cisco

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド



Cisco Wireless Phone 840 および 860 は、ユーザーがタスクと通信を簡単に管理できるモバイル コラボレー ション プラットフォームを提供します。Cisco Wireless Phone 840 および 860 は、セキュアなエンタープラ イズグレードのスマートフォンのパワーとパフォーマンスを提供しながら、シスコのコラボレーション ソリュ ーションを通じて管理しやすいデバイスを提供します。Wi-Fi の柔軟性を備えた Cisco Wireless Phone 840 お よび 860 は、企業内のどこにいても、従業員の生産性を向上させます。Cisco Wireless Phone 840 は、IP65 等級の防塵、防滴、防湿性能があります。Cisco Wireless Phone 860 は、IP68 等級の完全な防塵性能を備えて います。

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 Cisco Wireless Phone 840 および 860 を導 入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
01/08/21	1.1(0) リリース
03/30/21	1.2(0) リリース
08/30/21	1.3(0) リリース
10/29/21	1.4(0) リリース
04/15/22	1.5(0) リリース
07/26/22	1.6(0) リリース
10/04/22	1.7(0) リリース
04/21/23	1.8(0) リリース
07/23/23	1.9(0) リリース

目次

Cisco Wireless Phone 840 および 860 概要	7
電話機モデル	7
要件	8
サイト調査	
コール制御	
ワイヤレス LAN	
プロトコル	
Wi-Fi	
規格	
Bluetooth	31
言語	33
バッテリ寿命	33
840S および 860S バーコードスキャナ	35
電話機のお手入れ	36
アクセサリ	36
モ線 LAN の設計	39
802.11 ネットワーク	
5 GHz(802.11a/n/ac)	
2.4 GHz (802.11b/g/n)	
信号強度とカバレッジ	
テータ レート	
余件の厳しい環境	
$t \neq 2 \int f f$	
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)	
(FAP-TTI S: 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)	51
Protected Extensible Authentication Protocol (PEAP)	
Ouality of Service (OoS)	51
コール アドミッション制御(CAC)	
有線 QoS	53
ローミング	54
高速セキュア ローミング(FSR)	55
帯域間のローミング	57
電源管理	57
コール キャパシティ	58

マルチキャスト	59
Cisco ワイヤレス LAN の設定	59
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	
802.11 ネットワークの設定	61
WLAN の設定	
コントローラの設定	
コール アドミッション制御(CAC)	
RF プロファイル	88
FlexConnect グループ	
マルチキャスト ダイレクト	
QoS プロファイル	
詳細設定	
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	
802.11 ネットワークの設定	103
WLAN の設定	111
コントローラの設定	127
モビリティ設定	128
コール アドミッション制御(CAC)	129
マルチキャスト	130
詳細設定	132
設定例	
Cisco Mobility Express および Lightweight アクヤスポイント	
コントローラの設定	
WLAN の設定	
RF プロファイル	
マルチキャスト ダイレクト	
Cisco Autonomous (白倉) アクセス ポイント	150
CISCO AUTOMOTINOUS (日年) アクセス ホインド	
802.11 ネットノークの設定 M/I AN の設定	
VLAN の設定 コール アドミッシュン制御(CAC)	
コールフトミックヨン司政(CAC)	
Q05 ホック	180
电标目生 設定例	
ワイヤレス ネットワークの作成	
SSID の設定	
ノァ1 グワオール & トフノイツク ンエービンク	
Cisco Call Control の設定	199
Cisco Unified Communications Manager	

製造元の認証局(CA)証明書 200 「パイスブール(Device Pools)] 201 電話ボタンテンブレート 202 セキュリティブロファイル 202 SIP プロファイル 205 共通設定 208 QOS パラメータ 209 オーディオビット 209 オーディオビットレート 209 オーディオンレート 209 オージャート 210 Webex Calling 215 Cisco Wireless Phone 840 および 860 224 エンターブラインス電話機構成管理ツール 226 構成アイハロ作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 226 城市吉賀田 224 ジョンのデッググクレード	製造元の認証局(CA)証明書 200 「デバイスブール(Device Pools)] 201 電話ボタンテンブレート 202 セキュリティブロファイル 202 ワロファイル 203 SIP プロファイル 206 QoS パラメータ 209 QoS パラメータ 209 QoS パラメータ 209 QoS パラメーク 209 QoS パラメーク 209 製品固有の設定オブション 209 製品固有の設定オブション 210 Webex Calling 211 Webex Calling 216 デバイス設定 222 Clsco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Clsco Wireless Phone 840 および 860 の登量 251 Clsco Wireless Phone 840 および 860 の登量 254 手動設定 266 Webex Calling 266 Weiteless Phone 840 および 860 の登量 254 デ動設定 266 Webex Calling 289 Clsco Unified Communications Manager 286 </th <th>デバイスの有効化</th> <th></th>	デバイスの有効化	
「デバイスブール (Device Pools)] 201 電話ボタンテンブレート 202 SIP プロファイル 202 SIP プロファイル 205 共通設定 208 QoS パラメータ 209 G.722 および Opus のアドパタイズメント 209 オーディオ ビット レート 209 製品圖有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの校式 227 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi プロファイルの設定 260 Wi-Fi ブロファイルの設定 260 Wi-Fi ブロファイルの設定 260 Wi-Fi ブロファイションの設定 260 Stoco Unified Communicatio	「デバイスブール (Device Pools)] 201 電話ボタン デンプレート 202 SIP ブロファイル 205 SIP ブロファイル 205 YinaByz 206 QOS バラメーク 209 G. 722 および Opus のアドバタイズメント 209 オーディオ ビット レート 209 製品園有の設定オブション 210 Webex Calling 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ首曜 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成フィイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Unified Communications Manager の設定 256 ジェコワイヤレス電話機構成管理ツール 226 単酸定 217 Cisco Unified Communications Manager の設定 260 証明書管理 217 Cisco Unified Communications Manager の設定 261 運動管理 217 Cisco Unified Communications Manager 266 ジェンのデッブリケーションの設定 261 Eisco Unified Communications Manager 266 ジェンのごのデッググレード 268	製造元の認証局 (CA) 証明書	
電話ボタンテンプレート. 202 セキュリティブロファイル. 202 SIP プロファイル. 205 QOS バラメータ 209 QOS バラメータ 209 QOS バラメータ 209 QC 22 および Opus のアドバタイズメント 209 カーディオ ビット レート 209 製品圖有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話提供成管理ツール 226 ベロバドレラマ バロク 市成 227 Cisco Wireless Phone 840 および 860 の登録 251 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 260 Wireless Phone 840 および 860 の登録 254 アームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 289 Cisco Unified Communications Manager 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone	電話ボタン テンプレート. 202 セキ ユリティ プロファイル. 202 ビキ ユリティ プロファイル. 205 SIP プロファイル. 208 QOS バラメーク. 209 QOS バラメーク. 209 マーディオ ビット レート	[デバイスプール(Device Pools)]	
セキュリティブロファイル	セキュリティブロファイル 202 SIP プロファイル 205 Juit Sip プロファイル 206 QoS パラメータ 209 QoS パラメータ 209 QoS パラメータ 209 マ.72 および Opus のプドパタイズメント 209 オーディオ ビット レート 209 製品園有の設定オプション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wreless Phone 840 および 860 224 エンタープライズ モビリティ 蒼斑 (EMM) 224 シスコワイヤレス電話機構成首理ツール 226 構成ファイルの作成 227 Cisco Wireless Phone 840 および 860 の登録 254 デが記 Zin Sinfied Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 デ動設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアップグレード 286 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wirel	電話ボタン テンプレート	
SIP プロファイル 205 共通設定 208 QoS パラメータ 209 G.72 および Opus のアドパタイズメント 209 オーディオ ビットレート 209 製品固有の設定オブション 210 Webex Calling 215 「バイス設定 222 Clsco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコウイヤレス電話機構成管理ツール 226 構成フィイルの作成 227 Clsco Unified Communications Manager の設定 251 Clsco Vireless Phone 840 および 860 の登録 254 チ動設定 260 証明書管理 274 Clsco Unified Communications Manager の設定 251 Clsco Unified Communications Manager の設定 260 証明書管理 274 Clsco Unified Communications Manager の設定 260 証明書管理 274 Clsco Unified Communications Manager 280 グラビックアップグレード 280 Clsco Unified Communications Manager 280 ごesco Unified Communications Manager 285 ファームウェアのアップグレード 289 Clsco Unified Communications Manager 289 <	SIP プロファイル 205 共通設定 208 QOS パラメータ 209 Q.722 および Opus のアドパタイズメント 209 オーディオ ビットレート 209 製品固有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デパイス設定 222 Cisco Wreless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの管理 227 Cisco Wireless Phone 840 および 860 の登録 251 Cisco Wireless Phone 840 および 860 の登録 254 チ動設定 266 Wirel プロファイルの設定 260 延明書管理 274 Cisco Phone アブリケーションの設定 261 Bluetooth 設定 265 ファームウェアのデッブグレード 266 Vieless Phone 840 および 860 の使用 265 ファームウェアップグレード 266 Vieless Phone 840 および 860 の使用 265 フレームの設定 265 ブレート 266 ジスコの電話機 276 ジスコの電話機 277 ジュームの電話機 <td< td=""><td>セキュリティ プロファイル</td><td></td></td<>	セキュリティ プロファイル	
共通設定 208 QoS バラメータ 209 G.722 および Opus のアドバタイズメント 209 マーディオ ビット レート 209 製品固有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Wireless Phone 840 および 860 の登録 254 チ動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Wireless Phone 840 および 860 の登録 254 チ動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Unified Communications Manager の設定 260 証明書管理 274 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 288 Vebex Calling 289 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 288 Vebex	共通設定 208 QoS バラメータ 209 G.722 および Opus のアドバタイズメント. 209 オーディオ ビット レート 209 製品固有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 普理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Wireless Phone 840 および 860 の登建 254 F 新設定 226 Wi-Fi ブロファイルの設定 260 証明書管理 274 Cisco Phone 7ブリケーションの設定 261 Bluetooth 設定 262 ブアームウェアのアッブグレード 288 Cisco Virieless Phone 840 および 860 の使用 286 プレスロ電話機 296 ジスコの電話機 297 バーコード 303 バッテリ寿命 305 ズッコの電話機 307 ズック 307 ブレラーション 307 ブレラーション 307 ブルラーション 307 ブルラーション	SIP プロファイル	
QoS バラメータ 209 G.722 および Opus のアドバタイズメント 209 オーディオ ビット レート 209 製品園有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Wireless Phone 840 および 860 の登録 254 チ動設定 260 Wir-Fi プロファイルの作成 260 証明書管理 260 Wir-Fi プロファイルの段定 260 証明書管理 274 Cisco Phone アプリケーションの設定 260 証明書管理 274 Cisco Unified Communications Manager 280 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone 840 および 860 の使用	QoS バラメータ 209 G,722 および Opus のアドバタイズメント 209 オーディオ ピット レート 209 製品園有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンターブライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Wireless Phone 840 および 860 の登録 251 Cisco Wireless Phone 840 および 860 の登録 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 266 Wirel プロファイルの役定 266 Wirel ブロファイルの設定 274 Cisco Unified Communications Manager の設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 285 Cisco Unified Communications Manager 286 Cisco Wireless Phone 840 および 860 の使用 285 ファームウェアのアップグレード 285 ファームウェアのアップグレード 289 Cisco Wireless Phone 840 および 860 の使用 グロ デブリケーション	共通設定	
G.722 および Opus のアドバタイズメント 209 オーディオ ビット レート 209 製品固有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Unified Communications Manager の設定 251 ビisco Phone 7ブリケーションの設定 260 誕明書管理 274 Cisco Unified Communications Manager の設定 251 Sico Unified Communications Manager の設定 251 Fib設定 260 Wi-Fi プロファイルの設定 260 WiFi プロファイルの設定 260 Weige 274 Cisco Unified Communications Manager 280 Cisco Inified Communications Manager 288 Vebex Calling 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 288 Cisco Wireless Phone 840 および 860 の使用 289	G.722 および Opus のアドバタイズメント	QoS パラメータ	
オーディオ ビット レート 209 製品固有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wir-Fi プロファイルの設定 260 証明書管理 260 Eisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Webex Calling 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 288 Vebex Calling 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone 840 および 860 の使用 296 アブリケーション 296 シスコの電話機 297 バーコード 303	オーディオ ビット レート	G.722 および Opus のアドバタイズメント	
製品固有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 WiFI プロファイルの設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Vebex Calling 289 Cisco Phone アブリケーションの設定 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アブリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 307	製品国有の設定オブション 210 Webex Calling 215 個人的な使用 216 共同利用 218 アバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Unified Communications Manager の設定 266 証明書管理 274 Cisco Unified Communications Manager の設定 260 証明書管理 274 Cisco Unified Communications Manager の設定 260 証明書管理 274 Cisco Unified Communications Manager 280 Cisco Page 274 Bluetooth 設定 281 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone Upgrade ">ール 289 Cisco Wireless Phone Upgrade ">ール 289 Cisco Wireless Phone 840 および 860 の使用 296 アブリケーション 296 シスコの電話機 307 <t< th=""><th>オーディオ ビット レート</th><th></th></t<>	オーディオ ビット レート	
Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アブリケーション 296 ジスコの電話機 297 バーード 303 バッテリ寿命 307	Webex Calling 215 個人的な使用 216 共同利用 218 デバイス設定 222 Clsco Wireless Phone 840 および 860 224 エンターブライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 227 Cisco Wireless Phone 840 および 860 の登録 254 チ動設定 266 Wi-Fi ブロファイルの設定 260 証明書管理 224 Cisco Wireless Phone 840 および 860 の登録 254 チ動設定 260 証明書管理 260 証明書管理 274 Cisco Phone アブリケーションの設定 289 Zisco Unified Communications Manager 285 ファームウェアのアッブグレード 286 Cisco Unified Communications Manager 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話M 297 バーコード 303 バッテリ寿命 305 ボタン 307 近日 307 週間 307 </th <th>製品固有の設定オプション</th> <th></th>	製品固有の設定オプション	
Webex Calling 216 第四利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Wireless Phone 840 および 860 の登録 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 288 Vebex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 アプリケーション 296 アブリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 307	Precise Camp 216 興岡利用 216 大岡利用 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 266 Wireless Phone 7ブリケーションの設定 266 証明書管理 274 Cisco Unified Communications Manager の設定 266 証明書管理 266 ごsco Phone アブリケーションの設定 281 Bluetooth 設定 281 Dietorth 設定 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Unified Communications Manager 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アブリケーション 296 シスコの電話機 297 バッテリ寿命 307 ボージョン 307 ブスコの電話機 307 ブスクスの公	Webey Calling	215
Importing Berger 216 オースのション 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 285 ファームウェアのアップグレード 288 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone 840 および 860 の使用 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタシ 307	Impact System 210 大田和田 218 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 266 Wi-Fi プロファイルの設定 266 証明書管理 274 Cisco Phone アブリケーションの設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 286 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話経費設定 307 ブムラク 気設定 307 ブムラク 気設定 307 </td <td>Webex Calling</td> <td></td>	Webex Calling	
ス国村川 210 デバイス設定 222 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi ブロファイルの設定 260 証明書 管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 288 Cisco Wireless Phone 840 および 860 の使用 288 Vebex Calling 289 Cisco Wireless Phone Upgrade ツール 286 アブリケーション 296 シスコの電話機 297 バーコード 303 バッデリ寿命 305 ボタシ 305	スロヤカホ 210 デバイス設定 222 Clisco Wireless Phone 840 および 860 224 エンターブライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 266 Wi-Fi プロファイルの設定 266 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 アームウェアのアップグレード 286 Cisco Wireless Phone 840 および 860 の使用 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 289 Cisco Wireless Phone 840 および 860 の使用 296 ジスコの電話機 297 バーコード 303 バッテリ寿命 304 ブリン 305 ボタン 307 通話品質設定 309 緊急 314		210
フトイト&とと 224 Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi ブロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Cisco Wireless Phone 840 および 860	共同利用 デバイフ設定	
Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Vebex Calling 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バード 303 バッテリ寿命 307	Cisco Wireless Phone 840 および 860 224 エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成音理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 手動設定 266 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Wireless Phone Upgrade ツール 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone Upgrade ツール 289 グブリケーション 296 シスコの電話機 297 パーコード 303 パッテリ寿命 305 ボタン 307 適話品質設定 307 ウスシスの電話機 307 アンリ寿命 309 緊急 (Emergency) 312 ロギング 314)ハ1 入設と	
エンタープライズ モビリティ 管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 289 Cisco Unified Communications Manager 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バートド 303 バッテリ寿命 305 ボタン 307	エンタープライズモビリティ管理 (EMM) 224 シスコワイヤレス電話機構成管理ツール. 226 構成ファイルの作成. 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録. 254 手動設定. 260 誕い手i プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード. 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 パーード 303 パッテリ寿命 307 通話品質設定 307 ブムタム設定 309 緊急 (Emergency) 314	Cisco Wireless Phone 840 および 860	
シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成. 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録. 254 手動設定. 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード. 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 288 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーード 303 バッテリ寿命 307	シスコワイヤレス電話機構成管理ツール 226 構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 260 Wil-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話機 297 バーコード 303 パッデリ寿命 305 ボタン 307 ブロード 309 緊急 (Emergency) 314	エンタープライズ モビリティ管理 (EMM)	
構成ファイルの作成. 227 Cisco Unified Communications Manager の設定. 251 Cisco Wireless Phone 840 および 860 の登録. 254 <i>手動設定</i> . 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッデリ寿命 305 ボタン 307	構成ファイルの作成 227 Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話機 297 バーード 303 バッデリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 314	シスコワイヤレス電話機構成管理ツール	
Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Cisco Unified Communications Manager 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Cisco Unified Communications Manager の設定 251 Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 266 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アブリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 285 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話機 297 バッテリ寿命 303 バッテリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 314	構成ファイルの作成	
Cisco Wireless Phone 840 および 860 の登録	Cisco Wireless Phone 840 および 860 の登録 254 <i>手動設定</i> 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 314	Cisco Unified Communications Manager の設定	
手動設定	手動設定 260 Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 314	Cisco Wireless Phone 840 および 860 の登録	
Wi-Fi プロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Wi-Fi ブロファイルの設定 260 証明書管理 274 Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 シスコの電話機 297 パッテリ寿命 303 パッテリ寿命 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 314	手動設定	
証明書管理	証明書管理	Wi-Fi プロファイルの設定	
Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Cisco Phone アプリケーションの設定 281 Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 312 ロギング 314	証明書管理	
Bluetooth 設定 285 ファームウェアのアップグレード 288 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Bluetooth 設定 285 ファームウェアのアップグレード 286 Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 309 緊急 (Emergency) 312 ロギング 314	Cisco Phone アプリケーションの設定	
ファームウェアのアップグレード	ファームウェアのアップグレード	Bluetooth 設定	
Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Cisco Unified Communications Manager 288 Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 309 緊急 (Emergency) 312 ロギング 314	ファームウェアのアップグレード	
Webex Calling	Webex Calling 289 Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 312 ロギング 314	Cisco Unified Communications Manager	
Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307	Cisco Wireless Phone Upgrade ツール 289 Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 309 緊急 (Emergency) 312 ロギング 314	Webex Calling	
Cisco Wireless Phone 840 および 860 の使用	Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 309 緊急 (Emergency) 312 ロギング 314	Cisco Wireless Phone Upgrade ツール	
Cisco Wireless Phone 840 および 860 の使用	Cisco Wireless Phone 840 および 860 の使用 296 アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 312 ロギング 314		
<i>アプリケーション</i>	アプリケーション 296 シスコの電話機 297 バーコード 303 バッテリ寿命 305 ボタン 307 通話品質設定 307 カスタム設定 309 緊急 (Emergency) 312 ロギング 314	Cisco Wireless Phone 840 および 860 の使用	296
シスコの電話機	シスコの電話機297バーコード303バッテリ寿命305ボタン307通話品質設定307カスタム設定309緊急 (Emergency)312ロギング314	アプリケーション	
バーコード	 バーコード	シスコの電話機	
バッテリ寿命	 バッテリ寿命	バーコード	
ボタン	ボタン	バッテリ寿命	
	通話品質設定	ボタン	
通話品質設定	カスタム設定	通話品質設定	
カスタム設定	緊急(Emergency)312 ロギング	カスタム設定	
緊急(Emergency)	ロギング	緊急(Emergency)	
ロギング		ロギング	
	PTT	PTT	

サウンドステージ	
システムアップデータ	
Web API	322
アプリケーションストア	
[IP Phone サービス (IP Phone Services)]	325
トラブルシューティング	326
問題レポート ツール	
電話機の Web ページ	
デバイス情報	
ネットワーク情報	
登録情報	
デバイス ログ	
WLAN 信号インジケータ	
WLAN ネットワーク情報	
初期化	
電話機画面のスクリーンショットのキャプチャ	
その他のマニュアル	338

Cisco Wireless Phone 840 および 860 概要

Cisco Wireless Phone 840 および 860 は、企業内のコラボレーションを実現するプラットフォームです。無線 および有線の Cisco Unified Communication デバイスの強固な基盤として、Cisco Unified Communication ア プリケーションの機能を統合します。

Cisco の 802.11 ソリューションにより、音声といった、時間に影響を受けるアプリケーションをキャンパス全体の無線 LAN (WLAN) 環境で効率的に使用できます。無線 LAN 環境の拡張により、アクセス ポイント間のローミング時にセキュリティを維持しながら、高速ローミング機能とほぼシームレスなマルチメディア トラフィックのフローが実現します。

WLAN はライセンス不要の周波数帯を使用しているため、ライセンス不要の同一周波数帯を使用する他のデバ イスから干渉を受ける可能性があります。また、Bluetooth ヘッドセット、電子レンジやコードレス電話など、 2.4 GHz 周波数帯を使用するデバイスは急増しており、2.4 GHz 周波数帯では他の周波数帯よりも多くの輻輳が 発生する可能性もあります。5 GHz 周波数帯で動作するデバイスは非常に少数であるため、Cisco Wireless Phone 840 および 860 の運用において最大限の 802.11a/n/ac データレートを活用するにはこの周波数帯が推 奨されます。

Cisco Wireless Phone 840 および 860 は最適化されていますが、ライセンスのない周波数帯を使用する場合、 中断されない通信は保証できず、通話中に数秒の音声のギャップが生じる可能性があります。この導入ガイドラ インに従うことで、このような音声のギャップが発生する可能性は低減されますが、完全には解消されません。

ライセンス不要の周波数帯を使用しており、WLAN デバイスへのメッセージの配信は保証されません。 Cisco Wireless Phone 840 および 860 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。

電話機モデル

次の Cisco Wireless Phone 840 および 860 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。

製品番号	説明	ピーク アンテナ ゲイン	周波数範囲	使用可能な チャネル	チャネル セット
CP-840	Cisco Wireless Phone 840	2.4 GHz = 1.7 dBi 5 GHz = 1.8 dBi	2.412 ~ 2.472 GHz 5.180 ~	13 4	1 ~ 13 36, 40, 44, 48 52, 56, 60, 64
CP-840S	Cisco Wireless Phone 840S (バーコードス キャナ付き)		5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz	4 12	100 ~ 144 149、153、 157、161、165
			5.745 ~ 5.825 GHz	5	

CP-860	Cisco Wireless Phone 860	2.4 GHz = 0.6 dBi 5 GHz = 0.8 dBi	2.412 ~ 2.472 GHz 5.180 ~	13 4	1 ~ 13 36、40、44、48
CP-860S	Cisco Wireless Phone 860S (バーコードス キャナ付き)		5.240 GHz 5.260 ~ 5.320 GHz 5.500 ~ 5.720 GHz 5.745 ~ 5.825 GHz	12 5	52、56、60、64 100 ~ 144 149、153、 157、161、165

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。

要件

Cisco Wireless Phone 840 および 860 は、音声通信を提供する IEEE 802.11a/b/g/n/ac デバイスです。

Cisco Wireless Phone 840 および 860 の導入に必要な要件が満たされていることを確認するには、環境の検証 が必要です。

サイト調査

Cisco Wireless Phone 840 および 860 を実稼働環境に導入する前に、先進的なワイヤレス LAN を専門とする シスコ認定パートナーによって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 Wireless Phone 840 および 860 を基幹業務で使用する場合は 5 GHz の使用が強く推奨され ます。サイト調査には、その場所の対象カバレッジ プランを示すヒートマップも含まれます。さらにサイト調 査では、その場所で使用するアクセスポイント プラットフォーム タイプ、アンテナタイプ、アクセスポイント 設定 (チャンネルと送信電力)も決定されます。条件の厳しくない環境 (オフィス、医療機関、教育、サービス 業など)に対しては内蔵アンテナを持つアクセスポイントを選択し、条件の厳しい環境 (製造、倉庫、小売業な ど)に対しては、外部アンテナを必要とするアクセスポイント プラットフォームを推奨します。

Cisco Wireless Phone 840 および 860 の導入に必要な要件が満たされていることを確認するには、ワイヤレス LAN の検証が必要です。

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 Wireless Phone 840 および 860 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 Wireless Phone 840 および 860 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 Wireless Phone 840 および 860 が信号を 5 秒以上保持できるように設計するこ とを推奨します。

チャンネルの使用率

チャンネル使用率レベルは 40 % 未満に維持される必要があります。

<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 Wireless Phone 840 および 860 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があります。

パケット損失/遅延

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

ジッタは最小(100 ms 未満)に維持される必要があります。

再試行回数

802.11 再送信は 20 % 未満である必要があります。

<u>マルチパス</u>

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 Wireless Phone 840 および 860 は、次のコール制御プラットフォームでサポートされています。

• Cisco Unified Communications Manager (CUCM)

最小 = 11.5(1) 推奨 = 12.5(1)、14.0(1) 以降

• Cisco Unified Survivable Remote Site Telephony (SRST)

最小 = 14.1 推奨 = 14.3 以降

Webex Calling

注: Cisco Unified Communications Manager では、Cisco Wireless Phone 840 および 860 デバイスのサポート を有効にするために、デバイスパッケージまたはサービス リリース アップデートのインストールが必要です。 Cisco Unified Communications Manager 用のデバイスパッケージは、次の場所から入手できます。 <u>https://software.cisco.com/download/home/278875240</u>

ワイヤレス LAN

Cisco Wireless Phone 840 および 860 は、次のシスコ 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、8.10.183.0
- Cisco Catalyst IOS XE ワイヤレス LAN コントローラおよび Cisco Lightweight アクセスポイント 最小 = 16.12.1 秒

推奨 = 17.3.6、17.6.4、17.9.3、17.11.1

• 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、8.10.183.0

• Cisco Autonomous(自律)アクセス ポイント

最小 = 15.2(4)JB6 推奨 = 15.3(3)JPO

Cisco Meraki アクセスポイント

最小 = MR 25.9、MX 13.33 推奨 = MR 29.5.1、MX 17.10.2

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 Wireless Phone 840 および 860 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 トされます。





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

Cisco AP シリーズ	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	軽量	Mobility Express	自律型
1540	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1560	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1570	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
1700	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
1810	はい	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
1810W	はい	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ

1815	はい	はい	はい	はい	はい	いいえ	はい	はい(1815t ではありま せん)	いいえ
1830	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1840	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
1850	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
2700	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
2800	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
3700	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい
3800	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
4800	はい	はい	はい	はい	はい	いいえ	はい	はい	いいえ
9105	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9115	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9117	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
9120	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ
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 Wireless IP Phone 840 および 860 は、次の Cisco Meraki アクセス ポイント プラットフォームでサポ ートされます。





https://meraki.cisco.com/products/wireless#models https://meraki.cisco.com/products/appliances#models

次の表に、	各 Cisco	Meraki アク	7セスポイン	゚トでサポー	トされるモ	ードを示します。
-------	---------	-----------	--------	--------	-------	----------

Meraki AP シリーズ	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
MR20	はい	はい	はい	はい	はい	いいえ
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
MR70	はい	はい	はい	はい	はい	いいえ
MR74	はい	はい	はい	はい	はい	いいえ
MR76	はい	はい	はい	はい	はい	はい
MR78	はい	はい	はい	はい	はい	はい
MR84	はい	はい	はい	はい	はい	いいえ
MR86	はい	はい	はい	はい	はい	はい
MX64W	はい	はい	はい	はい	はい	いいえ
MX65W	はい	はい	はい	はい	はい	いいえ
MX67W	はい	はい	はい	はい	はい	いいえ
MX68W	はい	はい	はい	はい	はい	いいえ
Z3	はい	はい	はい	はい	はい	いいえ

注:上に明記されていないアクセスポイントモデルはサポートされません。

Cisco Aironet 1500 シリーズ屋外アクセスポイントのサポートは、ローカル アクセス ポイント モードの みに制限されています。

MESH モードで動作するアクセスポイントモデルはサポートされません。

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

主な機能の一部を以下に示します。

- 5 GHz (802.11a/n/ac)
- Wi-Fi Protected Access v2 (WPA2+AES)
- Wi-Fi マルチメディア (WMM)
- Traffic Specification (TSPEC)
- DiffServ コードポイント (DSCP)
- サービスクラス (CoS/802.1p)

アンテナシステム

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

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

https://www.cisco.com/c/ja_jp/products/collateral/wireless/aironet-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、r、ac
- Wi-Fi マルチメディア (WMM)
- Traffic Specification (TSPEC)
- 不定期自動省電力配信(UAPSD)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
 - \circ Opus, G.722, G.711, G.729
- Dynamic Host Configuration Protocol (DHCP)
- HyperText Transfer Protocol (HTTP/HTTPS)

Wi-Fi

次の表に、Cisco Wireless Phone 840 および 860 で使用される 802.11 モードごとの最大送信電力と データレートを示します。

Cisco Wireless Phone 840

5 GHz の仕様

5 GHz - 802.11a	データレート	空間スト	変調
		リーム	
最大 Tx パワー = 16 dBm	6 Mbps	1	OFDM - BPSK
(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	データレート	空間スト	変調
(H120)		リーム	
最大 Tx パワー = 16 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
(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 Mbp (MCS 13)	2	OFDM - 64 QAM
	130 Mbp (MCS 14)	2	OFDM - 64 QAM
	144 Mbp (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 15 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
最大 Tx パワー = 16 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
(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	空間ストリーム	変調
最大 Tx パワー = 15 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
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM
	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
	300 Mbps (MCS 7)	2	OFDM - 64 QAM

	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)	データレート	空間ストリーム	変調
最大 Tx パワー = 14 dBm	33 Mbps (MCS 0)	1	OFDM - BPSK
(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 - 802.11b	データレート	空間ストリーム	変調
最大 Tx パワー = 19 dBm	1 Mbps	1	DSSS - BPSK
(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 Tx パワー = 18 dBm	6 Mbps	1	OFDM - BPSK
(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 Tx パワー = 18 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
(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

Cisco Wireless Phone 860

5 GHz の仕様

5 GHz - 802.11a	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm	6 Mbps	1	OFDM - BPSK
(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	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK

	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM

	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	30 Mbps (MCS 8)	2	OFDM - BPSK
	60 Mbps (MCS 9)	2	OFDM - QPSK
	90 Mbps (MCS 10)	2	ofdm - qpsk
	120 Mbps (MCS 11)	2	OFDM - 16 QAM
	180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM
	270 Mbps (MCS 14)	2	OFDM - 64 QAM
	300 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11ac (VHT20)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	ofdm - qpsk
	21 Mbps (MCS 2)	1	ofdm - qpsk
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM

	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	87 Mbps (MCS 8)	1	OFDM - 256 QAM
	14 Mbps (MCS 0)	2	OFDM - BPSK
	28 Mbps (MCS 1)	2	ofdm - qpsk
	43 Mbps (MCS 2)	2	OFDM - QPSK
	58 Mbps (MCS 3)	2	OFDM - 16 QAM
	87 Mbps (MCS 4)	2	OFDM - 16 QAM
	116 Mbps (MCS 5)	2	OFDM - 64 QAM
	130 Mbps (MCS 6)	2	OFDM - 64 QAM
	144 Mbps (MCS 7)	2	OFDM - 64 QAM
	173 Mbps (MCS 8)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT40)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	ofdm - qpsk
	45 Mbps (MCS 2)	1	ofdm - qpsk
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM

	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM
	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
	300 Mbps (MCS 7)	2	OFDM - 64 QAM
	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)	データレート	空間ストリーム	変調
最大 Tx パワー = 17 dBm (地域によって異なる)	33 Mbps (MCS 0)	1	OFDM - BPSK
	65 Mbps (MCS 1)	1	ofdm - qpsk
	98 Mbps (MCS 2)	1	OFDM - QPSK
	130 Mbps (MCS 3)	1	OFDM - 16 QAM

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

2.4 GHz - 802.11b	データレート	空間ストリーム	変調
最大 Tx パワー = 19 dBm	1 Mbps	1	DSSS - BPSK
(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 Tx パワー = 17 dBm	6 Mbps	1	OFDM - BPSK
(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 Tx パワー = 16 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
(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: 802.11n/ac 接続を実現するには、Cisco Wireless Phone 840 および 860 をアクセスポイントから約 30 m (100 フィート) 以内に配置することをお勧めします。

規格

ワールドモード(802.11d)では、さまざまな領域でクライアントを使用できます。ローカル環境のアクセスポ イントによってアドバタイズされるチャ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 Wireless Phone 840 および 860 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。

ー部の 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 Wireless Phone 840 および 860 は、まず DFS チャンネルをパッシブにスキャンし、その後でアクティ ブにスキャンします。

802.11d が有効になっていない場合、Cisco Wireless Phone 840 および 860 は、少ない送信電力でアクセス ポイントへの接続を試みることができます。 次に、Cisco Wireless Phone 840 および 860 でサポートされる国とその 802.11d コードを示します。

オーストラリア(AU)	ギリシャ(GR)	ポーランド(PL)
オーストリア(AT)	ハンガリー (HU)	ポルトガル(PT)
ベルギー(BE)	アイスランド(IS)	ルーマニア (RO)
ブルガリア(BG)	アイルランド(IE)	スロバキア(SK)
カナダ(CA)	イタリア(IT)	スロベニア (SI)
クロアチア(HR)	ラトビア(LV)	スペイン(ES)
キプロス (CY)	リヒテンシュタイン(LI)	スウェーデン (SE)
チェコ共和国(CZ)	リトアニア(LT)	スイス (CH)
デンマーク(DK)	ルクセンブルク(LU)	トルコ (TR)
エストニア(EE)	マルタ(MT)	イギリス (GB)
フィンランド(FI)	オランダ(NL)	アメリカ合衆国(US)
フランス(FR)	ニュージーランド (NZ)	
ドイツ (DE)	ノルウェー(NO)	

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

Bluetooth

Cisco Wireless Phone 840 および 860 は、ワイヤレスヘッドセット通信を可能にする Bluetooth テクノロジーをサポートします。

Bluetooth では、約9m (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。ただし、 Bluetooth デバイスは、常に Cisco Wireless Phone 840 および 860 から約3m (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 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 Wireless Phone 840 および 860 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)
- 属性プロファイル (ATT)
- オーディオ / ビデオリモート制御プロファイル (AVRCP)
- デバイス ID プロファイル (DIP)
- 汎用アクセスプロファイル (GAP)
- 汎用属性プロファイル (GATT)
- 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)
- ヘッドセットプロファイル (HSP)
- ヒューマン インターフェイス デバイス プロファイル (HID)
- HID over GATT プロファイル (HOGP)
- メッセージ アクセス プロファイル (MAP)
- オブジェクト プッシュ プロファイル (OPP)
- パーソナル エリア ネットワーク プロファイル (PAN)
- 電話帳アクセス プロファイル (PBAP)
- スキャン パラメータ プロファイル (ScPP)
- シリアルポートプロファイル (SPP)
- サービス検出アプリケーション プロファイル (SDAP)

共存(802.11b/g/n + Bluetooth)

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

<u>キャパシティ</u>

共存 (802.11b/g/n + Bluetooth)を使用する場合、802.11g/n と Bluetooth の送受信を保護する CTS の利用により、コールキャパシティが減少します。

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

言語

Cisco Wireless Phone 840 および 860 は現在、次の言語をサポートしています。

デンマーク語	ドイツ語	ロシア語
オランダ語	ハンガリー語	スロベニア語
英語	イタリア語	スペイン語
フィンランド語	ノルウェー語	スウェーデン語
フランス語	ポルトガル語	

バッテリ寿命

Cisco Wireless Phone 840 には 3040 mAh のバッテリが搭載され、Cisco Wireless Phone 860 には 3000 m Ah のバッテリが搭載されています。

Cisco Wireless Phone 840 および 860 のバッテリ容量は、500 回のフル充電サイクル(空の状態からフル充電)後に 80% 以下になるため、Cisco Wireless Phone 840 および 860 のバッテリは約2年ごとに交換することをお勧めします。

Cisco Wireless Phone 860 はホットスワップ可能なバッテリ機能をサポートしており、最大 60 秒でバッテリ を交換できます。Cisco Wireless Phone 840 にはホットスワップ可能なバッテリ機能は含まれていません。 次の表に、電話機のモデルごとの最大通話時間とアイドル時間を示します。

電話機のモデル	コール状態	バッテリ時間
840 / 840S	通話時	最大 17 時間
	アイドル	最大 168 時間
860 / 860S	通話時	最大 12 時間
	アイドル	最大 120 時間

実際のバッテリ持続時間には、さまざまな要因が影響します。

使用方法

Cisco Wireless Phone 840 または 860 のユーザーが通話中か、ローミング中か、ディスプレイをオンにしているか、Bluetooth やアプリケーションを使用しているか、メッセージを受信しているか、電話機のメニューを操作していると、バッテリ持続時間が短くなります。

<u>カバレッジ</u>

Cisco Wireless Phone 840 および 860 が適切な RF カバレッジエリア内にあり、通話サーバーへの常時接続を 維持できることを確認してください。

Cisco Wireless Phone 840 および 860 のユーザーがカバレッジエリア外で長時間とどまっていると、バッテリ 持続時間が短くなることがあります。

<u>プロキシ ARP</u>

アイドル時のバッテリ持続時間を最適化するために、プロキシ ARP 機能をサポートするアクセスポイントを使用することを推奨します。Cisco Wireless Phone 840 および 860 でプロキシ ARP を使用すると、DTIM 周期のたびに起動する必要がなくなり、サスペンドモードをより長く維持できるため、消費電力が低減されます。 アクセスポイントがプロキシ ARP をサポートしていない場合、Cisco Wireless Phone 840 および 860 ではDTIM 周期のたびに起動が必要になります。これにより、バッテリ持続時間が最大 50 % 短くなります。

送信電力

Cisco Compatible Extensions (CCX) ダイナミック伝送パワーコントロール (DTPC) 機能をサポートするア クセスポイントを使用することを推奨します。DTPC が有効になっている場合、アクセスポイントはその送信電 力をすべてのクライアントにアドバタイズします。これにより、Cisco Wireless Phone 840 および 860 は、接 続先のアクセスポイントとの通信に最小限必要なレベルまで送信電力を調整できます。また、これによって他の エリアの不要なノイズも減少します。

マルチキャスト

Cisco Wireless Phone 840 または 860 がマルチキャストストリームにサブスクライブしている場合、 Cisco Wireless Phone 840 または 860 は DTIM 周期のたびに起動し、マルチキャストフレームを受信す る必要があります。このため、電力消費量が増大します。

省電力プロトコル

アクセスポイントは、通話時やアイドル時に使用される省電力プロトコルである U-APSD をサポートしている 必要があります。

840S および 860S バーコードスキャナ

Cisco Wireless Phone 840S および 860S には、2D バーコードスキャナが搭載されています。 スキャナを呼び出すには、Android アプリケーションが必要です。

Cisco Wireless Phone 840S および 860S は、次のバーコード記号をサポートしています。

 Aztec, CCA EAN-128, CCA EAN-13, CCA EAN-8, CCA GS1 DataBar Expanded, CCA GS1 DataBar Limited, CCA GS1 DataBar-14, CCA UPC-A, CCA UPC-E, CCB EAN-128, CCB EAN-13, CCB EAN-8, CCB GS1 DataBar Expanded, CCB GS1 DataBar Limited, CCB GS1 DataBar-14, CCB UPC-A, CCB UPC-E, CCC EAN-128, Codabar, Code 11, Code 128, Code 32, Code 39 Full ASCII, Code 39 Trioptic, Code 93, DataMatrix, Discrete (Standard) 2 of 5, EAN-128, EAN-13, EAN-13 + 2 Supplemental, EAN-13 + 5 supplemental, EAN-8, EAN-8 + 2 Supplemental, EAN-8 + 5 supplemental, GS1 DataBar Expanded, GS1 DataBar Limited, GS1 DataBar-14, Han Xin, Interleaved 2 of 5, ISBT-128, ISBT-128 Con, Macro Micro PDF, Macro PDF, Macro QR, Matrix 2 of 5, Micro PDF, Micro QR, MSI, PDF-417, QR Code, UPC-A, UPC-A + 2 Supplemental, UPC-A + 5 supplemental, UPC-E0, UPC-E0 + 2 Supplemental, UPC-E0 + 5 supplemental

詳細については、次の URL にある『**Cisco Wireless Phone 840 および 860 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/td/docs/voice ip comm/cuipph/800-series/adminguide/w800 b wireless-800-administration-guide.html

電話機のお手入れ

Cisco Wireless Phone 840 は、IP65 等級の防塵、防滴、防湿性能があります。Cisco Wireless Phone 860 は、IP68 等級の完全な防塵性能を備えています。

通常の清掃の場合は、柔らかい湿った布で電話機を拭くだけでかまいません。

完全にクリーニングするには、過酸化水素水(最大 3%)またはイソプロピル アルコール溶液(最大 91%) を使用することを推奨します。

ブリーチ液(最大 10%)も使用できます。ただし、金属製の充電接点のクリーニングには使用しないでく ださい。

これより多量の純粋なイソプロパノールや、代替となるアルコール ベースの液体が含まれるクリーニング液 は、電話機を傷つける可能性があります。

キャリー ケースを使用すると、電話機の保護をさらに強化し、電話機を落とした場合にも保護されます。

詳細については、次の URL にある『**Cisco Wireless Phone 840 および 860 ユーザーガイド**』を参照 してください。

https://www.cisco.com/content/en/us/td/docs/voice ip comm/cuipph/800-series/userguide/w800 b wireless-800-user-guide.html

アクセサリ

Cisco Wireless Phone 840 および 860 では、次のアクセサリを使用できます。

- バッテリ
- 電話機の電源
- キャリーケース
- ベルトクリップ
- デスクトップチャージャー
- マルチ充電器
- ストラップ(840のみ)
- スキャナハンドル (840Sのみ)


860 充電器



詳細については、『Cisco Wireless Phone 840 および 860 アドミニストレーション ガイド』または 『Cisco Wireless Phone 840 および 860 ユーザーガイド』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800administration-guide.html

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html **注:** シスコでは、Cisco Wireless Phone 840 または 860 のサードパーティ製ケースまたはカバーを推奨、サ ポート、またはテストしていません。Cisco Wireless Phone 840 または 860 でサードパーティ製のケースまた はカバーを使用した場合、保証が無効となる場合があります。

無線 LAN の設計

Cisco Wireless Phone 840 および 860 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

次のガイドラインに従ってワイヤレス LAN を導入し、設定します。

5 GHz (802.11a/n/ac)

Cisco Wireless Phone 840 および 860 の運用では、5 GHz の周波数帯域を使用することを推奨します。

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 Wireless Phone 840 および 860 は、802.11h の動的周波数選択(DFS)と伝送パワーコントロール (TPC)をサポートします。これらは、5.260 ~ 5.720 GHz で動作するチャンネルを使用する場合に必要です。 使用可能な 25 チャンネルのうち 16 チャンネルがこれに該当します。

802.11a/n/ac 環境に Cisco Wireless Phone 840 および 860 を導入する場合は、隣接するチャンネルと 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 Wireless Phone 840 および 860 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 か所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。





動的周波数選択 (DFS)

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

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

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

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

レーダーアクティビティに備えて、非 DFS チャネル (UNII-1)を使用するアクセスポイントをエリアごとに少なくとも 1 つ設置します。これにより、新しい使用可能チャ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。



最小 20% のオーバーラップ

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

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

UNII-2 拡張チャネル(チャネル 100 ~ 144)の使用を予定している場合は、アクセス ポイント上で UNII-2 (チャネル 52 ~ 64)を無効にして、有効になるチャネルの数が多くなり過ぎないようにすることが推奨され ます。

ワイヤレス LAN で多数の 5 GHz チャネルを有効にすると、新しいアクセス ポイントの検出が遅れる可能 性があります。

2.4 GHz (802.11b/g/n)

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

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

2.4 GHz(802.11b/g/n)環境では、VoWLAN を導入するとき、オーバーラップのないチャネルだけを利用する 必要があります。オーバーラップのないチャネルには 22 MHz の間隔があり、少なくとも 5 チャネル離れてい ます。

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

802.11b/g/n 環境に Cisco Wireless Phone 840 および 860 を導入する場合は、オーバーラップのないチャン ネルを使用する必要があり、隣接チャンネルとのオーバーラップが少なくとも 20% 許容される必要がありま す。これにより、シームレスなローミングが実現します。

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



次に、2.4 GHz ワイヤレス LAN の導入例を示します。



最小 20% のオーバーラップ

信号強度とカバレッジ

Cisco Wireless Phone 840 および 860 で最低限の音声品質を確保するには、5 GHz または 2.4 GHz で常に -67 dBm 以上の信号レベルを保持する必要があります。アクセスポイントの受信感度については、送信データレ ートに対して要求される信号レベルも満たしている必要があります。

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

ほとんどの電子レンジ、Bluetooth、および周波数ホッピング デバイスは、5 GHz 周波数に対しても同様の悪影 響を与えることはありません。802.11a/n/ac テクノロジーでは、オーバーラップのないチャネルが増えるた め、通常はより低い初期 RF 使用率となります。音声導入の場合、音声には 802.11a/n/ac を使用し、データに は 802.11b/g/n を使用することを推奨します。

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



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

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

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



データ レート

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

Cisco Wireless Phone 840 および 860 には、両方ともデュアルアンテナがあるため、802.11n(最大 300 Mbps)の最大 MCS 15 データレートをサポートします。

802.11ac の場合、Cisco Wireless Phone 840 および 860 は、最大 VHT80 MCS 9 2SS データレート (最大 867 Mbps) をサポートします。

これより高い MCS レートを使用できる、同じ帯域周波数を使って MIMO(複数入力/出力)アンテナ テクノロ ジーを利用する他の 802.11n/ac クライアント向けに、より高いレートを有効にしておくことができます。

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

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

802.11 モード	必須データレート	サポートされているデー タ レート	無効化された データレート
802.11a/n/ac	12 Mbps	18 ~ 54 Mbps、	6、9 Mbps
		VHT MCS 0 - MCS 9 1SS、	
		VHT MCS 0 - MCS 9 2SS、	
		(VHT MCS 0 - MCS 9 3SS) 、	
		(VHT MCS 0 - MCS 9 4SS)	
802.11a/n	12 Mbps	18 ~ 54 Mbps、	6、9 Mbps
		HT MCS 0 - MCS 15、	
		(HT MCS 16 - MCS 31)	
802.11g/n	12 Mbps	18 ~ 54 Mbps,	1、2、5.5、6、
		HT MCS 0 - MCS 15、	9、11 Mbps
		(HT MCS 16 - MCS 31)	
802.11b/g/n	11 Mbps	12 ~ 54 Mbps、	1、2、5.5、6、
		HT MCS 0 - MCS 15、	9 Mbps
		(HT MCS 16 - MCS 31)	
802.11a	12 Mbps	18 ~ 54 Mbps	6、9 Mbps
802.11g	12 Mbps	18 ~ 54 Mbps	1、2、5.5、6、
			9、11 Mbps
802.11b/g	11 Mbps	12 ~ 54 Mbps	1、2、5.5、6、 9 Mbps
802.11b	11 Mbps	なし	1、2、5.5 Mbps

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

ビデオなどの他のアプリケーションでは、24 Mbps よりも高いデータ レートを有効にすると、恩恵が受けられ る場合があります。

高いキャパシティとスループットを維持するには、24 Mbps 以上のデータ レートを有効にしてください。

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

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

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

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

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

条件の厳しい環境

Cisco Wireless Phone 840 および 860 を条件の厳しい環境(製造、倉庫、小売業など)に導入する場合、標準の推奨事項に追加の調整が必要となる場合があります。

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

アクセス ポイントおよびアンテナの選択

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

アクセス ポイントの配置

Cisco Wireless Phone 840 または 860 とアクセスポイント間の障害物を最小限にし、アクセスポイントのアンテナからのラインオブサイトを確保することが重要です。アクセス ポイントまたはアンテナ、またはその両方が障害物の背後または金属面やガラス面の近くに配置されていないことを確認します。

一部のエリアで一体型内部アンテナを搭載したアクセス ポイントを使用する場合は、アクセス ポイント を天井に取り付けることを推奨します。これらのアクセス ポイントは無指向性アンテナを装備してお り、壁面への設置を想定していません。

周波数帯域

これまで通り、5 GHz の使用が推奨されます。2.4 GHz を使用すると、正常に機能しない場合があります。802.11b レートが有効な場合は特に注意が必要です。

5 GHz チャネル セットでは、8 または 12 チャネル計画のみを使用することを推奨します。可能な場合 は、UNII-2 拡張チャネルを無効にします。

<u>データ レート</u>

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 Wireless Phone 840 および 860 の送信電力も制限する必要があります。これは、条件の厳しい環境に 2.4 GHz を導入しようと計画している場合にさらに重要です。

自動送信電力を使用する場合は、アクセス ポイントの送信電力が指定した範囲(最大および最小の電力 レベル)を使用するように設定して、アクセス ポイント出力の過不足を防ぎます(5 GHz の場合、最低 11 dBm、最小 16 dBm)。

Cisco Wireless Phone 840 および 860 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)

音声およびコール制御フレームの WMM UP タグが正しく設定されるように、DSCP 値が有線ネットワ ーク全体で保持されることを確認する必要があります。

ビームフォーミング

Cisco 802.11n 対応アクセス ポイントを使用している場合は、ビーム フォーミング (ClientLink) を有効にする必要があります。これは、クライアントからの電波の受信に役立ちます。

マルチパス

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

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

異なる波形を組み合わせると歪みが発生し、信号品質が低下するため、受信機のデコード機能にも悪影響を与えます。 マルチパスは、反射面(金属やガラスなど)の存在する環境で発生する場合があります。このような反射面に は、アクセス ポイントを取り付けないでください。

次に、マルチパスの影響を示します。

データ破損

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

信号の空白

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

信号振幅の増大

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

信号振幅の減少

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



802.11a/n/ac と 802.11g/n で使用される直交周波数分割多重方式(OFDM)を使用することで、高マルチパス 環境に見られる問題が軽減される場合があります。

高マルチパス環境で 802.11b を使用する場合、それらのエリアには低いデータ レートを使用してください (1 Mbps や 2 Mbps など)。

このような環境には、ダイバーシティ アンテナが役立つことがあります。

セキュリティ

ワイヤレス LAN を導入する場合、セキュリティが不可欠です。

Cisco Wireless Phone 840 および 860 は、次のワイヤレスセキュリティ機能をサポートしています。

WLAN 認証

- WPA2 (802.1x 認証)
- WPA2-PSK (事前共有キー)
- 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)

- 802.11r/Fast Transition (FT)
- CCKM (Cisco Centralized Key Management)
- なし

WLAN 暗号化

• AES (Advanced Encryption Standard)

注: WPA3 はサポートされていません。 802.1x-SHA2 キー管理はサポートされていません。 CCMP256、GCMP128、および GCMP256 暗号化方式はサポートされていません。

Cisco Wireless Phone 840 および 860 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
- Secure Cisco Unified SRST
- 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-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 Wireless Phone 840 または 860 にインポートされた証明書の共通名と一致する認証サ ーバー上に、ユーザーアカウントを作成する必要が生じることがあります。 このユーザ アカウントには複雑なパスワードを使用し、RADIUS サーバ上で有効にする EAP タイプは EAP-TLS のみにすることを推奨します。

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

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

EAP-TTLS-GTC、EAP-TTLS-MSCHAP、EAP-TTLS-MSCHAPv2、および EAP-TTLS-PAP は、サポートされ ている内部認証プロトコルです。

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、証明書を Cisco Wireless Phone 840 および 860 にインポートすることで検証できます。

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-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、証明書を Cisco Wireless Phone 840 および 860 にインポートすることで検証できます。

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を優先できます。

音声トラフィックおよびコール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。
- QoS ポリシーを作成し、アクセス ポイント上で音声トラフィックとコール制御トラフィック を優先させます。

