



Cisco IP 会議用電話 8832 アドミニストレーションガイド（Cisco Unified Communications Manager 用）

初版：2017 年 9 月 15 日

最終更新：2021 年 7 月 12 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2021 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

新規および変更情報 1

- ファームウェアリリース 14.1(1) の新規および変更情報 1
- ファームウェアリリース 14.0(1) の新規および変更情報 1
- ファームウェアリリース 12.8(1) の新規および変更情報 2
- ファームウェアリリース 12.7(1) の新規および変更情報 2
- ファームウェアリリース 12.1(1) の新規および変更情報 2
- ファームウェアリリース 12.5(1) SR3 の新規および変更情報 3
- ファームウェアリリース 12.5(1) SR2 の新規および変更情報 3
- ファームウェアリリース 12.5 (1) SR1 の新規および変更情報 3
- ファームウェアリリース 12.5(1) の新規および変更情報 4
- ファームウェアリリース 12.1(1) の新規および変更情報 4

第 1 部 :

Cisco IP 会議用電話について 7

第 2 章

Cisco IP 会議用電話ハードウェア 9

- Cisco IP 会議用電話 8832 9
- Cisco IP 会議用電話 8832 のボタンとハードウェア 11
 - 有線拡張マイク 12
 - ワイヤレス拡張マイク 13
- 関連資料 14
 - Cisco IP 会議用電話 8832 のマニュアル 14
 - Cisco Unified Communications Manager マニュアル 14
 - Cisco Unified Communications Manager Express マニュアル 15
 - Cisco ホステッド コラボレーション サービスのマニュアル 15

Cisco Business Edition 4000 のマニュアル	15
マニュアル、サポート、およびセキュリティ ガイドライン	15
シスコ製品のセキュリティの概要	15
用語の違い	16

第 3 章**技術的な詳細 17**

物理環境および動作環境に関する仕様	17
電話機の所要電力	18
停電	19
電力削減	20
ネットワーク プロトコル	20
Cisco Unified Communications Manager の連携	25
Cisco Unified Communications Manager Express の連携	25
ボイス メッセージ システムの連携	26
電話機設定ファイル	27
ネットワーク 輻輳時の電話機の挙動	27
アプリケーションプログラミング インターフェイス	27

第 II 部 :**Cisco IP 会議用電話の設置 29**

第 4 章**電話機の設置 31**

ネットワーク セットアップの確認	31
オンプレミス電話用のアクティベーションコードのオンボーディング	32
アクティベーション コード オンボーディングとモバイルおよびリモート アクセス	33
電話機の自動登録の有効化	34
デイジーチェーン モード	36
会議用電話の設置	36
会議用電話への給電方法	38
有線拡張マイクの取り付け	40
ワイヤレス拡張マイクの取り付け	41
ワイヤレス マイクの充電クレードルの取り付け	42

デジチェーンモードでの会議電話の設置	43
バックアップイメージから会議電話機を再起動する	44
セッアップメニューからの電話機のセッアップ	45
電話機パスワードの適用	47
電話機からのテキストとメニューの入力	47
ネットワークの設定	48
[ネットワークのセッアップ (Network Setup)] フィールド	48
[ドメイン名 (Domain Name)] フィールドの設定	54
電話機からのワイヤレス LAN の有効化	54
Cisco Unified Communications Manager からのワイヤレス LAN のセッアップ	55
電話機からのワイヤレス LAN のセッアップ	56
WLAN 認証試行の回数の設定	59
WLAN プロンプト モードの有効化	59
Cisco Unified Communications Manager を使用した Wi-Fi プロファイルの設定	60
Cisco Unified Communications Manager を使用した Wi-Fi グループの設定	62
電話機起動の確認	63
ユーザの電話モデルを変更	63
第 5 章	Cisco Unified Communications Manager での電話機の設置
	65
Cisco IP 会議用電話のセッアップ	65
電話機の MAC アドレスの決定	71
電話機の追加方法	71
電話機の個別の追加	72
BAT 電話テンプレートを使用した電話機の追加	72
Cisco Unified Communications Manager におけるユーザの追加	73
外部 LDAP ディレクトリからのユーザの追加	73
Cisco Unified Communications Manager にユーザを直接追加する	74
エンドユーザ グループにユーザを追加する	75
電話機とユーザの関連付け	76
Survivable Remote Site Telephony	76

第 6 章	セルフケアポータル の管理 81
	セルフケアポータル の概要 81
	セルフケアポータルへのユーザのアクセス の設定 82
	セルフケアポータル の表示のカスタマイズ 82

第 III 部 :	Cisco IP 会議用電話 の管理 83
-----------	------------------------------

第 7 章	Cisco IP 会議用電話 のセキュリティ 85
	Cisco IP 電話 セキュリティ の概要 85
	電話ネットワーク のセキュリティ強化機能 86
	サポート対象 のセキュリティ機能 87
	重要な証明書 のローカルでのセットアップ 92
	FIPS モード の有効化 93
	電話コール のセキュリティ 93
	セキュアな会議コール の特定 94
	セキュアな電話コール の識別 96
	割り込み の暗号化 97
	WLAN セキュリティ 97
	ワイヤレス LAN セキュリティ 100
	Cisco IP 電話 の管理ページ 101
	SCEP セットアップ 104
	802.1X 認証 105

第 8 章	Cisco IP 会議用電話 のカスタマイズ 107
	カスタム電話呼出音 107
	カスタム電話呼出音 のセットアップ 107
	カスタム呼出音 のファイル形式 108
	ダイヤル トーン のカスタマイズ 109

第 9 章	Cisco IP 会議用電話 の機能とセットアップ 111
-------	--------------------------------------

Cisco IP 電話 ユーザのサポート	111
マルチプラットフォーム フォンへの電話機の直接移行	112
新規ソフトキー テンプレートの設定	112
ユーザの電話サービスの設定	113
電話機の機能設定	114
すべての電話機の電話機能の設定	115
電話機グループの電話機能の設定	115
単一の電話機の電話機能の設定	116
プロダクト固有の設定	116
トランスポート層セキュリティ暗号を無効にする	132
Cisco IP 電話 での省電力のスケジュール	133
Cisco IP 電話 での EnergyWise のスケジュール	135
サイレントの設定	139
コールの転送通知のセットアップ	140
UCR 2008 のセットアップ	141
共通デバイス設定での UCR 2008 のセットアップ	142
共通の電話プロファイルでの UCR 2008 のセットアップ	143
エンタープライズ電話の設定での UCR 2008 のセットアップ	143
電話機での UCR 2008 のセットアップ	143
Expressway 経由でのモバイルおよび Remote Access	144
展開シナリオ	145
Expressway サインイン用ユーザ クレデンシャル パーシステントの設定	146
問題レポート ツール	146
カスタマー サポート アップロード URL の設定	147
回線のラベルの設定	149

 第 10 章

社内ディレクトリとパーソナル ディレクトリ	151
社内ディレクトリのセットアップ	151
パーソナル ディレクトリのセットアップ	151

 第 IV 部 :

Cisco IP 会議用電話のトラブルシューティング	153
----------------------------	-----

第 11 章

電話システムのモニタリング 155

電話システムの監視の概要 155

Cisco IP 電話のステータス 155

[電話の情報 (Phone Information)] ウィンドウの表示 156

[ステータス (Status)] メニューの表示 156

[ステータス メッセージ (Status Messages)] ウィンドウの表示 156

[ネットワーク統計情報 (Network Statistics)] ウィンドウの表示 165

[コール統計 (Call Statistics)] ウィンドウの表示 169

Cisco IP 電話の Web ページ 171

電話機の Web ページへのアクセス 172

[デバイス情報 (Device Information)] Web ページ 172

[ネットワークのセットアップ (Network Setup)] Web ページ 174

[イーサネット情報 (Ethernet Information)] Web ページ 182

[ネットワーク (Network)] の Web ページ 183

コンソールのログ、コアダンプ、ステータスメッセージ、およびデバッグ表示用 Web ページ 185

[ストリーミング統計 (Streaming Statistics)] Web ページ 185

XML での電話からの情報要求 188

CallInfo の出力例 189

LineInfo の出力例 190

ModeInfo の出力例 190

第 12 章

電話機のトラブルシューティング 193

一般的なトラブルシューティング情報 193

起動時の問題 196

Cisco IP 電話が通常の起動プロセスを実行しない 196

Cisco IP 電話が Cisco Unified Communications Manager に登録されない 197

電話機にエラー メッセージが表示される 197

電話機が TFTP サーバまたは Cisco Unified Communications Manager に接続できない 198

電話機が TFTP サーバに接続できない 198

電話機がサーバに接続できない	198
電話機が DNS を使用して接続できない	198
Cisco Unified Communications Manager および TFTP サービスの未作動	199
設定ファイルの破損	199
Cisco Unified Communications Manager での電話機の登録	199
Cisco IP 電話が IP アドレスを取得できない	200
電話機のリセットの問題	200
断続的なネットワークの停止によって電話機がリセットされる	200
DHCP の設定エラーによって電話機がリセットされる	201
誤ったスタティック IP アドレスによる電話機のリセット	201
ネットワーク使用量が多いときの電話機のリセット	201
意図的なリセットによる電話機のリセット	202
DNS エラーまたは他の接続の問題による電話機のリセット	202
電話機に電源が入らない	202
電話機が LAN に接続できない	203
Cisco IP 電話のセキュリティの問題	203
CTL ファイルの問題	203
認証エラー。電話機が CTL ファイルを認証できない	203
電話機が CTL ファイルを認証できない	203
CTL ファイルは認証されるが、他の設定ファイルが認証されない	204
ITL ファイルは認証されるが、他の設定ファイルが認証されない	204
TFTP 認証が失敗する	204
電話機が登録されない	205
署名付き設定ファイルが要求されない	205
オーディオに関する問題	205
通話路がない	205
音声の途切れ	206
デジチェーンモードの 1 台の電話機が機能しない	206
コールに関する一般的な問題	206
コールを確立できない	207
電話機が DTMF デジットを認識しないか、または数字が遅い	207

トラブルシューティング手順	207
Cisco Unified Communications Manager から電話機の問題レポートを作成する	208
TFTP 設定の確認	208
DNS または接続の問題の特定	209
DHCP 設定の確認	209
電話機の新しい設定ファイルの作成	210
DNS 設定の確認	211
サービスの開始	211
Cisco Unified Communications Manager からのデバッグ情報の制御	212
トラブルシューティングに関する追加情報	213

第 13 章**メンテナンス 215**

会議電話の再起動またはリセット	215
会議電話の再起動	215
電話メニューからの会議電話の設定のリセット	215
キーパッドから会議電話を工場出荷時の初期状態にリセットする	216
音声品質のモニタリング	217
音声品質のトラブルシューティングのヒント	217
Cisco IP 電話のクリーニング	218

第 14 章**各言語ユーザのサポート 221**

Unified Communications Manager Endpoints Locale Installer	221
国際コールのロギングのサポート	221
言語の制限	222



第 1 章

新規および変更情報

- ・ [ファームウェアリリース 14.1\(1\) の新規および変更情報 \(1 ページ\)](#)
- ・ [ファームウェアリリース14.0\(1\) の新規および変更情報 \(1 ページ\)](#)
- ・ [ファームウェアリリース 12.8\(1\) の新規および変更情報 \(2 ページ\)](#)
- ・ [ファームウェア リリース 12.7\(1\) の新規および変更情報 \(2 ページ\)](#)
- ・ [ファームウェア リリース 12.1\(1\) の新規および変更情報 \(2 ページ\)](#)
- ・ [ファームウェア リリース 12.5\(1\) SR3 の新規および変更情報 \(3 ページ\)](#)
- ・ [ファームウェア リリース 12.5\(1\) SR2 の新規および変更情報 \(3 ページ\)](#)
- ・ [ファームウェアリリース12.5 \(1\) SR1の新規および変更情報 \(3 ページ\)](#)
- ・ [ファームウェア リリース 12.5\(1\) の新規および変更情報 \(4 ページ\)](#)
- ・ [ファームウェア リリース 12.1\(1\) の新規および変更情報 \(4 ページ\)](#)

ファームウェアリリース 14.1(1) の新規および変更情報

次の情報は、ファームウェアリリース 14.1(1) の新規または変更された情報です。

機能	新機能および変更情報
プロキシ TFTP サポート用の SIP OAuth	電話ネットワークのセキュリティ強化機能 (86 ページ)
移行読込のない電話機の移行	マルチプラットフォーム フォンへの電話機の直接移行 (112 ページ)

ファームウェアリリース14.0(1) の新規および変更情報

表 1: 新規および変更情報

機能	新機能および変更情報
コール パーク モニタリングの機能拡張	プロダクト固有の設定 (116 ページ)

機能	新機能および変更情報
SIP OAuth の機能拡張	電話ネットワークのセキュリティ強化機能 (86 ページ)
MRA の OAuth の機能拡張	Expressway 経由でのモバイルおよび Remote Access (144 ページ)
ユーザ インターフェイスの強化	Survivable Remote Site Telephony (76 ページ)

ファームウェア リリース 14.0 では、電話機は DTLS 1.2 をサポートしています。DTLS 1.2 には、Cisco Adaptive Security Appliance (ASA) リリース 9.10 以降が必要です。ASA の VPN 接続用に DTLS の最低バージョンを構成します。詳細については、*ASDM ブック 3: Cisco ASA シリーズ VPN ASDM 7.12 コンフィギュレーション ガイド* (<https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>) をご覧ください。

ファームウェアリリース 12.8(1) の新規および変更情報

以下の情報は、ファームウェアリリース 12.8 (1) に対して新規または変更事項です。

機能	新しいまたは変更されたコンテンツ
電話データの移行	ユーザの電話モデルを変更 (63 ページ)
[Web アクセス (Web Access)] フィールドに関する情報の追加	プロダクト固有の設定 (116 ページ)

ファームウェア リリース 12.7(1) の新規および変更情報

ファームウェアバージョン12.7(1) では、管理ガイドのアップデートの必要はありませんでした。

ファームウェア リリース 12.1(1) の新規および変更情報

ファームウェアバージョン12.6 (1) は、管理ガイドのアップデートは必要ありませんでした。

ファームウェア リリース 12.5(1) SR3 の新規および変更情報

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルへのすべての参照が更新されています。

表 2: ファームウェア リリース 12.5 (1) SR3 に関する Cisco IP 電話 8832 アドミニストレーションガイドのリビジョン

改訂	更新されたセクション
アクティベーションコードオンボーディングとモバイルおよび Remote Access へのサポート	アクティベーションコードオンボーディングとモバイルおよびリモートアクセス (33 ページ)
Cisco Unified Communications Manager の問題レポートツール使用のサポート。	Cisco Unified Communications Manager から電話機の問題レポートを作成する (208 ページ)

ファームウェア リリース 12.5(1) SR2 の新規および変更情報

ファームウェアリリース12.5 (1) SR2に管理ガイドのアップデートは必要ありませんでした。

ファームウェアリリース 12.5 (1) SR2 は、ファームウェアリリース 12.5 (1)およびファームウェア 12.5 (1) SR1 に代わるものです。ファームウェアリリース 12.5 (1)およびファームウェアリリース 12.5 (1) SR1 は、ファームウェアリリース 12.5 (1) を優先して使用が延期されています。

ファームウェアリリース12.5 (1) SR1の新規および変更情報

次の表に、ファームウェアリリース12.5 (1) SR1をサポートするためにCisco Unified Communications Manager用 Cisco IP 会議用電話 8832アドミニストレーションガイドの変更点について説明します。

表 3: ファームウェアリリース 12.5 (1) SR1に関する Cisco IP 会議用電話 8832 アドミニストレーションガイドの改訂

改訂	新規または更新されたセクション
楕円曲線のサポート	サポート対象のセキュリティ機能 (87 ページ)

ファームウェア リリース 12.5(1) の新規および変更情報

次の表に、ファームウェアリリース12.5 (1) をサポートするためにCisco Unified Communications Manager用 Cisco IP 会議用電話 8832アドミニストレーションガイドの変更点について説明します。

表 4: ファームウェアリリース 12.5 (1) に関する Cisco IP 会議用電話 8832アドミニストレーションガイドの改訂

改訂	新規または更新されたセクション
Cisco Unified Communications Manager Expressでのささやきページのサポート	Cisco Unified Communications Manager Express の連携 (25 ページ)
TLS 暗号の無効化のサポート	プロダクト固有の設定 (116 ページ)
桁間タイマーT.302拡張のための一括ダイヤルのサポート。	プロダクト固有の設定 (116 ページ)

ファームウェア リリース 12.1(1) の新規および変更情報

次の表に、ファームウェアリリース 12.1 (1) をサポートするための『Cisco IP 会議用電話 8832 アドミニストレーションガイド (Cisco Unified Communications Manager 向け)』の変更点について説明します。

改訂	新規または更新されたセクション
Cisco IP 会議用電話 8832 PoE インジェクタ のサポート	<ul style="list-style-type: none"> • 電話機の所要電力 (18 ページ) • 会議用電話への給電方法 (38 ページ) • 会議用電話の設置 (36 ページ)
ワイヤレス マイクのサポート	<ul style="list-style-type: none"> • Cisco IP 会議用電話 8832 (9 ページ) • ワイヤレス拡張マイク (13 ページ) • ワイヤレス拡張マイクの取り付け (41 ページ) • ワイヤレス マイクの充電クレードルの取り付け (42 ページ)

改訂	新規または更新されたセクション
デジチェーンのサポート	<ul style="list-style-type: none"> • Cisco IP 会議用電話 8832 (9 ページ) • デジチェーン モード (36 ページ) • デジチェーンモードでの会議電話の設置 (43 ページ) • デジチェーンモードの 1 台の電話機が機能しない (206 ページ)
Cisco IP 会議用電話 8832非 PoE イーサネット インジェクタ のサポート	<ul style="list-style-type: none"> • 会議用電話の設置 (36 ページ) • 会議用電話への給電方法 (38 ページ)
Wi-Fi のサポート	<ul style="list-style-type: none"> • 会議用電話の設置 (36 ページ) • 会議用電話への給電方法 (38 ページ) • [ドメイン名 (Domain Name)] フィールドの設定 (54 ページ) • 電話機からのワイヤレス LAN の有効化 (54 ページ) • Cisco Unified Communications Manager からのワイヤレス LAN のセットアップ (55 ページ) • 電話機からのワイヤレス LAN のセットアップ (56 ページ) • WLAN 認証試行の回数の設定 (59 ページ) • WLAN プロンプト モードの有効化 (59 ページ) • Cisco Unified Communications Manager を使用した Wi-Fi プロファイルの設定 (60 ページ) • Cisco Unified Communications Manager を使用した Wi-Fi グループの設定 (62 ページ)
Expressway 経由モバイルおよび Remote Access のサポート	<ul style="list-style-type: none"> • Expressway 経由でのモバイルおよび Remote Access (144 ページ) • 展開シナリオ (145 ページ) • Expressway サインイン用ユーザ クレデンシャル パーシステントの設定 (146 ページ)

改訂	新規または更新されたセクション
Webサーバーアクセス用のTLS 1.2の有効化または無効化のサポート。	プロダクト固有の設定 (116 ページ)
G722.2 AMR-WB オーディオコーデックのサポート	<ul style="list-style-type: none">• Cisco IP 会議用電話 8832 (9 ページ)• コール統計のフィールド (169 ページ)



第 1 部

Cisco IP 会議用電話 について

- [Cisco IP 会議用電話ハードウェア \(9 ページ\)](#)
- [技術的な詳細 \(17 ページ\)](#)



第 2 章

Cisco IP 会議用電話ハードウェア

- [Cisco IP 会議用電話 8832](#) (9 ページ)
- [Cisco IP 会議用電話 8832 のボタンとハードウェア](#) (11 ページ)
- [関連資料](#) (14 ページ)
- [マニュアル、サポート、およびセキュリティガイドライン](#) (15 ページ)
- [用語の違い](#) (16 ページ)

Cisco IP 会議用電話 8832

Cisco IP 会議用電話 8832 と 8832NR は、人を中心としたコミュニケーションを強化します。中規模から大規模の会議室や役員室で 360 度の範囲をカバーする高解像度 (HD) のオーディオ性能を実現します。また、全二重の双方向ワイドバンド (G.722) オーディオハンズフリースピーカーにより、高品質のサウンドを実現しています。この電話機では、シンプルなソリューションを提供することで、大部分の会議室が抱える課題に答えます。

図 1: Cisco IP 会議用電話 8832



会議電話機は、360 度のカバレッジを実現する感度の良いマイクを備えています。このカバレッジにより、普通の声で話しても、最大 3 メートル離れた場所から相手にはっきりと聞こえます。

す。また、電話機やその他のワイヤレス デバイスからの干渉に抵抗する技術が採用されており、妨害のないクリアな通信を確実に実現します。電話機はカラー画面と、さまざまなユーザ機能を操作するためのソフトキー ボタンを備えています。ベースユニットのみの場合、会議電話は、6.1 x 6.1 m の部屋で 10 人までのカバレッジを実現できます。

2つの有線拡張マイクを使用できます。拡張マイクをベースユニットから離れた場所に設置することで、より大きな会議室に対応できるカバレッジを実現できます。ベースユニットと有線拡張マイクを使用した場合、会議電話は、6.1 x 10 m の部屋で 22 人までのカバレッジを実現できます。

電話機は、オプションのワイヤレス拡張マイク 2 個のセットもサポートしています。ベースユニットとワイヤレス拡張マイクを使用した場合、会議電話は、6.1 x 12.2 m の部屋で 26 人までのカバレッジを実現できます。6.1 x 12.2 m の部屋をカバーするには、各マイクをベースから最大 3 m の距離に配置することを推奨します。

部屋のカバレッジを高めるため、2つの基本ユニットを接続することができます。この設定ではオプションのデジチェーンキットが必要で、2つの拡張マイク（有線またはワイヤレス、組み合わせは不可）をサポートできます。デジチェーンキットで有線マイクを使用する設定では、6.1 X 15.2 m（20 X 50 フィート）までの部屋と最大 38 人のカバレッジを提供します。デジチェーンキットでワイヤレス マイクを使用する設定では、6.1 X 17.4 m（20 X 57 フィート）までの部屋と最大 42 人のカバレッジを提供します。

Cisco IP 会議用電話 8832NR（非無線）バージョンでは、Wi-Fi や無線拡張マイクや Bluetooth はサポートされません。

他のデバイスと同様に、Cisco IP 電話 は設定し、管理する必要があります。これらの電話機は、次のコーデックのエンコードとデコードを行います。

- G.711 a-law
- G.711 mu-law
- G.722
- G.722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus



注意 セル方式の電話、携帯電話、GSM 電話、または双方向ラジオを Cisco IP 電話のすぐ近くで使用すると、相互干渉が発生することがあります。詳細については、干渉が発生するデバイスの製造元のマニュアルを参照してください。

Cisco IP 電話は、コール転送や転送、リダイヤル、短縮ダイヤル、会議コール、ボイス メッセージング システムへのアクセスなど、従来のテレフォニー機能を提供します。Cisco IP 電話では、さらにその他の各種の機能も提供します。

Cisco IP 電話は、他のネットワーク デバイスと同様に、Cisco Unified Communications Manager および IP ネットワークの他の部分にアクセスできるように設定する必要があります。DHCP を使用すると、電話機上で設定する内容が少なくなります。ただし、お使いのネットワークで必要な場合は、IP アドレス、TFTP サーバ、サブネット情報などの情報を手動で設定できます。

Cisco IP 電話は、IP ネットワーク上の他のサービスやデバイスと連携することで、高度な機能を提供できます。たとえば、Cisco Unified Communications Manager を社内の Lightweight Directory Access Protocol 3 (LDAP3) 標準ディレクトリと統合すると、ユーザが同僚の連絡先情報を IP 電話で直接検索できるようになります。XML を使用すると、天気予報、株価情報、商品相場などの Web ベースの情報にユーザがアクセスできるようになります。

さらに、Cisco IP 電話はネットワーク デバイスであるため、詳細なステータス情報を電話機から直接取得することができます。この情報は、ユーザが IP 電話を使用しているときに生じた問題をトラブルシューティングするのに役立ちます。また、アクティブコールに関する統計情報や、ファームウェアのバージョンも電話機で取得できます。

Cisco IP 電話を IP テレフォニー ネットワークで機能させるには、IP 電話を Cisco Catalyst スイッチなどのネットワーク デバイスに接続する必要があります。また、コールを送受信する前に、Cisco IP 電話を Cisco Unified Communications Manager システムに登録する必要があります。

Cisco IP 会議用電話 8832 のボタンとハードウェア







次の図は Cisco IP 会議用電話 8832 です。

図 2: Cisco IP 会議用電話 8832 の各ボタンと機能



次の表に、Cisco IP 会議用電話 8832 の各ボタンを示します。

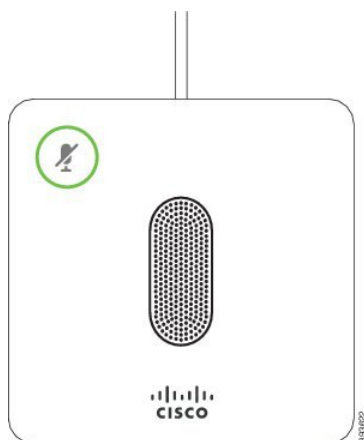
表 5: Cisco IP 会議用電話 8832 の各ボタン

1	LED バー	<p>コール状態を示します。</p> <ul style="list-style-type: none"> • 緑、点灯：アクティブ コール • 緑（点滅）：着信コール • 緑（速い点滅）：保留中のコール • 赤、点灯：ミュート中のコール
2	拡張マイク ポート	有線拡張マイク ケーブルはポートに差し込みます。
3	ミュート バー	[ミュート ]：マイクロフォンのオン/オフを切り替えます。マイク音声ミュートになっているとき、LED バーは赤色に点灯します。
4	ソフトキー ボタン	[ミュート ]：機能とサービスにアクセスします。
5	ナビゲーションバーと [選択 (Select)] ボタン	 <p>[ミュート ]：メニューをスクロールして項目を強調表示し、強調表示された項目を選択できます。</p>
6	[音量 (Volume)] ボタン：	 <p>[ミュート ]：スピーカーフォンの音量（オフフック）と着信音の音量（オンフック）を調整します。</p> <p>音量を変更するとLEDバーが白く点灯し、音量の変化を表示します。</p>

有線拡張マイク

Cisco IP 会議用電話 8832 は、オプションキットで用意されている有線拡張マイク 2 個をサポートします。大きな会議室または混雑している会議室で、拡張マイクを使用します。最適な効果を得るために、携帯電話から3フィート（0.91メートル）から7フィート（2.1メートル）の間にマイクを置くことをお勧めします。

図 3: 有線拡張マイク



通話時は、[ミュート (Mute)] ボタンの周りの拡張マイク LED が緑色に点灯します。

マイク音声ミュートになっているとき、LED バーは赤色です。[ミュート (Mute)] ボタンを押すと、電話機と拡張マイクはミュートされます。

関連トピック

[有線拡張マイクの取り付け](#) (40 ページ)

ワイヤレス拡張マイク

Cisco IP 会議用電話 8832 は、オプションキットで充電クレードルと一緒に用意されている 2 つの拡張ワイヤレスマイクをサポートしています。ワイヤレスマイクを充電クレードルの上に配置して充電すると、クレードルの LED が白く点灯します。

図 4: ワイヤレスマイクロフォン

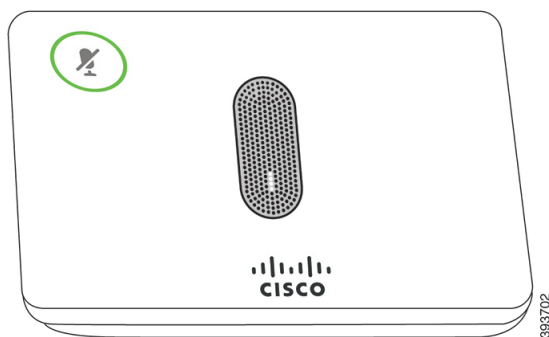
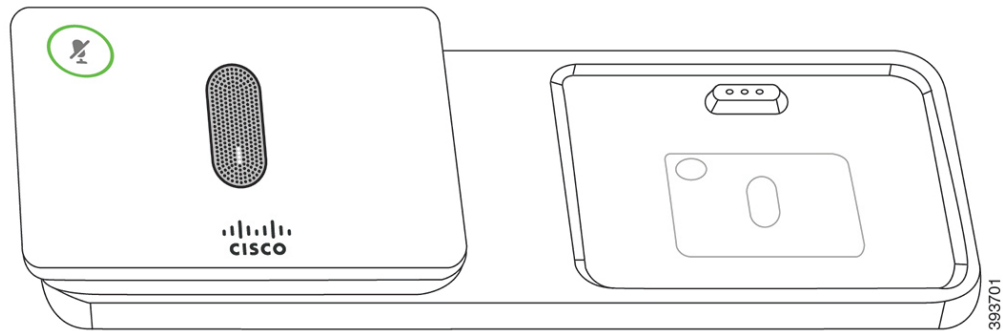


図 5: 充電クレードルに載せたワイヤレス マイク



会議電話での通話時は、[ミュート (Mute)]  ボタンの周りの拡張マイク LED が緑色に点灯します。

マイクをミュートにすると、LED が赤く点灯します。[ミュート (Mute)] ボタンを押すと、電話機と拡張マイクはミュートされます。

電話機がワイヤレスマイク（たとえばワイヤレスマイク 1）とペアリングされていて、充電器にワイヤレスマイクを接続している場合、[詳細表示 (Show detail)] ソフトキーを押すとマイクの充電レベルが表示されます。

電話機がワイヤレスマイクとペアリングされている時に有線マイクを接続すると、ワイヤレスマイクのペアリングが解除され、電話機は有線マイクとペアリングされます。有線マイクが接続されたことを示す通知が電話機の画面上に表示されます。

関連トピック

[ワイヤレス拡張マイクの取り付け](#) (41 ページ)

[ワイヤレスマイクの充電クレードルの取り付け](#) (42 ページ)

関連資料

関連情報を入手するには、以下のセクションを参照してください。

Cisco IP 会議用電話 8832 のマニュアル

お使いの言語、電話機モデル、およびコール制御システムに固有のマニュアルは、Cisco IP Phone 7800 Series の [製品サポート](#) ページで確認してください。

Cisco Unified Communications Manager マニュアル

[製品のサポート](#) ページで『Cisco Unified Communications Manager Documentation Guide』およびお使いの Cisco Unified Communications Manager リリースに特化したその他の文書を参照してください。

Cisco Unified Communications Manager Express マニュアル

お使いの言語、電話機モデル、および [Cisco Unified Communications Manager Express](#) 向けの資料を参照してください。

Cisco ホステッド コラボレーション サービスのマニュアル

Cisco Hosted Collaboration Solution ドキュメンテーション ガイドおよびご使用の *Cisco Hosted Collaboration Solution* リリースバージョン用の他の資料を参照してください。次の URL から入手できます。

<https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html>

Cisco Business Edition 4000 のマニュアル

Cisco Business Edition 4000 ドキュメンテーション ガイドおよびご使用の *Cisco Business Edition 4000* リリースバージョン用の他の資料を参照してください。次の URL から入手できます。

<https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/tsd-products-support-series-home.html>

マニュアル、サポート、およびセキュリティガイドライン

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。Cisco の新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。Cisco は現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国の法律の対象となります。Cisco の暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意したものと見なされます。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、<https://www.bis.doc.gov/policiesandregulations/ear/index.htm> をご覧ください。

用語の違い

このドキュメントの用語 Cisco IP 電話 には、Cisco IP 会議用電話 8832 が含まれています。

次の表に、『Cisco IP 会議用電話 8832 ユーザ ガイド』、『Cisco IP Conference Phone 8832 シリーズアドミニストレーションガイド (Cisco Unified Communications Manager 用)』、および Cisco Unified Communications Manager のマニュアルの間に見られる用語の違いを示します。

表 6:用語の違い

ユーザ ガイド	アドミニストレーション ガイド
メッセージ インジケータ	メッセージ受信インジケータ (MWI)
ボイスメール システム	ボイス メッセージ システム



第 3 章

技術的な詳細

- 物理環境および動作環境に関する仕様 (17 ページ)
- 電話機の所要電力 (18 ページ)
- ネットワーク プロトコル (20 ページ)
- Cisco Unified Communications Manager の連携 (25 ページ)
- Cisco Unified Communications Manager Express の連携 (25 ページ)
- ボイス メッセージ システムの連携 (26 ページ)
- 電話機設定ファイル (27 ページ)
- ネットワーク 輻輳時の電話機の挙動 (27 ページ)
- アプリケーション プログラミング インターフェイス (27 ページ)

物理環境および動作環境に関する仕様

次の表に、会議電話機の物理仕様と動作環境仕様を示します。

表 7: 物理仕様および動作環境仕様

仕様	値または範囲
動作温度	0 ~ 40 °C (32 ~ 104 °F)
動作相対湿度	10 ~ 90% (結露しないこと)
保管温度	-10 ~ 60 °C (14 ~ 140 °F)
高さ(T) :	278 mm (10.9 インチ)
幅	278 mm (10.9 インチ)
奥行	61.3 mm (2.4 インチ)
重量	1852 g (4.07 ポンド)

仕様	値または範囲
電源	<p>PoE インジェクタを介した IEEE PoE クラス 3。この電話機は、IEEE 802.3af および 802.3at スイッチ ブレードの両方に対応しており、Cisco Discovery Protocol と Link Layer Discovery Protocol - Power over Ethernet (LLDP-PoE) の両方をサポートします。</p> <p>接続された LAN スイッチが PoE をサポートしていない場合、他のオプションには非 PoE イーサネット インジェクタが含まれます。WiFi を導入するには、Cisco IP 会議用電話 8832 電源アダプタが必要です。</p>
セキュリティ機能	セキュア ブート
ケーブル	USB-C
距離要件	イーサネット仕様では、各電話機とスイッチ間のケーブル長を 100 メートル以内と想定しています。

詳細については、次の『Cisco IP 会議用電話 8832 データシート』を参照してください：
<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html>

電話機の所要電力

Cisco IP 会議用電話 8832 では、以下の電源を使用できます。

- を使用した PoE (Power over Ethernet) の導入 Cisco IP 会議用電話 8832 PoE インジェクタ
- を使用した非 PoE イーサネットの導入 Cisco IP 会議用電話 8832 非 PoE イーサネット インジェクタ
- Cisco IP 会議用電話 8832 電源アダプタを使用した Wi-Fi の導入

表 8: Cisco IP 会議用電話電源のガイドライン

電源の種類	ガイドライン
<p>PoE 電源 : USB-C ケーブルを介して電話機に接続されている Cisco IP 会議用電話 8832 PoE インジェクタ または Cisco IP 会議用電話 8832 イーサネット インジェクタ を通じて電力を供給。</p>	<p>Cisco IP 会議用電話 8832 PoE インジェクタ または Cisco IP 会議用電話 8832 イーサネット インジェクタ を使用している場合は、スイッチのバックアップ電源を確保して、停電時でも電話機の動作が中断しないようにします。</p> <p>スイッチ上で実行されている CatOS または IOS のバージョンが、予定している電話機配置をサポートしていることを確認します。オペレーティング システムのバージョンに関する情報については、スイッチのマニュアルを参照してください。</p> <p>PoE を使用して給電される電話機を設置する場合は、インジェクタを LAN に接続した後、USB-C ケーブルを電話機に接続してください。PoE を使用した電話機を撤去する場合は、電話機から USB-C ケーブルを取り外した後、アダプタの電源を切断してください。</p>
<p>外部電源</p> <ul style="list-style-type: none"> • を使用した非 PoE イーサネットの導入 Cisco IP 会議用電話 8832 非 PoE イーサネット インジェクタ • Cisco IP 会議用電話 8832 電源アダプタを使用した Wi-Fi の導入 • Cisco IP 会議用電話 8832 イーサネット インジェクタ および Cisco IP 会議用電話 8832 電源アダプタを使用した、非 PoE イーサネットの導入 	<p>外部電源を使用して給電される電話機を設置する場合は、インジェクタを電源とイーサネットに接続した後、USB-C ケーブルを電話機に接続してください。外部電源を使用した電話機を撤去する場合は、電話機から USB-C ケーブルを取り外した後、アダプタの電源を切断してください。</p>

停電

電話機を経由して緊急サービスにアクセスするには、その電話機が電力を受信する必要があります。停電が発生した場合、電源が復旧するまでは、電話サービスおよび緊急コールサービスダイヤルが機能しません。電源の異常および障害が発生した場合は、装置をリセットまたは再設定してから、電話サービスおよび緊急コールサービスダイヤルを利用する必要があります。

電力削減

省電力モードまたは EnergyWise (Power Save Plus) モードを使用して、Cisco IP 電話が消費する電力を削減できます。

省電力 (Power Save)

PowerSave モードでは、電話機が使用されていないときにはスクリーンのバックライトが消灯します。電話機は、スケジュールされた期間が終了するかユーザがいずれかのボタンを押すまで、省電力モードのままです。

Power Save Plus (EnergyWise)

Cisco IP 電話は Cisco EnergyWise (Power Save Plus) モードをサポートします。ネットワークに EnergyWise (EW) コントローラが含まれている場合 (たとえば、Cisco スイッチで EnergyWise 機能が有効になっている場合)、これらの電話機をスケジュールに基づいてスリープ状態 (電源オフ) およびウェイク状態 (電源オン) になるように設定して、電力消費をさらに抑えることができます。

EnergyWise は、電話機ごとに有効または無効に設定します。EnergyWise を有効にした場合は、他のパラメータとともに、スリープと復帰の時刻を設定します。これらのパラメータは、電話機設定 XML ファイルの一部として電話機へ送信されます。

関連トピック

[Cisco IP 電話 での省電力のスケジュール \(133 ページ\)](#)

[Cisco IP 電話 での EnergyWise のスケジュール \(135 ページ\)](#)

ネットワーク プロトコル

Cisco IP 会議用電話 8832 では、音声通信に必要な複数の業界標準およびシスコのネットワークプロトコルがサポートされています。次の表に、電話機でサポートされるネットワークプロトコルの概要を示します。

表 9: Cisco IP 会議用電話サポートのネットワークプロトコル

ネットワーク プロトコル	目的	使用方法に関する特記事項
ブートストラップ プロトコル (BootP)	BOOTP は、電話機などのネットワーク デバイスを有効化し、IP アドレスなどの確かなスタートアップ情報を見つけます。	—

ネットワーク プロトコル	目的	使用方法に関する特記事項
Cisco Discovery Protocol (CDP)	<p>CDPは、シスコの製造するすべての装置で動作するデバイス検出プロトコルです。</p> <p>デバイスは、CDPを使用して自身の存在をネットワーク内の他のデバイスにアドバタイズし、ネットワーク内の他のデバイスの情報を受信できます。</p>	<p>電話機は CDP を使用して、ポートの電源管理ごとの Auxiliary VLAN ID などの情報と Cisco Catalyst スイッチの Quality of Service (QoS) 設定情報を通信します。</p>
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP は、IP アドレスを動的に確保して、ネットワークデバイスに割り当てるものです。</p> <p>DHCP を使用すると、IP 電話をネットワークに接続すれば、その電話機が機能するようになります。IP アドレスを手動で割り当てたり、ネットワークパラメータを別途設定したりする必要はありません。</p>	<p>DHCP は、デフォルトでは有効になっています。無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネットマスク、ゲートウェイ、および TFTP サーバを手動で設定する必要があります。</p> <p>DHCP のカスタム オプション 150 を使用することを推奨します。この方式では、TFTP サーバの IP アドレスをオプション値として設定しています。サポートされている DHCP 設定を追加するには、お使いの Cisco Unified Communications Manager のリリースにあるドキュメンテーションを確認してください。</p> <p>(注) オプション 150 を使用できない場合は、DHCP オプション 66 を使用します。</p>
Hypertext Transfer Protocol (HTTP)	<p>HTTP は、インターネットや Web 経由で情報を転送し、ドキュメントを移送するための標準プロトコルです。</p>	<p>電話機は、XML サービス、プロビジョニング、アップグレード、トラブルシューティングの目的で HTTP を使用します。</p>
Hypertext Transfer Protocol Secure (HTTPS)	<p>Hypertext Transfer Protocol Secure (HTTPS) は、サーバの暗号化とセキュアな ID を確保できるように、ハイパーテキスト転送プロトコルと SSL/TLS プロトコルを組み合わせたものです。</p>	<p>HTTP と HTTPS の両方をサポートしている Web アプリケーションでは、2 つの URL が設定されています。HTTPS をサポートする電話機では、HTTPS URL を選択します。</p> <p>サービスへの接続が HTTPS 経由である場合、鍵のアイコンがユーザに表示されます。</p>

ネットワーク プロトコル	目的	使用方法に関する特記事項
IEEE 802.1X	<p>IEEE 802.1X 標準規格では、クライアントサーバベースのアクセス制御と、認証されていないクライアントがパブリックにアクセスできるポートから LAN に接続するのを規制する認証プロトコルを定義します。</p> <p>802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL) トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。</p>	<p>電話機は、認証方式 EAP-FAST および EAP-TLS をサポートする IEEE 802.1X 標準規格を実装します。</p> <p>電話機で 802.1X 認証が有効である場合は、ボイス VLAN を無効にします。</p>
インターネット プロトコル (IP)	<p>IP は、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。</p>	<p>IP を使用して通信するには、ネットワーク デバイスに対して、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。</p> <p>Dynamic Host Configuration Protocol (DHCP) を使用できる電話機を使用している場合、IP アドレス、サブネット、ゲートウェイ ID は自動的に割り当てられます。DHCP を使用しない場合は、個々の電話機がある場所で、これらのプロパティを手動で割り当てる必要があります。</p> <p>電話機は、IPv6 アドレスをサポートしています。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。</p>
リンク層検出プロトコル (LLDP)	<p>LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコデバイスとサードパーティ製デバイスでサポートされています。</p>	<p>電話機は PC ポートの LLDP をサポートしています。</p>

