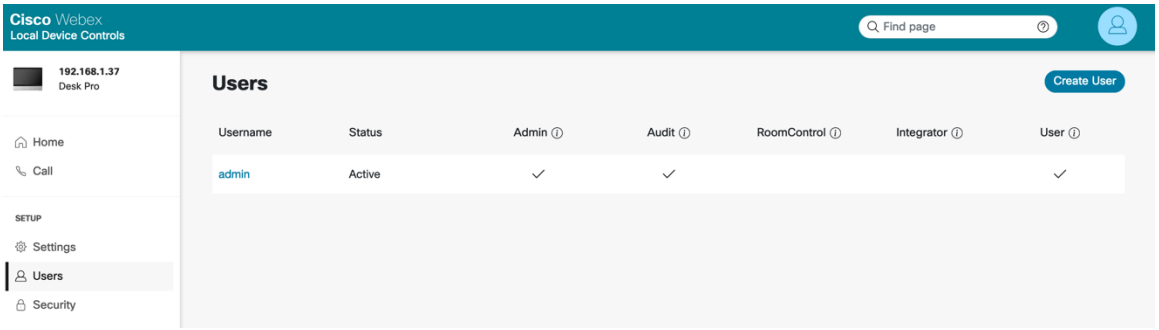
セットアップ

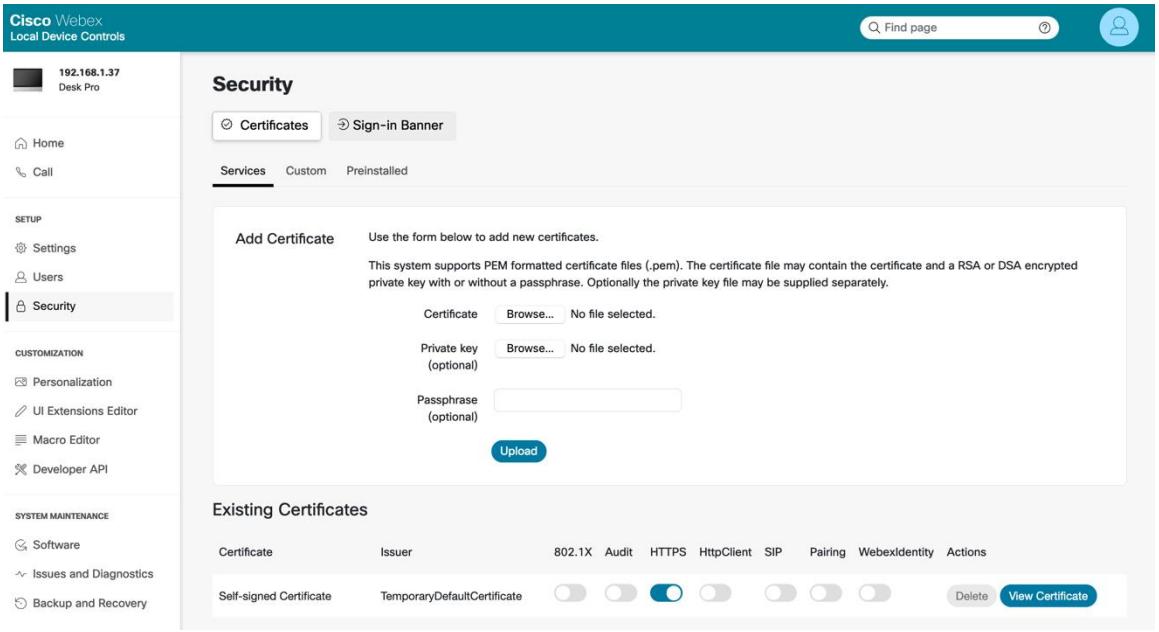
Webex Desk Series は、さまざまな構成オプションとステータス情報を提供します。

Webex Desk Series の Web インターフェイス（https://x.x.x.x）を参照し、**[セットアップ（Setup）]** で目的のオプションを選択して、この情報を表示します。


Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
SYSTEM MAINTENANCE
Software
Issues and Diagnostics
Backup and Recovery
Settings
Configurations
Statuses
Send Whiteboard to Email
Audio and Video
Search...
Audio
Bluetooth
Bookings
BYOD
CallHistory
Cameras
Conference
FacilityService
HttpClient
HttpFeedback
Logging
Macros
Network
NetworkServices
Peripherals
Phonebook
Provisioning
Proximity
RoomAnalytics
Configuration / SystemUnit
Collapse All
Expand All
CustomDeviceId
(0 to 255 characters)
Name
(0 to 50 characters)
CrashReporting
Advanced
On
Mode
Off
URL
(0 to 255 characters)


Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Settings
Configurations
Statuses
Send Whiteboard to Email
Audio and Video
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
SYSTEM MAINTENANCE
Software
Issues and Diagnostics
Backup and Recovery
Search...
Audio
Bookings
Cameras
Capabilities
Conference
Diagnostics
Logging
Network
NetworkServices
Phonebook
Provisioning
Proximity
RoomAnalytics
RoomPreset
Security
Spark
Standby
SystemUnit
Time
Status / SystemUnit
Collapse All
Expand All
DeveloperPreview Mode Off
LastShutdownReason Restart
LastShutdownTime 2021-05-07T18:20:48Z
ProductId Cisco Webex Desk Pro
ProductPlatform Desk Pro
ProductType Cisco Codec
Uptime 516
Hardware
HasWifi True
Monitoring Temperature Status Normal
MonitoringSoftware 27
UDI CS-DESKPRO-K9 V01 FOC2449NS4C
MainBoard
Revision C
SerialNumber FOC2448NPJB
Module
CompatibilityLevel 2
DeviceId 7e75011a-0740-5813-8949-4d1cde1d477f
SerialNumber FOC2449NS4C
USBC 1
Connected True
DPAltMode Negotiated