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	EF (46)	5	6	RTP (UDP 16384 - 32767)		
	Webex Calling	EF (46)	5	6	RTP (UDP 19560 ~ 65535)		
コール制御	CUCM	CS3 (24)	3	4	SIP (TCP 5060 ~ 5061)		
	Webex Calling	CS3 (24)	3	4	SIP (TCP 8934)		

- 音声パケットおよびコール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 Wireless Phone 840 および 860 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 Calling のネットワーク要件については、次の URL にある『**Port Reference Information for Webex Calling**』ドキュメントを参照してください。

https://help.webex.com/en-US/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

コール アドミッション制御 (CAC)

アクセス ポイントでコール アドミッション制御を有効化できます。

- 音声用のコール アドミッション制御/Wi-Fi MultiMedia Traffic Specification (TSPEC) を有効にします。
- 音声トラフィック用に割り当てられる最大 RF 帯域幅を設定します(デフォルト = 75 %)。
- ローミング音声クライアント用に予約する帯域幅を設定します(デフォルト=6%)。

Pre-Call アドミッション制御

コール アドミッション コントロールがアクセスポイント上で有効な場合、Cisco Wireless Phone 840 および 860 は、Add Traffic Stream(ADDTS)をアクセスポイントに送信して、コールを発信または受信するための 帯域幅を要求します。

AP が ADDTS 成功メッセージを送信すると、Cisco Wireless Phone 840 または 860 はコールを確立します。 アクセスポイントがコールを拒否し、Cisco Wireless Phone 840 または 860 のローミング先となるアクセスポ イントが他に存在しなければ、電話機に「**ネットワークがビジーです(Network Busy)**」と表示されます。 インバウンドコールに対してアドミッションが拒否されても、コールを確立するために必要な帯域幅が不足して いることを Cisco Wireless Phone 840 または 860 からリモートエンドポイントに通知することはありません。 そのため、リモートユーザーがコールを終了するまで、コールが要求され続ける可能性があります。

ローミング アドミッション制御

通話中、Cisco Wireless Phone 840 および 860 は、現在のアクセスポイントおよび利用可能なすべてのアクセ ス ポイントの Received Signal Strength Indicator (RSSI) と Packet Error Rate (PER)の値を測定して、ロ ーミングに関する決定を行います。

コールが確立されていた元のアクセスポイントでコール アドミッション コントロールが有効になっていた場 合、Cisco Wireless Phone 840 および 860 はローミング時に ADDTS 要求を新しいアクセスポイントに送信し ます。これは、再アソシエーション要求フレームに埋め込まれます。

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。

<u>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</u>

mls qos ! interface X mls qos trust cos

Cisco 製アクセス ポイントに対して DSCP 信頼状態を有効にする

mls qos ! interface X mls qos trust dscp

Cisco Meraki MS スイッチを使用する場合は、『**Cisco Meraki MS Switch VoIP 導入ガイド**』を 参照してください。

https://meraki.cisco.com/lib/pdf/meraki whitepaper msvoip.pdf

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

有線 IP フォンの Cisco スイッチ ポートの設定

Cisco 製の有線 IP フォンのスイッチ ポートで Cisco 製電話機の信頼状態を有効にします。

スイッチ設定の例を次に示します。

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

ローミング

Cisco Wireless Phone 840 および 860 では、802.11 モードがデフォルトで「自動」に設定されています。こ れにより、Cisco Wireless Phone 840 および 860 が 5 GHz または 2.4 GHz のいずれかに接続でき、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/Fast Transition (FT) は、頻繁にローミングが発生するすべての種類の環境で推奨される導入モデルです。

CCKM を使用するには、802.1x 認証が必要です。

802.11r (FT) または CCKM 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。WPA2 では、一時的なキーが追加されるため、ローミング時間が長くなる可 能性があります。

802.11r (FT) または CCKM を使用すると、ローミング時間を 100 ミリ秒未満に短縮できます。この場合、 アクセスポイント間の移行時間をユーザーが体感することはありません。

Cisco Wireless Phone 840 および 860 では、WPA2 (AES) または WPA2-PSK (AES) を使用する 802.11r (FT) と WPA2 (AES) を使用する CCKM がサポートされます。

認証	ローミング時間
WPA2 パーソナル	150 ミリ秒
WPA2 エンタープライズ	300 ミリ秒
802.11r (FT)	100 ミリ秒未満
ССКМ	100 ミリ秒未満

Cisco Wireless Phone 840 および 860 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。

シームレスなローミングを実現するため、Cisco Wireless Phone 840 および 860 は、少なくとも 3 秒間アク セスポイントに関連付けられる必要があります。そうでない場合、パケット損失(最大 tx 回の再送信数または ビーコン受信の失敗数)の発生に基づいてローミングが発生する可能性があります。

高速セキュア ローミング (FSR)

802.11r/Fast Transition (FT) は、頻繁にローミングが発生するすべての種類の環境で推奨され る導入モデルです。

Cisco Centralized Key Management (CCKM) もサポートされていますが、802.1x 認証が必要です。

802.11r (FT) と CCKM は、高速セキュア ローミングを可能にし、ネットワーク非接続時間を抑制して、通話 中のオーディオ ギャップを最小限に抑えます。

802.11r (FT)を使用しない 802.1x または PSK と、CCKM 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。WPA2 では、一時的なキーが追加されるた め、ローミング時間が長くなる可能性があります。

802.11r (FT) と CCKM はキー管理を一元化して、キー交換の回数を減らします。

802.11r (FT) または CCKM を使用すると、ローミング時間を 400 ~ 500 ミリ秒から 100 ミリ秒未満に短縮 できます。この場合、アクセス ポイント間の移行時間をユーザが体感することはありません。 802.11r (FT) ローミングには次の2つの方式があります。

Over the Air

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

Over the Distribution

クライアントは、現在のアクセス ポイント経由でターゲット アクセス ポイントと通信します。クライ アントとターゲット アクセス ポイントの間の通信は、WLAN コントローラを介してクライアントと現 在のアクセス ポイントとの間で FT アクション フレームを介して伝送されます。

802.11r (FT) では、高速セキュア ローミング モデルとして、Over the Air 方式の使用が推奨されます。

802.11r (FT) と Over the Distribution 方式の組み合わせを使用する場合は、現在関連付けられているアクセス ポイントへの接続が必要になるため、現在のアクセス ポイントやターゲット アクセス ポイントと必ずしも通信 できるとは限らない状況では適切に動作しない可能性があります。このような状況は、閉鎖環境においてローミ ング イベントが発生したときに、現在のアクセス ポイントとターゲット アクセス ポイントの両方へのライン オブ サイトを保持できない場合に発生する可能性があります。

Cisco Wireless Phone 840 および 860 では、WPA2-PSK または WPA2 を使用する 802.11r (FT) と、WPA2 または WPA を使用する CCKM がサポートされます。

FSR タイプ	認証	キーの管理	暗号化
802.11r (FT)	PSK	WPA2	AES
802.11r (FT)	EAP-TLS	WPA2	AES
802.11r (FT)	EAP-TTLS	WPA2	AES
802.11r (FT)	PEAP	WPA2	AES
ССКМ	EAP-TLS	WPA2	AES
ССКМ	EAP-TTLS	WPA2	AES
ССКМ	PEAP	WPA2	AES

注: Cisco Wireless Phone 840 または 860 を導入する環境に他の Wi-Fi 電話機が存在し、それらの電話機が 802.11r (FT) をサポートしていない場合は、既存の同じ SSID を Cisco Wireless Phone 840 または 860 に使 用できます。ただし(他の Wi-Fi 電話機が 802.11r (FT)を使用せず、802.11r (FT)対応ネットワークで相互 運用可能である限り)、他の既存のキー管理タイプ(802.1x、CCKM、802.1x + CCKM など)に加えて、Over the Air 方式を使用する 802.11r (FT) を有効にすることを推奨します。

帯域間のローミング

Cisco Wireless Phone 840 および 860 では、周波数帯域モードがデフォルトで「自動」に設定されています。 自動モードではインターバンドローミングが有効になり、最も強い信号を優先します。電力レベルが同じである 場合、一般的に信号強度のより強い 2.4 GHz が 5 GHz よりも優先されます。

電源オン時に Cisco Wireless Phone 840 および 860 が自動モードであれば、すべての 2.4 GHz チャネルと 5 GHz チャネルをスキャンした後、設定済みネットワーク用のアクセスポイント(使用可能な場合)への関連付 けを試みます。

5 GHz のみまたは 2.4 GHz のみモードに設定されている場合、これらのチャネルだけがスキャンされます。

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

電源管理

Cisco Wireless Phone 840 および 860 は、Wi-Fi Multimedia (WMM) がアクセスポイントの設定で有効であ るかどうかに応じて、U-APSD の省電力方式を使用します。

アクセスポイントが プロキシ ARP をサポートしていない場合、アイドル時のバッテリ持続時間は最大 50 % 短 くなります。

Cisco Wireless Phone 840 および 860 は、アイドル時または通話時に主に U-APSD 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)

Cisco Wireless Phone 840 および 860 は、ユニキャストパケット、ブロードキャストパケット、およびマルチ キャストパケットをチェックする起動周期をスケジューリングするために、DTIM 周期を使用します。

プロキシ ARP が有効になっている場合、Cisco Wireless Phone 840 および 860 は DTIM 時に起動する必要は ありません。

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。

DTIM 周期は、バッテリ持続時間とマルチキャスト パフォーマンスの間でトレードオフの関係になっています。 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。

ダイナミック伝送パワー コントロール (DTPC)

Cisco Wireless Phone 840 または 860 とアクセスポイント間で正常にパケットを交換するには、ダイナミック 伝送パワーコントロール (DTPC) を有効にする必要があります。

DTPC により、RF トラフィックが一方向のみに聞こえる場合に一方向オーディオを防止できます。

アクセスポイントで DTPC がサポートされていない場合、Cisco Wireless Phone 840 および 860 は、現在の チャンネルおよびデータレートに応じて使用可能な最大送信電力を使用します。

アクセスポイントの無線送信電力は、Cisco Wireless Phone 840 および 860 がサポートできる送信電力を超え ないようにしてください。

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。

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

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

音声通話(Audio Calls)

次に、アクセスポイント/チャンネルごとにサポートされる音声通話(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	802.11 モード	オーディオ	オーディオ ビ	データレー
の最大致		」ーテック	ットレート	4
13	5 GHz または	G.722/G.711	64 Kbps	6 Mbps
	2.4 GHz			
20	5 GHz または	G.722/G.711	64 Kbps	12 Mbps
	2.4 GHz			
27	5 GHz または G.722/G.711		64 Kbps	24 Mbps 以上
	2.4 GHz			

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。

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 Wireless Phone 840 および 860 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せます。

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

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

Cisco ワイヤレス LAN の設定

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

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

- [802.11r (FT)]または [CCKM] が [有効 (Enabled)]になっていることを確認します。
- [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 を [有効 (Enabled)] に設定することを推奨
- 802.11v を有効に設定することを推奨
- [セッションタイムアウト (Session Timeout)]が有効で、正しく設定されていることを確認します
- [キーのブロードキャスト間隔 (Broadcast Key Interval)]が有効になっていて、正しく設定されてい ることを確認します
- [Aironet IE] が [有効 (Enabled)] になっていることを確認します
- [DTPC サポート (DTPC Support)]を[有効 (Enabled)]に設定します。

- [P2P (ピアツーピア) ブロッキング アクション (P2P (Peer to Peer) Blocking Action)] を 無効にします。
- [クライアント除外 (Client Exclusion)]が正しく設定されていることを確認します
- [DHCP アドレス割り当て必須 (DHCP Address Assignment Required)]を無効にします。
- [保護された管理フレーム (PMF) (Protected Management Frame (PMF)]は、[任意 (Optional)]または[無効 (Disabled)]に設定する必要があります
- [MFP クライアント保護 (MFP Client Protection)]を[任意 (Optional)]または[無効 (Disabled)]に設定します
- [DTIM 周期 (DTIM Period)] を [2] に設定します
- [クライアントの負荷分散 (Client Load Balancing)]を[無効 (Disabled)]に設定します
- [クライアントの帯域選択 (Client Band Select)]を[無効 (Disabled)]に設定します
- [IGMP スヌーピング (IGMP Snooping)] を [有効 (Enabled)] に設定します
- レイヤ3モビリティを使用している場合は、[シンメトリックモバイルトンネリングモード (Symmetric Mobile Tunneling Mode)]を有効にします
- Cisco 802.11n 対応のアクセスポイントを使用している場合は、[クライアントリンク (ClientLink)]
 を有効にします
- 必要に応じて [データレート (Data Rates)]を設定します
- 必要に応じて [自動 RF (Auto RF)]を設定します
- [ボイス (Voice)]で、[アドミッション制御必須 (Admission Control Mandatory)]を[有効 (Enabled)]に設定します。
- [ボイス (Voice)]で [ロードベース CAC (Load Based CAC)]を [有効 (Enabled)]に設定します。
- [ボイス (Voice)]で[トラフィック ストリーム メトリック (Traffic Stream Metrics)]を有効にします。
- [ビデオ (Video)]で[アドミッション制御必須 (Admission Control Mandatory)]を[無効 (Disabled)]に設定します。
- [EDCA プロファイル (EDCA Profile)]を[音声の最適化 (Voice Optimized)]または[音声およびビデオの最適化 (Voice and Video Optimized)]に設定します
- [低遅延 MAC を有効にする (Enable Low Latency MAC)]を[無効 (Disabled)]に設定します
- [電力制限 (Power Constraint)]が [無効 (Disabled)]になっていることを確認します。
- [チャンネル通知 (Channel Announcement)]および [チャンネル静音モード (Channel Quiet Mode)]を有効にします
- 必要に応じて[高スループットデータレート (High Throughput Data Rates)]を設定します
- [フレームの集約 (Frame Aggregation)] 設定を設定します
- CleanAir テクノロジーを搭載した Cisco 製アクセス ポイントを使用している場合は、[CleanAir] を有効にします。

- 必要に応じて [マルチキャストダイレクト機能 (Multicast Direct Feature)]を設定します
- 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 Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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

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

[DTPC サポート (DTPC Support)]が有効になっていることを確認します。

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

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

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

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ON	TROLLER W <u>I</u> RELESS	<u>s</u> ecurity	M <u>a</u> nagement c	C <u>o</u> mmands I	HELP	<u>F</u> EEDBACK
Wireless	802.11a Global Parame	eters					
 Access Points All APs Radios 	General			Data Rates**			_
Global Configuration	802.11a Network Status	Enabled		6 Mbps	Disa	bled	0
Advanced	Beacon Period (millisecs)	100		9 Mbps	Disa	bled	0
Mesh	Fragmentation Threshold (bytes)	2346		12 Mbps	Man	datory	٥
AP Group NTP	DTPC Support.	Enabled		18 Mbps	Supp	ported	٥
ATE	Maximum Allowed Clients	100		24 Mbps	Supp	ported	٥
PE Profiles	RSSI Low Check	Enabled		36 Mbps	Supp	ported	٥
FlexConnect Groups	RSSI Threshold (-60 to -90	-80		48 Mbps	Supp	ported	\$
FlexConnect ACLs	802.11a Band Status			54 Mbps	Supp	ported	0
FlexConnect VLAN Templates	Low Band	Enabled		CCX Location M	leasurement		
Network Lists	Mid Band	Enabled		Mode	🗹 Ena	abled	
▼ 802.11a/n/ac/ax	High Band	Enabled		Interval (seconds	s) 60		
Network RRM				TWT Configurat	tion ***		
RF Grouping				Target Waketime	e 🗹 Ena	abled	
TPC DCA				Broadcast TWT S	Support 🗹 Ena	abled	

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

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

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

[DTPC サポート (DTPC Support)]が有効になっていることを確認します。

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

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

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

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

ululu cisco	MONITOR WLANS CONT	ROLLER W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP FEED	DBACK
Wireless	802.11b/g Global Param	eters					
 Access Points All APs Radios 	General			Data Rates*	*		
Global Configuration	802.11b/g Network Status	Enabled		1 Mbps	Dis	abled ᅌ	
Advanced	802.11g Support	Enabled		2 Mbps	Dis	abled ᅌ	
Mesh	Beacon Period (millisecs)	100		5.5 Mbps	Dis	abled ᅌ	
AP Group NTP	Short Preamble	Enabled		6 Mbps	Dis	abled ᅌ	
> ATF	Fragmentation Threshold	2346]	9 Mbps	Dis	abled ᅌ	
PE Profiles	DTPC Support.	Enabled		11 Mbps	Dis	abled ᅌ	
FlexConnect Groups	Maximum Allowed Clients	100		12 Mbps	Ma	ndatory ᅌ	
FlexConnect ACLs	RSSI Low Check	Enabled		18 Mbps	Su	pported ᅌ	
FlowConnect V/LAN	RSSI Threshold (-60 to -90	-80	24 Mbps		Su	Supported ᅌ	
Templates	dBm)			36 Mbps	Su	pported ᅌ	
Network Lists	CCX Location Measurem	ent		48 Mbps	Su	pported ᅌ	
▶ 802.11a/n/ac/ax	Mode	Enabled		54 Mbps	Su	pported ᅌ	
 802.11b/g/n/ax Network 	Interval (seconds)	60		TWT Configu	ration ***		
▼ RRM				Target Waket	ime	~	Enabled
RF Grouping TPC				Broadcast TW	T Support	<	Enabled

ビームフォーミング (ClientLink)

Cisco 802.11n 対応のアクセスポイントを、[クライアントリンク (ClientLink)]を有効にします。

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

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

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

次のコマンドを使用して、ビーム フォーミング機能の現在のステータスを表示できます。

(Cisco Controller) > show 802.11a

(Cisco Controller) > show 802.11b

Legacy Tx Beamforming setting......有効

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMEN	r c <u>o</u> mmands he <u>l</u> p <u>f</u> eedba	лск		
Wireless	802.11a/n/ac/ax Cisco APs > C	onfigure				
Access Points All APs All APs Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Global Configuration Advanced	General A ^P Name Admin Status Operational Status Slot #	rtp9-31a-ap1 Enable 0 UP 1	RF Channel Assignment Current Channel Channel Width * * Channel width can be configur mode Assignment Method	(48,44) 40 MHz C ed only when channel configuration is in custom		
AP Group NTP	11n Parameters			Custom		
ATF RF Profiles	11n Supported	Yes	Radar Information			
FlexConnect Groups	CleanAir		Channel Las	t Heard(Secs)		
FlexConnect ACLs FlexConnect VLAN Templates	CleanAir Capable CleanAir Admin Status	Yes Enable	No radar detected channels Tx Power Level Assignment			
Network Lists 802.11a/n/ac/ax 802.11b/g/n/ax Media Stream	* CleanAir enable will take effect only Number of Spectrum Expert connections Antenna Parameters	if it is enabled on this band. O	Current Tx Power Level Assignment Method	1 Global Custom		
Application Visibility And Control Lync Server Country	Antenna Type Antenna	Internal O A Ø C Ø D Ø	Performance Profile View and edit Performance Pro	ofile for this AP		
Timers Netflow QoS			Note: Changing any of the parai and thus may result in loss of co	meters causes the Radio to be temporarily disabled nnnectivity for some clients.		

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。

 cısco	MONITOR WLANS CONTROLLER WIRELESS	<u>S</u> ECURITY M <u>A</u> NAGEMEN	T C <u>o</u> mmands He <u>l</u>	P <u>F</u> EEDBACK
Wireless	802.11a > RRM > Tx Power Control(TPC)			
Access Points All APs Radios Global Configuration Advanced	TPC Version Interference Optimal Mode (TPCv2) Coverage Optimal Mode (TPCv1) Tx Power Level Assignment Algorithm			
Mesh AP Group NTP	Power Level Assignment Method		OAutomatic	Every 600 sec:
ATF			On Demand	Invoke Power Update Once
RF Profiles FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates Network Lists 802.11a/n/ac/ax Network RRM RF Grouping TPC DCA Coverage General	Maximum Power Level Assignment (-10 to 30 dBm) Minimum Power Level Assignment (-10 to 30 dBm) Power Assignment Leader Last Power Level Assignment Power Threshold (-80 to -50 dBm) Channel Aware Power Neighbor Count		Fixed 17 11 RTP9-32A-WLC3 (1 463 secs ago -65 Enabled 3	1 0.81.6.70)

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

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

uluili. cisco	<u>M</u> ONITOR	<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	
Wireless	802.11a >	02.11a > RRM > Dynamic Channel Assignment (DCA)								
Access Points All APs	Dynamic	Channel	Assignment A	lgorithm						
 Radios Global Configuration 	Channel A	Assignment	Method	 Automatic 	Interval:	10 minutes ᅌ	AnchorTime: 0	\$		
Advanced				Freeze	Invoke	Channel Update	Once			
Mesh				OFF						
AP Group NTP	Avoid For	eign AP inte	erference	Enabled						
ATE	Avoid Cise	co AP load		Enabled						
PE Profiles	Avoid non	n-802.11a r	noise	Enabled						
RF Profiles	Avoid Per	sistent Non	-WiFi Interference	e Enabled RTP9-32A-WLC3 (10.81.6.70)						
FlexConnect Groups	Channel A	Assignment	Leader							
FlexConnect ACLs	Last Auto	Channel A	ssianment	556 secs ago						
FlexConnect VLAN Templates	DCA Chan	nnel Sensiti	vity	Medium ᅌ	(15 dB)					
Network Lists	Channel V	Vidth		🔾 20 MHz 📀	40 MHz ()80	MHz 🗌 160 MHz 🤇	80+80 MHz 0	Best		
802.11a/n/ac/ax	Avoid che	ck for non-	DFS channel	Enabled						
Network RRM	DCA Chan	nel List								
RF Grouping TPC DCA Coverage General Client Roaming Media EDCA Parameters	DCA Chan	nnels	36, 40, 44, 157, 161	48, 52, 56, 60,	64, 100, 153,	li				

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

2.4 GHz 帯域で使用可能なチャネルの数が限られているために、40 MHz に対応した Cisco 製の 802.11n アク セス ポイントを使用する場合でも、20 MHz には 2.4 GHz チャネルを設定することを推奨します。

iiļiiiļii 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	802.11b >	RRM >	Dynamic Cha	nnel Assigr	nment (DC	A)			
Access Points All APs	Dynamic	Channel	Assignment A	lgorithm					
 Radios Global Configuration 	Channel A	Assignment	Method	 Automatic 	Interval:	10 minutes ᅌ	AnchorTime: 0	٥	
Advanced				Freeze	Invoke	Channel Update	Once		
Mesh				OFF					
AP Group NTP	Avoid For	eign AP int	erference	Enabled					
▶ ATF	Avoid Cis	co AP load		Enabled					
RF Profiles	Avoid nor	n-802.11b r	noise	Enabled					
FlexConnect Groups	Avoid Per	sistent Non	-WiFi Interference	Enabled					
FlexConnect ACLs	Channel A	Assignment	Leader	RTP9-32A-WL	C3 (10.81.6.7	0)			
ElexConnect VLAN	Last Auto	Channel A	ssignment	75 secs ago					
Templates	DCA Char	nnel Sensiti	vity	Medium ᅌ	(10 dB)				
Network Lists	DCA Char	nel List							
802.11a/n/ac/ax									
 802.11b/g/n/ax Network RRM RF Grouping TPC DCA Coverage 	DCA Char	nnels	6, 11		ţi.				

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

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

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

راریاں cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	C <u>o</u> mmands he <u>l</u> p <u>f</u> ee	DBACK
Wireless	802.11a/n/ac/ax Cisco APs > Cor	nfigure		
 Access Points All APs Radios 	General		RF Channel Assignme	ent
802.11b/g/n/ax Dual-Band Radios Global Configuration	AP Name Admin Status	rtp9-31a-ap1 Enable ᅌ	Current Channel Channel Width *	(48,44) 40 MHz 3 fraured only when channel configuration is in custom
Advanced Mesh	Slot #	1	<i>mode</i> Assignment Method	Global
AP Group NTP	11n Parameters		- Dedau Tufannatian	Custom
RF Profiles	11n Supported	Yes		
FlexConnect Grou	s CleanAir		Channel	Last Heard(Secs)
 FlexConnect ACLs FlexConnect VLAN Templates 	CleanAir Capable CleanAir Admin Status	Yes Enable	No radar detected channels	Inment
Network Lists	* CleanAir enable will take effect only if	f it is enabled on this band.	Current Tx Power Level	1
 802.11a/n/ac/ax 802.11b/g/n/ax 	Number of Spectrum Expert connections	0	Assignment Method	Global
Media Stream	Antenna Parameters		_	Custon
Application Visibil	ty Antenna Type	Internal ᅌ A 🗸	Performance Profile	
Lync Server	Antenna	B 🗹 C 🗹	View and edit Performan	ce Profile for this AP
Country		D 🗹	Performance Profile	1
Timers			Note: Changing any of the p	parameters causes the Radio to be temporarily disabled
Netflow			and thus may result in loss	of connectivity for some clients.
▶ QoS				

クライアントのローミング

Cisco Wireless Phone 840 および 860 は、シスコ 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電話機側が独立して管理します。

EDCA パラメータ

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

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

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

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
Wireless											
Access Points All APs	General										
Radios Global Configuration	EDCA Pro	file		Voice	Voice & Video Optimized						
Advanced	Enable Lo	ow Latency	MAC 1								
Mesh											
AP Group NTP	Low Istency	Mac featur	a is not supported	for 1140/1250	/3500 platform	is if more than 3 da	ta rates are enal	led			
▶ ATF	Low latency	mac reatur	e is not supported	10/ 11+0/1250	ssoo placionn	is in more than 5 da		neu.			

DFS (802.11h)

Cisco Wireless Phone 840 および 860 では送信電力の制御に DTPC が使用されるため、[電力制限 (Power Constraint)]を未設定のままにするか、0 dBm に設定します。

最新バージョンのシスコ ワイヤレス LAN コントローラでは、TPC(電力制限)とダイナミック伝送パワーコン トロール(DTPC)の両方を同時に有効にすることはできません。

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

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELES	5 <u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11h GI	obal Pa	arameters						
 Access Points All APs Radios Global Configuration 	Local Power	straint r Constrai	int(0-30)	0 0	в				
Advanced	Channel Sv	vitch Aı	nnouncement						
Mesh AP Group NTP ATF	Channel An Channel Sw	nouncem vitch Cour	ent ht	0					
RF Profiles FlexConnect Groups	Radar Blac	klist							
FlexConnect ACLs	Smart DFS								

高スループット (802.11n/ac)

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

802.11ac データレートは5GHzにのみ適用できます。

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

Cisco Wireless Phone 840 および 860 は、HT MCS 0 ~ MCS 15 と VHT MCS 0 ~ MCS 9 1SS および 2SS データレートのみをサポートしますが、MIMO アンテナテクノロジーを含む同じ帯域を利用する他の 802.11n/ac クライアントが存在するため、より高いレートが利用可能な場合には、オプションでより高い MCS レートを有効にできます。

.։ ։ cis	ւի. co	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDB	ACK	
Wireless		802.11n/a	nc/ax (5 (GHz) Through	put							
All APs	pints	General							мся	(Data	Rate ¹) Settings	
Radios Global Coni	figuration	11n Mode			🗹 Enat	oled 3			0	(7	Mbps)	Supported
Advanced	1	11ac Mod	le		🗹 Enat	oled ²			1	(14	Mbps)	Supported
Mesh		11ax Mod	le		🗹 Enat	oled 3			2	(21	Mbps)	Supported
AP Group	NTP		Pater						3	(29	Mbps)	Supported
ATE		VITINCS	Rates						4	(43	Mbps)	Supported
PE Profile		SS1							5	(58	Mbps)	Supported
FlexConn	ect Groups	0-8			Enat	oled 4			6	(65	Mbps)	Supported
ElexConn	ect ACLs	0-9			🗹 Enat	oled 4			7	(72	Mbps)	Supported
FlaxConn									8	(14	Mbps)	Supported
Template	S	552							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 Gro	uping	0-8			🗸 Enat	oled 4			13	(116	Mbps)	Supported
TPC		0-9			🗹 Enat	oled 4			14	(130	Mbps)	Supported
Covera	ge								15	(144	Mbps)	Supported
Genera	d	SS4							16	(22	Mbps)	Supported
Client Roan Media	ning	0-8			Enat	oled 4			17	(43	Mbps)	Supported
EDCA Para	meters	0-9			🗹 Enat	oled 4			18	(65	Mbps)	Supported
DFS (802.1 High Throu	L1h) Ighput	HE MCS R	ates						19	(87	Mbps)	Supported
(802.11n/a	ac/ax)								20	(130	Mbps)	Supported
CleanAir		SS1			SS2				21	(173	Mbps)	Supported
▶ 802.11b/	g/n/ax	0-7	✓ Er	nabled	0-7	✓ E	nabled		22	(195	Mbps)	Supported
Media Str	eam	0-9	✓ Er	nabled	0-9	✓ E	nabled		23	(217	Mbps)	Supported
Applicatio	on Visibility	0-11	🗹 Er	nabled	0-11	🗹 E	nabled		24	(29	Mbps)	Supported
Lync Serv		553			554				25	(58	Mbps)	Supported
Country	rer	0-7		nabled	0-7		nabled		26	(87	Mbps)	Supported
Timerc		0-9		nabled	0-0		nabled		27	(116	Mbps)	Supported
 Notflow 		0-11		nabled	0-11		nabled		28	(173	Mbps)	Supported
h Ore		0-11			0-11		naoidu		29	(231	Mbps)	Supported
₽ QoS		SS5			SS6				30	(260	Mbps)	Supported
		0-7	✓ Er	nabled	0-7	✓ E	nabled		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 Wireless Phone 840 および 860 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をお勧めします。

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

Cisco Wireless Phone 840 および 860 の推奨事項に従って A-MPDU および A-MSDU 設定を設定するには、 次のコマンドを使用します。

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

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

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

802.11n Status:

A-MSDU Tx:

	優先度 0	 無効
	優先度 1	 有効
	優先度 2	 有効
	優先度 3	 無効
	優先度 4	 無効
	優先度 5	 無効
	優先度 6	 無効
	優先度 7	 無効
A-M	PDU Tx:	
	優先度 0	 有効
	優先度 1	 無効
	優先度 2	 無効
	優先度 3	 有効
	優先度 4	 有効
	優先度 5	 有効
	優先度 6	 無効
	優先度 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	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 >	CleanA	ir										
Access Points All APs Radios Global Configuration Advanced	CleanAir/ CleanAir Spectrum	CleanAir/Spectrum Intelligence Parameters CleanAir CleanAir Spectrum Intelligence ³ CleanAir											
Mesh	Report In	Report Interferers ¹											
AP Group NTP	Persisten	Device Pro	pagation				Enabled						
▶ ATF	Interfer	ences to T	anore		Interfe	rences to Detect							
RF Profiles	Canon	,	gnore			Transmitter							
FlexConnect Groups	WiMax	Fixed		>	Jamn	ner							
FlexConnect ACLs	SI_FH:	SS	ter										
FlexConnect VLAN Templates		Video Camera											
Network Lists	Trap Cont	Trap Configurations											
 802.11a/n/ac/ax Network RRM RF Grouping TPC DCA Coverage General Client Roaming Media EDCA Parameters DFS (802.11h) High Throughput (802.11h/ac/ax) S02.11b/g/n/ax Media Stream Application Visibility 	Enable Ad AQI Alarr Enable tr Threshold Enable In Do not t TDD T Contin DECT- Video Super/	QI (Air Quali an Threshold ap for Unclas ap for Unclas ap for Classif terference rap on the ransmitte uous Trar ike Phonn. Camera AG	ty Index) Trap ((1 to 100) ² assified Interference: ified Interference: ied category trap For Security Alarm ase types r hsmitter e (Change Setting:	ces p (1 to 99) s (1 to 99)	Trap o Jamn WiFi WiFi	n these types ner Inverted Invalid Channel	Enabled Control Enabled E						
And Control	EDRRM	Ven KKP	(<u>change Setting</u>	2. Disabled									
Country	Sensitivit	v Threshold		N/A									
Timers	Roque Co	ntribution		N/A									
Netflow	Rogue Du	ty-Cycle		N/A									
▶ QoS	(1)Device So (2)AQI value (3)Spectrum	ecurity aları 100 is bes Intelligenc	ms, Event Driven i and 1 is worst te does not send t	RRM and Persis raps to Prime II	tence Device A nfrastructure a	voidance algorithm nd CMX	n will not work if I	nterferer	s reporting is disabled.				

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MA	NAGEMENT COMMANDS	HELP <u>F</u> EEDBACK	
Wireless	802.11a/n/ac/ax Cisco APs > 0	Configure			
 Access Points All APs Radios	General		RF Channe	el Assignment	
802.11b/g/n/ax	AP Name	rtp9-31a-ap1	Current Cl	hannel	(48,44)
Global Configuration	Admin Status	Enable ᅌ	Channel W	Vidth *	40 MHz 🗘
Advanced	Operational Status	UP	* Channel wi mode	dth can be configured	only when channel configuration is in custom
Mesh	Slot #	1	Assignmer	nt Method	Global
AP Group NTP	11n Parameters				Custom
▶ ATF			Radar Inf	ormation	
RF Profiles	11n Supported	Yes			
FlexConnect Groups	CleanAir		Channel	Last H	eard(Secs)
FlexConnect ACLs			No radar det	ected channels	
FlexConnect VLAN	CleanAir Capable	Yes	Tr Dower	Lough Acciment	
Templates	CleanAir Admin Status	Enable ᅌ	TX Power	Level Assignmen	t
Network Lists	CleanAir enable will take effect onl	y if it is enabled on this band.	Current To	k Power Level	1
802.11a/n/ac/ax	Number of Spectrum Expert connections	0	Assignmer	nt Method	• Global
802.11b/g/n/ax					Custom
Media Stream	Antenna Parameters				
Application Visibility And Control	Antenna Type	A S	Performa	nce Profile	
Lync Server	Antenna	C Z	View and	edit Performance Profil	e for this AP
Country		D 🗹	Perform	mance Profile	
Timers			Note: Chang	ing any of the paramet	ers causes the Radio to be temporarily disabled
Netflow			and thus may	y result in loss of conne	ectivity 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。

uluili. cisco	<u>m</u> onitor <u>w</u>	LANs <u>C</u> ON	ROLLER	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 Thre	eshold							
 Access Points All APs Radios Global Configuration 	Rx Sop Three Rx Sop Three	shold 802.11a shold 802.11b	Defau Defau	ilt ᅌ O	Custom				
 Advanced RF Management Flexible Radio Assignment Load Balancing DTLS Band Select Rx Sop Threshold Optimized Roaming Network Profile 	1 Rxsop only	supported in L	ocal,Flex,Br	idge and Flex+	Bridge mode A	ips.			

WLAN の設定

Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ (たとえば 802.11a のみ)適用するよう指定できます。
Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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

ululu cisco	<u>M</u> ONITOR <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
WLANs	WLANs > New							
WLANs WLANs Advanced	Type Profile Name SSID ID	WLA voice voice 6						

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ON	NTROLLER 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 > Edit 'voice'	3"
WLANs WLANs	General Security	QoS Policy-Mapping Advanced
Advanced	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID	voice WLAN voice C Enabled [WPA2][Auth(FT 802.1X)] (Modifications done under security tab will appear after applying the changes.) 802.11a only C rtp-9 voice C Enabled C Enabled RTP9-32A-WLC3
	Lobby Admin Access	

高速セキュア ローミングに 802.11r(FT)を利用するには、Fast Transition を有効にするボックスをオ ンにします。

[Over the DS] をオフにして、Over the Distribution システム方式の代わりに Over the Air 方式を使用することを推奨します。

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

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

ululu cisco	MONITOR W	LANs <u>C</u> ON	TROLLER	WIRELESS	<u>s</u> ecur	ITY M <u>a</u> nag	GEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > E	dit 'voice'								
WLANs WLANs	General	Security	QoS	Policy-Map	ping	Advanced				
Advanced	Layer 2	Layer 3	AAA S	ervers						
	Layer 2	Security 🧕	WPA	A+WPA2	0					
	Security	Туре	Ente	erprise ᅌ						
	MAC Filt	ering <mark>9</mark>								
	WPA+WPA	2 Parameters	-							_
	WPA Poli	cy								
	WPA2 PC	cryption		MP128(AES)	TKIP	CCMP25	56	GCMP128	GCMP25	6
	OSEN Po	licy								
	Fast Transi	tion								
	Fast Tra	nsition	Ena	ble ᅌ						
	Over the	DS								
	Reassoci	ation Timeout	20	Seconds						
راریاں cısco	MONITOR W	LANs <u>C</u> ON	TROLLER	W <u>I</u> RELESS	<u>s</u> ecur	ITY M <u>A</u> NAG	EMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > E	dit 'voice'								
▼ WLANs	General	Security	QoS	Policy-Map	ping	Advanced				
WLANs	Protected I	Management	Frame							
Auvanceu	PMF		Disa	ibled ᅌ						
	Authentica	tion Key Man	agement	<u>19</u>						
	802.1X-	SHA1	🗌 En	able						
	802.1X-	SHA2	🗆 Er	nable						
	FT 802.3	LX	✓ Er	nable						
	ССКМ		🗌 En	able						
	WPA GTK-ra	andomize State	e 14 Disa	able ᅌ						



،، ،،، ،، cısco	MONITOR	<u>W</u> LANs <u>C</u> C	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
WLANs	WLANs > I	Edit 'voic	e'						
▼ WLANs	General	Security	QoS	Policy-Map	ping Adv	vanced			
WLANs	Protected	d Manageme	nt Frame						
Advanced	PMF		Disa	abled ᅌ					
	Authentic	cation Key M	anagement	<u>19</u>					
	PSK Fo	ormat <mark>21</mark>	ASC	сн ᅌ					
	PSK		🗆 Er	able					
	PSK-S	HA2	E	nable					
	FT PS	ĸ	✓ E	nable					
	WPA GTK	-randomize St	ate 14 Dis	able ᅌ					

高速セキュア ローミングに CCKM を利用するには、AES 暗号化を使用した WPA2 ポリシーと認証キー管 理タイプ用の CCKM を有効にします。

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <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
WLANs	WLANs > Edit 'voice'
WLANs WLANs	General Security QoS Policy-Mapping Advanced
- Auvanceu	Layer 2 Security WPA+WPA2
	Security Type Enterprise 🗢
	WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy Image: Complex com
	OSEN Policy
	Fast Transition Disable

رابیان دisco	<u>M</u> ONITOR <u>W</u> LANS	<u>C</u> ONTROLLER WIRELESS	<u>S</u> ECURITY M <u>A</u> NAGEMEN	IT C <u>O</u> MMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'v	oice'			
 WLANS Mdvanced 	General Secu Protected Manage PMF Authentication Ke 802.1X-SHA1 802.1X-SHA2 CCKM	rity QoS Policy-Ma ment Frame Disabled © my Management 12 Enable Enable Enable Enable	pping Advanced		

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、CCKM、PSK も有効にできます。802.1x や PSK を使用するかどうかに応じて、802.11r(FT)をサポートしない音声クライアントも含まれます。

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

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

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

،، ،،، ،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> I	RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT	C <u>o</u> mmands He <u>l</u> p <u>F</u> eedback
WLANs	WLANs > Edit 'voice'		
VLANs	General Security QoS Pol	icy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Server	s	
	Select AAA servers below to override u RADIUS Servers RADIUS Server Overwrite interface Apply Cisco ISE Default Settings Authentication Servers C Enabled Server 1 None Server 2 None Server 3 None Server 3 None Server 4 None Server 5 None Server 6 None Authorization ACA Server Enabled	Enabled Enabled Counting Servers C Enabled None None None None None None None None	EAP ParametersEnableImage: Colspan="2">Image: Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2"Colspan

WMM ポリシーは、この SSID が Cisco Wireless Phone 840 および 860 などの WMM 対応電話機で使用され ている場合にのみ、[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。

非 WMM クライアントが Cisco Wireless Phone 840 および 860 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。

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER W <u>I</u> RE	LESS <u>S</u> ecurit	TY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
WLANs 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 (voi Platinum (voi none none Disable Disable Other dwidth Contra	ce) 0				
		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						

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER W <u>I</u> RELES	SS <u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
 WLANs WLANs Advanced 	General Security Override Per-SSID Bar	QoS Policy-M ndwidth Contract	lapping Adv s (kbps) ¹⁶	vanced			
	Average Data Rate Burst Data Rate Average Real-Time Rate Burst Real-Time Rate Clear						
	WMM Policy 7920 AP CAC 7920 Client CAC Media Stream Multicast Direct	Required ᅌ 🖉 Enabled 🗆 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)]を無効にする必要があります。

必要に応じて [クライアント除外 (Client Exclusion)]を設定します。

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

[オフチャンネルスキャンの待機 (Off Channel Scanning Defer)]を調整することで、スキャンの待機時間だ けでなく、特定のキューに対するスキャンを待機させることができます。

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

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

[DHCP アドレス割り当て必須 (DHCP Address Assignment Required)]を無効にする必要があります。

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

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

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

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

802.11k および 802.11v を有効にすることを推奨します。

cisco	Monitor Wlans Controller Wireless Security Management	T C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'	
WLANs WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Allow AAA Override Enabled	DHCP
	Coverage Hole Detection 🗸 Enabled	DHCP Server Override
	Airopet IE Session Timeout (secs)	DHCP Addr. Assignment Required
	Diagnostic Channel 18 Enabled	Management Frame Protection (MFP)
	Override Interface ACL IPv4 None C IPv6 None C IPv6 None C	MFP Client Protection ⁴ Optional Company Optional Optio
	URL ACL None	802.11a/n (1 - 255) 2
	P2P Blocking Action Disabled 🕤 Client Exclusion 3 Disabled	802.11b/g/n (1 - 255) 2
	Maximum Allowed Clients	NAC State None O
	Static IP Tunneling 11 Enabled	Load Balancing and Band Select
	Wi-Fi Direct Clients Policy Disabled	Client Load Balancing
	Maximum Allowed Clients 200	Client Band Select

cisco	MONITOR WLANS CONTR	ROLLER 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 > Edit 'voice'				
WLANS	General Security	QoS Policy-Mapping Adv	anced		
Advanced	Clear HotSpot		Passiv	ve Client	
Autoneeu	Configuration	Enabled	Pa	ssive Client	
	Client user idle		Voice	1	
	timeout(15-100000)		Me	edia Session Snooping	Enabled
	Client user idle threshold (0-10000000)	0 Bytes	Re	e-anchor Roamed Voice Clients	Enabled
	Radius NAI-Realm	0	KT	S based CAC Policy	Enabled
	11ac MU-MIMO		Radiu	is Client Profiling	
	WGB PRP	Enabled	DH	HCP Profiling	
	MBO State		нт	TTP Profiling	
	Off Channel Scanning Defe	r	Local	Client Profiling	
	Scan Defer Priority	0 1 2 3 4 5 6 7	DH	HCP Profiling	
			нт	TTP Profiling	
	Scan Defer Time(msecs)	100	PMIP		
	ElexConnect	100	PMI	IP Mobility Type	
	riexconnect		DMT		Hevadecimal
	Switching ²	Enabled	P MI		

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

ululu cisco	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		
h Advanced	802.11ax BSS Configuration		mDNS	
F Auvanceu	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
			Umbrella DHCP Override	
			Fabric Configuration	
			Fabric	Enabled
			M-1-110	
			Coloritius December	
			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。

uluilu cisco	<u>m</u> onitor <u>w</u> la	Ns <u>C</u> ONTROLL	ER 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	AP Groups							
WLANs WLANs	Add New AP G	roup						
 Advanced AP Groups 	AP Group Name Description	rtp						
		Add Cano	el					

،، ،،، ،، cısco	MONITOR <u>W</u> LANS <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
WLANs	Ap Groups > Edit 'rtp'				
WLANs	General WLANs RF Profil	e 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 ᅌ			

[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。

۱۱۱۱۱۱۰ cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	Ap Group	s > Edit	'rtp'					
WLANs WLANs	General	WLA	Ns RF Profi	e APs	802.11u	Location	Ports/Module	Intelligent Capture
Advanced AP Groups	Add Nev	v						Add New
	WLAN S Interfac /Interfa Group(O SNMP N	SID ce G) AC State	voice(6) rtp-9 voice Enabled Add Can	cel	• •	1		

[**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。

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	COMMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	Ap Group	os > Edit	'rtp'					
WLANs WLANs	General	WLA	Ns RF Profil	e APs	802.11u	Location	Ports/Module	Intelligent Capture
Advanced AP Groups	802.111 802.111	a none	e e	••••••••••••••••••••••••••••••••••••••	I		Apply	

[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。

ululu cisco	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER V	VIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EE	EDBACK
WLANs	Ap Groups > Edit	'rtp'						
VLANs WLANs	General WLAI	Ns RF Profile	APs	802.11u	Location	Ports/Module	Intellige	ent Capture
 Advanced AP Groups 	APs currently in th	e Group		Remove APs	Add APs	to the Group		Add AF
	AP Name	Ethernet M	IAC		AP Na	me	Group Nam	e
	rtp9-31a-ap14	00:81:c4:9	6:78:28		1			
	rtp9-32a-ap20	00:81:c4:3	2:b9:b8					
	rtp9-32a-ap23	00:81:c4:9	6:74:10					

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 ᅌ							
Interface Groups	AP Multicast Mode 1	Multicast ᅌ 239.1.1.9 Multicast Group Address							
Multicast	AP IPv6 Multicast Mode 1	Multicast ᅌ 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 ᅌ							
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 ᅌ							
▶ mDNS	Operating Environment	Commercial (10 to 35 C)							
Advanced	Internal Temp Alarm Limits	10 to 38 C							
I surful Intercention	WebAuth Proxy Redirection Mode	Disabled 📀							
Lawrul Interception	WebAuth Proxy Redirection Port	0							
	Captive Network Assistant Bypass	Disabled 📀							
	Global IPv6 Config	Disabled 📀							
	Web Color Theme 2	Default 🗘							
	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 😂							
	1. Multicast is not supported with Fle. 2.Changes in Web color Theme will g	«Connect on this platform. Multicast-Unicast mode does not support IGMP/MLD Snooping. Disable Global Multicast first et 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。

،،ا،،،ا،، cısco	<u>M</u> ONITOR	<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
Controller	Multicast								
General	Enable Glo	obal Multica	ast Mode						
Inventory	Enable IG	MP Snoopir	ng						
Interfaces	IGMP Time	eout (30-7	200 seconds)	60					
Interface Groups	IGMP Que	ry Interval	(15-2400 seconds	s) 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	est 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。

،،ا،،،ا،، cısco	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
Controller	Mobility /	Anchor (Config						
General Icons Inventory Interfaces Interface Groups Multicast Network Routes Fabric Configuration Redundancy Mobility Anchor Config Mubility Anchor Config Mubility Anchor Config Multicast Messaging	Keep Aliv Keep Aliv Symmetri DSCP Vali	e Count e Interval (ic Mobility T ue	(1-30 seconds) 'unneling mode	3 10 Enabled 0					

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。

	uluilu cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELES	S <u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Co	ntroller	Static Mo	obility Gr	oup Members						
	General Icons	Local M	lobility Gro	up CTG-VoW	LAN2					
1	Inventory	MAC Ac	ldress	IP Address(Ipv4/	Ipv6) Gr	oup Name	M	ulticast IP	Status	
	Interface Groups	00:5d:7	3:1a:c3:49	10.81.6.70	СТ	G-VoWLAN2	0.	0.0.0	Up	
	Multicast									
€ I	Network Routes									
€ I	Fabric Configuration									
€ I	Redundancy									
•	Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging									

コール アドミッション制御 (CAC)

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

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

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

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

ロードベース CACは、チャンネル上のすべての出力を考慮します。

ululu 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	802.11a(5	GHz) >	Media						
 Access Points All APs Radios Global Configuration 	Voice Call Adm	Video nission C	Media						
 Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups 	Admissi CAC Me Max RF Reserve Expedite	on Control thod 4 Bandwidth d Roaming ed bandwid	(ACM) (5-85)(%) Bandwidth (0-25)	 ✓ Er Loa 75 (%) 6 ✓ 	abled d Based 🗘				
 FlexConnect ACLs FlexConnect VLAN Templates 	SIP CAC	Support	2 dwidth ²	🗌 Er	abled				
Network Lists	SIP Cod SIP Ban SIP Void	lec dwidth (kb ce Sample I Stream M	ps) Interval (msecs) I etrics	G.7 64 20	11 ¢				
Coverage General Client Roaming Media	Metrics	Collection		2					
EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac/ax) CleanAir 802.11b/g/n/ax	Foot Not 1 11a rate 11n rate 2 SIP CAC 3 SIP CAC 4 Static C	es es(Kbps): 6 es(Kbps): 6 S should on C will be sup AC method	000,9000,12000, 55000,72200,1300 ly be used for pho pported only if SIF l is radio based an	18000,24000,3 100,144400,13 nes that suppo 9 snooping is en d load-based C	6000,48000,54 5000,150000,2 rt status code 1 abled. AC method is c	1000 70000,300000 17 and do not supp rhannel 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)**]を無効にする必要があります。

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	GHz) >	Media						
 Access Points All APs Radios Global Configuration 	Voice Call Adm	Video hission C	Media						
 Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates 	Admissic CAC Met Max RF I Reserver SIP CAC	on Control thod 4 Bandwidth d Roaming	(ACM) (5-85)(%) Bandwidth (0-25)	□ E Sta 0(%) 0 □ E	nabled tic O				
 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 Note 1 11a rate 11n rate 2 SIP CAC	es ts(Kbps): 6 ts(Kbps): 6	5000,9000,12000, 55000,72200,1300 ly be used for pho	18000,24000, 100,14440,13 nes that suppo	36000,48000,55 5000,15000,2 rt status code :	1000 70000,300000 17 and do not suppi	ort TSPEC-based	admissio	n control.
802.11b/g/n/ax	3 SIP CAC 4 Static CA	will be su AC methoo	pported only if SIP I is radio based and	snooping is e d load-based (nabled. AC method is c	hannel based.			

