コラボレーション エンドポイント ソフトウェア バージョン
9.9 OCTOBER 2019

管理者ガイド

cisco Webex DX70 および DX80

Cisco 製品をお選びいただきありがとうございます。

お使いの Cisco 製品は、長年にわたり安全かつ信頼できる操作を行えるよう設計されています。

製品ドキュメンテーションのこの部分は、ビデオ会議デバイスのセットアップと設定を担当する管理者を対象としています。

このアドミニストレータ ガイドの主な目的は、ユーザの目標とニーズに対応することです。本書についてのご意見やご感想があれば、ぜひお伝えください。

定期的に Cisco のウェブ サイトにアクセスし、このガイドの最新版を入手することを推奨します。

ユーザ ドキュメンテーションは次の URL から入手できます。

► https://www.cisco.com/go/dx-docs

本ガイドの使用方法

本書上部のメニュー バーと目次の各項目には、すべてハイパーリンクが設定されています。クリックすると、そのトピックに移動します。

目次

はじめに 4
ユーザ ドキュメンテーションとソフトウェア 5
CE9の新機能 6
DX70 および DX80 の概要 37
電源のオンとオフ 38
LED インジケータ 40
ビデオ会議デバイスの管理方法 41

設定 45
ユーザ管理 46
デバイス パスフレーズの変更 47
[設定 (Settings)] メニューへのアクセスの制限 48
デバイス設定 49
サインインバナーの追加 50
ウェルカムバナーの追加 51
デバイスのサービス証明書の管理 52
信頼できる認証局 (CA) のリストの管理 53
セキュア監査ロギングのセットアップ 57
CUCM 信頼リストを削除する 58
永続モードを変更する 59
強力なセキュリティ モードの設定 60
アドホック マルチポイント会議のセットアップ 61
コンテンツ共有のためにインテリジェント プロキシミティをセットアップする 63
ビデオ品質の対コール レート比調整 68
画面に企業ブランディングを追加 69
カスタム壁紙の追加 71
着信音の選択と着信音量の設定 72
お気に入りリストの管理 73
アクセシビリティ機能のセットアップ 74
CUCM からの製品固有の設定のプロビジョニング 75

周辺機器 77
コンピュータの接続 78
入力ソース数の拡大 79
Bluetooth ヘッドセット 80
ISDN リンクの接続 81

メンテナンス 82
デバイス ソフトウェアのアップグレード 83
オプション キーを追加する 85
デバイスのステータス 86
診断の実行 87
ログ ファイルをダウンロードする 88
リモート サポート ユーザを作成する 89
設定とカスタム要素のバックアップ/復元 90
カスタム要素の CUCM プロビジョニング 91
カスタム要素の TMS プロビジョニング 92
以前に使用していたソフトウェア イメージに復元する 93
ビデオ会議デバイスの初期設定へのリセット 94
ユーザ インターフェイスのスクリーンショットをキャプチャする 98

デバイスの設定 99
デバイス設定の概要 100
音声設定 105
Bluetooth 設定 107
CallHistory の設定 108
カメラの設定 109
会議設定 110
FacilityService の設定 114
H323 の設定 115
HttpClient の設定 118
HTTP フィードバック設定 119
ロギングの設定 120
マクロ設定 122
ネットワーク設定 123
NetworkPort 設定 131
NetworkServices の設定 132
周辺機器の設定 139
電話帳の設定 140
プロビジョニング設定 142
プロキシミティの設定 145
ルームリセット設定 146
RTP の設定 147
セキュリティの設定 148
シリアルポート設定 151
SIP の設定 152
スタンバイの設定 156
システムユニット設定 157
時刻の設定 158
ユーザ インターフェイス設定 161
ユーザ管理設定 166
ビデオ設定 168
試験的設定 175

付録 176
ユーザ インターフェイス 177
リモートモニタリングのセットアップ 178
ウェブ インターフェイスを使用した通話情報へのアクセスとコール応答 179
ウェブ インターフェイスを使用してコールをかける 180
Web インターフェイスを使用したコンテンツの共有 182
ローカル レイアウトの制御 183
相手先カメラの制御 184
パケット損失の復元力 : ClearPath 185
ビデオ会議デバイスのユーザーインターフェイスのカスタマイズ 186
マクロを使用したビデオ会議デバイスの動作のカスタマイズ 188
ユーザ インターフェイスからデフォルトボタンを削除する 189
サードパーティ USB 入力デバイスの使用 190
HTTP(S) 要求の送信 191
スタートアップ スクリプトを管理する 192
デバイスの XML ファイルへのアクセス 193
ウェブ インターフェイスからの API コマンドとコンフィギュレーションの実行 194
イーサネットポートについて 195
シリアル インターフェイス 196
TCP ポートの開放 197
TMS からの HTTPFeedback アドレス 198
Cisco Webex Cloud サービスへのデバイスの登録 199
サポートされている RFC 200
技術仕様 201
Cisco ウェブ サイト内のユーザ ドキュメンテーション 203
Cisco のお問い合わせ先 204

第 1 章

はじめに

ユーザ ドキュメンテーションとソフトウェア

このガイドの対象となる製品

- Cisco TelePresence DX70
- Cisco TelePresence DX80

コラボレーション ソフトウェア バージョン 8.2 (CE8.2) 以降、すべての DX80 ユニットおよび DX70 ユニットで CE ソフトウェアを実行できます。このソフトウェアは、Cisco TelePresence SX および MX シリーズで動作するソフトウェアと同じものです。

なお、Cisco DX650 は CE ソフトウェアでサポートされておらず、今後のサポート予定もありません。

ユーザ ドキュメンテーション

このガイドでは、ビデオ会議デバイスの管理に必要な情報を提供します。

主にオンプレミス登録のデバイス (CUCM、VCS) の機能と設定について説明していますが、その機能と設定の一部は、クラウド サービス (Cisco Webex) に登録されたデバイスにも適用されます。

本製品に関する詳しいガイドは、付録
► Cisco Web サイト内のユーザ マニュアルを参照してください。

Cisco ウェブ サイト内のドキュメンテーション

次の Cisco ウェブ サイトに定期的にアクセスして、ガイドの最新バージョンを確認してください。

► https://www.cisco.com/go/dx-docs

クラウドに登録されたデバイスのドキュメンテーション

Cisco Webex クラウド サービスに登録されたデバイスの詳細については、以下のサイトを参照してください。

►https://help.webex.com

Cisco Project Workplace

オフィスやミーティング ルームをビデオ会議用に整備する際にインスピレーションを得たり、ガイドラインを確認したりするには、次の Cisco Project Workplace をご覧ください。

► https://www.cisco.com/go/projectworkplace

ソフトウェア

次の Cisco ウェブ サイトからエンドポイント用のソフトウェアをダウンロードします。

► https://software.cisco.com/download/home

ソフトウェア リリース ノート (CE9) を参照することをお勧めします。

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

CE ソフトウェアへの変換

2016 年 9 月まで、DX80 と DX70 は、Android ベースのソフトウェアを付属して出荷されていました。CE ソフトウェアに変換する前に、変換の要件、および Android ベースのソフトウェアと比較した機能の変更点を注意深く確認することが重要です。この確認を行わないと、導入環境が機能せず、再度変換して前に戻すことが必要になる可能性があります。

ソフトウェア リリース ノートと、「システム ソフトウェアのアップグレード」の章を参照してください。

CE9 の最新情報

この章では、現行の Cisco Collaboration Endpoint ソフトウェア バージョン 9 (CE9) について、新規および変更されたデバイス設定 (構成) の概要と、新機能および改善点を CE8 と比較して説明します。

CE9 では以下の Webex 製品が新しくなっています。

- CE9.0： Room Kit
- CE9.1： Codec Plus、および Room 55
- CE 9.2: Room 70
- CE 9.4: Codec Pro、Room 70 G2、および Room 55 Dual
- CE 9.6：Room Kit Mini
- CE 9.8：Board 55/55S、Board 70/70S、および Board 85S

詳細については、次のソフトウェア リリース ノートを読むことをお勧めします。

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

CE9.9 の新機能および改善点

UI 拡張エディタのアップデート

（すべての製品）

室内制御エディタは、利用可能になった追加機能を反映して UI 拡張エディタという名称に変更されました。エディタを起動するには、Web インターフェイスで [統合 (Integration)] > [UI拡張エディタ (UI Extension Editor)] に移動します。また、エディタの UI が更新されました。

詳細については、▸https://www.cisco.com/go/in-room-control-docs にある CE9.9 向けのカスタマイズ ガイドを参照してください。

Web アプリ *(Board)*

UI 拡張エディタを使用して Web アプリを作成できます。それにより、Jira、Miro、Office 365、Google ドキュメントなどのアプリに Board からアクセスできます。

デジタル サイネージ

（Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board）

デジタル サイネージでは、デバイスがハーフ ウェイク モードになっているときに、会社のニュース、ビルの案内図、緊急情報などのカスタム コンテンツを表示することができます。

ユーザは、サイネージ コンテンツを Webex Board だけで操作できます。

外部 URL からのブランディング イメージとカスタム壁紙の取得 (すべての製品)

`xCommand UserInterface Branding Fetch` API コマンドを使用して、外部 URL からブランディングイメージやカスタム壁紙をダウンロードできます。

カスタム壁紙は、Webex Board では使用できません。

ネットワーク設定メニューの変更

（すべての製品）

デバイスのユーザーインターフェイスの [ネットワーク接続 (Network connection)] ページが変更されました。まず、現在のネットワーク設定が表示され、設定を変更する場合はイーサネットまたは Wi-Fi の設定を開くことができます。以前利用できなかった GUI からの設定がいくつか追加されました。

超音波設定の変更 (すべての製品)

すべての製品で、Audio Ultrasound MaxVolume 設定に同じデフォルト値が使用されるようになりました。異なる製品間で音量範囲の調整も行われました。製品固有の違いは内部処理され、値の範囲やデフォルト値に反映されなくなりました。デバイスから再生される音声レベルは変更されていません。

TLS 設定の変更 *(すべての製品)*

セキュリティ上の理由から、HTTPS クライアント、syslog、および SIP 接続の TLS 設定にいくつかの変更が加えられました。

- 証明書チェックを実行しない場合は、証明書の検証を明示的にオフにする必要があります。デフォルトでは、すべての TLS 接続で証明書がチェックされます。
- TLS の最小バージョンが、バージョン 1.0 から 1.1に上がりました (バージョン 1.0 を許可している CUCM と SIP を除く)。Webex クラウドでは TLS バージョン 1.2 を使用していることに注意してください。
- プロビジョニング、電話帳、およびその他の HTTP サーバについて、証明書の検証を個別に設定できます。これらのすべてのサーバータイプを対象としていた以前の NetworkServices HTTPS VerifyServerCertificate 設定は、Provisioning TLSVerify、Phonebook Server [1] TlsVerify、および HTTPFeedback TlsVerify の 3 つの設定に置き換えられました。
- 外部ロギングの証明書の検証 (監査ロギングと通常のロギングの両方) を設定できます。
- SIP の場合、証明書はカスタム CA リストに照らして検証されます。このリストは、Web インターフェイスまたは API を使用して手動でデバイスにアップロードします。その他の接続の場合、証明書は、デバイスにプレインストールされている CA リストまたはカスタム CA リストに照らして検証されます。

ホワイトボードと注釈に対するアップデート

(Board)

- ホワイトボードで付箋や注釈を作成、編集、および移動できます。
- ホワイトボードと注釈を使用するときに、3 つの異なるペン サイズから選択できます。
- ホワイトボードと注釈のコピーを作成できます。ホワイトボード メニューには、プレゼンテーションのホワイトボードまたは注釈付きのスナップショットが保存されています。他のホワイトボードやスナップショットの場合と同じように、このコピーに戻って作業を続けることができます。

有線タッチリダイレクト *(Board)*

タッチリダイレクトを使用すると、Webex Board の画面からラップトップを制御することができます。ラップトップは、HDMI ケーブル (有線共有) と USB-C ケーブルを使用して Webex Board に接続する必要があります。

タッチ リダイレクトは、コール中でないときにのみ機能します。

この機能は、第 2 世代のボード (Webex Board 55S、70S、および 85S) でのみ使用できます。

CE9.8 の新機能および改善点

新商品

以前にはクラウド登録でしか利用できなかった Cisco Webex Board が、オンプレミス登録でも利用できるようになりました。

- Cisco Webex Board 55/55S
- Cisco Webex Board 70/70S
- Cisco Webex Board 85S

USB ヘッドセットのサポート

(Room Kit、Room Kit Mini、Room 55)

USB ヘッドセット、ハンドセット、または USB Bluetooth ドングルをデバイスの USB-A ポートに接続することができます。これは、DX シリーズと同様です。

HTTP 要求の拡張サポート *(すべての製品)*

CE9.6 以降、デバイスは任意の HTTP(S) Post および Put 要求を HTTP(S) サーバーに送信できるようになりました。この機能が、さらに多くの要求タイプ (Get、Patch、および Delete) をサポートすることになり、サーバから返されるデータ (応答ヘッダおよび本文) の処理機能が拡張されています。

USB-C エクスペリエンスの改善 *(Room Kit Mini)*

USB-C ポートを介してコンピュータにメディアをストリーミングする場合にのみ、Room Kit Mini は USB カメラ モードとなります。以前のリリースでは、コンピュータに USB-C ポートを接続するだけでこのモードになりました。

デバイス UI から CMS 会議への参加者の追加

(すべての製品)

どのユーザーでも、デバイスのユーザーインターフェイスを使用して、進行中の CMS 会議に別の参加者を追加できます。これには PSTN コールも含まれます。参加者がコールを受け入れると、参加者は同じ CMS 会議に追加されます。

この場合、デバイスが CMS に対し、アクティブ コントロールの仕組みを利用してその参加者にダイヤルするよう指示します。それを受けて CMS は、追加する参加者に直接ダイヤルします。

この機能が動作するためには、デバイス上でアクティブ コントロールが有効であること、コール プロトコルが SIP であること、CMS がバージョン 2.4 以降であることが必要です。マルチポイント モードが CUCMMediaResourceGroupList に設定されている場合、この機能は動作しません。

API またはローカル Web インターフェイスを使用した Cisco Webex へのデバイスの登録

(すべての製品)

デバイスは、Cisco Webex にリモートで登録することができます。その際、デバイスと同じ室内にいる必要はありません。この操作は、API からプログラムによって実行するか、ローカル Web インターフェイス経由で行います。以前のリリースでは、画面上のセットアップ アシスタントを使用する必要がありました。

Web インターフェイスからは、デバイスが現在登録されていない場合のみ、Webex 登録を開始できます。API を使用している場合は、デバイスがオンプレミスのシステム (CUCM または VCS) に現在登録されていても、Webex 登録を開始できます。

プレインストールされている認証局 (CA) のリスト

(すべての製品)

一般に使用される CA 証明書のリストがビデオ会議デバイスに事前にインストールされています。デバイスは、通信している外部サーバからの証明書を検証するときに、このリストを使用します。

- HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバー
- SMTP メール サーバ (Webex Board にのみ該当)

工場出荷時設定へのリセットを行っても、このリストは削除されません。

WebSocket 経由の xAPI：認証プロトコルヘッダーを使用した認証 *(すべての製品)*

認証プロトコルヘッダーを使用した認証がサポートされます。これは、HTTP ヘッダー フィールドを使用したベーシック認証に加えて使用されます。

つまり、HTTP ヘッダーを直接制御できないブラウザベースのクライアントでは、Javascript を使用してブラウザから直接デバイスに対して認証を行うことができます。

Cisco UCM からプロビジョニング可能なデバイス設定の追加 *(すべての製品)*

デバイスが Cisco UCM 12.5(1)SU1 に登録されている場合は、これまでよりも多くの設定とパラメータを UCM からプロビジョニングできます ([デバイス (Device)] > [製品固有の設定レイアウト (Product Specific Configuration Layout)])。また、これらの設定がデバイス上でローカルに変更されている場合は、新しい値を UCM に書き戻すことができます。

これには、公開されているデバイス設定 (xConfiguration) のほとんどが該当します。ネットワーク、プロビジョニング、および SIP 設定については例外が設けられています。

詳細については、► Cisco Unified Communications Manager および IM and Presence Service リリース 12.5(1) SU1 のリリース ノートの「ビデオ エンドポイント管理の概要」の項をご覧ください。

CE9.7 の新機能および改善点

WebSocket を介した xAPI への接続

（すべての製品）

WebSocket 経由で xAPI に接続できるようになりました。WebSocket 上の通信チャネルは、明示的に閉じられるまで両方向に開かれています。つまり、サーバは新しいデータが利用可能になり次第、クライアントにデータの送信が行えるようになります。また、各要求に対して再認証を行う必要はありません。これは、HTTP と比較してかなり速度が改善されます。

各メッセージには、完全な JSON ドキュメント以外は含まれていません。WebSocket と JSON-RPC では多くのプログラミング言語の優れたライブラリサポートがあります。

WebSocket はデフォルトでは有効ではありません。Websocket を使用する前に、WebSocket が HTTP に関連付けられていること、および HTTP または HTTPS が有効になっていることに注意してください。

詳細は、► WebSocket 経由の xAPI ガイドを参照してください。

音声コンソールで使用可能なグラフィックサウンドミキサー

(Codec Pro、MX700、MX800、Room 70 G2、Room 70D G2、SX80)

オーディオ コンソールで、グラフィック サウンド ミキサーが利用できるようになりました。これには 8 つのユーザー定義可能なパラメータ化された均等化設定があります。設定は、1 つのフィルタタイプ、ゲイン、中央、クロスオーバー周波数、および Q 値を持つ最大 6 つのセクションで構成されています。各セクションは独自の色で表示され、パラメータのいずれかを変更した結果がすぐにグラフに表示されるようになります。

詳細は、以下の カスタマイズ ガイドCE9.7向け を参照してください ► https://www.cisco.com/go/in-room-control-docs

環境ノイズ レポート

(Codec Plus、Codec Pro、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini)

ルームシリーズデバイスは、室内の固定周囲ノイズを報告するように設定可能です。レポートされた値はA荷重デシベル値(dBA)で、人間の耳の応答に反響します。レポートされたノイズを元に、施設管理または建物マネージャーは介入して問題をトラブルシュートできます。

この機能に関連するすべてのシグナリング処理はローカルで、転送されるデータは算出されたノイズレベルだけです。

マルチ SRG-120DH/PTZ-12 カメラのサポート

(Codec Plus)

HDMI およびイーサネット スイッチを使って最大 3 代の SRG-120DH/PTZ-12 を Codec Plus に接続できるようになりました。

その他のアップデート

- 1080p は USB カメラとして使用されている場合に Room Kit Mini をサポートします。(Room Kit Mini)
- 通話中にビデオをオフまたはオンにできます。
  （すべての製品）
- システム管理者は HTTP の使用を防ぎ、HTTPS ポストおよび HTTPS プットリクエストだけを許可できます。
  （すべての製品）

CE9.6 の新機能および改善点

新製品

- Cisco Webex Room Kit Mini

HDCP サポート

(Codec Plus、Codec Pro、Room 55 Dual、Room 70、Room 70 G2)

デバイスの HDMI 入力の 1 つを、HDCP（高帯域幅デジタルコンテンツ保護）で保護されたコンテンツをサポートするように設定できます。このため Google ChromeCast、AppleTV、または HDTV デコーダなどのデバイスを接続してビデオシステムの画面を再利用できます。通話中にこの種のコンテンツを共有することはでません。

HDCP をサポートするようにコネクタを設定すると、この種類のコンテンツのために予約されます。これは通話中に特定のコネクタの内容を共有することは、ラップトップからの非保護内容であってもできないことを意味します。

ユーザ インターフェイスからデフォルトボタンを削除する

（すべての製品）

ユーザインターフェイスにあるデフォルトのボタン全てが不要の場合、不要なものを削除できます。これによりユーザインターフェイスを完全にカスタマイズできます。この設定はボタンだけを削除し、機能などは削除しません。カスタマイズされたルーム内制御パネルは表示されたままです。

詳しくは、次のリンク先にある CE カスタマイズ ガイド を参照してください ► https://www.cisco.com/go/in-room-control-docs

HTTP ポストおよびプットリクエスト（全製品）

この機能は任意の HTTP(S) ポストおよびプットリクエストをあるデバイスから HTTP(S) サーバに送信することができます。

マクロを使用すると、必要に応じて HTTPs サーバにデータを送信できます。送信するデータを選択して、必要に応じて構造化することができます。この方法で、データをすでに確立されているサービスに適用することが可能です。

セキュリティ対策：

- HTTP(S) ポスト機能・プット機能はデフォルトで無効に設定されています。
- システム管理者は、デバイスがデータを送信可能な先であるHTTP(S) サーバのリストを指定することができます。
- 同時に行える Post および Put 要求の数は制限されています。

サードパーティUSB コントローラのサポート

(Codec Plus、Codec Pro、DX70、DX80、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit)

サードパーティ USB 入力デバイスを使用して、ルームデバイスの特定の機能を制御することができます。USB ドングルや USB キーボードでの Bluetooth リモート制御はこのような入力デバイスの一例です。マクロ経由で所定の機能をセットアップできます。

この機能は、Touch 10 または DX ユーザ インターフェイスの機能の補正を行います。Touch 10 および DXのユーザ インターフェイスを置き換えるという意味ではありません。

詳しくは、次のリンク先にある CE カスタマイズ ガイド を参照してください ► https://www.cisco.com/go/in-room-control-docs

コンテンツのの優先順位 *（すべての製品）*

メインビデオチャネルまたはプレゼンテーションチャネルのいずれかの帯域幅の使用を優先するようにデバイスを設定できるようになりました。

x**ビデオプレゼンテーション優先度設定**： <**同等、高**>

「同等」がデフォルト設定で、帯域幅は50%ずつ分割されます。「高」を選択すると、プレゼンテーションチャンネルが優先され、20%対70%の帯域幅分割となります。

その他の更新情報 *（すべての製品）*

- デバイスのユーザ インターフェイスから会議の録画の開始および操作ができるようになりました（使用するインフラストラクチャで録画がサポートされている場合のみ）。
- ユーザインターフェイスでの連絡先情報の編集
- SIP コール IDでログに SIP セッション ID フィールドが追加され、コールの特定が容易になりました。
- MRA 経由で ICE を利用してベストパスが入手できるようになりました。

CE9.5 の新機能および改善点

プレゼンテーションソースの構成

(SX10、DX70、DX80 を除く全製品)

2 つ以上のソースを1 つのイメージとして送信することで、会議での共有において新たな体験を届けることができます。

これにより、遠隔でのプレゼンテーションを柔軟に行うことができます。マクロまたは外部コントローラーと室内のコントローラーを使って、プレゼンテーションの構成の設定変更することができます。

ソースの最大利用可能数は、使用するデバイスによって異なります。

- SX20、MX200 G2、MX300 G2、*および* Room Kit: 2 *つのソース*
- Codec Plus、Room 55、Room 55 Dual、*および* Room 70*:* 3 *つのソース*
- SX80、MX700、MX800、Codec Pro、*および* Room 70 G2*:* 4 *つのソース*

ケーブル経由で共有されているコンテンツのみ構成に組み込むことができます。

ウェブ インターフェイスのオーディオ コンソール

(SX80、Codec Pro)

新しいオーディオ コンソールは、ウェブ インターフェイスでネイティブに利用可能です。オーディオ コンソールを音声ルーティング ツールとして使用することで、音声を入力から出力に簡単にルーティングできます。オーディオ コンソールは、メンテナンスされなくなった古い Java ベースの CE コンソールに代わるものです。

初めてオーディオ コンソールにアクセスすると、デフォルトのシステム音声ルートが表示されます。オーディオ コンソールは基礎となるマクロによって制御されます。このマクロは、現在のデバイス構成を上書きするオプションを選択すると、保存されて起動されます。

詳しくは、次のリンク先にある CE カスタマイズ ガイド を参照してください ► https://www.cisco.com/go/in-room-control-docs

教室のセットアップ

(SX80、MX700、MX800、Codec Plus、Codec Pro、Room 55 Dual、Room 70、Room 70 G2)

Classroom テンプレートではマクロを使用してルーム セットアップを調整し、シナリオのプレゼンテーションと指導に最適なものにします。テンプレートを使用すると、ルームを簡単にセットアップ、管理、使用できます。

教室のセットアップは会議室のセットアップと同じように機能しますが (SX80、Codec Pro、MX700、MX800 および Room 70 G2 で利用可能) 、3 つの画面は必要ありません。

韓国語キーボードのサポート *(すべての製品)*

ユーザーインターフェイス言語を韓国語に設定すると、韓国語キーボードでの入力が Touch 10 でサポートされます。

画面ステータスのリモート モニタリング *(SX20、SX80)*

Webex Room シリーズと SX10 で利用可能だった画面ステータスのリモートモニタリングは、SX20 と SX80 で利用可能になりました。

コーデックは、スタンバイモードから画面を起動でき、コーデックがスタンバイ状態になったときに画面をスタンバイ状態にできます。コールの受信時に入力ソースを自動的に変更することもできます。

CEC は、デフォルトではデバイス上で無効になっており、Video Output Connector [n] CEC Mode 設定で有効化する必要があります。リモートモニタリングが機能するには、お使いのスクリーンが CEC をサポートしている必要があります。

ウェルカムバナー *(すべての製品)*

デバイスの Web インターフェイスまたはコマンドラインインターフェイスへのサインイン後にユーザーに表示される、ウェルカムバナーを設定できます。バナーには、使い始めるうえで必要な情報や、デバイスのセットアップ時に知っておく必要があることなどを記載できます。

CE9.4 の新機能および改善点

新商品

- Cisco Webex Codec Pro
- Cisco Webex Room 55 Dual
- Cisco Webex Room 70 G2

Cisco Spark から Cisco Webex へのリブランディング *(すべての製品)*

Cisco Spark は Cisco Webex に名称が変更され、Spark と表示されるユーザ インターフェイスの要素は Webex へと変更されます。アクティベーション フローで今すぐに Cisco Spark ではなく登録オプションとして Cisco Webex を表示します。

以下の製品は、新たな名称を得ます。

- Cisco Spark Room Kit は Cisco Webex Room Kit となりました
- Cisco Spark Room Kit Plus は Cisco Webex Room Kit Plus となりました
- Cisco Spark Codec Plus は Cisco Webex Codec Plus となりました
- Cisco Spark Quad Camera は Cisco Quad Camera となりました
- Cisco Spark Room 55 は Cisco Webex Room 55 となりました
- Cisco Spark Room 70 は Cisco Webex Room 70 となりました
- Cisco DX70 は Cisco Webex DX70 となりました
- Cisco DX80 は Cisco Webex DX80 となりました

プロクシミティクライアントの最大数が増加しました

(Codec Plus、Codec Pro、Room Kit、Room 55、Room 55 Dual、Room 70、Room 70 G2)

プロクシミティサービスの ContentShare ToClients が無効にしてある場合、Cisco Webex Room Series デバイスは最大 30 のペアリングクライアントを同時に設定できます。ContentShare ToClients が有効である場合、ペアリングクライアントの制限はソフトウェアの以前のバージョン内容と同じ 7 となります。

Cisco Webex Room Series およびレガシー MXP デバイス間でのコールで H.263 を使用したコンテンツ共有のサポート

(Codec Plus、Codec Pro、Room Kit、Room 55、Room 55 Dual、Room 70、Room 70 G2)

MXP および Cisco Webex Room Series 間で、H.263 コンテンツが共有できるようになります。これまでの Room Series では、別のコンテンツチャネル内のコンテンツの受信または共有を行うことはできませんでした。Room Series デバイスから MXP デバイスへコンテンツを共有すると、以前のバージョンではプレゼンテーションがメイン ビデオ ストリームに合成されます。

これは、特定のシナリオでのみサポートされます。

- Room Series デバイスと MXP デバイス間の H.323 ダイレクト発信 (IP ダイヤラ) 。
- H.323 上の VCS に登録された MXP および SIP または H.323 のいずれかにある同一 VCS 上に登録された Room Series デバイス。VCS 上において H.323 で SIP 発信を行うには、インターワーキング オプション キーが VCS 上にインストールされている必要があることにご留意ください。

本機能に関するその他制限についての詳細は、CE9 リリースノートをご参照ください。

管理設定ロックダウン構成の CUCM プロビジョニング (すべての製品)

CE9.2.1 で導入された管理設定ロックダウン構成は、CUCM からプロビジョニングできるようになります。CUCM を通じて構成を行う際、設定メニュー上でお使いのデバイスの全設定について、選択のロックを同時に行うことができます。

この構成に新たなフィールドを公開するには、CUCM に新たなデバイス パッケージが必要となる場合があります。

ユーザインターフェイスから逆光補正を有効にすることができるようになりました *(DX70、DX80)*

DX70 および DX80 のメインメニューで新しい設定を有効にし、逆光補正を無効にします。これは、ユーザの背後の日光やその他の明るい光源を補正するために、センサーの明るさのレベルを上げる (オン) または下げる (オフ) 固定設定です。逆光補正によってセンサーは固定レベルに設定され、逆光に合わせて自動調整されることはありません。

デフォルトの HTTP モードを HTTP + HTTPS から HTTPS へ変更 *(すべての製品)*

NetworkServices HTTP モードのデフォルト値が HTTPS + HTTP から HTTPS に変更されます。これによって、デフォルト構成でのルーム デバイスのセキュリティを強化します。以前のバージョンからのアップグレードはデフォルト値を自動的に変更せず、現行の HTTP 実装の破損を回避するために HTTP + HTTPS が維持されます。

この変更は、CE9.4.0 以降を実行している新しいデバイス、または CE9.4.0 で初期設定にリセットされたデバイスに表示されます。HTTP リクエストは HTTPS にリダイレクトされ、デバイスのウェブ インターフェイスへの初回訪問時に、デバイスに「安全でない接続の警告」が表示されます。ウェブ インターフェイスへと進むには、ブラウザで例外を作成する必要があります。これは、これまでに訪問したことがない、異なるブラウザを使ってウェブ インターフェイスにアクセスした場合、またはデバイスが工場出荷時の設定にリセットされている場合を除き、1 回限りの操作となります。

室内制御の更新 *(すべての製品)*

ホーム スクリーン上やユーザ インターフェイス上の通話中のスクリーン上で、必要な数のパネル ボタンを追加することができます。

CE9.3 の新機能および改善点

設定とカスタム要素のバックアップ/復元

（すべての製品）

バックアップ ファイル バンドル (zip) には、設定とともにカスタム要素を含めることができます。以下の要素のいずれをバンドルに含めるかを選択できます。

- ブランディング イメージ
- マクロ
- お気に入り
- サインイン バナー
- 室内制御パネル
- 設定 (すべてまたはサブセット)

以前のバージョンのソフトウェアでは、設定をバックアップすることしかできませんでした。

バックアップ ファイルは、デバイスの Web インターフェイスから手動で復元できます。または、Cisco UCM や TMS などを使用して複数のデバイスにプロビジョニングできるように、バックアップ バンドルを一般化することもできます。