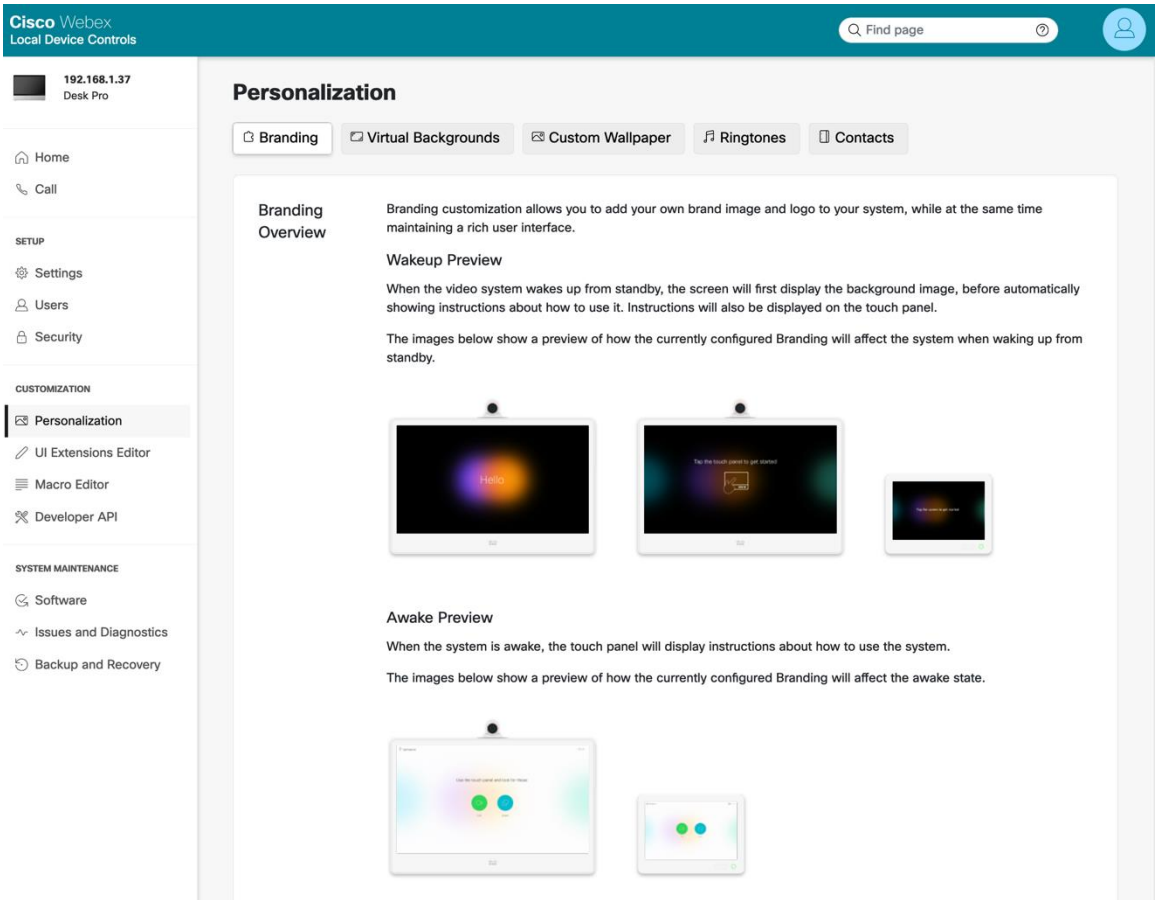

Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Users
Create User
Home
Call
SETUP
Settings
Users
Security
Username
Status
Admin
Audit
RoomControl
Integrator
User
admin
Active