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

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

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

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

(Cisco Controller) >show wlan <WLAN id>

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。

ւվովո 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	802.11a(5	5 GHz) >	Media						
 Access Points All APs Radios Global Configuration 	Voice	Video	Media						
Advanced	Unicast	Video Redi	rect						
Mesh AP Group NTP ATF RF Profiles FlexConnect Groups	Multicas Maximu Client M Maximu	im Media Bi Minimum Ph Im Retry Pe	Admission Co andwidth (0-85(% ny Rate 1 ercent (0-100%)	ntrol)) 85 6000 80)				
 FlexConnect ACLs FlexConnect VLAN Templates Network Lists 	Media S	tream - I	Multicast Dire	ct Paramete	ers				
 802.11a/n/ac/ax Network RRM RF Grouping TPC DCA Coverage General Client Roaming Media 	Max Str Max Str Best Eff	reams per F reams per C fort QoS Ad	Radio Client Imission	No- No- Er	limit ᅌ limit ᅌ nabled				
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 CAC 3 SIP CAC 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 SIF I is radio based an	18000,24000,3 000,144400,13 nes that suppo snooping is en d load-based C	6000,48000,54 5000,150000,2 rt status code : abled. AC method is c	4000 270000,300000 17 and do not supp channel 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 Wireless Phone 840 および 860 で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。

作成した RF プロファイルは、AP グループに適用されます。

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

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

uluulu 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 > New							
 Access Points All APs Radios Global Configuration 	RF Profile Name Radio Policy Use default RF Profile	rtp-5 802. e Template Non	11a ᅌ		\$			
Advanced Mesh								
AP Group NTP ATF RE Brofiles								

[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。

 cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIR	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 All APs 	General	802.1	1 RRM	High	Density	Client	Distribution			
Radios Global Configuration	Data Rate	es <u>1</u>	м	CS Se	ttinas					
Advanced					cango					
Mesh	6 Mbps	Disabled	٥	0	🗹 Suppo	rted				
AP Group NTP	9 Mbps	Disabled	\$	1	🗹 Suppo	rted				
▶ ATF	12 Mbps	Mandato	ory ᅌ	2	🗹 Suppo	rted				
RF Profiles	18 Mbps	Support	ed ᅌ	3	🗹 Suppo	rted				
FlexConnect Groups	24 Mbps	Support	ed ᅌ	4	🗹 Suppo	rted				
FlexConnect ACLs	36 Mbps	Support	ed ᅌ	5	🗹 Suppo	rted				
FlexConnect VLAN	48 Mbps	Support	ed ᅌ	6	🗹 Suppo	rted				
Templates	54 Mbps	Support	ed ᅌ	7	🗹 Suppo	rted				
Network Lists				8	🗹 Suppo	rted				
802.11a/n/ac/ax				9	🗹 Suppo	rted				
802.11b/g/n/ax				10	🗹 Suppo	rted				
Media Stream				11	🗹 Suppo	rted				
Application Visibility				12	🗹 Suppo	rted				
And Control				13	🗹 Suppo	rted				
Lync Server				14	🗹 Suppo	rted				
Country				15	🔽 Suppo	rted				
Timers				16	🔽 Suppo	rted				
Netflow					• •				_	
▶ 0oS										

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

uluilu cisco	MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS	SECURITY MANAGEMENT	T CQMMANDS HELP <u>F</u> EEDBACK	
Wireless	RF Profile > Edit 'rtp-5'			
Access Points All APs Radios	General 802.11 RRM High Densit	y Client Distribution	<u> </u>	
Global Configuration	трс		Coverage Hole Detection	
Mesh	Maximum Power Level Assignment (-10 to 30 dBm)	30	Data RSSI(-90 to -60 dBm) -80	
AP Group NTP	Minimum Power Level Assignment (-10 to 30 dBm)	-10	Voice RSSI(-90 to -60 dBm) -80	
▶ ATF	Power Threshold v1(-80 to -50 dBm)	-70	Coverage Exception(0 to 100 %) 25	
RF Profiles	Power Threshold v2(-80 to -50 dBm)	-67	Coverage Level(1 to 200 Clients) 3	
FlexConnect Groups	DCA		Profile Threshold For Traps	
FlexConnect ACLs	Avoid Foreign AP interference	Enabled	Interference (0 to 100%)	10
FlexConnect VLAN Templates	Channel Width 🔵 20 MHz 💽 40 MHz 🔵 80 MHz 🔅	160 MHz 0 80+80 MHz 0 Be	Best 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			Client Network Preference	
Media Stream			Connectivity Throughput O Automatic	
Application Visibility And Control			Client Aware	
Lync Server			CEnable Olisable	
Country	High-Speed Roam			
Timers	HSR mode		Enabled	
Netflow				
▶ QoS				

	uluulu cisco	MONITOR WLAM	s <u>C</u> ON	TROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u>	FEEDBACK	
٧	Vireless	RF Profile > Ec	it 'rtp	-5'							
,	Access Points	General 80	2.11	RRM	High Density	y Client	Distribution				
	All APs ▶ Radios Global Configuration								Client	: Aware	
I	Advanced	High-Speed Roa	Igh-Speed Roam								
,	Mesh AP Group NTP	HSR mode						Enabled			
1	ATF	Neighbor Time	out Factor								
	RF Profiles FlexConnect Groups	Dea channer	36, 40,	44, 48, 52,	56, 60, 64, 149	9, 153,					
1	FlexConnect ACLs	DCA Channels	157, 16	1							
	Templates										
,	802.11a/n/ac/ax	Select Ch	nnel								
1	802.11b/g/n/ax	2 3	6			1					
1	Application Visibility		4								
	Lync Server	 ✓ 4 ✓ 5 	8								
	Country	Extended UNIT	2 channel		abled						
1	Netflow	CATENDED ONIT	z channei		aorea						
	0.05										

[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。

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
Wireless	RF Profile > Edit 'rtp-5'
 Access Points All APs Radios 	General 802.11 RRM High Density Client Distribution
Global Configuration Advanced	High Density Parameters Multicast Parameters
Mesh	Maximum Clients(1 to 200) 200 Multicast Data Rates ² auto ᅌ
AP Group NTP	Rx Sop Threshold Parameters ⁵
 ATF RF Profiles 	Rx Sop Threshold ⁶ Default ³ 0 Custom

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。

802.11r (FT) または CCKM を使用している場合は、同じ FlexConnect グループ内のアクセス ポイン トにローミングするときにのみ、シームレスなローミングを実現できます。

	ululu cisco	<u>M</u> ON	NITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGE	MENT C <u>O</u>	MMANDS	HELP	<u>F</u> EEDBACK
w	ireless	Flex	xConn	ect Gro	ups > New							
•	Access Points All APs Radios Global Configuration	G	roup Nar	ne rtp	-1							
Þ	Advanced											
	Mesh											
Þ	AP Group NTP											
Þ	ATF											
	RF Profiles											
	FlexConnect Grou	ps										
	cisco	MONITOR	<u>W</u> LANs		R WIRELESS S	ECURITY M <u>A</u> NA	GEMENT COMI	MANDS HEL	P <u>F</u> EEDBAC	ĸ		
Wi	reless	FlexConne	ect Grou	ıps > Edit	'rtp-1'							
-	Access Points											
,	All APs Radios	General	Local	Authentica	tion Image Up	grade ACL M	apping Cen	tral DHCP	WLAN VLAN	I mapping	WLAN A	VC mapping
	Global Configuration	Group N	ame		rtp-1							
×.	Advanced	VLAN Ter	mplate Nam	ne	none ᅌ							
	Mesn	Enable AF	P Local Aut	hentication ²								
	ATF	FlexConnec	ct AP									
	RF Profiles	HTTP-Pro	oxv									
	FlexConnect Groups	In Addres	cc/Inv4/Inv	(6)								
×.	FlexConnect ACLs	Port	55(1044/104	vo)	0							
	FlexConnect VLAN Templates			_	-							
	Network Lists				Add							
Ľ.	802.11a/n/ac/ax											
Ľ		AAA										
- P -	802.11b/g/n/ax	AAA Server I	p Address									
	802.11b/g/n/ax Media Stream	AAA Server I Server T	p Address Type		Primary ᅌ							
F	802.11b/g/n/ax Media Stream Application Visibility And Control	AAA Server I Server T Shared S	p Address Type Secret		Primary ᅌ							
×	802.11b/g/n/ax Media Stream Application Visibility And Control Lync Server	AAA Server I Server T Shared S Confirm	p Address Type Secret Shared Ser	cret	Primary ©							
÷	802.11b/g/n/ax Media Stream Application Visibility And Control Lync Server Country	AAA Server I Shared S Confirm Port Nur	p Address Type Secret Shared See nber	cret	Primary C							
×	802.11b/g/n/ax Media Stream Application Visibility And Control Lync Server Country Timers	AAA Server I Server T Shared S Confirm Port Nur Add	p Address Type Secret Shared Sec mber	cret	Primary C							
•	802.11b/g/n/ax Media Stream Application Visibility And Control Lync Server Country Timers Netflow	AAA Server I Shared S Confirm Port Nur Add	p Address Type Secret Shared Sea nber	cret	Primary S 1812							

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。

uluili. 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	
Wireless	FlexConne	ect Gro	up AP List							
 Access Points All APs Radios Global Configuration 	Group Na	ime			rtp-1					
Advanced	FlexConne	ect APs								
Mesh AP Group NTP ATF RF Profiles FlexConnect Groups	Add AP Entries 0	- 0 of 0 Address	AP Name	S	tatus	AP Mo	de	Тур	96	Conflict with PnP

۱۱۱۱۱۱۱ cısco	<u>M</u> ONITOR <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	FlexConnect Grou	up AP List						
 Access Points All APs Radios Global Configuration 	Group Name			rtp-1				
Advanced	FlexConnect APs							
Mesh AP Group NTP ATF RF Profiles FlexConnect Groups	Add AP Select APs from curr Ethernet MAC	ent controller	Add Canc	el				

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。

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	Media Stro	eam >G	eneral						
 Access Points All APs Radios Global Configuration 	Multicast D Session Mo)irect featu essage (ire 🗸	Enabled					
Advanced	Session an	nounceme	nt State 🗌 I	Enabled					
Mesh	Session an	nounceme	nt URL						
▶ ATF	Session an	nounceme	ent Email						
RF Profiles FlexConnect Groups FlexConnect ACLs	Session an	nounceme	nt Note		/				
FlexConnect VLAN Templates									
Network Lists									
802.11a/n/ac/ax									
802.11b/g/n/ax									
 Media Stream General Streams 									

次に、ストリームを設定します。

	رایتران cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
W	lireless	Media Str	eams						En	tries 1 - 1 of 1		
•	Access Points All APs	Stream Na	me				Start IP	Address(Ipv4/I	pv6) E	nd IP Address(Ipv4/Ipv6)	Operation Status	_
	 Radios Global Configuration 	10.195.19.2	<u></u>				239.1.1.1		2	39.1.1.1	Multicast Direct	
Þ	Advanced											
	Mesh											
Þ	AP Group NTP											
Þ	ATF											
	RF Profiles											
	FlexConnect Groups											
Þ	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 WIRELESS	S <u>S</u> ECURITY M <u>A</u> NA	GEMENT C <u>O</u> MMANDS	HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'				
 WLANs WLANs Advanced 	General Security Override Per-SSID Bar	QoS Policy-Ma ndwidth Contracts	Advanced (kbps) ¹⁶		
	Average Data Rate Burst Data Rate Average Real-Time Rate Durst Real-Time Rate Clear WMM WMM Policy 7920 AP CAC 7920 Client CAC Media Stream Multicast Direct Lync Policy	DownStream Up: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Stream		

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	なし
Gold	802.1p	4
Bronze	802.1p	1
Silver	802.1p	0

ایرزارد cisc	11 0	<u>M</u> ONITOR	<u>w</u> lans	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP
Wireless		Edit QoS	Profile						
 Access Poir All APs Radios Global Config 	its uration	QoS Profi Descriptio	ile Name on	platinum For Voice App	lications				
Advanced		Por-licor	Bandwid	th Contracts (khne) *				
Mesh		Fei-Osei	Danuwiu	Dever Street					
AP Group N	тр	A	Data Data	DownStre		am			
▶ ATF		Rurst Dat	Dala Rale	0					
RF Profiles		Average [a Kale	oto 0					
FlexConnec	t Groups	Average F	Keal-Time R						
FlexConnect	t ACLs	Durst Red	I-TIME Rate	0	0				
FlexConnec Templates	t VLAN	Per-SSID	Bandwid	ith Contracts	(kbps) *				
Network Lis	sts			DownStre	am UpStre	am			
▶ 802.11a/n/	/ac/ax	Average [Data Rate	0	0				
▶ 802.11b/g	/n/ax	Burst Dat	a Rate	0	0				
Media Streat	m	Average F	Real-Time R	ate 0	0				
Application	Visibility	Burst Rea	al-Time Rate	0	0				
And Contro	I	WLAN Qo	S Param	eters					
Lync Serve	r	Maximum	Priority	voice	~				
Country		Unicast D	efault Prior	ity besteffor	t v				
Timers		Multicast	Default Prio	ority besteffor	t v				
Netflow				-					
QoS		Wired Qo	S Protoc						
Roles		Protocol 1	Гуре	None	•				
Qos Map									

uluili. cisco	MONITOR	<u>w</u> lans	CONTROLLER	WIRELES	S <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Wireless	Edit QoS	Profile						
 Access Points All APs Radios Global Configuration 	QoS Profi	le Name	gold	lications				
Advanced	Description	on	For video Ap	hicacions]
Mesh	Per-User	Bandwid	th Contracts ((kbps) *				
AP Group NTP			DownStre	am UpS	tream			
▶ ATF	Average I	Data Rate	0	0				
RF Profiles	Burst Dat	a 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	Per-SSID	Bandwid	Ith Contracts	(kbps) *				
Network Lists			DownStre	am Ups	tream			
802.11a/n/ac/ax	Average [Data Rate	0					
802.11b/g/n/ax	Burst Dat	a Rate	0					
Media Stream	Average I	Real-Time R	ate 0					
Application Visibility And Control	Burst Rea	al-Time Rate	e 0	0				
Lync Server	WLAN Qo	S Param	eters					
Country	Maximum	n Priority	video	~				
Timers	Unicast D	efault Prior	ity video	~				
Netflow	Multicast	Default Pric	video	~				
▼ 0oS	Wired Qo	S Protoc	ol					
Profiles	Protocol 1	Гуре	802.1p	~				
Roles Qos Map	802.1p Ta	ag	4					

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>a</u> nagement	C <u>O</u> MMANDS	HE <u>L</u> P
Wireless	Edit QoS	Profile						
 Access Points All APs Radios Global Configuration 	QoS Profi	ile Name	bronze					
 Advanced 	Descripti	on	For Backgroun	10				
Mesh	Per-User	Bandwid	th Contracts (kbps) *				
AP Group NTP			DownStre	am UpStre	am			
▶ ATF	Average	Data Rate	0	0				
RF Profiles	Burst Dat	ta Rate	0	0				
FlexConnect Groups	Average	Real-Time R	ate 0	0				
FlexConnect ACLs	Burst Rea	al-Time Rate	0	0				
FlexConnect VLAN Templates	Per-SSID	Bandwid	ith Contracts	(kbps) *				
Network Lists			DownStre	am UpStre	am			
802.11a/n/ac/ax	Average	Data Rate	0					
802.11b/g/n/ax	Burst Dat	ta Rate	0					
Media Stream	Average	Real-Time R	ate 0					
Application Visibility	Burst Rea	al-Time Rate	0	0				
And Control	WLAN Qo	S Param	eters					
Lync Server	Maximum	n Priority	backgrou	nd 🗸				
Country	Unicast D	Default Prior	ity backgrou	nd 🗸				
Timers	Multicast	Default Prio	backgrou	nd 🗸				
Netflow	Wined On	6 Brotos	al					
QoS	wired Qo							
Roles	Protocol	туре	802.1p \					
Qos Map	802.1p Ta	ag	1					

uluili. cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Wireless	Edit QoS	Profile						
 Access Points All APs Radios Global Configuration Advanced 	QoS Profil Descriptio	le Name on	silver For Best Effor	t				
Mesh	Per-User I	Bandwid	th Contracts (kbps) *				
AP Group NTP			DownStre	am UpStre	am			
▶ ATF	Average D	ata Rate	0	0				
RF Profiles	Burst Data	a Rate	0	0				
FlexConnect Groups	Average R	eal-Time R	ate 0	0				
FlexConnect ACLs	Burst Real	I-Time Rate	0	0				
FlexConnect VLAN Templates	Per-SSID	Bandwid	Ith Contracts	(kbps) *				
Network Lists			DownStre	am UpStre	am			
802.11a/n/ac/ax	Average D	ata Rate	0					
802.11b/g/n/ax	Burst Data	a Rate	0					
Media Stream	Average R							
Application Visibility And Control		S Daramo	otors	U				
Lync Server	Maximum	Priority	hostoffor					
Country	Unicast De	efault Priori	ty besteffor					
Timers	Multicast [Default Pric	rity besteffor					
Netflow	, fulled be t			•				
▼ QoS	Wired Qos	S Protoco	ol	_				
Profiles Roles	Protocol Ty	уре	802.1p \	•				
Qos Map	802.1p Ta	g	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。

،، ،،، ،، 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> EEDBA	CK
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 	Identity F Identity r Dynamic Request 1 Request 1 Max-Logii EAPOL-Ke EAPOL-Ke EAP-Broa	Request Tim equest Max WEP Key Ir Fimeout (in Max Retries In Ignore Id ay Timeout ay Max Retri dcast Key J	neout (in secs) k Retries ndex secs) entity Response (in milliSeconds) ries interval(in secs)						30 2 0 30 2 enable 400 4 3600	C
Advanced EAP										_

コマンドラインを介して Cisco Wireless LAN Controller の EAP パラメータを表示するには、次のコマンドを 入力します。

(Cisco Controller) > show advanced eap

EAP-Identity-Request Timeout (seconds)
EAP-Identity-Request Max Retries 2
EAP Key-Index for Dynamic WEP0
EAP Max-Login Ignore Identity Response enabl
EAP-Request Timeout (seconds)
EAP-Request Max Retries 2
EAPOL-Key Timeout (milliseconds)400
EAPOL-Key Max Retries4
EAP-Broadcast Key Interval

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

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

EAP の失敗が頻繁に発生する展開では、**[EAP 要求タイムアウト (EAP-Request Timeout)**]を 30 秒未満に減 らす必要があります。

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

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

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

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

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

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

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

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

[EAP-Broadcast Key Interval] が 3600 秒(1 時間)以上に設定されていることを確認します。

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

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

Auto-Immune

Auto-Immune(自己免疫)機能は、サービス拒否(DoS)攻撃に対する保護のために任意選択で有効にできます。 この機能を有効にしても、Voice over Wireless LAN によって中断が引き起こされる可能性があります。そのた め、Cisco ワイヤレス LAN コントローラで Auto-Immune 機能を無効にすることを推奨します。

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

(Cisco Controller) > show wps summary

Auto-Immune

Auto-Immune.......[無効 (Disabled)]

Client Exclusion Policy Excessive 802.11-association failures......有効 Excessive 802.11-authentication failures......有効 Excessive 802.1x-authentication.....有効 IP-theft.......有効 Excessive Web authentication failure.......有効

Signature Policy 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

CCKM タイムスタンプの許容値

デフォルトの CCKM タイムスタンプ許容値は 1000 ミリ秒に設定されます。

Cisco Wireless Phone 840 および 860 のローミングエクスペリエンスを最適化するために、CCKM タイムス タンプ許容値は 5000 ミリ秒に調整することをお勧めします。

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?

<tolerance><tolerance> Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msecs

シスコの推奨事項に従って CCKM タイムスタンプの許容値を設定するには、次のコマンドを使用します。

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >

変更を確認するには、show wlan<WLAN id> と入力します。これにより、次のように表示されます。

CCKM tsf Tolerance.....5000

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。

ll cisco	MONITOR <u>w</u> lans <u>c</u> ontroller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback	
Security	Rogue Policies	
 AAA General RADIUS TACACS+ LDAP Local Net Users MAC Fittering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies r Rogue Policies 	Rogue Detection Security Level Low High Critical Crita Critica Critical	Custom
General Rogue Rules Friendly Rogue Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection Web Auth TrustSec Local Policies Umbrella Advanced	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 AdHoc Rogue AP Enabled	

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

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

- [802.11r (FT)]または [CCKM] が [有効 (Enabled)]になっていることを確認します。
- [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 を [有効 (Enabled)] に設定することを推奨
- 802.11v を [有効 (Enabled)]に設定することを推奨
- [セッションタイムアウト (Session Timeout)]が有効で、正しく設定されていることを確認します

- [キーのブロードキャスト間隔 (Broadcast Key Interval)]が有効になっていて、正しく設定されていることを確認します
- [Aironet IE] が [有効 (Enabled)] になっていることを確認します
- [DTPC サポート (DTPC Support)]を[有効 (Enabled)]に設定します。
- [P2P (ピアツーピア) ブロッキング アクション (P2P (Peer to Peer) Blocking Action)] を 無効にします。
- [クライアント除外タイムアウト (Client Exclusion Timeout)]が正しく設定されていることを確認し ます
- [DHCP が必要です (DHCP Required)]を無効にします
- [保護された管理フレーム (PMF) (Protected Management Frame (PMF)]は、[任意 (Optional)]または[無効 (Disabled)]に設定する必要があります
- [DTIM 周期 (DTIM Period)] を [2] に設定します
- [負荷分散 (Load Balance)] を [無効 (Disabled)]に設定します
- [帯域選択 (Band Select)]を[無効 (Disabled)]に設定します
- [IGMP スヌーピング (IGMP Snooping)] を[有効 (Enabled)]に設定します。
- 必要に応じて [データレート (Data Rates)]を設定します
- 必要に応じて [RRM] を設定します
- [ボイス (Voice)]で、[アドミッション制御必須 (Admission Control Mandatory)]を[有効 (Enabled)]に設定します。
- [ボイス (Voice)]で[ロードベース CAC (Load Based CAC)]を[有効 (Enabled)]に設定します。
- **[ボイス (Voice)**] で **[トラフィック ストリーム メトリック (Traffic Stream Metrics)**] を 有効にします。
- [EDCA プロファイル (EDCA Profile)]を[音声の最適化 (Voice Optimized)]または[音声およびビデオの最適化 (Voice and Video Optimized)]に設定します
- [電力制限 (Power Constraint)]が [無効 (Disabled)]になっていることを確認します。
- [チャンネルスイッチステータス (Channel Switch Status)]と[スマート DFS (Smart DFS)] を有効にします
- [チャンネル スイッチ アナウンス モード (Channel Switch Announcement Mode)] を[待機 (Quiet)]に設定します
- 必要に応じて [高スループットデータレート (High Throughput Data Rates)]を設定します
- [CleanAir] を有効にします
- [マルチキャストダイレクト対応 (Multicast Direct Enable)]を有効にします

802.11 ネットワークの設定

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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。

[DTPC サポート (DTPC Support)]が有効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。

Cisco Catalyst	9800-40 Wireless Controller Welcome alpha 🖌 🎓 🖺 🏟 🕲 🤣 Search APs and Clients Q
Q Search Menu Items	nfiguration - > Radio Configurations - > Network
詞 Dashboard	5 GHz Band 2.4 GHz Band
Monitoring >	General 🖹 Apply
✓ Configuration →	5 GHz Network Status
() Administration →	▲ Please disable 5 GHz Network Status to configure Beacon Interval, Fragmentation Threshold, DTPC Support.
X Troubleshooting	Beacon Interval* 100
	Fragmentation 2346 Threshold(bytes)*
	DTPC Support 🗸
	CCX Location Measurement
	Mode
	Data Rates
	Please disable 5 GHz Network Status to configure Data Rates
	6 Mbps Mbps Disabled v12 Mandatory v
	18 Supported v24 Supported v36 Supported v
	48 Supported v54 Supported v

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

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

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

Cisco Cataly	yst 9800-40 Wireless (Controller Welcome a	lpha 🖀 🕏 🖹 🏟 🖗 🥹	Search APs 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	\checkmark		
\bigcirc Administration \rightarrow $\%$ Troubleshooting	A Please disable 2.4 GH 802.11g Network Status, Be Fragmentation Thre	z Network Status to configure eacon Interval, Short Preamble, eshold, DTPC Support.		
	802.11g Network Status	~		
	Beacon Interval*	100		
	Short Preamble	\checkmark		
	Fragmentation Threshold(bytes)*	2346		
	DTPC Support	\checkmark		
	CCX Location Measure	ement		
	Mode			
	Interval*	60		
	Data Rates			
	A Please disable 2.4 GHz N R	letwork Status to configure Data Rates		
	1 Disabled	v 2 Mbps Disabled v 5	.5 Disabled v	
	6 Disabled	• 9 Disabled • 1	1 Disabled v	
	12 Mandatory Mbps	• 18 Supported • 2 Mbps	4 Supported v	
	36 Mbps	• 48 Supported • 5 Mbps	4 Supported v	

高スループット (802.11n/ac)

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

802.11ac データ レートは 5 GHz にのみ適用できます。

[WMM] が有効になっていること、および [WPA2 (AES)] が 802.11n/ac データレートを使用するように設定 されていることを確認します。 Cisco Wireless Phone 840 および 860 は、HT MCS 0 ~ MCS 15 と VHT MCS 0 ~ MCS 9 1SS および 2SS データレートのみをサポートしますが、MIMO アンテナテクノロジーを含む同じ帯域を利用する他の 802.11n/ac クライアントが存在するため、より高いレートが利用可能な場合には、オプションでより高い MCS レートを有効にできます。

Cisco Cata	lyst 9800-40 Wireless	Controller Welcome a	lipha 🎢 🌾 🖺 🌣 🕅	Search APs and Clier	ts Q
Q Search Menu Items	Configuration - > Radio Co	onfigurations - > High Thro	ughput		
🔜 Dashboard	5 GHz Band 2.4 GHz	Band			
Configuration >	✓ 11n				
۔ (َ) Administration ،	Ena	ble 11n 🗸		Select All	
℅ Troubleshooting	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	
	(7Mbps)	(14Mbps)		3 /(29Mbps)	
	4/(43Mbps)	58/(58Mbps)	65Mbps)	/(72Mbps)	
	-8/(14Mbps)	9/(29Mbps)	0/(43Mbps)	1/(58Mbps)	
	2/(87Mbps)	3/(116Mbps)	4/(130Mbps)	5/(144Mbps)	
	6/(22Mbps)	7/(43Mbps)	8/(65Mbps)	9/(87Mbps)	
	20/(130Mbps)	21/(173Mbps)	2/(195Mbps)	23/(217Mbps)	
	24/(29Mbps)	25/(58Mbps)	26/(87Mbps)	27/(116Mbps)	
	28/(173Mbps)	29/(231Mbps)	30/(260Mbps)	31/(289Mbps)	
	✓ 11ac	▲ The I	Data rates are for 20MHz channels and S interval	Short Guard	
	Enable 🔢	с		Select All	
	SS/MCS	SS/MCS	SS/MCS	SS/MCS	
	√/8/(86.7Mbps)	🗸 1/9/(n/a)	2/8/(173.3Mbps)	✓ 2/9/(n/a)	
	3/8/(260.0Mbps)	3/9/(288.9Mbps)	4/8/(346.7Mbps)	✓ 4/9/(n/a)	
	✓ 11ax				
	Enable 11a	x 🗹		Select All	
	Multiple	sid			
	SS/MCS	SS/MCS	SS/MCS	SS/MCS	
		1/9	✓ 1/11	2/7	
	2/9	2/11	3/7	3/9	
	3/11	✓ 4/7	✓ 4/9	4/11	
	.5/7	5/9	5/11	6/7	
	.6/9	6/11	7/7	7/9	
	7 /11	8/7	8/9	8/11	

パラメータ

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

DFS (802.11h) セクションで、Cisco Wireless Phone 840 および 860 では送信電力の制御に DTPC が使用されるため、**[電力制限 (Power Constraint)]**を未設定のままにするか、0 dB に設定します。

[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)]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 Catalyst S	9800-40 Wireless	Controller	Welcome alpha	r 🖹 🌣 🖄 G	Search APs and Clients Q	•
Q Search Menu Items	figuration - > Radio C	onfigurations - > Pa	arameters			
Dashboard	GHz Band 2.4 GH	z Band				
Monitoring >	EDCA Parameters				🖺 Appiy	
Configuration >						
() Administration →	EDCA Profile	optimized-video-v	۲			
% Troubleshooting	DFS (802.11h)					
	DTPC Support is enable Network to configure	ed. Please disable it at Power Constraint				
	Power Constraint*	0				
	Channel Switch Status					
	Channel Switch Announcement Mode	Quiet	•			
	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 Catal	lyst 9800-40 Wireless Controller Welcome alpha	9 Ø Ø # # #	Search APs and Clients Q
Q Search Menu Items	Configuration • > Radio Configurations • > RRM		
Dashboard	5 GHz Band 2.4 GHz Band FRA		
Monitoring	General Coverage DCA TPC RF Grouping		
Configuration >	Power Assignment Method	Power Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9) by
() Administration >		Transmit Power Update	600 second(s)
₩ Troubleshooting	• Automatic	Last Run:	365 second(s) ago
	O 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 GHz を使用する場合は、多数のチャンネルをスキャンするために発生するアクセスポイント検出の遅延の可 能性を回避するためにチャンネルの数を制限できます(例: 12 チャンネルのみ)。

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

Cisco Cataly	vst 9800-40 Wireless Contro	Viller Welcome alpha # % Image: Comparison of the state of the sta
Q Search Menu Items	Configuration > Radio Configurati	ons* > RRM
Dashboard	5 GHz Band 2.4 GHz Band	FRA
Monitoring >	General Coverage DCA	TPC RF Grouping
Configuration >	Dynamic Channel Assignment	t Algorithm
 ⊘ Administration → ≫ Troubleshooting 	Channel Assignment Mode	Automatic Freeze Invoke Channel Update Once Off
	Interval	10 minutes •
	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 ↓ 20 MHz ● 40 MHz ● 80 MHz ● 160 MHz ● Best
	Auto-RF Channel List	
	✓ ✓ ✓ ✓ ✓ ✓ 36 40 44 48 52 56 60 64 100 ✓ ✓ ✓ ✓ ✓ 140 143 153 157 161 165	V V V 104 108 112 116 120 124 128 132 136
	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。
Cisco Catalys	t 9800-40 Wireless Contro	bller Welcome alpha 🛛 🌴 🏗 🖨 🖄 😡 📿 Ser	rch APs and Clients Q
Q Search Menu Items	onfiguration * > Radio Configuratio	ons* > RRM	
Dashboard	5 GHz Band 2.4 GHz Band	FRA	
Monitoring >	General Coverage DCA	TPC RF Grouping	
	Dynamic Channel Assignment	t Algorithm	
() Administration >			
₩ Troubleshooting	Channel Assignment Mode	Automatic	
		O off	
	Interval	10 minutes V	
	Anchortime	0 •	
	Avoid Foreign AP Interference		
	Avoid Cisco AP load		
	Avoid Non 5 GHz Noise		
	Avoid Persistent Non-wifi Interference		
	Channel Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9)	
	Last Auto Channel Assignment	531 second(s) ago	
	DCA Channel Sensitivity	medium	
	Auto-RF Channel List		
	1 2 3 4 5 6 7 8		
	9 10 11		
	Event Driven RRM		
	EDRRM		

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

Cisco Cata	alyst 9800-40 Wirel	less Controller	Welcome alpha 🛛 🏠 📢	B 🏶 🖗 O C	Search APs and Clients Q
Q. Search Menu Items	Configuration - > W	Edit Radios 5 GHz Ban	d		×
Dashboard		Configure Detail			
	Number of AP(s): 1	General		RF Channel Assignmen	it
		AP Name	rcdn6-22a-ap1	Current Channel	149
	Name Model	Admin Status		Channel width	40 MHz v
(O) Administration >	rcdn6-22a- ap1 AP380 B-K9	CleanAir Admin Status	ENABLED	Assignment Method	Global 🔻
X Troubleshooting	⊨ ∢ 1 ≻	Antenna Parameters		Tx Power Level Assign	ment
		Antenna Type	Internal v	Current Tx Power Level	2
	✓ 5 GHz Radios	Antenna Mode	Omni	Assignment Method	Global
	AP v Slot	Antenna A			
	Name No rcdn6-22a-	Antenna B			
	ap1	Antenna C			
		Antenna D	✓ 10		
	> 2.4 GHz Radi				
	> 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 Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ (たとえば 802.11a のみ) 適用するよう指定できます。

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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



高速セキュアローミングに 802.11r(FT)を利用するには、**[高速移行(Fast Transition)]** を**[有効 (Enabled)]**にするボックスをオンにします。

[Over the DS] をオフにして、Over the Distribution システム方式の代わりに Over the Air 方式を使用することを推奨します。

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

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

¢	cisco Cis	sco Catal	Catalyst 9800-40 Wireless Controller						Welcome al	oha 🔺 🕯	\$ 🖺 🔅	000	Search APs	and Clients Q	•
٩	Search Menu Items		Conf	iguratio	n • > Tags	& Profiles - >	Edit WLAN								×
							General	Security	Advanced						
	Dashboard						Layer2	Layer3	AAA						
٢	Monitoring	>	Numb	er of WL	ANs selected	ı : O	Lover 3 Coourit	u Mode							
Ľ	Configuration	>		Status	Name	√. ID	Layer 2 Securi	y wode		WFA T WFA2	•	Fast Tran	sition	Enabled	۳
- 563	Administration	>		0	Voice	1 <	MAC Filtering					Over the	DS		
~ S	Troubloobootin			U	Data	2	Protected Ma	anagement	Frame			Reassoci	ation Timeout	20	
<i>8</i> 5	rroubleshoolin	ıg					PMF			Disabled	•				
							WPA Parame	ters							
							WPA Policy								
							WPA2 Policy			\checkmark					
							WPA2 Encrypti	on		AES(CCMP128) CCMP256					
										GCMP128 GCMP256					
							MPSK								
							Auth Key Mami			802 1x					
							Add Rey Mgm			PSK					
										CCKM					
										FT + 802.1x FT + PSK					
										802.1x-SHA256					
										PSK-SHA256					
													_		
							Cancel						Ē	Update & Apply 1	o Device
						I									

÷	Cisco Cisco Ca	Cisco Catalyst 9800-40 Wireless Controller							lpha 🖌 🏠	6 B	• 19	02		s and Clients Q	•
٩	Search Menu Items	Con	figuratio	on•> Tags	& Profiles * >	Edit WLAN									×
		_				General	Security	Advanced							
	Dashboard				Enable WLAN	Layer2	Layer3	AAA							
\odot	Monitoring >	Num	ber of W	LANs selected	d : 0										
Z,	Configuration >		Status	Name	v: ID	Layer 2 Security	Mode		WPA + WPA2	•	I	Fast Transition		Enabled	•
~	Administration		o	Voice	1 <	MAC Filtering						Over the DS			
167	Administration		O	Data	2	Protected Ma	nagement	Frame			1	Reassociation	Timeout	20	
X	Troubleshooting	14	∢ 1	▶ ►	10 🔻 items p										
						PMF			Disabled	•					
						WPA Paramet	ers								
						WPA Policy									_
						WPA2 Policy			~						_
						WPA2 Encryptio	n		AES(CCMP128)						
									CCMP256 GCMP128						
									GCMP256						
						MPSK									
						Auth Kev Mamt			802.1x						
									PSK						- 1
									CCKM						- 1
									FT + 802.1x						- 1
									FT + PSK						- 1
									802.1x-SHA256	6 🗌					- 1
									PSK-SHA256						
						PSK Format			ASCII	•					
						DSK Tupe			Unencrynted	-					
						Cancel							6	Update & App	ly 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、CCKM、PSK も有効にできます。802.1x や PSK を使用するかどうかに応じて、802.11r(FT)をサポートしない音声クライアントも含まれます。

高速セキュア ローミングに CCKM を利用するには、AES 暗号化を使用した WPA2 ポリシーと認証キー管理タ イプ用の 802.1x + CCKM を有効にします。

デフォルトの CCKM タイムスタンプ許容値は 1000 ミリ秒に設定されます。

Cisco Wireless Phone 840 および 860 のローミングエクスペリエンスを最適化するために、**CCKM タイムス タンプ許容値**は 5000 ミリ秒に調整することをお勧めします。

٠	cisco Cisco Cal	talyst 9800	-40 Wirele	ess Controller		Welcome alpha	** 8	000	Search Affs and Clerce Q	
	Search Menu Items	Configurati	on•> Tags	& Profiles * >	Edit WLAN					×
	Dashboard	+ Add		Enable WLA	General Security	Advanced				
	Monitoring >	Number of V	LANs selected	d : 0	Layer2 Layer3	AAA				
2	Configuration >	Statut	Name	~ 10	Authentication List	authentica	tion_dot1x +			
ŝ	Administration >	0	Voice	1 <	Local EAP Authentication					
×	Troubleshooting		E F F	10 • items p						
										_
					D Cancel				🗄 Update & Apply 1	o Device

[Aironet IE] は [有効 (Enabled)] にしないでください。

[ピアツーピア (P2P) のブロッキングアクション (Peer to Peer (P2P) Blocking Action)] を 無効にする必要があります。

WMM ポリシーは、この SSID が Cisco Wireless Phone 840 および 860 などの WMM 対応電話機で使用され ている場合にのみ、**[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。

非 WMM クライアントが Cisco Wireless Phone 840 および 860 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。

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

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

[オフチャンネルスキャンの待機 (Off Channel Scanning Defer)]を調整することで、スキャンの待機時間だけでなく、特定のキューに対するスキャンを待機させることができます。

キュー4~6の遅延優先順位を有効にすることをお勧めします。

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

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

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

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

802.11k および 802.11v を有効にすることを推奨します。

Cisco Cata	lyst 9800-40 Wireless Controller	Welcome alpha 🛛 😭 👘	🖺 🏟 🔞 🗭 🎜 Search APs and Clients Q
Q Search Menu Items	Configuration * > Tags & Profiles * > WLANs	Edit WLAN	×
		General Security Advanced	
Dashboard		Coverage Hole Detection	Universal Admin
Monitoring >	Number of WLANs selected : 0	Aironet IE	Load Balance
Configuration >	Status Name - ID - SSID	P2P Blocking Action Disabled +	Band Select
(○) Administration →	Voice 1 voice	Multicast Buffer	IP Source Guard
Y Troubleshooting	H 4 1 > H 10 v items per page	Media Stream Multicast-	WMM Policy Required v
		Max Client Connections	mDNS Mode Bridging v
			Off Channel Scanning Defer
		Per WLAN 0	
		Per AP Per 0 WLAN	Priority 0 1 2
		Per AP Radio 200 Per WLAN	3 4 5
		11v BSS Transition Support	6 7
			Scan Defer 100 Time
		BSS Transition	Assisted Roaming (11k)
		Disassociation Imminent(0 200 to 3000 TBTT)	
		Optimized Roaming 40	Optimization
		40 TBTT)	Neighbor List
		BSS Max Idle Service	Dual Band Neighbor
		BSS Max Idle Protected	DTIM Period (in beacon intervals)
		Directed Multicast Service	
		11ax	5 GHz Band (1-255) 2
		Downlink OFDMA	2.4 GHz Band (1-255) 2
		Unlink OFDMA	
		D Cancel	T Undate & Apply to Device

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 Cisco Cata	alyst 9800-40 Wirel	less Controller Weld	come alpha 🛛 🐔 🥵	8	🖄 😧 🎜 Search Al	Ps and Clients Q
٩	Search Menu Items	Configuration - > T	dit Policy Profile				×
	Dashboard	+ Add × Delt	General Access Policies	QOS and AVC Mo	loss of conne	Advanced ectivity for clients associated wi	th this profile.
٢	Monitoring >	Status v Pol					
Ľ	Configuration >	Dat	Name*	Voice		WLAN Switching Policy	
ক্ট্য	Administration >	Ø defi	Description	Enter Description		Central Switching	
×	Troubleshooting	⊨ 1 ⊨ ⊨	Status			Central Authentication	ENABLED
			Passive Client	DISABLED		Central DHCP	
			Encrypted Traffic Analytics	DISABLED		Central Association	
			CTS Policy			Flex NAT/PAT	DISABLED
			Inline Tagging				
			SGACL Enforcement				
			Default SGT	2-65519			
		(D Cancel				Update & Apply to Device

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 Cata	alyst 9800–40 Wi	reless Controller Welco	ome alpha 🛛 😭 🌾 🖺 🕯	0 10	Search	APs and Clients Q	•
Q Search Menu Items	Configuration - >	Edit Policy Profile					×
	+ Add X D	General Access Policies	QOS and AVC Mobility	Advanced			
		RADIUS Profiling			WLAN ACL		
Monitoring >	Status 🗸 F	Local Subscriber Policy Name	Search or Select		IPv4 ACL	Search or Select	•
Configuration >		WLAN Local Profiling			IPv6 ACL	Search or Select	v
Administration >	□ Ø c	Global State of Device Classification	Disabled (i)		URL Filters		
X Troubleshooting		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。

Cisco Cata	alyst 9800-40 Wi	reless Controlle	er Welcome alpha	* * 🗎 🔅	902	Search APs and Clients Q	•
Q Search Menu Items	Configuration - >	Edit Policy Profile					×
	+ Add X D	General Acc	QOS and AV	C Mobility Ad	dvanced		
		Auto QoS	None v		Flow Monitor I	Pv4	
() Monitoring >	Status V	QoS SSID Policy	r	E	Egress	Search or Select	
Configuration >		Egress	platinum 🗙 🔻	1	ngress	Search or Select	
() Administration >	□ Ø ¢	Ingress	platinum-up 🗙 🔻		Flow Monitor I	Pv6	
💥 Troubleshooting		QoS Client Polic	У	E	Egress	Search or Select	
		Egress	Search or Select 🔻	1	ngress	Search or Select 🚽	
		Ingress	Search or Select 🔻				
		SIP-CAC					
		Call Snooping					
		Send Disassociate					
		Send 486 Busy					
		Cancel				Update & Apply to D	evice

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

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

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

¢	Cisco Cat	alyst 9800-40 W	ireless Controller	elcome alpha	6 🖹 🔅	🕸 🛛 🗶 Sear	ch APs and Clients Q
٩	Search Menu Items	Configuration - >	Edit Policy Profile				×
			General Access Policies	QOS and AVC	Mobility	Advanced	
	Dashboard	+ Add × D	WLAN Timeout			Fabric Profile	Search or Select
٢	Monitoring >	Status v F	Session Timeout (sec)	86400		Umbrella Parameter Map	Not Configured 🗸
Ľ	Configuration >		Idle Timeout (sec)	300		mDNS Service	default-mdns-servic
ট্ট	Administration >	□ Ø ¢	Idle Threshold (bytes)	0		Policy	Clear
X	Troubleshooting	⊣	Client Exclusion Timeout (sec)	60]	WLAN Flex Policy	
			DHCP			VLAN Central Switching	
			IPv4 DHCP Required			Split MAC ACL	Search or Select
			DHCP Server IP Address			Air Time Fairness Po	licies
			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 👻)		
		_	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、および詳細設定を指定できます。

Cisco Wireless Phone 840 および 860 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	Catalyst	9800-40	Wireless Controller	Welcome alpha	* 🕏 🖺	* * • • •	Search APs and Clients Q	•
Q Search Menu Items	Cor	nfiguration -	> Tags & Profiles - > RF					
Dashboard		Add						
Monitoring	>	State 🖂	RF Profile Name	Band	 Descrip 	tion		Υ.
Configuration	, C	•	Low_Client_Density_rf_5gh	5 GHz	pre cont	figured Low Client Density rf		
		o	High_Client_Density_rf_5gh	5 GHz	pre cont	figured High Client Density r		
(O) Administration	> Add	RF Profile					×	
💥 Troubleshooting		General	802.11 RRM Advanced					
	N	lame*	Enter Name					
	R	adio Band	5 GHz Band 🔻				1 - 6 of 6 it	
	s	tatus	DISABLE					
	D	escription	Enter Description					
	c	Cancel				Apply to Device		

[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 Catalyst 9800-40 Wireless Controller Welcome alpha 🖌 🛪 🛱 🖗 🖗 🖉 Search APs and Clients Q										
Q Search Menu Items	Configuration - > Tags & Profiles -	> RF								
📰 Dashboard	+ Add × Delete									
Monitoring >	State 🖂 RF Profile Name	M Band	V Description		~.					
<pre> Configuration</pre>	Low_Client_Density_rf_	_5gh 5 GHz	pre configure	d Low Client Density rf						
~~	High_Client_Density_rf	_5gh 5 GHz	pre configure	d High Client Density r						
205 Administration >	Add RF Profile			×						
% Troubleshooting	General 802.11 RRM	Advanced								
	Operational Rates	802.11	n MCS Rates							
	6 Mbps Disabled	▼ Enabled	Data Rates:		1 - 6 of 6 items					
	9 Mbps Disabled	9 Mbps Disabled v [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,	22,23,24,25,26,27,28,29,30,31]							
	18 Mbps Supported	▼ Enable	MCS Index V							
	24 Mbps Supported	•	0							
	36 Mbps Supported	•	1							
	48 Mbps Supported	•	2							
	54 Mbps Supported	•	3							
			4							
			5							
			6							
			1							
			8							
		\checkmark	Э							

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

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

Cisco Ca	atalyst 9800-40 Wireless Controller Welcome	alpha 🌴 📽 🖺 🏟 🚳 🥹 📿 🛛 Search APs and Clients 🔍 🛛 🖬
Q Search Menu Items	Configuration • > Tags & Profiles • > RF	
Dashboard	+ Add × Delete	
Monitoring	State v RF Profile Name v Band	 Description
<pre> Configuration > </pre>	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
(O) Administration >	Add RF Profile	×
💥 Troubleshooting	General 802.11 RRM Advanced	
	General Coverage TPC DCA	
		1.0.40 hours
	Coverage Hole Detection	i - o or o items
	Minimum Client Level (clients)*	
	Data RSSI Threshold (dBm)* -80	
	Voice RSSI Threshold (dBm)* -80	
	Exception Level(%)* 25	
	S Cancel	Apply to Device

Cisco Cata	alyst 9800-40 Wireless Controller	Welcome alpha	📽 🖺 🏟 👰 😧 Search APs and Clients Q
Q Search Menu Items	Configuration - > Tags & Profiles - > RF		
📰 Dashboard	+ Add × Delete		
Monitoring >	State 🖂 RF Profile Name	v Band v	Description
Configuration >	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
∑ Administration →	Add RF Profile		×
💥 Troubleshooting	General 802.11 RRM Advanced		
	General Coverage TPC DCA		
	Transmit Power Control		1 - 6 of 6 items
	Maximum Power Level(dBm)* 30		
	Minimum Power Level(dBm)* -10		
	Power Threshold V1(dBm)* -70		
	Cancel		Apply to Device

Cisco Cisco Cat	alyst 9800-40 Wireless Control	ler Welcome alpha 🖀	\$ B \$ \$ 0 2 [Search APs and Clients Q
Q Search Menu Items	Configuration • > Tags & Profiles • >	RF		
📰 Dashboard	+ Add Celete			
Monitoring >	State 🖂 RF Profile Name	 Band 	Description	v
<pre>Configuration ></pre>	Low_Client_Density_rf_5g	gh 5 GHz	pre configured Low Client Density rf	
~	High_Client_Density_rf_5	gh 5 GHz	pre configured High Client Density r	
Administration >	Add RF Profile		3	ĸ
💥 Troubleshooting	General 802.11 RRM	Advanced		
	Oreand Oreans TDO	D04		
	General Coverage TPC	DCA		
	Dynamic Channel Assignment			1 - 6 of 6 items
	Avoid AP Foreign AP Interference	V		
	Channel Width	20 MHz 40 MHz 80 MHz Best	0 160 MHz	
	DCA Channels	y y	✓ ✓ ✓ ✓ ✓ ✓ 104 108 112 116 120 124 165	
	High Speed Roam			
	Mode Enable			
	Neighbor Timeout*	5		
	Client Network Preference	Default v		
	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)]、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。

Cisco Catal	yst 9800-40 Wireless Controlle	er Welcome alpha 🖌 👫	🌾 🖺 🌣 🖄 🛛 🎜 Search	APs and Clients Q
Q Search Menu Items	Configuration • > Tags & Profiles • >	RF		
📰 Dashboard	+ Add X Delete			
Monitoring >	State 🖂 RF Profile Name	Band	V Description	×.
	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf	
~~	High_Client_Density_rf_5gh	n 5 GHz	pre configured High Client Density r	
¿O∫ Administration →	Add RF Profile		×	
X Troubleshooting	General 802.11 RRM Ac	dvanced		
	High Density Parameters			
	Max Clients*	200		1 - 6 of 6 items
	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		
	Bridge Client Access	DISABLED		
	Airtime Allocation	5		
	FRA			
	Client Aware		I	

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。

802.11r (FT) または CCKM を使用している場合は、同じ Flex プロファイル内のアクセスポイントにローミン グするときにのみ、シームレスなローミングを実現できます。

使用するアクセスポイントのネイティブ VLAN ID と、許可された VLAN を設定します。

[ARPキャッシング (ARP Caching)]が[有効 (Enabled)]になっていることを確認します。

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

¢	ului cisc	Cisco Catalyst 980	0-40 Wireless Contro	oller	Welcome alpha	V o	₿ \$	Ø 3	0		Q	•
۵ ۵	Search Me	nu Items	ration - > Tags & Profiles -	> Flex								
	Dashbo	pard + Add	d X Delete									
(j) I	Moni A	dd Flex Profile									×	~
2,0	Conf	General Local Auth	nentication Policy ACL	VLAN							•	
(j) /	Admi	Name*	Enter Name		Fallback Radio Shut							
X 1	Froul	Description	Enter Description		Flex Resilient							
		Native VLAN ID	1		ARP Caching		\checkmark					
		HTTP Proxy Port	0		Efficient Image Upgrade		\checkmark					
		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 Devi	ce	

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。

16.12.2s		NCOller Welcome alpha		
Q Search Menu Items	Configuration - > Tags & Profil	Edit Policy Tag		×
📰 Dashboard	Policy Site RF A	A Changes may result in los	s of connectivity for some clients that are associated t	o APs with this Policy Tag.
Monitoring >	+ Add × Delete	Name* default-p	olicy-tag	
Configuration >	Policy Tag Name	Description default po	licy-tag	
() Administration >	default-policy-tag	VULAN-POLICY Maps: 2	2	
💥 Troubleshooting	ia a 1 ⊳ ⊨ 10			
		WLAN Profile	V Policy Profile	¥.
		Data	Data	
		Voice	Voice	
		⊣	items per page	1 - 2 of 2 items
		Map WLAN and Policy		
		Map WLAN and Policy WLAN Profile* Voice	▼ Policy Profile*	Voice 🔻
		Map WLAN and Policy WLAN Profile* Voice	Policy Profile* X	Voice
		Map WLAN and Policy WLAN Profile* Voice RLAN-POLICY Maps: 0	Policy Profile*	Voice
		Map WLAN and Policy WLAN Profile* Voice RLAN-POLICY Maps: 0	Policy Profile*	Voice
		Map WLAN and Policy WLAN Profile* Voice RLAN-POLICY Maps: 0	Policy Profile*	Voice
		Map WLAN and Policy WLAN Profile* Voice RLAN-POLICY Maps: 0	Policy Profile*	Voice

<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。

16.12.2s	
Q. Search Menu Items Configuration - > Tags & Profiles - > Tags	
Dashboard Policy Site RF AP	
(Monitoring > + Add × Delete	
Configuration Site Tag Name Description	~
Administration default-site-tag default site tag	
Add Site Tag Add Si	
S Cancel	

<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 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 Cisco	Catalyst 9800-40 Wireless Controller	Welcome alpha		Search APs and Clients Q
Q Search Menu Items	Configuration - > Tags & Profiles - > Ta	gs		
E Dashboard	Policy Site RF AP			
Monitoring	> + Add × Delete			
Configuration	> RF Tag Name	×.	Description	×
S Administration	> default-rf-tag		default RF tag	
X Troubleshooting	Add RF Tag		×	1 - 1 of 1 items
	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	

タグを定義したら、アクセスポイントに適用できます。

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

Cisco Cat cisco 16.12.2s	talyst 9800-40 W	ireless Controller	Welcome alpha	♥ 🖹 ♥ 🖄 0 📿 🖻	Search APs and Clients Q
	Configuration - >	Edit AP		ing the second	
Dashboard	 All Access Number of AP(c): 1 	General	High Availability In	Version	
Monitoring >	Number of AF(5).	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- AP	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
X Troubleshooting	api ••• B-k	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status	ENABLED	Boot Version	1.1.2.4
	> 5 GHz Rac	AP Mode	Local v	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 IPv4	1
	A	LED Brightness Level	8 🔻	DHCP IPv4 Address 10.	201.81.125
	Country	CleanAir NSI Key		Static IP (IPv4/IPv6)	
	LSC Provis	Tags		Time Statistics	
		Policy	default-policy-tag v	Up Time	10 days 18 hrs 16 mins 54 secs
		Site	default-site-tag	Controller Association Latency	2 mins 4 secs
		KF	derault-rf-tag v		
		Cancel			Update & Apply to Devic

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。

Cisco Cat	alyst 9800-40 W	/ireless Controller	Welcome alpha	6 B ¢ Ø Ø C S	earch APs and Clients Q
Q Search Menu Items	Configuration - >	Edit AP			×
Dashboard	✓ All Acces	General Interfaces	High Availability Inver	ntory ICap Advanced	
Monitoring >	Number of AP(s): 1	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
$<\!$	AP × A Name M	Location*	rcdn6-22	Predownloaded Status	N/A
() Administration >	rcdn6-22a- A	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
💥 Troubleshooting	B. I ≪ 1	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-Bar	LED State		CAPWAP Preferred Mode IPv4	
	Country	LED Brightness Level	8 🔻	DHCP IPv4 Address 10.2	201.81.125
		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	Controller Association Latency	10 secs
		RF	default-rf-tag v		
		Cancel			Update & Apply to Device

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 Cat	alyst 9800-40	Wireless Controller	Welcome alpha	0 🖄 🌣 🖪 🔊 I	Search APs and	Clients Q
Q Search Menu Items	Configuration -	> Wireless - > Wireless	s Global			
Dashboard	Default Mobility	CTG-VoWLAN3		Assisted Roaming		
Monitoring >	Domaiń *			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。

Cisco Cata	lyst 9800-40 Wireless Controller	Welcome alpha	6 B \$ \$ 0 C	Search APs and Clients Q
Q Search Menu Items	Configuration - > Wireless - > Mobility			
📻 Dashboard	Global Configuration Peer Configuration			
Monitoring >	Mobility Group Name*	CTG-VoWLAN3		🖹 Apply
<pre>Configuration ></pre>	Multicast IPv4 Address	0.0.0.0		
、 の Administration	Multicast IPv6 Address	:		
	Keep Alive Interval (sec)*	10		
X Troubleshooting	Mobility Keep Alive Count*	3		
	Mobility DSCP Value*	48		
	Mobility MAC Address*	706d.153d.b50b		
Cisco Cataly 16.12.2s	st 9800-40 Wireless Controller	Welcome alpha	S O Ø 🕸 & 🛯 🔊	Search APs and Clients Q
🔜 Dashboard	Global Configuration Peer Configuration			
Monitoring >	 Mobility Peer Configuration 			
Configuration >	+ Add × Delete			
() Administration →	MAC Address \checkmark IP Address \checkmark	Public IP v Group Nam	e v Multicast IPv4 v Sta	tus v PMTU v
₩ Troubleshooting	706d.153d.b50b 10.201.81.9	N/A CTG-VoWL	AN3 0.0.0.0 N/A	N/A
	Image: Second control of the second contro	10.201.81.10 CTG-VOWE	AN3 0.0.0.0 Up	1 - 2 of 2 items
	> Non-Local Mobility Group Multicast	Configuration		