バックアップと復元機能は、デバイスの Web インターフェイスの [メンテナンス (*Maintenance*)] > [バックアップと復元 (*Backup and Restore*)] から実行できます。

カスタム要素のプロビジョニング *（すべての製品）*

上記のバックアップ バンドルは、Cisco UCM または TMS を使用して、多数のデバイスにプロビジョニングできます。複数のデバイスで使用するバックアップ バンドルを作成するときは、デバイス固有の情報を削除することが重要です。バンドルにデバイス固有の情報が含まれていると、複数のデバイスに接続できなくなる可能性があります。

デバイス固有でないバックアップ バンドルをプロビジョニングすることにより、たとえば、マクロ、ブランディング情報、室内制御パネルを含むデバイスの設定を、複数のデバイスにコピーできます。

現在、Cisco UCM によるプロビジョニングでは、設定は復元されず、その他のカスタム情報のみが復元されます。TMS は、バックアップ バンドルに含まれるすべてのものを復元します。

プロビジョニングの詳細については、リリース ノートを参照してください。

室内制御の更新 *（すべての製品）*

室内制御機能には次の機能が追加されています。

- 合計で最大 20 のパネルにボタンを追加できます。ボタンは、パネル タイプに応じて、ユーザ インターフェイスのホーム画面または通話中画面に表示されます。
- 従来どおり、グローバル パネル (常時利用可能) 、通話中パネル (通話中のみ利用可能) 、外部発信パネル (通話中でない場合にのみ利用可能) の 3 種類の室内制御パネルがあります。グローバル パネルへのエントリ ポイントは、ステータス バー (ユーザ インターフェイスの右上隅) から削除されました。それに代えて、グローバル パネルを開くボタンが、ホーム画面と通話中画面の両方に追加されました。さらにそれぞれの画面には、外部発信のみパネルを開くボタンと、通話中のみパネルを開くボタンが追加されました。
- スタンドアロンのトリガー ボタンを作成することができます。このボタンは、ユーザ インターフェイス上のパネルを開かずに、イベントを直接トリガーするボタンです。

また、室内制御エディタに次の機能が追加されました。

- いくつかの新しいアイコンを利用できます。
- 室内制御のボタンの色を選択できる、色のセット。
- テキスト要素をダブルクリックすると、テキストを直接編集できます。
- 室内制御の XML ファイルをエディタにドラッグアンドドロップできます。

室内制御の詳細は、カスタマイズ ガイド (https://www.cisco.com/go/in-room-control-docs) を参照してください。

ISDN リンクのサポート *（すべての製品）*

ソフトウェア バージョンが IL1.1.7 である ISDN Link は、CE9.3.0 をサポートするすべてのデバイスでサポートされます。

これまでのように、(ビデオ会議デバイスによる ISDN Link の自動検出を可能にする) 自動ペアリングを使用する場合は、ビデオ会議デバイスで IPv6 を有効化する必要があります。

ワンボタン機能のスヌーズ *（すべての製品）*

ワンボタン機能 (OBTP) ミーティング アラームで 5 分間のスヌーズが可能です。スヌーズの時間を変更することはできません。通常リマインダは、通話中で、スケジュールされた会議が開始される場合に表示されます。会議が終了するまで、リマインダが表示されるたびに、5 分間スヌーズできます。

発信前のコール レートの調整

（すべての製品）

[検索またはダイヤル (Search or Dial)]フィールドへの入力を開始するとすぐに、ダイアログを開いてカスタムコールレートを選択できます。以前のリリースでは、この機能は、ディレクトリからエントリを選択するときにだけ使用できました。

カスタム コール レートを選択しない場合は、[会議のデフォルト コール レート (Conference DefaultCall Rate)] 設定で指定されているレートが設定されます。

着信音の選択と着信音の音量の調整 *（すべての製品）*

ユーザ インターフェイスの設定メニューから着信音を選択し、着信音の音量を調整することができます。以前のリリースでは、これはウェブ インターフェイスから行われていました。

延期されたアップグレードの再開 *（すべての製品）*

ソフトウェア アップグレードの通知を受け取ったら、[今すぐアップグレード (Upgrade now)] または[延期 (Postpone)]を選択することができます。アップグレードを延期した場合には、必要なときに、ユーザ インターフェイスの [設定 (Settings)] > [このデバイスについて (About this device)] メニューからアップグレードを再開できます。以前のように 6 時間待つ必要はなくなりました。

手動でアップグレードを再開しない場合、アップグレードは 6 時間後に自動的に開始されます。

デバイス情報がユーザ インターフェイスに公開されることの防止 *（すべての製品）*

次のような重要なデバイス情報をユーザ インターフェイスに表示させないように設定できます。

IP アドレス (ビデオ会議デバイス、Touch コントローラ、UCM/VCS レジストラ)

- MAC アドレス
- シリアル番号
- ソフトウェア バージョン

この機能を有効にするには、次の操作が必要です。

- 管理者権限を持つすべてのユーザにパスフレーズを設定する
- [ユーザインターフェイス設定メニューモード (UserInterface SettingsMenu Mode)] を[ロック (Locked)]に設定する必要があります
- [ユーザインターフェイスセキュリティモード (UserInterface Security Mode)]を [強 (Strong)] に設定する必要があります

また、この機能により、タッチ コントローラの接続を切断するときに IP アドレスがスクリーンに表示されなくなります。

ミラード セルフビュー (DX70、DX80)

自身を鏡映しにしたときのような、相手に見える状態のセルフビュー イメージを表示するようにデバイスを設定できます。[ビデオ セルフビュー ミラード (Video Selfview Mirrored)] 設定を使います。これまで、ミラード セルフビューは、Android ソフトウェアを実行している Cisco DX デバイスでのみ利用できました。

ミラーリングは、セルフビューの画像にのみ適用され、相手に送信されるビデオには影響しません。

アクセシビリティ : 着信時の画面の点滅

（すべての製品）

デバイスがコールを着信したときに、画面と Touch コントローラが赤色と薄グレー色で点滅するように、デバイスを設定できます。この機能は主に聴覚が不自由なユーザが着信コールに気づきやすくするようにしています。

この機能はデフォルトでは無効化されているため、[着信コール通知アクセシビリティ (Accessibility IncomingCallNotification)] 設定で有効にする必要があります。

画面ステータスのモニタリングと制御 *(SX10)*

SX10 は、Room シリーズのデバイスと同様の CEC (Consumer Electronics Control) の動作をするようになりました。

デバイスは CEC を使用して、デバイス自体がスタンバイ モードになると画面をスタンバイ モードに設定し、デバイス自体がスタンバイ モードから復帰すると、画面を復帰して正しいビデオ入力を選択します。画面からの CEC 情報は、デバイスのステータスに含まれます。この場合、画面も CEC をサポートしており、関連情報をデバイスに送信する必要があります。

CEC は、デフォルトではデバイスで無効になっており、Video Output Connector [1] CEC Mode 設定で有効化する必要があります。

共通 API ガイド *（すべての製品）*

すべての API 情報を、すべての製品を対象とした 1 つの API ガイドにまとめました。これは、製品ごとに 1 冊の API ガイドが用意されていた以前のリリースとは対照的です。

CE9.2 の新機能および改善点

新製品

- Cisco Webex Room 70 （旧 Cisco Spark Room 70）

マクロ フレームワーク *(SX10 を除くすべての製品)*

マクロ フレームワークにより、ユーザおよびインテグレータは、個々の顧客の要件に合うように、JavaScript のマクロを記述して、シナリオを自動化したり、エンドポイントの動作をカスタマイズしたりすることができます。

イベント/ステータス変更のリスニング、コマンドの実行や設定の自動化、室内制御機能のローカル制御機能の提供といった強力な機能とマクロを組み合わせることで、カスタム セットアップに多くの可能性を生み出します。

わずかな動作の変更をマクロを使って簡単に実現できます。たとえば、デバイスを無期限に応答不可にすることができます。設定を自動的にリセットする、特定の日の特定の時間に呼び出しを行う、状況の変化に応じて警告やヘルプ メッセージを発行するといったことも行えます。

マクロ エディタは、デバイスの Web インターフェイスから使用でき、いくつかのサンプル マクロも用意されています。

HDCP サポート *(Room 55)*

デバイスの 2 番目の HDMI 入力 (コネクタ 3) が HDCP (High-bandwidth Digital Content Protection) 保護コンテンツをサポートするように設定することができます。これにより、Google ChromeCast、AppleTV、HDTV デコーダなどのデバイスを接続してデバイスの画面を再利用できるようになります。通話中にこの種のコンテンツを共有することはでません。

HDCP をサポートするようにコネクタを設定すると、この種類のコンテンツのために予約されます。これは通話中に特定のコネクタの内容を共有することは、ラップトップからの非保護内容であってもできないことを意味します。

ブランディングとハーフウェイクのカスタマイズ

(SX10 を除くすべての製品)

独自のテキストと画像をアップロードして、ハーフウェイク状態とアウェイク状態の両方のスクリーンとユーザ インターフェイスの表示をカスタマイズできます。

ハーフウェイク状態では、次のことができます。

- スクリーンとユーザ インターフェイスに背景ブランド イメージを追加します。
- スクリーン右下隅とユーザ インターフェイスのロゴを追加します。

アウェイク状態では、次のことができます。

- スクリーン右下隅とユーザ インターフェイスのロゴを追加します。
- スクリーン左下隅にラベルとメッセージを追加します (ユーザ インターフェイスには追加しない) 。

ソース構成 *(DX70、DX80、SX10 を除くすべての製品)*

1 つの画像への入力ソースを最大 4 つ構成することができます (コーデックで利用できる入力ソースの数によって異なります) 。これは、メイン ビデオ ストリームでコールの遠端に送信されるイメージです。ソース構成は API 経由でのみ有効にできるので、ユーザ インターフェイスの拡張機能をマクロと組み合わせて作成し、オンデマンドで構成を制御することをお勧めします。

この機能によって、TC ソフトウェア用の TC コンソール アプリケーションによって提供されていた機能の一部が置き換えられます。

HTTP プロキシのサポート *(すべての製品)*

シスコのクラウド サービスである Cisco Spark にデバイスを登録する場合は、HTTP プロキシを経由するようにビデオ システムをセットアップできます。

ユーザ インターフェイスの機能 *(すべての製品)*

- 設定パネルが再構成されています。
- ユーザ インターフェイスの [設定 (Settings)] パネルは、デバイスの管理者パスワードで保護することができます。このパスワードが空白の場合、誰でも [設定 (Settings)] にアクセスし、デバイスを初期設定にリセットすることができます。
- ユーザ インターフェイスでロシア語を選択した場合は、ロシア語のキーボードとラテン語文字セットのキーボードを選択できます。
- アラビア語とヘブライ語がユーザ インターフェイスに追加されています。またローカライズされたキーボードも含まれています。
- IEEE 802.1 x の基本設定が、ユーザ インターフェイスの設定パネルに追加されています。

Cisco TelePresence Precision 60 カメラのサポート

(Codec Plus)

Cisco TelePresence Precision 60 のカメラを Codec Plus に接続できます。複数のカメラを使用する場合は、カメラ コントロール ケーブルのスイッチが必要です。Precision 60 がコーデックに接続されている唯一のカメラ タイプである場合、人数のカウント機能はサポートされません。

Cisco Spark Quad Camera のサポート *(SX80)*

Cisco Spark Quad Camera を SX80 に接続することができます。Quad Cameraではコーデックの HDMI 入力の 1 つのみを使用しますが、SpeakerTrack 60 カメラでは 2 つ使用することに注意してください。Quad Camera を使用すると、人数カウント機能 (通話中) も使用できます。

ホワイトボードへのスナップ機能のサポート

(SX80, MX700、MX800、Codec Plus、Room Kit、Room 55、Room 70)

スピーカートラック機能にあるカメラを備えたすべての製品（Cisco TelePresence スピーカートラック 60 カメラまたは Cisco Spark Quad Camera を備えた SX80、デュアルカメラを備えた MX700/MX800、Room Kit、Room Kit Plus、Room 55、および Room 70）でホワイトボードへのスナップ機能を使用できるようになりました。

ホワイトボードの近くで話している人をデバイスが検出すると、カメラのビューがホワイトボード領域に切り替わります。Touch 10 ユーザ インターフェイスの設定パネルのウィザードでは、機能を設定したり、ホワイトボード領域の場所を定義したりするのに役立ちます。

ブリーフィング ルーム モード *(SX80、MX700、MX800)*

すでに TC ソフトウェアに導入されているブリーフィング ルームの機能が改良されました。室内制御フレームワークは、関連付けられたユーザ インタフェース要素を作成するために使用します。

MX700 および MX800 では、ブリーフィングルームはデュアルカメラ デバイスでのみサポートされています。また、Precision 60 カメラと合計 3 つの画面が必要です。

SX80では、ブリーフィングルームは、スピーカートラックカメラ、Precision 60 カメラ、および 3 つの画面が接続されている場合のみサポートされています。スピーカートラックカメラには、Cisco TelePresence SpeakerTrack 60 または Cisco Spark Quad Camera のいずれかを利用できます。

USB -シリアル ポートのサポート

(Codec Plus、Room Kit、Room 55、Room 70)

USB (Type A) をシリアル (D-Sub 9) アダプタに接続して、デバイスの API にアクセスできます。シスコでは、UC232R 10 USB to RS232 (FTDI) アダプタをお勧めします。

CMS ホスト会議でのリモート参加者のミュートとミュート解除 (アクティブ コントロール) *(すべての製品)*

CMS (2.1 以降) による会議でデバイスがアクティブ コントロールに対応している場合は、ユーザー インターフェイスの参加者一覧からリモート参加者をミュートおよびミュート解除できます（この機能は CMS でも有効になっている必要があります）。

ソフトウェア バージョン CE9.2 を実行しているデバイスでは、ミュートが直接解除されません。このようなデバイスをリモートでミュート解除しようとすると、ローカルで音声をミュート解除するようユーザに求めるメッセージが画面上に表示されます。

カスタム入力プロンプトの API コマンドAPI

(すべての製品)

ユーザ インターフェイスに入力プロンプトを表示できる `xCommand UserInterface Message TextInput *` の API コマンドが導入されました。表示コマンドを発行すると、カスタム テキスト、ユーザ用のテキスト入力フィールド、送信ボタンを備えたプロンプトが、ユーザ インターフェイス上に表示されます。たとえば、終了したコールの後にフィードバックを残すようにユーザに求めることができます。ユーザの入力タイプ (単一行のテキスト、数値、パスワード、または PIN コード) を指定できます。

プロンプトは API 経由でのみ有効にできるので、プロンプトを、マクロおよびカスタム ユーザ インターフェイス パネルまたは自動トリガー イベントのいずれかと組み合わせることをお勧めします。

API 経由での証明書のアップロード *(すべての製品)*

ASCII PEM 形式の証明書は、複数の API コマンド (`xCommand Security Certificates CA Add` または `xCommand Security Certificates Services Add`) を使用して直接インストールできます。従来のように証明書を Web インターフェイスからデバイスにアップロードすることもできます。

ユーザ管理用 API コマンド *(すべての製品)*

API コマンド (`xCommand UserManagement User *`) を使用してユーザアカウントを直接作成し、管理することができます。また、デバイスのユーザ インターフェイスからもアップロードできます。

室内制御のプレビューモード *(すべての製品)*

室内制御エディタには、新しいプレビュー モードがあります。仮想タッチインターフェイスを利用して、デザインがユーザインターフェイスでどのように見えるかを確認できます。ユーザ インターフェイスはインタラクティブであるため、機能をテストできます。テストでは、デバイスに実際のイベントが生成され、サードパーティ製の制御システムを使用して作成したすべての機能をトリガーすることができます。右ペインのコンソールには、対話する際のウィジェット値と、制御システムのフィードバック メッセージの両方が表示されます。

Intelligent Proximity の変更点 *(すべての製品)*

Cisco Proximity を使用して 1 つ以上のクライアントがデバイスとペアになっていることを通知するプロキシミティ インジケータが画面 (中央右側) に表示されます。Proximity が有効になっているときに常に表示されていたこれまでのインジケータ（左上）は削除されました。

ユーザ インターフェイスから Proximity サービスを無効にすることができなくなりました。

超音波設定が [周辺機器 (Peripherals)] > [ペアリング (Pairing)] > [超音波 (Ultrasound)] から [オーディオ (Audio)] > [超音波 (Ultrasound)] に移動されました。

コールサービスを変更する際の初期設定への自動リセット（デバイスの有効化） （すべての製品）

ユーザー インターフェイスからデバイス アクティブ化方法が変更されると（たとえば VCS から Cisco UCM への変更）、デバイスは自動的に初期設定にリセットして再起動します。これにより、新しいサービスに対してデバイスをプロビジョニングするときに設定の競合が回避されます。

API からプロビジョニングを変更する場合、デバイスは自動的には初期設定にリセットされません。

音声とその他のメディアで別個の RTP ポート範囲のサポート（すべての製品）

オーディオが他のメディアと異なる RTP ポート範囲を使用するようにデバイスを設定できます。これらの 2 つの範囲は重複できません。デフォルトでは、すべてのメディアは同じ RTP ポート範囲を使用します。

CE9.1 の新機能および改善点

新商品

- Cisco Webex Codec Plus (以前は Cisco Spark Codec Plus)
- Cisco Webex Room 55 (以前は Cisco Spark Room 55)

CMS ベースのミーティング用のデュアル スクリーン エクスペリエンスおよびアクティブ コントロール

(SX80、MX700、MX800、Codec Plus、Room Kit、Room 55)

デュアル スクリーンのデバイスで、両方の画面を CMS ベースの会議で利用できるようになりました。デバイスは、トランスコードされたビデオ ストリーム 2 系統と CMS からのコンテンツ ストリーム 1 系統を受信し、両方の画面を使用してこれらのストリームをレンダリングします。

アクティブ コントロールを有効にすると、すべてのミーティング参加者と参加者の現在のアクティビティ ステータス (ミュート、共有、アクティブ スピーカーなど) を示す参加者リストを取得できます。レイアウト選択パネルを使用して、タッチ インターフェイスからシームレスにレイアウトを変更できます。

新しいウェイクアップ エクスペリエンス *(すべての製品)*

SX10、DX70、DX80 : ウェイクアップエクスペリエンスには、ハーフウェイク という追加のスタンバイ状態があります。ハーフウェイク状態では、デバイスが使用されていないときに画面上に簡単な操作ガイドが表示されます。

その他の製品 : ウェイクアップ エクスペリエンスには、ハーフウェイクとモーション検知スタンバイの 2 つの追加のスタンバイ状態があります。自動復帰が有効化されている場合、デバイスは、超音波を使用してプレゼンスを検出 (モーション検知) するか、Cisco Proximity クライアントとペアリングされたときにプレゼンスを検出します。ハーフウェイク状態 (簡単なインタラクティブ操作ガイドがスクリーンに表示されている状態) になる前であれば、デバイスはグリーティングによって復帰します。

Bluetooth ヘッドセットのサポート *(DX70、DX80)*

ビデオ会議デバイスで Bluetooth ヘッドセットを使用できます。ヘッドセットは HFP (Hands Free Protocol) をサポートする必要があります。ユーザ インターフェースから、Bluetooth を有効化し、ビデオ会議デバイスを Bluetooth ペアリング モードに設定することで使用できます。

ワイヤレス ネットワーク用の EAP 認証フレームワークのサポート

(DX70、DX80、Codec Plus、Room Kit、Room 55)

デバイスの Wi-Fi 接続で、WPA-PSK と WPA2-PSK に加えて、WPA-EAP 認証フレームワークをサポートするようになりました。全部で次の方式がサポートされています。

- オープン
- WPA-PSK (AES)
- WPA2-PSK (AES)
- EAP-TLS
- EAP-TTLS
- EAP-FAST
- PEAP
- EAP-MSCHAPv2
- EAP-GTC

ルーム分析の追加

(SX10、DX70、DX80 を除く全製品)

室内の人の存在を検知 : デバイスは、室内に人がいるかどうかを検出する機能を備えています。この機能には超音波が使用されており、部屋が使用されているかどうかのみを判断し、部屋にいた人物の記録は保持されません。

人数カウント (Room Kit、Codec Plus、Room 55 のみ) : 通話中、およびセルフビュー画像の表示中に、デバイスは室内にいる人の数をカウントします。通話時以外でも人数をカウントするようにデバイスを設定できますが、デバイスがスタンバイ状態のときは人数をカウントできません。室内にいた人物の記録を保持することはなく、顔の数だけを検知します。

ネットワーク ポート 2 は無効にできます *(DX70、DX80)*

ビデオ会議デバイスの 2 番目のネットワーク ポートを介して、コンピュータをネットワークに接続することができます。これにより、壁面ネットワーク ソケット 1 個でビデオ会議デバイスとコンピュータの両方をサポートできます。

セキュリティ上の理由から、公共の環境でビデオ会議デバイスを使用する場合は、このネットワーク ポートを無効にすることを推奨します。そうすることで、第三者がデバイスを介してコンピュータをネットワークに接続するのを防ぐことができます。

CE9.0 の新機能および改善点

新製品

- Cisco Spark Room Kit (旧称 Cisco Webex Room Kit)

ユーザ インターフェイスの更新 *(すべての製品)*

Touch 10 のユーザ インターフェイス、画面上のユーザ インターフェイス、統合タッチ画面のユーザ インターフェイスが更新されました。ホーム画面上のメイン メニュー項目は、より目立つアクティビティで置き換えられました。

画面上に表示されるメニューに合わせて、一部の設定が Touch 10 の詳細設定メニューから削除されました。

動作検出のウェイク アップ *(すべての製品)*

モーション検知ウェイク アップは、会議室に誰かが入室したことを感知し、デバイスを自動的に起動します。この機能を有効にするには、次の設定を有効にする必要があります。

```
xConfiguration Standby WakeupOnMotionDetection
```

この機能が有効なときに、デバイスを手動でスタンバイ状態に設定することはできません。

室内制御エディタの更新 *(すべての製品)*

室内制御エディタが更新されて外観が新しくなり、ロジックと使い勝手が改善された、より効率的なコントロール インターフェイスになりました。さらに、新しい方向パッド ウィジェットと室内制御シミュレータが追加されています。

言語サポートの追加 *(すべての製品)*

オンスクリーン表示と Touch コントローラ メニューに、ポルトガル語 (ポルトガル) のサポートが追加されました。

その他の変更点 *(すべての製品)*

- HTTPS クライアント証明書のサポートが追加されました。
- プレゼンテーション ケーブルを抜くと、すぐにプレゼンテーション共有が停止します。

CE9.9 での設定の変更点

新しい設定

Audio Input ARC [1] Mode *(Codec Plus)*

Audio Input HDMI [2..3] Level *(Room 55D, Room 70)*

udio Input HDMI [2..3] Mode *(Room 55D, Room 70)*

Audio Input HDMI [2..3] VideoAssociation MuteOnInactiveVideo *(Room 55D、Room 70)*

BYOD TouchForwarding Enabled *(Board)*

CE9.9.0 では使用できません。

HttpFeedback TlsVerify *(すべての製品)*

Logging External TlsVerify *(すべての製品)*

Phonebook Server [1] TlsVerify *(すべての製品)*

Provisioning TlsVerify *(すべての製品)*

Standby Signage Audio *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)*

Standby Signage InteractionMode *(Board)*

Standby Signage Mode *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)*

Standby Signage RefreshInterval *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)*

Standby Signage Url *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)*

UserInterface WebcamOnlyMode *(Room Kit Mini)*

WebEngine Mode *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)*

WebEngine RemoteDebugging *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)*

削除された設定

NetworkServices HTTPS VerifyServerCertificate *(すべての製品)*

後継の設定:

- HttpFeedback TlsVerify
- Phonebook Server [1] TlsVerify
- Provisioning TlsVerify

変更された設定

Audio Ultrasound MaxVolume *(すべての製品)*

多くの製品で値スペースとデフォルト値が変更されました。製品固有の違いは内部処理され、デフォルト値や指定可能な値の範囲に反映されなくなりました。

新しい値スペース: 整数 (0 ～ 90) *(Codec Pro、Codec Plus、SX80、SX20)*

新しい値スペース: 整数 (0 ～ 70) *(Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board、SX10、MX700、MX800、MX200 G2、MX300 G2、DX70、DX80)*

新しいデフォルト値: 70 *(すべての製品)*

RTP Ports Range Stop *(すべての製品)*

旧: デフォルト: 70
新: デフォルト: 2487
旧: 整数 (1120 ～ 65535)
旧: 整数 (1121 ～ 65535)

SIP ListenPort *(すべての製品)*

旧: オフ/オン
新: Auto/Off/On

SIP ListenPort *(Board)*

旧: デフォルト値: オン
新: デフォルト:自動

SIP TlsVerify (すべての製品)

旧: デフォルト: オフ
新: デフォルト: オン

Video Output Connector [n] Location HorizontalOffset *(Codec Pro、Codec Plus、Room Kit、Room 55、Room 55D、Room 70、Room 70 G2、SX80、SX20、MX700、MX800、MX200 G2、MX300 G2)*

旧 : 整数 (-100～100)

新 : 文字列 (1、12)

Video Output Connector [n] Location VerticalOffset *(Codec Pro、Codec Plus、Room Kit、Room 55、Room 55D、Room 70、Room 70 G2、SX80、SX20、MX700、MX800、MX200 G2、MX300 G2)*

旧 : 整数 (-100～100)

新 : 文字列 (1、12)

CE9.8 での設定の変更点

新しい設定

Conference Multipoint Mode *(SX10、DX70、DX80)*

NetworkServices SMTP From *(Board)*

NetworkServices SMTP Mode *(Board)*

NetworkServices SMTP Password *(Board)*

NetworkServices SMTP Port *(Board)*

NetworkServices SMTP Security *(Board)*

NetworkServices SMTP Server *(Board)*

NetworkServices SMTP Username *(Board)*

SerialPort LoginRequired *(Codec Pro、Room 70 G2)*

UserInterface Phonebook DefaultSearchFilter *(すべての製品)*

UserInterface SoundEffects Mode *(すべての製品)*

削除された設定

Video DefaultLayoutFamily Remote *(SX10、DX70、DX80)*

変更された設定

Audio KeyClickDetector Attenuate *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2)*

旧 : デフォルト値 : オン
新 : デフォルト : True
旧 : オフ/オン
新 : False/True

Audio KeyClickDetector Enabled *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2)*

旧 : デフォルト : オフ
新 : デフォルト : True
旧 : オフ/オン
新 : False/True

Audio Output Line[1..6] Delay Mode *(Room 70 G2)*

旧 : デフォルト : RelativeToHDMI
新 : デフォルト : Fixed

CE9.7 での設定の変更点

新しい設定

HttpClient AllowHTTP *(すべての製品)*

Logging Debug Wifi *(Codec Plus、Codec Pro、DX70、DX80、Room Kit、Room Kit Mini、Room 55、Room 55 D、Room 70、Room 70 G2)*

Logging Internal Mode *(すべての製品)*

NetworkServices Websocket *(すべての製品)*

Phonebook Server [1] Pagination *(すべての製品)*

RoomAnalytics AmbientNoiseEstimation Mode (Codec Plus, Codec Pro, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)

UserInterface Features Call VideoMute (Codec Plus、Codec Pro、MX200 G2、MX300 G2、MX700、MX800、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、SX10、SX20、SX80)

UserInterface Features Whiteboard Start (DX70、DX80)

UserInterface Phonebook Mode *(すべての製品)*

UserInterface SettingsMenu Visibility *(すべての製品)*

UserInterface UsbPromotion *(Room Kit Mini)*

削除された設定

RoomAnalytics PeopleCountOutOfCall *(MX700、MX800)*

変更された設定

Audio Input Line [1..4] VideoAssociation VideoInputSource (MX700、MX800、SX80)

旧: 1/2/3/4/5

新: 1/2/3/4

Audio Input Microphone [1..8] VideoAssociation VideoInputSource *(Codec Pro、Room 70 G2)*

旧: 1/2/3/4/5

New: /1/2/3/4/5/6

Audio Input Microphone [1..8] VideoAssociation VideoInputSource *(MX700、MX800、SX80)*

旧: 1/2/3/4/5

新: 1/2/3/4

Video Input Connector [6] CameraControl Mode *(Codec Pro、Room 70 G2)*

旧 : デフォルト値 : オン

新 : デフォルト値 : オフ

旧 : オン

新 : オン/オフ

Video Presentation Priority *(すべての製品)*

旧 : Equal/High

新 : Equal/High/Low

CE9.6 での設定の変更点

新しい設定

オーディオ入力マイク[1..8] チャンネル *(Codec Pro、Room 70 G2)*

オーディオ入力 HDMI [n] レベル *(Code Plus、Room 55、Room 70 G2、Room Kit)*

オーディオ入力 HDMI [n] モード (Room 70 G2、Room Kit)

オーディオ入力 HDMI [2..5] VideoAssociation MuteOnInactiveVideo (Room 70 G2)

オーディオマイク PhantomPower *(Codec Plus、MX200 G2、MX300 G2、Room 55、Room Kit、SX20)*

オーディオ出力コネクタ設定 *(Codec Pro、Room 70 G2)*

オーディオ出力 HDMI [n] レベル *(MX700、MX800)*

オーディオ出力 HDMI [n] モード *(Codec Plus、MX700、MX800)*

オーディオ出力 InternalSpeaker モード *(MX700、MX800、Room 55 Dual、Room 70)*

オーディオ出力ライン [1..6] Equalizer ID (Room 70 G2)

オーディオ出力ライン [1..6] Equalizer モード *(Room 70 G2)*

HttpClient AllowInsecureHTTPS *(すべての製品)*

HttpClient モード *(すべての製品)*

NetworkServices NTP サーバ [1..3] キー *(すべての製品)*

NetworkServices NTP サーバ [1..3] KeyId *(すべての製品)*

NetworkServices NTP サーバ [1.. 3] KeyAlgorithm *(すべての製品)*

周辺機器の入力デバイスモード *(DX70、DX80)*

UserInterface ブランド AwakeBranding 色 *(すべての製品)*

UserInterface 機能 : 通話の終了 *(すべての製品)*

UserInterface 機能 : 通話 MidCallControls *(すべての製品)*

UserInterface 機能 : 通話開始 *(すべての製品)*

UserInterface 機能 : すべて非表示 *(すべての製品)*

UserInterface 機能 : 共有開始 *(すべての製品)*

ビデオ入力コネクタ [n] HDCP モード *(Codec Plus、Codec Pro、Room 55 Dual、Room 70、Room 70 G2)*

ビデオ出力コネクタ [2] CECモード (Room 70 Single)

ビデオ プレゼンテーション 優先順位 *(すべての製品)*

削除された設定

会議の MultiStream モード (MX200 G2, MX300 G2, SX20)

