



Cisco Desk、Board、および Room Series ワイヤレス LAN 導入ガイド



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

Cisco RoomOS Series

は、従業員の生産性に新しい時代をひらきます。コラボレーション対応のビジネスプロセスとワークフローに新しい機会を生成し、ビジネス上の効果を促進します。

Cisco RoomOS Series は、業界や地域、職場や家庭において現在および将来に新しく発生するニーズに対応します。

このガイドでは、ネットワーク管理者がワイヤレス LAN 環境内でこの Cisco RoomOS Series を展開するのに役立つ情報と手引きを提供します。

更新履歴

日付	コメント
07/14/21	10.5(1) リリース
10/19/21	10.8(1) リリース
01/17/22	10.11(1) リリース
03/25/22	10.13(1) リリース
02/15/24	11.13(1) リリース

目次

Cisco RoomOS Series Overview	6
<i>Models</i>	6
<i>Requirements</i>	8
Site Survey.....	8
Call Control	9
Wireless LAN	10
<i>Protocols</i>	15
<i>Wi-Fi</i>	15
Regulatory	27
<i>Bluetooth</i>	28
<i>Languages</i>	29
<i>Video Calls</i>	29
<i>Device Care</i>	29
Wireless LAN Design	31
<i>802.11 Network</i>	31
5 GHz (802.11a/n/ac/ax)	31
2.4 GHz (802.11b/g/n/ax).....	32
Signal Strength and Coverage.....	33
Data Rates.....	36
Rugged Environments.....	37
<i>Security</i>	39
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST).....	40
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS).....	41
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS).....	41
Protected Extensible Authentication Protocol (PEAP).....	41
<i>Quality of Service (QoS)</i>	42
Call Admission Control (CAC).....	43
Wired QoS	43
<i>Roaming</i>	44
Interband Roaming	44
<i>Power Management</i>	44
<i>Call Capacity</i>	45
<i>Multicast</i>	46
Configuring the Cisco Wireless LAN	47
<i>Cisco AireOS Wireless LAN Controller and Lightweight Access Points</i>	47
802.11 Network Settings.....	47
WLAN Settings	58
Controller Settings	66
Call Admission Control (CAC).....	68
RF Profiles	71
FlexConnect Groups	73
Multicast Direct	75
QoS Profiles.....	77
Advanced Settings	81
<i>Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points</i>	84
802.11 Network Settings.....	85

WLAN Settings	93
Controller Settings	108
Mobility Settings.....	109
Call Admission Control (CAC).....	110
Multicast	110
Advanced Settings	113
Sample Configuration	115
<i>Cisco Mobility Express and Lightweight Access Points</i>	122
Controller Settings	123
802.11 Network Settings.....	124
WLAN Settings	127
RF Profiles	134
Multicast Direct	136
<i>Cisco Autonomous Access Points</i>	137
802.11 Network Settings.....	137
WLAN Settings	141
Call Admission Control (CAC).....	151
QoS Policies	152
Power Management	155
Sample Configuration	156
<i>Cisco Meraki Access Points</i>	161
Creating the Wireless Network	161
SSID Configuration	164
Radio Settings	167
Firewall and Traffic Shaping	169
Configuring Cisco Call Control	171
<i>Webex</i>	171
Personal Usage	171
Shared Usage	173
<i>Cisco Unified Communications Manager</i>	176
Device Enablement	176
Device Pools	177
Phone Button Templates	177
Security Profiles.....	178
SIP Profiles	179
QoS Parameters.....	182
Audio and Video Bit Rates	183
Product Specific Configuration Options	184
Configuring the Cisco RoomOS Series	241
<i>Wi-Fi Profile Configuration</i>	241
<i>Certificate Management</i>	252
Installing Certificates	252
Removing Certificates.....	254
<i>Call Control Configuration</i>	255
<i>Bluetooth Settings</i>	258
<i>Upgrading Firmware</i>	259
Using the Cisco RoomOS Series	261
Troubleshooting	263
<i>About Device</i>	263
<i>Network Connection Status</i>	264

<i>Advanced Wi-Fi Details</i>	264
<i>Issues and Diagnostics</i>	266
<i>Device Webpages</i>	267
System Information.....	267
Setup.....	268
Customization	271
System Maintenance	274
<i>Restoring Factory Defaults</i>	276
<i>Capturing a Screenshot of the Device Display</i>	277
Additional Documentation	279

Cisco RoomOS Series 概要

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

Cisco の 802.11

ソリューションにより、音声やビデオといった、時間に影響を受けるアプリケーションをキャンパス全体の無線 LAN (WLAN) 環境で効率的に使用できます。無線 LAN 環境の拡張により、アクセスポイント間のローミング時にセキュリティを維持しながら、高速ローミング機能とほぼシームレスなマルチメディアトラフィックのフローが実現します。

WLAN

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

Cisco では Cisco RoomOS Series

に最適化を行ってはいますが、ライセンスのない周波数帯を使用している以上、中断されない通信は保証できず、マルチメディア通話中に数秒の音声のギャップが生じる可能性があります。この導入ガイドラインに従うことで、このような音声のギャップが発生する可能性は低減されますが、完全には解消されません。

ライセンス不要の周波数帯を使用しているため、WLAN デバイスへのメッセージの配信は保証されません。Cisco RoomOS Series は医療機器として使用されることを意図しておらず、医療診断用途では使用できません。

モデル

次の Cisco RoomOS シリーズ モデルを使用できます。

下記は、各モデルでサポートされるピークアンテナゲイン、周波数範囲とチャンネルの概要です。

Cisco RoomOS Series 1

モデル	製品番号	ピーク アンテナ ゲイン	周波数範囲	チャンネル セット (チャ ネル数)
Cisco Board 55	CS-BOARD55	2.4 GHz = 4.23 dBi 5 GHz = 6.00 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz	1 ~ 13 (13) 36, 40, 44, 48 (4)
Cisco Board 55s	CS-BOARD55S	2.4 GHz = 4.50 dBi 5 GHz = 5.80 dBi	5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz	52, 56, 60, 64 (4) 100 ~ 144 (12)
Cisco Board 70	CS-BOARD70	2.4 GHz = 4.23 dBi 5 GHz = 6.00 dBi	5.745 ~ 5.825 GHz	149, 153, 157, 161, 165 (5)
Cisco Board 70s	CS-BOARD70S=	2.4 GHz = 4.40 dBi		

		5 GHz = 5.50 dBi		
Cisco Board 85s	CS-BOARD85S	2.4 GHz = 4.40 dBi 5 GHz = 4.40 dBi		
Cisco Board Pro 55	CS-BRD55P	2.4 GHz = 5.91 dBi 5 GHz = 5.72 dBi		
Cisco Board Pro 75	CS-BRD75P	2.4 GHz = 6.17 dBi 5 GHz = 4.95 dBi		
Cisco Codec Plus	CS-CODEC-PLUS	2.4 GHz = 3.28 dBi 5 GHz = 5.12 dBi		
Cisco Codec Pro	CS-CODEC-PRO	2.4 GHz = 4.58 dBi 5 GHz = 4.48 dBi		
Cisco Desk Limited Edition	CS-DESK-LE	2.4 GHz = 4.13 dBi 5 GHz = 5.95 dBi		
Cisco Desk Pro	CS-DESKPRO	2.4 GHz = 4.13 dBi 5 GHz = 5.95 dBi		
Cisco Room 55	CS-ROOM55	2.4 GHz = 4.00 dBi 5 GHz = 7.10 dBi		
Cisco Room 55 Dual	CS-ROOM55D	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Single	CS-ROOM70S	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Dual	CS-ROOM70D	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Single G2	CS-ROOM70SG2	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Dual G2	CS-ROOM70DG2	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Panorama	CS-ROOM70-PANO	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room Panorama	CS-ROOM-PANO85	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room Kit	CS-KIT	2.4 GHz = 4.30 dBi 5 GHz = 5.70 dBi		
Cisco Webex Room Kit Mini	CS-KITMINI	2.4 GHz = 3.70 dBi 5 GHz = 5.30 dBi		

Cisco Room USB	CS-ROOM-USB	2.4 GHz = 3.70 dBi 5 GHz = 5.30 dBi		
----------------	-------------	--	--	--

Cisco RoomOS Series 2

モデル	製品番号	ピーク アンテナ ゲイン	周波数範囲	チャンネル セット (チャ ネル数)
シスコ デスク	CS-DESK	2.4 GHz = 3.40 dBi 5 GHz = 6.10 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz	1 ~ 13 (13) 36、40、44、48 (4)
Cisco Desk Mini	CS-DESKMINI	2.4 GHz = 5.00 dBi 5 GHz = 4.90 dBi	5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz	52、56、60、64 (4) 100 ~ 144 (12)
Cisco Room Bar	CS-BAR	2.4 GHz = 4.96 dBi 5 GHz = 7.85 dBi	5.745 ~ 5.825 GHz	149、153、157、161、165 (5)

Cisco RoomOS Series 3

モデル	製品番号	ピーク アンテナ ゲイン	周波数範囲	チャンネル セット (チャ ネル数)
Cisco Codec EQ	CS-CODEC-EQ	2.4 GHz = 3.50 dBi 5 GHz = 3.40 dBi	2.412 ~ 2.472 GHz 5.180 ~ 5.240 GHz	1 ~ 13 (13) 36、40、44、48 (4)
Cisco Room Bar Pro	CS-BARPRO	2.4 GHz = 6.70 dBi 5 GHz = 5.70 dBi	5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	52、56、60、64 (4) 100 ~ 144 (12) 149、153、157、161、165 (5)

注：実際に使用されるチャンネルは、地域の規制によって異なります。

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

日本用のチャンネル 14 はサポートされていません。

要件

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

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

サイト調査

Cisco RoomOS Series を実稼働環境に展開する前に、先進的なワイヤレス LAN を専門とする Cisco

Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

認定パートナーによるサイト調査を実施する必要があります。サイト調査時に、RF 周波数帯を分析して、対象帯域（5 GHz または 2.4 GHz）内で使用可能なチャンネルを決定できます。一般に、5 GHz 帯域では干渉が少なく、オーバーラップしないチャンネルが多く存在します。そのため動作帯域は 5 GHz が推奨されています。特に Cisco RoomOS Series を基幹業務で使用する場合は強く推奨されます。サイト調査には、その場所の対象カバレッジプランを示すヒートマップも含まれます。また、サイト調査では、アクセスポイントのプラットフォームタイプ、アンテナタイプ、

アクセスポイントの構成（チャンネルおよび送信電力）を決定します。条件の厳しくない環境（オフィス、医療機関、教育、サービス業など）に対しては内蔵アンテナを持つアクセスポイントを選択し、条件の厳しい環境（製造、倉庫、小売業など）に対しては、外部アンテナを必要とするアクセスポイントプラットフォームを推奨します。

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

電波状態表示

セルエッジは、-67 dBm の信号レベルで隣接アクセスポイントとの間に 20 ~ 30 % のオーバーラップを維持する必要があります。

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

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

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

チャンネルの使用率

チャンネル使用率レベルは 40 % 未満に維持される必要があります。

ノイズ

ノイズレベルは -92 dBm を超過しないようにします。それにより、-67 dBm の信号が維持される場合に 25 dB の信号対雑音比（SNR）が実現します。

また、Cisco RoomOS Series からのアップストリーム信号が、送信データレートに関するアクセスポイントの信号対雑音比に適合している必要もあります。

パケット損失/遅延

音声ガイドラインによると、パケット損失は 1 % を超過しない必要があります。1 % を超過すると、音声品質が大幅に低下する可能性があります。

ジッタは最小（100 ms 未満）に維持される必要があります。

再試行回数

802.11 再送信は 20 % 未満である必要があります。

マルチパス

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

コール制御

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

- **Cisco RoomOS Series 1**

- Webex

- Cisco Unified Communications

- Manager (CUCM) 、最小 = 10.5(2)

- 推奨 = 11.5(1)、12.0(1)、12.5(1)、14.0(1) 以降

- **Cisco RoomOS Series 2**
 - Webex
 - Cisco Unified Communications Manager (CUCM) 、最小 = 11.5(1)
推奨 = 12.5(1)、14.0(1) 以降

- **Cisco RoomOS Series 3**
 - Webex
 - Cisco Unified Communications Manager (CUCM) 、最小 = 12.5(1)
推奨 = 14.0(1) 以降

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

Cisco Unified Communications Manager 用のデバイスパッケージは、<https://software.cisco.com/download/home/278875240> から入手できます。

ワイヤレス LAN

Cisco RoomOS Series は、次の Cisco ワイヤレス LAN ソリューションでサポートされています。

- Cisco AireOS ワイヤレス LAN コントローラおよび Cisco Lightweight
アクセスポイント、最小 = 8.3.143.0
推奨 = 8.3.150.0、8.5.182.0、8.8.130.0、8.10.190.0
- Cisco IOS ワイヤレス LAN コントローラおよび Cisco Lightweight
アクセスポイント、最小 = 16.12.1s
推奨 = 17.3.8a、17.6.6a、17.9.4a、17.12.2、17.13.1
- Cisco Mobility Express および Cisco Lightweight
アクセスポイント、最小 = 8.3.143.0
推奨 = 8.3.150.0、8.5.182.0、8.8.130.0、8.10.190.0
- Cisco Autonomous (自律) アクセス ポイント
最小 = 15.2(4)JB6、推奨 =
15.3(3)JPP
- Cisco Meraki アクセスポイント
最小 = MR 25.9、MX 13.33
推奨 = MR 30.5、MX 18.107.2

アクセスポイント

サポートされるシスコのアクセスポイントを以下に示します。
一覧にないアクセスポイントモデルはサポートされません。

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



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

Cisco AP シリー	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	軽量	Mobility Express	自律型
---------------------	----------------	----------------	----------------	----------------	-----------------	-----------------	-----------	-------------------------	------------

ズ									
1700	はい	はい	はい	はい	はい	いいえ	○	いいえ	○
1810	はい	はい	はい	はい	はい	いいえ	○	いいえ	いいえ
1810W	はい	はい	はい	はい	はい	いいえ	○	いいえ	いいえ
1815	はい	はい	はい	はい	はい	いいえ	○	はい (1815t ではありません)	いいえ
1830	はい	はい	はい	はい	はい	いいえ	○	はい	いいえ
1840	はい	はい	はい	はい	はい	いいえ	○	はい	いいえ
1850	はい	はい	はい	はい	はい	いいえ	○	はい	いいえ
2700	はい	はい	はい	はい	はい	いいえ	○	いいえ	○
2800	はい	はい	はい	はい	はい	いいえ	○	はい	いいえ
3700	はい	はい	はい	はい	はい	いいえ	○	いいえ	○
3800	はい	はい	はい	はい	はい	いいえ	○	はい	いいえ
4800	はい	はい	はい	はい	はい	いいえ	○	はい	いいえ
9105	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9115	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9117	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9120	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9124	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9130	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9136	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9162	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9164	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9166	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ

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



MR20



MR28



MR30H



MR32



MR33



MR34



MR36



MR36H



MR42



MR44



MR45



MR46



MR52



MR53



MR55



MR56



MR57



9162



9164



9166



MX64W



MX65W



MX67W



MX68W



Z3

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

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

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

Meraki AP シリー ズ	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
9162	はい	はい	はい	はい	はい	はい
9164	はい	はい	はい	はい	はい	はい
9166	はい	はい	はい	はい	はい	はい
MR20	はい	はい	はい	はい	はい	いいえ
MR28	はい	はい	はい	はい	はい	はい
MR30H	はい	はい	はい	はい	はい	いいえ
MR32	はい	はい	はい	はい	はい	いいえ
MR33	はい	はい	はい	はい	はい	いいえ
MR34	はい	はい	はい	はい	はい	いいえ
MR36	はい	はい	はい	はい	はい	はい
MR36H	はい	はい	はい	はい	はい	はい
MR42	はい	はい	はい	はい	はい	いいえ
MR44	はい	はい	はい	はい	はい	はい
MR45	はい	はい	はい	はい	はい	はい
MR46	はい	はい	はい	はい	はい	はい
MR52	はい	はい	はい	はい	はい	いいえ
MR53	はい	はい	はい	はい	はい	いいえ
MR55	はい	はい	はい	はい	はい	はい
MR56	はい	はい	はい	はい	はい	はい
MR57	はい	はい	はい	はい	はい	はい
MX64W	はい	はい	はい	はい	はい	いいえ
MX65W	はい	はい	はい	はい	はい	いいえ
MX67W	はい	はい	はい	はい	はい	いいえ

MX68W	はい	はい	はい	はい	はい	いいえ
Z3	はい	はい	はい	はい	はい	いいえ

注：上に明記されていないアクセスポイントモデルはサポートされません。C

isco Aironet 1500

シリーズ屋外用アクセスポイントは、現在サポートされていません。

MESH モードで動作するアクセスポイントモデルはサポートされません。

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

主な機能の一部を以下に示します。

- 5 GHz (802.11a/n/ac/ax)
- Wi-Fi Protected Access v3 (WPA3+AES)
- Wi-Fi マルチメディア (WMM)
- DiffServ コードポイント (DSCP)
- サービスクラス (CoS/802.1p)

アンテナシステム

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

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

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

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

プロトコル

次の音声およびワイヤレス LAN のプロトコルがサポートされています。

- 802.11a、b、d、e、g、h、i、n、ac、ax
- Wi-Fi マルチメディア (WMM)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
 - AAC-LD、Opus、G.722、G.711、G.722.1、G.729
 - H.264、H.263
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- Hypertext Transfer Protocol (HTTP)

Wi-Fi

次の表は、Cisco RoomOS Series で使用される各 802.11 モードのデータレートごとの最大送信電力と受信感度の情報を示しています。

Cisco RoomOS Series 1

5 GHz の仕様

モデル	5 GHz - 802.11a	データレート	空間ストリー	変調		
Cisco Board 55 Cisco Board 55s Cisco Board 70 Cisco Board 70s Cisco Board 85s Cisco Board Pro 55 Cisco Board Pro 75 Cisco Codec Plus Cisco Codec Pro	最大 Tx パワー = 20 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK		
		9 Mbps	1	OFDM - BPSK		
		12 Mbps	1	OFDM - QPSK		
		18 Mbps	1	OFDM - QPSK		
		24 Mbps	1	OFDM - 16 QAM		
		36 Mbps	1	OFDM - 16 QAM		
		48 Mbps	1	OFDM - 64 QAM		
		54 Mbps	1	OFDM - 64 QAM		
		5 GHz - 802.11n (HT20)				
		データレート 空間ストリー 変調				
Cisco Desk Limited Edition Cisco Desk Pro Cisco Room 55 Cisco Room 55 Dual Cisco Room 70 Single Cisco Room 70 Dual Cisco Room 70 Single G2 Cisco Room 70 Dual G2 Cisco Room 70 Panorama Cisco Room Panorama Cisco Room Kit Cisco Webex Room Kit Mini Cisco Room USB	最大送信電力 = 19 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK		
		14 Mbps (MCS 1)	1	OFDM - QPSK		
		21 Mbps (MCS 2)	1	OFDM - QPSK		
		29 Mbps (MCS 3)	1	OFDM - 16 QAM		
		43 Mbps (MCS 4)	1	OFDM - 16 QAM		
		58 Mbps (MCS 5)	1	OFDM - 64 QAM		
		65 Mbps (MCS 6)	1	OFDM - 64 QAM		
		72 Mbps (MCS 7)	1	OFDM - 64 QAM		
		14 Mbps (MCS 8)	2	OFDM - BPSK		
		28 Mbps (MCS 9)	2	OFDM - QPSK		
		43 Mbps (MCS	2	OFDM - QPSK		
		58 Mbps (MCS	2	OFDM - 16 QAM		
		87 Mbps (MCS	2	OFDM - 16 QAM		
		116 Mbps (MCS 13)	2	OFDM - 64 QAM		
		130 Mbps (MCS 14)	2	OFDM - 64 QAM		
		144 Mbps (MCS 付近)	2	OFDM - 64 QAM		
5 GHz - 802.11n (HT40)						
データレート 空間ストリーム 変調						
	最大 Tx パワー = 18 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK		
		30 Mbps (MCS 1)	1	OFDM - QPSK		
		45 Mbps (MCS 2)	1	OFDM - QPSK		
		60 Mbps (MCS 3)	1	OFDM - 16 QAM		

		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		30 Mbps (MCS 8)	2	OFDM - BPSK
		60 Mbps (MCS 9)	2	OFDM - QPSK
		90 Mbps (MCS 10)	2	OFDM - QPSK
		120 Mbps (MCS 11)	2	OFDM - 16 QAM
		180 Mbps (MCS 12)	2	OFDM - 16 QAM
		240 Mbps (MCS 13)	2	OFDM - 64 QAM
		270 Mbps (MCS 14)	2	OFDM - 64 QAM
		300 Mbps (MCS 15)	2	OFDM - 64 QAM
	5 GHz - 802.11ac (VHT20)	データレート	空間ストリーム	変調
	最大送信電力 = 19 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		87 Mbps (MCS 8)	1	OFDM - 256 QAM
		14 Mbps (MCS 0)	2	OFDM - BPSK
		28 Mbps (MCS 1)	2	OFDM - QPSK
		43 Mbps (MCS 2)	2	OFDM - QPSK
		58 Mbps (MCS 3)	2	OFDM - 16 QAM
		87 Mbps (MCS 4)	2	OFDM - 16 QAM
		116 Mbps (MCS 5)	2	OFDM - 64 QAM
		130 Mbps (MCS 6)	2	OFDM - 64 QAM
		144 Mbps (MCS 7)	2	OFDM - 64 QAM
		173 Mbps (MCS 8)	2	OFDM - 256 QAM
		5 GHz - 802.11ac (VHT40)	データレート	空間ストリーム
	最大送信電力 = 18	15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK

dBm (地域によって異なる)	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM
	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
	300 Mbps (MCS 7)	2	OFDM - 64 QAM
	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT80)	データレート	空間ス トリー ム
最大送信電力 = 18 dBm (地域によって異なる)	33 Mbps (MCS 0)	1	OFDM - BPSK
	65 Mbps (MCS 1)	1	OFDM - QPSK
	98 Mbps (MCS 2)	1	OFDM - QPSK
	130 Mbps (MCS 3)	1	OFDM - 16 QAM
	195 Mbps (MCS 4)	1	OFDM - 16 QAM
	260 Mbps (MCS 5)	1	OFDM - 64 QAM
	293 Mbps (MCS 6)	1	OFDM - 64 QAM
	325 Mbps (MCS 7)	1	OFDM - 64 QAM
	390 Mbps (MCS 8)	1	OFDM - 256 QAM
	433 Mbps (MCS 9)	1	OFDM - 256 QAM
	65 Mbps (MCS 0)	2	OFDM - BPSK
	130 Mbps (MCS 1)	2	OFDM - QPSK
	195 Mbps (MCS 2)	2	OFDM - QPSK
	260 Mbps (MCS 3)	2	OFDM - 16 QAM
	390 Mbps (MCS 4)	2	OFDM - 16 QAM
	520 Mbps (MCS 5)	2	OFDM - 64 QAM
	585 Mbps (MCS 6)	2	OFDM - 64 QAM
650 Mbps (MCS 7)	2	OFDM - 64 QAM	
780 Mbps (MCS 8)	2	OFDM - 256 QAM	
867 Mbps (MCS 9)	2	OFDM - 256 QAM	

2.4 GHz の仕様

モデル	2.4 GHz - 802.11b	データレート	空間ストリーム	変調
Cisco Board 55 Cisco Board 55s	最大送信電力 = 19 dBm (地域によって異なる)	1 Mbps	1	DSSS - BPSK
		2 Mbps	1	DSSS - QPSK
Cisco Board 70 Cisco Board 70s Cisco Board 85s		5.5 Mbps	1	DSSS - CCK
		11 Mbps	1	DSSS - CCK
Cisco Board Pro 55 Cisco Board Pro 75 Cisco Desk Pro Cisco Desk Limited Edition Cisco Room 55 Cisco Room 55 Dual Cisco Room 70 Single Cisco Room 70 Dual Cisco Room 70 Single G2 Cisco Room 70 Dual G2 Cisco Room 70 Panorama Cisco Room Panorama Cisco Room Kit Cisco Room Kit Mini Cisco Room Kit Plus Cisco Room Kit Pro Cisco Room USB	2.4 GHz - 802.11g	データレート	空間ストリーム	変調
	最大送信電力 = 19 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	2.4 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
最大送信電力 = 19 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK	
	14 Mbps (MCS 1)	1	OFDM - QPSK	
	21 Mbps (MCS 2)	1	OFDM - QPSK	
	29 Mbps (MCS 3)	1	OFDM - 16 QAM	
	43 Mbps (MCS 4)	1	OFDM - 16 QAM	
	58 Mbps (MCS 5)	1	OFDM - 64 QAM	
	65 Mbps (MCS 6)	1	OFDM - 64 QAM	
	72 Mbps (MCS 7)	1	OFDM - 64 QAM	
	14 Mbps (MCS 8)	2	OFDM - BPSK	
	28 Mbps (MCS 9)	2	OFDM - QPSK	
	43 Mbps (MCS 10)	2	OFDM - QPSK	
	58 Mbps (MCS 11)	2	OFDM - 16 QAM	
	87 Mbps (MCS 12)	2	OFDM - 16 QAM	
	116 Mbps (MCS 13)	2	OFDM - 64 QAM	
	130 Mbps (MCS 14)	2	OFDM - 64 QAM	
144 Mbps (MCS 15)	2	OFDM - 64 QAM		

Cisco RoomOS Series 2

5 GHz の仕様

モデル	5 GHz - 802.11a	データレート	空間ストリーム	変調	
Cisco Desk Cisco Desk Mini Cisco Room Bar	最大送信電力 = 19 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK	
		9 Mbps	1	OFDM - BPSK	
		12 Mbps	1	OFDM - QPSK	
		18 Mbps	1	OFDM - QPSK	
		24 Mbps	1	OFDM - 16 QAM	
		36 Mbps	1	OFDM - 16 QAM	
		48 Mbps	1	OFDM - 64 QAM	
		54 Mbps	1	OFDM - 64 QAM	
		5 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
	最大送信電力 = 19 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK	
		14 Mbps (MCS 1)	1	OFDM - QPSK	
		21 Mbps (MCS 2)	1	OFDM - QPSK	
		29 Mbps (MCS 3)	1	OFDM - 16 QAM	
		43 Mbps (MCS 4)	1	OFDM - 16 QAM	
		58 Mbps (MCS 5)	1	OFDM - 64 QAM	
		65 Mbps (MCS 6)	1	OFDM - 64 QAM	
		72 Mbps (MCS 7)	1	OFDM - 64 QAM	
		14 Mbps (MCS 8)	2	OFDM - BPSK	
		28 Mbps (MCS 9)	2	OFDM - QPSK	
		43 Mbps (MCS 10)	2	OFDM - QPSK	
		58 Mbps (MCS 11)	2	OFDM - 16 QAM	
		87 Mbps (MCS 12)	2	OFDM - 16 QAM	
	116 Mbps (MCS 13)	2	OFDM - 64 QAM		
130 Mbps (MCS 14)	2	OFDM - 64 QAM			

		144 Mbps (MCS 付近)	2	OFDM - 64 QAM	
	5 GHz - 802.11n (HT40)	データレート	空間ストリーム	変調	
最大送信電力 = 18 dBm (地域によって異なる)		15 Mbps (MCS 0)	1	OFDM - BPSK	
		30 Mbps (MCS 1)	1	OFDM - QPSK	
		45 Mbps (MCS 2)	1	OFDM - QPSK	
		60 Mbps (MCS 3)	1	OFDM - 16 QAM	
		90 Mbps (MCS 4)	1	OFDM - 16 QAM	
		120 Mbps (MCS 5)	1	OFDM - 64 QAM	
		135 Mbps (MCS 6)	1	OFDM - 64 QAM	
		150 Mbps (MCS 7)	1	OFDM - 64 QAM	
		30 Mbps (MCS 8)	2	OFDM - BPSK	
		60 Mbps (MCS 9)	2	OFDM - QPSK	
		90 Mbps (MCS 10)	2	OFDM - QPSK	
		120 Mbps (MCS 11)	2	OFDM - 16 QAM	
		180 Mbps (MCS 12)	2	OFDM - 16 QAM	
		240 Mbps (MCS 13)	2	OFDM - 64 QAM	
		270 Mbps (MCS 14)	2	OFDM - 64 QAM	
		300 Mbps (MCS 15)	2	OFDM - 64 QAM	
	5 GHz - 802.11ac (VHT20)	データレート	空間ストリーム	変調	
	最大送信電力 = 19 dBm (地域によって異なる)		7 Mbps (MCS 0)	1	OFDM - BPSK
			14 Mbps (MCS 1)	1	OFDM - QPSK
			21 Mbps (MCS 2)	1	OFDM - QPSK
			29 Mbps (MCS 3)	1	OFDM - 16 QAM
			43 Mbps (MCS 4)	1	OFDM - 16 QAM
			58 Mbps (MCS 5)	1	OFDM - 64 QAM
			65 Mbps (MCS 6)	1	OFDM - 64 QAM
			72 Mbps (MCS 7)	1	OFDM - 64 QAM
			87 Mbps (MCS 8)	1	OFDM - 256 QAM
			14 Mbps (MCS 0)	2	OFDM - BPSK
			28 Mbps (MCS 1)	2	OFDM - QPSK
		43 Mbps (MCS 2)	2	OFDM - QPSK	
	58 Mbps (MCS 3)	2	OFDM - 16 QAM		
	87 Mbps (MCS 4)	2	OFDM - 16 QAM		

		116 Mbps (MCS 5)	2	OFDM - 64 QAM
		130 Mbps (MCS 6)	2	OFDM - 64 QAM
		144 Mbps (MCS 7)	2	OFDM - 64 QAM
		173 Mbps (MCS 8)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT40)	データレート	空間ストリーム	変調
最大送信電力 = 18 dBm (地域によって異なる)		15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK
		45 Mbps (MCS 2)	1	OFDM - QPSK
		60 Mbps (MCS 3)	1	OFDM - 16 QAM
		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		180 Mbps (MCS 8)	1	OFDM - 256 QAM
		200 Mbps (MCS 9)	1	OFDM - 256 QAM
		30 Mbps (MCS 0)	2	OFDM - BPSK
		60 Mbps (MCS 1)	2	OFDM - QPSK
		90 Mbps (MCS 2)	2	OFDM - QPSK
		120 Mbps (MCS 3)	2	OFDM - 16 QAM
		180 Mbps (MCS 4)	2	OFDM - 16 QAM
		240 Mbps (MCS 5)	2	OFDM - 64 QAM
		270 Mbps (MCS 6)	2	OFDM - 64 QAM
		300 Mbps (MCS 7)	2	OFDM - 64 QAM
	最大送信電力 = 17 dBm (地域によって異なる)		360 Mbps (MCS 8)	2
		400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)		データレート	空間ストリーム	変調
		33 Mbps (MCS 0)	1	OFDM - BPSK
		65 Mbps (MCS 1)	1	OFDM - QPSK
		98 Mbps (MCS 2)	1	OFDM - QPSK
		130 Mbps (MCS 3)	1	OFDM - 16 QAM
		195 Mbps (MCS 4)	1	OFDM - 16 QAM
		260 Mbps (MCS 5)	1	OFDM - 64 QAM
		293 Mbps (MCS 6)	1	OFDM - 64 QAM
		325 Mbps (MCS 7)	1	OFDM - 64 QAM
		390 Mbps (MCS 8)	1	OFDM - 256 QAM
		433 Mbps (MCS 9)	1	OFDM - 256 QAM
	65 Mbps (MCS 0)	2	OFDM - BPSK	
	130 Mbps (MCS 1)	2	OFDM - QPSK	

	195 Mbps (MCS 2)	2	OFDM - QPSK
	260 Mbps (MCS 3)	2	OFDM - 16 QAM
	390 Mbps (MCS 4)	2	OFDM - 16 QAM
	520 Mbps (MCS 5)	2	OFDM - 64 QAM
	585 Mbps (MCS 6)	2	OFDM - 64 QAM
	650 Mbps (MCS 7)	2	OFDM - 64 QAM
	780 Mbps (MCS 8)	2	OFDM - 256 QAM
	867 Mbps (MCS 9)	2	OFDM - 256 QAM

2.4 GHz の仕様

モデル	2.4 GHz - 802.11b	データレート	空間ストリーム	変調	
Cisco Desk Cisco Desk Mini Cisco Room Bar	最大送信電力 = 22 dBm (地域によって異なる)	1 Mbps	1	DSSS - BPSK	
		2 Mbps	1	DSSS - QPSK	
		5.5 Mbps	1	DSSS - CCK	
		11 Mbps	1	DSSS - CCK	
	2.4 GHz - 802.11g	データレート	空間ストリーム	変調	
	最大送信電力 = 21 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK	
		9 Mbps	1	OFDM - BPSK	
		12 Mbps	1	OFDM - QPSK	
		18 Mbps	1	OFDM - QPSK	
		24 Mbps	1	OFDM - 16 QAM	
		36 Mbps	1	OFDM - 16 QAM	
		48 Mbps	1	OFDM - 64 QAM	
			54 Mbps	1	OFDM - 64 QAM
		2.4 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
最大送信電力 = 20 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK		
	14 Mbps (MCS 1)	1	OFDM - QPSK		
	21 Mbps (MCS 2)	1	OFDM - QPSK		
	29 Mbps (MCS 3)	1	OFDM - 16 QAM		
	43 Mbps (MCS 4)	1	OFDM - 16 QAM		
	58 Mbps (MCS 5)	1	OFDM - 64 QAM		
	65 Mbps (MCS 6)	1	OFDM - 64 QAM		
	72 Mbps (MCS 7)	1	OFDM - 64 QAM		
	14 Mbps (MCS 8)	2	OFDM - BPSK		
	28 Mbps (MCS 9)	2	OFDM - QPSK		

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

Cisco RoomOS Series 3

5 GHz の仕様

モデル	5 GHz - 802.11a	データレート	空間ストリーム	変調
Cisco Codec EQ Cisco Room Bar Pro	最大送信電力 = 19 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	5 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
	最大送信電力 = 19 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
			43 Mbps (MCS 4)	1
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK

	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 付近)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	データレート	空間ストリーム	変調
最大送信電力 = 18 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	30 Mbps (MCS 8)	2	OFDM - BPSK
	60 Mbps (MCS 9)	2	OFDM - QPSK
	90 Mbps (MCS 10)	2	OFDM - QPSK
	120 Mbps (MCS 11)	2	OFDM - 16 QAM
	180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM
	270 Mbps (MCS 14)	2	OFDM - 64 QAM
300 Mbps (MCS 15)	2	OFDM - 64 QAM	
5 GHz - 802.11ac (VHT20)	データレート	空間ストリーム	変調
最大送信電力 = 19 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM

		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		87 Mbps (MCS 8)	1	OFDM - 256 QAM
		14 Mbps (MCS 0)	2	OFDM - BPSK
		28 Mbps (MCS 1)	2	OFDM - QPSK
		43 Mbps (MCS 2)	2	OFDM - QPSK
		58 Mbps (MCS 3)	2	OFDM - 16 QAM
		87 Mbps (MCS 4)	2	OFDM - 16 QAM
		116 Mbps (MCS 5)	2	OFDM - 64 QAM
		130 Mbps (MCS 6)	2	OFDM - 64 QAM
		144 Mbps (MCS 7)	2	OFDM - 64 QAM
		173 Mbps (MCS 8)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT40)	データレート	空間ストリーム	変調
	最大送信電力 = 18 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK
		45 Mbps (MCS 2)	1	OFDM - QPSK
		60 Mbps (MCS 3)	1	OFDM - 16 QAM
		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		180 Mbps (MCS 8)	1	OFDM - 256 QAM
		200 Mbps (MCS 9)	1	OFDM - 256 QAM
		30 Mbps (MCS 0)	2	OFDM - BPSK
		60 Mbps (MCS 1)	2	OFDM - QPSK
		90 Mbps (MCS 2)	2	OFDM - QPSK
		120 Mbps (MCS 3)	2	OFDM - 16 QAM
		180 Mbps (MCS 4)	2	OFDM - 16 QAM
		240 Mbps (MCS 5)	2	OFDM - 64 QAM
		270 Mbps (MCS 6)	2	OFDM - 64 QAM
		300 Mbps (MCS 7)	2	OFDM - 64 QAM
		360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM	
	5 GHz - 802.11ac (VHT80)	データレート	空間ストリーム	変調
	最大送信電力 = 17 dBm (地域によって異なる)	33 Mbps (MCS 0)	1	OFDM - BPSK
		65 Mbps (MCS 1)	1	OFDM - QPSK
		98 Mbps (MCS 2)	1	OFDM - QPSK
		130 Mbps (MCS 3)	1	OFDM - 16 QAM
		195 Mbps (MCS 4)	1	OFDM - 16 QAM

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

2.4 GHz の仕様

モデル	2.4 GHz - 802.11b	データレート	空間ストリーム	変調
Cisco Codec EQ Cisco Room Bar Pro	最大送信電力 = 22 dBm (地域によって異なる)	1 Mbps	1	DSSS - BPSK
		2 Mbps	1	DSSS - QPSK
		5.5 Mbps	1	DSSS - CCK
		11 Mbps	1	DSSS - CCK
	2.4 GHz - 802.11g	データレート	空間ストリーム	変調
	最大送信電力 = 21 dBm (地域によって異なる)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	2.4 GHz - 802.11n (HT20)	データレート	空間ストリーム	変調
	最大送信電力 = 20 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
21 Mbps (MCS 2)		1	OFDM - QPSK	

		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK
		58 Mbps (MCS 11)	2	OFDM - 16 QAM
		87 Mbps (MCS 12)	2	OFDM - 16 QAM
		116 Mbps (MCS 13)	2	OFDM - 64 QAM
		130 Mbps (MCS 14)	2	OFDM - 64 QAM
		144 Mbps (MCS 15)	2	OFDM - 64 QAM

注：受信感度は、特定のデータレートでパケットをデコードするのに最低限必要な信号強度です。
上記の値は、純粋な無線仕様であって、一体型デュアルアンテナのゲインは考慮されていません。

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

規制

ワールドモード（802.11d）では、さまざまな領域でクライアントを使用できます。ローカル環境のアクセスポイントによってアドバタイズされるチャンネルと送信電力の使用に対してクライアントを適合させることができます。

Cisco RoomOS Series は、アクセスポイントが 802.11d に対応していて、地域ごとに使用するチャンネルと送信電力を決定できる場合に最適に動作します。

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

一部の 5 GHz チャンネルはレーダー技術でも使用されており、該当レーダー周波数（DFS チャンネル）を使用するには、802.11 クライアントとアクセスポイントが 802.11h に準拠している必要があります。802.11h では、802.11d を有効にする必要があります。

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

802.11d が有効になっていない場合、Cisco RoomOS Series は、少ない送信電力でアクセスポイントへの接続を試みます。

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

オーストラリア(AU)	ハンガリー(HU)	フィリピン(PH)
オーストリア(AT)	アイスランド(IS)	ポーランド(PL)
バーレーン(BH)	インド(IN)	ポルトガル (PT)
ベルギー (BE)	アイルランド(IE)	プエルトリコ(PR)
ブラジル(BR)	イスラエル(IL)	ルーマニア (RO)

ブルガリア (BG)	イタリア (IT)	ロシア連邦(RU)
カナダ(CA)	日本 (JP)	サウジアラビア(SA)
チリ(CL)	韓国 (KR)	セルビア(RS)
中国(CN)	ラトビア(LV)	シンガポール (SG)
コロンビア (CO)	リヒテンシュタイン(LI)	スロバキア (SK)
コスタリカ (CR)	リトアニア(LT)	スロベニア (SI)
クロアチア (HR)	ルクセンブルク(LU)	南アフリカ (ZA)
キプロス (CY)	マケドニア (MK)	スペイン (ES)
チェコ共和国 (CZ)	マレーシア (MY)	スウェーデン (SE)
デンマーク (DK)	マルタ (MT)	スイス (CH)
ドミニカ共和国 (DO)	メキシコ (MX)	台湾 (TW)
エクアドル (EC)	モナコ (MC)	タイ (TH)
エジプト (EG)	モンテネグロ (ME)	トルコ (TR)
エストニア (EE)	オランダ (NL)	ウクライナ (UA)
フィンランド (FI)	ニュージーランド (NZ)	アラブ首長国連邦 (AE)
フランス (FR)	ナイジェリア (NG)	イギリス (GB)
ドイツ (DE)	ノルウェー (NO)	アメリカ合衆国 (US)
ジブラルタル (GI)	パナマ(PA)	ウルグアイ (UY)
ギリシャ (GR)	パラグアイ (PY)	ベトナム (VN)
香港(HK)	ペルー(PE)	

注：コンプライアンス情報は、Cisco Product Approval Status Web サイト、<https://cae-cnc-prd.cisco.com/pdtcnc>で入手できます。

[Bluetooth]

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

Bluetooth では、30 フィートの範囲内であれば低帯域幅のワイヤレス接続が可能です。Bluetooth デバイスは常に Cisco RoomOS Series から 10 フィート以内で使用することを推奨します。

Bluetooth

デバイスは、電話機から直接見通せる場所にある必要はありませんが、壁や扉などの障害物があると、品質に悪影響を及ぼす可能性があります。

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

Bluetooth プロファイル

Cisco RoomOS Series は、次の Bluetooth プロファイルをサポートしています。

- 高度なオーディオ配信プロファイル (A2DP)
- オーディオ/ビデオリモート制御プロファイル (AVRCP)
- 汎用アクセスプロファイル (GAP)
- 汎用オーディオ/ビデオ配信プロファイル (GAVDP)
- ハンズフリープロファイル (HFP)

共存 (802.11b/g/n/ax + Bluetooth)

802.11b/g/n/ax と Bluetooth を共存させて同時に使用する場合、両方とも 2.4 GHz の周波数範囲を利用するので、いくつかの制限と導入要件を考慮する必要があります。

容量

802.11b/g/n/ax + Bluetooth を共存させる場合、802.11g/n/ax と Bluetooth の送受信を保護する CTS の利用により、コール キャパシティが減少します。

マルチキャストオーディオ

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

音声品質

現在のデータレート設定に応じて、共存モードの使用時に Bluetooth 転送を保護するために CTS を送信できます。

一部の環境では、6 Mbps を有効にする必要があります。

注：802.11b/g/n/ax と Bluetooth は両方とも 2.4 GHz を利用しますが、上記の制限もあるため、Bluetooth を使用する場合には 802.11a/n/ac/ax を使用することを推奨します。

言語

Cisco RoomOS Series は、次の言語をサポートしています。

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

ビデオ コール

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

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

H.264 は 30

fps (フレーム/秒) がサポートされるビデオストリームで使用されるプロトコルです。サポートするオーディオコーデックの 1

つを使用する音声セッション用に別のストリームがあります。

Cisco RoomOS Series

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

次のビデオ形式がサポートされます：

- QnHD 180p (320 x 180)
- CIF 288p (512x288)

- nHD 360p (640 X 360)
- SD 448p (768×448)
- WSVGA 576p (1024 x 576)
- HD 720p (1280 X 720)
- HD 1080p (1920 X 1080)

デバイスの手入れ

Cisco RoomOS Series をクリーニングするには、柔らかい布を湿らせてデバイスを拭いてください。デバイスを損傷する可能性があるため、液体や粉末をデバイスに直接塗布しないでください。デバイスの清掃に漂白剤などの腐食作用のある製品を使用しないでください。デバイスを損傷する可能性があるため、デバイスのクリーニングに圧縮空気を使用しないでください。

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

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

ワイヤレス LAN の設計

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

802.11 ネットワーク

次のガイドラインを使用して、各ワイヤレス環境でのチャンネル使用を計画します。

5 GHz (802.11a/n/ac/ax)

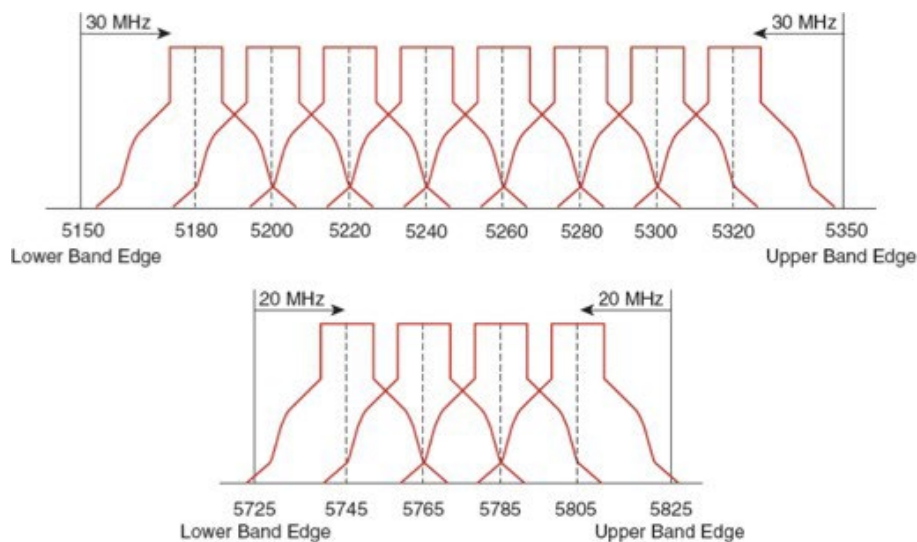
5 GHz は、Cisco RoomOS Series の運用で使用するよう推奨されている周波数帯域です。

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

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

Cisco RoomOS Series は、802.11h の動的周波数選択 (DFS) と Transmit Power Control (TPC) をサポートしています。これらは、5.260 ~ 5.720 GHz で動作するチャンネルを使用する場合に必要です。使用可能な 25 チャンネルのうち 16 チャンネルがこれに該当します。

802.11a/n/ac/ax 環境に Cisco RoomOS Series を展開する場合は、隣接チャンネルと 20% 以上オーバーラップさせる必要があります。これにより、シームレスなローミングが実現します。重要なエリアでは、Cisco RoomOS Series がアクセスポイントの受信感度 (現在のデータレートに必要な信号レベル) を満たしながら、少なくとも 2 台のアクセスポイントで -67 dBm 以上の信号レベルを確保できるように、オーバーラップを増やす (30% 以上) ことを推奨します。



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

動的周波数選択 (DFS)

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

TPC ではクライアントとアクセスポイントが情報を交換できるため、クライアントは送信電力を動的に調整できます。クライアントは、アクセスポイントとのアソシエーションを所定のデータレートで維持するために、必要最低限のエネルギーを使用します。結果として、クライアントが隣接セルの干渉原になる可能性が低下するため、より密集したパフォーマンスの高いワイヤレス LAN を実現できます。

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

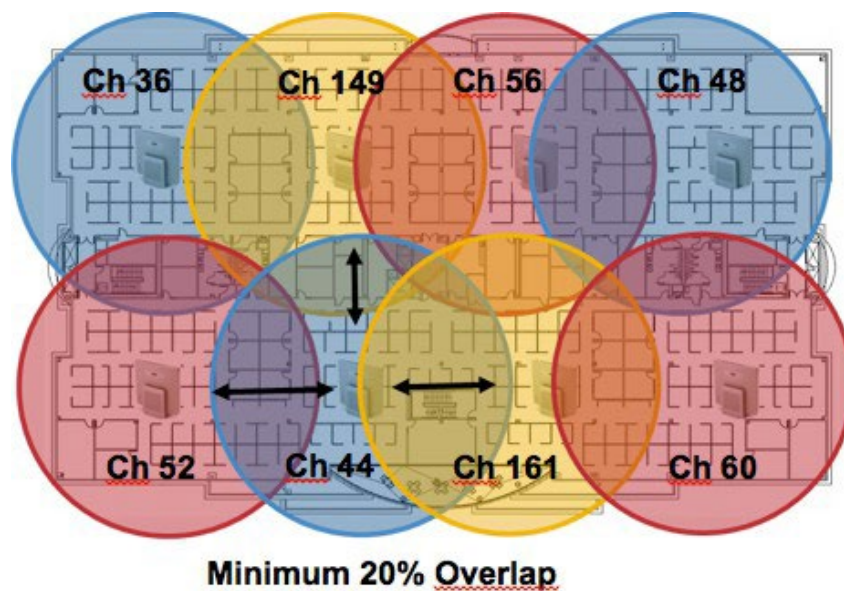
非 DFS チャンネルにアクセスポイントが存在する場合は、音声の中断を最小限に抑えられます。

レーダーアクティビティに備えて、非 DFS チャンネル (UNII-1) を使用するアクセスポイントをエリアごとに少なくとも一つ設置します。これにより、新しい使用可能チャンネルのスキャン中にアクセスポイントの無線がホールドオフ期間になっているときもチャンネルを使用できます。

UNII-3 チャンネル (5.745 ~ 5.825

GHz) は (利用可能であれば) 任意で使用できます。次に、5 GHz

ワイヤレス LAN の導入例を示します。



5 GHz の場合、南・北・中央アメリカでは 25 チャンネル、欧州では 16 チャンネル、日本では 19 チャンネルを使用できます。

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

UNII-2 拡張チャンネル（チャンネル 100 ～ 144）の使用を予定している場合は、アクセス ポイント上で UNII-2（チャンネル 52 ～ 64）を無効にして、有効になるチャンネルの数が多くなり過ぎないようにすることが推奨されます。ワイヤレス LAN で多数の 5 GHz チャンネルを有効にすると、新しいアクセス ポイントの検出が遅れる可能性があります。

2.4 802.11 (b/g/n/ax)

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

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

2.4 GHz (802.11b/g/n/ax) 環境では、VoWLAN

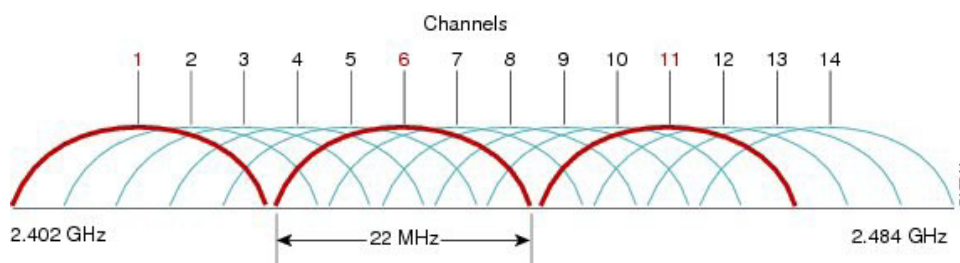
を導入するとき、帯域の重なりのないチャンネルだけを利用する必要があります。帯域の重なりのないチャンネルとは、22 MHz の間隔があり、少なくとも 5 チャンネル離れたもののことです。

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

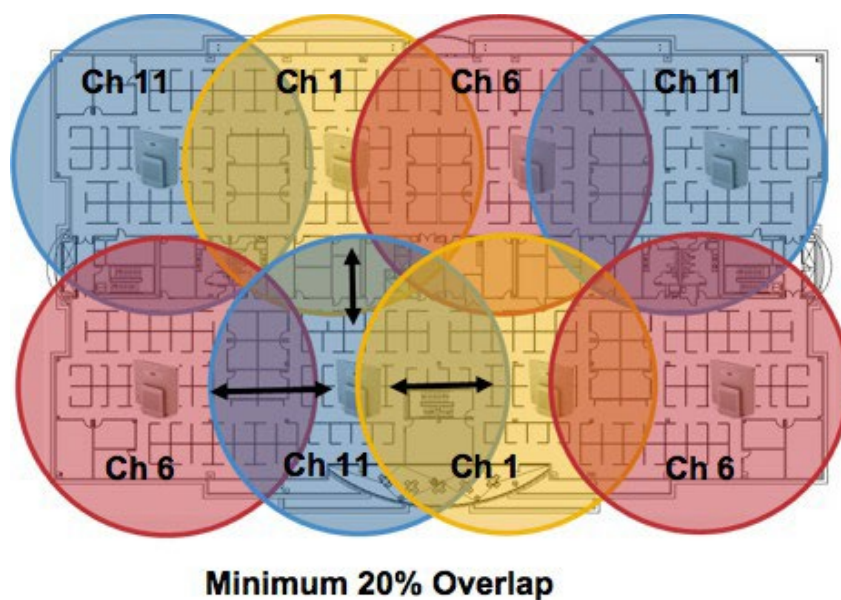
802.11b/g/n/ax 環境に Cisco RoomOS Series

を展開する場合は、帯域の重なりのないチャンネルを使用する必要があり、隣接チャンネルとのオーバーラップは少なくとも 20% 許容される必要があります。これにより、シームレスなローミングが実現します。

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



次に、2.4 GHz ワイヤレス LAN の導入例を示します。



信号強度とカバレッジ

許容可能な音声品質を保証するため、Cisco RoomOS Series は 5 GHz または 2.4 GHz を使用する際、-67 dBm 以上の信号を常に維持します。これはまた、アクセスポイントの受信機感度で、送信されたデータレートに対応するために必要な信号レベルを満たすことにもなります。

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

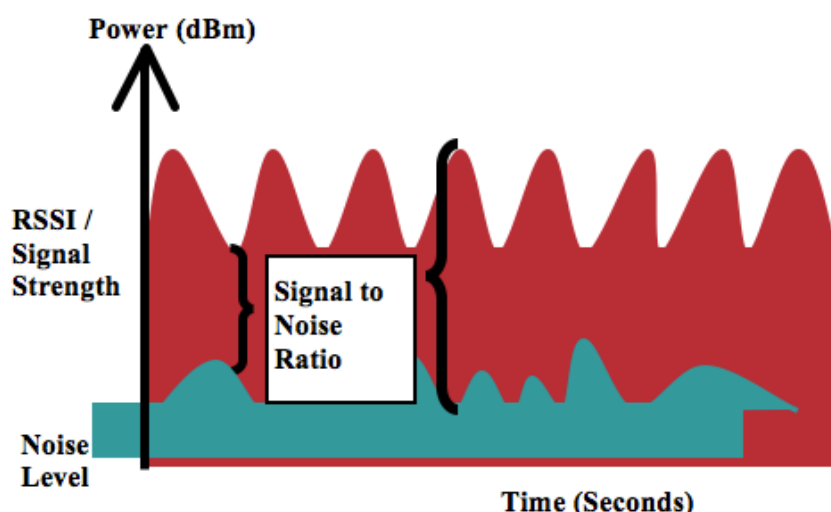
少なくとも 25 dB の信号対雑音比 (SNR) 、つまり -67 dBm の信号に対して -92 dBm のノイズレベルを維持する必要があります。

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

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

2.4 GHz の場合は最小データ レートを 11 Mbps または 12 Mbps に（802.11b クライアント サポート ポリシーに従う）、5 GHz の場合は最小データ レートを 12 Mbps に設定することが推奨されます。これは、唯一の必須/基本レートとして設定する必要もあります。一部の環境では、必須/基本レートとして 6 Mbps

を有効する必要があります。上記の各要件を考慮すると、シングル チャンネル計画は導入すべきではありません。



アクセス

ポイントの設置を設計するときには、必ず、すべての重要エリアが適切にカバー（信号が到達）されるようにしてください。

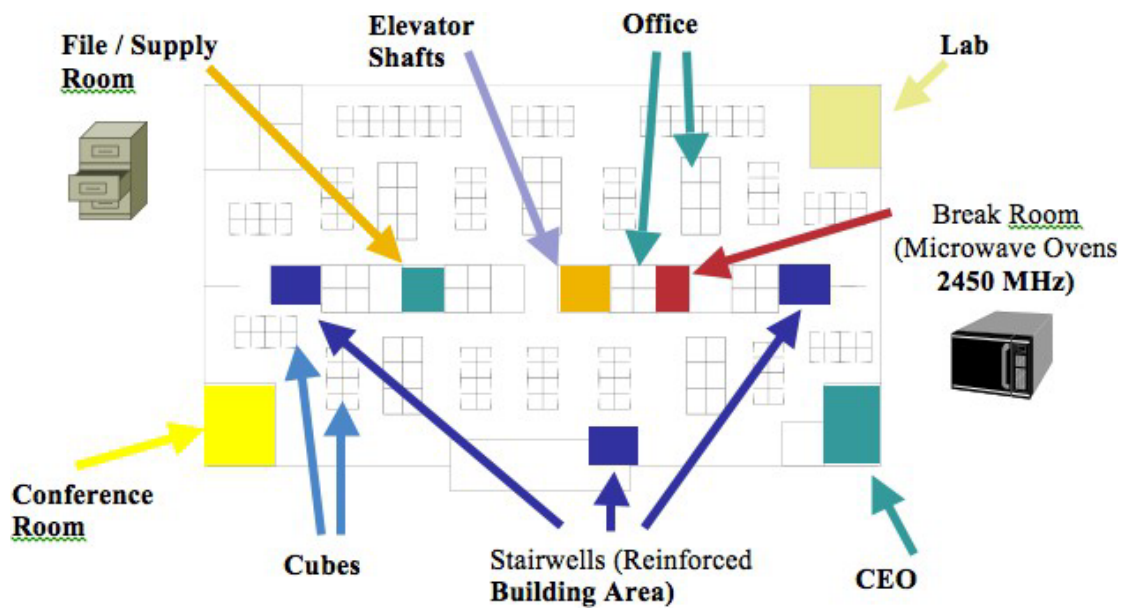
データ専用アプリケーションのための一般的なワイヤレス LAN 導入では、エレベータ、階段、屋外通路といった、VoWLAN サービスで必要とされる一部のエリアにはカバレッジが提供されません。

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

電子レンジは、2450 MHz で動作します。これは、802.11b/g/n/ax のチャンネル 8 と 9 の間に位置します。一部の電子レンジは他のものよりもシールドが強化されており、エネルギーの拡散が低減されています。電子レンジのエネルギーは、チャンネル 11 に悪影響を及ぼす可能性もあります。さらに一部の電子レンジは、周波数範囲全体（チャンネル 1 ～ 11）に影響します。電子レンジの干渉を回避するために、電子レンジの近くに配置されるアクセスポイントでは、チャンネル 1 を使用してください。

ほとんどの電子レンジ、Bluetooth、および周波数ホッピング デバイスは、5 GHz 周波数に対しても同様の悪影響を与えることはありません。802.11a/n/ac/ax テクノロジーでは、帯域の重なりのないチャンネルが増えるため、通常、初期 RF 使用率はより低くなります。音声展開の場合、音声には 802.11a/n/ac/ax を使用し、データには 802.11b/g/n/ax を使用することを推奨します。

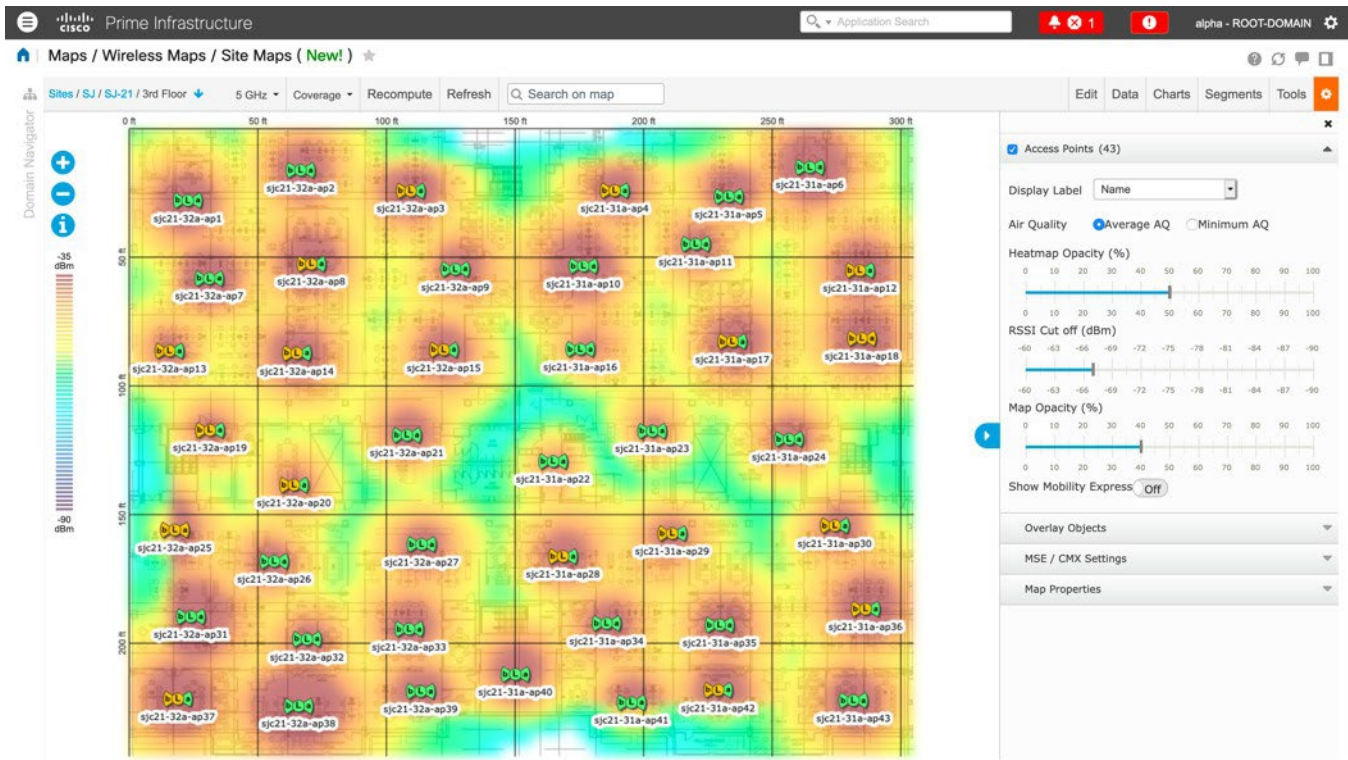
ただし、免許申請の必要のない 5 GHz 周波数を利用する製品も存在します（たとえば、5.8 GHz コードレス電話機も、UNII-3 チャンネルに悪影響を及ぼす可能性があります）。



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

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

Cisco Prime Infrastructure を使用して、信号強度とカバレッジを確認できます。



データ レート

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

Cisco RoomOS Series にはデュアルアンテナがあるため、802.11n の最大 MCS 15

データレートをサポートします (最大 300 Mbps)。802.11ac の場合、Cisco RoomOS Series は最大 VHT80 MCS 9 2SS をサポートします (最大 867 Mbps)。

802.11ax の場合、対応する Cisco RoomOS Series は最大 HE80 MCS 11 をサポートします (最大 1200 Mbps)。

一部の 802.11n/ac/ax クライアントは、MIMO (複数入力/出力) アンテナテクノロジーを利用し、同じ帯域周波数でこれより高い MCS レートを使用できるので、より高いレートを有効にしておくこともできます。

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

802.11b クライアントがワイヤレス ネットワーク内に存在する場合は、802.11b のレートを有効にする必要があります。802.11b のレートのみを必須/基本レートとして設定できます。

推奨されるデータ レート設定は次のとおりです。

5 GHz

802.11 モード	必須 データ レート	サポートされる データ レート	無効な データ レート
------------	---------------	--------------------	----------------

802.11ax	12 Mbps	18 ~ 54 Mbps、 HE MCS 0 ~ MCS 11 1SS、HE MCS 0 ~ MCS 11 2SS	6、9 Mbps
802.11ac	12 Mbps	18 ~ 54 Mbps、	6、9 Mbps
		VHT MCS 0 ~ MCS 9 1SS、VHT MCS 0 ~ MCS 9 2SS、(VHT MCS 0 ~ MCS 9 3SS)、(VHT MCS 0 ~ MCS 9 4SS)	
802.11n	12 Mbps	18 ~ 54 Mbps、 HT MCS 0 - MCS 15、 (HT MCS 16 - MCS 31)	6、9 Mbps
802.11a	12 Mbps	18 ~ 54 Mbps	6、9 Mbps

2.4 GHz

802.11 モード	必須 データ レート	サポートされる データ レート	無効な データ レート
802.11ax	12 Mbps	18 ~ 54 Mbps、 HE MCS 0 ~ MCS 11 1SS、HE MCS 0 ~ MCS 11 2SS	1、2、5.5、6、9、11 Mbps
802.11n	12 Mbps	18 ~ 54 Mbps、 HT MCS 0 - MCS 15、 (HT MCS 16 - MCS 31)	1、2、5.5、6、9、11 Mbps
802.11g	12 Mbps	18 ~ 54 Mbps	1、2、5.5、6、9、11 Mbps
802.11b	11 Mbps	なし	1、2、5.5 Mbps

音声専用アプリケーションでは、24 Mbps よりも高いデータ レートを有効にも、無効にも選択できますが、キャパシティとスループットには影響しません。また、これらのレート を有効にすると、データ フレームの再試行回数が増える可能性があります。

ビデオなどの他のアプリケーションでは、24 Mbps よりも高いデータ レートを有効にすると、恩恵が受けられる場合があります。高いキャパシティとスループットを維持するには、24 Mbps 以上のデータ レートを有効にしてください。

過度の再試行数が問題となる可能性がある環境への展開の場合、データレートの制限付きセットを使用できます。この場合、最低の有効なレートは必須/基本レートです。

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

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

単一必須/基本レートとして、有効な最低データ レートだけを設定します。マルチキャストパケットは、有効な最高必須/基本データ レートで送信されます。

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

条件の厳しい環境

Cisco RoomOS Series

を条件の厳しい環境（製造、倉庫、小売業など）に展開する場合、標準の推奨事項に追加の調整が必要となる場合があります。

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

アクセス ポイントおよびアンテナの選択

条件の厳しい環境では、外部アンテナを必要とするアクセスポイントプラットフォームを選択することを推奨します。条件の厳しい環境で適切に機能するアンテナタイプを選択することも大切です。

アクセス ポイントの配置

Cisco RoomOS Series
とアクセスポイント間の障害物を最小限にし、アクセスポイントのアンテナからの見通しが可能なようにすることが重要です。アクセスポイントまたはアンテナ、またはその両方が障害物の背後または金属面やガラス面の近くに配置されていないことを確認します。一部のエリアで一体型内部アンテナを搭載したアクセスポイントを使用する場合は、アクセスポイントを天井に取り付けることを推奨します。これらのアクセスポイントは無指向性アンテナを装備しており、壁面への設置を想定していません。

周波数帯域

これまで通り、5 GHz の使用が推奨されます。2.4 GHz を使用すると、正常に機能しない場合があります。802.11b レートが有効な場合は特に注意が必要です。5 GHz チャネルセットでは、8 または 12 チャネル計画のみを使用することを推奨します。可能な場合は、UNII-2 拡張チャネルを無効にします。

データ レート

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

送信電力

条件の厳しい環境ではマルチパスが高くなる可能性があることから、アクセスポイントと Cisco RoomOS Series の送信電力にも制限をかける必要があります。これは、条件の厳しい環境に 2.4 GHz を導入しようと計画している場合にさらに重要です。自動送信電力を使用する場合は、アクセスポイントの送信電力が指定した範囲（最大および最小の電力レベル）を使用するように設定して、アクセスポイント出力の過不足を防ぎます（5 GHz の場合、最低 11 dBm、最小 16 dBm）。Cisco RoomOS Series は、アクセスポイントの設定で DTPC が有効になっている場合、アクセスポイントの現在の送信電力設定を基に送信フレームの送信電力を決定します。

高速ローミング

高速ローミングには 802.11r/Fast Transition (FT) の使用が推奨されています。また 802.11r (FT) を有効にすると、2 つのフレームのみにローミングする場合にハンドシェイクのフレーム数も減少します。ローミング中にフレーム数が減ると、ローミングが成功する確率が向上します。802.1x 認証を使用している場合は、推奨された EAPOL キー設定を使用することが大切です。

Quality of Service (QoS)

音声、ビデオ、およびコール制御フレームの WMM UP タグが正しく設定されるように、DSCP

値が有線ネットワーク全体で保持されることを確認する必要があります。

ビームフォーミング

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

マルチパス

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

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

異なる波形を組み合わせると歪みが発生し、信号品質が低下するため、受信機のデコード機能にも悪影響を与えます。

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

次に、マルチパスの影響を示します。

データ破損

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

信号の空白

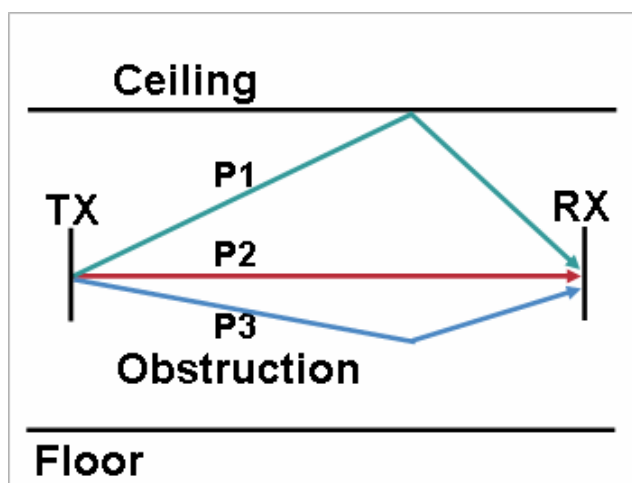
反射した波長が、メイン信号とちょうど位相がずれて到達し、メイン信号を完全に打ち消すような場合に発生します。

信号振幅の増大

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

信号振幅の減少

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



802.11a/n/ac/ax と 802.11g/n/ax

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

高マルチパス環境で 802.11b を使用する場合、それらのエリアには低いデータ

レートを使用してください（1 Mbps や 2 Mbps など）。このような環境には、ダイバーシティアンテナが役立つことがあります。

セキュリティ

ワイヤレス LAN を導入する場合、セキュリティが不可欠です。

Cisco RoomOS Series は、次のワイヤレスセキュリティ機能をサポートしています。

WLAN 認証

- エンタープライズ
 - WPA3 802.1x
 - EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
 - EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
 - EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)
 - PEAP (保護拡張認証プロトコル)
 - WPA2 802.1x
 - EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
 - EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
 - EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)
 - PEAP (保護拡張認証プロトコル)
- 個人
 - WPA3-SAE (Simultaneous Authentication of Equals)
 - WPA2-PSK (事前共有キー)
- なし

