Cisco DX シリーズ管理ガイド、リリース 10.2 (5)

最終更新：2025 年 10 月 29 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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている式、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。 これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。 この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。 これらの制限は、住宅地で使用したときに、有害な干渉を防止する適切な保護を規定したものです。 この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン/オフによって判断できます。

- 受信アンテナの向きを変えるか、場所を移動します。
- 機器と受信装置の距離を広げる。
- 受信装置が接続されている回路とは別の回路のコンセントに機器を接続する。
- 販売業者またはラジオやテレビに詳しい技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

　定型　このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。　定型　マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。 最新版については、現在のオンライン バージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。 各オフィスの住所と電話番号は、当社の Web サイト www.cisco.com/jp/go/offices をご覧ください。

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)

© 2015–2020 Cisco Systems, Inc. All rights reserved.

【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。

Bluetooth のワードマークおよびロゴは Bluetooth SIG, Inc. が所有する登録商標であり、Cisco Systems, Inc. によるこれらのマークの使用はライセンスに基づいています。

© 2015–2020 Cisco Systems, Inc. All rights reserved.

【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。

Google、Google Play、Android、およびその他の特定のマークは、Google Inc. の商標です。

© 2015–2020 Cisco Systems, Inc. All rights reserved.

【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。

HDMI、HDMI High-Definition Multimedia Interface、および HDMI ロゴは、米国およびその他の国における HDMI Licensing LLC の商標または登録商標です。

© 2015–2020 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xix

概要 xix

ガイドの表記法 xix

関連資料 xx

用語の違い xxii

マニュアル、サポート、およびセキュリティ ガイドライン xxii

シスコ製品のセキュリティの概要 xxii

第 1 章

新規および変更情報 1

リリース 10.2(5) の新機能および変更された機能 1

第 2 章

技術仕様 3

物理環境および動作環境に関する仕様 3

ネットワーク ポートとコンピュータ ポートのピン割り当て 5

ネットワーク ポート コネクタのピン割り当て 5

コンピュータポートコネクタのピン配置 5

Cisco DX シリーズデバイスで使用されるポート 6

ネットワーク プロトコル 7

電力要件 11

電力ガイドライン 12

電力削減 13

省電力モード 13

EnergyWise モード 13

LLDP での電力ネゴシエーション 14

電力に関する追加情報 15
外部デバイス 15
USB ポートと USB シリアルコンソールのデータ情報 16
USB コンソールを使用する 17
ネットワーク混雑時の動作 17

第 3 章 デバイスの説明 19
Cisco DX70 ハードウェア 19
Cisco DX70 ケーブルの取り付け 20
Cisco DX80 ハードウェア 21
Cisco DX80 ケーブルの取り付け 22
Cisco DX650 ハードウェア 23
Cisco DX650 ケーブルの取り付け 24
無線ハードウェアなし 24

第 4 章 Wi-Fi ネットワークの設定 25
ネットワーク要件 25
ワイヤレス LAN 26
Wi-Fi ネットワーク コンポーネント 27
AP、チャネル、規制区域の関係 27
AP の相互作用 27
アクセス ポイントとのアソシエーション 28
無線ネットワークにおける QoS 28
フレキシブル DSCP の設定 30
Cisco Unified Communications Manager の連携 31
WLAN 通信の 802.11 規格 31
ワールド モード（802.11d） 33
無線変調技術 33
無線周波数範囲 34
WLAN 通信のセキュリティ 34
認証方法 34

認証キー管理 35
暗号化方式 35
AP 認証および暗号化のオプション 36
WLAN とローミング 37

第 5 章 展開 39
設定ファイル 39
MAC アドレスを決定する 40
Cisco Unified Communications Manager デバイスの追加方法 40
自動登録 41
自動登録と TAPS 41
Cisco Unified Communications Manager でデバイスを追加する 42
一括管理ツールの電話テンプレートを使用してデバイスを追加する 43
セルフプロビジョニング 43
セルフプロビジョニングを有効にする 44
Cisco Unified Communications Manager のユーザーの追加 44
Cisco Unified Communications Manager へのユーザの直接追加 44
外部 LDAP ディレクトリからユーザを追加する 45
デバイスモデルを確認する 45
回線設定を構成する 46
ユーザーとデバイスの関連付け 47
Survivable Remote Site Telephony 48

第 6 章 インストール 49
Cisco DX シリーズデバイスのインストール 49
無線 LAN の設定 51
Cisco Unified Communications Manager 管理でのワイヤレス LAN の設定 51
ワイヤレス LAN プロファイルのプロビジョニング 51
ワイヤレス LAN プロファイルグループのプロビジョニング 52
ネットワーク設定の構成 52
IPv4 の設定 52

IPv4 を更新する 53
IPv6 の設定 53
IPv6 を更新する 54
イーサネット Web プロキシを構成する 54
管理 VLAN を設定する 54
SW ポート速度の設定 54
PC ポート速度の設定 55
Wi-Fi ネットワークに接続する 55
非表示の Wi-Fi ネットワークに接続する 55
Wi-Fi Web プロキシを構成する 56
Wi-Fi IP 設定を構成する 56
Wi-Fi 周波数帯域を設定する 57
Expressway 経由でのモバイルおよび Remote Access 57
Expressway のユーザ資格情報の永続性を有効にする 58
Expressway 経由でデバイスをモバイルおよび Remote Access に変換する 58
Expressway デバイスを VPN に変換する 59
オフプレミスデバイスをオンプレミスに変換する 59
問題報告ツールサーバを Expressway HTTP 許可リストに追加する 59
許可される承認リクエストレートを設定する 60
代替 TFTP サーバを有効にする 60
TFTP サーバ 1 の設定 60
TFTP サーバ 2 の設定 61
AnyConnect VPN 61
VPN 接続プロファイルを追加する 61
VPN 経由のビデオ コールエクスペリエンスを最適化 62
Cisco Unified Communications Manager で VPN を設定する 62
起動プロセス 65
起動時に TFTP サーバを手動で設定する 67
起動検証 68

第 7 章 連絡先 69

操作モード別の連絡先とディレクトリ 69
ローカル連絡先 69
社内ディレクトリ(Corporate Directory) 70
代替電話帳サーバを設定する 70
会社の写真ディレクトリを設定する 71
連絡先検索 71
アプリケーション ダイヤル ルール 72
アプリケーション ダイヤル ルールの設定 72

第 8 章 セルフケアポータルの管理 75
セルフケアポータルの概要 75
セルフケアポータルへのユーザのアクセスの設定 76
セルフケアポータルの表示のカスタマイズ 76

第 9 章 アクセサリ 77
Bluetooth アクセサリ 77
Bluetooth デバイスプロファイル 77
ハンズフリープロファイル 77
電話帳アクセスプロファイル 78
デバイスプロファイルを有効にする 78
Bluetooth アクセサリをペアリングする 79
Bluetooth を無効にする 79
ケーブル ロック 79
外部カメラ 80
外部カメラの設定 80
外部カメラの設置後チェックを実行する 80
外部スピーカーおよびマイクロフォン 80
ヘッドセット 81
Bluetooth ワイヤレス ヘッドセット 82
Bluetooth ワイヤレスヘッドセットを追加 82
Bluetooth ヘッドセットを取り外す 83

USB ヘッドセット 84
USB ヘッドセットを有効にする 84
USB ヘッドセットを無効にする 84
有線ヘッドセット 84
有線ヘッドセットに接続する 85
有線ヘッドセットを無効にする 85
ビデオディスプレイ 85
Cisco DX650 壁掛けキット 85
事前準備 85
壁掛け部品 86
壁掛け金具を取り付ける 86

第 10 章 セキュリティ機能 91
デバイスのセキュリティ 91
セキュリティ機能の概要 92
セキュリティプロファイル 94
SE Android 95
アップグレードと SE Android 95
SE Android トラブルシューティング 95
ローカルで有効な証明書のセットアップ 96
SHA-256 製造インストール証明書 97
セキュアな通話 98
セキュアな電話コールの識別 99
セキュアな会議コールの特定 99
通話セキュリティの相互作用と制限 100
デバイスのセキュリティ情報をリモートで確認する 101
Barge の暗号化 101
802.1X 認証サポート 102
必要なネットワークコンポーネント 102
ベストプラクティス 102
画面ロックと自動ロックの設定 103

画面ロック解除/パスワードリセットの設定 104
設定用の管理者パスワードを設定する 105

第 11 章 機能とサービス 107
利用可能な電話機能 107
エージェントのグリーティング 108
エージェント グリーティングの有効化 108
すべてのコール 108
プライマリ回線のすべての通話 108
自動応答 109
自動ダイヤル 109
割込み 109
ビジー ランプ フィールド 109
通話転送 110
発信者番号通知 110
[発呼者回線IDの表示（Calling Line Identification Presentation）] 110
Cisco Extension Mobility 110
Extension Mobility マルチユーザ 111
Cisco Extension Mobility の設定 111
Cisco モビリティ 112
会議 112
セキュアな会議 113
即転送 113
取り込み中 113
ゲートウェイレコーディング 114
保留状態 114
保留と再開 114
保留音 114
無視 114
メッセージ受信インジケータ 114
ミュート 115

プラス ダイヤル 115
保護された通話 115
呼出音の設定 115
呼出音 115
安全および非セキュア指示トーン 115
Serviceability 116
共有回線 116
スピード ダイヤル 116
転送 117
Uniform Resource Identifier ダイヤリング 117
ビデオ切り替え 117
ボイス メッセージ システム 117
ビジュアル ボイスメールのセットアップ 117
特定のユーザまたはグループにビジュアルボイスメールを設定する 118
機能ボタン 119
機能管理ポリシーの設定 120
機能制御ポリシーのデフォルト値 120
電話ボタン テンプレート 121
電話ボタンテンプレートの変更 121
製品固有のオプションを構成する 122
ビデオ送信解像度のセットアップ 136
インスタントメッセージとプレゼンスの設定 137
アプリケーションのセットアップ 137
Cisco UCM アプリケーション クライアントを有効にする 138
UCM アプリにログインするためのエンドユーザを作成する 138
UCM アプリでユーザをサブスクライブする 139
Cisco Unified Communications Manager 経由で Android APK ファイルをプッシュする 139
Cisco Unified Communications Manager 管理で Android サービスを追加する 140
Android Phone サービスにデバイスを登録する 140

第 12 章 **[カスタマイズ（Customization）]** 143

ワイドバンドコーデックのセットアップ 143
動作モード 144
動作モードの設定 145
デフォルトの壁紙 145
壁紙コントロールの割り当て 145
デフォルトの壁紙を指定する（DX70 および DX80） 146
デフォルトの壁紙を指定する (DX650) 146
SSH アクセス 147
Unified Communications Manager Endpoints Locale Installer 147
国際コールのロギングのサポート 148

第 13 章 メンテナンス 149
デバイスをリセットする 149
オプションをリセットしてアップグレードをロードする 151
リモートロック 151
リモートロック デバイス 152
リモートワイプ 152
デバイスのリモートワイプ 152
Cisco DX70 の代替イメージを起動する 153
Cisco DX80 の代替イメージを起動する 153
Cisco DX650 の代替イメージを起動する 153
データ移行 154
デバッグログプロファイル 154
通話処理のデバッグログプロファイルを設定する 154
デバッグログプロファイルをリセットしてデフォルトにする 155
ユーザサポート 155
問題レポート ツール 155
カスタマー サポート アップロード URL の設定 156
Web ブラウザからスクリーンショットを撮る 157
デバイスからスクリーンショットを撮る 157
アプリケーションサポート 157

第 14 章 モデル情報のステータスと統計 159

モデル情報 159

デバイスのステータス 160

ステータス メッセージ 161

イーサネット統計 165

WLAN 統計 165

音声通話統計 166

第 15 章 リモートモニタリング 169

Web ページへのアクセスを有効または無効にする 169

デバイスの Web ページにアクセスする 170

デバイス情報 171

ネットワークのセットアップ 172

セキュリティ情報 178

イーサネット統計 180

WLAN セットアップ 183

デバイス ログ 184

ストリームの統計 185

はじめに

- 概要 （xix ページ）
- ガイドの表記法 （xix ページ）
- 関連資料 （xx 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 （xxii ページ）

概要

この本では、ネットワーク上のデバイスを理解、インストール、構成、管理するために必要な情報を提供します。 Cisco DX シリーズ

ネットワーク技術者、システム管理者、および電気通信技術者は、このガイドを見てCisco DX シリーズ デバイスの設定に必要な手順を学ぶ必要があります。 このドキュメントで説明するタスクには、ユーザ向けではないネットワーク設定の構成が含まれます。 このマニュアルのタスクを実行するには、 Cisco Unified Communications Manager に精通している必要があります。

IP テレフォニー ネットワークは複雑なため、このガイドでは、 Cisco Unified Communications Managerまたはその他のネットワーク デバイスで実行する必要がある手順について、完全かつ詳細な情報は提供していません。

ガイドの表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で表記されています。
[]	角カッコの中の要素は、省略可能です。
{x | y | z}	必ずどれか1つを選択しなければならない必須キーワードは、波カッコで囲区切って示しています。

表記法	説明
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角括弧で囲み、縦棒で区切っています。
文字列	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符すると、その引用符も含めて string とみなされます。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示してい
input フォント	ユーザが入力しなければならない情報は、**input** フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の *screen* フォントで示しています
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組わせは、Ctrl キーを押しながら D キーを押すことを意味します。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。

注目 安全上の重要な注意事項

「危険」の意味です。 人身事故を予防するための注意事項が記述されています。 装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。 各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。 ステートメント 1071

これらの注意事項を保管しておいてください。

関連資料

Cisco DX シリーズ

すべてのドキュメントは次の URL から入手できます。 Cisco DX シリーズ

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

ユーザ向けのドキュメントは次の URL から入手できます。

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

管理者向けのドキュメントは次の URL から入手できます。

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

『*Cisco DX Series Wireless LAN* 導入ガイド』 は次の URL から入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-implementation-design-guides-list.html

翻訳された出版物は次の URL から入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-translated-end-user-guides-list.html

オープンソース ライセンス情報は、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-licensing-information-listing.html

規制コンプライアンスおよび安全性に関する情報は、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-installation-guides-list.html

Cisco Unified Communications Manager

『 *Cisco Unified Communications Manager Documentation Guide* 』およびご使用のリリースに固有のその他の資料を参照してください。 Cisco Unified Communications Manager 次のドキュメント URL から参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Business Edition 6000

『*Cisco Business Edition 6000* ドキュメンテーション ガイド』 および、Cisco Business Edition 6000 リリースに固有のその他の出版物を参照してください。 次の URL から入手できます。

http://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Ciscoと環境

関連出版物は次の URL から入手できます。

http://www.cisco.com/go/ptrdocs

用語の違い

次の表に、『Cisco DX シリーズ User Guide』、『*Cisco DX* シリーズ*Administration Guide*』、*Cisco Unified Communications Manager* アドミニストレーション ガイド で使用される用語の違いを示します。

表 *1:* 用語の違い

ユーザガイド	管理ガイド
回線ステータス	話中 ランプ フィールド（BLF）
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）またはメッセージ受信ランプ
ボイスメール システム	ボイス メッセージ システム

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。

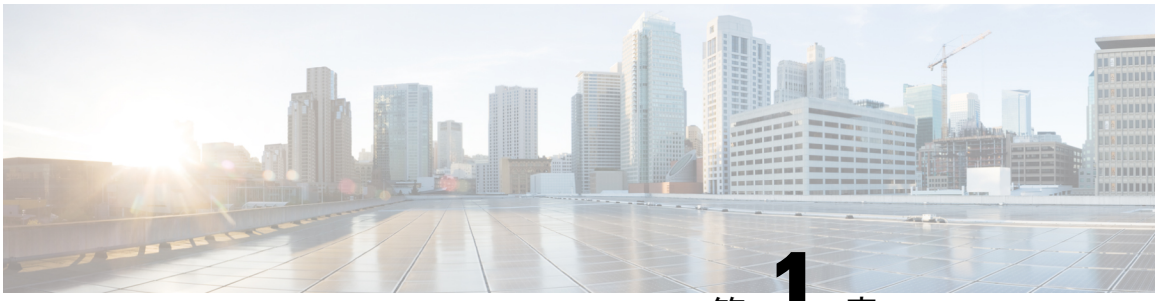
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*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.gov/ear をご覧ください。



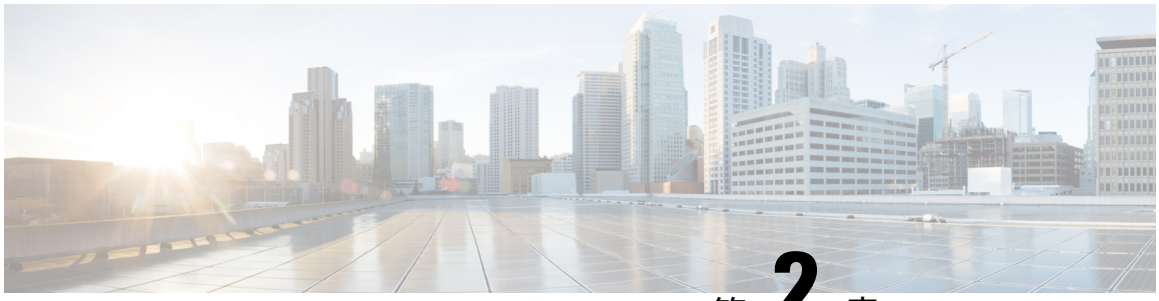
第 1 章

新規および変更情報

- リリース 10.2(5) の新機能および変更された機能 （1 ページ）

リリース 10.2(5) の新機能および変更された機能

新しいコンテンツおよび変更されたコンテンツ	項
無線ハードウェアは追加されませんでした	無線ハードウェアなし （24 ページ）
代替電話帳サービスを追加しました	代替電話帳サーバを設定する （70 ページ）
FIPS モードを追加	製品固有のオプションを構成する （122 ページ）
Cisco DX650 のデフォルトの壁紙のサイズとフォルダを更新しました	デフォルトの壁紙を指定する (DX650) （146 ページ）
更新された連絡先検索	連絡先検索 （71 ページ）
自動問題レポートアップロードを追加しました	製品固有のオプションを構成する （122 ページ）
設定に管理者パスワードを追加しました	設定用の管理者パスワードを設定する （105 ページ）



第 2 章

技術仕様

- 物理環境および動作環境に関する仕様 （3 ページ）
- ネットワーク ポートとコンピュータ ポートのピン割り当て （5 ページ）
- ネットワーク プロトコル （7 ページ）
- 電力要件 （11 ページ）
- 外部デバイス （15 ページ）
- USB ポートと USB シリアルコンソールのデータ情報 （16 ページ）
- ネットワーク混雑時の動作 （17 ページ）

物理環境および動作環境に関する仕様

表 *2 : Cisco DX* シリーズ デバイスの物理的および動作仕様

仕様	値または範囲
外形寸法（高さ x 幅 x 奥行き）	Cisco DX70: 14.84 インチ (377.1 mm) x 13.91 インチ (353.1 mm) x 2.45 インチ (62.3 mm) Cisco DX80: 20.2 インチ (512 mm) x 22.2 インチ (565 mm) x 3.5 インチ (89 mm) Cisco DX650: 8.46 インチ (215 mm) x 10.35 インチ (263 mm) x 8.19 インチ (208 mm)
重量	Cisco DX70: 8.5 ポンド (3.9 kg) Cisco DX80: 15.65 ポンド (7.1 kg) Cisco DX650: 3.81 ポンド (1.73 kg)
動作温度	0 ～ 40°C（32 ～ 104°F）
動作時の相対湿度	10 ～ 95%（結露しないこと）
保管温度	–10 ～ 60 °C（14 ～ 140 °F）

仕様	値または範囲
電源、Cisco DX70	定格: 最大 12V で 3.5A 低電力スタンバイモード 統合された EnergyWise サポート
電源、Cisco DX80	定格: 最大 60 W 低電力スタンバイモード 統合された EnergyWise サポート
電源、Cisco DX650	IEEE 802.3af (クラス 3) または IEEE 802.3at (クラス 4) Power over Ethernet (PoE) 規格がサポートされています。 Cisco Discovery Protocol および Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) PoE スイッチ ブレードの両方と互換性があります。 電力バジェット: 802.3AF および低電力 USB 周辺機器のサポートの場合は 13.7W (Cisco Discovery Protocol) または 15.1W (LLDP)。高電力 USB 周辺機器のサポートには 15.4W 以上および 802.3AT が必要です。
接続性	内部 2 ポート Cisco イーサネット スイッチ IEEE 802.11 a/b/g/n Wi-Fi
音声コーデックのサポート	狭帯域オーディオ圧縮コーデック: G.711a、G.711u、G.729a、G.729ab、および iLBC 広帯域オーディオ圧縮コーデック:G.722、インターネット音声オーディオ コーデック (iSAC)、iLBC、および AAC-LD オーディオ圧縮コーデック。
オペレーティング システム	Android™ 4.1.1 (ジェリービーン)
Processor	Cisco DX70: TI OMAP 4470 1.5GHz デュアルコア ARM Cortex-A9 プロセッサ Cisco DX80: TI OMAP 4470 1.5GHz デュアルコア ARM Cortex-A9 プロセッサ Cisco DX650: TI OMAP 4460 1.5-GHz デュアルコア ARM Cortex-A9 プロセッサ
メモリ	2 GB RAM; 低電力ダブルデータレート同期ダイナミックランダム アクセスメモリ (LPDDR2 SDRAM)
ストレージ	8 GB eMMC NAND フラッシュメモリ (組み込みマルチメディアカード、不揮発性)

ネットワーク ポートとコンピュータ ポートのピン割り当て

Cisco DX シリーズ デバイスには、ネットワーク接続に使用されるネットワーク ポートとコンピューター (アクセス) ポートが含まれます。 これらは目的が異なり、ポートのピン配置も異なります。

- ネットワーク ポートは 110/100/1000 SW ポート です。
- コンピュータ（アクセス）ポートは 10/100/1000 PC ポート です。

ネットワーク ポート コネクタのピン割り当て

表 *3:* ネットワーク ポート コネクタのピン割り当て

ピン番号	機能
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
BI は 双方向を意味し、DA、DB、DC、DD はそれぞれ データ *A*、 データ *B*、データ *C* 、 データ *D* を意味します。	

コンピュータポートコネクタのピン配置

表 *4:* コンピュータ（アクセス）ポート コネクタのピン割り当て

ピン番号	機能
1	BI_DB+
2	BI_DB-
3	BI_DA+

ピン番号	機能
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-

（注）
BI は 双方向を意味し、DA、DB、DC、DD はそれぞれ データ *A*、 データ *B*、 データ *C* 、 データ *D*を意味します。

Cisco DX シリーズデバイスで使用されるポート

次の表は、デバイスが使用するポートについて説明しています。 Cisco DX シリーズ 詳細については、『 *Cisco Unified Communications Manager* の *TCP* および *UDP* ポート使用ガイド』を参照してください。

表 *5 : Cisco DX* シリーズ デバイスポート

送信元ポート（**Source Port**）	リモートデバイスポート	基礎プロトコル	プロトコル/サービス	注記
68	67	-	DHCP クライアント	動的 IP アドレスを取得するための DHCP サポート
49152-53248	53	UDP	DNS クライアント	名前解決のための DNS サポート
49152-53248	69	UDP	TFTP クライアント	中央サーバからさまざまな構成ファイルやイメージファイルを取得するには、TFTP サポートが必要です。
49152-53248	80	TCP および UDP	HTTP クライアント	
80	サーバ設定済み	TCP および UDP	[HTTP サーバ（DHCP server）]	
123	123	UDP	NTP クライアント	時刻を取得するためのネットワークタイムプロトコル

送信元ポート（Source Port）	リモートデバイスポート	基礎プロトコル	プロトコル/サービス	注記
49152-53248	サーバ設定済み	[TCP]	HTTP クライアント	
49152-53248	6970	[TCP]	TFTP クライアント	中央サーバからさまざまな構成ファイルやイメージファイルを取得するには、TFTP サポートが必要です。
49152-53248	5060	[TCP]	SIP/TCP	デフォルトは 5060 です。管理者は変更できます。
49152-53248	5061	[TCP]	SIP/TLS	デフォルトは 5061 です。管理者は変更できます。
16384- 32767	受信範囲	UDP	RTP	管理者はポート範囲を設定できます。
16384- 32767	受信範囲	UDP	RTCP	RTCP ポートは RTP +1 です。
4224	PC ダイナミックレンジ	[TCP]		
22	サーバ設定済み	[TCP]	セキュアシェル	
4051		[TCP]		ロードのアップグレード
4052		RDP		アップグレードをロードする
4061				特別なデバッグ
8443				連絡先検索

ネットワーク プロトコル

Cisco DX シリーズデバイスは、音声通信に必要ないくつかの業界標準および Cisco ネットワーク プロトコルをサポートしています。 次の表に、デバイス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 *6*：サポートされるネットワーク プロトコル

ネットワーク プロトコル	目的	使用方法に関
Binary Floor Control Protocol（BFCP）	BFCP を使用すると、ユーザーは通話中のビデオによる会話内でプレゼンテーションを共有できます。	BFCP は自動

ネットワーク プロトコル	目的	使用方法に関する
Bluetooth	Bluetooth は、短距離におけるデバイスの通信方法を指定する Wireless Personal Area Network（WPAN）プロトコルです。	デバイスは Bluet います。 デバイスは、ハン (HFP)、高度オー ファイル、ヒュー デバイス プロフ クト プッシュ プ び電話帳アクセス をサポートしてい
Bootstrap Protocol (BootP)	BootP により、ネットワーク デバイスは IP アドレスなどの特定の起動情報を検出できるようになります。	—
Cisco Discovery Protocol（CDP）	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。 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、他のデバイスの情報を受信することができます。	補助 VLAN ID、 詳細情報、Qualit 情報などの情報を とやり取りするた が使用されます。
Cisco Peer-to-Peer Distribution Protocol（CPPDP）	CPPDP は、デバイスのピアツーピア階層を形成するために使用される Cisco 独自のプロトコルです。 この階層はピア デバイスからネイバー デバイスにファームウェア ファイルを配布するために使用されます。	ピア ファームウ を使用します。
Dynamic Host Configuration Protocol（DHCP）	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。 DHCP を使用すると、手動で IP アドレスを割り当てたり追加のネットワーク パラメータを構成したりすることなく、デバイスをネットワークに接続するだけで、そのデバイスを運用できるようになります。	DHCP は、デフォ います。 無効に で個別に IP アド ク、ゲートウェイ を手動で設定する Cisco では、DHC 150 を使用するこ の方法では、TF をオプション値と ポートされていな いては、『*Cisco* *Manager* システム ミック ホスト コ プロトコル」」の の章を参照して （注） オプション 150 を DHCP オプション ができます。

ネットワーク プロトコル	目的	使用方法に関
Hypertext Transfer Protocol（HTTP）	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的な手段です。	デバイスは、ルシューティします。
Hypertext Transfer Protocol Secure（HTTPS）	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。	HTTP と HTT Web アプリケ設定されてい るデバイスは
IEEE 802.1X	IEEE 802.1X 標準は、クライアント/サーバベースのアクセス コントロールと認証プロトコルを定義します。これにより、未承認のクライアントが一般にアクセス可能なポートから LAN に接続するのを制限します。 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。 認証が成功すると、通常のトラフィックがポートを通過できるようになります。	デバイスでは EAP-TLS 認証 より IEEE 802 デバイスで 80 る場合は、PC 効にする必要
IEEE 802.11a/b/g/n	IEEE 802.11 標準は、ワイヤレス ローカル エリア ネットワーク（WLAN）におけるデバイスの通信方法を指定します。 802.11a は 5 GHz 帯域で動作し、802.11b と 802.11g は 2.4 GHz 帯域で動作します。 802.11n は 2.4 GHz または 5 GHz 帯域で動作します。	802.11 インタ トのケーブル しくない場合
インターネット プロトコル（IP）	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。	IP を使用して クデバイスに ゲートウェイ り当てられて Dynamic Host （DHCP）を通 る場合、IP ア びゲートウェ り当てられま 合は、各デバ パティを手動 す。 デバイスは、 ます。 詳細に *Services Guide Communication* トプロトコル を参照してく

ネットワーク プロトコル	目的	使用方法に関する
リンク層検出プロトコル（LLDP）	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。	デバイスはPC ポします。
Link Layer Discovery Protocol-Media Endpoint Devices（LLDP-MED）	LLDP-MEDは、音声製品用LLDP標準の拡張です。	デバイスは、次のために、SW ポートしていま • ボイス VLA • デバイスの • 電源管理 • インベント LLDP-MED サポ LLDP-MED およ Protocol』ホワイ ださい。 http://www.cisco.c technologies_whit paper0900aecd804
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。	デバイスは RTP リアルタイム音声 話機やゲートウェ
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、より優れたビデオエクスペリエンスを提供するために、オーディオとビデオのストリームを同期するためにも使用されます。	音声通話の RTCP なっています。 デオ コール内の ビデオ ストリー フォルトで有効 Unified Communi Administration から を有効または無効
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 フォート ノイズ 常、運用中の Cis Manager またはア よってグローバル エンドポイントの メータをエンドポ 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
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 VoIP プ グナリングと ケットテレフ で処理します ネットワーク 送することが ン管理は、エ 性を制御する
テレプレゼンス相互運用プロトコル (TIP)/多重化 (MUX)	TIP/MUX は、メディアの受信または送信前にエンドポイント間でオーディオおよびビデオ メディア オプションをネゴシエートするために使用される IP プロトコルです。	TIP/MUX は、 めに呼び出さ 能にします。
Transmission Control Protocol（TCP）	TCP は、接続型の転送プロトコルです。	デバイスは T Communicatio サービスにア
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 は Cisco Unifi に安全に登録 を使用します
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。 デバイスで TFTP を使用すると、デバイス タイプ固有の設定ファイルを取得できます。	TFTP は DHC る TFTP サー です。 DHCP 外の TFTP サ には、デバイ を使用して、 を手動で割り 詳細について を『 *Cisco Uni* システム ガイ
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 す。 デバイス UDP をサポー

電力要件

Cisco DX シリーズ デバイスは外部電源で稼働します。 外部電源は個別の電源装置によって提供されます。

Cisco DX650 Power over Ethernet (PoE) による電源供給も可能です。 スイッチは、イーサネットケーブルを介して PoE を提供できます。

（注） 外部電源で動作するデバイスをインストールする場合は、イーサネット ケーブルをデバイスに接続する前に、電源装置を電話機と電源コンセントに接続します。外部電源から電力が供給されているデバイスを取り外す場合は、電源装置を取り外す前に、イーサネット ケーブルをデバイスから取り外してください。

電力ガイドライン

Cisco DX70 および Cisco DX80に電力を供給するには、付属の Lite-On PA-1600-2A-LF 電源または FSP075-DMAA1 を使用します。 Cisco DX650に電力を供給するには、下の表を参照してください。

表 *7:* 電源に関するガイドライン *Cisco DX650*

電源の種類	ガイドライン
外部電源：CP-PWR-CUBE-4 = 外部電源を通じて電力を供給	このデバイスは CP-PWR-CUBE-4 電源を使用します。 （注） デバイスをワイヤレス ネットワークに展開する場合は、CP-PWR-CUBE-4 る必要があります。
外部電源 - Cisco Unified IP Phone Power Injector から供給	Cisco Unified IP Phone パワー インジェクタは、いずれの機種でも使用でき DX650。 インジェクタは、ミッドスパン デバイスとして機能し、接続さ 話機にインライン パワーを供給します。 Cisco Unified IP 電話パワー イン は、スイッチ ポートと電話間に接続されます。また、通電していないス 電話 間で最大 100 m のケーブル長をサポートします。
PoE 電源 - 電話機に接続されたイーサネットケーブルを介してスイッチから供給されます	Cisco DX650 IEEE 802.3af クラス 3 電源オン信号ペアおよびスペア ペアを ます。 これらのデバイスは、外部アドオン デバイス用の IEEE 802.3at をサポー す。 電話機を無停電で運用するには、スイッチがバックアップ電源を備えてい ります。 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、目的と 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 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。 NG-PoE+ のサポート: NG-PoE+ スイッチがサポートされている限り、デバ 802.3at よりも多くの電力を消費できます。

電力削減

Power Save または EnergyWise (Power Save Plus) モードを使用すると、デバイスが消費するエネルギー量を削減できます。

省電力モード

省電力モードでは、デバイスが使用されていないときに画面のバックライトは点灯しません。デバイスは、スケジュールされた期間中、またはユーザが受話器を持ち上げたり、いずれかのボタンを押したりするまで、省電力モードのままになります。 Cisco Unified Communications Manager の **[電話の設定]** ウィンドウの製品固有の設定領域で、次のパラメータを設定します。

ディスプレイ非点灯日（Days Display Not Active）

バックライトを非アクティブにする日を指定します。

ディスプレイ点灯時刻（Display On Time）

バックライトが自動的に点灯する時刻をスケジュールします。

ディスプレイ点灯継続時間（Display On Duration）

プログラムされたスケジュールによってバックライトが有効にされた後、バックライトがアクティブな時間の長さを示します。

EnergyWise モード

デバイスは、省電力モードに加えて、Cisco EnergyWise (Power Save Plus) モードもサポートしています。 ネットワークに EnergyWise (EW) コントローラ (EnergyWise 機能が有効になっている Cisco スイッチなど) が含まれている場合は、これらのデバイスをスケジュールに従ってスリープ (電源オフ) およびウェイク (電源オン) するように設定して、電力消費をさらに削減できます。

各デバイスを設定して、EnergyWise 設定を有効または無効にします。 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、構成 XML ファイルの一部としてデバイスに送信されます。 **[電話の設定]** ウィンドウで、 Cisco Unified Communications Manager次のパラメータを設定します。

Enable Power Save Plus

デバイスの電源をオフにする日のスケジュールを選択します。

電話機をオンにする時刻（Phone On Time）

[Power Save Plus を有効にする] フィールドで選択された日にデバイスが自動的にオンになる時刻を決定します。

電話機をオフにする時刻（Phone Off Time）

[Power Save Plus を有効にする] フィールドで選択された日にデバイスの電源をオフにする時刻を決定します。

Phone Off Idle Timeout

デバイスの電源をオフにするまでのアイドル時間の長さを決定します。

音声アラートを有効にする

有効にすると、**[電話の電源をオフにする時間]** フィールドで指定した時刻の 10 分前に音声アラートを再生するようにデバイスに指示します。

EnergyWise Domain

デバイスが存在する EnergyWise ドメインを指定します。

EnergyWise シークレット

EnergyWise ドメイン内で通信するために使用されるセキュリティ シークレット パスワードを指定します。

Allow EnergyWise Overrides

EnergyWise ドメイン コントローラー ポリシーがデバイスに電源レベルの更新を送信することを許可するかどうかを決定します。

デバイスがスリープ状態のとき、電源供給装置(PSE)はデバイスに最小限の電力を供給して **電源/ロック** ボタンを点灯させます。 **電源/ロック** ボタンを使用すると、スリープ状態のデバイスを起動できます。

LLDP での電力ネゴシエーション

デバイスとスイッチは、デバイスが消費する電力をネゴシエートします。 デバイスは複数の電力設定で動作し、利用可能な電力が少ないときに電力消費を削減します。

デバイスが再起動すると、スイッチは電力ネゴシエーションのために 1 つのプロトコル (CDP または LLDP) にロックします。 スイッチは、デバイスが送信する最初のプロトコル (電力しきい値制限値 (TLV) を含む) にロックします。 システム管理者がデバイス上でそのプロトコルを無効にすると、スイッチが他のプロトコルの電源要求に応答しないため、デバイスはアクセサリに電源を投入できなくなります。

Cisco では、デバイスが電力ネゴシエーションをサポートするスイッチに接続する場合は、電力ネゴシエーションを常に有効（デフォルト）にすることを推奨しています。

電力ネゴシエーションが無効になっている場合、スイッチはデバイスへの電源を切断する可能性があります。 スイッチが電力ネゴシエーションをサポートしていない場合は、アクセサリの電源を PoE+ で投入する前に、電力ネゴシエーション機能を無効にしてください。 電力ネゴシエーション機能が無効になっている場合、デバイスは IEEE 802.3af-2003 標準で許可されている最大値までアクセサリに電力を供給できます。

（注） CDP と電力ネゴシエーションが無効になっている場合、デバイスはアクセサリに最大 15.4 W の電力を供給できます。

電力に関する追加情報

次の表にあるドキュメントは、次のトピックに関する詳細情報を提供します。

- Cisco Unified IP Phones と連携する Cisco スイッチ
- 双方向電力ネゴシエーションをサポートしている Cisco IOS リリース
- 電力に関するその他の要件および制限事項

ドキュメントトピック	URL
Cisco Unified IP 電話パワー インジェクタ	http://www.cisco.com/c/en/us/products/collaboration-endp unified-ip-phone-power-injector/index.html
PoE ソリューション	http://www.cisco.com/c/en/us/solutions/enterprise-networ power-over-ethernet-solutions/index.html
Cisco Catalyst スイッチ	http://www.cisco.com/cisco/web/psa/default.html?mode=p http://www.cisco.com/c/en/us/products/switches/index.htr
サービス統合型ルータ	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS ソフトウェア	http://www.cisco.com/c/en/us/products/ios-nx-os-software

外部デバイス

不要な無線周波数（RF）信号および可聴周波数（AF）信号を遮断する高品質の外部デバイスを使用することをお勧めします。外部デバイスには、ヘッドセット、ケーブル、コネクタが含まれます。

これらのデバイスの品質や、携帯電話および双方向ラジオなど他のデバイスとの間隔によっては、雑音が入ることもあります。その場合は、次の方法で対処することをお勧めします。

- RF または AF の信号源から外部デバイスを離す。
- RF または AF の信号源から外部デバイスのケーブルの経路を離す。
- 外部デバイス用にシールドされたケーブルを使用するか、高品質なシールドおよびコネクタを備えたケーブルを使用する。
- 外部デバイスのケーブルを短くする。
- 外部デバイスのケーブルに、フェライトまたは同様のデバイスを適用する。

シスコでは、外部デバイス、ケーブル、およびコネクタのパフォーマンスを保証できません。

注意 欧州連合諸国では、EMC Directive [89/336/EC] に完全に準拠した外部スピーカ、マイクロフォン、ヘッドセットだけを使用してください。

USB ポートと USB シリアルコンソールのデータ情報

Cisco DX シリーズ デバイスには USB ポートがあり、場合によってはマイクロ USB ポートもあります。 デバイスは、USB ポートへの最大 10 個のアクセサリの接続をサポートします。 デバイスに接続する各アクセサリも最大数に含まれます。 サポートされているアクセサリには、USB シリアル ケーブル、USB マウス、USB キーボード、USB 電源ハブ、USB メモリ スティックなどがあります。

（注） すべての USB ハブには電源を供給する必要があるため、1 つ以上のハブを含むキーボードは、電源が供給されていないハブが含まれているため、これらのデバイスでは使用できません。

Android Debug Bridge (ADB) アクセスには USB 接続を使用することもできます。 ADB アクセスには、 Cisco DX650 および Cisco DX70 のマイクロ USB ポートと、 Cisco DX80 の USB タイプ B ポートを使用します。 ADB の使用に関する詳細については、http://developer.android.com/index.html を参照してください。

USB シリアル コンソールを使用すると、USB ポートをコンソールとして使用できるため、シリアル ポートが不要になります。 次の表は、USB コンソールの設定を示しています。

表 *8 : USB* コンソールの設定

パラメータ	設定
ボーレート	115200
データ：	8 ビット
パリティ	なし
停止	1 ビット
フロー制御	なし

（注） デバイスにはドライバーがプリロードされているため、Cisco は限られた数のケーブル タイプのみをサポートします。 Cisco では、IOGEAR USB シリアル アダプタの使用を推奨しています。

USB コンソールを使用する

USB コンソール ケーブルには、一方の端に USB インターフェイスがあり、もう一方の端にシリアル インターフェイスがあります。 USB インターフェイスは、デバイス上の任意の USB ポートに接続できます。 シリアル インターフェイスは、PC のシリアル ポートに接続します。

Cisco DX650の場合は、側面または背面の USB タイプ A ポートを使用します。 Cisco DX70 および Cisco DX80 マイクロ USB ポートを使用します。

ヒント PC/ラップトップにシリアル ポートがない場合は、2 本の USB コンソール ケーブルを、その間にヌル モデム ケーブルを挟んで背中合わせに接続できます。

手順

ステップ 1 Cisco Unified Communications Managerで、デバイス ページで資格情報を設定します。

ステップ 2 ウィンドウの製品固有の構成レイアウト部分で USB デバッグを有効にします。

ステップ 3 USB シリアル ケーブルをデバイスに接続します。 デバイス コンソールの出力がターミナル画面に表示されます。

ステップ 4 出力が停止したら、**[戻る]** をタップしてログインします。

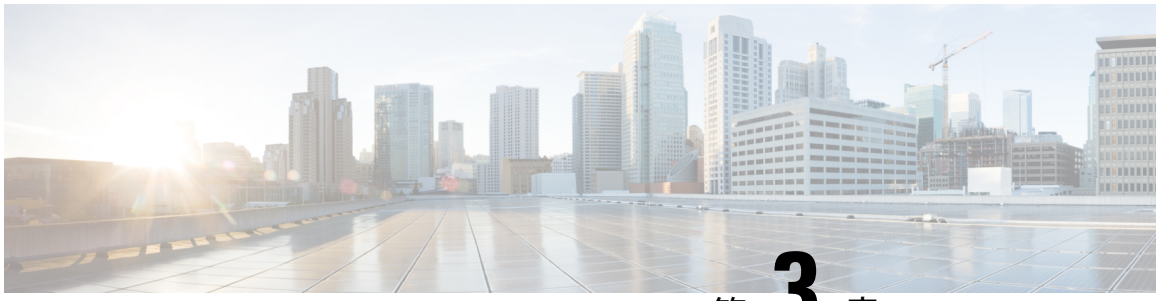
ステップ 5 $prompt 画面の後、debugsh などのツールを使用して問題を診断できます。

