

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。シスコの桌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スペ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	8
モデル	8
要件	9
サイト要件	9
コール制御	10
ワイヤレス LAN	10
アクセスポイント	11
アンテナシステム	11
プロトコル (Protocols)	12
Wi-Fi	12
5 GHz の仕様	12
2.4 GHz の仕様	14
規制	15
Bluetooth®	16
Bluetooth プロファイル (Bluetooth Profiles)	16
共存 (802.11b/g/n + Bluetooth)	16
端末のケア	17
ワイヤレス LAN の設計	18
802.11 ネットワーク	18
5 GHz (802.11a/n/ac)	18
動的周波数選択 (DFS)	18
2.4 GHz (802.11b/g/n)	19
信号強度とカバレッジ	20
データ レート	21
厳しい環境	21
マルチパス	22
セキュリティ	23
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)	24
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)	25
保護された拡張認証プロトコル (PEAP)	25
Quality of Service (QoS)	25
コール アドミッション制御 (CAC)	26
有線 QoS	26

ローミング.....	27
高速セキュア ローミング (FSR).....	27
帯域間ローミング.....	28
電源管理.....	28
配信トラフィックインジケータメッセージ (DTIM).....	29
通話容量.....	29
マルチキャスト.....	29
Cisco ワイヤレス LAN を設定する.....	31
<i>Cisco AireOS</i> ワイヤレス LAN コントローラおよび <i>Lightweight</i> アクセスポイント.....	31
802.11 ネットワーク設定.....	32
自動 RF (RRM).....	33
クライアントのローミング.....	35
EDCA パラメータ.....	35
DFS (802.11h).....	36
高スループット (802.11n/ac).....	36
フレーム集約.....	37
クリーンエア.....	39
Rx Sop Threshold.....	41
[IVR設定(WLAN Settings)].....	41
AP グループ.....	47
コントローラの設定.....	48
コール アドミッション制御 (CAC).....	50
RF プロファイル.....	52
FlexConnect グループ.....	54
マルチキャストダイレクト.....	55
QoS プロファイル.....	56
詳細設定.....	59
高度な EAP 設定.....	59
自己免疫.....	60
不正ポリシー.....	61
<i>Cisco Catalyst IOS XE</i> ワイヤレス LAN コントローラおよび <i>Lightweight</i> アクセスポイント.....	61
802.11 ネットワーク設定.....	62
高スループット (802.11n/ac).....	64
パラメータ.....	65
RRM.....	66
クリーンエア.....	68
[IVR設定(WLAN Settings)].....	69

ポリシープロファイル.....	72
RF プロファイル.....	75
Flex プロファイル.....	78
タグ.....	79
コントローラの設定.....	82
モビリティ設定.....	82
コール アドミッション制御 (CAC).....	84
マルチキャスト.....	84
詳細設定.....	86
EAP の詳細設定.....	86
Rx Sop Threshold.....	86
不正ポリシー.....	87
<i>Cisco Mobility Express および Lightweight アクセス ポイント.....</i>	<i>87</i>
コントローラの設定.....	87
802.11 ネットワーク設定.....	88
RF 最適化.....	89
[IVR設定(WLAN Settings)].....	91
AP グループ.....	96
RF プロファイル.....	98
マルチキャストダイレクト.....	99
<i>Cisco Autonomous (自律) アクセス ポイント.....</i>	<i>101</i>
802.11 ネットワーク設定.....	101
[IVR設定(WLAN Settings)].....	105
ワイヤレス ドメイン サービス (WDS).....	109
コール アドミッション制御 (CAC).....	114
QoS ポリシー.....	114
電源管理.....	116
<i>Cisco Meraki アクセス ポイント.....</i>	<i>117</i>
ワイヤレスネットワークの作成.....	117
SSID の設定.....	119
無線設定.....	123
ファイアウォールとトラフィック シェーピング.....	125
Cisco 通話制御を設定する.....	127
<i>Cisco Webex Calling.....</i>	<i>127</i>
個人使用.....	127
ワークスペース利用.....	127
Wi-Fi 機能.....	128

<i>Cisco Unified Communications Manager</i>	129
デバイスの有効化	129
共通設定	130
QoS パラメータ	130
ワイヤレス LAN プロファイル	130
ワイヤレス LAN プロファイルの作成	131
ワイヤレス LAN プロファイル グループの作成	135
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	136
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。	137
Cisco Desk Phone 9800 シリーズの設定	138
<i>自動プロビジョニング</i>	138
<i>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</i>	138
<i>電話 UI での Wi-Fi 設定の構成</i>	140
非公開のワイヤレスネットワークに参加する	142
接続済みネットワークの削除	142
<i>証明書</i> の管理	143
手動インストール	143
Manufacturing Installed Certificate (MIC)	144
User Installed 証明書	144
LSC 証明書	144
サーバ証明書	147
証明書の削除	147
シンプル証明書登録プロトコル (SCEP)	148
認証局 (CA) の設定	149
RADIUS 構成	157
SCEP RA 設定	162
トラブルシューティング	165
<i>問題レポート ツール</i>	165
<i>Wi-Fi 統計</i>	166
<i>ストリーミング統計の表示</i>	166
<i>Wi-Fi 信号インジケータ</i>	167
<i>接続されたアクセスポイントに関する情報を表示する</i>	167
<i>電話ディスプレイのスクリーンショットを撮る</i>	168
<i>パケットのキャプチャ</i>	168

その他の資料 170

 その他の参照ドキュメント 170

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 ユーザーがアクセス 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/チャンネルの概要です。

部品番号	説明	ピーク アンテナ ゲイン	周波数範囲	使用可能なチャンネル	チャンネル 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) で使用可能なチャン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ンネルが多いため、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 (チャンネルと送信電力) 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。

チャンネル使用率

チャン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

マルチパス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/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/286328117/type/282074299/release/14.0(1.14056))

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

✖️: 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 (地域による)	6 Mbps	1	OFDM-BPSK
	9 Mbps	1	OFDM-BPSK
	12 Mbps	1	OFDM-QPSK
	18 Mbps	1	OFDM-QPSK
	24 Mbps	1	OFDM-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 (地域による)	7 Mbps (MCS 0)	1	OFDM-BPSK
	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK

	29 Mbps (MCS 3)	1	OFDM-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 (地域による)	15 Mbps (MCS 0)	1	OFDM-BPSK
	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-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 (地域による)	7 Mbps (MCS 0)	1	OFDM-BPSK
	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK
	29 Mbps (MCS 3)	1	OFDM-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 (地域による)	15 Mbps (MCS 0)	1	OFDM-BPSK
	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-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 (地域による)	33 Mbps (MCS 0)	1	OFDM-BPSK
	65 Mbps (MCS 1)	1	OFDM-QPSK
	98 Mbps (MCS 2)	1	OFDM-QPSK
	130 Mbps (MCS 3)	1	OFDM-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 (地域による)	1 Mbps	1	DSSS-BPSK
	2 Mbps	1	DSSS-QPSK
	5.5 Mbps	1	DSSS-CCK
	11 Mbps	1	DSSS-CCK
2.4 GHz - 802.11g	データレート	空間ストリーム	変調
最大 Tx 電力=18 dBm (地域による)	6 Mbps	1	OFDM-BPSK
	9 Mbps	1	OFDM-BPSK
	12 Mbps	1	OFDM-QPSK

	18 Mbps	1	OFDM-QPSK
	24 Mbps	1	OFDM-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 (地域による)	7 Mbps	1	OFDM-BPSK
	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ダプタイズされたチャン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ン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 チャン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 チャンネル) を利用するために 802.11h に準拠している必要があります。802.11h 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、これらのチャンネルのアクティブ スキャンを行う前に、まず DFS チャン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、プッシュトゥートーク (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ン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ンネルを割り当ててではなく、チャン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、チャンネルを静的に割り当てる必要がある場合があります。

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 で動作するチャンネルに必要で、25 個の可能なチャンネルのうち 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、隣接するチャンネルと少なくとも 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認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、送信機に別のチャン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ン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ンネル (狭帯域) または複数のチャンネル (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ンネルを無効にする可能性があります。

非 DFS チャン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 チャンネル (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ンネルをスキャンするときに、チャンネルが使用可能な状態を維持できます。

UNII-3 チャンネル (5.745 - 5.825 GHz) は、可能な場合はオプションで使用できます。

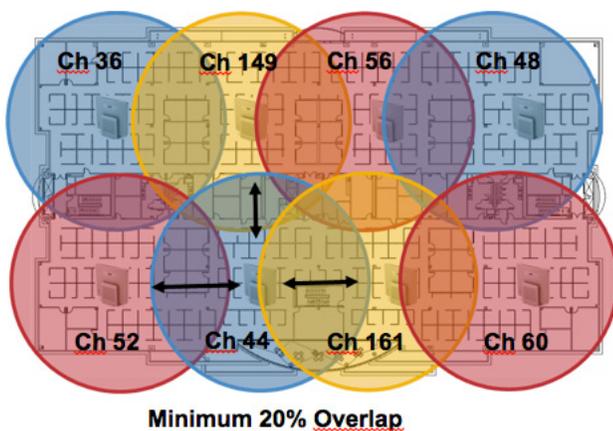
5 GHz では、25 チャンネルが南北アメリカ、16 チャンネルがヨーロッパ、19 チャンネルが日本で利用できます。

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 チャンネルセットを利用することが推奨されます。

UNII-2 拡張チャンネル (チャンネル 100 - 144) の使用を計画している場合、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 チャン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ンネルをアクセスポイントに指定するのではなく、自動チャン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、チャンネルを静的に割り当てる必要があります。

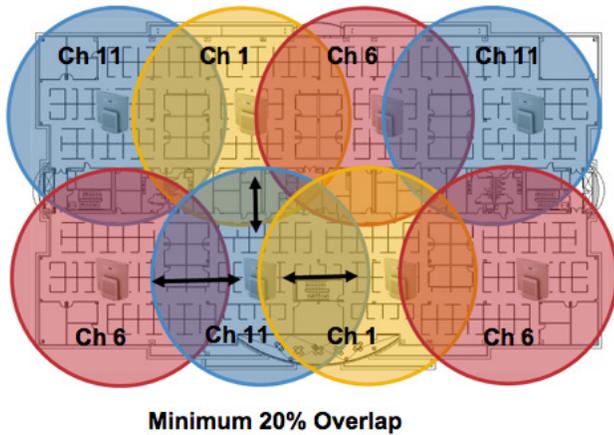
2.4 GHz (802.11b/g/n) 環境では、VoWLAN を展開するときに、非重複チャンネルのみを利用する必要があります。非重複チャンネルには 22 MHz の間隔があり、少なくとも 5 チャンネル離れています。

2.4 GHz の周波数範囲で重複しないチャンネルは 3 つだけです (チャンネル 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、非重複チャンネルを使用し、隣接するチャンネルと少なくとも 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ン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ンネルに少なくとも 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、単一チャン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ンネル 11
に影響を与える可能性があります。一部のマイクロ波は 2.4 GHz 周波数範囲全体 (チャンネル 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 UNI 1-3 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 チャンネル セットについては、8 または 12 チャンネル 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せられると、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징 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징 RADIUS サーバがセカンダリ EAP-FAST サーバとしてセットアップされる必要があります。コンポーネントが製品のプライマリ EAP-FAST サーバから複製されます。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 (Call 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 チャンネルをスキャンし、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イ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
- [チャンネルアナウンス (Channel Announcement)] と [チャン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 帯のみでを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。

The screenshot shows the Cisco Wireless configuration interface for 802.11a Global Parameters. The left sidebar contains a navigation menu with options like Access Points, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, and 802.11a/n/ac/ax. The main content area is divided into three sections: General, 802.11a Band Status, and Data Rates. The General section includes settings for 802.11a Network Status (Enabled), Beacon Period (100), Fragmentation Threshold (2346), DTPC Support (Enabled), Maximum Allowed Clients (100), RSSI Low Check (Disabled), and RSSI Threshold (-80). The 802.11a Band Status section shows Low, Mid, and High Band all set to Enabled. The Data Rates section shows a list of rates from 6 Mbps to 54 Mbps, with 6 Mbps and 9 Mbps set to Disabled, 12 Mbps set to Mandatory, and 18 Mbps through 54 Mbps set to Supported. There are also sections for CCX Location Measurement (Mode Enabled, Interval 60) and TWT Configuration (Target Waketime and Broadcast TWT Support both Enabled).

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、ロングプリアンプ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、[ショートプリアンプル (Short Preamble)] を [有効 (Enabled)] にします。ロングプリアンプルの代わりにショートプリアンプ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。

The screenshot shows the Cisco Wireless LAN Controller configuration interface for 802.11b/g Global Parameters. The left sidebar lists various configuration categories, with 802.11b/g/n/ax selected. The main content area is divided into three sections: General, Data Rates, and TWT Configuration.

Parameter	Value
802.11b/g Network Status	Enabled
802.11g Support	Enabled
Beacon Period (milliseconds)	100
Short Preamble	Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support	Enabled
Maximum Allowed Clients	100
RSSI Low Check	Enabled
RSSI Threshold (-60 to -90 dBm)	-80

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

TWT Configuration	Status
Target Waketime	Enabled
Broadcast TWT Support	Enabled

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、チャン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。

The screenshot shows the Cisco Wireless LAN Controller configuration interface for 802.11a RRM Tx Power Control (TPC). The left sidebar lists various configuration categories, with 802.11a/n/ac/ax selected. The main content area is divided into two sections: TPC Version and Tx Power Level Assignment Algorithm.

TPC Version

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

Tx Power Level Assignment Algorithm

Power Level Assignment Method	Automatic	Every 600 sec:
	On Demand	Invoke Power Update Once
	Fixed	1
Maximum Power Level Assignment (-10 to 30 dBm)	17	
Minimum Power Level Assignment (-10 to 30 dBm)	11	
Power Assignment Leader	RTP9-32A-WLC3 (10.81.6.70)	
Last Power Level Assignment	463 secs ago	
Power Threshold (-80 to -50 dBm)	-65	
Channel Aware	<input type="checkbox"/> Enabled	
Power Neighbor Count	3	

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 チャンネル幅は、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ンネル幅を使用することを推奨します。

The screenshot shows the Cisco Wireless LAN Controller configuration interface for 802.11a Dynamic Channel Assignment (DCA). The left sidebar shows the navigation menu with '802.11a/n/ac/ax' selected. The main content area is titled '802.11a > RRM > Dynamic Channel Assignment (DCA)'. Under 'Dynamic Channel Assignment Algorithm', the 'Channel Assignment Method' is set to 'Automatic' with an interval of '10 minutes' and 'AnchorTime' of '0'. Other options like 'Freeze' and 'OFF' are unselected. Several interference avoidance options are checked: 'Avoid Foreign AP interference', 'Avoid non-802.11a noise', and 'Avoid Persistent Non-WiFi Interference'. The 'Channel Assignment Leader' is 'RTP9-32A-WLC3 (10.81.6.70)' and the 'Last Auto Channel Assignment' was '556 secs ago'. The 'DCA Channel Sensitivity' is 'Medium (15 dB)'. The 'Channel Width' is set to '40 MHz'. The 'DCA Channel List' shows a list of channels: '36, 40, 44, 48, 52, 56, 60, 64, 100, 153, 157, 161'.

2.4 GHz を使用する場合、チャンネル 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 で利用できるチャン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 チャンネルを 20 MHz として設定することを推奨します。

The screenshot shows the Cisco Wireless LAN Controller configuration interface for 802.11b Dynamic Channel Assignment (DCA). The left sidebar shows the navigation menu with '802.11b/g/n/ax' selected. The main content area is titled '802.11b > RRM > Dynamic Channel Assignment (DCA)'. Under 'Dynamic Channel Assignment Algorithm', the 'Channel Assignment Method' is set to 'Automatic' with an interval of '10 minutes' and 'AnchorTime' of '0'. Other options like 'Freeze' and 'OFF' are unselected. Several interference avoidance options are checked: 'Avoid Foreign AP interference', 'Avoid non-802.11b noise', and 'Avoid Persistent Non-WiFi Interference'. The 'Channel Assignment Leader' is 'RTP9-32A-WLC3 (10.81.6.70)' and the 'Last Auto Channel Assignment' was '75 secs ago'. The 'DCA Channel Sensitivity' is 'Medium (10 dB)'. The 'DCA Channel List' shows a list of channels: '1, 6, 11'.

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ン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 チャンネル幅は、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、チャンネル 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ンネル幅を使用することを推奨します。

The screenshot displays the Cisco configuration page for an 802.11a/n/ac/ax Cisco AP. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled '802.11a/n/ac/ax Cisco APs > Configure'. The configuration is organized into several sections:

- General:** AP Name (rtp9-31a-ap1), Admin Status (Enable), Operational Status (UP), Slot # (1).
- 11n Parameters:** 11n Supported (Yes).
- CleanAir:** CleanAir Capable (Yes), CleanAir Admin Status (Enable), Number of Spectrum Expert connections (0). A note states: '* CleanAir enable will take effect only if it is enabled on this band.'
- Antenna Parameters:** Antenna Type (Internal), Antenna (A, B, C, D) with checkboxes for A, B, and C.
- RF Channel Assignment:** Current Channel (48,44), Channel Width (40 MHz), Assignment Method (Global).
- Radar Information:** Channel and Last Heard (Secs) section with a note: 'No radar detected channels'.
- Tx Power Level Assignment:** Current Tx Power Level (1), Assignment Method (Global).
- Performance Profile:** View and edit Performance Profile for this AP, with a 'Performance Profile' button.

A note at the bottom states: 'Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.'

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。

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the configuration tree with 'Wireless' expanded to 'Access Points' > 'Radios' > 'Global Configuration'. The main content area is titled 'General' and shows the 'EDCA Profile' dropdown menu set to 'Voice & Video Optimized'. Below it, the 'Enable Low Latency MAC' checkbox is unchecked. A note at the bottom states: 'Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled.'

DFS (802.11h)

[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。

[チャンネルアナウンス (Channel Announcement)] と [チャンネルサイレントモード (Channel Quiet Mode)] は [有効 (Enabled)] に設定します。

The screenshot shows the Cisco Wireless configuration interface for '802.11h Global Parameters'. The top navigation bar is the same as the previous screenshot. The left sidebar shows the configuration tree with 'Wireless' expanded to 'Access Points' > 'Radios' > 'Global Configuration'. The main content area is titled '802.11h Global Parameters' and is divided into three sections: 'Power Constraint', 'Channel Switch Announcement', and 'Radar Blacklist'. In the 'Power Constraint' section, 'Local Power Constraint(0-30)' is set to 0 dB. In the 'Channel Switch Announcement' section, 'Channel Announcement' and 'Channel Quiet Mode' are checked, and 'Channel Switch Count' is set to 0. In the 'Radar Blacklist' section, 'Smart DFS' is checked.

高スループット (802.11n/ac)

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

802.11ac データ レートは 5 GHz にのみ適用されます。

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ー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。

The screenshot displays the Cisco Wireless configuration interface for 802.11n/ac/ax (5 GHz) Throughput. The main content area is divided into several sections:

- General:** 11n Mode, 11ac Mode, and 11ax Mode are all enabled.
- VHT MCS Rates:** SS1, SS2, SS3, SS4, and SS5 are configured with 0-8 and 0-9 rates, all enabled.
- HE MCS Rates:** SS1, SS2, SS3, SS4, SS5, and SS6 are configured with 0-7, 0-9, and 0-11 rates, all enabled.
- MCS (Data Rate) Settings:** A table showing MCS values from 0 to 31, with their corresponding data rates and a 'Supported' status (all are supported).

The left sidebar shows the navigation menu with '802.11a/n/ac/ax' selected, and sub-items like 'Network', 'RRM', '802.11b/g/n/ax', 'Media Stream', 'Application Visibility And Control', 'Lync Server', 'Country', 'Timers', 'Netflow', and 'QoS'.

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 テクノロジー搭載の 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。

Wireless

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

802.11a > CleanAir

CleanAir/Spectrum Intelligence Parameters

CleanAir Enabled

Spectrum Intelligence Enabled

Report Interferers Enabled

Persistent Device Propagation Enabled

Interferences to Ignore

- Canopy
- WiMax Fixed
- SI_FHSS

Interferences to Detect

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

Trap Configurations

Enable AQI(Air Quality Index) Trap Enabled

AQI Alarm Threshold (1 to 100)

Enable trap for Unclassified Interferences Enabled

Threshold for Unclassified category trap (1 to 99)

Enable trap for Classified Interferences Enabled

Threshold for Classified category trap (1 to 99)

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

Wireless

- 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

802.11a/n/ac/ax Cisco APs > Configure

General

AP Name: rtp9-31a-ap1

Admin Status:

Operational Status: UP

Slot #: 1

11n Parameters

11n Supported: Yes

CleanAir

CleanAir Capable: Yes

CleanAir Admin Status:

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections: 0

Antenna Parameters

Antenna Type:

Antenna:

- A
- B
- C
- D

RF Channel Assignment

Current Channel: (48,44)

Channel Width:

* 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

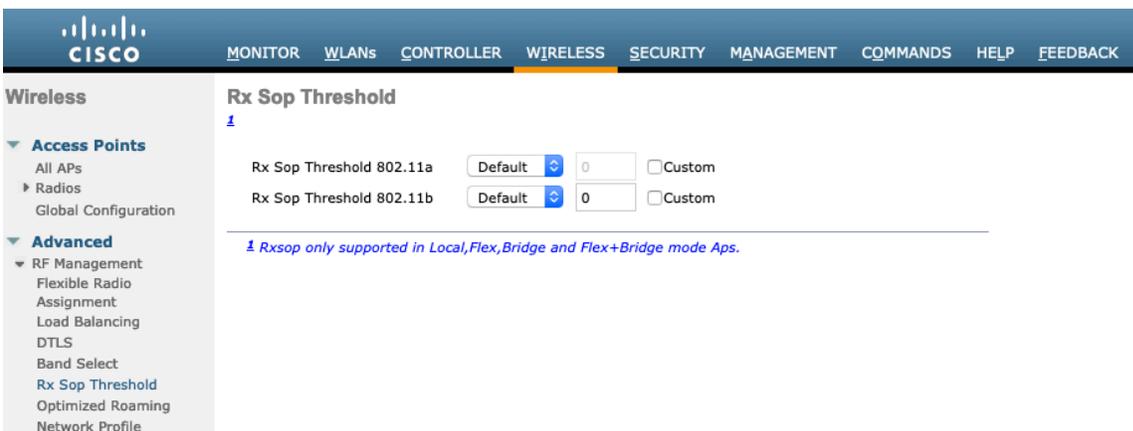
Performance Profile

View and edit Performance Profile for this AP

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。



The screenshot shows the Cisco configuration interface for the 'Rx Sop Threshold' under the 'Wireless' section. The left sidebar contains a navigation menu with 'Access Points' and 'Advanced' sections. The main content area shows two configuration rows: 'Rx Sop Threshold 802.11a' and 'Rx Sop Threshold 802.11b'. Each row has a dropdown menu set to 'Default', a text input field containing '0', and a 'Custom' checkbox which is unchecked. A note below the configuration states: 'Rx sop only supported in Local, Flex, Bridge and Flex+Bridge mode Aps.'

[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。

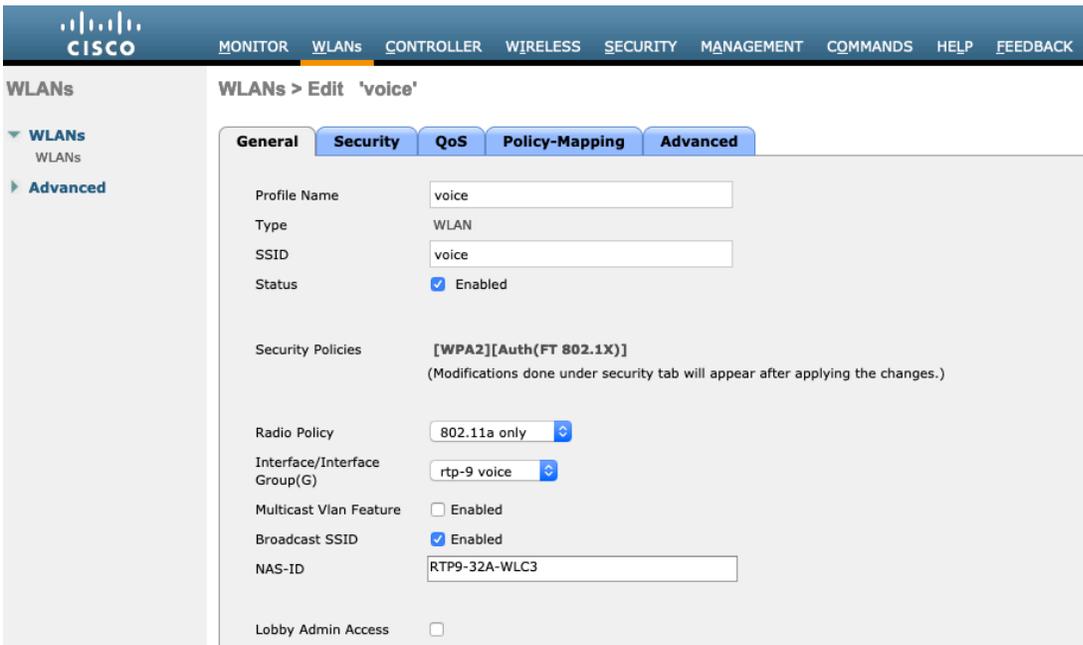
Cisco Desk Phone 9800 シリーズで使用される SSID は、特定の 802.11 無線タイプのみにも適用されるように設定できます (例、802.11a のみ)。

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。多くのチャンネルが利用でき、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。



The screenshot shows the Cisco configuration interface for 'WLANs > New'. The left sidebar has 'WLANs' and 'Advanced' sections. The main content area shows configuration fields: 'Type' is a dropdown menu set to 'WLAN', 'Profile Name' is a text input field containing 'voice', 'SSID' is a text input field containing 'voice', and 'ID' is a dropdown menu set to '6'.

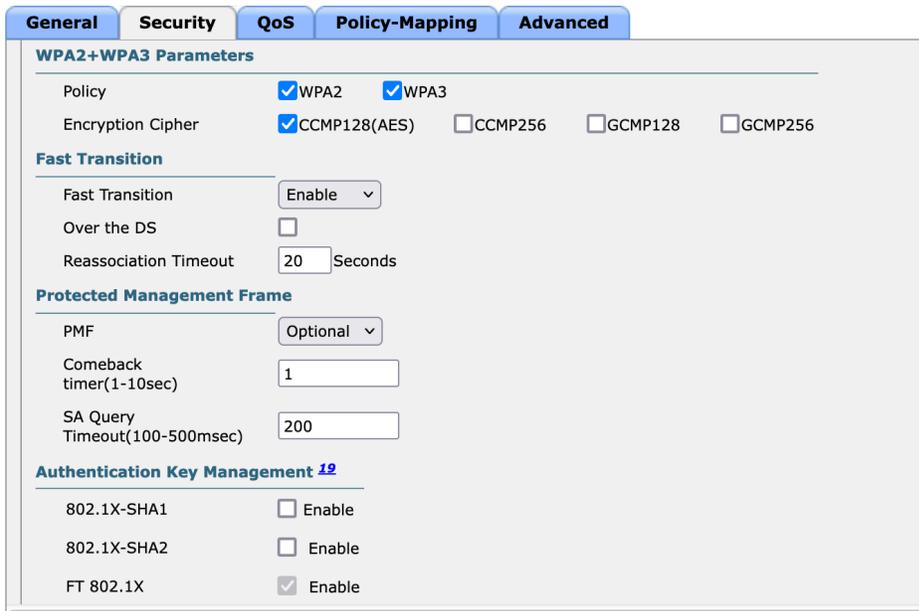


高速セキュア ローミングに 802.11r (FT) を利用するには、高速移行を有効にします。
Over the Distribution System 方法ではなく、Over the Air方法を使用するには、**[Over the DS]** チェックボックスをオフにすることが推奨されます。

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。

WLANs > Edit 'Wifi_cisco'



General	Security	QoS	Policy-Mapping	Advanced
WPA2+WPA3 Parameters				
Policy	<input type="checkbox"/> WPA2	<input checked="" type="checkbox"/> WPA3		
Encryption Cipher	<input checked="" type="checkbox"/> CCMP128(AES)	<input type="checkbox"/> CCMP256	<input type="checkbox"/> GCMP128	<input type="checkbox"/> GCMP256
Fast Transition				
Fast Transition	Enable			
Over the DS	<input type="checkbox"/>			
Reassociation Timeout	20 Seconds			
Protected Management Frame				
PMF	Required			
Comeback timer(1-10sec)	1			
SA Query Timeout(100-500msec)	200			
Authentication Key Management 19				
802.1X-SHA1	<input type="checkbox"/> Enable			
802.1X-SHA2	<input type="checkbox"/> Enable			
FT 802.1X	<input checked="" type="checkbox"/> Enable			

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。

MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK																																																																																										
WLANs																																																																																																		
WLANs > Edit 'voice'																																																																																																		
<table border="1"> <thead> <tr> <th>General</th> <th>Security</th> <th>QoS</th> <th>Policy-Mapping</th> <th>Advanced</th> </tr> </thead> <tbody> <tr> <td colspan="5">Layer 2</td> </tr> <tr> <td colspan="5">Layer 3</td> </tr> <tr> <td colspan="5">AAA Servers</td> </tr> <tr> <td colspan="5">Select AAA servers below to override use of default servers on this WLAN</td> </tr> <tr> <td colspan="5">RADIUS Servers</td> </tr> <tr> <td colspan="5">RADIUS Server Overwrite interface <input type="checkbox"/> Enabled</td> </tr> <tr> <td colspan="5">Apply Cisco ISE Default Settings <input type="checkbox"/> Enabled</td> </tr> <tr> <td colspan="2">Authentication Servers</td> <td colspan="2">Accounting Servers</td> <td>EAP Parameters</td> </tr> <tr> <td colspan="2">Enabled <input checked="" type="checkbox"/></td> <td colspan="2">Enabled <input checked="" type="checkbox"/></td> <td>Enable <input checked="" type="checkbox"/></td> </tr> <tr> <td>Server 1</td> <td>None</td> <td>None</td> <td>None</td> <td>EAPOL Key Timeout(200 to 5000 millisec) 400</td> </tr> <tr> <td>Server 2</td> <td>None</td> <td>None</td> <td>None</td> <td>EAPOL Key Retries(0 to 4) 4</td> </tr> <tr> <td>Server 3</td> <td>None</td> <td>None</td> <td>None</td> <td>Identity Request Timeout(1 to 120 sec) 30</td> </tr> <tr> <td>Server 4</td> <td>None</td> <td>None</td> <td>None</td> <td>Identity Request Retries(1 to 20) 2</td> </tr> <tr> <td>Server 5</td> <td>None</td> <td>None</td> <td>None</td> <td>Request Timeout(1 to 120 sec) 30</td> </tr> <tr> <td>Server 6</td> <td>None</td> <td>None</td> <td>None</td> <td>Request Retries(1 to 20) 2</td> </tr> <tr> <td colspan="2">Authorization ACA Server</td> <td colspan="2">Accounting ACA Server</td> <td></td> </tr> <tr> <td colspan="2"><input type="checkbox"/> Enabled</td> <td colspan="2"><input type="checkbox"/> Enabled</td> <td></td> </tr> </tbody> </table>									General	Security	QoS	Policy-Mapping	Advanced	Layer 2					Layer 3					AAA Servers					Select AAA servers below to override use of default servers on this WLAN					RADIUS Servers					RADIUS Server Overwrite interface <input type="checkbox"/> Enabled					Apply Cisco ISE Default Settings <input type="checkbox"/> Enabled					Authentication Servers		Accounting Servers		EAP Parameters	Enabled <input checked="" type="checkbox"/>		Enabled <input checked="" type="checkbox"/>		Enable <input checked="" type="checkbox"/>	Server 1	None	None	None	EAPOL Key Timeout(200 to 5000 millisec) 400	Server 2	None	None	None	EAPOL Key Retries(0 to 4) 4	Server 3	None	None	None	Identity Request Timeout(1 to 120 sec) 30	Server 4	None	None	None	Identity Request Retries(1 to 20) 2	Server 5	None	None	None	Request Timeout(1 to 120 sec) 30	Server 6	None	None	None	Request Retries(1 to 20) 2	Authorization ACA Server		Accounting ACA Server			<input type="checkbox"/> Enabled		<input type="checkbox"/> Enabled		
General	Security	QoS	Policy-Mapping	Advanced																																																																																														
Layer 2																																																																																																		
Layer 3																																																																																																		
AAA Servers																																																																																																		
Select AAA servers below to override use of default servers on this WLAN																																																																																																		
RADIUS Servers																																																																																																		
RADIUS Server Overwrite interface <input type="checkbox"/> Enabled																																																																																																		
Apply Cisco ISE Default Settings <input type="checkbox"/> Enabled																																																																																																		
Authentication Servers		Accounting Servers		EAP Parameters																																																																																														
Enabled <input checked="" type="checkbox"/>		Enabled <input checked="" type="checkbox"/>		Enable <input checked="" type="checkbox"/>																																																																																														
Server 1	None	None	None	EAPOL Key Timeout(200 to 5000 millisec) 400																																																																																														
Server 2	None	None	None	EAPOL Key Retries(0 to 4) 4																																																																																														
Server 3	None	None	None	Identity Request Timeout(1 to 120 sec) 30																																																																																														
Server 4	None	None	None	Identity Request Retries(1 to 20) 2																																																																																														
Server 5	None	None	None	Request Timeout(1 to 120 sec) 30																																																																																														
Server 6	None	None	None	Request Retries(1 to 20) 2																																																																																														
Authorization ACA Server		Accounting ACA Server																																																																																																
<input type="checkbox"/> Enabled		<input type="checkbox"/> Enabled																																																																																																

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 を使用する場合にはのみ、**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。

The screenshot shows the Cisco WLC configuration interface for the 'voice' WLAN. The 'QoS' tab is selected. The 'Quality of Service (QoS)' dropdown is set to 'Platinum (voice)'. 'Application Visibility' is checked and 'Enabled'. 'AVC Profile' is set to 'none'. 'Flex AVC Profile' is set to 'none'. 'Netflow Monitor' is set to 'none'. 'Fastlane' is set to 'Disable'. Below this, the 'Override Per-User Bandwidth Contracts (kbps)' section has a table with columns 'DownStream' and 'UpStream'. All values (Average Data Rate, Burst Data Rate, Average Real-Time Rate, Burst Real-Time Rate) are set to 0. A 'Clear' button is at the bottom.

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

The screenshot shows the Cisco WLC configuration interface for the 'voice' WLAN. The 'Policy-Mapping' tab is selected. The 'Override Per-SSID Bandwidth Contracts (kbps)' section has a table with columns 'DownStream' and 'UpStream'. All values (Average Data Rate, Burst Data Rate, Average Real-Time Rate, Burst Real-Time Rate) are set to 0. A 'Clear' button is at the bottom. Below this, the 'WMM' section has 'WMM Policy' set to 'Required', '7920 AP CAC' checked and 'Enabled', and '7920 Client CAC' unchecked. The 'Media Stream' section has 'Multicast Direct' checked and 'Enabled'. The 'Lync Policy' section has 'Audio' set to 'Silver'.

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

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 **DTIM 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。

The screenshot displays the Cisco WLAN configuration interface for the 'voice' WLAN. The 'Security' tab is selected, showing various security settings. Key settings include: Allow AAA Override (Disabled), Coverage Hole Detection (Enabled), Enable Session Timeout (86400), Aironet IE (Enabled), Diagnostic Channel (Disabled), Override Interface ACL (IPv4: None, IPv6: None), Layer2 Acl (None), URL ACL (None), P2P Blocking Action (Disabled), Client Exclusion (Disabled), Maximum Allowed Clients (0), Static IP Tunneling (Disabled), Wi-Fi Direct Clients Policy (Disabled), Maximum Allowed Clients Per AP Radio (200). On the right, the 'DHCP' section shows DHCP Server (Override) and DHCP Addr. Assignment (Required). The 'Management Frame Protection (MFP)' section shows MFP Client Protection (Optional). The 'DTIM Period (in beacon intervals)' section shows 802.11a/n (1 - 255) and 802.11b/g/n (1 - 255) both set to 2. The 'NAC' section shows NAC State (None). The 'Load Balancing and Band Select' section shows Client Load Balancing and Client Band Select both disabled.

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

WLANs > Edit 'voice'

General Security QoS Policy-Mapping **Advanced**

PER AP Radio

Clear HotSpot Configuration Enabled

Client user idle timeout(15-100000)

Client user idle threshold (0-10000000) Bytes

Radius NAI-Realm

11ac MU-MIMO

WGB PRP Enabled

MBO State

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching Enabled

Passive Client

Passive Client

Voice

Media Session Snooping Enabled

Re-anchor Roamed Voice Clients Enabled

KTS based CAC Policy Enabled

Radius Client Profiling

DHCP Profiling

HTTP Profiling

Local Client Profiling

DHCP Profiling

HTTP Profiling

PMIP

PMIP Mobility Type

PMIP NAI Type

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

WLANs > Edit 'voice'

General Security QoS Policy-Mapping **Advanced**

FlexConnect

FlexConnect Local Auth Enabled

Learn Client IP Address Enabled

Vlan based Central Switching Enabled

Central DHCP Processing Enabled

Override DNS Enabled

NAT-PAT Enabled

Central Assoc Enabled

Lync

Lync Server

11k

Neighbor List Enabled

Neighbor List Dual Band Enabled

Assisted Roaming Prediction Optimization Enabled

802.11ax BSS Configuration

Down Link MU-MIMO Enabled

PMIP Profile

PMIP Realm

Universal AP Admin Support

Universal AP Admin

11v BSS Transition Support

BSS Transition

Disassociation Imminent

Disassociation Timer(0 to 3000 TBTT)

Optimized Roaming Disassociation Timer(0 to 40 TBTT)

BSS Max Idle Service

Directed Multicast Service

Tunneling

Tunnel Profile

EOGRE Vlan Override

mDNS

mDNS Snooping Enabled

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

WLANs > Edit 'voice'

General Security QoS Policy-Mapping **Advanced**

802.11ax BSS Configuration

Down Link MU-MIMO Enabled

Up Link MU-MIMO Enabled

Down Link OFDMA Enabled

Up Link OFDMA Enabled

mDNS

mDNS Snooping Enabled

TrustSec

Security Group Tag

Umbrella

Umbrella Mode

Umbrella Profile

Umbrella DHCP Override

Fabric Configuration

Fabric Enabled

Mobility

Selective Reanchor Enabled

U3 Interface

U3 Interface Enabled

U3 Reporting Interval

AP グループ

AP グループを作成して、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。

The screenshot shows the Cisco WLC interface for adding a new AP group. The 'WLANs' sidebar is visible on the left. The main content area is titled 'AP Groups' and contains a form for 'Add New AP Group'. The form has two input fields: 'AP Group Name' with the value 'rtp' and 'Description'. Below the fields are 'Add' and 'Cancel' buttons.

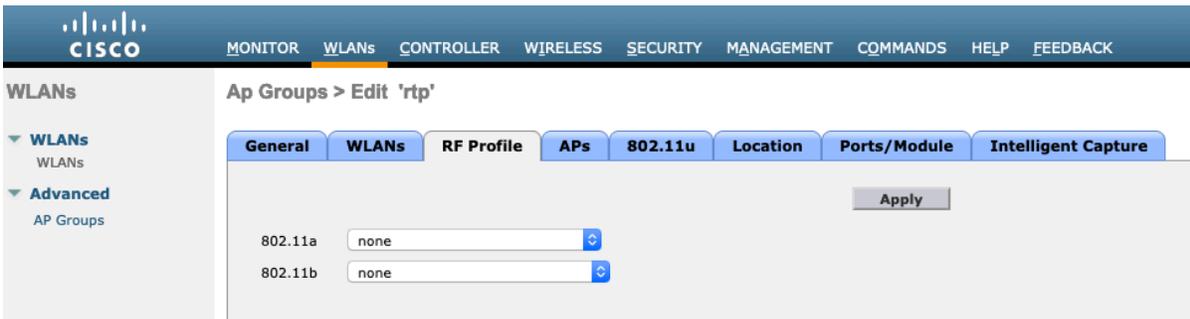
The screenshot shows the 'Edit' form for the 'rtp' AP group. The 'WLANs' sidebar is visible on the left. The main content area is titled 'Ap Groups > Edit 'rtp''. There are several tabs: 'General', 'WLANs', 'RF Profile', 'APs', '802.11u', 'Location', 'Ports/Module', and 'Intelligent Capture'. The 'General' tab is selected. The form contains various configuration options: 'AP Group Name' (rtp), 'AP Group Description', 'NAS-ID' (RTP9-32A-WLC3), 'Enable Client Traffic QinQ' (checkbox), 'Enable DHCPv4 QinQ' (checkbox), 'QinQ Service Vlan Id' (0), 'Fabric ACL Template' (None), 'CAPWAP Preferred Mode' (Not-Configured), 'Custom Web Override-Global' (checkbox), 'External Web auth URL' (none), 'NTP Auth' (checkbox), and 'NTP Server' (None). An 'Apply' button is located at the top right of the form.