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

Cisco Cata	alyst 9800-40 Wireless Controller Wei	Icome alpha 🛛 🕋 🌾 🛛	8 ¢ 0 0 ¢	Search APs and Clients Q
Q Search Menu Items	Configuration - > Interface - > Wireless			
Dashboard	+ Add X Delete			
Monitoring >	Interface Name v Interface Type v Trustpo	pint Name v VLAN ID	V IP Address V	IP Netmask v MAC Address v
Configuration >	Vlan310 Management	310	10.201.81.9	255.255.255.240 70:6d:15:3d:b5:0b
💥 Troubleshooting				

コール アドミッション制御 (CAC)

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

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

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

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

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

音声ストリームのサイズと音声ストリームの最大数の値は、必要に応じて調整できます。 SRTP を使用している場合は、音声ストリームのサイズを増やす必要がある場合があります。

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

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

Cisco Catalys	t 9800-40 Wireless Co	ontroller We	elcome alpha	* 🖹 🌣 🖄 O 2	Search APs and Clier	nts Q
Q Search Menu Items	onfiguration - > Radio Confi	gurations - > Mec	dia Parameters			
E Dashboard	5 GHz Band 2.4 GHz Ba	nd				
Monitoring >						
	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 (%)*	05	, 1	Expedited 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 Parameters	Direct		Metrics Collection		
	Multiment Direct Fredela			Stream Size*	84000	
	Multicast Direct Enable	No. 1 Jacob		Max Streams*	2	
	Max streams per Radio	No Limit		Inactivity Timeout		
	Max streams per Client		•			
	Best Effort OOS 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)**]を有効にする必要があります。

Cisco Ca 16.12.2s	Configuration -> Services -> Multicast	Welcome alpha 🛛 👫 🌾 🖺 🌞 🖄 🌘	Search APs and Clients Q
Dashboard Monitoring	Global ENABLED NUTreless Multicast Mode	IGMP Snooping	臣 Apply
Configuration >	Wireless Mon-	Disabled	Q Search
Administration >	Ureless DisableD	Status VLAN ID Name	Status VLAN ID Name
X Troubleshooting	AP Capwap Unicast		↓ 1 default ← ↓ 310 VLAN0310 ←
	MULTICAST	No Vlan available	 ✓ 400 VLAN0400 € ✓ 500 VLAN0500 €
	IGMP Snooping Querier		
	IGMP ENABLED		
	Last Member Querier Interval (milliseconds)		Disable All
	Wireless Broadcast and Wireles	s Non-IP Multicast	

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

次に、ストリームを設定します。

Cisco Cisco (16.12.2s	Catalyst 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 🔽
🔧 Configuration	> Session Message Config
() Administration	Session Announcement
💥 Troubleshooting	Session Announcement URL
	Session Announcement Email
	Session Announcement Phone
	Session Announcement Note

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

Cisco Cata	alyst 9800-40 W	ireless Controller Welcome alpha 💣 🕏	🖹 🏶 🖄 🚱 🎜 Search APs and Clients Q
Q Search Menu Items	Configuration - >	Edit WLAN	×
📰 Dashboard	+ Add × I	General Security Advanced	Universal Admin
Monitoring >	Number of WLANs s	Aironet IE	Load Balance
Configuration >	Status Name	P2P Blocking Action Disabled	Band Select
() Administration >	Voić.	Multicast Buffer	IP Source Guard
💥 Troubleshooting		Media Stream Multicast-	WMM Policy Required v
		Max Client Connections	mDNS Mode Bridging V
			Off Channel Scanning Defer
		Per WLAN 0 Per AP Per 0 WLAN	Defer 0 1 2 Priority 3 2 4 5
		Per AP Radio 200 Per WLAN	✓ 6 7
		11v BSS Transition Support	Scan Defer 100 Time
		BSS Transition	Assisted Roaming (11k)
		Disassociation Imminent(0 200 to 3000 TBTT) Optimized Reaming	Prediction Optimization
		40 TBTT)	Neighbor List
		Cancel	📄 Update & Apply to Device

詳細設定

EAP の詳細設定

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

Cisco Cat	alyst 9800-40 Wireless Controller	Welcome alpha	🕈 🛱 🛱 🖗 🖗 📿 🛛 Searc	h APs and Clients Q
Q Search Menu Items	Configuration - > Security - > Advance	ed EAP		
Dashboard	EAP-Identity-Request Timeout (sec)*	30		
Monitoring >	EAP-Identity-Request Max Retries*			
Configuration >	Response			
() Administration >	EAP-Request Max Retries*	2		
💥 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。

EAP の失敗が頻繁に発生する展開では、**[EAP 要求タイムアウト (EAP-Request Timeout)**]を 30 秒未満に減 らす必要があります。

PSK を使用する場合は、**[EAPOL キーのタイムアウト (EAPOL-Key Timeout)**]をデフォルトの 1000 ミリ秒から 400 ミリ秒に減らし、**[EAPOL キーの最大試行回数 (EAPOL-Key Max Retries)**]をデフ ォルトの 2 から 4 に設定することを推奨します。 802.1x を使用する場合は、**[EAPOL キーのタイムアウト (EAPOL-Key Timeout)**]および **[EAPOL キ 一の最大試行回数 (EAPOL-Key Max Retries)**]のデフォルト値 (それぞれ 1000 ミリ秒および 2) を 使用しても正しく動作しますが、それぞれ 400 および 4 に設定することを推奨します。

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

[EAP-Broadcast Key Interval] が 3600 秒(1 時間)以上に設定されていることを確認します。

Rx SOP しきい値

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

Cisco Cat	alyst 9800-40 Wireless Controller Welcome alpha 🛛 🏶 <table-cell> 🏶 🕲 🖉 Search APs and Clients Q</table-cell>	•
Q Search Menu Items	Configuration - > Wireless - > Advanced	
詞 Dashboard	Load Balancing Band Select Optimized Roaming High Density Preferred Calls	
Monitoring >		
Configuration >	Rx Sop Threshold	
رِنَ Administration ،	Rx Sop Threshold 5 GHz (dbm)	
✓ Troubleshooting	Rx Sop Threshold 2.4 GHz (dbm)	
	Multicast Data Rate	
	Multicast Data Rate 5 GHz (Mbps)	
	Multicast Data Rate 2.4 GHz (Mbps)	

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 Cata	alyst 9800-40 Wireless Controlle	er Welcome alpha	* 📽 😬 * 🕅 6	Search APs and Clients Q
Q. Search Menu Items	Configuration - > Security - > Wirele	ess Protection Policies		
📰 Dashboard	Rogue Policies RLDP Rogue	AP Rules Client Exclusi	on Policies	
Monitoring >	Rogue Location Discovery	Disable 🔻		
Configuration >	Retry Count	1		
() Administration >	Schedule RLDP)		
💥 Troubleshooting	Day Start Time	e End Time		
	Monday	©		
	Tuesday	•		
	Wednesday	•		
	Thursday	•		
	Friday	•		
	Saturday	•		
	Sunday	©		

設定例

バージョン 16.12 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption service internal service call-home platform qfp utilization monitor load 80 no platform punt-keepalive disable-kernel-core I. hostname RCDN6-21A-WLC5 L boot-start-marker boot system flash bootflash:packages.conf boot-end-marker L vrf definition Mgmt-intf 1 address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! no logging console ! aaa new-model I. I

aaa group server radius RADIUS_SERVER_GROUP_DAY0 server name RADIUS_SERVER_DAY0_1 server name RADIUS_SERVER_DAY0_2 L 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 L aaa server radius dynamic-author aaa session-id common clock timezone CST -6 0 clock summer-time CDT recurring call-home ! call-home の連絡先電子メールアドレスが <u>sch-smart-licensing@cisco.com</u> 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 L ip domain name cisco.com login on-success log subscriber templating parameter-map type webauth global virtual-ip ipv4 1.1.1.6 flow exporter wireless-local-exporter destination local wlc flow monitor wireless-avc-basic exporter wireless-local-exporter cache timeout active 60 record wireless avc basic no device-tracking logging theft access-session mac-move deny multilink bundle-name authenticated L 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 CB84C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520 1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE 4AA4E80D D86FD1C9 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
```

```
Į.
license udi pid C9800-40-K9 sn TTM231803A3
memory free low-watermark processor 375973
service-template webauth-global-inactive
inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
diagnostic bootup level minimal
username <REMOVED> privilege 15 password 7 <REMOVED>
redundancy
mode sso
vlan internal allocation policy ascending
class-map match-any AVC-Reanchor-Class
match protocol cisco-jabber-audio
match protocol cisco-jabber-video
match protocol webex-media
match protocol webex-app-sharing
match protocol webex-control
match protocol webex-meeting
match protocol wifi-calling
L
interface Port-channel3
switchport trunk native vlan 310
switchport trunk allowed vlan 310,400,500
switchport mode trunk
ŗ.
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 1 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 L 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 1 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 1 interface GigabitEthernet0 vrf forwarding Mgmt-intf ip address 10.201.81.25 255.255.255.240 negotiation auto no cdp enable L interface Vlan1 no ip address shutdown L interface Vlan310 description Management ip address 10.201.81.9 255.255.255.240 L 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 I. interface Vlan500 description Voice ip address 10.201.83.14 255.255.255.0 ip helper-address 72.163.42.112 ip helper-address 173.37.137.70 ip default-gateway 10.201.81.1 ip forward-protocol nd

```
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ip tftp blocksize 8192
ip route 0.0.0.0 0.0.0.0 10.201.81.1
L
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
L
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
L
line con 0
exec-timeout 60 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
ntp server 10.81.254.202
ntp server 10.115.162.212
wireless mobility group member mac-address 6c31.0e7b.b8eb ip 10.201.81.10 public-ip
10.201.81.10 group CTG-VoWLAN3
wireless mobility group name CTG-VoWLAN3
wireless mobility mac-address 706d.153d.b50b
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile
wireless management interface Vlan310
wireless profile airtime-fairness default-atf-policy 0
wireless profile flex default-flex-profile
description "default flex profile"
wireless profile mesh default-mesh-profile
description "default mesh profile"
wireless profile policy Data
```

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

no shutdown ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh coverage data rssi threshold -90 coverage level 2 coverage voice rssi threshold -90 description "pre configured Low Client Density rfprofile for 2.4gh radio" high-density rx-sop threshold low tx-power v1 threshold -65 no shutdown ap dot11 24ghz rf-profile High_Client_Density_rf_24gh description "pre configured High Client Density rfprofile for 2.4gh radio" high-density rx-sop threshold medium rate RATE_11M disable rate RATE_12M mandatory rate RATE_1M disable rate RATE_2M disable rate RATE_5_5M disable rate RATE_6M disable tx-power min 7 no shutdown ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh description "pre configured Typical Client Density rfprofile for 2.4gh radio" rate RATE_11M disable rate RATE_12M mandatory rate RATE_1M disable rate RATE_2M disable rate RATE_5_5M disable rate RATE_6M disable no shutdown ap dot11 24ghz media-stream multicast-direct ap dot11 24ghz media-stream video-redirect no ap dot11 24ghz cac voice tspec-inactivity-timeout ap dot11 24ghz cac voice tspec-inactivity-timeout ignore ap dot11 24ghz cac voice acm ap dot11 24ghz edca-parameters optimized-video-voice ap dot11 24ghz exp-bwreg 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)]または [CCKM] が [有効 (Enabled)]になっていることを確認します。
- [Quality of Service (QoS)]を[プラチナ (Platinum)]に設定します
- 802.11k を [有効 (Enabled)]に設定することを推奨
- 802.11v を有効に設定することを推奨
- **[P2P(ピアツーピア)ブロッキング アクション(P2P (Peer to Peer) Blocking Action)]** を 無効にします
- [クライアントの帯域選択 (Client Band Select)]を[無効 (Disabled)]に設定します
- [クライアントの負荷分散 (Client Load Balancing)] を [無効 (Disabled)]に設定します
- 必要に応じて [データレート (Data Rates)]を設定します
- 必要に応じて [RF 最適化 (RF Optimization)]を設定します
- [トラフィックタイプ (Traffic Type)]を[音声とデータ (Voice and Data)]に設定します
- CleanAir テクノロジーを搭載した Cisco 製アクセス ポイントを使用している場合は、 [CleanAir] を有効にします。
- 必要に応じて [マルチキャストダイレクト (Multicast Direct)]を設定します

コントローラの設定

[コントローラ (Controller)]機能を含むように、1 つ以上の Mobility Express 対応アクセスポイントの **[動作モード (Operating Mode)**]を設定します。

必要に応じて [AP 名 (AP Name)]と [IP 設定 (IP settings)]を設定します。

B	Monitoring	Cisco Aironet 1850 Series Mobility Express		Q	A	٩	Ð	Ħ		٥
\$	Wireless Settings ⋒ wLANs	ACCESS POINTS ADMINISTRATION								
		Access Points 2								
	Access Points Groups	AP1850-1 (Active Controller) General Controller Radio 1/2.4 GHz) Radio 2 (5GHz) 802-11	Global AP C	onfiguratio	n Cor	wert to M	0	Convert to	CAPWAP	0
	ở WLAN Users		0.1							
	管 Guest WLANs		er 😲 Pri	mary Con	troller and	I Preferre	ed Maste	r 19 Pre	ferred M	laster
		Refresh								
	* Mesh	Sele Mans Type Location		Up Time			AP Mo	del		
÷.	Management	AP Model AIR-AP1852LA-K9		0 days, 14	h 37 m 4	4 s	AIR-AP	1852I-A-K	9	
J.C	Services	IP Configuration Obtain from DH •		0 days, 14	ih 37 m 4	4 s	AIR-AP	1852I-B-K	9	
÷	Services	IP Address 10.0.0.100								
~	Advanced	Subnet Mask 255:255.0								
		Gateway 10.0.0.1								
		AP Name AP1850-1								
		Location default location								
		Set as Preferred Master								
		H < 1 1 + H 10 v items per page To apply change in Preferred Master setting, save configuration and reset controller.								ems
		Network Spectrum Interface 55D850E30AE588853DC7FD05FA58BF52C								
		C Apply Cancel								

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

🍪 Monitoring	Cisco Aironet 1850 Series Mobility Express	Q ▲ ⓒ ≞ ≓ ≝ ¢
Wireless Settings	ACCESS POINTS ADMINISTRATION	
2 Access Points	Access Points 2	
Access Points Groups	AP1850-1(Active Controller) General Controller General Controller General Controller	Global AP Configuration Convert to ME Convert to CAPWAP 0
쌀 WLAN Users	and the second	
📽 Guest WLANs	System Name WI C1850.1	er 12 Primary Controller and Preferred Master 12 Preferred Master
OHCP Server	Refresh	
⁵ Mesh	Sele Mans Type Location	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
Services	C OLD CAPWAP default loc Subnet Mask 255.255.0	0 days, 14 h 13 m 31 s AIR-AP1852I-B-K9
📥 Advanced	Gateway 10.0.0.1	
	Country United States (🔻 😮	
	Changing country code requires controller reset.	
	C Apply & Cancel	

802.11 ネットワークの設定

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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

必須(基本)レートとして 12 Mbps を、サポート対象(任意)レートとして 18 Mbps 以上をそれぞれ設 定することをお勧めします。ただし、環境によっては、6 Mbps を必須(基本)レートとして有効にする 必要があります。
2.4 GHz を使用する場合は、[2.4 GHz 帯域 (2.4 GHz Band)]が[有効 (Enabled)]になっていること を確認します。

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

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

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

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

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

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

8	Monitoring	Advanced RF Parameters	
\$	Wireless Settings		
ġ.	Management	5.0 GHz Band	
عر ا	Services	Automatic Flexible Radio Assignment	
<u>۴</u>	Services	2.4 GHz Optimized Roaming	
~	Advanced	5 GHz Optimized Roaming	
	▼ SNMP	Event Driven RRM	
	Logging	CleanAir detection	
	RF Optimization	5.0 GHz Channel Width	40 MHz •
	I RF Profiles		
	Controller Tools	2.4 GHz Data Bates	Lower Density Higher Density
	Security Settings		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 hates	6 9 12 18 24 36 48 54
			Some legacy devices not supported
		Select DCA Channels	2.4 GHz 🗌 1 2 3 4 5 6 7 8 9 10
			11 5 0 011 36 40 44 48 52 56 60 64 100 104
			108 112 116 120 124 128 132 136 140 144
			<u>149</u> <u>153</u> <u>157</u> <u>161</u> 165
			At least one Channel Number should be selected
		Apply	

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

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 S	eries Mobility Express	Q	A	۲	₽	\geq	٥	
•	Wireless Settings									
ġ.	Management	RF OPTIMIZATION								
J.C.	Services	Il RF Optimization Enable	d							
*	Advanced ✔ SNMP									
	🗟 Logging	RF Optimization	Enabled	•	0					
	IRF Optimization	Client Density	Low Typical	High	0					
	I RF Profiles	Traffic Type	Voice and Data	•	0					
	& Controller Tools									
	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。

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

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

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

🍄 Monitoring	•	cisc	o Cisc	o Aironet 18	350 Series Mobilit	y Express					Q	▲	۲	B	≓	\geq	٥
Wireless Settings	ACC	ESS P	OINTS .	ADMINISTI	RATION												
Access Points	010	Access	s Points	2													
별 Access Points Groups	Q. Sei	arch		-						Global A	P Configuration	Com	vert to ME	0	Convert to	CAPWAP	0
SWLAN Users										-					~		
थ WLAN Users थ Guest WLANs										Primary Controller 🖸	Primary Cont	roller and	Preferre	d Master	Pre	eferred M	Aaster
알 WLAN Users 알 Guest WLANs 양 DHCP Server	Br	rfresh								Primary Controller	Primary Cont	roller and	Preferre	d Master	r 🖸 Pre	aferred M	Master
YUAN Users 양 Guest WLANs 양 DHCP Server 카 Mesh	R	sfresh Sele	Mana	Туре	Location	Na	ame	IP Addre	5	Primary Controller	Primary Cont	roller and	Preferre	d Master	r 🖸 Pre	aferred M	Aaster
Y WLAN Users Y Guest WLANs 양 DHCP Server 가 Mesh 서anagement	Re Ø	sfresh Sele	Mana	Type ME Capable	Location default location	Na	ame P1850-1	IP Addre: 10.0.0.10	8	Primary Controller P AP Mac 38:ed:18:c8:1b:78	Primary Cont Up Time 0 days, 14	h 37 m 44	Preferre	d Master	r 🖸 Pre	aferred M	Master
 WLAN Users Guest WLANs ⊕ DHCP Server f Mesh Management ✓ Services 	Re B B	sfresh Sele	Mana	Type ME Capable CAPWAP	Location default location default location	Na AP AP	ame P1850-1 P1850-2	IP Addres 10.0.0.10 10.0.0.10	8	Primary Controller Primary Controller AP Mac 38:ed:18:c8:28:40	Primary Cont Up Time 0 days, 14 0 days, 14	noller and h 37 m 44 h 37 m 44	Preferre s	d Master AP Moo AIR-AP	del 18521-A-K 18521-B-K	3ferred M (9	Aaster

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

æ	Monitoring	CISCO Alronet 1850 Series Mobility Express	ଦ ▲ ଡ	₿ ≓ ⊻ \$
\$	Wireless Settings ৯ WLANs	ACCESS POINTS ADMINIS General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u		
	थ Access Points 앱 Access Points Groups 營 WLAN Users	Admin Mode Enabled Q. Search Channel Automatic Total	guration Convert to ME	0 Convert to CAPWAP 0
	 In the second se	Refresh Transmit Power Automatic •	ry Controller and Preferred	Master 💮 Preferred Master
ġ.	≁ _{Mesh} Management	Select Mana Type Ø Image: Constant of the second s	Up Time 0 days, 13 h 15 m 06 s	AP Model AIR-AP1852I-A-K9
ير *	Services Advanced	CAPWAP default location AP1850-2 10.0.0.101 38:ed:18:ca:28:40	0 0 days, 13 h 15 m 06 :	AIR-AP1852I-B-K9
B	Monitoring	Cisco Aironet 1850 Series Mobility Express	ଦ 🛦 ⊙	8 ≓ 2 ¢
8 \$	Monitoring Wireless Settings ⋒ WLANs	Cisco Alronet 1850 Series Mobility Express AP1850-1(Active Controller) ACCESS POINTS ADMINIS	ଦ ▲ ଡ	≞ ≓ ⊠ ¢
83 \$	Monitoring Wireless Settings WLANs Access Points Croups	Clsco Aironet 1850 Series Mobility Express AP1850-1(Active Controller) ACCESS POINTS ADMINIS General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u Admin Mode Enabled	Q A @	₽ ≓ 2 \$
8 \$	Monitoring Wireless Settings 차 WLANs 핵 Access Points 핵 Access Points Groups 약 WLAN Users 약 Guest WLANs	Cisco Aironet 1850 Series Mobility Express AP1850-1(Active Controller) ACCESS POINTS ADMINIS General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u Access Points 2 Admin Mode Enabled General Automatic General Automatic Channel Automatic General Controller B02.11a/n/ac	Q A O	 Convert to CAPWAP Convert to CAPWAP Master Preferred Master
89 #	Monitoring Wireless Settings & WLANs ^{III} Access Points Groups III Access Points III Access III Access III Access Points III Access III Access III Access III Access III Access III Access III Access III Access III Access III Access III Access III Access III Acc	Cisco Aronet 1850 Series Mobility Express AP1850-1(Active Controller) ACCESS POINTS ADMINIS General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u Admin Mode Enabled Admin Mode Enabled Gannel Automatic Gannel Midth Dhannel Automatic Gannel Width Dhannel Transmit Power Automatic	Q A O	Convert to CAPWAP @ Master () Preferred Master
89 本 ・ チ	Monitoring Wireless Settings ≫ WLANs [™] Access Points [™] Access Points [™] Access Points Groups [™] WLAN Users [™] Guest WLANs [®] DHCP Server [↑] Mesh Management Services	Channel Width @ Wirz Search Mana Type CAPWAP CAPWAP CAPWAP Captol CAPWAP Captol Captol	Current to ME ry Controller and Preferred Up Time 0 days, 13 h 15 m 06 m 0 days, 13 h 15 m 06 m	Convertis CAPWAP © Convertis CAPWAP © Master Preferred Master AP Model AR-AP18521-A-K9 AIR-AP18521-B-K9



8 20	Monitoring	8	cisc	o Cis	ico Airone	et 1850 Series N	lobility Expre	ess		Q	A	٩		₽		\$
\$	Wireless Settings 아 WLANs	ACC	ESS P	OINTS	AP185	50-2										
	Access Points Access Points Groups		Access	s Point	General	Radio 1 (2.4 GHz)	Radio 2 (5G	Hz) 802.11	u	ration	Con	vert to ME	0	Convert to	CAPWAP	0
	뿔 WLAN Users 營 Guest WLANs					Admin Mode Channe	Enabled Automatic	v	5GHz 802.11a/n/ac	Controll	er and	Preferre	d Master	Pre	ferred Ma	aster
	OHCP Server Mesh	Re	efresh Select	Mana		Channel Width	20 MHz	v		¢	l	Up Time		AP Mod	del	
ġ.	Management	C		P		Transmit Powe	Automatic	•		8:c8:1b	:78 2	2 days, 23	h 44	AIR-AP	1852I-A-H	19
æ	Services	C		(() () ====				⊖ App	oly 8 Cancel	8:ca:28	:40 2	2 days, 23	h 38	AIR-AP	1852I-B-I	(9
*	Advanced															

WLAN の設定

Cisco Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ (たとえば 5 GHz のみ) 適用するよう指定できます。

Cisco Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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

🍘 Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	٩	₽ ≓	٥
Wireless Settings	WLAN/RLAN CONFIGURATION					
🕍 Access Points						
Access Points Groups	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling					
管 WLAN Users						
📽 Guest WLANs	Add n WLAN ID 1		Policy		Padio Policy	
OHCP Server			roncy		5 GHz only	
∱ Mesh	WLAN V					
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 •					
	Radio Policy 5 GHz only V					
	Broadcast SSID					
	Local Profiling 🕖 😧					
	(Apply Can	col				

高速セキュア ローミング用に 802.11r (FT) を使用するには、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			
🍘 Monitoring	General WLAN Security VLAN & Firewall Traffic Sha	ping Advanced 802.11u Hotspot2.0 Sched	uling	
🍄 Wireless Sei	ti			
N WLANS	Guest Network 🕜 ?			
	Captive Network Assistant 🕜 ?			
Groups	MAC Filtering			
📽 WLAN User	Security Type WPA2Enterprise v			
📽 Guest WLA	Authentication Server External Radius 🔻	0		
THCP Serve	Radius Profiling 🕜 🕜			dio Policy 3Hz only
∮ Mesh	BYOD			
📥 Managemer	RADIUS Server			
📌 Services				-
📥 Advanced	Authentication Caching			
	Add RADIUS Authentication Server			
	State	Server IP Address	Port	
	K Enabled	10.0.20	1812	
	Add RADIUS Accounting Server			
	State	Server IP Address	Port	
	Enabled	10.0.0.20	1813	
	Gisco Aironet 1850 Se	ries Mobility Exoress	Q 🗛 🕑	🕒 💳 🛥 🏟
🍘 Monitoring				
🏶 Wireless Set	tings			
MUANs	Add new WLAN/RLAN			
Access Poin	S General WLAN Security VLAN & Firewall Traffic Sha	iping Advanced 802.11u Hotspot2.0 Schedi	uling	
Access Poin Groups	s			
📽 WLAN User:	Guest Network			
📽 Guest WLAN	S Captive Network Assistant			odio Dollov
OHCP Serve	MAC Filtering			GHz only
7 Mesh	Security Type Personal v			
📩 Managemen	WPA2 WPA3			
🖋 Services	AutoConfig iPSK 🕜 💡			
+	Passphrase Format ASCII v			

WLAN 設定の [詳細 (Advanced)] タブで、[802.11r] を [有効 (Enabled)] に設定します。

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

Apply
 Sancel

802.11k および 802.11v を有効にすることを推奨します。

Passphrase *

Show Passphrase

A 		Add new WLAN/RLAN			×q	A	٩		= _	¢
Monitoring		General WLAN Security VLAN & Firewal	I Traffic Shaping Advanced	802.11u Hotspot2.0						
₩ireless Settings WLANs	WLAN/RLA	Scheduling								
Maccess Points	ふ Active	Allow AAA Override								
별 Access Points Groups		Maximum Allowed Clients	Unlimited(Default) v							
📽 WLAN Users		Maximum Allowed Clients Per AP Radio	200 🕄							
📽 Guest WLANs	Add new WL	802.11k	Disabled •		curity	Policy		Radio Po	llev	
DHCP Server	⊠ ×	802.11r	Enabled v		Journy	roncy		5 GHz on	lv	
4 Mesh		802.11v	Disabled •							
🏟 Management		сскм								
🗲 Services		Client Band Select								
📥 Advanced		Client Load Balancing								
		Umbrella Profile	None •							
		Umbrella Mode	Ignore v							

高速セキュアローミングに CCKM を使用するには、**[セキュリティタイプ (Security Type)**]を **[WPA2Enterprise]**に設定します。

		Add	new WLAN/RLAN								×	₽	\$
æ	Monitoring	Genera	WLAN Security	VLAN & Firewall	Traffic Shapin	g Advanced	802.11u	Hotspot2.0	Scheduli	ing			
\$	Wireless Setti												
	MLANs		Guest Network										
	access Points	Cap	ive Network Assistant										
	Access Points Groups		MAC Filtering										
	· 曾 WLAN Users		Security Type	WPA2Enterprise	Ð v								
	📽 Guest WLANs		Authentication Server	External Radius	s 🔻 🕄								
	OHCP Server		Radius Profiling	0								Hz only	
	∮ Mesh		BYOD								Í	in only	
ġ.	Management	RAD	US Server										
J.C.	Services												
Ł	Advanced		Authentication Cachi	ing									
			Add RADIUS Authentication	n Server									
			State			Server IP Addre	155			Port			
		ж	Enabled			10.0.0.20				1812			
			Add RADIUS Accounting Se	erver									
_			State			Server IP Addre	185			Port			
		×	Enabled			10.0.0.20				1813			

WLAN 設定の [詳細 (Advanced)] タブで、[CCKM] を [有効 (Enabled)] に設定します。

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

802.11k および 802.11v を有効にすることを推奨します。

6		e alta	Add new WLAN/RLAN		×	Q	A	٩		≓	\$
	Monitoring		General WLAN Security VLAN & Firewal	Traffic Shaping Advanced 802.11u Hotspo	ot2.0						
\$	Wireless Settings ຈັ wLANs	WLAN/RLA	Scheduling								
	🖆 Access Points	ふ Active	Allow AAA Override								
	≌ Access Points Groups		Maximum Allowed Clients	Unlimited(Default)							
	📽 WLAN Users		Maximum Allowed Clients Per AP Radio	200 (3)							
	📽 Guest WLANs	Add new WL	802.11k	Disabled v							
	OHCP Server	8 ×	802.11r	Disabled v	3	curity P	olicy		5 GHz	only	
	4 Mesh		802.11v	Disabled v							
ġ.	Management		сскм								
æ	Services		Client Band Select								
*	Advanced		Client Load Balancing								
			Umbrella Profile	None v							
			Umbrella Mode	Ignore v							

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) ≓	•
æ	Monitoring	Genera	WI AN Security	VI AN & Firewall	Traffic Shaping	n Advanced	802 110	Hotspot2.0	Schedul	ling		
\$	Wireless Setti	Gonore	- How obtainly		france on april	g naturota		Therefore	Contract			
			Guest Network									
	Access Points	Can	ive Network Accietant									
	Access Points Groups	Cap	MAC Filtering									
	📽 WLAN Users		Security Type	WPA2Enterpris	0 v							
	📽 Guest WLANs		Authentication Server	r External Radius	s 🔻 😧							
	OHCP Server		Radius Profiling	a 🚺 🔞							dio Policy	
	∮ Mesh		BYOD								anz only	
÷.	Management	RADI	US Server									
J.C.	Services											
÷	Advanced		Authentication Cachi	ing								
	Auvanceu		Add RADIUS Authentication	n Server								
			State			Server IP Addre	855			Port		
		ж	Enabled			10.0.0.20				1812		
		/	Add RADIUS Accounting Se	erver								
			State			Server IP Addre	985			Port		
		×	Enabled			10.0.0.20				1813		

•		cisco	Cisco Aironet 1850 Ser		Q	▲	۲	B	≓	\geq	٥			
626	Monitoring													
٥	Wireless Settings	ADMIN ACCOL	INTS											
÷.	Management	Sers 2	1											
	😤 Admin Accounts													
	O Time	Management	User Priority Order	Local Admin Acco	unts TACACS+	RADIUS Auth C	ached Users							
	✤ Software Update	-												
æ	Services	Authentication	n Call Station ID Type	AP MAC Address:	SSID +									
*	Advanced	Authenti	cation MAC Delimiter	Hyphen	•									
		Accounting	g Call Station ID Type	IP Address	•									
		Acco	unting MAC Delimiter	Hyphen	•									
			Fallback Mode	Passive	•									
			Username	cisco-probe										
			Interval	300	e Seco	nds								
		A	P Events Accounting											
				Арріу										
				0										
	Monitoring	Add HAD	US Authentication Server											
•	Wireless Settings	Action	Server Index	Network User	Management	State	Server IP Address	Share	d Key		Port			-
ġ.	Management	6 X	1				10.0.020				1812			
	Access													
	🐸 Admin Accounts													
	O Time													
	✤ Software Update	Add RAD	IUS Accounting Server											
Je.	Services	Action	Server Index	Network User	Management	State	Server IP Address	Share	d Key		Port			
Ł	Advanced	© ×	1				10.0.0.20		***		1813			

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

🙆 Monitoring	Gisco Aironet 1850 Series Mobility Express	Q ×	A	٩		1	•
Wireless Settings	Add new WLAN/RLAN WLAN General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling						
교 Access Points 웹 Access Points Groups	Client IP Management Network(Default)						
ঔ WLAN Users ঔ Guest WLANs	Addr Native VLAN ID 1 Use VLAN Tagging Yes		Policy		Radio Po	licy	
↔ DHCP Server	C * * DHCP Scope Store VLAN ID * 3 • No DHCP Scope associated with VLAN ID				5 GHz onl	у	
Services	Enable Firewall No +						
🛥 Advanced	Add New VLAN						
	VLAN Name VLAN Id						
	Contra 2 Contra 2 Voice 3						
	и и 1 1 н н 10 т Items per page 1 - 2 of 2 Item	15					
	VLAN and Firenall configuration apply to all VLANs and RLANs configured with same VLAN	el					

[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				>	⇒ ⊠	¢
€9 \$2	Monitorii Wireless	General WLAN Security VLAN & Firewall	raffic Shaping Advanced	802.11u Hotspot2.0 Scheduling				
	₩LANs [®] Access F	QoS	Platinum (Voice) v	0				
	Access F	Average real-time band	width limit should be atleast Ave	rage bandwidth limit				
		Rate limits per clien	t					
	Cupet M	Average downstream bandwidth limit	0	kbps 😮				
		Average real-time downstream bandwidth limit	0	kbps 😮			cy	
	4 Mash	Average upstream bandwidth limit	0	kbps 😮			, ,	
<u>+</u>	/ Westi	Average real-time upstream bandwidth limit	0	kbps 🕜				
- 11 	Manager							
<i>.</i>	Services	Rate limits per BSSI	0	kbps 👩				
*	Advance		0	kbps				
		Average real-time downstream bandwidth limit	0	kbps				
		Average upstream bandwidth limit	0	kbps				
		Average real-time upstream bandwidth limit		June 🕜				
B	Monitorii	Fastlane	Disabled •					
•	Wireless		Enabling Fastlane will update G	oS value to platinum.				
	₩LANs	Application Visibility Control	Enabled •					
	🖆 Access F	AVC Profile	voice					
	🖆 Access F							
	Groups	Add Rule						
	양 WLAN U	S Application	Action		Average Rate	Burst Rate		
	📽 Guest W							
	INCP S							
	7 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。

		Add new	WLAN/HLAN			×		
æ			Active	Add new WLAN/RLAN			Security Policy	Radio Policy
	Monitoring	8 ×	Enabled	General WLAN Security VLAN & Firewal	II Traffic Shaping Advanced 802.11u Hotsp	ot2.0		5 GHz only
\$	Wireless Settings _{WLANs}			Scheduling				
	🖆 Access Points							
	Access Points Groups			Allow AAA Override Maximum Allowed Clients	Unlimited(Default) v			
	📽 WLAN Users			Maximum Allowed Clients Per AP Radio	200 🔋			
	쓸 Guest WLANs			802.11k	Disabled •			
				802.11r	Enabled			
	⁵ Mesh			202.11	Disabled			
÷.	Management			002.11V				
J.C.	Services			Cliant Band Select				
÷	Advanced			Client Load Balancing				
-	Advanced			Client Load Balancing				
				Umbrella Profile	None •			
				Umbrella Mode	Ignore •			
				Umbrella DHCP Override				
				mDNS				
				mDNS Profile	None v			
				Passive Client	0			
				Please enable Globa when Global Multica	al Multicast in Services->Media Stream. Passive Client will n sst is disabled.	not work		
				Multicast IP	239.1.1.1 😯			
				Multicast Direct	0			

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。

8 30	Monitoring	Cisco Aironet 1850 Series Mobility Express		Q	A	٩	Ð	#	\$
\$	Wireless Settings ৯ _{WLANs}	ACCESS POINT GROUP							
	🕍 Access Points	Access Points Groups							
		Add new group							
	쓸 WLAN Users	Q Search General WLANs Access Points RF Profile Ports Intelligent Capture							
	🖆 Guest WLANs	Add new group Refree							
	OHCP Server	AP Group name express-1	AP count						
	∱ Mesh	AP Group description							
ň.	Management	LE default-grou NAS-ID							
"C	Services	Venue Group UNSPECIFIED +							
Ł	Advanced	Venue Type UNSPECIFIED *							
		Add New Venue 🛛							
		Language Venue Name							
									ems
		Apply Sancel							

[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	Cisco Aironet 1850 Series Mobility Express	Q	A	٩	#	0
•	Wireless Settings ৯ _{WLANs}	ACCESS POINT GROUP					
	📲 Access Points	Access Points Groups					
		Add new group					
	쓸 WLAN Users	Q Search General WLANs Access Points RF Profile Ports Intelligent Capture					
	📽 Guest WLANs	Add new group Refresh					
	OHCP Server	AP Group name	AP count				
	4 Mesh	Add new WLAN/RLAN	0				
ň.	Management	US default-group X W Type WLAN V	2				
se.	Services	Profile Name voice •					
*	Advanced	Cancel					

🍘 Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	٩	Ð	Ħ	\$
Wireless Settings	ACCESS POINT GROUP						
별 Access Points 별 Access Points Groups	Access Points Groups Add new group						
營 WLAN Users 營 Guest WLANs	Q. Sketch General WLANs Access Points RF Profile Ports Intelligent Capture Add new group Refresh Add new Yil AM/01 AM Access Vil AM/01 AM						
♥ DHCP Server [#] Mesh	Type Profile Name Status 0 Cf default-group WLAN voice Enabled 2						
Services							
	H 1 1 + H 10 + 1 1 + H 10 + Items per page 1 - 1 of 1 Items						ims
	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。

B	Monitoring		Cisco Air	ironet 1850 Se	eries Mobility Express						Q	A	٩	6	#		٥
\$	Wireless Settings 차 WLANs 앱 Access Points	ACCESS P	Add new g	group /LANs Access	Pointa BF Profile Porta	Intelligent	Capture			×							
	발 Access Points Groups 참 WLAN Users 참 Guest WLANs	Q. Search Add new grou	Q Search				Cuptoro			Refresh							
	[⊗] DHCP Server [∲] Mesh	8 ×	APs in "ex	xpress-1" group	MAC Address			0	AP Group	All v							
іін "С	Management Services		AP1 AP1	1850-1 1850-2	38:ed:18:c8:1b:78 38:ed:18:ca:28:40												
*	Advanced	H - 1 1				2	2 2									2 of 2 ite	ems
			4 1	1	1 - 2 of 2 items			4	0 0 + H	No items to display							

[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。

🙆 Monitoring	Cisco Aironet 1850 Series Mobility Express	۹	A	٩	Ð	₽	\$
♥ Wireless Settings	ACCESS POINT GROUP						
Access Points	Access Points Groups						
Access Points Groups							
睿 WLAN Users	Q Search						
管 Guest WLANs	Add new group Refresh						
OHCP Server	AP Group name AP count						
∲ Mesh	Image: Weight and the second secon						
ሱ Management	Lef default-group General WLANs Access Points RF Profile Ports Intelligent Capture						
Services							
📥 Advanced	2.4GHz None • 5GHz None • C 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 Wireless Phone 840 および 860 で使用する SSID は 5 GHz 無線にのみ適用することを推奨します。 作成した RF プロファイルは、AP グループに適用されます。

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

[無線ポリシー (Radio Policy)]に [5GHz] または [2.4GHz] を選択します。

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

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

æ	Monitoring		Cisco Aironet 1850 Serie	s Mobility Express			(۵ 🛦	٩	Ð	₽	\$
\$	Wireless Settings											
÷.	Management	RF Profile	es									
an C	Services	RF pro	file 6									
*	Advanced ✔ SNMP	Q Search										
	🗟 Logging	⊕ Add n	ew RF Profile	Add RF Profile								
			RF profile	General 802.11 RRM Cli	ent Distribution		Applied					
		8 ×	express-1									
	✗ Controller Tools	C	High-Client-Density-802.11a	RF profile name	express-1	1	40					
	Ö Security Settings	ß	High-Client-Density-802.11bg	RF profile description		1	40					
		ß	Low-Client-Density-802.11bg	Band			40					
	CMX	C C C C C C C C C C C C C C C C C C C	Typical-Client-Density-802.11a	Banu	5GHZ ¥	, in the second s	40					
		ß	Typical-Client-Density-802.11bg	Maximum clients per radio	200	P	No					
				Rx SOP Threshold	Auto 🔻							
				Multicast datarates	Auto 🔻							
		н 4 1	1 ► ► 10 ▼ items per page		⊘ Apply S Cancel							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。

🍘 Monitoring	Cisco Aironet 1850 Series Mobility Express	A		#	•
Wireless SettingsManagement	RF Profiles				
🖋 Services	RF profile 6				
Advanced	Q Search				
🗟 Logging	Add new RF Profile				
I RF Optimization	×				
all RF Profiles	C x Add HF Profile				
✗ Controller Tools	General 802.11 RRM Client Distribution				
🍄 Security Settings	2				
🖾 смх	Data rates Data sates 6 9 12 18 24 35 48 54				
	MCS settings				
	 ● Apply ● Cancel 				

[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。

8 20	Monitoring	e di	Cisco Aironet	1850 Series Mobility E	press					Q	A	٩	Ð	t	¢
\$	Wireless Settings														
÷.	Management	RF Profile	9S												
se.	Services	RF pro	file 6												
*	Advanced ✔ SNMP	Q Search													
	🗟 Logging	⊕ Add n	ew RF Profile	Add RF Profile											
	I RF Optimization		RF profile						Арр	lied					
		G 🗙	express-1	General 802.11 RRM	Client Distr	ibution									
	& Controller Tools	ß	High-Client-Density-802						No						
		ß	High-Client-Density-802	Channel Wi	ith 40 MHz	•			No						
	Security Settings	8	Low-Client-Density-802	Select DCA Channels	Select All 🗆	36 40 4	14 48 52 56 60	64 100 104 108	No						
	CMX		Low-Client-Density-802			112 116 1	120 124 128 132 136	140 144 149 153	No						
		8	Typical-Client-Density-8						No						
		8	Typical-Client-Density-f		Some of the enabled. The At least one	channels are sse channels Channel Num	not allowed to configure can be enabled in RF Opt ber should be selected O Apply	as they are not imization screen.	No						
		H 4 1	1 ► H 10 ▼ it												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。

e Pa	Monitoring		co Cisco Aironet 1850 Se	ries Mobility	Express		Q	▲	٢	B	₽	\geq	٥
\$	Wireless Settings	Media Str	eam Settings										
ام عر	Management	Medi	a Stream Disabled										
ľ	Media Stream												
	[♥] TLS		Global Multicast										
	♥ mDNS		Multicast Direct										
	line Assurance		Mariodot Diroot										
	🌥 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									
		Ses	sion Announcement Note	Note	lin								
				Apply									
		Add New S	Stream										
		Action	Stream Name		Start IP Address	End IP Address	0	Operation	Status				
		×	10.0.0.40		239.1.1.40	239.1.1.40	N	fulticast-d	irect				

[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 new	WLAWHLAN			×		
æ			Active	Add new WLAN/RLAN			Security Policy	Radio Policy
92.00	Monitoring	ĭ × 8	Enabled	General WLAN Security VLAN & Firewal	I Traffic Shaping Advanced 802	2.11u Hotspot2.0		5 GHz only
\$	Wireless Settings ⋒ _{WLANs}			Scheduling				
	🔮 Access Points							
	Access Points Groups			Allow AAA Override Maximum Allowed Clients	Unlimited(Default)			
	📽 WLAN Users			Maximum Allowed Clients Per AP Radio	200 🔅			
	뿔 Guest WLANs			802.11k	Disabled •			
				802.11r	Enabled v			
	∜ Mesh			802.11v	Disabled •			
÷.	Management			сски				
J.C.	Services			Client Band Select				
*	Advanced			Client Load Balancing				
				Umbrella Profile	None			
				Umbrollo Mode				
				Under Street a wode	Ignore v			
				Umbrella DHCP Override				
				mDNS				
				mDNS Profile	None v			
				Passive Client	0			
				Please enable Globa when Global Multica	I Multicast in Services->Media Stream. Pass st is disabled.	sive 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)]または [CCKM] が [有効 (Enabled)]になっていることを確認します。
- 802.11k を [有効 (Enabled)] に設定することを推奨
- 802.11v を有効に設定することを推奨
- 必要に応じて [データレート (Data Rates)]を設定します
- **[DTPC]** を有効にします。
- [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 Wireless Phone 840 および 860 は、5 GHz 帯域での動作を推奨します。5 GHz 帯域では多数のチャネ ルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。 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	<u>H</u> OME <u>N</u> ETWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	Sa <u>v</u> e C <u>M</u> ANAGEMENT	onfiguration	Ping Logout	<u>R</u> efresl
NETWORK	Hostname ap-1					ap-1 i	uptime is 1 day	, 4 hours, 51 minu	utes
NETWORK MAP Summary	Network Interface	s: 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			18e7.281b.3f54					
Radio1-802.11AC 5GHz	Interface Status	Gi	gabitEthernet		Radio0-802.1	1N ^{2.4GHz}	Radio1-802.1	1AC ^{5GHz}	
	Software Status			Enabled 1		Disabled	ŀ	Enabled	1 1
	Hardware Status			Up î		Down	ŀ	Up	^
	Interface Resets			5		(8

11r over Air を有効にして高速セキュア ローミングを有効にすることを推奨します。

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

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

Cisco Autonomous アクセス ポイントの場合、動的周波数選択(DFS)を選択して、自動チャネル選択を使用します。

DFS が有効にされている場合、少なくとも1つの帯域(帯域1~4)を有効にします。

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

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

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

この設定は、エリア内に断続的な干渉が存在する場合に必要です。

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

すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

[クライアント電力(Client Power)] が正しく設定されていることを確認します。Cisco Autonomous アクセ ス ポイントでは、クライアント電力のデフォルト設定である**[最大(Max)]**を使用しないでください。デフォ ルトを使用すると、DTPC がクライアントにアドバタイズされません。

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

[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。



	a9.3-2Mb/sec	Require		Enable	Disable
MCS Rates: 0 1	2 3 4 5	6 7 8 9 1	0 11 12 13 1	4 15 16 17 1	18 19 20 21 22 23
Enable O					
Disable 💿 🗌	0000				
Transmitter Power (dBm)):	015 012 09 0	6 🔾 3 💿 Max		Power Translation Tal (mW/dBm)
Client Power (dBm):		●Local ○15 ○12	9 06 03 0	Max	
DefaultRadio Channel:		Channel 36 - 5180 MH	lz ᅌ	Channel 36 5180	MHz
Dynamic Frequency Sele	ection Bands:	Band 1 - 5.150 to 5.250 Band 2 - 5.250 to 5.350) GHz		
		Band 2 - 5.250 to 5.35 Band 3 - 5.470 to 5.72 Band 4 - 5.725 to 5.82	5 GHz		
Channel Width:		Below 40 MHz 22	0 MHz		
World Mode		 Disable 		C Legacy	Dot11d
Multi-Domain Operation:			0.11	U	• • • • • • • • • • • • • • • • • • • •
Country Code:			Outdoor		
Radio Preamble		Short			
Antenna:		a-antenna	ab-antenna (abc-antenna	abcd-antenna
Internal Antenna Configu	uration:	Enable		 Disable 	
Jeres and the second second		Antenna Gain(dBi):	0 (-	128 - 128)	
				,	
Gratuitous Probe Respo	nse(GPR):	C Enable		 Disable 	
		Period(Kusec): DIS	SABLED (10-25	55)	
		Transmission Spee	d: none		
Traffic Stream Metrics:		Enable		 Disable 	
Aironet Extensions:		 Enable 		O Disable	
Ethernet Encapsulation	Transform:	RFC1042		O 802.1H	
Reliable Multicast to WG	iB:	 Disable 		Enable	
Public Secure Packet For	rwarding:	PSPF must be set per	VLAN. See VLAN p	age	
Beacon Privacy Guest-M	lode:	Enable		 Disable 	
Passan Paris di	100	(20,4000 (/	Date Date		0 (1 400)
Beacon Period:	100	(20-4000 NUSEC)		rtate (DTIM):	2 (1-100)
wax. Data ketries:	64	(1-128)	RIS Max. Re	etries:	o4 (1-128)
Fragmentation Threshole	d: 2346	(256-2346)	RTS Thresh	old:	2347 (0-2347)
Poot Porent Time out		0	(0 GEEDE		
Root Parent HAC 4 (onal):	U	(0-00000 Sec	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
ROOL Parent MAC 1 (Optio	onal):			1.0000	
Poot Parent MAC 0 /	onal):				
Root Parent MAC 2 (option					
Root Parent MAC 2 (option Root Parent MAC 3 (option	onal):		(нннн.ннн		

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 Wireless Phone 840 および 860 には個別の SSID を割り当てることを推奨します。

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 Wireless Phone 840 および 860 で使用される SSID の設定では、特定の 802.11 無線機タイプにのみ (たとえば 802.11a のみ) 適用するよう指定できます。

[WPA2] キー管理を有効にします。

[11r] または [CCKM] が有効になっていることを確認します。11r を推奨します。

			Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efr
cisco	HOME NETWORK ASSOCIATION	W <u>I</u> RELESS <u>S</u> ECURITY <u>S</u> ERVICES	<u>M</u> ANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG
Security			
Admin Accord	Hostname ap-1		ap-1 uptime is 1 day, 4 hours, 33 minutes
Encryption Manager	Security: Global SSID Manager		
SSID Manager	SSID Properties		
Dot11u Manager	Current SSID Liet		
Server Manager		2017	
AP Authentication	data	SSID:	voice
Intrusion Detection	voice	VLAN:	3 Oefine VLANs
Local RADIUS Server			Backup 1:
Advance Security			Backup 3:
		Band-Select:	Band Select
		Universal Admin Mode:	Universal Admin Mode
		Interface:	Radio0-802 11N2.4GHz
		interface.	Radio1-802.11AC ^{5GHz}
	Network ID: (0-4096	3)	
	 Open Authentication: Web Authentication Shared Authentication: Vetwork EAP: 	with EAP Web Pass < NO ADDITION> < NO ADDITION >	0
	Server Priorities:		
	EAP Authentication Serve	rs	MAC Authentication Servers
	 Use Defaults Define Define Define 	efaults	O Use Defaults Define Defaults
	Customize		Customize
	Priority 1: < NONE >	0	Priority 1: <pre>< NONE > </pre>
	Priority 2: < NONE >	•	Priority 2: < NONE > 🗘
	Priority 3: < NONE >		
	Findity 0. CONVES		
	Client Authenticated Key Managemer	nt	
	Key Management:	Mandatory O	CCKM Z Enable WPA WPAv2 dot11r

11w Configuration:	(Disable ᅌ	
11w Association-comeback:		1000	(1000-20000)
11w Saquery-retry:		100	(100-500)
IDS Client MFP			
Enable Client MFP of the second se	on this SSID	Coptional	3
AP Authentication			
Credentials:		< NONE >	Define Credentials
Authentication Methods P	rofile:	< NONE >	Define Authentication Methods Profiles
Accounting Settings			
Enable Accounting			Accounting Server Priorities:
			O Use Defaults Define Defaults
			◯ Customize
			Priority 1: < NONE > ᅌ
			Priority 2: < NONE > 😒
			Priority 2: < NONE >
			Priority 2: < NONE > C Priority 3: < NONE > C
Rate Limit Parameters			Priority 2: < NONE > C Priority 3: < NONE > C
Rate Limit Parameters Limit TCP:			Priority 2: < NONE > C Priority 3: < NONE > C
Rate Limit Parameters Limit TCP:	Rate:	Burst-Siz	Priority 2: < NONE > C Priority 3: < NONE > C e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output:	Rate:	Burst-Siz Burst-Siz	Priority 2: < NONE > 0 Priority 3: < NONE > 0 e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP:	Rate: Rate:	Burst-Siz Burst-Siz	Priority 2: < NONE > C Priority 3: < NONE > C e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input:	Rate: Rate: Rate:	Burst-Siz Burst-Siz Burst-Siz	Priority 2: < NONE > 3 Priority 3: < NONE > 3 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-Siz Burst-Siz Burst-Siz Burst-Siz	Priority 2: < NONE > 3 Priority 3: < NONE > 3 e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings	Rate: Rate: Rate: Rate:	Burst-Siz Burst-Siz Burst-Siz Burst-Siz	Priority 2: < NONE > C Priority 3: < NONE > C e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extended 0	Rate: Rate: Rate: Rate: Capabilites	Burst-Siz Burst-Siz Burst-Siz Burst-Siz	Priority 2: < NONE > C Priority 3: < NONE > C e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extended C	Rate: Rate: Rate: Rate: Capabilites of Ivertise Win	Burst-Siz Burst-Siz Burst-Siz Burst-Siz	Priority 2: < NONE > 3 Priority 3: < NONE > 3 e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extended C	Rate: Rate: Rate: Rate: Capabilites of Ivertise Win Ivertise this	Burst-Siz Burst-Siz Burst-Siz Burst-Siz Dof this SSID eless Provisio SSID as a Se	Priority 2: < NONE > 3 Priority 3: < NONE > 3 e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Extended O Ac	Rate: Rate: Rate: Rate: Capabilites of dvertise Win dvertise this	Burst-Siz Burst-Siz Burst-Siz Burst-Siz of this SSID eless Provisio SSID as a Se	Priority 2: < NONE > C Priority 3: < NONE > C e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Output: Output: General Settings Advertise Extended O Ac Ac Ac C	Rate: Rate: Rate: Capabilites of dvertise Win dvertise this	Burst-Siz Burst-Siz Burst-Siz Burst-Siz Dof this SSID eless Provisio SSID as a Se ID	Priority 2: < NONE > 3 Priority 3: < NONE > 3 e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000) e: (0-500000)