ネットワーク プロトコル	目的	使用方法に関する特記事項
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED は、音声製品用に開発された、LLDP 標準の拡張です。	<p>電話機は、SW ポートで LLDP-MED をサポートし、次のような情報を通信します。</p> <ul style="list-style-type: none"> • ボイス VLAN の設定 • デバイスの検出 • 電源管理 • インベントリ管理 <p>LLDP-MED サポートの詳細については、次の URL にある <i>LLDP-MED and Cisco Discovery Protocol</i> ホワイトペーパーを参照してください。</p> <p>https://www.cisco.com/c/en/us/td/docs/wireless/voice/9000/lldp-med.html</p>
Real-Time Transport Protocol (RTP)	RTP は、インタラクティブな音声やビデオなどのリアルタイムデータをデータネットワーク経由で転送するための標準プロトコルです。	電話機は RTP プロトコルを使用して、他の電話機およびゲートウェイとの間でリアルタイム音声トラフィックを送受信します。
Real-Time Control Protocol (RTCP)	RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッタ、遅延、ラウンドトリップ遅延など）を伝送します。	RTCP は、デフォルトでは有効になっています。
Session Description Protocol (SDP)	SDP は SIP プロトコルの一部であり、2 つのエンドポイント間で接続が確立されている間に、どのパラメータを使用できるかを決定します。会議は、会議に参加するすべてのエンドポイントがサポートする SDP 機能だけを使用して確立されます。	コーデックタイプ、DTMF 検出、コンフォートノイズなどの SDP 機能は、通常は運用中の Cisco Unified Communications Manager またはメディアゲートウェイでグローバルに設定されています。SIP エンドポイントの中には、これらのパラメータをエンドポイント上で設定できるものがあります。

ネットワーク プロトコル	目的	使用方法に関する特記事項
Session Initiation Protocol (SIP)	SIP は、IP を介したマルチメディア会議のためのインターネット技術特別調査委員会 (IETF) 標準です。SIP は、アプリケーション層の ASCII ベースの制御プロトコルであり (RFC 3261 で規定)、2 つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。	他の Voice over IP (VoIP) プロトコルと同様に、SIP はパケットテレフォニーネットワークにおけるシグナリングとセッション管理の機能に対応するよう設計されています。シグナリングは、ネットワーク境界を越えて通話情報を伝送する機能です。セッション管理は、エンドツーエンドコールの属性を制御する機能です。
Secure Real-Time Transfer protocol (SRTP)	SRTP は、Real-Time Protocol (RTP) Audio/Video Profile の拡張で、RTP パケットと Real-Time Control Protocol (RTCP) パケットの整合性を保証して、2 つのエンドポイント間のメディアパケットの認証、整合性、および暗号化を実現します。	電話機は、メディア暗号化のために SRTP を使用します。
Transmission Control Protocol (TCP)	TCP は、接続型の転送プロトコルです。	電話機は TCP を使用して Cisco Unified Communications Manager に接続し、XML サービスにアクセスします。
Transport Layer Security (TLS)	TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。	セキュリティが実装されている場合、Cisco Unified Communications Manager でセキュアな登録をするときに、電話機は TLS プロトコルを使用します。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。
Trivial File Transfer Protocol (TFTP)	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 電話機で TFTP を使用すると、電話機のタイプ固有の設定ファイルを入手できます。	TFTP では、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバで自動的に識別できません。DHCP サーバが指定する以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークのセットアップ (Network Setup)] メニューを使用して、TFTP サーバの IP アドレスを手動で割り当てる必要があります。 詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

ネットワーク プロトコル	目的	使用方法に関する特記事項
User Datagram Protocol (UDP)	UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。	UDP は RTP ストリームにのみ使用されます。電話機の SIP シグナリングは UDP をサポートしていません。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

Cisco Unified Communications Manager の連携

Cisco Unified Communications Manager は、業界標準のオープンなコール処理システムです。Cisco Unified Communications Manager ソフトウェアは、従来の PBX 機能を企業の IP ネットワークに統合して、電話機間のコールを確立および切断します。Cisco Unified Communications Manager は、電話会議やルート プランなどの機能で必要になるテレフォニー システムのコンポーネント（電話機、アクセス ゲートウェイ、およびリソース）を管理します。また、Cisco Unified Communications Manager には、次の機能もあります。

- 電話機のファームウェアの提供
- TFTP と HTTP サービスのを使用した証明書信頼リスト (CTL) および Identity Trust List (ITL)
- 電話機の登録
- コールの保存。この機能により、プライマリ Communications Manager と電話機間でシグナリングが消失してもメディア セッションが続行されます。

この章で説明されている電話と連携するための Cisco Unified Communications Manager の設定方法については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。



- (注) 設定しようとする電話のモデルが、Cisco Unified Communications Manager Administration の [Phone Type] ドロップダウン リストに表示されない場合は、Cisco.com にアクセスして、使用している Cisco Unified Communications Manager の最新のデバイスパッケージをインストールします。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

Cisco Unified Communications Manager Express の連携

電話が Cisco Unified Communications Manager Express (Unified CME) と連携する場合は、電話機を CME モードにする必要があります。

ユーザが会議機能を起動すると、タグにより、電話機はローカルまたはネットワーク ハードウェアのどちらかの会議ブリッジを使用できます。

電話では、次のアクションはサポートされていません。

- [転送 (Transfer)] -接続されたコール転送のシナリオでのみサポートされます。
- [会議 (Conference)] -接続されたコール転送のシナリオでのみサポートされます。
- 参加 -[会議 (Conference)]ボタンまたはフックフラッシュアクセスを使用してサポートされます。
- 保留 -[保留 (Hold)]を使用してサポートされます。
- 割り込みおよびマージ - サポートされていません。
- 直接転送 - サポートされていません。
- 選択 - サポートされていません。

ユーザは、異なる回線にわたる会議および転送コールを作成できません。

Unified CME は、ウィスパーページングとも呼ばれるインターコムコールをサポートします。しかし、通話中は電話でページが拒否されます。

ボイス メッセージ システムの連携

Cisco Unified Communications Manager を使用すると、Cisco Unity Connection ボイス メッセージング システムなどのさまざまなボイス メッセージング システムと統合できます。各種システムと統合できるため、特定のシステムの使用法に関する情報をユーザに提供する必要があります。

ユーザがボイスメールに転送できるようにするには、*xxxxxダイヤルパターンを設定し、それを[すべてボイスメールに転送]として設定します。詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

次の情報を、各ユーザに提供してください：

- ボイス メッセージ システム アカウントへのアクセス方法。

Cisco Unified Communications Manager を使用して、Cisco IP 電話の [Messages] ボタンを設定しておく必要があります。

- ボイス メッセージ システムにアクセスするための初期パスワード。

すべてのユーザが使用できるボイス メッセージ システムのデフォルト パスワードを設定します。

- ボイス メッセージの受信が電話機でどのように示されるか。

Cisco Unified Communications Manager を使用して、メッセージ受信インジケータ (MWI) メソッドを設定します。

電話機設定ファイル

電話機設定ファイルは TFTP サーバに保存されており、Cisco Unified Communications Manager に接続するためのパラメータを定義しています。通常、電話機のリセットが必要となるような変更を Cisco Unified Communications Manager に加えると、その変更内容は、電話機設定ファイルに自動的に反映されます。

設定ファイルには、電話機がどのイメージ ロードを実行するかも記述されています。このイメージロードが電話機にロードされているものと異なる場合、電話機は TFTP サーバにアクセスし、必要なロード ファイルを要求します。

Cisco Unified Communications Manager Administration でセキュリティ関連の設定値を設定すると、電話機のコンフィギュレーションファイルに機密情報が保存されます。設定ファイルのプライバシーを確保するには、そのファイルを暗号化用に設定する必要があります。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。Cisco Unified Communications Manager でリセットおよび登録されるたびに、電話機は設定ファイルを要求します。

次の条件を満たしている場合、電話機は、TFTP サーバにある XmlDefault.cnf.xml という名前のデフォルト設定ファイルにアクセスします。

- Cisco Unified Communications Manager で自動登録を有効にした。
- 該当する電話機が、Cisco Unified Communications Manager データベースにまだ追加されていない。
- 該当する電話機を初めて登録する。

ネットワーク輻輳時の電話機の挙動

ネットワークパフォーマンスの低下の原因となるものは、電話の音声に影響を及ぼすため、場合によっては、通話が中断される可能性があります。ネットワーク パフォーマンスの低下は、次のような原因が考えられます。

- 内部ポート スキャンやセキュリティ スキャンなどの管理タスク
- サービス拒否攻撃など、ネットワーク上で発生した攻撃

アプリケーション プログラミング インターフェイス

シスコは、サードパーティ製アプリケーション開発者によってテストされ、シスコから認定されたサードパーティ製アプリケーションによる電話機の API 使用をサポートしています。認定されていないアプリケーション間のやりとりに関連する電話の問題は、サードパーティが対処する必要があり、シスコでは対処しません。

シスコ認定のサードパーティ製アプリケーション/ソリューションのサポート モデルについては、[シスコ ソリューション パートナー プログラムの Web サイト](#)で詳細を参照してください。



第 II 部

Cisco IP 会議用電話の設置

- [電話機の設置 \(31 ページ\)](#)
- [Cisco Unified Communications Manager での電話機の設置 \(65 ページ\)](#)
- [セルフケアポータルでの管理 \(81 ページ\)](#)



第 4 章

電話機の設置

- ネットワーク セットアップの確認 (31 ページ)
- オンプレミス電話用のアクティベーションコードのオンボーディング (32 ページ)
- アクティベーションコード オンボーディングとモバイルおよびリモート アクセス (33 ページ)
- 電話機の自動登録の有効化 (34 ページ)
- デイジーチェーン モード (36 ページ)
- 会議用電話の設置 (36 ページ)
- セットアップメニューからの電話機のセットアップ (45 ページ)
- 電話機からのワイヤレス LAN の有効化 (54 ページ)
- 電話機起動の確認 (63 ページ)
- ユーザの電話モデルを変更 (63 ページ)

ネットワーク セットアップの確認

新しい IP テレフォニー システムを導入するときは、システム管理者とネットワーク管理者がいくつかの初期設定作業を実施して、ネットワークを IP テレフォニー サービス用に準備する必要があります。Cisco IP テレフォニー ネットワークのセットアップと設定のチェックリストについては、特定の Cisco Unified Communications Manager リリース向けのドキュメントを参照してください。

電話機がネットワーク内のエンドポイントとして正常に動作するためには、電話ネットワークが特定の要件を満たしている必要があります。1 つの要件は適切な帯域幅です。電話機は、Cisco Unified Communications Manager への登録時には、推奨される 32 kbps を超える帯域幅を必要とします。QoS 帯域幅を設定する際は、これ以上の帯域幅要件を考慮してください。詳細については、『Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)』またはそれ以降 (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html) を参照してください。



(注) 電話機は、Cisco Unified Communications Managerから取得した日時を表示します。電話機に表示される時間は、Cisco Unified Communications Managerの時間と 10 秒以内の誤差がある場合があります。

手順

ステップ 1 次の要件を満たすように VoIP ネットワークを設定します。

- ルータおよびゲートウェイ上で VoIP が設定されている。
- Cisco Unified Communications Manager がネットワークにインストールされ、コール処理用に設定されている。

ステップ 2 次のいずれかをサポートするようにネットワークをセットアップします。

- DHCP のサポート
- 手動による IP アドレス、ゲートウェイ、およびサブネット マスクの割り当て

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

オンプレミス電話用のアクティベーションコードのオンボーディング

アクティベーションコードオンボーディングを使用すると、自動登録なしで新しい電話機をすばやく設定できます。この方法では、次のいずれかを使用して電話のオンボーディングプロセスを制御します。

- Cisco Unified Communications Manager 一括管理ツール (BAT)
- [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] インターフェイスを開きます。
- Administrative XML Web Service (AXL)

からこの機能を有効にする **デバイス情報 Phone Configuration** ページのセクション。選択する **オンボーディング用のアクティベーションコード** を要求するこの機能を 1 つのオンプレミス電話に適用したい場合。

電話を登録する前に、ユーザはアクティベーションコードを入力する必要があります。アクティベーションコードオンボーディングは、個々の電話機、電話機のグループ、またはネットワーク全体に適用できます。

ユーザは 16 桁のアクティベーションコードを入力するだけなので、ユーザが自分の電話機に搭載するのは簡単な方法です。コードは手動で入力するか、電話機にビデオカメラがある場合は QR コードを入力します。ユーザにこの情報を提供するには、安全な方法を使用することをお勧めします。ユーザーに電話機が割り当てられている場合、その情報は **Self Care Portal** で利用できます。監査ログは、ユーザがポータルからコードにアクセスしたときに記録します。

アクティベーションコードは 1 回しか使用できず、デフォルトでは 1 週間後に期限切れになります。コードの有効期限が切れた場合は、ユーザに新しいコードを提供する必要があります。

製造元設置証明書 (MIC) とアクティベーションコードが検証されるまで電話を登録できないため、このアプローチはネットワークを安全に保つための簡単な方法であることがわかります。この方法は、自動登録電話サポート (TAPS) または自動登録のためのツールを使用しないため、オンボード電話を一括処理するのにも便利な方法です。オンボーディングの速度は、1 秒あたり 1 台の電話、または 1 時間あたり約 3600 台の電話です。電話機は、Cisco Unified Communications Manager の管理機能、管理 XML Web サービス (AXL)、または BAT を使用して追加できます。

既存の電話機は、アクティベーションコードのオンボーディング用に設定された後にリセットされます。アクティベーションコードが入力され、電話機の MIC が確認されるまで、登録は行われません。あなたがそれを実装する前にあなたがアクティベーションコードオンボーディングに向かって動いていることを現在のユーザに知らせてください。

詳細については、*Cisco Unified Communications Manager* および *IM and Presence Service* リリース 12.0(1) 以降のアドミニストレーションガイドを参照します。

アクティベーションコードオンボーディングとモバイルおよびリモート アクセス

リモートユーザ用の Cisco IP 電話を導入する場合は、モバイルおよび **Remote Access** でアクティベーションコードオンボーディングを使用できます。この機能は、自動登録が不要な場合に、オフプレミスの電話機を導入するための安全な方法です。ただし、オンプレミスの場合は自動登録用に、電話機をオフプレミスの場合はアクティベーションコードとして設定できます。この機能は、オンプレミスの電話機のアクティベーションコードオンボーディングと似ていますが、オフプレミスの電話機でもアクティベーションコードを利用できます。

モバイルおよび **Remote Access** のアクティベーションコードのオンボーディングでは、Cisco Unified Communications Manager 12.5 (1) SU1 以降、および Cisco Expressway X12.5 以降が必要です。また、スマートライセンスも有効にする必要があります。

この機能は、Cisco Unified Communications Manager の管理から有効にすることができます。ただし、次の点に注意してください。

- この機能は、[電話の設定 (Phone Configuration)] ページの [デバイス情報 (Device Information)] セクションから有効にします。
- この機能を1つのオンプレミス電話に適用したい場合は、**オンボーディング用のアクティベーションコードを要求する**を選択します。
- アクティベーション オンボーディング機能を1つのオフプレミス電話に適用したい場合は、**MRA 経由でアクティベーションコードを許可する および オンボーディング用のアクティベーションコードを要求する**を選択します。電話機がオンプレミスの場合は、モバイルおよび Remote Access モードに変更され、Expressway を使用します。電話機が Expressway にアクセスできない場合、その電話機がオフプレミスになるまで登録されません。

詳細については、次のマニュアルを参照してください。

- *Cisco Unified Communications Manager* および *IM and Presence Service* リリース 12.0(1) アドミニストレーションガイド
- Cisco Expressway X12.5 以降用 *Cisco Expressway* 経由のモバイル & Remote Access

電話機の自動登録の有効化

Cisco IP 電話は、コールの処理に Cisco Unified Communications Manager を必要とします。Cisco Unified Communications Manager を正しくセットアップして、電話機を管理し、コールを適切にルーティングおよび処理するには、該当する Cisco Unified Communications Manager リリースまたは Cisco Unified Communications Manager Administration の状況依存ヘルプを参照してください。

Cisco IP 電話を設置する前に、電話機を Cisco Unified Communications Manager データベースに追加する方法を選択しておく必要があります。

電話機を設置する前に自動登録を有効にしておくこと、次のことが可能になります。

- 事前に電話機から MAC アドレスを収集することなく、電話機を追加する。
- Cisco IP 電話を IP テレフォニー ネットワークに物理的に接続したときに、その電話機を Cisco Unified Communications Manager データベースに自動的に追加する。自動登録中に、Cisco Unified Communications Manager は連続する電話番号の中から次に使用可能なものを電話機に割り当てます。
- 電話機を Cisco Unified Communications Manager データベースにすばやく登録し、電話番号などの設定を Cisco Unified Communications Manager から変更する。
- 自動登録された電話機を新しい場所に移動し、電話番号を変更しないまま別のデバイスプールに割り当てる。

自動登録は、デフォルトでは無効になっています。自動登録を使用しない方がよい場合もあります。たとえば、電話機に特定の電話番号を割り当ててる場合や、Cisco Unified Communications Manager とのセキュア接続を使用する場合です。自動登録の有効化の詳細については、該当す

る Cisco Unified Communications Manager リリースのマニュアルを参照してください。Cisco CTL クライアントを通じてクラスタを混合モードに設定すると、自動登録が自動的に無効になりますが、これを有効に設定できます。Cisco CTL クライアントを通じてクラスタを非セキュアモードに設定すると、自動登録は自動的に有効になりません。

自動登録と TAPS (Tool for AutoRegistered Phones Support) を使用すると、MAC アドレスを最初に電話機から収集しなくても、電話機を追加することができます。

TAPS は、一括管理ツール (BAT) と連携して、Cisco Unified Communications Manager データベースにダミー MAC アドレスを使用して追加された一連の電話機をアップデートします。TAPS を使用して、MAC アドレスを更新し、デバイス向けに事前定義された設定をダウンロードします。

自動登録と TAPS は、ネットワークに追加する電話機が 100 台未満の場合に使用することを推奨します。100 台を超える電話機をネットワークに追加するには、一括管理ツール (BAT) を使用します。

TAPS を利用するには、管理者またはエンドユーザが TAPS の電話番号をダイヤルして、音声プロンプトに従います。このプロセスが完了した後、電話機には電話番号とその他の設定値が含まれており、電話機は正しい MAC アドレスを使用して Cisco Unified Communications Manager の管理ページで更新されます。

ネットワークに Cisco IP 電話を接続する前に、自動登録が Cisco Unified Communications Manager の管理ページで有効になっていて、正しく設定されていることを確認します。自動登録の有効化および設定の詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

TAPS が機能するためには、Cisco Unified Communications Manager の管理ページで自動登録を有効にする必要があります。

手順

- ステップ 1 Cisco Unified Communications Manager の管理で、[システム (System)] > [Cisco Unified CM] をクリックします。
- ステップ 2 [検索 (Find)] をクリックして、必要なサーバを選択します。
- ステップ 3 [自動登録の情報 (Auto-registration Information)] で、これらのフィールドを設定します。
 - [ユニバーサルデバイステンプレート(Universal Device Template)]
 - [ユニバーサル回線テンプレート(Universal Line Template)]
 - [開始電話番号(Starting Directory Number)]
 - 終了電話番号 (Ending Directory Number)
- ステップ 4 [この Cisco Unified CM では自動登録は無効にする (Auto-registration Disabled on this Cisco Unified Communications Manager)] チェックボックスをオフにします。
- ステップ 5 [保存 (Save)] をクリックします。

ステップ6 [設定の適用 (Apply Config)] をクリックします。

デジチェーンモード

スマートアダプタと、部屋の中の音声カバレッジエリアを拡大するためにデジチェーンキットに用意されているUSB-Cケーブルを使用して、2つの会議電話を接続することができます。

デジチェーンモードでは、どちらのユニットも、電源アダプタに接続されているスマートアダプタから電力を供給されます。ユニットごとに1つだけ外部マイクを使用できます。有線マイクとユニットのペア、またはワイヤレスマイクとユニットのペアのいずれかを使用できますが、これらのマイクを組み合わせることはできません。いずれかのユニットに有線マイクを接続した場合、同じユニットに接続しているワイヤレスマイクのペアを解除します。アクティブな通話があるたびに、両方のユニットの端末画面上のLEDとメニューオプションが同期されます。

関連トピック

[デジチェーンモードでの会議電話の設置 \(43 ページ\)](#)

[デジチェーンモードの1台の電話機が機能しない \(206 ページ\)](#)

会議用電話の設置

電話機をネットワークに接続すると、電話機の起動プロセスが開始され、電話機がCisco Unified Communications Managerに登録されます。DHCPサービスを無効にした場合は、電話機のネットワーク設定を構成する必要があります。

自動登録を使用した場合は、電話機をユーザに関連付ける、ボタンテーブルやディレクトリ番号を変更するなど、電話機の特定の設定情報をアップデートする必要があります。

電話機は、接続されると、新しいファームウェアのロードを電話機にインストールする必要があるかどうかを判定します。

会議電話をデジチェーン接続モードで使用する場合は、[デジチェーンモードでの会議電話の設置 \(43 ページ\)](#) を参照してください。

始める前に

Cisco Unified Communications Manager に最新のファームウェアがインストールされていることを確認します。ここで、更新されたデバイスのパッケージがあるかどうかを確認します。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

手順

ステップ 1 電話機の電源を次の中から選択します。

- を使用した PoE (Power over Ethernet) の導入 Cisco IP 会議用電話 8832 PoE インジェクタ
- を使用した非 PoE イーサネットの導入 Cisco IP 会議用電話 8832非 PoE イーサネット インジェクタ
- Cisco IP 会議用電話 8832 電源アダプタを使用した Wi-Fi の導入

詳細については、[会議用電話への給電方法 \(38 ページ\)](#) を参照してください。

ステップ 2 電話機をスイッチに接続します。

- PoE を使用する場合：
 1. LAN ポートにイーサネット ケーブルを差し込みます。
 2. イーサネット ケーブルのもう一方の端を Cisco IP 会議用電話 8832 PoE インジェクタ または Cisco IP 会議用電話 8832 イーサネット インジェクタ に差し込みます。
 3. USB-C ケーブルを使用してインジェクタを会議電話に接続します。
- PoE を使用しない場合：
 1. Cisco IP 会議用電話 8832 イーサネット インジェクタ を使用している場合、電源アダプタを電源コンセントに差し込みます。
 2. USB-C ケーブルを使用して電源アダプタをイーサネットインジェクタに接続します。
または
Cisco IP 会議用電話 8832非 PoE イーサネット インジェクタ を使用している場合、電源コンセントに差し込みます。
 3. イーサネット ケーブルを非 PoE インジェクタまたはイーサネット インジェクタに差し込みます。
 4. LAN ポートにイーサネット ケーブルを差し込みます。
 5. USB-C ケーブルを使用して、非 PoE インジェクタまたはイーサネット インジェクタを会議電話に接続します。
- Wi-Fi を使用する場合：
 1. Cisco IP 会議用電話 8832 電源アダプタを電源コンセントに差し込みます。
 2. USB-C ケーブルを使用して、電源アダプタを会議電話に接続します。

(注) 電源アダプタの代わりに、非PoEイーサネットインジェクタを使用して、電話機に電力を供給できます。ただし、LANケーブルを抜く必要があります。イーサネット接続が利用できない場合、電話機は wi-fi にのみ接続します。

- ステップ 3** 電話機の起動プロセスをモニタします。この手順により、電話機が正しく設定されていることを確認できます。
- ステップ 4** 自動登録を使用しない場合は、電話機のセキュリティ設定を手動で構成します。
- ステップ 5** 電話機で、Cisco Unified Communications Manager に保存されている現在のファームウェアイメージにアップグレードできます。
- ステップ 6** 電話機を使用してコールを発信し、電話機と機能が正常に動作することを確認します。
- ステップ 7** ユーザに対して、電話機の使用法および電話機のオプションの設定方法を通知します。この手順により、ユーザは十分な情報を得て、Cisco 電話を適切に使用できるようになります。

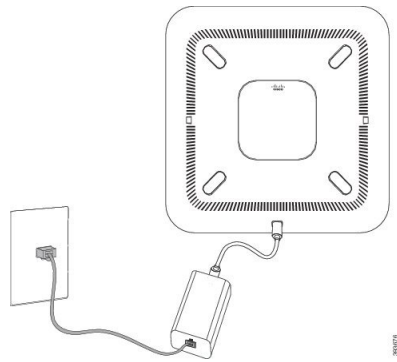
会議用電話への給電方法

会議用電話には、次のいずれかの電源からの給電が必要です。

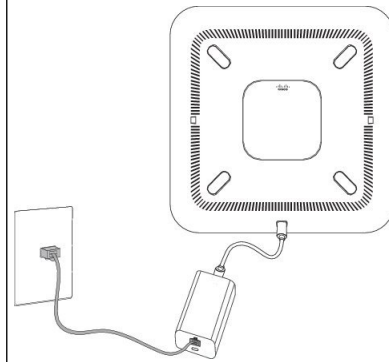
- Power over Ethernet (PoE)
 - 北米
 - Cisco IP 会議用電話 8832 PoE インジェクタ
 - Cisco IP 会議用電話 8832 イーサネット インジェクタ
 - 北米以外 —Cisco IP 会議用電話 8832 PoE インジェクタ
- 非 PoE イーサネット
 - 北米
 - Cisco IP 会議用電話 8832非 PoE イーサネット インジェクタ
 - Cisco IP 会議用電話 8832 イーサネット インジェクタ と Cisco IP 会議用電話 8832 (電源アダプタがコンセントに接続されている)。
 - 北米以外 —Cisco IP 会議用電話 8832非 PoE イーサネット インジェクタ
- Wi-Fi- コンセントに接続されている Cisco IP 会議用電話 8832 電源アダプタを使用します。

図 6: 会議用電話の PoE 電源オプション

次の図は、2 つの PoE 電源オプションを示しています。



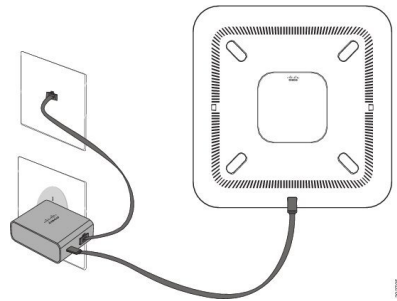
Cisco IP 会議用電話 8832 PoE インジェクタ
と PoE 電源オプション



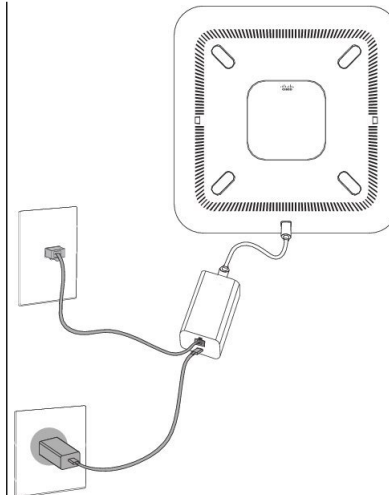
Cisco IP 会議用電話 8832 イーサネット インジェ
クタ と PoE 電源オプション

図 7: 会議電話のイーサネット電源オプション

次の図は、2つのイーサネット電源オプションを示しています。



Cisco IP 会議用電話 8832 非 PoE イーサネット
インジェクタ とイーサネット電源オプ
ション



Cisco IP 会議用電話 8832 イーサネット インジェ
クタ とイーサネット電源オプション

図 8: 会議電話の Wi-Fi ネットワーク接続時の電源オプション

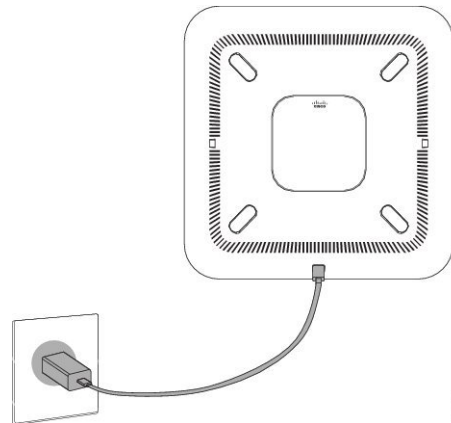
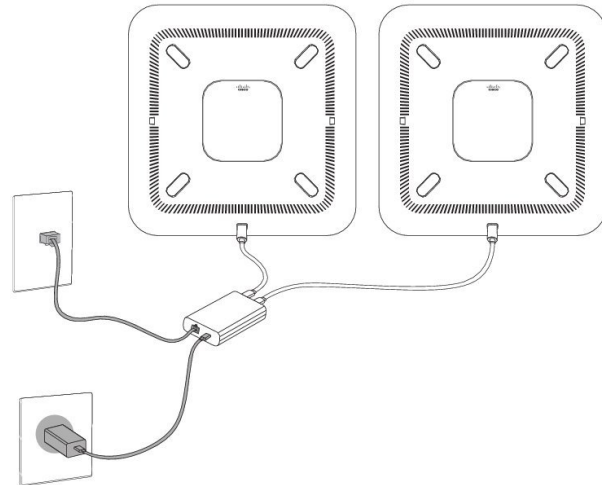


図 9: デイジーチェーンモードでの電源オプション

次の図は、電話機をデイジーチェーンモードで接続した場合の電源オプションです。



有線拡張マイクの取り付け

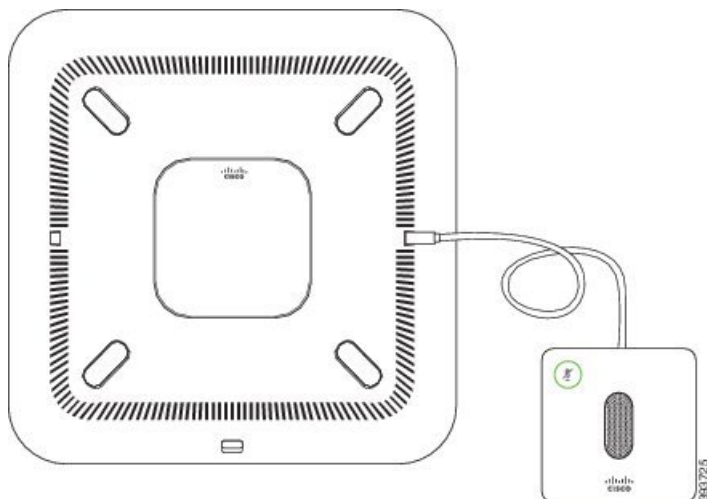
電話は、2つの有線拡張マイクを備えたオプションキットをサポートしています。マイクは電話機から最大 2.13 m (7 フィート) まで延長できます。最適な効果を得るために、携帯電話から 3 フィート (0.91 メートル) から 7 フィート (2.1 メートル) の間にマイクを置きます。

手順

- ステップ 1 電話の側面のポートにマイク ケーブルの端を差し込みます。
- ステップ 2 マイクのケーブルを希望する位置まで延長します。

次の図は、有線拡張マイクの取り付けを示しています。

図 10: 有線拡張マイクの取り付け



ワイヤレス拡張マイクの取り付け

会議電話には、2つのワイヤレス拡張マイクを接続するオプションがあります。



- (注) 電話機と一緒に2つの有線マイクまたは2つのワイヤレスマイクを使用できますが、2種類のマイクを組み合わせることはできません。

電話機の通話時は、拡張マイクのLEDが緑色に点灯します。拡張マイクをミュートするには、[ミュート (Mute)] キーを押します。マイクをミュートにすると、LEDが赤く点灯します。マイクのバッテリーが少なくなると、電池残量表示 LED がすばやく点滅します。

始める前に

ワイヤレス拡張マイクを取り付ける前に、有線拡張マイクを取り外します。有線およびワイヤレス拡張マイクは同時に使用できません。

手順

- ステップ 1** マイクを配置するテーブルの表面で、テーブルマウントプレートを置く位置を決めます。
- ステップ 2** テーブルマウントプレートの底面に付いている両面テープの接着面を剥がします。テーブルマウントプレートを配置し、テーブルの表面に接着します。
- ステップ 3** テーブルマウントプレートにマイクを取り付けます。マイクには磁石が埋め込まれているので、ユニットが所定の場所にくっつきます。

マイクと取り付けしたテーブルマウントは、必要に応じてテーブルの表面上の別の場所に移動できます。ユニットを保護するため、移動する際は慎重に行ってください。

関連トピック

[ワイヤレス拡張マイク](#) (13 ページ)

[ワイヤレスマイクの充電クレードルの取り付け](#) (42 ページ)

ワイヤレスマイクの充電クレードルの取り付け

ワイヤレスマイクの電池を充電するには、充電クレードルを使用します。

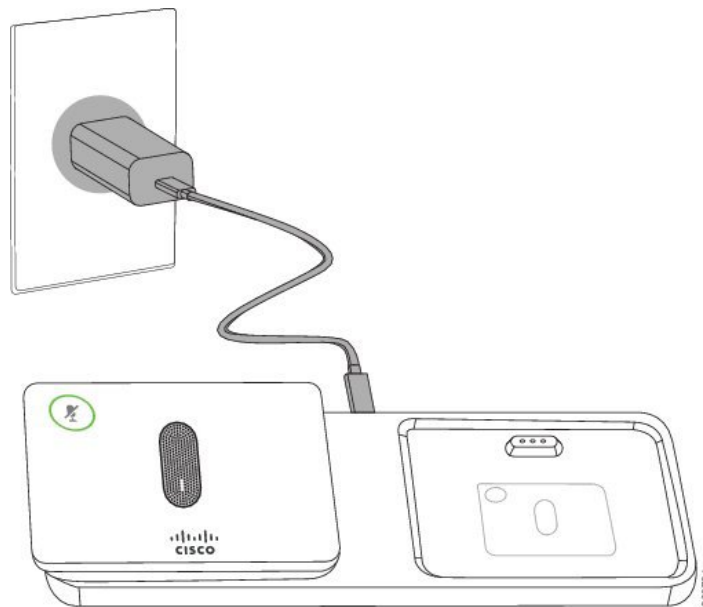
手順

ステップ 1 充電クレードルの電源アダプタを電源コンセントに差し込みます。

ステップ 2 充電クレードルに USB-C ケーブルの一方の端を差し込み、もう一方の端を電源アダプタに差し込みます。

次の図は、ワイヤレスマイク充電クレードルの取り付けを示しています。

図 11: ワイヤレスマイクの充電クレードルへの充電



関連トピック

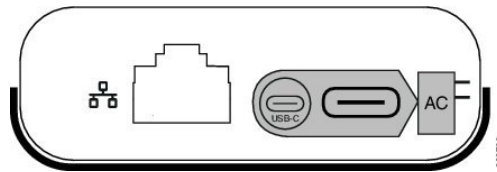
[ワイヤレス拡張マイク](#) (13 ページ)

[ワイヤレス拡張マイクの取り付け](#) (41 ページ)

デジチェーンモードでの会議電話の設置

デジチェーンキットにはスマートアダプタ、短いLANケーブル、2本の長くてより太いUSB-Cケーブル、および短くて薄いUSB-Cケーブルが含まれています。デジチェーンモードでは、会議電話をコンセントからの外部電源に接続する必要があります。スマートアダプタを使用して電話機を接続する必要があります。長いUSB-Cケーブルは電話機に到達して、短いものは電源アダプタに到達します。電源アダプタとLANポートをスマートアダプタに接続するときは、次の図を参照してください。

図 12: スマートアダプタの電源ポートと LAN ポート



ユニットごとに1つのみマイクを使用できます。



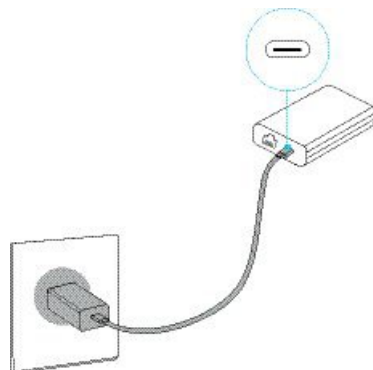
- (注) 電話機と一緒に2つの有線マイクまたは2つのワイヤレスマイクを使用できますが、2種類のマイクを組み合わせることはできません。

電源アダプタ用のUSB-Cケーブルは、電話機に接続されているUSB-Cケーブルよりも薄型です。

手順

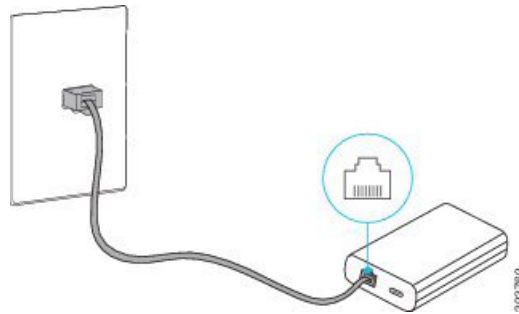
- ステップ 1** 電源アダプタを電源コンセントに差し込みます。
- ステップ 2** 電源アダプタからスマートアダプタには、短くて薄型のUSB-Cケーブルを接続します。

図 13: 電源コンセントに接続されたスマートアダプタのUSBポート



- ステップ 3** 必須: イーサネットケーブルをスマートアダプタとLANポートに接続します。

図 14: 壁面のコンセントの LAN ポートに接続されたスマートアダプタの LAN ポート

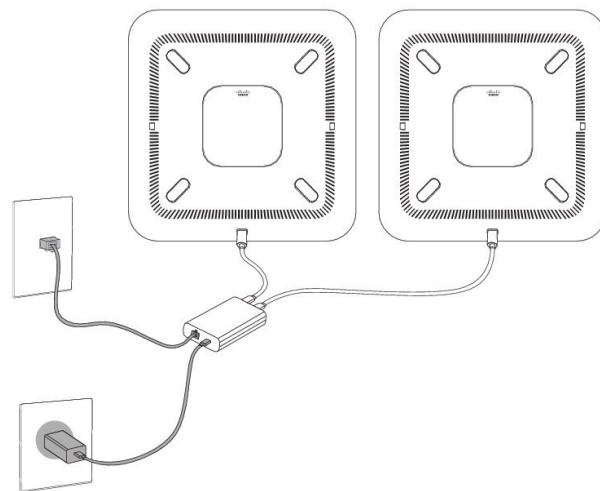


ステップ 4 より長くて太い USB-C ケーブルを使用して、1 台目の電話機を スマート アダプタ に接続します。

ステップ 5 USB-C ケーブルを使用して、2 台目の電話機を スマート アダプタ に接続します。

次の図に、デージーチェーン モードで会議電話を 設置する 様子 を示 します。

図 15: デージーチェーンモードでの会議電話機の設置



関連トピック

[デージーチェーンモード](#) (36 ページ)

[デージーチェーンモードの 1 台の電話機が機能しない](#) (206 ページ)

バックアップイメージから会議電話機を再起動する

Cisco IP 会議用電話 8832 には、デフォルトイメージが侵害されたときに電話機を回復するための 2 番目のバックアップイメージがあります。

バックアップイメージから電話機を再起動するには、次の手順を実行します。

手順

-
- ステップ 1** 電源を会議電話機に接続する際に * キーを押し続けます。
- ステップ 2** LED バーのライトが緑色に点灯してから消灯すると、* キーを放すことができます。
- ステップ 3** 会議電話機がバックアップイメージから再起動されます。
-

セットアップメニューからの電話機のセットアップ

電話機には多くの設定可能なネットワーク設定が含まれており、ユーザが利用できるように設定を変更することが必要な場合があります。電話機のメニューを使用して、これらの設定値にアクセスし、その一部を変更することができます。

電話機には次のセットアップメニューがあります。

- [ネットワークのセットアップ (Network Setup)] : さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。
 - [IPv4 のセットアップ (IPv4 Setup)] : このサブメニューは追加のネットワーク オプションを提供します。
 - [IPv6 のセットアップ (IPv6 Setup)] : このサブメニューは追加のネットワーク オプションを提供します。
- [セキュリティのセットアップ (Security Setup)] : さまざまなセキュリティ設定を表示および設定するためのオプションを提供します。




(注) 電話機が [設定 (Settings)] メニューにアクセスするかまたはそのメニューのオプションにアクセスするかどうかは制御できます。アクセスを制御するには、[電話機の設定 (Phone Configuration)] ウィンドウの [設定のアクセス (Settings Access)] Cisco Unified Communications Manager Administration フィールドを使用します。[設定アクセス (Settings Access)] フィールドでは、次の値を設定できます。

- [有効 (Enabled)] : [設定 (Settings)] メニューへのアクセスを許可します。
- [無効 (Disabled)] : [設定 (Settings)] メニューのほとんどのエントリへのアクセスを禁止します。ユーザは引き続き [設定 (Settings)] > [ステータス (Status)] にアクセスできます。
- [非許可 (Restricted)] : [ユーザ設定 (User Preferences)] メニュー項目および [ステータス (Status)] メニュー項目へのアクセスを許可し、音量の設定変更の保存を許可します。[設定 (Settings)] メニューの他のオプションへのアクセスは禁止します。

[管理者設定 (Admin Settings)] メニューのオプションにアクセスできない場合は、[設定アクセス (Settings Access)] フィールドを確認してください。

Cisco Unified Communications Manager Administration の電話機で、表示専用になっている設定値を設定します。

手順

- ステップ 1** [設定 (Settings)] を押します。
- ステップ 2** [管理者設定 (Admin Settings)] を選択します。
- ステップ 3** 要求されたらパスワードを入力し、[サインイン (Sign-In)] をクリックします。
- ステップ 4** [ネットワークのセットアップ (Network Setup)] または [セキュリティのセットアップ (Security Setup)] を選択します。
- ステップ 5** 次のいずれかの操作を実行して、目的のメニューを表示します。
 - ナビゲーション矢印を使用して目的のメニューを選択し、[選択 (Select)] を押します。
 - 電話機のキーパッドを使用して、メニューに対応する番号を入力します。
- ステップ 6** サブメニューを表示するには、ステップ 5 を繰り返します。
- ステップ 7** メニューを終了するには、[戻る (Back)]  を押します。

関連トピック

- [会議電話の再起動またはリセット \(215 ページ\)](#)
- [ネットワークの設定 \(48 ページ\)](#)
- [セキュリティの設定](#)

電話機パスワードの適用

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] で、[共通の電話プロファイルの設定 (Common Phone Profile Configuration)] ウィンドウに移動します ([デバイス (Device)] > [デバイス設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)])。
- ステップ 2 [電話ロック解除パスワード (Local Phone Unlock Password)] オプションで、パスワードを入力します。
- ステップ 3 電話機が使用する共通の電話プロファイルに、パスワードを適用します。