[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。

The screenshot shows the 'Add New' form in the 'WLANs' tab of the 'Edit' form for the 'rtp' AP group. The 'WLANs' sidebar is visible on the left. The main content area is titled 'Ap Groups > Edit 'rtp''. The 'WLANs' tab is selected. The form contains the following fields: 'WLAN SSID' (voice(6)), 'Interface /Interface Group(G)' (rtp-9 voice), and 'SNMP NAC State' (checkbox). Below the fields are 'Add' and 'Cancel' buttons.

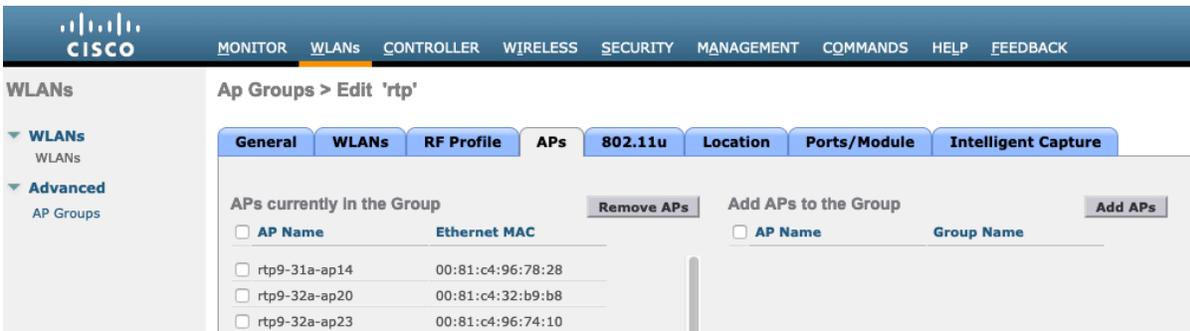
[RFプロファイル (RF Profile)] タブで、目的の 802.11a または 802.11b RF プロファイルを選択して、[適用 (Apply)] を選択します。

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。

Controller

General

Name: RTP9-32A-WLC3

802.3x Flow Control Mode: Disabled

LAG Mode on next reboot: Enabled

Broadcast Forwarding: Disabled

AP Multicast Mode: Multicast (Multicast Group Address: 239.1.1.9)

AP IPv6 Multicast Mode: Multicast (IPv6 Multicast Group Address: ff1e::239:100:100:21)

AP Fallback: Enabled

CAPWAP Preferred Mode: ipv4

Fast SSID change: Enabled

Link Local Bridging: Disabled

Default Mobility Domain Name: CTG-VoWLAN2

RF Group Name: RTP9-VoWLAN2

User Idle Timeout (seconds): 300

ARP Timeout (seconds): 300

ARP Unicast Mode: Disabled

Web Radius Authentication: PAP

Operating Environment: Commercial (10 to 35 C)

Internal Temp Alarm Limits: 10 to 38 C

WebAuth Proxy Redirection Mode: Disabled

WebAuth Proxy Redirection Port: 0

Captive Network Assistant Bypass: Disabled

Global IPv6 Config: Disabled

Web Color Theme: Default

HA SKU secondary unit: Disabled

Nas-Id: RTP9-32A-WLC3

HTTP Profiling Port: 80

DNS Server IP (IPv4/IPv6): 171.70.168.183

HTTP-Proxy Ip Address (IPv4/IPv6): 0.0.0.0

WGB Vlan Client: Disabled

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

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。

Controller

Multicast

Enable Global Multicast Mode:

Enable IGMP Snooping:

IGMP Timeout (30-7200 seconds): 60

IGMP Query Interval (15-2400 seconds): 20

Enable MLD Snooping:

MLD Timeout (30-7200 seconds): 60

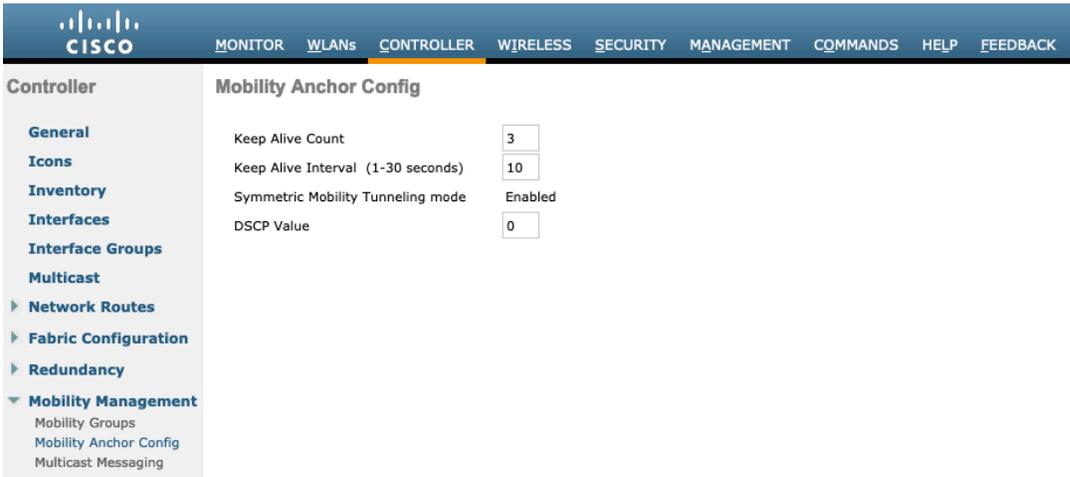
MLD Query Interval (15-2400 seconds): 20

Foot Notes

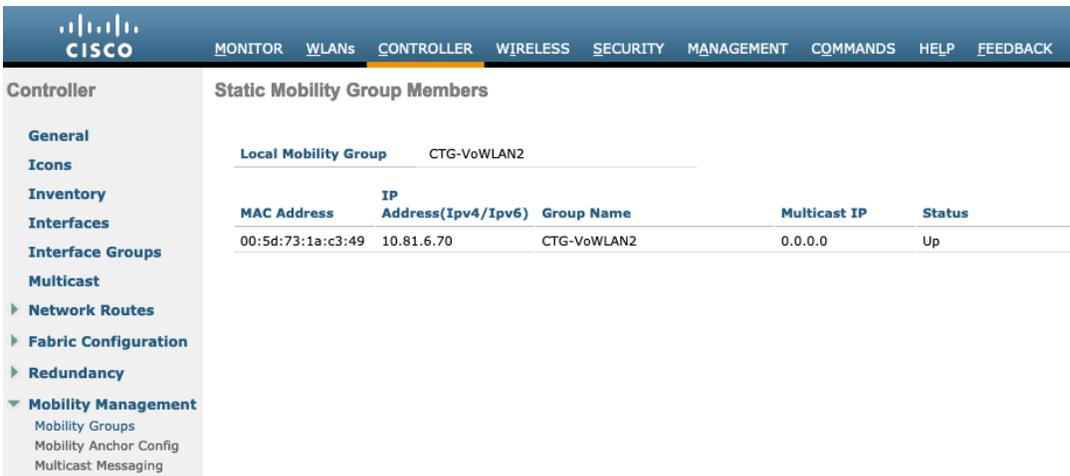
Changing Global Multicast configuration parameters removes configured Multicast VLAN from WLAN.

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。



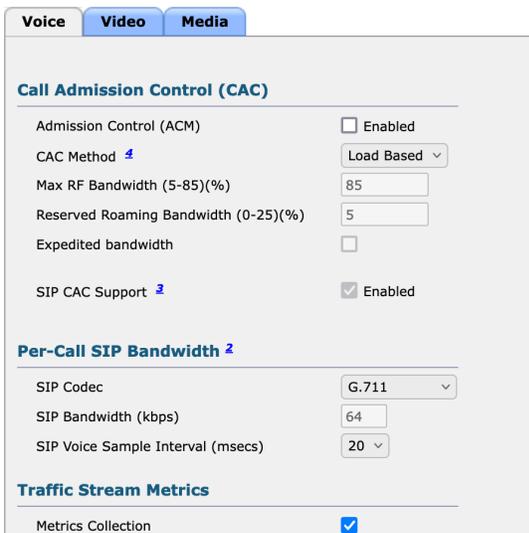
複数の Cisco Wireless LAN Controller が同じモビリティグループの一部である場合は、Cisco Wireless LAN Controller の IP アドレスと MAC アドレスを Static Mobility Group Members 構成に追加します。



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。

802.11a(5 GHz) > Media



Wireless

802.11a(5 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method

Max RF Bandwidth (5-85)(%)

Reserved Roaming Bandwidth (0-25)(%)

SIP CAC Support Enabled

Foot Notes

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

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。

Wireless

802.11a(5 GHz) > Media

General

Unicast Video Redirect

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85)(%)

Client Minimum Phy Rate

Maximum Retry Percent (0-100%)

Media Stream - Multicast Direct Parameters

Multicast Direct Enable

Max Streams per Radio

Max Streams per Client

Best Effort QoS Admission Enabled

Foot Notes

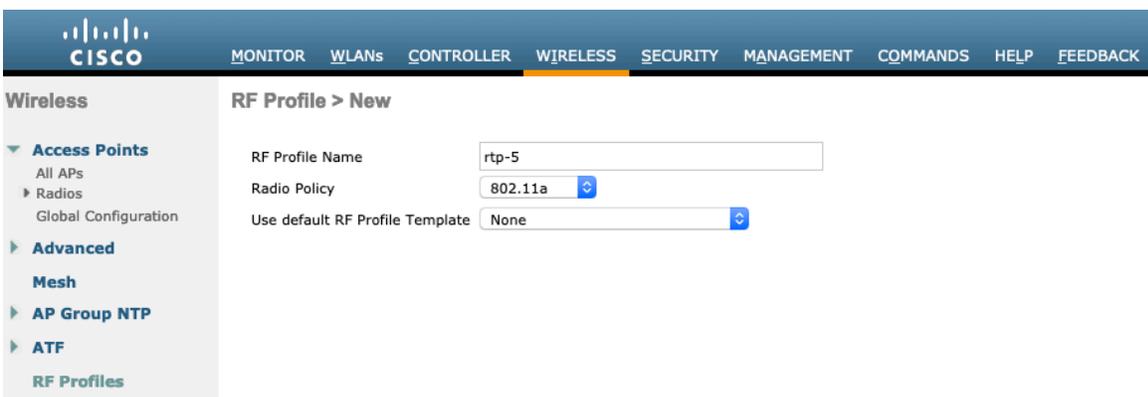
1 11a rates(Kbps): 6000,9000,12000,18000,24000,36000,48000,54000
 11n rates(Kbps): 65000,72200,130000,144400,135000,150000,270000,300000
 2 SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
 3 SIP CAC will be supported only if SIP snooping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

RF プロファイル

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。

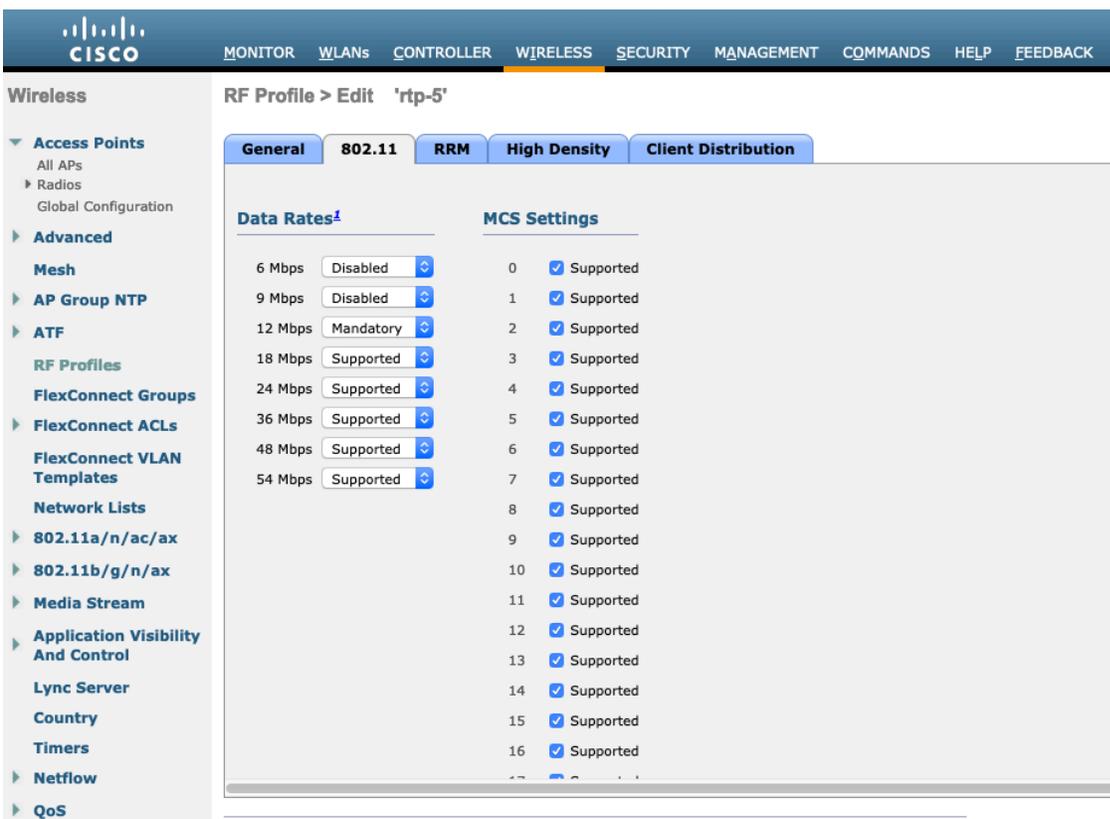
Cisco デスクフォン 9800 シリーズで使用される SSID については、5 GHz 無線にのみ適用することを推奨します。いったん作成されると、RF プロファイルは AP グループに適用されます。

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 Mbps 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。

The screenshot shows the Cisco Wireless configuration interface for an RF Profile named 'rtp-5'. The 'RRM' tab is active, and the 'High Density' sub-tab is selected. The configuration is divided into several sections:

- TPC (Transmit Power Control):**
 - Maximum Power Level Assignment (-10 to 30 dBm): 30
 - Minimum Power Level Assignment (-10 to 30 dBm): -10
 - Power Threshold v1(-80 to -50 dBm): -70
 - Power Threshold v2(-80 to -50 dBm): -67
- DCA (Dynamic Channel Allocation):**
 - Avoid Foreign AP Interference: Enabled
 - Channel Width: 20 MHz 40 MHz 80 MHz 160 MHz 80+80 MHz Best
- Coverage Hole Detection:**
 - Data RSSI(-90 to -60 dBm): -80
 - Voice RSSI(-90 to -60 dBm): -80
 - Coverage Exception(0 to 100 %): 25
 - Coverage Level(1 to 200 Clients): 3
- Profile Threshold For Traps:**
 - Interference (0 to 100%): 10
 - Clients (1 to 200): 12
 - Noise (-127 to 0 dBm): -70
 - Utilization (0 to 100 %): 80
- Client Network Preference:**
 - Connectivity Throughput Automatic
- Client Aware:**
 - Enable Disable
- High-Speed Roam:**
 - HSR mode: Enabled

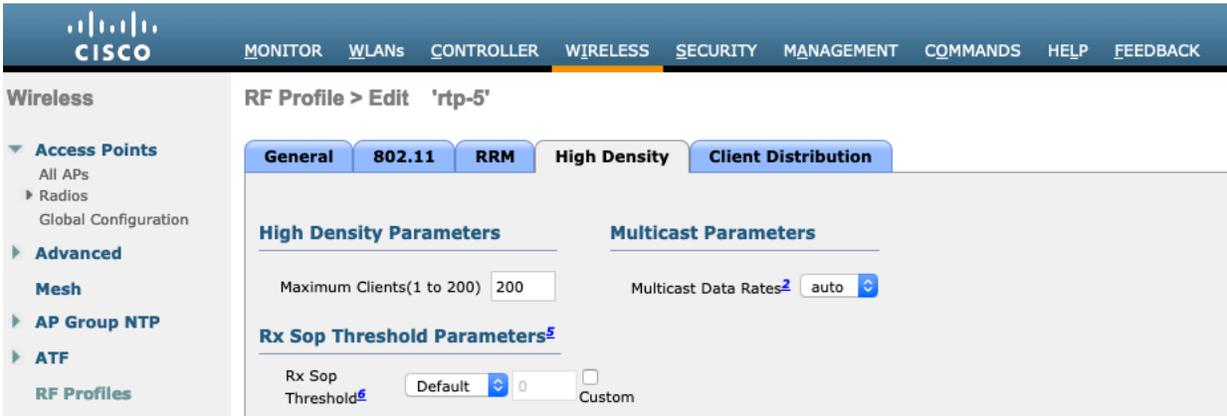
This screenshot shows the same configuration page for 'rtp-5', but with the 'Client Distribution' sub-tab selected. The 'High Density' sub-tab is also visible. The configuration includes:

- Client Aware:**
 - Enable Disable
- High-Speed Roam:**
 - HSR mode: Enabled
 - Neighbor Timeout Factor: 5
- DCA Channel List:**
 - DCA Channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
- DCA Channel Selection Table:**

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52
<input type="checkbox"/>	56
<input type="checkbox"/>	60
<input type="checkbox"/>	64
<input type="checkbox"/>	149
<input type="checkbox"/>	153
<input type="checkbox"/>	157
<input type="checkbox"/>	161
- Extended UNII-2 channels:** Enabled

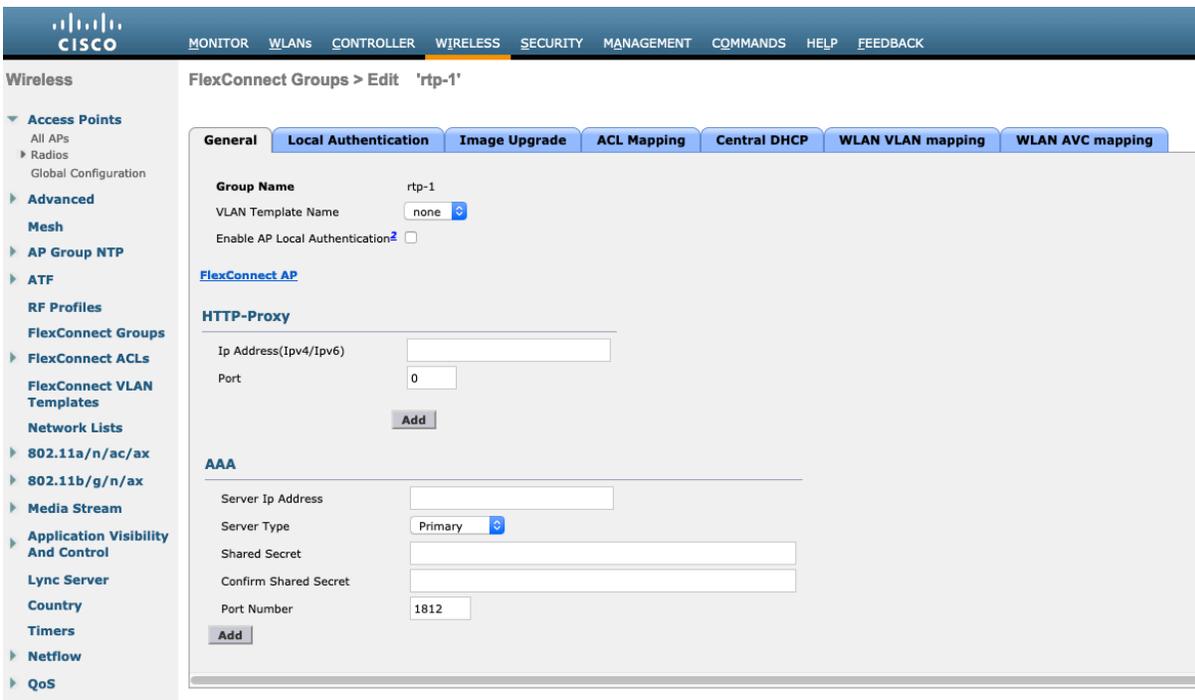
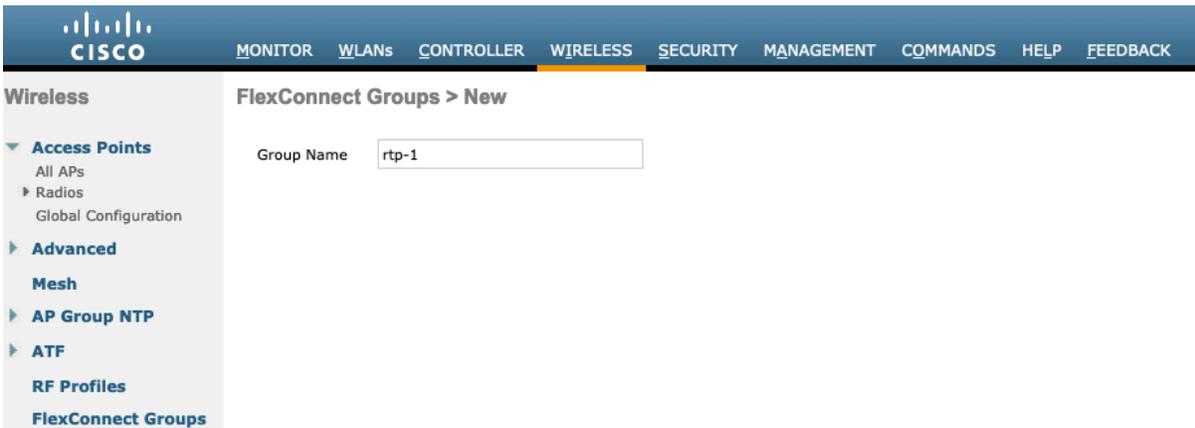
[高密度 (High Density)] タブで、[最大クライアント数 (Maximum Clients)]、[マルチキャストデータレート (Multicast Data Rates)]、[Rx Sopしきい値 (Rx Sop Threshold)] を設定できます。

[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。

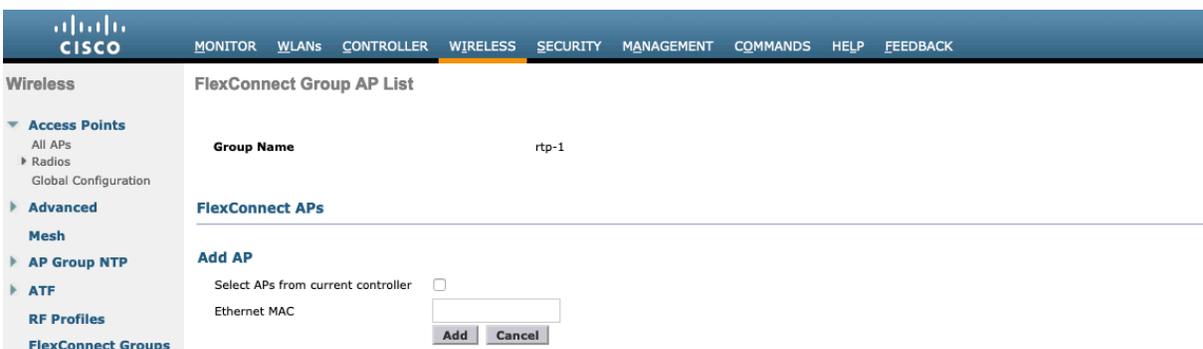


FlexConnect グループ

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。

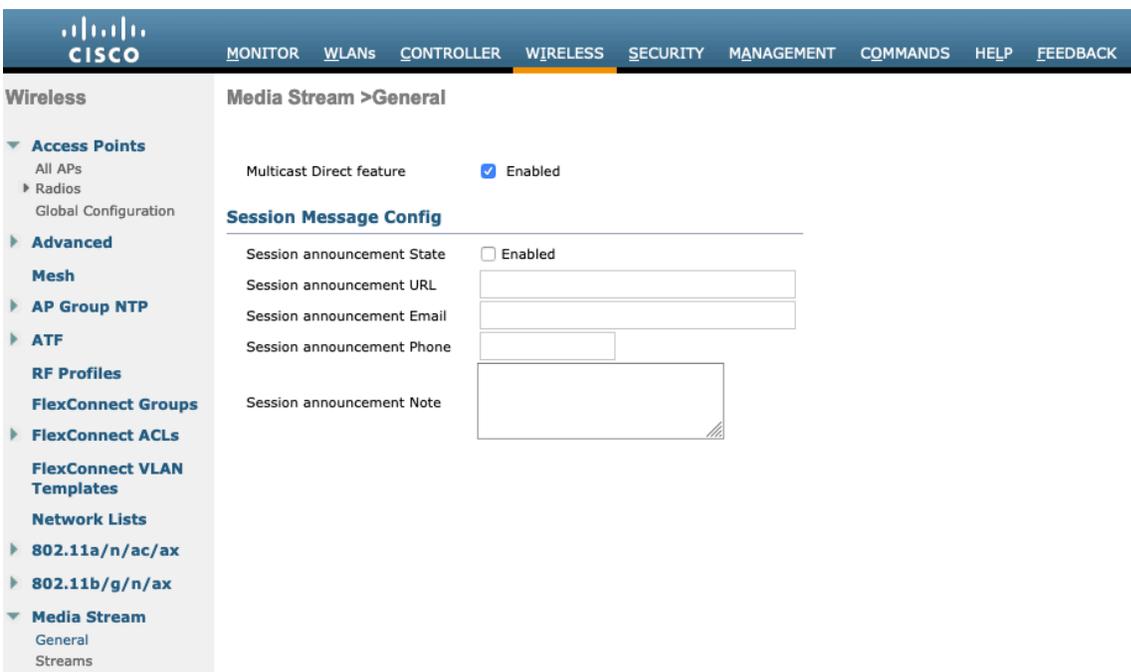


FlexConnect グループごとに許可されるアクセス ポイントの最大数には制限があり、これは WLC モデルによって異なります。



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。



Wireless

Media Streams Entries 1 - 1 of 1

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

[マルチキャストダイレクト (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。

WLANs

WLANs > Edit 'voice'

General Security **QoS** Policy-Mapping Advanced

Override Per-SSID Bandwidth Contracts (kbps) ¹⁶

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

Clear

WMM

WMM Policy

7920 AP CAC Enabled

7920 Client CAC Enabled

Media Stream

Multicast Direct Enabled

Lync Policy

Audio

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

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

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
- 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	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: voice

Unicast Default Priority: besteffort

Multicast Default Priority: besteffort

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 5

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

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
- 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	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: video

Unicast Default Priority: video

Multicast Default Priority: video

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 4

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

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

Edit QoS Profile

QoS Profile Name silver

Description For Best Effort

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: besteffort

Unicast Default Priority: besteffort

Multicast Default Priority: besteffort

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 0

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
- 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	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: background

Unicast Default Priority: background

Multicast Default Priority: background

Wired QoS Protocol

Protocol Type: 802.1p

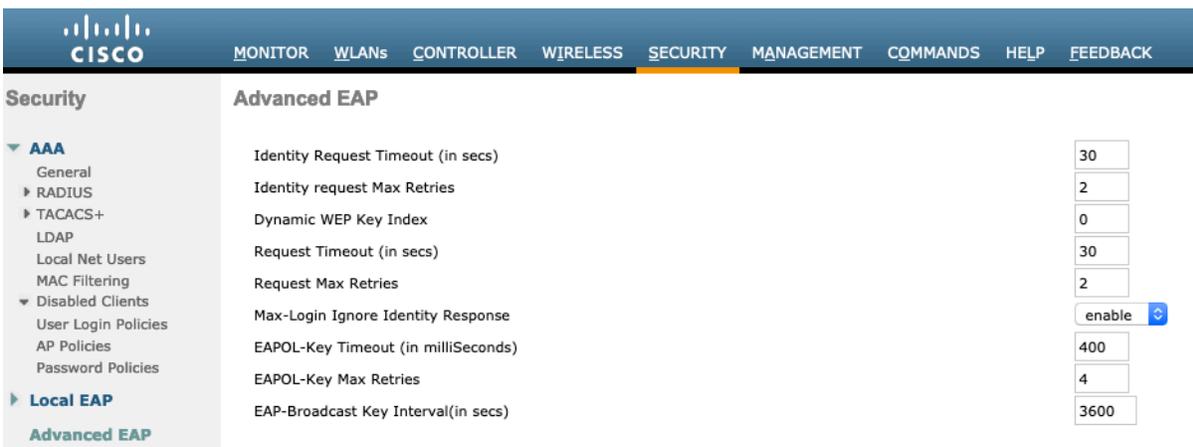
802.1p Tag: 1

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。

The screenshot displays the Cisco Catalyst IOS XE Security configuration page for Rogue Policies. The page is divided into two main sections: Rogue Policies and Auto Contain. The Rogue Policies section includes settings for Rogue Detection Security Level (set to Custom), Rogue Location Discovery Protocol (set to Disable), Expiration Timeout for Rogue AP and Rogue Client entries (set to 1200 Seconds), Validate rogue clients against AAA (set to Disabled), Validate rogue AP against AAA (set to Disabled), Polling Interval (set to 0 Seconds), Validate rogue clients against MSE (set to Disabled), Detect and report Ad-Hoc Networks (set to Enabled), Rogue Detection Report Interval (set to 10), Rogue Detection Minimum RSSI (-70 to -128) (set to -90), Rogue Detection Transient Interval (0, 120 to 1800 Sec) (set to 0), Rogue Client Threshold (0 to disable, 1 to 256) (set to 0), and Rogue containment automatic rate selection (set to Disabled). The Auto Contain section includes settings for Auto Containment Level (set to 1), Auto Containment only for Monitor mode APs (set to Disabled), Auto Containment on FlexConnect Standalone (set to Disabled), Rogue on Wire (set to Disabled), Using our SSID (set to Disabled), Valid client on Rogue AP (set to Disabled), and AdHoc Rogue AP (set to Disabled).

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
- **[チャン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

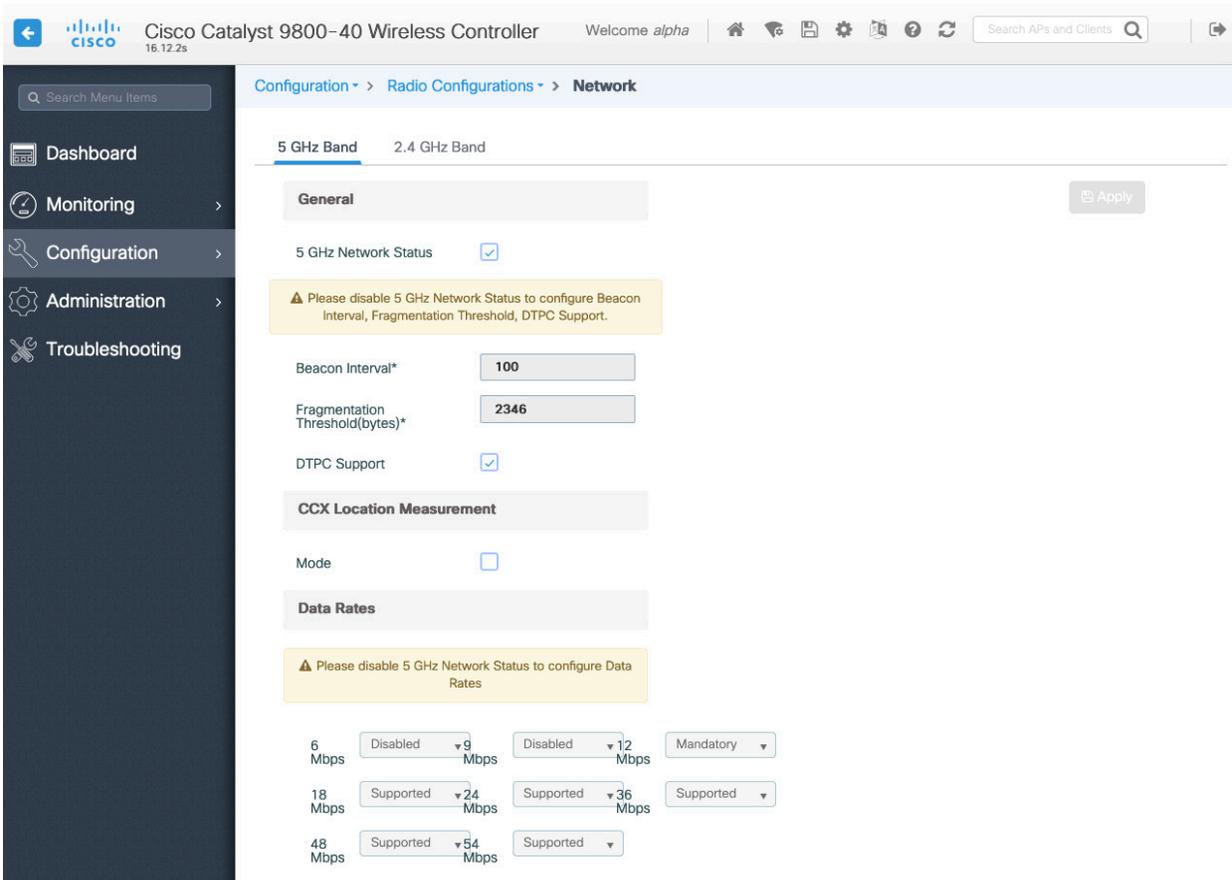
802.11 ネットワーク設定

Cisco Desk Phone 9800 シリーズは 5 GHz 帯のみでを使用することをお勧めします。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 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。



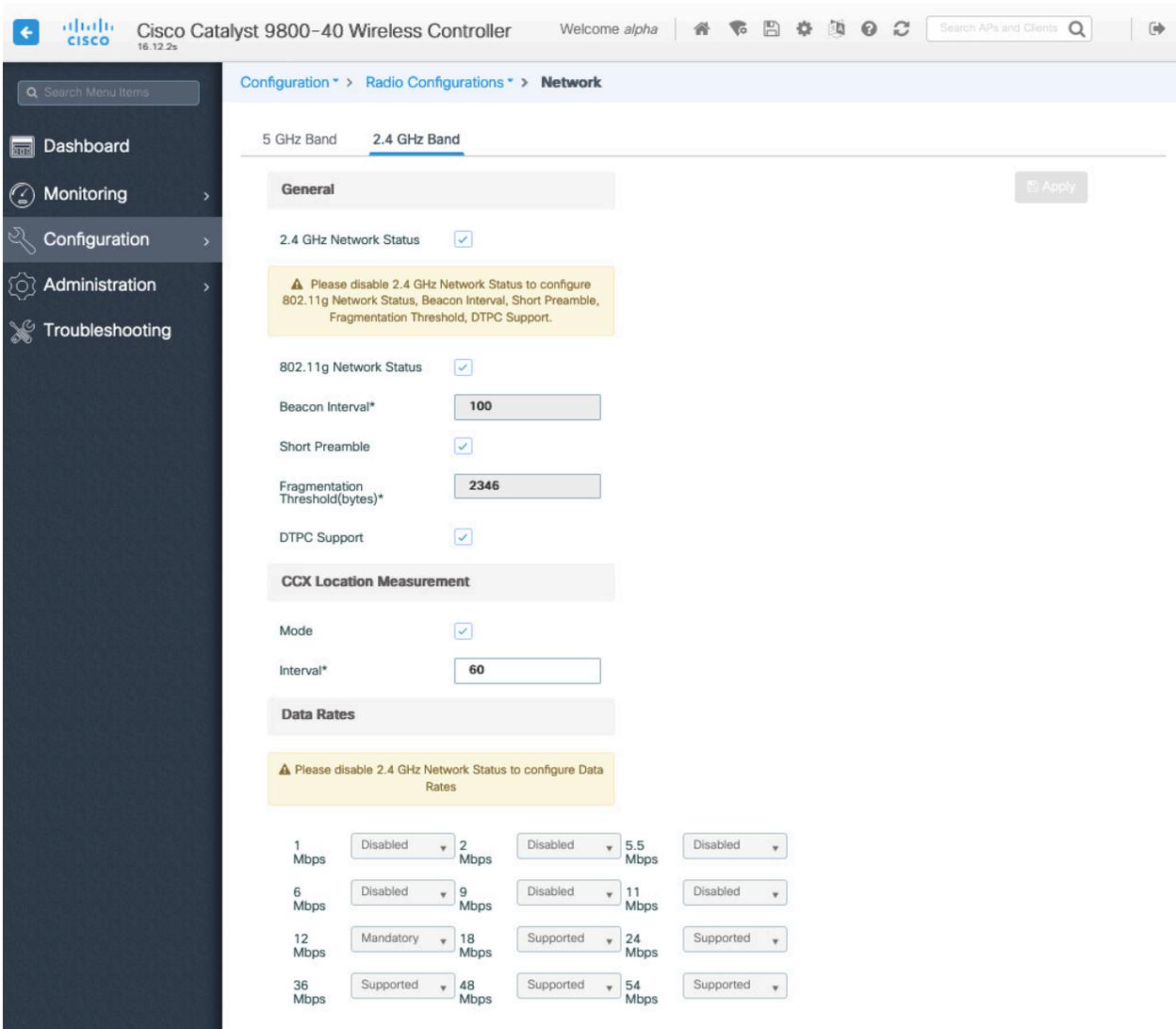
2.4 GHz を使用するには、[2.4 GHz ネットワークステータス (2.4 GHz Network Status)] と [802.11g ネットワークステータス (802.11g Network Status)] を [有効 (Enabled)] にします。

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ー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。

Cisco Catalyst 9800-40 Wireless Controller 16.12.2s Welcome alpha

Configuration > Radio Configurations > High Throughput

5 GHz Band 2.4 GHz Band

Apply

11n

Enable 11n Select All

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

11ac

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

Enable 11ac Select All

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

11ax

Enable 11ax Select All

Multiple Bssid

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

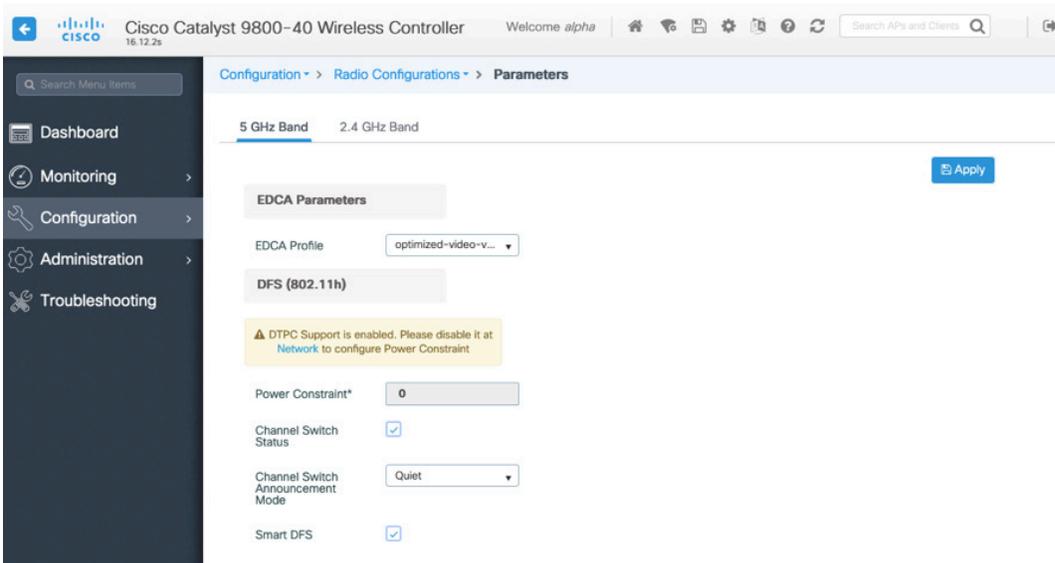
パラメータ

[EDCAパラメータ (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。

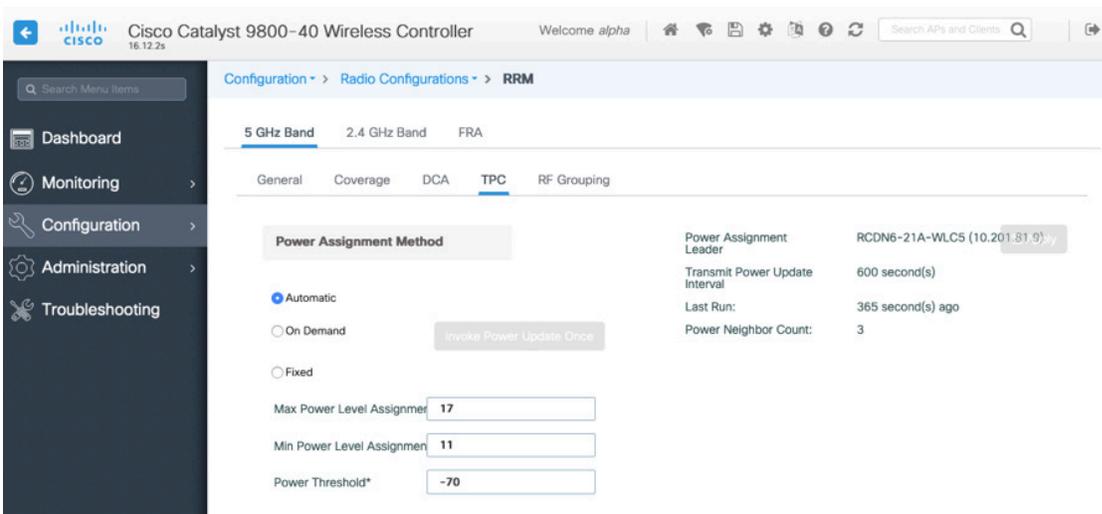
[チャンネル切り替えアナウンスモード (Channel Switch Announcement Mode)]を [サイレント (Quiet)]に設定します。



