Cisco Desk Phone 9800 シリーズワイヤレス LAN 展開ガイド

9861　　9871

Cisco は、モダンオフィス環境での作業のために構築されたポートフォリオにより、デスクフォンに新しい標準をもたらします。 デスクフォン 9800 シリーズは、IT とファシリティを考慮して設計され、4 つの新しい電話機のモデルを提供します。 各電話には、ユーザーエクスペリエンスを簡素化し、ビデオポートフォリオ RoomOS デバイスを補完する新しくリリースされた PhoneOS ソフトウェアが含まれており、デスクスペースから会議室までシームレスなエクスペリエンスを提供します。 拡張された機能により、9800 シリーズは安全なエンタープライズ通話、ミーティング、デスク予約、持続可能性、緊急アラート、通話のすべてを 1 つのデバイスに統合します。 機能ごとに専用のデバイスを購入する必要はありません。すべての機能が各電話に組み込まれています。

デスクフォン 9800 シリーズは、複雑な購入、展開、管理、トレーニングを軽減します。 さらに簡素化するために、1 つのデバイスを Cisco Unified Communications Manager（CUCM）、Webex Calling、Broadworks またはその他のサードパーティのクラウド通話プラットフォームに使用できます。 シスコの卓上デバイスの幅広いポートフォリオと並んで、9800 シリーズは、ハイブリッドワーク、通話、ミーティングの間のギャップを埋めることでワークプレースを変革するのに役立つ、市場で独自の地位を確立しており、大規模なワークステーションにとって最も費用対効果の高いソリューションです。

このガイドは、ネットワーク管理者が 9800 シリーズをワイヤレス LAN 環境に展開するのに役立つ情報とガイダンスを提供します。

改訂履歴

日付（Date）	コメント
07/12/24	初期バージョン

目次

Cisco Desk Phone 9800 シリーズの概要

Cisco の 802.11 実装により、通話や音声などの時間的制約のあるアプリケーションが、ワイヤレス LAN（WLAN）デプロイでキャンパス全体にわたって効率的に動作することができます。 これらの拡張機能は、エンド ユーザがアクセス ポイント間をローミングする際のセキュリティを維持しながら、高速ローミング機能とマルチメディア トラフィックのほぼシームレスなフローを提供します。
WLAN は未認可の周波数帯を使用するため、未認可の周波数帯を使用する他のデバイスからの干渉が発生する場合があります。 Bluetooth ヘッドセット、電子レンジ、コードレス電話など、2.4 GHz 帯域を使用するデバイスの急増により、2.4 GHz 帯域が他の帯域よりも輻輳している可能性があります。 5 GHz 帯域では、この帯域で動作するデバイスがはるかに少なく、802.11a/n データレートを最大限に活用するために、Cisco Desk Phone 9800 シリーズを運用するための優先帯域です。

Cisco Desk Phone シリーズで Cisco が最適化を実行しても、未認可の帯域を使用しているため、中断のない通信は保証できず、会話中に数秒間の音声ギャップが生じる可能性があります。 これらの導入ガイドラインに従うことで、音声ギャップが発生する可能性を減らすことができますが、この可能性は常にあります。

未認可の周波数帯を使用し、WLAN デバイスへのメッセージの配信を保証できないため、Cisco Desk Phone 9800 シリーズ は医療機器としての使用を意図したものではなく、医療に関する意思決定を行うことはできません。

モデル

次の表は、WLAN 機能で利用できる電話モデルを示しています。

以下は、各モデルでサポートされているピーク アンテナ ゲインと周波数範囲/チャネルの概要です。

部品番号	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
DP-9871-K9= DP-9871-L-K9= DP-9871-K9++= DP-9871-K9--=	Cisco デスクフォン 9871	2.400-2.483GHz: 3.22dBi 5.150-5.250GHz: 3.60dBi 5.250-5.350GHz: 3.62 dBi 5.470-5.725GHz: 4.23 dBi 5.725-5.850GHz: 4.13 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-144 149,153,157,161,165
DP-9861-K9= DP-9861-L-K9= DP-9861-K9++= DP-9861-K9--=	Cisco デスクフォン 9861	2.400-2.483GHz: 3.06 dBi 5.150-5.250GHz: 3.98dBi 5.250-5.350GHz: 4.07dBi 5.470-5.725GHz: 4.11dBi 5.725-5.850GHz: 3.76dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-144 149,153,157,161,165

要件

Cisco Desk Phone 9800 シリーズのユニットは、音声およびデータ通信を提供する IEEE 802.11a/b/g/n/ac 協働デバイスです。 ワイヤレス LAN が Cisco Desk Phone シリーズの展開要件を満たしていることを確認する必要があります。

サイト要件

Cisco Desk Phone 9800 シリーズを本番環境にデプロイする前に、高度なワイヤレス LAN 専門知識を持つ Cisco 認定パートナーによってサイト調査を完了する必要があります。 サイト調査中に、RF スペクトルを分析して、目的の帯域（5GHz または 2.4GHz）で使用可能なチャネルを判別することができます。 通常、5GHz 帯域では干渉が少なく、非オーバーラップ チャネルが多いため、5GHz は動作のための優先帯域であり、Cisco Desk Phone 9800 シリーズ ユニットがミッション クリティカルな環境で使用される場合には、さらに強く推奨されます。 サイト調査には、その場所で想定されるカバレッジ プランを示すヒートマップが含まれます。 サイト調査では、そのロケーション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 ポイント構成 (チャネルと送信電力) も決定します。 非堅牢な環境 (オフィス、医療、教育、ホスピタリティなど) では統合型アンテナを選択し、堅牢な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 (製造、倉庫、小売店など) を選択することをお勧めします。
ワイヤレス LAN が Cisco Desk Phone 9800 シリーズの展開要件を満たしていることを確認する必要があります。

シグナル

セルの端は、その信号レベルで隣接するアクセスポイントの 20 30% のオーバーラップがある場所で、-67 dBm に設計する必要があります。

これにより、Cisco Desk Phone 9800 シリーズには常に適切な信号があり、信号ベースのトリガーとパケット損失トリガーを比較した場合に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、電話からのアップストリーム信号が、送信データ レートに対するアクセス ポイントの受信感度を満たす必要があります。 経験則として、アクセスポイントでの受信信号が -67 dBm 以上であることを確認します。

電話が少なくとも 5 秒間信号を保持できるように、セル サイズを設計することをお勧めします。

チャネル使用率

チャネル使用率レベルを 40% 未満に維持する必要があります。

ノイズ

ノイズレベルは -92 dBm を超えてはならず、これにより -67 dBm 信号が維持される場合の SN 比（SNR）が 25 dB になります。

また、Cisco Desk Phone 9800 シリーズからのアップストリーム信号が、アクセスポイントの送信データレートの SNR を満たすことも必要です。

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% を超えてはいけません。 そうしないと、音声品質が著しく低下する可能性があります。

ジッターは最小限 (< 100 ms) に維持する必要があります。

再試行

802.11 の再送信は 20% 未満でなければなりません。

マルチパス

ヌルが作成され信号レベルが低下する可能性があるため、マルチパスは最小限に抑える必要があります。

コール制御

Cisco Desk Phone 9800 シリーズは、次のコール制御プラットフォームに対応しています。

- Cisco Webex Calling
- Cisco Unified Communications Manager (CUCM) (12.5 以降)
- Webex 専用インスタンス (DI)
- Cisco BroadWorks

メモ: Cisco Desk Phone 9800 シリーズデバイスのサポートを有効にするには、Cisco Unified Communications Manager でデバイスパッケージをインストールするか、サービスリリースを更新する必要があります。

Cisco Desk Phone 9800 シリーズのデバイス パッケージは、次の場所で入手できます。

https://software.cisco.com/download/home/286322286/type/282074299/release/12.5(1.19210)

https://software.cisco.com/download/home/286328117/type/282074299/release/14.0(1.14056)

https://software.cisco.com/download/home/286331940/type/282074299/release/15.0(1.12004)

ワイヤレス LAN

Cisco Desk Phone 9800 シリーズは、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
    - 最小値 = 8.10.185.0
    - 推奨値 = 8.10.190.0, 8.10.196.0
- Cisco IOS Wireless LAN コントローラおよび Cisco 中央管理型アクセスポイント
    - 最小値 = 17.3.5
    - 推奨 = 17.9.5、17.6.6、17.12.1
- Cisco Mobility Expres sおよび Cisco 中央管理型アクセスポイント

    - 最小値 = 8.10.105.0
    - 推奨値 = 8.10.105.0, 8.10.130.0, 8.10.142.0, 8.10.196.0

- Cisco Autonomous（自律）アクセス ポイント
    - 最小値 = 15.3(3)JPK2
    - 推奨値 = 15.3(3)JPK2, 15.3(3)JPK3, 15.3(3)JPK4, 15.3(3)JPK6
- Cisco Meraki アクセス ポイント
    - 最小値 = MR 27.X, MX 13.33
    - 推奨値 = MR 30.6, MX 18.211.2

アクセスポイント

サポートされている Cisco アクセスポイントについては、次の表を参照してください。

コントローラー モデル	AP モデル
AireOS	1700, 1810, 1810W, 1815, 1830, 1840, 1850, 2700, 2800, 3700, 3800, 4800, 9105, 9115, 9117, 9120, 9130
IOS XE	1700, 1810, 1810W, 1815, 1830, 1840, 1850, 2700, 2800, 3700, 3800, 4800, 9105, 9115, 9117, 9120, 9130, 9136, 9162, 9164, 9166
Mobility Express	1815 (1815t ではない)、1830、1840、1850、2800、3800、4800
自律型	1700, 2700, 3700
Meraki	9162, 9164, 9166, MR20, MR28, MR30H, MR32, MR33, MR34, MR36, MR36H, MR42, MR44, MR45, MR46, MR52, MR53, MR55, MR56, MR57, MX64W, MX65W, MX67W, MX68W, Z3

アンテナシステム

一部の Cisco アクセスポイントでは、外部アンテナが必要または許可されます。

Cisco Aironet アクセスポイントの対応アンテナおよび外部アンテナの取付方法については、以下の URL を参照してください。

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennasaccessories/product_data_sheet09186a008008883b.html

メモ: 統合型内部アンテナ付きの Cisco アクセスポイント（壁に取り付けることを想定しているモデル以外）には、全方向性のアンテナがあるので、壁に取り付けること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（Protocols）

サポートされているワイヤレス LAN プロトコルには以下が含まれます。

- 802.11a,b,d,e,g,h,i,n,ac
- Wi-Fi マルチメディア（WMM）
- Session Initiation Protocol （SIP）
- リアルタイム プロトコル (RTP)
- Opus、G.722、G.711、G.722.1、G.729
- Dynamic Host Configuration Protocol（DHCP）
- Trivial File Transfer Protocol（TFTP）
- ハイパーテキスト転送プロトコル (HTTP)

Wi-Fi

Cisco Desk Phone 9800 シリーズは 2.4GHz (HT20) または 5GHz (HT20/HT40/VHT20/VHT40/VHT80) モードで動作します。 802.11n/ac 接続を実現するには、Cisco Desk Phone 9800 シリーズをアクセス ポイントから 30 フィート以内にすることを推奨します。

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 電力=18 dBm	6 Mbps	1	OFDM-BPSK
(地域による)	9 Mbps	1	OFDM-BPSK
	12 Mbps	1	OFDM-QPSK
	18 Mbps	1	OFDM-QPSK
	24 Mbps	1	OFDM-16QAM
	36 Mbps	1	OFDM-16QAM
	48 Mbps	1	OFDM-64QAM
	54 Mbps	1	OFDM-64QAM
5 GHz-802.11n (HT20)	**データレート**	**空間ストリーム**	**変調**
最大 Tx 電力=18 dBm	7 Mbps (MCS 0)	1	OFDM-BPSK
(地域による)	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK

	29 Mbps (MCS 3)	1	OFDM-16QAM
	43 Mbps (MCS 4)	1	OFDM-16QAM
	58 Mbps (MCS 5)	1	OFDM-64QAM
	65 Mbps (MCS 6)	1	OFDM-64QAM
	72 Mbps (MCS 7)	1	OFDM-64QAM
5 GHz-802.11n (HT40)	**データレート**	**空間ストリーム**	**変調**
最大 Tx 電力=17 dBm	15 Mbps (MCS 0)	1	OFDM-BPSK
(地域による)	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-16QAM
	90 Mbps (MCS 4)	1	OFDM-16QAM
	120 Mbps (MCS 5)	1	OFDM-64QAM
	135 Mbps (MCS 6)	1	OFDM-64QAM
	150 Mbps (MCS 7)	1	OFDM-64QAM
5 GHz-802.11ac (VHT20)	**データレート**	**空間ストリーム**	**変調**
最大 Tx 電力=18 dBm	7 Mbps (MCS 0)	1	OFDM-BPSK
(地域による)	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK
	29 Mbps (MCS 3)	1	OFDM-16QAM
	43 Mbps (MCS 4)	1	OFDM-16QAM
	58 Mbps (MCS 5)	1	OFDM-64QAM
	65 Mbps (MCS 6)	1	OFDM-64QAM
	72 Mbps (MCS 7)	1	OFDM-64QAM
	87 Mbps (MCS 8)	1	OFDM-256QAM
5 GHz-802.11ac (VHT40)	**データレート**	**空間ストリーム**	**変調**
最大 Tx 電力=17 dBm	15 Mbps (MCS 0)	1	OFDM-BPSK
(地域による)	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-16QAM

	90 Mbps (MCS 4)	1	OFDM-16QAM
	120 Mbps (MCS 5)	1	OFDM-64QAM
	135 Mbps (MCS 6)	1	OFDM-64QAM
	150 Mbps (MCS 7)	1	OFDM-64QAM
	180 Mbps (MCS 8)	1	OFDM-256QAM
	200 Mbps (MCS 9)	1	OFDM-256QAM
5 GHz-802.11ac (VHT80)	**データレート**	**空間ストリーム**	**変調**
最大 Tx 電力=15 dBm	33 Mbps (MCS 0)	1	OFDM-BPSK
(地域による)	65 Mbps (MCS 1)	1	OFDM-QPSK
	98 Mbps（MCS 2)	1	OFDM-QPSK
	130 Mbps (MCS 3)	1	OFDM-16QAM
	195 Mbps (MCS 4)	1	OFDM-16QAM
	260 Mbps (MCS 5)	1	OFDM-64QAM
	293 Mbps (MCS 6)	1	OFDM-64QAM
	325 Mbps (MCS 7)	1	OFDM-64QAM
	390 Mbps (MCS 8)	1	OFDM-256QAM
	433 Mbps (MCS 9)	1	OFDM-256QAM

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 電力=18 dBm	1 Mbps	1	DSSS-BPSK
(地域による)	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 電力=18 dBm	6 Mbps	1	OFDM-BPSK
(地域による)	9 Mbps	1	OFDM-BPSK
	12 Mbps	1	OFDM-QPSK

	18 Mbps	1	OFDM-QPSK
	24 Mbps	1	OFDM-16QAM
	36 Mbps	1	OFDM-16QAM
	48 Mbps	1	OFDM-64QAM
	54 Mbps	1	OFDM-64QAM
2.4 GHz - 802.11n (HT20)	**データレート**	**空間ストリーム**	**変調**
最大 Tx 電力=16 dBm	7 Mbps	1	OFDM-BPSK
(地域による)	14 Mbps	1	OFDM-BPSK
	21 Mbps	1	OFDM-QPSK
	29 Mbps	1	OFDM-QPSK
	43 Mbps	1	OFDM-16QAM
	58 Mbps	1	OFDM-16QAM
	65 Mbps	1	OFDM-64QAM
	72 Mbps	1	OFDM-64QAM

メモ: 送信電力にはアンテナゲインが含まれます。

規制

ワールド モード (802.11d) では、クライアントを異なる地域で使用できます。クライアントは、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たチャネルと送信電力の使用に適応できます。

Cisco Desk Phone 9800 シリーズは、地域ごとに使用するチャネルと送信電力を決定できる 802.11d が有効になっているアクセスポイントで最適に動作します。

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

一部の 5 GHz チャネルはレーダ技術でも使用されます。このため、802.11 クライアントとアクセス ポイントは、これらのレーダ周波数 (DFS チャネル) を利用するために 802.11h に準拠している必要があります。 802.11 h では 802.11d を有効にする必要があります。

Cisco Desk Phone 9800 シリーズは、これらのチャネルのアクティブ スキャンを行う前に、まず DFS チャネルをパッシブにスキャンします。

802.11d が有効になっていない場合、Cisco Desk Phone 9800 シリーズは下げられた送信電力を使ってアクセスポイントへの接続を試みます。

Cisco Desk Phone 9800 シリーズは、WFA の定義に従う国コードをサポートしています。

Bluetooth®

Cisco Desk Phone 9800 シリーズは Bluetooth® 技術をサポートし、ワイヤレスヘッドセット通信を可能にします。
Bluetooth は、30 フィートの範囲内で低帯域幅のワイヤレス接続を可能にします。 ただし、 を保持することが推奨されます。Cisco Desk Phone 9800 シリーズから 10 フィート以内の Bluetooth デバイス。
Bluetooth デバイスは、電話機から直接見える範囲内にある必要はありませんが、壁やドアなどの障害物がある場合でも、品質に影響を与える可能性があります。
Bluetooth は、802.11b/g/n および他のさまざまなデバイス (例えば、電子レンジ、コードレス電話など) と同様に、2.4 GHz の周波数で動作します。 そのため、Bluetooth の品質は、このライセンスされていない周波数を使用する他のデバイスからの潜在的な干渉の影響を受ける可能性があります。

Bluetooth プロファイル（Bluetooth Profiles）

Cisco Desk Phone 9800 シリーズは、以下の Bluetooth プロファイルをサポートしています。

- 高度音声配信プロファイル (A2DP)
- 音声/ビデオ リモート コントロール プロファイル (AVRCP)
- 汎用アクセス プロファイル (GAP)
- 汎用音声/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)

802.11b/g/n と Bluetooth が同時に使用される共存を使用する場合、両方とも 2.4 GHz の周波数範囲を利用するため、以下の制限と展開要件を考慮することが重要です。

容量

共存 (802.11b/g/n + Bluetooth) を使用する場合、802.11g/n および Bluetooth 伝送を保護するための CTS の利用により、コール容量が減少します。

マルチキャスト音声

共存を使用している場合、プッシュツートーク (PTT)、保留音 (MMOH)、および他のアプリケーションからのマルチキャスト音声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、共存を使用しているときに、Bluetooth 伝送を保護するために CTS が送信される場合があります。

一部の環境では、6 Mbps を有効にする場合があります。

メモ: Bluetooth を使用する場合は 802.11a/n/ac を使用することをお勧めします。これは、802.11b/g/n と Bluetooth の両方が 2.4 GHz の周波数を使用するためだけでなく、上記の制限によるものでもあります。

端末のケア

Cisco Desk Phone 9800 シリーズの汚れを落とす場合は、柔らかく湿った布で拭いてください。
デバイスに損傷を与える可能性があるため、デバイスに液体や粉末を直接かけないでください。
端末の掃除に、ブリーチやかせい性製品を使用しないでください。
デバイスの破損の原因となるため、デバイスの掃除に圧縮空気を使用しないでください。
詳細については、『Cisco Desk Phone 9800 Series User Guide』を次の場所で参照してください。 https://cisco.com/go/dp9800help

ワイヤレス LAN の設計

Cisco Desk Phone 9800 シリーズで適切なカバレッジ、コール キャパシティ、シームレスなローミングを確保するには、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

以下のガイドラインを使用して、これらのワイヤレス環境のチャネルの使用を計画します。

5 GHz (802.11a/n/ac)

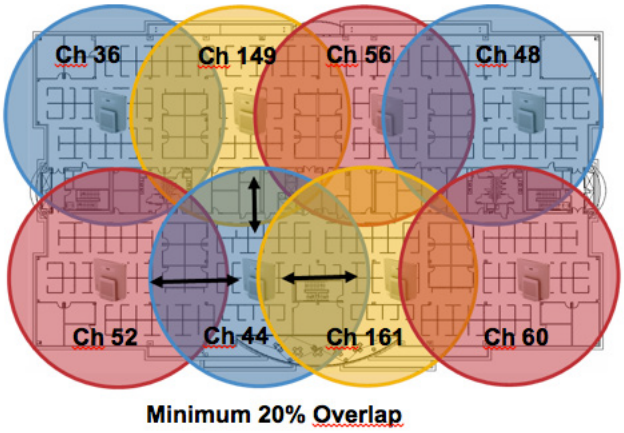
5 GHz は Cisco Desk Phone 9800 シリーズの動作で推奨される周波数帯です。
一般的に、アクセスポイントは手動でチャネルを割り当てるのではなく、チャネルの自動選択を使用することが推奨されます。
断続的な干渉がある場合、そのエリアにサービスを提供するアクセスポイントに、チャネルを静的に割り当てることが必要になる場合があります。
Cisco Desk Phone 9800 シリーズは、802.11h に準拠した Dynamic Frequency Selection（DFS）と Transmit Power Control（TPC）をサポートしています。これは、5.260 - 5.720 GHz で動作するチャネルに必要で、25 個の可能なチャネルのうち 16 個を網羅します。
802.11a/n/ac 環境でシームレスなローミングを確保するには、隣接するチャネルと少なくとも 20% オーバーラップすることが重要です。 重要なエリアでは、オーバーラップを 30% 以上に増やして、-67 dBm 以上の信号で利用できる少なくとも 2 つのアクセス ポイントを確保することをお勧めします。 さらに、Cisco Desk Phone 9800 シリーズはアクセス 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) に準拠しています。

動的周波数選択 (DFS)

DFS は、レーダー信号が検出されるたびに、送信機に別のチャネルに切り替えるように動的に指示します。 アクセス ポイントがレーダーを検出すると、アクセス ポイントの無線は少なくとも 60 秒間一時停止し、その間、アクセス ポイントは別の使用可能なチャネルをパッシブにスキャンします。
TPC により、クライアントとアクセスポイントは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、指定されたデータ レートでアクセス ポイントとの関連付けを維持するのに十分なエネルギーのみを使用します。 結果として、クライアントが隣接セル干渉に与える影響が少なくなり、より密に展開された高性能ワイヤレス LAN が可能になります。
アクセス ポイントが繰り返されるレーダ イベントを検出すると、真偽の警告かどうかにかかわらず、アクセス ポイントはまず、レーダ信号が単一のチャネル (狭帯域) または複数のチャネル (広帯域) に影響を与えるかどうかを判断します。 次に、アクセス ポイントは、ワイヤレス LAN の影響を受けるチャネルを無効にする可能性があります。
非 DFS チャネルで動作するアクセスポイントがあると、音声の中断を最小限に抑えることができます。

レーダー アクティビティの場合、非 DFS チャネル (UNII-1) を使用するエリアごとに少なくとも 1 つのアクセス ポイントを持つことをお勧めします。 これにより、アクセス ポイントの無線がホールドオフ期間中に、新しい使用可能なチャネルをスキャンするときに、チャネルが使用可能な状態を維持できます。
UNII-3 チャネル (5.745 - 5.825 GHz) は、可能な場合はオプションで使用できます。

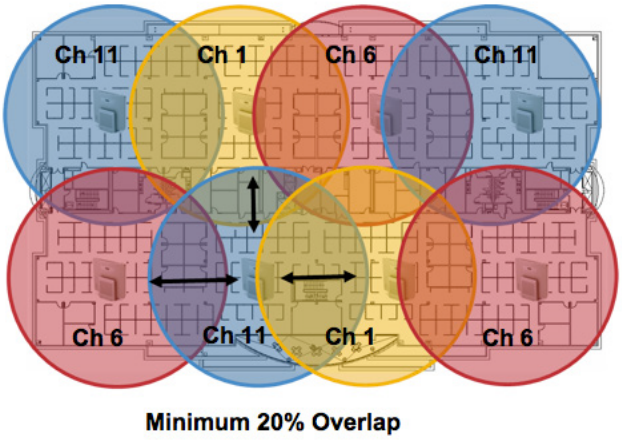
5 GHz では、25 チャネルが南北アメリカ、16 チャネルがヨーロッパ、19 チャネルが日本で利用できます。
UNII-3 が利用できる場所では、UNII-1、UNII-2、UNII-3 だけを使って 12 チャネルセットを利用することが推奨されます。
UNII-2 拡張チャンネル (チャンネル 100 - 144) の使用を計画している場合、アクセス ポイントで UNII-2 (チャンネル 52-64) を無効にして、多数のチャンネルを有効にすることを推奨します。
ワイヤレス LAN で多くの 5 GHz チャネルが有効になっていると、新しいアクセスポイントの検出に遅延が発生します。
5 GHz ワイヤレス LAN 展開の例を次に示します。



2.4 GHz (802.11b/g/n)

一般に、アクセスポイントは手動でチャネルをアクセスポイントに指定するのではなく、自動チャネル選択を利用することを推奨します。
断続的な干渉がある場合、そのエリアにサービスを提供するアクセス ポイントには、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 を展開するときに、非重複チャネルのみを利用する必要があります。 非重複チャネルには 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 の周波数範囲で重複しないチャネルは 3 つだけです (チャネル 1、6、11)。
シームレスなローミングを可能にする 802.11b/g/n 環境で Cisco Desk Phone 9800 シリーズを展開する場合、非重複チャネルを使用し、隣接するチャネルと少なくとも 20% 重複する必要があります。
1、5、9、13 などの重複するチャネルセットの使用は、サポートされている構成ではありません。

2.4 GHz ワイヤレス LAN 展開の例を次に示します。



信号強度とカバレッジ

許容できる音声品質を確保するために、Cisco Desk Phone 9800 シリーズは、5GHz または 2.4 GHz を使用する場合、常に -67 dBm 以上の保持する必要があります。一方、Cisco Desk Phone 9800 シリーズは、伝送データレートのために必要なアクセスポイントの受信感度の信号レベルも満たしている必要があります。

パケット エラー率 (PER) が 1% 以下であることを確認します。

最小の SN 比（SNR）25 dB = -67 dBm 信号の -92 dBm ノイズレベルを維持する必要があります。

冗長性を提供するために、25 dB SNR で少なくとも -67 dBm の信号を持つ重複しないチャネルに少なくとも 2 つのアクセス ポイントを配置することをお勧めします。

最大のキャパシティとスループットを達成するには、ワイヤレス LAN の設計は 24 Mbps にするべきです。 より高いデータレートは、これらのより高いデータレートを利用できる音声専用以外のアプリケーションに対して、オプションで有効にすることができます。

最小データレートを、2.4 GHz では 11 Mbps または 12 Mbps（802.11b クライアント サポート ポリシーによる）、5 GHz では 12 Mbps に設定することが推奨されます。これは、必須/基本レートとして設定されるべき唯一のレートでもあります。

一部の環境では、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。

上記の要件により、単一チャネルプランは展開すべきではありません。

アクセスポイントの配置を設計する場合、すべての重要なエリアに適切なカバレッジ (信号) があることを確認してください。

データ専用アプリケーション向けの一般的なワイヤレス LAN 展開では、エレベータ、階段、外の回廊など、VoW LAN サービスが必要な一部のエリアをカバーできません。

電子レンジ、2.4 GHz コードレス電話、Bluetooth デバイス、または 2.4 GHz 帯域で動作するその他の電子機器は、ワイヤレス LAN に干渉を与える場合があります。

電子レンジは 802.11b/g/n のチャンネル 8 と 9 の間、つまり 2450 MHz で動作します。 一部のマイクロ波は他のものよりも強力にシールドされており、エネルギーの広がりを減らします。 マイクロ波の放出はチャネル 11 に影響を与える可能性がありますが、一部のマイクロ波は 2.4 GHz 周波数範囲全体（チャネル 1 から 11）に影響を与える可能性があります。 電子レンジの近くでアクセスポイントを使用する場合は、電子レンジの干渉を避けるため、チャンネル 1 を選択してください。

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 の周波数に同じ影響を与えません。 802.11a/n/ac テクノロジーは、より多くの非重複チャネルを提供し、通常、初期の RF 使用率を下げます。
音声展開の場合、音声には 802.11a/n/ac、データには 802.11b/g/n を使用することを推奨します。
しかし、ライセンスのない 5 GHz の周波数を使用する製品もあります (例: 5.8 GHz コードレス電話。これは UNII-3 チャンネルに影響を与える可能性があります)。

データ レート

最良の結果を得るために、容量と範囲が考慮された場合、5 GHz デプロイに対して 12 Mbps 以下のレートおよび 2.4 GHz デプロイに対して 12 Mbps 以下のレートは無効にすることが推奨されます。
Cisco Desk Phone 9800 シリーズは、シングル アンテナ付き 1x1 であるため、802.11n で最大 MCS 7 データ レート (最大 72 Mbps) をサポートします。 802.11ac の場合、Cisco Desk Phone 9800 シリーズは最大 VHT80 MCS 9 1SS (最大 433 Mbps) をサポートします。
802.11b クライアントがワイヤレスネットワークで許可されていない場合、12 Mbps 以下のデータレートを無効にすることを強く推奨します。 これにより、802.11b クライアントがこれらの OFDM フレームを検出できないため、802.11g/n 保護のための CTS フレームを送信する必要がなくなります。
802.11b クライアントがワイヤレスネットワークに存在する場合、802.11b レートが有効になっている必要があります。802.11b レートだけが必須/基本レートとして設定できます。
音声専用アプリケーションの場合、24 Mbps を超えるデータ レートはオプションで有効または無効にできます。
高い容量とスループットを維持するには、24 Mbps 以上のデータ レートを有効にする必要があります。
過度の再試行が懸念される環境にデプロイする場合、有効な最低のレートが必須/基本レートであるデータレートの限定されたセットを使用できます。
最大範囲を必要とする厳しい環境またはデプロイでは、6 Mbps を必須/基本レートとして有効にすることが推奨されます。
メモ: より低いレートが有効になると、容量とスループットが低下します。

厳しい環境

Cisco Desk Phone 9800 シリーズを厳しい環境 (例えば、製造、倉庫、小売) で展開する場合、標準的な設計推奨に加えて、追加の調整が必要になる場合があります。
以下は、厳しい環境でワイヤレス LAN を展開する際にフォーカスすべき主な項目です。

アクセスポイントとアンテナの選択

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お勧めします。 厳しい環境で適切に動作するように、アンテナタイプを選択することも重要です。

アクセスポイントの配置

Cisco Desk Phone 9800 シリーズとアクセス ポイントの間の障害物を最小限に抑え、アクセス ポイントのアンテナに対する見通し線を最大化することが重要です。 アクセスポイントおよび/またはアンテナが障害物の背後、または金属やガラスの表面またはその近くに取り付けられていないことを確認します。
統合型内部アンテナを備えたアクセス ポイントを一部のエリアで使用する場合、これらのアクセス ポイントは、全方向性アンテナを備え、壁に取り付けるように設計されていないため、シーリングに取り付けることを推奨します。

周波数帯域

いつも通り、5 GHz の使用が推奨されます。 2.4 GHz を使用すると、特に 802.11b レートが有効な場合に適切に動作しない場合があります。

5 GHz チャネル セットについては、8 または 12 チャネル プランのみを使用することをお勧めします。可能な場合は、UNII-2 拡張チャンネルを無効にしてください。

データ レート

マルチパスが高いレベルで存在する場合、標準の推奨データレートセットは適切に機能しない可能性があります。

そのため、このような環境ではより低いデータレート (例えば 6 Mbps) を有効にすることをお勧めします。音声のみで使用する場合、24 Mbps を超えるデータレートを無効にすることで、初回送信の成功率を高めることができます。 同じ帯域がデータ、ビデオ、またはその他のアプリケーションにも使用されている場合、高いデータ レートを有効にしておくことをお勧めします。

送信電力

厳しい環境ではマルチパスが上昇する可能性があるため、アクセス ポイントおよび Cisco Desk Phone 9800 シリーズの送信電力も制限する必要があります。 厳しい環境で 2.4 GHz の展開を計画している場合、これはより重要です。 自動送信電力を使用している場合、アクセスポイント送信電力は、特定の範囲（最大レベルと最小電源レベル）を使用して設定し、アクセスポイントを過度に強くまたは弱く送信（例: 5 GHz の最大値が 16 dBm、最小値が 11 dBm）するのを防ぎます。

高速ローミング

高速ローミングには 802.11r/Fast Transition (FT) を使用することを推奨します。 802.11r (FT) を有効にすると、ローミング時のハンドシェイクのフレーム数もわずか 2 フレームに減ります。 ローミング中のフレーム数を減らすと、ローミングが成功する可能性が高くなります。

802.1x 認証を使用する場合、推奨される EAPOL キー設定を使用することが重要です。

Quality of Service（QoS）

音声、ビデオ、通話制御フレームの WMM UP タグを正しく設定できるように、DSCP 値が有線ネットワーク全体で保存されていることを確認する必要があります。

マルチパス

マルチパスは、RF 信号が送信元から送信先まで複数のパスを取る場合に発生します。

一部の信号は目的地まで、また一部は障害物にぶつかってその後、目的地に向かいます。 その結果、信号の一部で遅延が発生し、目的地までにより長いパスを移動することで、信号のエネルギー損失が発生します。

異なる波形が組み合わされると、信号品質が低くなるため、歪みが発生し、受信機のデコード機能に影響を与えます。

マルチパスは、反射面 (例えば、金属、ガラスなど) がある環境に存在する可能性があります。 これらの表面にアクセスポイントを取り付けることは避けてください。

マルチパス効果のリストは以下のとおりです。

データ破損

マルチパスが深刻なため、受信側が送信された情報を検出できない場合に発生します。

信号の Null 化

反射波が主信号と正確に逆相で到達し、主信号を完全にキャンセルするときに発生します。

信号振幅の増加

反射波が主信号と同相で到達し、主信号に加わることで信号強度が増加するときに発生します。

信号振幅の減少

反射波が主信号とある程度ずれた状態で到達し、信号の強度が低下した場合に発生します。

直交周波数分割多重方式（OFDM）の使用 これは 802.11a/n/ac および 802.11g/n で使用され、高マルチパス環境で見られる問題を減らすのに役立ちます。

高マルチパス環境で 802.11b を使用している場合、これらのエリアでは低いデータレートを使用する必要があります（例、1 および 2 Mbps）。

アンテナダイバーシティの使用は、このような環境でも役立ちます。

セキュリティ

ワイヤレス LAN を展開する場合、セキュリティは不可欠です。 Cisco Desk Phone 9800 シリーズは、次のワイヤレス セキュリティ機能をサポートしています。

WLAN 認証

- WPA2 および WPA (802.1x 認証)
- WPA2-PSK および WPA-PSK (事前共有キー)
- WPA3-SAE（等価の同時認証）
- EAP-FAST (拡張認証プロトコル - セキュアなトンネリングによる柔軟な認証)
- EAP-TLS (拡張認証プロトコル - トランスポート層セキュリティ)
- PEAP (保護された拡張可能な認証プロトコル - 汎用トークン カード/ Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2)
- None

WLAN 暗号化

- AES (最低 128 ビット Advanced Encryption Standard)
- Temporal Key Integrity Protocol/Message Integrity Check（TKIP/MIC）

WPA3-エンタープライズ

- キーの導出と確認

  最小 256 ビットのセキュア ハッシュ アルゴリズム（HMAC-SHA256）によるハッシュメッセージ認証モード（HMAC)

- 堅牢な管理フレーム

  最小 128 ビットのブロードキャスト/マルチキャスト整合性プロトコル暗号ベースのメッセージ認証コード（BIP-CMAC-128）

  メモ: CCMP256、GCMP128 および GCMP256 暗号化はサポートされていません。

Cisco Desk Phone 9800 シリーズは、次の追加セキュリティ機能もサポートしています。

- イメージ認証（Image authentication）
- [デバイス認証（Device authentication）]
- ファイル認証（File authentication）
- シグナリング認証
- メディア暗号化 (SRTP)
- シグナル暗号化 (TLS)
- 認証局のプロキシ機能 (CAPF)
- 安全なプロファイル
- 暗号化された設定ファイル（Encrypted configuration files）

拡張認証プロトコル - セキュア トンネリングによるフレキシブル認証 (EAP-FAST)

拡張認証プロトコル - セキュアトンネリングによるフレキシブル認証（EAP-FAST）は、アクセスポイントと Cisco Identity Service エンジン（ISE）などのリモート認証ダイヤルイン ユーザー サービス（RADIUS）サーバー間の Transport Level Security（TLS）トンネル内の EAP トランザクションを暗号化します。
TLS トンネルは、クライアント (Cisco Desk Phone 9800 シリーズ) と RADIUS サーバ間の認証に Protected Access Credentials (PAC) を使用します。 サーバは権限 ID (AID) をクライアントに送信し、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。 サーバーは、プライマリキーで PAC を復号します。 両方のエンドポイントが PAC キーを持ち、TLS トンネルが作成されます。 EAP-FAST では、自動 PAC プロビジョニングがサポートされていますが、RADIUS サーバー上で有効にする必要があります。
EAP-FAST を有効にするには、証明書が RADIUS サーバにインストールされている必要があります。
Cisco Desk Phone 9800 シリーズは現在、PAC の自動プロビジョニングのみをサポートしています。 そのため、[**匿名インバンド PAC プロビジョニングを許可する**] を RADIUS サーバで有効にします。
[**匿名インバンド PAC プロビジョニングを許可する**] が有効な場合、EAP-GTC と EAP-MSCHAPv2 の両方が有効になっている必要があります。
EAP-FAST では、認証サーバ上にユーザアカウントが作成されている必要があります。
本番用のワイヤレス LAN 環境で匿名 PAC プロビジョニングが許可されない場合、ステージング RADIUS サーバを Cisco Desk Phone 9800 シリーズの最初の PAC プロビジョニング用にセットアップできます。
これには、ステージング RADIUS サーバーがセカンダリ EAP-FAST サーバーとしてセットアップされる必要があり、コンポーネントが製品のプライマリ EAP-FAST サーバーから複製されます。これにはユーザーとグループのデータベース、および EAP-FAST プライマリキーとポリシー情報が含まれます。

本番のプライマリ EAP-FAST RADIUS サーバーが、EAP-FAST プライマリキーとポリシーをステージングのセカンダリ EAP-FAST RADIUS サーバーに送信するようにセットアップされていることを確認します。これにより、Cisco Desk Phone 9800 シリーズは、**[匿名のインバンドPACプロビジョニングを許可する（Allow anonymous in-band PAC provisioning）]** が無効になっている本番環境で、プロビジョニングされた PAC を使用できます。PAC の更新時になると、認証済みインバンド PAC プロビジョニングが使用されます。 このため、[**認証済みインバンド PAC プロビジョニングを許可する**] が有効になっていることを確認してください。
Cisco Desk Phone 9800 シリーズが猶予期間中にネットワークに接続されていることを確認します。これにより、アクティブまたは廃止されたプライマリキーを使用して作成された既存の PAC を使用して新しい PAC を取得できます。
ステージングのワイヤレス LAN がステージングの RADIUS サーバーを指すようにすることだけが推奨され、ステージングのアクセスポイントが使用されていないときは無線を無効にすることが推奨されます。

拡張認証プロトコル - トランスポート層セキュリティ (EAP-TLS)

拡張認証プロトコル - トランスポート レイヤ セキュリティ（EAP-TLS）は、PKI で TLS プロトコルを使用してセキュリティを保護します。認証サーバへの通信。
TLS は、ユーザとサーバの両方の認証、および動的なセッションキー生成のため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 は優れたセキュリティを提供しますが、クライアント証明書管理が必要です。
EAP-TLS では、Cisco Desk Phone 9800 シリーズにインポートされた証明書の共通名と一致するユーザアカウントが認証サーバ上で作成されることも要求する場合があります。
このユーザーアカウントには複雑なパスワードを使用することをお勧めします。また、RADIUS サーバー上で有効にする EAP の種類は EAP-TLS のみです。

保護された拡張認証プロトコル (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。
その後の認証情報の交換は暗号化され、ユーザの資格情報は盗聴から安全です。
PEAP-GTC および 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が作成されている必要があります。

Quality of Service（QoS）

Quality of Service により、音声と通話トラフィックに高い優先順位を確保するためのキューイングができるようになります。
音声と通話制御トラフィックの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います。
- アクセスポイントで WMM が有効になっていることを確認します。
- 音声および通話制御トラフィックに優先順位を与える QoS ポリシーをアクセスポイントに作成します。

トラフィックタイプ	DSCP	802.1p	WMM UP	ポート範囲

音声	EF（46）	5	6	リモートピアとネゴシエートされた RTP/RTCP ポート。
コール制御（C Control）	CS3 (24)	3	4	管理者により設定された TCP/UDP ポート

- 音声および呼制御パケットに適切な QoS マーキングがあり、他のプロトコルが同じ QoS マーキングを使用していないことを確認してください。
- Cisco IOS スイッチで、Differentiated Services Code Point (DSCP) 保存を有効にします。

コール アドミッション制御（CAC）

Cisco Desk Phone 9800 シリーズは、音声ストリームの通話受付管理をサポートしていません。
アクセス ポイントの音声に対して TSPEC が有効になっている場合、音声フレームの優先順位が下げられます。

有線 QoS

必要なネットワーク デバイスの QoS 設定とポリシーを構成します。
WLAN デバイス用の Cisco スイッチ ポートの設定
Cisco ワイヤレス LAN コントローラと Cisco 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構成します。
Cisco IOS スイッチを利用する場合、以下のスイッチポート設定を使用します。

Cisco ワイヤレス LAN コントローラの COS トラストを有効にする

```
mls qos
!
インターフェイス X
mls qos trust cos
```

Cisco アクセスポイントの DSCP トラストを有効にする

```
mls qos
!
インターフェイス X
mls qos trust dscp
```

Cisco Meraki MS スイッチを利用する場合は、「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
メモ: Cisco Wireless LAN Controller を使用する際、DSCP トラストを実装するか、QoS マーク が正常に設定されていることを確実にするために、ワイヤレスパッケージがトラバースしているすべてのインターフェイスの Cisco Wireless LAN Controller（CAPWAP = UDP 5246 and 5247）が使用する UDP データポートを信頼する必要があります。
有線 IP 電話用の Cisco スイッチ ポートの設定
Cisco 有線 IP 電話のスイッチポートを Cisco 電話トラストに対して有効にします。
以下はスイッチ構成の例です。

```
mls qos
!
```

インターフェイス X
MLS qos trust デバイス cisco-phone
mls qos trust dscp

ローミング

Cisco Desk Phone 9800 シリーズは両方の周波数セットに対応します。これにより、Cisco Desk Phone 9800 シリーズは 5 GHz または 2.4GHz のいずれかに接続し、帯域間ローミングのサポートを有効にします。
802.11r (FT) なしの 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、WPA2、WPA3 は追加の一時キーを導入し、ローミング時間が長くなる可能性があります。
802.11r (FT) が利用されている場合、ローミング時間は 100 ms 未満に短縮され、1 つのアクセスポイントから別のアクセスポイントへの移行時間はユーザに聞こえないほどです。
Cisco Desk Phone 9800 シリーズは 802.11r (FT) をサポートしています。
認証ローミングタイムテーブル

認証	ローミング時間
WPA/WPA2/WPA3 パーソナル	150 ms
WPA2 エンタープライズ	300 ms
802.11r (FT)	< 100 ms

Cisco Desk Phone 9800 シリーズは、スキャンとローミング イベントを管理します。
ほとんどのローミング イベントのローミング トリガーは、現在の RSSI に基づいて必要な RSSI 差を満たす必要があります。 これにより、音声の中断のないシームレスなローミングが保証されます。

高速セキュア ローミング (FSR)

802.11r / 高速移行 (FT) は、頻繁なローミングが発生するすべての環境タイプで推奨される展開モデルです。
Cisco Centralized Key Management（CCKM）はサポートされていませんが、802.1x 認証が必要です。
802.11r (FT) は高速でセキュアなローミングを可能にし、ネットワークオフ時間を制限して通話中のギャップを最小限に抑えます。
802.11r (FT) なしの 802.1x または PSK、および FT なしの 802.1x では、完全な再認証の要件により、ローミング中に遅延が発生する可能性があります。 WPA、WPA2、WPA3 は追加の一時キーを導入し、ローミング時間が長くなる可能性があります。
802.11r (FT) はキー管理を一元化し、キー交換の回数を減らします。
802.11r (FT) が利用されている場合、ローミング時間が 400-500 ms から 100 ms 未満に短縮されます。この場合、アクセスポイント間の移行時間はユーザには聞こえません。
802.11r (FT) ローミングには 2 つの方法があります。

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

Over the Distribution

クライアントは現在のアクセスポイントを通じてターゲットのアクセスポイントと通信します。 クライアントとターゲットのアクセスポイント間の通信は、WLAN コントローラ経由のクライアントと現在のアクセスポイント間の FT アクションフレームで実行されます。

Over the Air 方式を利用する 802.11r (FT) は、展開に推奨される高速セキュア ローミング モデルです。

802.11r (FT) および Over the Distribution 方式では、現在関連付けられているアクセスポイントへの接続が必要です。この方法は、ローミングイベントが発生したときに現在のアクセスポイントと対象のアクセスポイントの両方への見通し線が保持できない非オープン環境ではうまく機能しない可能性があります。

Cisco Desk Phone 9800 シリーズは 802.11r (FT) with WPA2-PSK、WPA3-SAE または WPA2/WPA3 Enterprise をサポートします。

FSR タイプ	認証	Key Management	暗号化	PMF
802.11r (FT)	PSK	WPA-PSK WPA-PSK-SHA256 FT-PSK	AES	なし
802.11r (FT)	WPA3	SAE FT-SAE	AES	はい
802.11r (FT)	EAP-TLS	WPA-EAP FT-EAP	AES	なし
802.11r (FT)	EAP-TLS (WPA3)	WPA-EAP-SHA256 FT-EAP	AES	はい
802.11r (FT)	EAP-FAST	WPA-EAP FT-EAP	AES	なし
802.11r (FT)	EAP-FAST(WPA3)	WPA-EAP-SHA256 FT-EAP	AES	はい
802.11r (FT)	EAP-PEAP	WPA-EAP FT-EAP	AES	なし
802.11r (FT)	EAP-PEAP(WPA3)	WPA-EAP-SHA256 FT-EAP	AES	はい

メモ: 他の Wi-Fi 電話モデルが存在する環境に Cisco Desk Phone 9800 シリーズを展開するが、それらの Wi-Fi 電話モデルが 802.11r (FT) をサポートしていない場合、Cisco Desk Phone 9800 シリーズ用の同じ既存の SSID を使用できるはずですが、802.11r (FT) を使用していない間でも他の Wi-Fi 電話モデルが 802.11r (FT) 対応ネットワークで相互運用されることを想定し、他の既存のキー管理タイプ（例えば 802.1x）に加えて、Over the Air メソッドを使用する 802.11r (FT) を有効にすることが推奨されます。

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。これは TKIP がブロードキャスト/マルチキャスト暗号としてのみ使用できるためです。

帯域間ローミング

Cisco Desk Phone 9800 シリーズは両方の周波数セットに対応するため、帯域間ローミングが可能になり、現在最も強い信号が優先されます。 通常、これは 5 GHz より 2.4 GHz を優先します。電力レベルが同じであると想定すると、一般的に 2.4 GHz の方が信号が強いためです。

電源がオンになると、Cisco Desk Phone 9800 シリーズはすべての 2.4 および 5 GHz チャネルをスキャンし、構成されたネットワークのアクセスポイントが利用可能な場合に関連付けを試みます。

目的の帯域が帯域間で操作できることを確実にするため、スペクトル分析を実行することが推奨されます。

ローミング。

電源管理

Cisco Desk Phone 9800 シリーズでワイヤレス LAN モードを有効にするには電源が必要です。内部バッテリーがないためです。
イーサネットが Cisco Desk Phone 9800 シリーズに接続されている間は、ワイヤレス LAN は一時的に自動的に無効になります。しかし、以前にワイヤレス LAN が有効になっていた場合は、イーサネットが切断されると自動的に再度有効になります。
Cisco Desk Phone 9800 シリーズは、アイドル状態または通話中、主に高速スリープ モード (Wi-Fi の省電力なし) を使用します。
ヌル省電力 (PS-NULL) フレームは、オフチャネル スキャンに利用されます。

配信トラフィックインジケータメッセージ (DTIM)

DTIM 期間を 2 に設定し、100 ms のビーコン期間を設定することを推奨します。
Cisco Desk Phone 9800 シリーズはファストスリープモードを使用するため、DTIM 期間は、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を確認するためのウェークアップ期間をスケジュールするために使用されません。
ブロードキャストおよびマルチキャストトラフィックは、アクセスポイントに関連付けられた省電力対応のクライアントがある場合、DTIM 期間までキューに入れられるため、DTIM はこれらのパケットがクライアントに配信される速さを決定します。 マルチキャストアプリケーションを使用する場合、より短い DTIM 期間を使用することができます。
ワイヤレス LAN 上に複数のマルチキャストストリームが頻繁に存在する場合、DTIM 期間を 1 に設定することをお勧めします。

通話容量

希望するコール キャパシティに対応するようにネットワークを設計します。
Cisco アクセス ポイントは、24 Mbps 以上のデータ レートで、802.11a/n/ac および 802.11g/n の両方で最大 27 個の双方向音声ストリームをサポートできます。 この容量を達成するには、最小のワイヤレス LAN バックグラウンド トラフィックと初期の無線周波数 (RF) 使用率が必要です。
呼び出し数は、データ レート、初期チャネル使用率、および環境によって異なります。

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、パフォーマンスと容量を考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 期間までキューに入れられます。
Cisco Desk Phone 9800 シリーズは主にファストスリープ モードを使用しますが、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、すべてのマルチキャスト パケットは DTIM 期間までキューに入れられます。
マルチキャストでは、クライアントがパケットをタイムリーに受信するという保証はありません。
マルチキャストトラフィックは、アクセスポイントで有効になっている最高の必須/基本データレートで送信されるため、有効になっている最低のレートだけが、唯一必須/基本レートとして設定されていることを確認します。

クライアントは、そのマルチキャスト ストリームを受信するために、IGMP 参加要求を送信します。 セッションが終了されると、クライアントは IGMP リーブを送信します。

Cisco Desk Phone 9800 シリーズは、不要時にワイヤレス LAN 上のマルチキャストトラフィックの量を減らすために使用できる IGMP クエリ機能をサポートしています。

IGMP スヌーピングがすべてのスイッチで有効になっていることを確認します。

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

Cisco ワイヤレス LAN を設定する

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 AireOS ワイヤレス LAN コントローラおよび Lightweight アクセス ポイントを設定する場合、以下のガイドラインを使用してください。

- **802.11r (FT)** を有効にします
- **CCKM** は無効になっています
- **[Quality of Service（QoS）]** を [プレミアム（Platinum）] に設定します
- **[WMMポリシー（WMM Policy）]**を [必須（Required）] に設定します
- **セッション タイムアウト** が有効になっており、正しく設定されていることを確認します
- **ブロードキャスト キー間隔** が有効になっており、正しく設定されていることを確認します
- **Aironet IE** が無効になっていることを確認します
- **[P2P（ピアツーピア）ブロックアクション（P2P (Peer to Peer) Blocking Action）]** を無効にします
- **[クライアント除外（Client Exclusion）]** 正しく設定されていることを確認します
- **[DHCPアドレスの割り当てが必要（DHCP Address Assignment Required）]** を無効にします
- **[保護管理フレーム（PMF）（Protected Management Frame (PMF)）]** を [任意（Optional）] または [WPA3に必要（Required for WPA3）] に設定します
- **[MFPクライアントと保護（MFP Client Protection）]**を [任意（Optional）] または [WPA3に必要（Required for WPA3）] に設定します
- **DTIM 期間** を 2 に設定します
- **クライアント負荷分散** を無効に設定します
- **[クライアント帯域選択（Client Band Select）]** [無効（Disabled）] に設定します
- **IGMP スヌーピング** を有効に設定します
- Layer 3 モビリティが使用されている場合は、**[対称モバイルトンネリングモード（Symmetric Mobile Tunneling Mode）]** を有効にします
- 必要に応じて **データレート** を設定します
- 必要に応じて、**[自動RF（Auto RF）]** を設定します
- EDCA プロファイルを [音声に最適化] または [音声とビデオに最適化] に設定します。
- **[低遅延MACを有効化（Enable Low Latency MAC）]** を [無効（Disabled）] に設定します
- **[電力制限（Power Constraint）]** が [無効（Disabled）] になっているかを確認します
- **[チャネルアナウンス（Channel Announcement）]** と [チャネルサイレントモード（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** を設定します
- **フレーム集約** 設定を行います
- **CleanAir** を有効にする (CleanAir テクノロジーで Cisco アクセスポイントを利用する場合)
- 必要に応じて **マルチキャストダイレクト機能** を設定します
- **[802.1pタグ（802.1p tag）]** を [プレミアムQoSプロファイル（Platinum QoS profile）] に対して 5 に設定します

802.11 ネットワーク設定

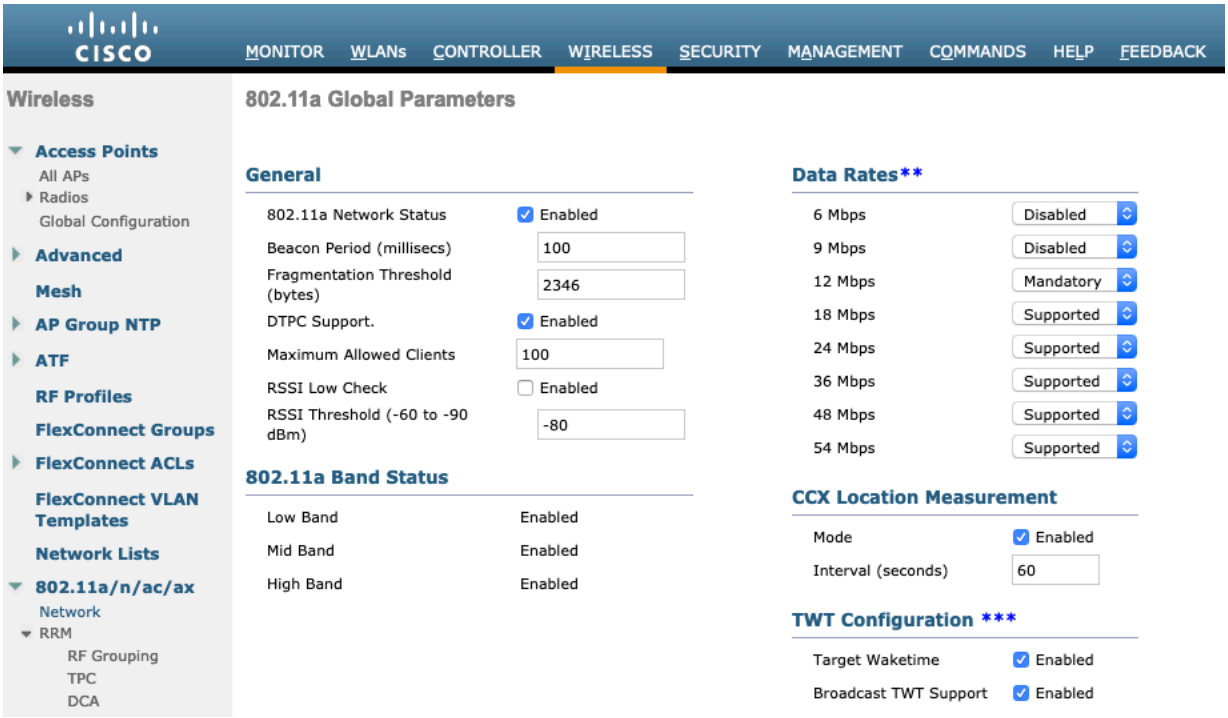
Cisco Desk Phone 9800 シリーズは 5 GHz 帯のみで使用することをおすすめします。 利用できるチャンネル数が多く、2.4 GHz 帯に比べて干渉が少ないためです。

5 GHz の周波数を使用するには、[802.11a/n/ac ネットワーク状況] が [**有効] になっていることを確認してください。**

[ビーコン期間（Beacon Period）] を **[100 ms]** に設定します。

[最大クライアント数（Maximum Allowed Clients）] は必要に応じて設定します。

必須 (基本) レートとして 12 Mbps を設定し、サポートされている (オプション) レートとして 18 Mbps 以上を設定することをお勧めします。 ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。



2.4 GHz を使用するには、802.11b/g/n ネットワークステータスと 802.11g が、**[有効（Enabled）]** であることを確認します。

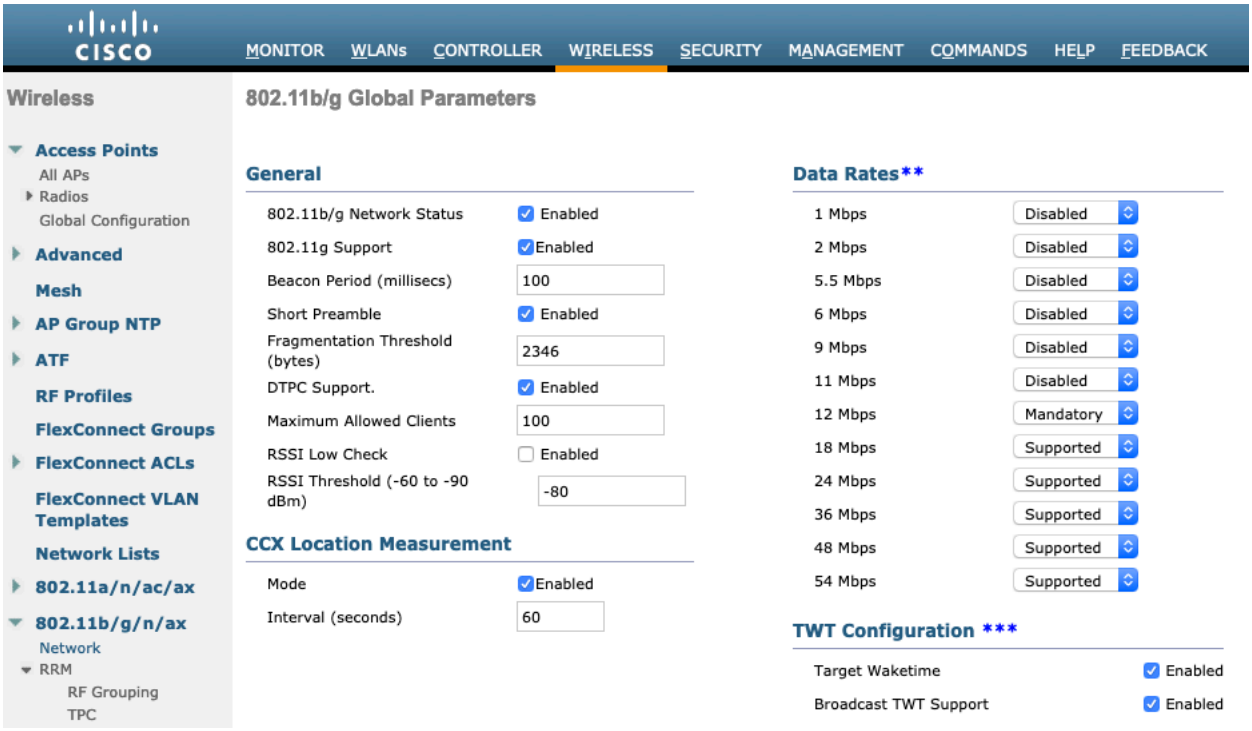
[ビーコン期間（Beacon Period）] を **[100 ms]** に設定します。

ワイヤレス LAN で、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存在しない場合、アクセスポイントで設定された 2.4 GHz 無線構成で、**[ショートプリアンブル（Short Preamble）]** を **[有効（Enabled）]** にします。 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で、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。

最大クライアント数 は必要に応じて設定します。

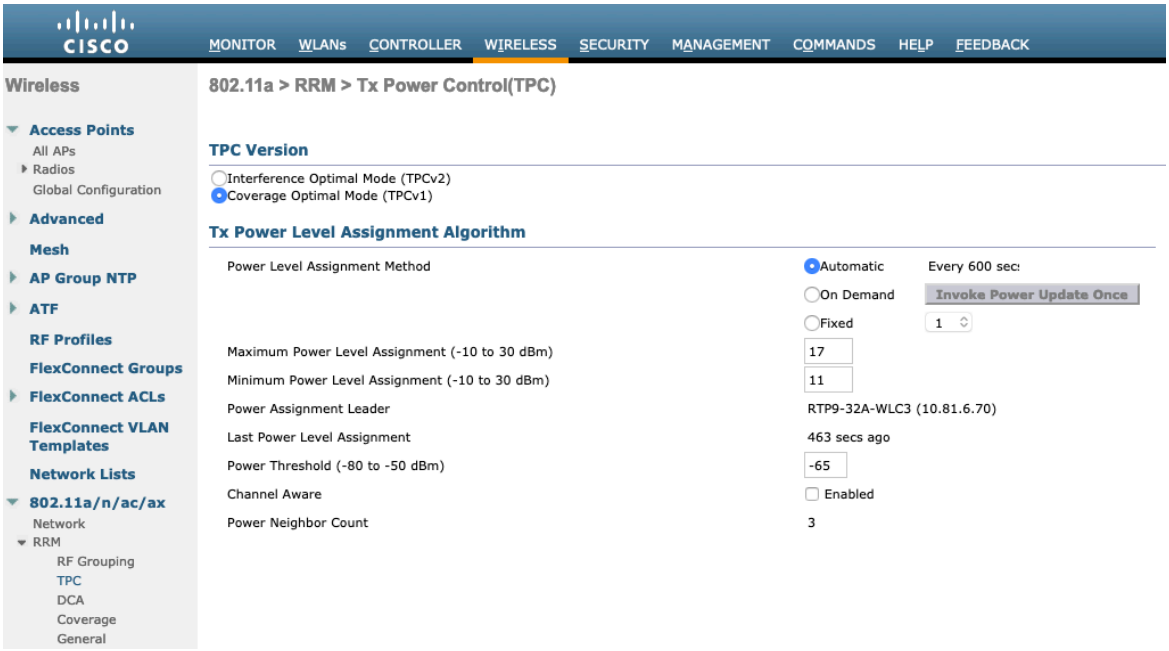
ワイヤレス LAN に接続する 802.11b のみのクライアントが存在しないことを想定して、12 Mbps を必須（基本）レートとして、サポートされている（オプション）のレートとして 18 Mbps を設定することが推奨されます。ただし、一部の環境では、必須（基本）レートとして、6 Mbps を有効にする必要があります。

802.11b クライアントが存在する場合、11 Mbps を必須 (基本) レートとして設定し、12 Mbps 以上をサポート (オプション) として設定する必要があります。



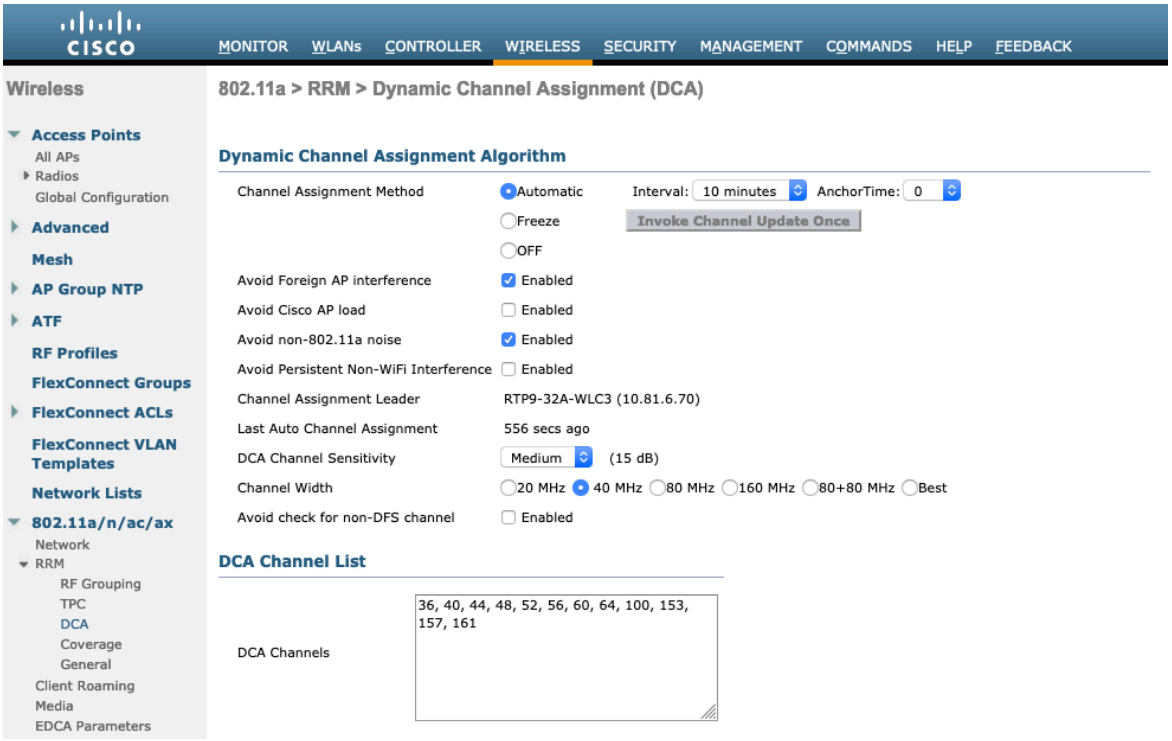
自動 RF (RRM)

Cisco Wireless LAN Controller を使用する際は、[自動RF（Auto RF）] を有効にして、チャネルと送信電力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に応じて、5 または 2.4 GHz のアクセスポイント送信電力レベル割り当て方法を設定します。
自動出力レベル割り当てを使用する場合、最大および最小の出力レベルを指定することができます。

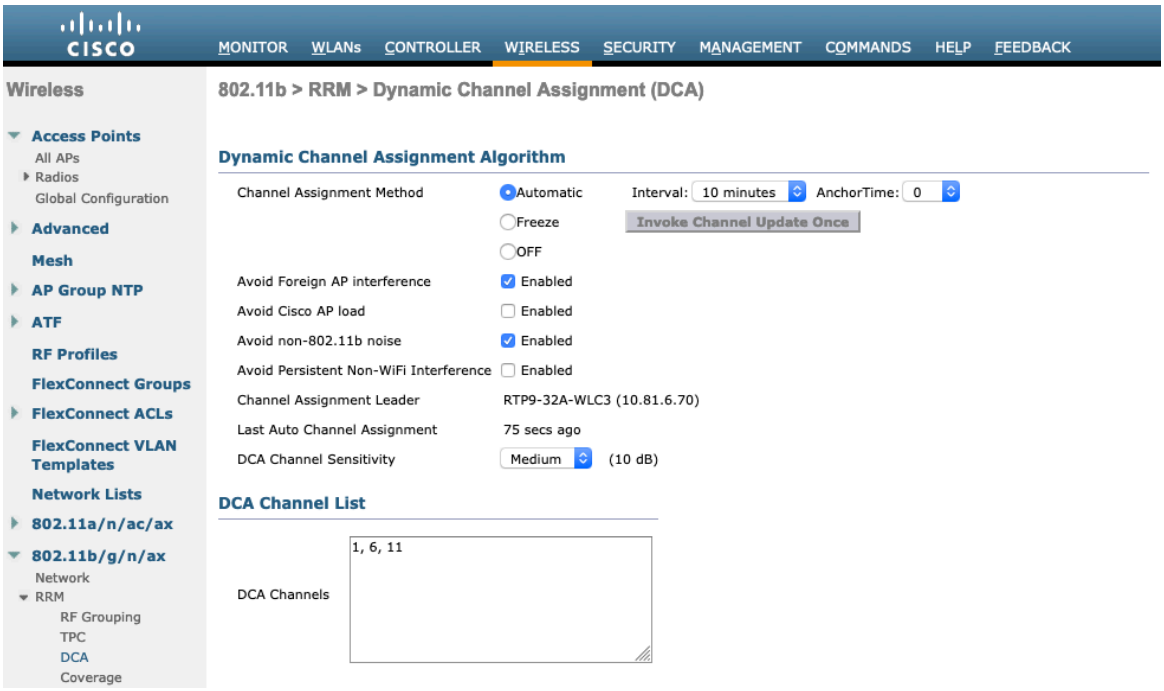


5 GHz を使用する場合、多くのチャンネルをスキャンすることによって引き起こされるアクセスポイント検出の潜在的な遅延を回避するために、チャンネル数を制限することをお勧めします (例、12 チャンネルのみ)。

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 として、Cisco 802.11ac アクセスポイントを使用する場合は 20 MHz、40MHz、または 80 MHz として構成できます。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、チャネル 1、6、および 11 のみを DCA リストで有効にする必要があります。2.4 GHz で利用できるチャネル数には限りがあるため、40 MHz に対応する Cisco 802.11n アクセス ポイントを使用する場合でも、2.4 GHz チャネルを 20 MHz として設定することを推奨します。



利用する周波数に周波数帯に応じて、5GHz または 2.4GHz のいずれかで動的チャネルと送信電力の割り当てを使用するように、個々のアクセスポイントは全体設定をオーバーライドするように設定できます。

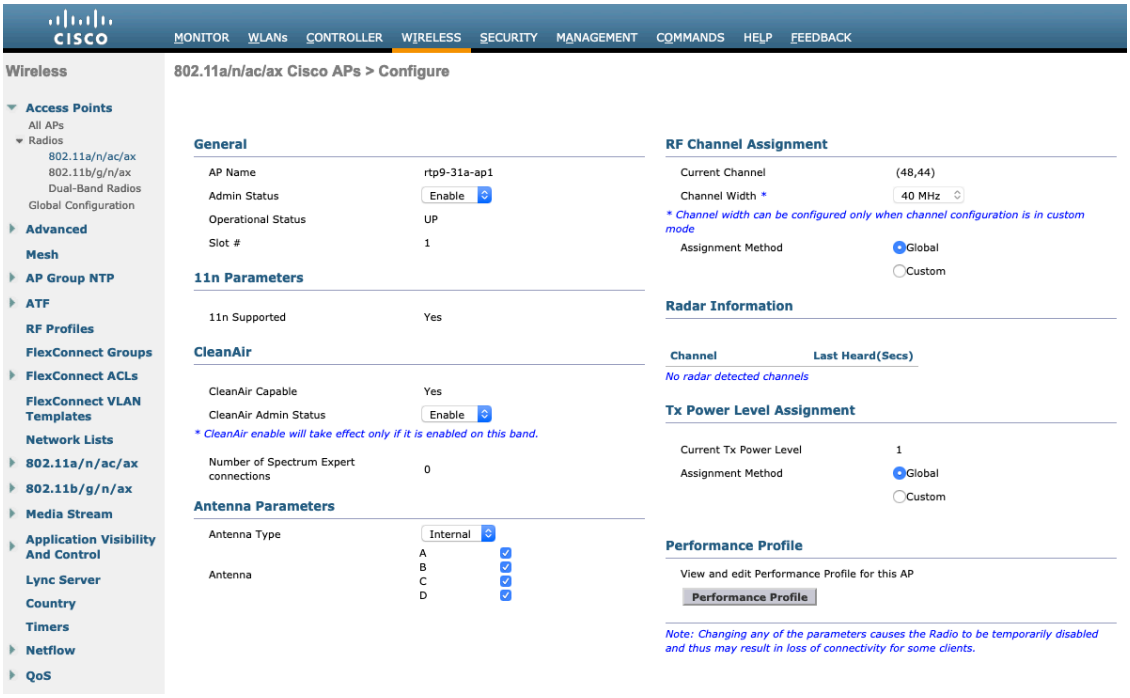
他のアクセス ポイントは、自動割り当て方法に対して有効にでき、静的に構成されたアクセス ポイントを考慮します。

これは、その地域で断続的な干渉源がある場合に必要になります。

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、80 MHz として設定できます。

5 GHz を使用する場合にのみ、チャネル バインディングを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

スキャンとローミングはデバイス自体によって個別に管理されるため、Cisco Desk Phone 9800 シリーズは、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 パラメータを利用しません。

EDCA パラメータ

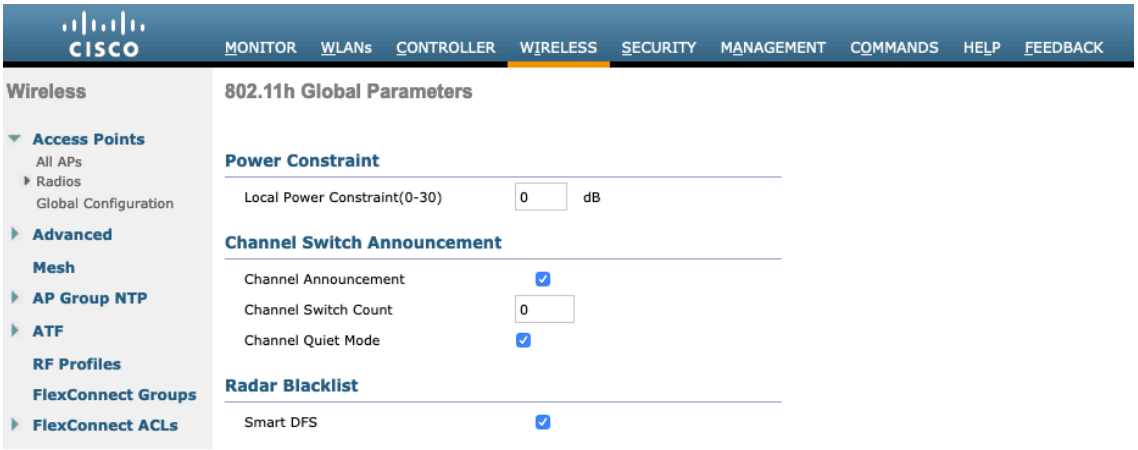
EDCA プロファイルを **[音声に最適化（Voice Optimized）]** または **[音声とビデオに最適化（Voice & Video Optimized）]** のいずれかに設定し、使用する周波数帯域に応じて、5 または 2.4 GHz のいずれかに対して **[低遅延 MAC（Low Latency MAC）]** を無効にします。

低遅延 MAC（LLM）は、アクセスポイント プラットフォームに応じて、パケットごとの再送信数を 2 ~ 3 減らします。これにより、複数データが有効な場合は、問題が発生する場合があります。

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

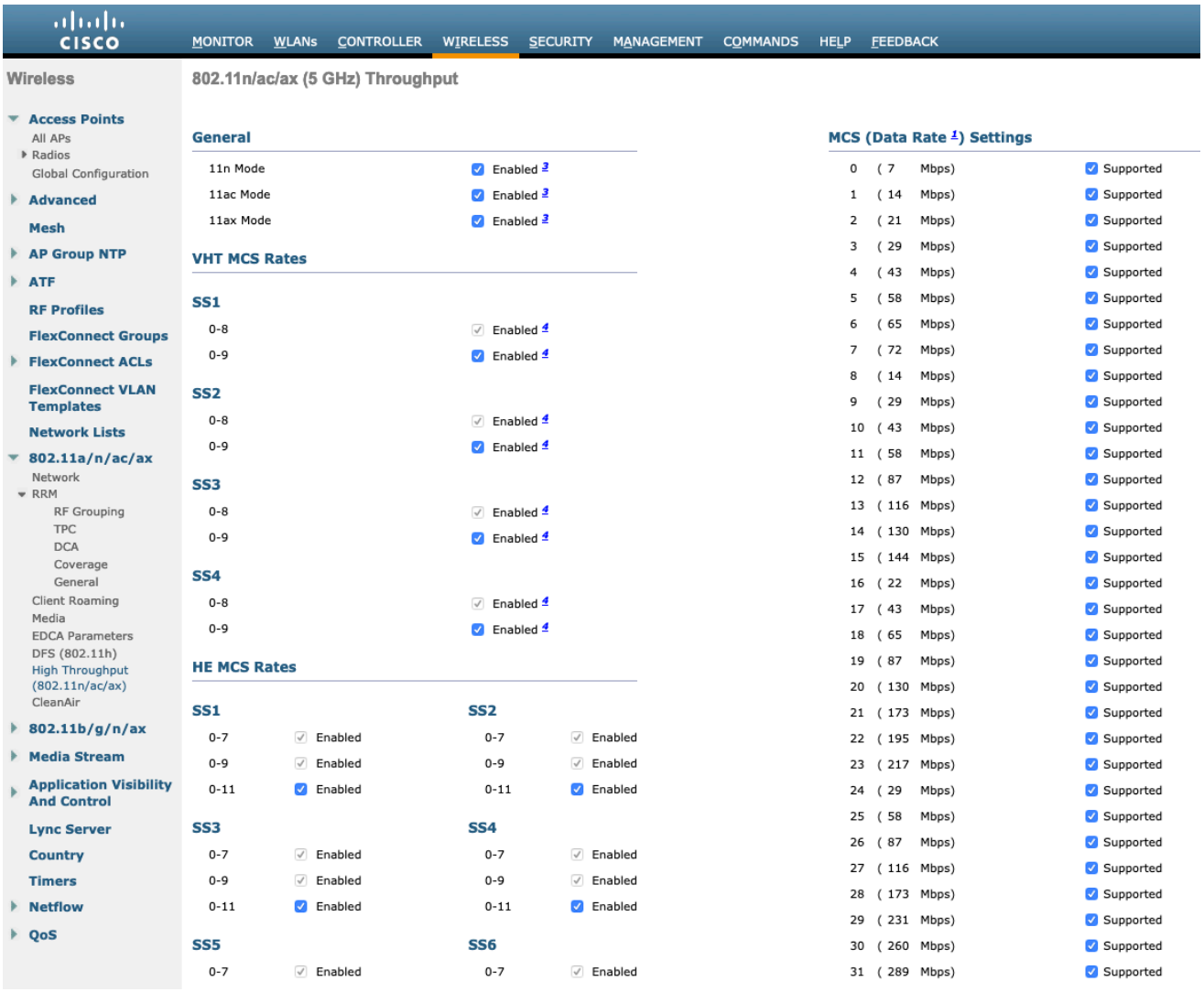
DFS (802.11h)

[電力制限（Power Constraint）] は、未設定のままにするか、0 dB に設定します。
[チャネルアナウンス（Channel Announcement）] と**[チャネルサイレントモード（Channel Quiet Mode）]** は **[有効（Enabled）]** に設定します。