電話機からのテキストとメニューの入力

オプション設定値を編集するときは、次のガイドラインに従ってください。

- ナビゲーションパッドの矢印を使用して、編集するフィールドを強調表示します。ナビゲーションパッドの**選択**を押して、フィールドをアクティブにします。フィールドがアクティブになったら、値を入力できます。
- 数値と文字を入力するには、キーパッド上のキーを使用します。
- キーパッドを使用して文字を入力するには、対応する数値キーを使用します。キーを1回または何回か押して、個々の文字を表示します。たとえば、**2**キーを1回押すと「a」、すばやく2回押すと「b」、すばやく3回押すと「c」です。一時停止した後、カーソルは自動的に進み、次の文字を入力できます。
- 間違えた場合は、ソフトキー **x** を押します。このソフトキーを押すと、カーソルの左側にある文字が削除されます。
- 変更内容を破棄するには、[適用 (Apply)] を押す前に [元に戻す (Revert)] を押します。
- (IP アドレスなどに含まれる) ピリオドを入力するには、キーパッドの [*****] を押します。
- IPv6 アドレスのコロンを入力するには、キーパッドの ***** を押します。



- (注) Cisco IP 電話では、必要に応じて、いくつかの方法でオプション設定値をリセットまたは復元することができます。

ネットワークの設定

手順

- ステップ 1 [設定 (Settings)] を押します。
- ステップ 2 [管理者設定 (Admin Settings)] > [ネットワーク設定 (Network Setup)] > [イーサネットのセットアップ (Ethernet setup)] の順に選択します。
- ステップ 3 [ネットワークのセットアップ (Network Setup)] フィールド (48 ページ) の説明に従って、フィールドを設定します。
フィールドを設定したあと、電話を再起動する必要があります。

[ネットワークのセットアップ (Network Setup)] フィールド

[ネットワークのセットアップ (Network Setup)] メニューには、IPv4 と IPv6 のためのフィールドとサブメニューが含まれています。

一部のフィールドを変更するには、DHCP をオフにする必要があります。

表 10: [ネットワークのセットアップ (Network Setup)] メニュー

エントリー	タイプ	デフォルト	説明
IPv4 のセットアップ (IPv4 setup)	メニュー		表「IPv4 設定サブメニュー」「」を参照してください。 このオプションは、デュアルスタックモードの場合のみ表示されます。
IPv6 のセットアップ (IPv6 setup)	メニュー		表「IPv6 設定サブメニュー」「」を参照してください。
ホスト名 (Host Name)	文字列		電話機のホスト名。DHCP を使用すると、この名前が自動的に割り当てられます。
ドメイン名 (Domain Name)	文字列		電話機が所属するドメイン ネーム システム (DNS) ドメインの名前。 このフィールドを変更するには、DHCP を無効にしてください。
接続先 VLAN ID (Operational VLAN ID)			電話機が所属する、Cisco Catalyst スイッチに設定された接続先 Virtual Local Area Networks (VLAN)。

エントリー	タイプ	デフォルト	説明
[管理 VLAN ID (Admin VLAN ID)]			電話機がメンバーになっている補助 VLAN。
SW ポートのセットアップ (SW Port Setup)	自動ネゴシエーション 10 ハーフ (100 Half) 10 フル (10 Full) 100 ハーフ (100 Half) 100 フル (10 Full)	Auto Negotiate	スイッチ ポートの速度とデュプレックス。次のいずれかになります。 <ul style="list-style-type: none"> • [10 ハーフ (10 Half)] : 10-BaseT/半二重 • [10 フル (10 Full)] : 10-BaseT/全二重 • [100 ハーフ (100 Half)] : 100-BaseT/半二重 • [100 フル (100 Full)] : 100-BaseT/全二重
LLDP-MED : SW ポート (LLDP-MED: SW Port)	無効 有効	有効	スイッチ ポートで Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) が有効になっているかどうかを示します。

表 11: IPv4 設定サブメニュー

エントリー	タイプ	デフォルト	説明
DHCP	無効 有効	有効	DHCP の使用を有効または無効にします。
IP アドレス (IP Address)			電話機のインターネットプロトコルバージョン 4 (IPv4) アドレス。 このフィールドを変更するには、DHCP を無効にしてください。
サブネットマスク			電話機で使用されるサブネットマスク。 このフィールドを変更するには、DHCP を無効にしてください。

[ネットワークのセットアップ (Network Setup)] フィールド

エントリー	タイプ	デフォルト	説明
デフォルト ルータ 1 (Default Router 1)			電話機で使用される、デフォルト ルータ。 このフィールドを変更するには、 DHCP を無効にしてください。
DNS サーバ 1			電話機が使用するプライマリ ドメ インネーム システム (DNS) サー バ (DNS サーバ 1)。 このフィールドを変更するには、 DHCP を無効にしてください。
DNS Server 2			電話機が使用するプライマリ ドメ インネーム システム (DNS) サー バ (DNS サーバ 2)。
DNS Server 3			電話機が使用するプライマリ ドメ インネーム システム (DNS) サー バ (DNS サーバ 3)。
代替 TFTP	不可 可	不可	電話機が代替 TFTP サーバを使用 しているかどうかを示します。

エントリー	タイプ	デフォルト	説明
TFTP サーバ 1 (TFTP Server 2)			<p>電話機で使用される、プライマリの Trivial File Transfer Protocol (TFTP) サーバ。</p> <p>[代替 TFTP (Alternate TFTP)] オプションを [オン (On)] に設定した場合は、[TFTP サーバ 1 (TFTP Server 1)] オプションに 0 以外の値を入力する必要があります。プライマリ TFTP サーバもバックアップ TFTP サーバも、電話機の CTL ファイルまたは ITL ファイルに記述されていない場合は、[TFTP サーバ 1 (TFTP Server 1)] オプションの変更内容を保存する前に、これらのファイルをロック解除する必要があります。この場合、[TFTP サーバ 1 (TFTP Server 1)] オプションへの変更を保存すると、ファイルは削除されます。新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 1 アドレスからダウンロードされます。</p> <p>最後の表の後の TFTP に関する注を参照してください。</p>

エントリー	タイプ	デフォルト	説明
TFTP サーバ 2 (TFTP Server 2)			<p>電話機が使用するセカンダリ TFTP サーバ。</p> <p>プライマリ TFTP サーバもバックアップ TFTP サーバも、電話機の CTL ファイルまたは ITL ファイルに記述されていない場合は、[TFTP サーバ 2 (TFTP Server 1)] オプションの変更内容を保存する前に、これらのファイルをロック解除する必要があります。この場合、[TFTP サーバ 2 (TFTP Server 1)] オプションへの変更を保存すると、ファイルは削除されます。新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 2 アドレスからダウンロードされます。</p> <p>最後の表の後の TFTP に関する注のセクションを参照してください。</p>
DHCP アドレス解放 (DHCP Address Released)	不可 可	不可	

表 12: IPv6 設定サブメニュー

エントリー	タイプ	デフォルト	説明
DHCPv6 有効 (DHCPv6 Enabled)	無効 有効	有効	IPv6 DHCP の使用を有効または無効にします。
IPv6 Address			<p>電話機の IPv6 アドレス。</p> <p>このフィールドを変更するには、DHCP を無効にしてください。</p>
IPv6 プレフィックス長 (IPv6 Prefix Length)			<p>IPv6 アドレスの長さ。</p> <p>このフィールドを変更するには、DHCP を無効にしてください。</p>

エントリ	タイプ	デフォルト	説明
IPv6 デフォルト ルータ 1 (IPv6 Default Router 1)			デフォルトの IPv6 ルータ。 このフィールドを変更するには、DHCP を無効にしてください。
IPv6 DNS サーバ 1 (IPv6 DNS Server 1)			プライマリ IPv6 DNS サーバ。 このフィールドを変更するには、DHCP を無効にしてください。
IPv6 代替 TFTP (IPv6 Alternate TFTP)	不可 可	不可	電話機が代替 IPv6 TFTP サーバを使用しているかどうかを示します。
IPv6 TFTP サーバ 1 (IPv6 TFTP Server 1)			電話機が使用するプライマリ IPv6 TFTP サーバ。 この表の後の TFTP に関する注を参照してください。
IPv6 TFTP サーバ 2 (IPv6 TFTP Server 2)			電話機が使用するセカンダリ IPv6 TFTP サーバ。 この表の後の TFTP に関する注を参照してください。
IPv6 アドレス解放 (IPv6 Address Released)	不可 可	不可	

IPv6 セットアップ オプションをデバイスで設定する前に、IPv6 を Cisco Unified Communication Administration で有効化し、設定する必要があります。次のデバイス設定フィールドが IPv6 設定に適用されます。

- IP アドレッシング モード (IP Addressing Mode)
- シグナリング用の IP アドレッシングモード設定 (IP Addressing Mode Preference for Signalling)

IPv6 が Unified クラスタで有効な場合、IP アドレッシング モードのデフォルト設定は [IPv4 と IPv6 (IPv4 and IPv6)] です。このアドレッシングモードでは、電話機が IPv4 アドレス 1 個と IPv6 アドレス 1 個を取得して使用します。メディアの必要に応じて IPv4 および IPv6 アドレスを使用できます。電話機は、コール制御シグナリングに IPv4 または IPv6 のいずれかのアドレスを使用します。

IPv6 の詳細については、

- 『Cisco Unified Communications Manager 機能とサービス ガイド』の「一般的なデバイス構成」および「Cisco Unified Communications デバイスの IPv6 サポート」の章、

- こちら : <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html>のシスコ コラボレーション システム リリース 12.0 の IPv6 展開ガイドを参照してください。

TFTP に関する注

電話機が TFTP サーバを探るとき、プロトコルに関係なく、手動で割り当てられた TFTP サーバが優先されます。IPv6 と IPv4 の両方の TFTP サーバが設定に含まれる場合、電話機は、手動で割り当てられた IPv6 TFTP サーバおよび IPv4 TFTP サーバを優先することによって、TFTP サーバを探す順序の優先順位を決定します。電話機は、次の順序で TFTP サーバを探します。

1. 手動で割り当てられた IPv4 TFTP サーバ
2. 手動で割り当てられた IPv6 サーバ
3. DHCP が割り当てられた TFTP サーバ
4. DHCPv6 が割り当てられた TFTP サーバ

CTL ファイルおよび ITL ファイルの詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。

[ドメイン名 (Domain Name)]フィールドの設定

手順

-
- ステップ 1 [DHCP を使う (DHCP Enabled)]オプションを [いいえ (No)]に設定します。
- ステップ 2 [ドメイン名 (DomainName)]オプションまでスクロールし、[選択 (Select)]を押して、新しいドメイン名を入力します。
- ステップ 3 [適用 (Apply)]を押します。
-

電話機からのワイヤレス LAN の有効化

ワイヤレス LAN が導入されている場所の Wi-Fi カバレッジが音声パケットの送信に最適であることを確認します。

Wi-Fi ユーザには、高速セキュア ローミング方式をお勧めします。802.11 r (FT) を使用することを推奨します。

完全な設定情報については、次の場所にある『Cisco IP 電話 8832 Wireless LAN Deployment Guide』を参照してください。

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>

『Cisco IP 電話 8832 Wireless LAN Deployment Guide』には、次の設定情報が記載されています。

- ワイヤレス ネットワークの設定
- [Cisco Unified CMの管理 (Cisco Unified Communications Manager Administration)]でのワイヤレス ネットワークの設定
- Cisco IP 電話 でのワイヤレス ネットワークの設定

始める前に

Wi-Fi が電話で有効であり、イーサネット ケーブルが切断されていることを確認します。

手順

-
- ステップ 1** アプリケーションを有効にするには、**設定**を押します。
- ステップ 2** [管理者設定 (Admin settings)]>[ネットワークのセットアップ (Network setup)]>[Wi-Fi クライアントのセットアップ (Wi-Fi client setup)]>[ワイヤレス (Wireless)]に移動します。
- ステップ 3** [オン (On)]を押します。
-

Cisco Unified Communications Manager からのワイヤレス LAN のセットアップ

Cisco Unified Communications Manager の管理ページで、会議用電話の「Wi-Fi」 というパラメータを有効にする必要があります。



- (注) Cisco Unified Communications Manager Administration の [電話の設定 (Phone Configuration)] ウィンドウ ([デバイス (Device)]>[電話機 (Phone)]) で、MAC アドレスの設定時に、有線の MAC アドレスを使用します。Cisco Unified Communications Manager の登録では、無線 MAC アドレスを使用しません。

[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] で、次の手順を実行します。

手順

-
- ステップ 1** 特定の電話機でワイヤレス LAN を有効にするには、次の手順を実行します。
- a) [デバイス (Device)]>[電話 (Phone)] の順に選択します。
 - b) 対象の電話を特定します。
 - c) [プロダクト固有の設定 (Product Specific Configuration Layout)] セクションの [Wi-Fi] パラメータに対して [有効化 (Enabled)] 設定を選択します。
 - d) [共通設定の上書き (Override Common Settings)] チェックボックスをオンにします。

- ステップ 2** 電話機のグループに対してワイヤレス LAN を有効にするには、
- [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)] の順に選択します。
 - [Wi-Fi] パラメータに対して [有効化 (Enabled)] 設定を選択します。

(注) この手順の設定を機能させるには、手順 1d で言及されている [共通設定の上書き (Override Common Settings)] チェック ボックスのチェックを外します。
 - [共通設定の上書き (Override Common Settings)] チェックボックスをオンにします。
 - [デバイス (Device)] > [電話 (Phone)] を使用して、電話機を共通プロファイルと関連付けます。
- ステップ 3** ネットワークのすべての WLAN 対応電話機に対してワイヤレス LAN を有効にするには、
- [システム (System)] > [エンタープライズ電話の設定 (Enterprise Phone Configuration)] を選択します。
 - [Wi-Fi] パラメータに対して [有効化 (Enabled)] 設定を選択します。

(注) この手順の設定を機能させるには、手順 1d と手順 2c で言及されている [共通設定の上書き (Override Common Settings)] チェック ボックスのチェックを外します。
 - [共通設定の上書き (Override Common Settings)] チェックボックスをオンにします。

電話機からのワイヤレス LAN のセットアップ

Cisco IP 電話を WLAN に接続可能にするには、先に適切な WLAN 設定で電話機のネットワークプロファイルを設定する必要があります。電話機の [ネットワークのセットアップ (Network Setup)] メニューを使用して [Wi-Fi クライアントのセットアップ (Wi-Fi client setup)] サブメニューにアクセスし、WLAN 設定をセットアップすることができます。



- (注) Wi-Fi が Cisco Unified Communications Manager で無効にされている場合、[ネットワーク設定 (Network Setup)] メニューには [Wi-Fi クライアントのセットアップ (Wi-Fi client setup)] オプションが表示されません。

詳細については、次で入手可能な『Cisco IP 会議用電話 8832 Series WLAN Deployment Guide』を参照してください。 <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>

始める前に

Cisco Unified Communications Manager からワイヤレス LAN を設定します。

手順

ステップ 1 [設定 (Settings)] を押します。

ステップ 2 [管理者設定 (Administrator Settings)] > [ネットワークのセットアップ (Network Setup)] > [Wi-Fi クライアントのセットアップ (Wi-Fi client setup)] の順に選択します。

ステップ 3 次の表に示すようにワイヤレス設定をセットアップします。

表 13: [Wi-Fi クライアントのセットアップ (Wi-Fi client setup)] メニュー オプション

オプション	説明	変更の手順
ワイヤレス	Cisco IP 電話の無線をオンまたはオフにします。	[ワイヤレス (Wireless)] オプションまでスクロールしてからトグル スイッチを使用すると、オンとオフの設定値を切り替えることができます。
ネットワーク名	[ネットワークの選択 (Choose a Network)] ウィンドウを使用して、ワイヤレスネットワークに接続できます。このウィンドウには、2つのソフトウェア - [バック (Back)] と [その他 (Other)] が表示されます。	[ネットワークの選択 (Choose a Network)] ウィンドウで、接続先のネットワークを選択します。
Wi-Fi サインイン アクセス (Wi-Fi sign in access)	[Wi-Fi サインイン (Wi-Fi sign in)] ウィンドウを表示できるようにします。	[Wi-Fi サインイン アクセス (Wi-Fi sign in access)] オプションまでスクロールしてから、トグル スイッチを使用すると、オンとオフの設定値を切り替えることができます。

オプション	説明	変更の手順
IPv4 のセットアップ (IPv4 setup)	<p>[IPv4 のセットアップ (IPv4 Setup)] 設定サブメニューでは、次の作業を実行できます。</p> <ul style="list-style-type: none"> • DHCP サーバが割り当てた IP アドレスの、電話機による使用のオン/オフ。 • IP アドレス、サブネットマスク、デフォルトルータ、DNS サーバ、および代替 TFTP サーバの手動設定。 <p>IPv4 アドレス フィールドの詳細については、[IPv6 のセットアップ サブメニュー (IPv4 Setup Submenu)] テーブルを参照してください。</p>	[IPv4 のセットアップ (IPv4 Setup)] までスクロールし、[選択 (Select)] を押します。
IPv6 のセットアップ (IPv6 setup)	<p>[IPv6 のセットアップ (IPv6 Setup)] 設定サブメニューでは、次の作業を実行できます。</p> <ul style="list-style-type: none"> • IPv6 対応ルータを介して SLAAC が取得した、または DHCPv6 サーバによって割り当てられた IPv6 アドレスの使用を、電話機で有効または無効にします。 • IPv6 アドレス、プレフィックス長、デフォルトルータ、DNS サーバ、および代替 TFTP サーバを手動設定します。 <p>IPv6 アドレス フィールドの詳細については、[IPv6 のセットアップ サブメニュー (IPv6 Setup Submenu)] テーブルを参照してください。</p>	IPv6 setup [IPv6 のセットアップ (IPv6 Setup)] までスクロールし、[選択 (Select)] を押します。

オプション	説明	変更の手順
MAC アドレス	電話機固有のメディア アクセスコントロール (MAC) アドレス。	表示のみ。変更不可。
ドメイン名	電話機が所属するドメインネームシステム (DNS) ドメインの名前。	[ドメイン名 (Domain Name) フィールドの設定 (54 ページ)] を参照してください。

ステップ 4 [保存 (Save)] を押して変更を行うか、[復元 (Revert)] を押して接続を破棄します。

WLAN 認証試行の回数の設定

認証要求は、ユーザのサインインクレデンシャルの確認です。これは、Wi-Fi ネットワークにすでに参加している電話機が Wi-Fi サーバへの再接続を試行するたびに発生します。たとえば、Wi-Fi セッションがタイムアウトしたとき、また Wi-Fi 接続が失われて再取得される時などです。

Wi-Fi 電話機が Wi-Fi サーバに認証要求を送信する回数を設定できます。デフォルトの試行回数は 2 ですが、このパラメータは 1～3 の範囲で設定できます。電話機が認証に失敗すると、ユーザは再度ログインするように求められます。

個々の電話機、電話機のプール、またはネットワーク内のすべての Wi-Fi 電話機に [WLAN 認証の試行 (WLAN Authentication Attempts)] を適用できます。

手順

- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択し、電話機を見つけます。
- ステップ 2 [プロダクト固有の設定 (Product Specific Configuration)] 領域に移動して、[WLAN 認証の試行 (WLAN Authentication Attempts)] フィールドを設定します。
- ステップ 3 [保存 (Save)] を選択します。
- ステップ 4 [設定の適用 (Apply Config)] を選択します。
- ステップ 5 電話機を再起動します。

WLAN プロンプト モードの有効化

ユーザの電話機で電源を入れるかリセットしたときに Wi-Fi ネットワークにログインする場合には、WLAN プロファイル 1 プロンプト モードを有効にします。

手順

- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2 設定する電話機を特定します。
- ステップ 3 [プロダクト固有の設定 (Product Specific Configuration)] 領域に移動し、[WLAN プロファイル 1 のプロンプトモード (WLAN Profile 1 Prompt Mode)] フィールドを [有効 (Enable)] に設定します。
- ステップ 4 [保存 (Save)] を選択します。
- ステップ 5 [設定の適用 (Apply Config)] を選択します。
- ステップ 6 電話機を再起動します。

Cisco Unified Communications Manager を使用した Wi-Fi プロファイルの設定

Wi-Fi プロファイルを設定して、そのプロファイルを、Wi-Fi をサポートする電話機に割り当てることができます。プロファイルには、電話機が Wi-Fi を使用して Cisco Unified Communications Manager に接続するために必要なパラメータが含まれています。Wi-Fi プロファイルを作成して使用する際、管理者およびユーザが個々の電話機に対してワイヤレスネットワークの設定を行う必要はありません。

Wi-Fi プロファイルは、Cisco Unified Communications Manager リリース 10.5(2) 以降でサポートされます。EAP-FAST、PEAP-GTC-GTC、および PEAP-MSCHAPv2 は、Cisco Unified Communications Manager リリース 10.0 以降でサポートされています。Cisco Unified Communications Manager リリース 11.0 以降では、EAP-TLS もサポート対象です。

Wi-Fi プロファイルによって、ユーザが電話機の Wi-Fi 設定を変更できないようにしたり、制限したりすることができます。

Wi-Fi プロファイルを使用する際、キーとパスワードを保護するため、TFTP 暗号化が有効にされたセキュアなプロファイルを使用することをお勧めします。

EAP-FAST、PEAP-MSCHAPV、または PEAP-GTC 認証を使用するように電話機を設定する場合、ユーザは個々のユーザー ID とパスワードを使用して、電話機にサインインする必要があります。

Cisco IP 電話 8832 は、SCEP または手動インストール方法のいずれかでインストールできるサーバ証明書を 1 つだけサポートしています。両方の方法ではサポートされていません。電話機は TFTP による証明書のインストール方法をサポートしていません。

手順

ステップ 1 Cisco Unified Communications Administration で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [ワイヤレス LAN プロファイル (Wireless LAN Profile)] の順に選択します。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 [ワイヤレス LAN プロファイル情報 (Wireless LAN Profile Information)] セクションで、以下のようにパラメータを設定します。

- [名前 (Name)] : Wi-Fi プロファイルの固有の名前を入力します。電話機にこの名前が表示されます。
- [説明 (Description)] : このプロファイルを他の Wi-Fi プロファイルから区別するための Wi-Fi プロファイルの説明を入力します。
- [ユーザが変更可能 (User Modifiable)] : 次のオプションの中から選択します。
 - [許可 (Allowed)] : ユーザが電話機から Wi-Fi 設定を変更できることを示します。このオプションは、デフォルトで選択されます。
 - [拒否 (Disallowed)] : ユーザが電話機から Wi-Fi 設定を変更できないことを示します。
 - [制限 (Restricted)] : ユーザが電話機の Wi-Fi ユーザ名およびパスワードを変更できることを示します。ただし、電話機のその他の Wi-Fi 設定は変更できません。

ステップ 4 [Wireless Settings] セクションで、次のパラメータを設定します。

- [SSID (ネットワーク名) (SSID (Network Name))] : 電話機を接続可能なユーザ環境で使用できるネットワーク名を入力します。この名前は、電話機で使用可能なネットワークリストの下に表示され、その電話機はこのワイヤレス ネットワークに接続できます。
- [周波数帯域 (Frequency Band)] : 使用可能なオプションは [自動 (Auto)]、[2.4 GHz]、[5 GHz] です。このフィールドは、ワイヤレス接続で使用する周波数帯域を決定します。[自動 (Auto)] を選択すると、電話機は 5 GHz 帯域の使用を最初に試行し、5 GHz 帯域が使用できない場合のみ、2.4 GHz 帯域を使用します。

ステップ 5 [Authentications Settings] セクションで、[Authentication Method] を [EAP-FAST]、[EAP-TLS]、[PEAP-MSCHAPv2]、[PEAP-GTC]、[PSK]、[WEP]、または [None] のいずれかの認証方式に設定します。

このフィールドを設定したら、設定する必要がある追加フィールドが表示されることがあります。

- [ユーザ証明書 (User certificate)] : EAP-TLS 認証に必要です。[製造元でインストール (Manufacturing installed)] または [ユーザによってインストール (User installed)] を選択します。電話機では証明書を、SCEP から自動で、または電話の管理ページから手動でインストールする必要があります。

- [PSK パスフレーズ (PSK passphrase)] : PSK 認証に必要です。8 ~ 63 文字の ASCII または 64 文字の 16 進数文字のパスフレーズを入力します。
 - [WEP キー (WEP Key)] : WEP 認証に必要です。40/102 または 64/128 の ASCII または 16 進数の WEP キーを入力します。
 - 40/104 ASCII は 5 文字です。
 - 64/128 ASCII は 13 文字です。
 - 40/104 の 16 進数は 10 文字です。
 - 64/128 の 16 進数は 26 文字です。
 - **共有ログイン情報の指定** : EAP-FAST、PEAP-MSCHAPv2、および PEAP-GTC 認証に必要です。
 - ユーザがユーザ名とパスワードを管理する場合、[ユーザ名 (Username)] と [パスワード (Password)] のフィールドは空白のままにします。
 - すべてのユーザが同じユーザ名とパスワードを共有する場合、ここで [ユーザ名 (Username)] と [パスワード (Password)] のフィールドに情報を入力できます。
 - [パスワードの説明 (Password Description)] フィールドに説明を入力します。
- (注) 各ユーザに固有のユーザ名とパスワードを割り当てる必要がある場合、各ユーザのプロファイルを作成する必要があります。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

[WLAN プロファイル グループ (WLAN Profile Group)] をデバイス プール ([システム (System)] > [デバイス プール (Device Pool)])、または直接電話機に ([デバイス (Device)] > [電話 (Phone)]) に適用します。

Cisco Unified Communications Manager を使用した Wi-Fi グループの設定

ワイヤレス LAN プロファイル グループを作成し、そのグループにワイヤレス LAN プロファイルを追加することができます。その後、電話機のセットアップ時に、プロファイルグループを電話機に割り当てることができます。

手順

ステップ 1 Cisco Unified Communications Administration で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [ワイヤレス LAN プロファイル グループ (Wireless LAN Profile Group)] の順に選択します。

また、[システム (System)] > [デバイス プール (Device Pool)] からワイヤレス LAN プロファイル グループを定義できます。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 [ワイヤレス LAN プロファイル グループ情報 (Wireless LAN Profile Group Information)] セクションで、グループ名と説明を入力します。

ステップ 4 [ワイヤレス LAN プロファイル グループのプロファイル (Profiles for this Wireless LAN Profile Group)] セクションで、[使用可能なプロファイル (Available Profiles)] リストから使用可能なプロファイルを選択し、選択したプロファイルを [選択したプロファイル (Selected Profiles)] リストに移動します。

複数のワイヤレス LAN プロファイルを選択した場合、電話機は最初のワイヤレス LAN プロファイルのみを使用します。

ステップ 5 [保存 (Save)] をクリックします。

電話機起動の確認

電話機が電源に接続されると、起動診断プロセスが自動的に実行されます。

手順

電話機の電源をオンにします。

メイン画面が表示されたら、電話機が正しく起動されています。

ユーザの電話モデルを変更

ユーザは、ユーザの電話機モデルを変更できます。この変更は、次のようにいくつかの理由で必要になる場合があります。

- Cisco Unified Communications Manager (ユニファイド CM) を電話機モデルをサポートしていないソフトウェアバージョンに更新しました。
- ユーザは、現在のモデルからの別の電話機モデルが必要です。

- 電話機を修理または交換する必要があります。

Unified CM は、古い電話機を識別し、古い電話機の MAC アドレスを使用して古い電話機の設定を識別します。Unified CM によって、古い電話機の設定が新しい電話機のエントリにコピーされます。その後、新しい電話機は古い電話機と同じ設定になります。

制限 (Limitation) : 古い電話機が新しい電話よりも多くの回線または回線ボタンを使用している場合は、新しい電話機に追加回線や回線ボタンは設定されません。

設定が完了すると、電話機が再起動します。

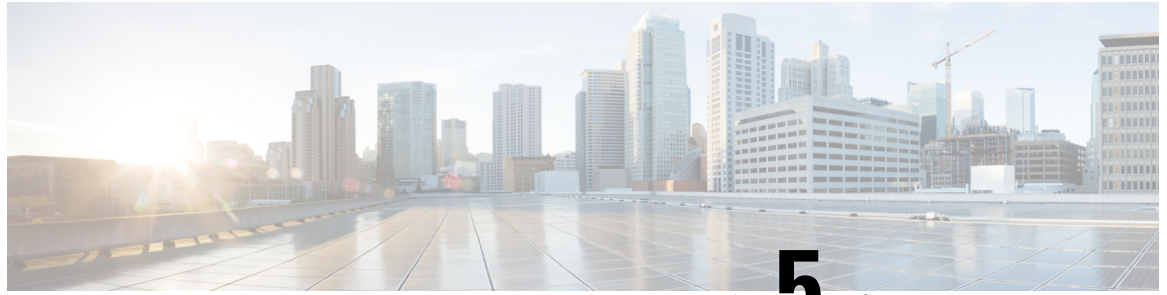
始める前に

Feature Configuration Guide for Cisco Unified Communications Manager にしたがって、Cisco Unified Communications Manager をセットアップします。

ファームウェアリリース 12.8 (1) 以降に、新しい、使用されていない電話機がプレインストールされている必要があります。

手順

-
- ステップ 1** 古い電話機の電源をオフにします。
 - ステップ 2** 新しい電話機の電源を入れます。
 - ステップ 3** 新しい電話機で、**[既存の電話を置き換える (Replace)]** を選択します。
 - ステップ 4** 古い電話機のプライマリ内線番号を入力します。
 - ステップ 5** 古い電話機に暗証番号が割り当てられている場合は、暗証番号を入力します。
 - ステップ 6** [送信] を押します。
 - ステップ 7** ユーザに複数のデバイスが存在する場合は、置き換えるデバイスを選択して**[続行 (Continue)]** を押します。
-



第 5 章

Cisco Unified Communications Manager での 電話機の設置

- [Cisco IP 会議用電話のセットアップ \(65 ページ\)](#)
- [電話機の MAC アドレスの決定 \(71 ページ\)](#)
- [電話機の追加方法 \(71 ページ\)](#)
- [Cisco Unified Communications Manager におけるユーザーの追加 \(73 ページ\)](#)
- [エンド ユーザ グループにユーザを追加する \(75 ページ\)](#)
- [電話機とユーザの関連付け \(76 ページ\)](#)
- [Survivable Remote Site Telephony \(76 ページ\)](#)

Cisco IP 会議用電話のセットアップ

自動登録が有効ではなく、電話機が Cisco Unified Communications Manager データベースに存在しない場合、Cisco Unified Communications Manager の管理で手動で Cisco IP 電話を設定する必要があります。この手順の一部のタスクは、システムおよびユーザのニーズによっては省略できます。

この手順の詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco Unified Communications Manager の管理ページを使用して、次の手順で設定を実行してください。

手順

ステップ 1 電話機について、次の情報を収集します。

- 電話機モデル
- MAC アドレス : [電話機の MAC アドレスの決定 \(71 ページ\)](#) 参照
- 電話機の設置場所

- 電話機のユーザの名前または ID
- デバイス プール
- パーティション、コーリング サーチ スペース、およびロケーションの情報
- 電話機に割り当てるための電話番号 (DN)
- 電話機に関連付ける Cisco Unified Communications Manager ユーザ
- ソフトキー テンプレート、電話機能、IP 電話サービス、または電話アプリケーションに影響する、電話機の使用状況情報

詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルおよび関連リンクを参照してください。

- ステップ 2** 電話機に対応する十分なユニット ライセンスがあることを確認します。
- 詳細については、ご使用の Cisco Unified Communications Manager リリースのライセンス マニュアルを参照してください。
- ステップ 3** デバイス プールを定義します。[システム (System)] > [デバイス プール (Device Pool)] を選択します。
- デバイス プールは、デバイスに共通の特性 (リージョン、日時グループ、ソフトキー テンプレートなど) を定義します。
- ステップ 4** 共通の電話プロファイルを定義します。[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)] の順に選択します。
- 共通の電話プロファイルは Cisco TFTP サーバが要求するデータとともに、サイレント オプションおよび機能制御オプションなど、共通の電話の設定を提供します。
- ステップ 5** コーリング サーチ スペースを定義します。Cisco Unified Communications Manager の管理ページで、[コールルーティング (Call Routing)] > [コントロールのクラス (Class of Control)] > [コーリングサーチスペース (Calling Search Space)] をクリックします。
- コーリングサーチスペースは、着信番号のルーティング方法を決定するために検索されるパーティションのコレクションです。デバイス用のコーリングサーチスペースと電話番号用のコーリングサーチスペースは併用することができます。電話番号の CSS は、デバイスの CSS に優先します。
- ステップ 6** デバイス タイプおよびプロトコルのセキュリティ プロファイルを設定します。[システム (System)] > [セキュリティ (Security)] > [電話セキュリティ プロファイル (Phone Security Profile)] を選択します。
- ステップ 7** 電話機をセット アップします。[デバイス (Device)] > [電話 (Phone)] を選択します。
- a) 変更する電話機を検索するか、新しい電話機を追加します。
 - b) [電話の設定 (Phone Configuration)] ウィンドウの [デバイス情報 (Device Information)] ページに必須フィールドを入力して、電話機を設定します。
 - MAC アドレス (必須) : 値は必ず 12 個の 16 進文字列で構成してください。

- 説明：このユーザに関する情報検索が必要な場合に役立つ有用な説明を入力します。
- デバイス プール（必須）
- 共通の電話プロファイル（Common Phone Profile）
- コーリング サーチ スペース（Calling Search Space）
- 所在地（Location）
- 所有者（ユーザまたは匿名）。ユーザを選択した場合は、所有者のユーザー ID

デバイスを、デフォルト設定値を使用して Cisco Unified Communications Manager データベースに追加します。

[プロダクト固有の設定（Product Specific Configuration）] フィールドについては、「?」「」を参照してください。ヘルプ ボタンと関連リンクを参照してください。

(注) Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

- c) このウィンドウの [プロトコル固有情報（Protocol Specific Information）] 領域で、[デバイスセキュリティプロファイル（Device Security Profile）] を選択し、セキュリティモードを設定します。

(注) 企業全体のセキュリティ戦略に基づいて、セキュリティプロファイルを選択します。電話機でセキュリティがサポートされていない場合は、非セキュアプロファイルを選択してください。

- d) この電話機が Cisco Extension Mobility をサポートしている場合は、[内線情報（Extension Information）] 領域で、[エクステンションモビリティの有効化（Enable Extension Mobility）] チェックボックスをオンにします。

- e) [保存（Save）] をクリックします。

ステップ 8 [デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP プロフィール（SIP Profile）] を選択して、SIP パラメータを設定します。

ステップ 9 [デバイス（Device）] > [電話（Phone）] を選択し、[電話番号の設定（Directory Number Configuration）] ウィンドウの必須フィールドに値を入力して、電話機に電話番号（回線）を設定します。

- a) 電話機を検索します。
- b) [電話の設定（Phone Configuration）] ウィンドウで、ウィンドウの左ペインにある [回線 1（Line 1）] をクリックします。

会議電話が保有する回線は 1 本のみです。

- c) [電話番号（Directory Number）] フィールドで、ダイヤル可能な有効な番号を入力します。

(注) このフィールドには、[エンドユーザの設定（End User Configuration）] ウィンドウの [電話番号（Telephone Number）] フィールドに表示されるのと同じ番号が表示されます。

- d) [ルートパーティション (Route Partition)] ドロップダウンリストから、電話番号が属するパーティションを選択します。電話番号へのアクセスを制限しない場合、パーティションに対して [なし (<None>)] を選択します。
- e) [コーリング検索スペース (Calling Search Space)] ドロップダウンリストボックスから、該当するコーリング検索スペースを選択します。選択した値は、この電話番号を使用するすべてのデバイスに適用されます。
- f) [コールピックアップとコール転送の設定 (Call Forward and Call Pickup Settings)] 領域で、項目 ([不在転送 (Forward All)]、[話中転送 (内部) (Forward Busy Internal)] など) と、それに対応するコールの送信先を選択します。

例 :

内線コールと外線コールがビジー信号を受信した場合に、この回線のボイスメールに転送するには、[コールピックアップとコール転送の設定 (Call Pickup and Call Forward Settings)] 領域の左側の列で、[話中転送 (内部) (Forward Busy Internal)] と [話中転送 (外部) (Forward Busy External)] の横の [ボイスメール (Voice Mail)] ボックスをオンにします。

- g) [デバイス (Device)] ペインの [回線 1 (Line 1)] で、次のフィールドを設定します。
 - [表示 (内線発信者 ID フィールド) (Display (Internal Caller ID field))] : このデバイスのユーザの姓と名を入力します。入力した名前は、すべての内線コールに表示されるようになります。このフィールドを空白にして、電話機の内線番号をシステムに表示させることもできます。
 - [外線電話番号マスク (External Phone Number Mask)] : この回線からコールを発信したときに、発信者 ID 情報の送出に使用される電話番号 (マスク) を指定します。最大 24 個の番号と文字「X」「」を入力できます。X は電話番号を表し、パターンの末尾に使用する必要があります。

例 :

たとえば、マスク 408902XXXX を指定すると、内線 6640 からの外線コールには、発信者 ID の番号として 4089026640 が表示されます。

この設定は、右側にあるチェックボックス ([共有デバイス設定の更新 (Update Shared Device Settings)]) をオンにして [選択対象を反映 (Propagate Selected)] をクリックしない限り、現在のデバイスだけに適用されます。右側のチェックボックスは、この電話番号を他のデバイスと共有している場合のみ表示されます。

- h) [保存 (Save)] を選択します。

電話番号の詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルおよび関連リンクを参照してください。

ステップ 10 (任意) ユーザを電話機に関連付けます。設定されている回線にユーザに関連付けるには、[電話の設定 (Phone Configuration)] ウィンドウの下部にある [エンドユーザの関連付け (Associate End Users)] をクリックします。

- a) ユーザを検索するには、検索フィールドとともに [検索 (Find)] を使用します。
- b) ユーザ名の横にあるボックスをチェックして、[選択項目の追加 (Add Selected)] をクリックします。

ユーザ名とユーザー ID は [電話番号の設定 (Directory Number Configuration)] ウィンドウの [回線に関連付けられているユーザ (Users Associated With Line)] ペインに表示されます。

- c) **[保存 (Save)]** を選択します。

これでユーザが、電話機の回線 1 に関連付けられました。

ステップ 11 (任意) ユーザをデバイスに関連付けます。

- a) **[ユーザ管理 (User Management)] > [エンド ユーザ (End User)]** の順に選択します。
b) 追加したユーザを検索するには、検索ボックスと **[検索 (Find)]** を使用します。
c) ユーザー ID をクリックします。
d) 画面の **[電話番号の割り当て (Directory Number Associations)]** 領域で、ドロップダウンリストからプライマリ内線を設定します。
e) (任意) **[モビリティ情報 (Mobility Information)]** 領域で、**[モビリティの有効化 (Enable Mobility)]** ボックスをオンにします。
f) **[権限情報 (Permissions Information)]** 領域で、**[アクセスコントロールグループに追加 (Add to Access Control Group)]** ボタンを使用して、このユーザを任意のユーザグループに追加します。

たとえば、「標準 CCM エンド ユーザ グループ」として定義されたグループに、ユーザを追加することができます。

- g) グループの詳細を表示するには、グループを選択し、**[詳細の表示 (View Details)]** をクリックします。
h) **[エクステンション モビリティ (Extension Mobility)]** 領域で、ユーザがクラスタ間のエクステンションモビリティサービスを使用できる場合は、**[クラスタ間のエクステンションモビリティの有効化 (Enable Extension Mobility Cross Cluster)]** チェックボックスをオンにします。
i) **[デバイス情報 (Device Information)]** 領域で、**[デバイスの割り当て (Device Association)]** を選択します。
j) 各種検索フィールドと **[検索 (Find)]** ボタンを使用して、ユーザに関連付けるデバイスを見つけます。
k) デバイスを選択し、**[選択/変更の保存 (Save Selected/Changes)]** をクリックします。
l) 画面の右上隅にある「ユーザの設定に戻る (Back to User) 」 「」 関連リンクの横の **[移動 (Go)]** をクリックします。
m) **[保存 (Save)]** を選択します。

ステップ 12 ソフトキーテンプレートをカスタマイズします。 **[デバイス (Device)] > [デバイス設定 (Device Settings)] > [ソフトキー テンプレート (Softkey Template)]** の順に選択します。

このページを使用して、ユーザの電話機に表示されるソフトキー機能を追加、削除、または順序変更し、機能の利用ニーズに対応します。

会議電話には特殊なソフトキー要件があります。詳細については、関連リンクを参照してください。

ステップ 13 Cisco IP 電話サービスを設定し、サービスを割り当てます。[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [電話サービス (Phone Services)] の順に選択します。

電話機に IP 電話サービスを提供します。

(注) ユーザは、Cisco Unified Communications Manager セルフケアポータルを使用して、電話機のサービスを追加または変更できます。

ステップ 14 (任意) Cisco Unified Communications Manager のグローバルディレクトリにユーザ情報を追加します。[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択し、[新規追加 (Add New)] をクリックして、必須のフィールドを設定します。必須のフィールドにはアスタリスク (*) が付いています。

(注) ユーザに関する情報を保存するために会社が Lightweight Directory Access Protocol (LDAP) ディレクトリを使用している場合、既存の LDAP ディレクトリを使用するために Cisco Unified Communications Manager をインストールして設定できます。[社内ディレクトリのセットアップ \(151 ページ\)](#) を参照してください。[LDAP サーバからの同期を有効にする (Enable Synchronization from the LDAP Server)] フィールドを有効にした後は、Cisco Unified Communications Manager の管理ページから別のユーザを追加できなくなります。

- a) ユーザー ID と姓のフィールドを設定します。
- b) パスワードを割り当てます (セルフケアポータル用)。
- c) PIN を割り当てます (Cisco エクステンション モビリティおよびパーソナル ディレクトリ用)。
- d) ユーザを電話機に関連付けます。

ユーザが、コール転送やスピードダイヤルの追加などの電話機能やサービスを設定できるようにします。

(注) 電話機の中には、会議室にある電話機など、ユーザが関連付けられないものもあります。

ステップ 15 (任意) ユーザグループにユーザを関連付けます。[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセスコントロールグループ (Access Control Group)] の順に選択します。

ユーザグループ内のすべてのユーザに適用される、共通のロールと権限のリストをユーザに割り当てます。管理者は、ユーザグループ、ロール、および権限を管理することによって、システムユーザのアクセスレベル (つまり、セキュリティのレベル) を制御できます。

エンドユーザが Cisco Unified Communications Manager セルフケアポータルにアクセスするには、ユーザを標準の Cisco Communications Manager エンドユーザグループに追加する必要があります。