RRM

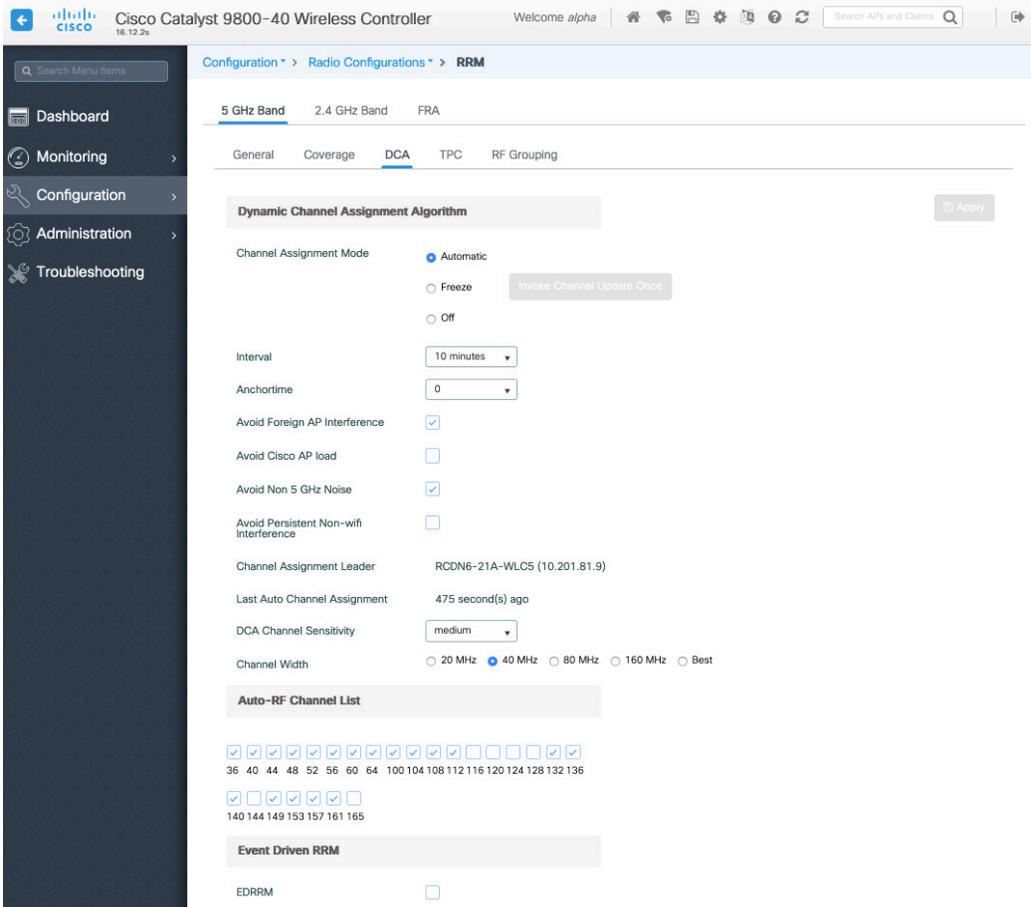
チャンネルと送信電力の設定を管理するには、自動割り当て方法を有効にすることをお勧めします。

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。

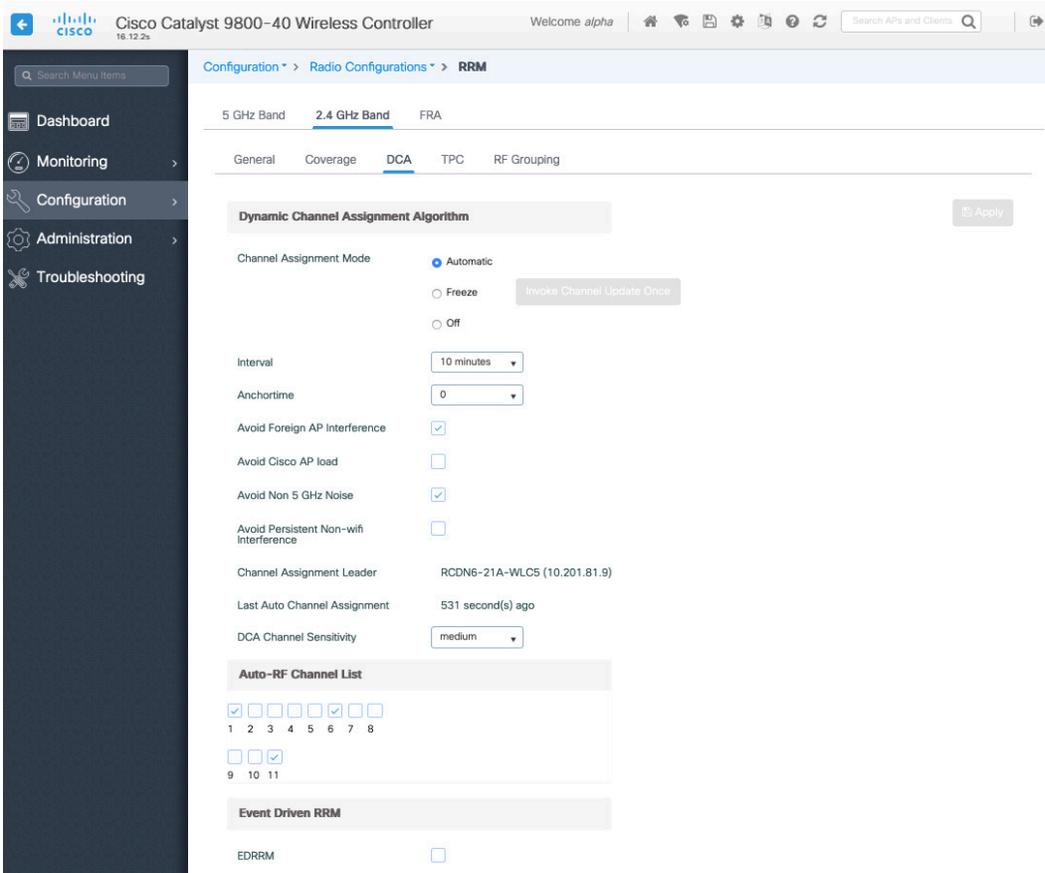


5 GHz を使用する場合、多くのチャンネルをスキャンすることによるアクセスポイント検出の遅延を避けるために、チャンネル数を制限することをお勧めします (例: 12 チャンネルのみ)。

5 GHz チャンネル幅は、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ンネル幅を使用することを推奨します。



2.4 GHz を使用する場合、チャンネルリストでチャンネル 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ン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 チャンネル幅は、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ンネル幅を使用することを推奨します。

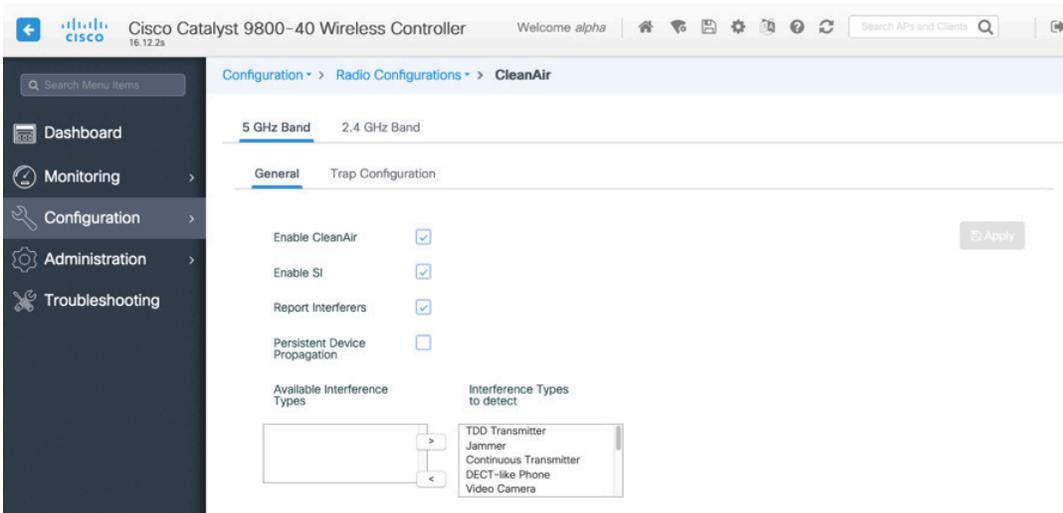
The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration interface. The main content area is titled 'Edit Radios 5 GHz Band' and is divided into several sections:

- General:** AP Name: rcdn6-22a-ap1, Admin Status: ENABLED, CleanAir Admin Status: ENABLED.
- RF Channel Assignment:** Current Channel: 149, Channel width: 40 MHz, Assignment Method: Global.
- Tx Power Level Assignment:** Current Tx Power Level: 2, Assignment Method: Global.
- Antenna Parameters:** Antenna Type: Internal, Antenna Mode: Omni, Antenna A, B, C, and D are all checked, Antenna Gain: 10.

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

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 テクノロジー搭載の 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)]

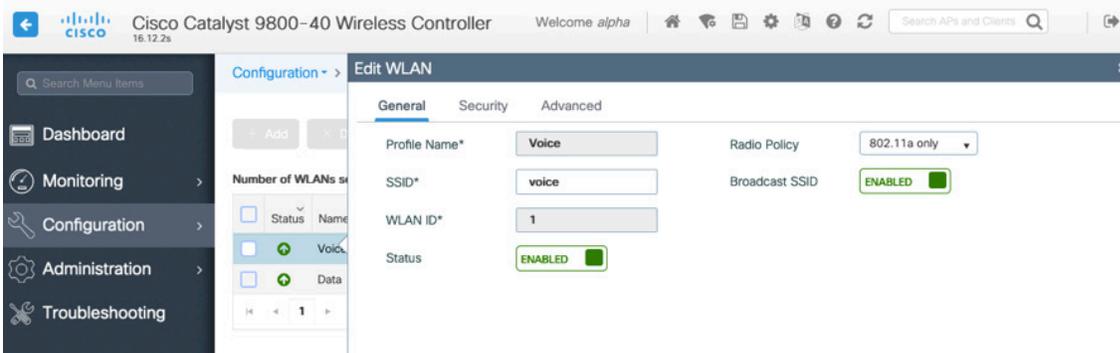
Cisco Desk Phone 9800 シリーズには別の SSID を割り当てることを推奨します。

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ンネルが利用でき、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。

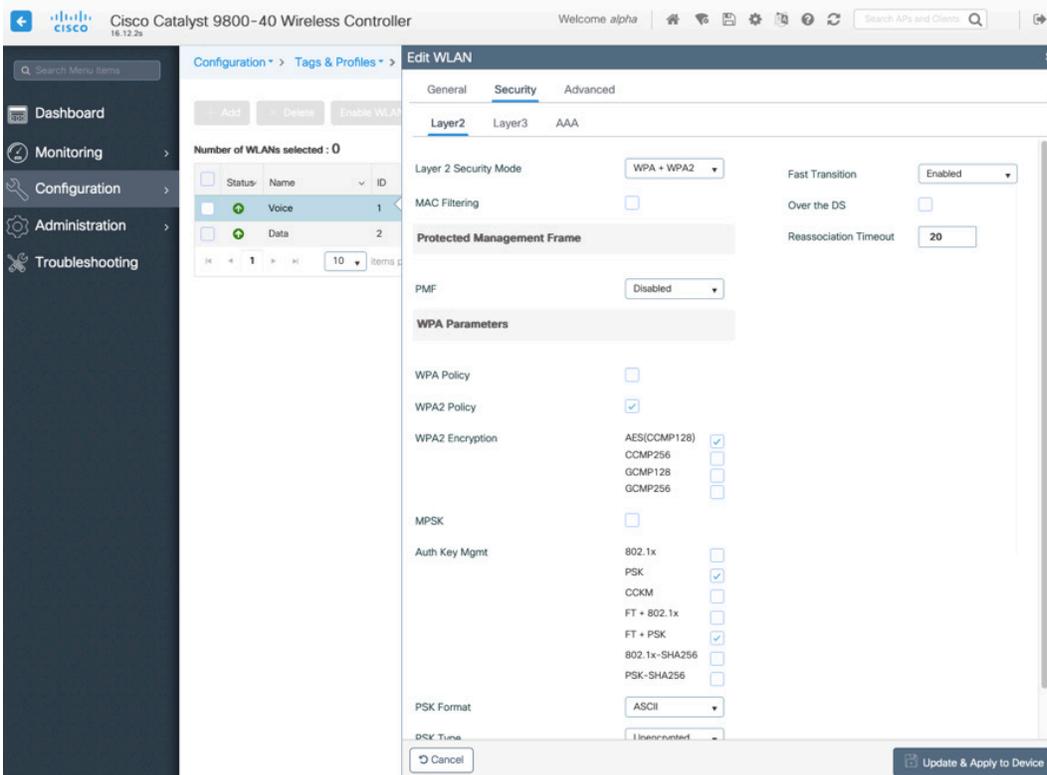
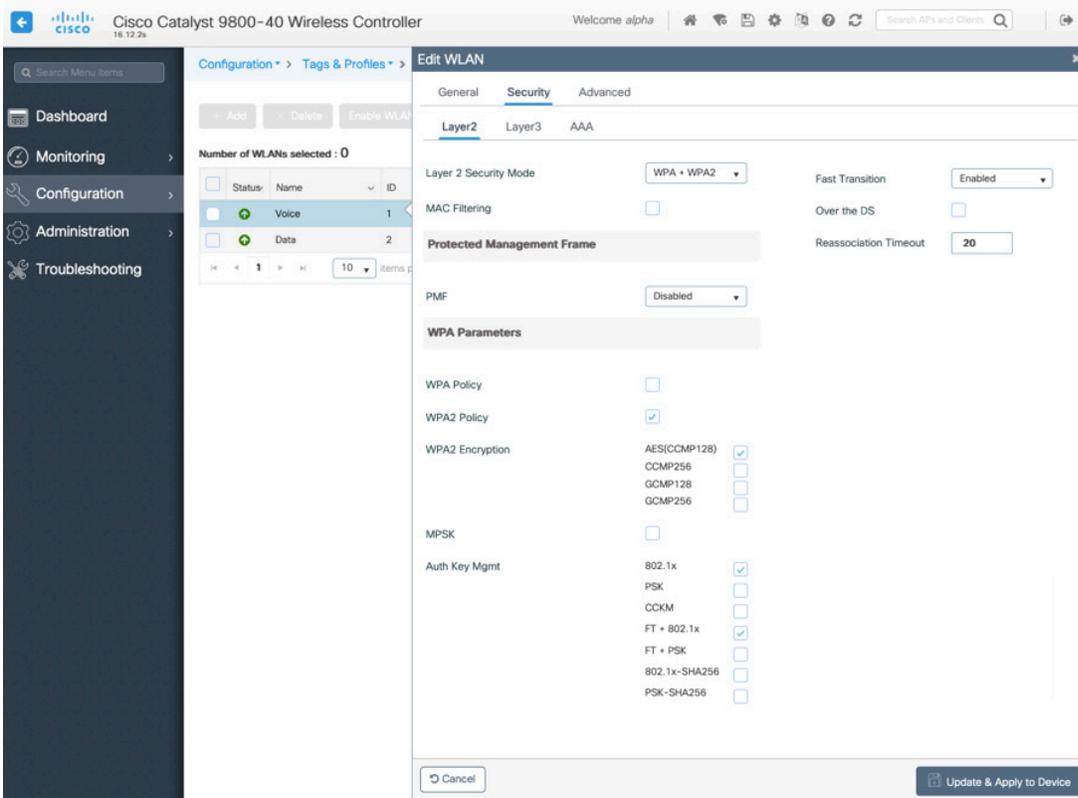


高速セキュア ローミングに 802.11r (FT) を使用するには、[高速移行] を [有効] に設定します。

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。

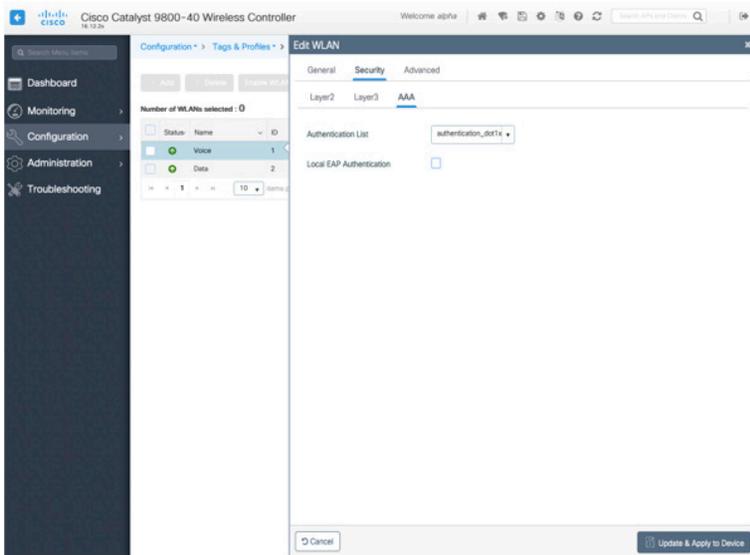
AES(CCMP128) 暗号化の WPA2/WPA3 ポリシーを有効にし、802.1x、PSK または SAE のどちらかを使用するかに応じて、認証キー管理タイプの 802.1x、PSK または SAE を使用するかを選択します。



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 サーバグループで定義された RADIUS サーバにマッピングする 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。

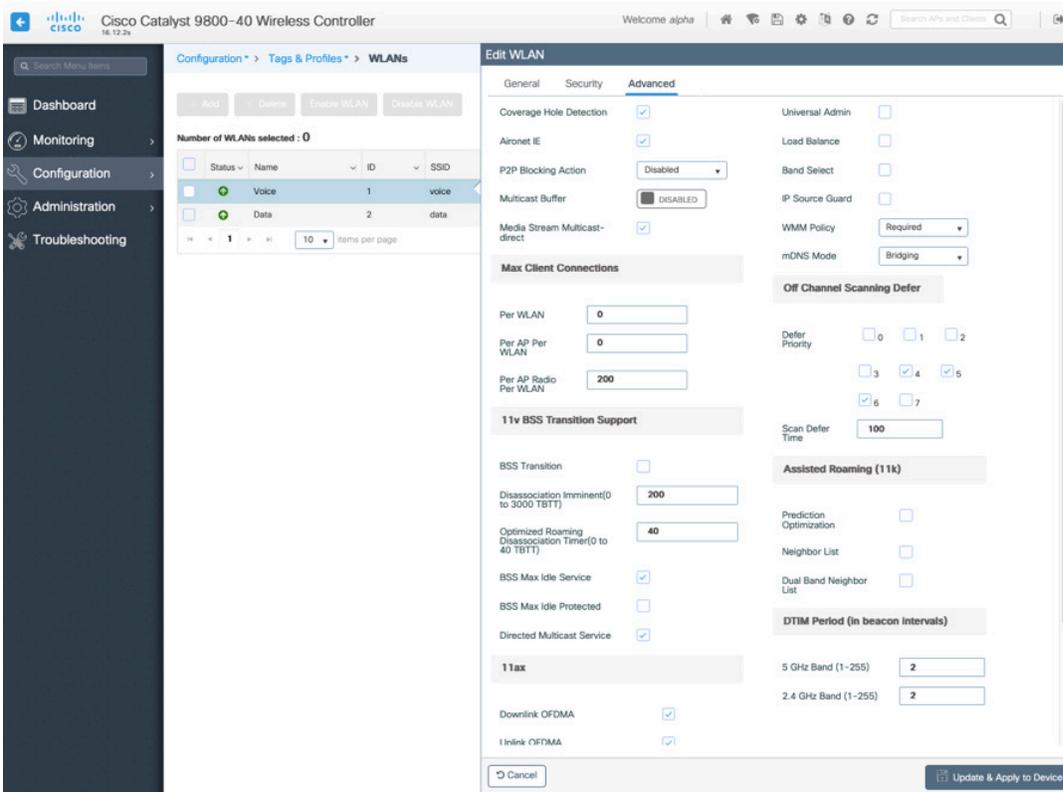
アクセスポイントへのベスト エフォート アプリケーションを頻繁に使用するか、優先アプリケーション（音声および通話コントロールなど）の DSCP 値を保存しない場合、オフチャネルスキャンを保留し、スキャン保留時間を長くするために、低いキュー優先度 (0-3) と高いキュー優先度 (4-6) を有効にすることが推奨されます。

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。

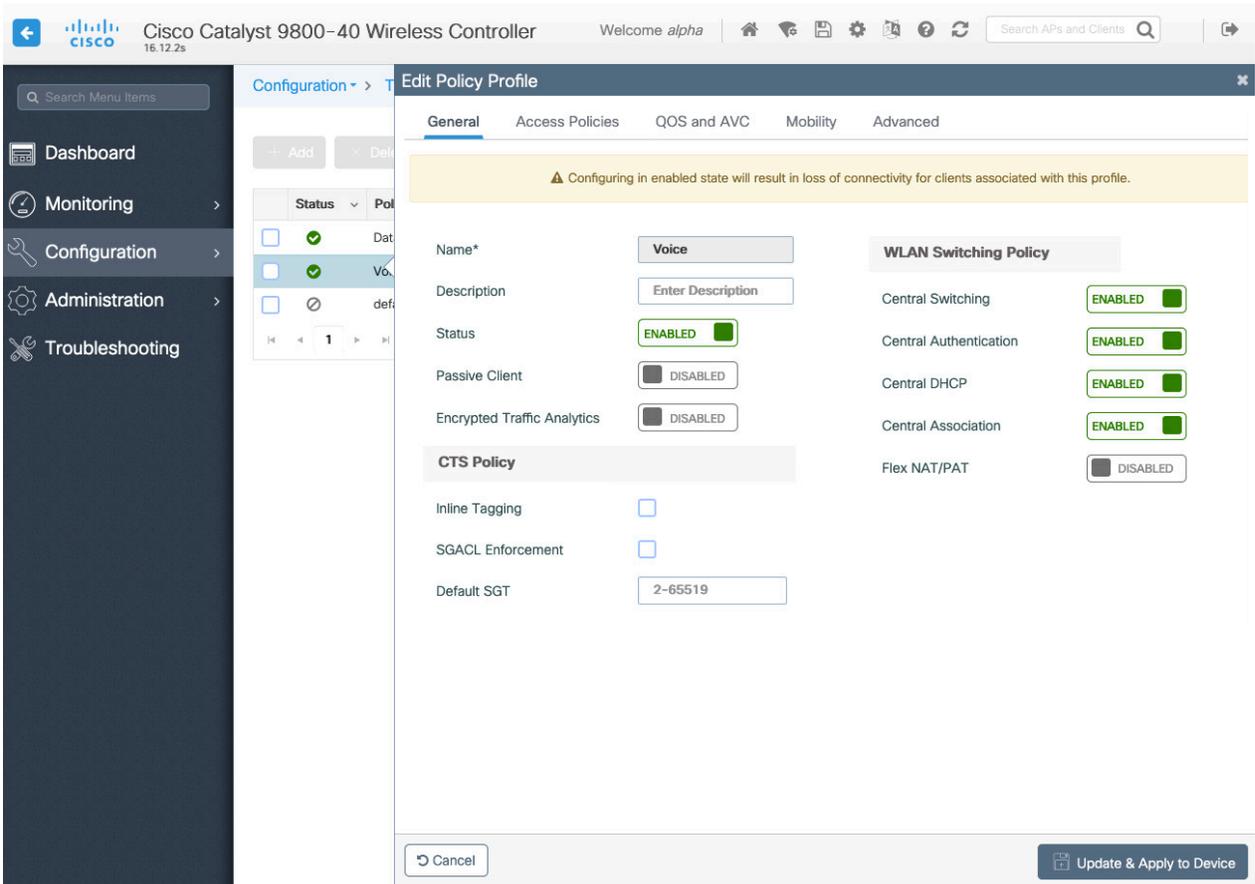


ポリシープロファイル

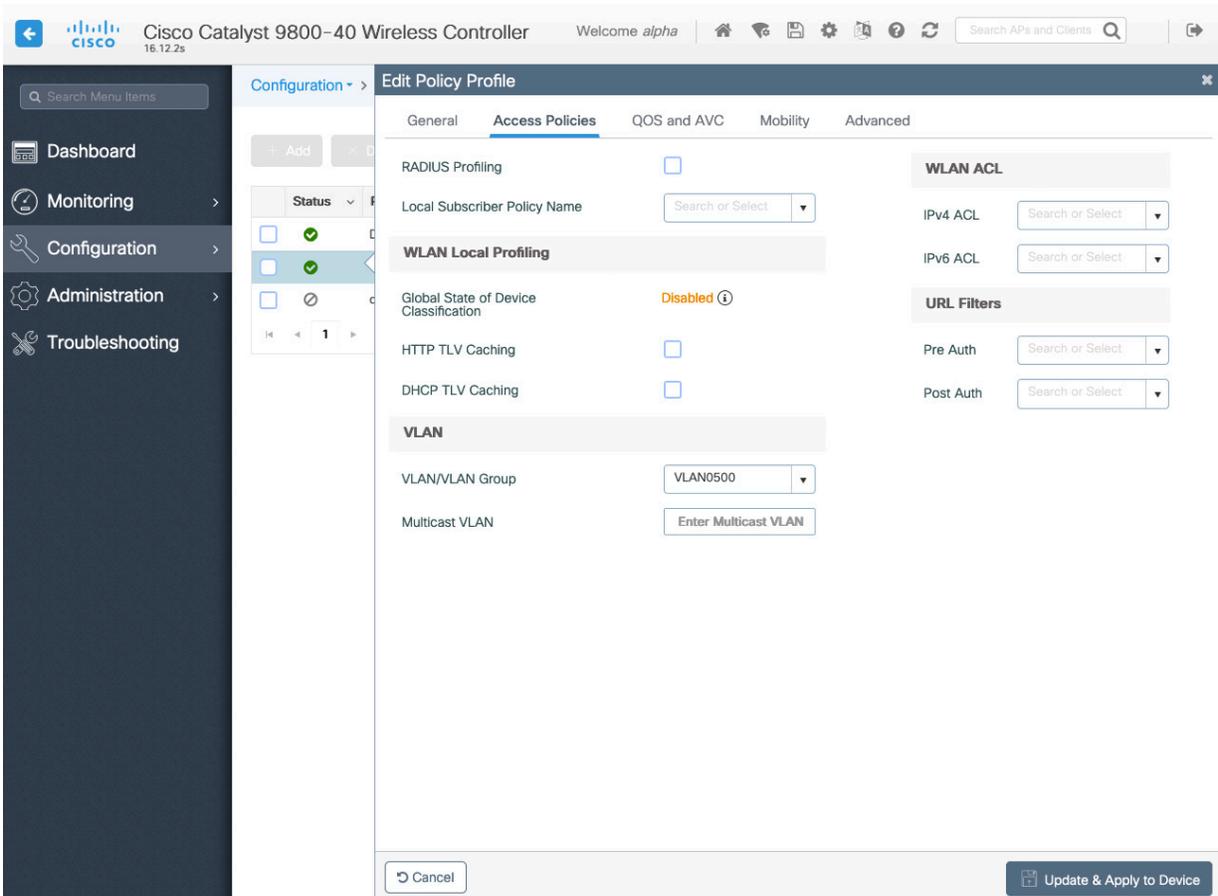
ポリシー プロファイルは、アクセス、QoS、モビリティ、および詳細設定に関する追加設定を定義するために使用されます。

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。

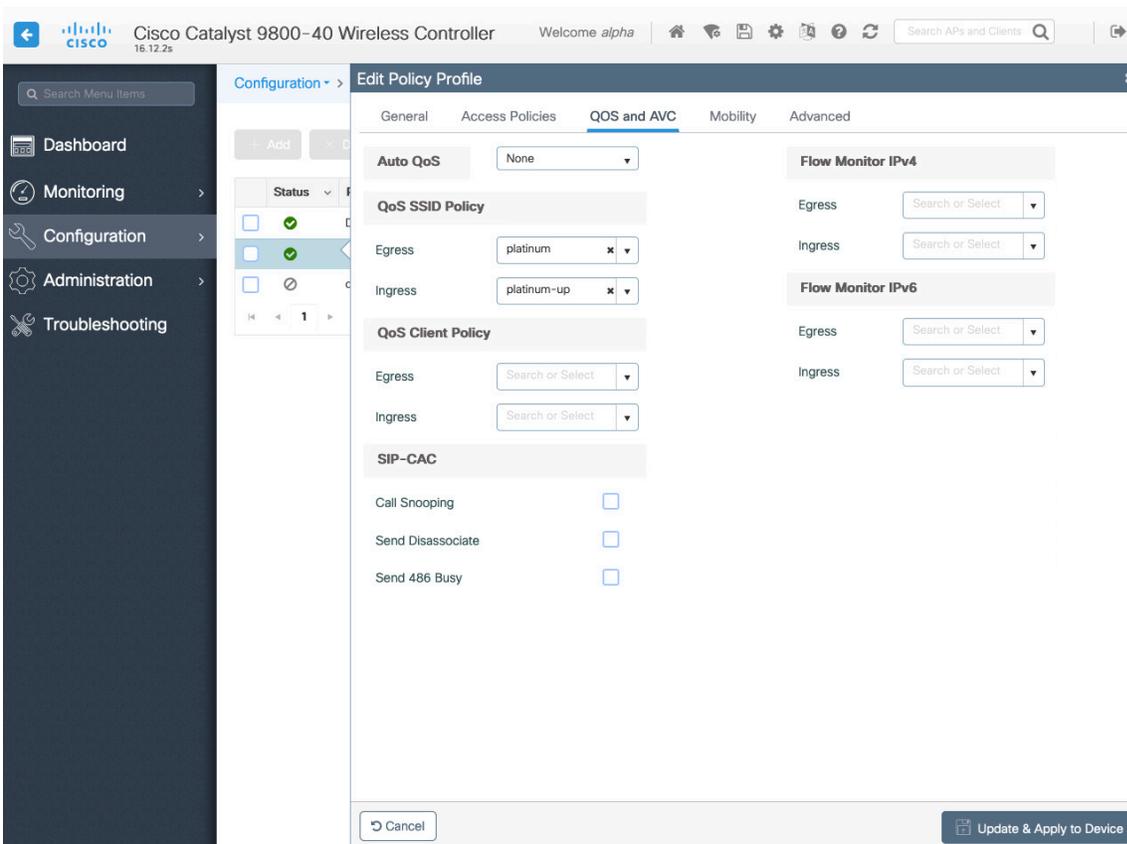
ポリシープロファイルの **ステータス** が **有効になっていることを確認してください**。



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。



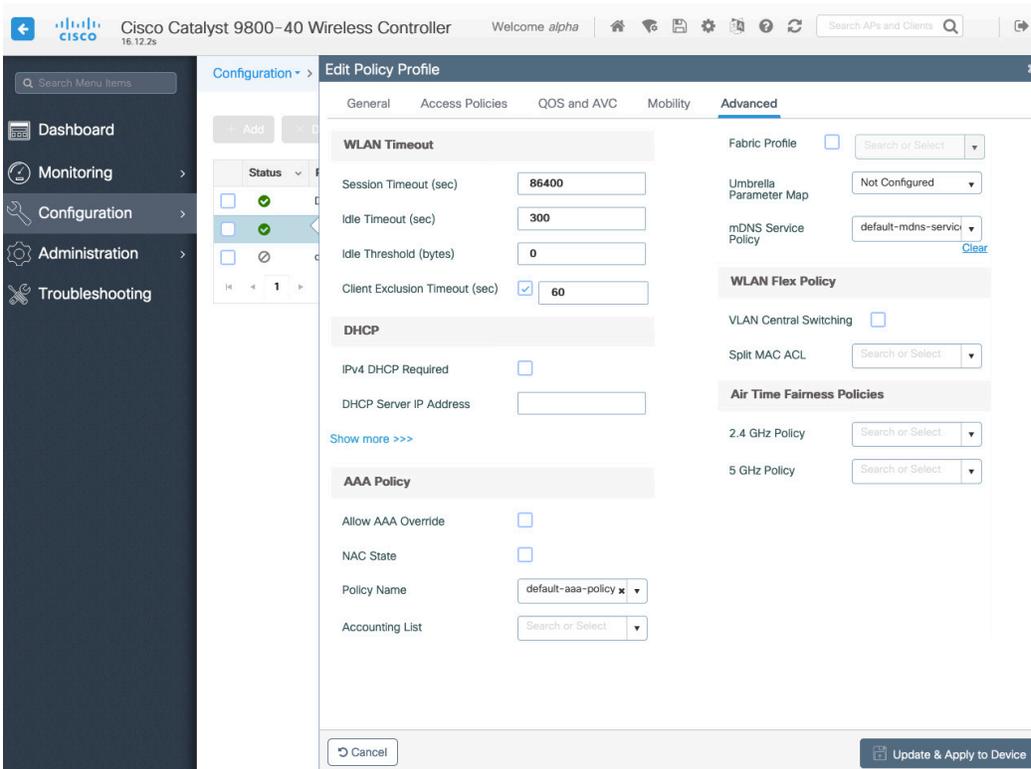
[QoS SSIDポリシー (QoS SSID Policy)] のエグレスを [プレミアム (Platinum)] に、イングレスを [プラチナアップ (Platinum-up)] に設定します。



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

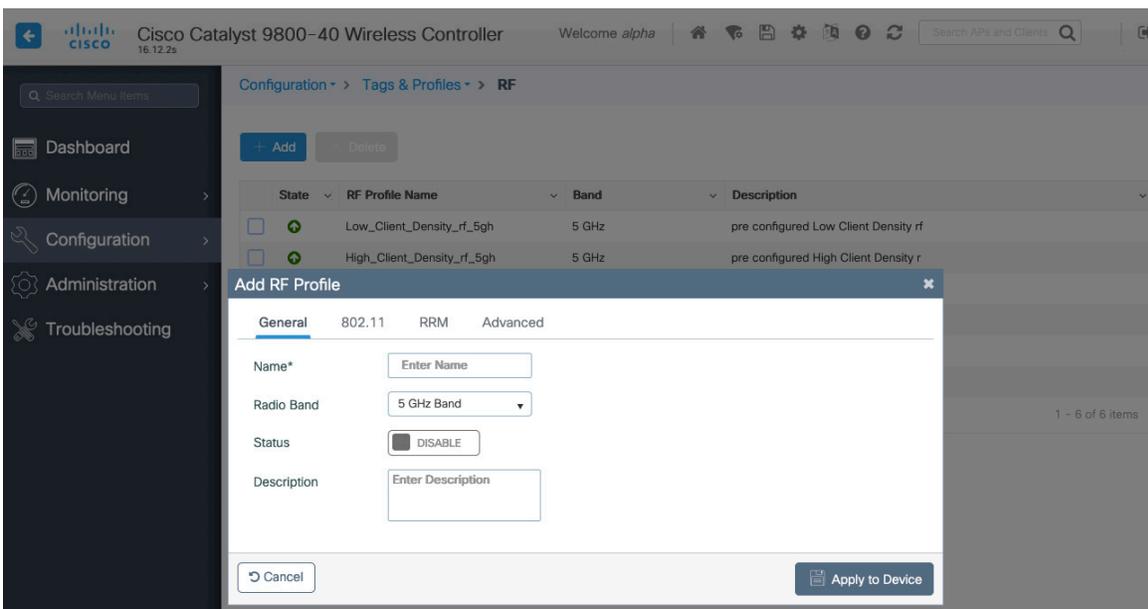
RF プロファイルを作成して、アクセスポイントのグループが使用する周波数帯域、データレート、RRM 設定、および詳細設定を指定することができます。

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。

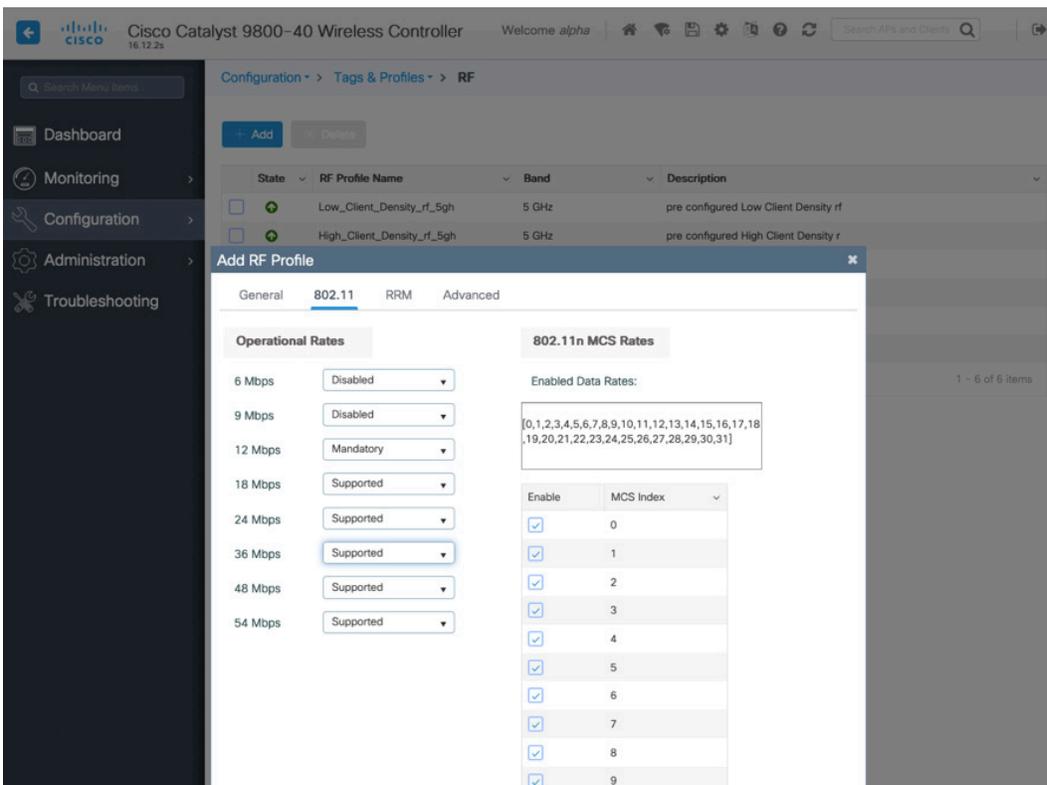
RF プロファイルの作成時に、**名前** と **無線帯域** を定義する必要があります。