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 にのみ適用されます。
WMM が有効になっていること、そして WPA2/WPA3(AES) が 802.11n/ac データレートを利用するように設定されていることを確認してください。
Cisco Desk Phone 9800 シリーズは、HT MCS 0 - MCS 7 および VHT MCS 0 - MCS 9 1SS データ レートのみをサポートしますが、それ以上の MCS レートは、他の 802.11n/ac クライアントが、より高いデータレートを利用できる MIMO アンテナテクノロジを含む同じ帯域周波数を利用している場合、オプションで有効にできます。



フレーム集約

フレームアグリゲーションは、オーバーヘッドを削減するために、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化するプロセスであり、その結果、スループットと容量を最適化できます。

MAC プロトコル データ ユニット (A-MPDU) の集約では、ブロック確認応答を使用する必要があります。

Cisco Desk Phone 9800 シリーズでのエクスペリエンスを最適化するには、A-MPDU および A-MSDU 設定を次のように調整する必要があります。

A-MSDU

ユーザ優先順位 1、2 = 有効

ユーザ優先順位 0、3、4、5、6、7 = 無効

A-MPDU

ユーザ優先順位 0、3、4、5 = 有効

ユーザ優先順位 1、2、6、7 = 無効

以下のコマンドを使用して、Cisco Desk Phone 9800 シリーズの要件に従って、A-MPDU および A-MSDU を設定します。

5 GHz 設定を構成するには、まず 802.11a ネットワークを有効にし、変更が完了したら再度有効にします。

```
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 設定を構成するには、まず 802.11b/g ネットワークを有効にし、
変更が完了した後、再度有効にします。

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

現在の A-MPDU および A-MSDU の構成を表示するには、5 GHz の場合は show 802.11a、2.4 GHz の場合は show 802.11b と入力します。

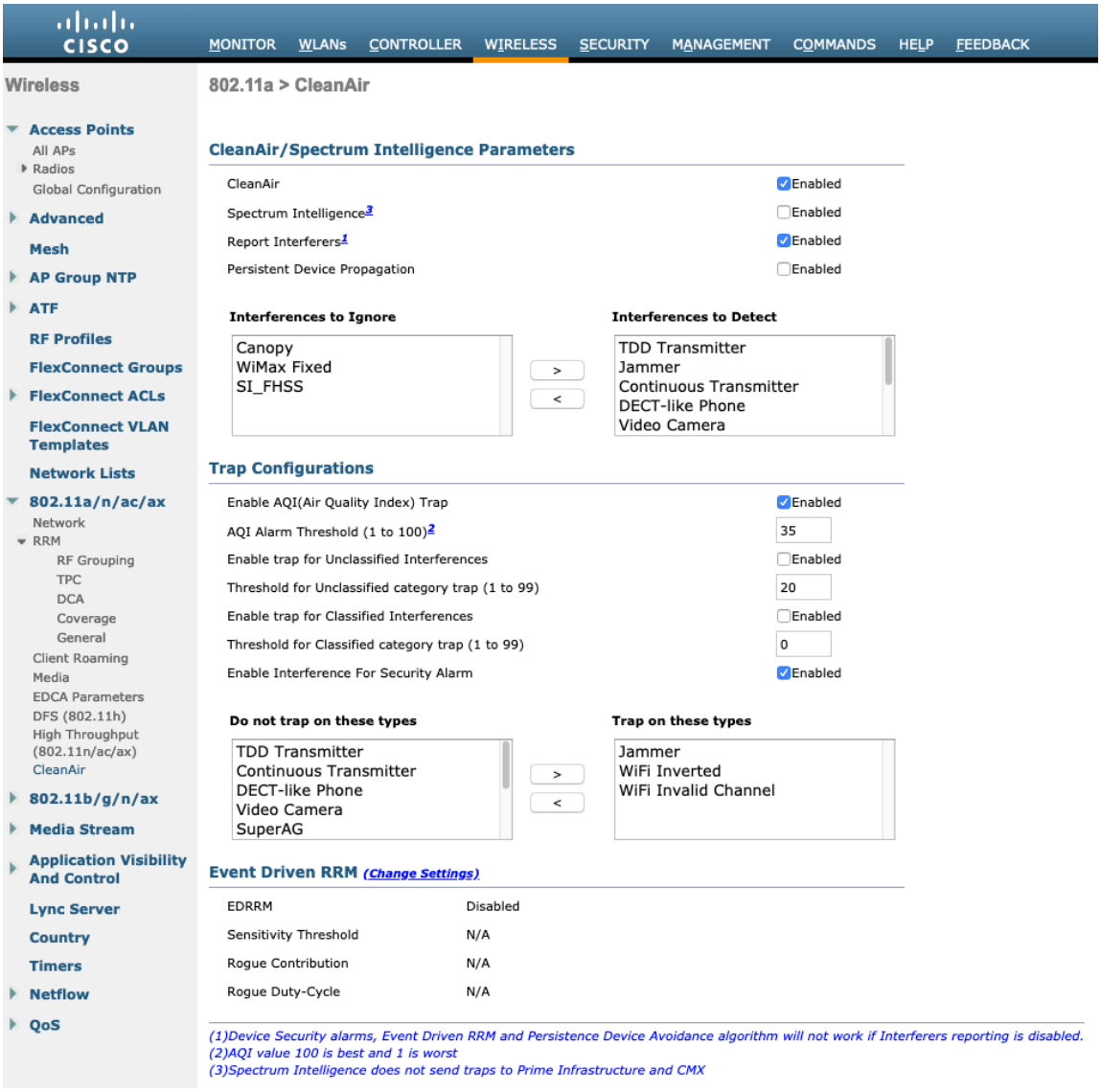
802.11n ステータス:

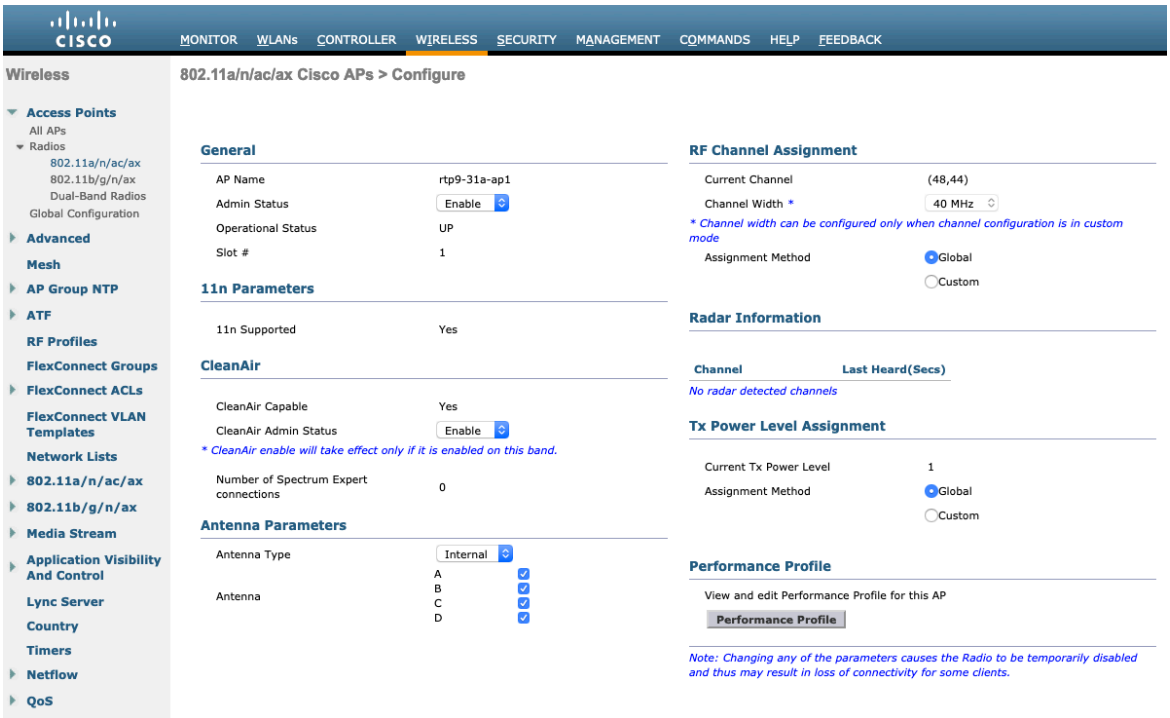
A-MSDU 送信:

優先順位 0..... 無効
優先順位 1..... [有効（Enabled）]
優先度 2..... [有効（Enabled）]
優先順位 3..... 無効
優先順位 4..... 無効
優先順位 5..... 無効
優先順位 6..... 無効
優先度 7..... 無効
A-MPDU 送信:
優先順位 0..... [有効（Enabled）]
優先度 1..... 無効
優先順位 2..... 無効
優先度 3..... [有効（Enabled）]
優先度 4..... [有効（Enabled）]
優先度 5..... [有効（Enabled）]
優先順位 6..... 無効
優先順位 7..... 無効

クリーンエア

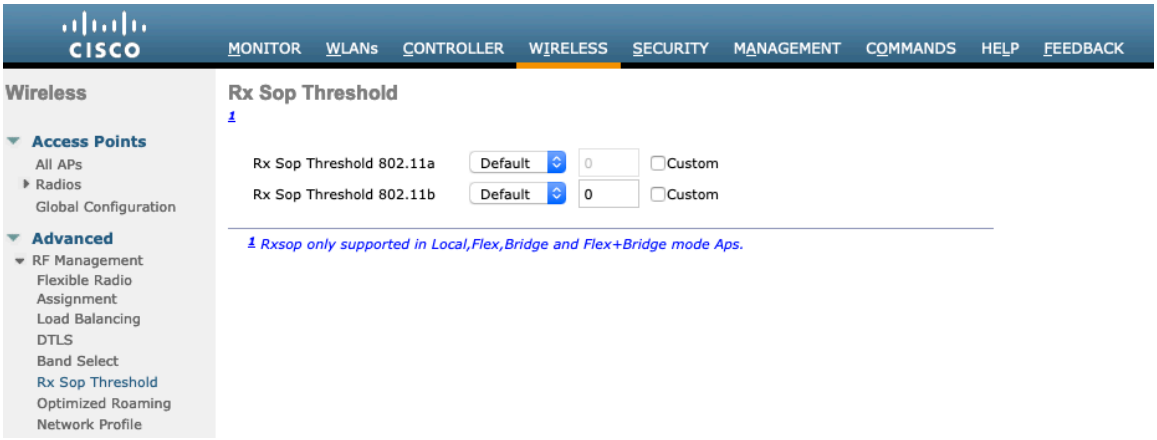
CleanAir テクノロジ搭載の Cisco アクセスポイントを使用して、既存の干渉源を検出するには、**[CleanAir]** を [有効（Enabled）] にします。


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
802.11a > CleanAir
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
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


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
802.11a/n/ac/ax Cisco APs > Configure
Access Points
All APs
Radios
802.11a/n/ac/ax
802.11b/g/n/ax
Dual-Band 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
General
AP Name
rtp9-31a-ap1
Admin Status
Enable
Operational Status
UP
Slot #
1
11n Parameters
11n Supported
Yes
CleanAir
CleanAir Capable
Yes
CleanAir Admin Status
Enable
* CleanAir enable will take effect only if it is enabled on this band.
Number of Spectrum Expert connections
0
Antenna Parameters
Antenna Type
Internal
Antenna
A
B
C
D
RF Channel Assignment
Current Channel
(48,44)
Channel Width *
40 MHz
* Channel width can be configured only when channel configuration is in custom mode
Assignment Method
Global
Custom
Radar Information
Channel
Last Heard(Secs)
No radar detected channels
Tx Power Level Assignment
Current Tx Power Level
1
Assignment Method
Global
Custom
Performance Profile
View and edit Performance Profile for this AP
Performance Profile
Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Rx Sop Threshold

[Rx Sopしきい値（Rx Sop Threshold）] には、デフォルト値を使用することが推奨されます。



[IVR設定(WLAN Settings)]

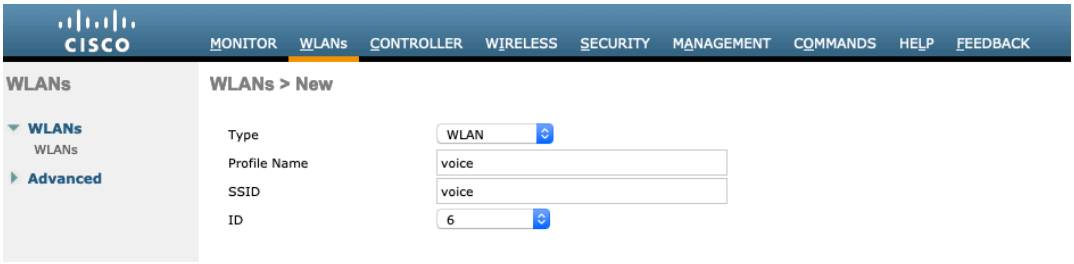
Cisco Desk Phone 9800 シリーズには別の SSID を割り当てることを推奨します。

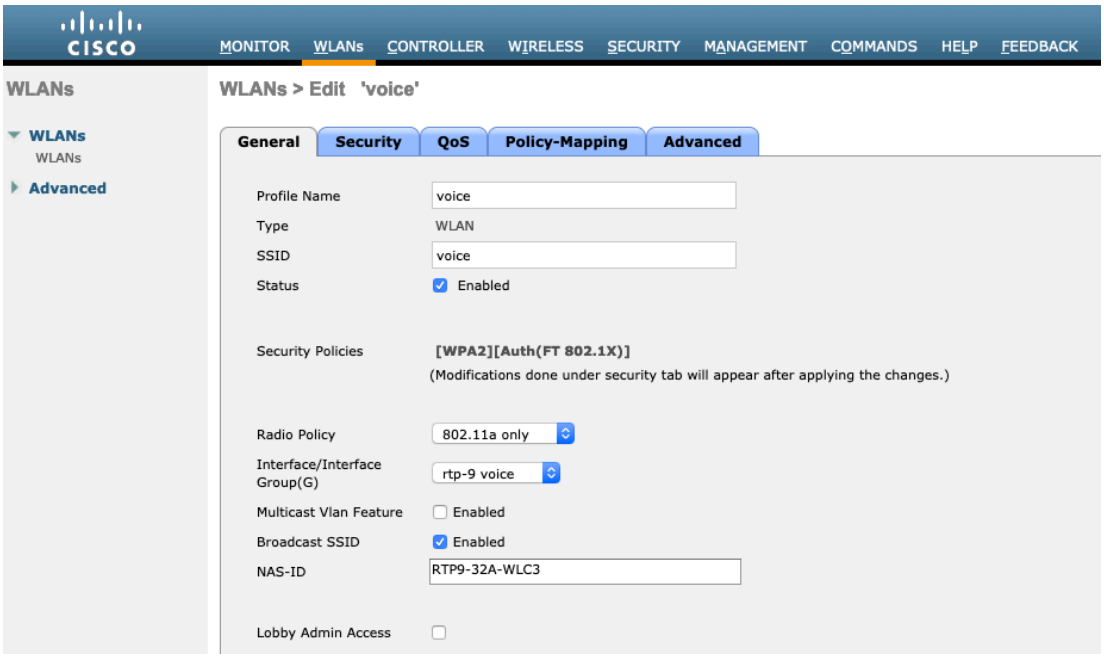
しかし、音声対応 Cisco ワイヤレス LAN エンドポイントをサポートするように設定された既存の SSID を使用することもできます。

Cisco Desk Phone 9800 シリーズで使用される SSID は、特定の 802.11 無線タイプのみに適用されるように設定できます (例、802.11a のみ)。

Cisco Desk Phone 9800 シリーズは 5 GHz 帯のみで使用することを推奨します。 多くのチャネルが利用でき、2.4 GHz 帯に比べて干渉が少ない ためです。

選択した SSID が他のワイヤレス LAN で使用されていないことを確認してください。異なるセキュリティタイプが使用されている場合は特に、電源オン時またはローミング中に障害が発生する可能性があります。



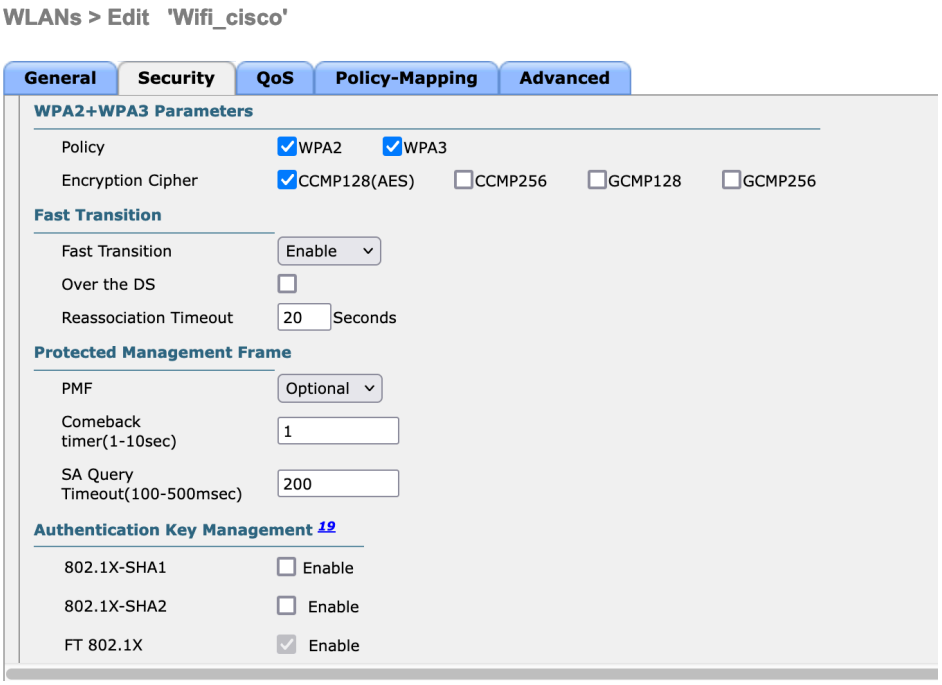


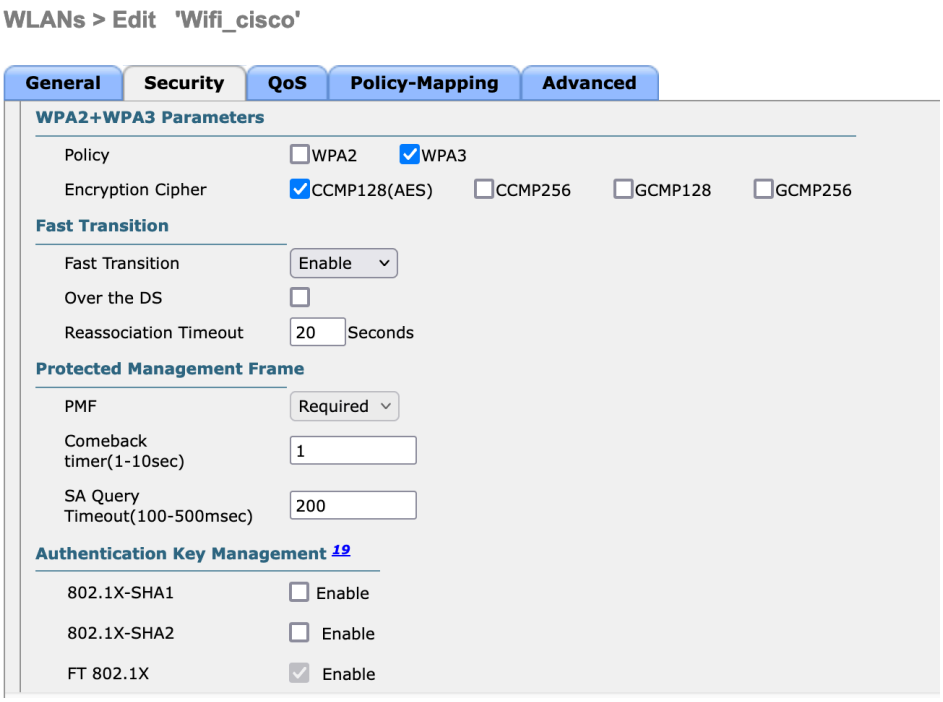
高速セキュア ローミングに 802.11r (FT) を利用するには、高速移行を有効にします。

Over the Distribution System 方法ではなく、Over the Air方法を使用するには、**[Over the DS]** チェックボックスをオフにすることが推奨されます。

WPA3 の場合、[保護された管理フレーム] は [**任意**] または [**必須**] に設定します。

AES 暗号化の WPA2/WPA3 ポリシーを有効にし、802.1x または PSK/SAE のどちらかを使用するかに応じて、認証キー管理タイプの FT 802.1x、FT PSK または FT SAE を使用するかを選択します。



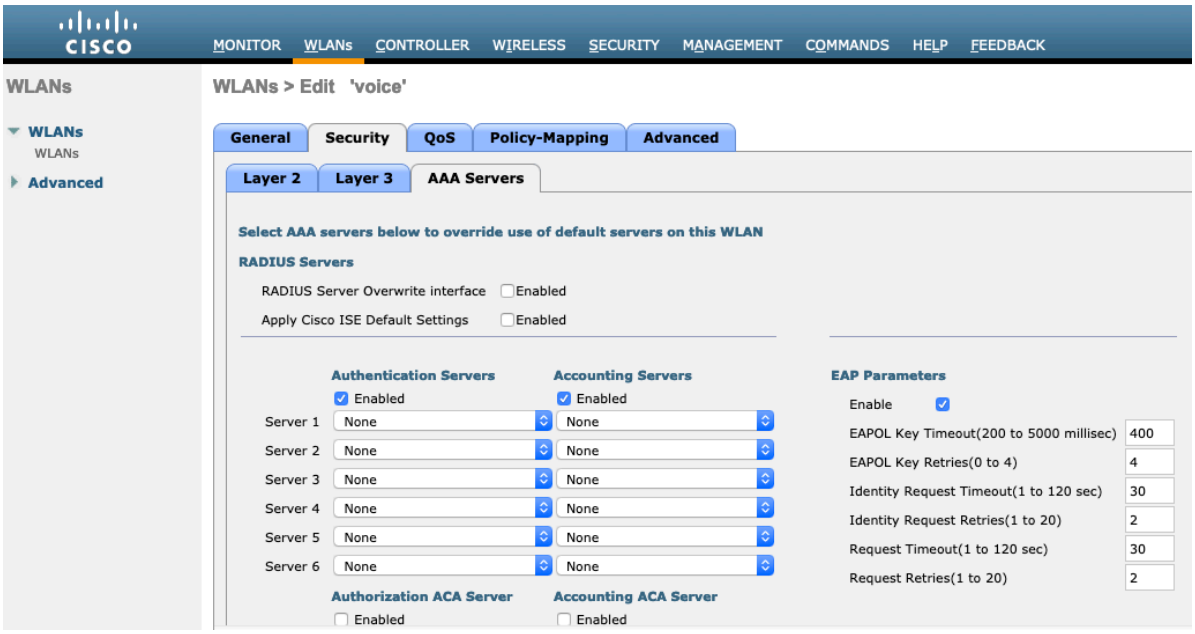


802.11x、PSK、または SAE は、さまざまなタイプの音声クライアントに対して同じ SSID を利用するために有効にできます。 802.1x、PSK、SAE のいずれが使用されるかによって、一部のクライアントは 802.11r (FT) をサポートしない場合があります。

SSID ごとに RADIUS 認証およびアカウント サーバを設定して、グローバル リストを上書きすることができます。**有効**または指定しない場合（**[なし（None）]**に設定）、RADIUS サーバーの共通リストが使用されます（**[セキュリティ（Security）]** > [AAA] > **[RADIUS]** の順に選択）。

EAP ブロードキャスト キー間隔を除くすべての EAP パラメータは、SSID ごとに、またはグローバルに設定できます。 EAP ブロードキャスト キー間隔は、グローバル レベルでのみ設定できます。

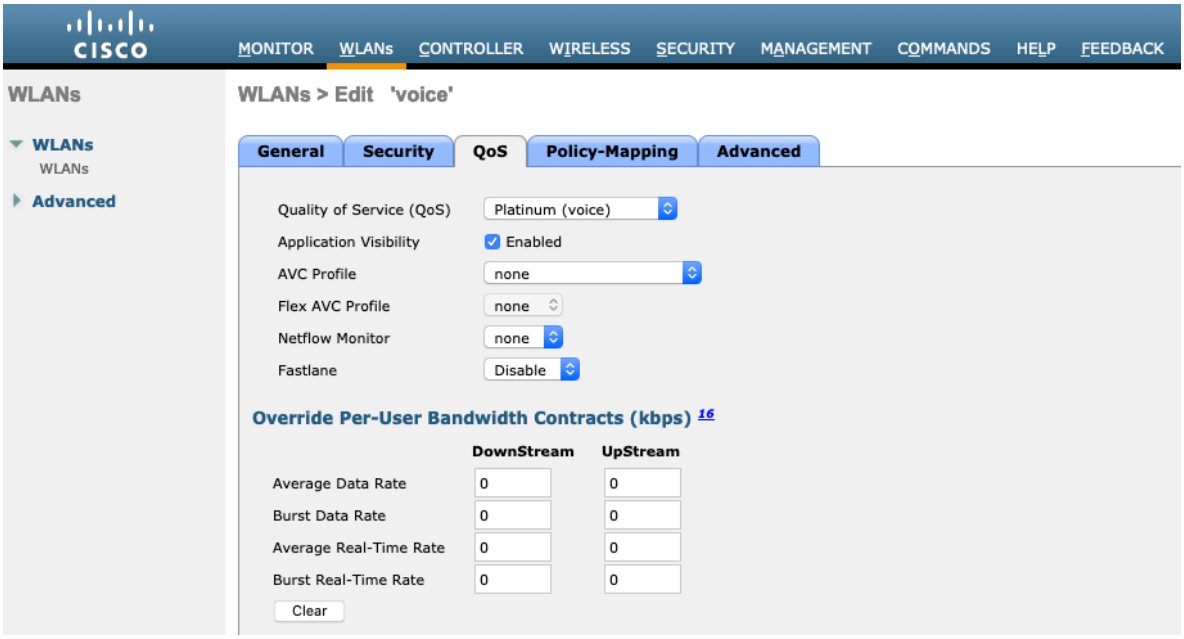
SSID ごとに EAP パラメータを設定するには、[EAP パラメータ] セクションで [**有効にする**] にチェックを入れ、適切な値を入力します。

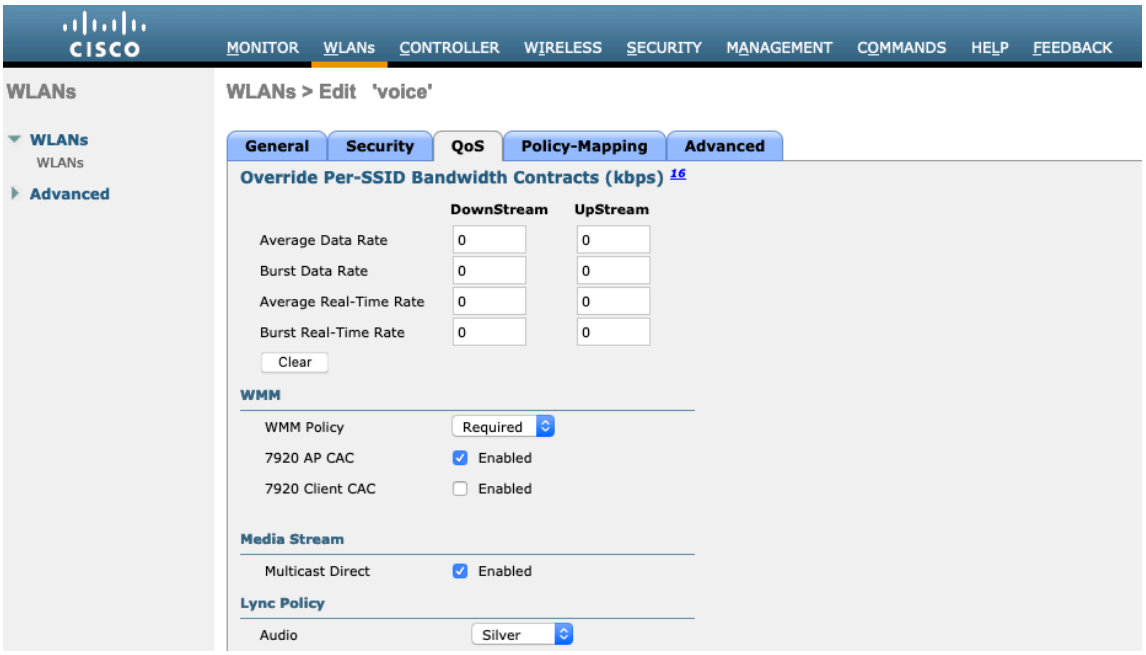


WMM ポリシーは、Cisco Desk Phone 9800 シリーズまたは他の WMM 対応電話がこの SSID を使用する場合にのみ、 **必須** に設定する必要があります。

WLAN 上に非 WMM クライアントがある場合、これらのクライアントを別の WLAN に配置することを推奨します。非 WMM クライアントは、Cisco Desk Phone 9800 シリーズとおなじ SSID を使用して、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。 音声通話中の潜在的な中断を回避するために、86400 秒のセッションタイムアウトを有効にし、クライアント資格情報を定期的に再検証して、クライアントが有効な資格情報を使用していることを確認することをお勧めします。

Aironet 拡張機能 (**Aironet IE**) を無効にします。

ピアツーピア (P2P) ブロックアクション を無効にする必要があります。

必要に応じて **クライアントの除外** を設定します。

AP 無線ごとの最大クライアント数 は必要に応じて設定できます。

[オフチャネルスキャンの保留（Off Channel Scanning Defer）] は、特定のキューのスキャンとスキャンの保留時間を調整するためにオンにできます。

アクセスポイントへのベスト エフォート アプリケーションを頻繁に使用するか、優先アプリケーション（音声および通話コントロールなど）の DSCP 値を保存しない場合、オフチャネルスキャンを保留し、スキャン保留時間を長くするために、低いキュー優先度（0-3）と高いキュー優先度（4-6）を有効にすることが推奨されます。頻繁な EAP 失敗による展開では、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アドレス割り当てが必要（DHCP Address Assignment Required）] を無効にします。

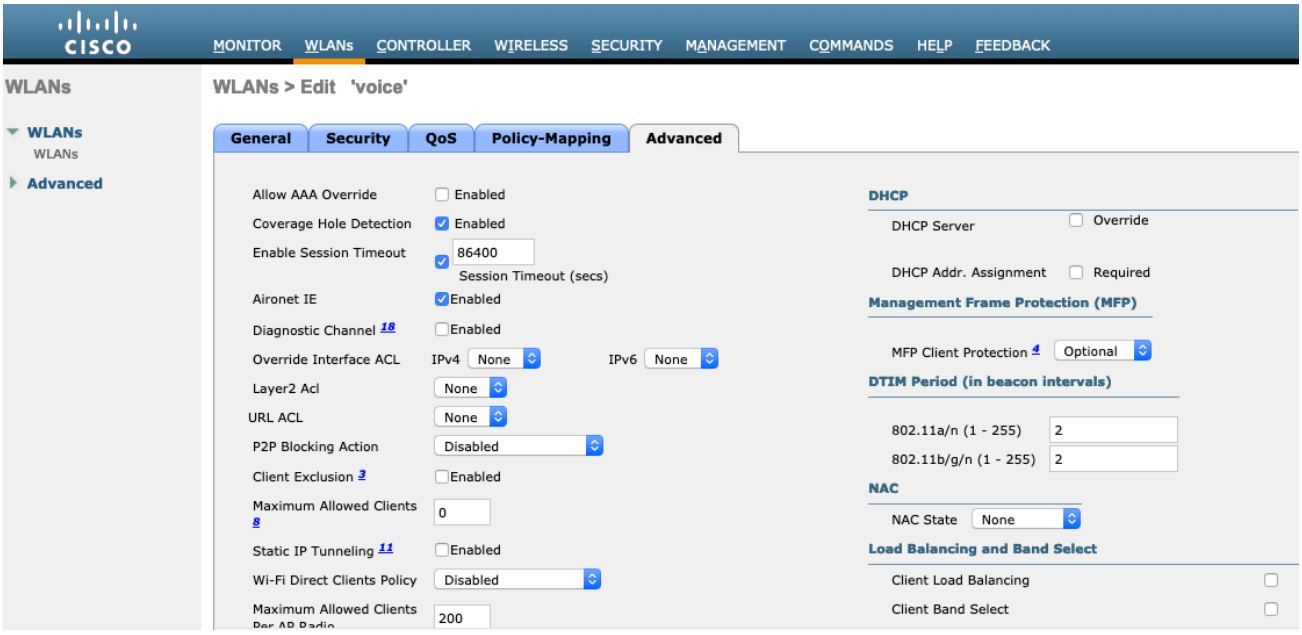
[管理フレーム保護（Management Frame Protection）] を、[オプション（Optional）] または [WPA3に必要（Required for WPA3）] に設定します。

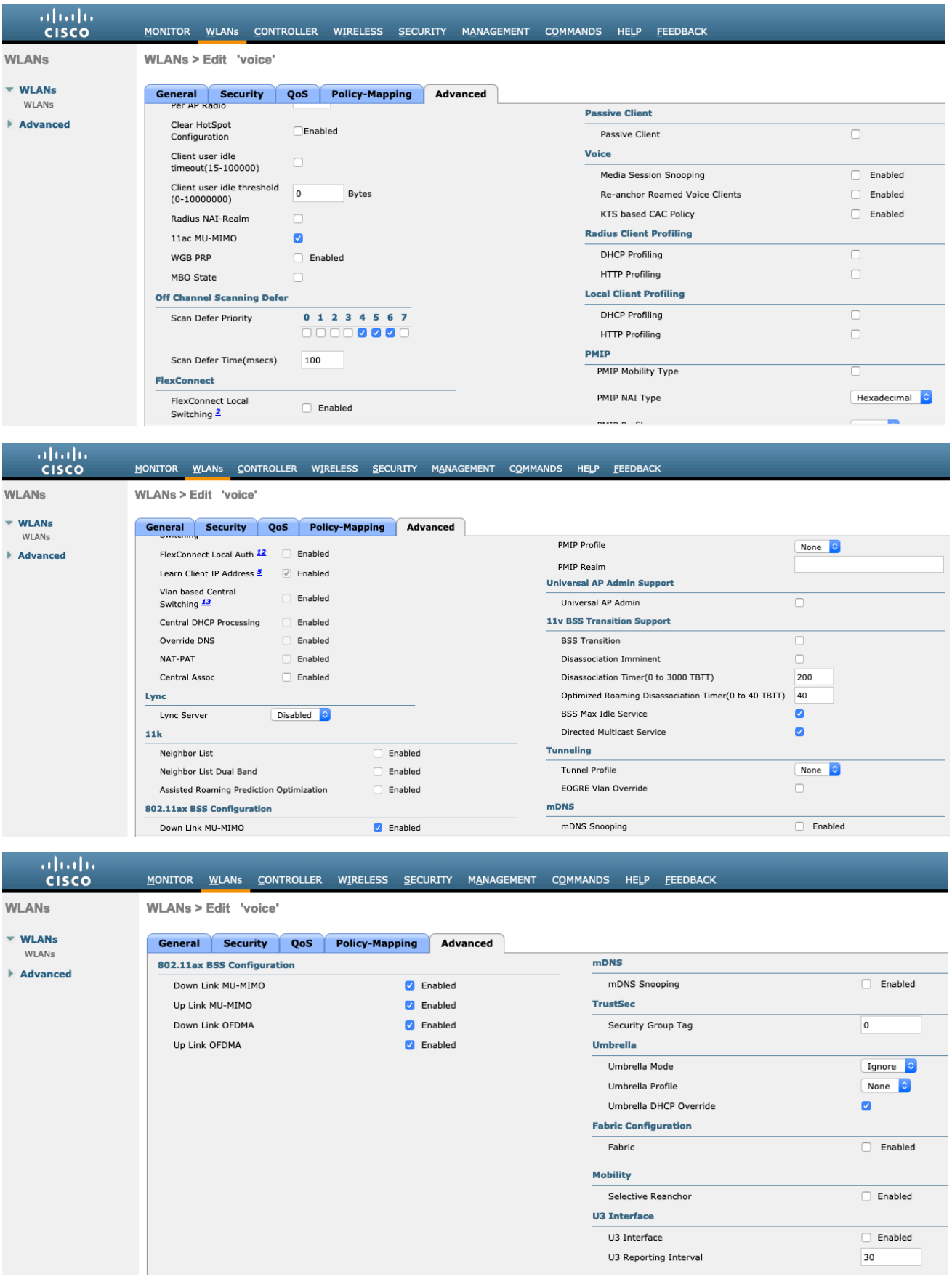
ビーコン期間が **100 ms** の 2 の**DTIF 期間**を使用します。

クライアント負荷分散 および **クライアント帯域選択** が無効になっていることを確認してください。

コントローラ間のローミングを実行した後に通話を終了する際に、ワイヤレス LAN 接続によって短期間中断する可能性があるため、**[ローミングした音声クライアントのリアンカー（Re-anchor Roamed Voice Clients）]**を [無効（Disabled）] に設定することが推奨されます。

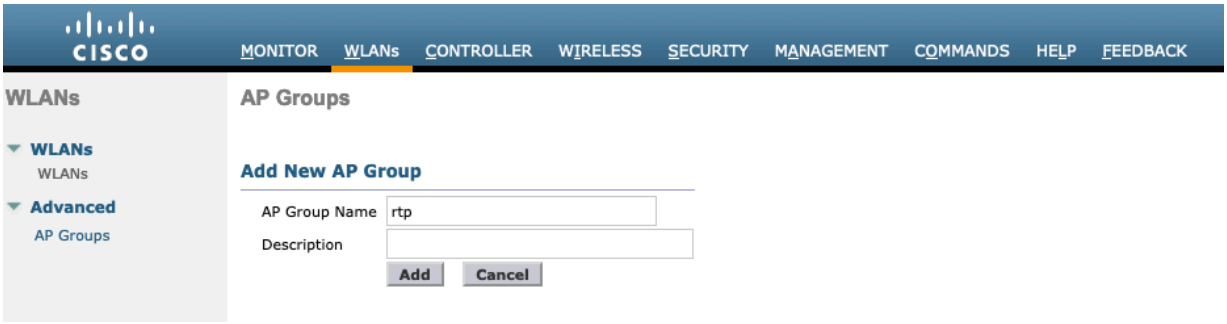
802.11k および 802.11v はデフォルト設定のままにします。

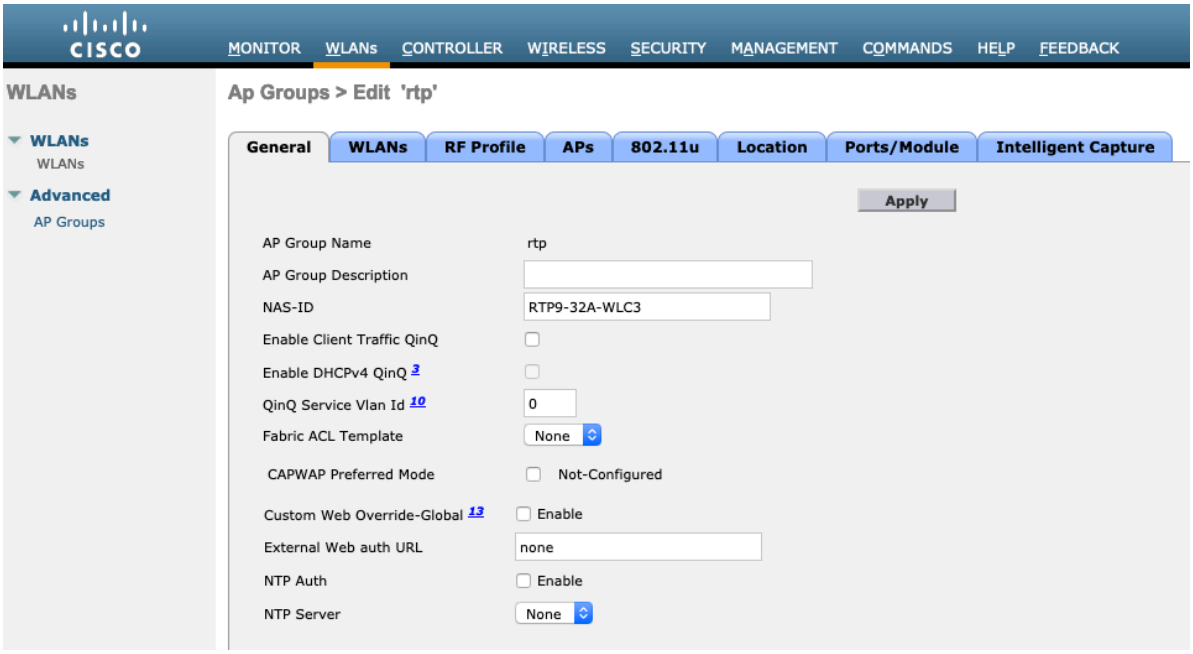



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Clear HotSpot Configuration
Enabled
Client user idle timeout(15-100000)
Client user idle threshold (0-10000000)
0
Bytes
Radius NAI-Realm
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 2
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'
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
FlexConnect Local Auth 12
Enabled
Learn Client IP Address 5
Enabled
Vlan based Central Switching 13
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'
WLANs
WLANs
Advanced
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

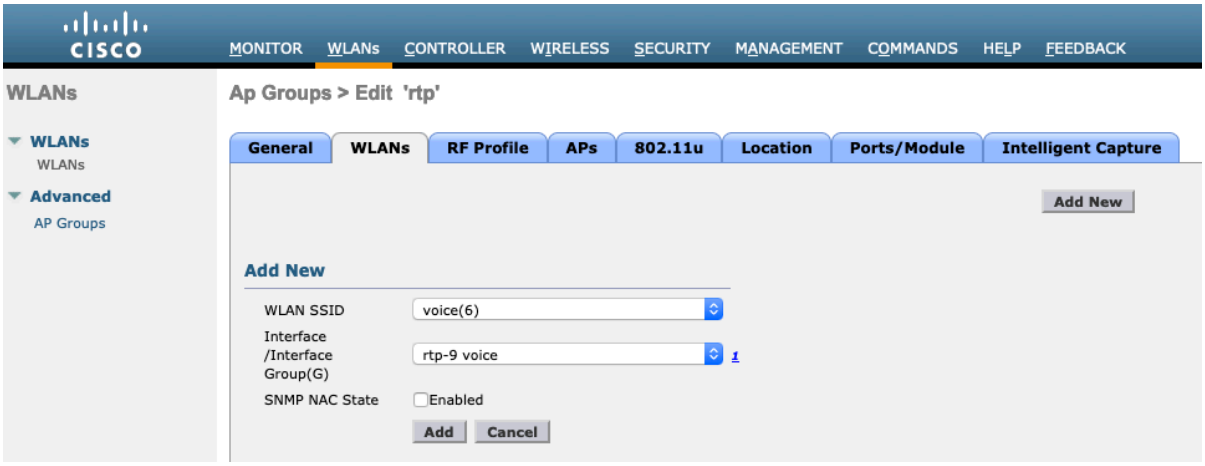
AP グループ

AP グループを作成して、どの WLAN/SSID を有効にするか、どのインターフェイスにマッピングするかを指定し、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 RF プロファイルのパラメータを指定することができます。



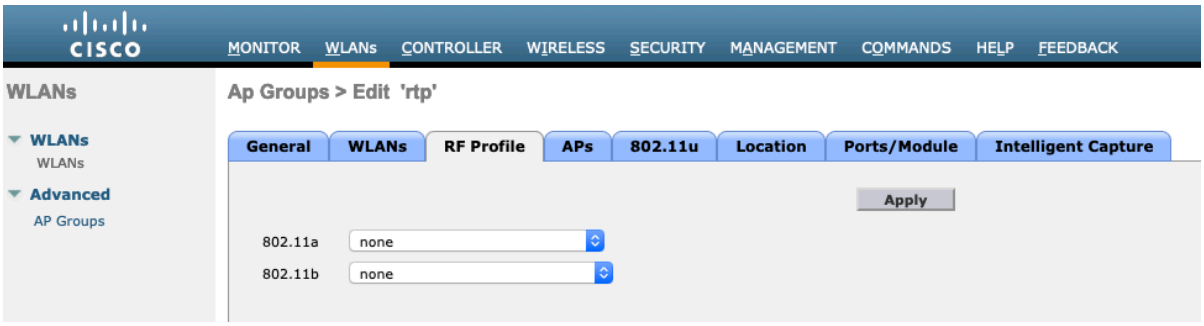


[WLAN] タブで、マッピングする SSID とインターフェイスを選択し、[**追加**] を選択します。



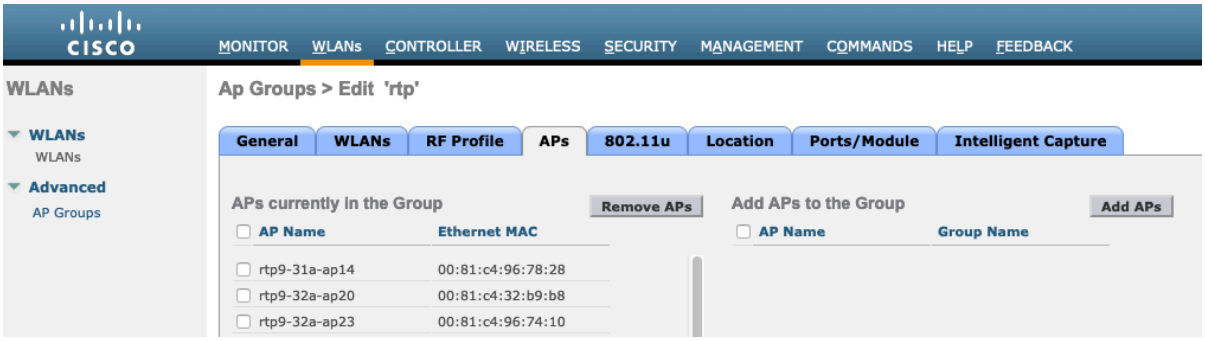
[RFプロファイル（RF Profile）] タブで、目的の 802.11a または 802.11b RF プロファイルを選択して、**[適用（Apply）]** を選択します。

アクセスポイントが AP グループに参加した後に変更が加えられた場合、変更が行われた時点でこれらのアクセスポイントは再起動されます。



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

これらのアクセスポイントはリブートします。

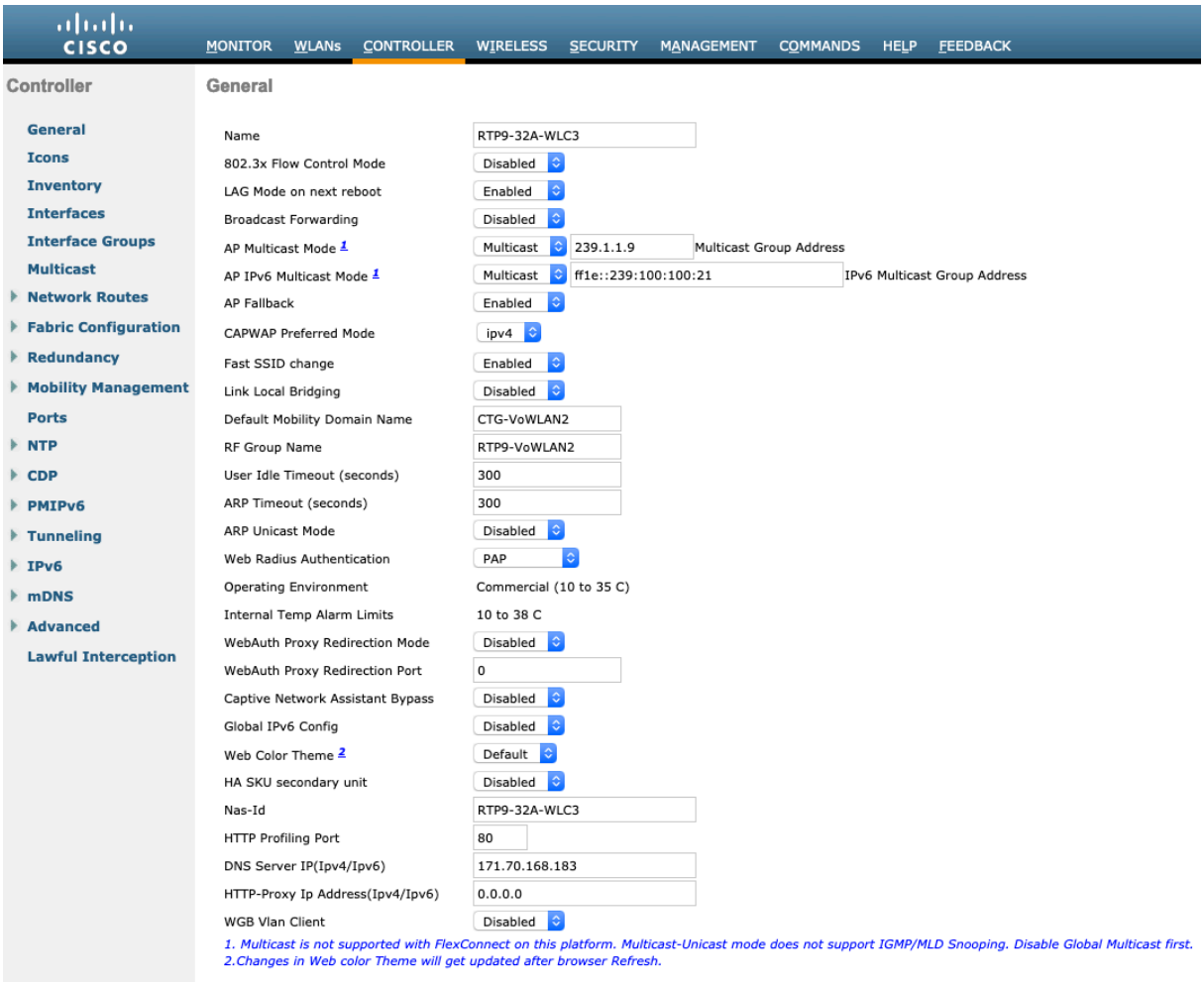


コントローラの設定

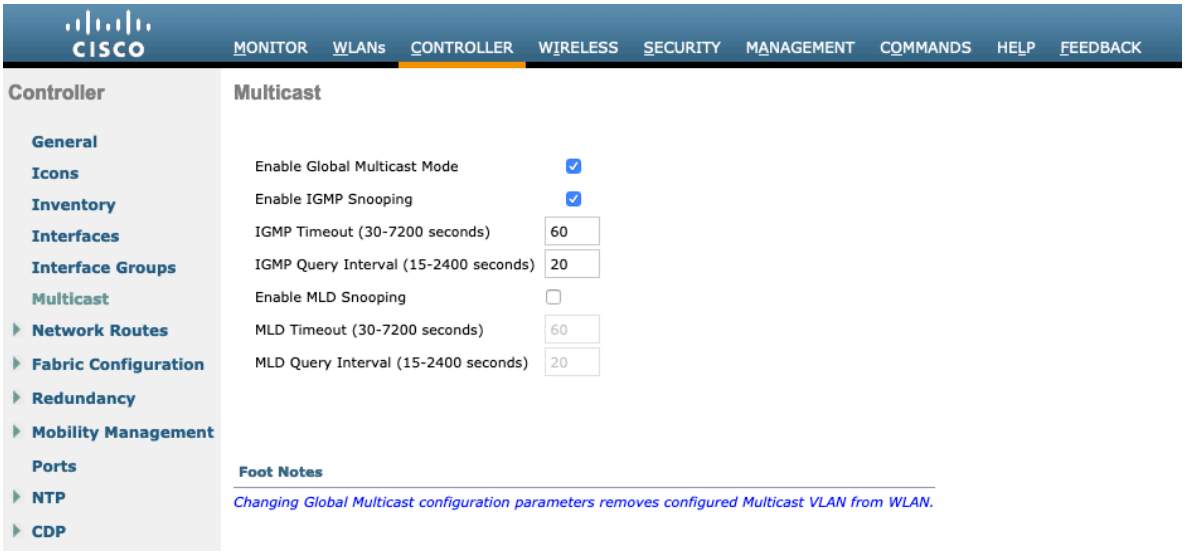
Cisco Wireless LAN Controller ホスト名が正しく設定されていることを確認します。

Cisco ワイヤレス LAN コントローラで複数のポートを利用する場合は、Link Aggregation (LAG) を有効にします。

目的の AP マルチキャストモードを設定します。

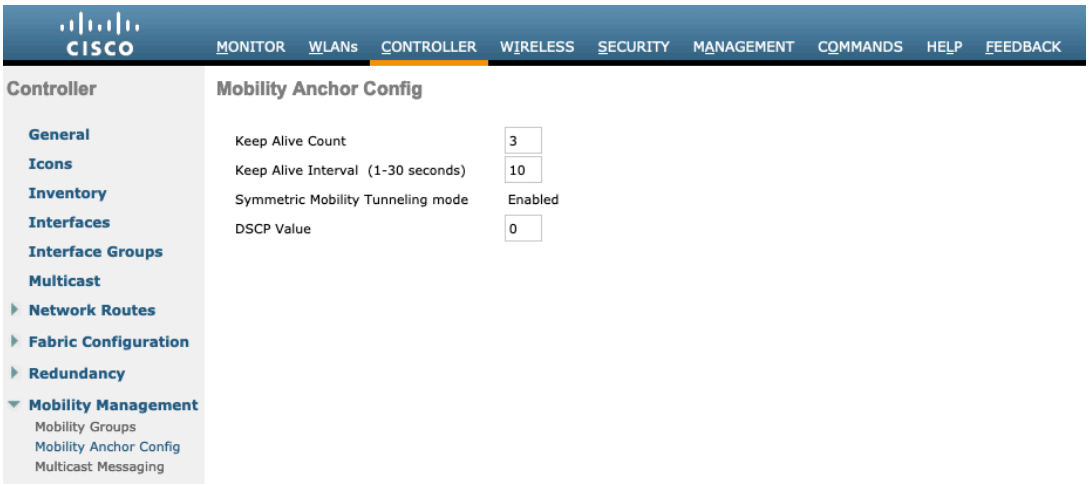


マルチキャストを使用するには、**[共通マルチキャストモードを有効化（Enable Global Multicast Mode）]** と **[IGMPスプーフィングを有効化（Enable IGMP Snooping）]** をオンにします。

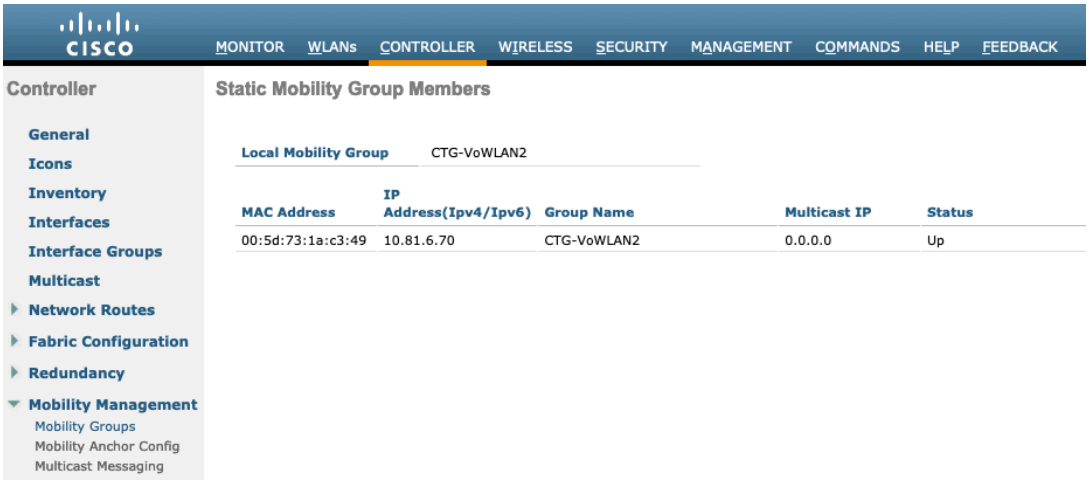


レイヤ 3 モビリティを使用する際は、**[対称モビリティトンネリング（Symmetric Mobility Tunneling）]** を **[有効（Enabled）]** にします。

最新のバージョンでは、[対称モビリティトンネリング（Symmetric Mobility Tunneling）] は、デフォルトでは有効になっており、校正不可です。

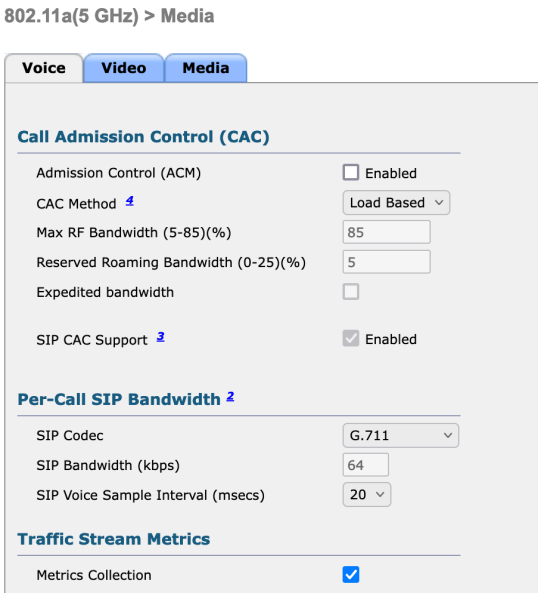


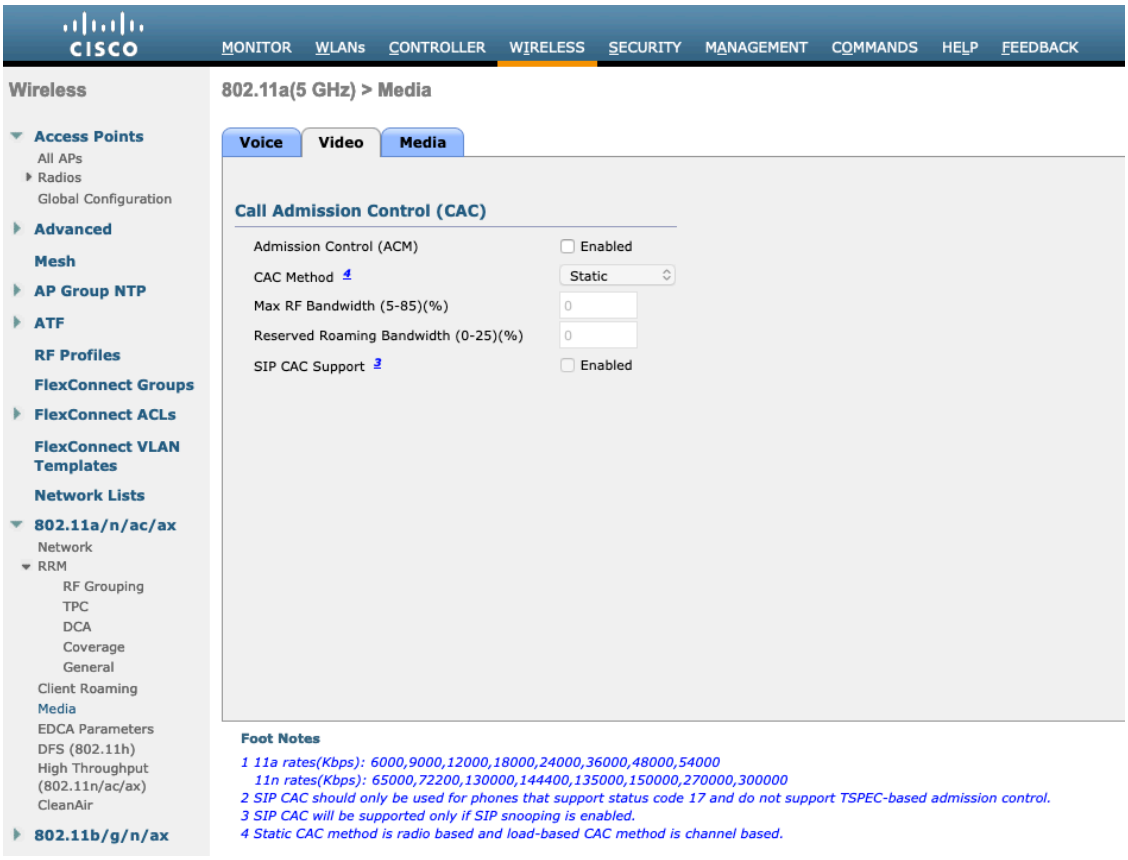
複数の Cisco Wireless LAN Controller が同じモビリティグループの一部である場合は、Cisco Wireless LAN Controller の IP アドレスと MAC アドレスを Static Mobility Group Members 構成に追加します。



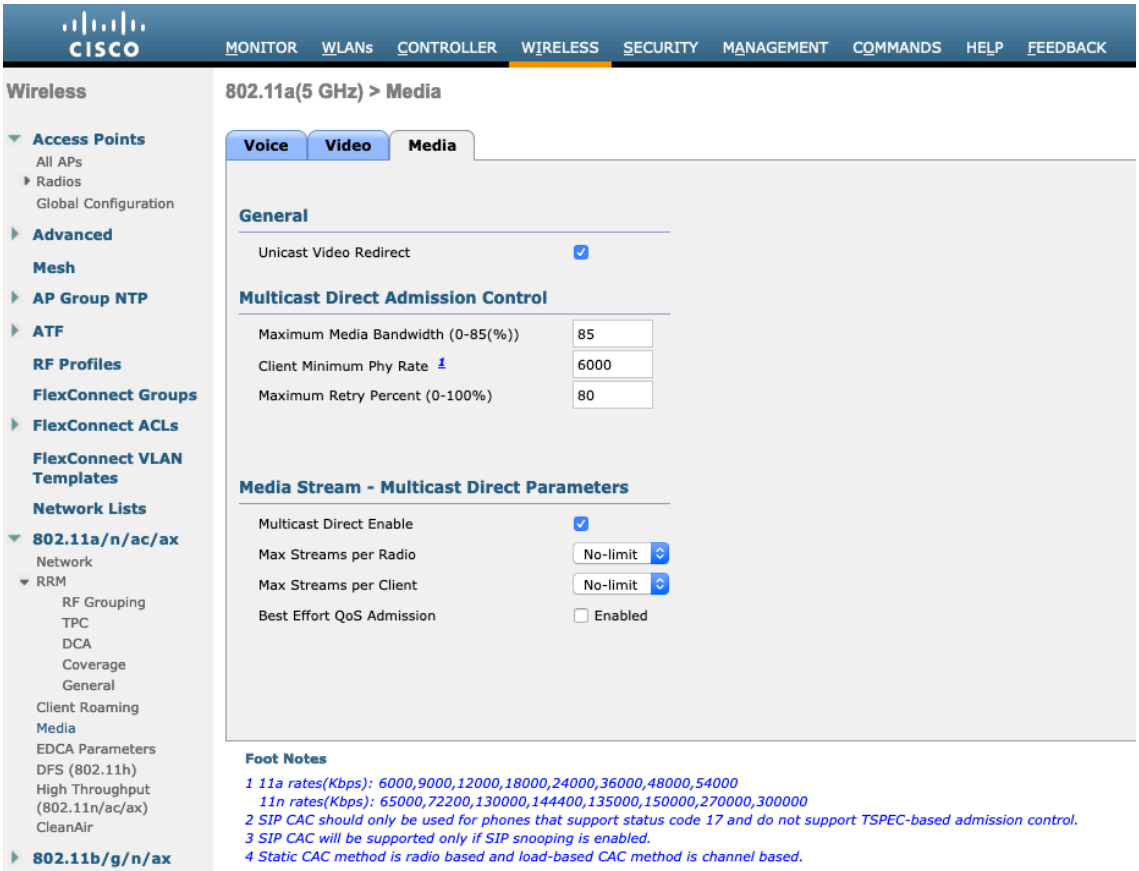
コール アドミッション制御（CAC）

[音声とビデオに必須のアドミッション制御（Admission Control Mandatory for Voice and Video）] を無効にします。





メディア設定で、 **ユニキャストビデオリダイレクト** と **マルチキャストダイレクト** を有効にする必要があります。



RF プロファイル

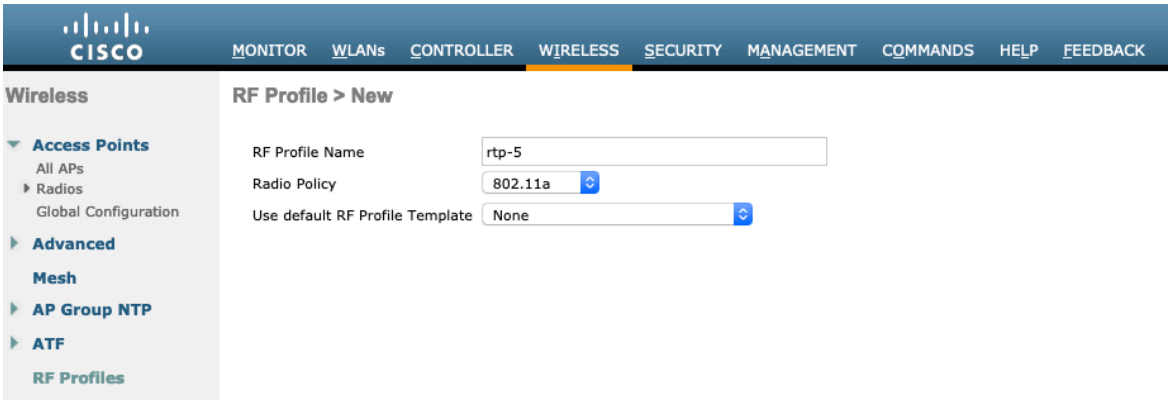
アクセス ポイントのグループが使用する周波数帯域、データ レート、RRM 設定などを指定するために、RF プロファイルを作成できます。

Cisco デスク フォン 9800 シリーズで使用される SSID については、5 GHz 無線にのみ適用することを推奨します。

いったん作成されると、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** と **無線ポリシー** を定義する必要があります。

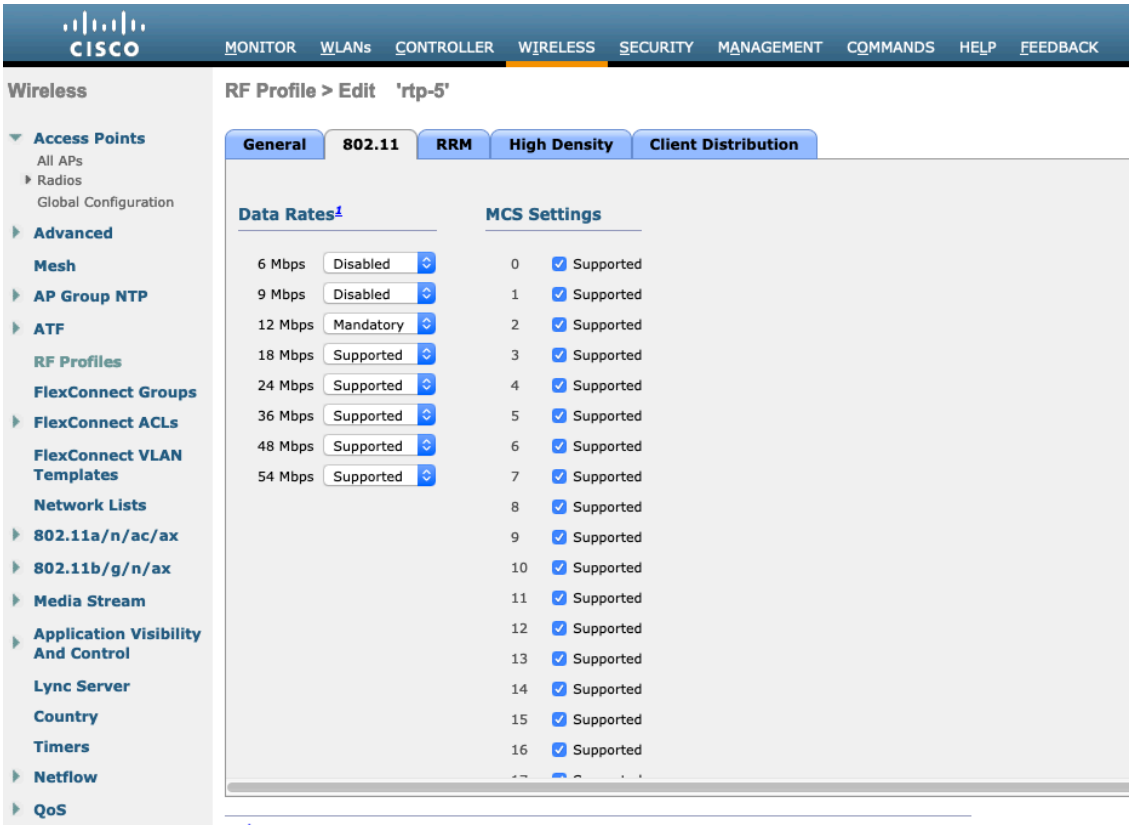
無線ポリシーの 802.11a または 802.11b/g を選択します。



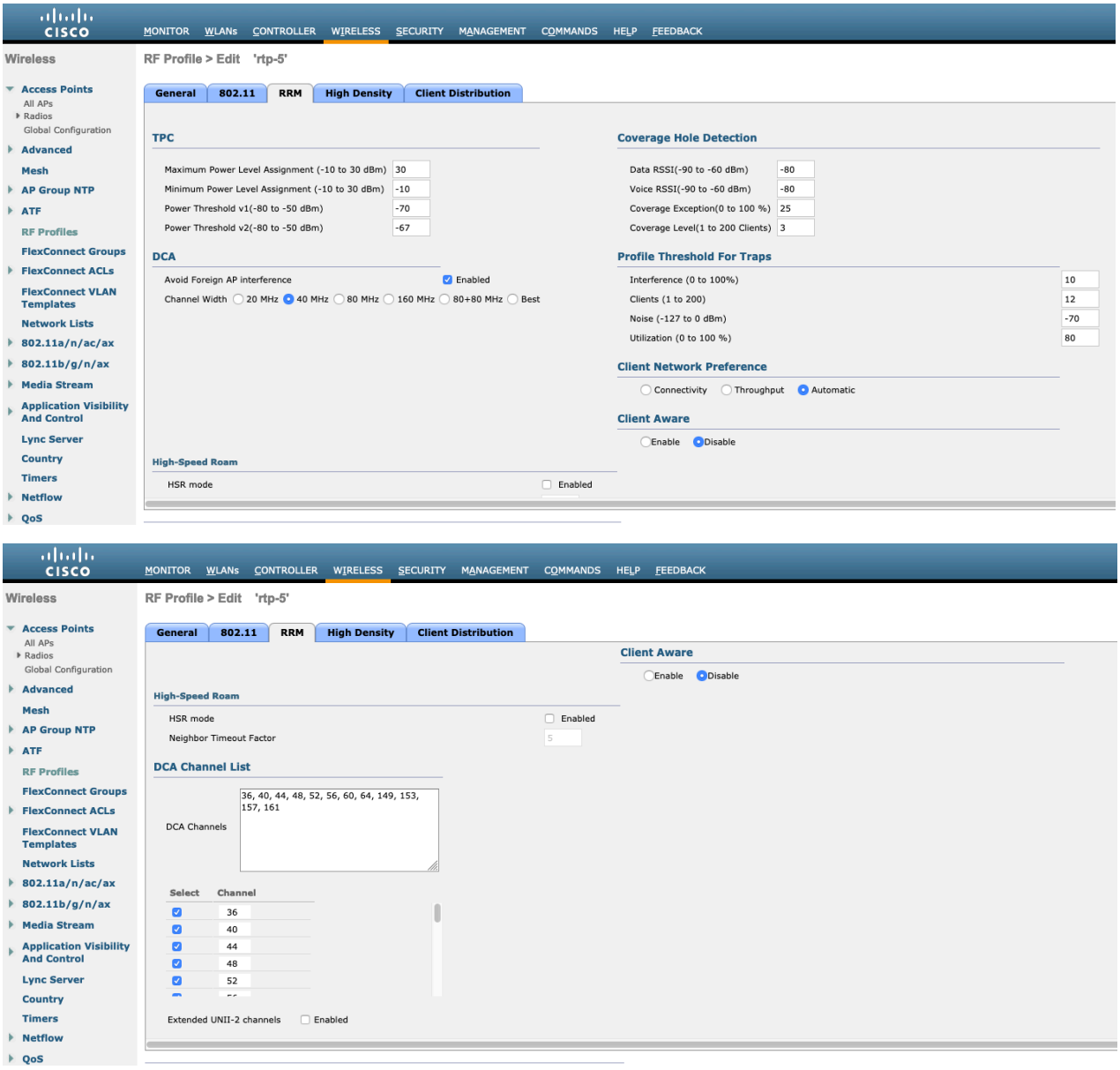
[**802.11**] タブでデータレートを必要に応じて設定します。

12 Mbp を **[必須（Mandatory）]** に 18 Mbps 以上を **[サポート対象（Supported）]** にすることが推奨されます。

ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。

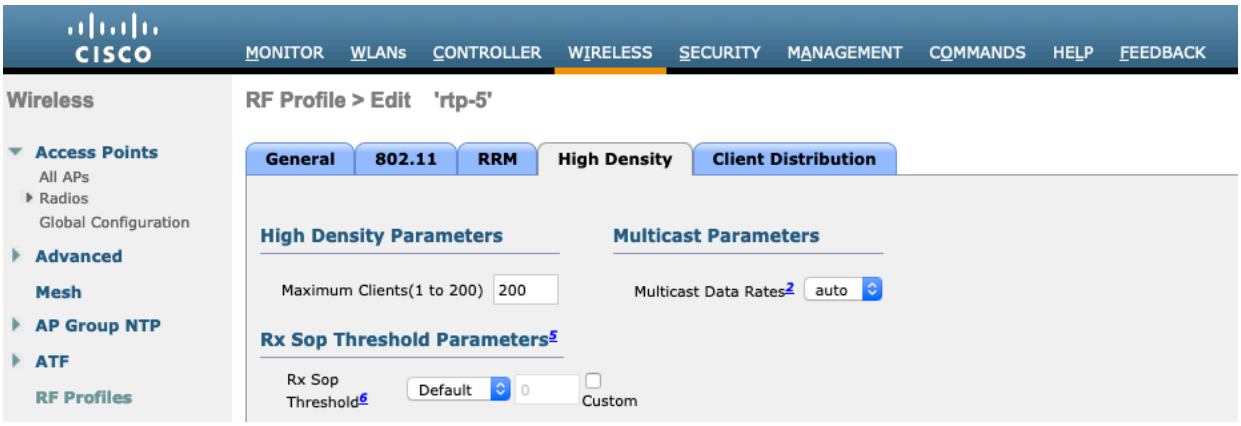


[RRM] タブで、[最大電力レベルの割り当て（Maximum Power Level Assignment）] と [最小電力レベルの割り当て（Minimum Power Level Assignment）] およびその他 [DCA]、[TPC] および [カバレッジホール検出（Coverage Hole Detection）] 設定を構成します。



[高密度（High Density）] タブで、[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）]、[Rx Sopしきい値（Rx Sop Threshold）] を設定できます。

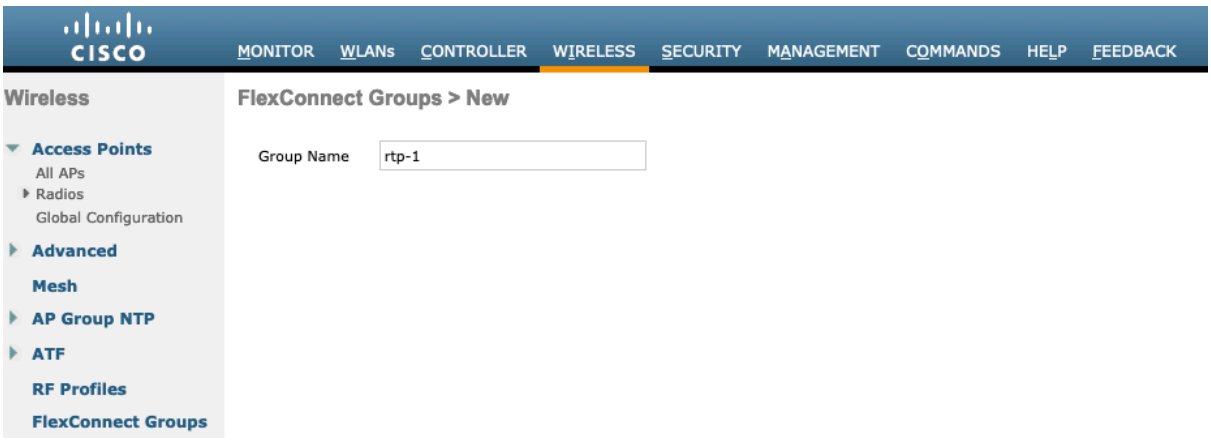
[Rx Sopしきい値（Rx Sop Threshold）] には、デフォルト値を使用することが推奨されます。

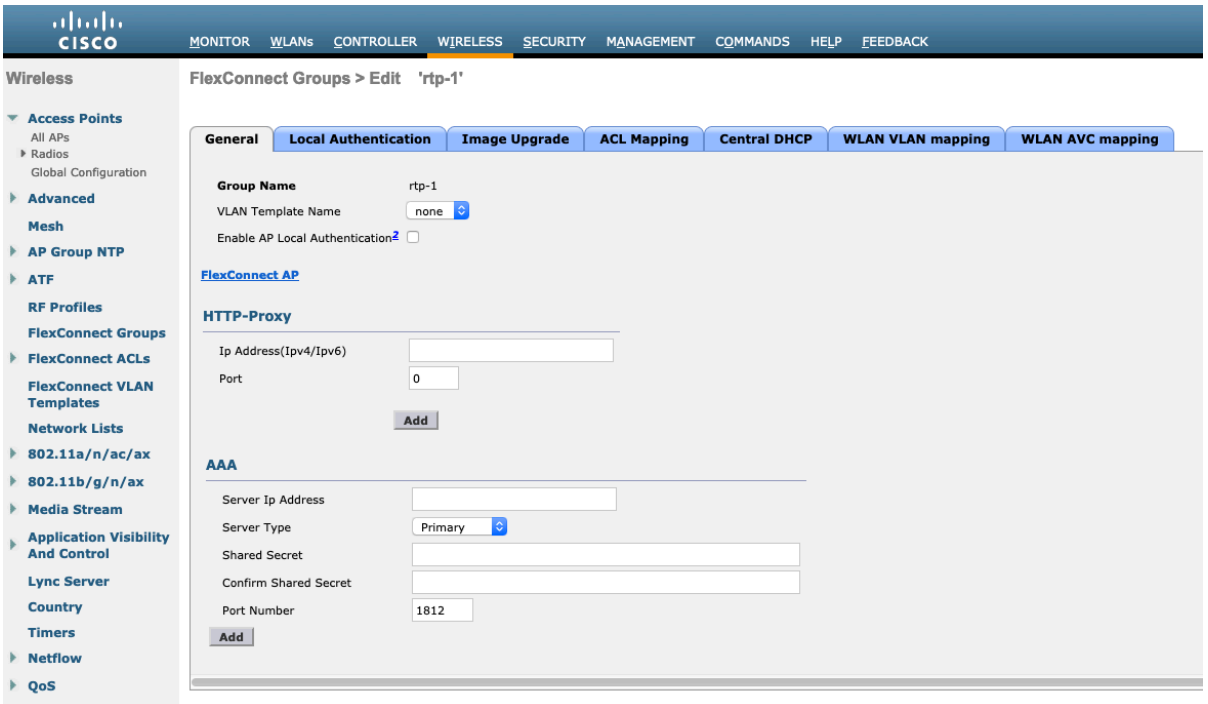


FlexConnect グループ

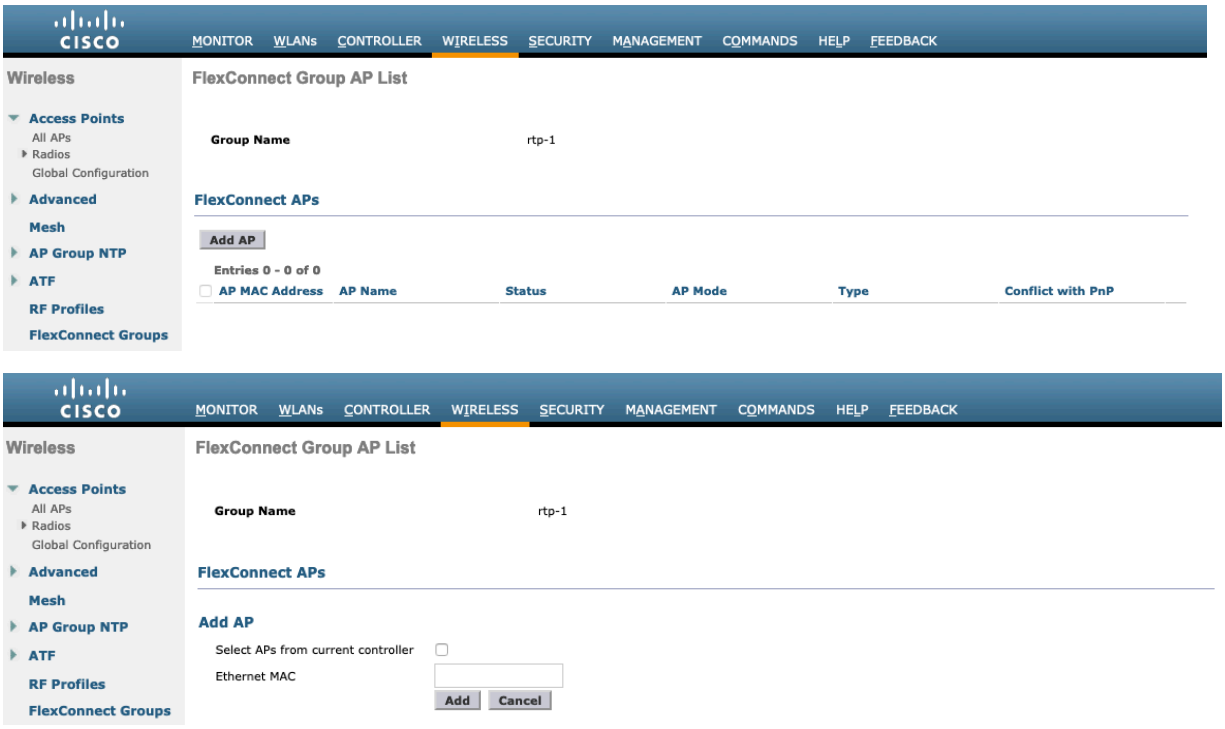
FlexConnect モードに設定されたすべてのアクセスポイントは、FlexConnect グループに追加する必要があります。

802.11r (FT) を利用する場合、シームレスローミングは、同じ FlexConnect グループ内のアクセスポイントにローミングする場合にのみ発生します。



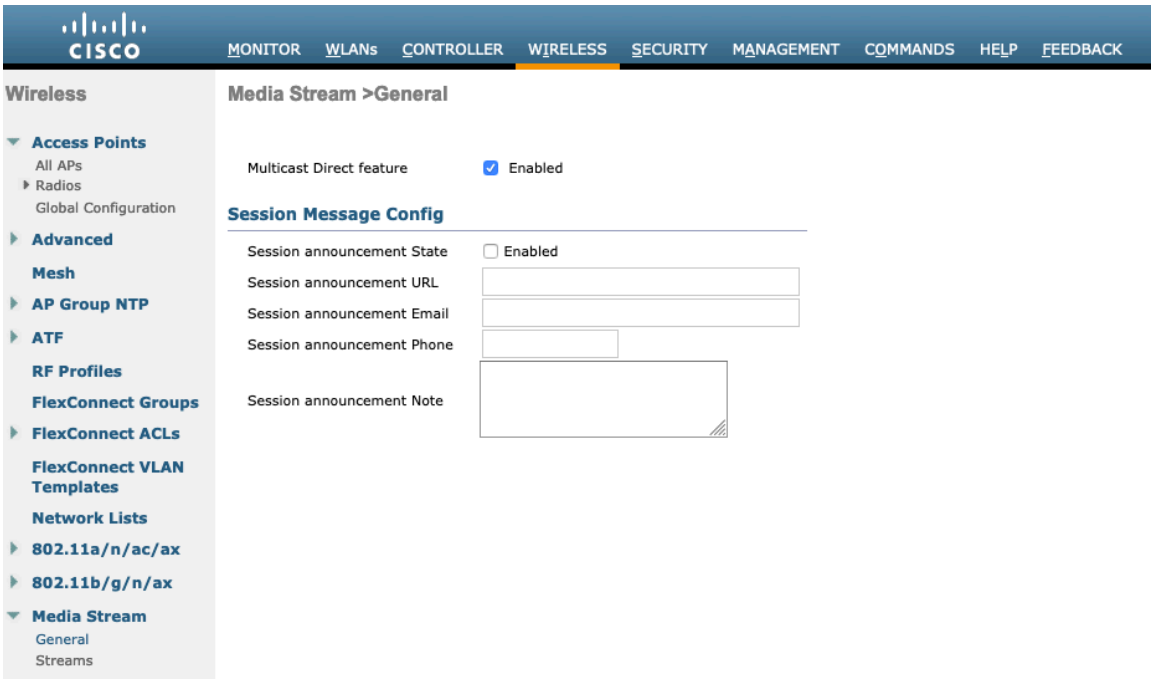


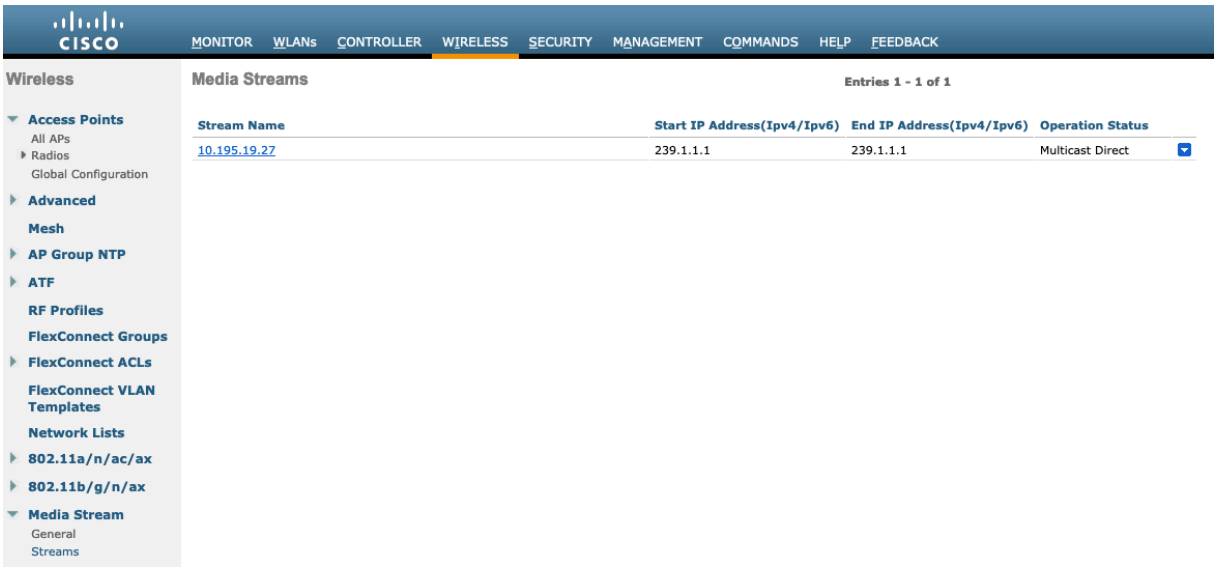
FlexConnect グループごとに許可されるアクセス ポイントの最大数には制限があり、これは WLC モデルによって異なります。



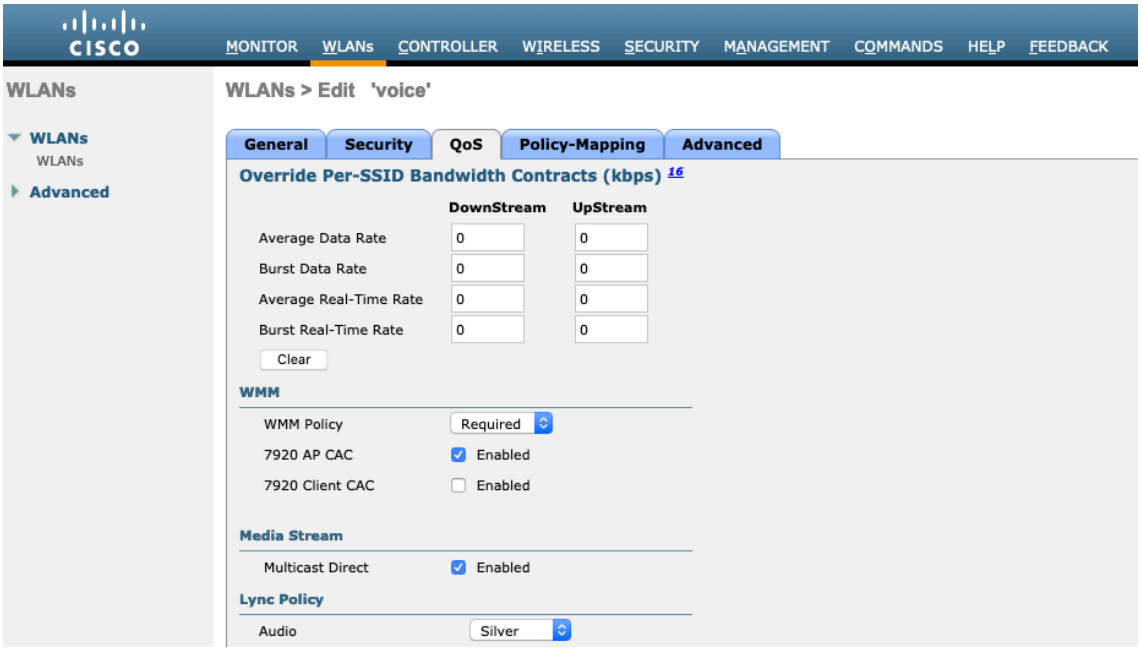
マルチキャストダイレクト

メディア ストリーム設定で **マルチキャスト ダイレクト機能** を有効にする必要があります。





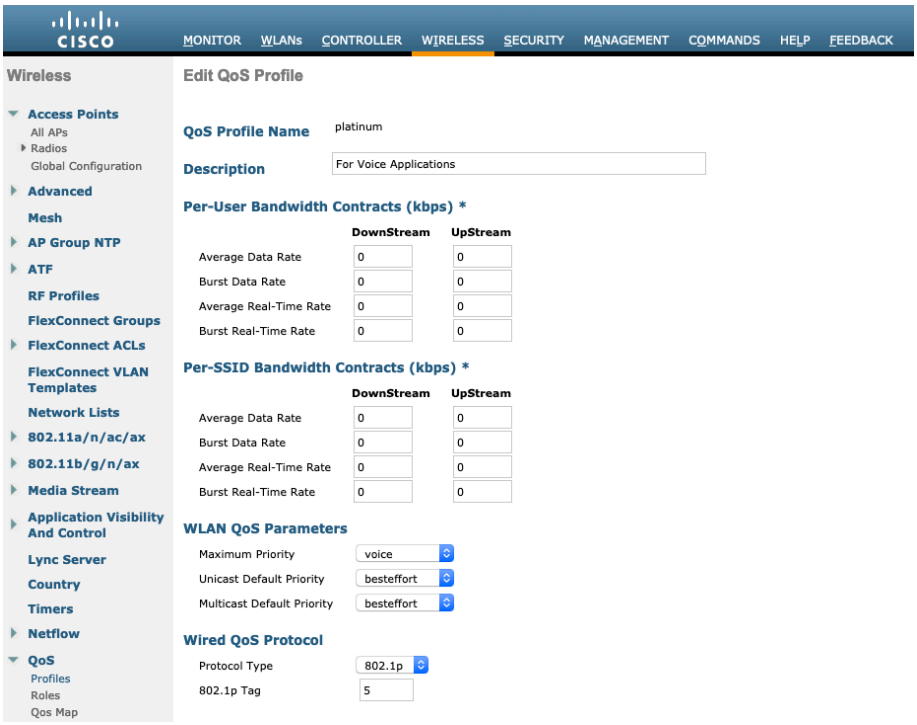
[マルチキャストダイレクト（Multicast Direct）] 機能を有効化したら、WLAN 構成の QoS メニューの **[マルチキャストダイレクト（Multicast Direct）]** を有効にするオプションが表示されます。

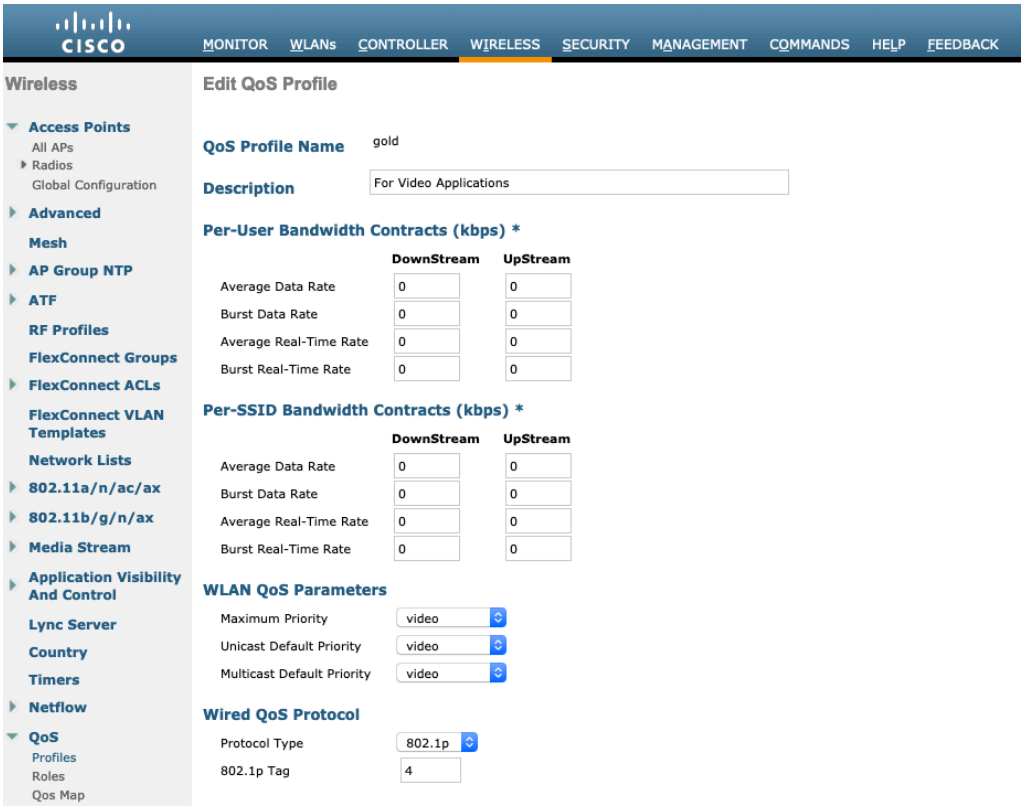


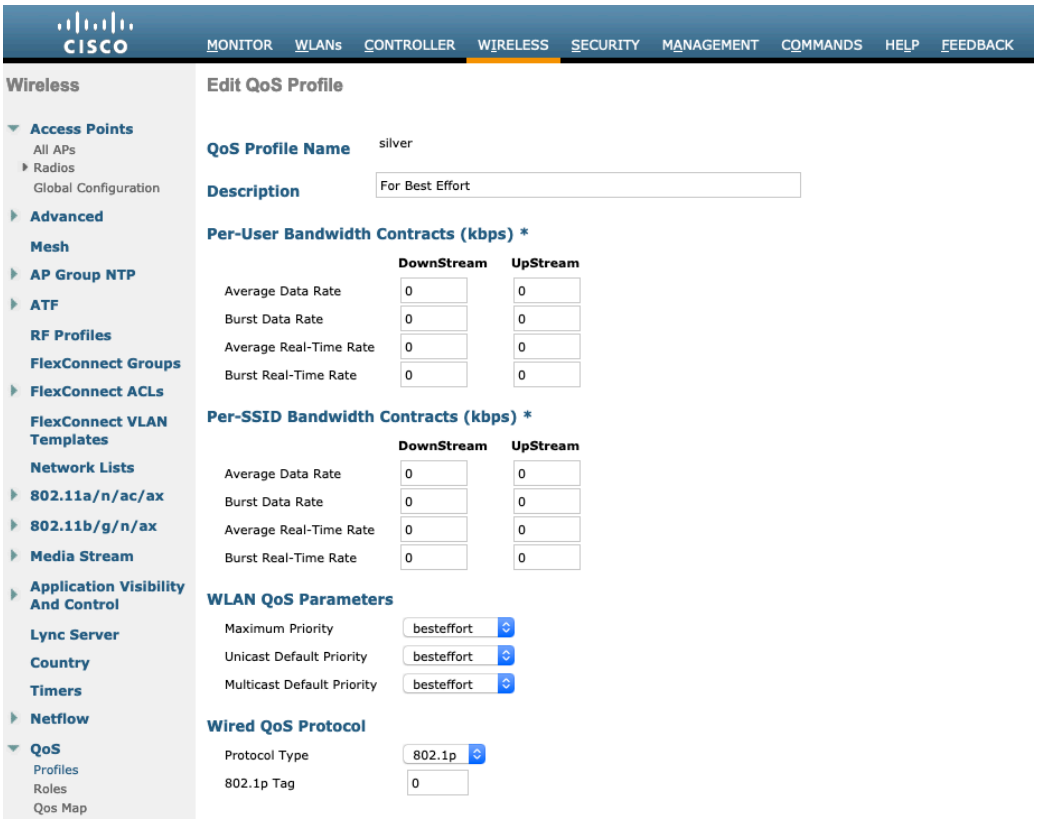
QoS プロファイル

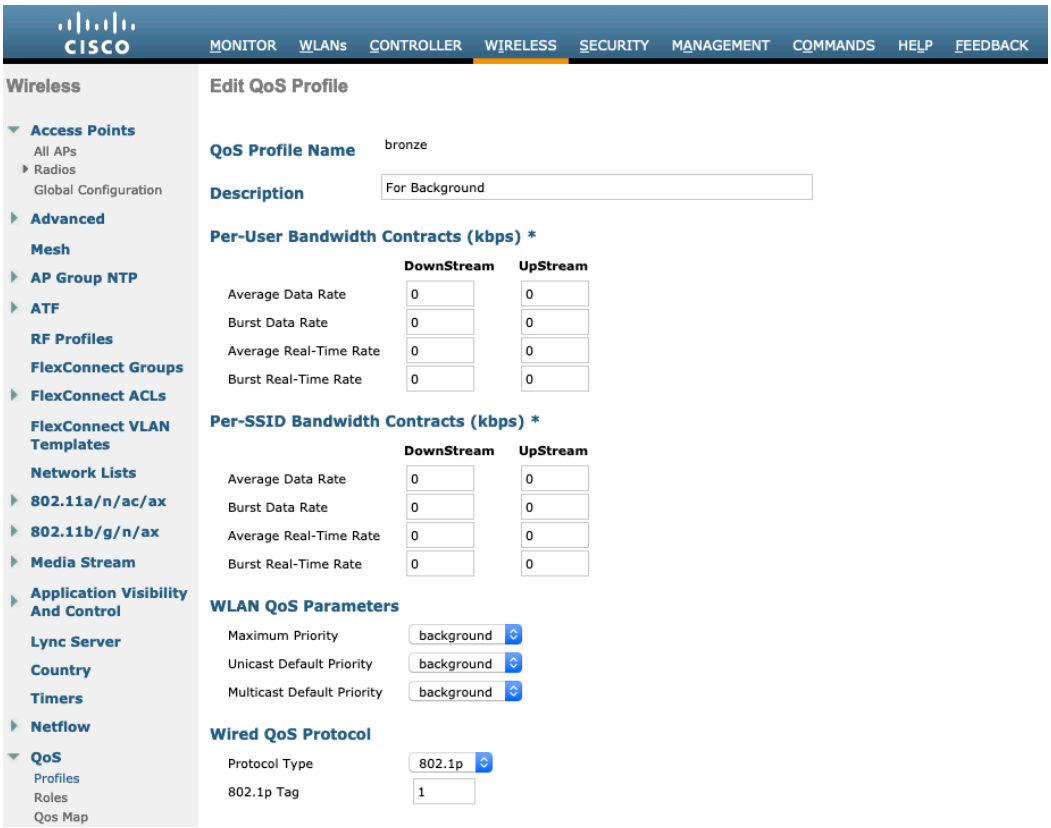
プロトコルタイプで 802.1p を選択して 4 つの QoS プロファイル Platinum、Gold、Silver、Bronze を設定し、各プロファイルに **802.1p** タグを設定します。

- プラチナ = 5
- ゴールド = 4
- シルバー = 2
- ブロンズ = 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
video
Unicast Default Priority
video
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
0
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

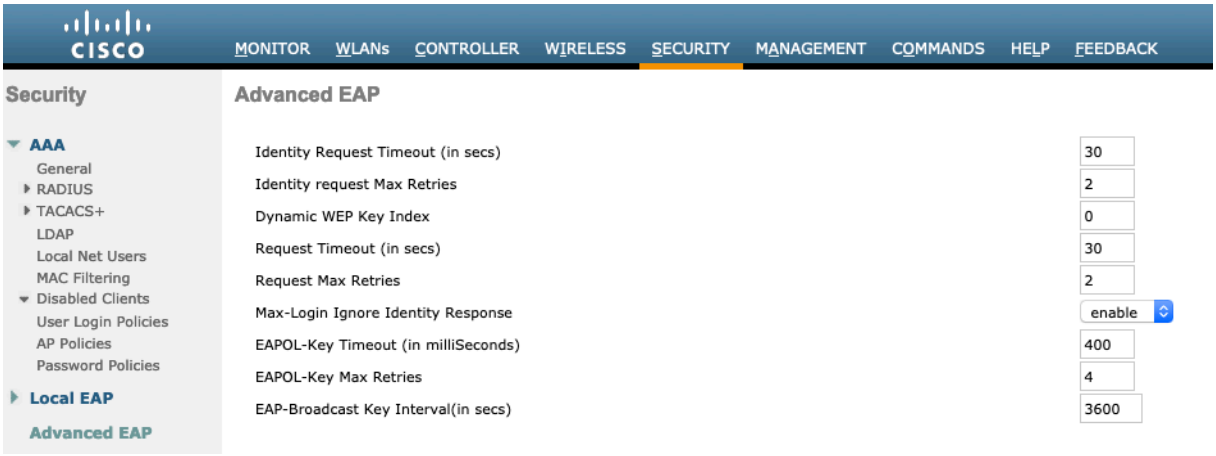

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
Global Configuration
Advanced
Mesh
AP Group NTP
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
Network Lists
802.11a/n/ac/ax
802.11b/g/n/ax
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
Profiles
Roles
Qos Map
Edit QoS Profile
QoS Profile Name
bronze
Description
For Background
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
0
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
background
Unicast Default Priority
Multicast Default Priority
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
1

詳細設定

高度な EAP 設定

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

EAP パラメータを表示または構成するには、**[セキュリティ（Security）]** > **[高度なEAP（Advanced EAP）]** の順に選択します。



コマンドライン経由で Cisco ワイヤレス LAN コントローラの 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 アイデンティティ要求タイムアウト (秒)..... 30
EAP アイデンティティ要求の最大再試行回数..... 2
ダイナミック WEP の EAP キーインデックス..... 0
EAP 最大ログイン Identity Responseの無視..... 有効
EAP 要求のタイムアウト (秒)..... 30
EAP 要求の最大再試行回数..... 2
EAPOL キータイムアウト (ミリ秒)..... 400
EAPOL キーの最大再試行回数..... 4
EAP ブロードキャスト キー間隔..... 3600
```