関連トピック

[プロダクト固有の設定 \(116 ページ\)](#)

[Cisco IP 会議用電話の機能とセットアップ \(111 ページ\)](#)

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)
[新規ソフトキー テンプレートの設定 \(112 ページ\)](#)

電話機の MAC アドレスの決定

Cisco Unified Communications Manager に電話機を追加するには、電話機の MAC アドレスを決定する必要があります。

手順

次のいずれかの操作を実行します。

- 電話機で、[設定 (Settings)] > [電話の情報 (Phone Information)] を選択し、[MAC アドレス (MAC Address)] フィールドを確認する。
 - 電話機の背面にある MAC ラベルを確認する。
 - 電話機の Web ページを表示し、[デバイス情報 (Device Information)] を選択する。
-

電話機の追加方法

Cisco IP 電話をインストールしたら、次のオプションの 1 つを選択して、電話機を Cisco Unified Communications Manager データベースに追加できます。

- Cisco Unified Communications Manager の管理で個別に電話機を追加する
- 一括管理ツール (BAT) を使用して複数の電話を追加する
- 自動登録
- BAT と Tool for Auto-Registered Phones Support (TAPS)

個別に、または BAT を使用して電話機を追加する前に、電話機の MAC アドレスが必要です。詳細については、[電話機の MAC アドレスの決定 \(71 ページ\)](#) を参照してください。

一括管理ツールの詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

電話機の個別の追加

Cisco Unified Communications Manager に追加する電話機の MAC アドレスおよび電話機情報を収集します。

手順

-
- ステップ 1 Cisco Unified Communications Manager の管理ページで、[デバイス (Device)] > [電話 (Phone)] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 電話機のタイプを選択します。
 - ステップ 4 [Next] を選択します。
 - ステップ 5 MAC アドレスを含む電話機の情報を入力します。

Cisco Unified Communications Manager の手順の詳細と概要については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

- ステップ 6 保存を選択します。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

BAT 電話テンプレートを使用した電話機の追加

Cisco Unified Communications 一括管理ツール (BAT) を使用すると、複数の電話機の登録などのバッチ操作を実行できます。

(TAPS と組み合わせずに) BAT だけを使用して電話機を追加するには、各電話機の適切な MAC アドレスを取得する必要があります。

BAT の使用の詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

-
- ステップ 1 Cisco Unified Communications Administration から、[一括管理 (Bulk Administration)] > [電話 (Phones)] > [電話テンプレート (Phone Template)] の順に選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 [電話のタイプ (Phone Type)] を選択し、[次へ (Next)] をクリックします。
 - ステップ 4 [デバイスプール (Device Pool)]、[電話ボタンテンプレート (Phone Button Template)]、[デバイスセキュリティプロファイル (Device Security Profile)] など、電話固有の詳細なパラメータを入力します。
 - ステップ 5 [Save (保存)] をクリックします。

ステップ 6 BAT 電話テンプレートを使用して電話機を追加するには、[デバイス (Device)] > [電話 (Phone)] > [新規追加 (Add New)] を選択します。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

Cisco Unified Communications Manager におけるユーザーの追加

Cisco Unified Communications Manager に登録されているユーザに関する情報を表示および管理できます。また、Cisco Unified Communications Manager で各ユーザは次のタスクを実行できます。

- Cisco IP 電話 から、社内ディレクトリや他のカスタマイズ済みディレクトリにアクセスする。
- パーソナル ディレクトリを作成する。
- 短縮ダイヤルとコール転送の番号をセットアップする。
- Cisco IP 電話 からアクセスできるサービスに登録する。

手順

ステップ 1 ユーザを個別に追加するには、[Cisco Unified Communications Manager にユーザを直接追加する \(74 ページ\)](#) を参照してください。

ステップ 2 ユーザを一括して追加するには、一括管理ツールを使用します。この方法では、すべてのユーザに対して同一のデフォルト パスワードを設定することもできます。

詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

外部 LDAP ディレクトリからのユーザーの追加

ユーザを LDAP ディレクトリ (Cisco Unified Communications Server ではないディレクトリ) に追加した場合、LDAP ディレクトリと、ユーザおよびその電話機が追加される Cisco Unified Communications Manager を即時に同期できます。



- (注) LDAPディレクトリを Cisco Unified Communications Manager と即時に同期しない場合は、[LDAPディレクトリ (LDAP Directory)] ウィンドウの [LDAPディレクトリ同期スケジュール (LDAP Directory Synchronization Schedule)] で、次回の自動同期化スケジュールを決定できます。新規ユーザをデバイスに関連付けるには、その前に同期を完了しておく必要があります。

手順

- ステップ 1 Cisco Unified Communications Manager の管理ページにサインインします。
- ステップ 2 [システム (System)] > [LDAP] > [LDAPディレクトリ (LDAP Directory)] を選択します。
- ステップ 3 [検索 (Find)] を使用して LDAPディレクトリを見つけます。
- ステップ 4 LDAPディレクトリ名をクリックします。
- ステップ 5 [Perform Full Sync Now (完全同期を今すぐ実施)] をクリックします。

Cisco Unified Communications Manager にユーザを直接追加する

Lightweight Directory Access Protocol (LDAP) ディレクトリを使用しない場合、次の手順に従って、Cisco Unified Communications Manager Administration で直接ユーザを追加することができます。



- (注) LDAP が同期している場合、ユーザを Cisco Unified Communications Manager の管理ページに追加できません。

手順

- ステップ 1 Cisco Unified Communications Manager の管理で、[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択します。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 [ユーザ情報 (User Information)] ペインで、次の情報を入力します。
- [ユーザー ID (User ID)] : エンドユーザの識別名を入力します。Cisco Unified Communications Manager では、ユーザー ID の作成後の変更はできません。姓に使用できる特殊文字は、=、+、<、>、#、;、\、,、「」、および空白です。例 : johndoe
 - [パスワード (Password)] および [パスワードの確認 (Confirm Password)] : エンドユーザのパスワードとして、5 文字以上の英数字または特殊文字を入力します。姓に使用できる特殊文字は、=、+、<、>、#、;、\、,、「」、および空白です。

- [姓 (Last Name)] : エンドユーザの姓を入力します。姓に使用できる特殊文字は、=、+、<、>、#、;、\、,、'、および空白です。例 : doe
- [電話番号 (Telephone Number)] : エンドユーザのプライマリ電話番号を入力します。エンドユーザは、電話機に複数の回線を接続できます。例 : 26640 (John Doe の社内電話番号)

ステップ 4 [保存 (Save)] をクリックします。

エンドユーザ グループにユーザを追加する

ユーザを Cisco Unified Communications Manager の標準エンドユーザグループに追加するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページから、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセス コントロール グループ (Access Control Group)] を選択します。

[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索 (Find)] をクリックします。

ステップ 3 [標準 CCM エンドユーザ (Standard CCM End Users)] リンクを選択します。対象の標準 CCM エンドユーザについての [ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。

ステップ 4 [グループにエンドユーザを追加 (Add End Users to Group)] を選択します。[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。

ステップ 5 [ユーザの検索 (Find User)] ドロップダウン リスト ボックスを使用して、追加するユーザを探し、[検索 (Find)] をクリックします。

検索条件に一致するユーザのリストが表示されます。

ステップ 6 表示されるレコードのリストで、このユーザグループに追加するユーザのチェックボックスをクリックします。リストが長い場合は、下部のリンクを使用すると、さらに多くの結果を表示できます。

(注) 検索結果のリストには、すでにそのユーザグループに属しているユーザは表示されません。

ステップ 7 [選択項目の追加 (Add Selected)] を選択します。

電話機とユーザの関連付け

Cisco Unified Communications Manager の [エンド ユーザ (End User)] ウィンドウから、電話機をユーザに関連付けます。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページから、[ユーザ管理 (User Management)] > [エンド ユーザ (End User)] の順に選択します。

[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索 (Find)] をクリックします。

ステップ 3 表示されるレコードのリストで、ユーザのリンクを選択します。

ステップ 4 [デバイスの割り当て (Device Associations)] を選択します。

[ユーザ デバイス割り当て (User Device Association)] ウィンドウが表示されます。

ステップ 5 適切な検索条件を入力し、[検索 (Find)] をクリックします。

ステップ 6 デバイスの左にあるボックスをオンにして、ユーザに関連付けるデバイスを選択します。

ステップ 7 [選択/変更の保存 (Save Selected/Changes)] を選択して、デバイスをユーザに関連付けます。

ステップ 8 ウィンドウの右上にある [関連リンク (Related Links)] ドロップダウンリストから、[ユーザの設定に戻る (Back to User)] を選択し、[移動 (Go)] をクリックします。

[エンド ユーザの設定 (End User Configuration)] ウィンドウが表示され、選択した関連付けられたデバイスが [制御するデバイス (Controlled Devices)] ペインに表示されます。

ステップ 9 [選択/変更の保存 (Save Selected/Changes)] を選択します。

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) は、制御する Cisco Unified Communications Manager との通信が切断されたときに、電話機の基本的な機能へのアクセスを確保します。このシナリオでは、電話機は進行中のコールをアクティブなまま保持し、ユーザは使用可能な機能のサブセットにアクセスできます。フェールオーバーが発生すると、ユーザの電話機にアラートメッセージが表示されます。

SRST については、「」を参照してください。 <https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html>

次の表は、フェールオーバー中の機能の利用可能性について説明します。

表 14: SRST 機能のサポート

機能	サポートあり	注
発信	はい	
終了	はい	
リダイヤル	はい	
回答	はい	
保留	はい	
再開	はい	
会議	はい	3 ウェイのみ、ローカル ミキシングのみ。
会議リスト	なし	
転送	はい	打診のみ。
アクティブ コールへの転送 (直接転送)	なし	
自動応答	はい	
コール待機	はい	
発信者 ID	はい	
統合セッション表示	はい	他の機能により制限されるため、会議が唯一サポートされている機能です。
ボイスメール	はい	ボイスメールは Cisco Unified Communications Manager クラスタの他のユーザと同期されません。

機能	サポートあり	注
不在転送	はい	転送ステートは SRST モードにシェア ドラインアピアランスがないため転送 を設定する電話機でのみ使用できます。 [すべてのコールの転送 (Call Forward All)] 設定は、Cisco Unified Communications Manager から SRST へ のフェールオーバーまたは SRST から Communications Manager へのフェール バックには保存されません。 Communications Manager で引き続きア クティブな元の [すべてのコールの転送 (Call Forward All)] は、フェールオー バー後にデバイスが Communications Manager に再接続されると表示される 必要があります。
短縮ダイヤル	はい	
ボイスメールへ (即転送)	なし	[即転送 (iDivert)] ソフトキーは表示 されません。
回線フィルタ	一部	回線はサポートされますが、共有でき ません。
パーク モニタリング	なし	[パーク (Park)] ソフトキーが表示さ れません。
拡張メッセージ待機インジ ケータ	はい	メッセージのカウントバッジが電話の 画面に表示されます。
ダイレクト コール パーク	なし	ソフトキーは表示されません。
保留復帰	はい	
リモート回線の保留	なし	コールは、内線保留コールとして表示 されます。
ミーティング	なし	[ミーティング (Meet Me)] ソフトキーが 表示されません。
ピックアップ	はい	
グループ ピックアップ	なし	ソフトキーは表示されません。
その他のグループ ピック アップ	なし	ソフトキーは表示されません。

機能	サポートあり	注
迷惑呼 ID	はい	
QRT	はい	
ハントグループ	なし	ソフトキーは表示されません。
モビリティ	なし	ソフトキーは表示されません。
プライバシー	なし	ソフトキーは表示されません。
折り返し	なし	[折返し (Call Back)] ソフトキーが表示されません。
サービス URL	はい	サービス URL が割り当てられているプログラム可能なラインキーは表示されません。



第 6 章

セルフケアポータルへの管理

- [セルフケアポータルの概要 \(81 ページ\)](#)
- [セルフケアポータルへのユーザのアクセスの設定 \(82 ページ\)](#)
- [セルフケアポータルの表示のカスタマイズ \(82 ページ\)](#)

セルフケアポータルの概要

Cisco Unified Communications セルフケアポータルから、電話の機能や設定をカスタマイズし、制御できます。

管理者は、セルフケアポータルへのアクセスを制御します。また、ユーザがセルフケアポータルにアクセスできるように、情報を提供する必要があります。

ユーザを Cisco Unified Communications セルフケアポータルにアクセス可能にする前に、Cisco Unified Communications Manager Administration を使用して、ユーザを標準の Cisco Unified Communications Manager エンドユーザグループに追加する必要があります。

エンドユーザには、必ず、セルフケアポータルに関する次の情報を提供してください。

- アプリケーションにアクセスするための URL。この URL は、次のとおりです。
`https://<server_name:portnumber>/ucmuser/` (server_name は Web サーバーがインストールされているホスト、portnumber はホストのポート番号です)。
- アプリケーションにアクセスするためのユーザー ID とデフォルトパスワード。
- ユーザがポータルを使用して実行できるタスクの概要。

これらの設定値は、ユーザを Cisco Unified Communications Manager に追加したときに入力した値と同じです。

詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

セルフケアポータルへのユーザのアクセスの設定

セルフケアポータルにアクセスするには、事前にアクセスを許可しておく必要があります。

手順

- ステップ 1 Cisco Unified Communications Manager Administration で、**[User Management]** > **[End User]** を選択します。
- ステップ 2 ユーザを検索します。
- ステップ 3 ユーザー ID リンクをクリックします。
- ステップ 4 ユーザのパスワードと PIN が設定されていることを確認します。
- ステップ 5 **[Permissions Information]** セクションで、グループリストに **[Standard CCM End Users]** が含まれていることを確認します。
- ステップ 6 **保存** を選択します。

セルフケアポータルの表示のカスタマイズ

セルフケアポータルにはほとんどのオプションが表示されます。ただし、Cisco Unified Communications Manager Administration のエンタープライズ パラメータ設定で次のオプションを指定する必要があります。

- Show Ring Settings
- Show Line Label Settings



(注) この設定値は、サイトのすべてのセルフケアポータル ページに適用されます。

手順

- ステップ 1 Cisco Unified Communications Manager Administration で、**[System]** > **[Enterprise Parameters]** を選択します。
- ステップ 2 **[Self Care Portal]** 領域で、**[Self Care Portal Default Server]** フィールドを設定します。
- ステップ 3 ポータルでユーザがアクセスできるパラメータをイネーブルまたはディセーブルにします。
- ステップ 4 **保存** を選択します。



第 III 部

Cisco IP 会議用電話の管理

- [Cisco IP 会議用電話のセキュリティ \(85 ページ\)](#)
- [Cisco IP 会議用電話のカスタマイズ \(107 ページ\)](#)
- [Cisco IP 会議用電話の機能とセットアップ \(111 ページ\)](#)
- [社内ディレクトリとパーソナルディレクトリ \(151 ページ\)](#)



第 7 章

Cisco IP 会議用電話のセキュリティ

- [Cisco IP 電話 セキュリティの概要 \(85 ページ\)](#)
- [電話ネットワークのセキュリティ強化機能 \(86 ページ\)](#)
- [サポート対象のセキュリティ機能 \(87 ページ\)](#)

Cisco IP 電話 セキュリティの概要

セキュリティ機能は、電話機の ID やデータへの脅威など、複数の脅威を防止します。セキュリティ機能は、電話機と Cisco Unified Communications Manager サーバ間に認証された通信ストリームを確立し、これを維持するとともに、電話機がデジタル署名されたファイルのみを使用することを確認します。

Cisco Unified Communications Manager リリース 8.5(1) 以降のはデフォルトでセキュリティ機能が搭載されており、CTL クライアントを実行しなくても、Cisco IP 電話に次のセキュリティ機能が提供されます。

- 電話機の設定ファイルの署名
- 電話機の設定ファイルの暗号化
- HTTPS with Tomcat および他の Web サービスの利用



(注) シグナリングおよびメディア機能を保護するには、引き続き、CTL クライアントを実行し、ハードウェア eToken を使用する必要があります。

セキュリティ機能の詳細については、ご使用の Cisco Unified Communications Manager のマニュアルを参照してください。

認証局プロキシ関数 (CAPF) に関連付けられた必要なタスクの実行後、ローカルで有効な証明書 (LSC) が電話機にインストールされます。LSC は Cisco Unified Communications Manager の管理ページから設定できます。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

WLAN 認証を使用する EAP-TLS のユーザ証明書として LSC を使用することはできません。

あるいは、電話機の [セキュリティのセットアップ (Security Setup)] メニューから LSC のインストールを開始することもできます。このメニューでは、LSC の更新および削除も実行できます。

Cisco IP 会議用電話 8832 は、連邦情報処理標準 (FIPS) に準拠します。正常に機能するには、FIPS モードで 2048 ビット以上の RSA キー サイズが必要です。RSA サーバ証明書が 2048 ビット以上でない場合、電話機は Cisco Unified Communications Manager に登録されず、[電話機を登録できませんでした。(Phone failed to register.)] [証明書のキー サイズは FIPS に準拠していません (Cert key size is not FIPS compliant)] と表示されます。

FIPS モードで秘密キー (LSC または MIC) を使用することはできません。

2048 ビットより小さい LSC がすでに電話機にある場合、FIPS を有効にする前に、LSC キー サイズを 2048 ビット以上に更新しておく必要があります。

関連トピック

[重要な証明書のローカルでのセットアップ \(92 ページ\)](#)

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

電話ネットワークのセキュリティ強化機能

Cisco Unified Communications Manager 11.5(1) および 12.0(1) では、強化されたセキュリティ環境での動作が可能です。これらの強化機能により、電話ネットワークが、一連の厳密なセキュリティ管理とリスク管理の制御下で動作するようになり、自分自身とユーザが保護されます。

Cisco Unified Communications Manager 12.5 (1) は拡張セキュリティ環境に対応していません。Cisco Unified Communications Manager 12.5 (1) にアップグレードする前に FIPS を無効にすると、TFTP やその他のサービスが正しく機能しなくなります。

強化されたセキュリティ環境には、次の機能が含まれています。

- 連絡先検索認証。
- リモート監査ロギングのデフォルトプロトコルとしての TCP。
- FIPS モード。
- クレデンシャル ポリシーの改善。
- デジタル署名のための SHA-2 ファミリー ハッシュのサポート。
- 512 および 4096 ビットの RSA キー サイズのサポート。

Cisco Unified Communications Manager リリース 14.0 および Cisco IP 電話ファームウェア リリース 14.0 以降では、電話機は SIP OAuth 認証をサポートします。

OAuth は、Cisco Unified Communications Manager リリース 14.0(1) SU1 以降のプロキシトリビアルファイル転送プロトコル (TFTP) および Cisco IP 電話ファームウェア リリース 14.1(1) でサポートされます。プロキシ TFTP およびプロキシ TFTP 用の OAuth は、Mobile and Remote Access (MRA) ではサポートされません。

セキュリティ設定に関するその他の情報については、以下を参考にしてください。

- *Cisco Unified Communications Manager* システム設定ガイド、リリース 14.0(1) 以降 (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)。
- *Cisco Unified Communications Manager* セキュリティガイド (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>)
- SIP OAuth: *Cisco Unified Communications Manager* 機能設定ガイド (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)



-
- (注) Cisco IP 電話には、限られた数の Identity Trust List (ITL) ファイルのみ保存できます。Cisco Unified Communications Manager が電話機に送信できるファイルの数を制限する必要があるため、電話機の ITL ファイルは最大 64K に制限されています。
-

サポート対象のセキュリティ機能

セキュリティ機能は、電話機の ID やデータへの脅威など、複数の脅威を防止します。セキュリティ機能は、電話機と Cisco Unified Communications Manager サーバ間に認証された通信ストリームを確立し、これを維持するとともに、電話機がデジタル署名されたファイルのみを使用することを確認します。

Cisco Unified Communications Manager リリース 8.5(1) 以降のはデフォルトでセキュリティ機能が搭載されており、CTL クライアントを実行しなくても、Cisco IP 電話に次のセキュリティ機能が提供されます。

- 電話機の設定ファイルの署名
- 電話機の設定ファイルの暗号化
- HTTPS with Tomcat および他の Web サービスの利用



-
- (注) シグナリングおよびメディア機能を保護するには、引き続き、CTL クライアントを実行し、ハードウェア eToken を使用する必要があります。
-

Cisco Unified Communications Manager システムにセキュリティを実装すると、電話機や Cisco Unified Communications Manager サーバの ID 盗用、データの改ざん、およびコール シグナリングとメディア ストリームの改ざんを防止できます。

これらの脅威を軽減するため、Cisco Unified IP テレフォニー ネットワークは、電話機とサーバの間にセキュアな（暗号化された）通信ストリームを確立し、維持します。ファイルはデジタル署名してから電話機に転送し、Cisco IP 電話 間では、メディア ストリームとコール シグナリングを暗号化します。

認証局プロキシ関数（CAPF）に関連付けられた必要なタスクの実行後、ローカルで有効な証明書（LSC）が電話機にインストールされます。LSC は Cisco Unified Communications Manager の管理ページで設定できます。詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。あるいは、電話機の [セキュリティのセットアップ（Security Setup）] メニューから LSC のインストールを開始することもできます。このメニューでは、LSC の更新および削除も実行できます。

WLAN 認証を使用する EAP-TLS のユーザ証明書として LSC を使用することはできません。

電話機では電話セキュリティ プロファイルを使用します。この中では、デバイスがセキュリティ保護の対象になるかどうかを定義します。電話へセキュリティプロファイルを適用する方法の詳細は、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco Unified Communications Manager の管理でセキュリティ関連の設定を行うと、電話機の設定ファイルに重要な情報が保存されます。設定ファイルのプライバシーを確保するには、そのファイルを暗号化用に設定する必要があります。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco Unified Communications Manager システムにセキュリティを実装すると、電話機や Cisco Unified Communications Manager サーバの ID 盗用、データの改ざん、およびコールシグナリングとメディア ストリームの改ざんを防止できます。

次の表に、Cisco IP 会議用電話 8832 シリーズでサポートされるセキュリティ機能の概要を示します。これらの機能と、Cisco Unified Communications Manager および Cisco IP 電話セキュリティの詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

表 15: セキュリティ機能の概要

機能	説明
イメージ認証（Image authentication）	ファームウェア イメージが電話機にロードされる前に、署名付きバイナリ ファイル（拡張子 .sbn）を使用して、ファームウェア イメージに対する改ざんを防止します。イメージが改ざんされると、電話機は認証プロセスに失敗し、新しいイメージを拒否します。

機能	説明
カスタマーサイト証明書のインストール (Customer-site certificate installation)	各電話機は、デバイス認証に一意の証明書が必要とします。電話機には製造元でインストールされる証明書 (MIC) が含まれますが、追加のセキュリティについては、Cisco Unified Communications Manager の管理ページで、認証局プロキシ関数 (CAPF) を使用して証明書をインストールするように指定できます。あるいは、電話機の [セキュリティ設定 (Security Configuration)] メニューからローカルで有効な証明書 (LSC) をインストールします。
デバイス認証 (Device authentication)	Cisco Unified Communications Manager サーバと電話機間で、一方のエンティティが他方のエンティティの証明書を受け入れるときに行われます。電話機と Cisco Unified Communications Manager の間でセキュアな接続を確立するかどうかを判別し、必要に応じて TLS プロトコルを使用してエンティティ間にセキュアなシグナリングパスを作成します。Cisco Unified Communications Manager で電話機を認証できない限り、Cisco Unified Communications Manager ではそれらの電話機は登録されません。
ファイル認証 (File authentication)	電話機がダウンロードするデジタル署名ファイルを検証します。ファイルの作成後にファイルの改ざんが発生していないことを確認するため、電話で署名が検証されます。認証できないファイルは、電話機のフラッシュメモリに書き込まれません。電話機はこのようなファイルを拒否し、処理を続行しません。
シグナリング認証 (Signaling Authentication)	TLS プロトコルを使用して、シグナリングパケットが転送中に改ざんされていないことを検証します。
Manufacturing Installed Certificate (製造元でインストールされる証明書)	各電話機には、固有の製造元でインストールされる証明書 (MIC) が内蔵されており、デバイス認証に使用されます。MIC は、電話機に固有の永続的な ID 証明であり、Cisco Unified Communications Manager ではそれを利用して電話機を認証します。

機能	説明
セキュアな SRST リファレンス (Secure SRST reference)	セキュリティ目的で SRST リファレンスを設定してから、Cisco Unified Communications Manager の管理ページで従属デバイスをリセットすると、TFTP サーバは電話機の cnf.xml ファイルに SRST 証明書を追加し、そのファイルを電話機に送信します。その後、セキュアな電話機は TLS 接続を使用して、SRST 対応ルータと相互に対話します。
メディア暗号化	SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであることを証明し、意図したデバイスのみがデータを受け取り、読み取れるようにします。デバイスのメディアプライマリキーペアの作成、デバイスへのキーの配布、キーが転送される間のキーの配布のセキュリティの確保などが含まれます。
CAPF (Certificate Authority Proxy Function)	電話機に非常に高い処理負荷がかかる、証明書生成手順の一部を実装します。また、キーの生成および証明書のインストールのために電話機と対話します。電話機の代わりに、お客様指定の認証局に証明書を要求するよう CAPF を設定できます。または、ローカルで証明書を生成するように CAPF を設定することもできます。
セキュリティプロファイル (Security profiles)	電話機が非セキュア、認証済み、暗号化済みのいずれであるかを定義します。
暗号化された設定ファイル (Encrypted configuration files)	電話機の設定ファイルのプライバシーを確保できるようにします。
電話機の Web サーバ機能の無効化 (オプション)	電話機の多様な操作統計情報を表示する Web ページへのアクセスを禁止できます。

機能	説明
電話のセキュリティ強化 (Phone hardening)	<p>Cisco Unified Communications Manager の管理ページから制御する追加セキュリティオプションです。</p> <ul style="list-style-type: none"> 電話機の Web ページへのアクセスを無効にする <p>(注) [GARP を使う (GARP Enabled)] および [ボイス VLAN を使う (Voice VLAN enabled)] の各オプションの現在の設定値は、電話機の [設定 (Configuration)] メニューで確認できます。</p>
802.1X 認証	<p>電話機では、802.1X 認証を使用して、ネットワークへのアクセス権を要求および取得できます。</p>
AES 256 暗号化 (AES 256 Encryption)	<p>Cisco Unified Communications Manager リリース 10.5(2)以降の以降に接続している電話機は、シグナリングとメディア暗号化に関する TLS および SIP の AES 256 暗号化をサポートします。これにより電話機は、SHA-2 (Secure Hash Algorithm) 標準および Federal Information Processing Standard (FIPS) に準拠する AES-256 ベースの暗号を使用して TLS 1.2 接続を開始し、サポートすることができます。新しい暗号は次のとおりです。</p> <ul style="list-style-type: none"> TLS 接続用 : <ul style="list-style-type: none"> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 sRTP 用 : <ul style="list-style-type: none"> AEAD_AES_256_GCM AEAD_AES_128_GCM <p>詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。</p>

機能	説明
楕円曲線デジタル署名アルゴリズム (ECDSA) 証明書	コモンクライテリア (共通基準、CC) 認証の一部として、バージョン 11.0 の ECDSA 証明書が Cisco Unified Communications Manager によって追加されました。これは、バージョン Cisco Unified Communications Manager 11.5 以降のすべての Voice Operating System (VOS) 製品に影響します。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

重要な証明書のローカルでのセットアップ

この作業は、認証文字列方式を使用した LSC の設定に適用されます。

始める前に

次の点を調べて、対象の Cisco Unified Communications Manager および認証局プロキシ関数 (CAPF) のセキュリティ設定が完了していることを確認してください。

- CTL ファイルまたは ITL ファイルに CAPF 証明書が含まれていること。
- Cisco Unified Communications オペレーティングシステムの管理ページで、CAPF 証明書がインストールされていることを確認してください。
- CAPF が実行および設定されていること。

これらの設定の詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 CAPF の設定時に設定された CAPF 認証コードを入手します。

ステップ 2 電話機から、[設定 (Settings)] を選択します。

ステップ 3 [管理設定 (Admin Settings)] > [セキュリティ設定 (Security Setup)] を選択します。

(注) Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration)] ウィンドウにある設定アクセスフィールドを使用すると、[設定 (Settings)] メニューへのアクセスを制御できます。

ステップ 4 [LSC] を選択し、[選択 (Select)] または [更新 (Update)] を押します。

認証文字列を要求するプロンプトが電話機に表示されます。

ステップ 5 認証コードを入力し、[送信 (Submit)] を押します。

CAPF の設定に応じて、電話機で LSC のインストール、更新、または削除が開始されます。この作業の間、[セキュリティ設定 (Security Configuration)] メニューの [LSC] オプションフィールドに一連のメッセージが表示されるので、進捗状況をモニタできます。手順が完了すると、電話機に [インストール済み (Installed)] または [未インストール (Not Installed)] と表示されます。

LSC のインストール、更新、または削除プロセスは、完了するのに長時間かかることがあります。

電話機のインストール手順が正常に実行されると、「インストール済み (Installed)」メッセージが表示されます。電話機に「未インストール (Not Installed)」と表示された場合は、認証文字列に誤りがあるか、電話機のアップグレードが有効になっていない可能性があります。CAPF 操作で LSC を削除し、電話機に「未インストール (Not Installed)」と表示された場合、それは操作が成功したことを示しています。CAPF サーバはこのエラーメッセージをログに記録します。ログを見つけ、エラーメッセージの意味を理解するには、CAPF サーバドキュメントを参照してください。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

FIPS モードの有効化


手順

-
- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択し、電話機を見つけます。
 - ステップ 2 [Product Specific Configuration] 領域まで移動します。
 - ステップ 3 [FIPS モード (FIPS Mode)] フィールドを [有効 (Enabled)] に設定します。
 - ステップ 4 [設定の適用 (Apply Config)] を選択します。
 - ステップ 5 [保存 (Save)] を選択します。
 - ステップ 6 電話機を再起動します。
-

電話コールのセキュリティ

電話機にセキュリティを実装している場合は、電話スクリーンに表示されるアイコンによって、セキュアな電話コールや暗号化された電話コールを識別できます。また、コールの開始時にセキュリティトーンが再生される場合は、接続された電話機がセキュアであり保護されているかどうか判断できます。

セキュアなコールでは、すべてのコール シグナリングとメディア ストリームが暗号化されます。セキュアなコールは高度なレベルのセキュリティを提供し、コールに整合性とプライバ

シーを提供します。処理中のコールが暗号化されているときは、電話スクリーンのコール時間タイマーの右側にあるコール進捗アイコンが、次のアイコン  に変化します。



- (注) コールが PSTN などの非 IP コール レッグを経由してルーティングされる場合、コールが IP ネットワーク内で暗号化されており、鍵のアイコンが関連付けられていても、そのコールはセキュアではないことがあります。

セキュアなコールではコールの開始時にセキュリティ トーンが再生され、接続先の電話機もセキュアな音声を送受信していることを示します。セキュアでない電話機にコールが接続されると、セキュリティ トーンは再生されません。



- (注) セキュアなコールは、2台の電話機の間でサポートされます。セキュアな会議ブリッジにより、セキュアな会議、Cisco Extension Mobility、および共有回線を設定できます。


Cisco Unified Communications Manager で電話機をセキュア（暗号化および信頼された）として設定した場合、その電話機には「保護」ステータスを割り当てることができます。その後、必要に応じて、保護された電話機は、コールの初めに通知トーンを再生するように設定できます。

- [保護されたデバイス (Protected Device)] : セキュアな電話機のステータスを保護に変更するには、Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration)] ウィンドウにある [保護されたデバイス (Protected Device)] チェックボックスをオンにします ([デバイス (Device)] > [電話 (Phone)])。
- [セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] : 保護された電話機で、セキュアまたは非セキュアな通知トーンの再生を有効にするには、[セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] 設定を [はい (True)] に設定します。デフォルトでは、[セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] は [いいえ (False)] に設定されます。このオプションは、Cisco Unified Communications Manager の管理 ([システム (System)] > [サービス パラメータ (Service Parameters)]) で設定します。サーバを選択してから、Unified Communications Manager サービスを選択します。[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで、[機能 - セキュア トーン (Feature - Secure Tone)] 領域内にあるオプションを選択します。デフォルトは False です。

セキュアな会議コールの特定

セキュアな会議コールを開始し、参加者のセキュリティレベルをモニタすることができます。セキュアな電話会議は、次のプロセスに従って確立されます。

1. ユーザがセキュアな電話機で会議を開始します。
2. Cisco Unified Communications Manager が、コールにセキュアな会議ブリッジを割り当てます。

3. 参加者が追加されると、Cisco Unified Communications Manager は、各電話機のセキュリティモードを検証し、セキュアな会議のレベルを維持します。
4. 電話機に会議コールのセキュリティレベルが表示されます。セキュアな会議では、電話機の画面の [会議 (Conference)] の右側にセキュアアイコン  が表示されます。



(注) セキュアなコールは、2 台の電話機の間でサポートされます。保護された電話機では、セキュアなコールが設定されている場合、会議コール、シェアドライン、エクステンション モビリティなどの一部の機能を使用できません。

次の表は、発信側の電話機のセキュリティレベル、参加者のセキュリティレベル、およびセキュアな会議ブリッジの可用性に応じた、会議のセキュリティレベルの変更に関する情報を示しています。

表 16: 会議コールのセキュリティの制限事項


発信側の電話機のセキュリティレベル	使用する機能	参加者のセキュリティレベル	動作結果
非セキュア	会議	セキュア	非セキュアな会議ブリッジ 非セキュアな会議
セキュア	会議	少なくとも1台のメンバーが非セキュア。	セキュアな会議ブリッジ 非セキュアな会議
セキュア	会議	セキュア	セキュアな会議ブリッジ セキュアな暗号化レベルの会議
非セキュア	ミーティング	最小限のセキュリティレベルが暗号化。	発信側は「セキュリティレベルを満たしていません。コールを拒否します (Does not meet Security Level, call rejected)」というメッセージを受け取る。

発信側の電話機のセキュリティレベル	使用する機能	参加者のセキュリティレベル	動作結果
セキュア	ミーティング	最小限のセキュリティレベルは非セキュア。	セキュアな会議ブリッジ 会議はすべてのコールを受け入れる。

セキュアな電話コールの識別

ユーザの電話機および相手側の電話機でセキュアなコールが設定されている場合にセキュアなコールが確立されます。相手側の電話機は、同じ Cisco IP ネットワーク内にあっても、Cisco IP ネットワーク以外のネットワークにあってもかまいません。セキュアなコールは2台の電話機間でのみ形成できます。セキュアな会議ブリッジのセットアップ後、電話会議ではセキュアなコールがサポートされます。

セキュアなコールは、次のプロセスに従って確立されます。

1. ユーザがセキュアな電話機（セキュリティモードで保護された電話機）でコールを開始します。
2. 電話スクリーンにセキュアアイコン  が表示されます。このアイコンは、この電話機がセキュアなコール用に設定されていることを示しますが、接続する他の電話機もセキュアであるという意味ではありません。
3. そのコールが別のセキュアな電話機に接続された場合は、ユーザにセキュリティトーンが聞こえ、通話の両端が暗号化および保護されていることを示します。コールが非セキュアな電話機に接続された場合は、ユーザにはセキュリティトーンが聞こえません。



- (注) セキュアなコールは、2台の電話機の間でサポートされます。保護された電話機では、セキュアなコールが設定されている場合、会議コール、シェアライン、エクステンション モビリティなどの一部の機能を使用できません。

保護された電話機だけで、セキュアまたは非セキュアなインディケーショントーンが再生されます。保護されていない電話機ではトーンは聞こえません。コール中にコール全体のステータスが変化すると、それによって通知トーンも変化し、保護された電話機は対応するトーンを再生します。

このような状況にない場合、保護された電話機はトーンを再生しません。

- [セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] オプションが有効になっている場合
 - エンドツーエンドのセキュアなメディアが確立され、コールステータスがセキュアになった場合、電話機はセキュア インディケーション トーン（間に小休止を伴う3回の長いビーブ音）を再生します。

- エンドツーエンドの非セキュアなメディアが確立され、コールステータスが非セキュアになった場合、電話機は、非セキュアのインディケーション トーンを再生します（間に小休止を伴う 6 回の短いビープ音）。

[セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] オプションが無効になっている場合、トーンは再生されません。

割り込みの暗号化

Cisco Unified Communications Manager は、会議の確立時に電話機のセキュリティ ステータスを確認し、会議のセキュリティ表示を変更するか、またはコールの確立をブロックしてシステムの整合性とセキュリティを維持します。

電話機に暗号化が設定されていない場合、その電話機を使用して暗号化されたコールに割り込むことはできません。この場合、割り込みに失敗すると、割り込みが開始された電話機でリオーダー トーン（速いビジー音）が聞こえます。

割り込みの開始側の電話機に暗号化が設定されている場合、割り込みの開始側は暗号化された電話機からセキュアでないコールに割り込むことができます。割り込みが発生すると、Cisco Unified Communications Manager はそのコールをセキュアでないコールに分類します。

割り込みの開始側の電話機に暗号化が設定されている場合、割り込みの開始側は暗号化されたコールに割り込むことができ、電話機はそのコールが暗号化されていることを示します。

WLAN セキュリティ

通信圏内にあるすべての WLAN デバイスは他の WLAN トラフィックをすべて受信できるため、WLAN 内の音声通信の保護は重要です。侵入者による音声トラフィックの操作や傍受を防止するため、Cisco SAFE セキュリティアーキテクチャは、Cisco IP 電話と Cisco Aironet AP をサポートします。ネットワーク内のセキュリティの詳細については、http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html を参照してください。

Cisco Wireless IP テレフォニー ソリューションは、ワイヤレス Cisco IP 電話がサポートする次の認証方式を使用して、不正ログインおよび改ざんされた通信を防ぐワイヤレスネットワークセキュリティを提供します。

- オープン認証：オープン システムでは、任意のワイヤレス デバイスが認証を要求できません。要求を受けた AP は、任意のリクエストまたはユーザのリスト上にあるリクエストだけに認証を与える場合があります。ワイヤレス デバイスと AP との間の通信は暗号化されない可能性もあります。暗号化される場合、デバイスは有線と同等のプライバシー (WEP) キーを使用してセキュリティを提供できます。WEP を使用しているデバイスは、WEP を使用している AP での認証だけを試みます。
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) 認証：このクライアント サーバのセキュリティアーキテクチャは、AP と、Cisco Access Control Server (ACS) などの RADIUS サーバとの間の Transport Level Security (TLS) トンネル内の EAP トランザクションを暗号化します。

TLS トンネルでは、クライアント（電話機）と RADIUS サーバの間の認証に Protected Access Credential (PAC) が使用されます。サーバは Authority ID (AID) をクライアント（電話機）に送信します。それを受けてクライアントは適切な PAC を選択します。クライアント（電話機）は PAC-Opaque を RADIUS サーバに返します。サーバは、プライマリキーで PAC を復号します。これで両方のエンドポイントに同じ PAC キーが含まれ、TLS トンネルが構築されます。EAP-FAST では、自動 PAC プロビジョニングがサポートされていますが、RADIUS サーバ上で有効にする必要があります。



注 Cisco ACS での PAC の有効期限は、デフォルトで 1 週間です。電話機に期限切れの PAC が存在する場合、電話機が新しい PAC を取得するまでの間は、RADIUS サーバでの認証に比較的長い時間がかかります。PAC プロビジョニングの遅延を回避するには、ACS サーバまたは RADIUS サーバで PAC の有効期間を 90 日以上に設定します。

- 拡張認証プロトコル-トランスポート層セキュリティ (EAP-TLS) 認証：EAP-TLS では、認証とネットワークアクセスにクライアント証明書が必要です。有線 EAP-TLS の場合、クライアント証明書は電話機の MIC または LSC のいずれかです。LSC は、有線 EAP-TLS に推奨されるクライアント認証証明書です。
- Protected Extensible Authentication Protocol (PEAP)：クライアント（電話機）と RADIUS サーバ間の、シスコ独自のパスワードベースの相互認証方式です。Cisco IP 電話は、ワイヤレス ネットワークでの認証に PEAP を使用できます。PEAP-MSCHAPV2 のみサポートされます。PEAP-GTC はサポートされていません。

次の認証方式では、RADIUS サーバを使用して認証キーを管理します。

- WPA/WPA2: 一意の認証キーを生成するために RADIUS サーバの情報を使用します。これらのキーは、中央集中型の RADIUS サーバで生成されるため、WPA/WPA2 は、AP および電話機に格納されている WPA 事前共有キーよりも高いセキュリティを提供します。
- 高速安全ローミング：RADIUS サーバとワイヤレス ドメイン サーバ (WDS) 上の情報を使用してキーを管理および認証します。WDS は、高速でセキュアな再認証用に、CCKM 対応クライアント デバイスのセキュリティ クレデンシャルのキャッシュを作成します。Cisco IP 電話 8800 シリーズは 802.11r (FT) をサポートしています。高速セキュアローミングを可能にするために、11r (FT) と CCKM の両方がサポートされています。しかしシスコは 802.11r (FT) 無線方式を利用することを強く推奨します。

WPA/WPA2 および CCKM では、暗号化キーは電話機に入力されず、AP と電話機の間で自動的に生成されます。ただし認証で使用する EAP ユーザ名とパスワードは、各電話機に入力する必要があります。

音声トラフィックの安全性を確保するため、Cisco IP 電話 では、暗号化方式として WEP、TKIP、および Advanced Encryption Standards (AES) をサポートします。暗号化にこれらのメ

カニズムを使用すると、AP と Cisco IP 電話 との間で、シグナリング SIP パケットと音声リアルタイム トランスポート プロトコル (RTP) パケットの両方が暗号化されます。

WEP

ワイヤレス ネットワークで WEP を使用すると、オープン認証または共有キー認証を使用することにより、AP で認証が行われます。正常に接続させるには、電話機で設定された WEP キーと AP で設定された WEP キーが一致する必要があります。Cisco IP 電話 は、40 ビット暗号化または 128 ビット暗号化を使用し、電話機および AP で静的なままの WEP キーをサポートしています。

EAP と CCKM の認証では、暗号化に WEP キーを使用できます。RADIUS サーバは WEP キーを管理し、すべての音声パケットの暗号化を認証した後で一意的なキーを AP に渡します。そのため、次の WEP キーを各認証で変更できます。

