cisco

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。魅力的かつ強力に統合され、常時接続でセキュア、ミッションクリティカルなユニファイド コミュニケーションと、HD

ビデオおよびクラウドコンピューティング体験を含むコラボレーションを組み合わせ、そのインタラクティブで使いやすく、カスタマイズ可能なパーソナライゼーションとワークフローのオプションは、エンタープライズグレードのプラットフォームから使用することができます。

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

Models	
	•••••
Requirements	
Site Survey	
Call Control	
Wireless LAN	
Protocols	
Wi-Fi	
Regulatory	
Bluetooth	
Languages	
Video Calls	
Device Care	
ireless LAN Design	
802.11 Network	
5 GHz (802.11a/n/ac/ax)	
2.4 GHz (802.11b/g/n/ax)	
Signal Strength and Coverage	
Data Rates	
Rugged Environments	
Security	
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)	
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)	1
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS)	
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) Quality of Service (QoS)	4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC)	4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS	4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS	4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming	4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) Quality of Service (QoS) Call Admission Control (CAC) Wired QoS Roaming Interband Roaming Power Management	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Canacity</i>	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Capacity</i>	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Capacity</i>	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Capacity</i> <i>Multicast</i>	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) Quality of Service (QoS) Call Admission Control (CAC) Wired QoS Roaming Interband Roaming Power Management Call Capacity Multicast nfiguring the Cisco Wireless LAN . Cisco AireOS Wireless LAN Controller and Lightweight Access Points	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Capacity</i> <i>Multicast</i> <i>Multicast</i> <i>Solution Controller and Lightweight Access Points</i> 802.11 Network Settings WLAN Settings	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	$ \begin{array}{c} 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ 4\\ $
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	$ \begin{array}{c} 4 \\ 5 \\ 6 \\ 6 \\ 6 \\ \end{array} $
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	$ \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c}$
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Capacity</i> <i>Multicast</i> <i>mfiguring the Cisco Wireless LAN</i> <i>Cisco AireOS Wireless LAN Controller and Lightweight Access Points</i> 802.11 Network Settings. WLAN Settings Controller Settings Controller Settings Call Admission Control (CAC) RF Profiles FlexConnect Groups	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) Quality of Service (QoS) Call Admission Control (CAC) Wired QoS Roaming Interband Roaming Power Management Call Capacity Multicast Multicast onfiguring the Cisco Wireless LAN Cisco AireOS Wireless LAN Cisco AireOS Wireless LAN Controller settings. WLAN Settings Controller Settings WLAN Settings Controller S	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP)	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) Protected Extensible Authentication Protocol (PEAP) <i>Quality of Service (QoS)</i> Call Admission Control (CAC) Wired QoS <i>Roaming</i> Interband Roaming <i>Power Management</i> <i>Call Capacity</i> <i>Multicast</i> <i>mfiguring the Cisco Wireless LAN</i> . <i>Cisco AireOS Wireless LAN Controller and Lightweight Access Points</i> 802.11 Network Settings. WLAN Settings Controller Settings Controller Settings Call Admission Control (CAC) RF Profiles FlexConnect Groups Multicast Direct QoS Profiles. Advanced Settings	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4

WLAN Settings	
Controller Settings	
Mobility Settings	
Call Admission Control (CAC)	
Mulucast	
Sample Configuration	
Cisco Mohility Express and Lightweight Access Points	122
Controller Settings	
802.11 Network Settings	
WLAN Settings	
RF Profiles	
Multicast Direct	
Cisco Autonomous Access Points	
802.11 Network Settings	
WLAN Settings	
Call Admission Control (CAC)	
QOS FOIICIES Power Management	
Sample Configuration	
Cisco Marabi Accass Points	161
Creating the Wireless Network	101
SSID Configuration	
Radio Settings	
Firewall and Traffic Shaping	
Configuring Cisco Call Control	171
Webex	
Personal Usage	
Shared Usage	
Cisco Unified Communications Manager	
Device Enablement	
Device Pools Phone Button Templates	
Security Profiles	
SIP Profiles	
QoS Parameters	
Audio and Video Bit Rates	
Product Specific Configuration Options	
Configuring the Cisco RoomOS Series	241
W: E: Duefle Conformation	
W1-F1 Profile Configuration	
Certificate Management	
Installing Certificates	
Removing Certificates	
Call Control Configuration	
Bluetooth Settings	
Upgrading Firmware	
Using the Cisco RoomOS Series	
Troubleshooting	
About Device	
Network Connection Status	
Cisco RoomOS DX Series ワイヤレス LAN 違入ガイド	
	4

Advanced Wi-Fi Details	
Issues and Diagnostics	
Device Webpages	
System Information	
Setup	
Customization	
System Maintenance	
Restoring Factory Defaults	
Capturing a Screenshot of the Device Display	
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 @ 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とゆえタイの短続が発生する可能性またります。5 CH-

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	周波数範囲	チャネル
		アンテナ		セット (チャ
		ゲイン		ネル数)
Cisco Board 55	CS-BOARD55	2.4 GHz = 4.23 dBi	$2.412\sim 2.472~\mathrm{GHz}$	$1 \sim 13$ (13)
		5 GHz = 6.00 dBi	$5.180 \sim 5.240~\mathrm{GHz}$	36、40、44、48(4)
Cisco Board 55s	CS-BOARD55S	2.4 GHz = 4.50 dBi	$5.260 \sim 5.320 \text{ GHz}$	52、56、60、64(4)
		5 GHz = 5.80 dBi	$5.500 \sim 5.720 \mathrm{GHz}$	$100 \sim 144$ (12)
			$5.745 \sim 5.825~\mathrm{GHz}$	149, 153, 157, 161, 1
Cisco Board 70	CS-BOARD70	$2.4 \text{ GHz} = 4.23 \text{ dB}_1$		65 (5)
		5 GHz = 6.00 dBi		
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	製品番号 ピーク 周波数範		チャネル
		アンテナ		セット (チャ
		ゲイン		ネル数)
シスコデスク	CS-DESK	2.4 GHz = 3.40 dBi	$2.412\sim 2.472~\mathrm{GHz}$	$1 \sim 13$ (13)
		5 GHz = 6.10 dBi	$5.180 \sim 5.240~\mathrm{GHz}$	36、40、44、48(4)
Cisco Desk Mini	CS-DESKMINI	2.4 GHz = 5.00 dBi	$5.260 \sim 5.320~\mathrm{GHz}$	52、56、60、64(4)
		5 GHz = 4.90 dBi	$5.500 \sim 5.720 \mathrm{~GHz}$	$100 \sim 144$ (12)
Cisco Room Bar	CS-BAR	2.4 GHz = 4.96 dBi	$5.745 \sim 5.825 \text{ GHz}$	149、153、157、161、1
		5 GHz = 7.85 dBi		65 (5)

Cisco RoomOS Series 3

モデル	製品番号	ピーク	周波数範囲	チャネル
		アンテナ		セット (チャ
		ゲイン		ネル数)
Cisco Codec EQ	CS-CODEC-EQ	2.4 GHz = 3.50 dBi	$2.412\sim 2.472~\mathrm{GHz}$	$1 \sim 13$ (13)
		5 GHz = 3.40 dBi	$5.180 \sim 5.240~\mathrm{GHz}$	36、40、44、48(4)
Cisco Room Bar Pro	CS-BARPRO	2.4 GHz = 6.70 dBi	$5.260 \sim 5.320 \mathrm{~GHz}$	52、56、60、64(4)
		5 GHz = 5.70 dBi	$5.500 \sim 5.720 \mathrm{~GHz}$	$100 \sim 144$ (12)
			$5.745 \sim 5.825~\mathrm{GHz}$	149、153、157、161、1
				65 (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(チャネル34、38、42、46)はサポートされていません。 日本用のチャネル14はサポートされていません。

要件

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

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。

<u>チャンネルの使用率</u>

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。

<u>ノイズ</u>

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。

<u>パケット損失/遅延</u>

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

- o 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

- o Webex
- o Cisco Unified Communications

Manager (CUCM) 、最小=11.5(1)

推奨=12.5(1)、14.0(1)以降

• Cisco RoomOS Series 3

- o 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、<u>https://software.cisco.com/download/home/278875240</u>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	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	軽量	Mobility Express	自律型
シリー								-	

ズ									
1700	はい	はい	はい	はい	はい	いいえ	0	いいえ	0
1810	はい	はい	はい	はい	はい	いいえ	0	いいえ	いいえ
1810W	はい	はい	はい	はい	はい	いいえ	0	いいえ	いいえ
1815	はい	はい	はい	はい	はい	いいえ	0	はい(1 815t ではあ りませ ん)	いいえ
1830	はい	はい	はい	はい	はい	いいえ	0	はい	いいえ
1840	はい	はい	はい	はい	はい	いいえ	0	はい	いいえ
1850	はい	はい	はい	はい	はい	いいえ	0	はい	いいえ
2700	はい	はい	はい	はい	はい	いいえ	0	いいえ	0
2800	はい	はい	はい	はい	はい	いいえ	0	はい	いいえ
3700	はい	はい	はい	はい	はい	いいえ	0	いいえ	0
3800	はい	はい	はい	はい	はい	いいえ	0	はい	いいえ
4800	はい	はい	はい	はい	はい	いいえ	0	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。



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

次の表に、	各 Cisco	o Meraki ア	クセスポイ	ントでサプ	ポートされ	るモード	を示します。
-------	---------	------------	-------	-------	-------	------	--------

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-antennasaccessories/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)
 - o AAC-LD、Opus、G.722、G.711、G.722.1、G.729
 - oH.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	最大 Tx パワー=20 dBm	6 Mbps	1	OFDM - BPSK
Cisco Board 55s	(地域によって異なる)	9 Mbps	1	OFDM - BPSK
Cisco Board 70		12 Mbps	1	OFDM - QPSK
Cisco Board 70s		18 Mbps	1	OFDM - QPSK
Cisco Board 85s		24 Mbps	1	OFDM - 16 QAM
Cisco Board Pro 75		36 Mbps	1	OFDM - 16 QAM
Cisco Codec Plus		48 Mbps	1	OFDM - 64 QAM
Cisco Codec Pro		54 Mbps	1	OFDM - 64 QAM
Cisco Desk Limited Edition Cisco Desk Pro	5 GHz - 802.11n (HT20)	データレート	空間ス トリー	変調
Cisco Room 55 Cisco Room 55 Dual	最大送信電力=19	7 Mbps (MCS 0)	1	OFDM - BPSK
Cisco Room 70 Single	dBm(地域によって異なる)	14 Mbps (MCS 1)	1	OFDM - QPSK
Cisco Room 70 Dual		21 Mbps (MCS 2)	1	OFDM - QPSK
Cisco Room 70 Single G2		29 Mbps (MCS 3)	1	OFDM - 16 QAM
Cisco Room 70 Dual G2		43 Mbps (MCS 4)	1	OFDM - 16 QAM
Cisco Room 70 Panorama		58 Mbps (MCS 5)	1	OFDM - 64 QAM
Cisco Room Kit		65 Mbps (MCS 6)	1	OFDM - 64 QAM
Cisco Webex Room Kit Mini		72 Mbps (MCS 7)	1	OFDM - 64 QAM
Cisco Room USB		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	15 Mbps (MCS 0)	1	OFDM - BPSK
	(地域によって異なる)	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
	7 Mbps (MCS 0)	1	OFDM - BPSK
dBm (地域によって異たろ)	$\frac{14 \text{ Mbps}}{14 \text{ Mbps}} (\text{MCS } 1)$	1	OFDM - OPSK
	$\frac{21 \text{ Mbps} (\text{MCS } 1)}{21 \text{ Mbps} (\text{MCS } 2)}$	1	OFDM - OPSK
	29 Mbps (MCS 3)	1	OFDM - 16 OAM
	43 Mbps (MCS 4)	1	OFDM - 16 OAM
	58 Mbps (MCS 5)	1	OFDM - 64 OAM
	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
 	15 Mbps (MCS 0)	1	OFDM - BPSK
取八心山电月-10	$\frac{10 \text{ WOPS}}{30 \text{ Mbps}} (\text{WCS} 1)$	1	OFDM - OPSK
	JU MUPS (MCSI)	1	OLDM - GLOK

i de la constante de			
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 -	データレート	空間ス	変調
802.11ac (VHT80)		トリー	
		<i>I</i> .	
	22 Ming (MCS 0)		OEDM DDSV
最大送信電力=18 dPm (地域によって異なる)	33 Mbps (MCS 0)	1 1	OFDM - BPSK
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 08 Mbps (MCS 2)	1 1 1	OFDM - BPSK OFDM - QPSK
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 120 Mbps (MCS 2)	1 1 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4)	1 1 1 1 1 1 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5)	1 1 1 1 1 1 1 1 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 203 Mbps (MCS 6)	L 1 1 1 1 1 1 1 1 1 1 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM
最大送信電力 = 18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8)	L 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 9)	L 1	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0)	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 9) 65 Mbps (MCS 0) 130 Mbps (MCS 1)	1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - BPSK
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 9) 65 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 2)	A 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - BPSK OFDM - QPSK
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 9) 65 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 2)	Image: Image and the second	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 9) 65 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 3)	I 1 1 1 1 1 1 1 1 1 1 2 <t< td=""><td>OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - BPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - QPSK OFDM - QPSK OFDM - 16 QAM</td></t<>	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - BPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - QPSK OFDM - QPSK OFDM - 16 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 3) 390 Mbps (MCS 2) 260 Mbps (MCS 2) 260 Mbps (MCS 4)	A 1 1 1 1 1 1 1 1 1 1 2 <t< td=""><td>OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 16 QAM OFDM - 16 QAM OFDM - 16 QAM</td></t<>	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 16 QAM OFDM - 16 QAM OFDM - 16 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0) 130 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 4) 520 Mbps (MCS 5) 585 Mbps (MCS 6)	A 1 1 1 1 1 1 1 1 1 1 1 1 2 <t< td=""><td>OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 04 QAM OFDM - 256 QAM OFDM - 10 QAM OFDM - 04 QAM OFDM - 04 QAM OFDM - 04 QAM OFDM - 04 QAM OFDM - 16 QAM OFDM - 64 QAM</td></t<>	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 04 QAM OFDM - 256 QAM OFDM - 10 QAM OFDM - 04 QAM OFDM - 04 QAM OFDM - 04 QAM OFDM - 04 QAM OFDM - 16 QAM OFDM - 64 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0) 130 Mbps (MCS 7) 390 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 3) 390 Mbps (MCS 4) 520 Mbps (MCS 5) 585 Mbps (MCS 6) 650 Mbps (MCS 7)	A 1 1 1 1 1 1 1 1 1 1 1 1 2 <t< td=""><td>OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - 100 QAM OFDM - 00000000000000000000000000000000000</td></t<>	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - 100 QAM OFDM - 00000000000000000000000000000000000
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0) 130 Mbps (MCS 7) 390 Mbps (MCS 1) 195 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 3) 390 Mbps (MCS 4) 520 Mbps (MCS 5) 585 Mbps (MCS 6) 650 Mbps (MCS 7) 780 Mbps (MCS 8)	Image: Constraint of the second state of the seco	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 0PSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM
最大送信電力=18 dBm(地域によって異なる)	33 Mbps (MCS 0) 65 Mbps (MCS 1) 98 Mbps (MCS 2) 130 Mbps (MCS 3) 195 Mbps (MCS 4) 260 Mbps (MCS 5) 293 Mbps (MCS 6) 325 Mbps (MCS 7) 390 Mbps (MCS 8) 433 Mbps (MCS 0) 130 Mbps (MCS 7) 390 Mbps (MCS 0) 130 Mbps (MCS 1) 195 Mbps (MCS 0) 390 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 1) 195 Mbps (MCS 2) 260 Mbps (MCS 3) 390 Mbps (MCS 4) 520 Mbps (MCS 4) 520 Mbps (MCS 5) 585 Mbps (MCS 6) 650 Mbps (MCS 7) 780 Mbps (MCS 8) 867 Mbps (MCS 9)	I 1 1 1 1 1 1 1 1 1 1 1 1 1 2 <t< td=""><td>OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - QPSK OFDM - 04 QAM OFDM - 256 QAM OFDM - 16 QAM OFDM - 04 QAM OFDM - 256 QAM OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM</td></t<>	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - QPSK OFDM - 04 QAM OFDM - 256 QAM OFDM - 16 QAM OFDM - 04 QAM OFDM - 256 QAM OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM 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	変調
			Д	
Cisco Board 55 Cisco	最大送信電力=19	1 Mbps	1	DSSS - BPSK
Board 55s	dBm(地域によって異なる)	2 Mbps	1	DSSS - QPSK
Cisco Board 70		5.5 Mbps	1	DSSS - CCK
Cisco Board 70s		11 Mbps	1	DSSS - CCK
Cisco Board 85s	2.4 GHz - 802.11g	データレート	空間ス	変調
Cisco Board Pro 55			トリー	
Cisco Desk Pro			Д	
Cisco Desk Limited	最大送信電力=19	6 Mbps	1	OFDM - BPSK
Edition	dBm(地域によって異なる)	9 Mbps	1	OFDM - BPSK
Cisco Room 55 Cisco		12 Mbps	1	OFDM - QPSK
Room 55 Dual		18 Mbps	1	OFDM - QPSK
Cisco Room 70 Single		24 Mbps	1	OFDM - 16 QAM
Room 70 Single G2 Cisco		36 Mbps	1	OFDM - 16 QAM
Room 70 Dual G2 Cisco		48 Mbps	1	OFDM - 64 QAM
Room 70 Panorama Cisco		54 Mbps	1	OFDM - 64 QAM
Room Panorama Cisco Room Kit	2.4 GHz - 802.11n (HT20)	データレート	空間ス トリー	変調
Cisco Room Kit Mini			Д	
Cisco Room Kit Plus Cisco Room Kit Pro Cisco Room	最大送信電力=19	7 Mbps (MCS 0)	1	OFDM - BPSK
USB	dBm(地域によって異なる)	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	2	OFDM - 64 QAM
		13) 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	最大送信電力=19	6 Mbps	1	OFDM - BPSK
Desk Mini Cisco	dBm(地域によって異なる)	9 Mbps	1	OFDM - BPSK
Room Bar		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	7 Mbps (MCS 0)	1	OFDM - BPSK
	dBm(地域によって異なる)	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	変調
		トリー	
最大送信電刀=18	15 Mbps (MCS 0)	1	OFDM - BPSK
dBm(地域によって異なる)	30 Mbps (MCS I)	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	変調
			OFDM DRGV
	/ Mbps (MCS 0)	1	OFDM OPSK
dBm(地域によつ(異なる)	$\frac{14 \text{ Mbps}}{14 \text{ Mbps}} (\text{MCS I})$	1	OFDM - QPSK
	$\frac{21 \text{ Mbps}}{20 \text{ MCS}} (\text{MCS} 2)$	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	変調
		4	
最大送信電力=18	15 Mbps (MCS 0)	1	OFDM - BPSK
dBm(地域によって異なる)	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	33 Mbps (MCS 0)	1	OFDM - BPSK
dBm(地域によって異なる)	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	変調
			トリー	
			Д	
Cisco Desk Cisco	最大送信電力=22	1 Mbps	1	DSSS - BPSK
Desk Mini Cisco	dBm(地域によって異なる)	2 Mbps	1	DSSS - QPSK
Room Bar		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	変調
			トリー	
			Д	
	最大送信電力=21	6 Mbps	1	OFDM - BPSK
	dBm(地域によって異なる)	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	変調
			トリー	
			4	
	最大送信電力=20	7 Mbps (MCS 0)	1	OFDM - BPSK
	dBm(地域によって異なる)	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

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	変調
			トリーム	
Cisco Codec EQ	最大送信電力=19	6 Mbps	1	OFDM - BPSK
Cisco Room Bar Pro	dBm(地域によって異なる)	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	変調
			トリー	
			<u></u> Д	
	最大送信電力=19	7 Mbps (MCS 0)	1	OFDM - BPSK
	dBm(地域によって異なる)	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	2	OFDM - 16 QAM
	12) 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	15 Mbps (MCS 0)	1	OFDM - BPSK
dBm(地域によって異なる)	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	7 Mbps (MCS 0)	1	OFDM - BPSK
dBm (地域によって異なる)	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	変調
		トリー	
		<u> </u>	
最大送信電力=18	15 Mbps (MCS 0)	1	OFDM - BPSK
dBm(地域によって異なる)	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	変調
		トリーム	
最大送信電力=17	33 Mbps (MCS 0)	1	OFDM - BPSK
dBm(地域によって異なる)	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	最大送信電力=22	1 Mbps	1	DSSS - BPSK
Cisco Room Bar Pro	dBm(地域によって異なる)	2 Mbps	1	DSSS - QPSK
		5.5 Mbps	1	DSSS - CCK
		11 Mbps	1	DSSS - CCK
	2.4 GHz - 802.11g	データレート	空間ス トリー ム	変調
	最大送信電力=21	6 Mbps	1	OFDM - BPSK
	dBm (地域によって異なる)	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	7 Mbps (MCS 0)	1	OFDM - BPSK
	dBm (地域によって異なる)	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、<u>https://cae-cnc-</u> 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が、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。

<u>容量</u>

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。

<u>マルチキャストオーディオ</u>

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

<u>音声品質</u>

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	ドイツ語	ポルトガ
語		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	イタリア語	スウェー
語		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	ノルウェー語	
ド語		

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

デバイスの手入れ

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に推奨されている周波数帯域です。

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

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

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。



39

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



Minimum 20% Overlap

5 GHz の場合、南・北・中央アメリカでは 25 チャネル、欧州では 16 チャネル、日本では 19 チャネルを使用できます。 UNII-3 を使用可能な場所では、UNII-1、UNII-2、および UNII-3 を使用して 12 チャネル セットを利用することが推奨されます。 Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド

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

2.4 802.11 (b/g/n/ax)

通常は、アクセスポイントに手動でチャネルを割り当てる代わりに、アクセス ポイントで自動チャネル選択を使用することを推奨します。 断続的な干渉源が存在する場合は、そのエリアにサービスを提供しているアクセス ポイントにチャネルを静的に割り当てる必要があります。

2.4 GHz (802.11b/g/n/ax) 環境では、VoWLAN

を導入するとき、帯域の重なりのないチャ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ネルとは、22 MHz の間隔があり、少なくとも5 チャ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ネルは3つしか存在しません(チャネル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ネルを使用する必要があり、隣接チャ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。



Minimum 20% Overlap

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ネル上に SNR が 25 dB の最低でも -67 dBm の信号を持つアクセス ポイントを 2 つ以上設置することが推奨されます。

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

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

を有効する必要があります。上記の各要件を考慮すると、シングル

チャネル計画は導入すべきではありません。



アクセス

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

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

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

電子レンジは、2450 MHz で動作します。これは、802.11b/g/n/ax のチャネル8と9 の間に位置します。一部の電子レンジは他のものよりもシールドが強化されており、エネルギーの拡散が低減され ています。電子レンジのエネルギーは、チャネル11 に悪影響を及ぼす可能性もあります。さらに一部の電子レンジは、周波数範囲全体(チャネル1~ 11)に影響します。電子レンジの干渉を回避するために、電子レンジの近くに配置されるアクセスポイントでは、 チャネル1を使用してください。 ほとんどの電子レンジ、Bluetooth、および周波数ホッピングデバイスは、5 GHz

はとんどの電子レンシ、Bluetooth、およい周波数ホッピンクテハイスは、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。 Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド ただし、免許申請の必要のない5 GHz 周波数を利用する製品も存在します(たとえば、5.8 GHz コードレス電話機も、UNII-3 チャネルに悪影響を及ぼす可能性があります)。



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

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

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

ites / S1/	SI-21/3rd Floor 4 5	Gidt * Coverson *	Recompute Refresh	O Search on man			Edit Data Charts Segments Tools
1007 007		GHZ · Coverage ·	Recompute Reliesh	o dearen en map			Luit Data Charts Segments Tools
0	OR THE	50 m		150 m 200 m	25	0 m 300 m	Access Points (43)
ŏ	D(L)A)	sjc21-32a-ap2	000	000	000	sjc21-31a-ap6	Display Label Name
1	sjc21-32a-ap1	in ante	sjc21-32a-ap3	sjc21-31a-ap4	sjc21-31a-ap5	18 8 3 1 1 8 8	Air Quality OAverage AQ CMinimum AQ
35	4 9		And the state	and and a start of	(21-31a:an11)	542 0 142 0 1	Heatmap Opacity (%)
Im	004	sjc21-32a-ap8	600	sic21-31a-an10	,	(CLO)	0 10 20 30 40 50 60 70 80 90 100
	sjc21-32a-ap7	1 INTERNA	sjc21-32a-ap9	COLUMN STREET		sjc21-31a-ap12	
			MARTIN ALE TALK		1361	ALL AND A	0 10 20 30 40 50 60 70 80 90 100
	I I I I I I I	and the second	- 000	600	000	600	KSSI Cut on (dBm)
	sic21,32a,a013	(CO)	sic21-32a-an15	sic21-31a-ap16	sjc21-31a-ap17	sjc21-31a-ap18	
	e star star spins	5)C21-328-8014		- 0g0 g		no los significantes	60 63 66 69 77 75 78 81 84 87 90
	10	4 D	toria di	2000		Contraction of the second second	Map Opacity (%)
	600	March March	AND COM	- Maria	100		0 10 20 30 40 50 60 70 80 90 100
	sjc21-32a-ap1	9		sic21-31a	-ap23	000	
		The second second	sjc21-328-ap21	000	sjc2	1-31a-ap24	0 10 20 30 40 50 60 70 80 90 100
	-	5jc21-32a-ap20		sjc21-31a-ap22	HAT		Show Mobility Express Off
	100	Barri and	P.	-		600	Overlay Objects
	sjc21-32a-ap25	000	600) sjc21-32a-ap27	sic21-31a-ap28	31a-ap29	sjc21-31a-ap30	MSE / CMX Settings
		Jc21-328-8026	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The second second			Map Properties
	900	· ·	Telet	1 Later -			
	e sjc21-32a-ap31	60.0	000	sic21-31a-an34	6 C 0	sjc21-31a-ap36	
	R	sjc21-32a-ap32	sjc21-32a-ap33		5/21-518-8955		
	100	La partienzam	the second se	000	and the second second	The second second	
	600	Tomas 12	(blba) sjc2	1-31a-ap40	(CL)	6.0.0	
	sjc21-32a-ap37	Cic21-222-2028	sjc21-32a-ap39	sic21-31a-ap	sjc21-31a-ap42	sjc21-31a-ap43	

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。

<u>5 GHz</u>

802.11 モード	必須	サポートされる	無効な
	データ レート	データ レート	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	$18 \sim 54 \text{ Mbps}$	6、9 Mbps
		VHT MCS 0 \sim MCS 91SS、VHT MCS 0 \sim MCS 92SS、(VHT MCS 0 \sim MCS9 3SS)、(VHT MCS 0 \sim 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	$18 \sim 54 \text{ Mbps}$	6、9 Mbps

2.4 GHz

802.11 モード	必須	サポートされる	無効な
	データ レート	データ レート	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	$18 \sim 54 \text{ Mbps}$	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ことがあります。

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。

ー部のエリアで一体型内部アンテナを搭載したアクセス ポイントを使用する場合は、アクセス ポイントを天井に取り付けることを推奨します。これらのアクセス

ポイントは無指向性アンテナを装備しており、壁面への設置を想定していません。

周波数帯域

これまで通り、5 GHzの使用が推奨されます。2.4 GHz

を使用すると、正常に機能しない場合があります。802.11b レートが有効な場合は特に注意が必要です。 5 GHz チャネル セットでは、8 または 12

チャネル計画のみを使用することを推奨します。可能な場合は、UNII-2 拡張チャネルを無効にします。

データ レート

マルチパスが高いレベルにある場合は、標準の推奨データレート セットが適切に機能しない可能性があります。そのため、低いデータレート(6 Mbps など)を有効にしてこのような環境での運用を改善させることを推奨します。 音声専用に使用する場合は、24 Mbpsを超えるデータ

レートを無効にして最初の伝送成功率を上げることができます。同じ帯域をデータ、ビデオ、その他のア プリケーションにも使用する場合は、より高いデータレートを有効にすることをお勧めします。

送信電力

条件の厳しい環境ではマルチパスが高くなる可能性があることから、アクセスポイントと 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)。

CiscoRoomOSSeries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。

<u>信号振幅の増大</u>

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 \geq 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 サーバー上で **[匿名インバンドPACプロビジョニングを許可する(Allow anonymous in-band PAC provisioning)]** を有効にしてください。

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

が有効な場合、EAP-GTCと EAP-MSCHAPv2の両方も有効にする必要があります。EAP-FAST

では、認証サーバ上にユーザアカウントを作成する必要があります。

実稼働ワイヤレス LAN 環境内で匿名 PAC プロビジョニングが許可されていない場合は、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 サーバーをセットアップできます。

これには、ステージング RADIUS サーバをスレーブ EAP-FAST

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

EAP-FAST のマスターキーおよびポリシーがステージングスレーブ EAP-FAST RADIUS

サーバーに送信されるように、実稼働マスター EAP-FAST RADIUS

サーバーがセットアップされていることを確認します。これにより、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ー上に、ユーザーアカウントを作成する必要が生じることがあります。

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

Extensible Authentication Protocol - Tunneled Transport Layer Security(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。

認証サーバーは、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	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
Voice	Webex	EF (46)	5	6	RTP (UDP 5004)
TelePresence	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
ヒナオ	Webex	AF41 (34)	4	5	RTP (UDP 5004)
コール制御	CUCM	CS3 (24)	3	4	SIP (TCP 5060 \sim 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。<u>https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf</u>

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。

Cisco RoomOS Series にはバッテリ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	オデオコデク	オーデ イオ 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	802.11 チード	オーディ	オーディ	ビデ オタ	ビデオ解 	ビデオ ビット
コール		オ	ビット	イプ		レート
		デック				
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。

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTI	ROLLER W <u>I</u> RELESS	SECURITY	M <u>A</u> NAGEMENT C <u>O</u> MMA	NDS HELP	<u>F</u> EEDBACK
Wireless	802.11a Global Paramet	ers				
Access Points All APs Radios	General			Data Rates**		
Global Configuration	802.11a Network Status	Enabled		6 Mbps	Disabled	٥
Advanced	Beacon Period (millisecs)	100		9 Mbps	Disabled	٥
Mesh	Fragmentation Threshold	2346		12 Mbps	Mandatory	0
AP Group NTP	DTPC Support.	Enabled		18 Mbps	Supported	۵
> ATE	Maximum Allowed Clients	100		24 Mbps	Supported	0
PE Profiler	RSSI Low Check	Enabled		36 Mbps	Supported	0
FlexConnect Groups	RSSI Threshold (-60 to -90	-80		48 Mbps	Supported	0
FlexConnect ACLs				54 Mbps	Supported	٥
FlexConnect VLAN	802.11a Band Status		CCX Location Measurement			
Templates	Low Band	Enabled		Mode	Enabled	
Network Lists	Mid Band	Enabled		Interval (seconds)	60	
▼ 802.11a/n/ac/ax	High Band	Enabled		,		
Network RRM				TWT Configuration *	**	
RF Grouping				Target Waketime	Enabled	
TPC DCA				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。

 cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTR	OLLER W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11b/g Global Parame	ters					
Access Points All APs	General			Data Rates*	*		
Global Configuration	802.11b/g Network Status	Enabled		1 Mbps	C	isabled	0
Advanced	802.11g Support	Enabled		2 Mbps	D	isabled	0
Mesh	Beacon Period (millisecs)	100		5.5 Mbps		isabled	0
AP Group NTP	Short Preamble	Enabled		6 Mbps		isabled	0
ATF	Fragmentation Threshold (bytes)	2346		9 Mbps		Disabled 📀	
PF Profiles	DTPC Support.	Enabled		11 Mbps		isabled	\$
ElexConnect Groups	Maximum Allowed Clients	100		12 Mbps	M	landatory	٥
FlexConnect ACLs	RSSI Low Check	Enabled		18 Mbps	S	upported	0
ElexConnect VI AN	RSSI Threshold (-60 to -90	-80		24 Mbps	s	upported	0
Templates	abm)			36 Mbps	S	upported	
Network Lists	CCX Location Measureme		48 Mbps	S	upported		
802.11a/n/ac/ax	Mode	Enabled		54 Mbps	S	upported	0
802.11b/g/n/ax Network	Interval (seconds)	Interval (seconds) 60		TWT Configuration ***			
▼ RRM				Target Waket	ime		C Enabled
RF Grouping TPC				Broadcast TW	T Support		🗹 Enabled

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

	uluilu cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
W	ireless	802.11a/n	/ac/ax C	isco APs > C	onfigure							
•	Access Points All APs Radios 802.11a/n/ac/ax	Genera	I					RF Chann	el Assig	nment		
	802.11b/g/n/ax	AP Na	me		rtp9-31a	i-ap1		Current C	hannel		(48,44)	
	Global Configuration	Admin	Status		Enable	0		Channel V	Vidth *		40 MHz 🗘	
	Advanced	Operat	tional State	s	UP			* Channel wi mode	dth can be	e configured or	nly when channel configuration is in custor	n
	Mesh	Slot #			1			Assignme	nt Method		Global	
•	AP Group NTP	11n Pa	rameter	s							Custom	
	ATF	-						Radar Inf	ormatio	n		
	RF Profiles	11n Supported Yes						ormatio				
	FlexConnect Groups	CleanA	ir					Channel		Last Hea	ard(Secs)	
•	FlexConnect ACLs							No radar det	ected char	nnels		
	FlexConnect VLAN	CleanA	Air Capable		Yes			21203				
	Templates	CleanA	Air Admin S	Status	Enable			Tx Power Level Assignment				
	Network Lists	* CleanA	ir enable w	ill take effect only	if it is enabled	on this band.		Current T	e Power Le	evel	1	
۲	802.11a/n/ac/ax	Numbe	er of Spect	rum Expert	0			Assignme	nt Method		Global	
Þ	802.11b/g/n/ax	connex	Cuons								Custom	
Þ	Media Stream	Antenn	a Param	eters								
Þ	Application Visibility And Control	Antenr	па Туре		Interna A			Performa	nce Prof	file		
	Lync Server	Antenr	na		B C			View and	edit Perfor	rmance Profile	for this AP	
	Country				D			Perform	mance Pro	ofile		
	Timers							Note: Chang	ing any of	the parameter	rs causes the Padio to be temporarily disa	blad
•	Netflow							and thus ma	y result in	loss of connec	tivity for some clients.	
•	QoS											

Auto RF (RRM)

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

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

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

5 GHz

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

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネルの幅を 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ネル幅を使用することを推奨します。

	uluili. cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
1	Wireless	802.11a > RRM > Dynamic Channel Assignment (DCA)								
	 Access Points All APs Radios Global Configuration 	Dynamic Channel Assignment Algorithm								
+		n Channel Assignment Method Avoid Foreign AP interference			OAutomatic Interval: 10 minutes OAutomatic O OFreeze Invoke Channel Update Once					
	Advanced									
	Mesh				OFF					
	AP Group NTP				Enabled					
•	ATF	Avoid Cisco AP load			Enabled					
	RF Profiles	Avoid non-802.11a noise Avoid Persistent Non-WiFi Interference			Enabled					
	ElexConnect Groups				Enabled					
	ElexConnect ACLs	Channel Assignment Leader			RTP9-32A-WLC3 (10.81.6.70)					
	FlexConnect VLAN Templates	Last Auto Channel Assignment			556 secs ago					
		DCA Channel Sensitivity			Medium ᅌ (15 dB)					
	Network Lists	Channel Width			○20 MHz					
	802.11a/n/ac/ax	Avoid chee	ck for non-l	DFS channel	Enabled					
	Network RRM RE Grouping	DCA Channel List								
	TPC DCA Coverage General Client Roaming Media EDCA Parameters	36, 40, 44, 48, 52, 56, 60, 64, 100, 153, 157, 161 DCA Channels								

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

2.4 GHz 帯域では使用可能なチャネルの数が限られているために、40 MHz に対応した Cisco 製の 802.11n/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。
ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK			
Wireless	802.11b >	RRM >	Dynamic Cha	nnel Assigr	nment (DC	A)						
Access Points All APs Radios	Dynamic	Channel	Assignment A	Igorithm	Interval	10 minutes	AnchorTime					
Global Configuration	channer	ssignment	Hethou	Crease	Terrela	Channel Hadata	one l					
Advanced				OFfeeze	TUACK	Channel Opdate	Once					
Mesh				OFF								
AP Group NTP	Avoid For	eign AP int	erference	Enabled								
) ATE	Avoid Cise	co AP load		Enabled								
RF Profiles	Avoid non-802.11b noise			C Enabled								
FlexConnect Groups	Avoid Per	sistent won	-wiri interierence	Enabled								
FlexConnect ACLs	Channel A	Assignment	Leader	RTP9-32A-WLC3 (10.81.6.70)								
ElevConnect VI AN	Last Auto	Channel A	ssignment	75 secs ago								
Templates	DCA Char	nnel Sensiti	vity	Medium ᅌ	(10 dB)							
Network Lists	DCA Chan	nel List										
802.11a/n/ac/ax												
 802.11b/g/n/ax Network 		1,	6, 11									
▼ RRM	DCA Char	nnels										
RF Grouping												
DCA					11.							
Coverage												

使用する周波数帯域に応じて 5 GHz または 2.4 GHz

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネルの幅を 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。

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

すべてのアクセスポイントで同じチャネル幅を使用することを推奨します。

	սիսիս cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
Wir	eless	802.11a/n	/ac/ax C	isco APs > C	onfigure							
+ / +	Access Points All APs Radios	Genera	al					RF Channe	el Assig	nment		
	802.11b/g/n/ax Dual-Band Radios	AP Na Admir	ime Status		rtp9-31a	a-ap1		Current C Channel V	hannel Vidth *		(48,44)	
+ /	Global Configuration	n Operational Status UP					* Channel wi mode	idth can be	e configured or	nly when channel configuration is in custom		
	1esh	Slot #			1			Assignme	nt Method		Global	
+ /	AP Group NTP	11n Pa	rameter	s							Custom	
+ 1	TF							Radar Inf	ormatio	n		
	RF Profiles	11n Supported		Yes	Yes						_8	
	lexConnect Groups	CleanA	lir					Channel		Last Hea	ard(Secs)	
E I	FlexConnect ACLs		0.21.222					No radar det	ected char	nnels		
	lexConnect VLAN	Clean	Air Capable		Yes			Tx Power	Level A	ssianment		
	emplates	* CleanA	Air Admin s Air enable w	ill take effect only	if it is enabled	on this band.						18
	Retwork Lists	Numb	er of Spect	rum Expert				Current T	k Power Le	evel	1	
	02.11a/11/ac/ax	conne	ctions	rum expert	0			Assignme	nt Method		Global	
	soz.110/g/n/ax	Antenr	na Param	eters							Custom	
1	redia Stream	Anten	na Type		Interna							
+ 1	And Control				A			Performa	nce Prof	file		
	ync Server	Anten	na		B C			View and	edit Perfor	mance Profile	for this AP	
	Country				D			Perform	mance Pro	ofile		
1	Timers							Note: Chang	ing any of	the parameter	rs causes the Radio to be temporarily disabled	-3
) I	letflow							and thus ma	y result in	loss of connec	tivity for some clients.	
+ 0	QoS											

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。スキャニングとローミングはデバイス側が独立して管理します。

EDCA パラメータ

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

cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless									
 Access Points All APs Radios 	General	ile		Vaice	& Video Ontim	ized			
Global Configuration Advanced Mech	Enable Lov	w Latency I	MAC 1						
 AP Group NTP ATF 	Low latency I	Mac feature	e is not supported	for 1140/1250,	/3500 platform	s if more than 3 da	ta rates are enal	bled.	