ネットワーク混雑時の動作

ネットワーク パフォーマンスを低下させるものは音声やビデオの品質に影響する可能性があり、場合によっては通話が切断されることもあります。 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

悪影響を軽減または排除するには、デバイスが使用されていない時間帯に管理ネットワーク タスクをスケジュールするか、デバイスをテストから除外します。

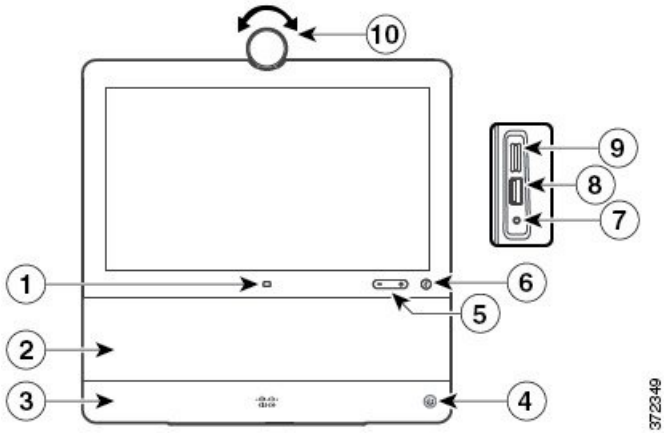


第 3 章

デバイスの説明

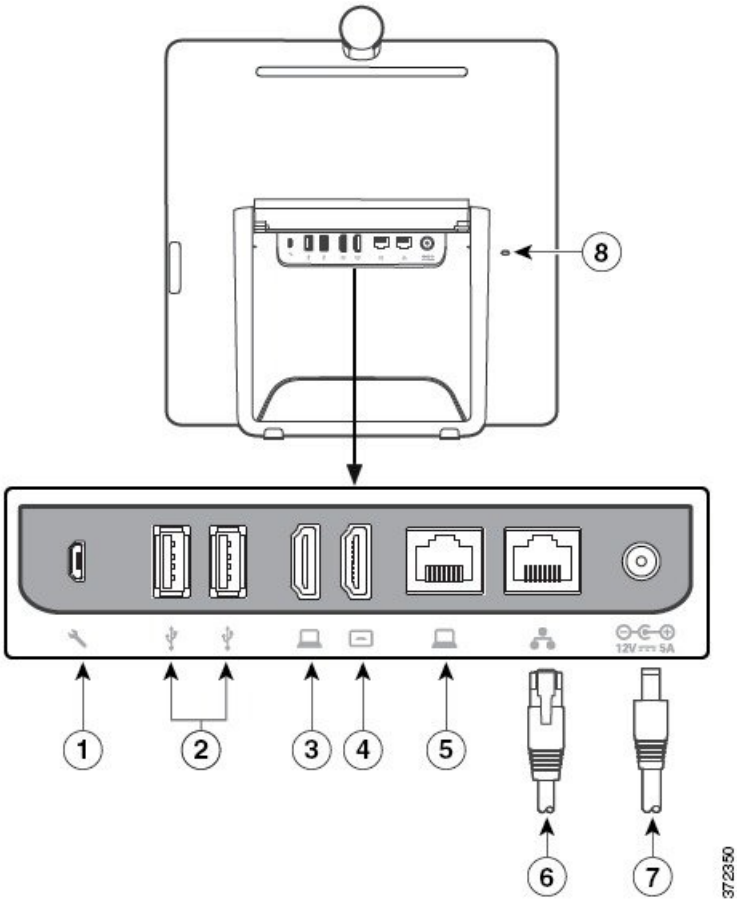
- Cisco DX70 ハードウェア （19 ページ）
- Cisco DX80 ハードウェア （21 ページ）
- Cisco DX650 ハードウェア （23 ページ）
- 無線ハードウェアなし （24 ページ）

Cisco DX70 ハードウェア



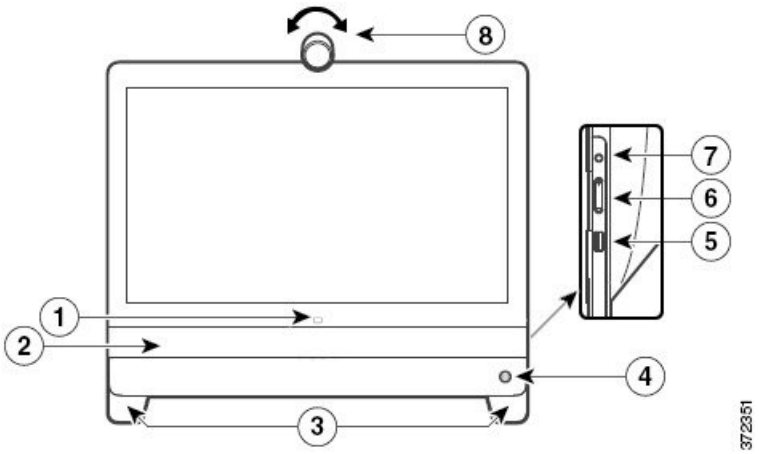
1	ソースボタン	6	ミュートボタン
2	[スピーカー（Speaker）]	7	ミニジャック 3.5 mm 出力
3	マイクロフォン	8	USB 充電ポート
4	電源ボタン	9	microSD カードスロット
5	音量ボタン	10	プライバシーシャッター付きカメラ

Cisco DX70 ケーブルの取り付け



1	マイクロ-B USB ポート	5	コンピュータポート
2	USB ポート	6	ネットワークポート
3	HDMI 入力	7	電源ポート
4	HDMI 出力		

Cisco DX80 ハードウェア

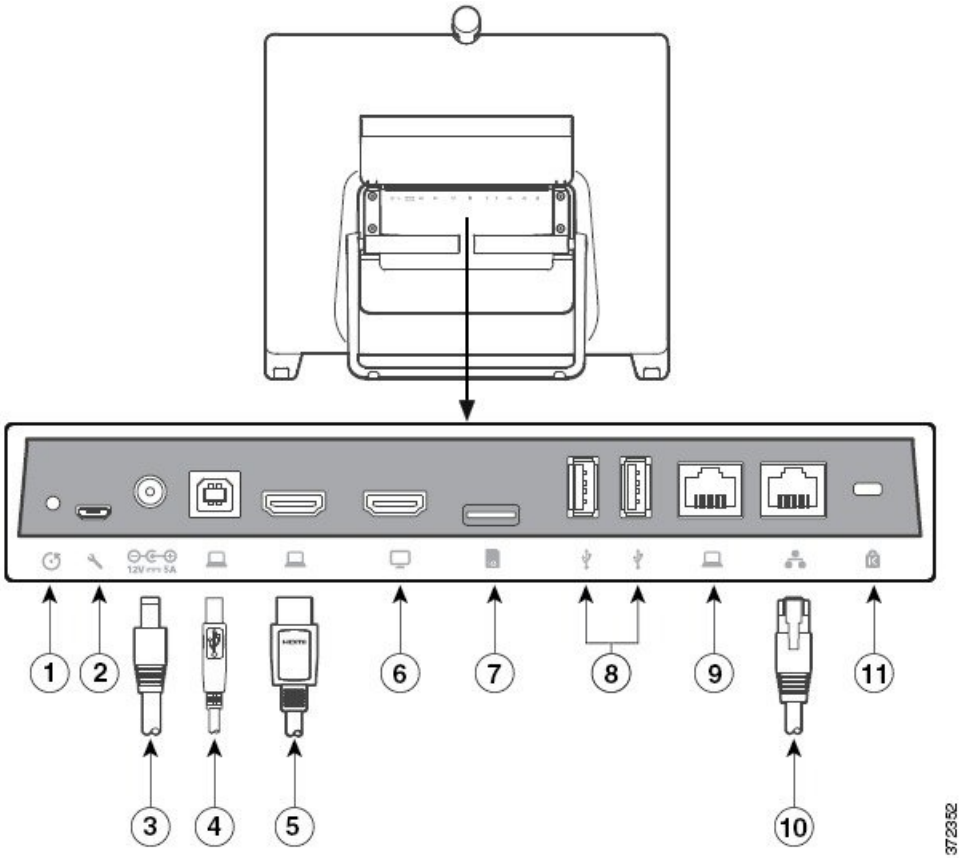


1	ソースボタン	5	USB ポート
2	[スピーカー（Speaker）]	6	音量ボタン
3	両脚にマイク	7	ミュートボタン
4	電源ボタン	8	プライバシーシャッター付きカメラ

Cisco DX80 音響エコーキャンセラー (AEC) とラップトップ シャドウイングが含まれます。 通話の相手側のユーザは、マイクの前にノートパソコンなどの障害物を置いても、クリアな音質を体験できます。 現在のマイクが物体によって遮られている場合、デバイスは自動的にもう一方の脚にある別のマイク アレイに切り替わります。

Cisco DX80 マイクアレイのビームフォーミングも含まれています。 ユーザがビームの外側（つまり、カメラの視野外）に移動すると、遠端に送信される音声が弱くなります。 ピックアップビーム内（ユニットの前方）にないすべての音源は減衰します。

Cisco DX80 ケーブルの取り付け

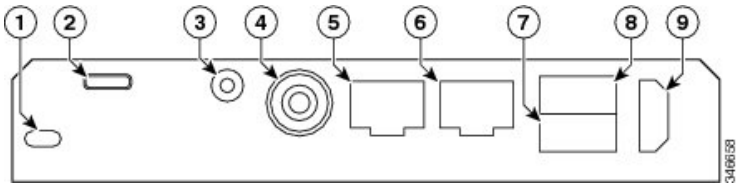


1	初期設定へのリセットピンホール	7	microSD カードスロット
2	マイクロ B USB ポート	8	USB ポート
3	電源ポート	9	コンピュータ ポート
4	USB タイプ B ポート	10	ネットワーク ポート
5	HDMI 入力	11	ケンジントン セキュリティ スロット (K-Slot)
6	HDMI 出力		

Cisco DX650 ハードウェア

1	プライバシーシャッタースライドスイッチ	10	会議ボタン
2	カメラ	11	転送ボタン
3	タッチスクリーン	12	音量ボタン
4	12 キーダイヤルパッド	13	スピーカー ボタン
5	マイクロセキュアデジタル標準容量（HDSC）スロット	14	ビデオ停止ボタン
6	ロックボタン	15	ヘッドセットボタン
7	USB ポート	16	ミュートボタン
8	通話終了ボタン	17	ライトストリップ付きハンドセット
9	ホールドボタン		

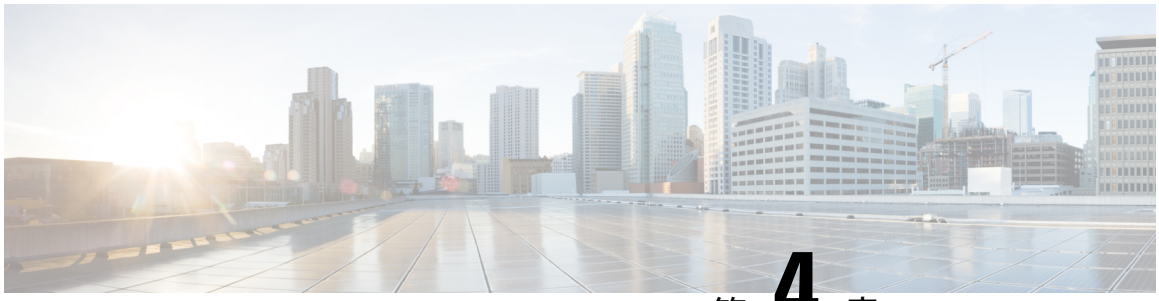
Cisco DX650 ケーブルの取り付け



1	ケンジントンセキュリティスロット (K-Slot)	6	コンピュータ ポート
2	マイクロ-B USB ポート	7	補助ポート
3	3.5 mm ステレオライン入力/出力ジャック	8	USB 2.0 ポート
4	電源ポート	9	HDMI タイプ A ポート
5	ネットワークポート		

無線ハードウェアなし

Cisco DX70 および Cisco DX80 の No Radio (NR) ハードウェア バージョンは、Wi-Fi または Bluetooth 機能をサポートしていません。



第 4 章

Wi-Fi ネットワークの設定

- ネットワーク要件 （25 ページ）
- ワイヤレス LAN （26 ページ）
- Wi-Fi ネットワーク コンポーネント （27 ページ）
- WLAN 通信の 802.11 規格 （31 ページ）
- WLAN 通信のセキュリティ （34 ページ）
- WLAN とローミング （37 ページ）

ネットワーク要件

デバイス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には、ネットワークが次の要件を満たしている必要があります。

- VoIP ネットワーク
  - Cisco ルータおよびゲートウェイ上で VoIP が設定されています。
  - 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。
- IP ネットワークが DHCP をサポートしているか、IP アドレス、ゲートウェイ、およびサブネット マスクの手動割り当てをサポートしている

（注） デバイスは、Cisco Unified Communications Managerから取得した日時を表示します。 ユーザが設定アプリケーションで **日付と時刻の自動設定** のチェックを外すと、時刻がサーバの時刻と同期しなくなる可能性があります。

- ワイヤレス LAN
  - アクセス ポイント (AP) は、WLAN 経由の音声とビデオをサポートするように構成されています。
  - コントローラとスイッチは、音声とビデオをサポートするように構成されています。

- ワイヤレス音声デバイスおよびユーザを認証するためのセキュリティが実装されています。

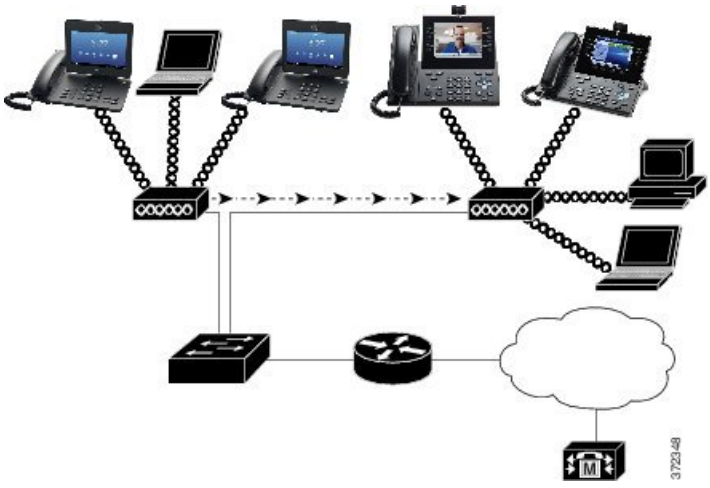
ワイヤレス LAN

（注） ワイヤレス Cisco DX シリーズ デバイスの展開と構成の手順については、『*Cisco DX Series Wireless LAN* 導入ガイド』 を参照してください。

ワイヤレス機能を備えたデバイスでは、企業 WLAN 内での音声通信を行うことができます。デバイスは、ワイヤレス音声通信を提供するために、ワイヤレス アクセス ポイント（AP）や、Cisco Unified Communications Manager Administration などの主要な Cisco IP テレフォニー コンポーネントに依存していて、これらと相互に対話します。

Cisco DX シリーズ デバイスは、802.11a、802.11b、802.11g、および 802.11n Wi-Fi を使用できる Wi-Fi 機能を備えています。

次の図に、ワイヤレス IP テレフォニーのワイヤレス音声伝送を可能にする典型的な WLAN トポロジを示します。



デバイスの電源がオンになると、デバイスのワイヤレスアクセスがオンに設定されている場合は、AP を検索して関連付けます。 Cisco DX シリーズ 記憶されているネットワークが圏外の場合は、ブロードキャストされているネットワークを選択するか、手動でネットワークを追加することができます。

AP は、有線ネットワークへの接続を使用して、スイッチとルータとの間でデータ パケットおよび音声パケットを送受信します。 音声信号は、通話処理とルーティングのためにサーバに送信されます。 Cisco Unified Communications Manager

AP は、ネットワークにワイヤレス リンクまたは「ホットスポット」を提供するため、WLAN の重要なコンポーネントとなっています。 一部の WLAN では、各 AP が、LAN 上に構成され

た Cisco Catalyst 3750 などのイーサネット スイッチに有線接続されています。 スイッチは、ゲートウェイおよびサーバへのアクセスを提供し、ワイヤレス IP テレフォニーをサポートします。 Cisco Unified Communications Manager

一部のネットワークには、ワイヤレス コンポーネントをサポートする有線コンポーネントが含まれます。 そのような有線コンポーネントには、ワイヤレス機能を有効にする特別なモジュールを装備したスイッチ、ルータ、ブリッジなどがあります。

Cisco Unified Wireless Network の詳細については、http://www.cisco.com/c/en/us/products/wireless/index.htmlを参照してください。

Wi-Fi ネットワーク コンポーネント

デバイスは、通話を正常に発信および受信するために、WLAN 内の複数のネットワーク コンポーネントと対話する必要があります。

AP、チャネル、規制区域の関係

アクセス ポイント (AP) は、2.4GHz または 5GHz 周波数帯域内のチャネルを介して RF 信号を送受信します。 安定したワイヤレス環境を提供し、チャネルの干渉を減少させるために、各 AP に重複しないチャネルを指定する必要があります。

AP チャネルとドメインの関係の詳細については、『『*Cisco DX Series Wireless LAN* 導入ガイド』』の「「Designing the Wireless LAN for Voice」」の項を参照してください。

AP の相互作用

Cisco DX シリーズ デバイスはワイヤレス データ デバイスと同じ AP を使用します。 ただし、WLAN の音声トラフィックには、データ トラフィック専用の WLAN とは異なる機器の設定とレイアウトが必要です。 データ伝送では、音声伝送よりも高いレベルの RF ノイズ、パケット損失、およびチャネル コンテンションに耐えることができます。 音声伝送時のパケット損失では、不安定な音声や途切れた音声によって結果的に通話が聞き取れなくなる可能性があります。 パケット エラーにより、ビデオにブロック ノイズが発生したり、ビデオがフリーズしたりすることもあります。

デバイスはデスクトップ（モバイルではない）エンドポイントであるため、ローカル環境の変更によりデバイスがアクセス ポイント間をローミングし、音声とビデオのパフォーマンスに影響する可能性があります。 これとは対照的に、データ ユーザは一箇所に留まって、ときどき別の場所に移動します。 コールを保持しながらローミングが可能であることは、ワイヤレス音声の 1 つの利点です。そのため、RF カバレッジには、吹き抜け、エレベータ、会議室の外にある人気のない場所、通路などを含める必要があります。

優れた音声品質と最適な RF 信号カバレッジを確保するために、サイトの調査を実行する必要があります。 サイトの調査により、ワイヤレス音声に適した設定が決定されます。またサイトの調査は、AP の位置、電力レベル、チャネル割り当てなど、WLAN の設計とレイアウトに役立ちます。

ワイヤレス音声を導入し、使用できるようにした後も、引き続き設置後のサイトの調査を実施する必要があります。 新規ユーザ グループの追加、機器の追加設置、または大量のインベントリのスタックを行うと、ワイヤレス環境が変化します。 設置後の調査で、AP のカバレッジがそれまでと同様に最適な音声通信にとって十分であるかを検証します。

（注） ローミング中にはパケット損失が発生します。しかし、セキュリティ モードおよび高速ローミングの存在により、伝送中のパケット損失数が決まります。 Cisco Centralized Key Management（CCKM）を実装して、高速ローミングを有効にすることを推奨します。

ワイヤレス ネットワークでの音声 QoS の詳細については、『『*Cisco DX Series Wireless LAN* 導入ガイド』』を参照してください。

アクセス ポイントとのアソシエーション

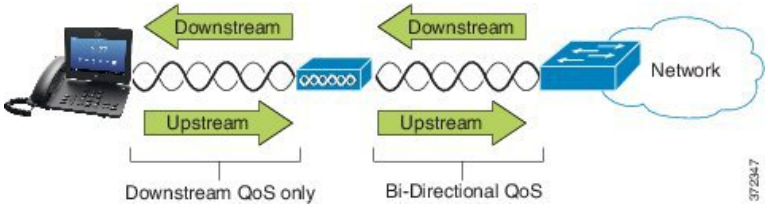
起動時に、デバイスは認識できる SSID と暗号化タイプを持つ AP をスキャンします。 デバイスは適格な AP のリストを構築および維持し、現在の構成に基づいて最適な AP を選択します。

無線ネットワークにおける QoS

ワイヤレス LAN の音声およびビデオ トラフィックは、データ トラフィックの場合と同様に、遅延、ジッター、およびパケット損失の影響を受けます。 これらの問題は、データのエンドユーザには影響しませんが、音声またはビデオ コールに重大な影響を及ぼすことがあります。遅延やジッターを抑えて、音声およびビデオ トラフィックがタイムリーかつ確実に処理されるようにするには、Quality Of Service（QoS）を使用します。

デバイスをボイス VLAN に分離し、より高い QoS を音声パケットに割り当てることで、音声トラフィックがデータ トラフィックよりもプライオリティの高い処理を確実に受けるようにできます。その結果、パケットの遅延や損失パケットを低下させることができます。

専用帯域幅を持つ有線ネットワークとは異なり、ワイヤレス LAN では、QoA の実装時にトラフィックの方向を考慮します。 次の図に示すように、トラフィックは AP によってアップストリームまたはダウンストリームに分類されます。



Enhanced Distributed Coordination Function（EDCF）タイプの QoS には、ダウンストリーム（802.11b/g クライアント方向）QoS 用に最大 8 つのキューがあります。 キューは次のオプションに基づいて割り当てることができます。

- パケットの QoS または DiffServ コード ポイント（DSCP）設定

- レイヤ 2 またはレイヤ 3 アクセス リスト
- 特定のトラフィックの VLAN
- デバイスの動的登録

AP で最大 8 つのキューを設定できますが、可能な限り高い QoS を保障するため、それぞれ音声トラフィック、ビデオ トラフィック、およびシグナリング トラフィック用の 3 つのキューのみを使用する必要があります。音声は音声キュー（UP6）に、ビデオはビデオキュー（UP5）に、シグナリング（SIP）トラフィックはビデオ キュー（UP4）に、データ トラフィックはベストエフォート キュー（UP0）に入れます。 802.11b/g EDCF では音声トラフィックがデータ トラフィックから保護される保証はありませんが、このキューイング モデルを使用することで、統計的に最高の結果が得られます。

各キューは次のとおりです。

- ベスト エフォート（BE）：0、3
- バックグラウンド（BK）：1、2
- ビデオ（VI）：4、5
- ビデオ（VO）：6、7

（注） デバイスは、SIP シグナリング パケットに DSCP 値 24（CS3）をマークし、RTP パケットに DSCP 値 46（EF）をマークします。

（注） コール制御（SIP）は、UP4（VI）として送信されます。 アドミッション制御必須（ACM）がビデオに対して無効になっている場合（Traffic Specification（TSpec）無効）、ビデオは UP5（VI）として送信されます。 ACM が音声に対して無効になっている場合（TSpec 無効）、音声は UP6（VO）として送信されます。

次の表に、音声、ビデオ、およびコール制御（SIP）のトラフィックの優先順位を指定する、AP 上の QoS プロファイルを示します。

表 *9 : QoS* プロファイルとインターフェイス設定

トラフィック タイプ	DSCP	802.1p	WMM UP	ポート範囲
音声	EF（46）	5	6	UDP：16384 ～ 32767
インタラクティブ ビデオ	AF41（34）	4	5	UDP：16384 ～ 32767
コール制御	CS3（24）	3	4	TCP 5060-5061

非決定性環境での音声伝送の信頼性を改善するため、デバイスは IEEE 802.11e 業界規格をサポートし、Wi-Fi Multimedia（WMM）に対応しています。 WMM は、音声、ビデオ、ベストエフォート データ、およびその他のトラフィックの差別化サービスを可能にします。 これらの差別化サービスが音声パケットに十分な QoS を提供するために、一度に 1 つのチャネルで一定量の音声帯域幅だけが使用可能または許可されています。 ネットワークが予約済み帯域幅で処理可能なボイスコールが「N」個で、音声トラフィックの量がこの制限を超えた（N+1「」個のコール）場合、すべてのコールの品質が低下します。

コール品質の問題に対処するには、初期コールアドミッション制御（CAC）方式が必要です。 WLAN 上で SIP CAC が有効になっている場合、アクティブな音声コールの数が AP に設定された制限を超過しないように制限することで、ネットワークが過負荷の場合でも QoS が維持されます。 ネットワークが輻輳している間、システムは「」AP が「フル キャパシティ」の場合でも、ワイヤレス デバイス クライアントが隣接 AP へローミングできる程度の帯域幅の予約を維持します。 音声帯域幅の制限に達すると、チャネルの既存コールの品質に影響を与えないように、その次のコールと隣接 AP との間でロード バランシングが行われます。

（注） Cisco DX シリーズ デバイスは SIP 通信に TCP を使用します。AP がいっぱいになると、Cisco Unified Communications Manager の登録が失われる可能性があります。 CAC によって「承認」されていないクライアントとの間のフレームはドロップされ、 Cisco Unified Communications Manager 登録解除につながる可能性があります。 したがって、シスコでは SIP CAC を無効にすることを推奨します。

（注） DSCP、COS、および WMM UP マーキングが正しく表示され、ビデオ フレームの最適な伝送が実現します。 デバイスは音声およびビデオ CAC をサポートしていないため、シスコでは SOP CAC を実装することを推奨します。

デバイスは、フレキシブル DSCP およびビデオプロモーション機能を使用して、異なるタイプのデバイスでビデオが発生した場合の QoS の不一致と帯域幅のアカウンティングの不一致を解決します。

フレキシブル DSCP の設定

手順

ステップ 1 Cisco Unified Communications Manager 管理で、 **システム** > **サービス パラメータ**に移動します。

ステップ 2 [Clusterwide Parameters (System - Location and Region)] で、[Use Video BandwidthPool for Immersive Video Calls] を [False]に設定します。

ステップ 3 [Clusterwide Parameters (Call Admission Control)] で、[Video Call QoS Marking Policy] を [Promote to Immersive]に設定します。

ステップ 4 変更を保存します。

Cisco Unified Communications Manager の連携

Cisco Unified Communications Manager 通話会議やルート計画などの機能のための IP テレフォニー システムのコンポーネント (エンドポイント、アクセス ゲートウェイ、リソース) を管理します。

Cisco DX シリーズ デバイスは Cisco Unified Communications Manager リリース 8.5 (1), 8.6 (2), 9.1 (2), 10.5 (1) 以降でサポートされます。

Cisco Unified Communications Manager デバイスがデータベースに登録され構成されるまで、デバイスを認識できません。

Cisco Unified Communications Manager アドミニストレーション ガイド で IP デバイスを操作するための Cisco Unified Communications Manager の設定の詳細については、『*Cisco Unified Communications Manager* システム ガイド』、および『*Cisco DX Series Wireless LAN* 導入ガイド』 を参照してください。

WLAN 通信の 802.11 規格

ワイヤレス LAN は、すべてのイーサネット ベースのワイヤレス トラフィックを制御するプロトコルを定義する米国電気電子学会 (IEEE) 802.11 標準に準拠する必要があります。Cisco DX シリーズ デバイスは次の標準をサポートしています。

- 802.11a：5 GHz 周波数帯を使用して OFDM テクノロジーを使用することで、より多くのチャネルを提供し、データ レートを向上させます。 Dynamic Frequency Selection（DFS）および伝送パワー制御（TPC）は、この規格をサポートしています。
- 802.11b：低データ レート（1、2、5.5、11 Mbps）でデータを送受信するために 2.4 GHz の無線周波数（RF）を指定します。
- 802.11d：アクセス ポイントが、現在サポートされている無線チャネルおよび送信電力レベルを通知できるようにします。 802.11d が有効なクライアントは、その情報を使用して使用するチャネルと電力を決定します。 特定の国で合法的に許可されているチャネルを判断するには、デバイスにワールド モード (802.11d) が必要です。 サポートされているチャネルについては、次の表を参照してください。 Cisco IOS アクセス ポイントまたは Cisco Unified Wireless LAN Controller で 802.11d が適切に設定されていることを確認してください。
- 802.11e：無線 LAN アプリケーションの一連の Quality of Service（QoS）拡張を定義します。
- 802.11g：802.11b と同じ免許不要の 2.4 GHz 周波数帯を使用します。ただし、直交周波数分割多重方式（OFDM）テクノロジーを使用することで、データ レートを高め、より高い

パフォーマンスを提供します。 OFDM は、RF を使用して信号を伝送するための物理層の符号化テクノロジーです。

- 802.11h: 5 GHz スペクトルと送信電力の管理。 802.11a メディア アクセス コントロール（MAC）に、DFS と TPC を提供します。
- 802.11i：無線ネットワークにセキュリティ メカニズムを指定します。
- 802.11n: データの送受信に 2.4 GHz または 5 GHz の無線周波数を使用し、MIMO (複数入力複数出力) テクノロジ、チャネル ボンディング、ペイロード最適化を使用することでデータ転送を強化します。

（注） Cisco DX シリーズ デバイスには単一のアンテナがあり、MCS 0 ～ MCS 7 のデータ レート (20 MHz チャネルで 72 Mbps、40 MHz チャネルで 150 Mbps) のみをサポートするシングル入力シングル出力 (SISO) システムを使用します。 より高いデータ レートを利用可能な MIMO テクノロジーを 802.11n クライアントが使用している場合は、オプションとして MCS 8 ～ MCS 15 を有効にすることができます。

表 *10 : Cisco DX* シリーズ デバイスでサポートされているチャネル

帯域範囲	使用可能なチャネル	チャネル セット
2.412 ～ 2.472 GHz	13	1 - 13
5.180 ～ 5.240 GHz	4	36, 40, 44, 48
5.260 ～ 5.320 GHz	4	52, 56, 60, 64
5. 500 ～ 5.700 GHz	11	100 - 140
5.745 ～ 5.825 GHz	5	149, 153, 157, 161, 165

（注） （注）チャネル 120、124、128 はアメリカ、ヨーロッパ、日本ではサポートされていませんが、他の地域ではサポートされている場合があります。

WLANのサポートされているデータ レート、送信電力、および受信感度については、『『*Cisco DX Series Wireless LAN* 導入ガイド』』を参照してください。

ワールド モード（802.11d）

Cisco DX シリーズ デバイスは 802.11d を使用して、使用するチャネルと送信電力レベルを決定します。 デバイスは、関連付けられた AP からクライアント構成を継承します。 デバイスをワールド モードで使用するには、AP でワールド モード (802.11d) を有効にします。 ワールド モードを有効にする方法の詳細については、『*Cisco DX Series Wireless LAN* 導入ガイド』

（注） 周波数が 2.4GHz で、現在のアクセス ポイントが 1 ～ 11 のチャネルで送信している場合は、ワールド モード (802.11d) を有効にする必要がない場合があります。

すべての国でこれらの周波数はサポートされているため、ワールドモード（802.11d）をサポートしているかどうかに関係なくこれらのチャネルのスキャンを試行できます。2.4GHzをサポートしている国については、『*Cisco DX Series Wireless LAN* 導入ガイド』 をご覧ください。

アクセスポイントが設置されている国に応じて、ワールドモード（802.11d）を有効にします。ワールド モードは、Cisco Unified Wireless LAN Controller に対して自動的に有効になります。

無線変調技術

無線通信では、信号送信に次の変調技術が使用されます。

直接拡散スペクトル（DSSS）

信号を周波数範囲または帯域幅全体に拡散することで干渉を防止します。 DSSS テクノロジーは、複数のデバイスが干渉なく通信できるように、データの断片を複数の周波数にわたって多重化します。 各デバイスには、デバイスのデータ パケットを識別する特別なコードがあり、その他のデータ パケットはすべて無視されます。 Cisco ワイヤレス 802.11b/g 製品は、DSSS テクノロジーを使用して WLAN 上の複数のデバイスをサポートします。

直交周波数分割多重方式（OFDM）

RF を使用して信号を送信します。 OFDM は、1 つの高速データ キャリアを複数の低速キャリアに分割し、RF スペクトル全体で並列に送信する物理層エンコーディング技術です。 802.11g および 802.11a と組み合わせて使用すると、OFDM は最大 54Mbps のデータ レートをサポートできます。

次の表は、データ レート、チャネル数、変調技術を規格別に比較したものです。

表 *11 : IEEE* 規格によるデータレート、チャネル数、変調技術

項目	802.11b	802.11g	802.11a	802.1
データレート	1、2、5.5、11Mbps	6、9、12、18、24、36、48、54Mbps	6、9、12、18、24、36、48、54Mbps	• •

項目	802.11b	802.11g	802.11a	802.11n
重複しないチャネル	3	3	最大 24	最大 24
無線変調	DSSS	OFDM	OFDM	OFDM

無線周波数範囲

WLAN 通信では、次の無線周波数（RF）範囲が使用されます。

- 2.4GHz: 2.4GHz を使用する多くのデバイスは、802.11b/g 接続に干渉する可能性があります。 干渉によってサービス妨害（DoS）シナリオが発生する可能性があり、正常な 802.11 伝送が阻止されるおそれがあります。
- 5GHz: この範囲は、UNII (Unlicensed National Information Infrastructure) バンドと呼ばれる複数のセクションに分かれており、各セクションには 4 つのチャネルがあります。 チャネルは 20 MHz 間隔で配置され、重複しないチャネルと 2.4GHz よりも多くのチャネルを提供します。

WLAN 通信のセキュリティ

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 における音声通信のセキュリティは非常に重要です。 侵入者が音声トラフィックを操作したり傍受したりできないようにするために、Cisco SAFE セキュリティ アーキテクチャはデバイスと Cisco Aironet AP をサポートしています。 Cisco DX シリーズ ネットワークでのセキュリティの詳細については、http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html を参照してください。

認証方法

Cisco ワイヤレス IP テレフォニー ソリューションは、デバイスがサポートする次の認証方法を使用して、不正なサインインや通信の侵害を防ぐワイヤレス ネットワーク セキュリティを提供します。 Cisco DX シリーズ

WLAN 認証

- WPA（802.1x 認証 + TKIP または AES 暗号化）
- WPA2（802.1x 認証 + AES または TKIP 暗号化）
- WPA-PSK（事前共有キー + TKIP 暗号化）
- WPA2-PSK（事前共有キー + AES 暗号化）
- Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling（EAP-FAST）
- Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）
- PEAP（Protected Extensible Authentication Protocol）MS-CHAPv2 および GTC

- CCKM（Cisco Centralized Key Management）
- Open

WLAN 暗号化

- AES（Advanced Encryption Scheme）
- Temporal Key Integrity Protocol/Message Integrity Check（TKIP/MIC）
- WEP（Wired Equivalent Protocol）40/64 および 104/128 ビット

（注） 802.1x 認証を使用した動的 WEP および共有キー認証はサポートされません。

認証方式の詳細については、『『*Cisco DX Series Wireless LAN* 導入ガイド』』の「「Wireless Security」」の項を参照してください。

認証キー管理

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 およびデバイスに格納されている WPA 事前共有キーよりも高いセキュリティを提供します。
- Cisco Centralized Key Management（CCKM）：RADIUS サーバとワイヤレス ドメイン サーバ（WDS）の情報を使用して、キーの管理および認証をします。 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。

WPA/WPA2 および CCKM では、暗号キーはデバイスに入力されず、AP とデバイス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、各デバイスに入力する必要があります。

暗号化方式

音声トラフィックの安全性を確保するために、Cisco DX シリーズ デバイスは暗号化に WEP、TKIP、および AES をサポートしています。 これらのメカニズムが暗号化に使用される場合、AP とデバイスの間で音声 Real-Time Transport Protocol（RTP）パケットが暗号化されます。

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。 接続を成功させるには、デバイスに設定されている WEP キーが、AP で設定されている WEP キーと一致する必要があります。 デバイスは、40 ビット暗号化または 128 ビット暗号化を使用し、デバイスと AP 上で静的に保持される WEP キーをサポートします。

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。

暗号化方式の詳細については、『『*Cisco DX Series Wireless LAN* 導入ガイド』』の「「Wireless Security」」の項を参照してください。

AP 認証および暗号化のオプション

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 とデバイスに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、事前共有キーをデバイスに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 DX シリーズ デバイスは自動 EAP ネゴシエーションをサポートしていないため、EAP-FAST モードを使用するには、これを指定する必要があります。

次の表は、デバイスがサポートする Cisco Aironet AP で設定されている認証および暗号化方式の一覧を示します。 この表には、AP の設定に対応するデバイスのネットワーク設定オプションを示します。

表 *12*：認証方式と暗号化方式

Cisco WLAN の設定			**Cisco DX シリーズ 構成**
認証（Authentication）	キー管理	共通の暗号化	認証（Authentication）
Open	None	None	None
Static WEP	None	WEP	WEP
[EAP-FAST]	WPA または WPA2 とオプションの CCKM	TKIP または AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA または WPA2 とオプションの CCKM	TKIP または AES	802.1x EAP > PEAP > MSCHAPV2

Cisco WLAN の設定			Cisco DX シリーズ 構成
PEAP-GTC	WPA または WPA2 とオプションの CCKM	TKIP または AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA または WPA2 とオプションの CCKM	TKIP または AES	802.1x EAP > TLS
WPA/WPA2-PSK	WPA-PSK または WPA2-PSK	TKIP または AES	WPA/WPA2 PSK

Cisco WLAN セキュリティの詳細については、http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html を参照してください。

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。

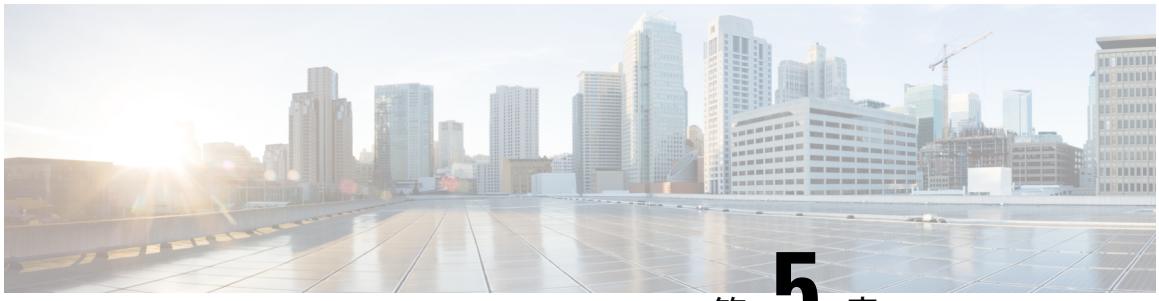
http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

WLAN とローミング

Cisco DX シリーズデバイスは、Cisco Centralized Key Management（CCKM）をサポートします。これは、ワイヤレス ドメイン サーバ（WDS）上でセッション クレデンシャルのキャッシュを提供する集中型キー管理プロトコルです。

CCKM の詳細については、次の URL にある『*Cisco Fast Secure Roaming Application Note*』を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html



第 5 章

展開

- 設定ファイル （39 ページ）
- MAC アドレスを決定する （40 ページ）
- Cisco Unified Communications Manager デバイスの追加方法 （40 ページ）
- Cisco Unified Communications Manager のユーザーの追加 （44 ページ）
- デバイスモデルを確認する （45 ページ）
- 回線設定を構成する （46 ページ）
- ユーザーとデバイスの関連付け （47 ページ）
- Survivable Remote Site Telephony （48 ページ）

設定ファイル

TFTP サーバは、接続のパラメータを定義するデバイス設定ファイルをCisco Unified Communications Managerに保存します。 一般に、Cisco Unified Communications Manager でデバイスのリセットが必要となる変更を行うと、設定ファイルも自動的に変更されます。

構成ファイルには、デバイスが実行する必要があるイメージのロードに関する情報も含まれています。 このイメージ ロードがデバイスに現在ロードされているものと異なる場合、デバイスは TFTP サーバに接続して必要なロード ファイルを要求します。 イメージのロードサイズが大きいため、デバイスと TFTP サーバ間の TCP ポート 6970 が開いている必要があります。

次の条件が存在する場合、デバイスは TFTP サーバから XmlDefault.cnf.xml という名前のデフォルト構成ファイルにアクセスします。

- 自動登録を有効にします Cisco Unified Communications Manager。
- デバイスを Cisco Unified Communications Manager データベースに追加していません。
- デバイスが初めて登録されます。

（注） 設定ファイル内のデバイス セキュリティー モードが認証済みまたは暗号化済みに設定されているが、デバイスが CTL ファイルまたは ITL ファイルを受信していない場合、デバイスは安全に登録するためにファイルの取得を 4 回試行します。

自動登録が有効になっておらず、デバイスがデータベースに追加されていない場合、登録要求は拒否されます。 Cisco Unified Communications Manager デバイスの画面に サービス外 と表示されます。

Cisco DX シリーズ デバイスは構成ファイル SEPmac_address.cnf.xml にアクセスします。ここで、mac_address はデバイスの Ethernet MAC アドレスです。 CTL または ITL ファイルがインストールされている場合、デバイスは代わりに SEPmac_address.cnf.xml.sgn という名前の構成ファイルにアクセスします。 デバイスが最初に設定されるとき、Cisco Unified Communications Manager管理の**電話の設定**ウィンドウ内の**説明**フィールドは事前に入力されます。 MAC アドレスはデバイスを一意に識別します。