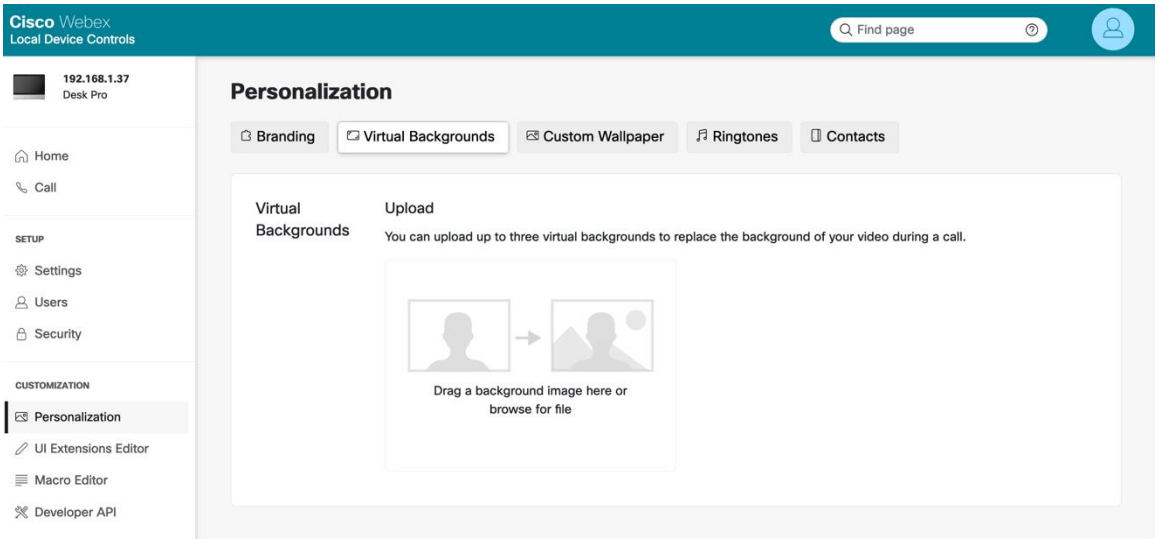


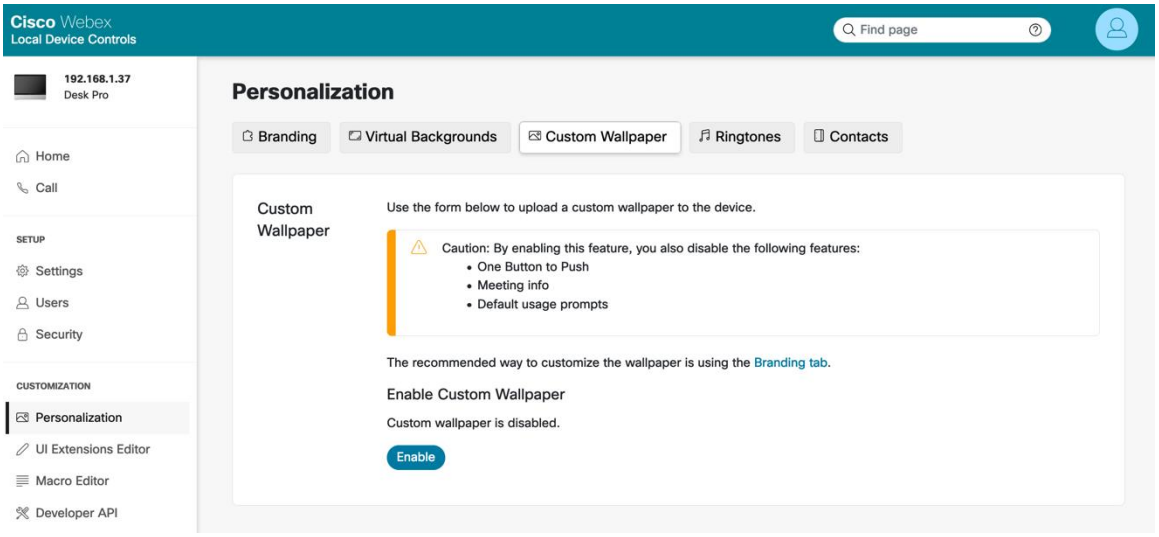
カスタマイゼーション

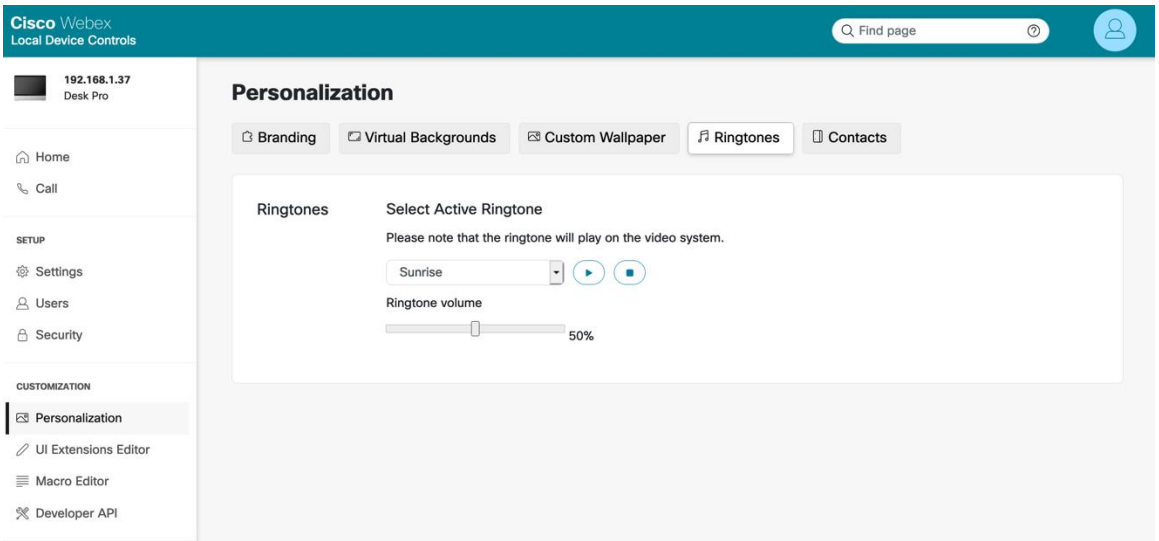
Webex Desk Series には、さまざまなパーソナライゼーション オプションとその他のカスタマイズオプションが用意されています。