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。

uluili. cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> REL	ESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless Access Points All APs Radios Global Configuration	802.11h G	Biobal P nstraint	int(0-30)	0	dB					
 Auvanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups 	Channel S Channel A Channel S Channel C Radar Bla	Switch A Announcem Switch Cour Quiet Mode Ocklist	nnouncement lent nt	0						
FlexConnect ACLs	Smart DF	S								

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に構成されていることを確認します。

Cisco RoomOS Series は、HT MCS 0 \sim MCS 15 と VHT MCS 0 \sim 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。

	uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurit	Y M <u>A</u> NAGEM	ent c <u>o</u>	MMANDS	HELP	<u>F</u> EEDB	ACK	
Wi	reless	802.11n/a	c/ax (5	GHz) Through	put								
•	Access Points All APs	General								MCS	Data	Rate ¹) Settings	
	Radios Global Configuration	11n Mode			🗹 Enat	oled 3				0	(7	Mbps)	Supported
	Advanced	11ac Mode	е		🗹 Enat	oled 3				1	(14	Mbps)	Supported
	Mesh	11ax Mod	e		🗹 Enat	oled 3				2	(21	Mbps)	Supported
	AP Group NTP	VUT MCC	Dates							3	(29	Mbps)	Supported
1	ATE	VHIMCS	Rates				7.5			4	(43	Mbps)	Supported
1	DE Drofilos	SS1								5	(58	Mbps)	Supported
	ElexConnect Grouns	0-8			Enat	oled 4				6	(65	Mbps)	Supported
	FlexConnect ACLs	0-9			C Enat	oled 4				7	(72	Mbps)	Supported
	FlexConnect Acts									8	(14	Mbps)	Supported
	Templates	SS2								9	(29	Mbps)	Supported
	Network Lists	0-8			Enat	oled 4				10	(43	Mbps)	Supported
•	802.11a/n/ac/ax	0-9			Enat	oled 4				11	(58	Mbps)	Supported
	Network	SS3								12	(87	Mbps)	Supported
*	RF Grouping	0-8			Enat	oled 4				13	(116	Mbps)	Supported
	TPC	0-9			C Enat	oled 4				14	(130	Mbps)	Supported
	Coverage									15	(144	Mbps)	Supported
	General	SS4								16	(22	Mbps)	Supported
	Client Roaming Media	0-8			Enat	oled 4				17	(43	Mbps)	Supported
	EDCA Parameters	0-9			Enat	oled 4				18	(65	Mbps)	Supported
	DFS (802.11h) High Throughput	HE MCS R	ates							19	(87	Mbps)	Supported
	(802.11n/ac/ax)									20	(130	Mbps)	Supported
	CleanAir	SS1			SS2					21	(173	Mbps)	Supported
	802.11b/g/n/ax	0-7	✓ E	nabled	0-7	1	Enabled			22	(195	Mbps)	Supported
*	Media Stream	0-9	E	nabled	0-9	1	Enabled			23	(217	Mbps)	Supported
F.	Application Visibility And Control	0-11	E	nabled	0-11		Enabled			24	(29	Mbps)	Supported
	Lunc Server	553			554					25	(58	Mbps)	Supported
	Country	0-7		nabled	0-7		Enabled			26	(87	Mbps)	🗹 Supported
	Timore	0-9		nabled	0-0		Enabled			27	(116	Mbps)	Supported
	Netflow	0-11		nabled	0-11		Enabled			28	(173	Mbps)	Supported
	Action and a second sec	0-11		naoidu	0-11		LINGUICU			29	(231	Mbps)	Supported
P	Qos	SS5			SS6					30	(260	Mbps)	Supported
		0-7	✓ E	nabled	0-7	\checkmark	Enabled			31	(289	Mbps)	Supported

フレームの集約

フレームの集約は複数の MAC プロトコル データ ユニット(MPDU)または MAC サービス データ ユニット(MSDU)を一緒にパッケージングして、順スループットとキャパシティが最適になる点でオーバーヘッ ドを低減するためのプロセスです。 MAC プロトコル データ ユニット(A-MPDU)の集約にはブロックの確認応答を使用する必要があります。

Cisco 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。

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:			

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

802.11n Status:

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。

ululu cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK			
Wireless	802.11a >	CleanA	ir	-								
Access Points All APs Radios Global Configuration	CleanAir/ CleanAir	Spectru										
Advanced	Spectrum	Intelligend										
Muvanceu	Report In	terferers										
Mesn	Persistent	t Device Pr										
P AP Group NTP												
▶ ATF	Interfer	ences to I	gnore		Interfe	erences to Detect						
RF Profiles	Canop	y			TDD	Transmitter						
FlexConnect Groups	WiMax	Fixed		>	Jamn	ner	tor					
FlexConnect ACLs	51_FH:	55		<	DECT	-like Phone	ller					
FlexConnect VLAN					Video	Camera						
Network Lists	Trap Conf	rap Configurations										
▼ 802.11a/n/ac/ax	Enable AC	QI(Air Qual										
Network	AQI Alarn	n Threshold	i (1 to 100) ²				35					
RF Grouping	Enable tra	ap for Uncla	assified Interferend	es								
TPC	Threshold	for Unclas	sified category tra	p (1 to 99)								
Coverage	Enable tra	ap for Class	sified Interferences				Enabled					
General	Threshold	for Classif	ied category trap (1 to 99)			0					
Client Roaming	Enable In	terference	For Security Alarm				Enabled					
EDCA Parameters												
DFS (802.11h)	Do not t	rap on the	ese types		Trap o	n these types						
High Throughput (802.11n/ac/ax)	TDD Tr	ransmitte	r		Jamn	ner		1				
CleanAir	Contin	uous Trai	nsmitter	>	WiFi	Inverted						
802.11b/g/n/ax	DECT-I Video (like Phon Camera	e	<	WiFi	Invalid Channel						
Media Stream	SuperA	AG										
Application Visibility And Control	Event Driv	ven RRM	(<u>Change Settings</u>	D.								
Lync Server	EDRRM			Disabled								
Country	Sensitivit	y Threshold	и н	I/A								
Timers	Rogue Co	ntribution	Ν	I/A								
Netflow	Rogue Du	ity-Cycle	Ν	I/A								
▶ QoS	(1)Device Se (2)AQI value (3)Spectrum	ecurity alar 100 is bes Intelligen	ms, Event Driven I st and 1 is worst ce does not send ti	RRM and Persisi	ence Device A	voidance algorithm	n will not work if I	nterferer	s reporting is disabled.			

սիսիս cisco	MONITOR WLANS CONTROLLER	. WIRELESS SECURITY MANAGEMENT	. COMMANDS HELP FEEDBAC	ж		
Wireless	802.11a/n/ac/ax Cisco APs >	Configure				
Access Points All APs Radios Ro2 112/p/oc/or	General		RF Channel Assignment			
802.11b/g/n/ax	AP Name	rtp9-31a-ap1	Current Channel	(48,44)		
Dual-Band Radios	Admin Status	Enable ᅌ	Channel Width * 40 MHz 🗘			
Advanced	Operational Status	UP	* Channel width can be configured mode	d only when channel configuration is in custom		
Mesh	Slot #	1	Assignment Method	Global		
AP Group NTP	11n Parameters			Custom		
▶ ATF			Radar Information			
RF Profiles	11n Supported	Yes				
FlexConnect Groups	CleanAir		Channel Last	Heard(Secs)		
FlexConnect ACLs			No radar detected channels			
FlexConnect VLAN	CleanAir Capable	Yes	To Devent work Andrews			
Templates	CleanAir Admin Status	Enable ᅌ	TX Power Level Assignme	nt		
Network Lists	* CleanAir enable will take effect on	ly if it is enabled on this band.	Current Tx Power Level	1		
802.11a/n/ac/ax	Number of Spectrum Expert	0	Assignment Method	Global		
802.11b/g/n/ax	connections			Custom		
Media Stream	Antenna Parameters		-	0		
Application Visibility And Control	Antenna Type	Internal ᅌ A 🗹	Performance Profile			
Lync Server	Antenna	в 🗹 с 🗸	View and edit Performance Pro	file for this AP		
Country		D 🗹	Performance Profile			
Timers			Note: Changing any of the param	eters causes the Radio to be temporarily disabled		
Netflow			and thus may result in loss of con	nectivity for some clients.		
▶ QoS						

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。

 cısco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	Rx Sop T	hreshol	d	-					
 Access Points All APs Radios Global Configuration 	Rx Sop T Rx Sop T	hreshold 8 hreshold 8	02.11a Defa 02.11b Defa	ult ᅌ O	Custom				
 Advanced RF Management Flexible Radio Assignment Load Balancing DTLS Band Select Rx Sop Threshold Optimized Roaming Network Profile 	1 Rxsop o	nly suppor	ted in Local,Flex,B	ridge and Flex-	-Bridge mode A	ips.			

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。

.ılı.ılı. cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs >	New							
WLANs WLANs Advanced	Type Profile Na SSID ID	me	WLA voice 6	N O					

،، ،،، ،، cısco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> ON	ITROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK								
WLANs	WLANs > Edit 'voice'									
VLANs	General Security	QoS Policy-Mapping Advanced								
Advanced	Profile Name	voice								
	Туре	WLAN								
	SSID	voice								
	Status	C Enabled								
	Security Policies	[WPA2][Auth(FT 802.1X)] (Modifications done under security tab will appear after applying the changes.)								
	Radio Policy	802.11a only								
	Interface/Interface Group(G)	rtp-9 voice								
	Multicast Vlan Feature	Enabled								
	Broadcast SSID	Enabled								
	NAS-ID	RTP9-32A-WLC3								
	Lobby Admin Access									

[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。

uluulu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'voice'
WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 2 WPA+WPA2 3 Security Type Enterprise 3 MAC Filtering 2 WPA+WPA2 Parameters WPA Policy WPA2 Policy 3 WPA2 Encryption CCCMP128(AES) TKIP CCMP256 GCMP128 GCMP256 OSEN Policy Fast Transition Fast Transition Enable 3 Over the DS
	Reassociation Timeout 20 Seconds
UIIIII CISCO WLANS	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANS	General Security QoS Policy-Mapping Advanced
▶ Advanced	PMF Disabled Authentication Key Management 12 802.1X-SHA1 © Enable 802.1X-SHA2 Enable FT 802.1X ✓ Enable CCKM Enable WPA GTK-randomize State 14 Disable



ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	ONTROLLER WIRELESS	<u>s</u> ecurity M <u>A</u> I	NAGEMENT C <u>O</u> MM	ANDS HE <u>L</u> P <u>F</u> EEDBAC	ск
WLANs	WLANs > Edit 'voi	ce'				
VLANS WLANS Advanced	General Security Protected Management PMF	y QoS Policy-Maj	oping Advance	d		
	PSK Format 21	ASCII ©				
	PSK PSK-SHA2	Enable Enable Enable				
	WPA GTK-randomize Sta	te 14 Disable 😌				

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。

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	<u>F</u> EEDBACK
VLANS VLANS VLANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS > Edit 'voice' General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled Authentication Servers Cenabled Server 1 None Servers Server 2 None None Server 3 None None Server 4 None None Server 5 None None	EEEDBACK but(200 to 5000 millisec) 400 es(0 to 4) 4 Timeout(1 to 120 sec) 30 Retries(1 to 20) 2 (1 to 120 sec) 30
	Server 6 None None Request Retries(1 Authorization ACA Server Enabled	1 to 20) 2

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 QBSS が有効になります。

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER W <u>I</u> RE	eless <u>s</u> ecur	RITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
WLANs	General Security	QoS Polic	y-Mapping	Advanced			
▶ Advanced	Quality of Service (QoS) Application Visibility AVC Profile Flex AVC Profile Netflow Monitor Fastlane Override Per-User Ban	Platinum (vo Platinum (vo Finaled none none Disable Disable Disable Disable Disable	ice) O C acts (kbps) ¹ UpStream	<u>e</u>			
	Average Data Rate	0	0				
	Burst Data Rate	0	0				
	Average Real-Time Rate	0	0				
	Burst Real-Time Rate	0	0				

cisco	MONITOR WLANS CONT	roller w <u>i</u> rei	LESS <u>S</u> ECURIT	Y M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'					
WLANS WLANS	General Security Override Per-SSID Ba	QoS Policy	-Mapping A acts (kbps) <u>16</u>	Advanced		
		DownStream	UpStream			
	Average Data Rate	0	0			
	Burst Data Rate	0	0			
	Average Real-Time Rate	0	0			
	Burst Real-Time Rate	0	0			
	Clear					
	WMM					
	WMM Policy	Required ᅌ	J.	70		
	7920 AP CAC	Enabled				
	7920 Client CAC	Enabled				
	Media Stream			28		
	Multicast Direct	Enabled				
	Lync Policy					
	Audio	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もお勧めします。

[Aironet 拡張機能 (Aironet IE)]を有効にします。

[ピアツーピア (P2P) のブロッキングアクション (Peer

to Peer (P2P) Blocking Action)] は

[無効 (Disabled)]にします。必要に応じて

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

[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。

տիտիս cisco	MONITOR WLANS CONTROL	LLER WIRELESS <u>S</u> ECURITY MANAGEMEN	IT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'		
 ▼ WLANs ▶ Advanced 	General Security Quadratic control of the security Allow AAA Override Coverage Hole Detection Coverage Hole Detection Enable Session Timeout Coverage Hole Detection Coverage Hole Detection	oS Policy-Mapping Advanced Carabled Sensabled Session Timeout (secs) Carabled	DHCP DHCP Server DHCP Addr. Assignment Required Management Frame Protection (MFP)
	Diagnostic Channel 18 Override Interface ACL IF Layer2 Acl URL ACL P2P Blocking Action Client Exclusion 3 Maximum Allowed Clients 8 Static IP Tunneling 11	Enabled Pv4 None © IPv6 None © None © Disabled © Enabled 0 Enabled	MFP Client Protection 4 Optional C DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 2 802.11b/g/n (1 - 255) 2 NAC NAC State None C Load Balancing and Band Select
	Maximum Allowed Clients	200	Client Load Balancing

	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY MANAGEMENT	C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	
WLANs	WLANs > Edit 'voice'			
WLANS	General Security	QoS Policy-Mapping Advanced		
Advanced	Clear HotSpot		Passive Client	
	Configuration	Enabled	Passive Client	
	Client user idle		Voice	
	timeout(15-100000)		Media Session Snooping	Enabled
	Client user idle threshold (0-10000000)	0 Bytes	Re-anchor Roamed Voice Clients	Enabled
	Radius NAI-Realm		KTS based CAC Policy	Enabled
	11ac MU-MIMO		Radius Client Profiling	
	WGB PRP	Enabled	DHCP Profiling	
	MBO State		HTTP Profiling	
	Off Channel Scanning Defe	r	Local Client Profiling	
	Scan Defer Priority	0 1 2 3 4 5 6 7	DHCP Profiling	
			HTTP Profiling	
	Scan Defer Time(msecs)	100	РМІР	
	Stan Dater Time(insets)	100	PMIP Mobility Type	0
	FlexConnect Local Switching 2	Enabled	PMIP NAI Type	Hexadecimal ᅌ

iiliiilii cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COM	IMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'voice'			
WLANS	General Security QoS Policy-Mapp	Advanced		
Advanced	FlexConnect Local Auth 12 Enabled		PMIP Profile	None 📀
	Learn Client IP Address 5 🗸 🗸 Enabled		PMIP Realm	
	Vian based Central		Universal AP Admin Support	
	Switching 13 Enabled		Universal AP Admin	
	Central DHCP Processing Enabled		11v BSS Transition Support	
	Override DNS Enabled		BSS Transition	0
	NAT-PAT Enabled		Disassociation Imminent	
	Central Assoc Enabled		Disassociation Timer(0 to 3000 TBTT)	200
	Lync		Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
	Lync Server Disabled ᅌ		BSS Max Idle Service	0
	11k		Directed Multicast Service	
	Neighbor List	Enabled	Tunneling	
	Neighbor List Dual Band	Enabled	Tunnel Profile	None ᅌ
	Assisted Roaming Prediction Optimization	Enabled	EOGRE Vlan Override	0
	802.11ax BSS Configuration		mDNS	
	Down Link MU-MIMO	C Enabled	mDNS Snooping	Enabled

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	
WLANs	WLANs > Edit 'voice'			
▼ WLANs	General Security QoS	Policy-Mapping Advanced		
Advanced	802.11ax BSS Configuration		mDNS	
	Down Link MU-MIMO	Enabled	mDNS Snooping	Enabled
	Up Link MU-MIMO	Enabled	TrustSec	
	Down Link OFDMA	Enabled	Security Group Tag	0
	Up Link OFDMA	Enabled	Umbrella	
			Umbrella Mode	Ignore ᅌ
			Umbrella Profile	None ᅌ
			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。

cisco	MONITOR WLA	Ns <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	AP Groups							
VLANs WLANs	Add New AP G	roup						
 Advanced AP Groups 	AP Group Name Description	Add Cancel						

uluilu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EEDBACK
WLANs	Ap Groups > Edit 'rtp'				
WLANs	General WLANs RF Prof	ile APs 802.11u	Location	Ports/Module	Intelligent Capture
 Advanced AP Groups 				Apply	
	AP Group Name	rtp			
	AP Group Description				
	NAS-ID	RTP9-32A-WLC3			
	Enable Client Traffic QinQ				
	Enable DHCPv4 QinQ 3				
	QinQ Service Vlan Id 10	0			
	Fabric ACL Template	None ᅌ			
	CAPWAP Preferred Mode	Not-Configured			
	Custom Web Override-Global 13	Enable			
	External Web auth URL	none			
	NTP Auth	Enable			
	NTP Server	None			

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

uluilu cisco	MONITOR	<u>W</u> LANs		W <u>I</u> RELESS	SECURITY	MANAGEMENT	r c <u>o</u> mmands	HELP <u>F</u> EEDBACK	
WLANs	Ap Group	os > Edit	'rtp'						
WLANs	General	WLA	Ns RF Profi	le APs	802.11u	Location	Ports/Module	Intelligent Capture	
Advanced AP Groups	Add Nev	v						Add New	
	WLAN S	SID	voice(6)		\$				
	/Interfac /Interfa Group(0	ce G)	rtp-9 voice		\$	1			
	SNMP N	IAC State	Enabled	cel					

[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。

WLANS Ap Groups > Edit 'rtp' WLANS General WLANS R	RF Profile APs	802.11u	Location	Ports/Module	Intelligent Capture
WLANS General WLANS R	RF Profile APs	802.11u	Location	Ports/Module	Intelligent Capture
Advanced AP Groups 802.11a none	>			Арріу	

[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。

uluilu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	ONTROLLER WIRELESS	<u>s</u> ecurity	MANAGEMEN	IT C <u>O</u> MMANDS	HELP FEEDBAC	ĸ
WLANs	Ap Groups > Edit 'r	tp'					
WLANs	General WLANs	RF Profile APs	802.11u	Location	Ports/Module	Intelligent Ca	pture
Advanced AP Groups	APs currently in the	Group	Remove APs	Add AP	s to the Group		Add APs
	AP Name	Ethernet MAC			lame	Group Name	
	🗌 rtp9-31a-ap14	00:81:c4:96:78:28					
	rtp9-32a-ap20	00:81:c4:32:b9:b8					
	rtp9-32a-ap23	00:81:c4:96:74:10					

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。

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller	General	
General	Name	RTP9-32A-WLC3
Icons	802.3x Flow Control Mode	Disabled 🗘
Inventory	LAG Mode on next reboot	Enabled 🗘
Interfaces	Broadcast Forwarding	Disabled 🗘
Interface Groups	AP Multicast Mode 1	Multicast 📀 239.1.1.9 Multicast Group Address
Multicast	AP IPv6 Multicast Mode	Multicast 📀 ff1e::239:100:100:21 IPv6 Multicast Group Address
Network Routes	AP Fallback	Enabled 🗘
Fabric Configuration	CAPWAP Preferred Mode	ipv4 ᅌ
Redundancy	Fast SSID change	Enabled 🗘
Mobility Management	Link Local Bridging	Disabled 🗘
Ports	Default Mobility Domain Name	CTG-VoWLAN2
▶ NTP	RF Group Name	RTP9-VoWLAN2
+ CDP	User Idle Timeout (seconds)	300
▶ PMIPv6	ARP Timeout (seconds)	300
Tunneling	ARP Unicast Mode	Disabled 🗘
▶ IPv6	Web Radius Authentication	PAP 📀
▶ mDNS	Operating Environment	Commercial (10 to 35 C)
Advanced	Internal Temp Alarm Limits	10 to 38 C
Lawful Intercention	WebAuth Proxy Redirection Mode	Disabled ᅌ
cawful interception	WebAuth Proxy Redirection Port	0
	Captive Network Assistant Bypass	Disabled 🗘
	Global IPv6 Config	Disabled 🗘
	Web Color Theme 2	Default ᅌ
	HA SKU secondary unit	Disabled ᅌ
	Nas-Id	RTP9-32A-WLC3
	HTTP Profiling Port	80
	DNS Server IP(Ipv4/Ipv6)	171.70.168.183
	HTTP-Proxy Ip Address(Ipv4/Ipv6)	0.0.0.0
	WGB Vlan Client	Disabled 🤤

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

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

cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Multicast	8	S						
General Icons Inventory	Enable Glo Enable IG	obal Multica MP Snoopii	ast Mode	2					
Interfaces	IGMP Time	eout (30-7	200 seconds)	60					
Interface Groups	IGMP Que	ry Interval	(15-2400 seconds	5) 20					
Multicast	Enable ML	D Snoopin	g						
Network Routes	MLD Time	out (30-72	00 seconds)	60					
Fabric Configuration	MLD Quer	y Interval	(15-2400 seconds)	20					
Redundancy									
Mobility Management									
Ports	Foot Notes								
▶ NTP	Changing Glo	bal Multica	ast configuration p	arameters rem	oves configured	d Multicast VLAN fro	om WLAN.		
► CDP									

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。

uluili. cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller General Icons Inventory Interfaces Interface Groups Multicast	Mobility / Keep Aliv Keep Aliv Symmetri DSCP Vali	weaks Anchor (e Count e Interval ic Mobility T ue	Config (1-30 seconds) Funneling mode	3 10 Enabled 0	SECORITY	MANAGEMENT	COMMANDS	неГь	FEEDBACK
 Fabric Configuration Redundancy Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 									

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。

	ဂျက်က cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELES	s <u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
C	ontroller	Static Mo	bility Gr	oup Members	6					
	General Icons	Local M	obility Gro	up CTG-VoV	VLAN2					
	Inventory Interfaces	MAC Ad	dress	IP Address(Ipv4,	(Ipv6) Gro	oup Name	M	ulticast IP	Status	
	Interface Groups	00:5d:7	3:1a:c3:49	10.81.6.70	СТО	G-VoWLAN2	0.0	0.0.0	Up	
	Multicast									
Þ	Network Routes									
۴	Fabric Configuration									
Þ	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。

ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a(5	i GHz) >	Media						
 Access Points All APs Radios Global Configuration 	Voice Call Adm	Video nission C	Media ontrol (CAC)						
 Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ACLs FlexConnect VLAN 	Admissi CAC Me Max RF Reserve Expedit	ion Control ethod 4 Bandwidth ed Roaming ed bandwid C Support	(ACM) (5-85)(%) Bandwidth (0-25) th	 ✓ Er Loa 75 6 ✓ ✓ 	nabled d Based 🗘				
Templates	Per-Call	SIP Ban	dwidth ²						
× 802.11a/n/ac/av	SIP Cod	lec		G.7	11 0				
Network	SIP Bar	ndwidth (kb	ps)	64					
▼ RRM	SIP Voi	ce Sample I	interval (msecs)	20	0				
TPC DCA	Traffic S	Stream M	etrics						
Coverage General Client Roaming Media	Metrics	Collection							
EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac/ax) CleanAir 802.11b/g/n/ax	Foot Not 1 11a rat 11n rat 2 SIP CAO 3 SIP CAO 4 Static C	es es(Kbps): 6 es(Kbps): 6 C should on C will be su CAC methoo	000,9000,12000, 5000,72200,1300 ly be used for pho pported only if SIF is radio based an	18000,24000,3 000,144400,13 nes that suppo snooping is er d load-based C	6000,48000,54 5000,150000,2 rt status code : nabled. AC method is c	4000 270000,300000 17 and do not supp channel based.	ort TSPEC-based	admissio	n control.

[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。

cisco	<u>m</u> onitor <u>w</u> lan	s <u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a(5 GHz)	> Media						
 Access Points All APs Radios Global Configuration Advanced 	Voice Video	Media Control (CAC)						
Mesh	Admission Cont	ol (ACM)	En En	abled				
AP Group NTP	Max RF Bandwie	lth (5-85)(%)	o	ic v				
▶ ATF	Reserved Roam	ng Bandwidth (0-25)	(%) 0					
RF Profiles	SIP CAC Suppor	t 2	🗍 En	abled				
FlexConnect Groups								
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	Foot Notes 1 11a rates(Kbps, 11n rates(Kbps, 2 SIP CAC should 3 SIP CAC will be 4 Static CAC meth	: 6000,9000,12000,1 : 65000,72200,1300 only be used for pho supported only if SIP ord is radio based an	18000,24000,3 00,144400,13 nes that suppo snooping is en load-based C	5000,48000,54 5000,150000,2 t status code : abled. AC method is c	1000 70000,300000 17 and do not supp hannel based.	ort TSPEC-based	admissio	n control.

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)]
[6]
[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)]
[音声最大ストリームサイズ(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)]
[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

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

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。

uhuhu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a(5 GHz) >	Media						
 Access Points All APs Radios Global Configuration 	Voice	Video	Media						
 Advanced Mesh AP Group NTP 	Unicast	Video Redi st Direct	rect Admission Co	Ø ntrol					
ATF RF Profiles FlexConnect Groups	Maximu Client Maximu	ım Media Bi 1inimum Ph ım Retry Pe	andwidth (0-85(% ny Rate 1 ercent (0-100%)	e)) 85 6000 80					
 FlexConnect ACLs FlexConnect VLAN Templates 	Media S	tream - I	Multicast Dire	ct Paramete	irs				
Network Lists • 802.11a/n/ac/ax Network • RRM RF Grouping TPC DCA Coverage General Client Roaming Media	Multica Max St Max St Best Ef	st Direct En reams per F reams per C fort QoS Ad	able Radio Client Imission	Vo No- No- Er	limit 오 limit 😏 labled				
EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac/ax) CleanAir 802.11b/g/n/ax	Foot Not 1 11a rat 11n rat 2 SIP CA 3 SIP CA 4 Static C	es(Kbps): 6 es(Kbps): 6 C should on C will be su CAC method	5000,9000,12000, 55000,72200,1300 Iy be used for pho pported only if SIH I is radio based an	18000,24000,3 000,144400,13 ones that suppo P snooping is en d load-based C	6000,48000,54 5000,150000,2 rt status code abled. AC method is c	4000 170000,300000 17 and do not supp thannel based.	ort TSPEC-based	admissio	n control.

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。

cisco	MONITOR WLANS CONTRO	LER WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile > New						
Access Points All APs Radios	RF Profile Name Radio Policy	rtp-5 802.11a ᅌ					
Global Configuration Advanced	Use default RF Profile Template	None		0			
Mesh AP Group NTP							
ATF RF Profiles							

[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。

uluilu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> R	ELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile	> Edit	'rtp-5'							
Access Points	General	802.1	I1 RRM	High	Densit	y Client	Distribution			
 Radios Global Configuration 	Data Rat	es <u>1</u>	м	ICS Se	ettings					
Advanced										
Mesh	6 Mbps	Disable	d 📀	0	🗹 Supp	orted				
AP Group NTP	9 Mbps	Disable	d ᅌ	1	🖸 Supp	orted				
▶ ATF	12 Mbps	Mandat	ory ᅌ	2	🖸 Supp	orted				
RF Profiles	18 Mbps	Support	ted ᅌ	3	🖸 Supp	orted				
FlexConnect Groups	24 Mbps	Support	ted ᅌ	4	🖸 Supp	orted				
FlexConnect ACLs	36 Mbps	Support	ted ᅌ	5	🖸 Supp	orted				
FlexConnect VLAN	48 Mbps	Support	ted 😒	6	🖸 Supp	orted				
Templates	54 Mbps	Support	ted ᅌ	7	🖸 Supp	orted				
Network Lists				8	🖸 Supp	orted				
802.11a/n/ac/ax				9	🖸 Supp	orted				
802.11b/g/n/ax				10	🖸 Supp	orted				
Media Stream				11	🖸 Supp	orted				
Application Visibility				12	🖸 Supp	orted				
And Control				13	🖸 Supp	orted				
Lync Server				14	Supp	orted				
Country				15	Supp	orted				
Timers				16	🖸 Supp	orted				
Netflow	0									
▶ QoS										

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

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

[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。

cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HEL	LP <u>F</u> EEDBACK		
Wireless	RF Profile > Edit 'rtp-5'					
Access Points All APs Radios Clobal Configuration	General 802.11 RRM High Density	Client Distribution				
Advanced	TPC		Co	overage Hole Detection		
Mesh	Maximum Power Level Assignment (-10 to 30 dBm)	30		Data RSSI(-90 to -60 dBm)	-80	
AP Group NTP	Power Threshold v1(-80 to -50 dBm)	-70		Coverage Exception(0 to 100 %)	-80	
P AIF	Power Threshold v2(-80 to -50 dBm)	-67		Coverage Level(1 to 200 Clients)	3	
FlexConnect Groups	DCA		Pr	rofile Threshold For Traps		
FlexConnect ACLs	Avoid Foreign AP interference	C Enabled		Interference (0 to 100%)		10
Templates	Channel Width 🔷 20 MHz 🧿 40 MHz 🔷 80 MHz 🤇) 160 MHz () 80+80 MHz () Be	st	Clients (1 to 200)		12
Network Lists				Noise (-127 to 0 dBm)		-70
▶ 802.11a/n/ac/ax				Utilization (0 to 100 %)		80
802.11b/g/n/ax			CII	ient Network Preference		
Media Stream				O Connectivity O Throughp	ut 🧿 Automatic	
Application Visibility And Control			Cli	ient Aware		
Lync Server				Enable ODisable		
Country	High-Speed Roam					
Timers	HSR mode		Enabled			
Netflow						
▶ QoS						

iiliiilii cisco	NITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	
Wireless	Profile > Edit 'rtp-5'	
Access Points	eneral 802.11 RRM High Density Client Distribution	
All APS ▶ Radios	Client Aware	
Global Configuration		
Advanced	gh-Speed Roam	
Mesh	HSR mode Enabled	
AP Group NTP	Neighbor Timeout Factor 5	
ATF		
RF Profiles	CA Channel List	
FlexConnect Groups	36, 40, 44, 48, 52, 56, 60, 64, 149, 153,	
FlexConnect ACLs	157, 161	
FlexConnect VLAN Templates	DCA Channels	
Network Lists		
▶ 802.11a/n/ac/ax	Salart Channel	
802.11b/g/n/ax		
Media Stream	40	
Application Visibility	☑ 44	
And Control	48	
Lync Server	S2 52	
Country		
Timers	Extended UNII-2 channels Enabled	
Netflow		
005		

[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。

 cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
Wireless	RF Profile	> Edit	'rtp-5'								
 Access Points All APs Radios Global Configuration 	General	802.1	II RRM	High Density	Client	Distribution					
 Advanced Mesh AP Group NTP 	Maximun Rx Son T	Maximum Clients(1 to 200) 200 Multicast Data Rates ² auto 😳									
ATF RF Profiles	Rx Sop Thresho	Ide C	Default ᅌ O	Custom							

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

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。

	ဂျကျက cisco	MON	IITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEME	NT C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
w	ireless	Flex	conn	ect Gro	ups > New						
•	Access Points All APs Radios Global Configuration	G	roup Nan	ne rtp	-1						
Þ	Advanced										
	Mesh										
۶	AP Group NTP										
۲	ATF										
	RF Profiles										
	FlexConnect Grou	ips									
_	a: a:										
	cisco	MONITOR	<u>W</u> LANs	CONTROLL	ER W <u>I</u> RELESS <u>S</u>	ECURITY MAN	AGEMENT C <u>O</u> M	IMANDS HELP	FEEDBACK		
Wi	reless	FlexConne	oct Grou	ps > Edit	'rtp-1'			200			
	Access Points										
,	All APs Radios	General	Local /	Authentica	tion Image Up	grade ACL M	lapping Cer	ntral DHCP W	LAN VLAN mapping	WLAN A	VC mapping
	Global Configuration	Group N	ame		rtp-1						
*	Advanced	VLAN Ter	nplate Nam	e	none ᅌ						
	AP Group NTP	Enable Al	P Local Auth	nentication ²							
	ATF	FlexConner	t AP								
	RF Profiles	HTTP-Pro	xv								
	FlexConnect Groups	In Addre	es/Inv4/Inv	(6)							
•	FlexConnect ACLs	Port	55(1914)191)	0						
	Templates										
	Network Lists				Add						
F	802.11a/n/ac/ax	AAA									
*	802.11b/g/n/ax	Server I	p Address								
	Media Stream	Server T	уре		Primary 💿						
۲	And Control	Shared S	Secret								
	Lync Server	Confirm	Shared Sec	cret							
	Country	Port Nur	nber		1812						
	Timers	Add									
F	Netflow										
	Qos										

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。

	<u>W</u> LANs		WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
FlexConne	ct Gro	up AP List							
Group Nar	ne			rtp-1					
FlexConnec	ct APs								
Add AP Entries 0 AP MAC A	- 0 of 0 Address	AP Name	SI	tatus	АР Мо	de	Тур	e	Conflict with PnP
	MONITOR FlexConner Group Nat FlexConner Add AP Entries 0	MONITOR WLANS FlexConnect Grou Group Name FlexConnect APS Add AP Entries 0 - 0 of 0 AP MAC Address	MONITOR WLANS CONTROLLER FlexConnect Group AP List Group Name FlexConnect APs Add AP Entries 0 - 0 of 0 AP MAC Address AP Name	MONITOR WLANS CONTROLLER WIRELESS FlexConnect Group AP List Group Name FlexConnect APs Add AP Entries 0 - 0 of 0 AP MAC Address AP Name Si	MONITOR WLANS CONTROLLER WIRELESS SECURITY FlexConnect Group AP List rtp-1 FlexConnect APs	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT FlexConnect Group AP List rtp-1 rtp-1 rtp-1 FlexConnect APs rtp-1 rtp-1 rtp-1 Entries 0 - 0 of 0 AP MAC Address AP Name Status AP Modement	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS FlexConnect Group AP List rtp-1 rtp-1 Group Name rtp-1 rtp-1 FlexConnect APs security rdd AP Entries 0 - 0 of 0 Status AP Mode	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FlexConnect Group AP List rtp-1 rtp-1 FlexConnect APs Image: second application of the second application o	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK FlexConnect Group AP List rtp-1 rtp-1

 cısco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	FlexConn	ect Gro	up AP List						
 Access Points All APs Radios Global Configuration 	Group Na	ime			rtp-1				
Advanced	FlexConn	ect APs							
Mesh AP Group NTP ATF	Add AP Select APs from current controller								
RF Profiles FlexConnect Groups	Ethernet	MAC		Add Cane	cel				

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。

	cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wi	reless	Media Str	ream >G	eneral						
•	Access Points All APs Radios Global Configuration	Multicast Session M	Direct featu	ure 🗹 Config	Enabled					
۲	Advanced	Session a	nnounceme	ent State	Enabled					
	Mesh	Session a	nnounceme	ent URL						
•	AP Group NTP	Session a	nnounceme	ent Email						
÷.	ATF	Session a	nnounceme	ent Phone						
	RF Profiles									
	FlexConnect Groups	Session a	nnounceme	nt Note						
•	FlexConnect ACLs					1				
	FlexConnect VLAN Templates									
	Network Lists									
×.	802.11a/n/ac/ax									
¥.	802.11b/g/n/ax									
•	Media Stream General Streams									

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。
ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless	Media Stream > New
Access Points All APs Radios Global Configuration Advanced Mesh	Stream Name
AP Group NIP ATF RF Profiles FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates	Select from predefined templates Select Average Packet Size (100-1500 bytes) 1200 RRC Periodic update Image: Compare the second
Network Lists 802.11a/n/ac/ax 802.11b/g/n/ax	
 Media Stream General Streams 	

保存すると、メディアストリームが表示されます。

	uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>o</u> mmands he	LP <u>F</u> EEDBACK		
W	ireless	Media Str	reams						Entries 1 - 1 of 1		
•	Access Points All APs Radios	Stream Na 10.195.19.2	me 27				Start IP / 239.1.1.1	Address(Ipv4/Ipv6) End IP Address(Ipv4/Ipv6) 239.1.1.1	Operation Status Multicast Direct	
Þ	Advanced										
Þ	Mesh AP Group NTP										
Þ	ATF RE Profiles										
	FlexConnect Groups										
•	FlexConnect ACLs FlexConnect VLAN Templates										
	Network Lists										
Þ	802.11a/n/ac/ax										
Þ	802.11b/g/n/ax										
•	Media Stream General Streams										

[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。

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER WIRELES	5 <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
WLANs WLANs Advanced	General Security Override Per-SSID Bar Average Data Rate	QoS Policy-Ma ndwidth Contracts DownStream Up	apping Adv 5 (kbps) <u>16</u> Stream	anced			
	Burst Data Rate Average Real-Time Rate Burst Real-Time Rate Clear	0 0 0 0 0 0					
	WMM Policy 7920 AP CAC 7920 Client CAC Media Stream	Required 📀 S Enabled					
	Multicast Direct Lync Policy Audio	 Enabled Silver 					

QoS プロファイル

次の4つの QoS プロファイルを設定します。

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

	uluulu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELES	S <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP				
Wi	reless	Edit QoS	Profile										
•	Access Points All APs Radios Global Configuration	QoS Profi	le Name	platinum For Voice App	lications								
	Advanced												
	Mesh	Per-User	er-User Bandwidth Contracts (kbps) *										
•	AP Group NTP			DownStre	am UpS	ream							
	ATF	Average [Data Rate	0	0								
	RF Profiles	Burst Dat	a Rate	0	0								
	FlexConnect Groups	Average F	Real-Time R	ate 0	0								
	FlexConnect ACLs	Burst Rea	I-Time Rate	0	0								
	FlexConnect VLAN Templates	Per-SSID	Bandwid	th Contracts	(kbps) *								
	Network Lists			DownStre	am UpS	ream							
	802.11a/n/ac/ax	Average [Data Rate	0									
	802.11b/g/n/ax	Burst Dat	a Rate	0									
	Media Stream	Average F	Real-Time R	ate 0									
	Application Visibility	Burst Rea	I-Time Rate	0	0								
1	And Control	WLAN Qo	S Paramo	eters									
	Lync Server	Maximum	Priority	voice	~								
	Country	Unicast D	efault Priori	ty besteffor	t 🗸								
	Timers	Multicast	Default Pric	rity besteffor	t 🗸								
•	Netflow												
-	QoS	Wired Qo	S Protoco										
	Roles	Protocol T	Туре	None	•								
	Qos Map												