Association Limit	(optional): (1-255)	
EAP Client (optio	nal):	
	Usemame: rassworu.	
Multiple BSSID Beacon	Settings	
Multiple BSSID B	eacon	
	□ Set SSID as Guest Mode	
	Set DataBeacon Rate (DTIM): DISABLED (1-100)	
		Apply Cance
Guest Mode/Infrastruct	ure SSID Settings	
Guest Mode/Infrastruct	ure SSID Settings	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} :	ure SSID Settings	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} : Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: < NONE > 0	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID	Single BSSID Set Single Guest Mode SSID: < NONE > OMUltiple BSSID CONNE > OMULtiple BSSID CO	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID	Single BSSID Set Single Guest Mode SSID: NONE > Set Single Guest Mode SSID: NONE > Set Single Guest Mode SSID: Set Single Gues	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID Radio1-802.11AC ^{5GHz} :	Single BSSID Set Single Guest Mode SSID: NONE > Solution Nultiple BSSID CONE > Solution Force Infrastructure Devices to associate only to this SSID	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID Radio1-802.11AC ^{5GHz} : Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: < NONE > Multiple BSSID <	
Guest Mode/Infrastruct Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID Radio1-802.11AC ^{5GHz} : Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: < NONE > Multiple BSSID <	
Guest Mode/Infrastructi Radio0-802.11N ^{2.4GHz} : Set Beacon Mode: Set Infrastructure SSID Radio1-802.11AC ^{SGHz} : Set Beacon Mode: Set Infrastructure SSID	Single BSSID Set Single Guest Mode SSID: < NONE > C Multiple BSSID <	
Guest Mode/Infrastruct 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 > Multiple BSSID . . Single BSSID . . Multiple BSSID . . Mu	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。

սիսիս						Sa <u>v</u> e (Ping Logout Refres
CISCO	HOME NETWORK	ASSOCIATION	W <u>I</u> RELESS	SECURITY	SERVICES	MANAGEMENT	<u>S</u> OFTWARE	<u>E</u> VENT LOG
Services	Hostname ap-1					a	p-1 uptime is 1 o	day, 4 hours, 48 minutes
Telnet/SSH								
Hot standby	Services: VLAN							
CDP	Global VLAN Pro	operties						
DNS								
Filters	Current Native	VLAN: VLAN 10						
НТТР	Assigned VLAN	s						
QOS	Current VI AN I	ist	Create			Define SSID	s	
Stream			orouto				-	
SNMP	VLAN 2	_						
SNTP	VLAN 3 VLAN 10		VLA	AN ID:		3	(1-409	4)
VLAN			VLA	AN Name (op	tional):			
ARP Caching		Delete		Native VL	AN			
Band Select				Enable P	ublic Secure P	Packet Forwarding		
Auto Config							5	
				Radiou-80	J2.11N ^{2.40H2}			
				Radio1-80	02.11AC ^{5GHz}			
				Managem	ent VLAN (If r	non-native)		
							C	Apply Cancel
	VLAN Informatio	on						
	View Information	n for: VLAN 2 ᅌ						
		GigabitEtherne	et Packets	Radio	-802.11N ^{2.4GHz}	Packets	Radio1-802.1	1AC ^{5GHz} Packets
	Received		65884					65884
	Transmitted		5462					5462
								Refresh

暗号化タイプとして **[AES]** が選択されていることを確認します。

ululu cisco	HOME NETWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	Sa <u>v</u> e (MANAGEMENT	Configuration	Ping Logout <u>R</u> efree EVENT LOG		
Security	Hostname ap-1					ap-1	uptime is 1 day	, 4 hours, 32 minutes		
Admin Access Encryption Manager	Security: Encryp	tion Manager								
SSID Manager	Set Encryption Mode and Keys for VLAN:							Define VLANs		
Dot11u Manager	Encryption Mode	Encryption Modes								
AP Authentication	○ None	○ None								
Local RADIUS Server	O WEP Encryp	optional	0							
in and second	 Cipher 	Cisco Comp AES CCMP	oliant TKIP Fea	tures: DEn	able Message able Per Pack	Integrity Check (M et Keying (PPK)	IC)			
	Encryption Keys									
			Transmit Ke	у	Encryptio	n Key (Hexadecim	al)	Key Size		
	Enc	ryption Key 1:	\bigcirc					128 bit ᅌ		
	Enc	ryption Key 2:	0					128 bit ᅌ		
	Enc	ryption Key 3:	\bigcirc					128 bit ᅌ		
	Enc	ryption Key 4:	0					128 bit ᅌ		
	Global Properties									
	Broadcast Key I	Rotation Interval:		usable Rotatio	on n with Interiol		1000000 ccc)			
			Û		a with milefval	(10-	1000000 SEC)			
	WPA Group Key	Update:		nable Group	Key Update O	n Membership Tern	nination			
				nable Group	Key Update O	n Member's Capab	ility Change			
								Apply Cancel		
								Cancel		

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。

SERVER MANAGER OLGBAL PROPERTIES Admin Access Security: SERVER MANAGER ap1 uptime is 1 day, 4 hours, 42 min. SECURITION Manager Security: Server Manager Backup RADIUS Server Distitu Manager Backup RADIUS Server IP Version: IP Version: Turvsion Detection Local RADIUS Server Backup RADIUS Server Apply Oeides Advance Security IP Version: IP Version: IP Version: Apply Oeides Cancel Corporate Server IP Version: IP Version: IP Version: IP Version: IP Version: Apply Oeides Cancel INVERSION Server IP Version: IP Version: </th <th>uluili. cisco</th> <th><u>H</u>ome <u>N</u>etwork <u>A</u>ssoci<i>i</i></th> <th>ATION W<u>I</u>RELESS <u>S</u>ECURITY</th> <th>Sa <u>S</u>ERVICES <u>M</u>ANAGEME</th> <th>a<u>v</u>e Configuration <u>P</u>ing Logout <u>R</u>efrest NT <u>S</u>OFTWARE <u>E</u>VENT LOG</th>	uluili. cisco	<u>H</u> ome <u>N</u> etwork <u>A</u> ssoci <i>i</i>	ATION W <u>I</u> RELESS <u>S</u> ECURITY	Sa <u>S</u> ERVICES <u>M</u> ANAGEME	a <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efrest NT <u>S</u> OFTWARE <u>E</u> VENT LOG
Admin Access Fostame sp-1 sp-1 general sp-1 sp-1 general sp-1 Security: Server Manager Security: Server Manager Security: Server Manager Backup RADIUS Server DPV4 PV6 Backup RADIUS Server Name: Backup RADIUS Server Itrusion Detection Local RADSUS Server Advance Security IP Version: PPV4 PV6 Server Manager Backup RADIUS Server Apply Device Cancel Corporate Servers Current Server List Server: 100.020 Advance Security IP Version: 100.020 (Hostname or IP Address) Shared Secret: 100.020 (Hostname or IP Address) Priority 1 0.020 Priority 2 (Pointy 2) Priority 2 0.000 S Priority 1 100.020 Priority 2 Priority 1 100.020 Priority 2 Priority 2 Priority 2 Priority 2 0.000 S Prio	Security				
Encryption Manager SSID Manager Backup RADIUS Server Backup RADIUS Server Defit Manager P Version: Lantrusion Detection Backup RADIUS Server Advance Security Corporate Server Current Server List RADIUS © PV4 (PV6 Server Name: 10.0.0.0 Proving P Version: Proving P Version: Proving Proving P Version: Proving Proving P Version: Proving P Version: Proving P Version: Proving P Version:	Admin Access	Hostname ap-1			ap-1 uptime is 1 day, 4 hours, 42 minutes
SSID Manager DotLiu Manager Bortiu Manager AP Authentication Backup RADIUS Server Name: Intrusion Detection Local RADIUS Server Data RADIUS Server Corporate Server Current Server List RADIUS @ IN Addition @ Server Name: IN 0.0.0 Server: IN 0.0.0.0 Server: IN 0.0.0.0 Server: IN 0.0.0.0 Pere Authentication Port (optional): IN 2 IN 4.0445535) Accounting Priority 1: IN 0.00.0 Priority 2: Nonte 5 Prio	Encryption Manager	Security: Server Manager			
Doflut Manager Berver Manager RP Authentication Intrusion Detection Local RADIUS Server Backup RADIUS Server Backup RADIUS Server Backup RADIUS Server Backup RADIUS Server Corporate Servers Current Server List Intrusion Intrusion Server Name: Intrusion Server: Intrusion Server: Intrusion Reter Authentication Port (optional): Bits: Intrusion Priority 1: Intrusion Mack Authentication Mack Authentication Priority 1: Intrusion Reter Priority 1: Intrusion Reter Priority 1: Intrusion Reter Priorit	SSID Manager	Backup RADIUS Server			
Backup RADUS Server Name: Backup RADUS Server: Ndvance Security Apply Delete Corporate Servers Corporate Servers Corporate Servers Corporate Servers Delete Corporate Servers Server: 10.0.20 Shared Secret: 00.0.20 (Hostname or IP Address) Server: 10.0.20 Server: 10.0.20 Shared Secret: 00.0.20 (Hostname or IP Address) Server: 10.0.20 Server: 10.0.20 Shared Secret: Corporate Server Priorities EAP Authentication Priority 1: 10.0.20 Priority 1: 10.0.20 Priority 2: NONE> 5 Priority 2: NONE> 5 Priority 2: NONE> 5 Priority 3: NONE> 5 <	Oot11u Manager	IP Version:	●IPV4 ○IPV6		
Intrusion Detection Local RADIUS Server Advance Security Advance Security Advance Security Corporate Server Current Server List RADIUS Provent Server Name: 10.00.20 Server: 10.00.20 Server: 10.00.20 Server: 10.00.20 Server: 10.00.20 Priority 1: 0.00.20 Priority 1:	AP Authentication	Backup RADIUS Server Nar	me:		
Accounting Priority 1: NoNE > 0 Priority 1: NONE > 0 Default Server Priorities EAP Authentication MAC Authentication Accounting Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 3: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0	Intrusion Detection	Backup RADIUS Server:		(Hostname or IP Add	tress)
Advance Security Apply Delete Cancel Corporate Servers IP Version: IP Versio: IP Versio: IP Ve	ocal RADIUS Server	Shared Secret:			
Corporate Servers Current Server List Imply	Advance Security				Apply Delete Cancel
Current Server List IRADUS IP Version: IP Version: Server Name: D0.020 Server: D0.020 Shared Secret: Current Server Priorities EAP Authentication Port (optional): 10.0.0.20 Priority 1: 0.0.0.20 Priority 2: eXDME > 6 Priority 3: eXDME > 6 Priority 1: 0.0.0.20 Priority 2: eXDME > 6 Priority 3: eXDME > 6 Priority 1: 0.0.0.20 Priority 2: eXDME > 6 Priority 3: eXDME > 6 Priority 1: eXDME > 6 Priority 1: eXDME > 6 Priority 1: eXDME > 6 Priority 2: eXDME > 6 Priority 2: eXDME > 6 Priority 3: eXDME > 6 Priority 3: eXDME > 6 <		Corporate Servers			
IP Version: IP V4 IPV6 Server Name: 100.020 Server Name: 100.020 Server: 100.020 Shared Secret: 100.020 Delete Authentication Port (optional): 1812 Delete Authentication Port (optional): 1812 Delete Authentication Port (optional): 1812 Delete Authentication Port (optional): 1813 Output 1813 0.65535) Accounting Port (optional): 1813 0.65535) Apply Cancel Priority 1: 00.020 Priority 1: 00.022 9 Priority 2: NONE> 0 Priority 1: 00.022 9 Priority 1: 00.020 Priority 1: 00.022 9 Priority 2: NONE> 0 Priority 1: 00.022 9 Priority 1: 00.020 Priority 1: 00.022 9 Priority 2: NONE> 0 Priority 2: NONE> 0 Priority 3: NONE> 0 Priority 1: NONE> 0 Priority 1: NONE> 0 Priority 3: NONE> 0		Current Server List			
IP Version: IP V4 IPV6 Server Name: 100.020 100.0.20 Server: 100.0.20 Shared Secret: Interface Delete Authentication Port (optional): 1812 (0-65535) Accounting Port (optional): 1813 (0-65535) Accounting Port (optional): 1813 (0-65535) Priority 1: 100.020 Priority 1: (NONE> 0 Priority 2: (NONE> 0 Priority 2: (NONE> 0 Priority 3: (NONE> 0 Priority 3: (NONE> 0 Priority 1: (NONE> 0 Priority 2: (NONE> 0 Priority 1: (NONE> 0 Priority 2: (NONE> 0 Priority 2: (NONE> 0 Priority 2: (NONE> 0 Priority 3: (NONE> 0 Priority 3: (NONE> 0 Priority 3: Priority 3: (NONE> 0 Priority 3: Priority 3:		RADIUS			
Server Name: 1000.20 100.0.20 General Control (Hostname or IP Address) Shared Secret: Server: Delete Authentication Port (optional): 1812 (0-65535) Accounting Port (optional): 1813 (0-65535) Accounting Port (optional): 1813 (0-65535) Priority 1: 100.0.20 Priority 1: 100.0.20 Priority 1: 100.0.20 Priority 1: 100.0.20 Server Priority 1: 100.0.20 Priority 1: NONE > 0 Priority 1: 100.0.20 Server Priority 1: 100.0.20 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0 Priority 2: NONE > 0 Priority 1: NONE > 0 Priority 2: NONE > 0		< NEW >	IP Version:		
Server: 1000220 (ridsidane of it = Address) Shared Secret:		10.0.0.20 10.9.0.9	Server Name:	10.0.0.20	(Hostname or IR Address)
Delete Authentication Port (optional): 1812 (0-65535) Accounting Port (optional): 1813 (0-65535) Default Server Priorities			Server:	10.0.0.20	(Hostilame of IF Address)
Delete Authentication Port (optional): 1812 (0-65535) Accounting Port (optional): 1813 (0-65535) Apply Cancel Default Server Priorities EAP Authentication Accounting Priority 1: 10.0.0.20 © Priority 1: <0.0.0.20 © Priority 1: 10.0.0.20 © Priority 1: <0.0.0.20 © Priority 2: <none> © Priority 1: <0.0.0.20 © Priority 2: <none> © Priority 1: <0.0.0.20 © Priority 2: <none> © Priority 2: <none> © Priority 2: <none> © Priority 3: <none> © Priority 3: <none> © Priority 3: <none> © Priority 1: <none> © Priority 1: <none> © Priority 2: <none> © Priority 2: <none> © Priority 3: <none> © Priority 3: <none> © Priority 3: <none> © Priority 3: <none> © Priority 3: <none> ©</none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>					
Accounting Port (optional): 1813 (0-65535) Apply Cancel Default Server Priorities MAC Authentication Accounting Priority 1: 10.0.0.20 9 Priority 1: (NONE > 0 Priority 1: 10.0.0.20 9 Priority 1: 10.0.0.20 9 Priority 1: (NONE > 0 Priority 1: 10.0.0.20 9 Priority 2: (NONE > 0 Priority 1: (NONE > 0 Priority 2: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (NONE > 0 Priority 2: (NONE > 0 Priority 2: (NONE > 0 Priority 3: (Priority 2: (Priority 3: (Priority		Delete	Authentication Port (optional):	1812 (0-65535)	
Default Server Priorities EAP Authentication MAC Authentication Accounting Priority 1: 10.0.20 © Priority 1: 10.0.20 © Priority 2: NONE > © Priority 1: 10.0.20 © Priority 2: NONE > © Priority 1: 10.0.20 © Priority 2: NONE > © Priority 2: NONE > © Priority 2: NONE > © Priority 3: NONE > © Priority 3: NONE > © Priority 3: NONE > © Priority 1: NONE > © Priority 1: NONE > © Priority 2: NONE > © Priority 1: NONE > © Priority 2: NONE > © Priority 2: NONE > © Priority 3: NONE > © Priority 2: NONE > © Priority 3: NONE > © Priority 3: NONE > © Priority 3: NONE > © Priore			Accounting Port (optional):	1813 (0-65535)	
Default Server Priorities EAP Authentication MAC Authentication Accounting Priority 1: 10.0.0.20 0 Priority 1: 10.0.0.20 0 Priority 1: 10.0.0.20 0 Priority 1: 10.0.0.20 0 Priority 1: 10.0.0.20 0 Priority 1: 10.0.0.20 0 Priority 2: <none> 0 Priority 1: <inone> 0 Priority 2: <inone> 0 Priority 3: <none> 0 Priority 1: <inone> 0 Priority 3: <inone> 0 Admin Authentication (RADIUS) Admin Authentication (TACACS+) Priority 1: <inone> 0 Priority 2: <inone> 0 Priority 2: <inone> 0 Priority 2: <inone> 0 Priority 3: <inone> 0 Priority 3: <inone> 0 Priority 3: Priority 3: <inone> 0 </inone></inone></inone></inone></inone></inone></inone></inone></inone></none></inone></inone></none>					Apply Cancel
EAP Authentication MAC Authentication Accounting Priority 1: 10.0.0.20 0 Priority 1: (NONE > 0 Priority 1: 10.0.0.20 0 Priority 1: 10.0.0.20 0 Priority 1: (NONE > 0 Priority 1: 10.0.0.20 0 Priority 2: (NONE > 0 Priority 1: (NONE > 0 Priority 2: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (NONE > 0 Admin Authentication (RADIUS) Admin Authentication (TACACS+) Priority 1: (NONE > 0 Priority 2: (NONE > 0 Priority 2: (NONE > 0 Priority 2: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (NONE > 0 Priority 3: (Apply) Cancel		Default Server Priorities			
Priority 1: 10.0.20 G Priority 1: < NONE > G Priority 1: 10.0.20 G Priority 2: <none> G Priority 2: <none> G Priority 2: <none> G Priority 3: <none> G Priority 3: <none> G Priority 2: <none> G Admin Authentication (RADIUS) Admin Authentication (TACACS+) Priority 1: <none> G Priority 1: <none> G Priority 2: <none> G Priority 2: <none> G Priority 2: <none> G Priority 3: <none> G Priority 1: <none> G Priority 3: <none> G Priority 3: <none> G Priority 3: <none> G Priority 3: <none> G</none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>		EAP Authentication	MAC Authentica	tion	Accounting
Priority 2: < NONE > © Priority 2: < NONE > © Priority 3: < NONE > © Priority 1: < NONE > © Priority 1: < NONE > © Priority 1: < NONE > © Priority 2: < NONE > © Priority 2: < NONE > © Priority 3: < NONE > © Priority 3: < NONE > © Apply Cancel		Priority 1: 10.0.0.20 📀	Priority 1: < NO	NE > 🗘	Priority 1: 10.0.0.20 📀
Admin Authentication (RADIUS) Admin Authentication (TACACS+) Priority 1: <none> © Priority 2: <none> © Priority 3: <none> ©</none></none></none></none></none></none></none></none>		Priority 2: < NONE > O	Priority 2: < NO		Priority 2: < NONE > 🗘
Admin Authentication (RADIUS) Admin Authentication (TACACS+) Priority 1: < NONE > © Priority 2: < NONE > © Priority 3: < NONE > © Priority 3: < NONE > ©		Phonty 3. < NONE >	Phonty 3. KNO	NE > 🗸	Phonty 3. < NONE > V
Priority 1: < NONE > 0 Priority 2: < NONE > 0 Priority 3: < NONE > 0 Priority 3: < NONE > 0		Admin Authentication (RAD	DIUS) Admin Authentic	cation (TACACS+)	
Priority 2: < NONE > Priority 2: < NONE > Priority 3: < NONE > Priority 3: < NONE > Apply Cancel		Priority 1: < NONE > 🗘	Priority 1: < NO	NE > 🗘	
Priority 3: < NONE > Priority 3: < NONE > Apply Cancel		Priority 2: < NONE > ᅌ	Priority 2: < NOT	NE > 🗘	
Apply Cancel		Priority 3: < NONE > ᅌ	Priority 3: < NO	NE > 🗘	
					Apply Cancel

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。

.ı ı.ı ı. cısco	Save 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	UNDS STATUS
АР	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。

	HOME NETWORK	ASSOCIATION WIRE	LESS SECURITY	SERVICES	Sa <u>v</u> e (MANAGEMENT	Configuration	Ping Logout <u>R</u> efresh
Services	Hostname ap-1		_	T	a	p-1 uptime is 1 o	day, 4 hours, 48 minutes
Hot standby	Services: VI AN						
CDP	Global VI AN Pro	nortion					
DNS	GIODAI VEAN PIC	percies					
Filters	Current Native	/LAN: VLAN 10					
нттр	Assigned VLANs	i .					
QOS	Current VI AN I	iat			Define SSID	•	
Stream		191	Greate VLAN		Denne 331D	2	
SNMP	VLAN 2						
SNTP	VLAN 3 VLAN 10		VLAN ID:		10	(1-409	4)
VLAN			VLAN Name (or	tional):			
ARP Caching		Delete	Native VI	AN			
Band Select			Enable P	ublic Secure P	acket Forwarding	3	
Auto Config			Radio0-8	02.11N ^{2.4GHz}			
			Radio1-8	02.11AC5GHz			
			Manager	nent VLAN (if n	ion-native)		
						C	Apply Cancel
	VLAN Informatio	n					
	View Information	for: VLAN 2 ᅌ					
		GigabitEthernet Pack	ets Radio	0-802.11N ^{2.4GHz}	Packets	Radio1-802.1	1AC ^{5GHz} Packets
	Received		65884				65884
	Transmitted		5462				5462
							Refresh

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

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。

սիսիս	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
CISCO	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
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
	Server Group Name: WDS
	Group Server Priorities: Define Servers
	Delete Priority 1: 10.9.0.9
	Priority 2: < NONE > O
	Priority 3: <pre> </pre> <pre> </pre>
	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。

սիսիս		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
CISCO	HOME NETWORK ASSOCIATION WIRELESS	S <u>S</u> ECURITY <u>S</u> ERVICES <u>M</u> ANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG
Wireless Services	🚊 WDS STATUS 📋 GEN	ERAL SET-UP
AP	Hostname ap-1	ap-1 uptime is 2 days, 2 hours, 31 minutes
WDS	Wireless Services: WDS - Server Groups	
	Server Group List	
	Ser	rver Group Name: Clients
	< NEW > WDS	
	Clients	nun Server Priorities: Define Servers
	Delete	Priority 1: 10.0.20 0
		Priority 2: < NONE > 😒
		Priority 3: <pre> </pre> <pre> </pre>
	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	Remove
		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。

ılıılı cısco	Sa <u>v</u> e Configuration Ping Lo HOME <u>N</u> ETWORK ASSOCIATION WIRELESS <u>S</u> ECURITY <u>S</u> ERVICES <u>M</u> ANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT L	gout <u>R</u> efres OG
Security	E STATISTICS	
	Hostname ap-1 uptime is 1 day, 4 hours,	13 minutes
Admin Access	Security: Least DADIIIS Server - Constal Set Lin	
SSID Manager	Local Radius Server Authentication Settings	
Dot11u Manager		
Server Manager	Enable Authentication Protocols: Z EAP FAST	
AP Authentication	C LEAP	
Intrusion Detection	MAC	
Local RADIUS Server	Apply	ancel
Advance Security	Network Access Servers (AAA Clients)	
	Current Network Access Servers	
	Network Access Server: 10.9.0.9 (IP Address	is)
	Shared Secret:	
	Delete	
	Apply C	ancel
	Individual Users	
	Current Users	
	Username: wds	
	< NEW > wds	
	Password:	
	Confirm Password:	
	Delete Group Name: < NONE > 🗘	
	MAC Authentication Only	
		ancel
	lieer Groupe	
	Current User Groups	
	Group Name:	
	Session Timeout (optional): (1-42949672	295 sec)
	Delete Failed Authentications before Lockout (optional): (1-4294967295)	
	Lockout (optional): O Infinite	
	Interval (1-4294967295	sec)
	VLAN ID (optional):	
	SSID (optional):	
	Delete	
	Apply	Cancel

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

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

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

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

WDS サーバーに対する認証に使用する **[ユーザー名 (Username)]** と **[パスワード (Password)]** を入力します。

. cisco	<u>H</u> OME <u>N</u> ETWORK	<u>A</u> SSOCIATION WI	<u>I</u> RELESS <u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e (<u>M</u> ANAGEMENT	Configuration	Ping Logout	<u>R</u> efresh
Wireless Services	Hostname ap-1				ар	-1 uptime is 1 d	ay, 4 hours, 50	minutes
WDS	Wireless Servio	ces: AP SWAN Infrastructure:	• Enable 🔾	Disable				
		WDS Discover	y: Auto Discov Specified D	very iscovery: 10.9.0.	9	(IP Address)		
		Username: Password:	wds					
		Confirm Passy Authentication Methods Profil	None >	<mark>≎</mark> _Defi	ine Authentication I	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	<u>H</u> ome <u>N</u> etwork <u>A</u> s	SSOCIATION W <u>I</u> RE	LESS	SECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	e Configui <u>S</u> OFT	ration <u>P</u> ing WARE <u>E</u> V	Logout <u>R</u> efres ENT LOG	
Wireless Services	WDS STATU: Hostname ap-1	s	GENER	AL SET-UP	Ĩ	SERVER GROU	JPS ap-1 up	otime is 1 day	, 5 hours, 1 minute	
WDS	Wireless Services: W WDS Information	VDS - Wireless Doma	in Servi	ces - Status						
	MAC Address	IPv4 Address		IPv6 Addre	255	Priority		State		
	18e7.281b.3f54	10.9.0.9		::		255		Administra - ACTIVE	tively StandAlone	
	WDS Registration									
	APs: 1			Mobile Not	es: 0					
	AP Information									
	Hostname	MAC Address		IPv4 Addro	255	IPv6 Address		CDP Neighbor	State	
	ap-1	18e7.281b.3f54		10.9.0.9		::		Switch-2.gi	I REGISTERED	
	Mobile Node Information									
	MAC Address	IP Address	State			SSID	VLAN I	D BS	SID	
	Wireless Network Manager Information									
	IP Address	Authentication Statu	IS							
									Refresh	

コール アドミッション制御 (CAC)

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

Cisco Autonomous アクセスポイントは、1 ストリームのみに対応しており、ストリームサイズはカスタマイズ できないので、CAC が有効である場合に SRTP および Barge(割り込み)、サイレントモニタリング、コール 録音は機能しません。

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

Dot11 ssid voice vlan 3 authentication open eap eap_methods authentication network-eap eap_methods authentication key-management wpa version 2 dot11r admit-traffic

ces	QoS POLICIES	R AC	ADIO0-802.11N ^{2.4GHZ}	RADIO1-802.11AC ^{5G} ACCESS CATEGORIE	HZ ADVAN	CED
et/SSH	Hostname ap-1				ap-1 uptime i	s 1 day, 4 hours, 47 min
standby						
	Services: QoS Policies	s - Acces	s Category			
	Access Category Defin	nition				
rs						
•	Access Categor	У	Background (CoS 1-2)	Best Effort (CoS 0.3)	Video (CoS 4-5)	Voice (CoS 6-7)
		4.5	(000)	(000 0,0,	(000 + 0)	(00001)
am	Window	AP	4	4	3	2
Р	(2x-1; x can be 0-10)	Client	4	4	3	2
•	Max Contention	AP	10	6	4	3
4	Window					
Caching	(2x-1; x can be 0-10)	Client	10	10	4	3
Select	Fixed Slot Time	AP	7	3	1	1
Config	(0-20)	Client	7	3	2	2
	Transmit Opportunity	AP	0	0	3008	1504
	(0-65535 µS)	Client	0	0	3008	1504
	Admission Control for	Video ar	nd Voice	Optimized Voice W	/FA Default	Apply Cancel
	Video(CoS 4-5)	Admis	sion Control			
	Voice(CoS 6-7)					
		Admis:	sion Control			
		Max Ch	annel Capacity (%): 7	5		
		Roam C	Channel Capacity (%): 6			

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。

ces		RADIO0-802.11N ^{2.4GHZ} ACCESS CATEGORIES	RADIO1-802.11AC ^{5GHZ} ACCESS CATEGORIES	ADVANCED
et/SSH	Hostname ap-1		ap	1 uptime is 1 day, 4 hours, 44 min
standby				
	Services: QoS Policies			
rs	Create/Edit Policies			
P	Create/Edit Policy:	Voice 🗘		
am	Policy Name:	Voice		
IP	-			
Р	Classifications:	DSCP - COS Controlled Load (4)		
N	olussinoulionsi	DSCP - COS Voice < 10ms Latency (F	(5)	
Caching		DSCP - COS Voice C Ionis Latency (C)	
d Select				
Config		Delete Classification		
	Match Classification	e.	Anniv Class	of Service
	IR Presedence	Poutino (0)	Rest Effort (0)	Add
	IP Precedence.		Dest Effort (0)	
	IP DSCP:	Best Effort	Best Effort (U)	Add
		0 (0-6	3)	
	IP Protocol 119		Best Effort (0)	Add
	Filter:	No Filters defined. Define Filters.		
	Default Classificati	on for Packets on the VLAN:	Best Effort (0)	Add
	Rate Limiting:			
	Bits per Sec.:	(8000-200000000)	Burst Rate (Bytes):	(1000-512000000)
	Conform Action:	Transmit ᅌ	Exceed Action: Drop	Add
				Apply Delete Cancel
	Apply Policies to Interfa	ce/ VLANs		
	VLAN 2	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
	Incoming		Data ᅌ	Data ᅌ
	Outgoing		Data ᅌ	Data ᅌ
	VLAN 3	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
	Incoming		Voice	Voice
	Outgoing		< NONE > 📀	< NONE > ᅌ
	VI 41 40		-	Circh HEthamat (
		Kadio0-802.11N ^{2.46h2}	Radio1-802.11AC	GigabitEthernetU
	Outcoing			< NONE > C
	Outdoing		< NONE > 😂	< NONE > 😴

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

[Dot11e] をオンにすると、両方の CCA バージョン (802.11e および Cisco バージョン 2) が有効 になります。

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

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

 cısco	Sa <u>v</u> e 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
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	Ose Element for Wireless Dearses
нттр	QOS Element for Wireless Phones : O Enable O Dot ne
QOS	○ Disable
Stream	IGMP Snooping
SNMP	
SNTP	Snooping Helper: 🧿 Enable 🔿 Disable
VLAN	
Rand Select	AV//D Priority Manning
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 (Stream)]機能を有効にする場合は、音声パケットのみが音声キューに追加されることを確認し ます。シグナリングパケットは、別個のキューに追加する必要があります。SIP を別個のキューに入れるには、 DSCP を適切なキューにマッピングする QoS ポリシーを設定します。

ululu cisco	<u>H</u> OME <u>N</u> ETWORK <u>A</u> SSOCIAT	ION W <u>I</u> RELES	s <u>s</u> ecurity	<u>S</u> ERVICES	Sa <u>v</u> e (<u>M</u> ANAGEMENT	Configuration	Ping Logout <u>R</u> efres
Services	RADIO0-802.11N ^{2.4GHZ}	RADIO1-802.11	AC ^{5GHZ}				
Telnet/SSH	Hostname ap-1				ar	-1 uptime is 1 d	ay, 4 hours, 48 minutes
Hot standby							
CDP	Services: Stream						
DNS	Packet Handling per User P	riority:					
Filters	User Priority	Packet Hand	lling	Max Retries for Pa	acket Discard		
нттр	CoS 0 (Best Effort)	Reliable	0	NO DISCARD	(0-128)		
QOS	CoS 1 (Background)	Dellable			(0.129)		
Stream	eee (basigioand)	Reliable		NO DISCARD	(0-120)		
SNMP	CoS 2 (Spare)	Reliable	0	NO DISCARD	(0-128)		
SNTP	CoS 3 (Excellent)	Reliable	٥	NO DISCARD	(0-128)		
VLAN	CoS 4 (Controlled Load)	Reliable		NO DISCARD	(0-128)		
ARP Caching		(
Band Select	CO3 5 (VIDEO)	Reliable	0	NO DISCARD	(0-128)		
Auto Config	CoS 6 (Voice)	Reliable	0	NO DISCARD	(0-128)		
	CoS 7 (Network Control)	Reliable	0	NO DISCARD	(0-128)		
	Low Latency Packet Rates:						
	6.0Mb/sec :	O Nominal	Non-Nominal	 Disable 			
	9.0Mb/sec :	O Nominal	Non-Nominal	 Disable 			
	12.0Mb/sec :	Nominal	Non-Nominal	Disable			
	18.0Mb/sec :	Nominal	Non-Nominal	Disable			
	24.0Mb/sec :	Nominal	Non-Nominal	Disable			
	36.0Mb/sec :		Non-Nominal	Disable			
	48 0Mb/sec 1						
	54.0Mb/sec :	Nominal	Non-Nominal	 Disable Disable 			
				-			Analy Oraci
							Apply Cancel

電源管理

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> 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
Services	Hostopme and states for minutes
Telnet/SSH	
Hot standby	Services: ARP Caching
CDP	Client ARP Caching: Disable Disable
DNS	
Filters	Constant ADD Descents To Desite Interfaces Million Net All Officer ID Addresses Are Known
НТТР	Forward ARP Requests to Radio Interfaces when Not All Client IP Addresses are known
QOS	
Stream	
SNMP	Apply Cancel

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド
設定例

```
バージョン 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
Į.
hostname ap-1
logging rate-limit console 9
aaa new-model
aaa group server radius rad_eap
server name 10.0.0.20
I.
aaa group server radius rad_mac
aaa group server radius rad_acct
server name 10.0.0.20
L
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
н
aaa group server radius rad_pmip
L
aaa group server radius dummy
н
aaa group server radius WDS
server name 10.9.0.9
L
aaa group server radius Clients
server name 10.0.0.20
I.
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
I.
aaa session-id common
clock timezone -0500 -5 0
```

```
clock summer-time -0400 recurring
no ip source-route
no ip cef
ip domain name cisco.com
ip name-server 10.0.0.30
ip name-server 10.0.0.31
dot11 pause-time 100
dot11 syslog
dot11 ssid data
 vlan 2
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa version 2
dot11 ssid voice
 vlan 3
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa version 2 dot11r
dot11 arp-cache optional
dot11 phone dot11e
L
no ipv6 cef
crypto pki trustpoint TP-self-signed-672874324
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-672874324
revocation-check none
rsakeypair TP-self-signed-672874324
L
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> ļ 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 1 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 I 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 L interface Dot11Radio1 no ip address ! encryption vlan 2 mode ciphers aes-ccm 1

encryption vlan 3 mode ciphers aes-ccm L ssid data 1 ssid voice L 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 dot11r pre-authentication over-air dot11 dot11r reassociation-time value 1000 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 I. interface Dot11Radio1.2 encapsulation dot1Q 2 bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 spanning-disabled bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding service-policy input Data service-policy output Data L 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 I. 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 I interface GigabitEthernet0 no ip address duplex auto speed auto 1 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 1 interface GigabitEthernet0.10 encapsulation dot1Q 10 native bridge-group 1 bridge-group 1 spanning-disabled no bridge-group 1 source-learning 1 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 L radius-server local nas 10.9.0.9 key 7 <REMOVED> user wds nthash 7 <REMOVED> L 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>
ŗ.
radius server 10.9.0.9
address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
key 7 <REMOVED>
ŗ.
access-list 111 permit tcp any any neg telnet
bridge 1 route ip
1
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 vtv 0 4
access-class 111 in
transport input all
1
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。

- [WPA2-Enterprise] または [事前共有キー (Pre-shared key)]で [802.11r] を有効にします。
- [スプラッシュページ (Splash page)] を [なし (None)] に設定します。
- [ブリッジモード (Bridge mode)]を有効にします。
- [VLAN タギング (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。

ululu cisco Meraki	Q Search Dashboard		
NETWORK	Create networ	k	
Meraki MX64 🛛 🔫			
	Setup network		
Network-wide	Networks provide a way physically distinct sites	to logically group, configure, and mor within an Organization. ()	itor devices. This is a useful way to separate
Security & SD-WAN	Network name	Scranton Branch Office	
Organization			
	Network type	Wireless -	
	Network configuration	O Default Meraki configuration	
		Bind to template No templat	tes to bind to
		Clone from existing network	Select a network 👻
	Select devices fro	om inventory	
		You have no unused dev Add new devices or go to the invento that are already in networks	ices ry page to select devices
		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 number	rs (one per row). <u>Wi</u>	here can I find the	se numbers?		
			Close	Claim	

要求した Cisco Meraki アクセスポイントは、**[組織 (Organization)]>[設定 (Configure)]>[インベントリ** (Inventory)] ページで対象ワイヤレスネットワークに追加できます。

cisco Meraki	Q Search Dashboard	
NETWORK Meraki WLAN -	Inventory View used and unused devices in your organization. You can <u>cla</u>	aim new devices to add the list below.
	Add to Unclaim Unused Used Both Search inventory	
Notwork-wide	• Existing network	Model A Claimed on
Network-wide		
Network-wide	Meraki WLAN *	MR53 4/29/2020 2:59 PM
Wireless	Meraki WLAN	MR53 4/29/2020 2:59 PM

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

cisco Meraki	Q Search Dashboard			
NETWORK	Add access points	6		
Meraki WLAN 👻	Add access points from your o devices in the order will be ad	organization's inventory. When you ded to your inventory. When you	u claim an order claim a device by	by order number, the y its serial number, that
	device will be added to your in	nventory. Once in your inventory,	you can add devi	ces 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 の設定

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

Cisco Wireless Phone 840 および 860 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。

ululu cisco Meraki	Q Search Dashboard		
NETWORK	Configuration ov	verview	
Meraki WLAN 👻	SSIDs	Showing 4 of 15 SSIDs	. Show all my SSIDs.
			meraki-voice
Network odda	Enabled		enabled 🗘
Network-wide	Name		rename
	Access control		edit settings
Wireless	Encryption		802.1X with Meraki RADIUS
	Sign-on method		None
Organization	Bandwidth limit		unlimited
	Client IP assignment		Local LAN
	Clients blocked from us	sing LAN	no
	Wired clients are part o	f Wi-Fi network	no
	VLAN tag 📵		3
	VPN		Disabled
	Splash page		
	Splash page enabled		no
	Splash theme		n/a

[ワイヤレス (Wireless)]>[設定 (Configure)]>[アクセス制御 (Access control)]ページで、[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。

[802.11r] が有効になっていることを確認します。

[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	•
Network-wide	Network access Association requirements	Open (no encryption) Any user can associate
Wireless 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 🕲	Enabled 😚
	802.11w	Disabled (never use)
	Splash page	• None (direct access) Users can access the network as soon as they associate

注: Cisco Meraki アクセスポイントは、802.11r (FT) による高速セキュアローミングをサポートしますが、 Cisco Centralized Key Management (CCKM) はサポートしません。

[WPA2-Enterprise] が有効になっている環境で Cisco Meraki 認証サーバを RADIUS サーバとして使用する場 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、Cisco Wireless Phone 840 および 860 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。

ululu cisco Meraki	Q Search Dashboard				
	User management pe	ortal			
Meraki WLAN 👻	SSID: meraki-voice	vith Meraki authentication. These	e 802.1X accounts are mar	naged separately from Administrator o	r Guest accounts.
	Authorization + Remove Users	Search			
Network-wide	Description	Email (Username)	Account type	Authorized for SSID *	Authorized by
				Save Changes or cancel	
			(Pleas	se allow 1-2 minutes for changes to take effect.	
		Create user	000 AV		×
		Account type: meraki	802.1X		_
		Description:			
		Email (Username):			
		Password:	Gene	rate	
		Authorized: No 😜			_
				Close Print Creat	e 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 Wireless Phone 840 および 860 は、コール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、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 VolP 導入ガイド』を参照 してください。

https://meraki.cisco.com/lib/pdf/meraki whitepaper msvoip.pdf [英語]

Cisco IOS スイッチを使用する場合は、Cisco Meraki アクセス ポイントが接続するスイッチ ポートを次のよう に構成して、802.1g 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 cisco Meraki	Addressing and trat	ffic
NETWORK	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.
Meraki WLAN 🔫		Bridge mode: Make clients part of the LAN Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras.
Network-wide		Layer 3 roaming
Wireless		clients receive UPCP leases from the LAN or use state IPS, similar to noge mode. If the client totams to an AP where their original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.
Organization		Layer 3 roaming with a concentrator Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
		 VPN: tunnel data to a concentrator Meraki devices send traffic over a secure tunnel to an MX concentrator.
	VLAN tagging Bridge mode and layer 3 roaming only	Use VLAN tagging
	VLAN ID	AP tags VLAN ID Actions
		All other APs 3
		Add VLAN
	Content filtering () NAT mode only	Don't filter content
	Bonjour forwarding Bridge mode and layer 3	Enable Bonjour Gateway
	roaming 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 Wireless Phone 840 および 860 で使用する SSID の周波数帯域を設定できます。

Cisco Wireless Phone 840 および 860 は、**5 GHz 帯域のみ**での動作を推奨します。5 GHz 帯域では多数のチャネルを使用できるうえ、2.4 GHz 帯域ほど干渉が多くないためです。

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。

uludu cisco Meraki	Wireless options	Wireless options		
NETWORK	. Band selection an	d minimum bitrate settings may be overridden by RF profiles. Go to RF Profiles		
Meraki WLAN	Band selection	O Dual band operation (2.4 GHz and 5 GHz)		
Network-wide Wireless		 5 GHz band only 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it. Dual band operation with Band Steering Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients. 		
Organization	Minimum bitrate (Mbps) 🛞	Lower Density Higher Density 1 2 5.5 6 9 11 12 18 24 26 48 54 B02.11b devices not supported		

[ワイヤレス (Wireless)]>[設定 (Configure)]>[SSID の可用性 (SSID availability)]ページでは、[可視性 (Visibility)]を[この SSID をパブリックにアドバタイズする (Advertise this SSID publicly)]に設定することで SSID をブローキャストできます。

[AP ごとの可用性 (Per-AP Availability)]は[この SSID をすべての AP で有効にする (This SSID is enabled on all APs)]に設定することを推奨します。

必要に応じて SSID の可用性をスケジュール設定できますが、[スケジュールされた可用性 (Scheduled Availability)]は[無効 (Disabled)]に設定することを推奨します。

cisco Meraki	Q Search Dashboard	
NETWORK	SSID availability	
Meraki WLAN 👻	SSID: meraki-voice	0
	Visibility	Advertise this SSID publicly
Network-wide	Per-AP availability	This SSID is enabled on all APs
Wireless	Scheduled availability	disabled 😨
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 5 GHz または 2.4 GHz 無線のいずれかに、チャンネルと送信電力を静的に設定できます。これは、エリアに断続的な干渉源が存在する場合に必要になることがあります。一方で、他のアクセスポイントで[自動 (Auto)]を有効にし、静的チャンネルが割り当てられているチャンネルを回避できます。

cisco Meraki	Q Search Dashboard
NETWORK	Radio settings
Meraki WLAN 👻	Overview RF profiles
Network-wide	BAND CHANNEL AP TAG RF PROFILE REGULATORY DOMAIN 5 ~ AII ~ AII ~
Wireless	Search by AP name Update auto channels Edit settings •
Organization	Image: Status ● AP name ▲ Channel Ch. Width (MHz) Target power (dBm) ● Transmit power (dBm) ● RF Profile ✓ Image: 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	Q Search Dashboard
NETWORK	RF PROFILES Edit Basic Indoor Drafilo
Meraki WLAN 👻	
	General 2.4 GHz 5 GHz
Network-wide	General
Wireless	Band selection Per AP Per SSID
Organization	The Access Points configured to use this profile will follow the band selection set on the Access Control page for the respective SSID. date.
	Minimum bitrate configuration Per band Set the minimum bitrates for the 2.4 & 5 GHz radios separately below. Per SSID The Access Points configured to use this profile will follow the minimum bitrate selection set on the <u>Access Control page</u> for the respective SSID. Per SSID minimum bitrate selection will be moved to RF profiles at a later date.
	Client balancing On Off Client Balancing uses information about the state of the network and wireless client probes to steer the client to the best available access point during association. Read more about client balancing here.

RF プロファイルでは、5 GHz 無線の **[チャンネル幅(Channel width)]** は、20 MHz、40 MHz、または 80 MHz チャンネルを使用するように設定できます。

2.4 GHz 無線は 20 MHz チャンネルを使用し、他のチャンネル幅に設定することはできません。 すべてのアクセス ポイントで同じチャネル幅を使用することを推奨します。

[AutoChannel] で使用される 5 GHz チャンネルも RF プロファイルで設定できます。 [AutoChannel] で使用される 2.4 GHz チャンネルは、チャンネル 1、6、および 11 のみに制限されています。

[無線送信電力範囲 (Radio transmit power range)] も RF プロファイルで設定されます。

[最小ビットレート構成 (Minimum bitrate configuration)]が[バンドごと (Per band)]に設定されている 場合、SSID 構成で定義されている内容が上書きされます。

従来の 2.4 GHz クライアントがワイヤレス LAN に接続できるようにする必要がある場合を除き、12 Mbps 未 満のデータレートは無効することを推奨します。



ululu useo Meraki	General 2.	4 GHz	5 GHz														_
		Chang	je 5 GHz	channels	used by A	utoChanr	nel										22
NETWORK	5 GHz rad	Availabl	e channels	for AutoCha	nnel												
Meraki WLAN 👻	Turn off 5GHz	lf you de	iselect a ch	annel, AutoCh	annel will not	assign it to	any AP w	ith this pro	ofile. Click	on a channel	to toggle its s	election.					_
	Channel width			UNII-1	UNI	1-2	UNII=2+	Extended		Wear	ther Radar					UNII-3	ISM
		20 MHz	36 40	44 48	52 56	60 64	100	104 1	08 112	116 120	124 128	3 132	136	140 144	149 15	3 157 161	165
Wireless		40 MHz	38	46	54	62	10	2	110	118	126	134		142	151	159	
		80 MHz		42	51	3		106			122		13	18		155	
								DFS cha	nnels	Deselect DFS	channels						
																	-
																Cancel	Done
			-	For low to	o medium de	ensity depl	oyments		-	-	-	-		-	-		_
) 80 MHz (5 channels)												
				For low d bandwidt problems	ensity areas th and data i	a with few o rates for m	or zero n odern de	eighborir vices. In	ng netwo creases i	ks. Higher isk of interfe	erence						

注: Cisco Meraki アクセス ポイントでは、ダイナミック伝送パワーコントロール (DTPC) がサポートされま せん。そのため、Cisco Wireless Phone 840 および 860 は、現在のチャンネルとデータレートでサポートされ る最大送信電力を使用します。

ファイアウォール & トラフィック シェーピング

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

ワイヤレスクライアントのローカル LAN アクセスを許可するように、**[レイヤ 3 ファイアウォールルール** (Layer 3 firewall rule)]が構成されていることを確認します。

トラフィック シェーピング ルールを定義できるようにするには、**[トラフィックのシェープ (Shape traffic)**]ドロップダウンメニューで **[この SSID のトラフィックをシェープ (Shape traffic on this SSID)**]を選択します。

[この SSID のトラフィックをシェープ (Shape traffic on this SSID)]を適用した後、[新しいルールを作成 (Create a new rule)]を選択して [トラフィック シェーピング ルール (Traffic shaping rules)]を 定義します。

Cisco Meraki アクセス ポイントのデフォルトでは、DSCP EF (46) とマークされた音声フレームに WMM UP 6 ではなく WMM UP 5 のタグを、DSCP CS3 (24) とマークされたコール制御フレームに WMM UP 4 ではな く WMM UP 3 のタグを付けます。

cisco Meraki	Q Search Dashboard						
NETWORK Meraki WLAN -	Firewall & traffic s	shaping ©					
Network-wide Wireless	Block IPs and ports Layer 2 LAN isolation	Disabled 😮 (b	ridge mode	only)			
Organization	Layer 3 firewall rules 😈	# Policy Allow Allow Add a layer 3 f	Protocol Any Any rewall rule	Destination Local LAN Any	Port Any Any	Comment Wireless clients accessing LAN Default rule	Actions
	Block applications ar Layer 7 firewall rules	nd content c There are no ru <u>Add a layer 7 f</u>	ategories ules defined <u>irewall rule</u>	S for this SSID.			
	Traffic shaping rules Per-client bandwidth limit Per-SSID bandwidth limit	unlimited unlimited	details details	Enable Sp	peedBu	rst 🖲	
	Shape traffic	Shape traffic on t	his 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 Call Control の設定

Cisco Unified Communications Manager

Cisco Unified Communications Manager は、さまざまな電話機機能、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 Wireless Phone 840 または 860 のデバイスタイプを有効 にするには、対応するデバイスイネーブラ (QED) の COP ファイルを、各 Cisco Unified Communications Manager サーバーの Cisco Unified Operating System Administration Web ページからインストールする必要 があります。

デバイスイネーブラ(QED)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-managercallmanager/products-maintenance-guides-list.html

Cisco Wireless Phone 840 または 860 を Cisco Unified Communications Manager に追加する場合は、Wi-Fi MAC アドレスを使用してプロビジョニングする必要があります。

Cisco Wireless Phone 840 または 860 の Wi-Fi MAC アドレスは、[設定 (Settings)]>[電話について (About phone)]>[Wi-Fi MAC アドレス (Wi-Fi MAC address)]の順に選択して確認できます。

1.3(0) リリースの時点で、Cisco Wireless Phone 840 および 860 は、複数回線(最大 6)、共有回線、 およびプライバシーをサポートしています。

Cisco Wireless Phone 840 および 860 は自動登録をサポートしていません。

Device Information		
Device is trusted		
MAC Address*		
Description		
Device Pool*	Not Selected	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Not Selected	٥]
Softkey Template	< None >	٥
Common Phone Profile *	Standard Common Phone Profile	View Details

注: Cisco Wireless Phone 840 および 860 は、直接コールにはコーリングサーチスペースを使用し、転送に は再ルーティング コーリング サーチ スペースを使用するため、両方のオプションが正しく設定されていること を確認します。

Cisco Unified Communications Manager サーバーのホスト名と関連する証明書は、完全修飾ドメイン名 (FQDN) または IP アドレスを使用して一致する必要があります。

製造元の認証局 (CA) 証明書

Cisco Wireless Phone 840 および 860 には、新しい製造元の認証局(CA)が使用されています。

新しいルート証明書と中間証明書が Cisco Unified Communications Manager にネイティブに含まれるまで、 新しい製造元でインストールされた証明書(MIC)を信頼するには、ルート証明書と中間証明書を証明書チェー ンに手動で追加する追加の手順が必要です。

 外部で入手可能な Cisco PKI Web サイトから、不足しているルート証明書と中間証明書をダウン ロードします。
 https://www.cisco.com/security/pki

新しい MIC のルートを含む、信頼チェーンを完了するために不足している証明書は次のとおりです。

- <u>Cisco Manufacturing CA III (cmca3)</u> 一 中間 <u>http://www.cisco.com/security/pki/certs/cmca3.pem</u>
- <u>Cisco Basic Assurance Root CA 2099 (cbarc2099)</u> Cisco Manufacturing CA III のルート http://www.cisco.com/security/pki/certs/cbarc2099.pem
- 2. Web ブラウザで、Cisco Unified Operating System Administration Web ページにログインします。
- 3. [セキュリティ (Security)]メニューで、[証明書管理 (Certificate Management)]を選択します。

- 4. [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)]を選択します。
- 5. **[証明書の目的 (Certificate Purpose)**]に対して CallManager-trust を選択し、証明書を参照し、 [アップロード (Upload)]を選択します。

注: 証明書は他のすべての Cisco Unified Communication Manager ノードに複製されるため、Cisco Unified Communication Manager パブリッシャのすべての証明書に対してこの手順を繰り返します。

6. **[証明書の目的 (Certificate Purpose)]** に対して CAPF-trust を選択し、証明書を参照し、**[アップロ** ード (Upload)]を選択します。

注: 証明書は他のすべての Cisco Unified Communication Manager ノードに自動的に複製されないた め、すべての Cisco Unified Communication Manager ノードのすべての証明書に対してこの手順を繰 り返します。

[デバイスプール (Device Pools)]

Cisco Wireless Phone 840 または 860 を作成する場合は、デバイスプール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。

۲I	Device Pool Settings			
	Device Pool Name*		Default	
	Cisco Unified Communications Mar	nager Group*	Default	\$
	Calling Search Space for Auto-regi	stration	< None >	٥
	Adjunct CSS		< None >	٥
	Reverted Call Focus Priority		Default	٥
1	Intercompany Media Services Enro	lled Group	< None >	٥
L				
Γ'	Roaming Sensitive Settings			
	Date/Time Group*	CMLocal		٥
	Region*	Default		٥
	Media Resource Group List	< None >		٥
1	Location	< None >		٥
	Network Locale	< None >		٥
1	SRST Reference*	Disable		٥
	Connection Monitor Duration ***			
	Single Button Barge*	Default		•
	Join Across Lines*	Default		٥
	Physical Location	< None >		٥
	Device Mobility Group	< None >		٥
1	Wireless LAN Profile Group	< None >		View Details

電話ボタン テンプレート

新しい Cisco Wireless Phone 840 または 860 を作成する場合は、**電話ボタン テンプレート**を設定する 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。

utton I	Information		
Button	Feature	Label	
1	Line **	Line	
2	✓ Line	Line	
3	Privacy	None	
4	None	None	
5	None	None	
6	None	None	
Save Thone B	Delete Copy Reset Apply Config Add	New	
Save Thone B Sutton Te	Delete Copy Reset Apply Config Add	New	
Save Phone B Button Te Button I Button	Delete Copy Reset Apply Config Add	New	
Save hone B Button Te Button I 1	Delete Copy Reset Apply Config Add Sutton Template Information emplate Name * Cisco 860 Information Feature Line **	New Label Line	
Save thone B sutton Te sutton I Button 1 2	Delete Copy Reset Apply Config Add button Template Information emplate Name * Cisco 860 Information Feature Line **	New Label Line Line Line Line Line Line Line Line	
Save Phone B Button Te Button I Button 1 2 3	Delete Copy Reset Apply Config Add Sutton Template Information emplate Name * Cisco 860 Information Feature Line ** ✓ Line Privacy	New Label Line Line None	
Save hone B utton Te utton I Button 1 2 3 4	Delete Copy Reset Apply Config Add Button Template Information emplate Name * Cisco 860 Information Feature Line ** V Line Privacy None	New Label Line Line None None	
Save Phone B Button Te Button I 1 2 3 4 5	Delete Copy Reset Apply Config Add Button Template Information Template Name * Cisco 860 Enformation Feature Line ** / Line Privacy None None S	New Label Line Line None None None None	

セキュリティ プロファイル

Cisco Wireless Phone 840 または 860 を作成する場合は、デバイス セキュリティ プロファイルを設定する必要があります。

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

セキュリティ プロファイルで Locally Signed Certificate(LSC)を使用するには、認証局プロキシ機能 (CAPF)が動作している必要があります。

Cisco Wireless Phone 840 および 860 には、製造元でインストールされる証明書(MIC)を備えています。この証明書もセキュリティプロファイルから使用できます。

Protocol Specific Information	tion —	
Packet Capture Mode*	None	\$
Packet Capture Duration	0	
SRTP Allowed - When this to end security. Failure to do	s flag is checked, IPSec needs to be configured in so will expose keys and other information.	the network to provide end
BLF Presence Group*	Standard Presence group	\diamond
MTP Preferred Originating Codec*	711ulaw	\$
Device Security Profile*	Cisco 840 - Standard SIP Non-Secure Profile	\Diamond
Rerouting Calling Search Space	< None >	0
SUBSCRIBE Calling Search Space	< None >	0
SIP Profile*	Standard SIP Profile	Siew Details
Digest User	< None >	\$
Media Termination Point	Required	
Unattended Port		
Require DTMF Reception		
Early Offer support for vo	pice and video calls (insert MTP if needed)	
Protocol Specific Informa	tion	
Protocol Specific Information Packet Capture Mode*	tion None	>
Protocol Specific Informa Packet Capture Mode* Packet Capture Duration	None 0	`
Protocol Specific Informa Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do	tion None 0 s flag is checked, IPSec needs to be configured in p so will expose keys and other information.	the network to provide end
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group*	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group	the network to provide end
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating	tion None 0 s flag is checked, IPSec needs to be configured in so will expose keys and other information. Standard Presence group 711ulaw	the network to provide end
Protocol Specific Informa Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec*	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw	the network to provide end
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile*	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile	the network to provide end
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None >	the network to provide end
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None > < None >	Image: state of the
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile*	tion None 0 s flag is checked, IPSec needs to be configured in so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None > < None > Standard SIP Profile	 the network to provide end <
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None > < None > Standard SIP Profile < None >	 the network to provide end the network to provid
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User Media Termination Point	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None > < None > Standard SIP Profile < None > Required	 the network to provide end the network to provid
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User Media Termination Point Unattended Port	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None > < None > Standard SIP Profile < None > Required	 the network to provide end the network to provid
Protocol Specific Informat Packet Capture Mode* Packet Capture Duration SRTP Allowed - When thi to end security. Failure to do BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User Media Termination Point Unattended Port Require DTMF Reception	tion None 0 s flag is checked, IPSec needs to be configured in o so will expose keys and other information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Non-Secure Profile < None > < None > Standard SIP Profile < None > Required	 the network to provide end the network to provid

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:	Cisco 840 SIP
Name*	Cisco 840 - Standard SIP Non-Secure Profile
Description	Cisco 840 - Standard SIP Non-Secure Profile
Nonce Validity Time*	600
Device Security Mode	Non Secure
Transport Type*	TCP+UDP
Enable Digest Auth	nentication
TFTP Encrypted Co	onfig
Phone Security Prof	ile CAPF Information
Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >
Note: These fields are	related to the CAPF Information settings on the Phone Configuration page.
Parameters used in	Phone
SIP Phone Port [*] 506	0

Phone Security Prof	ile Information
Product Type: Device Protocol:	Cisco 860 SIP
Name*	Cisco 860 - Standard SIP Non-Secure Profile
Description	Cisco 860 - Standard SIP Non-Secure Profile
Nonce Validity Time*	600
Device Security Mode	Non Secure
Transport Type*	TCP+UDP
Enable Digest Auth	nentication
TFTP Encrypted Co	onfig
Phone Security Prof	ile CAPF Information
Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >
Note: These fields are	related to the CAPF Information settings on the Phone Configuration page.
Parameters used in	Phone
SIP Phone Port*	
5060	,

注: UDP はサポートされていないため、トランスポートタイプは TCP + UDP または TCP に設定する必要があります。

SIP プロファイル

Cisco Wireless Phone 840 または 860 を作成する場合は、SIP プロファイルを設定する必要があります。

Cisco Wireless Phone 840 および 860 のカスタム SIP プロファイルを作成することを推奨します(モバイルデ バイスの**標準 SIP プロファイル**または**標準 SIP プロファイル**を使用しないでください)。

Protocol Specific Info	rmation
Packet Capture Mode*	None
Packet Capture Duration	0
SRTP Allowed - Whe provide end to end secu	in this flag is checked, IPSec needs to be configured in the network to irity. Failure to do so will expose keys and other information.
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile	Cisco 860 - Standard SIP Secure Profile
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Custom 860 SIP Profile
Digest User	< None >
Media Termination P	Point Required
Unattended Port	
Require DTMF Recep	ption
Early Offer support 1	for voice and video calls (insert MTP if needed)

Cisco Wireless Phone 840 および 860 の SIP プロファイルを作成するには、**標準 SIP プロファイル**を参照テ ンプレートとして使用します。

標準 SIP プロファイルをコピーし、次のパラメータを変更します。

[レジスタの再送間隔の調整値(秒) (Timer Register Delta (seconds))]: 30 (デフォルトは 5) に設定。

[キープアライブのタイムアウト値(秒) (Timer Keep Alive Expires (seconds))]:

300**(デフォルトは 120)に設定。**

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

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