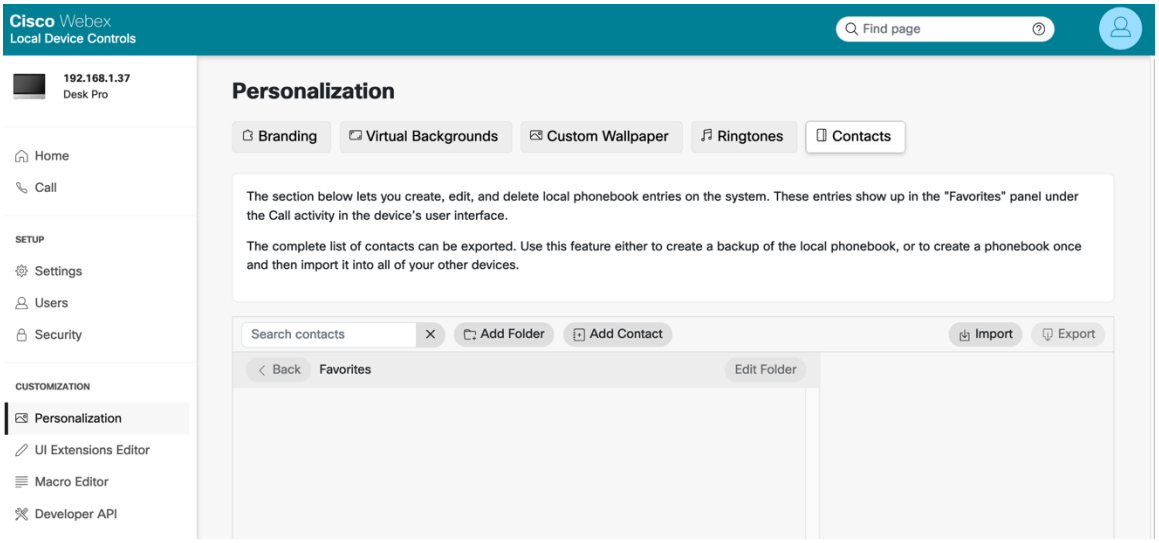
Webex Desk Series の Web インターフェイス（https://x.x.x.x）を参照し、**[カスタマイズ（Customization）]** で目的のオプションを選択して、この情報を表示します。




Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
Personalization
Branding
Virtual Backgrounds
Custom Wallpaper
Ringtones
Contacts
Virtual Backgrounds
Upload
You can upload up to three virtual backgrounds to replace the background of your video during a call.
Drag a background image here or browse for file


Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
Personalization
Branding
Virtual Backgrounds
Custom Wallpaper
Ringtones
Contacts
Custom Wallpaper
Use the form below to upload a custom wallpaper to the device.
Caution: By enabling this feature, you also disable the following features:
One Button to Push
Meeting info
Default usage prompts
The recommended way to customize the wallpaper is using the Branding tab.
Enable Custom Wallpaper
Custom wallpaper is disabled.
Enable

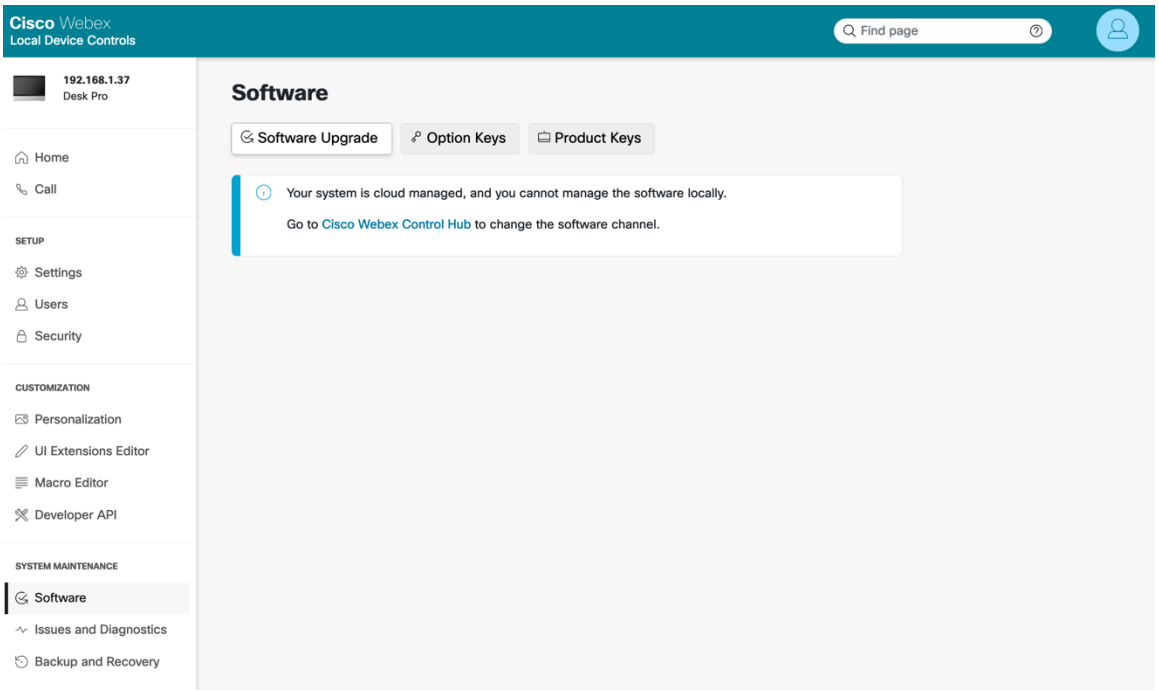

Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
Personalization
Branding
Virtual Backgrounds
Custom Wallpaper
Ringtones
Contacts
Ringtones
Select Active Ringtone
Please note that the ringtone will play on the video system.
Sunrise
Ringtone volume
50%