802.1x を使用する場合、Cisco Wireless LAN Controller の **[EAPリクエストタイムアウト（EAP-Request Timeout）]** を 少なくとも 20 秒に設定する必要があります。

Cisco Wireless LAN Controller の新しいバージョンでは、デフォルトの **[EAPリクエストタイムアウト（EAP-Request Timeout）]** は、2 秒 ~ 30 秒に変更されました。

頻繁な EAP エラーを伴うデプロイの場合、**[EAPリクエストタイムアウト（EAP-Request Timeout）]** を30 秒以下に減らします。

Cisco ワイヤレス LAN コントローラの **EAP リクエストのタイムアウト** を変更するには、telnet または SSH でコントローラに接続してから次のコマンドを入力します。

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

PSK を使用する場合は、**[EAPOLキータイムアウト（EAPOL-Key Timeout）]** を、デフォルトの 1000 ミリ秒から 400 ミリ秒にして、**[EAPOLキー最大試行回数（EAPOL-Key Max Retries）]** をデフォルト値の 2 から 4 に設定します。
802.1x を使用する場合、**[EAPOLキータイムアウト（EAPOL-Key Timeout）]** と **[EAPOLキー最大試行回数（EAPOL-Key Max Retries）]** のデフォルト値で問題ありませんが、これらの値をそれぞれ 400 と 4 に設定することが推奨されます。
EAPOL-Key タイムアウト は 1000 ミリ秒 (1 秒) を超えることはできません。
Cisco Wireless LAN Controller の **[EAPOLキータイムアウト（EAPOL-Key Timeout）]** を変更するには、telnet または SSH でコントローラに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 コントローラで **EAPOL キー最大再試行回数** 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 ブロードキャストキー間隔 が最低でも 3600 秒 (1 時間) に設定されていることを確認してください。
Cisco ワイヤレス LAN コントローラの **EAP ブロードキャストキー間隔** を変更するには、telnet または SSH でコントローラに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

自己免疫

[自動免疫（Auto-Immune）] 機能は、サービス拒否（DoS）攻撃に対する保護のためにオプションで有効にすることができます。
ただし、この [自動免疫（Auto-Immune）] 機能を有効にすると、Voice over Wireless LAN が途切れる可能性があります。 そのため、Cisco Wireless LAN Controller の [自動免疫（Auto-Immune）] 機能を無効にすることが推奨されます。
Cisco Wireless LAN Controller の [自動免疫（Auto-Immune）] 設定を表示するには、telnet または SSH をコントローラに接続して、次のコマンドを入力します。

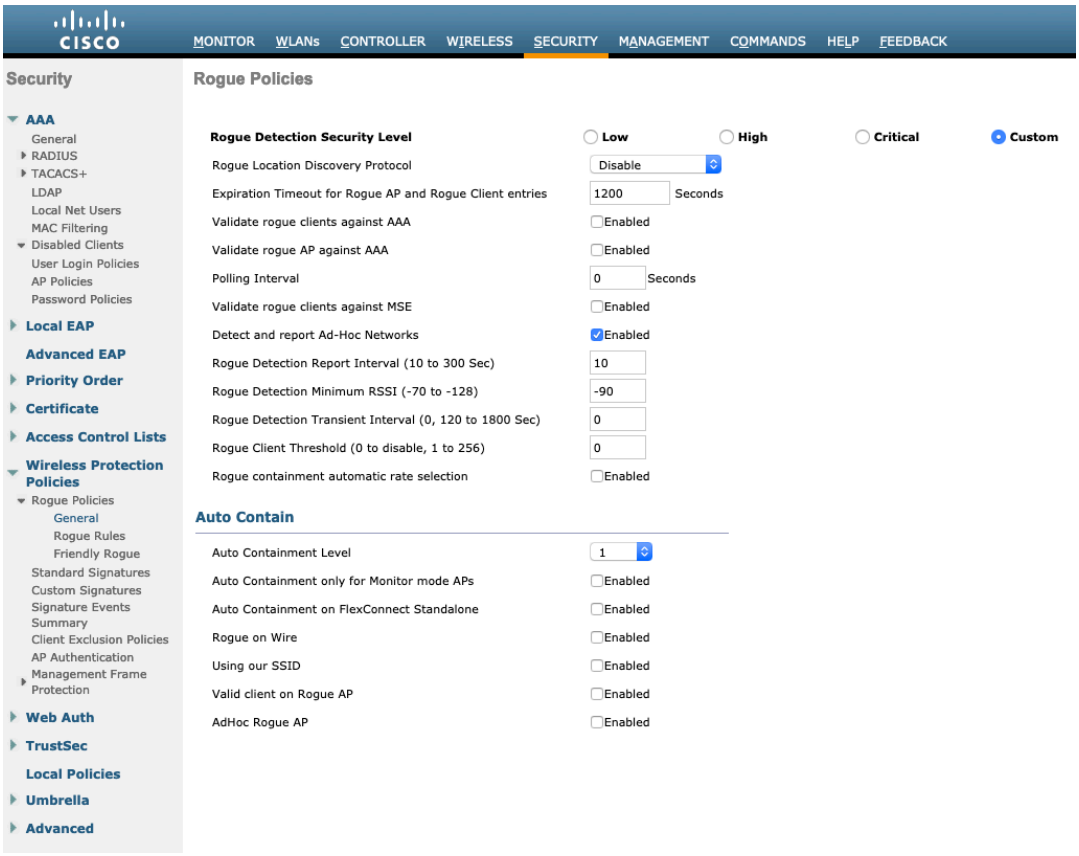
```
(Cisco Controller) >show wps summary
自己免疫
        Auto-Immune..................................... 無効
クライアント除外ポリシー
        Excessive 802.11-association failures..... [有効（Enabled）]
        802.11 認証の失敗が多すぎます..... [有効（Enabled）]
        Excessive 802.1x-authentication..... [有効（Enabled）]
        IP の盗難..... [有効（Enabled）]
        Excessive Web authentication failure..... [有効（Enabled）]
署名ポリシー
        Signature Processing..... [有効（Enabled）]
```

Cisco ワイヤレス LAN コントローラの 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、次のコマンド。

(Cisco Controller) >config wps auto-immune disable

不正ポリシー

[不正デバイスの位置検出プロトコル（Rogue Location Discovery Protocol）] に対してデフォルト値（**[無効（Disabled）]**）を使用することが推奨されます。



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場合、次のガイドラインに従ってください。

- **802.11r** を有効にします。
- **[CCKM]** は [無効（Disabled）] です。
- **Quality of Service（QoS）** SSID ポリシーを、**[プラチナ（Platinum）]** に設定します
- **WMM ポリシー** を **必須に設定します。**
- **セッションタイムアウト** が有効になっており、正しく設定されていることを確認してください
- **[ブロードキャストキー間隔（Broadcast Key Interval）]** を有効にし、正しく設定されていることを確認します。

- **[Aironet IE]** 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) ブロックアクションを無効にする
- **クライアント除外** タイムアウトが正しく設定されていることを確認します
- **[DHCPは必須（DHCP Required）]** を [無効（Disabled）] にします
- **[保護管理フレーム（PMF）（Protected Management Frame (PMF)）]**を**[オプション（Optional）]** または [**WPA3**に必須（Required for WPA3）] に設定します
- **DTIM 期間** を **2 に設定します。**
- **負荷分散** を **無効に設定します**
- **[帯域選択（Band Select）]** を、**[無効（Disabled）]** に設定します
- **IGMP スヌーピング** を **有効に設定します**
- 必要に応じて **データレート** 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、**[音声に最適化（Voice Optimized）]** または **[音声とビデオに最適化（Voice and Video Optimized）]** に設定します
- **[電力制限（Power Constraint）]** が **[無効（Disabled）]** になっているかを確認します
- **[チャンネル切り替えステータス（Channel Switch Status）]** および **[スマートDFS（Smart DFS）]** を有効にします
- **[チャネル切り替えアナウンスモード（Channel Switch Announcement Mode）]** を **[サイレント（Quiet）]** に設定します
- 必要に応じて、**[高いスループット（High Throughput）]** データレートを設定します
- **クリーンエアを有効にする**
- **[マルチキャストダイレクトを有効化（Multicast Direct Enable）]** を有効にします

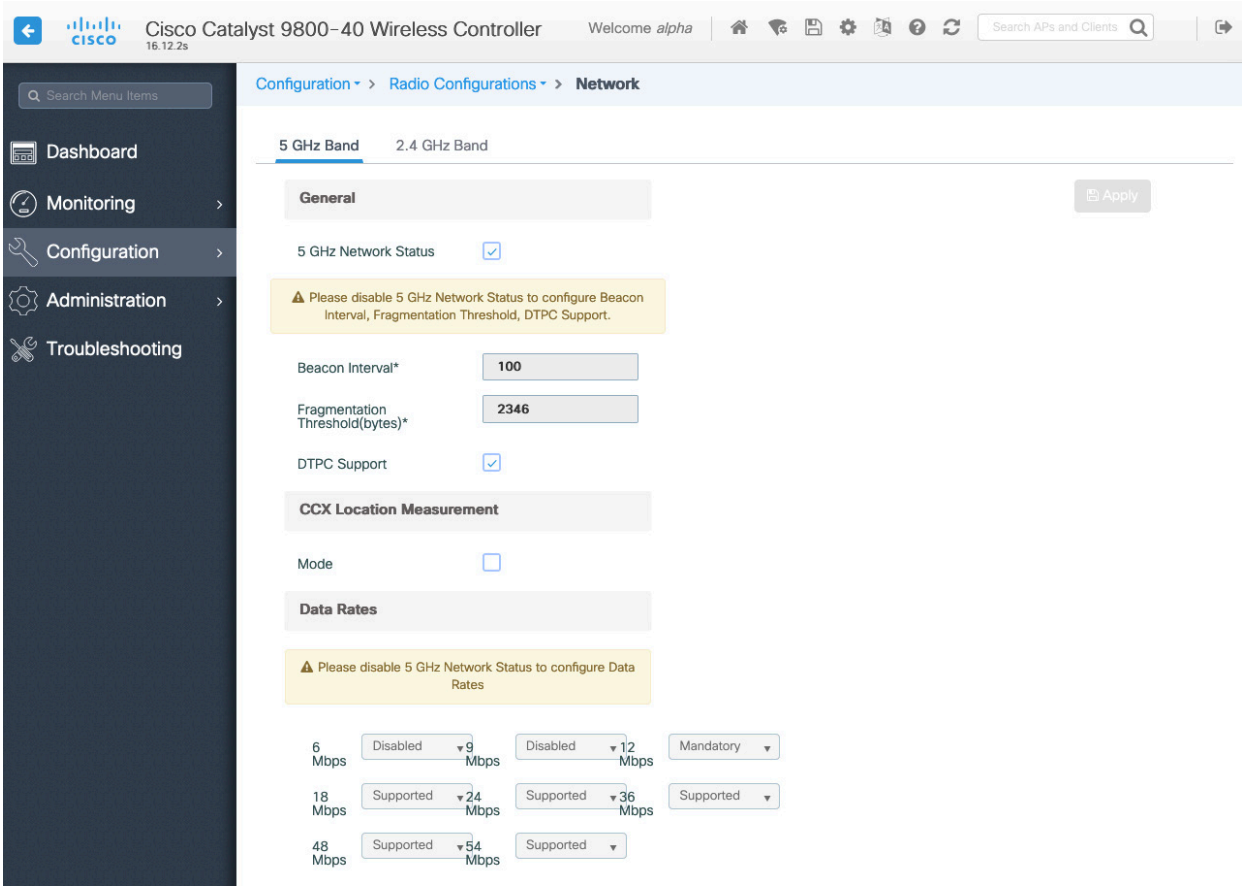
802.11 ネットワーク設定

Cisco Desk Phone 9800 シリーズは 5 GHz 帯のみで使用することをお勧めします。 利用できるチャネル数が多く、2.4 GHz 帯に比べて干渉が少ないためです。

5 GHz を使用するには、**[5 GHzネットワークステータス（5 GHz Network Status）]** を **[有効（Enabled）]** にします。

標識期間 を **100 ms**に設定します。

必須 (基本) レートとして 12 Mbps を設定し、サポートされている (オプション) レートとして 18 Mbps 以上を設定することをお勧めします。 ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。



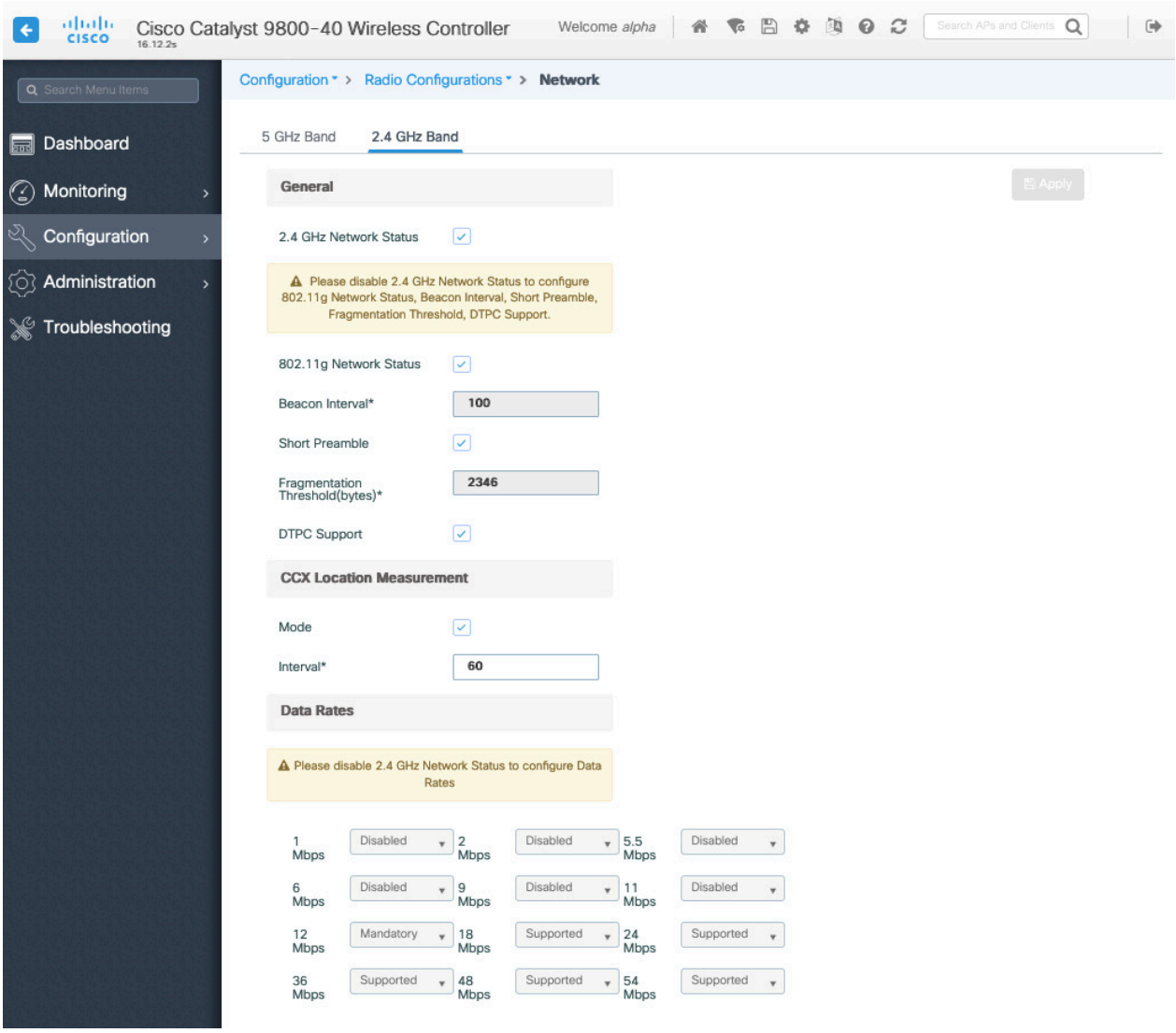
2.4 GHz を使用するには、**[2.4 GHzネットワークステータス（2.4 GHz Network Status）]** と **[802.11gネットワークステータス（802.11g Network Status）]** を **[有効（Enabled）]** にします。

標識期間を 100 ms に設定します。

ワイヤレス LAN でロングプリアンブルが必要なレガシークライアントが無い場合、アクセスポイントで設定した 2.4 GHz 無線設定で、**[ショートプリアンブル（Short Preamble）]** を **[有効（Enabled）]** にします。 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で、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。

12 Mbps を必須（基本）レートとして、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と想定して、18 Mbps 以上をサポート対象（オプション）レートとして設定することが推奨されます。 ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を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、11 Mbps を必須 (基本) レートとして設定し、12 Mbps 以上をサポート (オプション) として設定する必要があります。



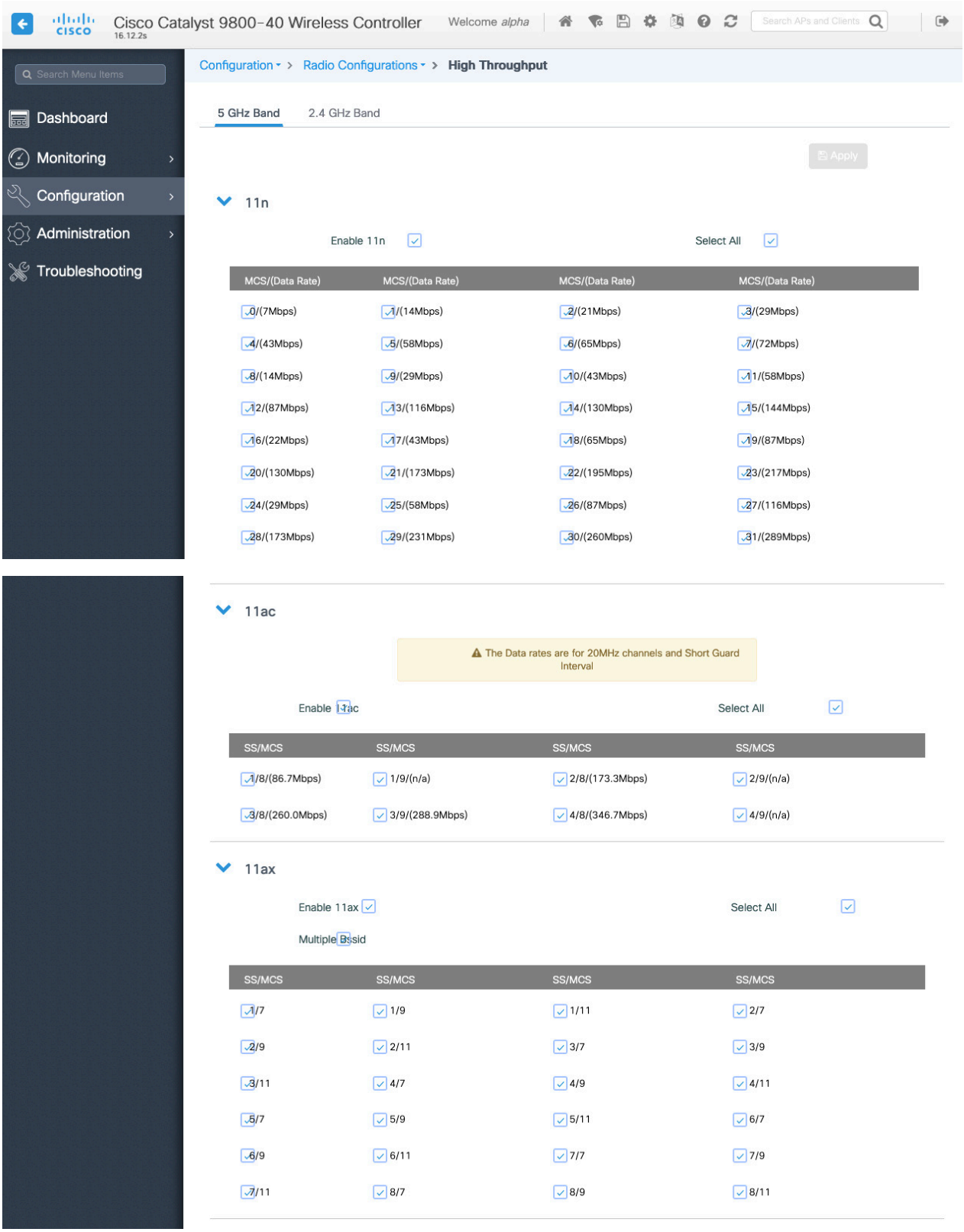
高スループット (802.11n/ac)

802.11n データレートはラジオ（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 にのみ適用されます。

[WMM] を **[WPA2/WPA3(AES)]** に設定し 802.11n/ac データレートを使用できるかを確認します。

Cisco Desk Phone 9800 シリーズは、HT MCS 0 – MCS 7 と VHT MCS 0 – MCS 9 1SS のみをサポートしますが、より高いデータレートを有効活用できる MIMO アンテナテクノロジ搭載の同じ帯域周波数を使用するその他の 802.11n/ac がある場合、より高い MCS レートをオプションで有効化できます。

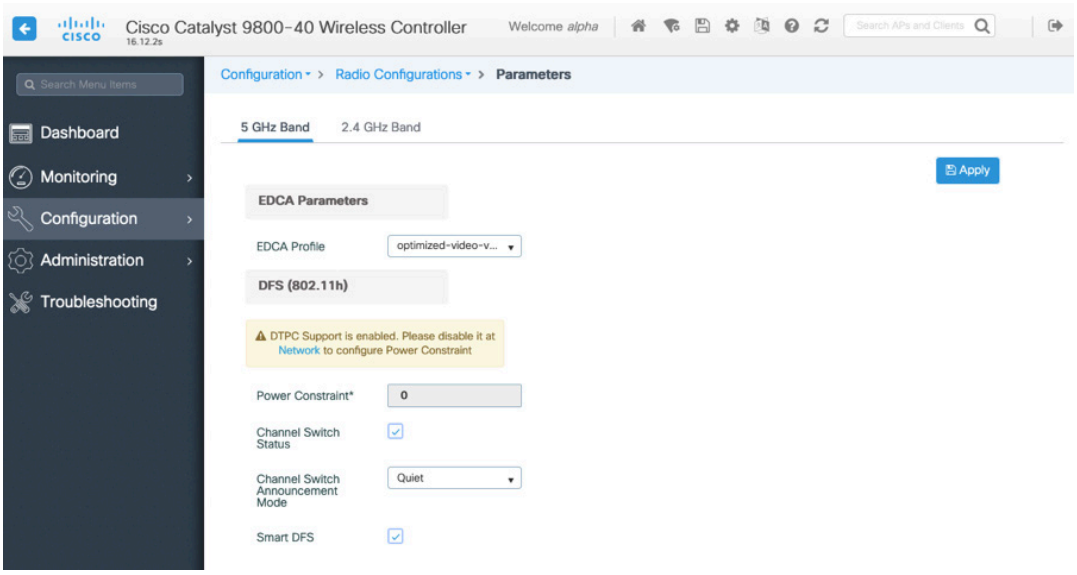


パラメータ

[EDCAパラメータ（EDCA Parameters）] セクションで、EDCA プロファイルを、使用する周波数帯に応じて、5または 24 GHz に対して、**[Optimized-voice]** または **[Optimized-video-voice]** に設定します。

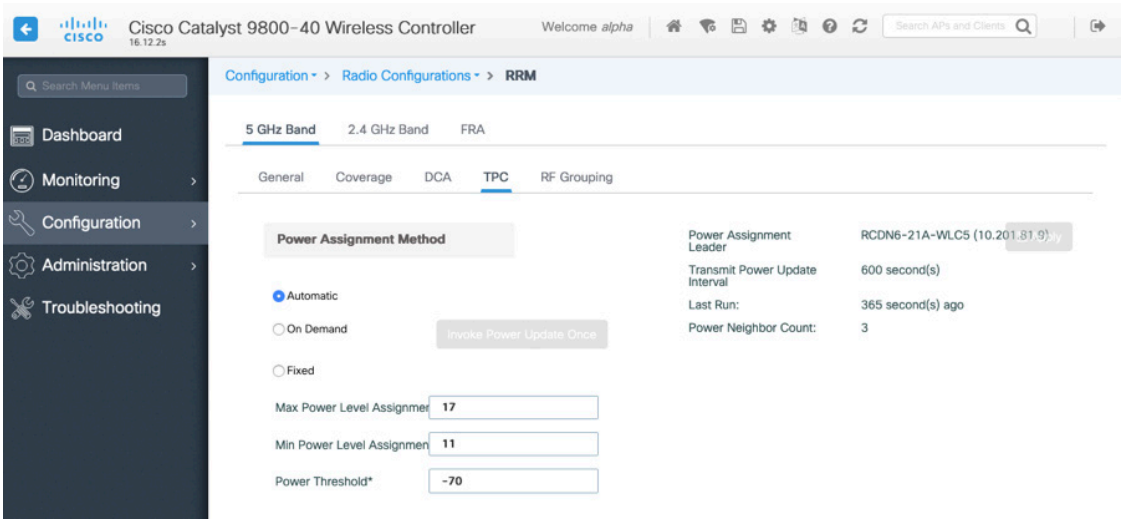
DFS (802.11h) セクションで、 **Power Constraint** を未構成のままにするか、0 デシベルに設定する必要があります。

チャンネル切り替えステータス および **スマート DFS** で **有効** である必要があります。
[チャネル切り替えアナウンスモード（Channel Switch Announcement Mode）] を **[サイレント（Quiet）]** に設定します。



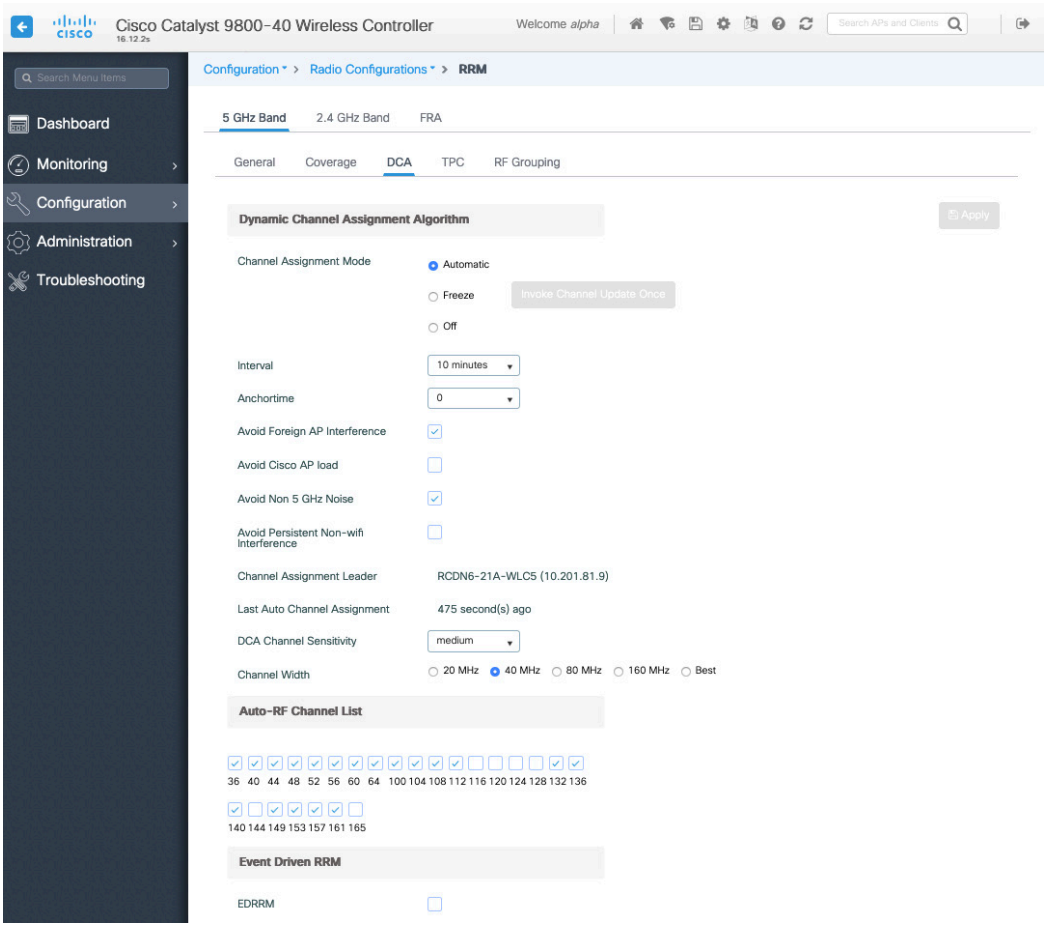
RRM

チャネルと送信電力の設定を管理するには、自動割り当て方法を有効にすることをお勧めします。
使用する周波数帯域に応じて、5 または 2.4 GHz のアクセスポイント送信電力レベル割り当て方法を設定します。
電力レベルの自動割り当てを使用する場合、最大および最小の電力レベルを指定することができます。

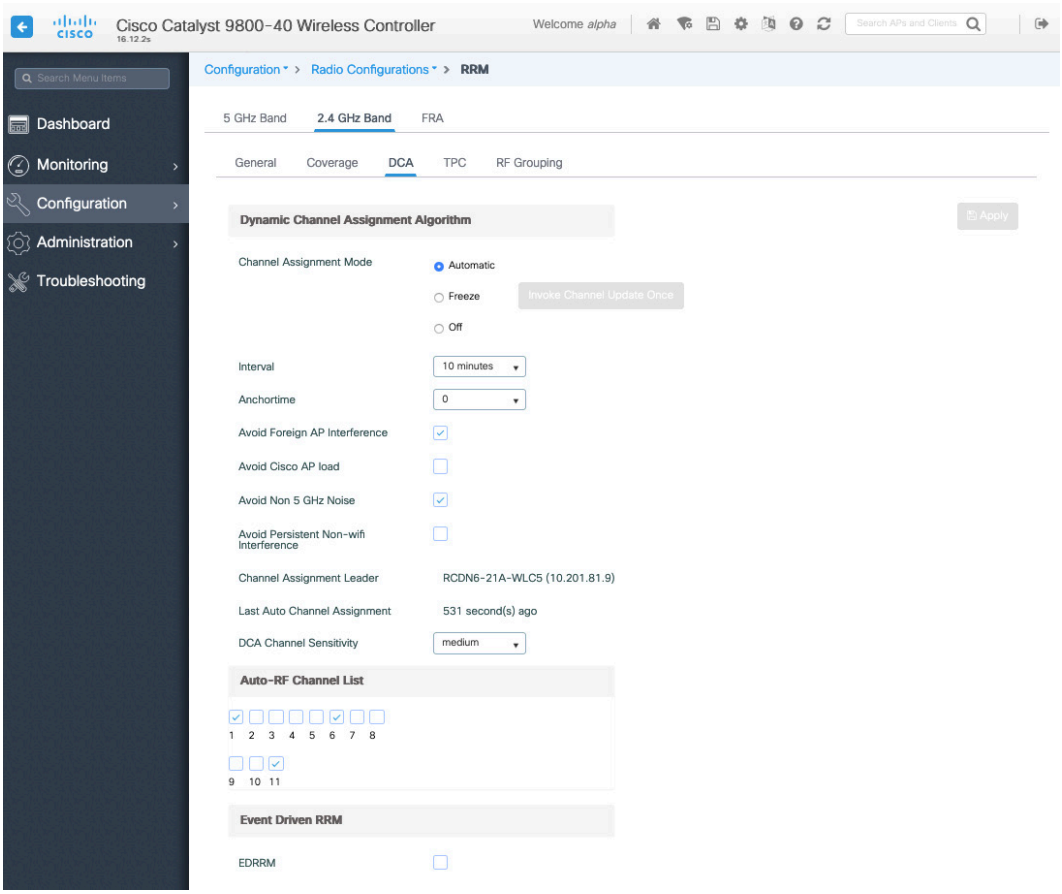


5 GHz を使用する場合、多くのチャンネルをスキャンすることによるアクセスポイント検出の遅延を避けるために、チャンネル数を制限することをお勧めします (例: 12 チャンネルのみ)。

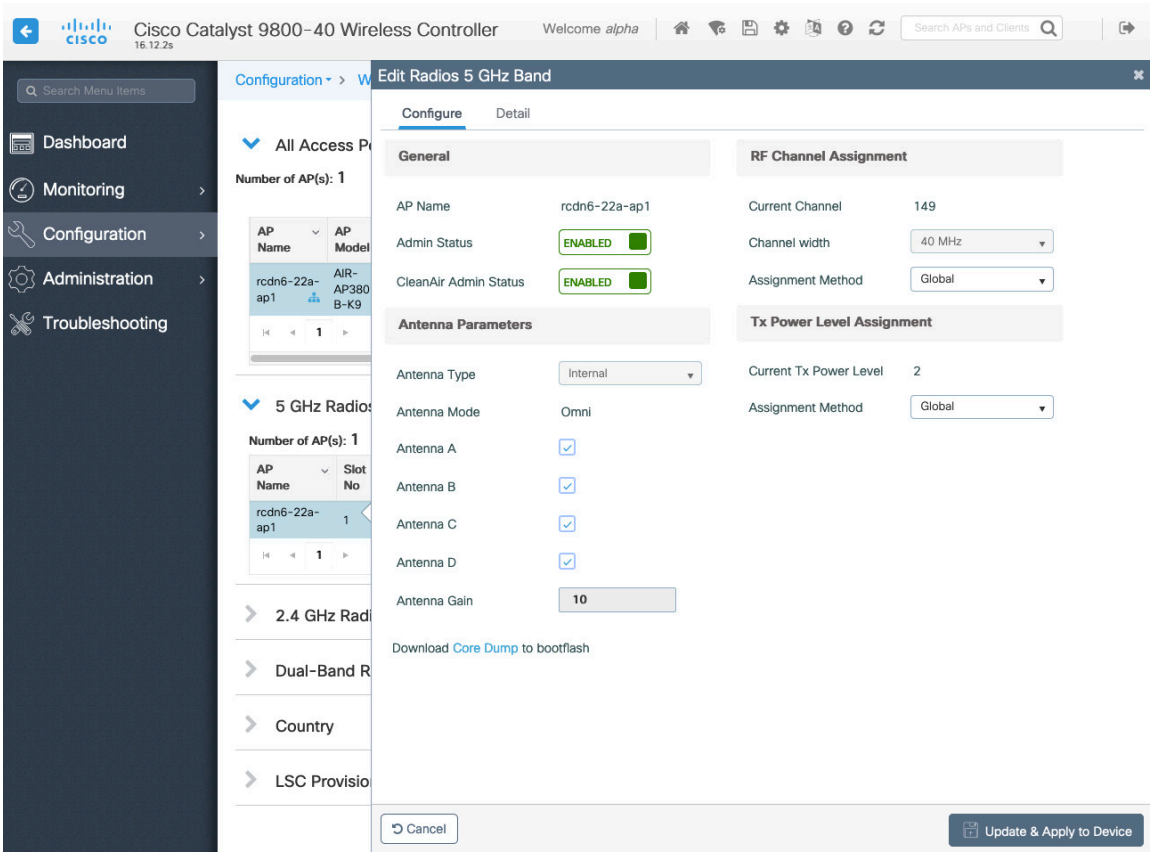
5 GHz チャネル幅は、Cisco 802.11n アクセスポイントを使用する場合は 20 MHz または 40 MHz として、Cisco 802.11ac アクセスポイントを使用する場合は 20 MHz、40 MHz、または 80 MHz として構成できます。
すべてのアクセスポイントで同じチャネル幅を使用することを推奨します。



2.4 GHz を使用する場合、チャネル リストでチャネル 1、6、および 11 のみを有効にする必要があります。

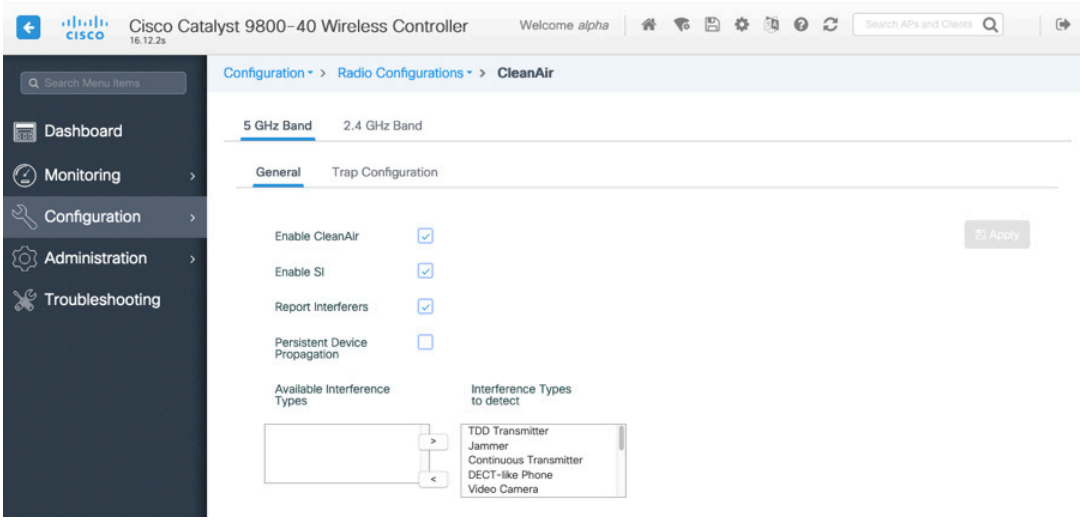


利用する周波数に周波数帯に応じて、5GHz または 2.4GHz のいずれかで動的チャネルと送信電力の割り当てを使用するように、個々のアクセスポイントは全体設定をオーバーライドするように設定できます。
その他のアクセスポイントは、自動割り当てメソッドと、静的に設定したアクセスポイントのアカウントに対して有効化できます。
これは、その地域で断続的な干渉源がある場合に必要になります。
5 GHz チャネル幅は、Cisco 802.11n アクセスポイントを使用する場合は 20 MHz または 40 MHz として、Cisco 802.11ac アクセスポイントを使用する場合は 20 MHz、40 MHz、または 80 MHz として構成できます。
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。



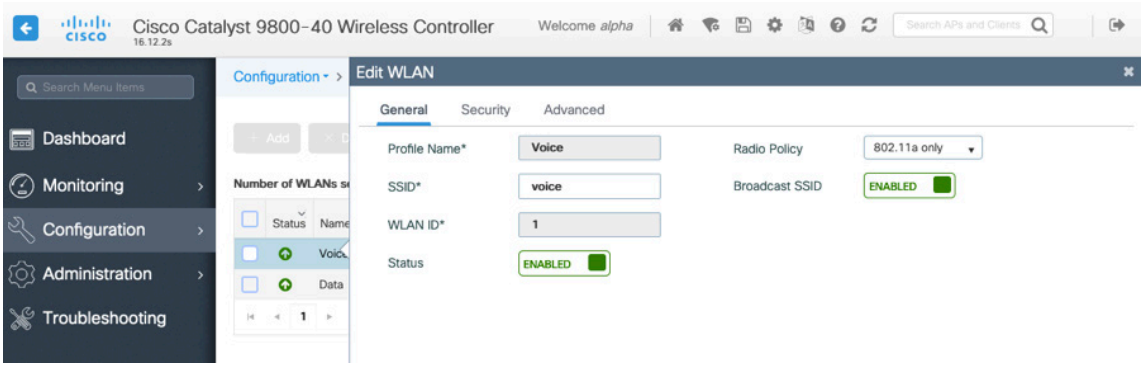
クリーンエア

[CleanAirを有効化（Enable CleanAir）] チェックボックスは、既存の干渉を検出する CleanAir テクノロジ搭載の Cisco アクセスポイントを使用する際は、オンにします。

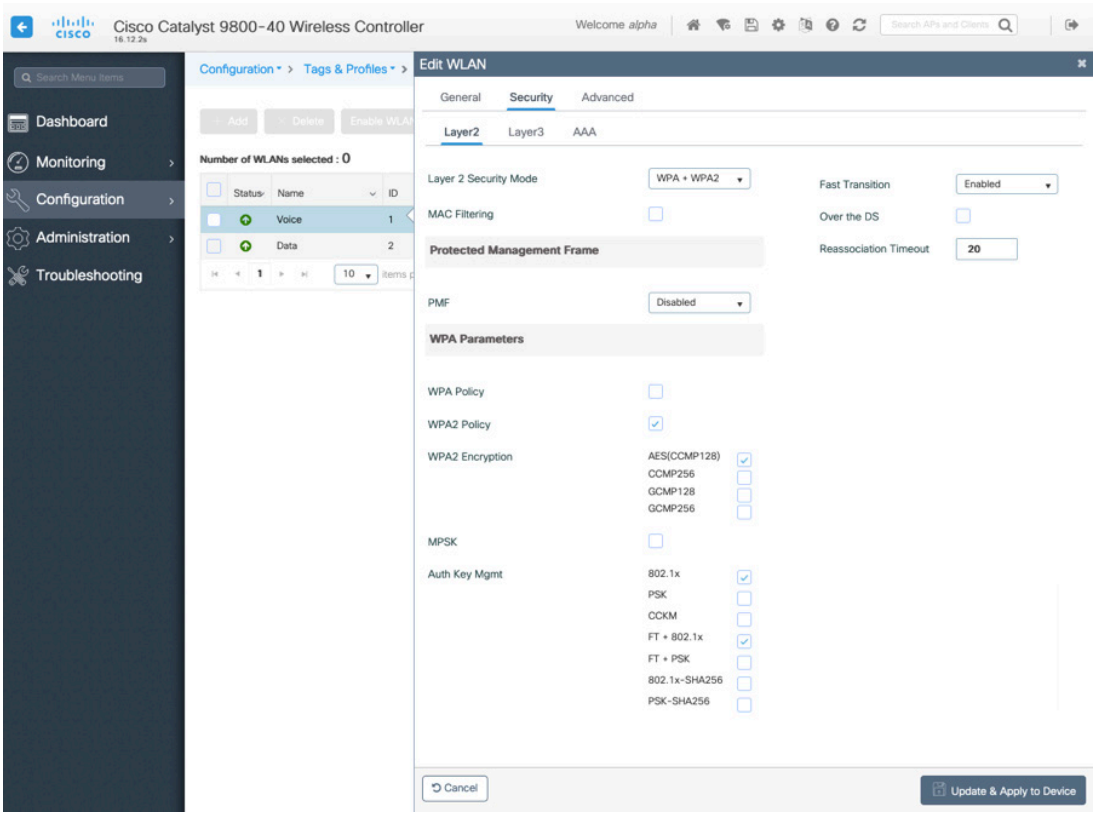


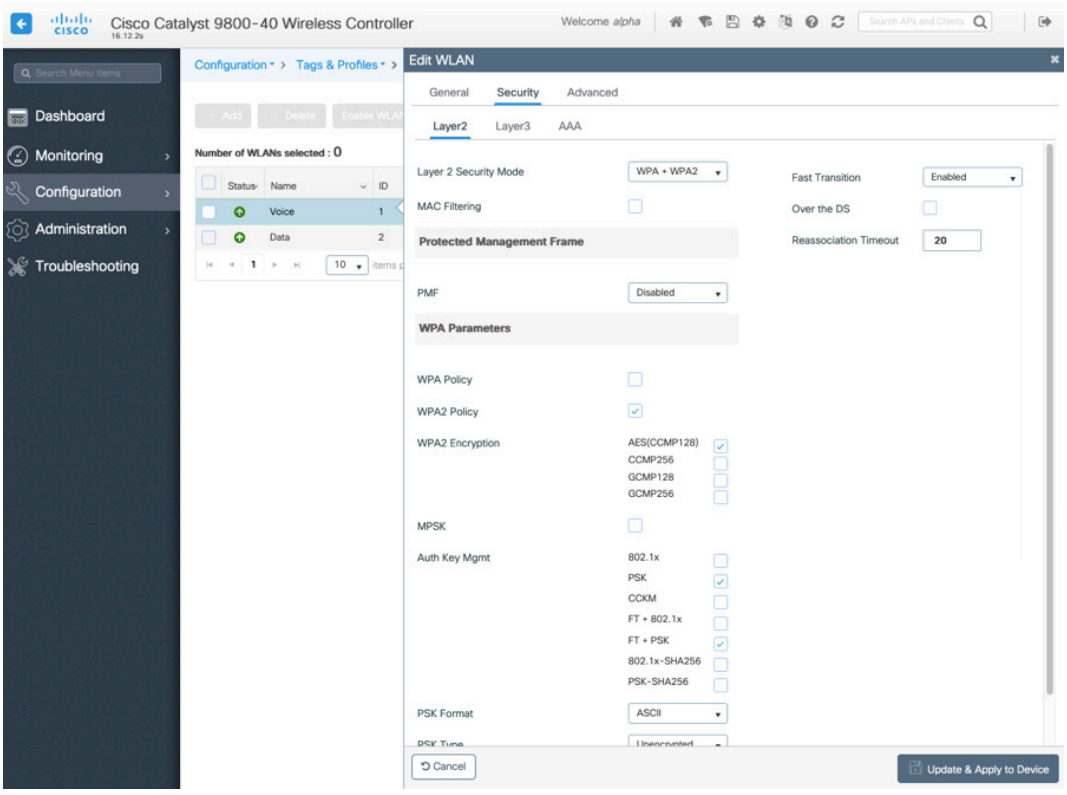
[IVR設定(WLAN Settings)]

Cisco Desk Phone 9800 シリーズには別の SSID を割り当てることを推奨します。
音声対応 Cisco ワイヤレス 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 を使用することもできます。
特定の 802.11 無線タイプのみ（例: 802.11a のみ）を適用できるように Cisco Desk Phone Esrepsso が使用する SSID を設定します。
Cisco Desk Phone 9800 シリーズは 5 GHz 帯のみで使用することを推奨します。 2.4 GHz 帯に比べて多くのチャネルが利用でき、干渉が少ないためです。
選択した SSID が他のワイヤレス LAN で使用されていないことを確認してください。これは、電源オン時またはローミング中に障害につながる可能性があり、特に異なるセキュリティタイプが使用されている場合にはその可能性が高まります。



高速セキュア ローミングに 802.11r (FT) を使用するには、[**高速移行**] を [**有効**] に設定します。
Over the Distribution System 方法ではなく、Over the Air方法を使用するには、**[Over the DS]** チェックボックスをオフにすることが推奨されます。
保護された管理フレーム は **任意** または **必須**に設定してください。
AES(CCMP128) 暗号化の WPA2/WPA3 ポリシーを有効にし、802.1x、PSK または SAE のどちらかを使用するかに応じて、認証キー管理タイプの 802.1x、PSK または SAE を使用するかを選択します。

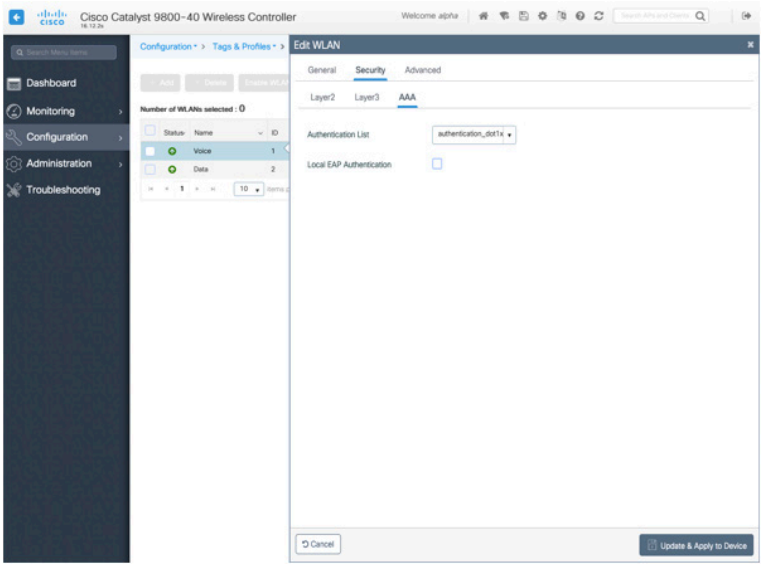




802.11r (FT)、PSK または SAE を有効にして、さまざまなタイプの音声クライアントに同じ SSID を使用することもできます。

802.1x または PSK/SAE のどちらが利用されているかによって異なります。

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



Aironet IE は **無効にする必要があります。**

ピアツーピア (P2P) ブロックアクション は **無効**にする必要があります。

Cisco Desk Phone 9800 シリーズ または WMM 対応電話が SSID を使用している場合のみ**[WMMポリシー（WMM Policy）]** を **[必須（Required）]** に設定します。

WLAN に WMM 以外のクライアントが存在する場合、こ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。

その他の 非 WMM クライアントは、Cisco Desk Phone 9800 シリーズとおなじ SSID を使用して、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、または AP 無線ごとの最大クライアント接続は、必要に応じて設定できます。

[オフチャネルスキャンの保留（Off Channel Scanning Defer）] は、特定のキューのスキャンとスキャンの保留時間を調整するためにオンにできます。

キュー 4-6 の保留優先順位を有効にすることをお勧めします。

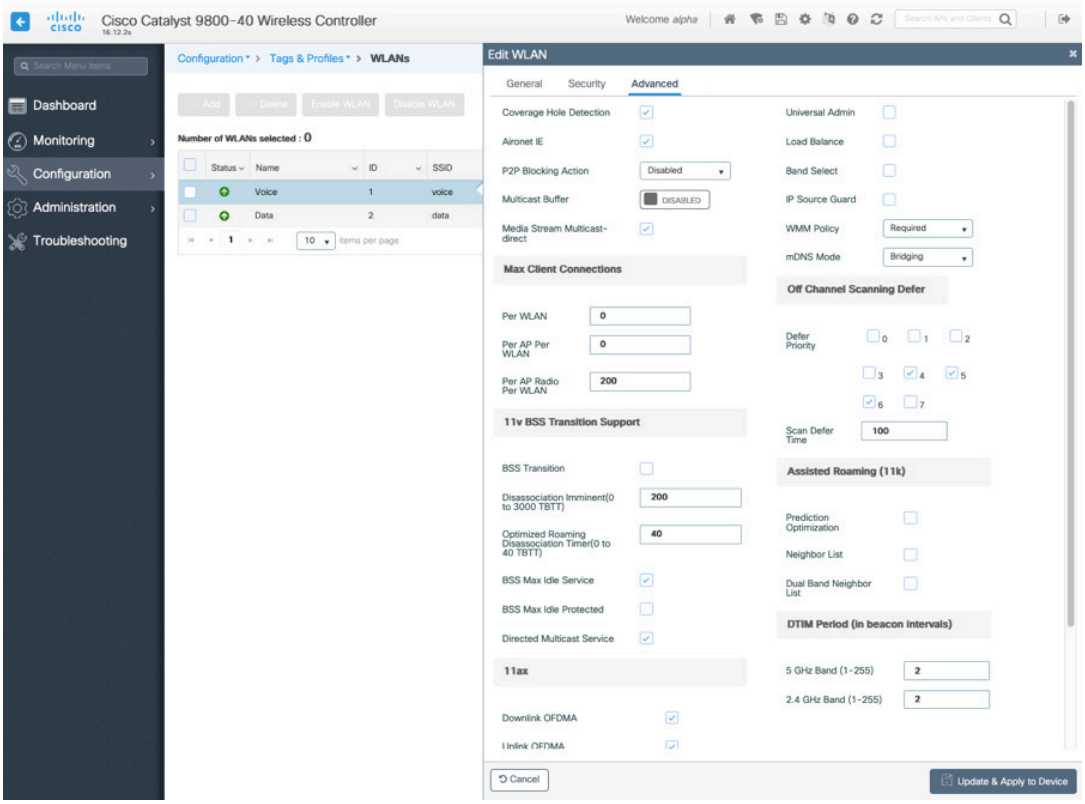
アクセスポイントへのベスト エフォート アプリケーションを頻繁に使用するか、優先アプリケーション（音声および通話コントロールなど）の DSCP 値を保存しない場合、オフチャネルスキャンを保留し、スキャン保留時間を長くするために、低いキュー優先度（0-3）と高いキュー優先度（4-6）を有効にすることが推奨されます。