SIP PreferredIPMedia *(すべての製品)*

変更された設定

オーディオ出力 ARC[1] モード *(Codec Pro、Room 70 G2)*

旧 : デフォルト値 : 自動
新: デフォルト: オン
旧 : 値スペース : オフ / オン / 自動
新 : 値スペース : オフ / オン

オーディオ出力 HDMI [1...3] モード *(Codec Pro、Room 70 G2)*

旧: デフォルト値 : 自動 *(Codec Pro)*
新: デフォルト値 : オン *(Codec Pro)*
旧 : デフォルト値、HDMI [2..3]: 自動 *(Room 70G2 Single)*
新 : デフォルト値、HDMI [2..3]: オフ *(Room 70G2 Single)*
旧 : デフォルト値、HDMI [3]: 自動 *(Room 70G2 Dual)*
新 : デフォルト値、HDMI [3]: オフ *(Room 70G2 Dual)*
旧 : 値スペース : オフ / オン / 自動 *(Codec Pro、Room 70 G2)*
新 : 値スペース : オフ / オン *(Codec Pro、Room 70 G2)*

オーディオ出力内部スピーカーモード *(Room 55、Room 70 G2、Room Kit)*

旧 : デフォルト値: 自動 *(Room 70 G2)*
新 : デフォルト値 : オン *(Room 70 G2)*
旧 : 値スペース : オフ / オン / 自動 *(Room 70 G2)*
新 : 値スペース : オフ / オン / ウルトラサウンドのみ *(Room 70 G2)*
旧 : 値スペース : オフ / オン *(Room 55、Room Kit)*
新 : 値スペース : オフ / オン / ウルトラサウンドのみ *(Room 55、Room Kit)*

オーディオ ウルトラ サウンド最大音量 *(SX20)*

旧 : デフォルト : 70
新: デフォルト: 60

Provisioning Mode *（すべての製品）*

旧 : 値スペース : Auto / CUCM / Edge / Off / TMS / VCS / Spark

新 : 値スペース : Auto / CUCM / Edge / Off / TMS / VCS / Webex

Provisioning Mode *(Room 55 Dual)*

旧 : デフォルト : オフ

新: デフォルト: オン

Standby WakeupOnMotionDetection *(Room 55 Dual)*

旧 : デフォルト : オフ

新: デフォルト: オン

CE9.5 での設定の変更点

新しい設定

オーディオ入力 ARC[n] モード *(Codec Pro、Room 70 G2)*

オーディオ出力 ARC[1] 遅延 DelayMs *(Codec Pro, Room 70 G2)*

オーディオ出力 ARC[1] 遅延モード *(Codec Pro、Room 70 G2)*

オーディオ出力 ARC[1] モード *(Codec Pro、Room 70 G2)*

オーディオ出力内部スピーカーモード *(Room 70 G2)*

オーディオ出力ライン[1] モード *(Codec Plus、Room 55)*

オーディオ出力ライン[1] 出力タイプ *(Codec Plus, Room 55)*

NetworkServices SSH HostKeyAlgorithm *(すべての製品)*

周辺機器 InputDevice モード *(Codec Plus、Codec Pro、Room Kit、Room 55、Room 55 Dual、Room 70、Room 70 G2)*

RoomAnalytics PeopleCountOutOfCall *(SX80)*

削除された設定

オーディオ出力内部スピーカーモード *(Codec Pro)*

Cameras SpeakerTrack ConnectorDetection CameraLeft *(Room 70 G2)*

Cameras SpeakerTrack ConnectorDetection CameraRight *(Room 70 G2)*

Cameras SpeakerTrack ConnectorDetection モード *(Codec Pro、Room 70 G2)*

Cameras SpeakerTrack TrackingMode *(Codec Pro、Room 70 G2)*

Provisioning RoomType ClassroomEnabled *(SX80、MX700、MX800、Codec Pro、Room 70 G2)*

変更された設定

オーディオ入力マイク[1..8] イコライザ ID *(Codec Pro、Room 70 G2)*

旧 : 値スペース : 整数 (1..14)

新 : 値スペース : 整数 (1..8)

オーディオウルトラサウンド最大音量 *(SX80, MX700, MX800, Codec Pro, Room 70 G2)*

旧 : デフォルト値: 70 *(SX80, Codec Pro、MX700、MX800、Room 70 G2)*

新 : デフォルト値 : 60 *(SX80、Codec Pro、Room 70 G2)*

新 : デフォルト値: 66 *(MX700、MX800)*

旧 : 値スペース : 整数 (0..90) *(Room 70 G2)*

新 : 値スペース : 整数 (0..80) *(Room 70 G2)*

カメラ PresenterTrack コネクタ *(Codec Plus、Codec Pro、Room 70、Room 70 G2)*

旧 : デフォルト値 : 1 *(Codec Pro、Room 70 G2)*

新 : デフォルト値 : 6 *(Codec Pro、Room 70 G2)*

旧 : 値スペース : 整数 (1..5) *(Codec Plus, Codec Pro, Room 70, Room 70 G2)*

新 : 値スペース : 整数 (1..3) *(Codec Plus, Room 70)*

新 : 値スペース : 整数 (1..6) *(Codec Pro、Room 70 G2)*

ビデオ入力コネクタ[3,4,5] PreferredResolution *(Codec Pro、Room 70 G2)*

旧 : デフォルト値 : 3840_2160_30

新 : デフォルト値 : 1920_1080_60

CE9.4 での設定の変更点

新しい設定

オーディオ入力 HDMI [1..2] モード *(Room 55)*

オーディオ入力 HDMI [1..2] VideoAssociation MuteOnInactiveVideo *(Room 55)*

オーディオ出力 [1] OutputType *(Room 70)*

Cameras Camera [1] Backlight DefaultMode

Cameras Camera [1..2] Mirror *(MX700、MX800)*

Conference FarendMessage Mode *(すべての製品)*

SIP MinimumTLSVersion *(すべての製品)*

削除された設定

NetworkServices HTTP Proxy Allowed *(すべての製品)*

Video Output Connector [2] CEC Mode *(DX70、DX80)*

ビデオ出力コネクタ [2] ロケーション水平 HorizontalOffset *(DX70、DX80)*

ビデオ出力コネクタ [2] ロケーション垂直オフセット *(DX70、DX80)*

Video Output Connector [2] OverscanLevel *(DX70、DX80)*

Video Output Connector [2] Resolution *(DX70、DX80)*

ビデオ出力コネクタ [2] RGBQuantizationRange *(DX70、DX80)*

変更された設定

オーディオ出力 [1] OutputType *(Room Kit)*

旧 : デフォルト値 : LineOut (ライン出力)
新 : デフォルト値 : Loudspeaker
旧 : 値スペース : LineOnt/Subwoofer
新 : 値スペース : LineOut/Loudspeaker/Recorder/Subwoofer

オーディオ ウルトラサウンド最大音量 *(MX200 G2、MX300 G2、Codec Plus、Room 55、Room 70)*

旧 : デフォルト値 : 60 *(MX200 G2、 MX300 G2)*
旧 : デフォルト値 : 70 *(Codec Plus、Room 55、Room 70)*
旧 : デフォルト値 : 50 *(MX200 G2、 MX300 G2)*
新 : デフォルト値 : 60 *(Codec Plus、Room 70)*
新 : デフォルト値 : 64 *(Room 55)*
旧 : 値スペース : 整数 (0..80) *(MX200 G2、MX300 G2)*
旧 : 値スペース : 整数 (0..90) *(Room 55、Room 70)*
新 : 値スペース : 整数 (0..70)) *(MX200 G2、MX300 G2)*
新 : 値スペース : 整数 (0..80) *(Room 70)*
新 : 値スペース : 整数 (0..84) *(Room 55)*

Network [1] DNS DNSSEC Mode *(すべての製品)*

旧 : ユーザ ロール : ADMIN、USER
新 : ユーザ ロール : ADMIN

Network [1] Speed *(すべての製品)*

旧 : ユーザ ロール : ADMIN、USER
新 : ユーザ ロール : ADMIN、INTEGRATOR

NetworkServices HTTP Mode *(すべての製品)*

旧 : デフォルト値 : HTTP+HTTPS
新 : デフォルト値 : HTTPS

NetworkServices SNMP CommunityName *(すべての製品)*

旧 : ユーザ ロール : ADMIN
新 : ユーザ ロール : ADMIN、INTEGRATOR

NetworkServices SNMP Host [1..3] Address *(すべて製品)*

旧 : ユーザ ロール : ADMIN
新 : ユーザ ロール : ADMIN、INTEGRATOR

NetworkServices SNMP Mode *(すべての製品)*

旧 : ユーザ ロール : ADMIN
新 : ユーザ ロール : ADMIN、INTEGRATOR

NetworkServices SNMP SystemContact *（すべての製品）*

旧 : ユーザ ロール : ADMIN

新 : ユーザ ロール : ADMIN、INTEGRATOR

NetworkServices SNMP SystemLocation *（すべての製品）*

旧 : ユーザ ロール : ADMIN

新 : ユーザ ロール : ADMIN、INTEGRATOR

UserInterface ContactInfo Type *(SX10、DX70、DX80)*

旧 : 設定可能な値 : Auto / DisplayName / IPv4 / IPv6 / None / SipUri / SystemName

新 : 設定可能な値 : Auto / DisplayName / E164Alias / H320Number / H323Id / IPv4 / IPv6 / None / SipUri / SystemName

ビデオ出力コネクタ [1] CEC モード *(SX10)*

旧 : デフォルト値 : Off

新 : デフォルト値 : On

ビデオ出力コネクタ [3] 解像度 *(SX80)*

旧 : ユーザ ロール : Admin、INTEGRATOR

新 : ユーザ ロール : ADMIN、INTEGRATOR、USER

CE9.3 での設定の変更点

新しい設定

Audio KeyClickDetector 減衰 *(Codec Plus、Room Kit、Room 55、Room 70)*

オーディオ KeyClickDetector 有効化 *(Codec Plus, Room Kit, Room 55, Room 70)*

カメラ カメラ [1..3] AssignedSerialNumber *(Codec Plus、Room 70)*

カメラ カメラ [3] バックライト DefaultMode *(Codec Plus、Room 70)*

カメラ カメラ [3] 明るさ DefaultLevel *(Codec Plus, Room 70)*

カメラ カメラ [3] 明るさモード *(Codec Plus、Room 70)*

カメラ カメラ [3] 焦点モード *(Codec Plus、Room 70)*

カメラ カメラ [3] ガンマ レベル *(Codec Plus、Room 70)*

カメラ カメラ [3] ガンマ モード *(Codec Plus、Room 70)*

カメラ カメラ [3] ミラリング *(Codec Plus、Room 70)*

カメラ カメラ [3] ホワイト バランス レベル *(Codec Plus、Room 70)*

カメラ カメラ [3] ホワイト バランス モード *(Codec Plus、Room 70)*

Network [1] DNS DNSSEC Mode *(すべての製品)*

NetworkServices HTTP Proxy PACUrl *(すべての製品)*

SystemUnit CrashReporting Advanced *(すべての製品)*

SystemUnit CrashReporting Mode *(すべての製品)*

SystemUnit CrashReporting URL *(すべての製品)*

UserInterface Accessibility IncomingCallNotification *(すべての製品)*

UserInterface Security Mode *(すべての製品)*

ビデオ セルフビュー ミラリング *(DX70、DX80)*

削除された設定

Provisioning HttpMethod *(すべての製品)*

変更された設定

NetworkServices HTTP Proxy Allowed *(すべての製品)*

旧 : デフォルト値 : True

新 : デフォルト値 : False

NetworkServices HTTP Proxy Mode *(すべての製品)*

旧 : 値スペース : Manual/Off

新 : 値スペース : Manual/Off/PACUrl/WPAD

プロキシミティ (Room 70)

旧 : デフォルト値 : Off

新 : デフォルト値 : On

Security Session MaxSessionsPerUser *(すべての製品)*

旧 : デフォルト値 : 0

新 : デフォルト値 : 20

旧 : 値スペース : 整数 (0..100)

新 : 値スペース : 整数 (1..20)

Security Session MaxTotalSessions *(すべての製品)*

旧 : デフォルト値 : 0

新 : デフォルト値 : 20

旧 : 値スペース : 整数 (0..100)

新 : 値スペース : 整数 (1..20)

スタンドバイ WakeupOnMotionDetection *(Room 70)*

旧 : デフォルト値 : Off

新 : デフォルト値 : On

ビデオ入力コネクタ [2] 名 *(Room 55)*

旧 : デフォルト値 : “PC 1 (HDMI)”

新 : デフォルト値 : “”

ビデオ入力コネクタ[3] 名 *(Room 55)*
旧 : デフォルト値 : “PC 2 (HDMI)”
新 : デフォルト値 : “”

ビデオ入力コネクタ [1] CEC モード *(Room 70)*
旧 : 値スペース : Off/On
新 : 値スペース : On

CE9.2 での設定の変更点

新しい設定

Audio Input HDMI [n] Mode *(Codec Plus)*

オーディオ入力 HDMI[n] VideoAssociation MuteOnInactiveVideo *(Codec Plus, Room Kit)*

Audio Output InternalSpeaker Mode *(Room 55)*

Audio Ultrasound MaxVolume *(すべての製品)*
周辺機器ペアリング ウルトラサウンド音量最大レベルの置き換え

オーディオ ウルトラサウンド モード *(すべての製品)*
周辺機器ペアリング ウルトラサウンド音量モデルの置き換え

カメラ カメラ [1..2] 焦点モード *(MX700、MX800)*
統合カメラの追加

カメラ SpeakerTrack ホワイトボード モード *(Codec Plus、Room Kit,、Room 55)*

Macros AutoStart *(SX10 を除くすべての製品)*

Macros Mode *(SX10 を除くすべての製品)*

NetworkServices HTTP Proxy Allowed *(すべての製品)*

NetworkServices HTTP Proxy LoginName *(すべての製品)*

NetworkServices HTTP Proxy Mode *(すべての製品)*

NetworkServices HTTP プロキシ パスワード *(すべての製品)*

NetworkServices HTTP Proxy Url *(すべての製品)*

RTP ビデオポート範囲開始 *(すべての製品)*

RTP ビデオポート範囲終了 *(すべての製品)*

セキュリティセッション FailedLoginsLockoutTime *(すべての製品)*

セキュリティセッション MaxFailedLogins *(すべての製品)*

UserInterface CustomMessage *(すべての製品)*

UserInterface OSD HalfwakeMessage *(すべての製品)*

UserInterface SettingsMenu Mode *(すべての製品)*

Video Input Connector[n] HDCP Mode *(Room 55)*

削除された設定

会議マルチストリームモード *(SX10、DX70、 DX80)*

周辺機器ペアリングウルトラサウンド音量最大レベル *(すべての製品)*
オーディオ ウルトラサウンド最大音量 に置き換え

周辺機器ペアリングウルトラサウンド音量モード *(すべての製品)*
オーディオ ウルトラサウンド モードに置き換え

変更された設定

オーディオ入力 MicrophoneMode *(DX70、DX80)*
旧 : ユーザ ロール : ADMIN
新 : ユーザ ロール : ADMIN、INTEGRATOR

Audio Input Microphone[n] Level *(Room Kit、Room 55)*
旧 : 値スペース : 0 ～ 36
新 : 値スペース : 0 ～ 26

カメラ カメラ[n]フォーカスモード *(SX80、MX700、MX800、Codec Plus)*
旧 : 値スペース : Auto/Manual
新 : 値スペース : Auto/AutoLimited/Manual

カメラ SpeakerTrack クローズアップ *(SX80、MX700、MX800、Room Kit、Codec Plus、Room 55)*
旧 : ユーザ ロール : Admin、INTEGRATOR
新 : ユーザ ロール : ADMIN、INTEGRATOR、USER

カメラ SpeakerTrack ホワイトボードモード *(SX80、MX700、MX800)*
旧 : ユーザ ロール : Admin、INTEGRATOR
新 : ユーザ ロール : ADMIN、INTEGRATOR、USER

セキュリティ監査ロギングモード *(すべての製品)*
旧 : デフォルト値 : Off
新 : デフォルト値 : Internal

UserInterface Language *(すべての製品)*
新 : Arabic および Hebrew が値スペースに追加されました。

UserInterface OSD 出力 *(Room Kit)*
- 旧 : デフォルト値 : 1
- 新 : デフォルト値 : Auto

ビデオ入力コネクタ[2] 名称 *(Codec Plus、Room 55)*
- 旧 : デフォルト値 : PC (HDMI1)
- 新 : デフォルト値 : PC 1 (HDMI)

ビデオ入力コネクタ[3] 名称 *(Codec Plus、Room 55)*
- 旧 : デフォルト値 : PC (HDMI2)
- 新 : デフォルト値 : PC 2 (HDMI)

ビデオ出力コネクタ[1] 解像度 *(MX200G2、MX300G2、DX70、DX80、Room 55)*
- 旧 : ユーザ ロール : Admin、INTEGRATOR
- 新 : ユーザ ロール : ADMIN、INTEGRATOR、USER

ビデオ Selfview OnCall モード *(Room Kit)*
- 旧 : デフォルト値 : Off
- 新 : デフォルト値 : On

CE9.1 での設定の変更点

新しい設定

Bluetooth 可 *(DX70、DX80)*

Bluetooth 有効 *(DX70、DX80)*

カメラ カメラ フレーム レート *(Room Kit)*

NetworkPort [2] Mode *(DX70、DX80)*

RoomAnalytics PeopleCountOutOfCall *(Codec Plus、Room Kit)*

RoomAnalytics PeoplePresenceDetector *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800、Codec Plus、Room Kit)*

ビデオ入力コネクタ [n] CEC モード *(Codec Plus、Room Kit)*

削除された設定

なし

変更された設定

会議 DefaultCall レート *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800、Codec Plus、Room Kit)*

旧 : デフォルト値 : 3072

新 : デフォルト値 : 6000

会議 MultiStream モード *(SX80、MX700、MX800、Codec Plus、Room Kit)*

旧 : デフォルト値 : Off

新 : デフォルト値 : Auto

旧 : 値スペース : Off

新 : 値スペース : Auto/Off

ネットワーク[1] IEEE8021X パスワード *(すべての製品)*

旧 : 値スペース : 文字列 (0、32)

新 : 値スペース : 文字列 (0、50)

NetworkServices WiFi 有効化 *(DX70、DX80)*

旧 : デフォルト値 : False

新 : デフォルト値 : True

周辺機器プロファイル TouchPanels *(SX80、Codec Plus、Room Kit)*

旧 : デフォルト値 : NotSet

新 : デフォルト値 : Minimum1

スタンバイ WakeupOnMotionDetection *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800、Codec Plus、Room Kit)*

旧 : デフォルト値 : Off

新 : デフォルト値 : On

ビデオ入力コネクタ[n] PresentationSelection *(すべての製品)*

旧 : 値スペース : AutoShare/Manual/OnConnect *(SX10、SX20、SX80、MX200 G2、MX300 G2、MX700、MX800、Codec Plus、Room Kit)*

旧 : 値スペース : AutoShare/Desktop/Hidden/Manual/OnConnect (DX70、DX80)

新 : 値スペース : AutoShare/Desktop/Manual/OnConnect (すべての製品)

ビデオ出力コネクタ [1..2] MonitorRole *(Room Kit、Codec Plus)*

旧 : デフォルト値 : Connector [1] : First Connector [2] : Second

新 : デフォルト値 : Auto

CE9.0 での設定の変更点

新しい設定

Cameras SpeakerTrack Closeup *(SX80、MX700、MX800)*

NetworkServices HTTPS Server MinimumTLSVersion *(すべての製品)*

NetworkServices HTTPS StrictTransportSecurity *(すべての製品)*

Peripherals Pairing CiscoTouchPanels EmcResilience *(SX10、SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Standby WakeupOnMotionDetection *(すべての製品)*

削除された設定

UserInterface UserPreferences *(すべての製品)*

Audio Microphones PhantomVoltage *(SX20、MX200 G2、MX300 G2)*

Conference VideoBandwidth PresentationChannel Weight *(すべての製品)*

Standby AudioMotionDetection *(すべての製品)*

Video Layout DisableDisconnectedLocalOutputs *(SX20、MX200 G2、MX300 G2、DX70、DX80)*

変更された設定

Cameras Camera [n] * *(SX10、SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

旧 : ユーザ ロール : ADMIN、USER

新 : ユーザ ロール : ADMIN、INTEGRATOR

Cameras PresenterTrack * *(SX80、MX700、MX800)*

旧 : ユーザ ロール : ADMIN、USER

新 : ユーザ ロール : ADMIN、INTEGRATOR

Cameras SpeakerTrack * *(SX80、MX700、MX800)*

旧 : ユーザ ロール : ADMIN、USER

新 : ユーザ ロール : ADMIN、INTEGRATOR

Conference MultiStream Mode *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

旧 : 値スペース : Auto/Off

新 : 値スペース : Off

NetworkServices Wifi Allowed *(DX70、DX80)*

名前が NetworkServices WIFI Allowed から変更されました

旧 : ユーザ ロール : ADMIN

新 : ユーザ ロール : ADMIN、USER

NetworkServices WiFi 有効化 *(DX70、DX80)*

名前が NetworkServices WIFI Enabled から変更されました

旧 : ユーザ ロール : ADMIN

新 : ユーザ ロール : ADMIN、USER

UserInterface Language *(すべての製品)*

新 : 値スペースに Portuguese が追加されました。

新しい INTEGRATOR ユーザ ロールに関する設定

新しいユーザ ロール INTEGRATOR が、CE9.0 で導入されました。これは、次の設定に追加されています。

Audio DefaultVolume *(すべての製品)*

Audio Input HDMI [n] * *(SX80、MX700、MX800)*

Audio Input Line [n] * *(SX20、SX80、MX700、MX800)*

Audio Input Microphone [n] * *(SX10、SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Audio MicrophoneReinforcement * *(SX80、MX700、MX800)*

オーディオマイクをミュートに有効する *(すべての製品)*

Audio Output HDMI [n] * *(SX80)*

Audio Output Line [n] * *(SX10、SX20、SX80、MX700、MX800)*

オーディオ音声とアラート* *(すべての製品)*

CallHistory モード *(すべての製品)*

Cameras Camera [n] * *(SX10、SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Cameras PowerLine Frequency *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Cameras PresenterTrack * *(SX80、MX700、MX800)*

Cameras SpeakerTrack * *(SX80、MX700、MX800)*

会議のデフォルト通話料金 *(すべての製品)*

会議はデフォルトタイムアウトを邪魔しない *(すべての製品)*

FacilityService * *(すべての製品)*

GPIO Pin [n] Mode *(SX80、MX700、MX800)*

周辺機器ペアリングウルトラサウンド音量最大レベル *(すべての製品)*

周辺機器ペアリングウルトラサウンド音量モード *(すべての製品)*

周辺機器プロファイル * *(SX10、SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

SerialPort BaudRate *(SX20、SX80、MX700、MX800)*

シリアルポートモード *(すべての製品)*

スタンバイ * *(SX10、SX20、SX80、MX200 G2、MX300 G2、DX70、DX80)*

待機ブートアクション *(MX700、MX800)*

待機コントロール *(MX700、MX800)*

待機遅延 *(MX700、MX800)*

待機 待機アクション *(MX700、MX800)*

待機 ウェイクアップアクション *(MX700、MX800)*

モーション検知ウェイクアップのスタンバイ *(MX700、MX800)*

システムユニット名 *(すべての製品)*

Time Zone *(すべての製品)*

UserInterface OSD Output *(すべての製品)*

UserInterface Wallpaper *(すべての製品)*

Video ActiveSpeaker DefaultPIPPosition *(すべての製品)*

Video Input Connector [n] * *(SX10、DX70、DX80)*

Video Input Connector [n] CameraControl CameraId *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] CameraControl CameraId *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] InputSourceType *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] Name *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] OptimalDefinition Profile *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] PresentationSelection *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] Quality *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] RGBQuantizationRange *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

Video Input Connector [n] Visibility *(SX20、SX80、MX200 G2、MX300 G2、MX700、MX800)*

ビデオ モニター *(すべての製品)*

Video Output Connector [n] * *(SX80、MX700、MX800)*

Video Output Connector [n] CEC Mode *(SX10、SX20、MX200 G2、MX300 G2、DX70、DX80)*

Video Output Connector [n] Location HorizontalOffset *(SX20、MX200 G2、MX300 G2、DX70、DX80)*

Video Output Connector [n] Location VerticalOffset *(SX20、MX200 G2、MX300 G2、DX70、DX80)*

Video Output Connector [n] MonitorRole *(SX20)*

Video Output Connector [n] Resolution *(SX10、SX20、MX200 G2、MX300 G2、DX70、DX80)*

Video Output Connector [n] RGBQuantizationRange *(SX10、SX20、MX200 G2、MX300 G2、DX70、DX80)*

Video Presentation DefaultPIPPosition *（すべての製品）*

Video Selfview Default * *（すべての製品）*

Video Selfview OnCall * *（すべての製品）*

<path> * は、*<path>* で始まるすべての設定に変更が適用されることを意味します。

DX70 および DX80 の概要

Cisco Webex DX70 と DX80 は、ビデオに対応した小型コラボレーション スペース向けに設計されたオールインワン装置です。

これらの装置には、高解像度 (HD) ビデオ、ユニファイド コミュニケーション機能、ラップトップ用の表示、各種拡張機能など高度な機能が搭載されています。

機能とメリット

- 専用の常時接続の 1080p 高解像度ビデオ コミュニケーション デバイス
- スピーカーフォン用の高品位音声システム
- ワイヤレス Bluetooth ヘッドセット、USB ドングルを使用する Bluetooth ヘッドセット、および USB ヘッドセットのサポート
- 23 インチ (DX80) または 14 インチ (DX70) の 16:9 画面が、ビデオ通話に魅力的なエクスペリエンスを提供
- 静電容量方式マルチタッチスクリーンの洗練されたパワフルなユーザ インターフェイス
- デバイスの簡単なセルフプロビジョニングで、開封後は即座に使用可能
- 管理者は Cisco Expressway を利用してリモート ワーカーのセキュアな接続を実現
- Cisco Unified Communications Manager (UCM) 、Cisco TelePresence Video Communication Server (VCS) 、および Cisco Webex に登録

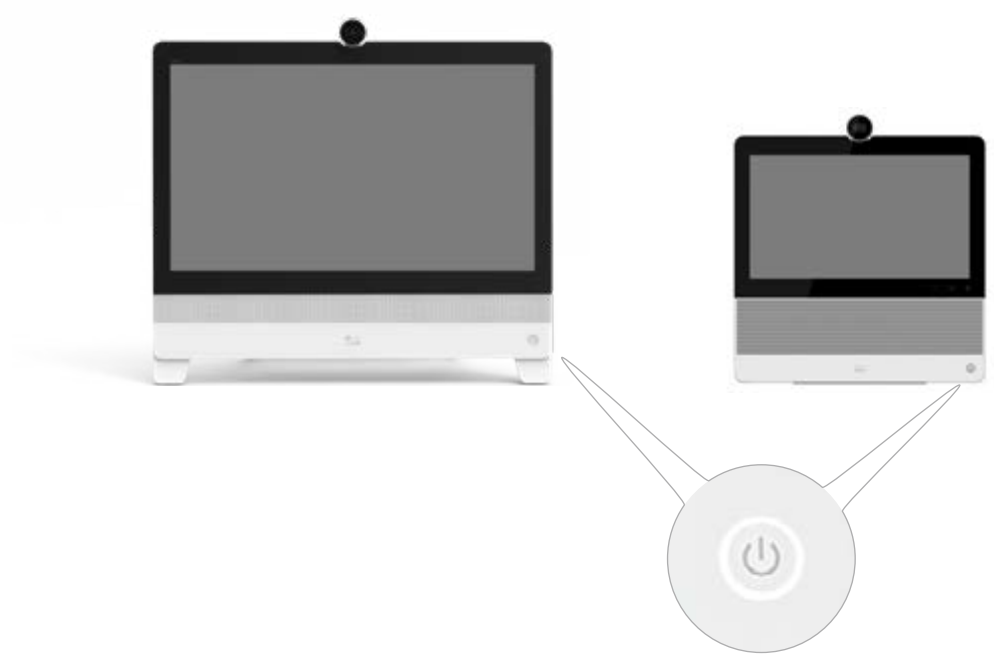
Cisco Webex DX70

Cisco Webex DX80

電源のオンとオフ (1/2 ページ)

電源ボタンによる電源のオン/オフ

LED インジケータ付きの電源ボタンが、図に示すように前面にあります。



電源ボタン (LED が電源ボタンを囲んでいます)

スイッチを入れる

デバイスは自動的に起動しません。電源ボタンを軽く押して数秒間押し続けます。

デバイスの起動中は LED が点灯しています。

スイッチを切る

電源ボタンを軽く押して消灯するまで押し続けます。

スタンバイ モードの開始/終了

電源ボタンを短く押します。デバイスがスタンバイ状態になるまでに数秒かかります。

電源のオンとオフ (2/2 ページ)

ユーザインターフェイスを使用した再起動とスタンバイ

デバイスの再起動

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [設定 (*Settings*)]、[再起動 (*Restart*)] の順に選択します。
3. [再起動 (*Restart*)] を再度選択して、選択内容を確認します。

スタンバイ モードの開始

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [スタンバイ (*Standby*)] を選択します。

スタンバイ モードの終了

- 画面をタップします。

リモートからのデバイスの電源オフまたは再起動

ウェブ インターフェイスにサインインして、[メンテナンス (Maintenance)] > [再起動 (Restart)] に移動します。

デバイスの再起動

[デバイスの再起動... (Restart device...)] をクリックして、選択を確定します。

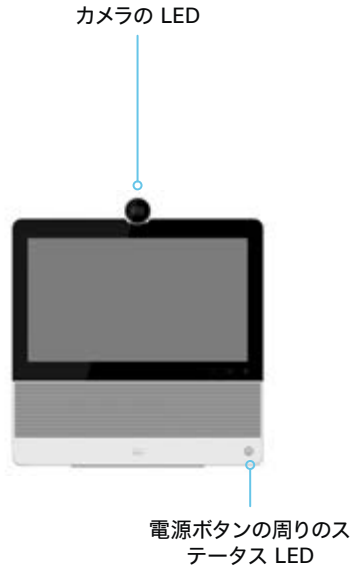
デバイスが使用可能になるまでに数分かかります。

デバイスの電源オフ

[デバイスのシャットダウン... (Shutdown device...)] をクリックして、選択を確定します。

デバイスの電源をリモートから再度オンにすることはできません。 電源ボタンを使用する必要があります。

LED インジケータ



ステータス LED

ステータス LED は、電源ボタンの周りの円形状の部分です。LED の通常の色は白です。赤色のライトは、ハードウェア障害を示します。

通常の動作（非スタンバイ状態）：

点灯します。

スタンバイ モード時：

LED がゆっくり点滅します。

ネットワーク接続がない場合：

LED が 2 回ずつ、繰り返し点滅します。

スタートアップ（起動）時:

LED が点滅します。

カメラの LED

カメラの LED はカメラのレンズのすぐ上にあります。

コールの着信時:

LED が点滅します。

コール中:

点灯状態になります。

ビデオ会議デバイスの管理方法 (1/4 ページ)