	ဂျကျက cisco	MONITOR	WLANs	CONTROLLER	WIR	ELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
W	ireless	Edit QoS	Profile							
•	Access Points All APs Radios Global Configuration Advanced	QoS Profi Descriptio	le Name on	gold For Video Ap	plicatior	15				
	Mesh	Per-User	Bandwid	th Contracts	(kbps) *				
•	AP Group NTP			DownStre	eam	UpStrea	im			
	ATF	Average [Data Rate	0		0				
	RF Profiles	Burst Dat	a Rate	0		0				
	FlexConnect Groups	Average F	Real-Time R	ate 0		0				
	FlexConnect ACLs	Burst Rea	I-Time Rate	0		0				
	FlexConnect VLAN Templates	Per-SSID	Bandwid	Ith Contracts	(kbps	;) *				
	Network Lists			DownStro	am	UpStrea	am			
	802.11a/n/ac/ax	Average [Data Rate	0		0	_			
. •	802.11b/g/n/ax	Burst Dat	a Rate	0		0				
•	Media Stream	Average F				0				
•	Application Visibility And Control	WLAN OO	S Param	eters		0				
	Lync Server	Maximum	Priority	video	~					
	Country	Unicast D	efault Priori	ity video	~					
	Timers	Multicast	Default Pric	ority video	~					
	Netflow)					
-	QoS	Wired Qo	S Protoco	ol						
	Profiles Roles	Protocol 1	Гуре	802.1p	~					
	Qos Map	802.1p Ta	ag	4						

	ာါကျက cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P				
W	ireless	Edit QoS	Profile										
+	Access Points All APs Radios Global Configuration Advanced	QoS Profi Descriptio	ile Name on	bronze For Backgrou	nd								
	Mesh	Per-User	er-User Bandwidth Contracts (kbps) *										
	AP Group NTP			DownStre	am UpStr	eam							
	ATF	Average [Data Rate	0	0								
	RF Profiles	Burst Dat	a Rate	0	0								
	FlexConnect Groups	Average F	Real-Time R	ate 0	0								
	FlexConnect ACLs	Burst Rea	al-Time Rate	0	0								
	FlexConnect VLAN Templates	Per-SSID	Bandwic	Ith Contracts	(kbps) *								
	Network Lists			DownStre	am UpStr	am							
•	802.11a/n/ac/ax	Average [Data Rate	0	0								
	802.11b/g/n/ax	Burst Dat	a Rate	0									
	Media Stream	Average F	Real-Time R	ate 0									
	Application Visibility	Burst Rea	al-Time Rate	U	0								
	And Control	WLAN Qo	S Param	eters									
	Lync Server	Maximum	Priority	backgrou	ind v								
	Country	Unicast D	efault Prior	ity backgrou	ind v								
	Timers	Multicast	Default Pric	backgrou	ind v								
	Netflow	Wined Oo	C Drotos										
*	QoS Profiles	wired Qo	S Protoco										
	Roles	Protocol I	туре	802.1p									
	Qos Map	802.1p la	ag	[1									

ւվաիս cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP			
Wireless	Edit QoS	Profile									
 Access Points All APs Radios Global Configuration 	QoS Profi Descripti	escription silver									
Advanced											
Mesh	Per-User	Bandwid	th Contracts (kbps) *							
AP Group NTP			DownStrea	am UpStre	am						
> ATF	Average I	Data Rate	0	0							
RF Profiles	Burst Dat	ta Rate	0	0							
FlexConnect Groups	Average I	Real-Time R	ate 0	0							
FlexConnect ACLs	Burst Rea	al-Time Rate	0	0							
FlexConnect VLAN Templates	exConnect VLAN Per-SSID Bandwidth Contracts (kbps) *										
Network Lists			DownStrea	am UpStre	am						
802.11a/n/ac/ax	Average I	Data Rate	0	0							
802.11b/g/n/ax	Burst Dat	ta Rate	0	0							
Media Stream	Average I	Real-Time R	ate 0	0							
Application Visibility	Burst Rea	al-Time Rate	0	0							
And Control	WLAN Qo	S Paramo	eters								
Lync Server	Maximum	n Priority	besteffort	: ~							
Country	Unicast D	Default Priori	ty besteffort	: ~							
Timers	Multicast	Default Prio	rity besteffor	: •							
Netflow)							
▼ QoS	Wired Qo	S Protoco	bl								
Profiles	Protocol 7	Туре	802.1p \	·							
Qos Map	802.1p Ta	ag	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。

uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
Security	Advance	d EAP							
 AAA General RADIUS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP 	Identity R Identity n Dynamic Request 1 Max-Login EAPOL-Ke EAPOL-Ke EAP-Broa	Request Tim equest Max WEP Key Ir Fimeout (in Max Retries n Ignore Id ey Timeout ey Max Retri dcast Key I	neout (in secs) a Retries ndex secs) i entity Response (in milliSeconds) ries interval(in secs)						30 2 0 30 2 enable 3 400 4 3600

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

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

[EAP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)] [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。 Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド [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 bcast-key-interval 3600

Auto-Immune

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

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

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

(Cisco Controller) > show wps summary

Auto-Immune

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

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAG	SEMENT COMMANDS HELP FEEDBACK
Security	Rogue Policies	
 AAA General RADIUS TTACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate 	Rogue Detection Security Level Low Rogue Location Discovery Protocol Disable Expiration Timeout for Rogue AP and Rogue Client entries 1200 Validate rogue clients against AAA Enabled Validate rogue AP against AAA Enabled Polling Interval 0 Validate rogue clients against MSE Enabled Validate rogue clients against MSE Enabled Detect and report Ad-Hoc Networks Ø Enabled Rogue Detection Report Interval (10 to 300 Sec) 10 Rogue Detection Minimum RSSI (-70 to -128) -90 Rogue Detection Transient Interval (0, 120 to 1800 Sec) 0	High Critical O Custom
Access Control Lists Wireless Protection Policies General Desuge Pulses	Rogue Client Threshold (0 to disable, 1 to 256) 0 Rogue containment automatic rate selection □Enabled Auto Contain	
Friendly Rogue Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Auto Containment Level 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	
 Web Auth TrustSec Local Policies Umbrella Advanced 	AdHoc Rogue AP	

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。

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

- [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。

Cisco Cataly	rst 9800-40 Wireless Controller Welcome alpha 🛛 希 🖷 🔅 🖄 🥝 🌫	Search APs and Clients Q
Q Search Menu Items	Configuration - > Radio Configurations - > Network	
Dashboard	5 GHz Band 2.4 GHz Band	
Monitoring >	General	
Configuration >	5 GHz Network Status	
() Administration >	▲ Please disable 5 GHz Network Status to configure Beacon Interval, Fragmentation Threshold, DTPC Support.	
☆ Troubleshooting	Beacon Interval* 100	
	Fragmentation Threshold(bytes)*	
	DTPC Support	
	CCX Location Measurement	
	Mode	
	Data Rates	
	Please disable 5 GHz Network Status to configure Data Rates	
特别特别特别特别特别	6 Disabled v 9 Mbps Mandatory v	
相同相同相同的時間	18 Supported v24 Supported v36 Supported v	
	48 Supported v 54 Supported v Mbps	

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

ネットワークのステータスが [有効 (Enabled)]

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

に設定します。

ロングプリアンブルを必要とするレガシークライアントがワイヤレス LAN に存在しない場合は、アクセスポイントの 2.4 GHz 無線設定で [ショートプリアンブル(Short Preamble)] を [**有効(Enabled)]** に設定します。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。

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。

Cisco Cata	alyst 9800-40 Wireless (Controller	Welcome	e alpha	*	B •	000	Search /	Ws and Clients Q	•
Q Search Menu Items	Configuration * > Radio Cor	figurations *	> Network							
📻 Dashboard	5 GHz Band 2.4 GHz B	Band								
Monitoring >	General									
Configuration >	2.4 GHz Network Status									
\bigcirc Administration \rightarrow \gg Troubleshooting	A Please disable 2.4 GH 802.11g Network Status, B Fragmentation Thre	z Network State eacon Interval, eshold, DTPC S	us to configure Short Preamble, Support.							
-	802.11g Network Status									
	Beacon Interval*	100								
	Short Preamble									
	Fragmentation Threshold(bytes)*	2346								
	DTPC Support	~								
	CCX Location Measure	ement								
	Mode									
이 김 의 의 의 일을	Interval*	60								
	Data Rates									
	A Please disable 2.4 GHz N	etwork Status ates	to configure Data							
	1 Mbps	▼ 2 Mbps	Disabled _v	5.5 Mbps	Disabled	*				
	6 Disabled Mbps	• 9 Mbps	Disabled _v	11 Mbps	Disabled	•				
	12 Mandatory Mbps	✓ 18 Mbps	Supported ,	24 Mbps	Supported	*				
	36 Supported	▼ 48 Mbps	Supported _v	54 Mbps	Supported	¥				

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に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 Cisco Cata	,				
, Search Menu Items	Configuration - > Radio C	configurations - > High Thro	ughput		
Dashboard	5 GHz Band 2.4 GHz	z Band			
Monitoring >					
Configuration					
Administration	✓ 11n				
	Ena	able 11n		Select All	
Troubleshooting	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data R	ate)
	0/(7Mbps)	/(14Mbps)	2/(21Mbps)	3/(29Mbps)	
	4/(43Mbps)	5/(58Mbps)	6/(65Mbps)	J/(72Mbps)	0
	_8/(14Mbps)	9/(29Mbps)	_10/(43Mbps)	11/(58Mbps	s)
	(22/(8/MDps)	77/(43Mbps)	(130Mbps)	10/(144Mb)	2)
	20/(130Mbos)	21/(173Mbos)	22/(195Mbps)	23/(217Mbr	os)
	24/(29Mbps)	25/(58Mbps)	26/(87Mbps)	27/(116Mb	ps)
	28/(173Mbps)	29/(231Mbps)	30/(260Mbps)	31/(289Mbr	ps)
	✓ 11ac				
	✓ 11ac	A The D	ata rates are for 20MHz channels and \$ Interval	Short Guard	
	✓ 11ac Enable 14	▲ The D	ata rates are for 20MHz channels and s Interval	Short Guard Select All	
	11ac Enable SS/MCS SS/MCS	The D ss/Mcs	ata rates are for 20MHz channels and 3 Interval SS/MCS	Short Guard Select All SS/MCS	
	 ✓ 11ac Enable to SS/MCS √/8/(86.7Mbps) 	ic SS/MCS ✓ 1/9/(n/a)	ata rates are for 20MHz channels and 3 Interval SS/MCS 2/8/(173.3Mbps)	Short Guard Select All SS/MCS 2/9/(n/a)	
	 ✓ 11ac Enable SS/MCS √/8/(86.7Mbps) √/8/(260.0Mbps) 	▲ The D inc SS/MCS ✓ 1/9/(n/a) ✓ 3/9/(288.9Mbps)	ata rates are for 20MHz channels and S Interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps)	Short Guard Select All SS/MCS 2/9/(n/a) V 4/9/(n/a)	V
	 ✓ 11ac Enable SS/MCS √/8/(86.7Mbps) √/8/(86.0Mbps) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) √/8/(81.2000) × 11ax	▲ The D ac SS/MCS ✓ 1/9/(r/a) ✓ 3/9/(288.9Mbps)	ata rates are for 20MHz channels and 5 Interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps)	Short Guard Select All SS/MCS 2/9/(n/a) V 4/9/(n/a)	
	 11ac Enable 3 SS/MCS I/8/(86.7Mbps) I/8/(260.0Mbps) 11ax Enable 11a 	▲ The D bc SS/MCS ✓ 1/9/(n/a) ✓ 3/9/(288.9Mbps)	ata rates are for 20MHz channels and 3 Interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps)	Short Guard Select All SS/MCS 2/9/(n/a) V 4/9/(n/a) Select All	
	 11ac Enable 3 SS/MCS SS/8/(86.7Mbps) S/8/(260.0Mbps) 11ax Enable 11a Multiple 3 	Le D SS/MCS V 1/9/(n/a) V 3/9/(288.9Mbps)	ata rates are for 20MHz channels and 5 Interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps)	Short Guard Select All SS/MCS 2/9/(n/a) C 4/9/(n/a) Select All	
	 11ac Enable 1 SS/MCS J/B/(86.7Mbps) J/B/(260.0Mbps) 11ax Enable 11a Multiple 3 SS/MCS 	▲ The D Ac SS/MCS ✓ 1/9/(n/a) ✓ 3/9/(288.9Mbps) ax ✓ ssid SS/MCS	ata rates are for 20MHz channels and 3 Interval SS/MCS 2/8/(173.3Mbps) 4/8/(346.7Mbps) SS/MCS	Short Guard Select All SS/MCS 2/9/(n/a) C 4/9/(n/a) Select All SS/MCS	
	 11ac Enable 3 SS/MCS Ø/8/(86.7Mbps) Ø/8/(260.0Mbps) 11ax Enable 11a Multiple 3 SS/MCS Ø/7 	▲ The D ic SS/MCS ✓ 1/9/(r/a) ✓ 3/9/(288.9Mbps) ax ✓ isid SS/MCS ✓ 1/9	ata rates are for 20MHz channels and 5 Interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps) SS/MCS SS/MCS	Short Guard Select All SS/MCS 2/9/(n/a) C 4/9/(n/a) Select All SS/MCS V 2/7	
	 11ac Enable 11 SS/MCS J/B/(86.7Mbps) J/B/(260.0Mbps) 11ax Enable 11a Multiple 3 SS/MCS J/7 J/9 	▲ The D A The D A The D SS/MCS ✓ 1/9/(n/a) ✓ 3/9/(288.9Mbps) ax ✓ sid SS/MCS ✓ 1/9 ✓ 2/11	ata rates are for 20MHz channels and 3 Interval SS/MCS 2/8/(173.3Mbps) 4/8/(346.7Mbps) SS/MCS SS/MCS x 1/11 x 3/7	Short Guard Select All SS/MCS 2/9/(n/a) C 4/9/(n/a) Select All SS/MCS 2/7 C 2/7 C 3/9	
	 11ac Enable 3 SS/MCS Ø/8/(86.7Mbps) Ø/8/(260.0Mbps) 11ax Enable 11a Multiple 3 SS/MCS Ø/7 Ø/9 3/11 	▲ The D Ac SS/MCS ✓ 1/9/(r/a) ✓ 3/9/(288.9Mbps) ax ✓ ssid SS/MCS ✓ 1/9 ✓ 2/11 ✓ 4/7	ata rates are for 20MHz channels and s interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps) SS/MCS SS/MCS 2/1/11 2/3/7 2/4/9	Short Guard Select All Select All 2/9/(n/a) 3 4/9/(n/a) Select All Ss/MCS 2/7 2/7 2/7 2/3/9 2/11	
	 11ac Enable 11 SS/MCS 1/8/(86.7Mbps) 3/8/(260.0Mbps) 11ax Enable 11a Multiple 3 SS/MCS 1/7 2/9 3/11 3/7 	▲ The D A The D A The D SS/MCS ✓ 1/9/(n/a) ✓ 3/9/(288.9Mbps) ax ✓ ssid SS/MCS ✓ 1/9 ✓ 2/11 ✓ 4/7 ✓ 5/9	ata rates are for 20MHz channels and 3 Interval SS/MCS 2/8/(173.3Mbps) 2/8/(346.7Mbps) SS/MCS SS/MCS SS/MCS (v) 1/11 (v) 3/7 (v) 4/9 (v) 5/11	Short Guard Select All SS:/MCS 2/9/(n/a) (v 4/9/(n/a) Select All SS:/MCS v 2/7 v 3/9 v 4/11 (v 6/7	
	 ✓ 11ac Enable 11 SS/MCS J/8/(260.0Mbps) ④/8/(260.0Mbps) ✓ 11ax Enable 11a Multiple B SS/MCS J/7 J/9 ④/11 ⑤/7 ⑤/9 	▲ The D Action of the formation of the	ata rates are for 20MHz channels and 5 interval SS/MCS 2/8/(173.3Mbps) 4/8/(346.7Mbps) SS/MCS SS/MCS 4/9 5/11 5/11 7/7	Short Guard Select All Select All 2/9/(n/a) 2/9/(n/a) 2/9/(n/a) 2/7 Select All Ss/MCS 2/7 2/7 2/3/9 2/4/11 2/6/7 2/9	

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)]

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

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。

Cisco Cata	yst 9800-40 Wireless Controller Welcome alpha 🖌 🌾 🖺 🏟 🙆 🧭 🎜 Search APs and Cleres C	ξ Φ
Q Search Menu Items	Configuration • > Radio Configurations • > Parameters	
Dashboard	5 GHz Band 2.4 GHz Band	
Monitoring	EDCA Parameters	У
(c) Administration →	EDCA Profile optimized-video-v DFS (802.11h)	
X Troubleshooting	▲ DTPC Support is enabled. Please disable it at Network to configure Power Constraint	
	Power Constraint*	
	Channel Switch	
	Channel Switch Quiet Announcement Mode	
	Smart DFS 📿	

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。

Cisco Cisco C	atalyst 9800-40 Wireless Controller Welcome alpha		C Search APs and Clients Q
Q. Search Meriu Items	Configuration • > Radio Configurations • > RRM		
Dashboard	5 GHz Band 2.4 GHz Band FRA		
	General Coverage DCA TPC RF Grouping		
المركم Configuration	> Power Assignment Method	Power Assignment	RCDN6-21A-WLC5 (10.201.81.9)
O Administration	>	Transmit Power Update	600 second(s)
Y Troubleshooting	 Automatic 	Last Run:	365 second(s) ago
	On Demand Invoke Power Update Once	Power Neighbor Count:	3
) Fixed		
	Max Power Level Assignmen 17		
	Min Power Level Assignmen 11		
	Power Threshold* -70		

$5 \, \mathrm{GHz}$

を使用する場合は、多数のチャンネルをスキャンするために発生するアクセスポイント検出の遅延の可能性を回避 するためにチャンネルの数を制限できます(例:12 チャンネルのみ)。 Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネルの幅を 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ネル幅を使用することを推奨します。

Cisco Catalys	st 9800-40 Wireless Contro	oller Welcome alpha 🖌 🌾 🖺 🔅 🔞 🕢 🌫 Search	th APs and Clients Q
Q Search Menultems	Configuration * > Radio Configuration	ons* > RRM	
Dashboard	5 GHz Band 2.4 GHz Band	FRA	
Monitoring >	General Coverage DCA	A TPC RF Grouping	
Configuration >	Dynamic Channel Assignment	t Algorithm	
 ⊘ Administration → ∑ Troubleshooting 	Channel Assignment Mode	Automatic Freeze Off	
	Interval	10 minutes v	
	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 v 20 MHz 40 MHz 80 MHz 160 MHz Best	
	Auto-RF Channel List		
	✓ ✓ ✓ ✓ ✓ 36 40 44 48 52 56 60 64 100	V V V V V 104 108 112 116 120 124 128 132 136	
	Image: 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。

Search Menu Items	Configuration > Radio Configura	tions * > RRM	
Dashboard	5 GHz Band 2.4 GHz Band	FRA	
Monitoring >	General Coverage DC	CA TPC RF Grouping	
Configuration >	Dynamic Channel Assignme	nt Algorithm	
Administration >			
Troubleshooting	Channel Assignment Mode	 Automatic 	
		Freeze Invoke Channel Update Once	
		⊖ Off	
	Interval	10 minutes 👻	
	Anchortime	0 •	
	Avoid Foreign AP Interference		
	Avoid Cisco AP load		
방송방송	Avoid Non 5 GHz Noise		
	Avoid Persistent Non-wifi Interference		
	Channel Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9)	
	Last Auto Channel Assignment	531 second(s) ago	
	DCA Channel Sensitivity	medium	
	Auto-RF Channel List		
	Event Driven RRM		
	LTOIL DITTOI INN		

使用する周波数帯域に応じて5GHzまたは2.4GHz

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネルの幅を 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ネル幅を使用することを推奨します。

Cisco Cata	alyst 9800-40 Wirel	ess Controller	Welcome alpha	684802	Search APs and Clients Q
Q Search Menu Items	Configuration - > W	Edit Radios 5 GHz Ban	d		×
Dashboard	 All Access Person All Access Person	Configure Detail General		RF Channel Assignment	nt
Configuration	AP v AP Name Model	AP Name Admin Status	rcdn6-22a-ap1	Current Channel Channel width	149 40 MHz 💌
() Administration →	rcdn6-22a- ap1	CleanAir Admin Status		Assignment Method	Global
X Troubleshooting	∺	Antenna Parameters		Tx Power Level Assign	ment
		Antenna Type	Internal 🔻	Current Tx Power Level	2
	S GHz Radios	Antenna Mode	Omni	Assignment Method	Global
	Number of AP(s): 1	Antenna A			
	AP V Slot Name No	Antenna B			
	rcdn6-22a- 1 <	Antenna C			
	H 4 1 H	Antenna D			
	> 2.4 GHz Radi	Antenna Gain	10		
	> Dual-Band R	Download Core Dump to b	pootflash		
	> Country				
	LSC Provisio				
		Cancel			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。



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 Cisco Cat	alyst 9800-40 Wireless Controlle	er Welcome	alpha 🛛 🖨 🐔 🖺 🗘	0 0 C Search APs	end Clerch Q
16.12.26	Configuration * > Tags & Profiles * >	Edit WLAN			×
		General Security Advance	d		
Dashboard	- Add - Delete Enable WLAN	Layer2 Layer3 AAA			
Monitoring >	Number of WLANs selected : 0	Laura 2 Consults Mada	MDA + MDA2		
	Status- Name - ID	Layer 2 Security Woole		Fast Transition	Enabled
Administration	Voice 1	MAC Filtering		Over the DS	
Y Troubleshooting	H + 1 + H 10 + items p	Protected Management Frame		Reassociation Timeout	20
		PMF	Disabled v		
		WPA Parameters			
		WPA Policy			
		WPA2 Policy			
		WPA2 Encryption	CCMP256		
			GCMP128 GCMP256		
		MPSK			
		Auth Key Mgmt	802.1x		
			PSK		
			FT + 802.1x		
			802.1x-SHA256		
			PSK-SHA256		
		D Cancel			Lindate & Apply to Davide
168년 전 전 1989년 - 1989년 1989년 - 1999년 - 1999년 - 1989년 - 1989년 1989년 - 1989년					
Cisco Cata	alyst 9800-40 Wireless Controlle	er Welcome Edit WLAN	alpha 🗌 🏶 🖺 🔅	Search APa	and Clients Q
	Configuration / Taga & Fromea /	General Security Advance	d		
Dashboard	+ Add + Delete Enable WLA	Layer2 Layer3 AAA			
Monitoring >	Number of WLANs selected : 0				1
	Status Name v ID	Layer 2 Security Mode	WPA + WPA2 🔻	Fast Transition	Enabled •
Administration	Voice 1	MAC Filtering		Over the DS	
M Traublachasting	Deta 2	Protected Management Frame		Reassociation Timeout	20
Troubleshooting		PMF	Disabled +		
		WPA Parameters			
		WPA Policy			
		WPA2 Policy			
		WPA2 Encryption	AES(CCMP128)		
			GCMP128 GCMP256		
		MPSK			
		Auth Key Mgmt	802.1x		
			PSK		
			FT + 802.1x		
			FT + PSK		
			PSK-SHA256		
		PSK Format	ASCII		
		DSK Tuno	Linencomted -		
		"D Cancel		E	Update & Apply to Device

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

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

A Stand Meria Inner Dashboard Monitoring Monitoring Configuration Administration Troubleshooting	Configuration - > Tags & Profil Add Common Tags & Profil Number of WLANs selected : 0 Status Name Voice O Data H = 1 b H 10 +	Edit WLAN General Security Layer2 Layer3 Authentication List Local EAP Authentication	Advanced Advanced authentication_dot1k •	×
Deshboard Monitoring Monitoring Administration Troubleshooting	Add Deers Lod Number of WLANs selected : 0 Status Name v Visce Deta H = 1 & H 20 v	General Security Layer2 Layer3 Authentication List Local EAP Authentication	Advanced Advanced authentication_dot1x •	
Monitoring Monitoring Configuration Administration Markan Troubleshooting	Number of WLANs selected : 0 Status Name Visce O Usice O Data In a 1 5 4 10 •	Authentication List Local EAP Authentication	authentication_dot1k •	
Configuration Configuration C	Status Name Visce O Visce O Data In n 1 h ni 10 y	10 Authentication List 2 Local EAP Authentication	authentication_dot1k •	
 Administration Troubleshooting 	O Usice O Data In 1 x 1 10 y	Local EAP Authentication		
* Traubleshooting	и « 1 » и 10 •	anna a		
Troubleshouling		3-10110		

[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

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

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 [帯城選択(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。

Search Manu terris	Configuration	 Tags 8 	Profiles* > WL	ANs	Edit WLAN				
					General Security	Advanced			
Dashboard					Coverage Hole Detection		Universal Admin		
) Monitoring	Number of WLA	Ns selected :	0		Aironet IE		Load Balance		
Configuration >	Status ~	Name	~ ID	~ SSID	P2P Blocking Action	Disabled +	Band Select		
	• •	Voice	1	voice	Multicast Buffer	DISABLED	IP Source Guard		
Toublachesta	0	Data	2	data	Media Stream Multicast-		WMM Policy	Required +	
Troubleshooting	2.2.9		10 + Herris per pa	90			mDNS Mode	Bridging +	
					Max Client Connections		Off Channel Scar	ining Defer	
					Per WLAN 0				
					Per AP Per 0		Defer Priority	0 1 2	
Tel distant in the					WLAN			3 🖌 4 🟹 5	
					Per WLAN			6 7	
					11v BSS Transition Sup	port	Scan Defer	100	
							Time -		
					BSS Transition		Assisted Roamin	ə (11k)	
					Disassociation Imminent(0 to 3000 TBTT)	200	Prediction		
					Optimized Roaming Disassociation Timer(0 to	40	Optimization		
					40 TBTT)		Neighbor List		
					BSS Max Idle Service		Dual Band Neighbor List		
					BSS Max Idle Protected		DTIM Period (in b	eacon intervals)	
					Directed Multicast Service	×			
					11ax		5 GHz Band (1-255	2	
					Downlink OFDMA	2	2.4 GHz Band (1-25	.5) 2	
					Liste orpita				

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。

Cisco Cata	alyst 9800-40 Wire	eless Controller We	elcome <i>alpha</i> 🔺 🕏 🖺	Search Af	es and Clients Q
Q Search Menu Items	Configuration - > T	Edit Policy Profile General Access Policies	OOS and AVC Mobili	ty Advanced	3
Dashboard	+ Add × Dele	A Configure	ng in anabled state will result in loss	of connectivity for clients associated wi	th this profile
Monitoring >	Status v Pol	Conngun	ng in enabled state will result in loss	or connectivity for clients associated wi	
Configuration >	Dat	Name*	Voice	WLAN Switching Policy	
) Administration >	 Ø Ø def: 	Description	Enter Description	Central Switching	
Troubleshooting	H H 1 > H	Status	ENABLED	Central Authentication	
		Passive Client	DISABLED	Central DHCP	
		Encrypted Traffic Analytics	DISABLED	Central Association	
		CTS Policy		Flex NAT/PAT	DISABLED
		Inline Tagging			
		SGACL Enforcement	2.65510		
		Default SG1	2*03313		
		"O Cancel			

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。

Cisco Cisco Catalys	st 9800-40 Wire	less Controller Welcor	me alpha 🛛 🛠 🥵 🖺 🕻	0 10 1	Search	APs and Clients Q	•
Q Search Menu Items	Configuration - > Edi	it Policy Profile					×
		General Access Policies	QOS and AVC Mobility	Advanced			
Dashboard	+ Add × D	RADIUS Profiling			WLAN ACL		
Monitoring >	Status v F	Local Subscriber Policy Name	Search or Select 🔹		IPv4 ACL	Search or Select	T
🔧 Configuration >		WLAN Local Profiling			IPv6 ACL	Search or Select	•
() Administration →	0 0	Global State of Device Classification	Disabled (i)		URL Filters		
% Troubleshooting	∺ ∢ 1 ⊨	HTTP TLV Caching			Pre Auth	Search or Select	•
		DHCP TLV Caching			Post Auth	Search or Select	•
		VLAN					
		VLAN/VLAN Group	VLAN0500				
		Multicast VLAN	Enter Multicast VLAN				
) Cancel				📄 Update & Apply	to Device

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。

O Search Manu Items	Configuration - >	Edit Policy Profile				×
		General Acc	cess Policies QOS and AV	C Mobility	Advanced	
Dashboard	+ Add 🗼 🖂 D	Auto QoS	None 🔻		Flow Monite	or IPv4
Monitoring >	Status v F	QoS SSID Policy	r		Egress	Search or Select
Configuration >		Egress	platinum x v		Ingress	Search or Select
() Administration >	0 0	Ingress	platinum-up x v		Flow Monite	or IPv6
X Troubleshooting	H H H	QoS Client Polic	у		Egress	Search or Select
		Egress	Search or Select 👻		Ingress	Search or Select
		Ingress	Search or Select			
		SIP-CAC				
		Call Snooping				
		Send Disassociate				
		Send 486 Busy				
		Cancel				Update & Apply to Device

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。

2 Search Menu Items	Configuration - >	Edit Policy Profile					
		General Access Policies	QOS and AVC	Mobility	Advanced		
Dashboard		WLAN Timeout			Fabric Profile	Search or Select 🗸	
) Monitoring >	Status v I	Session Timeout (sec)	86400		Umbrella Barameter Man	Not Configured]
Configuration >		Idle Timeout (sec)	300		mDNS Service	default-mdns-service 👻	1
Administration >		Idle Threshold (bytes)	0		Policy	Clea	ar
ू Troubleshooting	H H 1 H	Client Exclusion Timeout (sec)	60		WLAN Flex Policy		
		DHCP			VLAN Central Switching	ng	
		IPv4 DHCP Required			Split MAC ACL	Search or Select 🔹]
		DHCP Server IP Address			Air Time Fairness	Policies	
		Show more >>>			2.4 GHz Policy	Search or Select]
		AAA Policy			5 GHz Policy	Search or Select 🔹]
		Allow AAA Override					
		NAC State					
		Policy Name	default-aaa-policy x	•			
		Accounting List	Search or Select	•			
						10	

RFプロファイル

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

Cisco 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。

¢	cisco	Cisco Cat	alyst 9800-40	Wireless Controller	Welcome alpha	6 B \$ 8 0 C	Search APs and Clients Q
٩	, Search Menu Iter	ns	Configuration -	> Tags & Profiles - > RF			
	Dashboard		+ Add				
	Monitoring		State v	RF Profile Name v	Band v	Description	~
R	Configuratio	on →	•	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf	
			0	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r	
£03	Administrati	ion >	Add RF Profile	Ő.		×	·
X	Troubleshoo	oting	General	802.11 RRM Advanced			
			Name*	Enter Name			
			Radio Band	5 GHz Band			
							1 - 6 of 6 items
			Status	DISABLE			
			Description	Enter Description			
							-
			"O Cancel			Apply to Device	
			3				

[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。

Cisco Cata	alyst 9800-4	0 Wireless Controller	Welcome alpha	* * 8	0 0 C Sean	on APs and Clents Q	🗭
Q. Search Menu Items	Configuration	- > Tags & Profiles - > RI	ŧ.				
📷 Dashboard	+ Add						
Monitoring >	State ~	RF Profile Name	< Band	 Description 			~
	0	Low_Client_Density_rf_5gh	5 GHz	pre configure	d Low Client Density rf		
Configuration	0	High_Client_Density_rf_5gh	5 GHz	pre configure	d High Client Density r		
() Administration >	Add RF Profil	e			×		
% Troubleshooting	General	802.11 RRM Adva	inced				
	Operationa	Rates	802.11n	MCS Rates			
	6 Mbps	Disabled •	Enabled Da	ta Rates:			
김 부모 그 가격했다.	9 Mbps	Disabled 🔹	[0,1,2,3,4,5,6	7,8,9,10,11,12,13,14,15,16,	17,18		
	12 Mbps	Mandatory 👻	,19,20,21,22,	23,24,25,20,27,28,29,30,31			
	18 Mbps	Supported 👻	Enable	MCS Index v			
	24 Mbps	Supported 🗸		0			
	36 Mbps	Supported +		1			
신 방문 감사 있는	48 Mbps	Supported v		2			
	54 Mbps	Supported v		3			
이 아직 관감 이성형	23			4			
				5			
				6			
وموالكم تقلدها				7			
				8			
				9			

[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 Ca	talyst 9800-40 Wireless Controller	Welcome alpha	🕫 🖺 🏟 👰 🤪 Search Allis and Clarins Q
Q. Search Menu Items	Configuration • > Tags & Profiles • > RF		
Dashboard	+ Add Sciente		
Monitoring >	State ~ RF Profile Name	~ Band	 Description
	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r
\bigcirc Administration \rightarrow	Add RF Profile		×
₩ Troubleshooting	General 802.11 RRM Advanced General Coverage TPC DCA		
	Coverage Hole Detection		1 - 6 of 6 items
유하면 요. 전세	Minimum Client Level (clients)*	3	1
	Data RSSI Threshold (dBm)*	-80	
	Voice RSSI Threshold (dBm)*	-80	
	Exception Level(%)*	25	
	Cancel		Apply to Device

Cisco Cisco	Catalyst 9800-40 Wireless Controller Welcome alpha 🖌 🌾 🖺 🏟 🖗 🖉 📿 Search APa and Clarits Q	
Q Search Menu Items	Configuration -> Tags & Profiles -> RF	
🔚 Dashboard	Add Concernent Concern	
Monitoring	State v RF Profile Name v Band v Description	~
	Low_Client_Density_rf_Sgh 5 GHz pre configured Low Client Density rf	
	High_Client_Density_rf_Sgh 5 GHz pre configured High Client Density r	
	Add RF Profile *	
💥 Troubleshooting	General 802.11 RRM Advanced	
	General Coverage TPC DCA	
	Transmit Power	
	Maximum Power Level(dBm)* 30	
	Minimum Power Level(dBm)* -10	
	Power Threshold V1(dBm)* -70	
	Cancel Cancel	

Cisco Cat	alyst 9800-40 Wireless Control	ller Welcome alpha	***	Is APs and Clents Q
Q. Search Mehu Items	Configuration • > Tags & Profiles • :	> RF		
Dashboard	+ Add X Delete			
Monitoring >	State v RF Profile Name	~ Band	 Description 	
Configuration	Low_Client_Density_rf_5	igh 5 GHz	pre configured Low Client Density rf	
- Conniguration	High_Client_Density_rf_5	igh 5 GHz	pre configured High Client Density r	
(j) Administration →	Add RF Profile		×	
💥 Troubleshooting	General 802.11 RRM	Advanced		
이 관광성을 망	General Coverage TPC	DCA		
없는 방법 등 가장	Dynamic Channel Assignment			
	Avoid AP Foreign AP Interference			
	Channel Width	20 MHz 40 MHz 8 Best	30 MHz 160 MHz	
	DCA Channels	Image: Constraint of the state of the s	 ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ 100 104 108 112 116 120 124 ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ 	
	High Speed Roam			
	Mode Enable			
	Neighbor Timeout*	5		
	Client Network Preference	Default 🔹		
	ී Cancel		Apply to Device	

[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。

Cisco	Catalyst 9800-40 Wireless Contro	oller Welcome alpha 🖌 🌴 阳 🕅 👰 🥥 📿 Gesch Afte stre	Ctenta Q
Q. Search Menu Items	Configuration - > Tags & Profiles -	> RF	
Dashboard	+ Add		
Monitoring	State V RF Profile Name	 Band Description 	~
	> Low_Client_Density_rf_	.5gh 5 GHz pre configured Low Client Density rf	
A	High_Client_Density_rf_	_5gh 5 GHz pre configured High Client Density r	
205 Administration	Add RF Profile	×	
💥 Troubleshooting	General 802.11 RRM	Advanced	
	High Density Parameters		
	Max Cliente*	200	
	Max Cilents		
	Multicast Data Rate (Mbps)	Auto 👻	
	Rx Sop Threshold (dbm)	auto	
	Client Distribution		
	Load Balancing Window*	5	
	Load Balancing Denial Count*	3	
	ATF Configuration		
	Status	DISABLED	
김 씨의 비행 성지.	Bridge Client Access	DISABLED	
	Airtime Allocation	5	
	FRA		
	Client Aware		

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。

C dia	Cisco Catalyst 98	00-40 Wireless Controll	er Welcome alpha	0 0 0 0 0	Search APIs and Clients	Q 🖗
Q Search M	Aenu Items	uration • > Tags & Profiles • >	Flex			
📰 Dashb	board + A	dd Delete				
🕜 Moni	Add Flex Profile					×
🖏 Conf	General Local Aut	thentication Policy ACL	VLAN			•
ঠি Admi	Name*	Enter Name	Fallback Radio Shut			Ji i territa
💥 Troul	Description	Enter Description	Flex Resilient			
	Native VLAN ID	1	ARP Caching			
	HTTP Proxy Port	0	Efficient Image Upgrade			
	HTTP-Proxy IP Address	0.0.0.0	Office Extend AP			
	CTS Policy		Join Minimum Latency			
	Inline Tagging					
	SGACL Enforcement					
	CTS Profile Name	default-sxp-profile x				
	Cancel				Apply to Devic	:e

タグ

<u>ポリシー タグ</u>

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

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。
Cisco Cata	alyst 9800-40 Wireless Cor	Itroller Welcome alpha		Search APs and Clients Q
Q Search Menu Items	Policy Site RF A	Changes may result in	loss of connectivity for some clients that are asso	ciated to APs with this Policy Tag.
Monitoring A	+ Add. × Delete	Name* defau Description defau	It-policy-tag It policy-tag	
 Administration Troubleshooting 	default-policy-tag	WLAN-POLICY Maps Add	s: 2	
		WLAN Profile Data	 ✓ Policy Profile Data 	~
		Voice	Voice	1 - 2 of 2 items
		WLAN Profile* Voice	Policy Profile*	Voice v
		RLAN-POLICY Maps	: 0	
	-	Cancel		Update & Apply to Device

<u>サイトタグ</u>

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。

Cisco Catalyst	9800-40 Wireless Controller Well	come alpha 🛛 🏘 🎨 🗎 🏟 🚳 🛛 🎜 🛛 Sealch (Pos	
Q. Search Menu tierns	nfiguration - > Tags & Profiles - > Tags		
🔜 Dashboard	Policy Site RF AP		
Monitoring	+ Add Colors		
💫 Configuration 💦 🔸	Site Tag Name	 Description 	v
Administration	default-site-tag	default site tag	
Name* Description AP Join Profile Flex Profile Control Plane Name Enable Local Site	Enter Name Enter Description default-ap-profile default-flex-profile	Apply to De	• - 1 of 1 itoms

<u>RF タグ</u>

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

Cisco Cata	lyst 9800-40 Wireless Contro	oller Welcome alpha	50004 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	earch APs and Chents Q
Q Search Menu Items	Configuration • > Tags & Profiles •	> Tags		
📷 Dashboard	Policy Site RF AP			
	+ Add > Dolete			
\ll Configuration \rightarrow	RF Tag Name		< Description	×
(☉) Administration →	default-rf-tag		default RF tag	
% Troubleshooting	Add RF Tag	teme nar nana.	×	
	Name*	Enter Name		
	Description	Enter Description		
	5 GHz Band RF Profile	Global Config 🗸		
	2.4 GHz Band RF Profile	Global Config 🔹		
	S Cancel		Apply to Device	