頻繁な EAP エラーを伴うデプロイの場合、キュー優先度 7 を有効にして、EAP 交換中にオフチャネルスキャンを延期することが推奨されます。

[負荷分散（Load Balance）] と **[帯域選択（Band Select）]** を無効にします。

ビーコン期間が **100 ms** の 2 の**DTIF 期間**を使用します。

802.11k および 802.11v はデフォルト設定のままにします。

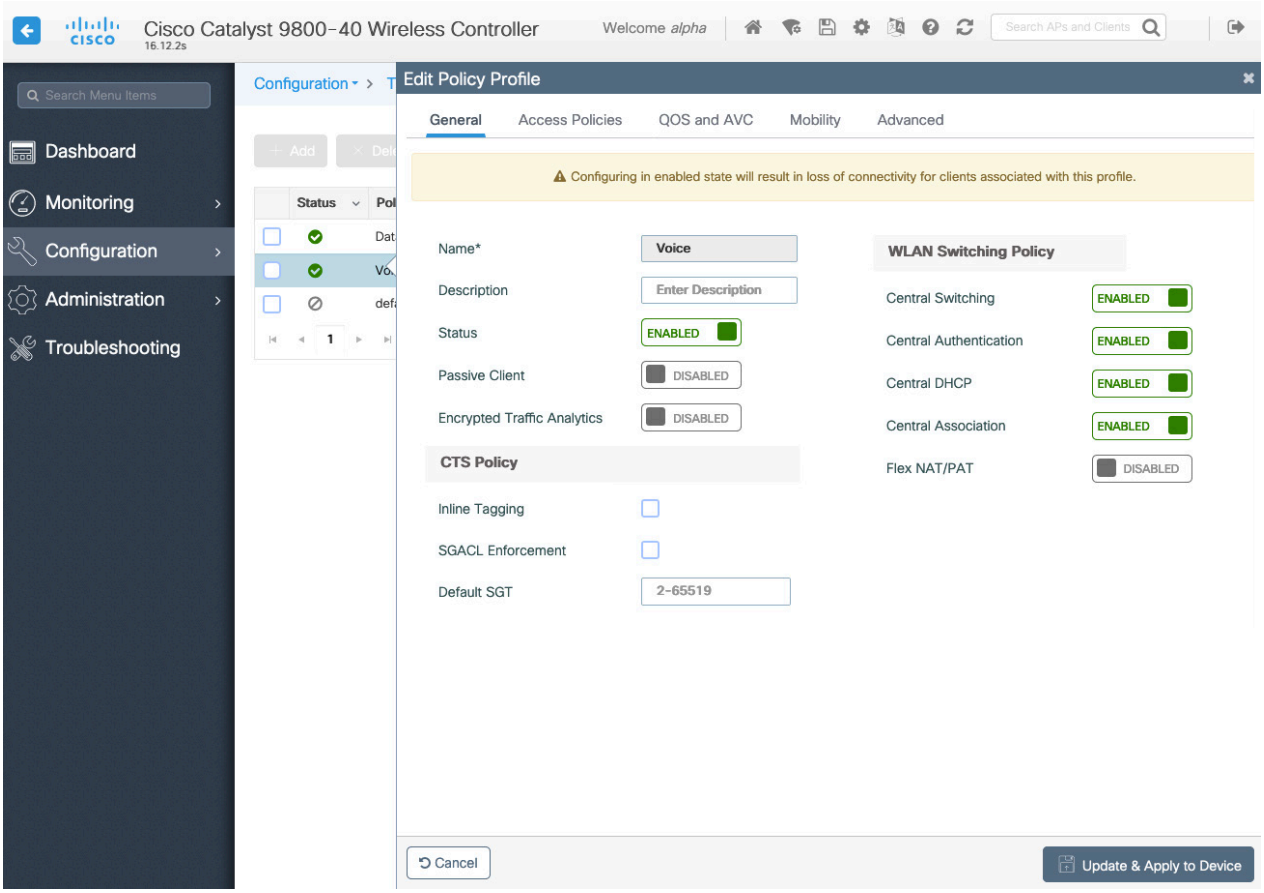


ポリシープロファイル

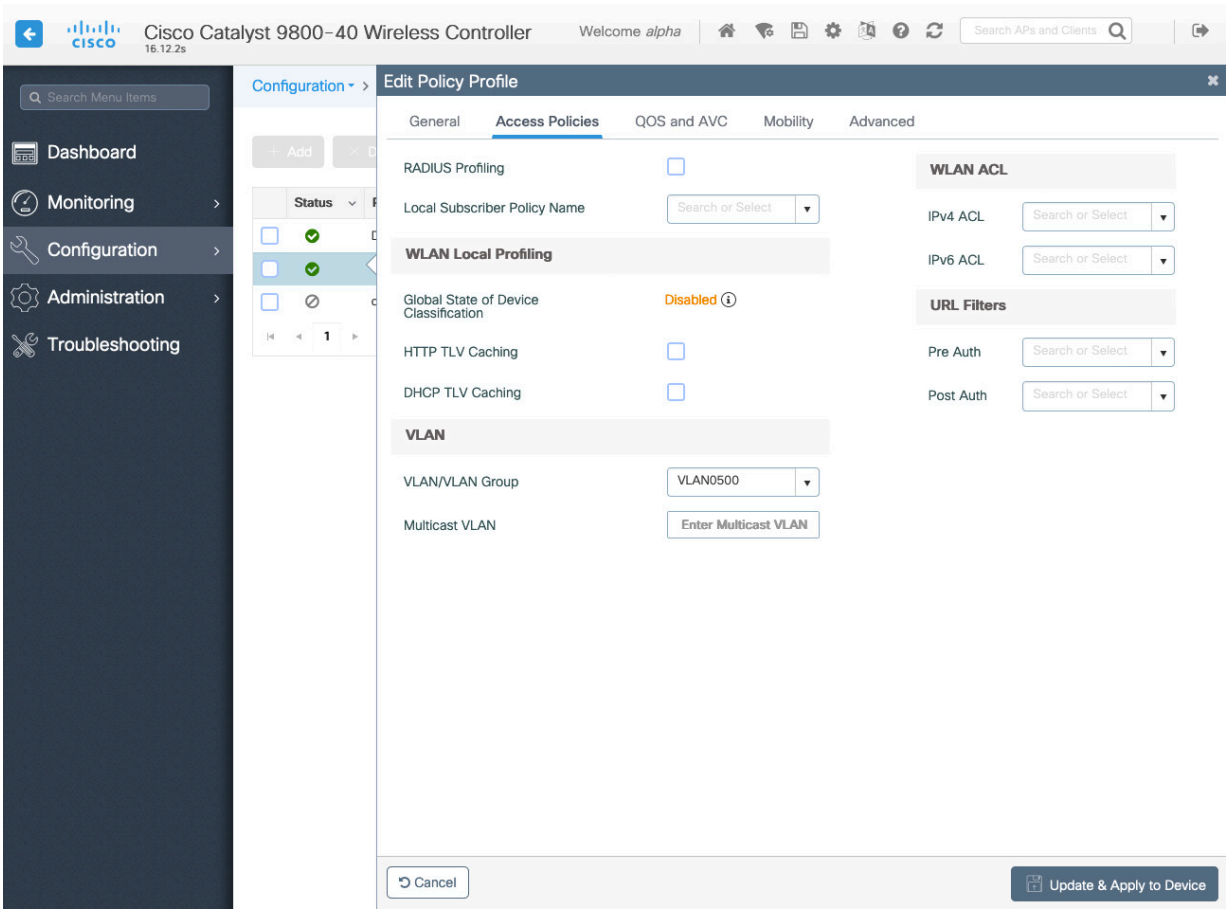
ポリシー プロファイルは、アクセス、QoS、モビリティ、および詳細設定に関する追加設定を定義するために使用されます。

その後、[ポリシープロファイル（Policy Profiles）] は [ポリシータグ（Policy Tag）] を介して [WLANプロファイル（WLAN Profile）] にマッピングされ、これをアクセスポイントに適用できます。

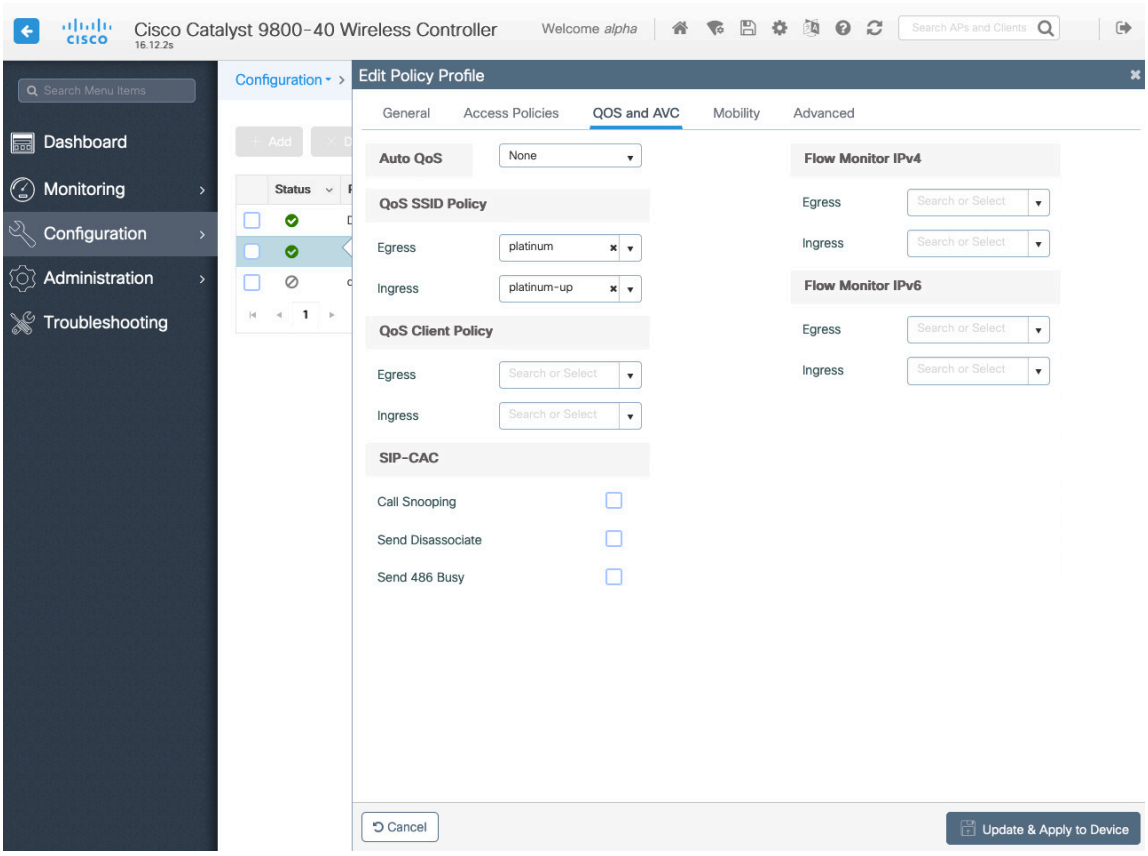
ポリシープロファイルの **ステータス** が **有効になっていることを確認してください。**



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



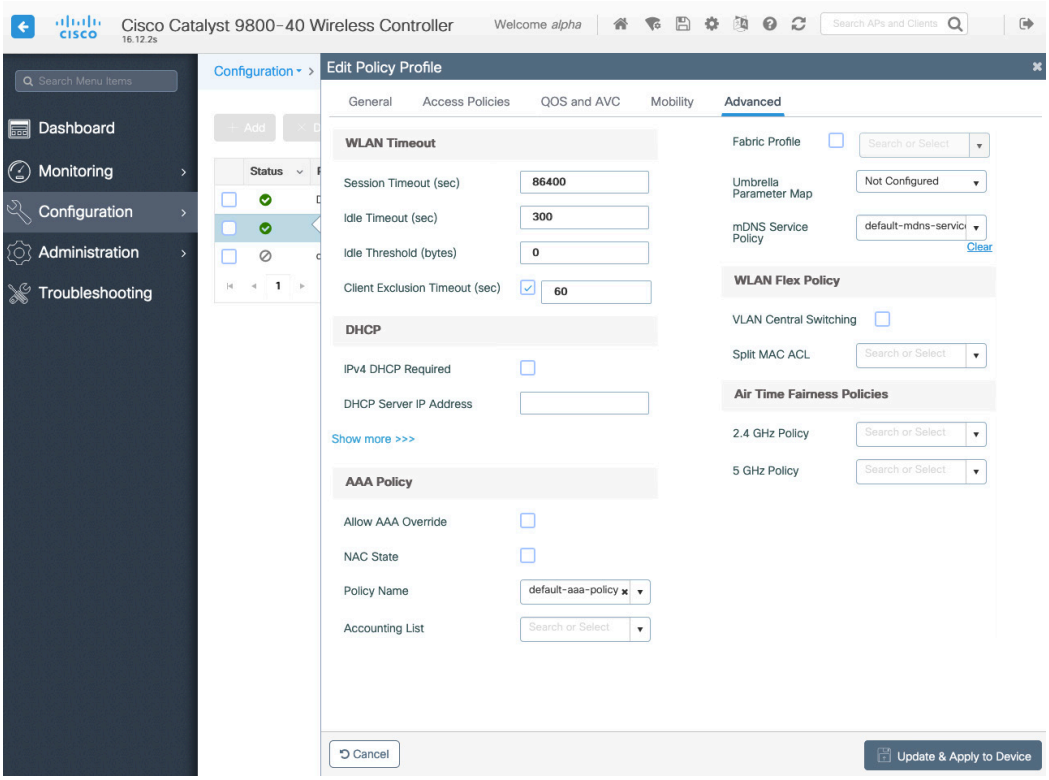
[QoS SSIDポリシー（QoS SSID Policy）] の エグレスを **[プレミア（Platinum）]** に、イングレスを **[プラチナーアップ（Platinum-up）]**に設定します。



必要に応じて **セッションタイムアウト** を設定します。 音声通話中の中断を避けるために、86400 秒のセッションタイムアウトを有効にすることをお勧めします。また、クライアント資格情報を定期的に再検証して、クライアントが有効な資格情報を使用していることを確認します。

必要に応じて **クライアント除外タイムアウト** を設定してください。

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



RF プロファイル

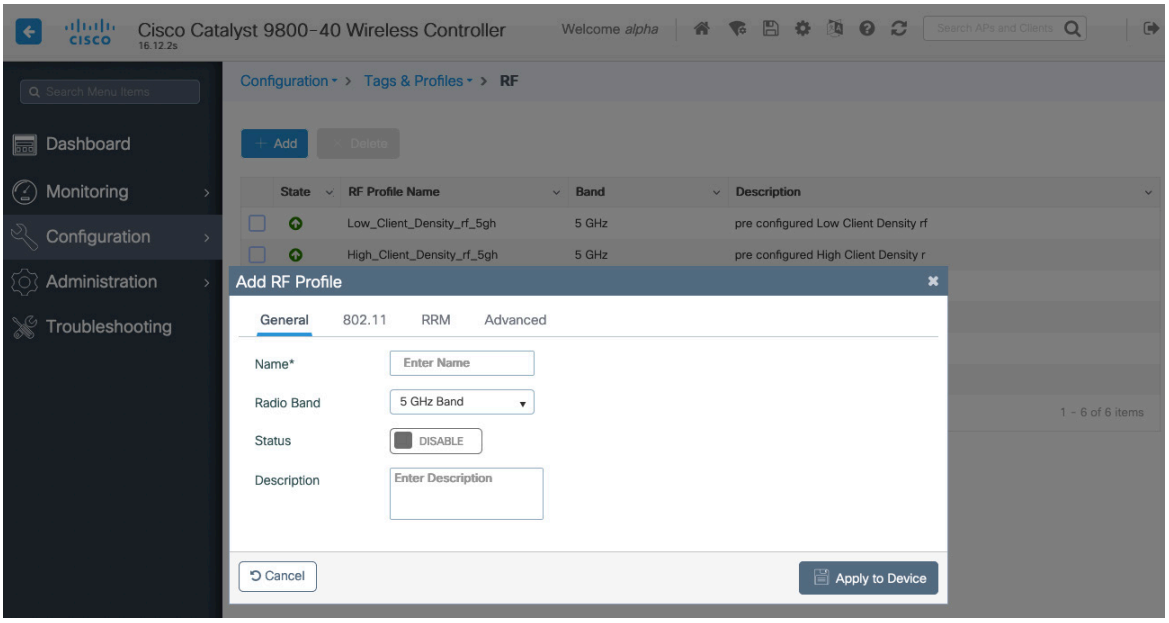
RF プロファイルを作成して、アクセスポイントのグループが使用する周波数帯域、データレート、RRM 設定、および詳細設定を指定することができます。

Cisco デスク フォン 9800 シリーズで使用される SSID については、5 GHz 無線のみに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、その後、アクセスポイントに適用できます。

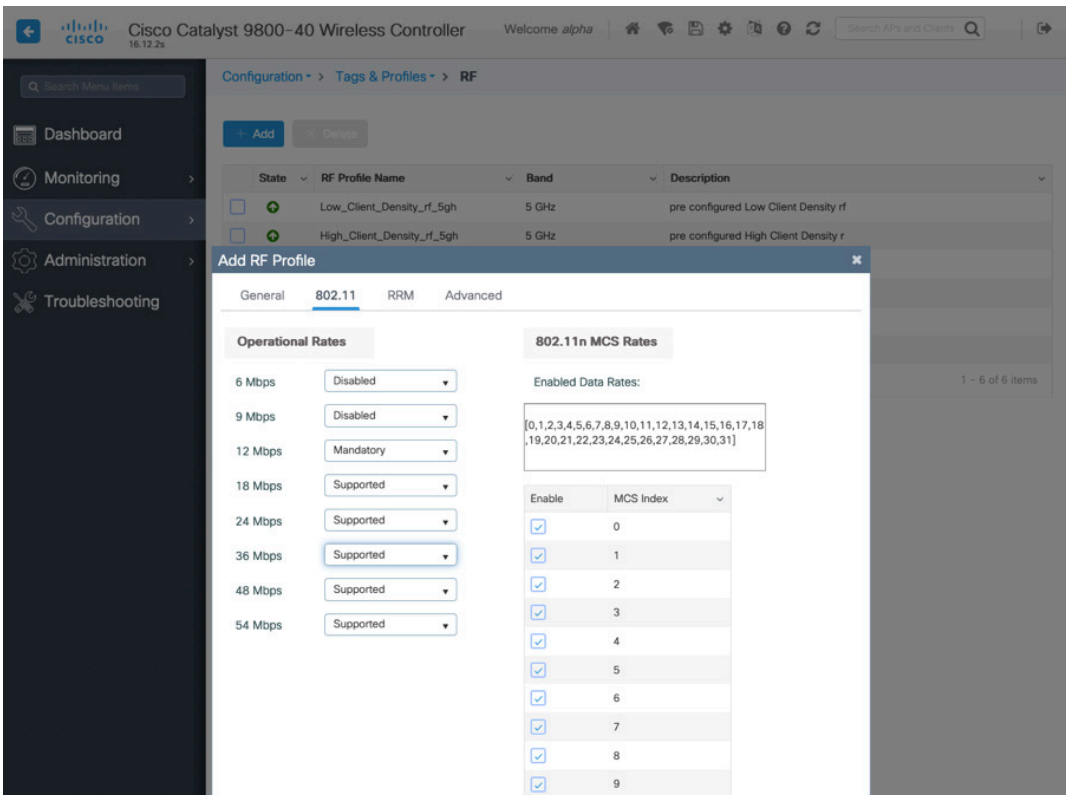
RF プロファイルの作成時に、 **名前** と **無線帯域** を定義する必要があります。

[無線帯域（Radio Band）] に対して、**[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。

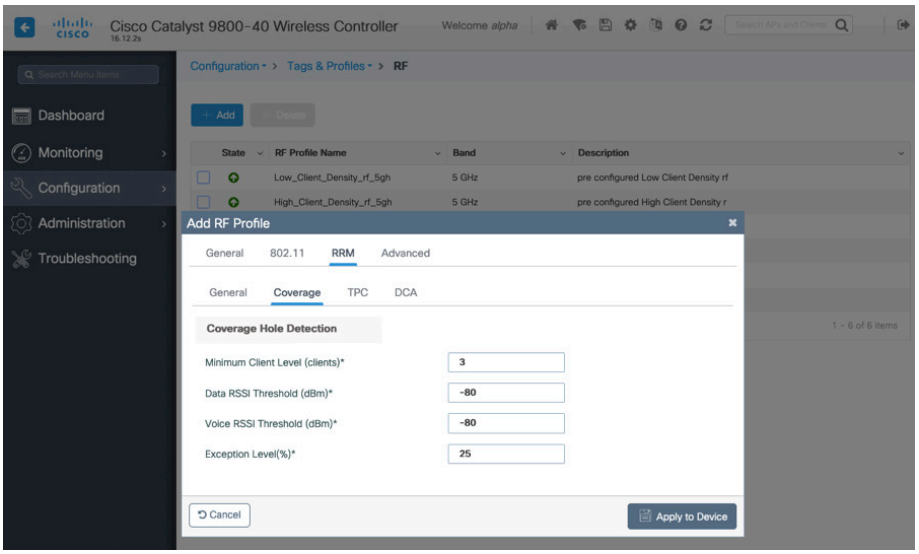


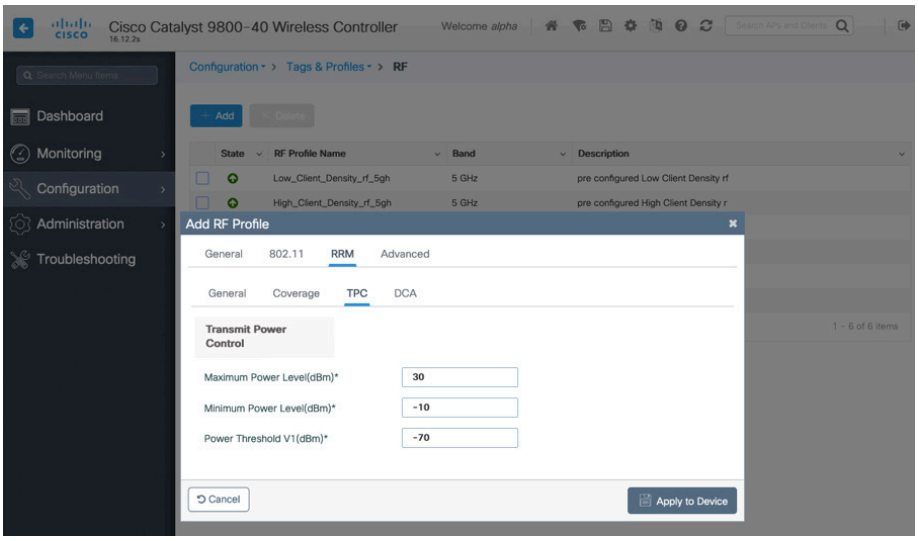
[802.11] タブで、必要に応じて、データレートを構成します。

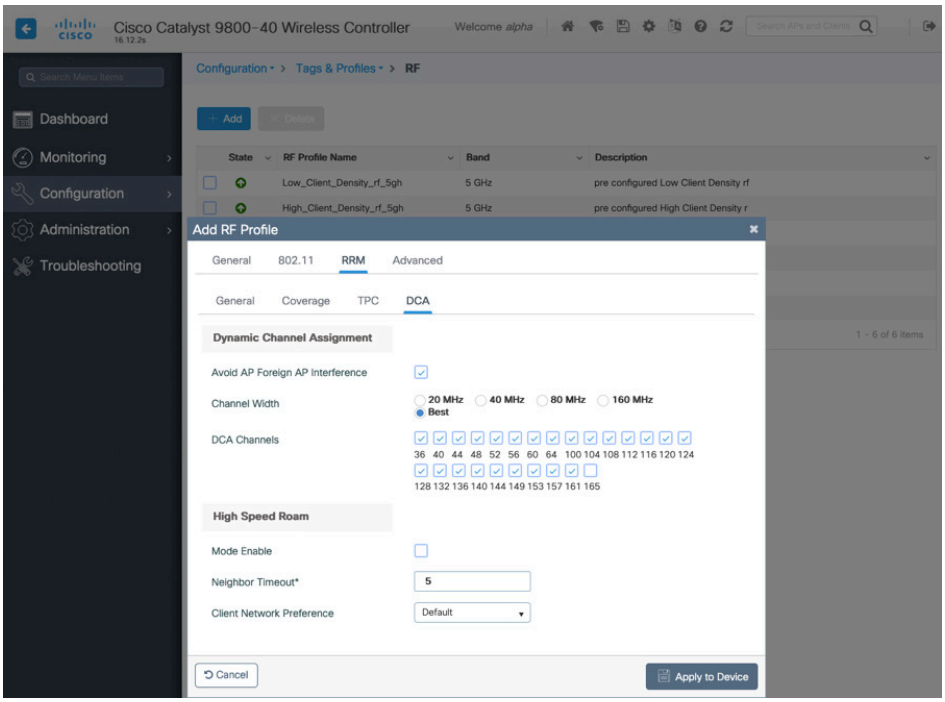
12 Mbps を **[必須（Mandatory）]** として、18 Mbps 以上を **[サポート対象（Supported）]** として有効化することが推奨されますが、一部の環境では、必須（基本）レートとして 6 Mbps を有効にする必要がある場合があります。



[RRM]タブで、**[最大電力レベル（Maximum Power Level）]** と **[最小電力レベル（Minimum Power Level）]** 設定および **[DCA]**、**[TPC]** および **[カバレッジ（Coverage）]** 設定を構成します。

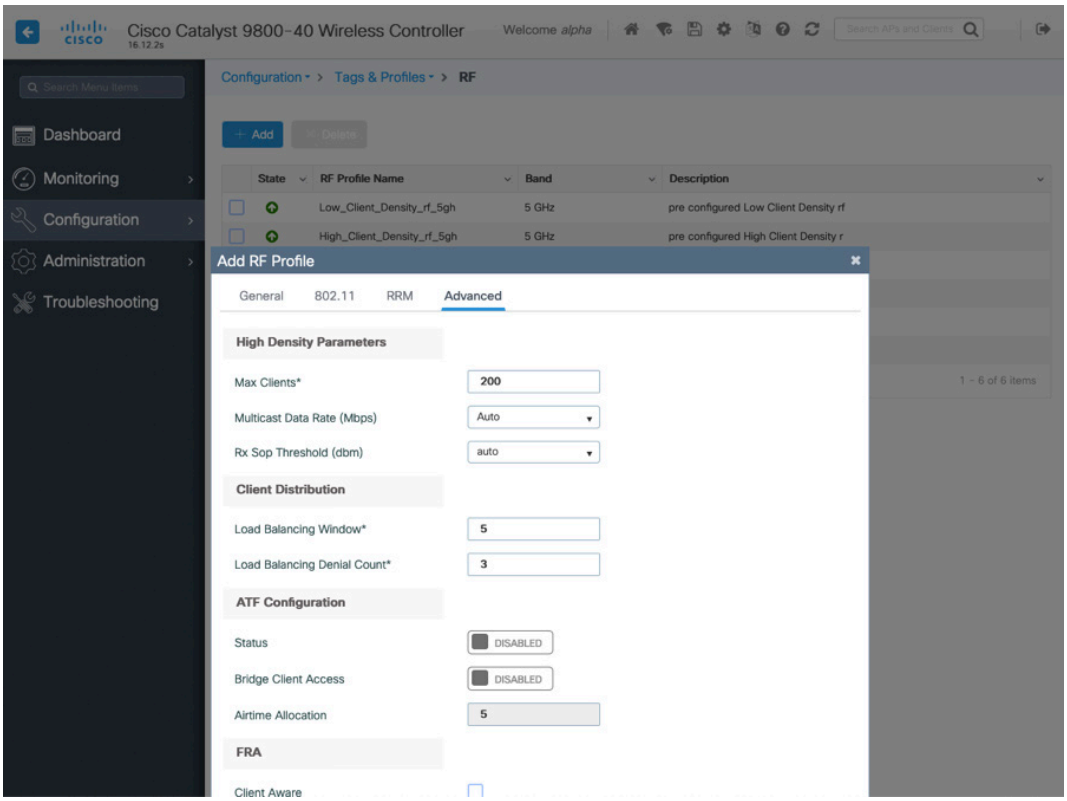






[詳細設定（Advanced）] タブの **[最大クライアント数（Maximum Clients）]**、 **[（Multicast Data Rate）]**, **[Rx Sopしきい値（Rx Sop Threshold）]** およびその他詳細設定を設定できます。

[Rx Sopしきい値（Rx Sop Threshold）] には、デフォルト値（**[自動（Auto）]**）を使用することが推奨されます。



Flex プロファイル

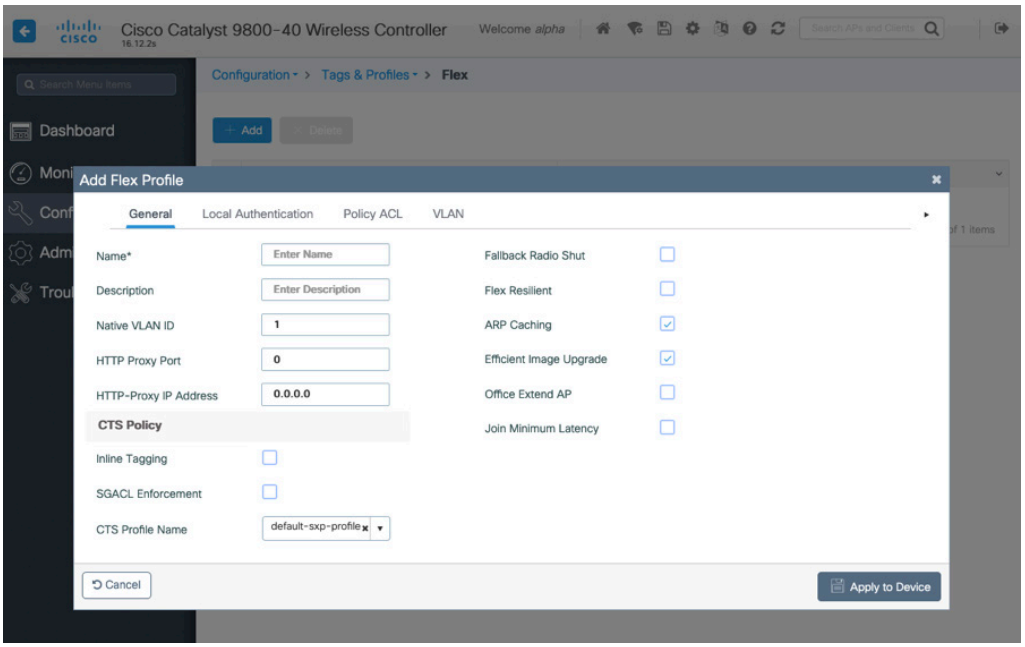
Flex プロファイルは、アクセスポイントが Flexconnect モードの場合に使用する設定を定義するために使用されます。

次に、[フレックスプロファイル（Flex Profiles）] を [サイトタグ（Site Tag）] にマッピングして、アクセスポイントに適用します

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

[ARPキャッシュ（ARP Caching）] を **[有効（Enabled）]** になっているかを確認します。

必要に応じて **ローカル認証** を有効にします。



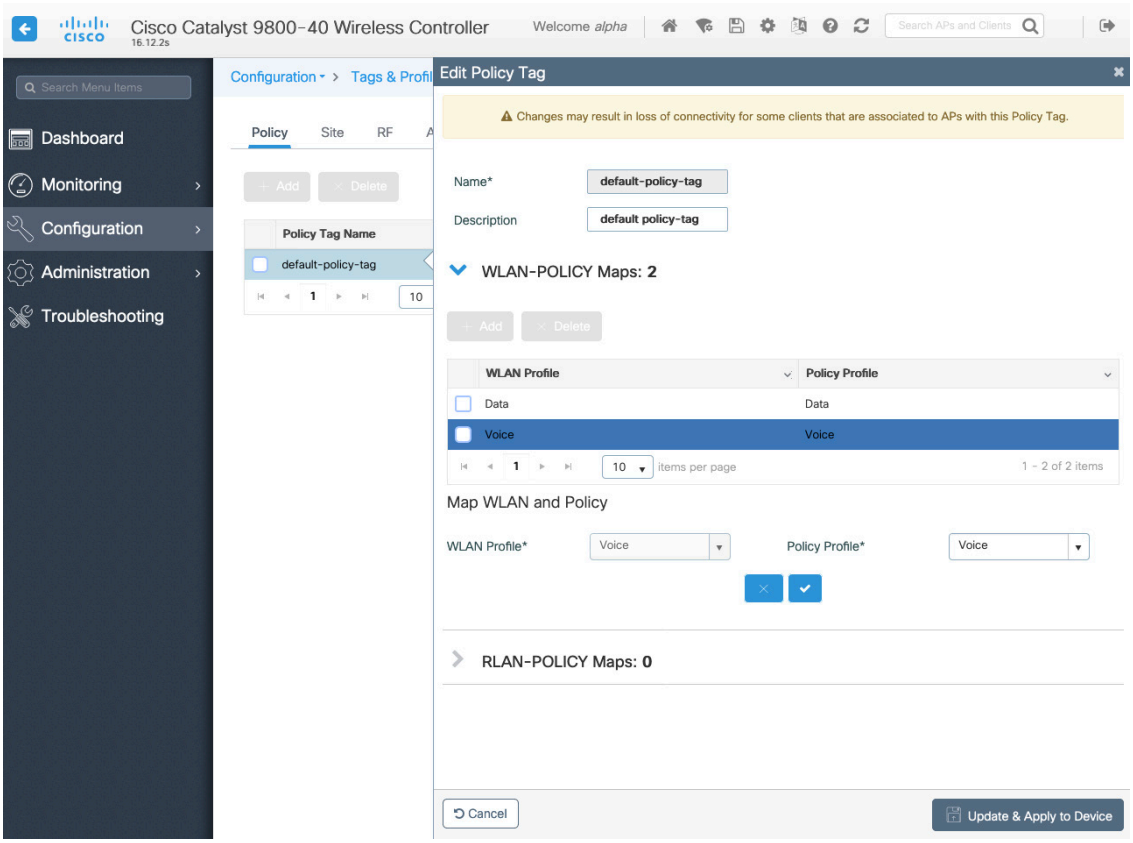
タグ

<u>ポリシータグ</u>

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定義します。

ポリシータグはアクセスポイントに適用され、有効にする WLAN / SSID、マッピングす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（Policy Tag）] を作成する際は、**[追加（Add）]** をクリックして、設定する **[WLANプロファイル（WLAN Profile）]** を選択して、使用する **[ポリシープロファイル（Policy Profile）]**を選択します。



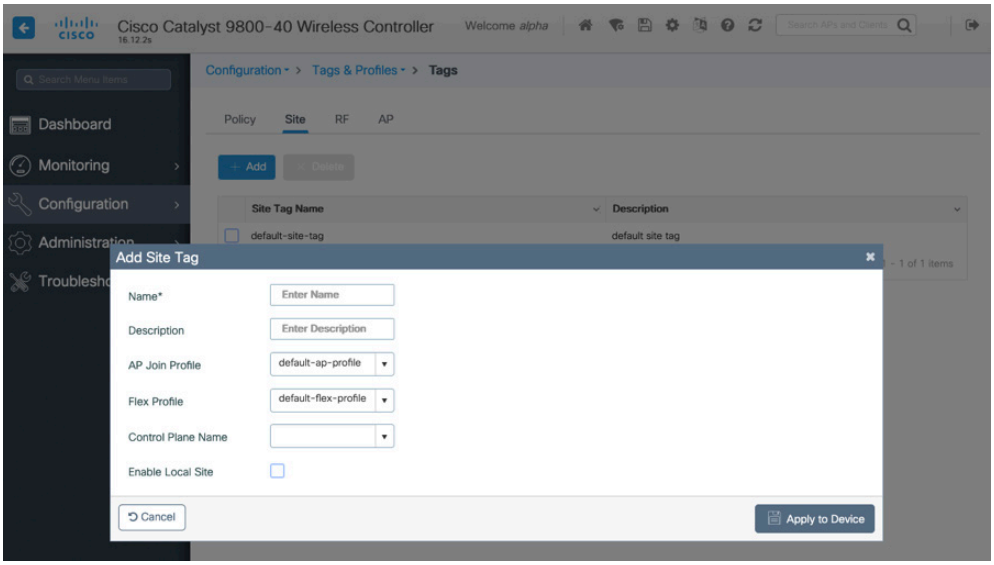
サイトタグ

サイト タグは、どの AP 参加プロファイルと Flex プロファイルを使用するかを定義します。

サイト タグはアクセス 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 Flex プロファイル パラメータを指定します。

サイトタグの作成時に、[**追加**] をクリックして、使用する [**AP 参加プロファイル**] を選択します。

[フレックスプロファイル（Flex Profile）] を含む [サイトタグ（Site Tag）] を作成する際は、**[ローカルサイトを有効化（Enable Local Site）]** をオフにして、必要な **[フレックスプロファイル（Flex Profile）]** を選択します。

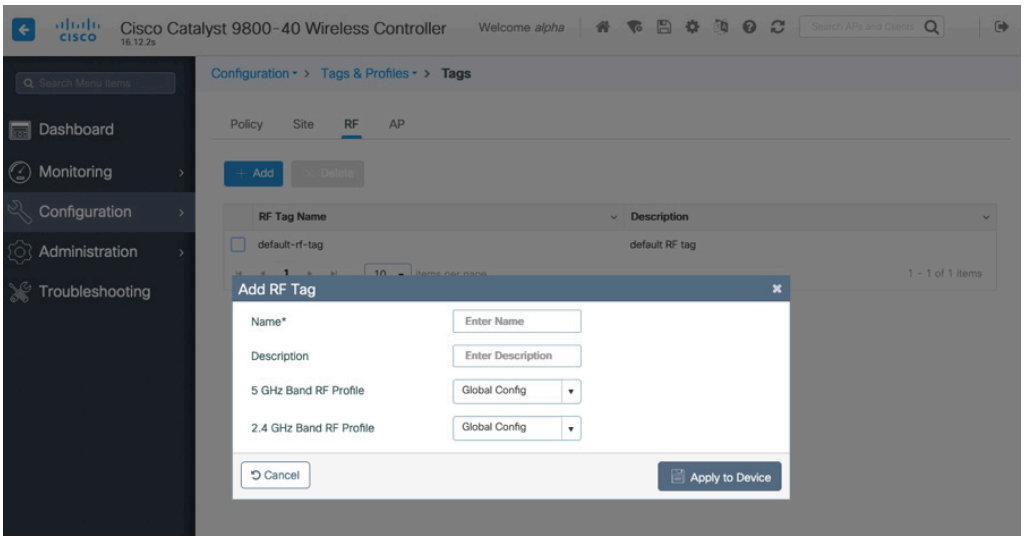


RF タグ

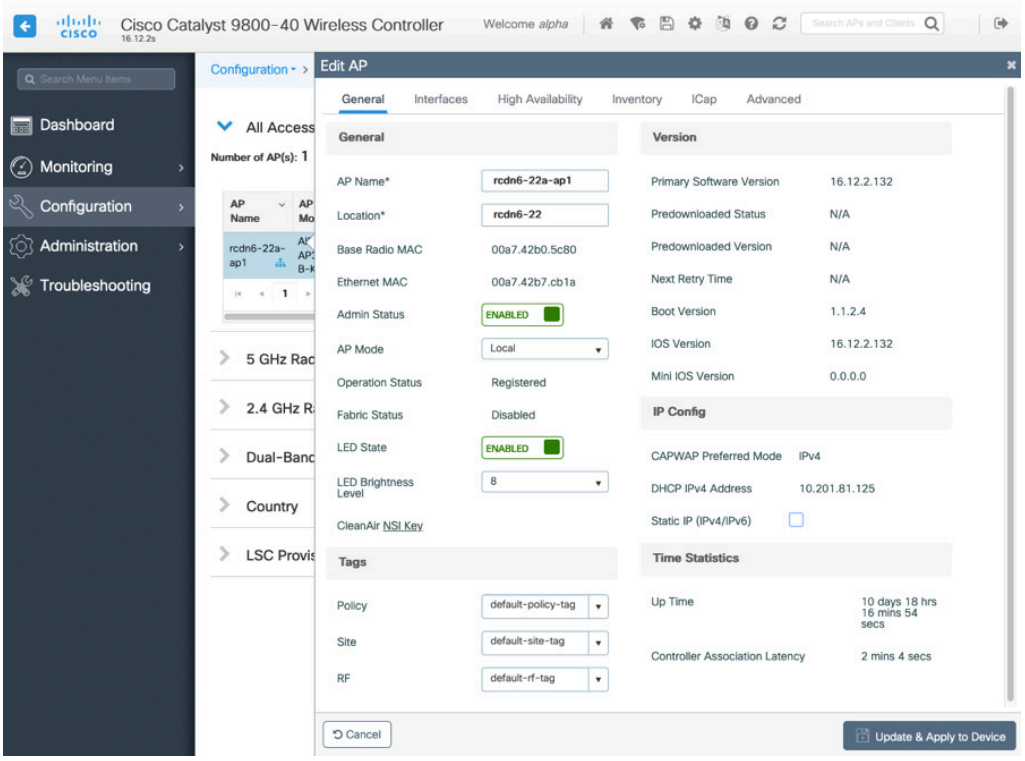
[RF タグ] は、2.4 GHz および 5 GHz で使用される RF プロファイルを定義します。

その後、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 パラメータが指定されます。

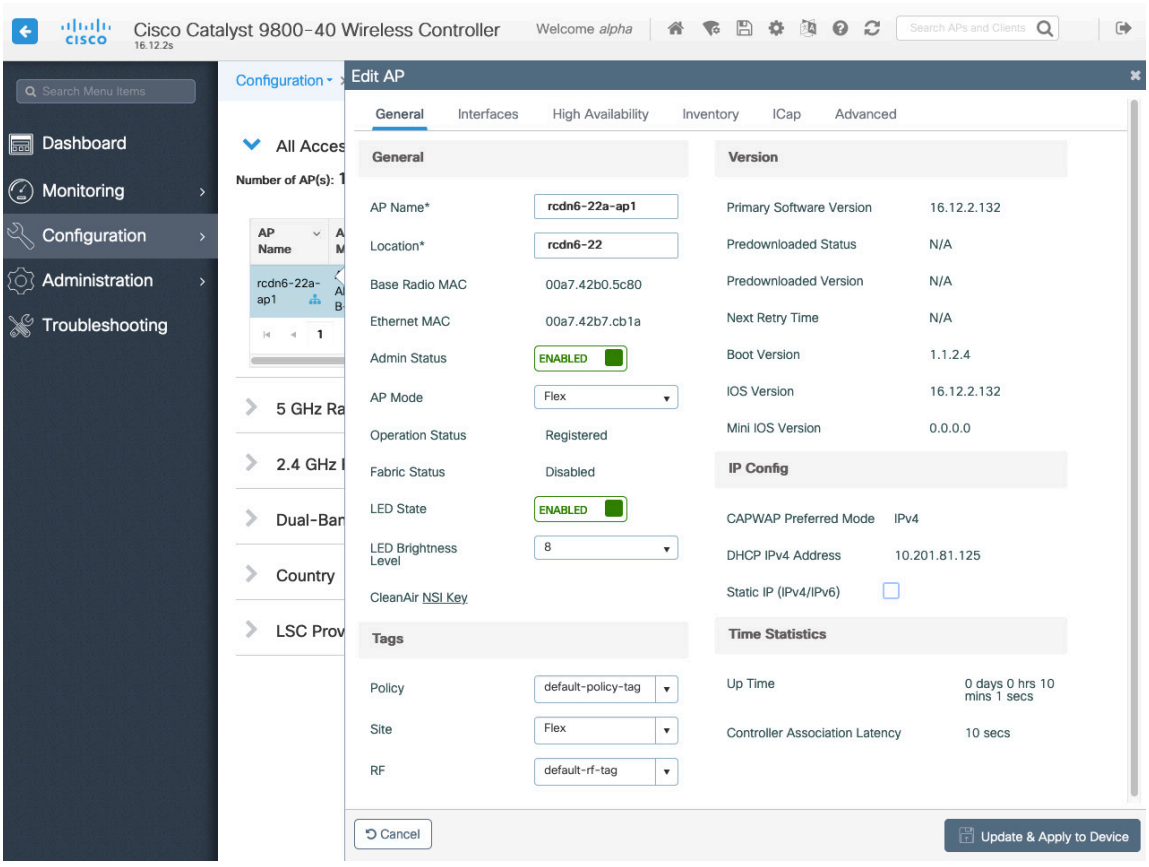
[RFタグ（RF Tag）] を作成する際は、使用する **[5 GHz帯域RFプロファイル（5 GHz Band RF Profile）]** と **[2.4 GHz帯域RFプロファイル（2.4 GHz Band RF Profile）]** を選択します。



タグが定義されると、アクセスポイントに適用することができます。

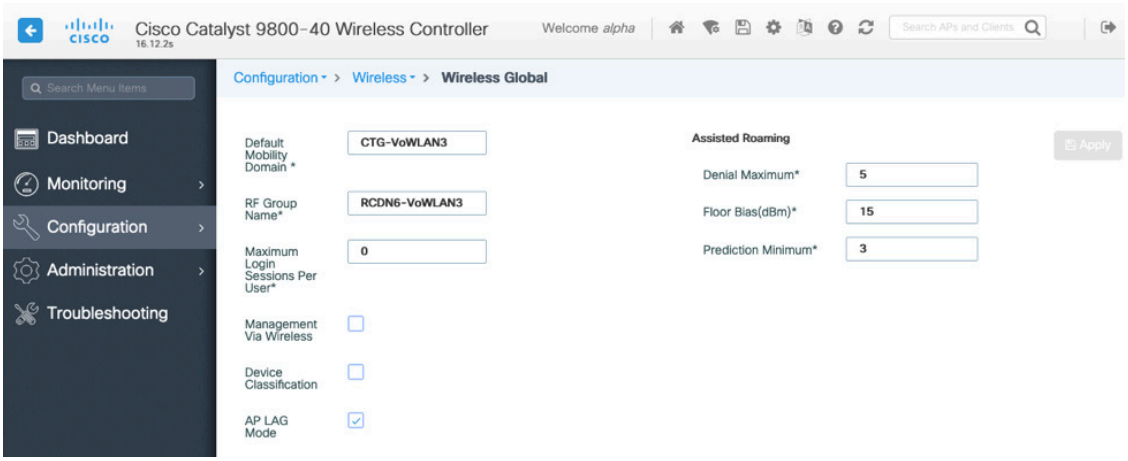


設定済み [フレックスプロファイル（Flex Profile）] を含む [サイトタグ（Site Tag）] を適用する際は、**[APモード（AP もで）]** が自動で **[フレックス（Flex）]** に変更されます。



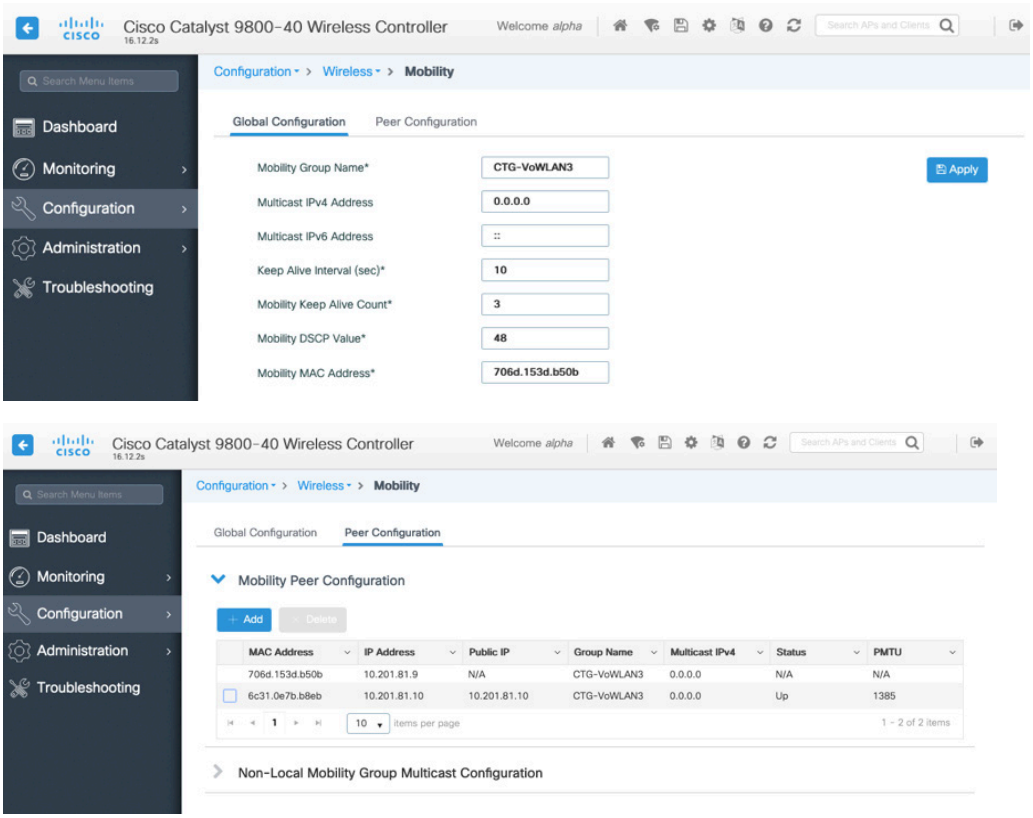
コントローラの設定

デフォルトモビリティドメイン が正しく設定されていることを確認してください。
[AP LAGモード（AP LAG Mode）] を有効にします。

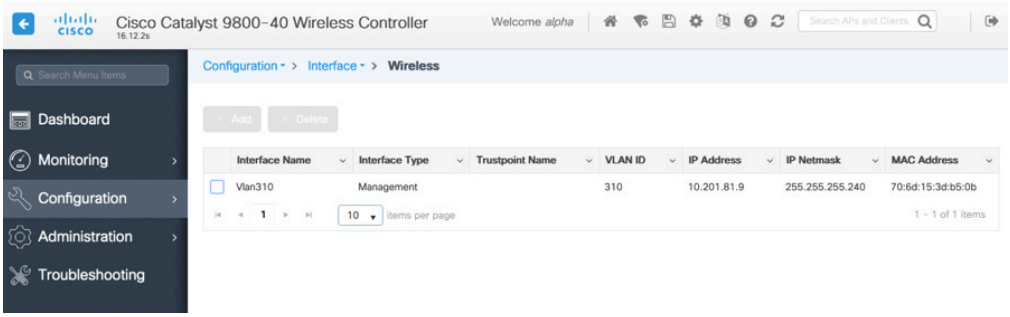


モビリティ設定

複数の Cisco ワイヤレス LAN コントローラが同じモビリティ グループの一部である場合、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。
Cisco Wireless LAN Controller が同じ**モビリティグループ名**で設定されていることを確認します。

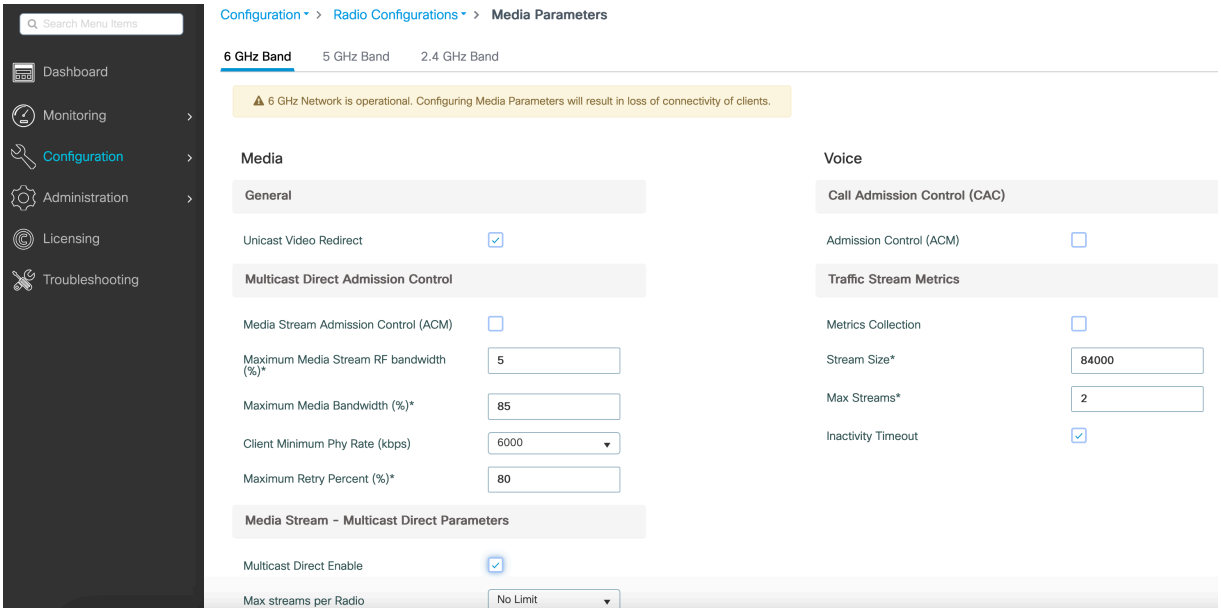


モビリティ MAC アドレス がワイヤレス管理インターフェイスの MAC アドレスと一致していることを確認してください。


Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Interface > Wireless
Add
Delete
Interface Name
Interface Type
Trustpoint Name
VLAN ID
IP Address
IP Netmask
MAC Address
Vlan310
Management
310
10.201.81.9
255.255.255.240
70:6d:15:3d:b5:0b
1
10
items per page
1 - 1 of 1 items

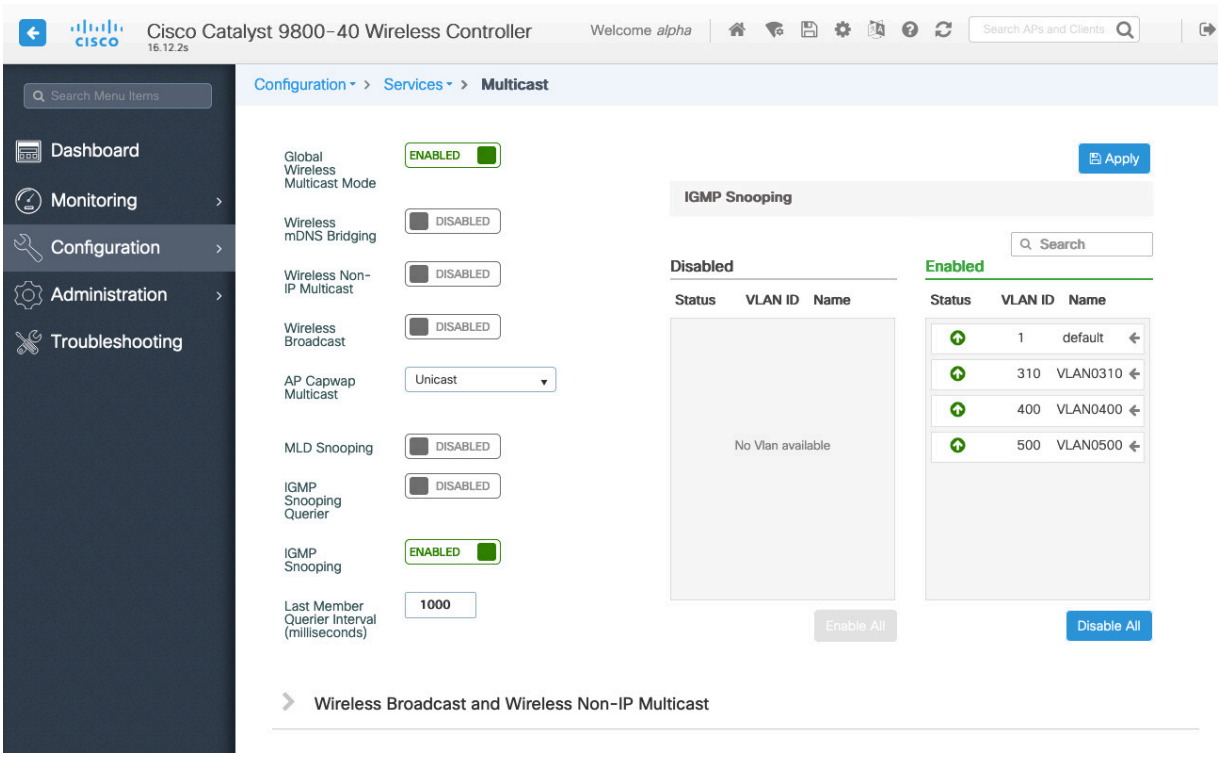
コール アドミッション制御（CAC）

[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を有効化（Multicast Direct Enable）]** を **[有効（Enabled）]** にします。

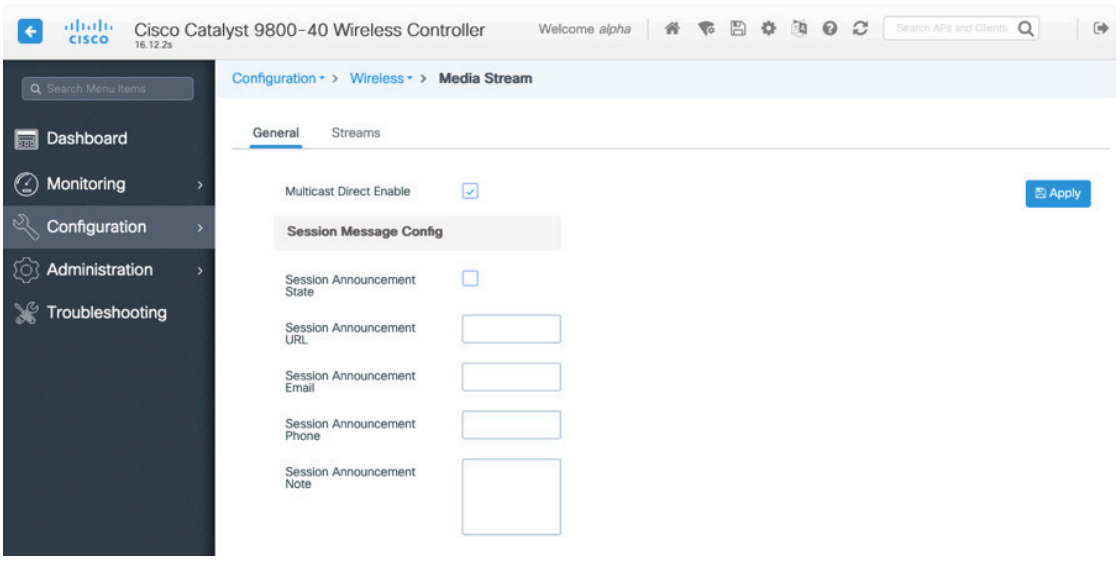


マルチキャスト

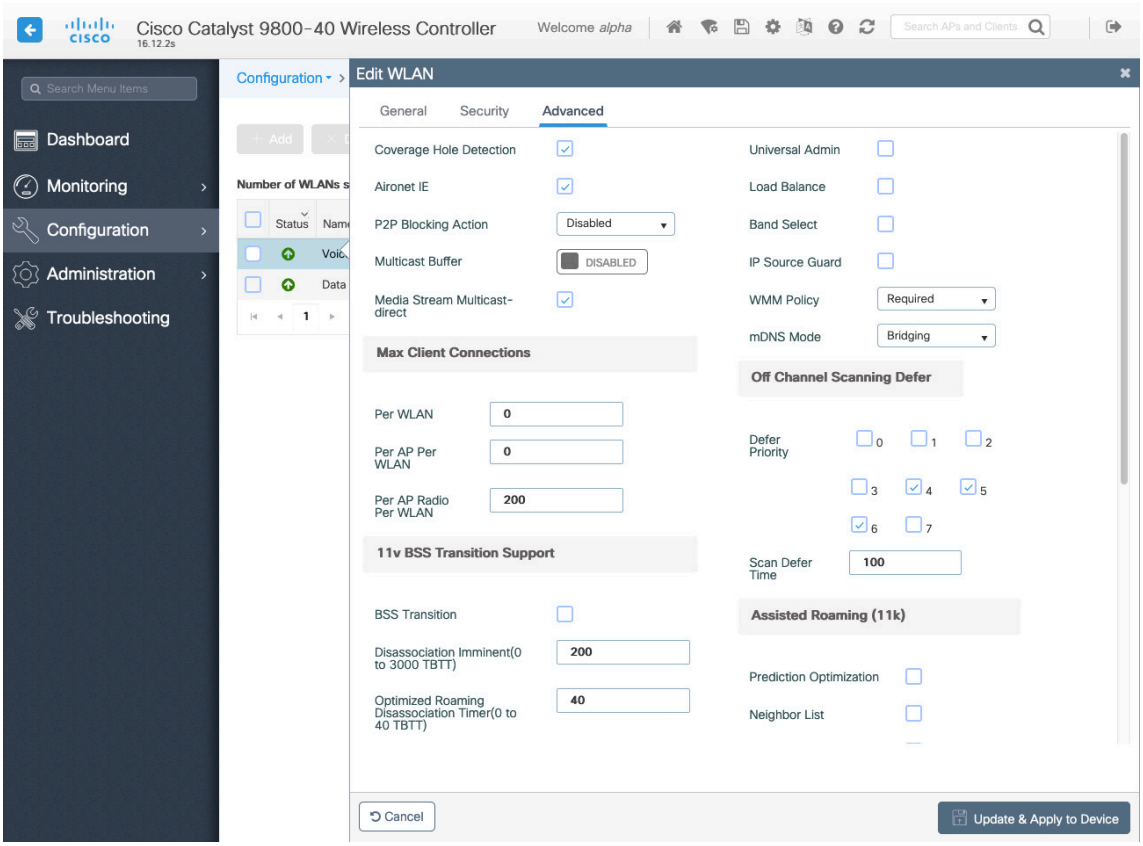
マルチキャストを利用するには、**[共通ワイヤレスマルチキャスト モード（Global Wireless Multicast Mod）]** と **[IGMPスヌーピング（IGMP Snooping）]** を **[有効（Enabled）]** にします。



[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を有効化（Multicast Direct Enable）]** を **[有効（Enabled）]** にします。



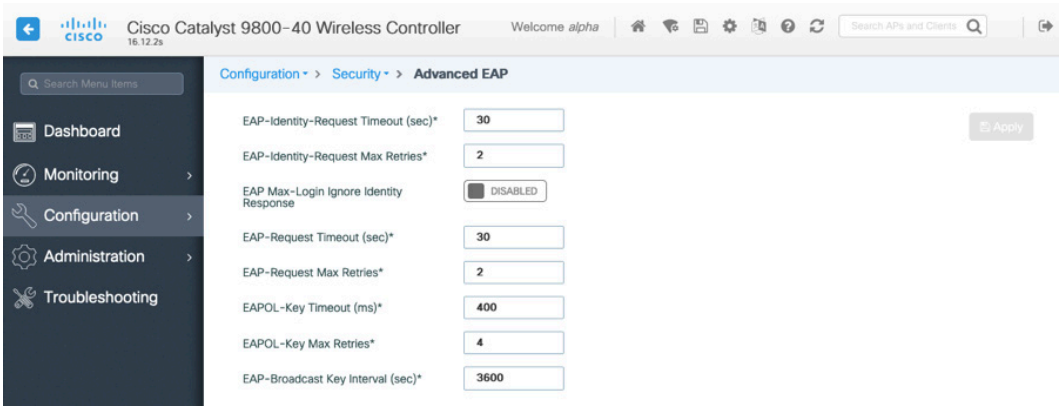
WLAN 設定で **マルチキャストダイレクト** を有効にします。



詳細設定

EAP の詳細設定

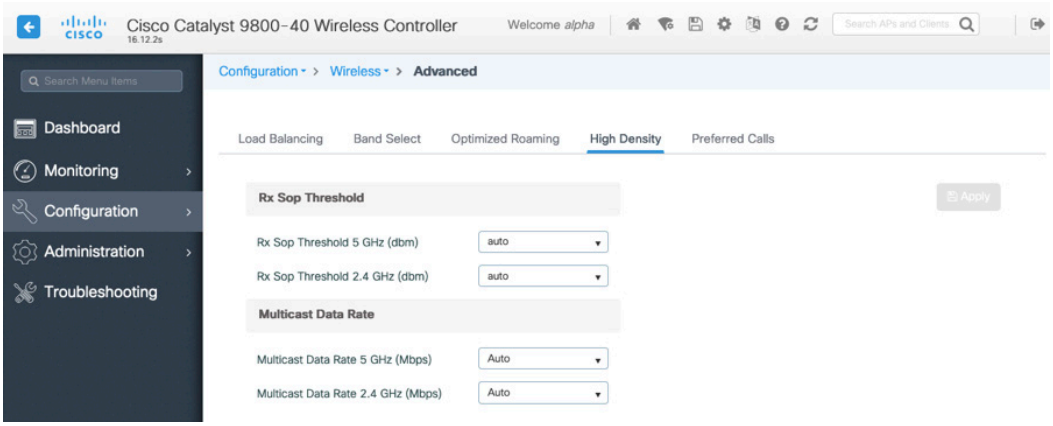
EAP パラメータを表示または構成するには、**[設定（Configuration）]** > **[セキュリティ（Security）]** > **[高度なEAP（Advanced EAP）]**.の順に選択します。



802.1x を使用する場合、Cisco ワイヤレス LAN コントローラの **EAP リクエストのタイムアウト** を 30 秒に設定する必要があります。
頻繁な EAP エラーを伴うデプロイの場合、**[EAPリクエストタイムアウト（EAP-Request Timeout）]** を30 秒以下に減らします。
PSK を使用する場合は、**[EAPOLキータイムアウト（EAPOL-Key Timeout）]** を、デフォルトの 1000 ミリ秒から 400 ミリ秒にして、**[EAPOLキー最大試行回数（EAPOL-Key Max Retrie）]** をデフォルト値の 2 から 4 に設定します。
802.1x を使用する場合、**[EAPOLキータイムアウト（EAPOL-Key Timeout）]** と **[EAPOLキー最大試行回数（EAPOL-Key Max Retries）]** のデフォルト値で問題ありませんが、これらの値をそれぞれ 400 と 4 に設定することが推奨されます。
[EAPOLキータイムアウト（EAPOL-Key Timeout）] は、1000 ミリ秒（1 秒）を超えないようにします。
[EAP-Broadcastキー間隔（EAP-Broadcast Key Interval）]が、最低でも 最低でも 3600 秒（1 時間）に設定されていることを確認します。

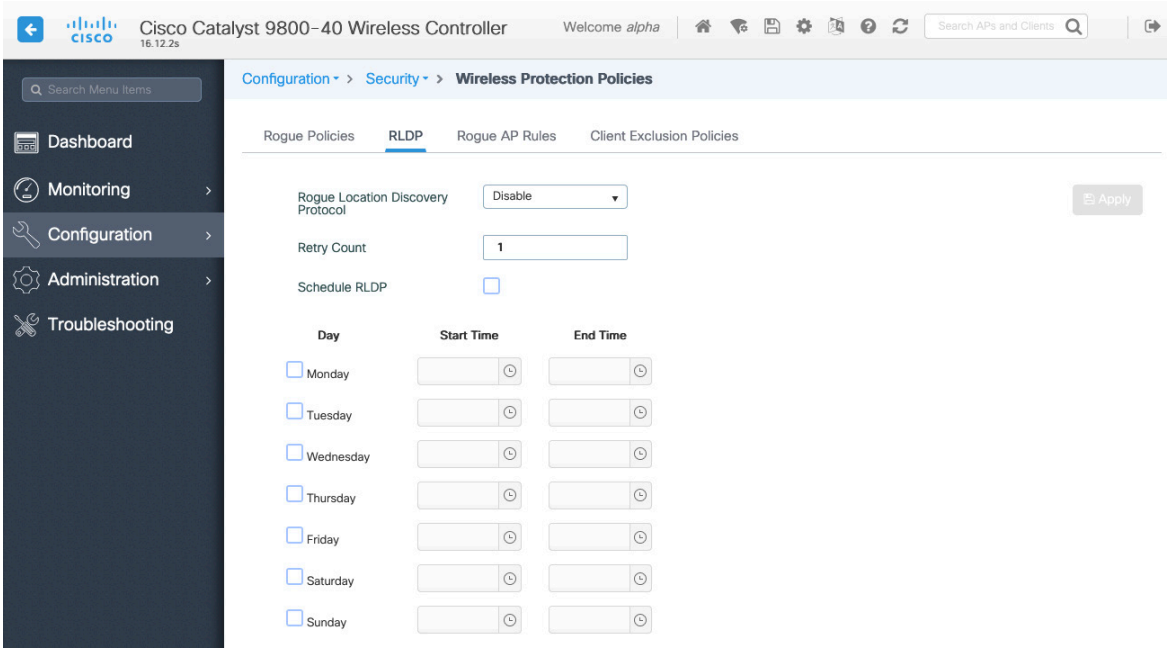
Rx Sop Threshold

[Rx Sopしきい値（Rx Sop Threshold）] には、デフォルト値（**[自動（Auto）]**）を使用することが推奨されます。



不正ポリシー

[不正デバイスの位置検出プロトコル（Rogue Location Discovery Protocol）] に対してデフォルト値（**[無効（Disabled）]**）を使用することが推奨されます。



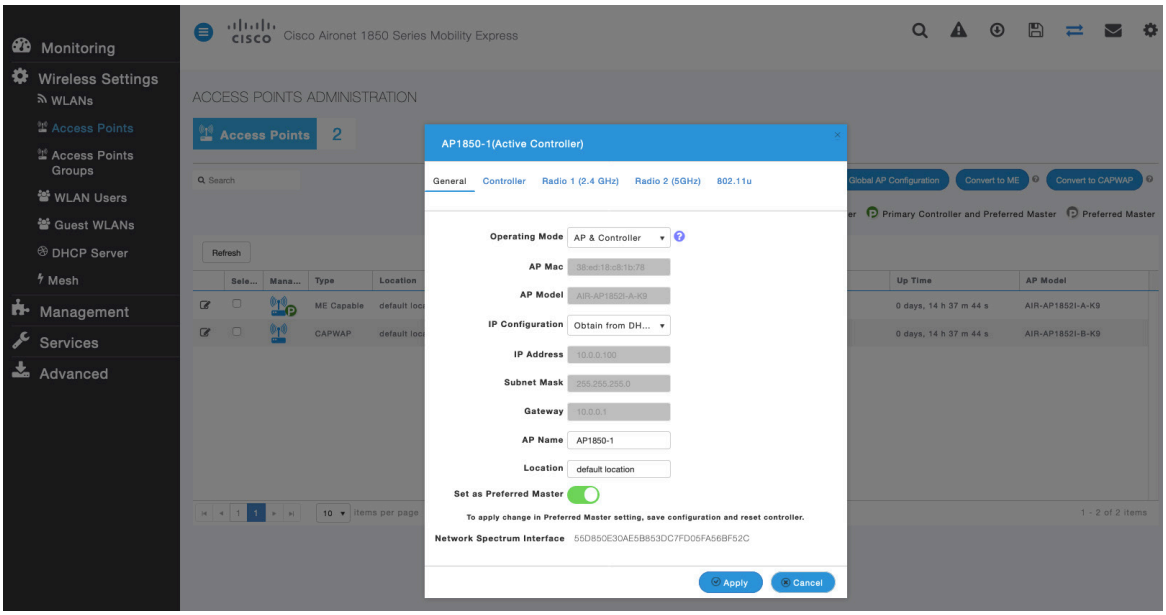
Cisco Mobility Express および Lightweight アクセス ポイント

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

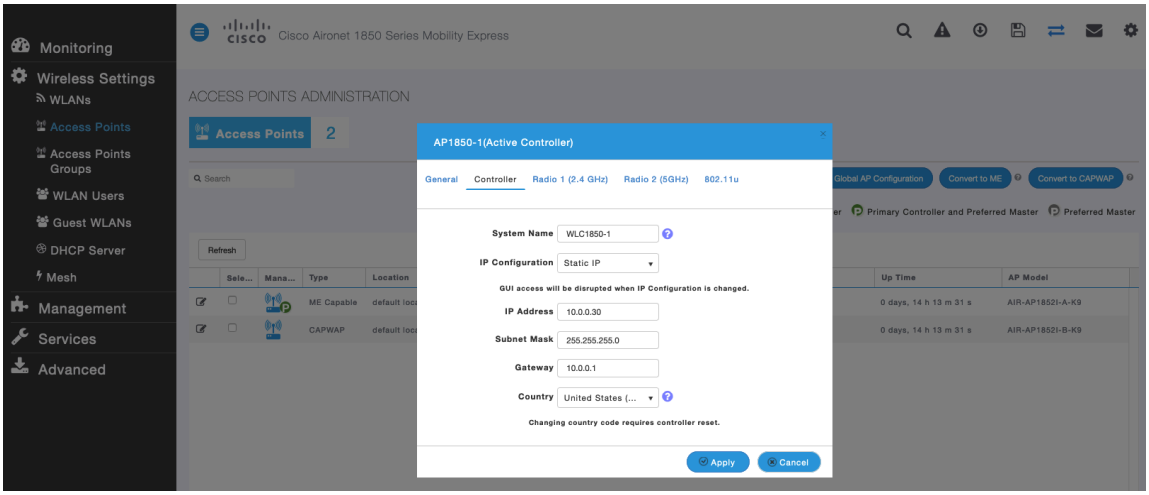
- **802.11r (FT) を有効にする**
- **[CCKM]** を無効にします。
- **[Quality of Service（QoS）]** を **[プラチナ（Platinum）]** に設定します
- **802.11k** が **無効になっていることを確認する**
- **[802.11v]** が **[無効（Disabled）]** になっていることを確認します
- P2P (ピアツーピア) ブロックアクションを無効にする
- **[クライアント帯域選択（Client Band Select）]** を **[無効（Disabled）]** に設定します
- **[クライアント負荷分散（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** を設定します
- 必要に応じて **RF 最適化** を設定します
- **トラフィックタイプ** を音声とデータに設定します
- CleanAir テクノロジ搭載の Cisco アクセスポイントを使用する場合は、**[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** を設定します

コントローラの設定

1 つ以上の Mobility Express に対応したアクセスポイントの**操作モード**を構成して、**[コントローラ（Controller）]**機能を含めます。
必要に応じて、**[AP名（AP Name）]** と IP 設定を設定します。



必要に応じて、Cisco Wireless LAN Controller の **システム名** と IP 設定をします。



802.11 ネットワーク設定

Cisco Desk Phone 9800 シリーズは 5 GHz 帯域のみで運用することを推奨します。利用できるチャネル数が多く、2.4 GHz 帯域に比べて干渉が少ないためです。
5 GHz を使用するには、 **5.0 GHz 帯域 有効**であることを確認してください。
必須 (基本) レートとして 12 Mbps を設定し、サポートされている (オプション) レートとして 18 Mbps 以上を設定することをお勧めします。 ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。
2.4 GHz を使用するには、 **2.4 GHz 帯域** で **有効**であることを確認してください。

802.11b のみのクライアントがワイヤレス LAN に接続されないことを前提として、必須 (基本) レートとして 12 Mbps を設定し、サポートされている (オプション) レートとして 18 Mbps 以上を設定することをお勧めします。ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。

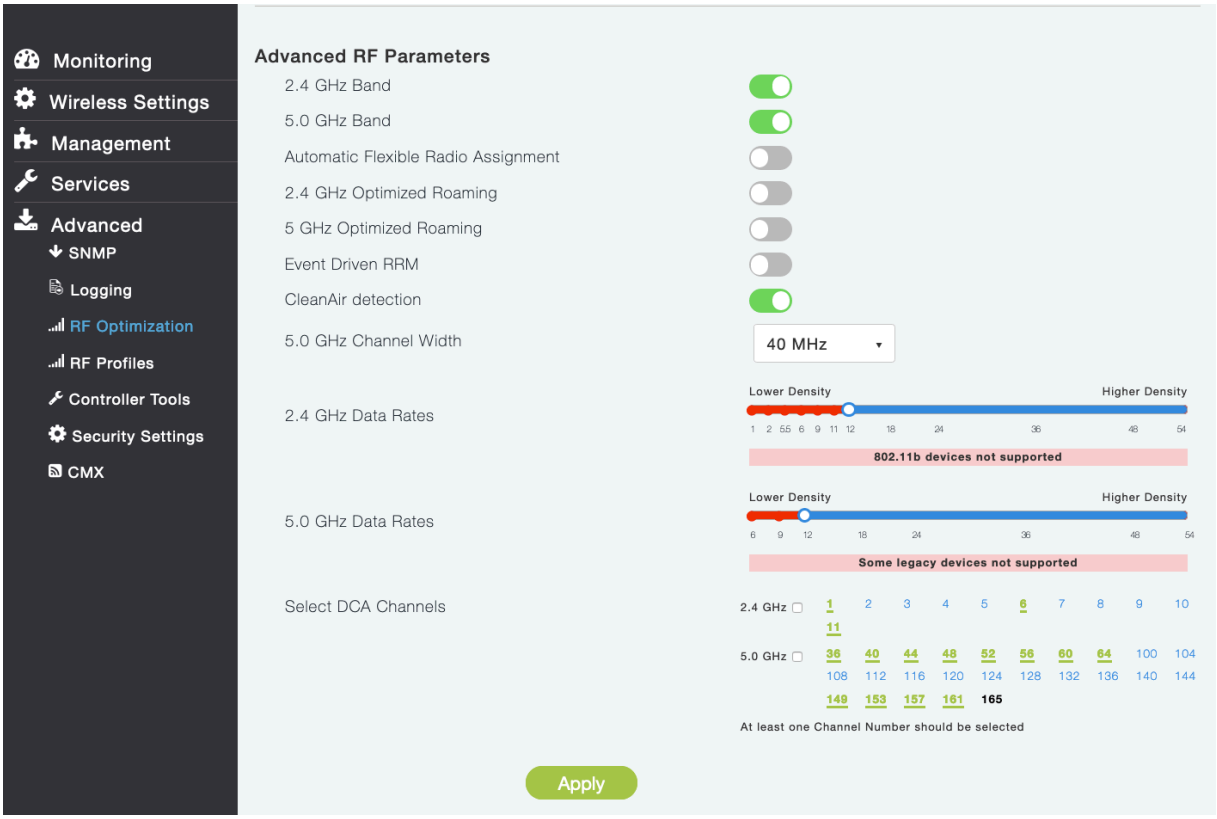
802.11b クライアントが存在する場合、11 Mbps を必須 (基本) レートとして設定し、12 Mbps 以上をサポート (オプション) として設定する必要があります。

5 GHz を使用する場合、多くのチャンネルをスキャンすることによるアクセスポイント検出の遅延を避けるために、チャンネル数を制限することをお勧めします (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 として、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 として構成できます。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。