TKIP

WPA と CCKM は、WEP にいくつかの改良が加えられた TKIP 暗号化を使用します。TKIP は、パケットごとのキーの暗号化、および暗号化が強化されたより長い初期ベクトル (IV) を提供します。さらに、メッセージ完全性チェック (MIC) は、暗号化されたパケットが変更されていないことを確認します。TKIP は、侵入者が WEP を使用して WEP キーを解読する可能性を排除します。

AES

WPA2 認証に使用される暗号化方式。この暗号化の国内規格は、暗号化と復号化に同じキーを持つ対称型アルゴリズムを使用します。AES は、128 ビットサイズの暗号ブロック連鎖 (CBC) 暗号化を使用し、最小のキー サイズとして 128、192、および 256 ビットのキーをサポートします。Cisco IP 電話 は 256 ビットのキー サイズをサポートします。



(注) Cisco IP 電話 は、CMIC による Cisco Key Integrity Protocol (CKIP) をサポートしません。

認証方式と暗号化方式は、ワイヤレス LAN 内で設定されます。VLAN は、ネットワーク内および AP 上で設定され、認証と暗号化の異なる組み合わせを指定します。SSID は、VLAN と VLAN の特定の認証および暗号化方式に関連付けられます。ワイヤレス クライアント デバイスを正常に認証するには、認証および暗号化方式で使用する SSID と同じ SSID を AP と Cisco IP 電話 に設定する必要があります。

一部の認証方式では、特定のタイプの暗号化が必要です。オープン認証では、セキュリティを高めるために、暗号化で静的 WEP を使用できます。ただし、共有キー認証を使用している場合は、暗号化に静的 WEP を設定し、電話機で WEP キーを設定する必要があります。



- (注)
- WPA 事前共有キーまたは WPA2 事前共有キーを使用する場合、その事前共有キーを電話機で静的に設定する必要があります。これらのキーは、AP に存在するキーと一致している必要があります。
 - Cisco IP 電話 は、自動 EAP ネゴシエーションをサポートしていません。EAP-FAST モードを使用するには、EAP-FAST モードを指定する必要があります。

次の表に、Cisco IP 電話がサポートしている、Cisco Aironet AP で設定される認証方式と暗号化方式のリストを示します。表には、AP の設定に対応する電話機のネットワーク設定オプションを示します。

表 17: 認証方式と暗号化方式

Cisco IP 電話の設定	AP の設定			
Security Mode	セキュリティ	Key Management	暗号化	高速ローミング
なし	なし	なし	なし	該当なし
WEP	Static WEP	スタティック	WEP	該当なし
PSK	PSK	WPA	TKIP	なし
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

認証方式と暗号化方式を AP に設定する方法の詳細については、次の URL で入手可能なご使用のモデルおよびリリースの『Cisco Aironet Configuration Guide』を参照してください。

<http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243>

ワイヤレス LAN セキュリティ

Wi-Fi をサポートするシスコの電話機には追加のセキュリティ要件があり、追加の設定が必要になります。これらの追加手順には、証明書のインストール、および電話機と Cisco Unified Communications Manager でのセキュリティの設定が含まれます。

追加情報については、『Security Guide for Cisco Unified Communications Manager』を参照してください。

Cisco IP 電話の管理ページ

Wi-Fiをサポートするシスコの電話機には、他の電話機のページとは異なる特別な Web ページがあります。Simple Certificate Enrollment Protocol (SCEP) を使用できない場合に、電話機のセキュリティを設定するため、これらの特別な Web ページを使用します。これらのページを使用して、セキュリティ証明書を手動で電話機にインストールしたり、セキュリティ証明書をダウンロードしたり、電話機の日時を手動で設定したりします。

これらの Web ページには、デバイス情報、ネットワーク設定、ログ、統計情報など、他の電話機の Web ページに表示されるものと同じ情報が表示されます。

電話機の管理ページの設定

管理 Web ページは、電話機が工場から出荷された時点で有効になっていて、パスワードは「Cisco」に設定されています。ただし、電話機を Cisco Unified Communications Manager に登録する場合は、管理 Web ページを必ず有効にし、新しいパスワードを設定する必要があります。

電話機を登録した後、Web ページを初めて使用する前に、この Web ページを有効にして、サインインクレデンシャルを設定します。

有効にすると、管理 Web ページには、HTTPS ポート 8443 (<https://x.x.x.x:8443> (x.x.x.x は電話機の IP アドレスです)) でアクセスできます。

始める前に

管理 Web ページを有効にする前に、パスワードを決定します。パスワードには文字と数字を任意に組み合わせて指定できますが、長さは 8 ~ 127 文字の間にする必要があります。

ユーザ名は admin に固定されています。

手順

-
- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
 - ステップ 2 電話機を特定します。
 - ステップ 3 [Product Specific Configuration Layout] 領域で、[Web Admin] パラメータを [Enable] に設定します。
 - ステップ 4 [Admin Password] フィールドにパスワードを入力します。
 - ステップ 5 [保存 (Save)] を選択し、[OK] をクリックします。
 - ステップ 6 [設定の適用 (Apply Config)] を選択し、[OK] をクリックします。
 - ステップ 7 電話機を再起動します。
-

電話管理の Web ページにアクセスします。

管理 Web ページにアクセスするとき、管理ポートを指定する必要があります。

手順

ステップ 1 次のように電話機の IP アドレスを取得します。

- Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択し、電話機を見つけます。Cisco Unified Communications Manager に登録されている電話機の IP アドレスが、[Find and List Phones] ウィンドウと [Phone Configuration] ウィンドウの上部に表示されます。

ステップ 2 Web ブラウザを開いて、次の URL を入力します。ここで、*IP_address* は Cisco IP 電話の IP アドレスです。

https://<IP_address>:8443

ステップ 3 [Password] フィールドにパスワードを入力します。

ステップ 4 [送信 (Submit)] をクリックします。

電話機の管理 Web ページからユーザ証明書をインストールする

Simple Certificate Enrollment Protocol (SCEP) を使用できない場合、電話機にユーザ証明書を手動でインストールすることができます。

製造元でインストールされる証明書 (MIC) を EAP-TLS 用のユーザ証明書として使用できます。

ユーザ証明書をインストールした後、RADIUS サーバの信頼リストに追加する必要があります。

始める前に

電話機のユーザ証明書をインストールするには、その前に以下を用意する必要があります。

- PC に保存されたユーザ証明書。証明書は PKCS #12 形式である必要があります。
- 証明書の抽出パスワード。

手順

ステップ 1 電話機の管理 Web ページで、[証明書 (Certificates)] を選択します。

ステップ 2 PC の証明書を参照します。

ステップ 3 [抽出パスワード (Extract password)] フィールドに、証明書の抽出パスワードを入力します。

ステップ 4 [アップロード (Upload)] をクリックします。

ステップ 5 アップロードが完了したら、電話機を再起動します。

電話機の管理 Web ページから認証サーバ証明書をインストールする

Simple Certificate Enrollment Protocol (SCEP) を使用できない場合、電話機に認証サーバ証明書を手動でインストールすることができます。

RADIUS サーバ証明書を発行したルート CA 証明書は、EAP-TLS 用にインストールする必要があります。

始める前に

電話機に証明書をインストールするには、その前に認証サーバ証明書を PC に保存する必要があります。証明書は PEM (Base 64) または DER 形式でエンコードする必要があります。

手順

ステップ 1 電話機の管理 Web ページで、[証明書 (Certificates)] を選択します。

ステップ 2 [認証サーバ CA (管理 Web ページ) (Authentication server CA (Admin webpage))] フィールドを見つけて [インストール (Install)] をクリックします。

ステップ 3 PC の証明書を参照します。

ステップ 4 [アップロード (Upload)] をクリックします。

ステップ 5 アップロードが完了したら、電話機を再起動します。

複数の証明書をインストールする場合は、電話機を再起動する前に、すべての証明書をインストールします。

電話機の管理 Web ページからセキュリティ証明書を手動で削除する

Simple Certificate Enrollment Protocol (SCEP) を使用できない場合、電話機からセキュリティ証明書を手動で削除することができます。

手順

ステップ 1 電話機の管理 Web ページで、[証明書 (Certificates)] を選択します。

ステップ 2 [Certificates] ページで証明書を見つけます。

ステップ 3 [Delete] をクリックします。

ステップ 4 削除プロセスが完了したら、電話機を再起動します。

手動での電話機の日時の設定

証明書ベースの認証では、電話機に正しい日時を表示する必要があります。認証サーバは、電話機の日時を証明書の失効日と照合します。電話機とサーバの日時が一致しないと、電話機は動作を停止します。

電話機がネットワークから正しい情報を受信していない場合、次の手順を使用して電話機の日時を手動で設定します。

手順

ステップ 1 電話機の管理 Web ページで、[Date & Time] までスクロールします。

ステップ 2 次のいずれかの選択肢を実行します。

- ローカル サーバに電話機を同期する場合は、[電話機のローカルの日時を設定 (Set Phone to Local Date & Time)] をクリックします。
- [日付および時刻の指定 (Specify Date & Time)] フィールドで、メニューを使用して、月、日、年、時、分、秒を選択し、[電話機を特定の日時に設定 (Set Phone to Specific Date & Time)] をクリックします。

SCEP セットアップ

Simple Certificate Enrollment Protocol (SCEP) は、証明書の自動プロビジョニングおよび更新の標準です。これにより、電話機に証明書を手動でインストールせずに済みます。

SCEP プロダクト固有の設定パラメータの設定

電話機の Web ページで次の SCEP パラメータを設定する必要があります。

- RA IP アドレス
- SCEP サーバのルート CA 証明書の SHA-1 または SHA-256 フィンガープリント

Cisco IOS の登録局 (RA) は、SCEP サーバへのプロキシとして機能します。電話機の SCEP クライアントは、Cisco Unified Communications Manager からダウンロードされたパラメータを使用します。パラメータを設定すると、電話機から RA に SCEP getcs 要求が送信され、定義されたフィンガープリントを使用してルート CA 証明書が検証されます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。

ステップ 2 電話機を特定します。

ステップ 3 [Product Specific Configuration Layout] 領域までスクロールします。

ステップ 4 [WLAN SCEP Server] チェックボックスをオンにして、SCEP パラメータをアクティブ化します。

ステップ 5 [WLAN Root CA Fingerprint (SHA256 or SHA1)] チェックボックスをオンにして、SCEP QED パラメータをアクティブ化します。

Simple Certificate Enrollment Protocol サーバのサポート

Simple Certificate Enrollment Protocol (SCEP) サーバを使用する場合、サーバはユーザとサーバ証明書自動的に維持できます。SCEP サーバで、次のように SCEP 登録エージェント (RA) を設定します。

- PKI トラスト ポイントとして機能する
- PKI RA として機能する
- RADIUS サーバを使用してデバイス認証を実行する

詳細については、SCEP サーバのマニュアルを参照してください。

802.1X 認証

Cisco IP 電話は 802.1X 認証をサポートします。

Cisco IP 電話と Cisco Catalyst スイッチは、従来 Cisco Discovery Protocol (CDP) を使用して互いを識別し、VLAN 割り当てやインライン所要電力などのパラメータを決定します。

802.1X 認証のサポートには、次のようなコンポーネントが必要です。

- Cisco IP 電話: 電話機は、ネットワークへのアクセス要求を開始します。電話機には 802.1x サプリカントが含まれています。このサプリカントを使用して、ネットワーク管理者は IP 電話と LAN スイッチ ポートの接続を制御できます。電話機に含まれる 802.1X サプリカントの現在のリリースでは、ネットワーク認証に EAP-FAST オプションと EAP-TLS オプションが使用されています。
- Cisco Catalyst スイッチ (またはその他のサードパーティ製スイッチ) : スイッチは、オーセンティケータとして機能し、電話機と認証サーバの間でメッセージを渡すことができるように、802.1X をサポートしている必要があります。この交換が完了した後、スイッチはネットワークへの電話機のアクセスを許可または拒否します。

802.1X を設定するには、次の手順を実行する必要があります。

- 電話機で 802.1X 認証をイネーブルにする前に、他のコンポーネントを設定します。
- ボイス VLAN の設定 : 802.1X 標準では VLAN が考慮されないため、ボイス VLAN の設定はスイッチのサポートに基づいて行う必要があります。
 - 有効 : 複数ドメインの認証をサポートするスイッチを使用している場合は、ボイス VLAN を引き続き使用できます。
 - 無効 : スイッチがマルチドメイン認証をサポートしていない場合は、ボイス VLAN を無効にし、ネイティブ VLAN へのポートの割り当てを検討します。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)



第 8 章

Cisco IP 会議用電話のカスタマイズ

- [カスタム電話呼出音 \(107 ページ\)](#)
- [ダイヤルトーンのカスタマイズ \(109 ページ\)](#)

カスタム電話呼出音

Cisco IP 電話には Chirp1 と Chirp2 という 2 つのデフォルト呼出音（着信音）が付属しており、これらはハードウェアに内蔵されています。Cisco Unified Communications Manager にはいくつかの追加の電話呼出音もデフォルトで付属しており、これらはパルス符号変調（PCM）ファイルとしてソフトウェアに実装されています。PCM ファイル、およびサイトで使用できる呼出音リスト オプションを記述した XML ファイルが、各 Cisco Unified Communications Manager サーバの TFTP ディレクトリに配置されています。



注目 すべてのファイル名で大文字と小文字が区別されます。ファイル名の大/小文字を間違っていると、電話機には変更が適用されません。

詳細については、『[Feature Configuration Guide for Cisco Unified Communications Manager](#)』の「Custom Phone Rings and Backgrounds」の章を参照してください。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

カスタム電話呼出音のセットアップ

手順

ステップ 1 各カスタム呼出音の PCM ファイルを作成します（ファイルごとに呼出音 1 つ）。

PCM ファイルが「カスタム呼出音のファイル形式」のセクションに示す形式のガイドラインに従っていることを確認します。

ステップ 2 作成した新しい PCM ファイルを、クラスタ内の各 Cisco Unified Communications Manager の Cisco TFTP サーバにアップロードします。

詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

ステップ 3 修正内容を保存し、Ringlist-wb ファイルを閉じます。

ステップ 4 新しい Ringlist-wb ファイルをキャッシュに入れるには：

- Cisco Unified Serviceability を使用して TFTP サービスを停止し、開始します。
- [拡張サービス パラメータ (Advanced Service Parameters)] 領域にある [起動時の定数および bin ファイルのキャッシングの有効化 (Enable Caching of Constant and Bin Files at Startup)] TFTP サービス パラメータを無効にして、再び有効にします。「」

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

カスタム呼出音のファイル形式

Ringlist-wb.xml ファイルは、電話呼出音タイプのリストを含む XML オブジェクトを定義しています。このファイルには、呼出音タイプを 50 個まで記述します。呼出音タイプごとに、呼出音タイプに使用される PCM ファイルへのポインタ、および Cisco IP 電話の [呼出音タイプ (Ring Type)] メニューに表示されるテキストを記述します。このファイルは、各 Cisco Unified Communications Manager の Cisco TFTP サーバに保持されます。

CiscoIPPhoneRinglist XML オブジェクトは、次の簡単なタグセットを使用して情報を記述します。

```
<CiscoIPPhoneRingList>
  <Ring>
    <DisplayName/>
    <FileName/>
  </Ring>
</CiscoIPPhoneRingList>
```

定義名については、次の規則があります。それぞれの電話呼出音タイプについて、必須の DisplayName と FileName を記述する必要があります。

- DisplayName には、関連付けられた PCM ファイルのカスタム呼出音の名前を指定します。この名前は、Cisco IP 電話の [呼出音タイプ (Ring Type)] メニューに表示されます。
- FileName には、DisplayName に関連付けるカスタム呼出音の PCM ファイルの名前を指定します。



(注) DisplayName フィールドと FileName フィールドは、長さ 25 文字以下にする必要があります。

次に、2 つの電話呼出音タイプを定義した Ringlist-wb.xml ファイルの例を示します。

```
<CiscoIPPhoneRingList>
  <Ring>
    <DisplayName>Analog Synth 1</DisplayName>
    <FileName>Analog1.rwb</FileName>
  </Ring>
  <Ring>
    <DisplayName>Analog Synth 2</DisplayName>
    <FileName>Analog2.rwb</FileName>
  </Ring>
</CiscoIPPhoneRingList>
```

呼出音の PCM ファイルを Cisco IP 電話で正常に再生するには、ファイルが次の要件を満たしている必要があります。

- 未加工の PCM（ヘッダーなし）。
- サンプリング回数：8,000 回/秒。
- 1 サンプルあたり 8 ビット。
- Mu-law 圧縮
- 呼出音の最大サイズ = 16080 サンプル
- 呼出音の最小サイズ = 240 サンプル
- 呼出音のサンプル数 = 240 の倍数。
- 呼出音は、ゼロ交差で開始および終了する。

カスタム呼出音用の PCM ファイルを作成するには、次のファイル形式の要件に対応する任意の標準オーディオ編集パッケージを使用します。

ダイヤル トーンのカスタマイズ

内部コールと外部コールで異なるダイヤル トーンが鳴るように電話機をセットアップできます。必要に応じて、3つのダイヤル トーンのオプションから選択できます。

- [デフォルト (Default)] : 内部コールと外部コールに異なるダイヤル トーンを使用します。
- [内部 (Inside)] : 内部用のダイヤル トーンをすべてのコールに使用します。
- [外部 (Outside)] : 外部用のダイヤル トーンをすべてのコールに使用します。

[常に使用するダイヤル トーン (Always Use Dial Tone)] は、Cisco Unified Communications Manager の必須フィールドです。

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。

ステップ 2 該当するサーバを選択します。

ステップ 3 サービスとして [Cisco CallManager] を選択します。

ステップ 4 [クラスタ全体のパラメータ (Clusterwide Parameters)] ペインまでスクロールします。

ステップ 5 [常に使用するダイヤルトーン (Always Use Dial Tone)] を次のいずれかに設定します。

- 外側
- 内側
- デフォルト (Default)

ステップ 6 [保存 (Save)] を選択します。

ステップ 7 電話機を再起動します。



第 9 章

Cisco IP 会議用電話の機能とセットアップ

- [Cisco IP 電話 ユーザのサポート \(111 ページ\)](#)
- [マルチプラットフォーム フォンへの電話機の直接移行 \(112 ページ\)](#)
- [新規ソフトキーテンプレートの設定 \(112 ページ\)](#)
- [ユーザの電話サービスの設定 \(113 ページ\)](#)
- [電話機の機能設定 \(114 ページ\)](#)

Cisco IP 電話 ユーザのサポート

システム管理者は、多くの場合、ネットワーク内や社内の Cisco IP 電話 ユーザの主な情報源になります。最新の詳細な情報をエンド ユーザに提供する必要があります。

Cisco IP 電話の機能（サービスおよびボイスメッセージシステムのオプションなど）を正常に使用するには、ユーザはシステム管理者やシステム管理者のネットワーク チームから情報入手する必要があります。また、システム管理者に支援を依頼できる環境が必要です。支援を求める際の連絡先の担当者名前、およびそれらの担当者に連絡する手順をユーザに提供しておく必要があります。

エンド ユーザに Cisco IP 電話に関する重要な情報を提供するために、社内のサポート サイトに Web ページを作成することをお勧めします。

このサイトには、次のタイプの情報を含めるように考慮してください。

- サポートされているすべての Cisco IP 電話 モデルのユーザ ガイド
- Cisco Unified Communications セルフケアポータルへのアクセス方法について
- サポートされている機能のリスト
- ボイスメール システムのユーザ ガイドまたはクイック リファレンス

マルチプラットフォーム フォンへの電話機の直接移行

移行ファームウェアロードを使用せずに、1つの手順で企業の電話機をマルチプラットフォームフォンに簡単に移行することができます。必要なのは、サーバーから移行ライセンスを取得して承認することだけです。

詳細については、「https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html」を参照してください。

新規ソフトキー テンプレートの設定

ユーザが一部の機能にアクセスできるようにするにはソフトキーテンプレートにソフトキーを追加する必要があります。たとえば、ユーザがサイレントを使用できるようにするには、該当するソフトキーを有効にする必要があります。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

複数のテンプレートを作成する場合があります。たとえば、会議室に設置する電話機のためのテンプレートや経営幹部のオフィスに設置する電話機のための別のテンプレートが必要になる場合があります。

この手順では、新しいソフトキーテンプレートを作成し、特定の電話機に割り当てる手順を示します。他の電話機能と同様に、すべての会議電話または電話グループにテンプレートを使用することもできます。

手順

-
- ステップ 1 Cisco Unified Communications Manager 管理に管理者としてサインインします。
 - ステップ 2 [デバイス (Device)] > [デバイス設定 (Device Settings)] > [ソフトキー テンプレート (Softkey Template)] の順に選択します。
 - ステップ 3 [Find] をクリックします。
 - ステップ 4 次のオプションのいずれかを選択します。
 - Cisco Unified Communications Manager 11.5 以前のリリース：[標準ユーザ (Standard User)]
 - Cisco Unified Communications Manager 12.0 以降のリリース：[パーソナル会議ユーザ (Personal Conference User)] または [パブリック会議ユーザ (Public Conference User)]。
 - ステップ 5 [Copy] をクリックします。
 - ステップ 6 テンプレートの名前を変更します。
たとえば、8832 会議室テンプレート。
 - ステップ 7 [Save (保存)] をクリックします。
 - ステップ 8 右上のメニューから [ソフトキー レイアウトの構成 (Configure Softkey Layout)] ページに移動します。

- ステップ 9 各発信状態について、表示する機能を設定します。
- ステップ 10 [Save (保存)] をクリックします。
- ステップ 11 右上のメニューで [検索/一覧画面 (Find/List screen)] に戻ります。
テンプレートの一覧に新しいテンプレートが表示されます。
- ステップ 12 [デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 13 新しいテンプレートを割り当てる電話機を検索し、選択します。
- ステップ 14 [ソフトキー テンプレート (Softkey Template)] フィールドで、新しいソフトキー テンプレートを選択します。
- ステップ 15 [保存 (Save)] と [設定の適用 (Apply Config)] をクリックします。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

ユーザの電話サービスの設定

ユーザが IP フォンの Cisco IP 電話サービスにアクセスできるように設定することができます。また、さまざまな電話のサービスにボタンを割り当てることも可能です。IP フォンは各サービスを個別のアプリケーションとして管理します。

ユーザがサービスにアクセスできるようにするには、前もって次の作業が必要です。

- Cisco Unified Communications Manager Administration を使用して、デフォルトで提供されないサービスを設定する必要があります。
- ユーザが Cisco Unified Communications セルフケアポータルを使用してサービスを登録する必要があります。この Web ベース アプリケーションは、IP フォンのアプリケーションをエンドユーザが設定するための限定的なグラフィカル ユーザ インターフェイス (GUI) を提供します。ただし、エンタープライズ登録として設定するサービスにユーザは登録できません。

詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

サービスを設定する前に、設定するサイトの URL アドレスをすべて入手し、ユーザが社内 IP テレフォニー ネットワークからこれらのサイトにアクセスできるかどうかを確認してください。このアクティビティは、シスコが提供するデフォルト サービスには適用されません。

手順

-
- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [Phone サービス (Phone Services)] を選択します。

ステップ 2 ユーザがCisco Unified Communications セルフケアポータルにアクセスでき、そこから設定済みのサービスを選択して登録できることを確認します。

エンドユーザに提供する必要がある情報については、[セルフケアポータルの概要 \(81 ページ\)](#) を参照してください。

関連トピック

[Cisco Unified Communications Manager マニュアル \(14 ページ\)](#)

電話機の機能設定

ユーザのニーズに基づいて、さまざまな機能を備えるように電話機をセットアップできます。すべての電話、電話機のグループ、または個々の電話機に機能を適用することもできます。

機能を設定する際には、Cisco Unified Communications Manager Administration ウィンドウに、すべての電話機に適用される情報、およびその電話機モデルに適用される情報が表示されます。電話機モデルに固有の情報は、ウィンドウの [プロダクト固有の設定 (Product Specific Configuration Layout)] のエリアにあります。

すべての電話モデルに適用されるフィールドについては、Cisco Unified Communications Manager のマニュアルを参照してください。

ウィンドウ間には優先順位があるため、フィールドを設定する際に重要なのは、フィールド設定の対象となるウィンドウです。優先順序は、次のとおりです。

1. 個々の電話 (優先順位最高)
2. 電話機グループ
3. すべての電話 (優先順位最低)

たとえば、特定のユーザ群が電話機 Web ページにアクセスしないようにしつつ、その他のユーザはそのページにアクセスできるようにするには、次のようにします。

1. すべてのユーザに対して、電話機 Web ページへのアクセスを有効にします。
2. 個々のユーザそれぞれについて、電話機 Web ページへのアクセスを無効にするか、またはユーザグループを設定し、そのユーザグループから電話機 Web ページへのアクセスを無効にします。
3. ユーザグループ内の特定のユーザが電話機 Web ページへのアクセスを必要とする場合には、その特定のユーザに対して有効にすることができます。

関連トピック

[Expressway サインイン用ユーザ クレデンシャル パーシステントの設定 \(146 ページ\)](#)

すべての電話機の電話機能の設定

手順

- ステップ 1 Cisco Unified Communications Manager 管理に管理者としてサインインします。
- ステップ 2 [システム]>[エンタープライズ電話の設定] を選択します。
- ステップ 3 変更するフィールドを設定します。
- ステップ 4 変更フィールドの[エンタープライズ設定を上書き (Override Enterprise Settings)] チェックボックスを選択します。
- ステップ 5 [保存 (Save)] をクリックします。
- ステップ 6 [設定の適用 (Apply Config)] をクリックします。
- ステップ 7 電話機を再起動します。

(注) これは、組織内のすべての電話機に影響します。

関連トピック

[プロダクト固有の設定](#) (116 ページ)

電話機グループの電話機能の設定

手順

- ステップ 1 Cisco Unified Communications Manager 管理に管理者としてサインインします。
- ステップ 2 [デバイス (Device)]>[デバイスの設定 (Device Settings)]>[共通の電話プロファイル (Common Phone Profile)] の順に選択します。
- ステップ 3 プロファイルを探します。
- ステップ 4 [製品固有の構成レイアウト (Product Specific Configuration Layout)] ペインに移動し、フィールドを設定します。
- ステップ 5 変更フィールドの[エンタープライズ設定を上書き (Override Enterprise Settings)] チェックボックスを選択します。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 [設定の適用 (Apply Config)] をクリックします。
- ステップ 8 電話機を再起動します。

関連トピック

[プロダクト固有の設定](#) (116 ページ)

単一の電話機の電話機能の設定

手順

- ステップ 1 Cisco Unified Communications Manager 管理に管理者としてサインインします。
- ステップ 2 [デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 3 ユーザに関連付けられた電話機を見つけます。
- ステップ 4 [製品固有の構成レイアウト (Product Specific Configuration Layout)] ペインに移動し、フィールドを設定します。
- ステップ 5 変更されたフィールドについて、[共通設定の上書き (Override Common Settings)] チェックボックスをオンにします。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 [設定の適用 (Apply Config)] をクリックします。
- ステップ 8 電話機を再起動します。

関連トピック

[プロダクト固有の設定 \(116 ページ\)](#)

プロダクト固有の設定

次の表に、[プロダクト固有の設定 (Product Specific Configuration Layout)] ペインのフィールドを示します。この表の一部のフィールドは、[デバイス (Device)] > [電話機 (Phone)] ページにのみ表示されます。

表 18: [プロダクト固有の設定 (Product Specific Configuration)] フィールド

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
アクセスの設定	無効 有効 [制限 (Restricted)]	有効	設定アプリのローカル設定へのアクセスを有効化、無効化、または制限します。 制限 (Restricted) モードでは、[設定 (Preferences)] および [システム情報 (System Information)] メニューにアクセスできます。Wi-Fi メニューの一部の設定にもアクセスできます。 アクセスを無効にしている場合、[Settings] メニューにオプションが表示されません。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Gratuitous ARP	無効 有効	無効	電話機が Gratuitous ARP から MAC アドレスを学習する能力を有効または無効にします。この機能は、音声ストリームをモニタまたは記録するために必要です。
Web アクセス (Web Access)	無効 有効	無効	Web ブラウザによる電話 Web ページへのアクセスを有効または無効にします。 注意 このフィールドを有効にすると、電話機に関する機密情報が公開される場合があります。
Webアクセス用のTLS 1.0およびTLS 1.1を無効にする	無効 有効	有効	Web サーバ接続に TLS 1.2 の使用を制御します。 <ul style="list-style-type: none"> • [無効 (Disabled)] : TLS1.0、TLS 1.1 または TLS1.2 用に設定されている電話機は、HTTPS サーバとして機能できます。 • [有効 (Enabled)] : TLS1.2 用に設定されている電話機のみ HTTPS サーバとして機能できます。
一括ダイヤル	無効 有効	無効	ダイヤル方法を制御します。 <ul style="list-style-type: none"> • [無効 (Disabled)] : ダイヤルプランまたはルートパターンの重複がある場合、Cisco Unified Communications Manager は桁間タイマーが満了するのを待ちます。 • [有効 (Enabled)] : ダイヤルが完了すると、ダイヤルされた文字列全体が Cisco Unified Communications Manager に送信されます。T.302 タイマーのタイムアウトを回避するために、ダイヤルプランまたはルートパターンが重複している場合は常に一括ダイヤルを有効にすることをお勧めします。 <p>強制承認コード (FAC) またはクライアント識別コード (CMC) は一括ダイヤルに対応していません。FAC または CMC を使用して通話アクセスとアカウントिंगを管理している場合は、この機能を使用できません。</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Days Backlight Not Active	Days of the week		<p>[バックライト点灯時刻 (Backlight On Time)] フィールドで指定された時刻になっても、バックライトを自動的にオンにしない日を定義します。</p> <p>ドロップダウンリストから単一または複数の曜日を選択します。複数の曜日を選択するには、Ctrl キーを押しながら目的の各曜日をクリックします。</p> <p>Cisco IP 電話 での省電力のスケジュール (133 ページ) を参照してください。</p>
Backlight On Time	hh:mm		<p>毎日バックライトを自動的にオンにする時刻 ([バックライト表示非点灯 (Backlight Display Not Active)] フィールドで指定されている日を除く) を定義します。</p> <p>このフィールドには、24 時間形式で入力します (0:00 は午前 0 時)。</p> <p>たとえば、午前 7:00 時 (0700) にバックライトを自動的にオンにするには、07:00 と入力します。午後 2:00 時 (1400) にバックライトをオンにするには、14:00 と入力します。</p> <p>このフィールドがブランクの場合、バックライトは午前 0 時に自動的にオンになります。</p> <p>Cisco IP 電話 での省電力のスケジュール (133 ページ) を参照してください。</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Backlight On Duration	hh:mm		<p>[バックライト点灯時刻 (Backlight On Time)] フィールドで指定した時刻にバックライトがオンになった後、オン状態を保つ時間の長さを定義します。</p> <p>たとえば、バックライトを自動的にオンにしてから 4 時間 30 分にわたってオン状態を保つには、04:30 と入力します。</p> <p>このフィールドがブランクの場合、電話機は午前 0 時 (0:00) にオフになります。</p> <p>[バックライト点灯時刻 (Backlight On Time)] が 0:00 で、バックライト点灯継続時間がブランク (または 24:00) の場合、バックライトはオフになりません。</p> <p>Cisco IP 電話 での省電力のスケジュール (133 ページ) を参照してください。</p>
Backlight Idle Timeout	hh:mm		<p>バックライトをオフにするまでの電話機のアイドル時間を定義します。バックライトがスケジュールどおりにオフで、ユーザが (電話機ボタンを押す、またはハンドセットを持ち上げる操作で) オンにした場合にのみ適用されます。</p> <p>たとえば、ユーザがバックライトをオンにしてから 1 時間 30 分にわたって電話機がアイドル状態にあった場合にバックライトをオフにするには、01:30 と入力します。</p> <p>Cisco IP 電話 での省電力のスケジュール (133 ページ) を参照してください。</p>
Backlight On When Incoming Call	無効 有効	有効	着信コールがあるとバックライトがオンに変わります。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Enable Power Save Plus	Days of the week		<p>電話機の電源をオフにする日のスケジュールを定義します。</p> <p>ドロップダウンリストから単一または複数の曜日を選択します。複数の曜日を選択するには、Ctrl キーを押しながら目的の各曜日をクリックします。</p> <p>[Power Save Plus の有効化 (Enable Power Save Plus)] がオンになっていると、緊急 (e911) の問題について警告するメッセージを受け取ります。</p> <p>注意 Power Save Plus モード (「モード」) が有効である間は、モードに設定されたエンドポイントは、緊急コールでは無効で、着信コールの受信ができません。このモードを選択することにより、次の条項に同意したものと見なされます。(i) モードが有効である間、緊急コールとコールの受信用の代替方法を責任を持って用意する必要があります。(ii) シスコはこのモードの選択に関して何の責任を負いません。このモードを有効にすることは、お客様の責任で行っていただきます。(iii) コール、発信、およびその他について、このモードを有効にした場合の影響をユーザにすべて通知する必要があります。</p> <p>Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオフにする必要があります。[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。</p> <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
電話機をオンにする時刻 (Phone On Time)	hh:mm		<p>[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドにある日について、電話機の電源を自動的にオンにする時刻を決定します。</p> <p>このフィールドには、24 時間形式で入力します (0:00 は午前 0 時)。</p> <p>たとえば、午前 7 時 (0700) に自動的に電話機の電源をオンにする場合は、7:00 と入力します。午後 2 時 (1400) に電話機の電源をオンにするには、14:00 と入力します。</p> <p>デフォルト値はブランクで、これは 00:00 を意味します。</p> <p>[電話機をオンにする時刻 (Phone On Time)] は、[電話機をオフにする時刻 (Phone Off Time)] より 20 分以上遅い時刻に設定する必要があります。たとえば、[電話機をオフにする時刻 (Phone Off Time)] が 7:00 の場合、[電話機をオンにする時刻 (Phone On Time)] は 7:20 より前に設定しないでください。</p> <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
電話機をオフにする時刻 (Phone Off Time)	hh:mm		<p>[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで選択した日について、電話機の電源をオフにする時刻を定義します。[電話機をオンにする時刻 (Phone On Time)] フィールドと [電話機をオフにする時刻 (Phone Off Time)] フィールドに同じ値が含まれている場合、電話機はオフになりません。</p> <p>このフィールドには、24 時間形式で入力します (0:00 は午前 0 時)。</p> <p>たとえば、午前 7 時 (0700) に自動的に電話機の電源をオフにする場合は、7:00 と入力します。午後 2 時 (1400) に電話機の電源をオフにするには、14:00 と入力します。</p> <p>デフォルト値はブランクで、これは 00:00 を意味します。</p> <p>[電話機をオンにする時刻 (Phone On Time)] は、[電話機をオフにする時刻 (Phone Off Time)] より 20 分以上遅い時刻に設定する必要があります。たとえば、[電話機をオフにする時刻 (Phone Off Time)] が 7:00 の場合、[電話機をオンにする時刻 (Phone On Time)] は 7:20 より前に設定しないでください。</p> <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
電話機をオフにするアイドル タイムアウト (Phone Off Idle Timeout)	hh:mm		<p>電話機の電源をオフにする前に、電話機をアイドル状態にしておく必要がある時間の長さを示します。</p> <p>タイムアウトは次の条件で発生します。</p> <ul style="list-style-type: none"> • 電話機がスケジュールどおりに Power Save Plus モードになっていたが、電話機のユーザが [選択 (Select)] キーを押したために、Power Save Plus モードが解除された場合。 • 接続スイッチで電話機が再びオンになった場合。 • [電話機をオフにする時刻 (Phone Off Time)] になったが、通話中の場合。 <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>
Enable Audible Alert	チェックボックス	オフ	<p>これを有効にすると、[電話機をオフにする時刻 (Phone Off Time)] で指定した時刻の 10 分前に電話機で音声アラートの再生が開始されます。</p> <p>このチェックボックスが表示されるのは、[Power Save Plus の有効化 (Enable Power Save Plus)] リストボックスで 1 日以上が選択されている場合だけです。</p> <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>
EnergyWise Domain	最大 127 文字です。		<p>その電話機が含まれる EnergyWise ドメインを特定します。</p> <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>
EnergyWise シークレット	最大 127 文字です。		<p>EnergyWise ドメイン内でエンドポイントとの通信に使用されるセキュリティの秘密パスワードを指定します。</p> <p>Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。</p>

■ プロダクト固有の設定

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Allow EnergyWise Overrides	チェックボックス	オフ	

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
			<p>電話機に電源レベルの更新を送信するための EnergyWise ドメイン コントローラのポリシーを許可するかどうかを決定します。次の条件が適用されます。</p> <ul style="list-style-type: none"> • [Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで 1 日以上を選択する必要があります。 • Cisco Unified Communications Manager の管理ページの設定は、EnergyWise がオーバーライドを送信しても、スケジュールに適用されます。 <p>たとえば、[電話機をオフにする時刻 (Phone Off Time)] が 22:00 (午後 10 時) に設定されていると仮定すると、[電話機をオンにする時刻 (Phone On Time)] フィールドの値は 06:00 (午前 6 時) となり、[Power Save Plus の有効化 (Enable Power Save Plus)] では 1 日以上が選択されています。</p> <ul style="list-style-type: none"> • EnergyWise が 20:00 (午後 8 時) に電話機をオフにするように指示すると、この指示は、午前 6 時に設定された [電話機をオンにする時刻 (Phone On Time)] まで有効となります (電話機ユーザによる介入が発生しないと仮定した場合)。 • 午前 6 時になると、電話機はオンとなり、Cisco Unified Communications Manager の管理での設定から電力レベルの変更の受信を再開します。 • 電力レベルを電話機で再び変更するには、EnergyWise は電力レベル変更コマンドを新たに再発行する必要があります。 <p>Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオフにする必要があります。[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオンにしたままにしておくと、Power Save</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
			Plus は無効になりません。 Cisco IP 電話 での EnergyWise のスケジュール (135 ページ) を参照してください。
Join And Direct Transfer Policy	[同一回線で有効 (Same line enable)] [同一回線で無効 (Same line disable)]	[同一回線、回線全体で有効 (Same line, across line enable)]	コールに参加し、転送するユーザの機能を制御します。 <ul style="list-style-type: none"> • [同一回線で有効 (Same line enable)] : ユーザは、現在の回線上のコールを同一回線上の別のコールに直接転送するか、コールに参加できます。 • [同一回線、回線全体で無効 (Same line disable)] : ユーザは、同一回線上のコールに参加したり転送したりできません。参加機能と転送機能は無効であり、ユーザは直接転送も参加機能も実行できません。
録音トーン	無効 有効	無効	ユーザがコールを記録する際のトーンの再生を制御します
録音トーンのローカルボリューム	整数 0 ~ 100	100	ローカルユーザに対する録音トーンのボリュームを制御します。
録音トーンのリモート音量	整数 0 ~ 100	50	リモートユーザに対する録音トーンのリモート音量を制御します。
録音トーンの長さ	整数、1 ~ 3000 ミリ秒		録音トーンの長さを制御します。
ログサーバー	256 文字以下の文字列。		電話デバッグ出力用の IPv4 syslog サーバを指定します。 [アドレスの形式] : address : <port>@<base=<0-7>;pfs=<0-1>
リモート ログ (Remote Log)	無効 有効	無効	Syslog サーバにログを送信する機能を制御します。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
ログプロファイル	デフォルト プリセット テレフォニー SIP UI ネットワーク Media アップグレード アクセサリ セキュリティ EnergyWise MobileRemoteAccess	プリセット	<p>事前定義されたロギング プロファイルを指定します。</p> <ul style="list-style-type: none"> • [デフォルト (Default)] : デフォルトのデバッグ ロギング レベル • [プリセット (Preset)] : 電話ローカル デバッグ ロギングの設定を上書きしません • [テレフォニー (Telephony)] : 電話またはコール機能に関する情報をログに記録します • [SIP] : SIP シグナリングに関する情報をログに記録します • [UI] : 電話ユーザ インターフェイスに関する情報をログに記録します • [ネットワーク (Network)] : ネットワーク情報をログに記録します • [メディア (Media)] : メディア情報をログに記録します • [アップグレード (Upgrade)] : アップグレード情報をログに記録します • [アクセサリ (Accessory)] : アクセサリ情報をログに記録します • [セキュリティ (Security)] : セキュリティ情報をログに記録します • [Energywise] : 省エネルギー情報をログに記録します • [MobileRemoteAccess] : Expressway によるモバイルおよび Remote Access の情報をログに記録します。
IPv6 ログサーバー	256 文字以下の文字列。		電話デバッグ出力用の IPv6 syslog サーバを指定します。
Cisco Discovery Protocol (CDP) : Switch Port	無効 有効	有効	電話機の Cisco Discovery Protocol を制御します。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED) : スイッチポート (Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED) : Switch Port)	無効 有効	有効	SW ポートで LLDP-MED を有効にします。
LLDP Asset ID	32 文字以下の文字列。		在庫管理のため電話機に割り当てられているアセット ID を識別します。
Energy Efficient Ethernet (EEE) : スイッチポート	無効 有効	無効	スイッチポート上の EEE を制御します。
LLDP 電力の優先順位 (LLDP Power Priority)	不明 (Unknown) 低 大きい クリティカル	不明 (Unknown)	電話機の電源優先度をスイッチに割り当て、スイッチが電力を適切に電話機に供給できるようにします。
802.1X 認証	ユーザ制御 (User Controlled) 無効 有効	ユーザ制御 (User Controlled)	802.1x 認証機能のステータスを指定します。 <ul style="list-style-type: none"> • [ユーザ制御 (User Controlled)] : ユーザは電話機に 802.1x を設定できます。 • 無効 (Disabled) : 802.1x 認証は使用されません。 • [有効 (Enabled)] : 802.1x 認証が使用され、電話の認証を設定します。
Switch Port Remote Configuration	無効 Auto Negotiate 10 ハーフ (100 Half) 10 フル (10 Full) 100 ハーフ (100 Half) 100 フル (10 Full)	無効	電話機 SW ポートの速度とデュプレックス機能のリモート設定ができます。これにより、具体的なポート設定を伴う大規模な導入のパフォーマンスが向上します。 Cisco Unified Communications Manager のリモートポート設定用に SW ポートが設定されている場合は、電話機のデータを変更することはできません。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
SSH アクセス	無効 有効	無効	ポート 22 を経由する SSH デーモンへのアクセスを制御します。ポート 22 を開いたままにしておくと、電話機はサービス拒否 (DoS) 攻撃を受けやすい状態になります。
呼出音ロケール (Ring Locale)	デフォルト 日本	デフォルト	呼出音パターンを制御します。
TLS 再開タイマー	整数、0 ~ 3600 秒	3600	TLS 認証プロセス全体を繰り返すことなく TLS セッションを再開する機能を制御します。このフィールドが 0 に設定されている場合、TLS セッション再開は無効です。
FIPS モード	無効 有効	無効	電話機上で連邦情報処理標準 (FIPS) モードを有効または無効にします。
共有電話からの通話履歴を記録 (Record Call Log from Shared Line)	無効 有効	無効	共有電話からの通話履歴を記録するかどうかを指定します。
呼出音の最小音量 (Minimum Ring Volume)	0 : サイレント 1 ~ 15	0 : サイレント	電話機の呼出音の最小音量を制御します。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Peer Firmware Sharing	無効 有効	有効	<p>電話機がサブネット上にある同一モデルの他の電話機を検出し、更新されたファームウェアファイルを共有できるようにします。電話機に新しいファームウェアロードがある場合、他の電話機とそのロードを共有できます。他の電話機の1つに新しいファームウェアロードがある場合、TFTPサーバからではなくその電話機からファームウェアをダウンロードできます。</p> <p>ピア ファームウェア共有：</p> <ul style="list-style-type: none"> • 中央集中型リモート TFTP サーバへの TFTP 転送における輻輳が制限されます。 • ファームウェアのアップグレードを手動で制御する必要がなくなります。 • アップグレード時に多数のデバイスが同時にリセットされた場合の電話機のダウンタイムが削減されます。 • 帯域幅が制限された WAN リンクを経由するブランチまたはリモートオフィス導入シナリオでのファームウェアのアップグレードに役立ちます。
ロードサーバ	256文字以下の文字列。		電話機がファームウェアロードとアップグレードを取得するために使用する代替 IPv4 サーバを指定します。
IPv6 負荷サーバ (IPv6 Load Server)	256文字以下の文字列。		電話機がファームウェアロードやアップグレードを取得する際に使用する代替 IPv6 サーバを指定します。