[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。

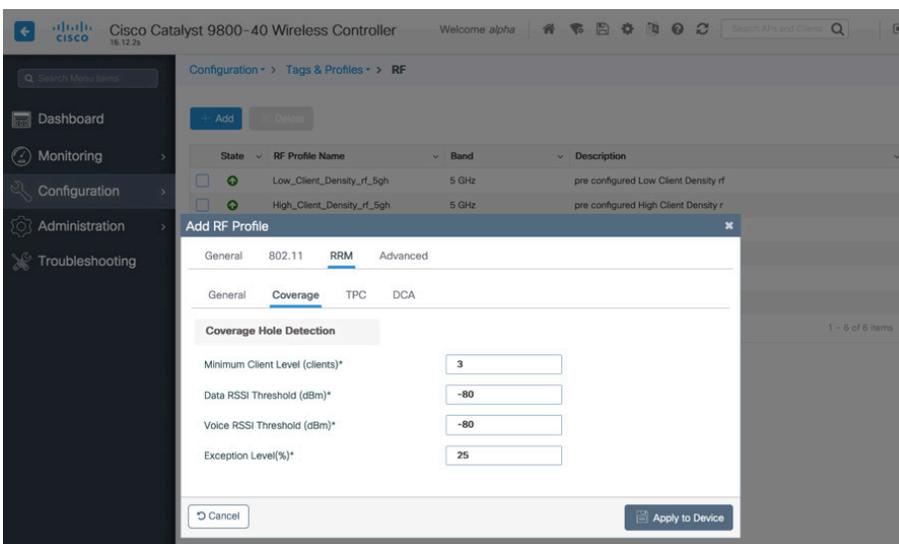


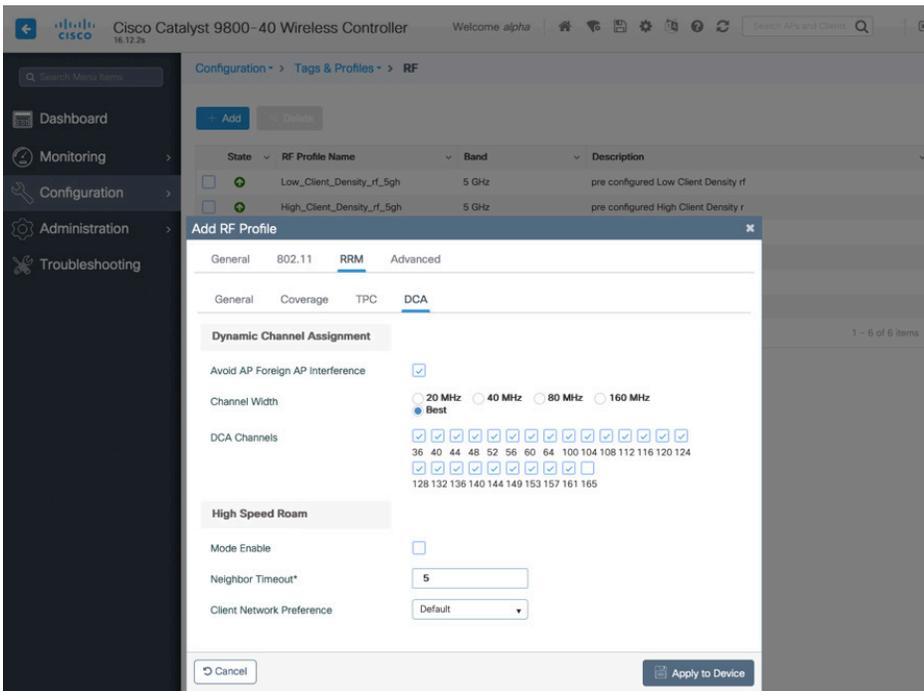
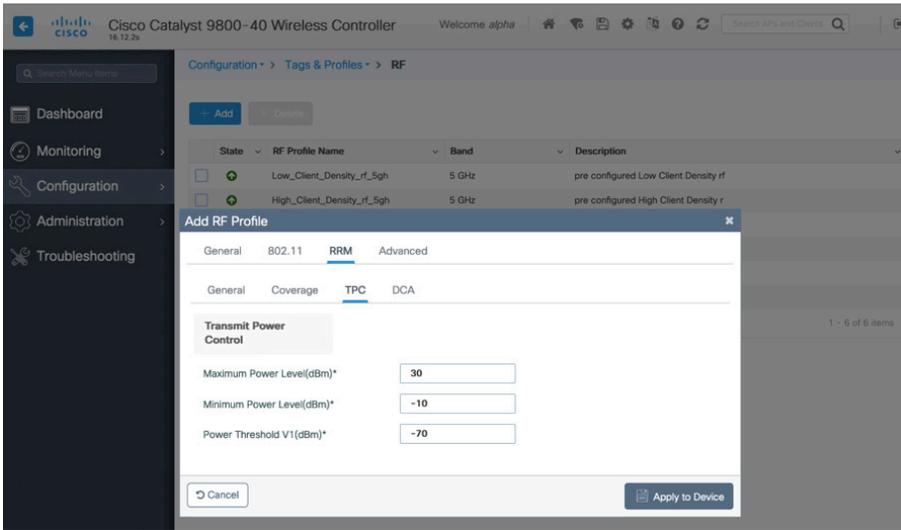
[802.11] タブで、必要に応じて、データレートを構成します。

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。

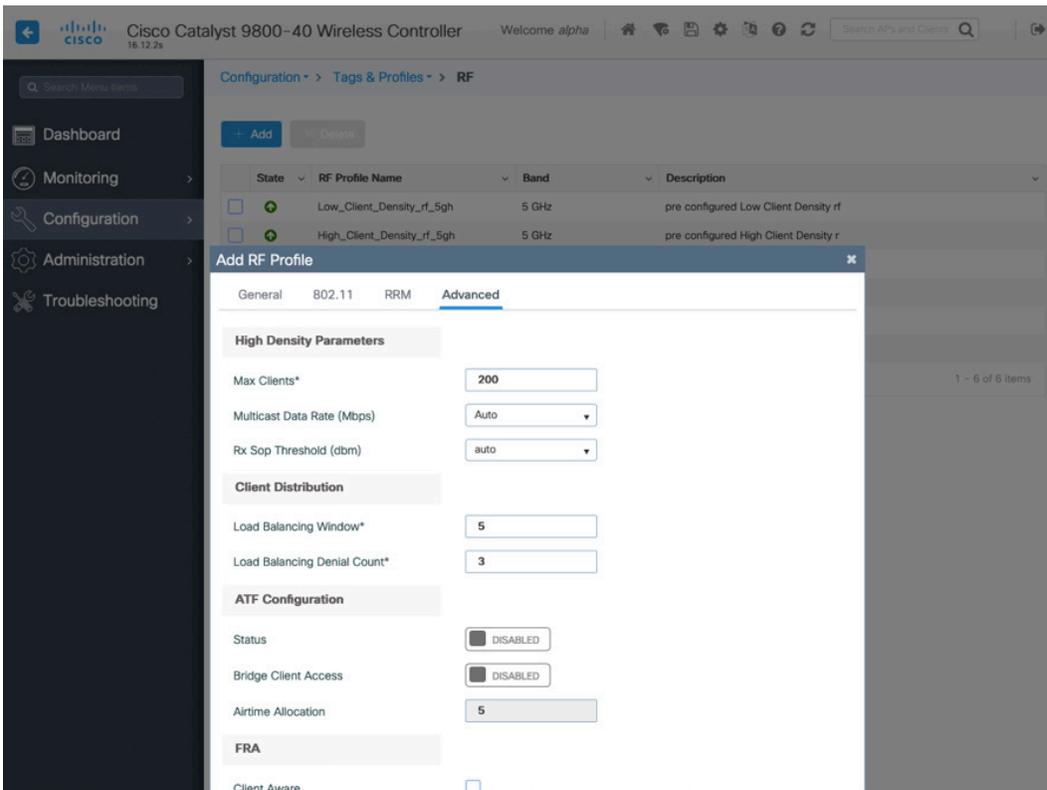


[RRM] タブで、[最大電力レベル (Maximum Power Level)] と [最小電力レベル (Minimum Power Level)] 設定および [DCA]、[TPC] および [カバレッジ (Coverage)] 設定を構成します。





[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

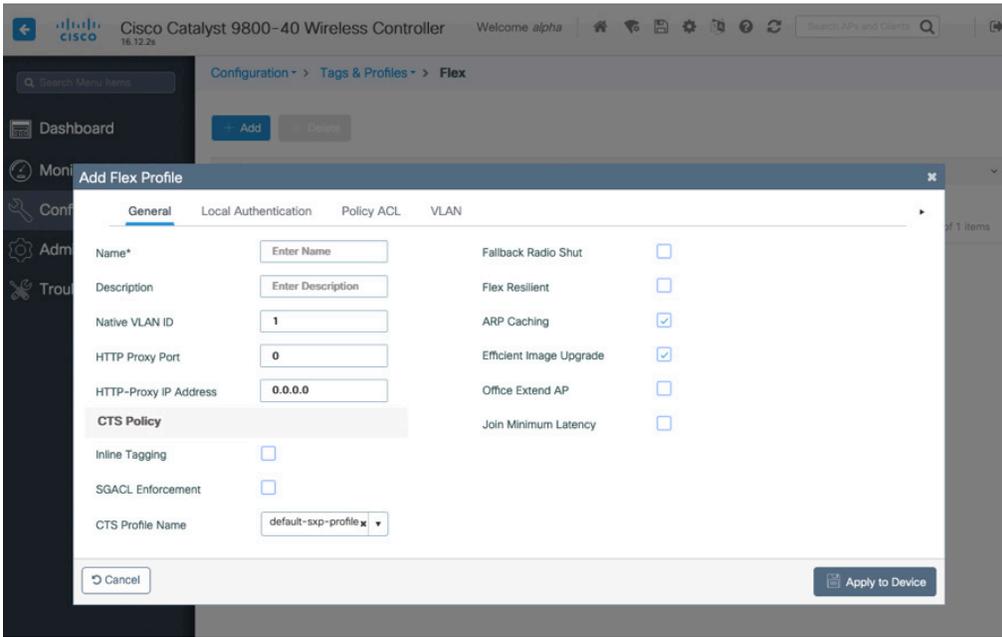
Flex プロファイルは、アクセスポイントが Flexconnect モードの場合に使用する設定を定義するために使用されます。

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。



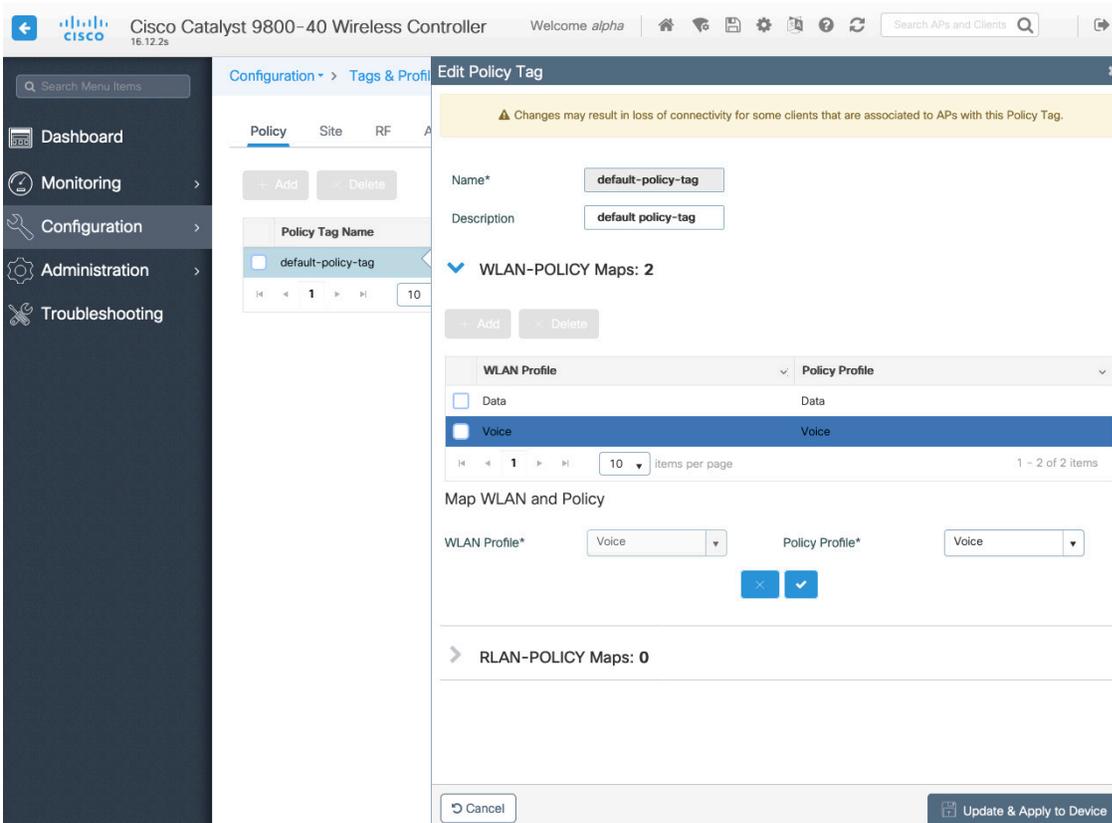
タグ

ポリシータグ

ポリシー タグは、WLAN プロファイルとポリシー プロファイルのマッピングを定義します。

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。



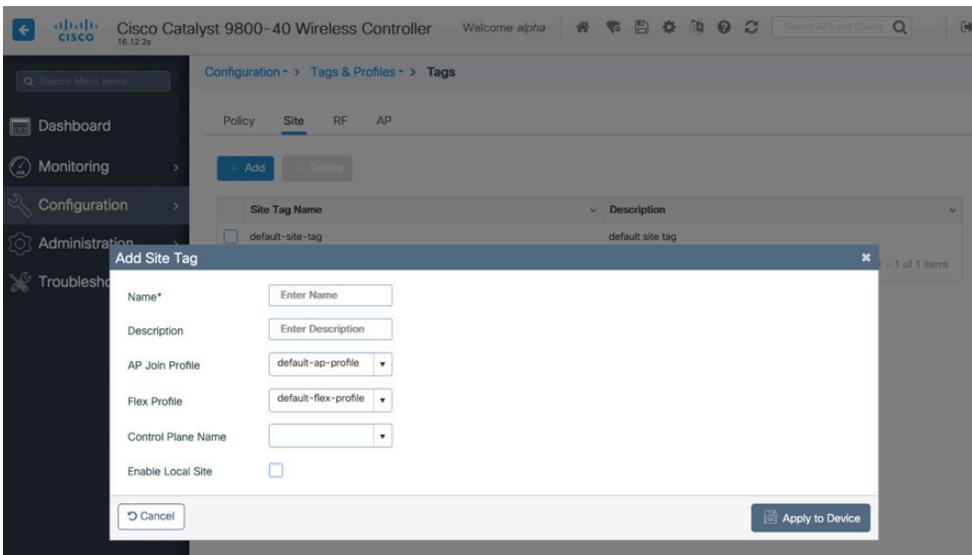
サイトタグ

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。

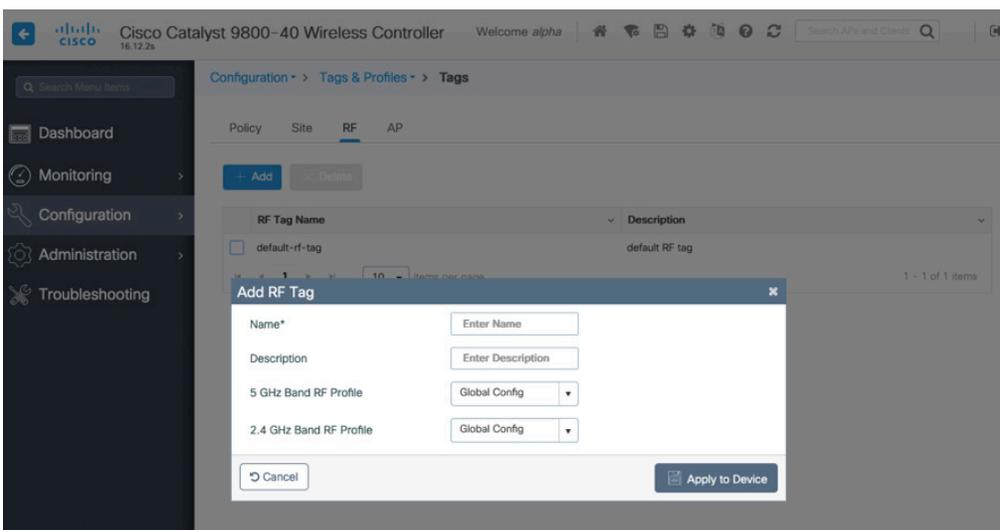


RF タグ

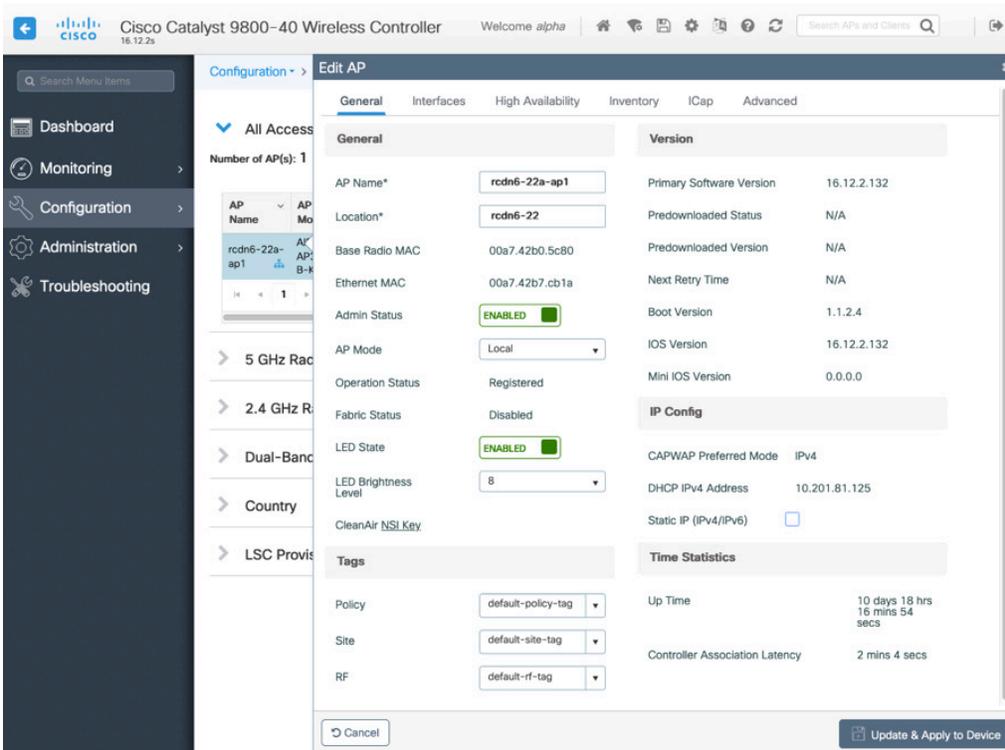
[RF タグ] は、2.4 GHz および 5 GHz で使用される RF プロファイルを定義します。

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。

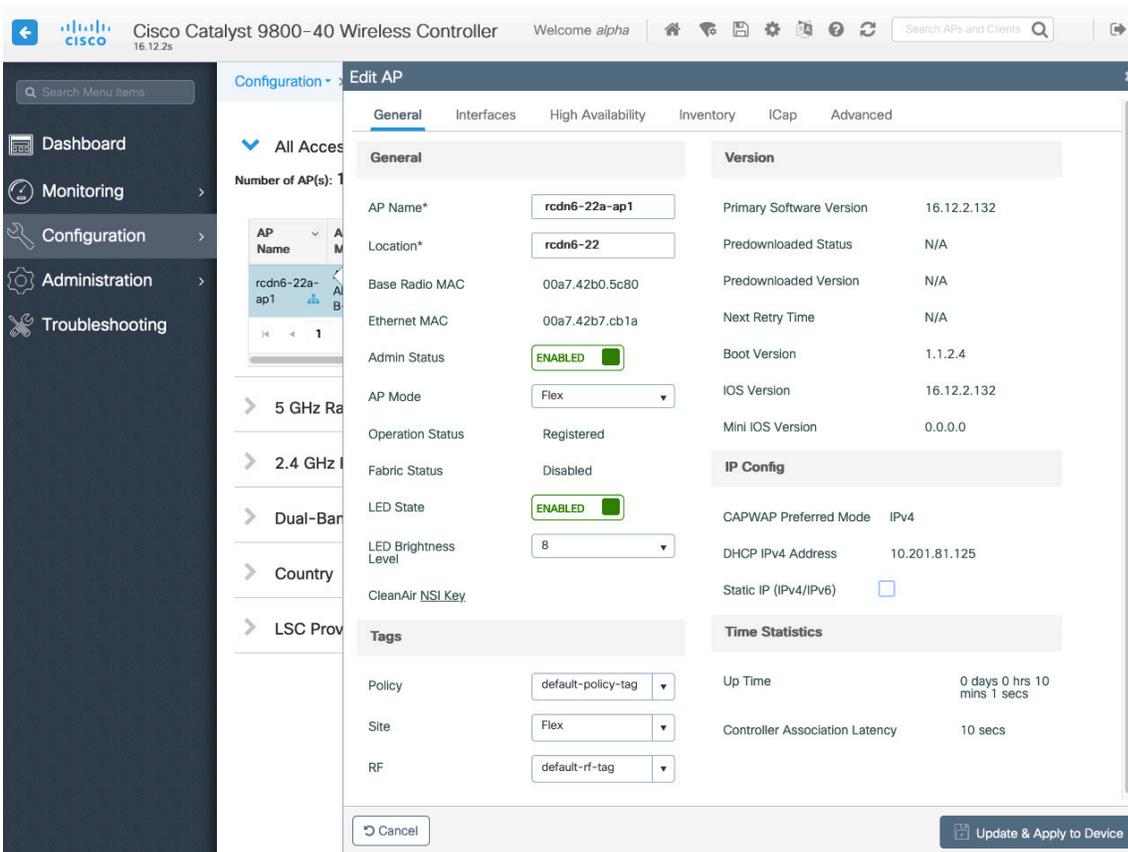
[RFタグ (RF Tag)]を作成する際は、使用する [5 GHz帯域RFプロファイル (5 GHz Band RF Profile)]と [2.4 GHz帯域RFプロファイル (2.4 GHz Band RF Profile)]を選択します。



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。

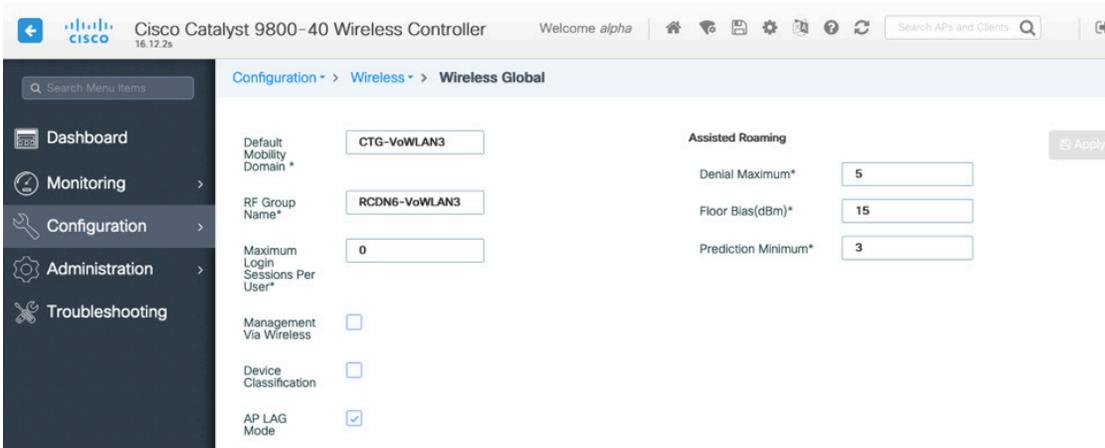


設定済み [フレックスプロファイル (Flex Profile)]を含む [サイトタグ (Site Tag)]を適用する際は、[APモード (AP もで)]が自動で [フレックス (Flex)]に変更されます。



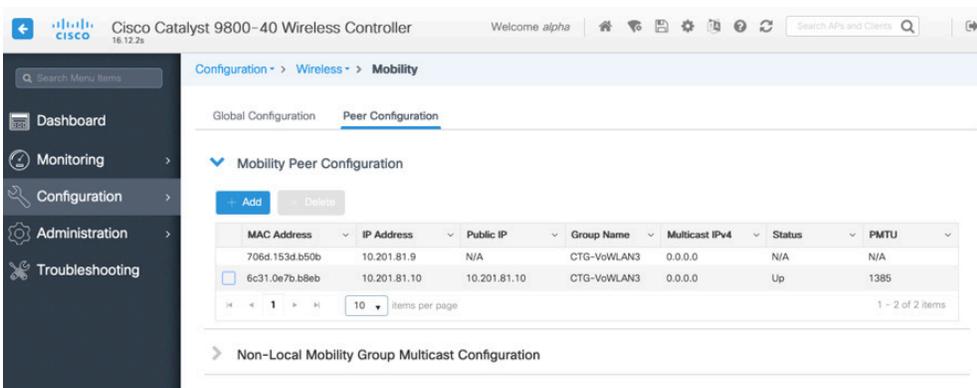
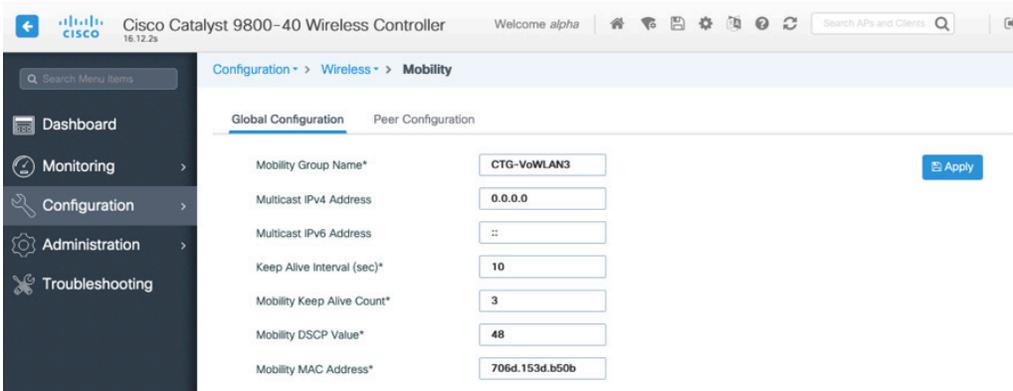
コントローラの設定

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
16.12.2a

Welcome *alpha*

Search APs and Clients

Configuration > Interface > Wireless

Dashboard
Monitoring
Configuration
Administration
Troubleshooting

Add Delete

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

10 items per page 1 - 1 of 1 items

コール アドミッション制御 (CAC)

[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。

The screenshot shows the configuration page for Media Parameters on a Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Radio Configurations > Media Parameters. The page is divided into several sections:

- 6 GHz Band**: A warning message states "6 GHz Network is operational. Configuring Media Parameters will result in loss of connectivity of clients."
- Media - General**:
 - Unicast Video Redirect:
 - Multicast Direct Admission Control:
 - Media Stream Admission Control (ACM):
 - Maximum Media Stream RF bandwidth (%)*: 5
 - Maximum Media Bandwidth (%)*: 85
 - Client Minimum Phy Rate (kbps): 6000
 - Maximum Retry Percent (%)*: 80
- Media Stream - Multicast Direct Parameters**:
 - Multicast Direct Enable:
 - Max streams per Radio: No Limit
- Voice - Call Admission Control (CAC)**:
 - Admission Control (ACM):
- Traffic Stream Metrics**:
 - Metrics Collection:
 - Stream Size*: 84000
 - Max Streams*: 2
 - Inactivity Timeout:

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。

The screenshot shows the configuration page for Multicast on a Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Services > Multicast. The page is divided into several sections:

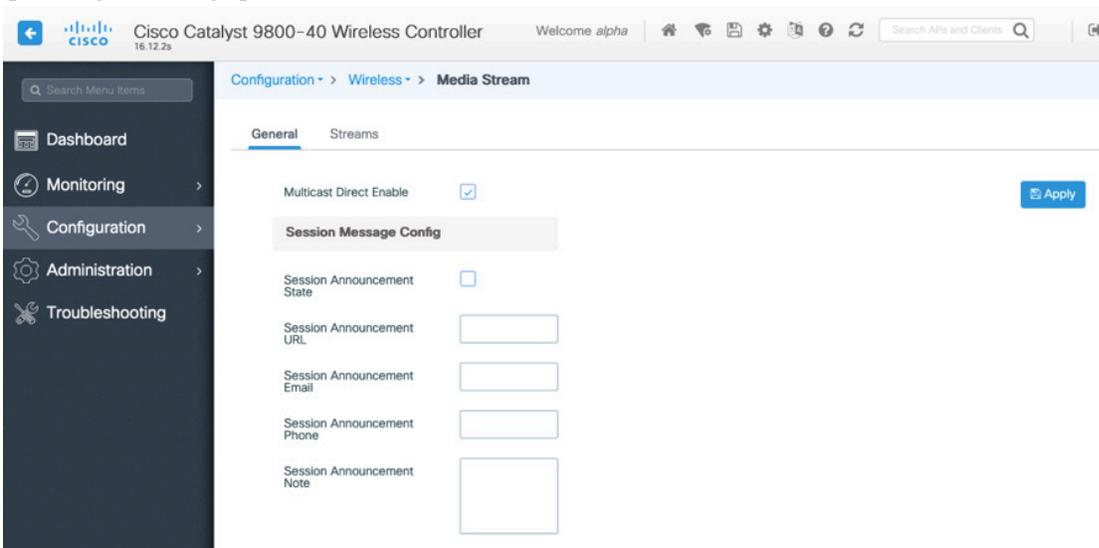
- Global Wireless Multicast Mode**: ENABLED
- Wireless mDNS Bridging**: DISABLED
- Wireless Non-IP Multicast**: DISABLED
- Wireless Broadcast**: DISABLED
- AP Capwap Multicast**: Unicast
- MLD Snooping**: DISABLED
- IGMP Snooping Querier**: DISABLED
- IGMP Snooping**: ENABLED
- Last Member Querier Interval (milliseconds)**: 1000

IGMP Snooping section:

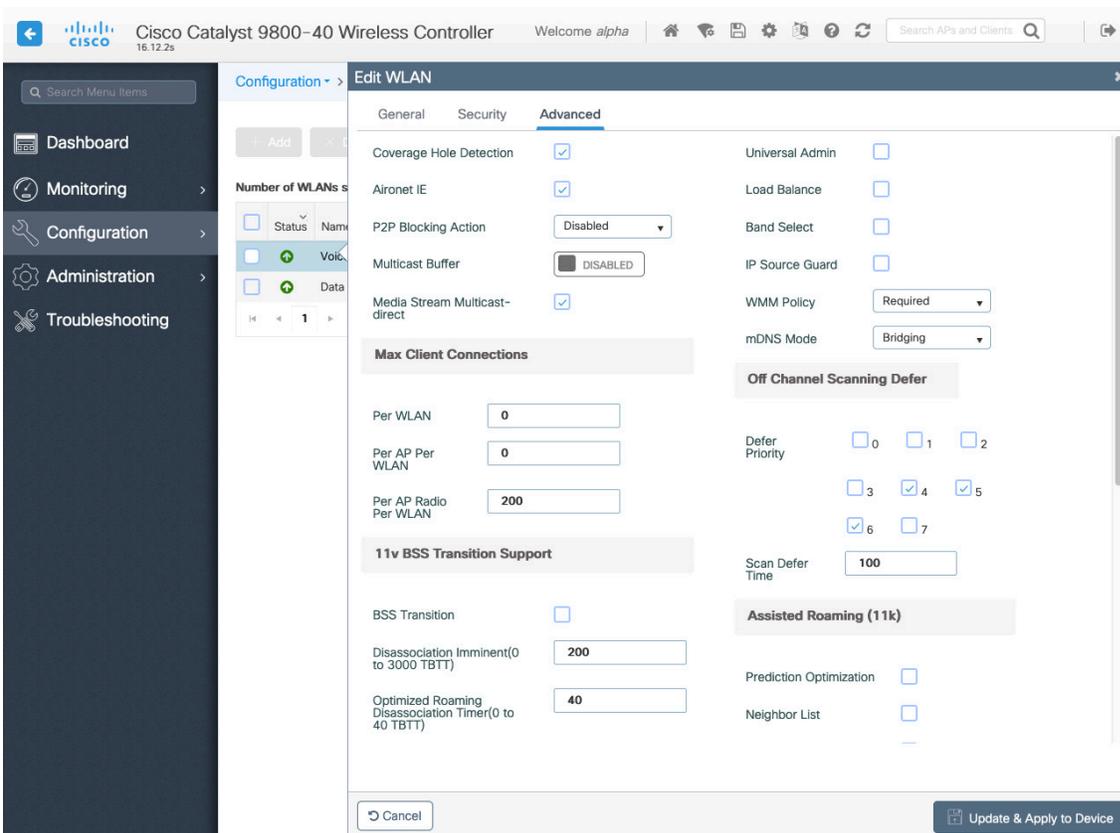
- Disabled**: No Vlan available
- Enabled**:

Status	VLAN ID	Name
<input checked="" type="checkbox"/>	1	default
<input checked="" type="checkbox"/>	310	VLAN0310
<input checked="" type="checkbox"/>	400	VLAN0400
<input checked="" type="checkbox"/>	500	VLAN0500

[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。



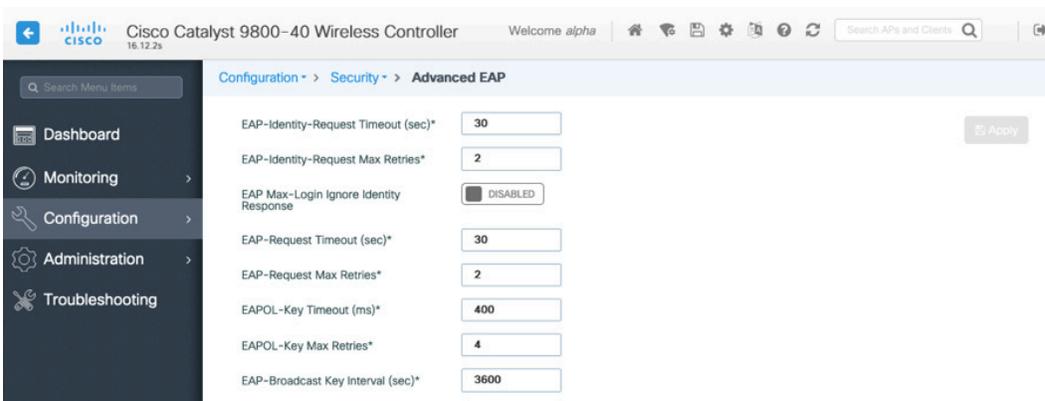
WLAN 設定で マルチキャストダイレクト を有効にします。



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 Retries)]** をデフォルト値の 2 から 4 に設定します。

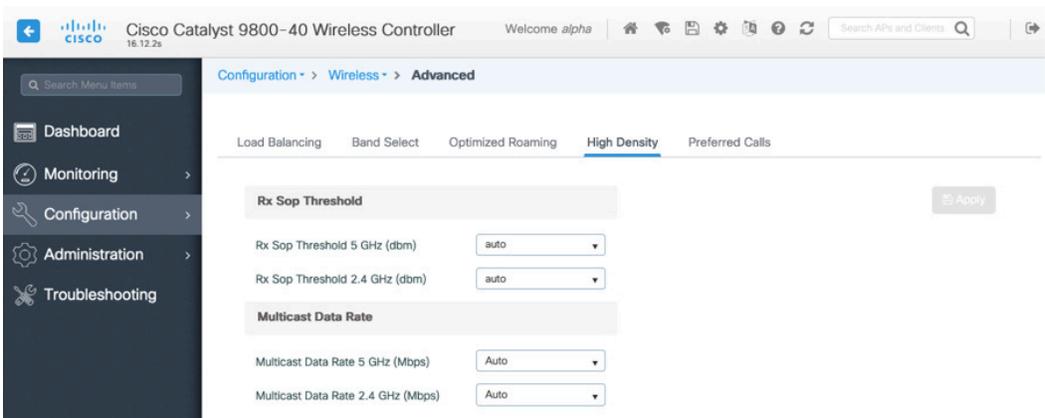
802.1x を使用する場合、**[EAPOL キータイムアウト (EAPOL-Key Timeout)]** と **[EAPOL キー最大試行回数 (EAPOL-Key Max Retries)]** のデフォルト値で問題ありませんが、これらの値をそれぞれ 400 と 4 に設定することが推奨されます。

[EAPOL 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 3600 秒 (1 時間) に設定されていることを確認します。

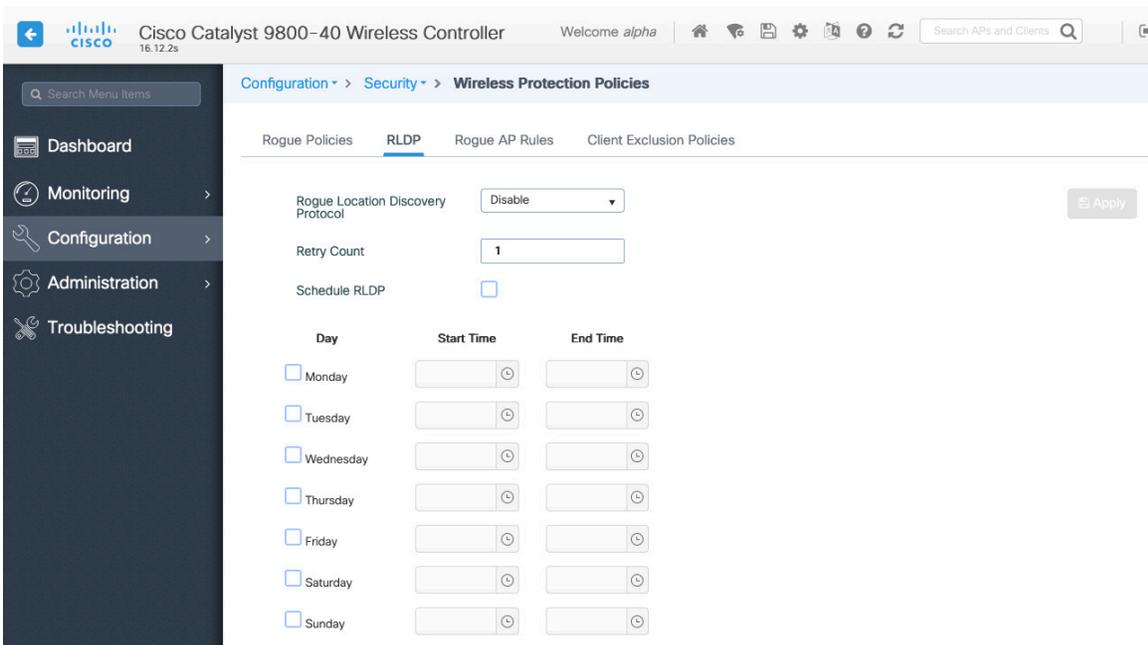
Rx Sop Threshold

[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

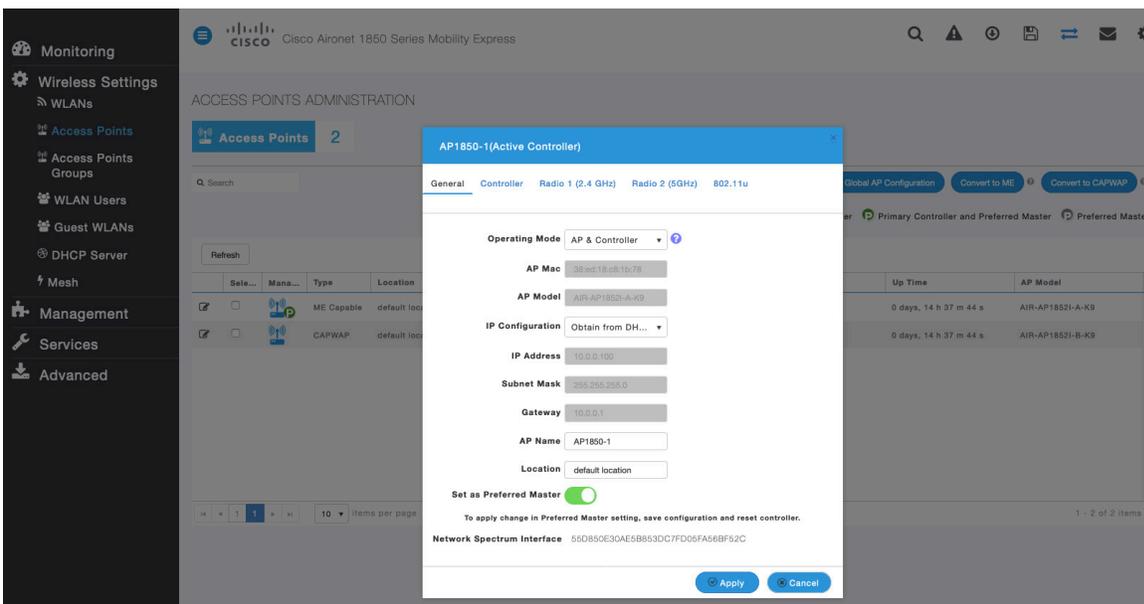
Cisco Mobility Express および Lightweight アクセスポイントを設定する場合、以下のガイドラインを使用してください。