WLAN 暗号化

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

注：TKIP はブロードキャスト/マルチキャスト暗号としてしか使用できないため、アクセスポイントは AES (CCMP128) をサポートしている必要があります。CCMP256、GCMP128、および GCMP256 暗号化方式はサポートされていません。

Cisco RoomOS Series は、次の追加のセキュリティ機能もサポートしています。

- イメージ認証
- デバイス認証
- ファイル認証
- シグナリング認証
- メディア暗号化 (SRTP)
- シグナリング暗号化 (TLS)
- 認証局プロキシ機能 (CAPF)
- セキュア プロファイル
- 暗号化された設定ファイル

Extensible Authentication Protocol - セキュアなトンネリング経由の柔軟な認証 (EAP-FAST)

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

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

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

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

[匿名インバンドPACプロビジョニングを許可する (Allow anonymous in-band PAC provisioning)]

が有効な場合、EAP-GTC と EAP-MSCHAPv2 の両方も有効にする必要があります。EAP-FAST では、認証サーバ上にユーザ アカウントを作成する必要があります。

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

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

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

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

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

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

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

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

TLS は、ユーザとサーバの両方の認証用およびダイナミック セッション

キーの生成用に、証明書を使用する方法を提供します。証明書をインストールする必要があります。

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

EAP-TLS では、Cisco RoomOS Series

にインポートされた証明書の共通名と一致する認証サーバ上に、ユーザアカウントを作成する必要が生じることがあります。

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

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

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

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

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

Protected Extensible Authentication Protocol (PEAP)

Protected Extensible Authentication

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

構築後の認証情報の交換は暗号化されるため、ユーザクレデンシャルは盗聴から保護されます。PEAP-NONE、PEAP-GTC と PEAP-MSCHAPv2 はサポートされている内部認証プロトコルです。

PEAP では、認証サーバ上にユーザアカウントを作成する必要があります。

認証サーバは、Cisco RoomOS Series に証明書をインポートして検証されます。

Quality of Service (QoS)

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

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

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

トラフィックタイプ	コールサーバ	DSCP	802.1p	WMM UP	プロトコル
音声	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
	Webex	EF (46)	5	6	RTP (UDP 5004)
TelePresence Voice	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
	Webex	EF (46)	5	6	RTP (UDP 5004)
TelePresence ビデオ	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
	Webex	AF41 (34)	4	5	RTP (UDP 5004)
コール制御	CUCM	CS3 (24)	3	4	SIP (TCP 5060 ~ 5061)
	Webex	デフォルト (0)	0	0	HTTPS (TCP 443)

- 音声、インタラクティブビデオ、および呼制御パケットが適切な QoS マーキングを持ち、他のプロトコルがそれと同じ QoS マーキングを使用していないことを確認します。
- Cisco IOS スイッチ上で Differentiated Services Code Point (DSCP) の保護を有効にします。

Cisco IP Phone 8861 および 8865 と Cisco Unified Communications Manager で使用される TCP ポートおよび UDP ポートの詳細については、次の URL にある『Cisco Unified Communications Manager TCP and UDP Port Usage』を参照してください。

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

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

<https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services>

コール アドミッション制御 (CAC)

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

アクセスポイントで TSPEC

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

有線 QoS

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

WLAN デバイスのCisco スイッチ ポートの設定

Cisco ワイヤレス LAN コントローラ、Cisco 製アクセス ポイントのスイッチ

ポート、および任意のアップリンク スイッチ ポートを設定します。Cisco IOS

スイッチを使用する場合は、次のスイッチ ポート設定を使用します。

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

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

Cisco 製アクセス ポイントに対して DSCP 信頼状態を有効にする

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

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

導入ガイド』を参照してください。 https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf

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

有線 IP フォンのCisco スイッチ ポートの設定

Cisco 製の有線 IP フォンのスイッチ ポートでCisco

製電話機の信頼状態を有効にします。スイッチ設定の例を次に示

します。

```

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

```

ローミング

Cisco RoomOS Series は、両方の周波数セットを有効にします。これにより、Cisco RoomOS Series は 5 GHz または 2.4 GHz に接続でき、インターバンド ローミングのサポートが有効になります。

802.11r (FT) を使用しない 802.1x

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

802.11r (FT) を使用すると、ローミング時間を 100

ミリ秒未満に短縮できます。アクセスポイント間の移行時間をユーザーが体感することはありません。

セキュリティ タイプ	ローミング時間
個人	150 ミリ秒
エンタープライズ	300 ミリ秒

Cisco RoomOS Series は、スキャンおよびローミング イベントを管理します。

大半のローミングは、現在の RSSI に基づく必須 RSSI

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

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

帯域間のローミング

Cisco RoomOS Series

は両方の周波数セットを有効にし、インターバンドローミングを可能にし、その時点で最も強い信号を優先します。電力レベルが同じである場合、一般的に 2.4 GHz の方が信号強度がより強くなるので、2.4 GHz が 5 GHz よりも優先されます。

電源投入時に、Cisco RoomOS Series は、2.4 および 5 GHz

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

対象帯域を有効化して帯域間のローミングを実現するためにも、周波数帯分析を実施することが推奨されます。

電源管理

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

イーサネットを Cisco RoomOS Series に接続すると、ワイヤレス LAN は一時的に無効になります。ワイヤレス LAN が以前に有効化されていた場合は、イーサネットが切断された時点で、自動的に有効に復帰します。

Webex Desk Series は、アイドル状態または着信時に、主としてアクティブモード（Wi-Fi 節電なし）を使用します。電力節約なし（PS-NULL）フレームはオフチャネル スキャンで使用されます。

Delivery Traffic Indicator Message (DTIM)

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

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

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

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

コール キャパシティ

目的のコール キャパシティに対応するネットワークを設計します。

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

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

オーディオのみのコール

次に、アクセス ポイント/チャネルごとにサポートされるオーディオのみのコール（単一の双方向音声ストリーム）の最大数を示します。

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

ビデオ コール

ワイヤレス LAN 上でビデオ コールを行うと、コール キャパシティが著しく低下します。
Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

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

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

最大数 ビデオ コール	802.11 モード	オー ディ オ コー デッ ク	オーディ オ ビット レート	ビデ オタ イプ	ビデオ解 像度	ビデオ ビット レート
2-11+	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	HD 720p	1280 X 720	1000 kbps
1-7+	5 GHz または 2.4 GHz	G.722/G.711	64 Kbps	FHD 1080p	1920 X 1080	2500 Kbps

注：現在、コールアドミッションコントロールはサポートされていません。

マルチキャスト

ワイヤレス LAN でマルチキャストを有効にする場合は、パフォーマンスおよびキャパシティに配慮する必要があります。省電力モードのクライアントが関連付けられている場合、すべてのマルチキャストパケットは、DTIM 周期までキューイングされます。

Cisco RoomOS Series

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

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

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

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

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

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

注：802.11b/g/n/ax と Bluetooth

が同時に使用される共存モードを使用する場合、マルチキャスト音声はサポートされません。

Cisco ワイヤレス LAN の構成

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

Cisco ワイヤレス LAN コントローラおよび Lightweight アクセスポイントを設定するときは、次のガイドラインを使用してください。

- **[802.11r (FT)]** と **[CCKM]** が必須として構成されていないことを確認します
- **[Quality of Service (QoS)]** を **[プラチナ (Platinum)]** に設定します。
- **[WMMポリシー (WMM Policy)]** を **[必須 (Required)]** に設定します
- **[802.11k]** が **[無効 (Disabled)]** になっていることを確認します
- **[802.11v]** が **[無効 (Disabled)]** になっていることを確認します
- **[セッションのタイムアウト (Session Timeout)]** が有効で、正しく設定されていることを確認します。
- **[キーのブロードキャスト間隔 (Broadcast Key Interval)]** が有効になっていて、正しく構成されていることを確認します
- **[Aironet IE]** が **[有効 (Enabled)]** になっていることを確認します。
- **[P2P (ピアツーピア) ブロッキングアクション (P2P (Peer to Peer) Blocking Action)]** を無効にします。
- **[クライアント除外 (Client Exclusion)]** が正しく設定されていることを確認します。
- **[DHCP アドレス割り当て必須 (DHCP Address Assignment Required)]** を無効にします。
- **[保護された管理フレーム (PMF) (Protected Management Frame (PMF)]** は、**[任意 (Optional)]**、**[必須 (Required)]** または **[無効 (Disabled)]** に設定する必要があります
- **[MFPクライアント保護 (MFP Client Protection)]** を、**[任意 (Optional)]**、**[必須 (Required)]** または **[無効 (Disabled)]** に設定します。
- **[DTIM周期 (DTIM Period)]** を **[2]** に設定します
- **[クライアントロードバランシング (Client Load Balancing)]** を **[無効 (Disabled)]** に設定します。
- **[クライアントの帯域選択 (Client Band Select)]** を **[無効 (Disabled)]** に設定します。
- **[IGMPスヌーピング (IGMP Snooping)]** を **[有効 (Enabled)]** に設定します。
- レイヤ3 モビリティを使用している場合は、**[シンメトリック モバイル トンネリング モード (Symmetric Mobile Tunneling Mode)]** を有効にします
- Cisco 802.11n/ac/ax 対応のアクセスポイントを使用している場合は、**[クライアントリンク (ClientLink)]** を有効にします
- 必要に応じて **[データレート (Data Rates)]** を設定します。
- 必要に応じて **[Auto RF]** を設定します。
- **[EDCAプロファイル (EDCA Profile)]** を **[音声の最適化 (Voice Optimized)]** または **[音声およびビデオの最適化 (Voice and Video Optimized)]** に設定します
- **[低遅延MACを有効にする (Enable Low Latency MAC)]** を **[無効 (Disabled)]** に設定します。
- **[電力制限 (Power Constraint)]** が **[無効 (Disabled)]** になっていることを確認します。
- **[チャネル通知 (Channel Announcement)]** および **[チャネル Quiet モード (Channel Quiet Mode)]** を有効にします。
- 必要に応じて **[高スループットデータレート (High Throughput Data Rates)]** を構成します
- **[フレームの集約 (Frame Aggregation)]** 設定を構成します

- CleanAir テクノロジーを搭載したCisco 製アクセス ポイントを使用している場合は、**[CleanAir]** を有効にします。
- 必要に応じて **[マルチキャストダイレクト機能 (Multicast Direct Feature)]** を構成します
- Platinum QoS プロファイルの **[プロトコルタイプ (Protocol Type)]** を **[なし (None)]** に設定します。

802.11 ネットワークの設定

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

5 GHz を使用する場合は、802.11a/n/ac/ax ネットワークのステータスが

[有効 (Enabled)]

に設定されていることを確認します。[ビーコン周期 (Beacon Period)]

を [100 ms] に設定します。

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

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

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

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

- General:** 802.11a Network Status (Enabled), Beacon Period (100), Fragmentation Threshold (2346), DTTPC Support (Enabled), Maximum Allowed Clients (100), RSSI Low Check (Disabled), and RSSI Threshold (-60 to -90 dBm) (-80).
- 802.11a Band Status:** Low Band (Enabled), Mid Band (Enabled), High Band (Enabled).
- Data Rates**:** A list of data rates with dropdown menus: 6 Mbps (Disabled), 9 Mbps (Disabled), 12 Mbps (Mandatory), 18 Mbps (Supported), 24 Mbps (Supported), 36 Mbps (Supported), 48 Mbps (Supported), 54 Mbps (Supported).
- CCX Location Measurement:** Mode (Enabled), Interval (seconds) (60).
- TWT Configuration ***:** Target Waketime (Enabled), Broadcast TWT Support (Enabled).

2.4 GHz を使用する場合は、802.11b/g/n/ax ネットワークのステータスと 802.11g が

[有効 (Enabled)] に設定されていることを確認します。[ビーコン周期 (Beacon

Period)] を [100 ms] に設定します。

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

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

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

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

Mbps を必須（基本）レートとして有効にする必要があります。

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

ビームフォーミング (ClientLink)

Cisco 802.11n/ac/ax 対応のアクセスポイントを使用している場合は、[クライアントリンク (ClientLink)] を有効にします。次のコマンドを使用して、すべてのアクセスポイントにグローバルに、または個別アクセスポイントからの無線ビームフォーミング機能を有効にします。

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

次のコマンドを使用して、ビーム

フォーミング機能の現在のステータスを表示できます。(Cisco Controller) >show

802.11a

```
(Cisco Controller) >show 802.11b
```

```
Legacy Tx Beamforming setting.....Enabled
```

Auto RF (RRM)

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

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

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

5 GHz

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

Cisco 802.11n アクセスポイントを使用している場合は5 GHz チャンネルの幅を20 MHz または40 MHz として構成でき、Cisco 802.11ac または802.11ax アクセスポイントを使用している場合はチャンネルの幅を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 Wireless Configuration Manager interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows a tree view with 'Wireless' expanded, containing sections for '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'. Under '802.11a/n/ac/ax', 'RRM' is expanded to show 'RF Grouping', 'TPC', 'DCA', 'Coverage', 'General', 'Client Roaming', 'Media', and 'EDCA Parameters'. The main content area is titled '802.11a > RRM > Dynamic Channel Assignment (DCA)'. It features a 'Dynamic Channel Assignment Algorithm' section with the following settings: 'Channel Assignment Method' set to 'Automatic' (with options for Freeze and OFF), 'Interval' set to '10 minutes', and 'AnchorTime' set to '0'. A button 'Invoke Channel Update Once' is visible. Below this, several checkboxes are checked: 'Avoid Foreign AP interference', 'Avoid Cisco AP load', 'Avoid non-802.11a noise', and 'Avoid Persistent Non-WiFi Interference'. Other settings include 'Channel Assignment Leader' (RTP9-32A-WLC3 (10.81.6.70)), 'Last Auto Channel Assignment' (556 secs ago), 'DCA Channel Sensitivity' (Medium (15 dB)), 'Channel Width' (40 MHz selected, with options for 20 MHz, 80 MHz, 160 MHz, 80+80 MHz, and Best), and 'Avoid check for non-DFS channel' (unchecked). The 'DCA Channel List' section shows a list of channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 153, 157, 161.

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

2.4 GHz 帯域では使用可能なチャンネルの数が限られているために、40 MHz に対応した Cisco 製の 802.11n/ax アクセスポイントを使用する場合でも、2.4 GHz 帯域では20 MHz として構成することを推奨します。

The screenshot displays the Cisco configuration interface for Dynamic Channel Assignment (DCA) on a 802.11b network. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled '802.11b > RRM > Dynamic Channel Assignment (DCA)'. Under the 'Dynamic Channel Assignment Algorithm' section, the 'Channel Assignment Method' is set to 'Automatic'. Other settings include 'Interval: 10 minutes' and 'AnchorTime: 0'. A button labeled 'Invoke Channel Update Once' is visible. Below this, several options are checked: 'Avoid Foreign AP interference', 'Avoid non-802.11b noise', and 'Avoid Persistent Non-WiFi Interference'. The 'Channel Assignment Leader' is identified as 'RTP9-32A-WLC3 (10.81.6.70)'. The 'Last Auto Channel Assignment' occurred '75 secs ago'. The 'DCA Channel Sensitivity' is set to 'Medium (10 dB)'. The 'DCA Channel List' shows a list of channels: '1, 6, 11'.

使用する周波数帯域に応じて 5 GHz または 2.4 GHz

にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセスポイントの設定をグローバル設定よりも優先させることができます。

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネルの幅を 20 MHz または 40 MHz として構成でき、Cisco 802.11ac または 802.11ax アクセスポイントを使用している場合はチャンネルの幅を 20 MHz、40 MHz、または 80 MHz として構成できます。

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

すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

The screenshot shows the Cisco RoomOS configuration interface for a radio. The left sidebar contains a navigation menu with categories like Access Points, Radios, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, and specific radio standards (802.11a/n/ac/ax, 802.11b/g/n/ax, Media Stream, Application Visibility And Control, Lync Server, Country, Timers, Netflow, QoS).

The main configuration area is titled "802.11a/n/ac/ax Cisco APs > Configure" and is divided into several sections:

- General:** AP Name (rtp9-31a-ap1), Admin Status (Enable), Operational Status (UP), Slot # (1).
- 11n Parameters:** 11n Supported (Yes).
- CleanAir:** CleanAir Capable (Yes), CleanAir Admin Status (Enable). 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 B, C, and D.
- RF Channel Assignment:** Current Channel (48,44), Channel Width (40 MHz). A note states: "* Channel width can be configured only when channel configuration is in custom mode". Assignment Method (Global).
- Radar Information:** Channel and Last Heard (Secs) section with the message "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. A button labeled "Performance Profile" is visible.

A note at the bottom of the configuration area 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

Cisco RoomOS Series は、Cisco ワイヤレス LAN コントローラのクライアント ローミング セクションの RF パラメータを使用しません。スキャンングとローミングはデバイス側が独立して管理します。

EDCA パラメータ

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

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

Cisco 802.11n/ac/ax アクセス ポイントでは LLM はサポートされません。

The screenshot shows the Cisco RoomOS configuration interface for the EDCA Profile. The left sidebar is the same as in the previous screenshot.

The main configuration area is titled "General" and contains the following settings:

- EDCA Profile:** Voice & Video Optimized (dropdown menu).
- Enable Low Latency MAC:** Unchecked (checkbox).

A note at the bottom of the configuration area 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 に設定する必要があります。

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

The screenshot shows the Cisco RoomOS configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS (selected), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the 'Wireless' section with a tree view: Access Points (All APs, Radios, Global Configuration), Advanced (Mesh), AP Group NTP, ATF, RF Profiles, FlexConnect Groups, and FlexConnect ACLs. The main content area is titled '802.11h Global Parameters' and contains three sections: 'Power Constraint' with 'Local Power Constraint(0-30)' set to 0 dB; 'Channel Switch Announcement' with 'Channel Announcement' checked, 'Channel Switch Count' set to 0, and 'Channel Quiet Mode' checked; and 'Radar Blacklist' with 'Smart DFS' checked.

高スループット (802.11n/ac/ax)

802.11n および 802.11ax のデータ レートは、無線帯域 (2.4 GHz および 5 GHz) ごとに設定できます。802.11ac データ レートは 5 GHz にのみ適用できます。

[WMM] が有効になっていること、および [WPA3 (AES)] または [WPA2 (AES)] が 802.11n/ac/ax データレートを使用するよう構成されていることを確認します。

Cisco RoomOS Series は、HT MCS 0 ~ MCS 15 と VHT MCS 0 ~ MCS 9 1SS および 2SS データレートのみをサポートしますが、同じ帯域を使用し、MIMO アンテナテクノロジーを利用する他の 802.11n/ac/ax クライアントが存在していて、より高いレートが利用可能な場合には、オプションでより高い MCS レートを有効にできます。

General			MCS (Data Rate) Settings		
11n Mode	<input checked="" type="checkbox"/>	Enabled	0 (7 Mbps)	<input checked="" type="checkbox"/>	Supported
11ac Mode	<input checked="" type="checkbox"/>	Enabled	1 (14 Mbps)	<input checked="" type="checkbox"/>	Supported
11ax Mode	<input checked="" type="checkbox"/>	Enabled	2 (21 Mbps)	<input checked="" type="checkbox"/>	Supported
VHT MCS Rates			3 (29 Mbps)	<input checked="" type="checkbox"/>	Supported
SS1			4 (43 Mbps)	<input checked="" type="checkbox"/>	Supported
0-8	<input checked="" type="checkbox"/>	Enabled	5 (58 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	6 (65 Mbps)	<input checked="" type="checkbox"/>	Supported
SS2			7 (72 Mbps)	<input checked="" type="checkbox"/>	Supported
0-8	<input checked="" type="checkbox"/>	Enabled	8 (14 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	9 (29 Mbps)	<input checked="" type="checkbox"/>	Supported
SS3			10 (43 Mbps)	<input checked="" type="checkbox"/>	Supported
0-8	<input checked="" type="checkbox"/>	Enabled	11 (58 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	12 (87 Mbps)	<input checked="" type="checkbox"/>	Supported
SS4			13 (116 Mbps)	<input checked="" type="checkbox"/>	Supported
0-8	<input checked="" type="checkbox"/>	Enabled	14 (130 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	15 (144 Mbps)	<input checked="" type="checkbox"/>	Supported
HE MCS Rates			16 (22 Mbps)	<input checked="" type="checkbox"/>	Supported
SS1			17 (43 Mbps)	<input checked="" type="checkbox"/>	Supported
0-7	<input checked="" type="checkbox"/>	Enabled	18 (65 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	19 (87 Mbps)	<input checked="" type="checkbox"/>	Supported
0-11	<input checked="" type="checkbox"/>	Enabled	20 (130 Mbps)	<input checked="" type="checkbox"/>	Supported
SS2			21 (173 Mbps)	<input checked="" type="checkbox"/>	Supported
0-7	<input checked="" type="checkbox"/>	Enabled	22 (195 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	23 (217 Mbps)	<input checked="" type="checkbox"/>	Supported
0-11	<input checked="" type="checkbox"/>	Enabled	24 (29 Mbps)	<input checked="" type="checkbox"/>	Supported
SS3			25 (58 Mbps)	<input checked="" type="checkbox"/>	Supported
0-7	<input checked="" type="checkbox"/>	Enabled	26 (87 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	27 (116 Mbps)	<input checked="" type="checkbox"/>	Supported
0-11	<input checked="" type="checkbox"/>	Enabled	28 (173 Mbps)	<input checked="" type="checkbox"/>	Supported
SS4			29 (231 Mbps)	<input checked="" type="checkbox"/>	Supported
0-7	<input checked="" type="checkbox"/>	Enabled	30 (260 Mbps)	<input checked="" type="checkbox"/>	Supported
0-9	<input checked="" type="checkbox"/>	Enabled	31 (289 Mbps)	<input checked="" type="checkbox"/>	Supported
0-11	<input checked="" type="checkbox"/>	Enabled			
SS5					
0-7	<input checked="" type="checkbox"/>	Enabled			
SS6					
0-7	<input checked="" type="checkbox"/>	Enabled			

フレームの集約

フレームの集約は複数の MAC プロトコルデータ ユニット (MPDU) または MAC サービスデータ ユニット (MSDU) を一緒にパッケージングして、順スルーputとキャパシティが最適になる点でオーバーヘッドを低減するためのプロセスです。

MAC プロトコルデータ ユニット (A-MPDU) の集約にはブロックの確認応答を使用する必要があります。

Cisco RoomOS Series の操作性を最適化するために、A-MPDU と A-MSDU の設定を次のように調整することが必要です。

A-MSDU

ユーザプライオリティ 1、2 = 有効

ユーザプライオリティ 0、3、4、5、6、7 = 無効

A-MPDU

ユーザプライオリティ 0、3、4、5 = 有効

ユーザプライオリティ 1、2、6、7 = 無効

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

5 GHz の設定を設定するには、802.11a

ネットワークを最初に無効にし、変更が完了したら再び有効にする必要があります。

```
config 802.11a 11nSupport a-msdu tx priority 1 enable
```

Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

```
config 802.11a 11nSupport a-msdu tx priority 2 enable  
config 802.11a 11nSupport a-msdu tx priority 0 disable
```

```
config 802.11a 11nSupport a-msdu tx priority 3 disable
config 802.11a 11nSupport a-msdu tx priority 4 disable
config 802.11a 11nSupport a-msdu tx priority 5 disable
config 802.11a 11nSupport a-msdu tx priority 6 disable
config 802.11a 11nSupport a-msdu tx priority 7 disable
```

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

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

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

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

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

802.11n Status:

A-MSDU Tx:

```
Priority 0.....[無効 (Disabled) ]
Priority 1.....有効
Priority 2.....有効
Priority 3.....[無効 (Disabled) ]
Priority 4.....[無効 (Disabled) ]
Priority 5.....[無効 (Disabled) ]
Priority 6.....[無効 (Disabled) ]
Priority 7.....無効
```

A-MPDU Tx:

Priority 0.....有効
Priority 1.....[無効 (Disabled)]

- Priority 2.....[無効 (Disabled)]
- Priority 3.....有効
- Priority 4.....有効
- Priority 5.....有効
- Priority 6.....[無効 (Disabled)]
- Priority 7.....無効

CleanAir

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

The screenshot shows the Cisco Prime Infrastructure configuration page for CleanAir. The left sidebar contains a navigation menu with categories like Access Points, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, and RRM. The main content area is titled '802.11a > CleanAir' and contains the following sections:

- CleanAir/Spectrum Intelligence Parameters:**
 - CleanAir: Enabled
 - Spectrum Intelligence: Enabled
 - Report Interferers: Enabled
 - Persistent Device Propagation: Enabled
- Interferences to Ignore:** Canopy, WiMax Fixed, SI_FHSS
- Interferences to Detect:** TDD Transmitter, Jammer, Continuous Transmitter, DECT-like Phone, Video Camera
- Trap Configurations:**
 - Enable AQI(Air Quality Index) Trap: Enabled
 - AQI Alarm Threshold (1 to 100): 35
 - Enable trap for Unclassified Interferences: Enabled
 - Threshold for Unclassified category trap (1 to 99): 20
 - Enable trap for Classified Interferences: Enabled
 - Threshold for Classified category trap (1 to 99): 0
 - Enable Interference For Security Alarm: Enabled
- Do not trap on these types:** TDD Transmitter, Continuous Transmitter, DECT-like Phone, Video Camera, SuperAG
- Trap on these types:** Jammer, WiFi Inverted, WiFi Invalid Channel
- Event Driven RRM (Change Settings):**
 - EDRRM: Disabled
 - Sensitivity Threshold: N/A
 - Rogue Contribution: N/A
 - Rogue Duty-Cycle: N/A

Footnotes at the bottom of the page:

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

Rx SOPしきい値

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

WLAN の設定

Cisco RoomOS Series には個別の SSID を使用することをお勧めします。

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

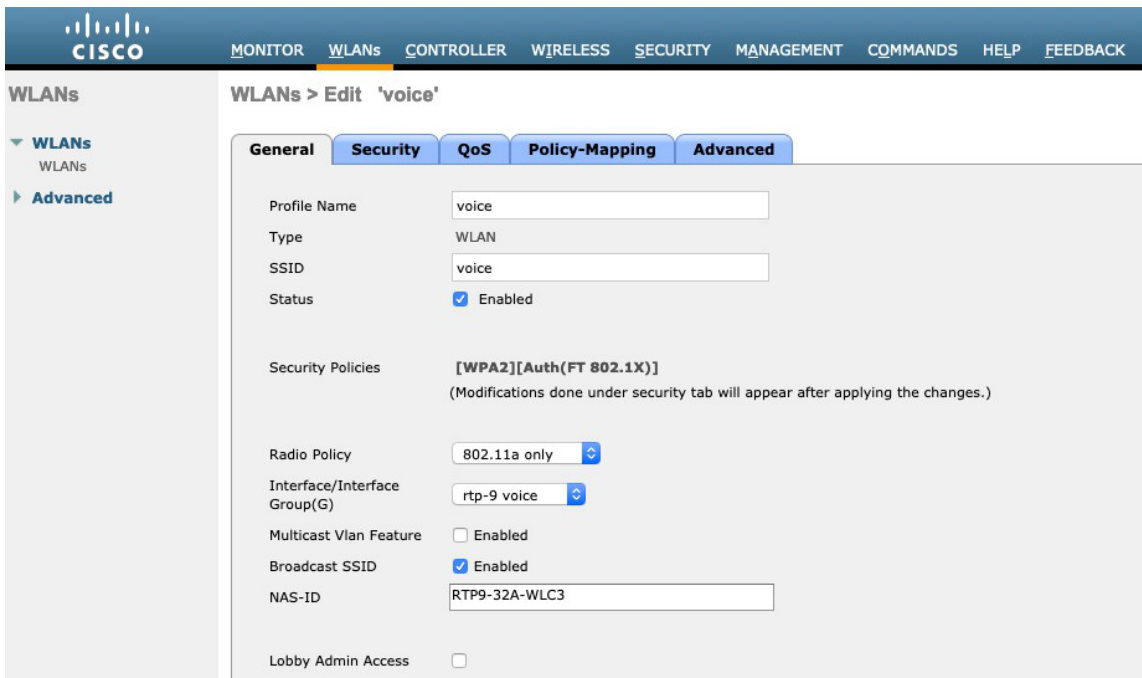
Cisco RoomOS Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように構成できます (802.11a のみなど)。

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

選択した SSID が他の LAN

Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

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



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

AES 暗号化を使用した WPA2 ポリシーを有効にします。その後、802.1x-SHA2、802.1x-SHA1 または PSK のどれを使用するかに応じて、認証キー管理タイプとして FT 802.1x と PSK のどちらかを有効にします。

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

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security ⁶ WPA+WPA2

Security Type Enterprise

MAC Filtering ²

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption CCMP128(AES) TKIP CCMP256 GCMP128 GCMP256

OSEN Policy

Fast Transition

Fast Transition Enable

Over the DS

Reassociation Timeout 20 Seconds

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

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

Protected Management Frame

PMF Disabled ³

Authentication Key Management ¹²

802.1X-SHA1 Enable

802.1X-SHA2 Enable

FT 802.1X Enable

CCKM Enable

WPA GTK-randomize State ¹⁴ Disable

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

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security ⁶ WPA+WPA2

Security Type Personal

MAC Filtering ²

AutoConfig iPSK Enable

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

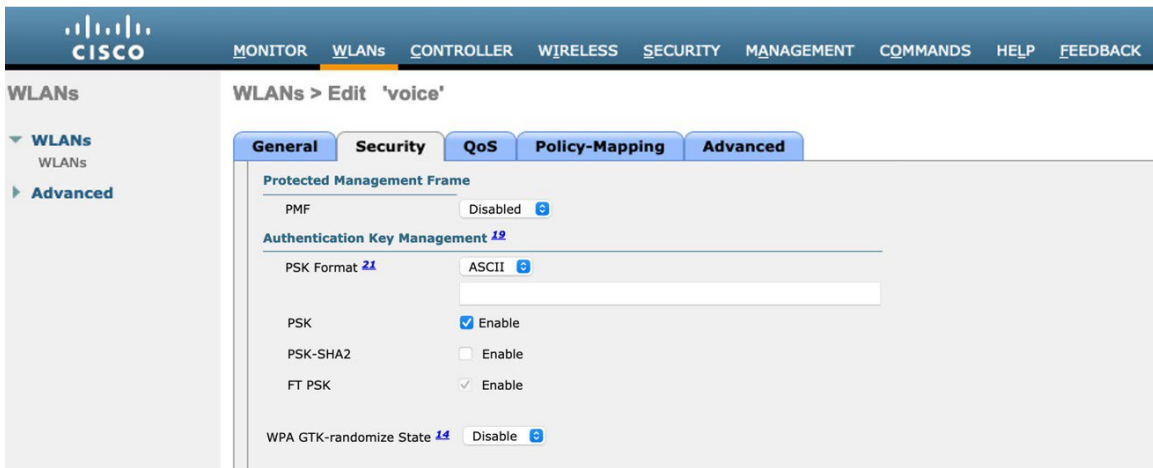
WPA2 Encryption CCMP128(AES) TKIP

Fast Transition

Fast Transition Enable

Over the DS

Reassociation Timeout 20 Seconds

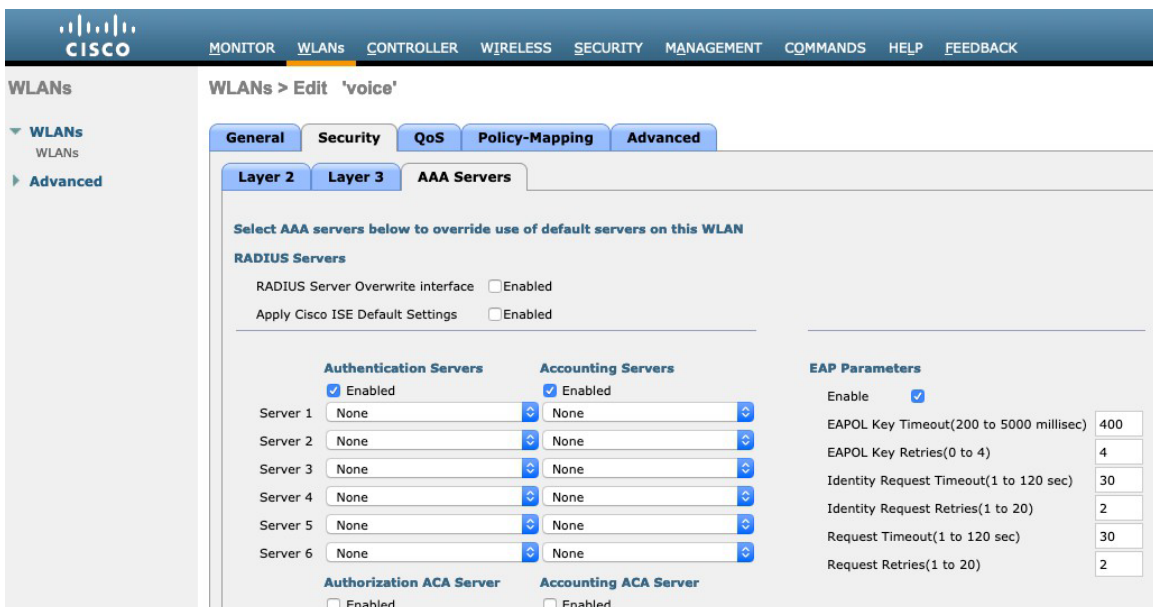


各種の音声クライアントに同じ SSID を使用する場合は、802.1x や PSK を使用するかどうかに応じて、802.11r (FT)、CCKM、PSK も有効にできます。

RADIUS 認証およびアカウントサーバーは、SSID レベルごとに設定して、グローバルリストを上書きできます。**[有効 (Enabled)]** にして、指定しない場合 (**[なし (None)]** に設定)、**[セキュリティ (Security)]** > **[AAA]** > **[RADIUS]** で定義された RADIUS サーバーのグローバルリストが使用されます。

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

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



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

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

他の非 WMM クライアントで Cisco RoomOS Series と同じ SSID を使用する必要がある場合は、WMM ポリシーが [許可 (Allowed)] に設定されていることを確認します。

WMM を有効にすると、802.11e バージョンの QoS が有効になります。

The screenshot shows the Cisco RoomOS configuration interface for a WLAN named 'voice'. The 'QoS' tab is selected, and the 'Quality of Service (QoS)' is set to 'Platinum (voice)'. Other settings include 'Application Visibility' (Enabled), 'AVC Profile' (none), 'Flex AVC Profile' (none), 'Netflow Monitor' (none), and 'Fastlane' (Disable). Below this, the 'Override Per-User Bandwidth Contracts (kbps)' section is visible, with a table of settings:

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

A 'Clear' button is located below the table.

The screenshot shows the Cisco RoomOS configuration interface for a WLAN named 'voice'. The 'WMM' section is expanded, showing 'WMM Policy' set to 'Required', '7920 AP CAC' set to 'Enabled', and '7920 Client CAC' set to 'Disabled'. The 'Media Stream' section shows 'Multicast Direct' set to 'Enabled'. The 'Lync Policy' section shows 'Audio' set to 'Silver'.

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

[Aironet 拡張機能 (Aironet IE)] を有効にします。

[ピアツーピア (P2P) のブロッキングアクション (Peer to Peer (P2P) Blocking Action)] は

[無効 (Disabled)] にします。必要に応じて

[クライアント除外 (Client Exclusion)] を構成します。

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

[オフチャンネル スキャンの待機 (Off Channel Scanning Defer)]

を調整することで、スキャンの待機時間だけでなく、特定のキューに対するスキャンを待機させることができます。

ベスト エフォート

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

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

[DHCP アドレス割り当て必須 (DHCP Address Assignment Required)] は無効にします。

[管理フレーム保護] は、[任意 (Optional)]、[必須 (Required)] または

[無効 (Disabled)] に設定できます。[DTIM 周期 (DTIM Period)] を [2]

に、ビーコン周期を [100 ミリ秒] に設定します。

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

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

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

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'voice'. The 'QoS' tab is selected, showing various settings for Quality of Service. Key settings include:

- Allow AAA Override: Enabled
- Coverage Hole Detection: Enabled
- Enable Session Timeout: 86400 (Session Timeout in secs)
- Aironet IE: Enabled
- Diagnostic Channel: Enabled
- Override Interface ACL: IPv4: None, IPv6: None
- Layer2 Acl: None
- URL ACL: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled
- Maximum Allowed Clients: 0
- Static IP Tunneling: Enabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200

Other tabs visible include General, Security, Policy-Mapping, and Advanced. The Security tab shows DHCP and Management Frame Protection (MFP) settings.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'voice'. The 'Security' tab is selected, showing various security settings. Key settings include:

- Clear HotSpot Configuration: Enabled
- Client user idle timeout(15-100000):
- Client user idle threshold(0-10000000): 0 Bytes
- Radius NAI-Realm:
- 11ac MU-MIMO:
- WGB PRP: Enabled
- MBO State:

The 'Advanced' tab is also visible, showing settings for Passive Client, Voice, Radius Client Profiling, Local Client Profiling, and PMIP.

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

FlexConnect Local Auth Enabled
 Learn Client IP Address Enabled
 Vlan based Central Switching Enabled
 Central DHCP Processing Enabled
 Override DNS Enabled
 NAT-PAT Enabled
 Central Assoc Enabled

Lync
 Lync Server Disabled

11k
 Neighbor List Enabled
 Neighbor List Dual Band Enabled
 Assisted Roaming Prediction Optimization Enabled

802.11ax BSS Configuration
 Down Link MU-MIMO Enabled

PMIP Profile None
 PMIP Realm
 Universal AP Admin Support
 Universal AP Admin

11v BSS Transition Support
 BSS Transition
 Disassociation Imminent
 Disassociation Timer(0 to 3000 TBTT) 200
 Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40
 BSS Max Idle Service
 Directed Multicast Service

Tunneling
 Tunnel Profile None
 EOGRE Vlan Override

mDNS
 mDNS Snooping Enabled

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

802.11ax BSS Configuration
 Down Link MU-MIMO Enabled
 Up Link MU-MIMO Enabled
 Down Link OFDMA Enabled
 Up Link OFDMA Enabled

mDNS
 mDNS Snooping Enabled

TrustSec
 Security Group Tag 0

Umbrella
 Umbrella Mode Ignore
 Umbrella Profile None
 Umbrella DHCP Override

Fabric Configuration
 Fabric Enabled

Mobility
 Selective Reanchor Enabled

U3 Interface
 U3 Interface Enabled
 U3 Reporting Interval 30

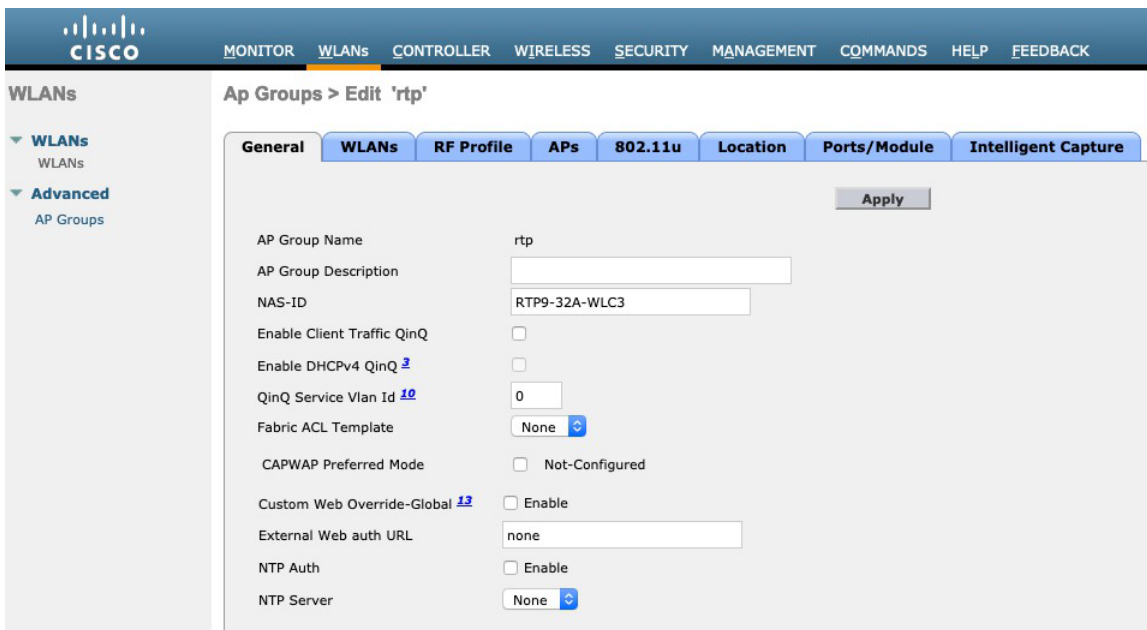
AP グループ

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

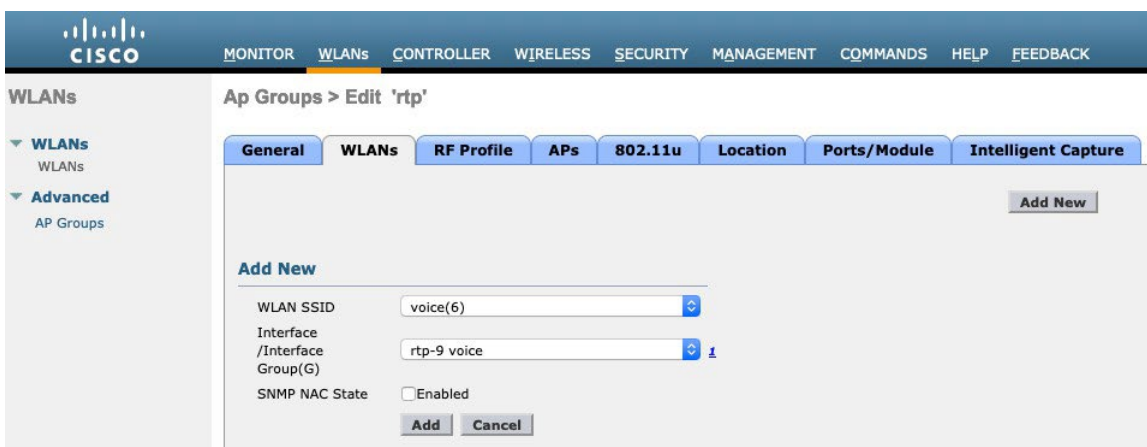
WLANs > AP Groups

Add New AP Group

AP Group Name rtp
 Description
 Add Cancel

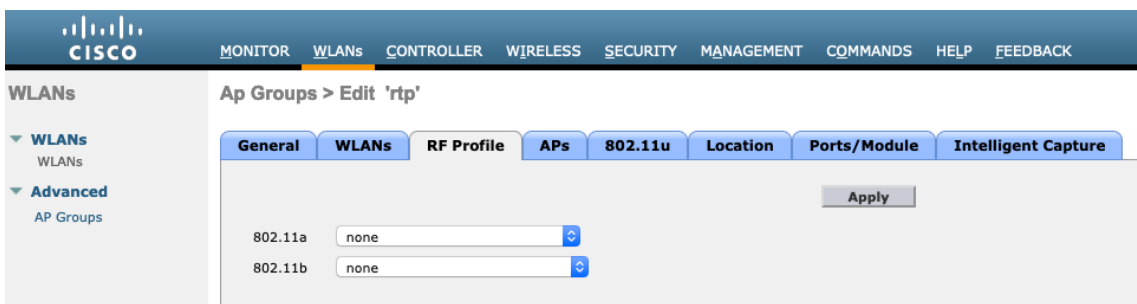


[WLAN (WLANs)] タブで、対象 SSID と、マッピングするインターフェイスを選択して、[追加 (Add)] を押します。



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

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



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

その後、選択したアクセス ポイントが再起動します。

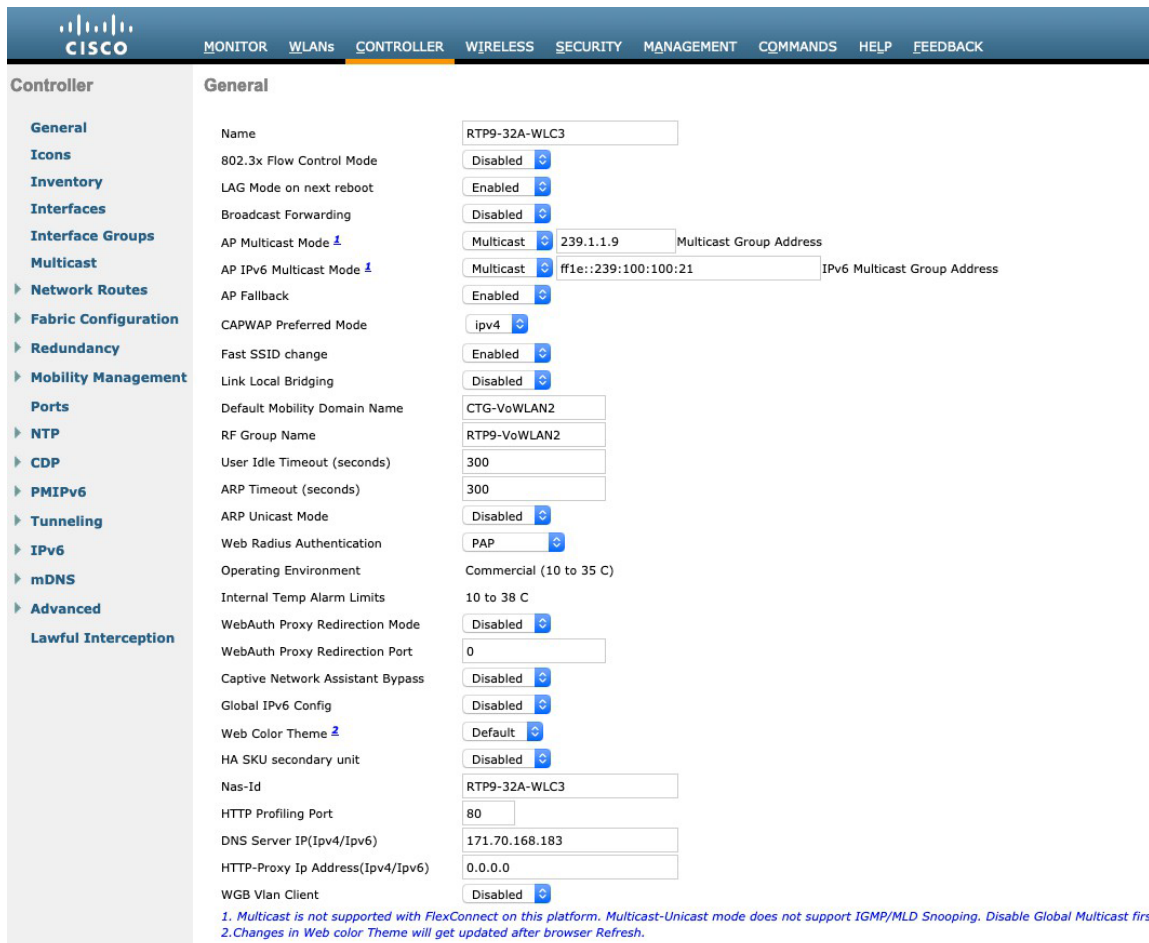


コントローラの設定

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

Cisco ワイヤレス LAN

コントローラで複数のポートを使用している場合はリンク集約 (LAG) を有効にします。対象の AP マルチキャスト モードを設定します。



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

Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
- Ports
- NTP
- CDP

Multicast

Enable Global Multicast Mode

Enable IGMP Snooping

IGMP Timeout (30-7200 seconds)

IGMP Query Interval (15-2400 seconds)

Enable MLD Snooping

MLD Timeout (30-7200 seconds)

MLD Query Interval (15-2400 seconds)

Foot Notes

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

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

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

Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
 - Mobility Groups
 - Mobility Anchor Config
 - Multicast Messaging

Mobility Anchor Config

Keep Alive Count

Keep Alive Interval (1-30 seconds)

Symmetric Mobility Tunneling mode

DSCP Value

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

Controller

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Static Mobility Group Members

Local Mobility Group CTG-VoWLAN2

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

Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
 - Mobility Groups
 - Mobility Anchor Config
 - Multicast Messaging

コール アドミッション制御 (CAC)

[ボイス (Voice)]で [アドミッション制御必須 (Admission Control Mandatory)]を有効にして、使用する帯域 (5 GHz または 2.4

GHz) に対して最大帯域幅および予約済みのローミング帯域幅の各割合を設定することを推奨します。

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

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

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

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

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

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

802.11a(5 GHz) > Media

Voice Video **Media**

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method ⁴ Load Based ▾

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

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

Expedited bandwidth

SIP CAC Support ³ Enabled

Per-Call SIP Bandwidth ²

SIP Codec G.711 ▾

SIP Bandwidth (kbps) 64

SIP Voice Sample Interval (msecs) 20 ▾

Traffic Stream Metrics

Metrics Collection

Foot Notes

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

[ビデオ (Video)] で [アドミッションコントロール必須 (Admission Control Mandatory)] を無効にします。

Wireless

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

802.11a(5 GHz) > Media

Voice Video Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method [4](#) Static

Max RF Bandwidth (5-85)(%)

Reserved Roaming Bandwidth (0-25)(%)

SIP CAC Support [3](#) Enabled

Foot Notes

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

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

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

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

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

コールアドミッション制御 (CAC) 設定

[音声 AC - アドミッション制御 (Voice AC - Admission control (ACM))] **[有効 (Enabled)]**
 [音声最大 RF 帯域幅 (Voice max RF bandwidth)] **[75]**
 [音声予約ローミング帯域幅 (Voice reserved roaming bandwidth)] **[6]**
 [音声負荷ベース CAC モード (Voice load-based CAC mode)] **有効**
 [音声 TSPEC 非アクティブタイムアウト (Voice tspec inactivity timeout)] **[無効 (Disabled)]**
 [ビデオ AC - アドミッション制御 (Video AC - Admission control (ACM))] **[無効 (Disabled)]**
 [音声ストリームサイズ (Voice Stream-Size)] **84000**
 [音声最大ストリーム (Voice Max-Streams)] **[2]**
 [ビデオ最大 RF 帯域幅 (Video max RF bandwidth)] **[25]**
 [ビデオ予約ローミング帯域幅 (Video reserved roaming bandwidth)] **[6]**

voice stream-size および voice max-streams

の値は、必要に応じて次のコマンドを使用により調整できます。SRTP を使用している場合は、音声 Stream-Size を増やす必要がある場合があります。

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

WLAN 設定で QoS

が正しくセットアップされていることを確認します。この設定は、次のコマンドを使って表示可能です。

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

[サービス品質 (Quality of Service)] [プラチナ (音声) (Platinum (voice))]
 [WMM].....[必須 (Required)]
 [ドット 11-電話モード (Dot11-Phone Mode (7920))] [ap-cac-limit]
 [優先プロトコル (Wired Protocol)] [なし (None)]

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

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

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


The screenshot shows the Cisco Wireless configuration interface for the 802.11a(5 GHz) Media settings. The left sidebar shows the navigation menu with '802.11a/n/ac/ax' selected. The main content area is titled '802.11a(5 GHz) > Media' and has tabs for 'Voice', 'Video', and 'Media'. Under the 'Media' tab, there are three sections: 'General', 'Multicast Direct Admission Control', and 'Media Stream - Multicast Direct Parameters'. In the 'General' section, 'Unicast Video Redirect' is checked. In the 'Multicast Direct Admission Control' section, 'Maximum Media Bandwidth (0-85(%))' is set to 85, 'Client Minimum Phy Rate' is 6000, and 'Maximum Retry Percent (0-100%)' is 80. In the 'Media Stream - Multicast Direct Parameters' section, 'Multicast Direct Enable' is checked, 'Max Streams per Radio' and 'Max Streams per Client' are both set to 'No-limit', and 'Best Effort QoS Admission' is unchecked. A 'Foot Notes' section at the bottom provides additional information about rates and CAC methods.

RFプロファイル

RF プロファイルを作成し、アクセス ポイントのグループが使用する必要がある周波数帯域、データ レート、RRM 設定などを指定できます。Cisco RoomOS Series で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

作成した RF プロファイルは、AP グループに適用されます。

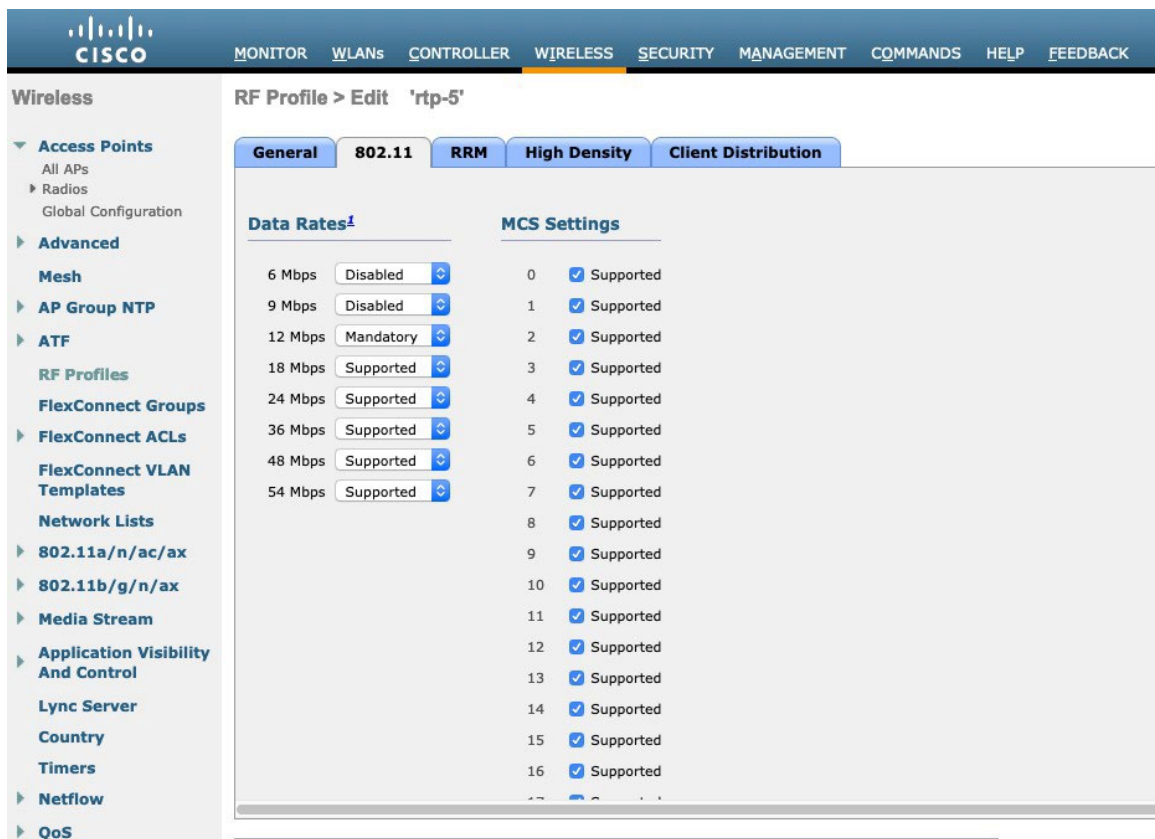
RF プロファイルを作成する場合、[RF プロファイル名 (RF Profile Name)] と [無線ポリシー (Radio Policy)] を定義する必要があります。[無線ポリシー (Radio Policy)] で 802.11a または 802.11b/g を選択します。



The screenshot shows the 'RF Profile > New' configuration page. The 'RF Profile Name' field contains 'rtp-5'. The 'Radio Policy' dropdown menu is set to '802.11a'. The 'Use default RF Profile Template' dropdown menu is set to 'None'.

[802.11] タブで、希望に応じてデータレートを設定します。

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



The screenshot shows the 'RF Profile > Edit 'rtp-5'' configuration page. The '802.11' tab is selected. The 'Data Rates' section shows the following settings:

Data Rate	Setting
6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

The 'MCS Settings' section shows the following settings:

MCS	Setting
0	Supported
1	Supported
2	Supported
3	Supported
4	Supported
5	Supported
6	Supported
7	Supported
8	Supported
9	Supported
10	Supported
11	Supported
12	Supported
13	Supported
14	Supported
15	Supported
16	Supported

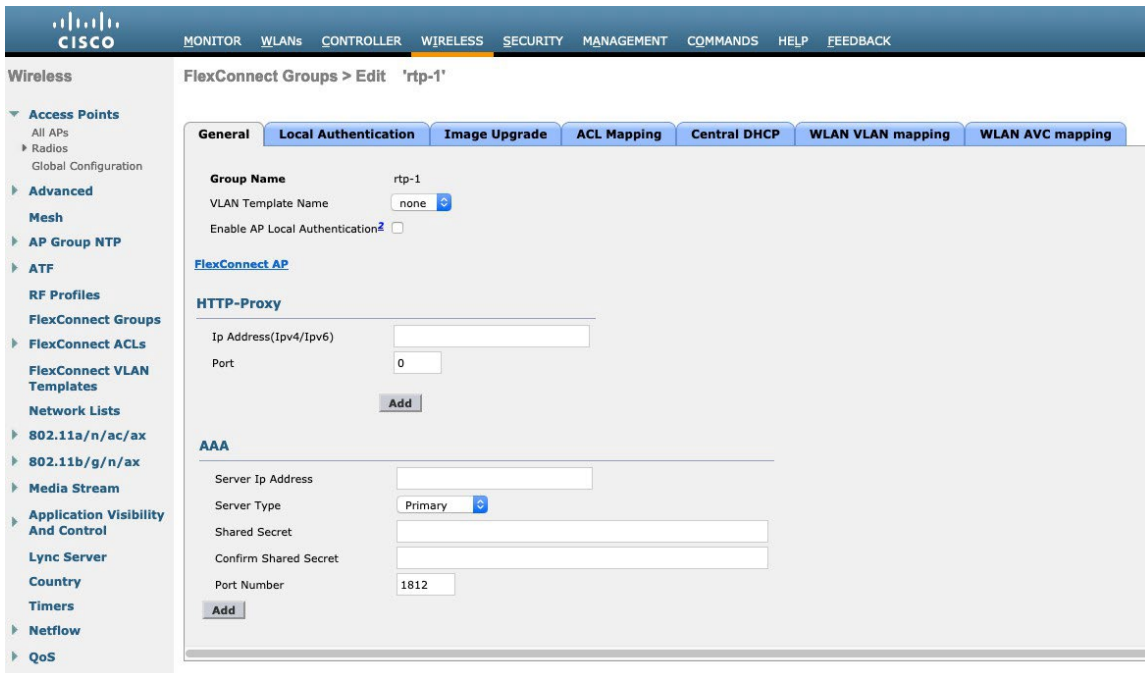
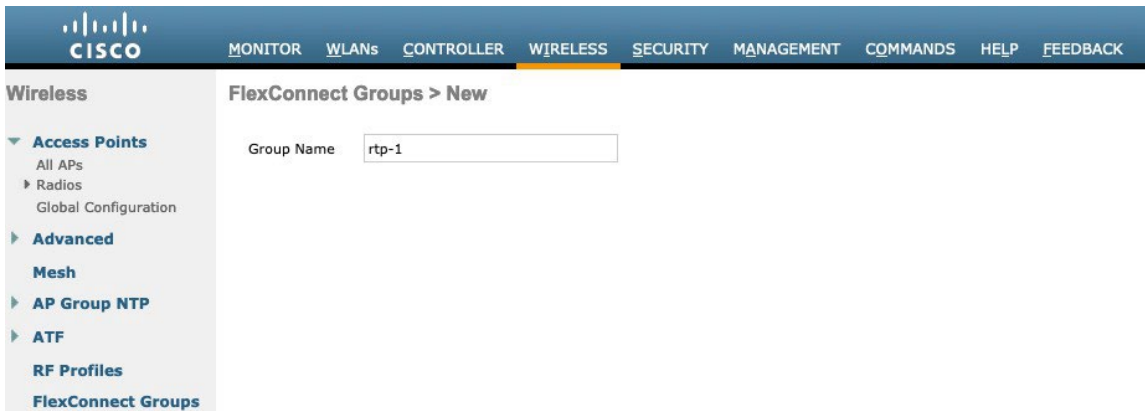
[RRM] タブでは、[最大電力レベルの割り当て (Maximum Power Level Assignment)] および

[最小電力レベルの割り当て (Minimum Power Level Assignment)] 設定と、その他の [DCA]、[TPC]、および [カバレッジホール検出 (Coverage Hole Detection)] 設定を構成できます。

[高密度 (High Density)]タブでは、[最大クライアント数 (Maximum Clients)]、[マルチキャストデータレート (Multicast Data Rates)]、および[Rx Sop のしきい値 (Rx Sop Threshold)]を設定できます。[Rx Sopのしきい値 (Rx Sop Threshold)]にはデフォルト値を使用することを推奨します。

FlexConnect グループ

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



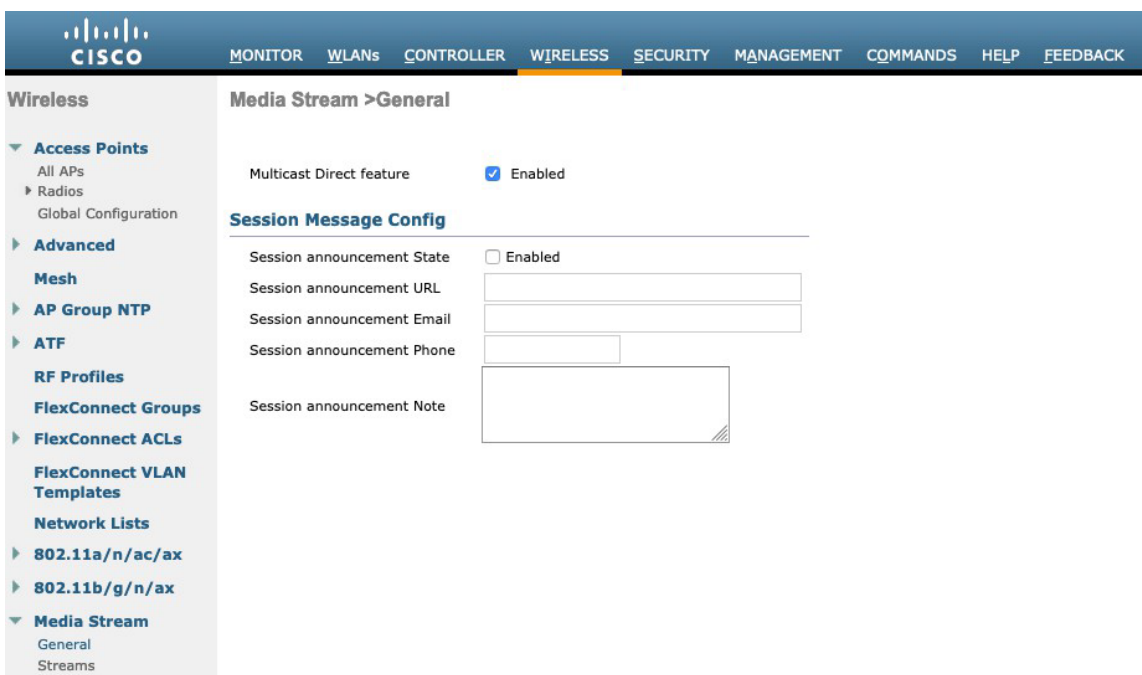
FlexConnect グループごとに許可されるアクセスポイントの最大数は制限されており、これは WLC モデル固有です。





マルチキャスト ダイレクト

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



それから、必要に応じてメディア ストリームを設定します。

Media Stream > New

Stream Name

Multicast Destination Start IP Address(ipv4/ipv6)

Multicast Destination End IP Address(ipv4/ipv6)

Maximum Expected Bandwidth(1 to 35000 Kbps)

Resource Reservation Control(RRC) Parameters

Select from predefined templates

Average Packet Size (100-1500 bytes)

RRC Periodic update

RRC Priority (1-8)

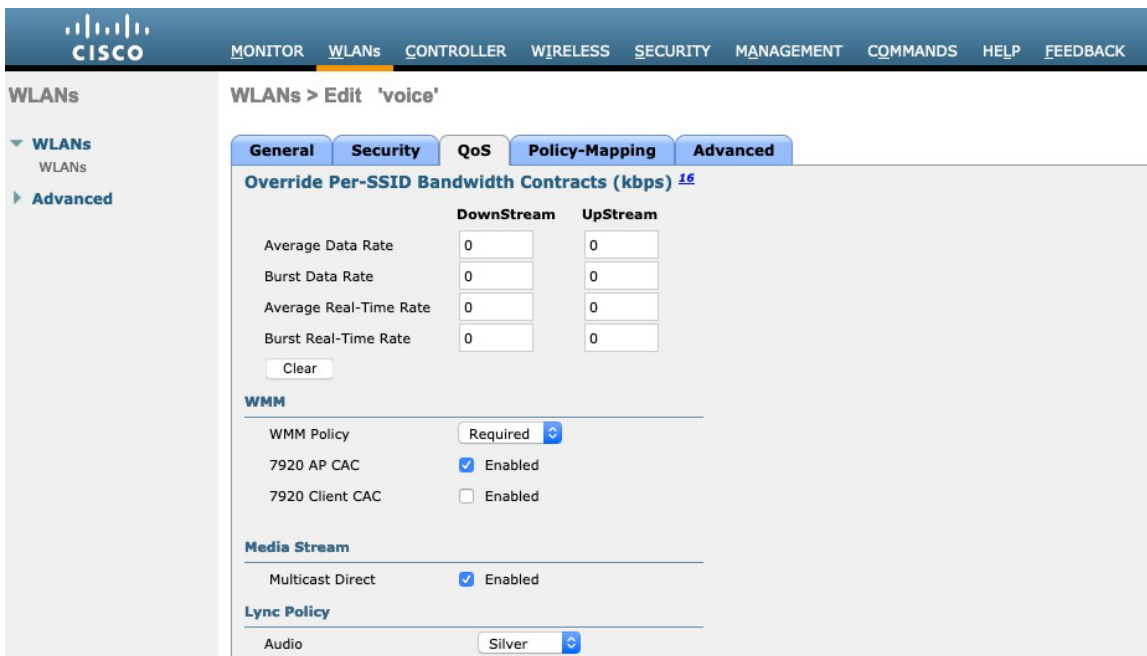
Traffic Profile Violation

保存すると、メディアストリームが表示されます。

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



QoS プロファイル

次の4つの QoS プロファイルを設定します。

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

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

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority

Unicast Default Priority

Multicast Default Priority

Wired QoS Protocol

Protocol Type

Wireless

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

Edit QoS Profile

QoS Profile Name gold

Description

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority ▼

Unicast Default Priority ▼

Multicast Default Priority ▼

Wired QoS Protocol

Protocol Type ▼

802.1p Tag

Wireless

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

Edit QoS Profile

QoS Profile Name bronze

Description

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority ▼

Unicast Default Priority ▼

Multicast Default Priority ▼

Wired QoS Protocol

Protocol Type ▼

802.1p Tag

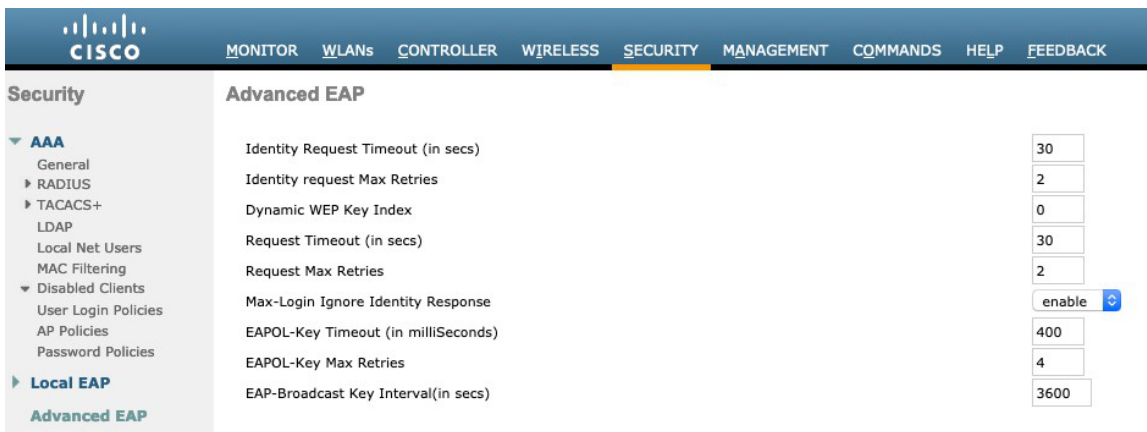
The screenshot displays the 'Edit QoS Profile' configuration page. The 'QoS Profile Name' is set to 'silver'. The 'Description' field contains 'For Best Effort'. Under 'Per-User Bandwidth Contracts (kbps)', there are four rows of input fields for Average and Burst Data/Real-Time Rates, with DownStream and UpStream columns. All values are currently set to 0. The 'Per-SSID Bandwidth Contracts (kbps)' section has an identical layout. In the 'WLAN QoS Parameters' section, Maximum Priority, Unicast Default Priority, and Multicast Default Priority are all set to 'besteffort'. The 'Wired QoS Protocol' section shows the Protocol Type as '802.1p' and the 802.1p Tag as '0'.