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。 Cisco RoomOS DX Series ワイヤレス LAN 導入ガイド タグを定義したら、アクセスポイントに適用できます。

Search Menu Items	ingu auon · /				
		General Interfaces	High Availability In	iventory ICap Advanced	
Dashboard	All Access	General		Version	
) Monitoring >	nber of AP(s): I	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
Configuration >	AP v AP Name Mo	Location*	rcdn6-22	Predownloaded Status	N/A
} Administration >	rcdn6-22a- Al'	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
² Troubleshooting	H 4 1 ->	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status		Boot Version	1.1.2.4
· · · · · · · · · · · · · · · · · · ·	5 GHz Rac	AP Mode	Local	IOS Version	16.12.2.132
		Operation Status	Registered	Mini IOS Version	0.0.0.0
	2.4 GHz R	Fabric Status	Disabled	IP Config	
>	Dual-Banc	LED State		CAPWAP Preferred Mode IP	v4
	Country	LED Brightness Level	8 🗸	DHCP IPv4 Address 10	0.201.81.125
· · · · · · · · · · · · · · · · · · ·	Country	CleanAir NSI Key		Static IP (IPv4/IPv6)	
>	LSC Provis	Tags		Time Statistics	
		Policy	default-policy-tag	Up Time	10 days 18 hrs 16 mins 54
		Site	default-site-tag 🔻	Controller Association Latency	2 mins 4 secs
		RF	default-rf-tag	Sectored resources reletivy	a mina 4 0000

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。

2 Search Menu Items	Configuration • >	Edit AP			
Dashboard		General Interfaces	High Availability Inv	ventory ICap Advanced	
	 All Acces Number of AP(s): 1 	General		Version	
) Monitoring >	namber er ru (e).	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
Configuration >	AP v A Name M	Location*	rcdn6-22	Predownloaded Status	N/A
Administration >	rcdn6-22a- Al	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
C Troubleshooting	api B	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status		Boot Version	1.1.2.4
	> 5 GHz Ra	AP Mode	Flex v	IOS Version	16.12.2.132
		Operation Status	Registered	Mini IOS Version	0.0.0.0
	> 2.4 GHz I	Fabric Status	Disabled	IP Config	
	> Dual-Ban	LED State		CAPWAP Preferred Mode IP	/4
	Country	LED Brightness Level	8 🔻	DHCP IPv4 Address 10	.201.81.125
	Country	CleanAir NSI Key		Static IP (IPv4/IPv6)	
	LSC Prov	Tags		Time Statistics	
		Policy	default-policy-tag	Up Time	0 days 0 hrs 10 mins 1 secs
		Site	Flex v	Controller Association Latency	10 secs
		RF	default-rf-tag 🗸		

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。

Cisco Ca	atalyst 9800-40	Wireless Controller	Welcome alpha	6 8 4 6 0	Search APs and C	ients Q
Q Search Menu Items	Configuration -	Wireless - > Wireless	Global			
📷 Dashboard	Default Mobility	CTG-VoWLAN3		Assisted Roaming		
Monitoring >	Domain *			Denial Maximum*	5	
Configuration >	RF Group Name*	RCDN6-VoWLAN3		Floor Bias(dBm)*	15	
() Administration	Maximum Login Sessions Per User*	0		Prediction Minimum*	3	
💥 Troubleshooting	Management Via Wireless					
	Device Classification					
	AP LAG Mode					

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。

	Configuration * > Wireless * > Mobili						
Dashboard	Global Configuration Peer Config	uration					
) Monitoring >	Mobility Group Name*	CTG-VoWLAN3					Apply
Configuration >	Multicast IPv4 Address	0.0.0					
	Multicast IPv6 Address	:					
	Keep Alive Interval (sec)*	10					
Troubleshooting	Mobility Keep Alive Count*	3					
	Mobility DSCP Value*	48	7				
cisco Catal	Mobility MAC Address* yst 9800-40 Wireless Controller	706d.153d.b50b Welcome alpha	** **) ¢ (4 6	Smarch	APs and Clients C	2
-tiuti- cisco Cisco Catal 16 12 2a Search Menu Items	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration - > Wireless - > Mobility	706d.153d.b50b Welcome alpha	1 1 1) \$ (9) 6	Search	APs and Clients	X
··liuli: Cisco Catal cisco: 16 12.25 Search Menu Items Dashboard	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration - > Wireless - > Mobility Global Configuration Peer Configurati	706d.153d.b50b Welcome alpha	3 7 %) ¢ (9 6	Search	APs and Clients C	2
Cisco Catal 16.1229 Search Menu Items Dashboard Monitoring >	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration > Wireless > Mobility Global Configuration Peer Configuratio Mobility Peer Configuration	706d.153d.b50b Welcome alpha	A 7) 🌣 🖄 G	C Search	APs and Clients C	2
Italia Cisco Catal 16:12.2s 16:12.2s Search Menu Items Items Dashboard Items Monitoring > Configuration >	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration - > Wireless - > Mobility Global Configuration Peer Configuration Wobility Peer Configuration Hobility Deleto	706d.153d.b50b Welcome alpha	A 70 E) ¢ (9) 6	Search	APs and Clients C	
•IIIIII Cisco Catal I6 12.25 Search Menu Items Dashboard Monitoring Monitoring > Configuration > Administration >	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration > Wireless > Mobility Global Configuration Mobility Peer Configuration Add Deleto MAC Address > IP Address	Velcome alpha	Group Name V) 🌣 🖄 G	 Search Status 	APs and Clients C	<u>\</u>
•IIIIII Cisco Catal I61225 Search Mercu Items Dashboard Monitoring Monitoring > Configuration > Administration >	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration - > Wireless - > Mobility Global Configuration Peer Configuration Wobility Peer Configuration + Add Deleto MAC Address - IP Address 706d.153d.b50b 10.201.81.9	Velcome alpha	Group Name ~ CTG-VoWLAN3	Multicast IPv4 0.0.0	 Senter Status N/A 	APs and Clients C	\
•IIntll: Cisco Catal 16.122s Search Mercu Items Dashboard Monitoring Monitoring > Configuration > Administration > Troubleshooting >	Mobility MAC Address* yst 9800-40 Wireless Controller Configuration - > Wireless - > Mobility Global Configuration Peer Configuration Mobility Peer Configuration Add Delete MAC Address - IP Address 706d.153d.b50b 10.201.81.9 6c31.0e7b.b8eb 10.201.81.10	Velcome alpha v Public IP N/A 10.201.81.10	Group Name ~ CTG-VoWLAN3 2TG-VoWLAN3	Multicast IPv4 0.0.0 0.0.0	 Search Status N/A Up 	APs and Clients C PMTU N/A 1385	<u>۲</u>

[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。

Cisco Cisco Ca	talyst 9800-40 Wireless Controller Welcome al	alpha 🖌 🏶 🖏 🏟 🚱 🧭 Search Al ¹ s and Clerits Q
Q Search Menu Items	Configuration • > Interface • > Wireless	
Dashboard	+ Add × Delata	
Monitoring >	Interface Name v Interface Type v Trustpoint Name	me v VLAN ID v IP Address v IP Netmask v MAC Address v
Configuration	Vian310 Management	310 10.201.81.9 255.255.250 70:6d:15:3d:b5:0b 1 - 1 of 1 items
() Administration →		
💥 Troubleshooting		

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

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

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

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

SRTP

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

[非アクティブタイムアウト (Inactivity Timeout)] が [無効 (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。

Cisco Catalys	st 9800-40 Wireless Co	ontroller w	elcome alpha		Search APs and Clien	• Q 🕩
Q Search Menu Items	Configuration - > Radio Config	gurations - > Me	dia Parameters			
🚃 Dashboard	5 GHz Band 2.4 GHz Ban	nd				
Monitoring >						
Configuration >	Media			Voice		
() Administration >	General			Call Admission Control (C	CAC)	
💥 Troubleshooting	Unicast Video Redirect			Admission Control (ACM)		
	Multicast Direct Admission	Control		Load Based CAC		
	Media Stream Admission			Max RF Bandwidth (%)*	75	
	Maximum Media Stream RF	5]	Reserved Roaming Bandwidth (%)*	6	
	bandwidth (%)*		1	Expedited Bandwidth		
	Maximum Media Bandwidth (%)*	85		SIP CAC and Bandwidth		
	Client Minimum Phy Rate (kbps)	6000	•	SIP CAC Support		
	Maximum Retry Percent (%)*	80]	Traffic Stream Metrics		
	Media Stream - Multicast I Parameters	Direct		Metrics Collection		
		-		Stream Size*	84000	
	Multicast Direct Enable			Max Streams*	2	
	Max streams per Radio	No Limit	•	Inactivity Timeout		
	Max streams per Client	No Limit	•			
	Best Effort QOS Admission					

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。

Dashboard	Global Wireless	ENABLED				Apply
) Monitoring >	Multicast Mode		IGMP Snooping			
Configuration >	Wireless mDNS Bridging	DISABLED	Disabled	Enabled	Q Se	arch
Administration >	Wireless Non- IP Multicast	DISABLED	Status VLAN ID Name	Status	VLAN ID	Name
Troubleshooting	Wireless Broadcast	DISABLED		O	1	default 🗲
	AP Capwap	Unicast 🔹		Q	310	VLAN0310 🗲
	Multicast			O	400	VLAN0400 🗲
	MLD Snooping	DISABLED	No Vlan available	Q	500	VLAN0500 🗲
	IGMP Snooping Querier	DISABLED				
	IGMP Snooping	ENABLED				
	Last Member Querier Interval (milliseconds)	1000				Disable All

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。

Cisco Ca	talyst 9800-40 Wireless Controller Welcome alpha 🖌 🍖 🖺 🏟 🕲 🧭 Search APs and Clients Q	•
Q Search Menu Items	Configuration - > Wireless - > Media Stream	
📰 Dashboard	General Streams	
Monitoring >	Multicast Direct Enable 🔽	pply
Configuration >	Session Message Config	
(○) Administration →	Session Announcement	
💥 Troubleshooting	Session Announcement URL	
	Session Announcement Email	
	Session Announcement Phone	
	Session Announcement Note	

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。

Cisco Cisco	o Cataly	/st 9800-40 ^v	Wireless Controller Welcome	alpha 🛛 🏠 🌾	A 🖹 🌣	1 0 C Sear	ch APs and Clients Q	Feedback
Q. Search Menu Items		Configuration - >	Wireless • > Media Stream					
Dashboard		General Stre	ams					
	>	+ Add	Add Media Stream	_	_	×	▼ Status	Ŧ
Configuration	>	ii ii 0	General					No items to display
O Administration	>		Stream Name*					
C Licensing			Multicast Destination Start IPv4/IPv6 Address*			_		
X Troubleshooting			Multicast Destination End IPv4/IPv6 Address*					
			Maximum Expected Bandwidth (Kbps)*	1000		_		
Walk Me Through >			Resource Reservation Control (RRC) F	Parameters		_		
			Average Packet Size*	1200		_		
			Policy	admit	•	_		
			Priority	4	•	_		
			QOS	Video		_		
			Violation	Drop	•	_		
			D Cancel		Ē	Apply to Device		

保存すると、メディアストリームが表示されます。

Cisco	Cisco Cata	lyst 9800-40	Wireless Control	er	Welcome alpha	*	\$ 0	▲	8 1	¢ (9	0	C		Q	Feedback	e ^p	•
Q. Search Menu Ite	ims	Configuration -	> Wireless - > Med	ia Stream													
📻 Dashboard		General S	reams														
	>	Add	De N	_	0			_								_	
	, ×		10.195.19.27	Ţ	239.1.1.1			1	239.	1.1.1	855		Enabl	s ed		T	
() Administratio	n >	H 4 1	⊨ ⊨ 10 ▼												1 - 1 of 1	items	
© Licensing																	
X Troubleshoot	ing																

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。

Cisco Cata Cisco Cata Casco Cata Co Search Manu Herrs	alyst 9800-40 W	ireless Controller Welcome alpha 🛛 🏾 🕷 😨	Search APs and Clients Q
 Dashboard Monitoring > Configuration > Administration > Troubleshooting 	+ Add × I Number of WLANs s Status Name Voic Data H < 1 >	General Security Advanced Coverage Hole Detection Image: Coverage Hole Detection Image: Coverage Hole Detection Aironet IE Image: Coverage Hole Detection Image: Coverage Hole Detection P2P Blocking Action Image: Disabled Image: Coverage Hole Detection Multicast Buffer Image: Disabled Image: Coverage Hole Detection Media Stream Multicast- Image: Coverage Hole Detection Image: Coverage Hole Detection	Universal Admin Load Balance Band Select IP Source Guard WMM Policy Required mDNS Mode Bridging
		Max Client Connections Per WLAN O Par AP Per WLAN Per AP Radio Per WLAN 11v BSS Transition Support	Off Channel Scanning Defer Defer Priority 0 1 2 3 4 5 6 7 Scan Defer Time 100
		BSS Transition Disassociation Imminent(0 200 to 3000 TBTT) Optimized Roaming Disassociation Timer(0 to 40 TBTT) Cancel	Assisted Roaming (11k) Prediction Optimization Neighbor List

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。

Cisco Cata	alyst 9800-40 Wireless Controlle	r Welcome a	lpha 🖌 🏠 🕈	• 🖻 🔊		Q	۲
Q Search Menu Items	Configuration • > Security • > Advan	ced EAP					
📰 Dashboard	EAP-Identity-Request Timeout (sec)*	30					
Monitoring >	EAP-Identity-Request Max Retries*	2					
Configuration >	EAP Max-Login ignore identity Response	DISABLED					
(○) Administration →	EAP-Request Timeout (sec)*	30					
X Troubleshooting	EAPOL-Key Timeout (ms)*	400					
	EAPOL-Key Max Retries*	4					
	EAP-Broadcast Key Interval (sec)*	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 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。

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

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。

Cisco Cat	alyst 9800-40 Wireless Controller	Welcome alpha 🛛 👫 🌾		arch APs and Clients Q
Q Search Menu Items	Configuration - > Wireless - > Advanced	1		
Dashboard	Load Balancing Band Select Opti	mized Roaming High Density	Preferred Calls	
Monitoring >				
🔧 Configuration 🛛 >	Rx Sop Threshold			
() Administration >	Rx Sop Threshold 5 GHz (dbm)	auto 🗸		
💥 Troubleshooting	Rx Sop Threshold 2.4 GHz (dbm)	auto		
	Multicast Data Rate			
	Multicast Data Rate 5 GHz (Mbps)	Auto		
	Multicast Data Rate 2.4 GHz (Mbps)	Auto		

不正ポリシー

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

Cisco Catal	yst 9800-40 Wireless Cont	roller	Welcome alpha	* • •	 Search APs and Clients Q
Q Search Menu Items	Configuration - > Security - > W	/ireless Prote	ection Policies		
📰 Dashboard	Rogue Policies RLDP R	ogue AP Rules	Client Exclusio	n Policies	
Monitoring >	Rogue Location Discovery Protocol	Disable	•		
Representation Configuration	Retry Count	1			
() Administration >	Schedule RLDP				
X Troubleshooting	Day Start	Time	End Time		
	Monday	G	©		
	Tuesday	C	C		
	Wednesday	G	٢		
	Thursday	©	C		
	Friday	•	٢		
	Saturday	9	C		
	Sunday	0	O		

```
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
١
vrf definition Mgmt-intf
1
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
no logging console
aaa new-model
١
١
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 -60
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
١
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 denv multilink
bundle-name authenticated
crypto pki trustpoint TP-self-signed-3110682001
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3110682001
revocation-check none
rsakeypair TP-self-signed-3110682001
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki certificate chain TP-self-signed-3110682001
certificate self-signed 01
 30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33313130 36383230 3031301E 170D3139 30373130 30343236
 35375A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31313036
 38323030 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
 0A028201 0100B74F D6A0DE5D DFB2CDD2 5196AAB1 86C8BD48 3AAAF455 C4E7D559
 41A10FE1 87EC742C C5014113 9A0FD83A F490EA64 DF68A513 AA6900C4 810A9FED
 870309EA 781EB999 882F7374 EC79D592 DEC6C126 A5FB5666 905C24D8 B2064CD4
 66823D6E 7E9A07F3 B043D632 EEDF4CAF D306C303 843493AA F44126E3 A07DE905
 6B6C5B8E C8E6C9E6 45D79F62 B813FF8C B44FA7AC AEDB8A9E 55B75096 E4E76BC3
 D5B90900 1A0C7CD0 910B6C63 920E9666 39EC3702 387757F1 C26F0BB5 89D4733D FED71CF4
 33002C77 0F721B21 5578C850 590BC846 7CB79469 A51CEBA5 96EA8672 DDB82A44 69EEDA13
 DD83B0FA 3221A839 5F985C86 F2C57B78 8E6608B6 18A346D2 035D3B68 26BF0203 010001A3
 53305130 0F060355 1D130101 FF040530 030101FF
 301F0603 551D2304 18301680 141B4651 019E0AEC 8E64EB65 C0E023ED 60F6062C
 0F301D06 03551D0E 04160414 1B465101 9E0AEC8E 64EB65C0 E023ED60 F6062C0F
 300D0609 2A864886 F70D0101 05050003 82010100 3319F2A7 3E88539F 85C08F28
 67553F93 408DCCC6 EFE2704E C142766C 5FFE0E97 0AFDE0EA 816CB4E2 60FFBC26
 6E411C57 3F1AB3F8 2F1E9959 AED26C86 2C0B059D B692C72C B5859A15 999916F8
 699587DC 94409E7C FF685698 2FB9ACEC 9315F1AA 357E3877 7AE1E37C F5CD7E46
 EB3ADC44 3F22A9E0 EA35E6B8 E5508721 0E8754A1 6A6E3A6A C7FD8E64 6C3C722C
 F90919C9 DE675E5C 301FF83A 0593ACE6 4A469209 CAAEC53F 5102FDD3 AE378090 46282E00
 BCF65EB7 4C257EFD 57986F82 B6DD8336 CEA82E27 63B4C6C5 F92945E8
 2AFE9A95 2AD21793 50FF7987 F4A79079 6FE92AE5 66DFC8B8 14021984 0B1E3F6E
 45D57889 B04883C5 114D79AD FBB2CAFF 587ECF9D
```