MAC アドレスを決定する

デバイスの MAC アドレスは次の方法で確認できます。

手順

- デバイスから、**[アプリケーション]**>**[設定]**>**[デバイス情報]**>**[ステータス]** をタップし、**[イーサネット MAC アドレス]** フィールドを確認します。
- デバイスの背面にある MAC ラベルを確認します。
- デバイスの Web ページを表示し、 **デバイス情報** ハイパーリンクをクリックします。

Cisco Unified Communications Manager デバイスの追加方法

デバイスをインストールする前に、エンドポイントをデータベースに追加する方法を選択する必要があります。 Cisco Unified Communications Manager

次の表は、データベースにデバイスを追加する方法の概要を示しています。 Cisco Unified Communications Manager

表 *13 : Cisco Unified Communications Manager* にデバイスを追加する方法

方法	MAC アドレスが必要ですか?	注記
自動登録	未対応	ディレクトリ番号が自動的に割り当てられます。
自動登録電話サポートツール (TAPS) による自動登録	未対応	自動登録と一括管理ツールが必要です。デバイスと Cisco Unified Communications Manager 管理の情報が更新されます。
Cisco Unified Communications Manager の管理	対応	デバイスを個別に追加する必要があります。

方法	MAC アドレスが必要ですか?	注記
Cisco Unified Communications Manager 一括管理ツール	対応	複数のデバイスの同時登録が可能です。
セルフプロビジョニング	未対応	ユーザが独自のデバイスをプロビジョニングできるようにします。

自動登録

デバイスのインストールを開始する前に自動登録を有効にすると、次のことが可能になります。

- 事前にデバイスから MAC アドレスを収集せずにデバイスを追加します。
- デバイスを IP テレフォニー ネットワークに物理的に接続すると、デバイスがデータベースに自動的に追加されます。 Cisco Unified Communications Manager 自動登録時に、Cisco Unified Communications Manager は、次に使用可能な電話番号を順にデバイスに割り当てます。
- デバイスを Cisco Unified Communications Manager データベースに素早く入力し、Cisco Unified Communications Manager からディレクトリ番号などの設定を変更します。
- 自動登録されたデバイスを新しい場所に移動し、ディレクトリ番号に影響を与えずに別のデバイス プールに割り当てます。

（注） Cisco では、自動登録を使用してネットワークに追加するデバイスが 100 台未満であることをお勧めします。 100 台を超えるデバイスをネットワークに追加するには、一括管理ツールを使用します。

自動登録は、デフォルトでは無効になっています。 Cisco Unified Communications Manager で説明されているように、場合によっては、自動登録を使用しないこともあります。たとえば、デバイスに特定のディレクトリ番号を割り当てる場合や、『*Cisco Unified Communications Manager* セキュリティ機能』でセキュリティ保護された接続を使用する場合などです。 自動登録を有効にする方法については、『*Cisco Unified Communications Manager* セキュリティ機能』の「「自動登録の設定」」セクションを参照してください。

自動登録と TAPS

事前にデバイスから MAC アドレスを収集しなくても、自動登録と TAPS (自動登録電話サポート ツール) を使用してデバイスを追加できます。

TAPS は一括管理ツールと連携して、ダミーの MAC アドレスを使用してデータベースにすでに追加されているデバイスのバッチを更新します。 Cisco Unified Communications Manager TAPS を使用して MAC アドレスを更新し、定義済みの構成をダウンロードします。

（注） Cisco では、ネットワークに 100 台未満のデバイスを追加する場合は、自動登録と TAPS を使用することをお勧めします。 100 台を超えるデバイスをネットワークに追加するには、一括管理ツールを使用します。

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。プロセスが完了すると、デバイスにはディレクトリ番号とその他の設定が含まれ、デバイスはCisco Unified Communications Manager正しい MAC アドレスで管理で更新されます。

TAPS が機能するには、 Cisco Unified Communications Manager 管理（**システム** > **Cisco Unified CM**）で自動登録を有効にする必要があります。

（注） 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、自動登録は自動的に無効になります。 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は有効になりません。

詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*（*Cisco Unified* コミュニケーションマネージャー一括管理ガイド）』を参照してください。

Cisco Unified Communications Manager でデバイスを追加する

デバイスを個別にデータベースに追加できます。 Cisco Unified Communications Manager そのためには、まず各デバイスの MAC アドレスを取得する必要があります。

手順

ステップ 1 MAC アドレスを収集したら、 Cisco Unified Communications Manager 管理で、 **デバイス** > **電話** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[電話の種類]** ドロップダウン リスト ボックスからデバイスの種類を選択します。

（注）
バージョンによっては、デバイスを追加するときに、ファームウェアをインストールする前にデバイス イネーブラーをインストールする必要がある場合があります。 Cisco Unified Communications ManagerCisco DX シリーズ

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 デバイス固有のパラメータ (デバイス プール、デバイス セキュリティ プロファイルなど) の詳細を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

詳細については、『 *Cisco Unified Communications Manager* システム ガイド』の「システム設定の概要」の章を参照してください。

一括管理ツールの電話テンプレートを使用してデバイスを追加する

Cisco Unified Communications Manager 一括管理ツールを使用すると、複数のデバイスの登録などの一括操作を実行できます。

一括管理ツールの詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*（*Cisco Unified* コミュニケーションマネージャー一括管理ガイド）』 を参照してください。

手順

ステップ 1 各デバイスの MAC アドレスを取得します。

ステップ 2 Cisco Unified Communications Managerから **一括管理** > **電話** > **電話テンプレート**を選択します。

ステップ 3 [新規追加] をクリックします。

ステップ 4 電話の種類を選択し、 **[次へ]** を選択します。

ステップ 5 デバイス プールやデバイス セキュリティ プロファイルなどのデバイス固有のパラメータの詳細を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 Cisco Unified Communications Manager 管理から、**デバイス** > **電話** > **新規追加**を選択し、既存の一括管理ツール テンプレートを使用してデバイスを追加します。

セルフプロビジョニング

セルフプロビジョニングにより、ユーザは管理者の手間を省いてデバイスをセットアップできます。セルフプロビジョニングが有効になっている場合、ユーザはデバイスのセットアップ中に資格情報を入力します。デバイスのMACアドレスおよびその他の構成情報は、Cisco Unified Communications Manager サーバと共有されます。

セルフプロビジョニングにはCisco Unified Communications Manager リリース 10.0 以降が必要です。 詳細については、*Cisco Unified Communications Manager* アドミニストレーション ガイドの「セルフプロビジョニング」の章を参照してください。

セルフプロビジョニングを有効にする

手順

ステップ 1 Cisco Unified Communications Manager 管理で **ユーザー管理** > **ユーザー設定** > **ユーザープロファイル**に移動します。

ステップ 2 セルフプロビジョニングを **有効に設定します**。

ステップ 3 **[ユーザー管理]** > > **[エンドユーザー]** の順に選択します。

ステップ 4 セルフサービス ユーザ ID を設定します。[

ステップ 5 **ユーザ管理** > **セルフプロビジョニング** に移動して、認証モードを選択します。

Cisco Unified Communications Manager のユーザーの追加

このセクションでは、 Cisco Unified Communications Manager にユーザを追加する手順について説明します。 オペレーティング システムとユーザを追加する方法に応じて、このセクションのいずれかの手順に従います。

Cisco Unified Communications Manager へのユーザの直接追加

LDAP ディレクトリを使用していない場合は、Cisco Unified Communications Manager に直接ユーザを追加できます。

（注） LDAP が同期されている場合、 Cisco Unified Communications Manager にユーザを追加することはできません。

手順

ステップ 1 **[ユーザ管理]** > **[エンドユーザ]** を選択し、 **[新規追加]** をクリックします。
[**エンド ユーザーの設定**（**End User Configuration**）] ウィンドウが表示されます。

ステップ 2 このウィンドウの「ユーザ情報」ペインで、次の情報を入力します。

- ユーザ ID - エンドユーザの識別名を入力します。 Cisco Unified Communications Manager 作成後のユーザ ID の変更は許可されません。 姓に使用できる特殊文字は、**=**、**+**、**<**、**>**、**#**、**;**、****、**""**、および空白です。
- パスワードとパスワードの確認 - 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 - エンドユーザの姓を入力します。使用できる特殊文字は =、+、<、>、#、;、\、"" および空白スペースです。
- 電話番号 - エンドユーザの主要なディレクトリ番号を入力します。 エンド ユーザはデバイス上で複数の回線を持つことができます。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 デバイスモデルを確認する （45 ページ） に進みます。

外部 LDAP ディレクトリからユーザを追加する

LDAP ディレクトリ（Cisco Unified Communications Server 以外のディレクトリ）にユーザを追加した場合は、次の手順に従って、そのディレクトリを、同じユーザとデバイスを追加している Cisco Unified Communications Manager にただちに同期できます。

手順

ステップ 1 Cisco Unified Communications Manager 管理にログインします。

ステップ 2 **[システム（System）]** > **[LDAP]** > **[LDAP ディレクトリ（LDAP Directory）]** の順に選択します。

ステップ 3 LDAP ディレクトリを見つけるには、 **検索** ボタンを使用します。

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。

（注）
LDAP ディレクトリをすぐに同期する必要がない場合は、LDAP ディレクトリ ウィンドウの LDAP ディレクトリ同期スケジュールによって、次回の自動同期のスケジュールが決まります。 Cisco Unified Communications Manager ただし、新しいユーザをデバイスに関連付ける前に、同期を行う必要があります。

ステップ 6 デバイスモデルを確認する （45 ページ） に進みます。

デバイスモデルを確認する

手順

ステップ 1 Cisco Unified Communications Manager [管理] から、[**デバイス** > **電話**] を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[電話の種類]** ドロップダウン リストからデバイス モデルを選択し、**[次へ]** をクリックします。[電話の設定（Phone Configuration）]ウィンドウが表示されます。

ステップ 4 回線設定を構成する （46 ページ） に進みます。

回線設定を構成する

電話の設定 ウィンドウでは、ほとんどのフィールドでデフォルト値を使用できます。

手順

ステップ 1 **[電話の設定]** ウィンドウで、ウィンドウの左側のペインにある **[回線 1]** をクリックします。[電話番号の設定（Directory Number Configuration）]ウィンドウが表示されます。

ステップ 2 **[ディレクトリ番号]** フィールドに、**[ユーザー設定]** ウィンドウの **[電話番号]** フィールドに表示されるのと同じ番号を入力します。

ステップ 3 **[ルート パーティション]** ドロップダウン リストから、ディレクトリ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 [<None>] を選択します。

ステップ 4 **[Calling Search Space]** ドロップダウン リスト（ **[Directory Number Configuration]** ウィンドウの [Directory Number Settings] ペイン）から、適切なコール検索スペースを選択します。 コーリング サーチ スペースは、この電話番号からコールが行われる番号を検索するパーティションの集合から構成されています。 選択した値は、このディレクトリ番号を使用するすべてのデバイスに適用されます。

ステップ 5 **[ディレクトリ番号設定]** ウィンドウの **[コール転送設定]** ペインで、項目 ([全転送]、[話中転送 (内部)] など) と、コールの送信先となる対応する宛先を選択します。

例：

話し中信号を受信した内部および外部の着信通話をこの回線のボイスメールに転送する場合は、[通話転送設定] ペインの **[ボイスメール]** ボックスをオンにします。

ステップ 6 **[電話番号設定]** ウィンドウの [デバイス] ペインにある [**回線 1**] フィールドで、以下を設定します。

a) 表示 (**内線発信者 ID** フィールド): このデバイスのユーザの名と姓を入力すると、この名前がすべての内部通話で表示されます。 このフィールドを空白のままにして、システムに電話の内線番号を表示させることもできます。

b) [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 文字の数字と「X」文字を入力できます。 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 555902XXXX, 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 5559026640 が表示されます。

c) **[保存（Save）]** をクリックします。

（注）
設定は、**[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)]** ボタン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が表示されるのは、他のデバイスがこの電話番号を共有している場合だけです）。

ステップ 7 設定している回線にユーザを関連付けるには、ウィンドウの下部にある **[エンド ユーザの関連付け]** 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にチェックを入れ、 **[選択した項目を追加]** を選択します。**[電話番号の設定]** ウィンドウの [回線に関連付けられているユーザ] ペインに、ユーザ名とユーザ ID が表示されます。

c) **[保存（Save）]** をクリックします。

これで、ユーザはデバイスの Line 1 に関連付けられました。

ステップ 8 デバイスに 2 番目の回線がある場合は、回線 2 を設定します。

ステップ 9 ユーザーとデバイスの関連付け （47 ページ） に進みます。

ユーザーとデバイスの関連付け

手順

ステップ 1 Cisco Unified Communications Manager 管理から、 **ユーザ管理 > エンドユーザを選択します。**[ユーザーの検索と一覧表示（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 [**デバイスの関連付け（Device Association**）] 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。

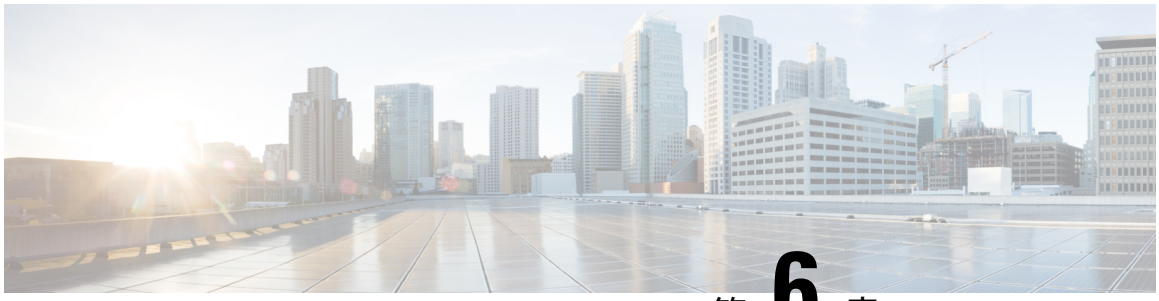
ステップ 8 [関連リンク（Related Links）]ドロップダウン リストで [ユーザの設定に戻る（Back to User）] を選択し、[検索（Go）]をクリックします。
[エンド ユーザ構成] ウィンドウが表示され、選択した関連デバイスが [制御されたデバイス] ペインに表示されます。

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、Cisco Unified Communications Manager 制御側との通信が切断された場合でも、基本的な通話機能にアクセスできることを保証します。 このシナリオでは、デバイスは進行中の通話をアクティブに保つことができ、ユーザは利用可能な機能のサブセットにアクセスできます。 フェイルオーバーが発生すると、ユーザはデバイス上で警告メッセージを受け取ります。 SRST には、Cisco IOS バージョン 12.4 (20) 以上が必要です。

（注） SRST は IPv6 をサポートしていません。



第 6 章

インストール

- Cisco DX シリーズデバイスのインストール （49 ページ）
- 無線 LAN の設定 （51 ページ）
- ネットワーク設定の構成 （52 ページ）
- 起動プロセス （65 ページ）
- 起動検証 （68 ページ）

Cisco DX シリーズデバイスのインストール

デバイスをデータベースに追加したら、デバイスのインストールを完了できます。 Cisco Unified Communications Manager あなた (またはユーザ) は、ユーザの場所にデバイスをインストールできます。

（注） デバイスをインストールする前に、たとえ新しいデバイスであっても、デバイスを最新のファームウェア イメージにアップグレードしてください。 アップグレードの詳細については、次の場所にあるデバイスの Readme ファイルを参照してください。

http://software.cisco.com/download/release.html?mdfid=284721679&flowid=46173&softwareid=282074288

デバイスがネットワークに接続すると、デバイスの起動プロセスが開始され、デバイスが登録されます Cisco Unified Communications Manager。 デバイスのインストールを完了するには、DHCP サービスを有効にするか無効にするかに応じて、デバイスのネットワーク設定を構成します。

自動登録を使用した場合は、デバイスをユーザに関連付けたり、ディレクトリ番号を変更したりするなど、デバイスの特定の設定情報を更新する必要があります。

次の手順では、デバイスのインストール タスクの概要とチェックリストを示します。 Cisco DX シリーズ 手順では、デバイスのインストールをガイドするための推奨順序を示します。 一部のタスクは、システムとユーザのニーズに応じてオプションになります。

手順

ステップ 1 電源を選択してください。

- 外部電源
- [Cisco DX650のみ] Power over Ethernet (PoE)

（注）
PoE+ 802.3at では、マウスやキーボードなど、デバイスに接続されたアクセサリが電力をネゴシエートします。アクセサリに十分な電力が供給されていない場合は、画面にエラーメッセージが表示されます。 デバイスを WLAN 環境で使用する場合は、外部電源が必要です。

ステップ 2 デバイスを組み立て、ネットワーク ケーブルを接続します。 デバイスを WLAN 環境で使用する場合は、手順 5 を参照してください。
この手順では、ネットワーク内でデバイスを検索してインストールします。

ステップ 3 デバイスの起動プロセスを監視します。 この手順では、プライマリおよびセカンダリ ディレクトリ番号と、ディレクトリ番号に関連付けられている機能をデバイスに追加し、デバイスが適切に設定されていることを確認します。

ステップ 4 デバイスをワイヤレス ネットワークに展開することを選択した場合は、手順 5 に進みます。

IP ネットワーク用にデバイス上でイーサネット ネットワーク設定を構成する場合、DHCP を使用するか、IP アドレスを手動で入力してデバイスの IP アドレスを設定できます。

ステップ 5 デバイスをワイヤレス ネットワークに展開することを選択した場合は、次の操作を実行する必要があります。

- ワイヤレス ネットワークを構成します。
- Cisco Unified Communications Manager 管理のデバイスに対してワイヤレス LAN を有効にします。
- デバイスでワイヤレス ネットワーク プロファイルを構成します。

（注）
デバイスにイーサネット ケーブルが接続されていると、デバイスの無線 LAN はアクティブになりません。

ステップ 6 デバイスで通話を発信し、通話アプリケーションと機能が正しく動作することを確認します。

ステップ 7 エンドユーザにデバイスの使用方法と構成方法に関する情報を提供します。

無線 LAN の設定

無線 LAN が展開されている場所の Wi-Fi カバレッジが、ビデオ パケットと音声パケットの送信に適していることを確認します。

ワイヤレス ネットワークの構成に関する詳細については、『*Cisco DX Series Wireless LAN* 導入ガイド』 を参照してください。

Cisco Unified Communications Manager 管理でのワイヤレス LAN の設定

Cisco Unified Communications Managerでは、デバイスの 「Wi-Fi」 というパラメータを有効にする必要があります。 このパラメータは、 Cisco Unified Communications Manager 管理の次のいずれかの場所で有効にできます。

- 特定のデバイスでワイヤレス LAN を有効にするには、特定のデバイスの製品固有の設定レイアウト セクション (**デバイス** > **電話**) で Wi-Fi パラメータに対して**有効**を選択し、**共通設定の上書き** をオンにします。
- デバイスのグループに対してワイヤレス LAN を有効にするには、**共通の電話プロファイルの設定**ウィンドウ (**デバイス** > **デバイス設定** > **共通の電話プロファイル**) で Wi-Fi パラメータに対して**有効**を選択し、**共通設定の上書き**をオンにして、デバイス (**デバイス** > **電話**) を共通の電話プロファイルに関連付けます。
- ネットワーク内のすべての WLAN 対応デバイスに対してワイヤレス LAN を有効にするには、**エンタープライズ電話の構成**ウィンドウ (**システム** > **エンタープライズ電話の構成**) で Wi-Fi パラメータに対して**有効**を選択し、**共通設定の上書き**をオンにします。

（注） Cisco Unified Communications Manager管理の**電話設定**ウィンドウ (**デバイス** > **電話**)で、Ethernet MAC アドレスを使用して MAC アドレスを設定します。Cisco Unified Communications Manager 登録ではワイヤレス MAC アドレスは使用されません。

ワイヤレス LAN プロファイルのプロビジョニング

手順

ステップ 1 Cisco Unified Communications Manager 管理で、 **デバイス** > **電話** > **ワイヤレス LAN プロファイル**を選択します。

ステップ 2 ワイヤレス LAN プロファイルを設定し、 **[保存]** をクリックします。

ワイヤレス LAN プロファイルグループのプロビジョニング

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**デバイス** > **電話** > **ワイヤレス LAN プロファイル グループ**を選択します。

ステップ 2 ワイヤレス LAN プロファイル グループを構成し、**[保存]** をクリックします。

ステップ 3 **[システム]** > **[デバイス プール]** を選択し、ワイヤレス LAN プロファイル グループをデバイス プールに追加して、**[保存]** をクリックします。 または、**[デバイス]** > **[電話]** を選択し、ワイヤレス LAN プロファイル グループを特定のデバイスに追加して、**[保存]** をクリックします。

ネットワーク設定の構成

ネットワークでDHCPを使用していない場合は、デバイスをネットワークにインストールした後、デバイス上で次のネットワーク設定を構成する必要があります。

- IP アドレス(IP address)
- IP サブネット情報
- IPv6 アドレス
- TFTP サーバの IP アドレス

必要に応じて、ドメイン名と DNS サーバ設定値も設定できます。

IPv4 の設定

手順

ステップ 1 設定アプリケーションで、 **イーサネット** > **IPv4 構成**をタップします。

ステップ 2 **静的 IP を使用する** にチェックを入れます。

ステップ 3 次のオプションを設定します。

- IP アドレス(IP address)
- ゲートウェイ（Gateway）
- ネットマスク（Netmask）
- ドメイン名（Domain Name）

（注）
オプション 15 を使用すると、複数のドメイン名をデバイスに送信できます。 各ドメイン名はスペースで区切る必要があります。 カンマなどの他の区切り文字はサポートされてい

ません。 静的 IP アドレスを使用している場合は、ドメイン名を手動で入力することもできます。 ここでも、有効な区切り文字はスペースのみです。 現在、オプション 119 はサポートされていません。

- DNS 1
- DNS 2

IPv4 を更新する

手順

設定アプリケーションで、 **イーサネット** > **IPv4 を更新する**をタップします。

IPv6 の設定

手順

ステップ 1 設定アプリケーションで、 **イーサネット** > **IPv6 構成**をタップします。

ステップ 2 **静的 IP を使用する** にチェックを入れます。

ステップ 3 次のオプションを設定します。

- IP アドレス(IP address)
- [デフォルト ルータ（Default router）]
- プレフィックス長
- ドメイン名（Domain Name）

（注）
オプション 15 を使用すると、複数のドメイン名をデバイスに送信できます。 各ドメイン名はスペースで区切る必要があります。 カンマなどの他の区切り文字はサポートされていません。 静的 IP アドレスを使用している場合は、ドメイン名を手動で入力することもできます。 ここでも、有効な区切り文字はスペースのみです。 現在、オプション 119 はサポートされていません。

- DNS 1
- DNS 2

IPv6 を更新する

手順

設定アプリケーションで、**[イーサネット]** > **[IPv6 を更新する]**をタップします。

イーサネット Web プロキシを構成する

手順

ステップ 1 設定アプリケーションで、 **イーサネット** > **プロキシ設定**をタップします。

ステップ 2 プロキシ設定の種類を選択します。

a) 手動プロキシを設定するには、プロキシ ホスト名、プロキシ ポート、およびプロキシ バイパスを入力します。 該当する場合は、 **プロキシに認証が必要** をチェックします。

b) 自動プロキシを設定するには、PAC の場所とプロキシ バイパスを入力します。 該当する場合は、 **プロキシに認証が必要** をチェックします。

管理 VLAN を設定する

手順

ステップ 1 設定アプリケーションで、 **イーサネット** > **管理 VLAN**をタップします。

ステップ 2 管理 VLAN ID 値を入力し、 **[OK]**をタップします。

SW ポート速度の設定

手順

ステップ 1 設定アプリケーションで、**イーサネット** > **SW ポート速度**をタップします。

ステップ 2 ポート速度を選択します。

デバイスがスイッチに接続されている場合は、スイッチのポートをデバイスと同じ速度/デュプレックスに設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定を変更する場合は、PC ポート速度を同じ設定に変更する必要があります。

PC ポート速度の設定

手順

ステップ 1 設定アプリケーションで、**イーサネット** > **PC ポート速度**をタップします。

ステップ 2 ポート速度を選択します。

デバイスがスイッチに接続されている場合は、スイッチのポートをデバイスと同じ速度/デュプレックスに設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定を変更する場合は、SW ポート速度を同じ設定に変更する必要があります。

Wi-Fi ネットワークに接続する

手順

ステップ 1 設定アプリケーションで、 **Wi-Fi** をオンに切り替えます。

ステップ 2 **Wi-Fi**をタップします。

ステップ 3 使用可能なネットワークのリストからワイヤレス ネットワークを選択します。

ステップ 4 資格情報を入力し、 **[接続]** をタップします。

非表示の Wi-Fi ネットワークに接続する

手順

ステップ 1 設定アプリケーションで、 **Wi-Fi** をオンに切り替えます。

ステップ 2 **Wi-Fi をタップします。**

ステップ 3 **+をタップします。**

ステップ 4 ネットワーク SSID を入力し、セキュリティ タイプと資格情報 (該当する場合) を選択します。

ステップ 5 **保存**をタップします。

Wi-Fi Web プロキシを構成する

手順

ステップ 1 設定アプリケーションで、 **Wi-Fi をタップします**。
ステップ 2 利用可能なネットワークのリストからワイヤレス ネットワークを長押ししてタップします。
ステップ 3 **ネットワークの変更をタップします**。
ステップ 4 **詳細オプションを表示** をチェックします。
ステップ 5 プロキシ設定の種類を選択します。

a) 手動プロキシを設定するには、プロキシ ホスト名、プロキシ ポート、およびプロキシ バイパスを入力します。 該当する場合は、 **プロキシに認証が必要** をチェックします。
b) 自動プロキシを設定するには、PAC の場所とプロキシ バイパスを入力します。 該当する場合は、 **プロキシに認証が必要** をチェックします。

ステップ 6 **保存**をタップします。

Wi-Fi IP 設定を構成する

手順

ステップ 1 設定アプリケーションで、 **Wi-Fi をタップします**。
ステップ 2 利用可能なネットワークのリストからワイヤレス ネットワークを長押ししてタップします。
ステップ 3 **ネットワークの変更をタップします**。
ステップ 4 **詳細オプションを表示**をチェックします。
ステップ 5 IP 設定タイプを選択し、以下を構成します。

- IP アドレス(IP address)
- ゲートウェイ（Gateway）
- ネットワークプレフィックス長
- DNS 1
- DNS 2
- ドメイン名（Domain Name）

ステップ 6 **保存**をタップします。

Wi-Fi 周波数帯域を設定する

手順

ステップ 1 設定アプリケーションで、 **Wi-Fi をタップします。**
ステップ 2 タップ **...**
ステップ 3 **Wi-Fi 周波数帯域** をタップして設定を選択します。

Expressway 経由でのモバイルおよび Remote Access

Expressway 経由のモバイルおよびリモート アクセスには、Cisco Expressway 8.6 以降と Cisco Unified Communications Manager 10.5.2 SU2 または Cisco Unified Communications Manager 11.0 以降が必要です。

Cisco Expressway は、仮想プライベート ネットワーク (VPN) クライアント トンネルを使用せずに、リモート ワーカーが Cisco DX シリーズ デバイスを企業ネットワークに簡単かつ安全に接続できる方法を提供します。 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。 DX シリーズ デバイスが Expressway 証明書を認証し、TLS セッションを確立するには、Expressway 証明書が DX シリーズ ファームウェアによって信頼されているパブリック証明機関によって署名されている必要があります。 Expressway 証明書を認証するために、DX シリーズ デバイスに他の 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。 サポートされている CA 証明書のリストについては、www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-technical-reference-list.html を参照してください。

ユーザが問題レポートツールを使用できるようにするには、問題レポートツールのサーバアドレスを Expressway HTTP サーバの許可リストに追加する必要があります。

Expressway にログインするときに、サービス名、ユーザ ID、およびパスワードの入力が求められます。 最初の起動時に、オフプレミスのユーザはセットアップ アシスタントによって Expressway にログインするように求められます。 オンプレミスまたはオフプレミスで以前に導入されたデバイスの場合は、Expressway を使用するようにデバイスを変換する必要があります。

Cisco Unified Communications Manager の製品固有のオプションで **User Credentials Persistent for Expressway Sign In** パラメータを設定すると、デバイスはユーザのログイン資格情報を保存するため、ユーザはこの情報を再入力する必要がなくなります。デバイスに保存されるユーザ資格情報は暗号化されます。

詳細については、『*Cisco Expressway* 経由の統合コミュニケーション モバイルおよび *Remote Access* 導入ガイド』を参照してください。

モバイルおよび Remote Access の制限と制約

- Expressway 経由で接続された DX シリーズデバイスは、企業ネットワーク内でホストされている Web ブラウジングや電子メール サービスにアクセスできません。
- オフフック/KPML ダイヤリング、モビリティ、DND、コールバック、会議参加者のドロップ機能は、Expressway 8.6 以降でのみサポートされます。
- ビジー ライン フィールド機能には、Cisco Unified Communications Manager 11.0 以降が必要です。
- Expressway 経由で接続されたデバイスは、企業ネットワーク内の APK サーバから APK をダウンロードできません。 ホストにアクセスできる限り、デバイスはパブリック ネットワーク上の APK サーバから APK をダウンロードできます。
- 企業ネットワークからデバイスへの SSH アクセスがありません。
- 企業ネットワークからデバイスの Web ページにアクセスできません。
- セルフプロビジョニングは Expressway 経由ではサポートされません。

Expressway のユーザ資格情報の永続性を有効にする

手順

ステップ 1 個々のデバイス設定ウィンドウまたは **共通の電話プロファイル** ウィンドウの [製品固有の設定レイアウト] 領域に移動します。

ステップ 2 **Expressway サインイン用のユーザ資格情報**をオンに設定します。

Expressway 経由でデバイスをモバイルおよび Remote Access に変換する

始める前に

デバイスのファームウェアは 10.2 (4) 以降である必要があります。

手順

ステップ 1 設定アプリケーションで、 **[その他...]** をタップします。

ステップ 2 **ネットワーク設定をリセット**をタップします。

ステップ 3 **自動ローカルテレフォニー検出を有効にする**のチェックを外して、**リセット**をタップします。 ネットワーク接続がリセットされます。 デバイスが有線ネットワークに接続されている場合は、自動的に再接続されます。 デバイスがワイヤレスで展開されている場合は、Wi-Fi ネット

ワークに接続する必要があります。デバイスがネットワークに接続すると、**TFTP サーバ入力**画面が表示されます。

ステップ 4 **Expressway**をタップします。

ステップ 5 **サービス ドメイン**、**ユーザ名**、**パスワード** の各フィールドに入力します。

ステップ 6 **サインイン**をタップします。

Expressway デバイスを VPN に変換する

手順

ステップ 1 設定アプリケーションで、**[その他...] をタップします。**

ステップ 2 **ネットワーク設定をリセット**をタップします。

ステップ 3 ネットワークに接続します。

ステップ 4 TFTP サーバの設定を入力します。

ステップ 5 VPN プロファイルを追加して接続します。

オフプレミスデバイスをオンプレミスに変換する

手順

デバイスを企業ネットワークに接続します。
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。

問題報告ツールサーバを Expressway HTTP 許可リストに追加する

手順

ステップ 1 Expressway で、**[構成]** > **[統合コミュニケーション]** > **[構成]**に移動します。

ステップ 2 **HTTP サーバ許可リスト** をクリックします。

ステップ 3 問題報告ツール HTTP サーバのホスト名または IP アドレスを設定します。

許可される承認リクエストレートを設定する

デバイスのモバイルおよび Remote Access 認証のレートは、デフォルトで制御されます。 デフォルト設定は、300 秒間に 3 回の承認です。 Expressway サーバが HTTP 429 「Too Many Requests」 エラーを発行している場合は、このレートを上げることを検討してください。

手順

ステップ 1 Expressway で、 **[構成]** > **[ユニファイド コミュニケーション]** > **[構成]** > **[詳細]** に移動します。
ステップ 2 認証レート制御を設定します。

代替 TFTP サーバを有効にする

手順

ステップ 1 設定アプリケーションで、 **[その他]** をタップします。
ステップ 2 **[TFTP サーバ設定]** をタップします。
ステップ 3 **代替 TFTP サーバを使用する**をチェックします。

TFTP サーバ 1 の設定

手順

ステップ 1 設定アプリケーションで、 **[その他]** をタップします。
ステップ 2 **[TFTP サーバ設定]** をタップします。
ステップ 3 **代替 TFTP サーバを使用する**をチェックします。
ステップ 4 **TFTP サーバ 1** をタップします。
ステップ 5 TFTP サーバのアドレスを入力し、 **[OK]** をタップします。

TFTP サーバ 2 の設定

手順

ステップ 1 設定アプリケーションで、**[その他] をタップします。**
ステップ 2 **TFTP サーバ設定をタップします。**
ステップ 3 **代替 TFTP サーバを使用するをチェックします。**
ステップ 4 **TFTP サーバ 2** をタップします。
ステップ 5 TFTP サーバのアドレスを入力し、**[OK]** をタップします。

AnyConnect VPN

AnyConnect は、ASA バージョン 8.0 以降（AnyConnect Mobile ライセンス付き）または Adaptive Security Device Manager（ASDM）6.0 以降を実行している Cisco 5500 シリーズ ASA への安全な VPN 接続をリモート ユーザに提供する VPN クライアントです。

ASA の詳細については、以下を参照してください。 https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

VPN 接続プロファイルを追加する

手順

ステップ 1 設定アプリケーションで、**その他**をタップします。
ステップ 2 **VPN** をタップします。
ステップ 3 **[VPN プロファイルを追加]** をタップします。
ステップ 4 説明とサーバのアドレスを入力します。
ステップ 5 **保存**をタップします。

VPN に接続する

手順

ステップ 1 設定アプリケーションで、**[その他] をタップします。**
ステップ 2 **VPN をタップします。**
ステップ 3 VPN 接続をタップして長押しします。
ステップ 4 必要に応じて、次のいずれかを実行します。

- 資格情報を入力します。プロンプトが表示されたら、二重認証をサポートするためにセカンダリ資格情報も入力します。
- **[証明書を取得]**をタップし、システム管理者から提供された証明書登録資格情報を入力します。 AnyConnect は証明書を保存し、VPN セキュア ゲートウェイに再接続して、認証に証明書を使用します。

ステップ 5 [接続（Connect）]をタップします。

VPN 経由のビデオ コールエクスペリエンスを最適化

ビデオ帯域幅の設定を調整して、VPN経由のビデオコールエクスペリエンスを最適化します。 720p のビデオ解像度には 1.5 Mbps の帯域幅が必要です。 帯域幅の設定が低いと、ビデオ解像度も低くなります。

（注） スループットは、ネットワーク上で共有される他のトラフィックや時間帯などの要因により、時間の経過とともに変化します。 これらの変化はビデオ体験に影響を及ぼす可能性があります。

手順

ステップ 1 VPN から切断します。

ステップ 2 デバイスの速度テストを実行し、テスト結果のアップロード速度をメモします。

Speed A.I. のインターネット スピード テストなどのスピード テスト アプリケーションは、Google Play から入手できます。

ステップ 3 VPN に再接続します。

ステップ 4 通話アプリケーションで、 。

ステップ 5 [設定（Settings）]をタップします。

ステップ 6 **ビデオ帯域幅をタップします。**

ステップ 7 速度テストの結果のアップロード速度よりも低いビデオ帯域幅を選択します。

Cisco Unified Communications Manager で VPN を設定する

VPN 設定メニューでは、Secure Sockets Layer (SSL) を使用して VPN クライアント接続を有効にすることができます。デバイスが信頼できるネットワークの外部にある場合、またはデバイスと Cisco Unified Communications Manager 間のネットワーク トラフィックが信頼できないネットワークを経由する必要がある場合は、VPN 接続を使用します。

VPNプロファイルを構成するには、次の手順に従ってください。 詳細については、『『*Cisco Unified Communications Manager* セキュリティ機能』 および *Cisco Unified Communications* オペレーティング システム管理ガイド』を参照してください。

手順

ステップ 1 各 VPN ゲートウェイに VPN コンセントレータを設定します。

ステップ 2 VPN 証明書を新しい Phone-VPN-Trust にアップロードします。

ステップ 3 VPN ゲートウェイを構成します。

a) **[高度な機能]** > **[VPN]** > **[VPN ゲートウェイ]**を選択します。

b) ゲートウェイ名、説明、URL を入力します。

（注）
VPN ゲートウェイには最大 10 個の証明書を割り当てることができます。 各ゲートウェイに少なくとも 1 つの証明書を割り当てます。 利用可能な VPN 証明書リストには、VPN ロールに関連付けられている証明書のみが表示されます。

VPN ゲートウェイ URL は、ゲートウェイ内のメイン コンセントレータの URL です。

ステップ 4 VPN グループを構成します。 [**高度な機能** > **VPN** > **VPN グループ] を選択します。**

（注）
VPN グループには最大 3 つの VPN ゲートウェイを追加できます。 VPN グループ内の証明書の合計数は 10 を超えることはできません。

ステップ 5 VPN プロファイルを構成します。 [**高度な機能** > **VPN** > **VPN プロファイル] を選択します。**

（注）
[ネットワーク接続の自動検出を有効にする]が有効になっている場合、VPNクライアントは、企業ネットワークの外部にあることを検出した場合にのみ実行されます。

ホスト ID チェック が有効になっている場合、VPN ゲートウェイ証明書の共通名は、VPN クライアントが接続している URL と一致する必要があります。

[パスワードの永続性を有効にする]が有効になっている場合、ユーザ パスワードはキャッシュされます。 「VPN パスワードをデバイスに保存する」も有効になっている場合は、サインインに失敗するまでユーザ パスワードがデバイスに保存されます。

ステップ 6 VPN 機能を設定します。 **[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN 機能設定（VPN Feature Configuration）]**を選択します。

ステップ 7 共通の電話プロファイルを割り当てます。 **[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。

VPN の設定項目

次の表は、Cisco Unified Communications Manager のデバイスの VPN 構成オプションについて説明しています。

表 *14 : VPN* 設定オプション

オプション	説明	変更の手順
管理者がプロビジョニングした VPN ゲートウェイ	VPN グループ構成で VPN が有効になりました。	表示のみ - 変更できません。
ユーザ定義の VPN プロファイル	オプションが有効か無効かを表示します。	個々のデバイス設定ウィンドウま**の電話プロファイル」** ウィンドウの設定] レイアウト領域) で、「ロファイルを許可する」を [オン] フ] に設定します。 **（注）** マルチレベル構成に使用できますデバイス、共通、またはエンターベルで変更できます。 この機能が無効になっている場合Unified Communications Managerユ VPNプロファイルはデバイスのリ除され、**「新しい VPN 接続の追**になります。
常に VPN を必要とする	オプションが有効か無効かを表示します。	**デバイス** > **デバイス設定** > **共通のファイル**を選択します。 希望するプロファイルを選択しま 「常にVPNを必要とする」をオンに設定します。 **（注）** 「常に VPN を必要とする」設定はenable および autoNetworkDetect の に上書きされます。

オプション	説明	変更の手順
VPN パスワードをデバイスに保存する	オプションが有効か無効かを表示します。	**デバイス** > **デバイス設定** > **共** **イル** または **デバイス** > **電話** > ' します。 デバイスに VPN パスワードを オンまたはオフに設定します。 （注） 「デバイスに VPN パスワード は、構成された VPN プロファ パスワードの永続性が有効にな ライアント認証方法が 「ユー ド」 または 「パスワードのみ み機能します。

（注） ネットワーク構成の変更は、アクティブな VPN 接続に影響を与える可能性があります。

VPN が有効になっている場合、VPN にプロキシは構成されず、使用されません。

[XCP認証(VPN Authentication)]

Cisco DX シリーズ デバイスは次の VPN 認証方法をサポートしています。

- ユーザ名とパスワード
- 証明書のみ
- [パスワードのみ(Password only)]

（注） パスワードのみの認証の場合、デバイス ID がユーザ名として事前に入力され、Cisco Adaptive Security Appliance（ASA）によってユーザ名が設定されます。

Cisco Unified Communications Manager で指定される認証は、ASA で設定されている認証と一致する必要があります。 認証が ASA のものと一致しない場合でも、ユーザ VPN は許可されますが、パスワードの永続性および自動接続機能は適用されません。

起動プロセス

ネットワークに接続すると、Cisco DX シリーズ デバイスは標準の起動プロセスを実行します。特定のネットワーク構成によっては、これらの手順の一部のみがデバイス上で実行される場合があります。

1. スイッチからの電力の取得。 デバイスが外部電源を使用していない場合、スイッチはデバイスに接続されているイーサネット ケーブルを通じてインライン パワーを供給します。 **起動中...** 画面が約 30 秒間表示されます。

   デバイスはイーサネット接続を検出しようとします。イーサネット接続が検出されたもののIPアドレスが割り当てられていない場合は、管理者に問い合わせてサポートを受けるよう求められます。 イーサネット接続が見つからない場合、デバイスはワイヤレスネットワーク接続を確立しようとします。

2. (無線 LAN の場合のみ) アクセス ポイントをスキャンします。 デバイスは RF カバレッジ エリアをスキャンします。 デバイスはネットワーク プロファイルを検索し、一致するサービス セット識別子 (SSID) と認証タイプを含むアクセス ポイントをスキャンします。 デバイスは、ネットワーク プロファイル構成に一致するアクセス ポイントに関連付けられます。