詳細設定

EAP の詳細設定

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

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



コマンドラインを介して Cisco Wireless LAN Controller の EAP

パラメータを表示するには、次のコマンドを入力します。(Cisco Controller) >show advanced eap

```
[EAPアイデンティティ要求のタイムアウト (EAP-Identity-Request Timeout) (秒) ] [30]
[EAP アイデンティティ要求の最大試行回数 (EAP-Identity-Request Max Retries) ] [2]
[ダイナミック WEP の EAP キーインデックス (EAP Key-Index for Dynamic WEP) ] [0]
[ログイン最大数に EAP アイデンティティ応答を反映させない (EAP Max-Login Ignore Identity Response) ]
.....[有効 (enable) ]
[EAP要求のタイムアウト (EAP-Request Timeout) (秒) ] [30]
[EAP 要求の最大試行回数 (EAP-Request Max Retries) ] [2]
[EAPOL キーのタイムアウト (EAPOL-Key Timeout) (ミリ秒) ] [400]
[EAPOL キーの最大試行回数 (EAPOL-Key Max Retries) ] [4]
[EAP ブロードキャスト キーの間隔 (EAP-Broadcast Key Interval) ] [3600]
```

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

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

展開において、EAP の失敗が頻繁に発生する場合には、**[EAP 要求のタイムアウト (EAP-Request Timeout)]** を 30 秒未満に減らす必要があります。

Cisco ワイヤレス LAN コントローラに対する **[EAP 要求のタイムアウト (EAP-Request Timeout)]** を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

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

PSK を使用する場合は、**[EAPOL キーのタイムアウト (EAPOL-Key Timeout)]** をデフォルトの 1000 ミリ秒から 400 ミリ秒に減らし、**[EAPOL キーの最大試行回数 (EAPOL-Key Max Retries)]** をデフォルトの 2 から 4 に変更することを推奨します。

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

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

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

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

Cisco ワイヤレス LAN コントローラに対する [EAPOL キー最大試行のタイムアウト (EAPOL-Key Max Retries Timeout)] を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

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

[EAP ブロードキャスト キーの間隔 (EAP-Broadcast Key Interval)] が 3600 秒 (1 時間) 以上に設定されていることを確認します。

Cisco ワイヤレス LAN コントローラに対する [EAP ブロードキャスト キーの間隔 (EAP-Broadcast Key Interval)] を変更するには、コントローラに Telnet または SSH で接続して、次のコマンドを入力します。

```
(Cisco Controller) >config advanced eap bcst-key-interval 3600
```

Auto-Immune

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

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

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

```
(Cisco Controller) >show wps summary
```

Auto-Immune

```
[自動免疫 (Auto-Immune) ]..... [無効 (Disabled) ]
```

Client Exclusion Policy

```
[802.11 の過剰な関連付け障害 (Excessive 802.11-association failures) ] [有効 (Enabled) ]
```

```
[802.11 の過剰な認証障害 (Excessive 802.11-authentication failures) ] [有効 (Enabled) ]
```

```
[802.11 の過剰な認証 (Excessive 802.11-authentication) ] イネーブル
```

```
[IP 盗難 (IP-theft) ] ..... イネーブル
```

```
[Web の過剰な認証障害 (Excessive Web authentication failures) ] [有効 (Enabled) ]
```

Signature Policy

```
署名処理 (Signature Processing) ..... 有効
```

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

```
(Cisco Controller) >config wps auto-immune disable
```

不正ポリシー

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

The screenshot displays the Cisco Catalyst IOS XE configuration interface for Rogue Policies. The left sidebar shows the navigation menu with 'Wireless Protection Policies' expanded to 'Rogue Policies'. The main content area is divided into two sections: 'Rogue Policies' and 'Auto Contain'.

Rogue Policies

- Rogue Detection Security Level:** Radio buttons for Low, High, Critical, and Custom (selected).
- Rogue Location Discovery Protocol:** Dropdown menu set to 'Disable'.
- Expiration Timeout for Rogue AP and Rogue Client entries:** Text input '1200' followed by 'Seconds'.
- Validate rogue clients against AAA:** Enabled
- Validate rogue AP against AAA:** Enabled
- Polling Interval:** Text input '0' followed by 'Seconds'.
- Validate rogue clients against MSE:** Enabled
- Detect and report Ad-Hoc Networks:** Enabled
- Rogue Detection Report Interval (10 to 300 Sec):** Text input '10'.
- Rogue Detection Minimum RSSI (-70 to -128):** Text input '-90'.
- Rogue Detection Transient Interval (0, 120 to 1800 Sec):** Text input '0'.
- Rogue Client Threshold (0 to disable, 1 to 256):** Text input '0'.
- Rogue containment automatic rate selection:** Enabled

Auto Contain

- Auto Containment Level:** Dropdown menu set to '1'.
- Auto Containment only for Monitor mode APs:** Enabled
- Auto Containment on FlexConnect Standalone:** Enabled
- Rogue on Wire:** Enabled
- Using our SSID:** Enabled
- Valid client on Rogue AP:** Enabled
- AdHoc Rogue AP:** Enabled

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

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

- [802.11r (FT)] と [CCKM] が必須として構成されていないことを確認します
- [Quality of Service (QoS) SSIDポリシー (Quality of Service (QoS) SSID Policy)] を [プラチナ (Platinum)] に設定します
- [WMMポリシー (WMM Policy)] を [必須 (Required)] に設定します
- [802.11k] が [無効 (Disabled)] になっていることを確認します
- [802.11v] が [無効 (Disabled)] になっていることを確認します
- [セッションのタイムアウト (Session Timeout)] が有効で、正しく設定されていることを確認します。
- [キーのブロードキャスト間隔 (Broadcast Key Interval)] が有効になっていて、正しく構成されていることを確認します
- [Aironet IE] が [有効 (Enabled)] になっていることを確認します。

- [P2P (ピアツーピア) ブロッキング アクション (P2P (Peer to Peer) Blocking Action)] を無効にします。
- [クライアント除外タイムアウト (Client Exclusion Timeout)] が正しく構成されていることを確認します
- [DHCPが必要です (DHCP Required)] を無効にします
- [保護された管理フレーム (PMF) (Protected Management Frame (PMF)] は、[任意 (Optional)]、[必須 (Required)] または [無効 (Disabled)] に設定する必要があります

- [DTIM周期 (DTIM Period)] を [2] に設定します
- [負荷分散 (Load Balance)] を [無効 (Disabled)] に設定します
- [帯域選択 (Band Select)] を [無効 (Disabled)] に設定します
- [IGMPスヌーピング (IGMP Snooping)] を [有効 (Enabled)] に設定します。
- 必要に応じて [データレート (Data Rates)] を設定します。
- 必要に応じて [RRM] を設定します
- [EDCAプロファイル (EDCA Profile)] を [音声の最適化 (Voice Optimized)] または [音声およびビデオの最適化 (Voice and Video Optimized)] に設定します
- [電力制限 (Power Constraint)] が [無効 (Disabled)] になっていることを確認します。
- [チャンネルスイッチステータス (Channel Switch Status)] と [スマート DFS (Smart DFS)] を有効にします
- [チャンネルスイッチアナウンス モード (Channel Switch Announcement Mode)] を [待機 (Quiet)] に設定します
- 必要に応じて [高スループットデータレート (High Throughput Data Rates)] を構成します
- [CleanAir] を有効にします
- [マルチキャストダイレクト対応 (Multicast Direct Enable)] を有効にします

802.11 ネットワークの設定

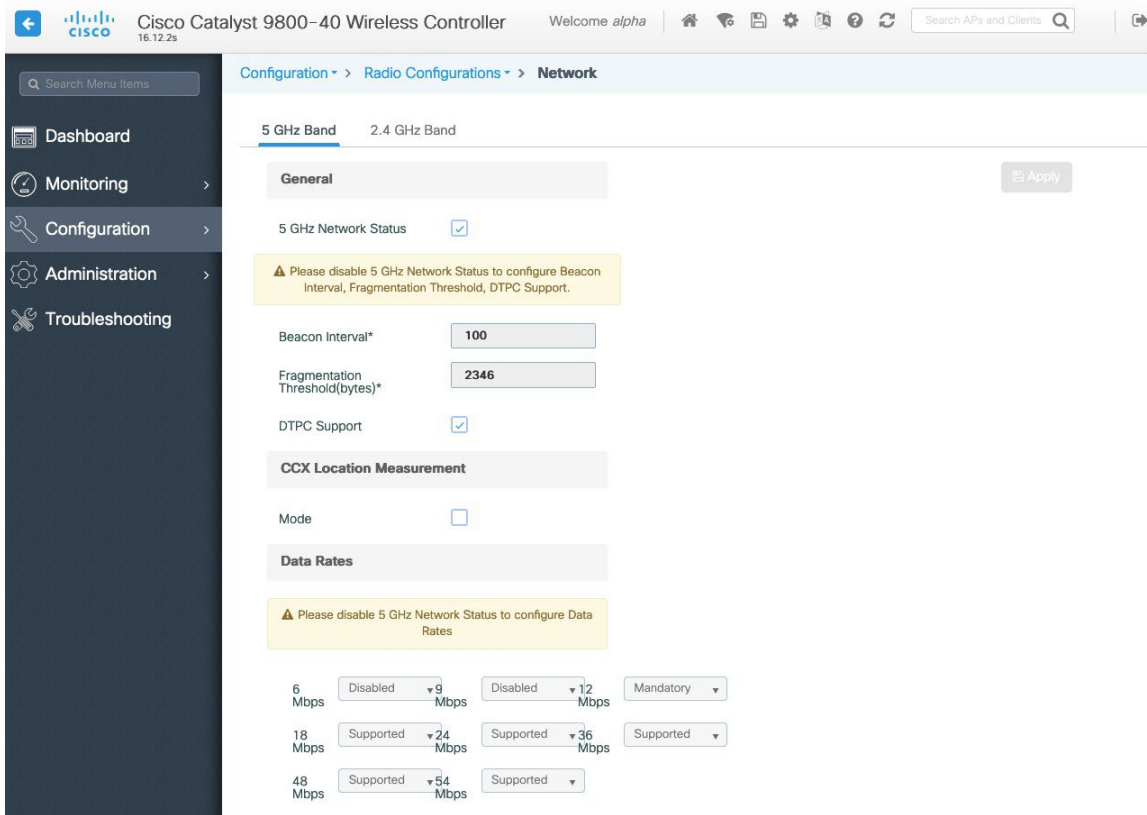
Cisco RoomOS Series は、5 GHz 帯域のみでの動作を推奨します。多数のチャンネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

5 GHz を使用する場合は、5 GHz ネットワークのステータスが

[有効 (Enabled)]

に設定されていることを確認します。[ビーコン周期 (Beacon Period)] を [100 ms] に設定します。

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



2.4 GHz を使用する場合は、2.4 GHz ネットワークのステータスと 802.11g

ネットワークのステータスが **[有効 (Enabled)]**

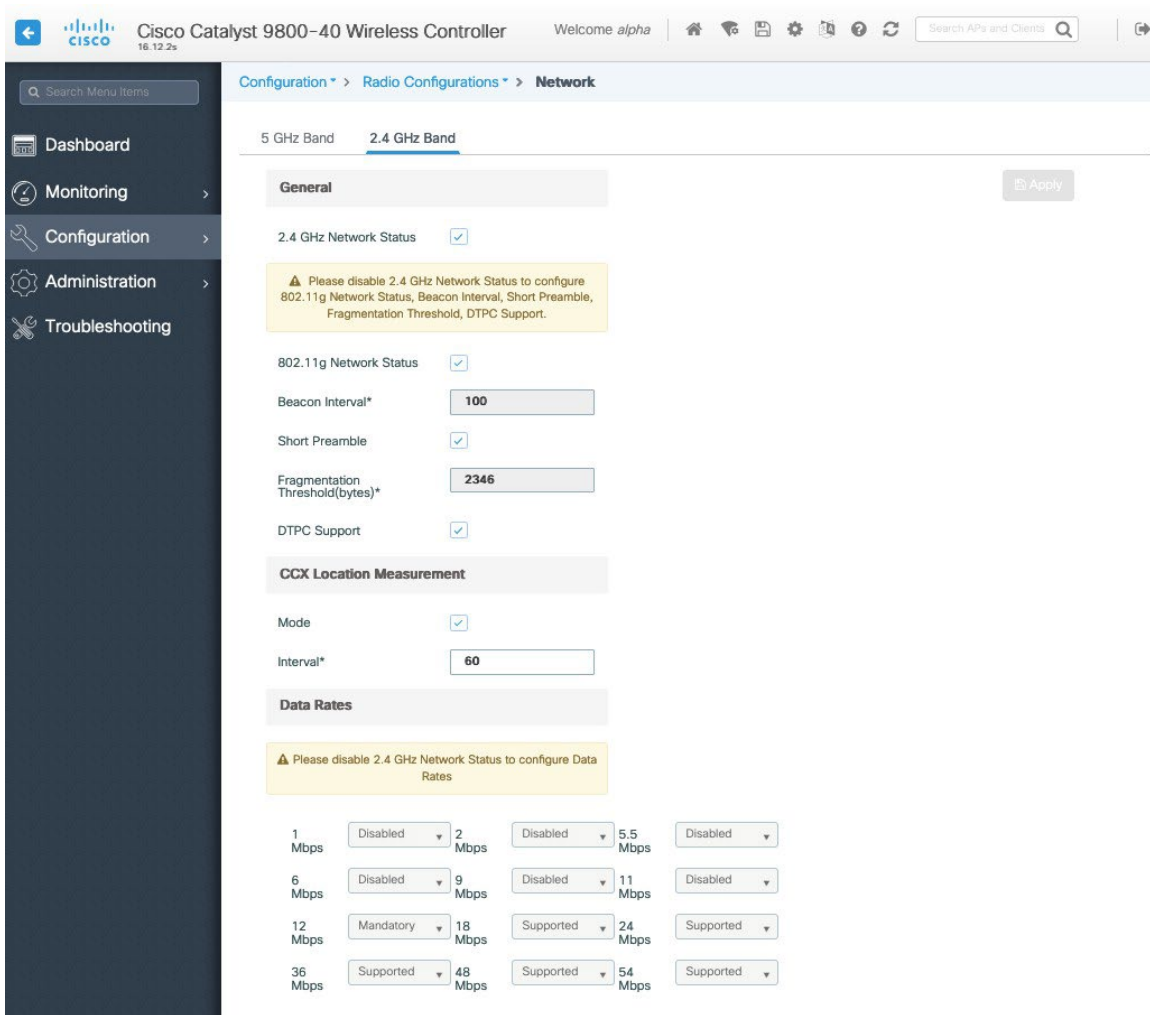
に設定されていることを確認します。 **[ビーコン周期 (Beacon Period)]** を **[100 ms]**

に設定します。

ロングプリアンプルを必要とするレガシークライアントがワイヤレス LAN に存在しない場合は、アクセスポイントの 2.4 GHz 無線設定で **[ショートプリアンプル (Short Preamble)]** を **[有効 (Enabled)]** に設定します。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によって、ワイヤレス ネットワークのパフォーマンスが向上します。

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

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



高スループット (802.11n/ac/ax)

802.11n および 802.11ax のデータ レートは、無線帯域 (2.4 GHz および 5 GHz) ごとに設定できます。802.11ac データ レートは 5 GHz にのみ適用できます。

[WMM] が有効になっていること、および [WPA3 (AES)] または [WPA2 (AES)] が 802.11n/ac/ax データレートを使用するよう構成されていることを確認します。

Cisco RoomOS Series は、HT MCS 0 ~ MCS 15 と VHT MCS 0 ~ MCS 9 1SS および 2SS データレートのみをサポートしますが、同じ帯域を使用し、MIMO アンテナテクノロジーを利用する他の 802.11n/ac/ax クライアントが存在していて、より高いレートが利用可能な場合には、オプションでより高い MCS レートを有効にできます。

Cisco Catalyst 9800-40 Wireless Controller 16.12.2a 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

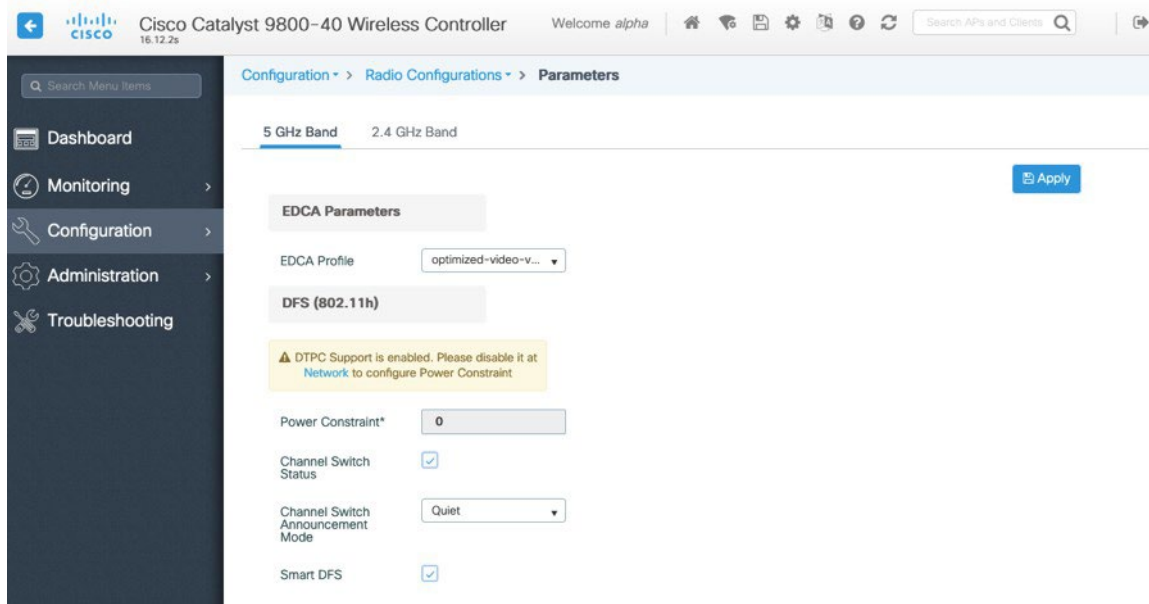
パラメータ

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

DFS (802.11h) セクションで、[電力制限 (Power Constraint)] は未設定のままにするか、0 dB に設定する必要があります。
[チャンネルスイッチステータス (Channel Switch Status)] と [スマートDFS (Smart DFS)]

が有効になっている必要があります。

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

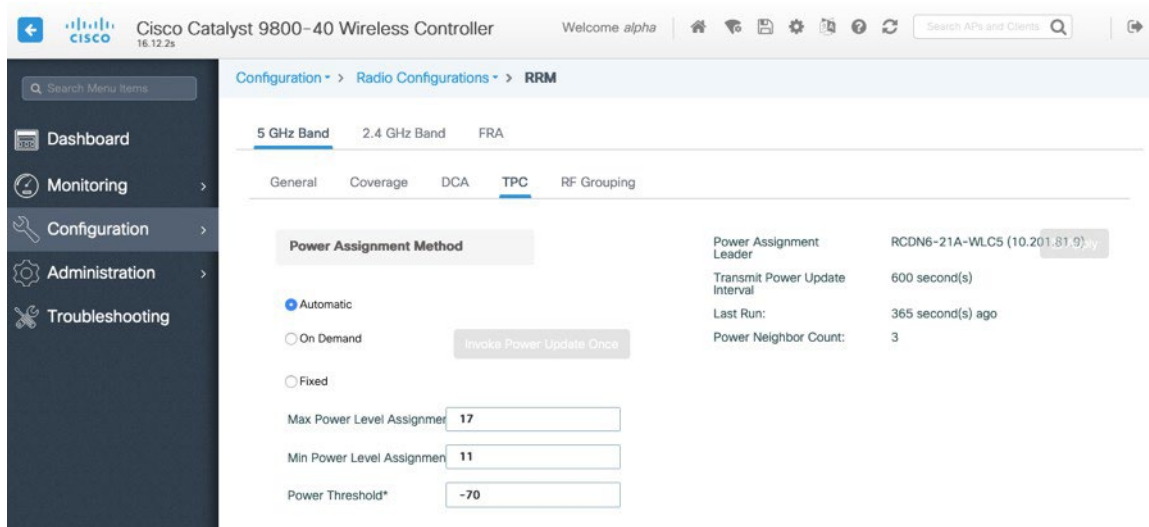


RRM

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

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

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



5 GHz

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

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャンネルの幅を 20 MHz または 40 MHz として構成でき、Cisco 802.11ac または 802.11ax アクセス ポイントを使用している場合はチャンネルの幅を 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。

Cisco Catalyst 9800-40 Wireless Controller

Welcome alpha

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band FRA

General Coverage **DCA** TPC RF Grouping

Dynamic Channel Assignment Algorithm [Apply]

Channel Assignment Mode

- Automatic
- Freeze [Invoke Channel Update Once]
- Off

Interval: 10 minutes

Anchortime: 0

Avoid Foreign AP Interference:

Avoid Cisco AP load:

Avoid Non 5 GHz Noise:

Avoid Persistent Non-wifi Interference:

Channel Assignment Leader: RCDN6-21A-WLC5 (10.201.81.9)

Last Auto Channel Assignment: 475 second(s) ago

DCA Channel Sensitivity: medium

Channel Width: 20 MHz 40 MHz 80 MHz 160 MHz Best

Auto-RF Channel List

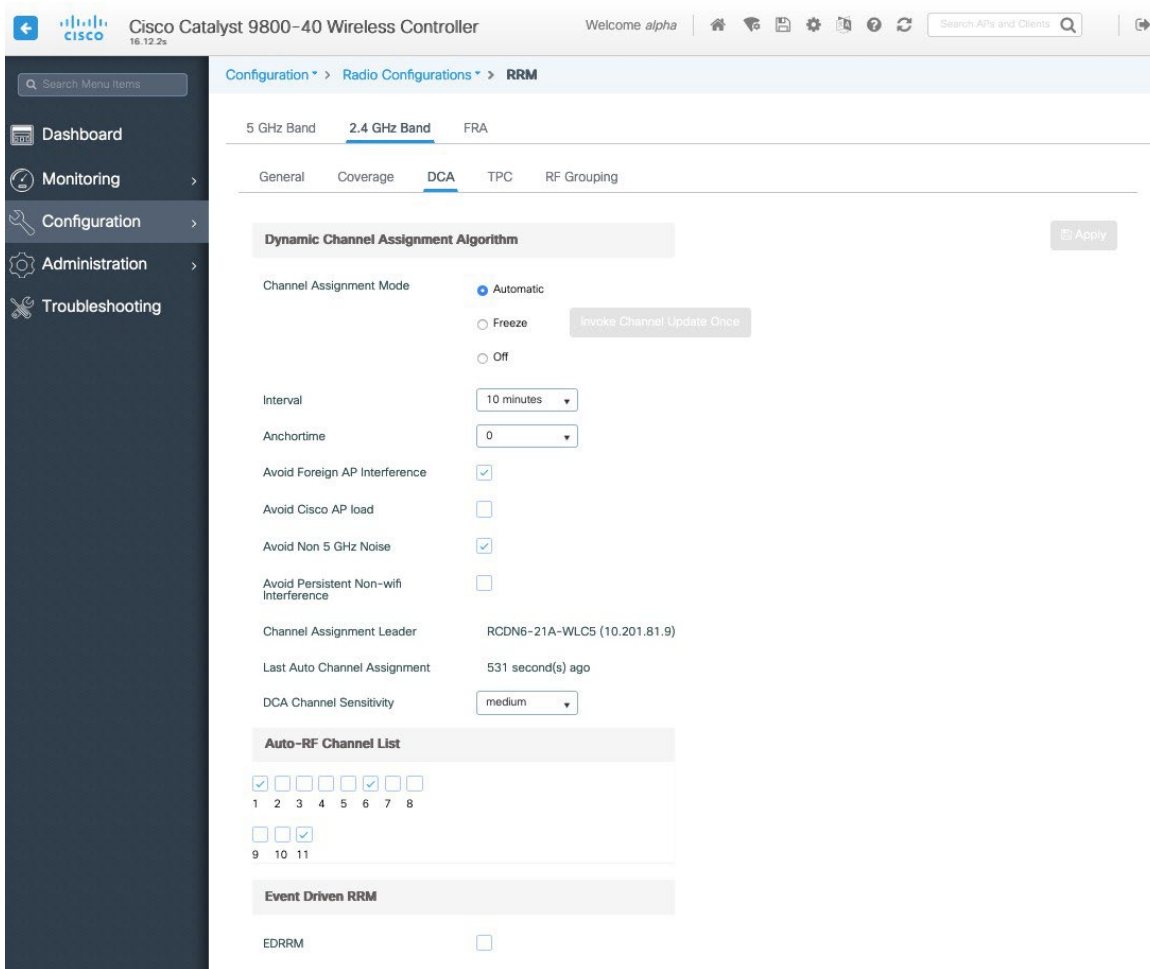
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136

140 144 149 153 157 161 165

Event Driven RRM

EDRRM:

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



使用する周波数帯域に応じて 5 GHz または 2.4 GHz

にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセスポイントの設定をグローバル設定よりも優先させることができます。

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネルの幅を 20 MHz または 40 MHz として構成でき、Cisco 802.11ac または 802.11ax アクセスポイントを使用している場合はチャンネルの幅を 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 configuration page for a 5 GHz radio on a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "Edit Radios 5 GHz Band" and has two tabs: "Configure" (selected) and "Detail".

General

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

RF Channel Assignment

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

Antenna Parameters

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

Tx Power Level Assignment

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

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

CleanAir

CleanAir テクノロジーを搭載したCisco

製のアクセスポイントを使用して既存の干渉を検出する場合は、**[CleanAirの有効化 (Enable CleanAir)]** を **[有効 (Enabled)]** にする必要があります。

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

General

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

Available Interference Types

Interference Types to detect

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

Buttons: "Apply".

WLAN の設定

Cisco RoomOS Series には個別の SSID を使用することをお勧めします。

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

Cisco RoomOS Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように構成できます (802.11a のみなど)。

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

選択した SSID が他の LAN

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



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

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

Cisco Catalyst 9800-40 Wireless Controller

Welcome alpha

Search APs and Clients

Configuration > Tags & Profiles > Edit WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode: WPA + WPA2

Fast Transition: Enabled

MAC Filtering:

Over the DS:

Protected Management Frame

Reassociation Timeout: 20

PMF: Disabled

WPA Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption: AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

MPSK:

Auth Key Mgmt: 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

Cancel Update & Apply to Device

Cisco Catalyst 9800-40 Wireless Controller

Welcome alpha

Search APs and Clients

Configuration > Tags & Profiles > Edit WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode: WPA + WPA2

Fast Transition: Enabled

MAC Filtering:

Over the DS:

Protected Management Frame

Reassociation Timeout: 20

PMF: Disabled

WPA Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption: AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

MPSK:

Auth Key Mgmt: 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

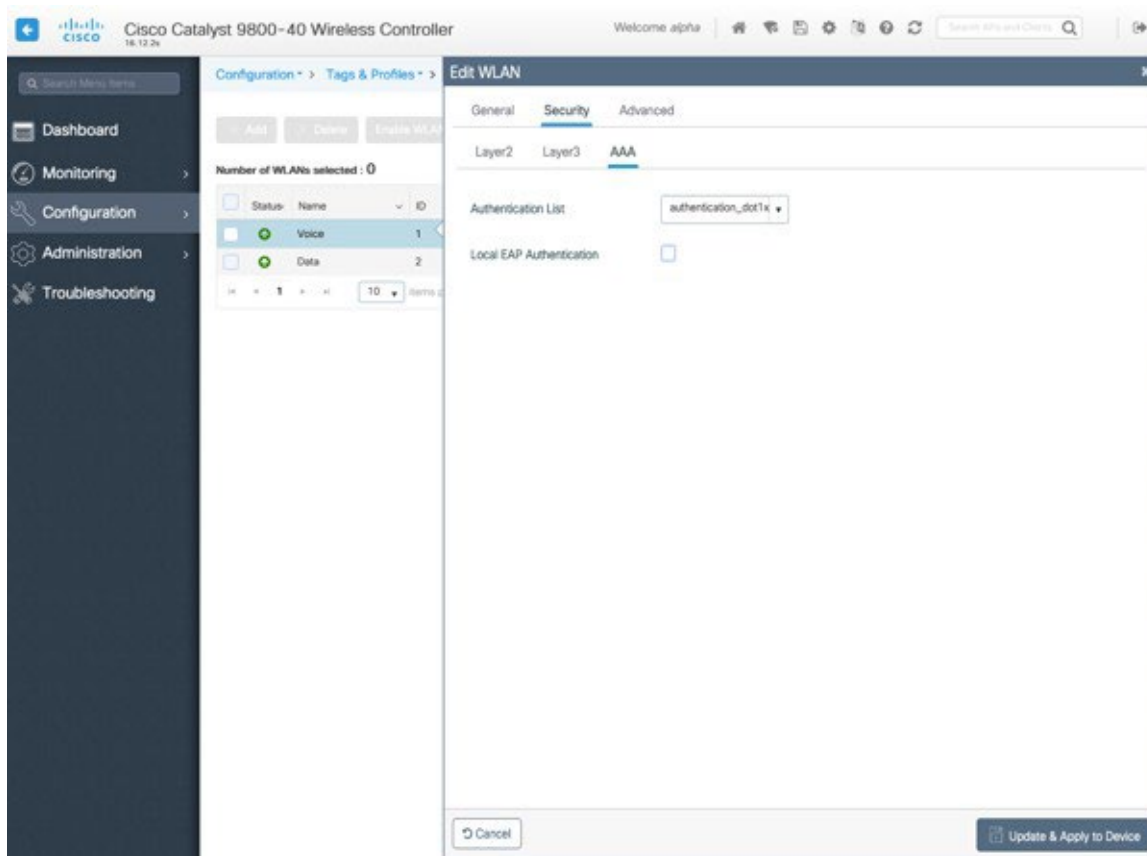
PSK Format: ASCII

DCX Type: Unauthenticated

Cancel Update & Apply to Device

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

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



[Aironet IE] は [有効 (Enabled)] にします。

[ピアツーピア (P2P) のブロッキングアクション (Peer to Peer (P2P) Blocking Action)] は [無効 (Disabled)] にします。

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

WLAN に非 WMM クライアントが存在する場合、それらのクライアントを別の WLAN に配置することを推奨します。他の非 WMM クライアントで Cisco RoomOS Series と同じ SSID を使用する必要がある場合は、WMM ポリシーが [許可 (Allowed)] に設定されていることを確認します。

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

[オフチャンネル スキャンの待機 (Off Channel Scanning Defer)]

を調整することで、スキャンの待機時間だけでなく、特定のキューに対するスキャンを待機させることができます。キュー 4～6 の遅延優先順位を有効にすることをお勧めします。

ベスト エフォート

アプリケーションを頻繁に使用する場合、または優先順位の高いアプリケーション (音声、呼制御など) の DSCP

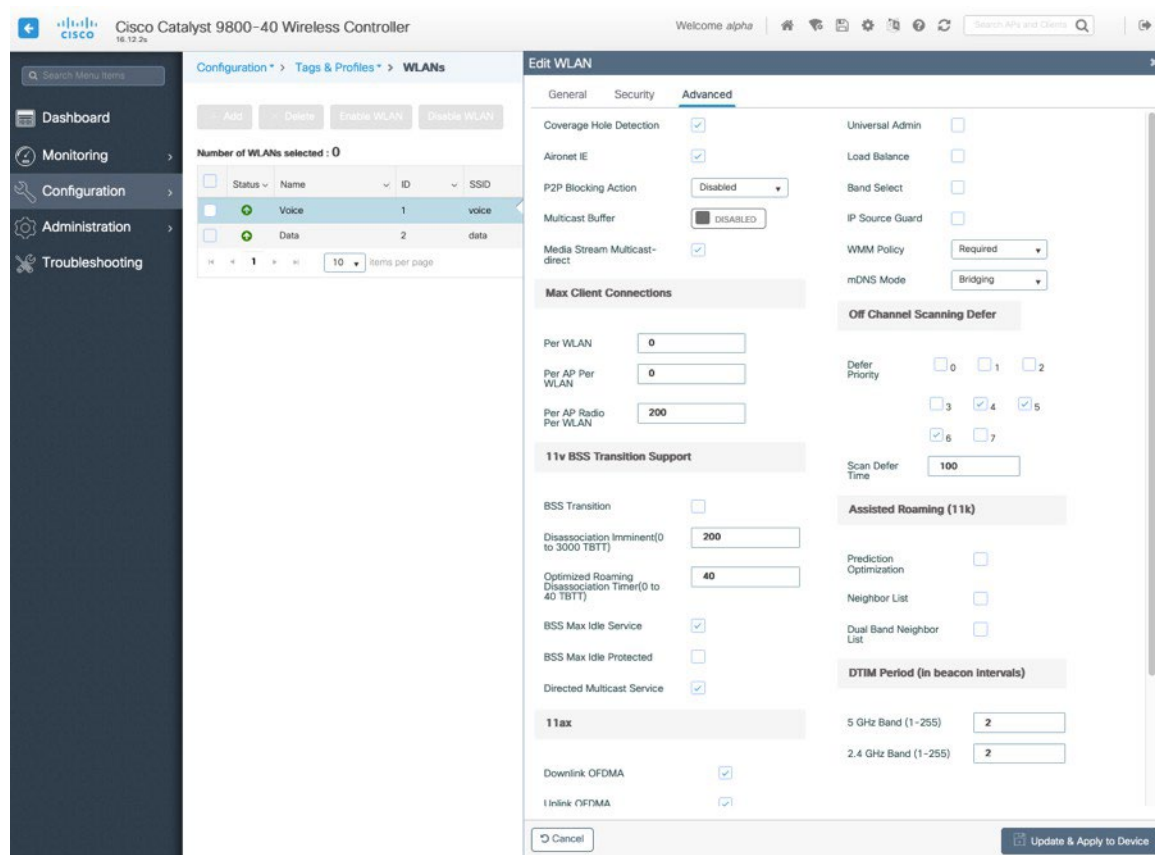
値がアクセスポイントに保持されていない場合は、優先順位の高いキュー（4～6）と共に優先順位の低いキュー（0～3）を有効にしてオフチャンネルスキャンを待機させるとともに、場合によってはスキャンの待機時間を長くすることを推奨します。

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

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

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

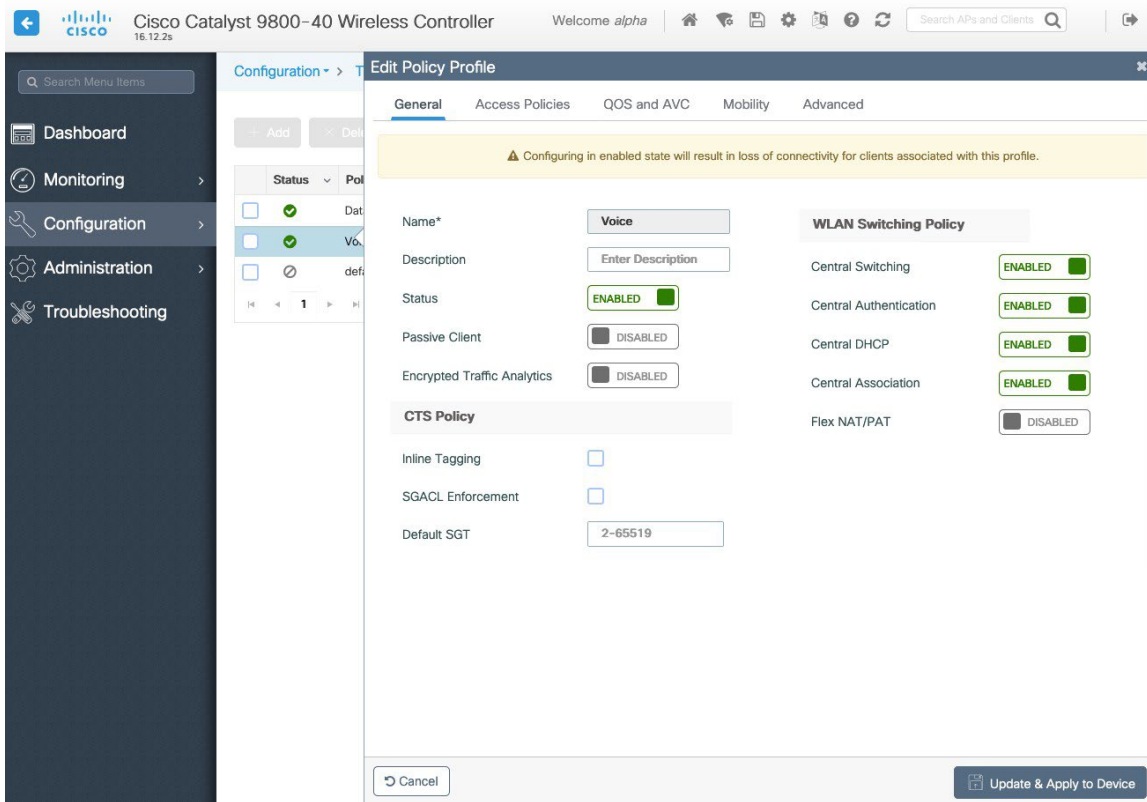
802.11k と 802.11v はサポートされていないため、無効にする必要があります。



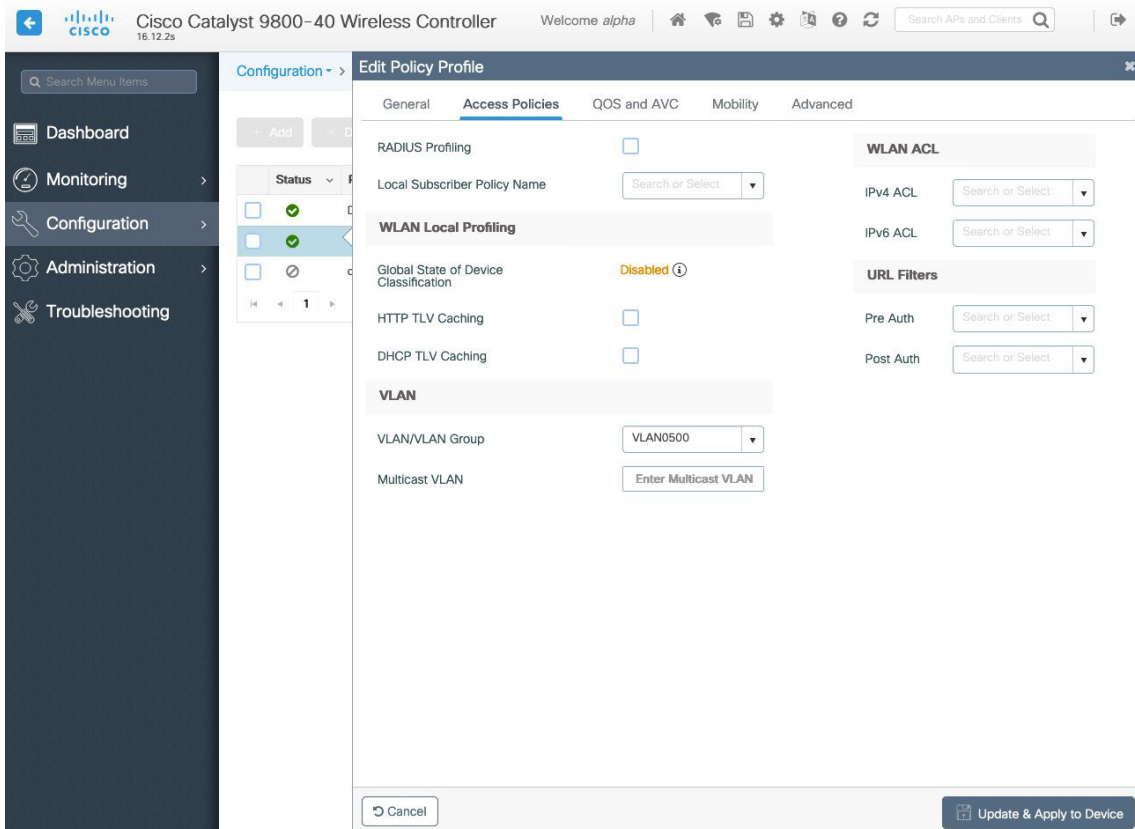
ポリシープロファイル

ポリシープロファイルは、アクセス、QoS、モビリティ、および詳細設定に関する追加設定を定義するために使用されます。次に、ポリシープロファイルは、アクセスポイントに適用できるポリシータグを介して WLAN プロファイルにマッピングされます。

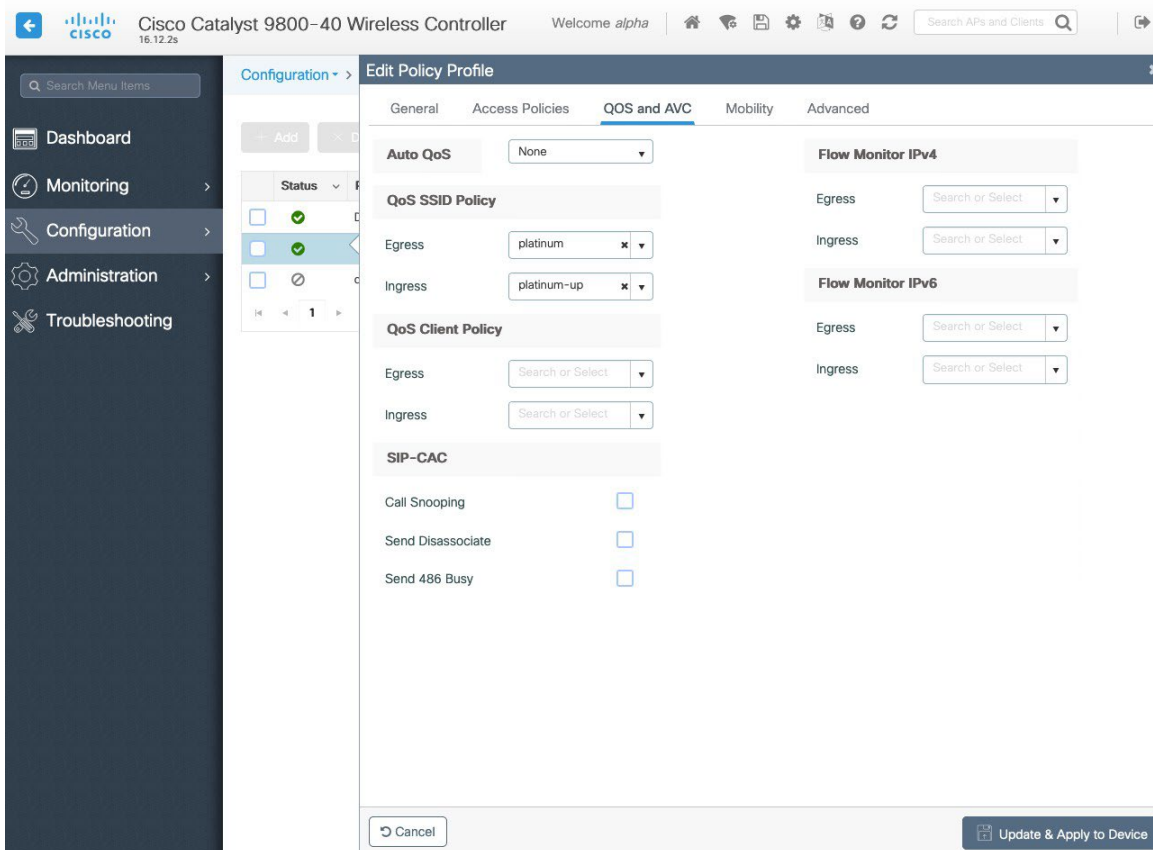
ポリシープロファイルの [ステータス (Status)] が [有効 (Enabled)] になっていることを確認します。



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



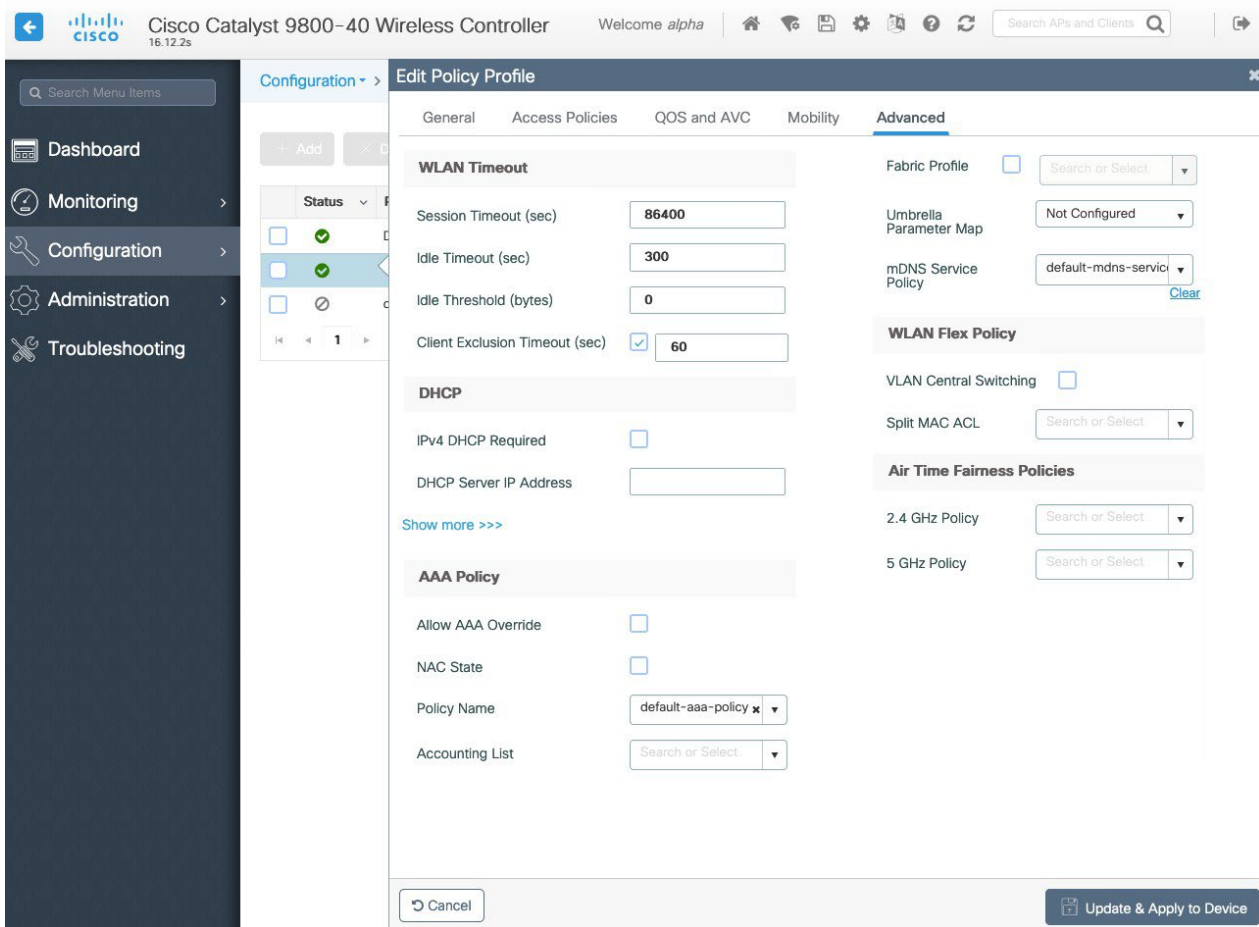
QoS SSID ポリシーが、出力の場合は [プラチナ (Platinum)] に、入力の場合は [プラチナアップ (Platinum-up)] に設定されていることを確認します。



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

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

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



RFプロフィール

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

Cisco RoomOS Series で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。RF プロファイルは RF タグに適用され、アクセスポイントに適用できます。

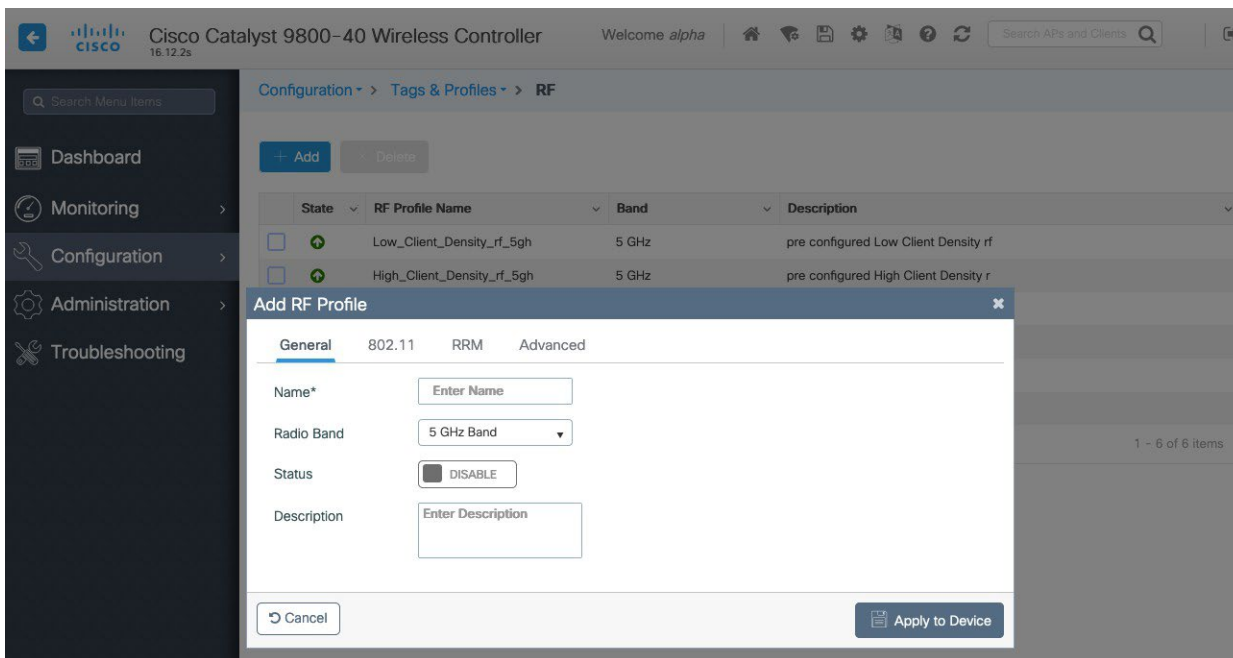
RF プロファイルを作成する場合、[名前 (Name)] と

[無線ポリシー (Radio Policy)]

を定義する必要があります。[無線帯域 (Radio Band)] には、[5

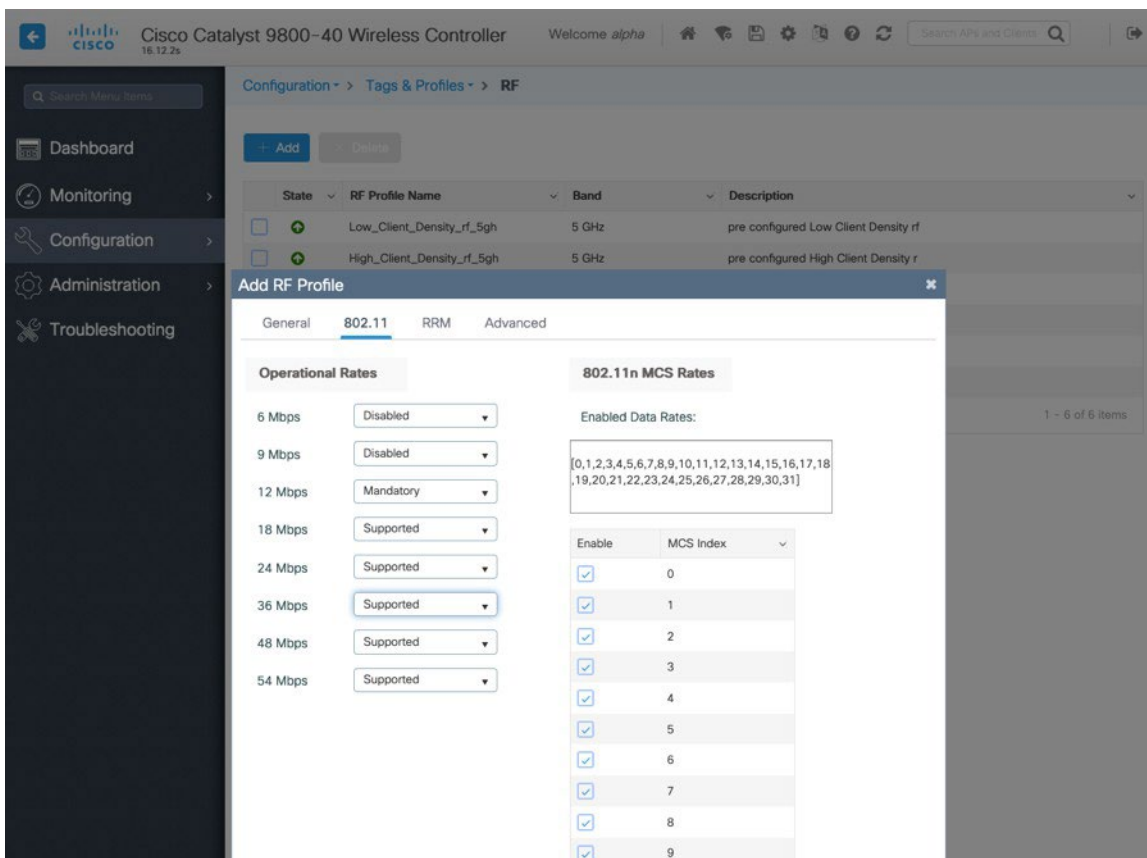
GHz帯域 (5 GHz Band)] または [2.4 GHz帯域 (2.4 GHz Band)]

を選択します。



[802.11] タブで、必要に応じてデータレートを設定します。

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



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

Cisco Catalyst 9800-40 Wireless Controller 16.12.2a

Welcome alpha

Configuration > Tags & Profiles > RF

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

Add RF Profile

General 802.11 **RRM** Advanced

General Coverage **TPC** DCA

Coverage Hole Detection

Minimum Client Level (clients)*

Data RSSI Threshold (dBm)*

Voice RSSI Threshold (dBm)*

Exception Level(%)*

Cisco Catalyst 9800-40 Wireless Controller 16.12.2a

Welcome alpha

Configuration > Tags & Profiles > RF

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

Add RF Profile

General 802.11 **RRM** Advanced

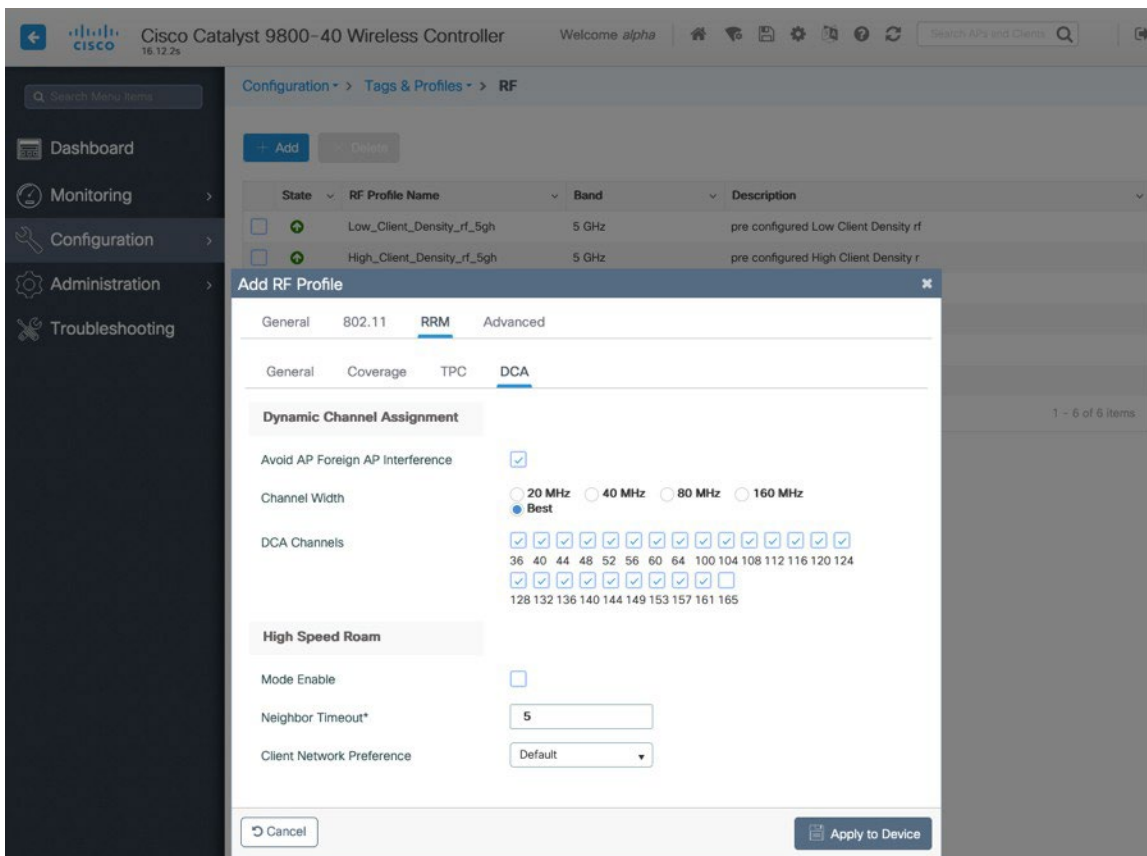
General Coverage **TPC** DCA

Transmit Power Control

Maximum Power Level(dBm)*

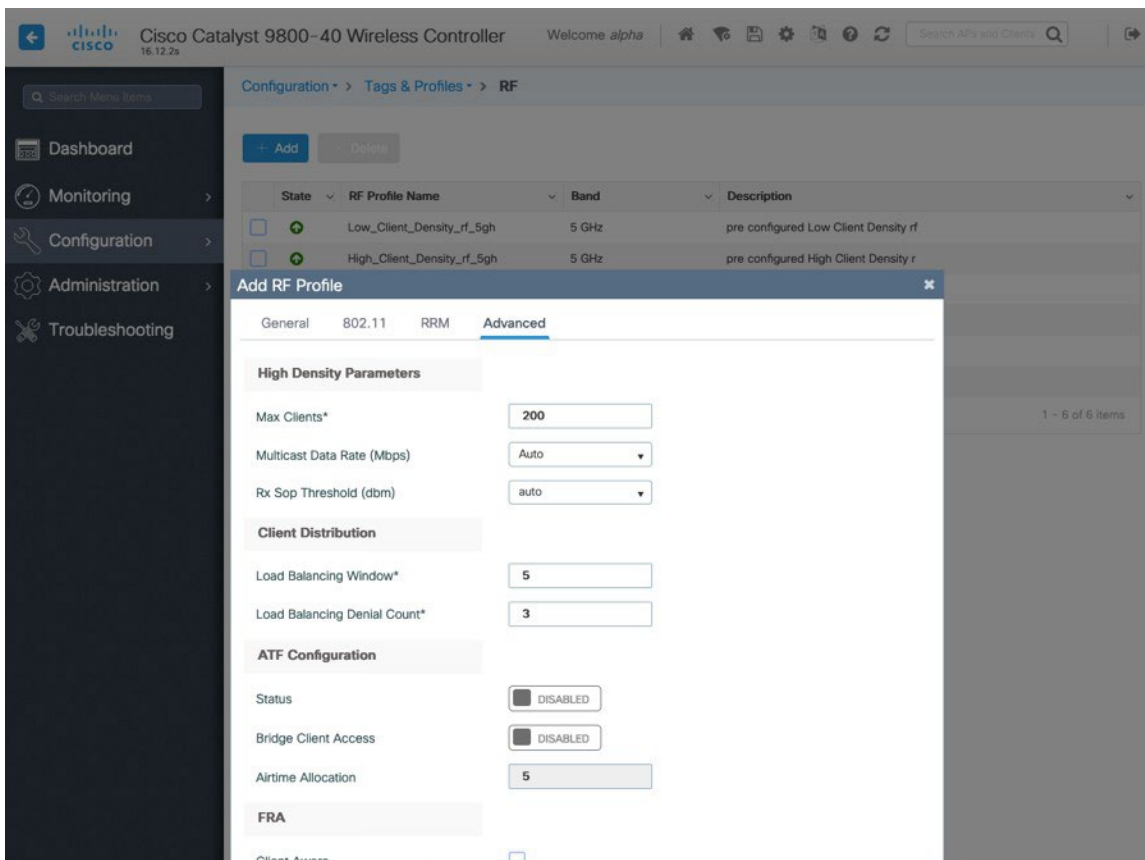
Minimum Power Level(dBm)*

Power Threshold V1(dBm)*



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

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



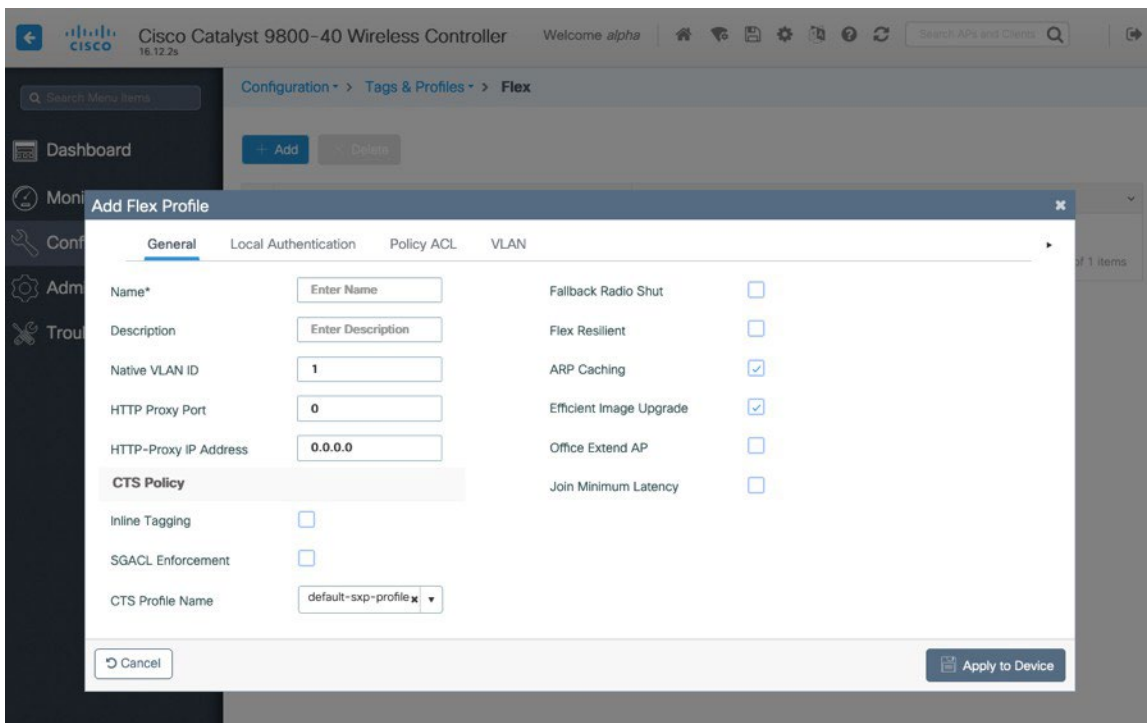
Flexプロファイル

Flex プロファイルは、アクセスポイントが Flexconnect

モードで使用する必要がある設定を定義するために使用されます。次に、Flex プロファイルはサイトタグに適用され、アクセスポイントに適用できます。

使用するアクセスポイントのネイティブ VLAN ID と、許可された VLAN を構成します。[ARPキャッシング (ARP Caching)] が [有効 (Enabled)] になっていることを確認します。

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



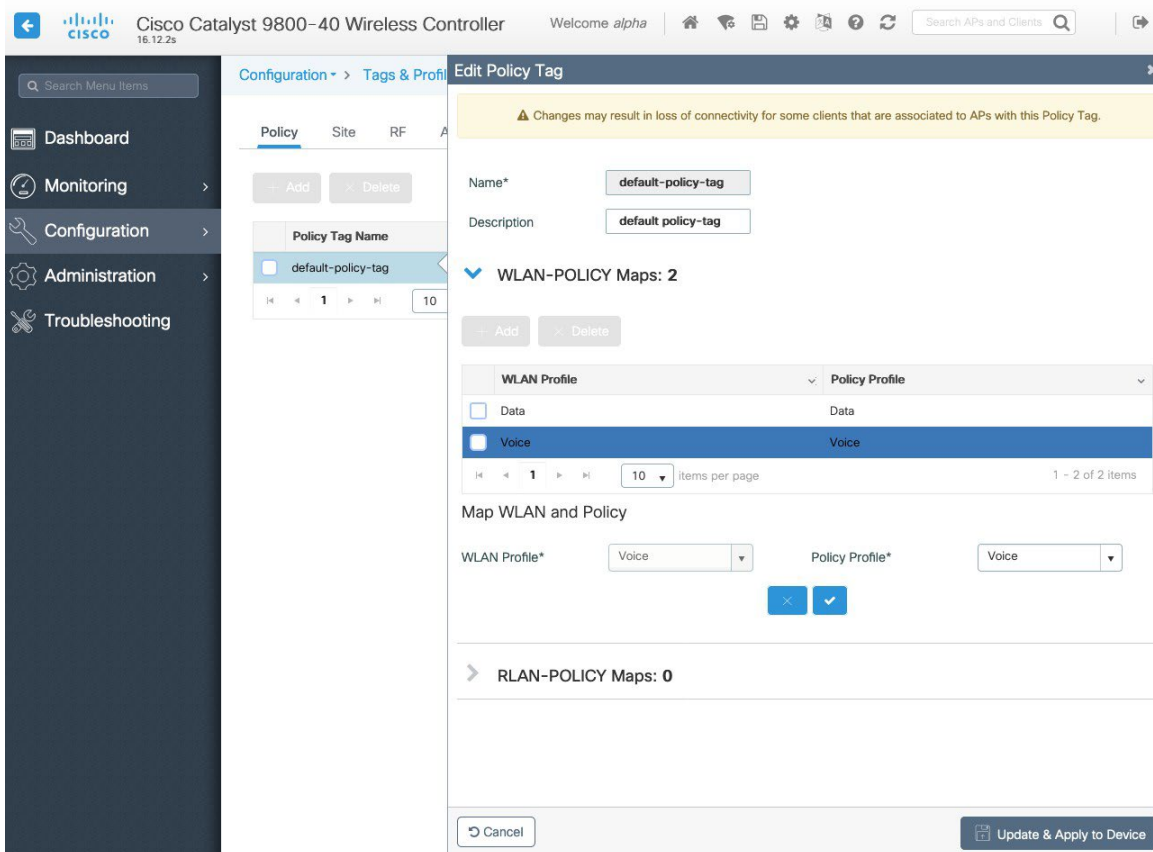
タグ

ポリシータグ

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

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

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



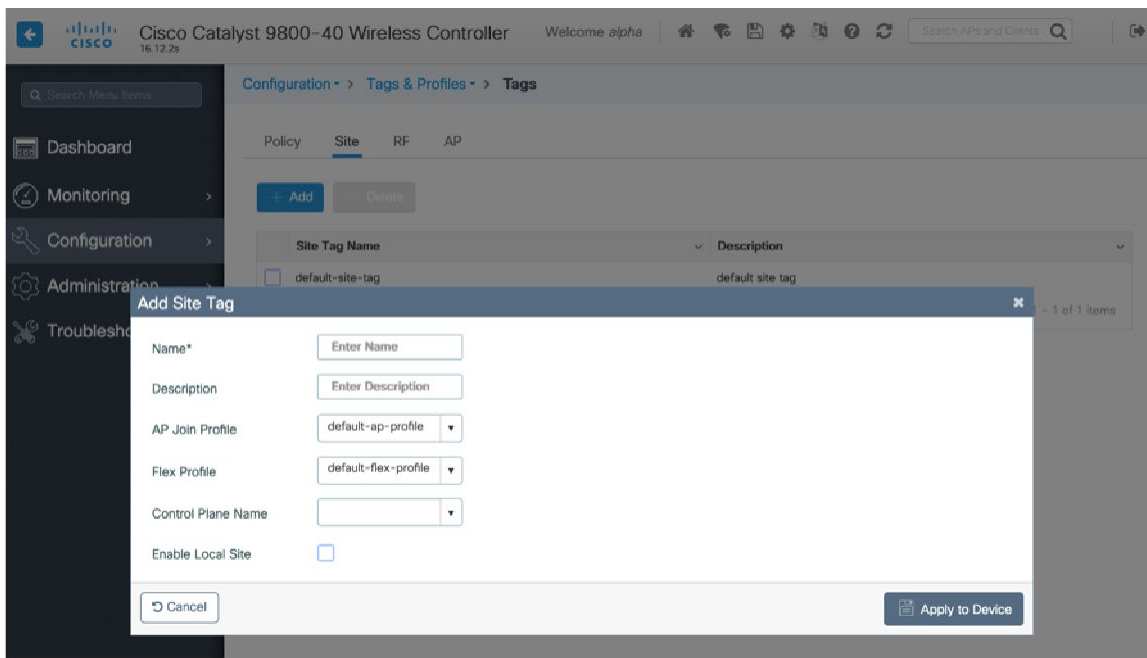
サイトタグ

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

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

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

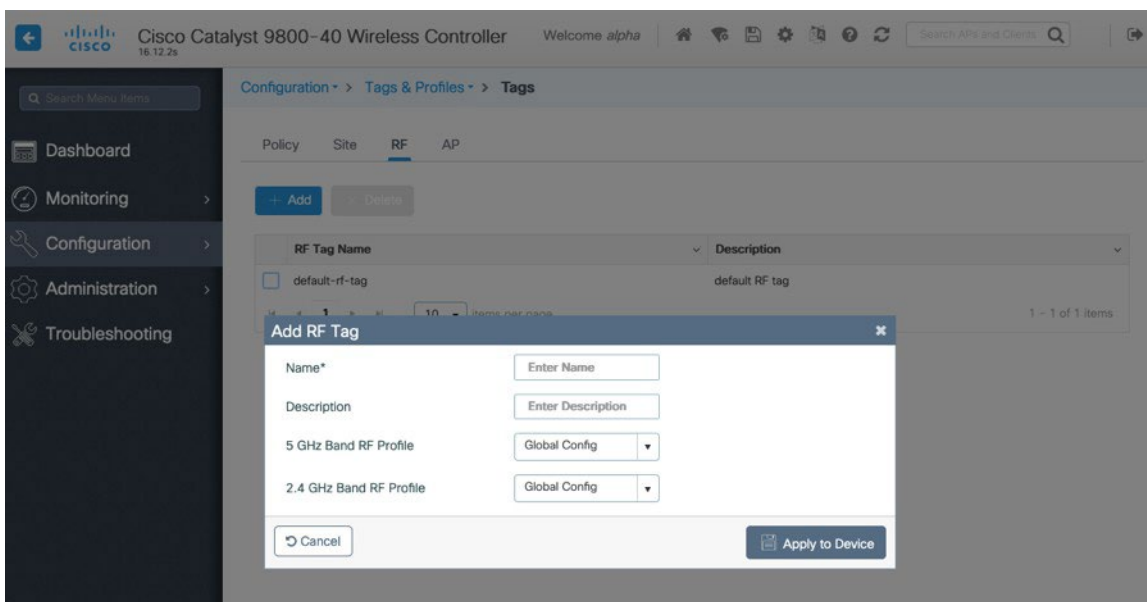
Flex プロファイルを含むサイトタグを作成する場合は、**[ローカルサイトの有効化 (Enable Local Site)]** がチェックされていないことを確認してから、必要な **[Flexプロファイル (Flex Profile)]** を選択します。



RF タグ

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

次に、RF タグがアクセスポイントに適用され、使用する RF



プロファイルパラメータを指定します。RF タグを作成する場合は、使用する [5

GHz帯域RFプロファイル (5 GHz Band RF Profile)] と [2.4 GHz帯域RFプロファイル (2.4

GHz Band RF Profile)] を選択します。

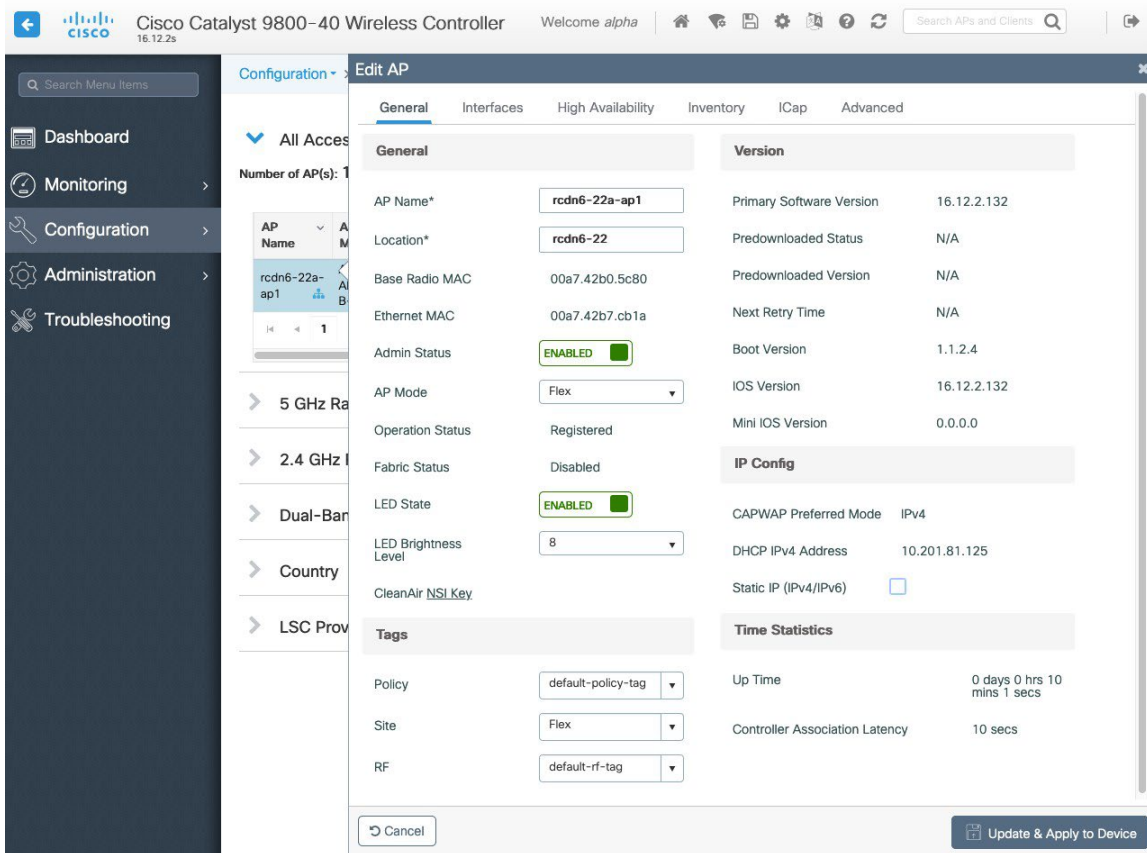
タグを定義したら、アクセスポイントに適用できます。

The screenshot shows the 'Edit AP' configuration page for a Cisco Catalyst 9800-40 Wireless Controller. The page is divided into several sections:

- General:**
 - AP Name*: rcdn6-22a-ap1
 - Location*: rcdn6-22
 - Base Radio MAC: 00a7.42b0.5c80
 - Ethernet MAC: 00a7.42b7.cb1a
 - Admin Status: ENABLED
 - AP Mode: Local
 - Operation Status: Registered
 - Fabric Status: Disabled
 - LED State: ENABLED
 - LED Brightness Level: 8
 - CleanAir NSI Key: (empty)
- Version:**
 - Primary Software Version: 16.12.2.132
 - Predownloaded Status: N/A
 - Predownloaded Version: N/A
 - Next Retry Time: N/A
 - Boot Version: 1.1.2.4
 - IOS Version: 16.12.2.132
 - Mini IOS Version: 0.0.0.0
- IP Config:**
 - CAPWAP Preferred Mode: IPv4
 - DHCP IPv4 Address: 10.201.81.125
 - Static IP (IPv4/IPv6):
- Tags:**
 - Policy: default-policy-tag
 - Site: default-site-tag
 - RF: default-rf-tag
- Time Statistics:**
 - Up Time: 10 days 18 hrs 16 mins 54 secs
 - Controller Association Latency: 2 mins 4 secs

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

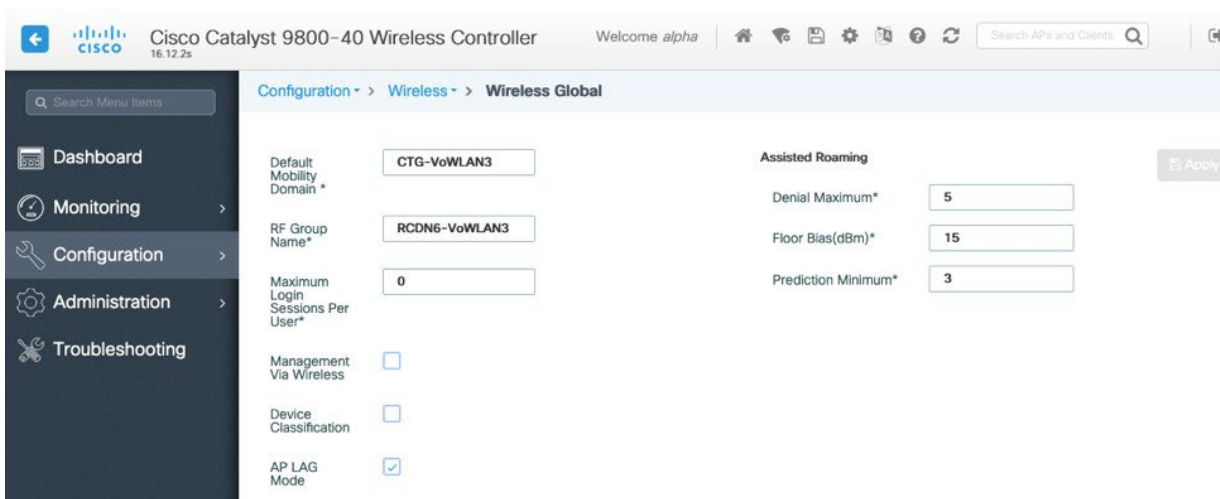
設定されたフレックスプロファイルを含むサイトタグが適用されている場合、[APモード (AP Mode)] は自動的に [フレックス (Flex)] に変更されます。



コントローラの設定

[デフォルトのモビリティドメイン (Default Mobility Domain)]

が正しく設定されていることを確認します。 [AP LAG モード (AP LAG Mode)] を有効にします。



モビリティ設定

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

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

The screenshot shows the 'Global Configuration' tab for the 'Mobility' section. The following fields are visible:

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

The screenshot shows the 'Peer Configuration' tab for the 'Mobility' section. It displays a table of Mobility Peer Configuration entries:

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

Below the table, there is a section for 'Non-Local Mobility Group Multicast Configuration'.