quit

crypto pki certificate chain SLA-TrustPoint certificate

ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030 32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934 3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720 526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520 1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE 4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC 7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188 68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7 C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191 C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44 DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201 06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85 4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500 03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905 604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8 467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C 7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B 5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678 80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB 418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0 D697DF7F 28 quit license udi pid C9800-40-K9 sn TTM231803A3 memory free low-watermark processor 375973 service-template webauth-global-inactive inactivity-timer 3600 service-template DEFAULT LINKSEC POLICY MUST SECURE linksec policy must-secure service-template DEFAULT LINKSEC POLICY SHOULD SECURE linksec policy should-secure service-template DEFAULT CRITICAL VOICE TEMPLATE service-template DEFAULT_CRITICAL_DATA_TEMPLATE diagnostic bootup level minimal ! username <REMOVED> privilege 15 password 7 <REMOVED> redundancy mode sso ۱ 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 ! interface TenGigabitEthernet0/0/1 switchport trunk native vlan 310 switchport trunk allowed vlan 310,400,500 switchport mode trunk no negotiation auto channel-group 3 mode active ! interface TenGigabitEthernet0/0/2 switchport trunk native vlan 310 switchport trunk allowed vlan 310,400,500 switchport mode trunk no negotiation auto channel-group 3 mode active ! interface TenGigabitEthernet0/0/3 switchport trunk native vlan 310 switchport trunk allowed vlan 310,400,500 switchport mode trunk no negotiation auto channel-group 3 mode active ! interface GigabitEthernet0 vrf forwarding Mgmt-intf ip address 10.201.81.25 255.255.255.240 negotiation auto no cdp enable ۱ interface Vlan1 no ip address shutdown ۱ 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 ١

```
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
۱
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
۱
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 vtv 0 4
transport input ssh
line vty 5 15
transport input ssh
ntp server 10.81.254.202
ntp server 10.115.162.212
١
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 channelscan 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 txpower 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

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

- [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。

6 26	Monitoring	Cisco Aironet 1850 Series Mobility Express	۹ ک	• 🗠 💳 单
•	Wireless Settings ⋒ wLANs	ACCESS POINTS ADMINISTRATION		
		Access Points 2		
	Access Points Groups	AP1850-1(Active Controller) Search General Controller Brdin 1(2,4,6Hz) Brdin 2(6,6Hz) BR2 11 D	Global AP Continuration Convert	to ME 9 Convert to CAPWAP 9
	📽 WLAN Users			
	📽 Guest WLANs	System Name MIC1960.1	r Difference of the second sec	ferred Master 12 Preferred Master
	DHCP Server	Refresh		
	^{\$} Mesh	Sele Mana Type Location Gill access will be discussed when IP Configuration is changed	Up Time	AP Model
÷.	Management	ME Capable default loc: IP Address 10.0.030	0 days, 14 h 13 m 31 s	AIR-AP1852I-A-K9
se.	Services	CAPWAP default loc: Subnet Mask 255.255.0	0 days, 14 h 13 m 31 s	AIR-AP18521-B-K9
*	Advanced	Gateway 10.0.0.1		
		Country United States (•		
		Changing country code requires controller reset.		
		O Apply O Cancel		

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ネル幅を使用することを推奨します。

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

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

æ	Monitoring	Advanced RF Parameters	
\$	Wireless Settings	2.4 GHz Band	
÷.	Management	5.0 GHz Band	
s.	0	Automatic Flexible Radio Assignment	
-	Services	2.4 GHz Optimized Roaming	
*	Advanced	5 GHz Optimized Roaming	
	◆ SNMP	Event Driven RRM	
	🗟 Logging	CleanAir detection	
	I RF Optimization	5.0 GHz Channel Width	40 MHz
	I RF Profiles		40 MIT2
	& Controller Tools		Lower Density Higher Density
	Security Settings	2.4 GHZ Data Rates	1 2 55 6 9 11 12 18 24 36 48 54
	🖾 смх		802.11b devices not supported
			Lower Density Higher Density
		5.0 GHz Data Rates	6 9 12 18 24 36 48 54
			Some legacy devices not supported
		Select DCA Channels	2.4 GHz □ <u>1</u> 2 3 4 5 <u>6</u> 7 8 9 10 <u>11</u>
			5.0 GHz 🗆 36 40 44 48 52 56 60 64 100 104
			108 112 116 120 124 128 132 136 140 144 149 153 157 161 165
			At least one Channel Number should be selected
		Apply	

RF 最適化

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

æ	Monitoring	Cisco Aironet 1850 Series Mobility Express							٢	₽	\geq	¢
\$	Wireless Settings	(i) (i)										
ġ.	Management	RF OPTIMIZATION										
æ	Services	Il RF Optimization Enable	əd									
*	Advanced ✔ SNMP											
	🗟 Logging	RF Optimization	Enabled		۲	0						
	IRF Optimization	Client Density	Low	Typical	High	0						
	Il RF Profiles	Traffic Type	Voice an	nd Data	Ŧ	0						
	F Controller Tools					1.1						
	Security Settings		Apply									
	🖾 СМХ											

使用する周波数帯域に応じて 5 GHz または 2.4 GHz

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

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネルの幅を 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。

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

£ 30	Monitoring	Cisco Aironet 1850 Series Mobility Express	Q 🛦 @ 🖺 💳 🛎 🌣
\$	Wireless Settings ଇ _{WLANs}	ACCESS POINTS ADMINISTRATION	
	2 Access Points	M Access Points 2	
	Access Points Groups		
	출 WLAN Users	4 Search	sobal AP Configuration Convert to ME Convert to CAPWAP
	🖆 Guest WLANs	Primary Controlle	r 🧿 Primary Controller and Preferred Master 🧔 Preferred Master
	[®] DHCP Server	Refresh	
	4 Mesh	Sele Mana Type Location Name IP Address AP Mac	Up Time AP Model
÷.	Management	Image: Comparison of the state of	0 days, 14 h 37 m 44 s AIR-AP1852I-A-K9
£	Sonvisoo	C Image: CapWap default location AP1850-2 10.0.0.101 38:ed:18:ca:28:40	0 days, 14 h 37 m 44 s AIR-AP1852I-B-K9
Ł	Advanced		
æ) Monitoring	Cisco Aironet 1850 Series Mobility Express	Q ▲ ③ 🖺 ≓ ⊠ ♦
\$	Wireless Settings ⋒ wLANs	AP1850-1(Active Controller) ACCESS POINTS ADMINIS	
		General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	
	웹 Access Points Groups	Admin Mode Enabled	
	📽 WLAN Users	Q Search 2.4 GHz	guration Convert to ME Convert to CAPWAP
	管 Guest WI ANs	802.11b/g/n	ry Controller and Preferred Master 💿 Preferred Master
		Channel Width 20 MHz	
	L	Transmit Power Automatic V	- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1
	7 Mesn	Select Mana Type	Up Time AP Model
	Management	ME Capable	0 days, 13 h 15 m 06 s AIR-AP1852I-A-K9
"	Services	CAPWAP default location AP1850-2 10.0.0.101 38:ed:18:ce:26	3:40 0 days, 13 h 15 m 06 s AIR-AP1852I-B-K9
*	Advanced		
8) Monitoring	Cisco Aironet 1850 Series Mobility Express	Q & ③ ≞ ≕ ■ ❖
\$	Wireless Settings	AP1850-1(Active Controller)	
	M WLANs	AUGESS POINTS ADMINIS General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	
		🔛 Access Points 2	
	Access Points Groups	Admin Mode Enabled	guration Convert to ME Convert to CAPWAP C
	📽 WLAN Users	Channel Automatic	
	📽 Guest WLANs	Channel Width 40 MHz	y Controller and Preferred Master
	DHCP Server	Refresh Transmit Power Automatio	
	∮ Mesh	Select Mana Type	Up Time AP Model

0 days, 13 h 15 m 06 s AIR-AP1852I-A-K

13 h 15 m 06 s

Apply

Cancel

P ME Car

010

C

8	Monitoring Wireless Settings	CISCO Oisco Aironet 1850 Series Mobility Express AP1850-2	Q & @ ≞ ≍ ⊠ ¢
	ຈັ WLANs	ACCESS POINTS ADMINIS General Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	
	2 Access Points	Access Points 2	
	Access Points Groups	Admin Mode Enabled v	obal AP Configuration Convert to ME 0 Convert to CAPWAP 0
	SWLAN Users	Channel Automatic ¥ 802.11b/g/n	
	📽 Guest WLANs	Channel Width 20 MHz v	Primary Controller and Preferred Master Preferred Master
ŝ	DHCP Server	Refresh Transmit Power Automatic	
	∜ Mesh	Select Mana Type	c Up Time AP Model
ġ.	Management	C Apply O Cancel	8:c8:1b:78 0 days, 13 h 15 m 06 s AIR-AP1852I-A-K9
JC.	Services	CAPWAP default location AP1850-2 10.0.0.101 38:e	d:18:ca:28:40 0 days, 13 h 15 m 06 s AIR-AP1862I-B-K9
*	Advanced		
89 47	Monitoring Wireless Settings ৯ wLANs	CISCO Cisco Aironet 1850 Series Mobility Express	
	TACCESS Points	AP1850-2	
	Access Points Groups	General Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	
	📽 WLAN Users	Admin Mode Enabled	ration Convert to ME Convert to CAPWAP
	📽 Guest WLANs	Channel Automatic 5GHz	Controller and Preferred Master 💿 Preferred Master
	DHCP Server	Refresh 802.11a/n	'ac
	4 Mesh	Channel Width 20 MHz +	c Up Time AP Model
÷.	Management	Transmit Power Automatic •	8:c8:1b:78 2 days, 23 h 44 AIR-AP1852I-A-K9
JC	Services	Can Can Can	8:ca:28:40 2 days, 23 h 38 AIR-AP1852I-B-K9
*	Advanced		

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。

🖚 Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	6	11	M	\$
Wireless Settings	WLAN/RLAN CONFIGURATION						
🏪 Access Points							
≌ Access Points Groups	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling						
📽 WLAN Users							
쯓 Guest WLANs	Add n WLAN ID 1		Bollow	Padlo P	allou		
OHCP Server	2 ×		Folicy	5 GHz o	only		
∮ Mesh	Yype WLAN Y						
h Management	Profile Name * voice						
C	SSID * voice						
Services	WLANs with same SSID can be configured, unless layer-2 security settings are different.						
📥 Advanced	Admin State Enabled v						
	Radio Policy 5 GHz only •						
	Broadcast SSID						
	Local Profiling 🔵 🥝						
		ancel					

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。

		Add new WLAN/RLAN			
æ	Monitoring	General WLAN Security VLAN & Firewall Traffic Sha	ning Advanced 802.11u Hotspot2.0 Schedu	ling	
\$	Wireless Setti				
	WLANs	Guest Network			
	Access Points	Captive Network Assistant			
	Access Points Groups	MAC Filtering			
	📽 WLAN Users	Security Type WPA2Enterprise •			
	📽 Guest WLANs	Authentication Server External Radius v	0		
	DHCP Server	Radius Profiling 🕜 💡			dio Policy
	∮ Mesh	BYOD			anz only
÷.	Management	RADIUS Server			
æ	Services				
*	Advanced	Authentication Caching			
	navanooa	Add BADIIIS Authentication Server			
		State	Sarvar ID Addraes	Port	
		X Enabled	10.0.0.20	1812	
		Add RADIUS Accounting Server			
		State	Server IP Address	Port	
		X Enabled	10.0.0.20	1813	

B	Monitoring		Cisco Aironet 1850	Series Mobility Ex	press			Q	A	٩	B	₽	\$
\$	Wireless Settin	ngs											
	WLANs	Add new WLAN/RLAN											
	💾 Access Points												
	^⁰ Access Points Groups	General WLAN Security V	VLAN & Firewall Traffic	Shaping Advanced	802.11u	Hotspot2.0	Scheduling						
	📽 WLAN Users	Guest Network	0										
	📽 Guest WLANs	Captive Network Assistant	0								1846 - 66		
	③ DHCP Server	MAC Filtering									adio P	olicy	
	∮ Mesh	Security Type	Personal								dil di	,	
n -	Management	WPA2	WPA3										
عر	Services	AutoConfig iPSK	00										
-	Services	Passphrase Format	ASCII	•									
-	Advanced	Passphrase *											
		Confirm Passphrase *											
			Show Passphrase										
								Apply		Cancel			

[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。

	dd new WLAN/RLAN	a	A ©	=	
Monitoring	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0				
Wireless Settings	WLAN/RLA Scheduling				
Access Points	Active Allow AAA Override				
🖆 Access Points Groups	Maximum Allowed Clients Unimited(Default) + 0				
📽 WLAN Users	Maximum Allowed Clients Per AP Radio 200				
📽 Guest WLANs	Add new WL 802.11k Disabled +				
DHCP Server	62 M B02.11r Disabled v	sourity Po	lloy	5 GHz only	
∲ Mesh	802.11v Disabled				
🏟 Management	сски				
📌 Services	Client Band Select				
🕹 Advanced	Client Load Balancing				
	Umbrella Profile None +				
	Umbrella Mode Ignore +				

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。

		Add new WLAN/RLAN		×	≓		\$
8	Monitoring	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling					
•	Wireless Setti			_			
	Access Points	Guest Network					
	Maccess Points	Captive Network Assistant 🕜 🕜					
	Groups	MAC Filtering					
	WLAN Users	Security Type WPA2Enterprise v					
		Authentication Server External Radius		dio Pol	licy		
	Mesh	BYOD		3Hz onl	у		
	Management	RADIUS Server					
s.	Somioon			- 11			
÷	Advanced	Authentication Caching					
		Add RADIUS Authentication Server					
		State Server IP Address Port					
		X Enabled 10.0.0.20 1812					
		Add RADIUS Accounting Server					
		State Server IP Address Port					
		Ciliaulian 10.9.9.20 1013					
		G Jululu Gisco Aironet 1850 Series Mobility Express	Q 🛦 🖲	B	≓	\searrow	ф
æ	Monitoring						
۵	Wireless Setting	ADMIN ACCOUNTS					
÷.	Management	St Hears 1					
	Access						
	 Admin Accounts Time 						
	Software Update	Management User Priority Order Local Admin Accounts TACACS+ RADIUS Auth Cached Users					
r	Services	Authentication Call Station ID Type AP MAC Address:SSID •					
*	Advanced	Authentication MAC Delimiter Hyphen					
		Accounting Call Station ID Type IP Address					
		Fallback Mode					
		AP Events Accounting					
		Apply					
~							
626	Monitoring	Add RADIUS Authentication Server					
\$	Wireless Setti	Ings Action Server Index Network User Management State Server IP Address	Shared Key	Port		_	
ġ.	Management			1812			
	Access	e					
		nis					
		Add RADIUS Accounting Server					
c	Software Upda	Action Server Index Network User Management State Server IP Address	Shared Key	Port			
-	Services			1813			
~	Advanced						

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。

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

Monitoring	Cisco Aironet 1850 Series Mobility Express		٩	A	۲	₽ ≓	M	\$
Wireless Settings WLANs Control Contr	Add new WLAN/RLAN W General WLAN Security VLAN & Firewall Traffic Shaping Adv	anced 802.11u Hotspot2.0 Sc	cheduling					
발 Access Points Groups ঔ WLAN Users	Client IP Management Network(Default) Peer to Peer Block							
양 Guest WLANs 왕 DHCP Server 카 Mesh	Use VLAN Tagging Yes • HDHCP Scope Fickle	3 •		Policy		Radio Policy 5 GHz only		
Management Services Advanced	No DHCP Scope associated with VLAN ID Enable Firewall No •							
	Add New VLAN	VLAN Id						
	Image: Contract of the second seco	2 3						
	H 4 1 b MI 10 Terms per page VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN	C Apply	1 - 2 of 2 items					

[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。

		Add new WLAN/RLAN			× 🕇	¢
æ	Monitori	General WLAN Security VLAN & Firewall T	raffic Shaping Advanced	802.11u Hotspot2.0 Scheduling		
\$	Wireless	-				
	WLANs	0.8	Platinum (Voice)	0		
	Access I	403				
	Access F Groups	Average real-time band	width limit should be atleast Aver	age bandwidth limit		
	양 WLAN U	Rate limits per client		khos o		
	📽 Guest W	Average downstream bandwidth limit	0			
	® DHCP S	Average real-time downstream bandwidth limit	0	kbps 📀	icy	
	4 Monh	Average upstream bandwidth limit	0	kbps 🕢	1	
*	/ Wesh	Average real-time upstream bandwidth limit	0	kbps 📀		
D +	Manager					
"	Services	Rate limits per BSSID				
*	Advance	Average downstream bandwidth limit	0	kbps 🕜		
		Average real-time downstream bandwidth limit	0	kbps 😮		
		Average upstream bandwidth limit	0	kbps 🕜		
		Average real-time upstream bandwidth limit	0	kbps 📀		

æ	Monitorii			Fastlane	Disabled	•			
٥	Wireless ๑ wlans		Ap	plication Visibility Control	Enabling Fast	tane will update GoS value to platinum.			
	🖞 Access F			AVC Profile	voice				
	Access F Groups	Add Rule							
	양 WLAN U		s	Application		Action	Average Rate	Burst Rate	
	📽 Guest W								
	THCP S								
	∲ Mesh								

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。

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

		Add new V	WLAN/HLAN					
æ			Active	Add new WLAN/HLAN			Security Policy	Radio Policy
	Monitoring	₿ ×	Enabled	General WLAN Security VLAN & Firewal	Traffic Shaping Advanced 802.	.11u Hotspot2.0		5 GHz only
*	Wireless Settings			Scheduling				
	N WLANs							
	2 Access Points			Allow AAA Override				
	Access Points Groups			Maximum Allowed Clients	Unlimited(Default) v			
	📽 WLAN Users			Maximum Allowed Clients Per AP Radio	200 3			
	📽 Guest WLANs			802.11k	Disabled •			
	[®] DHCP Server			802.11r	Enabled *			
	* Mesh			802 11v	Disabled			
÷.	Management			COMM				
J.C	Services							
<u>т</u>	00111000			Client Band Select				
- X 23	Advanced			Client Load Balancing				
				Umbrella Profile	None 🔻			
				Umbrella Mode	Ignore v			
				Umbrella DHCP Override				
				mDNS				
				mDNS Profile	None 🔻			
				Passive Client	0			
				Please enable Globa when Global Multica	l Multicast in Services->Media Stream. Passi at is disabled.	ive Client will not work		
				Multicast IP	239.1.1.1			
				Multicast Direct	0			
						1		

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。

æ	Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	٩	Ð	11	¢
\$	Wireless Settings ゕ _{WLANs}	ACCESS POINT GROUP						
	🕍 Access Points	Access Points Groups						
		Add new group						
	불 WLAN Users	Q Search General WLANs Access Points RF Profile Ports Intelligent Capture						
	출 Guest WLANs	Add new group Refres						
	OHCP Server	AP Group ni AP Group name express-1 AP of	ount					
	∮ Mesh	AP Group description						
di-	Management	default-grou 2						
Je.	Services	Venue Group UNSPECIFIED +						
*	Advanced	Venue Type UNSPECIFIED v						
		Add New Venue						
		Language Venue Name						
		@ Apply @ Cancel						

[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。

æ	Monitoring		SCO Cisco Airone	t 1850 Serie	s Mobility Express			Q	A	٩	6	11	M	\$			
٠	Wireless Settings ଲ _{WLANs}	ACCESS	S POINT GROUP														
	🖞 Access Points	Acces	s Points Groups	and some													
				Add new	group				đ	_							
	管 WLAN Users	Q Search		General V	VLANs Access Points RF	Profile Po	rts Intelligent (Capture									
	쓥 Guest WLANs	Add new	v group Refresh														
	OHCP Server		AP Group name	⊕ Add n	ew WLAN/RLAN					AP co	unt						
	[∲] Mesh	C ×	express-1		Add new WLAN/RLAN					٥							
÷.	Management	ß	default-group	×	Туре	WLAN	•			2							
"	Services				Profile Name	voice	•										
*	Advanced						9 Update	Cancel									



[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。

8 36	Monitoring		Cisco Aironet 1850 Seri	es Mobility Express				Q	A	٩	B	#		٥
\$	Wireless Settings ৯ WLANs	ACCESS P	Add new group					×						
	별 Access Points Groups	Access P	General WLANs Access Po	ints RF Profile Ports In	telligent Capture									
	^쓸 WLAN Users ^쓸 Guest WLANs	Add new grou	Q Search				Refresh							
	[⊗] DHCP Server ∮ Mesh	C ×	APs in "express-1" group	MAC Address		AP G	All AP Group name							
њ. "С	Management Services		AP1850-1 AP1850-2	38:ed:18:c8:1b:78 38:ed:18:ca:28:40										
*	Advanced				2 K									
		H 4 1 1											of 2 ite	ns
			R 4 1 1 P H	1 - 2 of 2 items		H 4 0 0 + H	No items to disp	icel						

[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。

B	Monitoring		Cisco Airone	t 1850 Series Mot	billity Express					۹	A	٩	Ð	t	M	0
\$	Wireless Settings ৯ _{WLANs}	ACCESS	POINT GROUP													
	🖞 Access Points	Access	s Points Groups	1												
	WLAN Users	Q Search														
	📽 Guest WLANs	Add new	group Refresh													
	³ DHCP Server		AP Group name						AP count							
	⁴ Mesh	⊗ ×	express-1	Add new group					0							
ń-	Management	C	default-group	General WLANs	Access Points R	F Profile Ports	Intelligent Capture		2							
"	Services			-												
*	Advanced				2.4GHz None	•	O Apply	Cancel								

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

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

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。

6 20	Monitoring		Cisco Cieco Aironet 1850 Series Mobility Express									6	11		٥
Ф	Wireless Settings														
ń.	Management	RF Profile	9S												
æ	Services	RF proi	file 6												
*	Advanced ✔ SNMP	Q Search													
	🗟 Logging	() Add n	ew RF Profile	Add RF Profile											
	I RF Optimization	-	RF profile	General 802.11 RRM Clie	nt Distribution		Applied								
		Ø ×	RF profile General express-1 High-Client-Density-802.11a												
		ß	High-Client-Density-802.11a	RF profile name	express-1			No							
		Ø	High-Client-Density-802.11bg					No							
	Security Settings	Ø	Low-Client-Density-802.11a	RF profile description				No							
	CMX	Ø	Low-Client-Density-802.11bg	Band	5GHz		_	No							
		ß	Typical-Client-Density-802.11a	Maximum clients per radio	200			No							
		œ	Typical-Client-Density-802.11bg	Rx SOP Threshold Multicast datarates	Auto	•		No							
		и и 3	1 + H 10 V items per page		(Apply	Cancel								7 of 7 ite	ms

[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。

686 м	lonitoring	Cisco Aircnet 1850 Series Mobility Express									٩	8	11		٥
🍄 w	ireless Settings														
й⊷ м	anagement	RF Profiles													
Se Se	ervices	RF profile 6													
📥 Ac	dvanced SNMP	Q Search													
6	Logging	🛞 Add new RF Profile													
I														1	
I		Z x Add RF Profile													
F	Controller Tools	General 802.11 RRM Client Distribution													
\$	Security Settings	G													
	смх	Ø Data rat			10 24			49	_						
		B NGS settin	6 9	12	18 24		36	46	54						
		C MCS settin	0 1 2	34567	8 9 10 11	12 13 14 15 16 17	18 19 20 21 22 23 24	25 26 27 28 29	30 31						
							(e	pply 8 Cr	incel						

[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。

🍄 Monitoring	e dia	co Cisco Aironet		Q	A	٩	B	#		٥				
Wireless Settings														
📥 Management	RF Profile:	S												
🖋 Services	RF prof	RF profile 6												
Advanced	Q Search													
🗟 Logging	⊕ Add ne	w RF Profile	Add RF Profile											
I RF Optimization		RF profile					Applied							
RF Profiles	🕑 🕱 express-1		General 802.11 RRM Client Distribution											
& Controller Tools	C#	High-Client-Density-802					No							
	C	High-Client-Density-802	Channel Widt Select DCA Channels	dth 40 MHz 🔻			No							
Security Settings	8	Low-Client-Density-802		Select All 🗆 36 40	40 44 48 52 56 60 64 100	4 100 104 108	No							
CMX	C.	Low-Client-Density-802		112 116 120 124 128 132 136 140 144 149 153 157 161 165			No							
	ß	Typical-Client-Density-8					No							
	Ø	Typical-Client-Density-E		Some of the channels a enabled. These channel At least one Channel N	are not allowed to configure a Is can be enabled in RF Optir umber should be selected @ Apply	as they are not mization screen.	No							
												1 -	7 of 7 iter	ms
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。

			co Cisco Aironet 1850 Se	ries Mobility	Express		Q	A	۲	B	₽	\geq	٥
2	Monitoring												
\$	Wireless Settings	Media Str	eam Settings										
ġ.	Management	M Med	a Stream Disabled										
æ	Services Media Stream		Disabica										
	♥ TLS		Global Multicast										
	♥ mDNS		Multiment Direct										
	Network Assurance		Multicast Direct	_									
	🚔 Webhook	Ses	sion Announcement State										
	Intelligent Capture	Se	ssion Announcement URL	URL									
	🛎 Umbrella	Ses	sion Announcement Email	Email									
Ł	Advanced	Sess	ion Announcement Phone	Phone									
		Sea	ssion Announcement Note	Note	li.								
				Apply									
		Add New S	Stream										
		Action	Stream Name		Start IP Address	End IP Address		Operation	Status				
		×	10.0.0.40		239.1.1.40	239.1.1.40	1	Multicast-c	lirect				

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

		Add ne	W WLAWHLAN			×		
æ			Active	Add new WLAN/RLAN		0	Security Policy	Radio Policy
\$	wonitoring Wireless Settings WLANs	₿×	Enabled	General WLAN Security VLAN & Firewal Scheduling	I Traffic Shaping Advanced	802.11u Hotspot2.0		5 GHz only
	🕍 Access Points				-			
	Access Points Groups			Allow AAA Override Maximum Allowed Clients	Unlimited(Default) v			
	암 WLAN Users			Maximum Allowed Clients Per AP Radio	200 3			
	📽 Guest WLANs			802.11k	Disabled •			
	DHCP Server			802.11r	Enabled •			
	⁴ Mesh							
÷.	Management			802.11				
J.C	Services			Olivert Band Select				
-				Client Band Select				
	Advanced			Client Load Balancing				
				Umbrella Profile	None v			
				Umbrella Mode	Ignore v			
				Umbrella DHCP Override				
				mDNS				
				mDNS Profile	None 🔻			
				Passive Client	0			
				Please enable Globa when Global Multica	Il Multicast in Services->Media Stream est is disabled.	. Passive Client will not work		
				Multicast IP	239.1.1.1			
				Multicast Direct	0			

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。

cisco	HOME NETWORK A	SSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e C <u>M</u> ANAGEMENT	onfiguration	Ping Logout Refre		
NETWORK	Hostname ap-1					ap-1	uptime is 1 day	, 4 hours, 51 minutes		
NETWORK MAP Summary	Network Interfaces: Summary									
Adjacent Nodes	System Settings									
NETWORK INTERFACE	IP Address (Static)			10.9.0.9						
Summary	IP Subnet Mask			255.255.255.0						
IP Address	Default Gateway			10.9.0.2						
GigabitEthernet0 Radio0-802.11N 2.4GHz	MAC Address		1	8e7.281b.3f54						
Radio1-802.11AC 5GHz	Interface Status	Giga	abitEthernet		Radio0-802.1	1N ^{2.4GHz}	Radio1-802.1	1AC ^{5GHz}		
	Software Status			Enabled		Disabled	k in the second s	Enabled 1		
	Hardware Status			Up		Down	ŀ	Up î		
	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。

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

帯域1は、UNII-1 チャネル(チャネル36、40、44、または48)を使用するアクセスポイントでのみ選択できます。 使用する周波数帯域に応じて5 GHz または2.4 GHz

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

その他のアクセスポイントを自動割り当て方式と静的に設定されているアクセスポイントのアカウントに対して有 効にできます。 この設定は、エリア内に断続的な干渉が存在する場合に必要です。

Cisco 802.11n アクセス ポイントを使用している場合は 5 GHz チャネルの幅を 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。



a9.3-21	Mb/sec 🤇	Require	•	Enable	Oisable
MCS Rates: 0 1 2 3	4 5	6 7 8 9 10	11 12 13 14	15 16 17 18 1	9 20 21 22 23
Enable O O O	00	00000	0000	0000	
	00	000000	00000	0 0 0 0 0 0	
Transmitter Power (dBm):)15 () 12 () 9 () 6	🔾 3 💿 Max		Power Translation Tab
Client Power (dBm):	c	Local 015 012	9 6 3 Ma	ах	(mwabiii)
DefaultPadio Channel		Nannal 26 - 5190 MH	Cha	annel 36 5180 MH	
Dynamic Frequency Selection E	Bands: B	and 1 - 5 150 to 5 250	GH7		-
	Bi Bi Bi	and 2 - 5.250 to 5.250 and 2 - 5.250 to 5.350 and 3 - 5.470 to 5.725 and 4 - 5.725 to 5.825	GHz GHz GHz		
Channel Width:		3elow 40 MHz ᅌ 20	MHz		
World Mode	C	Disable	C		 Dot11d
Multi-Domain Operation:			Outdoor		-
Country Code.			Outdoor		
Radio Preamble	c	Short	(Long	
Antenna:	\sim	a-antenna Oa	b-antenna 🛛 🔾 a	bc-antenna 📀	abcd-antenna
Internal Antenna Configuration:	•	Enable	(Disable	
	A	ntenna Gain(dBi):	0 (-128	3 - 128)	
Gratuitous Probe Response(GP	R):) Enable		 Disable 	
	Р	eriod(Kusec): DIS	ABLED (10-255)		
	Т	ransmission Speed	: none	0	
Traffic Stream Metrics:	C) Enable		Disable	
Aironet Extensions:	c	Enable	C	Disable	
Ethernet Encapsulation Transfo	rm: 🕻	RFC1042	C	802.1H	
Reliable Multicast to WGB:		Disable		Enable	
Public Secure Packet Forwardir	ng: <u>PS</u>	PF must be set per V	LAN. See VLAN page	2	
Beacon Privacy Guest-Mode:	\sim	Enable	Ċ	Disable	
Beacon Period:	100 ()	20-4000 Kusec)	Data Beacon Ra	ate (DTIM):	(1-100)
Max. Data Retries:	64 (1-128)	RTS Max. Retrie	es:	34 (1-128)
Fragmentation Threshold	2346 /	256-2346)	RTS Threshold		(0-2347)
ragnentation micenola.	2040 (200-20407	Are meshold.	4	(0-2047)
Root Parent Timeout:		0	(0-65535 sec)		
Poot Parant MAC 1 (antional):			(НННН.НННН.Н	ннн)	
Root Parent MAC 1 (optional).			(НННН.НННН.Н	ННН)	
Root Parent MAC 2 (optional):					
Root Parent MAC 2 (optional): Root Parent MAC 2 (optional):			(НННН.НННН.НІ	HHH)	

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。

،، ،،، ،، cısco	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efre MANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG				
Security	Hostname ap-1	ap-1 uptime is 1 day, 4 hours, 33 minutes				
Admin Access						
Encryption Manager	Security: Global SSID Manager					
SSID Manager	SSID Properties					
Dot11u Manager	Current SSID List					
Server Manager	< NEW > SSID:	voice				
AP Authentication	data voice VLAN:	3 Define VLANs				
Intrusion Detection		Backup 1:				
Local RADIUS Server		Backup 2:				
Advance Security		Backup 3:				
	Band-Select:	Band Select				
	Universal Admin Mode:	Universal Admin Mode				
	Interface:	Radio0-802.11N ^{2.4GHz}				
		Radio1-802.11AC ^{5GHz}				
	Network ID: (0-4096)					
	Client Authentication Settings					
	Methods Accepted:					
	Open Authentication: with EAP	0				
	Web Authentication Web Pass					
	Shared Authentication: <pre>< NO ADDITION></pre>	٥				
	Network EAP: NO ADDITION >					
	Server Priorities:					
	EAP Authentication Servers	MAC Authentication Servers				
	Use Defaults <u>Define Defaults</u>	• Use Defaults Define Defaults				
	Customize	◯ Customize				
	Priority 1: < NONE > 📀	Priority 1: < NONE > 📀				
	Priority 2: < NONE > 3	Priority 2: < NONE > C				
	Priority 3: < NONE > 3	Priority 3: <pre>< NONE > </pre>				
	Client Authenticated Key Management					
	Key Management: Mandatory					

	-		O ASCII O Hexadecimal
11w Configuration:		Disable ᅌ	
11w Association-co	meback:	1000	(1000-20000)
11w Saquery-retry:		100	(100-500)
IDS Client MFP			
Enable Client M	FP on this SSI	D: Optional	0
AP Authentication			
Credentials:		< NONE >	Define Credentials
Authentication Method	ds Profile:	< NONE >	Define Authentication Methods Profiles
Accounting Settings			
Enable Account	ling		Accounting Server Priorities:
			Use Defaults Define Defaults
			◯ Customize
			Priority 1: < NONE > ᅌ
			Priority 2: < NONE > ᅌ
			Priority 3: <pre>< NONE > </pre>
			Priority 3: <pre> </pre> <pre> </pre>
Rate Limit Parameters			Priority 3: < NONE > 📀
Rate Limit Parameters Limit TCP:			Priority 3: <pre> NONE > S </pre>
Rate Limit Parameters Limit TCP:	Rate:	Burst-Size	Priority 3: <a>NONE > <a>S e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output:	Rate:	Burst-Siz Burst-Siz	Priority 3: < NONE > 3 e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP:	Rate: Rate:	Burst-Size Burst-Size	Priority 3: <pre></pre>
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input:	Rate: Rate: Rate:	Burst-Sizi Burst-Sizi Burst-Sizi	Priority 3: <a>NONE > e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: Output:	Rate: Rate: Rate: Rate:	Burst-Size Burst-Size Burst-Size Burst-Size	Priority 3: <a>NONE > (0-500000) (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings	Rate: Rate: Rate: Rate:	Burst-Size Burst-Size Burst-Size Burst-Size	Priority 3: <a>NONE > (0-500000) (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: Output: General Settings	Rate: Rate: Rate: Rate: ed Capabilites	Burst-Size Burst-Size Burst-Size of this SSID	Priority 3: <pre> NONE > Priority 3: </pre> Priority 3: Priority 3: <pre> Priority 3: </pre> Priority 3: <pre> Priority 3: </pre> Priority 3: <pre> Priority 4: </pre> Priority 4: <pre> Pri</pre>
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extended	Rate: Rate: Rate: Rate: ed Capabilites	Burst-Size Burst-Size Burst-Size Burst-Size of this SSID reless Provisio	Priority 3: <pre> NONE > </pre> <pre> e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) </pre>
Rate Limit Parameters Limit TCP: Input: Output: Input: Output: Output: General Settings Advertise Extend	Rate: Rate: Rate: Rate: Rate: ed Capabilites	Burst-Size Burst-Size Burst-Size Burst-Size of this SSID reless Provisio s SSID as a Sec	Priority 3: <a>NONE > e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (WPS) Support condary Broadcast SSID
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extend	Rate: Rate: Rate: Rate: ed Capabilites Advertise Wit	Burst-Size Burst-Size Burst-Size Burst-Size of this SSID reless Provisio s SSID as a Sec	Priority 3: <pre> NONE > </pre> e: (0-500000) e: (0-5000000) e: (0-5000
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extend Enable IP Redirect	Rate: Rate: Rate: Rate: d Capabilites Advertise Will Advertise this	Burst-Size Burst-Size Burst-Size Burst-Size of this SSID reless Provisio s SSID as a Sec	Priority 3: <a>NONE > a: <a>(0-500000) b: (0-500000) b: (0-500000) b: <a>(0-500000) c: <a>(0-50000

IP Filte	er (optional): < NONE > O Define Filter	
Association Limit	(optional): (1-255)	
EAP Client (option	al):	
	Usendine. Passworu.	
Multiple BSSID Beacon	Settings	
Multiple BSSID Be	acon	
	Set SSID as Guest Mode	
	Set DataBeacon Rate (DTIM): DISABLED (1-100)	
		Apply Cancel
Guest Mode/Infrastructu	re SSID Settings	Apply Cancel
Guest Mode/Infrastructu	re SSID Settings	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} :	re SSID Settings	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: < NONE > C	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: << NONE > C Multiple BSSID	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID:	Single BSSID Set Single Guest Mode SSID: << NONE > C Multiple BSSID C Force Infrastructure Devices to associate only to this SSID	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID: Radio1-802.11AC ^{5GHz} -	Single BSSID Set Single Guest Mode SSID: << NONE > C Multiple BSSID << NONE > C Force Infrastructure Devices to associate only to this SSID	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID: Radio1-802.11AC ^{5GHz} : Set Beacon Mode:	Image: Single BSSID Set Single Guest Mode SSID: NONE > C Multiple BSSID Force Infrastructure Devices to associate only to this SSID Single BSSID Set Single Guest Mode SSID: NONE > C	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID: Radio1-802.11AC ^{5GHz} : Set Beacon Mode:	Image: Single BSSID Set Single Guest Mode SSID: < NONE > C Multiple BSSID < NONE > C Force Infrastructure Devices to associate only to this SSID Single BSSID Set Single Guest Mode SSID: < NONE > C Multiple BSSID Set Single Guest Mode SSID: < NONE > C	Apply Cancel
Guest Mode/Infrastructu Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID: Radio1-802.11AC ^{5GHz} : Set Beacon Mode: Set Infrastructure SSID:	Single BSSID Set Single Guest Mode SSID: < NONE > C • Multiple BSSID < NONE > C • Single BSSID Single BSSID Single BSSID Single BSSID Single BSSID Set Single Guest Mode SSID: < NONE > C • Multiple BSSID • Multiple BSSID • NONE > C • Force Infrastructure Devices to associate only to this SSID	Apply Cancel

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。

ululu cisco	<u>H</u> OME <u>N</u> ETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping Logout	<u>R</u> efrest		
Services	Hostname ap-1					a	p-1 uptime is 1	day, 4 hours, 48 i	minutes		
Telnet/SSH											
Hot standby	Services: VLAN										
CDP	Global VLAN Pr	operties									
DNS	Current Native	VLAN: VLAN 10									
Filters	ounoninauto										
НТТР	Assigned VLAN	S									
QOS	Current VLAN	_ist	Create	VLAN		Define SSID	<u>s</u>				
Stream	< NEW >										
SNMP	VLAN 2 VLAN 3		VL	NID:		3	(1-409	4)			
SNTP	VLAN 10							.,			
VLAN		Delete	VLA	AN Name (op	tional):						
ARP Caching		Delete		Native VL	AN						
Band Select				Enable Pu	iblic Secure P	acket Forwarding	9				
Auto Config				Radio0-80	2.11N ^{2.4GHz}						
				Radio1-80	2.11AC ^{5GHz}						
				Managem	ent VLAN (If r	non-native)					
							C	Apply Can	icel		
	VLAN Informatio	on									
	View Informatio	n for: VLAN 2 ᅌ									
		GigabitEthern	et Packets	Radio0	-802.11N ^{2.4GHz}	Packets	Radio1-802.1	11AC ^{5GHz} Packet	s		
	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。

ululu cisco	<u>H</u> OME	<u>N</u> ETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping Logout <u>R</u> efre	
Security	Hostn	ame ap-1					ap-1	uptime is 1 day	/, 4 hours, 32 minutes	
Encryption Manager	Secu	urity: Encrypt	tion Manager							
SSID Manager	Set	Encryption I	Mode and Keys fo	or VLAN:			3 ᅌ		Define VLANs	
Server Manager	Encr	yption Mode	5							
AP Authentication	0	None								
Local RADIUS Server	WEP Encryption Optional									
Autonice Security			Cisco Comp	pliant TKIP Fea	itures: 🗌 Er	iable Message	Integrity Check (N et Keving (PPK)	1IC)		
	0	Cipher	AES CCMP	\$	0 -		arria)			
	Encr	yption Keys								
	Transmit Key					Encryptio	n Key (Hexadecim	nal)	Key Size	
		Encr	yption Key 1:	\circ					128 bit ᅌ	
		Encr	yption Key 2:	0					128 bit ᅌ	
		Encr	yption Key 3:	0					128 bit ᅌ	
		Encr	yption Key 4:	0					128 bit ᅌ	
	Glob	al Properties	i.							
	Bro	adcast Key R	otation Interval:	0	Disable Rotatio	on				
				0	Enable Rotatic	n with Interval	DISABLED (10-	10000000 sec)		
	WPA Group Key Update: Enable Group Key Update On Membership Terminatio							nination		
		Enable Group Key Update On Member's Capability Change								
									Apply Capcel	

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

				Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh		
CISCO	HOME NETWORK ASSOC	IATION WIRELESS SECURIT	Y <u>S</u> ERVICES <u>M</u> ANAGEM	ENT <u>S</u> OFTWARE <u>E</u> VENT LOG		
ecurity			S			
Admin Access	Hostname ap-1			ap-1 uptime is 1 day, 4 hours, 42 minutes		
Encryption Manager	Security: Server Manager					
SSID Manager	Backup RADIUS Server					
Dot11u Manager	IP Version:					
Server Manager	Backup RADIUS Server Na	ame:				
AP Authentication	Backup RADIUS Server:		(Hostname or IP Address)			
Intrusion Detection	Shared Secret:		(Hostilane of h 74	uu (555)		
Advance Security	Shared Secret.			Apply Delete Cancel		
,						
	Corporate Servers					
	Current Server List					
	RADIUS					
	< NEW >	IP Version:	○IPV4 ○IPV6			
	10.0.0.20 10.9.0.9	Server Name:	10.0.0.20			
		Server:	10.0.020	(Hostname or IP Address)		
		Shared Secret:	•••••			
	Delete	Authentication Port (optional	: 1812 (0-65535)			
		Accounting Port (optional):	1813 (0-65535)			
				Apply Cancel		
	Default Server Priorities					
	EAP Authentication	MAC Authenti	cation	Accounting		
	Priority 1: 10.0.0.20 ᅌ	Priority 1: < N	IONE > 📀	Priority 1: 10.0.0.20		
	Priority 2: < NONE > ᅌ	Priority 2: < N	IONE > 🗘	Priority 2: < NONE > 🗘		
	Priority 3: < NONE > ᅌ	Priority 3: < N	IONE > 🗘	Priority 3: < NONE > ᅌ		
	Admin Authentication (RA	DIUS) Admin Authen	tication (TACACS+)			
	Priority 1: < NONE > ᅌ	Priority 1: < N	IONE > 📀			
	Priority 2: < NONE > ᅌ	Priority 2: < N	IONE > 📀			
	Priority 3: < NONE > ᅌ	Priority 3: < N	IONE > 📀			
				Apply Cancel		
	1					

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。

،، ،،، ،، cısco	Saye Configuration Ping Logout <u>R</u> efresh HOME <u>N</u> ETWORK <u>A</u> SSOCIATION WIRELESS <u>S</u> ECURITY <u>S</u> ERVICES <u>M</u> ANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG										
Wireless Services	UNDE STATUS										
AP	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 50 minutes										
WDS	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。

սիսիս						Sa <u>v</u> e (Configuration	Ping Logout <u>R</u> efres
CISCO	<u>H</u> OME <u>N</u> ETW	ORK <u>A</u> SSOCIATION	WIRELESS	SECURITY	<u>S</u> ERVICES	<u>M</u> ANAGEMENT	<u>S</u> OFTWARE	<u>E</u> VENT LOG
Services	Hostname ap	-1				ar	o-1 uptime is 1 o	lay, 4 hours, 48 minutes
Telnet/SSH								
Hot standby	Services: V	LAN						
CDP	Global VLA	N Properties						
DNS								
Filters	Current Na	ative VLAN: VLAN 10						
НТТР	Assigned V	LANs						
QOS	Current VI	AN List	Create			Define SSID	\$	
Stream			Greate			Denne Gold	2	
SNMP	VLAN 2							
SNTP	VLAN 3 VLAN 10		VLA	AN ID:		10	(1-409	4)
VLAN			VLA	AN Name (op	tional):			
ARP Caching		Delete		Native VL	AN			
Band Select	Enable Public Secure Packet Forwarding							
Auto Config								
				Radiou-80	2.11N ^{2.4612}			
	☑ Radio1-802.11AC ^{5GHz}							
	Management VLAN (If non-native)							
								Apply Cancel
	VLAN Inform	mation						
	View Inform	nation for: VLAN 2						
		GigabitEthern	et Packets	Radio	-802.11N ^{2.4GHz}	Packets	Radio1-802.1	1AC ^{5GHz} 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。

ululu cisco	Save Configuration Ping Logout Refrest
Wireless Services	WDS STATUS
AP	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 51 minutes
WDS	Wireless Services: WDS - Server Groups
	Server Group List
	<pre>Server Group Name: WDS </pre>
	Group Server Priorities: Define Servers
	Delete Priority 1: 10.9.0.9
	Priority 2: < NONE > 😒
	Priority 3: < NONE > 📀
	Use Group For: Infrastructure Authentication
	Client Authentication
	Authentication Settings SSID Settings
	EAP Authentication Apply to all SSIDs
	LEAP Authentication Restrict SSIDs (Apply only to listed SSIDs)
	MAC Authentication SSID: DISABLED Add
	Default (Any) Authentication
	Apply Cancel

次に、クライアント認証に使用するサーバ グループを定義します。

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

uluilu cisco	Save Configuration Ping Logout <u>R</u> efresh HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Wireless Services	WDS STATUS
AD	Hostname ap-1 ap-1 uptime is 2 days, 2 hours, 31 minutes
WDS	Wireless Services: WDS - Server Groups
	Server Group List
	Server Group Name: Clients <new> WDS</new>
	Clients Group Server Priorities: Define Servers
	Delete Priority 1: 10.0.0.20 0
	Priority 2: < NONE >
	Priority 3: < NONE > 😒
	Use Group For:
	O Client Authentication
	Authentication Settings SSID Settings
	EAP Authentication Apply to all SSIDs
	LEAP Authentication Restrict SSIDs (Apply only to listed SSIDs)
	MAC Authentication SSID: DISABLED Add
	Default (Any) Authentication
	Apply Cancel

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。

.ı ı.ı ı. cısco	<u>H</u> OME <u>N</u>	ETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping Logout	<u>R</u> efresh
Security		STATISTIC	cs 👔	GENER/	AL SET-UP		EAP-FAST SET-UP	•		
Admin Access	Hostnam	e ap-1					ap-	1 uptime is 1 da	y, 4 hours, 43 mi	nutes
Encryption Manager	Securit	y: Local RA	DIUS Server - G	eneral Set-Up						
SSID Manager	Local Radius Server Authentication Settings									
Dot11u Manager	Enable	Authentica	tion Protocols:	E/	AP FAST					
Server Manager					AP					
Intrusion Detection				2 M	AC					
Local RADIUS Server								A	Cance	
Advance Security										
	Networ	k Access Se	ervers (AAA Clie	nts)						
	Currer	nt Network A	ccess Servers							
	< NEW 10.9.0.9) > 9			Network Acce	ess Server:	10.9.0.9		(IP Address)	
					Sharad Saara					
					Silareu Secre					
	D	elete								
								4	opply Cance	я
	Individu	ual Users								
	Currer	nt Users								
	< NEW	>		Username:		wds				
	wds			Password:		•••••		🔿 Text 💿 N	T Hash	
				Confirm Pa	ssword:					
	D	elete		Group Nam	e:	< NONE >	0			
							thentication Only			
							dientication only		Cance	
	User Gr	oups								
	Curren	t User Grou	ps							
	< NEW	>	Grou	p Name:						
		,								
			Sess	ion Timeout (optional):			(1-4294967295 s	ec)
	De	elete	Faile	d Authenticat	ions before L	ockout (optio	onal):	(1-4294967295	i)	
			Lock	out (optional)	:		Infinite			
							 Interval 	(1-4	294967295 sec)	
			VLA	N ID (optional)	:					
			SSID	(optional):					Add	
				(
									Delete	
								A	Apply Cance	н

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。

. cısco	HOME NETWORK ASSOCIATION WIRELE	Save Configuration <u>P</u> ing Logout <u>R</u> efresh SS <u>SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG</u>
Wireless Services	Hostname ap-1	ap-1 uptime is 1 day, 4 hours, 50 minutes
WDS	Wireless Services: AP	
	Participate in SWAN Infrastructure:	• Enable 🔿 Disable
	WDS Discovery:	Auto Discovery
		Specified Discovery: 10.9.0.9 (IP Address)
	Username:	wds
	Password:	••••••
	Confirm Password:	
	Authentication Methods Profile:	< NONE > 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。

ululu cisco	HOME NETWORK	ASSOCIATION WIRE		SECURITY	SERVICES	Sa <u>v</u> e MANAGEMENT	Configui	ration <u>P</u> ii	ng Logout	<u>R</u> efresh
Wireless Services		JS	GENER	AL SET-UP		SERVER GROU	IPS			
AP	Hostname ap-1						ap-1 up	otime is 1 d	ay, 5 hours, 1	minute
WDS	Wireless Services: WDS - Wireless Domain Services - Status									
	WDS Information									
	MAC Address	IPv4 Address		IPv6 Addre	ess	Priority		State		
	18e7.281b.3f54	10.9.0.9		:		255		Administr - ACTIVE	atively Stand	Alone
	WDS Registration			_						
	APs: 1			Mobile Nod	es: 0					
	AP Information									
	Hostname	MAC Address		IPv4 Addre	955	IPv6 Address		CDP Neighbo	r State	
	ap-1	18e7.281b.3f54	18e7.281b.3f54			::		Switch-2.g		ERED
	Mobile Node Inform	ation								
	MAC Address	IP Address	State			SSID	VLAN I	D B	SSID	
	Wireless Network N	lanager Information								
	IP Address	Authentication Statu	15							
									F	tefresh

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

rvices	QoS POLICIES	AC	ADIO0-802.11N ^{2.4GHZ} CESS CATEGORIES	ACCESS	802.11AC ^{5GHZ}	I	ADVANCED		
elnet/SSH	Hostname ap-1					ap-1	uptime is 1 da	ay, 4 hour	s, 47 minu
ot standby									
DP	Services: QoS Policies	s - Acces	s Category						
NS	Access Category Defin	nition							
ilters									
ттр	Access Categor	У	Background (CoS 1-2)	Be: (C	oS 0.3)	Vid (CoS	eo 4-5)	(Cos	6-7)
os		40			1				
tream	Window	AP	4	4		3	1	2	
NMP	(2x-1; x can be 0-10)	Client	4	4		3		2	
NTP	Max Contention	AP	10	6	1	4		3	
LAN	Window	100			1				
RP Caching	(2 ^x -1; x can be 0-10)	Client	10	10		4		3	
and Select	Fixed Slot Time	AP	7	3		1	-		
uto Config	(0-20)	Client	7	3		2	:	2	
	Transmit Opportunity	AP	0	0		3008		1504	
	(0-65535 µS)	Client	0	0		3008	1	1504	
	Admission Control for	Video ar	nd Voice	Optimized	Voice WFA	Default		Apply	Cancel
	Video(CoS 4-5)	Admis	sion Control						
	Voice(CoS 6-7)								
		Admis:	sion Control						
		Max Ch	annel Capacity (%):	75					
		Roam C	channel Capacity (%):	6					
								Analy	Onneri

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。

ices		RADIO0-802.11N ^{2.4GHZ} ACCESS CATEGORIES	RADIO1-802.11AC ^{5GH} ACCESS CATEGORIES		VANCED
net/SSH	Hostname ap-1			ap-1 upti	me is 1 day, 4 hours, 44 m
standby					
,	Services: QoS Policies				
, ars	Create/Edit Policies				
P	Create/Edit Policy:	Voice ᅌ			
3					
am	Policy Name:	Voice			
IP					
Р	Classifications	DSCB - COS Controlled Lood (4)			
N	classifications.	DSCP - COS Video < 100ms Latence	y (5)		
Caching		DSCP - COS Voice < Toms Latency	(6)		
d Select					
o Config		Delete Classification			
	Match Classification	15:	A	pply Class of Ser	vice
	IP Precedence:	Routine (0)		Best Effort (0)	Add
	IP DSCP:	Best Effort	•	Best Effort (0)	Add
		0 (0-	63)		
	IP Protocol 119			Best Effort (0)	Add
	Filter:	No Filters defined. Define Filters.			
	Default Classificat	ion for Packets on the VLAN:		Best Effort (0)	Add
	Rate Limiting:				
	Bits per Sec.:	(8000-20000000	0) Burst Rate (Bytes)	:	(1000-512000000)
	Conform Action:	Transmit	Exceed Action:	Drop ᅌ	Ad
				Ap	ply Delete Cance
	Apply Policies to Interfa	ice/ VLANs			
	VLAN 2	Radio0-802.11N ^{2.4GHz}	Radio1-802.11/	AC ^{5GHz}	GigabitEthernet0
	Incoming		Data	0	Data ᅌ
	Outgoing		Data	0	Data ᅌ
	VLAN 3	Radio0-802.11N ^{2.4GHz}	Radio1-802.11/	AC ^{5GHz}	GigabitEthernet0
	Incoming		Voice	`	Voice
	Outgoing		< NONE >	\$	< NONE > ᅌ
	VLAN 10	Radio0-802.11N ^{2.4GHz}	Radio1-802.11	AC ^{5GHz}	GigabitEthernet0
	Incoming		< NONE >	٥	< NONE > ᅌ
	Outgoing		< NONE >	\$	< NONE > ᅌ

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。

uluili. cisco	Save Configuration Ping Logout Refresh
Services	QoS POLICIES
Telnet/SSH	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 47 minutes
Hot standby	
CDP	Services: QoS Policies - Advanced
DNS	IP Phone
Filters	
НТТР	QoS Element for Wireless Phones : Enable Dot11e
QOS	 Disable
Stream	
SNMP	
SNTP	Snooping Helper: O Enable O Disable
VLAN	
ARP Caching	
Band Select	AVVID Priority Mapping
Auto Config	Map Ethernet Packets with CoS 5 to CoS 6: O Yes O No
	WiFi MultiMedia (WMM)
	Enable on Radio Interfaces:
	Radio0-802.11N ^{2.4GHz}
	Radio1-802.11AC ^{5GHz}
	Apply Cancel

[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。

CISCO			233 <u>3</u> 200ki11	<u>SERVICES</u>	MANAGEMENT	<u>3</u> OFTWARE	EVENTLOG
ervices	[≣ RADIO0-802.11N ^{2.4GHZ}]	RADIO1-802	2.11AC ^{5GHZ}				- 1910 - 1920 - 24 (B)
Telnet/SSH	Hostname ap-1				a	p-1 uptime is 1 c	lay, 4 hours, 48 minute
lot standby	Services: Stream						
CDP							
INS	Packet Handling per User P	riority:		25.28. NSS			
ilters	User Priority	Packet H	andling	Max Retries for Pa	icket Discard		
ITTP	CoS 0 (Best Effort)	Reliable	0	NO DISCARD	(0-128)		
ios	CoS 1 (Background)	Reliable	0	NO DISCARD	(0-128)		
NMP	CoS 2 (Spare)	Reliable	0	NO DISCARD	(0-128)		
NTP	CoS 3 (Excellent)	Reliable	•	NO DISCARD	(0-128)		
LAN RP Caching	CoS 4 (Controlled Load)	Reliable	\$	NO DISCARD	(0-128)		
and Select	CoS 5 (Video)	Reliable	\$	NO DISCARD	(0-128)		
uto Config	CoS 6 (Voice)	Reliable	\$	NO DISCARD	(0-128)		
	CoS 7 (Network Control)	Reliable	0	NO DISCARD	(0-128)		
	Low Latency Packet Rates:						
	6.0Mb/sec :	O Nominal	O Non-Nominal	 Disable 			
	9.0Mb/sec :	O Nominal	O Non-Nominal	 Disable 			
	12.0Mb/sec :	O Nominal	Non-Nominal	 Disable 			
	18.0Mb/sec :	O Nominal	O Non-Nominal	 Disable 			
	24.0Mb/sec :	O Nominal	Non-Nominal	 Disable 			
	36.0Mb/sec :	O Nominal	O Non-Nominal	 Disable 			
	48.0Mb/sec :	O Nominal	O Non-Nominal	 Disable 			
	54.0Mb/sec :	O Nominal	O Non-Nominal	 Disable 			
							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。

،، ،،، ،، cısco	Sa <u>v</u> e Configuration Ping Logout <u>R</u> efress HOME <u>N</u> ETWORK <u>A</u> SSOCIATION WIRELESS <u>S</u> ECURITY <u>S</u> ERVICES <u>M</u> ANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG
Services	Hostname and and the state of t
Telnet/SSH	
Hot standby	Services: ARP Caching
CDP	
DNS	
Filters	E Francisk ADD Descents To Destin Interfaces Million Mark 10 Addresses Are Kanne
нттр	Forward AKP Requests to Radio Interfaces when Not All Client IP Addresses Are Known
QOS	
Stream	
SNMP	Apply Cancel

Cisco RoomOS DX Series ワイヤレス LAN 導入カイド

```
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
١
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
۱
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
۱
crypto pki trustpoint TP-self-signed-672874324
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-672874324
revocation-check none
rsakeypair TP-self-signed-672874324
crypto pki certificate chain TP-self-signed-672874324 certificate
self-signed 01
 30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 36373238 37343332 34301E17 0D313630 38303332 33303533
 385A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
 532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3637 32383734
 33323430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 CB155DD1
 3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9 5F5A1B75
 7910F9F5 6E9EDEF4 730942C7 17DC4CBC E5AE3E49 0AF79419 0BEF34BC
 5DCEB4E2 FF2978CB C34D5AEE ED1DFB58 C7BF6592 61C1AD25 3EF87205 15EA58C2
 0A5E2B15 7F08FAEA 5DA2BFA7 95E56C60 22C229C7 024A91D7 A4FEB50B 5425357F
 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
 23041830 168014FC 2FE6CF0E E0380A40 11381459 5D596E3E A684DA30 1D060355
 1D0E0416 0414FC2F E6CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
 4886F70D 01010505 00038181 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
 A8B174BC A46EB56A 857166C3 B9FD71DF 7264F5AF DC804A67 16BD35A2 4F39AFD7
 0BD24F71 BAF916AC E984343C A54B7395 E5D15237 8897D436 A150BFB2 DC23E8D3
 AFF0A51C B6253153 C4E2C022 66F1E361 B2EE49E2 763FCBC7 6381E7F7 61B6E14D
 60CDF947 2C044617 37211E5F CE
     quit
username <REMOVED> privilege 15 password 7 <REMOVED>
class-map match-all class Voice0 match
ip dscp cs3
class-map match-all _class_Voice1 match
ip dscp af41
class-map match-all class Voice2 match
ip dscp cs4
class-map match-all class Voice3 match
ip dscp ef
policy-map Voice
class_class_Voice0
set cos 4
```

```
class_class_Voice1
 set cos 5
class class Voice2
 set cos 5
class class Voice3
 set cos 6
policy-map Data
class class-default
set cos 0
!
bridge irb
interface Dot11Radio0
no ip address
shutdown
antenna gain 0
traffic-metrics aggregate-report
stbc
mbssid
speed basic-12.0 18.0 24.0 36.0 48.0 54.0 m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m14. m15.
m16. m17. m18. m19. m20. m21. m22. m23.
power client local
channel 2412
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
!
encryption vlan 2 mode ciphers aes-ccm
encryption vlan 3 mode ciphers aes-ccm
ssid data
ssid voice
۱
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 gos class voice local
  admission-control
  admit-traffic narrowband max-channel 75 roam-channel 6
!
```

```
dot11 gos class voice cell
  admission-control
!
world-mode dot11d country-code US both
interface Dot11Radio1.2
encapsulation dot1O 2
bridge-group 2
bridge-group 2 subscriber-loop-control
bridge-group 2 spanning-disabled
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
service-policy input Data
service-policy output Data
!
interface Dot11Radio1.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 subscriber-loop-control
bridge-group 3 spanning-disabled
bridge-group 3 block-unknown-source
no bridge-group 3 source-learning
no bridge-group 3 unicast-flooding
service-policy input Voice
!
interface Dot11Radio1.10
encapsulation dot1Q 10 native
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0.2
encapsulation dot1Q 2
bridge-group 2
bridge-group 2 spanning-disabled
no bridge-group 2 source-learning
service-policy input Data
service-policy output Data
!
interface GigabitEthernet0.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 spanning-disabled
no bridge-group 3 source-learning
service-policy input Voice
!
interface GigabitEthernet0.10
encapsulation dot1Q 10 native
```