3. (無線LANの場合のみ)アクセスポイントで認証します。デバイスは認証プロセスを開始します。

4. 保存されたデバイス イメージを読み込みます。 デバイスには不揮発性フラッシュ メモリが搭載されており、ファームウェアイメージとユーザ定義の設定が保存されます。 起動時に、デバイスはブートストラップ ローダーを実行し、フラッシュ メモリに保存されているファームウェアイメージをロードします。 このイメージを使用して、デバイスはソフトウェアとハードウェアを初期化します。

5. VLAN の設定。 デバイスが Cisco Catalyst スイッチに接続されている場合、次にスイッチは、スイッチで定義されている音声VLANをデバイスに通知します。 デバイスは、IP アドレスのダイナミック ホスト コンフィギュレーション プロトコル (DHCP) 要求を続行する前に、VLAN メンバーシップ情報を必要とします。

6. IP アドレスの取得。 デバイスが DHCP を使用して IP アドレスを取得する場合、デバイスは DHCP サーバに問い合わせて IP アドレスを取得します。 ネットワークで DHCP を使用していない場合は、各デバイスにローカルで静的IPアドレスを割り当てる必要があります。

7. TFTP サーバへのアクセス。 DHCP サーバは、IP アドレスを割り当てるだけでなく、デバイスをTFTPサーバに誘導します。 デバイスのIPアドレスが静的に定義されている場合は、デバイス上で TFTP サーバをローカルに設定する必要があります。その後、デバイスは TFTP サーバに直接接続します。

   TFTP サーバが見つからない場合、ユーザは Expressway にログインするように求められます。

（注） DHCP によって割り当てられるサーバの代わりに、代替 TFTP サーバを割り当てることもできます。

8. (Expressway に接続されたデバイスはこの手順をスキップします)

CTL ファイルの要求。 TFTP サーバに、CTL ファイルが保管されています。 このファイルには、デバイスと Cisco Unified Communications Manager の間に安全な接続を確立するために必要な証明書が含まれています。

9. (Expressway に接続されたデバイスはこの手順をスキップします)

   ITL ファイルの要求。 デバイスは、CTL ファイルを要求した後、ITL ファイルを要求します。 ITL ファイルには、デバイスが信頼できるエンティティの証明書が含まれています。 証明書は、サーバとの安全な接続を認証するため、またはサーバによって署名されたデジタル署名を認証するために使用されます。 Cisco Unified Communications Manager 8.5 以降では ITL ファイルがサポートされます。

10. 設定ファイルの要求。 TFTP サーバには、構成ファイルがあり、Cisco Unified Communications Manager に接続するためのパラメーターとデバイスのその他の情報を定義します。

11. Cisco Unified Communications Manager にお問い合わせください。 構成ファイルは、デバイスが Cisco Unified Communications Manager と通信する方法を定義し、デバイスにロード ID を提供します。 デバイスは、TFTP サーバからファイルを取得した後、リスト上の最も優先度の高い Cisco Unified Communications Manager サーバに接続しようとします。

    デバイスのセキュリティ プロファイルがセキュア シグナリング (暗号化または認証済み) 用に設定され、 Cisco Unified Communications Manager がセキュア モードに設定されている場合、デバイスは TLS 接続を行います。 それ以外の場合、デバイスは安全でない TCP 接続を確立します。

    デバイスがデータベースに手動で追加された場合は、 Cisco Unified Communications Manager デバイスを識別します。 デバイスがデータベースに手動で追加されておらず、自動登録が Cisco Unified Communications Manager で有効になっている場合、デバイスは Cisco Unified Communications Manager データベースに自動登録しようとします。

（注） CTL クライアントを設定している場合、自動登録は無効になっています。 この場合、デバイスを Cisco Unified Communications Manager データベースに手動で追加する必要があります。

12. デバイスを初めて起動する場合は、 **ようこそ** 画面を表示し、セットアップ アシスタントを実行します。

起動時に TFTP サーバを手動で設定する

手順

ステップ 1 画面に「起動中...」と表示されている間に、画面の左上隅を 3 回タップします

ステップ 2 キー シーケンスが検出されたことを示すために、 起動中... の末尾にピリオドが追加されます。

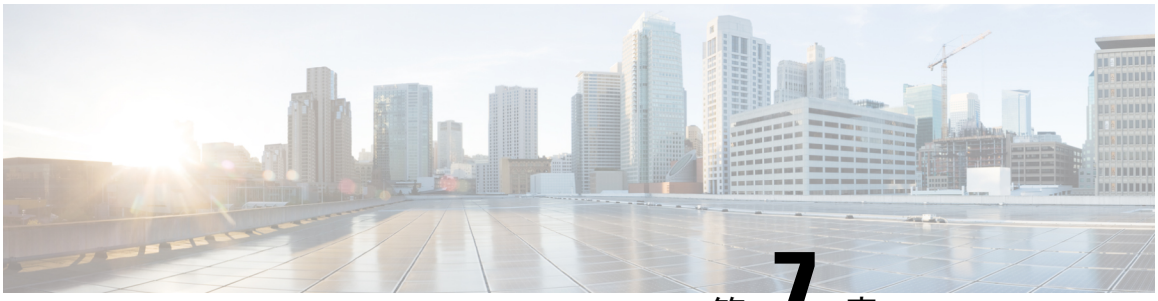
ステップ 3 TFTP 設定画面が表示されます。 TFTP サーバのアドレスを入力し、 **[確認]** をタップします。

起動検証

デバイスに電源が接続されると、デバイスは次の手順を繰り返して起動診断プロセスを開始します。

1. 起動のさまざまな段階でデバイスがハードウェアをチェックしている間 (Cisco DX650 のみ: 受話器のライトとミュート ボタンが赤く点灯し、ヘッドセット ボタンとスピーカー ボタンが緑色に点灯します)、ロック/電源ボタンが点灯します (白)。
2. ステータス バーに電話アイコンが表示されます。

デバイスがこれらの段階を正常に完了すると、正常に起動し、ロック/電源ボタンが点灯したままになります。



第 7 章

連絡先

- 操作モード別の連絡先とディレクトリ （69 ページ）
- ローカル連絡先 （69 ページ）
- 社内ディレクトリ(Corporate Directory) （70 ページ）
- 連絡先検索 （71 ページ）
- アプリケーション ダイヤル ルール （72 ページ）

操作モード別の連絡先とディレクトリ

連絡先ソース	パブリックモード	シンプルモード	拡張モード
デバイス上で作成	対応	対応	対応
Bluetooth からインポート	対応	対応	対応
シスコ ユーザ データ サービス (UDS)	対応	対応	対応
Jabber	未対応	未対応	対応
Exchange グローバル アドレスリスト	未対応	未対応	対応
Google	未対応	未対応	対応
ネイティブのサードパーティ Web アプリ	未対応	未対応	対応

ローカル連絡先

ローカル連絡先は、ユーザが DX デバイスで作成する連絡先です。 ローカル連絡先には、Bluetooth 経由で携帯電話からインポートされた連絡先も含まれます。

ユーザは一度に 200 件を超える連絡先をインポートしないことをお勧めします。

拡張モードでは、ローカル連絡先に、Jabber、Exchangeアカウント、Googleアカウント、またはサードパーティ アプリケーションから同期された連絡先も含めることができます。

電話番号を持つローカル連絡先は、通話アプリケーションの [連絡先] タブで利用できます。すべてのローカル連絡先は、People アプリケーションで利用できます。

社内ディレクトリ(Corporate Directory)

企業ディレクトリを使用すると、ユーザは同僚の連絡先情報を検索できます。 この機能をサポートするには、企業ディレクトリを構成する必要があります。

Cisco Unified Communications Manager は、Lightweight Directory Access Protocol (LDAP) ディレクトリを使用して、 Cisco Unified Communications Manager のユーザに関する情報を保存し、Active Directory (AD) と同期します。

Cisco DX シリーズ デバイスは、Cisco User Data Services（UDS）を使用して、企業のディレクトリ情報を照会します。 Cisco Unified Communications Manager

LDAP の設定の詳細については、 *Cisco Unified Communications Manager* アドミニストレーション ガイド を参照してください。

代替電話帳サーバを設定する

始める前に

代替電話帳サーバでは、UDS と HTTPS プロトコルのみがサポートされます。

Expressway 経由でモバイルおよびリモート アクセスを使用している場合は、代替電話帳サーバを Expressway サーバの HTTP 許可リストに追加し、UDS サーバの CA 証明書を Expressway サーバの信頼リストにインポートします。 Expressway 経由の代替電話帳サポートでは、リクエストが 256 文字に制限されます。 これには、代替電話帳サーバのホスト名、API 文字列、およびユーザが入力した検索クエリ名が含まれます。

手順

ステップ 1 デバイスの [デバイス設定] ウィンドウの [製品固有の設定レイアウト] 部分で、 **[代替電話帳サーバ タイプ]** を UDS に設定します。

ステップ 2 **代替電話帳サーバ アドレス** フィールドに電話帳サーバの URL を入力します。 URL にポートを含めない場合、デバイスは自動的にデフォルト ポート (8443) を使用します。

会社の写真ディレクトリを設定する

このパラメータを設定すると、ユーザが UDS を使用して企業ディレクトリを検索するとき、およびユーザがローカル連絡先として追加したディレクトリ検索結果にディレクトリの写真が表示されます。

（注） 会社の写真ディレクトリでは、資格情報(ユーザ名やパスワードなど)による認証を必要としてはいけません。認証が必要な写真ディレクトリを指定した場合、ディレクトリの写真はDXデバイスに表示されません。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、次のいずれかのウィンドウを選択します。

- **[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）]**
- **システム > エンタープライズ電話**

複数のウィンドウにパラメータを設定した場合、優先順位は次のとおりです。

1. **[デバイス（Device）] > [電話（Phone）]**
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）]**
3. **システム > エンタープライズ電話**

ステップ 2 **会社の写真ディレクトリ** を **`http://<servername>/<path>/%%uid%%.<image file extension>`**に設定します。

ステップ 3 **共通設定を上書き**をチェックします。

連絡先検索

Cisco DX シリーズ ユーザは、ローカルに保存された連絡先、最近使用した連絡先、企業ディレクトリ (UDS) を検索できます。 DX シリーズ デバイスを拡張モードで操作するユーザは、Jabber の連絡先や Exchange などのオンライン ディレクトリも検索できます。

ユーザは以下の方法で検索できます:

- 名

- 姓
- 電話番号
- ユーザ名

ユーザが [通話] タブに番号を入力すると、デバイスは最近の通話のみを検索します。 ユーザが [通話] タブにテキストを入力すると、デバイスは利用可能なすべてのソースを名と姓で検索します。 重複する連絡先は検索結果から削除されます。

ユーザは、[ディレクトリ] タブで企業ディレクトリを検索できます。企業ディレクトリ検索では最大 25 件の結果が表示されます。

検索結果には、写真（ある場合）、名、姓、URI または電話番号が表示されます。検索結果に URI と電話番号の両方が含まれている場合は、URI が表示されます。

アプリケーション ダイヤル ルール

アプリケーション ダイヤル ルールは、携帯電話の連絡先共有番号をネットワークでダイヤル可能な番号へ変換するために使用されます。 アプリケーション ダイヤル ルールは、ユーザが番号を手動でダイヤルしている時、もしくはユーザによってコールが発信される前に番号が編集された場合は、適用されません。

アプリケーション ダイヤル ルールがCisco Unified Communications Managerに設定されます。

ダイヤル ルールの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』「の「Configure Dial Rules」」の章を参照してください。

アプリケーション ダイヤル ルールの設定

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[コール ルーティング（Call Routing）]** > **[ダイヤル ルール（Dial Rules）]** > **[アプリケーション ダイヤル ルール（Application Dial Rules）]** に移動します。

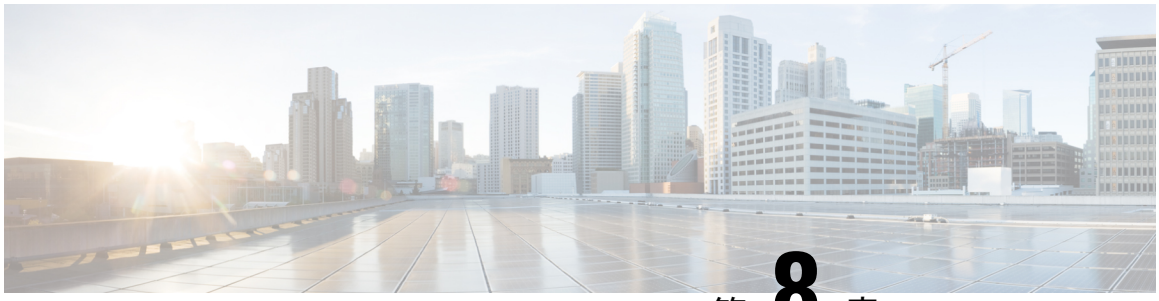
ステップ 2 [新規追加（Add New）] をクリックして新しいアプリケーション ダイヤル ルールを作成するか、既存のアプリケーション ダイヤル ルールを選択して編集します。

ステップ 3 次のフィールドに入力します。

- [名前（Name）]：ダイヤルルールの一意の名前を入力します。名前には最長 20 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、アンダースコア（_）を任意に組み合わせて使用できます。
- [説明（Description）]：このフィールドには、ダイヤルルールの簡単な説明を入力します。
- [開始番号（Number BeginsWith）]：このアプリケーション ダイヤル ルールを適用するディレクトリ番号の先頭部分の数字を入力します。

- [桁数（Number ofDigits）]：この必須フィールドには、アプリケーション ダイヤル ルールを適用するディレクトリ番号の先頭部分の数字を入力します。
- [削除する合計桁数（Total Digitsto be Removed）]：この必須フィールドには、ダイヤル ルールに適用する、Cisco Unified Communications Manager によってディレクトリ番号から削除する桁数を入力します。
- [プレフィックス パターン（Prefix WithPattern）]：この必須フィールドには、アプリケーションダイヤルルールに適用する、ディレクトリ番号に付加するパターンを入力します。
- [アプリケーション ダイヤル ルール優先順位（Application Dial RulePriority）]：このフィールドは、[プレフィックス パターン（Prefix With Pattern）] に入力すると表示されます。 アプリケーション ダイヤル ルールの優先順位を設定することができます。

ステップ 4 Cisco Unified Communications Manager を再起動します。



第 8 章

セルフケアポータルの管理

- セルフケアポータルの概要 （75 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 （76 ページ）
- セルフケアポータルの表示のカスタマイズ （76 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。

ユーザーが Cisco Unified Communications セルフケアポータルにアクセスする前に、Cisco Unified Communications Manager Administration を使用してそのユーザーを標準の 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、ユーザーを Cisco Unified Communications Manager に追加したときに入力した値と同じです。

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

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管理で、**[ユーザ管理]** > **[エンドユーザ]** を選択します。
ステップ 2 ユーザーを検索します。
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

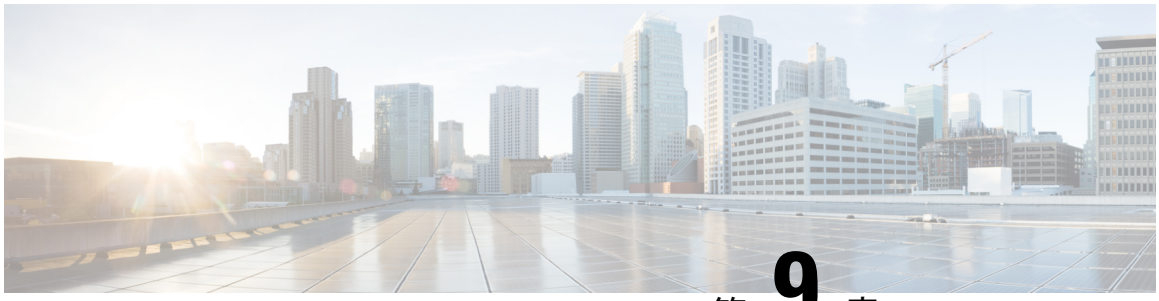
セルフケアポータルにはほとんどのオプションが表示されます。 ただし、Cisco Unified Communications Manager Administration のエンタープライズパラメータ設定で次のオプションを指定する必要があります。

- 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、**[システム（System）]** > **[エンタープライズパラメータ（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 9 章

アクセサリ

- Bluetooth アクセサリ （77 ページ）
- ケーブル ロック （79 ページ）
- 外部カメラ （80 ページ）
- 外部スピーカーおよびマイクロフォン （80 ページ）
- ヘッドセット （81 ページ）
- ビデオディスプレイ （85 ページ）
- Cisco DX650 壁掛けキット （85 ページ）

Bluetooth アクセサリ

ユーザは、ヘッドセット、キーボード、携帯電話などの Bluetooth アクセサリを DX シリーズ デバイスにペアリングできます。

ユーザは一度に複数の Bluetooth デバイスをペアリングできますが、一度にペアリングできる Bluetooth オーディオ デバイスは 1 つだけです。

Bluetooth を有効にすると、ワイヤレス ネットワーク接続が低下する可能性があります。 ワイヤレス ネットワークのパフォーマンスを向上させるには、使用していないときに Bluetooth を無効にするか、ワイヤレス ネットワーク接続に 5 GHz 帯域を使用する必要があります。

Bluetooth デバイスプロファイル

デバイスプロファイル設定画面には、ペアリングされたデバイスで使用できるプロファイルが表示されます。 プロファイルを無効にすると、プロファイルのチェックが外れ、ユーザはそれを有効にできなくなります。

ハンズフリープロファイル

Cisco DX シリーズ デバイスは、デバイスを操作せずにアクセサリ (Bluetooth ワイヤレス ヘッドセットや Bluetooth 対応の携帯電話など) を使用して特定のタスクを実行できるようにするさまざまなハンズフリープロファイル機能をサポートしています。 たとえば、デバイス上で [リ

ダイヤル] をタップするのではなく、ユーザはヘッドセットの製造元の指示に従って Bluetooth ワイヤレス ヘッドセットから番号をリダイヤルできます。

次のハンズフリー機能は Bluetooth アクセサリに適用されます。

- Bluetooth HFP の接続/切断ステータスを処理します。
- 通話するには、オーディオ ゲートウェイ (AG) で電話番号をダイヤルします。
- 通話が接続されたか切断されたかを示します。
- 通話が着信したときにアプリケーションに通知します (インバンド着信音)。
- インバンド着信音を有効または無効にします。
- 電話のステータス (発信者 ID、信号強度、バッテリー レベルなど、AG から) を報告します。
- 通話に応答するか拒否します。
- 発信者 ID 付きの通話待機通知を受信します。
- 通話を保留にして、待機中の通話に切り替えます。
- AG と通話アプリケーションで、保留中の通話とアクティブな通話を切り替えます。
- オーディオを携帯電話に切り替え、オーディオをハンズフリー ユニットに戻します。
- 携帯電話の通話リストを取得します。

ハンズフリーデバイスでは、機能の有効化方法が異なる場合があります。 デバイスの製造元は、同じ機能を指すために異なる用語を使用する場合もあります。 詳細については、製造元のドキュメントを参照してください。

電話帳アクセスプロファイル

Bluetooth 電話帳アクセス プロファイル (PBAP) を使用すると、ユーザはペアリングされた携帯電話の連絡先や通話履歴をデバイスと共有できます。 Cisco DX シリーズ ユーザは、携帯電話をペアリングするときに、連絡先と通話履歴を手動または自動でダウンロードすることを選択でき、連絡先をデバイスに保存することを選択できます。

デバイスプロファイルを有効にする

手順

ステップ 1 Cisco Unified Communications Manager Administrationで、**[デバイス]**>**[電話]**を選択し、変更するデバイスを見つけて、そのデバイスの **[電話の設定]** ウィンドウに移動します。

ステップ 2 **[電話の設定]** ウィンドウで、Bluetooth 設定の **[有効にする]** を選択します。

ステップ 3 デバイス プロファイルを有効にします。

ステップ 4 変更を保存します。

Bluetooth アクセサリをペアリングする

手順

ステップ 1 デバイスの設定アプリケーションで、 **Bluetooth** をオンに切り替えます。
ステップ 2 利用可能なデバイスのリストからペアリングするデバイスをタップします。
ステップ 3 パスキーを確認し、**ペアリング**をタップします。

Bluetooth を無効にする

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話機（Phone）]** を選択します。
ステップ 2 **[電話の検索と一覧表示]** ウィンドウで、変更するデバイスの検索条件を入力し、 **[検索] をクリックします**。
ステップ 3 **[電話の設定]** ウィンドウの [製品固有の設定レイアウト] 領域で、Bluetooth ドロップダウン リスト ボックスから **[無効]** を選択します。

ケーブル ロック

ラップトップ ケーブル ロックを使用して、デバイスをデスクトップに固定できます。 ロックはデバイスの背面にある盗難防止セキュリティ コネクタに接続し、ケーブルをデスクトップに固定できます。

セキュリティ スロットには、最大 20 mm 幅のロックを収容できます。 互換性のあるラップトップ ケーブル ロックには、Kensington ラップトップ ケーブル ロックや、デバイス背面のセキュリティ スロットに収まる他のメーカーのラップトップ ケーブル ロックなどがあります。

外部カメラ

Cisco DX650 外部カメラとしてアドオンの Logitech C920-C ウェブカメラまたは Logitech C930e をサポートします。

外部カメラをデバイスに接続し、ユーザがポイント・ツー・ポイントのビデオコールを行うことを可能にします。 外部カメラを動作させるには、ビデオ コールと USB デバイスを有効にする必要があります。

（注） Cisco DX650 が Power over Ethernet によって電源供給される場合、外部カメラには 802.3at が必要です。 電話機が Power over Ethernet によって電源供給されていない場合は、外部カメラに外部電源が必要です。

外部カメラの設定

外部カメラをデバイスに接続すると、ユーザは外部カメラの設定を制御できるようになります。 内部カメラとは異なり、外部カメラの明るさ設定は調整できません。

外部カメラの設置後チェックを実行する

手順

ステップ 1 外部カメラが接続されました というメッセージが表示されるまで待ちます。

ステップ 2 通話アプリケーションで、 。

ステップ 3 **セルフビューをタップします**。

ステップ 4 デバイスと外部カメラを、視野内に明るい光がない位置に移動します。

ステップ 5 ユーザが正面から照らされるように、デバイスと外部カメラを移動します。

外部スピーカーおよびマイクロフォン

外部スピーカおよびマイクロフォンは、プラグアンドプレイ式のアクセサリです。 ライン入力/出力ジャックを使用して、デバイスの外部 PC タイプのマイクとパワードスピーカー (アンプ付き) を接続できます。 外部マイクへの接続は内部マイクを無効にし、外部スピーカーへの接続は内部スピーカーを無効にします。

（注） 低品質の外部オーディオ デバイスを使用したり、非常に大きな音量でスピーカーを使用したり、マイクをスピーカーの非常に近くに配置したりすると、スピーカーフォン通話で相手側に望ましくないエコーが発生する可能性があります。

ヘッドセット

Cisco ではサードパーティのヘッドセットの内部テストを実施していますが、ヘッドセット ベンダーまたはハンドセット ベンダーの製品を認定したりサポートしたりすることはありません。

このデバイスは、ヘッドセットのマイクによって検出されたバックグラウンド ノイズの一部を低減しますが、バックグラウンド ノイズをさらに低減して全体的なオーディオ品質を向上させたい場合は、ノイズ キャンセリング ヘッドセットを使用します。

Cisco では、不要な無線周波数 (RF) および音声周波数 (AF) 信号を遮断したヘッドセットなどの高品質の外部デバイスの使用を推奨しています。 ヘッドセットの品質と、携帯電話や双方向ラジオなどの他のデバイスとの近さにより、音声ノイズやエコーが発生する場合があります。 リモート側、またはリモート側とユーザの両方に、聞こえるハム音やブザー音が聞こえる場合があります。 ハム音やバズ音は、電灯、電気モーター、大型の PC モニタなど、さまざまな外部ソースが原因で生じることもあります。

（注） 場合によっては、ローカル電源キューブまたはパワーインジェクタを使用すると、ハムが軽減または除去されることがあります。

デバイスが展開される場所における環境とハードウェアの不一致により、単一のヘッドセット ソリューションがすべての環境に最適であるということはあり得ません。

Cisco では、ヘッドセットを購入して大規模に導入する前に、対象環境でヘッドセットをテストしてパフォーマンスを確認することを推奨しています。

（注） 一度に機能するヘッドセット タイプは 1 つだけなので、デバイスに接続された Bluetooth ヘッドセットとアナログ ヘッドセットの両方を使用する場合、Bluetooth ヘッドセットを有効にするとアナログ ヘッドセットは無効になります。 アナログ ヘッドセットを有効にする場合は、Bluetooth ヘッドセットを無効にします。 Bluetooth ヘッドセットが有効になっているデバイスに USB ヘッドセットを接続すると、Bluetooth とアナログ ヘッドセットの両方が無効になります。 USBヘッドセットの接続を外した場合は、Bluetoothヘッドセットの有効化またはアナログ ヘッドセットを使用するためのBluetoothヘッドセットの無効化のいずれかができるようになります。

Bluetooth ワイヤレス ヘッドセット

デバイスは、共有キー認証および暗号化方式を使用してBluetoothヘッドセットに接続します。デバイスは一度に最大5台のヘッドセットに接続できます。最後に接続されたヘッドセットがデフォルトとして使用されます。通常、ペアリングはヘッドセットごとに1回実行されます。

デバイスがペアリングされると、デバイスとヘッドセットの両方が有効になっていて互いの範囲内にある限り、Bluetooth 接続が維持されます。通常は、いずれかのデバイスの電源が切断して再投入されると、それだけで接続が自動的に再確立されます。ただし、一部のヘッドセットでは、ユーザによる接続の再確立が必要です。

Bluetooth ヘッドセットのワイドバンドはサポートされていません。Bluetooth ヘッドセットを使用すると音声品質が低下する場合があります。

最高のパフォーマンスは、3 ～ 6 フィート (1 ～ 2 メートル) の範囲で得られます。5 個以上のヘッドセットをペアリングできますが、最後に接続されたヘッドセットのみがデフォルトとして使用されます。ヘッドセットがデバイスから 30 フィート (10 メートル) 以上離れると、Bluetooth は 15 ～ 20 秒のタイムアウト後に接続を切断します。ペアリングされたヘッドセットがデバイスの範囲内に戻り、デバイスが別の Bluetooth ヘッドセットに接続されていない場合、範囲内の Bluetooth ヘッドセットは自動的に再接続します。省電力モードで動作する特定のデバイスの場合、ユーザは操作ボタンをタップして再接続を開始し、ヘッドセットを 起動することができます。

干渉の問題が発生する可能性があります。他の 802.11 b/g デバイス、Bluetooth デバイス、電子レンジ、大型の金属製の物体の近くに置かないことをお勧めします。可能であれば、他の 802.11 デバイスで 802.11a チャネルを使用するように設定してください。

Bluetooth ワイヤレス ヘッドセットが機能するには、ヘッドセットがデバイスの直接の見通し線内にある必要はありませんが、壁やドアなどの障害物や、他の電子デバイスからの干渉が接続に影響を及ぼす可能性があります。

Bluetooth ヘッドセットの詳細については、ヘッドセットに付属のユーザ ガイドを参照してください。

Bluetooth ワイヤレスヘッドセットを追加

手順

ステップ 1 ヘッドセットを検出/ペアリング モードに設定します。

（注）
ヘッドセットを検出/ペアリング モードにする手順は、ヘッドセットによって異なります。ペアリング手順については、ヘッドセット製造元のマニュアルを参照してください。

デバイスと正常にペアリングして接続するには、ヘッドセットが検出/ペアリングモードになっている必要があります。

ステップ 2 まだオンにしていない場合は、デバイスの Bluetooth をオンにします。

Bluetooth がオンになっているかどうかを確認するには、ステータス バーの Bluetooth アイコンを確認します。

ステップ 3 **デバイスのスキャンを選択します。**

Bluetooth デバイスが見つかると、その名前がウィンドウに表示されます。

デバイスは自動的に PIN 0000 を使用してヘッドセットとペアリングします。 ヘッドセットで異なる PIN が使用されている場合は、ヘッドセットに付属のユーザ ガイドに記載されている正しい PIN を入力します。

（注）
ペアリングが失敗した場合、デバイスは正しい PIN を入力するように要求します。

デバイスが正しい PIN を取得すると、デバイスはアクセサリに接続しようとします。 デバイスが接続できない場合は、エラーアラートが表示され、ユーザに失敗の理由が通知されます。デバイスがアクセサリに接続を試みるために、10 秒のタイムアウトが設定されます。 接続が成功せずにタイマーが期限切れになると、エラー アラートが表示されます。

アクセサリがペアリングされると、Cisco DX シリーズ デバイスとヘッドセットの両方が有効になっていて、互いの範囲内にある限り、Bluetooth 接続が維持されます。 通常、いずれかのデバイスの電源がオフになってからオンになると、接続は自動的に再確立されます。 ただし、一部のヘッドセットでは、ユーザによる接続の再確立が必要です。

ヘッドセットがデバイスの範囲外にある場合、Bluetooth は 15 ～ 20 秒のタイムアウト後に接続を切断します。 ペアリングされたヘッドセットがデバイスの範囲内に戻った場合 (デバイスが別の Bluetooth ヘッドセットに接続されていない場合)、範囲内の Bluetooth ヘッドセットは自動的に再接続されます。 ヘッドセットを起動して再接続プロセスを開始するには、ユーザがヘッドセットの操作ボタンをタップする必要がある場合があります。

ユーザが通話中に Bluetooth ヘッドセットを使用していて、ヘッドセットがオフになっているか、範囲外にあるか、何らかの理由で切断されている場合、スピーカー/ヘッドセットで通話を続行するか、通話を切断するかを選択するようユーザに促すアラートが表示されます。 ユーザが 30 秒以内に操作を行わない場合、通話は終了します。

Bluetooth ヘッドセットを取り外す

手順

ステップ 1 設定アプリケーションで、 **Bluetooth** を選択します。
ステップ 2 デバイス名の横にある **設定** アイコンをタップします。
ステップ 3 **ペア解除**をタップします。

USB ヘッドセット

有線およびワイヤレスの USB ヘッドセットがサポートされています。 USB ヘッドセット (またはワイヤレス ヘッドセットのベース ステーション) を任意の USB ポートに接続できます。

USB ヘッドセットを有効にする

USB ヘッドセットを使用するには、USB ポートを有効にする必要があります。 USB ポートはデフォルトで有効になっています。 USB ポートが無効になっている場合は、Cisco Unified Communications Manager Administration の **Phone Configuration** ウィンドウ（**[デバイス]** > **[電話]**）、**Enterprise Phone Configuration** ウィンドウ（**[システム]** > **[エンタープライズ電話の設定]**）、または **Common Phone Profile** ウィンドウ（**[デバイス]** > **[デバイス設定]** > **[共通の電話プロファイル]**）で有効にすることができます。

手順

ステップ 1 ウィンドウの製品固有の構成レイアウト部分で、該当する USB ポートを有効にします。

ステップ 2 USB クラスの有効化/無効化パラメータで**オーディオ クラス**を選択し、**共通設定の上書き**をオンにします。

USB ヘッドセットを無効にする

手順

Cisco Unified Communications Manager 管理で有効にした USB ポートを無効にします (またはオーディオ クラス パラメータを無効にします)。

有線ヘッドセット

Cisco DX70 および Cisco DX650 は 3.5 mm シングルプラグ ヘッドセットをサポートします。 ユーザはヘッドセットを使用して電話をかけたり受けたりすることができます。

有線ヘッドセットに接続する

手順

ヘッドセットをヘッドセット ポートに差し込みます。

有線ヘッドセットを無効にする

ヘッドセットを無効にするには、 Cisco Unified Communications Manager 管理を使用します。 これを実行すると、スピーカーフォンも無効になります。

手順

ステップ 1 Cisco Unified Communications Manager 管理からヘッドセットを無効にするには、 **デバイス** > **電話** を選択し、変更するデバイスを見つけます。

ステップ 2 **[電話の設定]** ウィンドウ (製品固有の設定レイアウト領域) で、**[スピーカーフォンとヘッドセットを無効にする]** チェックボックスをオンにします。

ビデオディスプレイ

Cisco DX650 HDMI ポートを介して外部ディスプレイ デバイスをサポートします。 HDMI ケーブルの一方の端をHDMIポートに挿入し、もう一方の端をモニタのHDMIポートに挿入して、モニタをデバイスに接続します。

Cisco DX650 壁掛けキット

Cisco DX650 を壁に取り付けるには、Cisco DX650 壁取り付けキットに含まれている特殊なブラケットを使用します。 壁掛けキットはデバイスとは別に注文する必要があります。

事前準備

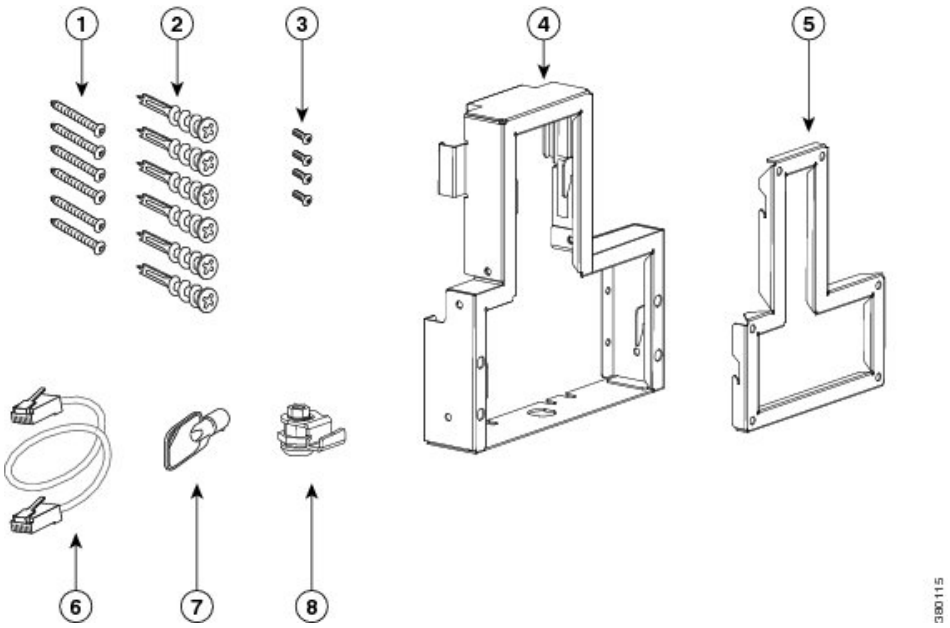
ブラケットの取り付けには、次の工具が必要です。

- プラスドライバー No.1 と No.2
- レベル

壁掛け部品

（注） この壁取り付けキットに含まれるハードウェアは、乾式壁取り付け用です。 レンガやコンクリートなどの他の表面への取り付けには、独自のハードウェアを用意する必要があります。

図 *1:* 単一の電話アセンブリ用壁面取り付けキット



1	8-18 x 1.25 インチのプラスネジ 6 本	5	壁面用ブラケット x 1 個
2	6 つのアンカー	6	6 インチのイーサネット ケーブル X 1 本
3	3 x 6mm の小ネジ 4 本	7	ロックダウンキー 1 個
4	電話機用ブラケット x 1 個	8	1 つのロック

壁掛け金具を取り付ける

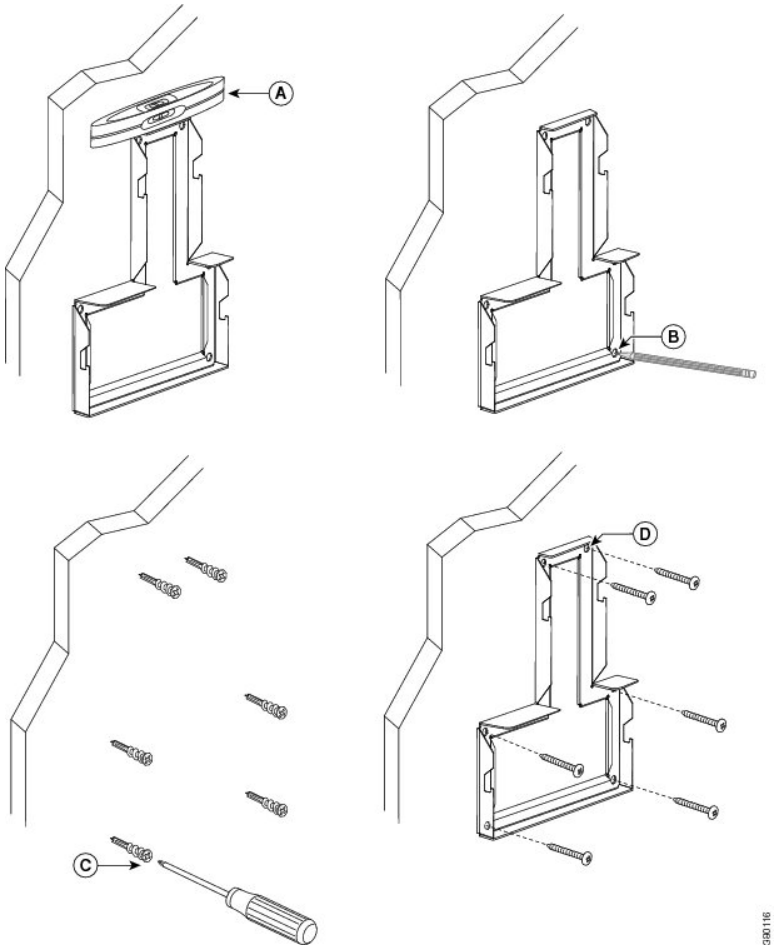
手順

ステップ 1 壁掛けブラケットを希望の位置に取り付けます。 ブラケットをイーサネット ジャックにかぶせて取り付けることも、近くのジャックまでイーサネット ネットワーク ケーブルを配線することもできます。

a) 水準器を使用してブラケットが水平であることを確認した後、鉛筆でネジ穴の位置に印を付けます。

b) アンカーを鉛筆で付けた印の中央に慎重に置き、No. 2 プラスドライバーを使用してアンカーを壁に押し込みます。
c) アンカーが壁にぴったりと収まるまで、アンカーを時計回りにねじ込みます。
d) 付属のネジと No. 2 プラスドライバーを使用して、ブラケットを壁に取り付けます。

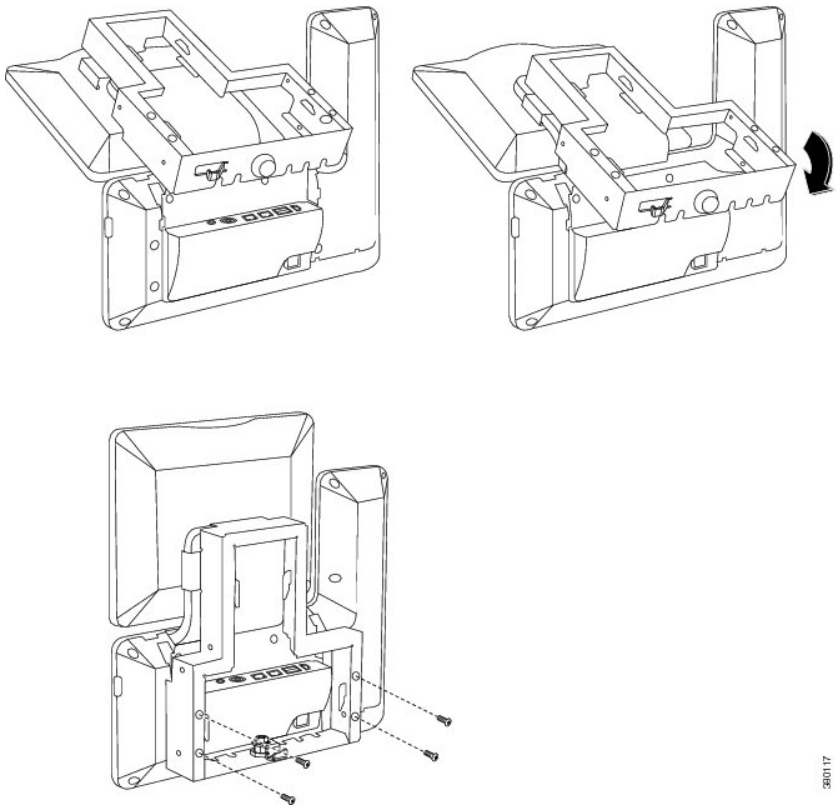
図 *2:* 壁掛けブラケットを取り付ける



ステップ 2 電話ブラケットをデバイスに取り付けます。

a) デバイスのベースに接続されているコードを取り外します。
b) 電話ブラケットを電話機にスライドさせます。 ブラケットの穴からデバイス ポートにアクセスできることを確認します。
c) 機械ネジを使用して、電話ブラケットをデバイスに固定します。
d) コードを再度接続し、デバイス本体に組み込まれているクリップに固定します。