```
[システム (System)] > [Service Parameters (サービスパラメータ)] > [Cisco CallManager] で SIP ステ
ーションのキープアライブインターバルが 120 秒間設定されたままになっていることを確認します。
```

<u>カスタム SIP プロファイルの例</u>

SIP Profile Information			
Name*	Custom 860 SIP Profile		
Description	Custom 860 SIP Profile		
Default MTP Telephony Event Payload Type*	101		
Early Offer for G.Clear Calls*	Disabled		9
User-Agent and Server header information*	Send Unified CM Version	Information as User-Age	9
Version in User Agent and Server Header st	Major And Minor		9
Dial String Interpretation*	Phone number consists of	of characters 0-9, *, #, ar 🕻	9
Confidential Access Level Headers*	Disabled		9
Redirect by Application			
Disable Early Media on 180			
Outgoing T.38 INVITE include audio mline	2		
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 Ea	arly Offer and Re-invites *	TIAS and AS	0
SDP Transparency Profile		Pass all unknown SDP attri	butes 🗘
Accept Audio Codec Preferences in Received	l Offer*	Default	©
Require SDP Inactive Exchange for Mid-	Call Media Change		
Allow RR/RS bandwidth modifier (RFC 3	556)		
Parameters used in Phone			
Timer Invite Expires (seconds)*	180		
Timer Register Delta (seconds)*	30		
Timer Register Expires (seconds)*	3600		

Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Media Port Ranges	 Common Port Range for Audio and Video
	 Separate Port Ranges for Audio and Video
Start Media Port*	16384

Stop Media Port*	32766	
DSCP for Audio Calls	Use System Default	
DSCP for Video Calls	Use System Default	
DSCP for Audio Portion of Video Calls	Use System Default	
DSCP for TelePresence Calls	Use System Default	
DSCP for Audio Portion of TelePresence Calls	Use System Default	
Call Pickup URI*	x-cisco-serviceuri-pickup	
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup	
Call Pickup Group URI*	x-cisco-serviceuri-gpickup	
Meet Me Service URI*	x-cisco-serviceuri-meetme	
User Info*	None	
DTMF DB Level*	Nominal	
Call Hold Ring Back*	Off	
Anonymous Call Block*	Off	
Caller ID Blocking*	Off	
Do Not Disturb Control*	User	3
Telnet Level for 7940 and 7960 st	Disabled	
Resource Priority Namespace	< None >	3
Timer Keep Alive Expires (seconds) st	300	
Timer Subscribe Expires (seconds) *	300	
Timer Subscribe Delta (seconds) st	15	
Maximum Redirections*	70	
Off Hook To First Digit Timer (milliseconds)*	15000	
Call Forward URI*	x-cisco-serviceuri-cfwdall	
Speed Dial (Abbreviated Dial) ${\sf URI}^{*}$	x-cisco-serviceuri-abbrdial	
Conference Join Enabled		
RFC 2543 Hold		
🗹 Semi Attended Transfer		
Enable VAD		
Stutter Message Waiting		
MLPP User Authorization		
Normalization Script		
Normalization Script < None >	٥	

Enable Trace			
Parameter Name	Parameter Value		
1			
- Incoming Requests FROM URI Settings			
Caller ID DN			
Coller Name			
Trunk Specific Configuration			
Reroute Incoming Request to new Trunk based on *	Never		
Resource Priority Namespace List	< None >		
SIP Rel1XX Options*	Disabled		
Video Call Traffic Class*	Mixed		
Calling Line Identification Presentation st	Default		
Session Refresh Method*	Invite		
Early Offer support for voice and video calls st	Disabled (Default value)		
Enable ANAT			
Deliver Conference Bridge Identifier			
Allow Passthrough of Configured Line Device Call	er Information		
Reject Anonymous Incoming Calls			
Reject Anonymous Outgoing Calls			
Send ILS Learned Destination Route String			
Connect Inbound Call before Playing Queuing An	nouncement		
SIP OPTIONS Ping			
Enable OPTIONS Ping to monitor destination sta	atus for Trunks with Service Type "None (Default)"		
Ping Interval for In-service and Partially In-service	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			

共通設定

Web アクセスなどの一部の設定は、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 Wireless Phone 840 および 860 では、Web アクセスはデフォルトで無効になっています。

共通設定のオーバーライドは、いずれかの設定レベルで有効にできます。

			_
Web Access*	Disabled	\$	

QoS パラメータ

SIP 通信、電話設定、および電話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)	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

G.722 および Opus のアドバタイズメント

Cisco Unified Communications Manager では、G.722 と Opus をコーデック システム全体でサポートするか どうかを設定する機能がサポートされています。

G.722 コーデックと Opus コーデックは、**[G.722 および Opus コーデックのアドバタイズ (Advertise G.722** and Opus Codecs)]を **[無効 (Disabled)**]に設定することで、会社の電話、共通の電話プロファイル、また は個々の電話単位で無効化できます。

Advertise G.722 and	Use System Default	\$
OPUS Codecs*		

オーディオ ビット レート

オーディオビット 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。

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) kbps	 Keep Current Setting Use System Default None 2000 kbps 	Keep Current Setting Use System Default None kbps

音声通話で使用するオーディオ ビット レートを設定するには、次の情報を使用します。

オーディオ コーデック	オーディオ ビ ット レート
Opus	6 ~ 510 Kbps
G.722/G.711	64 Kbps
G.729	8 Kbps

製品固有の設定オプション

Cisco Unified Communications Manager の管理では、次の Cisco Wireless Phone 840 および 860 向け設定 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 Wireless Phone 840 および 860 設定オプション

Product Specific Configuration Layout		
?	Parameter Value	Override Enterprise/Common Phone Profile Settings
Web Access*	Disabled	✓ □
Web Password		
Reboot immediately after downloading software updates *	Disabled	~
Emergency Numbers		_
Visual Voicemail Access*	Disabled	~
Voicemail Server (Primary)		
Voicemail Server (Backup)		
Load Server		
Advertise G.722 and OPUS Codecs*	Use System Default	~
Customer support upload URL		
Secondary SIP Server		
Secondary SIP Server Port		
Secondary SIP Transport*	UDP	~
Secondary SIP Extension		
Secondary SIP Username		
Secondary SIP Password		
Enterprise Mobility Management (EMM) Alternative Configuration		
Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key		
Recording Tone*	Disabled	~
Announce Caller ID*	Disabled	~
Mute SIP Registration Notifications*	Enabled	~
Line 1 Ringtone		
Line 2 Ringtone		
Line 3 Ringtone		
Line 4 Ringtone		
Line 5 Ringtone		
Line 6 Ringtone		
Notification Sound		
Alarm Sound		
Wallpaper		

<u>フィールド名</u>	<u>説明</u>
Web アクセス	電話機が Web ブラウザまたは他の HTTP クライアントからの接続を受 け入れるかどうかを指定します。電話機の Web サーバ機能を無効にする と、電話機の内部 Web ページへのアクセスがブロックされます。これら のページは、統計情報と設定情報を提供します。
Web パスワード(Web Password)	このパラメータは、電話機の Web インターフェイスにアクセスするため のパスワードを指定します。8 ~ 127 文字のパスワードを入力します。
ソフトウェア アップデートをダ ウンロードした直後にリブート します。	このパラメータは、ソフトウェアアップデートをダウンロードした直後 に電話機を再起動するか、手動で再起動するように電話機がユーザーに 通知するかを指定します。ソフトウェアアップデートを適用するには、 電話機を再起動する必要があります。

緊急電話番号	このパラメータは、電話機のキーパッドをロック解除せずにダイヤルで きる緊急電話番号を指定します。たとえば日本では、電話機をロック解 除せずにダイヤルできる緊急電話番号の有力な候補として 110 番が挙げ られます。複数の番号を指定するには、カンマを区切り文字として使用 します。たとえば、411、511、911 などを緊急電話番号として入力する 場合は、フィールドに「411,511,911」とスペースなしで入力します。
ビジュアルボイスメールのア	このパラメータは、ボイスメールへのアクセスを有効または無
クセス	効にします。
ボイスメールサーバー	このパラメータには、ビジュアルボイスメールのプライマリ Voicemail
(プライマリ)	サーバーのアドレスが含まれています。
ボイスメールサーバー	このパラメータには、ビジュアルボイスメールのバックアップ Voicemail
(バックアップ)	サーバーのアドレスが含まれています。
ロード サーバー	電話機が、定義されている TFTP サーバではなく、代替サーバを使用し てファームウェア ロードとアップグレードを取得するように指定しま す。このオプションでは、ファームウェアのアップグレードに使用され るローカル サーバを指定して、特に WAN を介したアップグレードの場 合に、インストール回数を減らすことができます。サーバのホスト名ま たは IP アドレスを入力します (標準の IP アドレス形式を使用しま す)。指定されるサーバは TFTP サービスを実行している必要があり、 TFTP パスにロード ファイルが必要です。ロード ファイルが見つからな い場合、ロードがインストールされません。電話は TFTP サーバにリダ イレクトされません。このフィールドが空白のままの場合、電話は指定 された TFTP サーバを使用してロード ファイルおよびアップグレードを 取得します。
G.722 および Opus コーデック をアドバタイズする	このパラメータは、電話機が G.722 および Opus コーデックをアドバタ イズするかどうかを指定します。コーデックのネゴシエーションでは、 次の 2 つの手順が実行されます。まず、電話機が、サポートされるコー デックを Cisco Unified CallManager にアドバタイズします(すべての エンドポイントが同じコーデックのセットをサポートしているわけでは ありません)。次に、Cisco Unified Communications Manager が、コ ール試行に関与するすべての電話機でサポートされるコーデックのリス トを取得すると、現地のペアリング設定といった各要因を元に、一般に サポートされるコーデックを選択します。オプションは、[システムデフ ォルトの使用(Use System Default)](エンタープライズ パラメータの [G.722 コーデックをアドバタイズ(Advertise G.722 Codecs)]で指定 されている設定に従う)、[無効(Disabled)](G.722 または Opus サ ポートをアドバタイズしない)、および [有効(Enabled)](G.722 お よび Opus サポートをアドバタイズする)です。

カスタマー サポートのアップロ ード URL(Customer support upload URL)	この URL は、ユーザーがエンドポイントで「エラー レポート ツー ル」を実行したときに、問題レポートファイルのアップロードに使 用されます。
セカンダリ SIP サーバー	このパラメータには、オプションの 2 番目の登録用のサーバーのアドレ スが含まれています。
セカンダリ SIP サーバーポート	このパラメータには、オプションの 2 番目の登録用遠端ポート番号が含 まれています。
セカンダリ SIP トランスポート	このパラメータには、オプションの 2 番目の登録用転送タイプが含まれ ています。
セカンダリ SIP 内線	このパラメータには、オプションの 2 番目の SIP 拡張機能が含ま れています。
セカンダリ SIP ユーザー名	このパラメータには、オプションの 2 番目の SIP ユーザー名が含 まれています。
セカンダリ SIP パスワード	このパラメータには、オプションの 2 番目の SIP パスワードが含 まれています。
エンタープライズモビリティ管 理 (EMM) 代替構成	このパラメータは、電話機がエンタープライズモビリティ管理(EMM) ソリューションによって管理されていない場合に、ネイティブ シスコ ア プリケーションを設定するためのファイルを指定します。
エンタープライズモビリティ管 理 (EMM) 代替構成暗号化キー	このパラメータは、エンタープライズモビリティ管理(EMM)代 替コンフィギュレーション ファイルの生成に使用される暗号キー を指定します。
[録音トーン(Recording Tone)]	電話機で録音トーンを有効にするかどうかを設定するために使用で きます。有効の場合、電話機は、すべてのコールの両方向に録音ト ーンを混合します。
発信者番号を通知	このパラメータは、電話機が着信コールの発信者識別情報をアナウンス するかどうかを指定します。
SIP 登録通知のミュート	このパラメータは、SIP 登録イベントの通知をミュートするかどうかを 指定します。
回線 1 の着信音	このパラメータは、回線 1 の呼び出し音を指定します。ダウンロ ードして回線 1 に使用する既存の着信音または着信音ファイルを 指定できます。
回線 2 の着信音	このパラメータは、回線 2 の呼び出し音を指定します。ダウンロ ードして回線 2 に使用する既存の着信音または着信音ファイルを 指定できます。

回線 3 の着信音	このパラメータは、回線 3 の呼び出し音を指定します。ダウンロ ードして回線 3 に使用する既存の着信音または着信音ファイルを 指定できます。
回線 4 の着信音	このパラメータは、回線 4 の呼び出し音を指定します。ダウンロ ードして回線 4 に使用する既存の着信音または着信音ファイルを 指定できます。
回線 5 の着信音	このパラメータは、回線 5 の呼び出し音を指定します。ダウンロ ードして回線 5 に使用する既存の着信音または着信音ファイルを 指定できます。
回線 6 の着信音	このパラメータは、回線 6 の呼び出し音を指定します。ダウンロ ードして回線 6 に使用する既存の着信音または着信音ファイルを 指定できます。
通知音	このパラメータは、ダウンロードする通知サウンドファイルを指定しま す。カンマ区切り形式を使用して複数のファイルを指定できます。ファ イルがダウンロードされたら、カスタム設定アプリケーション、Android 設定、またはその他のアプリケーション設定で通知音を設定する必要が あります。
アラーム音	このパラメータは、ダウンロードするアラームサウンドファイルを指定 します。カンマ区切り形式を使用して複数のファイルを指定できます。 ファイルをダウンロードしたら、カスタム設定アプリケーション、 Android 設定、またはその他のアプリケーション設定でアラーム音を設 定する必要があります。
Wallpaper	このパラメータは、ダウンロードする壁紙ファイルを指定します。カ ンマ区切り形式を使用して複数のファイルを指定できます。ファイル をダウンロードしたら、カスタム設定アプリケーションまたは Android 設定を使用して、ロック画面の壁紙とホーム画面の壁紙を設 定する必要があります。

注:Web パスワードまたはセカンダリ SIP パスワードを長期間有効にしたままにする場合、またはエンタープ ライズ モビリティ管理 (EMM) 代替設定暗号キー オプションを使用する場合は、TFTP 暗号化が有効になって いるセキュア プロファイルを使用する必要があります。

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

これらの機能の詳細については、『**Cisco Wireless Phone 840 and 860 Administration Guide』**または 『Cisco Wireless Phone 840 and 860 Release Notes』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

https://www.cisco.com/c/en/us/support/collaboration-endpoints/webex-wireless-phone/productsrelease-notes-list.html

Webex Calling

Webex はクラウド登録を有効にするため、Cisco Wireless Phone 840 または 860 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 Wireless Phone 840 および 860 は、Webex Calling に登録できるように、ファームウェアバージョン 1.6(0) 以降を実行している必要があります。

webex Control Hub	Q Search		$\Diamond \odot$
G Overview	Overview		
⊘ Getting Started Guide			
	Getting Started Guide	Updates	New offers ····
MONITORING	0 of 7 tasks completed	Update your services to the new	Good news! Boost your users'
In Analytics	View the Getting Started Guide and the	Webex experience. Learn more	with Basic Meetings.
√ Troubleshooting	recommended tasks		Learn more
Reports			
	Webex services ALL ONLINE		Onboarding
MANAGEMENT		Devices	91 T
으 Users	Webex Calling Meetings	88 Total devices	There is no CSV upload within 180 days
悉 Workspaces		Online 6	
Devices	Hybrid Services Control Hub Developer API		- Not Verified 88%
88 Apps		Online with issues 0	- Verified 0%
Account	Room Devices Contact Center	Offline 2	- Active 12%
Organization Settings		•	
SEDVICES		Expired 0	Potential New Users 0
SERVICES		Unknown 76	Review Enable Directory Sync
C Updates & Migrations		Activation 4	
Messaging			
% Calling			Quick links
Connected UC		What's new	Learn more
 Hybrid 		webex + 🔝	= Admin canabilities
		The latest update is here!	Manage subscriptions
			Organization tasks
		Lean nore	Audit log

Cisco Wireless Phone 840 または 860 は、Webex Calling 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 Wireless Phone 840 または 860 は、**[デバイス (Devices)**]を介してユーザが個人的に使用するように 設定できます。

ユーザーのデバイスを追加するには、**[デバイス (Devices)]**に移動し、**[デバイスの追加 (Add Device)]**を 選択します。

次の画面で、[既存のユーザー (Existing User)]を選択し、[次へ (Next)]をクリックします。

webex Control Hub	Q Search	
G Overview	Add Device	\times
⊘ Getting Started Guide	Assign to a user or a workspace?	
	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 recention with a shared phone.	
MONITORING		
🔝 Analytics		
~ Troubleshooting		
Reports	\bigcirc	
MANAGEMENT		
은 Users		
悉 Workspaces	Existing User Workspace Personal Usage Shared Usage	
Devices		
88 Apps		
🛅 Account	Multiple Cisco IP Phones: To bulk activate devices, Import/Upload CSV file.	
Organization Settings		
SERVICES		
C Updates & Migrations		
○ Messaging		
℁ Calling	Cancel	
Se Connected UC		
→ Hybrid		

Cisco Wireless Phone 840 または 860 を割り当てるユーザを検索し、[次へ (Next)]をクリックします。
webex Control H	ub Q Search	
Coverview Cover	Add Device Which user will this device belong to? Or search for another user	
MANAGEMENT A Users Workspaces Devices Apps Account Organization Settings		
SERVICES C Updates & Migrations Messaging Calling Connected UC	Back Next	
 △ Hybrid 		

[Cisco IP 電話 (Cisco IP Phone)]を選択し、ドロップダウンリストから [Cisco 840] または [Cisco 860] を 選択します。

webex Control Hu	Q Search		
G Overview	Add Device		
⊘ Getting Started Guide	What kind of device do you want to set up for this user?		
		[]	
MONITORING			
Malytics			
√ Troubleshooting			
Reports			
MANAGENERIT	Room, Board or Desk series	Cisco IP Phone	
MANAGEMENT	e.g. Cisco Webex Board, Room, and Desk series, and	e.g. Cisco 8845, 8865, 8800 and Analog Telephone	
은 Users	Webex Share.	Adapter ports	
恐 Workspaces		Select Device	
Devices		Select Device	
BB Apps		Select a Device V	
Account	(85)	Cisco 840	
Organization Settings	CH Y	Cisco 860	
SERVICES			
	Webex Go Device	Cisco 8811	
C Updates & Migrations	e.g. iPhone 11 models, iPhone XS, etc. See Compatible	Cisco 8832	
Messaging	uevices	Circo 9941	
℅ Calling		CISCO 804 I	
Seconnected UC		Cisco 8845 Save	
→ Hybrid		Cisco 8851	
		Cisco 8861	

Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

Cisco Wireless Phone 840 または 860 の MAC アドレスを入力し、下のボックスをオンにして、**【保存** (Save)]を選択します。

webex Control Hub	Q Search			
Overview Control Children	Add Device ×			
	What kind of device do you want to set up for this user?			
Alerts center MONTORING Analytics Troubleshooting Reports				
Management A Users	Room, Board or Desk series 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		
悉 Workspaces				
Devices		Select Device		
88 Apps	T Cin	Cisco 860 V		
🛅 Account		Enter MAC Address		
Organization Settings	CH Y	Enter the MAC address of the IP phone you want to add.		
SERVICES	Webex Go Device	*By provisioning this device, you acknowledge that this		
C Updates & Migrations	e.g. iPhone 11 models, iPhone XS, etc. See Compatible	device is Wifi only without any native cellular or location		
O Messaging	devices	services, and as such, you acknowledge that this device's associated 911 location must be maintained		
℅ Calling		manually in Control Hub and that it is your sole		
Se Connected UC		responsibility to maintain the accuracy of the device's location information at all times. You agree that Cisco is		
Hybrid		not responsible for any emergency calls from this device.		
		Back Save		

[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 Wireless Phone 840 または 860 は、[デバイス (Devices)]または [ワークスペース (Workspaces)] を使用してワークスペースとして設定できます。

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

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

webex Control Hu	Q Search	
Overview Getting Started Guide Alerts center	Add Dev Assign to a user or a workspace? Devices for personal usage should be assigned to a specific user. A wo owned by a specific user, such as a meeting room with a Webex Board	rkspace represents a physical location containing a device not 55 or a reception with a shared phone.
al Analytics ≁ Troubleshooting B Reports	Q	(\circ)
MANAGEMENT 요 Users & Workspaces	Existing User Personal Usage	Workspace Shared Usage
Devices Apps Account	Multiple Cisco IP Phones: To bulk activate devices, Import	/Upload CSV file.
Organization Settings services Cludates & Migrations		
Opulates a migrations Messaging Calling Connected UC Dubrid		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。

webex Control Hub		
		×
G Overview	Add De	evice
⊘ Getting Started Guide	Assign to an existing workspace or a new works	pace?
	Select Existing Workspace to assign a device to an existing workspace	e. If you add multiple devices to the same workspace that are not
MONITORING	designed to work together, there may be interference issues. Note the	at there can only be one Cisco IP Phone per workspace.
0. Americaliza		
→ Iroubleshooting	\bigcirc	
E Reports		
MANAGEMENT	V	I
Q Lisers		
A Workspaces	Existing Workspace	New Workspace
	Which Workspace will the device be assigned to	?
The Account	Workspaces containing Cisco IP Phones will not be shown, since you	can only have one of these devices in a workspace.
Account	Search for a Workspace	
Settings		
SERVICES		
C Updates & Migrations		
Messaging		
S Calling		
S Connected UC		
→ Hybrid		
		Back
webex Control Hub	Q Search	
webex Control Hub	Q Search	×
webex Control Hub	Q Search Add De	evice
webex Control Hub ☆ Overview ⊙ Getting Started Guide	Q Search Add De Assign to an existing workspace or a new works	evice ×
Webex Control Hub	Q Search Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace	evice pace? e. If you add multiple devices to the same workspace that are not
Webex Control Hub	Q Search Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the	Evice pace? te. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Hub Control Started Guide Control Alerts center MONITORING Control Alertado	Q Seach Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note the	evice pace? se. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Hub Control Started Guide Control Alerts center MONITORING Control Analytics Control Analytic	Q Search Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note th	evice pace? e. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Overview ⊙ Getting Started Guide Alerts center MONITORING Analytics Troubleshooting Descarts	Q Search Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note th	evice pace? e. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Control Hub Overview Getting Started Guide Alerts center MONTTORING Analytics Troubleshooting Reports	Q Search Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the	evice pace? e. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub G Overview G Getting Started Guide Alerts center MONITORING Analytics Troubleshooting Reports MANAGEMENT	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the	evice pace? se. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Coverview Getting Started Guide Alerts center MONITORING Analytics ~ Troubleshooting Reports MANAGEMENT A Users	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note th	evice pace? se. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Coverview Getting Started Guide Alerts center MONITORING Analytics Troubleshooting Reports MANAGEMENT AUSers A Vorkspaces	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note th Existing Workspace	evice pace? e. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Hub Control Started Guide Control Alerts center MONITORING Control Analytics Control Troubleshooting Control Contro Control	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note th	evice pace? re. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Hub Control Started Guide Control Alerts center MONITORING Control Analytics Troubleshooting Reports MANAGEMENT Control Con	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note th Existing Workspace	evice pace? e. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub O Overview O Getting Started Guide Alerts center MONITORING Analytics Troubleshooting Reports MANAGEMENT Users Workspaces Devices Apps Chaccount	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note the Existing Workspace Existing Workspace	evice pace? Is If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Started Guide Control Hub Controling Started Guide Controling Controlin	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the Existing Workspace Existing Workspace Where will this device be located? What would you like to call the Workspace that this device will be ass Insert name of device location, e.g. 'Recepti	evice pace? Is. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the Existing Workspace Existing Workspace Where will this device be located? What would you like to call the Workspace that this device will be ass Insert name of device location, e.g. 'Recepti	evice pace? The If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Started Guide Control Alerts center MONITORING Alerts center MONITORING Analytics Troubleshooting Reports MANAGEMENT Suborts Devices Apps Contarts Contarts Services Contarts Contarts	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the Existing Workspace Existing Workspace Where will this device be located? What would you like to call the Workspace that this device will be ass Insert name of device location, e.g. 'Recepti	evice pace? Is if you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Started Guide Control Alerts center MONITORING Control Alerts Center MANAGEMENT Control	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note th	evice pace? se. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace.
Webex Control Hub Control Started Guide Control Alerts center MONTORING Control Alerts center MONTORING Control Contro Con	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note the Existing Workspace Where will this device be located? What would you like to call the Workspace that this device will be asso Insert name of device location, e.g. 'Recepti	evice pace? s. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace. New Workspace
Webex Control Hub O Cerview C Getting Started Guide A Alerts center MONITORING A Analytics Troubleshooting Reports MANAGEMENT Users SWorkspaces Devices Apps Account O Organization Settings SERVICES Updates & Migrations Messaging Calling	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspac designed to work together, there may be interference issues. Note the Existing Workspace Where will this device be located? What would you like to call the Workspace that this device will be asso Insert name of device location, e.g. 'Recepti	exice pace? s. If you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace up to the workspace New Workspace
Webex Control Hub O Overview O Getting Started Guide A Alerts center MONITORING A Analytics Troubleshooting Reports MANAGEMENT Users SWorkspaces Devices Apps Account O Organization Settings SERVICES Updates & Migrations Messaging Calling Connected UC	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the	evice pace? Is if you add multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace (we Workspace) igned to?
Webex Control Hub Overview Getting Started Guide Alerts center MONITORING Analytics Troubleshooting Reports MANAGEMENT Devices Apps Account Organization Settings Ubdates & Migrations Messaging Calling Connected UC Hybrid	Add De Assign to an existing workspace or a new works Select Existing Workspace to assign a device to an existing workspace designed to work together, there may be interference issues. Note the Existing Workspace Existing Workspace Where will this device be located? What would you like to call the Workspace that this device will be asson Insert name of device location, e.g. 'Recepti	evice pace? the form and multiple devices to the same workspace that are not at there can only be one Cisco IP Phone per workspace (were workspace) igned to?

[Cisco IP 電話 (Cisco IP Phone)]を選択し、ドロップダウンリストから **[Cisco 840] または [Cisco 860]** を 選択します。



Cisco Wireless Phone 840 または 860 の MAC アドレスを入力し、下のボックスをオンにして、 [次へ (Next)] を選択します。

webex Control Hu	Q Search	
 ☆ Overview ⊘ Getting Started Guide 	Add De What kind of device do you war	vice $ imes$ to set up in this workspace?
 △ Alerts center MONITORING all Analytics ~ Troubleshooting □ Pagents 		
MANAGEMENT	Room, Board or Desk series 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
Workspaces Devices Apps Account Organization Settings	Select Device Cisco 860 V Enter MAC Address Enter the MAC address of the IP phone you want to add.	
SERVICES C Updates & Migrations Messaging C Calling	"By provisioning this device, you acknowledge that this device as such, you acknowledge that this device's associated 911 your sole responsibility to maintain the accuracy of the device responsible for any emergency calls from this device.	e is Wifi only without any native cellular or location services, and location must be maintained manually in Control Hub and that it is e's location information at all times. You agree that Cisco is not Back Next
 Connected UC Hybrid 		

次の画面でロケーション、電話番号、内線番号、および通話プランを設定し、[保存 (Save)]を選択します。

ワークスペースを介して既存の [ワークスペース (Workspaces)]を選択して、サービスを設定また は変更します。

デバイス設定

Cisco Wireless Phone 840 および 860 では、次の設定オプションを使用できます。

Device	Set	tings
--------	-----	-------

Apply the location's default settings or customize the settings for this device. Then resync the device to apply these changes.

 Use the location settings Define custom device settings 		
Q Search	Quarida racional	
Audio Codec Priority 🛈	defaults with custom	
LDAP 🕡	values	\sim
Phone Security Password 🛈		
Web Access ①		^
Set Password 🛈		

Webex Calling のネットワーク要件については、次の URL にある『**Port Reference Information for Webex Calling』**ドキュメントを参照してください。

https://help.webex.com/en-US/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

詳細については、次の URL にある**『Cisco Wireless Phone 840 and 860 Administration Guide』**を参 照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Cisco Wireless Phone 840 および 860

Cisco Wireless Phone 840 および 860 を設定するには、エンタープライズ モビリティ管理 (EMM) アプリケ ーションまたは Cisco Wireless Phone Configuration Management ユーティリティを使用して中央プロビジョ ニングを行うか、ローカル ユーザ インターフェイスを使用して手動で設定します。

エンタープライズ モビリティ管理 (EMM)

管理ツールを使用して Cisco Wireless Phone 840 および 860 の設定を管理し、サードパーティ製アプリケー ションを許可する機能を使用する場合は、エンタープライズ モビリティ管理(EMM)アプリケーションを活用 する必要があります。

エンタープライズ モビリティ管理 (EMM) アプリケーションを介して Cisco Wireless Phone 840 および 860 を手動で設定するには、次のガイドラインを使用します。

起動画面で、ディスプレイをすばやく 6 回タップすると、QR コードをスキャンして、デバイス所有者方式で Cisco Wireless Phone 840 または 860 を EMM に登録できます。



次のアプリケーションは、デバイス所有者方式を使用して電話機を登録するときに、Cisco Wireless Phone 840 および 860 で使用できるように、許可されたアプリケーションとして追加する必要があります。これらの アプリケーションは Google Play ストアで使用できないためです。

- **Cisco Phone** = com.cisco.phone
- Application URLs = com.cisco.appurl
- **Diagnostics** = com.cisco.diagnostics
- **Logging** = com.cisco.logging
- **Port Manager** = com.cisco.portmanager
- System Updater = com.cisco.sysupdater
- UCM Client = com.cisco.ucmclient

cisco Meraki	Q Search Dashboard				
ORGANIZATION	Profiles list / Cisco 860 / Android System Apps				
Cisco 👻	Cisco 860				
NETWORK					
Systems Manager 🛛 👻	နို္င်္ဂိ Profile configuration		Android System Apps 🔹 A	ndroid Android Enterprise	
	Restrictions	×	By default all system apps are disabl	led.	
Systems Manager	💮 meraki-psk	×	List Type	Allowlist v	
Organization	Call Quality Settings settings	×	Allowites	_	
	Barcode settings	×	Allowlist	💮 com.cisco.phone	×
	Buttons settings	×		com.cisco.appurl	×
	জি Web API settings	×		com.cisco.logging	×
	Emergency settings	×		💮 com.cisco.portmanager	×
	Rottony Life settings			💮 com.cisco.sysupdater	×
	Custom Settings settings	×		💮 com.cisco.ucmclient	×
	PTT settings	×			*
	() Android Device Owner	×			
	Contractions	×			
	n Android System Apps	×			
	 Add settings 	_			

以下は、Google Play ストアで入手可能で、デバイス所有者方式を使用して電話機を登録するときにオプション で追加できる、Cisco Wireless Phone 840 および 860 に固有のシスコ アプリケーションのリストです。

- Battery Life = com.cisco.batterylife
- **Buttons** = com.cisco.buttons
- Call Quality Settings = com.cisco.callquality
- Custom Settings = com.cisco.customsettings
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- Sound Stage = com.cisco.soundstage
- Web API = com.cisco.webapi
- Barcode (840s and 860s models only) = com.cisco.barcode.service

必要に応じて、他のアプリケーションを許可できます。

使用する EMM プラットフォームによっては、デバイス所有者方式を使用して電話を登録するときに、Gboard (Google キーボードアプリケーション) も追加する必要がある場合があります)



詳細については、EMM アプリケーションのマニュアルを参照してください。

注: Cisco Wireless Phone 840 および 860 に証明書を一括で自動的に発行する場合は、EMM アプリケーションを使用する必要があります。

シスコワイヤレス電話機構成管理ツール

管理ツールを使用して Cisco Wireless Phone 840 および 860 の設定を管理し、サードパーティ製アプリケー ションを使用できない場合は、Cisco Wireless Phone Configuration Management ユーティリティを使用する ことをお勧めします。

1.5(0) リリースでは、Cisco Wireless Phone Configuration Management ユーティリティ (<u>https://configure.cisco.com</u>) が、Cisco Wireless Phone 840 および 860 電話管理の追加オプションにな りました。

Cisco Wireless Phone Configuration Management ユーティリティにアクセスするには、Cisco.com アカウントが必要です。

注: Cisco Wireless Phone Configuration Management Utility は、Webex Calling に登録されている Cisco Wireless Phone 840 または 860 では現在サポートされていません。

構成ファイルの作成

Cisco Wireless Phone Configuration Management ユーティリティを使用してダウンロード可能な設定ファイ ルを作成するには、**[展開設定 (Deployment Configuration)]**タブに移動し、必要なアプリケーション パラメ ータを設定します。

[エクスポート (Export)]を選択して、ZIP 形式でエクスポートされる設定ファイルを保存します。

<u>アプリケーション設定の構成</u>

ドロップダウンリストから必要なアプリケーションを選択し、必要なパラメータを設定します。

バーコード

バーコード設定を構成するには、ドロップダウンリストから[バーコード (Barcode)]を選択します。

Webex Wireless Phone Configuration Management
Deployment Configuration Initial Provisioning
Choose Application Barcode
Import Export
Enable Barcode Scanner False True
> General (1)
> Data Manipulation (1)
> Custom Intent Settings (1)
> Symbology Settings 🚯
> Replace Control Characters (1)
> ScanFlex (3)
1.9.0.555E Terms and Conditions Privacy Statement Cookie Policy Trademarks

バッテリ寿命

[バッテリ寿命 (Battery Life)]を設定するには、ドロップダウンリストから [バッテリ寿命 (Battery Life)] を選択します。

Webex Wireless Phone Configuration Management		
Deployment Configuration Initial Provisio	oning	
Choose Application 🔲 Battery Life	v	
Import Export		
Enable Battery Monitoring	False True	6
Low Battery Threshold	15% 🗸	8
Vibrate	False True	3
Sound	False True	3
Alarm Tone	Cesium	3
Snooze Time	2 min 🗸	3

ボタン

ボタン設定を構成するには、ドロップダウンリストから**[ボタン (Buttons)]**を選択します。

Webex Wireless Phone C	Configuration Management
Deployment Configuration	Initial Provisioning
Choose Application	Buttons
Import Export	
> Left Button i	
> Right Button i	
> Top Button 🚺	
> Fingerprint Button i	
> Volume up Button i	
> Volume Down Button	9

通話品質設定

[コール品質設定 (Call Quality Settings)]を設定するには、ドロップダウンリストから[コール品質設定 (Call Quality Settings)]を選択します。

ebex Wireless Phone Co	onfiguration Manage	ement	
Deployment Configuration	Initial Provisioning		
Choose Application	Call Quality Settings	~	
Import Export			
Wi-Fi Low RSSI Threshold	_	0	-67 🚯
 Channel Selection (1) 			
✓ Wi-Fi Band Selection (8		
Auto Band Selection	False	True	3
2.4 GHz Wi-Fi Band	False	True	3
5 GHz Wi-Fi Band	False	True	3
> 2.4 GHz: Channels 1 - 13	6		
> 5 GHz 🚯			
> Wi-Fi Preferences i			

Webex Wireless Phone Config	juration Management	
Deployment Configuration Init	ial Provisioning	
Choose Application Call C	Quality Settings	
Import Export		
Wi-Fi Low RSSI Threshold	O	-67 (1)
> Channel Selection 🚯		
∨ Wi-Fi Preferences i		
FT	No Yes	6
ССКМ	No Yes	3
CAC	No Yes	6

注: 1.8(0) リリースでは、**CAC**(コール アドミッション コントロール)を無効にするオプションが有効になっています。

1.9(0) リリースでは、**CAC**(コールアドミッション コントロール)はデフォルトで無効になっており、オプト イン機能になりました。

カスタム設定

[カスタム設定 (Custom Settings)]を設定するには、ドロップダウンリストから [カスタム設定 (Custom Settings)]を選択します。

Webex Wireless Phone Configuration Management
Deployment Configuration Initial Provisioning
Choose Application Custom Settings
Export Export
> User Restrictions (i)
> Time (1)
> Edit Device Name (
> Battery (1)
> Keyboard 🧯
> Sleep (i)
> Display 🚯
> Touch (i)
> Sounds (1)
> Camera (1)
> Wallpaper (i)

デフォルトの着信音は、**[サウンド (Sounds)]**メニューで管理できます。

カスタム着信音をデフォルトの着信音として設定する場合は、通知音の名前を入力し、**[項目の追加** (Add item)]を選択します。

∨ Sounds 🚯	
	Andromeda × Aquila × Argo Navis × Atria × Beat Plucker × Bell Phone × Big Easy × Boötes × Canis Major × Carina × Cassiopeia × Centaurus × Chimey Phone × Cygrus × Digital Phone × Ding × Draco × Dream Theme × Eridani ×
Ringtones	Flutey Phone × Free Flight × Girtab × Growl × Hydra × Insert Coin × Kuma × Lyra × Machina × Mildly Alarming × New Player × Noisey One × Orion × Pegasus × Perseus × Pyxis × Rasalas × Rigel × Scarabaeus × Sceptrum × Solarium × Testudo × Third Eye × Very Alarmed × Vespa × Zeta ×
Default Ringtone	Flutey Phone Chimey Phone Cygnus Digital Phone Ding Draco Dream Theme Eridani Flutey Phone tra ×
	Please e Add item Sallium ×

デフォルトの通知音は、**[サウンド (Sounds)]**メニュー内で管理できます。

カスタム通知音をデフォルトの通知音として設定する場合は、通知音の名前を入力し、**[項目の追加** (Add item)]を選択します。

Default Notification Sound	Pixie Dust 🗸	·	•
	Moonbeam		
	On The Hunt	ep Alarm ×	
		Buzzer Alarm $ imes$	
	Palladium	nium ×	
Alarm Sounds	Pixie Dust	otunium ×	•
	Pizzicato	iezo Alarm $ imes$	
	Plastic Pipe	Rooster Alarm $ imes$	
	Polaris		
Default Alarm Sound	Procyon		
	Please e Add item		U

デフォルトのアラーム音は、[サウンド (Sounds)]メニューで管理できます。

カスタムアラーム音をデフォルトのアラーム音として設定する場合は、アラーム音の名前を入力し、**[項目の追** 加(Add item)]を選択します。

	Argon		
Default Notification Sound	Barium		()
	BeeBeep Alarm	ep Alarm ×	
	Beep-Beep-Beep Alarm	Buzzer Alarm ×	
	Buzzer Alarm	nium ×	
Alarm Sounds	Carbon	atunium ×	3
	Cesium	iezo Alarm ×	
	Fermium	Rooster Alarm ×	
	Please e Add item	_	
Default Alarm Sound	Cesium v		3

[ロック画面の壁紙 (Lock Screen Wallpaper)]と[ホーム画面の壁紙 (Home Screen Wallpaper)]は、 [壁紙 (Wallpaper)]メニュー内で管理できます。

v Wallpaper i	
Lock Screen Wallpaper	3
Home Screen Wallpaper	6

緊急 (Emergency)

緊急設定を構成するには、ドロップダウンリストから[緊急 (Emergency)]を選択します。

Webex Wireless Phone Configuration	Management	
Deployment Configuration Initial Provisi	oning	
Choose Application 🔒 Emergency	V	
Import Export		
Enable Emergency Monitoring	False True	3
No Movement Sensitivity	Disabled V	3
No Movement Timeout (Seconds)	30 ~	3
Tilt Sensitivity	Disabled V	3
Tilt Timeout (Seconds)	10 ~	3
Running Sensitivity	Disabled V	3
Running Timeout (Seconds)	10 ~	3
Snooze Timeout (Seconds)	0 ~	3
Warning Timeout (Seconds)	10 🗸	3
Panic Button	Disabled \vee	6

Panic Button Alarm Timeout (Seconds)	5 ~	3
Panic Button Silent Alarm	False True	6
Emergency Call	False True	3
Emergency Dial Force Speaker	False True	3
Emergency Dial Number	911	3
Warning Tone	Pixie Dust 🗸	6
Alarm Tone	Cesium	3

PTT

PTT 設定を構成するには、ドロップダウンリストから [PTT] を選択します。

Webex Wireless Phone Configuration Management			
Deployment Configuration Initial Provision	ning		
Choose Application	v		
Import Export			
Enable PTT	False True	8	
Allow PTT Transmission when Phone Is Locked	False	6	
Username		6	
Multicast Address	224.0.1.116	6	
Codec	G.726 V	6	
Default Channel UI State	Enabled \vee	6	
PTT Volume UI State	Enabled \vee	6	
Channel 1	ALL	8	
Channel I Can Transmit	False True	6	
Channel 1 Can Subscribe	False 🚺 True	3	

サウンドステージ

[サウンドステージ (Sound Stage)]を設定するには、ドロップダウンリストから**[サウンドステージ (Sound Stage)]**を選択します。



事前設定されたプロファイル(**[標準 (Normal)**]、**[大音量 (Loud)**]、**[ソフト (Soft)**]、**[サイレント** (Silent)])およびカスタムの個人プロファイルは、必要に応じて設定および調整できます。

Normal Profile Alarm Volume		20	•
Normal Profile Alarm Minimum Volume	-0	14	6
Normal Profile Alarm Maximum Volume	O	75	•
Normal Profile Ringer Volume	— 0	20	•
Normal Profile Ringer Minimum Volume	-0	14	6
Normal Profile Ringer Maximum Volume	O	75	•
Normal Profile Media Volume		20	•
Normal Profile Media Minimum Volume	••	7	•
Normal Profile Media Maximum Volume	O	75	•
Normal Profile Call Volume	— O	20	•
Normal Profile Call Minimum Volume	— O	20	•
Normal Profile Call Maximum Volume	O	75	6
Normal Profile Web API Volume		20	6
Normal Profile Web API Minimum Volume	••	7	6
Normal Profile Web API Maximum Volume	O	95	6
Normal Profile PTT Volume		20	6
Normal Profile PTT Minimum Volume		20	•
Normal Profile PTT Maximum Volume	O	85	•
Normal Profile Low Battery Alarm Volume	O	50	•
Normal Profile Low Battery Alarm Minimum Volume	O	50	•
Normal Profile Low Battery Alarm Maximum Volume	O	80	•

その後、特定の条件が満たされたときにプロファイルに切り替えるようにルールを設定できます。

Apply Rule 1	False True	3
Select Profile to Switch for Rule 1	Loud	3
Type for Rule 1	Charging	6
Apply Rule 2	False True	6
Select Profile to Switch for Rule 2	Normal	()
Type for Rule 2	Time	3
Select Time Slot for Rule 2	08:00 AM V	6
Apply Rule 3	False True	3
Select Profile to Switch for Rule 3	Soft V	6
Type for Rule 3	Time	0
Select Time Slot for Rule 3	10:00 AM 🗸	6
Apply Rule 4	False	6
Select Profile to Switch for Rule 4	Personal V	3
Type for Rule 4	Time	3
Select Time Slot for Rule 4	08:00 PM V	3
Apply Rule 5	False True	0
Select Profile to Switch for Rule 5	Silent	8
Type for Rule 5	Time	3
Select Time Slot for Rule 5	12:00 AM V	3

Web API

Web API 設定を構成するには、ドロップダウンリストから [Web API] を選択します。

Webex Wireless Phone Configuration Mc	inagement	
Deployment Configuration Initial Provisionin	ıa	
Choose Application 💮 Web API	\checkmark	
Import Export		
Enable Web API	False True	3
Data Format	XML	3
Polling Username		3
Polling Password	ø	3
Respond Mode	Requester V	3
URL		8
Push Username		6
Push Password	Ø	8
Push Alert Priority	All	•
Server Root URL		3
Enable Notification Ringtone	False True	3
Web API Volume	50	0 🚯
Shortcut Title 1		6
Shortcut URL 1		0
Shortcut Title 2		6
Shortcut URL 2		8
Shortcut Title 3		6
Shortcut URL 3		•



<u>Device Policy Controller アプリケーションの設定</u>

Device Policy Controller は、Cisco Wireless Phone 840 および 860 が Cisco Wireless Phone で管理されてい る場合に、管理者がアプリケーション全体を無効にしたり、Wi-Fi プロファイルパラメータとオプションの電話 ロック解除ピン/パスワードを定義したりできる新しいアプリケーションです。 [設定管理ユーティリティ (Configuration Management Utility)]。

最大 5 つの Wi-Fi プロファイルを設定できます。

次のセキュリティ設定がサポートされています。

[セキュリティモード (Security Mode)]	EAP 方法	フェース 2 認証
なし	該当なし	なし
WPA2-Personal	該当なし	なし
WPA2-Enterprise	PEAP	GTC、MSCHAPV2
WPA2-Enterprise	TTLS	GTC、MSCHAP、MSCHAPV2、PAP

注: Cisco Wireless Phone Configuration Management Utility は、EAP-TLS (TLS) をサポートしていません。

オープン Wi-Fi ネットワークに接続するには、SSID を入力し、[セキュリティ (Security)]を[なし (None)]に設定します。

Webex Wireless Phone Configuration Mar	nagement	
Deployment Configuration Initial Provisioning	3	
Choose Application Ovice Policy Contro	oller v	
Import Export		
✓ Wi-Fi Profile (i)		
Wi-Fi Profile •		
Security	None	6
* SSID		6
Hidden SSID	False True	6
Phone Unlock Pin/password		ø

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

Vebex Wireless Phone Configuration Mc	anagement		
Deployment Configuration Initial Provisionir	ng		
Choose Application () Device Policy Contr	roller v		
Import Export			
✓ Wi-Fi Profile i			
Wi-Fi Profile i			
Security	WPA2-Personal		• ()
* SSID			8
* Password		Ø	6
Hidden SSID	False True		3
Phone Unlock Pin/password		Ø	3

EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)]を [WPA2-EAP] に設定してから、[認証方式 (Authentication method)]を選択します。

PEAP または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、フェーズ2認証方式を選択し、必要 に応じてヘッダーとフッターを除いた Base-64 (PEM) エンコーディング形式で CA 証明書を設定し、ID とパ スワードを入力します。

pyment Configuration Initial Pr	ovisioning	
oose Application 💿 Device Pol	icy Controller 🗸 🗸	
Import Export		
Wi-Fi Profile 🧯		
∕i-Fi Profile ● 🚺		
• •		
ecurity	WPA2-Enterprise V	• (1)
SSID		3
Password		Ø
idden SSID	False	6
✓ WPA2-Enterprise Parameters 3		
EAP Method	PEAP	0
Phase 2 Authentication	MSCHAPV2 V	0
Domain		6
* Identity		6
Anonymous Identity		6
CA Certificate		<i>(</i>)
	Select CA Certificate	

注: ブロードキャストされていない Wi-Fi ネットワークは、非表示の SSID として設定する必要があります。 それ以外の場合、Wi-Fi ネットワークは範囲内にないと表示されます。非ブロードキャスト Wi-Fi ネットワーク に接続するには、[非表示 SSID (Hidden SSID)]を[はい (True)]に設定します。

設定された Wi-Fi ネットワークが Cisco Unified Communications Manager を指していることを確認します。 それ以外の場合は、Cisco Wireless Phone 840 および 860 の電話アプリケーションで TFTP サーバーを手動で 設定する必要があります。

ヘッダーとフッターが削除され、スペースや改行が含まれていない CA 証明書の形式が正しいことを 確認します。

次のアプリケーションはデフォルトで許可されません。ただし、無効化されたアプリケーションのリスト は、必要に応じてさらに設定できます。

- **Chrome** = com.android.chrome
- Digital Wellbeing = com.google.android.apps.wellbeing
- Google = com.google.android.googlequicksearchbox
- Google TV = com.google.android.videos
- Maps = com.google.android.apps.maps
- **Photos** = com.google.android.apps.photos
- Play Store = com.android.vending
- Sound Recorder = com.android.soundrecorder
- **YouTube** = com.google.android.youtube

novment Configuration Initial Pro	visioning
	, , , , , , , , , , , , , , , , , , ,
Choose Application 💿 Device Polic	cy Controller 🗸 🗸
Import Export	
> Wi-Fi Profile i	
hone Unlock Pin/password	Ø
	com.google.android.youtube \times
	com.google.android.googlequicksearchbox \times
	com.android.soundrecorder ×
nisallow These Apps	com.google.android.apps.wellbeing ×
	com.google.android.videos ×
	com.google.android.apps.photos ×
	com.android.vending × com.android.chrome ×

注: 重要なアプリケーションが Device Policy Controller の設定で許可されていないことを確認してください。

- Smart Launcher = com.cisco.smartlauncher
- Device Policy Controller = com.cisco.devicepolicycontroller
- **Cisco Phone** = com.cisco.phone
- Application URLs = com.cisco.appurl
- Logging = com.cisco.logging
- **Port Manager** = com.cisco.portmanager
- System Updater = com.cisco.sysupdater
- UCM Client = com.cisco.ucmclient
- Web API = com.cisco.webapi
- Settings = com.android.settings

スマート ランチャ アプリケーションの設定

スマート ランチャは、Cisco Wireless Phone 840 および 860 が Cisco Wireless Phone Configuration Management Utility によって管理されている場合に、エンド ユーザがアクセスできるアプリケーションを制限 する新しいアプリケーションです。

次のアプリケーションは、デフォルトでスマートランチャービューに表示されるようになっています。ただし、 許可されたアプリケーションのリストは、必要に応じてさらに設定できます。

- **Cisco Phone** = com.cisco.phone
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- Web API = com.cisco.webapi
- Webex = com.cisco.wx2.android

Webex Wireless Phone Configuration Manc	igement
Deployment Configuration Initial Provisioning	
Choose Application 😡 Smart Launcher	~
Import Export	
	com.cisco.phone × com.cisco.ptt ×
Set Allow-List of Applications	com.cisco.emergency × com.cisco.webapi ×
	com.cisco.wx2.android × + New Tag
Set Title of Launcher Application	Smart Launcher

以下は、Cisco Wireless Phone 840 および 860 にプレインストールされているアプリケーションのリストです。 これらのアプリケーションを許可しない場合は、Device Policy Controller の設定に追加するか(**【設定**

(Settings)]アプリケーションを除く)、スマートランチャーの設定に追加して、スマート ランチャー ビュー からアクセスできるようにする必要があります。

シスコのプリインストール アプリケーション

- **Barcode** = com.cisco.barcode.service
- Battery Life = com.cisco.batterylife
- Buttons = com.cisco.buttons
- Call Quality Settings = com.cisco.callquality
- **Custom Settings** = com.cisco.customsettings
- **Diagnostics** = com.cisco.diagnostics
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- Sound Stage = com.cisco.soundstage
- Web API = com.cisco.webapi
- Webex = com.cisco.wx2.android

<u>その他のプリインストールされたアプリケーション</u>

- Calculator = com.google.android.calculator
- Calendar = com.google.android.calendar
- **Camera** = com.android.camera2
- Chrome = com.android.chrome
- **Clock** = com.android.deskclock
- Contacts = com.google.android.contacts

- Digital Wellbeing = com.google.android.apps.wellbeing
- **Drive** = com.google.android.apps.docs
- **Duo** = com.google.android.apps.tachyon
- Files = com.google.android.documentsui
- **Gmail** = com.google.android.gm
- **Google** = com.google.android.googlequicksearchbox
- Google TV = com.google.android.videos
- Keep Notes = com.google.android.keep
- **Maps** = com.google.android.apps.maps
- Photos = com.google.android.apps.photos
- Play Store = com.android.vending
- Settings = com.android.settings
- Sound Recorder = com.android.soundrecorder
- YouTube = com.google.android.youtube
- **YT Music** = com.google.android.apps.youtube.music

注: スマートランチャーは、Cisco Phone アプリケーションのみを許可することで、電話専用モードに設定できます。

設定アプリケーションとその他の重要なアプリケーションが Device Policy Controller の設定で許可されていないことを確認します。

コンフィギュレーションファイルのエクスポート

必要なアプリケーション設定の変更がすべて完了し、設定を保存する準備ができたら、[エクスポート (Export)]を選択します。

変更内容を確認するための確認画面が表示されます。

ファイルを保護するには、**[エクスポート (Export)**]を選択する前に、**[設定の暗号化 (Encrypt Configuration)**]がオンになっていることを確認します(デフォルト設定)。

変更が確認されたら、**[エクスポート (Export)**]を選択します。



設定ファイルは、次のファイルを含む ZIP 形式(CP8x0_config_6-8-2023.zip など)でエクスポー トされます。

• **CP8x0_config_<MM-DD-YYYY>.json.enc**= Cisco Unified Communications Manager にアップロー ドされる暗号化された設定ファイル

Х

• CP8x0_key_<MM-DD-YYYY.txt= Encryption key used to encrypt the config file

複数のファイルが Cisco Unified Communications Manager にアップロードされる場合は、必要に応じて CP8x0_config_<MM-DD-YYYY>.json.enc ファイルの名前を変更できます。

注: 暗号化されていない設定オプションは、トラブルシューティング専用です。

Import Configuration Files

以前にエクスポートした ZIP ファイルを使用して追加の設定変更を行う場合は、【インポート(Import)】 を選択します。

保存した ZIP ファイルを **[インポート設定 (Import Configuration)**] ウィンドウにドラッグし、**[インポート** (Import)]を選択します。

The Import Configuration upload allows you to upload a zip file containing configuration parameters and values exported from this tool using the export functionality.



Import

Х

注: 以前に保存した ZIP ファイルが変更されていないことを確認します。

ZIP ファイルの名前は変更できますが、インポートが失敗するため、内部ファイルを変更することはできません。

Cisco Unified Communications Manager の設定

Cisco Wireless Phone Configuration Management ユーティリティを使用するように Cisco Unified Communications Manager を設定するには、次のガイドラインを使用します。

TFTP 暗号化を使用したセキュア プロファイルの作成

Cisco Wireless Phone Configuration Management ユーティリティからエクスポートされたファイルをホスト するように Cisco Unified Communications Manager を設定する前に、TFTP 暗号化が有効になっているセキュ リティプロファイルを使用するように Cisco Wireless Phone 840 および 860 を設定する必要があります。 Cisco 無線電話 840 および 860 をクリア テキストで入力します。

Phone Security Prof	ile Information	
Product Type:	Cisco 840	
Device Protocol:	SIP	
Name*	Cisco 840 - Standard SIP Secure Profile	
Description	Cisco 840 - Standard SIP Secure Profile	
Nonce Validity Time*	600	
Device Security Mode	Encrypted	•
Transport Type*	TLS	•
🗌 Enable Digest Aut	hentication	
TFTP Encrypted C	onfig	
Phone Security Prof	ile Information	
Phone Security Prof Product Type:	ile Information	
Phone Security Prof Product Type: Device Protocol:	ile Information Cisco 860 SIP	
Phone Security Prof Product Type: Device Protocol: Name*	ile Information Cisco 860 SIP Cisco 860 - Standard SIP Secure Profile	
Phone Security Prof Product Type: Device Protocol: Name* Description	Ile Information Cisco 860 SIP Cisco 860 - Standard SIP Secure Profile Cisco 860 - Standard SIP Secure Profile	
Phone Security Prof Product Type: Device Protocol: Name* Description Nonce Validity Time*	Ile Information Cisco 860 SIP Cisco 860 - Standard SIP Secure Profile Cisco 860 - Standard SIP Secure Profile 600	
- Phone Security Prof Product Type: Device Protocol: Name* Description Nonce Validity Time* Device Security Mode	Ile Information Cisco 860 SIP Cisco 860 - Standard SIP Secure Profile Cisco 860 - Standard SIP Secure Profile 600 Encrypted	
- Phone Security Prof Product Type: Device Protocol: Name* Description Nonce Validity Time* Device Security Mode Transport Type*	Ile Information Cisco 860 SIP Cisco 860 - Standard SIP Secure Profile Cisco 860 - Standard SIP Secure Profile 600 Encrypted v TLS v	
Phone Security Prof Product Type: Device Protocol: Name* Description Nonce Validity Time* Device Security Mode Transport Type* Enable Digest Auth	Ile Information Cisco 860 SIP Cisco 860 - Standard SIP Secure Profile Cisco 860 - Standard SIP Secure Profile 600 Encrypted v TLS v mentication	

セキュリティ プロファイルを作成したら、そのプロファイルを Cisco Wireless Phone 840 および 860 に適用 して、Cisco Wireless Phone 840 および 860 の設定ファイルの TFTP 暗号化を有効にする必要があります。

[デバイスセキュリティプロファイル (Device Security Profile)]ドロップダウン メニューから設定済みのセ キュリティ プロファイルを選択します。
Protocol Specific Information		
Packet Capture Mode*	None	•
Packet Capture Duration	0	_
SRTP Allowed - When this flag security. Failure to do so will expo	is checked, IPSec needs to be configured in the netwo see keys and other information.	ork to provide end to end
BLF Presence Group*	Standard Presence group	•
MTP Preferred Originating Codec *	711ulaw	•
Device Security Profile*	Cisco 840 - Standard SIP Secure Profile	•
Rerouting Calling Search Space	< None >	•
SUBSCRIBE Calling Search Space	< None >	•
SIP Profile*	Custom 840 SIP Profile	View Details
Digest User	< None >	•
Media Termination Point Requ	ired	
Unattended Port		
Require DTMF Reception		
Early Offer support for voice a	and video calls (insert MTP if needed)	
Protocol Specific Information		
Protocol Specific Information Packet Capture Mode*	None	
Protocol Specific Information Packet Capture Mode* Packet Capture Duration	None 0	v]
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp	None 0 g is checked, IPSec needs to be configured in the network to be configured in the network to be configured in the network to be keys and other information.	v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will expe BLF Presence Group*	None 0 g is checked, IPSec needs to be configured in the network of the second	v pork to provide end to end
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp BLF Presence Group* MTP Preferred Originating Codec	None 0 g is checked, IPSec needs to be configured in the network ose keys and other information. Standard Presence group 711ulaw	v i ork to provide end to end v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp BLF Presence Group* MTP Preferred Originating Codec * Device Security Profile*	None 0 g is checked, IPSec needs to be configured in the network with the network with the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile	v provide end to end v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp BLF Presence Group* MTP Preferred Originating Codec Device Security Profile* Rerouting Calling Search Space	None 0 g is checked, IPSec needs to be configured in the network on the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None >	v vork to provide end to end v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will expi BLF Presence Group* MTP Preferred Originating Codec Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space	None 0 g is checked, IPSec needs to be configured in the network between the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None > < None >	v ork to provide end to end v v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp BLF Presence Group* MTP Preferred Originating Codec * Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile*	None 0 g is checked, IPSec needs to be configured in the network on the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None > < None > Custom 860 SIP Profile	v v v v v v v v v v v v v v v v v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp BLF Presence Group* MTP Preferred Originating Codec Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User	None 0 g is checked, IPSec needs to be configured in the network of the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None > < None > Custom 860 SIP Profile < None >	v v v v v v v v v v v v v v v v v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will expi BLF Presence Group* MTP Preferred Originating Codec Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User Media Termination Point Reque	None 0 g is checked, IPSec needs to be configured in the network of the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None > < None > Custom 860 SIP Profile < None > irred	v v v v v v v v v v v v v v v v v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will expe BLF Presence Group* MTP Preferred Originating Codec Terret Originating Codec BUBSCRIBE Calling Search Space SIP Profile* Digest User Media Termination Point Require Unattended Port	None 0 g is checked, IPSec needs to be configured in the network on the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None > < None > Custom 860 SIP Profile < None > irred	v v v v v v v v v v v v v v v v v v v
Protocol Specific Information Packet Capture Mode* Packet Capture Duration SRTP Allowed - When this flag security. Failure to do so will exp BLF Presence Group* MTP Preferred Originating Codec Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User Unattended Port Require DTMF Reception	None 0 g is checked, IPSec needs to be configured in the network on the information. Standard Presence group 711ulaw Cisco 860 - Standard SIP Secure Profile < None > < None > Custom 860 SIP Profile < None > irred	v v v v v v v v v v v v v v v v v v v

Upload Configuration Files

ダウンロードした暗号化 ZIP ファイルから **CP8x0_config_json.enc** ファイルを抽出し、[Cisco Unified OS の 管理 (Cisco Unified OS Administration)] ページから TFTP サービスを実行しているすべての Cisco Unified Communications Manager ノードにファイルをアップロードします。**<MM-DD-YYYY>**次に、すべてのノード の TFTP サービスを再起動します。

必要に応じて、Cisco Unified Communications Manager の **[サーバーのロード (Load Server)**] オプション を使用して、設定ファイルをホストできます。

注:CP8x0_config_<MM-DD-YYYY>.json.enc ファイルは、複数のファイルが Cisco Unified Communications Manager にアップロードされる場合に備えて、必要に応じて名前を変更できます。

<u>Cisco Wireless Phone 840 および 860 製品固有の設定オプションの設定</u>

Cisco Wireless Phone 840 および 860 は、ダウンロードするファイルと、ファイルの復号に使用する暗号キー を通知するように設定する必要があります。

エンタープライズ モビリティ管理 (EMM) 代替設定製品固有の設定オプションを、抽出したファイルの名 前(例:CP8x0_config_<MM-DD-YYYY>.json.enc またはファイルの名前が変更された名前)を使用し て設定します。

エンタープライズ モビリティ管理 (EMM) 代替構成暗号化キーの製品固有の設定オプションを、抽出したファ イル (**CP8x0_key_<MM-DD-YYYY.txt**)を使用して設定します。

Enterprise Mobility Management (EMM) Alternative Configuration	
Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key	

電話ロック解除パスワードの設定

[電話ロック解除パスワード (Local Phone Unlock Password)] (デフォルト = **#) は、スマートランチ ャーを終了し、標準の Android インターフェイスにアクセスするために使用できます。 **[Device (デバイ ス)] > [Device Settings (デバイス設定)] > [Common Phone Profile (共通の電話プロファイル)]**の [Common Phone Profile (共通の電話プロファイル)]で [電話ロック解除パスワード (Local Phone Unlock Password)]を設定し、Cisco Wireless Phone 840 および 860 に適用することをお勧めします。