- 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 テクノロジー搭載の 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

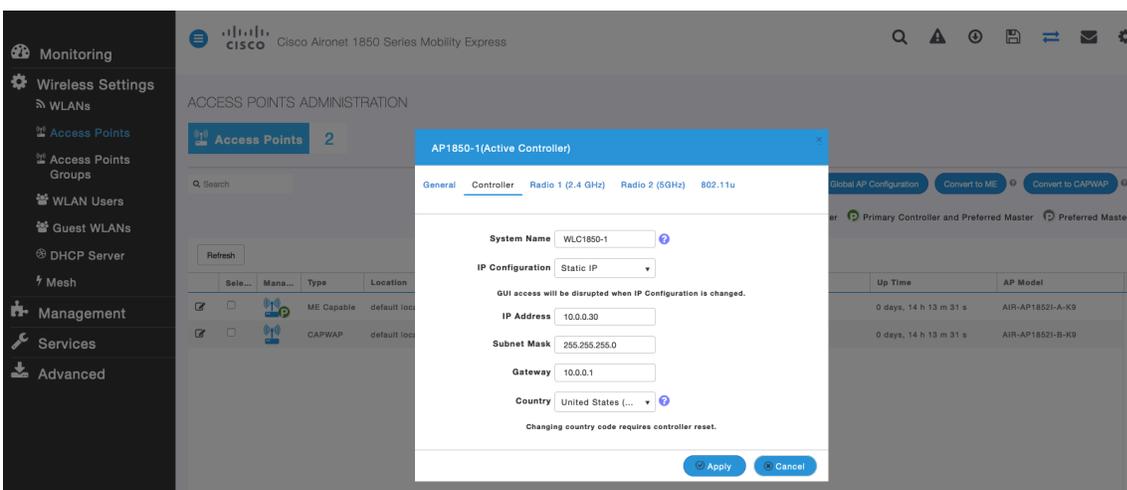
コントローラの設定

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。利用できるチャンネル数が多く、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 チャンネル幅は、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ンネル幅を使用することを推奨します。

2.4 GHz を使用する場合、チャンネル 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 テクノロジー搭載の 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。

The screenshot shows the 'Advanced RF Parameters' configuration page. The left sidebar contains navigation options: Monitoring, Wireless Settings, Management, Services, Advanced, SNMP, Logging, RF Optimization, RF Profiles, Controller Tools, Security Settings, and CMX. The main content area includes the following settings:

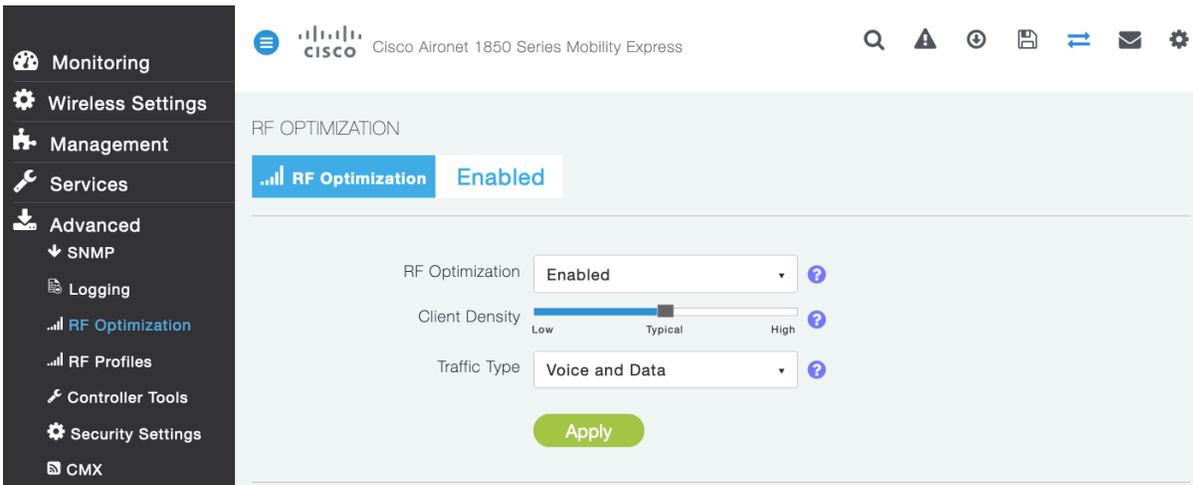
- 2.4 GHz Band:
- 5.0 GHz Band:
- Automatic Flexible Radio Assignment:
- 2.4 GHz Optimized Roaming:
- 5 GHz Optimized Roaming:
- Event Driven RRM:
- CleanAir detection:
- 5.0 GHz Channel Width: 40 MHz (dropdown menu)
- 2.4 GHz Data Rates: A slider from 1 to 54, with a red bar indicating '802.11b devices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

At least one Channel Number should be selected

Apply

RF 最適化

[RF最適化 (RF Optimization)] を有効にして、チャン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。



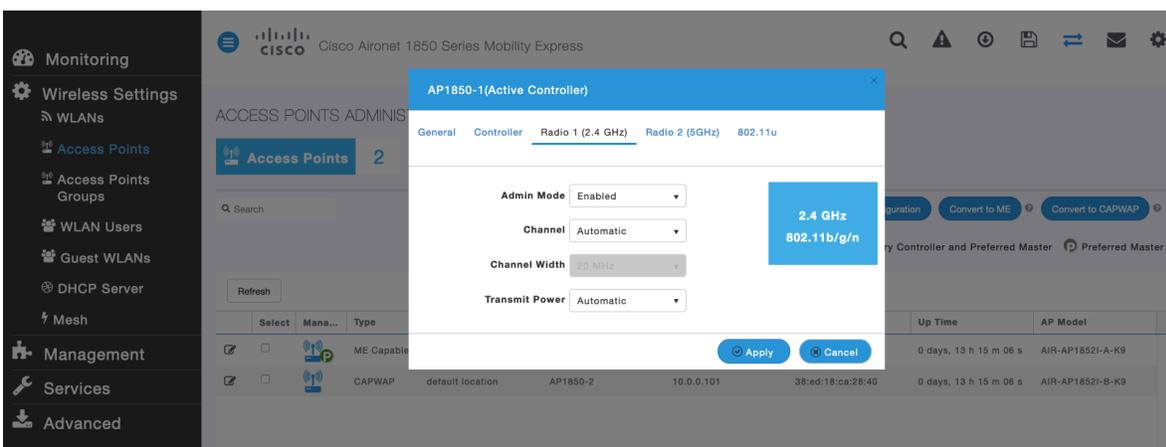
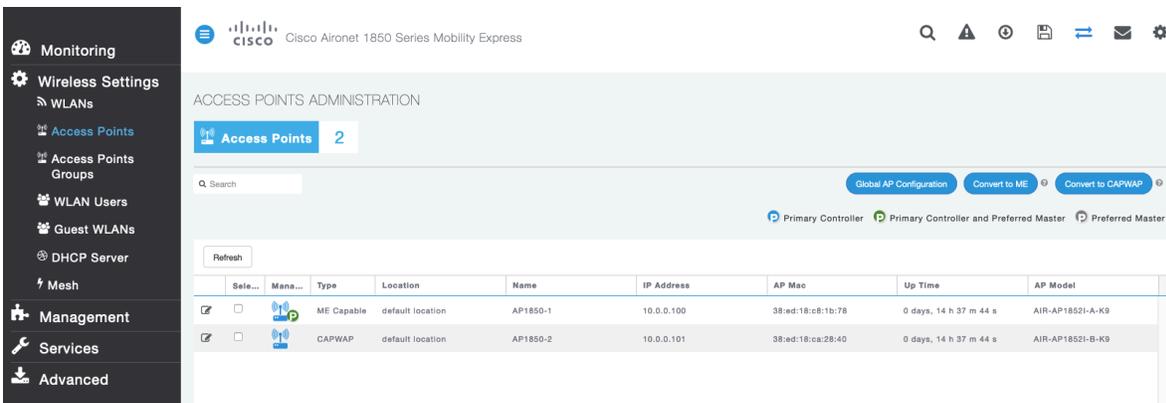
利用する周波数に周波数帯に応じて、5GHz または 2.4GHz のいずれかで動的チャンネルと送信電力の割り当てを使用するように、個々のアクセスポイントは全体設定をオーバーライドするように設定できます。

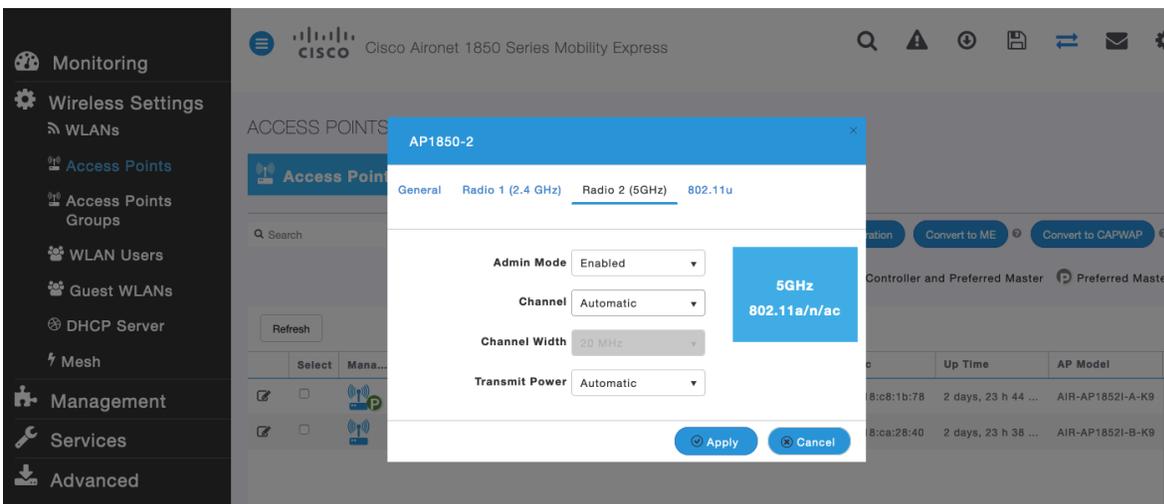
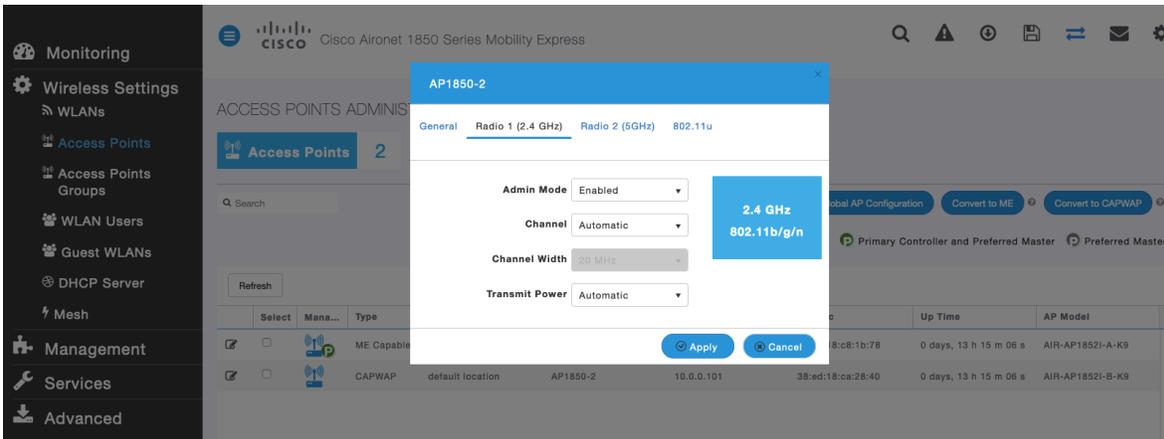
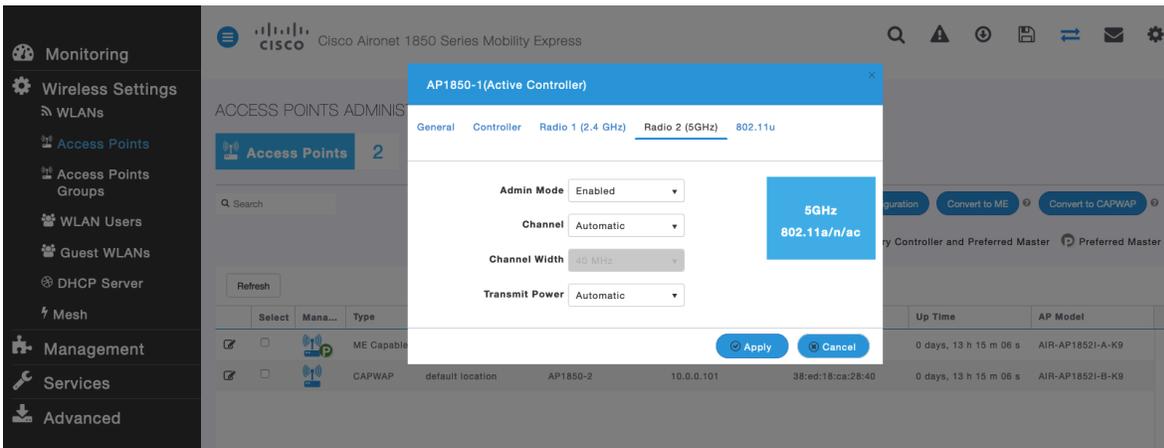
その他のアクセスポイントは、自動割り当てメソッドと、静的に設定したアクセスポイントのアカウントに対して有効化できます。

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 チャンネル幅は、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ンネル 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ン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。

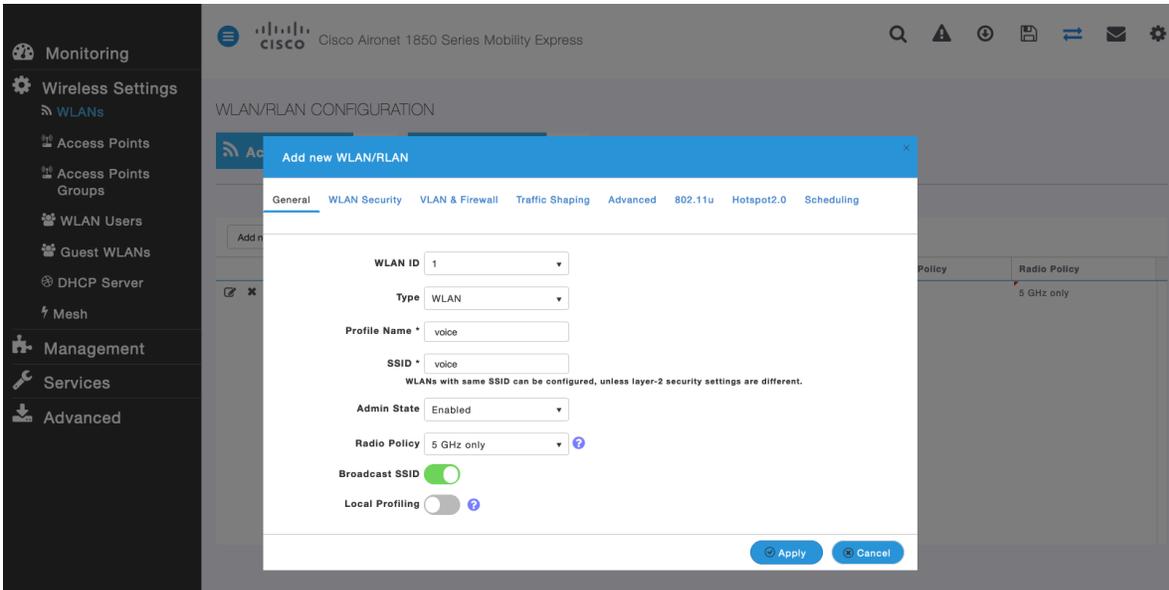
しかし、音声対応 Cisco ワイヤレス LAN エンドポイントをサポートするように設定された既存の SSID を使用することもできます。

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

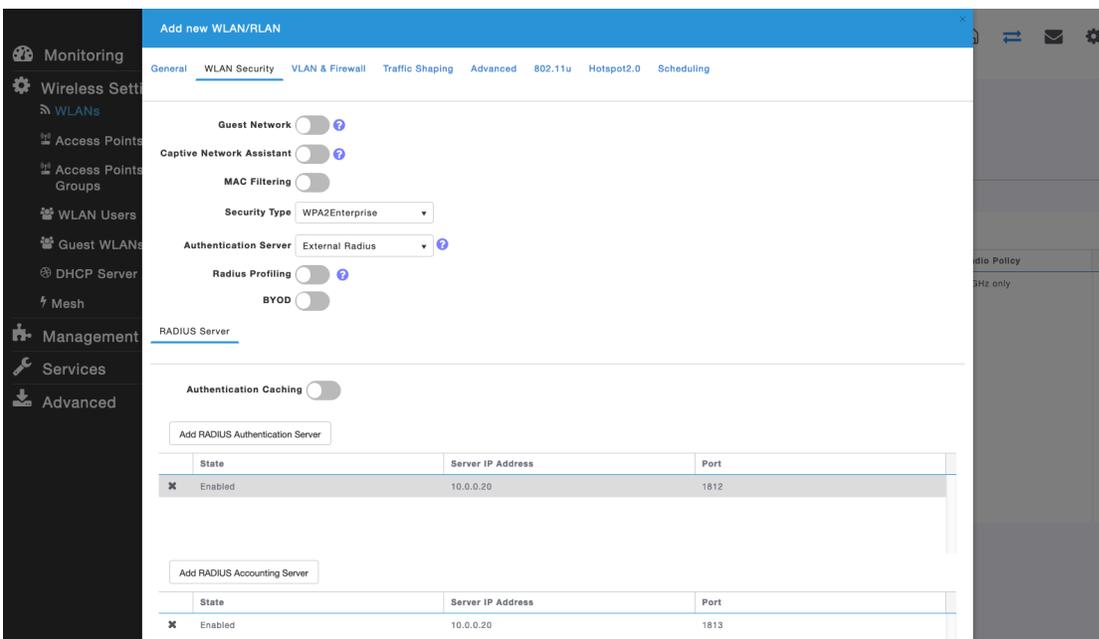
Cisco Desk Phone 9800 シリーズは 5 GHz 帯域のみで運用することを推奨します。利用できるチャンネル数が多く、2.4 GHz 帯域に比べて干渉が少ないためです。

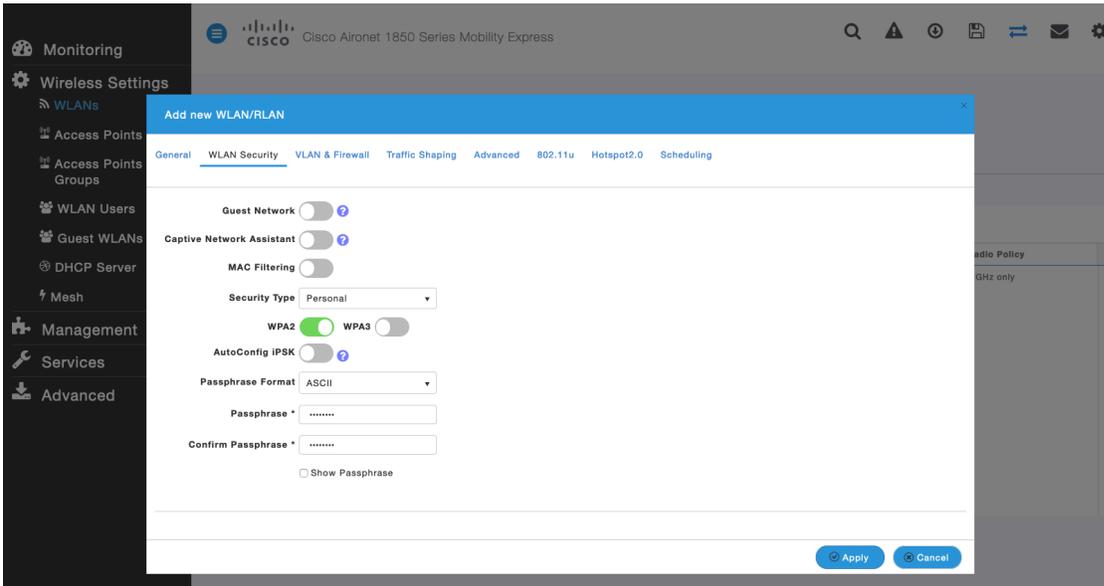
Cisco Desk Phone 9800 シリーズワイヤレス LAN 導入ガイド

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。



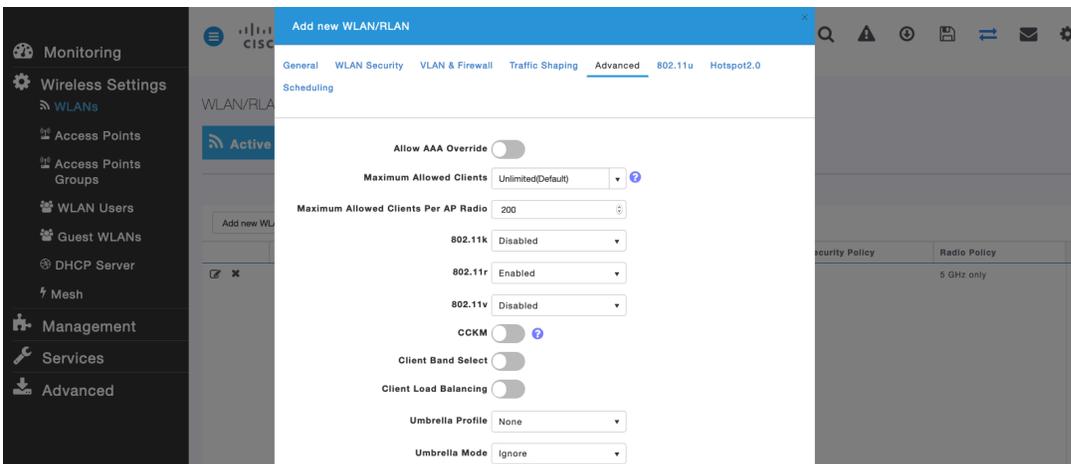
高速セキュア ローミングに 802.11r (FT) を使用するには、**セキュリティタイプ** を選択します。WPA2-エンタープライズ または パーソナル 802.1x または PSK/SAE のどちらを使用するかによって異なります。





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

State	Server IP Address	Port
✖ Enabled	10.0.0.20	1813

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

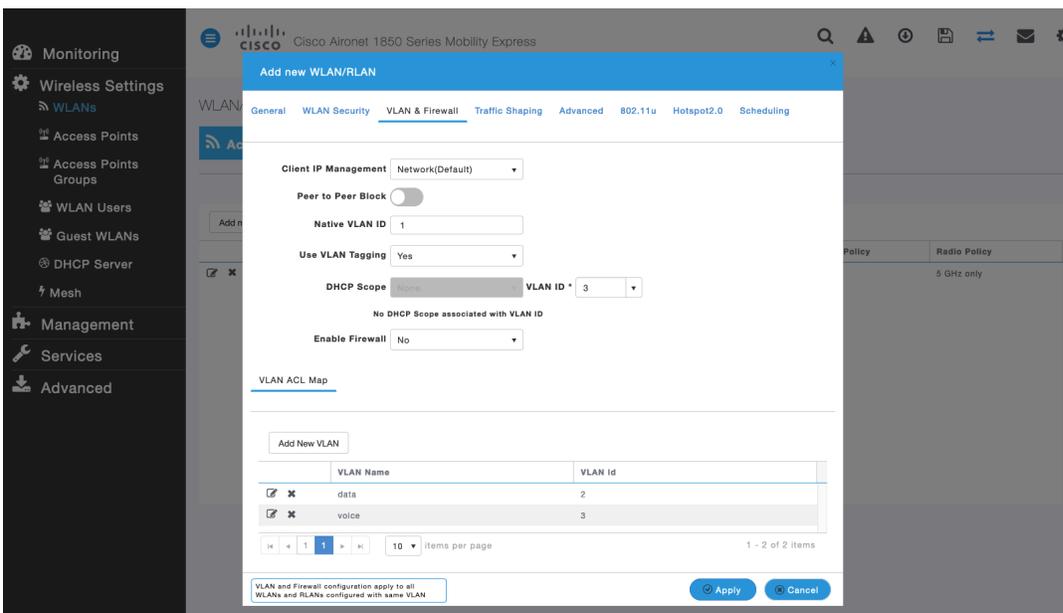
Add RADIUS Authentication Server

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

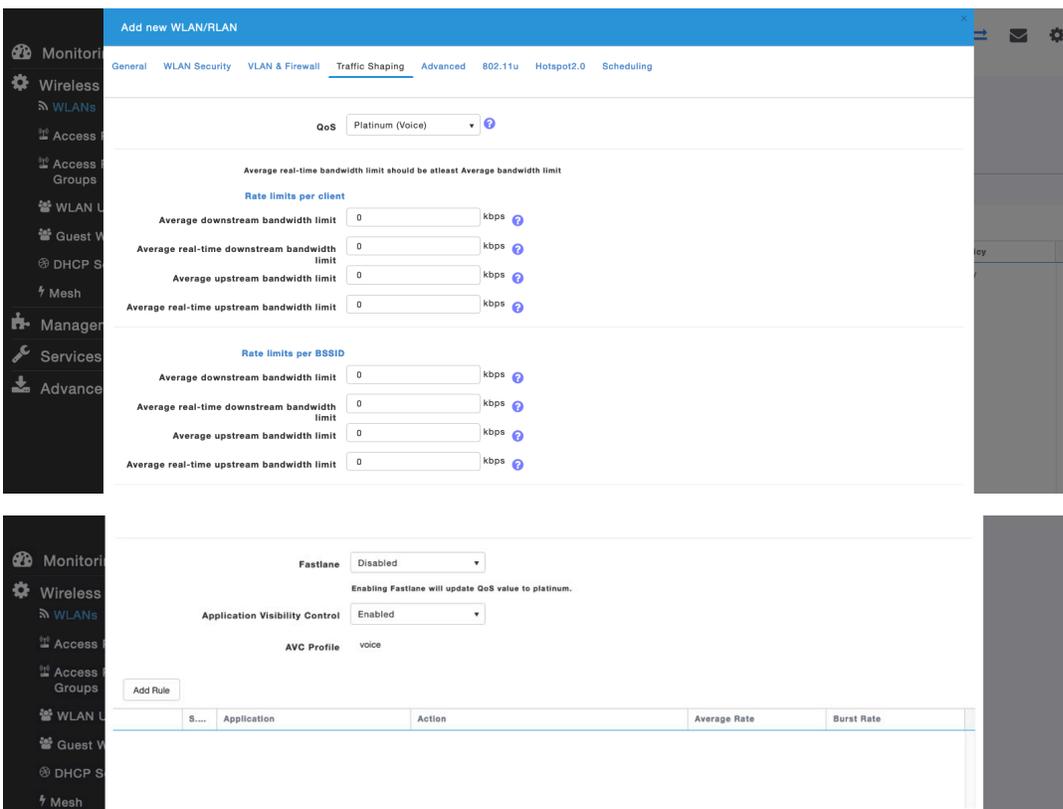
Add RADIUS Accounting Server

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

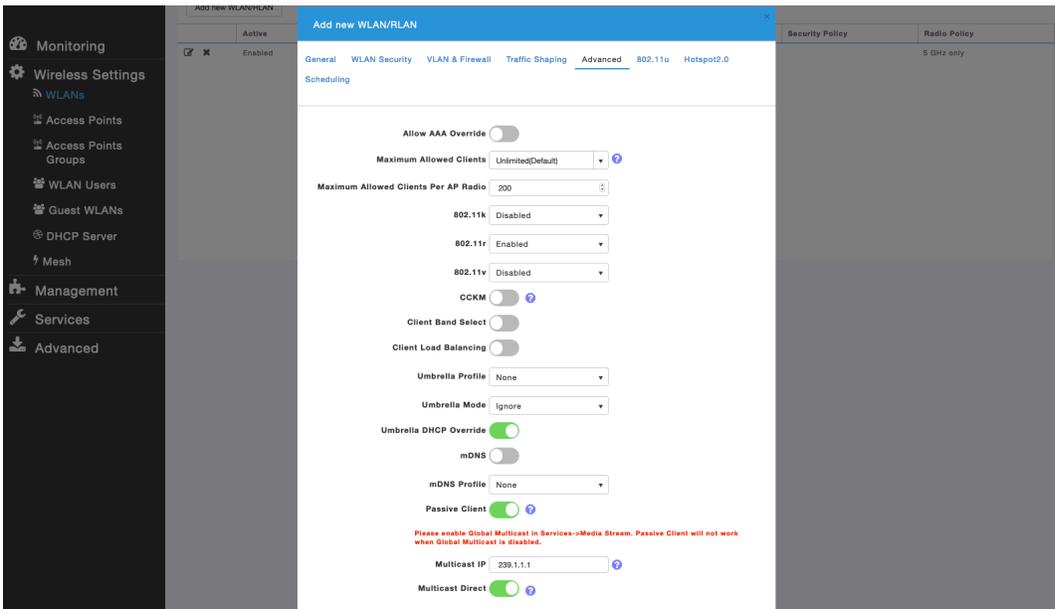
必要に応じて、WLAN のネイティブ VLAN ID と VLAN ID を設定します。
[ピアツーピアブロック (Peer to Peer Block)] を無効にします。



[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。

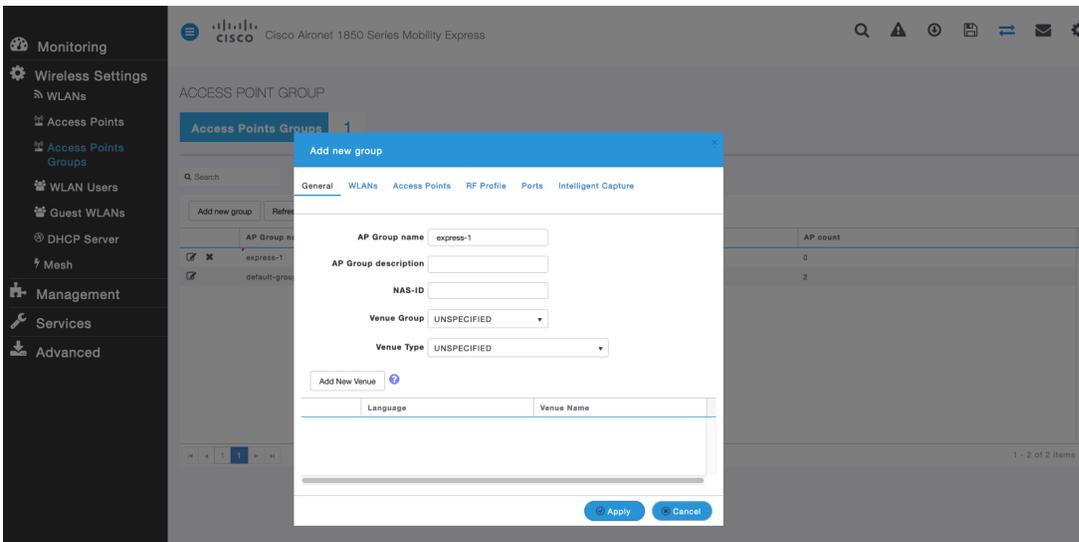


最大クライアント数 と AP 無線ごとの最大許容クライアント は必要に応じて設定します。

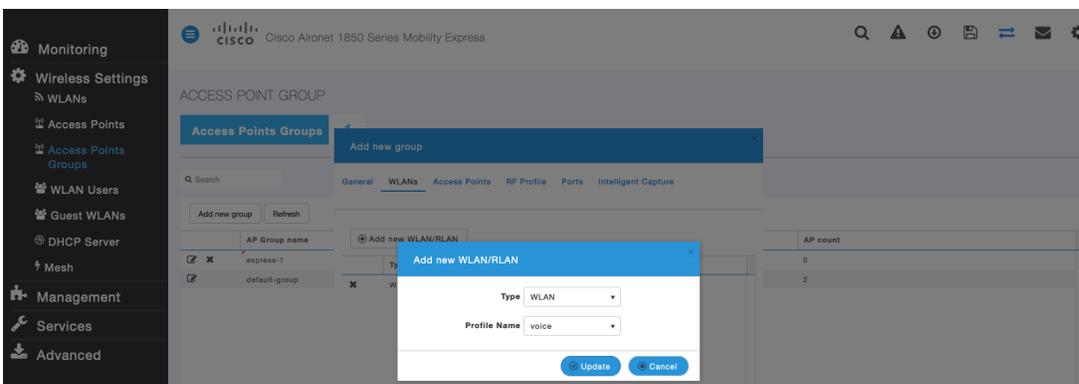


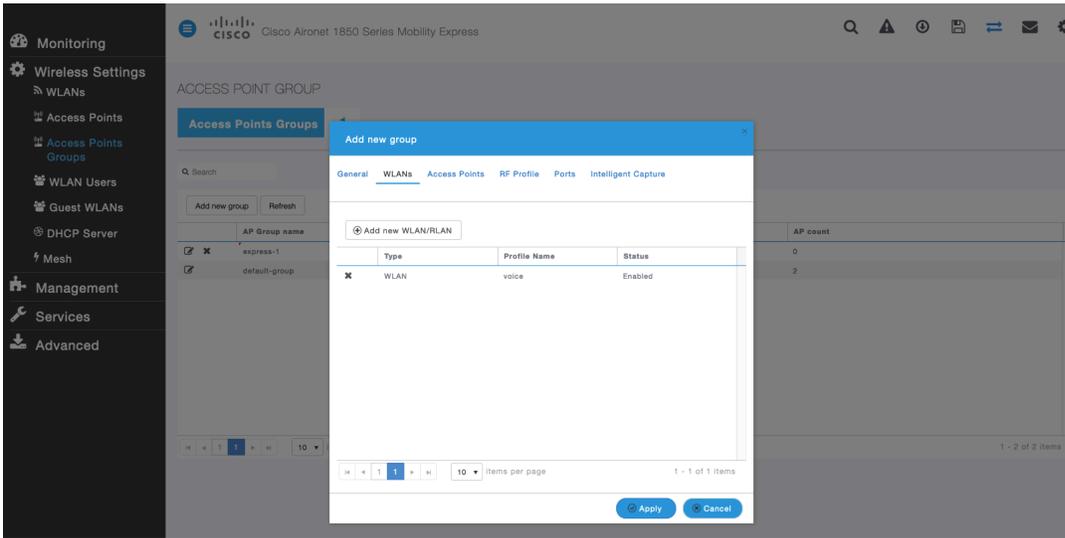
AP グループ

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。

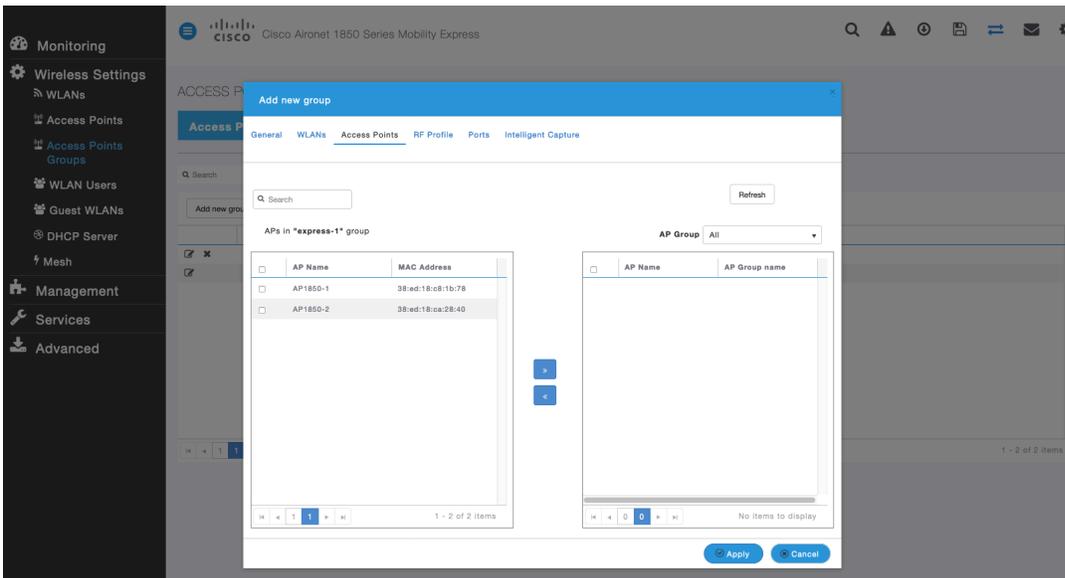


[WLAN (WLANs)] タブで、目的の WLAN とマッピングするインターフェイスを選択して、[追加 (Add)] を選択します。

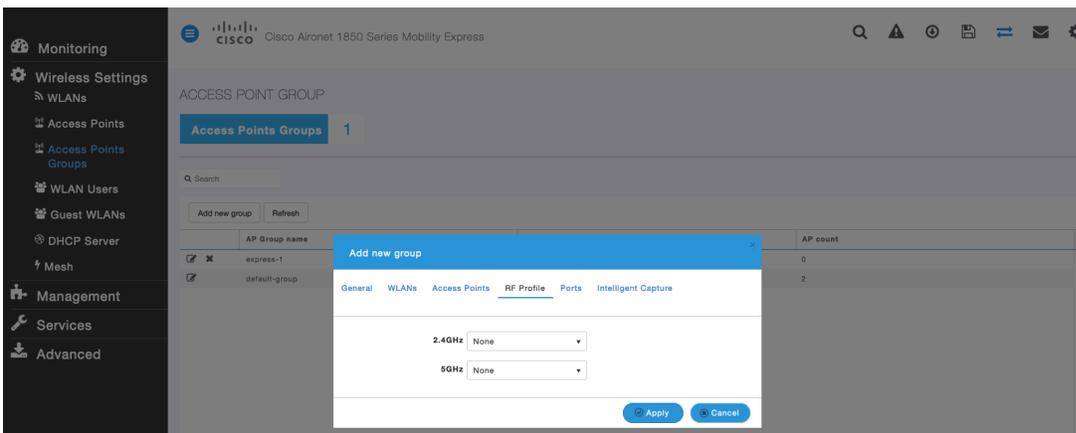




[アクセスポイント (Access Points)] タブで、目的のアクセスポイントを選択し、[適用 (Apply)] を選択します。次に、これらのアクセスポイントをリポートします。



[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。

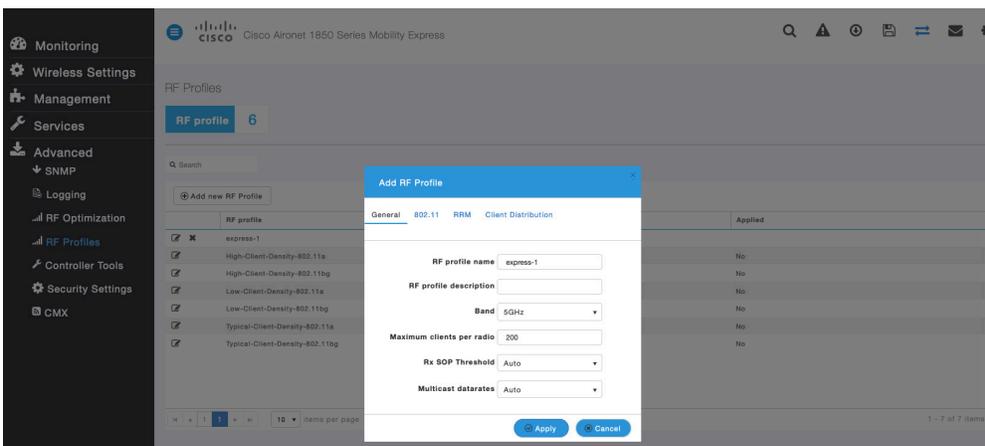
Cisco デスク フォン 9800 シリーズで使用される SSID については、5 GHz 無線にのみ適用することを推奨します。いったん作成されると、RF プロファイルは AP グループに適用されます。

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。

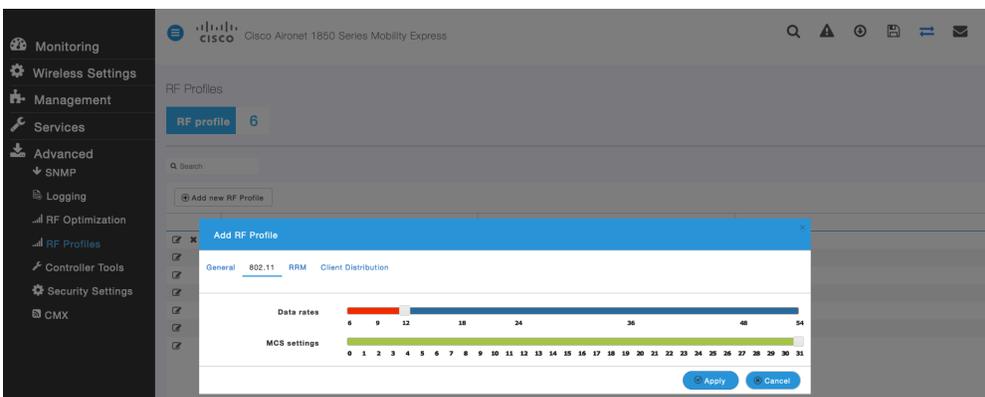
必要に応じて、[無線ごとの最大クライアント数 (Maximum clients per radio)]、[マルチキャストデータレート (Multicast data rates)]、[Rx Sopしきい値 (Rx Sop Threshold)] を設定します。

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

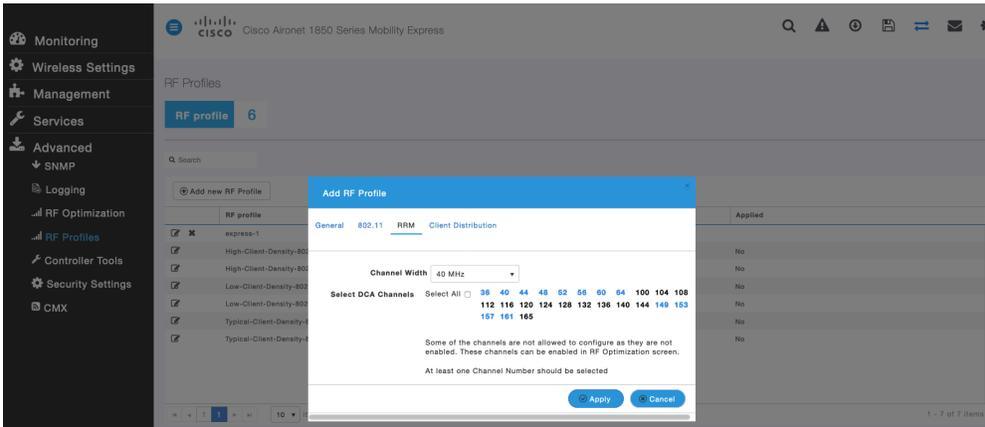


[802.11] タブで、必要に応じてデータレートを設定します。

12 Mbps 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。

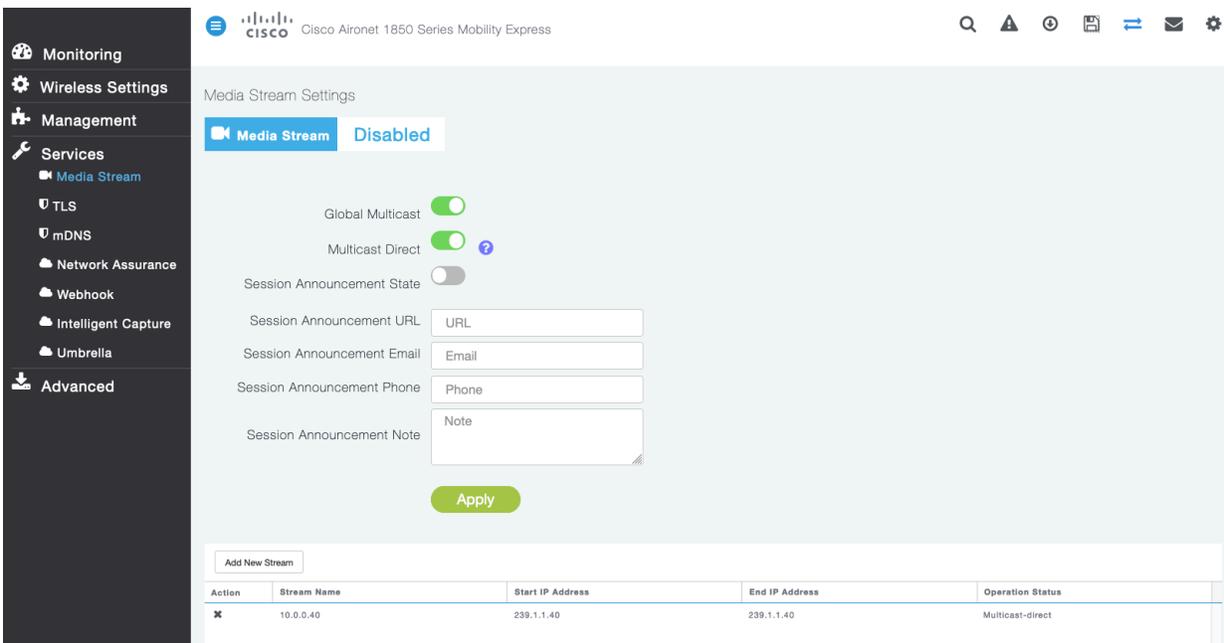


[RRM] タブで、[チャンネル幅 (Channel Width)] 設定と [DCA チャンネル (DCA Channels)] を構成できます。



マルチキャストダイレクト

[メディアストリーム (Media Stream)]設定で、[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

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 ?