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

The screenshot shows the 'Wireless' section under 'Interface' configuration. It displays a table of wireless interface entries:

Interface Name	Interface Type	Trustpoint Name	VLAN ID	IP Address	IP Netmask	MAC Address
Vlan310	Management		310	10.201.81.9	255.255.255.240	70:6d:15:3d:b5:0b

コール アドミッション制御 (CAC)

[ボイス (Voice)] で [アドミッション制御必須 (Admission Control Mandatory)] を有効にして、使用する帯域 (5 GHz または 2.4

GHz) に対して最大帯域幅および予約済みのローミング帯域幅の各割合を設定することを推奨します。

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

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

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

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

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

S RTP

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

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

[ユニキャストビデオリダイレクト (Unicast Video Redirect)] と [マルチキャストダイレクトの有効化 (Multicast Direct Enable)] を [有効 (Enabled)] にする必要があります。

The screenshot shows the configuration page for a Cisco Catalyst 9800-40 Wireless Controller, specifically the 'Media Parameters' section for the 5 GHz band. The page is divided into several sections:

- Media - General:** Unicast Video Redirect is checked.
- Multicast Direct Admission Control:** Multicast Direct Admission Control is checked.
- Media Stream Admission Control (ACM):** Media Stream Admission Control (ACM) is unchecked. Maximum Media Stream RF bandwidth (%) is 5, Maximum Media Bandwidth (%) is 85, Client Minimum Phy Rate (kbps) is 6000, and Maximum Retry Percent (%) is 80.
- Media Stream - Multicast Direct Parameters:** Multicast Direct Enable is checked. Max streams per Radio and Max streams per Client are both set to 'No Limit'. Best Effort QOS Admission is unchecked.
- Voice - Call Admission Control (CAC):** Admission Control (ACM) and Load Based CAC are checked. Max RF Bandwidth (%) is 75, Reserved Roaming Bandwidth (%) is 6, and Expedited Bandwidth is checked.
- SIP CAC and Bandwidth:** SIP CAC Support is unchecked.
- Traffic Stream Metrics:** Metrics Collection is checked. Stream Size is 84000, Max Streams is 2, and Inactivity Timeout is unchecked.

マルチキャスト

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

Configuration > Services > Multicast

Global Wireless Multicast Mode: **ENABLED**

Wireless mDNS Bridging: **DISABLED**

Wireless Non-IP Multicast: **DISABLED**

Wireless Broadcast: **DISABLED**

AP Capwap Multicast: Unicast

MLD Snooping: **DISABLED**

IGMP Snooping Querier: **DISABLED**

IGMP Snooping: **ENABLED**

Last Member Querier Interval (milliseconds): 1000

IGMP Snooping

Disabled: No Vlan available

Enabled:

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

Buttons: Enable All, Disable All

> Wireless Broadcast and Wireless Non-IP Multicast

メディアストリームの設定で、[マルチキャストダイレクト機能の有効化 (Multicast Direct Enable)] を [有効 (Enabled)] にする必要があります。

Configuration > Wireless > Media Stream

General | Streams

Multicast Direct Enable:

Session Message Config

Session Announcement State:

Session Announcement URL:

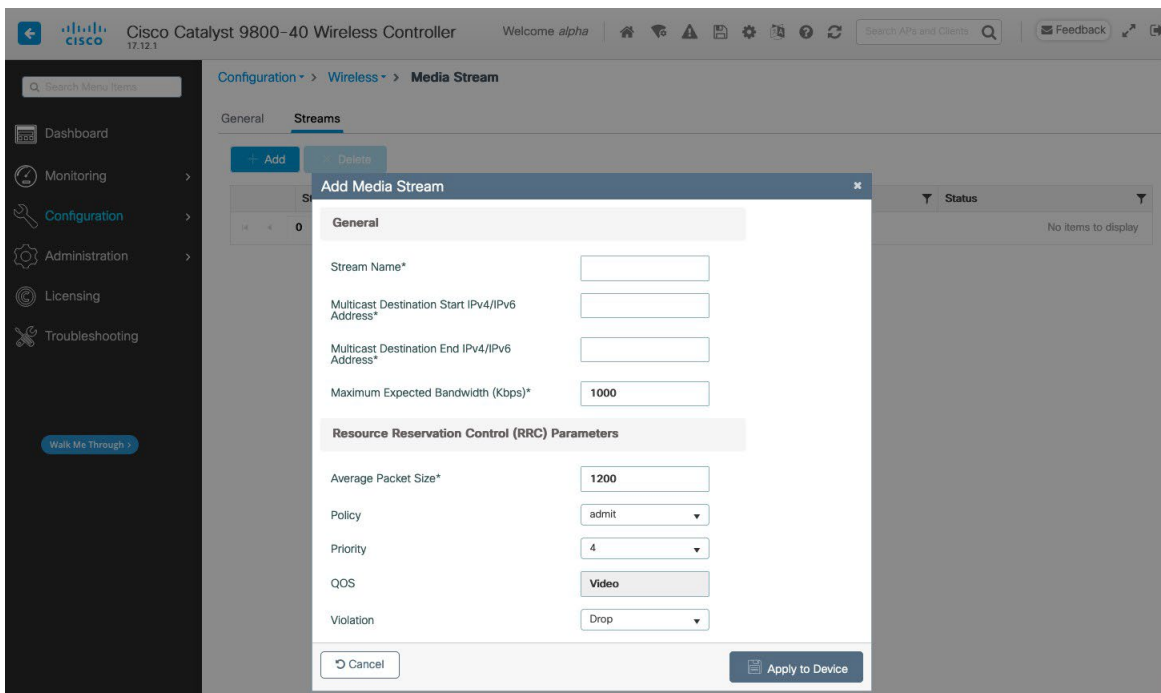
Session Announcement Email:

Session Announcement Phone:

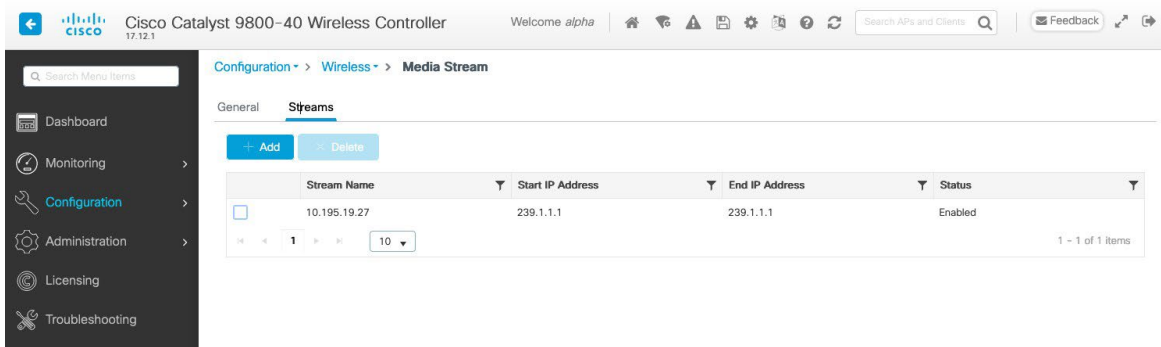
Session Announcement Note:

Buttons: Apply

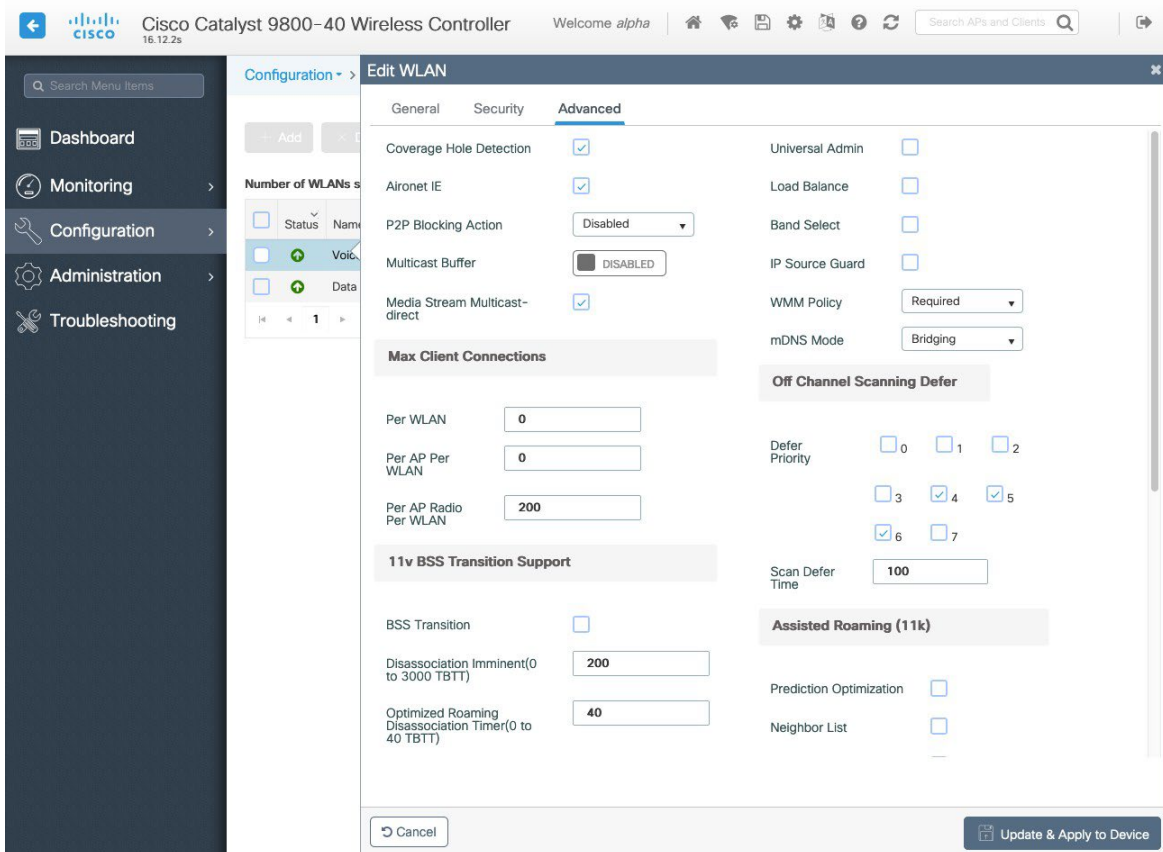
それから、必要に応じてメディア ストリームを設定します。



保存すると、メディアストリームが表示されます。



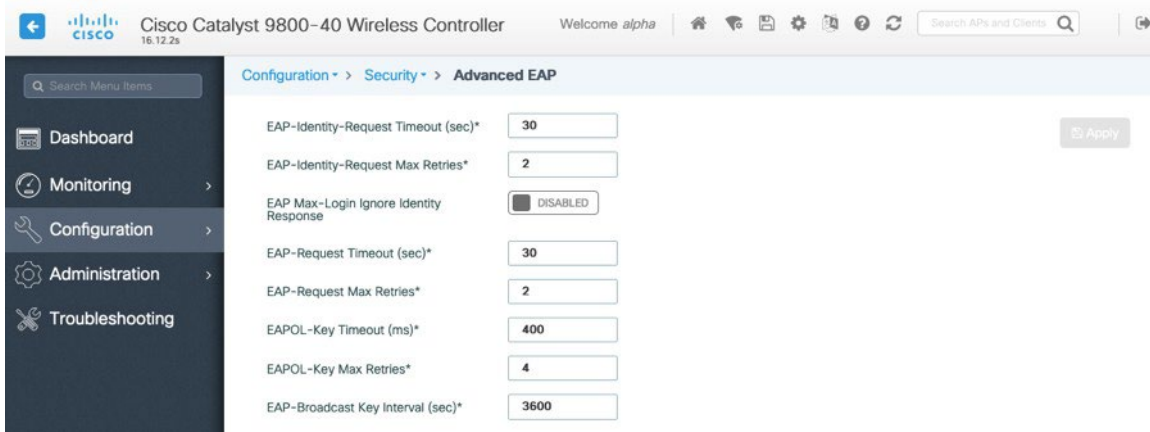
また、WLAN 構成で [マルチキャストダイレクト (Multicast Direct)] を有効にします。



詳細設定

EAP の詳細設定

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



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

展開において、EAP の失敗が頻繁に発生する場合には、**[EAP 要求のタイムアウト (EAP-Request Timeout)]** を 30 秒未満に減らす必要があります。

PSK を使用する場合は、**[EAPOL キーのタイムアウト (EAPOL-Key Timeout)]** をデフォルトの 1000 ミリ秒から 400 ミリ秒に減らし、**[EAPOL キーの最大試行回数 (EAPOL-Key Max Retries)]** をデフォルトの 2 から 4 に変更することを推奨します。

802.1x を使用する場合は、**[EAPOL キーのタイムアウト (EAPOL-Key Timeout)]** および **[EAPOL キーの最大試行回数 (EAPOL-Key Max Retries)]** のデフォルト値 (それぞれ 1000 ミリ秒および 2) を使用しても正しく動作しますが、それぞれ 400 および 4 に設定することを推奨します。
[EAPOL キーのタイムアウト (EAPOL-Key Timeout)] は、1000 ミリ秒 (1 秒) を超えないようにしてください。

[EAP ブロードキャスト キーの間隔 (EAP-Broadcast Key Interval)] が 3600 秒 (1 時間) 以上に設定されていることを確認します。

Rx SOPしきい値

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

The screenshot shows the configuration page for the Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Wireless > Advanced. The 'High Density' tab is selected. Under the 'Rx Sop Threshold' section, there are two dropdown menus: 'Rx Sop Threshold 5 GHz (dbm)' and 'Rx Sop Threshold 2.4 GHz (dbm)', both set to 'auto'. Below this is the 'Multicast Data Rate' section with two dropdown menus: 'Multicast Data Rate 5 GHz (Mbps)' and 'Multicast Data Rate 2.4 GHz (Mbps)', both set to 'Auto'. An 'Apply' button is visible in the top right of the configuration area.

不正ポリシー

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

The screenshot shows the configuration page for the Cisco Catalyst 9800-40 Wireless Controller, specifically the 'Wireless Protection Policies' section under 'Security'. The 'RLDP' tab is selected. The 'Rogue Location Discovery Protocol' is set to 'Disable'. The 'Retry Count' is set to '1'. The 'Schedule RLDP' checkbox is unchecked. Below this, there is a table for scheduling the policy by day, with columns for 'Day', 'Start Time', and 'End Time'. All days (Monday through Sunday) are currently unchecked.

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

サンプル構成

```
バージョン 16.12
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname RCDN6-21A-WLC5
!
boot-start-marker
boot system flash bootflash:packages.conf
boot-end-marker
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
no logging console
!
aaa new-model
!
!
aaa group server radius RADIUS_SERVER_GROUP_DAY0
server name RADIUS_SERVER_DAY0_1
server name RADIUS_SERVER_DAY0_2
!
aaa authentication login default local
aaa authentication login authentication_login_day0 group RADIUS_SERVER_GROUP_DAY0 aaa
authentication dot1x authentication_dot1x_day0 group RADIUS_SERVER_GROUP_DAY0 aaa
authorization exec default local
aaa authorization network default local
!
aaa server radius dynamic-author
!
aaa session-id common
clock timezone CST -6 0
clock summer-time CDT recurring
! call-home の連絡先電子メールアドレスが sch-smart-licensing@cisco.com として設定されている場合
! Cisco Smart License Portal で設定された電子メールアドレスは、SCH
通知を送信するための連絡先電子メールアドレスとして使用されます。
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
no destination transport-method email
!
ip domain name cisco.com
!
```

```

login on-success log
!
subscriber templating
!
parameter-map type webauth global
virtual-ip ipv4 1.1.1.6
!
flow exporter wireless-local-exporter
!
flow monitor wireless-avc-basic
exporter wireless-local-exporter
cache timeout active 60
record wireless avc basic
!
no device-tracking logging theft access-
session mac-move deny multilink
bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-3110682001
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3110682001
revocation-check none
rsa keypair TP-self-signed-3110682001
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki certificate chain TP-self-signed-3110682001
certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 33313130 36383230 3031301E 170D3139 30373130 30343236
35375A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31313036
38323030 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100B74F D6A0DE5D DFB2CDD2 5196AAB1 86C8BD48 3AAAF455 C4E7D559
41A10FE1 87EC742C C5014113 9A0FD83A F490EA64 DF68A513 AA6900C4 810A9FED
870309EA 781EB999 882F7374 EC79D592 DEC6C126 A5FB5666 905C24D8 B2064CD4
66823D6E 7E9A07F3 B043D632 EEDF4CAF D306C303 843493AA F44126E3 A07DE905
6B6C5B8E C8E6C9E6 45D79F62 B813FF8C B44FA7AC AEDB8A9E 55B75096 E4E76BC3
D5B90900 1A0C7CD0 910B6C63 920E9666 39EC3702 387757F1 C26F0BB5 89D4733D FED71CF4
33002C77 0F721B21 5578C850 590BC846 7CB79469 A51CEBA5 96EA8672 DDB82A44 69EEDA13
DD83B0FA 3221A839 5F985C86 F2C57B78 8E6608B6 18A346D2 035D3B68 26BF0203 010001A3
53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 141B4651 019E0AEC 8E64EB65 C0E023ED 60F6062C
0F301D06 03551D0E 04160414 1B465101 9E0AEC8E 64EB65C0 E023ED60 F6062C0F
300D0609 2A864886 F70D0101 05050003 82010100 3319F2A7 3E88539F 85C08F28
67553F93 408DCCC6 EFE2704E C142766C 5FFE0E97 0AFDE0EA 816CB4E2 60FFBC26
6E411C57 3F1AB3F8 2F1E9959 AED26C86 2C0B059D B692C72C B5859A15 999916F8
699587DC 94409E7C FF685698 2FB9ACEC 9315F1AA 357E3877 7AE1E37C F5CD7E46
EB3ADC44 3F22A9E0 EA35E6B8 E5508721 0E8754A1 6A6E3A6A C7FD8E64 6C3C722C
F90919C9 DE675E5C 301FF83A 0593ACE6 4A469209 CAAEC53F 5102FDD3 AE378090 46282E00
BCF65EB7 4C257EFD 57986F82 B6DD8336 CEA82E27 63B4C6C5 F92945E8
2AFE9A95 2AD21793 50FF7987 F4A79079 6FE92AE5 66DFC8B8 14021984 0B1E3F6E
45D57889 B04883C5 114D79AD FBB2CAFF 587ECF9D

```

```

quit
crypto pki certificate chain SLA-TrustPoint certificate
ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D CBB4C798
212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520 1C394D78 462EF239
C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
license udi pid C9800-40-K9 sn TTM231803A3
memory free low-watermark processor 375973
!
service-template webauth-global-inactive
inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
diagnostic bootup level minimal
!
username <REMOVED> privilege 15 password 7 <REMOVED>
!
redundancy
mode sso
!
vlan internal allocation policy ascending
!
class-map match-any AVC-Reanchor-Class
match protocol cisco-jabber-audio
match protocol cisco-jabber-video
match protocol webex-media match
protocol webex-app-sharing

```



```

match protocol webex-control
match protocol webex-meeting
match protocol wifi-calling
!
interface Port-channel3 switchport
trunk native vlan 310
switchport trunk allowed vlan 310,400,500
!
interface TenGigabitEthernet0/0/0
switchport trunk native vlan 310 switchport
trunk allowed vlan 310,400,500 switchport
mode trunk
no negotiation auto
channel-group 3 mode active[SEP]
!
interface TenGigabitEthernet0/0/1
switchport trunk native vlan 310 switchport
trunk allowed vlan 310,400,500 switchport
mode trunk
no negotiation auto
channel-group 3 mode active[SEP]
!
interface TenGigabitEthernet0/0/2
switchport trunk native vlan 310 switchport
trunk allowed vlan 310,400,500 switchport
mode trunk
no negotiation auto
channel-group 3 mode active[SEP]
!
interface TenGigabitEthernet0/0/3
switchport trunk native vlan 310 switchport
trunk allowed vlan 310,400,500 switchport
mode trunk
no negotiation auto
channel-group 3 mode active[SEP]
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 10.201.81.25 255.255.255.240
negotiation auto
no cdp enable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan310
description Management
IP
ip address 10.201.81.9 255.255.255.240
!
interface Vlan400
description Data
ip address 10.201.82.14 255.255.255.0
ip helper-address 72.163.42.112
ip helper-address 173.37.137.70
!

```

```

interface Vlan500
  description Data
  ip address 10.201.83.14 255.255.255.0
  ip helper-address 72.163.42.112
  ip helper-address 173.37.137.70
  !
  ip default-gateway 10.201.81.1 ip
  forward-protocol nd
  !
  ip http server
  ip http authentication local
  ip http secure-server
  ip tftp source-interface GigabitEthernet0 ip
  tftp blocksize 8192
  ip route 0.0.0.0 0.0.0.0 10.201.81.1
  !
  radius-server attribute wireless accounting mac-delimiter hyphen radius-
  server attribute wireless accounting call-station-id macaddress radius-
  server attribute wireless accounting callStationIdCase lower radius-
  server attribute wireless authentication callStationIdCase lower radius-
  server attribute wireless authentication mac-delimiter hyphen
  radius-server attribute wireless authentication call-station-id ap-macaddress-ssid
  radius-server load-balance method least-outstanding
  !
  radius server RADIUS_SERVER_DAY0_1
  address ipv4 10.42.136.30 auth-port 1812 acct-port 1813
  key 7 <REMOVED>
  !
  radius server RADIUS_SERVER_DAY0_2
  address ipv4 10.42.3.31 auth-port 1812 acct-port 1813
  key 7 <REMOVED>
  !
  control-plane
  !
  line con 0
  exec-timeout 60 0
  stopbits 1
  line aux 0
  stopbits 1
  line vty 0 4
  transport input ssh
  line vty 5 15
  transport input ssh
  !
  ntp server 10.81.254.202
  ntp server 10.115.162.212
  !
  wireless mobility group member mac-address 6c31.0e7b.b8eb ip 10.201.81.10 public-ip 10.201.81.10 group CTG-
  VoWLAN3
  wireless mobility group name CTG-VoWLAN3
  wireless mobility mac-address 706d.153d.b50b wireless
  aaa policy default-aaa-policy
  wireless cts-sxp profile default-sxp-profile
  wireless management interface Vlan310
  wireless profile airtime-fairness default-atf-policy 0
  wireless profile flex default-flex-profile
  description "default flex profile"

```

```

wireless profile mesh default-mesh-profile
description "default mesh profile" wireless
profile policy Data
  ipv4 flow monitor wireless-avc-basic input
  ipv4 flow monitor wireless-avc-basic output
  service-policy input silver-up
  service-policy output silver
  session-timeout 86400
  vlan VLAN0400
  no shutdown
wireless profile policy Voice
  ipv4 flow monitor wireless-avc-basic input
  ipv4 flow monitor wireless-avc-basic output
  service-policy input platinum-up
  service-policy output platinum
  session-timeout 86400
  vlan VLAN0500
  no shutdown
wireless profile policy default-policy-profile description
  "default policy profile"
  vlan default
wireless tag site default-site-tag
description "default site tag" wireless
tag policy default-policy-tag
description "default policy-tag" wlan
Data policy Data
  wlan Voice policy Voice
wireless tag rf default-rf-tag
description "default RF tag"
wireless rf-network RCDN6-VoWLAN3
wireless security dot1x eapol-key retries 4
wireless security dot1x eapol-key timeout 400
no wireless security dot1x max-login-ignore-identity-response
wireless fabric control-plane default-control-plane
wireless media-stream multicast-direct
wireless multicast
wlan Data 2 data
  band-select
  ccx aironet-iesupport
  load-balance
  security dot1x authentication-list authentication_dot1x_day0 no
  shutdown
wlan Voice 1 voice
  no assisted-roaming neighbor-list no
  bss-transition
  ccx aironet-iesupport channel-
  scan defer-priority 4 dtim
  dot11 24ghz 2
  dtim dot11 5ghz 2
  media-stream multicast-direct
  radio dot11a
  security ft
  security wpa akm ft dot1x
  security dot1x authentication-list authentication_dot1x_day0
  wmm require
  no shutdown
ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh

```

```

coverage data rssi threshold -90
coverage level 2
coverage voice rssi threshold -90
description "pre configured Low Client Density rfprofile for 2.4gh radio"
high-density rx-sop threshold low
tx-power v1 threshold -65
ap dot11 24ghz rf-profile High_Client_Density_rf_24gh
description "pre configured High Client Density rfprofile for 2.4gh radio"
high-density rx-sop threshold medium
rate RATE_11M disable rate
RATE_12M mandatory rate
RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable tx-
power min 7
no shutdown
ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh
description "pre configured Typical Client Density rfprofile for 2.4gh radio" rate
RATE_11M disable
rate RATE_12M mandatory rate
RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable no
shutdown
ap dot11 24ghz media-stream multicast-direct ap
dot11 24ghz media-stream video-redirect
no ap dot11 24ghz cac voice tspec-inactivity-timeout
ap dot11 24ghz cac voice tspec-inactivity-timeout ignore
ap dot11 24ghz cac voice acm
ap dot11 24ghz edca-parameters optimized-video-voice ap
dot11 24ghz exp-bwreq
ap dot11 24ghz tsm
ap dot11 24ghz rrm txpower max 14
ap dot11 24ghz rrm txpower min 5
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable ap
dot11 24ghz rate RATE_5_5M disable ap
dot11 24ghz rate RATE_6M disable ap
dot11 24ghz rate RATE_9M disable
ap dot11 5ghz rf-profile Low_Client_Density_rf_5gh
coverage data rssi threshold -90
coverage level 2
coverage voice rssi threshold -90
description "pre configured Low Client Density rfprofile for 5gh radio"
high-density rx-sop threshold low
tx-power v1 threshold -60
no shutdown
ap dot11 5ghz rf-profile High_Client_Density_rf_5gh
description "pre configured High Client Density rfprofile for 5gh radio"
high-density rx-sop threshold medium
rate RATE_6M disable
rate RATE_9M disable

```

```

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

```

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

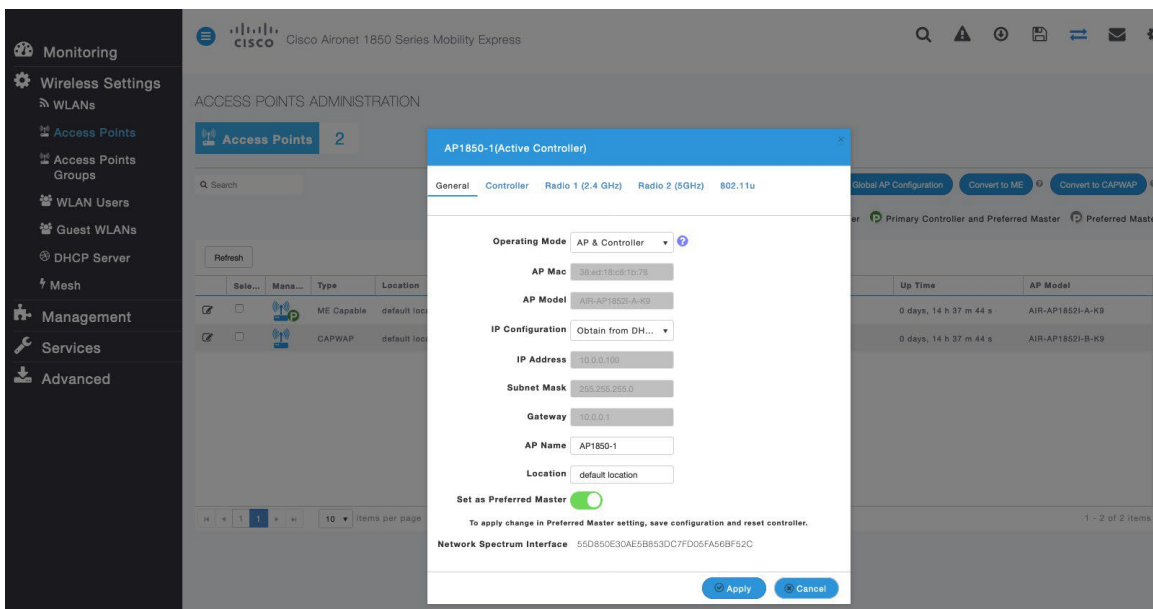
Cisco Mobility Express および Lightweight アクセスポイントを設定するときは、次のガイドラインを使用してください。

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

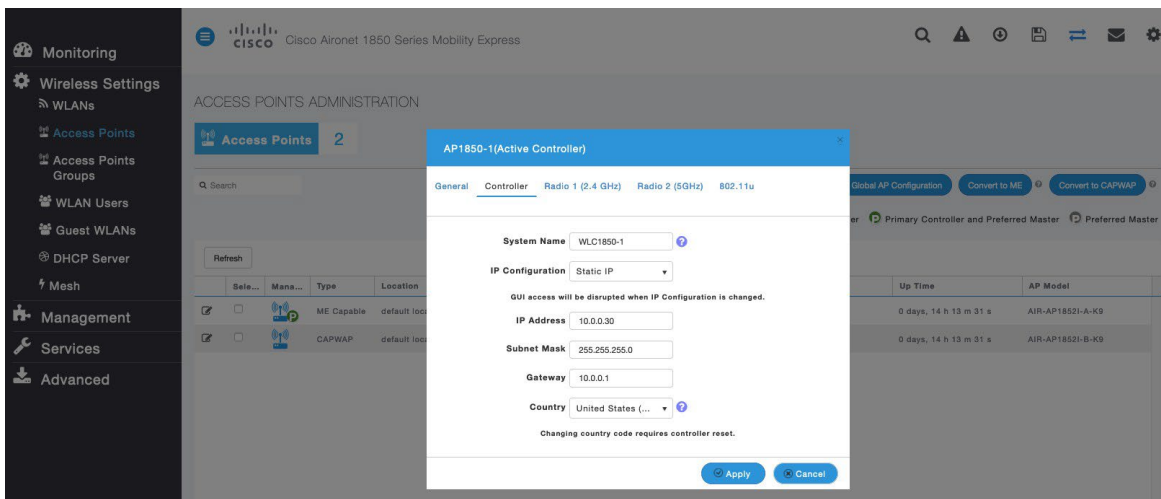
- [802.11v] が [無効 (Disabled)] になっていることを確認します
- [P2P (ピアツーピア) ブロッキング アクション (P2P (Peer to Peer) Blocking Action)] を無効にします
- [クライアントの帯域選択 (Client Band Select)] を [無効 (Disabled)] に設定します。
- [クライアントロードバランシング (Client Load Balancing)] を [無効 (Disabled)] に設定します。
- 必要に応じて [データレート (Data Rates)] を設定します。
- 必要に応じて [RF最適化 (RF Optimization)] を構成します
- [トラフィックタイプ (Traffic Type)] を [音声とデータ (Voice and Data)] に設定します
- CleanAir テクノロジーを搭載したCisco 製アクセス ポイントを使用している場合は、[CleanAir] を有効にします。
- 必要に応じて [マルチキャストダイレクト (Multicast Direct)] を構成します

コントローラの設定

[コントローラ (Controller)] 機能を含むように、1 つ以上の Mobility Express 対応アクセスポイントの [動作モード (Operating Mode)] を設定します。必要に応じて [AP名 (AP Name)] と [IP 設定 (IP settings)] を構成します。



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



802.11 ネットワークの設定

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

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

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

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

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

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

5 GHz

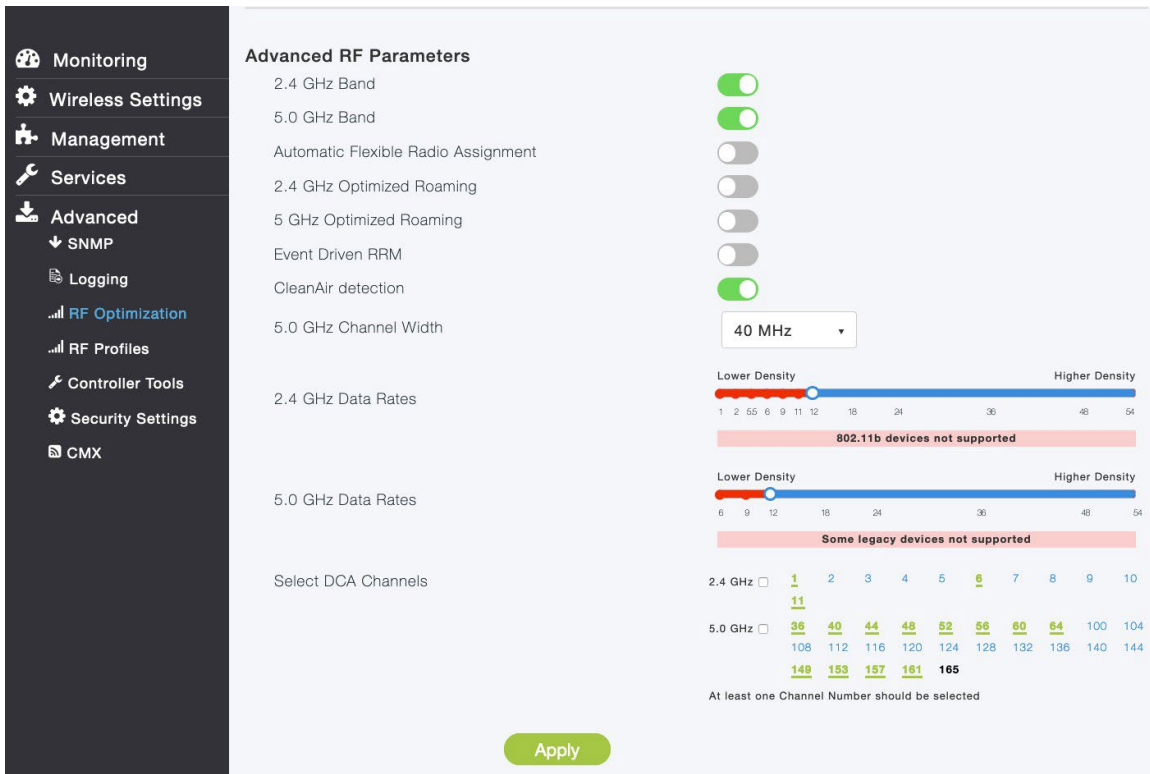
を使用する場合は、多数のチャンネルをスキャンするために発生するアクセスポイント検出の遅延の可能性を回避するためにチャンネルの数を制限できます（例：12 チャンネルのみ）。

Cisco 802.11n アクセスポイントを使用している場合は 5 GHz チャンネルの幅を 20 MHz または 40 MHz として構成でき、Cisco 802.11ac または 802.11ax アクセスポイントを使用している場合はチャンネルの幅を 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。

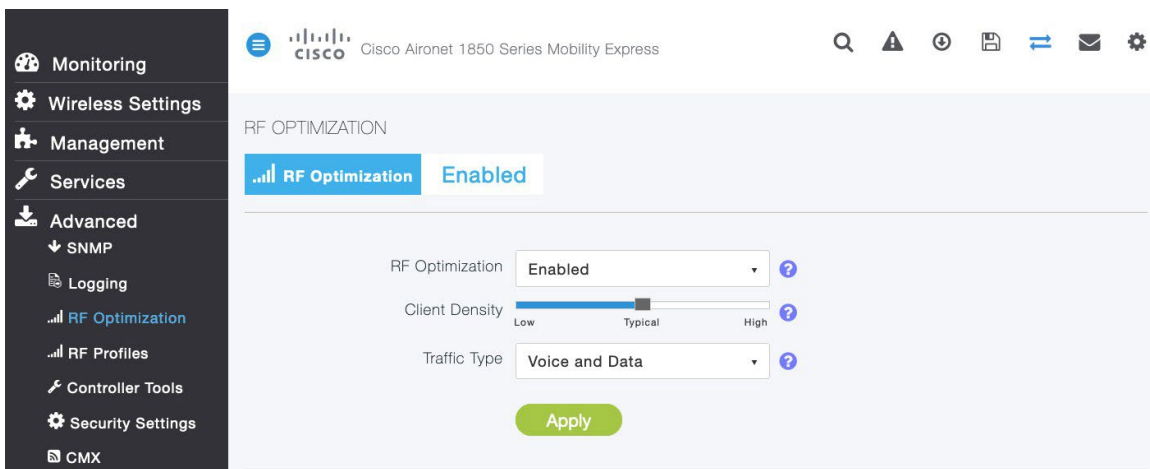
2.4 GHz を使用する場合、DCA リストではチャンネル 1、6、および 11 だけを有効にします。

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



RF 最適化

チャンネルと送信電力設定を管理するには、**[RF最適化 (RF Optimization)]** を有効にすることをお勧めします。**[トラフィックタイプ (Traffic Type)]** を **[音声とデータ (Voice and Data)]** に設定します。



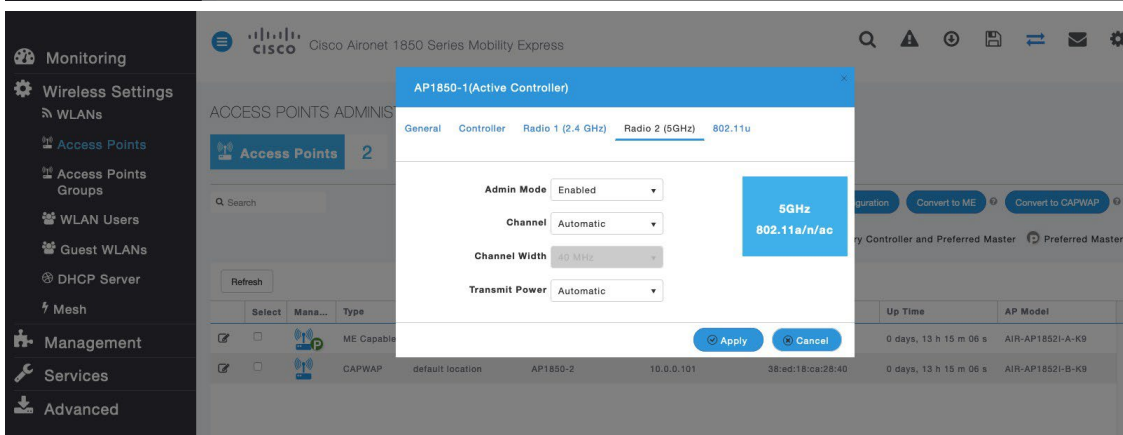
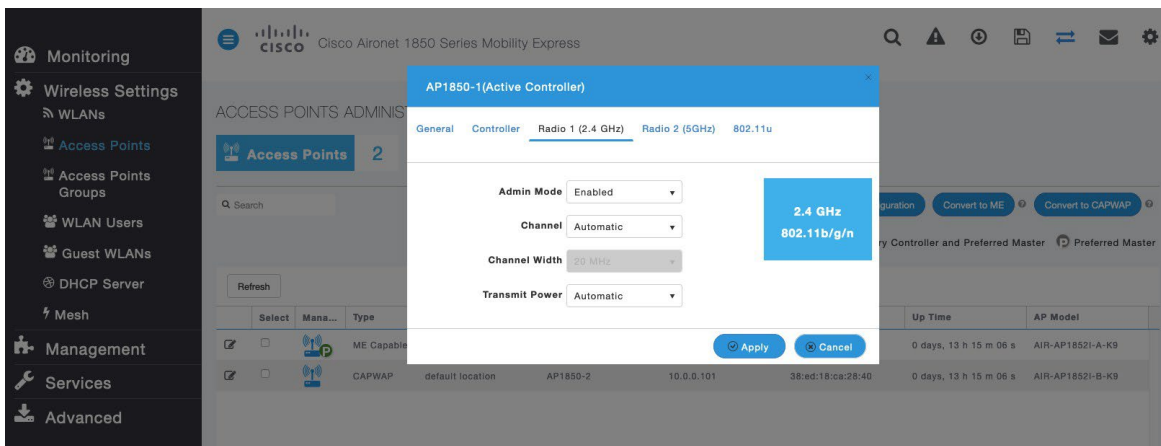
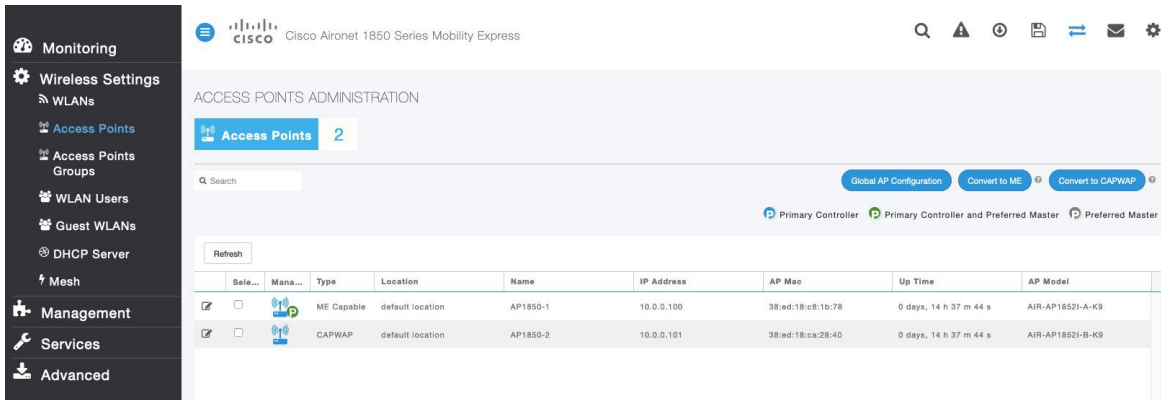
使用する周波数帯域に応じて 5 GHz または 2.4 GHz にチャンネルおよび送信電力をダイナミックに割り当てられるように、個々のアクセスポイントの設定をグローバル設定よりも優先させることができます。

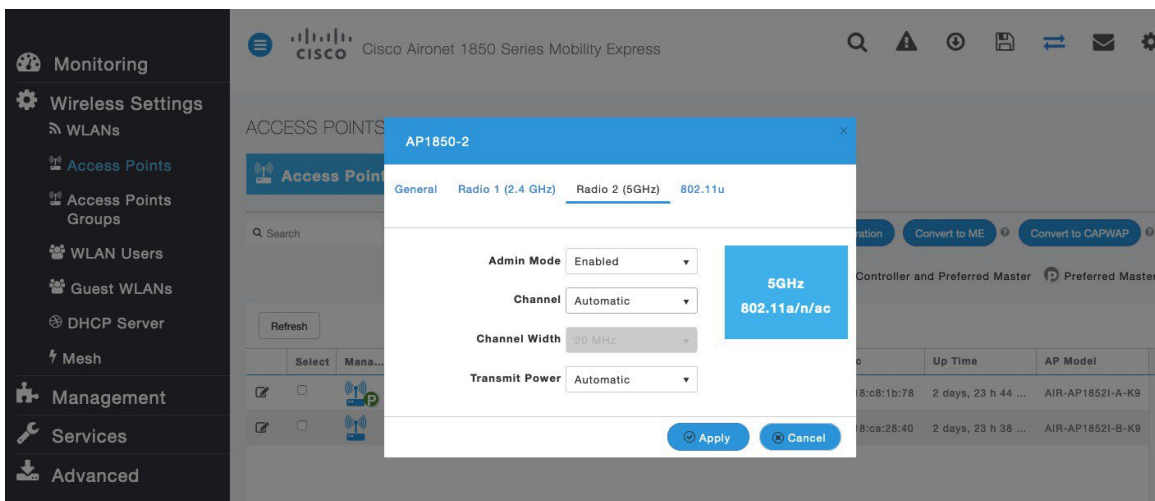
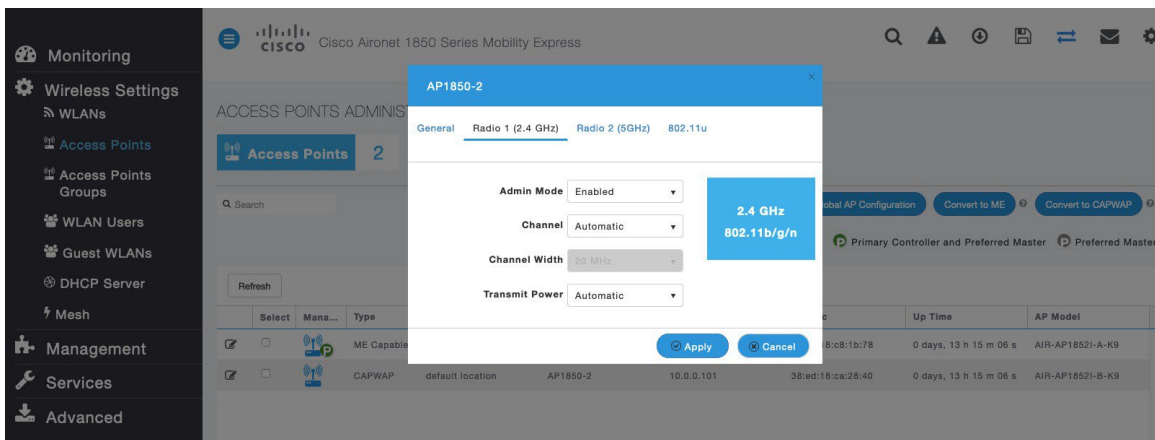
その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有効にできます。

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャンネルの幅を 20 MHz または 40 MHz として構成でき、Cisco 802.11ac または 802.11ax アクセス ポイントを使用している場合はチャンネルの幅を 20 MHz、40 MHz、または 80 MHz として構成できます。

チャンネルボンディングは、5 GHz を使用する場合にのみ使用することをお勧めします。
すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。





WLAN の設定

Cisco RoomOS Series には個別の SSID を使用することをお勧めします。

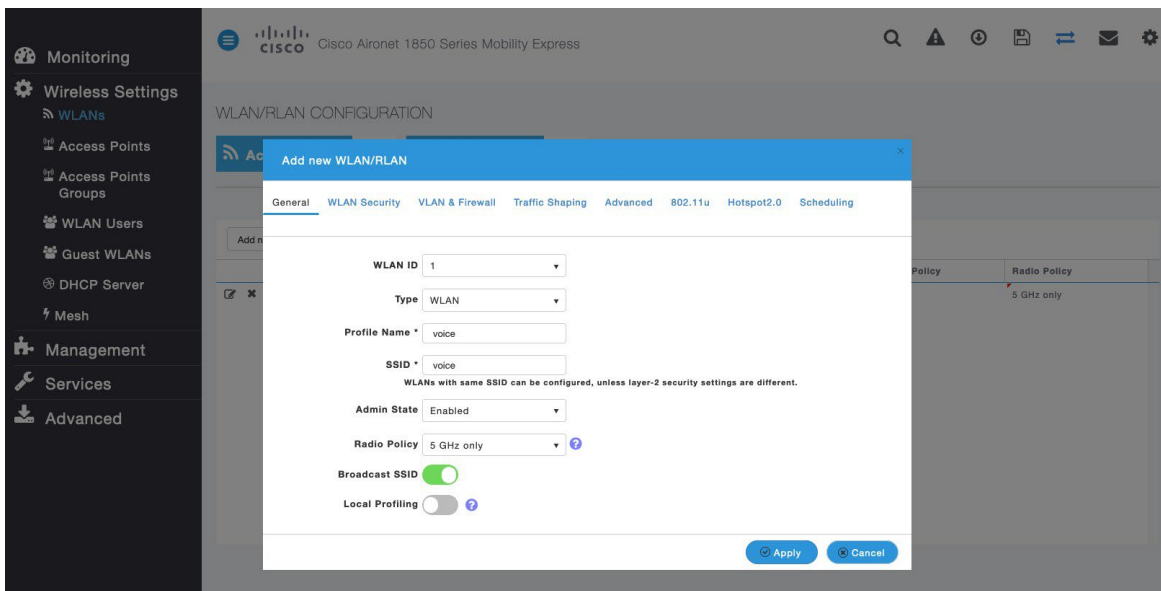
ただし、音声対応 Cisco Wireless LAN エンドポイントをサポートするように設定された既存の SSID がある場合、その WLAN を代わりに使用できます。

Cisco RoomOS Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように構成できます（5 GHz のみなど）。

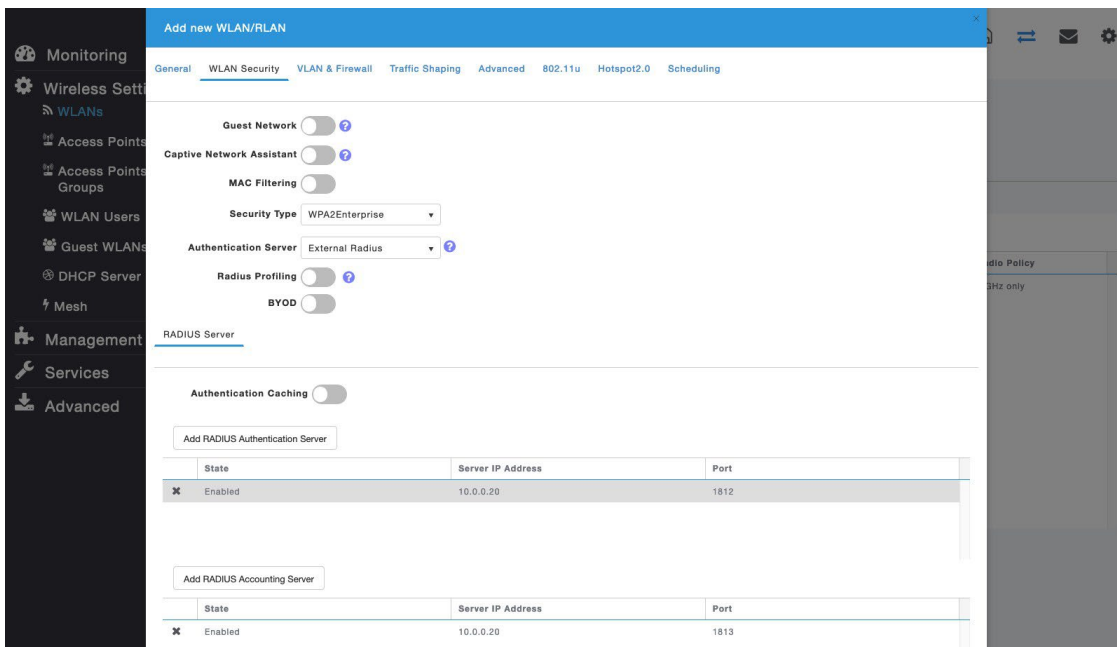
Cisco RoomOS Series は、5 GHz 帯域のみでの動作を推奨します。多数のチャンネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

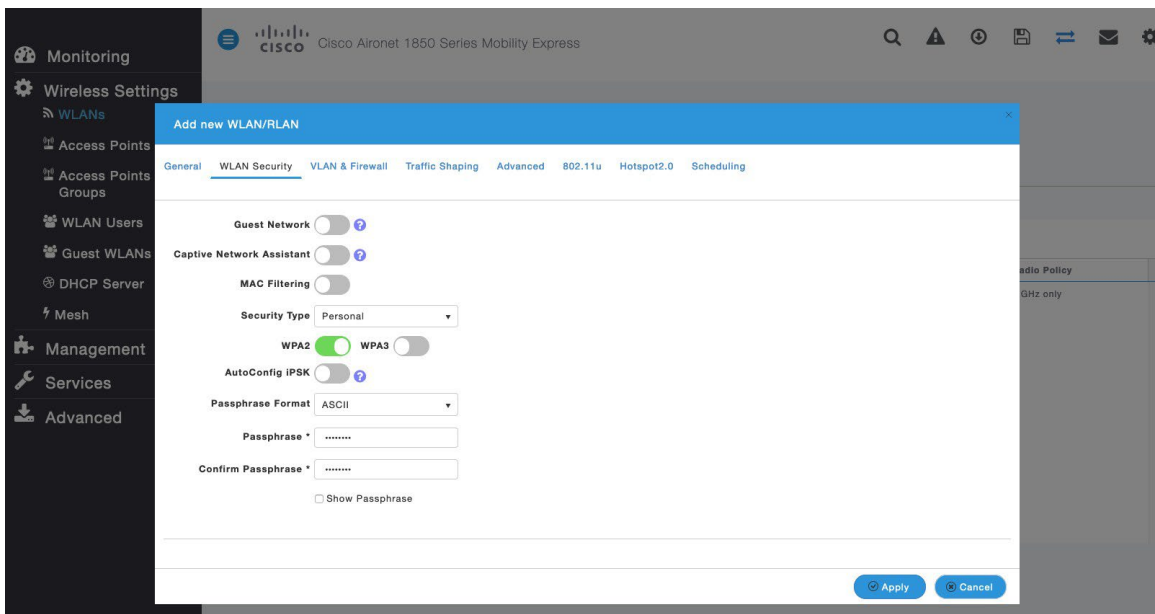
選択した SSID が他の LAN

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



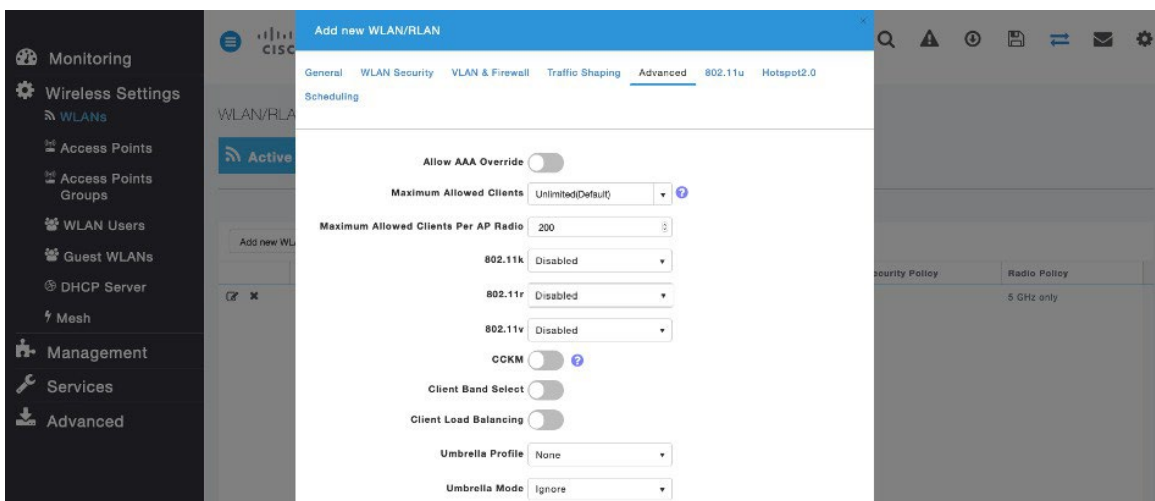
802.1x または PSK のどちらを使用するかに応じて、[セキュリティタイプ (Security Type)] を [WPA2Enterprise] または [パーソナル (Personal)] に設定します。



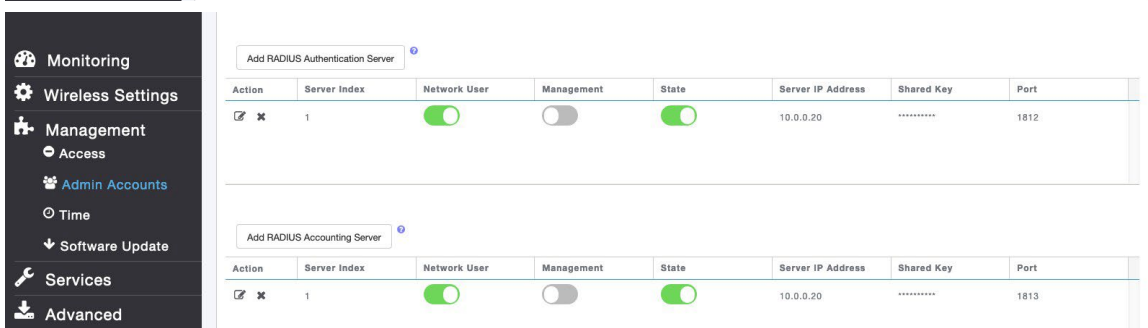
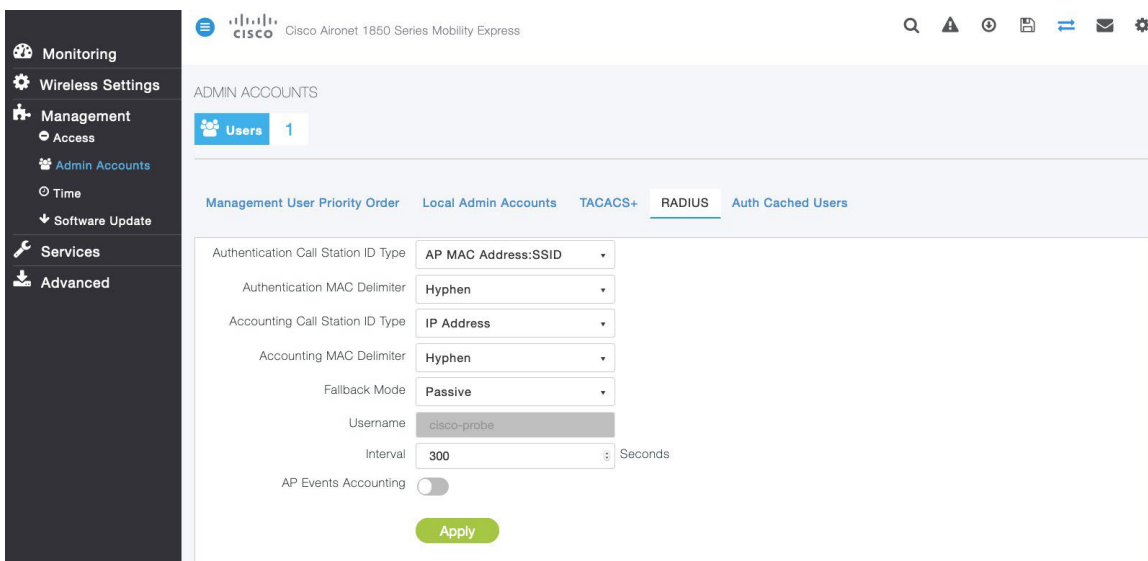
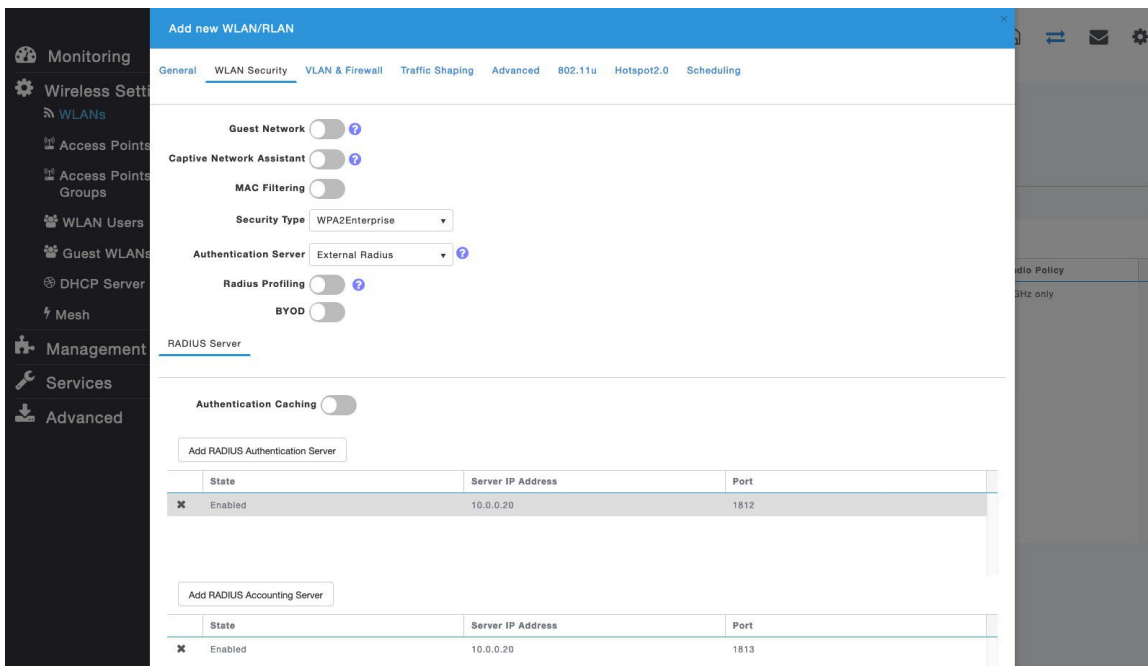


[クライアント帯域幅選択 (Client Band Select)] と [クライアントロードバランシング (Client Load Balancing)]