Common Phone Profile Inf	ormation	
Name*	Standard Common Phone Profile	
Description	Standard Common Phone Profile	
Local Phone Unlock Password		
DND Option*	Ringer Off	•
DND Incoming Call Alert*	Beep Only	•
Feature Control Policy	< None >	·)
Wi-Fi Hotspot Profile	< None >	View Details
Enable End User Access to	Phone Background Image Setting	

Cisco Wireless Phone 840 および 860 の登録

Cisco Wireless Phone Configuration Management ユーティリティを使用するには、最初に Cisco Wireless Phone 840 および 860 をファームウェア 1.5(0) 以降にアップグレードする必要があります。

Cisco Wireless Phone 840 および 860 を 1.5(0) 以降にアップグレードしたら、[設定 (Settings)]、[システム (System)]、[詳細 (Advanced)]、[オプションのリセット (Reset options)]、[すべてのデータの消去 (工 場出荷時のリセット) (Erase all data (factory reset))]の順に選択して、工場出荷時の状態にリセットする必要 があります。 **注**: Cisco Wireless Phone 840 および 860 が Cisco Wireless Phone Configuration Management ユー ティリティに登録されると、 は電話機を工場出荷時の状態にリセットすることなく、後続の更新をプッシ ュできます。

起動画面で、ディスプレイをすばやく 6 回タップすると、QR コードをスキャンして Cisco Wireless Phone 840 または 860 を Cisco Wireless Phone Configuration Management ユーティリティに登録するように求 められます。



Cisco Wireless Phone Configuration Management ユーティリティの [初期プロビジョニング (Initial **Provisioning**)] タブで、初期プロビジョニングに使用する Wi-Fi ネットワーク パラメータとオプション の電話ロック解除ピン/パスワードを設定します。

次のセキュリティ設定がサポートされています。

[セキュリティモード (Security Mode)]	EAP 方法	フェース2認証
なし	該当なし	なし
WPA2-Personal	該当なし	なし
WPA2-Enterprise	PEAP	GTC、MSCHAPV2
WPA2-Enterprise	TTLS	GTC、MSCHAP、MSCHAPV2、PAP

注: Cisco Wireless Phone Configuration Management Utility は、EAP-TLS (TLS) をサポートしてい ません。

オープン Wi-Fi ネットワークに接続するには、SSID を入力し、[セキュリティ (Security)]を[なし (None)]に設定します。

Webex Wireless Phone Con	figuration M	lanagement	
Deployment Configuration	Initial Provisioni	ing	
Scan 'n' Go Provisioning			
Wi-Fi Configuration			
	Security:	None	
	* SSID:		
	Hidden SSID:		
Security			
Phone Unloc	k Pin/Password:	Ø	
Generate			

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

Webex Wireless Phone Configuration N	lanagement
Deployment Configuration Initial Provision	ning
Scan 'n' Go Provisioning	
Wi-Fi Configuration	
Security:	WPA2-Personal V
* SSID:	
* Password:	Ø
Hidden SSID:	
Security	
Phone Unlock Pin/Password:	ø
Generate	

EAP 対応の Wi-Fi ネットワークに接続するには、**ネットワーク名**を入力し、**[セキュリティ (Security)**]を **[WPA2-EAP]** に設定してから、**[認証方式 (Authentication method)**]を選択します。

PEAP または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、フェーズ 2 認証方式を選択し、必要 に応じてヘッダーとフッターを除いた Base-64 (PEM) エンコーディング形式で CA 証明書を設定し、ID とパ スワードを入力します。

ebex Wireless Phone Configura	ation Mana	agement
eployment Configuration Initial Pr	rovisioning	
Scan 'n' Go Provisioning		
Wi-Fi Configuration		
	Security:	WPA2-Enterprise V
	* SSID:	
	* Password:	ø
	lidden SSID :	
0		
Security Phone Unlock Pin	n/Password:	ø
FAP Configuration		
E	AP Method:	PEAP V
Phase 2 Auth	nentication:	MSCHAPV2 V
	Domain	
	Domain.	
	* Identity:	
Anonymo	ous Identity:	
CA	Certificate:	
		li.
		Select CA Certificate
Generate		

注: ブロードキャストされていない Wi-Fi ネットワークは、非表示の SSID として設定する必要があります。 それ以外の場合、Wi-Fi ネットワークは範囲内にないと表示されます。非ブロードキャスト Wi-Fi ネットワーク に接続するには、[非表示 SSID (Hidden SSID)]を[はい (True)]に設定します。

設定された Wi-Fi ネットワークが、DHCP オプション 150 または DHCP オプション 66 を介して Cisco Unified Communications Manager を指していることを確認します。それ以外の場合は、Cisco Wireless Phone 840 および 860 の電話アプリケーションで TFTP サーバーを手動で設定する必要があります。

ヘッダーとフッターが削除され、スペースや改行が含まれていない CA 証明書の形式が正しいこと を確認します。

[生成 (Generate)]を選択して QR コードを作成すると、QR コードが表示されます。

QR Code

Scan this QR code on your Webex wireless phone device by tapping six times on the "Hi there" text on the Welcome screen



Done

注: QR コードを正常に生成するには、CA 証明書の文字を含む合計文字数が 2041 文字を超えないようにする 必要があります。

Cisco Wireless Phone 840 または 860 で QR コードをスキャンします。

Cisco Wireless Phone 840 または 860 が近くにない場合に備えて、QR コードを保存できます。その場合は、 QR コードを PDF ファイルまたはスクリーンショットとして保存することをお勧めします。PNG ファイルとし てファイルを保存するとファイルが変更され、QR コードのスキャンが失敗します。

Cisco Wireless Phone 840 および 860 は、指定されたファイルを Cisco Unified Communications Manager からダウンロードし、それに応じてアプリケーションとその他の設定を更新しようとします。



注: Cisco Wireless Phone 840 および 860 は、設定された Wi-Fi ネットワークの範囲内にある必要があります。 範囲内にない場合、セットアップは失敗します。

手動設定

ローカル ユーザ インターフェイスを介して Cisco Wireless Phone 840 および 860 を手動で設定するには、次のガイドラインを使用します。

Wi-Fi プロファイルの設定

ローカル ユーザー インターフェイスを介して Wi-Fi ネットワークを手動で設定するには、次のガイドラインを 使用します。

- 初期状態の電話機または工場出荷時の状態にリセットされた電話機の場合は、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するか、【オフラインでセットアップ (Set up offline)】を選択します。
- 構成オプションは、ブロードキャストされた Wi-Fi ネットワークが構成されているか、Wi-Fi ネットワ ークが手動で構成されているかによって決まります。
- 次に、サポートされる利用可能なセキュリティモードと、各モードで使用できるキー管理および暗号化タイプを示します。

[セキュリティモード (Security Mode)]	EAP 方法	キーの管理	暗号化
なし	該当なし	なし	なし
WPA2-Personal	該当なし	WPA2	AES
WPA2-Enterprise	PEAP	WPA2	AES
WPA2-Enterprise	TLS	WPA2	AES
WPA2-Enterprise	TTLS	WPA2	AES

ブロードキャスト Wi-Fi ネットワークの設定

- Wi-Fi ネットワークがブロードキャストされている場合は、スタートアップウィザー経由でリストから
 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。
- ブロードキャスト Wi-Fi ネットワークを(スタートアップウィザードを使用せずに)オフラインで設定 する場合は、電話機のディスプレイを下から上にスワイプして、インストールされているアプリケーションを表示し、【設定(Settings)]>[ネットワークとインターネット(Network and Internet)]>
 [Wi-Fi]を選択して Wi-Fi ネットワークを設定します。。

11:03 🕻	¢ m ♥	\Diamond
	¢	
	Connect to Wi-Fi	
	meraki-eap	
	meraki-psk	
	MySpectrumWiFi77-2G	
	MySpectrumWiFi77-5G	
	TP-Link_6205	
	TP-Link_6205_5G	
V A	DIRECT-79-HP ENVY 7640 series	
	< • •	

・ オープン Wi-Fi ネットワークに接続するには、Wi-Fi ネットワーク名をクリックするだけです。

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

11:09 🖪 🗢 🖬 🕈 🤍 🗘 🗘
?
meraki-psk
Password ::::
Show password
Advanced options V
Cancel Connect
TP-Link_6205_5G
Selieve-n-Hope
< ● ■

- 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、[EAP 方式] を選択します。
- PEAP または EAP-TTLS (TTLS) の Wi-Fi ネットワークを設定する場合は、使用するフェーズ2認証方 式と CA 証明書オプションを選択し、ID とパスワードを入力します。
- EAP-TLS (TLS) Wi-Fi ネットワークを設定する場合は、使用する [ユーザー証明書 (User certificate)]および [CA 証明書 (CA certificate)] オプションを選択します。

			v I
meraki-eap			I
EAP method			I
PEAP		-	
TLS			I
TTLS		*	I
Please select		-	I
Identity			I
Anonymous identity	1		ł
Password			
	Cancel	Connect	
•	•	•	
dualmode			
dualmode meraki-eap			
dualmode meraki-eap			
e dualmode meraki-eap EAP method PEAP		Ţ	
ear auaimode meraki-eap EAP method PEAP Phase 2 authentica	tion	Ţ	\Diamond
EAP method PEAP Phase 2 authentica MSCHAPV2	tion	•	
Caracteristicate	tion	•	
Caracteristical electronic electr	tion	•	
CA certificate Please select Identity	tion	•	
Caracteristical and a select and a select a sele	tion	•	
auaimode meraki-eap EAP method PEAP Phase 2 authentica MSCHAPV2 CA certificate Please select Identity Anonymous identity	tion ,	•	
auaimode meraki-eap EAP method PEAP Phase 2 authentica MSCHAPV2 CA certificate Please select Identity Anonymous identity Password	tion Y	•	

PEAP		~
Phase 2 authentica	ition	
MSCHAPV2		-
GTC		
Please select		-
Identity		
Anonymous identit	у	
Password		
	Cancel	

11 🖪 🏟 🕑 👩 dualmode	-	<
meraki-eap		
EAP method		
PEAP		-
Phase 2 authenticat	ion	
MSCHAPV2		-
CA certificate		_
Please select		•
Use system certif	icates	
Do not validate		11
,		- 1
Password		
	Cancel	Connect

meraki-eap		m	neraki-eap		meraki-eap
EAP method		EA	AP method		EAP method
TTLS	·	1	TLS	-	TTLS
Phase 2 authenticatio	on	Ph	nase 2 authentication		Phase 2 authenti
PAP	.	PA	AP	-	PAP
CA certificate		м	SCHAP		CA certificate
Please select	-				 Please select
Identity		M	SCHAPV2		Use system ce
		G	тс		
Anonymous identity		An	nonymous identity		Do not validate
Password		Pa	assword	- 1	Password
				_	
	Cancel Connect		Cancel	Connect	
 <!--</th--><th>Cancel Connect</th><th>11:22</th><th>Cancel</th><th></th><th>4</th>	Cancel Connect	11:22	Cancel		4
I ↔ ■ ♥ meraki-eap	Cancel Connect	11:22 E	Cancel		4
	Cancel Connect	11:22 E EA	Cancel		•
■	Cancel Connect	11:22 E M EA TL	Cancel		•
	Cancel Connect	11:22 E M EA TL CA	Cancel		•
	Cancel Connect	11:22 m EA TL CA PI	Cancel	Connect	•
EAP method TLS CA certificate Please select User certificate	Cancel Connect	11:22 = m EA TL CA PI	Cancel	Connect	•
 CA certificate Please select User certificate Do not provide 	Cancel Connect	11:22 m EA TL CA PI	Cancel	Connect	•
Reraki-eap EAP method TLS CA certificate Please select User certificate Do not provide Identity	Cancel Connect	11:22 = m EA TL CA PI US DO	Cancel	Connect	•
 meraki-eap EAP method TLS CA certificate Please select User certificate Do not provide Identity 	Cancel Connect	11:22 m EA TL CA Pl Us DC	Cancel	Connect	
 CA certificate Please select User certificate Do not provide Identity Advanced options 	Cancel Connect	11:22 = m EA TL CA Pl Us DC	Cancel	Connect	
EAP method TLS CA certificate Please select User certificate Do not provide Identity	Cancel Connect	11:22 = m EA TL CA Pl Us DC	Cancel	Connect	

 \Diamond 1

Cancel Conr

非ブロードキャスト Wi-Fi ネットワークの設定

- ・ 非ブロードキャスト(非表示)Wi-Fiネットワークを手動で設定する場合は、電話機のディスプレイを 下から上にスワイプして、インストールされているアプリケーションを表示し、【設定(Settings)]>
 【ネットワークとインターネット(Network and Internet)]>[Wi-Fi]を選択します。
- Wi-Fi 設定の一番下で、【ネットワークの追加(Add Network)】を選択し、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。
- ブロードキャストされていない Wi-Fi ネットワークは、Wi-Fi ネットワーク設定の [詳細オプション (Advanced options)] セクションで非表示ネットワークとしてマークする必要もあります。それ以外の場合、Wi-Fi ネットワークは範囲内にないと表示されます。



オープン Wi-Fi ネットワークに接続するには、**ネットワーク名**を入力し、**[セキュリティ (Security)**] を**[なし (None)**]に設定します。

9:11 🖪 🌣 🖬 🗘		
← Add network		
Network name		
Enter the SSID		84
Security		
None		•
Advanced options		~
	CANCEL	
•		

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

9:15 🖪 🌣 🗘	\bigcirc
← Add network	
Network name	
Enter the SSID	819
Security	
WPA2-Personal	*
Password	
Show password	
Advanced options	~
CAN	CEL SAVE
•	

 EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、【セキュリティ (Security)】を [WPA2-企業(WPA2-Enterprise)】に設定してから、[EAP 方式(EAP method)】 を選択します。

- PEAP または EAP-TTLS (TTLS) の Wi-Fi ネットワークを設定する場合は、使用するフェーズ2認証方 式と CA 証明書オプションを選択し、ID とパスワードを入力します。
- EAP-TLS (TLS) Wi-Fi ネットワークを設定する場合は、使用する[ユーザー証明書 (User certificate)]および[CA 証明書 (CA certificate)]オプションを選択します。

9:15 🖪 🌣 🗘		\bigtriangledown
← Add network		
Network name		
Enter the SSID		
Security		
WPA2-Enterprise		*
EAP method		
PEAP		*
TLS		
TTLS		*
or continuate		
Please select		*
Identity		
	CANCEL	
۰ ا		
9:15 🖪 🌣 🗘		\bigtriangledown
9:15		
9:15 Add network Network name		
9:15 Add network Network name Enter the SSID		
9:15 Add network Network name Enter the SSID Security		
9:15 Add network Network name Enter the SSID Security WPA2-Enterprise		<
9:15 Add network Network name Enter the SSID Security WPA2-Enterprise EAP method		↑
9:15 ■ ♥ ♥ ← Add network Network name Enter the SSID Security WPA2-Enterprise EAP method PEAP		•
9:15 ■ ♥ ♥		
9:15 ■ ♥ ♥ Add network Network name Enter the SSID Security WPA2-Enterprise EAP method PEAP Phase 2 authentication MSCHAPV2		♦ ■
9:15 ■ ♥ ♥		
9:15 ■ ♥ ♥ Add network Network name Enter the SSID Security WPA2-Enterprise EAP method PEAP Phase 2 authentication MSCHAPV2 CA certificate Please select		•
9:15 ■ ♥ ♥ Add network Network name Enter the SSID Security WPA2-Enterprise EAP method PEAP Phase 2 authentication MSCHAPV2 CA certificate Please select Identity		•
9:15 ■ ♥ ♥ Add network Network name Enter the SSID Security WPA2-Enterprise EAP method PEAP Phase 2 authentication MSCHAPV2 CA certificate Please select Identity		•
9:15 ■ ♥ ♥ Add network Network name Enter the SSID Security WPA2-Enterprise EAP method PEAP Phase 2 authentication MSCHAPV2 CA certificate Please select Identity	CANCEL	SAVE

:15 🖪 🌣 🏮		\bigcirc
← Add network		
Network name		
Enter the SSID		
Security		
WPA2-Enterprise		-
EAP method		
PEAP		-
Phase 2 authentication		
MSCHAPV2		-
GTC		
Please select		-
Identity		
	CANCEL	
• •		

9:16 🌣 🖸	\bigtriangledown
← Add network	
Network name	
Enter the SSID	
Security	
WPA2-Enterprise	~
EAP method	
PEAP	•
Phase 2 authentication	
MSCHAPV2	•
CA certificate	
Please select	-
Use system certificates	
Do not validate	
	CANCEL SAVE
• •	



9:16 🖪 🌣 🗘		\bigcirc
← Add network		
Network name		
Enter the SSID		
Security		
WPA2-Enterprise		-
EAP method		
TTLS		-
Phase 2 authentication		
PAP		.
MSCHAP		
MSCHAPV2		Ŧ
GTC		
	CANCEL	
•		

9:16 🖪 🌣 🗘		\bigtriangledown
← Add network		
Network name		
Enter the SSID		
Security		
WPA2-Enterprise		~
EAP method		
TTLS		~
Phase 2 authentication		
PAP		~
CA certificate		
Please select		-
Use system certificates		
Do not validate		_
	CANCEL	
•		

← Add network Network name Ènter the SSID Security WPA2-Enterprise EAP method TLS CA certificate Please select Do not provide Ldentity CANCEL SAVE	9:16 🖪 🌣 🗘	\bigtriangledown	9:16 🖪 🌣 🦁
Network name Enter the SSID Security WPA2-Enterprise EAP method TLS CA certificate Please select User certificate Do not provide Identity CANCEL Network name Enter the SSID Security WPA2-Enterprise EAP method TLS CA certificate Please select User certificate Do not provide Identity CANCEL SAVE	← Add network		← Add network
Enter the SSID Security WPA2-Enterprise EAP method TLS CA certificate Please select User certificate Do not provide Identity CANCEL EAP Security Security CA certificate Please select User certificate Do not provide Identity CANCEL SAVE	Network name		Network name
Security Security WPA2-Enterprise WPA2-Enterprise EAP method EAP method TLS TLS CA certificate CA certificate Please select Please select User certificate Use system certificates Do not provide Do not validate Identity CANCEL SAVE	Enter the SSID		Enter the SSID
WPA2-Enterprise EAP method TLS CA certificate Please select User certificate Do not provide Identity CANCEL SAVE WPA2-Enterprise EAP method TLS CA certificate Please select Use system certificates Do not validate Identity CANCEL SAVE	Security		Security
EAP method TLS CA certificate Please select User certificate Do not provide Identity CANCEL SAVE EAP method TLS CA certificate Please select Use system certificates Do not validate CANCEL SAVE	WPA2-Enterprise	-	WPA2-Enterprise
TLS TLS CA certificate CA certificate Please select Please select User certificate Use system certificates Do not provide Do not validate Identity CANCEL SAVE	EAP method		EAP method
CA certificate Please select User certificate Do not provide Identity CANCEL SAVE CANCEL SAVE CANCEL SAVE	TLS	-	TLS
Please select User certificates Do not provide Identity CANCEL SAVE 	CA certificate		CA certificate
User certificates Do not provide Identity CANCEL SAVE CANCEL SAVE	Please select	-	Please select
Do not provide Identity CANCEL SAVE CAN	User certificate		Use system certificates
Identity CANCEL SAVE CAN	Do not provide	-	Do not validate
CANCEL SAVE CAN	Identity		Monthy
CANCEL SAVE CAN			
< • • • • • • • • • • • • • • • • • • •	CANCEL		CAN
	- • E		• •



 \bigtriangledown

Wi-Fi ネットワークの詳細オプションの設定

- ・ 非ブロードキャスト Wi-Fi ネットワークは、Wi-Fi ネットワーク設定の[詳細オプション (Advanced options)] セクションで非表示ネットワークとして設定する必要があります。それ以外の場合、Wi-Fi ネットワークは範囲内にないと表示されます。
- ・ 非ブロードキャスト Wi-Fi ネットワークに接続するには、[非表示ネットワーク (Hidden network)]
 を[はい (Yes)]に設定します。

5:44 🌣 菌	\bigtriangledown	5:47 🌣 🛎	\heartsuit
← Add network		← Add network	
Security		Detect automatically	*
None	-	Proxy	
		None	-
Advanced options	^	IP settings	
Metered		DHCP	•
Detect automatically	-	Hidden network	
Proxy		Yes	-
None	-		
IP settings		If your router is not broadcasting a network ID you would like to connect to it in the future, you can set the network as hidden.	but
DHCP	-	This may create a security risk because your	
Hidden network		phone will regularly broadcast its signal to find network.	the
No	-	Setting the network as hidden will not change y router settings.	our
CANCEL	SAVE	CANCEL SA	AVE .
• • •			

IP 設定(静的または DHCP 設定)は、Wi-Fi ネットワーク設定の[詳細オプション (Advanced options)] セクションで設定できます。

5:44 🌣 🗂 🛇 🗎	5:47 🌣 🗎 🔷 🖓
← Add network	← Add network
Security	Static -
None 👻	IP address
Advanced options	192.168.1.128
Metered	100 160 1 1
Detect automatically -	192.108.1.1
Ргоху	Network prefix length
None 👻	DNS 1
IP settings	8 8 8 8
DHCP -	
Hidden network	8.8.4.4
No	
	Hidden network
CANCEL SAVE	No CANCEL SAVE
- • B	- • E

・ プロキシ設定は、Wi-Fi ネットワーク設定の【詳細オプション(Advanced options)】 セクションで 設定できます。

5:45 🌣 👗	\Diamond	5:45 🌣 🛋 🗇 🗎	5:45 🌣 👗
← Add network		← Add network	← Add network
Security None	•	Proxy Manual 👻	Advanced options
Advanced options Metered Detect automatically	~ •	The HTTP proxy is used by the browser but may not be used by the other apps. Proxy hostname proxy.example.com	Detect automatically Proxy Proxy Auto-Config
None	-	Proxy port 8080	https://www.example.com/proxy.pac
Manual Proxy Auto-Config	-	Bypass proxy for example.com,mycomp.test.com,localhc	IP settings DHCP
Hidden network	*	IP settings DHCP	Hidden network No
•	CANCEL SAVE	Hidden network CANCEL SAVE	CANCEL

 \heartsuit

~

-

.

通話品質設定の設定

有効なチャネルを含む Wi-Fi 帯域選択(自動、2.4 GHz、5 GHz)、高速セキュア ローミング設定(FT および CCKM)、および Wi-Fi 低 RSSI しきい値は、右上の3つの点を選択して設定できます。[コー ル品質設定(Call Quality Settings)]アプリケーションで、[設定(Settings)]を選択します。

7:44 🌣	\bigtriangledown	7:44 🌣	\bigtriangledown	7:44 🌣	\bigtriangledown
Wi-Fi information	÷	\leftarrow Settings		\leftarrow Settings	
		Wi-Fi low RSSI threshold -67		-67 Channel selection	
AP name		Channel selection		Wi-Fi band selection	
		WI-FI band selection		2.4 GHz	
ے۔ BSSID		2.4 GHz		5 GHz	
Channel		5 GHz		Wi-Fi preferences	
		Wi-Fi preferences		FT Preferred	•
RSSI		FT Preferred		ССКМ	
_{ျမျ} , Noise		CCKM Preferred			
4 • •				< •	
7:46 🌣	\bigtriangledown i	7:46 🌣	\Diamond î		
$\leftarrow~$ 2.4 GHz		$\leftarrow~$ 5 GHz			
2.4 GHz: channels 1 - 13 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13		Subband 1: channels 36 - 48 36, 40, 44, 48			
		Subband 2: channels 52 - 64 52, 56, 60, 64			
		Subband 3: channels 100 - 144 100, 104, 108, 112, 116, 120, 124, 128, 13 144	32, 136, 140,		
		Subband 4: channels 149 - 165 149, 153, 157, 161, 165			
< ● ■		◀ ● I			

単一の Wi-Fi 周波数帯域を使用する場合、または Wi-Fi 周波数帯域ごとに有効にするチャネルを制限する場合は、**[Wi-Fi 帯域選択(Wi-Fi Band Selection)]**を選択し、**[自動(Auto)]**をオフにして、2.4 GHz Wi-Fi 帯域のみ、5 GHz Wi -Fi 帯域のみ、または 2.4 GHz と 5 GHz の両方を使用する場合は両方。



【自動 (Auto)】がオフの場合、目的のチャネルセットをクリックするだけで、Wi-Fi 周波数帯域ごとに 有効にするチャネルを設定できます。



.

•



- 高速セキュア ローミングに 802.11r (FT) を使用する場合は、FT のスライダが右側にある [優先 (Preferred)] に設定されていることを確認します。
- 高速セキュア ローミングに CCKM を使用する場合は、CCKM のスライダが [優先 (Preferred)]に設定されていることを確認します。
- FT と CCKM の両方が [優先 (Preferred)] に設定されている場合、802.11r (FT) が CCKM よりも優先されます。

7:48 🌣	\bigtriangledown ii
\leftarrow Settings	
Wi-Fi low RSSI threshold -67	
Channel selection	
Wi-Fi band selection	
2.4 GHz	
5 GHz	
Wi-Fi preferences	
FT Preferred	
CCKM Preferred	
CAC	
• •	

注: EAP-TLS、EAP-TTLS、または PEAP を使用し、802.11r(FT)を優先に設定している場合は、アクセス ポイントで有効になっている 802.11r(FT)または CCKM がネゴシエートされます。

1.8(0) リリースでは、**CAC**(コール アドミッション コントロール)を無効にするオプションが有効に なっています。

1.9(0) リリースでは、**CAC**(コールアドミッション コントロール)はデフォルトで無効になっており、オプト イン機能になりました。

WPA3 はサポートされていません。

802.1x-SHA2 キー管理はサポートされていません。

CCMP256、GCMP128、および GCMP256 暗号化方式はサポートされていません。

詳細については、次の URL にある『**Cisco Wireless Phone 840 および 860 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/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

証明書管理

Cisco Wireless Phone 840 および 860 では、**EAP-TLS** に X.509 デジタル証明書を使用できます。**EAP-TTLS** または **PEAP** を使用する場合は、X.509 デジタル証明書を使用してサーバ検証を有効にできます。 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。

クライアントおよびサーバ証明書では、DER と Base-64(PEM)の両方のエンコーディングが使用できます。 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 Wireless Phone 840 および 860 との完全な相互運用性がない場合があります。

証明書のインストール

証明書は、EMM でサポートされている場合、エンタープライズ モビリティ管理(EMM)アプリケーションを 介して自動的にインストールできます。詳細は、EMM ドキュメントを参照してください。

証明書は、Wi-Fi 設定またはセキュリティ設定で手動でインストールすることもできます。

Wi-Fi 設定を使用して証明書を手動でインストールするには、[設定 (Settings)]、[ネットワークとインターネット (Network and Internet)]、[Wi-Fi]、[Wi-Fi 設定 (Wi-Fi Preferences)]、[詳細 (Advanced)]の順 に選択し、[証明書のインストール (Install certificates)]を選択します。

事前に電話機のストレージにダウンロードまたはコピーされた証明書を選択してインストールできます。



1:08 🗸 🗘			*♥∎
≡ Rec	ent	Q	0 0 0
RECENT FILES ON	PHONE		
	· · · · · · · · · · · · · · · · · · ·		
	No items		
•	•		

[セキュリティ (Security)]設定を使用して証明書をインストールするには、[設定 (Settings)]、[セキュリ ティ (Security)]、[暗号化とログイン情報 (Encryption and credentials)]の順に選択し、[ストレージから インストール (Install from storage)]を選択します。

事前に電話機のストレージにダウンロードまたはコピーされた証明書を選択してインストールできます。

1:09 🗸	0	•	1:09 🗸	0	•	1:09 🗸 🗘	;♥ 8
÷	Security	۹	÷	Encryption & credentials	Q	\equiv Recent	् :
	SECURITY STATUS			ENCRYPTION		RECENT FILES ON PHONE	
${}^{\odot}$	Google Play Protect Apps scanned at 11:18 AM			Encrypt phone Encrypted			
0	Find My Device No Google account on this device			CREDENTIAL STORAGE		· · · · ·	
	Security update August 5, 2020			Storage type Hardware-backed			
	DEVICE SECURITY			Trusted credentials Display trusted CA certificates			
	Screen lock Swipe			User credentials View and modify stored credentials		No items	
	Fingerprint			Install from storage Install certificates from storage			
	Smart Lock To use, first set a screen lock			Clear credentials Remove all certificates			
	D€ice admin €ps			< • B		< ●	

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。 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。 証明書名を入力できます。

ユーザ証明書を発行した CA チェーンが RADIUS サーバの信頼リストに追加されたことを確認します。



RADIUS サーバーの証明書を発行したルート CA の証明書は、**EAP-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。



証明書の設定

証明書がインストールされると、Wi-Fi プロファイル設定で使用する証明書を選択できます。

PEAP および EAP-TTLS の場合、サーバー検証を有効にするように CA 証明書をオプションで設定できます。



EAP-TLS の場合、ユーザー証明書を設定する必要があり、オプションでサーバー検証を有効にするように CA 証明書を設定できます。

1:44	✓ ◊	▼ û	1:44	✓ 0	◆ û	1:44	√ 0			20
~	Network details	1 9	~	Network details	1 Q	1				2
	halaa		10	L al an			baker			
	Daker FAR method	_		Daker EAR mothod	_				_	
	TIS	.		TIS	.		113		Ť	
		_					CA certificate			
	CA certificate						CISCO II ROOT		*	۲
	Please select	Ť		Please select	Ť		Domain			
	User certificate			Use system certificates						
	Please select	•		migilles	~		User certificate			
	Identity .	_					Please select		*	
a	migilles		6	Cisco IT Root	- 1	6	Identity			
	Advanced options	~		Do not validate	~		migilles			
	CANCEL	SAVE		CANCEL	SAVE		Advanced options		~	۲
	Advanced	_		Advanced	_			CANCEL		I
~	Network usage, Network det	ails, IPv6 addr	~	Network usage, Network details	, IPv6 addr		notion adago, i	termont actu	o, ii to ada	
	◀ ●						•	•		
1:44	✓ 0	◆ 0	1:44	✓ Ø	▼ 0	1:44	√ 0	_		2 6
))					,
	baker			baker			baker			Ì
	EAP method			EAP method			EAP method			
	TLS	-		TLS	-		TLS		*	
	CA certificate			CA certificate			CA certificate			
	Cisco IT Root	-		Cisco IT Root	-		Cisco IT Root		-	
	Domain			Domain			Domain			
	User certificate			User certificate			User certificate			
	Please select	-		Please select	-		migilles		-	
	Identity						Identity			
a.	miailles		G.	MacRandSecret		G	migilles			
		_		migilles			<u></u>			
1	Advanced options	~		Do not provide	~	1	Advanced options		~	
	CANCEL	SAVE		CANCEL	SAVE			CANCEL	SAVE	
1	netron usuge, netron det	uno, n. ro unon.		Herror usuge, Herror details	,	1	network adage, i		0, II TO 000	
					and the second					
	◀ ●						◀	•		

<u>証明書の削除</u>

証明書は個別またはまとめて削除できます。

個々の証明書を削除するには、**[設定 (Settings)**]、**[セキュリティ (Security)**]、**[暗号化とクレデンシャル (Encryption and credentials)**]、**[ユーザ クレデンシャル (User credentials)**]の順に選択し、**[削除 (Remove)**]を選択します。



すべての証明書を削除するには、**[設定(Settings)]、[セキュリティ(Security)]、[暗号化とログイン情報 (Encryption and credentials)]** の順に選択し、[OK] を選択して削除を確認します。



Cisco Phone アプリケーションの設定

Cisco Phone アプリケーションを設定するには、次のガイドラインを使用します。

 Cisco Phone の設定は、Cisco Phone アプリケーションで左上隅にある 3 本の線を選択して設 定できます。



着信音などのユーザ設定は、必要に応じて設定できます。

•

7:50 🌣	\bigtriangledown i	7:50 🌣	\bigcirc ii
\leftarrow		\leftarrow	
User settings		Secondary call server ringtone Default (Flutey Phone)	
Line 1 ringtone Default (Flutey Phone)		Announce caller ID Disabled	
Line 2 ringtone Default (Flutey Phone)		Hearing aid compatibility OFF	
Line 3 ringtone Default (Flutey Phone)		Automatic noise cancellation	
Line 4 ringtone Default (Flutey Phone)		Vibrate before ring OFF	
Line 5 ringtone Default (Flutey Phone)		Fade in ring OFF	
Line 6 ringtone Default (Flutey Phone)		Enable autodial OFF	
		< ●	

 ・ 信頼リストと TFTP サーバーは、[電話情報 (Phone information)]>[セキュリティ (Security)]の順
 に選択して管理できます。

7:51 🌣	\bigtriangledown
<u> </u>	
Vibrate before ring OFF	
Fade in ring OFF	
Enable autodial OFF	
Phone information	
Security Manage trust list, alternate TFTP servers	
Advanced debugging Configure advanced debugging	
Device information View configuration	
< ● ■	

[電話情報(Phone information)] > [セキュリティ(Security)]を選択したら、**[ローカル電話ロック解 除パスワード(Local Phone Unlock Password)]**を入力する必要があります(デフォルト = **#)。

	_		
7:51 🛱			/
\leftarrow			
U 11			
Vibrata bafara ring			
OFF			
Fade in ring			
UFF			1
E Security			
Please enter pa	assword		
Please enter pa	assword		H
Please enter pa	CANCEL	ок	l
P Security	CANCEL	ок	I
P Security Manage trust list, alterna	CANCEL	ок	
P Security Manage trust list, alterna	CANCEL	ок	
F Security Manage trust list, alterna Advanced debugging Configure advanced deb	CANCEL	ок	
P Security Manage trust list, alterna Advanced debugging Configure advanced debu	CANCEL te TFTP servers	ок	
P Security Manage trust list, alterna Advanced debugging Configure advanced debu	CANCEL te TFTP servers	ОК	
P Security Manage trust list, alterna Advanced debugging Configure advanced debu Device information View configuration	CANCEL	ок	
P Security Manage trust list, alterna Advanced debugging Configure advanced debug Device information View configuration	CANCEL CANCEL ugging	ок	

•

1.6(0) リリースでは、コール サーバー モードは [自動検出 (Auto detect)] に設定されます。この場合、ネットワークが DHCP オプション 150 または DHCP オプション 66 を提供し、 Cisco Wireless Phone 840 または 860 は Cisco Unified Communications Manager で設定されます。それ以外の場合は、Webex Calling に登録しようとします。

7:52 🌣	\bigtriangledown i	7:52 🌣	
\leftarrow		\leftarrow	
Call server mode Auto detect	^	Call server mode Auto detect	^
		Auto detect	/
		UCM	
		WxC	
< ● ■		< • B	

- Cisco Unified Communications Manager に登録する必要があり、登録先の Cisco Unified Communications Manager にネットワークが DHCP オプション 150 または DHCP オプション 66 を提 供していないため、TFTP サーバーを手動で設定する必要がある場合は、コールサーバーモードを UCM に設定します。 [Alternate TFTP] を有効にしてから、TFTP サーバーのアドレスを入力します。
- Cisco Wireless Phone 840 または 860 が以前に Cisco Unified Communications Manager に登録されていて、別の Cisco Unified Communications Manager クラスタに登録する場合は、【信頼リストのクリア(Clear trust list)】を選択します。

7:52 🍄	\bigcirc ii
\leftarrow	
Call server mode UCM	^
Clear trust list	
Alternate TFTP OFF	
TFTP address 1	
TFTP address 2	



 Webex Calling に登録し、手動で設定を構成する必要がある場合は、コールサーバーモードを WxC に 設定し、[プロファイルルール (Profile rule)]を選択して、プロファイルルール情報を入力します。

7:52 🌣	\bigcirc îi
\leftarrow	
Call server mode	
WxC	~
Profile rule	



・ 左上隅にある戻る矢印を 2 回選択して [設定 (Settings)] メニューを終了し、設定を保存します。

詳細については、次の URL にある『**Cisco Wireless Phone 840 および 860 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/td/docs/voice ip comm/cuipph/800-series/adminguide/w800 b wireless-800-administration-guide.html

注: DHCP オプション 66 は、1.2(0) リリースでサポートされています。

Bluetooth 設定

Cisco Wireless Phone 840 および 860 では、ハンズフリー通信を可能にする Bluetooth がサポートされます。 Bluetooth ヘッドセットと Cisco Wireless Phone 840 および 860 をペアリングする手順は次のとおりです。

• [設定 (Settings)] > [接続済みデバイス (Connected devices)]の順に選択します。

11:23 🗸 🗘	† ♥ ≘	11:23	× 0	. ♥ 🕯
Q Search settings		←	Connected devices	Q
^		+	Pair new device	
Finish setting up your device Copy your data, set wallpaper, and more			Connection preferences Bluetooth, NFC	
Network & internet Wi-Fi and data usage		(j	Visible as "Cisco yklh01bdujd000c devices	q" to other
Connected devices Bluetooth, NFC				
Apps & notifications Recent apps, default apps				
Battery 84% - More than 2 days remaining				
Display Wallpaper, sleep, font size				
Seind Seind			• • •	

- [設定 (Settings)]、[接続済みデバイス (Connected devices)]、[接続設定 (Connection Preferences)]、[Bluetooth]の順に選択して、Bluetooth が [オン (On)]に設定されていることを確認します。
- Bluetooth デバイス名は、必要に応じて変更することもできます。



- Bluetooth デバイスがペアリングモードになっていることを確認し、[新しいデバイスをペアリング (Pair new device)]を選択します。
- Bluetooth デバイスがリストに表示されたら、それを選択します。
- Cisco Wireless Phone 840 および 860 は、Bluetooth デバイスと自動的にペアリングしようとします。
 失敗した場合、プロンプトが表示されたら PIN コードを入力します。



 ペアリングに成功すると、Cisco Wireless Phone 840 および 860 は Bluetooth デバイスへの接続 を試みます。



- Bluetooth デバイス名は、デバイスの詳細で変更できます。
- Bluetooth デバイスを選択してから [切断 (Disconnect)]を選択すると、現在接続されている Bluetooth デバイスが切断されます。
- 選択した Bluetooth デバイスのペアリングを解除するには[切断 (Forget)]を選択します。

11:44	\$	* 🕈 🕯			
←	Device details	1 9			
Cisco HS 730-0ZG Active, 85% battery					
	Ū	×			
	FORGET	DISCONNECT			
	Phone calls	•			
	Media audio				
	Input device	•			
	Contact sharing				
í	Device's Bluetooth ac	ldress: 3C:			
	۰ ا				

ファームウェアのアップグレード

現在のビルド番号は、**[設定 (Settings)]>[電話情報 (About phone)]**>**[ビルド番号 (Build number)]** で確認できます。

8:02 🗸		†♥ 🗑
÷	About phone	Q
	Model & hardware Model: CP-860S	
	Android version	
	IP address fe80::5c74:c991:b44f:b6c9 10.81.12.28	
	Wi-Fi MAC address 10:f9:20:19:32:ed	
	Bluetooth address 10:f9:20:19:32:ec	
	Up time 25:24	
	Build number sip860 QKQ1.201230.002 1.9.0.2409	
	· · ·	

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 の署名済み COP ファイ ルをインストールしてから、Cisco TFTP サービスを実行しているすべてのノードで Cisco TFTP サービスを再 起動します。

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

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

ダウンロードされた電話機設定ファイルが解析され、デバイスのロードが識別されます。Cisco Wireless Phone 840 または 860 は、指定されたイメージを実行していない場合、ファームウェア ファイルをフラッシュ メモリにダウンロードします。
ロード サーバを、ファームウェア ファイルを取得する代替 TFTP サーバとして指定できます。この設定オプションは、TCP ポート 6970 の HTTP (UDP ポート 69 の TFTP がサポートされていないため) 経由で、Cisco Unified Communications Manager Administration 内の Cisco Wireless IP Phone 8821/8821-EX の製品固有の設定セクションにあります。ファームウェアを ZIP ファイル形式でダウンロードし、内容を抽出してから、それらのファイルをロード サーバーにコピーします。

コールサーバーで **[ソフトウェア更新のダウンロード後すぐに再起動する (Reboot successfully after** download software updates)] オプションが有効になっていない場合、ユーザーは再起動して新しいファー ムウェアを適用することを確認するプロンプトが表示されます。

注: Cisco Unified Communications Manager のバージョンが 14 SU1 より前の場合は、TCP ポート 6970 で 動作する外部 HTTP ロード サーバーを展開して使用することをお勧めします。14 SU1 より前のバージョンに は HTTP 範囲ヘッダーのサポートが含まれていないため、ファームウェアのダウンロード中にネットワークが 中断された場合、ダウンロードは中断したところから再開するのではなく、再開する必要があります。

Webex Calling

Cisco Wireless Phone 840 および 860 にインストールされるファームウェアバージョンは、Webex Control Hub (安定版、ベータ版、最新版) で構成されたソフトウェア アップグレード チャンネルによって決定され、 そのソフトウェア アップグレード チャンネルで新しいファームウェアが利用可能になると、自動的にプッシュ ダウンされます。

Cisco Wireless Phone Upgrade ツール

Cisco Wireless Phone Upgrade Tool (<u>https://webexphoneupgrade.cisco.com</u>) は、Cisco Wireless Phone 840 または 860 を 1.6(0) リリースにアップグレードできるクラウドベースのツールです。

新しいクラウドベースのツールを使用すると、Wi-Fi プロファイル設定とロードサーバー情報を含む生成された QR コードをスキャンすることで、Cisco Wireless Phone 840 および 860 ファームウェアを 1.6(0) リリースに 簡単にアップグレードできます。

1.6(0) リリースには Webex Calling のサポートが含まれているため、このアップグレード方法は、Cisco Wireless Phone 840 または 860 を使用しており、Webex Calling に登録したいが、 Cisco Wireless Phone 840 または 860 ファームウェア。

Cisco Wireless Phone Configuration Management ユーティリティにアクセスするには、Cisco.com アカウントが必要です。

Cisco Wireless Phone 840 または 860 が新品でない場合は、[設定 (Settings)]、[システム (System)]、[詳細 (Advanced)]、[オプションのリセット (Reset options)]、[すべてのデータの消去 (工場出荷時の状態へのリ セット) (Erase all data (factory reset))]の順に選択して、初期設定にリセットする必要があります。 起動画面で、ディスプレイをすばやく 6 回タップすると、QR コードをスキャンして Cisco Wireless Phone 840 または 860 ファームウェアをアップグレードするように求められます。



Wi-Fi 設定とロードサーバーパラメータを設定します。

次のセキュリティ設定がサポートされています。

[セキュリティモード (Security Mode)]	EAP 方法	フェース2認証
なし	該当なし	なし
WPA2-Personal	該当なし	なし
WPA2-Enterprise	PEAP	GTC、MSCHAPV2
WPA2-Enterprise	TTLS	GTC、MSCHAP、MSCHAPV2、PAP

注: Cisco Wireless Phone Upgrade Tool は EAP-TLS (TLS) をサポートしていません。

オープン Wi-Fi ネットワークに接続するには、SSID を入力し、[セキュリティ (Security)]を[なし (None)]に設定します。

Webex Wireless	Phone L	Jpgrade	Tool
----------------	---------	---------	------

Wi-Fi Configuration		
Security:	None	\vee
* SSID :		
Hidden SSID:		
Load Server		
Network Protocol:	HTTP v	6
Server Address:	wxcmppupgrade.bcld.webex.com	•
Server Port:	80	8
Relative Path on Server:	cp_840_860	6

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

Webex Wireless Phone Upgrade Tool

Security:	WPA2-Personal	\vee
* SSID:		
* Password:		
Show:		
Hidden SSID:		
Load Server		
Network Protocol:	HTTP v	6
Server Address:	wxcmppupgrade.bcld.webex.com	6
Server Port:	80	•

EAP 対応の Wi-Fi ネットワークに接続するには、ネットワーク名を入力し、[セキュリティ (Security)]を [WPA2-EAP] に設定してから、[認証方式 (Authentication method)]を選択します。

PEAP または EAP-TTLS (TTLS) Wi-Fi ネットワークを設定する場合は、フェーズ2認証方式を選択し、必要 に応じてヘッダーとフッターを除いた Base-64 (PEM) エンコーディング形式で CA 証明書を設定し、ID とパ スワードを入力します。

Webex Wireless Phone Upgrade Tool

Initial Provisioning

Security:	WPA2-Enterprise	\sim
* SSID:		
* Password:		
Show:		
Hidden SSID:		
Load Server		•
Network Protocol:	HIIP	U
Server Address:	wxcmppupgrade.bcld.webex.com	6
Server Port:	80	8
Relative Path on Server:	cp_840_860	1
EAP Configuration		
EAP Method:	PEAP	~
Phase 2 Authentication:	MSCHAPV2	\sim
Domain:		
Domain:		
Domain: * Identity:		
Domain: * Identity: Anonymous Identity:		
Domain: * Identity: Anonymous Identity: CA Certificate:		
Domain: * Identity: Anonymous Identity: CA Certificate:		
Domain: * Identity: Anonymous Identity: CA Certificate:		

注: ブロードキャストされていない Wi-Fi ネットワークは、非表示の SSID として設定する必要があります。 それ以外の場合、Wi-Fi ネットワークは範囲内にないと表示されます。 非ブロードキャスト Wi-Fi ネットワーク に接続するには、[非表示 SSID (Hidden SSID)]を[はい (True)]に設定します。

ヘッダーとフッターが削除され、スペースや改行が含まれていない CA 証明書の形式が正しいことを確認します。

Cisco Wireless Phone 840 および 860 ファームウェア ファイルは、ファームウェア アップグレードにシスコ が管理するロード サーバーを使用する代わりに、代替のロード サーバーにダウンロードしてホストすることも できます。

次のファイルをダウンロードして、代替 HTTP または HTTPS ロードサーバーにアップロードする必要 があります。

- http://wxcmppupgrade.bcld.webex.com/cp_840_860/UpgradeDPC.apk
- http://wxcmppupgrade.bcld.webex.com/cp_840_860/sip840-ota_update-signed-1.6.0.1409.zip
- <u>http://wxcmppupgrade.bcld.webex.com/cp_840_860/sip860-ota_update-signed-1.6.0.1852.zip</u>

注: HTTPS 方式を使用するには、Android の証明書信頼ストアに含まれる信頼できる CA から証明書が HTTPS サーバーに発行されていることを確認する必要があります。

デフォルトのロードサーバー(**wxcmppupgrade.bcld.webex.com**)の証明書は、Android の証明書信頼スト アに含まれる信頼できる CA から発行されません。したがって、HTTPS は使用せず、デフォルトの HTTP TCP ポート 80 設定を使用する必要があります。

設定が完了したら、[生成 (Generate)]を選択して QR コードを作成すると、QR コードが表示されます。

QR Code

Scan this QR code on your Webex wireless phone device by tapping seven times on the "Hi there" text on the Welcome screen



Done

Cisco Wireless Phone 840 または 860 で QR コードをスキャンします。

Cisco Wireless Phone 840 または 860 が近くにない場合に備えて、QR コードを保存できます。その場合は、 QR コードを PDF ファイルまたはスクリーンショットとして保存することをお勧めします。PNG ファイルとし てファイルを保存するとファイルが変更され、QR コードのスキャンが失敗します。

Cisco 無線電話 840 および 860 は、設定された Wi-Fi ネットワークへの接続を試み、ロード サーバーからフ ァームウェア ファイルをダウンロードします。

Cisco Wireless Phone 840 および 860 は、自動的に初期設定にリセットされます。

注: Cisco Wireless Phone 840 および 860 は、設定された Wi-Fi ネットワークの範囲内にある必要があります。 範囲内にない場合、ファームウェアのアップグレードは失敗します。

Cisco Wireless Phone 840 および 860 の使用

アプリケーション

Cisco Wireless Phone 840 および 860 には、次のカスタム アプリケーションがプリインストールされています。

- **Cisco Phone** 音声コールとビデオ コール
- バッテリ寿命 バッテリ モニタリング
- **ボタン**:ボタンのカスタマイズ
- 通話品質設定 Wi-Fi のカスタマイズ
- カスタム設定: ユーザー制限とデバイス設定
- 診断 ハードウェアのトラブルシューティング
- **緊急** パニック ボタン機能
- **ロギング** 高度なデバッグ
- **PTT**: プッシュツートーク機能
- システム アップデータ ファームウェア更新通知
- Web API Web API の設定
- バーコード: バーコードスキャン機能 (840 および 860 モデルのみ)



シスコの電話機

電話アプリケーションを起動するには、メイン ページまたはアプリケーション メニューから [**Cisco Phone**] ア イコンを選択します。

Cisco Wireless Phone 840 および 860 は、電源投入後に Cisco Unified Communications Manager または Webex Calling への登録を試行するため、コールを発信または受信するためにアプリケーションを手動で起動す る必要はありません。

通知ステータスバーにチェックマークアイコンがあり、内線番号が Cisco Phone アプリケーションに表示され ている場合、Cisco Wireless Phone 840 および 860 は Cisco Unified Communications Manager または Webex Calling に登録されています。



通話履歴には、[通話 (Calls)]タブからアクセスできます。

連絡先とお気に入りには、**[連絡先 (Contacts)**]タブからアクセスできます。連絡先を追加するには、[+]アイ コンを選択し、連絡先を追加するディレクトリを選択します。 その連絡先リストを表示または管理するには、 パーソナルディレクトリにログインする必要があります。

手動コールは、[キーパッド (Keypad)]タブを使用して発信できます。

コールサーバーで [ビジュアルボイスメールアクセス (Visual Voicemail Access)]が有効になっている場合 は、[ボイスメール (Voicemail)]タブからボイスメールにアクセスできます。



着信音を設定するには、左上隅にある 3 本の線を選択し、**[ユーザー設定(User settings)]**を選択します。 1.7(0) リリースでは、着信音は回線ごとに設定できますが、以前のリリースでは 1 つの着信音しか設定できま せんでした。

1.8(0) リリースでは、事前にインストールされている着信音を Cisco Unified Communications Manager 内の 回線ごとに設定および管理できます。

1.9(0) リリースでは、Cisco Unified Communications Manager 内で回線ごとにカスタム着信音を設定および管理し、電話機にダウンロードできます。

10:38 🗸		● 🔒
\leftarrow		
User settings		
Line 1 ringtone Default (Flutey Phone)		
Line 2 ringtone Default (Flutey Phone)		
Line 3 ringtone Default (Flutey Phone)		
Line 4 ringtone Default (Flutey Phone)		
Line 5 ringtone Default (Flutey Phone)		
Line 6 ringtone Default (Flutey Phone)		
O		
•	•	

Cisco Unified Communications Manager 内の **[回線 1 ~ 6 の着信音(Line 1-6 Ringtone)]** オプションに設 定できる、事前にインストールされている着信音を以下に示します。

- Andromeda
- Aquila
- Argo Navis
- Atria
- Beat Plucker
- Bell Phone
- Big Easy
- Bootes
- Canis Major
- Carina
- Cassiopeia
- Centaurus
- Chimey Phone
- Cygnus
- Digital Phone
- Ding
- Draco
- Dream Theme
- Eridani
- Flutey Phone
- Free Flight
- Girtab
- Growl
- Hydra
- Insert Coin
- Kuma
- Lyra
- Machina
- Mildly Alarming
- New Player
- Noisey One
- Orion
- Pegasus
- Perseus
- Pyxis
- Rasalas
- Rigel
- Scarabaeus
- Sceptrum
- Solarium
- Testudo
- Third Eye
- Very Alarmed
- Vespa
- Zeta

短縮ダイヤル、コール転送、プライバシー(有効な場合)、ピックアップ、アプリケーション(設定されている 場合)などの機能にアクセスするには、左上隅にある3本の線を選択し、[機能(Features)]を選択します。

10:38 🗸	≑♥ 🔒
cisco	
Line: 1014	
Admin settings	
User settings	} : F
Clear call log	5
Features	~)
Speed dial	Y Z
Call forward	F
Privacy	
Pickup	
Applications	
Report problem	CO Voicemail
< ●	

短縮ダイヤルを設定するには、**[機能 (Features)]、[短縮ダイヤル (Speed dial)**]の順に選択します。 既存のローカル連絡先の番号にマッピングして短縮ダイヤルを設定したら、**[キーパッド (Keypad)**]タブで、 関連付けられた番号を押し続けます。

10:39 ✓ ←	-,₩ 🔒
1. Voicemail	
2. Not assigned	
3. Not assigned	
4. Not assigned	
5. Not assigned	
6. Not assigned	
7. Not assigned	
8. Not assigned	
< • B	

Cisco Wireless Phone 840 および 860 が Cisco Unified Communications Manager に登録されている場合に コール転送を有効にするには、【機能 (Features)】、【コール転送 (Call forward)】の順に選択し、スライダを タップしてスライダを右に移動し、すべてのコールを転送する宛先番号を入力します。

Cisco Wireless Phone 840 および 860 が Webex Calling に登録されている場合にコール転送を有効にするに は、[機能 (Features)]、[常にコール転送 (Call forward always)]、または[機能 (Features)]、[話中の場 合のコール転送 (Call Forward when busy)]を選択し、スライダをタップして右に移動し、すべてのコール を転送する宛先番号を入力します。に設定します。

コール転送を無効にするには、スライダをタップして左に移動します。

右上隅の[保存 (SAVE)]を選択して設定を保存します。

0:40 🗸	
\leftarrow	SAVE
Enable call forward for Line: 1	014
000-000-000	
Enter call forward number or s from the list of contacts below	elect number v



1.3(0) リリースでは、プライバシー機能がサポートされるようになりました。

プライバシー機能を使用するには、回線の 1 つを共有回線にし、ボタンの 1 つに**プライバシー**が設定されたカ スタム電話ボタン テンプレートを作成し、電話機に適用する必要があります。

次に、プライバシーを有効にするには、**[機能 (Features)]、[プライバシー (Privacy)]**の順に選択します。 [**プライバシー (Privacy)]**の右側にチェックマークが表示され、この機能が有効になっているかどうか が示されます。



注: Webex Calling に登録されている場合、プライバシーは Cisco Wireless Phone 840 および 860 ではサポ ートされません。

1.9(0) リリースでは、コール ピックアップ機能がサポートされるようになりました。

Cisco Unified Communications Manager 内の Cisco Wireless Phone 840 および 860 の回線に対してコール ピックアップ グループが設定されていることを確認します。

コール ピックアップ機能を使用するには、[機能 (Features)]、[ピックアップ (Pickup)]の順に選択します。



設定済みのアプリケーションにアクセスするには、**[機能 (Features)] > [アプリケーション (Applications)]**の順に選択します。

10:43 🗸	♥ 🔒
\leftarrow	
Applications	
Extension Mobility	



注: Webex Calling に登録されている場合、アプリケーションは Cisco Wireless Phone 840 および 860 では サポートされません。

バーコード

バーコードスキャナは、Cisco 無線電話 840S および 860S モデルでのみ使用できます。 バーコードスキャナの設定は、**バーコード**アプリケーションでカスタム設定できます。

8:10 🗸	¢ ♥ ≘
Barcode settings	÷
Barcode is running	
General settings	
Default settings	
ScanFlex	



バーコードスキャナをテストするには、**バーコード**アプリケーションで右上隅にある3つのドットを選択し、 [**スキャンのテスト (Test scan)**]を選択します。

下のバーコードアイコンを押して、バーコードスキャンを開始します。

バーコードがスキャンされると、は検索アイコンを選択して検索を実行できます。



バッテリ寿命

West Tasman Drive ; San Jose CA 94568 ; Country,

.

United states ; Country code, US. 4

バッテリ寿命のモニタリングを有効にするには、[バッテリ寿命 (Battery Life)]アプリケーションで右上隅に ある3つのドットを選択し、[設定 (Settings)]を選択します。

8:13 🗸	†	8:14 🗸	♥ 🔒
Battery Life	:	$\leftarrow~$ Battery Life settings	
		User settings	
		Alarm volume	
		50%	
Please enable battery monitoring from application settings		Admin settings	
	from	Enable battery monitoring Off	
		Vibrate Off	
		Sound Off	
		Alarm tone Default (Cesium)	
		Low battery threshold	
< ● ■		< ●	

バッテリ寿命のモニタリングを有効にするには、[バッテリのモニタリングを有効にする (Enable backup monitoring)]スライダが右側にある [オン (On)]に設定されていることを確認します。

フル充電サイクルの数も表示できます。

充電サイクルの数が 500 に達すると、通知が表示され、バッテリを交換する必要があります。

8:14 🗸	♥ 🕯	8:14 🗸	†	8:14 🗸	♥ 🕯
$\leftarrow~$ Battery Life settings		Battery Life	:	Battery Life	:
User settings		_		22.0 °C (80.6 °E)	
Alarm volume				Temperature	
50%		84%		co Good	
Admin settings				Health	
Enable battery monitoring				Discharging	
On	-	✓ VK21072522532		Status	
Vibrate Off		Serial		A.132V	
Sound		<mark>∩</mark> 3020 mAh			
Off		Battery capacity		Li-ion _{Type}	
Alarm tone Default (Cesium)		Mathematical Secondary battery		@ 4	
Low battery threshold		a 32 0 ℃ (89 6 ℃)		Charge cycle completed	
< ● ■		•		< ●	

ボタン

Cisco 無線電話 840 および 860 のハード ボタンは、ボタン アプリケーションでカスタム設定できます。



注: [フィンガープリント (Fingerprint)]ボタンは、Cisco ワイヤレス 電話 860 でのみ使用できます。

通話品質設定

有効なチャネルを含む Wi-Fi 帯域選択(自動、2.4 GHz、5 GHz)、高速セキュア ローミング設定(FT および CCKM)、および Wi-Fi 低 RSSI しきい値は、右上の 3 つの点を選択して設定できます。[コール品質設定 (Call Quality Settings)] アプリケーションで、[設定 (Settings)]を選択します。



注: 1.8(0) リリースでは、**CAC**(コール アドミッション コントロール)を無効にするオプションが有効になっています。

1.9(0) リリースでは、**CAC**(コールアドミッション コントロール)はデフォルトで無効になっており、オプト イン機能になりました。 ユーザー制限、時間設定などのさまざまな設定は、カスタム設定アプリケーションでカスタム設定できます。





通知音を表示および管理するには、[サウンド (Sounds)]、[通知音 (Notifications)]の順に選択します。 アラーム音を表示および管理するには、[サウンド (Sounds)]>[アラーム音 (Alarm サウンド)]を 選択します。

デフォルトの通知音とデフォルトのアラーム音は、[サウンド (Sounds)]メニューでも管理できます。

1.9(0) リリースでは、カスタム通知音とアラーム音を Cisco Unified Communications Manager 内で設定およ び管理し、電話機にダウンロードできます。

以下は、デフォルトの通知音として設定できるプレインストールされた通知音です。

- Adara
- Aldebaran
- Altair
- Alya
- Antares
- Antimony
- Arcturus
- Argon
- Beat Box Android
- Bellatrix
- Beryllium
- Betelgeuse
- Caffeinated Rattlesnake
- Canopus
- Capella
- Captain's Log
- Castor
- Ceti Alpha

- Cobalt
- Cricket
- Dear Deer
- Deneb
- Doink
- Don't Panic
- Drip
- Electra
- Fluorine
- Fomalhaut
- Gallium
- Heaven
- Helium
- Highwire
- Hojus
- Iridium
- Krypton
- Kzurb Sonar
- Lalande
- Look At Me
- Merope
- Mira
- Missed It
- Moonbeam
- On The Hunt
- Palladium
- Pixie Dust
- Pizzicato
- Plastic Pipe
- Polaris
- Procyon
- Proxima
- Radon
- Regulus
- Selenium
- Shaula
- Sirius
- Sirrah
- Space Seed
- Spica
- Strontium
- Syrma
- Ta Da
- Talitha
- Tejat
- Thallium
- Tinkerbell
- Tweeters
- Upsilon
- Vega
- Voila
- Xenon
- Zirconium

以下は、デフォルトのアラーム音として設定できるプレインストールされたアラーム音です。

- Argon
- Barium
- BeeBeep Alarm
- Beep-Beep-Beep Alarm
- Buzzer Alarm
- Carbon
- Cesium
- Fermium
- Hassium
- Helium
- Neptunium
- Nobelium
- Osmium
- Piezo Alarm
- Platinum
- Plutonium
- Rooster Alarm
- Scandium

注: 1.5(0) リリースでは、インターネット上のデフォルトの NTP サーバーにアクセスできない場合に備えて、 DHCP オプション 42 を NTP サーバーの設定に使用できるようになりました。

緊急 (Emergency)

モーションセンサー、パニックボタン、緊急コール、トーンの設定などの緊急設定は、**緊急**アプリケーションで 右上隅にある3つのドットを選択し、【設定(Settings)】を選択することで設定できます。



Emergency call behavior

Emergency tone configuration Emergency tone selection



C C		Ū	
lonitoring ff		Panic button Disabled	
No movement sensitivity Disabled		Panic button silent alarm	•
No movement timeout (seconds) 30		Panic button alarm timeout (se	conds)
Tilt sensitivity Disabled			
Tilt timeout (seconds)			
Running sensitivity Disabled			
Running timeout (seconds) 10			
Running timeout (seconds)		< ●	
Running timeout (seconds)	•	● 10:43 \$ ✓ \$	Ŷ
Running timeout (seconds)	♥ i Iration	 ■ 10:43 ♥ ✓ ♥ ← Emergency tone cont 	€ ¶ figuration
Running timeout (seconds) 10 0:43 • • • • Cemergency call configu Emergency call Off	• • • Iration	10:43 ♥ ✓ ♥ ← Emergency tone con Warning tone Default (Pixie Dust)	€ figuration
Running timeout (seconds) 10 0:43 • ✓ • Emergency call configu Emergency call Off Emergency dial force speaker On	aration	10:43 I I I I I I I I I I I I I I I I I I I	© ∎
Running timeout (seconds) 10 0:43 • • • Emergency call configu Emergency call Off Emergency dial force speaker Dn Emergency dial number	aration	10:43 ♥ ✓ ♥ ← Emergency tone con Warning tone Default (Pixie Dust) Alarm tone Default (Cesium)	© ∎
Running timeout (seconds) 10 0:43 • • • • Emergency call configu Emergency call Off Emergency dial force speaker On Emergency dial number 211	uration	10:43 ♥ ✓ ♥ ← Emergency tone con Warning tone Default (Pixie Dust) Alarm tone Default (Cesium)	© ∎
Running timeout (seconds) 10 O:43 • • • Emergency call configu Emergency call Off Emergency dial force speaker On Emergency dial number 911	uration	10:43 ♦ ✓ ♥ ← Emergency tone con Warning tone Default (Pixie Dust) Alarm tone Default (Cesium)	€
Running timeout (seconds) 10 Constant in the second secon	uration	10:43 � < • Emergency tone con Warning tone Default (Pixie Dust) Alarm tone Default (Cesium)	♥ In the second sec
Running timeout (seconds) 10 0:43 • • • Emergency call configu Emergency call Off Emergency dial force speaker On Emergency dial number 911	aration	10:43	♥ Interpretent of the second seco
Running timeout (seconds)	uration	10:43 ♥ ✓ ♥ ← Emergency tone con Warning tone Default (Pixie Dust) Alarm tone Default (Cesium)	€

注: Cisco Wireless Phone 840 および Cisco Wireless Phone 860 の右上には、緊急ボタン(赤色のボタン) があります。

ロギング

ロギング アプリケーションでは、さまざまなデバッグ オプションを使用できます。

入力画面で、ローカル電話機ロック解除パスワードを入力します(デフォルト = **#)。

10:45 🗸 🛱 🗘 🕴	10:45 🌣 🗸 🛱 🗘 🕴 🕈	10:46 🌣 🗸 🖏 🗘 🔷 🕈
Logging	Logging	$\leftarrow~$ Advanced debugging
(iii) Advanced debugging	(iii) Advanced debugging	Advanced Logging Admin-level features for debugging
	Password	MMI self test Dial Code *#2886#
	CANCEL OK	Phone and Wi-Fi information Dial Code *#*#4636#*#*
		Feedback Dial Code *#*#0574#*#
		I MEI number Dial Code *#06#
		BT test mode Dial Code *#*#2581#*#*
		Engineering menu Dial Code *58468#
		Device information Dial Code *#0000#

PTT

プッシュ ツー トーク (PTT) 設定は、PTT アプリケーションで右上隅にある 3 つのドットを選択し、【設定 (Settings)]を選択することで設定できます。



6:18 🎄 🗸	≑♥ ∎	6:18 🌞 🗸	÷ • 🛔	6:19 🌣 🗸	†♥ ≜
$\leftarrow~$ PTT settings		$\leftarrow~$ PTT settings		$\leftarrow~$ Channel setup	
User settings		Admin settings		PTT channels	
PTT volume		Enable PTT OFF		Channel #1 - ALL Transmit: Yes, Subscribed: Yes	
Default channel Channel 1 - ALL		Allow PTT transmission when phone is locked OFF		Channel #2 Transmit: No, Subscribed: No	
Admin settings		llsername		Channel #3 Transmit: No. Subscribed: No	
Enable PTT OFF		Multicast address		Channel #4 Transmit: No, Subscribed: No	
Allow PTT transmission when phone is locked OFF		Codec G.726		Channel #5 Transmit: No, Subscribed: No	
Username		Channel setup		Channel #6	
Multicast address		Labels, subscriptions, etc.		Transmit, No, Subscribed, No	
< ● ■		< ● ■		< ●	

サウンドステージ

サウンド ステージの設定を構成するには、サウンド ステージ アプリケーションで右上隅にある 3 つのドットを 選択し、**[設定 (Settings)]**を選択します。



サウンドステージを有効にするには、**[管理設定 (Admin settings)]**を選択し、**[サウンドステージの有効化** (Enable Sound Stage)]のスライダが右側にあることを確認します。

5:29 🏟 🗸	♥ 🛔	5:29 🔹 🏟 🗸	�∎
$\leftarrow~$ Admin settings		$\leftarrow~$ Admin settings	
Enable Sound Stage		Enable Sound Stage	
Enable sound profile switch		Enable sound profile switch	
Enable normal profile		Enable normal profile	
Enable loud profile		Enable loud profile	
Enable soft profile		Enable soft profile	
Enable silent profile		Enable silent profile	
Enable personal profile		Enable personal profile	
Persist active profile notification		Persist active profile notification	
Switch profiles silently		Switch profiles silently	
< • •		< ● ■	

[サウンドステージの有効化 (Enable Sound Stage)]を有効にすると、デフォルトで[標準 (Normal)]プロ ファイルが選択されます。



現在のオーディオプロファイルは、メインの [サウンドステージ(Sound Stage)] 画面で [変更(Change)] を選択して変更できます。

5:31 🌣 🐠 🗸	▼ 1
Sound Stage	:
Normal profile on	Change
System	
CHANGE AUDIO PROI	FILE
■ Normal	~
■ v Loud	



The audio profile could also be changed by scanning a programmed NFC tag without the phone open.



6:02 📣 🌣 🗸	♦ 1
Sound Stage	÷
I oud profile on	Change
System	
ପ Alarm	75%
Media ្ជា	75%
A Ringer	75%
© In-call	75%
Apps	
Web A PI	75%

オーディオプロファイルを設定するには、**[オーディオプロファイル (Audio profiles)**]を選択します。 システムとアプリケーションのデフォルト、最小、および最大音量は、オーディオプロファイルごとに 設定できます。

5:30 🔹 🌣 🗸 🔹 🗲 🗎	5:30 🂠 🔶 🗸	★ 1	5:30 🂠 🐠 🗸	▼ 1
$\leftarrow~$ Audio profiles	\leftarrow Normal profile		\leftarrow Normal profile	
Normal profile	System		System	
Loud profile	🖸 ALARM	~	🖸 ALARM	^
Soft profile	ာ MEDIA	\sim	Default	20%
V Silent profile	¢ RINGER	~	Minimum	14%
	S IN-CALL	~	Maximum	75%
	Apps			~
	WEB API	\sim		
	TT (~	⊖ RINGER	~
∢ ● ■	< ●		< ●	

プロファイル切り替えルールを設定するには、**[プロファイル切り替えルール(Profiles switch rules)]** を選択します。



[NFC タグをビーム (Beam NFC tag)]を選択することで、特定のオーディオプロファイルに対して NFC タグ をプログラムできます。

これは、ユーザーがある環境から別の環境に移動する際に、より少ないボリュームまたはより大きなボリューム を必要とする場合に役立ちます。



NFC タグがスキャンされ、音声プロファイルが設定されると、確認画面が表示されます。



Device profile changed successfully



システムアップデータ

管理者は、ファームウェアの更新を管理し、Cisco 無線電話 840 および 860 にプッシュダウンします。コール サーバーで **[ソフトウェア アップデートのダウンロード後すぐに再起動する (Reboot successfully after** download software updates)] オプションが有効になっていない限り、ユーザーは再起動して新しいファー ムウェアを適用することを確認するように求められます。

9:14 🗸	≑♥ 🔒
System Updater	:
cisco	
Current OS version	
1.9.0.2409	
Available OS version	
1.9.0.2409	
Current Apps bundle version	
None	
System update: Already up-to-date	
Apps bundle update: Already up-to-date	
CHECK FOR UPDATE	

注: システム アップデータ アプリケーションは、ファームウェアの更新に直接使用しないでください。

Web API

Web API 設定は、Web API アプリケーションでカスタム設定できます。

0:47 🌣 🗸 😪 💟	•	
Web API settings	:	
Web service is running		
Web API settings		
Enable Web API Off		
Enable Web access On		
Data format XML		
Phone state polling Access phone state polling settings		
Push settings Access phone data/URL push settings		
Web application shortcuts		
Add or remove Web app shortcuts		
Add or remove Web app shortcuts		
0:47 ✿ ✓ ⅔ ♥	: ▼ ≘	10:47 🌣 🗸 😒 🕽
Add or remove Web app shortcuts 0:47 ♥ ✓ ⅔ ♥ ← Phone state polling	; ₽	10:47 ♥ ✓ ☜ ♥ ← Push settings
Add or remove Web app shortcuts 0:47	•♥ ĝ	10:47 ♦ ✓ ଔ ♥ ← Push settings Web service is run
Add or remove Web app shortcuts 0:47 ✓ ✓ Phone state polling Web service is running Authentication	÷♥ û	10:47 ✿ ✓ ㉓ ♥ ← Push settings Web service is run Authentication
Add or remove Web app shortcuts 0:47	÷♥ â	10:47 ♦ ✓ 🐼 ♥ ← Push settings Web service is run Authentication Username
Add or remove Web app shortcuts 0:47		10:47 ♥ ✓ Ø ♥ ← Push settings Web service is run Authentication Username Password
Add or remove Web app shortcuts	÷♥ â	10:47 ♥ ✓ ☑ ♥ ← Push settings Web service is run Authentication Username Password Other push settings
Add or remove Web app shortcuts	÷♥ ĝ	10:47 ♦ ✓ 🐼 ♥ ← Push settings Web service is run Authentication Username Password Other push settings Push alert priority All
Add or remove Web app shortcuts		10:47 🔹 🗸 😒 🔍 C Push settings Web service is run Authentication Username Password Other push settings Push alert priority All Server root URL
Add or remove Web app shortcuts		10:47 Image: Constraints Image: Constraints Image: Constraints Muthentication Image: Constraints Authentication Image: Constraints Mush alert priority Image: Constraints Aul Server root URL Enable notification ringtone Off
Add or remove Web app shortcuts		10:47 Image: Constraints Image: Constraints Image: Constraints Web service is runn Image: Constraints Authentication Image: Constraints Authentication Image: Constraints Authentication Image: Constraints Password Image: Constraints Other push settings Image: Constraints Push alert priority All Server root URL Enable notification ringtone Off Image: Constraints Web API volume Image: Constraints

₹ i

10:47 🌣 🗸 🌝 🟮	₹	10:47 🌣 🗸 😒 🕽	÷ •
$\leftarrow~$ Web application shortcuts		\leftarrow Device event notifications	
Web service is running		Web service is running	
Shortcut 1 Shortcut URL		Add new notification URL	
Shortcut URL			
Shortcut 3			
Shortcut URL			
Shortcut 4			
Shortcut one			
Shortcut 5 Shortcut URL			
Shortcut 6			
Shortcut URL			
Shortcut 7			
		< ● ■	

注: 詳細については、『Cisco Wireless Phone 800 Series Developer's Guide』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

アプリケーションストア

さまざまなアプリケーションを Google Play からダウンロードして入手できます。

Google Play は、Google™ によって開発された Android OS 用アプリケーション市場です。**Play Store** アプリ ケーションで、ユーザは、サードパーティの開発者が公開したアプリケーションを参照し、ダウンロードするこ とができます。

Google のアカウントはアプリケーションをダウンロードするために必要です。

最初に Google Play を起動した時、まだアカウントを持っていない場合はクレデンシャルを使用してサインイ ンまたは登録するようプロンプトが表示されます。

Google Play は、次の URL でもアクセスできます。

https://play.google.com/store
IP Phone サービス (IP Phone Services)

次のドキュメントには、アプリケーション開発者が Cisco Wireless Phone 840 および 860 用の IP 電話サービ スを作成および展開するために必要な情報が記載されています。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

トラブルシューティング

問題レポート ツール

問題レポートを作成するには、Cisco Phone アプリケーションで左上隅にある 3 本の線を選択し、[問題の報告 (Report problem)]を選択します。

Cisco Unified Communications Manager **のカスタマー サポート アップロード URL** オプションは、電話機ごと に設定して、ログを自動的に取得するか、[デバイスログ (Device Logs)]の下にある電話機の Web ページか らログを手動でダウンロードできます。

9:24 🗸	♥ 🔒	9:25 🗸	≑♥ 🔒
 cisco		$\leftarrow~$ Report Problem	
Line: 1014		Issue type	
Admin settings		 Audio quality 	
User settings	} : F	O Battery O Other	
Clear call log	5	User comment (optional)	
Features	>)	Comment	
Report problem	, ₽		~
Cisco Phone status			
About		Submit	
	() Keypad		
< ●		< • E	

カスタマー サポート アップロード URL の設定

サーバでアップロード スクリプトを使用して PRT ファイルを受信する必要があります。PRT は、HTTP POST メカニズムを使用し、次のパラメータをアップロード(マルチパート MIME エンコーディングを使用)に含め ます。

- devicename (例: "SEP001122334455")
- serialno (例: "FCH12345ABC")
- username (Cisco Unified Communications Manager で設定される、デバイス所有者のユーザ名)
- prt_file (例: "probrep-20141021-162840.tar.gz」)

サンプル スクリプト

<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