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
Unified CM接続障害の 検出	標準 [遅延 (Delayed)]	標準	<p>バックアップ Unified CM/SRST へのデバイスのフェールオーバーが発生する前の最初のステップである、Cisco Unified Communications Manager (Unified CM) への接続失敗を検出するための電話機の感度を決定します。</p> <p>有効な値は、[Normal] (標準のシステム レートで Unified CM 接続エラーの検出を実行) または [Delayed] (標準より約 4 倍遅いレートで Unified CM 接続エラーの検出を実行) です。</p> <p>Unified CM 接続エラーの高速認識のためには、[Normal] を選択します。接続を再確立できるようにするためにフェールオーバーを少し遅らせる場合は、[Delayed] を選択します。</p> <p>[Normal] と [Delayed] の接続エラー検出の正確な時間の差は、常に変化する多数の変数に応じて異なります。</p>
Special Requirement ID	文字列		Engineering Special (ES) ロードからのカスタム機能を制御します。
HTTPS サーバ (HTTPS Server)	http および https 対応 https のみ	http および https 対応	電話機への通信のタイプを制御します。[HTTPS のみ (HTTPS only)]を選択すると、電話通信がよりセキュアになります。
Expressway サインイン に対するユーザクレ デンシャルの永続性 (User Credentials Persistent for Expressway Sign In)	無効 有効	無効	<p>電話機にユーザのサインイン クレデンシャルを保存するかどうかを制御します。無効にすると、ユーザに対して、モバイルおよび Remote Access (MRA) の Expressway サーバにサインインするためのプロンプトが常に表示されます。</p> <p>ユーザが簡単にログインできることが望ましい場合は、このフィールドを有効にすることによって、Expressway のログイン クレデンシャルを永続的なものとすることができます。ユーザは初回のみログイン クレデンシャルを入力する必要があります。それ以降は (オフプレミスで電話機の電源を入れたとき)、常にログイン情報がサインイン画面に事前入力されます。</p> <p>詳細については、Expressway サインイン用ユーザ クレデンシャル パーシステントの設定 (146 ページ) を参照してください。</p>

フィールド名	フィールドタイプ または選択肢	デフォルト	説明
カスタマーサポートのアップロード URL (Customer support upload URL)	256文字以下の文字列。		問題レポート ツール (PRT) の URL を入力します。 Expressway 経由でのモバイルおよび Remote Access を使用してデバイスを導入している場合、Expressway サーバの HTTP サーバ許可リストへの PRT サーバアドレスの追加も必要となります。 詳細については、 Expressway サインイン用ユーザ クレデンシャル パーシステントの設定 (146 ページ) を参照してください。
TLS暗号を無効にする	トランスポート層セキュリティ暗号を無効にする (132 ページ) を参照してください。	なし	選択した TLS 暗号を無効にします。 複数の暗号スイートを無効にするには、コンピュータのキーボードで Ctrl キーを押したままにします。
コールパーク専用の1回線	無効 有効	有効	パークされたコールが1回線を占有するかどうかを制御します。 詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

関連トピック

[Expressway サインイン用ユーザ クレデンシャル パーシステントの設定 \(146 ページ\)](#)

トランスポート層セキュリティ暗号を無効にする

[TLS暗号の無効化]パラメータを使用して、トランスポート層セキュリティ (TLS) 暗号を無効にできます。これにより、既知の脆弱性に合わせてセキュリティを調整したり、ネットワークを暗号化に関する会社のポリシーに合わせるすることができます。

すべてデフォルト設定ではありません。

複数の暗号スイートを無効にするには、コンピュータのキーボードで **Ctrl** キーを押したままにします。すべての電話暗号を選択した場合、電話 TLS サービスが影響を受けます。選択肢は、次のとおりです。

- なし
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

電話セキュリティの詳細については、Cisco IP 電話 7800 および 8800 シリーズセキュリティの概要ホワイトペーパー (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html>) を参照してください。

Cisco IP 電話 での省電力のスケジュール

電力を節約し、電話スクリーンディスプレイの寿命を確実に延ばすには、不要なときに表示をオフにするように設定します。

Cisco Unified Communications Manager の管理ページを使用すると、ディスプレイを特定の曜日の指定時刻にオフにし、他の曜日では終日オフにするように設定できます。たとえば、ディスプレイを平日の勤務時間後にオフにし、土曜日と日曜日では終日オフにするように選択できます。

ディスプレイがオフのときはいつでも、次の操作でディスプレイをオンにできます。

- 電話機の任意のボタンを押す。
ディスプレイがオンになり、そのボタンで指定されているアクションが実行されます。
- ハンドセットを持ち上げる。

ディスプレイは、オンにするとそのままオン状態になりますが、指定された期間にわたって電話機がアイドル状態にあると、自動的にオフになります。

手順

- ステップ 1** Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2** 設定する電話機を特定します。
- ステップ 3** [プロダクト固有の設定 (Product Specific Configuration Layout)] 領域に移動して、次のフィールドを設定します。
 - Days Display Not Active
 - Display On Time
 - Display On Duration
 - Display Idle Timeout

表 19: PowerSave の設定フィールド

フィールド	説明
Days Display Not Active	<p>[ディスプレイ点灯時刻 (Display On Time)] フィールドで指定された時刻になっても、ディスプレイを自動的にオンにしない日。</p> <p>ドロップダウンリストから単一または複数の曜日を選択します。複数の曜日を選択するには、Ctrl キーを押しながら目的の各曜日をクリックします。</p>
Display On Time	<p>毎日ディスプレイを自動的にオンにする時刻 ([ディスプレイ非点灯日 (Days Display Not Active)] フィールドで指定されている日を除く)。</p> <p>このフィールドには、24 時間形式で入力します (0:00 は午前 0 時)。</p> <p>たとえば、午前 7:00 (0700) にディスプレイを自動的にオンにするには、07:00 と入力します。02:00p.m. にディスプレイをオンにするには (1400) にバックライトをオンにするには、14:00 と入力します。</p> <p>このフィールドがブランクの場合、ディスプレイは午前 0 時に自動的にオンになります。</p>
Display On Duration	<p>[ディスプレイ点灯時刻 (Display On Time)] フィールドで指定した時刻にディスプレイがオンになった後、オン状態を保つ時間の長さ。</p> <p>このフィールドには、時間:分の形式で値を入力します。</p> <p>たとえば、ディスプレイを自動的にオンにしてから 4 時間 30 分にわたってオン状態を保つには、4:30 と入力します。</p> <p>このフィールドがブランクの場合、電話機は午前 0 時 (0:00) にオフになります。</p> <p>(注) [ディスプレイ点灯時刻 (Display On Time)] が 0:00 で、[ディスプレイ点灯継続時間 (Display On Duration)] がブランク (または 24:00) の場合、電話機は常にオン状態になります。</p>
Display Idle Timeout	<p>ディスプレイをオフにするまでの電話機のアイドル時間。ディスプレイがスケジュールどおりにオフで、ユーザが (電話機ボタンを押す、またはハンドセットを持ち上げる操作で) オンにした場合にのみ適用されます。</p> <p>このフィールドには、時間:分の形式で値を入力します。</p> <p>たとえば、ユーザがディスプレイをオンにしてから 1 時間 30 分にわたって電話機がアイドル状態にあった場合にディスプレイをオフにするには、1:30 と入力します。</p> <p>デフォルト値は 1:00 です。</p>

ステップ 4 [保存 (Save)] を選択します。

ステップ 5 [設定の適用 (Apply Config)] を選択します。

ステップ 6 電話機を再起動します。

Cisco IP 電話 での EnergyWise のスケジュール

消費電力を減らすには、ご使用のシステムに EnergyWise コントローラが含まれている場合に、電話機をスリープ（電源オフ）とウェイク（電源オン）に設定します。

Cisco Unified Communications Manager の管理で、EnergyWise を有効にして、スリープ時間とウェイク時間の設定を行います。これらのパラメータは、電話機の表示設定パラメータと緊密に結びついています。

EnergyWise が有効になっていて、スリープ時間が設定されていると、電話機を設定時刻に復帰させるように、電話機からスイッチに要求が送信されます。この要求の受諾または拒否が、スイッチから戻ります。スイッチが要求を拒否した場合、またはスイッチが応答しない場合は、電話機はオフになりません。スイッチが要求を受諾すると、アイドル状態の電話機がスリープ状態となり、消費電力をあらかじめ決められたレベルに減らすことができます。アイドル状態になっていない電話機にはアイドルタイマーが設定され、タイマーの期限が切れると、電話機がスリープ状態になります。

電話機をウェイクさせるには、選択ボタンを押します。スケジュールされているウェイク時間になると、システムは電話機の電力を元に戻して電話機を復帰させます。

手順

- ステップ 1** Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2** 設定する電話機を特定します。
- ステップ 3** [プロダクト固有の設定 (Product Specific Configuration Layout)] 領域に移動して、次のフィールドを設定します。
 - Power Save Plus の有効化 (Enable Power Save Plus)
 - 電話機をオンにする時刻 (Phone On Time)
 - 電話機をオフにする時刻 (Phone Off Time)
 - 電話機をオフにするアイドル タイムアウト (Phone Off Idle Timeout)
 - 音声アラートを有効にする (Enable Audio Alert)
 - EnergyWise ドメイン (EnergyWise Domain)
 - EnergyWise シークレット (EnergyWise Secret)
 - EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)

表 20: EnergyWise Configuration Fields

フィールド	説明
Enable Power Save Plus	<p>電話機の電源をオフにする日のスケジュールを選択します。スケジュールを設定する日をクリックしたら、Control キーを押したままにして、複数日を選択します。</p> <p>デフォルトでは、どの日も選択されていません。</p> <p>[Power Save Plus の有効化 (Enable Power Save Plus)] がオンになっていると、緊急 (e911) の問題について警告するメッセージを受け取ります。</p> <p>注意 Power Save Plus モード (「モード」) が有効である間は、モードに設定されたエンドポイントは、緊急コールでは無効で、インバウンドコールの受信ができません。このモードを選択することにより、次の条項に同意したものと見なされます。(i) モードが有効である間、緊急コールとコールの受信用の代替方法を責任を持って用意する必要があります。(ii) シスコはこのモードの選択に関して何の責任を負いません。このモードを有効にすることは、お客様の責任で行っていただきます。(iii) コール、発信、およびその他について、このモードを有効にした場合の影響をユーザにすべて通知する必要があります。</p> <p>(注) Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオフにする必要があります。[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。</p>
電話機をオンにする時刻 (Phone On Time)	<p>[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドにある日について、電話機の電源を自動的にオンにする時刻を決定します。</p> <p>このフィールドには、24 時間形式で入力します (0:00 は午前 0 時)。</p> <p>たとえば、午前 7 時 (0700) に自動的に電話機の電源をオンにする場合は、7:00 と入力します。午後 2 時 (1400) に電話機の電源をオンにするには、14:00 と入力します。</p> <p>デフォルト値はブランクで、これは 00:00 を意味します。</p> <p>(注) [電話機をオンにする時刻 (Phone On Time)] は、[電話機をオフにする時刻 (Phone Off Time)] より 20 分以上遅い時刻に設定する必要があります。たとえば、[電話機をオフにする時刻 (Phone Off Time)] が 7:00 の場合、[電話機をオンにする時刻 (Phone On Time)] は 7:20 より前に設定しないでください。</p>

フィールド	説明
電話機をオフにする時刻 (Phone Off Time)	<p>[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで選択した日について、電話機の電源をオフにする時刻。[電話機をオンにする時刻 (Phone On Time)] フィールドと [電話機をオフにする時刻 (Phone Off Time)] フィールドに同じ値が含まれている場合、電話機はオフになりません。</p> <p>このフィールドには、24 時間形式で入力します (0:00 は午前 0 時)。</p> <p>たとえば、午前 7 時 (0700) に自動的に電話機の電源をオフにする場合は、7:00 と入力します。午後 2 時 (1400) に電話機の電源をオフにするには、14:00 と入力します。</p> <p>デフォルト値はブランクで、これは 00:00 を意味します。</p> <p>(注) [電話機をオンにする時刻 (Phone On Time)] は、[電話機をオフにする時刻 (Phone Off Time)] より 20 分以上遅い時刻に設定する必要があります。たとえば、[電話機をオフにする時刻 (Phone Off Time)] が 7:00 の場合、[電話機をオンにする時刻 (Phone On Time)] は 7:20 より前に設定しないでください。</p>
Phone Off Idle Timeout	<p>電話機の電源をオフにする前に、電話機をアイドル状態にしておく必要がある時間の長さ。</p> <p>タイムアウトは次の条件で発生します。</p> <ul style="list-style-type: none"> • 電話機がスケジュールどおりに Power Save Plus モードになっていたが、電話機のユーザが [選択 (Select)] キーを押したために、Power Save Plus モードが解除された場合。 • 接続スイッチで電話機が再びオンになった場合。 • [電話機をオフにする時刻 (Phone Off Time)] になったが、通話中の場合。 <p>このフィールドの範囲は 20 ~ 1440 分です。</p> <p>デフォルト値は 60 分です。</p>

フィールド	説明
Enable Audible Alert	<p>これを有効にすると、[電話機をオフにする時刻 (Phone Off Time)] で指定した時刻の 10 分前に電話機で音声アラートの再生が開始されます。</p> <p>音声アラートは、電話機の呼出音を使用します。この音は、10 分間のアラート期間中の特定期間、短く再生されます。呼出音は、ユーザが指定した音声レベルで再生されます。音声アラートのスケジュールは次のとおりです。</p> <ul style="list-style-type: none"> • 電源オフの 10 分前に、呼出音が 4 回再生されます。 • 電源オフの 7 分前に、呼出音が 4 回再生されます。 • 電源オフの 4 分前に、呼出音が 4 回再生されます。 • 電源オフの 30 秒前に、呼出音は、15 回再生されるか、電話機の電源がオフになるまで再生されます。 <p>このチェックボックスが表示されるのは、[Power Save Plus の有効化 (Enable Power Save Plus)] リストボックスで 1 日以上が選択されている場合だけです。</p>
EnergyWise Domain	<p>その電話機が含まれる EnergyWise ドメイン。</p> <p>このフィールドの最大長は 127 文字です。</p>
EnergyWise Secret	<p>EnergyWise ドメイン内でエンドポイントとの通信に使用されるセキュリティの秘密パスワード。</p> <p>このフィールドの最大長は 127 文字です。</p>

フィールド	説明
Allow EnergyWise Overrides	<p>このチェックボックスにより、電話機に電源レベルの更新を送信するためのEnergyWiseドメインコントローラのポリシーを許可するかどうかを決定します。次の条件が適用されます。</p> <ul style="list-style-type: none"> • [Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで 1 日以上を選択する必要があります。 • Cisco Unified Communications Manager の管理ページの設定は、EnergyWise がオーバーライドを送信しても、スケジュールに適用されます。 <p>たとえば、[電話機をオフにする時刻 (Phone Off Time)] が 22:00 (午後 10 時) に設定されていると仮定すると、[電話機をオンにする時刻 (Phone On Time)] フィールドの値は 06:00 (午前 6 時) となり、[Power Save Plus の有効化 (Enable Power Save Plus)] では 1 日以上が選択されています。</p> <ul style="list-style-type: none"> • EnergyWise が 20:00 (午後 8 時) に電話機をオフにするように指示すると、この指示は、午前 6 時に設定された [電話機をオンにする時刻 (Phone On Time)] まで有効となります (電話機ユーザによる介入が発生しないと仮定した場合)。 • 午前 6 時になると、電話機はオンとなり、Unified Communications Manager の管理ページの設定から電力レベルの変更の受信を再開します。 • 電力レベルを電話機で再び変更するには、EnergyWise は電力レベル変更コマンドを新たに再発行する必要があります。 <p>(注) Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオフにする必要があります。[Power Save Plus の有効化 (Enable Power Save Plus)] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可 (Allow EnergyWise Overrides)] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。</p>

ステップ 4 [保存 (Save)] を選択します。

ステップ 5 [設定の適用 (Apply Config)] を選択します。

ステップ 6 電話機を再起動します。

サイレントの設定

サイレント (DND) をオンにすると、会議用電話画面のヘッダーが赤く表示されます。

詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルの取り込み中情報を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。

ステップ 2 設定する電話を特定します。

ステップ 3 次のパラメータを設定します。

- [サイレント (Do Not Disturb)] : このチェックボックスを使用すると、電話機の DND を有効にすることができます。
- DND オプション : [呼出音オフ (Ring Off)]、[コール拒否 (Call Reject)]、または [共通の電話プロファイル設定を使用 (Use Common Phone Profile Setting)]。
- [DND 着信呼警告 (DND Incoming Call Alert)] : 電話機で DND がアクティブのときに着信コールに対して発生させるアラート (存在する場合) のタイプを選択します。

(注) このパラメータは、[共通の電話プロファイル (Common Phone Profile)] ウィンドウと [電話の設定 (Phone Configuration)] ウィンドウにあります。[電話の設定 (Phone Configuration)] ウィンドウの値が優先されます。

ステップ 4 保存を選択します。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

コールの転送通知のセットアップ

コール転送設定を制御できます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。

ステップ 2 セットアップする電話を特定します。

ステップ 3 [コールの転送通知 (Call Forward Notification)] フィールドを設定します。

フィールド	説明
Caller Name	このチェックボックスをオンにした場合、発信者名が通知ウィンドウに表示されます。 デフォルトでは、このチェックボックスはオンになっています。

フィールド	説明
Caller Number	このチェックボックスをオンにした場合、発信者番号が通知ウィンドウに表示されます。 デフォルトでは、このチェックボックスはオフになっています。
Redirected Number	このチェックボックスをオンにした場合、コールを最後に転送した発信者に関する情報が通知ウィンドウに表示されます。 例：発信者 A が B にコールを発信したが、B はすべてのコールを C に転送し、C はすべてのコールを D に転送した場合、D に対して表示される通知ボックスには、発信者 C の電話機情報が表示されます。 デフォルトでは、このチェックボックスはオフになっています。
Dialed Number	このチェックボックスをオンにした場合、コールの最初の受信者に関する情報が通知ウィンドウに表示されます。 例：発信者 A が B にコールを発信したが、B はすべてのコールを C に転送し、C はすべてのコールを D に転送した場合、D に対して表示される通知ボックスには、発信者 B の電話機情報が表示されます。 デフォルトでは、このチェックボックスはオンになっています。

ステップ 4 保存を選択します。

UCR 2008 のセットアップ

UCR 2008 をサポートするパラメータは、Cisco Unified Communications Manager の管理ページに存在します。次の表に、これらのパラメータと、設定を変更するための手順を示します。

表 21 : UCR 2008 のパラメータの場所

パラメータ	管理パス
FIPS モード	[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)]
	[システム (System)] > [エンタープライズ電話の設定 (Enterprise Phone Configuration)]
	[デバイス (Device)] >> [電話 (Phone)]

パラメータ	管理パス
SSH アクセス	[デバイス (Device)] > [電話 (Phone)]
	[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)]
[Webアクセス(Web Access)]	[デバイス (Device)] > [電話 (Phone)]
	[システム (System)] > [エンタープライズ電話の設定 (Enterprise Phone Configuration)]
	[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)]
[システム (System)] > [エンタープライズ電話の設定 (Enterprise Phone Configuration)]	
[IPアドレッシングモード(IP Addressing Mode)]	[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通デバイス設定 (Common Device Configuration)]
[シグナリング用のIPアドレッシングモード設定(IP Addressing Mode Preference for Signaling)]	[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通デバイス設定 (Common Device Configuration)]

共通デバイス設定での UCR 2008 のセットアップ

次の UCR 2008 のパラメータを設定するには、次の手順を実行します。

- IP アドレッシング モード (IP Addressing Mode)
- [シグナリング用の IP アドレッシング モード設定 (IP Addressing Mode Preference for Signaling)]

手順

- ステップ 1** Cisco Unified Communications Manager の管理で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通デバイス設定 (Common Device Configuration)] を選択します。
- ステップ 2** [IP アドレッシング モード (IP Addressing Mode)] パラメータを設定します。
- ステップ 3** [シグナリング用の IP アドレッシングモード設定 (IP Addressing Mode Preference for Signaling)] パラメータを設定します。
- ステップ 4** 保存を選択します。

共通の電話プロフィールでの UCR 2008 のセットアップ

次の UCR 2008 のパラメータを設定するには、次の手順を実行します。

- FIPS モード
- SSH アクセス
- Web アクセス

手順

- ステップ 1** Cisco Unified Communications Manager の管理で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロフィール (Common Phone Profile)] を選択します。
- ステップ 2** [FIPS モード (FIPS Mode)] パラメータを [有効 (Enabled)] に設定します。
- ステップ 3** [SSH アクセス (SSH Access)] パラメータを [無効 (Disabled)] に設定します。
- ステップ 4** [Web アクセス (Web Access)] パラメータを [無効 (Disabled)] に設定します。
- ステップ 5** [80 ビット SRTCP (80-bit SRTCP)] パラメータを [有効 (Enabled)] に設定します。
- ステップ 6** 保存を選択します。

エンタープライズ電話の設定での UCR 2008 のセットアップ

次の UCR 2008 のパラメータを設定するには、次の手順を実行します。

- FIPS モード
- Web アクセス

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズ電話の設定 (Enterprise Phone Configuration)] を選択します。
- ステップ 2** [FIPS モード (FIPS Mode)] パラメータを [有効 (Enabled)] に設定します。
- ステップ 3** [Web アクセス (Web Access)] パラメータを [無効 (Disabled)] に設定します。
- ステップ 4** 保存を選択します。

電話機での UCR 2008 のセットアップ

次の UCR 2008 のパラメータを設定するには、次の手順を実行します。

- FIPS モード
- SSH アクセス

- Web アクセス

手順

-
- ステップ 1** Cisco Unified Communications Manager の管理ページで、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2** [SSH アクセス (SSH Access)] パラメータを [無効 (Disabled)] に設定します。
- ステップ 3** [FIPS モード (FIPS Mode)] パラメータを [有効 (Enabled)] に設定します。
- ステップ 4** [Web アクセス (Web Access)] パラメータを [無効 (Disabled)] に設定します。
- ステップ 5** 保存を選択します。
-

Expressway 経由でのモバイルおよび Remote Access

Expressway 経由でのモバイルおよび Remote Access(MRA) を使用すると、リモート ワーカーは、仮想プライベート ネットワーク (VPN) クライアント トンネルを使用しなくても企業のネットワークに簡単かつ安全に接続できます。Expressway は、Transport Layer Security (TLS) を使用してネットワーク トラフィックを保護します。電話機が Expressway 証明書を認証し、TLS セッションを確立するには、Expressway 証明書に、電話機のファームウェアが信頼しているパブリック認証局による署名が必要です。Expressway 証明書の認証に対して、電話機で他の CA 証明書をインストールしたり信頼したりすることはできません。

電話機ファームウェアに組み込まれているの CA 証明書の一覧は、
<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html> から入手できます。

Expressway 経由でのモバイルおよび Remote Access (MRA) は、Cisco Expressway で動作します。このため、『Cisco Expressway Administrator Guide』、『Cisco Expressway Basic Configuration Deployment Guide』などの Cisco Expressway のマニュアルをよくお読みいただく必要があります。Cisco Expressway のマニュアルは、
<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html> にあります。

ユーザに対しては、IPv4 プロトコルのみが Expressway 経由でのモバイルおよび Remote Access サポートされます。

Expressway 経由でのモバイルおよび Remote Access の操作方法については、以下の資料も参照してください。

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides*
- *Cisco Expressway* 展開ガイドによるモバイルおよび Remote Access

電話の登録プロセス中に、電話機に表示される日時が Network Time Protocol (NTP) サーバと同期されます。MRA では、日時の同期に指定される NTP サーバの IP アドレスを特定するために DHCP オプション 42 タグが使用されます。DHCP オプション 42 タグが設定情報の中に見つからない場合、電話機は 0.tandberg.pool.ntp.org タグを検索して NTP サーバを識別します。

登録後、電話機は SIP メッセージの情報を使って表示日時を同期します（ただし Cisco Unified Communications Manager 電話設定で NTP サーバが設定されている場合を除く）。



- (注) いくつかの電話機の電話セキュリティプロファイルで TFTP 暗号化設定にチェックマークが付いている場合、Mobile and Remote Access でその電話機を使用することはできません。MRA ソリューションでは、認証局プロキシ機能 (CAPF) とデバイスとのインタラクティブなやり取りをサポートしていません。

SIP OAuth モードは、MRA でサポートされています。このモードでは、セキュアな環境での認証に OAuth アクセス トークンを使用できます。



- (注) モバイルおよびリモート アクセス (MRA) モードの SIP OAuth の場合は、電話機を導入する際に、モバイルおよびリモート アクセスでのアクティベーション コードの導入のみを使用します。ユーザ名とパスワードを使用したアクティベーションはサポートされていません。

SIP OAuth モードでは、Expressway x14.0(1) 以降、または Cisco Unified Communications Manager 14.0 (1) 以降が必要です。

SIP OAuth モードの詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』、リリース 14.0(1) 以降を参照してください。

展開シナリオ

次の表に、Expressway 経由でのモバイルおよび Remote Access のさまざまな導入シナリオを示します。

シナリオ	Actions
Expressway 経由でのモバイルおよび Remote Access 導入後に、社内ユーザが企業ネットワークにログインします。	企業ネットワークが検出され、電話機が Cisco Unified Communications Manager に正常に登録されます。

シナリオ	Actions
<p>オフプレミスユーザが Expressway 経由でのモバイルおよび Remote Access で企業ネットワークにログインします。</p>	<p>電話機はオフプレミス モードになっていることを検出し、Expressway 経由でのモバイルおよび Remote Access サインイン ウィンドウが表示されて、ユーザが企業ネットワークに接続します。</p> <p>ユーザがネットワークに接続するには、有効なサービス名、ユーザ名、パスワードが必要です。</p> <p>また、ユーザは、企業ネットワークにアクセスする前に、サービスモードをリセットして、代替 TFTP 設定をクリアする必要があります。これにより代替 TFTP サーバ設定がクリアされ、電話機がオフプレミス ネットワークを検出します。</p> <p>電話機が出荷状態のまま導入される場合、ユーザはネットワーク設定のリセット要件をスキップできます。</p> <p>ユーザのネットワーク ルータで DHCP オプション 150 またはオプション 66 が有効になっている場合は、企業ネットワークにサインインできない場合があります。ユーザはこれらの DHCP 設定を無効にするか、スタティック IP アドレスを直接設定する必要があります。</p>

Expressway サインイン用ユーザ クレデンシャル パーシステントの設定

Expressway 経由でのモバイルおよび Remote Access でネットワークにサインインすると、そのユーザはサービス ドメイン、ユーザ名、パスワードの入力を求められます。Expressway サインイン用のユーザ クレデンシャル パーシステントのパラメータを有効化すると、ユーザのログイン クレデンシャルが保存され、この情報を再入力する必要がなくなります。このパラメータはデフォルトでは無効になっています。

単一の電話機、電話機グループ、またはすべての電話機について、クレデンシャルが永続的なものとなるように設定できます。

関連トピック

[電話機の機能設定](#) (114 ページ)

[プロダクト固有の設定](#) (116 ページ)

問題レポート ツール

ユーザが問題レポートを送信する際は、問題レポート ツールを使用します。



- (注) 問題レポート ツールのログは、Cisco TAC で問題をトラブルシューティングするとき必要となります。電話機を再起動すると、ログは消去されます。電話機を再起動する前に、ログを収集してください。

問題レポートを発行するには、ユーザは問題レポートツールにアクセスし、問題の発生日時、および問題の説明を提供します。

PRT のアップロードが失敗した場合は、電話機を使用して URL

http://<phone-ip-address>/FS/<prt-file-name> から PRT ファイルにアクセスできます。この URL は、次の場合に電話機に表示されます。

- 電話機が工場出荷時の状態の場合。URL の表示時間は 1 時間です。1 時間経過後は、電話機ログの送信を再度試行する必要があります。
- 電話機に設定ファイルをダウンロード済みで、コール制御システムで電話への Web アクセスが許可されている場合。

Cisco Unified Communications Manager の [カスタマーサポートアップロード URL (Customer Support Upload URL)] フィールドにサーバアドレスを追加する必要があります。

Expressway 経由で Mobile and Remote Access を使用してデバイスを導入している場合、Expressway サーバの HTTP サーバ許可リストへの PRT サーバアドレスの追加も必要となります。

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 機構を使用します。その際、アップロードに次のパラメータを含めます (マルチパート MIME 符号化を使用)。

- devicename (例: 「SEP001122334455」)
- serialno (例: 「FCH12345ABC」)
- ユーザ名 (Cisco Unified Communications Manager に設定されているユーザ名、デバイスの所有者)
- prt_file (例: 「probrep-20141021-162840.tar.gz」)

スクリプトのサンプルを次に示します。このスクリプトは参考用としてのみ提供されます。シスコでは、お客様のサーバにインストールされたアップロードスクリプトのサポートは提供していません。

```
<?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.");
}

?>
```



(注) 電話機は、HTTP Url のみをサポートしています。

手順

- ステップ 1 PRT アップロード スクリプトを実行できるサーバを設定します。
- ステップ 2 上記パラメータを処理できるスクリプトを記述するか、必要に応じて提供されたサンプルスクリプトを編集します。
- ステップ 3 サーバにスクリプトをアップロードします。
- ステップ 4 Cisco Unified Communications Manager で、個々のデバイス設定ウィンドウ、[共通の電話プロフィール (Common Phone Profile)]ウィンドウ、または[エンタープライズ電話の設定 (Enterprise Phone Configuration)]ウィンドウの [プロダクト固有の設定 (Product Specific Configuration Layout)]領域に移動します。
- ステップ 5 [カスタマーサポートのアップロード URL (Customer support upload URL)]をオンにし、アップロードサーバ URL を入力します。

例 :

<http://example.com/prtscript.php>

- ステップ 6 変更を保存します。

回線のラベルの設定

電話番号の代わりにテキスト ラベルを表示するよう電話機をセットアップすることができます。このラベルを使用し、回線を名前または機能で特定します。たとえば、ユーザが電話機の回線を共有している場合、回線を共有するユーザの名前で回線を特定できます。

キー拡張モジュールにラベルを追加すると、最初の 25 文字だけが行に表示されます。

手順

-
- ステップ 1** Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
 - ステップ 2** 設定する電話を特定します。
 - ステップ 3** 回線インスタンスを特定し、[回線のテキスト ラベル (Line Text Label)] フィールドを設定します。
 - ステップ 4** (任意) 回線を共有する別のデバイスにラベルを適用する必要がある場合は、[共有デバイス設定の更新 (Update Shared Device Settings)] チェックボックスをオンにして、[選択対象を反映 (Propagate Selected)] をクリックします。
 - ステップ 5** 保存を選択します。
-



第 10 章

社内ディレクトリとパーソナル ディレクトリ

- [社内ディレクトリのセットアップ](#) (151 ページ)
- [パーソナルディレクトリのセットアップ](#) (151 ページ)

社内ディレクトリのセットアップ

社内ディレクトリによって、ユーザが同僚の電話番号を調べることができます。この機能をサポートするには、社内ディレクトリを設定する必要があります。

Cisco Unified Communications Manager では、Cisco Unified Communications Manager と連動する Cisco Unified Communications Manager アプリケーションのユーザの認証情報と認可情報を保存するために、Lightweight Directory Access Protocol (LDAP) ディレクトリを使用しています。認証によって、システムに対するユーザのアクセス権が確立します。認可とは、ユーザが使用を許可されるテレフォニーリソース、たとえば特定の電話内線などを識別することです。

詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

LDAP ディレクトリの設定が完了すると、ユーザは電話機の社内ディレクトリサービスを使用して、社内ディレクトリでユーザを検索できるようになります。

関連トピック

- [Cisco Unified Communications Manager マニュアル](#) (14 ページ)

パーソナル ディレクトリのセットアップ

パーソナルディレクトリには、ユーザが一連の個人の番号を保存できます。

パーソナルディレクトリは、次の機能で構成されています。

- 個人アドレス帳 (PAB)
- スピードダイヤル

ユーザはこれらの方法を使用してパーソナル ディレクトリの機能を利用できます。

- Webブラウザから：ユーザは、Cisco Unified CommunicationsセルフケアポータルからPABおよびスピードダイヤル機能にアクセスできます。
- Cisco IP 電話から：企業ディレクトリまたはユーザの個人ディレクトリを検索するには、**[連絡先 (Contact)]**を選択します。

パーソナル ディレクトリを Web ブラウザから設定するには、ユーザがセルフケアポータルにアクセスする必要があります。管理者は、ユーザに対して URL とサインイン情報を提供する必要があります。



第 **IV** 部

Cisco IP 会議用電話のトラブルシューティング

- [電話システムのモニタリング \(155 ページ\)](#)
- [電話機のトラブルシューティング \(193 ページ\)](#)
- [メンテナンス \(215 ページ\)](#)
- [各言語ユーザのサポート \(221 ページ\)](#)



第 11 章

電話システムのモニタリング

- [電話システムの監視の概要](#) (155 ページ)
- [Cisco IP 電話のステータス](#) (155 ページ)
- [Cisco IP 電話の Web ページ](#) (171 ページ)
- [XML での電話からの情報要求](#) (188 ページ)

電話システムの監視の概要

電話機および電話機 Web ページの電話機ステータス メニューを使用すると、電話機に関するさまざまな情報を表示できます。この情報には、次のものが含まれます。

- 機器情報
- ネットワークのセットアップ情報
- ネットワーク統計
- デバイス ログ
- ストリームの統計

この章では、電話機の Web ページから取得可能な情報について説明します。この情報は、電話機の操作のリモート モニタやトラブルシューティングに役立てることができます。

関連トピック

- [電話機のトラブルシューティング](#) (193 ページ)

Cisco IP 電話のステータス

ここでは、Cisco IP 電話のモデル情報、ステータス メッセージ、およびネットワーク統計を表示する方法について説明します。

- [モデル情報 (Model Information)] : 電話機のハードウェアとソフトウェアに関する情報を表示します。

- [ステータス (Status)]メニュー：ステータスメッセージ、ネットワーク統計、および現在のコールに関する統計を表示する画面にアクセスできます。

これらの画面に表示される情報は、電話機の操作のモニタやトラブルシューティングに役立てることができます。

また、これらの情報の大半およびその他の関連情報は、電話機の Web ページからリモートで取得することもできます。

[電話の情報 (Phone Information)]ウィンドウの表示

手順

ステップ1 [設定 (Settings)]>[システム情報 (System information)]を押します。

ステップ2 このメニューを終了するには、[終了 (Exit)]を押します。

[ステータス (Status)]メニューの表示

手順

ステップ1 [設定 (Settings)]>[ステータス (Status)]を押します。

ステップ2 このメニューを終了するには、[終了 (Exit)]を押します。

[ステータス メッセージ (Status Messages)]ウィンドウの表示

手順

ステップ1 [設定 (Settings)]>[ステータス (Status)]>[ステータス メッセージ (Status Messages)]を押します。

ステップ2 このメニューを終了するには、[終了 (Exit)]を押します。

ステータス メッセージのフィールド

次の表に、電話機の [ステータス メッセージ (Status Messages)]画面に表示されるステータスメッセージを示します。

表 22: Cisco IP 電話のステータス メッセージ

メッセージ	説明	考えられる状況と対処方法
DHCP から IP アドレスを取得できませんでした (Could not acquire an IP address from DHCP)	電話機は DHCP サーバから IP アドレスを取得していません。工場出荷時の状態にリセットした場合に、このメッセージが表示される可能性があります。	DHCP サーバが使用可能であり、この電話機の IP アドレスが利用できることを確認します。
TFTP サイズエラー (TFTP Size Error)	電話機のファイルシステムに対して、設定ファイルのサイズが大きすぎます。	電話機の電源をオフ/オンにします。
ROM チェックサム エラー (ROM Checksum Error)	ダウンロードしたソフトウェアファイルが破損しています。	電話機のファームウェアの新しいコピーを入手し、それを TFTPPath ディレクトリに置きます。ファイルをこのディレクトリにコピーできるのは、TFTP サーバソフトウェアがシャットダウンされているときだけです。それ以外の場合にコピーすると、ファイルが破損する可能性があります。
IP が重複しています (Duplicate IP)	別のデバイスが、電話機に割り当てられた IP アドレスを使用中です。	電話機にスタティック IP アドレスが割り当てられている場合は、重複する IP アドレスを割り当てていないことを確認してください。 DHCP を使用している場合は、DHCP サーバの設定を確認してください。
CTL および ITL ファイルを削除中 (Erasing CTL and ITL files)	CTL および ITL ファイルを削除中です。	ありません。これは情報メッセージです。

メッセージ	説明	考えられる状況と対処方法
ロケールの更新エラー (Error Updating Locale)	1 つまたは複数のローカリゼーションファイルが、TFTP パス ディレクトリで見つからなかったか、または無効でした。ロケールは変更されませんでした。	<p>Cisco Unified Communications Operating System の管理ページから、次のファイルが [TFTP ファイルの管理 (TFTP File Management)] のサブディレクトリに存在することを確認してください。</p> <ul style="list-style-type: none"> • ネットワーク ロケールと同じ名前のサブディレクトリに存在するファイル： <ul style="list-style-type: none"> • tones.xml • ユーザ ロケールと同じ名前のサブディレクトリに存在するファイル： <ul style="list-style-type: none"> • glyphs.xml • dictionary.xml • kate.xml

メッセージ	説明	考えられる状況と対処方法
ファイルが見つかりません <Cfg ファイル> (File not found <Cfg File>)	TFTP サーバで、名前ベースのデフォルトの設定ファイルが見つかりませんでした。	<p>電話機の設定ファイルは、電話機が Cisco Unified Communications Manager データベースに追加されたときに作成されます。電話機が Cisco Unified Communications Manager データベースに存在しない場合、TFTP サーバは「CFG ファイルが見つかりません (CFG File Not Found)」という応答を生成します。</p> <ul style="list-style-type: none"> • 電話機が Cisco Unified Communications Manager に登録されていません。 電話機を自動登録できない場合は、手動で電話機を Cisco Unified Communications Manager に追加する必要があります。 • DHCP を使用している場合は、DHCP サーバが正しい TFTP サーバを指定していることを確認してください。 • スタティック IP アドレスを使用している場合は、TFTP サーバの設定を確認してください。
「ファイルが見つかりません <CTLFile.tlv> (File Not Found <CTLFile.tlv>)」	Cisco Unified Communications Manager クラスタがセキュアモードでない場合にこのメッセージが電話機に表示されます。	影響はありません。引き続き電話機は Cisco Unified Communications Manager に登録できます。
IP アドレス解放 (IP Address Released)	電話機は、IP アドレスを解放するように設定されます。	電話機は、電源をオフ/オンにするか、または DHCP アドレスをリセットするまで、アイドル状態のままです。

メッセージ	説明	考えられる状況と対処方法
IPv4 DHCP タイムアウト (IPv4 DHCP Timeout)	IPv4 DHCP サーバが応答しませんでした。	<p>ネットワークがビジーになっている：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。</p> <p>IPv4 DHCP サーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。</p> <p>IPv4 DHCP サーバがダウンしている：IPv4 DHCP サーバの設定を確認してください。</p> <p>エラーが続く：静的IPv4アドレスを割り当てることを検討してください。</p>
IPv6 DHCP タイムアウト (IPv6 DHCP Timeout)	IPv6 DHCP サーバが応答しませんでした。	<p>ネットワークがビジーになっている：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。</p> <p>IPv6 DHCP サーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。</p> <p>IPv6 DHCP サーバがダウンしている：IPv6 DHCP サーバの設定を確認してください。</p> <p>エラーが続く：静的IPv6アドレスを割り当てることを検討してください。</p>
IPv4 DNS タイムアウト (IPv4 DNS Timeout)	IPv4 DNS サーバが応答しませんでした。	<p>ネットワークがビジーになっている：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。</p> <p>IPv4 DNS サーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。</p> <p>IPv4 DNS サーバがダウンしている：IPv4 DNS サーバの設定を確認してください。</p>