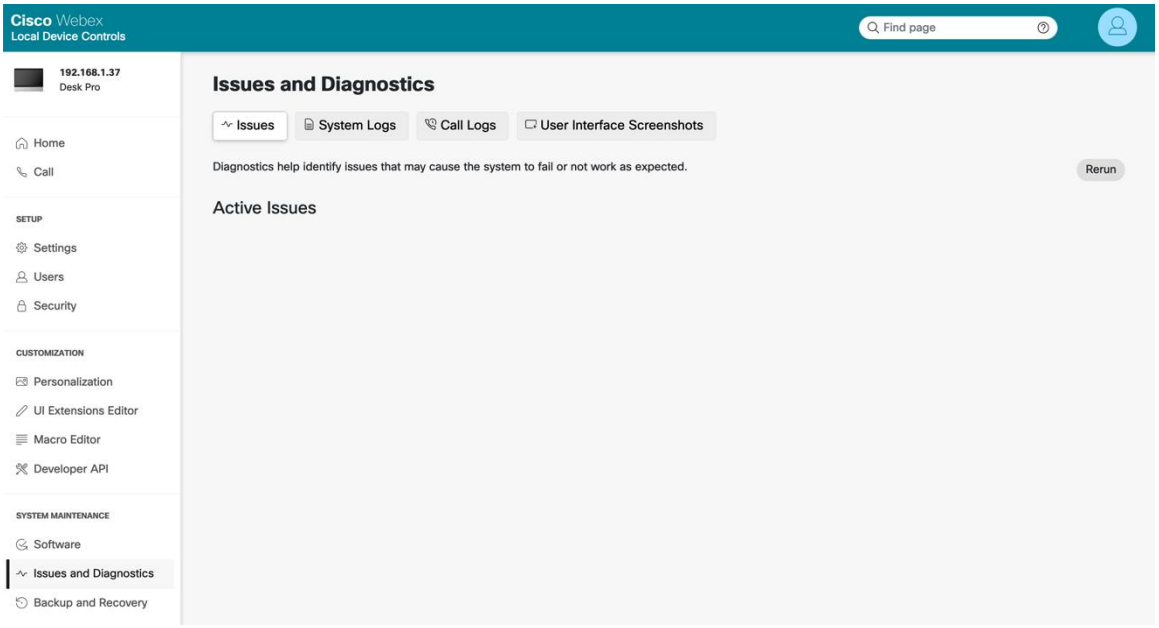


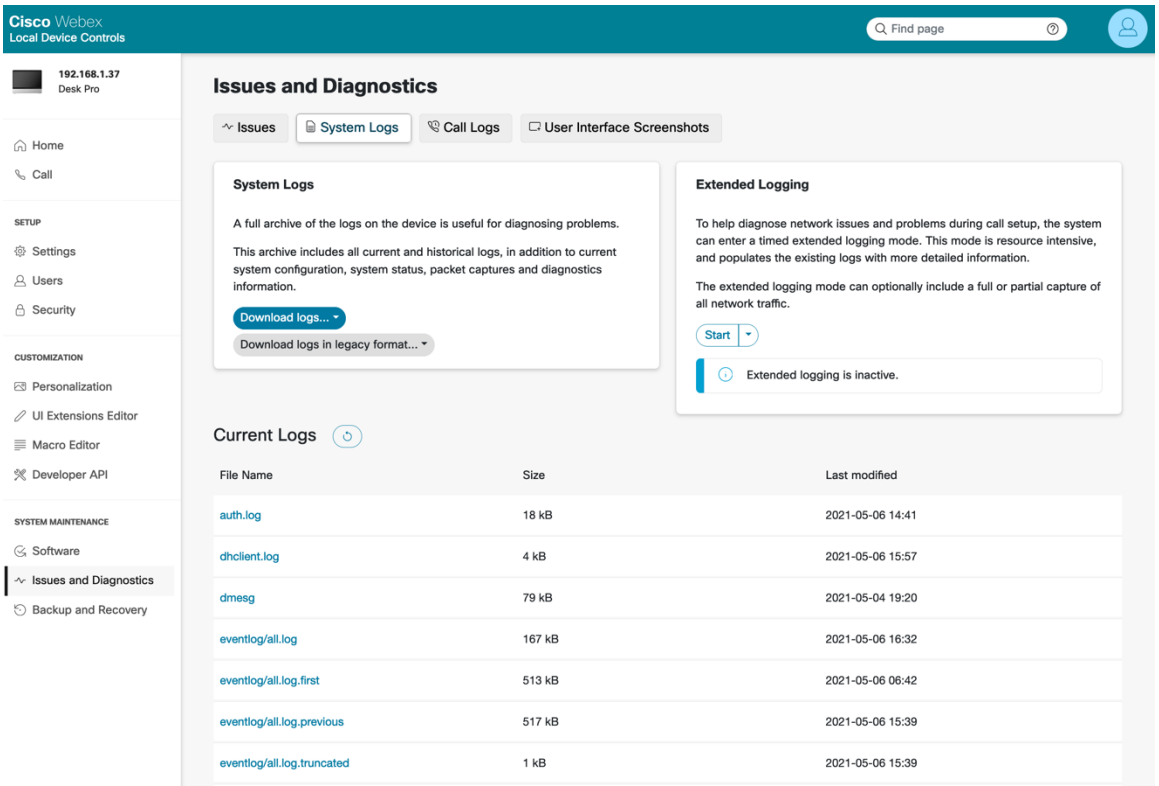
システムメンテナンス

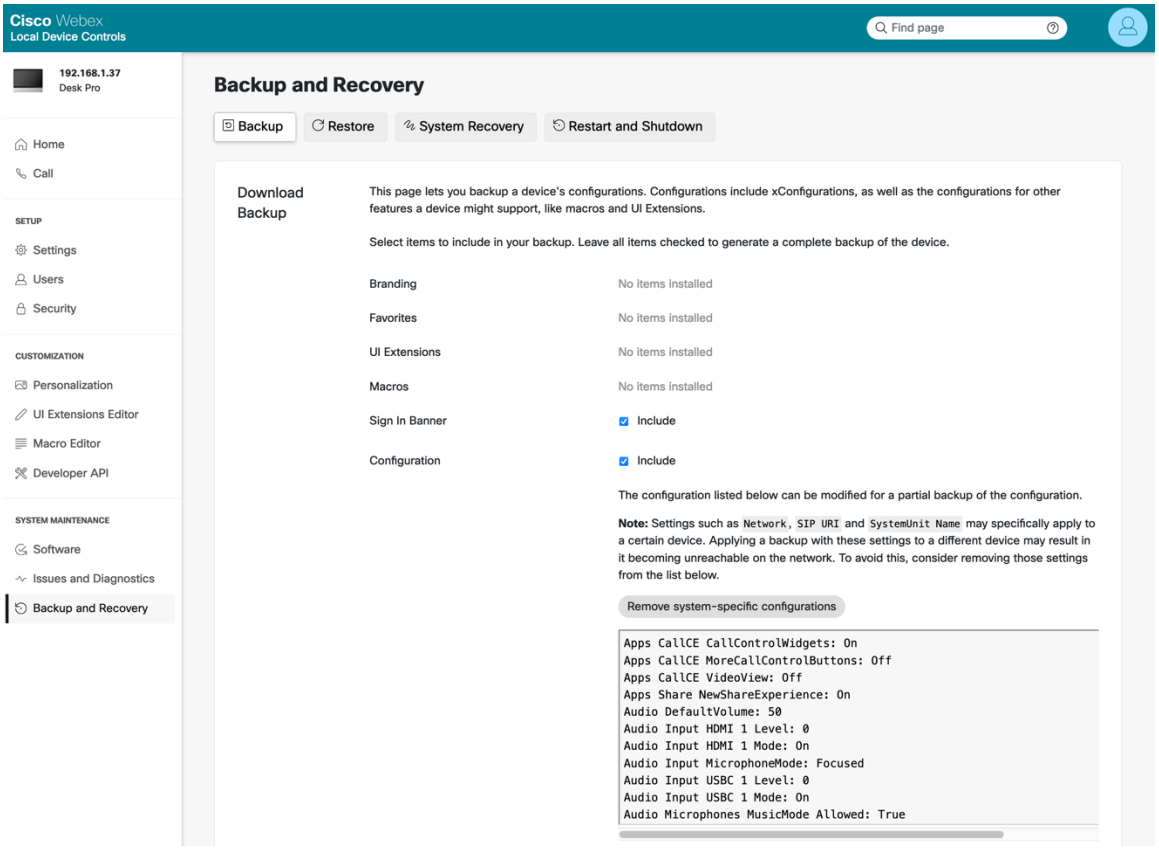
Webex Desk Series は、デバイスログを含むさまざまな有用性オプションを提供します。

Webex Desk Series の Web インターフェイス（https://x.x.x.x）を参照し、**[システムメンテナンス（System Maintenance）]** で目的のオプションを選択して、この情報を表示します。




Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
SYSTEM MAINTENANCE
Software
Issues and Diagnostics
Backup and Recovery
Issues and Diagnostics
Issues
System Logs
Call Logs
User Interface Screenshots
Diagnostics help identify issues that may cause the system to fail or not work as expected.
Rerun
Active Issues