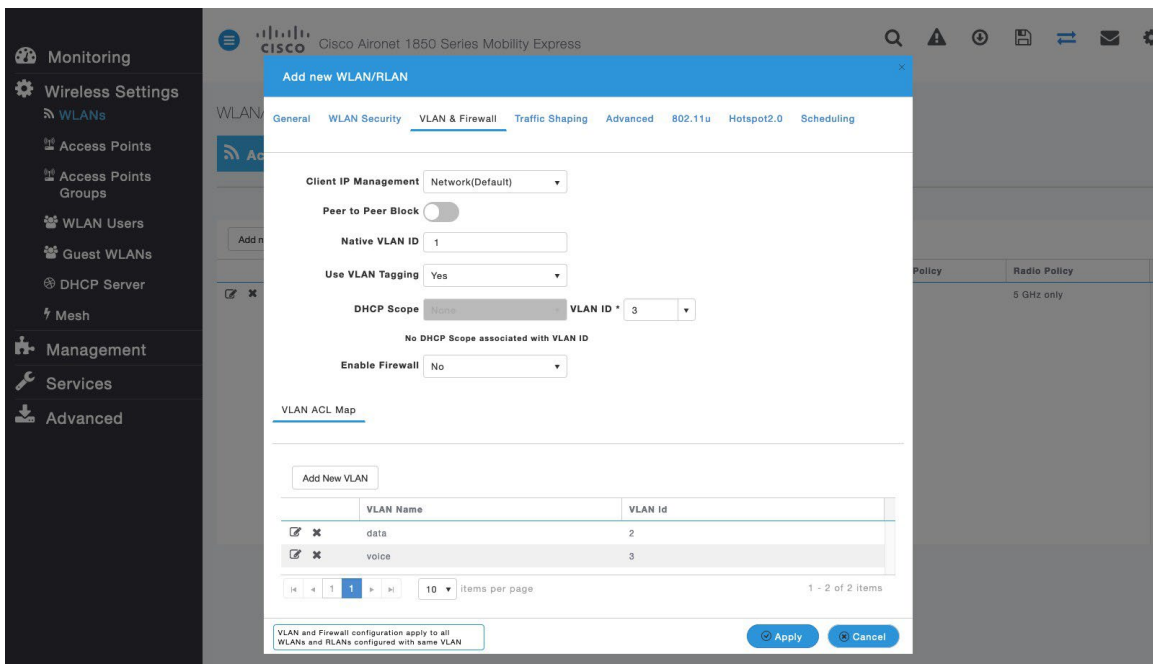
が無効になっていることを確認します。802.11k、802.11r、および802.11v はサポートされていないため、無効にする必要があります。



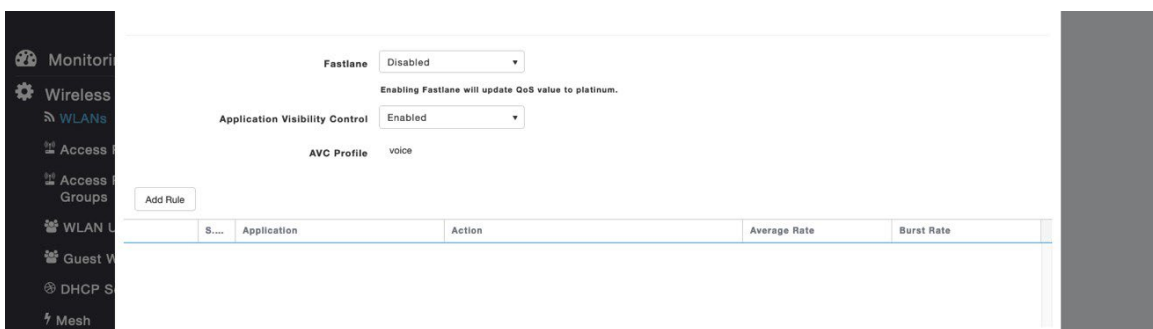
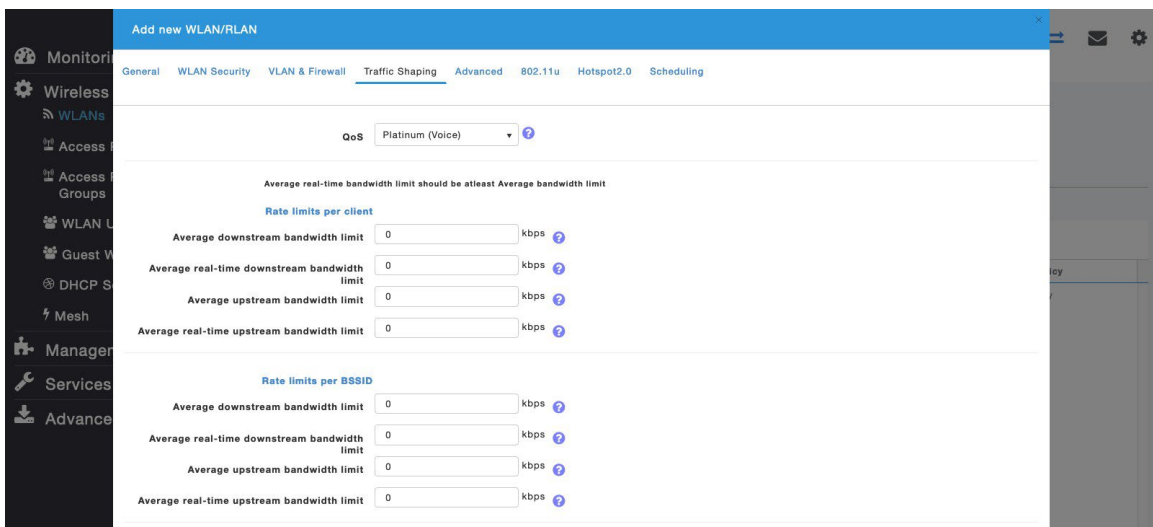
RADIUS 認証サーバーおよびアカウントサーバーは、WLAN レベルごとに設定して、グローバルリストを上書きできます。



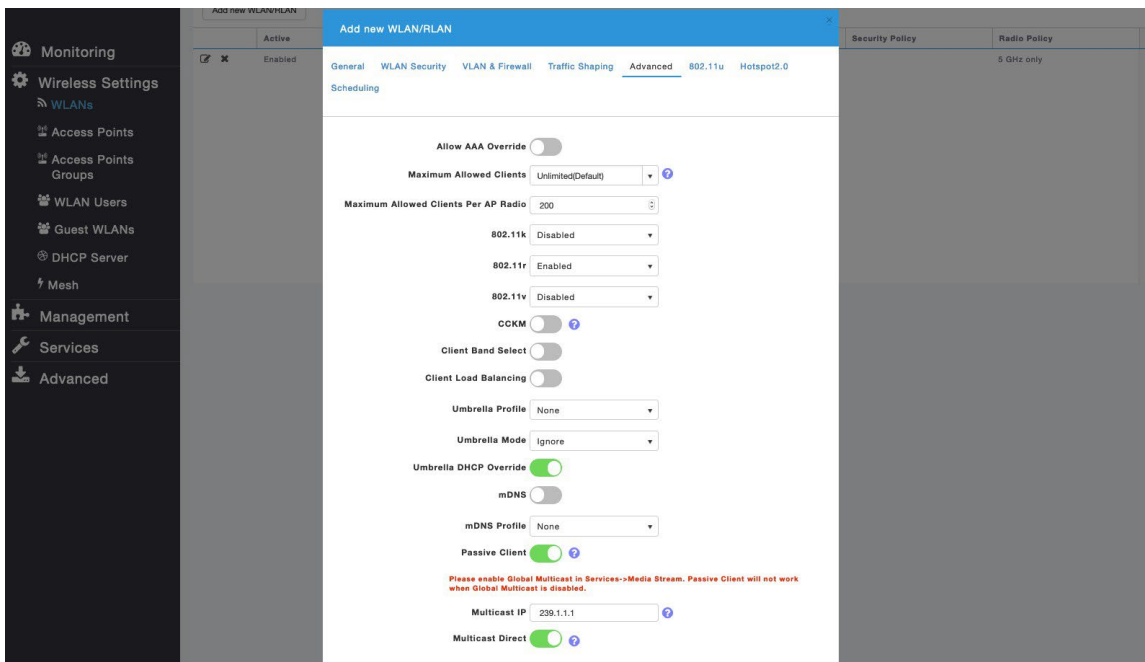
必要に応じて、WLAN の [ネイティブVLAN ID (Native VLAN ID)] と [VLAN ID] を構成します。[ピアツーピアブロック (Peer to Peer Block)] が無効になっていることを確認します。



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

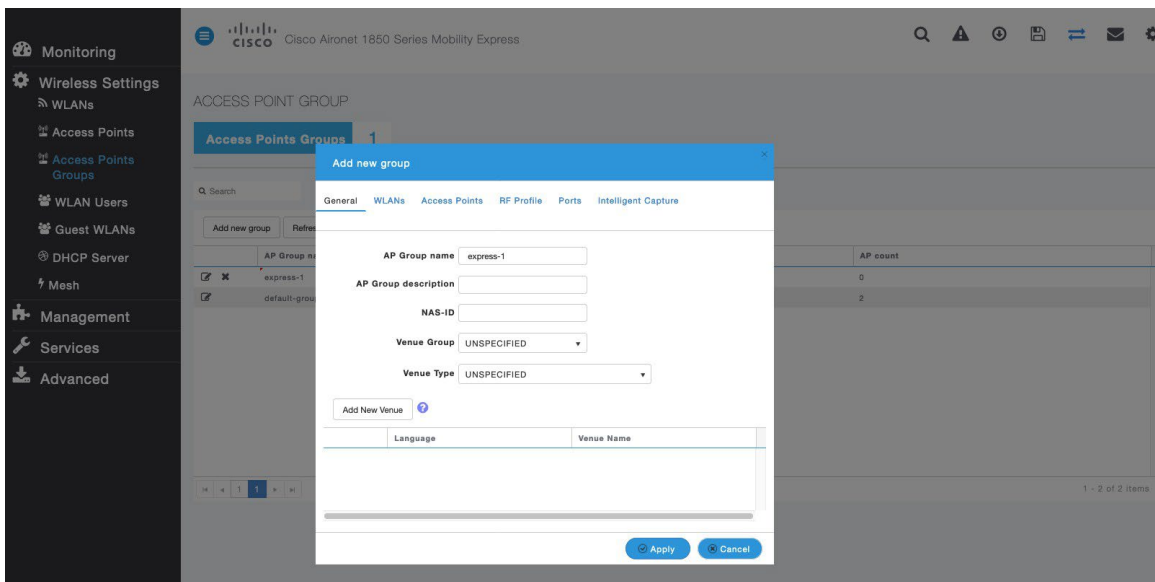


必要に応じて、[許可される最大クライアント数（Maximum Allowed Clients）] と [AP無線機ごとに許可される最大クライアント数（Maximum Allowed Clients Per AP Radio）] を設定できます。

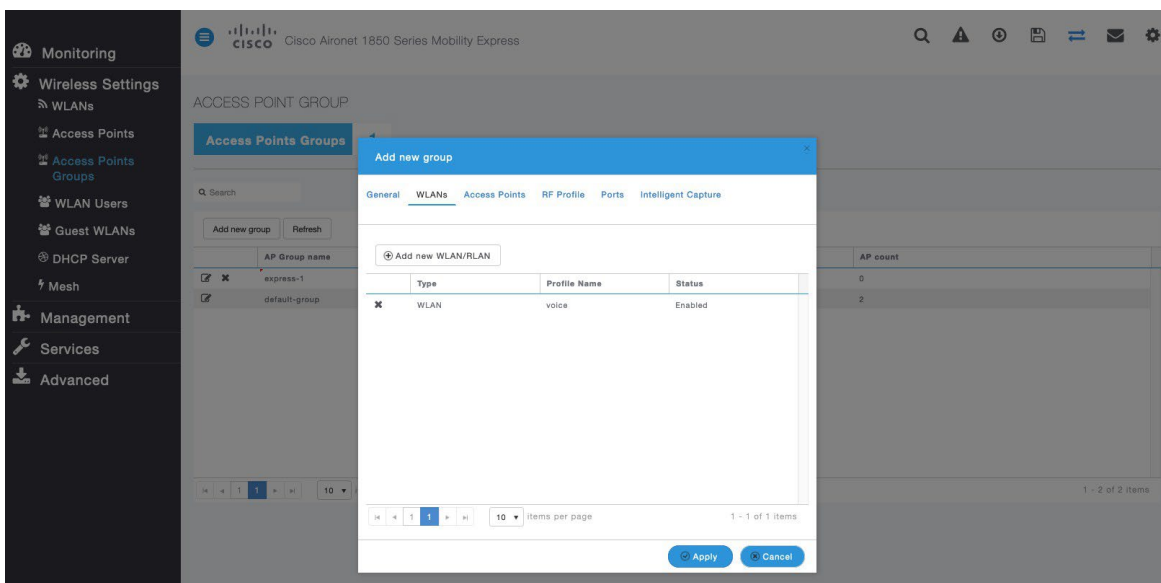
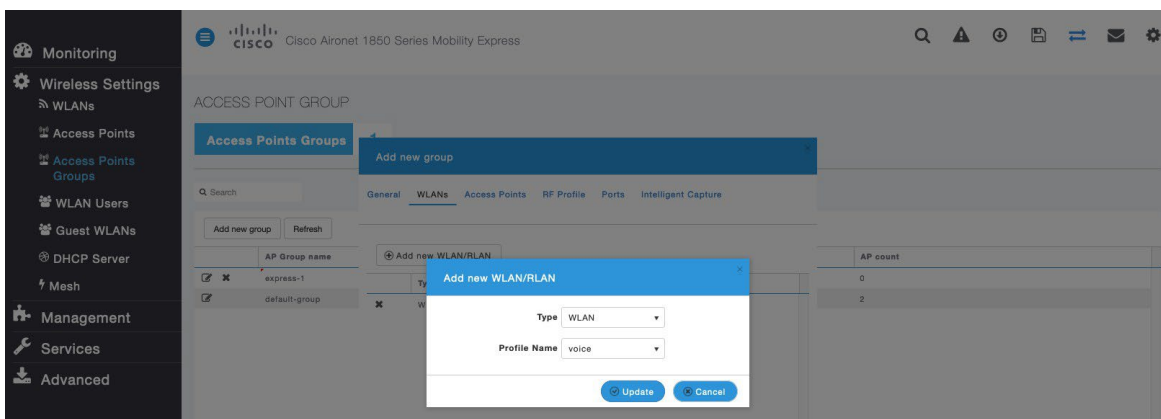


AP グループ

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

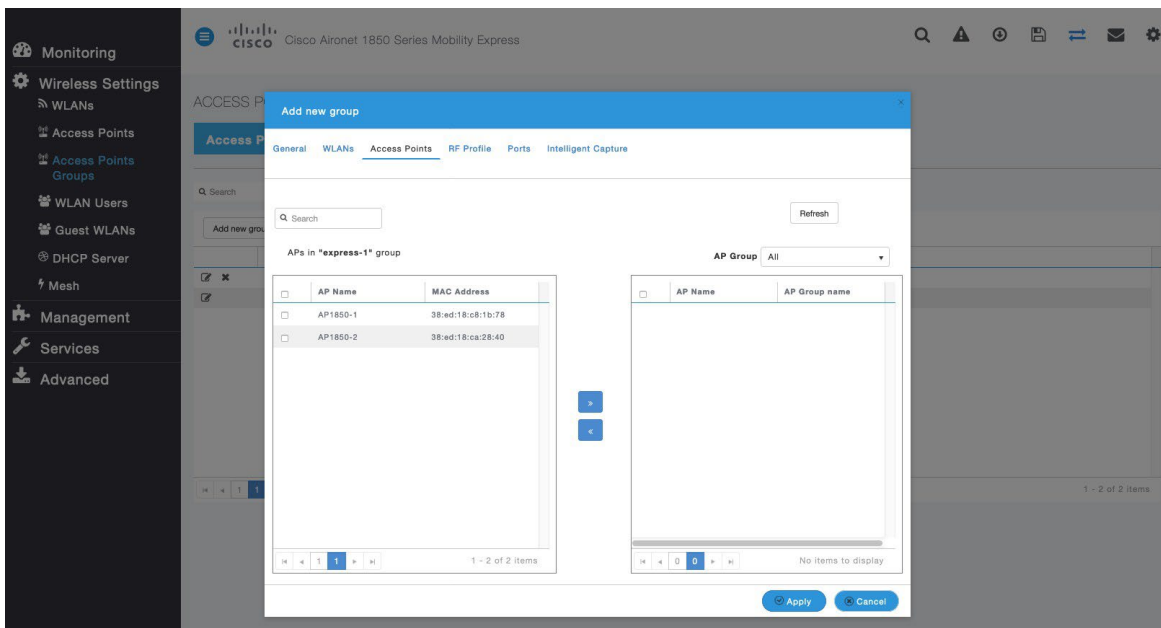


[WLAN (WLANs)] タブで、対象 WLAN と、マッピングするインターフェイスを選択して、[追加 (Add)] を選択します。

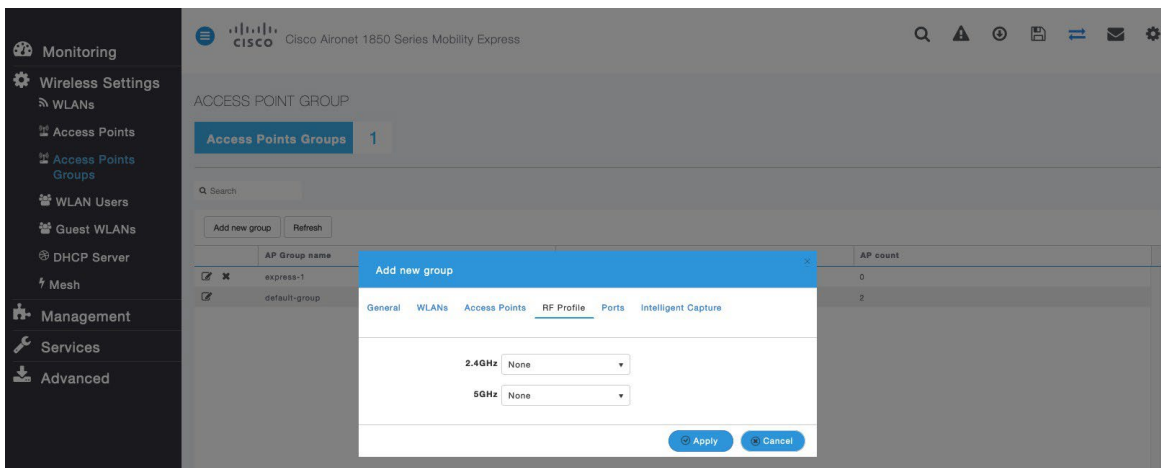


[アクセスポイント (Access Points)]

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



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



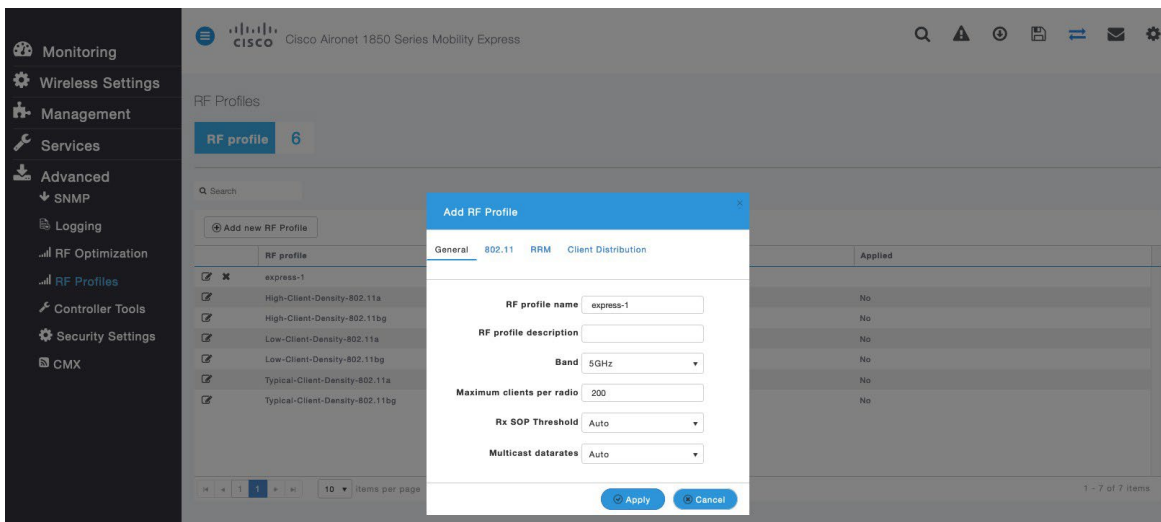
RFプロファイル

RF プロファイルを作成し、アクセス ポイントのグループが使用する必要がある周波数帯域、データ レート、RRM 設定などを指定できます。Cisco RoomOS Series で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。作成した RF プロファイルは、AP グループに適用されます。

RF プロファイルを作成する場合、[RF プロファイル名 (RF Profile Name)] と [無線ポリシー (Radio Policy)] を定義する必要があります。[無線ポリシー (Radio Policy)] に [5GHz] または [2.4GHz] を選択します。

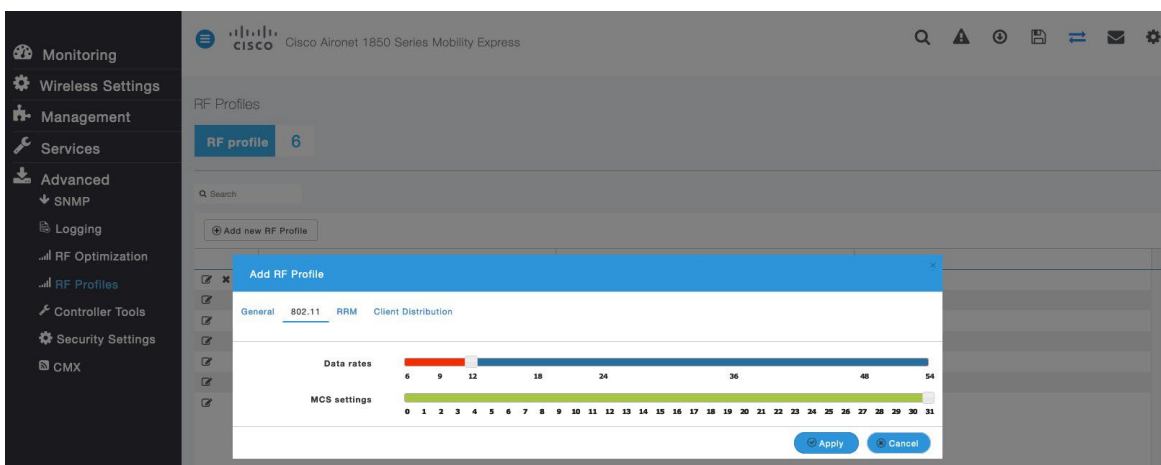
必要に応じて、[無線ごとの最大クライアント数 (Maximum clients per radio)]、[マルチキャスト

データ レート (Multicast Data Rates)]、および [Rx Sop のしきい値 (Rx Sop Threshold)]
を設定できます。 [Rx Sop のしきい値 (Rx Sop Threshold)]
にはデフォルト値 ([自動 (Auto)]) を使用することを推奨します。

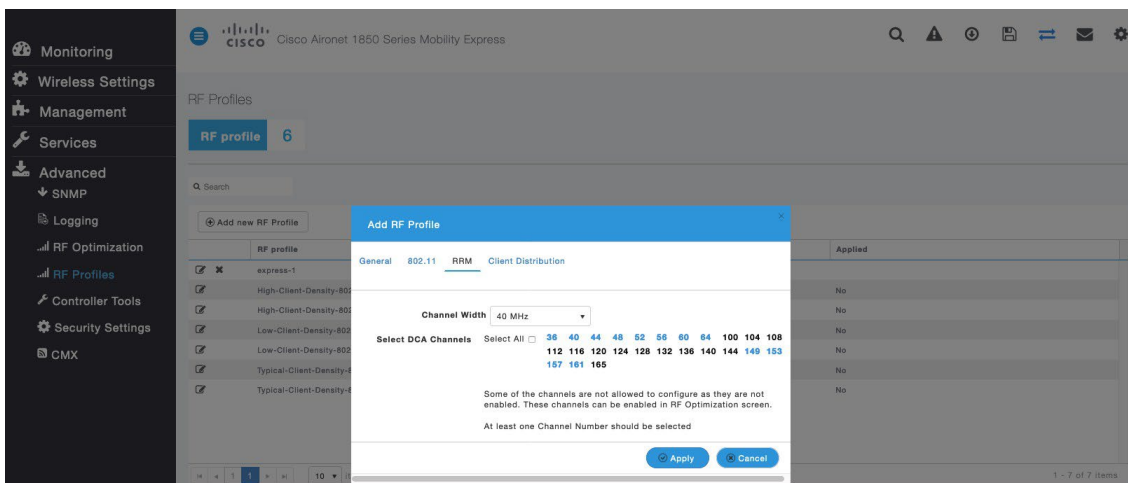


[802.11] タブで、必要に応じてデータ レートを設定します。

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

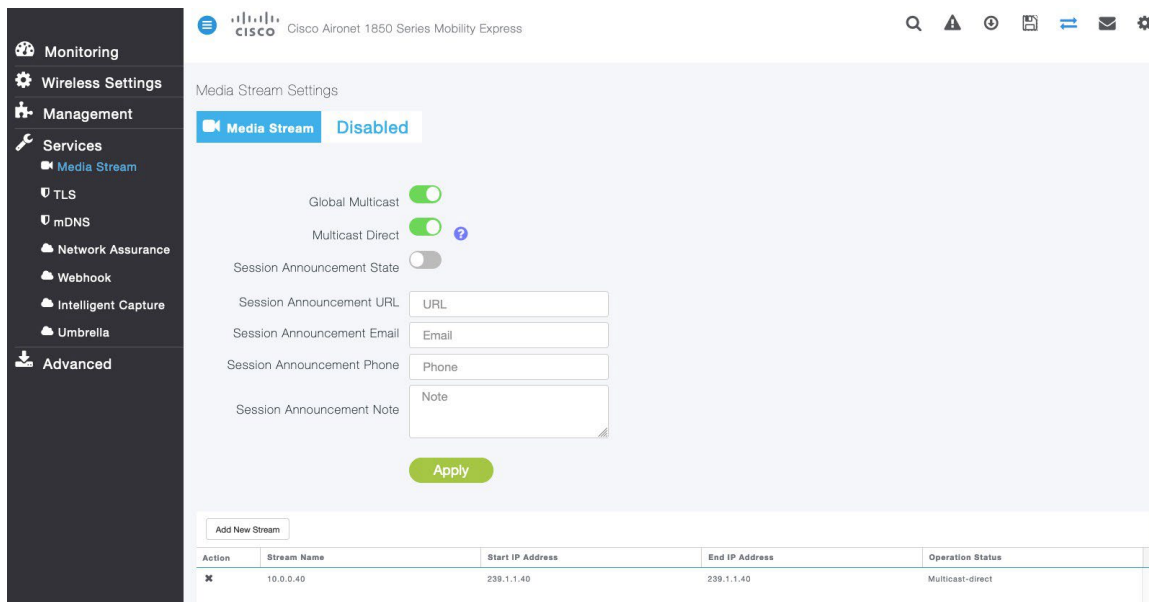


[RRM] タブでは、[チャンネル幅 (Channel Width)]設定と [DCA チャンネル (DCA Channels)]を構成できます。



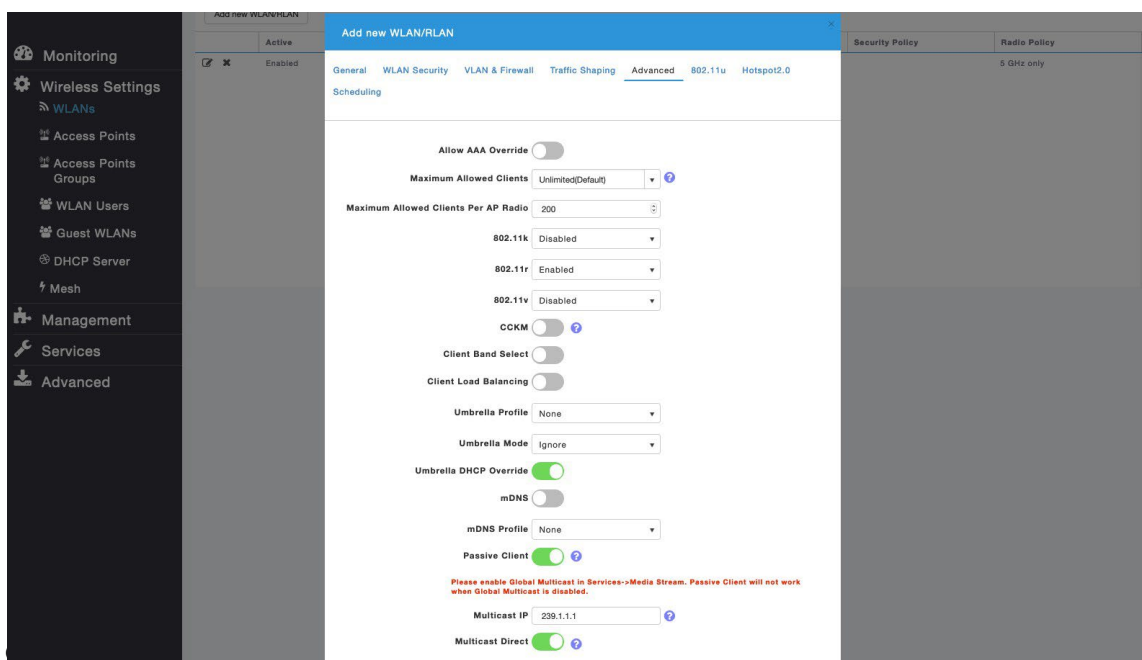
マルチキャスト ダイレクト

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



Action	Stream Name	Start IP Address	End IP Address	Operation Status
✖	10.0.0.40	239.1.1.40	239.1.1.40	Multicast-direct

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



Please enable Global Multicast in Services->Media Stream. Passive Client will not work when Global Multicast is disabled.

Multicast IP: 239.1.1.1

Multicast Direct:

Cisco Autonomous（自律）アクセスポイント

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

- **[802.11r (FT)]** と **[CCKM]** が必須として構成されていないことを確認します
- **[802.11k]** が **[無効 (Disabled)]** になっていることを確認します
- **[802.11v]** が **[無効 (Disabled)]** になっていることを確認します
- 必要に応じて **[データレート (Data Rates)]** を設定します。
- **[Quality of Service (QoS)]** を設定します。
- **[WMMポリシー (WMM Policy)]** を **[必須 (Required)]** に設定します
- **[Aironet拡張機能 (Aironet Extensions)]** が **[有効 (Enabled)]** になっていることを確認します。
- **[Public Secure Packet Forwarding (PSPF)]** を無効にします。
- **[IGMPスヌーピング (IGMP Snooping)]** を **[有効 (Enabled)]** に設定します。

802.11 ネットワークの設定

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

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

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

5 GHz

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

Cisco Autonomous アクセス

ポイントの場合、動的周波数選択（DFS）を選択して、自動チャンネル選択を使用します。DFS が有効にされている場合、少なくとも 1 つの帯域（帯域 1～4）を有効にします。

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

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャンネルの幅を 20 MHz または 40 MHz として構成でき、Cisco 802.11ac または 802.11ax アクセス ポイントを使用している場合はチャンネルの幅を 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)] で [Dot11d] を有効にし、適切な

[国コード (Country Code)]

を設定します。[Aironet拡張機能 (Aironet Extensions)] が

[有効 (Enabled)] になっていることを確認します。

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

Save Configuration Ping Logout Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

NETWORK

▼ NETWORK MAP
Summary
Adjacent Nodes

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

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

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

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

Enable Radio: Enable Disable

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

Role in Radio Network:

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

Max-Client: enable disable (1-255)

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

Data Rates:

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

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

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

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

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

DefaultRadio Channel: Channel 36 5180 MHz

Dynamic Frequency Selection Bands:
Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz
Band 4 - 5.725 to 5.825 GHz

Channel Width: 20 MHz

World Mode Multi-Domain Operation: Disable Legacy Dot11d

Country Code: Indoor Outdoor

Radio Preamble: Short Long

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

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

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

Traffic Stream Metrics: Enable Disable

Aironet Extensions: Enable Disable

Ethernet Encapsulation Transform: RFC1042 802.1H

Reliable Multicast to WGB: Disable Enable

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

Beacon Privacy Guest-Mode: Enable Disable

Beacon Period: (20-4000 Kusec) Data Beacon Rate (DTIM): (1-100)
Max. Data Retries: (1-128) RTS Max. Retries: (1-128)
Fragmentation Threshold: (256-2346) RTS Threshold: (0-2347)

Root Parent Timeout: (0-65535 sec)
Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)
Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)
Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)
Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)

2.4 GHz を使用する場合は、802.11b/g/nネットワークのステータスと 802.11g が有効に設定されていることを確認します。ワイヤレス LAN に接続する 802.11b のみのクライアントがない場合、必須（基本）レートとして 12 Mbps、サポート対象（任意）レートとして 18 Mbps を設定することをお勧めします。ただし、環境によっては、6 Mbps を必須（基本）レートとして有効にする必要があります。

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

WLAN の設定

Cisco RoomOS Series には個別の SSID を使用することをお勧めします。

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

Cisco RoomOS Series で使用する SSID は、特定の 802.11 無線タイプにのみ適用するように構成できます (802.11a のみなど)。

[WPA2] キー管理を有効にします。

The screenshot shows the Cisco RoomOS Security configuration interface for a Global SSID Manager. The page is titled "Security: Global SSID Manager" and is for Hostname "ap-1". The top navigation bar includes "HOME", "NETWORK", "ASSOCIATION", "WIRELESS", "SECURITY", "SERVICES", "MANAGEMENT", "SOFTWARE", and "EVENT LOG". The left sidebar lists various security features like "Admin Access", "Encryption Manager", "SSID Manager", etc. The main content area is divided into several sections:

- SSID Properties:** Contains a "Current SSID List" with entries for "data" and "voice". The "voice" SSID is selected. Fields for "SSID:" (voice), "VLAN:" (3), "Backup 1:", "Backup 2:", and "Backup 3:" are visible. There are also checkboxes for "Band-Select:", "Universal Admin Mode:", and "Interface:" (Radio1-802.11AC5GHz is selected).
- Client Authentication Settings:** Includes "Methods Accepted:" with checkboxes for "Open Authentication:" (checked, with EAP), "Web Authentication", "Web Pass", "Shared Authentication:", and "Network EAP:" (checked, < NO ADDITION >). It also has "Server Priorities:" for "EAP Authentication Servers" and "MAC Authentication Servers", each with "Use Defaults" selected and priority dropdowns set to "< NONE >".
- Client Authenticated Key Management:** Shows "Key Management:" set to "Mandatory", with checkboxes for "CCKM" (unchecked) and "Enable WPA" (checked, 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 Capabilites of this SSID

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

Enable IP Redirection on this SSID

IP Address:

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

Association Limit (optional): (1-255)

EAP Client (optional):
 Username: Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

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

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N2.4GHz:

Set Beacon Mode: Single BSSID Multiple BSSID

Set Single Guest Mode SSID:

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

Radio1-802.11AC5GHz:

Set Beacon Mode: Single BSSID Multiple BSSID

Set Single Guest Mode SSID:

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

ワイヤレス音声/データを別個の VLAN にセグメント化します。

音声 VLAN に対して、パブリック セキュア パケット

フォワーディング (PSPF) が有効になっている場合は、PSPF が無効になっていることを確認します。PSPF が有効になっている場合にクライアントが同じアクセス

ポイントに関連付けられると、直接通信できません。PSPF を有効にすると、オーディオは無指向となります。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

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](#)

< NEW >

VLAN 2

VLAN 3

VLAN 10

Delete

VLAN ID: (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N^{2.4GHz}

Radio1-802.11AC^{5GHz}

Management VLAN (If non-native)

Apply Cancel

VLAN Information

View Information for: VLAN 2

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

Refresh

暗号化タイプとして [AES] が選択されていることを確認します。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

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

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

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 3

Encryption Modes

None

WEP Encryption Optional

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

Cipher AES CCMP

Encryption Keys

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

Global Properties

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

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

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

The screenshot displays the Cisco RoomOS configuration interface for the Security > Server Manager > Global Properties section. The page shows settings for a Backup RADIUS Server, Corporate Servers, and Default Server Priorities.

Backup RADIUS Server

- IP Version: IPV4 IPV6
- Backup RADIUS Server Name:
- Backup RADIUS Server: (Hostname or IP Address)
- Shared Secret:

Corporate Servers

Current Server List

RADIUS

- < NEW >
- 10.0.0.20
- 10.9.0.9

IP Version: IPV4 IPV6

Server Name:

Server: (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): (0-65535)

Accounting Port (optional): (0-65535)

Default Server Priorities

EAP Authentication

Priority 1:

Priority 2:

Priority 3:

MAC Authentication

Priority 1:

Priority 2:

Priority 3:

Accounting

Priority 1:

Priority 2:

Priority 3:

Admin Authentication (RADIUS)

Priority 1:

Priority 2:

Priority 3:

Admin Authentication (TACACS+)

Priority 1:

Priority 2:

Priority 3:

無線ドメイン サービス (WDS)

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

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

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

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Wireless Services

WDS STATUS GENERAL SET-UP SERVER GROUPS

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

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

Use this AP as Wireless Domain Services

Wireless Domain Services Priority: 255 (1-255)

Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

Configure Wireless Network Manager

Wireless Network Manager Address: DISABLED (IP Address or Hostname)

Apply Cancel

Cisco Autonomous アクセス ポイントはマルチキャストプロトコルである Inter-Access Point Protocol (IAPP) を使用するため、専用のネイティブ VLAN を使用する必要があります。ネイティブ VLAN については、IAPP パケットが正常に交換されるためにも、VLAN 1 は使用しないことを推奨します。Cisco Autonomous アクセス ポイントが直接接続しているスイッチポートでは、ポートセキュリティを無効にする必要があります。

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

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: < NEW > VLAN 2 VLAN 3 **VLAN 10** Delete

Create VLAN [Define SSIDs](#)

VLAN ID: 10 (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N2.4GHz

Radio1-802.11AC5GHz

Management VLAN (If non-native)

Apply Cancel

VLAN Information

View Information for: VLAN 2

	GigabitEthernet Packets	Radio0-802.11N2.4GHz Packets	Radio1-802.11AC5GHz Packets
Received	65884		65884
Transmitted	5462		5462

Refresh

無線ドメインサービス用のサーバグループを定義する必要があります。
最初に、インフラストラクチャ認証に使用するサーバグループを定義します。

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

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

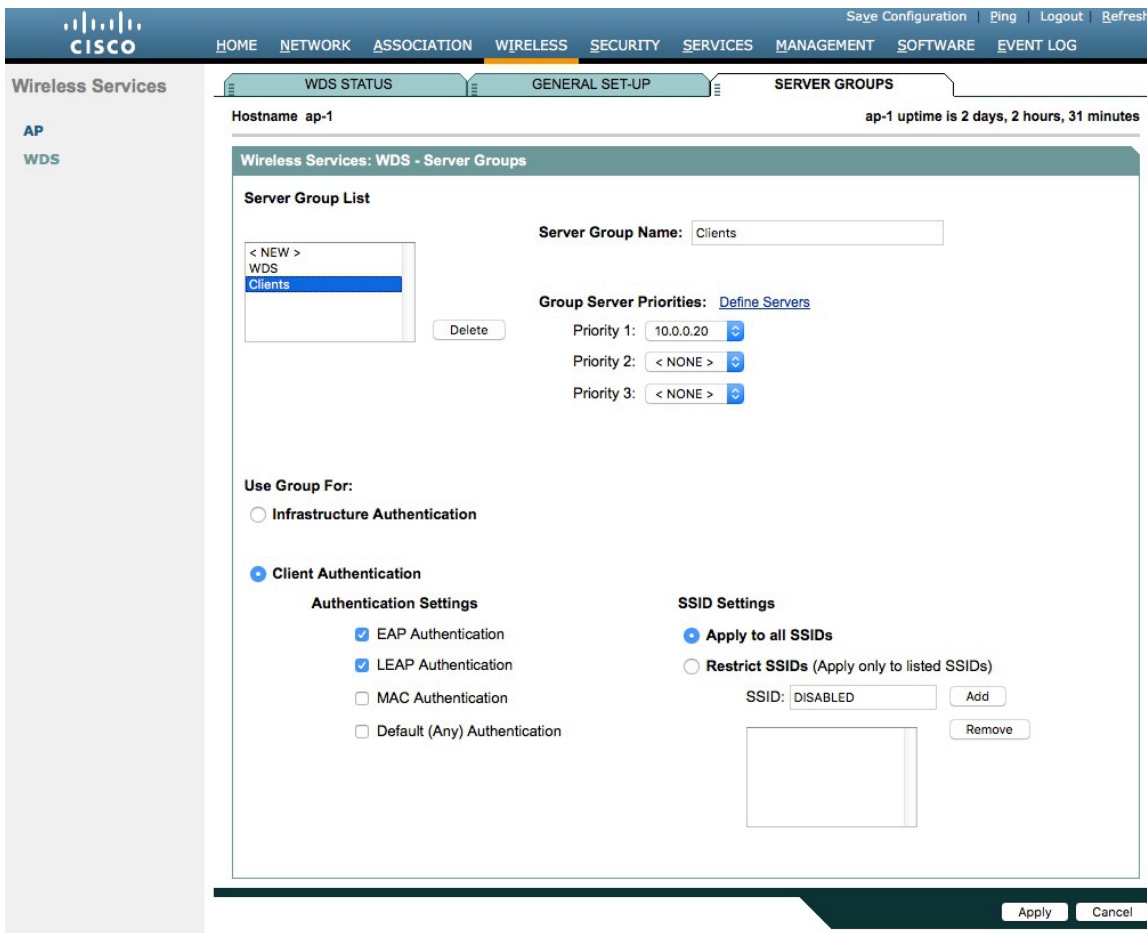
The screenshot shows the Cisco RoomOS DX Series configuration interface for WDS Server Groups. The top navigation bar includes 'HOME', 'NETWORK', 'ASSOCIATION', 'WIRELESS', 'SECURITY', 'SERVICES', 'MANAGEMENT', 'SOFTWARE', and 'EVENT LOG'. The 'WIRELESS' tab is selected, and the 'SERVER GROUPS' sub-tab is active. The hostname is 'ap-1' and the uptime is '1 day, 4 hours, 51 minutes'. The main content area is titled 'Wireless Services: WDS - Server Groups' and contains the following sections:

- Server Group List:** A list with a '< NEW >' button and a 'Delete' button. The 'WDS' group is selected.
- Server Group Name:** A text input field containing 'WDS'.
- Group Server Priorities:** A link 'Define Servers' and three priority dropdown menus: Priority 1 (10.9.0.9), Priority 2 (< NONE >), and Priority 3 (< NONE >).
- Use Group For:** Radio buttons for 'Infrastructure Authentication' (selected) and 'Client Authentication'.
- Authentication Settings:** Checkboxes for 'EAP Authentication', 'LEAP Authentication', 'MAC Authentication', and 'Default (Any) Authentication'.
- SSID Settings:** Radio buttons for 'Apply to all SSIDs' (selected) and 'Restrict SSIDs (Apply only to listed SSIDs)'. Below is an 'SSID' input field with 'DISABLED' and 'Add'/'Remove' buttons.

At the bottom right, there are 'Apply' and 'Cancel' buttons.

次に、クライアント認証に使用するサーバグループを定義します。

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



インフラストラクチャ認証にローカル RADIUS

を使用する場合は、すべての認証プロトコルを有効にします。ローカルアクセスポイント用のネットワーク アクセス サーバー エントリを作成します。

無線ドメイン サービスが有効になっているアクセス ポイントに対して認証を行うようにアクセス ポイントが設定されるユーザ アカウントを定義します。

無線ドメイン サービスに参加する各アクセス ポイント上でローカル RADIUS を設定します。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

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

STATISTICS GENERAL SET-UP EAP-FAST SET-UP

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

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols: EAP FAST
 LEAP
 MAC

Apply Cancel

Network Access Servers (AAA Clients)

Current Network Access Servers

< NEW >
10.9.0.9

Delete

Network Access Server: 10.9.0.9 (IP Address)

Shared Secret:

Apply Cancel

Individual Users

Current Users

< NEW >
wds

Delete

Username: wds

Password: Text NT Hash

Confirm Password:

Group Name: < NONE >

MAC Authentication Only

Apply Cancel

User Groups

Current User Groups

< NEW >

Delete

Group Name:

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

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

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

VLAN ID (optional):

SSID (optional): Add

..... Delete

Apply Cancel

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

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

単一の WDS サーバを使用する場合は、その WDS サーバの IP

アドレスを指定できます。そうでない場合は、**[自動検出 (Auto Discovery)]** を有効にします。WDS
サーバに対する認証に使用する **[ユーザ名 (Username)]** と **[パスワード (Password)]** を入力します。

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Wireless Services

AP
WDS

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

Wireless Services: AP

Participate in SWAN Infrastructure: Enable Disable

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

Username:

Password:

Confirm Password:

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

Apply Cancel

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

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Wireless Services

AP
WDS

WDS STATUS GENERAL SET-UP SERVER GROUPS

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

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

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

WDS Registration

APs: 1 Mobile Nodes: 0

AP Information

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

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

Wireless Network Manager Information

IP Address	Authentication Status

Refresh

コールアドミッション制御 (CAC)

Cisco Autonomous アクセスポイントには、負荷ベースのCACと複数ストリームのサポートは存在しないので、Cisco Autonomous アクセスポイントでCACを有効にすることは推奨されません。

Cisco Autonomous アクセスポイントは、1

ストリームのみに対応しており、ストリームサイズはカスタマイズできないので、CAC が有効である場合に SRTP および Barge（割り込み）、サイレントモニタリング、コール録音は機能しません。

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

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

Services: QoS Policies - Access Category

Access Category Definition

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

Optimized Voice WFA Default Apply Cancel

Admission Control for Video and Voice

Video(CoS 4-5)
 Admission Control

Voice(CoS 6-7)
 Admission Control

Max Channel Capacity (%): 75

Roam Channel Capacity (%): 6

Apply Cancel

QoS ポリシー

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

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

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

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

QoS POLICIES

RADIO0-802.11N2.4GHZ ACCESS CATEGORIES

RADIO1-802.11AC5GHZ 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	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz	GigabitEthernet0
Incoming		Data	Data
Outgoing		Data	Data
VLAN 3	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz	GigabitEthernet0
Incoming		Voice	Voice
Outgoing		< NONE >	< NONE >
VLAN 10	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz	GigabitEthernet0
Incoming		< NONE >	< NONE >
Outgoing		< NONE >	< NONE >

Apply Cancel

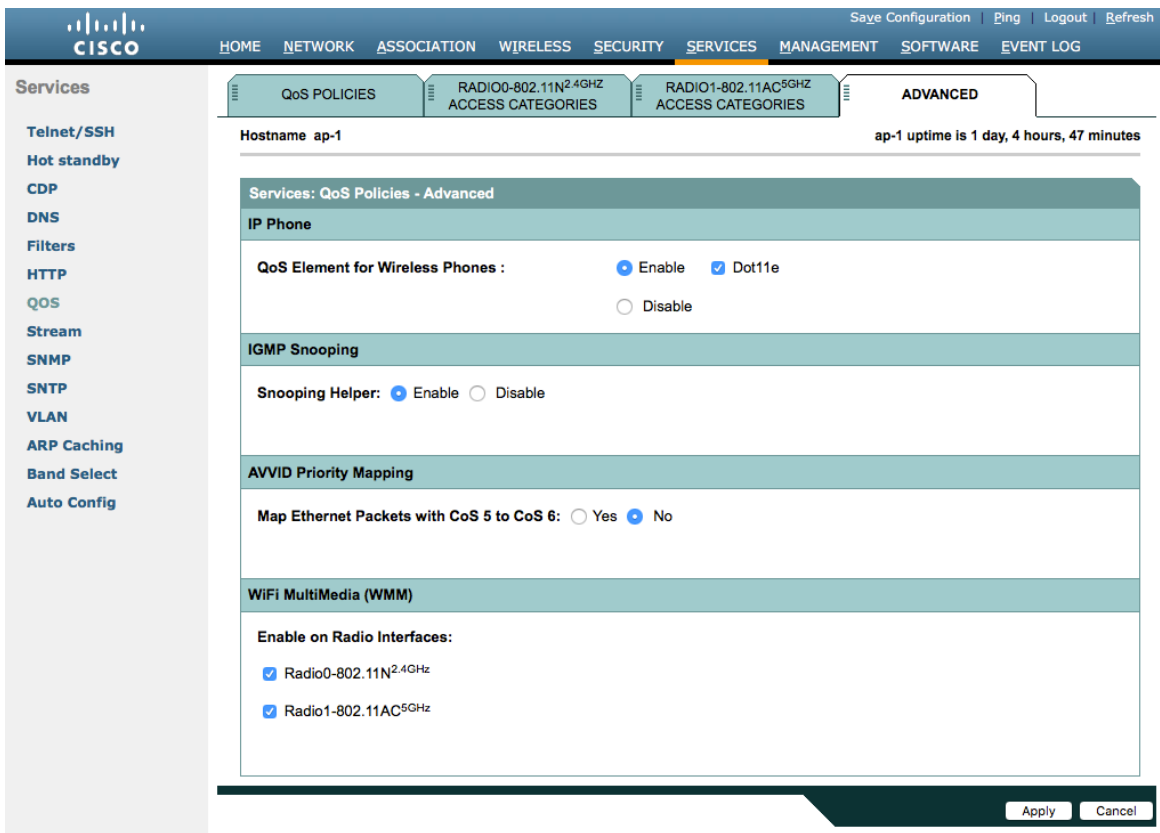
QBSS を有効にするには、[有効 (Enable)] を選択し、[Dot11e] をオンにします。

[Dot11e] をオンにすると、両方の CCA バージョン (802.11e およびシスコバージョン

2) が有効になります。[IGMPスヌーピング (IGMP Snooping)]

が有効になっていることを確認します。

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



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

ストリーム機能を有効にする場合は、音声パケットのみが音声キューに追加されることを確認します。シグナリングパケットは、別個のキューに追加する必要があります。SIP を別個のキューに入れるには、DSCP を適切なキューにマッピングする QoS ポリシーを設定します。

Services: Stream

Packet Handling per User Priority:

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

Low Latency Packet Rates:

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

Buttons: Apply, Cancel

電源管理

プロキシ ARP は、デバイスに代わって ARP

要求に応答するのに役立ちます。プロキシ ARP

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

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

Services: ARP Caching

Client ARP Caching: Enable Disable

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

Buttons: Apply, Cancel

サンプル構成

```
version 15.3 no
service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap-1
!
logging rate-limit console 9
!
aaa new-model
!
aaa group server radius rad_eap
server name 10.0.0.20
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
server name 10.0.0.20
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius WDS
server name 10.9.0.9
!
aaa group server radius Clients
server name 10.0.0.20
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap aaa
authentication login mac_methods local
aaa authentication login method_WDS group WDS aaa
authentication login method_Clients group Clients aaa
authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
clock timezone -0500 -5 0
clock summer-time -0400 recurring no
ip source-route
no ip cef
ip domain name cisco.com
ip name-server 10.0.0.30
ip name-server 10.0.0.31
!
dot11 pause-time 100
dot11 syslog
!
dot11 ssid data
```

```

vlan 2
authentication open eap eap_methods authentication
network-eap eap_methods authentication key-
management wpa version 2
!
dot11 ssid voice
vlan 3
authentication open eap eap_methods authentication
network-eap eap_methods authentication key-
management wpa version 2
!
dot11 arp-cache optional
dot11 phone dot11e
!
no ipv6 cef
!
crypto pki trustpoint TP-self-signed-672874324
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-672874324
revocation-check none
rsa keypair TP-self-signed-672874324
!
crypto pki certificate chain TP-self-signed-672874324 certificate
self-signed 01
30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 36373238 37343332 34301E17 0D313630 38303332 33303533
385A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3637 32383734
33323430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 CB155DD1
3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9 5F5A1B75
7910F9F5 6E9EDEF4 730942C7 17DC4CBC E5AE3E49 0AF79419 0BEF34BC
5DCEB4E2 FF2978CB C34D5AEE ED1DFB58 C7BF6592 61C1AD25 3EF87205 15EA58C2
0A5E2B15 7F08FAEA 5DA2BFA7 95E56C60 22C229C7 024A91D7 A4FEB50B 5425357F
02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
23041830 168014FC 2FE6CF0E E0380A40 11381459 5D596E3E A684DA30 1D060355
1D0E0416 0414FC2F E6CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
4886F70D 01010505 00038181 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
A8B174BC A46EB56A 857166C3 B9FD71DF 7264F5AF DC804A67 16BD35A2 4F39AFD7
0BD24F71 BAF916AC E984343C A54B7395 E5D15237 8897D436 A150BFB2 DC23E8D3
AFF0A51C B6253153 C4E2C022 66F1E361 B2EE49E2 763FCBC7 6381E7F7 61B6E14D
60CDF947 2C044617 37211E5F CE
quit
username <REMOVED> privilege 15 password 7 <REMOVED>
!
class-map match-all _class_Voice0 match
ip dscp cs3
class-map match-all _class_Voice1 match
ip dscp af41
class-map match-all _class_Voice2 match
ip dscp cs4
class-map match-all _class_Voice3 match
ip dscp ef
!
policy-map Voice
class _class_Voice0
set cos 4

```

```

class _class_Voice1
  set cos 5
class _class_Voice2
  set cos 5
class _class_Voice3
  set cos 6
policy-map Data
class class-default
  set cos 0
!
bridge irb
!
interface Dot11Radio0
  no ip address
  shutdown
  antenna gain 0
  traffic-metrics aggregate-report
  stbc
  mbssid
  speed basic-12.0 18.0 24.0 36.0 48.0 54.0 m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m14. m15.
  m16. m17. m18. m19. m20. m21. m22. m23.
  power client local
  channel 2412
  station-role root
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 spanning-disabled
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
  no ip address
  !
  encryption vlan 2 mode ciphers aes-ccm
  !
  encryption vlan 3 mode ciphers aes-ccm
  !
  ssid data
  !
  ssid voice
  !
  antenna gain 0
  peakdetect
  dfs band 3 block
  stbc
  mbssid
  speed basic-12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m14.
  m15. m16. m17. m18. m19. m20. m21. m22. m23. a1ss9 a2ss8 a3ss9
  power client local
  channel width 40-below
  channel 5180
  station-role root
  dot11 qos class voice local
    admission-control
    admit-traffic narrowband max-channel 75 roam-channel 6
  !

```

```

dot11 qos class voice cell
  admission-control
!
world-mode dot11d country-code US both
!
interface Dot11Radio1.2
encapsulation dot1Q 2
bridge-group 2
bridge-group 2 subscriber-loop-control
bridge-group 2 spanning-disabled
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
service-policy input Data
service-policy output Data
!
interface Dot11Radio1.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 subscriber-loop-control
bridge-group 3 spanning-disabled
bridge-group 3 block-unknown-source
no bridge-group 3 source-learning
no bridge-group 3 unicast-flooding
service-policy input Voice
!
interface Dot11Radio1.10
encapsulation dot1Q 10 native
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0.2
encapsulation dot1Q 2
bridge-group 2
bridge-group 2 spanning-disabled
no bridge-group 2 source-learning
service-policy input Data
service-policy output Data
!
interface GigabitEthernet0.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 spanning-disabled
no bridge-group 3 source-learning
service-policy input Voice
!
interface GigabitEthernet0.10
encapsulation dot1Q 10 native

```



```

bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
mac-address 18e7.281b.3f54
ip address 10.9.0.9 255.255.255.0
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip default-gateway 10.9.0.2
ip forward-protocol nd
no ip http server
ip http authentication aaa ip
http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
nas 10.9.0.9 key 7 <REMOVED>
user wds nhash 7 <REMOVED>
!
radius-server attribute 32 include-in-access-req format %h
!
radius server 10.0.0.20
address ipv4 10.0.0.20 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
radius server 10.9.0.9
address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
access-list 111 permit tcp any any neq telnet
bridge 1 route ip
!
wlccp ap username wds password 7 <REMOVED>
wlccp ap wds ip address 10.9.0.9
wlccp authentication-server infrastructure method_WDS
wlccp authentication-server client eap method_Clients wlccp
authentication-server client leap method_Clients wlccp wds
priority 255 interface BVI1
!
line con 0
access-class 111 in
line vty 0 4
access-class 111 in
transport input all
!
ntp server 10.0.0.2
ntp broadcast client
end

```

Cisco Meraki アクセスポイント

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

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

ワイヤレス ネットワークの作成

Cisco Meraki アクセスポイントを追加して WLAN サービスを提供する前に、ワイヤレス ネットワークを作成する必要があります。ドロップダウンメニューから

[新規ネットワークの作成 (Create a new network)] を選択します。

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

Search Dashboard

Meraki

NETWORK

Meraki MX64

Network-wide

Security & SD-WAN

Organization

Create network

Setup network

Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization. ⓘ

Network name

Network type ⓘ


Network configuration

Default Meraki configuration

Bind to template No templates to bind to ⓘ

Clone from existing network

Select devices from inventory

 You have no unused devices

Add new devices or go to the inventory page to select devices that are already in networks

[Add devices](#) [Go to inventory](#)

[Create network](#)

Cisco Meraki アクセス

ポイントは、シリアル番号または注文番号を指定して要求できます。要求した Cisco Meraki アクセスポイントは、使用可能なインベントリに表示されます。

Cisco Meraki アクセスポイントは、**[ネットワークの作成 (Create network)]** または **[組織 (Organization)]**]> **[設定 (Configure)]**]> **[インベントリ (Inventory)]**] ページで **[デバイスの追加 (Add Devices)]**] を選択して要求できます。

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

Claim by serial and/or order number

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

Close

Claim

要求した Cisco Meraki アクセスポイントは、[組織 (Organization)] > [設定 (Configure)] > [インベントリ (Inventory)] ページで対象ワイヤレスネットワークに追加できます。

Model ^	Claimed on
MR53	4/29/2020 2:59 PM

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

MAC address	Serial number	Model ^	Claimed on
88:15:44:60:18:8c	Q2MD-MWQS-J9K7	MR53	4/29/2020 2:59 PM

SSID の構成

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

Cisco RoomOS Series には個別の SSID

を割り当てることを推奨します。データクライアントやその他のタイプのクライアントは、それぞれ異なる SSID と VLAN を使用する必要があります。

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

SSID 名を設定するには、[名前の変更 (Rename)] を選択します。

SSID を有効にするには、ドロップダウンメニューから [有効 (Enabled)] を選択します。

The screenshot shows the Cisco Meraki dashboard interface. On the left is a navigation sidebar with 'Wireless' selected. The main content area is titled 'Configuration overview' and shows details for a SSID named 'meraki-voice'. The 'Enabled' status is set to 'enabled'. The 'Name' field has a 'rename' link. Under 'Access control', 'Encryption' is set to '802.1X with Meraki RADIUS'. Other settings include '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), and 'VPN' (Disabled). A 'Splash page' section shows 'Splash page enabled' (no) and 'Splash theme' (n/a).

meraki-voice	
Enabled	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)] > [アクセスポイント (Access points)] ページで、[WPA2-Enterprise] を選択して 802.1x 認証を有効にします。

[WPA2-Enterprise] を選択する際には、Cisco Meraki 認証サーバや外部の RADIUS

サーバを使用できます。Cisco Meraki 認証サーバは PEAP 認証をサポートします。PEAP 認証では有効なメールアドレスが必要です。

他の認証タイプ (事前共有キーなど) も使用できます。[スプラッシュページ (Splash page)] が [なし (None)]

に設定されていて、ダイレクトアクセスが有効になっていることを確認します。

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 Disabled

802.11w Disabled (never use)

Splash page

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

[WPA2-Enterprise] が有効になっている環境で Cisco Meraki 認証サーバーを RADIUS サーバーとして使用する場合は、[ネットワーク全体 (Network-wide)] > [設定 (Configure)] > [ユーザー (Users)] ページでユーザーアカウントを作成し、Webex Desk Series が 802.1x 認証に認証サーバーを使用するように設定する必要があります。

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

User management portal

SSID: meraki-voice

This SSID uses WPA2-Enterprise with Meraki authentication. These 802.1X accounts are managed separately from Administrator or Guest accounts.

Authorization Remove Users Search...

Description	Email (Username)	Account type	Authorized for SSID *	Authorized by

Save Changes or cancel

(Please allow 1-2 minutes for changes to take effect.)

Create user

Account type: Meraki 802.1X

Description:

Email (Username):

Password:

Authorized:

[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (Access control)] ページで、[ブリッジモード (Bridge mode)] を有効にすることを推奨します。この場合、Cisco RoomOS Series は、呼制御やその他のエンドポイントがクラウドベースでない限り、Cisco Meraki ネットワークではなくローカルの LAN から DHCP を取得します。

[ブリッジモード (Bridge mode)] を有効にすると、VLAN タギング オプションが使用できるようになります。SSID の

[VLAN タギング (VLAN tagging)] を有効にすることを推奨します。

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

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

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 スイッチを使用する場合は、Cisco Meraki アクセス ポイントが接続するスイッチ ポートを次のように構成して、802.1q トランッキングを有効にします。

```
Interface GigabitEthernet X switchport
trunk encapsulation dot1q switchport
mode trunk
mls qos trust dscp
```

The screenshot shows the Cisco Meraki configuration page for 'Addressing and traffic'. The left sidebar has 'Wireless' selected. The main content area shows 'Client IP assignment' with 'Bridge mode: Make clients part of the LAN' selected. Below this is a 'VLAN tagging' section with 'Use VLAN tagging' checked. A table for 'VLAN ID' shows 'All other APs' with a value of '3' and an 'Add VLAN' link. The 'Content filtering' section is set to 'Don't filter content', and 'Bonjour forwarding' is set to 'Enable Bonjour Gateway'.

AP tags	VLAN ID	Actions
All other APs	3	Add VLAN

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

[5 GHz 帯域のみ (5 GHz band only)] を選択して、Cisco RoomOS Series を 5 GHz 帯域で動作させることを推奨します。多数のチャンネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

距離が離れているために 2.4 GHz 帯域を使用する必要がある場合は、**[デュアルバンド運用 (2.4 GHz および 5 GHz) (Dual band operation (2.4 GHz and 5 GHz))]** を選択する必要があります。**[バンドステアリングを使用するデュアルバンド運用 (Dual band operation with Band Steering)]** オプションは使用しないでください。

従来の 2.4 GHz クライアントがワイヤレス LAN に接続できるようにする必要がある場合を除き、12 Mbps 未満のデータ レートは無効することを推奨します。

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

Wireless options

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)

Lower Density Higher Density

1 2 5.5 6 9 11 12 18 24 36 48 64

802.11b devices not supported

[ワイヤレス (Wireless)] > [設定 (Configure)] > [SSIDの可用性 (SSID availability)] ページでは、[可視性 (Visibility)] を [このSSIDをパブリックにアドバタイズする (Advertise this SSID publicly)] に設定することで SSID をブローキャストできます。

[APごとの可用性 (Per-AP Availability)] は [この SSIDをすべての AP で有効にする (This SSID is enabled on all APs)] に設定することを推奨します。

必要に応じて SSID の可用性をスケジュール設定できますが、[スケジュールされた可用性 (Scheduled Availability)] は [無効 (Disabled)] に設定することを推奨します。

Search Dashboard

SSID availability

SSID: meraki-voice

Visibility: Advertise this SSID publicly

Per-AP availability: This SSID is enabled on all APs

Scheduled availability: disabled

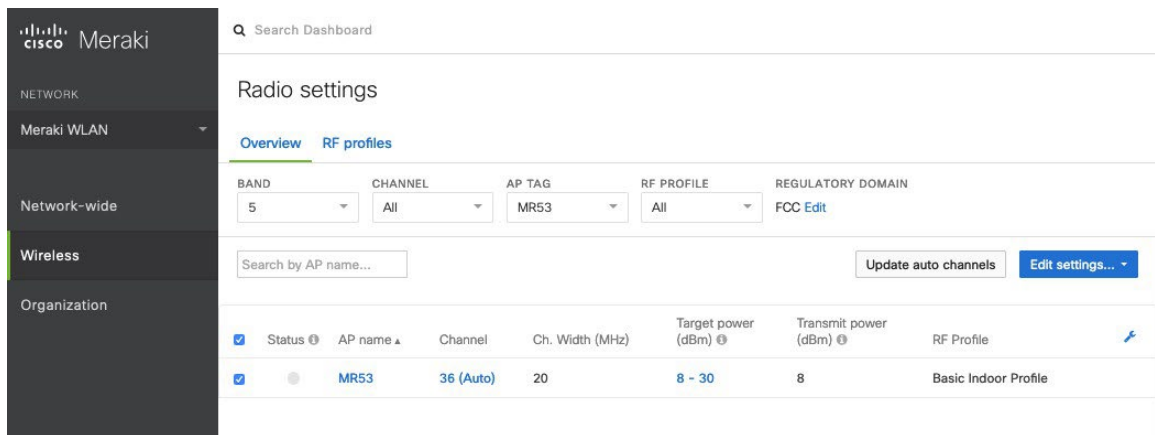
無線の設定

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

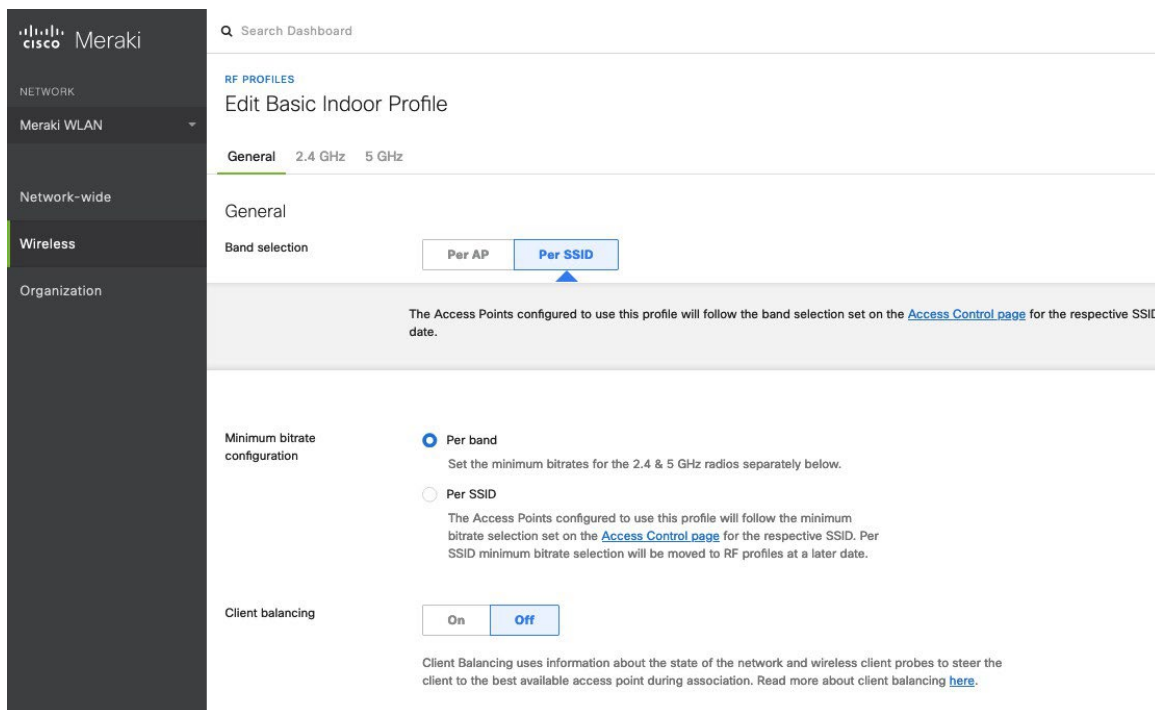
Cisco Meraki アクセスポイントを使用する場合は、チャンネルおよび送信電力に **[自動 (Auto)]** を選択し、RF プロファイルで定義されているものを利用することを推奨します。

ただし、個々のアクセスポイントの 5 GHz または 2.4 GHz

無線のいずれかに、チャンネルと送信電力を静的に設定できます。これは、エリアに断続的な干渉源が存在する場合に必要なことがあります。一方で、他のアクセスポイントで **[自動 (Auto)]** を有効にし、静的チャンネルが割り当てられているチャンネルを回避できます。



標準の [基本屋内プロファイル (Basic Indoor Profile)] を変更するか、[バンド選択 (Band selection)] を [SSID ごと (Per SSID)] に設定し、[クライアントバランシング (Client balancing)] を [オフ (Off)] に設定して新しい RF プロファイルを作成することをお勧めします。



RF プロファイルでは、5 GHz 無線の [チャンネル幅 (Channel width)] として、20 MHz、40 MHz、または 80 MHz を使用するように設定できます。

2.4 GHz 無線は 20 MHz

チャンネルを使用し、他のチャンネル幅に設定することはできません。すべてのアクセスポイントで同じチャンネル幅を使用することを推奨します。

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

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

[無線送信電力範囲 (Radio transmit power range)] も RF プロファイルで構成されます。

[最小ビットレート構成 (Minimum bitrate configuration)] が [バンドごと (Per band)] に設定されている場合、SSID 構成で定義されている内容が上書きされます。

従来の 2.4 GHz クライアントがワイヤレス LAN に接続できるようにする必要がある場合を除き、12 Mbps 未満のデータレートは無効することを推奨します。

General 2.4 GHz **5 GHz**

5 GHz radio settings

Turn off 5GHz radio See band selection above.