Security Policy

Radio Policy

5 GHz only

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。利用できるチャンネル数が多く、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。

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

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、最大 12 チャン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ン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 チャンネル (チャンネル 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ン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 チャンネル幅は、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ン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

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

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

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

Enable Radio: Enable Disable

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

Role in Radio Network:

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

Max-Client: enable disable (1-255)

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

Data Rates:

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

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

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

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

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

DefaultRadio Channel: Channel 36 5180 MHz

Dynamic Frequency Selection Bands:

Channel Width: 20 MHz

World Mode Multi-Domain Operation: Disable Legacy Dot11d

Country Code: Indoor Outdoor

Radio Preamble: Short Long

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

Internal Antenna Configuration: Enable Disable

Antenna Gain(dBi): (-128 - 128)

Gratuitous Probe Response(GPR): Enable Disable

Period(Kusec): (10-255)

Transmission Speed:

Traffic Stream Metrics: Enable Disable

Aironet Extensions: Enable Disable

Ethernet Encapsulation Transform: RFC1042 802.1H

Reliable Multicast to WGB: Disable Enable

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

Beacon Privacy Guest-Mode: Enable Disable

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

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

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

Root Parent Timeout: (0-65535 sec)

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

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

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

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

2.4 GHz を使用するには、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 無線タイプのみにも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。

The screenshot shows the Cisco configuration interface for a wireless access point (ap-1). The main menu includes: HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY (selected), SERVICES, MANAGEMENT, SOFTWARE, and EVENT LOG. The left sidebar lists various security and management tools. The main content area is titled "Security: Global SSID Manager" and shows the configuration for a specific SSID named "voice".

SSID Properties

Current SSID List

< NEW >	SSID:	voice
data	VLAN:	3 Define VLANs
voice	Band-Select:	<input type="checkbox"/> Band Select
	Universal Admin Mode:	<input type="checkbox"/> Universal Admin Mode
	Interface:	<input type="checkbox"/> Radio0-802.11N2.4GHz <input checked="" type="checkbox"/> Radio1-802.11AC5GHz

Network ID: (0-4096)

[Delete](#)

Client Authentication Settings

Methods Accepted:

- Open Authentication: with EAP
- Web Authentication
- Web Pass
- Shared Authentication: < NO ADDITION >
- Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

- Use Defaults [Define Defaults](#)
- Customize

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

MAC Authentication Servers

- Use Defaults [Define Defaults](#)
- Customize

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

Client Authenticated Key Management

Key Management: Mandatory CCKM Enable WPA WPAv2 dot11r

WPA Pre-shared Key: ASCII Hexadecimal
11w Configuration:
11w Association-comeback: (1000-20000)
11w Saquery-retry: (100-500)

IDS Client MFP

Enable Client MFP on this SSID:

AP Authentication

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

Accounting Settings

Enable Accounting

Accounting Server Priorities:
 Use Defaults [Define Defaults](#)
 Customize

Priority 1:
Priority 2:
Priority 3:

Rate Limit Parameters

Limit TCP:

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

Limit UDP:

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

General Settings

Advertise Extended Capabilities of this SSID

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

Enable IP Redirection on this SSID

IP Address:

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

Association Limit (optional): (1-255)

EAP Client (optional):
 Username: Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

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

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

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

Multiple BSSID

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

Radio1-802.11AC^{5GHz}:

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

Multiple BSSID

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

ワイヤレス音声とデータを個別の 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。

Save Configuration | Ping | Logout | Refresh

CISCO HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

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

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

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

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

VLAN ID: (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N^{2.4GHz}

Radio1-802.11AC^{5GHz}

Management VLAN (if non-native)

VLAN Information

View Information for:

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

暗号化タイプで [AES] が選択されていることを確認します。

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

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 3 [Define VLANs](#)

Encryption Modes

None

WEP Encryption Optional

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

Cipher AES CCMP

Encryption Keys

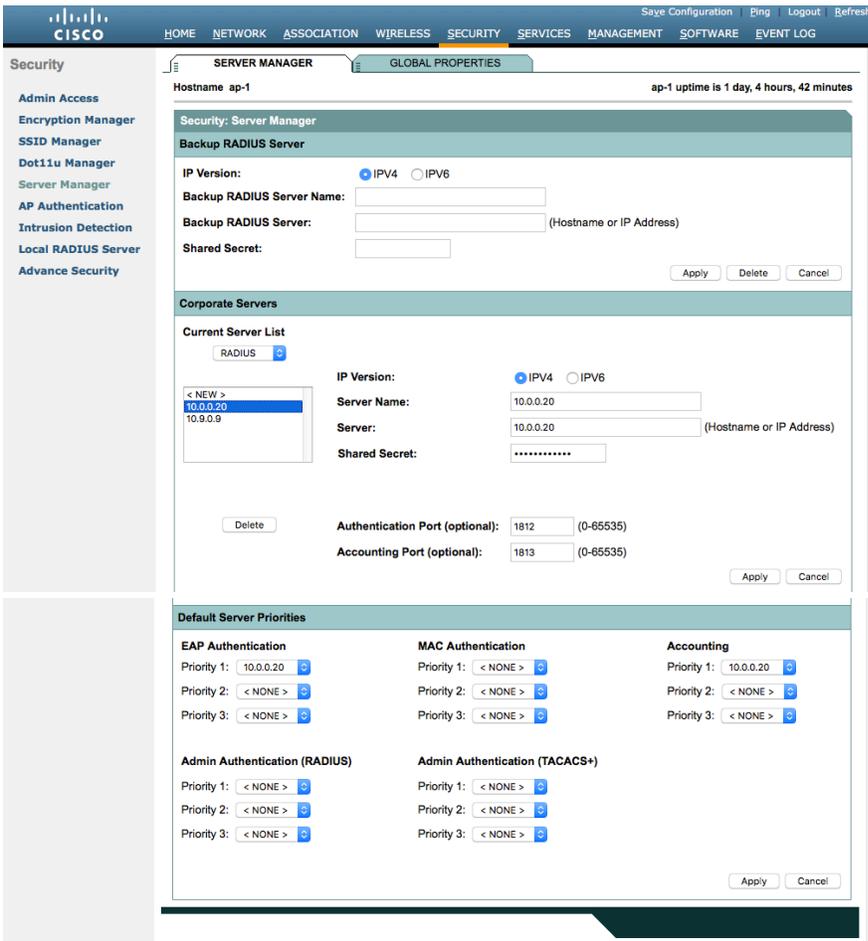
	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>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

Global Properties

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

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

認証とアカウントのために RADIUS サーバーを設定します。

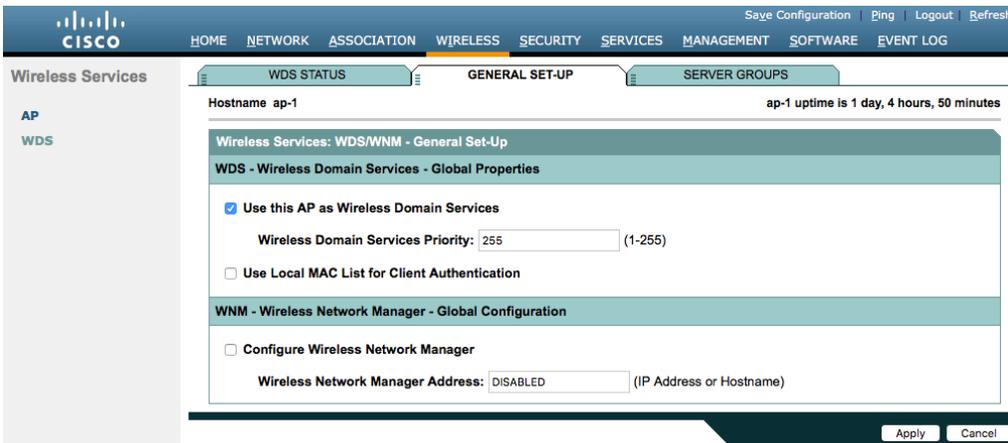


ワイヤレス ドメイン サービス (WDS)

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。

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

Current VLAN List

- < NEW >
- VLAN 2
- VLAN 3
- VLAN 10

Create VLAN

VLAN ID: 10 (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N^{2.4GHz}

Radio1-802.11AC^{5GHz}

Management VLAN (if non-native)

Apply Cancel

VLAN Information

View Information for: VLAN 2

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

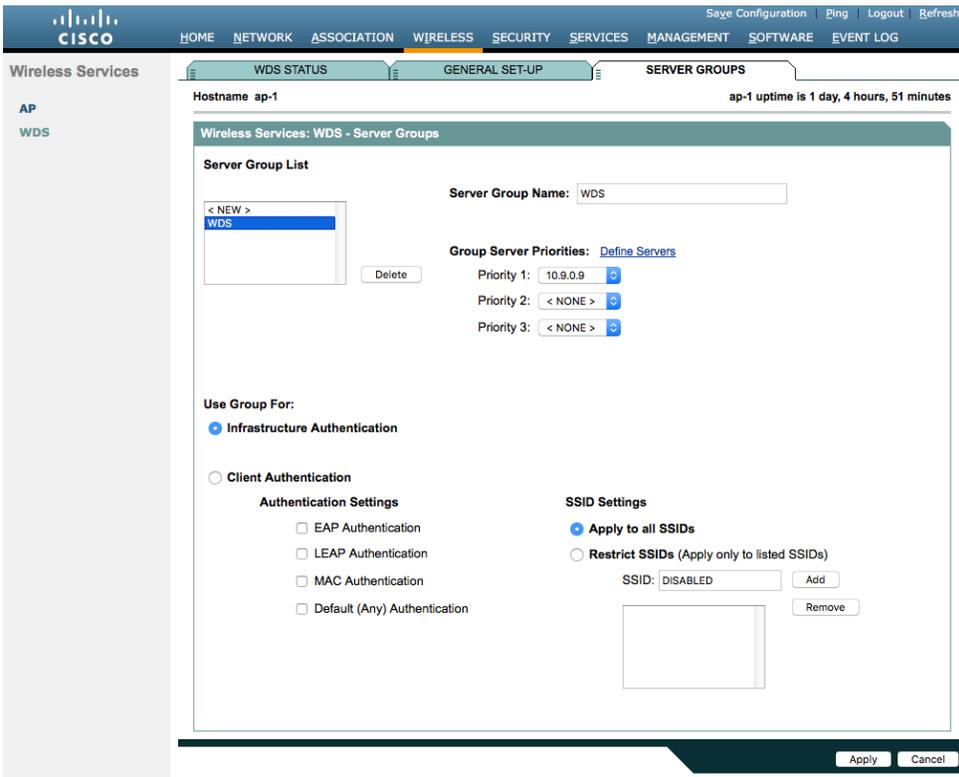
Refresh

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。

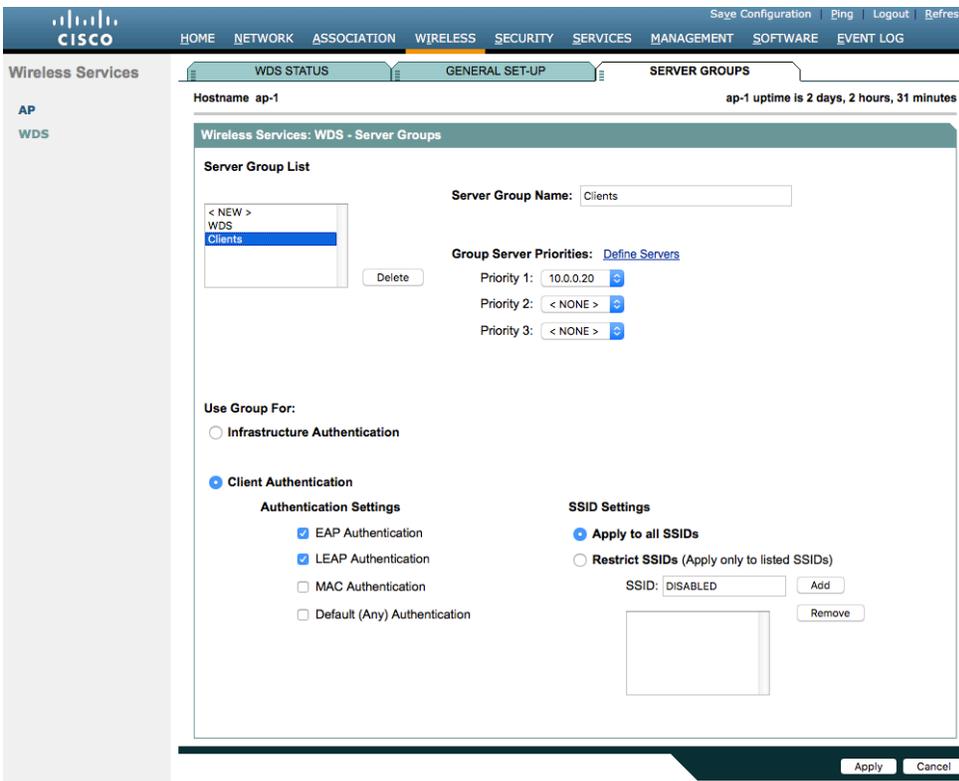
インフラストラクチャ認証にはローカル RADIUS の使用が推奨されます。

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。

The screenshot shows the Cisco configuration interface for a Local RADIUS Server. The interface is divided into several sections:

- Security: Local RADIUS Server - General Set-Up**
 - Local Radius Server Authentication Settings**
 - Enable Authentication Protocols: EAP FAST, LEAP, MAC
 - Buttons: Apply, Cancel
 - Network Access Servers (AAA Clients)**
 - Current Network Access Servers: A list containing 10.9.0.9 with a Delete button.
 - Network Access Server: 10.9.0.9 (IP Address)
 - Shared Secret: [Redacted]
 - Buttons: Apply, Cancel
 - Individual Users**
 - Current Users: A list containing wds with a Delete button.
 - Username: wds
 - Password: [Redacted] (Text/NT Hash options)
 - Confirm Password: [Redacted]
 - Group Name: < NONE >
 - MAC Authentication Only:
 - Buttons: Apply, Cancel
 - User Groups**
 - Current User Groups: A list with a Delete button.
 - Group Name: [Redacted]
 - Session Timeout (optional): [Redacted] (1-4294967295 sec)
 - Failed Authentications before Lockout (optional): [Redacted] (1-4294967295)
 - Lockout (optional): Infinite, Interval [Redacted] (1-4294967295 sec)
 - VLAN ID (optional): [Redacted]
 - SSID (optional): [Redacted] (Add/Delete buttons)
 - Buttons: Apply, Cancel

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。

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

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

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。

Save Configuration Ping Logout Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

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

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

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

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: Voice

Policy Name: Voice

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

Delete Classification

Match Classifications:

IP Precedence: Routine (0)

IP DSCP: Best Effort (0-63)

IP Protocol 119

Filter: No Filters defined. [Define Filters.](#)

Default Classification for Packets on the VLAN: Best Effort (0)

Rate Limiting:

Bits per Sec.: (8000-2000000000) Burst Rate (Bytes): (1000-512000000)

Conform Action: Transmit Exceed Action: Drop

Apply Delete Cancel

Apply Policies to Interface/ VLANs

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

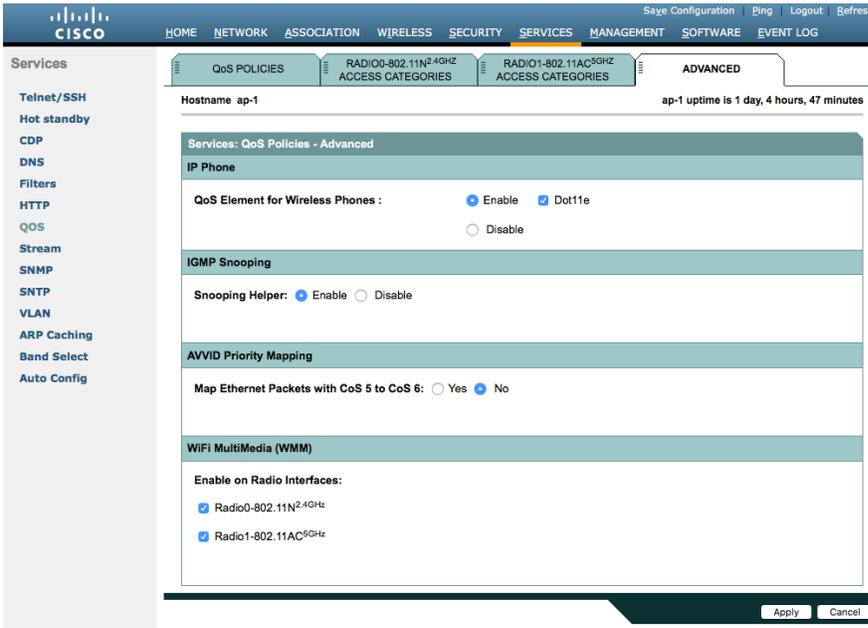
Apply Cancel

QBSS を有効にするには、[有効にする] 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。

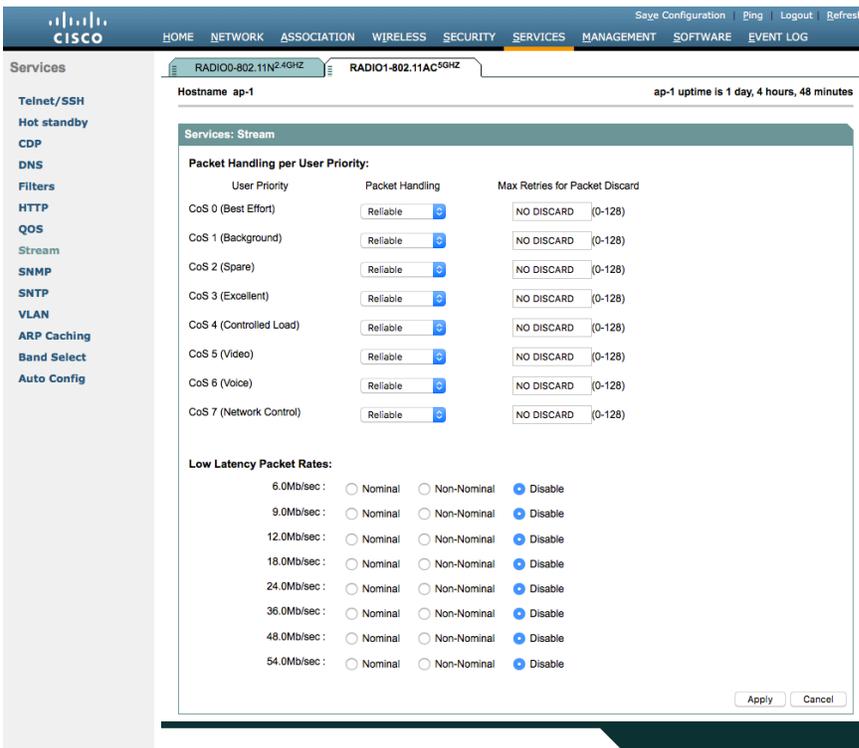
IGMP スヌーピング が有効になっていることを確認してください。

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 (Optimize d Voice)] を介するか、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。

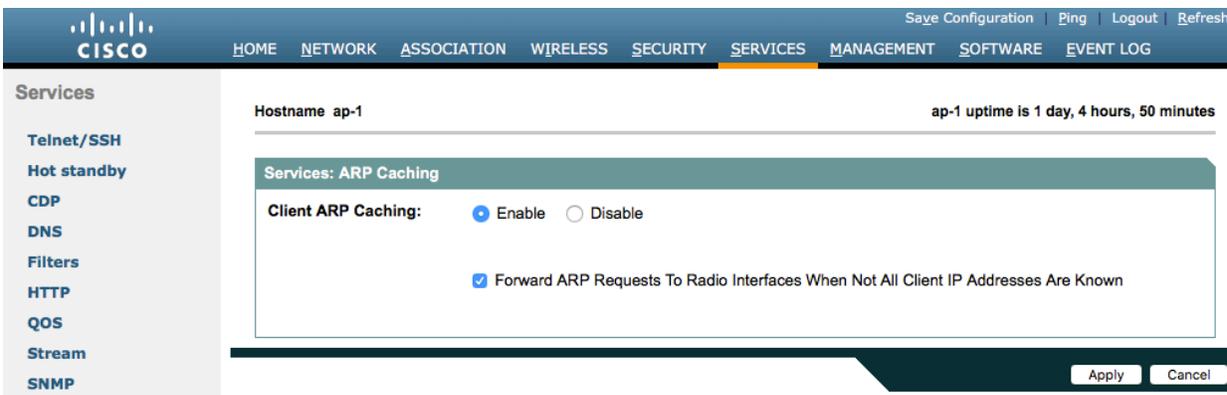


電源管理

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。

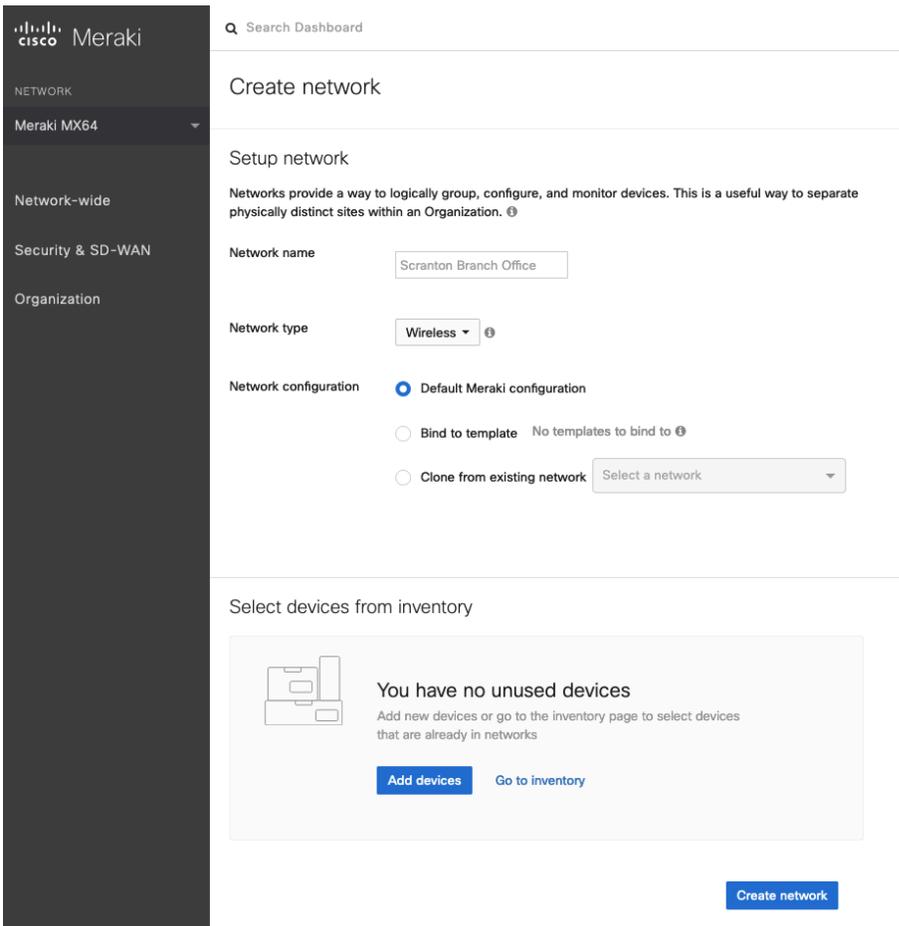
- [WPA2/WPA3-Enterprise] または [事前共有キー (Pre-shared key)] に対して [802.11r] を有効にします。
- [スプラッシュページ (Splash page)] を [なし (None)] に設定します
- [ブリッジモード (Bridge mode)] を有効にします
- VLAN タグ付けを有効にする
- [帯域 (Band)] の選択 を [5 GHz帯のみ (5 GHz band only)] に設定します
- 必要に応じて データレート を設定します
- [Quality of Service (QoS)] を設定します

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、[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。

Claim by serial and/or order number

Enter one or more serial/order numbers (one per row). [Where can I find these numbers?](#)

Close Claim

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。

Search Dashboard

Configuration overview

Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)

meraki-voice	
Enabled	<input type="button" value="enabled"/>
Name	rename
Access control	edit settings
Encryption	802.1X with Meraki RADIUS
Sign-on method	None
Bandwidth limit	unlimited
Client IP assignment	Local LAN
Clients blocked from using LAN	no
Wired clients are part of Wi-Fi network	no
VLAN tag ⓘ	3
VPN	Disabled
Splash page	
Splash page enabled	no
Splash theme	n/a

[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (Access control)] ページの順に選択し、[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。

Search Dashboard

Access control

SSID: meraki-voice

Network access

Association requirements

- Open (no encryption)
Any user can associate
- Pre-shared key (PSK)
Users must enter a passphrase to associate
- MAC-based access control (no encryption)
RADIUS server is queried at association time
- Enterprise with Meraki Cloud Authentication
User credentials are validated with 802.1X at association time

WPA encryption mode: WPA2 only (recommended for most deployments)

802.11r ⓘ: Enabled

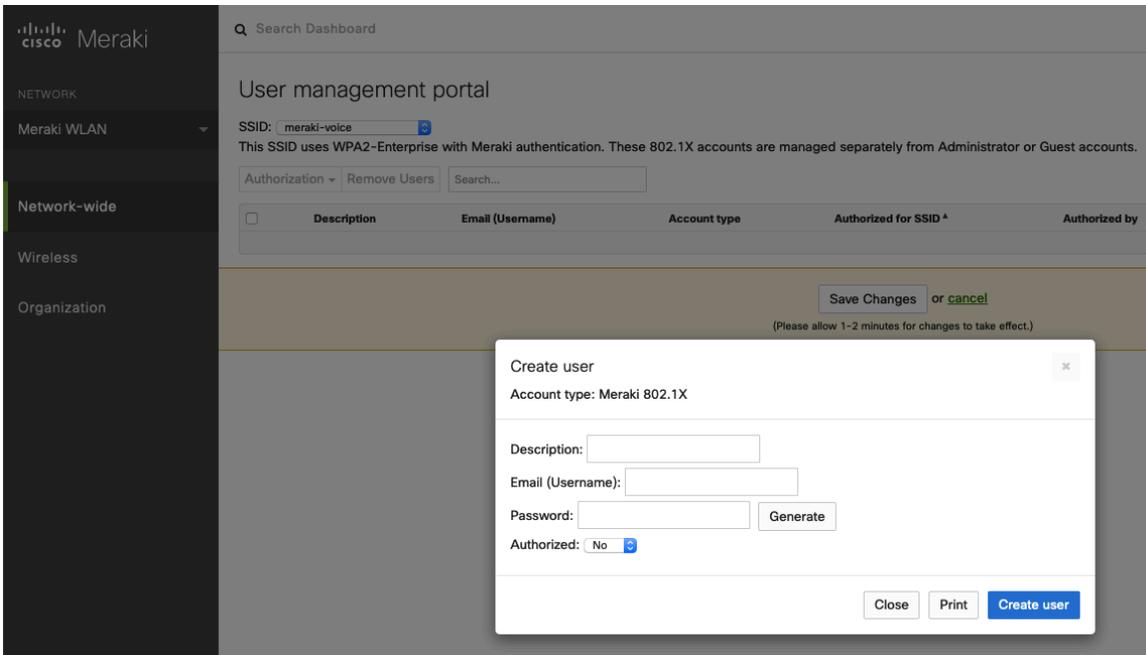
802.11w ⓘ: Disabled (never use)

Splash page

- None (direct access)
Users can access the network as soon as they associate

[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。

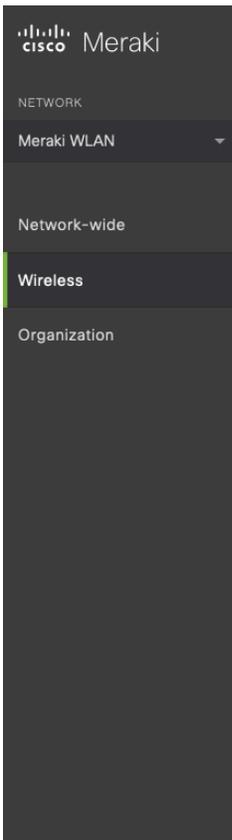
VLAN タギングが利用される場合、Cisco Meraki アクセス ポイントが VLAN を許可するトランク モードに設定されたスイッチ ポートに接続されていることを確認してください。