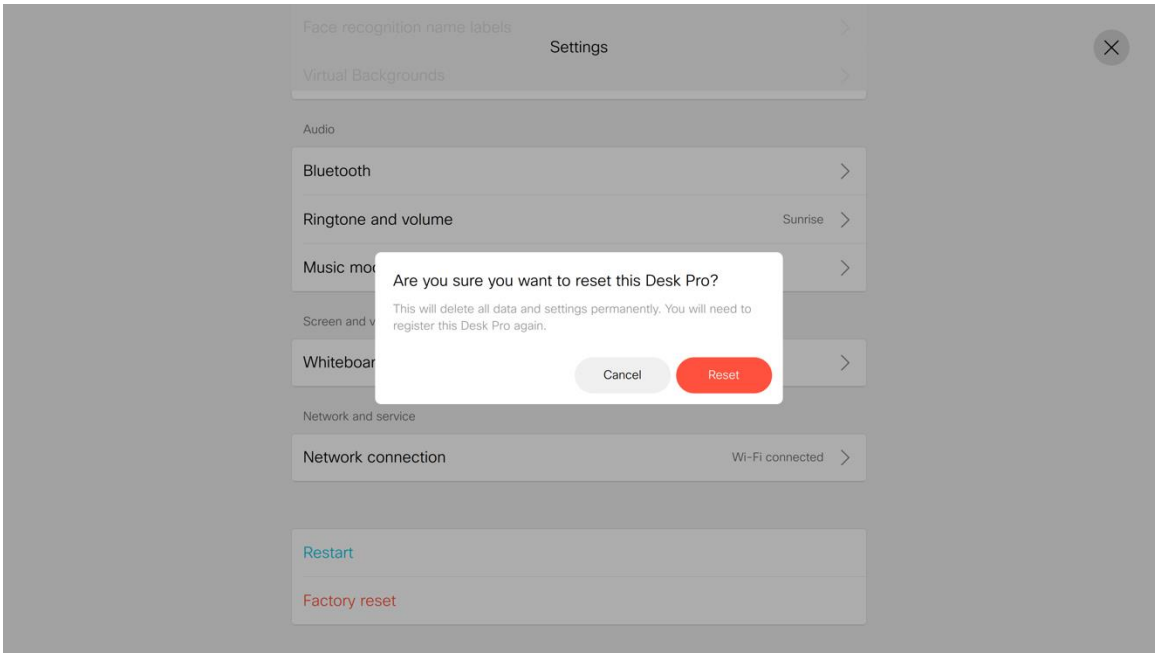

Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
SYSTEM MAINTENANCE
Software
Issues and Diagnostics
Backup and Recovery
Issues and Diagnostics
Issues
System Logs
Call Logs
User Interface Screenshots
System Logs
A full archive of the logs on the device is useful for diagnosing problems.
This archive includes all current and historical logs, in addition to current system configuration, system status, packet captures and diagnostics information.
Download logs...
Download logs in legacy format...
Extended Logging
To help diagnose network issues and problems during call setup, the system can enter a timed extended logging mode. This mode is resource intensive, and populates the existing logs with more detailed information.
The extended logging mode can optionally include a full or partial capture of all network traffic.
Start
Extended logging is inactive.
Current Logs
File Name
Size
Last modified
auth.log
18 kB
2021-05-06 14:41
dhclient.log
4 kB
2021-05-06 15:57
dmesg
79 kB
2021-05-04 19:20
eventlog/all.log
167 kB
2021-05-06 16:32
eventlog/all.log.first
513 kB
2021-05-06 06:42
eventlog/all.log.previous
517 kB
2021-05-06 15:39
eventlog/all.log.truncated
1 kB
2021-05-06 15:39



初期化

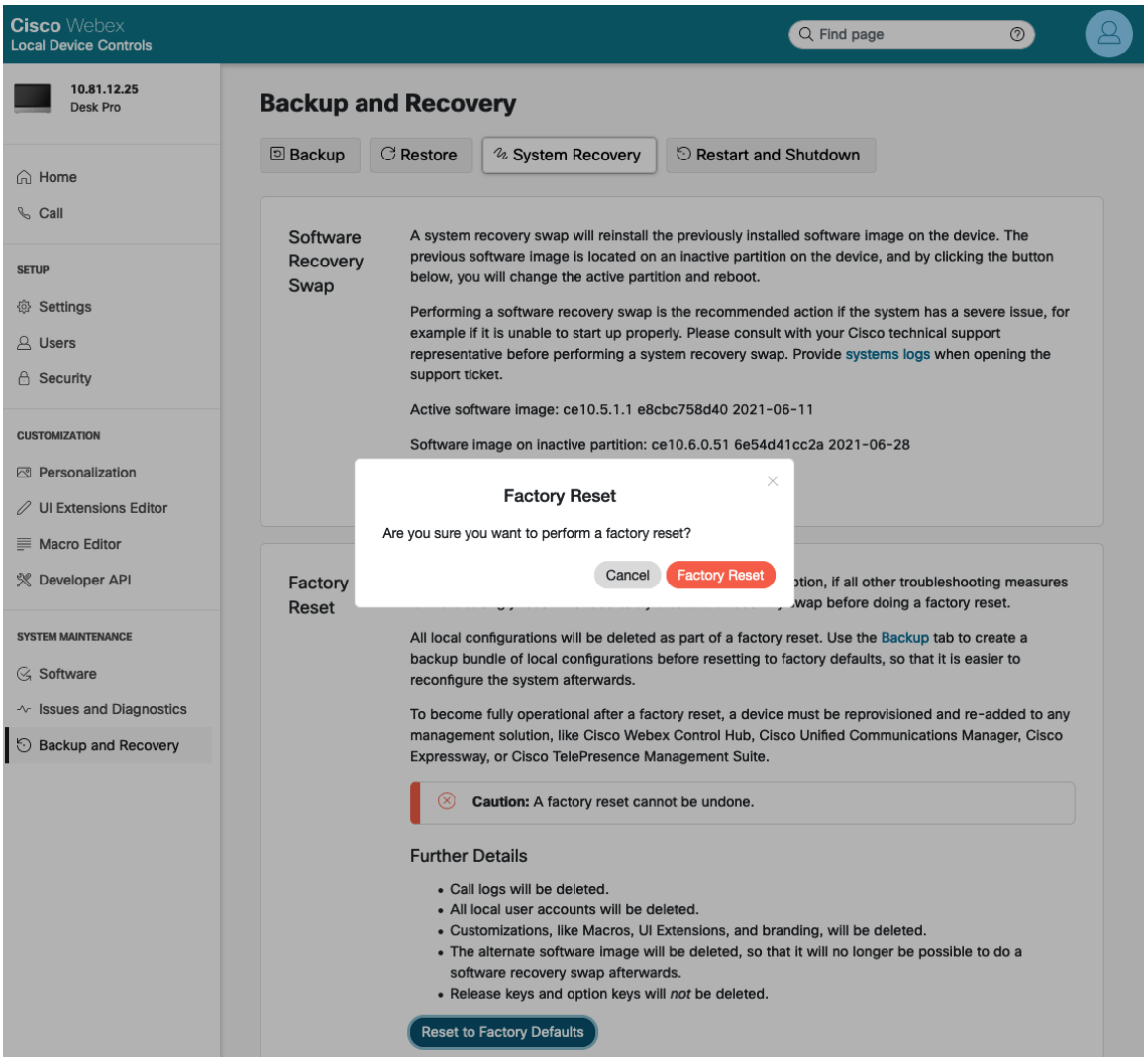
[設定（Settings）] で **[工場出荷時設定にリセット（Factory reset）]** を選択することで、Webex Desk Series からすべてのデータを消去できます。