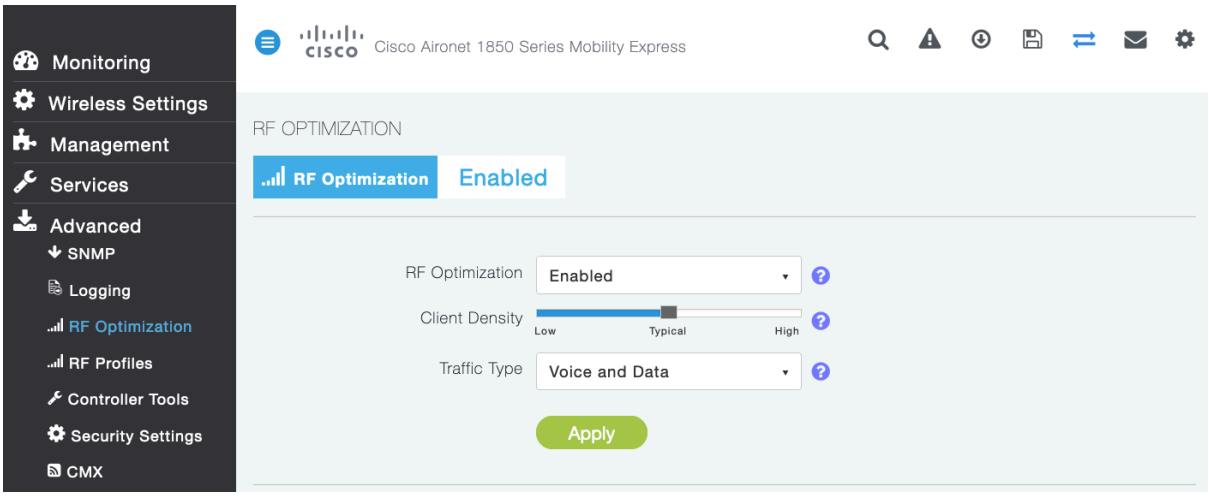
2.4 GHz を使用する場合、チャネル 1、6、および 11 のみを DCA リストで有効にする必要があります。

CleanAir テクノロジ搭載の Cisco アクセスポイントを使用して、既存の干渉源を検出するには、**[CleanAir検出（CleanAir detection）]** を **[有効（Enabled）]** にします。



RF 最適化

[RF最適化（RF Optimization）] を有効にして、チャネルや送信電力設定を管理することが推奨されます。**[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。



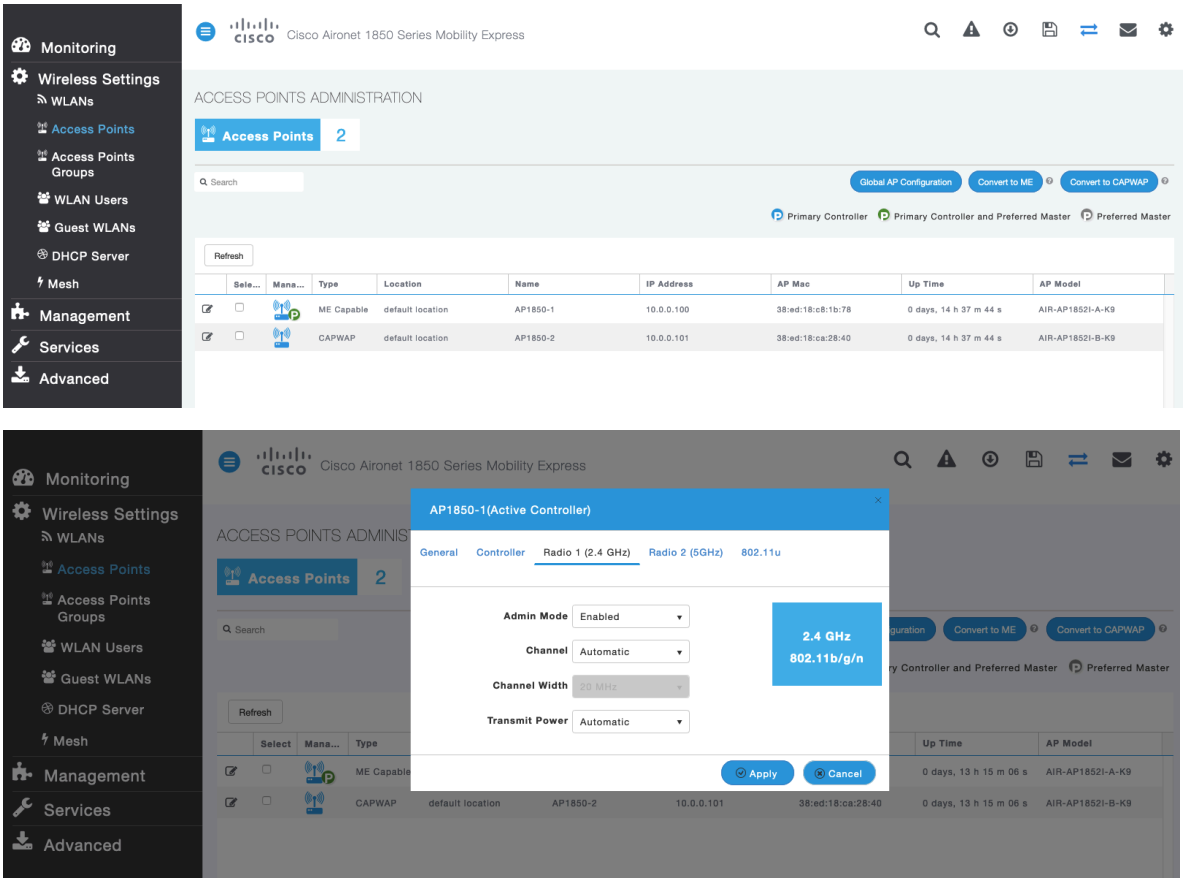
利用する周波数に周波数帯に応じて、5GHz または 2.4GHz のいずれかで動的チャネルと送信電力の割り当てを使用するように、個々のアクセスポイントは全体設定をオーバーライドするように設定できます。

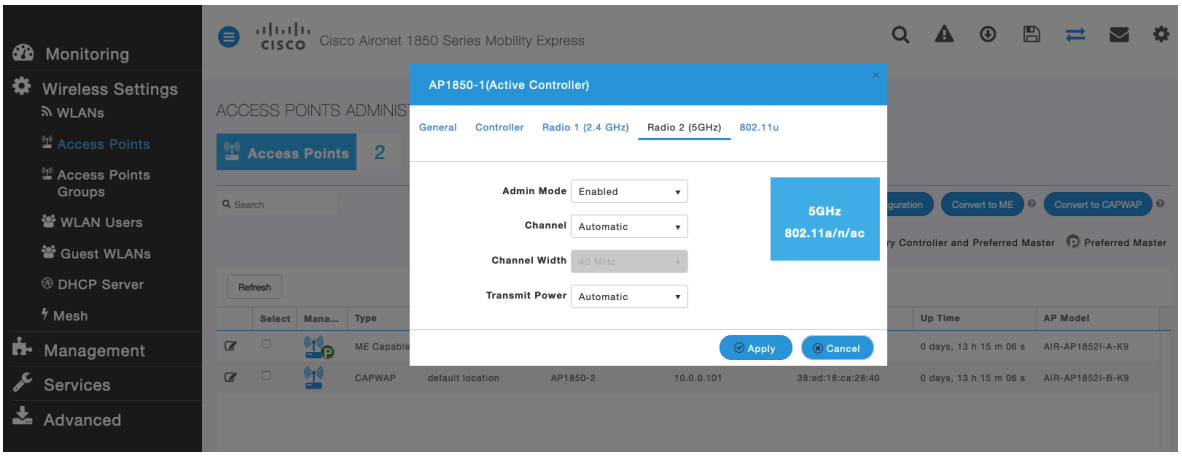
その他のアクセスポイントは、自動割り当てメソッドと、静的に設定したアクセスポイントのアカウントに対して有効化できます。

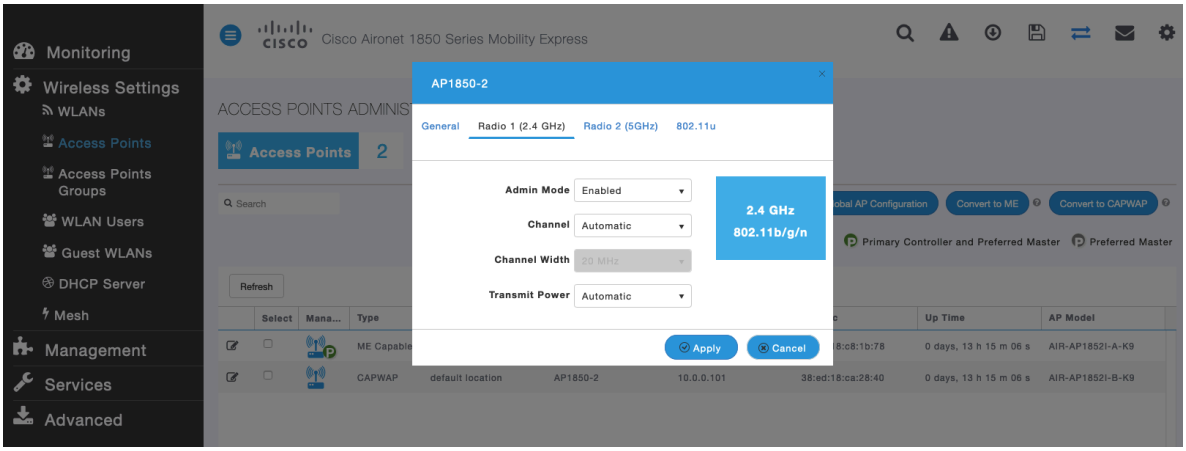
これは、その地域で断続的な干渉源がある場合に必要になります。

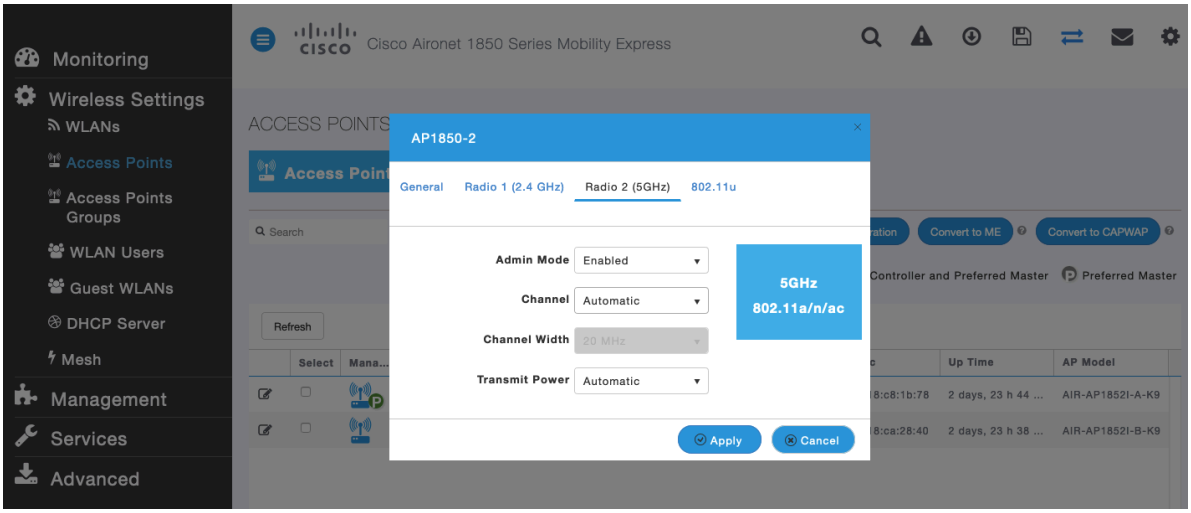
5 GHz チャネル幅は、Cisco 802.11n アクセスポイントを使用する場合は 20 MHz または 40 MHz として、Cisco 802.11ac アクセスポイントを使用する場合は 20 MHz、40 MHz、または 80 MHz として構成できます。

5 GHz を使用する場合にのみチャネル バインディングを使用し、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。









[IVR設定(WLAN Settings)]

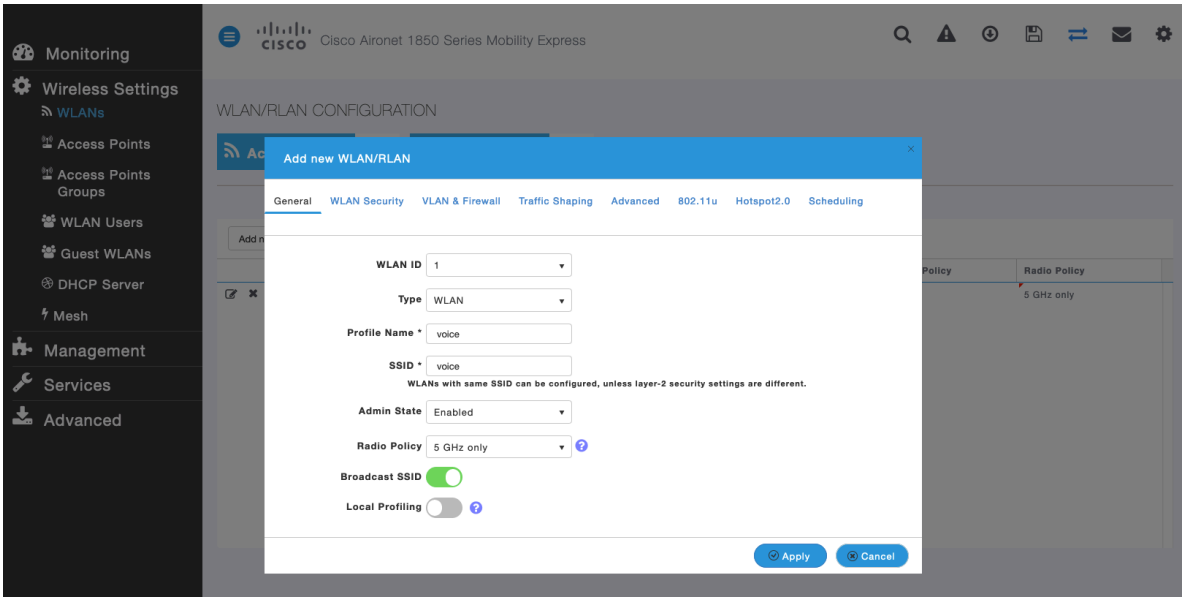
Cisco Desk Phone 9800 シリーズには別の SSID を割り当てることを推奨します。

しかし、音声対応 Cisco ワイヤレス 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 を使用することもできます。

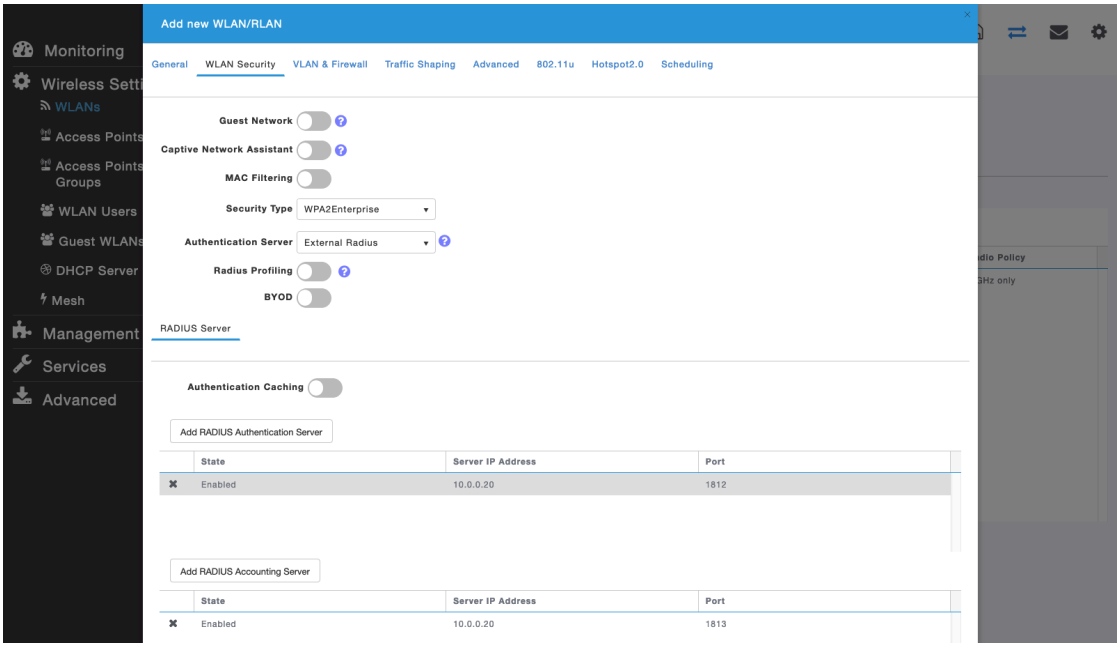
Cisco Desk Phone 9800 シリーズで使用される SSID は、特定の 802.11 無線タイプのみに適用されるように設定できます (例、5 GHz のみ)。

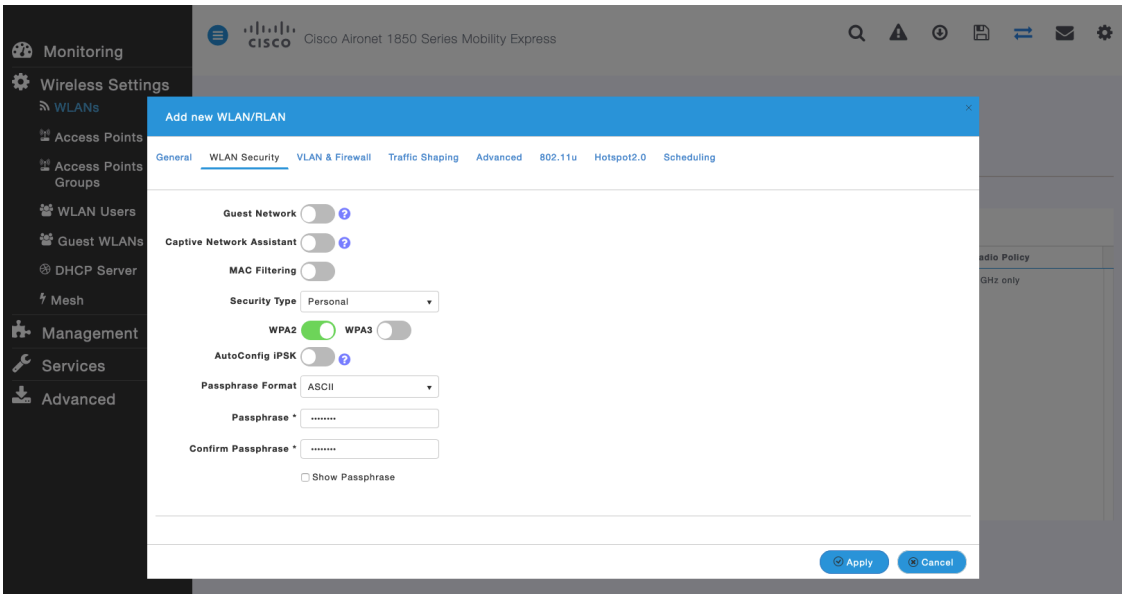
Cisco Desk Phone 9800 シリーズは 5 GHz 帯域のみで運用することを推奨します。利用できるチャネル数が多く、2.4 GHz 帯域に比べて干渉が少ないためです。

選択した SSID が他のワイヤレス LAN で使用されていないことを確認してください。これは、電源オン時またはローミング中に障害につながる可能性があるためです。特に別のセキュリティタイプが使用されている場合。



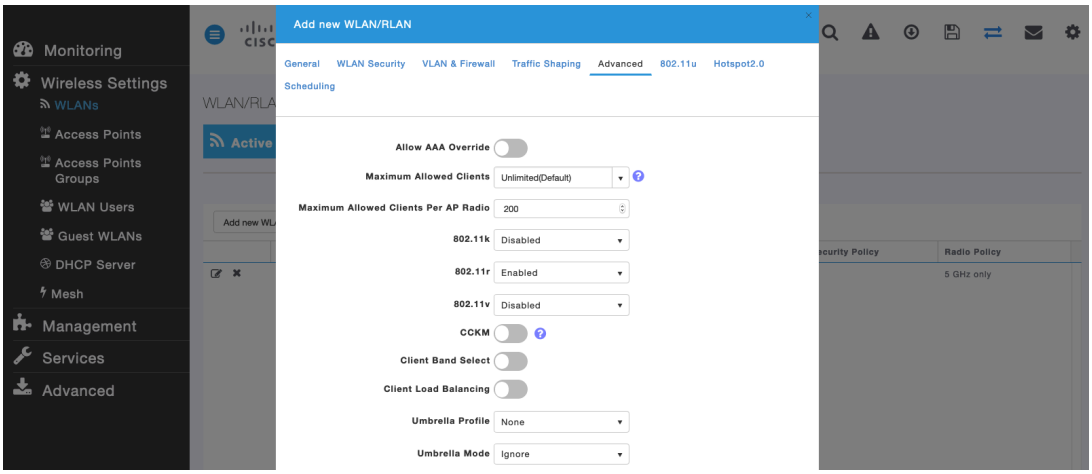
高速セキュア ローミングに 802.11r (FT) を使用するには、 **セキュリティタイプ** を選択します。 **WPA2-エンタープライズ** または **パーソナル** 802.1x または PSK/SAE のどちらを使用するかによって異なります。



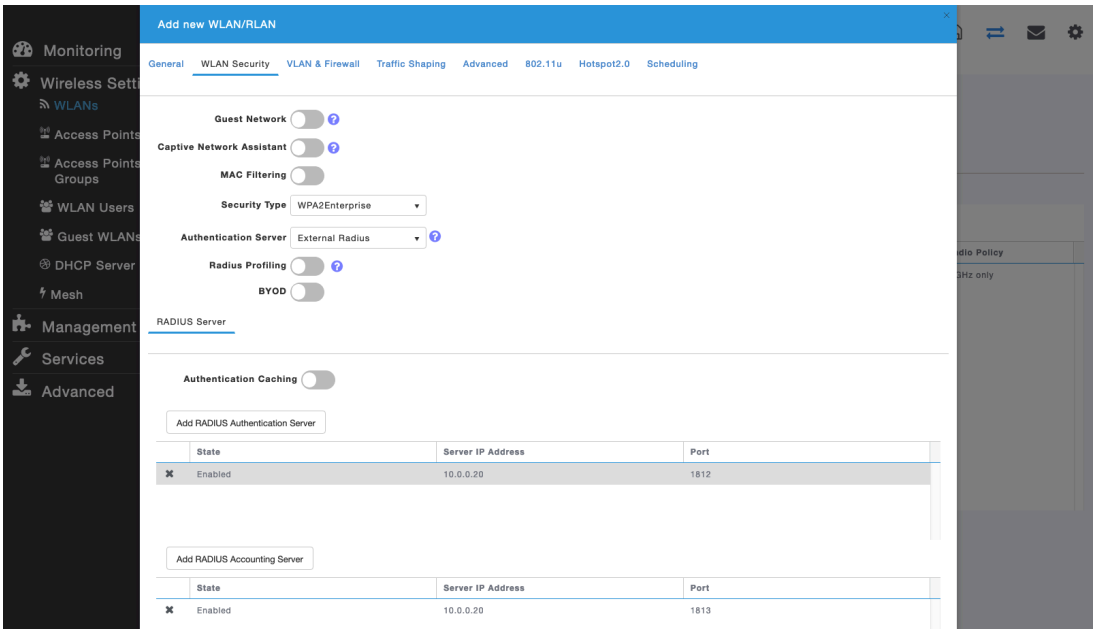


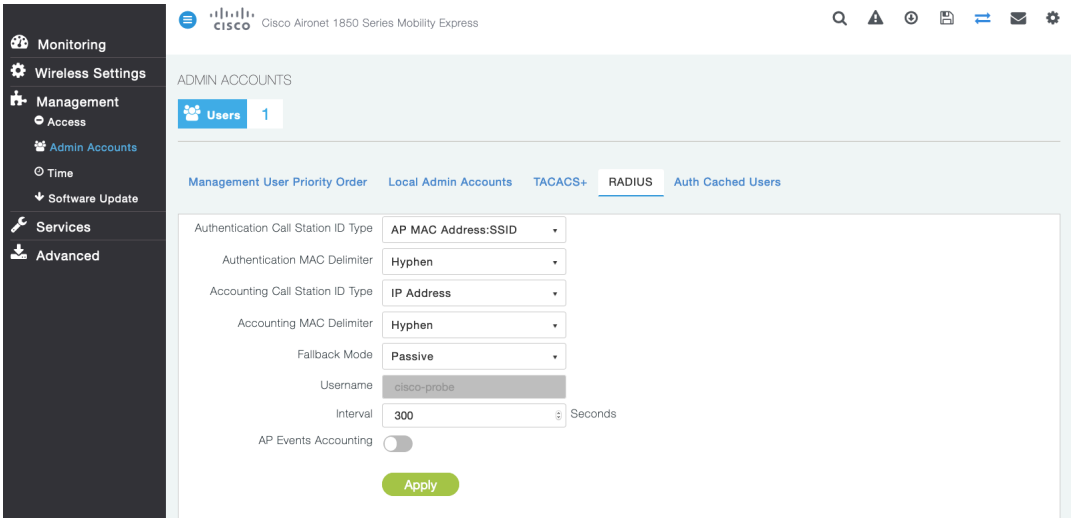
WLAN 設定の **[詳細設定（Advanced）] タブ** で、**[802.11r]** を **[有効（Enabled）]** に設定します。 **クライアント帯域選択** と **クライアント負荷分散** が無効になっていることを確認してください。

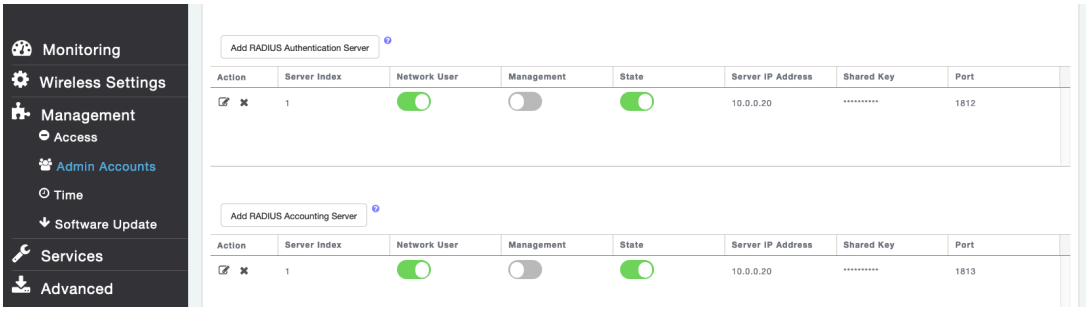
802.11k、802.11r、および 802.11v はサポートされていないため、無効にする必要があります。



RADIUS 認証サーバ および **アカウントサーバ** は、グローバルリストを上書きするために、WLAN レベルごとに設定することができます。

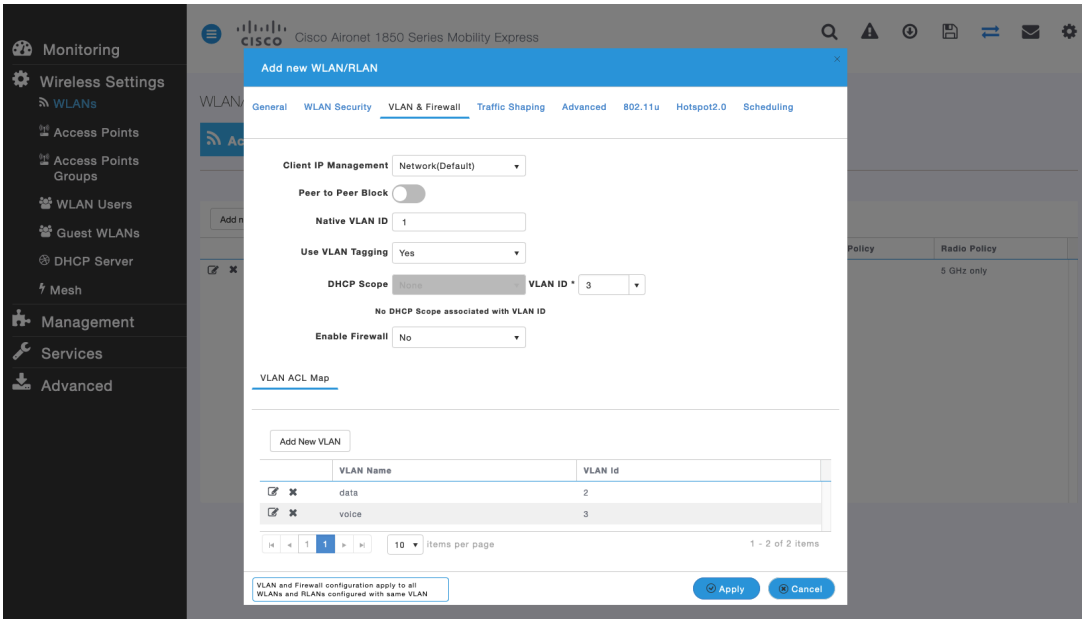

Add new WLAN/RLAN
General
WLAN Security
VLAN & Firewall
Traffic Shaping
Advanced
802.11u
Hotspot2.0
Scheduling
Guest Network
Captive Network Assistant
MAC Filtering
Security Type
WPA2Enterprise
Authentication Server
External Radius
Radius Profiling
BYOD
RADIUS Server
Authentication Caching
Add RADIUS Authentication Server
State
Server IP Address
Port
Enabled
10.0.0.20
1812
Add RADIUS Accounting Server
1813
Monitoring
Wireless Setti
WLANs
Access Points
Access Points Groups
WLAN Users
Guest WLANs
DHCP Server
Mesh
Management
Services
Advanced


Cisco Aironet 1850 Series Mobility Express
ADMIN ACCOUNTS
Users
1
Management User Priority Order
Local Admin Accounts
TACACS+
RADIUS
Auth Cached Users
Authentication Call Station ID Type
AP MAC Address:SSID
Authentication MAC Delimiter
Hyphen
Accounting Call Station ID Type
IP Address
Accounting MAC Delimiter
Hyphen
Fallback Mode
Passive
Username
cisco-probe
Interval
300
Seconds
AP Events Accounting
Apply
Monitoring
Wireless Settings
Management
Access
Admin Accounts
Time
Software Update
Services
Advanced

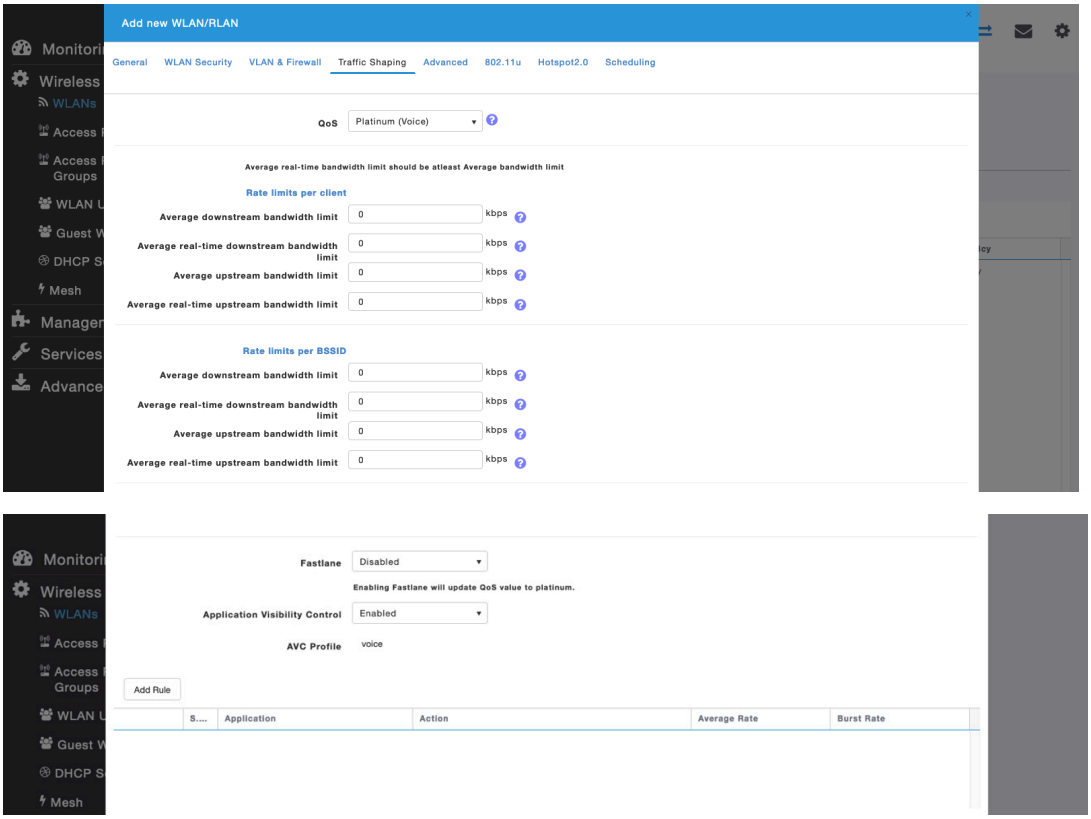

Add RADIUS Authentication Server
Action
Server Index
Network User
Management
State
Server IP Address
Shared Key
Port
1
10.0.0.20
1812
Add RADIUS Accounting Server
1813
Monitoring
Wireless Settings
Management
Access
Admin Accounts
Time
Software Update
Services
Advanced

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

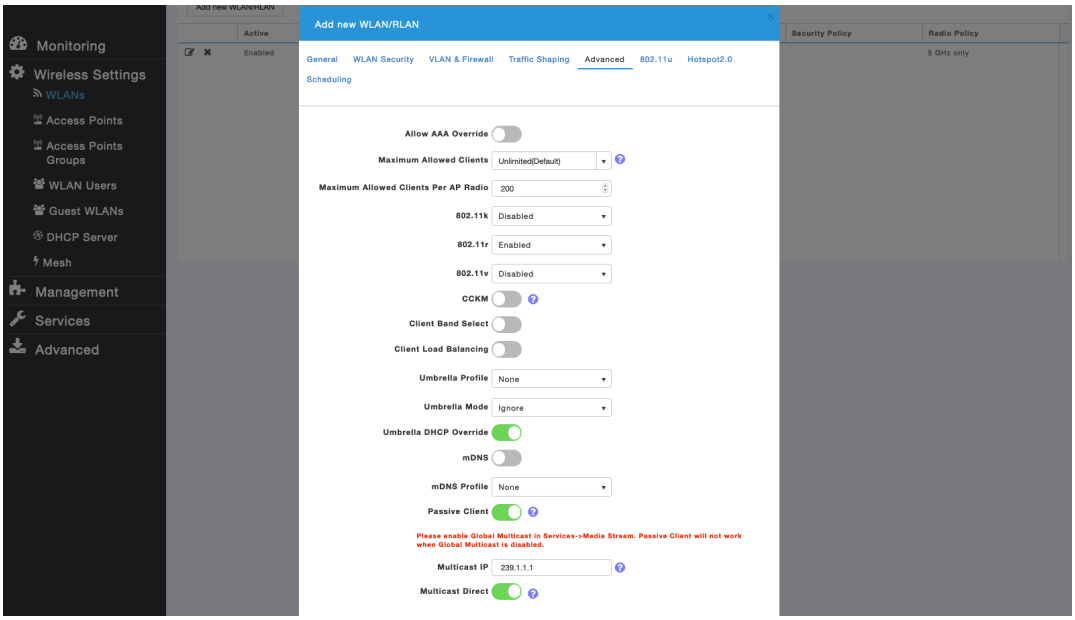
[ピアツーピアブロック（Peer to Peer Block）] を無効にします。



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

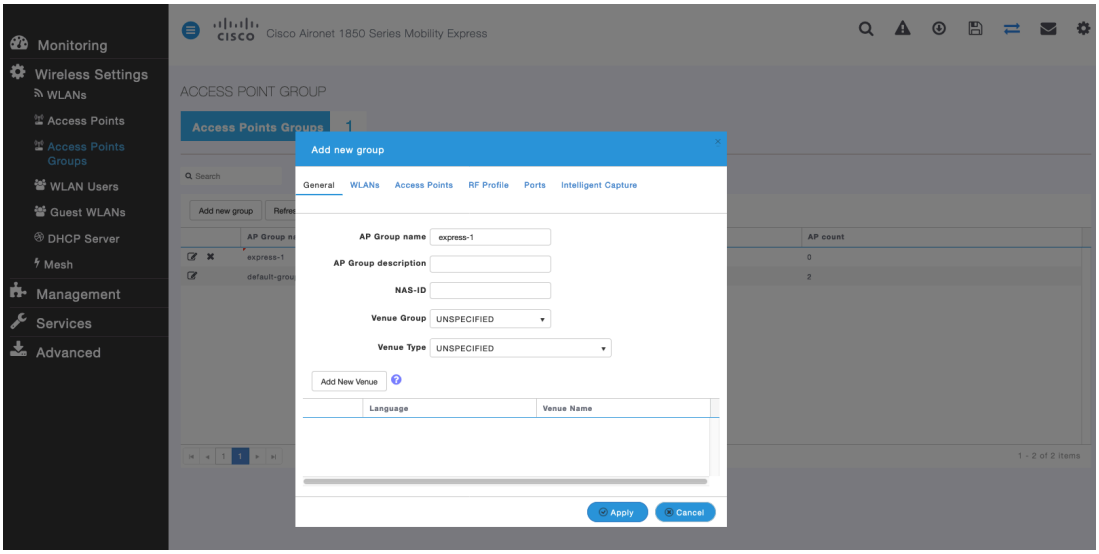


最大クライアント数 と **AP 無線ごとの最大許容クライアント** は必要に応じて設定します。

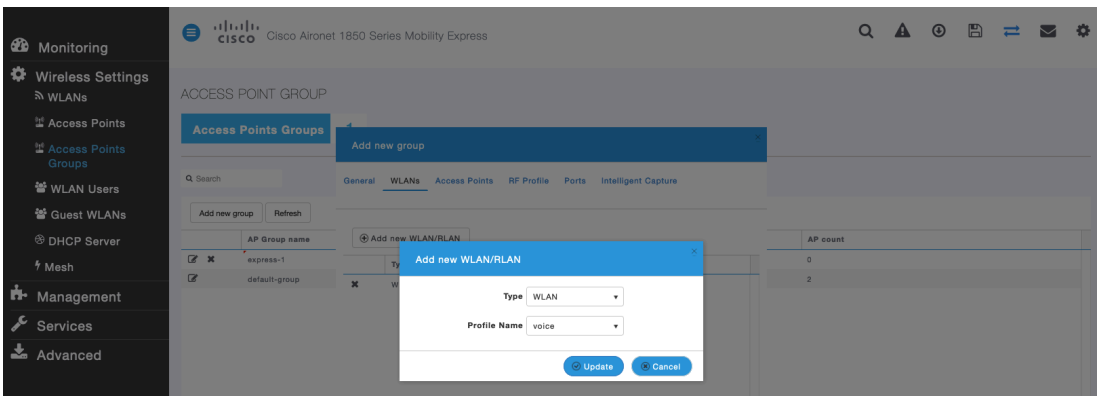


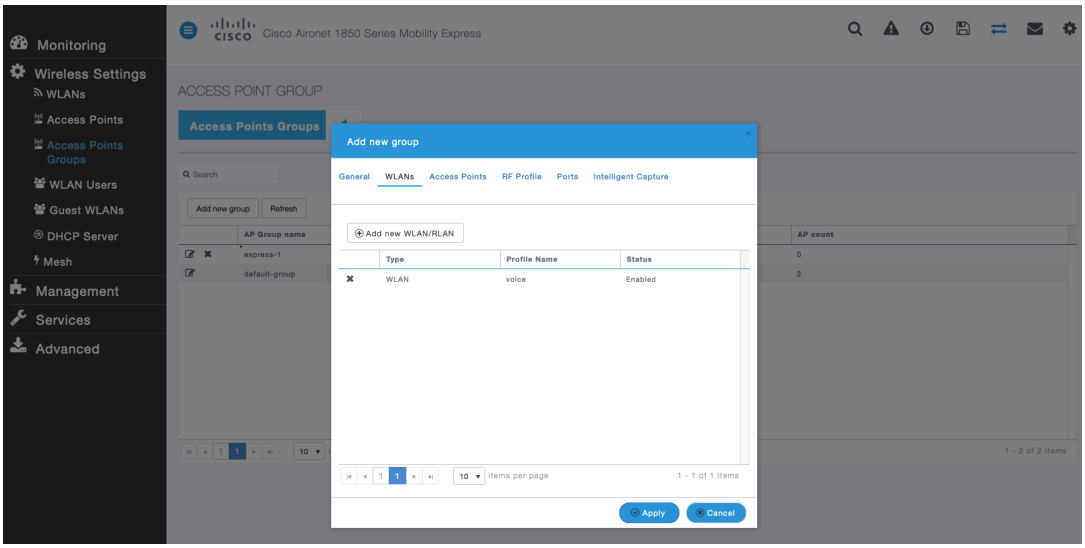
AP グループ

AP グループを作成して、どの WLAN を有効にするか、どのインターフェイスをマッピングするか、および 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 RF プロファイル パラメータを指定することができます。

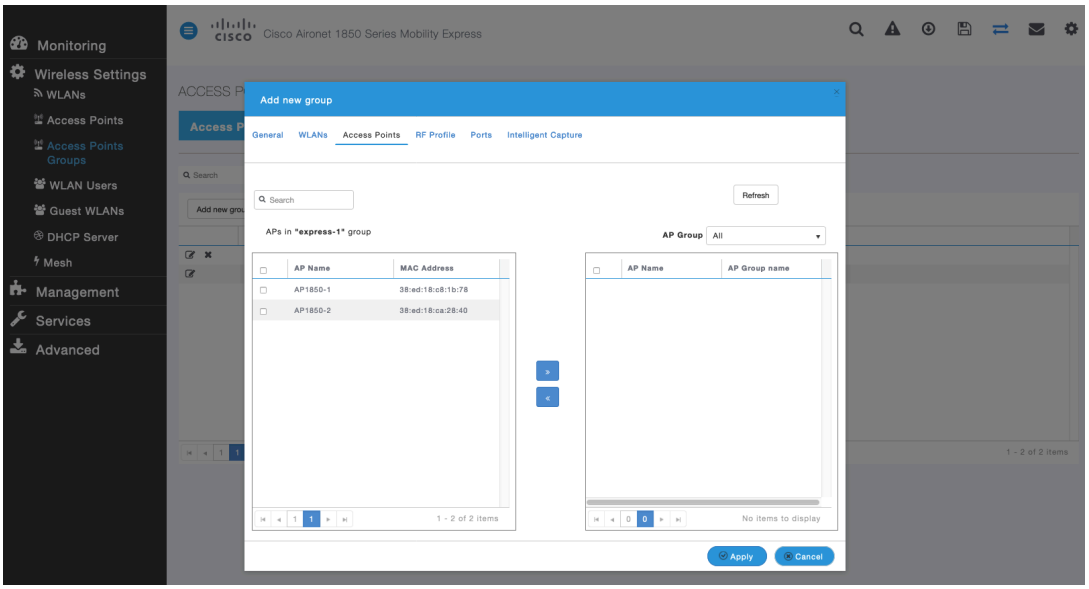


[WLAN（WLANs）] タブで、目的の WLAN とマッピングするインターフェイスを選択して、**[追加（Add）]** を選択します。

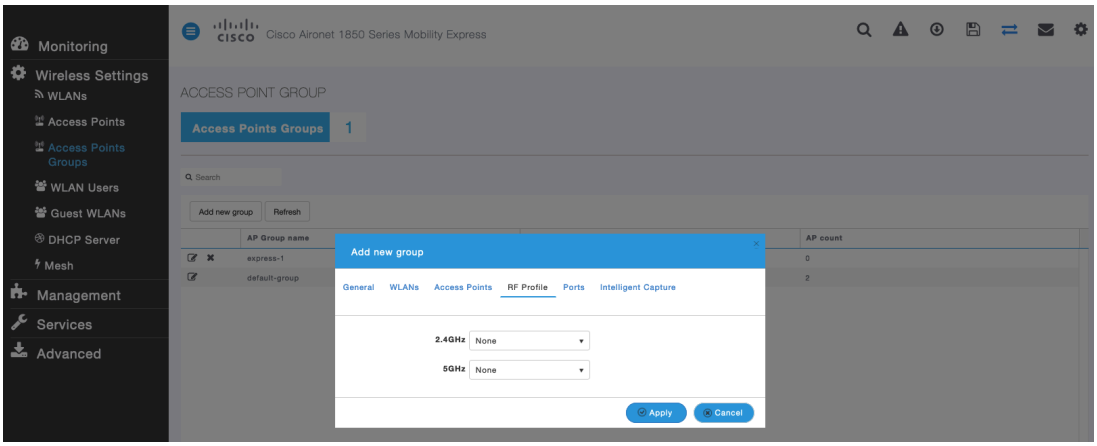




[アクセスポイント（Access Points）] タグで、目的のアクセスポイントを選択し、**[適用（Apply）]** を選択します。次に、これらのアクセスポイントをリブートします。



[RF プロファイル] タブで、目的の **2.4GHz** または **5GHz** RF プロファイルを選択するには、**[適用] を選択します。**



RF プロファイル

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

Cisco デスク フォン 9800 シリーズで使用される SSID については、5 GHz 無線にのみ適用することを推奨します。

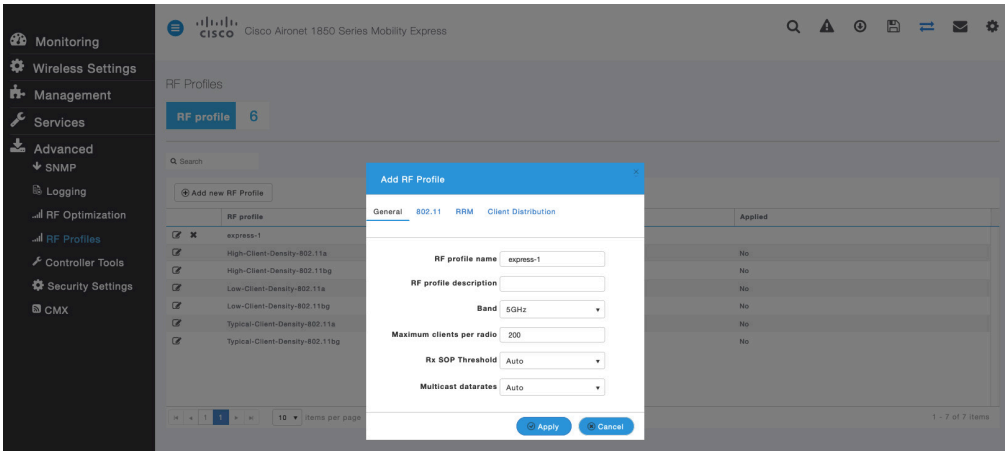
いったん作成されると、RF プロファイルは AP グループに適用されます。

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）] に対して、**[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）]、[Rx Sopしきい値（Rx Sop Threshold）] を設定します。

Rx Sop Threshold はデフォルト値 (**Auto**) にすることを推奨します。

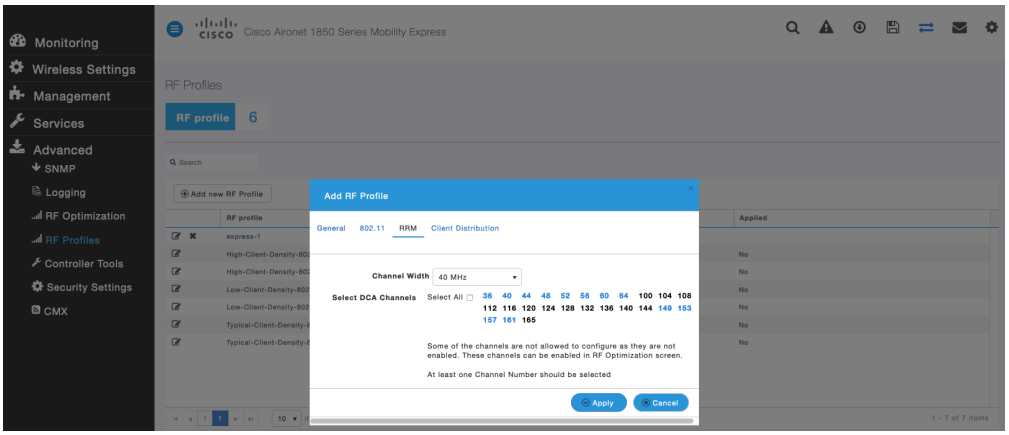


[802.11] タブで、必要に応じてデータレートを設定します。

12 Mbp を **[必須（Mandatory）]** に 18 Mbps 以上を **[サポート対象（Supported）]** にすることが推奨されます。

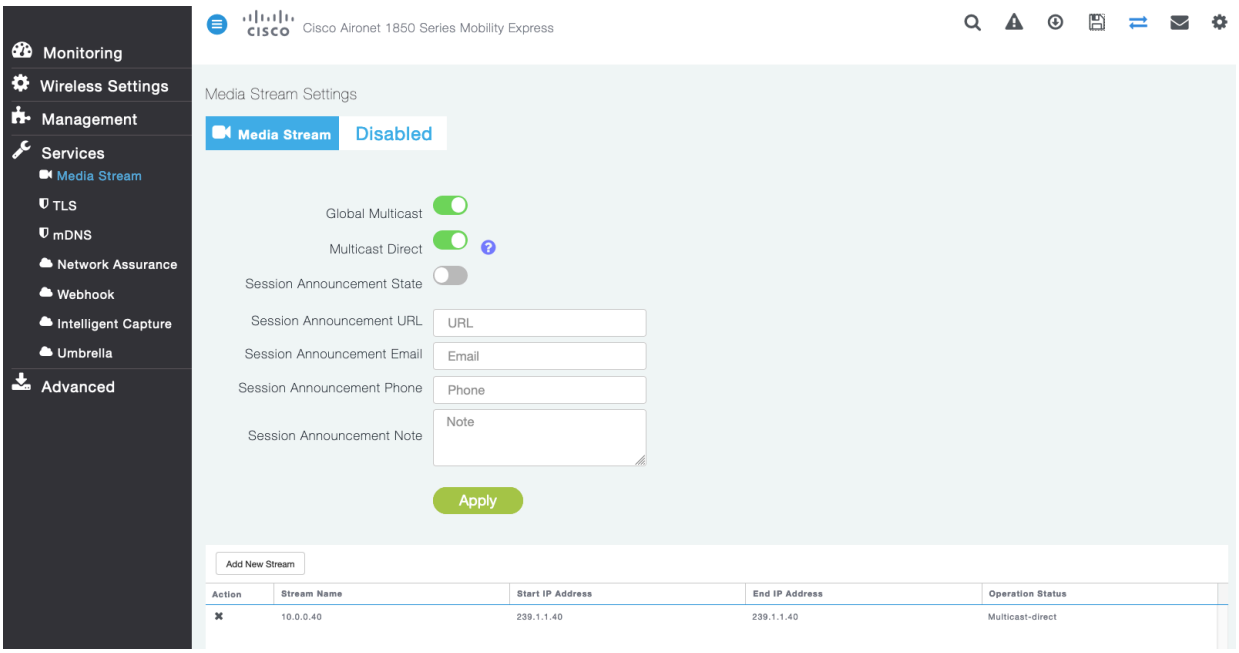
ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。

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

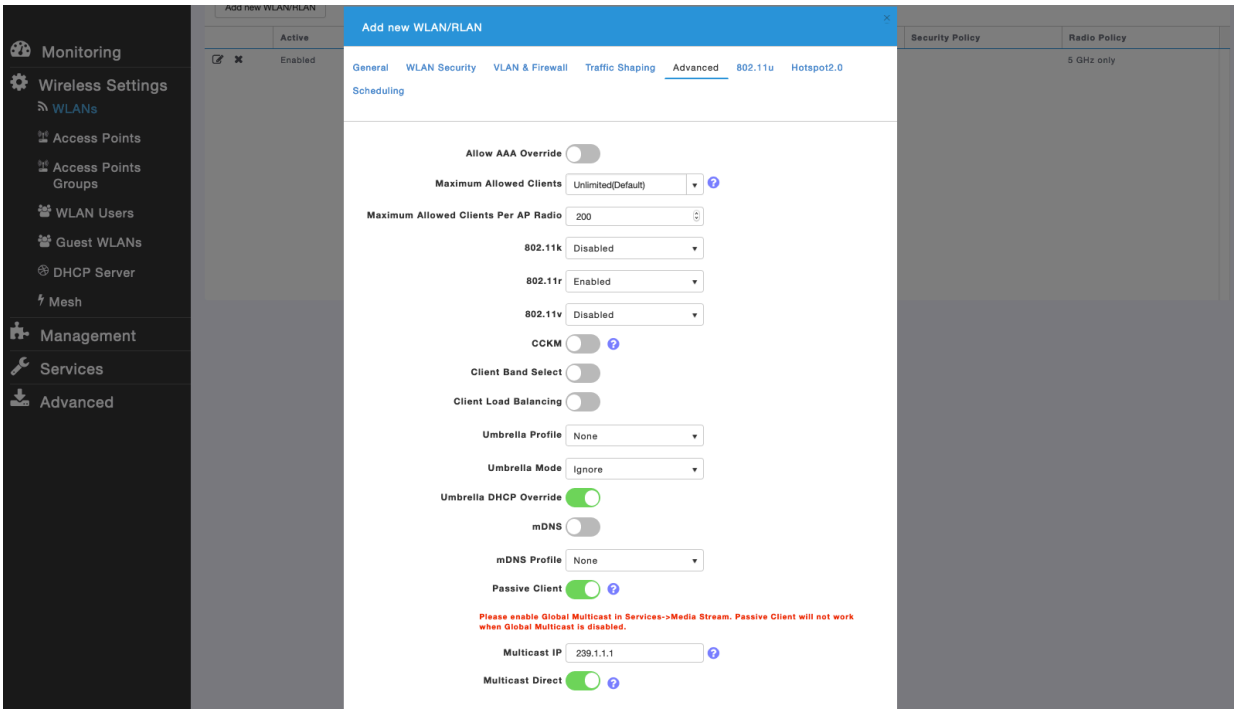


マルチキャストダイレクト

[メディアストリーム（Media Stream）]設定で、**[ゴールドマルチキャスト（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 Direct）]** を有効にした後、WLAN 設定の**[詳細設定（Advanced）]** タブで、**[マルチキャストダイレクト（Multicast Direct）]** を有効にします。


Monitoring
Wireless Settings
WLANs
Access Points
Access Points Groups
WLAN Users
Guest WLANs
DHCP Server
Mesh
Management
Services
Advanced
Add new WLAN/RLAN
Active
Enabled
Security Policy
Radio Policy
5 GHz only
Add new WLAN/RLAN
General
WLAN Security
VLAN & Firewall
Traffic Shaping
Advanced
802.11u
Hotspot2.0
Scheduling
Allow AAA Override
Maximum Allowed Clients
Unlimited(Default)
Maximum Allowed Clients Per AP Radio
200
802.11k
Disabled
802.11r
Enabled
802.11v
Disabled
CCKM
Client Band Select
Client Load Balancing
Umbrella Profile
None
Umbrella Mode
Ignore
Umbrella DHCP Override
mDNS
mDNS Profile
None
Passive Client
Please enable Global Multicast in Services->Media Stream. Passive Client will not work when Global Multicast is disabled.
Multicast IP
239.1.1.1
Multicast Direct

Cisco Autonomous（自律）アクセス ポイント

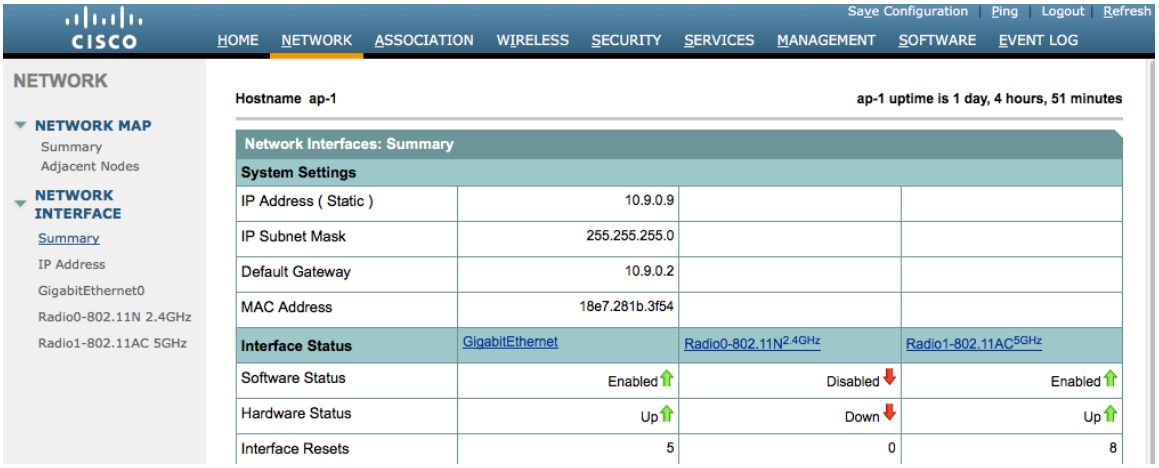
Cisco Autonomous アクセス ポイントを設定する場合、次のガイドラインに従ってください。

- **802.11r (FT) を有効にする**
- **[CCKM]** を無効にします
- **[802.11k]**を無効にします
- **[802.11v]**を無効にします
- 必要に応じて **データレート** を設定します
- **Quality of Service（QoS）** の設定
- **WMM ポリシー** を「**必須**」**に設定します。**
- **Aironet 拡張機**を無効にします
- **パブリックセキュアパケット転送 (PSPF) を無効にする**
- **IGMP スヌーピング** を **有効に設定する**

802.11 ネットワーク設定

Cisco Desk Phone 9800 シリーズは 5 GHz 帯域のみで運用することを推奨します。利用できるチャネル数が多く、2.4 GHz 帯域に比べて干渉が少ないためです。

5 GHz を使用するには、802.11a/n ネットワークの状況が **有効** になっていることを確認してください。



必須 (基本) レートとして 12 Mbps を設定し、サポートされている (オプション) レートとして 18 Mbps 以上を設定することをお勧めします。 ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を有効にする必要があります。

5 GHz を使用する場合、多くのチャネルをスキャンすることによるアクセスポイント検出の遅延を避けるために、最大 12 チャネルのみを有効にすることをお勧めします。

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 が有効な場合、少なくとも 1 つの帯域 (帯域 1-4) を有効にします。

アクセスポイントが UNII-1 チャネル (チャネル 36、40、44、または 48) を使用する場合にのみ、帯域 1 を選択できます。

利用する周波数に周波数帯に応じて、5GHz または 2.4GHz のいずれかで動的チャネルと送信電力の割り当てを使用するように、個々のアクセスポイントは全体設定をオーバーライドするように設定できます。

他のアクセスポイントは、自動 RF に対して有効にすることができ、静的に設定されたアクセスポイントを対処します。

これは、その地域で断続的な干渉源がある場合に必要になります。

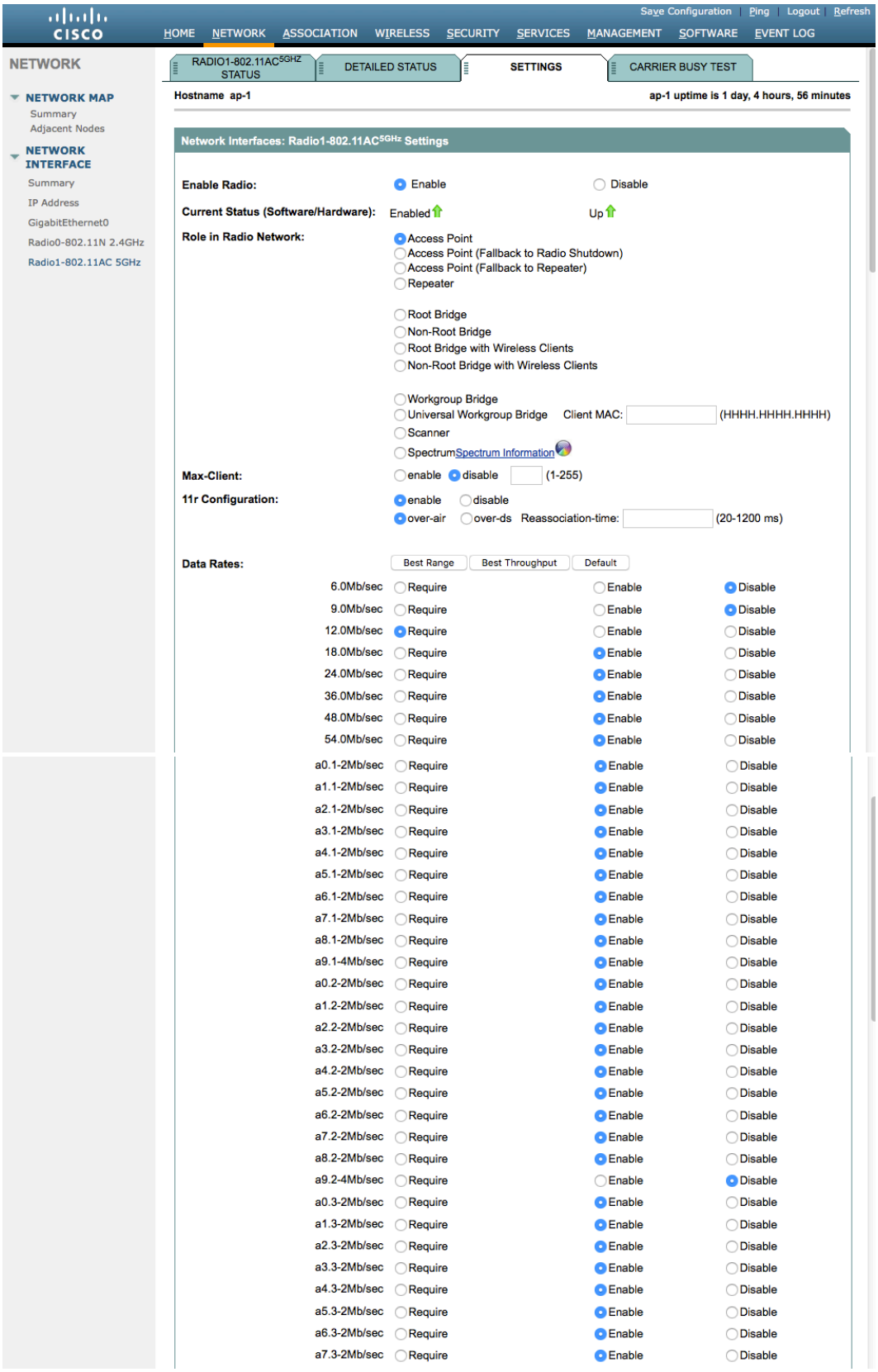
5 GHz チャネル幅は、Cisco 802.11n アクセスポイントを使用する場合は 20 MHz または 40 MHz として、Cisco 802.11ac アクセスポイントを使用する場合は 20 MHz、40 MHz、または 80 MHz として構成できます。

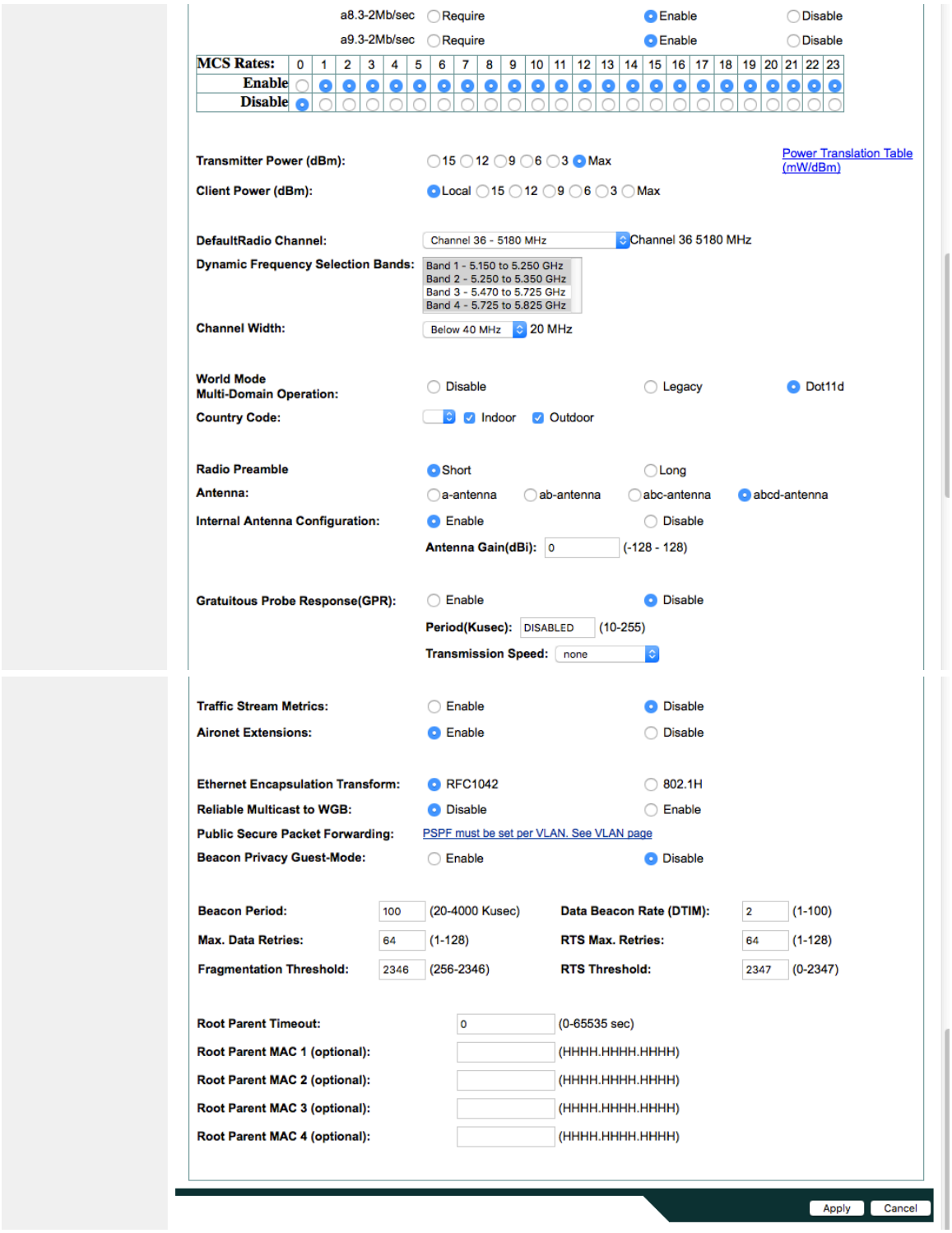
すべてのアクセスポイントで同じチャネル幅を使用することを推奨します。

[ワールドモード（World Mode）] に対して、**[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 が無効になっていることを確認してください。

[ビーコン期間（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 を使用するには、802.11b/g/n ネットワーク状況と 802.11g が有効になっていることを確認してください。

必須 (基本) レートとして 12 Mbps を設定し、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と想定して、サポートされている (オプション) レートとして 18 Mbps 以上を設定することをお勧めします。ただし、一部の環境では、必須の (基本) レートとして 6 Mbps を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、11 Mbps を必須 (基本) レートとして設定し、12 Mbps 以上をサポート (オプション) として設定する必要があります。

[IVR設定(WLAN Settings)]

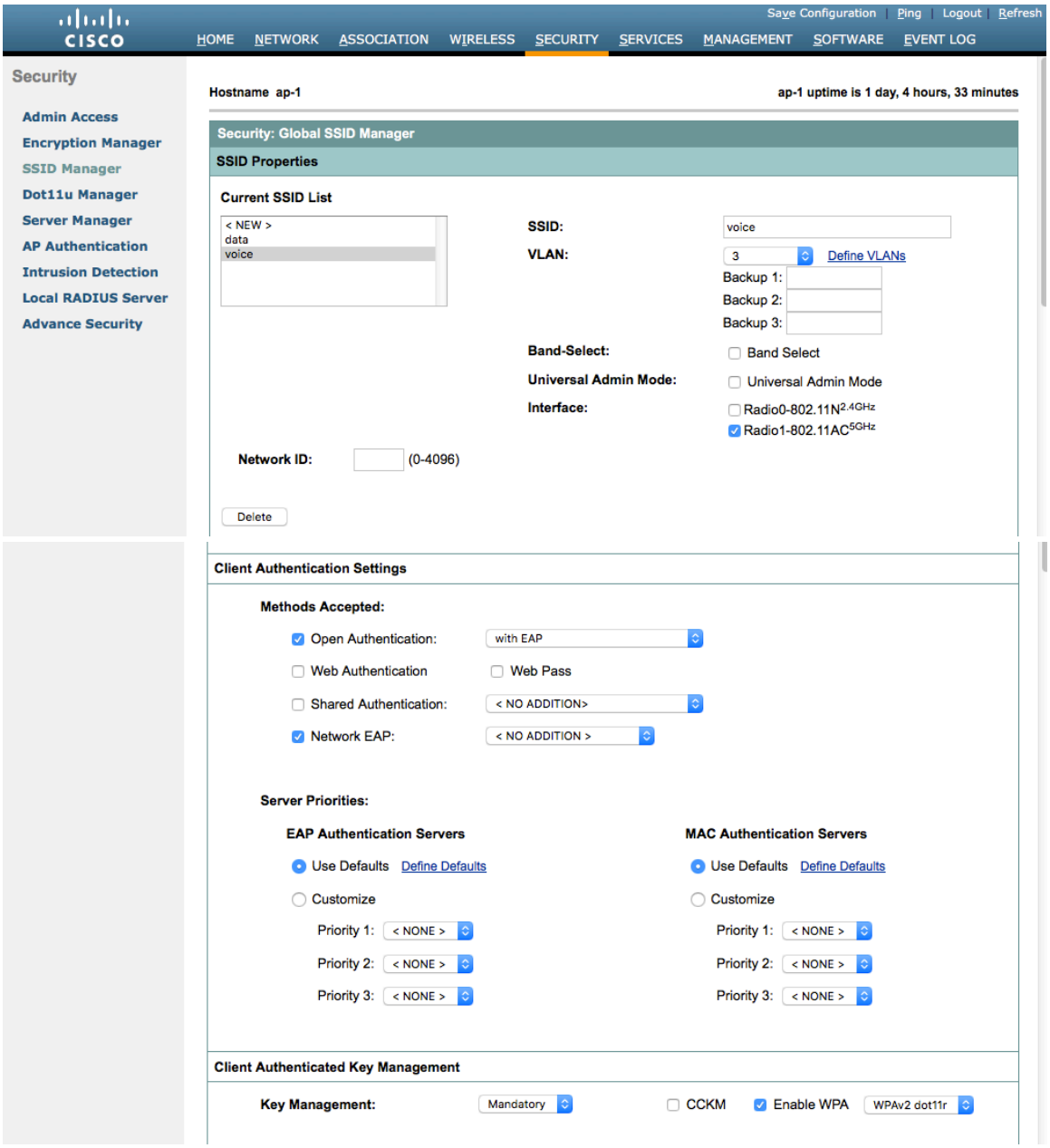
Cisco Desk Phone 9800 シリーズには別の SSID を割り当てることを推奨します。

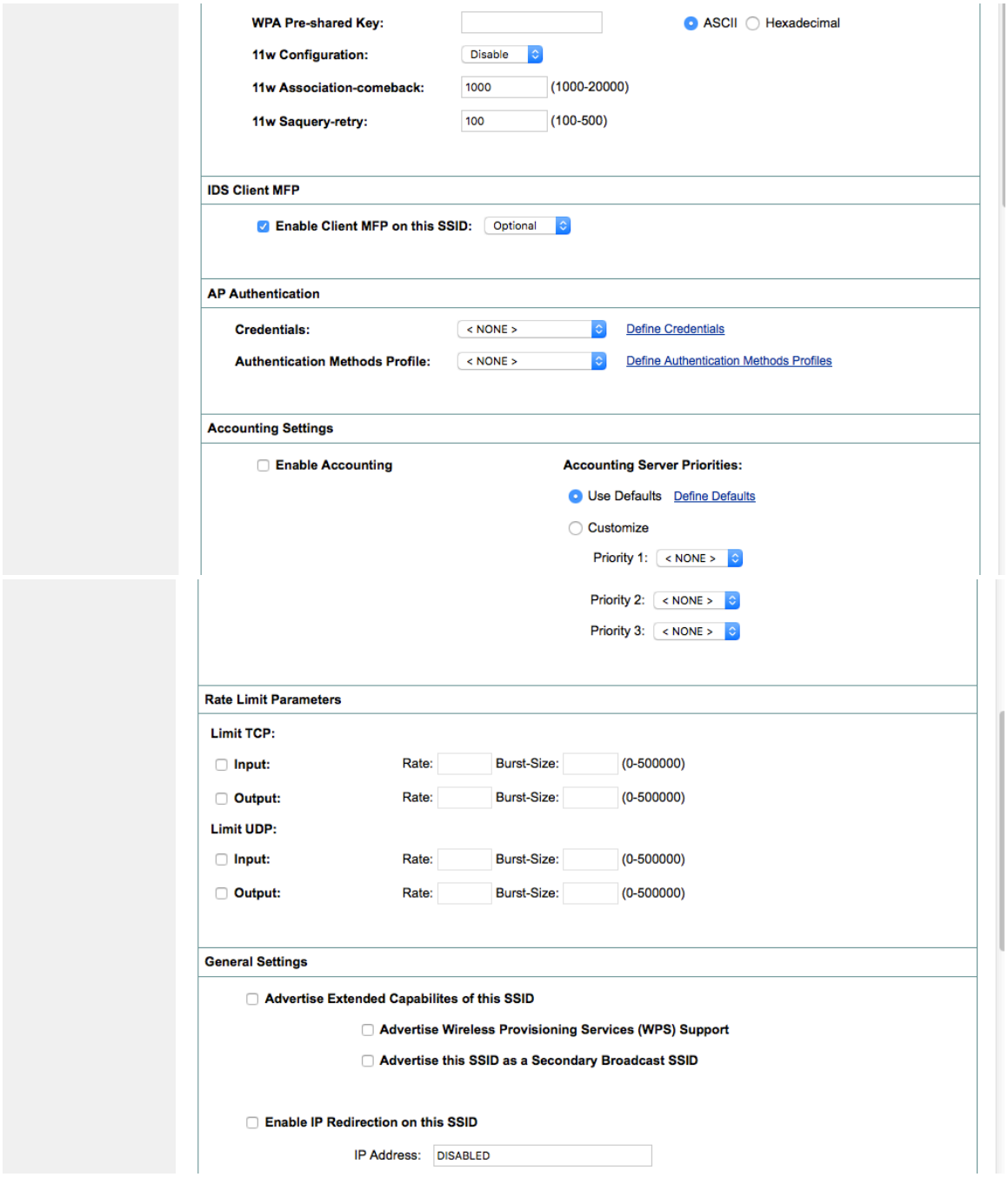
しかし、音声対応 Cisco ワイヤレス LAN エンドポイントをサポートするように設定された既存の SSID を使用することもできます。

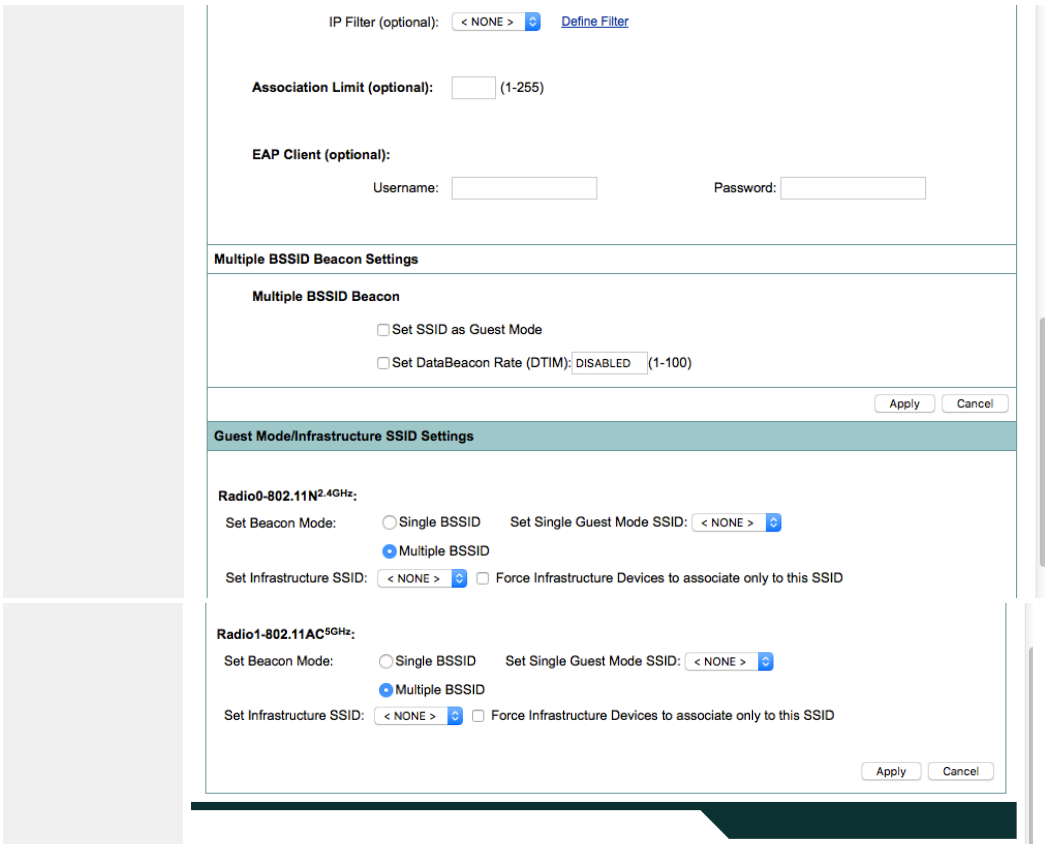
Cisco Desk Phone 9800 シリーズで使用される SSID は、特定の 802.11 無線タイプのみに適用されるように設定できます (例、802.11a のみ)。