一般的には、この管理者ガイドで説明するように、デバイスの管理とメンテナンスに Web インターフェイスを使用することを推奨します。

それ以外にも次の方法でデバイスの API にアクセスできます。

- HTTP/HTTPS (Web インターフェイスでも使用)
- WebSocket
- Telnet
- SSH
- シリアル接続

他のアクセス方法や API の使用方法の詳細については、デバイスの API ガイドをご覧ください。

ヒント

設定またはステータスが API で使用可能な場合、ウェブ インターフェイスの設定またはステータスは次のような API の設定またはステータスに変換されます。

X > Y > Z への Value の設定 (Web)
　次と同等です。
`xConfiguration X Y Z: 値 (API)`

(ウェブで) X > Y > Z ステータスにチェックマークを付けることは
　以下と同じです。
`xStatus X Y Z (API)`

次に例を示します。

[システムユニット (SystemUnit)] > [名前 (Name)] を [MySystem] と設定すると、
　次と同等です。
`xConfiguration SystemUnit Name: MySystem`

[システムユニット (SystemUnit)] > [ソフトウェア (Software)] > [バージョン (Version)] ステータスにチェックマークを付けることは
　以下と同じです。
`xStatus SystemUnit Software Version`

ウェブ インターフェイスでは、API の場合よりも多くの設定とステータスを使用できます。

アクセス方式	注	方式の有効化/無効化方法
HTTP/HTTPS	・デバイスの Web インターフェイスで使用されます。 ・非セキュア (HTTP) 通信またはセキュア (HTTPS) 通信 ・HTTPS : デフォルトで有効 ・HTTP : デバイスを以前のソフトウェア バージョンから CE9.4 以降にアップグレードし、アップグレード後に初期設定にリセットしていない場合にのみ、デフォルトで有効	[ネットワークサービス (NetworkServices)] > [HTTP] > [モード (Mode)] 変更を有効にするには、デバイスを再起動してください。
WebSocket	・HTTP に関連付けられるため、WebSocket を使用するには HTTP または HTTPS も有効化する必要があります ・暗号化 (wss) または非暗号化 (ws) の通信 ・デフォルトで [無効 (Disabled)]	[ネットワークサービス (NetworkServices)] > [HTTP] > [モード (Mode)] [ネットワークサービス (NetworkServices)] > [WebSocket] 変更を有効にするには、デバイスを再起動してください。
Telnet	・非セキュア TCP/IP 接続 ・デフォルトで [無効 (Disabled)]	[ネットワークサービス (NetworkServices)] > [Telnet] > [モード (Mode)] デバイスを再起動する必要はありません。変更が有効になるまでに少し時間がかかる場合があります。
SSH	・セキュアな TCP/IP 接続 ・デフォルトでイネーブルになっている。	[ネットワークサービス (NetworkServices)] > [SSH] > [モード (Mode)] デバイスを再起動する必要はありません。変更が有効になるまでに少し時間がかかる場合があります。
シリアル接続	・ケーブルを使用してデバイスに接続します。IP アドレス、DNS、ネットワークは不要。 ・デフォルトでイネーブルになっている。 ・セキュリティ上の理由から、デフォルトではサインインを求められます ([シリアルポート (SerialPort)] > [ログイン必須 (LoginRequired)]) 。	[シリアルポート (SerialPort)] > [モード (Mode)] 変更を有効にするには、デバイスを再起動してください。

すべてのアクセス方式を無効にする ([**オフ (Off)**] に設定する) と、デバイスを設定できなくなります。再び有効にする ([**オン (On)**] に設定する) ことはできないため、復元するにはデバイスを初期設定にリセットする必要があります。

ビデオ会議デバイスの管理方法 (2/4 ページ)

デバイスの Web インターフェイス

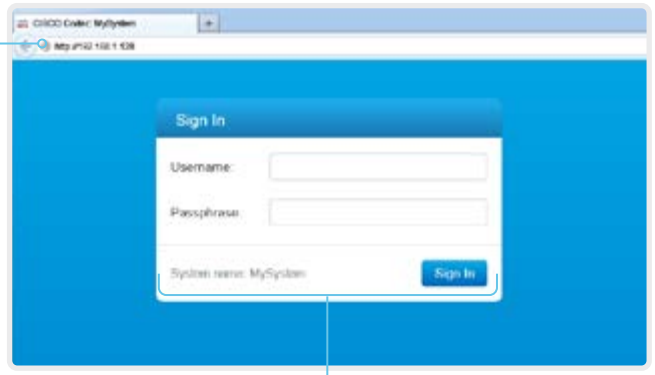
Web インターフェイスは、デバイスの管理ポータルです。コンピュータから接続して、デバイスをリモートで管理できます。フル設定アクセスが提供され、メンテナンス用のツールやメカニズムを利用できます。

注 : ウェブ インターフェイスを使用するには HTTP または HTTPS が有効になっている必要があります ([ネットワークサービス (*NetworkServices*)] > [*HTTP*] > [モード (*Mode*)] 設定を参照) 。

ウェブ ブラウザは最新版を使用することを推奨します。

デバイスへの接続

Web ブラウザを開き、デバイスの IP アドレスをアドレスバーに入力します。



IP アドレスの確認方法

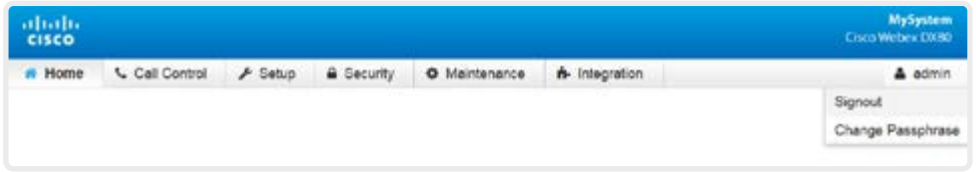
1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [このデバイスについて (*About this device*)] に続き、[設定 (*Settings*)] を選択します。

サインイン

エンドポイントのユーザ名とパスフレーズを入力して、[サインイン (*Sign In*)] をクリックします。

デバイスには、admin というデフォルト ユーザがパスフレーズなしで用意されています。初めてサインインするときは、[パスフレーズ (*Passphrase*)] フィールドを空白のままにします。

admin ユーザのパスワードを設定する必要があります。



サインアウト

ユーザ名の上にカーソルを移動し、ドロップダウンリストから [サインアウト (*Signout*)] を選択します。

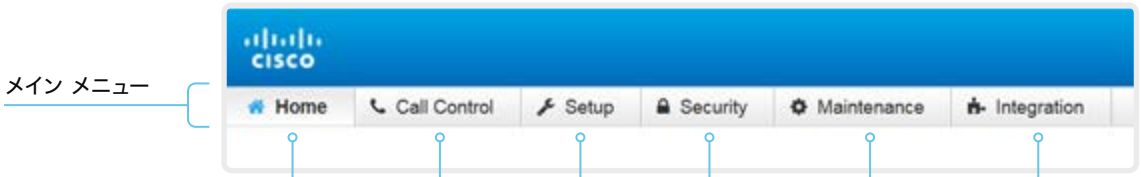
ビデオ会議デバイスの管理方法 (3/4 ページ)

ウェブ インターフェイスの構成

ウェブ インターフェイスは、各サブページから構成されています。デバイスがオンプレミス サービス (CUCM、VCS) に登録されている場合は、以下のすべてのサブページを使用できます。デバイスがシスコのクラウド サービス (Cisco Webex) に登録されている場合は、灰色で示されているページを使用できません。

どちらの場合も、サインインしているユーザには、アクセス権のあるページだけが表示されます。

ユーザ管理、ユーザ ロール、およびアクセス権の詳細については、
► 「ユーザ管理」の章をお読みください。



ホーム (Home)

コール制御 (Call Control)

セットアップ (Setup)
- 設定 (Configuration)
- ステータス (Status)
- 周辺機器 (Peripherals)
- パーソナライゼーション (Personalization)
- お気に入り (Favorites)

セキュリティ (Security)
- ユーザ (Users)
- サービス証明書 (Service Certificates)
- CUCM 証明書 (CUCM Certificates)
- CA
- 強力なセキュリティ モード (Strong Security Mode)
- バナーにサインインする (Sign In Banner)
- 非永続モード (Non-persistent Mode)

メンテナンス (Maintenance)
- 診断 (Diagnostics)
- システム ログ (System Logs)
- 通話履歴 (Call Logs)
- ユーザ インターフェイスのスクリーンショット (User Interface Screenshots)
- ソフトウェア アップグレード (Software Upgrade)
- オプション キー (Option Keys)
- バックアップと復元 (Backup and Restore)
- システム リカバリ (System Recovery)
- 再起動 (Restart)

統合 (Integration)
- UI 拡張エディタ (UI Extensions Editor)
- マクロ エディタ (Macro Editor)
- スタートアップ スクリプト (Startup Scripts)
- 開発者 API (Developer API)

ビデオ会議デバイスの管理方法 (4/4 ページ)

ユーザ インターフェイス上の設定とデバイス情報

デバイス情報および一部の基本設定とデバイス テストには、デバイスのユーザ インターフェイスからアクセスできます。

デバイスの重要な設定と機能 (ネットワーク設定、サービスの有効化、初期設定へのリセットなど) は、パスフレーズで保護できます。► 「[設定 (Settings)] メニューへのアクセスの制限」の章をご覧ください。

一部の設定とテストは、デバイスの電源を初めてオンにしたときに起動するセットアップ アシスタントでも表示されます。セットアップ アシスタントについては、CE ソフトウェアを実行しているデバイスのスタートアップ ガイドをご覧ください。

設定へのアクセス

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [設定 (*Settings*)] を選択します。

   南京錠の記号 は、設定が保護されている (ロックされている) ことを示しています。
3. 変更する設定または実行するテストを選択します。

   設定がロックされている場合は認証ウィンドウが表示され、続行するには ADMIN クレデンシャルでサインインする必要があります。

第 2 章

設定

ユーザ管理

ウェブとコマンドライン インターフェイスにアクセスするには、サインインする必要があります。ユーザには、アクセス権を持つ対象を決める、異なるロールを割り当てることができます。

デフォルトのユーザ アカウント

デバイスには、初期状態でデフォルトの管理者ユーザ アカウントにフル アクセス権が付与されています。ユーザ名は admin で、パスフレーズは初期状態では設定されていません。

必ず admin ユーザのパスフレーズを設定する必要があります。

パスフレーズの設定方法については、► 「デバイス パスフレーズの変更」の章をご覧ください。

新しいユーザ アカウントの作成

1. Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [ユーザ (*Users*)] に移動します。
2. [新規ユーザを追加 (Add New User)] を選択します。.
3. [ユーザ名 (Username)]、[パスフレーズ (Passphrase)]、[パスフレーズの確認 (Repeat passphrase)] の各入力フィールドに入力します。

   デフォルトでは、ユーザが初めてサインインしたときにパスフレーズを変更する必要があります。

   認証にクライアント証明書を使用する場合にのみ、[クライアント証明書 DN (識別名) (Client Certificate DN)] フィールドに値を入力してください。
4. 適切な [ロール (Roles)] チェックボックスをオンにします。
   admin ロールをユーザに割り当てた場合は、[自分のパスフレーズ (Your passphrase)] 入力フィールドに自分自身のパスフレーズを確認のために入力します。
5. ユーザをアクティブにするには、[ステータス (Status)] を [アクティブ (Active)] に設定します。
6. [*ユーザの作成 (Create User)*] をクリックします。

   変更を加えないで終了するには、[戻る (*Back*)] ボタンを使用します。

既存のユーザ アカウントの編集

ADMIN ロールが割り当てられているユーザを変更する場合は 常に、[パスフレーズ (Your passphrase)] 入力フィールドに確認のため各自のパスフレーズを入力する必要があります。

ユーザ特権を変更する

1. Web インターフェイスにサインインし、[セキュリティ (Security)] > [ユーザ (Users)] に移動します。
2. リスト内の該当ユーザをクリックします。
3. ユーザ ロールを選択し、ステータスを [アクティブ (Acitve)] または [非アクティブ (Inactive)] に設定してから、そのユーザが次回ログインしたときにパスフレーズを変更する必要があるかどうかを決定します。

   HTTPS で証明書ログインを使用する場合にのみ、[クライアント証明書 DN (識別名) (Client Certificate DN)] フィールドに値を入力してください。
4. [ユーザの編集 (Edit User)] をクリックして変更内容を保存します。

   変更を加えないで終了するには、[戻る (*Back*)] ボタンを使用します。

パスフレーズを変更する

1. Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [ユーザ (*Users*)] に移動します。
2. リスト内の該当ユーザをクリックします。
3. 該当する入力フィールドに新しいパスフレーズを入力します。
4. [パスフレーズの変更 (Change Passphrase)] をクリックして、変更を保存します。

   変更を加えないで終了するには、[戻る (*Back*)] ボタンを使用します。

ユーザ アカウントを削除する

1. Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [ユーザ (*Users*)] に移動します。
2. リスト内の該当ユーザをクリックします。
3. [ユーザの削除... (*Delete user...*)] をクリックし、プロンプトが表示されたら確定します。

ユーザ ロール

1 つのユーザ アカウントは、1 つのユーザ ロールまたは複数の組み合わせを保持できます。デフォルトの admin ユーザなどの、フル アクセス権を持つユーザ アカウントは、admin、user、audit の各役割も持つ必要があります。

これらはユーザ ロールです。

ADMIN : このロールを持つユーザは、新規ユーザの作成、ほとんどの設定の変更、通話、および連絡先リストの検索ができます。このユーザは監査証明書のアップロードもセキュリティ監査設定の変更も行えません。

USER : このロールを持つユーザはコールの発信と連絡先リストの検索が可能です。このユーザは呼び出し音量の調整や時刻と日付の表示形式の変更など、いくつかの設定を変更できます。

AUDIT: このロールを持つユーザは、セキュリティ監査の設定の変更および監査証明書のアップロードが可能です。

ROOMCONTROL : このロールを持つユーザは、カスタマイズされた UI パネル (室内制御など) を作成できます。このユーザは、UI 拡張エディタおよび対応する開発ツールにアクセスできます。

INTEGRATOR : このロールを持つユーザは、高度な AV シナリオを設定したり、デバイスをサードパーティの機器と統合したりするために必要な設定、コマンド、およびステータスにアクセスできます。このユーザは、カスタマイズした UI パネルを作成することもできます。

デバイス パスフレーズの変更

次の操作を行うには、デバイスのパスフレーズを知っている必要があります。

- ウェブ インターフェイスへのログイン
- コマンドライン インターフェイスへのログインと、使用する

デフォルトのユーザ アカウント

デバイスは、デフォルトのユーザ アカウントにフル アクセス権が付与された状態で提供されます。ユーザ名はadminで、初期状態ではパスフレーズは設定されていません。

デバイス設定へのアクセスを制限するには、デフォルトの admin ユーザにパスフレーズを設定する必要があります。さらに、管理者権限を持つ他のすべてのユーザにもパスフレーズを設定する必要があります。

admin ユーザのパスフレーズが設定されるまでは、デバイス パスフレーズが設定されていないことを示す警告が画面に表示されます。

他のユーザ アカウント

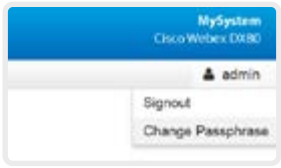
デバイスのユーザ アカウントは複数作成できます。

ユーザ アカウントを作成および管理する方法の詳細については、▶「ユーザ管理」の章を参照してください。

パスフレーズを変更する

1. ウェブ インターフェイスにログインし、ユーザ名の上にマウスを移動し、ドロップダウン リストから [パスフレーズの変更 (*Change Passphrase*)] を選択します。
2. 入力フィールドに現在のパスフレーズと新しいパスフレーズを入力して、[パスフレーズの変更] をクリックします。

   パスフレーズの形式は、0 ～ 64 文字の文字列です。



現在パスフレーズが設定されていない場合は、[現在のパスフレーズ (*Current passphrase*)] フィールドを空白のままにします。

別のユーザのパスフレーズの変更

管理者アクセス権がある場合は、すべてのユーザのパスフレーズを変更できます。

1. Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [ユーザ (*Users*)] に移動します。
2. リスト内の該当ユーザをクリックします。
3. 新しいパスフレーズを、[パスフレーズ (*Passphrase*)] および [パスフレーズの確認 (*Repeat passphrase*)] 入力フィールドに入力します。

   該当ユーザが admin ロールを持っている場合は、[自分のパスフレーズ (Your passphrase)] 入力フィールドに自分自身のパスフレーズを確認のために入力する必要があります。
4. [パスフレーズの変更 (Change Passphrase)] をクリックして、変更を保存します。

   変更を加えないで終了するには、[戻る (*Back*)] ボタンを使用します。

[設定 (Settings)] メニューへのアクセスの制限

デフォルトでは、すべてのユーザがユーザ インターフェイスから [設定 (Settings)] メニューにアクセスできます。

権限のないユーザがデバイスの設定を変更できないようにするために、このアクセスを制限することを推奨します。

[設定 (Settings)] メニューのロック

1. ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。
2. [ユーザインターフェイス (*UserInterface*)] > [設定メニュー (*SettingsMenu*)] > [モード (*Mode*)] に移動して、[ロック (Locked)] を選択します。
3. [保存 (*Save*)] をクリックして変更を有効にします。

   これで、ユーザは、ADMIN クレデンシャルでサインインしないとユーザ インターフェイスでデバイスの重要な設定にアクセスできなくなります。

[設定 (Settings)] メニューのロック解除

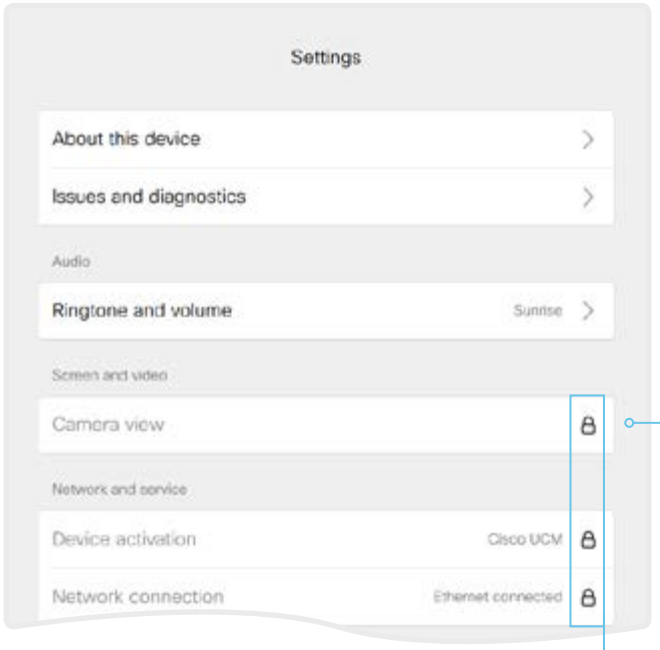
1. ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。
2. [ユーザインターフェイス (*UserInterface*)] > [設定メニュー (*SettingsMenu*)] > [モード (*Mode*)] に移動して、[ロックなし (Unlocked)] を選択します。
3. [保存 (*Save*)] をクリックして変更を有効にします。

   これで、どのユーザでもユーザ インターフェイスの [設定 (Settings)] メニューにアクセスできます。

ユーザ インターフェイスの [設定 (Settings)] メニュー

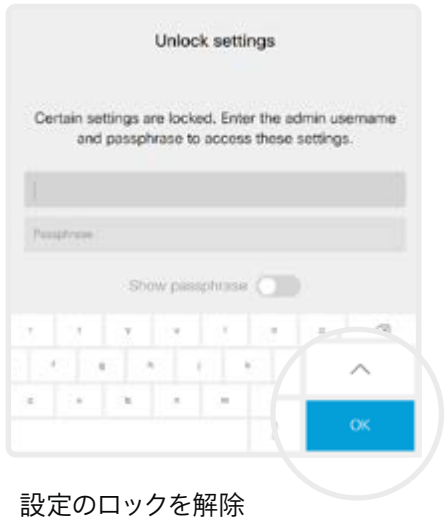
このメニューがロックされている場合は、サインインしないと、デバイスの重要な設定にアクセスできません。

[設定 (*Settings*)] メニューを開くには、ユーザ インターフェイスの上部にあるデバイス名またはアドレスを選択し、[設定 (Settings)] を選択します。



ロックされた設定

ロックされた設定には南京錠のマークが付いています。



設定のロックを解除

南京錠をクリックすると、ADMIN ユーザでサインインするように求められます。

サインインすると、[設定 (Settings)] メニューを閉じるまで、すべての設定にアクセスできます。

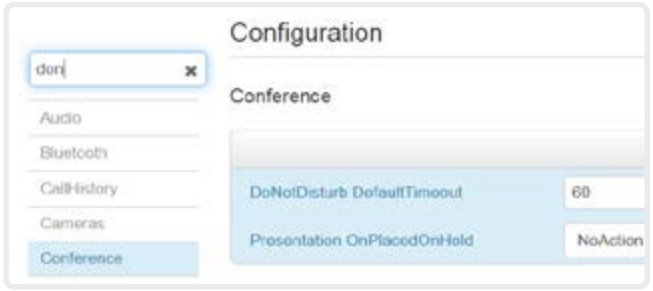
デバイス設定

ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。

デバイス設定の検索

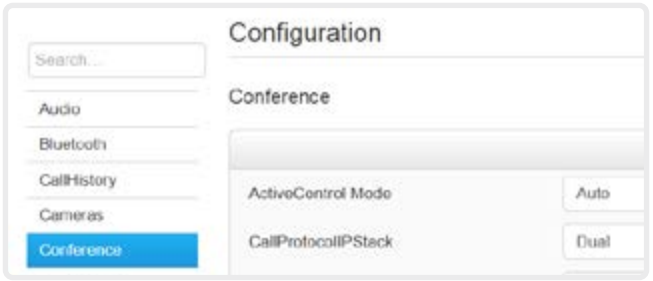
設定を検索する

検索フィールドに必要な数の文字を入力します。これらの文字が含まれているすべての設定が右側のペインに表示されます。値スペースにこれらの文字が含まれている設定も表示されます。



カテゴリを選択して設定に移動する

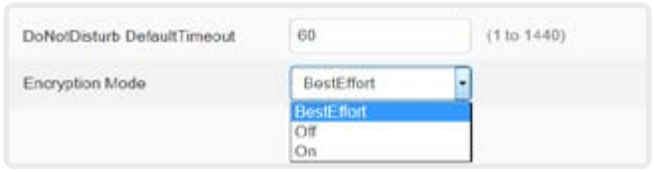
デバイス設定はカテゴリ別にグループ化されています。左側のペインのカテゴリを 1 つ選択して、関連付けられている設定を表示します。



デバイス設定の変更

値スペースを確認する

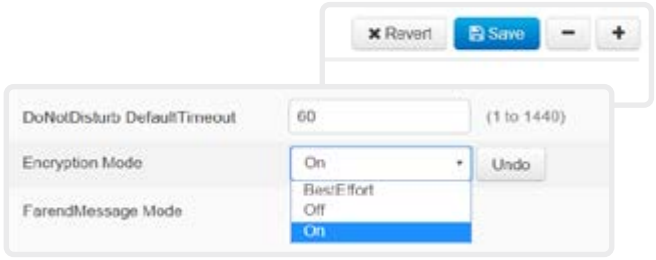
設定の値スペースは、入力フィールドに続くテキストか、矢印をクリックすると開くドロップダウン リストで指定します。



値の変更

1. ドロップダウン リストから望ましい値を選択するか、入力フィールドに新しいテキストを入力します。
2. [保存 (*Save*)] をクリックして変更を有効にします。

   変更しない場合は、[元に戻す (*Undo*)] ボタンまたは [復元 (*Revert*)] ボタンを使用します。



変更が保存されていないカテゴリには、編集記号 ( ) のマークが付きます。

デバイスの設定について

すべてのデバイス設定を Web インターフェイスから変更できます。

個別のデバイス設定については、
▶ 「デバイス設定」の章で説明しています。

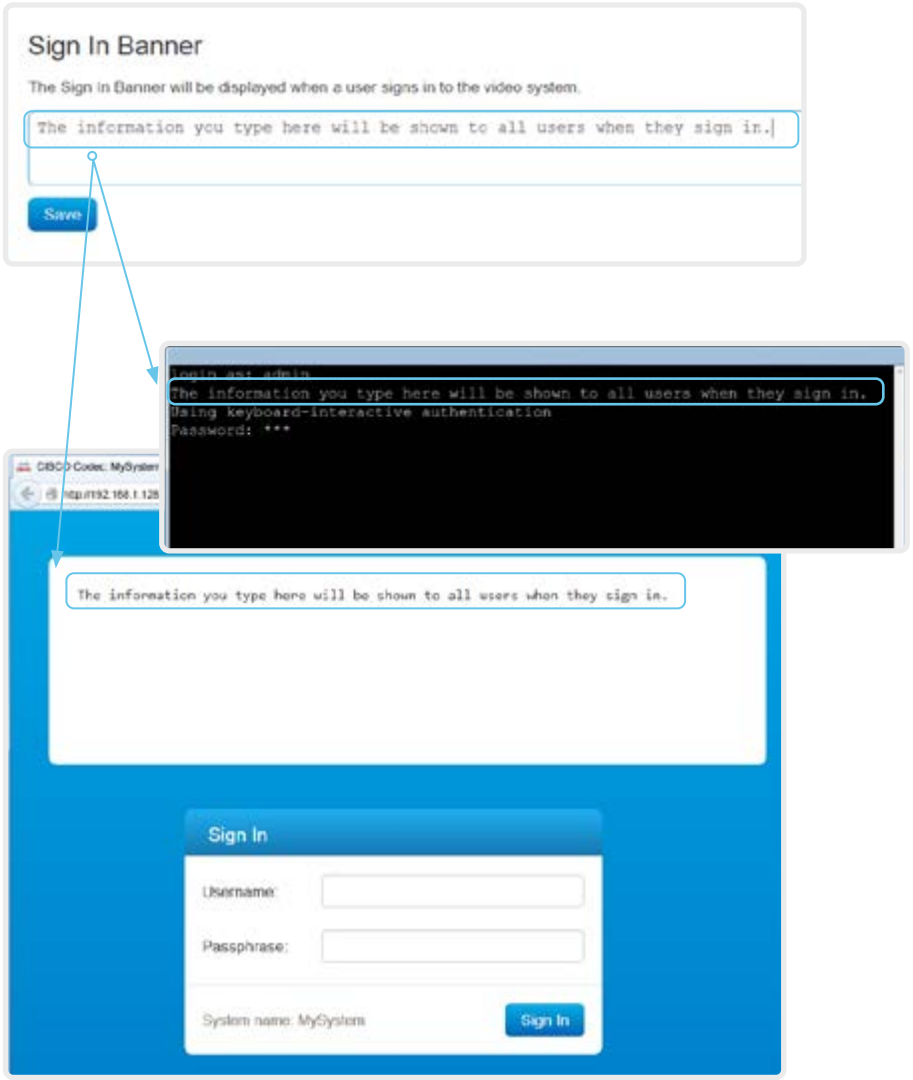
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者がすべてのデバイス設定を変更できるように、管理者にはすべてのユーザ ロールを割り当てる必要があります。

ユーザ管理およびユーザ ロールに関する詳細情報は、▶ 「ユーザ管理」の章で確認できます。

サインイン バナーの追加

Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [サインインバナー (*Sign In Banner*)] に移動します。

1. サインインしたユーザに表示するメッセージを入力します。
2. **[保存 (*Save*)] をクリックしてバナーをアクティブにします。**



サインイン バナーについて

デバイス管理者がすべてのユーザに初期情報を提供する場合に、サインイン バナーを作成できます。メッセージは、ユーザがウェブ インターフェイスまたはコマンドライン インターフェイスにサインインすると表示されます。

最大サイズは 4 kByte です。

ウェルカムバナーとサインインバナーの比較

サインインバナー

- サインインバナーは、ユーザーがウェブインターフェイスまたはコマンドラインインターフェイスにサインインする前に表示されます。

ウェルカムバナー

- ウェルカムバナーは、ユーザーがウェブインターフェイスまたはコマンドラインインターフェイスにサインインした後に表示されます。

ウェルカムバナーの追加

ウェルカムバナーの追加は API コマンドを使用してのみ利用可能です。専用のユーザーインターフェイスは提供されません。

API コマンド

```
xCommand SystemUnit WelcomeBanner Set
```

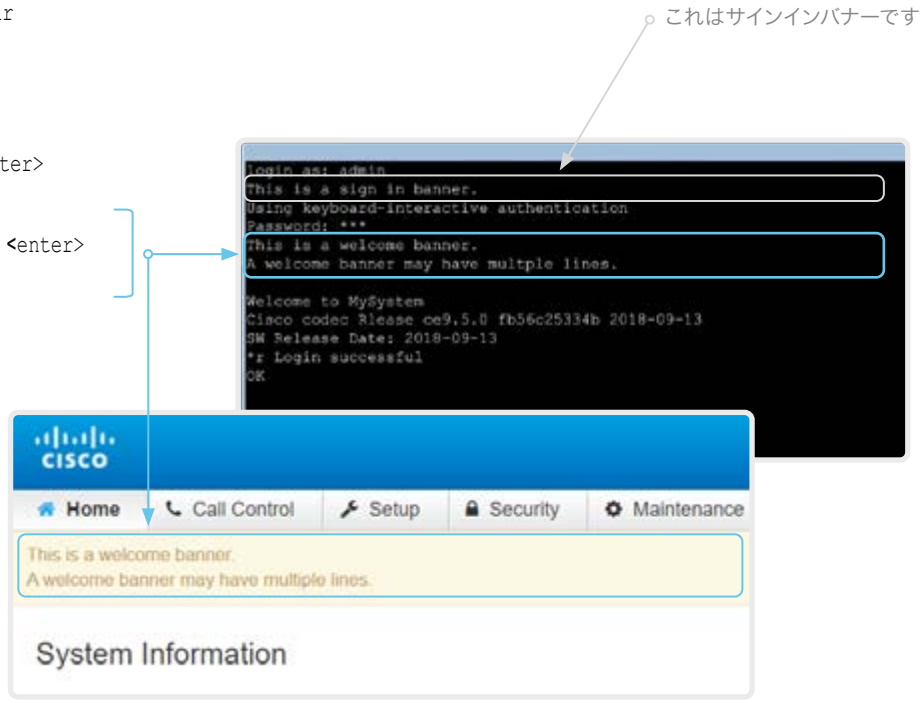
これはマルチライン コマンドです。このコマンド実行後に入力した文字が、コマンドに対する入力となります （改行を含む）。ピリオドを含み改行で終わる別の行を用いて、入力を終了します。

他にもいくつかウェルカムバナーのコマンドが存在します。API ガイドにて詳細をご確認ください。

```
xCommand SystemUnit WelcomeBanner Clear
xCommand SystemUnit WelcomeBanner Get
```

例

```
xCommand SystemUnit WelcomeBanner Set <enter>
これはウェルカムバナーです。<enter>
ウェルカムバナーには複数の行を表示することができます。<enter>
. <enter>
```