図 *3:* 電話機用ブラケットの装着

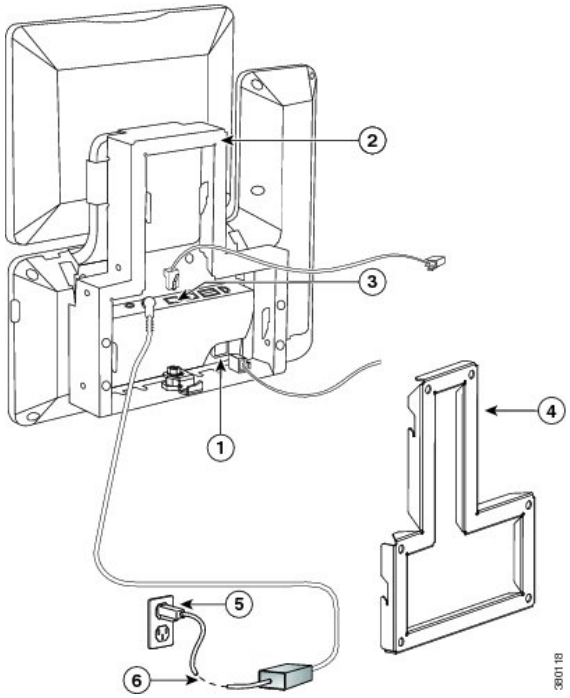


ステップ 3 イーサネット ケーブルを 10/100/1000 SW ネットワーク ポートと壁面のジャックに接続します。

ネットワーク デバイス(コンピュータなど)をデバイスに接続する場合は、ケーブルを 10/100/1000 コンピュータ (PC アクセス) ポートに接続します。

外部電源を使用している場合は、電源コードをデバイスに差し込みます。

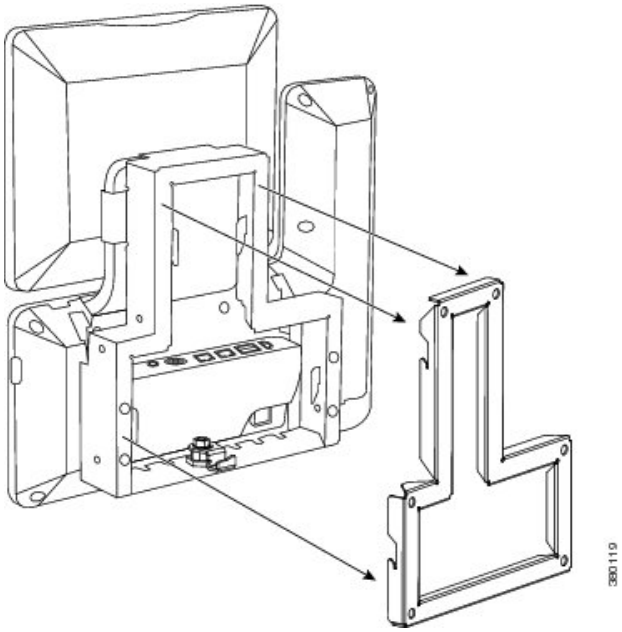
図 *4 :* ケーブルの接続



1	ハンドセットポート	4	壁掛け用ブラケット
2	電話機用ブラケット	5	AC アダプターポート
3	ネットワークポート	6	電源ケーブル

ステップ 4 デバイスを壁面ブラケットに取り付けるには、電話ブラケットの上部にあるタブを壁面ブラケットのスロットに挿入します。ブラケット背後の壁面に差し込み口がある場合を除き、すべての電源コードやその他のケーブルが、ブラケット下部のケーブルアクセス用開口部を通っていることを確認します。電話機用ブラケットと壁面用ブラケットの開口部によって、複数の円形の開口部ができ、1 つの開口部に 1 本のケーブルを通すことができるようになっています。

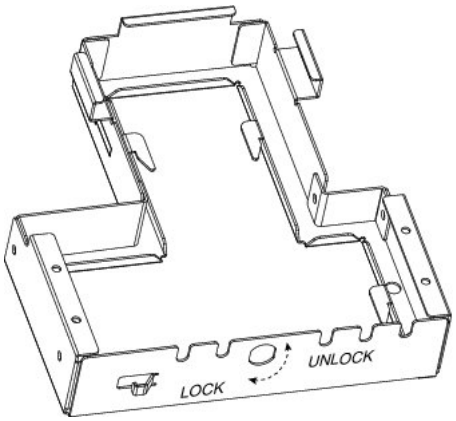
図 *5:* デバイスを壁掛けブラケットに取り付ける

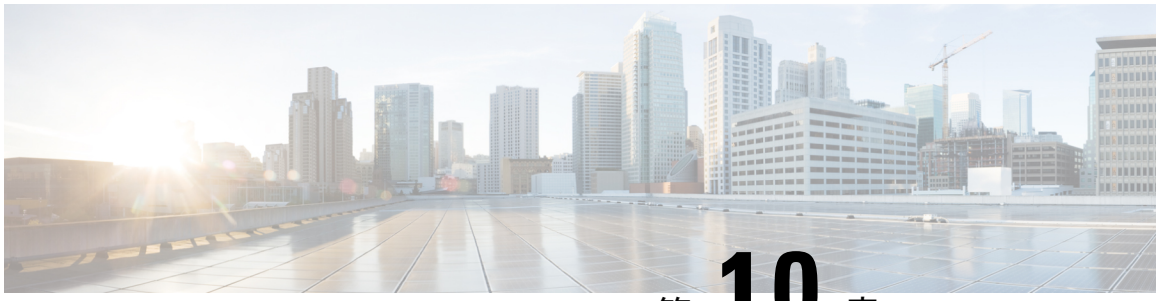


ステップ 5 ロックダウン キーを使用して、デバイスを壁面ブラケットにロックします。

ロックダウンキーは、電話ブラケットの下部にあるキーフックに保管できます。

図 *6:* キーフック付き電話ブラケット





第 10 章

セキュリティ機能

- デバイスのセキュリティ （91 ページ）
- 画面ロックと自動ロックの設定 （103 ページ）
- 設定用の管理者パスワードを設定する （105 ページ）

デバイスのセキュリティ

セキュリティ機能は、デバイスの ID やデータに対する脅威など、さまざまな脅威から保護します。 これらの機能は、デバイスとサーバ Cisco Unified Communications Manager 間の認証された通信ストリームを確立および維持し、デバイスがデジタル署名されたファイルのみを使用するようにします。

Cisco Unified Communications Manager リリース 8.5 (1) 以降には、CTL クライアントを実行しなくてもデバイスに次のセキュリティ機能を提供する、デフォルトのセキュリティが含まれています。

- 設定ファイルの署名
- 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） 安全なシグナリングとメディア機能には CTL ファイルが必要です。

証明機関プロキシ機能 (CAPF) に関連付けられている必要なタスクを実行した後、ローカルで有効な証明書 (LSC) がデバイスにインストールされます。 『*Cisco Unified Communications Manager* セキュリティ機能』で説明されているように、Cisco Unified Communications Manager 管理を使用して LSC を設定できます。

あるいは、デバイスの設定アプリケーションから LSC のインストールを開始することもできます。 この設定アプリケーションでは、LSC を更新または削除することもできます。

セキュリティ機能の概要

Cisco Unified Communications Manager システムにセキュリティを実装すると、デバイスと Cisco Unified Communications Manager サーバのなりすましを防ぎ、データの改ざんを防ぎ、通話信号とメディア 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に、Cisco IP テレフォニー ネットワークは、デバイスとサーバ間の安全な（暗号化された）通信ストリームを確立して維持し、ファイルがデバイスに転送される前にデジタル署名し、デバイス間のメディア ストリームと通話シグナリングを暗号化します。

Cisco DX シリーズ デバイスではデバイス セキュリティー 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。デバイスにセキュリティー プロファイルを適用する方法については『*Cisco Unified Communications Manager* セキュリティ機能』 を参照してください。

Cisco Unified Communications Manager 管理でセキュリティ関連の設定を構成する場合、構成ファイルには機密情報が含まれます。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、『「暗号化された電話機設定ファイルの設定」』の章を『*Cisco Unified Communications Manager* セキュリティ機能』 で参照してください。

次の表は、デバイスがサポートするセキュリティ機能の概要を示しています。

表 *15* : セキュリティ機能の概要

特長	説明
イメージ認証	署名されたバイナリ ファイル (拡張子 .sbn) と暗号化されたバイナリ ファイル (拡張子 .sebn) は、ファームウェア イメージがデバイスにロードされる前にそのイメージが改ざんされるのを防ぎます。 イメージを改ざんすると、デバイスは認証プロセスに失敗し、新しいイメージを拒否します。
カスタマーサイト証明書のインストール（Customer-site certificate installation）	各デバイスには、デバイス認証用の固有の証明書が必要です。デバイスには製造元でインストールされた証明書 (MIC) が含まれていますが、セキュリティを強化するために、Certificate Authority Proxy Function (CAPF) を使用して証明書をインストールするように Cisco Unified Communications Manager 管理において指定できます。 あるいは、デバイスの [エンタープライズ セキュリティ] 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	各エンティティが他のエンティティの証明書を受け入れるときに、サーバとデバイスの間で発生します。 Cisco Unified Communications Manager デバイスと Cisco Unified Communications Manager 間の安全な接続を確立するかどうかを決定します。必要に応じて、TLS プロトコルを介してエンティティ間に安全なシグナリング パスを作成します。デバイスを認証できない限り、 Cisco Unified Communications Manager デバイスを登録しません。

特長	説明
ファイル認証	デバイスがダウンロードするデジタル署名されたファイルを検証します。デバイスは署名を検証し、ファイルの作成後にファイルの改ざんが行われていないことを確認します。認証に失敗したファイルはデバイスのフラッシュメモリに書き込まれません。デバイスはそのようなファイルをそれ以上処理せずに拒否します。
ファイルの暗号化	暗号化により、ファイルがデバイスに転送されている間に機密情報が漏洩することを防止します。さらに、デバイスは署名を検証し、ファイルの作成後にファイルの改ざんが行われていないことを確認します。認証に失敗したファイルはデバイスのフラッシュメモリに書き込まれません。デバイスはそのようなファイルをそれ以上処理せずに拒否します。
シグナリング認証	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）	各デバイスには、デバイス認証に使用される固有の製造元でインストールされた証明書 (MIC) が含まれています。 MIC は、デバイスの永続的な一意の ID 証明を提供し、Cisco Unified Communications Manager でのデバイスの認証を可能にします。
メディア暗号化	SRTP を使用して、サポート対象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、および意図したデバイスのみがデータを受信し、読み取ることを保証します。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）	デバイスの処理負荷が大きすぎる証明書生成手順の一部を実装し、キー生成と証明書のインストールのためにデバイスと対話します。CAPFは、デバイスに代わって顧客指定の証明機関に証明書を要求するように設定することも、ローカルで証明書を生成するように設定することもできます。
セキュリティ プロファイル	デバイスがセキュリティ保護、認証、または暗号化の対象になるかどうかを定義します。この表の他の項目は、セキュリティ機能について説明しています。これらの機能の詳細については、『*Cisco Unified Communications Manager* セキュリティ機能』を参照してください。
暗号化された設定ファイル	デバイス構成ファイルのプライバシーを確保できます。
電話機のWebサーバの無効化（オプション）	セキュリティ上の理由から、デバイスの Web ページ (デバイスのさまざまな動作統計情報を表示するページ) へのアクセスを禁止できます。

特長	説明
電話のセキュリティ強化（Phone hardening）	追加のセキュリティー オプションは、Cisco Unified Communications Manager 管理から制御できます。 • PC ポートの無効化 • Gratuitous ARP (GARP) を無効にする • PC ボイス VLAN の無効化 • ウェブアプリケーションへの制限付きアクセスを提供する • Bluetooth アクセサリポートを無効にする • デバイスのウェブページへのアクセスを無効にする • 画面ロックを要求する • Google Play へのアクセスを制御する™ • 不明なソースからのアプリケーションのインストールへのアクセスを制御する
802.1X 認証	デバイスは 802.1X 認証を使用してネットワークへのアクセスを要求し、取得することができます。
SRST 向けのセキュアな SIP フェールオーバー	セキュリティ目的で Survivable Remote Site Telephony（SRST）リファレンスを設定してから、Cisco Unified Communications Manager Administration で従属デバイスをリセットすると、TFTP サーバーはデバイスの cnf.xml ファイルに SRST 証明書を追加し、そのファイルをデバイスに送信します。 その後、セキュアデバイスは TLS 接続を使用して SRST 対応ルータと対話します。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバ間で送信されるすべての SIP シグナリング メッセージが暗号化されていることを確認します。
AES 256 暗号化（AES 256 Encryption）	Cisco Unified Communications Manager リリース 10.5(2)以降の 以降に接続している DX シリーズ デバイスは、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。 これによりデバイスは、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。

セキュリティプロファイル

Cisco DX シリーズ デバイスはセキュリティ プロファイルを使用します。セキュリティ プロファイルは、デバイスが安全でない、認証されている、または暗号化されているかどうかを定義します。 セキュリティー プロファイルの構成とデバイスへのプロファイルの適用については、『*Cisco Unified Communications Manager* セキュリティ機能』 を参照してください。

デバイスに設定されているセキュリティ モードを表示するには、設定アプリケーションの [セキュリティ] メニューを表示します。

SE Android

Android のセキュリティ強化機能™ (SE Android) により、デバイスのセキュリティーが向上します。 SE Android は、デバイス上で不正なコードや危険なコードを実行しようとする試みを防ぐことで、悪意のあるアプリケーションから保護します。 SE Android は次のことを行います。

- プロセスによる権限昇格を防止できる
- ルートなどの特権プロセスが侵害された場合に、悪用を防ぎ、被害を制限することができます。
- 集中管理され、強制され、分析可能なポリシーを提供する
- 未発見の脆弱性から保護します。

デバイスには、アプリケーション、プロセス、またはユーザがアクセスできるデータを指定するポリシーが含まれています。 SE Android は次の 2 つのモードをサポートしています。

- 寛容な
- 強制モード

ポリシーに違反するものはすべて記録されます。 モードが強制モードである場合、アクションは拒否されます。 ポリシーまたはモードに対してユーザまたは管理者による制御は存在しません。

アップグレードと SE Android

リリース 10.2(2) にアップグレードすると、既存のフィールドユニットで動作する必要があり、強制モードを有効にする前に工場出荷時設定にリセットする必要があるため、Cisco DX650 は許可モードのままになります。 許可モードでは、SE Android はエンドポイントの操作に影響を与えません。

Cisco DX650 が工場出荷時設定にリセットされると、モードは自動的に強制モードに切り替わります。 このアクションは、SE Android 保護を有効にし、ポリシーに違反するアクションの拒否を開始します。

デバイスが 10.2(2) より下のファームウェアリリースにダウングレードされない限り、強制モードは有効なままです。 リリース 10.2(2) 以降にアップグレードすると、工場出荷時設定へのリセットが実行されるまで、デバイスは許可モードに戻ります。

Cisco DX70 および Cisco DX80 デバイスは工場出荷時から常に強制モードになっています。 Cisco DX70 および Cisco DX80 デバイスを許可モードにすることはできません。

SE Android トラブルシューティング

ポリシーは、アプリケーションに許可する操作の期待に合わせて調整されます。ただし、ポリシーにより、許可されるべき操作が禁止される場合があります。 ポリシー エラーの症状には次のようなものがあります:

- サードパーティ製アプリまたはその他のアプリで、起動時または実行中にエラーが表示されます。
- アプリまたは機能は、 Cisco DX650 などの許可モードのエンドポイントでは動作しますが、強制モードの同様に構成されたデバイスでは動作しません。

- SE Android は常時オンの機能であり、管理者による制御は行われません。 フィールドの問題は診断され、欠陥として報告される必要があります。

SE Android ポリシーの問題を診断する

手順

ステップ 1 SE Android モードを決定します。

a) 設定アプリケーションから、**デバイス情報** > **SELinux ステータス**をタップします。

b) Debugsh から、コマンド **show selinux status** を入力します。

モードがパーミッシブである場合、問題は SE Android に関連するものではありません。

ステップ 2 モードがエンフォースである場合は、パーミッシブモードのデバイスで再テストします。 問題がパーミッシブモードで再現しない場合は、その問題は SE Android に関連している可能性が高くなります。

ステップ 3 問題が SE Android 関連であるか、特定できない場合は、ログを収集して報告してください。

ADB シェルの制限

エンドポイントが強制モードの場合、Android Debug Bridge (adb) シェルは制限されます。 **ls** や **ps** などのコマンドでは、完全な結果が表示されない場合があります。

完全な結果を得るには debugsh コマンドを使用してください。 たとえば、シェルから **ps** ではなく、debugsh **show process** を使用します。

強制モードでは多くのディレクトリが立ち入り禁止となるため、強制モードではファイルシステムを自由に参照することもできなくなります。

SE Android ログ収集

問題を報告するには、次の情報を収集します。

- 問題の簡単な説明（発生時刻を含む）
- 可能であれば問題のスクリーンショット
- debugsh **show selinux all** コマンドの出力
- 問題報告ツール（PRT）の出力

ローカルで有効な証明書のセットアップ

始める前に

適切な Cisco Unified Communications Manager および証明機関プロキシ機能 (CAPF) のセキュリティ構成が完了していることを確認します。

- 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。

詳細については『*Cisco Unified Communications Manager* セキュリティ機能』をご覧ください。

手順

ステップ 1 CAPF の設定後に設定された CAPF 認証コードを取得します。

ステップ 2 設定アプリケーションで、**[セキュリティ]**>**[エンタープライズ セキュリティ設定]** を選択します。

ステップ 3 **LSC** をタップします。
デバイスは認証文字列の入力を要求します。

ステップ 4 認証文字列を入力し、**「送信」** をタップします。

デバイスは、CAPF の設定方法に応じて、LSC のインストール、更新、または削除を開始します。 手順の実行中は、進行状況を監視できるように一連のメッセージが表示されます。

（注）
LSC のインストール、更新、または削除のプロセスは完了するまでに長い時間がかかる場合があります。 **[キャンセル] をタップすると、いつでもプロセスを停止できます**。

インストール手順が正常に完了すると、デバイスに「インストール済み」と表示されます。 デバイスに「インストールされていません」と表示される場合は、認証文字列が正しくないか、デバイスがアップグレードに対応していない可能性があります。 CAPF 操作によって LSC が削除された場合、デバイスは操作が成功したことを示すために `Not Installed` と表示します。 CAPF サーバで生成されたエラー メッセージを確認し、適切なアクションを実行します。

（注）
LSC がインストール、アップグレード、または削除された後、デバイスが再起動します。

SHA-256 製造インストール証明書

Cisco DX70 そして Cisco DX80 RSA 2048 キーを使用した SHA-256 の署名アルゴリズムを備えた製造元でインストールされた証明書 (MIC) を使用します。 署名アルゴリズムには、 Cisco Unified Communications Manager、Cisco Secure Access Control Server (ACS)、および Secure SRST のサポートが必要です。

SHA-256 MIC 機能には次のサポート要件があります。

- Cisco Unified Communications Manager リリース 9.1 (2) 以降
- ACS リリース 5.2 以降。

（注） ACS 5.2 以降では、EAP-TLS 内部方式を使用した EAP-FAST はサポートされません。 EAP-TLS を使用するか、EAP-TLS 内部方式を使用した EAP-FAST の場合は ISE に移行します。

- IOS 12.4(15)T1 以降
- Cisco Identity Service Engine リリースは 1.1 以降です。 EAP-TLS 内部方式を使用した EAP-FAST は、ISE リリース 1.2 以降でサポートされています。

別のアプリケーションが使用されており、これらのアプリケーションが電話機から MIC を認証する必要がある場合、このシリーズの電話機の MIC を発行する Cisco 認証局は、次のリンクから取得できます。

- http://www.cisco.com/security/pki/certs/cmca2.cer
- http://www.cisco.com/security/pki/certs/crcam2.cer

アプリケーションがデバイスの MIC を認証できるようにするには、これらの Cisco 証明機関をアプリケーションにインポートする必要があります。 Cisco DX シリーズ

セキュアな通話

Cisco DX シリーズ デバイスのセキュリティを実装するには、Cisco Unified Communications Manager Administration の [**電話の設定**] ウィンドウから [保護されたデバイス] パラメータを有効にします。セキュリティが実装されている場合、通話アプリケーションにセキュア通話アイコンが表示され、安全な通話であることが示されます。

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。安全な通話は高いレベルのセキュリティを提供し、通話の整合性とプライバシーを確保します。 通話中の通話が暗号化されている場合、設定アプリケーションの **エンタープライズ セキュリティ** のセキュリティ モードのステータスは「暗号化済み」と表示されます。

（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。

安全な通話では、通話が暗号化され、両方のデバイスが保護されたデバイスとして設定され、安全なトーン機能が有効になっている場合、2 秒間のトーンでユーザに通知されます Cisco Unified Communications Manager。 このトーンは、コールが応答されたときに両方の電話機で再生されます。 このトーンは、発側と着側の両方のデバイスが保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。 システムが通話が暗号化されていないと判断した場合、デバイスは非セキュア通知音（ビープ音 6 回）を再生し、通話が保護されていないことをユーザに警告します。 セキュア通知トーン機能および設定要件の詳細な説明については、『*Cisco Unified Communications Manager* セキュリティ機能』を参照してください。

（注） オーディオとビデオは安全な状態で送信されますが、プレゼンテーションは安全でない状態で送信されます。 プレゼンテーションのある通話では、デフォルトで **暗号化された** ロック アイコンが表示されます。 **[セキュア コール アイコン表示ポリシーが必須]** を、Cisco Unified Communications Manager の **[システム]** > **[サービス パラメータ]** の別のオプションに設定できます。 デフォルト設定は、 **BFCP および iX トランスポートを除くすべてのメディアを暗号化する必要がある**です。

セキュアな電話コールの識別

Cisco DX シリーズ デバイスと相手側のデバイスがセキュア通話用に設定されている場合に、セキュア通話が確立されます。 両方のデバイスは、同じ Cisco IP ネットワーク内に存在することも、IP ネットワーク外のネットワーク上に存在することもできます。 安全な電話会議は、次のプロセスを通じて確立されます。

1. ユーザは、セキュリティ保護されたデバイス(暗号化されたセキュリティ モード)から通話を開始します。
2. デバイスは、設定アプリケーションのエンタープライズ セキュリティで暗号化されたステータスを示します。 このステータスは、デバイスが安全な通話用に設定されていることを示しますが、接続されている他の電話も安全であることを意味するものではありません。
3. 通話が別のセキュリティ保護されたデバイスに接続されると、セキュリティ トーンが再生され、会話の両端が暗号化され、セキュリティ保護されていることを示します。 それ以外の場合は、非セキュア トーンが再生されます。

（注） セキュア トーンは、Cisco Unified Communications Manager で有効になっている 場合にのみ再生されます。 セキュア トーンが無効になっている場合、通話が安全であってもセキュア トーンは再生されません。 詳細については、「セキュアおよび非セキュア通知トーンの設定」 章を『*Cisco Unified Communications Manager* セキュリティ機能』 で参照してください。

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。 安全な電話会議は、次のプロセスを通じて確立されます。

1. ユーザは安全なデバイスから会議を開始します。
2. Cisco Unified Communications Manager 通話に安全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 各デバイスのセキュリティ モードを確認し、会議の安全なレベルを維持します。
4. デバイスは電話会議のセキュリティ レベルを示します。

さまざまな相互作用、制約、制限が電話会議のセキュリティー レベルに影響を及ぼします。セキュリティー レベルは、参加デバイスのセキュリティー モードとセキュア会議ブリッジの可用性によって決定されます。Cisco DX シリーズ デバイスは、安全な音声およびビデオ電話会議をサポートします。

オーディオとビデオは安全な状態で送信されますが、プレゼンテーションは安全でない状態で送信されます。 デフォルトで、プレゼンテーションを含む電話会議には**暗号化**ロック アイコンが表示されます。 **[セキュア コール アイコン表示ポリシーが必須]** を、Cisco Unified Communications Manager の **[システム]** > **[サービス パラメータ]** の別のオプションに設定できます。 デフォルト設定は、 **BFCP および iX トランスポートを除くすべてのメディアを暗号化する必要がある**です。

通話セキュリティの相互作用と制限

Cisco Unified Communications Manager 会議が確立されるとデバイスのセキュリティ ステータスをチェックし、会議のセキュリティ表示を変更したり、通話の完了をブロックしたりして、システムの整合性とセキュリティを維持します。 次の表は、割り込み機能による通話セキュリティ レベルの変更に関する情報を示します。

表 *16*：割り込み機能との通話セキュリティーの相互作用

発信側の電話機のセキュリティ レベル	使用する機能	通話セキュリティ レベル	動作結果
非セキュア	割込み	暗号化された通話	通話は割り込まれ、非セキュア通話として識れます
セキュア	割込み	暗号化された通話	通話はバージングされ、安全な通話として識れます。

次の表は、発信側の電話のセキュリティ レベル、参加者のセキュリティ レベル、および安全な会議ブリッジの可用性によって決定される会議のセキュリティ レベルの変更に関する情報を示します。

表 *17*：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

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	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	ミートミー	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 ん。コールを拒否します（Does not Level, call rejected）」というメッセ る。
セキュア	ミートミー	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

VPN および Cisco Virtualization Experience Client (VXC) VPN 経由でセキュア ビデオを使用する場合、サポートされる最大帯域幅は 320 kbps です。

デバイスが Cisco TelePresence を呼び出す場合、最大帯域幅は 320 kbps です。

デバイスのセキュリティ情報をリモートで確認する

手順

ステップ 1 デバイスのセキュリティ情報をリモートで確認するには、デバイスがサーバに登録されているか、以前に登録されていたこと、またデバイス構成ページで Web アクセスが有効になっていることが必要です。 Cisco Unified Communications Manager

ステップ 2 Web ブラウザで、**http://<device ip>/SecurityInformation** にアクセスしてデバイスのセキュリティ情報を表示するか、**http://<device ip>/SecurityInformationX** にアクセスして XML 形式でデバイスのセキュリティ情報を表示します。

Barge の暗号化

割り込みに使用するデバイスが暗号化用に設定されていない場合、ユーザは暗号化された通話に割り込むことができません。 この場合、割り込みに失敗すると、割り込みが開始されたデバイスでリオーダー トーン（速いビジー音）が聞こえます。

割り込みの開始側のデバイス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デバイス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 通話は非セキュアとして分類されます。

割り込みの開始側のデバイス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、デバイスはそのコールが暗号化されていることを示します。

802.1X 認証サポート

Cisco DX シリーズ デバイスと Cisco Catalyst スイッチは、従来、Cisco Discovery Protocol (CDP) を使用して相互を識別し、VLAN割り当てやインライン電源要件などのパラメータを決定します。 CDP は、ローカルに接続されたワークステーションを識別しません。 Cisco DX シリーズ デバイスは、EAPOL パススルー メカニズムを提供します。 このメカニズムにより、デバイスに接続されたワークステーションは、LAN スイッチの 802.1X 認証システムに EAPOL メッセージを渡すことができます。 パススルー メカニズムにより、デバイスがネットワークにアクセスする前に、データ エンドポイントを認証するための LAN スイッチとしてデバイスが機能することがなくなります。

Cisco DX シリーズ デバイスはプロキシ EAPOL ログオフ メカニズムも提供します。 ローカルに接続された PC がデバイスから切断された場合でも、LAN スイッチとデバイス間のリンクは維持されるため、LAN スイッチは物理リンクの障害を認識しません。 ネットワークの整合性を維持するために、デバイスはダウンストリーム PC に代わってスイッチに EAPOL-Logoff メッセージを送信します。これにより、LAN スイッチはダウンストリーム PC の認証エントリをクリアします。

Cisco DX シリーズ デバイスには 802.1X サプリカントも含まれています。 このサプリカントにより、ネットワーク管理者は LAN スイッチ ポートへのデバイスの接続を制御できます。 デバイス 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 および EAP-TLS オプションが使用されます。

必要なネットワークコンポーネント

デバイス上での 802.1X 認証のサポートには、いくつかのコンポーネントが必要です。 Cisco DX シリーズ これらには次のものが含まれます。

- 802.1X サプリカントとして機能し、ネットワークへのアクセス要求を開始するデバイス自体。
- Cisco Secure Access Control Server (ACS) (またはその他のサードパーティ認証サーバ)。 認証サーバは、デバイスを認証する共有シークレットを使用して構成する必要があります。
- 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 802.1X をサポートする必要があるため、オーセンティケーターとして機能し、デバイスと認証サーバー間でメッセージを送受信します。 交換が完了すると、スイッチはデバイスのネットワークへのアクセスを許可または拒否します。

ベストプラクティス

次のリストでは、802.1X 構成の要件と推奨事項について説明します。

- 802.1X 認証を有効にする: 802.1X 標準を使用してデバイスを認証する場合は、デバイスで認証を有効にする前に、他のコンポーネントが適切に構成されていることを確認してください。 Cisco DX シリーズ
- PC ポートの構成: 802.1X 標準では VLAN の使用が考慮されていないため、特定のスイッチ ポートに対して 1 つのデバイスのみを認証することを推奨しています。 ただし、一部

のスイッチ（Cisco Catalyst スイッチなど）はマルチドメイン認証をサポートしています。スイッチの設定によって、デバイスの PC ポートに PC を接続できるかどうかが決まります。

- 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、PC ポートを有効化し、そのポートに PC を接続できます。 この場合、デバイスはプロキシ EAPOL-Logoff をサポートし、スイッチと接続された PC 間の認証交換を監視します。Cisco Catalyst スイッチでの IEEE 802.1X サポートの詳細については、次の URL にある Cisco Catalyst スイッチのコンフィギュレーション ガイドを参照してください。

  http://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/tsd-products-support-series-home.html

- 無効：スイッチで同じポート上の複数の 802.1X 準拠デバイスがサポートされていない場合は、802.1X 認証を有効にするときに PC ポートを無効にするようにしてください。 このポートを無効にせずに PC を接続しようとすると、スイッチはデバイスと PC の両方へのネットワーク アクセスを拒否します。

- ボイス VLAN の設定：802.1X 標準では VLAN が考慮されないため、この設定をスイッチのサポートに基づいて行うようにしてください。
  - 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、音声 VLAN を無効にし、ポートをネイティブ VLAN に割り当てることを検討してください。

画面ロックと自動ロックの設定

画面ロック タイムアウト値は、画面がオフになり、画面ロックがアクティブになったときの通常のデバイスアイドル タイムアウトを制御します。 変数は 1 ～ 60 分の範囲で設定可能です。

自動ロックは、ディスプレイが暗くなったり消えたりするまでの時間を制御します。デバイスが常時オンモードの場合、デバイスは暗くなります。デバイスが省電力モードになっている場合は、完全に電源がオフになります。 省電力モードの詳細については 電力削減 （13 ページ）を参照してください。

自動ロックの値は、最大 10 分に設定できます。 自動ロックの値を構成するには、**[設定]** > **[セキュリティ]** > **[自動ロック]** に移動します。

表 *18* : 画面ロックのタイムアウトと自動ロック値の関係

条件	結果
画面ロックのタイムアウト値が自動ロック値より低い	画面ロックのタイムアウト値に達すると、画面は最大の明るさのままになり、ロックされた画面が表示されます。

条件	結果
自動ロックの値が画面ロックのタイムアウト値より低い	自動ロック値に達すると、次の 2 つの結果が考えられます。 • デバイスが常時オン モードの場合、自動ロック値に達するとデバイスの明るさが下がります。 画面ロックのタイムアウト値に達すると、デバイスはロックされ、暗くなったままになります。 • デバイスが省電力モードの場合、自動ロック値に達するとデバイスはロックされ、オフになります。 画面ロックのタイムアウト値に達すると、追加の変更は行われません。
画面ロックのタイムアウト値は自動ロックの値と同じです	値に達すると、画面は最大の明るさのままになり、ロックされた画面が表示されます。

画面ロック解除/パスワードリセットの設定

この機能を使用すると、ユーザは画面のロックを解除するために使用される PIN/パスワードをリセットできます。 ユーザは、 Cisco Unified Communications Manager または設定された Google™ アカウント認証情報を使用して PIN/パスワードをリセットできます。 次の手順に従って Cisco Unified Communications Manager で PIN/パスワードをリセットします。

手順

ステップ 1 Cisco Unified Communications Manager 管理から **ユーザ管理** > **エンドユーザ**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 必要なユーザ情報を入力します。

ステップ 4 **[デバイス情報]** ウィンドウで、ユーザを関連付けたいデバイスを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **[権限情報]** ウィンドウで、ユーザに Cisco Unified Communications Manager 管理権限を割り当てます。

ステップ 7 **[権限情報]** ウィンドウで、 **[標準 CCM エンド ユーザ] を選択します**。

ステップ 8 **[保存（Save）]** と **[設定の適用（Apply Config）]** をクリックします。 デバイスが再登録されると、ユーザはデバイスに関連付けられます。

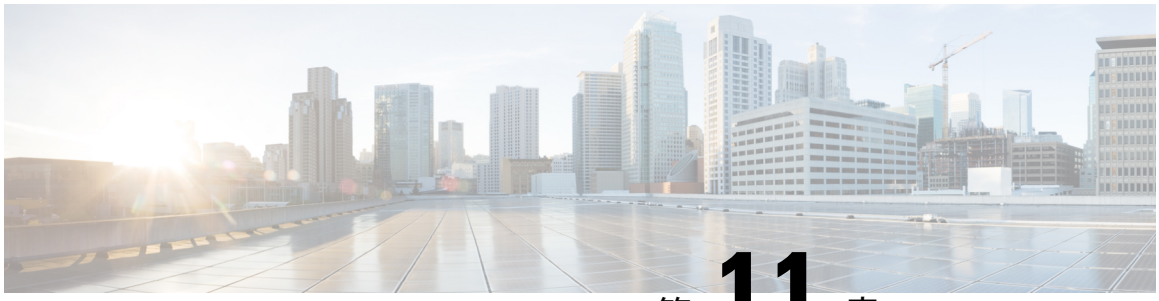
設定用の管理者パスワードを設定する

[共通の電話プロファイル] ウィンドウの **[ローカル電話ロック解除パスワード]** フィールドにパスワードを設定することで、設定アプリケーションへのアクセスを制限できます。

共通の電話プロファイルがデバイスに適用されると、ユーザは設定アプリケーションを開いたときにパスワードの入力を求められます。サインイン画面に、問題報告ツールで問題を報告するリンクがあります。 すべての設定ショートカットがデスクトップから削除されます。 設定のショートカットはシステム トレイから削除されますが、ユーザは通話中に引き続き通話統計にアクセスできます。 ユーザはデスクトップの壁紙を変更できません。

手順

ステップ 1 DX デバイスの **共通電話プロファイル** ウィンドウに移動します。
ステップ 2 **[ローカル電話ロック解除パスワード]** フィールドに英数字のパスワードを入力します。
ステップ 3 変更を保存し、**[構成の適用]** をクリックします。



第 11 章

機能とサービス

- 利用可能な電話機能 （107 ページ）
- 機能ボタン （119 ページ）
- 機能管理ポリシーの設定 （120 ページ）
- 電話ボタン テンプレート （121 ページ）
- 製品固有のオプションを構成する （122 ページ）
- ビデオ送信解像度のセットアップ （136 ページ）
- インスタントメッセージとプレゼンスの設定 （137 ページ）
- アプリケーションのセットアップ （137 ページ）
- Cisco Unified Communications Manager 経由で Android APK ファイルをプッシュする （139 ページ）

利用可能な電話機能

Cisco DX シリーズ デバイスは、Cisco WebEx、Cisco Unified Presence、インスタント メッセージング、電子メール、ビジュアル ボイスメール、音声およびビデオテレフォニー機能を含む、統合されたコラボレーション アプリケーション スイートを提供します。 Cisco Unified Communications Manager これらのデバイスは、Google Play のアプリケーションもサポートします。

ネットワークに Cisco DX シリーズ デバイスをインストールし、ネットワーク設定を構成してデバイスを Cisco Unified Communications Manager 追加した後、Cisco Unified Communications Manager 管理ツールを使用してテレフォニー機能を構成し、サービスをセットアップする必要があります。

（注） Cisco Unified Communications Manager また、さまざまなテレフォニー機能を構成するために使用できるいくつかのサービス パラメータも提供します。 サービス パラメータのアクセスと設定の詳細については、 *Cisco Unified Communications Manager* アドミニストレーション ガイドを参照してください。 サービスの機能の詳細については、**[サービス パラメータ設定（Service Parameter Configuration）]** ウィンドウでパラメータ名をクリックするか、ヘルプ ボタン（?）を選択します。

エージェントのグリーティング

エージェントが事前録音したグリーティングを作成したり更新したりできるようにします。このグリーティングは、エージェントが発信者と話しはじめる前に、顧客コールの開始時に再生されます。エージェントは、必要に応じて1つまたは複数のグリーティングを事前録音できます。

詳細については、以下を参照してください。

- *Cisco Unified Communications Manager* システムガイド、「Cisco Unified IP Phones」の章
- 『*Features and Services Guide for Cisco Unified Communications Manager*』、「割り込みとプライバシー」の章

エージェント グリーティングの有効化

手順

ステップ 1 **[デバイス]**、> **[電話機]** の順に選択します。

ステップ 2 設定するデバイスを見つけます。

ステップ 3 [デバイス情報レイアウト（Device Information Layout）]ペインまでスクロールし、[ビルトインブリッジ（Built In Bridge）] を [オン（On）]または [デフォルト（Default）] 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 ブリッジの設定を確認します。

a) **[System（システム）]** > **[Service Parameters（サービス パラメータ）]** を選択します。
b) 適切なサーバおよびサービスを選択します。
c) [クラスタワイド パラメータ（デバイス - 電話）（Clusterwide Parameters (Device - Phone)）]ペインまでスクロールして、[ビルト イン ブリッジの有効（Builtin Bridge Enable）]を [オン（On）] に設定します。
d) [**保存（Save**）] を選択します。

すべてのコール

ユーザーは、アクティブな通話と保留中の通話のリストを表示できます。このリストは時系列順（古い順）で並べ替えられます。ユーザは着信通話と完了通話のリストも表示できます。このリストは新しいものから古いものの順に並べられています。

プライマリ回線のすべての通話

プライマリ回線ですべての通話機能を利用できるようになります。すべての着信通話はプライマリ回線の通話リストに表示され、プライマリ回線で応答できます。

自動応答

呼出音を 1 ～ 2 回鳴らした後に、着信コールを自動的に接続します。 自動応答はスピーカーフォンでもヘッドセットでも機能します。デバイスでヘッドセットの自動応答が有効になっているが、デバイスにヘッドセットが接続されていない場合、デバイスは通話に自動的に応答しません。

詳細については、*Cisco Unified Communications Manager* アドミニストレーション ガイド、「ディレクトリ番号の設定 「」の章を参照してください。」

自動ダイヤル

発信、着信、不在着信を含む最近の通話履歴から一致する番号をユーザが選択できるようにします。電話をかけるには、ユーザはこれらの通話リストから番号を選択するか、手動で数字を入力し続けることができます。

割込み

ユーザが共有電話回線で非プライベート通話に参加できるようにします。 Barge は、通話にユーザを追加し、通話を会議に変換します。その後、ユーザと他の関係者は会議機能にアクセスできるようになります。

（注） Built In Bridge Enable サービス パラメータがオフに設定されている場合でも、ユーザは引き続き Barge を使用できます。 ユーザがデバイス上で Barge 機能を使用できないようにするには、デバイスの機能管理ポリシーで Barge を無効にする必要があります。

詳細については、以下を参照してください。

- *Cisco Unified Communications Manager* アドミニストレーション ガイド、「Cisco Unified IP Phone のセットアップ」 の章
- *Cisco Unified Communications Manager* システム ガイド、「Cisco Unified IP Phones」 の章
- 『*Features and Services Guide for Cisco Unified Communications Manager*』、「割り込みとプライバシー」 の章
- *Cisco Unified Communications Manager* アドミニストレーション ガイド、「機能制御ポリシーの設定」 の章

ビジー ランプ フィールド

ユーザは、デバイスのスピード ダイヤル ボタン、通話履歴、またはディレクトリ リストに関連付けられているディレクトリ番号の通話状態を監視できます。

詳細については、『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「「IM およびプレゼンス サービス」」の章を参照してください。

通話転送

ユーザは、着信コールを別の番号にリダイレクトできます。コール転送オプションには、すべてのコールの転送、話中転送、無応答時転送、およびカバレッジなし時転送があります。

追加のオプションは次のとおりです:

- ターゲット番号から発信された通話を転送せずにそのまま着信させることができます。
- 転送ループが転送チェーン内のリンクの最大数を超えないようにします。

転送オプションは回線ごとに割り当てることができます。

詳細については、以下を参照してください。

- *Cisco Unified Communications Manager* アドミニストレーション ガイド、「ディレクトリ番号の設定」の章。
- 『*Cisco Unified Communications Manager* システム ガイド』、「「Cisco Unified IP Phones」」の章。

発信者番号通知

ユーザは、完全な外線番号を発信者番号通知に使用できるようになります。

詳細については、『「Cisco Unified IP Phones」』の章を *Cisco Unified Communications Manager* システム ガイドで参照してください。

[発呼者回線IDの表示（Calling Line Identification Presentation）]

ユーザは、ケースバイケースで発信元番号を有効化または制限できます。

詳細については、『「Cisco Unified IP Phones」』の章を *Cisco Unified Communications Manager* システム ガイドで参照してください。

Cisco Extension Mobility

ユーザは、共有デバイス上の Cisco Extension Mobility サービスにログインすることで、そのデバイスから回線アピアランス、サービス、スピードダイヤルなどのデバイス設定に一時的にアクセスできるようになります。

Cisco Extension Mobility は、社内の複数の場所でユーザが業務を行う場合や、作業場を同僚と共有する場合に便利です。

（注） この機能は、Expressway経由のモバイルおよびリモートアクセスで展開されているDXシリーズ デバイスではサポートされません。

デバイスにログインするには、ユーザは管理者が提供する extension mobility 資格情報を入力します。 これらの資格情報は、ユーザの画面ロック PIN とは異なります。