[WPA2/WPA3] キー管理を有効にします。

高速セキュアローミングに対して 11r が有効になっていることを確認します。

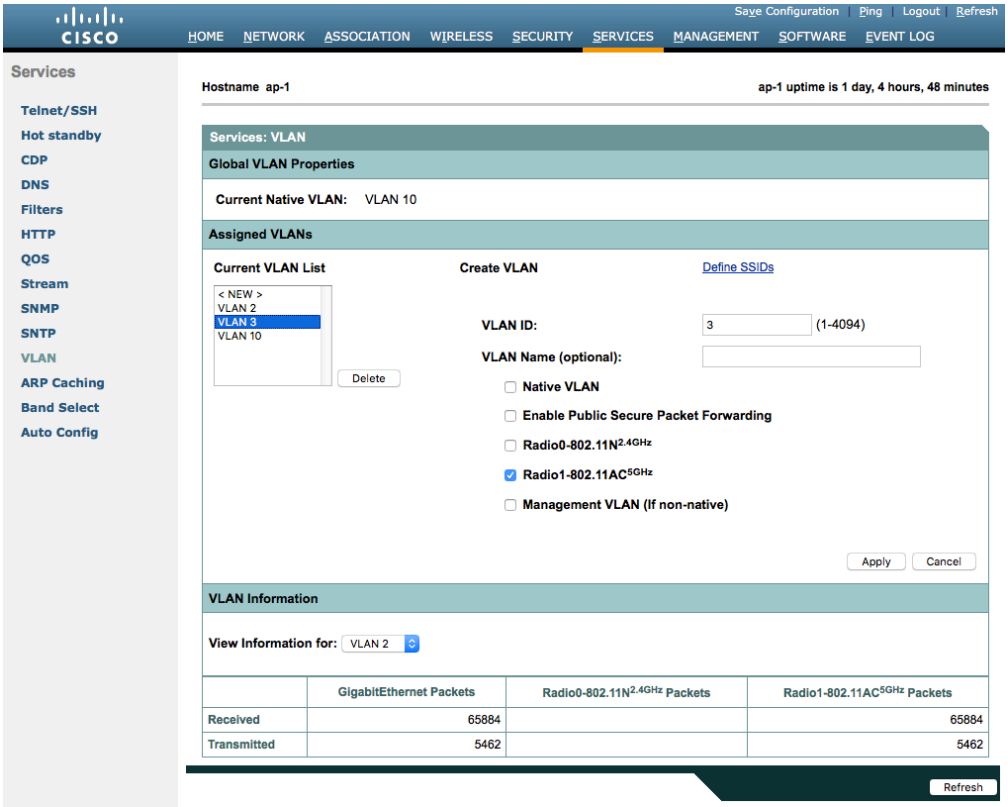



WPA Pre-shared Key:
ASCII
Hexadecimal
11w Configuration:
Disable
11w Association-comeback:
1000
(1000-20000)
11w Saquery-retry:
100
(100-500)
IDS Client MFP
Enable Client MFP on this SSID:
Optional
AP Authentication
Credentials:
< NONE >
Define Credentials
Authentication Methods Profile:
< NONE >
Define 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

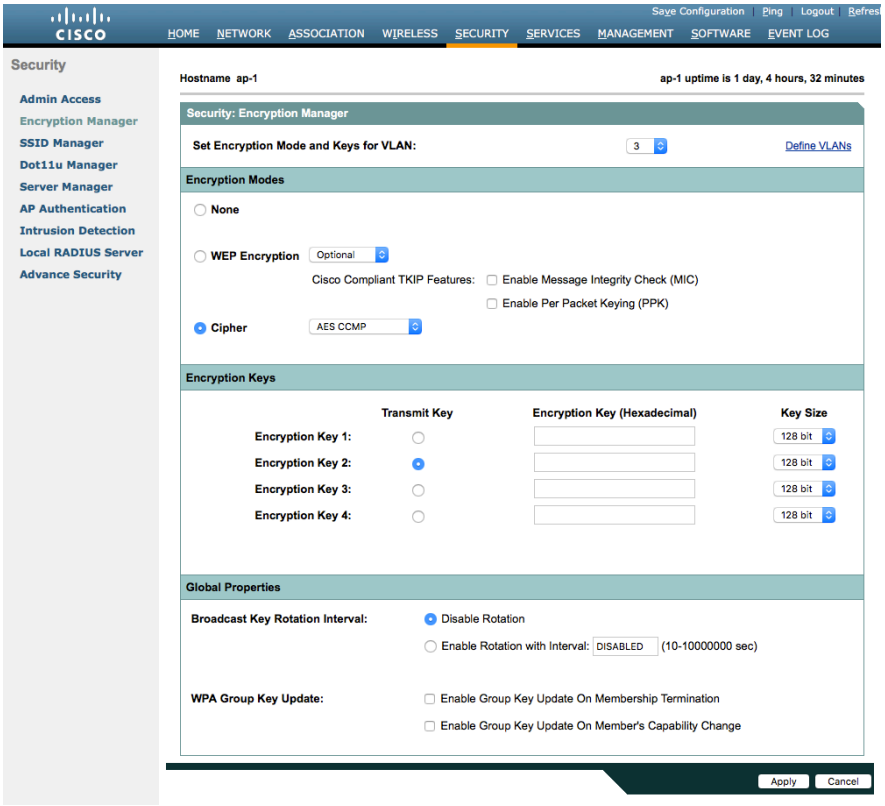


ワイヤレス音声とデータを個別の VLAN にセグメント化します。

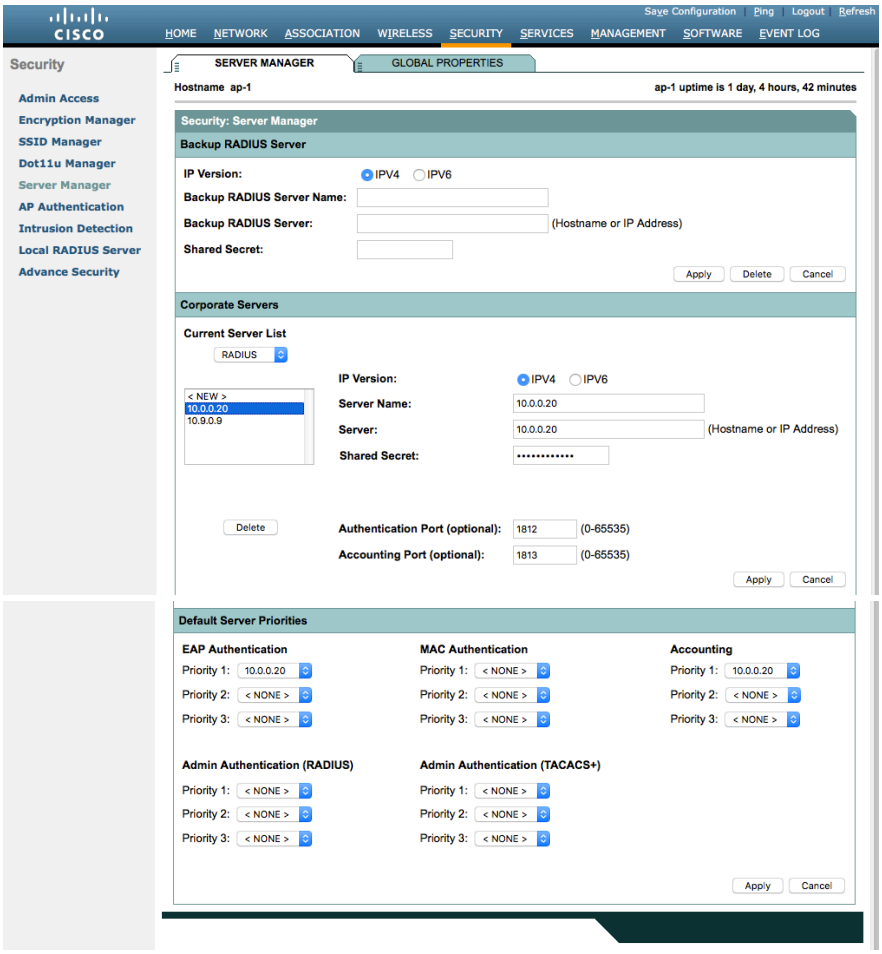
同じアクセスポイントに接続するクライアント間での直接通信を防ぐため、音声 VLAN に対してPublic Secure Packet Forwarding（PSPF）が有効になっていないことを確認します。 このシナリオで PSPF を有効にすると、音声通信が中断されます。



暗号化タイプで **[AES]** が選択されていることを確認します。



認証とアカウントのために RADIUS サーバーを設定します。

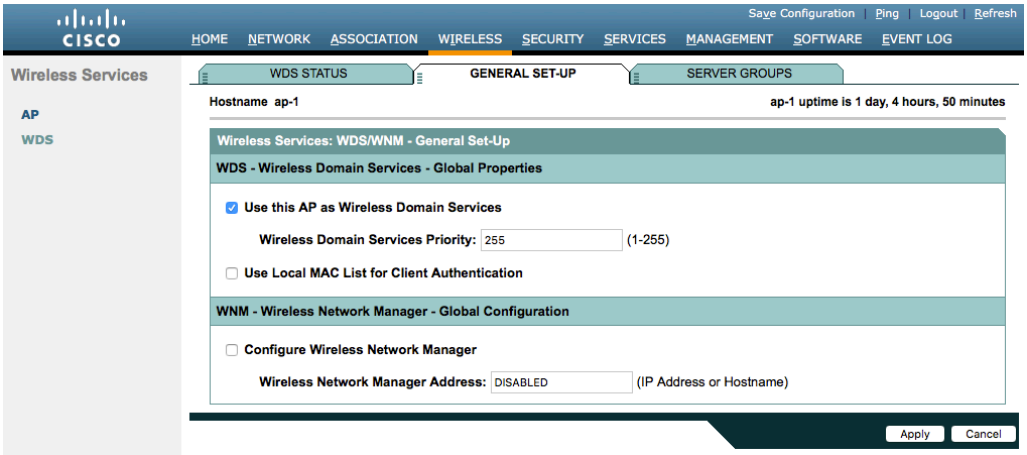


ワイヤレス ドメイン サービス (WDS)

Wireless Domain Services は、Cisco Autonomous Access Point 環境で利用する必要があり、これは、高速セキュアローミングを実現するためにも必要です。

1 台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、別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。

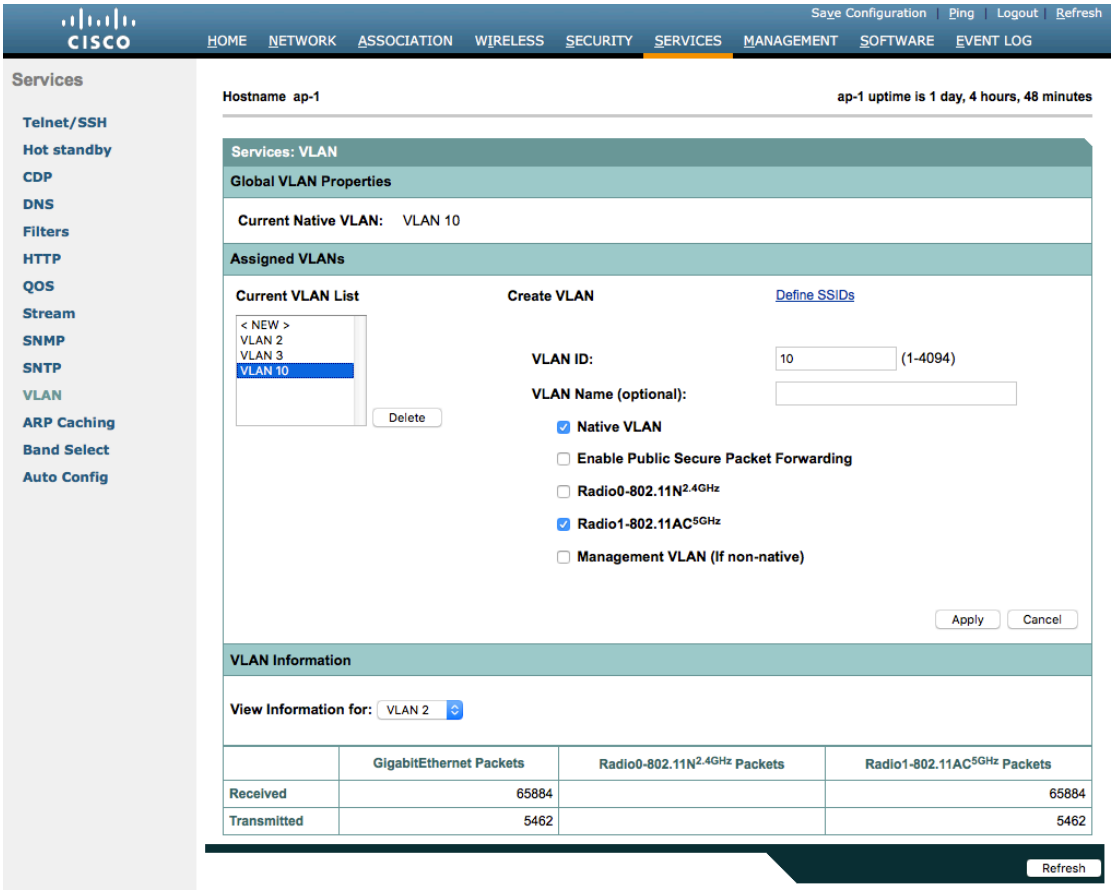
プライマリ WDS サーバを最高の優先順位 (例えば 255) で構成し、バックアップ WDS サーバをより低い優先順位 (例えば 254) で構成します。



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) を利用します。 そのため、Cisco Autonomous アクセスポイントには、専用のネイティブ VLAN が推奨されます。

ネイティブ VLAN については、IAPP パケットが正常に交換されるように、VLAN 1 を使用しないことをお勧めします。

Cisco Autonomous Access Point が直接接続されているスイッチ 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。

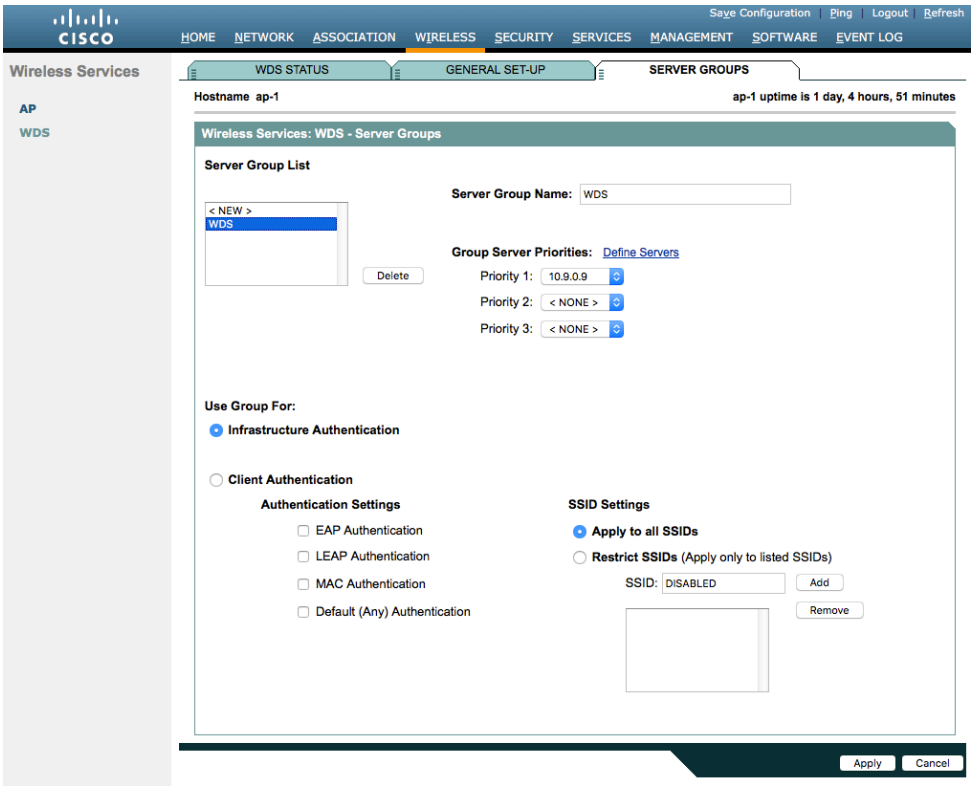


ワイヤレスドメインサービスのサーバグループが定義されている必要があります。

まず、インフラストラクチャ認証で使用するサーバグループを定義します。

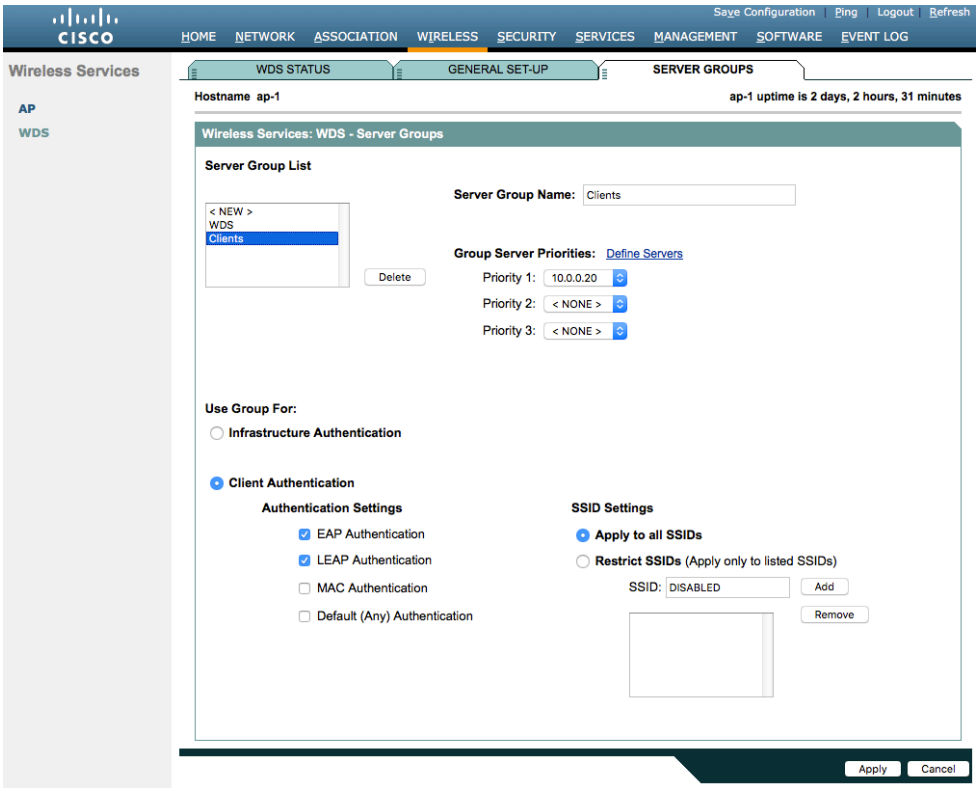
インフラストラクチャ認証にはローカル RADIUS の使用が推奨されます。

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、Wireless Domain Services が有効になっているすべてのアクセスポイントが RADIUS サーバーで構成されていることを確認します。

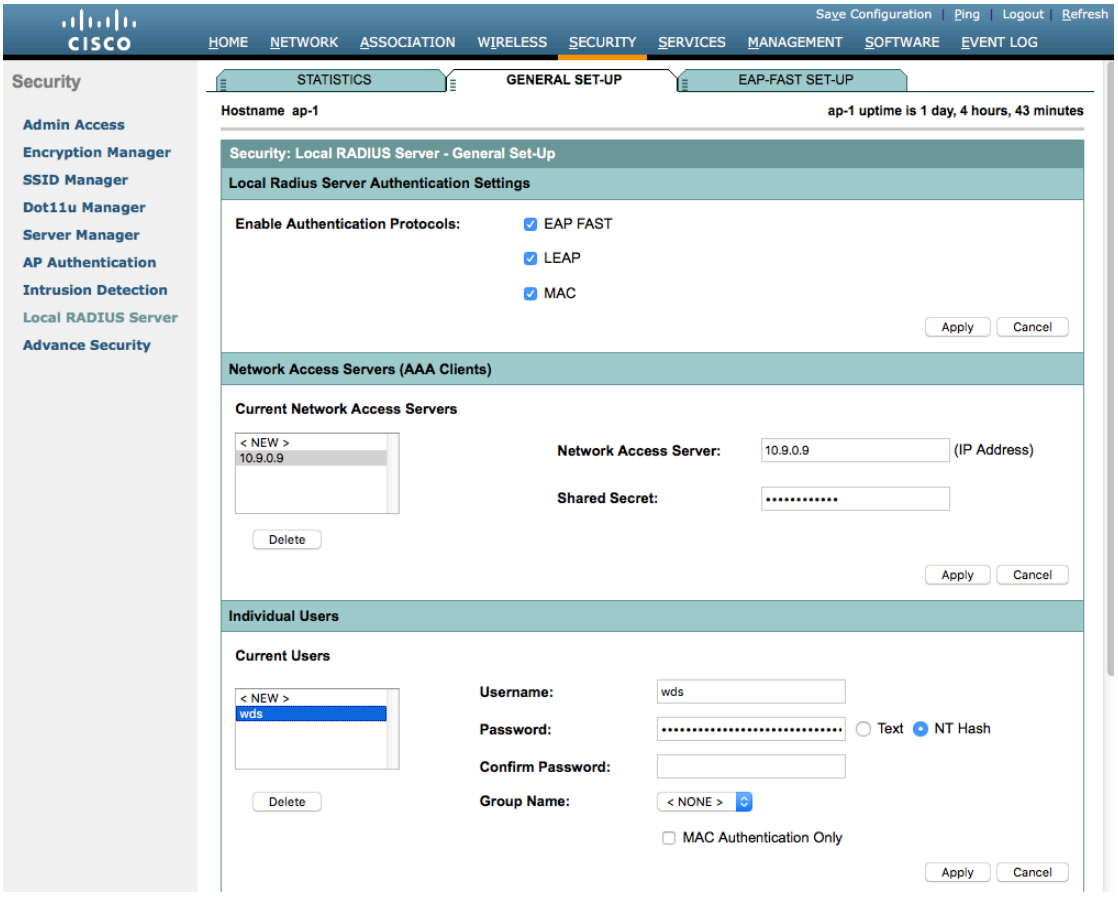


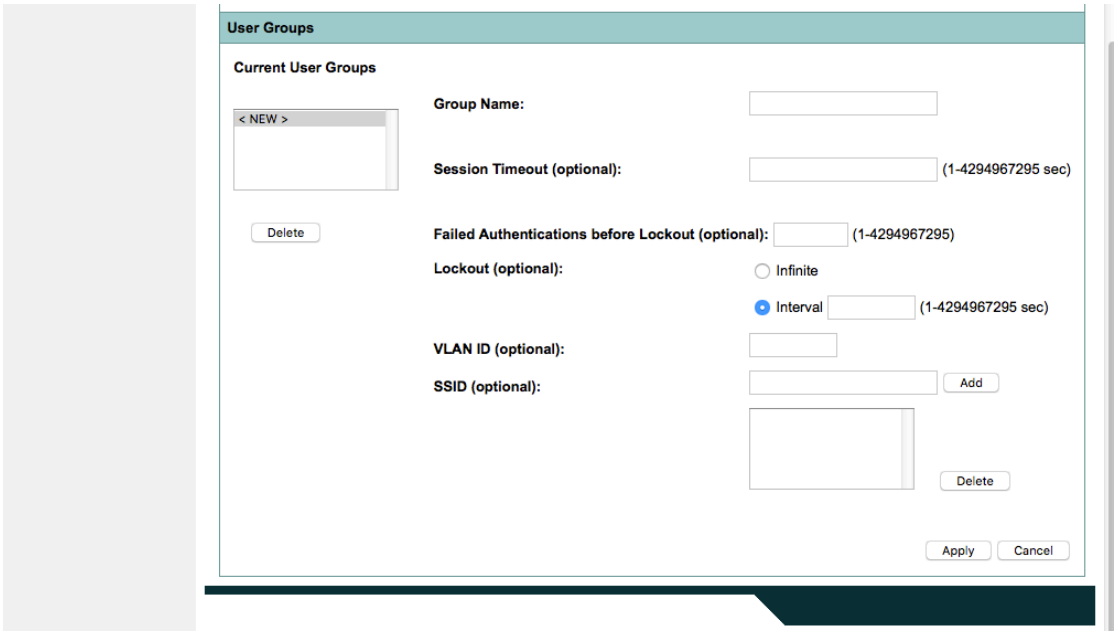
次に、クライアント認証に使用するサーバグループを定義します。

Wireless Domain Services が有効になっているすべてのアクセスポイントが RADIUS サーバーで構成されていることを確認します。



インフラストラクチャ認証にローカル RADIUS を使用するには、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に対して、**[ネットワークアクセスサーバー（Network Access Server）]** エントリを作成します。
有効になっているワイヤレス ドメイン サービスへの認証用のアクセス ポイントを構成するために使用するユーザ アカウントを定義しますアクセスポイント。
ワイヤレス ドメイン サービスに参加している各アクセス ポイントで、ローカル RADIUS を設定します。



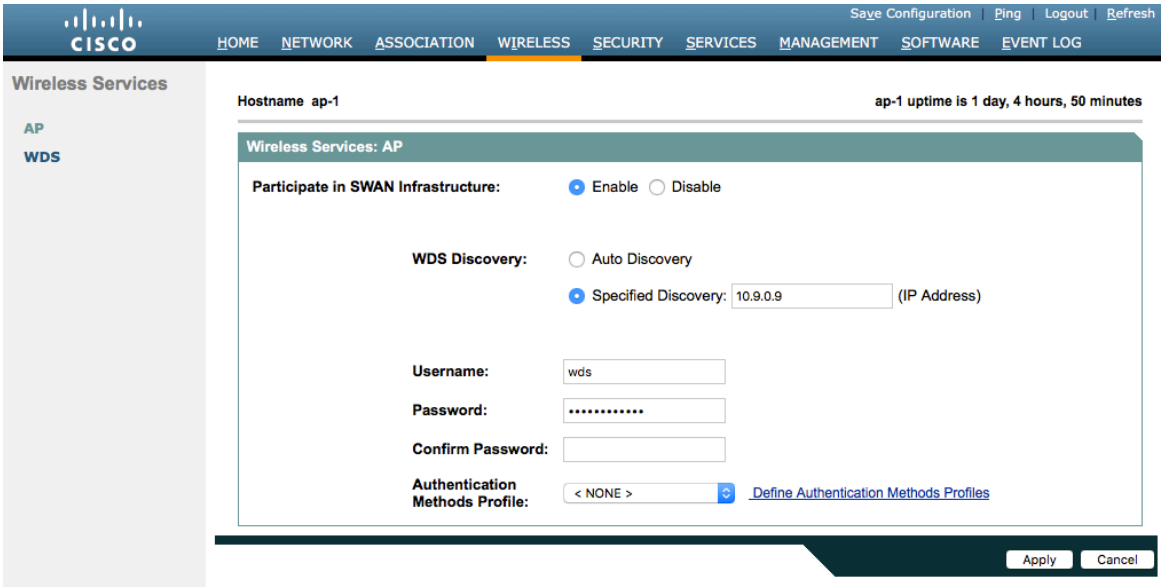


目的のアクセスポイントがワイヤレスドメインサービスを有効にするように構成されたら、WDS サーバとして機能するアクセスポイントを含むすべてのアクセスポイントが、WDS サーバに対して認証できるように構成される必要があります。

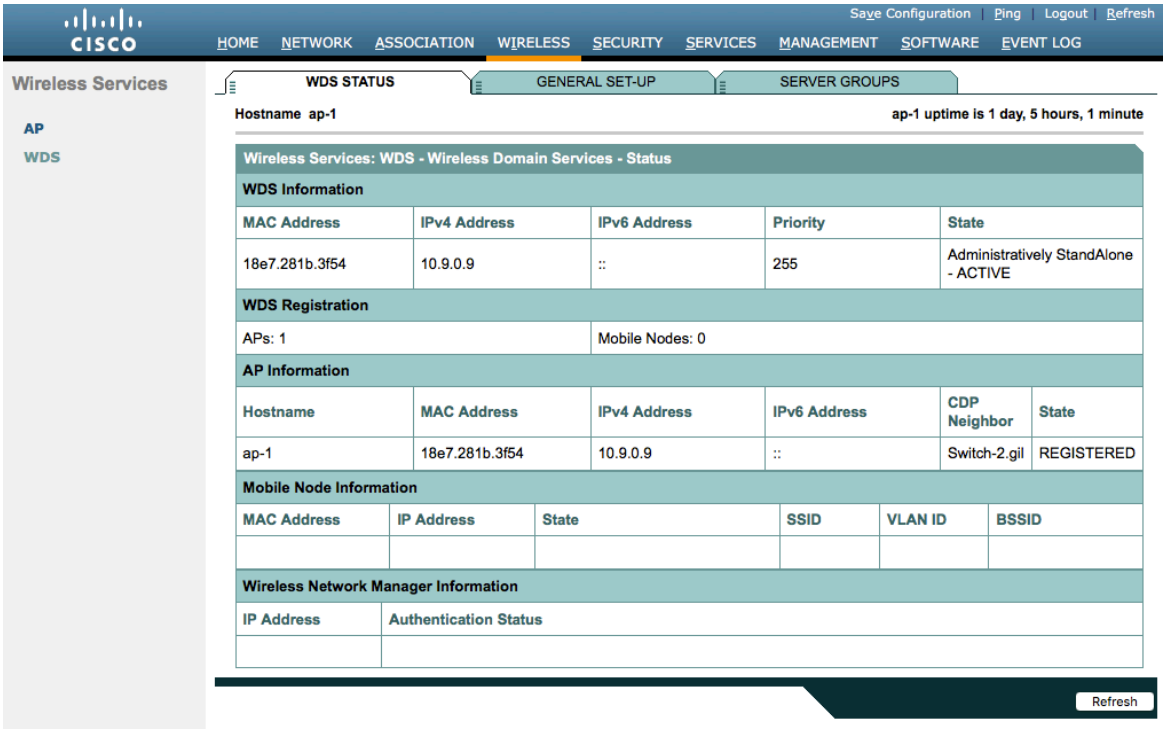
[SWANインフラストラクチャに参加（Participate in SWAN Infrastructure）] を有効にします。

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

ユーザ名 と **パスワード** を入力して WDS サーバの認証を行ってください。



WDS サーバ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と、[WDS ステータス] をチェックして、WDS サーバの状態および 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。



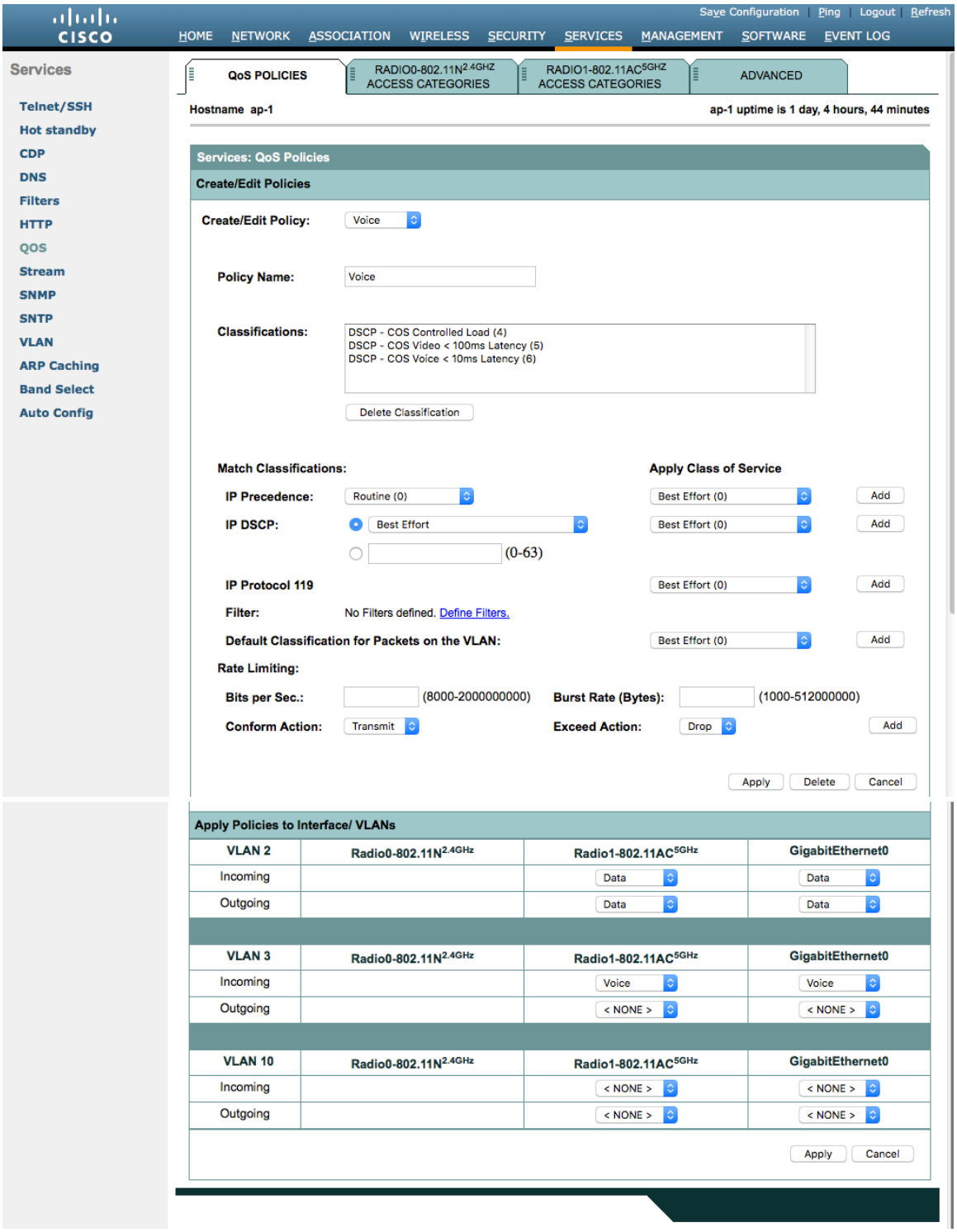
コール アドミッション制御（CAC）

無効になっています 。

QoS ポリシー

Cisco Autonomous アクセス ポイントで次の QoS ポリシーを設定し、DSCP から CoS (WMM UP) へのマッピングを有効にします。

これにより、アクセス ポイント レベルで受信されたときに正しくマークされている限り、パケットは適切なキューに配置されます。

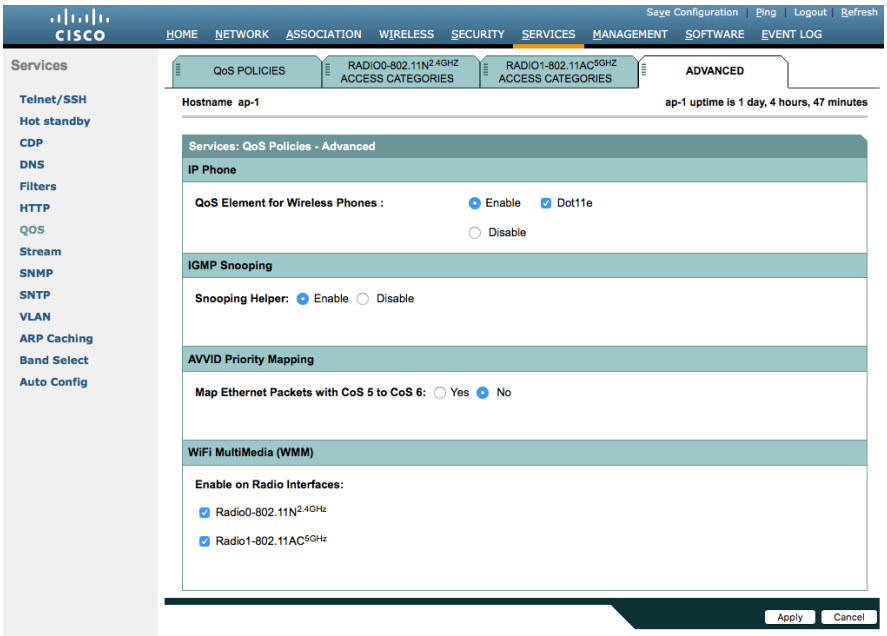


QBSS を有効にするには、[**有効にする**] を選択し、[**Dot11e**] にチェックを入れます。

Dot11e にチェックが入っている場合、CCA バージョン (802.11e および Cisco バージョン 2) の両方が有効になります。

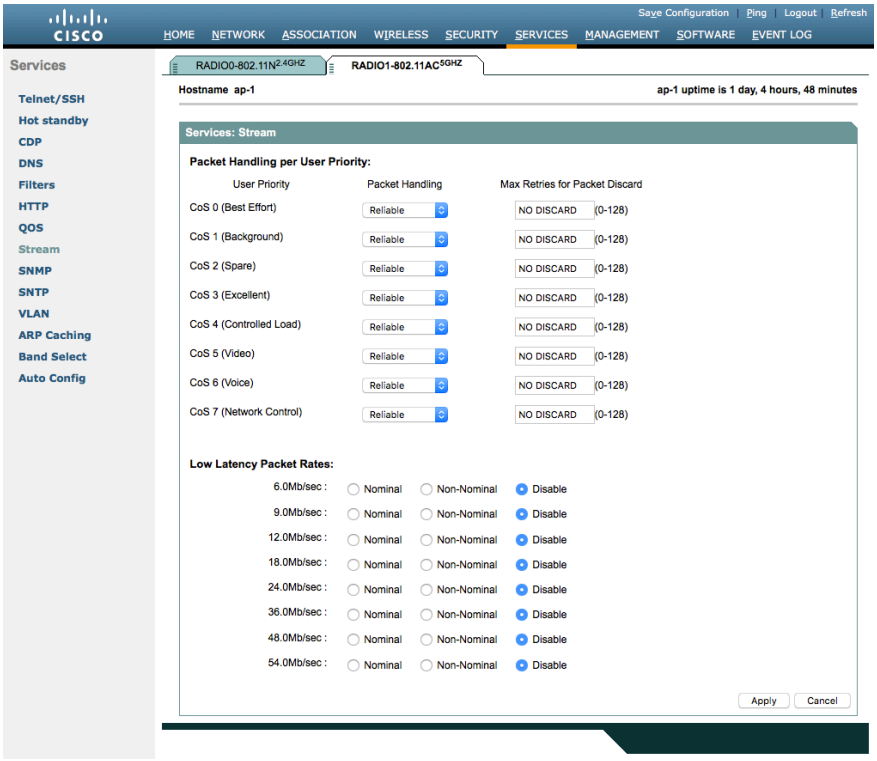
IGMP スヌーピング が有効になっていることを確認してください。

Wi-Fi マルチメディア (WMM) が有効になっていることを確認してください。



[QoS設定（QoS configuratio）] セクションの無線アクセスカテゴリーに対して選択した **[最適化音声（Optimized Voice）]** を介すか、直接 **[ストリーム（Stream）]** 機能を有効にする場合は、デフォルト設定を使用します。これらのデフォルトには、802.11b/g、6、12 向けの通常レートとして有効な 5.5、6、11、12、24 Mbps と 802.11a 向けの 24 Mbps と、802.11n 向けの 6.5、13 および 26 Mbps が含まれます。

ストリーム 機能が有効な場合、音声パケットのみを音声キューに入れるようにしてください。 シグナリング パケット (SIP) は別のキューに配置する必要があります。 これは、DSCP を適切なキューにマッピングする QoS ポリシーをセットアップすることで実現できます。

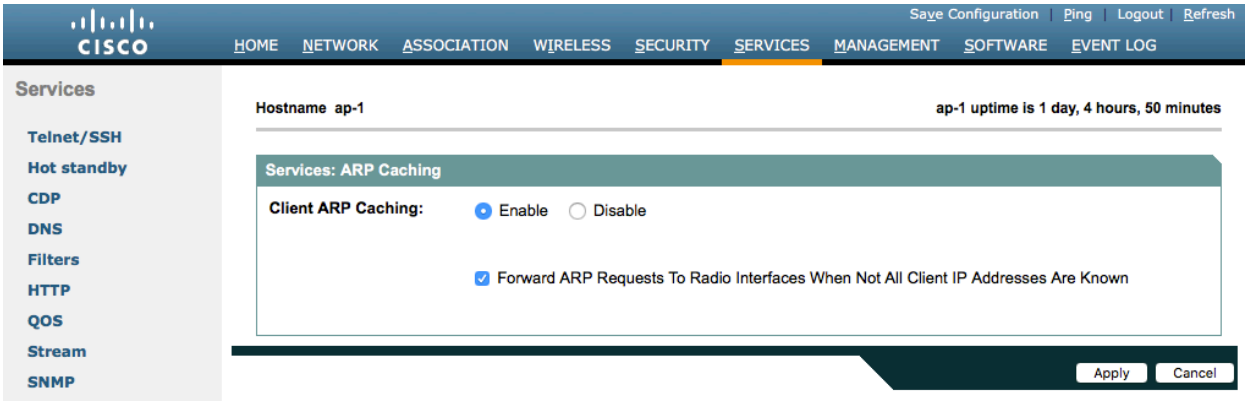


電源管理

プロキシ ARP は、デバイスに代わって、任意の 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 ARP キャッシュ**] を [**有効**] に設定します。

[ARP要求を転送する（Forward ARP Requests）] から [一部のクライアントのIP アドレスが不明な場合の無線インターフェイス（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。



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場合、以下のガイドラインを使用してください。

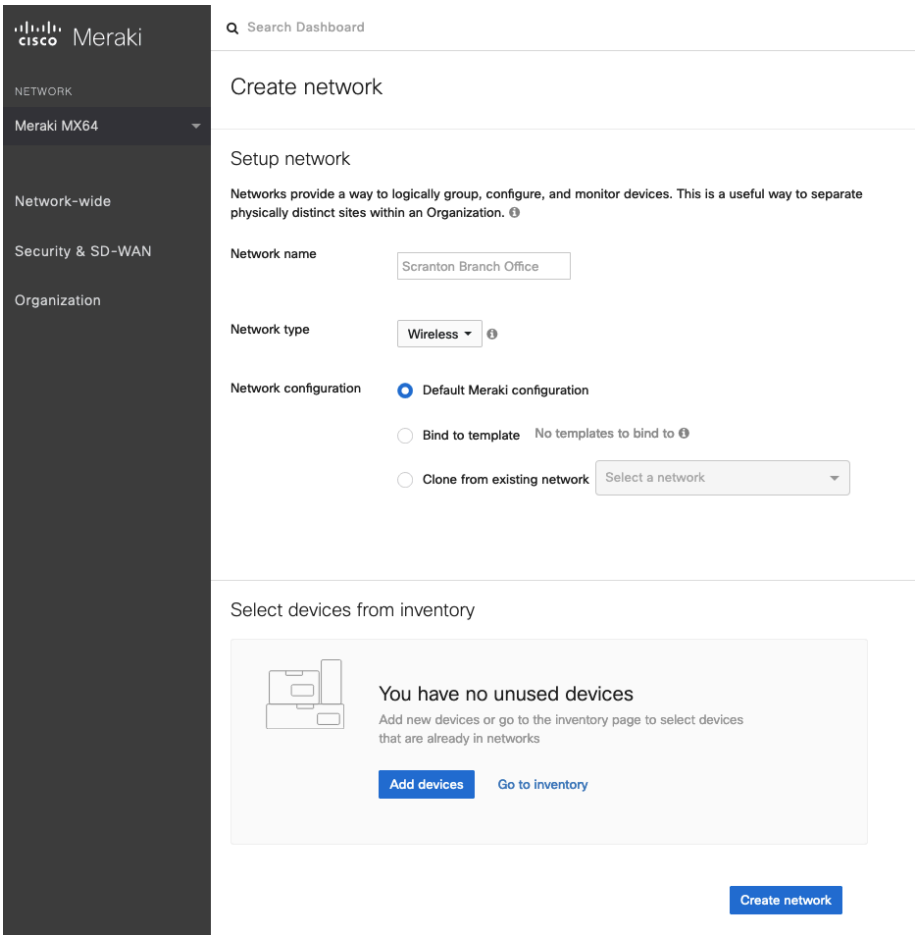
- **[WPA2/WPA3-Enterprise]** または **[事前共有キー（Pre-shared key）]** に対して **[802.11r]** を有効にします。
- **[スプラッシュページ（Splash page）]** を **[なし（None）]** に設定します
- **[ブリッジモード（Bridge mode）]** を有効にします
- **VLAN タグ付けを有効にする**
- **[帯域（Band）] の選択** を **[5 GHz帯のみ（5 GHz band only）]** に設定します
- 必要に応じて **データレート** を設定します
- **[Quality of Service（QoS）]** を設定します

ワイヤレスネットワークの作成

ワイヤレス ネットワークは、WLAN サービスを提供するために、Cisco Meraki アクセス ポイントを追加する前に作成する必要があります。

ドロップダウンメニューから **新しいネットワークの作成** を選択します。

ネットワークタイプに対して **[ワイヤレス（Wireless）]** を選択し、**[作成（Create）]** をクリックします。

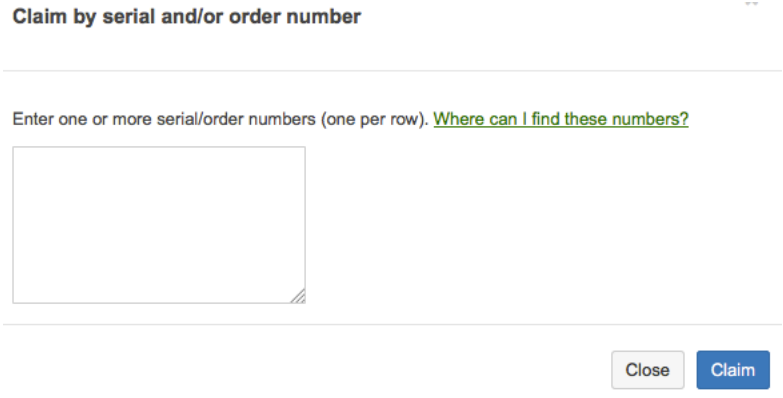


Cisco Meraki アクセス ポイントは、シリアル番号または注文番号を指定することで要求できます。

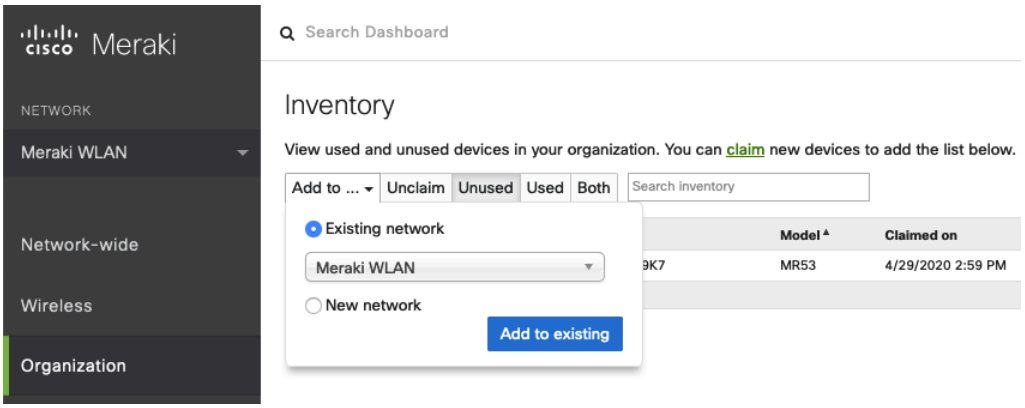
要求されると、これらの Cisco Meraki アクセス ポイントは利用可能なインベントリに一覧表示されます。

Cisco Meraki アクセスポイントは、**[ネットワークを作成（Create network）]** または **[組織（Organization）]** > **[設定（Configure）]** > **[インベントリ（Inventory）]** ページのいずれかで [デバイスを追加（Add Devices）] を選択することで、クレームできます。

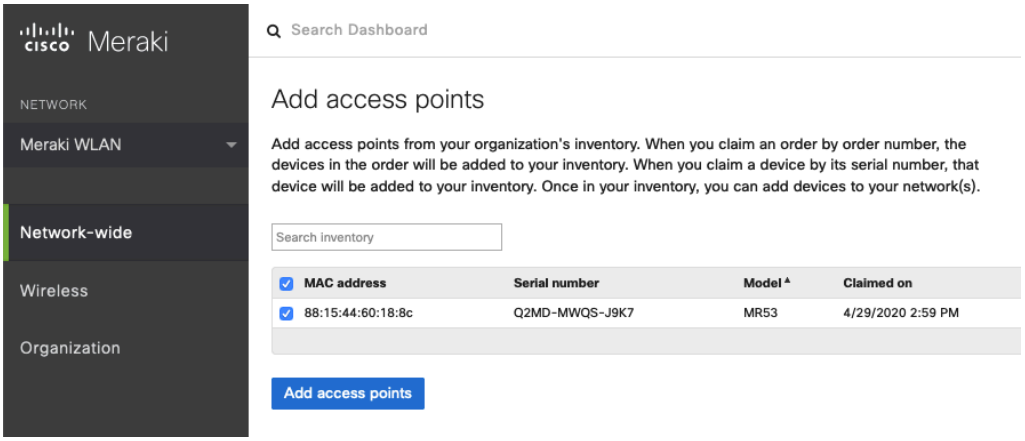
また、アクセスポイントは、**[ワイヤレス（Wireless）]** > **[監視（Monitor）]** > **[アクセスポイント（Access points）]** ページで **[APを追加（Add APs）]** を選択して、**[クレーム（Claim）]** を選択してもクレームできます。



クレームが完了したら、Cisco Meraki アクセスポイントを、**[組織（Organization）]** > **[設定（Configure）]** > の順に選択してアクセスできる目的のワイヤレスネットワークに追加できます。 **在庫** ページ



クレーム済みのアクセスポイントは、**[ワイヤレス（Wireless）]** > **[監視（Monitor）]** > **[アクセスポイント（Access points）]** ページ の順に選択してアクセスする **[APを追加（Add APs）]** を選択してもワイヤレスネットワークに追加できます。



SSID の設定

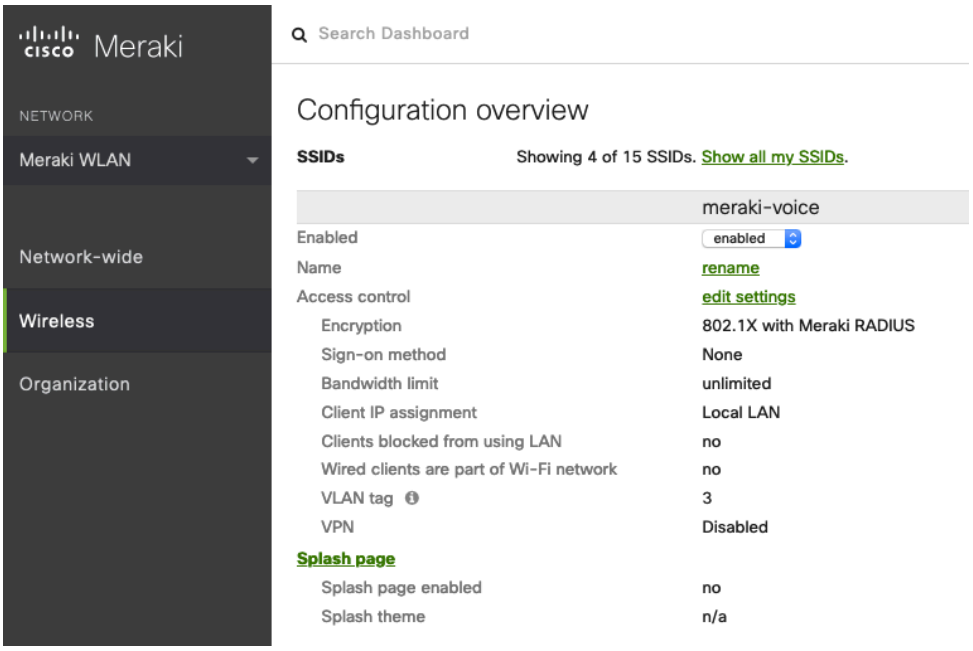
SSID を作成するには、ドロップダウンリスト メニューで目的のネットワークを選択し、**[ワイヤレス（Wireless）]** > **[設定（Configure）]** > **[SSID]** の順に選択します。

Cisco Desk Phone 9800 シリーズには別の SSID を割り当てることを推奨します。 データ クライアントおよび他のタイプのクライアントは、異なる SSID と VLAN を利用する必要があります。

しかし、音声対応 Cisco ワイヤレス LAN をサポートするように設定された既存の SSID を使用することもできます。

SSID 名を設定するには、**[名前を変更（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 [**有効化**] を選択します。



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

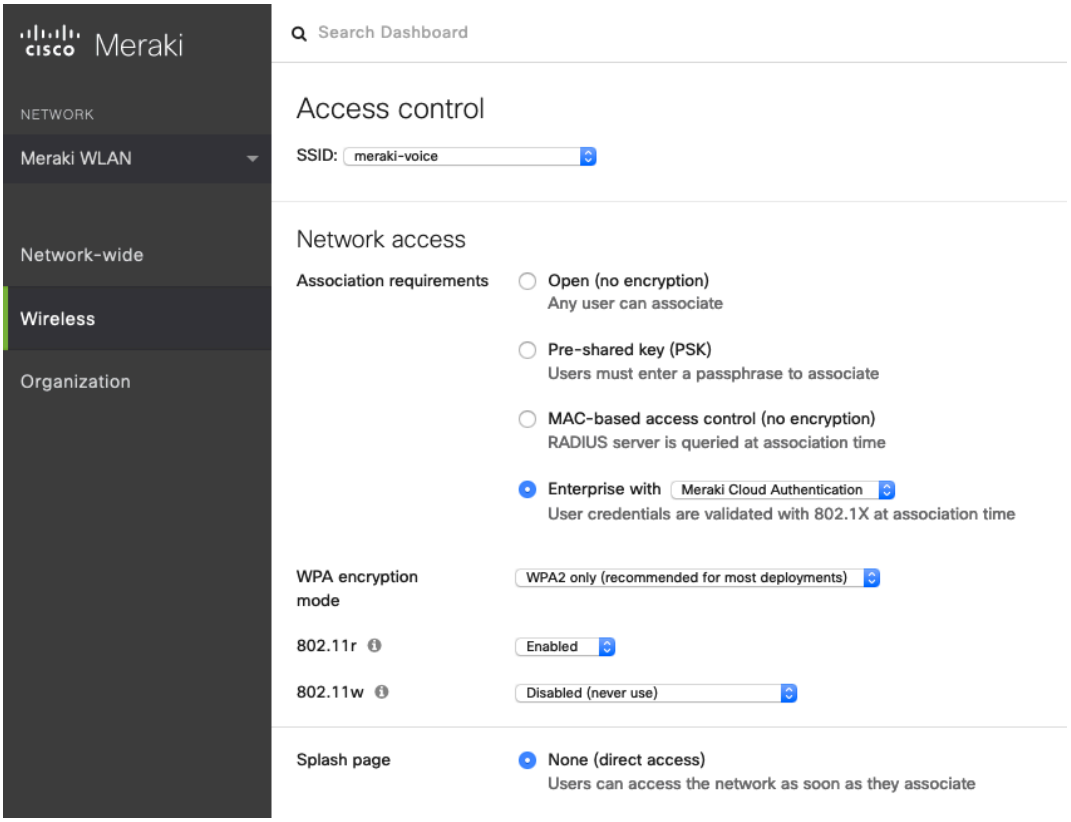
WPA2-Enterprise を選択すると、Cisco Meraki 認証サーバまたは外部 RADIUS サーバを利用できます。

Cisco Meraki 認証サーバは PEAP 認証をサポートしており、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) も利用できます。

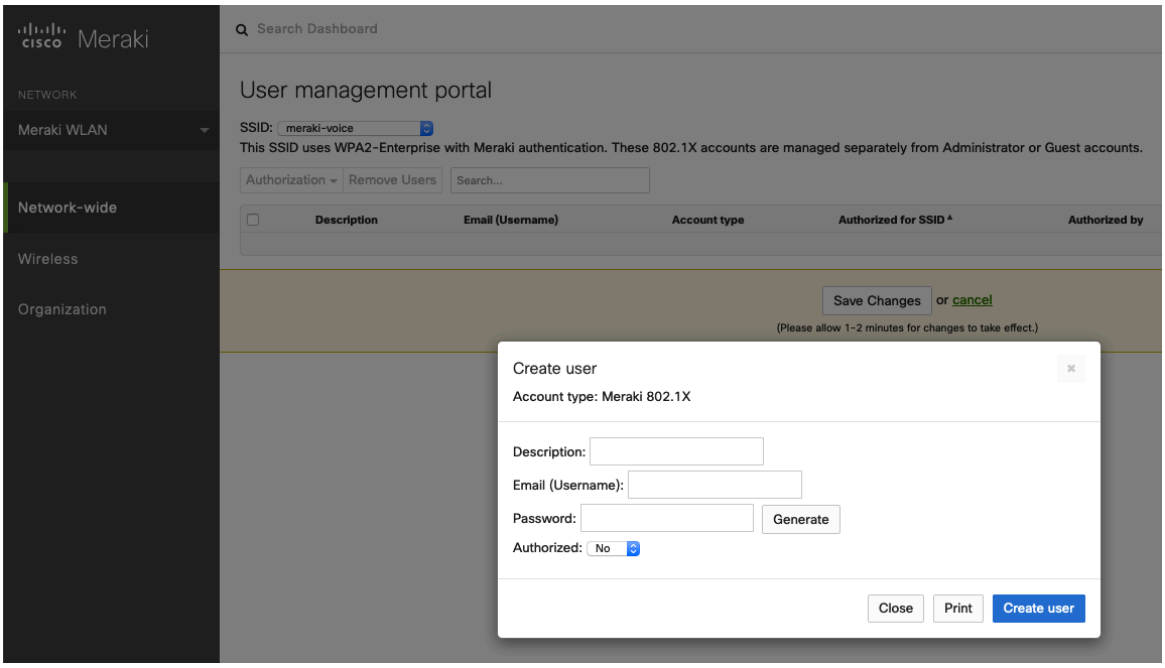
802.11r が有効になっていることを確認する

[スプラッシュ（Splash）] ページを、**[なし（None）]** に設定してダイレクトアクセスを有効にします。



[WPA2-Enterprise]が、有効で、RADIUS サーバーとして Cisco Meraki 認証サーバーを使用する場合は、**[ネットワーク全体（Network-wide）]** > **[設定（Configure）]** > **[ユーザー（Users）]** ページの順に選択して、ユーザーアカウントを作成する必要があります。これは、Cisco Desk Phone 9800 シリーズを 802.1x 認証で使用するために設定します。

メモ:Cisco Meraki アクセス ポイントは EAP-FAST をサポートしていません。



[ワイヤレス（Wireless）] > **[設定（Configure）]** > **[アクセス制御（Access control）]** ページの順に選択し、**[ブリッジモード（Bridge mode）]** を有効にすることが推奨されます。 この設定により、コール制御、他のエンドポイントなどがクラウドベースの場合を除き、Cisco Desk Phone 9800 シリーズは Cisco Meraki ネットワークの代わりにローカル LAN から DHCP を取得することができます。

ブリッジモード が有効になると、VLAN タグオプションが利用できるようになります。

SSID に対して **VLAN タグ** を有効にすることをお勧めします。

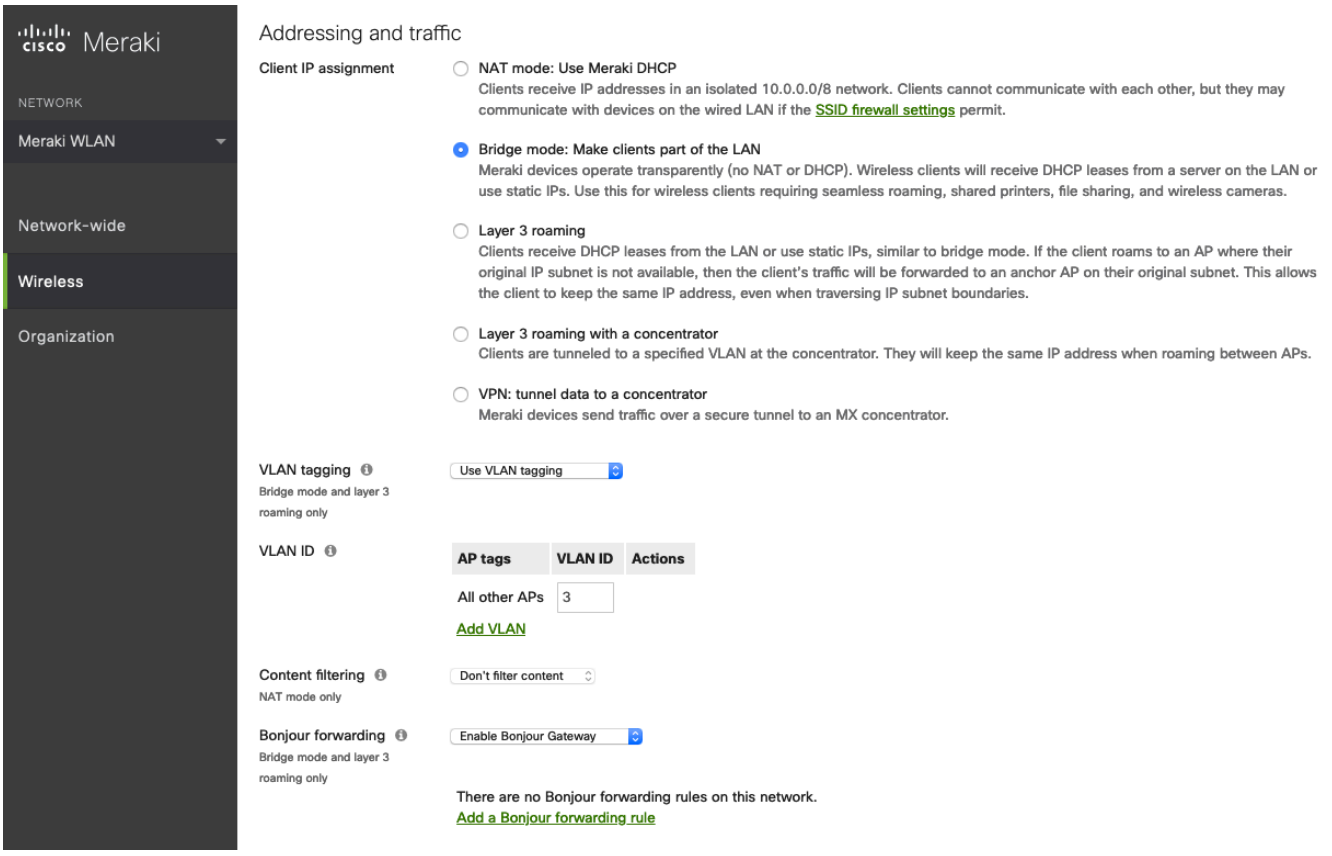
VLAN タギングが利用される場合、Cisco Meraki アクセス ポイントが VLAN を許可するトランク モードに設定されたスイッチ ポートに接続されていることを確認してください。

Cisco Meraki MS スイッチの詳細については、「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

Cisco IOS スイッチを利用する場合、802.1q トランキングを有効にするために、Cisco Meraki アクセスポイントが接続されているポートに次のスイッチポート設定を使用します。

```
インターフェイス ギガビット イーサネット X
switchport trunk encapsulation dot1q
switchport mode trunk
mls qos trust dscp
```



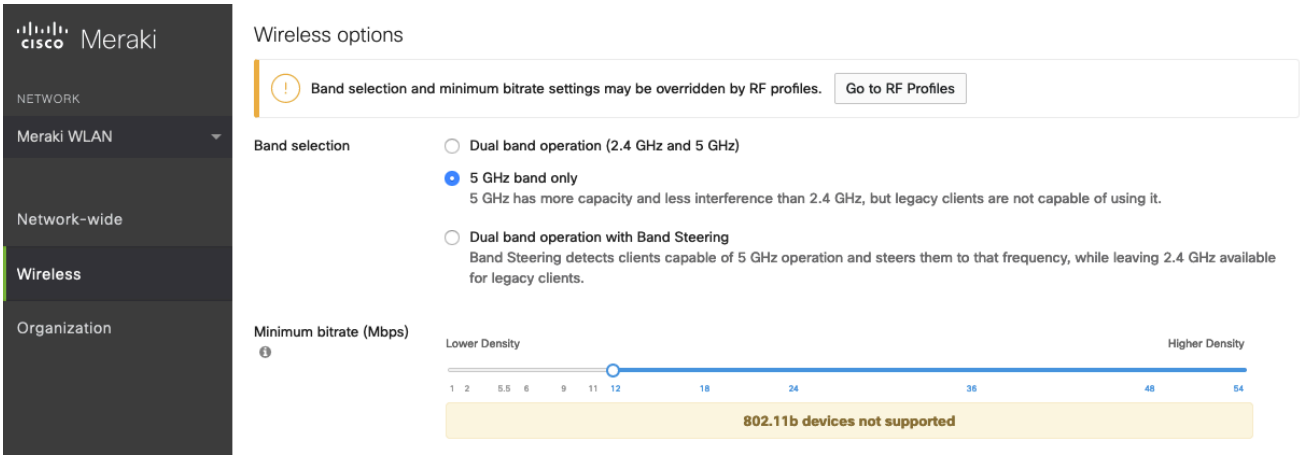
[ワイヤレス（Wireless）] > **[設定（Configure）]** > **[アクセス制御（Access control）]** ページの順に選択し、必要に応じて、Cisco Desk Phone 9800 シリーズが使用する SSID の周波数帯域をを設定します。

2.4 GHz 帯域と比較してチャネルが多く、干渉源が少ない事が理由で、Cisco Desk Phone 9800 シリーズを 5 GHz 帯で操作するには、**[5 GHz帯域のみ（5 GHz band only）]**を選択することが推奨されます。

距離が遠くなって 2.4 GHz 帯域を使用する必要がある場合は、 **デュアル帯域運用 (2.4 GHz と 5 GHz)** を選択します。 [**帯域ステアリングによるデュアル バンド操作**] オプションを利用しないでください。

レガシー 2.4 GHz クライアントをワイヤレス LAN に接続する必要がない限り、12 Mbps 以下のデータ レートを無効にすることを推奨します。

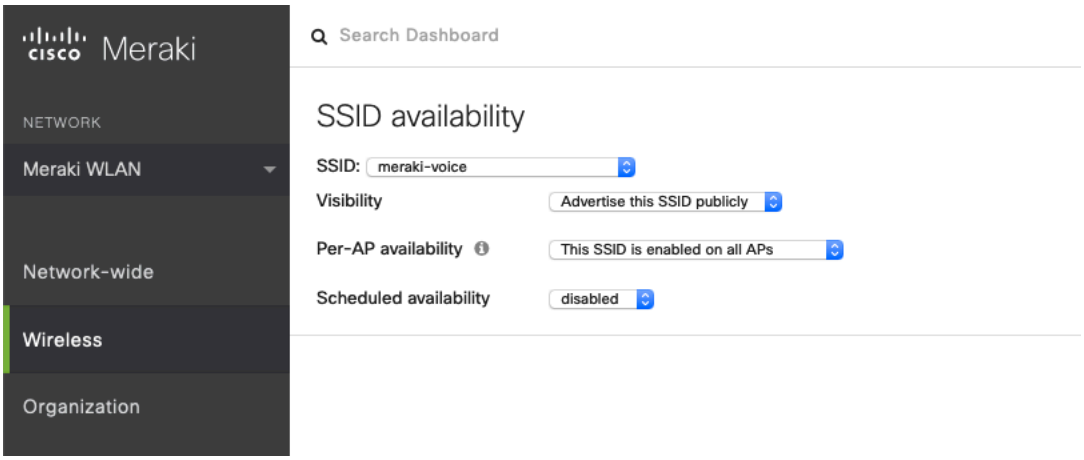
Cisco Meraki アクセス ポイントは現在、100 ms のビーコン周期で 1 の DTIM 周期を利用しています。これらの設定は構成できません。



[ワイヤレス（Wireless）] > **[設定（Configure）]** > **[SSIDの可用性（SSID availability）]** ページの順に選択し、**[可視性（Visibility）]** を **[このSSIDをパブリックでアドバタイズする（Advertise this SSID publicly）]** に設定すると、SSID をブロードキャストできます。

[AP別可用性（Per-AP Availability）] を **[すべてのAPでSSIDを有効化（This SSID is enabled on all APs）]** に設定することが推奨されます。

SSID の可用性のスケジュールは、必要に応じて設定できます。 ただし、**[スケジュールされた可用性（Scheduled Availability）]** は **[無効（Disabled）]** に設定することが推奨されます。



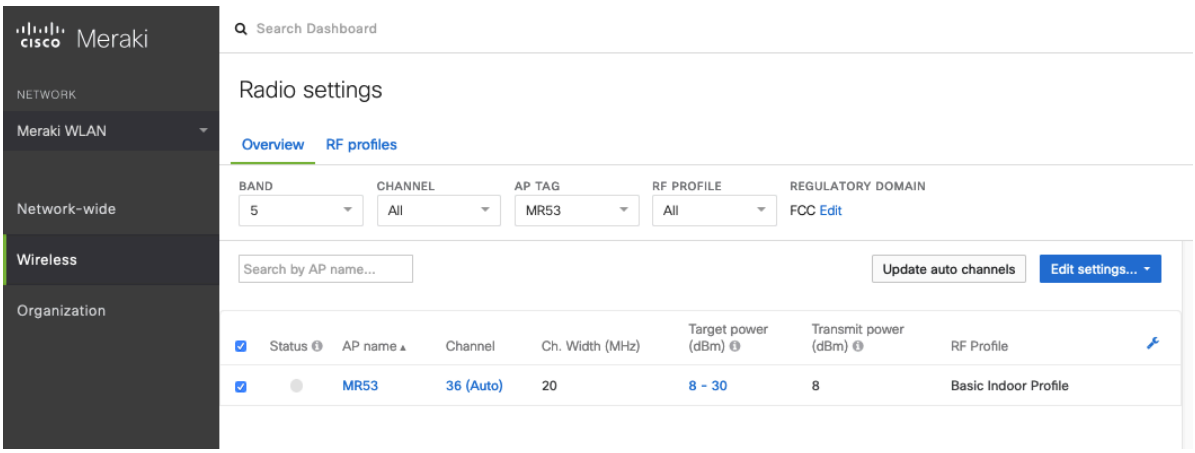
無線設定

[ワイヤレス（Wireless）] > **[設定（Configure）]** > **[無線設定（Radio settings）]**ページの順に選択して、アクセスポイントを一括または個別に構成して、自動または手動チャネルと送信電力設定を定義します。

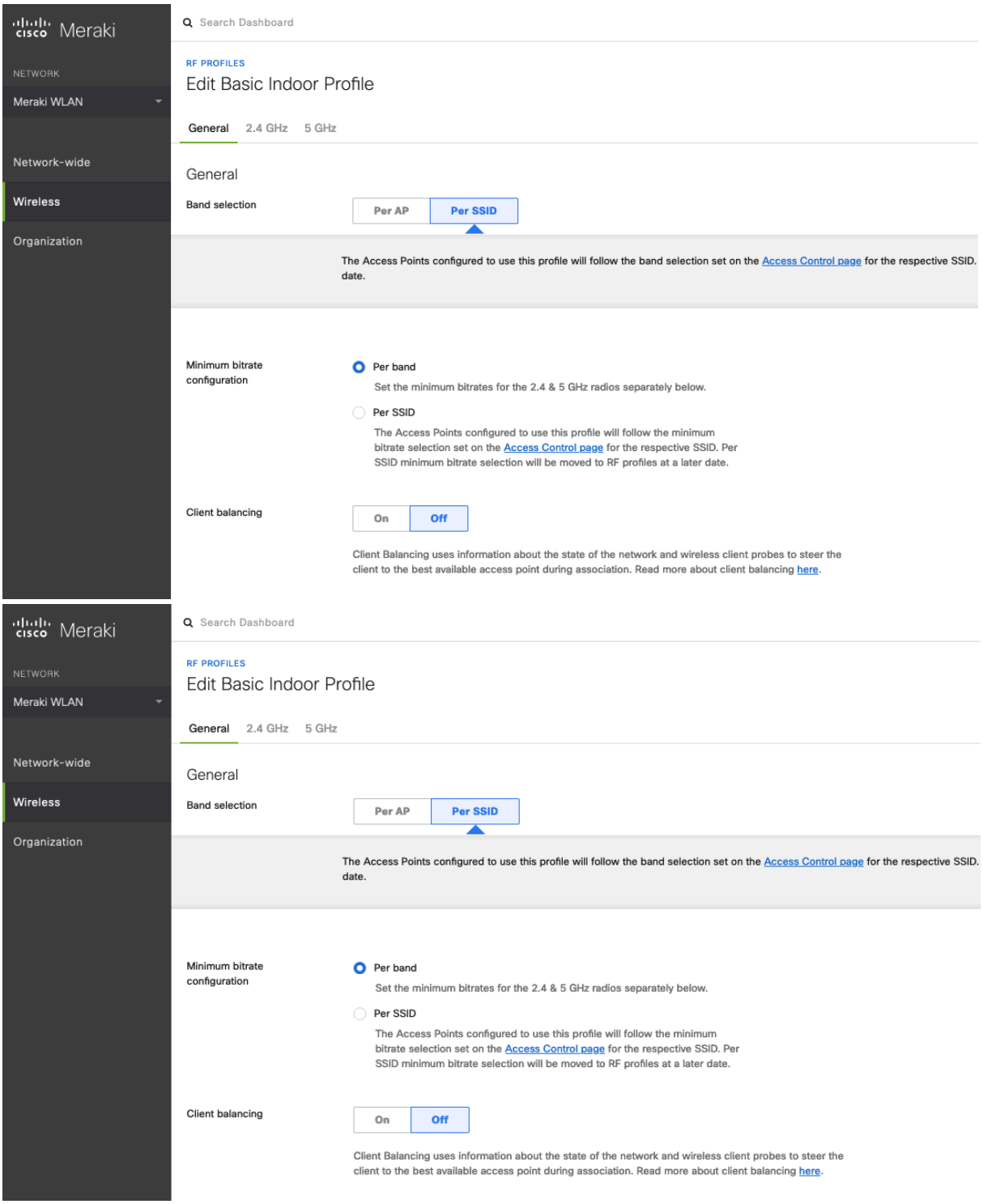
Cisco Meraki アクセスポイントを使用する場合、チャネルと送信電力に [**自動**] を選択して、RF プロファイルで定義されている値を使用することを推奨します。

ただし、個々のアクセス ポイントは、5 または 2.4 GHz 無線の静的チャネルと送信電力で設定できます。

この設定は、その地域で断続的な電波障害が発生している場合に必要になります。 他のアクセスポイントを **[自動（Auto）]** に設定すると、静的に割り当てられたチャネルがあるアクセスポイントを回避することができます。



標準の**[基本インドアプロファイル（Basic Indoor Profile）]**を修正するか、**[帯域選択（Band selection）]** が **[SSIDごと（Per SSID）]** に設定され、**[クライアントバランス（Client balancing）]** が **[オフ（Off）]** に設定された状態の新しいRF プロファイルを作成します。



[RF プロファイル] で、5 GHz 無線の **チャネル幅** を 20 MHz、40 MHz、80 MHz チャネルに使用するように設定できます。

2.4 GHz 無線は 20 MHz チャネル幅を使用し、他のチャネル幅には設定できません。

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。

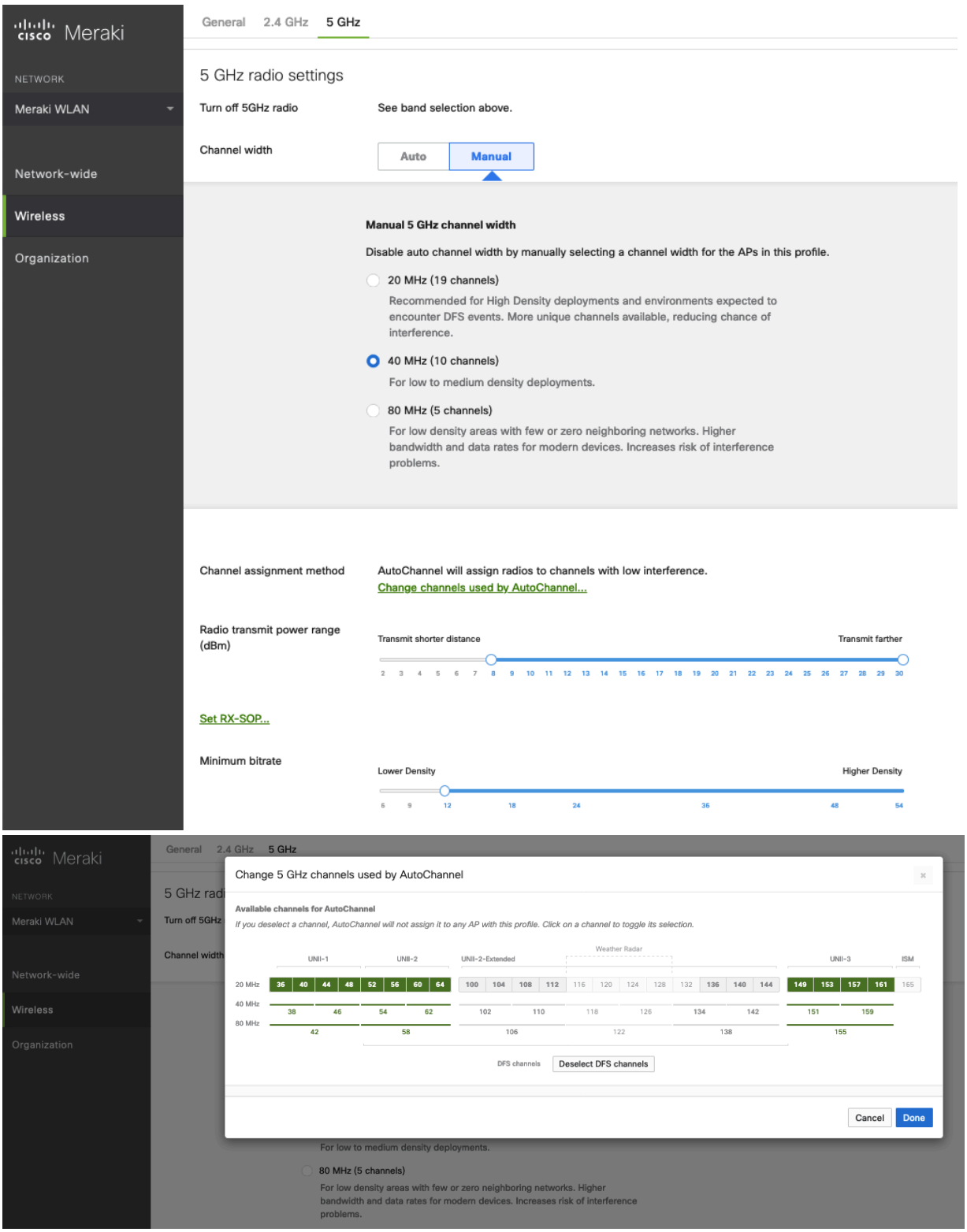
[AutoChannel] が使用する 5 GHz チャネルも RF プロファイルで設定できます。