```
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
mac-address 18e7.281b.3f54
ip address 10.9.0.9 255.255.255.0
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ip default-gateway 10.9.0.2
ip forward-protocol nd
no ip http server
ip http authentication aaa ip
http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
radius-server local
 nas 10.9.0.9 key 7 <REMOVED>
 user wds nthash 7 <REMOVED>
!
radius-server attribute 32 include-in-access-req format %h
radius server 10.0.0.20
address ipv4 10.0.0.20 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
radius server 10.9.0.9
address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
access-list 111 permit tcp any any neq telnet
bridge 1 route ip
١
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 04
access-class 111 in
transport input all
!
sntp server 10.0.0.2
sntp broadcast client
end
```

Cisco Meraki アクセスポイント

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

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

ワイヤレス ネットワークの作成

Cisco Meraki アクセス ポイントを追加して WLAN サービスを提供する前に、ワイヤレス ネットワークを作成する必要があります。ドロップダウンメニューから

[新規ネットワークの作成 (Create a new network)]を選択します。

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

'uluulu cisco Meraki	Q Search Dashboard
NETWORK	Create network
Meraki MX64 🛛 👻	
	Setup network
Network-wide	Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization.
Security & SD-WAN	Network name Scranton Branch Office
Organization	
	Network type Wireless - 0
	Network configuration O Default Meraki configuration
	Bind to template No templates to bind to ①
	Clone from existing network Select a 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?

Clos	e 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。

ululu cisco Meraki	Q Search Dashboard		
NETWORK	Inventory		
Meraki WLAN 👻	View used and unused devices in your organization. Yo	ou can <u>claim</u> new devices to add the list below.	
	Add to Unclaim Unused Used Both Search i	inventory	
Network-wide	S Existing network	Model A Claimed on	
	Meraki WLAN v	MR53 4/29/2020 2:59 PM	
Wireless	O New network		
Organization	Add to existing		

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。

ululu cisco Meraki	Q Search Dashboard			
NETWORK	Add access point	ts		
Meraki WLAN 👻	Add access points from your organization's inventory. When you claim an order by order number, the devices in the order will be added to your inventory. When you claim a device by its serial number, that			
	device will be added to your	inventory. Once in your inventory,	you can add dev	ices to your network(s).
Network-wide	Search inventory			
Wireless	MAC address	Serial number	Model *	Claimed on
	✓ 88:15:44:60:18:8c	Q2MD-MWQS-J9K7	MR53	4/29/2020 2:59 PM
Organization				
	Add access points			

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。

cisco Meraki	Q Search Dashboard		
NETWORK	Configuration overvie	W	
Meraki WLAN 👻	SSIDs Showi	ng 4 of 15 SSIDs. Show all my SSIDs.	
		meraki-voice	
	Enabled	enabled	
Network-wide	Name	rename	
Wireless	Access control	edit settings	
	Encryption	802.1X with Meraki RADIUS	
	Sign-on method	None	
Organization	Bandwidth limit	unlimited	
	Client IP assignment	Local LAN	
	Clients blocked from using LAN	no	
	Wired clients are part of Wi-Fi n	no 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。

ululu cisco Meraki	Q Search Dashboard	
NETWORK Meraki WLAN 👻	Access control	D
Network-wide Wireless	Network access Association requirements	Open (no encryption) Any user can associate
Organization		 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 C 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。

cisco Meraki	Q Search Dashboard				
	User management p	oortal			
Meraki WLAN 👻	SSID: meraki-voice	with Meraki authentication. The	ese 802.1X accounts are r	managed separately from Administrator	or Guest accounts.
	Authorization - Remove Users	Search			
Network-wide	Description	Email (Username)	Account type	Authorized for SSID *	Authorized by
			(P	Save Changes or <u>cancel</u>	ct)
		Create upor	U.	lease show it 2 minutes for changes to take end	
		Account type: Mera	aki 802.1X		
		Description:			
		Email (Username):			
		Password:	Ge	enerate	
		Authorized: No	9		
				Close Print Cre	ate user

[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。<u>https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf</u>

Cisco IOS スイッチを使用する場合は、Cisco Meraki アクセス ポイントが接続するスイッチ ポートを次のように構成して、802.1q トランキングを有効にします。

Interface GigabitEthernet X switchport trunk encapsulation dot1q switchport mode trunk mls qos trust dscp

ululu usco Meraki	Addressing and traffic			
NETWORK Meraki WLAN	Client IP assignment	 NAT mode: Use Meraki DHCP Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the <u>SSID firewall settings</u> permit. Pridge mode: Make clients part of the LAN 		
Network-wide	Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the L use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras Layer 3 roaming Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client roams to an AP where the original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This a the client to keep the same IP address, even when traversing IP subnet boundaries.			
Wireless				
Organization	VI AN Associate	 Layer 3 roaming with a concentrator Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs. VPN: tunnel data to a concentrator Meraki devices send traffic over a secure tunnel to an MX concentrator. 		
	VLAN tagging III Bridge mode and layer 3 roaming only	Use VLAN tagging 🗾		
	VLAN ID	AP tags VLAN ID Actions All other APs 3 Add VLAN		
	Content filtering NAT mode only	Don't filter content 0		
	Bonjour forwarding Bridge mode and layer 3 reaming only	Enable Bonjour Gateway		
	country only	There are no Bonjour forwarding rules on this network. Add a Bonjour forwarding rule		

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

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

[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 and	d minimum bitrate settings may be overridden by RF profiles. Go to RF Profiles	
Band selection	O 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 Dual band operation with Band Steering Band Steering detects clients canable of 5 GHz exercision and steers them to that frequency, while leaving 	it.
	for legacy clients.	ing 2.4 Gi iz available
Minimum bitrate (Mbps)	Lower Density	Higher Density
	1 2 5.5 6 9 11 12 18 24 26 802.11b devices not supported	48 54
	Band selection and Band selection Minimum bitrate (Mbps)	Band selection and minimum bitrate settings may be overridden by RF profiles. Go to RF Profiles Band selection Dual band operation (2.4 GHz and 5 GHz) S GHz bash only 5 GHz bash only S GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using Dual band operation with Band Steering Band selection Unimum bitrate (Mbps) Lower Density 1 Lower Density 1 1 1 2 1

[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。

cisco Meraki	Q Search Dashboard		
NETWORK	SSID availability		
Meraki WLAN 👻	SSID: meraki-voice	0	
	Visibility	Advertise this SSID publicly	
Network-wide	Per-AP availability ①	This SSID is enabled on all APs	
Wireless			
Organization			

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5GHzまたは2.4GHz

無線のいずれかに、チャンネルと送信電力を静的に設定できます。これは、エリアに断続的な干渉源が存在する場合に必要になることがあります。一方で、他のアクセスポイントで[自動(Auto)] を有効にし、静的チャンネルが割り当てられているチャンネルを回避できます。

ululu cisco Meraki	Q Search Da	shboard						
	Radio se	ettings						
Meraki WLAN 👻	Overview	RF profiles						
	BAND	CHANN	IEL	AP TAG	RF PROFILE	REGULATORY DOMA	N	
Network-wide	5	✓ All	*	MR53 *	All	FCC Edit		
Wireless	Search by AP	name				Upda	te auto channels	Edit settings +
Organization								
	Status 🛈	AP name 🛦	Channel	Ch. Width (MHz)	Target power (dBm)	Transmit power (dBm) ()	RF Profile	×
		MR53	36 (Auto)	20	8 - 30	8	Basic Indoor	Profile

標準の [基本屋内プロファイル (Basic Indoor Profile)]を変更するか、[バンド選択 (Band selection)]を [SSID ごと (Per SSID)]に設定し、[クライアントバランシング (Client balancing)]を [オフ (Off)]に設定して新しい RF プロファイルを作成することをお勧めします。

cisco [°] Meraki	3 Search Dashboard	
NETWORK	RF PROFILES	
Moroki M/LAN	Edit Basic Indoor Profile	
	General 2.4 GHZ 5 GHZ	
Network-wide	General	
Wireless	Band selection Per AP Per SSID	
Organization		
	date. Minimum bitrate configuration Per band Set the minimum bitrates for the 2 Per SSID The Access Points configured to u bitrate selection set on the Access SSID minimum bitrate selection will Client balancing Client Balancing uses information about client to the best available access points	4 & 5 GHz radios separately below. se this profile will follow the minimum <u>Control page</u> for the respective SSID. Per be moved to RF profiles at a later date. the state of the network and wireless client probes to steer the during association. Bead more about client belonging berg

RF プロファイルでは、5 GHz 無線の [チャネル幅(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ネル幅を使用することを推奨します。