ウェルカムバナーについて

デバイスの Web インターフェイスまたはコマンドラインインターフェイスへのサインイン後にユーザーに表示される、ウェルカムバナーを設定できます。バナーには、複数の行を表示することができます。

バナーには、使い始めるうえで必要な情報や、デバイスのセットアップ時に知っておく必要があることなどを記載できます。

最大サイズは 4 kByte です。

ウェルカムバナーとサインインバナーの比較

サインインバナー

- サインインバナーは、ユーザーがウェブインターフェイスまたはコマンドラインインターフェイスにサインインする前に表示されます。

ウェルカムバナー

- ウェルカムバナーは、ユーザーがウェブインターフェイスまたはコマンドラインインターフェイスにサインインした後に表示されます。

デバイスのサービス証明書の管理

ウェブ インターフェイスにサインインして、[セキュリティ (*Security*)] > [サービス証明書 (*Service Certificates*)] に移動します。

次のファイルが必要です。

- 証明書 (ファイル形式 : .PEM)
- 個別のファイルとして、または証明書と同じファイルに含まれる秘密キー (ファイル形式 : .PEM 形式)
- パスフレーズ (秘密キーが暗号化されている場合にのみ必要)

証明書と秘密キーは、デバイス上の同じファイル内に保存されます。

証明書を有効/無効にし、表示、または削除する

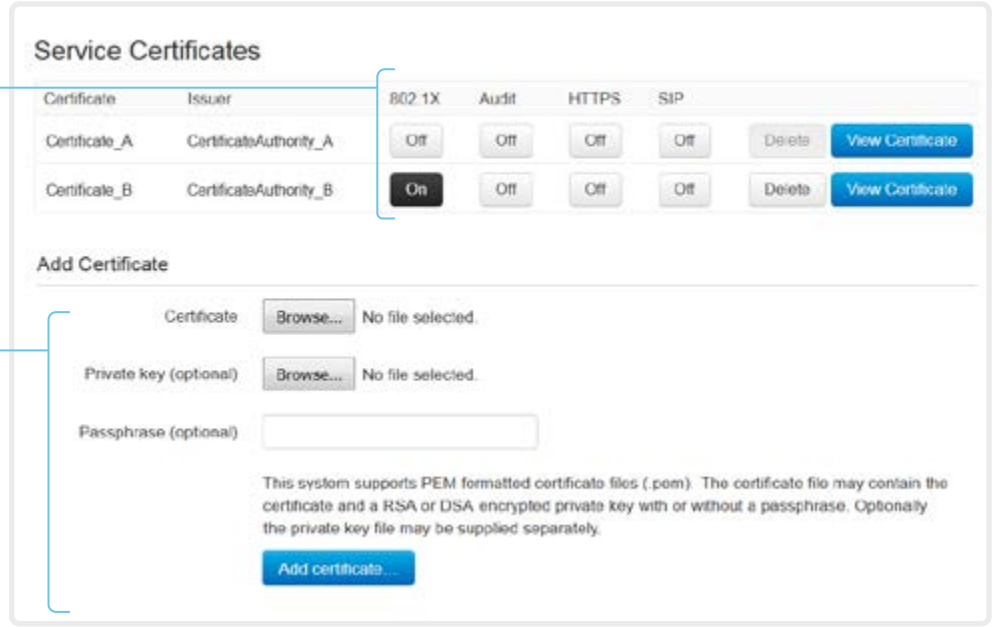
各サービスの証明書を有効または無効にするには、[オン (On)] および [オフ (Off)] ボタンを使用します。

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

証明書の追加

1. [参照 (Browse)] ボタンを押して、コンピュータ上の証明書ファイルと秘密キーファイル (オプション) を見つけます。
2. 必要な場合には [パスフレーズ (*Passphrase*)] に入力します。
3. [証明書の追加... (*Add certificate...*)] をクリックして、証明書をデバイスに保存します。

   有効期間が 10 年以内の証明書のみが受け付けられます。



図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

デバイスのサービス証明書について

証明書の検証は、TLS (Transport Layer Security) を使用する場合に必要になることがあります。

通信が確立される前に、有効な証明書をデバイスから提供するようにサーバまたはクライアントから要求されることがあります。

デバイスの証明書は、デバイスの信頼性を確認するテキスト ファイルです。これらの証明書は、認証局 (CA) によって発行されます。

これらの証明書は、HTTPS サーバ、SIP、IEEE 802.1X、および監査ロギングの各サービスで使用されます。

複数の証明書をデバイスに保存できますが、サービスごとに有効化できる証明書は一度に 1 つだけです。

認証が失敗した場合、接続は確立されません。

信頼できる認証局 (CA) のリストの管理

証明書の検証は、TLS (Transport Layer Security) を使用する場合に必要になることがあります。

通信が確立される前にサーバまたはクライアントに証明書の提供を要求するように、デバイスを設定できます。デバイスは、証明書を使用して、サーバまたはクライアントの信頼性を検証します。認証が失敗した場合、接続は確立されません。

証明書 (テキスト ファイル) は、信頼できる認証局 (CA) によって署名されている必要があります。信頼できる CA からの証明書のリストはデバイス上に保存されています。

CA 証明書リスト

信頼できる CA のリストの確認とメンテナンスは、デバイスの Web インターフェイスから実行できます。

- Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [認証局 (*Certificate Authorities*)] に移動します。CA リストごとにタブが 1 つ存在します。

CA リストは次のとおりです。

- プレインストール : デバイスと通信する外部サーバ (HTTPS、syslog) の証明書を検証するために使用される、プレインストールされた CA 証明書。
- コラボレーションエッジ : デバイスが Cisco Unified Communications Manager (CUCM) によって Expressway を介してプロビジョニングされている場合に、インターネット経由で通信するサーバーの証明書を検証するために使用される、プレインストールされた CA 証明書 (MRA またはエッジとも呼ばれます) 。
- カスタム : 自分でデバイスにアップロードした CA 証明書。ロギングおよびその他の接続で証明書を検証するためには、必要な証明書をすべてプレインストール リストに含める必要があります (まだ含まれていない場合) 。

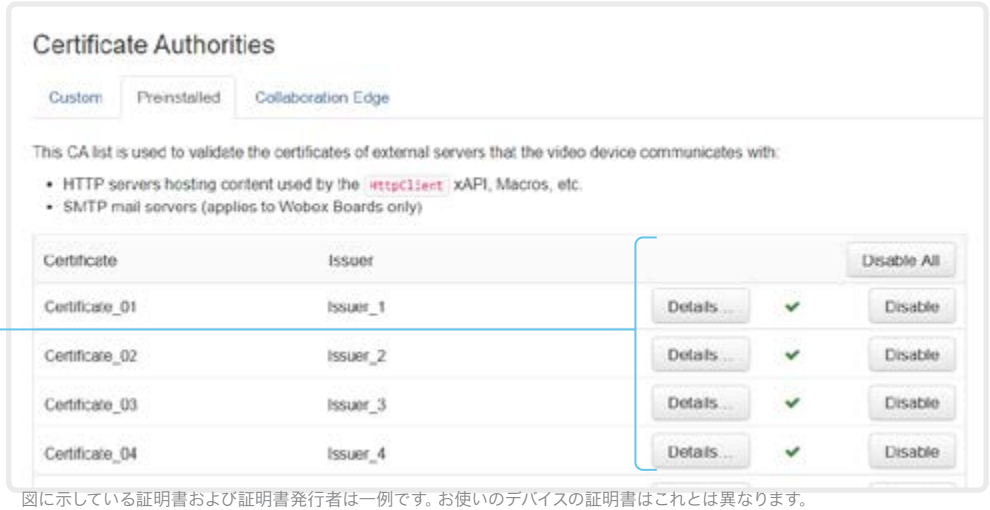
信頼できる認証局 (CA) のリストの管理 (2/4 ページ)

外部サーバ用にプレインストールされた CA 証明書の管理

Web インターフェイスにサインインし、[セキュリティ (Security)] > [認証局 (Certificate Authorities)] に移動して、[プレインストール (Preinstalled)] タブを開きます。

証明書の表示または無効化

証明書を表示または無効にするには、[詳細... (Details...)] ボタンまたは [無効化 (Disable)] ボタンを使用します。



図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

プレインストールされた証明書を使用する代わりに、必要な証明書を手動でカスタム証明書リストに追加することもできます。

信頼できる CA 証明書のリストを更新する方法については、
▶ 「デバイスへの CA 証明書のアップロード」の章をご覧ください。

プレインストールされた CA 証明書

デバイスには、よく使用される CA 証明書のリストがプレインストールされています。デバイスは、通信している外部サーバからの証明書を検証するときに、このリストを使用します。

- HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバー
- プロビジョニング サーバ
- 電話帳サーバ
- syslog サーバ (外部ロギング用)
- Cisco Webex クラウドによって使用されるサーバーおよびサービス

デバイスを初期設定にリセットしても、プレインストールされた証明書のリストは削除されません。

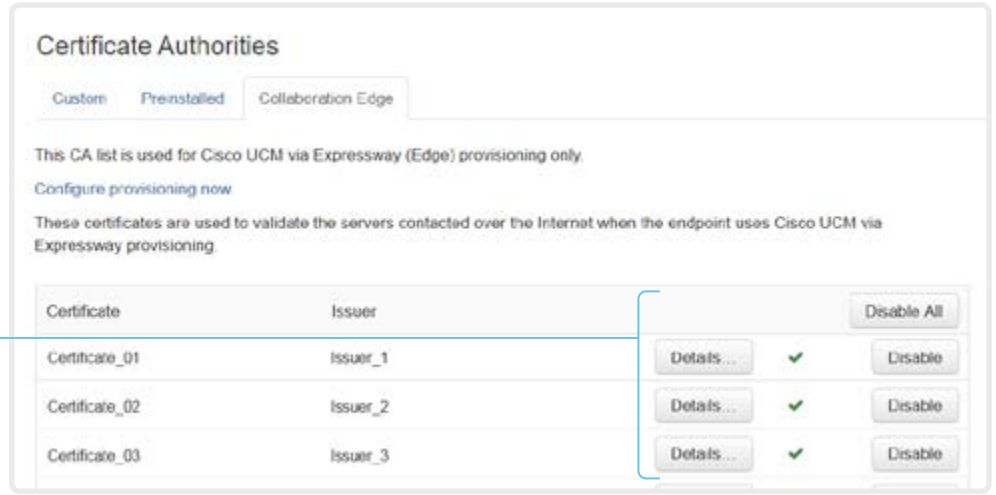
信頼できる認証局 (CA) のリストの管理 (3/4 ページ)

Expressway プロビジョニングを使用する CUCM 用のプレインストール済み CA 証明書の管理

Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [認証局 (*Certificate Authorities*)] に移動して、[コラボレーションエッジ (*Collaboration Edge*)] タブを開きます。

証明書の表示または無効化

証明書を表示または無効にするには、[詳細... (*Details...*)] ボタンまたは [無効化 (*Disable*)] ボタンを使用します。



図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

プレインストールされた証明書を使用する代わりに、必要な証明書を手動でカスタム証明書リストに追加することもできます。

信頼できる CA 証明書のリストを更新する方法については、
▶ 「デバイスへの CA 証明書のアップロード」の章をご覧ください。

Expressway を使用する CUCM 用のプレインストール済み CA 証明書

このリストにあるプレインストール CA 証明書は、デバイスを Cisco Unified Communications Manager (CUCM) によって Expressway 経由でプロビジョニングする場合 (エッジ) にのみ使用されます。

Cisco Expressway インフラストラクチャ証明書のみがこのリストと照合されます。

Cisco Expressway インフラストラクチャ証明書の検証に失敗した場合は、デバイスのプロビジョニングと登録が行われません。

デバイスを初期設定にリセットしても、プレインストールされた証明書のリストは削除されません。

信頼できる認証局 (CA) のリストの管理 (4/4 ページ)

デバイスへの CA 証明書のアップロード

Web インターフェイスにサインインし、[セキュリティ (*Security*)] > [認証局 (*Certificate Authorities*)] に移動して、[カスタム (*Customs*)] タブを開きます。

次のファイルが必要です。

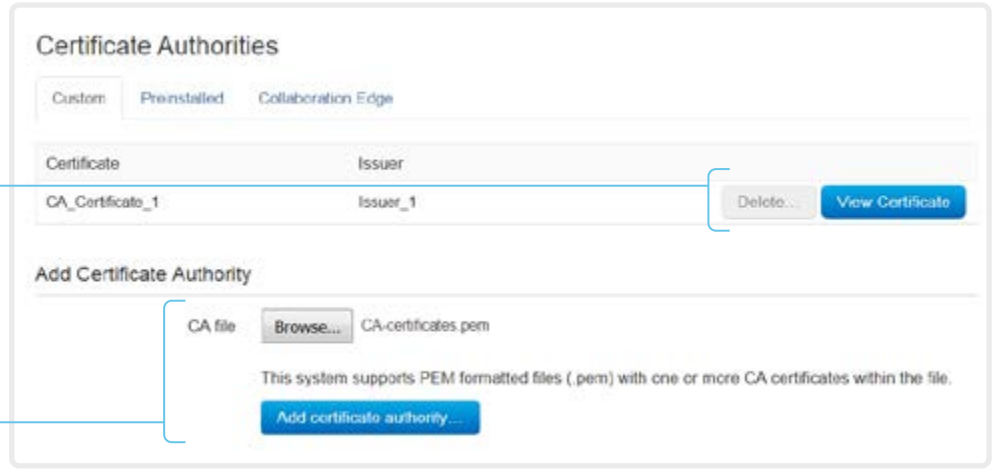
- CA 証明書のリスト (ファイル形式 : .PEM) 。

証明書を表示または削除する

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

CA 証明書のリストのアップロード

1. [参照 (Browse)] ボタンをクリックして、コンピュータから CA 証明書のリストを含むファイル (ファイル形式 : .PEM) を見つけます。
2. [認証局の追加... (*Add certificate authority...*)] をクリックして、新しい CA 証明書をデバイスに保存します。



図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

以前に保存した証明書は自動的には削除されません。

CA 証明書を含む新しいファイル内のエントリが既存のリストに付加されます。

信頼できる CA 証明書のカスタム リストについて

このリストには、自分でデバイスにアップロードした CA 証明書が含まれます。これらの証明書は、クライアント証明書とサーバ証明書の両方について、ロギングおよびその他の接続を検証するために使用できます。

次のものに使用できます。

- HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバー
- プロビジョニング サーバ
- 電話帳サーバ
- SIP サーバ
- syslog サーバ (外部ロギング用)
- Cisco Expressway インフラストラクチャ
- Cisco Webex クラウドによって使用されるサーバーおよびサービス

セキュア監査ロギングのセットアップ

ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。

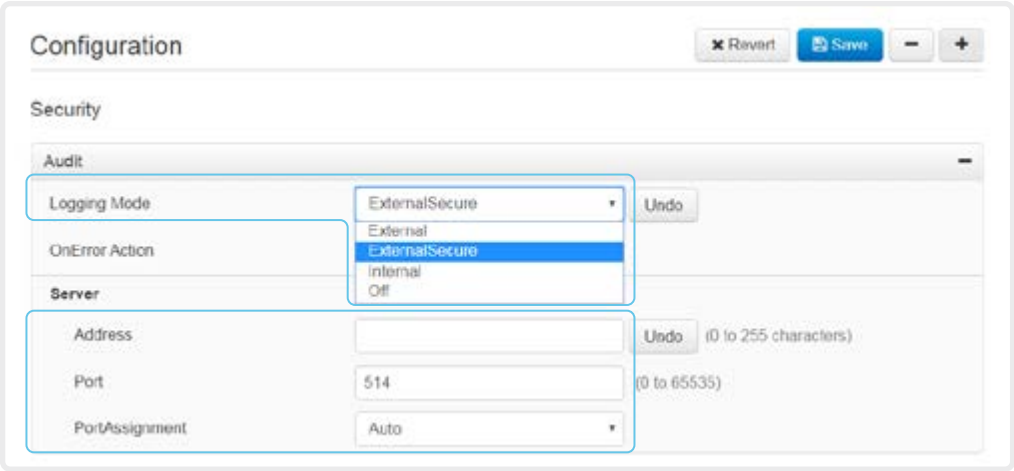
監査サーバの証明書を検証する認証局 (CA) が、デバイスの信頼できる認証局のリストに含まれている必要があります。含まれていない場合は、外部サーバにログが送信されません。

リストの更新方法については、► 「デバイスへの CA 証明書のアップロード」の章を参照してください。

1. [セキュリティ (*Security*)] カテゴリを開きます。
2. [監査 (*Audit*)] > [サーバ (*Server*)] 設定を探して、監査サーバの [アドレス (*Address*)] を入力します。

   [ポート割り当て (*PortAssignment*)] を [手動 (**Manual**)] に設定した場合は、監査サーバの [ポート (*Port*)] 番号も入力する必要があります。

   [監査 (*Audit*)] > [ロギング モード (*Logging Mode*)] を [外部セキュア (ExternalSecure)] に設定します。
3. [保存 (*Save*)] をクリックして変更を有効にします。



安全な監査ロギングについて

監査ロギングを有効にすると、そのデバイスでのすべてのサインイン アクティビティと設定変更が記録されます。

[セキュリティ (*Security*)] > [監査 (*Audit*)] > [ロギング モード (*Logging Mode*)] 設定を使用して、監査ロギングを有効にします。監査ロギングは、デフォルトでは無効になっています。

ExternalSecure 監査ログ モードでは、デバイスは、暗号化された監査ログを外部監査サーバ (syslog サーバ) に送信します。そのサーバの ID は、署名された証明書によって検証される必要があります。

監査サーバの署名は、プレインストールされている CA 証明書またはカスタム CA リストを使用して検証されます。

監査サーバ認証に失敗した場合は、監査ログが外部サーバに送信されません。

CUCM 信頼リストを削除する

この章の情報は、Cisco Unified Communications Manager (CUCM) に登録されているデバイスにのみ関連します。

Web インターフェイスにサインインし、[セキュリティ (Security)] > [CUCM 証明書 (CUCM Certificates)] に移動します。

CUCM 信頼リストを削除する

信頼リストを削除するには、[CTL/ITL の削除 (Delete CTL/ITL)] をクリックします。

一般的に、以前の CTL (証明書信頼リスト) ファイルと ITL (初期信頼リスト) ファイルは削除しません。

次のようなケースでは、これらのファイルを削除する必要があります。

- CUCM の IP アドレスを変更する場合。
- CUCM クラスタ間でエンドポイントを移動する場合。
- CUCM 証明書を再生成または変更する必要がある場合。

信頼リスト フィンガープリントと証明書の概要

信頼リストのフィンガープリントとリストの証明書の概要は、ウェブ ページに表示されます。

この情報は、トラブルシューティングに役立ちます。

信頼リストの詳細

CUCM と信頼リストの詳細については、Cisco のウェブ サイトから入手可能な『Deployment guide for TelePresence endpoints on CUCM』をお読みください。

永続モードを変更する

ウェブ インターフェイスにサインインして、[セキュリティ (*Security*)] > [非永続モード (*Non-persistent Mode*)] に移動します。

永続性ステータスの確認

アクティブなラジオ ボタンは、デバイスの現在の永続性ステータスを示しています。

または、[セットアップ (*Setup*)] > [ステータス (*Status*)] に移動し、[セキュリティ (*Security*)] カテゴリを開いて、[永続性 (*Persistency*)] ステータスを確認することもできます。

永続設定を変更する

すべての永続設定がデフォルトで [永続 (Persistent)] に設定されます。これらの設定は、[非永続 (Non-persistent)] にする場合にのみ変更する必要があります。

1. 設定、通話履歴、内部ロギング、ローカル電話帳 (ローカル ディレクトリとお気に入り) 、および IP 接続 (DHCP) 情報の永続性を設定するには、ラジオ ボタンをクリックします。
2. [保存して再起動... (*Save and restart...*)] をクリックします。

   デバイスが自動的に再起動します。再起動後、新しい永続設定に従って動作が変化します。

非永続モードに切り替える前に保存されたログ、設定および他のデータは、消去されたり削除されたりすることはありません。

永続モード

デフォルトでは、設定、通話履歴、内部ログ、ローカル電話帳 (ローカル ディレクトリとお気に入りリスト) 、および IP 接続情報が保存されます。すべての永続設定は [永続 (**Persistent**)] に設定されているので、デバイスを再起動してもこの情報は削除されません。

通常は、永続設定は変更しないことをお勧めします。[非永続 (**Non-persistent**)] モードへの変更は、前のセッションでログに記録された情報をユーザが参照したりトレースバックしたりしないようにする必要がある場合にのみ行ってください。

非永続モードでは、デバイスが再起動されるたびに次の情報が削除または消去されます。

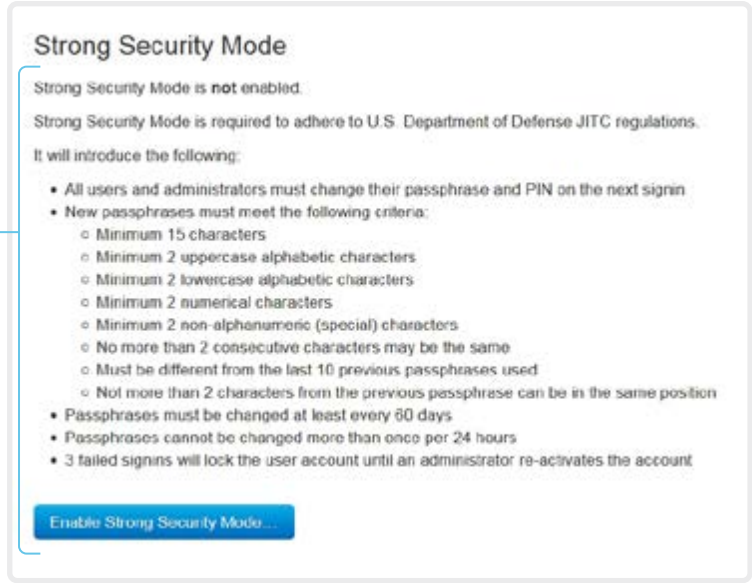
- デバイス設定の変更
- 通話の発信および受信に関する情報 (通話履歴)
- 内部ログ ファイル
- ローカル連絡先またはお気に入りリストの変更
- 前回のセッション以降のすべての IP 関連情報 (DHCP)

[非永続 (Non-persistent)] モードに変更する前に保存された情報は、自動的にクリアまたは削除されることはありません。そのような情報を削除するには、デバイスを初期設定にリセットする必要があります。

初期設定にリセットする方法については、► 「ビデオ会議デバイスの初期設定へのリセット」の章をご覧ください。

強力なセキュリティ モードの設定

1. Web インターフェイスにサインインし、[セキュリティ (Security)] > [強力なセキュリティモード (Strong Security Mode)] に移動します。



強力なセキュリティ モードの設定

続行する前に、強力なセキュリティ モードの影響について注意してお読みください。

1. 強力なセキュリティモードを使用する場合は、[強力なセキュリティモードの有効化... (Enable Strong Security Mode...)] をクリックします。. 表示されるダイアログボックスで選択内容を確認します。

   デバイスが自動的に再起動します。

2. プロンプトが表示されたら、パスフレーズを変更します。新しいパスフレーズは、説明に従って厳格な基準を満たす必要があります。

   デバイスのパスフレーズの変更方法については、 ► 「デバイスパスフレーズの変更」の章をご覧ください。

通常モードに戻る

1. デバイスを通常モードに戻すには、[強力なセキュリティモードの無効化... (Disable Strong Security Mode...)] をクリックします。表示されるダイアログボックスで選択内容を確認します。

デバイスが自動的に再起動します。

強力なセキュリティ モードについて

強力なセキュリティ モードは、DoD JITC 規制への準拠が必要な場合にのみ使用します。

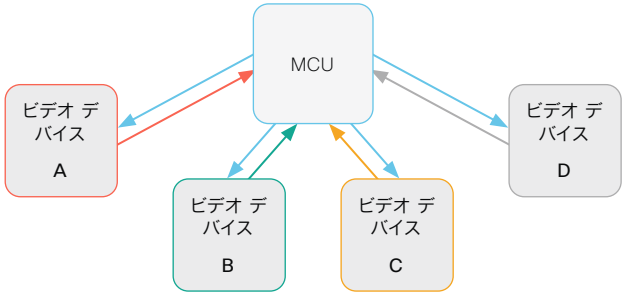
強力なセキュリティ モードでは、非常に厳密なパスフレーズ要件が設定され、すべてのユーザが次回のサインイン時にパスフレーズを変更する必要があります。

アドホック マルチポイント会議のセットアップ (1/2 ページ)

ポイントツーポイントのビデオ コール (2 者間のみのコール) を、より多くの参加者とのマルチポイント会議に拡大する方法はいくつかあります。

集中型会議インフラストラクチャ

ほとんどのソリューションは、一元化された会議インフラストラクチャである MCU (マルチポイントコントロールユニット) [1]を基盤としています。



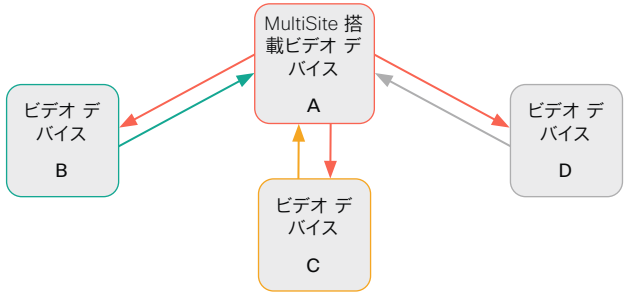
このセットアップでは、ビデオ デバイス A、B、C および D は、4 者会議に参加しています。MCU がすべてのデバイスからのメディア ストリームを受信し、ストリームを処理して、すべてのメディアを他の参加者に送信します。

[1] MCU : マルチポイント コントロール ユニットは、ビデオ会議ゲートウェイまたはビデオ会議ブリッジとも呼ばれます。

ローカル会議リソース - マルチサイト

(SX10、DX70、および DX80 では使用不可)

MultiSite のシナリオでは、ビデオ デバイスのうち 1 台に MCU 機能を担当させます。



このセットアップでは、ビデオ デバイス A、B、C および D は、4 者会議に参加しています。ここではデバイス A で MultiSite 機能を使用し、MCU として機能させます。このデバイスがすべてのデバイスからのメディア ストリームを受信し、ストリームを処理して、すべてのメディアを他の参加者に送信します。

マルチサイトは標準の製品デリバリには含まれていません。デバイスにマルチサイトオプションキーをインストールするには、アップグレードオプションの購入が必要です。

MultiSite でサポートされる参加者の最大数は次のとおりです。

- SX10、DX70、および DX80 : MultiSite サポートなし
- SX80、MX700、および MX800 : 参加者 5 人 (自身を含む) と追加の音声コール 1 つ
- Codec Pro、Room 70 G2 : 参加者 5 人 (自身を含む)
- その他の製品 : 参加者 4 人 (自身を含む)

マルチポイント設定

マルチポイント会議の処理方法を決定するには、[会議 (*Conference*)] > [マルチポイント (*Multipoint*)] > [モード (*Mode*)] 設定を使用します。この設定で使用できる値は次のとおりです。

- Auto
- CUCMMediaResourceGroupList
- MultiSite *(SX10、DX70、DX80 では使用不可)*
- Off *(SX10、DX70、DX80 では使用不可)*

次のページの表で、さまざまな会議オプションについて説明しています。

アドホック マルチポイント会議のセットアップ (2/2 ページ)

会議マルチポイント モード設定	MultiSite オプション キー	リモート デバイス タイプ [2]	参加者を追加する操作	
オフ (Off) [3]	該当なし	MCU	Direct Remote Add	• MCU が [参加者の追加 (*Add Participant*)] をサポートしている場合、UI に [追加 (Add)] ボタンが表示され、次の参加者を直接コールすることができます。新しい参加者がコールを受け入れるとすぐに会議に追加されます。 • MCU が [参加者の追加 (*Add Participant*)] をサポートしていない場合、UI に [追加 (Add)] ボタンは表示されません。
		ビデオ デバイス	Plus one audio	• 音声のみの参加者を 1 人追加できます。 • ビデオでの参加者は追加できません。
CUCM メディア リソースグループ リスト (CUCM-MediaResource-GroupList)	該当なし	ビデオ デバイス	Consultative Add	• CUCM に登録されたデバイスでのみ使用でき、[SIP タイプ (*SIP Type*)] 設定は [シスコ (*Cisco*)] にする必要があります。 • 新しい参加者をコールする間、会議は保留されます。新しい参加者がコールを受け入れると、その新しいコールを会議にマージできます。 • 会議に新しい参加者を最初に追加した参加者だけが、さらに参加者を追加できます。
マルチサイト (MultiSite) [3]	○	該当なし	Local Multisite[4]	• UI に [追加 (*Add*)] ボタンが表示され、次の参加者を直接呼び出すことができます。 • デバイスの上限に達するまで参加者の追加を続けることができます。
	×	該当なし	Plus one audio	• 音声のみの参加者を 1 人追加できます。 • ビデオでの参加者は追加できません。
自動 (Auto)	○	MCU	Direct Remote Add	• MCU が [参加者の追加 (*Add Participant*)] をサポートしている場合、UI に [追加 (*Add*)] ボタンが表示され、次の参加者を直接コールすることができます。新しい参加者がコールを受け入れるとすぐに会議に追加されます。 • MCU が [参加者の追加 (*Add Participant*)] をサポートしていない場合、UI に [追加 (*Add*)] ボタンは表示されません。
		ビデオ デバイス	Local Multisite without cascading[4]	• UI に [追加 (*Add*)] ボタンが表示され、次の参加者を直接呼び出すことができます。 • デバイスの上限に達するまで参加者の追加を続けることができます。 • MultiSite ホスト (MCU として機能しているデバイス) のみが参加者を追加できます。これにより、会議のカスケードを防ぎます。
	×	MCU	Direct Remote Add	• MCU が [参加者の追加 (*Add Participant*)] をサポートしている場合、UI に [追加 (*Add*)] ボタンが表示され、次の参加者を直接コールすることができます。新しい参加者がコールを受け入れるとすぐに会議に追加されます。 • MCU が [参加者の追加 (*Add Participant*)] をサポートしていない場合、UI に [追加 (*Add*)] ボタンは表示されません。
		ビデオ デバイス	Plus one audio	• 音声のみの参加者をさらに 1人追加できます ((SX10、DX70、および DX80 ではサポートされていません) 。 • ビデオでの参加者は追加できません。

[2] リモート デバイス タイプは、Call [n] DeviceType ステータスに表示されます。

[3] SX10、DX70、および DX80 ではサポートされません。

[4] 会議のカスケードを避けるために、Conference Multipoint Mode を **MultiSite** ではなく **Auto** に設定することを推奨します。

コンテンツ共有のためにインテリジェント プロキシミティをセットアップする

Cisco Proximity を使用すると、ユーザは自分のモバイル デバイス（スマートフォン、タブレット、またはラップトップ）がビデオ会議デバイスの近くにある場合に、コンテンツをデバイスで直接表示、制御、キャプチャ、共有することができます。