メッセージ	説明	考えられる状況と対処方法
IPv6 DNS タイムアウト (IPv6 DNS Timeout)	IPv6 DNS サーバが応答しませんでした。	<p>ネットワークがビジーになっている：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。</p> <p>IPv6 DNS サーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。</p> <p>IPv6 DNS サーバがダウンしている：IPv6 DNS サーバの設定を確認してください。</p>
DNS 不明 IPv4 ホスト (DNS unknown IPv4 Host)	IPv4 DNS が TFTP サーバまたは Cisco Unified Communications Manager の名前を解決できませんでした。	<p>TFTP サーバまたは Cisco Unified Communications Manager のホスト名が IPv4 DNS に正しく設定されていることを確認してください。</p> <p>ホスト名ではなく、IPv4 アドレスを使用することを検討してください。</p>
DNS 不明 IPv6 ホスト (DNS unknown IPv6 Host)	IPv6 DNS が TFTP サーバまたは Cisco Unified Communications Manager の名前を解決できませんでした。	<p>TFTP サーバまたは Cisco Unified Communications Manager のホスト名が IPv6 DNS に正しく設定されていることを確認してください。</p> <p>ホスト名ではなく、IPv6 アドレスを使用することを検討してください。</p>
拒否された HC のロード (Load Rejected HC)	ダウンロードされたアプリケーションには、電話機のハードウェアとの互換性がありません。	<p>この電話機でのハードウェア変更をサポートしていないバージョンのソフトウェアをインストールしようとするが発生します。</p> <p>電話機に割り当てられたロード ID を確認します (Cisco Unified Communications Manager で [デバイス (Device)] > [電話 (Phone)] を選択します)。電話機に表示されたロードを再入力します。</p>

メッセージ	説明	考えられる状況と対処方法
デフォルト ルータがありません (No Default Router)	DHCP またはスタティック設定でデフォルトルータが指定されていませんでした。	電話機にスタティック IP アドレスが割り当てられている場合は、デフォルトルータが設定されていることを確認してください。 DHCP を使用している場合は、DHCP サーバがデフォルトルータを提供していません。DHCP サーバの設定を確認してください。
IPv4 DNS サーバがありません (No IPv4 DNS Server)	名前は指定されていましたが、DHCP または静的 IP 設定で IPv4 DNS サーバのアドレスが指定されていませんでした。	電話機に静的 IP アドレスが割り当てられている場合は、IPv4 DNS サーバが設定されていることを確認してください。 DHCP を使用している場合は、DHCP サーバが IPv4 DNS サーバを提供していません。DHCP サーバの設定を確認してください。
IPv6 DNS サーバがありません (No IPv6 DNS Server)	名前は指定されていましたが、DHCP または静的 IP 設定で IPv6 DNS サーバのアドレスが指定されていませんでした。	電話機に静的 IP アドレスが割り当てられている場合は、IPv6 DNS サーバが設定されていることを確認してください。 DHCP を使用している場合は、DHCP サーバが IPv6 DNS サーバを提供していません。DHCP サーバの設定を確認してください。
信頼リストがインストールされていません (No Trust List installed)	CTL ファイルまたは ITL ファイルが電話機にインストールされていません。	信頼ファイルが Cisco Unified Communications Manager で設定されていません。Cisco Unified Communications Manager はデフォルトではセキュリティをサポートしません。 信頼リストが設定されていません。 信頼リストの詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。
電話機を登録できませんでした。 (Phone failed to register.) 証明書のキーサイズは FIPS に準拠していません。 (Cert key size is not FIPS compliant.)	FIPS では、RSA サーバ証明書は 2048 ビット以上である必要があります。	証明書を更新してください。

メッセージ	説明	考えられる状況と対処方法
「Cisco Unified Communications Manager 要求による再起動 (Restart requested by CUCM) 」	Cisco Unified Communications Manager (CUCM) からの要求に基づいて電話機が再起動します。	Cisco Unified Communications Manager で電話機の設定変更が行われ、変更を有効にするために [設定の適用 (Apply Config)] ボタンが押された可能性があります。
TFTP アクセス エラー (TFTP access error)	TFTP サーバが、存在しないディレクトリを指定しています。	DHCP を使用している場合は、DHCP サーバが正しい TFTP サーバを指定していることを確認してください。 スタティック IP アドレスを使用している場合は、TFTP サーバの設定を確認してください。
TFTP エラー (TFTP error)	電話機が TFTP サーバから提供されたエラー コードを認識しません。	Cisco TAC にお問い合わせください。
TFTP タイムアウト	TFTP サーバが応答しませんでした。	ネットワークがビジーになっている : このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。 TFTP サーバと電話機との間にネットワーク接続がない : ネットワーク接続を確認してください。 TFTP サーバがダウンしている : TFTP サーバの設定を確認してください。
タイムアウト (Timed Out)	サブリカントが 802.1X トランザクションを実行しようとしたますが、オーセンティケータが存在しないためにタイムアウトになりました。	通常は、802.1X がスイッチに設定されていない場合に認証がタイムアウトします。

メッセージ	説明	考えられる状況と対処方法
信頼リストの更新に失敗しました (Trust List update failed)	CTL ファイルおよび ITL ファイルの更新に失敗しました。	<p>電話機は CTL ファイルおよび ITL ファイルをインストールしていますが、新しい CTL ファイルおよび ITL ファイルの更新に失敗しました。</p> <p>失敗の理由として次が考えられます。</p> <ul style="list-style-type: none"> • ネットワークの障害が発生した。 • TFTP サーバがダウンしていた。 • CTL ファイルの署名に使用された新しいセキュリティトークン、および、ITL ファイルの署名に使用された TFTP 証明書が導入されたが、電話機の現在の CTL ファイルおよび ITL ファイルには使用できない。 • 内部的な電話障害が発生した。 <p>解決策として次が考えられます。</p> <ul style="list-style-type: none"> • ネットワーク接続を確認します。 • TFTP サーバがアクティブで、正常に機能しているかどうかを確認する。 • Transactional Vsam Services (TVS) サーバが Cisco Unified Communications Manager でサポートされている場合は、TVS サーバがアクティブで、正常に機能しているかどうかを確認する。 • セキュリティ トークンおよび TFTP サーバが有効かどうかを確認する。 <p>上述の解決策がすべて失敗した場合は、手動で CTL ファイルおよび ITL ファイルを削除し、電話機をリセットする。</p> <p>信頼リストの詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。</p>

メッセージ	説明	考えられる状況と対処方法
信頼リストが更新されました (Trust List updated)	CTL ファイル、ITL ファイル、またはその両方が更新されます。	ありません。これは情報メッセージです。 信頼リストの詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。
ルックアップエラー	電話機のロードファイルの名前が不正です。	電話機のロードファイルが正しい名前であることを確認してください。
XmlDefault.cnf.xml (または電話機のデバイス名に対応した.cnf.xml)	コンフィギュレーションファイルの名前。	ありません。このメッセージは、電話機の設定ファイル名を示します。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

[ネットワーク統計情報 (Network Statistics)]ウィンドウの表示

手順

-
- ステップ 1** [設定 (Settings)]>[ステータス (Status)]>[ネットワーク統計情報 (Call Statistics)]を押します。
- ステップ 2** このメニューを終了するには、[終了 (Exit)]を押します。
-

[ネットワーク統計 (Network Statistics)]フィールド

次の表では、[ネットワーク統計 (Network Statistics)]画面の情報について説明します。

表 23:[ネットワーク統計 (Network Statistics)]フィールド

項目	説明
Tx フレーム (Tx Frames)	電話機が送信したパケットの数。
Tx ブロードキャスト	電話機が送信したブロードキャストパケットの数。
Tx ユニキャスト	電話機が送信したユニキャストパケットの総数。
Rx フレーム	電話機が受信したパケットの数。

項目	説明
Rx ブロードキャスト	電話機が受信したブロードキャストパケットの数。
Rx ユニキャスト	電話機が受信したユニキャストパケットの総数。
CDP ネイバー デバイス ID	CDP プロトコルで検出された、このポートに接続されているデバイスの ID。
CDP ネイバー IP アドレス	IP を使用して CDP プロトコルで検出された、このポートに接続されているデバイスの ID。
CDP ネイバー ポート	CDP プロトコルで検出された、このポートに接続されているデバイスの ID。
[リスタートの原因 (Restart Cause)] : 次のいずれかの値になります。 <ul style="list-style-type: none"> • ハードウェアリセット (Hardware Reset) (電源を投入したままのリセット) • ソフトウェアリセット (Software Reset) (メモリ コントローラもあわせてリセット) • ソフトウェアリセット (Software Reset) (メモリ コントローラはリセットしない) • ウォッチドッグリセット (Watchdog Reset) • 初期化 • 不明 (Unknown) 	電話機が最後にリセットされた原因。
ポート 1	ネットワークポートのリンクステートと接続 (たとえば、100 Full は、PC ポートがリンクアップ状態で、全二重の 100 Mbps 接続を自動ネゴシエーションしたことを意味します)。

項目	説明
IPv4	<p>DHCP ステータスに関する情報。これには、次の状態があります。</p> <ul style="list-style-type: none">• CDP BOUND• CDP INIT• DHCP BOUND• DHCP DISABLED• DHCP INIT• DHCP INVALID• DHCP REBINDING• DHCP REBOOT• DHCP RENEWING• DHCP REQUESTING• DHCP RESYNC• DHCP UNRECOGNIZED• DHCP WAITING COLDBOOT TIMEOUT• DISABLED DUPLICATE IP• SET DHCP COLDBOOT• SET DHCP DISABLED• SET DHCP FAST

項目	説明
IPv6	<p>DHCP ステータスに関する情報。これには、次の状態があります。</p> <ul style="list-style-type: none"> • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

[コール統計 (Call Statistics)] ウィンドウの表示

手順

ステップ 1 [設定 (Settings)] > [ステータス (Status)] > [コール統計 (Call Statistics)] を押します。

ステップ 2 このメニューを終了するには、[終了 (Exit)] を押します。

コール統計のフィールド

次の表に、[コール統計 (Call Statistics)] 画面の項目を示します。

表 24: コールの統計の項目

項目	説明
[受信コーデック (Receiver Codec)]	受信した音声ストリームの種類 (コーデックからの RTP ストリーミング オーディオ) : <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
送信コーデック (Sender Codec)	送信した音声ストリームの種類 (コーデックからの RTP ストリーミング オーディオ) : <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
[受信サイズ (Receiver Size)]	受信中の音声ストリーム (RTP ストリーミング オーディオ) の音声パケットサイズ (ミリ秒)。

項目	説明
送信サイズ (Sender Size)	送信中の音声ストリームの音声パケット サイズ (ミリ秒)。
受信パケット (Rcvr Packets)	音声ストリームが開始されてから受信された RTP 音声パケットの数。 (注) コールが保留されていた可能性があるため、この数値は、必ずしもコールが開始されてから受信された RTP 音声パケットの数と同じであるとは限りません。
送信パケット (Sender Packets)	音声ストリームが開始されてから送信された RTP 音声パケットの数。 (注) コールが保留されていた可能性があるため、この数値は、必ずしもコールが開始されてから送信された RTP 音声パケットの数と同じであるとは限りません。
平均ジッター (Avg Jitter)	受信中の音声ストリームが開始されてから測定された、RTP パケット ジッターの推定平均値 (パケットがネットワークを経由する際の動的な遅延) (ミリ秒単位)。
最大ジッター (Max Jitter)	受信中の音声ストリームが開始されてから測定された最大ジッター (ミリ秒単位)。
[受信破棄 (Receiver Discarded)]	受信中の音声ストリームで廃棄された RTP パケットの数 (不良パケット、過度の遅延などによる)。 (注) シスコゲートウェイが生成したペイロードタイプ 19 のコンフォート ノイズパケットはこのカウンタを増分するため、電話機はこれらのパケットを破棄します。
受信喪失パケット (Rcvr Lost Packets)	失われた RTP パケット (転送中に喪失)。
音声品質メトリック (Voice Quality Metrics)	
累積フレーム損失率 (Cumulative Conceal Ratio)	隠蔽フレームの総数を、音声ストリームの開始以降に受信された音声フレームの総数で割った値。

項目	説明
直近フレーム損失率 (Interval Conceal Ratio)	アクティブな音声に先行する 3 秒間の間隔における、音声フレームに対する隠蔽フレームの比率。音声アクティビティ検出 (VAD) を使用する場合は、アクティブな音声を 3 秒集めるために、もっと長い間隔が必要になる可能性があります。
最大フレーム損失率 (Max Conceal Ratio)	音声ストリームの開始以降、最も高い間隔の損失率。
[フレーム損失発生秒数 (Conceal Seconds)]	音声ストリームの開始以降、隠蔽イベント (フレーム損失) があった秒数 ([深刻なフレーム損失発生秒数 (Severely Conceal Secs)] の値を含む)。
[深刻なフレーム損失発生秒数 (Severely Conceal Seconds)]	音声ストリームの開始以降、5% を超える隠蔽イベント (フレーム損失) があった秒数。
遅延	ネットワーク遅延の推定値 (ミリ秒単位)。ラウンドトリップ遅延の実行中の平均値を表します。これは、RTCP 受信レポートブロックの受信時に測定されます。

Cisco IP 電話の Web ページ

Cisco IP 電話には、それぞれ Web ページがあります。この Web ページで、電話機に関する次のような情報を表示できます。

- [デバイス情報 (Device Information)] : 電話機のデバイス設定と関連情報を表示します。
- [ネットワークのセットアップ (Network Setup)] : ネットワークのセットアップ情報とその他の電話機の設定情報を表示します。
- [ネットワーク統計情報 (Network Statistics)] : ネットワークトラフィックに関する情報を提供するハイパーリンクを表示します。
- [デバイスログ (Device Logs)] : トラブルシューティングに利用できる情報を提供するハイパーリンクを表示します。
- [ストリームの統計 (Streaming Statistic)] : さまざまなストリーミング統計情報へのハイパーリンクが表示されます。

この項では、電話機の Web ページから取得可能な情報について説明します。この情報は、電話機の操作のリモートモニターやトラブルシューティングに役立てることができます。

また、この情報の多くは、電話機から直接取得することもできます。

電話機の Web ページへのアクセス



(注) Web ページにアクセスできない場合は、デフォルトでアクセスが無効になっている可能性があります。

手順

ステップ 1 次の方法のいずれかを使用して、Cisco IP 電話の IP アドレスを入手します。

- a) Cisco Unified Communications Manager の管理で [デバイス (Device)] > [電話 (Phone)] の順に選択して、電話機を検索します。Cisco Unified Communications Manager に登録されている電話機の IP アドレスが、[電話の検索と一覧表示 (Find and List Phones)] ウィンドウと [電話の設定 (Phone Configuration)] ウィンドウの上部に表示されます。
- b) 電話機で [設定 (Settings)] > [システム情報 (System Information)] を押して、[IPv4 アドレス (IPv4 address)] フィールドまでスクロールします。

ステップ 2 Web ブラウザを開いて、次の URL を入力します。ここで、*IP_address* は Cisco IP 電話の IP アドレスです。

`http://<IP_address>`

[デバイス情報 (Device Information)] Web ページ

電話機の Web ページの [デバイス情報 (Device Information)] エリアには、電話機のデバイス設定と関連情報が表示されます。次の表に、これらの項目を示します。

[デバイス情報 (Device Information)] 領域を表示するには、電話機の Web ページにアクセスしてから、[デバイス情報 (Device Information)] ハイパーリンクをクリックします。

表 25: [デバイス情報 (Device Information)] Web ページのフィールド

フィールド	説明
Service mode	電話機のサービス モード。
サービス ドメイン	サービスのドメイン。
サービスの状態 (Service state)	サービスの現在の状態。
[MAC アドレス (MAC Address)]	電話機のメディア アクセス コントロール (MAC) アドレス。

フィールド	説明
ホスト名 (Host Name)	電話機の MAC アドレスに基づいて電話機に自動的に割り当てられる一意の固定された名前。
電話機の電話番号	電話機に割り当てられている電話番号。
アプリケーションロード ID	アプリケーション ロード バージョンを識別します。
起動ロード ID	起動ロード バージョンを識別します。
Version	電話機で作動しているファームウェアの ID。
Hardware Revision	電話機のハードウェアのマイナーリビジョン値。
シリアル番号	電話機の固有のシリアル番号。
モデル番号 (Model Number)	電話機のモデル番号。
メッセージ受信	この電話機のプライマリ回線で受信したボイス メッセージがあるかどうかを示します。
UDI	電話機に関する次の Cisco Unique Device Identifier (UDI) 情報を表示します。 <ul style="list-style-type: none"> • ハードウェア タイプ • 電話機モデル名 • Product Identifier。 • バージョン ID (VID): 主要なハードウェアバージョン番号を指定します。 • Serial number
時刻 (Time)	電話機が属する日時グループの時間。この情報は、Cisco Unified Communications Manager から取得されます。
Time Zone	電話機が属する日時グループのタイムゾーン。この情報は、Cisco Unified Communications Manager から取得されます。
日付 (Date)	電話機が属する日時グループの日付。この情報は、Cisco Unified Communications Manager から取得されます。
システム空きメモリ	使用可能なシステム メモリの量。
Java ヒープ空きメモリ	Java ヒープ用の空きメモリ量。
Java プール空きメモリ	Java プール用の空きメモリ量。

フィールド	説明
FIPS モード有効	連邦情報処理標準 (FIPS) モードが有効かどうかを示します。

[ネットワークのセットアップ (Network Setup)] Web ページ

電話機の Web ページにある [ネットワークのセットアップ (Network Setup)] エリアには、ネットワークの設定情報と電話機のその他の設定に関する情報が表示されます。次の表に、これらの項目を示します。

これらの項目の多くは、Cisco IP 電話の [ネットワークのセットアップ (Network Setup)] メニューで表示し、設定できます。

[ネットワークのセットアップ (Network Setup)] 領域を表示するには、電話機の Web ページにアクセスし、次に [ネットワークのセットアップ (Network Setup)] ハイパーリンクをクリックします。

表 26: [ネットワークのセットアップ (Network Setup)] 領域の項目

項目	説明
MAC アドレス	電話機のメディア アクセス コントロール (MAC) アドレス。
ホスト名 (Host Name)	DHCP サーバが電話機に割り当てたホスト名。
ドメイン名 (Domain Name)	電話機が所属するドメイン ネーム システム (DNS) ドメインの名前。
DHCP サーバ (DHCP Server)	電話機の IP アドレス取得元となる Dynamic Host Configuration Protocol (DHCP) サーバの IP アドレス。
BOOTP Server	電話機が設定をブートストラップ プロトコル (BootP) サーバから取得するかどうかを示します。
DHCP	電話機が DHCP を使用するかどうかを示します。
IP アドレス (IP Address)	電話機のインターネット プロトコル (IP) アドレス。
サブネットマスク	電話機で使用されるサブネットマスク。
デフォルト ルータ 1 (Default Router 1)	電話機で使用される、デフォルト ルータ。

項目	説明
DNS サーバ 1 ~ 3 (DNS Server 1-3)	電話機で使用されるプライマリ DNS サーバ ([DNS サーバ 1 (DNS Server 1)]) およびオプションのバックアップ DNS サーバ ([DNS サーバ 2 (DNS Server 2)] ~ [DNS サーバ 3 (DNS Server 3)])。
代替 TFTP	電話機が代替 TFTP サーバを使用しているかどうかを示します。
TFTP サーバ 1 (TFTP Server 2)	電話機で使用される、プライマリの Trivial File Transfer Protocol (TFTP) サーバ。
TFTP サーバ 2 (TFTP Server 2)	電話機で使用される、バックアップの Trivial File Transfer Protocol (TFTP) サーバ。
DHCP アドレス解放 (DHCP Address Released)	[DHCP アドレス解放 (DHCP Address Released)] オプションの設定を示します。
接続先 VLAN ID (Operational VLAN ID)	電話機が所属する、Cisco Catalyst スイッチに設定された接続先 Virtual Local Area Networks (VLAN)。
[管理 VLAN ID (Admin VLAN ID)]	電話機がメンバーになっている補助 VLAN。

項目	説明
Unified CM 1 ～ 5	<p>電話機を登録可能な Cisco Unified Communications Manager サーバのホスト名または IP アドレス（優先度順）。限定された Cisco Unified Communications Manager 機能を提供できる SRST ルータが使用可能な場合、項目にそのルータの IP アドレスが表示されることもあります。</p> <p>使用可能なサーバについては、この項目に Cisco Unified Communications Manager サーバの IP アドレスと、次の状態のいずれかが表示されます。</p> <ul style="list-style-type: none"> • [アクティブ (Active)] : 電話機が現在コール処理サービスを受けている Cisco Unified Communications Manager サーバです。 • [スタンバイ (Standby)] : 現在のサーバがダウンした場合に、電話機が切り替える先の Cisco Unified Communications Manager サーバ。 • [空白 (Blank)] : この Cisco Unified Communications Manager サーバへの接続は現在ありません。 <p>項目には、Survivable Remote Site Telephony (SRST) 指定も含めることができます。これは、限定された Cisco Unified Communications Manager 機能を提供できる SRST ルータを特定します。このルータは、他のすべての Cisco Unified Communications Manager サーバが到達不能になった場合に、コールの処理を引き継ぎます。SRST Cisco Unified Communications Manager は、アクティブであっても、常にサーバのリストの最後尾に表示されます。SRST ルータ アドレスは、[Cisco Unified CM の設定 (Cisco Unified Communications Manager Configuration)] ウィンドウの [デバイスプール (Device Pool)] セクションで設定します。</p>
情報 URL	電話機に表示されるヘルプテキストの URL。
ディレクトリ URL (Directories URL)	電話機がディレクトリ情報を取得するサーバの URL。

項目	説明
メッセージ URL (Messages URL)	電話機でメッセージサービスの取得元となるサーバの URL。
Services URL	電話機が Cisco IP 電話 サービスを取得するサーバの URL。
Idle URL	電話機が [URL のアイドル時間 (Idle URL Time)] フィールドで指定された時間にわたって使用されず、メニューが開かれていない場合に表示される URL。
URL のアイドル時間 (Idle URL Time)	電話機がアイドル状態で、いかなるメニューも開かれない時間 (秒数) であり、この時間の経過後、[アイドル URL (Idle URL)] で指定した XML サービスがアクティブになります。
Proxy Server URL	電話機の HTTP クライアントの代わりにローカル以外のホストアドレスに HTTP 要求を送信し、ローカル以外のホストから電話機の HTTP クライアントへの応答を提供するプロキシサーバの URL。
認証 URL (Authentication URL)	電話機の Web サーバに発行された要求を検証するために、電話機が使用する URL。
SW ポートのセットアップ (SW Port Setup)	<p>スイッチポートの速度とデュプレックス。次のいずれかになります。</p> <ul style="list-style-type: none"> • [A] : 自動ネゴシエーション • [10H] : 10-BaseT/半二重 • [10F] : 10-BaseT/全二重 • [100H] : 100-BaseT/半二重 • [100F] : 100-BaseT/全二重 • [1000F] : 1000-BaseT/全二重 • [リンクがありません (NoLink)] : スイッチポートへの接続がありません。
User Locale	電話機のユーザに関連付けられているユーザロケール。言語、フォント、日付と時刻の形式、および英数字キーボードのテキスト情報など、ユーザをサポートするための一連の詳細情報を示します。

項目	説明
Network Locale	電話機のユーザに関連付けられているネットワーク ロケール。電話機が使用するトーンと断続周期の定義など、特定の場所にある電話機をサポートするための一連の詳細情報を示します。
ユーザ ロケール バージョン (User Locale Version)	電話機にロードされたユーザ ロケールのバージョン。
ネットワーク ロケール バージョン (Network Locale Version)	電話機にロードされたネットワーク ロケールのバージョン。
スピーカーを使う (Speaker Enabled)	電話機のスピーカーフォンが有効になっているかどうかを示します。
グループ リッスン (Group Listen)	電話機のグループ リッスン機能が有効になっているかどうかを示します。グループ リッスンを使用すると、ハンドセットを使用して話すと同時にスピーカで聞くことができます。
GARP を使う (GARP Enabled)	電話機が Gratuitous ARP 応答から MAC アドレスを取得するかどうかを示します。
自動回線選択を使う (Auto Line Select Enabled)	電話機が、すべての回線上でコール フォークラスを着信コールに移動するかどうかを指定します。
通話制御の DSCP (DSCP for Call Control)	コール制御シグナリングの DSCP IP 分類。
設定の DSCP (DSCP for Configuration)	電話機の設定転送の DSCP IP 分類。
サービスの DSCP (DSCP for Services)	電話機ベースのサービスの DSCP IP 分類。
セキュリティ モード	電話機に設定されているセキュリティモード。
Web アクセス可能 (Web Access Enabled)	電話機の Web アクセスが有効 ([はい (Yes)]) か無効 ([いいえ (No)]) かを示します。
SSH アクセス有効 (SSH Access Enabled)	電話機が SSH 接続を受け入れるか、またはブロックするかどうかを示します。

項目	説明
CDP : SW ポート (CDP: SW Port)	<p>スイッチポートでCDPがサポートされているかどうかを示します (デフォルトでは有効)。</p> <p>電話機、電力ネゴシエーション、QoS 管理、および 802.1x セキュリティに VLAN を割り当てる場合は、スイッチポートで CDP を有効にします。</p> <p>電話機を Cisco スイッチに接続した場合は、スイッチポートで CDP を有効にします。</p> <p>CDP が Cisco Unified Communications Manager で無効になっているときは、電話機を Cisco スイッチ以外のスイッチに接続した場合に限り、スイッチポートで CDP を無効にする必要があることを示す警告が表示されます。</p> <p>PC ポートとスイッチポートの CDP に関する現在の値は、[設定 (Settings)] メニューに表示されます。</p>
LLDP-MED : SW ポート (LLDP-MED: SW Port)	<p>スイッチポートで Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) が有効になっているかどうかを示します。</p>
LLDP 電力の優先順位 (LLDP Power Priority)	<p>電話機の電源優先度をスイッチにアダプタイズし、スイッチが電力を適切に電話機に供給できるようにします。次の設定があります。</p> <ul style="list-style-type: none"> • 不明 (Unknown) : これがデフォルト値です。 • 低 • 大きい • クリティカル
LLDP Asset ID	<p>在庫管理のため電話機に割り当てられているアセット ID を識別します。</p>
CTL ファイル	<p>CTL ファイルを識別します。</p>
ITL ファイル	<p>ITL ファイルには最初の信頼リストが含まれます。</p>
ITL 署名 (CTL Signature)	<p>CTL ファイルおよび ITL ファイルにセキュアハッシュアルゴリズム (SHA-1) を使用することにより、セキュリティを強化します。</p>
CAPF サーバ (CAPF Server)	<p>電話機で使用される CAPF サーバの名前。</p>

項目	説明
信頼検証サービス (TVS)	デフォルトセキュリティの主要コンポーネント。Cisco Unified IP 電話は Trust Verification Services (TVS) を使用して、HTTPS 確立時に EM サービス、ディレクトリ、MIDlet などのアプリケーションサーバを認証できます。
TFTP サーバ (TFTP Server)	電話機で使用される TFTP サーバの名前。
自動ポート同期	パケット損失を防止する低速度にポートを同期します。
Switch Port Remote Configuration	管理者は Cisco Unified Communications Manager の管理ページを使用して、Cisco Desktop Collaboration Experience のテーブルポートの速度と機能をリモートに設定できます。
PC Port Remote Configuration	PC ポートで速度およびデュプレックスモードのリモートポート設定が有効であるか無効であることを示します。
IP アドレッシングモード (IP Addressing Mode)	電話機で使用できる IP アドレッシングモードを表示します。
IP 設定モード制御 (IP Preference Mode Control)	電話機で IPv4 と IPv6 の両方が使用できる場合、電話機が Cisco Unified Communications Manager とのシグナリング中に使用する IP アドレスのバージョンを示します。
メディアの IP 設定モード (IP Preference Mode For Media)	メディアに関してデバイスが IPv4 アドレスを使用して Cisco Unified Communications Manager に接続することを示します。
IPv6 自動設定 (IPv6 Auto Configuration)	電話機で自動設定が有効になっているか無効になっているかを表示します。
IPv6 DAD 機能 (IPv6 DAD)	アドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を検証します。
IPv6 リダイレクトメッセージを許可 (IPv6 Accept Redirect Message)	宛先番号に使用されている同じルータからのリダイレクトメッセージを電話機が受け入れるかどうかを示します。
IPv6 マルチキャスト エコー要求に回答 (IPv6 Reply Multicast Echo Request)	IPv6 アドレスに送信されるエコー要求メッセージへの応答として電話機がエコー応答メッセージを送信することを示します。

項目	説明
IPv6 負荷サーバ (IPv6 Load Server)	各電話機のアップグレードで WAN リンクを通過する必要がないように、イメージをローカルに保存することによって、電話機ファームウェアのアップグレードのためのインストール時間を最適化し、WAN の負荷を軽減するために使用されます。
IPv6 ログ サーバー	電話機からのログ メッセージの送信先になるリモート ログ マシンの IP アドレスとポートを示します。
IPv6 CAPF サーバ (IPv6 CAPF Server)	電話機が使用する CAPF の通常名 (Cisco Unified Communications Manager の証明書から)。
DHCPv6	DHCP (ダイナミックホストコンフィギュレーションプロトコル) を使用している場合、ネットワークにデバイスを接続すると、デバイスの IPv6 アドレスが自動的に割り当てられます。Cisco Unified IP 電話では、DHCP がデフォルトで有効になります。
IPv6 アドレス	電話機の現在の IPv6 アドレスを表示したり、新しい IPv6 アドレスを入力したりすることができます。
IPv6 プレフィックス長 (IPv6 Prefix Length)	サブネットの現在のプレフィックス長を表示したり、新しいプレフィックス長を入力したりすることができます。
IPv6 デフォルト ルータ 1	電話機で使用されるデフォルト ルータを表示したり、新しい IPv6 デフォルトルータを入力したりすることができます。
IPv6 DNS サーバ 1 (IPv6 DNS Server 1)	電話機で使用されるプライマリ DNSv6 サーバを表示したり、新しいサーバを入力したりすることができます。
IPv6 DNS サーバ 2 (IPv6 DNS Server 1)	電話機で使用されるセカンダリ DNSv6 サーバを表示したり、新しいセカンダリ DNSv6 サーバを設定したりすることができます。
IPv6 代替 TFTP (IPv6 Alternate TFTP)	ユーザが代替 (セカンダリ) IPv6 TFTP サーバを使用できるようにします。

項目	説明
IPv6 TFTP サーバ 1 (IPv6 TFTP Server 1)	電話機で使用されるプライマリ IPv6 TFTP サーバを表示したり、新しいプライマリ TFTP サーバを設定したりすることができます。
IPv6 TFTP サーバ 2 (IPv6 TFTP Server 2)	プライマリ IPv6 TFTP サーバが使用不可のときにセカンダリ IPv6 TFTP サーバを表示するか、新しいセカンダリ TFTP サーバの設定をユーザに許可します。
IPv6 アドレス解放 (IPv6 Address Released)	ユーザが IPv6 関連情報を解放できるようにします。
EnergyWise 電力レベル (Energywise Power Level)	EnergyWise ネットワーク内のデバイスによって消費されるエネルギーを測定します。
Energywise Domain	電力のモニタリングと制御を目的とする管理上のデバイス グループ。

[イーサネット情報 (Ethernet Information)] Web ページ

次の表では、[イーサネット情報 (Ethernet Information)] Web ページの内容について説明しています。

表 27: [イーサネット情報 (Ethernet Information)] の項目

項目	説明
Tx フレーム (Tx Frames)	電話機が送信するパケットの総数。
Tx ブロードキャスト	電話機が送信するブロードキャストパケットの総数。
Tx マルチキャスト	電話機が送信するマルチキャストパケットの総数。
Tx ユニキャスト	電話機が送信するユニキャストパケットの総数。
Rx フレーム	電話機が受信したパケットの総数。
Rx ブロードキャスト	電話機が受信するブロードキャストパケットの総数。
Rx マルチキャスト	電話機が受信するマルチキャストパケットの総数。

項目	説明
Rx ユニキャスト	電話機が受信するユニキャストパケットの総数。
Rx PacketNoDes	ダイレクトメモリアクセス (DMA) 記述子がないため廃棄されたパケットの総数。

[ネットワーク (Network)] の Web ページ

次の表に [ネットワーク領域 (Network Area)] Web ページの情報を示します。



- (注) [ネットワーク統計情報 (Network statistics)] の下の [ネットワーク (Network)] リンクをクリックすると、ポート情報のページ「」が表示されます。

表 28: [ネットワーク領域 (Network Area)] の項目

項目	説明
Rx totalPkt	電話機が受信したパケットの合計数。
Rx マルチキャスト	電話機が受信したマルチキャストパケットの合計数。
Rx ブロードキャスト	電話機が受信したブロードキャストパケットの合計数。
Rx ユニキャスト	電話機が受信したユニキャストパケットの合計数。
Rx tokenDrop	リソース不足 (FIFO オーバーフローなど) が原因でドロップされたパケットの合計数。
Tx totalGoodPkt	電話機が受信した有効なパケット (マルチキャスト、ブロードキャスト、およびユニキャスト) の合計数。
Tx ブロードキャスト	電話機が送信したブロードキャストパケットの合計数。
Tx マルチキャスト	電話機が送信したマルチキャストパケットの合計数。
LLDP FramesOutTotal	電話機から送信された LLDP フレームの合計数。

項目	説明
LLDP AgeoutsTotal	キャッシュ内でタイムアウトになった LLDP フレームの合計数。
LLDP FramesDiscardedTotal	必須 TLV のいずれかについて、欠落している、順序に誤りがある、または範囲を超える文字列長が含まれているために廃棄された LLDP フレームの合計数。
LLDP FramesInErrorsTotal	検出可能なエラーが 1 つ以上含まれる状態で受信された LLDP フレームの合計数。
LLDP FramesInTotal	電話機が受信した LLDP フレームの合計数。
LLDP TLVDiscardedTotal	破棄された LLDP TLV の総数。
LLDP TLVUnrecognizedTotal	電話機で認識されなかった LLDP TLV の総数。
CDP ネイバー デバイス ID	CDP で検出されたこのポートに接続されているデバイスの ID。
CDP ネイバー IP アドレス	CDP で検出されたネイバー デバイスの IP アドレス。
CDP ネイバー IPv6 アドレス	CDP で検出されたネイバー デバイスの IPv6 アドレス。
CDP ネイバー ポート	CDP で検出された、電話機が接続されているネイバー デバイスのポート。
LLDP ネイバー デバイス ID	LLDP で検出された、このポートに接続されているデバイスの ID。
LLDP ネイバー IP アドレス	LLDP で検出されたネイバー デバイスの IP アドレス。
LLDP ネイバー IPv6 アドレス	CDP で検出されたネイバー デバイスの IPv6 アドレス。
LLDP ネイバー ポート	LLDP で検出された、電話機が接続されているネイバー デバイスのポート。
ポート情報	速度とデュプレックス モード。

コンソールのログ、コアダンプ、ステータスメッセージ、およびデバッグ表示用 Web ページ

デバイス ログ (Device Logs) という見出しで表示される、コンソール ログ、コアダンプ、ステータスメッセージ、およびデバッグ表示の各ハイパーリンクを参照することにより、電話機のモニタリングとトラブルシューティングが可能です。

- [コンソール ログ (Console Logs)] : 個々のログ ファイルへのハイパーリンクが含まれます。コンソール ログ ファイルには、電話機が受信したデバッグ メッセージとエラー メッセージが含まれます。
- [コア ダンプ (Core Dumps)] : 個々のダンプ ファイルへのハイパーリンクが含まれます。コア ダンプ ファイルには、電話のクラッシュ時のデータが含まれています。
- [ステータスメッセージ (Status Messages)] : 電話機に最後に電源が投入されてから電話機が生成したステータスメッセージの中で最近のものを最大 10 件表示します。この情報は、電話機の [ステータスメッセージ (Status Messages)] 画面にも表示されます。
- [デバッグの表示 (Debug Display)] : トラブルシューティングのサポートを依頼する際に、Cisco TAC に有用なデバッグ メッセージを提供します。

[ストリーミング統計 (Streaming Statistics)] Web ページ

Cisco IP 電話は、同時に最大で 5 つのデバイス間で情報をストリーミングできます。電話機は、コール中、または音声やデータの送受信サービスの作動中に、情報をストリーミングします。

電話機の Web ページにある [ストリーミングの統計 (Streaming Statistics)] 領域には、ストリーミングに関する情報が表示されます。

[ストリーミングの統計 (Streaming Statistics)] 領域を表示するには、電話機の Web ページにアクセスし、[ストリーミング (Stream)] ハイパーリンクをクリックします。

次の表に、[ストリーミングの統計 (Streaming Statistics)] 領域の項目を示します。

表 29: [ストリーミングの統計 (Streaming Statistics)] フィールド

項目	説明
Remote Address	ストリーミングの宛先の IP アドレスおよび UDP ポート。
Local Address	電話機の IP アドレスおよび UDP ポート。
Start Time	Cisco Unified Communications Manager が電話機にパケットの送信開始を要求した時間を示す内部タイムスタンプ。
ストリーミング ステータス (Stream Status)	ストリーミングがアクティブかどうかを示します。

項目	説明
ホスト名 (Host Name)	電話機の MAC アドレスに基づいて電話機に自動的に割り当てられる一意の固定された名前。
送信パケット (Sender Packets)	この接続の開始以降に電話機が送信した RTP データ パケットの総数。接続が受信専用モードに設定されている場合、値は 0 です。
送信オクテット (Sender Octets)	この接続の開始以降に電話機が RTP データ パケットで送信したペイロードオクテットの総数。接続が受信専用モードに設定されている場合、値は 0 です。
送信コーデック (Sender Codec)	送信ストリームに対応する音声符号化のタイプ。
送信した送信レポート (Sender Reports Sent) (注を参照)	RTCP 送信レポートが送信された回数。
送信した送信レポート時間 (Sender Report Time Sent) (注を参照)	最後に RTCP 送信レポートが送信された時間を示す内部タイム スタンプ。
受信喪失パケット (Rcvr Lost Packets)	この接続でのデータの受信を開始してから失われた RTP データ パケットの総数。予期されたパケット数から実際に受信されたパケット数を差し引いた値として定義されます。受信パケット数には、遅延または重複パケットも含まれます。接続が送信専用モードに設定されていた場合、値は 0 として表示されます。
平均ジッター (Avg Jitter)	RTP データ パケットの内部到着時間の平均偏差の推定値 (ミリ秒単位)。接続が送信専用モードに設定されていた場合、値は 0 として表示されます。
受信コーデック (Receiver Codec)	受信ストリームに使用された音声符号化のタイプ。
送信した受信レポート (Receiver Reports Sent) (注を参照)	RTCP 受信レポートが送信された回数。
送信した受信レポート時間 (Receiver Report Time Sent) (注を参照)	RTCP 受信レポートが送信された時間を示す内部タイム スタンプ。

項目	説明
受信パケット (Rcvr Packets)	この接続でのデータ受信開始以降に電話機が受信した RTP データパケットの総数。マルチキャスト コールの場合は、さまざまな送信元から受信したパケットが含まれます。接続が送信専用モードに設定されていた場合、値は 0 として表示されます。
受信オクテット (Rcvr Octets)	この接続でのデータ受信開始以降にデバイスが RTP データパケットで受信したペイロードオクテットの総数。マルチキャスト コールの場合は、さまざまな送信元から受信したパケットが含まれます。接続が送信専用モードに設定されていた場合、値は 0 として表示されます。
累積フレーム損失率 (Cumulative Conceal Ratio)	隠蔽フレームの総数を、音声ストリームの開始以降に受信された音声フレームの総数で割った値。
直近フレーム損失率 (Interval Conceal Ratio)	アクティブな音声の直前の 3 秒間の音声フレームに対する隠蔽フレームの比率。音声アクティビティ検出 (VAD) を使用している場合、3 秒間のアクティブな音声を蓄積するには、より長い間隔が必要になることがあります。
最大フレーム損失率 (Max Conceal Ratio)	音声ストリームの開始以降、最も高い間隔の損失率。
[フレーム損失発生秒数 (Conceal Seconds)]	音声ストリームの開始以降、隠蔽イベント (フレーム損失) があった秒数 ([深刻なフレーム損失発生秒数 (Severely Conceal Secs)]の値を含む)。
[深刻なフレーム損失発生秒数 (Severely Conceal Seconds)]	音声ストリームの開始以降、5% を超える隠蔽イベント (フレーム損失) があった秒数。
遅延 (注を参照)	ネットワーク遅延の推定値 (ミリ秒単位)。ラウンドトリップ遅延の実行中の平均値を表します。これは、RTCP 受信レポートブロックの受信時に測定されます。
最大ジッター (Max Jitter)	瞬時ジッターの最大値 (ミリ秒単位)。
送信サイズ (Sender Size)	送信ストリームの RTP パケットサイズ (ミリ秒単位)。

項目	説明
受信した送信レポート (Sender Reports Received) (注を参照)	RTCP 送信レポートが受信された回数。
受信した送信レポート時間 (Sender Report Time Received) (注を参照)	RTCP 送信レポートが最後に受信された時間。
受信サイズ (Receiver Size)	受信ストリームの RTP パケットサイズ (ミリ秒単位)。
受信破棄 (Receiver Discarded)	ネットワークから受信されたが、ジッターバッファから廃棄された RTP パケット。
受信した受信レポート (Receiver Reports Received) (注を参照)	RTCP 受信レポートが受信された回数。
受信した受信レポート時間 (Receiver Report Time Receiveds) (注を参照)	RTCP 受信レポートが最後に受信された時間。



(注) RTP 制御プロトコルが無効になっている場合、このフィールドのデータは生成されないため、0 が表示されます。

XML での電話からの情報要求

トラブルシューティングの目的で、電話機からの情報を要求できます。結果の情報は XML 形式です。表示される情報は次のとおりです。

- CallInfo は特定の回線のコールセッション情報です。
- LineInfo は電話機の回線設定情報です。
- ModeInfo は電話モードの情報です。

始める前に

情報を入手するために Web アクセスが有効になっている必要があります。

電話機がユーザに関連付けられている必要があります。

手順

ステップ 1 Call Info については、ブラウザに次の URL を入力します。**http://<phone ip address>/CGI/Java/CallInfo<x>**

値は次のとおりです。

- <phone ip address> は電話機の IP アドレスです。
- <x> は情報を取得する回線番号です。

コマンドは XML ドキュメントを返します。

ステップ 2 Line Info については、ブラウザに次の URL を入力します。**http://<phone ip address>/CGI/Java/LineInfo**