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
```



Addressing and traffic

Client IP assignment

- NAT mode: Use Meraki DHCP
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.
- Bridge mode: Make clients part of the LAN
Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras.
- Layer 3 roaming
Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client roams to an AP where their original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.
- Layer 3 roaming with a concentrator
Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
- VPN: tunnel data to a concentrator
Meraki devices send traffic over a secure tunnel to an MX concentrator.

VLAN tagging ⓘ Bridge mode and layer 3 roaming only

Use VLAN tagging

VLAN ID ⓘ

AP tags	VLAN ID	Actions
All other APs	<input type="text" value="3"/>	Add VLAN

[Add VLAN](#)

Content filtering ⓘ NAT mode only

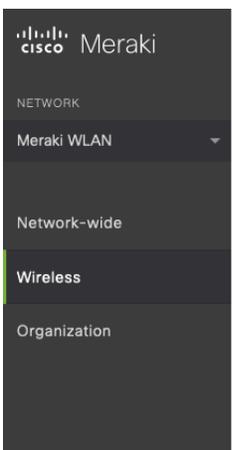
Don't filter content

Bonjour forwarding ⓘ Bridge mode and layer 3 roaming only

Enable Bonjour Gateway

There are no Bonjour forwarding rules on this network.
[Add a Bonjour forwarding rule](#)

[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (Access control)] ページの順に選択し、必要に応じて、Cisco Desk Phone 9800 シリーズが使用する SSID の周波数帯域を設定します。2.4 GHz 帯域と比較してチャンネルが多く、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。



Wireless options

Band selection and minimum bitrate settings may be overridden by RF profiles.

Band selection

- Dual band operation (2.4 GHz and 5 GHz)
- 5 GHz band only
5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.
- Dual band operation with Band Steering
Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

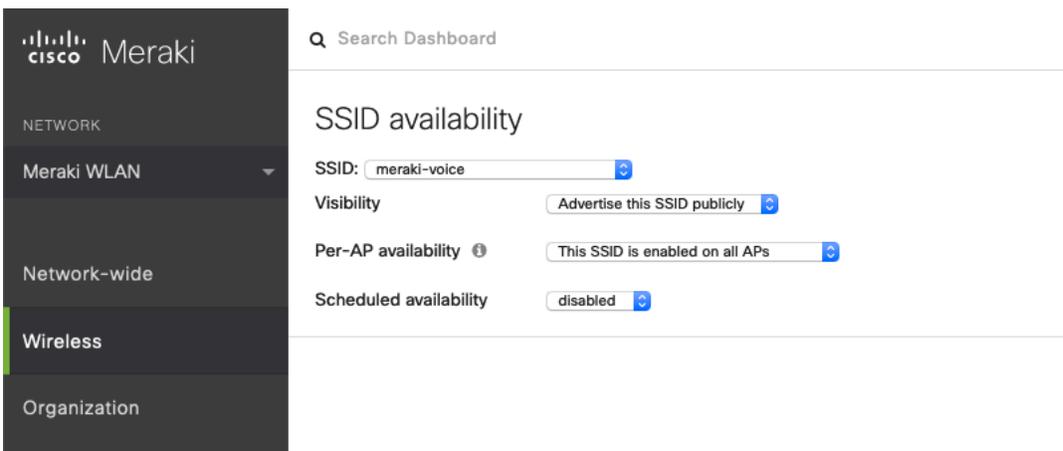
Minimum bitrate (Mbps) ⓘ



[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。



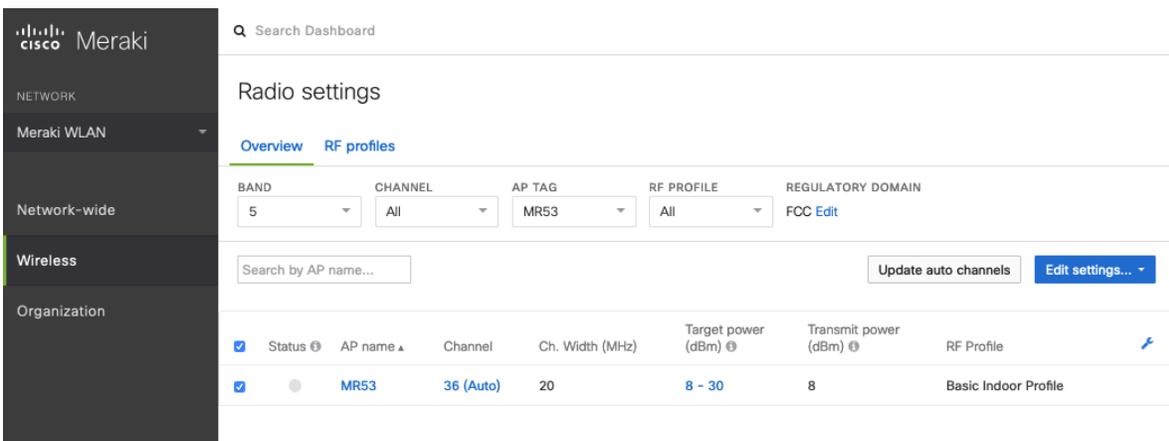
無線設定

[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ン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、チャンネルと送信電力に [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 無線の静的チャン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ン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。

The image displays two screenshots of the Cisco Meraki dashboard, specifically the 'Edit Basic Indoor Profile' page. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled 'Edit Basic Indoor Profile' and has tabs for 'General', '2.4 GHz', and '5 GHz'. The 'General' tab is active, showing 'Band selection' set to 'Per SSID' and 'Client balancing' set to 'Off'. Below this, there are two sections: 'Minimum bitrate configuration' and 'Client balancing'. In the top screenshot, 'Minimum bitrate configuration' is set to 'Per band'. In the bottom screenshot, it is set to 'Per SSID'. A note below the 'Band selection' section states: 'The Access Points configured to use this profile will follow the band selection set on the [Access Control page](#) for the respective SSID. date.'

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

2.4 GHz 無線は 20 MHz チャンネル幅を使用し、他のチャン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ンネル幅を使用することを推奨します。

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

[AutoChannel] が使用する 2.4 GHz チャンネルは、チャンネル 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。

General 2.4 GHz 5 GHz

5 GHz radio settings

Turn off 5GHz radio See band selection above.

Channel width

Manual 5 GHz channel width

Disable auto channel width by manually selecting a channel width for the APs in this profile.

20 MHz (19 channels)
Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.

40 MHz (10 channels)
For low to medium density deployments.

80 MHz (5 channels)
For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

Channel assignment method AutoChannel will assign radios to channels with low interference.
[Change channels used by AutoChannel...](#)

Radio transmit power range (dBm) Transmit shorter distance Transmit farther

[Set RX-SOP...](#)

Minimum bitrate Lower Density Higher Density

Change 5 GHz channels used by AutoChannel

Available channels for AutoChannel
If you deselect a channel, AutoChannel will not assign it to any AP with this profile. Click on a channel to toggle its selection.

	UNII-1				UNII-2				UNII-2-Extended				Weather Radar				UNII-3				ISM				
20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
80 MHz	42				58				106				122				138				155				

DFS channels

For low to medium density deployments.

80 MHz (5 channels)
For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

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。

The screenshot shows the Cisco Meraki dashboard interface. On the left is a navigation sidebar with 'Wireless' selected. The main content area is titled 'Firewall & traffic shaping' and is filtered for the 'meraki-voice' SSID. It contains three sections: 'Block IPs and ports' with a table of Layer 3 firewall rules, 'Block applications and content categories' with a message that no Layer 7 rules are defined, and 'Traffic shaping rules' with sliders for bandwidth limits and a dropdown for shaping traffic.

Search Dashboard

Firewall & traffic shaping

SSID: meraki-voice

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
	Allow	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules: There are no rules defined for this SSID.

[Add a layer 7 firewall rule](#)

Traffic shaping rules

Per-client bandwidth limit: unlimited [details](#) Enable SpeedBurst

Per-SSID bandwidth limit: unlimited [details](#)

Shape traffic: Shape traffic on this SSID

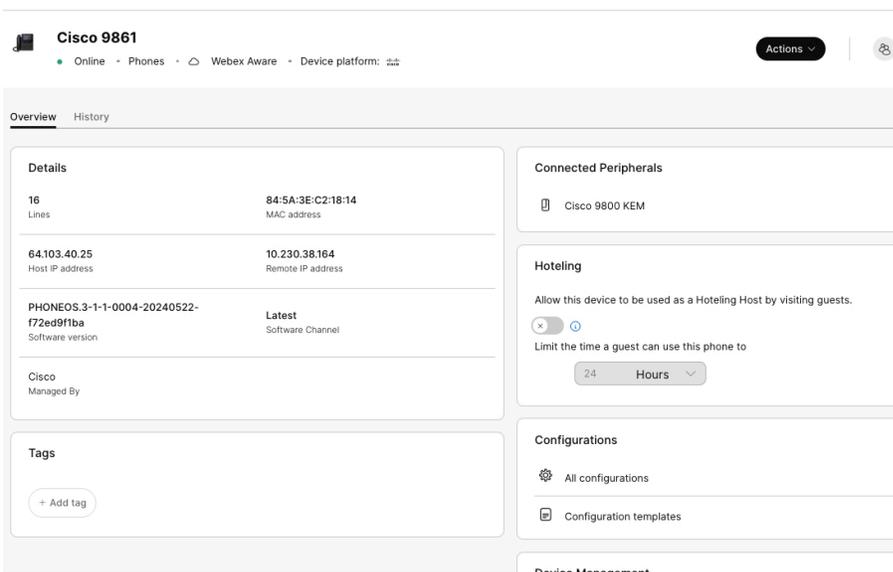
Cisco 通話制御を設定する

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。

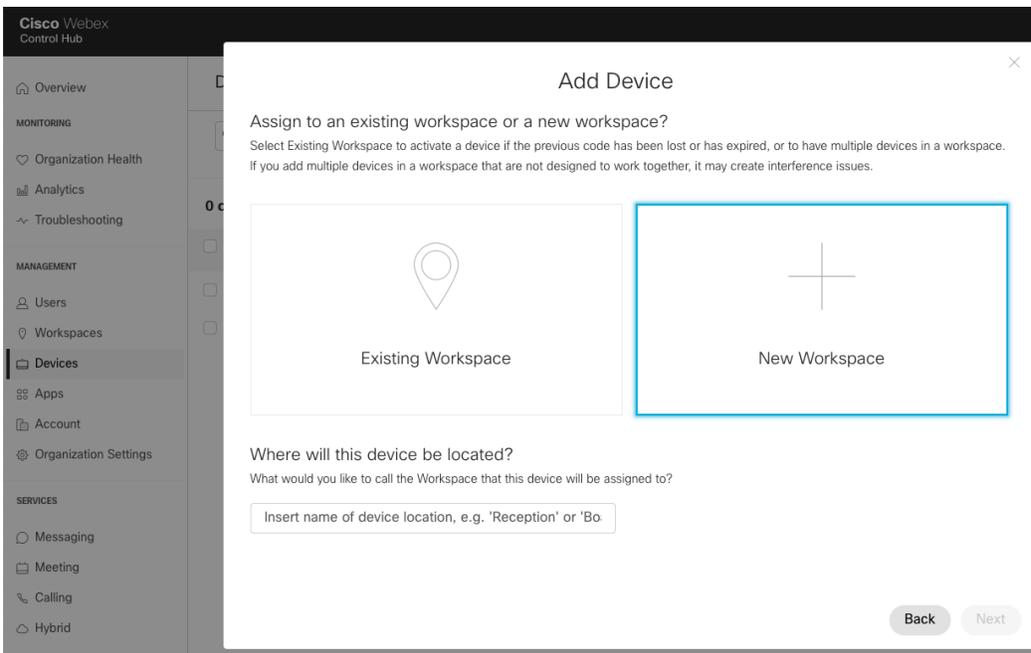
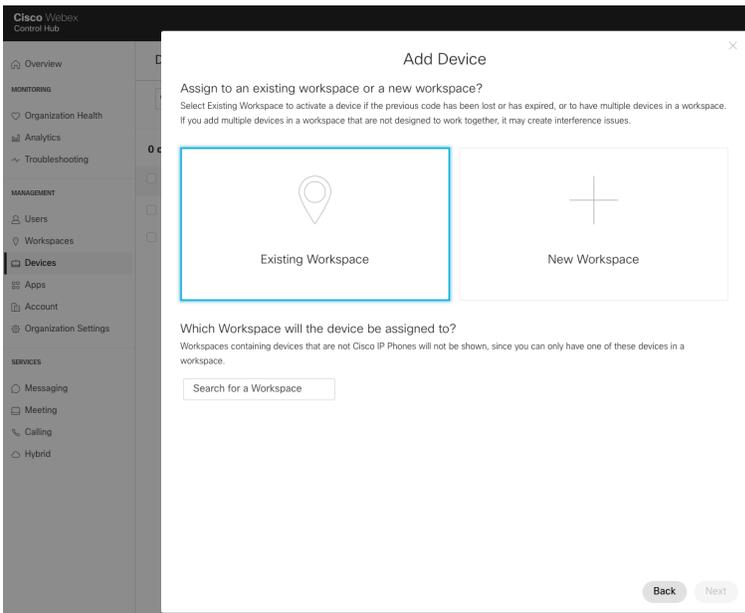
個人使用

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。



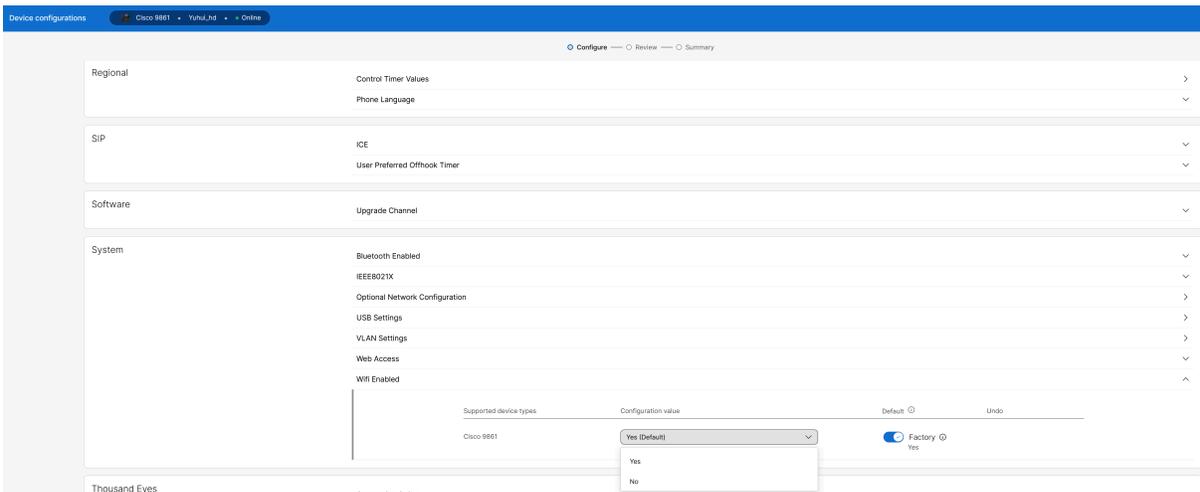
ワークスペース利用

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。

Device Information

Device is trusted

MAC Address*

Description

Device Pool* [View Details](#)

Common Device Configuration [View Details](#)

Phone Button Template* [View Details](#)

Softkey Template [View Details](#)

Common Phone Profile* [View Details](#)

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。

Wi-Fi*

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。

Parameter Name	Parameter Value	Suggested Value
Cluster ID *	StandAloneCluster	StandAloneCluster
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
Auto Registration Legacy Mode *	False	False
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	Disabled	Disabled
Services Provisioning *	Internal	Internal
Feature Control Policy	< None >	
Wi-Fi Hotspot Profile	< None >	
IMS Inter Operator Id *	IMS Inter Operator Identification	IMS Inter Operator Identification
URI Lookup Policy *	Case Sensitive	Case Sensitive

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。

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

Phone Security Profile Information

Product Type: Cisco 9871
Device Protocol: SIP

Name* Cisco 9871 - Standard SIP Secure Profile
Description Cisco 9871 - Standard SIP Secure Profile
Nonce Validity Time* 600
Device Security Mode Encrypted
Transport Type* TLS

Enable Digest Authentication
 TFTP Encrypted Config
 Enable OAuth Authentication

- 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。

Protocol Specific Information

Packet Capture Mode* None
Packet Capture Duration 0
BLF Presence Group* Standard Presence group
SIP Dial Rules < None >
MTP Preferred Originating Codec* 711ulaw
Device Security Profile* Cisco 9871 - Standard SIP Secure Profile
Rerouting Calling Search Space < None >
SUBSCRIBE Calling Search Space < None >
SIP Profile* Standard SIP Profile [View Details](#)
Digest User < None >

Media Termination Point Required
 Unattended Port
 Require DTMF Reception

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

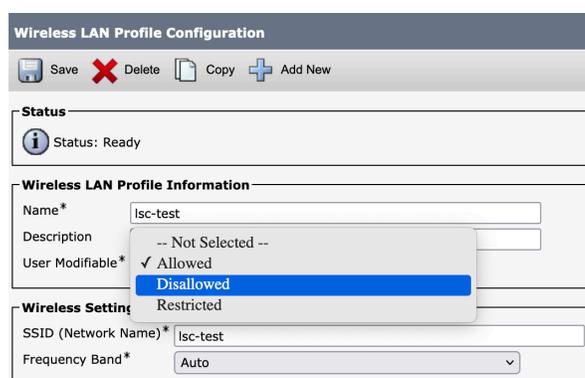
- ワイヤレス LAN プロファイルの名前を 50 文字以内で入力します。
- 必要に応じて説明を 63 文字以内で入力します。

Name*	<input type="text"/>
Description	<input type="text"/>

- **[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。

✖️: 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。

SSID (Network Name)*

- 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

Frequency Band*

- 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 Certificate) 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。

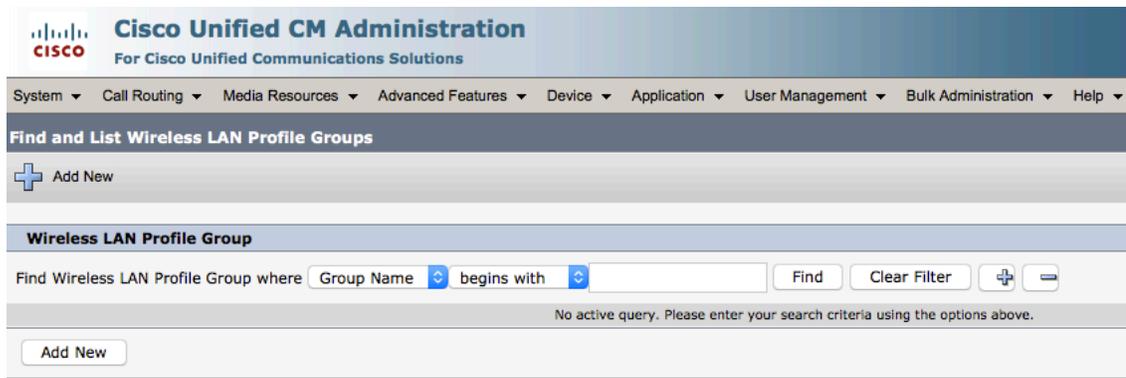
Authentication Method* None

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。

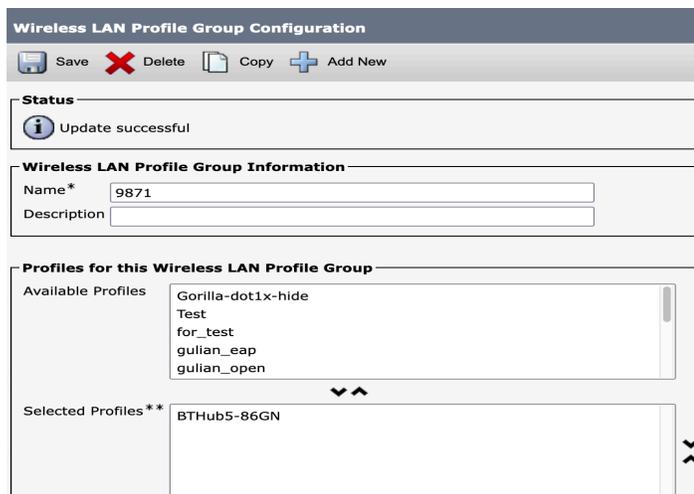
- Cisco Desk Phone 9800 シリーズは、ネットワークアクセスプロファイルオプションをサポートしていません。
- ワイヤレス LAN プロファイル構成が完了したら、**[保存 (Save)]** を選択します。

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。

Device Pool Settings	
Device Pool Name*	<input type="text" value="9871"/>
Cisco Unified Communications Manager Group*	<input type="text" value="Default"/>
Calling Search Space for Auto-registration	<input type="text" value="< None >"/>
Adjunct CSS	<input type="text" value="< None >"/>
Reverted Call Focus Priority	<input type="text" value="Default"/>
Intercompany Media Services Enrolled Group	<input type="text" value="< None >"/>
MRA Service Domain	<input type="text" value="< None >"/>

Roaming Sensitive Settings	
Date/Time Group*	<input type="text" value="ntp_server"/>
Region*	<input type="text" value="Default"/>
Media Resource Group List	<input type="text" value="< None >"/>
Location	<input type="text" value="< None >"/>
Network Locale	<input type="text" value="< None >"/>
SRST Reference*	<input type="text" value="Disable"/>
Connection Monitor Duration***	<input type="text"/>
Single Button Barge*	<input type="text" value="Default"/>
Join Across Lines*	<input type="text" value="Default"/>
Physical Location	<input type="text" value="< None >"/>
Device Mobility Group	<input type="text" value="< None >"/>
Wireless LAN Profile Group	<input type="text" value="9871"/> View Details

- 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。

Device Information

Device is Active

Device is trusted

MAC Address* 845A3EC211B6 (SEP845A3EC211B6)

Description Auto 99899

Current [On-Premise Onboarding Method](#) is set to Autoregistration. Activation Code will only apply to onboarding via MRA.

Require Activation Code for Onboarding

Allow Activation Code via MRA

Activation Code MRA Service Domain -- Not Selected -- [View Details](#)

Device Pool* 9871 [View Details](#)

Common Device Configuration < None > [View Details](#)

Phone Button Template* DocTest ModelID 118 Lines Button Template **Find**

Softkey Template < None >

Common Phone Profile* Standard Common Phone Profile [View Details](#)

- 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

The screenshot shows the 'Cisco IP Phone for 3rd Party Call Control DP-9871 Configuration Utility' web interface. The 'Wi-Fi Settings' section is expanded, showing the following configuration:

- Phone-wifi-on: Yes
- Wi-Fi Profile 1:
 - Network Name: xin-wpa3-23-SAE
 - Wi-Fi User ID: [empty]
 - Frequency Band: 5 GHz
 - Security Mode: PSK
 - Wi-Fi Password: [masked]

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。

The screenshot shows the 'Status' tab of the configuration utility. The 'System Information' section displays the following details:

- Host Name: SEP845A3EC2302B
- Domain: crd.cisco.com
- Primary NTP Server: 10.64.58.51
- Secondary NTP Server: [empty]
- Bluetooth Enabled: No
- Bluetooth Connected: No
- Bluetooth MAC: [empty]
- Connected Device ID: [empty]
- Active Interface: Wireless
- Wireless MAC: 84-5A-3E-C2-30-2D
- SSID: xin-wpa3-23-SAE
- AP MAC: 6C-8B-D3-F0-02-EF
- Channel: 64
- Frequency: 5320 MHz
- Security Mode: PSK

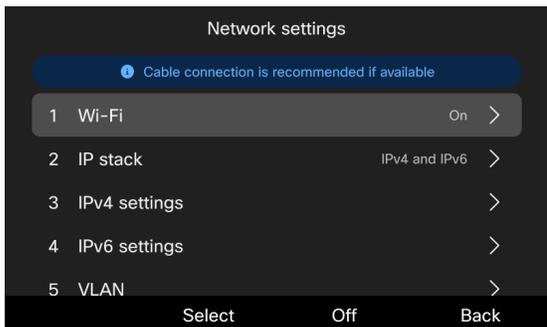
注:

- 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。

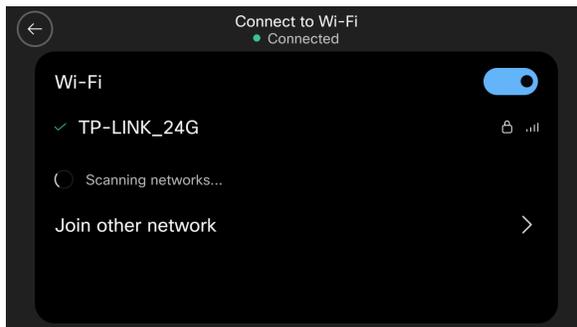
- 電話がイーサネット接続で接続されている場合、Wi-Fi はオフになります。電話が適切に設定されていれば、イーサネットケーブルが取り外されても、電話機は自動的にワイヤレスネットワークに接続されます。
- Wi-Fi 設定は電話の [設定] メニューの設定と同期されます。

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

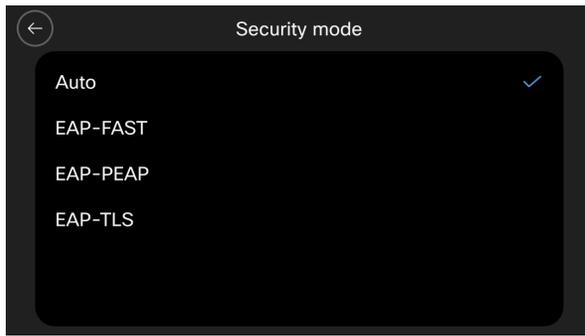


9871

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。

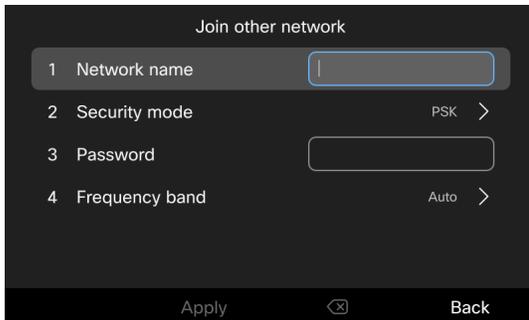
ネットワークが 802.1x に対応している場合、電話は EAP タイプに対して動的に [自動 (Auto)] を選択します。これは RADIUS サーバーの設定によって決まります。内部認証方法を選択できます。



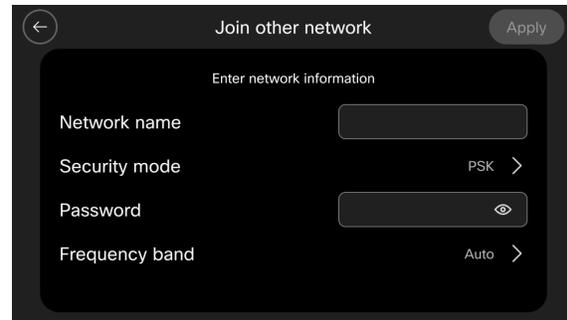
7. **[Apply]** を選択します。

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。

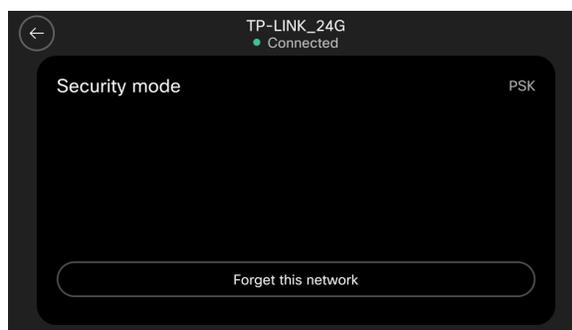
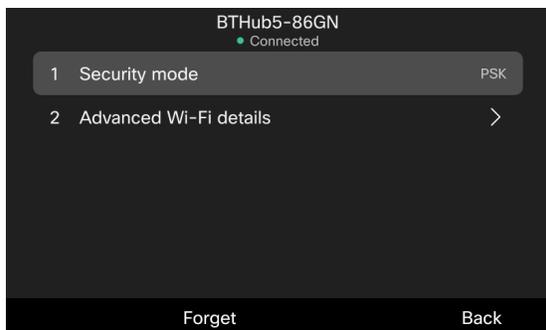
7. [適用 (Apply)] を選択します。

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。

- 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。

Web Admin*	Enabled
Admin Password

<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。



	Type	Common name	Issuer name	Valid from	Valid to	
Device information	Manufacturing issued	CN=CP-9861-SEP845A3EC22785, O=Cisco, OU=TPM SUDI, serialNumber=PID:DP-9861 SN:FVH281623FV	CN=High Assurance SUDI CA, O=Cisco	05/07/2024 02:44:00	08/09/2099 20:58:26	
Network setup	Manufacturing CA	CN=High Assurance SUDI CA, O=Cisco	O=Cisco, CN=Cisco Root CA 2099	08/11/2016 20:28:08	08/09/2099 20:58:27	Export
Setup	Manufacturing root CA	O=Cisco, CN=Cisco Root CA 2099	O=Cisco, CN=Cisco Root CA 2099	08/09/2016 20:58:28	08/09/2099 20:58:28	Export
Certificates	User installed	<Not installed>	<Not installed>			Install
Network statistics	Authentication server CA	<Not installed>	<Not installed>			Install
Ethernet information						
Access						
Network						

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。



Selected file (.p12 or .pfx) to upload: No file selected.

Extract password:

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。



Authentication Server CA certificate has been updated.

Phone will use the new certificate after reboot. You can restart the phone with:

`"System/Restart"`

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。

Service Parameter Configuration Parameters for All Servers

Status: Ready

Select Server and Service

Server*: 10.77.46.225--CUCM Voice/Video (Active)
 Service*: Cisco Certificate Authority Proxy Function (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Cisco Certificate Authority Proxy Function (Active) Parameters on server 10.77.46.225--CUCM Voice/Video (Active)

Parameter Name	Parameter Value	Suggested Value
Certificate Issuer to Endpoint *	Online CA	Cisco Certificate Authority Proxy Function
Duration Of Certificate Validity (in days) *	1825	1825
Maximum Allowable Time For Key Generation *	30	30
Maximum Allowable Attempts for Key Generation *	3	3

Online CA Parameters

Online CA Hostname	CUCM62.CA.cisco.com	
Online CA Port	443	
Online CA Template	CiscoRA_1	
Online CA Type *	Microsoft CA	Microsoft CA
Online CA Username	
Online CA Password	
Certificate Enrollment Profile Label		

Service Parameter Configuration Relat

Status: Ready

Select Server and Service

Server*: 10.79.57.147--CUCM Voice/Video (Active)
 Service*: Cisco Certificate Authority Proxy Function (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Cisco Certificate Authority Proxy Function (Active) Parameters on server 10.79.57.147--CUCM Voice/Video (Active)

Parameter Name	Parameter Value	Suggested Value
Certificate Issuer to Endpoint *	Cisco Certificate Authority Proxy Function	Cisco Certificate Authority Proxy Function
Duration Of Certificate Validity (in days) *	1825	1825
Maximum Allowable Time For Key Generation *	30	30
Maximum Allowable Attempts for Key Generation *	3	3

Online CA Parameters

Online CA Hostname		
Online CA Port		
Online CA Template	comadministrator	
Online CA Type *	Microsoft CA	Microsoft CA
Online CA Username	
Online CA Password	
Certificate Enrollment Profile Label		

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。

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (Bits)*

EC Key Size (Bits)

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: Operation Pending

Note: Security Profile Contains Addition CAPF Settings.

[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

Security settings

1 Security mode Non secure

2 LSC Installed >

3 Trust list >

4 802.1X Authentication >

Select Back

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

Certificate List (1 - 14 of 14)						
Find Certificate List where Certificate begins with CAPF Find Clear Filter						
Select item or enter search text						
Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	
CAPF	CAPF-50aa97cf	Identity	Self-signed	RSA	cucm-225	

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。

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
<input type="checkbox"/> 802.1x_mingzho_4096CA	Enabled	Cisco Services Endpoints Infrastructure	0F 3A 91 F2 B3 63 ...	test.sipura.cisco.com	test.sipura.cisco.com
<input type="checkbox"/> ASULIU-SCEP-CA#ASULIU-SCEP-CA#00009	Enabled	Infrastructure	62 F7 54 B0 81 B9 ...	ASULIU-SCEP-CA	ASULIU-SCEP-CA
<input type="checkbox"/> asuliu-SUBCA#ASULIU-SCEP-CA#00008	Enabled	Infrastructure	14 72 4E 9A 00 01 ...	asuliu-SUBCA	ASULIU-SCEP-CA
<input type="checkbox"/> Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...
<input type="checkbox"/> CAPF-50aa97cf	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	6A 4F 99 F8 B9 C0 ...	CAPF-50aa97cf	CAPF-50aa97cf

サーバ証明書

RADIUS サーバ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。

Cisco IP Phone DP-9861 (SEP845A3EC22785)

Select file (.cer) to upload: [Browse...](#) No file selected.

[Upload](#)

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。

Cisco IP Phone DP-9861 (SEP845A3EC21655)

Authentication Server CA certificate has been updated.

Phone will use the new certificate after reboot. You can restart the phone with:

"System/Restart"

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。

Cisco		Certificates				Signed in as admin, Sign out	
Cisco IP Phone DP-9861 (SEP845A3EC21655)							
Device information	Type	Common name	Issuer name	Valid from	Valid to		
Network setup	Manufacturing issued	CN=CP-9861-SEP845A3EC21655, O=Cisco, OU=TPM SUDI, serialNumber=PID:DP-9861 SN:FVH280322J6	CN=High Assurance SUDI CA, O=Cisco	01/29/2024 05:06:35	08/09/2099 20:58:26		
Setup	Manufacturing CA	CN=High Assurance SUDI CA, O=Cisco	O=Cisco, CN=Cisco Root CA 2099	08/11/2016 20:28:08	08/09/2099 20:58:27	Export	
Certificates	Manufacturing root CA	O=Cisco, CN=Cisco Root CA 2099	O=Cisco, CN=Cisco Root CA 2099	08/09/2016 20:58:28	08/09/2099 20:58:28	Export	
Network statistics	User installed	<Not installed>	<Not installed>			Install	
Ethernet information	Authentication server CA	DC=yan, DC=com, CN=yan-YANY2-CRDC-COM-CA	DC=yan, DC=com, CN=yan-YANY2-CRDC-COM-CA	01/27/2021 09:00:25	01/27/2026 09:10:25	Delete	

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。

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (Bits)*

EC Key Size (Bits)

Operation Completes By (YYYY:MM:DD:HH)

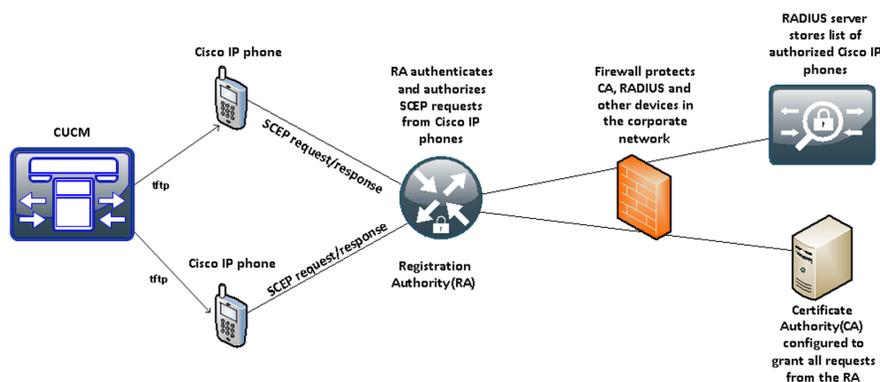
Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

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。

WLAN SCEP Server	10.195.19.65	<input checked="" type="checkbox"/>
WLAN Root CA Fingerprint (SHA256 or SHA1)	81512B4316429092925C6891701B374EBD254447	<input checked="" type="checkbox"/>

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。

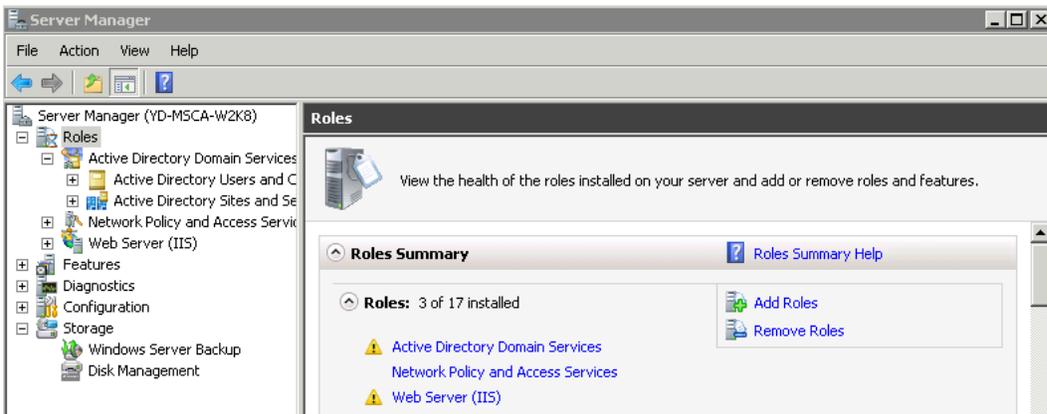
WLAN SCEP サーバ または **WLAN Root CA Fingerprint (SHA256 or SHA1)** が修正された場合、Cisco Desk Phone 9800 シリーズは CA とユーザー証明書を即時に更新しようとします。

認証局 (CA) の設定

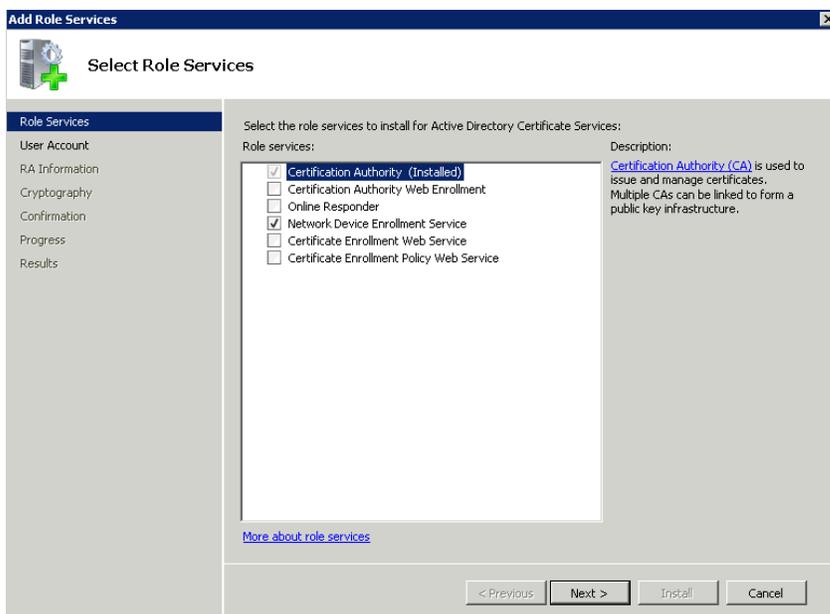
Microsoft® 認証局 (CA) サーバの使用を推奨します。

以下のガイドラインに従って、Microsoft CA を設定してください。

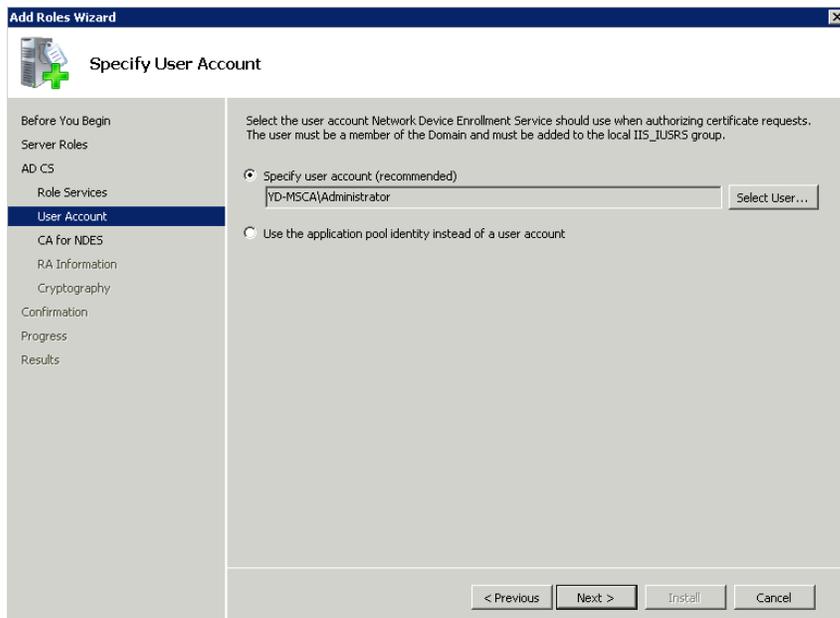
1. Microsoft Windows サーバ上に認証局と Active Directory ドメインサービスを作成します。
2. ネットワーク デバイス登録サービスを有効にします。
3. [ユーザープロパティ (user property)] 画面の[MemberOf]タブにアクセスして、**管理者**を IIS_IUSE RSのメンバーにします。
4. **Server Manager** を、起動して[ロールを追加 (Add roles)] をクリックします。



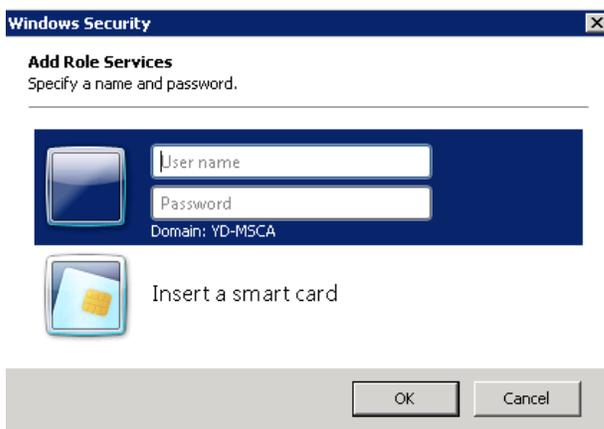
5. [サーバーロールを選択 (Select Server Role)] ページで、[Active Directory証明書 (Active Directory Certificate)] [サービス (Services)] ロールの順に選択し、[次へ (Next)] をクリックします。選択されているデフォルトサービスは、[認証局 (Certification Authority)] です。チェックボックスをオフにして移動します。
6. Network Device Enrollment Service の役割サービスを追加します。
7. [ロールウィザードを追加 (Add Roles Wizard)]、[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



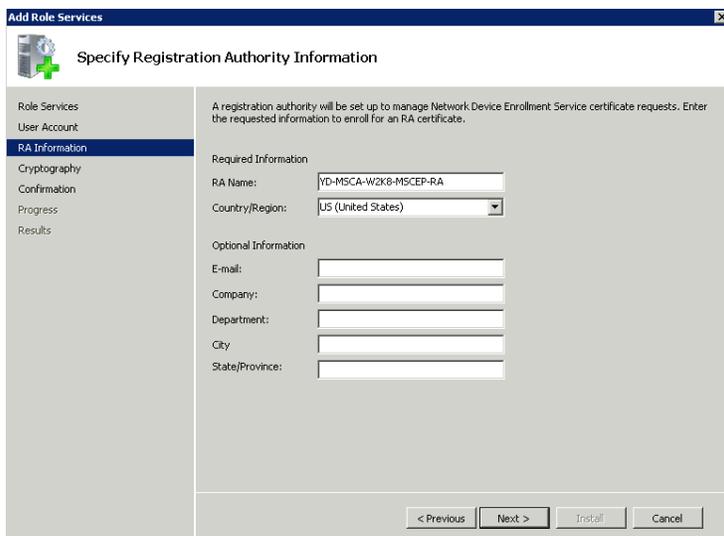
8. ウィザードは、必要なすべての依存関係がインストールされているかどうかを検出します。既存しない依存関係がある場合は、それについて説明するダイアログボックスが表示され、依存関係のインストールについての許可を求めます。インストールを続行するには、[はい (Yes)] をクリックします。
9. [ロールサービス (Role Services)] の [ユーザーアカウント (User Account)] をクリックし、[ユーザーを選択 (Select User)]... をクリックします。



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。

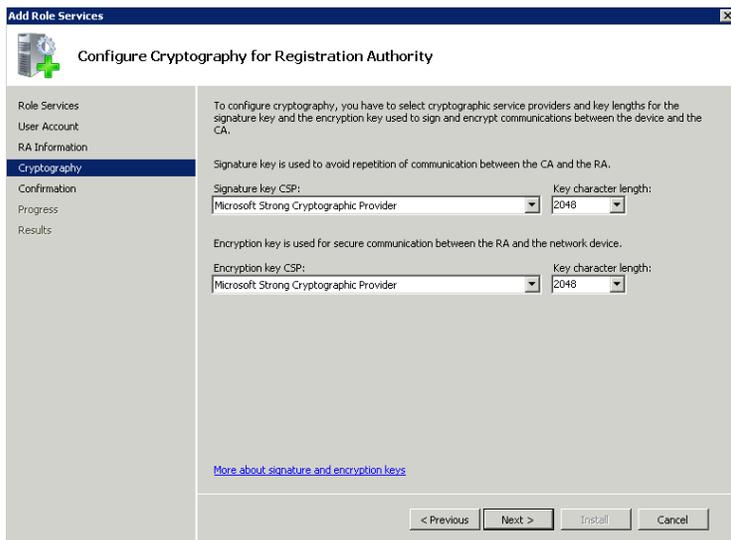


11. 登録機関情報を入力します。

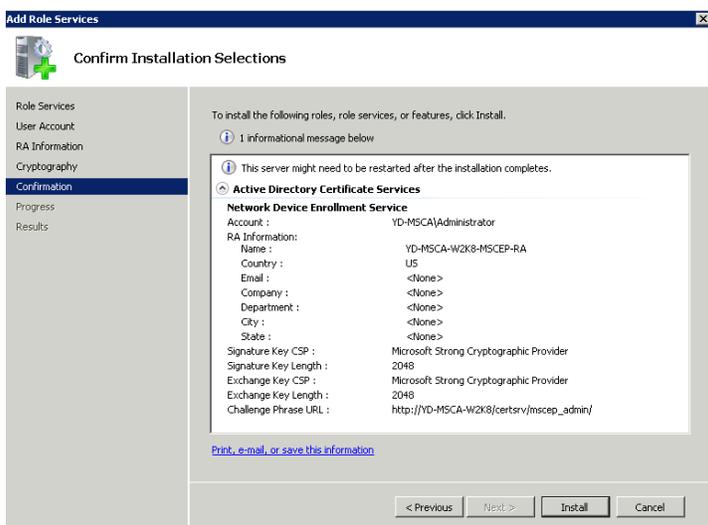


12. [Signature Key CSP] および [Encryption key CSP] に対して [Microsoft Strong Cryptographic Provider] を選択します。

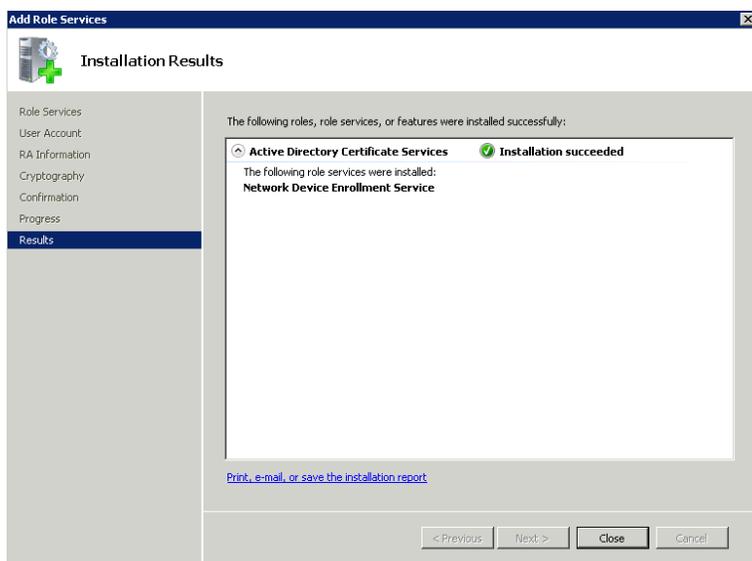
13. [キーの文字長 (Key character length)] に対して、2048 を選択します。



14. [インストール (Install)] を選択します。

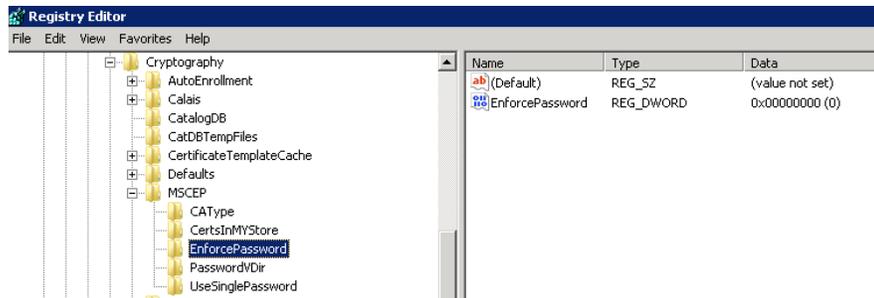


インストールが成功した場合、確認ページが表示されます。



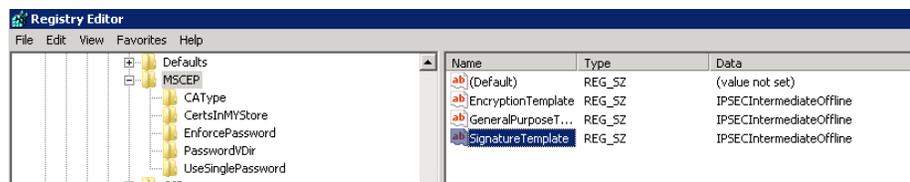
15. [EnforcePassword] を 0 を選択して、regedit 経由で [SCEP登録変更パスワード要件 (SCEP enrollment challenge password requirement)] を無効にします。

[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

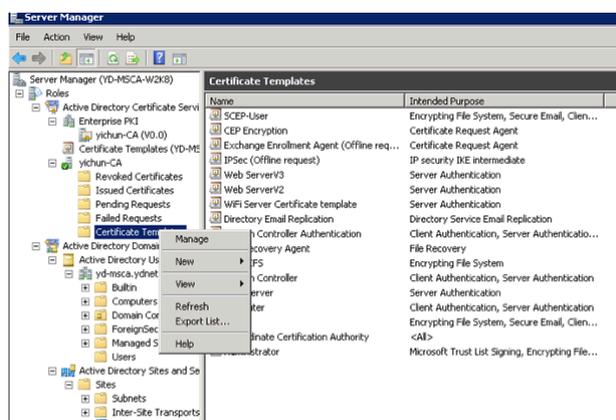
SCEP は、レジストリで設定されている証明書テンプレートを使用して証明書を発行します。 ([HKEY_LOCAL_MACHINE] > [ソフトウェア (SOFTWARE)] > [Microsoft] > [暗号化 (Cryptography)] > [MSCEP])



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。

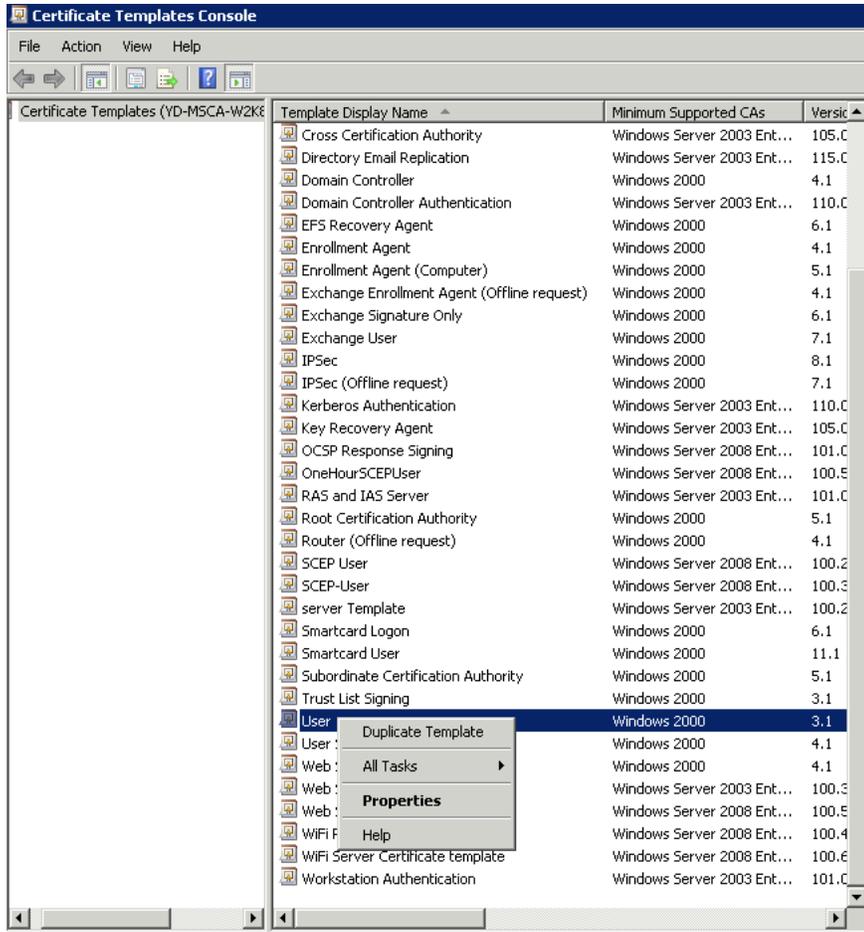
19. [Windows Server 2003 2008 テンプレート] を選択します。

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。

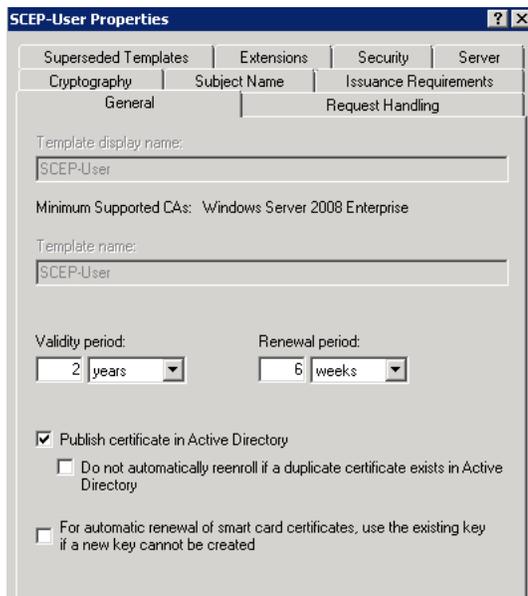
21. [拡張 (Extensions)] タブで、以下を確認します。

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。

The screenshot shows the 'SCEP-User Properties' dialog box with the 'Subject Name' tab selected. The 'Supply in the request' radio button is selected. Under 'Build from this Active Directory information', the 'Subject name format' dropdown is set to 'None'. There are several unchecked checkboxes for including alternate subject name information: 'Include e-mail name in subject name', 'Include this information in alternate subject name' (with sub-options for 'E-mail name', 'DNS name', 'User principal name (UPN)', and 'Service principal name (SPN)').

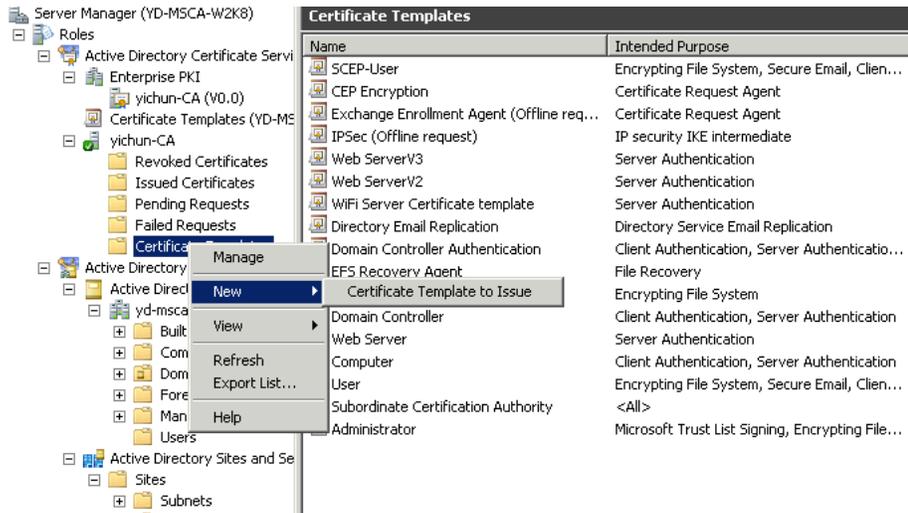
24. 以下に示すように、**拡張機能** タブを設定します。

The screenshot shows the 'Properties of New Template' dialog box with the 'Subject Name' tab selected. A list of extensions is shown, including 'Application Policies', 'Basic Constraints', 'Certificate Template Information', 'Issuance Policies', and 'Key Usage'. An 'Edit...' button is located below the list. The 'Description of Key Usage' section shows 'Signature requirements: Digital signature' and 'Allow key exchange only with key encryption Critical extension'.

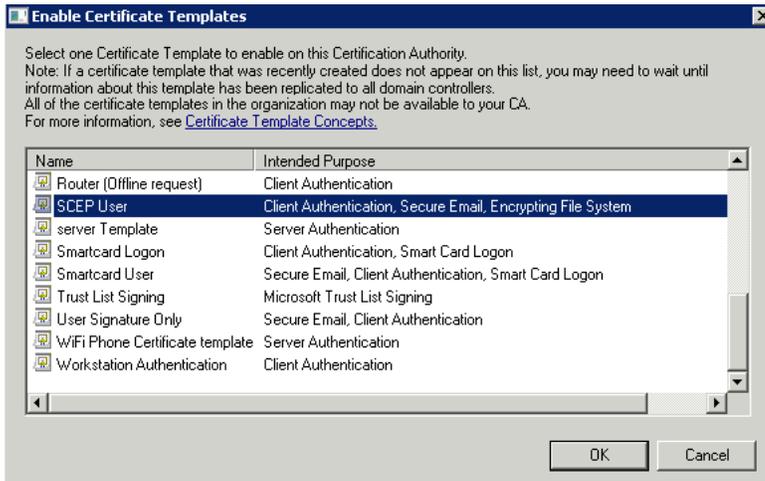
25. [アルゴリズム名 (Algorithm Name)]、[キーの最小サイズ (Minimum Key Size)] および [リクエストハッシュ (Request Hash)]、必要に応じて、[暗号化 (Cryptography)] タブを設定します。

The screenshot shows the 'SCEP-User Properties' dialog box with the 'Cryptography' tab selected. The 'Algorithm name' dropdown is set to 'RSA' and the 'Minimum key size' text box contains '2048'. The 'Choose which cryptographic providers can be used for requests' section has the first radio button selected: 'Requests can use any provider available on the subject's computer'. The 'Providers' list contains 'Microsoft Software Key Storage Provider'. The 'Request hash' dropdown is set to 'SHA1'. There is an unchecked checkbox for 'Use alternate signature format' with a link to 'here'.

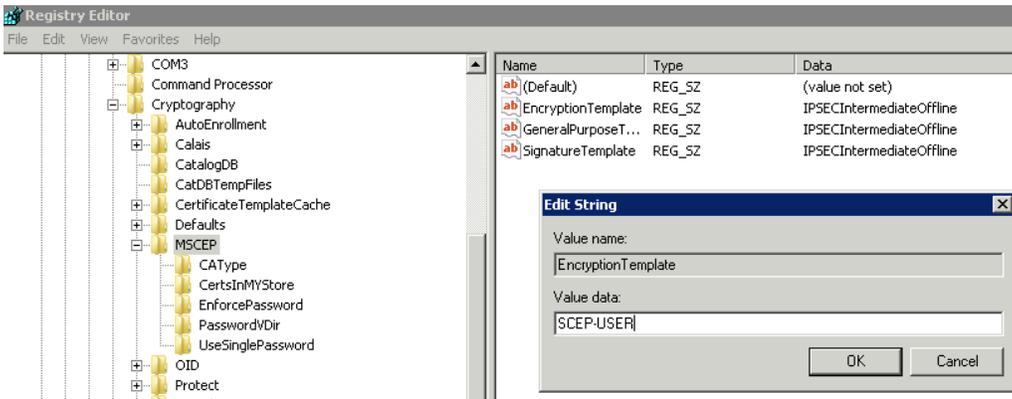
26. 新しく作成したテンプレートを有効にするには、[Certificateテンプレート (Certificate Templates)] を右クリックして、[新規 (New)] > [Certificateテンプレート (Certificate Templates)] の順に選択し、発行します。



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。

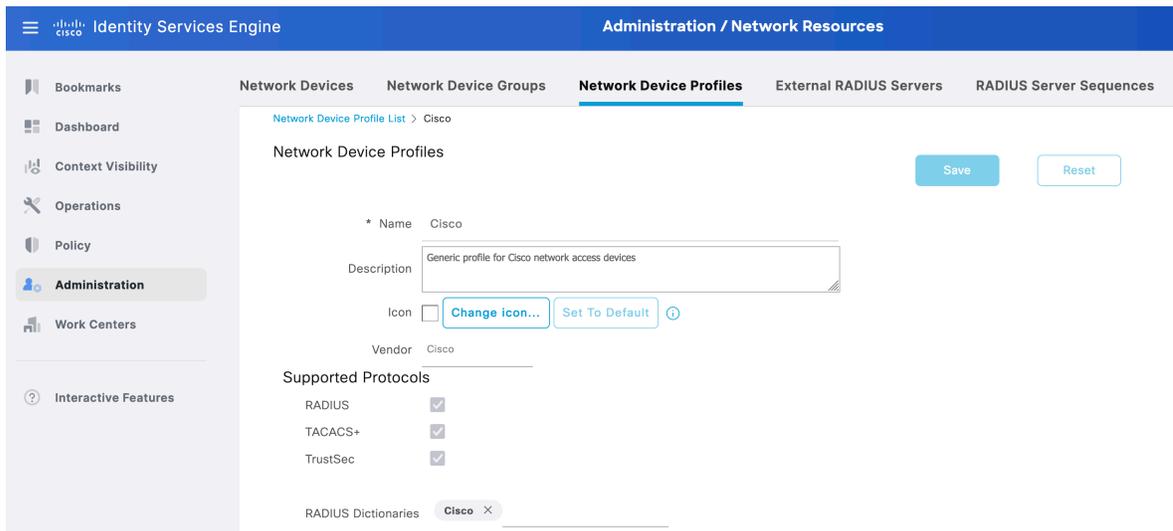
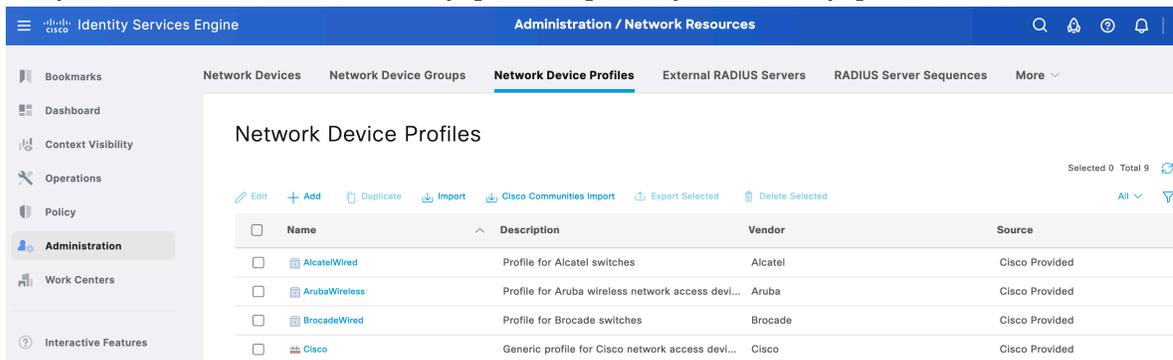


29. [IIS] [アプリケーションプール] に移動して SCEP サービスを再起動し、新しいテンプレートを有効にします。

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。



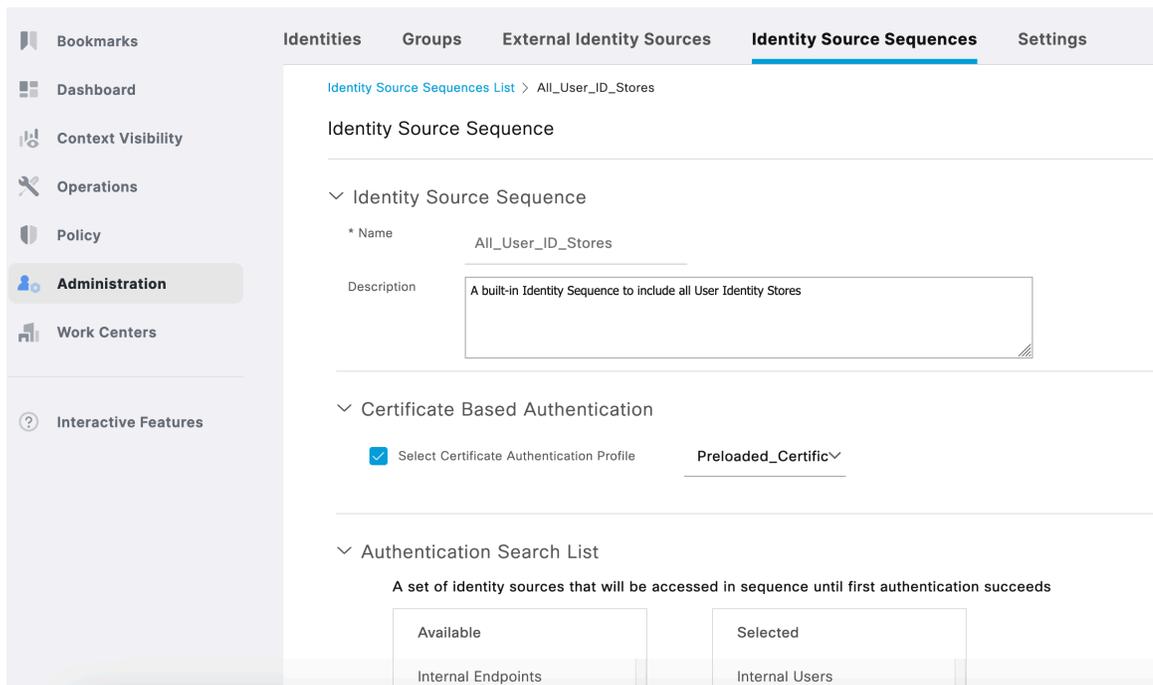
2. **[管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)]** の順に選択し、以下に示すように yan_RA_sudi などの Cisco IOS にデバイスを追加します

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services
<input type="checkbox"/>		ping_switch	10.74.133.13...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		rimo_switch	10.74.23.50/32	Cisco	All Locations	All Device Types	10.74.23.50
<input type="checkbox"/>		shihan-test	10.74.10.220/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		shugwang-rou...	10.74.133.115...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		ting_cube_sw2	10.74.53.202/32	Cisco	All Locations	All Device Types	ting_cube_sw2
<input type="checkbox"/>		ting_wlc9800	10.74.151.66/26	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		tiren_shield_wlc	100.100.101...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		tru-test-au	10.74.10.219/24	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		wangh_switch	100.100.30.7...	Cisco	All Locations	All Device Types	wangh_switch
<input type="checkbox"/>		wenjuaga_swi...	10.74.10.72/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		weny_switch	10.74.19.19/26	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		wexiao2_switch	10.79.57.18/24	Cisco	All Locations	All Device Types	wexiao2_switch
<input type="checkbox"/>		whale_WLC	10.74.18.31/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		wlc-public	100.100.66.1...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		yan-auto	100.100.116.2...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		yan-auto-3502	100.100.116.1...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		yan_RA_ca2	10.79.57.89/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		yan_RA_ca3	10.75.185.48/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/>		yan_RA_sudi	10.79.57.93/32	Cisco	All Locations	All Device Types	scep-for-sudi

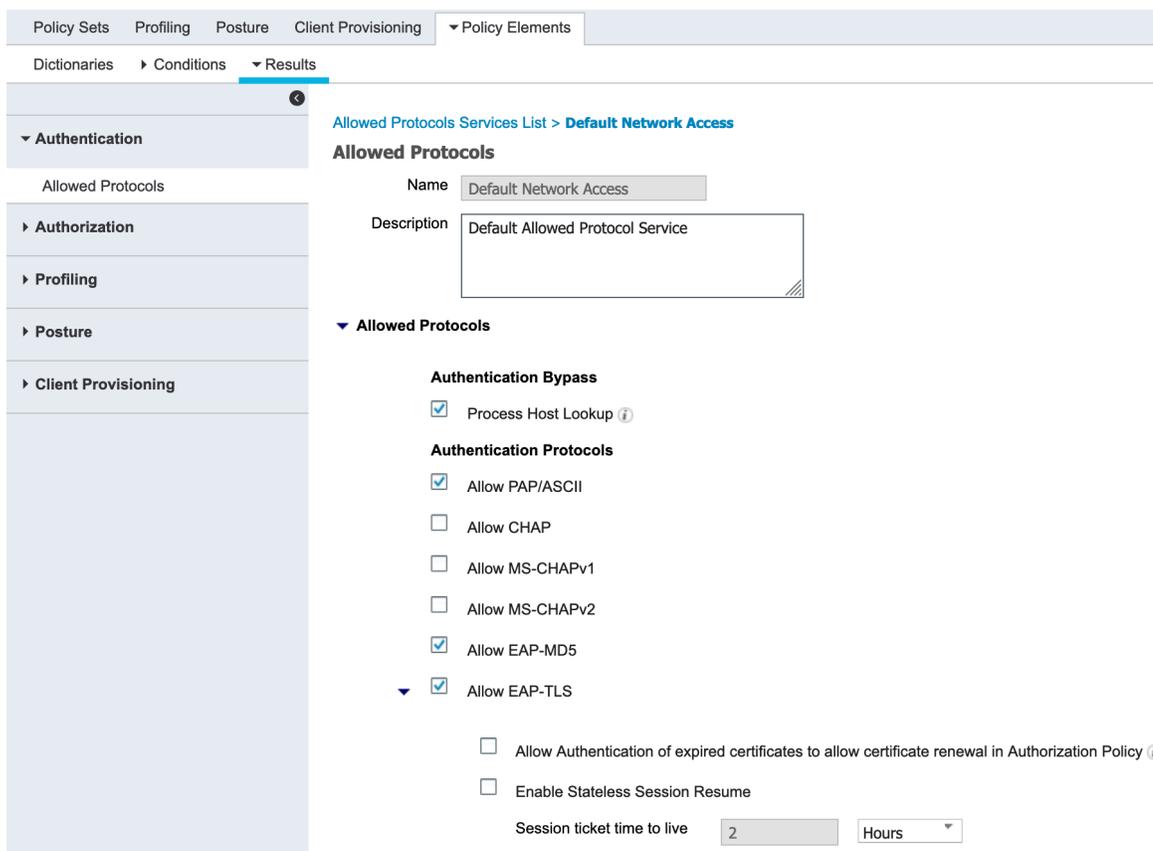
3. [ポリシー (Policy)] > [認証 (Authentication)] の順に選択し、[デフォルト (Default)] ルールを設定して、[デフォルトのネットワークアクセス (Default Network Access)] と [All_Uesr_ID_Stores] を使用します。

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。

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices.
<input type="checkbox"/> Cl_bbb_voice_vlan	Cisco	Cl_bbb_voice_vlan
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CW
<input type="checkbox"/> Eagle_PC_VLAN	Cisco	Access PC VLAN 165 of Eagle Team
<input type="checkbox"/> Eagle_Wired_Phone_VVLAN	Cisco	Access VVLAN 604 of Eagle Team
<input type="checkbox"/> FT_pc_vlan_96	Cisco	access vlan 96 for phenonix register
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant Prov
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input checked="" type="checkbox"/> Phone_SCEP_profile	Cisco	for scep

Identity Services Engine Home Context Visibility Operations Policy Administration Work Center

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > **Phone_SCEP_profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Advanced Attributes Settings

Cisco:cisco-av-pair = pki:cert-application=all

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。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings.

The main content area is titled "User Identity Groups > scep-group". It shows the configuration for the "scep-group" Identity Group. The Name is "scep-group" and the Description is "for SCEP". There are "Save" and "Reset" buttons.

Below the configuration is the "Member Users" section, which lists users associated with the group. The table has columns for Status, Email, Username, First Name, and Last Name.

Status	Email	Username	First Name	Last Name
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		PID:CP-8832 SN:FC...		
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		PID:CP-8821 SN:FC...		
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		PID:CP-8832 SN:FC...		
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		PID:CP-8875 SN:FC...		
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		PID:CP-8875 SN:FC...		
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		PID:DP-9861 SN:FV...		

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。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements.

The main content area shows a list of Authorization Policies. The "SCEP_Access" policy is selected. The "Conditions Studio" is open, showing the configuration for the "SCEP_Access" policy. The condition is "IdentityGroup Name" equals "User Identity Groups:scep-group". There are "Duplicate" and "Save" buttons.

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)。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Group
Enabled	PID:CP-8875 SN:FCH261738XL					
Enabled	PID:CP-8875 SN:FCH262831MF					scep-group
Enabled	PID:CP-8875 SN:FCH263038NM					
Enabled	PID:CP-8875 SN:FCH263038UY					scep-group
Enabled	PID:CP-8875 SN:FCH26332VH	cisco				scep-group
Enabled	PID:CP-8875 SN:FCH26452024					scep-group
Enabled	PID:CP-8875 SN:FCH264520NS					
Enabled	PID:CP-8875 SN:FCH264520NT	cisco				scep-group
Enabled	PID:DP-9861 SN:FCH27472020	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH280322J6	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623FQ	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623FV	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623U3	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623YE	cisco				scep-group
Enabled	PID:DP-9871 SN:FCH2738200Y	cisco				scep-group
Enabled	PID:DP-9871 SN:FCH2746202B	cisco				scep-group
Enabled	PID:DP-9871 SN:FCH27462048	cisco				scep-group
Enabled	PID:DP-9871 SN:FVH28080FNY	cisco				scep-group

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > PID:DP-9871 SN:FCH2738200Y

Network Access User

* Name: PID:DP-9871 SN:FCH2738200Y

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Password Re-Enter Password

* Login Password: *****

Enable Password:

User Information

First Name:

Last Name:

Account Options

Description: cisco

Change password on next login:

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
bzEZMBCGA1UEAxMQQ2IzY28gUm9vdCBDQSBNMjAeFw0xMjExMTIxMzUwNThaFw0z
NzExMTIxMzAwMTdaMDYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
YW51ZmFjdHvyaW5nIENBIFNIQTlwgGEMAA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AolBAQD0NktCAJn3kk98hU7wUVp6QIOFrlltEce6CpbfYpeLdUeZduAo+S0otzT
lJwS2BIMhZtacu9vUpfmW9w7nQo9zVT3eyPuhF/6/9TEdVBn75zb5CfV+E6ld+fH
nuPiFyBu+HDDJRd373Op+957ldoWyPvD8hHR1HJGFJ3JJKBg0UScL4JCwleu98Xq
/yPIAqBhExa7a2/fqSmZA0vZIG1bBfWZY8ZtSeTxKg3eWynV+xElabHqTDMYWF+2
obs4YB5IINTbYgHyRETP6T8Xr6TtD0h3654OUHcW+1meBu/jctluMKppeSjVtrof
5vt+pbkCg0iQAAjsL0qczT3yaNXvAgMBAAGjggGHMIIbGzAObgNVHQ8BAf8EBAMC
AQYwEgYDVR0TAQH/BAgwBgEB/wIBADBcBgNVHSAEVTBTMFEGCisGAQQBQRUBEGAw
QzBBBggrBgEFBQcCary1aHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L3BvbGljaWVzL2luZGV4Lmhh0bWwwHQYDVR0OBByEFHrXeZXKu0gruFUU/aPAD7yn
D5YZMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY2IzY28uY29tL3NIY3VyaXR5L3BraS9jcmwvY3JjYw0yLmNybDB8BgggrBgEFBQcCBAQRwMG4wPgYIKwYBBQUH
MAKGMmh0dHA6Ly93d3cuY2IzY28uY29tL3NIY3VyaXR5L3BraS9jZXJ0cy9jcmNh
bTluY2VyMCwGCCsGAQUFBzABhiBodHRwczovL3Rvb2xzLmNpc2NvLmNvbS9wa2kv
b2NzcDAfBgNVHSMEGDAWgBTJAPkfiH/CZr2l0m1IDiluNMMFoDANBgkqhkiG9w0B
AQsFAAOCAQEAc1k2rH6YT4juFxs9q70bzfcKbNvOyDsaU7av4IHFXmn/JxfnBmUv
YxAI2Hx3xRb0KtG1JGkffQjVAtBboTXynLaQso/jj46ZOubIF8y6Ho3nTAv7Q6VH