モバイル デバイスがビデオ会議デバイスから送信される超音波の範囲内に入ると、自動的にビデオ会議デバイスとペアリングできます。

プロキシミティの同時接続数は、ビデオ会議デバイスのタイプによって異なります。この最大接続数に達すると、新しいユーザはクライアントから警告されます。

TV会議本体	最大接続数
Room Kit, Room kit mini	30/7 *
Room Kit、Room 55 Dual、Room 70 、Room 70 G2	30/7 *
Codec Plus、Codec Pro	30/7 *
Board 55/55S、Board 70/70S、Board 85S	30/7 *
SX80	10
SX10, SX20	7
MX700、MX800	10
MX200 G2、MX300 G2	7
DX70、DX80	3

* モバイル デバイス上での共有コンテンツの表示サービスが無効になっている場合、接続数は 30 になります。このサービスが有効になっている場合、接続数は 7 になります。

プロキシミティ サービス

コールの発信とビデオ会議デバイスの制御：

- ダイヤル、ミュート、音量調節、切断
- ラップトップ（OS X と Windows）、スマートフォンとタブレット（iOS と Android）で使用可能

モバイル デバイス上での共有コンテンツの表示：

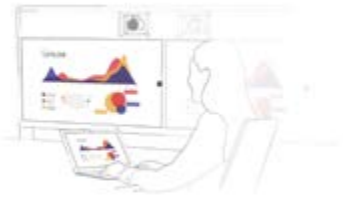
- 共有コンテンツの表示、以前のスライドのレビュー、選択されたスライドの保存
- スマートフォンとタブレット（iOS と Android）で使用可能
- DX70 および DX80 の場合、このサービスは通話時にのみ利用できる

ラップトップからワイヤレスで共有：

- プレゼンテーション ケーブルを接続しないコンテンツの共有
- ラップトップ（OS X と Windows）で使用可能


コールの発信とビデオ会議デバイスの制御


モバイル デバイスでの共有コンテンツの表示


モバイル デバイスからのワイヤレス共有

コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (2/5 ページ)

Cisco Proximity クライアントをインストールする

クライアントの入手場所

スマートフォンとタブレット (Android および iOS) 、およびラップトップ (Windows および OS X) 向けの Cisco Proximity クライアントは、► https://proximity.cisco.com から無償でダウンロードできます

また、Google Play (Android) や Apple App Store (iOS) でスマートフォン/タブレット用のクライアントを直接入手することもできます。

エンド ユーザ ライセンス契約書

次のページのエンド ユーザ ライセンス契約書をよくお読みください。

► https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html [英語]

サポートされるオペレーティング システム

- iOS 7 以降
- Android 4.0 以降
- Mac OS X 10.9 以降
- Windows 7 以降
- Windows 8 で導入されたタイル ベースのインターフェイスはサポートされていません。

コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (3/5 ページ)

超音波の放出

シスコのビデオ会議デバイスは、プロキシミティ機能の一部として超音波を発します。

[プロキシミティ (Proximity)] > [モード (Mode)] 設定を使用して、プロキシミティ機能 (および超音波の放出) の **[オン (On)]/[オフ (Off)]** を切り替えます。

業務用または商用アプリケーション、家電製品など、ほとんどの人は毎日さまざまな環境で、程度の差はあれ超音波にさらされています。

人によっては空中の超音波によって何らかの影響を自覚する場合もありますが、75 dB 未満のレベルで影響が生じることはほとんどありません。

Room 70、Room 70 G2、Room 55、Room 55 Dual、Room Kit、Room Kit Mini、Room Kit Plus、SX10N および MX シリーズ:

- スピーカーから 50 cm 以上の距離では、超音波の音圧レベルは 75 dB 未満になります。

DX70 および DX80:

- スピーカーから 20 cm 以上の距離では、超音波の音圧レベルは 75 dB 未満になります。

Board:

- 画面から 20 cm 以上の距離では、超音波の音圧レベルは 75 dB 未満になります。

  Board 50 および 70 (S シリーズ以外) の場合、スピーカーが下向きのため、画面の真下ではレベルが若干高くなることがあります。

Codec Plus、Codec Pro、SX10、SX20 および SX80:

- これらのビデオ会議デバイスでは、サードパーティのスピーカーで超音波が放出されるため、超音波の音圧レベルを予測できません。

  スピーカー自体の音量コントロール、および [音声 (Audio)] > [超音波 (Ultrasound)] > [最大音量 (MaxVolume)] での設定は、超音波の音圧レベルに影響を与えます。リモートコントロールまたはタッチコントローラでの音量調節は効果ありません。

ヘッドセット

DX70、DX80、および SX10N:

これらのデバイスでは、次の理由からヘッドセットを常に使用できます。

- DX70 および DX80 には、超音波を出さない専用ヘッドセット出力があります。
- SX10N では、内蔵スピーカーで超音波が放出されます。超音波は、HDMI またはオーディオ出力では放出されません。

Room 70、Room 70 G2、Room 55 Dual、Room Kit Plus、Codec Plus、Codec Pro、Board、SX10、SX20、SX80、および MX シリーズ:

- これらのデバイスは、ヘッドセットを使用するように設計されていません。

  これらのビデオ会議デバイスでヘッドセットを使用する場合は、超音波の送出をオフにしておくことを強くお勧めします ([プロキシミティ (Proximity)] > [モード (Mode)] を [オフ (**Off**)] に設定します)。この場合、[プロキシミティ (Proximity)] 機能を使用することはできません。
- これらのデバイスは専用のヘッドセット出力を備えていないため、接続されたヘッドセットから音圧レベルを制御することはできません。

Room 55、Room Kit、Room Kit Mini:

- これらのデバイスでは、USB 出力にいつでもヘッドセットを接続できます。この出力から超音波が送出されることはありません。
- Room 55 および Room Kit のオーディオライン出力 (ミニジャック) は、ヘッドセット向けには設計されていません。これらの出力のいずれかに接続されているヘッドセットから音圧レベルを制御することはできません。

  ヘッドセットをオーディオライン出力に接続する場合は、超音波の送出をオフにしておくことを強くお勧めします ([プロキシミティ (Proximity)] > [モード (Mode)] を [オフ (**Off**)] に設定します)。この場合、[プロキシミティ (Proximity)] 機能を使用することはできません。

コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (4/5 ページ)

プロキシミティ サービスを有効にする

1. ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。
2. [プロキシミティ (Proximity)] > [モード (Mode)] に移動して、Proximity を **[オン (On)]** にします。

   ビデオ会議デバイスが、超音波のペアリング メッセージの送信を開始します。

   許可するサービスを有効にします。デフォルトでは、[デスクトップ クライアントからのワイヤレス共有 (Wireless share from a desktop client)] のみが有効になっています。

   プロキシミティ機能を最大限に活用するために、すべてのサービスを有効にすることをお勧めします。

   コールの発信とビデオ会議デバイスの制御 :

   - [プロキシミティ (Proximity)] > [サービス (Services)] > [通話制御 (CallControl)] に移動して、**[有効 (Enabled)]** を選択します。

   モバイル デバイス上での共有コンテンツの表示 :

   - [プロキシミティ (Proximity)] > [サービス (Services)] > [コンテンツ共有 (ContentShare)] > [送信先クライアント (ToClients)] に移動して、**[有効 (Enabled)]** を選択します。

   デスクトップ クライアントからのワイヤレス共有 :

   - [プロキシミティ (Proximity)] > [サービス (Services)] > [コンテンツ共有 (ContentShare)] > [クライアントから (FromClients)] に移動して、**[有効 (Enabled)]** を選択します。

プロキシミティ インジケータ

1 つ以上の Proximity クライアントがデバイスとペアリングされていると、画面にプロキシミティ インジケータが表示されます。

最後のクライアントのペアリングが解除されても、インジケータはすぐには消えません。消えるまで数分かかることがあります。

プロキシミティについて

DX 製品は複数のデバイスが互いに近くにある、間仕切りのない広々としたオフィスに配置されることが多いため、プロキシミティ機能はデフォルトで [オフ (**Off**)] になっています。このような環境では、ペアリングが不安定になる可能性があります。プロキシミティは、通常 1 部屋につき 1 つのデバイス上でだけ[オン (On)] にしてください。

[プロキシミティ (Proximity)] を [オン (**On**)] にすると、ビデオ会議デバイスから超音波のペアリング メッセージが発信されます。

超音波のペアリング メッセージは、Proximity クライアントがインストールされた近くにあるデバイスによって受信され、デバイスの認証および許可をトリガーします。

プロキシミティがご使用の 環境, に適していることを確認した場合は、最適なユーザ エクスペリエンスを実現するために、プロキシミティを常に [オン (**On**)] **にしておくことを推奨します。**

プロキシミティに対する完全なアクセス権限を得るためには、プロキシミティ サービス ([プロキシミティ (*Proximity*)] > [サービス (*Services*)] > [...]) も [有効 (**Enabled**)] にする必要があります。

コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (5/5 ページ)

プライバシーについて

Cisco Privacy ポリシーと Cisco Proximity 付録には、クライアントにおけるデータ収集とプライバシーの懸案事項が記載されており、この機能を組織に導入する際にはこれを考慮する必要があります。次のページを参照してください。► https://www.cisco.com/web/siteassets/legal/privacy.html

また、ビデオ会議デバイスが通話中に、室内の各モバイル デバイスではコンテンツの受信および表示のみを行えることに注意してください。

基本的なトラブルシューティング

プロキシミティ クライアントを使用するデバイスを検出できない

- 一部の Windows ラップトップでは、超音波の周波数範囲 (20kHz-22kHz) の音を記録できません。これは、特定のデバイスのサウンドカード、サウンド ドライバ、または内蔵マイクに関する周波数の制限が原因である可能性があります。詳細については、サポート フォーラムを参照してください。
- ユーザ インターフェイスで [設定 (*Settings*)] > [問題と診断 (*Issues and diagnostics*)] を確認するか、ビデオ会議デバイスの Web インターフェイスで [メンテナンス (*Maintenance*)] > [診断 (*Diagnostics*)] を確認します。超音波に関する問題がリストに記載されていない場合 ([超音波信号を確認できません (Unable to verify the ultrasound signal)]) 、超音波のペアリング メッセージがビデオ会議デバイスから発信されます。クライアントで検出される問題のサポートには、プロキシミティのサポート掲示板を参照してください。

オーディオ アーチファクト

- ハムノイズやクリッピングノイズなどが聞こえる場合は、最大超音波音量を下げてください ([オーディオ (*Audio*)] > [超音波 (*Ultrasound*)] > [最大音量 (*MaxVolume*)]) 。

ラップトップから内容を共有できない

- コンテンツ シェアリングを機能させるには、ビデオ会議デバイスとラップトップを同じネットワーク上に配置する必要があります。この理由から、ビデオ会議デバイスが Expressway 経由で企業ネットワークに接続されており、ラップトップが VPN 経由 (VPN クライアント依存) で接続されている場合には、プロキシミティ シェアリングが失敗する可能性があります。

その他のリソース

Cisco Proximity のサイト:

► https://proximity.cisco.com

サポート フォーラム:

► https://www.cisco.com/go/proximity-support

ビデオ品質の対コール レート比調整

ビデオ入力品質の設定

ビデオをエンコードして送信する場合は、高解像度（シャープさ）と高フレーム レート（動き）との間でトレード オフが生じます。

最適鮮明度設定を有効にするには、Video Input Connector n Quality 設定を [モーション (Motion)] に設定する必要があります。ビデオ入力の品質を [シャープネス (Sharpness)] に設定すると、エンドポイントはフレーム レートに関係なく、可能な限り高解像度で送信します。

最適鮮明度プロファイル

最適鮮明度プロファイルは、ビデオ会議室の光（照明）の条件およびカメラ（ビデオ入力ソース）の品質を反映している必要があります。光の条件およびカメラの品質が良いほど、高いプロファイルを使用する必要があります。

通常、[中 (Medium)] プロファイルが推奨されます。ただし照明条件が非常に良好な場合は、プロファイルを決定する前に、さまざまな最適鮮明度プロファイル設定でエンドポイントをテストすることをお勧めします。特定の帯域の解像度を上げるために、[高 (High)] プロファイルを設定できます。

異なる最適鮮明度プロファイルに使用する標準的な解像度、帯域、および送信フレーム レートの一部を表に示します。解像度とフレーム レートは、発信側と着信側の両方のデバイスでサポートされている必要があります。

ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。

1. [ビデオ (*Video*)] > [入力 (*Input*)] > [コネクタ n (*Connector n*)] > [品質 (*Quality*)] を選択して、ビデオ品質パラメータを [モーション (Motion)] に設定します (Connector 1 (内蔵カメラ) ではこの手順をスキップします) 。
2. [ビデオ (*Video*)] > [入力 (*Input*)] > [コネクタ n (*Connector n*)] > [最適鮮明度 (*OptimalDefinition*)] > [プロファイル (*Profile*)] に移動して、適切な最適鮮明度プロファイルを選択します。

解像度とフレーム レート [w×h@fps] は、異なる最適な定義プロファイルとコール レートから取得します。

コール レート (kbps)	H.264、最大 30fps		
	標準	中	高
128	320 × 180 @ 30	512 × 288 @ 20	512 × 288 @ 30
160	512 × 288 @ 20	512 × 288 @ 30	640 × 360 @ 30
256	512x288 @ 30	640x360 @ 30	768x448@30
384	640x360 @ 30	768x448@30	768x448@30
512	768x448@30	1024x576@30	1024x576@30
576	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30
768	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30
1152	1280x720@30	1280x720@30	1280x720@30
1472	1280x720@30	1280x720@30	1920x1080@30
1920	1280x720@30	1920x1080@30	1920x1080@30
2560	1920x1080@30	1920x1080@30	1920x1080@30
3072	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30

画面に企業ブランディングを追加 (1/2 ページ)

Web インターフェイスにサインインし、[セットアップ (*Setup*)] > [パーソナライゼーション (*Personalization*)] に移動して、[ブランディング (*Branding*)] タブを開きます。

このページから、独自のブランディング要素 (背景ブランド画像、ロゴ、カスタム メッセージ) をビデオ会議デバイスに追加できます。

アウェイク状態のブランディング

アウェイク状態では、次のことができます。

- 右下隅にロゴを追加する
- 左下隅に短いメッセージ (テキストのみ) を追加する

推奨事項:

- 黒色のロゴ (デバイスでは不透明度が 40 % の白色のオーバーレイが追加されるため、ロゴおよびその他のユーザ インターフェイス要素が映えます)
- 背景が透明な PNG 形式
- 最小 272 × 272 ピクセル (自動的にスケーリングされます)

ブランディングについて

この章で説明しているように、ブランディング機能により、シスコの全体的なユーザ エクスペリエンスを損なうことなく、画面の表示をカスタマイズできます。

従来のカスタム壁紙機能ではなく、この機能を使用することをお勧めします。カスタム壁紙機能を使用すると、ワンボタン機能などの機能を使用できなくなります。

ブランド機能とカスタム壁紙は、同時に使用できません。

デバイスでカスタム壁紙がセットアップされている場合は、ブランディング要素を追加する前に [カスタム壁紙を無効にする (*Disable the custom wallpaper*)] をクリックする必要があります。

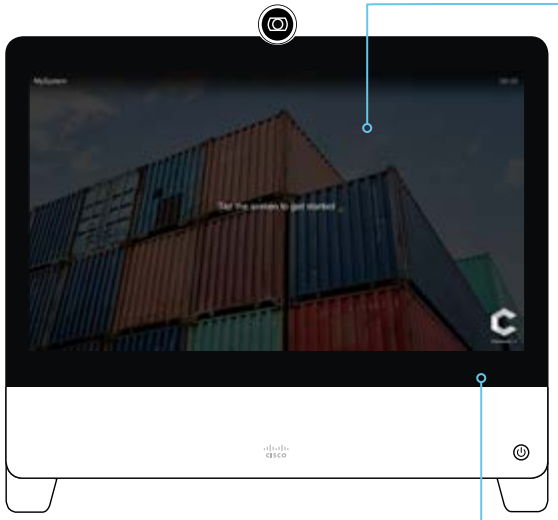
画面に企業ブランディングを追加 (2/2 ページ)

ハーフウェイク状態のブランディング

ハーフウェイク状態では、次のことができます。

- 背景のブランド イメージを追加する
- 右下隅にロゴを追加する
- スクリーン中央のメッセージをカスタマイズまたは削除します。これは、デバイスの使用開始方法をユーザに示すメッセージです。

  通常は標準メッセージのままにすることをお勧めします。サードパーティのユーザ インターフェイスがある場合など、別のシナリオに合わせる必要がある場合にのみ、メッセージを変更してください。



背景ブランド イメージ

- デバイスが復帰するときに、画像がフルカラーで表示され、数秒後に自動的に淡色表示になります（透明な黒色のオーバーレイ）
- イメージの形式：PNG または JPEG
- 推奨サイズ： 1920 × 1080 ピクセル

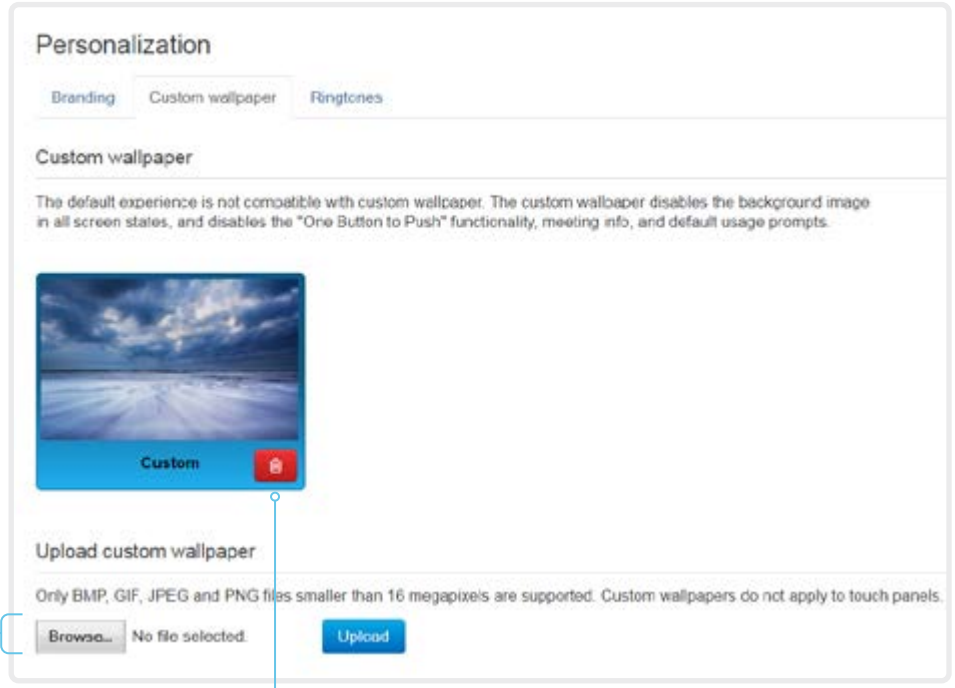
ロゴ

推奨事項：

- 白色のロゴ（暗い背景ブランド イメージに適合する）
- 背景が透明な PNG 形式
- 最小 272 × 272 ピクセル

カスタム壁紙の追加

Web インターフェイスにサインインし、[セットアップ (*Setup*)] > [パーソナライゼーション (*Personalization*)] に移動して、[カスタム壁紙 (*Custom wallpaper*)] タブを開きます。



カスタムの壁紙のアップロード

古いカスタム壁紙があれば上書きします。

1. [参照 (Browse)] ボタンを押して、カスタム壁紙のイメージ ファイルを見つけます。
2. [アップロード (*Upload*)] をクリックして、ファイルをデバイスに保存します。

   サポートされるファイル形式 : BMP、GIF、JPEG、PNG

   最大ファイル サイズ : 16 メガピクセル

カスタム壁紙をアップロードすると、自動的にアクティブになります。

カスタムの壁紙の削除

[削除 (Delete)] をクリックすると、カスタム壁紙がデバイスから完全に削除されます。

削除したカスタムの壁紙を再度使用する場合は、その壁紙を再度アップロードする必要があります。

カスタム壁紙について

カスタム画像をスクリーンの背景にする場合は、カスタム壁紙をアップロードして使用することができます。カスタム壁紙はタッチ コントローラには表示されません。

デバイスには一度に 1 枚のカスタム壁紙しか保存できません。以前のカスタム壁紙は新しいカスタム壁紙で上書きされます。

この従来のカスタム壁紙機能ではなく、新しいブランディング機能を使用することをお勧めします。それにより、Cisco の全体的なユーザ エクスペリエンスが向上し、ワンボタン機能や会議情報などの機能が使用できなくなることを回避できます。「画面に企業ブランディングを追加」の章を参照してください。

ブランド機能とカスタム壁紙は、同時に使用できません。

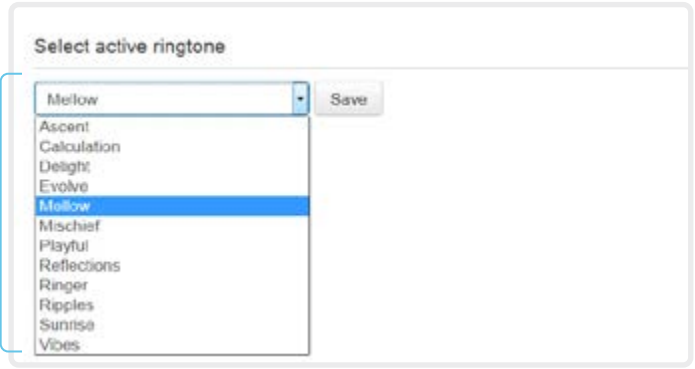
デバイスでブランディング要素がセットアップされている場合は、カスタム壁紙を追加する前に [ブランディングなしで続行 (Continue without branding)] をクリックする必要があります。

着信音の選択と着信音量の設定

Web インターフェイスにサインインし、[セットアップ (*Setup*)] > [パーソナライゼーション (*Personalization*)] に移動して、[着信音 (*Ringtones*)] タブを開きます。

呼び出し音の変更

1. ドロップダウン リストから呼び出し音を選択します。
2. [保存 (*Save*)] をクリックすると、それがアクティブな呼び出し音になります。



呼び出し音の音量の設定

呼び出し音の音量を調節するにはスライド バーを使用します。

呼び出し音の再生

呼び出し音を再生するには、再生ボタン (▶) をクリックします。

再生を終了するには、停止ボタン (■) を使用します。

着信音について

デバイスには着信音一式がインストールされています。着信音を選択して音量を設定するには、ウェブ インターフェイスを使用します。

ウェブ インターフェイスから、選択した呼び出し音を再生できます。呼び出し音が再生されるのはデバイス上であり、Web インターフェイスが実行されているコンピュータ上ではないことに注意してください。

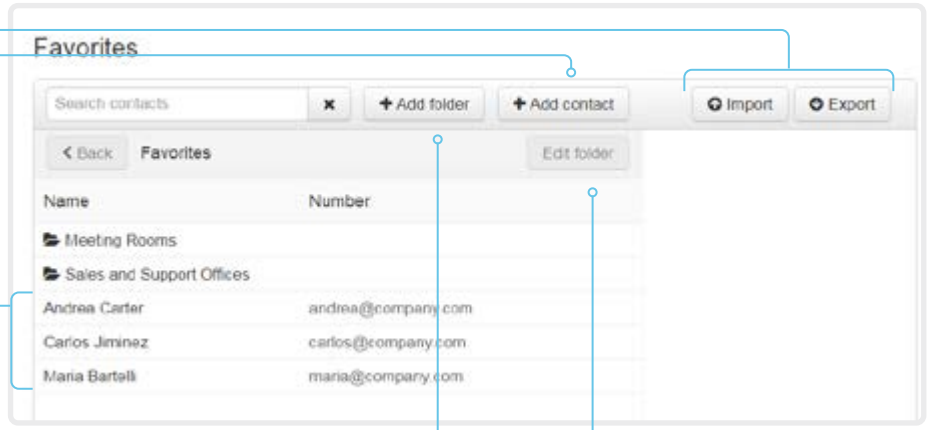
お気に入りリストの管理

ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [お気に入り (*Favorites*)] に移動します。

ファイルから連絡先をインポート/エクスポート

ローカルの連絡先をファイルに保存するには [エクスポート (*Export*)] をクリックし、ファイルから連絡先を取得するには [インポート (*Import*)] をクリックします。

ファイルから新しい連絡先をインポートすると、現在のすべてのローカル連絡先は破棄されます。



連絡先を追加または編集する

1. [連絡先の追加 (*Add contact*)] をクリックして新しいローカル連絡先を作成するか、連絡先の名前をクリックしてから [連絡先を編集 (*Edit contact*)] をクリックします。
2. ポップアップ表示されたフォームに値を入力するか、そのフォームを更新します。

   連絡先をサブフォルダに保存するために、フォルダ ドロップダウン リストでフォルダを選択します。

   連絡先に関する複数の連絡方法 (ビデオ アドレス、電話番号、携帯番号など) を保存する場合は、[連絡方法の追加 (*Add contact method*)] をクリックして、新しい入力フィールドに値を入力します。
3. [保存 (*Save*)] をクリックしてローカル連絡先を保存します。

コンタクトの削除

1. [連絡先を編集 (*Edit contact*)] に続いて連絡先の名前をクリックします。
2. [削除 (*Delete*)] をクリックしてローカル連絡先を削除します。

サブフォルダを追加または編集する

1. [フォルダの追加 (*Add folder*)] をクリックして新しいサブフォルダを作成するか、一覧表示されたフォルダの 1 つをクリックしてから [フォルダの編集 (*Edit folder*)] をクリックします。
2. ポップアップ表示されたフォームに値を入力するか、そのフォームを更新します。
3. [保存 (*Save*)] をクリックしてフォルダを作成または更新します。

サブフォルダを削除する

1. フォルダの名前をクリックし、[フォルダの編集 (*Edit folder*)] をクリックします。
2. フォルダとそのすべてのコンテンツおよびサブ フォルダを削除するには、[削除 (*Delete*)] をクリックします。ポップアップするダイアログで選択内容を確認します。

デバイスのユーザ インターフェイスによるお気に入りの管理

お気に入りリストへの連絡先の追加

1. ホーム画面の [発信 (Call)] を選択します。
2. 追加する連絡先を選択します。
3. 連絡先カードの [発信 (Call)] ボタンの下に表示されている 3 つの点を選択します。
4. [お気に入りに設定 (Mark as Favorite)] を選択します。

追加した連絡先は、最上位のフォルダに格納されます。サブフォルダを選択または作成することはできません。

お気に入りリストからの連絡先の削除

1. ホーム画面の [発信 (Call)] を選択します。
2. [お気に入り (Favorites)] タブを選択します。
3. 削除する連絡先を選択します。
4. 連絡先カードの [発信 (Call)] ボタンの下に表示されている 3 つの点を選択します。
5. [お気に入り設定を解除 (Unmark as favorite)] を選択します。

アクセシビリティ機能のセットアップ

着信時のスクリーンの点滅

聴覚に障がいのあるユーザが着信に気付きやすくするために、着信時にスクリーンが赤色と灰色で点滅するようにセットアップできます。

1. ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。
2. [ユーザインターフェイス (UserInterface)] > [アクセシビリティ (Accessibility)] > [着信コール通知 (IncomingCallNotification)] に移動して、**[画面表示の強調 (AmplifiedVisuals)]** を選択します。
3. [Save (保存)] をクリックします。

CUCM からの製品固有の設定のプロビジョニング (1/2 ページ)

この章では、Cisco UCM リリース 12.5(1)SU1 で導入された手法を使用して、設定やパラメータをデバイス (エンドポイント) にプロビジョニングする方法について説明します。

Cisco UCM リリース 12.5(1)SU1 より前のリリースでは、UCM からデバイスにプッシュできるのは製品固有の設定の一部だけに限定されていました。それ以外のすべての設定については、管理者が Cisco TMS またはデバイスの Web インターフェイスを使用する必要がありました。

CUCM リリース 12.5(1)SU1 以降では、CUCM からプロビジョニングできる設定またはパラメータが増えました。設定のリストは、デバイス上でユーザに表示される内容 (パブリック xConfiguration) と一致しますが、ネットワーク、プロビジョニング、SIP、および H.323 の設定は例外です。

CUCM の詳細については、► 『Cisco Unified Communications Manager リリース 12.5(1)SU1 機能設定ガイド』 [英語] の「Video Endpoints Management (ビデオ エンドポイント管理) 」の章をご覧ください。

設定制御モード

管理者は、導入のニーズに基づいて、CUCM 管理インターフェイスでさまざまな設定制御モードを構成できます。設定を CUCM とデバイスのどちらから制御するか、または両方を使用して制御するかを決定できます。

次のように、さまざまな設定制御モードがあります。

- **Unified CM とエンドポイント** (Unified CM and Endpoint) (デフォルト) : CUCM とデバイスを、デバイス データをプロビジョニングするためのマルチマスター ソースとして動作させる場合は、このモードを使用します。CUCM はデバイスから自動的に xConfiguration データを読み取ります。デバイスでローカルに行われた更新は、即座に CUCM サーバに同期されます。
- **Unified CM**: CUCM が、デバイス データをプロビジョニングするための集中管理型マスター ソースとして動作します。CUCM は、デバイスでローカルに行われた変更をすべて無視します。このような変更は、次回 CUCM が新しい設定をデバイスに適用するときに上書きされます。
- **エンドポイント (Endpoint)** : エンドポイントが設定データのマスター ソースとして動作します。このモードでは、エンドポイントは CUCM からの設定データを無視します。ローカルに行われた変更は同期されません。

  このモードは通常、インテグレータがデバイスをインストールし、デバイスからローカルに設定を制御する場合に使用されます。

オンデマンドによるデバイスからの設定の読み込み

管理者は、CUCM で [デバイスからxConfigを読み込む (*Pull xConfig. from Device*)] オプションを使用して、デバイスから設定の変更内容をいつでもオンデマンドで読み込むことができます。

このオプションは、デバイスが登録されている場合にのみ有効になります。

サポートされる CE ソフトウェアのバージョン

CE9.8 以降をサポートするすべてのデバイスで、CUCM のこの新しいプロビジョニング レイアウトを使用できます。

デバイスのソフトウェア バージョンが CE9.8 より前の場合は、CUCM のユーザ インターフェイスですべてのパラメータを表示できますが、設定できるのは "#" でマークされているサブセットのみです。"#" は各パラメータ値の右側に表示されます。