初期化の確認画面が表示されたら、**[リセット（Reset）]** を選択します。



工場出荷時のリセットは、**[システムメンテナンス（System Maintenance）] > [バックアップとリカバリ（Backup and Recovery）] > [システムリカバリ（System Recovery）]** の下にある **[工場出荷時のデフォルトにリセット（Reset to Factory Defaults）]** を選択して、Webex Desk Series の Web ページから実行することもできます。

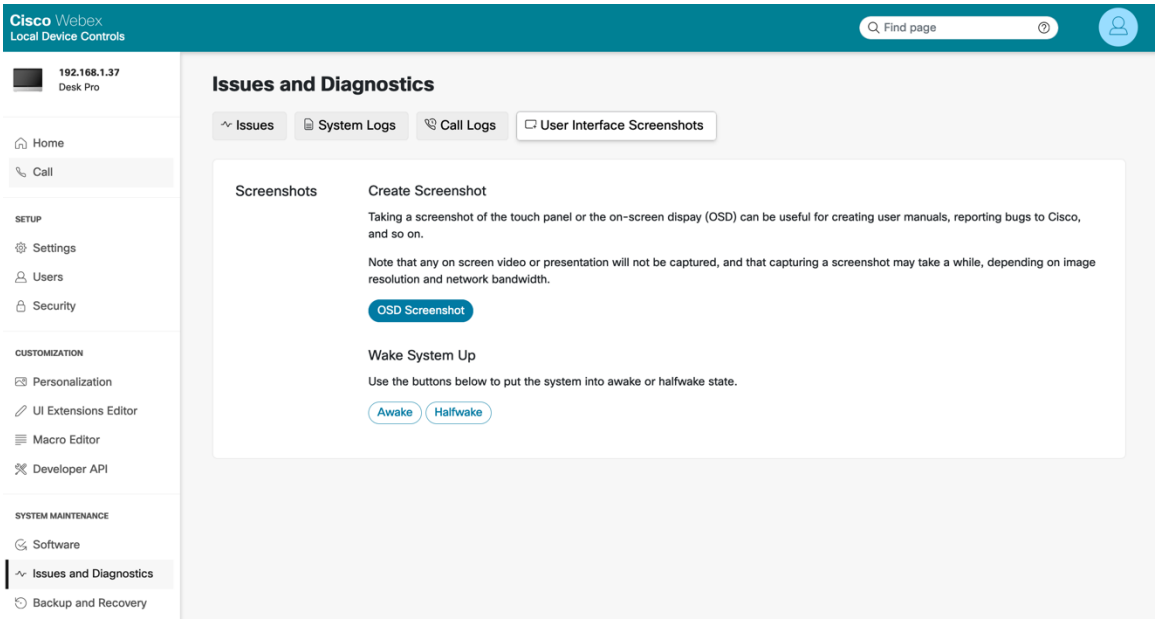
初期化の確認画面が表示されたら、**[工場出荷時の状態へのリセット（Factory Reset）]** を選択します。



デバイス画面のスクリーンショットのキャプチャ

Webex Desk Series の現在の表示は、Webex Desk Series の Web ページからキャプチャできます。

Webex Desk Series の Web インターフェイス（https://x.x.x.x）を参照し、**[システムメンテナンス（System Maintenance）] > [問題と診断（Issues and Diagnostics）] > [ユーザーインターフェイスのスクリーンショット（User Interface Screenshots）]** で **[OSD スクリーンショット（OSD Screenshot）]** を選択して、スクリーンショットをキャプチャします。


Cisco Webex
Local Device Controls
Find page
192.168.1.37
Desk Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
UI Extensions Editor
Macro Editor
Developer API
SYSTEM MAINTENANCE
Software
Issues and Diagnostics
Backup and Recovery
Issues and Diagnostics
Issues
System Logs
Call Logs
User Interface Screenshots
Screenshots
Create Screenshot
Taking a screenshot of the touch panel or the on-screen dispay (OSD) can be useful for creating user manuals, reporting bugs to Cisco, and so on.
Note that any on screen video or presentation will not be captured, and that capturing a screenshot may take a while, depending on image resolution and network bandwidth.
OSD Screenshot
Wake System Up
Use the buttons below to put the system into awake or halfwake state.
Awake
Halfwake

その他のマニュアル

Webex Desk Series データシート

https://www.cisco.com/c/ja_jp/products/collateral/collaboration-endpoints/collaboration-room-endpoints/datasheet-c78-743064.html

https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-desk-series/webex-desk-ds.html

https://assets.ctfassets.net/osq47g2esuw5/74GbQExgrlc1yELb11SOdG/6f86ffcb1cb1bc29e8e54c2f6fb048ea/CM-3239_-_Webex_Mini_Datasheet.pdf

https://www.webex.com/content/dam/wbx/us/data-sheet/desk_hub_datasheet_cm-1560.pdf

Webex Desk Series 管理者ガイド

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

Webex Desk Series ユーザーガイド

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

Webex Desk Series クイックリファレンスガイド

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

Webex Desk Series リリースノート

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

Webex Desk Series ソフトウェア

https://software.cisco.com/download/home/284711383

Cisco Unified Communications Manager

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/series.html

Cisco Voice ソフトウェア

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

Cisco IP Phone サービス アプリケーション開発ノート

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html

Real-Time Traffic over Wireless LAN

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-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_jp/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