```
// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);
```

```
// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");
```

```
$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");
```

```
$username = $_POST['username'];
$username = trim($username, "'\"");
```

```
// where to put the file
$fullfilename = "/var/prtuploads/".$filename;
```

// If the file upload is unsuccessful, return a 500 error and // inform the user to try again

```
if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}
```

?>

電話機の Web ページ

電話機の Web ページ インターフェイスにアクセスすると、Cisco Wireless Phone 840 および 860 の情報をリ モートから収集できます。

Web ページインターフェイス (<u>https://x.x.x.</u>) には、デバイス情報、ネットワーク情報、登録情報、およびデ バイスログに関する読み取り専用の情報が含まれています。Web ページインターフェイスにアクセスするに は、コールサーバーで **Web アクセ**スを有効にする必要があります。

デバイス情報

Cisco Wireless Phone 840 および 860 のデバイス情報が提供されます。ここには、MAC アドレス、およびバージョン情報が表示されます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<u>https://x.x.x.x</u>) にアクセスし、[デバイス情報 (Device information)]を選択します。

Cisco Unified Communications Manager

cisco	Device information Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)				Device information Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)		
Device information Network information Registration information Device logs	Device Serial No Device name Product ID Version ID Model number Time Time zone Platform version APK bundle version Cisco Dialer version Emergency version Emergency version UebAPI version Load ID Device admin app Certificate Trust List (CTL) download Status URI Time MD5 hash	tcl254301c0 SEP10f9201932ed CP-860S V01 CP-860S Sat Jun 03 21:58:46 EDT 2023 America/New_York sip860 QKQ1.201230.002 1.9.0.2409 None 21.5.65593 21.3.64939-cisco 21.3.64946-cisco sip860-1.9.0.2409-65593 Downloader file not found http://10.195.19.43:6970/CTLSEP10F92019 32ED.tlv Sat Jun 03 19:57:56 EDT 2023 Download successful http://10.195.19.43:6970/TTLSEP10F920193 2ED.tlv Sat Jun 03 19:57:57 EDT 2023 a7af30890e5ce7c5b2f957cc959eca23					

Webex Calling

cisco	Device information Cisco Webex Wireless Phone CP-860 (10F920194A8D)				Device information Cisco Webex Wireless Phone CP-860 (10F920194A8D)		
Device information Network information Registration information Device logs	Device Serial No Device name Product ID Version ID Model number Time Time zone Platform version APK bundle version Cisco Dialer version Emergency version WebAPI version Load ID Profile Rule Profile Rule B	tcl254400ds 10f920194a8d CP-860 V01 CP-860 Mon Jun 05 16:24:19 EDT 2023 America/New_York sip860 QKQ1.201230.002 1.9.0.2409 None 21.5.65593 21.3.64939-cisco 22.1.68093-cisco sip860-1.8.0.2136-55928 https://cisco-int.bcld.webex.com/dms/CP86 0/860.xml Download successful Mon Jun 05 15:51:07 EDT 2023					
	Upgrade Rule	https://binaries.webex.com/cisco-860-stable/ 20221201164830/sip860-1.8.0.2136-55928.Jo ads Download successful Mon Jun 05 15:51:12 EDT 2023					

ネットワーク情報

Cisco Wireless Phone 840 および 860 はネットワーク情報を提供し、無線 LAN とネットワークの情報が表示 されます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<u>https://x.x.x.x</u>) にアクセスし、[**ネットワーク情報 (Network information)**]を選択します。

cisco	Netwo Cisco Webex Wireless	Network information Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)			
Device information	Active network interface	WLAN			
Network information	MAC address	10:f9:20:19:32:ed			
Registration information	Bluetooth address	10:f9:20:19:32:ec			
Device logs	SSID	baker			
	BSSID	c8:28:e5:ef:04:7a			
	Frequency	5GHz			
	DHCP server	64.101.49.191			
	DHCP	Yes			
	IP address	10.81.12.28			
	Subnet mask	255.255.255.0			
	Gateway	10.81.12.1			
	DNS server 1	64.102.6.247			
	DNS server 2	171.70.168.183			
	NTP server address	2.android.pool.ntp.org			

登録情報

Cisco Wireless Phone 840 および 860 は登録情報を提供し、電話機の DN と登録ステータス情報が表示されます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<u>https://x.x.x.x</u>) にアクセスし、**[登録情報 (Registration information)**]を選択します。

Cisco Unified Communications Manager

cisco	Cis	Registration information Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)				
Device information		UCM				
Network information	Phone DN	Shared Line	Auto Answer	Call Forward	Forwarded Address	Status
Registration information	1014	True	Disabled	Disabled		Registered
Device logs		SECONDARY REGISTRATION				
	Phone DN					
	SIP Server					
	Server Port	Server Port				
	Protocol					
	SIP Code					
	Status					
			CALL SE	RVER FEATUR	RES	
	Hunt Grou	p			Enabled	
	Hunt Grou	p Status			Logged out	
	Visual Voic	email			Enabled	
	Privacy				Enabled	

Webex Calling

cisco	Registration information Cisco Webex Wireless Phone CP-860 (10F920194A8D)					
Device information	WEBEX					
Network information	Line Number	Line Name	Shared Line	Call Forward	Forwarded Address	Status
Registration information	2675	bbqfx45w29	True	Disabled		Registered
Device logs	ACCOUNT INFO					
	SIP Server			199.19.196.177		
	Server Port			8934		
	Protocol			TLS		
	CALL SERVER FEATURES					
	Voicemail Disabled				4	
	Voicemail	CALL SERVER FEATURES Voicemail Disabled				

デバイス ログ

トラブルシューティング用のデバイスログは、Cisco Wireless Phone 840 または 860 の Web インターフェイ スから入手できます。

この情報を表示するには、Cisco Wireless Phone 840 または 860 の Web インターフェイス (<u>https://x.x.x.x</u>) にアクセスし、**[デバイスログ (Device logs)]**を選択します。

cisco	Device logs Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)	
Device information	Problem reports	+
Network information Registration information	Network traces	+
Device logs	Device logs	+
	WLAN	+
	Android reports	+
	QXDM	+

ログファイルタイプ([問題レポート (Problem reports)]、[ネットワークトレース (Network Traces)]、[デバイスログ (Device logs)]、[WLAN]、[Android レポート (Android reports)]、 [QXDM])の右側にある[+]記号をクリックすると、これらのログファイルが一覧表示され、ダウンロードでき ます。

1.6(0) リリースでは、Cisco Wireless Phone 840 および 860 を介して問題レポートとネットワークトレースを キャプチャできます。

問題レポートを生成するには、**[問題レポート (Problem reports)**]の **[PRT の生成 (Generate PRT)**] を選択します。

ネットワーク トレースをキャプチャするには、[Network traces] で [Start Packet Capture] を選択します。パケ ットのキャプチャを停止するには、[**パケットキャプチャの停止 (Stop Packet Capture)**] を選択します。

cisco	Device logs Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)	
Device information	Problem reports	-
<u>Network information</u> <u>Registration information</u> <u>Device logs</u>	Generate PRT 10f9201932ed_tcl254301c0_20230603_2255_LogBundle_1.9.0.2409.zip	
	Network traces	-
	Start packet capture <u>10f9201932ed_capture-2023-06-03_22.48.49-1685847063801.zip</u>	
	Device logs	+
	WLAN	+
	Android reports	+
	QXDM	+

WLAN 信号インジケータ

Cisco Wireless Phone 840 および 860 の WLAN 信号インジケータは、ディスプレイの右上隅に表示されます。 Cisco Wireless Phone 840 および 860 がアクセスポイントに接続されると、次のようにアイコンが グレーになります。



WLAN ネットワーク情報

Cisco Wireless Phone 840 および 860 の現在の WLAN ネットワーク情報を表示するには、[設定 (Settings)]、 [ネットワークとインターネット (Network and Internet)]、[Wi-Fi] の順に選択し、接続されている Wi-Fi ネット ワークを選択します。

設定済みの Wi-Fi ネットワークは、[削除 (Forget)]を選択して削除できます。



Cisco Wireless Phone 840 および 860 ワイヤレス LAN 導入ガイド

初期化

Cisco Wireless Phone 840 および 860 の設定を工場出荷時のデフォルトにリセットするには、[Settings]、 [System]、[Advanced]、[Reset options]、[Erase all data (factory reset)] の順に選択します。

消去されるすべてのデータを示す情報画面が表示されます。初期設定へのリセットを続行するには、**[すべての** データを消去(Erase all data)] を選択する必要があります。

確認画面が表示されたら、**[すべてのデータを消去 (Erase all data)**]を選択して、データを初期化します。 電話機が再起動し、工場出荷時の設定が復元された状態で起動します。



9:23 🗸	♥ 1	9:23 🗸		♥ 🔒
 Image: Constant of the second s	Ctory reset) m your phone's : d settings	Eras All of your perso downloaded app You can't	e all da nal inform is & SIMs, : undo this	ita? ation, including will be deleted. action.
• •		•	•	

Cisco Wireless Phone 840 または 860 を正しく起動できない場合は、次の手順でも初期化を開始できます。

- 電源ボタン(Cisco ワイヤレス電話 840 の場合は左上のボタン、Cisco ワイヤレス電話 860 の場合は右側の上から 2 番目のボタン)を押して電話機の電源をオフにし、[電源オフ (Power off)]
 を選択します。
- ・ 緊急ボタン (Cisco Wireless Phone 840 および Cisco Wireless Phone 860 の右上にある赤いボタン) を押したままにして、電話機の電源をオンにします。
- 赤い**緊急**ボタンを押したまま、電話機が振動するまで**電源**ボタンを押したままにしてから、**電源**ボタン を放します。
- ・ [ブートローダー (Bootloader)]画面が表示されたら、赤い緊急ボタンを放します。
- リカバリモードが表示されるまで音量小ボタンを押し、電源ボタンを押してそのオプションを 選択します。
- 電話機が再起動し、Android アイコンを表示された新しい画面に戻ります。
- この画面で電源ボタンを押したまま、[音量を上げる (Volume up)]ボタンをすばやく押して放し、[リカバリメニュー (Recovery Menu)]画面に入力します。
- ・ [リカバリメニュー (Recovery Menu)]が表示されたら、電源ボタンを放します。
- ・ 音量小ボタンを押して[データの消去/初期設定へのリセット(Wipe data/factory reset)]を強調表示し、電源ボタンを押してそのオプションを選択します。
- ・ 音量小ボタンを押して [データの初期化 (Factory data reset)]を強調表示し、電源ボタンを押してそのオプションを選択します。
- Reboot system now が強調表示されたら、電源ボタンを再度押します。
- Cisco Wireless Phone 840 または 860 が再起動し、工場出荷時の設定に復元されます。

注: Cisco Wireless Phone 840 または 860 が Google アカウントにサインインしている場合、電話機は工場 出荷時のワイプ保護が有効になっています。この保護は、設定された Google アカウントが削除されるまで有効 のままです。

工場出荷時設定へのリセット方法を使用する場合、デフォルト設定を復元した後は工場出荷時のワイプ保護をバ イパスすることはできません。

したがって、設定済みの Google アカウントを正常に削除するには、電話機の Android ユーザ インターフェイ スを使用して Cisco Wireless Phone 840 または 860 を初期設定にリセットする必要があります。

ログイン情報が不明で、電話機の Android ユーザーインターフェイスにアクセスして電話機を初期設定にリセットできない Google アカウントが設定されている場合、電話機は回復不能であり、保証の下で交換することは できません。

電話機画面のスクリーンショットのキャプチャ

Cisco Wireless Phone 840 または 860 の現在の表示は、電源ボタンを押して [スクリーンショット (Screenshot)]を選択することでキャプチャできます。

その他のマニュアル

Cisco Wireless Phone 840 および 860 データシート

https://www.cisco.com/c/en/us/products/se/2020/11/Collateral/datasheet-c78-744461.html

Cisco Wireless Phone 840 および 860 ユーザーガイド

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Cisco Wireless Phone 840 および 860 ユーザーガイド

https://www.cisco.com/content/en/us/td/docs/voice ip comm/cuipph/800-series/userguide/w800 b wireless-800-user-guide.html

Cisco Wireless Phone 840 および 860 クイックリファレンスガイド

https://www.cisco.com/c/dam/en/us/td/docs/voice ip comm/cuipph/800series/qrg/webex wireless phone 840 qrg.pdf https://www.cisco.com/c/dam/en/us/td/docs/voice ip comm/cuipph/800series/qrg/webex wireless phone 860 qrg.pdf

Cisco Wireless Phone 840 および 860

https://www.cisco.com/c/en/us/support/collaboration-endpoints/webex-wireless-phone/productsrelease-notes-list.html

Cisco Wireless Phone 840 および 860

https://software.cisco.com/download/home/286327931

Cisco Unified Communications Manager

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

Webex Calling

https://help.webex.com

Cisco Voice ソフトウェア

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

Cisco Wireless Phone 800 Series 開発者向けガイド

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

Real-Time Traffic over Wireless LAN

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

Cisco Unified Communications 設計ガイド

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-managercallmanager/products-implementation-design-guides-list.html

Cisco AireOS ワイヤレス LAN コントローラに関するドキュメント

https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installationand-configuration-guides-list.html

Cisco Catalyst IOS XE ワイヤレス LAN コントローラに関するドキュメント

https://www.cisco.com/c/ja_jp/support/wireless/catalyst-9800-series-wireless-controllers/productsinstallation-and-configuration-guides-list.html

Cisco Mobility Express に関するドキュメント

https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-andconfiguration-guides-list.html

Cisco Autonomous アクセス ポイントに関するドキュメント

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/atnms-ap-8x/configuration/guide/cgbook.html

Cisco Meraki ワイヤレス LAN に関するドキュメント

https://documentation.meraki.com

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

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商 標または商標です。シスコの商標の一覧は、<u>http://www.cisco.com/web/JP/trademark_statement.html</u> でご 確認いただけます。Third-party trademarks mentioned are the property of their respective owners. 「パート ナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するも のではありません。(1110R)。

本ドキュメントまたは Web サイトに掲載されているその他の商標はそれぞれの所有者に帰属します。「パート ナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するも のではありません。(0809R)。

Bluetooth の用語マークとロゴは、Bluetooth SIG, Inc. が所有する登録商標であり、かかる商標の Cisco
Systems, Inc.による使用はライセンスに基づいています。

© 2023 Cisco Systems, Inc. All rights reserved.