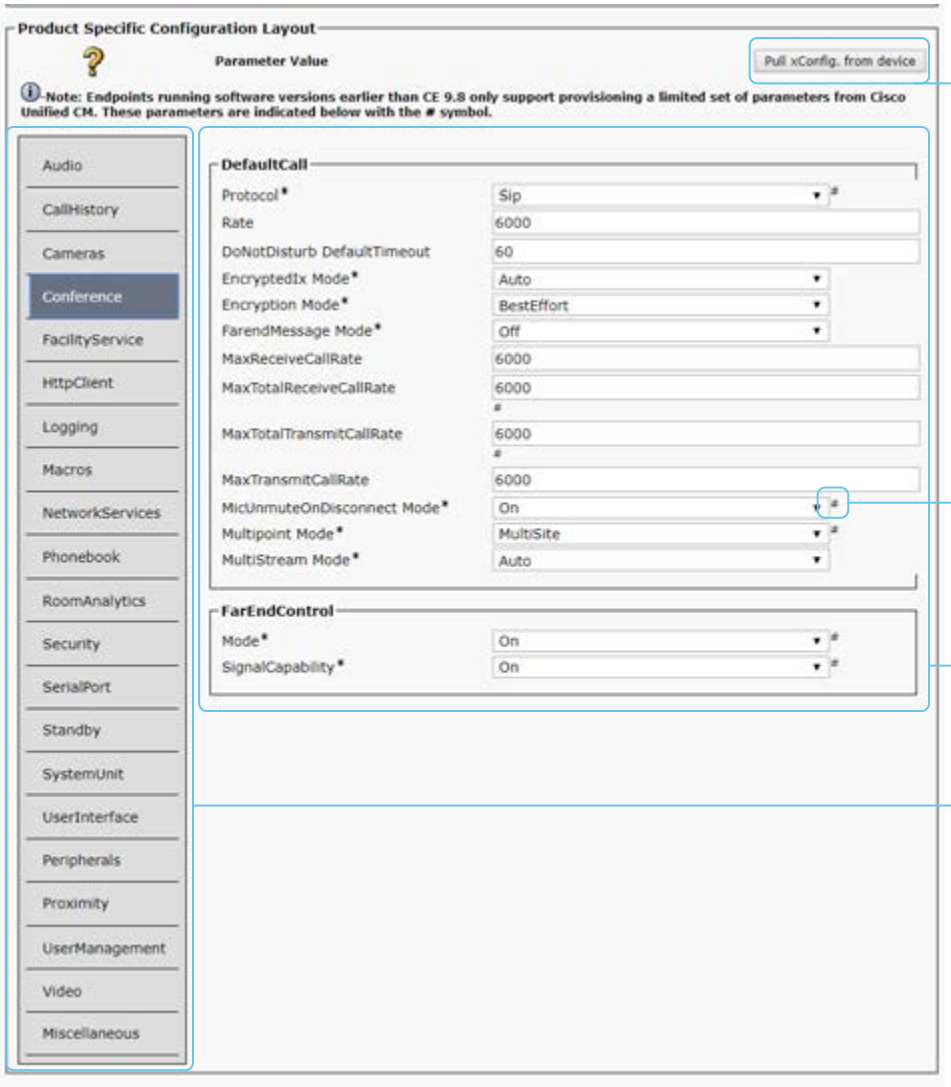
パラメータの完全なセットは、デバイスを CE9.8 以降にアップグレードした場合にのみ機能します。

CUCM からの製品固有の設定のプロビジョニング (2/2 ページ)

CUCM からのプロビジョニングのセットアップ

1. CUCM にサインインし、[デバイス (*Device*)] > [電話 (*Phone*)] に移動して、目的のデバイスを見つけます。
2. [製品固有の設定 (Product Specific Configuration Layout)] セクションを見つけます (図を参照) 。
3. [その他 (*Miscellaneous*)] カテゴリをクリックし、[設定制御モード (Configuration Control Mode)] 設定を見つけます。

   使用するモードを、[Unified CM]、[エンドポイント (Endpoint)]、または [Unified CMとエンドポイント (Unified CM and Endpoint)] から選択します (前のページの説明を参照) 。
4. デバイスから現在の設定を読み込む場合は、[デバイスからxConfigを読み込む (*Pull xConfig. from Device*)] ボタンをクリックします。
5. カテゴリを選択し、変更する設定の値を指定します。
6. 最後に、以前のバージョンの CUCM での手順と同様に、[保存 (*Save*)] と [設定の適用 (*Apply Config*)] をクリックします。



オンデマンドによるデバイスからの設定の読み込み

このボタンをクリックすると、デバイスからすべての構成がオンデマンドで読み込まれます。

ハッシュ (#) の付いた設定

Cisco UCM リリース 12.5(1)SU1 以前でも使用できていた設定です。

設定またはパラメータ

選択中のカテゴリに属している設定です。

カテゴリ

デバイス設定はカテゴリ別にグループ化されています。これらは、デバイスの Web インターフェイスで表示されるカテゴリと同じです。API コマンド パスにも対応しています。

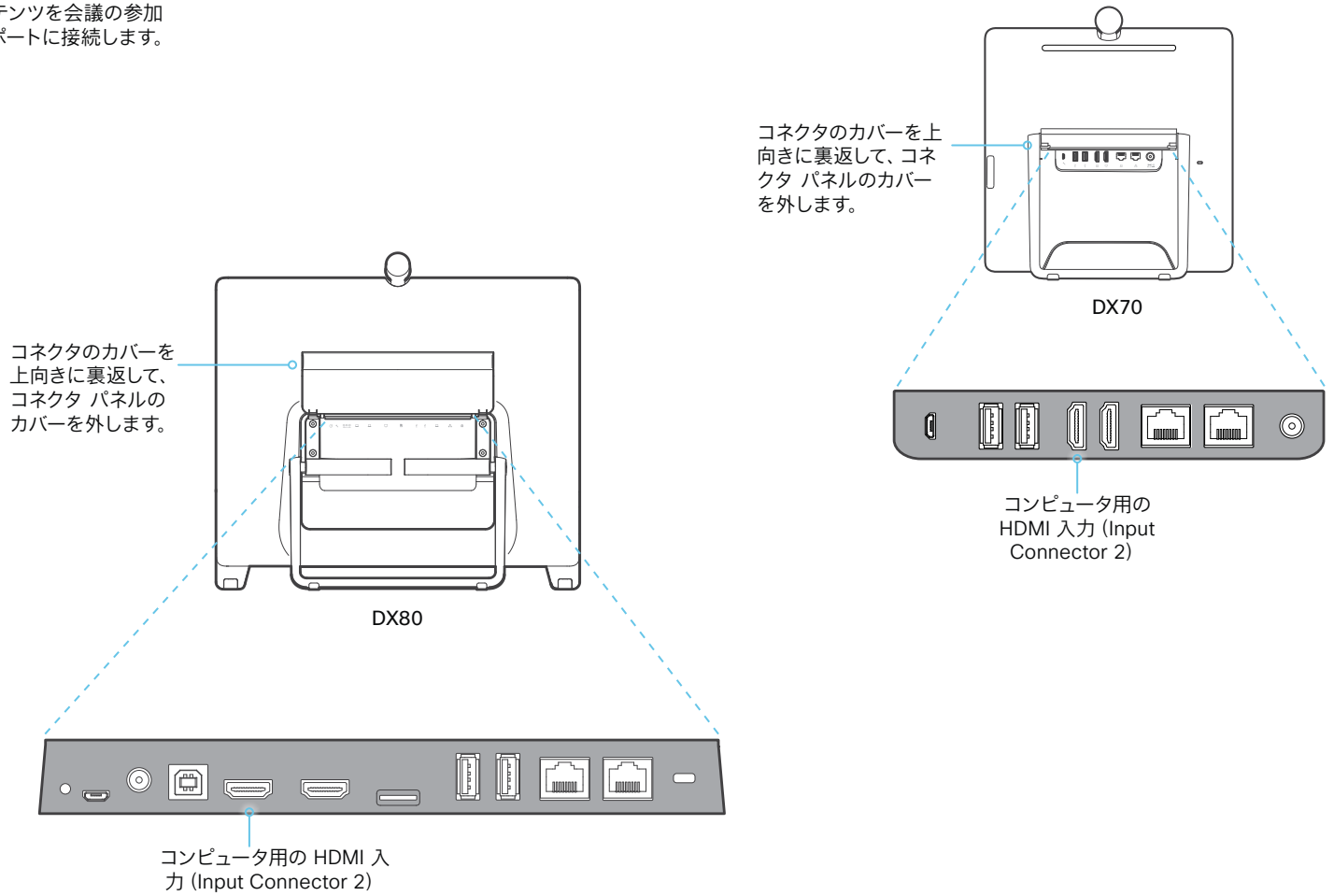
ただし、[その他 (*Miscellaneous*)] は例外です。このカテゴリには、CUCM でのみ設定可能な設定が表示されます。これらはデバイスのローカル設定に対応していません。

第 3 章

周辺機器

コンピュータの接続

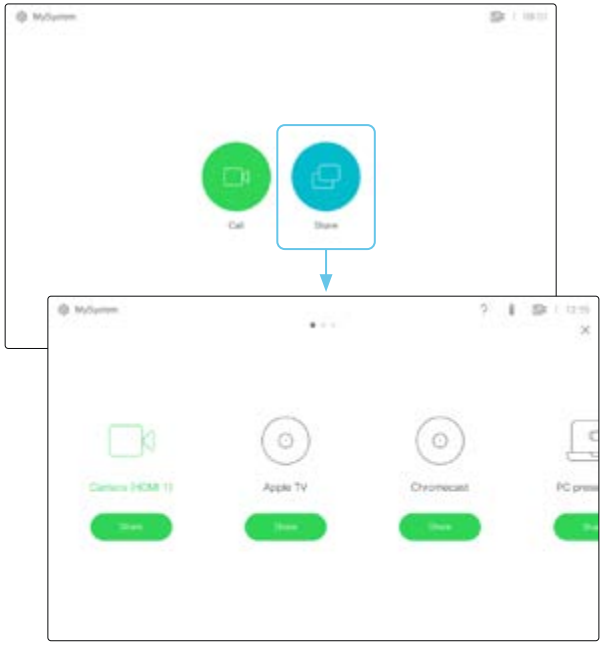
デバイスをコンピュータの画面として使用し、コンテンツを会議の参加者と共有するには、コンピュータを HDMI の入力ポートに接続します。



入力ソース数の拡大

Cisco のタッチ ユーザ インターフェイスは、サードパーティ製の外部ビデオ スイッチに接続された入力ソースが含まれるようにカスタマイズできます。

ソースは、ビデオ会議デバイスに直接接続されている他のビデオと同じように表示されて動作します。

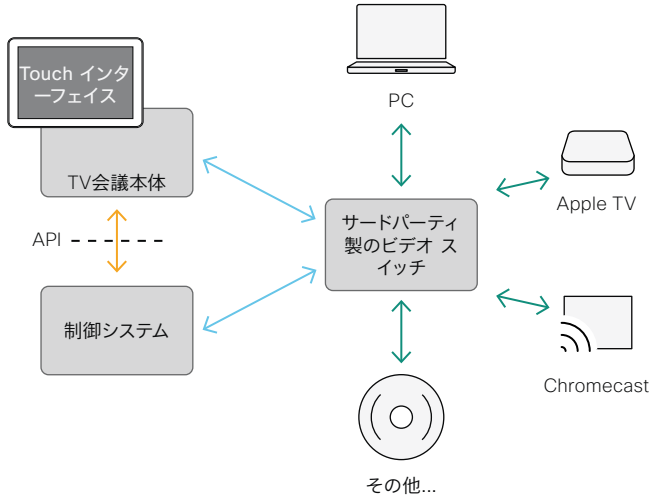


複数の外部入力ソースがあるユーザ インターフェイス (例)

アーキテクチャ

Touch インターフェイスを搭載したシスコのビデオ会議デバイス、サードパーティ製の制御システム (Crestron または AMX など) 、およびサードパーティ製ビデオ スイッチが必要です。ビデオ スイッチを制御するのは、ビデオ会議デバイスではなく、制御システムです。

制御システムをプログラミングするとき、ビデオ スイッチや Touch インターフェイスのコントロールに接続するには、ビデオ会議デバイスの API (イベントとコマンド) *を使用する必要があります。このようにして、ユーザ インターフェイス上に表示されて実行される事柄と、入力ソースの実際の状態とを同期できます。



ユーザ インターフェイスを拡張する方法と、それをデバイスの API を使用してセットアップする方法の詳細については、カスタマイズ ガイドをご覧ください。次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

* 制御システムをプログラミングするときに必要な API コマンドにアクセスするには、RoomControl、Integrator、または admin ユーザ ロールを持つユーザが必要です。

Bluetooth ヘッドセット

DX70 および DX80 では、次の Bluetooth プロファイルがサポートされています。

- HFP (ハンズフリー プロファイル)
- A2DP (高度なオーディオ配信プロファイル)
- ヘッドセットでは HFP と A2DP の両方、または HFP のみがサポートされている必要があります。A2DP 専用のヘッドセットはサポートされていません。

Bluetooth ヘッドセットは組み込みの Bluetooth 無線を直接使用してサポートされています。また USB Bluetooth ドングルを介して使用することもできます。ビデオ会議デバイスに複数のヘッドセットをペアリングすることができますが、一度に接続できるのは 1 つだけです。

範囲は最大 10m (30 フィート) です。通話中にこの範囲の外に出ると、音声がビデオ会議デバイスのスピーカーに切り替わります。

ほとんどのヘッドセットには音量コントロールが組み込まれています。通話中の場合は、ヘッドセットとビデオ会議デバイスの音量は同期しています。通話中でない場合は、ヘッドセットとビデオ会議デバイスの音量ボタンは独立して動作します。

サポート対象の Bluetooth 機能

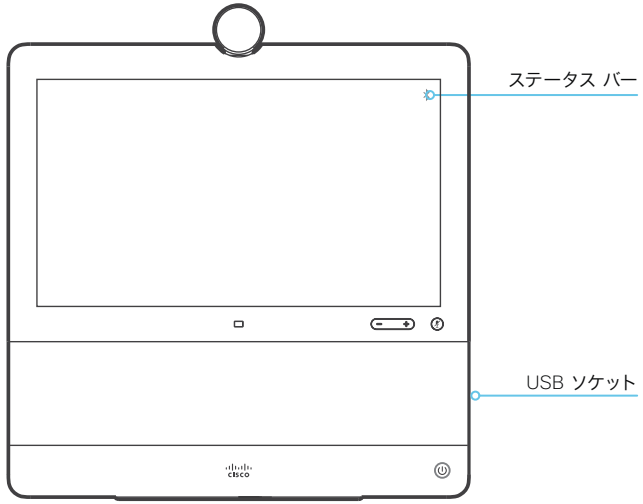
- 着信通話の応答
- 着信通話の拒否
- 通話の終了
- 音量の増減
- 一部のヘッドセットにはミュート コントロールがあります。これはビデオ会議デバイスのミュート コントロールとは独立して動作します。

USB Bluetooth ドングル

- 音質が向上するため、USB Bluetooth ドングルを使用することが推奨されます。
- USB Bluetooth ドングルを使用すると、ヘッドセットが USB ヘッドセットとして検出されます。
- ドングルを使用する場合、ヘッドセットの音量とビデオ会議デバイスの音量は同期されないことに注意してください。
- シスコでは Jabra Link 360、Plantronics BT300、および Plantronics BT600 についてテストを行っていますが、他の製品も同様に良好に動作するはずです。

Bluetooth ヘッドセットのペアリング

1. ヘッドセットで Bluetooth のペアリングをアクティブにします。ご不明な点がある場合は、ヘッドセットのマニュアルを参照してください。
2. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。[設定 (*Settings*)]、[*Bluetooth*] の順に選択します。Bluetooth が無効になっている場合は有効にします。Bluetooth はデフォルトで有効になっています。
3. ビデオ会議デバイスは、Bluetooth デバイスをスキャンします。検出された Bluetooth ヘッドセットがデバイス リストに表示されます。
4. デバイスを選択するとペアリングが開始されます。ペアリングが完了するまで数秒かかることがあります。
5. ペアリングが正常に行われると、ビデオ 会議デバイスはヘッドセットを接続済みとして表示します。これでペアリングが完了です。

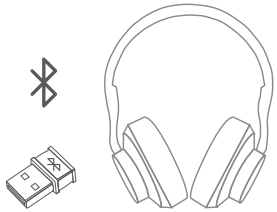


デバイス間の切り替え

ビデオ会議デバイスのスピーカーと、Bluetooth または USB で接続されたデバイスとを切り替えることができます。

ユーザ インターフェイスのステータス バーにあるアイコン (/ / / /) を選択し、使用可能なデバイスから選択します。

- スピーカー
- アナログ ヘッドセット (DX70 のみ)
- USB ヘッドセット
- USB ハンドセット
- Bluetooth デバイス



ビデオ 会議デバイスに直接 Bluetooth ペアリングを使用するか、USB ドングルを使用します。

ISDN リンクの接続

ISDN リンクを設定すると、ビデオ会議デバイスの接続に ISDN 回線を使用することができ、PSTN（公衆電話交換網）経由でのビデオ コールと電話が可能になります。

ISDN リンクは、ISDN BRI、ISDN PRI、および V.35 をサポートしています。ISDN は、SIP または H.323 コール用の通常の IP 接続に加えて使用できます。また、IP インフラストラクチャなしでも使用できます。

ISDN リンクは、ビデオ会議デバイスの Web インターフェイスから管理します。Web インターフェイスにサインインし、[セットアップ（*Setup*）] > [周辺機器（*Peripherals*）] に移動します。

要件および制約事項：

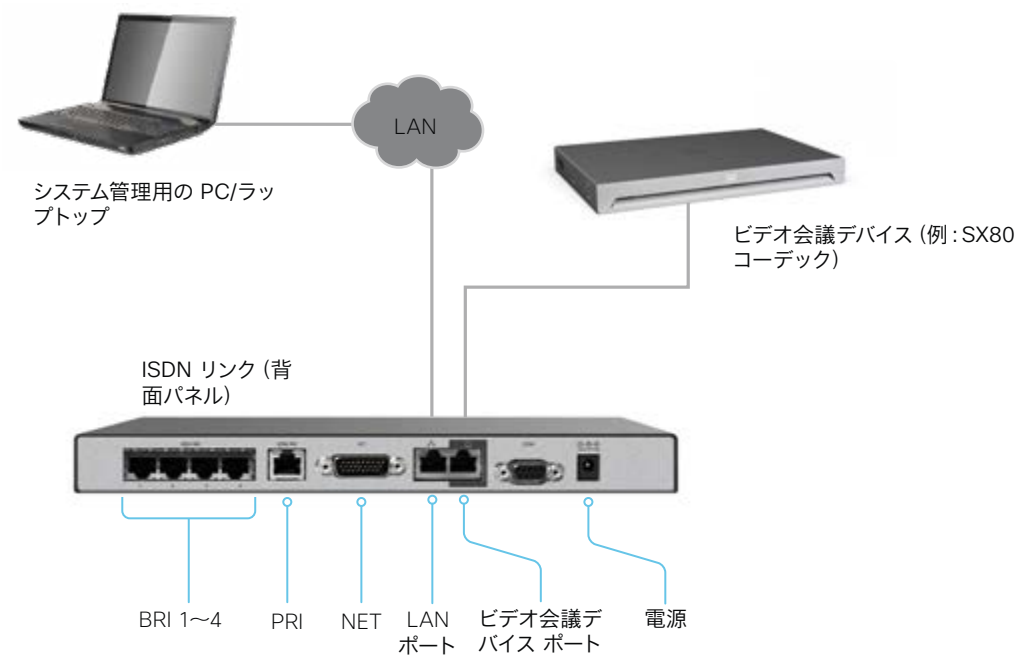
- ISDN リンクは、IL1.1.7 以降のソフトウェアを実行している必要があります。
- ビデオ会議デバイスで、CE9.3 以降のソフトウェアを実行している必要があります。ISDN リンクと通信するために、ビデオ会議デバイスの Web インターフェイスまたは API で IPv6 を有効にする必要があります。
- 確実にインストールするために、ISDN リンクのインストール ガイドでネットワーク トポロジを確認してください。
- ビデオ会議デバイスと ISDN リンクが同じサブネット上にある必要があります。エンドポイントまたは ISDN リンクに新しい IP アドレスが割り当てられている場合は、それらが同じサブネットに保持されている間だけペアリングが維持されます。
- Cisco Webex クラウド サービスに登録されているビデオ会議デバイスでは、ISDN リンクを使用できません。

セットアップと構成

ISDN リンクの詳細（リリース ノート、インストール ガイド、管理者ガイド、API ガイド、コンプライアンスおよび安全性ガイド）については、▶ https://www.cisco.com/go/isdnlink-docsを参照してください

LAN およびビデオ会議デバイスと ISDN リンクの直接接続を使用したセットアップ

これは推奨されるセットアップです。ただし、その他のオプションもあります。追加の例については、次のウェブ サイト にあるユーザ マニュアルを参照してください。▶ https://www.cisco.com/go/isdnlink-docsを参照してください



第 4 章

メンテナンス

デバイス ソフトウェアをアップグレードする (1/2 ページ)

Android ベースのソフトウェアと CE ソフトウェアとの間の変換

コラボレーション ソフトウェア バージョン 8.2 (CE8.2) 以降、すべての DX80 ユニットおよび DX70 ユニットで CE ソフトウェアを実行できます。このソフトウェアは、Cisco TelePresence SX および MX シリーズで動作するソフトウェアと同じものです。

DX80 と DX70 は、元々 Android ベースのソフトウェアとともに販売されていましたが、現在はCE ソフトウェアとともに出荷されています。

CE ソフトウェアに変換する前に、変換の要件、および Android ベースのソフトウェアと比較した機能の変化点を注意深く確認することが重要です。

DX デバイス上の CE ソフトウェアでは、CE9.1 の次の機能はサポートされていません。

- サードパーティ製アプリケーションのインストール
- キーボード コントロール、キーボードおよびマウスのリダイレクト

詳細については、ソフトウェア リリース ノートを参照してください。

Android ベースのソフトウェアから CE ソフトウェアへの変換、またはその逆の変換方法の詳細については、►https://www.cisco.com/go/dx-docs にある「Install and Upgrade Guides [英語]」で入手できる『Cisco DX70 and DX80 Convert between CE and Android based software』を参照してください。

CE8 から CE9 へのアップグレード

CE9 では、Cisco TelePresence Server を使用したマルチストリーム機能は廃止されます。

また、CE8 でタッチ インターフェイスから使用できたいくつかの機能は、最初の CE9 リリースでは使用できません。アップグレードを実行する前に、リリース ノートを参照してください。

デバイス ソフトウェアをアップグレードする (2/2 ページ)

以下の手順では、別の CE ソフトウェアのバージョンへのアップグレード (たとえば、CE8.2.x から CE8.2.y) のみを行えます。

Android ベースのソフトウェアと CE ソフトウェアの間で変換したい場合は、前のページを参照してください。

Web インターフェイスにログインし、[メンテナンス (*Maintenance*)] > [ソフトウェア アップグレード (*Software Upgrade*)] に移動します。

新しいソフトウェアをダウンロードする

各ソフトウェア バージョンに固有のファイル名があります。シスコのソフトウェア ダウンロード Web ページを開き、お使いの製品のページにアクセスします。► https://software.cisco.com/download/home [英語]

ファイル名フォーマットは :
“s52040ce9_9_x-yyy.pkg”

"x" はドット内のリリース番号、"yyy" は、ソフトウェアの一意の識別子を表します。

ソフトウェア リリース ノート

新着情報および変更の概要について、ソフトウェア リリース ノート (CE9) を読むことを推奨します。

► https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.htmlにアクセスしてください。

新しいソフトウェアのインストール

適切なソフトウェア パッケージをダウンロードして、コンピュータに保存します。これは .pkg ファイルです。ファイル名は変更しないでください。

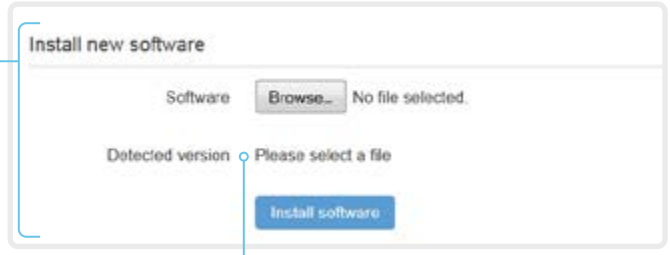
1. [参照... (*Browse...*)] をクリックして、新しいソフトウェアを含む .pkg ファイルを探します。

   ソフトウェアのバージョンが検出され、表示されます。

2. [ソフトウェアのインストール (*Install Software*)] をクリックして、インストール プロセスを開始します。

インストールの完了には、通常 15 分以上はかかりません。ウェブ ページから進捗状況を確認できます。インストール後、デバイスは自動的に再起動します。

再起動後に Web インターフェイスで作業を再開するには、再度サインインする必要があります。



新しいソフトウェア バージョンの確認

ファイルを選択すると、ここにソフトウェアのバージョンが表示されます。

ソフトウェアのダウンロード

Cisco Download Software ウェブ ページを開き、使用する製品のページにアクセスします。►https://software.cisco.com/download/home

Webex Board および Room シリーズは、COP ファイルを使用して Web インターフェイスからアップグレードできます。

SX、MX、および DX シリーズは、PKG ファイルを使用して Web インターフェイスからアップグレードできます。

オプション キーを追加する

ウェブ インターフェイスにログインし、[メンテナンス (*Maintenance*)] > [オプション キー (*Option Keys*)] に移動します。

すべてのオプション キーのリストと、デバイスにインストールされていないオプション キーのリストが表示されます。

アンインストールされたオプションのオプション キーを取得する方法については、Cisco の担当者にお問い合わせください。

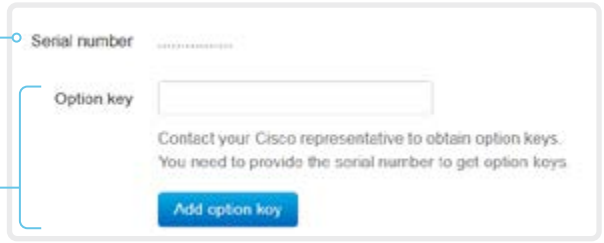
デバイスのシリアル番号

オプション キーの注文時にはデバイスのシリアル番号が必要です。

オプション キーの追加

1. テキストの入力フィールドにオプション キーを入力します。
2. [オプション キーの追加 (Add option key)] をクリックします。

オプション キーを複数追加する場合は、すべてのキーに対してこの手順を繰り返してください。



オプション キーについて

デバイスには、1 つ以上のソフトウェア オプションがインストールされている場合も、インストールされていない場合もあります。オプションの機能をアクティブにするには、対応するオプションキーがデバイスに存在している必要があります。

オプション キーは各デバイスに固有のものです。

オプション キーは、ソフトウェアのアップグレードまたは出荷時の状態にリセットしても削除されないため、一度追加するだけで済みます。

デバイスのステータス

デバイス情報の概要

[システム情報 (System Information)] ページを表示するには、ウェブ インターフェイスにログインします。

このページには、製品タイプ、デバイス名のほか、ハードウェア、ソフトウェア、インストール済みオプション、ネットワーク アドレスに関する基本情報が表示されます。ビデオ ネットワーク (SIP および H.323) の登録ステータスのほか、デバイスにコールする際に使用する番号および URI も含まれます。

デバイス ステータスの詳細

より詳細なステータス情報を確認するには、Web インターフェイスにサインインし、[セットアップ (*Setup*)] > [ステータス (*Status*)] に移動します*。

ステータス エントリを検索する

検索フィールドに必要な数の文字を入力します。これらの文字が含まれているすべてのエントリが右側のペインに表示されます。値スペースにこれらの文字が含まれているエントリも表示されます。

カテゴリを選択して適切なステータスに移動する

デバイス ステータスはカテゴリ別にグループ化されています。左側のペインでカテゴリを選択すると、関連するステータスが右側に表示されます。

* 図に示しているステータスは一例です。お使いのデバイスのステータスとは異なる場合があります。

診断の実行

ウェブ インターフェイスにサインインして、[メンテナンス (*Maintenance*)] > [診断 (*Diagnostics*)] に移動します。

[診断 (Diagnostics)] ページには、エラーの一般的な原因に関するステータスが示されます*。

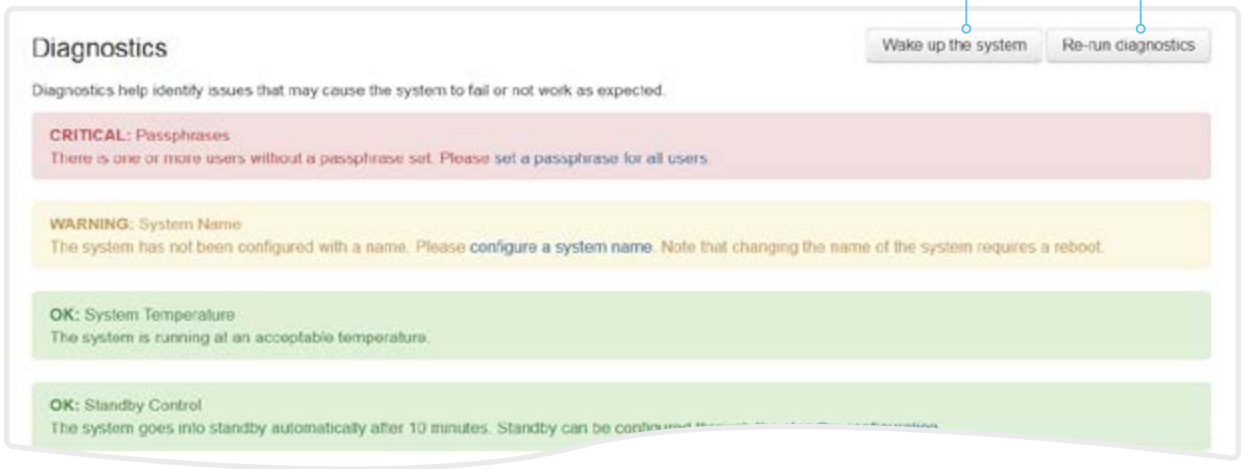
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

診断の実行

[診断の再実行 (*Re-run diagnostics*)] をクリックして、リストを最新の状態にします。

スタンバイ モードを離れる

スタンバイ モードのデバイスを復帰させるには、[システムの復帰 (*Wake up the system*)] をクリックします。

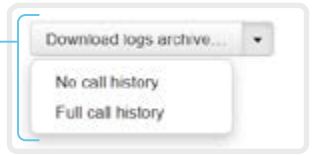


* 図に示しているメッセージは一例ですお使いのデバイスでは表示される情報が異なる場合があります。

ログ ファイルをダウンロードする

ウェブ インターフェイスにサインインして、[メンテナンス (Maintenance)] > [システム ログ (System Logs)] を選択します。

すべてのログ ファイルをダウンロードする



[ログ アーカイブのダウンロード... (Download logs archive...)] をクリックして、手順に従います。

匿名化された通話履歴はログ ファイルにデフォルトで含まれています。

ログ ファイルから通話履歴を除外する場合や、完全な通話履歴 (匿名以外の発信側/着信側) を含める場合は、ドロップダウン リストを使用します。

1 つのログファイルを開く/保存

ログ ファイルを開くにはウェブ ブラウザでファイル名をクリックし、ファイルをコンピュータに保存するにはファイル名を右クリックします。

拡張ロギングの開始

[拡張ロギングの開始... (Start extended logging...)] をクリックします。

拡張ロギングは、ネットワーク トラフィックの完全キャプチャが含まれているかどうかによって 3 分から 10 分かかります。

タイムアウトになる前に拡張ロギングを停止するには、[拡張ロギングの停止 (Stop extended logging)] をクリックします。

デフォルトとして、ネットワーク トラフィックはキャプチャされません。ネットワーク トラフィックの一部または全部のキャプチャを含めるには、ドロップダウン メニューを使用します。