詳細については、「Extension Mobility」の章を参照してください『*Features and Services Guide for Cisco Unified Communications Manager*』。

Extension Mobility マルチユーザ

extension mobility マルチユーザ機能では、extension mobility のログイン/ログアウト プロセスが使用されます。 ユーザがログインすると、Cisco Unified Communications Manager サーバはユーザの資格情報を認証します。サーバは、extension mobility機能と同じメッセージング スキームを使用します。

ユーザ A がデバイスに初めてログインすると、デバイスは再起動サイクルを実行し、デバイス上にユーザ A のユーザ パーティションを作成します。 デバイスはユーザ A にセットアップ ウィザードを提示します。 ユーザ A は個人用アプリとデータ専用のスペースを取得し、通話アプリケーションは他のデバイスと同じように動作します。 Cisco DX シリーズ 最初のログイン後、ユーザ A はアプリ関連の設定を構成します。 ユーザ A がこのデバイスからログアウトすると、ユーザ設定は保存され、次回ユーザ A がデバイスにログインするときに使用されます。

ユーザ A がデバイスからログアウトすると、ユーザ B はユーザ B の資格情報を使用してデバイスにログインできます。 ユーザ B は、ユーザ B パーティションを取得したときに同じエクスペリエンスを得ます。最初のログインでは、セットアップ ウィザードによってユーザ B に個人用アプリとデータを設定するように求められ、ユーザ B には Cisco DX シリーズ デバイスで通常どおりに動作する通話アプリケーションもあります。

パーティションは完全に分離されているため、どのユーザも他のユーザのデータを見ることはできません。

Extension Mobility マルチユーザは、エンタープライズ マルチユーザ アプローチを提供します。システム管理者は、Extension Mobility マルチユーザ用に設定するデバイスを決定し、特定のデバイスにログインできるユーザに資格情報を提供します。 適切な資格情報があれば、ユーザは特定のデバイスにのみログインして自分のアカウントを設定でき、自分のアカウントを削除することもできるようになります。 ユーザは同じデバイス上の他のユーザのアカウントを変更することはできません。

アルゴリズムにより、特定のデバイスにログインできるユーザの数が制限されます。デバイス上の最大ユーザ数は、各ユーザの使用状況によって異なります。 デバイスのフラッシュ メモリが特定の商を下回ると、最も最近ログインしていないユーザのアカウントが削除され、新しいユーザがログインするためのスペースが作成されます。そのため、デバイスのスペース不足が原因で新しいユーザがログインに失敗するという事態は発生しません。

Cisco Extension Mobility の設定

DX シリーズ デバイスに Cisco Extension Mobility を設定するには、次の手順に示す順序で手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、 **デバイス** > **デバイス設定** > **デバイス プロファイル** を選択し、 **新規追加**をクリックします。

a) デバイスタイプを入力します。
b) デバイス プロファイル名を入力し、 **[保存]** をクリックします。
c) ディレクトリ番号と必要な情報を入力し、 **[保存]** をクリックします。

ステップ 2 **[ユーザ管理]** > **[エンドユーザ]** を選択し、ユーザを選択または作成します。

a) Extension Mobility の使用可能なプロファイルで、ユーザ デバイス プロファイルを選択し、下矢印をクリックします。これにより、選択したサービスが [制御プロファイル] ボックスに配置されます。
b) **[保存（Save）]** をクリックします。

ステップ 3 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

a) デバイスの種類を選択してください。
b) ユーザ ID を選択します。
c) **[電話の設定]** ウィンドウの [製品固有の設定レイアウト] 領域の [内線情報] で、[**Extension Mobility を有効にする**] をオンにします。
d) **[電話の設定]** ウィンドウの [製品固有の設定レイアウト] 領域で、[マルチユーザ] ドロップダウン リスト ボックスの **[有効]** 値を選択します。

Cisco モビリティ

ユーザは、単一の電話番号を使用してビジネス通話を管理し、デスクトップ電話と携帯電話などのリモート デバイスで進行中の通話に応答できます。 また、電話番号や時刻に応じて、発信者グループを制限できます。

Cisco Mobility for Cisco DX シリーズ デバイスには、 Cisco Unified Communications Manager リリース 9.0 (1) 以降が必要です。

詳細については、 「Cisco Mobility」 の章を参照してください。 『*Features and Services Guide for Cisco Unified Communications Manager*』

会議

- ユーザは複数の相手と同時に会話することができます。そのために、この機能では各参加者を個別に呼び出します。
- 標準 (アドホック) 会議の参加者全員が参加者を追加または削除できるようにします。
- ユーザは、1 つの回線上にある 2 つ以上の通話を結合して電話会議を作成し、通話を継続することができます。

サービス パラメータ Advanced Adhoc Conference (Cisco Unified Communications Manager ではデフォルトで無効) を使用すると、これらの機能を有効にすることができます。

会議の詳細については、『*Cisco Unified Communications Manager* システム ガイド』の「「会議ブリッジ」」の章を参照してください。

セキュアな会議

セキュア カンファレンスでは、セキュアなデバイスがセキュアなカンファレンス ブリッジを使用して電話会議を行うことができます。新しい参加者が追加されると、すべての参加者が安全なデバイスを使用している限り、安全な通話アイコンが表示されます。

詳細については、以下を参照してください。

- *Cisco Unified Communications Manager* システム ガイド、「会議ブリッジ」の章
- *Cisco Unified Communications Manager* アドミニストレーション ガイド、「会議ブリッジの設定」の章
- 『*Cisco Unified Communications Manager* セキュリティ機能』

即転送

拡張即時転送を有効にすると、ユーザはこの機能を使用して着信コールを音声メッセージングシステムに直接転送できるようになります。

通話をボイスメールに転送する方法の詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』の「「即時転送」」の章を参照してください 。

拡張即時転送の詳細については、「「Cisco Unified IP Phones」」の章を『*Cisco Unified Communications Manager* システム ガイド』で参照してください。

取り込み中

DND をオンにすると、コールが呼び出し状態になっても呼出音が鳴らなくなります。またあらゆる種類の表示や音による通知も、一切行われません。

（注） DND は 911 通話には影響しません。

次の DND 関連のパラメータは、 Cisco Unified Communications Manager 管理で設定できます。

- Do Not Disturb - このチェックボックスを使用すると、デバイスごとに DND を有効にできます。 Cisco Unified Communications Manager 管理で、**デバイス** > **電話** > **電話設定**を選択します。
- [DND 着信呼警告（DND Incoming Call Alert）] : デバイスで 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。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。)

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』の「「Do Not Disturb」」の章を参照してください。

ゲートウェイレコーディング

この機能は、メディア ゲートウェイに通話を録音サーバに送信するように指示し、通話の監視を改善します。

詳細については、「「監視と記録」」 の章を 『*Features and Services Guide for Cisco Unified Communications Manager*』 で参照してください。

保留状態

共有回線を持つデバイスが、通話を保留にしたローカル回線とリモート回線を区別できるようにします。

保留と再開

ユーザは、接続されたコールをアクティブな状態から保留状態に移行できます。

保留音

発信者が保留状態になっている間、音楽を再生します。

詳細については、 「「保留音」」 の章を 『*Features and Services Guide for Cisco Unified Communications Manager*』 で参照してください。

無視

ユーザが通知ウィンドウからの着信を無視できるようにします。

メッセージ受信インジケータ

受話器のライトは、ユーザに 1 つ以上の新しい音声メッセージがあることを示します。

詳細については、以下を参照してください。

- *Cisco Unified Communications Manager* アドミニストレーション ガイド、「メッセージ待機のセットアップ」章
- *Cisco Unified Communications Manager* システム ガイド、 「Cisco Unified Communications Manager へのボイスメール接続」 の章

ミュート

デバイスのスピーカー、ハンドセット、ヘッドセットなど、すべての入力デバイスのオーディオ入力をミュートします。

プラス ダイヤル

ユーザが、 **+** 記号を前に付けて E.164 番号をダイヤルできるようにします。

+ 記号をダイヤルするには、 ***** キーを少なくとも 1 秒間押し続ける必要があります。 これは、オンフックまたはオフフック通話の最初の数字をダイヤルする場合にのみ適用されます。

保護された通話

2 つのデバイス間の安全な (暗号化された) 接続を提供します。 通話の開始時にセキュリティトーンが再生され、両方のデバイスが保護されていることを示します。 保護された通話が設定されている場合、電話会議、共有回線、回線をまたいで参加などの一部の機能は利用できません。 保護された通話は認証されません。

詳細は、『*Cisco Unified Communications Manager* セキュリティ機能』を参照してください。

呼出音の設定

デバイスに別のアクティブ通話があるときに、回線に使用される呼び出し音の種類を識別します。

詳細については、 *Cisco Unified Communications Manager* アドミニストレーション ガイド の『「ディレクトリ番号の設定」』の章を参照してください。

呼出音

ユーザは、着信コールや新しいボイスメッセージをデバイスで示す方法をカスタマイズできます。

安全および非セキュア指示トーン

Cisco Unified Communications Managerでデバイスが安全（暗号化され、信頼済み）として構成されたら、保護されたステータスを与えることができます。その後、必要に応じて、保護されたデバイスが通話の開始時に通知音を再生するように設定できます。

- 保護されたデバイス - Cisco Unified Communications Manager管理でセキュリティ保護されたデバイスのステータスを保護済みに変更するには、**デバイス** 電話**電話の構成** > **で** > **保護されたデバイス**をチェックします。
- [セキュア インディケーション トーンの再生（Play Secure Indication Tone）]：保護されたデバイスで、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）] を [はい（True）] に設定します。 (デフォルトは False です。) このオプションは、 Cisco Unified Communications Manager 管理の **システム** > **サービス パラメータ** で設定します。 サーバを選択し、Cisco CallManager 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。)

保護されたデバイスのみが、これらのセキュアまたは非セキュア通知トーンを聞きます。 (保護されていないデバイスではトーンは聞こえません。)通話中に通話全体の状態が変化すると、それに応じて通知音が変化します。 その時点で、保護されたデバイスは適切なトーンを再生します。

保護されたデバイスは、次の状況で音を再生したり再生しなかったりします。

- トーンを再生するオプションを有効にすると、セキュア通知トーンの再生オプションが有効になります (True)。
  - エンドツーエンドのセキュア メディアが確立され、通話ステータスがセキュアになると、デバイスはセキュア表示トーン (休止を伴う 3 回の長いビープ音) を再生します。
  - エンドツーエンドの非セキュア メディアが確立され、通話ステータスが非セキュアになると、デバイスは非セキュア表示音（短い休止を伴う 6 回の短いビープ音）を再生します。
- [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。

Serviceability

管理者がデバイスからデバッグ情報を迅速かつ簡単に収集できるようにします。

この機能は、SSH を使用して各電話にリモートでアクセスします。 この機能を使用するには、各電話機の SSH が有効になっている必要があります。

共有回線

ユーザは、複数のデバイスで同じディレクトリ番号を共有したり、同僚とディレクトリ番号を共有したりすることができます。

詳細については、*Cisco Unified Communications Manager*『システム ガイド』の「「ディレクトリ番号」」を参照してください。

スピード ダイヤル

ユーザが特定の宛先ディレクトリ番号へのスピードダイヤルを設定できるようにします。

転送

ユーザが自分のデバイスから接続された通話を別の番号にリダイレクトできるようにします。

ユーザは2つの通話を相互に接続できます。ユーザは、通話を続けるか、通話に残らずに転送することができます。

Uniform Resource Identifier ダイヤリング

URI (Uniform Resource Identifier) ダイヤル機能を使用すると、ユーザは、たとえば **bob@cisco.com** のように、英数字の URI アドレスをディレクトリ番号として使用して電話をかけることができます。 ユーザは連絡先を選択するために URI アドレスを入力する必要があります。

画面には URI 呼び出しの通話情報が表示されます。 通話ログには、通話履歴と詳細ページに URI 通話情報が記録されます。

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』 を参照してください。

ビデオ切り替え

ユーザはビデオ コール中にビデオのオン/オフを切り替えることができます。

ボイス メッセージ システム

コールに応答がない場合に、発信者がメッセージを残せるようにします。

詳細については、以下を参照してください。

- 『*Features and Services Guide for Cisco Unified Communications Manager*』
- *Cisco Unified Communications Manager* システム ガイド、「Cisco Unified Communications Manager へのボイスメール接続」 の章

ビジュアル ボイスメールのセットアップ

ビジュアル ボイスメールは、 Cisco Unified Communications Manager 管理からすべてのデバイス、または個々のユーザまたはユーザ グループに対して設定されます。 すべてのデバイスのビジュアル ボイスメールを設定するには、次の手順に従います。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、 **デバイス** > **デバイス設定** > **共通の電話プロファイル**を選択します。

ステップ 2 **[検索]** を選択し、**[標準の共通電話プロファイル]** を選択します。

ステップ 3 **[製品固有の設定レイアウト]** ウィンドウで、**[ボイスメール サーバ(プライマリ)]** フィールドに次の情報を入力します。

- Cisco Unified IP Phone スタンドアロン設定を構成する場合は、Cisco Unified IP Phone システムの完全修飾ドメイン名を入力します。
- Cisco Unified IP Phone フェールオーバー構成を設定する場合は、Cisco Unified IP Phone システムの DNS エイリアスを入力します。

ステップ 4 変更を保存し、**[構成を適用]** をクリックします。

ビジュアル ボイスメールの設定と同期の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「「ボイスメール プロファイルの設定」」の章を参照してください。

特定のユーザまたはグループにビジュアルボイスメールを設定する

特定のユーザまたはユーザ グループに対してビジュアル ボイスメールを設定するには、次の手順に従います。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**デバイス** > **デバイス電話**を選択します。

ステップ 2 検索するユーザに関連付けられているデバイスを選択します。

ステップ 3 **[製品固有の設定レイアウト]** ウィンドウで、**[ボイスメール サーバ(プライマリ)]** フィールドに次の情報を入力します。

- Cisco Unified IP Phone スタンドアロン設定を構成する場合は、Cisco Unified IP Phone システムの完全修飾ドメイン名を入力します。
- Cisco Unified IP Phone フェールオーバー構成を設定する場合は、Cisco Unified IP Phone システムの DNS エイリアスを入力します。

ステップ 4 変更を保存し、**[構成を適用]** をクリックします。

ステップ 5 **[リセット]** および **[再起動]** を選択して、新しい設定をデバイスに配信します。

ステップ 6 デバイス上で安全なメッセージを許可するには、 Cisco Unified Communications Manager 「管理」から、**「システム設定」** > **「詳細な API 構成」** を選択し、**「CUMI 経由で安全なメッセージ記録へのアクセスを許可する」** と **「CUMI 経由でメッセージ添付ファイルを許可する」** の両方を有効にします。

ステップ 7 ディレクトリの写真がビジュアル ボイス メールで構成されるように Cisco Unified Communications Manager を設定するには、**「デバイス」** > **「デバイス設定」** > **「共通の電話プロファイル」** を選択し、「共通の電話プロファイル」 を選択して、**「会社の写真ディレクトリ」** フィールドに組織の写真ディレクトリの URL を入力します。

ビジュアル ボイスメールの設定と同期の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「「ボイスメール プロファイルの設定」」の章を参照してください。

機能ボタン

次の表は、通話コントロールバーで使用できる機能と、プログラム可能な機能ボタンとして設定する必要がある機能に関する情報を示しています。 表内の「X」は、対応するボタンタイプで機能がサポートされていることを示します。 2種類のボタンのうち、プログラム可能な機能ボタンのみ、 Cisco Unified Communications Manager 管理で設定が必要です。

表 *19*：機能と対応するボタン

機能名	通話コントロールバーボタン	プログラマブル機能ボタン
コールバック		X
通話転送	X	
すべてのコールの転送		X
コール パーク	X	
コール ピックアップ		X
Cisco モビリティ		X
会議（追加）	X	
即転送		X
取り込み中		X
終了	X	
グループ ピックアップ		X
保留 (Hold)	X	
ハント グループ		X
インターコム		X
Malicious Call Identification（MCID; 迷惑呼 ID）		X
ミートミー		X
プライバシー		X
リダイヤル		X

機能名	通話コントロールバーボタン	プログラマブル機能ボタン
共有（DX70 および DX80 のみ）	X	
スピード ダイヤル		X
ビデオを停止		X
転送	X	

機能管理ポリシーの設定

機能制御ポリシー設定でこれらの機能を有効または無効にすることで、 Cisco DX シリーズ デバイス上の一部のテレフォニー機能の表示を制限できます。 機能管理ポリシー構成で機能を無効にすると、その機能へのユーザ アクセスが制限されます。

手順

ステップ 1 Cisco Unified Communications Manager 管理から、**デバイス** > **デバイス設定** > **機能管理ポリシー** を選択します。
[機能管理ポリシーの検索と一覧表示] ウィンドウが表示されます。

ステップ 2 **[新規追加]** をクリックして、一連のポリシーを定義します。

ステップ 3 次の設定値を入力します。

- 名前 - 新しい機能管理ポリシーの名前を入力します。
- 説明 - 説明を入力します。
- 機能制御セクション - デフォルト設定を変更する機能のチェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 次の設定にポリシーを含めることで、デバイスにポリシーを適用します。 Cisco DX シリーズ

- エンタープライズパラメータ構成 - システム内のすべてのデバイスに適用されます。 Cisco DX シリーズ
- 共通の電話プロファイル設定 - グループ内のすべてのデバイスに適用されます。 Cisco DX シリーズ
- 電話の構成 - 個々のデバイスに適用されます。 Cisco DX シリーズ

機能制御ポリシーのデフォルト値

次の表に、設定できる機能のリストとデフォルト値を示します。

表 *20* : 機能制御ポリシーのデフォルト値

特長	デフォルト値
割込み	Enabled
コールバック	Enabled
コールピックアップ	Disabled
会議リスト	Enabled
即転送(アラート)	Disabled
即転送(接続済み)	Disabled
[不在転送（Forward All）]	Enabled
グループ通話ピックアップ	Disabled
ミートミー	Disabled
モビリティ	Disabled
その他の通話ピックアップ	Disabled
パーク	Disabled
リダイヤル	Enabled
発信者を報告する	Disabled
品質のレポート	Disabled
スピード ダイヤル	Enabled

詳細については、*Cisco Unified Communications Manager* アドミニストレーション ガイドの『「機能管理ポリシーの設定」』の章を参照してください。

電話ボタン テンプレート

電話ボタン テンプレートを使用すると、スピード ダイヤルやコール処理機能をプログラム可能なボタンに割り当てることができます。

理想的には、ネットワークにデバイスを登録する前にテンプレートを変更します。 この方法では、登録中にカスタマイズされた電話ボタン テンプレートのオプションに Cisco Unified Communications Manager からアクセスできます。

電話ボタンテンプレートの変更

電話サービスの詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「「IP 電話サービスのセットアップ」」の章を参照してください。 回線ボタンの設定の詳細については、*Cisco Unified Communications Manager* アドミニストレーション ガイ

ドの「「Cisco Unified IP Phone のセットアップ」」の章と「「短縮ダイヤルボタンの設定」」の項を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager 管理から、 **デバイス** > **デバイス設定** > **電話ボタンテンプレート**を選択します。

ステップ 2 **[検索（Find）]** をクリックします。

ステップ 3 デバイスモデルを選択します。

ステップ 4 **コピー**を選択し、新しいテンプレートの名前を入力して、 **保存**を選択します。
電話ボタン テンプレートの設定 ウィンドウが開きます。

ステップ 5 割り当てるボタンを確認して、機能が表示されるドロップダウン リストから、その回線に関連付ける [サービス URL（Service URL）]を選択します。

ステップ 6 サービス URL を使用する新しい電話ボタン テンプレートを作成するには、 **[保存]** をクリックします。

ステップ 7 **[デバイス（Device）]** > **[電話（Phone）]** を選択して、デバイスの [**電話の設定（Phone Configuration**）] ウィンドウを開きます。

ステップ 8 **[電話ボタン テンプレート]** ドロップダウン リストから新しい電話ボタン テンプレートを選択します。

ステップ 9 変更を保存するには**[保存]**をクリックし、変更を実装するには**[リセット]**をクリックします。
ユーザはセルフケア ポータルにアクセスし、デバイス上のボタンにサービスを関連付けることができます。

製品固有のオプションを構成する

Cisco Unified Communications Manager 管理では、次のいずれかのウィンドウで、デバイスの製品固有の構成パラメータを設定できます。

- **エンタープライズ電話設定** ウィンドウ (**システム** > **エンタープライズ電話設定**)
- **共通電話プロファイル ウィンドウ** (**デバイス** > **デバイス設定** > **共通電話プロファイル**)、ウィンドウの製品固有の設定レイアウト部分
- **デバイス設定** ウィンドウ（**デバイス** > **電話** > **新規追加** > **Cisco DX650、 Cisco DX70、または Cisco DX80**）の製品固有の設定レイアウト領域

パラメータを設定したら、更新する設定ごとに「共通設定の上書き」チェックボックスをオンにします。 このチェックボックスをオンにしないと、対応するパラメータ設定が有効になりません。 3 つの構成ウィンドウでパラメータを設定すると、設定は次の順序で優先されます。

1. **デバイス構成** ウィンドウ

2. **共通電話プロファイル** ウィンドウ
3. **エンタープライズ電話設定** ウィンドウ

次の表は、デバイス構成ウィンドウで使用できる製品固有の構成オプションを示しています。共通電話プロファイルウィンドウとエンタープライズ電話設定ウィンドウには、デバイス設定ウィンドウにはない製品固有の設定オプションがありますが、それらのその他のオプションはDXシリーズデバイスに影響を与えない場合があります。

表 *21 : Cisco DX* シリーズ 製品固有の構成オプション

特長	説明
スピーカーフォンを無効にする	スピーカーフォン機能のみを無効にします。スピーカーフォン機能を無効にドセットには影響しません。ヘッドセット/ハンドセットで回線とスピードダできます。 デフォルト：False
スピーカーフォンとヘッドセットを無効にする（Disable Speakerphone and Headset）	すべてのスピーカーフォン機能とヘッドセットのマイク機能を無効にします デフォルト：False
USB を無効にする	デバイスの USB ポートを無効にします。 デフォルト：False
SDIO	デバイス上の SDIO デバイスが有効か無効かを示します。 デフォルト：[無効（Disabled）]
Bluetooth	デバイスの Bluetooth サービスが有効か無効かを示します。 デフォルト：[有効(Enabled)]
Bluetooth 連絡先のインポートを許可（Allow Bluetooth Contacts Import）	ユーザが Bluetooth デバイスから連絡先と通話履歴をインポートおよび同期ます。 デフォルト：[有効(Enabled)]
Bluetooth モバイル ハンズフリー モードを許可（Allow Bluetooth Mobile Handsfree Mode）	ユーザがデスクフォンで携帯電話回線を使用できるようにします。 デフォルト：[有効(Enabled)]

特長	説明
ディスプレイ非点灯日（Days Display Not Active）	バックライトをデフォルトでオフのままにする日をユーザが指定できるように デフォルト: 米国の法人顧客の場合、通常は土曜日と日曜日。 （注） リストにはすべての曜日が含まれています。 土曜日と日曜日にバックライトを るには、Control キーを押しながら土曜日と日曜日を選択します。
ディスプレイ点灯時刻（Display On Time）	オフスケジュールにリストされている日にディスプレイが自動的にオンになる ます。 デフォルト: 07:30 最大文字数: 5 （注） 値は 24 時間形式で入力します。00:00 が 1 日の始まり、23:59 が 1 日の終わりで
ディスプレイ点灯継続時間（Display On Duration）	プログラムされたスケジュールによってオンになったディスプレイの、アクテ ある時間を示します。 デフォルト: 10:30 最大文字数: 5 （注） 最大値は 24 時間です。 この値は時間と分の形式です。 たとえば、「01:30」に 分間ディスプレイをアクティブにします。
着信コール時に点灯（Display On When Incoming Call）	デバイスがスクリーンセーバーモードの場合、この設定により、通話が鳴った スプレイがオンになります。 デフォルト：[有効(Enabled)]

特長	説明
Enable Power Save Plus	Power Save Plus 機能を有効にするには、スケジュールに従ってデバイスの電 る日を選択します。 Power Save Plus を実行したい日をクリックする際に、C したままにすると、複数の日を選択できます。 Power Save Plus モードでは、 点灯するのに十分な電力が維持されます。デバイスのその他の機能はすべて す。 Power Save Plus モードでは、[電話の電源オン時間] フィールドと [電話 間] フィールドで指定された時間、デバイスの電源がオフになります。この時 組織の通常の業務時間外になります。点灯したキーを押すと、デバイスの電 復します。点灯したキーを押すと、電話機は電源を入れ直し、Unified CM に から完全に動作するようになります。このフィールドで日を選択すると、e 念事項を示す次の通知が表示されます。 Power Save Plus を有効にすると、こ されている条件に同意したことになります。 Power Save Plus モードが有効な間、このモードに設定されたエンドポイント よび着信通話の受信が無効になります。このモードを選択すると、以下のこ ことになります。 **1.** モードが有効になっている間、緊急通報および電話の受信のための代替 る責任は完全にお客様にあります。 **2.** Cisco は、モードの選択に関連する一切の責任を負いません。モードの有 るすべての責任はお客様が負うことになります。 **3.** モードが通話や呼び出しなどに与える影響について、ユーザに十分に通 デフォルト: 日が選択されていません
電話機をオンにする時刻（Phone On Time）	このフィールドは、[Power Save Plus を有効にする] リスト ボックスで選択さ イスが自動的にオンになる時刻を決定します。 時刻は 24 時間形式で入力し 午前 0 時を表します。 たとえば、午前 7 時 (0700) に自動的に電話をオンに 「07:00」と入力します。 午後 2 時に電話をオンにします。 （1400）の場合 力します。このフィールドが空白の場合、デバイスは 00:00 に自動的にオン デフォルト: 0:00 最大文字数: 5
電話機をオフにする時刻（Phone Off Time）	このフィールドは、[Power Save Plus を有効にする] リスト ボックスで選択さ イスの電源がオフになる時刻を決定します。 時間を「時間:分」の形式で入 のフィールドが空白の場合、デバイスは深夜 (00:00) に自動的にオフになり （注） 電話機の電源オンの時刻が空白（または 00:00）で、電話機の電源オフの時 たは 24:00）の場合、デバイスは継続的にオンの状態になり、EnergyWise に ライドの送信を許可しない限り、Power Save Plus 機能は事実上無効になりま デフォルト: 24:00 最大文字数: 5

特長	説明
Phone Off Idle Timeout	このフィールドは、デバイスが電源供給機器 (PSE) にデバイスの電源をオフに 要求するまでに、デバイスがアイドル状態である必要がある分数を表します。 ルドの値は有効になります。 • デバイスがスケジュールどおりに Power Save Plus モードになっていたが、 キーを押したために Power Save Plus モードが解除されたとき • 付属のスイッチでデバイスに電源が再投入されると • 電話の電源オフの時間が経過したが、デバイスが使用中の場合。 単位は分 フォルトは 60 です。範囲は 20 ～ 1440 です。
Enable Audible Alert	このチェックボックスを有効にすると、デバイスは、[電話の電源オフ時間] フ 指定された時刻の 10 分前に音声アラートを再生するように指示されます。 デ は無効になっています。 このチェックボックスは、[Power Save Plus を有効にす ボックスで 1 日以上が選択されている場合にのみ適用されます。
EnergyWise Domain	このフィールドは、電話デバイスが参加している EnergyWise ドメインを定義しま Save Plus 機能には EnergyWise ドメインが必要です。 [Power Save Plus を有効に ト ボックスで日数を選択した場合は、EnergyWise ドメインも指定する必要があ デフォルトは空白です。 最大文字数: 127
EnergyWise エンドポイントセキュリティシークレット	このフィールドは、EnergyWise ドメイン内で通信するために使用されるパスワ 秘密) を定義します。 Power Save Plus 機能には、EnergyWise ドメインとシーク 要です。 [Power Save Plus を有効にする] リスト ボックスで日数を選択した場合 EnergyWise ドメインとシークレットも提供する必要があります。 デフォルトは 最大文字数: 127

特長	説明
Allow EnergyWise Overrides	このチェックボックスは、EnergyWise ドメイン コントローラ ポリシーが電ベルの更新を送信することを許可するかどうかを決定します。 いくつかの条ます。まず、[Power Save Plus を有効にする] フィールドで 1 日以上を選択すます。 [Power Save Plus を有効にする] リスト ボックスで日が選択されていなイスはデバイスの電源をオフにする EnergyWise 指示を無視します。 2 番目にがオーバーライドを送信した場合でも、Unified CM Administration の設定はスおりに有効になります。 たとえば、ディスプレイの電源オフ時刻が 22:00 (午定され、ディスプレイの電源オン時刻フィールドの値が 06:00 (午前 6 時) でSave Plus の有効化で 1 日以上が選択されているとします。 EnergyWise がデを 20:00 (午後 8 時) にオフにするように指示した場合、その指示は (ユーザにい場合) 設定された電話の電源オン時刻の午前 6 時まで有効のままになりまに、デバイスの電源がオンになり、Unified CM Administration の設定から電力の受信を再開します。 デバイスの電力レベルを再度変更するには、EnergyW力レベル変更コマンドを再発行する必要があります。 また、ユーザによる操効になるため、EnergyWise がデバイスの電源をオフにするように指示した後キーを押すと、ユーザの操作の結果としてデバイスの電源がオンになりますではチェックされていません。
録音トーン	これを使用して、デバイス上で録音トーンを有効にするか無効にするかを設 デフォルト：[無効（Disabled）]
録音トーンのローカルボリューム	これを使用して、ローカル側で聞こえる録音トーンの音量設定を構成できま設定は、聴覚に使用される実際のデバイス (ハンドセット、スピーカーフォント) に関係なく適用されます。 音量設定は 0% ～ 100% の範囲で、0% では音では現在の音量設定と同じレベルになります。 デフォルト値は 100% です。
録音トーンのリモート音量	これを使用して、リモート側で聞こえる録音トーンの音量設定を構成できまは 0% ～ 100% の範囲で、0% は -66dBM 未満、100% は -4dBM になります。は -10dBM または 50% です。
録音トーンの長さ	録音トーンをオーディオ ストリームに挿入する時間の長さをミリ秒単位で示パラメータのデフォルトは、このフィールドのネットワーク ロケール ファイされます。 このパラメータの有効な範囲は 1 ～ 3000 ミリ秒の値です。

特長	説明
G.722およびiSACコーデックをアドバタイズする	通話アプリケーションがワイドバンド コーデックを Cisco Unified Communicatio にアドバタイズするかどうかを示します。 コーデックのネゴシエーションでは、次の 2 つの手順が実行されます。 **1.** 通話アプリケーションは、サポートされているコーデックを Cisco Unified Com Manager にアドバタイズする必要があります 。 **2.** Cisco Unified Communications Manager は、コール アテンプトに関連するす イスから、サポートされているコーデックのリストを取得する際に、地域 など、さまざまな要素に基づいて、一般的にサポートされているコーデッ ます。 [システムデフォルトの使用（Use System Default）] 有効な値は、次のとおりです。 • システムデフォルト - 通話アプリケーションは、エンタープライズパラメ および iSAC コーデックの通知」で指定された設定に従います。 • 無効 - 通話アプリケーションはワイドバンド コーデックを Cisco Unified Com Manager に通知しません。 • 有効 - 通話アプリケーションはワイドバンド コーデックを Cisco Unified Com Manager に通知します。
ビデオ コール（Video Calling）	有効にすると、デバイスがビデオ コールに参加することを示します。 デフォルト：[有効(Enabled)]
デバイス UI プロファイル	デバイスのユーザ インターフェイスの特性を変更して、基本的なビデオ発信者 モード) や一般的なコラボレーション ユーザ (拡張モード) などの特定のユーザ 最適化します。 デフォルト: シンプル

特長	説明
WiFi	デバイスの Wi-Fi が有効か無効かを示します。 （注） エンタープライズ設定と共通設定では、Wi-Fi パラメータがデフォルト値 (有れ、 **[共通設定を上書き]** チェックボックスがオンになっています。 （注） デバイス設定では、Wi-Fi パラメータはデフォルト値 (有効) のままですが、**上書きする]** チェックボックスはオンになっていません。 **ヒント** 企業ポリシーですべてのデバイスの Wi-Fi デフォルトを無効に設定していなレベルおよび共通レベルでの展開環境のデフォルト設定が無効になっている パラメータを有効に設定したデバイス用の新しい共通電話プロファイルを作推奨します。 デフォルト：[有効(Enabled)]
PC Port	PC ポートが有効か無効かを示します。 デフォルト：[有効(Enabled)]
Span to PC Port	デバイスが PC ポートで送受信されるパケットを転送するかどうかを示しま （注） 診断目的で使用される監視および記録アプリケーションやネットワーク パチャ ツールなど、デバイス トラフィックの監視を必要とするアプリケーシトで実行されている場合は、[**有効**] を選択します。 この機能を使用するにVLAN アクセスを有効にする必要があります。 デフォルト：[無効（Disabled）]
PC の音声 VLAN へのアクセス（PC Voice VLAN Access）	PC ポートに接続されたデバイスが音声 VLAN にアクセスできるかどうかを （注） 音声 VLAN アクセスを無効にすると、接続された PC は音声 VLAN 上でデができなくなります。 また、デバイスによって送受信されたデータを PC が防ぎます。 デフォルト：[有効(Enabled)]
PC Port Remote Configuration	リモートでデバイスの PC ポート速度とデュプレックスを設定できます。 デフォルト：[無効（Disabled）]
Switch Port Remote Configuration	デバイスのスイッチ ポート速度とデュプレックスをリモートで構成できまり、デバイス上の手動構成が上書きされます。 デフォルト：[無効（Disabled）]

特長	説明
Unified CM接続障害の検出	このフィールドは、バックアップ Unified CM/SRST へのデバイスのフェールオ生する前の最初のステップである、Cisco Unified Communications Manager（Unif 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。 有効な値は、[Norma 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 倍遅いレートで Unified CM 接続エラーの検出を実行）です。 Unified CM 接続エ 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 ルオーバーを少し遅らせる場合は、[Delayed] を選択します。 通常の接続障害検 続障害検出の間の正確な時間差は、常に変化する多くの変数によって決まるこ てください。 これは有線イーサネット接続にのみ適用されます。 デフォルト：[標準（Normal）]
Gratuitous ARP	デバイスが Gratuitous ARP 応答から MAC アドレスを学習するかどうかを示しま （注） デバイスの Gratuitous ARP 受け入れ機能を無効にすると、音声ストリームの監視 このメカニズムを使用するアプリケーションが動作しなくなります。 デフォルト：[無効（Disabled）]
Cisco Discovery Protocol（CDP）：Switch Port	管理者はスイッチ ポートで CDP を有効または無効にすることができます。 **Warning** デバイスが Cisco 以外のスイッチに接続する場合にのみ、ネットワーク ポート 無効にします。 詳細については、*Cisco Unified Communications Manager* アドミニ ション ガイドを参照してください。 デフォルト：[有効(Enabled)]
Cisco Discovery Protocol（CDP）：PC Port	PC 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：[有効(Enabled)]
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）	管理者はスイッチ ポートでリンク層検出プロトコル(LLDP-MED)を有効または ことができます。 デフォルト：[有効(Enabled)]
Link Layer Discovery Protocol（LLDP）：PC Port	管理者は、PC ポートでリンク層検出プロトコル (LLDP) を有効または無効にす きます。 デフォルト：[有効(Enabled)]

特長	説明
LLDP Asset ID	管理者がリンク層検出プロトコルのアセット ID を設定できるようにします 最大文字数: 32
LLDP 電力の優先順位（LLDP Power Priority）	管理者がリンク層検出プロトコルの電源優先度を設定できるようにします。 デフォルト: 不明
電力ネゴシエーション（Power Negotiation）	管理者が電力ネゴシエーションを有効または無効にできるようにします。 （注） デバイスが電力ネゴシエーションをサポートするスイッチに接続されている ネゴシエーション機能を有効にします。 ただし、スイッチが電力ネゴシエ ポートしていない場合は、PoE+経由でアクセサリに電源を投入する前に、電 ション機能を無効にしてください。 デフォルト：[有効(Enabled)]
Automatic Port Synchronization	電話で PC ポートおよび SW ポートを同じ速度およびデュプレックスに同期 効にします。 自動ネゴシエーション用に設定されているポートのみが速度を デフォルト：[無効（Disabled）]
802.1X 認証	802.1x 認証機能のステータスを指定します。 オプション： • 有効 - デバイスは 802.1X 認証を使用してネットワーク アクセスを要求 • 無効 - デバイスが CDP を使用して VLAN およびネットワーク アクセス フォルト設定。 デフォルト: ユーザ制御
FIPS モード	このパラメータは、デバイスの連邦情報処理標準 (FIPS) モードを設定しま ションを有効にすると、デバイスは FIPS 140-2 レベル 1 準拠デバイスにな デフォルト：[無効(Disabled)]
常時接続 VPN	デバイスが常に VPN AnyConnect クライアントを起動し、設定された VPN プ の接続を確立するかどうかを示します Cisco Unified Communications Manager デフォルト：False
VPN パスワードをデバイスに保存する	このパラメーターは、VPN パスワードをデバイスに保存できるかどうかを制 の値は、パスワードの永続性が true に設定されている場合にのみ使用されま ると、ユーザの VPN パスワードはメモリに保存され、次回の接続時に自動的 ます。 ただし、デバイスを再起動すると、ユーザは VPN パスワードを再度 があります。 有効にすると、ユーザの VPN パスワードがデバイスに保存さ ても保持されます。 デフォルト：False

特長	説明
ユーザ定義の VPN プロファイルを許可する	ユーザが AnyConnect VPN クライアントを使用して VPN プロファイルを作成でかを制御します。 無効にすると、ユーザは VPN プロファイルを作成できませ デフォルト：[True]
画面ロックを要求する	デバイスで画面ロックが必要かどうかを示します。 オプション： • ユーザー制御。 • PIN - 少なくとも 4 桁の数字のパスワード。 • パスワード - 少なくとも 4 文字の英数字で構成される英数字パスワード。文字は数字以外の文字で、もう 1 文字は大文字である必要があります。 デフォルト: PIN
最大画面ロックタイムアウト	デバイスが自動的に画面をロックするまでの最大アイドル時間を秒単位で示しがロックされた後は、ロックを解除するためにユーザパスワードが必要になり デフォルト：600 最小: 15 最大: 1800
ディスプレイオン時に画面ロックを強制する	このパラメータは、Cisco Unified Communications Manager で設定された間隔後がロックされることなく、ユーザが勤務時間中デバイスを自由に操作できるよ目立たないロック ポリシーを提供します。 作業後は、ポリシーで定義されたとイスがロックされ、権限のないユーザがアクセスできないようになります。 デ会議や昼休みなどにユーザが制御する手動ロック オプション (電源ボタン) を常します。 ユーザが次回使用時に PIN/パスワードを入力するまで、デバイスはロままになります。 オン - デバイスは就業時間中またはディスプレイのオン時間されます (デフォルト設定)。 オフ - 上記の曜日/時刻設定に基づいて、デバイスレイがオフになっている時間中または勤務時間後にのみロックされます。 デフォルト：[True] （注） このパラメータを無効にすると、デバイスにインストールされている、ロック画ムアウトに関連するすべてのサードパーティ製デバイス管理ポリシーが上書き
音声通話中にデバイスをロックする	デバイスが充電状態にあり、アクティブな音声通話が進行中の場合、管理者はPIN 強制タイマーをオーバーライドして、音声通話中に画面をアクティブに保きます。 音声通話が完了し、タイマーを超過すると、画面ロック タイマーが有す。 デフォルト：[無効（Disabled）]
Kerberos サーバ	Web プロキシ Kerberos の認証サーバ。 最大文字数: 256

特長	説明
Kerberos レルム	Web プロキシ Kerberos の認証レルム。 最大文字数: 256
ロード サーバ	デバイスが、定義された TFTP サーバではなく、代替サーバを使用してファ ロードとアップグレードを取得することを示します。 デフォルト: ホスト名またはローカルサーバの IP アドレス 最大文字数: 256
ピア ファームウェア共有	サブネット内の単一のデバイスがファームウェア イメージ ファイルを取得し に配布できるようにするために、P2P イメージ配布を有効または無効にしま デフォルト : [有効(Enabled)]
ログサーバー	ログ メッセージが送信されるリモート システムの IP アドレスとポートを指 デフォルト: リモートシステムの IP アドレス 最大文字数: 32
ログプロファイル	事前定義されたデバッグ コマンドをリモートで実行します。 デフォルト: プリセット
Web アクセス（Web Access）	デバイスが Web ブラウザまたはその他の HTTP クライアントからの接続を受 うかを示します。 デフォルト : [無効（Disabled）]
SSH アクセス	このパラメータは、デバイスが SSH 接続を受け入れるかどうかを示します。 SSH サーバ機能を無効にすると、デバイスへのアクセスがブロックされます デフォルト : [無効（Disabled）]
Android デバッグ ブリッジ (ADB)	デバイス上の ADB を有効または無効にします。 有効、無効、またはユーザ制御に設定できます。 デフォルト : [無効（Disabled）]
マルチユーザ	デバイス上でマルチユーザーが有効か無効かを示します。 デフォルト : [無効（Disabled）]
不明なソースからのアプリケーションを許可する	ユーザが URL から、または電子メール、インスタント メッセージ (IM)、ま デジタル (SD) カードから受信した Android アプリケーション パッケージ フ から、デバイスに Android アプリケーションをインストールできるかどうかを 有効、無効、またはユーザ制御に設定できます。 デフォルト : [無効（Disabled）]