Channel width Auto **Manual**

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

General 2.4 GHz **5 GHz**

5 GHz radio settings

Turn off 5GHz radio

Channel width

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	148	152	157	161	169
40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
80 MHz	42				58				106				122				138				155				

DFS channels Deselect DFS channels

Cancel Done

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 & トラフィック シェーピング

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

ワイヤレスクライアントのローカル LAN アクセスを許可するように、[レイヤ 3ファイアウォールルール (Layer 3 firewall rule)] が構成されていることを確認します。

トラフィックシェーピングルールを定義できるようにするには、[トラフィックのシェープ (Shape traffic)] ドロップダウンメニューで [このSSIDのトラフィックをシェープ (Shape traffic on this SSID)] を選択します。[このSSIDのトラフィックをシェープ (Shape traffic on this SSID)] を適用した後、[新しいルールを作成 (Create a new rule)] を選択して [トラフィックシェーピングルール (Traffic shaping rules)] を定義します。

Cisco Meraki アクセスポイントのデフォルトでは、DSCP EF (46) とマークされた音声フレームに WMM UP 6 ではなく WMM UP 5 のタグを、DSCP CS3 (24) とマークされたコール制御フレームに WMM UP 4 ではなく WMM UP 3 のタグを付けます。

The screenshot shows the Cisco Meraki dashboard interface for configuring Firewall & traffic shaping for the SSID 'meraki-voice'. The left sidebar contains navigation options: NETWORK, Meraki WLAN, Network-wide, Wireless (highlighted), and Organization. The main content area includes a search bar and several configuration sections:

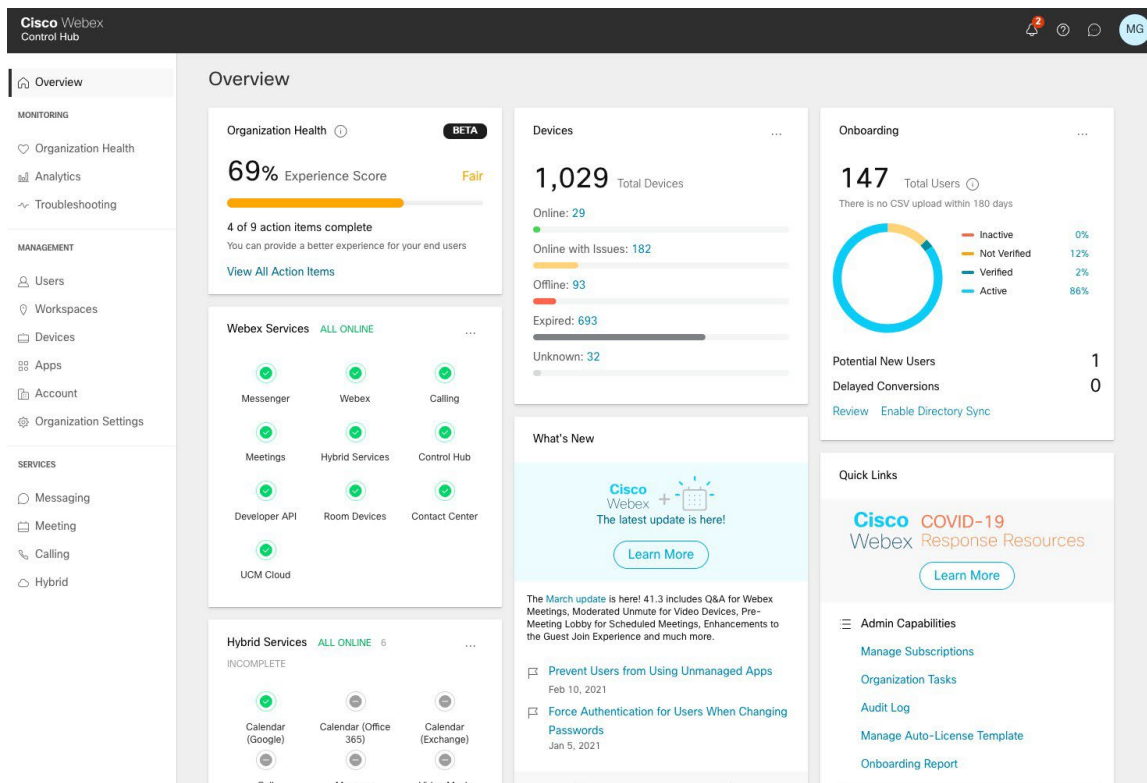
- Block IPs and ports:** Layer 2 LAN isolation is set to 'Disabled (bridge mode only)'. Layer 3 firewall rules are listed in a table with columns: #, Policy, Protocol, Destination, Port, Comment, and Actions. Two rules are shown: one for 'Wireless clients accessing LAN' and a 'Default rule'. A link 'Add a layer 3 firewall rule' is provided.
- Block applications and content categories:** Layer 7 firewall rules section states 'There are no rules defined for this SSID.' with a link 'Add a layer 7 firewall rule'.
- Traffic shaping rules:** Per-client bandwidth limit is 'unlimited' with a 'details' link and an 'Enable SpeedBurst' checkbox. Per-SSID bandwidth limit is also 'unlimited' with a 'details' link. The 'Shape traffic' dropdown is set to 'Shape traffic on this SSID'.

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

Cisco の呼制御の構成

Webex

Webex はクラウド登録を有効にするため、Cisco RoomOS Series に直接インターネット接続がある限り、VPN 接続は必要ありません。



Cisco RoomOS Series は、Webex

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

個人的な使用

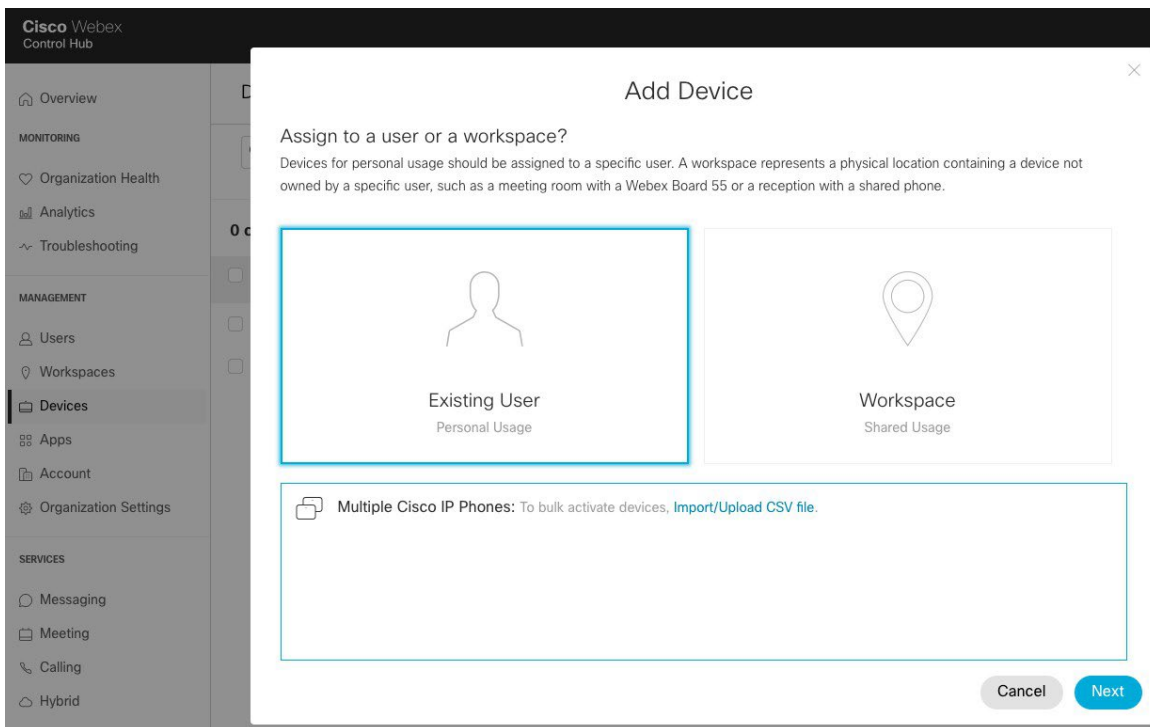
Cisco RoomOS Series は、[デバイス (Devices)] 経由でユーザーが個人的に使用できるように構成できます。

ユーザーのデバイスを追加するには、[デバイス (Devices)]

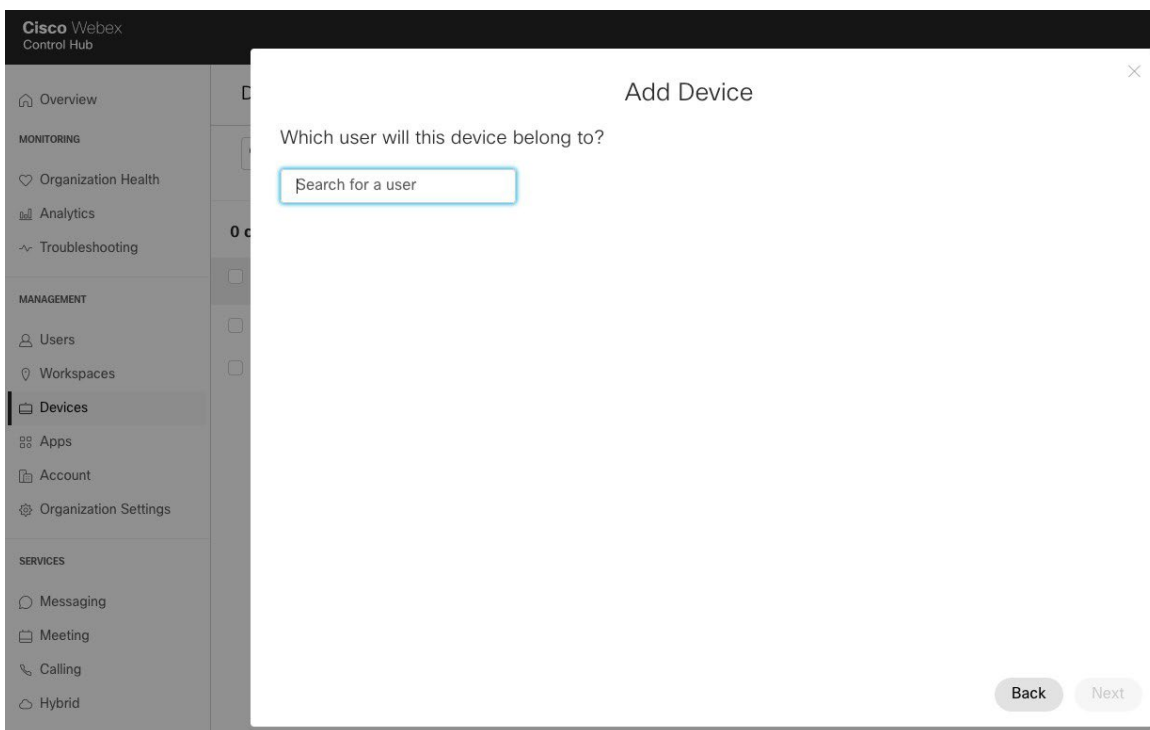
に移動し、[デバイスの追加 (Add Device)]

を選択します。次の画面で、[既存のユーザー (Existing User)]

を選択し、[次へ (Next)] をクリックします。



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



Cisco RoomOS Series に入力する **[アクティベーションコード (Activation Code)]** が表示されます。 **[ユーザー (Users)]**

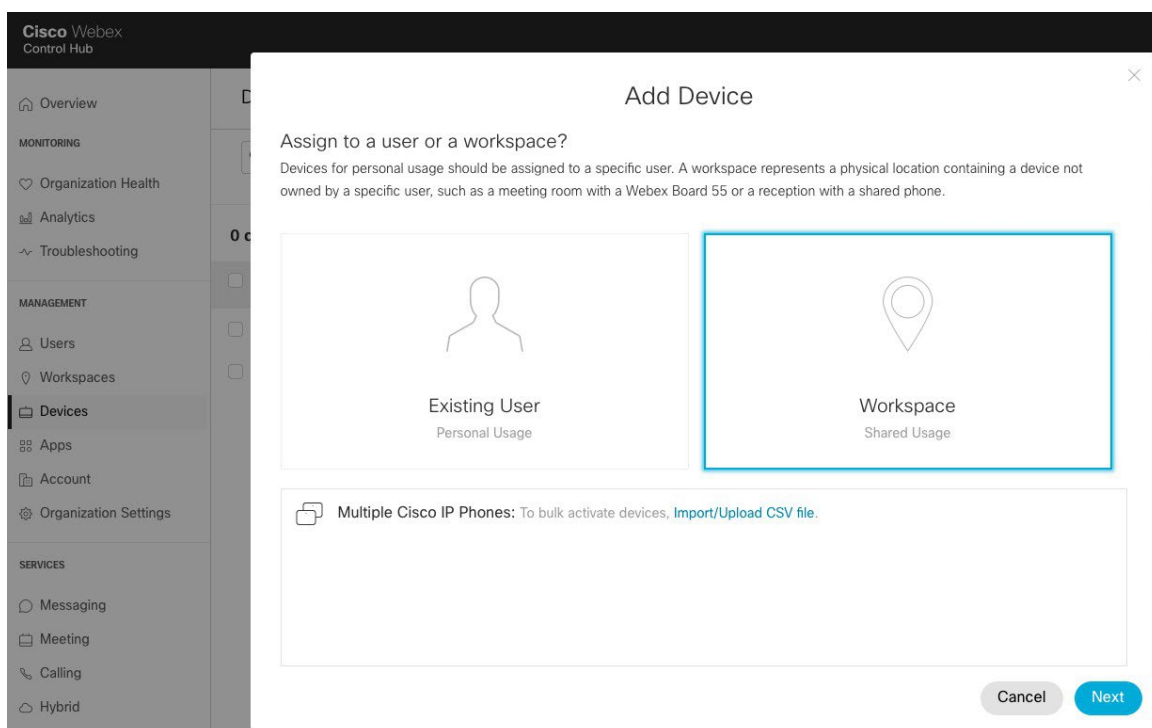
でユーザーを選択して、サービスを設定または変更します。

共同利用

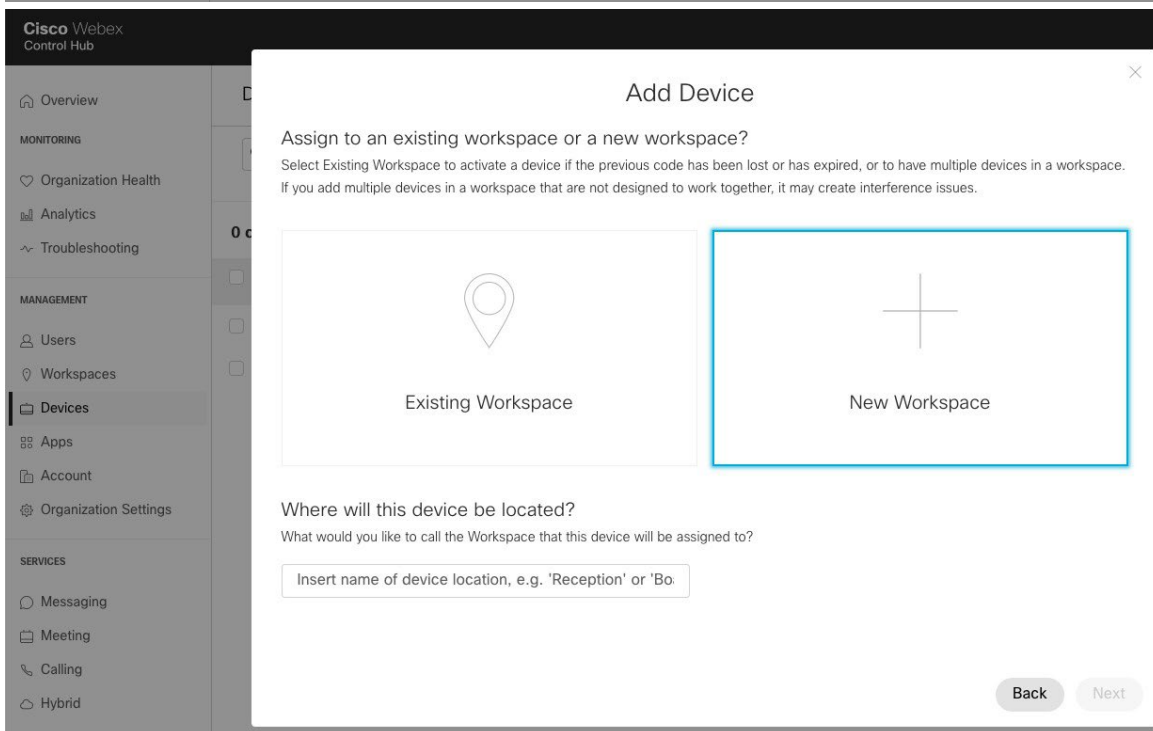
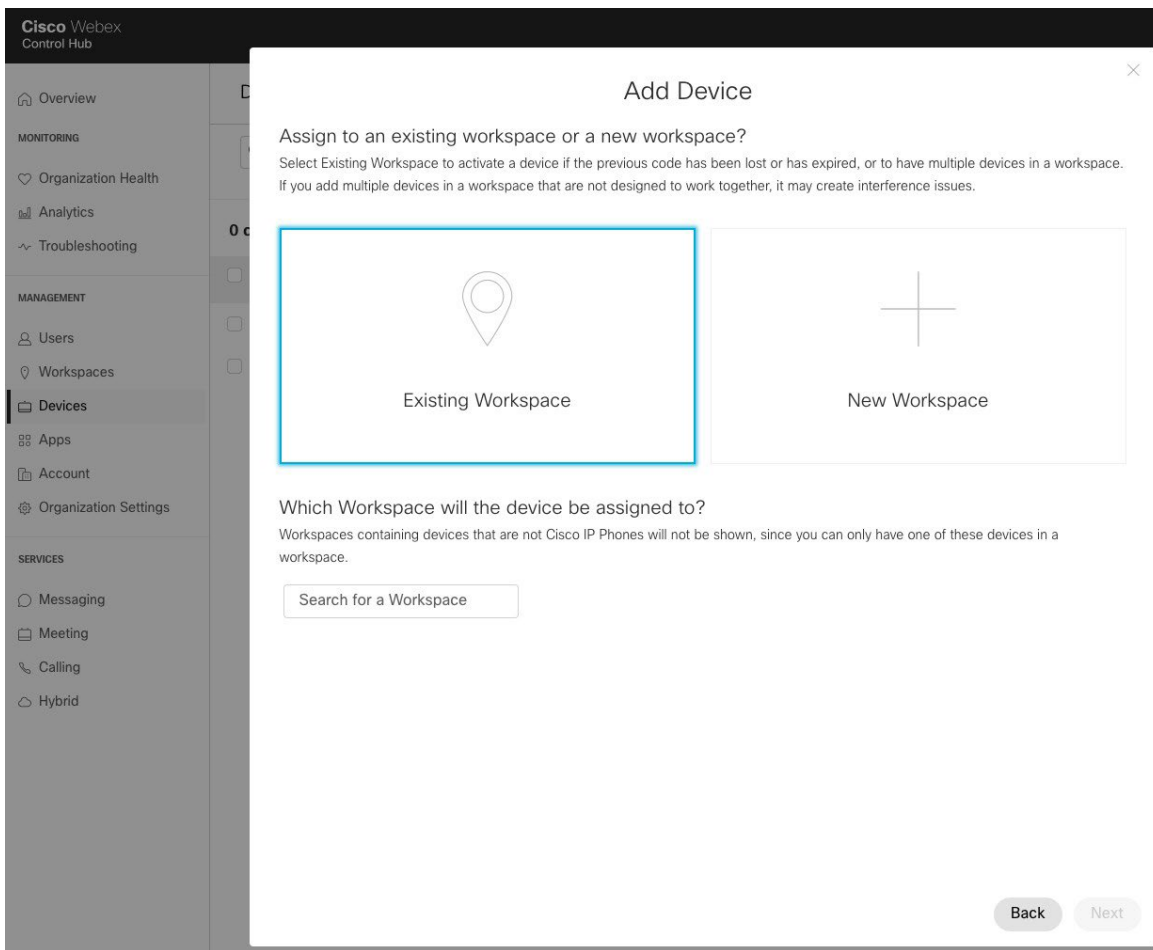
Cisco RoomOS Series は、[デバイス (Devices)] または [ワークスペース (Workspaces)] を介してワークスペースとして構成できます。

[デバイス (Devices)]

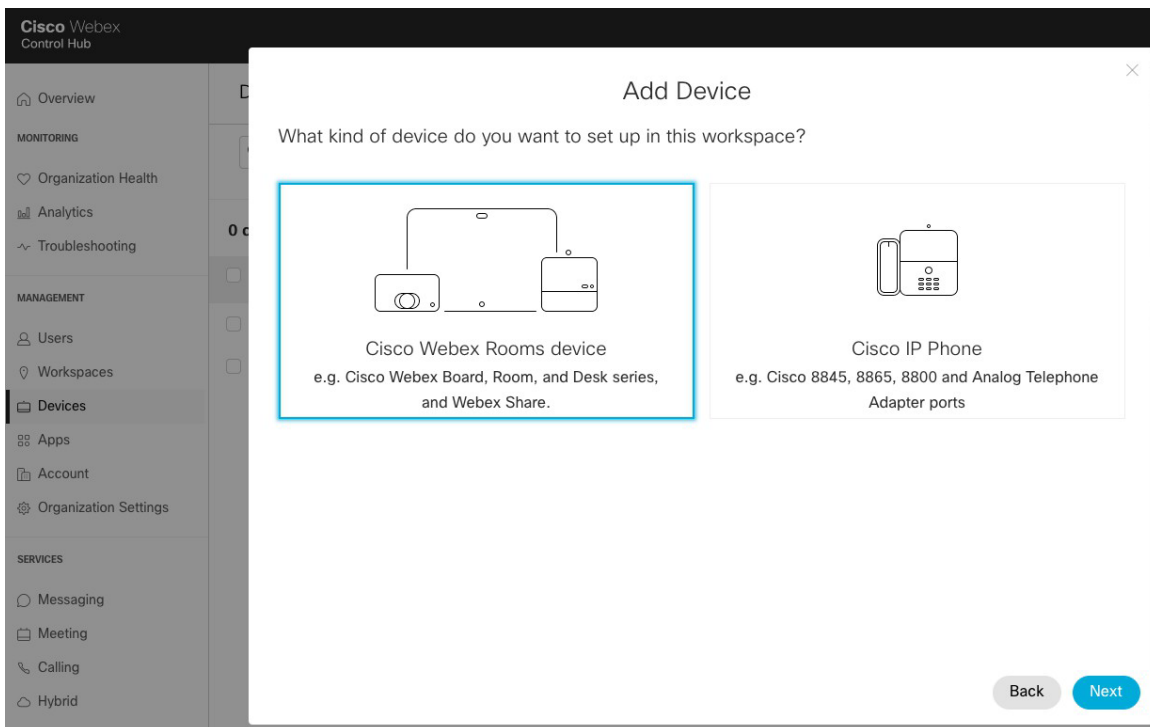
を介してワークスペースを追加するには、[デバイス (Devices)] に移動し、[デバイスの追加 (Add Device)] を選択します。次の画面で、[ワークスペース (Workspace)] を選択し、[次へ (Next)] をクリックします。



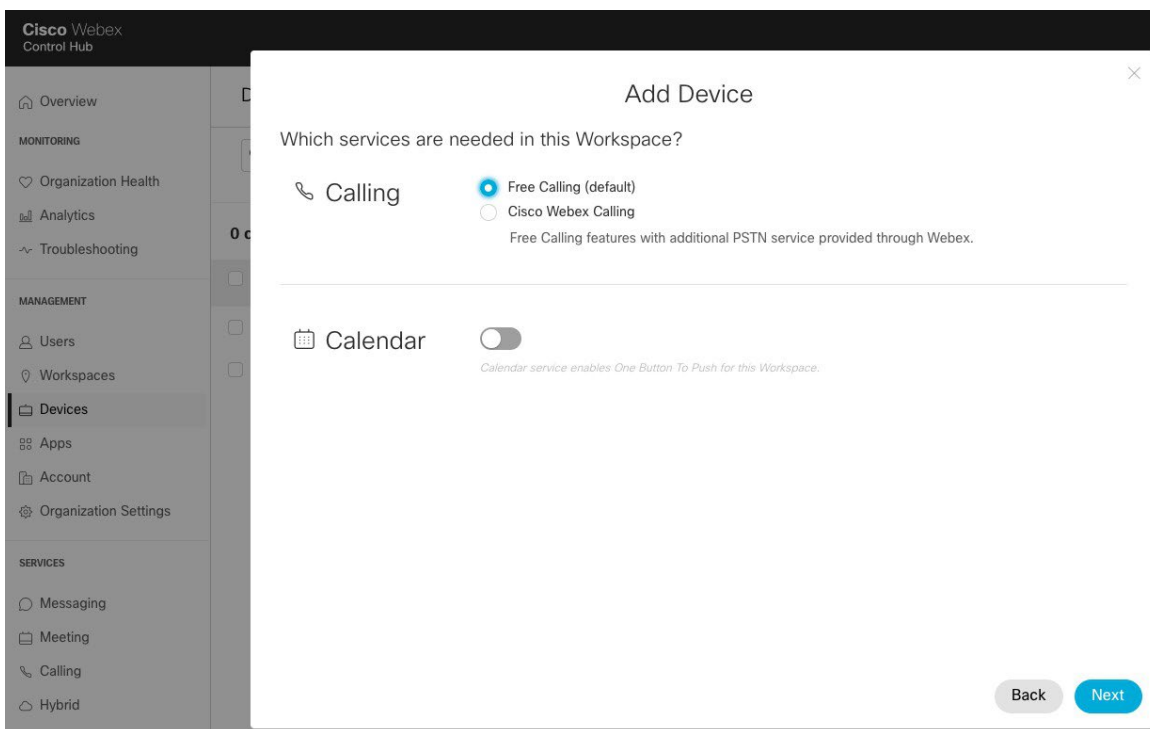
[既存のワークスペース (Existing Workspace)] または [新しいワークスペース (New Workspace)] を選択します。選択したオプションに応じて、ワークスペース名を検索または入力して、[次へ (Next)] をクリックします。



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



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



Cisco RoomOS Series に入力する [アクティベーションコード (Activation Code)] が表示されます。ワークスペースを介して既存の Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

[ワークスペース (Workspaces)]

を選択して、サービスを設定または変更します。

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

<https://help.webex.com/ja-jp/WBX000028782/Network-Requirements-for-Webex-Services>

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

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

Cisco Unified Communications Manager

Cisco Unified Communications Manager は、さまざまな製品、発呼機能、およびセキュリティ機能を提供します。

デバイスの有効化

Cisco Unified Communications Manager で Cisco RoomOS Series のデバイスタイプを有効にするには、対応するデバイスパッケージの COP ファイルを、各 Cisco Unified Communications Manager サーバーの Cisco Unified Operating System Administration Web ページからインストールする必要があります。

デバイスパッケージの COP ファイルのインストール後に、各 Cisco Unified Communication Manager ノードを再起動する必要がない場合があります。

Cisco Unified Communications Manager のバージョンに応じて、次を実行します。

11.5(1)SU4 以降

- すべての Cisco Unified Communications Manager ノードをリブートします。

11.5(1)SU5 以降または 12.5(1) 以降

- すべての Cisco Unified Communications Manager ノードで Cisco Tomcat サービスを再起動します。
- パブリッシャノードで Cisco CallManager サービスを実行している場合は、パブリッシャノードでのみサービスを再起動します。

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

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

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

Cisco RoomOS Series を Cisco Unified Communications Manager に追加する際、イーサネット MAC アドレスを使用して無線 LAN MAC を Wi-Fi 接続だけに使用するようにプロビジョニングする必要があります。イーサネット MAC アドレスは、Cisco RoomOS Series で [バージョン情報 (About)] または [設定 (Settings)] > [このデバイスについて (About this device)] に移動して見つけることができます。

Device Information	
<input checked="" type="checkbox"/> Device is trusted	
MAC Address*	<input type="text"/>
Description	<input type="text"/>
Device Pool*	-- Not Selected -- View Details
Common Device Configuration	< None > View Details
Phone Button Template*	-- Not Selected --
Common Phone Profile*	Standard Common Phone Profile

デバイスプール

新しい Cisco RoomOS Series を作成するときは、**[デバイスプール (Device Pool)]**を設定する必要があります。

デバイスプールでは、共通の設定 (Cisco Unified Communications Manager など)、ローミングに関連する設定 (日付/時刻グループ、地域など)、ローカルルートグループ設定、デバイスモビリティに関連する情報の設定、およびその他のグループ設定を定義します。

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

Device Pool Settings	
Device Pool Name*	Default
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >

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

電話ボタン テンプレート

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

を構成する必要があります。さまざまな機能に対するオプションを使用して、カスタムの電話ボタンテンプレートを作成できます。

Phone Button Template Information		
Button Template Name *	Standard Cisco Webex Desk Pro	

Button Information		
Button	Feature	
1	Line **	Line

セキュリティ プロファイル

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

セキュリティ

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

セキュリティ プロファイルで Locally Significant

Certificate (LSC) を使用するには、認証局プロキシ機能 (CAPF) が動作している必要があります。

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

Protocol Specific Information	
Packet Capture Mode *	None
Packet Capture Duration	0
BLF Presence Group *	Standard Presence group
MTP Preferred Originating Codec *	711ulaw
Device Security Profile *	Cisco Webex Desk Pro - Standard SIP Non-Secure
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile *	Standard SIP Profile View Details
Digest User	< None >
<input type="checkbox"/> Media Termination Point Required <input type="checkbox"/> Unattended Port <input type="checkbox"/> Require DTMF Reception	

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

Phone Security Profile Information

Product Type: Cisco Webex Desk Pro
Device Protocol: SIP
Name * Cisco Webex Desk Pro - Standard SIP Non-Secure Pr
Description Cisco Webex Desk Pro - Standard SIP Non-Secure Pr
Nonce Validity Time * 600
Device Security Mode Non Secure
Transport Type * TCP+UDP

Enable Digest Authentication
 TFTP Encrypted Config
 Exclude Digest Credentials in Configuration File

Phone Security Profile CAPF Information

Authentication Mode * By Null String
Key Order * RSA Only
RSA Key Size (Bits) * 2048
EC Key Size (Bits) < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port * 5060

SIP プロファイル

新しい Cisco RoomOS Series を作成するときは、**[SIP プロファイル (SIP Profile)]** を構成する必要があります。Cisco RoomOS Series のカスタム SIP プロファイルを作成することをお勧めします (標準 SIP プロファイルまたはモバイルデバイスの標準 SIP プロファイルを使用しないでください)。

Protocol Specific Information

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

Media Termination Point Required
 Unattended Port
 Require DTMF Reception

Cisco RoomOS Series 用のカスタム SIP プロファイルを作成するには、標準 SIP プロファイルを参照テンプレートとして使用します。標準 SIP

プロファイルをコピーし、次のパラメータを変更します。

[レジスタの再送間隔の調整値 (秒) (Timer Register Delta (seconds))] = **30** に設定 (デフォルト = 5)

[タイマー キープアライブの有効期限 (Timer Keep Alive

Expires) (秒)] = **300** (デフォルト = 120) [タイマー

サブスクライブの有効期限 (Timer Subscribe

Expires) (秒)] = **300** (デフォルト = 120) [タイマー

サブスクライブ デルタ (Timer Subscribe

Delta) (秒)] = **15** (デフォルト = 5)

[システム (System)] > [サービスパラメータ (Service Parameters)] > [Cisco CallManager] の [SIP Station KeepAlive 間隔 (SIP Station KeepAlive Interval)] が 120 秒であることを確認します。

カスタム SIP プロファイルの例

SIP Profile Information	
Name*	Custom Webex Desk Pro SIP Profile
Description	Custom Webex Desk Pro SIP Profile
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
User-Agent and Server header information*	Send Unified CM Version Information as User-Ager
Version in User Agent and Server Header*	Major And Minor
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, an
Confidential Access Level Headers*	Disabled
<input type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Offer valid IP and Send/Receive mode only for T.38 Fax Relay	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
<input type="checkbox"/> Assured Services SIP conformance	
<input type="checkbox"/> Enable External QoS**	
SDP Information	
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
SDP Transparency Profile	Pass all unknown SDP attributes
Accept Audio Codec Preferences in Received Offer*	Default
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Allow RR/RS bandwidth modifier (RFC 3556)	
Parameters used in Phone	
Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	30
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Media Port Ranges	<input checked="" type="radio"/> Common Port Range for Audio and Video <input type="radio"/> Separate Port Ranges for Audio and Video
Start Media Port*	16384

Stop Media Port*	<input type="text" value="32766"/>
DSCP for Audio Calls	<input type="text" value="Use System Default"/>
DSCP for Video Calls	<input type="text" value="Use System Default"/>
DSCP for Audio Portion of Video Calls	<input type="text" value="Use System Default"/>
DSCP for TelePresence Calls	<input type="text" value="Use System Default"/>
DSCP for Audio Portion of TelePresence Calls	<input type="text" value="Use System Default"/>
Call Pickup URI*	<input type="text" value="x-cisco-serviceuri-pickup"/>
Call Pickup Group Other URI*	<input type="text" value="x-cisco-serviceuri-opickup"/>
Call Pickup Group URI*	<input type="text" value="x-cisco-serviceuri-gpickup"/>
Meet Me Service URI*	<input type="text" value="x-cisco-serviceuri-meetme"/>
User Info*	<input type="text" value="None"/>
DTMF DB Level*	<input type="text" value="Nominal"/>
Call Hold Ring Back*	<input type="text" value="Off"/>
Anonymous Call Block*	<input type="text" value="Off"/>
Caller ID Blocking*	<input type="text" value="Off"/>
Do Not Disturb Control*	<input type="text" value="User"/>
Telnet Level for 7940 and 7960*	<input type="text" value="Disabled"/>
Resource Priority Namespace	<input type="text" value="< None >"/>
Timer Keep Alive Expires (seconds)*	<input type="text" value="300"/>
Timer Subscribe Expires (seconds)*	<input type="text" value="300"/>
Timer Subscribe Delta (seconds)*	<input type="text" value="15"/>
Maximum Redirections*	<input type="text" value="70"/>
Off Hook To First Digit Timer (milliseconds)*	<input type="text" value="15000"/>
Call Forward URI*	<input type="text" value="x-cisco-serviceuri-cfwdall"/>
Speed Dial (Abbreviated Dial) URI*	<input type="text" value="x-cisco-serviceuri-abbrdial"/>
<input checked="" type="checkbox"/> Conference Join Enabled <input type="checkbox"/> RFC 2543 Hold <input checked="" type="checkbox"/> Semi Attended Transfer <input type="checkbox"/> Enable VAD <input type="checkbox"/> Stutter Message Waiting <input type="checkbox"/> MLPP User Authorization	
Normalization Script	
Normalization Script	<input type="text" value="< None >"/>

<input type="checkbox"/> Enable Trace	
Parameter Name	Parameter Value
1	<input type="text"/> <input type="text"/> <input type="button" value="+"/> <input type="button" value="-"/>

Incoming Requests FROM URI Settings

Caller ID DN

Caller Name

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*

Resource Priority Namespace List

SIP Rel1XX Options*

Video Call Traffic Class*

Calling Line Identification Presentation*

Session Refresh Method*

Early Offer support for voice and video calls*

Enable ANAT

Deliver Conference Bridge Identifier

Allow Passthrough of Configured Line Device Caller Information

Reject Anonymous Incoming Calls

Reject Anonymous Outgoing Calls

Send ILS Learned Destination Route String

Connect Inbound Call before Playing Queuing Announcement

SIP OPTIONS Ping

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)*

Ping Interval for Out-of-service Trunks (seconds)*

Ping Retry Timer (milliseconds)*

Ping Retry Count*

SDP Information

Send send-receive SDP in mid-call INVITE

Allow Presentation Sharing using BFCP

Allow IX Application Media

Allow multiple codecs in answer SDP

QoS パラメータ

SIP 通信、電話設定、およびデバイスで使用される電話ベースのサービスに使用される DSCP 値は、Cisco Unified Communications Manager のエンタープライズパラメータで定義されます。

SIP 通信および電話設定の DSCP 値は、デフォルトで CS3 に設定されます。電話ベースのサービスは、デフォルトでベストエフォート型トラフィックに設定されます。

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

オーディオおよびビデオのビットレート

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

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

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

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

Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Keep Current Setting	<input checked="" type="radio"/> 64 kbps (G.722, G.711) <input type="radio"/> kbps	<input type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input checked="" type="radio"/> 2000 kbps	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input type="radio"/> kbps

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

オーディオ コーデック	オーディオ ビットレート
----------------	-----------------

AAC-LD	128 ~ 256 Kbps
Opus	6 ~ 510 Kbps
G.722/G.711	64 Kbps
G.722.1	32 Kbps
G.729	8 Kbps

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

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

Cisco RoomOS Series は、リモートデバイスの機能に応じ、最大 FHD 1080p ビデオまで受信できます。その際には、リージョン設定の構成を考慮に入れます。

Cisco RoomOS Series

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

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

製品固有の設定オプション

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

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

Cisco Unified Communications Manager

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

一部の製品固有の設定オプションは、エンタープライズ電話、共通の電話プロファイル、または個々の電話レベルで設定できます。

Cisco RoomOS Series 構成オプション (バージョン 12.5 より前)

Product Specific Configuration Layout		Parameter Value	Override Enterprise/Common Phone Profile Settings
Room Name (from Exchange(R))			
Web Access*	Disabled		
SSH Access*	Disabled		
Default Call Protocol*	SIP		
Quality Improvement Server			
Multipoint Mode*	Use Endpoint		
Telnet Access*	Off		
Microphone Unmute On Disconnect*	On		
Call Logging Mode*	On		
OSD Encryption Indicator*	Auto		
Alternate phone book server type*	UDS		
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	15000		
Max Total Upstream Rate	10000		
Load Server			
WiFi Allowed*	On		
System Name			
Wake-up On Motion Detection*	On		
Custom Message			
Settings Menu Mode*	Unlocked		
Accessibility Call Notification*	Default		
Configuration Control Mode*	Unified CM and Endpoint		
Webex Devices Onboarding Token			
Easy Webex join*	Auto		
Far End Camera Control Settings			
Far End Camera Control*	On		
Far End Camera Control Signaling Capability*	On		
Facility Service Settings			
Facility Service Type*	Helpdesk		
Facility Service Name			
Facility Service Number			
Facility Service Call Type*	Video		

Standby Settings	
Standby Mode*	On
Standby Delay	10
Serial Port Settings	
Serial Port*	On
Serial Port Login Required*	On
Admin username and password	
Admin Username	
Admin Password	
Proximity	
Proximity Mode*	On
Call Control*	Disabled
Proximity Content Share From Clients*	Disabled
Proximity Content Share To Clients*	Disabled
LDAP User Management	
LDAP Mode*	Off
LDAP Server Address	
LDAP Server Port	0
LDAP Attribute	
LDAP Base DN	
LDAP Encryption*	LDAPS
LDAP Minimum TLS Version*	TLSv1.2
LDAP Verify Server Certificate*	Off
LDAP Admin Filter	
LDAP Admin Group	
Customization Provisioning	
Customization File	
Customization Hash Type*	SHA512
Customization Hash	
SMTP Provisioning	
SMTP Mode*	Off
SMTP Server	
SMTP Port	0
SMTP Security type*	None
SMTP Username	
SMTP Password	
SMTP From address	

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

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

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

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

ファシリティ サービス コールタイプ	各ファシリティサービスにコールタイプを設定します。ファシリティサービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。タッチコントローラでは、FacilityService Service 1 だけを使用できます。ファシリティサービスは、リモートコントロールと画面上のメニューを使用する場合には使用できません。
スタンバイ設定	
スタンバイ モード	このパラメータは、システムをスタンバイモードにするかどうかを決定します。
Standby Delay	スタンバイ モードに入る前に、システムがアイドルモードのまま経過する時間の長さ（分単位）を定義します。注：[スタンバイ制御（Standby Control）]が有効である必要があります。
シリアルポートの設定	
シリアルポート	このパラメータは、デバイスがシリアルポートを有効にするかどうかを示します。
シリアルポートログインが必要です	このパラメータは、シリアルポートに接続するときにログインが必要かどうかを定義します。
管理者のユーザ名とパスワード	
[Admin ユーザ名（Admin Username）]	管理者ユーザのユーザ ID を入力します。
[管理パスワード（Admin Password）]	管理者ユーザのパスワードを入力します。
プロキシミティ	
プロキシミティ モード	プロキシミティアプリがエンドポイントとペアリングできるようにします。
コール制御	プロキシミティアプリに呼制御を許可します。
プロキシミティクライアントからのコンテンツ共有	プロキシミティアプリによるコンテンツ共有を許可し、コンテンツをプレゼンテーションとしてデバイスから TelePresence エンドポイントに送信します。
プロキシミティクライアントへのコンテンツ共有	プロキシミティアプリが TelePresence エンドポイントからプレゼンテーションスライドを受信できるようにします。
LDAP ユーザー管理	
LDAP モード	ビデオシステムは、LDAP（Lightweight Directory Access Protocol）サーバを、ユーザ名とパスワードを一元的に保存および検証する場所として使用することをサポートします。この設定を使用して、LDAP 認証を使用するかどうか設定します。実装は、Microsoft Active Directory（AD）サービスでテスト済みです。
LDAP サーバーアドレス	LDAP サーバーの IP アドレスまたはホスト名を設定します。

LDAP Server Port	LDAP サーバーに接続するポートをオンに設定します。0 に設定した場合は、選択したプロトコルのデフォルトを使用します（「UserManagement LDAP Encryption 設定」を参照）。
LDAP 属性	指定のユーザー名にマップするために使用する属性。設定しない場合、sAMAccountName が使用されます。
LDAP Base DN	検索を開始するエントリの識別名（ベース）。例："DC=company, DC=com"
LDAP 暗号化	ビデオ システムと LDAP サーバとの間の通信を保護する方法を定義します。ポート番号は、UserManagement LDAP Server Port 設定を使用してポート番号をオーバーライドできます。LDAPS：ポート 636 over TLS（Transport Layer Security）上の LDAP サーバに接続します。None：ポート 389 上の LDAP サーバに接続します（暗号化なし）。STARTTLS：ポート 389 上の LDAP サーバに接続し、次に STARTTLS を送信して TLS 暗号化を有効にします。
LDAP の最小 TLS バージョン	許可する最低バージョンの TLS（Transport Layer Security）プロトコルを設定します。TLSv1.0：TLS バージョン 1.0 以上をサポートします。TLSv1.1：TLS バージョン 1.1 以上をサポートします。TLSv1.2：TLS バージョン 1.2 以上をサポートします。
LDAP 検証サーバー証明書	ビデオ システムを LDAP サーバに接続すると、サーバはビデオ システムに証明書を提示して身元を示します。この設定は、ビデオ システムがサーバの証明書を確認するかどうかを決定するために使用します。
LDAP 管理フィルタ	LDAP フィルタは、管理者権限が付与されるユーザを判別するために使用します。設定したら、この設定は UserManagement LDAP Admin Group 設定よりも優先されるようになります。例：(CN=adminuser)。構文の詳細については、LDAP 仕様を参照してください。
LDAP 管理グループ	この AD（Active Directory）グループのメンバーには、管理者権限が付与されます。この設定は、(memberOf:1.2.840.113556.1.4.1941:=) の短縮形です。UserManagement LDAP Admin Filter が設定されている場合、この設定は無視されます。例：CN=admin_group, OU=company groups, DC=company, DC=com
カスタマイズ プロビジョニング	
カスタマイズ ファイル	カスタマイズ プロビジョニング ファイルが保存されているアドレス。このフィールドには、カスタマイズ バンドル ファイルの完全な URL、または使用中の CUCM でホストされている場合はファイル名のみが必要です。
カスタマイズ ハッシュの型	使用するハッシュ関数の種類を設定します。
カスタマイズ ハッシュ	エンドポイントがファイルの整合性を確認できるように、カスタマイズ プロビジョニング ファイルから生成されたハッシュチェックサムを設定します。

SMTP プロビジョニング	
SMTP モード	この設定は、エンドポイントで SMTP を有効または無効にします。
SMTP サーバ	使用する SMTP サーバーのアドレスを設定します。
SMTP ポート (SMTP Port)	SMTP サーバーに使用するポート番号を指定します。
SMTP セキュリティタイプ	使用する SMTP セキュリティタイプを設定します。
SMTP Username	使用する SMTP ユーザー名を設定します。
SMTP Password	使用する SMTP ユーザー名を設定します。
SMTP 送信元アドレス	エンドポイントから SMTP 経由で電子メールを送信するときに使用する送信元アドレスを設定します。

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

Product Specific Configuration Layout

Parameter Value Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

- Audio
- Bluetooth
- BYOD
- CallHistory
- Cameras
- Conference
- FacilityService
- HttpClient
- HttpFeedback
- Logging
- Macros
- NetworkServices
- Phonebook
- RoomAnalytics
- RoomScheduler

General Settings

DefaultVolume: 50 #

Microphones Mute Enabled*: True

Ultrasound MaxVolume: 70

Input

HDMI 1

Level: 0

Mode*: On

MicrophoneMode*: Focused

USBC 1

Level: 0

Mode*: On

SoundsAndAlerts

RingTone: Sunrise

RingVolume: 50

KeyClickDetector

Enabled*: True

Attenuate*: True

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

音声

General Settings	
DefaultVolume	<input type="text" value="50"/> *
Microphones Mute Enabled*	<input type="button" value="True"/> ▾
Ultrasound MaxVolume	<input type="text" value="70"/>
Input	
HDMI 1	
Level	<input type="text" value="0"/>
Mode*	<input type="button" value="On"/> ▾
MicrophoneMode*	<input type="button" value="Focused"/> ▾
USBC 1	
Level	<input type="text" value="0"/>
Mode*	<input type="button" value="On"/> ▾
SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>
KeyClickDetector	
Enabled*	<input type="button" value="True"/> ▾
Attenuate*	<input type="button" value="True"/> ▾

Bluetooth

General Settings

Allowed*	True	▼
Enabled*	False	▼

BYOD

General Settings

HidForwarding Enabled*	False	▼
TouchForwarding Enabled*	True	▼

通話履歴

General Settings

Mode*	On	▼ #
-------	----	-----

カメラ

Background

Enabled*	False	▼
UserImagesAllowed*	True	▼
PowerLine Frequency*	Auto	▼
SpeakerTrack Mode*	Auto	▼

Camera

Brightness

DefaultLevel	20	
Mode*	Auto	▼

ExposureCompensation

Level	0
-------	---

会議

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

FarEndControl	
Mode*	On #
SignalCapability*	On #

ファシリティサービス

Service 1	
CallType*	Video #
Name	Live Support #
Number	#
Type*	Helpdesk #

Service 2	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 3	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 4	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 5	
CallType*	Video
Name	
Number	
Type*	Helpdesk

HTTP クライアント

General Settings	
Mode*	Off ▼
AllowInsecureHTTPS*	False ▼
AllowHTTP*	True ▼
UseHttpProxy*	On ▼

HTTP フィードバック

General Settings	
TlsVerify*	On ▼
UseHttpProxy*	On ▼

ロギング

General Settings	
CloudUpload Mode*	Off ▼
Internal Mode*	On ▼

External	
Mode*	Off ▼
Protocol*	SyslogTLS ▼
TlsVerify*	On ▼

Server	
Address	<input type="text"/>
Port	514

マクロ

General Settings	
AutoStart*	On ▼
Mode*	Off ▼
UnresponsiveTimeout	5

ネットワーク サービス

General Settings

H323 Mode*	Off
UPnP Mode*	On
Websocket*	Off
WelcomeText*	On
Wifi Allowed*	True

HTTP

Mode*	Off
-------	-----

Proxy

Mode*	Off
Url	<input type="text"/>
LoginName	<input type="text"/>
Password	<input type="text"/>
PACUrl	<input type="text"/>

HTTPS

VerifyClientCertificate*	Off
StrictTransportSecurity*	Off

Server

MinimumTLSVersion*	TLSv1.1
--------------------	---------

SNMP

CommunityName	<input type="text"/>
Mode*	Off
SystemContact	<input type="text"/>
SystemLocation	<input type="text"/>

SSH

HostKeyAlgorithm*	RSA
Mode*	Off

SMTP

Mode*	Off
Server	<input type="text"/>
Port	0
Security*	StartTls
Username	<input type="text"/>
Password	<input type="text"/>
From	<input type="text"/>

電話帳 (Phone Book)

Server 1

ID	<input type="text"/>
Type*	CUCM
URL	<input type="text"/>
Pagination*	Enabled
TlsVerify*	On

Room 分析

General Settings	
PeopleCountOutOfCall*	Off ▼
PeoplePresenceDetector*	Off ▼

AmbientNoiseEstimation	
Mode*	Off ▼
Interval	10

ルームスケジューラ

General Settings	
Enabled*	False ▼

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0 ▼

セキュリティ

Audit	
Logging	
Mode*	Internal ▼
OnError	
Action*	Ignore ▼
Server	
Address	
Port	514
PortAssignment*	Auto ▼
Fips Mode*	Off ▼
Session	
InactivityTimeout	0
ShowLastLogon*	Off ▼
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

General Settings	
BaudRate*	115200 ▼
LoginRequired*	On ▼#
Mode*	On ▼#

スタンバイ

General Settings	
BootAction*	RestoreCameraPosition ▾
Control*	On ▾ #
Delay	10 #
StandbyAction*	PrivacyPosition ▾ #
WakeupAction*	RestoreCameraPosition ▾
WakeupOnMotionDetection*	On ▾ #

Signage	
Url	<input type="text"/>
Mode*	Off ▾
InteractionMode*	NonInteractive ▾
RefreshInterval	0 #
Audio*	Off ▾

システム ユニット

General Settings	
Name	<input type="text"/> #

CrashReporting	
Mode*	Off ▾
URL	<input type="text"/> #

ユーザ インターフェイス

機能	
すべて非表示*	{偽} [V]
コール (Call)	
開始*	[自動] [V]
MicCallu:,ntrols,i	{自動} [V]
終了*	[自動] [V]
JoinW@b@:	[自動]
キーボード	[自動] [V]
通信モード*	{非表示}
共有	
開始	[自動] [V]
ホワイトボード	
開始	[自動] [V]

音声	

入力デバイス	
モード	{アンロック}
可視性	[自動]

周辺機器

General Settings

InputDevice Mode*	Off	▼
Pairing CiscoTouchPanels RemotePairing*	On	▼

Profile

TouchPanels*	0	▼
Cameras*	0	▼
ControlSystems*	NotSet	▼

プロキシミティ

General Settings

Mode*	Off	▼	#
-------	-----	---	---

Services

ContentShare

ToClients*	Disabled	▼	#
FromClients*	Enabled	▼	#
CallControl*	Disabled	▼	#

ユーザー管理

LDAP

Mode*	Off	▼	#
Encryption*	LDAPS	▼	#
VerifyServerCertificate*	Off	▼	#
BaseDN	<input type="text"/>		
Attribute	<input type="text"/>		
MinimumTLSVersion*	TLSv1.2	▼	#

Server

Address	<input type="text"/>	#
Port	0	#

Admin

Group	<input type="text"/>	#
Filter	<input type="text"/>	#

PasswordPolicy

ReuseLimit	<input type="text" value="12"/>
MaxLifetime	<input type="text" value="0"/>

Complexity

MinimumLength	<input type="text" value="8"/>
MinimumUppercase	<input type="text" value="0"/>
MinimumLowercase	<input type="text" value="0"/>
MinimumDigits	<input type="text" value="0"/>
MinimumSpecial	<input type="text" value="0"/>

ビデオ

Input

Connector 1

InputSourceType* camera

Name Camera

Visibility* Never

CameraControl

CameraId* 1

Mode* On

Connector 2

InputSourceType* PC

Name PC (USB-C)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 3840_2160_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Connector 3

InputSourceType* PC

Name PC (HDMI)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 3840_2160_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Monitors* Auto

DefaultMainSource* 1

Output

Connector 1

BrightnessMode*

Resolution*

Connector 2

MonitorRole*

RGBQuantizationRange*

Resolution*

Location

HorizontalOffset

VerticalOffset

CEC

Mode*

Presentation

DefaultSource*

Priority*

Selfview

Default

FullscreenMode*

Mode*

OnMonitorRole*

PIPPosition*

OnCall

Duration

Mode*

音声管理

General Settings

Wakeword Mode*

Web エンジン

General Settings

Mode*

RemoteDebugging*

UseHttpProxy*

Webex

General Settings

CloudProximity Mode*

ルームクリーンアップ

AutoRun	
HourOfDay	<input type="text" value="0"/>
ContentType	
Whiteboards*	<input type="text" value="Daily"/>
WebData*	<input type="text" value="Daily"/>

ブッキング

General Settings	
ProtocolPriority*	<input type="text" value="Auto"/>

その他

General Settings	
Configuration Control Mode*	<input type="text" value="Unified CM and Endpoint"/>
Room Name (from Exchange(R))	<input type="text"/>
LoadServer	<input type="text"/>
Webex Devices Onboarding Token	<input type="text"/>

Admin username and password	
Admin Username	<input type="text" value="admin"/>
Admin Password	<input type="text"/>

Customization Provisioning	
Customization File	<input type="text"/>
Customization Hash Type*	<input type="text" value="SHA512"/>
Customization Hash	<input type="text"/>

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

Product Specific Configuration Layout

Parameter Value Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

- Audio
- Bluetooth
- BYOD
- CallHistory
- Cameras
- Conference
- FacilityService
- HttpClient
- HttpFeedback
- Logging
- Macros
- NetworkServices
- Phonebook
- RoomAnalytics
- RoomScheduler
- SIP
- Security
- SerialPort
- Standby
- SystemUnit

General Settings

DefaultVolume #

Ultrasound MaxVolume

USB Mode*

Input

HDMI 1

Level

Mode*

MicrophoneMode*

USBC 1

Level

Mode*

Microphones

Mute

Enabled*

NoiseRemoval

Mode*

SoundsAndAlerts

RingTone

RingVolume

KeyClickDetector

Enabled*

Attenuate*

- UserInterface
- Peripherals
- Proximity
- UserManagement
- Video
- VoiceControl
- WebEngine
- Webex
- RoomCleanup
- Bookings
- Miscellaneous

音声

General Settings	
DefaultVolume	50 #
Ultrasound MaxVolume	70
USB Mode*	SpeakerAndMicrophone v

Input	
HDMI 1	
Level	0
Mode*	On v
MicrophoneMode*	Focused v
USBC 1	
Level	0
Mode*	On v

Microphones	
Mute	
Enabled*	True v
NoiseRemoval	
Mode*	Manual v

SoundsAndAlerts	
RingTone	Sunrise
RingVolume	50

KeyClickDetector	
Enabled*	False v
Attenuate*	True v

Bluetooth

General Settings	
Allowed*	True v
Enabled*	False v

BYOD

General Settings	
HidForwarding Enabled*	False v
TouchForwarding Enabled*	True v

通話履歴

General Settings	
Mode*	On v #

カメラ

Background	
Enabled*	False
UserImagesAllowed*	True
PowerLine Frequency*	Auto
SpeakerTrack Mode*	Auto

Camera	
Brightness	
DefaultLevel	20
Mode*	Auto
ExposureCompensation	
Level	0

会議

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

FarEndControl	
Mode*	On
SignalCapability*	On

ファシリティサービス

Service 1	
CallType*	Video <input type="button" value="v"/>
Name	Live Support <input type="button" value="v"/>
Number	<input type="button" value="v"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 2	
CallType*	Video <input type="button" value="v"/>
Name	<input type="button" value="v"/>
Number	<input type="button" value="v"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 3	
CallType*	Video <input type="button" value="v"/>
Name	<input type="button" value="v"/>
Number	<input type="button" value="v"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 4	
CallType*	Video <input type="button" value="v"/>
Name	<input type="button" value="v"/>
Number	<input type="button" value="v"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 5	
CallType*	Video <input type="button" value="v"/>
Name	<input type="button" value="v"/>
Number	<input type="button" value="v"/>
Type*	Helpdesk <input type="button" value="v"/>

HTTP クライアント

General Settings	
Mode*	Off <input type="button" value="v"/>
AllowInsecureHTTPS*	False <input type="button" value="v"/>
AllowHTTP*	True <input type="button" value="v"/>
UseHttpProxy*	On <input type="button" value="v"/>

HTTP フィードバック

General Settings	
TlsVerify*	On <input type="button" value="v"/>
UseHttpProxy*	On <input type="button" value="v"/>

ロギング

General Settings	
CloudUpload Mode*	Off
Internal Mode*	On

External	
Mode*	Off
Protocol*	SyslogTLS
TlsVerify*	On

Server	
Address	
Port	514

マクロ

General Settings	
AutoStart*	On
Mode*	Off
UnresponsiveTimeout	5

ネットワーク サービス

General Settings

H323 Mode*	Off
UPnP Mode*	On
Websocket*	Off
WelcomeText*	On
Wifi Allowed*	True

HTTP

Mode*	Off
-------	-----

Proxy

Mode*	Off
Url	
LoginName	
Password	
PACUrl	

HTTPS

VerifyClientCertificate*	Off
StrictTransportSecurity*	Off

Server

MinimumTLSVersion*	TLSv1.1
--------------------	---------

SNMP

CommunityName	
Mode*	Off
SystemContact	
SystemLocation	

SSH

HostKeyAlgorithm*	RSA
Mode*	Off

SMTP

Mode*	Off
Server	
Port	0
Security*	StartTls
Username	
Password	
From	

電話帳 (Phone Book)

Server 1

ID	
Type*	CUCM
URL	
Pagination*	Enabled
TlsVerify*	On

Room 分析

General Settings	
PeopleCountOutOfCall*	Off ▼
PeoplePresenceDetector*	Off ▼

AmbientNoiseEstimation	
Mode*	Off ▼
Interval	10

ルームスケジューラ

General Settings	
Enabled*	False ▼

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0 ▼

セキュリティ

Audit	
Logging	
Mode*	Internal ▼
OnError	
Action*	Ignore ▼
Server	
Address	
Port	514
PortAssignment*	Auto ▼
Fips Mode*	Off ▼
Session	
InactivityTimeout	0
ShowLastLogon*	Off ▼
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

General Settings	
BaudRate*	115200 ▼
LoginRequired*	On ▼#
Mode*	On ▼#

スタンバイ

General Settings	
BootAction*	RestoreCameraPosition ▾
Control*	On ▾ #
Delay	10 #
StandbyAction*	PrivacyPosition ▾ #
WakeupAction*	RestoreCameraPosition ▾
WakeupOnMotionDetection*	On ▾ #

Signage	
Url	<input type="text"/>
Mode*	Off ▾
InteractionMode*	NonInteractive ▾
RefreshInterval	0 #
Audio*	Off ▾

システム ユニット

General Settings	
CustomDeviceId	<input type="text"/>
Name	<input type="text"/> #

CrashReporting	
Mode*	Off ▾
URL	<input type="text"/> #

ユーザ インターフェイス

一般設定

Ao:i:ssibllty Inc{lmlngCallNotttca1lon [D@la ult	"]"
予約 可視性タイトル連絡先情	[自動] V
報 タイプ* l診断通知	[自動] V
ブランディング.ブランディング	[自動] V
C<>lrs	[自動] V
K@yTo nils モード**	[自動] V
SouridlE'ff&ts モード@*	[自動] V
f>mKlmlty olfificationsカスタ	[オ] V
ムメッセージ	
ホワイトボード	[オン] V
ActivityIndicators Asslsta ril	[オン] V
...	[通常] V

機能

すべて非表示*	{偽} V
コール (Call)	
開始*	[自動] V
MlclCallu:,ntrols,i	[自動801] V
終了*	[自動] V
JoinW@b@:	[自動] V
キーパッド	[自動] V
通信モード*	[非表示] V

共有	
開始	[自動] V
ホワイトボード	
開始	[自動] V

OSD

暗号化インジケーター	[自動] V
出力	v
ハーフ ウェイク メッセージ	
モード	[自動] V

電話中長

モード	[読み書き] V
デフォルトの検索	

入力デバイス

モード	[アンロック] V
可視性	[自動] V

周辺機器

General Settings	
InputDevice Mode*	Off
Pairing CiscoTouchPanels RemotePairing*	On

Profile	
TouchPanels*	0
Cameras*	0
ControlSystems*	NotSet

プロキシミティ

General Settings	
Mode*	Off
AlternatePort Enabled*	False

Services	
ContentShare	
ToClients*	Disabled
FromClients*	Enabled
CallControl*	Disabled

ユーザー管理

LDAP	
Mode*	Off
Encryption*	LDAPS
VerifyServerCertificate*	Off
BaseDN	
Attribute	
MinimumTLSVersion*	TLSv1.2
Server	
Address	
Port	0
Admin	
Group	
Filter	

PasswordPolicy	
ReuseLimit	12
MaxLifetime	0
Complexity	
MinimumLength	8
MinimumUppercase	0
MinimumLowercase	0
MinimumDigits	0
MinimumSpecial	0

ビデオ

Input

Connector 1

InputSourceType* camera

Name Camera

Visibility* Never

CameraControl

CameraId* 1

Mode* On

Connector 2

InputSourceType* PC

Name PC (USB-C)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 1920_1080_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Connector 3

InputSourceType* PC

Name PC (HDMI)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 1920_1080_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Monitors* Auto

DefaultMainSource* 1

Output

Connector 1

BrightnessMode* ▾

Resolution* ▾

Connector 2

MonitorRole* ▾

RGBQuantizationRange* ▾

Resolution* ▾

Location

HorizontalOffset

VerticalOffset

CEC

Mode* ▾

Presentation

DefaultSource* ▾

Priority* ▾

Selfview

Default

FullscreenMode* ▾

Mode* ▾

OnMonitorRole* ▾

PIPPosition* ▾

OnCall

Duration

Mode* ▾

音声管理

General Settings

Wakeword Mode* ▾

Web エンジン

General Settings

Mode* ▾

RemoteDebugging* ▾

UseHttpProxy* ▾

MinimumTLSVersion* ▾

Webex

General Settings

Meetings JoinProtocol* ▼

CloudUpgrades Mode* ▼

CloudProximity

Mode* ▼

GuestShare* ▼

ルームクリーンアップ

AutoRun

HourOfDay

ContentType

Whiteboards* ▼

WebData* ▼

ブッキング

General Settings

ProtocolPriority* ▼

その他

General Settings

Configuration Control Mode* ▼ #

Room Name (from Exchange(R)) #

LoadServer #

Webex Devices Onboarding Token #

Admin username and password

Admin Username #

Admin Password #

Customization Provisioning

Customization File #

Customization Hash Type* ▼ #

Customization Hash #

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

Product Specific Configuration Layout

Parameter Value Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

Audio	<p>General Settings</p> <p>DefaultVolume <input type="text" value="50"/> #</p> <p>Input MicrophoneMode* <input type="text" value="Focused"/> ▾</p> <p>Ultrasound MaxVolume <input type="text" value="70"/></p> <p>USB Mode* <input type="text" value="SpeakerAndMicrophone"/> ▾</p> <p>Microphones</p> <p>Mute</p> <p>Enabled* <input type="text" value="True"/> ▾</p> <p>NoiseRemoval</p> <p>Mode* <input type="text" value="Manual"/> ▾</p> <p>SoundsAndAlerts</p> <p>RingTone <input type="text" value="Sunrise"/></p> <p>RingVolume <input type="text" value="50"/></p>
Bluetooth	
CallHistory	
Cameras	
Conference	
FacilityService	
HttpClient	
HttpFeedback	
Logging	
Macros	
NetworkServices	
Phonebook	
RoomAnalytics	
RoomScheduler	
SIP	
Security	
SerialPort	
Standby	
SystemUnit	
UserInterface	
Peripherals	
Proximity	
UserManagement	
Video	
VoiceControl	
WebEngine	
Webex	
RoomCleanup	
Bookings	
Miscellaneous	

音声

General Settings	
DefaultVolume	<input type="text" value="50"/> #
Input MicrophoneMode*	<input type="text" value="Focused"/> ▾
Ultrasound MaxVolume	<input type="text" value="70"/>
USB Mode*	<input type="text" value="SpeakerAndMicrophone"/> ▾

Microphones	
Mute	
Enabled*	<input type="text" value="True"/> ▾

NoiseRemoval	
Mode*	<input type="text" value="Manual"/> ▾

SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>

Bluetooth

General Settings	
Allowed*	<input type="text" value="True"/> ▾
Enabled*	<input type="text" value="False"/> ▾

通話履歴

General Settings	
Mode*	<input type="text" value="On"/> ▾ #

カメラ

Background	
Enabled*	<input type="text" value="True"/> ▾
UserImagesAllowed*	<input type="text" value="True"/> ▾
PowerLine Frequency*	<input type="text" value="Auto"/> ▾
SpeakerTrack Mode*	<input type="text" value="Auto"/> ▾

Camera	
Brightness	
DefaultLevel	<input type="text" value="20"/>
Mode*	<input type="text" value="Auto"/> ▾

ExposureCompensation	
Level	<input type="text" value="0"/>

会議

DefaultCall	
Protocol*	Sip #
Rate	6000
DoNotDisturb DefaultTimeout	60
Encryption Mode*	BestEffort
FarEndMessage Mode*	Off
MaxReceiveCallRate	6000
MaxTotalReceiveCallRate	6000 #
MaxTotalTransmitCallRate	6000 #
MaxTransmitCallRate	6000
MicUnmuteOnDisconnect Mode*	On #
Multipoint Mode*	Auto #

FarEndControl	
Mode*	On #
SignalCapability*	On #

ファシリティサービス

Service 1	
CallType*	Video #
Name	Live Support #
Number	#
Type*	Helpdesk #

Service 2	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 3	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 4	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 5	
CallType*	Video
Name	
Number	
Type*	Helpdesk

HTTP クライアント

General Settings	
Mode*	Off ▼
AllowInsecureHTTPS*	False ▼
AllowHTTP*	True ▼
UseHttpProxy*	On ▼

HTTP フィードバック

General Settings	
TlsVerify*	On ▼
UseHttpProxy*	On ▼

ロギング

General Settings	
CloudUpload Mode*	Off ▼
Internal Mode*	On ▼

External	
Mode*	Off ▼
Protocol*	SyslogTLS ▼
TlsVerify*	On ▼

Server	
Address	<input type="text"/>
Port	514

マクロ

General Settings	
AutoStart*	On ▼
Mode*	Off ▼
UnresponsiveTimeout	5 <input type="text"/>

ネットワーク サービス

General Settings

H323 Mode*	Off
UPnP Mode*	On
Websocket*	FollowHTTPService
WelcomeText*	On
Wifi Allowed*	True

HTTP

Mode*	Off	#
-------	-----	---

Proxy

Mode*	Off
Url	<input type="text"/>
LoginName	<input type="text"/>
PACUrl	<input type="text"/>

HTTPS

VerifyClientCertificate*	Off
StrictTransportSecurity*	Off

Server

MinimumTLSVersion*	TLSv1.1
--------------------	---------

SNMP

CommunityName	<input type="text"/>
Mode*	Off
SystemContact	<input type="text"/>
SystemLocation	<input type="text"/>

SSH

HostKeyAlgorithm*	RSA	
Mode*	Off	#

SMTP

Mode*	Off	#
Server	<input type="text"/>	#
Port	0	#
Security*	StartTls	#
Username	<input type="text"/>	#
From	<input type="text"/>	#

電話帳 (Phone Book)

Server 1

ID	<input type="text"/>	
Type*	CUCM	#
URL	<input type="text"/>	#
Pagination*	Enabled	
TlsVerify*	On	

Room 分析

General Settings	
PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation	
Mode*	Off
Interval	10

ReverberationTime	
Mode*	Off
Interval	1800

ルームスケジューラ

General Settings	
Enabled*	False

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0

セキュリティ

Audit	
Logging	
Mode*	Internal
OnError	
Action*	Ignore
Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off
Session	
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

General Settings	
BaudRate*	115200 ▼
LoginRequired*	On ▼ #
Mode*	On ▼ #

スタンバイ

General Settings	
BootAction*	DefaultCameraPosition ▼
Control*	On ▼ #
Delay	10 #
StandbyAction*	PrivacyPosition ▼ #
WakeupAction*	RestoreCameraPosition ▼
WakeupOnMotionDetection*	Off ▼ #

Signage	
Url	<input type="text"/>
Mode*	Off ▼
RefreshInterval	0
Audio*	Off ▼

システムユニット

General Settings	
CustomDeviceId	<input type="text"/>
Name	<input type="text"/> #

CrashReporting	
Mode*	Off ▼
URL	<input type="text"/> #

ユーザ インターフェイス

General Settings

Accessibility IncomingCallNotification*	Default	ⓘ
Bookings Visibility Title*	Auto	▼
ContactInfo Type*	Auto	▼
Diagnostics Notifications*	Auto	▼
Branding AwakeBranding Colors*	Auto	▼
KeyTones Mode*	On	▼
SoundEffects Mode*	On	▼
Proximity Notifications*	Auto	▼
CustomMessage		ⓘ
Whiteboard ActivityIndicators*	On	▼
Assistant Mode*	On	▼
Security Mode*	Normal	▼

Features

HideAll*	False	▼
----------	-------	---

Call

Start*	Auto	▼
MidCallControls*	Auto	▼
End*	Auto	▼
VideoMute*	Auto	▼
JoinWebex*	Auto	ⓘ
Keypad*	Auto	▼
MusicMode*	Hidden	▼

Share

Start*	Auto	▼
--------	------	---

Whiteboard

Start*	Auto	▼
--------	------	---

OSD

EncryptionIndicator*	Auto	ⓘ
Output*	1	▼
HalfwakeMessage		
Mode*	Auto	▼

Phonebook

Mode*	ReadWrite	▼
DefaultSearchFilter*	All	▼

SettingsMenu

Mode*	Unlocked	ⓘ
Visibility*	Auto	▼

周辺機器

General Settings

InputDevice Mode*	Off	▼
Pairing CiscoTouchPanels RemotePairing*	On	▼

Profile

TouchPanels*	0	▼
Cameras*	Minimum1	▼
ControlSystems*	NotSet	▼

プロキシミティ

General Settings	
Mode*	Off <input type="button" value="v"/> #
AlternatePort Enabled*	False <input type="button" value="v"/>

Services	
ContentShare	
ToClients*	Disabled <input type="button" value="v"/> #
FromClients*	Enabled <input type="button" value="v"/> #
CallControl*	Disabled <input type="button" value="v"/> #