値は次のとおりです。

- <phone ip address> は電話機の IP アドレスです。

コマンドは XML ドキュメントを返します。

ステップ 3 Model Info については、ブラウザに次の URL を入力します。**http://<phone ip address>/CGI/Java/ModelInfo**

値は次のとおりです。

- <phone ip address> は電話機の IP アドレスです。

コマンドは XML ドキュメントを返します。

CallInfo の出力例

次の XML コードは、CallInfo のコマンドの出力例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
    <CallState>CONNECTED</CallState>
    <CallType>INBOUND</CallType>
    <CallingPartyName/>
    <CallingPartyDirNum>9700</CallingPartyDirNum>
    <CalledPartyName/>
    <CalledPartyDirNum>1030</CalledPartyDirNum>
    <HuntPilotName/>
    <CallReference>30303060</CallReference>
    <CallDuration>12835</CallDuration>
    <CallStatus>null</CallStatus>
  </CiscoIPPhoneCallInfo>
</CiscoIPPhoneCallLineInfo>
```

```

    <CallSecurity>UNAUTHENTICATED</CallSecurity>
    <CallPrecedence>ROUTINE</CallPrecedence>
    <FeatureList/>
  </CiscoIPPhoneCallInfo>
  <VisibleFeatureList>
    <Feature Position="1" Enabled="true" Label="End Call"/>
    <Feature Position="2" Enabled="true" Label="Show Detail"/>
  </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>

```

LineInfo の出力例

次の XML コードは LineInfo コマンドからの出力例を示します。

```

<CiscoIPPhoneLineInfo>
  <Prompt/>
  <Notify/>
  <Status>null</Status>
  <CiscoIPPhoneLines>
    <LineType>9</LineType>
    <lineDirNum>1028</lineDirNum>
    <MessageWaiting>NO</MessageWaiting>
    <RingerName>Chirp1</RingerName>
    <LineLabel/>
    <LineIconState>ONHOOK</LineIconState>
  </CiscoIPPhoneLines>
  <CiscoIPPhoneLines>
    <LineType>9</LineType>
    <lineDirNum>1029</lineDirNum>
    <MessageWaiting>NO</MessageWaiting> <RingerName>Chirp1</RingerName>
    <LineLabel/>
    <LineIconState>ONHOOK</LineIconState>
  </CiscoIPPhoneLines>
  <CiscoIPPhoneLines>
    <LineType>9</LineType>
    <lineDirNum>1030</lineDirNum>
    <MessageWaiting>NO</MessageWaiting>
    <RingerName>Chirp1</RingerName>
    <LineLabel/>
    <LineIconState>CONNECTED</LineIconState>
  </CiscoIPPhoneLines>
  <CiscoIPPhoneLines>
    <LineType>2</LineType>
    <lineDirNum>9700</lineDirNum>
    <MessageWaiting>NO</MessageWaiting>
    <LineLabel>SD9700</LineLabel>
    <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>

```

ModeInfo の出力例

次の XML コードは ModeInfo コマンドからの出力例を示します。

```

<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
  <PlaneTitle>Applications</PlaneTitle>
  <PlaneFieldCount>12</PlaneFieldCount>
  <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
  <PlaneSoftKeyMask>0</PlaneSoftKeyMask>

```



```
<Prompt></Prompt>
<Notify></Notify>
<Status></Status>
<CiscoIPPhoneFields>
  <FieldType>0</FieldType>
  <FieldAttr></FieldAttr>
  <fieldHelpIndex>0</fieldHelpIndex>
  <FieldName>Call History</FieldName>
  <FieldValue></FieldValue>
</CiscoIPPhoneFields>
<CiscoIPPhoneFields>
  <FieldType>0</FieldType>
  <FieldAttr></FieldAttr>
  <fieldHelpIndex>0</fieldHelpIndex>
  <FieldName>Preferences</FieldName>
  <FieldValue></FieldValue>
</CiscoIPPhoneFields>
  ...
</CiscoIPPhoneModeInfo>
```




第 12 章

電話機のトラブルシューティング

- 一般的なトラブルシューティング情報 (193 ページ)
- 起動時の問題 (196 ページ)
- 電話機のリセットの問題 (200 ページ)
- 電話機が LAN に接続できない (203 ページ)
- Cisco IP 電話のセキュリティの問題 (203 ページ)
- オーディオに関する問題 (205 ページ)
- コールに関する一般的な問題 (206 ページ)
- トラブルシューティング手順 (207 ページ)
- Cisco Unified Communications Manager からのデバッグ情報の制御 (212 ページ)
- トラブルシューティングに関する追加情報 (213 ページ)

一般的なトラブルシューティング情報

次の表に、Cisco IP 電話の一般的なトラブルシューティング情報を示します。

表 30: Cisco IP 電話のトラブルシューティング

サマリー	説明
長時間のブロードキャストストームのために、IP 電話がリセットされたり、コールの発信や応答ができなかったりすることがあります。	ボイス LAN 上の長時間 (数分間) にわたるレイヤ 2 ブロードキャストストームのために、IP 電話がリセットされたり、アクティブなコールが失われたり、コールの発信や応答ができなくなる可能性があります。ブロードキャストストームが終了するまで、電話機が起動しないことがあります。

サマリー	説明
ネットワーク接続の電話機からワークステーションへの移行	<p>ネットワーク接続を介して電話機に電力を供給している場合は、電話機のネットワーク接続を外して、そのケーブルをデスクトップコンピュータに接続する際に注意する必要があります。</p> <p>注意 コンピュータのネットワークカードには、ネットワーク接続を介して電力を供給できないため、接続を介して電力を供給すると、ネットワークカードが破損する場合があります。ネットワークカードを保護するために、電話機からケーブルを抜いた後、10 秒以上待機してから、そのケーブルをコンピュータに接続してください。この待機している間に、スイッチは電話機が回線に存在しなくなったことを認識し、ケーブルへの電力供給を停止することができます。</p>
電話機の設定変更	<p>デフォルトでは、ネットワーク接続に影響を与える可能性のある変更をユーザが加えないように、管理者パスワード設定はロックされています。管理者パスワード設定をロック解除した後、設定できるようになります。</p> <p>詳細については、電話機パスワードの適用 (47 ページ) を参照してください。</p> <p>(注) 管理者パスワードが共通の電話プロファイルで設定されていない場合、ユーザはネットワーク設定を変更できます。</p>

サマリー	説明
電話機と他のデバイスのコーデックの不一致	RxType 統計および TxType 統計に、この Cisco IP 電話 と他のデバイスとのやり取りに使用されているコーデックが表示されます。これらの統計情報の値は、一致している必要があります。コーデックが一致しない場合、相手側のデバイスがコーデック会話を処理できるかどうか、またはトランスコーダがサービスを処理するように設置されているかどうかを確認します。詳細については、 [コール統計 (Call Statistics)] ウィンドウの表示 (169 ページ) を参照してください。
電話機と別のデバイスの音声サンプルの不一致	RxSize 統計および TxSize 統計に、この Cisco IP 電話 と他のデバイスとのやり取りに使用される音声パケットのサイズが表示されます。これらの統計情報の値は、一致している必要があります。詳細については、 [コール統計 (Call Statistics)] ウィンドウの表示 (169 ページ) を参照してください。
ループバック状態	<p>ループバック状態は、次の条件を満たすと発生します。</p> <ul style="list-style-type: none"> • 電話機の [SWポート設定 (SW Port Configuration)] オプションが [10ハーフ (10 Half)] (10-Base-T/半二重) に設定されている。 • 電話機に外部電源から電力が供給されている。 • 電話機の電源が切れている (電源装置が接続されていない)。 <p>この場合、電話機のスイッチポートが無効になり、次のメッセージがスイッチのコンソールログに表示されます。</p> <p>HALF_DUX_COLLISION_EXCEED_THRESHOLD</p> <p>この問題を解決するには、スイッチからポートを再度有効にします。</p>

起動時の問題

下の関連項目で説明するとおり、ネットワークに電話機を設置し、Cisco Unified Communications Manager に追加すると、電話機は起動します。

電話機が正しく起動しない場合は、次の各セクションのトラブルシューティング情報を参照してください。

関連トピック

[電話機起動の確認](#) (63 ページ)

Cisco IP 電話が通常の起動プロセスを実行しない

問題

Cisco IP 電話をネットワーク ポートに接続したとき、関連項目で説明されている通常の起動プロセスを電話機が実行せず、電話画面に情報が表示されません。

原因

電話機が起動プロセスを実行しない場合、ケーブル不良、不正な接続、ネットワークの停止、電力の不足、または電話機が機能していないなどの原因が考えられます。

ソリューション

電話機が動作しているかどうかを確認するには、次の推奨事項に従って、考えられる他の問題を排除します。

- ネットワーク ポートが動作していることを確認します。
 - イーサネット ケーブルを、動作することがわかっているケーブルと交換します。
 - 別のポートから正常に動作している Cisco IP 電話を取り外してこのネットワーク ポートに接続し、このポートがアクティブかどうかを確認します。
 - 起動しない Cisco IP 電話を、正常であることがわかっている別のネットワーク ポートに接続します。
 - 起動しない Cisco IP 電話をスイッチのポートに直接接続して、オフィスのパッチパネル接続を回避します。
- 電話機に電力が供給されていることを確認します。
 - 外部電源を使用している場合は、電気のコンセントが機能していることを確認します。
 - インラインパワーを使用している場合は、代わりに外部電源を使用します。

- 外部電源を使用している場合は、動作することがわかっているユニットに切り替えます。
- 電話機が正常に起動しない場合は、バックアップ ソフトウェア イメージから電話機の電源を入れます。
- これらを試しても、電話機が正常に起動しない場合は、電話機を工場出荷時の状態にリセットします。
- これらの解決策を試みた後、最低 5 分経過しても Cisco IP 電話の電話画面に何も表示されない場合は、シスコのテクニカルサポートの担当者に連絡して、サポートを受けてください。

関連トピック

[電話機起動の確認](#) (63 ページ)

Cisco IP 電話が Cisco Unified Communications Manager に登録されない

電話機が起動プロセスの第1段階 (LED ボタンが点滅する) を完了しても、引き続き電話スクリーンにメッセージが表示される場合、電話機は正常に起動していません。電話機は、イーサネットネットワークに接続され、Cisco Unified Communications Manager サーバに登録されていない限り、正常に起動できません。

これ以外に、セキュリティ上の問題によって電話機が正常に起動しないこともあります。詳細については、[トラブルシューティング手順](#) (207 ページ) を参照してください。

電話機にエラー メッセージが表示される

問題

ステータス メッセージには、起動中のエラーが表示されます。

ソリューション

電話機が起動プロセスを繰り返している間は、問題の原因に関する情報を提供するステータス メッセージにアクセスできます。ステータスメッセージへのアクセスに関する説明、および発生する可能性のあるエラーとその説明、解決策の一覧については、「[ステータスメッセージ (Status Messages)] ウィンドウの表示」のセクションを参照してください。

関連トピック

[\[ステータス メッセージ \(Status Messages\) \] ウィンドウの表示](#) (156 ページ)

電話機が TFTP サーバまたは Cisco Unified Communications Manager に接続できない

問題

電話機と、TFTP サーバまたは Cisco Unified Communications Manager の間のネットワークがダウンしている場合は、電話機が正しく起動できません。

ソリューション

現在、ネットワークが作動していることを確認してください。

電話機が TFTP サーバに接続できない

問題

TFTP サーバの設定が正しくない可能性があります。

ソリューション

TFTP 設定を確認します。

関連トピック

[TFTP 設定の確認](#) (208 ページ)

電話機がサーバに接続できない

問題

IP アドレッシングおよびルーティングのフィールドが正しく設定されていない可能性があります。

ソリューション

電話機の IP アドレッシングおよびルーティングの設定を確認する必要があります。DHCP を使用している場合は、DHCP サーバがこれらの値を提供します。電話機にスタティック IP アドレスを割り当てている場合は、これらの値を手動で入力する必要があります。

関連トピック

[DHCP 設定の確認](#) (209 ページ)

電話機が DNS を使用して接続できない

問題

DNS 設定が誤っている可能性があります。

ソリューション

TFTP サーバまたは Cisco Unified Communications Manager へのアクセスに DNS を使用する場合は、DNS サーバを指定してあることを確認してください。

関連トピック

[DNS 設定の確認](#) (211 ページ)

Cisco Unified Communications Manager および TFTP サービスの未作動

問題

Cisco Unified Communications Manager または TFTP サービスが作動していない場合は、電話機が正常に起動できないことがあります。このような状況では、システム全体にわたる障害が発生しており、他の電話機やデバイスも正しく起動できない可能性があります。

ソリューション

Cisco Unified Communications Manager サービスが作動していない場合は、コールを確立するためにこのサービスに依存しているネットワーク上のすべてのデバイスが影響を受けます。TFTP サービスが作動していない場合は、多数のデバイスが正常に起動できません。詳細については、[サービスの開始](#) (211 ページ) を参照してください。

設定ファイルの破損

問題

この章に記載された他の解決策を試みても解決しない問題が特定の電話機で存続する場合は、設定ファイルが破損している可能性があります。

ソリューション

電話機の新しい設定ファイルを作成します。

関連トピック

[電話機の新しい設定ファイルの作成](#) (210 ページ)

Cisco Unified Communications Manager での電話機の登録

問題

電話機が Cisco Unified Communications Manager に登録されていません。

ソリューション

Cisco IP 電話は、電話機がサーバに追加されている場合、または自動登録が有効になっている場合にのみ、Cisco Unified Communications Manager サーバに登録できます。[電話機の追加方法](#)

(71 ページ) の情報と手順を見直して、電話機が Cisco Unified Communications Manager データベースに追加されていることを確認します。

電話機が Cisco Unified Communications Manager データベースに登録されていることを確認するには、Cisco Unified Communications Manager Administration から [デバイス (Device)] > [検索 (Find)] を選択します。MAC アドレスに基づいて電話機を検索するには、[Find] をクリックします。MAC アドレスの確認方法については、[電話機の MAC アドレスの決定 \(71 ページ\)](#) を参照してください。

電話機がすでに Cisco Unified Communications Manager データベースに登録されている場合は、設定ファイルが損傷している可能性があります。解決策については、[設定ファイルの破損 \(199 ページ\)](#) を参照してください。

Cisco IP 電話が IP アドレスを取得できない

問題

電話機が起動時に IP アドレスを取得できない場合は、その電話機が DHCP サーバと同じネットワークまたは VLAN 上に存在しないか、または電話機が接続されている先のスイッチポートが無効になっている可能性があります。

ソリューション

電話機が接続されている先のネットワークまたは VLAN が DHCP サーバにアクセスできること、およびスイッチポートが有効になっていることを確認します。

電話機のリセットの問題

電話機が通話中やアイドル状態のときにリセットされるという報告をユーザから受けた場合は、原因を調査する必要があります。ネットワーク接続と Cisco Unified Communications Manager の接続が安定している場合は、電話機がリセットされることはありません。

一般的に、電話機がリセットされるのは、ネットワークまたは Cisco Unified Communications Manager への接続に問題がある場合です。

断続的なネットワークの停止によって電話機がリセットされる

問題

ネットワークで断続的な停止が発生している可能性があります。

ソリューション

断続的なネットワークの停止は、データトラフィックと音声トラフィックにそれぞれ異なる影響を与えます。ネットワークで断続的な停止が、検出されずに発生している可能性があります。この場合、データトラフィックでは喪失パケットを再送信し、パケットが受信および送信

されたことを確認できます。ただし、音声トラフィックでは、喪失パケットを取り戻すことはできません。電話機は、失われたネットワーク接続を再送信するのではなく、ネットワークをリセットして再接続しようとしています。音声ネットワークでの既知の問題については、システム管理者にお問い合わせください。

DHCP の設定エラーによって電話機がリセットされる

問題

DHCP 設定が正しくない可能性があります。

ソリューション

電話機が DHCP を使用するように正しく設定されていることを確認します。DHCP サーバが正しくセットアップされていることを確認します。DHCP リース期間を確認します。リース期間を 8 日に設定することを推奨します。

関連トピック

[DHCP 設定の確認](#) (209 ページ)

誤ったスタティック IP アドレスによる電話機のリセット

問題

電話機に割り当てられたスタティック IP アドレスが正しくない可能性があります。

ソリューション

電話機にスタティック IP アドレスが割り当てられている場合は、正しい設定値が入力されていることを確認します。

ネットワーク使用量が多いときの電話機のリセット

問題

ネットワーク使用量が多いときに電話機がリセットされるように思われる場合は、ボイス VLAN が設定されていない可能性があります。

ソリューション

電話機を個別の補助 VLAN に分離することで、音声トラフィックの品質が向上します。

意図的なリセットによる電話機のリセット

問題

Cisco Unified Communications Manager へのアクセス権を持つ管理者が 1 人だけではない場合は、他の管理者が意図的に電話機をリセットしていないかどうかを確認する必要があります。

ソリューション

Cisco IP 電話が Cisco Unified Communications Manager からリセット コマンドを受信したかどうかを確認するには、電話機の [設定 (Settings)] を押し、[管理者設定 (Admin Settings)] > [ステータス (Status)] > [ネットワーク統計 (Network Statistics)] の順に選択します。

- [リスタートの原因 (Restart Cause)] フィールドに [Reset-Reset] が表示される場合、電話機は Cisco Unified Communications Manager の管理ページからリセット/リセットを受信しています。
- [Restart Cause] フィールドに [Reset-Restart] が表示される場合、電話機は Cisco Unified Communications Manager Administration からリセット/リスタートを受信したために切断されました。

DNS エラーまたは他の接続の問題による電話機のリセット

問題

電話機のリセットが続いており、DNS またはその他の接続の問題が疑われます。

ソリューション

電話機が引き続きリセットされる場合は、[DNS または接続の問題の特定 \(209 ページ\)](#) の手順に従って、DNS またはその他の接続エラーを排除します。

電話機に電源が入らない

問題

電話機に電源が入っているように見えません。

ソリューション

電話機が再起動するのは、ほとんどの場合、外部電源から電源が供給されていたが、その接続が失われて PoE に切り替わったときです。同様に、PoE を使用して電力が供給されている電話機が外部電源に接続された場合にも、電話機が再起動することがあります。

電話機が LAN に接続できない

問題

LAN への物理的な接続が切断されている可能性があります。

ソリューション

Cisco IP 電話が接続されているイーサネット接続が動作していることを確認します。たとえば、電話機が接続されている先の特定のポートまたはスイッチがダウンしていないか、またスイッチが再起動中でないかどうかを確認します。また、ケーブルの切断が存在しないことも確認してください。

Cisco IP 電話のセキュリティの問題

ここでは、Cisco IP 電話のセキュリティ機能のトラブルシューティングに関する情報を示します。これらの問題の任意の解決方法、およびセキュリティに関するトラブルシューティングの詳細情報については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

CTL ファイルの問題

ここでは、CTL ファイルの問題のトラブルシューティングについて説明します。

認証エラー。電話機が CTL ファイルを認証できない

問題

デバイスの認証エラーが発生しました。

原因

CTL ファイルに Cisco Unified Communications Manager の証明書がないか、証明書が不正です。

ソリューション

適切な証明書をインストールします。

電話機が CTL ファイルを認証できない

問題

電話機が CTL ファイルを認証できない。

CTL ファイルは認証されるが、他の設定ファイルが認証されない**原因**

電話機の CTL ファイル内に、更新された CTL ファイルに署名したセキュリティ トークンがありません。

ソリューション

CTL ファイル内のセキュリティ トークンを変更し、新しいファイルを電話機にインストールします。

CTL ファイルは認証されるが、他の設定ファイルが認証されない**問題**

電話機が CTL ファイル以外の設定ファイルを認証できません。

原因

不正な TFTP レコードが存在するか、電話機の信頼リストの対応する証明書によって設定ファイルが署名されていない可能性があります。

ソリューション

TFTP レコード、および信頼リストの証明書を確認します。

ITL ファイルは認証されるが、他の設定ファイルが認証されない**問題**

電話機が ITL ファイル以外の設定ファイルを認証できない。

原因

設定ファイルは、電話機の信頼リストの対応する証明書によって署名されていない可能性があります。

ソリューション

正しい証明書を使用してコンフィギュレーション ファイルに再署名します。

TFTP 認証が失敗する**問題**

電話機が TFTP 認証の失敗を報告する。

原因

CTL ファイルに電話機の TFTP アドレスがありません。

新しい TFTP レコードを含む新しい CTL ファイルを作成した場合は、電話機上の既存の CTL ファイルには新しい TFTP サーバ用のレコードが含まれない可能性があります。

ソリューション

電話機の CTL ファイルの TFTP アドレス設定を確認します。

電話機が登録されない

問題

電話機が Cisco Unified Communications Manager に登録されない。

原因

CTL ファイルに Cisco Unified Communications Manager サーバ用の正しい情報が含まれていません。

ソリューション

CTL ファイル内の Cisco Unified Communications Manager サーバの情報を変更します。

署名付き設定ファイルが要求されない

問題

電話機が、署名付き設定ファイルを要求しない。

原因

CTL ファイルに証明書付きの TFTP エントリが含まれていません。

ソリューション

証明書付きの TFTP エントリを CTL ファイルに設定します。

オーディオに関する問題

ここでは、オーディオに関する問題を解決する方法について説明します。

通話路がない

問題

コール中の 1 人以上の通話者に音声聞こえません。

ソリューション

少なくとも 1 人の通話者がオーディオを受信できない場合、電話機間の IP 接続が確立されていません。ルータとスイッチの設定をチェックし、IP 接続が正しく設定されていることを確認します。

音声の途切れ

問題

ユーザからコールで音声途切れという苦情があります。

原因

ジッターの設定に不一致が存在する可能性があります。

ソリューション

AvgJtr 統計情報と MaxJtr 統計情報を確認します。これらの統計に大きな差がある場合は、ネットワークのジッターに問題があるか、または周期的にネットワークアクティビティが高くなっている可能性があります。

デジチェーンモードの 1 台の電話機が機能しない

問題

デジチェーンモードでは、会議電話機のいずれかが機能しません。

ソリューション

スマートアダプタに接続されているケーブルが正しいものかどうかを確認します。2 つの太いケーブルで、電話機をスマートアダプタに接続します。薄型のケーブルで、スマートアダプタを電源アダプタに接続します。

関連トピック

[デジチェーンモード \(36 ページ\)](#)

[デジチェーンモードでの会議電話の設置 \(43 ページ\)](#)

コールに関する一般的な問題

次の各項は、電話のコールに関する一般的な問題のトラブルシューティングに役立ちます。

コールを確立できない

問題

ユーザからコールを発信できないことについての苦情があります。

原因

DHCP IP アドレスが割り当てられていない電話機は、Cisco Unified Communications Manager に登録できません。LCD 画面付きの電話機には、「IP を設定中 (Configuring IP)」または「登録 (Registering)」というメッセージが表示されます。LCD 画面のない電話機では、ユーザがコールを発信しようとする、ハンドセットで (ダイヤルトーンの代わりに) リオーダー音が再生されます。

ソリューション

1. 次の点を確認してください。
 1. イーサネット ケーブルが接続されている。
 2. Cisco CallManager サービスが Cisco Unified Communications Manager サーバで作動している。
 3. 両方の電話機が同じ Cisco Unified Communications Manager に登録されている。
2. 両方の電話機で、オーディオサーバ デバッグとキャプチャ ログが有効になっています。必要な場合は、Java デバッグを有効にしてください。

電話機が DTMF デジットを認識しないか、または数字が遅い

問題

ユーザから、キーパッドを使用しているときに数字が消えるか、または遅いという苦情があります。

原因

キーを速く押しすぎると、数字が消えたり、遅くなったりすることがあります。

ソリューション

キーをあまり速く押さないでください。

トラブルシューティング手順

これらの手順を使用すると、問題を識別したり、解決したりすることができます。

Cisco Unified Communications Manager から電話機の問題レポートを作成する

Cisco Unified Communications Manager から電話機の問題レポートを生成することができます。この操作によって、Problem Report Tool (PRT) のソフトキーが電話機で生成するものと同じ情報が得られます。

問題レポートには、電話機とヘッドセットに関する情報が含まれています。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[デバイス (Device)] > [電話 (Phone)] を選択します。
 - ステップ 2** [検索 (Search)] をクリックして、1 つまたは複数の Cisco IP 電話を選択します。
 - ステップ 3** 選択した Cisco IP 電話 上で使用されているヘッドセットの PRT ログを収集するには、[選択対象の PRT を生成する (Generate PRT for Selected)] をクリックします。
-

TFTP 設定の確認

手順

-
- ステップ 1** [TFTP サーバ 1 (TFTP Server 1)] フィールドを確認します。
電話機にスタティック IP アドレスを割り当てている場合は、手動で [TFTP サーバ 1 (TFTP Server 1)] オプションに設定値を入力する必要があります。
DHCP を使用している場合は、電話機は TFTP サーバのアドレスを DHCP サーバから取得します。オプション 150 で、IP アドレスが設定されていることを確認します。
 - ステップ 2** また、電話機が代替 TFTP サーバを使用できるように設定することもできます。このような設定は、電話機の場所を最近移動した場合などに特に役立ちます。
 - ステップ 3** ローカル DHCP が正しい TFTP アドレスを提供しない場合は、電話機で代替 TFTP サーバが使用できるようにします。
これは多くの場合、VPN シナリオで必要です。
-

DNS または接続の問題の特定

手順

- ステップ 1 [Reset Settings] メニューを使用して、電話機をデフォルト値にリセットします。
- ステップ 2 次の操作を実行して、DHCP および IP の設定を変更します。
 - a) DHCP を無効にします。
 - b) 電話機にスタティック IP 値を割り当てます。機能している他の電話機で使用しているものと同じデフォルトルータの設定を使用します。
 - c) TFTP サーバを割り当てます。機能している他の電話機で使用しているものと同じ TFTP サーバを使用します。
- ステップ 3 Cisco Unified Communications Manager サーバで、正しい IP アドレスにマッピングされている正しい Cisco Unified Communications Manager サーバ名がローカル ホスト ファイルに指定されていることを確認します。
- ステップ 4 Cisco Unified Communications Manager から [システム (System)] > [サーバ (Server)] の順に選択し、サーバが DNS 名ではなく IP アドレスで参照されていることを確認します。
- ステップ 5 Cisco Unified Communications Manager から、[デバイス (Device)] > [電話 (Phone)] の順に選択します。この電話機を検索するには、[Find] をクリックします。この Cisco IP 電話に正しい MAC アドレスが割り当てられていることを確認します。
- ステップ 6 電話機の電源をオフ/オンにします。

関連トピック

[電話機の MAC アドレスの決定](#) (71 ページ)

[会議電話の再起動またはリセット](#) (215 ページ)

DHCP 設定の確認

手順

- ステップ 1 電話機で、設定ボタンを押します。
- ステップ 2 [管理者設定 (Admin Settings)] > [イーサネットのセットアップ (Ethernet Setup)] > [IPv4 のセットアップ (IPv4 Setup)] を選択します。
- ステップ 3 [DHCPサーバ (DHCP server)] フィールドを確認します。

電話機に静的 IP アドレスを割り当てている場合は、[DHCP サーバ (DHCP Server)] オプションに値を入力する必要はありません。ただし、DHCPサーバを使用している場合は、このオプションに値が指定されている必要があります。値が見つからない場合は、IPルーティングおよび VLAN の設定を確認してください。『*Troubleshooting Switch Port and Interface Problems*』を参照してください。このマニュアルは、次の URL から入手できます。

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

ステップ 4 [IPアドレス]、[サブネットマスク]、および[デフォルトルータ (Default Router)] フィールドを確認します。

電話機に静的 IP アドレスを割り当てる場合は、これらのオプションの設定を手動で入力する必要があります。

ステップ 5 DHCP を使用している場合は、DHCP サーバによって配布された IP アドレスを確認してください。

『*Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*』を参照してください。このマニュアルは、次の URL から入手できます。

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

電話機の新しい設定ファイルの作成

Cisco Unified Communications Manager データベースから電話機を削除すると、設定ファイルが Cisco Unified Communications Manager TFTP サーバから削除されます。電話機の電話番号（1 つまたは複数）は、Cisco Unified Communications Manager データベースに残ります。これらは、「未定義の DN」と呼ばれ、他のデバイスで使用できます。未定義の DN を他のデバイスで使わない場合は、Cisco Unified Communications Manager データベースから削除します。ルートプランレポートを使用すると、未定義の DN を表示および削除できます。詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

電話ボタンテンプレートのボタンを変更したり、異なる電話ボタンテンプレートを電話機に割り当てたりすると、電話機から電話番号にアクセスできなくなることがあります。Cisco Unified Communications Manager データベースでは、引き続き電話番号が電話機に割り当てられていますが、コールに応答するためのボタンがないためです。これらの電話番号は、電話機から消去し、必要に応じて削除してください。

手順

ステップ 1 Cisco Unified Communications Manager で、[デバイス (Device)] > [電話 (Phone)] を選択し、[検索 (Find)] をクリックして、問題が発生している電話機を特定します。

ステップ 2 [Delete] を選択して、電話機を Cisco Unified Communications Manager データベースから削除します。

(注) Cisco Unified Communications Manager データベースから電話機を削除すると、設定ファイルが Cisco Unified Communications Manager TFTP サーバから削除されます。電話機の電話番号（1 つまたは複数）は、Cisco Unified Communications Manager データベースに残ります。これらは、「未定義の DN」と呼ばれ、他のデバイスで使用できます。未定義の DN を他のデバイスで使わない場合は、Cisco Unified Communications Manager データベースから削除します。ルートプランレポートを使用すると、未定義の DN を表示および削除できます。

- ステップ3 電話機を Cisco Unified Communications Manager データベースに追加し直します。
- ステップ4 電話機の電源をオフ/オンにします。

関連トピック

[電話機の追加方法](#) (71 ページ)

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

DNS 設定の確認

手順

- ステップ1 電話機で、設定ボタンを押します。
- ステップ2 [管理者設定 (Admin Settings)] > [イーサネットのセットアップ (Ethernet Setup)] > [IPv4のセットアップ (IPv4 Setup)] を選択します。
- ステップ3 [DNSサーバ1 (DNS Server 1)] フィールドが正しく設定されていることを確認します。
- ステップ4 また、DNS サーバに、TFTP サーバと Cisco Unified Communications Manager システムの CNAME エントリが作成されていることを確認する必要があります。

また、DNS が逆ルックアップを実行するように設定されていることも確認する必要があります。

サービスの開始

サービスを開始または停止するには、事前にサービスをアクティブにする必要があります。

手順

- ステップ1 Cisco Unified Communications Manager の管理ページで、[ナビゲーション (Navigation)] ドロップダウン リストから [Cisco Unified サービスアビリティ (Cisco Unified Serviceability)] を選択し、[移動 (Go)] をクリックします。
- ステップ2 [ツール (Tool)] > > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択します。
- ステップ3 [サーバ (Server)] ドロップダウンリストで、プライマリの Cisco Unified Communications Manager サーバを選択します。
ウィンドウに、選択したサーバのサービス名、サービスのステータス、およびサービスを停止または開始するためのサービス コントロール パネルが表示されます。
- ステップ4 サービスが停止している場合は、対応するオプションボタンをクリックし、[Start] ボタンをクリックします。

[[サービスのステータス (Service Status)] 記号が四角形から矢印に変わります。

Cisco Unified Communications Manager からのデバッグ情報の制御

お客様が解決できない電話機の問題が発生した場合は、Cisco TAC でサポートを受けることができます。電話機のデバッグをオンにして問題を再現し、デバッグをオフにして、分析のために TAC にログを送信する必要があります。

デバッグでは詳細情報を取り込むため、通信量によって電話が遅くなり応答が遅れる可能性があります。ログを検出したら、電話の動作を確保するためにデバッグをオフにする必要があります。

デバッグ情報には、状況の重大度を表す1桁のコードが含まれることがあります。状況は次のようにランクが付けられています。

- 0 - 緊急事態
- 1 - アラート
- 2 - クリティカル
- 3 - エラー
- 4 - 警告
- 5 - 通知
- 6 - 情報
- 7 - デバッグ

詳細情報およびサポートについては、Cisco TAC にお問い合わせください。

手順

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] で次のウィンドウのいずれかを選択します。

- [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通の電話プロファイル (Common Phone Profile)]
- [システム (System)] > [エンタープライズ電話の設定 (Enterprise Phone Configuration)]
- [デバイス (Device)] > [電話 (Phone)]

ステップ 2 次のパラメータを設定します。

- ログのプロファイル-値：プリセット（デフォルト）、デフォルト、テレフォニー、SIP、UI、ネットワーク、メディア、アップグレード、アクセサリ、セキュリティ、EnergyWise、MobileRemoteAccess
 - リモート ログ - 値：無効（デフォルト）、有効
 - IPv6 ログ サーバまたはログ サーバ - IP アドレス（IPv4 アドレスまたは IPv6 アドレス）
- (注) ログサーバに到達できない場合、電話機はデバッグメッセージの送信を停止します。
- IPv4 ログ サーバのアドレスの形式は、**address:<port>@@base=<0-7>;pfs=<0-1>**
 - IPv6 ログ サーバのアドレスの形式は、**[address]:<port>@@base=<0-7>;pfs=<0-1>**
 - それぞれの説明は次のとおりです。
 - IPv4 アドレスはドット (.) で区切ります。
 - IPv6 アドレスはコロン (:) で区切ります。

トラブルシューティングに関する追加情報

電話機のトラブルシューティングに関する詳細については、次に示すシスコの Web サイトにアクセスして、該当の電話機モデルに移動してください。

<https://www.cisco.com/cisco/web/psa/troubleshoot.html>



第 13 章

メンテナンス

- [会議電話の再起動またはリセット \(215 ページ\)](#)
- [音声品質のモニタリング \(217 ページ\)](#)
- [Cisco IP 電話のクリーニング \(218 ページ\)](#)

会議電話の再起動またはリセット

電話機でエラーが発生した場合は、回復する電話の基本的なリセットを実行します。構成およびセキュリティ設定を工場出荷時デフォルト設定に戻すこともできます。

会議電話の再起動

電話機を再起動すると、電話機のフラッシュメモリにコミットされていないすべてのユーザーセットアップおよびネットワークセットアップに対する変更が失われます。

手順

[設定 (Settings)] > [管理者設定 (Admin Settings)] > [設定のリセット (Reset settings)] > [デバイスのリセット (Reset device)] を押します。

関連トピック

[電話機からのテキストとメニューの入力 \(47 ページ\)](#)

電話メニューからの会議電話の設定のリセット

手順

ステップ 1 [設定 (Settings)] を押します。

ステップ 2 [管理者設定 (Admin Settings)] > [設定のリセット (Reset Settings)] を選択します。

キーパッドから会議電話を工場出荷時の初期状態にリセットする

ステップ 3 リセットのタイプを選択します。

- [すべて (All)] : 工場出荷時の設定に戻します。
- [デバイスのリセット (Reset device)] : デバイスをリセットします。既存の設定は変更されません。
- [ネットワーク (Network)] : ネットワーク構成をデフォルトの設定にリセットします。
- [サービス モード (Service mode)] : 現在のサービス モードをクリアし、VPN を非アクティブ化して、電話機を再起動します。
- [セキュリティ (Security)] : セキュリティ構成をデフォルトの設定にリセットします。このオプションを選択すると、CTL ファイルが削除されます。

ステップ 4 [リセット (Reset)]または[キャンセル (Cancel)]をクリックします。

関連トピック

[電話機からのテキストとメニューの入力 \(47 ページ\)](#)

キーパッドから会議電話を工場出荷時の初期状態にリセットする

キーパッドから電話機をリセットすると、電話機は工場出荷時の設定に戻ります。

手順

ステップ 1 電話機のプラグを抜きます。

- PoE を使用している場合、LAN ケーブルを抜きます。
- 電源アダプタを使用している場合は、アダプタを取り外します。

ステップ 2 5 秒間待機します。

ステップ 3 [#] キーを押したままにして電話機を再接続します。

ステップ 4 電話機が起動する、LED ストリップが点灯します。LED 削除がオンになるとすぐに、続けて **123456789*0#**を押します。

これらのボタンを押すと、電話機を工場出荷時の状態にリセットするプロセスが実行されます。

ボタンを押す順番を間違えた場合、通常どおりに電話機が電源オンになります。

注意 工場出荷時の状態にリセットするプロセスが完了して、メイン画面が表示されるまで、電話機の電源を切らないでください。

関連トピック

[電話機からのテキストとメニューの入力 \(47 ページ\)](#)

音声品質のモニタリング

ネットワーク内で送受信されるコールの音声品質を測定するために、Cisco IP 電話では隠蔽イベントに基づく次の統計メトリックを使用します。DSP は、音声パケット ストリーム内でフレーム損失の部分のマスキングのために、隠蔽フレームを再生します。

- フレーム損失率のメトリック：音声フレームの総数に対する秘匿フレームの比率を示します。直近フレーム損失率は、3 秒ごとに計算されます。
- フレーム損失発生秒数のメトリック：損失フレームが原因で DSP が秘匿フレームを処理する場合の処理秒数を示します。深刻な「フレーム損失発生秒数」は、DSP が 5% を超える隠蔽フレームを処理する場合の秒数です。



(注) フレーム損失率とフレーム損失発生秒数は、フレーム損失に基づいた主要な測定値です。フレーム損失率がゼロの場合は、IP ネットワークが損失なく時間どおりにフレームやパケットを配信していることを示しています。

Cisco IP 電話 から音声品質メトリックにアクセスするには、[コール統計 (Call Statistics)] 画面を使用するか、または、リモートで [ストリーミング統計 (Streaming Statistics)] 画面を使用します。

音声品質のトラブルシューティングのヒント

メトリックに大幅な変化が継続的に見られた場合は、次の表の一般的なトラブルシューティング情報を使用してください。

表 31: 音声品質メトリックの変化

メトリックの変化	条件
フレーム損失率とフレーム損失発生秒数が大幅に増加した	パケット損失または高いジッターによるネットワーク障害。

メトリックの変化	条件
フレーム損失率はほとんどゼロであるが、音声品質が悪い。	<ul style="list-style-type: none"> 音声チャンネルのノイズや歪み（エコーレベルやオーディオレベルなど）。 複数のエンコード/デコードが使用されているタンデムコール（セルラーネットワークや電話カードネットワークへのコールなど）。 スピーカーフォン、ハンドフリー携帯電話、またはワイヤレスヘッドセットなどから発生する音響問題。 <p>送信パケット（TxCnt）と受信パケット（RxCnt）のカウンタをチェックし、音声パケットが流れていることを確認します。</p>
MOS LQK スコアが著しく減少	<p>パケット損失または高いジッターレベルによるネットワーク障害。</p> <ul style="list-style-type: none"> 平均 MOS LQK の減少は、広範囲の画一的な障害を示している可能性があります。 個別の MOS LQK の減少は、集中的な障害を示している可能性があります。 <p>フレーム損失率とフレーム損失発生秒数を照合して、パケット損失やジッターがないか確認してください。</p>
MOS LQK スコアが著しく増加	<ul style="list-style-type: none"> 電話機が適切なコーデック（RxType および TxType）を使用しているかどうかを確認してください。 MOS LQK のバージョンがファームウェアアップグレード以降に変更されたかどうかを確認してください。



(注) 音声品質メトリックでは、ノイズや歪みは考慮されません。フレーム損失だけが考慮されません。

Cisco IP 電話のクリーニング

Cisco IP 電話をクリーニングする際は、必ず乾いた柔らかい布を使用して電話機と画面を軽く拭いてください。液体や粉末を電話機に直接付けないでください。すべての非耐候性の電子機器と同様に、液体や粉末はコンポーネントを損傷し、障害を引き起こすことがあります。

電話機がスリープモードになっているときは、画面は空白で、選択ボタンは点灯していません。電話機がこの状態のときは画面をクリーニングできます。ただし、クリーニングを終了するまで電話機のスリープ状態が続くとわかっている場合に限りです。



第 14 章

各言語ユーザのサポート

- [Unified Communications Manager Endpoints Locale Installer](#) (221 ページ)
- [国際コールのロギングのサポート](#) (221 ページ)
- [言語の制限](#) (222 ページ)

Unified Communications Manager Endpoints Locale Installer

デフォルトでは、Cisco IP 電話は英語（米国）のロケール用に設定されます。それ以外のロケールで Cisco IP 電話を使用するには、そのロケール固有のバージョンの Unified Communications Manager Endpoints Locale Installer を、クラスタ内の各 Cisco Unified Communications Manager サーバにインストールする必要があります。Locale Installer は電話機のユーザインターフェイス用の最新版の翻訳テキストおよび国別の電話トーンをシステムにインストールし、Cisco IP 電話に使用できるようにします。

特定のリリースに必要なロケールインストーラにアクセスするには、[ソフトウェアのダウンロードページ](#)にアクセスし、お使いの電話機モデルに移動して、Unified Communications Manager エンドポイント ロケール インストーラのリンクを選択します。

手順の詳細については、特定のリリースのマニュアルを参照してください。Cisco Unified Communications Manager



(注) 最新の Locale Installer がすぐに利用できるとは限らないため、Web サイトの更新を継続的に確認してください。

関連トピック

[Cisco Unified Communications Manager マニュアル](#) (14 ページ)

国際コールのロギングのサポート

ご使用の電話システムで国際コールのロギング（発信側の正規化）が設定されている場合、通話履歴、リダイヤル、コールディレクトリの各エントリに通話場所の国際エスケープコード

を表す「+」記号が表示されることがあります。電話システムの設定によっては、「+」記号ではなく正しい国際ダイヤルコードが表示される場合があります。国際ダイヤルコードが表示されない場合は、必要に応じて、「+」記号を通話場所の国際エスケープコードに手動で置き換えて番号を編集した後にダイヤルします。また、コールログやディレクトリ エントリには受信コールの完全な国際電話番号が表示され、電話機のディスプレイには国際コード（国番号）が省略された国内用の短い番号が表示される場合もあります。

言語の制限

次のアジア ロケールについては、ローカライズされた Keyboard Alphanumeric Text Entry (KATE) のサポートはありません。

- 中国語（中国）
- 中国語（香港）
- 中国語（台湾）
- 日本語（日本）
- 韓国語（韓国）

その代わりに、デフォルトとして英語（米国）の KATE がユーザに表示されます。

たとえば、電話画面には韓国語でテキストが表示されるとしてもキーパッドの **2** キーには、**a b c 2 A B C** と表示されます。