[AutoChannel] が使用する 2.4 GHz チャネルは、チャネル 1、6、11 のみに制限されます。

[無線送信電力範囲（Radio transmit power range）] も、[RFプロファイル（RF Profile）] で設定します。

最小ビットレート設定 が帯域ごとに設定されている場合、SSID 設定の定義が上書きされます。

レガシー 2.4 GHz クライアントをワイヤレス LAN に接続できるようにする必要がない限り、12 Mbps 未満のデータ レートを無効にすることを推奨します。



ファイアウォールとトラフィック シェーピング

ワイヤレス > **設定** > **ファイアウォールとトラフィック シェーピング** ページでは、ファイアウォールとトラフィック シェーピング ルールを定義することができます。

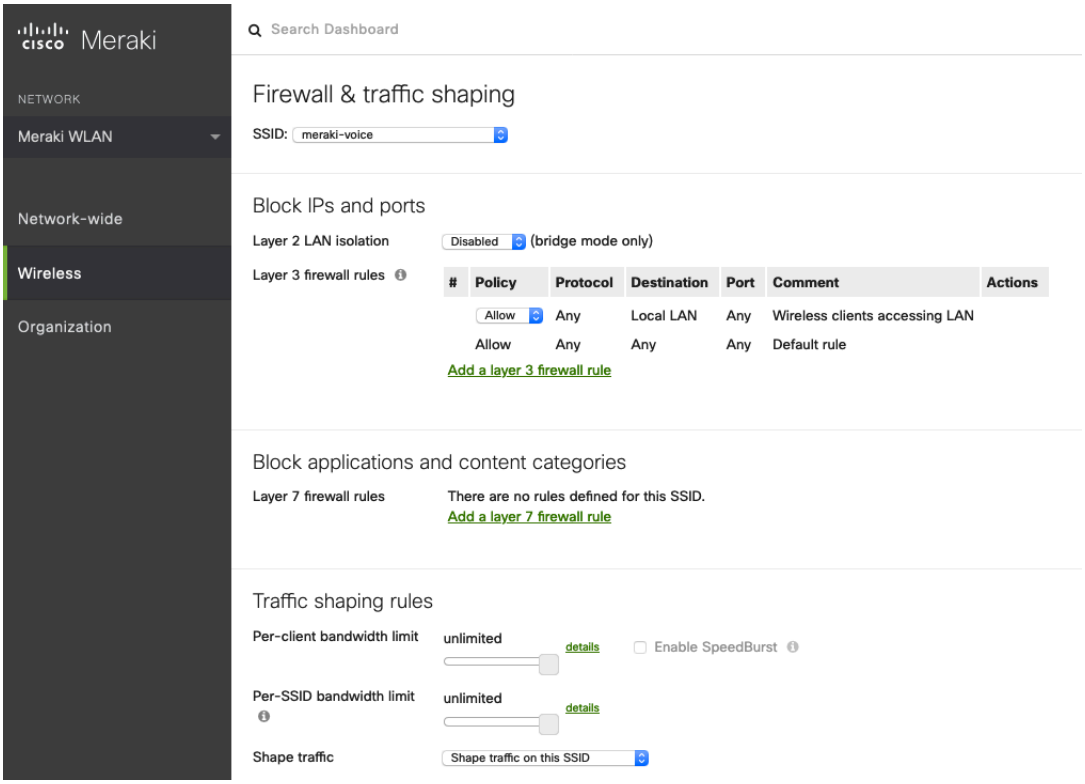
[レイヤ3ファイアウォールルール（Layer 3 firewall rule）] を設定して、ローカル LAN が、ワイヤレスクライアントにアクセスできるようにします。

トラフィック シェーピング ルールの定義を許可するには、**[シェープトラフィック（Shape traffic）]** に対して、ドロップダウンリスト メニューで、**[このSSIDでトラフィックをシェープする（Shape traffic on this SSID）]** を選択します。

一度、**[このSSIDでトラフィックをシェープする（Shape traffic on this SSID）]** を適用したら、**[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。

デフォルトでは、Cisco Meraki アクセス ポイントは現在、DSCP EF (46) でマークされた音声フレームを WMM ではなく WMM UP 5 としてタグ付けします。

UP 6 と、DSCP CS3 (24) でマークされた通話コントロールフレームを WMM UP 4 ではなく WMM UP 3 としてマークします。



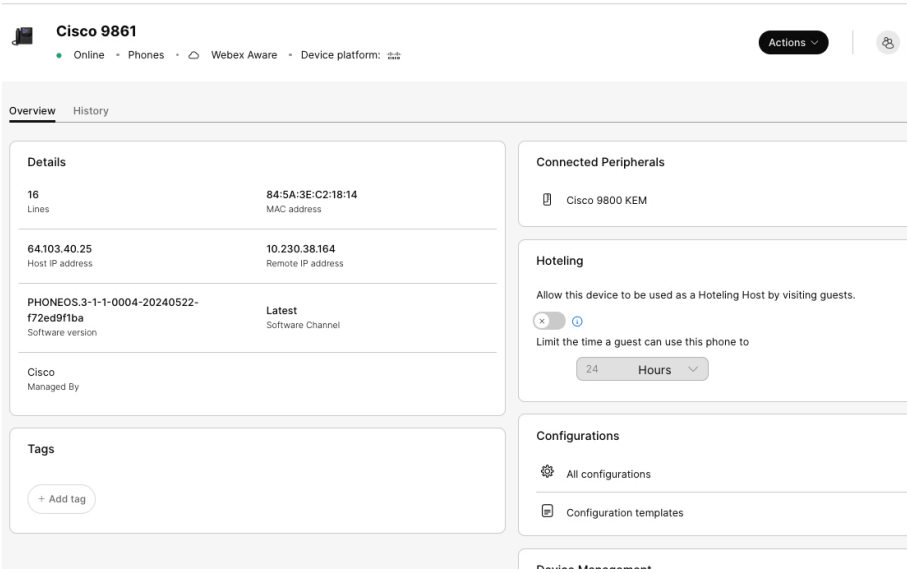
Cisco 通話制御を設定する

Cisco Webex Calling

Cisco Desk Phone 9800 シリーズを Cisco Webex Calling に追加し、それをユーザに割り当てて個人用として、またはワークスペースとして共有で使用することができます。

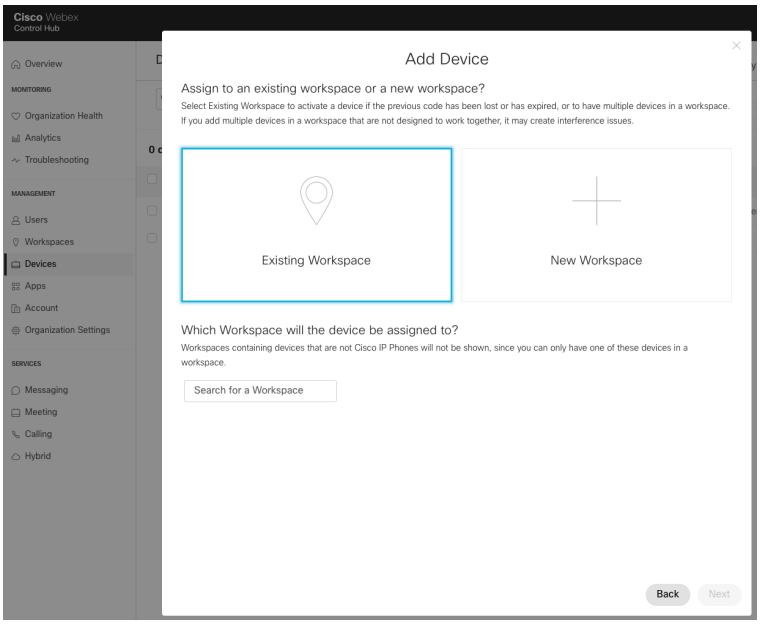
個人使用

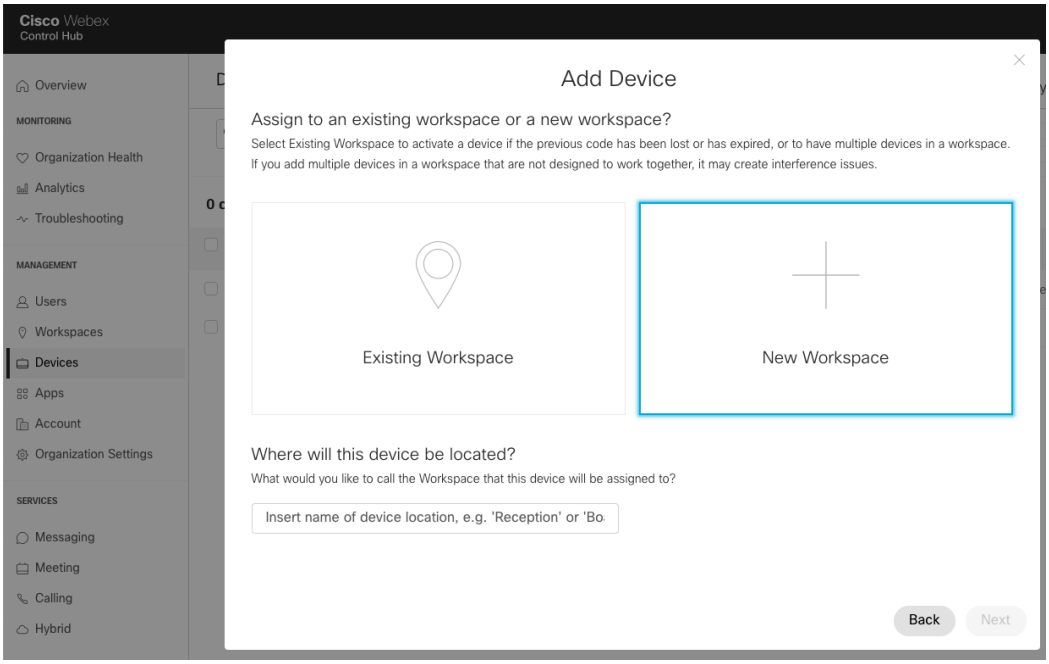
Control Hub で、Cisco Desk Phone 9800 シリーズをユーザーに割り当て、設定を構成します。



ワークスペース利用

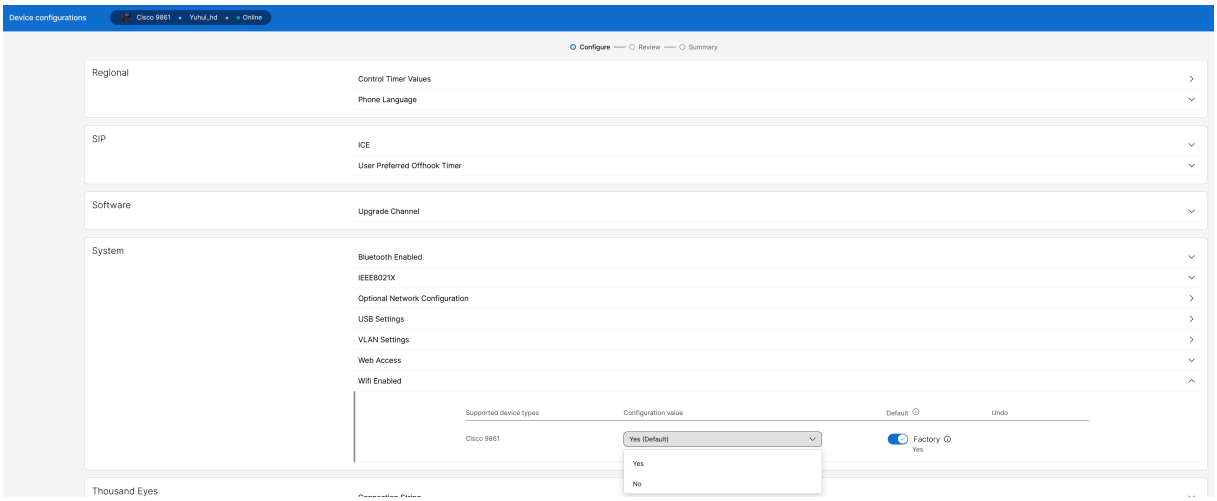
Cisco Desk Phone 9800 シリーズを Control Hub でワークスペース デバイスとして構成できます。





Wi-Fi 機能

Cisco Control Hub で、ワイヤレス環境で Cisco Desk Phone 9800 シリーズを使用するために Wi-Fi が有効になっていることを確認します。



Cisco Unified Communications Manager

Cisco Unified Communications Manager は異なる電話、発信、セキュリティ機能を提供します。

デバイスの有効化

Cisco Unified Communications Manager で Cisco Desk Phone 9800シリーズデバイスタイプを有効にするには、各 Cisco Unified Communications Manager サーバーの Cisco Unified オペレーティングシステム管理ウェブページから、対応するデバイスパッケージ COP ファイルを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 ファイルがインストールされた後で、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 のバージョンに基づいて次のアクションを実行します。

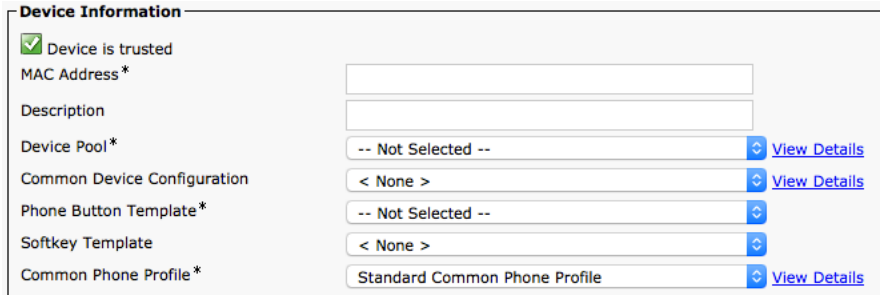
12.5 (1) 以降

- 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上で Cisco CallManager サービスを実行している場合、パブリッシャノード上でのみサービスを再起動します。

メモ: サブスクライバ ノード上の 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 Communication Manager オペレーション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/productsmaintenance-guides-list.html
Cisco Desk Phone 9800 シリーズを Cisco Unified Communications Manager に追加する場合、ワイヤレス LAN MAC は Wi-Fi 接続のみに使用されるため、イーサネット MAC アドレスを使用してプロビジョニングする必要があります。
Cisco Desk Phone 9800 シリーズのイーサネット MAC アドレスは、電話で**[設定（Settings）]** > **[このデバイスについて（About this device）]** の順に選択して確認できます。



共通設定

ワイヤレス LAN などの一部の設定は、企業の電話の共通の電話プロファイルまたは個々の電話レベルで設定できます。

ワイヤレス LAN は、イーサネットが Cisco Desk Phone 9800 シリーズに接続されると一時的に自動的に無効になり、電話機で Wi-Fi が有効になっている場合、イーサネットが切断されると自動的に再度有効になります。

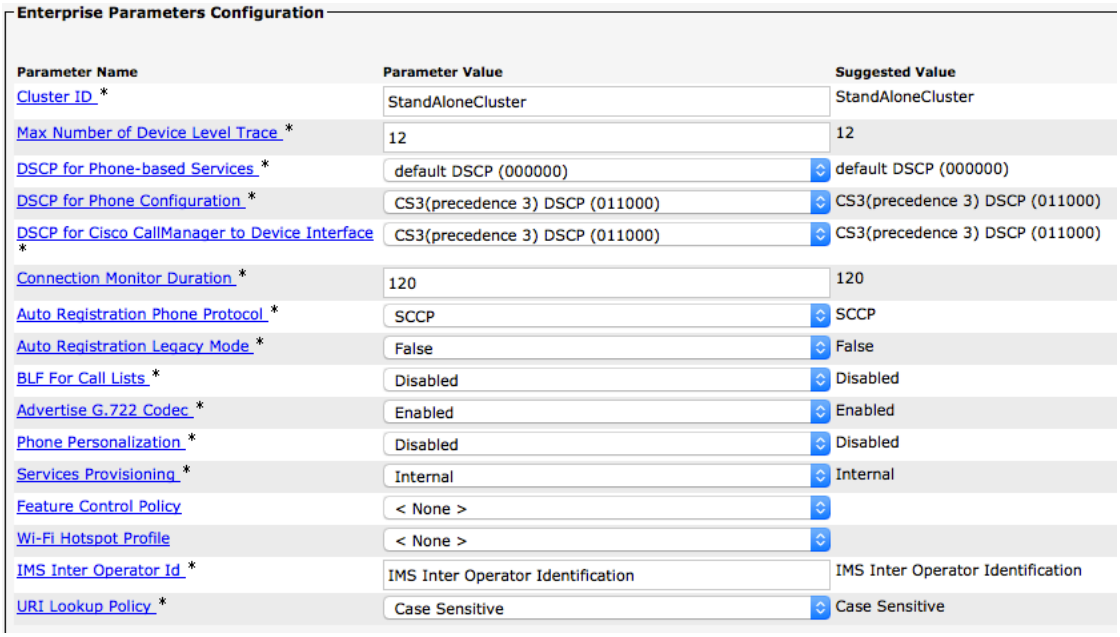
共通設定のオーバーライドは、どちらの構成レベルでも有効にできます。

QoS パラメータ

SIP 通信、電話の構成、および電話ベースのサービスの 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 通信と電話構成のデフォルトの DSCP 値は CS3 に設定されています。

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 トラフィックに設定されます。



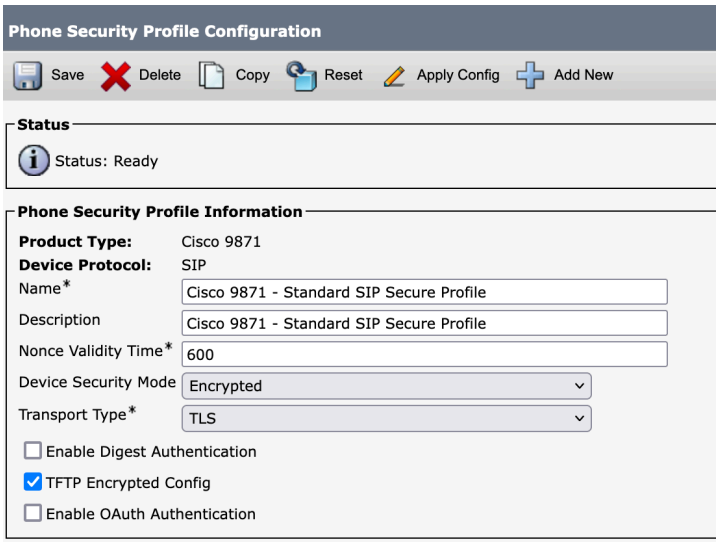
ワイヤレス LAN プロファイル

Cisco Unified Communications Manager 10.0 リリース以降では、ワイヤレス LAN プロファイルで Cisco Desk Phone 9800 シリーズをプロビジョニングできます。 EAP-TLS サポートが含まれています。

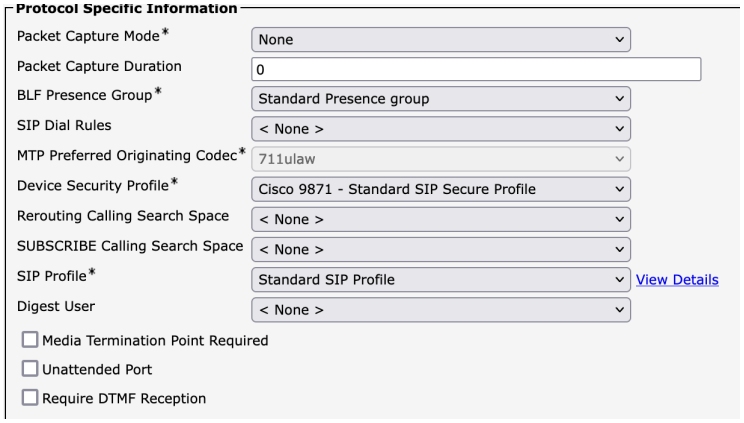
ワイヤレス LAN プロファイルの作成

以下の手順に従って、Cisco Unified Communications Manager でワイヤレス LAN プロファイルを使用して電話をプロビジョニングします。

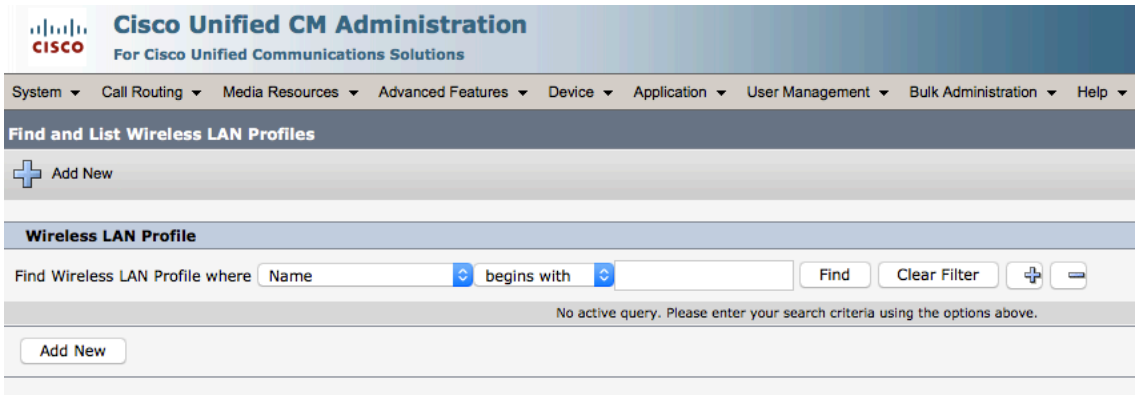
- ワイヤレス LAN プロファイルを作成して電話に関連付ける前に、TFTP 暗号化が有効になっているセキュリティプロファイルを利用するように電話を設定する必要があります。 これにより、ワイヤレス LAN プロファイルがクリア テキストから電話に送信されるのを防ぎます。



- セキュリティ プロファイルが作成されたら、電話に適用して、電話の構成ファイルの TFTP 暗号化を有効にする必要があります。
- **[デバイスセキュリティプロファイル（Device Security Profile）]**ドロップダウンリスト メニューで設定したセキュリティプロファイルを選択します。



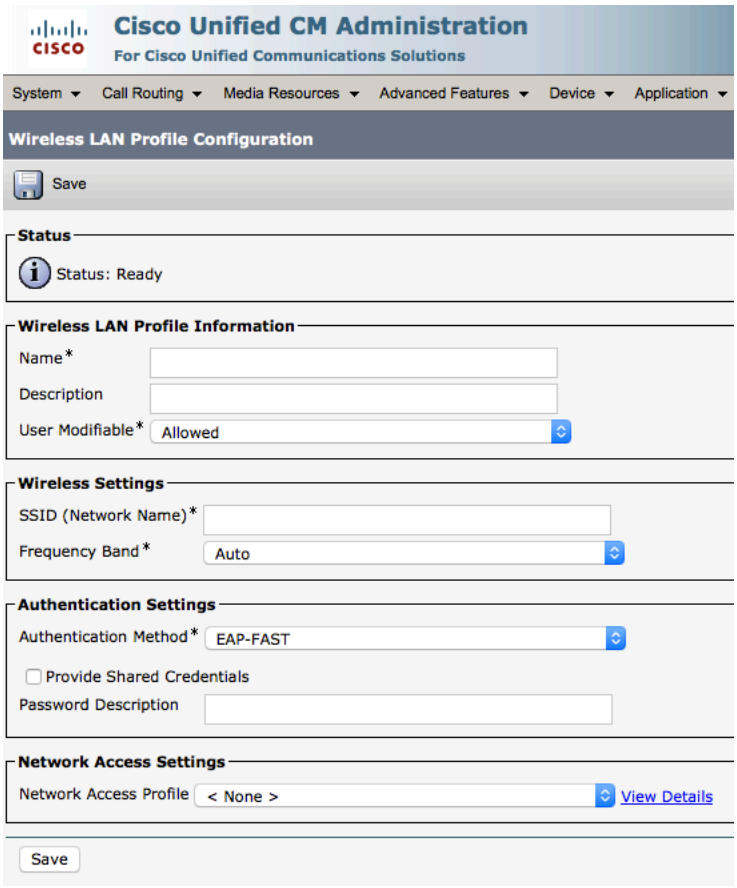
1. ワイヤレス LAN プロファイルを作成するには、Cisco Unified Communications Manager の管理者インターフェイスで、**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[ワイヤレスLANプロファイル（Wireless LAN Profile）]** の順に選択します。
2. [ワイヤレス LAN プロファイル] ページで **[新規を追加]** を選択します。



3. **名前、説明、ワイヤレス設定（SSID、周波数 帯域、ユーザーが変更可能）** および プロファイルの **認証設定**を指定します。

   以下は、ワイヤレス LAN プロファイルのデフォルトです。

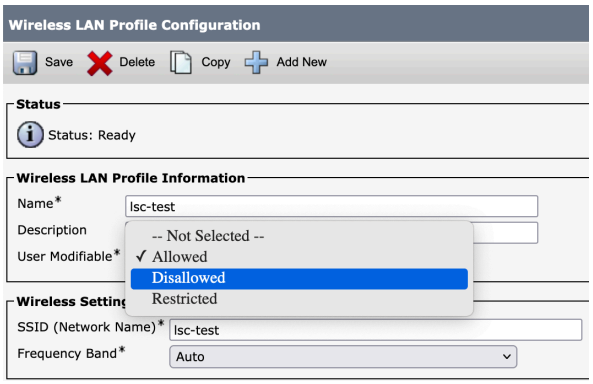
   - **周波数帯域** = 自動
   - **ユーザ変更可能** = 許可済み
   - **認証方法** = EAP-FAST



   - ワイヤレス LAN プロファイルの**名前**を 50 文字以内で入力します。
   - 必要に応じて **説明** を 63 文字以内で入力します。

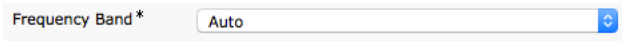
- **[ユーザーが変更可能（User Modifiable）]** ドロップダウンリストで、**[許可（Allowed）]** を選択します。
  ユーザは、ローカルのエンドポイント上の任意のワイヤレス LAN 設定 (有効化/無効化、SSID、周波数帯域、認証方法、ユーザ名とパスワード、PSK パスフレーズ、WEP キーなど) を変更することができます。

  メモ: Cisco Desk Phone 9800 シリーズでは、ユーザはこのパラメータに関係なく、WLAN 設定を変更できます。

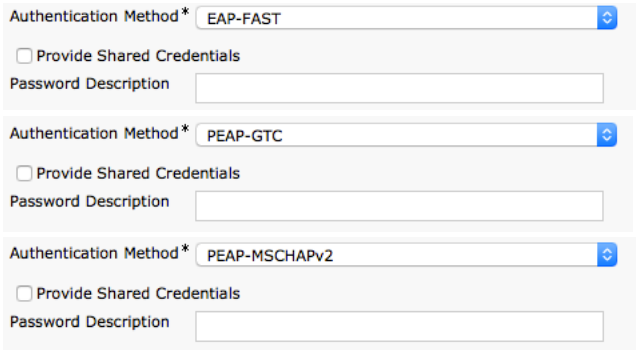


- 32 ASCII 文字以内で **SSID** を入力します。

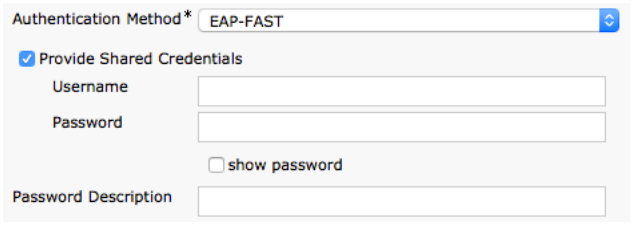
- 目的の **周波数帯域** を選択します。
  - **Auto** = 5 GHz チャンネルを優先しますが、5 GHz および 2.4 GHz チャンネルの両方で動作します
  - **2.4 GHz** = 2.4 GHz チャンネルのみで動作します
  - **5 GHz** = 5 GHz チャンネルのみで動作します



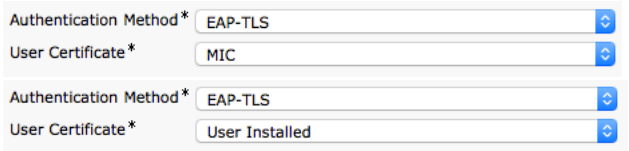
- 目的の**認証方法**オプションを選択します。
  - **EAP-FAST、PEAP-MSCHAPv2** または **PEAP-GTC** が選択されている場合は、共有資格情報（ユーザー名とパスワード）を入力オプションが使用できます。
  - **[共有資格情報を指定する（Provide Shared Credentials）]** がオフの場合、管理者かユーザーが電話で、ローカルにユーザー名とパスワードを設定する必要があります。



- **[共有資格情報を指定する（Provide Shared Credentials）]** がオンの場合、**ユーザー名**と**パスワード**は、ワイヤレス LAN プロファイルを使用するすべての Cisco Desk Phone 9800 シリーズで使用されます。
- [ユーザ名] および [パスワード] には、64 文字まで入力することができます。
- 必要に応じて **パスワードの説明**を入力します。

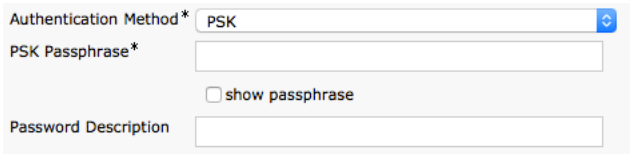


- **[EAP-TLS]** が選択されている場合、**[ユーザー証明書（User Certificate）]** を設定して、EAP-TLS 認証を使用するためにユーザー証明書の種類を指定します。
- **[ユーザー証明書（User Certificate）]** を **[MIC]**（Manufacturing Installed Certificate）、**[LSC]**（Locally Significant Certicate）または**[ユーザーがインストール]** に設定します。



- **[PSK]** [事前共有キー認証（Pre-Shared Key authentication）] に選択された場合、**PSK パスフレーズ** を入力する必要があります。

  PSK パスフレーズ は次のいずれかの形式である必要があります:
  - 8 ~ 63 桁のASCII 文字列
  - 64 HEX 文字列
- **パスワードの説明** は任意に入力することができます。



- **[なし（None）]** が選択されている場合、認証は、必要なく暗号化を使用されません。

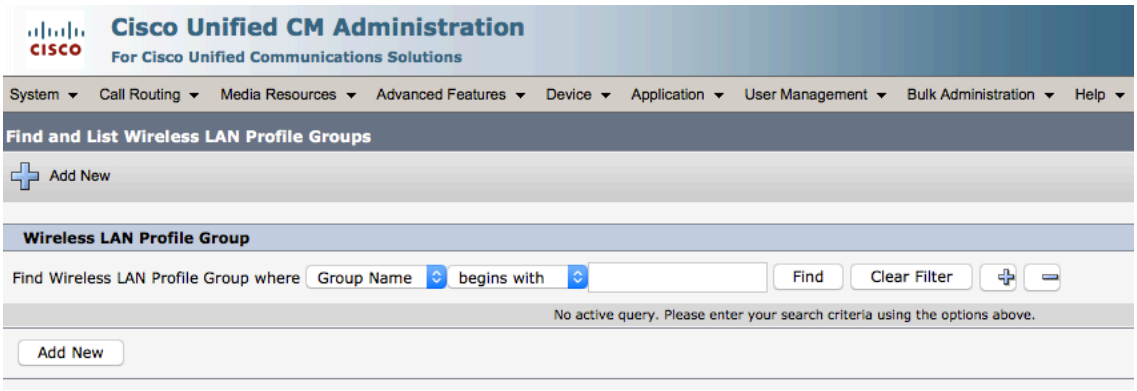
メモ: Cisco Desk Phone 9800 シリーズは WEP または LSC ECC 証明書をサポートしていません。

- Cisco Desk Phone 9800 シリーズは、ネットワークアクセスプロファイルオプションをサポートしていません。

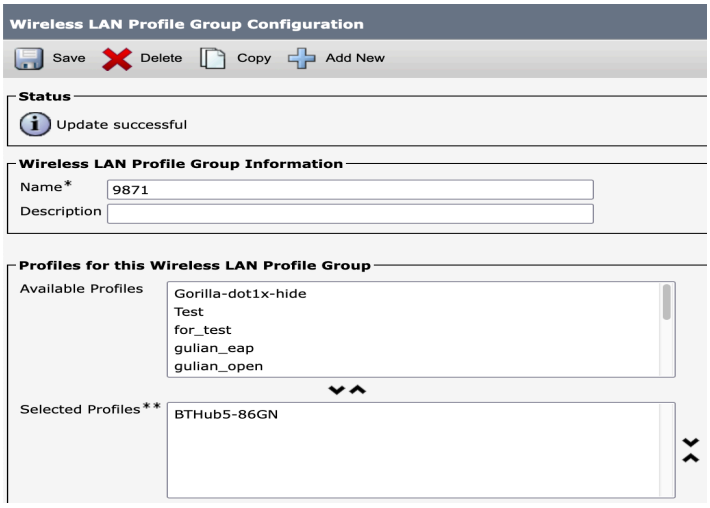
- ワイヤレス LAN プロファイル構成が完了したら、**[保存（Save）]**を選択します。

ワイヤレス LAN プロファイル グループの作成

1. ワイヤレス LAN プロファイルグループを作成するには、Cisco Unified Communications Manager の管理者インターフェイスで、**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[ワイヤレスLANプロファイルグループ（Wireless LAN Profile Group）]** の順に選択します。
2. [ワイヤレス LAN プロファイルグループ] ページで、[**新規の追加**] を選択します。



3. [名前]、[説明] を指定し、[ワイヤレス LAN プロファイル] を選択して追加します。



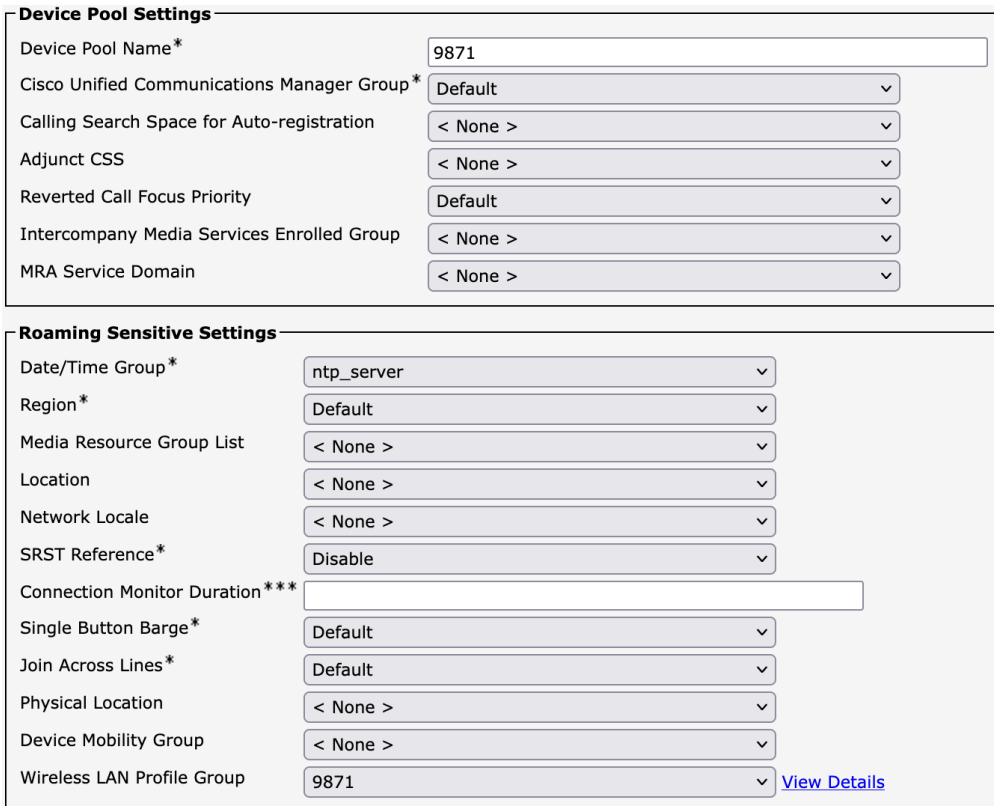
メモ: 1 つのワイヤレス LAN プロファイルグループに追加できるワイヤレス LAN プロファイルは 1 つだけです。

4. ワイヤレス LAN プロファイルグループの構成が完了したら、[**保存**] を選択します。

デバイスプールにワイヤレス LAN プロファイルグループを適用する

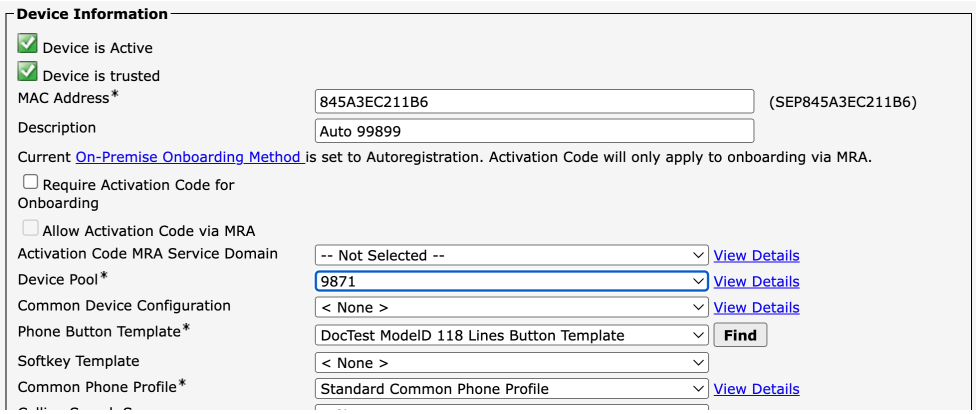
ワイヤレス LAN プロファイル グループが作成されると、デバイス プールまたは個々の電話に適用できます。

1. デバイスプールにワイヤレス LAN プロファイルグループを適用するには、Cisco Unified Communications Manager の 管理者インターフェイスで **[システム（System）]** > **[デバイスプール（Device Pool）]** の順に選択します。
2. 既存のデバイス プールに WLAN プロファイルを適用するには、次の操作を実行します。
   a. デバイス プールを見つけて開きます。
   b. [ローミング センシティブ設定] セクションの [ワイヤレス LAN プロファイル グループ] リストで、WLAN プロファイルを選択します。



   c. **[保存]** を選択します。
   d. **[設定の適用（Apply Config）]** を選択します。
3. WLAN プロファイルを新しいデバイス プールに適用するには、次の操作を実行します。

a. **[新規追加（Add New）]** を選択して、デバイスを作成します。
b. 名前と必要な情報を指定します。
c. [ローミング センシティブ設定] セクションの [ワイヤレス LAN プロファイル グループ] リストで、WLAN プロファイルを選択します。
d. **[保存]** を選択します。
e. **[設定の適用（Apply Config）]** を選択します。
f. **[デバイス（Device）] > [電話（Phone）]** の順に選択し、デバイスプールを追加する電話を見つけます。
g. **[端末情報]** の [**端末プール**] ドロップダウンリストで作成した端末プールを選択します。



h. [**保存**] を選択します。
i. **[設定の適用（Apply Config）]** を選択します。

個々の電話にワイヤレス LAN プロファイルグループを適用します。

1. Cisco Unified Communications Manager の管理インターフェイスの [**端末** > **電話**] に移動します。
2. 電話を見つけて、[電話機の設定（Phone Configuration）] ページを開きます。
3. [**デバイス情報**] セクションの [**無線 LAN プロファイルグループ**] ドロップダウンリストから WLAN プロファイルグループを選択します。
4. **[保存（Save）]** を選択します。
5. **[設定の適用（Apply Config）]** を選択します。

Cisco Desk Phone 9800 シリーズの設定

自動プロビジョニング

この方法は現在、Cisco Unified Communications Manager に登録されている電話でのみ利用できます。 Wi-Fi プロファイルの自動プロビジョニングの場合、イーサネットまたは Wi-Fi 経由でネットワークに接続される Cisco Desk Phone 9800 シリーズでは、Cisco Unified Communications Manager への接続が確立されます。
Cisco Unified Communications Manager 10.0 以降への接続では、Wi-Fi プロファイル構成データをダウンロードして Cisco Desk Phone 9800 シリーズに適用できます。
EAP-TLS 認証を含む Wi-Fi プロファイルをダウンロードして適用するには、Cisco Unified Communications Manager 11.0 以降が必要です。
詳細については、 **Cisco Unified Communications Manager** > **ワイヤレス LAN プロファイル** のセクションを参照してください。
証明書をネットワーク接続時に自動的にインストールすることもできます。
詳細は、 **Simplified Certificate Enrollment Protocol (SCEP)** のセクションを参照してください。

電話ウェブ ポータル経由の Wi-Fi プロファイルの設定/変更

有線またはワイヤレス接続により、Cisco Desk Phone 9800 シリーズに有効な IP アドレスが割り当てられていることを確認します。

メモ: 電話用ウェブポータルは、Webex Calling または Cisco BroadWorks に登録されている電話でのみ利用できます。

1. ウェブブラウザ アドレス バーに電話の IP アドレスを入力します。
   例: http://10.64.84.147/
2. **[管理者ログイン（Admin Login）]** をクリックして、**[詳細設定（Advanced）]** をクリックして管理者として設定にアクセスします。
3. **音声** > **システム**に移動します。
4. **[電話のWi-Fiをオン（Phone-wifi-on）]** を **[はい（Yes）]**に設定し、電話の Wi-Fi をオンにします。
5. 電話をワイヤレスアクセスポイントに接続するための Wi-Fi ネットワーク名と資格情報を指定します。

   セキュリティモードは、アクセスポイントの設定に応じて次のいずれかになります。

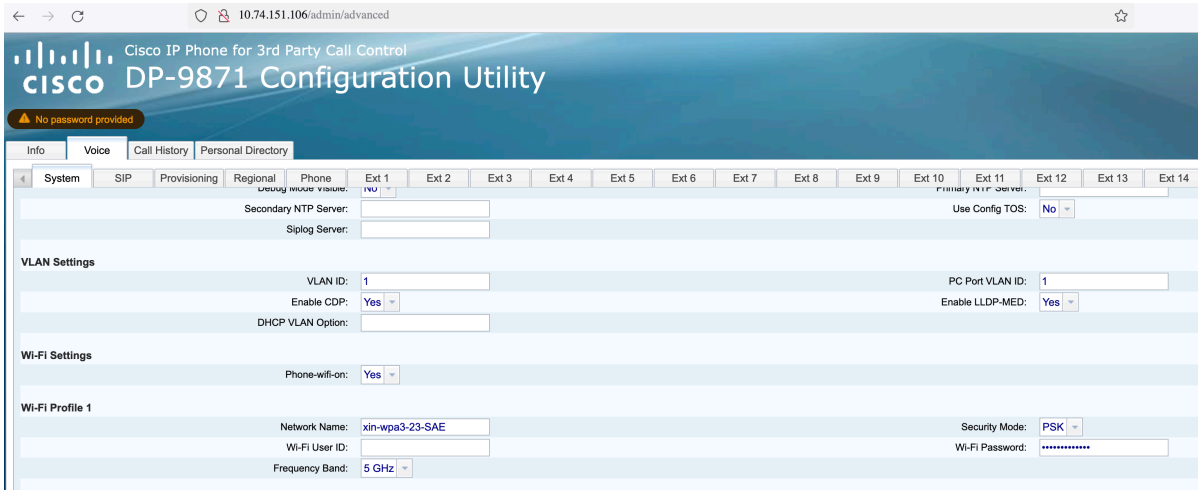
   - **[自動（Auto）]**、**[EAP-FAST]** または **[PEAP]** が選択されている場合は、**[Wi-Fiユーザー ID（Wi-Fi User ID）]** と **[Wi-Fiパスワード（Wi-Fi Password）]** が必要です。
   - 事前共有キー認証に **PSK** を選択した場合、 **PSK パスワード** を入力する必要があります。

     PSK パスワード は、8 ~ 63 桁の ASCII 文字列にする必要があります。

- **[WEP]** を選択して、静的 WEP（有線等価プライバシー）認証を利用する場合、**WEP キー** を入力する必要があります。
- **なし** が選択されている場合、認証は必要なく、暗号化も使用されません。
- **[自動（Auto）]** が選択されている場合、電話は、認証方法として対象 AP との通信に基づき、自動で **[EAP-FAST]** または **[EAP-PEAP]** を選択します。
- **[EAP-TLS]** が選択されている場合、現在、**MIC**証明書のみが、Webex Calling/Webex DI/Broadworks に登録されている電話でサポートされています。

目的の**周波数帯を選択します**:

- **自動:** 5 GHz チャンネルを優先しますが、5 GHz および 2.4 GHz チャンネルの両方で動作します
- **2.4 GHz:** 2.4 GHz チャンネルのみで動作します
- **5 GHz:** 5 GHz チャンネルのみで動作します



6. **[すべての変更を送信] をクリックします。**

[情報] [**ステータス**] タブに移動してネットワークステータスを確認できます。

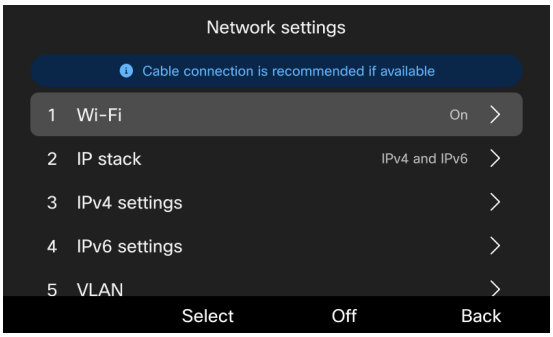
注：

- あるアクセスポイントから別のアクセスポイントに切り替えると、電話が再起動されます。

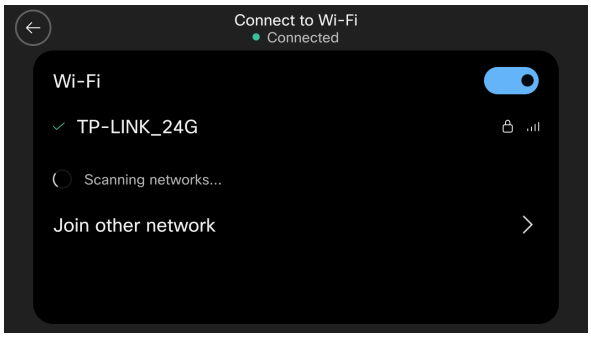
- 電話がイーサネット接続で接続されている場合、Wi-Fi はオフになります。 電話が適切に設定されていれば、イーサネットケーブルが取り外されても、電話機は自動的にワイヤレスネットワークに接続されます。
- Wi-Fi 設定は電話の [設定] メニューの設定と同期されます。

電話 UI での Wi-Fi 設定の構成

1. [設定] を押します。
2. プロンプトが表示されたら、パスワードを入力して [設定] メニューにアクセスします。
3. [ネットワークとサービス（Network and service）] > [ネットワーク設定（Network settings）] の順に選択します。
4. Wi-Fi 状況がオフの場合、Wi-Fi をオンにします。 電話が利用可能なワイヤレスネットワークのスキャンを開始します。

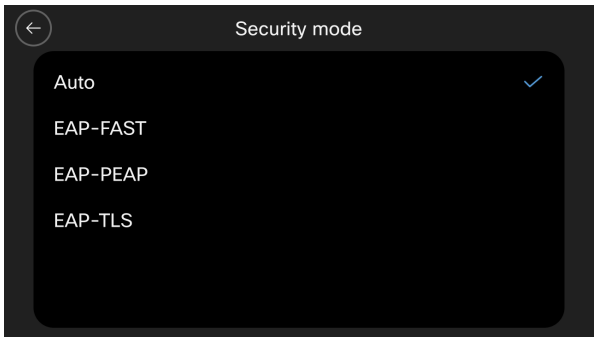


9861



9871

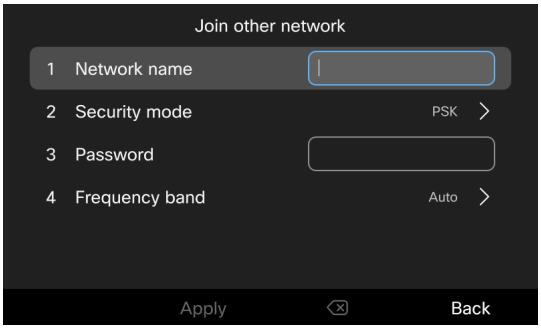
5. 9861 電話を使用している場合は、 **選択** を押して [Wi-Fi に接続] 画面を表示します。 9871 電話を使用している場合は、次のステップに進みます。
6. 利用可能なネットワークからアクセスポイントを選択し、ネットワーク認証が必要な場合は資格情報を入力します。
   セキュリティモードと利用可能な周波数帯域はアクセスポイントの設定によって異なります。
   ネットワークが 802.1x に対応している場合、電話は EAP タイプに対して動的に [自動（Auto）] を選択します。これは RADIUS サーバーの設定によって決まります。 内部認証方法を選択できます。



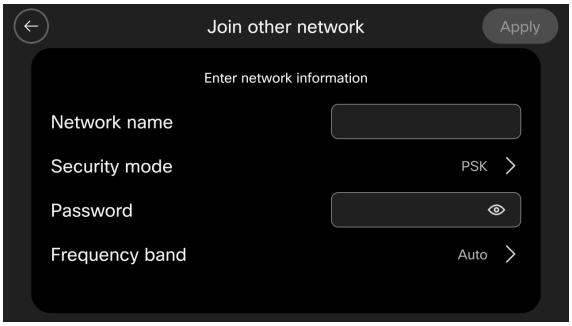
7. **[Apply]** を選択します。

非公開のワイヤレスネットワークに参加する

1. [設定] を押します 。
2. プロンプトが表示されたら、パスワードを入力して [設定] メニューにアクセスします。
3. **[ネットワークとサービス（Network and service）]** > **[ネットワーク設定（Network settings）]** の順に選択します。
4. Wi-Fi 状態がオフの場合、Wi-Fi をオンにします。
5. **[Wi-Fi]** を選択してから、**[他のネットワークに参加（Join other network）]** を選択します。
6. ネットワーク名を入力し、セキュリティモードを選択し、資格情報を入力します。



9861



9871

アクセスポイントの設定に合わせて適切なセキュリティモードが選択されていることを確認します。

- **なし:** 接続するワイヤレスネットワークがオープンネットワークの場合は、このオプション を選択します。 パスワードは必要ありません。
- **PSK:** ネットワークが事前共有キーまたは WPA3-SAE で保護されている場合、このオプションを選択してパスワードを入力します。 事前共有キーの長さは 8 ~ 63 バイトです。
- **自動/EAP-FAST/EAP-PEAP:** これらのオプションのいずれかを選択する場合、ユーザ ID とパスワードが必要になります。
- **EAP-TLS:** このオプションを選択すると、ユーザ証明書タイプが必要になります。 現在は、Manufacturing installed certificate（MIC）のみがサポートされています。
  メモ: 証明書の管理とルート CA のインストールは、現在 Webex Calling/DI/ブロードワークでのみ利用できます。

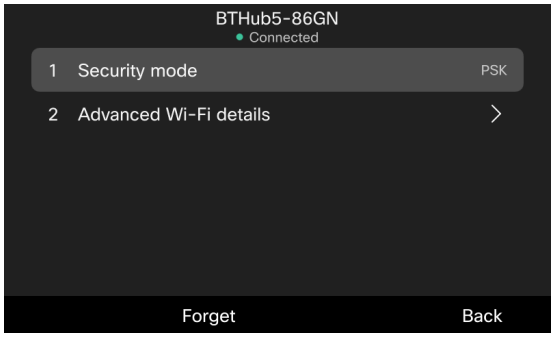
7. **[適用（Apply）]** を選択します。

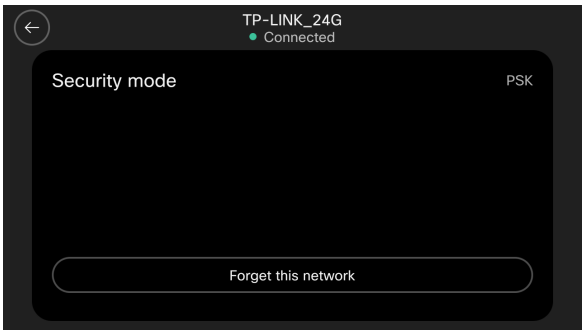
接続済みネットワークの削除

ユーザは [設定] メニューで現在接続されている AP を削除できます。

1. [ネットワーク設定] 画面で、電話が接続されているアクセスポイントを選択します。

2. お使いの電話機のモデルに応じて、**[忘れる（Forget）]** または **[このネットワークを忘れる（Forget this network）]** を選択します。



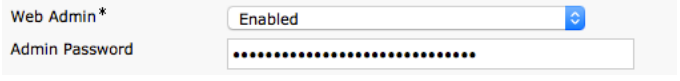


証明書の管理

Cisco Desk Phone 9800 シリーズは、EAP-TLS に X.509 デジタル証明書を利用したり、サーバ検証を有効にしたりできます。
ユーザ証明書は、Simple Certificate Enrollment Protocol (SCEP) で自動的に、または電話の管理者ウェブページインターフェイス (https://<phone_IP_address>:8443) から手動でインストールできます。
証明書タイプ別証明書は 1 つだけ許可されます。1 ユーザー証明書と 1 サーバー証明書（SCEP または手動のいずれか経由）方法)。
LSC 証明書は CUCM CAPF サービスによりインストールされます。
証明書がインストールされると、EAP-TLS が設定されている場合は、サーバ検証が自動的に有効になります。
Microsoft® Certificate Authority (CA) サーバの使用をお勧めします。 他の CA サーバ タイプは、Cisco Desk Phone 9800 シリーズと完全には相互運用できない場合があります。
クライアントとサーバー証明書には、DER および Base-64 (PEM) エンコードが使用できます。
キーサイズが 1024、2048、4096 の証明書がサポートされています。
クライアントとサーバの証明書が SHA-1 または SHA-2 アルゴリズムのいずれかを使用して署名されていることを確認してください。SHA-3 署名アルゴリズムはサポートされていません。
クライアント認証がユーザー証明書詳細の [強化されたキー使用（Enhanced Key Usage）] セクションにリストされていることを確認します。

手動インストール

管理者ウェブページインターフェイスが、**[有効（Enabled）]**に、ユーザー名が、**admin**に、**管理者パスワード**が CUCM によって設定されているかを確認します。

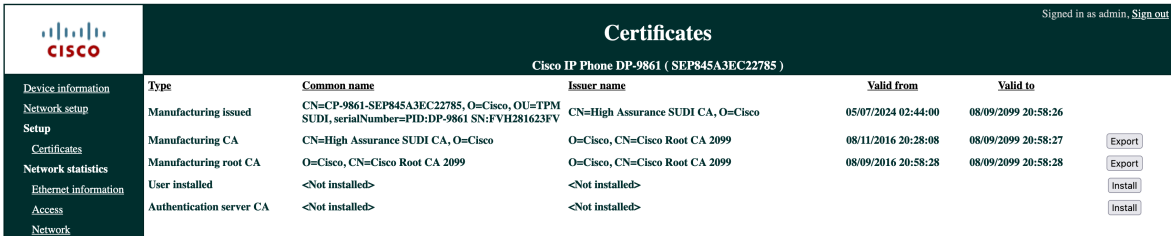


https://x.x.x.x:8443 で手動インストール ページを開く

EAP-TLS のユーザー証明書として、Manufacturing Installed Certificate（MIC）、LSC、または User Installed 証明書のいずれかを使用できます。

Manufacturing Installed Certificate（MIC）

事前インストールされている Manufacturing Installed Certificate（**MIC**）は、**EAP-TLS** では、**ユーザー証明書**として使用できます。
MIC の CA チェーンをエクスポートし、RADIUS サーバーのに追加して、**EAP-TLS** のユーザー証明書として使用する必要があります。
[**エクスポート**] をクリックして、管理者ウェブページインターフェイスからルートおよびサブ CA 証明書をダウンロードします。



このルート CA は Radius サーバの信頼リストに追加される必要があります。

User Installed 証明書

EAP-TLS に対して手動でユーザー証明書をインストールするには、メインの**[証明書（Certificates）]**ウェブページで **[User Installed]** に対して、**[インストール（Install）]** を選択します。
[参照（Browse）] を選択して、**PKCS #12** 形式（.p12 または .pfx）でユーザー証明書を指します。
抽出パスワードを入力して、[**アップロード**] を選択します。
ユーザー証明書を発行した CA チェーンが RADIUS サーバーの信頼リストに追加されていることを確認します。

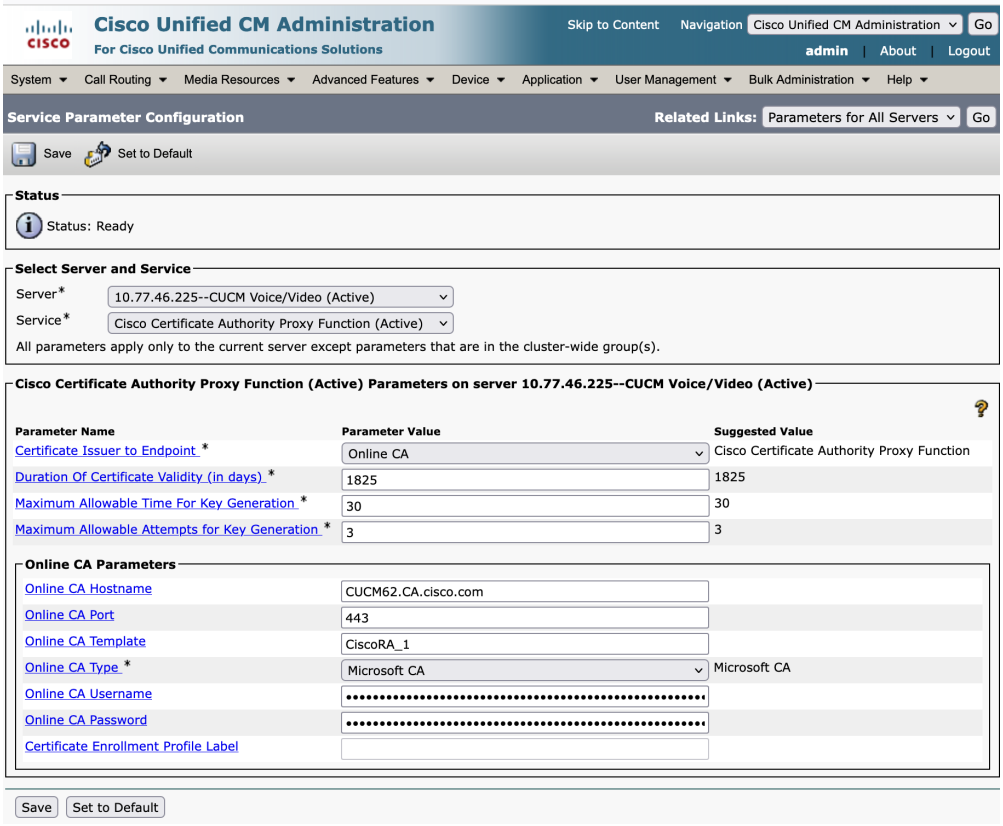
すべての証明書のインストールが完了したら、Cisco Desk Phone 9800 シリーズを再起動する必要があります。

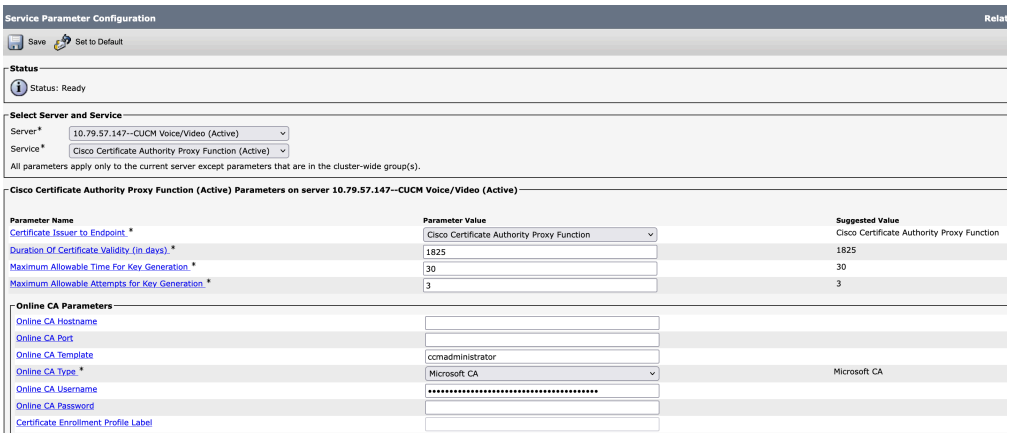
LSC 証明書

CUCM で CAPF サービスを有効にします。

1. **Cisco Unified CM Administration** にログインします。
2. **[システム（System）]** -> **[サービスパラメータ（Service Parameters）]** の順に選択します。
3. CUCM サーバを選択します。
4. **[Cisco Certificate Authority プロキシ機能] を選択します。**
5. **[エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）]** で証明書発行者を選択します。

6. **オンライン CA** が選択されている場合、 **オンライン CA パラメータで外部 CA を設定する必要があります。**
7. **[Cisco認証局プロキシ機能（Cisco 認証局プロキシ 機能）]**が選択されている場合、**組み込み** CAPF 機能を使用します。
8. [**保存**] ボタンをクリックします。





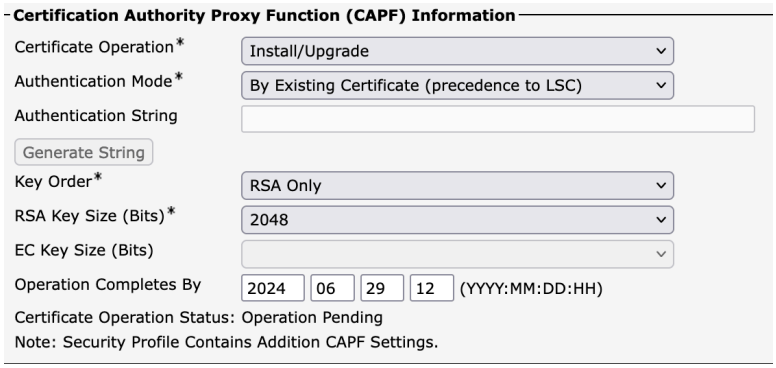
CAPF サーバーをアクティブにするか再起動します。

1. **Cisco Unified Serviceability にログインします。**
2. **[ツール（Tools）]** -> **[サービスの有効化（Service Activation）]** の順に選択します。
3. CUCM サーバを選択します。
4. **[Cisco認証局プロキシ機能（Cisco 認証局プロキシ 機能）]** が、[Activated（有効化）] になっていることを確認します。
5. [ツール（Tools）] > [Control Center機能サービス（Control center Feature Service）] の順に選択します。

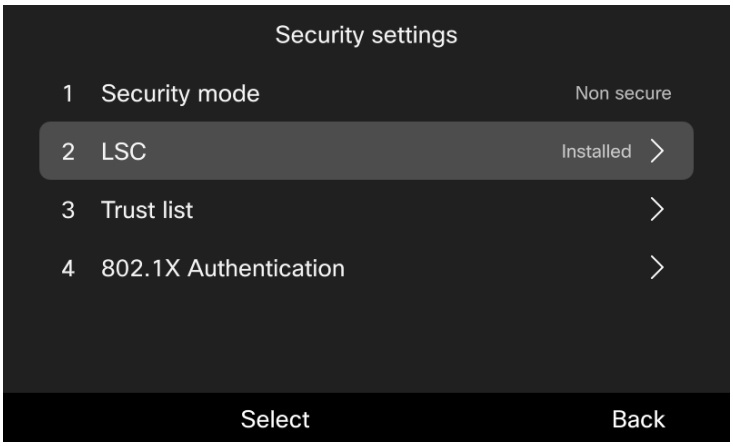
6. **[Cisco認証局プロキシ機能（Cisco 認証局プロキシ 機能）]** を選択して再起動します。

LSC 証明書を Cisco Desk Phone 9800 シリーズにインストールする

1. **Cisco Unified CM Administration** にログインします。
2. **端末** -> **電話**を入力し、端末のプロファイルページに移動します。
3. **[証明書操作（Certificate Operation）]** で**[インストール/アップグレード（Install/Upgrade）]** を選択し、**[保存（Save）]** > **[適用（Apply）]** の順に選択します。
4. 電話は LSC をインストールし、リブートします。



[設定（Settings）] > **[ネットワークとサービス（Network and services）]** > **[セキュリティ設定（Security settings）]** の順に選択し、電話 **LSC** ステータスをチェックします

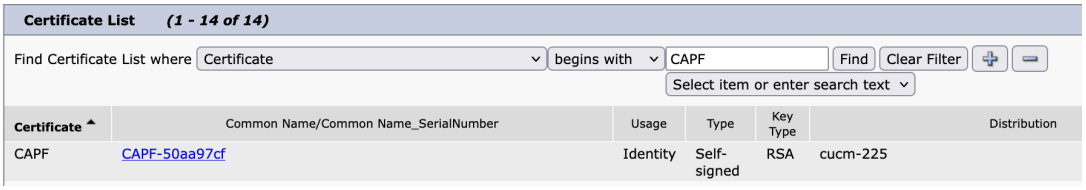


CAPF CA を ISE にインポートします。

CUCM から LSC CA 証明書をエクスポートします。

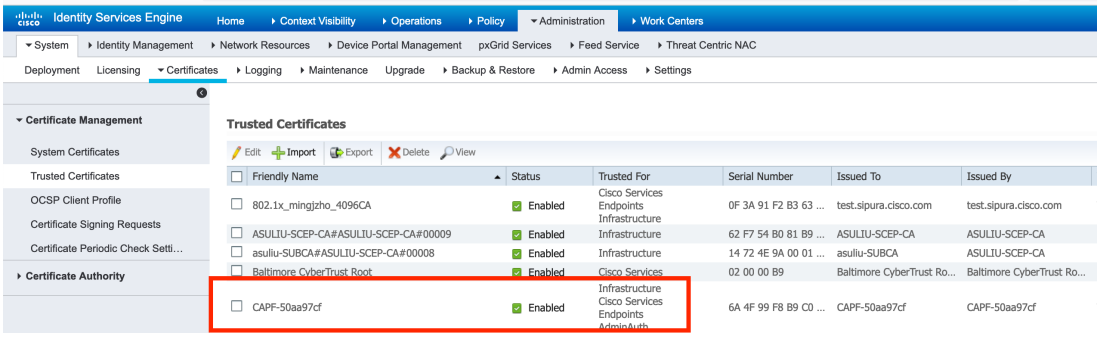
オンライン CAPF が使用されている場合は、ユーザーは管理者に外部 CA 証明書を要求します。 **組み込み** CAPF が使用されている場合、ユーザーは、CUCM から CA 証明書をダウンロードできます。

1. **Cisco Unified OS Administration** にログインします
2. **[セキュリティ（Security）]** -> **[証明書の管理（Certificate Management）]** の順に選択します。
3. CAPF アイデンティティ証明書をダウンロードします



LSC 証明書を信頼リストにインポートしてください。

LSC 証明書の CA チェーンが RADIUS サーバの信頼リストに追加されていることを確認します。

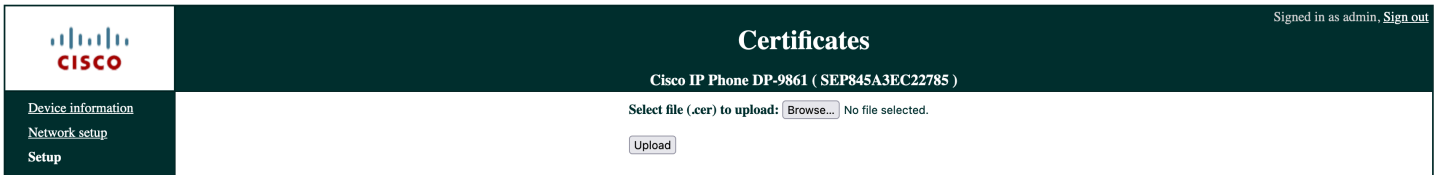


サーバ証明書

RADIUS サーバーの証明書を発行したルート CA 証明書を **EAP-TLS** に対してインストールするか [サーバー検証（Server Validation）] を有効にします。 サービス検証はオプションです。 ユーザがそれを望まない場合、この手順は省略できます。

手動でサーバー証明書をインストールするには、メインの**[証明書（Certificates）]**ウェブページの **[認証サーバーCA（Authentication Server CA）]** に対して **[インストール（Install）]**を選択します。

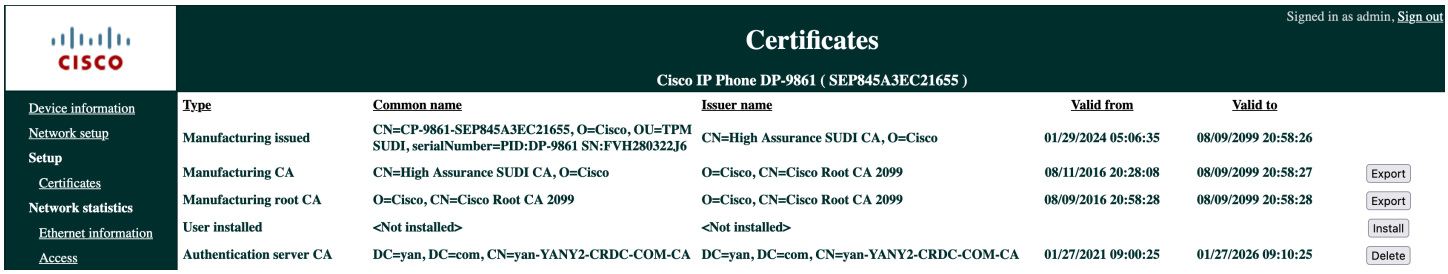
[参照（Browse）] を選択し、**PEM (Base-64)** または **DER** エンコーディングがあるサーバー証明書を指します。



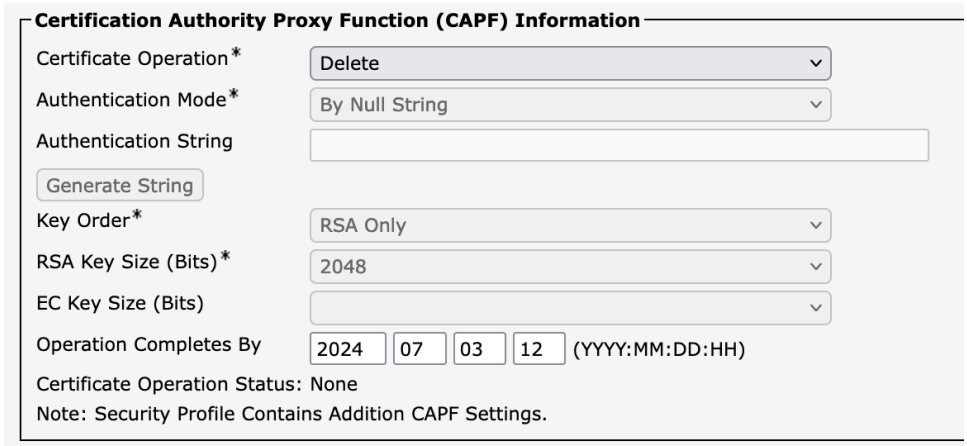
すべての証明書のインストールが完了したら、Cisco Desk Phone 9800 シリーズを再起動する必要があります。

証明書の削除

User Installed 証明書は、管理者ウェブページインターフェイスから削除できます。 管理ウェブページから証明書を削除するには、対応する証明書に対して [削除（Delete）] を選択し、証明書が削除されたら、電話を再起動します。



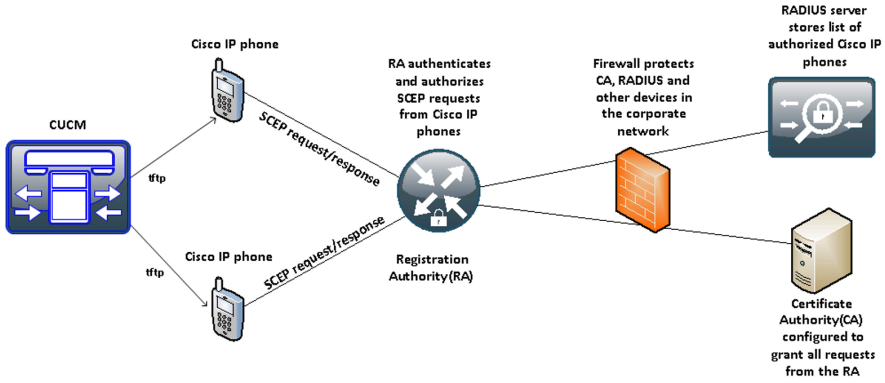
LSC 証明書を、CUCM 電話ページで削除したら、**[保存（Save）]** >**[適用（Apply）]** の順に選択します。



シンプル証明書登録プロトコル（SCEP）

SCEP は、証明書を自動的にプロビジョニングおよび更新するための標準であるため、クライアントへの証明書の手動インストールと再インストールを回避できます。

Cisco IOS 登録エージェント (RA) (例、Cisco IOS ルーター) は、証明書を発行する SCEP 対応 CA へのプロキシ (例、SCEP RA) として機能できます。 トポロジは、次の図のようになっています。



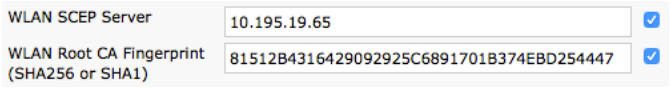
同じ CA チェーンが、電話および RADIUS サーバへの証明書の発行に使用されていることを確認します。そうしないと、サーバ検証が失敗する可能性があります。

SCEP による最初の証明書登録の場合、Cisco Desk Phone 9800 シリーズは、Cisco Unified Communications Manager に接続されているイーサネット ネットワークに接続されている必要があります。

Cisco Desk Phone 9800 シリーズは、SCEP 要求のために Cisco Unified Communications Manager で定義された次のパラメータを利用します。

SCEP RA の IP アドレスまたはホスト名のいずれかを含むように、 **WLAN SCEP サーバ** を設定する必要があります。

WLAN ルート CA 指紋 (SHA256 または SHA1) は、証明書を発行する CA の指紋を含むように設定する必要があります。 SCEP RA が登録されている発行 CA が下位 CA の場合、その指紋を入力しますが、ルート CA の指紋は入力しません。定義された指紋は受け取った証明書を検証するために使用されます。
これらのパラメータを削除すると SCEP が無効になります。

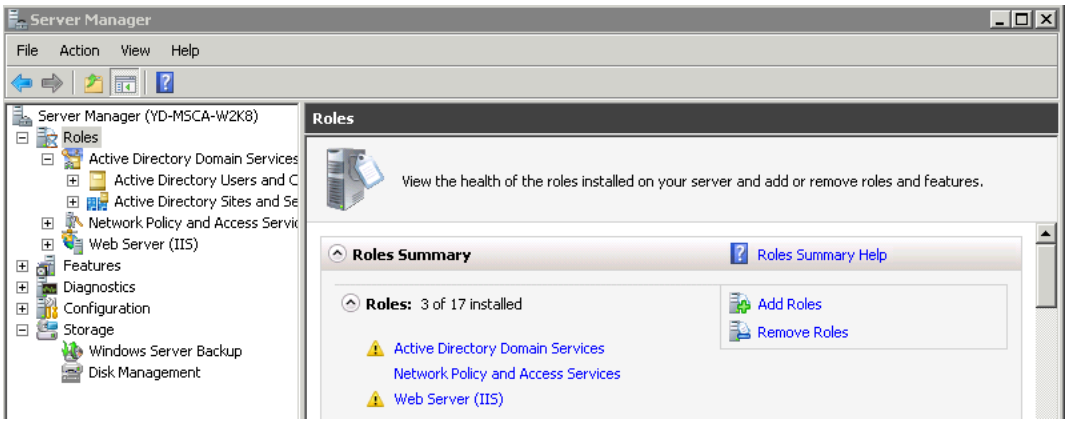


Cisco Desk Phone 9800 シリーズは SCEP 登録要求を SCEP RA に送信します。これには、身元証明（POI）として、電話のManufacturing Installed Certificate（MIC）も含まれます。
SCEP RA は、電話の MIC を発行した下位 CA の証明書を使用して、電話の MIC を検証し、以降のデバイス認証のために、それを RADIUS サーバに渡します。
RADIUS サーバはデバイスを検証し、SCEP RA に応答を送信します。
SCEP RA は、その後、RADIUS 認証が成功した場合、登録リクエストを CA に転送します。
SCEP RA は CA からユーザー証明書を受け取り、電話からポーリング要求を受け取った後でそれを電話に送信します。
Cisco Desk Phone 9800 シリーズは、ユーザとサーバの証明書の有効期限を定期的にチェックします。
証明書の更新は、有効期限が 50 日以内の場合、更新が成功するまで 24 時間ごとに行われます。
WLAN Root CA Fingerprint（SHA256 または SHA1）を定義するために使用される CA 証明書の有効期限が切れている場合、電話は新しい CA 証明書の SCEP getca 要求を送信します。しかし、それが正常に検証されるためには、管理者は新しい CA 証明書に合わせて、Cisco Unified Communication Manager 内で電話の設定の指紋を更新する必要があります。 CA から新しい証明書が正常に受信されると、古い CA 証明書は削除されます。
ユーザ証明書の有効期限が切れている場合、電話はユーザ証明書を更新するために新しい SCEP 登録要求を送信します。 新しいユーザの証明書が CA から正常に受信されると、古いユーザの証明書は削除されます。
WLAN SCEP サーバー または **WLAN Root CA Fingerprint（SHA256 or SHA1）** が修正された場合、Cisco Desk Phone 9800 シリーズは CA とユーザー証明書を即時に更新しようとします。