特長	説明
Google Play からのアプリケーションを許可する	ユーザが Google Play から Android アプリケーションをインストールできるかどします。 （注） Google Play にある一部のアプリケーションには、GPS や背面カメラなど、デバ利用できないハードウェア要件がある場合があります。 Cisco DX シリーズ Cisc ドパーティのサイトからダウンロードしたアプリケーションが動作することを保せん。 デフォルト：False
Cisco UCMアプリケーションクライアントを有効にする	アプリケーションクライアントがデバイス上で実行されるかどうかを制御しま ケーションクライアントが有効になっている場合、ユーザはインストールする ションを選択できます Cisco Unified Communications Manager。 デフォルト：False
企業写真ディレクトリ	デバイスがユーザを照会し、そのユーザに関連付けられている画像を取得でき 定します。 例: http://www.cisco.com/dir/photo/zoom/%%uid%% (uid は従業員のユーザ ID)。 デフォルト: 写真ディレクトリの URL 最大文字数: 256
ボイスメール サーバ (プライマリ)	プライマリ ビジュアル ボイスメール サーバのホスト名または IP アドレス。 デフォルト: プライマリビジュアルボイスメールサーバの IP アドレス 最大文字数: 256
ボイスメール サーバ (バックアップ)	バックアップ ビジュアル ボイスメール サーバのホスト名または IP アドレス。 デフォルト: バックアップビジュアルボイスメールサーバの IP アドレス 最大文字数: 256
プレゼンスおよびチャット サーバ (プライマリ)	プライマリプレゼンス サーバのホスト名または IP アドレス。 デフォルト: プライマリプレゼンスサーバの IP アドレス 最大文字数: 256
プレゼンスとチャットサーバの種類	デバイスが使用するセカンダリ プレゼンスおよび IM サーバの種類を指定しま Cisco Unified Presence または Cisco WebEx Connect に設定できます。 デフォルト: Cisco WebEx Connect

特長	説明
プレゼンスとチャットのシングルサインオン（SSO）ドメイン	Cisco WebEx Connect Cloud が企業に対してシングル サインオン (SSO) 認証を に使用する企業ドメイン。 デフォルト: 空のフィールド 最大文字数: 256
マルチユーザ URL	このパラメータは、エクステンション モビリティ サーバの URL を指定しま 最大文字数: 256
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）	このパラメータは、Expressway の認証情報をデバイスに保存できるかどうか す。 デフォルト：[無効（Disabled）]
カスタマー サポートのアップロード URL（Customer support upload URL）	これにより、ユーザがエンドポイントの「問題報告ツール」から問題報告フ できるサーバ アドレスが設定されます。 最大文字数: 256
クラッシュレポートを自動的にアップロードする	この機能を有効にすると、このエンドポイントからクラッシュレポートが自 ロードされます デフォルト：[無効（Disabled）]
代替電話帳サーバのタイプ	デフォルトでは、エンドポイントは登録先の UCM 上の UDS サーバを使用し の電話帳サーバを使用する場合は、このパラメーターを代替の電話帳アドレ せることで、エンドポイントのデフォルト設定が上書きされます。 UDS は代 プを UDS として設定します。 デフォルト: UDS
代替電話帳サーバアドレス	デフォルトでは、エンドポイントは登録先の UCM 上の UDS サーバを使用し の電話帳サーバを使用する場合は、このパラメーターと代替の電話帳タイプ ることで、エンドポイントのデフォルト設定が上書きされます。 このフィー 話帳サーバの完全な URL が必要です。 UDS サーバ URL の例: https://uds-host-name:8443/cucm-uds/users。 最大文字数: 256

（注） 校正の詳細については、『*Cisco DX Series Wireless LAN* 導入ガイド』を参照してください。

ビデオ送信解像度のセットアップ

Cisco DX シリーズ デバイスは、高解像度のマルチタッチカラー LCD と内蔵カメラを介してビデオ コールをサポートします。 デバイスがビデオを送受信するには、ビデオ機能を有効にする必要があります Cisco Unified Communications Manager。

（注） ビデオ コール オプションが オフに設定されている場合、ビデオの自動送信 設定は淡色表示になります。 **[製品固有の設定レイアウト]** ウィンドウでビデオ コールが無効になっている場合、[通話設定] メニューのすべてのビデオ設定は淡色表示されます。

表 *22 :* ビデオ送信解像度と機能

ビデオの種類	ビデオ解像度	FPS	ビデオビットレート範囲（帯域幅）	DX650 外部カメラのサポート
240P	432 x 240	15	64～149 kbps	はい、ただし、Logitech C930e は 424 x 240 のビデオ解像度を使用します。
240P	432 x 240	30	150-299 kbps	はい、ただし、Logitech C930e は 424 x 240 のビデオ解像度を使用します。
360p	640 x 360	30	300-599 kbps	対応
480p	848 x 480	30	600-799 kbps	はい、ただし、Logitech C920-C は 864 x 480 のビデオ解像度を使用します。
576p	1024 x 576	30	800-1299 kbps	対応
600p	1024 x 600	30	800-3000 kbps	未対応
720p	1,280 X 720	30	900-1999 kbps	対応
1080p	1920 X 1080	30	2000-4000 kbps	対応
CIF	352×288（4:3）	30	64 ～ 299 kbps	対応
VGA	640×480（4:3）	30	400-1500 kbps	対応

（注） 外部カメラは 600p などの一部の解像度をサポートしておらず、外部カメラが動作できる最小ビット レートは 64 kbps です。

（注） Logitech C920-C ウェブカメラを使用して通話していて、リモート デバイスがパケット化モード 0 のみをサポートしている場合、最大送信解像度は 640x360 になります。 Cisco DX650 パケット化モード 1 を使用する場合、最大送信解像度は 1920x1080 です。

（注） Cisco DX シリーズ デバイスの VGA 経由の最適解像度は w360p です。400 kbps から 999 kbps の範囲の帯域幅の場合、デバイスは w360p を送信します。

インスタントメッセージとプレゼンスの設定

インスタントメッセージングとプレゼンスにより、ユーザはいつでも、どこでも、どのデバイスでも通信できます。 Cisco DX シリーズ デバイスは、Cisco Unified Presence または WebEx バックエンド サーバのいずれかを使用して Jabber IM をサポートします。 セキュリティ上の理由から、クラウドベースの IM およびプレゼンス トラフィックはすべてプロキシ経由でルーティングされます。

インスタント メッセージングとプレゼンスは、デバイスの **[製品固有の設定]** ウィンドウで、デバイス、グループ、またはエンタープライズ レベルで設定されます。 プレゼンスおよび IM サーバ (プライマリ) とプレゼンスおよび IM サーバ (バックアップ) のホスト名または IP アドレスを入力し、プレゼンスおよび IM サーバのタイプを指定します。

アプリケーションのセットアップ

ユーザはアプリケーションをダウンロードして、デバイスの機能をカスタマイズおよび拡張できます。 アプリケーションは Google Play から入手できます。 Cisco Unified Communications Manager 管理では、次のパラメータを設定することでアプリケーションへのアクセスを提供します（個々のデバイス設定ウィンドウまたは **共通の電話プロファイル** ウィンドウの [製品固有の設定レイアウト] 領域）。

- 不明なソースからのアプリケーションを許可する: ユーザが Google Play 以外のソースからアプリケーションをインストールできるかどうかを制御します。
- Google Play からのアプリケーションを許可: ユーザが Google Play からアプリケーションをインストールできるかどうかを制御します。

- Cisco UCM アプリケーション クライアントを有効にする: 管理者がCisco Unified Communications Manager からアプリケーションを送信する機能を制御します。

  UCM アプリは、Cisco Unified Communications Manager で作成された Android アプリケーションを購読または購読解除するために使用できるデバイス上のクライアントです。このクライアントは、Cisco Unified Communications Manager から Android アプリケーションを購読または購読解除するのと同じ機能を提供しますが、デバイスから実行できるという利便性が追加されています。

Cisco UCM アプリケーション クライアントを有効にする

手順

ステップ 1 デバイスの **[デバイス設定]** ウィンドウの [製品固有の設定レイアウト] 部分で、**[Cisco UCM アプリケーション クライアントを有効にする]** チェック ボックスをオンにします。

ステップ 2 [保存（Save）]をクリックします。

ステップ 3 **[設定の適用（Apply Config）]** をクリックします。

このアクションにより、デバイスに UCM アプリ クライアントがインストールされます。

UCM アプリ クライアントがデバイスにインストールされた後、デバイス ユーザは UCM アプリ クライアントにログインして、Cisco Unified Communications Manager で作成されたアプリケーションを登録または登録解除できます。

UCM アプリにログインするためのエンドユーザを作成する

エンド ユーザが UCM アプリにログインできるようにするには、管理者がエンド ユーザを作成し、エンド ユーザをデバイスに関連付け、エンド ユーザをデバイス所有者として割り当てる必要があります。

手順

ステップ 1 エンドユーザを作成します。 （ Cisco Unified Communications Manager 管理で、 **ユーザ管理** > **エンドユーザ** を選択して、新しいエンドユーザを作成します。）

ステップ 2 デバイスをエンド ユーザに関連付けると、デバイスがエンド ユーザの [制御されたデバイス] の下に表示されるようになります。

ステップ 3 エンド ユーザに標準 CCM エンド ユーザ権限を割り当てます。

ステップ 4 デバイスの **[デバイス構成]** ウィンドウで、 **[所有者ユーザ ID]** フィールドにこのエンドユーザを割り当てます。

UCM アプリでユーザをサブスクライブする

デバイスユーザは、デバイス上のUCMアプリを使用して、Cisco Unified Communications Managerで作成されたアプリケーションを登録または登録解除します。

手順

ステップ 1 エンドユーザの資格情報を使用して、デバイス上の UCM アプリにログインします。

ログインに成功すると、UCM アプリには Cisco Unified Communications Manager で作成されたすべての Android アプリケーションが表示されます。

ステップ 2 アプリケーションをサブスクライブするには、アプリケーション名の横にあるチェックボックスをオンにします。

このアクションにより、デバイスへのアプリケーションのダウンロードとインストールがトリガーされます。

（注）
一部のアプリケーションでは、詳細な情報をユーザに提示します。ボックスにチェックを入れたり、アプリケーションを選択すると、ユーザには2番目の画面が表示されます。これらのアプリケーションを登録するには、2 番目の画面のボックスをオンにして、[戻る] をタップします。 このアクションによりインストールがトリガーされます。

ステップ 3 アプリケーションの登録を解除するには、アプリケーション名の横にあるチェックボックスをオフにします。

Cisco Unified Communications Manager 経由で Android APK ファイルをプッシュする

Cisco Unified Communications Managerから Android APK ファイルをプッシュするには、まずアプリケーションを電話サービスとして構成し、次にデバイスをサービスに登録します。

手順

ステップ 1 次の apktool を使用して、APK から AndroidManifest ファイルを抽出します。

http://code.google.com/p/android-apktool/

ステップ 2 Cisco Unified Communications Manager 管理で Android サービスを追加します。

ステップ 3 デバイスを Android サービスに登録します。

Cisco Unified Communications Manager 管理で Android サービスを追加する

Android サービスを Cisco Unified Communications Manager 管理で追加するには、次の手順に従います。

始める前に

APK から AndroidManifest ファイルを抽出した後、この手順を使用します。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、 **デバイス** > **デバイス設定** > **電話サービス**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **サービス名** フィールドに、APK から抽出した AndroidManifest ファイルのパッケージ名と一致する名前を入力します。

ステップ 4 **[サービス カテゴリ]** ドロップダウン リスト ボックスで、 **[Android APK]** を選択します。

ステップ 5 このウィンドウの他のフィールドはオプションです。AndroidManifest ファイルに表示される情報を入力できます。

ステップ 6 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 7 **[保存（Save）]** をクリックします。

Android Phone サービスにデバイスを登録する

始める前に

デバイスをその電話サービスに登録する前に、 Cisco Unified Communications Manager 管理で Android 電話サービスを追加する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、 **デバイス** > **電話**を選択します。

ステップ 2 表示される **[電話の検索と一覧表示]** ウィンドウで、Android電話サービスにサブスクライブするデバイスを見つけます。

ステップ 3 選択したデバイスのデバイス名エントリをクリックします。

ステップ 4 デバイスの [**電話の設定**（**Phone Configuration**）] ウィンドウで、[**関連事項**（**Related Links**）] ドロップダウン リストボックスの [**サービスの登録/登録解除**（**Subscribe/Unsubscribe Services**）] を選択します。

<device name> の [登録済みの Cisco IP Phone サービス] ウィンドウが開きます。

ステップ 5 デバイスの [登録済みの Cisco IP Phone サービス] ウィンドウで、[**サービスを選択**] ドロップダウン リスト ボックスを使用して、作成したサービスを選択します。

このアクションにより、指定したサービスへのデバイスの登録が開始されます。

ステップ 6 [次へ（Next）]をクリックします。

ステップ 7 [登録（Subscribe）]をクリックします。

第 12 章

[カスタマイズ（Customization）]

- ワイドバンドコーデックのセットアップ （143 ページ）
- 動作モード （144 ページ）
- デフォルトの壁紙 （145 ページ）
- SSH アクセス （147 ページ）
- Unified Communications Manager Endpoints Locale Installer （147 ページ）
- 国際コールのロギングのサポート （148 ページ）

ワイドバンドコーデックのセットアップ

デフォルトでは、G.722 コーデックはデバイスに対して有効になっています。 Cisco DX シリーズCisco Unified Communications Manager が G.722 を使用するように設定されており、通話先が G.722 をサポートしている場合、G.711 の代わりに G.722 コーデックを使用してコールします。

この状態は、ユーザがワイドバンド ヘッドセットまたはワイドバンド ハンドセットを有効にしているかどうかを問わず発生します。ヘッドセットまたはハンドセットが有効になっている場合、ユーザはコール中の音声の感度がより高く感じられます。感度が高いということは、音声の明瞭度が向上することを意味しますが、同時に、紙が擦れる音や近くの会話などの背景ノイズが、通話相手によく聞こえるようになることも意味します。ワイドバンドのヘッドセットやハンドセットがない場合でも、G.722 のさらなる感度を好むユーザもいるかもしれません。他のユーザにとっては、G.722 のさらなる感度が煩わしく感じられるかもしれません。

Advertise G.722 Codec サービス パラメータは、パラメータが設定されている管理ウィンドウに応じて、このサーバに登録されているすべてのデバイスまたは特定のデバイスに対してワイドバンド サポートが存在するかどうかに影響します。 Cisco Unified Communications ManagerCisco Unified Communications Manager

- G.722 コーデックのアドバタイズ フィールド: Cisco Unified Communications Manager 管理から、 **システム** > **エンタープライズ パラメータ** を選択します。 このエンタープライズ パラメータのデフォルト値は **True** です。つまり、このCisco Unified Communications Manager に登録されているすべての Cisco DX シリーズ デバイスが G.722 を Cisco Unified Communications Manager に通知します 。 試行された通話の各エンドポイントが機能セットで G.722 をサポートしている場合、Cisco Unified Communications Manager は可能な限りそのコーデックを通話に選択します。

- 特定のデバイスが G.722 コーデックを通知します。Cisco Unified Communications Manager 管理から、**[デバイス]**>**[電話] を選択します**。 この製品固有のパラメータのデフォルト値には、エンタープライズ パラメータで指定されている値を使用します。 デバイスごとにこれを上書きする場合は、[**電話の設定**] ウィンドウの [製品固有の設定] 領域にある [G.722 コーデックのアドバタイズ] パラメータで [**有効**] または [**無効**] を選択します。

動作モード

Cisco DX シリーズ デバイスはさまざまなモードで機能します。

- パブリックモード
- シンプルモード
- 拡張モード

デフォルトはシンプルモードです。

次の表は、各モードでユーザが利用できる機能を示しています。

特長	パブリックモード	シンプルモード	拡張モード
通話アプリケーション	対応	対応	対応
ロック画面	未対応	対応	対応
ネットワーク設定	未対応	対応	対応
ホーム画面	未対応	対応	対応
ウィジェットとショートカットを追加または削除する	未対応	対応	対応
ビジュアル ボイスメール	未対応	対応	対応
Cisco User Data Service	対応	対応	対応
Bluetooth	対応	対応	対応
日付と時刻を設定する	未対応	対応	対応
最近のアプリケーションリスト	未対応	対応	対応
外部ストレージデバイス	未対応	未対応	対応
Jabber IM	未対応	未対応	対応
Android アプリケーション	未対応	未対応	対応

動作モードの設定

始める前に

シンプル モードまたはパブリック モードのデバイスでは、Android Debug Bridge (ADB) を無効にすることをお勧めします。 シンプル モードまたはパブリック モードでは電子メール アプリケーションが無効になっているため、ユーザは問題レポート ツールを使用してログを管理者に電子メールで送信できません。 ログは、サービスアビリティ Web ページから収集する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager サーバに最新のデバイス パックをインストールします。デバイス パックのインストールの詳細については、 *Cisco DX* シリーズのリリース ノートを参照してください。

ステップ 2 **[エンタープライズ電話の構成]** ウィンドウ、 **[共通の電話プロファイル]** ウィンドウ、または **[電話の構成]** ウィンドウで、 **[デバイス UI プロファイル]** を必要なモードに設定します。

ステップ 3 **共通設定を上書き**をチェックします。
拡張モードからパブリック モードまたはシンプル モードに切り替えると、デバイスが再起動します。 パブリック モードまたはシンプル モードから拡張モードに切り替えると、デバイスも再起動します。パブリックモードとシンプルモードを切り替えても、デバイスは再起動しません。

デフォルトの壁紙

デバイスの Cisco Unified Communications Manager 管理ページから、管理者またはユーザがデバイスのデフォルトの壁紙を設定できるかどうかを制御できます。DX シリーズデバイスの各タイプには、5 つのホーム画面にまたがる異なるサイズの壁紙画像が必要です。

壁紙コントロールの割り当て

デフォルトでは、ユーザはデバイスの壁紙を変更できます。

手順

ステップ 1 **[デバイス（Device）]>[デバイスの設定（Device Setting）]>[共通の電話プロファイル（Common Phone Profile）]** に移動します。

ステップ 2 壁紙の制御を管理者に制限するには、**[エンドユーザによる電話の背景画像設定へのアクセスを有効にする]** のチェックを外します。

デフォルトの壁紙を指定する（DX70 および DX80）

Cisco DX70 および DX80 の壁紙には、2985x1080 の画像解像度を推奨します。 壁紙は 5 つの画面にまたがって表示され、各画面の幅は 1920 ピクセルです。

手順

ステップ 1 TFTP サービスを実行しているすべてのノードの Desktops/2985x1080x24 フォルダーに壁紙画像をアップロードします。

ステップ 2 TFTP を実行しているすべてのノードで TFTP サービスを再起動します。

ステップ 3 Cisco Unified Communications Manager 管理の DX70 および DX80 共通電話プロファイルに移動し、次の変更を行います。

a) **「エンドユーザによる電話の背景画像設定へのアクセスを有効にする」のチェックを外します。**

b) **壁紙画像**のファイル名を背景画像に入力します。

c) **共通設定を上書きするをチェックします。**

ステップ 4 設定を保存して、共通の電話プロファイルに適用します。

ステップ 5 電話デバイスのページに移動し、壁紙を読み込むデバイスに設定を適用します。

大規模なエンドポイントネットワークがある場合は、すべてのデバイスに設定を適用するか、Cisco Unified Communications Manager サーバを再起動して、すべてのエンドポイントがイメージを取得するようにします。

デフォルトの壁紙を指定する (DX650)

Cisco DX650 の壁紙には、1569x600 の画像解像度を推奨します。 壁紙は 5 つの画面にまたがって表示され、各画面の幅は 1024 ピクセルです。

手順

ステップ 1 TFTP サービスを実行しているすべてのノードの Desktops/1569x600x24 フォルダーに壁紙画像をアップロードします。

ステップ 2 TFTP を実行しているすべてのノードで TFTP サービスを再起動します。

ステップ 3 Cisco Unified Communications Manager 管理の DX650 共通電話プロファイルに移動し、次の変更を行います。

a) **[背景イメージ設定へのアクセスの有効化(Enable End User Access to Phone Background Image Setting)]** のチェックを解除します。

b) **壁紙画像**のファイル名を背景画像に入力します。

c) **共通設定を上書きするをチェックします。**

ステップ 4 設定を保存して、共通の電話プロファイルに適用します。

ステップ 5 電話デバイスのページに移動し、壁紙を読み込むデバイスに設定を適用します。

大規模なエンドポイントネットワークがある場合は、すべてのデバイスに設定を適用するか、すべてのエンドポイントがイメージを取得するように Cisco Unified Communications Manager サーバを再起動します。

SSH アクセス

ポート 22 経由の SSH デーモンへのアクセスを有効または無効にすることができます。ポート 22 を開いたままにすると、デバイスはサービス拒否 (DoS) 攻撃に対して脆弱になります。 デフォルトでは、SSH デーモンは無効になっています。

SSH アクセスでは、次の順序で 2 セットの資格情報を入力する必要があります。

1. Cisco Unified Communications Manager 構成のセキュアシェル情報セクションで指定されたセキュアシェルユーザとセキュアシェルパスワード
2. デバッグユーザ ID とパスワード

SSH アクセス フィールドは次のウィンドウにあります。

- 共通電話プロファイルの設定 (**デバイス** > **デバイス設定** > **共通電話プロファイル**)
- 電話の設定 (**デバイス** > **電話ウィンドウ**)

Unified Communications Manager Endpoints Locale Installer

デフォルトでは、デバイスは英語 (米国) ロケールに設定されています。 他のロケールでデバイスを使用するには、クラスタ内のすべてのサーバに、ロケール固有のバージョンの Unified Communications Manager Endpoints Locale Installer をインストールする必要があります。 Cisco Unified Communications Manager ロケール インストーラーは、電話のユーザ インターフェイスの最新の翻訳テキストと国固有の電話トーンをシステムにインストールし、デバイスで使用できるようにします。

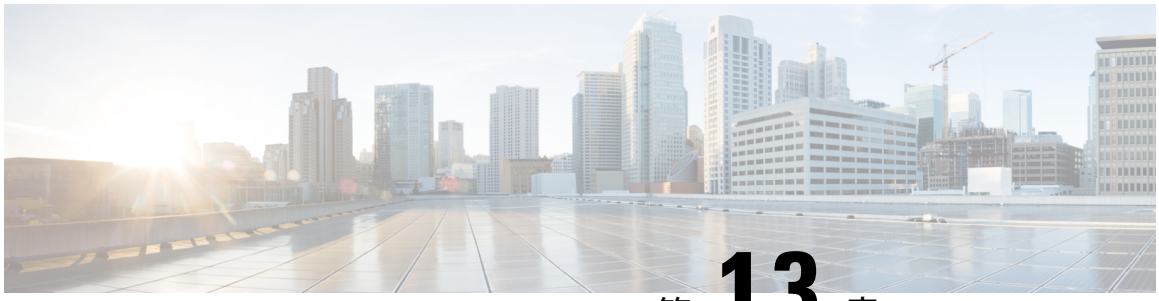
リリースに必要な Locale Installer にアクセスするには、http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245 にアクセスし、お使いのデバイス モデルに移動して、Unified Communications Manager Endpoints Locale Installer リンクを選択します。

詳細については、『*Cisco Unified Communications Operating System* 管理ガイド』の「「ロケールインストーラ」」のセクションを参照してください。

（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。

国際コールのロギングのサポート

電話システムが国際通話記録（発信者正規化）用に設定されている場合は、通話記録、リダイヤル、または通話ディレクトリのエントリに、現在地の国際エスケープ 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、 「+」 を正しい国際ダイヤル コードに置き換えるか、ダイヤルする前に番号を編集して、 「+」 を自分の場所の国際エスケープ コードに手動で置き換える必要がある場合があります。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。



第 13 章

メンテナンス

- デバイスをリセットする （149 ページ）
- オプションをリセットしてアップグレードをロードする （151 ページ）
- リモートロック （151 ページ）
- リモートワイプ （152 ページ）
- Cisco DX70 の代替イメージを起動する （153 ページ）
- Cisco DX80 の代替イメージを起動する （153 ページ）
- Cisco DX650 の代替イメージを起動する （153 ページ）
- データ移行 （154 ページ）
- デバッグログプロファイル （154 ページ）
- ユーザサポート （155 ページ）

デバイスをリセットする

デバイスのリセットは、さまざまな構成やセキュリティ設定をリセットまたは復元する方法、またはデバイスにエラーが発生した場合にデバイスを回復する方法を提供します。

次の手順では、実行できるリセットの種類について説明します。

（注） これら3つのリセット方法では、すべてのユーザデータが削除され、デバイスのすべての設定がリセットされます。

リセットを実行すると、デバイスでは次のことが起こります。

- ユーザ構成設定 - デフォルト値にリセットします。
- ネットワーク構成設定 - デフォルト値にリセットします。
- 通話履歴 – 消去されます。
- ロケール情報 - デフォルト値にリセットされます。

- セキュリティ設定 - デフォルト値にリセットします。これには、CTL ファイルの削除と、802.1x デバイス認証パラメータの 無効への変更が含まれます。

（注） 工場出荷時設定へのリセットプロセスが完了するまで、デバイスの電源を切らないでください。

手順

これらのいずれかの操作でデバイスをリセットできます。 状況に応じて適切な操作を選択します。

- 方法 1: Cisco Unified Communications Manager 管理者 Web GUI
  1. デバイス構成ウィンドウの製品固有の構成レイアウト領域から、**[デバイスをワイプ]** を有効にします。
  2. 管理 GUI から Apply Config、Restart、または Reset コマンドを発行して、デバイスにワイプをプッシュします。
- 方法 2: 設定アプリケーション
  1. 設定アプリケーションで、**[バックアップとリセット]** > **[工場出荷時のデータリセット]** を選択します。

     （注）
     デバイスに PIN またはパスワードが設定されている場合は、リセットを続行する前にそれを入力する必要があります。
- 方法 3: キー押下シーケンス

  デバイスが PIN またはパスワードロックで保護されており、PIN/パスワードを紛失した場合は、この方法を使用する必要があります。

  起動時に Cisco DX70 をリセットするには、次の手順に従ってください。
  1. デバイスの電源を入れ、ミュート LED が点滅するまで待ちます。
  2. **音量アップ** ボタンを、 **ミュート** ボタンが赤く点灯するまで押し続けます。
  3. **音量アップ** ボタンを放し、 **ミュート** ボタンを 3 秒間押し続けます。

  起動時に Cisco DX80 をリセットするには、次の手順に従ってください。
  1. **音量アップ** ボタンを押し続け、デバイスの電源を入れます。
  2. **音量アップ**ボタンを放し、**ミュート**ボタンが赤く点灯したら**ミュート**ボタンを押します。

起動時にリセットするには、次の手順に従ってください。 Cisco DX650

1. # キーを押したままデバイスの電源を入れます。
2. メッセージ待機インジケータ (MWI) が 1 回赤色に点滅してから点灯に変わったら、# キーを放します。

オプションをリセットしてアップグレードをロードする

Cisco DX シリーズ デバイスは構成の変更とロードのアップグレードを Cisco Unified Communications Manager から受け取ります。 次のプロトコルは、デバイスが変更要求を処理する方法を説明します。

- リセットはアクティブな通話が終了するまで待機します。
- デバイスの画面がオンの場合、変更内容と再起動の必要性についてユーザーに通知するポップアップ ダイアログ ボックスが表示されます。 ダイアログ ボックスには次のオプションがあります。
  - 再起動: ポップアップ ダイアログ ボックスを閉じて、デバイスを再起動します (デフォルトのアクション)。
  - スヌーズ: ポップアップ ダイアログ ボックスを 1 時間後に再表示します。 ユーザはデバイスを最大 24 時間スヌーズするように設定でき、その後デバイスは再起動します。

（注） ポップアップ ダイアログ ボックスには 60 秒のカウントダウン タイマーがあります。 ユーザが何も操作しない場合は、デフォルトのアクションが開始されます。

ユーザがデバイスをスヌーズに設定した後、通知リストからいつでもデバイスを手動でリセットすることができます。

- デバイスの画面がオフの場合、アクティブオーディオはリクエストを待機し続けます。

リモートロック

この機能を使用すると、 Cisco Unified Communications Manager のデバイス構成ウィンドウからデバイスをロックできます。

デバイスがリモートロック要求を受信すると、デバイスはアクティブな通話を直ちに終了し、デバイスがロックされます。要求時にデバイスがシステムに登録されていない場合、デバイスは次にシステムに登録されたときにロックされます。

（注） リモート ロック要求を発行した後は、その要求をキャンセルすることはできません。

リモートロック デバイス

手順

ステップ 1 デバイスの **電話の設定** ウィンドウで、 **ロック**をクリックします。

ステップ 2 ロック確認メッセージを受け入れるには、 **[ロック]** をクリックします。

デバイスの**「電話の設定」**ウィンドウの「デバイスのロック/ワイプ ステータス」セクションでロック ステータスを確認できます。

リモートワイプ

この機能を使用すると、Cisco Unified Communications Manager 内のデバイス構成ウィンドウからデバイス上のデータを消去できます。

デバイスはリモートワイプ要求を受信すると、アクティブな通話を直ちに終了し、デバイスのデータを消去します。要求時にデバイスがシステムに登録されていない場合は、デバイスが次にシステムに登録されたときにデータが消去されます。

（注） リモートワイプ要求を発行した後は、その要求をキャンセルすることはできません。

デバイスのリモートワイプ

手順

ステップ 1 デバイスの **[電話の設定]** ウィンドウで、 **[ワイプ] をクリックします。**

ステップ 2 ワイプ確認メッセージを受け入れるには、 **ワイプ** をクリックします。

デバイスの「**電話の設定**」ウィンドウの「デバイスのロック/ワイプ ステータス」セクションでワイプ ステータスを確認できます。

Cisco DX70 の代替イメージを起動する

手順

ステップ 1 デバイスの電源を入れ、ミュート LED が点滅するまで待ちます。
ステップ 2 **音量ダウン** ボタンを、 **ミュート** ボタンが赤く点灯するまで押し続けます。
ステップ 3 **音量ダウン** ボタンを放し、 **ミュート** ボタンを 3 秒間押し続けます。

Cisco DX80 の代替イメージを起動する

手順

ステップ 1 **音量ダウン** ボタンを押したままデバイスの電源を入れます。
ステップ 2 **音量ダウン**ボタンを放し、**ミュート**ボタンが赤く点灯したら**ミュート**ボタンを押します。

Cisco DX650 の代替イメージを起動する

手順

ステップ 1 デバイスをオフにするには電源を外します。
ステップ 2 ***** キーを押したまま、電源を接続します。
ステップ 3 メッセージ LED が点灯するまで、 ***** キーを押し続けます。
ステップ 4 メッセージ LED が 3 回点滅したら、 ***** キーを放します。
デバイスは代替イメージを使用して起動します。

データ移行

データ移行機能により、ファームウェアのアップグレード後にデータの非互換性が存在する場合でも、工場出荷時の状態にリセットする必要がなくなります。

（注） ファームウェアを以前のリリースにダウングレードすると、データが失われる可能性があります。 新しいファームウェア リリースにアップグレードすると、データを失うことなく以前のリリースに戻すことができなくなる可能性があります。

以前のファームウェアにダウングレードしてもデバイスがデータを移行できない場合は、アラームが表示されます。ユーザにユーザデータをバックアップするか、デバイスのリモートワイプを実行するように指示します。 デバイスが Cisco Unified Communications Manager に登録されると、デバイスは以前の工場出荷時設定へのリセットを検出し、移行、ダウングレード、および再起動を無効にします。デバイスが再起動すると、ダウングレードされたファームウェアがロードされます。

デバッグログプロファイル

デバイスまたはデバイス グループのデバッグ ログ プロファイルをリモートで有効にすることができます。

通話処理のデバッグログプロファイルを設定する

手順

ステップ 1 個々のデバイス設定ウィンドウまたは共通の電話プロファイル ウィンドウの [製品固有の設定レイアウト] 領域に移動します。

ステップ 2 **ログ プロファイル**をチェックし、テレフォニーを選択します。

ステップ 3 変更を保存します。

ステップ 4 通知領域でデバッグ ログが有効になっていることがユーザに通知されます。ユーザはメッセージを展開して詳細情報を確認できますが、通知を閉じることはできません。

デバッグログプロファイルをリセットしてデフォルトにする

手順

ステップ 1 個々のデバイス設定ウィンドウまたは共通の電話プロファイル ウィンドウの [製品固有の設定レイアウト] 領域に移動します。

ステップ 2 **ログ プロファイル**をチェックし、 **デフォルト** を選択して、すべてのデバッグをデフォルト値にリセットします。 これには、Android Debug Bridge から手動で設定されたデバッグが含まれます。

ステップ 3 変更を保存して適用します。

ステップ 4 現在のデバッグ レベルを維持するには、 **プリセット** を選択します。

ステップ 5 変更を保存します。

ユーザサポート

デバイスの一部の機能を正常に使用するには、ユーザは管理者またはネットワーク チームから情報を受け取るか、管理者に連絡してサポートを受ける必要があります。 支援を求める際の連絡先の担当者の名前、およびそれらの担当者に連絡する手順をエンドユーザに提供しておく必要があります。

Cisco では、社内サポート サイトに、デバイスに関する重要な情報をユーザに提供する Web ページを作成することを推奨しています。

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に必要となります。 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。