```

```
kqSCdZCIVu91zbHV9FFYQzJxjw1QgB0a4ltS4yhdmgI3oDNEcb3trQezrQ3/857/  
ISqBGVLEbKHOU8H6zOLhxAgZ08ae1oQQQJowki0lbd+LRLGovtEwLg8yyqiTIGve  
7VFL2sRa8Z3rK9tlwKVH2kpFKNAeN3rfKFqr0/weR0cyKpmLMrSBTBZcxQcJCYF4  
X6FO/32KOqcxJFIOKGVUjvAvioOqoducw==
```

-----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。

The first screenshot shows the 'Report problem' screen with the following fields:

- 1 Date of problem (mm/dd): 06/21
- 2 Time of problem (hh:mm + AM/PM): 7:18 PM
- 3 Problem description: Failed to place a call >
- 4 Last PRT file name
- 5 Last uploaded time

Buttons at the bottom: Submit, Select, Back.

The second screenshot shows the 'Issues and diagnostics' screen with the following items:

- 1 Issues: None
- 2 Problem submitted >
- 3 The PRT file is available at <http://10.79.63.52/FS/prt-20240621-192126-845A3EC22785.tar.gz> >

Button at the bottom: OK.

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。

Wireless statistics	
tx bytes	18259897
rx bytes	22422877
tx packets	00060529
rx packets	00068946
tx packets dropped	00000000
rx packets dropped	00000000
Back	

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。

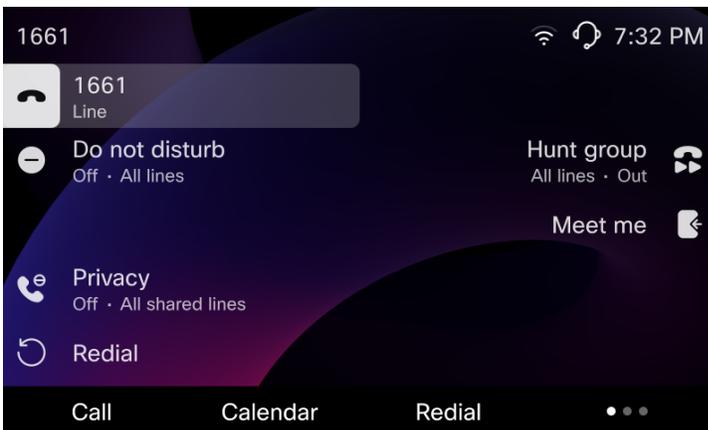
ウェブブラウザで電話の IP アドレスにアクセスし、ストリーミングの統計を表示します。

Line 1 Call 1 Status	
Call State:	Called Party Ringing
Tone:	None
Decoder:	PCMU
Remote Hold:	No
Mapped RTP Port:	19626 >> 0
Peer Phone:	+17139326004
Packets Sent:	335
Bytes Sent:	53600
Decode Latency:	20 ms
Round Trip Delay:	0 ms
Loss Rate:	0.00
Discard Rate:	0.32
Gap Duration:	0 ms
MOS-LQ:	4.26
Call Appearance:	Line 1 Call 1
Encoder:	PCMU
Type:	Outbound
Callback:	
Peer Name:	+17139326004
Duration:	
Packets Received:	308
Bytes Received:	52804
Jitter:	44 ms
Packets Lost:	0
Packet Discarded:	1
Burst Duration:	0 ms
R Factor:	87
MOS-CQ:	4.26

Streaming statistics	
Cisco IP Phone DP-9861 (SEP845A3EC229D4)	
Remote address	173.36.143.200/51302
Local address	10.79.63.51/22570
Start time	9:31:25am
Stream status	Active
Host name	SEP845A3EC229D4
Sender packets	237269
Sender octets	12263901
Sender codec	OPUS
Sender reports sent	835
Sender report time sent	10:50:31am
Receiver lost packets	583
Avg jitter	8
Receiver codec	OPUS
Receiver reports sent	0
Receiver report time sent	00:00:00
Receiver packets	236709
Rcvr octets	40713776
Cumulative conceal ratio	0.0013
Interval conceal ratio	0.0000
Max conceal ratio	0.0594
Conceal seconds	473

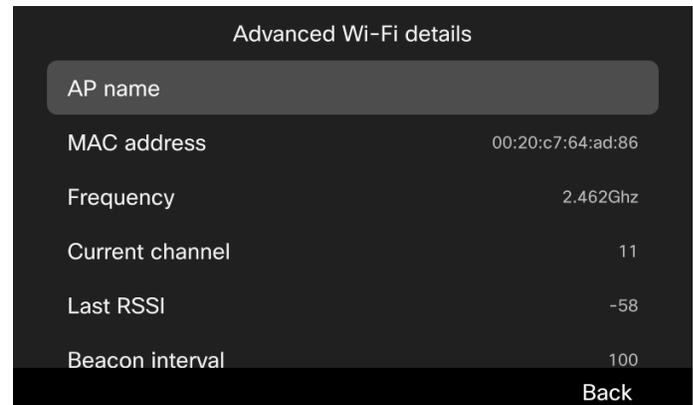
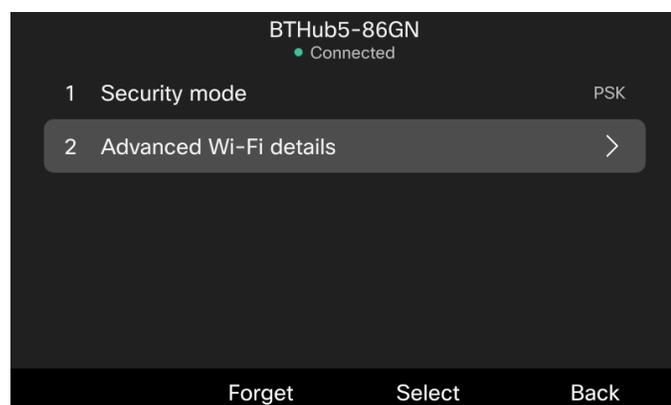
Wi-Fi 信号インジケータ

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

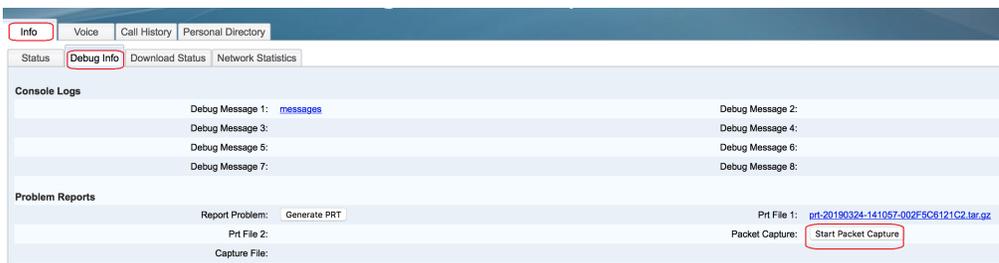
Webex Calling または BroadWorks に登録されている電話の場合は、電話の IP アドレスを取得し、ウェブブラウザで http://<phone_IP_address>/admin/screendump.bmp にアクセスします。たとえば、<http://192.168.16.43/admin/screendump.bmp> です。プロンプトが表示されたら、admin のパスワードを入力します。

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: <http://192.168.32.124/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。

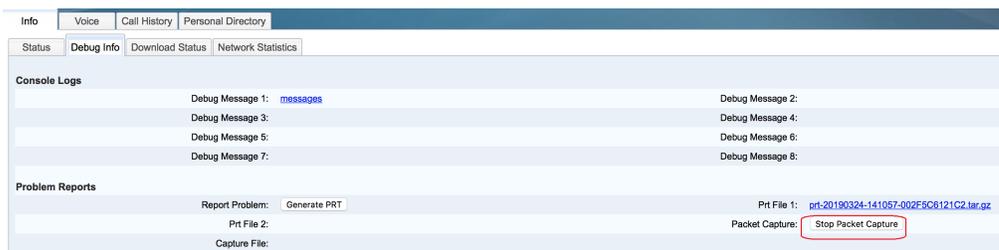
1. **[情報 (Info)] > [デバッグ情報 (Debug Info)]** の順に選択し、**[パケットキャプチャを開始 (Start Packet Capture)]** をクリックします。



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。

The screenshot shows the Cisco Unified Communications Manager (CUCM) interface. At the top, there are tabs for 'Info', 'Voice', 'Call History', and 'Personal Directory'. Below these, there are sub-tabs for 'Status', 'Debug Info', 'Download Status', and 'Network Statistics'. The 'Debug Info' tab is active, showing a 'Console Logs' section with eight debug messages. The first message is a link to 'messages'. Below this is a 'Problem Reports' section with a 'Generate PRT' button and links for 'Prt File 1' (prt-20190324-141057-002F5C6121C2.tar.gz) and 'Capture File' (prt-20190403-011835-002F5C6121C2.scam). The 'Capture File' link is highlighted with a red box.

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

CCDE、CCENT、Cisco Eos、Cisco Lumin、Cisco Nexus、Cisco StadiumVision、Cisco TelePresence、Cisco WebEx、Cisco ロゴ、DCE、Welcome to the Human Network は商標です。Changing the Way We Work, Live, Play, and Learn and Cisco Store はサービスマークです。および Access Registrar、ironet、AsyncOS、Bringing the Meeting To You、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、CCSP、CCVP、Cisco、Cisco Certified Internetwork Expert ロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems ロゴ、Cisco Unity、Collaboration Without Limitation、EtherFast、EtherSwitch、Event Center、Fast Step、Follow Me Browsing、FormShare、GigaDrive、HomeLink、Internet Quotient、IOS、iPhone、iQuick Study、IronPort、IronPort ロゴ、LightStream、Linksys、MediaTone、MeetingPlace、MeetingPlace Chime Sound、MGX、Networkers、Networking Academy、Network Registrar、PCNow、PIX、PowerPanels、ProConnect、ScriptShare、SenderBase、SMARTnet、Spectrum Expert、StackWise、The Fastest Way to Increase Your Internet Quotient、TransPath、WebEx、および WebEx ロゴは、米国および特定の国に所在する Cisco Systems, Inc. および/またはその関連会社の登録商標です。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。Cisco の商標の一覧は、<http://www.cisco.com/go/trademarks> を参照してください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

このドキュメントまたはウェブサイトに記載されているその他すべての商標は、それぞれの所有者に所有権があります。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

© 2024 Cisco Systems, All rights reserved.