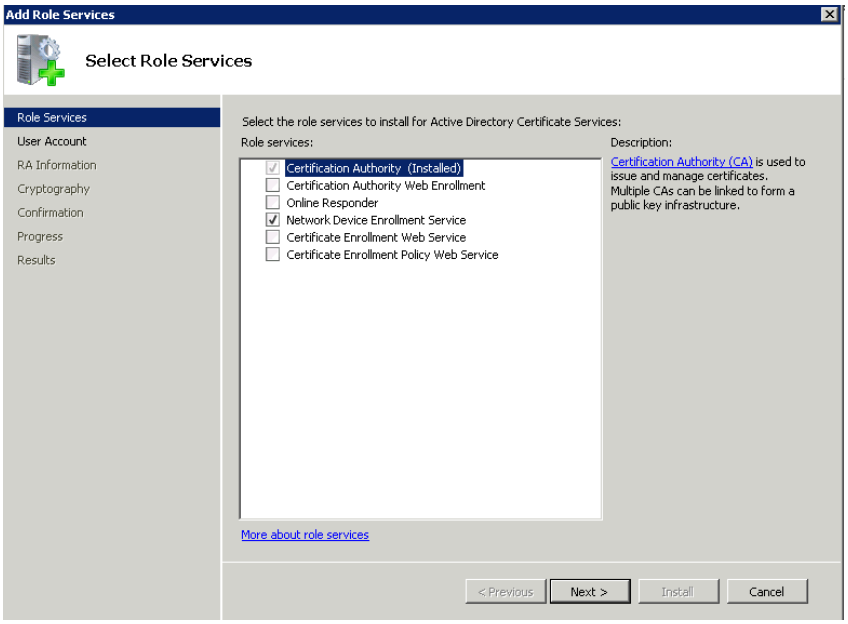
認証局 (CA) の設定

Microsoft® 認証局 (CA) サーバの使用を推奨します。
以下のガイドラインに従って、Microsoft CA を設定してください。

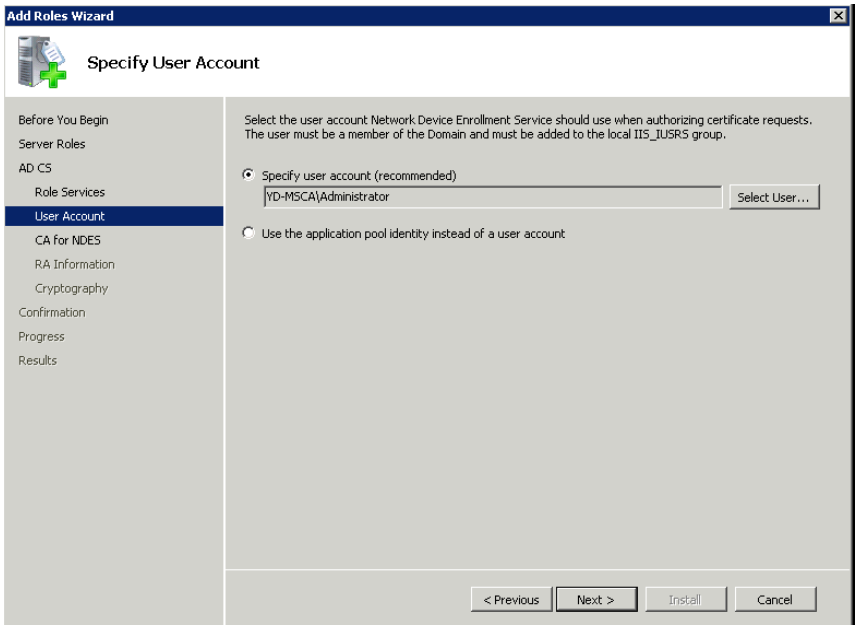
1. Microsoft Windows サーバ上に認証局と Active Directory ドメインサービスを作成します。
2. ネットワーク デバイス登録サービスを有効にします。
3. [ユーザープロパティ（user property）] 画面の**[MemberOf]**タブにアクセスして、**管理者**を **IIS_IUSERS**のメンバーにします。
4. **Server Manager** を、起動して**[ロールを追加（Add roles）]** をクリックします。



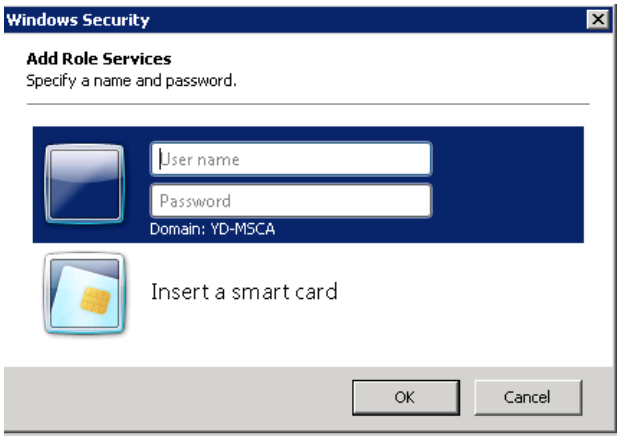
5. **[サーバーロールを選択（Select Server Role）]** ページで、**[Active Directory証明書（Active Directory Certificate）]** **[サービス（Services）]** ロールの順に選択し、**[次へ（Next）]** をクリックします。 選択されているデフォルトサービスは、**[認証局（Certification Authority）]**です。チェックボックスをオフにして移動します。
6. **Network Device Enrollment Service** の役割サービスを追加します。
7. **[ロールウィザードを追加（Add Roles Wizard）]**、**[ロールサービスを選択（Select Role Services）]** ページの、**[ネットワークデバイス登録サービス（Network Device Enrollment Service）]** チェックボックスをオンにしたら、**[次へ（Next）]** をクリックします。



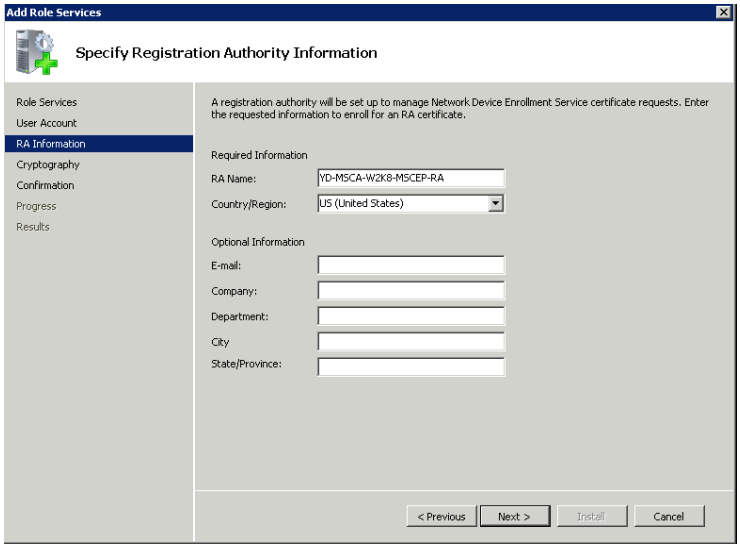
8. ウィザードは、必要なすべての依存関係がインストールされているかどうかを検出します。 既存しない依存関係がある場合は、それについて説明するダイアログボックスが表示され、依存関係のインストールについての許可を求めます。 インストールを続行するには、**[はい（Yes）]** をクリックします。
9. **[ロールサービス（Role Services）]**の **[ユーザーアカウント（User Account）]** をクリックし、**[ユーザーを選択（Select User）]**.... をクリックします。



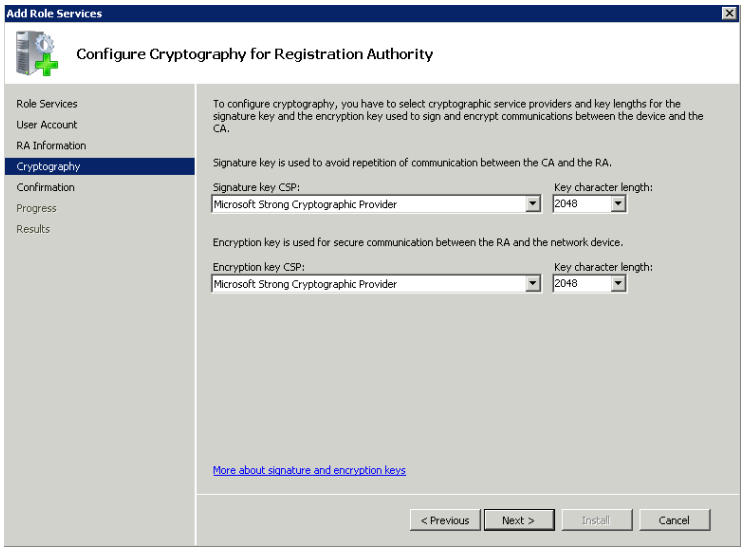
10. ユーザー名として**管理者**と入力し、パスワードを入力します。



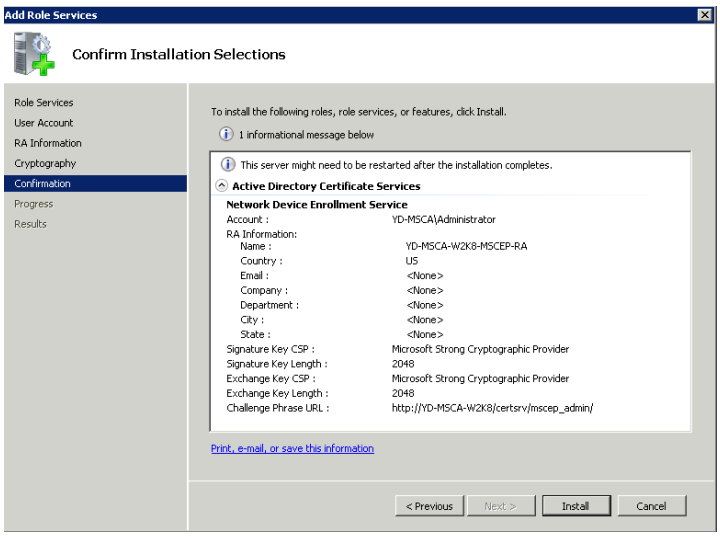
11. 登録機関情報を入力します。



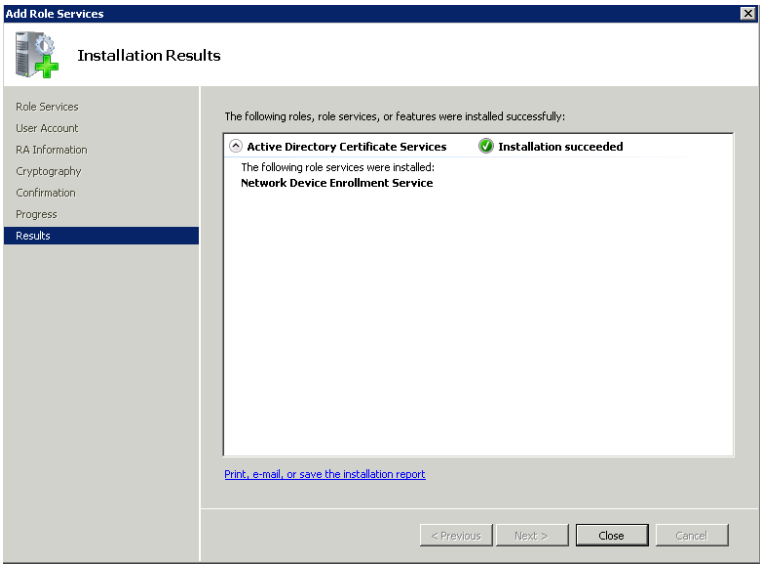
12. **[Signature Key CSP]** および **[Encryption key CSP]** に対して **[Microsoft Strong Cryptographic Provider]** を選択します。
13. **[キーの文字長（Key character length）]** に対して、**2048** を選択します。



14. **[インストール（Install]）** を選択します。

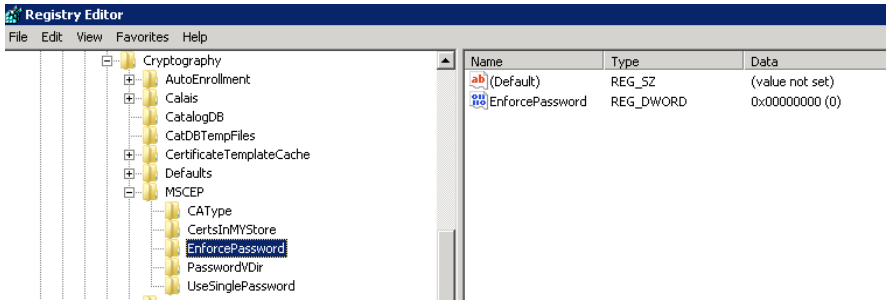


インストールが成功した場合、確認ページが表示されます。



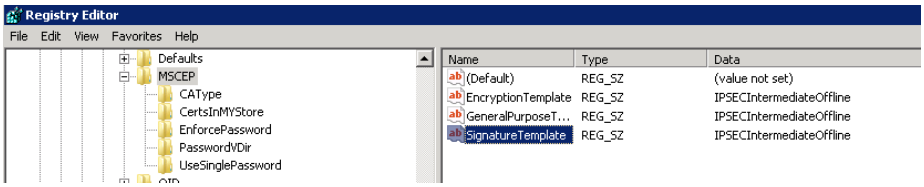
15. **[EnforcePassword]** を 0 を選択して、**regedit** 経由で [SCEP登録変更パスワード要件（SCEP enrollment challenge password requirement）] を無効にします。

（[HKEY_LOCAL_MACHINE] > [ソフトウェア（SOFTWARE）] > [Microsoft] > [暗号化（Cryptography）] > [MSCEP] > [EnforcePassword]）



16. SCEP の証明書テンプレートを指定する

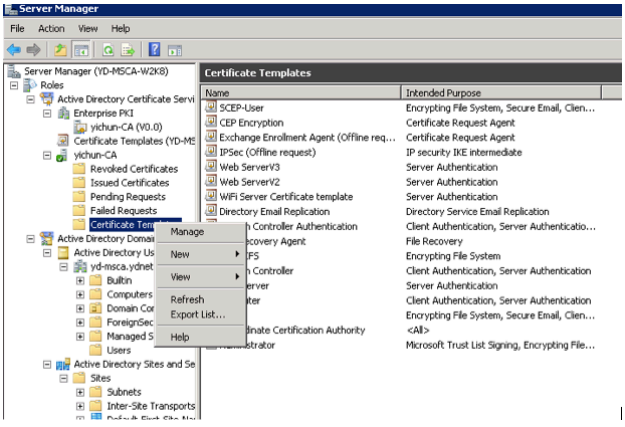
    SCEP は、レジストリで設定されている証明書テンプレートを使用して証明書を発行します。 （[HKEY_LOCAL_MACHINE] > [ソフトウェア（SOFTWARE）] > [Microsoft] > [暗号化（Cryptography）] > [MSCEP]）



    通常、RA にはより長い期間があります (CA 証明書の期間と同じ)。 RA を SCP サーバに登録するために使用するデフォルトのテンプレートは、上でハイライトした **IPSECIntermediateOffline** です。そのため、Cisco RA を SCEP サーバに登録する前に、正しいテンプレートが上記のレジストリに設定されていることを確認してください。

    Cisco RA が SCEP サーバに登録された後、管理者はレジストリのテンプレートを変更する必要があります (ユーザ証明書の期間をルート CA の期間より短くする必要がある場合)。

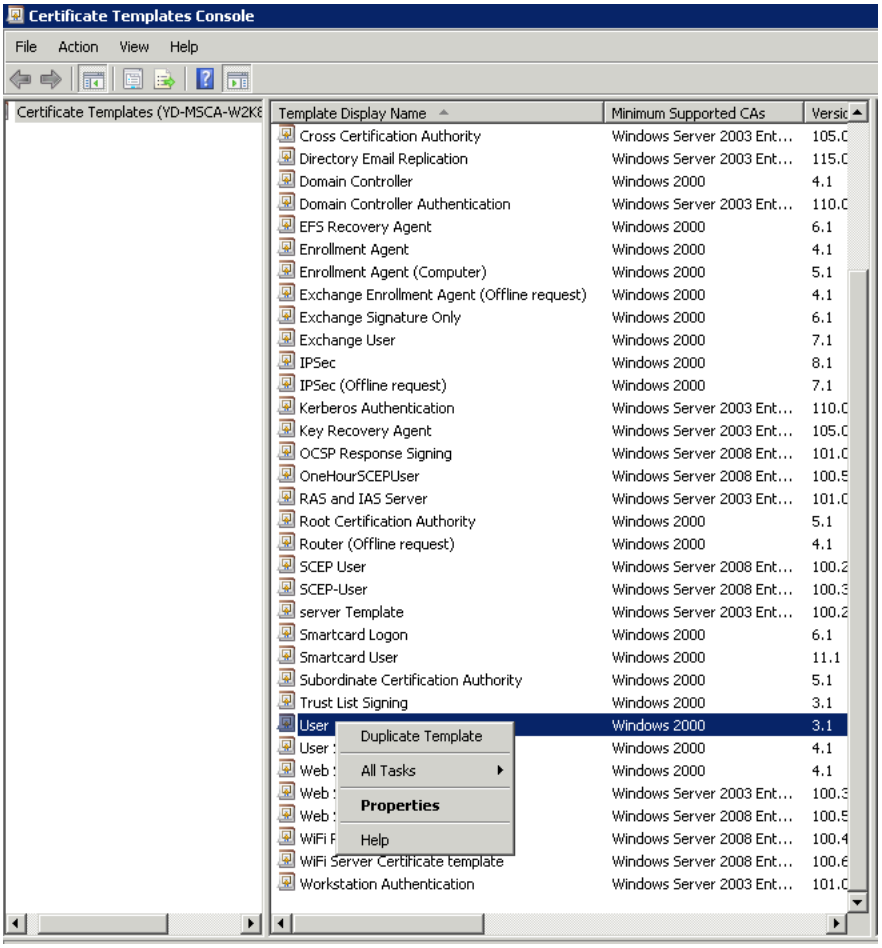
17. **[Certificateテンプレート（Certificate Templates）]** を右クリックし、**[管理（Manage）]**を選択します。



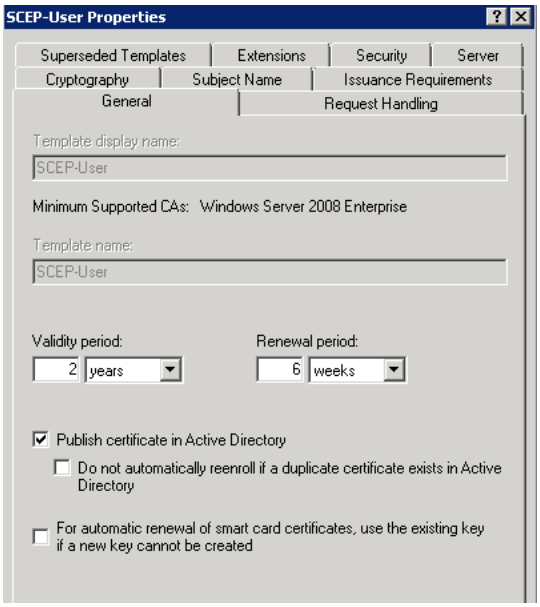
18. **[Userテンプレート（User template）]** を右クリックし、**[Duplicateテンプレート（Duplicate Template）]** を選択します。
19. **[Windows Server 2003 2008 テンプレート] を選択します。**
20. **[全般（General）]** タブで、テンプレート名と有効期間を変更します。
21. **[拡張（Extensions）]** タブで、以下を確認します。

クライアント認証 がアプリケーションポリシーの 1 つとして設定されています。

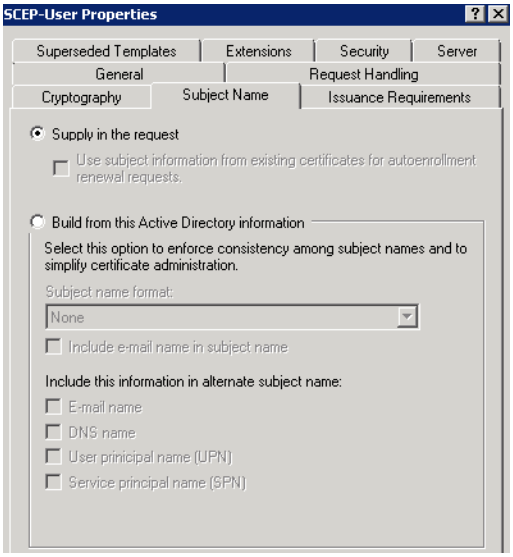
[キーの使用（Key Usage）] には、**[デジタル署名（Digital Signature）]** 属性があります



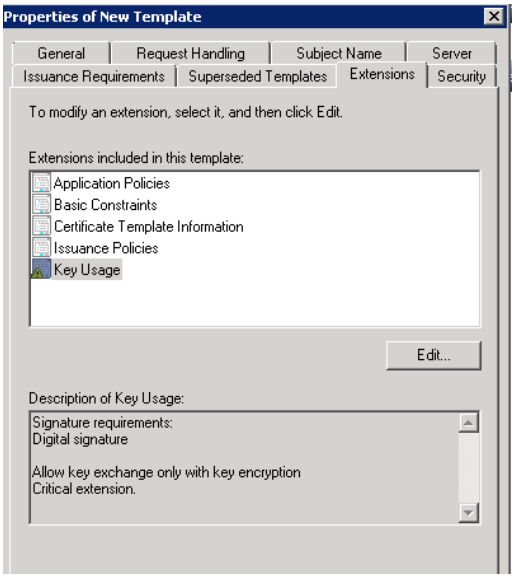
22. 必要に応じて、**[全般（General）]** の **[有効期限（Validity Period）]** タブを設定します。



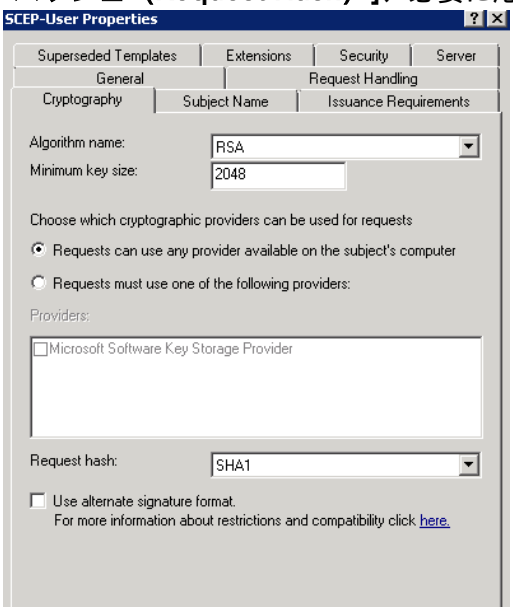
23. 以下に示すように、**[サブジェクト名（Subject Name）]** を設定します。



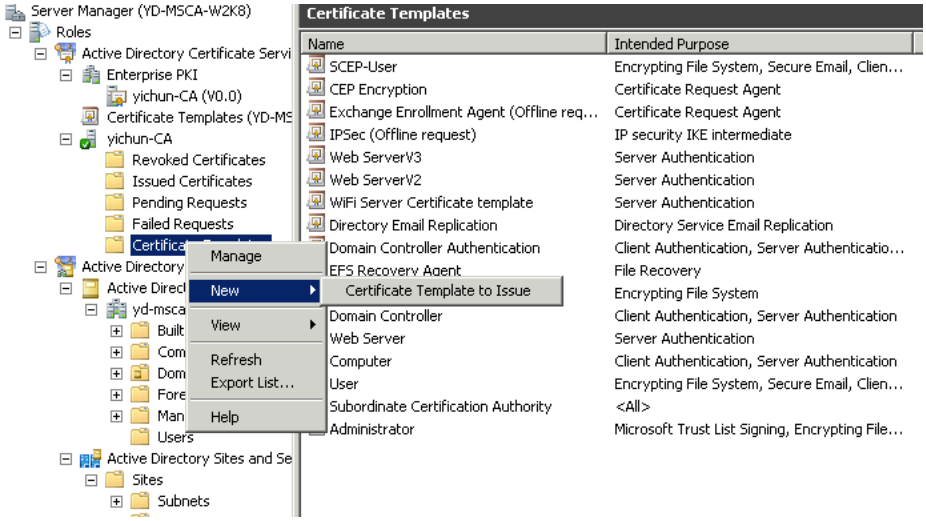
24. 以下に示すように、 **拡張機能** タブを設定します。



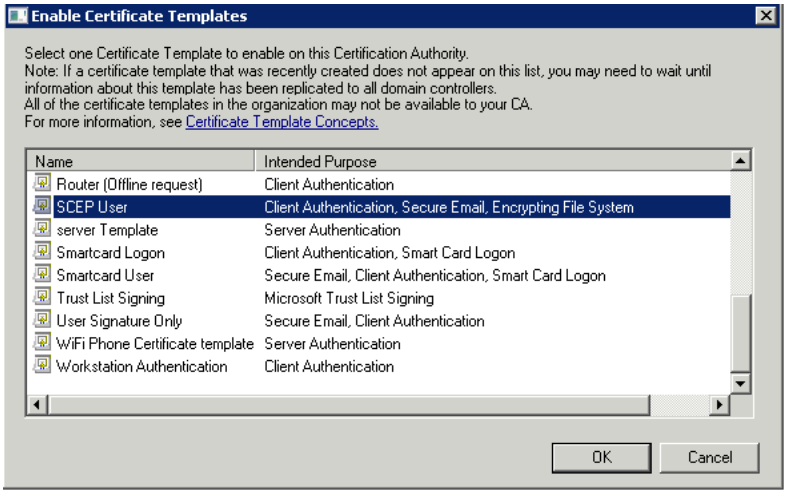
25. **[アルゴリズム名（Algorithm Name）]**、**[キーの最小サイズ（Minimum Key Size）]** および **[リクエストハッシュ（Request Hash）]**、必要に応じて、**[暗号化（Cryptography）]** タブを設定します。



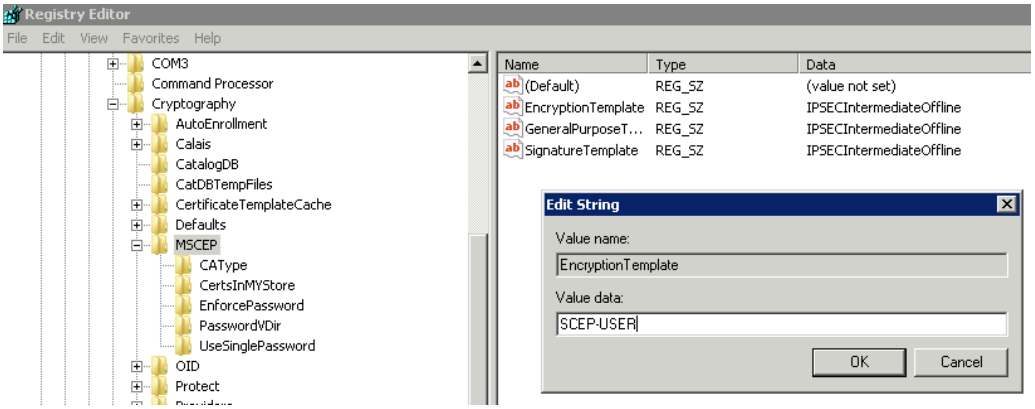
26. 新しく作成したテンプレートを有効にするには、**[Certificateテンプレート（Certificate Templates）]** を右クリックして、**[新規（New）]** > **[Certificateテンプレート（Certificate Templates）]** の順に選択し、**発行します。**



27. **SCEP ユーザ** テンプレートを選択します。



28. **regedit** 経由で、新規作成したテンプレートを SCEP に関連付けます。

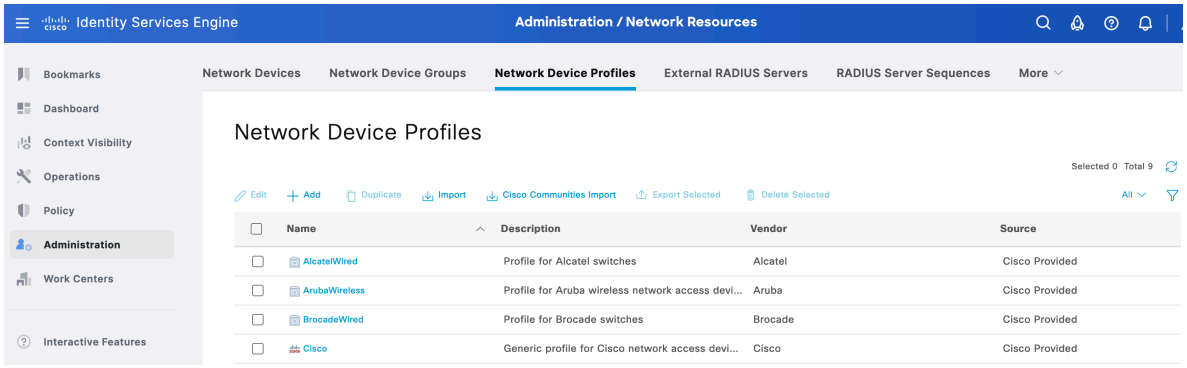


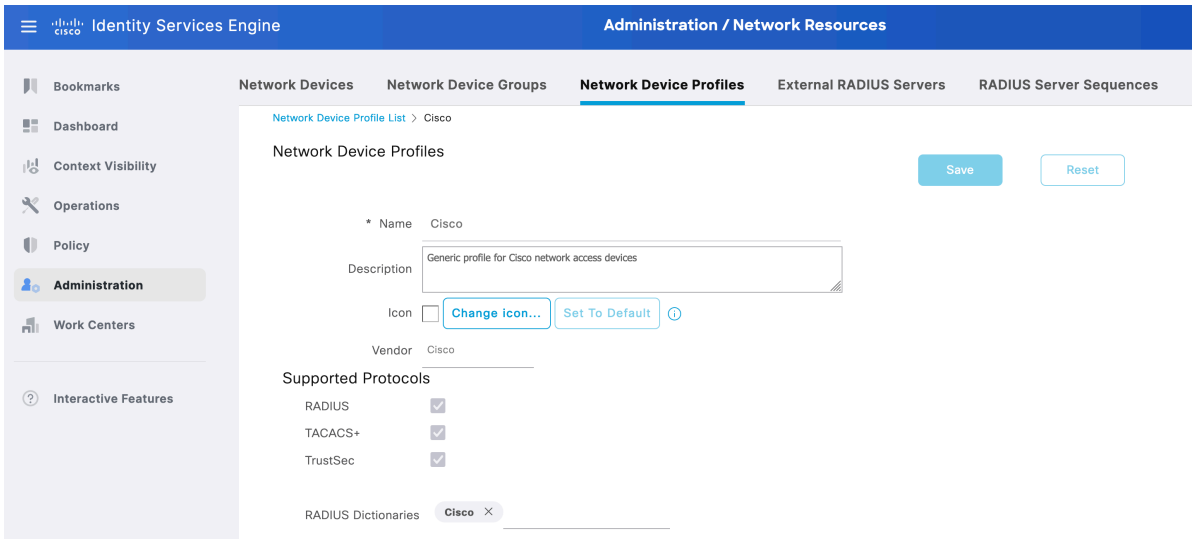
29. [**IIS**] [**アプリケーションプール**] に移動して SCEP サービスを再起動し、新しいテンプレートを有効にします。

RADIUS 構成

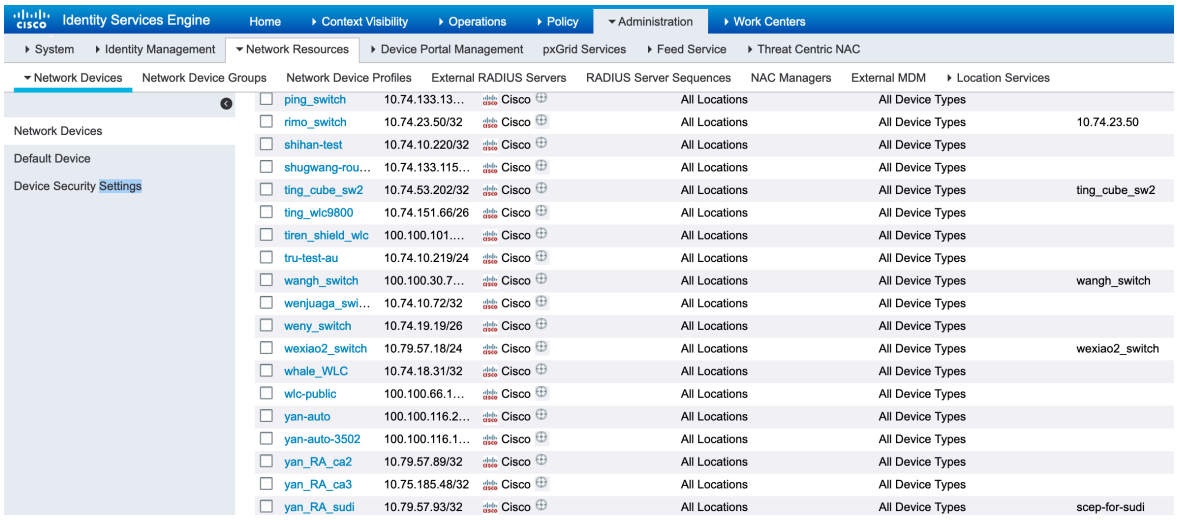
以下のガイドラインに従って、RADIUS サーバを設定します。 ISE サーバは登録のための SCEP デバイス認証の役割を果たし、SCEP ソリューションのための Cisco IOS RA との PKI 統合に使用できます。

1. **[管理（Administration）]** > **[ネットワークデバイスプロファイル（Network Device Profile）]** の順に選択し、新しいプロファイルを追加するか **Cisco** という既存のプロファイルを活用します。 新しいプロファイルを作成する際は、**[対応プロトコル（Supported Protocols）]**、**[認証/承認（Authentication/Authorization）]** および **[権限（Permission）]**を適切に設定します。

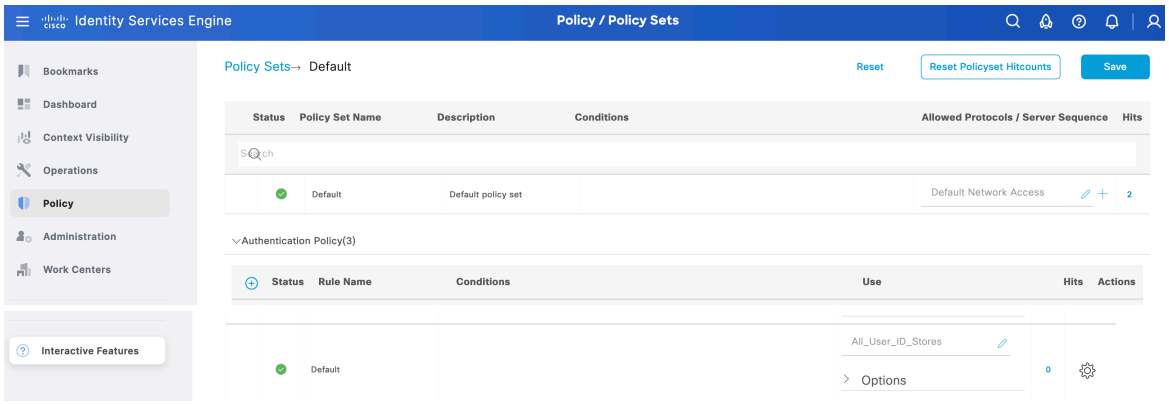




2. **[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** の順に選択し、以下に示すように yan_RA_sudi などの Cisco IOS にデバイスを追加します

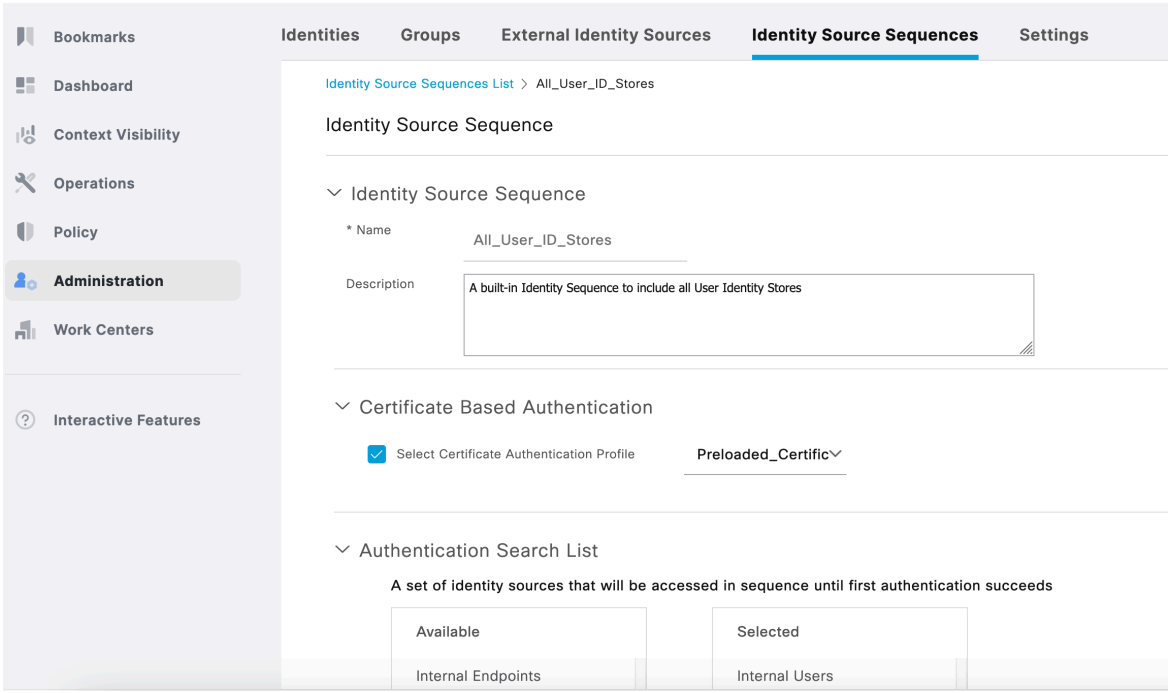


3. **[ポリシー（Policy）] > [認証（Authentication）]** の順に選択し、**[デフォルト（Default）]** ルールを設定して、**[デフォルトのネットワークアクセス（Default Network Access）]** と **[All_Uesr_ID_Stores]** を使用します。

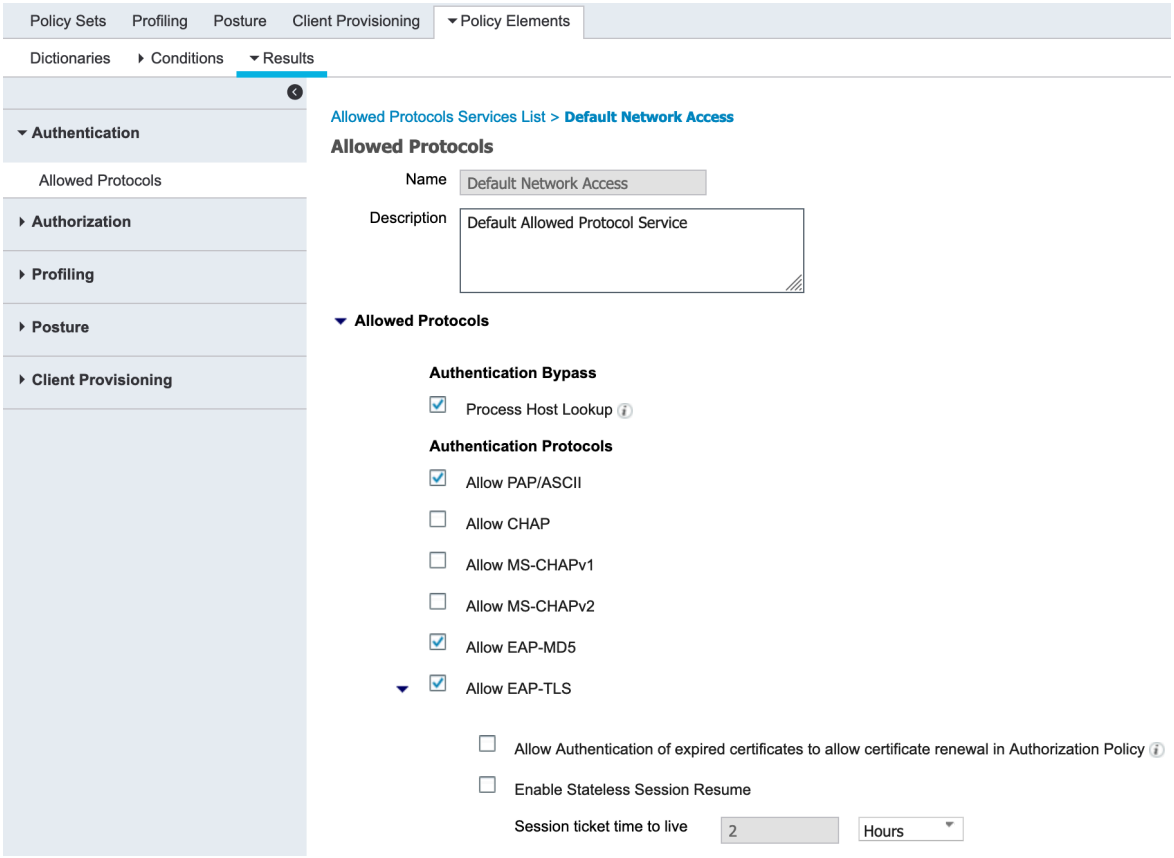


Cisco IOS RA では証明書ベースの認証がすでに完了しているため、認証オプションは「認証が失敗した場合」または「ユーザが見つからない場合」に対して続行するように設定できます。

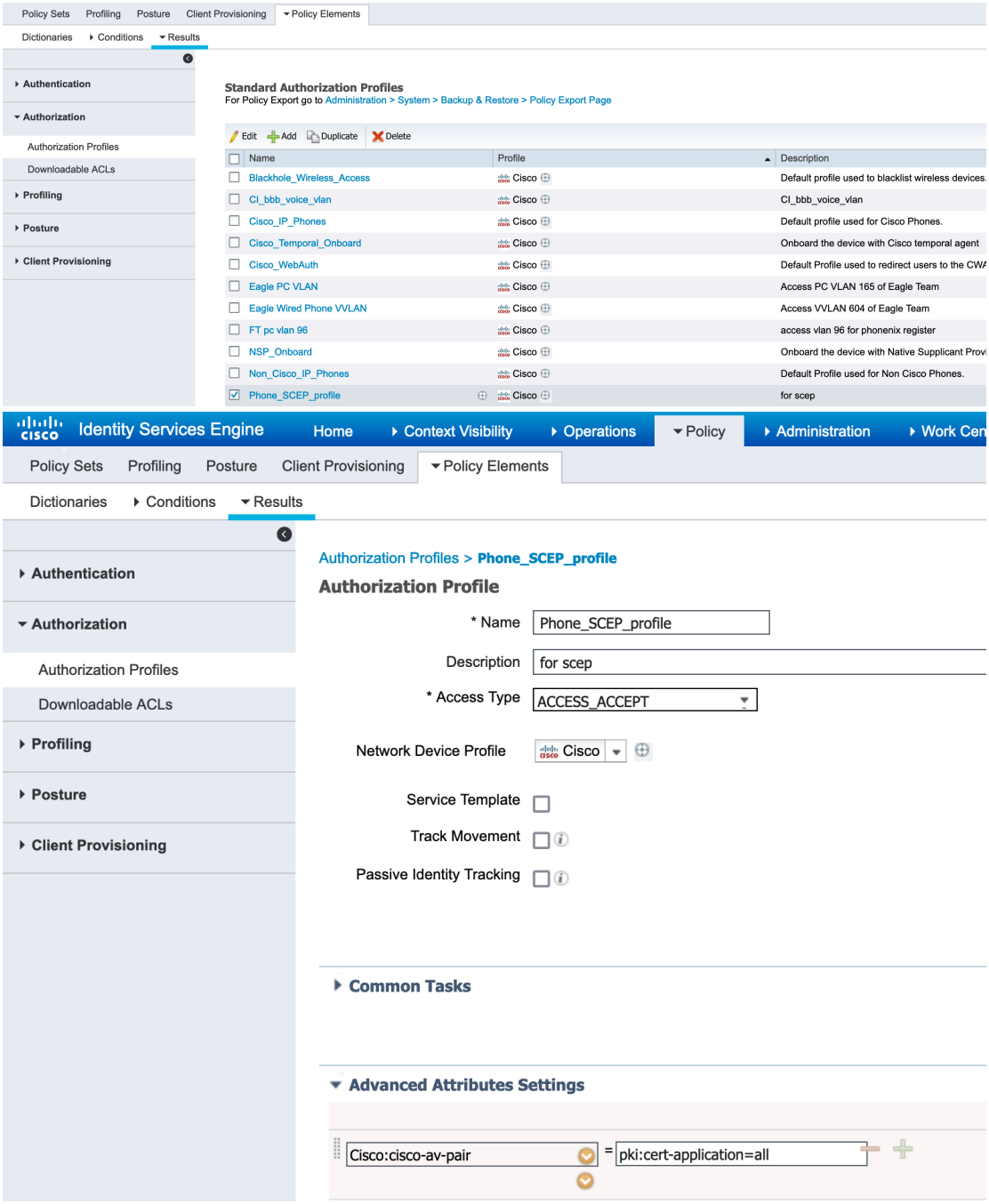
4. **[管理（Administration）] > [アイデンティティ管理（Identity Management）] > [アイデンティティソースシーケンス（Identity Source Sequence）]** の順に選択します。



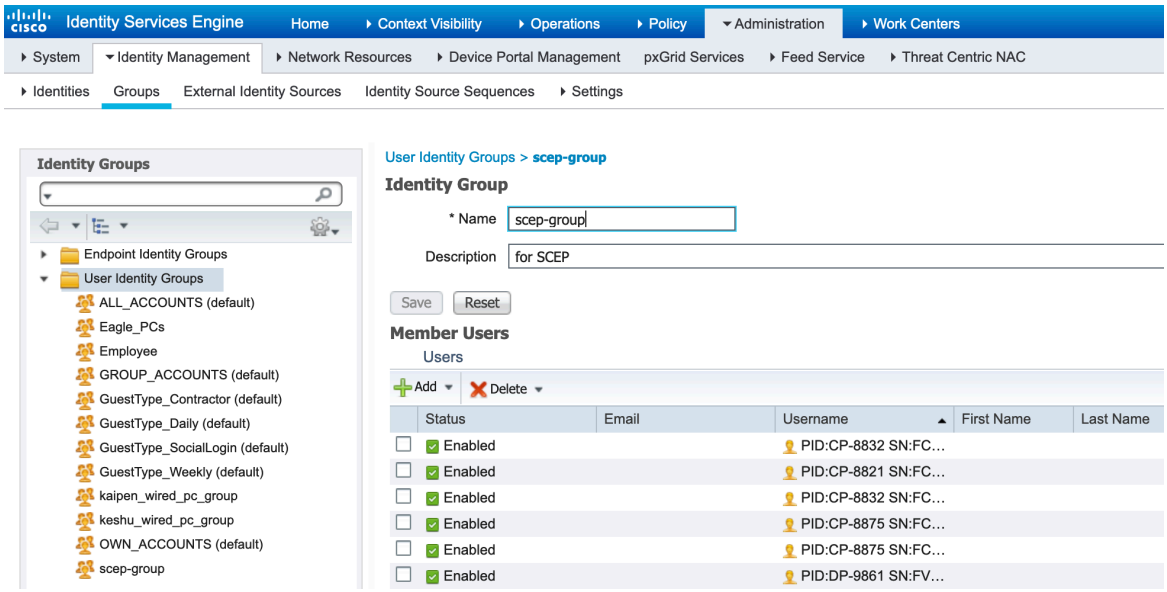
5. **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可済みプロトコル（Allowed Protocols）]** の順に選択し、以下に示すように、**[デフォルトのネットワークアクセス（Default Network Access）]** を編集します



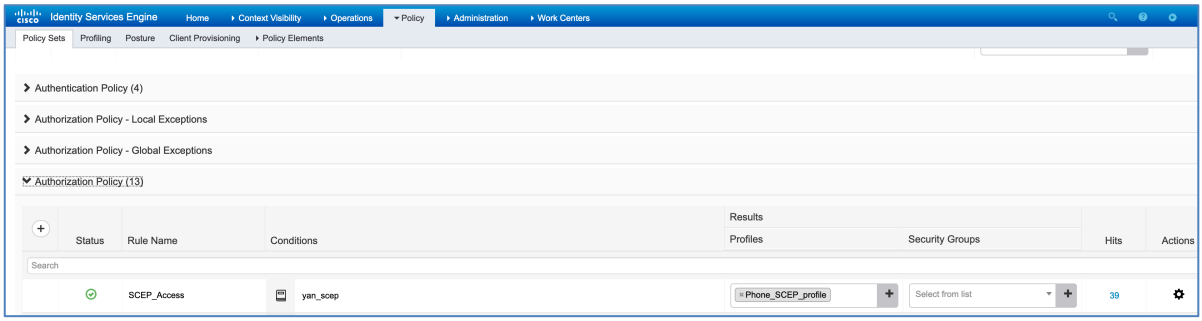
6. **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** の順に選択し、Phone_SCEP_profile などの SCEP にプロファイルを追加します。

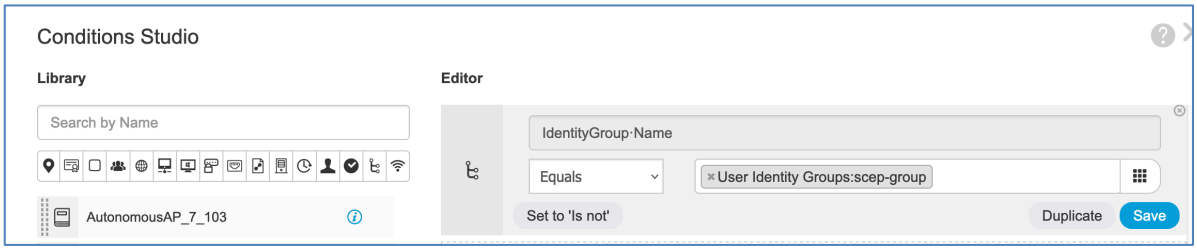


7. **[管理（Administration）] > [アイデンティティ管理（Identity Management）] > [グループ（Groups）] > [ユーザーアイデンティティグループ（User Identity Groups）]** の順に選択し、以下に示されているように、scep-group などの SCEP に対してユーザーグループを追加します。

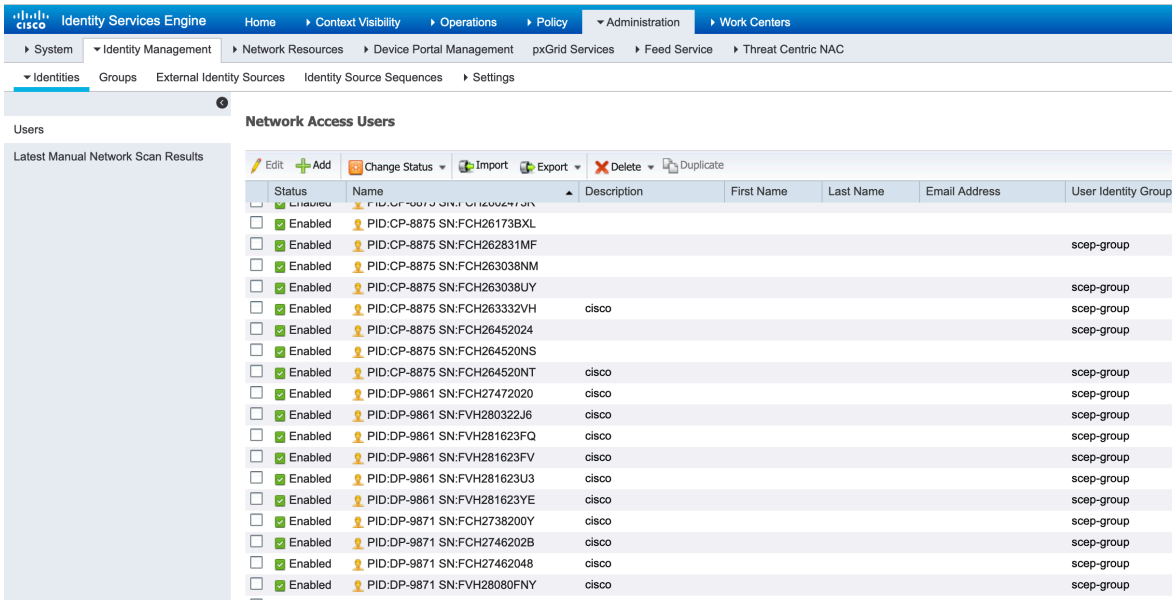


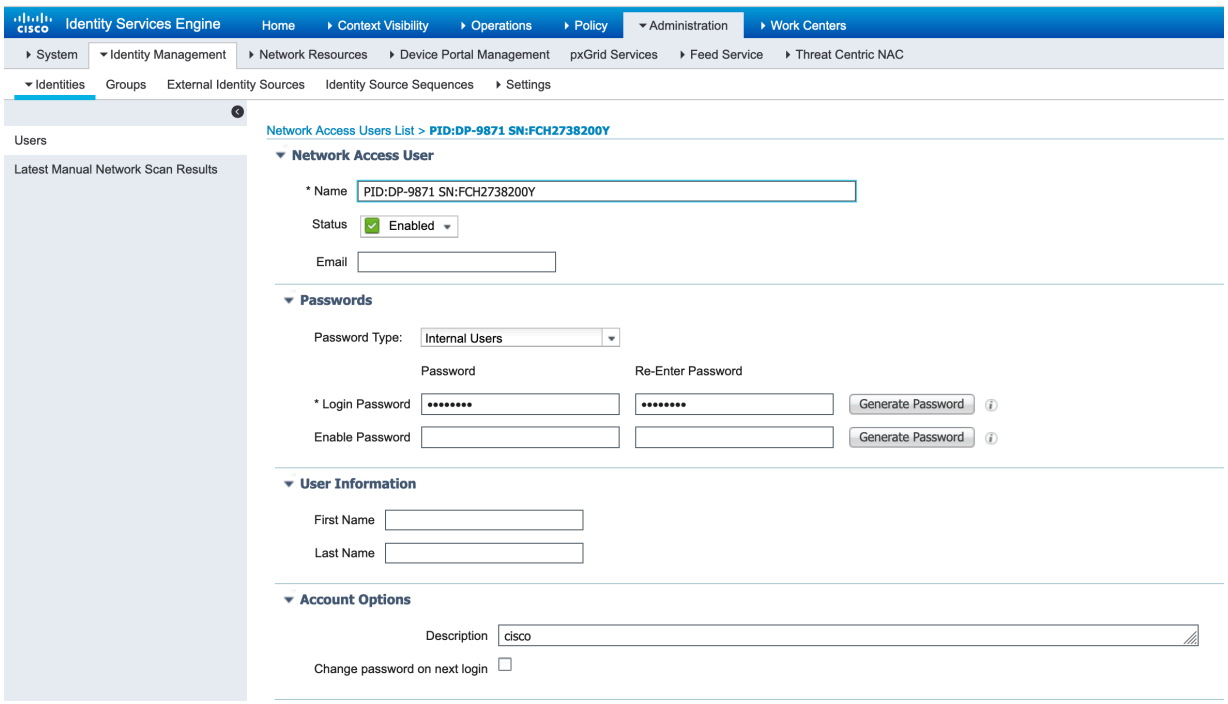
8. **[ポリシー（Policy）]** > **[認証ポリシー（Authorization Policy）]** の順に選択し、既存ポリシーの [Edit（編集）] の横にある下矢印をクリックして SCEP 認証ポリシーを追加し、**上記の [新ルールを挿入（Insert new rule）]** を選択します。





9. **[管理（Administration）]** > **[アイデンティティ（Identities）]** > **[ユーザー（Users）]** の順に選択し、Cisco Desk Phone 9800 シリーズのユーザーアカウントを作成します。 ユーザ名の形式は **serial Number** です (例、 PID:DP-9861 SN:FCH27472020)。





SCEP RA 設定

現在、IOS バージョン 15.1(4)M10 以降を実行している Cisco IOS ルーターのみが SCEP RA としてサポートされています。

以下のガイドラインに従って、Cisco IOS ルーターを SCEP RA として設定します。

- Cisco IOS ルーターで HTTP サーバを有効にします。

```
ISR_RA# configure terminal
ISR_RA(config)# ip http server
ISR_RA(config)# exit
```

- デバイス認証用に RADIUS サーバを設定します。

```
ISR_RA# configure terminal
ISR_RA(config)# radius server MyRadius
ISR_RA(config-radius-server)# address ipv4 10.195.19.63 auth-port 1812 acct-port 1813
ISR_RA(config-radius-server)# key <REMOVED>
ISR_RA(config-radius-server)# exit
ISR_RA(config)# aaa authorization network PhoneList group radius
ISR_RA(config)# exit
```

- 電話の MIC を検証するために、MIC の CA チェーンの PKI トラストポイントを設定します。

```
ISR_RA# configure terminal
ISR_RA(config)#crypto pki trustpoint MIC_trustpoint
ISR_RA(ca-trustpoint)# authorization list PhoneList
ISR_RA(ca-trustpoint)# authorization username subjectname commonname
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)#crypto pki trustpoint MIC_trustpoint
ISR_RA(ca-trustpoint)# enrollment terminal
ISR_RA(ca-trustpoint)# 失効確認なし
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki authenticate MIC_trustpoint
Base 64 エンコードされた製造 CA 証明書を入力します。 空行で終了するか、または「quit」という単語だけの行で終了します。
-----BEGIN CERTIFICATE-----
```

MIIEZTCCA02gAwIBAgIBAjANBgkqhkiG9w0BAQsFADArMQ4wDAYDVQQKEwVDaXNj
bzEZMBcGA1UEAxMQQ2lzY28gUm9vdCBDQSBNMjAeFw0xMjExMTIxMzUwNThaFw0z
NzExMTIxMzAwMTdaMDYxDjAMBgNVBAoTBUNpc2NvMSQwIgYDVQQDExtDaXNjbyBN
YW51ZmFjdHVyaW5nIENBIFNIQTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQD0NktCAjJn3kk98hU7wUVp6QlOFrlltEce6CpbfYpeLdUeZduAo+S0otzT
lJwS2BlMhZtacu9vUpfmW9w7nQo9zVT3eyPuhF/6/9TEdVBn75zb5CfV+E6ld+fH
nuPiFyBu+HDDJRd373Op+957ldoWyPvD8hHR1HJGFJ3JJKBg0UScL4JCwleu98Xq
/yPlAqBhExa7a2/fqSmZA0vZlG1bBfWZY8ZtSeTxKg3eWynV+xElabHqTDMYWf+2
obs4YB5llNTbYgHyRETP6T8Xr6TtD0h3654OUHcW+1meBu/jctluMKppeSjVtrof
5vt+pbkCg0iQAAjsL0qczT3yaNXvAgMBAAGjggGHMIIBgzAOBgNVHQ8BAf8EBAMC
AQYwEgYDVR0TAQH/BAgwBgEB/wIBADBcBgNVHSAEVTBTMFEGCisGAQQBCRUBEgAw
QzBBBggrBgEFBQcCary1aHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L3BvbGljaWVzL2luZGV4Lmh0bWwwHQYDVR0OBBYEFHrXeZXKu0gruFUU/aPAD7yn
D5YZMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jcmwvY3JjYW0yLmNybDB8BggrBgEFBQcBAQRwMG4wPgYIKwYBBQUH
MAKGMmh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jcmNh
bTIuY2VyMCwGCCsGAQUFBzABhiBodHRwczovL3Rvb2xzLmNpc2NvLmNvbS9wa2kv
b2NzcDAfBgNVHSMEGDAWgBTJAPkfih/CZr2l0m1lDiluNMMFoDANBgkqhkiG9w0B
AQsFAAOCAQEAc1k2rH6YT4juFxs9q7ObzfcKbNvOyDsaU7av4lHFXmn/JxfnBmUv
YxAI2Hx3xRb0KtG1JGkffQjVAtBboTXynLaQso/jj46ZOublF8y6Ho3nTAv7Q6VH

kqSCdZClVu91zbHV9FFYQzJxjw1QgB0a4ItS4yhdmgl3oDNEcb3trQezrQ3/857/
lSqBGVLEbKHOu8H6zOLhxAgZ08ae1oQQQJowki0lbd+LRLGovtEwLg8yyqiTlGve
7VFL2sRa8Z3rK9tlwKVH2kpFKNAeN3rfKFqr0/weR0cyKpmLMrSBTBZcxQcJCYF4
X6FO/32KOqcxJFlOKGVlUjvAvioOqoducw==
-----END CERTIFICATE-----

トラストポイント「MIC_trustpoint」は下位 CA であり、非自己署名証明書を保持しています。
証明書には次の属性があります。
指紋 MD5: AC14F08F C3780F8F D9EEE6C9 39111280
指紋 SHA1: 90B2E06B 7AD5DAFF CFD43187 2909F381 37471BF8
トラストポイント CA 証明書が承認されました。
ISR_RA(config)# exit

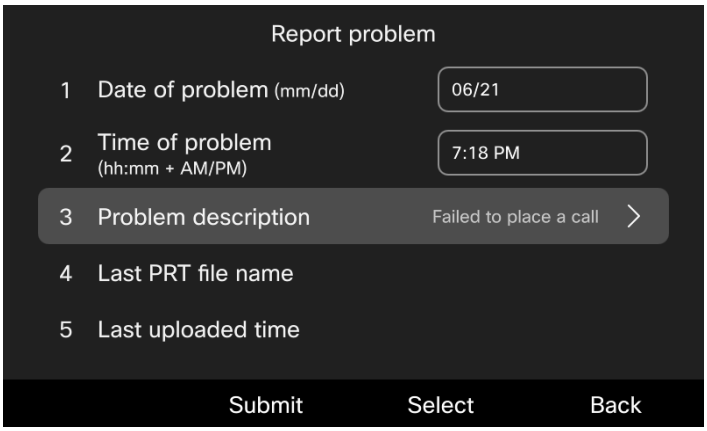
- CA サーバに登録するために、PKI トラストポイントおよび PKI サーバを設定します。

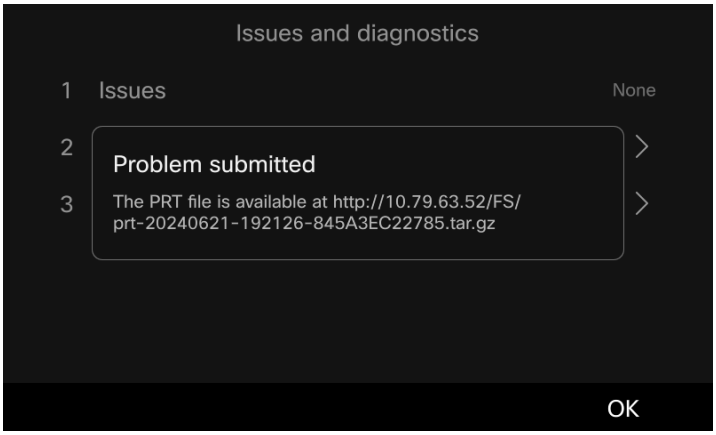
ISR_RA# configure terminal
ISR_RA(config)#crypto pki トラストポイント MSCA
ISR_RA(ca-trustpoint)# 登録モード ra
ISR_RA(ca-trustpoint)# 登録 url http://10.81.116.249/certsrv/mscep/mscep.dll
ISR_RA(ca-trustpoint)# シリアル番号
ISR_RA(ca-trustpoint)#指紋 81512B4316429092925C6891701B374EBD254447
ISR_RA(ca-trustpoint)# 失効確認なし
ISR_RA(ca-trustpoint)# rsakeypair MSCA_Key 2048
ISR_RA(ca-trustpoint)# 終了
ISR_RA(config)# crypto pki server MSCA
ISR_RA(cs-server)# grant auto trustpointMIC_trustpoint
ISR_RA(cs-server)# ハッシュ sha1
ISR_RA(cs-server)# mode ra transparent
ISR_RA(cs-server)# no shutdown

トラブルシューティング

問題レポート ツール

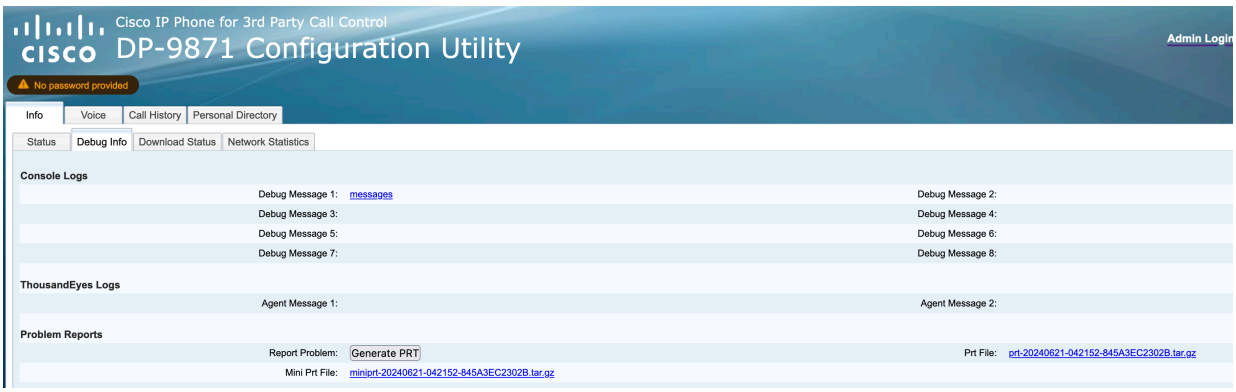
問題レポートは、電話の [設定] メニューにある問題レポート ツールから作成できます。**[設定（Settings）]** > **[問題と診断（Issues and diagnostics）]** > **[問題を報告（Report problem）]** の順に選択し、情報を入力したら、**[送信（Submit）]** を押して、問題レポートを生成します。

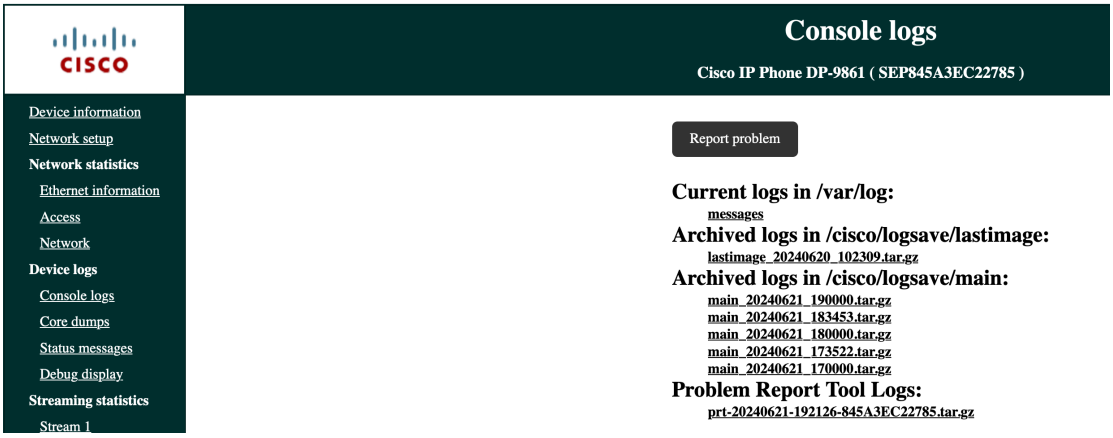




日時および問題の説明を指定します。

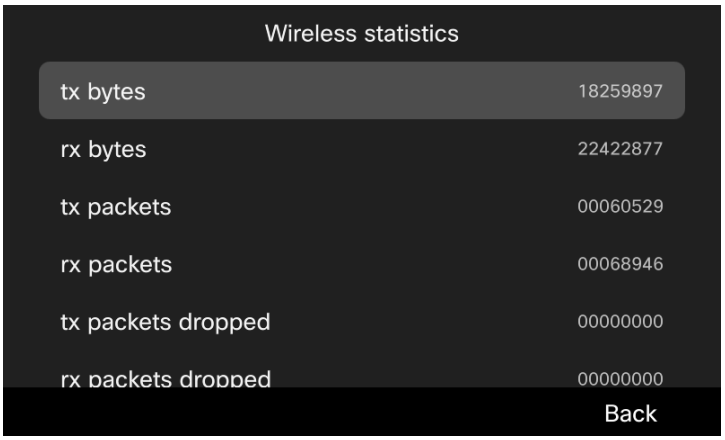
Cisco Unified Communications Manager または Broadwork のカスタマー サポートのアップロード URL オプションは、電話機ごとに設定して、ログを自動的に取得するか、電話機のウェブページからログを手動でダウンロードできます。





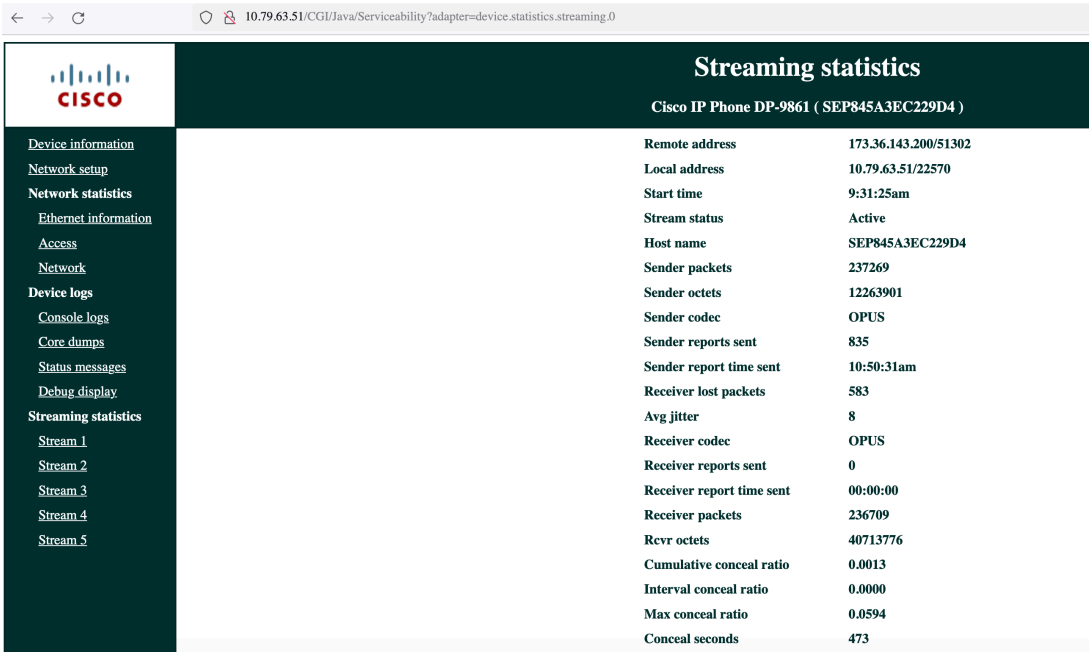
Wi-Fi 統計

[設定（Settings）] > [問題と診断（Issues and diagnostics）] > [診断（Diagnostics）] > [デバイス状態（Device status）] > [ワイヤレス統計（Wireless statistics）] の順に選択します。



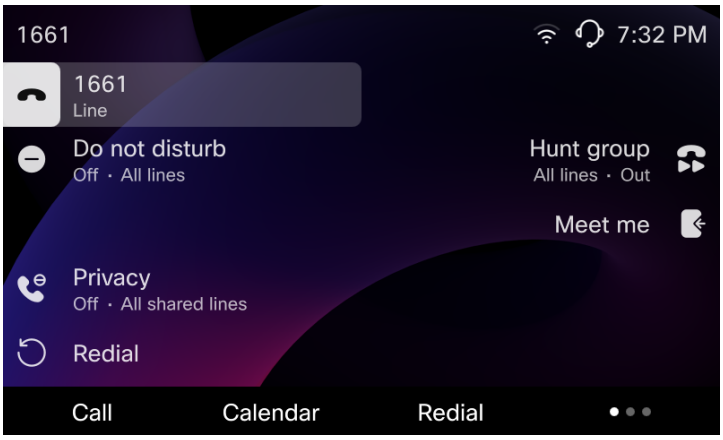
ストリーミング統計の表示

Cisco Desk Phone 9800 シリーズは、コール統計情報を提供します。コーデック タイプ、ジッター、パケットカウント情報などが表示されます。
ウェブブラウザで電話の IP アドレスにアクセスし、ストリーミングの統計を表示します。



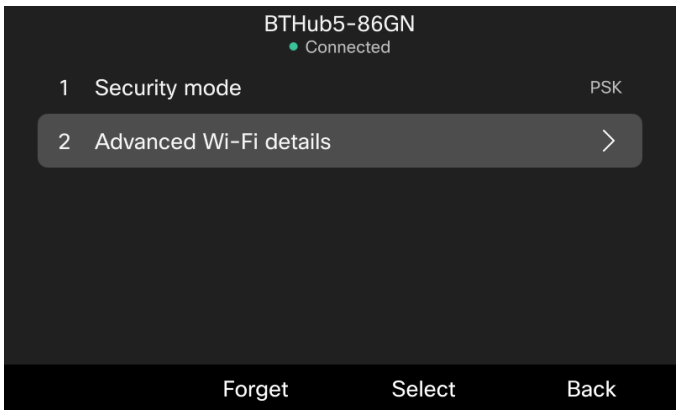
Wi-Fi 信号インジケータ

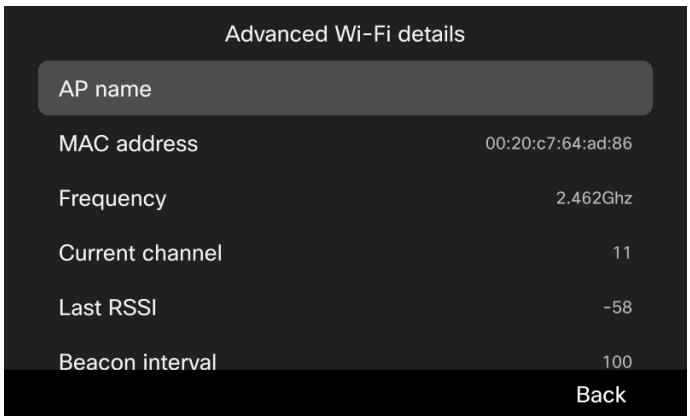
電話のホーム画面で、AP に接続されている場合、Wi-Fi 信号は右上隅に表示されます。



接続されたアクセスポイントに関する情報を表示する

[設定（Settings）] > **[NW接続（Network connection）]** > **[Wi-Fi]** の順に選択し、接続済み AP を選択したら、**[Wi-Fiの詳細情報（Advanced Wi-Fi details）]** を選択します。





メモ: Wi-Fi の問題が発生した場合は、接続された AP ステータス、AP パラメータ、電話側の信号強度、および電話 Wi-Fi 統計を確認してください。 構成が正しく、目的の AP が正常な場合、電話メニューから Wi-Fi をオフにしてからオンに切り替えると、Wi-Fi 接続が回復する可能性があります。 これで機能しない場合は、有線ケーブルを接続し、電話メニューで PRT を生成します。

電話ディスプレイのスクリーンショットを撮る

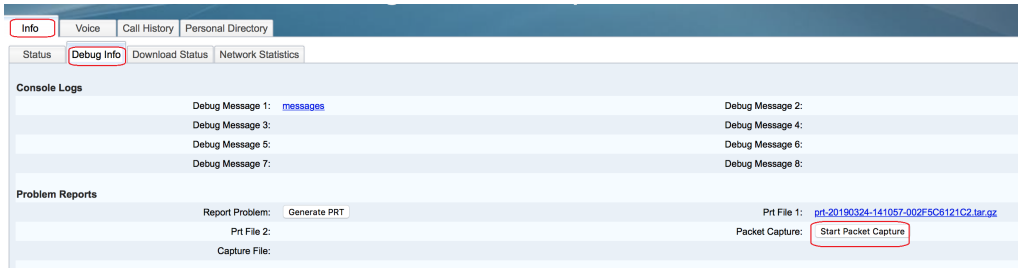
Webex Calling または BroadWorks に登録されている電話の場合は、電話の IP アドレスを取得し、ウェブブラウザで http://<phone_IP_address>/admin/screendump.bmp にアクセスします。 たとえば、http://192.168.16.43/admin/screendump.bmp です。 プロンプトが表示されたら、admin のパスワードを入力します。

Cisco Unified Communications Manager に登録されている電話の場合、電話の IP アドレスを取得し、http://<phone_IP_address>/CGI/Screenshot にアクセスします。 例: http192.168.32.124/CGI/Screenshot。プロンプトが表示されたら、Cisco Unified Communications Manager 内で電話が関連付けられているアカウントのユーザー名とパスワードを入力します。

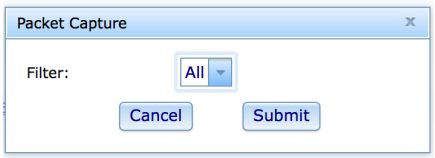
パケットのキャプチャ

Webex Calling または BroadWorks に登録されている電話の場合、ウェブブラウザで http://<phone_IP_address>/admin にアクセスすると、パケットをキャプチャできます。

1. **[情報（Info）]** > **[デバッグ情報（Debug Info）]** の順に選択し、**[パケットキャプチャを開始（Start Packet Capture）]** をクリックします。



2. プロンプトで **送信** をクリックします。



3. 処理が完了したら、[**パケットキャプチャの停止**] をクリックしてキャプチャを停止します。

キャプチャされたファイルをダウンロードできます。

その他の資料

Cisco Desk Phone 9800 シリーズ データシート: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/desk-phone-9800-series-ds.html

Cisco Desk Phone 9800 シリーズのユーザおよび管理者向け資料: https://cisco.com/go/dp9800help

その他の参照ドキュメント

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

http://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/116167-technote-scep-00.html

http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/certificates/CertsGuide_cgr1000.html#wp1000815

http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html#anc14

https://technet.microsoft.com/en-us/library/cc731183.aspx

https://technet.microsoft.com/en-us/library/cc772192.aspx

https://technet.microsoft.com/en-us/library/hh831498.aspx

https://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx#BKMK_BS2

http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book/sec-cfg-auth-rev-cert.html#GUID-4A2D2A66-F6FB-4FD1-AD40-B7D73531468E

http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfrad.html#wp1001000