ユーザー管理

LDAP	
Mode*	Off <input type="button" value="v"/> #
Encryption*	LDAPS <input type="button" value="v"/> #
VerifyServerCertificate*	Off <input type="button" value="v"/> #
BaseDN	<input type="text"/> #
Attribute	<input type="text"/> #
MinimumTLSVersion*	TLSv1.2 <input type="button" value="v"/> #

Server	
Address	<input type="text"/> #
Port	0 <input type="text"/> #

Admin	
Group	<input type="text"/> #
Filter	<input type="text"/> #

PasswordPolicy	
ReuseLimit	<input type="text" value="12"/>
MaxLifetime	<input type="text" value="0"/>

Complexity	
MinimumLength	<input type="text" value="8"/>
MinimumUppercase	<input type="text" value="0"/>
MinimumLowercase	<input type="text" value="0"/>
MinimumDigits	<input type="text" value="0"/>
MinimumSpecial	<input type="text" value="0"/>

ビデオ

Input

Connector 1

InputSourceType* camera

Name Camera

Visibility* Never

CameraControl

CameraId* 1

Mode* On

Connector 2

InputSourceType* PC

Name PC (USB-C)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 1920_1080_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Connector 3

InputSourceType* PC

Name PC (HDMI)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 1920_1080_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Monitors* Auto

Output Connector 1 Resolution* 1920_1080_60

DefaultMainSource* 1

Presentation	
DefaultSource*	2
Priority*	Equal

Selfview	
Default	
FullscreenMode*	Current
Mode*	Current
OnMonitorRole*	Current
PIPPosition*	Current
OnCall	
Duration	10
Mode*	Off

音声管理

General Settings	
Wakeword Mode*	On

Web エンジン

General Settings	
Mode*	Off
RemoteDebugging*	Off
UseHttpProxy*	On
MinimumTLSVersion*	TLSv1.1

Webex

General Settings	
Meetings JoinProtocol*	SIP
CloudUpgrades Mode*	Off

CloudProximity	
Mode*	Off
GuestShare*	Auto

ルームクリーンアップ

AutoRun	
HourOfDay	0
ContentType	
Whiteboards*	Daily
WebData*	Daily

ブッキング

General Settings

ProtocolPriority* ▾

その他

General Settings

Configuration Control Mode* ▾ #

Room Name (from Exchange(R))

LoadServer

Webex Devices Onboarding Token

Admin username and password

Admin Username

Admin Password

Customization Provisioning


Customization File

Customization Hash Type* ▾ #

Customization Hash

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

Product Specific Configuration Layout

 **Parameter Value** Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

Audio

Bluetooth

CallHistory

Cameras

Conference

FacilityService

HttpClient

HttpFeedback

Logging

Macros

NetworkServices

General Settings

DefaultVolume #

Input MicrophoneMode* ▾

Ultrasound MaxVolume

USB Mode* ▾

Microphones

Mute

Enabled* ▾

NoiseRemoval

Mode* ▾

SoundsAndAlerts

RingTone

RingVolume

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

音声

General Settings	
DefaultVolume	<input type="text" value="50"/> #
Input MicrophoneMode*	<input type="text" value="Focused"/> ▾
Ultrasound MaxVolume	<input type="text" value="70"/>
USB Mode*	<input type="text" value="SpeakerAndMicrophone"/> ▾
Microphones	
Mute	
Enabled*	<input type="text" value="True"/> ▾
NoiseRemoval	
Mode*	<input type="text" value="Manual"/> ▾
SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>

Bluetooth

General Settings	
Allowed*	True
Enabled*	False

通話履歴

General Settings	
Mode*	On

カメラ

Background	
Enabled*	True
UserImagesAllowed*	True
PowerLine Frequency*	Auto

Camera	
Brightness	
DefaultLevel	20
Mode*	Auto
ExposureCompensation	
Level	0

SpeakerTrack	
Mode*	Auto
TrackingMode*	Auto
Closeup*	Auto
Whiteboard	
Mode*	Off
ConnectorDetection	
Mode*	Auto
CameraRight	2
CameraLeft	1

会議

DefaultCall	
Protocol*	Sip #
Rate	6000
DoNotDisturb DefaultTimeout	60
Encryption Mode*	BestEffort
FarEndMessage Mode*	Off
MaxReceiveCallRate	6000
MaxTotalReceiveCallRate	6000 #
MaxTotalTransmitCallRate	6000 #
MaxTransmitCallRate	6000
MicUnmuteOnDisconnect Mode*	On #
Multipoint Mode*	Auto #

FarEndControl	
Mode*	On #
SignalCapability*	On #

ファシリティサービス

Service 1	
CallType*	Video #
Name	Live Support #
Number	#
Type*	Helpdesk #

Service 2	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 3	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 4	
CallType*	Video
Name	
Number	
Type*	Helpdesk

Service 5	
CallType*	Video
Name	
Number	
Type*	Helpdesk

HTTP クライアント

General Settings	
Mode*	Off ▼
AllowInsecureHTTPS*	False ▼
AllowHTTP*	True ▼
UseHttpProxy*	On ▼

HTTP フィードバック

General Settings	
TlsVerify*	On ▼
UseHttpProxy*	On ▼

ロギング

General Settings	
CloudUpload Mode*	Off ▼
Internal Mode*	On ▼

External	
Mode*	Off ▼
Protocol*	SyslogTLS ▼
TlsVerify*	On ▼

Server	
Address	<input type="text"/>
Port	514

マクロ

General Settings	
AutoStart*	On ▼
Mode*	Off ▼
UnresponsiveTimeout	5 <input type="text"/>

ネットワーク サービス

General Settings

H323 Mode*	Off
UPnP Mode*	On
Websocket*	FollowHTTPService
WelcomeText*	On
Wifi Allowed*	True

HTTP

Mode*	Off	#
-------	-----	---

Proxy

Mode*	Off
Url	<input type="text"/>
LoginName	<input type="text"/>
PACUrl	<input type="text"/>

HTTPS

VerifyClientCertificate*	Off
StrictTransportSecurity*	Off

Server

MinimumTLSVersion*	TLSv1.1
--------------------	---------

SNMP

CommunityName	<input type="text"/>
Mode*	Off
SystemContact	<input type="text"/>
SystemLocation	<input type="text"/>

SSH

HostKeyAlgorithm*	RSA	
Mode*	Off	#

SMTP

Mode*	Off	#
Server	<input type="text"/>	#
Port	0	#
Security*	StartTls	#
Username	<input type="text"/>	#
From	<input type="text"/>	#

電話帳 (Phone Book)

Server 1

ID	<input type="text"/>	
Type*	CUCM	#
URL	<input type="text"/>	#
Pagination*	Enabled	
TlsVerify*	On	

Room 分析

General Settings	
PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation	
Mode*	Off
Interval	10

ReverberationTime	
Mode*	Off
Interval	1800

ルームスケジューラ

General Settings	
Enabled*	False

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0

セキュリティ

Audit	
Logging	
Mode*	Internal
OnError	
Action*	Ignore
Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off
Session	
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

シリアルポート

General Settings	
BaudRate*	115200 ▼
LoginRequired*	On ▼ #
Mode*	On ▼ #

スタンバイ

General Settings	
BootAction*	DefaultCameraPosition ▼
Control*	On ▼ #
Delay	10 #
StandbyAction*	PrivacyPosition ▼ #
WakeupAction*	RestoreCameraPosition ▼
WakeupOnMotionDetection*	Off ▼ #

Signage	
Url	<input type="text"/>
Mode*	Off ▼
RefreshInterval	0
Audio*	Off ▼

システムユニット

General Settings	
CustomDeviceId	<input type="text"/>
Name	<input type="text"/> #

CrashReporting	
Mode*	Off ▼
URL	<input type="text"/> #

ユーザ インターフェイス

General Settings

Accessibility IncomingCallNotification*	Default	ⓘ
Bookings Visibility Title*	Auto	▼
ContactInfo Type*	Auto	▼
Diagnostics Notifications*	Auto	▼
Branding AwakeBranding Colors*	Auto	▼
KeyTones Mode*	On	▼
SoundEffects Mode*	On	▼
Proximity Notifications*	Auto	▼
CustomMessage		ⓘ
Whiteboard ActivityIndicators*	On	▼
Assistant Mode*	On	▼
Security Mode*	Normal	▼

Features

HideAll*	False	▼
----------	-------	---

Call

Start*	Auto	▼
MidCallControls*	Auto	▼
End*	Auto	▼
VideoMute*	Auto	▼
JoinWebex*	Auto	ⓘ
Keypad*	Auto	▼
MusicMode*	Hidden	▼

Share

Start*	Auto	▼
--------	------	---

Whiteboard

Start*	Auto	▼
--------	------	---

OSD

EncryptionIndicator*	Auto	ⓘ
Output*	1	▼
HalfwakeMessage		
Mode*	Auto	▼

Phonebook

Mode*	ReadWrite	▼
DefaultSearchFilter*	All	▼

SettingsMenu

Mode*	Unlocked	ⓘ
Visibility*	Auto	▼

周辺機器

General Settings

InputDevice Mode*	Off	▼
Pairing CiscoTouchPanels RemotePairing*	On	▼

Profile

TouchPanels*	0	▼
Cameras*	Minimum1	▼
ControlSystems*	NotSet	▼

プロキシミティ

General Settings	
Mode*	Off <input type="button" value="v"/> #
AlternatePort Enabled*	False <input type="button" value="v"/>

Services	
ContentShare	
ToClients*	Disabled <input type="button" value="v"/> #
FromClients*	Enabled <input type="button" value="v"/> #
CallControl*	Disabled <input type="button" value="v"/> #

ユーザー管理

LDAP	
Mode*	Off <input type="button" value="v"/> #
Encryption*	LDAPS <input type="button" value="v"/> #
VerifyServerCertificate*	Off <input type="button" value="v"/> #
BaseDN	<input type="text"/> #
Attribute	<input type="text"/> #
MinimumTLSVersion*	TLSv1.2 <input type="button" value="v"/> #

Server	
Address	<input type="text"/> #
Port	0 <input type="text"/> #

Admin	
Group	<input type="text"/> #
Filter	<input type="text"/> #

PasswordPolicy	
ReuseLimit	<input type="text" value="12"/>
MaxLifetime	<input type="text" value="0"/>

Complexity	
MinimumLength	<input type="text" value="8"/>
MinimumUppercase	<input type="text" value="0"/>
MinimumLowercase	<input type="text" value="0"/>
MinimumDigits	<input type="text" value="0"/>
MinimumSpecial	<input type="text" value="0"/>

ビデオ

Input

Connector 1

InputSourceType* camera

Name Camera

Visibility* Never

CameraControl

CameraId* 1

Mode* On

Connector 2

InputSourceType* PC

Name PC (USB-C)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 1920_1080_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Monitors* Auto

Output Connector 1 Resolution* 1920_1080_60

DefaultMainSource* 1

Presentation

DefaultSource* 2

Priority* Equal

Selfview

Default

FullscreenMode* Current

Mode* Current

OnMonitorRole* Current

PIPPosition* Current

OnCall

Duration 10

Mode* Off

音声管理

General Settings

Wakeword Mode* On

Web エンジン

General Settings

Mode*	Off
RemoteDebugging*	Off
UseHttpProxy*	On
MinimumTLSVersion*	TLSv1.1

Webex

General Settings

Meetings JoinProtocol*	SIP
CloudUpgrades Mode*	Off

CloudProximity

Mode*	Off
GuestShare*	Auto

ルームクリーンアップ

AutoRun

HourOfDay	0
-----------	---

ContentType

Whiteboards*	Daily
WebData*	Daily

ブッキング

General Settings

ProtocolPriority*	Auto
-------------------	------

その他

General Settings

Configuration Control Mode*	Unified CM and Endpoint
Room Name (from Exchange(R))	
LoadServer	
Webex Devices Onboarding Token	

Admin username and password

Admin Username	admin
Admin Password	

Customization Provisioning

Customization File	
Customization Hash Type*	SHA512
Customization Hash	

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

Cisco RoomOS Series および Cisco Unified Communications Manager で使用される TCP ポートおよび UDP ポートの詳細については、次の URL にある『**Cisco Unified Communications Manager TCP and UDP Port Usage**』を参照してください。

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

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

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

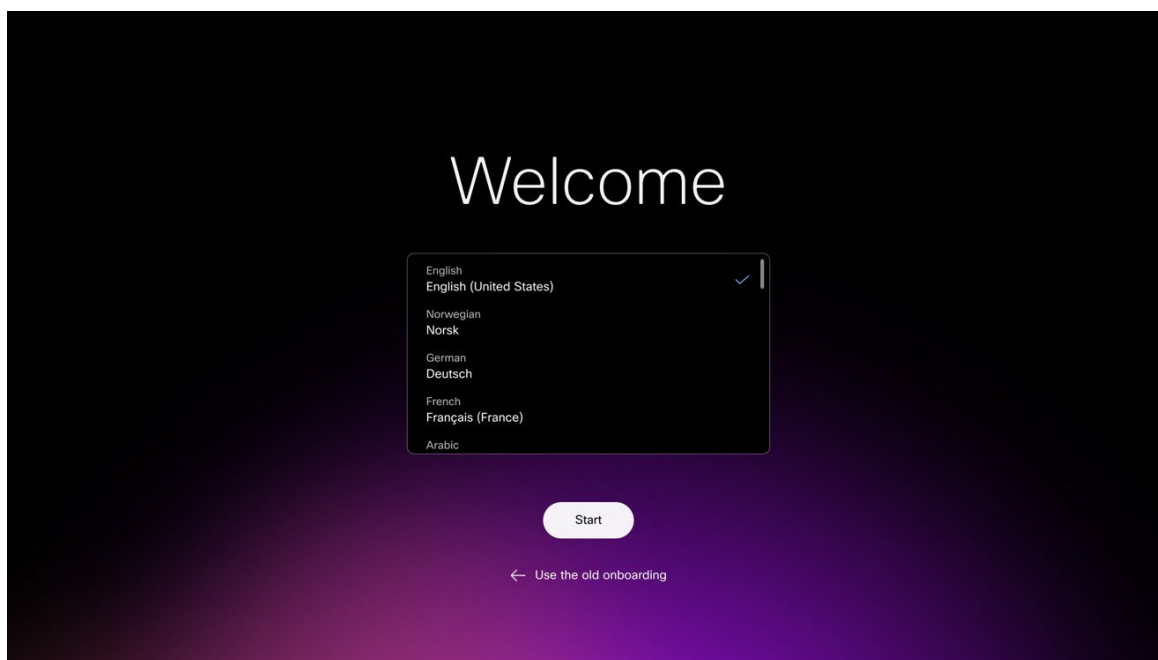
Cisco RoomOS シリーズの構成

Cisco RoomOS Series を構成するには、ローカル ユーザー インターフェイスを使用します。

Wi-Fi プロファイルの構成

ローカル ユーザー インターフェイスを介して Wi-Fi ネットワークを手動で設定するには、次のガイドラインを使用します。

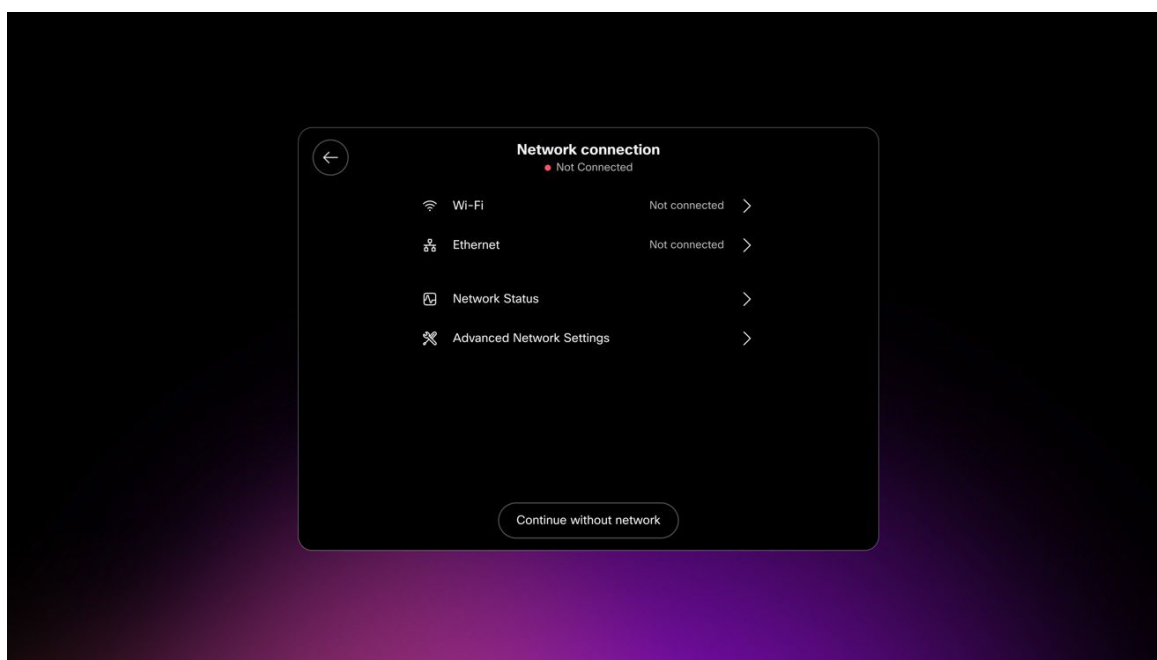
- すぐに使用できる（工場出荷時の状態にリセットされた）Cisco RoomOS Series の場合、スタートアップ ウィザードを使用して Wi-Fi ネットワークを構成します。



- 構成オプションは、ブロードキャストされた Wi-Fi ネットワークが構成されているか、Wi-Fi ネットワークが手動で構成されているかによって決まります。
- 次に、サポートされる利用可能なセキュリティモードと、各モードで使用できるキー管理および暗号化タイプを示します。
キー管理および暗号化タイプ（暗号化方式）は、アクセスポイントの現在の設定に基づいて自動構成されます。有効になっている最も強力なキー管理タイプ（WPA3 など）がまず優先され、次に有効になっている最も強力な暗号化方式（AES など）が優先されます。

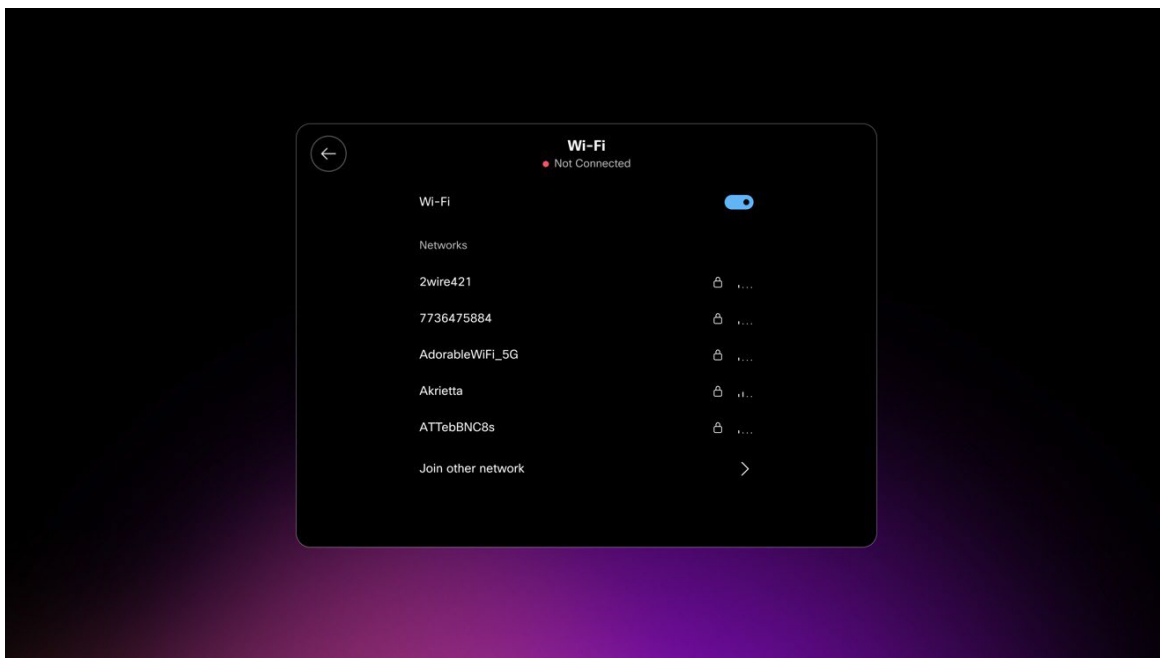
セキュリティ	802.1x タイプ	キーの管理	暗号化
なし	該当なし	なし	なし
個人	該当なし	WPA3-SAE WPA2-PSK-SHA256 WPA2-PSK	AES TKIP
エンタープライズ	FAST PEAP TLS TTLS	WPA3-802.1X-SHA256 WPA2-802.1X-SHA256 WPA2-802.1X	AES TKIP

- [Wi-Fi] を選択して Wi-Fi ネットワークを構成します。

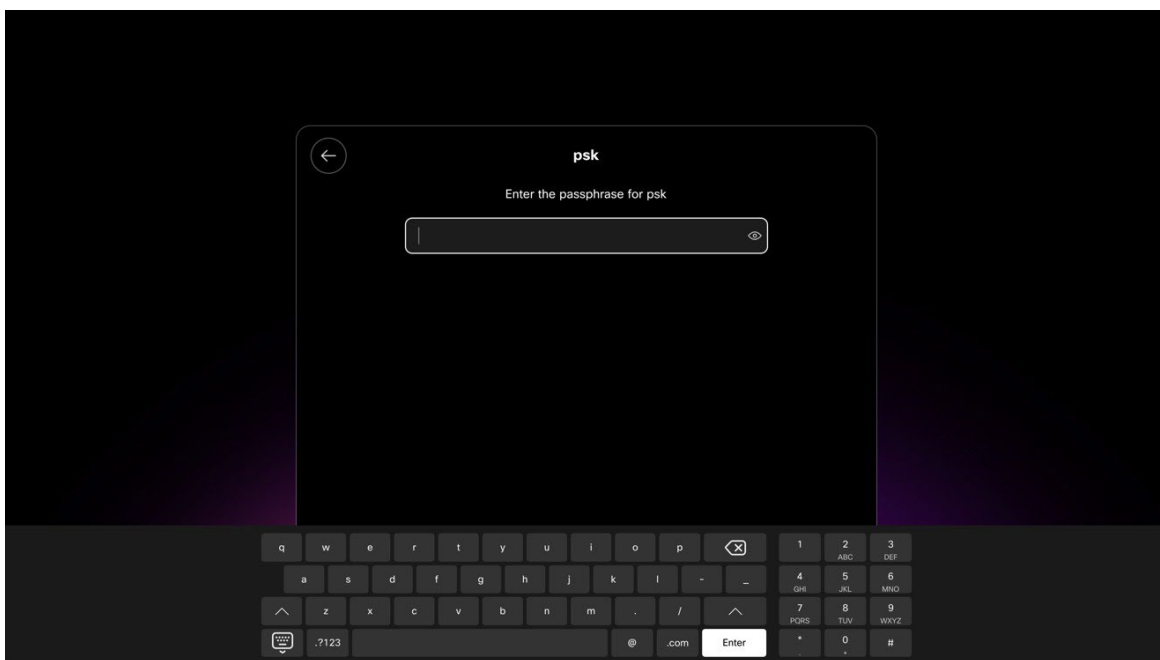


ブロードキャスト Wi-Fi ネットワークの設定

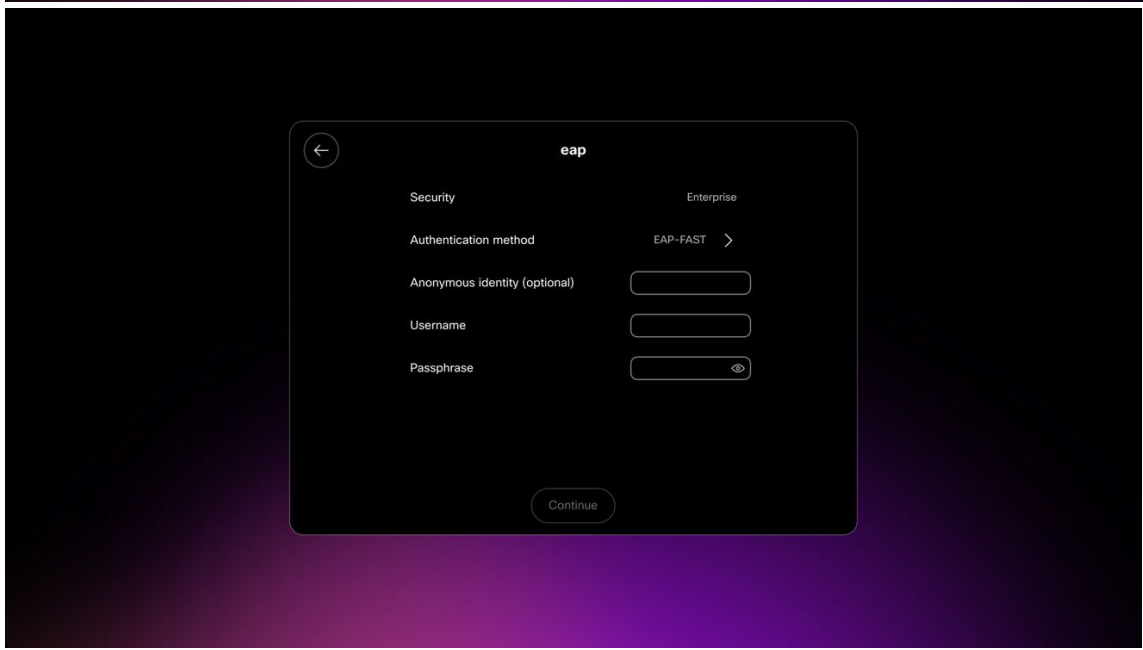
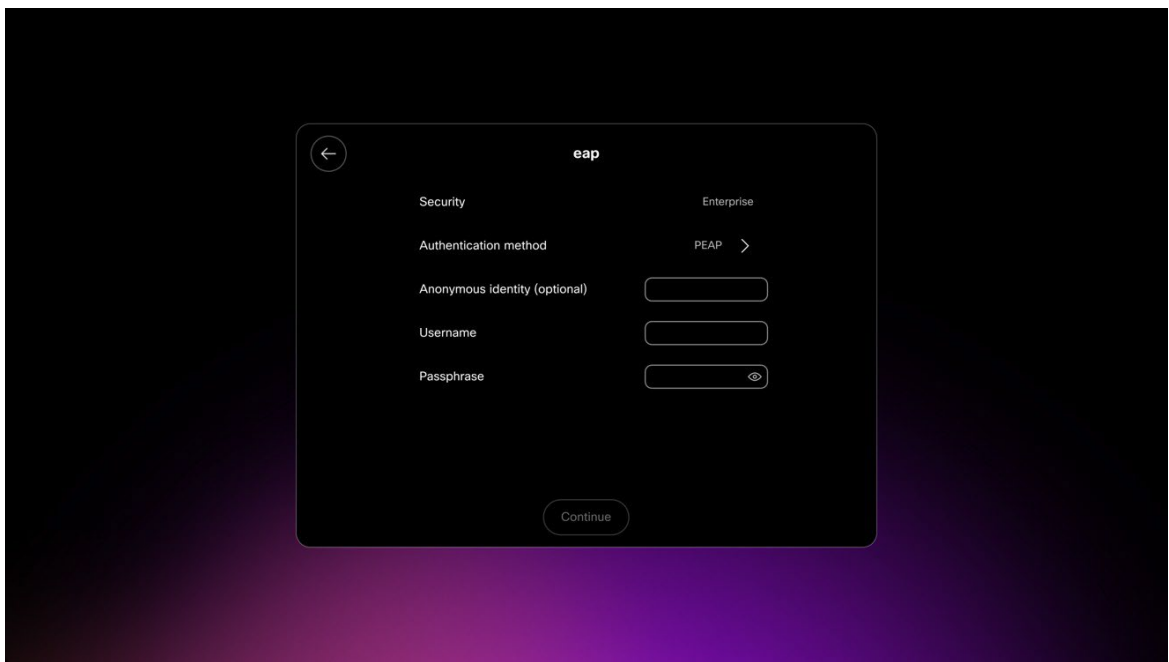
- Wi-Fi ネットワークがブロードキャストされている場合は、リストから目的の Wi-Fi ネットワークを選択し、Wi-Fi ネットワークのセキュリティ設定に応じて必要なログイン情報を入力します。

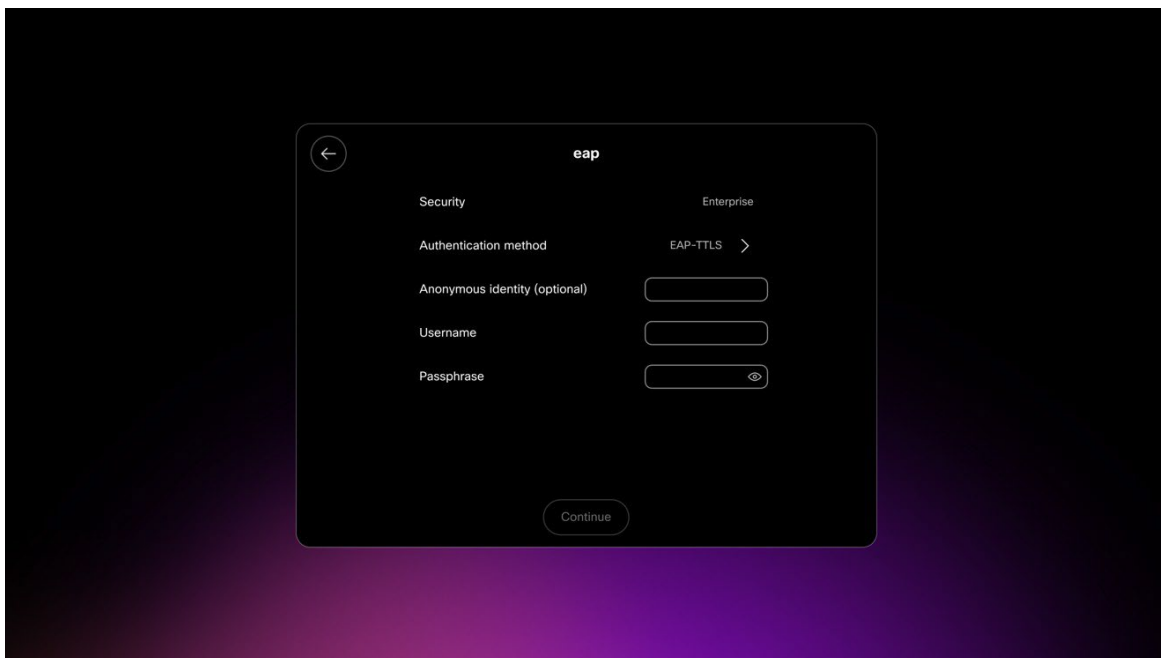


- オープン Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックするだけです。
- PSK 対応の Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックし、8～63 文字の ASCII、または 64 桁の 16 進パスワードを入力します。

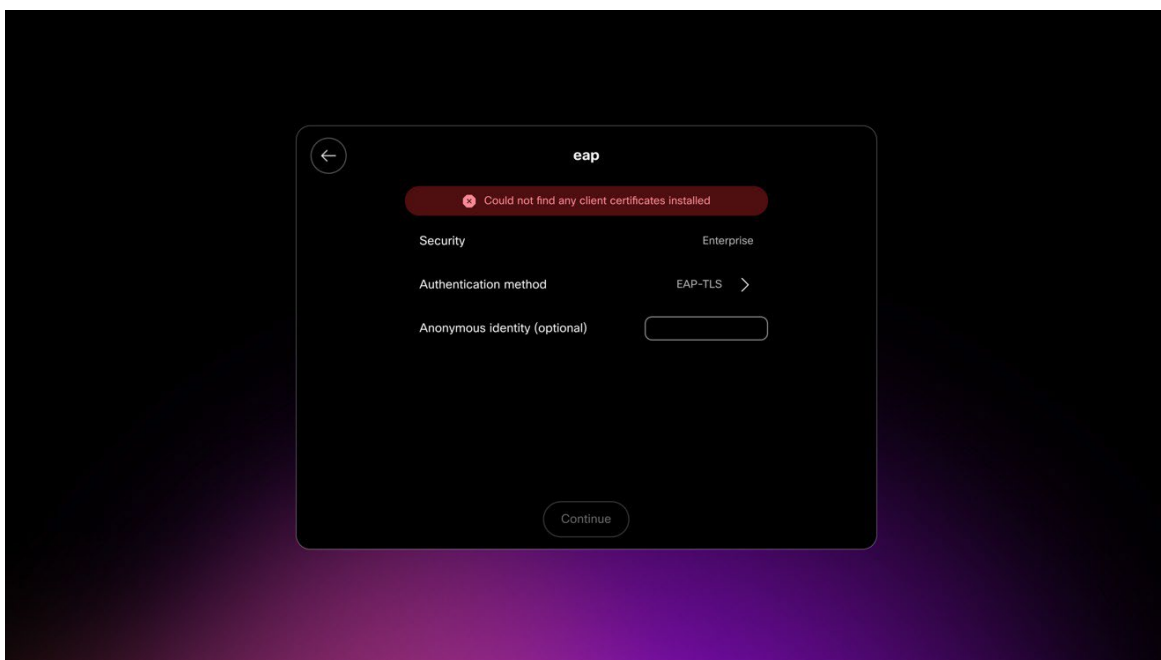


- EAP 対応 Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックしてから、**[認証方式 (Authentication method)]** を選択します。
- PEAP、EAP-FAST (FAST)、または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、**[ユーザー名 (Username)]** と **[パスワード (Password)]** を入力します。



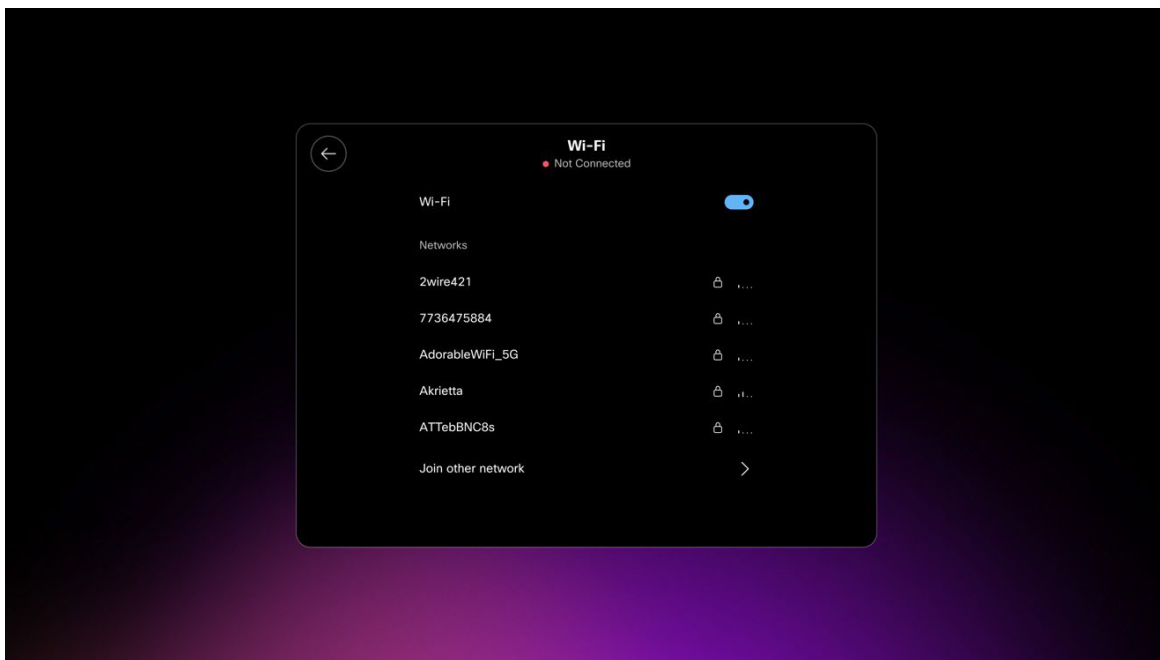


- EAP-TLS (TLS) Wi-Fi ネットワークを構成する場合は、デバイスの Web ページから適切なユーザー証明書と CA 証明書がインストールされていることを確認する必要があります。

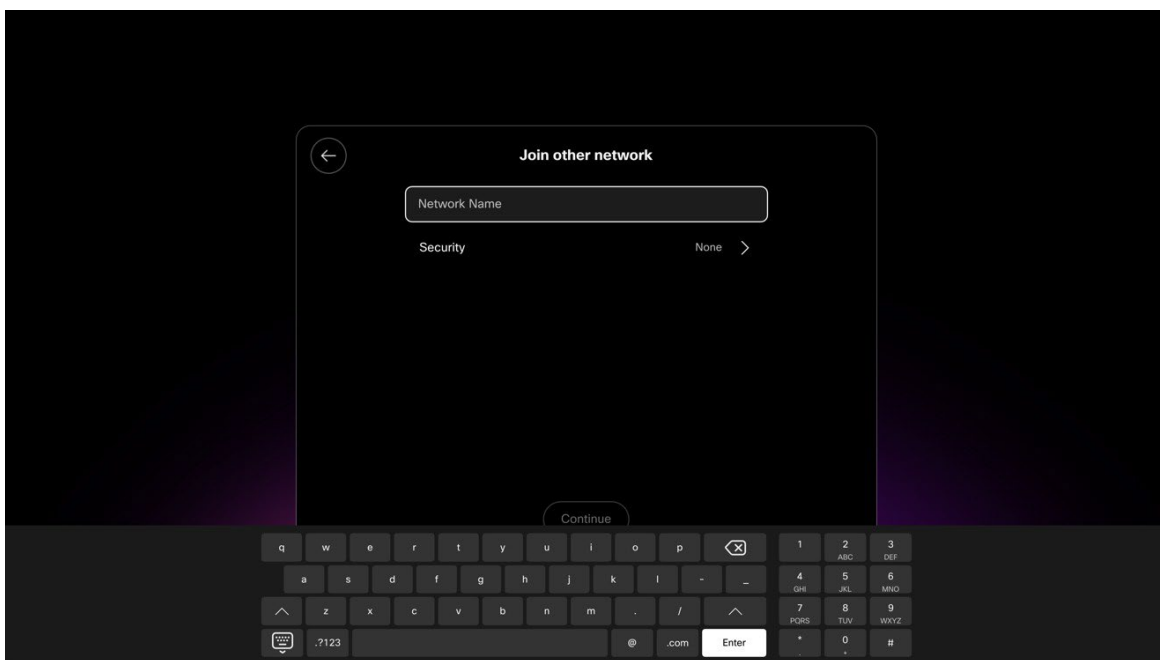


非ブロードキャスト Wi-Fi ネットワークの設定

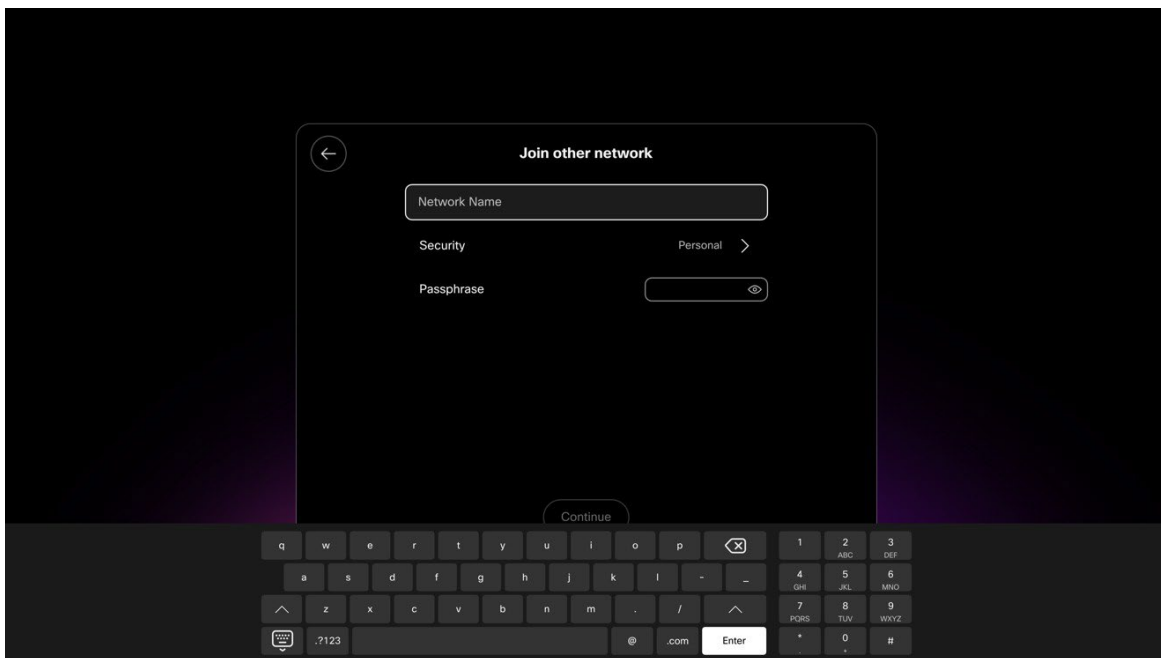
- 非ブロードキャスト（非表示） Wi-Fi ネットワークを手動で構成する場合は、**[他のネットワークに参加]** を選択します。
- 次に、**ネットワーク名 (SSID)**、**セキュリティタイプ**を設定し、Wi-Fi ネットワークのセキュリティ設定に応じて必要なログイン情報を入力します。



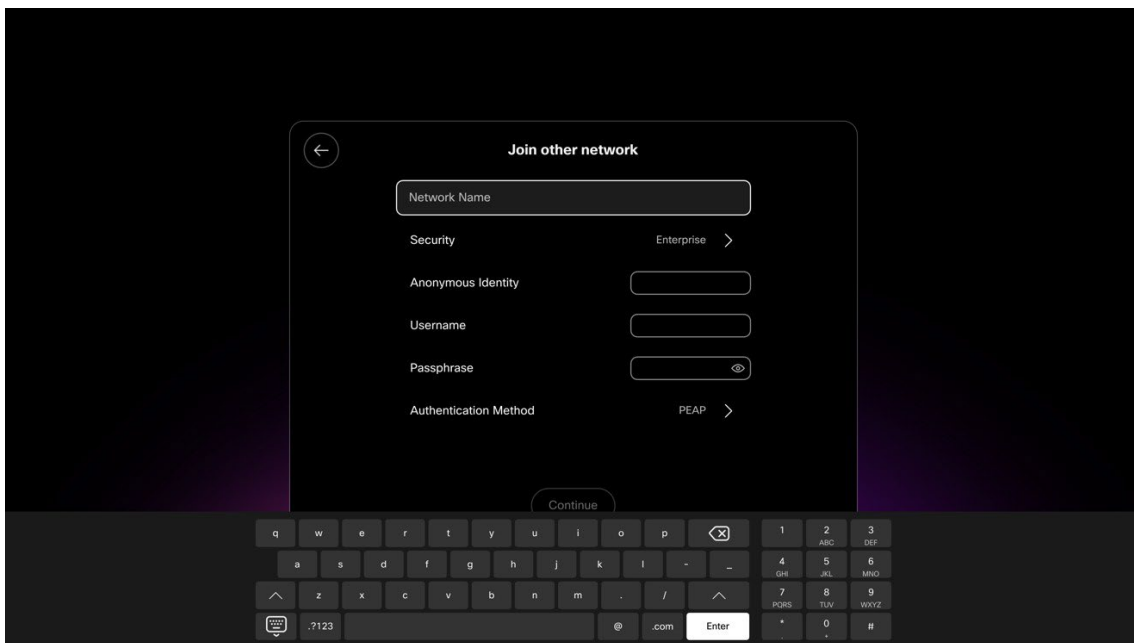
- オープン Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [なし (None)] に設定します。

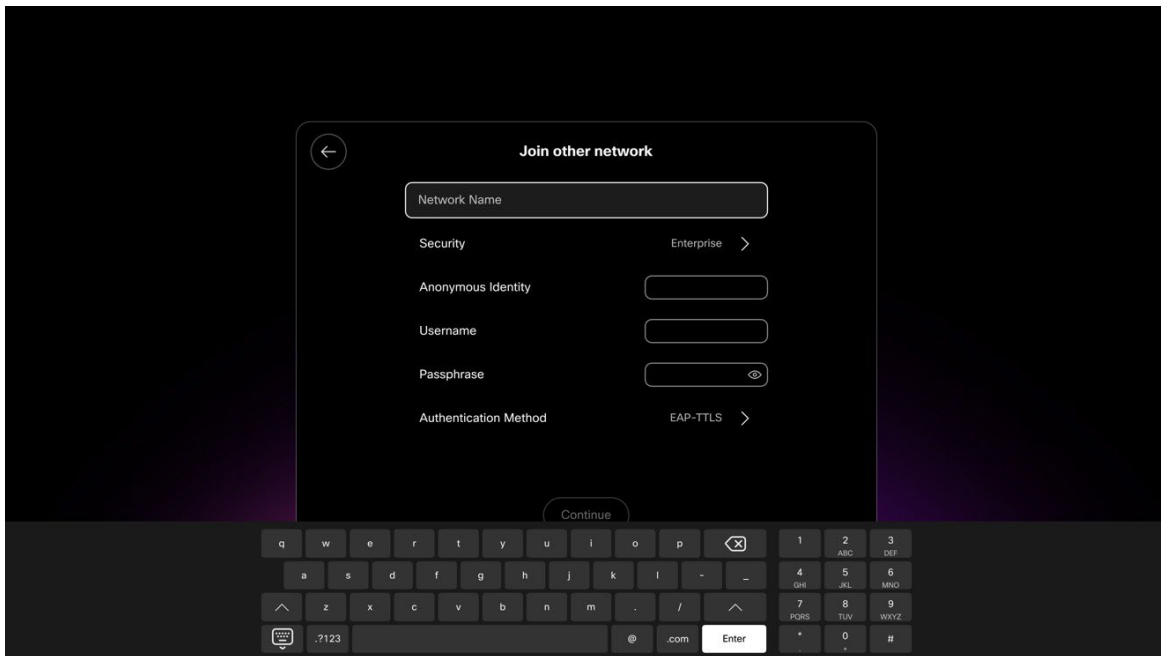
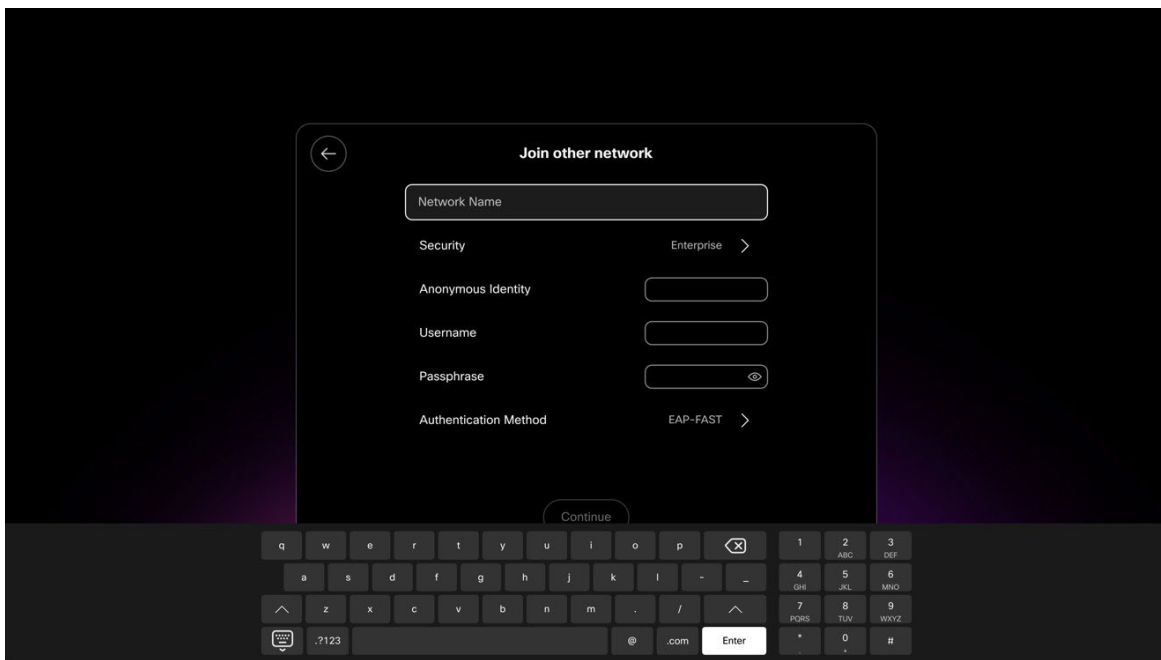


- PSK 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)] を [パーソナル (Personal)] に設定してから、8～63 文字の ASCII または 64 桁の 16 進パスワードを入力します。

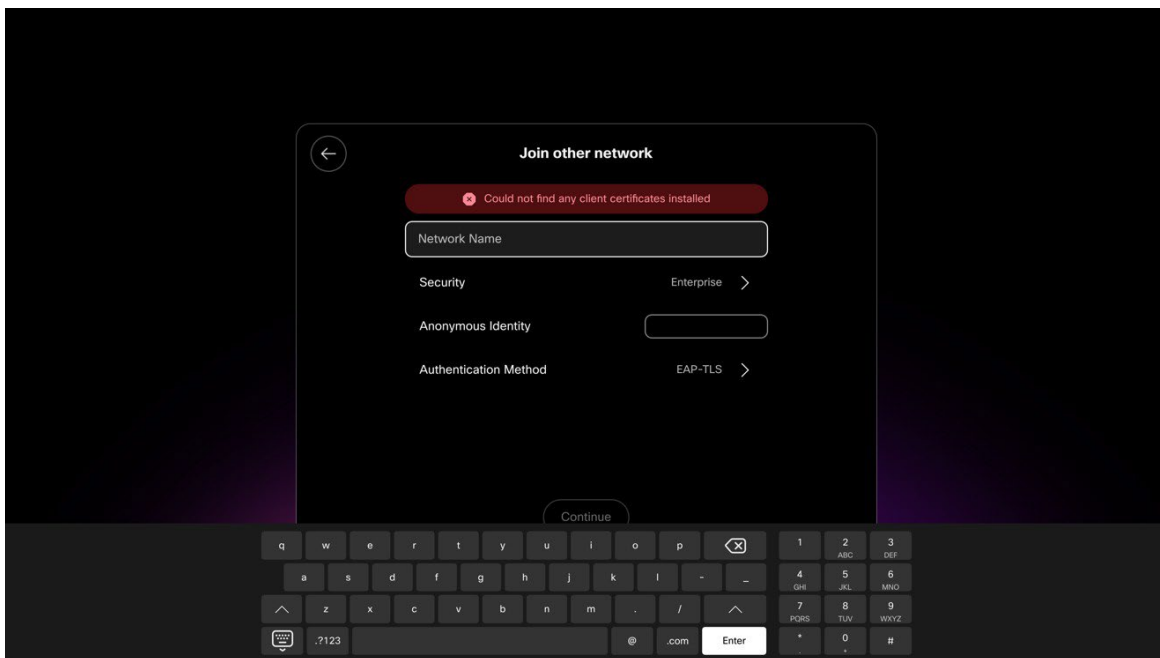


- EAP 対応の Wi-Fi ネットワークに接続するには、**ネットワーク名**を入力し、**[セキュリティ (Security)]**を**[エンタープライズ (Enterprise)]**に設定してから、**[認証方式 (Authentication method)]**を選択します。
- PEAP、EAP-FAST (FAST)、または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、**[ユーザー名 (Username)]**と**[パスフレーズ (Passphrase)]**を入力します。



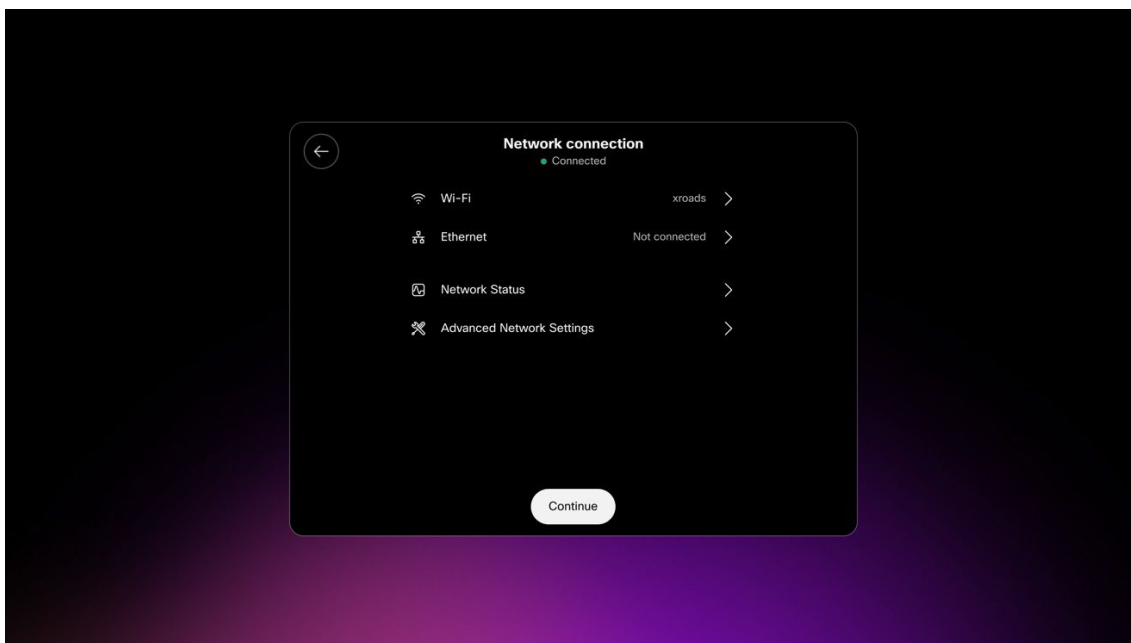


- EAP-TLS (TLS) Wi-Fi ネットワークを構成する場合は、デバイスの Web ページから適切なユーザー証明書と CA 証明書がインストールされていることを確認する必要があります。



Wi-Fi ネットワークの詳細オプションの設定

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



← **Advanced network settings** Apply

IP Stack

IPv4 and IPv6

IPv4

IPv6

DNS

DNS Domain Name

DNS address 1

DNS address 2

DNS address 3

← **Advanced network settings** Apply

DNS Domain Name

DNS address 1

DNS address 2

DNS address 3

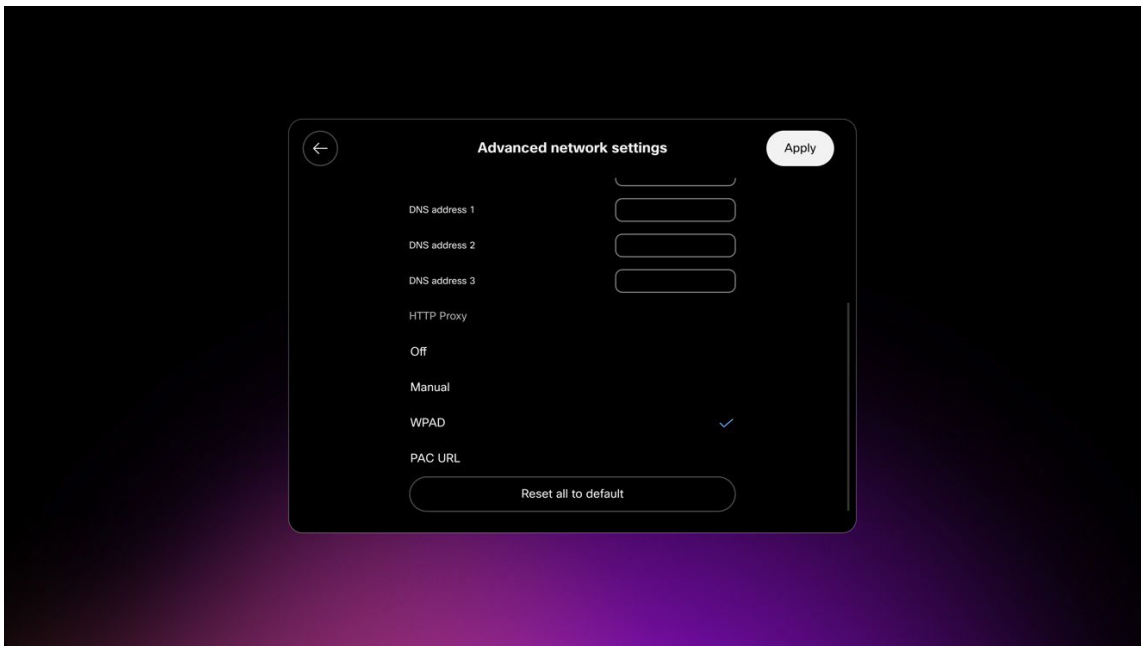
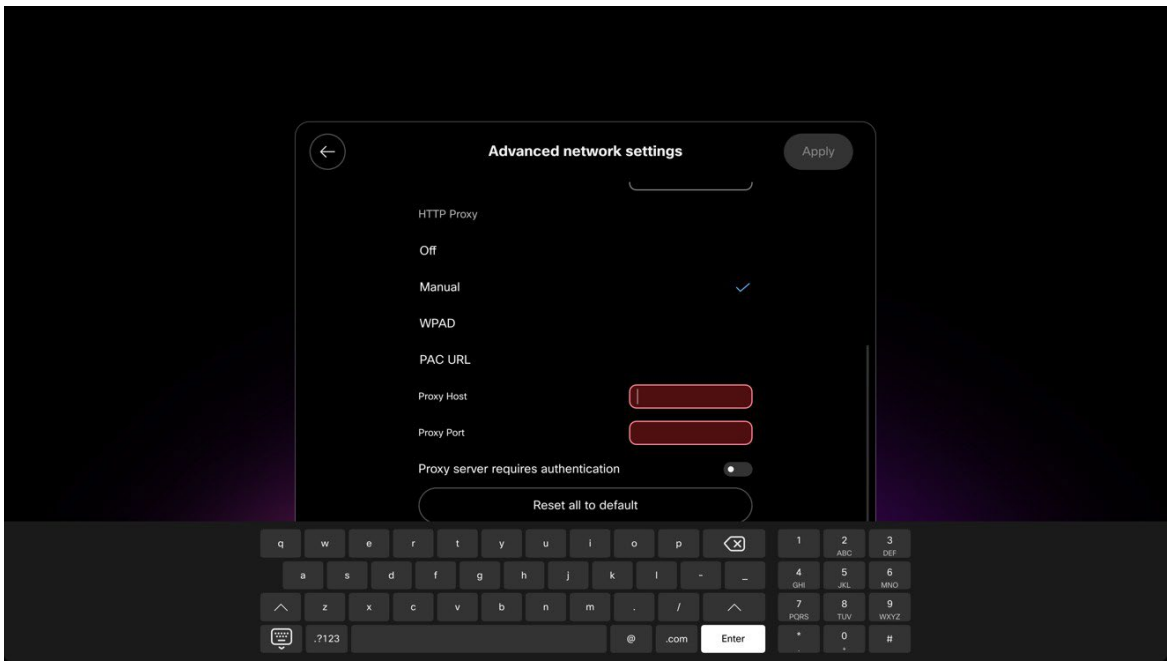
HTTP Proxy

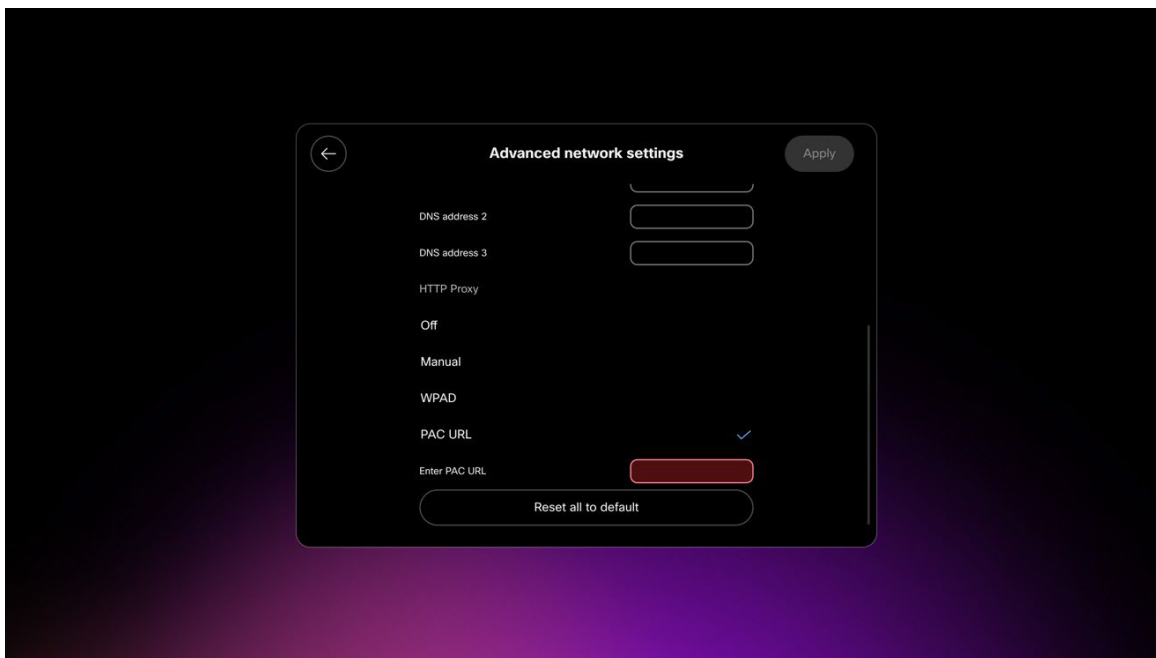
Off

Manual

WPAD

PAC URL





注：TKIP はブロードキャスト/マルチキャスト暗号としてしか使用できないため、アクセスポイントは AES (CCMP128) をサポートしている必要があります。CCMP256、GCMP128、および GCMP256 暗号化方式はサポートされていません。

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

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

証明書の管理

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

EAP-TLS を使用する場合は、日付と時刻が正しく設定されていることを確認する必要があります。

クライアント証明書とサーバー証明書には、**Base-64 (PEM)** エンコードのみを使用できます (DER エンコードはサポートされていません)。キー サイズが 1024、2048、および 4096 の証明書がサポートされます。

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

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

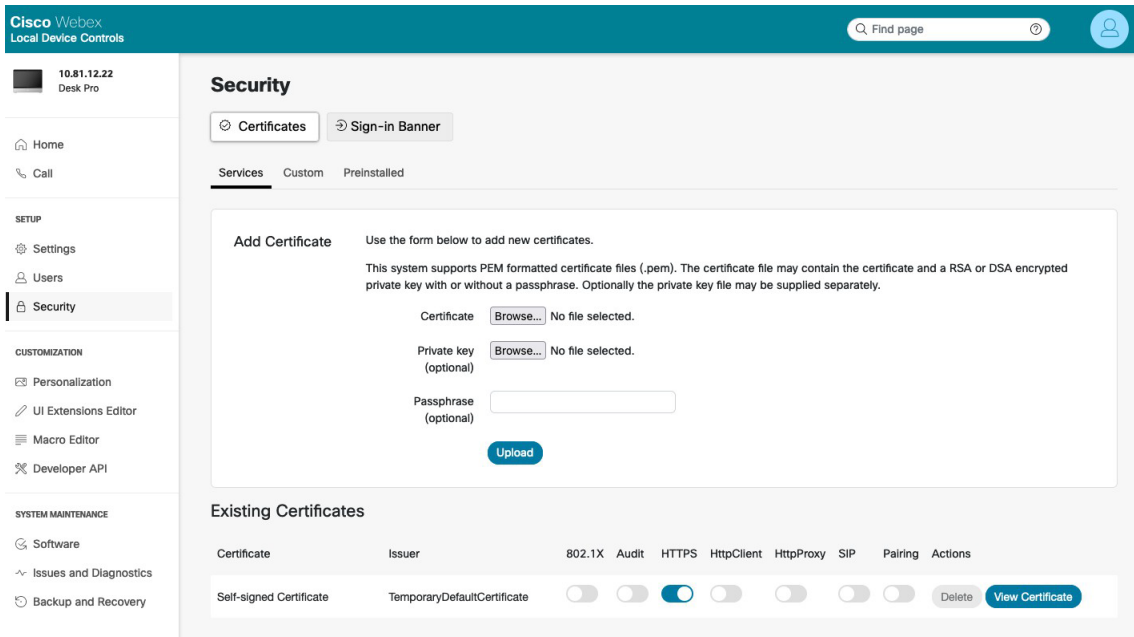
Microsoft® 認証局 (CA) サーバを使用することを推奨します。他の CA サーバータイプは Cisco RoomOS Series との完全な相互運用性がない場合があります。

証明書のインストール

Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

証明書は、Cisco RoomOS Series の Web ページからインストールできます。自動証明書の登録は現在サポートされていません。

Cisco RoomOS シリーズの Web ページから証明書をインストールするには、[セキュリティ (Security)] > [証明書 (Certificates)] を選択し、[サービス (Services)] または [カスタム (Custom)] を選択します。どちらを選択するかは、ユーザー証明書またはサーバー証明書 (ルート CA) をインストールするかどうかに応じて異なります。



EAP-TLS を利用するには、ユーザー証明書をインストールする必要があります。

必要に応じて、秘密キーを証明書と一緒にアップロードできます。証明書とキーを抽出するには、パスワードの入力が必要になる場合があります。

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

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

ユーザー証明書を発行した CA チェーンが RADIUS サーバの信頼リストに追加されたことを確認します。



10.81.12.22
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Security

Certificates

Sign-in Banner

Services Custom Preinstalled

Add Certificate

Use the form below to add new certificates.

This system supports PEM formatted certificate files (.pem). The certificate file may contain the certificate and a RSA or DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.

Certificate No file selected.

Private key (optional) No file selected.