```
[自動チャネル(AutoChannel)] で使用される 5 GHz チャネルも RF プロファイルで設定できます。
[自動チャネル(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。
```

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

[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。

ululu cisco Meraki	General 2.4 GHz 5 GHz	
NETWORK	5 GHz radio settings	
Meraki WLAN 🗸	Turn off 5GHz radio	See band selection above.
Network-wide	Channel width	Auto Manual
Wireless		Manual 5 GHz channel width
Organization		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.
		O 40 MHz (10 channels)
		For low to medium density deployments.
		0 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	Transmit shorter distance Transmit farther
	(asm)	O
		2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
	Set RX-SOP	
	Minimum bitrate	Lower Density Higher Density
		6 9 12 18 24 36 48 54

ululu Meraki	General 2.	4 GHz	5 GHz		_												
		Chang	e 5 GHz c	hannels u	used by A	utoChann	el										×
NETWORK	5 GHz radi	Auglish	la abaunala da	- AutoOhou	and a												
Meraki WLAN +	Turn off 5GHz	If you de	e channels ro select a chan	nel, AutoCha	annel will no	t assign it to	any AP with	this profile.	Click d	on a channel t	o toggle its	selection.					
	Channel width		UN	II-1	UN	1-2	UNII-2-Exte	nded		Weath	ier Radar					UNII-3	ISM
Network-wide	_	20 MHz	36 40	44 48	52 56	60 64	100 10	4 108	112	116 120	124	128 132	136	140 144	149 153	3 157 161	165
Wireless		40 MHz	38	46	54	62	102	11)	118	126		134	142	151	159	-1
Organization		80 MHz	42		5	8		106		8	122		1	138		155	
organization							1	OFS channels	D	eselect DFS	channels						
																Cancel	Done
		_	-	For low to	medium d	ensity depl	oyments.	-		-	-	-	-	-	-	_	_
				80 MHz (5	channels)												
				For low de bandwidth problems.	ensity area: n and data	s with few o rates for m	or zero neig odern devic	hboring ni es. Increa	etwork ses ri:	cs. Higher sk of interfe	rence						

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。

cisco Meraki	Q Search Dashboard							
NETWORK	Firewall & traffic s	shaping						
Meraki WLAN 👻	SSID: meraki-voice	0						
Network-wide	Block IPs and ports Layer 2 LAN isolation	Disabled 😮 (brid	dge mode	only)				
Wireless	Layer 3 firewall rules 0	# Policy	Protocol	Destination	Port	Comment	Actions	
Organization		Allow C Allow Add a layer 3 fire	Any Any ewall rule	Local LAN Any	Any Any	Wireless clients accessing LAN Default rule		
	Block applications and content categories Layer 7 firewall rules There are no rules defined for this SSID. Add a layer 7 firewall rule							
	Traffic shaping rules Per-client bandwidth limit	unlimited	details	Enable Sp	beedBu	st		
	Per-SSID bandwidth limit	unlimited	details					
	Shape traffic	Shape traffic on thi	s SSID	0				

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 Webex Control Hub		
G Overview	C Add Device	×
MONITORING	Assign to a user or a workspace?	
♡ Organization Health	Devices for personal usage should be assigned to a specific user. A workspace represents a physical location co owned by a specific user, such as a meeting room with a Webex Board 55 or a reception with a shared phone.	ntaining a device not
nalytics		
MANAGEMENT	Ω	
요 Users		
Ø Workspaces		
Devices	Existing User Workspace	
88 Apps	Personal Usage Shared Usage	
🛅 Account		
Ø Organization Settings	Multiple Cisco IP Phones: To bulk activate devices, Import/Upload CSV file.	
SERVICES		
O Messaging		
Meeting		
% Calling		
O Hybrid		Cancel

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 Webex Control Hub		
C Overview	Add Device	×
Controller -		
MONITORING	Which user will this device belong to?	
♡ Organization Health	Fearch for a user	
analytics		
->- Troubleshooting		
MANAGEMENT		
요 Users		
◊ Workspaces		
Devices		
B: Apps		
🗎 Account		
Organization Settings		
SERVICES		
○ Messaging		
Meeting		
% Calling		
Hybrid	Back	Next

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。

Cisco Webex Control Hub		
C Overview	Add Device Assign to a user or a workspace?	×
 ⊘ Organization Health ☑ Analytics ✓ Troubleshooting 	Devices for personal usage should be assigned to a specific user. A workspace represents a physical location containing a device not owned by a specific user, such as a meeting room with a Webex Board 55 or a reception with a shared phone.	
MANAGEMENT	\mathcal{A}	e
Workspaces		
Devices Apps	Existing User Workspace Personal Usage Shared Usage	
 Account Organization Settings 	Multiple Cisco IP Phones: To bulk activate devices, Import/Upload CSV file.	
SERVICES		
Meeting Calling		
 Hybrid 	Cancel Next	

[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。

Control Hub		
ର Overview	C Add Device	×
MONITORING	Assign to an existing workspace or a new workspace?	
♡ Organization Health	Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace	e.
nalytics	in you add mantple devices in a workspace that are not designed to work together, it may create interference issues.	
	0 c	
MANAGEMENT		6
A Users		
 Workspaces 	Existing Workspace	
Bo Apps		
Account	Which Warkspace will the device be assigned to?	
Urganization Settings	Workspace containing devices that are not Cisco IP Phones will not be shown, since you can only have one of these devices in a	
SERVICES	workspace.	
○ Messaging	Search for a Workspace	
Meeting		
% Calling		
🛆 Hybrid		
	Back Net	t
Cieco Webey	Back Nez	đ
Cisco Webex Control Hub	Back	d)
Cisco Webex Control Hub	Back Net C Add Device	tt 🔪
Cisco Webex Control Hub	Back Net Add Device Assign to an existing workspace or a new workspace?	rt X
Cisco Webex Control Hub	Back Net C Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace for an event work together it may create interference issues	e.
Cisco Webex Control Hub	Back Ner Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace If you add multiple devices in a workspace that are not designed to work together, it may create interference issues.	e.
Cisco Webex Control Hub Control Hub Control Hub Control Hub Control Hub Monitroring Control Hub Monitroring	Back Net C Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. 0 c	e.
Cisco Webex Control Hub Overview MONITORING Organization Health Analytics Troubleshooting	Back Ne	× e.
Cisco Webex Control Hub Control Hub Control Hub Control Hub Control Hub Monitroning Control Health Analytics Troubleshooting MANAGEMENT Control Hub Control Hub Co	Back Net	× e.
Cisco Webex Control Hub Control Hub Control Hub Correction MANNTORING Correction Correction Management Analytics Correction Management Correction Corr	Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace if you add multiple devices in a workspace that are not designed to work together, it may create interference issues.	e.
Cisco Webex Control Hub	Back Net C Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. O c Existing Workspace Existing Workspace New Workspace	x e.
Cisco Webex Control Hub Control Hub Control Hub Control Hub Monitroning Corganization Health Analytics Troubleshooting MANAGEMENT Users Vorkspaces Devices R Apps	Back Net C Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. O c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. D c Image: Compa	e.
Cisco Webex Control Hub Control Hub Overview MONITORING Organization Health Analytics Troubleshooting MANAGEMENT Users Workspaces Devices S Apps Th Account	Back Net C Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace if you add multiple devices in a workspace that are not designed to work together, it may create interference issues. Or Image: Comparison of the previous code has been lost or has expired, or to have multiple devices in a workspace if you add multiple devices in a workspace that are not designed to work together, it may create interference issues. Or Image: Comparison of the previous code has been lost or has expired, or to have multiple devices in a workspace if you add multiple devices in a workspace that are not designed to work together, it may create interference issues. Or Image: Comparison of the previous code has been lost or has expired, or to have multiple devices in a workspace if you add multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Comparison of the previous code has been lost or have multiple devices in a workspace issue. Image: Comparison of the previous code has been lost or have multiple devices in a workspace issue. Image: Comparison of the previous code has been lost or have multiple devices in a workspace issue. Image: Comparison of the previous code has been lost or have multiple devices in a workspace issue. Image: Comparison of the previous code has been lost or have multiple devices in a workspace issue. Image: Comparison o	e,
Cisco Webex Control Hub Overview MONITORING Organization Health Analytics Troubleshooting MANAGEMENT Surs Workspaces O Workspaces Devices Stapps Apps Account O Organization Settings	Back Add Device Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace if you add multiple devices in a workspace that are not designed to work together, it may create interference issues. Existing Workspace Existing Workspace Mew Workspace Mew Workspace	e.
Cisco Webex Control Hub Control Hub MONITORING Organization Health Analytics Troubleshooting MANAGEMENT Users Workspaces Devices Apps Account Organization Settings SERWICES	Image: Control of the control of th	e.
Cisco Webex Control Hub Overview MONITORING Organization Health Analytics Troubleshooting MANAGEMENT A Users Workspaces Devices B Apps Account Organization Settings SERVICES	Image: Constraints of the previous code has been lost or has expired, or to have multiple devices in a workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Constraint of the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Constraint of the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Constraint of the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Constraint of the previous code has been lost or has expired, or to have multiple devices in a workspace that previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint of the previous code has been lost or has expired. Image: Constraint o	× e.
Cisco Webex Control Hub Control Hub Control Hub Control Hub MONTORING Conganization Health Analytics Conganization Health Analytics Conganization Settings Conganization Settings Conganiza	Back Add Device Assign to an existing workspace or a new workspace? Stet Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Comparison of the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Comparison of the previous code has been lost or have multiple devices in a workspace that are not designed to work together, it may create interference issues. Image: Comparison of the previous code has been lost or have multiple devices in a workspace that this device will be assigned to? Image: Comparison of the previous code has been lost or have multiple devices in a workspace that this device will be assigned to? Image: Comparison of the previous code lost of the previous code have the previous code have the previous code have to be lost or "boot" or "bot"	x .
Cisco Webex Control Hub Control Hub Control Hub Control Hub Control Hub Control Hub Control Hub Control Health Analytics Control Health Analytics Control Health Control Health C	Image: Control Image: Contret Image:	e.

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。

Cisco Webex Control Hub	_			
	C	Add De What kind of device do you want to set up in this	evice workspace?	×
 ◇ Organization Health ▲ Analytics → Troubleshooting MANAGEMENT ▲ Users ◊ Workspaces ➡ Devices 	0 c	Cisco Webex Rooms device e.g. Cisco Webex Board, Room, and Desk series, and Webex Share.	Cisco IP Phone e.g. Cisco 8845, 8865, 8800 and Analog Telephone Adapter ports	
 8 Apps Account Organization Settings 				
SERVICES Messaging Meeting Calling Hybrid			Back Next	

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 Webex Control Hub					
Overview Monitoring Overview	C [Which services are r	Add Device needed in this Workspace?		×
 ✓ Organization nearth Manalytics 	0 c	℅ Calling	 Free Calling (default) Cisco Webex Calling Free Calling features with additional PSTN service provided through Webex. 		
MANAGEMENT		៉ Calendar	Calendar service enables One Button To Push for this Workspace.		
Devices Apps Account					
SERVICES					
Calling				Back	Next

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 サーバーの Communications Manager Cisco Unified Operating Administration Web System ページからインストールする必要があります。

デバイスパッケージの COP ファイルのインストール後に、各 Cisco Unified Communication Manager ノードを再起動する必要がない場合があります。

Cisco Unified Communications Manager のバージョンに応じて、次を実行します。

11.5(1)SU4 以降

• すべての Cisco Unified Communications Manager ノードをリブートします。

11.5(1)SU5 以降または 12.5(1) 以降

- すべての Cisco Unified Communications Manager ノードで Cisco Tomcat サービスを再起動します。
- パブリッシャノードで Cisco CallManager
- サービスを実行している場合は、パブリッシャノードでのみサービスを再起動します。

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

COP ファイルのインストール方法については、次の URL にある『Cisco Unified Communications Manager 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/productsmaintenance-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			
Context Context Device is trusted MAC Address *			
Description			
Device Pool*	Not Selected	÷) <u>V</u> i	iew Details
Common Device Configuration	< None >	\$ <u>V</u> i	iew 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 Mar	ager Group*	Default	•
Calling Search Space for Auto-regi	stration	< None >	0
Adjunct CSS		< None >	٥
Reverted Call Focus Priority		Default	٥
Intercompany Media Services Enro	lled Group	< None >	٥
-Roaming Sensitive Settings			
Date/Time Group*	CMLocal		٥
Region*	Default		0
Media Resource Group List	< None >		0
Location	< None >		0
Network Locale	< None >		0
SRST Reference*	Disable		0
Connection Monitor Duration ***			
Single Button Barge*	Default		0
Join Across Lines*	Default		0
Physical Location	< None >		0
Device Mobility Group	< None >		0
Wireless LAN Profile Group	< None >		View Details
	S HONG &		×

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。

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

Phone Button Templa	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。

Packet Capture Mode*	None	٢	
Packet Capture Duration	0		
BLF Presence Group*	Standard Presence group	٢	
MTP Preferred Originating Codec*	711ulaw	٥	
Device Security Profile*	Cisco Webex Desk Pro - Standard SIP Non-Secure	٢	
Rerouting Calling Search Space	< None >	٢	
SUBSCRIBE Calling Search Space	< None >	٢	
SIP Profile*	Standard SIP Profile	0	View Details
Digest User	< None >	٢	
Media Termination Point Require	red		
Unattended Port			
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 Prof	ile Information					
Product Type: Device Protocol:	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	8				
Transport Type*	TCP+UDP	•				
Enable Digest Auth	entication					
TFTP Encrypted Co	nfig					
Exclude Digest Cre	dentials in Configuration File					
Phone Security Prof	ile CAPF Information					
Authentication Mode*	By Null String	•				
Key Order*	RSA Only	0				
RSA Key Size (Bits)*	2048	0				
EC Key Size (Bits)	< None >	\$				
Note: These fields are	related to the CAPF Information settings on the Phon	e 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)。

Packet Capture Mode*	None	٥	
Packet Capture Duration	0		
BLF Presence Group*	Standard Presence group	0	
MTP Preferred Originating Codec*	711ulaw	¢	
Device Security Profile*	Cisco Webex Desk Pro - Standard SIP Non-Secure	0	
Rerouting Calling Search Space	< None >	0	
SUBSCRIBE Calling Search Space	< None >	0	
SIP Profile*	Custom Webex Desk Pro SIP Profile	0	View Details
Digest User	< None >	0	
Media Termination Point Require	red		
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

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

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 (imer 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

ame* 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*	ar Calls* Disabled				
Jser-Agent and Server header information * Send Unified CM Version Information as User-Ager 🜖					
Version in User Agent and Server Header*	User Agent and Server Header* Major And Minor 😌				
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, an 😌				
Confidential Access Level Headers *	Disabled	0			
Redirect by Application					
Disable Early Media on 180					
Outgoing T.38 INVITE include audio mline	3				
Offer valid IP and Send/Receive mode on	y for T.38 Fax Relay				
Use Fully Qualified Domain Name in SIP F	lequests				
Assured Services SIP conformance					
Enable External QoS**					
SDP Information					
SDP Session-level Bandwidth Modifier for E	arly Offer and Re-invites *	TIAS and AS	0		
SDP Transparency Profile Pass all unknown SDP attributes					
Accept Audio Codec Preferences in Received	l Offer*	Default	8		
Require SDP Inactive Exchange for Mid-	Call Media Change				
Allow RR/RS bandwidth modifier (RFC 3	556)				
Deve meters used in Dhene					
Parameters used in Phone					
Timer Inuite Evaluate (coconde)*					
Timer Invite Expires (seconds)*	180				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)*	180 30				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)*	190 30 3600				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)* Timer T1 (msec)*	180 30 3600 500				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)* Timer T1 (msec)* Timer T2 (msec)*	180 30 3600 500 4000				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)* Timer T1 (msec)* Timer T2 (msec)* Retry INVITE*	180 30 3600 500 4000 6				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)* Timer T1 (msec)* Timer T2 (msec)* Retry INVITE* Retry Non-INVITE*	180 30 3600 500 4000 6 10				
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)* Timer T1 (msec)* Timer T2 (msec)* Retry INVITE* Retry Non-INVITE* Media Port Ranges	180 30 3600 500 4000 6 10 • Common Port Range f	or Audio and Video			
Timer Invite Expires (seconds)* Timer Register Delta (seconds)* Timer Register Expires (seconds)* Timer T1 (msec)* Timer T2 (msec)* Retry INVITE* Retry Non-INVITE* Media Port Ranges	180 30 3600 500 4000 6 10 • Common Port Range f • Separate Port Ranges	or Audio and Video for Audio and Video			

DSCP for Audio Callis Use System Default DSCP for Video Callis Use System Default DSCP for Audio Portion of Video Callis Use System Default DSCP for Audio Portion of Video Callis Use System Default DSCP for Audio Portion of TelePresence Callis Use System Default Call Pickup Group UR1* x-clsco-serviceurl-ipickup Meet Me Service UR1* x-clsco-serviceurl-imeetme User Info* None DTMF DB Level* Nominal Call Hold Ring Back* Off Off Level for 7940 and 7960* Disabled Disabled Soo Timer Keep Alive Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15 Seeni Altended Transfer S	Stop Media Port*	32766	
DSCP for Video Calls Use System Default DSCP for Audio Portion of Video Calls Use System Default DSCP for Audio Portion of TelePresence Calls Use System Default DSCP for Audio Portion of TelePresence Calls Use System Default DSCP for Audio Portion of TelePresence Calls Use System Default Call Pickup UR1* x-cisco-serviceuri-pickup Call Pickup Group UR1* x-cisco-serviceuri-opickup Meet Me Service UR1* x-cisco-serviceuri-meetme User Info* None DTMF DB Level* Nominal Call Hold Ring Back* Off Call Hold Ring Back* Off O for Off 0 D Not Disturb Control* User Disabled 0 Caller fully Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 15 Maxim Redirections* 70 Off Hold Nor Instruct (milliseconds)* 15000 Call Forward UR1* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) UR1* x-cisco-serviceuri-	DSCP for Audio Calls	Use System Default	
DSCP for Audio Portion of Video Calls Use System Default Image: Call State System Default Image: Call System Default System Default Image: Call System Default <td>DSCP for Video Calls</td> <td>Use System Default</td> <td></td>	DSCP for Video Calls	Use System Default	
DSCP for TelePresence Calls Use System Default G DSCP for Audio Portion of TelePresence Calls Use System Default G Call Pickup Group Other URI* x-cisco-serviceurl-opickup G Call Pickup Group URI* x-cisco-serviceurl-opickup G Call Pickup Group URI* x-cisco-serviceurl-opickup G Meet Me Service URI* x-cisco-serviceurl-opickup G User Info* None G Call Hold Ring Back* Orf G Call Hold Ring Back* Orf G Caller ID Blocking* Orf G Do Not Disturb Control* User G Telnet Level for 7940 and 7960* Disabled G Resource Priority Namespace < None > G Timer Subscribe Expires (seconds)* 300 G Timer Subscribe Delta (seconds)* 15 G Maximum Redirections* 70 G Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceurl-oftwall Seed Dial (Abbreviated Dial) URI* x-cisco-serviceurl-oftwall Suctor Mathide Transfer Senviceurl-abbrdial Gali Attended Transfer Siturt Message Walting UH2P User Authorization Script None	DSCP for Audio Portion of Video Calls	Use System Default	
DSCP for Audio Portion of TelePresence Calls Use System Default Image: System Default <	DSCP for TelePresence Calls	Use System Default	•
Call Pickup URI* x-cisco-serviceuri-pickup Call Pickup Group Other URI* x-cisco-serviceuri-opickup Call Pickup Group URI* x-cisco-serviceuri-apickup Meet Me Service URI* x-cisco-serviceuri-meetme User Info* None DTMF DB Level* Nominal Call Hold Ring Back* Off Caller DB Bickvig* Calle Caller Off Caller DB Bickvig* Caller Caller Caller DB Control* Caller Caller DB Control* Caller Caller DB Control* Caller Caller DB Control* Caller Caller Caller DB Control* Caller Caller Caller Caller Caller Caller DB Control* Caller C	DSCP for Audio Portion of TelePresence Calls	Use System Default	•
Call Pickup Group Other URI * x-cisco-serviceuri-opickup Call Pickup Group URI * x-cisco-serviceuri-meetme User Info* None DTMF DB Level * Nominal Call Hold Ring Back * Off Caller ID Bickving* Off Caller Catron Caller ID Bickving* Catron Caller Catron Caller ID Catron	Call Pickup URI*	x-cisco-serviceuri-pickup	
Call Pickup Group URI *cisco-serviceuri-gpickup Meet Me Service URI *cisco-serviceuri-meetme User Info * None © DTMF DB Level * Nominal © Call Hold Ring Back * Off © Caller ID Biocking * Off © Caller ID Biocking * Off © D Not Disturb Control * User © Telnet Level for 7940 and 7960 * Disabled © Resource Priority Namespace < None > © Timer Keep Alive Expires (seconds) * 300 Timer Subscribe Expires (seconds) * 15 Maximum Redirections * 70 Off Hook To First Digit Timer (milliseconds) * 15000 Call Forward URI *cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI *cisco-serviceuri-abbrdial © Conference Join Enabled ■ RFC 2543 Hold © Smithtended Transfer = Enable VAD © Stutter Message Waiting MLPP User Authorization	Call Pickup Group Other URI*	x-cisco-serviceuri-opickup	
Meet Me Service URI* x-cisco-serviceuri-meetme User Info* None DTMF DB Level* Nominal Call Hold Ring Back* Off Caller ID Blocking* Off Caller ID Blocking* Off D Not Disturb Control* User Do Not Disturb Control* User Telnet Level for 7940 and 7960* Disabled Resource Priority Namespace < None > Timer Keep Allve Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-abbrdial Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Conference Join Enabled - Semi Attended Transfer - Is Semi Attended Transfer - Is Subit VAD - Stutter Message Waiting - MLPP User Authorization K-cisco-serviceuri-abbrdial Normalization Script	Call Pickup Group URI*	x-clsco-serviceuri-gpickup	
User Info* None DTMF DB Level* Nominal Call Hold Ring Back* Off Gall Hold Ring Back* Off Caller ID Blocking* Off Caller ID Blocking* Off D Not Disturb Control* User Do Not Disturb Control* User Telnet Level for 7940 and 7960* Disabled Resource Priority Namespace < None > Timer Keep Alive Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 300 Timer Subscribe Delta (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Conference Join Enabled - RFC 2543 Hold Semi Attended Transfer Inasfer -	Meet Me Service URI*	x-cisco-serviceuri-meetme	
DTMF DB Level* Nominal G Call Hold Ring Back* Off G Anonymous Call Block* Off G Caller ID Blocking* Off G Do Not Disturb Control* User G Do Not Disturb Control* User G Telnet Level for 7940 and 7960* Disabled G Resource Priority Namespace < None > G Timer Keep Alive Expires (seconds)* 300 G Timer Subscribe Expires (seconds)* 300 G Timer Subscribe Expires (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* IS000 Gall Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Z Conference Join Enabled @ RFC 2543 Hold G Semi Attended Transfer Enable VAD @ Stutter Message Waiting Lever Authorization Korept MLPP User Authorization Korept G	User Info*	None	
Call Hold Ring Back* Off Off Off Caller ID Blocking* Off Off Caller ID Blocking* Off Off Off Caller ID Blocking* Off Off Off Off Off Off Off Off Off Of	DTMF DB Level*	Nominal	
Anonymous Call Block * Off Off Off Off Off Off Off Off Off Of	Call Hold Ring Back*	Off	
Caller ID Blocking* Off Off Off Off Off Off Off Off Off Of	Anonymous Call Block*	Off	
Do Not Disturb Control* User Telnet Level for 7940 and 7960* Disabled Resource Priority Namespace < None > Timer Keep Alive Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 300 Timer Subscribe Delta (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization	Caller ID Blocking*	Off	
Telnet Level for 7940 and 7960* Disabled Image: Second Se	Do Not Disturb Control*	User	
Resource Priority Namespace < None > Timer Keep Alive Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 300 Timer Subscribe Delta (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization	Telnet Level for 7940 and 7960*	Disabled	•
Timer Keep Alive Expires (seconds)* 300 Timer Subscribe Expires (seconds)* 300 Timer Subscribe Delta (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization	Resource Priority Namespace	< None >	•
Timer Subscribe Expires (seconds)* 300 Timer Subscribe Delta (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial C Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script	Timer Keep Alive Expires (seconds)*	300	
Timer Subscribe Delta (seconds)* 15 Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceurl-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceurl-abbrdial © Conference Join Enabled © RFC 2543 Hold © Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization	Timer Subscribe Expires (seconds)*	300	
Maximum Redirections* 70 Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Image: Conference Join Enabled x-cisco-serviceuri-abb	Timer Subscribe Delta (seconds)*	15	
Off Hook To First Digit Timer (milliseconds)* 15000 Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Image: Conference Join Enabled RFC 2543 Hold Image: Semi Attended Transfer Enable VAD Stutter Message Walting MLPP User Authorization Normalization Script Normalization Script None >	Maximum Redirections*	70	
Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script Normalization Script Normalization Script Conference Join Enable Conference Join Enabled Conference Join Enable Conference Join	Off Hook To First Digit Timer (milliseconds)*	15000	
Speed Dial (Abbreviated Dial) URI* Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script Normalization Script Normalization Script Normalization Script Semi Attended Transfer Contemport	Call Forward URI*	x-cisco-serviceuri-cfwdall	
Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Walting MLPP User Authorization Normalization Script Normalization Script Conference Semi Attended Semi Atten	Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial	
RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script Normalization Script	Conference Join Enabled		
Semi Attended Transfer Enable VAD Stutter Message Walting MLPP User Authorization Normalization Script Normalization Script S	RFC 2543 Hold		
Enable VAD Stutter Message Walting MLPP User Authorization Normalization Script Normalization Script < None >	Semi Attended Transfer		
Stutter Message Walting MLPP User Authorization Normalization Script Normalization Script Nonmalization Script	Enable VAD		
MLPP User Authorization Normalization Script Normalization Script Normalization Script None >	Stutter Message Waiting		
Normalization Script	MLPP User Authorization		
Normalization Script < None >	Normalization Script		
	Normalization Script < None >	• • • • • • • • • • • • • • • • • • •	

Enable Trace		Barameter Value	
1			
Incoming Requests FROM URI Settings			
Caller ID DN	1		
Caller Name			
runk Specific Configuration			
Reroute Incoming Request to new Trunk based on	* Never		
tesource Priority Namespace List	< None >		
SIP Rel1XX Options*	Disabled		
/ideo Call Traffic Class*	Mixed		
Calling Line Identification Presentation*	Default		
Session Refresh Method *	Invite		
Early Offer support for voice and video calls*	Disabled (Default	value)	
Enable ANAT			
Deliver Conference Bridge Identifier			
Allow Passthrough of Configured Line Device C	aller 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 (De	fault)"
Ping Interval for In-service and Partially In-servi	ce Trunks (seconds)*	60	
Ping Interval for Out-of-service Trunks (seconds)*	120	
Ping Retry Timer (milliseconds)*		500	
Ping Retry Count*		6	
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。

- Enterprise Parameters Configuration		
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)	ᅌ 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	• 64 kbps (G.722, G.711)	C Keep Current Setting	• Keep Current Setting Use System Default
	kbps	Use System Default None 2000 kbps	None 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	オーディオ
コーデック	ビット レート

AAC-LD	$128\sim 256~{ m Kbps}$
Opus	$6\sim510~{ m Kbps}$
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 × 180	30	最大 128 Kbps
CIF 288p	512 x 288	30	129 \sim 256 Kbps
nHD 360p	640 x 360	30	$257\sim 384~{ m Kbps}$
SD 448p	768 x 448	30	$385\sim512~{ m Kbps}$
WSVGA 576p	1024 X 576	30	513 \sim 768 Kbps
HD 720p	1280 X 720	30	769 \sim 1472 Kbps
FHD 1080p	1920 X 1080	30	1473 \sim 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	0	
SSH Access*	Disabled	0	
Default Call Protocol*	SIP	0	
Quality Improvement Server			
Multipoint Mode*	Use Endpoint	0	
Telnet Access*	Off	0	
Microphone Unmute On Disconned	ct* On	0	
Call Logging Mode*	On	0	
OSD Encryption Indicator*	Auto	0	
Alternate phone book server type	* UDS	0	
Alternate phone book server addr	ess		
Default Volume	70		
Max Total Downstream Rate	15000		
Max Total Upstream Rate	10000		
Load Server			
WiFi Allowed*	On	0	
System Name			
Wake-up On Motion Detection*	On	0	
Custom Message			
Settings Menu Mode*	Unlocked	0	
Accessibility Call Notification*	Default	0	
Configuration Control Mode*	Unified CM and Endpoint	0	
Webex Devices Onboarding Token	1		
Easy Webex join*	Auto	0	
Far End Camera Control Setti	ngs		
Far End Camera Control*	On		0
Far End Camera Control Signalir	ng Capability* On		
Facility Service Settings			
Facility Service Type* Hel	pdesk	•	
Facility Service Name			
Facility Service Number			
Facility Service Call Type* Vide	eo	0	

Standby Settings				
Standby Mode* On		3		
Standby Delay 10				
Serial Port Settings				
Serial Port*			-	
Serial Port Login Required*	1			
Serial Port Login Required Of	1			
Admin username and passwo	ord			
Admin Username				
Admin Password				
Proximity				
Proximity Mode*	On			8
Call Control*	Disab	led		8
Proximity Content Share From C	lients* Disab	led		0
Proximity Content Share To Clie	nts* Disab	led		8
LDAP User Management				
LDAP Mode*	Off		6	
LDAP Server Address				
LDAP Server Port	0			
LDAR Attribute	U			
LDAP AUTIONE				
LDAP Base DN				
LDAP Encryption*	LDAPS		0	
LDAP Minimum TLS Version*	TLSv1.2		0	
LDAP Verify Server Certificate*	Off			
LDAP Admin Filter				
LDAP Admin Group				
Customization Provisioning				
Customization File				
Customization Hash Type* SH	A512		0	
Customization Hash				
SMTP Provisioning				
SMTP Mode* Off		0		
SMTP Server				
SMTP Port 0				
SMTP Security type* None		0		
SMTP Username				
SMTP Password				
SMTP From address			_	

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

OSD 暗号化インジケータ	暗号化インジケータ(鍵)が画面に表示される時間の長さを定義します 。この設定は、暗号化されたコールと暗号化されていないコール、つま りセキュアな会議と非セキュアな会議の両方に適用されます。暗号化さ れたコールはロックされた鍵のアイコンで示され、暗号化されていない コールはバツ印の付いたロックされた鍵のアイコンで示されます。 [自動(Auto)]: Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されている場合、暗号化インジケータがコ ールの最初の数秒間に表示されます。Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されていない場合、バツ印の付いた暗号化 インジケータがコール全体にわたり表示されます。Conference Encryption Mode 設定が BestEffort に設定されていない場合、暗号化インジケータはまったく表示されませ ん。AlwaysOn:暗号化インジケータはコール全体にわたり画面上に表示 されます。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用さ れます。
代替電話帳サーバのタイプ(Altern ate phone book server type)	デフォルトで、エンドポイントは登録先の UCM 上の UDS サーバーを使用しますが、代替電話帳サーバーの使用を希望する場合は 、このパラメータを代替電話帳のアドレスと組み合わせて、エンドポイ ントのデフォルト設定をオーバーライドします。 UDS は代替電話帳タイプを UDS に設定し、TMS はタイプを TMS に設定します。
代替電話帳サーバのアドレス(Alt ernate phone book server address)	デフォルトで、エンドポイントは登録先の UCM 上の UDS サーバを使用しますが、代替電話帳サーバーの使用を希望する場合は、こ のパラメータを代替電話帳のタイプと組み合わせて、
	エンドポイントのデフォルト設定を上書きします。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
デフォルトのボリューム	値は0から100の間で指定できます。1~100の値は-34.5 dB~15 dB(0.5 dB刻み)の範囲に対応します。値0 は、音声がオフになっていることを意味します。
ダウンストリーム速度合計の最大 値	この構成は、許可される全体の最大受信ビットレートを指定します。ビ ットレートは任意の時点におけるすべてのアクティブコール間で均等に 分割されます。値スペースの範囲は 64 ~ 10000 です。
アップストリーム速度合計の最大 値	この構成は、許可される全体の最大送信ビットレートを指定します。ビ ットレートは任意の時点におけるすべてのアクティブコール間で均等に 分割されます。値スペースの範囲は 64 ~ 10000 です。
ロードサーバ (Load Server)	デバイスのファームウェアを含む代替サーバーのアドレス。フルパスと ポートを指定してください。例: http://example.com/firmware
Wi-Fi が許可されています	エンドポイントで Wi-Fi の有効化を許可するかどうかを示す設定。
システム名 (System Name)	システムの名前。デバイスのホスト名として使用できます。

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

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、LD AP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(「Us erManagement 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、UserM anagement 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 サーバに接続します (暗号化なし)。STARTTLS:ポート 389 上の LDAP サーバに接続します。
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。UserManageme nt 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)

?	Parameter Value		Pull xConfig. from d
Note: Endpoints runn	ing software versions earlier than CE 9.	8 only support provisioning a limited set of p	arameters from Cisco Unified CN
se parameters are me	ncated below with the # symbol.		
Audio	General Settings		
Bluetooth	DefaultVolume	50	#
	Microphones Mute Enabled*	True	~
BYOD	Ultrasound MaxVolume	70	
CallHistory	-Toput-		
Cameras	HDMI 1		
	Level	0	
Conference	Mode*	On	~
FacilityService	MicrophoneMode*	Focused	~
	USBC 1		
HttpClient	Level	0	
HttpFeedback	Mode*	On	~
Logging	SoundsAndAlerts		
	RingTone	Sunrise	
Macros	RingVolume	50	
NetworkServices			
Phonebook	KeyClickDetector		
FIIOHEDOOK	Enabled*	True	~
RoomAnalytics	Attenuate*	True	~

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

<u>音声</u>

- General Settings		
DefaultVolume	50	#
Microphones Mute Enabled*	True 🗸	
Ultrasound MaxVolume	70	
Input		
HDMI 1		
Level	0	
Mode*	0n 🗸	
MicrophoneMode*	Focused V	
USBC 1		
Level	0	
Mode*	0n v	
SoundsAndAlerts		
RingTone	Sunrise	
RingVolume	50	
- KeyClickDetector		
Enabled*	True	
Attenuate*	True 🗸	

<u>Bluetooth</u>

General Settings		
Allowed*	True	v
Enabled*	False	v

<u>BYOD</u>

General Settings			
HidForwarding Enabled*	False	~	
TouchForwarding Enabled*	True	~	

通話履歴

General S	ettings		
Mode*		On	✓ #

<u>カメラ</u>

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

<u>会議</u>

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

ファシリティサービス

Service 1		
CallType*	Video	*
Name	Live Support	#
Number		#
Type*	Helpdesk	*
Service 2		
CallType*	Video	v
Name		
Number		
Type*	Helpdesk	<u>`</u>
Service 3		
CallType*	Video	v
Name		
Number		
Type*	Helpdesk	▼
Service 4		
CallType*	Video	~
Name		
Number		
Туре*	Helpdesk	v
Service 5		
CallType*	Video	~
Name		
Number		
Туре*	Helpdesk	v

<u>HTTP クライアント</u>

General Settings		
Mode*	Off	~
AllowInsecureHTTPS*	False	~
AllowHTTP*	True	~
UseHttpProxy*	On	v

<u>НТТР フィードバック</u>

deneral sectings		
TIsVerify*	On v	
UseHttpProxy*	On v	

ロギング

- General Settings			
General Settings			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External			
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	~	
Server			
Address			
Port	514		
Port	514		

<u>マクロ</u>

┌ General Settings				
	AutoStart*	On	•	
	Mode*	Off	•	
	UnresponsiveTimeout	5		

<u>ネットワーク サービス</u>
General Settings	
H323 Mode*	Off v
UPnP Mode*	On v
Websocket*	Off v
WelcomeText*	On v
Wifi Allowed*	True
Mode*	Off v
Proxy	
Mode*	Off v
Url	
LoginName	
Password	
PACUrl	
HTTPS	
VerifyClientCertificate*	Off v
StrictTransportSecurity*	Off v
Server	
MinimumTLSVersion*	TLSv1.1 v
SNMP	
CommunityName	
Mode*	Off
SystemContact	
SystemLocation	
-,	
SSH	
HostKeyAlgorithm*	RSA V
Mode*	Off v
Mode*	Off ✓ v ¢
Server	#
Port	0 #
Security*	StartTis v *
Username	#
Password	#
From	#

<u>電話帳(Phone Book)</u>

Server 1		
ID		
Туре*	CUCM	*
URL		*
Pagination*	Enabled	~
TIsVerify*	On	~

<u>Room 分析</u>

General Settings		
PeopleCountOutOfCall*	Off	~
PeoplePresenceDetector*	Off	v
AmbientNoiseEstimation		
Mode*	Off	v
Interval	10	

ルームスケジューラ

General Settings		
Enabled*	False v)

<u>SIP</u>

General Seconds			
MinimumTLSVersion*	TLSv1.0	v	

セキュリティ

Audit	
Logging Mode*	Internal v
OnError	
Action*	Ignore v
Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off v
Session	
InactivityTimeout	0
ShowLastLogon*	Off v
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

<u>シリアルポート</u>

General Settings		
BaudRate*	115200	~
LoginRequired*	On	*
Mode*	On	v)#

<u>スタンバイ</u>

General Settings		
BootAction*	RestoreCameraPosition	~
Control*	On	~]#
Delay	10	
StandbyAction*	PrivacyPosition	~]*
WakeupAction*	RestoreCameraPosition	~
WakeupOnMotionDetection*	On	v]#

Signage		
Url		
Mode*	Off	~
InteractionMode*	NonInteractive	~
RefreshInterval	0	
Audio*	Off	~

システム ユニット

General Settings	
Name	*
CrashReporting	
Mode*	Off
	*
UNL	^m

ユーザインターフェイス



周辺機器

General Settings			
InputDevice Mode*	Off	v	
Pairing CiscoTouchPanels	On	v	
RemotePairing*			
Profile			
TouchPanels*	0	~	
Cameras*	0	v	
ControlSystems*	NotSet	~	

<u>プロキシミティ</u>

General Settings			
Mode*	Off	✓ *	
Services			
ContentShare			
ToClients*	Disabled	*	
FromClients*	Enabled	*	
CallControl*	Disabled	v)#	

<u>ユーザー管理</u>

LDAP	
Mode*	Off v
Encryption*	LDAPS V
VerifyServerCertificate*	Off v)#
BaseDN	#
Attribute	*
MinimumTLSVersion*	TLSv1.2 v
Server	
Address	di d
Port	0
Admin	
Admin	w
Group	ð
Filter	jë i
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*	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*	Auto	~	
Resolution*	3840_2160_60	~	
Connector 2	(T.)		
MonitorRole*	Auto	v	
RGBQuantizationRange*	Full	~	
Resolution*	Auto	▼	
Location			
HorizontalOffset	1		
VerticalOffset	0		
CEC			
Mode*	On	v	
Presentation			
DefaultSource*	2	~	
Priority*	Equal	~	
- Selfview			
Default			
FullscreenMode*	Current	~	
Mode*	Current	~	
OnMonitorRole*	Current	~	
PIPPosition*	Current	~	
OnCall			
Duration	10		
Mode*	On	~	

音声管理

General Settings			
Wakeword Mode*	On	v	

<u>Web エンジン</u>

General Settings		
Mode*	Off	~
RemoteDebugging*	Off	~
UseHttpProxy*	On	~

<u>Webex</u>

General Settings		
CloudProximity Mode*	Off v)

ルームクリーンアップ

AutoRun		
HourOfDay	0	
ContentType		
Whiteboards*	Daily	~
WebData*	Daily	v

<u>ブッキング</u>

General Settings		
ProtocolPriority*	Auto 🗸	

<u>その他</u>

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 v
Customization Hash	¢

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

Product Specific Confi	guration Layout		
?	Parameter Value		Pull xConfig. from device
il-Note: Endpoints runn These parameters are inc	ing software versions earlier than CE dicated below with the # symbol.	9.8 only support provisioning a limited set of pa	arameters from Cisco Unified CM.
Audio	General Settings		
	DefaultVolume	50	#
Bluetooth	Ultrasound MaxVolume	70	
BYOD	USB Mode*	SpeakerAndMicrophone	~
CallHistory	_ Input		
Cameras	HDMI 1		
Conference	Level	0	
	Mode*	On	~
FacilityService	MicrophoneMode*	Focused	~
HttpClient	USBC 1		
· · · · · · · · · · · · · · · · · · ·	Level	0	
HttpFeedback	Mode	Oh	`
Logging	Microphones		
Macros	Mute		
NetworkServices	Enabled *	True	~
Phonebook	NoiseRemoval	Manual	
RoomAnalytics	Mode	manuai	
RoomScheduler	SoundsAndAlerts	(Constant	
	RingTone	Sunrise	
	kingvolume	50	
Security	KeyClickDetector		
SerialPort	Enabled*	False	~
Standby	Attenuate*	True	~
SystemUnit			
UserInterface			
Peripherals			
Proximity			
UserManagement			
Video			
VoiceControl			
WebEngine			
Webex			
RoomCleanup			
Bookings			
Miscellaneous			

<u>音声</u>

General Settings	
DefaultVolume	50 #
Ultrasound MaxVolume	70
USB Mode*	SpeakerAndMicrophone v
HDMI 1	
Level	0
Mode*	On v
MicrophoneMode*	Focused v
USBC 1	
Level	0
Mode*	On v
Mute	
Enabled*	True v
NoiseRemoval	
Mode*	Manual
SoundsAndAlerts	
RingTone	Sunrise
RingVolume	50
KeyClickDetector	
Enabled*	False v
Attenuate*	True v

<u>Bluetooth</u>

General Settings			
Allowed*	True	~	
Enabled*	False	~	

BYOD

1	- General Settings-				
	HidForwarding Enabled*	False	v		
		Taise			
	TouchForwarding Enabled*	True	~		

通話履歴

General Settings		
General Settings		
Modo [*]	0.0	. 0
Houe		
		_

<u>カメラ</u>

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

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

0

On

<u>会議</u>

Level

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

v)#

ファシリティサービス

SignalCapability*

Service 1		
CallType*	Video	✓ [¢]
Name	Live Support	*
Number		*
Туре*	Helpdesk	*
Service 2		
CallType*	Video	v
Name		
Number		
Type*	Helpdesk	¥
Service 3		
CallType*	Video	v
Name		
Number		
Type*	Helpdesk	v
Service 4		
CallType*	Video	×
Name		
Number		
Type*	Helpdesk	¥
Service 5		
CallType*	Video	v
Name		
Number		
Type*	Helpdesk	v

<u>HTTP クライアント</u>

General Settings			
Mode*	Off	~	
AllowInsecureHTTPS*	False	~	
AllowHTTP*	True	~	
UseHttpProxy*	On	~	

<u>HTTP フィードバック</u>

On	~	
On	~	
	On On	On v On v

<u>ロギング</u>

General Settings			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External]
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	~	
Server			
Address			
Port	514		

<u>マクロ</u>

- General Settings			
AutoStart*	On v		
Mode*	Off v		
UnresponsiveTimeout	5]	

<u>ネットワーク サービス</u>

General Settings				
H323 Mode*	Off v			
UPnP Mode*	On v			
Websocket*	Off v			
WelcomeText*	On v			
Wifi Allowed*	True			
Mode*	Off v			
Proxy				
Mode*	Off v			
Url				
LoginName				
Password				
PACUrl				
HTTPS				
VerifyClientCertificate*	Off v			
StrictTransportSecurity*	Off v			
Server				
MinimumTLSVersion*	TLSv1.1 v			
SNMP				
CommunityName				
Mode*	Off			
SystemContact				
SystemLocation				
-,				
SSH				
HostKeyAlgorithm*	RSA V			
Mode*	Off v			
Mode*	Off ✓ v ¢			
Server	#			
Port	0 #			
Security*	StartTis v *			
Username	#			
Password	#			
From	#			

<u>電話帳(Phone Book)</u>

Server 1	
ID	
Type*	CUCM v
URL	<i>k</i>
Pagination*	Enabled V
TIsVerify*	On v

<u>Room 分析</u>

General Settings		
PeopleCountOutOfCall*	Off	~
PeoplePresenceDetector*	Off	~
AmbientNoiseEstimation		
Mode*	Off	~
Interval	10	

ルームスケジューラ

General Settings		
Enabled*	False v)

<u>SIP</u>

-General Settings			
MinimumTLSVersion*	TLSv1.0	v	

セキュリティ

Audit		
Logging Mode*	Internal	
OnError		
Action*	Ignore v	
Server		
Address		
Port	514	
PortAssignment*	Auto	
Fips Mode*	Off v	
Session		
InactivityTimeout	0	
ShowLastLogon*	Off v	
MaxTotalSessions	20	
MaySectionsBerlicer	20	
MaxSessionsPeroser		
MaxFailedLogins	0	

シリアルポート

General Settings			
BaudRate*	115200	~	
LoginRequired*	On	*	
Mode*	On	*	

<u>スタンバイ</u>

General Settings		
BootAction*	RestoreCameraPosition	~
Control*	On	~ *
Delay	10	
StandbyAction*	PrivacyPosition	v]*
WakeupAction*	RestoreCameraPosition	~
WakeupOnMotionDetection*	On	~)≉

Signage		
Url		
Mode*	Off	~
InteractionMode*	NonInteractive	~
RefreshInterval	0	
Audio*	Off	~

システム ユニット

#
Off
n

<u>ユーザ インターフェイス</u>

一般設定			
Ao:i;ssibIIIty Inc{ImIngCalINotItIca1	on [D@la_ult	" <u>"</u>	
予約 可視性タイトル連絡先情	[自動	<u> </u>	
報 タイプ* 診断通知	[自動]	<u>v</u> j	
ブランディング.ブランディング	[自動	<u> </u>	
C<>I{Irs	#	<u> </u>	
K@ylonliis the F	 [<u>白動</u>		
SouridlE'ff&ts モード@*	<u>1</u>		
f>mKImIty ollficationsカスタ	<u>[才</u>	V	
ムメッセージ		it	
ホワイトボード	$\underline{ \lambda \rangle},$		
ActlvltyIndIcators AssIsta ril	<u>\</u> ,		
	[通常]	<u> </u>	
機配			
すべて非表示*	[偽	V	
コール (Call)			
開始*	[自動	1	
MiclCallu:,ntrols;;i	[自動	<u> </u>	
終了*	[自動]		
JolnW@b©:	「自動		
キーパッド	[自動]		
通信モード・	[非表示		
開始	[自動]		
ホワイトボード	白色	, <u> </u>	
用如			
OSD			
暗号化インジケーター	[自動]		
出力		V	
ハーフ ウェイク メッセージ			
モード	[自動	V	
			I
チード		77	
デフォルトの検索		C	
/ / 4/11 */15年			
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	v	
Pairing CiscoTouchPanels	On	v	
RemotePairing*			
- Profile			
TouchPapels*	0	×	
		•	
Cameras*	0	×	
ControlSystems*	NotSet	v	

<u>プロキシミティ</u>

General Settings	
Mode*	Off ~ *
AlternatePort Enabled*	False v
Services	
ContentShare	
ToClients*	Disabled v#
FromClients*	Enabled v #
CallControl*	Disabled v #
	_

<u>ユーザー管理</u>

LDAP	
Mode*	Off v
Encryption*	LDAPS V
VerifyServerCertificate*	Off v
BaseDN	#
Attribute	#
MinimumTLSVersion*	TLSv1.2 *
Server	
Address	Ø
Port	0 Ø
Admin	
Group	ø
Filter	ů.
PasswordPolicy	
ReuseLimit	12
MaxLifetime	0
Complexity	
MinimumLength	8
MinimumUppercase	0
MinimumLowercase	0
MinimumDigits	0
MinimumSpecial	0

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

Connector 1	
Deinhan seabhada *	
Auto	
Resolution* 3840_2160_60	v
Connector 2	
MonitorRole*	v
RGBQuantizationRange* Full	~
Resolution* Auto	v
Location	
HorizontalOffset 1	
VerticalOffset 0	
CEC	
Mode* On	~
- Presentation	
DefaultSource*	×]
_ Selfview	
Default	
FullscreenMode* Current	v
Mode* Current	~
OnMonitorRole* Current	~
PIPPosition* Current	v
OnCall	
Duration 10	

音声管理

General Settings		
Wakeword Mode*	On v	

<u>Web エンジン</u>

General Settings	
Mode*	Off ~
RemoteDebugging*	Off ~
UseHttpProxy*	On ~
MinimumTLSVersion*	TLSv1.1 ~

<u>Webex</u>

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	~	

<u>ブッキング</u>

General Settings		
ProtocolPriority*	Auto v	

<u>その他</u>

General Settings		
ocherar bettingb		
Configuration Control Mode*	Unified CM and Endpoint	
Room Name (from Exchange(R))		#
LoadServer		#
Webex Devices Onboarding Token		#
- Admin username and password		
Admin username and password		
Admin Username	admin	#
Admin Password		#
Customization Provisioning		
		#
Customization File		, w
Customization Hash Type*	SHA512 v	
Customization Hash		#

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

bauct Specific Con	figuration Layout		
?	Parameter Value		Pull xConfig. from devi
-Note: Endpoints rur ese parameters are i	nning software versions earlier than CE indicated below with the # symbol. —	9.8 only support provisioning a limited set of	parameters from Cisco Unified CM.
Audio	General Settings		
Rhisteath	DefaultVolume	50	#
Bluetooth	Input MicrophoneMode*	Focused	~
CallHistory	Ultrasound MaxVolume	70	
Cameras	USB Mode*	SpeakerAndMicrophone	~
Conference			
acility Service	Mute		
achicyService	Enabled *	True	~
HttpClient	NoiseRemoval		
HttpFeedback	Mode*	Manual	~
Logging	SoundsAndAlerts		
Macros	RingTone	Sunrise	
	RingVolume	50	
SIP Security SerialPort Standby SystemUnit			
Peripherals			
Proximity			
UserManagement			
/ideo			
/oiceControl			
WebEngine			
Webex			
RoomCleanup			
Bookings			
-			
Miscellansous			

<u>音声</u>

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

<u>Bluetooth</u>

General Settings			
Allowed*	True	~	
Enabled*	False	~	

通話履歴

General Settings	
Mode*	0n v)#

<u>カメラ</u>

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



DefaultCall	
Protocol*	Sip v#
Rate	6000
DoNotDisturb DefaultTimeout	60
Encryption Mode*	BestEffort v
FarendMessage Mode*	Off v
MaxReceiveCallRate	6000
MaxTotalReceiveCallRate	6000 #
MaxTotalTransmitCallRate	6000 <i>#</i>
MaxTransmitCallRate	6000
MicUnmuteOnDisconnect Mode*	On ~ #
Multipoint Mode*	Auto 🗸 🖌
FarEndControl	
Mode*	On v #
SignalCapability *	On v #

<u>ファシリティサービス</u>

Service 1		
CallType*	Video	✓ [#]
Name	Live Support	#
Number		#
Type*	Helpdesk	*
Service 2		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v
Service 3		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v
Service 4		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v
Service 5		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v

<u>HTTP クライアント</u>

General Settings		
Mode*	Off	v
AllowInsecureHTTPS*	False	~
AllowHTTP*	True	~
UseHttpProxy*	On	~

<u>НТТР フィードバック</u>

deneral sectings		
TIsVerify*	On v	
UseHttpProxy*	On v	

<u>ロギング</u>

- General Settings			
j -			
CloudUpload Mode*	Off	~	
Internal Mode*	On	v	
External			
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	×	
Server			
Address			
Port	514		

<u>マクロ</u>

General Settings			
AutoStart*	On	•	
Mode*	Off	•	
UnresponsiveTimeout	5		

<u>ネットワーク サービス</u>

General Settings	
H323 Mode*	Off v
UPnP Mode*	On v
Websocket*	FollowHTTPService V
WelcomeText*	On v
Wifi Allowed*	True v
Mode*	(Off ✓)#
Proxy	
Mode*	Off v
Url	
LoginName	
PACUrl	
VerifyClientCertificate*	Off v
StrictTransportSecurity*	Off v
Server	
MinimumTLSVersion*	TLSv1.1 v
SNMP	
CommunityName	
Mode*	Off
SystemContact	
SystemLocation	
_ssh	
HostKeyAlgorithm*	RSA V
Mode*	Off v
SMTP	
Mode*	Off v #
Server	······································
Port	"
Security*	StartTie
Username	startis *
From	"
	ſ

<u>電話帳(Phone Book)</u>

Server 1	
ID	
Type*	CUCM v
URL	#
Pagination*	Enabled v
TIsVerify*	On v

<u>Room 分析</u>

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

- General Settings		
deneral bettings		
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	~	

<u>SIP</u>

General Settings		
MinimumTLSVersion*	TLSv1.0 v	

セキュリティ

Audit	
Logging	
Mode*	Internal v
OnError	
Action*	Ignore v
Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off v
Session	
InactivityTimeout	0
ShowLastLogon*	Off v
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

<u>シリアルポート</u>

General Settings		
BaudRate*	115200	~
LoginRequired*	On	✓)#
Mode*	On	v #

<u>スタンバイ</u>

General Settings		
BootAction*	DefaultCameraPosition	~
Control*	On	~ #
Delay	10	#
StandbyAction*	PrivacyPosition	~ #
WakeupAction*	RestoreCameraPosition	~
WakeupOnMotionDetection*	Off	✓ #

Url		
Mode*	Off	~
RefreshInterval	0	
Audio*	Off	~

システム ユニット

General Settings	
CustomDeviceId	
Name	#
CrashReporting	
Mode*	Off v
URL	#

<u>ユーザ インターフェイス</u>

General Settings		
Accessibility IncomingCallNotification	Default	
*	Verault	
Bookings Visibility Title*	Auto	
ContactInfo Type*	Auto	
Diagnostics Notifications*	Auto	
Branding AwakeBranding Colors*	Auto v	
KeyTones Mode*	On •	
SoundEffects Mode*	On •	
Proximity Notifications*	Auto 🗸	
CustomMessage		#
Whiteboard ActivityIndicators*	On v	
Assistant Mode*	On v	
Security Mode*	Normal	
Features		
HideAll*	False v	
Call		
Start*	Auto 🗸	