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ーアドレスを追加する必要があります。

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.");
}

?>
```

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、[共通の電話プロファイル（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。

Web ブラウザからスクリーンショットを撮る

手順

ブラウザを使用して、次の URL にアクセスします:**http://<Endpoint IP Address>/CGI/Screenshot**
認証を求めるプロンプトが表示されます。 関連付けられているユーザーIDとパスワードを使用します。

デバイスからスクリーンショットを撮る

手順

音量ダウン ボタンと **電源/ロック** ボタンを 3 秒間押します。

アプリケーションサポート

問題がデバイスの問題なのか、アプリケーションの問題なのかを評価します。 問題がアプリケーション関連である場合は、アプリケーション support center に直接お問い合わせください。

第 14 章

モデル情報のステータスと統計

- モデル情報 （159 ページ）
- デバイスのステータス （160 ページ）

モデル情報

モデル情報を表示するには、設定アプリケーションで **「デバイスについて」** を選択します。モデル情報画面には、次の表に示す項目が含まれます。

表 *23 : Cisco DX* シリーズ デバイスのモデル情報

項目	説明
ステータス	デバイスに関する追加情報を提供するサブメニュー。
Cisco ユーザガイド	ドキュメントへのリンクを提供します。
法的情報	オープンソースライセンスが含まれています。
モデル番号	モデル番号。
Android バージョン	Android のバージョンを示します。
カーネルバージョン	Linux カーネル番号。
ビルド番号	現在のソフトウェア ビルド。
SELinux ステータス	強制または許容を示します。
Cisco 負荷情報	
アクティブ ロード（Active Load）	現在インストールされているファームウェアのバージョン。
前回のアップグレード（Last Upgrade）	前回ファームウェアをアップグレードした日付。

項目	説明
（注） デバイスがアップグレード中の場合、「Cisco 負荷情報」グループの下に「アップグレードの進行状況」メッセージが表示されます。	
Cisco Unified Communications Manager	
アクティブ サーバ（Active server）	デバイスが登録されているサーバの DNS または IP アドレス。
スタンバイサーバ	スタンバイ サーバの DNS または IP アドレス。
Cisco Collaboration 問題報告ツール	
Cisco Collaboration 問題報告ツール	問題を報告するためのツール。タップして、日付、時刻、問題アプリケーションの説明、およびカスタマーサポート電子メールアドレスを選択して入力します。ログ情報を収集してサポートに送信するには、**メールレポートの作成** をタップします。

ユーザがセキュアまたは認証済みのサーバに接続している場合、サーバオプションの右側にあるホーム画面に、対応するアイコン（錠前または証明書マーク）が表示されます。ユーザがセキュアまたは認証済みのサーバに接続していない場合、アイコンは表示されません。

デバイスのステータス

デバイスのステータスを表示するには、設定アプリケーションで **[デバイス情報]** > **[ステータス]** を選択します。

表 *24* : デバイスのステータス

項目	説明
ステータス メッセージ	重要なシステム メッセージのログが表示されるステータス メッセージ画面を提供します。
MDN	デバイスのモバイルディレクトリ番号を示します。
IP アドレス(IP address)	デバイスの IP アドレスを示します。
Wi-Fi MAC アドレス	現在の Wi-Fi 接続の MAC アドレスを提供します。
イーサネット MAC アドレス	現在のイーサネット接続の MAC アドレスを提供します。
Bluetooth アドレス	Bluetooth チップセットの MAC アドレスを提供します。
DHCP 情報	DHCP 情報画面を表示します。

項目	説明
Up time	デバイスの実行時間。
現在のアクセスポイント	該当する場合、現在のアクセスポイント画面が表示されます。
イーサネット統計	イーサネットトラフィックの統計を表示するイーサネット統計画面を提供します。
WLAN 統計	該当する場合、WLAN 統計画面が表示されます。
通話統計（音声）	現在の通話のオーディオ部分のカウンターと統計を提供します。
通話統計（ビデオ）	現在の通話のビデオ部分のカウンターと統計を提供します。
通話統計（プレゼンテーション）	現在の通話のプレゼンテーション部分のカウンターと統計を提供します。

ステータス メッセージ

ステータス メッセージ画面には、デバイスが生成した最新のステータス メッセージが 50 件表示されます。 次の表では、表示される可能性のあるステータス メッセージについて説明します。 この表には、エラーに対処するために実行できるアクションも含まれています。

ステータス メッセージ画面を表示するには、**[ステータス メッセージ] をタップします。**

現在のステータス メッセージを削除するには、**[クリア]** をタップします。

ステータス メッセージ画面を終了するには、**[OK]** をタップします。

表 *25 :* 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
CFG TFTP サイズ エラー（CFG TFTP Size Error）	構成ファイルがファイル システムに対して大きすぎます。	デバイスの電源を一度切ってから入れ直しま
チェックサム エラー（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。	デバイス ファームウェアの新しいコピーを取ディレクトリに配置します。 TFTP サーバ ソシャットダウンされている場合にのみ、このファイルをコピーしてください。そうしない破損する可能性があります。

メッセージ	説明	考えられる状況と対処方法
DHCP タイムアウト（DHCP timeout）	DHCP サーバが応答しませんでした。	• ネットワークがビジー状態です - ネットワー減されると、エラーは自動的に解決されます • DHCP サーバとデバイスの間にネットワークません - ネットワーク接続を確認してくださ • DHCP サーバがダウンしています - DHCP サを確認してください。 • エラーが続く場合 - 静的 IP アドレスの割り当てください。
DNS タイムアウト（DNS timeout）	DNS サーバが応答しませんでした。	• ネットワークがビジー状態です - ネットワー減されると、エラーは自動的に解決されます • DNS サーバとデバイスの間にネットワーク接せん - ネットワーク接続を確認してください • DNS サーバがダウンしています - DNS サー確認してください。
DNS 不明ホスト（DNS unknown host）	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。	• TFTP サーバのホスト名または Cisco Unified Communications Manager が DNS で正しく設ることを確認します。 • ホスト名ではなく IP アドレスの使用を検討い。
IP が重複しています（Duplicate IP）	デバイスに割り当てられた IP アドレスを別のデバイスが使用しています。	• デバイスに静的 IP アドレスがある場合は、アドレスが割り当てられていないことを確認い。 • DHCP を使用している場合は、DHCP サーバ認してください。

ロケールの更新エラー（Error update locale）	1 つ以上のローカリゼーション ファイルが TFTPPath ディレクトリで見つからなかったか、または有効ではありませんでした。 ロケールは変更されませんでした。	Cisco Unified Communications Managerから、次の TFTP ファイル管理のサブディレクトリ内にあるします。
		• ネットワーク ロケールと同じ名前のサブディ存在するファイル：
		  • tones.xml
		• ユーザ ロケールと同じ名前のサブディレクトるファイル：
		  • 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 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。	デバイスがデータベースに追加されたときに が作成されます。 Cisco Unified Communicatio イスが Cisco Unified Communications Manager 追加されていない場合、TFTP サーバは CFG Found という応答を生成します。 • デバイスが登録されていません Cisco Un Communications Manager。 デバイスの自動登録を許可していない場 を手動で Cisco Unified Communications M る必要があります。 • DHCP を使用している場合は、DHCP サ TFTP サーバを指定していることを確認 • スタティック IP アドレスを使用してい サーバの設定を確認してください。
IP アドレス解放（IP address released）	デバイスは IP アドレスを解放するように設定されています。	デバイスは、電源を入れ直すか、DHCP アド するまでアイドル状態のままになります。
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はデバイスと互換性がありません。	このデバイスのハードウェア変更をサポート ジョンのソフトウェアをこのデバイスにイン とした場合に発生します。 デバイスに割り当てられたロード ID を確認 Unified Communications Managerから **デバイス** ます)。 デバイスに表示されているロードを
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。	• デバイスに静的 IP アドレスがある場合 ルータが設定されていることを確認しま • DHCP を使用している場合は、DHCP サ ト ルータを提供していません。 DHCP サ 確認してください。
DNS サーバ IP がありません（No DNS server IP）	名前は指定されていましたが、DHCP またはスタティック IP 設定で DNS サーバのアドレスが指定されていませんでした。	• デバイスに静的 IP アドレスがある場合 が設定されていることを確認します。 • DHCP を使用している場合は、DHCP サー バを提供していません。 DHCP サーバの ください。

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 ファイルがデバイスにインストールされていません。	Cisco Unified Communications Manager で信頼リストれていないため、デフォルトではセキュリティがれません。 信頼リストの詳細については、『*Cisco Unified Co Manager* セキュリティ機能』 を参照してくださ
Cisco Unified Communications Manager 要求による再起動	デバイスは Cisco Unified Communications Manager からの要求に基づいて再起動しています。	Cisco Unified Communications Managerでデバイスが行われ、**[適用]** が押されて変更が有効になったます。
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 TFTP サーバを指定していることを確認して • スタティック IP アドレスを使用している場サーバの設定を確認してください。
TFTP エラー（TFTP error）	デバイスは、TFTP サーバが提供したエラー コードを認識しません。	Cisco Technical Assistance Center (TAC) にお問い合い。
TFTP タイムアウト（TFTP timeout）	TFTP サーバが応答しませんでした。	• ネットワークがビジー状態です - ネットワー減されると、エラーは自動的に解決されます • TFTP サーバとデバイスの間にネットワークません - ネットワーク接続を確認してくださ • TFTP サーバがダウンしています - TFTP サー確認してください。
タイムアウト（Timed Out）	サプリカントは 802.1X トランザクションを試行しましたが、認証子がないためタイムアウトしました。	通常は、802.1X がスイッチに設定されていない場タイムアウトします。
信頼リストの更新に失敗し、検証に失敗しました	CTL ファイルと ITL ファイルの更新に失敗しました。	エラーが発生した場合に表示されるメッセージ。
バージョン エラー（Version error）	ロードファイルの名前が正しくありません。	デバイス ロード ファイルの名前が正しいことをください。
XmlDefault.cnf.xml、またはデバイス名に対応する.cnf.xml	コンフィギュレーション ファイルの名前。	なし。 この構成ファイルは、構成ファイルの名前メッセージを提供します。

イーサネット統計

イーサネット統計画面には、デバイスとネットワークのパフォーマンスに関する情報が表示されます。 次の表では、この画面に表示される情報について説明します。

イーサネット統計を表示するには、設定アプリケーションで**デバイス情報**>**ステータス**>**イーサネット統計** を選択します。

Rx フレーム、Tx フレーム、および Rx ブロードキャストの統計を 0 にリセットするには、**[クリア] をタップします**。

イーサネット統計画面を終了するには、**[OK] をタップします**。

表 *26* : イーサネット統計メッセージ情報

項目	説明
Rx フレーム	受信パケット数
Tx フレーム（Tx Frames）	送信されたパケットの数
Rx Broadcasts	受信したブロードキャストパケットの数
ポート 1	スイッチポートの速度とデュプレックス
ポート 2	PC ポートの速度とデュプレックス
CDP ステータス	現在の CDP ステータス

WLAN 統計

WLAN 統計画面には、デバイスと WLAN に関する統計が表示されます。 次の表では、この画面に表示される情報について説明します。

WLAN 統計画面を表示するには、**[デバイス情報]** > **[ステータス]** > **[WLAN 統計] を選択します**。

WLAN 統計画面を終了するには、**[OK] をタップします**。

表 *27* : *WLAN* 統計

項目	説明
Tx バイト（tx bytes）	送信されたバイト数
Rx バイト（rx bytes）	受信されたバイト数
Tx パケット（tx packets）	送信されたデータパケットの数
rx パケット（rx packets）	受信したデータパケットの数

項目	説明
tx パケット ドロップ（tx packets dropped）	ドロップされた送信データパケットの数
Rx パケット ドロップ（rx packets dropped）	ドロップされた受信データパケットの数
Tx パケット エラー（tx packet errors）	送信データパケットエラーの数
Rx パケット エラー（rx packet errors）	受信データパケットエラーの数
Tx フレーム	送信されたフレームの数
tx マルチキャスト フレーム	ブロードキャストまたはマルチキャストとして送信されたフレームの数
tx リトライ	受信デバイスによって確認されて1回再送信されるメッセージの数
tx マルチ リトライ（tx multi retry）	成功までの送信再試行回数
Tx 失敗（tx failure）	送信に失敗したフレームの数
RTS 成功（rts success）	対応する CTS が受信されました
RTS 失敗（rts failure）	受信に失敗したフレームの数。
ACK 失敗（ack failure）	アクセスポイントが送信を確認しなかった
Rx 重複フレーム（rx duplicate frames）	送信された重複マルチキャストパケットの数
Rx フラグメント パケット（rx fragmented packets）	受信されたフラグメント パケットの数
ローミングカウント	現在のアクセスポイントからローミングした回数

音声通話統計

デバイスの「音声通話統計」にアクセスして、最新の通話のカウンター、統計、音声品質メトリックを表示します。

（注） Webブラウザを使用してストリーミング統計Webページにアクセスし、通話統計情報をリモートで表示できます。 この Web ページには、デバイスでは利用できない追加の RTP 制御プロトコル (RTCP) 統計が含まれています。

1回の通話に複数の音声ストリームが含まれる場合がありますが、最後の音声ストリームのデータのみがキャプチャされます。 音声ストリームは、2 つのエンドポイント間のパケット ストリームです。 一方のエンドポイントが保留になると、コールが引き続き接続されている場合でも、音声ストリームは停止します。 コールが再開されると、新しい音声パケット ストリームが開始され、以前のコール データは新しいコール データによって上書きされます。

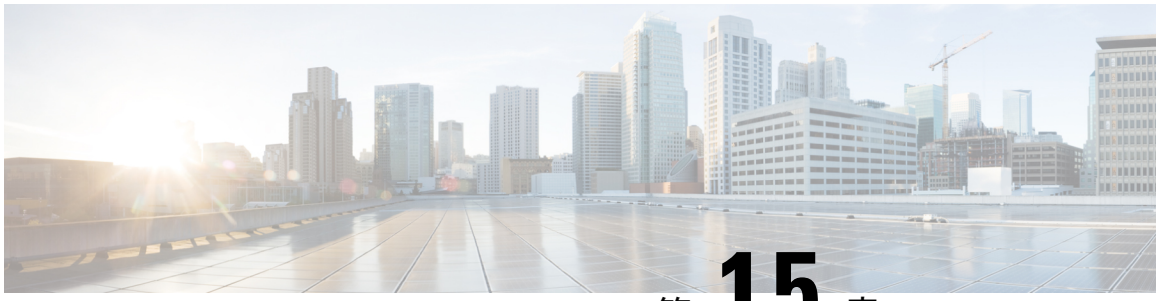
最新の音声ストリームに関する情報を表示するには、通話統計(音声)を表示するには、**[設定]**> **[端末情報]** > **[ステータス]** > **[通話統計 (音声)]** を選択します。

次の表では、「通話統計 (音声)」画面に表示される項目の一覧と説明を示します。

表 *28 :* コールの統計の項目

項目	説明
受信コーデック	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): AAC-LD、G.722、iSAC、G.711 u-law、G.711 A-law、iLBC、および G.729。
[送信コーデック（Sender Codec）]	送信される音声ストリームのタイプ (コーデックからの RTP ストリーミング オーディオ): AAC-LD、G.722、iSAC、G.711 u-law、G.711 A-law、iLBC、および G.729。
受信サイズ	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）。
[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かれてから受信された RTP 音声パケットの数。 （注） この数は、通話が保留になっている可能性があるため、通話開始以降に受信した RTP 音声パケットの数と必ずしも一致しません。
[送信パケット（Sender Packets）]	音声ストリームが開かれてから送信された RTP 音声パケットの数。 （注） この数は、通話が保留になっている可能性があるため、通話開始後に送信された RTP 音声パケットの数と必ずしも一致しません。

項目	説明
[平均ジッター（Avg Jitter）]	受信音声ストリームが開始されてから観測された、推定平均RTPパケットジッタ(パケットがネットワークを通過するときに発生する動的遅延)(ミリ秒単位)。
[最大ジッター（Max Jitter）]	受信音声ストリームが開始されてから観測された最大ジッター（ミリ秒単位）。
受信破棄	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） デバイスは、Ciscoゲートウェイが生成するペイロードタイプ19のコンフォートノイズパケットを破棄し、このカウンタが増加します。
[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）。 欠落したRTPパケットの割合が括弧内に表示されます。
Cumulative conceal ratio	隠蔽フレームの合計数を、音声ストリームの開始から受信した音声フレームの合計数で割ったもの。
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) が使用されている場合は、3秒間のアクティブな音声を蓄積するのに、より長い間隔が必要になることがあります。
Max conceal ratio	音声ストリームの開始以降、最も高い間隔の隠蔽率。
[フレーム損失発生秒数（Conceal Secs）]	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 Secs）]	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。
送信者 DSCP	送信側SIPシグナリングパケットのDSCP値
レシーバーのDSCP	受信側SIPシグナリングパケットのDSCP値
送信者 RTCP DSCP	送信側RTPパケットのDSCP値
受信側 RTCP DSCP	送信側RTPパケットのDSCP値



第 15 章

リモートモニタリング

- Web ページへのアクセスを有効または無効にする （169 ページ）
- デバイスの Web ページにアクセスする （170 ページ）
- デバイス情報 （171 ページ）
- ネットワークのセットアップ （172 ページ）
- セキュリティ情報 （178 ページ）
- イーサネット統計 （180 ページ）
- WLAN セットアップ （183 ページ）
- デバイス ログ （184 ページ）
- ストリームの統計 （185 ページ）

Web ページへのアクセスを有効または無効にする

セキュリティ上の理由から、デバイスの Web ページへのアクセスはデフォルトで無効になっています。 これにより、この章で説明されている Web ページおよびセルフ ケア ポータルへのアクセスが防止されます。

手順

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

ステップ 2 デバイスを検索するための条件を指定して **[検索]** をクリックするか、 **[検索]** をクリックしてすべての電話のリストを表示します。

ステップ 3 デバイス名をクリックして、そのデバイスの **[電話の設定（Phone Configuration）]** ウィンドウを開きます。

ステップ 4 「製品固有の構成」セクションまで下にスクロールします。 **[Web アクセス]** ドロップダウン リストから、 **[有効]** を選択して Web ページへのアクセスを有効にするか、 **[無効]** を選択して Web ページへのアクセスを無効にします。

ステップ 5 **[保存（Save）]** をクリックします。

（注）
Cisco 品質レポート ツールなどの一部の機能は、デバイスの Web ページにアクセスしないと正しく機能しません。 Web アクセスを無効にすると、Web アクセスに依存するすべての保守アプリケーションにも影響します。

デバイスの Web ページにアクセスする

手順

ステップ 1 デバイスの IP アドレスを取得するには、次のいずれかの方法を使用します。

- Cisco Unified Communications Manager のデバイスを検索するには、**[デバイス]** > **[電話]** を選択します。 Cisco Unified Communications Manager に登録されているデバイスの IP アドレスは、 **[電話の検索と一覧表示]** ウィンドウと **[電話の設定]** ウィンドウの上部に表示されます。
- デバイスで、 **[設定]** > **[デバイス情報]** > **[ステータス]** > **[DHCP 情報]** を選択し、Wi-Fi またはイーサネットの IP アドレスを取得します。

ステップ 2 Web ブラウザを開き、次の URL を入力します。 <IP_address> はデバイスの IP アドレスです。

```
http://<IP_address>
```

デバイスの Web ページには次のトピックが含まれています。

- デバイス情報 - デバイスの設定と関連情報を提供します。
- ネットワーク設定 - ネットワーク設定情報を提供します。
- セキュリティ情報 - セキュリティ情報を提供します。
- イーサネット統計 - ネットワーク トラフィックに関する情報を提供する次のハイパーリンクが含まれます。
  - イーサネット情報 - イーサネット トラフィックに関する情報を提供します。
  - アクセス - デバイスとの間のネットワーク トラフィックに関する情報を提供します。
  - ネットワーク - デバイスとの間のネットワーク トラフィックに関する情報を提供します。
- WLAN セットアップ
  - 現在の AP - 現在のアクセスポイントに関する情報を提供します
  - WLAN 統計 - WLAN トラフィックに関する情報を提供します

- デバイス ログ - トラブルシューティングに使用できる情報を提供する次のハイパーリンクが含まれます。
  - コンソール ログ - 個々のログ ファイルへのハイパーリンクが含まれます。
  - コア ダンプ - 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。
  - ステータス メッセージ - デバイスが最後に電源投入されてから生成された最新のステータス メッセージを最大 10 件提供します。
  - デバッグ表示 - トラブルシューティングのサポートが必要な場合に、Cisco Technical Assistance Center (TAC) に役立つ可能性のあるデバッグ メッセージを提供します。
- ストリーミング統計 - オーディオとビデオの統計、ストリーム 1、ストリーム 2、ストリーム 3、ストリーム 4、ストリーム 5、ストリーム 6 のハイパーリンクが含まれており、さまざまなストリーミング統計が表示されます。

デバイス情報

デバイス Web ページのデバイス情報領域には、デバイスの設定と関連情報が含まれます。

表 *29* : [デバイス情報（*Device Information*）] 領域の項目

項目	説明
イーサネットネットワークの状態	イーサネットネットワークの状態
Wi-Fi ネットワークの状態	Wi-Fi ネットワークの状態
MAC Address	イーサネット MAC アドレス
WLAN MAC アドレス	Wi-Fi 接続用の IP アドレス
ホスト名（Host Name）	MAC アドレスに基づいてデバイスに自動的に割り当てられる一意の固定名
電話機の電話番号	デバイスに割り当てられたディレクトリ番号
バージョン	デバイスで実行されているファームウェアの識別子
Hardware Revision	デバイスハードウェアのリビジョン値
シリアル番号（Serial Number）	デバイスの一意のシリアル番号

項目	説明
モデル番号（Model Number）	デバイスのモデル番号
メッセージ待機	デバイスのプライマリ回線で音声メッセージが待機中かどうかを示します。
UDI	デバイスに関する次の Cisco Unique Device Identifier (UDI) 情報を提供します。 • [デバイス タイプ（Device Type）] : ハードウェア タイプを示します。 • デバイスの説明: 指定されたモデル タイプに関連付けられているデバイスの名前を提供します。 • シリアル番号: デバイスの一意のシリアル番号を指定します。
時刻	デバイスが属する Cisco Unified Communications Manager の日付/時刻グループから取得した時刻です
タイムゾーン (Time zone)	デバイスが属する Cisco Unified Communications Manager の日付/時刻グループから取得したタイムゾーンです
日付	デバイスが属する Cisco Unified Communications Manager の日付/時刻グループから取得した日付です

ネットワークのセットアップ

デバイスの Web ページの [ネットワーク設定] 領域には、ネットワーク設定情報と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、デバイスの設定アプリケーションから表示および設定できます。

表 *30 :* ネットワーク設定項目

項目	説明
Wi-Fi 情報	
Wi-Fi DHCP サーバ	デバイスが Wi-Fi IP アドレスを取得する動的ホスト構成プロトコル (DHCP) サーバの IP アドレス。
Wi-Fi MAC アドレス	デバイスの Wi-Fi メディア アクセス コントロール (MAC) アドレス。
Wi-Fi ホスト名	DHCP サーバがデバイスに割り当てたホスト名。
Wi-Fi ドメイン名	デバイスが存在するドメイン ネーム システム (DNS) ドメインの名前。

項目	説明
Wi-Fi IP アドレス	デバイスのインターネット プロトコル (IP) アドレス。
Wi-Fi サブネット マスク	デバイスで使用されるサブネット マスク。
Wi-Fi デフォルトルータ	デバイスで使用されるデフォルトのルーター。
Wi-Fi DNS サーバ 1	デバイスで使用されるプライマリ ドメイン ネーム システム (DNS) サーバ。
Wi-Fi DNS サーバ 2	デバイスで使用されるオプションのバックアップ DNS サーバ。
Wi-Fi EAP 認証	EAP 認証設定を示します
Wifi SSID	現在の Wi-Fi SSID を表示します
Wi-Fi セキュリティモード	現在の Wi-Fi セキュリティモードを示します
Wi-Fi 80211 モード	現在の Wi-Fi 80211 モードを示します
イーサネット情報	
イーサネット DHCP サーバ	デバイスが IP アドレスを取得する動的ホスト構成プロトコル (DHCP) サーバの IP アドレス。
イーサネット MAC アドレス	デバイスのメディア アクセス制御 (MAC) アドレス。
イーサネットホスト名	DHCP サーバがデバイスに割り当てたホスト名。
イーサネットドメイン名	デバイスが存在するドメイン ネーム システム (DNS) ドメインの名前。
イーサネット IP アドレス	デバイスのインターネット プロトコル (IP) アドレス。
イーサネット サブネット マスク	デバイスで使用されるサブネット マスク。
イーサネット DNS サーバ 1	デバイスで使用されるプライマリ ドメイン ネーム システム (DNS) サーバ。
イーサネット DNS サーバ 2	デバイスで使用されるオプションのバックアップ DNS サーバ。
接続先 VLAN ID（Operational VLAN ID）	デバイスがメンバーとなっている Cisco Catalyst スイッチ上に設定された補助仮想ローカル エリア ネットワーク (VLAN)。
管理。 VLAN ID	デバイスがメンバーとなっている補助 VLAN。

項目	説明
PC VLAN	PC に送信されたパケットから 802.1P/Q タグを識別して削除するために使用される VLAN。
SW ポート速度	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。 • A - 自動ネゴシエーション • 10H - 10BaseT/半二重 • 10F - 10BaseT/全二重 • 100H - 100BaseT/半二重 • 100F - 100BaseT/全二重 • 1000F - 1000BaseT/全二重 • リンクなし - スイッチポートに接続されていません
PC ポート速度	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。 • 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 • リンクなし - スイッチポートに接続されていません
IPv6 情報	
IP アドレッシング モード（IP Addressing Mode）	IP アドレス指定モードを示します。
IP 設定モード制御（IP Preference Mode Control）	IP 優先モードを示します。
IPv6 自動設定（IPv6 Auto Configuration）	IPv6 自動構成が有効か無効かを示します。
重複アドレス検出	重複アドレス検出が有効か無効かを示します。
[リダイレクトメッセージを承認(Accept Redirect Messages)]	リダイレクト メッセージの受け入れが有効か無効かを示します。
[マルチキャストのエコー要求に応答(Reply Multicast Echo Request)]	マルチキャスト エコー要求への応答が有効か無効かを示します。
IPv6 アドレス	電話機のインターネット プロトコル バージョン 6 (IPv6) アドレス。

項目	説明
IPv6 プレフィックス長（IPv6 Prefix Length）	IPv6 プレフィックスの長さを示します。
IPv6デフォルトルータ	デフォルトのルーターを示します。
IPv6 DNS サーバ 1（IPv6 DNS Server 1）	デバイスで使用されるプライマリ DNS サーバ。
IPv6 DNS サーバ 2（IPv6 DNS Server 1）	デバイスで使用されるオプションのバックアップ DNS サーバ。
IPv6 代替 TFTP（IPv6 Alternate TFTP）	デバイスが代替 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）	デバイスで使用されるプライマリ TFTP (Trivial File Transfer Protocol) サーバ。
IPv6 TFTP サーバ 2（IPv6 TFTP Server 2）	デバイスで使用されるバックアップ TFTP (Trivial File Transfer Protocol) サーバ。
CUCM 設定	
CUCM サーバ 1-5	デバイスが登録できるサーバのホスト名または IP アドレス (優先順位順)。 Cisco Unified Communications Manager 限定的な機能を提供できる SRST ルーターが存在する場合、その IP アドレスが項目に表示されることもあります。 Cisco Unified Communications Manager 利用可能なサーバの場合、項目にはサーバの IP アドレスと次のいずれかの状態が表示されます。 Cisco Unified Communications Manager • **アクティブ** - デバイス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 • **スタンバイ** - Cisco Unified Communications Manager 現在のサーバが利用できなくなった場合にデバイスが切り替えるサーバ • **空白** - 現在このサーバに接続されていません Cisco Unified Communications Manager アイテムには、限定された機能セットで機能を提供できるSRSTルーターを識別する Survivable Remote Site Telephony (SRST) 指定も含まれる場合があります。 Cisco Unified Communications Manager 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、コール処理の制御を引き継ぎます。 SRST Cisco Unified Communications Manager は、アクティブな場合でも常にサーバ リストの最後に表示されます。 SRST ルータのアドレスは、Cisco Unified Communications Manager 管理の [デバイス プール] ウィンドウで設定します。

項目	説明
情報 URL	この機能は Cisco DX シリーズ デバイスではサポートされていません。
ディレクトリ URL（Directories URL）	この機能は Cisco DX シリーズ デバイスではサポートされていません。
メッセージURL（Messages URL）	この機能は Cisco DX シリーズ デバイスではサポートされていません。
Services URL	この機能は Cisco DX シリーズ デバイスではサポートされていません。
[自動転送遅延(Forwarding Delay)]	リスニング状態と学習状態に費やされる時間。
アイドルURL（Idle URL）	この機能は Cisco DX シリーズ デバイスではサポートされていません。
[URLのアイドル時間（Idle URL time）]	この機能は Cisco DX シリーズ デバイスではサポートされていません。
Proxy Server URL	この機能は Cisco DX シリーズ デバイスではサポートされていません。
認証 URL（Authentication URL）	この機能は Cisco DX シリーズ デバイスではサポートされていません。
TFTP サーバ 1（TFTP Server 2）	デバイスで使用されるプライマリ TFTP (Trivial File Transfer Protocol) サーバ。
TFTP サーバ 2（TFTP Server 2）	デバイスで使用されるバックアップ TFTP (Trivial File Transfer Protocol) サーバ。
代替 TFTP（Alternate TFTP）	デバイスが代替 TFTP サーバを使用しているかどうかを示します。
[ユーザロケール(User Locale)]	デバイス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、日付と時刻の書式、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詳細な情報のセットを識別します。
ネットワークロケール	デバイスユーザに関連付けられているネットワーク ロケール。デバイスが使用するトーンやリズムの定義など、特定の場所でデバイスをサポートするための詳細情報のセットを識別します。
ユーザ ロケール バージョン（User Locale Version）	デバイスに読み込まれているユーザ ロケールのバージョン。

項目	説明
ネットワーク ロケール バージョン（Network Locale Version）	デバイスにロードされているネットワーク ロケールのバージョン。
PC ポートを無効にする（PC Port Disabled）	デバイスの PC ポートが有効か無効かを示します。
GARP を使う（GARP Enabled）	デバイスが Gratuitous ARP 応答から MAC アドレスを学習するかどうかを示します。
ビデオ機能を使う	デバイスがビデオ コールに参加できるかどうかを示します。
音声 VLAN アクセスが有効	デバイスが PC ポートに接続されたデバイスに音声 VLAN へのアクセスを許可するかどうかを示します。
自動回線選択	デバイスで自動選択回線が有効になっているかどうかを示します。
通話制御用の DSCP	コール制御シグナリングの DSCP IP 分類。
セットアップのDSCP。	デバイス構成転送の DSCP IP 分類。
サービスのDSCP	デバイスベースのサービスのための DSCP IP 分類。
セキュリティ モード	デバイスに設定されているセキュリティ モード。
Web アクセス（Web Access）	デバイスの Web アクセスが有効 (はい) か無効 (いいえ) かを示します。
スパン PC ポート	デバイスがネットワーク ポートで送受信されるパケットをアクセス ポートに転送するかどうかを示します。
PC ポート上の CDP	PC 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）。 Cisco Unified Communications Managerで CDP が無効になっている場合、警告が表示され、PC ポートで CDP を無効にすると CVTA が動作しなくなることを示します。 現在の PC およびスイッチ ポート CDP 値は、設定アプリケーションに表示されます。

項目	説明
SW ポートの CDP	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)。 デバイスの VLAN 割り当て、電力ネゴシエーション、QoS 管理、および 802.1x セキュリティのために、スイッチ ポートで CDP を有効にします。 デバイスが Cisco スイッチに接続されている場合は、スイッチ ポートで CDP を有効にします。 Cisco Unified Communications Managerで CDP が無効になっている場合、デバイスがシスコ以外のスイッチに接続されている場合にのみ、スイッチ ポートでCDP が無効になっていることを示す警告が表示されます。 現在の PC およびスイッチ ポート CDP 値は、設定アプリケーションに表示されます。
LLDP-MED SW ポート	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。
LLDP PC ポート	リンク層検出プロトコル（LLDP）が PC ポートで有効かどうかを示します。
LLDP 電力の優先順位（LLDP Power Priority）	デバイスの電源優先度をスイッチに通知し、スイッチがデバイスに適切に電力を供給できるようにします。 次の設定があります。 • 不明 - デフォルト • 低 • 高 • クリティカル（Critical）
LLDP Asset ID	在庫管理のためにデバイスに割り当てられた資産 ID を識別します。
Switch Port Remote Configuration	管理者は、 Cisco Unified Communications Manager 管理を使用して、デバイス テーブル ポートの速度と機能をリモートで構成できます。
PC Port Remote Configuration	管理者は、 Cisco Unified Communications Manager 管理を使用して、デバイス テーブル ポートの速度と機能をリモートで構成できます。

セキュリティ情報

デバイスの Web ページのセキュリティ情報領域には、CTL ファイルと ITL ファイル、および 802.1X 認証に関する情報が含まれています。

表 *31* : セキュリティ情報項目

項目	説明
シグナリングセキュリティモード	シグナリング セキュリティ モードを示します。
LSC	デバイスに LSC がインストールされているかどうかを示します。
CAPF サーバ (IPv4)	IPv4 の CAPF サーバアドレスを示します
CAPF サーバ (IPv6)	IPv6 の CAPF サーバアドレスを示します
CAPF ポート（HTTP Port）	CAPF ポートを示します
CTL ファイル	
CTL 署名（CTL Signature）	CTL 署名を表示する
CUCM サーバ/TFTP サーバ	CUCM/TFTP サーバのアドレスを示します
アプリケーション サーバ	アプリケーションサーバを示します
CAPF サーバ（CAPF Server）	CAPF サーバを示します
ITL ファイル	
ITL 署名（CTL Signature）	ITL 署名を表示する
CAPF サーバ（CAPF Server）	CAPF サーバを示します
TVS	TVS アドレスを示す
CUCM サーバ/TFTP サーバ	CUCM/TFTP サーバのアドレスを示します
設定ファイル	ITL 構成ファイルがデバイスにインストールされているかどうかを示します
802.1X 認証	
デバイス認証	802.1X デバイス認証が有効かどうかを示します。
Transaction Status（トランザクション ステータス）	802.1X トランザクション ステータスが有効かどうかを示します。

項目	説明
プロトコル	802.1X プロトコルを示します。
デバイス ID	デバイス ID を表示します。

イーサネット統計

デバイスの Web ページにある次のイーサネット統計ハイパーリンクは、ネットワーク トラフィックに関する情報を提供します。 ネットワーク統計領域を表示するには、デバイスの Web ページにアクセスします。

- イーサネット情報: イーサネット トラフィックに関する情報を提供します。 最初の表では、この領域の項目について説明します。
- アクセス領域: デバイスとの間のネットワーク トラフィックに関する情報を提供します。 2 番目の表では、この領域の項目について説明します。
- ネットワーク領域: デバイスとの間のネットワーク トラフィックに関する情報を提供します。 2 番目の表では、この領域の項目について説明します。

表 *32 : [*イーサネット情報（*Ethernet Information***）*]* の項目**

項目	説明
Tx フレーム（Tx Frames）	デバイスによって送信されたパケットの合計数
Tx ブロードキャスト	デバイスによって送信され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	デバイスによって送信されたマルチキャスト パケットの合計数
Tx ユニキャスト	デバイスによって送信されたユニキャストパケットの合計数
Rx フレーム	デバイスが受信したパケットの総数
Rx ブロードキャスト	デバイスが受信したブロードキャストパケットの総数
Rx マルチキャスト	デバイスが受信したマルチキャスト パケットの総数
Rx ユニキャスト	デバイスが受信した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）記述子がないために破棄されたパケットの総数

表 *33* : アクセスとネットワークアイテム

項目	説明
Rx totalPkt	デバイスが受信したパケットの総数
Rx crcErr	CRC エラーの受信パケットの総数
Rx alignErr	フレーム チェック シーケンス (FCS) が不正な、長さが 64 ～ 1522 バイトの受信パケットの総数
Rx マルチキャスト	デバイスが受信したマルチキャスト パケットの総数
Rx ブロードキャスト	デバイスが受信したブロードキャスト パケットの総数
Rx ユニキャスト	デバイスが受信したユニキャスト パケットの総数
Rx shortErr	受信したFCSエラーパケットまたはAlignエラーパケットの合計数（サイズが 64 バイト未満）
Rx shortGood	サイズが 64 バイトより小さい、受信された有効なパケットの合計数
Rx longGood	サイズが1522バイトより大きい、受信された有効なパケットの合計数
Rx longErr	サイズが 1522 バイトより大きい、受信された FCS エラー パケットまたは Align エラー パケットの合計数
Rx size64	不良パケットを含む、サイズが 0 から 64 バイトまでの受信パケットの総数
Rx size65to127	不良パケットを含む、サイズが 65 ～ 127 バイトの受信パケットの総数
Rx size128to255	不良パケットを含む、サイズが 128～255 バイトの受信パケットの総数
Rx size256to511	不良パケットを含む、サイズが 256～511 バイトの受信パケットの総数
Rx size512to1023	不良パケットを含む、サイズが 512～1023 バイトの受信パケットの総数
Rx size1024to1518	不良パケットを含む、サイズが 1024～1518 バイトの受信パケットの総数
Rx tokenDrop	リソース不足（FIFO オーバーフローなど）によりドロップされたパケットの総数
Tx excessDefer	メディアがビジー状態のため送信が遅延されたパケットの総数
Tx lateCollision	パケット送信開始後 512 ビット時間経過後に衝突が発生した回数
Tx totalGoodPkt	デバイスが受信した正常なパケット（マルチキャスト、ブロードキャスト、ユニキャスト）の合計数

項目	説明
Tx Collisions	パケットの送信中に発生した衝突の合計数
Tx excessLength	パケットが16回の送信試行を経験したため送信されなかったパケットの合計数
Tx ブロードキャスト	デバイスによって送信され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	デバイスによって送信されたマルチキャスト パケットの合計数
LLDP FramesOutTotal	デバイスから送信された LLDP フレームの総数
LLDP AgeoutsTotal	キャッシュ内でタイムアウトした LLDP フレームの総数
LLDP FramesDiscardedTotal	必須TLVのいずれかが欠落しているか、順序が間違っているか、範囲外の文字列長が含まれている場合に破棄される LLDP フレームの合計数
LLDP FramesInErrorsTotal	1 つ以上の検出可能なエラーを伴って受信した LLDP フレームの総数
LLDP FramesInTotal	デバイスで受信した LLDP フレームの総数
LLDP TLVDiscardedTotal	破棄された LLDP TLV の合計数
LLDP TLVUnrecognizedTotal	デバイスで認識されない LLDP TLV の合計数
CDP ネイバー デバイス ID	CDP によって検出されたこのポートに接続されたデバイスの識別子
CDP ネイバー IP アドレス	CDP によって検出された隣接デバイスの IP アドレス
CDP ネイバー ポート	CDP で検出された、デバイス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 によって検出されたこのポートに接続されたデバイスの識別子
LLDP ネイバー IP アドレス	LLDP によって検出された隣接デバイスの IP アドレス
LLDP ネイバー ポート	LLDP で検出された、デバイス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情報

WLAN セットアップ

デバイスの Web ページにある次の WLAN セットアップ ハイパーリンクでは、ワイヤレス ネットワークのセットアップ情報とその他の設定に関する情報が提供されます。

- 現在の AP
- WLAN 統計

表 *34 :* 現在の *AP*

項目	説明
AP 名	現在のアクセス ポイント名を提供します。
MAC Address	アクセス ポイントの MAC アドレスを提供します。
現在のチャンネル	この AP で測定された最新のチャネル。
前回の RSSI（Last RSSI）	この AP で測定された最新の RSSI。
ビーコン間隔	ビーコン間の時間単位の数。 時間単位は 1.024 msec です。
最小レート	AP に必要な最小データ レート。
最大レート	AP に必要な最大データ レート。
WMM 対応	Wi-Fi マルチメディア エクステンションのサポート。
UAPSD サポート済み（UAPSD Supported）	AP は Unscheduled Automatic Power Save Delivery をサポートします。 WMM がサポートされている場合だけ使用可能です。 この機能は、通話時間と最大通話密度を実現するために重要です。
ノイズ	現在のノイズレベルを示します。
負荷	現在の負荷を示します。
品質	音声品質を示します。

表 *35 : WLAN* 統計

項目	説明
NetDevice Stats	
Tx bytes	デバイスが送信するバイトの合計数。
Rx Bytes	デバイスが受信するバイトの合計数。
Tx Packets	デバイスが送信するパケットの合計数。
Rx Packets	デバイスが受信するパケットの合計数。

項目	説明
Tx Packets Dropped	デバイスがドロップした送信パケットの合計数。
Rx Packets Dropped	デバイスがドロップした受信パケットの合計数。
Tx Packets Error	送信されたエラー パケットの合計数。
Rx Packets Error	受信したエラー パケットの合計数。
ファームウェア統計	
Multicast Tx Frames	デバイスが送信したマルチキャスト パケットの合計数。
失敗	パケットの送信に失敗しました。
再試行	合計再試行回数のカウンター。
Multiple Retry	パケットの送信が成功するまでに 2 回以上の再試行が必要でした。
フレーム重複	デバイスが受信した重複パケットの数。
RTS 成功	対応する CTS が受信されました。
RTS 失敗	対応する CTS が受信されませんでした。
Ack Failure	AP は送信を確認しませんでした。
Rx Frag	デバイスが受信した断片化されたパケットの数。
Multicast Rx Frame	デバイスが受信したマルチキャスト パケットの数。
FCS エラー	受信した MPDU でフレーム チェックサム (FCS) エラーが検出されると増加します。
Tx フレーム（Tx Frames）	デバイスが送信したパケットの数。
ローミング統計	
現在/合計	現在のローミング時間/合計ローミング時間（ミリ秒）。

デバイス ログ

デバイスの Web ページにある次のデバイス ログ ハイパーリンクには、デバイスの監視とトラブルシューティングに役立つ情報が提供されます。 デバイス ログ領域にアクセスするには、デバイスの Web ページにアクセスします。

- [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、現在の syslog、非アクティブなロードからのアーカ

イブ ログ、最後の再起動からのログ、現在のロードのアーカイブ ログ、および問題レポート ツールによって生成されるログの圧縮されたコレクションが含まれます。

- [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 (tombstone_xx) には、アプリケーションのクラッシュからのデータが含まれます。 ANR ファイル (traces.txt) には、デバイスが応答していないと判断し、ユーザがアプリケーションを終了することを選択したアプリケーションのデータが含まれます。
- ステータス メッセージ: デバイスが最後に電源投入されてから生成された最新のステータス メッセージが最大 50 件含まれます。 この情報は、デバイスのステータス メッセージ画面からも確認できます。
- デバッグ表示: トラブルシューティングのサポートが必要な場合に、Cisco TAC に役立つ可能性のあるデバッグ メッセージが含まれます。

ストリームの統計

デバイスは、通話中、または音声やデータを送受信するサービスを実行しているときに情報をストリーミングします。

デバイスの Web ページのストリーミング統計領域には、ストリームに関する情報が表示されます。

ストリーミング統計領域を表示するには、デバイスの Web ページにアクセスし、 **ストリーム** ハイパーリンクをクリックします。

次の表に、[ストリームの統計（Streaming Statistics）] 領域の項目を示します。

表 *36 : [*ストリームの統計（*Streaming Statistics***）*]* 領域の項目**

項目	説明
Remote Address	ストリームの宛先の IP アドレスおよび UDP ポート。
Local Address	デバイスの IP アドレスと UDP ポート。
開始時刻	デバイスがパケットの送信を開始するよう Cisco Unified Communications Manager が要求した時刻を示す内部タイムスタンプ。
ストリーム 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。
ホスト名（Host Name）	MACアドレスに基づいてデバイスに自動的に割り当てられる一意の固定名。
送信パケット（Sender Packets）	この接続を開始してからデバイスによって送信された RTP データパケットの合計数。 接続が受信専用に設定されている場合、値は 0 になります。

項目	説明
送信オクテット（Sender Octets）	この接続を開始してからデバイスによってRTPデータ パケットで送信されたペイロードオクテットの合計数。 接続が受信専用に設定されている場合、値は 0 になります。
送信コーデック（Sender Codec）	送信ストリームに使用されるオーディオ エンコーディングの種類。
送信者レポート送信（注記を参照）	RTCP 送信レポートが送信された回数。
送信者レポート送信時刻（注記参照）	最後の RTCP 送信レポートが送信されたときの内部タイムスタンプ表示。
受信喪失パケット	この接続でデータの受信を開始してから失われたRTPデータ パケットの合計数。 予想パケット数から受信パケット数を引いたものとして定義されます。受信パケット数には、遅延パケットや重複パケットも含まれます。 接続が送信のみに設定されている場合、値は 0 として表示されます。 この接続でデータの受信を開始してから失われたRTPデータ パケットの割合が括弧内に表示されます。
平均ジッター（Avg Jitter）	RTP データ パケットの到着間隔の平均偏差の推定値 (ミリ秒単位で測定)。 接続が送信のみに設定されている場合、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。
受信レポートの送信（注記参照）	RTCP 受信レポートが送信された回数。
受信レポート送信時刻（注記参照）	RTCP 受信レポートが送信されたときの内部タイムスタンプ表示。
受信パケット	この接続でデータの受信を開始してからデバイスが受信したRTPデータ パケットの合計数。マルチキャスト呼び出しの場合、異なるソースから受信したパケットが含まれます。 接続が送信のみに設定されている場合、値は 0 として表示されます。
受信オクテット	接続での受信を開始してからデバイスがRTPデータ パケットで受信したペイロードオクテットの合計数。マルチキャスト呼び出しの場合、異なるソースから受信したパケットが含まれます。接続が送信のみに設定されている場合、値は 0 として表示されます。

項目	説明
累積フレーム損失率（Cumulative Conceal Ratio）	隠蔽フレームの合計数を、音声ストリームの開始から受信した音声フレームの合計数で割ったもの。
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)が使用されている場合は、3 秒間のアクティブな音声を蓄積するのに、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、最も高い間隔の隠蔽率。
秘匿時間	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 Secs）	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。
レイテンシー（注記参照）	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）。
送信者レポート受信（注記参照）	RTCP 送信レポートが受信された回数。
送信者レポート受信時間（注記参照）	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）]	RTP パケットはネットワークから受信されましたが、ジッタ バッファから破棄されました。
受信者レポートの受信（注記参照）	RTCP 受信レポートが受信された回数。
受信者レポート受信時刻（注記参照）	RTCP 受信レポートが最後に受信された時間。
受信の暗号化	受信ストリームが暗号化されているかどうかを示します。
送信暗号化	送信ストリームが暗号化されているかどうかを示します。

項目	説明
送信フレーム	ビデオ ストリームが開始されてからデバイスによって送信されたビデオ フレームの数です。
送信部分フレーム	ビデオ ストリームが開かれてからデバイスが送信した P フレームの数。
送信者 IFrames	ビデオ ストリームが開かれてからデバイスが送信した I フレームの数。
送信フレームレート	ビデオ フレームが送信される速度 (フレーム/秒)。
送信帯域幅	送信されたビデオ ストリームの帯域幅 (kbps (キロ ビット/秒))。
送信解像度	デバイスが送信するビデオ ストリームの解像度。
受信フレーム	ビデオストリームが開かれてからデバイスが受信したビデオフレームの数。
受信不完全フレーム	ビデオ ストリームが開かれてからデバイスが受信した P フレームの数。
受信 Iフレーム	ビデオ ストリームが開かれてからデバイスが受信した I フレームの数。
受信 Iフレーム 要求	ビデオストリームが開始されてからデバイスがリモートエンドポイントに送信した IDR 要求の数。
受信フレームレート	ビデオ フレームが受信される速度 (フレーム/秒)。
受信フレームの損失	ビデオストリームが開かれてからビデオデコーダーが報告した失われたフレームの数。
受信フレームエラー	ビデオストリームが開かれてからビデオデコーダーが報告したエラーの数。
受信帯域幅	受信したビデオ ストリームの帯域幅 kbps (キロ ビット/秒)。
受信解像度	電話がリモートエンドポイントから受信したビデオストリームの解像度。
ドメイン名	ドメイン名を示します。
送信参加	デバイスがストリームの送信を開始した回数
受信参加	デバイスがストリームの受信を開始した回数
BYE（Byes）	デバイスがストリームの送信を停止した回数

項目	説明
送信開始時間	最初の RTP パケットがネットワークに送信された時刻を示すタイムスタンプ。
受信開始時間	ネットワークから最初の RTP パケットを受信した時刻を示すタイムスタンプ。
送信者 DSCP	送信側 SIP シグナリングパケットの DSCP 値
レシーバーのDSCP	受信側 SIP シグナリングパケットの DSCP 値
送信者 RTCP DSCP	送信側 RTP パケットの DSCP 値
受信側 RTCP DSCP	送信側 RTP パケットの DSCP 値
Is ビデオ	ビデオ通話を示します。
Is プレゼンテーション	プレゼンテーションの呼び出しを示します。
送信アクティブ	送信者がアクティブであることを示します。
受信アクティブ	受信機がアクティブであることを示します。

（注） RTP 制御プロトコルが無効になっている場合、このフィールドにはデータが生成されず、0 として表示されます。

翻訳について
このドキュメントは、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。