Passphrase (optional)

Existing Certificates

Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	HttpProxy	SIP	Pairing	Actions
Self-signed Certificate	TemporaryDefaultCertificate	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete <input type="button" value="View Certificate"/>
sep689e0bb0000d.cisco.com	Cisco Systems Inc.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete <input type="button" value="View Certificate"/>

RADIUS サーバーの証明書を発行したルート CA の証明書は、**EAP-FAST**、**EAP-TLS**、**EAP-TTLS**、または **PEAP** サーバー検証を有効にするためにインストールする必要があります。

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

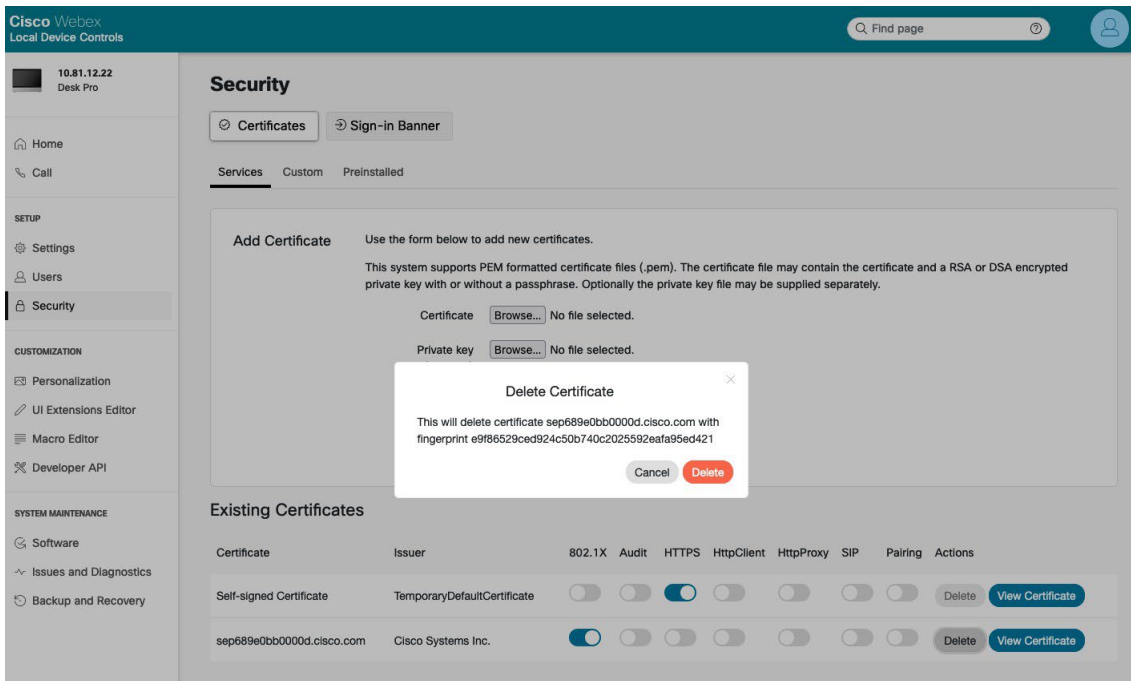
The screenshot displays the Cisco Webex Local Device Controls interface. The top navigation bar includes the Cisco Webex logo, 'Local Device Controls', a search bar, and a user profile icon. The left sidebar lists various system settings categories: Home, Call, SETUP (Settings, Users, Security), CUSTOMIZATION (Personalization, UI Extensions Editor, Macro Editor, Developer API), and SYSTEM MAINTENANCE (Software, Issues and Diagnostics, Backup and Recovery). The main content area is titled 'Security' and contains two tabs: 'Certificates' and 'Sign-in Banner'. Under 'Certificates', there are three sub-tabs: 'Services', 'Custom', and 'Preinstalled'. The 'Custom' sub-tab is selected, showing a section for 'Add Certificate Authority'. This section includes instructions to use the form to add new certificate authorities and notes that the system supports PEM formatted files (.pem). A 'Browse...' button is present, with the text 'No file selected.' below it. Below the form is a table titled 'Existing Certificate Authorities' with the following structure:

Certificate	Issuer	Details	Actions
IdenTrust Commercial Root CA 1	IdenTrust	View	Delete

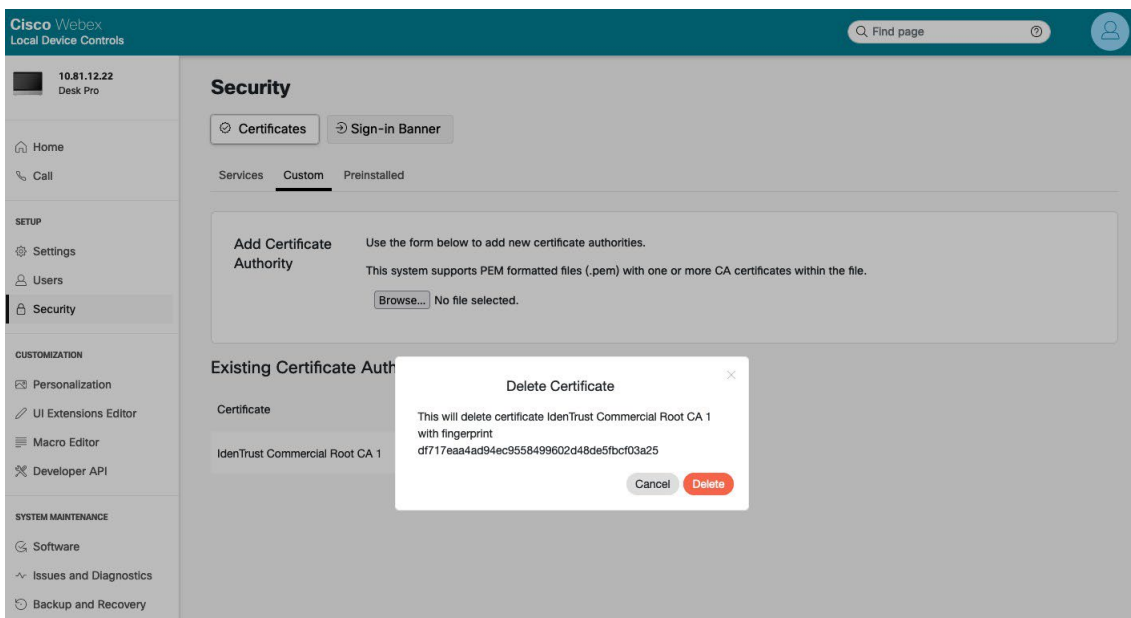
証明書の削除

証明書は個別に削除できます。

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



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



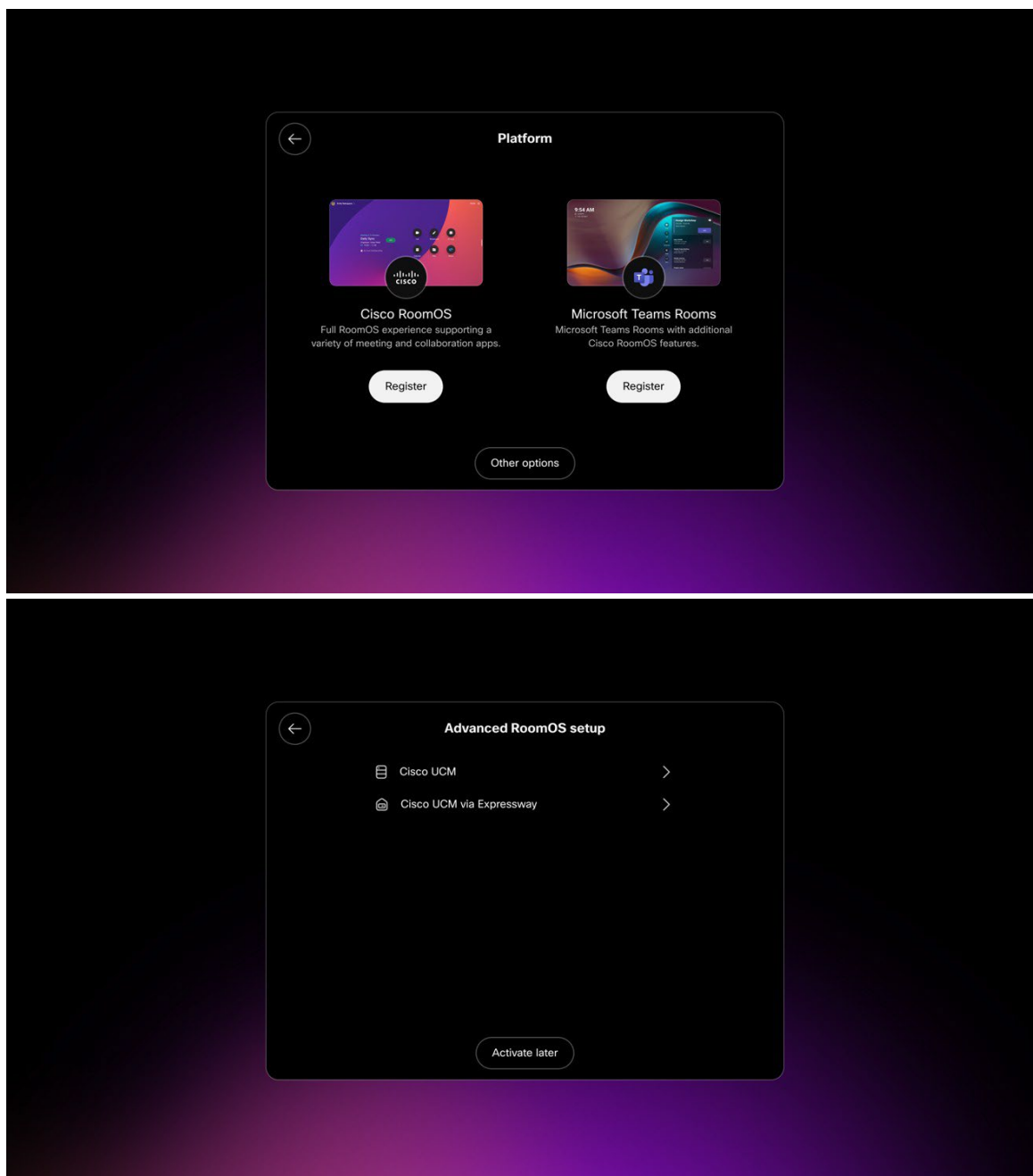
詳細については、次の URL にある『Cisco RoomOS Series 管理者ガイド』を参照してください。

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

呼制御の構成

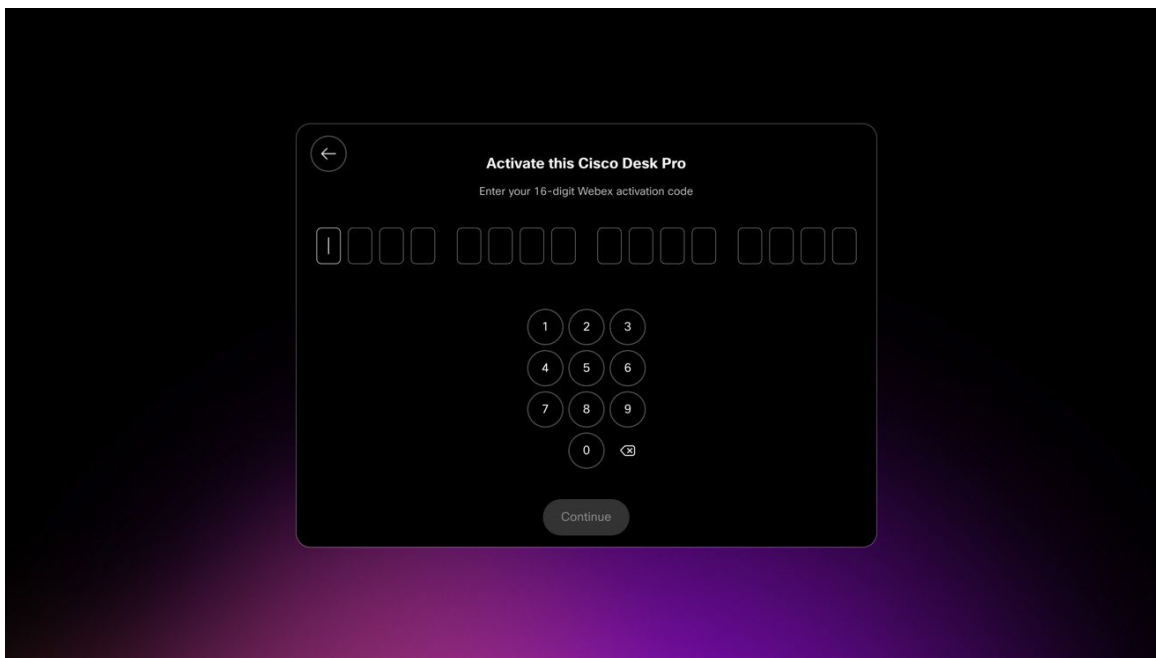
Cisco RoomOS Series は、さまざまな呼制御システムに登録できます。

スタートアップウィザードを使用して、目的の制御システムを選択します。



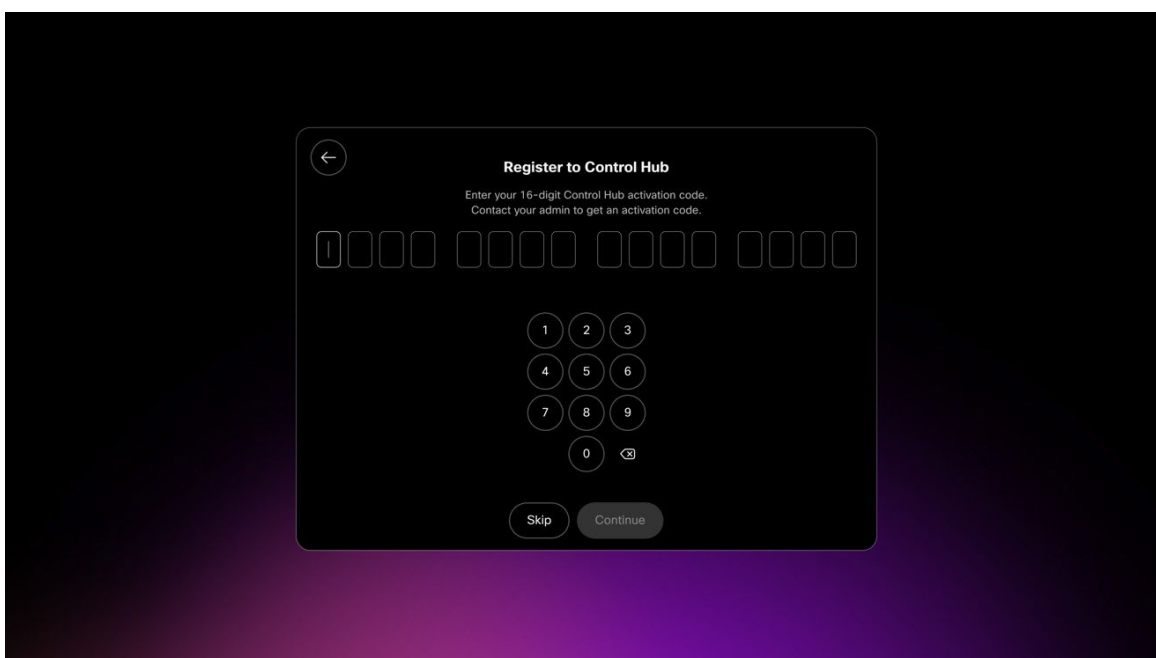
Webex

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



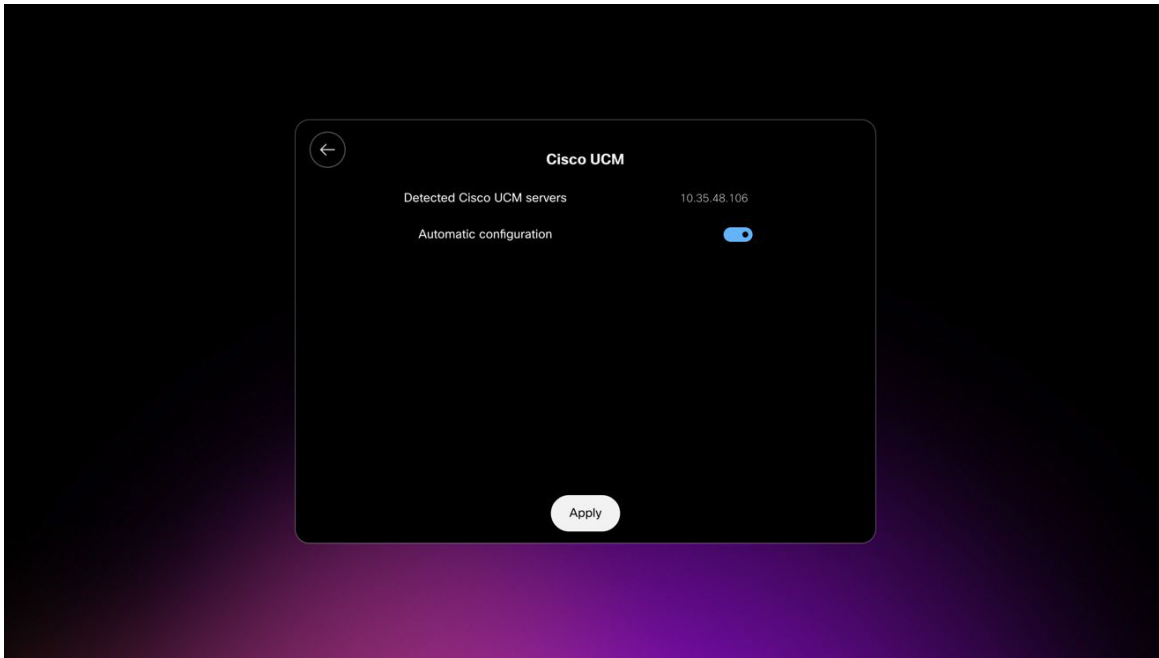
Microsoft Teams Rooms

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



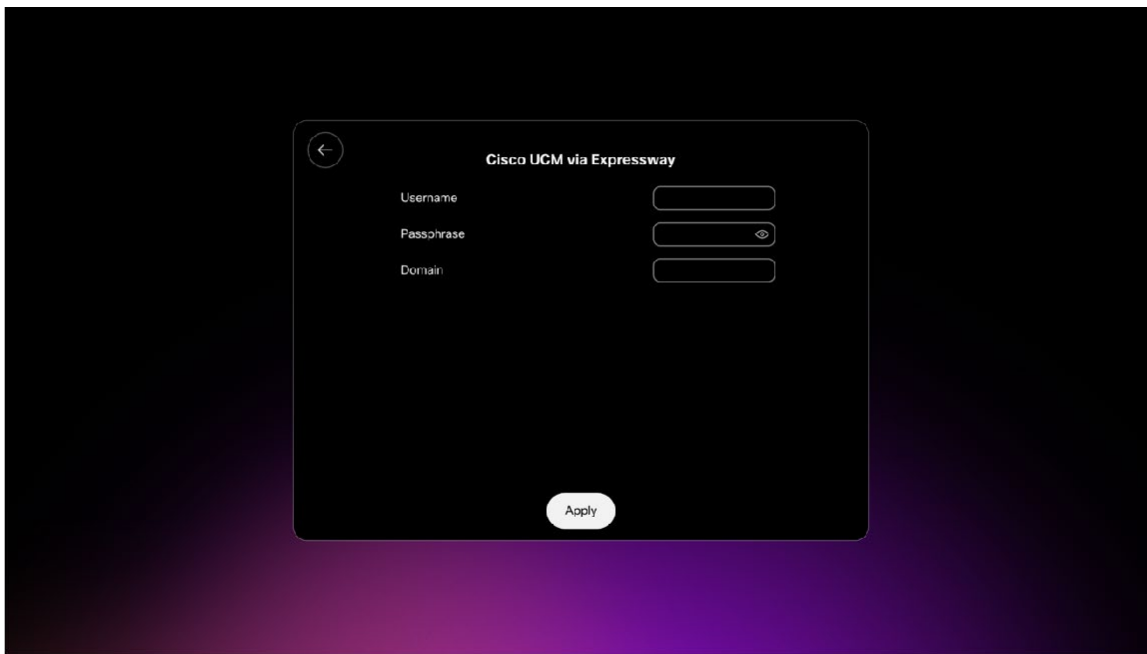
Cisco Unified Communications Manager (UCM)

[その他のオプション (Other Options)] で[Cisco UCM] が選択されている場合は、ネットワーク経由で提供されたCisco UCM サーバーのアドレスを使用するように自動構成選択を使用するか、Cisco UCM サーバーを手動で入力します。



Express 経由の Cisco Unified Communications Manager

[その他のオプション (Other Options)] で、Expressway 経由で Cisco UCM が選択されている場合は、ユーザー名、パスフレーズ、およびドメイン情報を入力します。

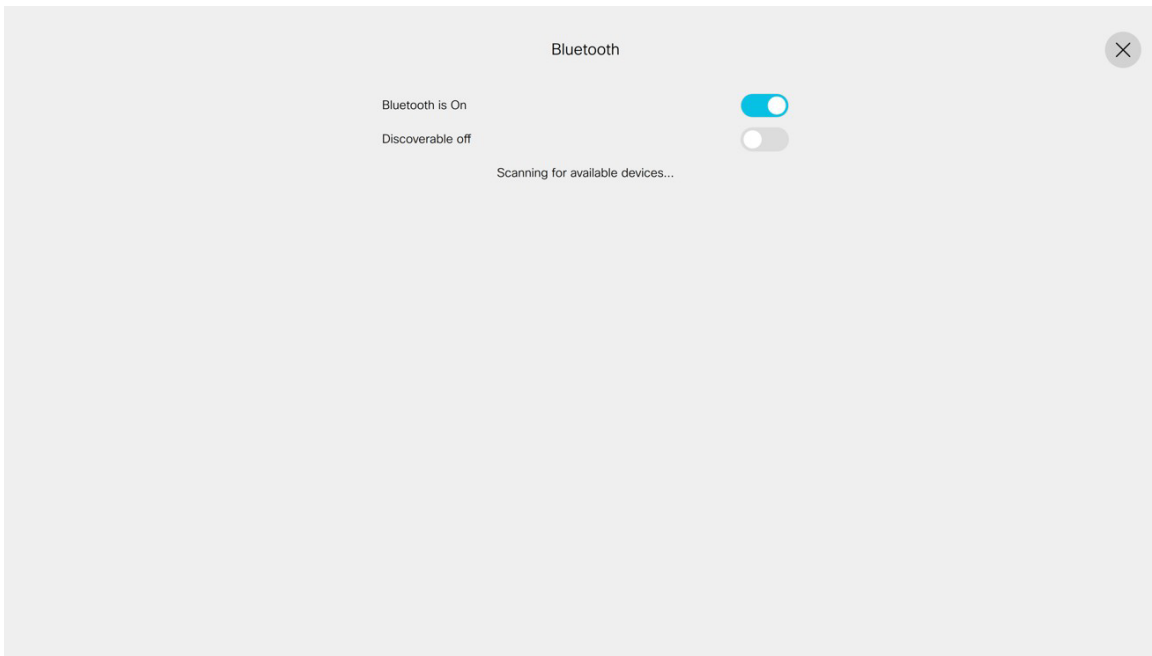


Bluetooth 設定

Cisco RoomOS Series には、ハンズフリー通信を可能にする Bluetooth サポートが含まれています。Bluetooth ヘッドセットと Cisco RoomOS Series をペアリングする手順は次のとおりです。
Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

- [設定 (Settings)] > [Bluetooth] に移動します。

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



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

ファームウェアのアップグレード

Webex

Cisco RoomOS Series にインストールされるファームウェアのバージョンは、Webex Control Hub (安定版、ベータ版、最新版) で構成されたソフトウェア アップグレード チャンネルによって決定され、そのソフトウェア アップグレード チャンネルで新しいファームウェアが利用可能になると、自動的にプッシュダウンされます。

Cisco Unified Communications Manager

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

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

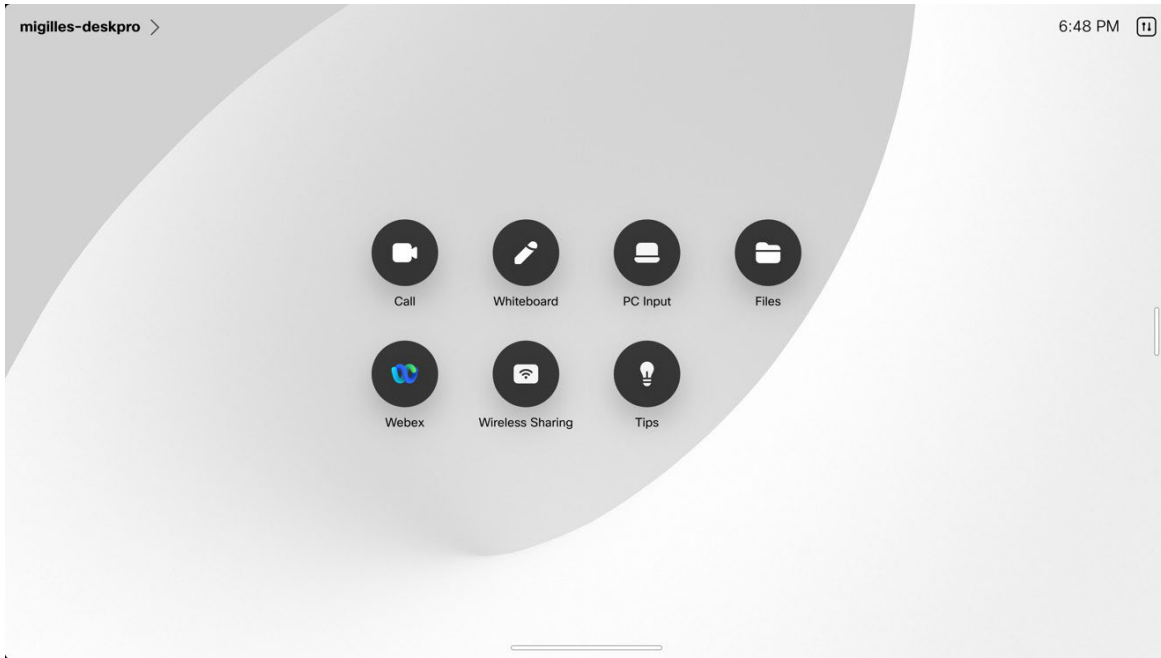
<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

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

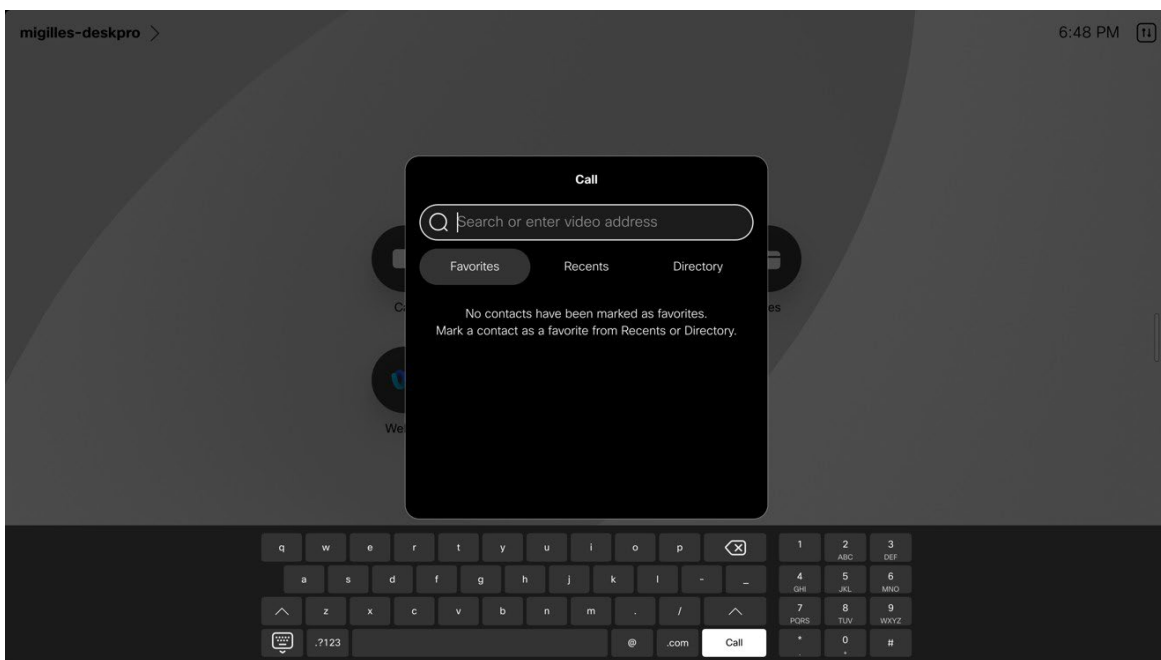
Cisco RoomOS シリーズの使用

Cisco RoomOS Series

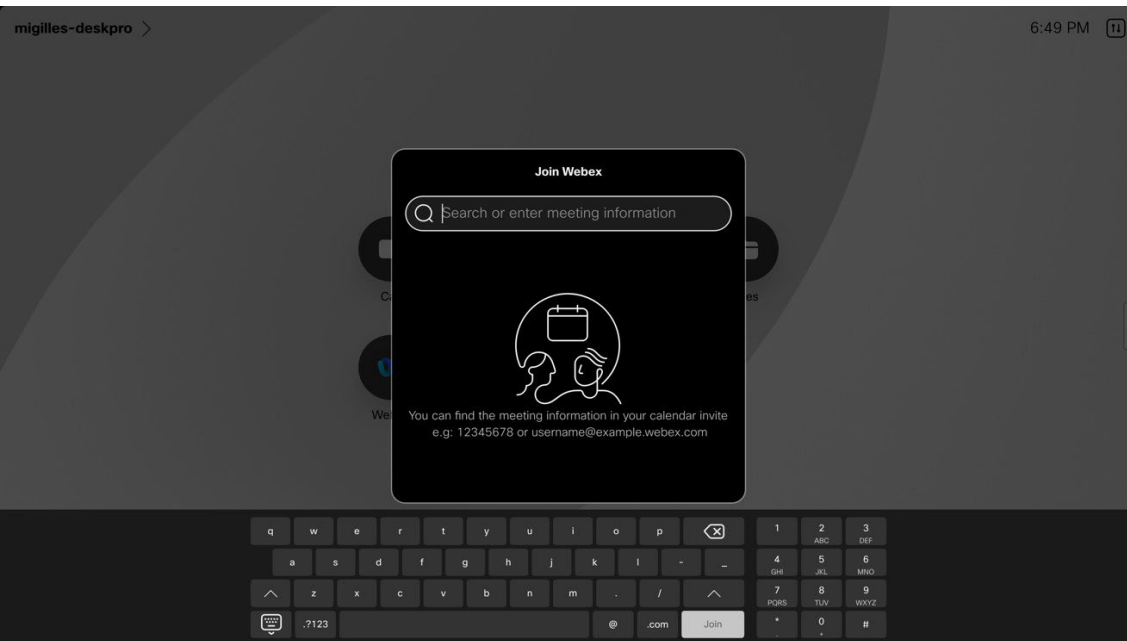
は、ローカルまたはミーティング経由での通話やコンテンツの共有など、さまざまなコラボレーションオプションを提供します。



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



ミーティングに参加するには、目的のミーティング オプションを選択して、ミーティング情報を入力します。

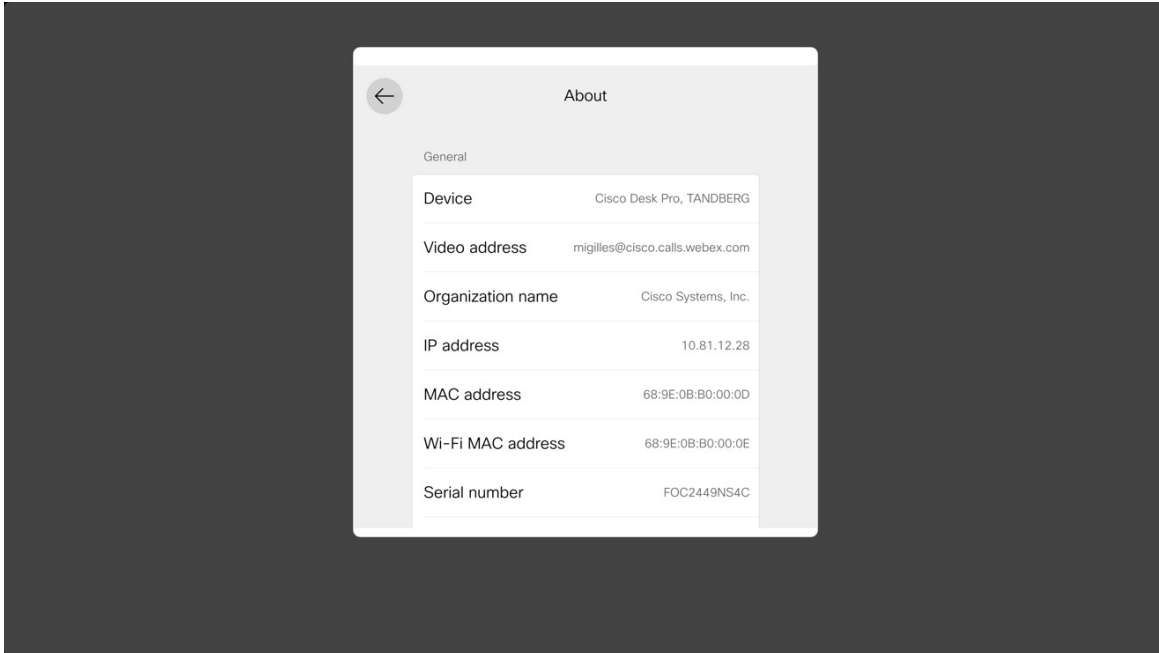


トラブルシューティング

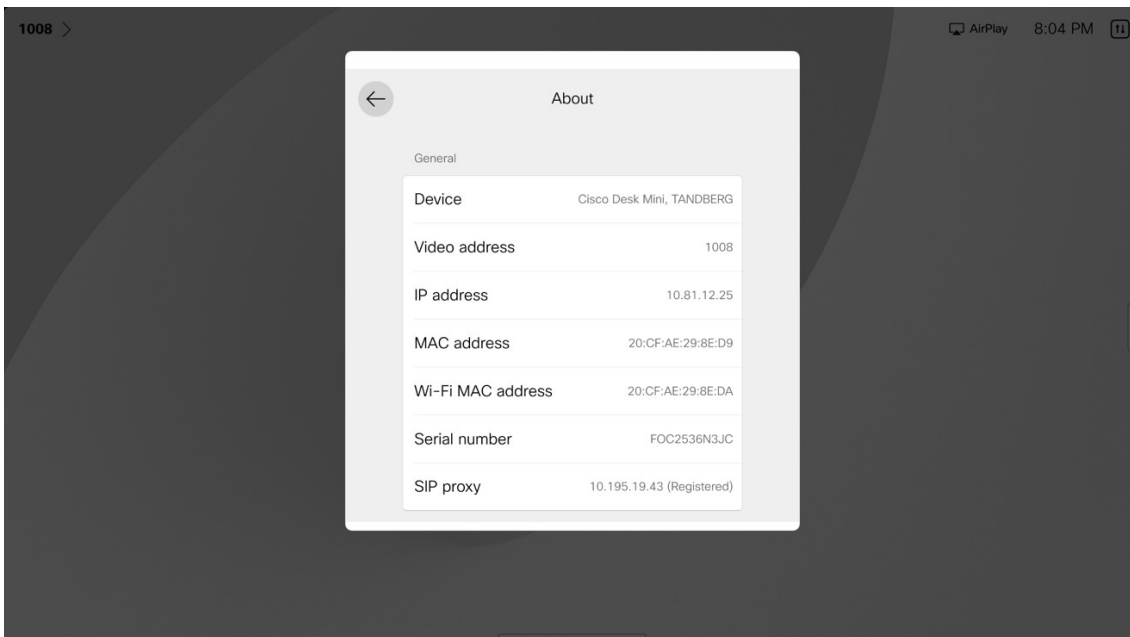
デバイスについて

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

Webex

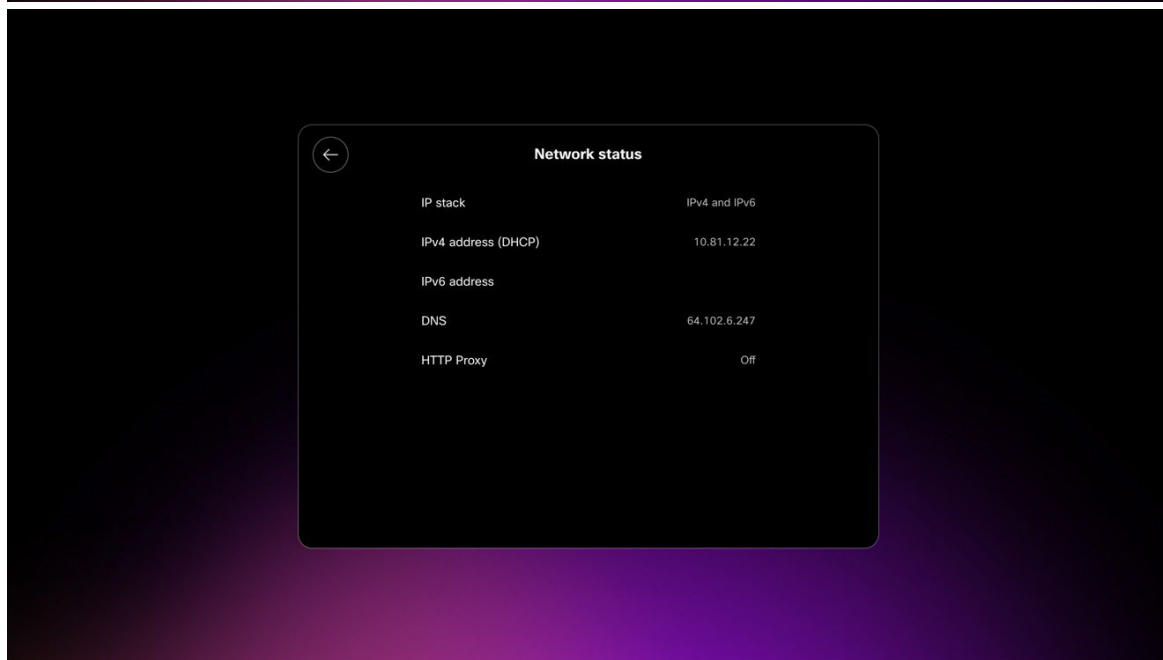
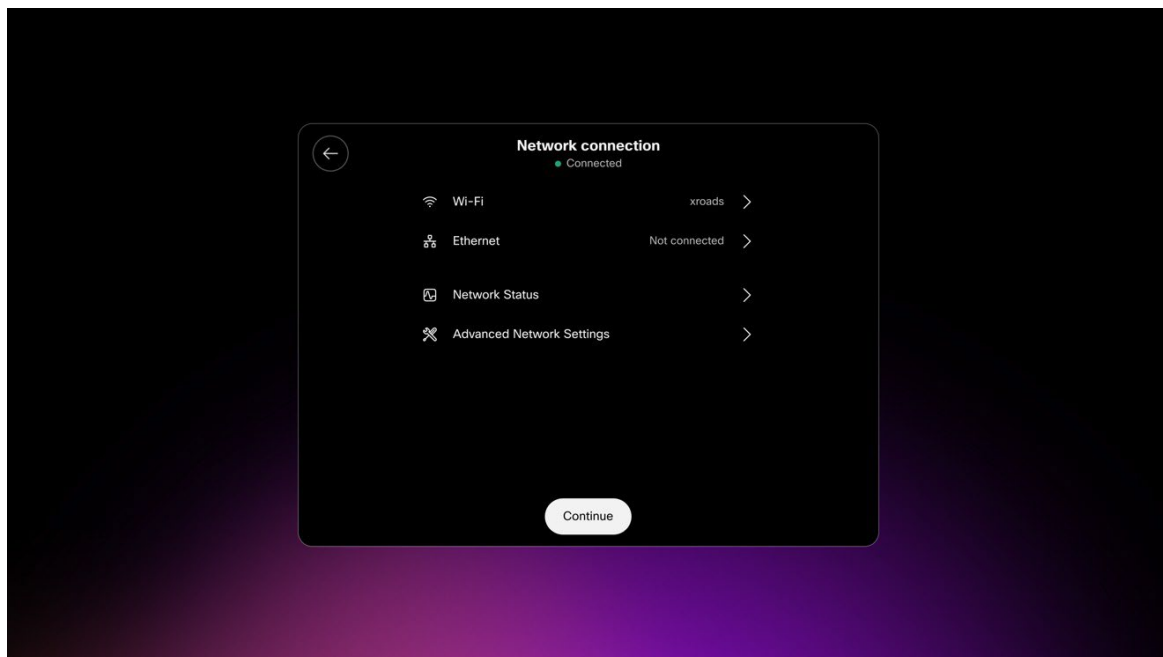


Cisco Unified Communications Manager



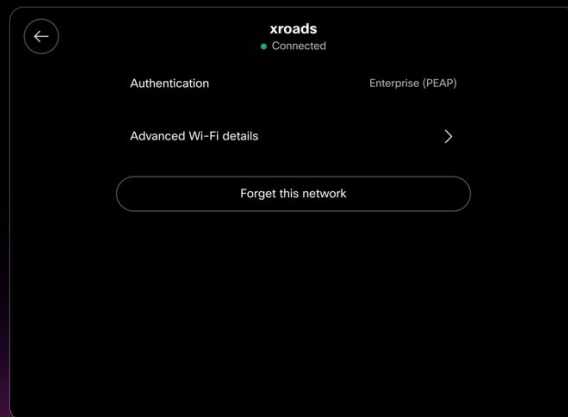
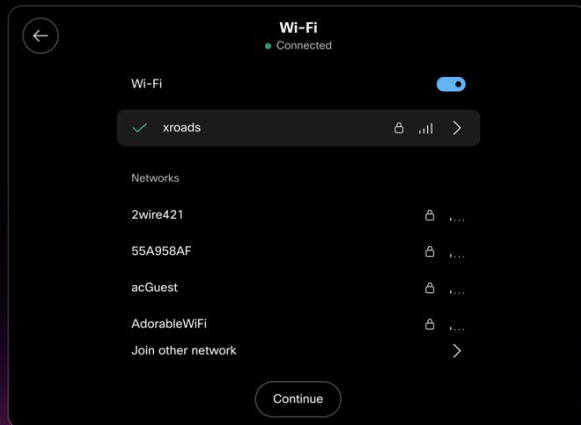
ネットワーク接続ステータス

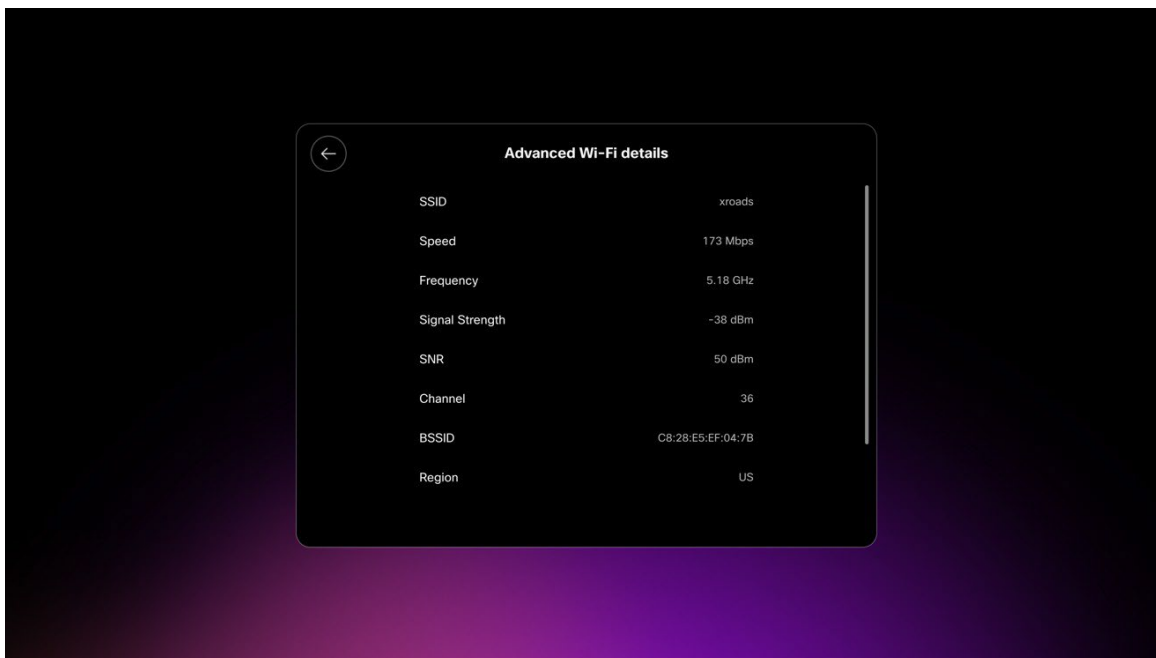
現在のネットワーク接続ステータスと IP アドレス情報は、[設定 (Settings)] > [ネットワーク接続 (Network connection)] に表示されます。



高度な Wi-Fi の詳細

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





問題と診断

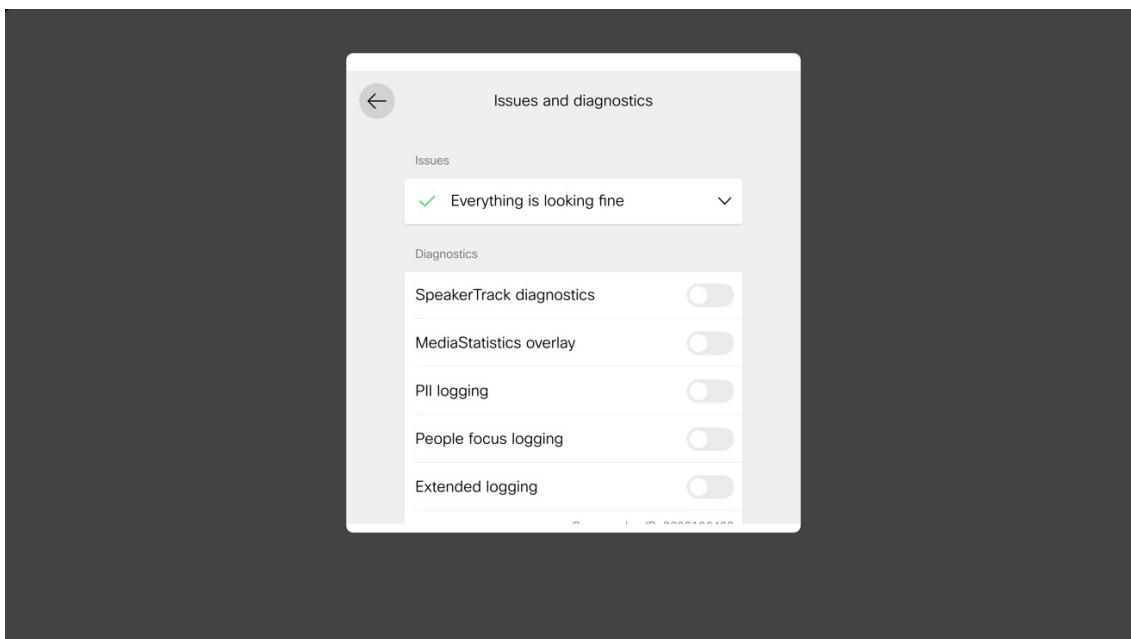
[設定 (Settings)] > [問題と診断 (Issues and Diagnostics)] を選択すると、現在の問題と診断オプションが表示されます。

Webex

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

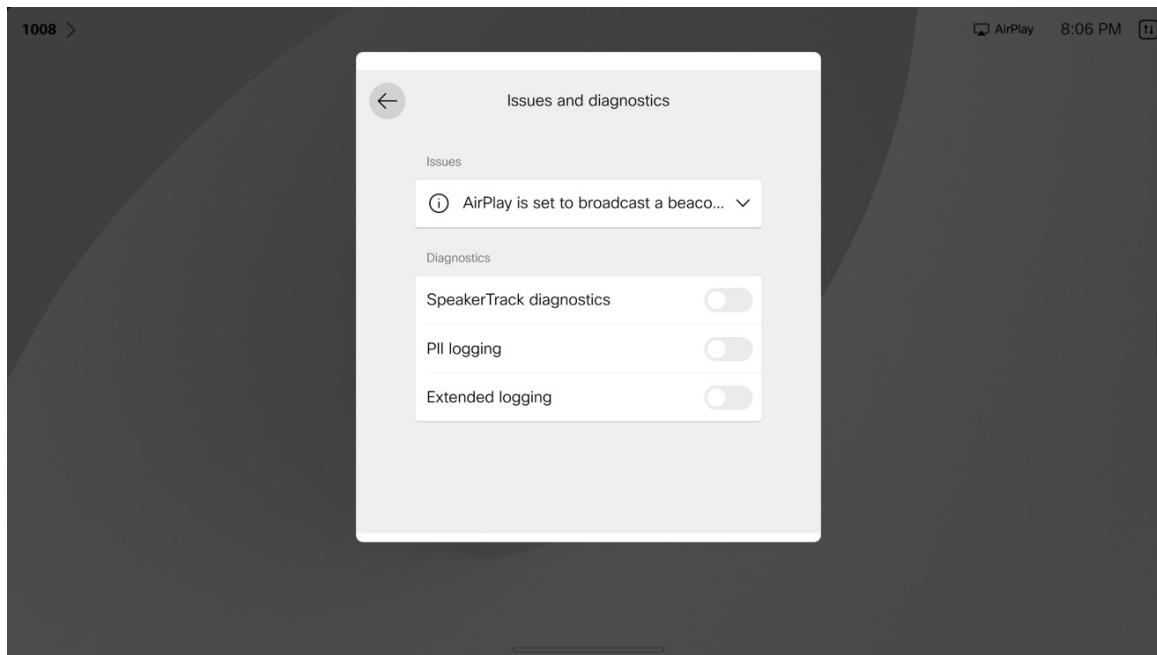
> [問題と診断 (Issues and Diagnostics)] > [システムログ (System Logs)] からダウンロードできます。

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



Cisco Unified Communications Manager

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



デバイスの Web ページ

Cisco RoomOS Series の Web ページには、システム情報、セットアップ、カスタマイズ、およびシステムメンテナンス オプションが用意されています。Web ページにアクセスするには、Cisco RoomOS Series の Web ページで設定された有効な管理者アカウントのログイン情報でログインします。

システム情報

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

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

The screenshot displays the Cisco Webex Local Device Controls interface. The top header includes the Cisco Webex logo, 'Local Device Controls', a search bar with 'Find page', and a user profile icon. The main content area is titled 'System Information' and is divided into several sections:

- General:**
 - IPV4: 10.81.12.28
 - MAC Address: 68:9E:0B:B0:00:0E
 - IPV6: -
 - Serial Number: FOC2449NS4C
 - Active Interface: Wireless
 - Temperature: Normal
 - SIP URI: 7e75011a-0740-5813-8949-4d1cde1d477f@broadcloud.org
 - Cloud SIP Address: migilles@cisco.calls.webex.com
- Issues:**
 - Everything is looking fine
- Provisioning:**
 - Webex: Registered
 - Personal Device Mode
 - Details button
- Calendar:**
 - 0 scheduled meeting(s) found for the next 24 hours.
 - Last updated: Thursday 3:59 PM
 - View Scheduled Meetings button
- Software:**
 - Stable Software Channel
 - RoomOS 11.13.1.5
 - 2f1a43e2808 Software Version

A left-hand navigation menu includes sections for Home, Call, SETUP (Settings, Users, Security), CUSTOMIZATION (Personalization, UI Extensions Editor, Macro Editor, Developer API), and SYSTEM MAINTENANCE (Software, Issues and Diagnostics, Backup and Recovery).

Setup

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

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

[設定 (Settings)]

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Settings

Configurations | Statuses | Send Whiteboard to Email | Audio and Video

Search...

Configuration / SystemUnit

Collapse All | Expand All

Apps

Audio

Bluetooth

Bookings

BYOD

CallHistory

Cameras

Conference

FacilityService

Files

HttpClient

HttpFeedback

Logging

Macros

Mari

MicrosoftTeams

BroadcastName (0 to 256 characters)

CustomDeviceld (0 to 255 characters)

Name (0 to 50 characters)

CrashReporting

Advanced On

Mode Off

URL (0 to 255 characters)

SoftwareUpgrade WebCache

Mode Off

Uri (0 to 255 characters)

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Settings

Configurations | Statuses | Send Whiteboard to Email | Audio and Video

Search...

Status / SystemUnit

Collapse All | Expand All

Audio

Bluetooth

Bookings

Cameras

Capabilities

Conference

Diagnostics

Logging

MicrosoftTeams

Network

NetworkServices

Peripherals

Phonebook

Provisioning

Proximity

BroadcastName Michael Gillespie Desk Pro

DeveloperPreview Mode Off

Extensions Microsoft Supported True

LastShutdownReason Upgrade

LastShutdownTime 2024-02-13T05:57:16Z

ProductId Cisco Desk Pro

ProductPlatform Desk Pro

ProductType Cisco Codec

Uptime 239953

Hardware

DRAM 8

HasWifi True

Monitoring Temperature Status Normal

MonitoringSoftware 34

UDI CS-DESKPRO-K9 V01 FOC2449NS4C

MainBoard

Revision C

SerialNumber FOC2448NPJB

ユーザー

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Users

Create User

Username	Status	Admin	Audit	RoomControl	Integrator	User
admin	Active	✓	✓			✓

セキュリティ

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Security

Certificates Sign-in Banner

Services Custom Preinstalled

Add Certificate

Use the form below to add new certificates.

This system supports PEM formatted certificate files (.pem). The certificate file may contain the certificate and a RSA or DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.

Certificate No file selected.

Private key (optional) No file selected.

Passphrase (optional)

Existing Certificates

Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	HttpProxy	SIP	Pairing	Actions
Self-signed Certificate	TemporaryDefaultCertificate	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete View Certificate

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Security

Certificates Sign-in Banner

Services Custom Preinstalled

Add Certificate Authority

Use the form below to add new certificate authorities.

This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

No file selected.

Existing Certificate Authorities

Certificate	Issuer	Details	Actions
No certificates			

The screenshot shows the Cisco Webex Local Device Controls interface. The top navigation bar includes the Cisco Webex logo, 'Local Device Controls', a search bar, and a user profile icon. The left sidebar contains navigation options: Home, Call, SETUP (Settings, Users, Security), CUSTOMIZATION (Personalization, UI Extensions Editor, Macro Editor, Developer API), and SYSTEM MAINTENANCE (Software, Issues and Diagnostics, Backup and Recovery). The main content area is titled 'Security' and has tabs for 'Certificates' and 'Sign-in Banner'. Under 'Certificates', there are sub-tabs for 'Services', 'Custom', and 'Preinstalled'. The 'Preinstalled Certificates' section contains a text box explaining that the listed Certificate Authorities validate external server certificates. Below this is a table of 'Certificate Details'.

Certificate	Issuer	Details	Enabled
AAA Certificate Services	Comodo CA Limited	View	<input checked="" type="checkbox"/>
ACCVRAIZ1	ACCV	View	<input checked="" type="checkbox"/>
Actalis Authentication Root CA	Actalis S.p.A./03358520967	View	<input checked="" type="checkbox"/>
AffirmTrust Commercial	AffirmTrust	View	<input checked="" type="checkbox"/>
AffirmTrust Networking	AffirmTrust	View	<input checked="" type="checkbox"/>

カスタマイゼーション

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

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

パーソナライゼーション (Personalization)

Cisco Webex Local Device Controls


10.81.12.28 Desk Pro

Find page

Personalization

Wallpaper and Halfwake Branding Virtual Backgrounds Ringtones Contacts

Halfwake The device enters halfwake after it has been idle for a while.



Default




[Upload image](#) Recommended size is 3840x2160 pixels. File format: jpg, png, webp

Turn off display after

10 minutes

[Preview on device](#)

Wallpaper The wallpaper is shown as a background on the home screen.

Custom image light night

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Personalization

Wallpaper and Halfwake Branding Virtual Backgrounds Ringtones Contacts

Brand Logo

Halfwake logo
Shows brand logo in halfwake

[Upload image](#) Recommended size is 272x272 pixels. File format: png

Home screen logo
Show brand logo on home screen

[Upload image](#) Recommended size is 272x272 pixels. File format: png

Custom Text Custom text displays in the bottom left corner of the main screen.
Example: A help desk number your end users can call for assistance.

Feedback? <https://cs.co/dt> [Apply](#)

Cisco Webex Local Device Controls 10.81.12.28 Desk Pro


Find page

Personalization

Wallpaper and Halfwake Branding **Virtual Backgrounds** Ringtones Contacts

Virtual Backgrounds Upload

You can upload up to three virtual backgrounds to replace the background of your video during a call.



Drag a background image here or browse for file

Home Call

SETUP

- Settings
- Users
- Security

CUSTOMIZATION

- Personalization**
- UI Extensions Editor
- Macro Editor
- Developer API

SYSTEM MAINTENANCE

- Software
- Issues and Diagnostics
- Backup and Recovery

Cisco Webex Local Device Controls 10.81.12.28 Desk Pro

Find page

Personalization

Wallpaper and Halfwake Branding Virtual Backgrounds **Ringtones** Contacts

Ringtones Select Active Ringtone

Please note that the ringtone will play on the video system.

Sunrise

Ringtone volume 50%

Home Call

SETUP

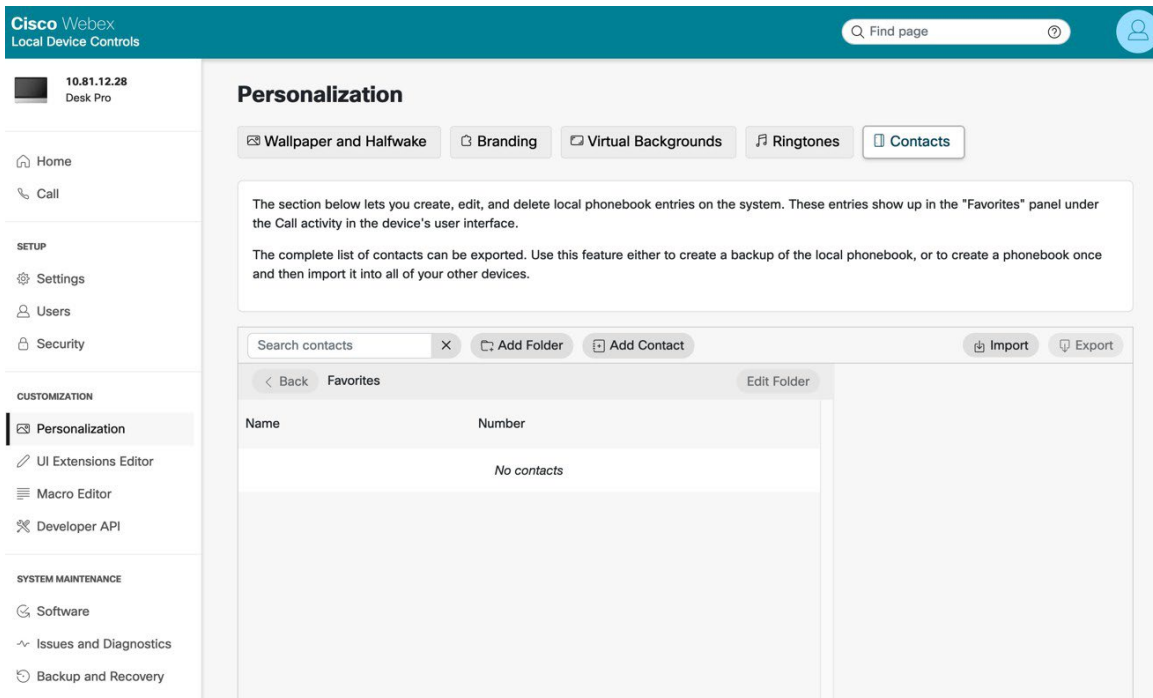
- Settings
- Users
- Security

CUSTOMIZATION

- Personalization**
- UI Extensions Editor
- Macro Editor
- Developer API

SYSTEM MAINTENANCE

- Software
- Issues and Diagnostics
- Backup and Recovery

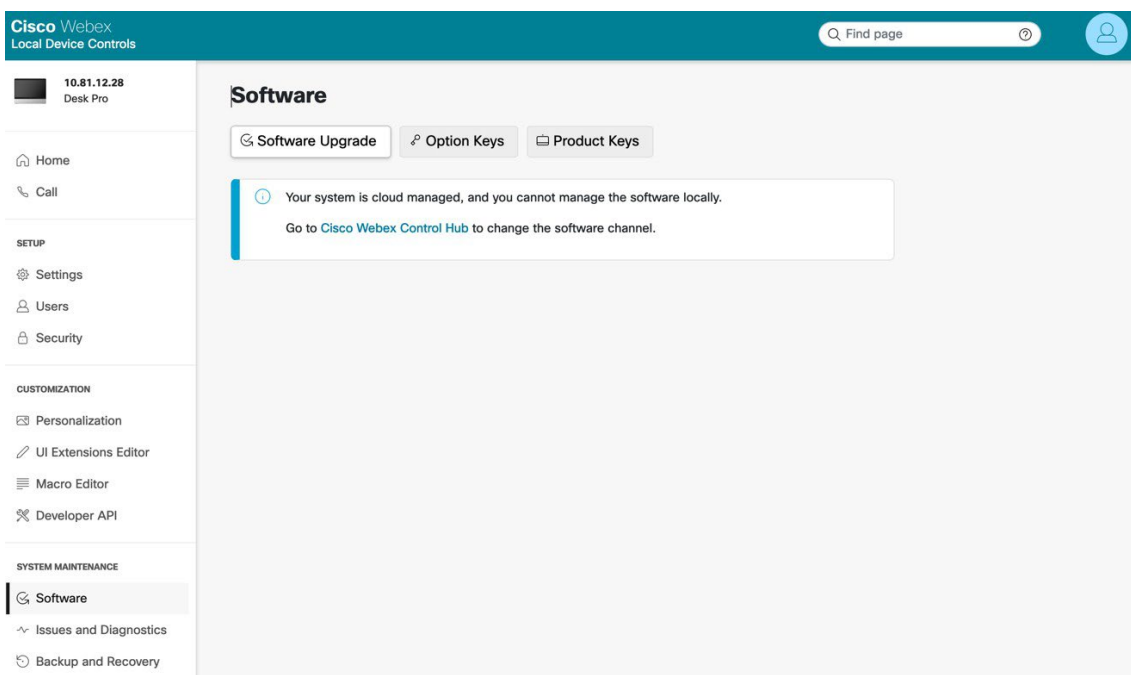


システムメンテナンス

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

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

ソフトウェア



問題と診断

The screenshot shows the Cisco Webex Local Device Controls interface. The top header includes the Cisco Webex logo, 'Local Device Controls', a search bar with 'Find page', and a user profile icon. The left sidebar contains navigation options: Home, Call, SETUP (Settings, Users, Security), CUSTOMIZATION (Personalization, UI Extensions Editor, Macro Editor, Developer API), and SYSTEM MAINTENANCE (Software, Issues and Diagnostics, Backup and Recovery). The main content area is titled 'Issues and Diagnostics' and features tabs for 'Issues', 'System Logs', 'Call Logs', and 'User Interface Screenshots'. A 'Rerun' button is visible. The 'Active Issues' section displays a green checkmark and the message: 'No Issues Found! The system appears to be in working order.'

This screenshot shows the same Cisco Webex Local Device Controls interface, but with the 'System Logs' and 'Extended Logging' sections expanded. The 'System Logs' section provides a full archive of logs for diagnosing problems and includes a 'Download logs...' button. The 'Extended Logging' section explains that this mode helps diagnose network issues during call setup and includes a 'Start' button. Below these sections is the 'Current Logs' table, which lists log files with their names, sizes, and last modified dates.

File Name	Size	Last modified
auth.log	22 kB	2024-02-15 19:28
dhclient.log	14 kB	2024-02-15 19:28
dmesg	75 kB	2024-02-13 00:59
eventlog/airplay.log	8 kB	2024-02-15 19:30

バックアップとリカバリ

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Home Call

SETUP

- Settings
- Users
- Security

CUSTOMIZATION

- Personalization
- UI Extensions Editor
- Macro Editor
- Developer API

SYSTEM MAINTENANCE

- Software
- Issues and Diagnostics
- Backup and Recovery**

Backup and Recovery

Backup Restore System Recovery Restart and Shutdown

Download Backup

This page lets you backup a device's configurations. Configurations include xConfigurations, as well as the configurations for other features a device might support, like macros and UI Extensions.

Select items to include in your backup. Leave all items checked to generate a complete backup of the device.

Branding	No items installed
Favorites	No items installed
UI Extensions	No items installed
Macros	No items installed
Sign In Banner	<input checked="" type="checkbox"/> Include
Configuration	<input checked="" type="checkbox"/> Include

The configuration listed below can be modified for a partial backup of the configuration.

Note: Settings such as Network, SIP URI and SystemUnit Name may specifically apply to a certain device. Applying a backup with these settings to a different device may result in it becoming unreachable on the network. To avoid this, consider removing those settings from the list below.

Remove system-specific configurations

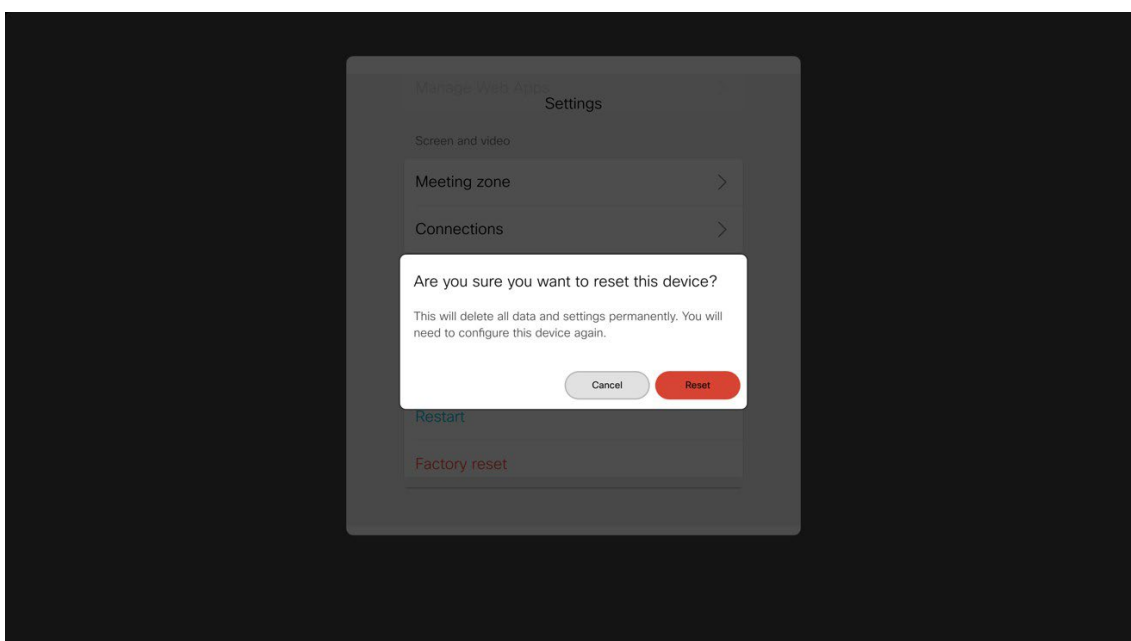
```

Apps WallpaperBundles HalfwakeImage: Auto
Audio DefaultVolume: 50
Audio Input HDMI 1 Level: -5
Audio Input HDMI 1 Mode: 0n
Audio Input HDMI 1 VideoAssociation MuteOnInactiveVideo: 0n
  
```

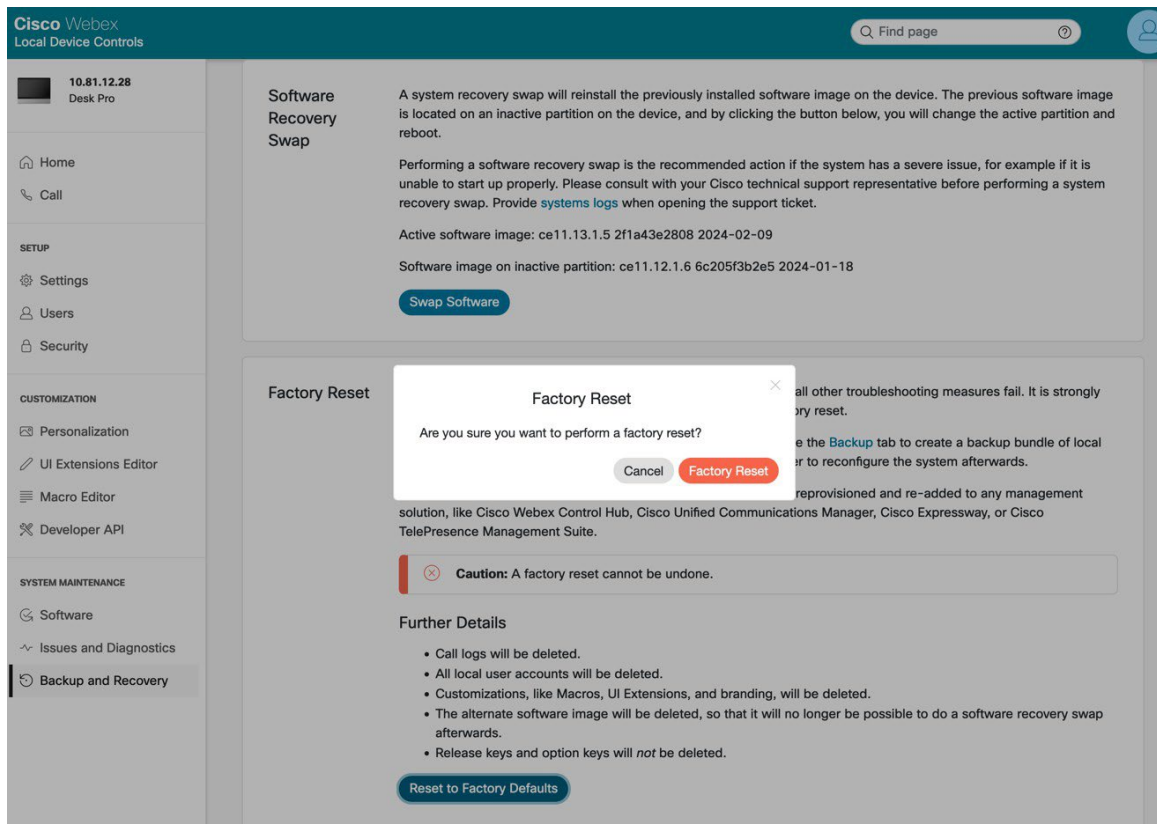
工場出荷時の初期状態の復元

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

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



工場出荷時設定へのリセットは、Cisco RoomOS シリーズの Web ページから [システム メンテナンス (System Maintenance)]、[バックアップとリカバリ (Backup and Recovery)]、[システム リカバリ (System Recovery)]、[工場出荷時設定へのリセット (Reset to Factory Defaults)] の順に選択します。初期化の確認画面が表示されたら、[工場出荷時の状態へのリセット (Factory Reset)] を選択します。



デバイス画面のスクリーンショットのキャプチャ

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

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



10.81.12.28
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Issues and Diagnostics

- Issues
- System Logs
- Call Logs
- User Interface Screenshots

Screenshots

Create Screenshot

Taking a screenshot of the touch panel or the on-screen display (OSD) can be useful for creating user manuals, reporting bugs to Cisco, and so on.

Note that any on-screen video or presentation will not be captured, and that capturing a screenshot may take a while, depending on image resolution and network bandwidth.

OSD Screenshot

Wake System Up

Use the buttons below to put the system into awake or halfwake state.

Awake

Halfwake

その他の資料

Cisco RoomOS Series データ シート

<https://www.cisco.com/c/en/us/products/collaboration-endpoints/webex-desk-pro/datasheet-c78-743105.html>

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

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

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

Cisco RoomOS Series 管理者ガイド

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

Cisco Room Series ユーザーガイド

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

Cisco RoomOS Series クイック リファレンス ガイド

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

Cisco RoomOS Series リリース ノート

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

Cisco RoomOS Series ソフトウェア

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

Cisco Unified Communications Manager

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

Cisco Voice

ソフトウェア <https://software.cisco.com/download/home/278875240>

無線 LAN でのリアルタイム

トラフィック設計ガイド https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

Cisco Unified Communications 設計ガイド

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

Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

Cisco AireOS ワイヤレス LAN コントローラに関するドキュメント

<https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

Cisco Catalyst IOS XE ワイヤレス LAN コントローラに関するドキュメント

<https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

Cisco Mobility Express に関するドキュメント

<https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-and-configuration-guides-list.html>

Cisco

自律アクセスポイントのドキュメント https://www.cisco.com/c/en/us/td/docs/wireless/access_point/atnms-ap-8x/configuration/guide/cg-book.html

Cisco Meraki ワイヤレス LAN

のドキュメント <https://documentation.meraki.com>

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

Cisco および Cisco ロゴは、Cisco Systems, Inc.

またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧は

<http://www.cisco.com/go/trademarks>

に記載されています。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」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

本ドキュメントまたは Web

サイトに掲載されているその他の商標はそれぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(0809R)。



Bluetooth の用語マークとロゴは、Bluetooth SIG, Inc. が所有する登録商標であり、かかる商標の Cisco Systems, Inc.による使用はライセンスに基づいています。

© 2024 Cisco Systems, All rights reserved.