MidCallControls*	Auto v	
End*	Auto 🗸	
VideoMute*	Auto 🗸	
JoinWebex*	Auto	#
Keypad*	Auto	
MusicMode*	Hidden v	
Share		
Start*	Auto	
Whiteboard		
Start*	Auto	
- OSD		
EncryptionIndicator*	Auto v	
Output*	1	
HalfwakeMessage		
Mode*	Auto	
- Phonebook		
Mode*	ReadWrite	
DefaultSearchFilter*	All v	
SattingeManu		
secongsment		
Mode *	Uniocked	
Visibility*	Auto v	

周辺機器

General Settings			
InputDevice Mode*	Off	~	
Pairing CiscoTouchPanels RemotePairing*	On	~	
Profile			
TouchPanels*	0	~	
Cameras*	Minimum1	v	
ControlSystems*	NotSet	~	

プロキシミティ

Off v# False v
Disabled v #
Enabled v#
Disabled v *

<u>ユーザー管理</u>

LDAF		
Mode*	Off v	
Encryption*	LDAPS v	
VerifyServerCertificate*	Off v	
BaseDN	[]	¢
Attribute	[]	¢
MinimumTLSVersion*	TLSv1.2 v	
Server		
Address		ŧ
Port	0	ŧ.
Admin		
Group		ð.
Filter		ð.
- PasswordPolicy		
rassivolaroney		
ReuseLimit	12	
MaxLifetime	0	
Complexity		
MinimumLength	8	
MinimumUppercase	0	
MinimumLowercase	0	
MinimumDigits	0	
MinimumSpecial	0	

<u>ビデオ</u>

Connector 1		
InputSourceType *	camera	~
Name	Camera	
Visibility*	Never	~
CameraControl		
CameraId*	1	~
Mode*	On	v)
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	v
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*	Ön	~
Monitors*	Auto	~
Output Connector 1 Resolution*	1920_1080_60	~
DefaultMainSource*	1	~

2	~	
Equal	~	
Current	~	
10		
Off	~	
	2 Equal Current Current Current Current 10 Off	2 v Equal v Current v Current v Current v Current v Off v

音声管理

General Settings			
Wakeword Mode*	On	~	

<u>Web エンジン</u>

General Settings			
Mode*	Off	~	
RemoteDebugging*	Off	~	
UseHttpProxy*	On	~	
MinimumTLSVersion*	TLSv1.1	~	

<u>Webex</u>

-General Settings			
General Settings			
Meetings JoinProtocol*	SIP	~	
CloudUpgrades Mode*	Off	~	
CloudProximity			
Mode*	Off	~	
GuestShare*	Auto	v	

<u>ルームクリーンアップ</u>

AutoRun			
HourOfDay	0		
ContentType			
Whiteboards*	Daily	~	
WebData *	Daily	~	
	<u> </u>		

<u>ブッキング</u>

General Settings		
ProtocolPriority*	Auto)

<u>その他</u>

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 v	
Customization Hash		ŧ.

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

Product Specific Con	figuration Layout		
?	Parameter Value		Pull xConfig. from device
I-Note: Endpoints run These parameters are in	nning software versions earlier than CE ndicated below with the # symbol.	9.8 only support provisioning a limited set of pa	arameters from Cisco Unified CM.
Audio	General Settings		
Bluetooth	DefaultVolume	50	#
	Input MicrophoneMode*	Focused	~
CallHistory	Ultrasound MaxVolume	70	
Cameras	USB Mode*	SpeakerAndMicrophone	~
Conference	Microphones		
FacilityService	Enabled *	True	~
HttpClient	NoiseRemoval		
HttpFeedback	Mode*	Manual	~
Logging	SoundsAndAlerts		
Macros	RingTone	Sunrise	
	RingVolume	50	
NetworkServices			

<u>音声</u>

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

<u>Bluetooth</u>

General Settings		
Allowed*	True	~
Enabled*	False	~

通話履歴

General Settings		
Mode *	On	* #

<u>カメラ</u>

Background		
Enabled*	True 🗸	
UserImagesAllowed*	True	
PowerLine Frequency*	Auto	
Camera		
Brightness		
DefaultLevel	20	
Mode*	Auto	
ExposureCompensation	-	
Level	0	
SpeakerTrack		
Mode*	Auto	
TrackingMode*		
	Auto 🗸	
Closeup *	Auto V	
Closeup * Whiteboard	Auto V Auto V	
Closeup* Whiteboard Mode*	Auto v Auto v	
Closeup* Whiteboard Mode*	Auto ~ Auto ~ Off ~	
Closeup* Whiteboard Mode* ConnectorDetection	Auto Auto Off	
Closeup* Whiteboard Mode* ConnectorDetection Mode*	Auto ~ Auto ~ Off ~ Auto ~	
Closeup* Whiteboard Mode* ConnectorDetection Mode* CameraRight	Auto Auto Off Auto Auto 2	

<u>会議</u>

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

<u>ファシリティサービス</u>

Service 1		
CallType*	Video	✓ #
Name	Live Support	#
Number		*
Туре*	Helpdesk	*
Service 2		
CallType*	Video	~
Name		
Number		
Туре*	Helpdesk	v
Service 3		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v
Service 4		
CallType*	Video	×
Name		
Number		
Туре*	Helpdesk	v
Service 5		
CallType*	Video	•
Name		
Number		
Type*	Helpdesk	v
<u>HTTP クライアント</u>

General Settings		
Mode*	Off	v
AllowInsecureHTTPS*	False	~
AllowHTTP*	True	v
UseHttpProxy*	On	~

<u>НТТР フィードバック</u>

General Settings			
TIsVerify*	On	~	
UseHttpProxy*	On	~	

ロギング

- General Settings			
General Settings			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External			
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	~	
Server			
Address			
Port	514		
Port	514		

マクロ

1	General Settings			
	2		_	
	AutoStart*	On	-	
	Mode*	Off	•	
	UnresponsiveTimeout	5		

<u>ネットワーク サービス</u>

General Settings	
H323 Mode*	Off v
UPnP Mode*	On v
Websocket*	FollowHTTPService V
WelcomeText*	On v
Wifi Allowed*	True v
Mode*	(Off ✓)#
Proxy	
Mode*	Off v
Url	
LoginName	
PACUrl	
VerifyClientCertificate*	Off v
StrictTransportSecurity*	Off v
Server	
MinimumTLSVersion*	TLSv1.1 v
SNMP	
CommunityName	
Mode*	Off
SystemContact	
SystemLocation	
_ssh	
HostKeyAlgorithm*	RSA V
Mode*	Off v
SMTP	
Mode*	Off v #
Server	······································
Port	"
Security*	StartTie
Username	startis *
From	"
	ſ

<u>電話帳(Phone Book)</u>

Server 1	
ID	
Type*	CUCM v
URL	#
Pagination*	Enabled v
TIsVerify*	On v

<u>Room 分析</u>

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

-General Settings		
General Settings		
PeopleCountOutOfCall*	Off	~
PeoplePresenceDetector*	Off	~
AmbientNoiseEstimation		
Mode*	Off	~
Interval	10	
ReverberationTime		
and the second sec	(
Mode*	Off	v
Interval	1800	

ルームスケジューラ

General Settings			
Enabled*	False	~	

<u>SIP</u>

General Settings		
MinimumTLSVersion*	TLSv1.0 v	

セキュリティ

Audit	
Logging	
Mode*	Internal v
OnError	
Action*	Ignore v
Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off v
Session	
InactivityTimeout	0
ShowLastLogon*	Off v
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

<u>シリアルポート</u>

General Settings		
BaudRate*	115200	~
LoginRequired*	On	✓)#
Mode*	On	v #

スタンバイ

General Settings		
BootAction*	DefaultCameraPosition	~
Control*	On	~ #
Delay	10	#
StandbyAction*	PrivacyPosition	~ #
WakeupAction *	RestoreCameraPosition	~
WakeupOnMotionDetection*	Off	✓ #

-Signage		
Url		
Mode*	Off	~
RefreshInterval	0	
Audio*	Off	~

システム ユニット

General Settings	
CustomDeviceId	
Name	#
CrashReporting	
Mode*	Off v
URL	#

<u>ユーザインターフェイス</u>

General Settings		
Accessibility IncomingCallNotification	Default	
*	Verault	
Bookings Visibility Title*	Auto	
ContactInfo Type*	Auto	
Diagnostics Notifications*	Auto	
Branding AwakeBranding Colors*	Auto v	
KeyTones Mode*	On •	
SoundEffects Mode*	On •	
Proximity Notifications*	Auto 🗸	
CustomMessage		#
Whiteboard ActivityIndicators*	On v	
Assistant Mode*	On v	
Security Mode*	Normal	
Features		
HideAll*	False v	
Call		
Start*	Auto 🗸	
MidCallControls*	Auto v	
End*	Auto 🗸	
VideoMute*	Auto 🗸	
JoinWebex*	Auto	#
Keypad*	Auto	
MusicMode*	Hidden v	
Share		
Start*	Auto	
Whiteboard		
Start*	Auto	
- OSD		
EncryptionIndicator*	Auto v	
Output*	1	
HalfwakeMessage		
Mode*	Auto	
- Phonebook		
Mode*	ReadWrite	
DefaultSearchFilter*	All v	
SattingeManu		
secongsment		
Mode *	Uniocked	
Visibility*	Auto v	

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* AlternatePort Enabled*	Off False	*
Services		
ContentShare		
ToClients*	Disabled	*
FromClients*	Enabled	*
CallControl*	Disabled	✓ #

<u>ユーザー管理</u>

Mode*	Off v
Encryption*	LDAPS v
VerifyServerCertificate*	Off v
BaseDN	#
Attribute	#
MinimumTLSVersion*	TLSv1.2 v
Server	
Address	<i>*</i>
Port	0 ø
Admin	
Group	ð
Filter	di d
- PasswordPolicy	
PasswordPolicy	
ReuseLimit	12
MaxLifetime	0
Complexity	
MinimumLength	8
MinimumUppercase	0
MinimumLowercase	0
MinimumDigits	0
MinimumSpecial	0

<u>ビデオ</u>

Connector 1		
InputSourceType*	camera	~
Name	Camera	
Visibility*	Never	v
CameraControl	-	
CameraId*	1	~
Mode *	On	v
Connector 2		
InputSourceType*	PC	v
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 st	1920_1080_60	×
DefaultMainSource*	1	~

Presentation DefaultSource* 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	~	

<u>Web エンジン</u>

General Settings

Mode*	Off	~
RemoteDebugging*	Off	~
UseHttpProxy*	On	~
MinimumTLSVersion*	TLSv1.1	~

<u>Webex</u>

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	~	

<u>ブッキング</u>

[General Settings		
	ProtocolPriority*	Auto 🗸)

<u>その他</u>

- General Settings		
et al bettings		
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 v	
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。

 $\underline{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}$

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。

Malaama
vveiconie
English English (United States)
Norwegian Norsk
German Deutsch
French Français (France)
Arabic
Start
← Use the old onboarding

- 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。

$\left(\leftarrow \right)$	Network connection Not Connected							
	((+	Wi-Fi	Not connected	>				
	*	Ethernet	Not connected	\geq				
	2	Network Status		>				
	×	Advanced Network Settings						
		Continue without netw	work					

<u>ブロードキャスト Wi-Fi ネットワークの設定</u>

 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。

(4)	Wi-	Fi
	 Not Cor Wi-Fi 	mected
	Networks	
	2wire421	
	7736475884	
	AdorableWiFi_5G	
	Akrietta ATTebBNC8s	8
	Join other network	

- 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。

	\leftarrow			Fata		psk									
				Enter	r the pa		ise for p	JSK	٥						
		r d								1	2 ABC 5	3 DEF 6			
<u>ک</u>					n			/ .com	Enter	GHI 7 PORS	JKL 8 TUV 0	9 WXYZ #			

- 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。

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

$\left(\leftarrow \right)$	eap		
	Security	Enterprise	
	Authentication method	PEAP	
	Anonymous identity (optional)		
	Username		
	Passphrase	۲	
(e)	eap		
(e)	eap Security	Enterprise	
(<-)	eap Security Authentication method	Enterprise EAP-FAST	
(e)	eap Security Authentication method Anonymous identity (optional)	Enterprise EAP-FAST >	
• • • • • • • • • • • • • • • • • • •	eap Security Authentication method Anonymous identity (optional) Jsername	Enterprise EAP-FAST >	
	eap Security Authentication method Anonymous identity (optional) Username Passphrase	Enterprise EAP-FAST >	
(c)	eap Security Authentication method Anonymous identity (optional) Username Passphrase	Enterprise EAP-FAST >	
	eap Security Authentication method Anonymous identity (optional) Username Passphrase	Enterprise EAP-FAST >	

(c)	eap	
	Security	Enterprise
	Authentication method	EAP-TTLS
	Anonymous identity (optional)	
	Username	
	Passphrase	۲

• 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。

$\left(\leftarrow \right)$	eap	ар				
Could not find	d any client certificates	lient certificates installed				
Security		Enterprise				
Authentication method		EAP-TLS				
Anonymous identity (opt	otional)					

<u>非ブロードキャスト Wi-Fi ネットワークの設定</u>

- 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。

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

\leftarrow	Wi-Fi Not Connected	Wi-Fi Not Connected					
	Wi-Fi						
	Networks						
	2wire421						
	7736475884						
	AdorableWiFi_5G						
	Akrietta						
	ATTebBNC8s						
	Join other network						

 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。

		\leftarrow			J	oin ot	her ne	twork								
			Netv	vork Na	me											
			Sec	urity					N	one >						
										\otimes		2 ABC	3 DEF			
			f	9	h						4 GHI	5 JKL	6 MNO			
	^									^	7 PQRS	8 TUV	9 WXYZ			
(Ŵ	.?123							.com	Enter						

 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。

(\			Jo	oin oth	er net	work								
	Netwo	ork Name	е											
	Secur	rity					Pers	onal >						
	Passp	ohrase						0)					
								$\langle X \rangle$		2 ABC	3 DEF			
									4 GHI	5 JKL	6 MNO			
								^	7 PQRS	8 TUV	9 wxyz			
.?123						0	.com	Enter	•					

- 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。

	(\leftarrow)					Joi	in othe	er net	work									
			N	letwork I	Name)						
			J	Security						Enterp	rise >							
			4	nonyma	ous Ide	ntity												
				Jsernam	е													
			F	assphra	se						0							
			A	Authentic	ation	Metho	d			Р	EAP							
											\otimes		2 ABC					
					9		j			ı .	-	4 GHI	5 JKL	6 MNO				
^					ь						^	7 PQRS	8 TUV	9 wxyz				
Ē	.?123	0							0	.com	Enter		0 •	#				

(Join other networ	ĸ		
	Network Name)	
	Security	Enterprise >		
	Anonymous Identity			
	Username			
	Passphrase			
	Authentication Method	EAP-FAST		
		° X	1 2 ABC	3 DEF
	f g h j k		4 5 GHI JKL	6 MNO
	c v b n m . @	.com Enter	PORS TUV	#
¢	Join other networ	×		
 (Join other network	X		
¢	Join other network Network Name Security	Enterprise >		
 Image: Construction 	Join other network Network Name Security Anonymous Identity	Enterprise]	
(c)	Join other network Network Name Security Anonymous Identity Username	Enterprise >)	
E	Join other network Network Name Security Anonymous Identity Username Passphrase	Enterprise >		
 Example 1 	Join other network Network Name Security Anonymous Identity Username Passphrase Authentication Method	Enterprise >		
(Contraction of the second se	Join other network Network Name Security Anonymous Identity Username Passphrase Authentication Method	Enterprise >		
(¢	Join other network Network Name Security Anonymous Identity Username Passphrase Authentication Method	Enterprise >		
¢ v	Join other network Network Name Security Anonymous Identity Username Passphrase Authentication Method Continue r t y i o	Enterprise > EAP-TTLS >	1 2 AGC	3 of
e a s d	Join other network Network Name Security Anonymous Identity Username Passphrase Authentication Method r t y u i o f g h j k	Enterprise > EAP-TTLS > I	1 2 ASC 4 5 04 5 .93	3 DPP 6 MMO

• 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。

$\left(\leftarrow \right)$	Join other netw	vork			
	Could not find any client cert	rtificates installed			
	Network Name				
	Security	Enterprise >			
	Anonymous Identity				
	Authentication Method	EAP-TLS			
		° P 🗙	1 2 ABC		
				6 MNO	
			7 8 PQRS TUV	9 wxyz	
.?123		@ .com Enter			
q w 8 s ~ z 1123	Network Name Security Anonymous Identity Authentication Method c r t g h d f g h x c v h m	Enterprise > EAP-TLS > EAP-TLS >	1 2 ABG 4 5 04 3 PORS 100 • 0	3 сег 6 Мию 9 WWYZ #	

<u>Wi-Fi ネットワークの詳細オプションの設定</u>

• **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。

Image: Wi-Fi transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status transformed Image: Status trans	(c)	Network C	onnection ected	
B Ethernet Not connected > Image: Continue Network Status > Image: Continue Continue >	(6	S Wi-Fi	xroads	>
Network Status > X Advanced Network Settings > Continue Continue	8	Ethernet	Not connected	>
Advanced Network Settings	E.	Network Status		>
Continue	*	Advanced Network Settin	ngs	
Continue				
Continue				
Continue				
		Conti	inue	

	(Advanced network	settings		
		IP Stack			
		IPv4 and IPv6			
		IPv4			
		IPv6			
		DNS			
		DNS Domain Name		l	
		DNS address 1			
		DNS address 2			
		DNIS addrose 3			
(
	÷	Advanced network s	ettings	Apply	
	(c)	Advanced network s	ettings	Арріу	
	(`	Advanced network s iNS Jomain Name INS address 1	ettings	Арріу	
	(e)	Advanced network s NNS Jomain Name NNS address 1 NNS address 2	ettings	Арріу	
	(c)	Advanced network s NVS JUOmain Name NVS address 1 IVNS address 2 IVNS address 3	ettings	Арріу	
	(←)	Advanced network s INS Joman Name INS address 1 INS address 3 INTP Proxy	ettings	Арріу	
		Advanced network s PNS uomain Name PNS address 1 PNS address 2 PNS address 3 ITTP Proxy	ettings	Арріу	
		Advanced network s MS Jomain Name MS address 1 MS address 2 MS address 3 ITTP Proxy Off Manual	ettings	Арріу	
		Advanced network s NVS Jomain Name NVS address 1 NVS address 2 NVS address 3 ITTP Proxy Off Aanual VPAD	ettings	Арріу	
		Advanced network s MVS Jomain Name MVS address 1 MVS address 2 MVS address 3 ITTP Proxy Off Manual VPAD	ettings	Apply	

(\		Advanced net	work settings		Apply		
	HTTP Proxy						
	Off						
	Manual			~			
						1	
	PAC URL		(1)			
	Proxy Port						
	Proxy server	requires authentic	cation				
		Reset all to	to default				
				$\langle X \rangle$		3	
					4 5	6	
					(3H) IK1		
		h j b n n	m . /	^	GHI JKL 7 8 PQRS TUV	MNO 9 WXYZ	
∠ z x	c v	h j	m . /	Enter	GHI JKL 7 8 PQRS TUV * 0	MNO 9 WXX72 #	
 2 x 2 x 2 2 x 2 x<td>a f g c v DNS address 1 DNS address 2 DNS address 3</td><td>h j</td><td>ork settings</td><td>Enter</td><td>Apply</td><td>мию 9 WVYZ #</td><td></td>	a f g c v DNS address 1 DNS address 2 DNS address 3	h j	ork settings	Enter	Apply	мию 9 WVYZ #	
 ∠ x 2 x 2.7123 	e e v c v DNS address 1 DNS address 2 DNS address 3 HTTP Proxy	h j	m . /	Enter	Apply	Minio 9 WXXYZ #	
× 2 × 2.7123	e e e e e e e e e e e e e e e e e e e	h j	m . /	Enter	Apply	мию 9 WVV7Z #	
 ∠ x ?123 	c v c v DNS address 1 DNS address 2 DNS address 3 HTTP Proxy Off Manual	h j	ork settings	Enter	Apply	мию 9 WVYZ #	
 ₹ x 2 x 3123 	i f g c v i c v i diamond i i DNS address 1 i DNS address 2 i DNS address 3 i HTTP Proxy Off Manual i WPAD i	h j	m · /	Enter	Apply	Minio 9 WrvrZ #	
× 2 × 2.7123	A g g g g g g g g g g g g g g g g g g g	h j	m . /	Enter	Apply	Mino 9 WVV7Z #	

\leftarrow	Advanced network settings Apply
	DNS address 2
	HTTP Proxy Off
	Manual
	PAC URL
	Reset all to default

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

 $\frac{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}{\laboration-endpoints/desktop-collaboration-experience-dx600-series/products-$

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。

Cisco Webex Local Device Controls	Q Find page ()
10.81.12.22 Desk Pro	Security
☆ Home	⊘ Certificates ∋ Sign-in Banner
℅ Call	Services Custom Preinstalled
SETUP	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 Browse No file selected. Private key Browse No file selected. (optional) Passphrase Uploate Uploate
SYSTEM MAINTENANCE	Existing Certificates
Software	Certificate Issuer 802.1X Audit HTTPS HttpClient HttpProxy SIP Pairing Actions
 Backup and Recovery 	Self-signed Certificate

EAP-TLS を利用するには、ユーザー証明書をインストールする必要があります。

必要に応じて、秘密キーを証明書と一緒にアップロードできま

す。証明書とキーを抽出するには、パスワードの入力が必要に

なる場合があります。

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

802.1X で有効にできるユーザー証明書は1つだけです。したがって、その証明書は EAP-TLS ユーザー証明書として自動的に使用され、追加の Wi-Fi プロファイルの構成は必要ありません。 ユーザ証明書を発行した CA チェーンが RADIUS サーバの信頼リストに追加されたことを確認します。

Cisco Webex Local Device Controls								QF	nd page		0	2
10.81.12.22 Desk Pro	Security Certificates ① Sign	-in Banner										
% Call	Services Custom Preinst	alled										
SETUP	Add Certificate Us Thi pri	e the form below to add new ce is system supports PEM formatt vate key with or without a passp Certificate Browse Private key Browse (optional) Passphrase (optional) Upload	rtificates. ed certificate hrase. Option No file select No file select	files (.pe ally the p ted. ted.	m). The o	certificate fil	e may contai	n the cer	tificate an	d a RSA or I	DSA encrypted	
SYSTEM MAINTENANCE	Existing Certificates											
Software • Issues and Diagnostics	Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	HttpProxy	SIP	Pairing	Actions		
Backup and Recovery	Self-signed Certificate	TemporaryDefaultCertificate								Delete	View Certificate	
	sep689e0bb0000d.cisco.com	Cisco Systems Inc.								Delete	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。

Cisco Webex Local Device Controls		Q Find page ⑦	8
10.81.12.22 Desk Pro	Security		
∩ Home	⊘ Certificates		
∿ Call	Services Custom Preinstalled		
SETUP	Add Certificate Authority Use the form below to add new certificate authorities. This system supports PEM formatted files (.pem) with one or more CA certificate authority Browse No file selected.	tificates within the file.	
CUSTOMIZATION	Existing Certificate Authorities		
UI Extensions Editor	Certificate Issuer Details Actions		
Macro Editor % Developer API	IdenTrust Commercial Root CA 1 IdenTrust View Delete		
SYSTEM MAINTENANCE			
G Software			
 Ssues and Diagnostics Backup and Recovery 			

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。

Cisco Webex Local Device Controls								Q Fli	nd page		0	8
10.81.12.22 Desk Pro	Security	i Danas										
G Home	Services Custom Preinsta	lled										
SETUP	Add Certificate Use	the form below to add new certi	ficates.									
은 Users	This priv	s system supports PEM formatted ate key with or without a passphr	certificate ase. Optio	files (.pe nally the	em). The oprivate ke	certificate file by file may be	e may contai e supplied se	n the cert eparately.	ificate an	d a RSA or	DSA encrypted	
合 Security		Certificate Browse N	o file selec	ted.								
CUSTOMIZATION		Private key Browse N	o file selec	ted.								
Personalization UI Extensions Editor Macro Editor X Developer API		Delete C This will delete certificate se fingerprint e9f86529ced9244	certificate p689e0bb0 c50b740c2	0000d.cls 025592e Can	co.com w afa95ed42 cel De	× ith t1 lete						
SYSTEM MAINTENANCE	Existing Certificates											
G Software	Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	HttpProxy	SIP	Pairing	Actions		
S Backup and Recovery	Self-signed Certificate	TemporaryDefaultCertificate								Delete	View Certificate	
	sep689e0bb0000d.clsco.com	Cisco Systems Inc.								Delete	View Certificate	

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。

Cisco Webex Local Device Controls			Q Find page	0	8
10.81.12.22 Desk Pro	Security				
(∩) Home	Certificates Sign-in I Services Custom Preinstaller	3anner			
Setup Settings A Users A Security	Add Certificate Use th Authority This sy Brow	form below to add new certificate authorities. stem supports PEM formatted files (.pem) with one or more CA certific rse) No file selected.	ates within the file.		
CUSTOMIZATION 전 Personalization	Existing Certificate Auth	Delete Certificate X This will delete certificate idenTrust Commercial Root CA 1			
Macro Editor More API	IdenTrust Commercial Root CA 1	with fingerprint df717eaa4ad94ec9558499602d48de5fbcf03a25 Cancel Delete			
SYSTEM MAINTENANCE					

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。

 $\underline{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}$

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、目的の呼制御システムを選択します。

Platform		
Cisco RoomOS Full RoomOS experience supporting a variety of meeting and collaboration apps.	Increase Rooms soft Teams Rooms clicco RoomOS features.	
Other options	Tegata	
← Advanced RoomOS so	etup	
← Advanced RoomOS so	etup >	
← Advanced RoomOS set 目 Cisco UCM Image: Cisco UCM via Expressway	etup > >	
Advanced RoomOS se	etup > >	
Advanced RoomOS set E Cisco UCM Cisco UCM via Expressway	ətup > >	

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。

← Activate this Cisco Desk Pro	
Enter your 16-digit Webex activation code	
Continue	

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。

← Register to Control Hub	
Enter your 16-digit Control Hub activation code. Contact your admin to get an activation code.	
() (8 () () () () () () () ()	
Skip Continue	

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。

	м	
Detected Cisco UCM servers	10.35.48.106	
Automatic configuration		
Apply		

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。

(\	Cisco UCM via Expressv	way	
Username			
Passphrase		۲	
Domain			
	Apply		

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	×
Bluetooth is On	
Discoverable off	
Scanning for available devices	

- 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。
 - o Bluetooth デバイスがリストに表示されたら、それを選択します。
 - o 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。
 - o 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。
 - o 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。

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

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

migilles-deskpro >			6:49 PM TI
	Join Webex © Search or enter meeting inf We We Vue can find the meeting information in e.g: 12345678 or username@example.	ormation os your calendar invite nple.webex.com	
	q w e r t y u i o a s d f g h j k ^ z x c v b n m . Image: 0.2123 Image: 0.2123 Image: 0.2123 Image: 0.2123 Image: 0.2123 Image: 0.2123 Image: 0.2123	p (X) 1 2 ABC 1 - 4 5 0H 3A 1 - 7 8 POBS TW .com Join 0	3 DEF 6 MARO 9 WXXY2 H
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。

<u>Webex</u>

CentralDeviceCisco Desk Pro, TANDBERGVideo addressmigilles@cisco.calls.webex.comOrganization nameCisco Systems, Inc.IP address10.81.12.28MAC address68:9E:0B:80:00:00Wi-Fi MAC address68:9E:0B:80:00:00Serial numberFOC2449NS4C			
General Device Cisco Desk Pro, TANDBERG Video address migilles@cisco.calls.webex.com Organization name Cisco Systems, Inc. IP address 10.81.12.28 MAC address 68:9E:08:80:00:00 Wi-Fi MAC address 68:9E:08:80:00:00 Serial number FOC2449NS4C	(About
Device Cisco Desk Pro, TANDBERG Video address migilles@cisco.calls.webex.com Organization name Cisco Systems, Inc. IP address 10.81.12.28 MAC address 68:9E:08:80:00:00 Wi-Fi MAC address 68:9E:08:80:00:00 Serial number FOC2449NS4C		General	
Video address migilles@cisco.calls.webex.com Organization name Cisco Systems, Inc. IP address 10.81.12.28 MAC address 68:9E:0B:80:00:00 Wi-Fi MAC address 68:9E:0B:80:00:00 Serial number FOC2449NS4C		Device	Cisco Desk Pro, TANDBERG
Organization name Cisco Systems, Inc. IP address 10.81.12.28 MAC address 68.9E:0B:80:00:0D Wi-Fi MAC address 68:9E:0B:80:00:0E Serial number FOC2449NS4C		Video address	migilles@cisco.calls.webex.com
IP address 10.81.12.28 MAC address 68:9E:0B:80:00:0D Wi-Fi MAC address 68:9E:0B:80:00:0E Serial number FOC2449NS4C		Organization name	Cisco Systems, Inc.
MAC address 68:9E:0B:B0:00:0D Wi-Fi MAC address 68:9E:0B:B0:00:0E Serial number FOC2449NS4C		IP address	10.81.12.28
Wi-Fi MAC address 68:9E:0B:B0:00:0E Serial number FOC2449NS4C		MAC address	68:9E:0B:B0:00:0D
Serial number FOC2449NS4C		Wi-Fi MAC address	68:9E:0B:B0:00:0E
		Serial number	FOC2449NS4C

Cisco Unified Communications Manager



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

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。

	Network connect	tion		
	Connected			
5	କି WI-FI	xroads	> 、	
ă	Ellemet	Not connected		
ß	Network Status		>	
\$	Advanced Network Settings			
	Continue			
(\	Network status	s		
(``)	Network status	S IPv4 and	IPv6	
ج) ۱ ۱	Network status ² stack Pv4 address (DHCP)	S IPv4 and 10.81.1	IPv6 2.22	
ب ج ا ا ا	Network status P stack Pv4 address (DHCP) Pv6 address	S IPv4 and 10.81.11	IPv6 2.22	
ai ai d d	Network status ² stack 2v4 address (DHCP) 2v6 address INS ITTP Provy	S IPv4 and 10.81.11 64.102.6	IPv6 2.22 247	
э а а ч ц н н	Network status P stack Pv4 address (DHCP) Pv6 address INS ITTP Proxy	S IPv4 and 10.81.1 64.102.6	IPv6 2.22 .247 Off	
عا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا	Network status ² stack ² v4 address (DHCP) ² v6 address ¹ NIS ITTP Proxy	S IPv4 and 10.81.1 64,102.6	IРиб 2.22 .247 Оff	
→ a a d d H	Network status P stack Pv4 address (DHCP) Pv6 address NNS ITTP Proxy	S IPv4 and 10.81.1 64.102.6	IPv6 2.22 .247 Off	
ج ا ا ا ا ا ا ا ا	Network status P stack Pv4 address (DHCP) Pv6 address JNNS ITTP Proxy	S IPv4 and 10.81.1 64.102.6	IPv6 2.22 .247 Off	
aı aı a H H	Network status P stack Pv4 address (DHCP) Pv6 address NNS HTTP Proxy	S IPv4 and 10.81.1: 64.102.6	IPv6 2.22 .247 Off	
⇒ aı a H H	Network status P stack Pv4 address (DHCP) Pv6 address INS ITTP Proxy	S IPv4 and 10.81.1 64.102.6	IPv6 2.22 .247 Off	

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。

(+	Wi-F Connec	ted	
	Wi-Fi		
	✓ xroads	< III. A	
	Networks		
	2wire421		
	55A958AF		
	acGuest		
	AdorableWiFi		
	Join other network	>	
	Join other network	>	
	Join other network	, ue	
	Join other network Continu Continu Stroads Connecte	d Entermine (BEAP)	
	Join other network Continu Continu Support Support Support Connecte Authentication	d Enterprise (PEAP)	
	Join other network Continu	d Enterprise (PEAP)	
	Join other network Continu Continu Second Connecte Authentication Advanced Wi-Fi details Forget this net	d Enterprise (PEAP)	
	Join other network Continu Continu Stroads • Connecte Authentication Advanced Wi-Fi details Forget this net	d Enterprise (PEAP)	

$\left(\leftarrow \right)$	Advanced Wi-Fi details	
SSID	xroads	
Speed	173 Mbps	
Frequency	5.18 GHz	
Signal Strengt	-38 dBm	
SNR	50 dBm	
Channel		
BSSID	C8:28:E5:EF:04:7B	
Region		

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。

<u>Webex</u>

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 按航フ ヘトは、	印題と診断	(Issues and diagnostics)]メニュー/	いり開始する	つーとも	じさより。

\leftarrow	Issues and diagnostics		l l
	Issues		
	 Everything is looking fine 	\sim	
	Diagnostics		
	SpeakerTrack diagnostics		
	MediaStatistics overlay		
	PII logging		
	People focus logging		
	Extended logging		
	a i m.a		

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

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。

1008 >			📮 AirPlay	8:06 PM (11
	/ Issues and diagnostic	rs			
	issues	a beaco 🗸			
	Diagnostics SpeakerTrack diagnostics	•			l
	PII logging Extended logging				
		_			

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(<u>https://x.x.x.x</u>)を参照し、[ホーム(Home)] を選択してこの情報を表示します。

Cisco Webex Local Device Controls			Q. Find page ()	
10.81.12.28 Desk Pro	System Informa	tion		
ි Home	General		Issues	
⊳ Call	10.81.12.28 IPv4	68:9E:0B:B0:00:0E MAC Address	Severything is looking fine	
TUP				
Settings	IPv6		Provisioning	
2 Users	FOC2449NS4C		Webey	
Security	Serial Number	Active Interface	Registered Device Mode	Details
JSTOMIZATION	Normal			
8 Personalization	Iemperature		Calendar	\$\$
² UI Extensions Editor	7e75011a-0740-5813	-8949-4d1cde1d477f@broadcloud.org	0 scheduled meeting(s) found for the next 24 hours.	
Macro Editor	migilles@cisco.calls.we	bex.com	Last updated: Thursday 3:59 PM	
& Developer API	Cloud SIP Address		View Scheduled M	eetings
YSTEM MAINTENANCE	Software	\$		
3 Software	Stable	RoomOS 11 13 1 5		
- Issues and Diagnostics	Software Channel	2f1a43e2808		
Backup and Recovery		Software Version		

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 (<u>https://x.x.x.x</u>) 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 ocal Device Controls							
10.81.12.28 Desk Pro	Settings						
△ Home	Configurations	Statuses	Send Whiteboard	to Email	$\ensuremath{\mathbb{Q}}$ Audio and Video		
∿ Call	Search	Configu	ration / SystemUr	nit			Collapse All Expand A
2CT1 ID	Apps						
Settings	Audio						
S Users	Bluetooth	Broadcas	stName	D			(0 to 256 characters)
Security	Bookings	CustomE	DeviceId	D			(0 to 255 characters)
USTOMIZATION	BYOD	Name		D			(0 to 50 characters)
Personalization	CallHistory						
2 UI Extensions Editor	Cameras	CrashRe	porting				
Macro Editor	Conformer	Advance	a	0		3	
S Developer API	Conterence	Mode	u) Off		~	
STEM MAINTENANCE	FacilityService	URI		ກ			(0 to 255 characters)
Software	Files	UNE					(0 to 200 charactels)
Issues and Diagnostics	HttpClient						
) Backup and Recovery	HttpFeedback	Software	eUpgrade WebCache				
	Logging			D Off		~	
		Mode					
	Macros	Url					(0 to 255 characters)
t isco Webex cal Device Controls	Macros Mari MicrosoftTeams	Url			G	λ Find page	(0 to 255 characters)
bisco Webex boal Device Controls	Macros Mari MicrosoftTeams Settings	Uri			C), Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Desk Pro	Macros Mari MicrosoftTeams Settings © Configurations	Url Statuses	⊠ Send Whiteboard	D Cui	€ Audio and Video	2 Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Dask Pro	Macros Mari MicrosoftTeams Settings @ Configurations Search	Mode Uri ■ Statuses Status /	⊠ Send Whiteboard	D Cin	€ Q Audio and Video), Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Desk Pro	Macros Mari MicrosoftTeams Settings © Configurations Search Audio	Mode Uri Statuses Status /	⊠ Send Whiteboard SystemUnit	to Email	Q ² Audio and Video), Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Desk Pro Home Call ETUP	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Blustooth	Wode Url Statuses Status /	⊠ Send Whiteboard SystemUnit	D Cur), Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Desk Pro besk Pro Call Ca	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Brokings	Mode Url Statuses Status / Broadca Developi	Send Whiteboard SystemUnit	to Email Michael C	Q Audio and Video), Find page	(0 to 255 characters)
Sco Webex cal Device Controls 10.81.12.28 Desk Pro besk Pro call 10.81.12.28 Desk Pro call 10.81.12.28 Desk Pro 20.81 20	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings	Statuses Status Broadca Develope Extensio	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported drawspassor	to Email Michael C Off True	Q Audio and Video), Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Desk Pro 2 Losk Pro 2 Call arup 3 Settings 3 Settings 3 Security	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras	Broadca Developi Extensio LastShut	Send Whiteboard SystemUnit stName arPreview Mode ns Microsoft Supported downRason downTime	D United Control of the second	Q Audio and Video Sillespie Desk Pro -13T05:57:16Z), Find page	(0 to 255 characters)
isco Webex cal Device Controls 10.81.12.28 Desk Pro 2 Home 5 Call Settings 3 Users 3 Security Users 4 Users 5 Security	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras Capabilities	Broadca Developi Extensio LastShut Producti	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported downReason downTime d	I to Email Michael C Off True Upgrade 2024-02: Cisco Des	Audio and Video), Find page	(0 to 255 characters)
SCO Webex cal Device Controls 10.81.12.28 Desk Pro 2 Home 2 Call Cal	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras Capabilities Conference	Statuses Status Status Broadca Develope Extensio LastShut Productf Produ	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported idownTime d Platform Type	to Email Michael C Off True Upgrade 2024-02: Cisco Des Posk Pro Cisco Co 230052	Q Audio and Video illespie Desk Pro -13T05:57:16Z sk Pro dec), Find page	(0 to 255 characters)
SCO Webex cal Device Controls 10.81.12.28 Desk Pro 2 Call TUP 2 Settings 3 Users 5 Security Users 5 Security Users 9 Security 10 Extensions Editor	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras Capabilities Conference Diagnostics	Broadca Developi Extensio LastShut Productt Productt Productt Uptime	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported downRason downTime d Platform Type	Michael G Off True Upgrade 2024-02- Cisco De: Desk Pro Cisco Co Cisco Co 239953	Q Audio and Video Sillespie Desk Pro -13T05:57:16Z sk Pro dec), Find page	(0 to 255 characters)
SCO Webex cal Device Controls 10.81.12.28 Desk Pro 10.81.12.28 Desk Pro 20.10 10.81.12.28 Desk Pro 20.10 20.	Macros Mari MicrosoftTeams Settings Search Audio Bluetooth Bluetooth Bluetooth Cameras Capabilities Conference Diagnostics Logging	Mode Url Statuses Status / Broadca Develop Extensio LastShut LastShut LastShut UstShut UstShut UstShut Uptime	Send Whiteboard SystemUnit stName arPreview Mode ns Microsoft Supported downReason downReason d downReason fype	Michael C Off True Upgrade 2024-02: Cisco De: Desk Pro Cisco Co 239953	Q Audio and Video aillespie Desk Pro -13T05:57:16Z sk Pro dec), Find page	(0 to 255 characters)
SCO Webex cal Device Controls 10.81.12.28 Desk Pro 2 Loser Pro 2 Call	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras Capabilities Conference Diagnostics Logging MicrosoftTeams	Mode Url Statuses Status / Broadca Developi Extensio LastShut LastShut LastShut Producti Producti Uptime Hardwar	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported idownTime d Platform Type	to Email Michael C Off True Upgrade 2024-02: Cisco Des Pro Cisco Co 239953	Q Audio and Video Aillespie Desk Pro -13T05:57:16Z sk Pro dec), Find page	(0 to 255 characters)
SCO Webex cal Device Controls 10.81.12.28 Desk Pro 2 Call TUP 2 Settings 3 Users 3 Security 3 S	Settings Settings Settings Search Audio Bluetooth Bookings Cameras Cameras Capabilities Conference Diagnostics Logging MicrosoftTeams Network	Mode Url Url Statuses Status / Broadca Develop: Extensio LastShut Productl Productl Productl Productl Uptime Hardwar DRAM HasWifi	Send Whiteboard SystemUnit stName arPreview Mode ns Microsoft Supported downRasson downTime d latform Type	Michael C Off True Upgrade 2024-02: Cisco De: Desk Pro Cisco Co 239953	Q Audio and Video Sillespie Desk Pro -13T05:57:16Z sk Pro dec), Find page	(0 to 255 characters)
isco Welbex cal Device Controls 10.81.12.28 Desk Pro 2 Home 5 Call ETUP 2 Settings 3 Security USTOMIZATION 8 Personalization 9 UI Extensions Editor 1 Macro Editor 2 UI Extensions Editor 3 Macro Editor 4 Developer API FISTEM MAINTENANCE 5 Software 1 November of Discussion	Settings Settings Search Audio Bluetooth Bookings Cameras Capabilities Conference Diagnostics Logging MicrosoftTeams Network NetworkServices	Broadca Develop Extensio LastShut Producti Produ	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported downReason downTime d Platform Type re	I to Email Michael C Off True Upgrade 2024-02: Cisco De: Desk Pro Cisco Co 239953	Audio and Video) Find page	(0 to 255 characters)
ISCO Webex cal Device Controls 10.81.12.28 Desk Pro Call Call Settings	Network Net	Mode Url Statuses Status / Broadca Developi Extensio LastShut Producti Producti Producti Uptime Hardwan DRAM HasWifi Monitorii Wonitorii	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported downTime d Platform Type re	to Email Michael C Off True Upgrade 2024-02: Cisco Des Pro Cisco Co 239953 8 8 True Normal 34 CS-DESK	Q Audio and Video	2, Find page	(0 to 255 characters)
ISCO WeDEX cal Device Controls	Nacros Mari MicrosoftTeams Settings Settings Search Audio Bluetooth Bookings Cameras Canference Diagnostics Logging MicrosoftTeams Network Peripherals Phonebook	Mode Url Url Statuses Status / Broadca Develop Extensio LastShut Producti Producti Producti Producti Producti DataShut Producti Producti Uptime Hardwal DRAM HasWifi Monitorii UDI Mainte	Send Whiteboard SystemUnit stName erPreview Mode ns Microsoft Supported downRason downTime d Patform Type re	Circo Email Michael C Off True Upgrade 2024-02: Cisco Des Pro Cisco Co 239953 S True Normal 34 CS-DESK	Q Audio and Video Sillespie Desk Pro -13T05:57:16Z sk Pro dec SPRO-K9 V01 FOC2449NS), Find page	(0 to 255 characters)
ISCO Webex cal Device Controls I 0.81.12.28 Desk Pro Call Call Settings	Settings Settings Search Audio Bluetooth Bookings Cameras Capabilities Canference Diagnostics Logging MicrosoftTeams Network Network Peripherals Phonebook Provisioning	Mode Url Url Statuses Status / Broadca Developy Extensio LastShut Producti	Send Whiteboard SystemUnit stName erPreview Mode downReason downTime d Patform 'ype re ng Temperature Status ngSoftware Board	I to Email Michael C Off True Upgrade 2024-02: Cisco De: Desk Pro Cisco Co 239953 8 True Normal 34 CS-DESK	Audio and Video Audio and Audio and Audio) Find page	(0 to 255 characters)

ユーザー

Cisco Webex Local Device Controls					Q Find	l page	0	2
10.81.12.28 Desk Pro	Users						Create Use	er
☆ Home	Username	Status	Admin (j)	Audit (j)	RoomControl (j)	Integrator (j)	User (j)	
℅ Call	admin	Active	\checkmark	~			~	

セキュリティ

Cisco Webex Local Device Controls						(2 Find page		0	2
10.81.12.28 Desk Pro	Security									
A Home	⊘ Certificates €	Sign-in Banner								
SETTIR	Services Custom	Preinstalled								
 Settings Users Security 	Add Certificate	Use the form below to This system supports & DSA encrypted private Certificate	add new cert PEM formatted key with or w Browse No	ficates. I certificate files ithout a passphr file selected.	(.pem). The c ase. Optional	certificate file	may contain the key file may be s	certificate and upplied separa	a RSA or ately.	
CUSTOMIZATION Personalization UI Extensions Editor Macro Editor Cuestion		Private key (optional) Passphrase (optional)	Browse No	file selected.						
SYSTEM MAINTENANCE	Existing Certificat	es								
G Software	Certificate	ssuer	802.1X	Audit HTTPS	HttpClient	HttpProxy	SIP Pairing	Actions		
S Backup and Recovery	Self-signed Certificate	TemporaryDefaultCertifica	ate					Delete	View Certific	cate
Cisco Webex Local Device Controls						QI	Find page	0		2
10.81.12.28 Desk Pro	Security									
G Home	\odot Certificates \ni	Sign-in Banner								
℅ Call	Services Custom P	reinstalled								
serup ② Settings A Users A Security	Add Certificate Authority	Use the form below to a This system supports PE Browse No file sele	dd new certific M formatted fi cted.	ate authorities. les (.pem) with c	ne or more C	A certificates	within the file.			
CUSTOMIZATION	Existing Certificate	Authorities								
	Certificate	Issuer		Details	Actions					
Macro Editor % Developer API	No certificates									
SYSTEM MAINTENANCE Software Subset of the second										

Cisco Webex Local Device Controls		Q Find	page 📀	
10.81.12.28 Desk Pro	Security			
G Home	⊘ Certificates ∋ Sign-in Banner			
🗞 Call	Services Custom Preinstalled			
ETUP	Preinstalled Certificates HTTP servers host • SMTP mail servers	is listed below are used to validate the certificates of external ing content used by the web views, the HttpClient xAPI, Ma (on video systems with touch screens)	servers that the video system	
JSTOMIZATION	Certificate Details			
² UI Extensions Editor	Certificate	Issuer	Details E	Enabled
Macro Editor	AAA Certificate Services	Comodo CA Limited	View	
STEM MAINTENANCE	ACCVRAIZ1	ACCV	View	
Software	Actalis Authentication Root CA	Actalis S.p.A./03358520967	View	
Issues and Diagnostics Backup and Recovery	AffirmTrust Commercial	AffirmTrust	View	•
	AffirmTrust Networking	AffirmTrust	View	

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(<u>https://x.x.x.x</u>)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。

<u>パーソナライゼーション(Personalization)</u>

Cisco Webex Local Device Controls	Q Find page @	8
10.81.12.28 Desk Pro	Personalization	
分 Home So Call	Image: Wallpaper and Halfwake Image: Branding Image: Virtual Backgrounds Image: Ringtones Image: Contacts	
SETUP Settings	Halfwake The device enters halfwake after it has been idle for a while.	
요 Users A Security	Default	
	Upload image Recommended size is 3840×2160 pixels. File format: jpg, png, webp	
 UI Extensions Editor Macro Editor Developer API 	Turn off display after 10 minutes	
SYSTEM MAINTENANCE	(Preview on device)	
 ∿ Issues and Diagnostics ☺ Backup and Recovery 	Wallpaper The wallpaper is shown as a background on the home screen.	
Cisco Webex Local Device Controls	Custom image light night	
10.81.12.28 Desk Pro	Personalization	
ි Home	☑ Wallpaper and Halfwake ☑ Branding ☑ Virtual Backgrounds ♬ Ringtones ☑ Contacts	
SETUP	Brand Logo Halfwake logo Shows brand logo in halfwake	
Implementation in the second second	Upload image Recommended size is 272×272 pixels. File format: png	
	Home screen logo Show brand logo on home screen	
Personalization UI Extensions Editor	Upload image Recommended size is 272×272 pixels. File format: png	
Macro Editor Control API	Custom Text Custom text displays in the bottom left corner of the main screen.	
SYSTEM MAINTENANCE	Feedback? https://cs.co/dt Apply	
Sackup and Recovery		

Cisco Webex Local Device Controls	Q Find page (2)	
10.81.12.28 Desk Pro	Personalization	
G Home	☑ Wallpaper and Halfwake ☑ Branding ☑ Virtual Backgrounds ♫ Ringtones ☑ Contacts	
 Settings Settings Users Security Customization ✓ UI Extensions Editor ✓ Macro Editor ※ Developer API 	Virtual Backgrounds Upload You can upload up to three virtual backgrounds to replace the background of your video during a call. Image: Comparison of the provided during a call of the provided	
SYSTEM MAINTENANCE So Software So Issues and Diagnostics So Backup and Recovery Cisco Webex Local Device Controls 10.81.12.28 10.81.12.28	Q Find page (2)	
☆ Home	☑ Wallpaper and Halfwake ☐ Branding ☑ Virtual Backgrounds ☐ Ringtones □ Contacts	
Security	Ringtones Select Active Ringtone Please note that the ringtone will play on the video system. Sunrise >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
CUSTOMIZATION CUSTOMIZATION P OI Extensions Editor Macro Editor Customered Customere		

Cisco Webex Local Device Controls					Q Find page		0
10.81.12.28 Desk Pro	Personalization						
ධ Home	I Wallpaper and Halfwake	Branding	C Virtual Backgrounds	☐ Ringtones	Contacts]	
s Call	The section below lets you or the Call activity in the device's The complete list of contacts and then import it into all of yo	eate, edit, and delete s user interface. can be exported. Use our other devices.	ocal phonebook entries on t	he system. These en a backup of the local	tries show up in the phonebook, or to c	"Favorites" pa reate a phonel	nel under book once
Security	Search contacts	X Ca Add Folde	Add Contact			الله السومين الله الله الله الما الله الما الله الله	Expo
USTOMIZATION	< Back Favorites			Edit Folder			
Personalization	Name	Number					
 ² UI Extensions Editor ⁵ Macro Editor ³ Developer API 		No contact	S				
SYSTEM MAINTENANCE S Software Ussues and Diagnostics D 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 (<u>https://x.x.x.</u>) 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。

<u>ソフトウェア</u>

Cisco Webex Local Device Controls		Q Find page	<u> </u>
10.81.12.28 Desk Pro	Software		
යි Home	Software Upgrade		
 Setup Settings Users Security 	 Your system is cloud managed, and you cannot manage the software Go to Cisco Webex Control Hub to change the software channel. 	re locally.	
CUSTOMIZATION			
SYSTEM MAINTENANCE G Software ↑ Issues and Diagnostics 5 Backup and Recovery			

<u>問題と診断</u>



バックアップとリカバリ

Cisco Webex Local Device Controls	Q Find page	0
10.81.12.28 Desk Pro	Backup and Recovery	
ධ Home	D Backup C Restore % System Recovery N Restart and Shutdown	
⊳ Call	Download This page lets you backup a device's configurations. Configurations include xConfigurations, as well as the product of other features a device might support. like macros and UI Extensions.	he configurations
Settings	Select items to include in your backup. Leave all items checked to generate a complete backup of the de	evice.
2 Users	Branding No items installed	
j Security	Favorites No items installed	
USTOMIZATION	UI Extensions No items installed	
Personalization Ul Extensions Editor	Macros No items installed	
Macro Editor	Sign in Banner 🔽 Include	
C Developer API	Configuration 🗹 Include	
YSTEM MAINTENANCE	The configuration listed below can be modified for a partial bac configuration.	ckup of the
S Software	Note: Settings such as Network, SIP URI and SystemUnit Na specifically apply to a certain device. Applying a backup with t	me may hese settings to
 Issues and Diagnostics 	a different device may result in it becoming unreachable on the avoid this, consider removing those settings from the list below	e network. To v.
Backup and Recovery	Remove system-specific configurations	
	Apps WallpaperBundles HalfwakeImage: Auto	
	Audio Deraultvolume: 50 Audio Input HDMI 1 Level: -5	
	Audio Input HDMI 1 Mode: On Audio Input HDMI 1 VideoAssociation MuteOnInact:	iveVideo: On

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。

_			
	Manage Web App Settings	8	
	Meeting zone		
	Connections	>	
	Are you sure you want to reset this device?		
	This will delete all data and settings permanently. You will need to configure this device again.		
	Cancel Reset		
	Restart		

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。

Cisco Webex Local Device Controls		Q Find page ③
10.81.12.28 Desk Pro	Software Recovery Swap	A system recovery swap will reinstall the previously installed software image on the device. The previous software image is located on an inactive partition on the device, and by clicking the button below, you will change the active partition and reboot. Performing a software recovery swap is the recommended action if the system has a severe issue, for example if it is unable to start up properly. Please consult with your Cisco technical support representative before performing a system recovery swap. Provide systems logs when opening the support ticket. Active software image: ce11.13.1.5 2f1a43e2808 2024-02-09 Software image on inactive partition: ce11.12.1.6 6c205f3b2e5 2024-01-18
 A Security CUSTOMIZATION I Personalization ✓ UI Extensions Editor I Macro Editor X Developer API 	Factory Reset	Factory Reset All other troubleshooting measures fail. It is strongly any reset. Are you sure you want to perform a factory reset? e the Backup tab to create a backup bundle of local in to reconfigure the system afterwards. Cancel Factory Reset solution, like Cisco Webex Control Hub, Cisco Unified Communications Manager, Cisco Expressway, or Cisco TelePresence Management Suite.
SYSTEM MAINTENANCE G Software ≁ Issues and Diagnostics S Backup and Recovery		 Caution: A factory reset cannot be undone. Eurther Details Call logs will be deleted. All local user accounts will be deleted. Customizations, like Macros, UI Extensions, and branding, will be deleted. The alternate software image will be deleted, so that it will no longer be possible to do a software recovery swap afterwards. Release keys and option keys will <i>not</i> be deleted.

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

Cisco Webex Local Device Controls					Q Find page	0	8
10.81.12.28 Desk Pro	Issues a	and Diagnost	ics				
ଲ Home % Call	~ Issues	System Logs	♥ Call Logs	User Interface Screenshots]		
SETUP © Settings C Users C Security	Screens	Taking a s bugs to Ci Note that i depending OSD Sci	creenshot of the to sco, and so on. any on screen video on image resolution eenshot	uch panel or the on-screen dispay (OSE o or presentation will not be captured, a on and network bandwidth.	can be useful for creating use nd that capturing a screenshot i	r manuals, reporting may take a while,	I
CUSTOMIZATION Personalization UI Extensions Editor Macro Editor X Developer API		Wake Sy Use the bu Awake	stem Up uttons below to put Halfwake	the system into awake or halfwake state	3.		
SYSTEM MAINTENANCE G Software A Issues and Diagnostics S Backup and Recovery							

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/productsmaintenance-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

 $y_7 https://software.cisco.com/download/home/278875240$

無線 LAN でのリアルタイム

トラフィック設計ガイド<u>https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F</u> 20 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/productsimplementation-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

 $\underline{https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html$

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-andconfiguration-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<u>https://www.cisco.com/c/en/us/td/docs/wireless/access_point/atnms</u> <u>-ap-8x/configuration/guide/cg-book.html</u>

Cisco Meraki ワイヤレス LAN

のドキュメント<u>https://documentation.meraki.c</u>

<u>om</u>

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)。

⑧Bluetooth 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.