ログ ファイル リストの表示更新

[現在のログ (Current logs)] または [履歴ログ (Historical logs)] の更新ボタンをクリックすると、対応するリストの表示が更新されます。

ログ ファイルについて

ログファイルは、テクニカル サポートが必要な場合に、Cisco のサポートから要求されることがある Cisco 固有のデバッグ ファイルです。

Current log ファイルはタイムスタンプ付きのイベント ログ ファイルです。

デバイスを再起動するたびに、現在のログ ファイルはタイムスタンプ付きの履歴ログ ファイルにすべてアーカイブされます。履歴ログ ファイルの最大数に到達すると、最も古いファイルは上書きされます。

拡張ロギング モード

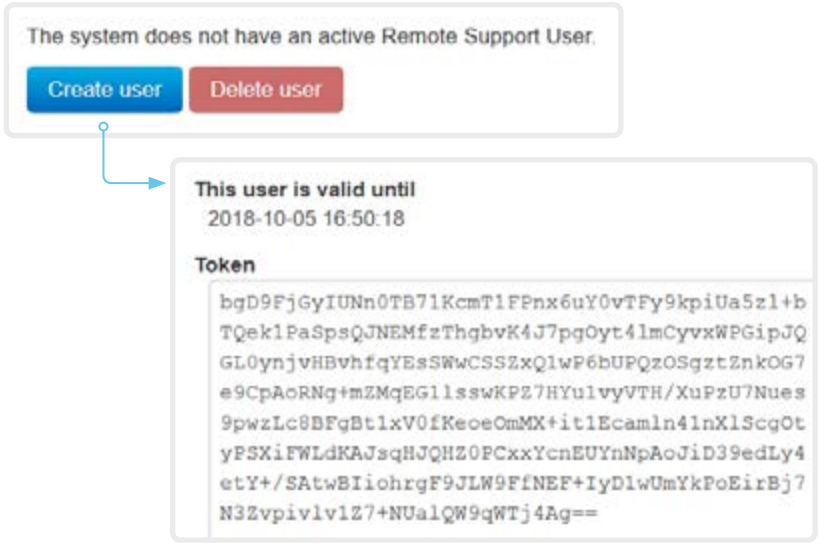
拡張ロギング モードをオンにすると、コールのセットアップ中にネットワークの問題の診断に役立つ場合があります。このモードの間は、より多くの情報がログ ファイルに保存されます。

拡張ロギングはデバイスのリソースをより多く使用するため、デバイスの動作が低下する場合があります。拡張ロギング モードは、トラブルシューティングのときにのみ使用してください。

リモート サポート ユーザを作成する

ウェブ インターフェイスにログインし、[メンテナンス (*Maintenance*)] > [システム リカバリ (*System Recovery*)] に移動して、[リモート サポート ユーザ (*Remote Support User*)] タブを選択します。

リモート サポート ユーザは、Cisco TAC から指示されたトラブルシューティングを行うためだけに有効にする必要があります。



リモート サポート ユーザの作成

1. [ユーザの作成 (*Create User*)] をクリックします。
2. Cisco TAC で案件を開きます。
3. [トークン (*Token*)] フィールドのテキストをコピーして、Cisco TAC に送信します。
4. Cisco TAC はパスワードを生成します。

リモート サポート ユーザは 7 日間、または削除されるまで有効です。

リモート サポート ユーザの削除

[ユーザの削除 (*Delete User*)] をクリックします。

リモート サポート ユーザについて

デバイスに診断の問題がある場合は、リモート サポート ユーザを作成できます。

リモート サポート ユーザにはデバイスに対する読み取りアクセス権が付与され、トラブルシューティングに役立つ限定された一連のコマンドにアクセスできます。

リモート サポート ユーザのパスワードを取得するには、Cisco Technical Assistance Center (TAC) アシスタントが必要です。

設定とカスタム要素のバックアップ/復元

ウェブ インターフェイスにサインインして、[メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)] に移動します。

バックアップ ファイル (zip 形式) には、設定とともにカスタム要素を含めることができます。以下の要素のいずれをバンドルに含めるかを選択できます。

- ブランディング イメージ
- マクロ
- お気に入り
- サインイン バナー
- UI 拡張
- 構成/設定 (すべてまたは一部)

バックアップ ファイルは、デバイスの Web インターフェイスから手動で復元できます。または、Cisco UCM や TMS などを使用して複数のデバイスにプロビジョニングできるように、バックアップ バンドルを一般化することもできます (**これ以降の章**を参照) 。

バックアップ ファイルの作成

1. [バックアップの作成 (Create backup)] タブを開きます。
2. バックアップ ファイルに含める要素を選択します。

   現在デバイス上に存在しない要素はグレー表示されます。
3. バックアップ ファイルに含める設定 (ある場合) を選択します。次の点に注意してください。
   - デフォルトでは、すべての設定がバックアップ ファイルに含まれます。
   - ウェブ ページの一覧から手動で設定を削除することにより、1 つ以上の設定を手動で削除できます。
   - 特定のデバイスに固有の設定をすべて削除する場合は、 [システム固有の設定の削除 (*Remove system-specific configurations*)] をクリックします。

     これは、他のデバイスでバックアップ バンドルを復元する予定がある場合に役立ちます。
4. [バックアップのダウンロード (Download backup)] をクリックして、コンピュータ上の zip ファイルに要素を保存します。

バックアップ ファイルの復元

1. [バックアップの復元 (Restore backup)] タブを選択します。
2. [参照... (Browse...)] をクリックして、復元するバックアップ ファイルを見つけます。

   バックアップ ファイル内のすべての設定と要素が適用されます。
3. [ファイルのアップロード (Upload File)] をクリックして、バックアップを適用します。

   設定によっては、有効にするためにデバイスを再起動する必要があります。

その他の情報

マクロの復元

マクロを含むバックアップ ファイルをデバイスで復元すると、次の処理が適用されます。

- マクロのランタイムを起動または再起動します。
- マクロは自動的に有効化 (開始) されます。

ブランド イメージの復元

バックアップバンドルにブランドイメージが含まれている場合、[ユーザインターフェイス壁紙 (UserInterface Wallpaper)] 設定は自動的に **[自動 (Auto)]** に設定されます。

したがって、ブランド イメージは自動的に表示されます。カスタム壁紙より優先される場合もあります。

バックアップ ファイル

バックアップ ファイルは、いくつかのファイルを含む zip 形式のファイルです。それらのファイルは zip ファイル内の最上位にあり、フォルダに含まれていないことが重要です。

カスタム要素の CUCM プロビジョニング

バックアップ ファイルは、「► 設定とカスタム要素のバックアップおよび復元」の章で説明されているとおり、複数のデバイスでカスタマイズ テンプレートとして使用できます。

カスタマイズ テンプレート (バックアップ ファイル) は、次のいずれかによってホストされています。

- CUCM TFTP ファイル サービス、または
- デバイスが HTTP または HTTPS で接続可能なカスタム Web サーバ。

デバイスが CUCM (Cisco Unified Communications Manager) からカスタマイズ テンプレートの名前と格納場所に関する情報を取得するときは、デバイスがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

カスタマイズ テンプレートとして使用するバックアップ ファイルに設定が含まれている場合でも、設定はデバイス上に復元されません。

カスタマイズ テンプレートの TFTP ファイル サーバへのアップロード

1. Cisco Unified OS の管理にサインインします。
2. [ソフトウェア アップグレード (Software Upgrades)] > [TFTP ファイル管理 (TFTP File Management)] に移動します。
3. [ファイルのアップロード (Upload File)] をクリックします。入力フィールドにカスタマイズ テンプレートの名前とパスを入力します。
4. [ファイルのアップロード (Upload File)] をクリックします。

デバイスごとのカスタマイズ プロビジョニング情報の追加

1. Cisco Unified CM の管理にサインインします。
2. [デバイス (Device)] > [電話 (Phone)] に移動します。
3. 関連するデバイスの製品固有の構成セクション内で、[カスタマイズ プロビジョニング (Customization Provisioning)] フィールドに以下を入力します。
   - カスタマイズ ファイル : カスタマイズ テンプレートのファイル名 (backup.zip など) *
   - カスタマイズ ハッシュの型 : SHA512
   - カスタマイズ ハッシュ : カスタマイズ テンプレートの SHA512 チェックサム。

   これらのフィールドが存在しない場合は、CUCM に新しいデバイス パッケージをインストールする必要があります。
4. [保存 (*Save*)] および [設定の適用 (*Apply Config*)] をクリックして、設定をデバイスにプッシュします。

* TFTP サービスを使用しない場合は、カスタマイズ テンプレートの完全な URI : `<host name>:<portnumber>/<path-and-filename>` を入力する必要があります。

次に例を示します。

- http://host:6970/backup.zip または
- https://host:6971/backup.zip

SHA512 チェックサム

ヒント : Web インターフェイスを使用してデバイスにファイルを復元すると、そのファイルの SHA512 チェックサムを確認できます。

1. ウェブ インターフェイスにサインインして、[メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)] に移動します。
2. [バックアップの復元 (Restore backup)] タブを選択します。
3. [参照 (Browse...)] をクリックして、チェックサムを計算したいファイルを検索します。

   ページの下部に SHA512 チェックサムが表示されていることが確認できます。

CUCM のドキュメンテーション

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

カスタム要素の TMS プロビジョニング

バックアップ ファイルは、「► 設定とカスタム要素のバックアップおよび復元」の章で説明されているとおり、複数のデバイスでカスタマイズ テンプレートとして使用できます。

バックアップ ファイルは、デバイスが HTTP または HTTPS で接続可能なカスタム Web サーバ上にホストする必要があります。

デバイスが TMS (TelePresence Management Suite) からバックアップ ファイルの名前と位置に関する情報を取得するときは、デバイスがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

構成テンプレートの作成と適用

1. 構成テンプレートを作成します。
2. 次の XML 文字列を含むカスタム コマンドを構成テンプレートに追加します。

```
<Command>
  <Provisioning>
    <Service>
      <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
      </Fetch>
    </Service>
  </Provisioning>
</Command>
```

   where

   web-server-address: バックアップ ファイルへの URI (例 : http://host/backup.zip) 。

   checksum: バックアップ ファイルの SHA512 チェックサム。

   origin: プロビジョニング *

3. 設定テンプレートのプッシュ先のデバイスを選択し、[システムのセット (*Set on systems*)] をクリックします。

TMS 構成テンプレートおよびカスタムコマンドの作成方法の詳細については、► Cisco TMS 管理者ガイド を参照してください。

* このパラメータを **Provisioning** に設定しない場合は、バックアップ ファイルに含まれる設定もデバイスにプッシュされます。特定の 1 台のデバイスに固有の構成 (静的 IP アドレス、システム名、連絡先情報など) がバックアップ ファイルに含まれていると、接続できないデバイスができる可能性があります。

SHA512 チェックサム

ヒント : Web インターフェイスを使用してデバイスにファイルを復元すると、そのファイルの SHA512 チェックサムを確認できます。

1. ウェブ インターフェイスにサインインして、[メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)] に移動します。
2. [バックアップの復元 (Restore backup)] タブを選択します。
3. [参照 (*Browse...*)] をクリックして、チェックサムを計算したいファイルを検索します。

   ページの下部に SHA512 チェックサムが表示されていることが確認できます。

以前に使用していたソフトウェア イメージに復元する

ウェブ インターフェイスにサインインして、[メンテナンス (*Maintenance*)] > [システム回復 (*System Recovery*)] に移動します。

注 : 以下の手順では、別の CE ソフトウェアのバージョンへの復元 (たとえば、CE8.3.y から CE8.2.x) のみを行えます。

Android ベースのソフトウェアに変換して戻す場合は、►「デバイス ソフトウェアをアップグレードする」の章を参照してください。

以前使用していたソフトウェア イメージに切り替える前に、デバイスのログ ファイル、構成、およびカスタム要素をバックアップすることを推奨します。

ログ ファイル、構成、カスタム要素のバックアップ

1. [バックアップ (Backup)] タブを選択します。
2. [ログのダウンロード (*Download logs*)] をクリックし、指示に従ってログ ファイルをコンピュータに保存します。
3. [バックアップのダウンロード (*Download Backup*)] をクリックし、指示に従ってバックアップ バンドルをコンピュータに保存します。

以前使用していたソフトウェア イメージに復元する

管理者以外、または、Cisco テクニカル サポートの指示のもとで行う場合以外はこの手順を実行しないでください。

1. [ソフトウェア回復交換 (Software Recovery Swap)] タブを選択します。
2. [ソフトウェア : cex.y.z への切り替え... (*Switch to software: cex.y.z...*)] をクリックします。ここで x.y.z はソフトウェア バージョンを示します。
3. [はい (*Yes*)] をクリックして選択を確定します。または、操作をやめる場合は [キャンセル (*Cancel*)] をクリックします。

デバイスがリセットされるまでお待ちください。完了するとデバイスが自動的に再起動します。この手順は数分かかることがあります。

以前に使用されたソフトウェア イメージについて

デバイスに重大な問題がある場合は、以前使用していたソフトウェア イメージに切り替えることで、問題の解決に役立つ場合があります。

ソフトウェアを最後にアップグレードしてからデバイスを初期設定にリセットしていない場合は、それまで使用していたソフトウェア イメージがデバイスに存在しています。ソフトウェアをダウンロードする必要はありません。

ビデオ会議デバイスの初期設定へのリセット (1/4 ページ)

デバイスに重大な問題が発生した場合、最後の手段としてデフォルトの初期設定にリセットすることができます。

初期設定にリセットすると元に戻すことはできません。

工場出荷時の状態にリセットする前に以前使用したソフトウェア イメージに戻すことを常に検討してください。多くの場合これでデバイスが回復します。ソフトウェアの切り替えについては、▶ 「以前に使用していたソフトウェア イメージへの復元」の章を参照してください。

デバイスを初期設定にリセットする際は、Web インターフェイスまたはユーザ インターフェイスを使用することを推奨します。これらのインターフェイスを使用できない場合は、DX80 ではリセット pin ホールを、DX70 ではミュート ボタンと音量ボタンを使用します。

工場出荷時設定リセットにより、次のような影響が発生します。

- 通話履歴が削除されます。
- パスフレーズがデフォルト設定にリセットされます。
- すべてのデバイス パラメータがデフォルト値にリセットされます。
- デバイスにアップロード済みのファイルがすべて削除されます。これには、カスタム壁紙、ブランディング要素、証明書、お気に入りリストなどが含まれます。
- 以前の (非アクティブな) ソフトウェア イメージが削除されます。
- オプション キーは影響を受けません。

初期設定にリセットした後は、デバイスが自動的に再起動します。これは、以前と同じソフトウェア イメージを使用しています。

初期設定へのリセットを実行する前に、デバイスのログ ファイル、設定、カスタム要素をバックアップすることを推奨します。バックアップしない場合、これらのデータは失われます。

ビデオ会議デバイスの初期設定へのリセット (2/4 ページ)

ウェブ インターフェイスを使用した初期設定へのリセット

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

ウェブ インターフェイスにサインインして、[メンテナンス (*Maintenance*)] > [システム回復 (*System Recovery*)] に移動します。

1. [初期設定へのリセット (Factory Reset)] タブを選択して、表示される情報を注意深く読みます。
2. [初期設定へのリセットの実行 (Perform a factory reset...)] クリックします。
3. [はい (*Yes*)] をクリックして選択を確定するか、[キャンセル (*Cancel*)] をクリックして操作を取り消します。
4. デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。

   デバイスが正常に初期設定にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。

ユーザ インターフェイスからの初期設定へのリセット

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [設定 (Settings)] を選択します。
3. [初期設定へのリセット (Factory Reset)] を選択します。
4. 選択を確認するには[リセット (reset)]を選択し、気が変わったら[戻る (Back)]を選択します。
5. デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。

   デバイスが正常に初期設定にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。

ログ ファイル、構成、カスタム要素のバックアップ

ウェブ インターフェイスにサインインして、[メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)] に移動します。

1. [バックアップ (Backup)] タブを選択します。
2. [ログのダウンロード (Download logs)] をクリックし、指示に従ってログ ファイルをコンピュータに保存します。
3. [バックアップのダウンロード (Download Backup)] をクリックし、指示に従ってバックアップ バンドルをコンピュータに保存します。

ビデオ会議デバイスの初期設定へのリセット (3/4 ページ)

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

ミュート ボタンと音量ボタンを使用した DX80 の工場出荷時設定へのリセット

次の手順を実行して、起動時に DX80 を工場出荷時設定にリセットします。デバイスの電源がオンになっている場合、先に進む前に電源ボタンを押して、デバイスがシャットダウンするまで押し続けます。

1. ミュート ボタンと音量アップ ボタンを探してください。
2. 音量アップ ボタンを押したままにして、デバイスの電源をオンにします。
3. ミュート ボタンが赤色に点灯したら、音量アップ ボタンを放し、ミュート ボタンを押します。

   デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。

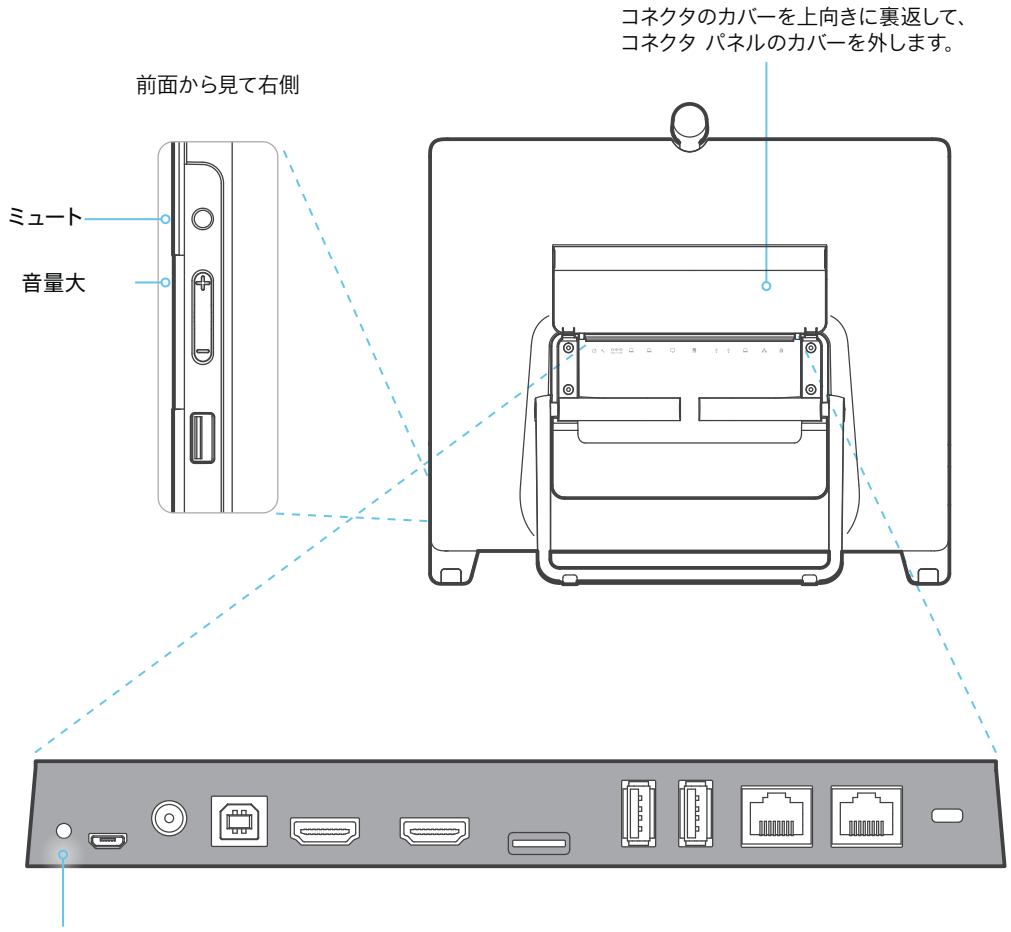
   デバイスが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。

リセット ボタンを使用した DX80 の工場出荷時設定へのリセット

この方法を使用するには、DX80 が稼動している必要があります。

1. デバイスの背面で、コネクタのカバーを上向きに裏返して、コネクタ パネルのカバーを外します。
2. ペン先 (または同等のもの) を使用して、引っ込んでいるリセット ボタンを押して、[初期設定へのリセットを実行しています (*Resetting to factory settings*)] という通知が画面に表示されるまで、このボタンを 1 ～ 2 秒間押し続けます。
3. デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。

   デバイスが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。



ビデオ会議デバイスの初期設定へのリセット (4/4 ページ)

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

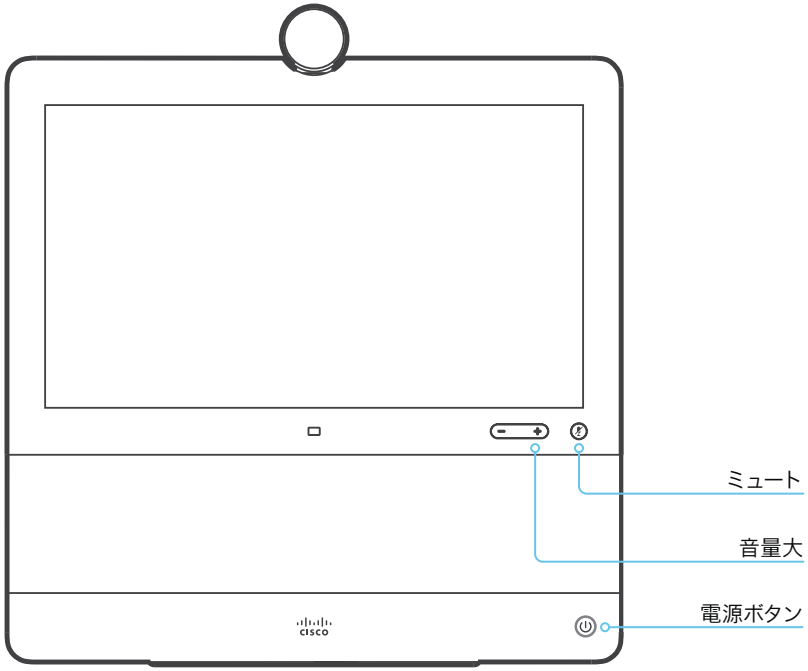
ミュート ボタンと音量ボタンを使用した DX70 の工場出荷時設定へのリセット

次の手順を実行して、起動時に DX70 を工場出荷時設定にリセットします。デバイスの電源がオンになっている場合、先に進む前に電源ボタンを押して、デバイスがシャットダウンするまで押し続けます。

1. ミュート ボタン (LED) と音量アップ ボタン (LED) を探してください。
2. 電源ボタンを押して、ミュート ボタンに注目してください。
3. ミュート ボタンが 2 回点滅したら、音量アップ ボタンを押し、そのすぐ後に約 4 秒間ミュート ボタンを押し続けます。このプロセス中に、ミュート ボタンが数秒間赤になります。

   デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。

   デバイスが正常に初期設定にリセットされると、セットアップアシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。



ユーザ インターフェイスのスクリーンショットをキャプチャする

ウェブ インターフェイスにサインインして、[メンテナンス (*Maintenance*)] > [ユーザ インターフェイスのスクリーンショット (*User Interface Screenshots*)] に移動します。

スクリーンショットのキャプチャ

メイン画面の (画面上の表示の) スクリーンショットをキャプチャするには、[OSD のスクリーンショットを撮る (*Take screenshot of OSD*)] をクリックします。

スクリーンショットはボタンの下のエリアに表示されます。スクリーンショットの準備ができるまで最大 30 秒かかる場合があります。

キャプチャされたすべてのスナップショットはボタンの上のリストに含まれています。イメージを表示するには、スクリーンショット ID をクリックします。

スクリーンショットを削除する

すべてのスクリーンショットを削除する場合は、[すべて削除 (*Remove all*)] をクリックします。

1 つのスクリーンショットのみを削除するには、そのスクリーンショットの ✖ ボタンをクリックします。

ユーザ インタフェースのスクリーンショットについて

メイン画面上の表示を、メニュー、インジケータ、メッセージ (オンスクリーン画面) とともにスクリーンショットでキャプチャできます。

第 5 章

デバイスの設定

デバイス設定の概要

これ以降のページでは、Web インターフェイスの [セットアップ (*Setup*)] > [設定 (*Configuration*)] ページで設定する、すべてのデバイス設定のリストを示します。

Web ブラウザを開き、デバイスの IP アドレスを入力して、サインインします。

IP アドレスの確認方法

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [このデバイスについて (*About this device*)]に続き、[設定 (*Settings*)]を選択します。

音声設定 105
Audio DefaultVolume 105
Audio Input MicrophoneMode 105
Audio Microphones Mute Enabled 105
Audio SoundsAndAlerts RingTone 105
Audio SoundsAndAlerts RingVolume 105
Audio Ultrasound MaxVolume 106
Audio Ultrasound Mode 106

Bluetooth 設定 107
Bluetooth Allowed 107
Bluetooth Enabled 107

CallHistory の設定 108
CallHistory Mode 108

カメラの設定 109
Cameras Camera [n] Backlight DefaultMode 109

会議設定 110
Conference ActiveControl Mode 110
Conference AutoAnswer Delay 110
Conference AutoAnswer Mode 110
Conference AutoAnswer Mute 110
Conference CallProtocolIPStack 110
Conference DefaultCall Protocol 111
Conference DefaultCall Rate 111
Conference DoNotDisturb DefaultTimeout 111
Conference Encryption Mode 111
Conference FarEndControl Mode 111
Conference FarEndControl SignalCapability 112
Conference FarEndMessage Mode 112
Conference MaxReceiveCallRate 112
Conference MaxTotalReceiveCallRate 112
Conference MaxTotalTransmitCallRate 112
Conference MaxTransmitCallRate 112
Conference MicUnmuteOnDisconnect Mode 113

Conference Multipoint Mode 113
Conference Presentation OnPlacedOnHold 113
Conference VideoBandwidth Mode 113

FacilityService の設定 114
FacilityService Service [n] CallType 114
FacilityService Service [n] Name 114
FacilityService Service [n] Number 114
FacilityService Service [n] Type 114

H323 の設定 115
H323 Authentication LoginName 115
H323 Authentication Mode 115
H323 Authentication Password 115
H323 CallSetup Mode 115
H323 Encryption KeySize 116
H323 Gatekeeper Address 116
H323 H323Alias E164 116
H323 H323Alias ID 116
H323 NAT Address 117
H323 NAT Mode 116
H323 PortAllocation 117

HttpClient の設定 118
HttpClient AllowHTTP 118
HttpClient AllowInsecureHTTPS 118
HttpClient Mode 118

HTTP フィードバック設定 119
HttpFeedback TlsVerify 119

ロギングの設定 120
Logging Debug Wifi 120
Logging External Mode 120
Logging External Protocol 120
Logging External Server Address 120
Logging External Server Port 120
Logging External TlsVerify 121
Logging Internal Mode 121
Logging Mode 121

マクロ設定 122
Macros AutoStart 122
Macros Mode 122

ネットワーク設定 123
Network [n] DNS DNSSEC Mode 123
Network [n] DNS Domain Name 123
Network [n] DNS Server [m] Address 123
Network [n] IEEE8021X AnonymousIdentity 124
Network [n] IEEE8021X Eap Md5 125
Network [n] IEEE8021X Eap Peap 125
Network [n] IEEE8021X Eap Tls 125
Network [n] IEEE8021X Eap Ttls 125
Network [n] IEEE8021X Identity 124
Network [n] IEEE8021X Mode 123
Network [n] IEEE8021X Password 124
Network [n] IEEE8021X TlsVerify 124
Network [n] IEEE8021X UseClientCertificate 124
Network [n] IPStack 125
Network [n] IPv4 Address 126
Network [n] IPv4 Assignment 126
Network [n] IPv4 Gateway 126
Network [n] IPv4 SubnetMask 126
Network [n] IPv6 Address 127
Network [n] IPv6 Assignment 126
Network [n] IPv6 DHCPOptions 127
Network [n] IPv6 Gateway 127
Network [n] MTU 127
Network [n] QoS Diffserv Audio 128
Network [n] QoS Diffserv Data 128
Network [n] QoS Diffserv ICMPv6 129
Network [n] QoS Diffserv NTP 129
Network [n] QoS Diffserv Signalling 128
Network [n] QoS Diffserv Video 128
Network [n] QoS Mode 127
Network [n] RemoteAccess Allow 129
Network [n] Speed 129
Network [n] TrafficControl Mode 130

Network [n] VLAN Voice Mode 130
Network [n] VLAN Voice VlanId 130

NetworkPort 設定 131
NetworkPort [n] Mode 131

NetworkServices の設定 132
NetworkServices CDP Mode 132
NetworkServices H323 Mode 132
NetworkServices HTTP Mode 132
NetworkServices HTTP Proxy LoginName 132
NetworkServices HTTP Proxy Mode 133
NetworkServices HTTP Proxy PACUrl 133
NetworkServices HTTP Proxy Password 133
NetworkServices HTTP Proxy Url 133
NetworkServices HTTPS OCSP Mode 133
NetworkServices HTTPS OCSP URL 134
NetworkServices HTTPS Server MinimumTLSVersion 134
NetworkServices HTTPS StrictTransportSecurity 134
NetworkServices HTTPS VerifyClientCertificate 134
NetworkServices NTP Mode 134
NetworkServices NTP Server [n] Address 135
NetworkServices NTP Server [n] Key 135
NetworkServices NTP Server [n] KeyAlgorithn 135
NetworkServices NTP Server [n] KeyId 135
NetworkServices SIP Mode 135
NetworkServices SNMP CommunityName 136
NetworkServices SNMP Host [n] Address 136
NetworkServices SNMP Mode 136
NetworkServices SNMP SystemContact 136
NetworkServices SNMP SystemLocation 136
NetworkServices SSH AllowPublicKey 137
NetworkServices SSH HostKeyAlgorithm 137
NetworkServices SSH Mode 137
NetworkServices Telnet Mode 137
NetworkServices Websocket 137
NetworkServices WelcomeText 137
NetworkServices Wifi Allowed 138
NetworkServices Wifi Enabled 138
NetworkServices XMLAPI Mode 138

周辺機器の設定 139
Peripherals InputDevice Mode 139
Peripherals Profile ControlSystems 139

電話帳の設定 140
Phonebook Server [n] ID 140
Phonebook Server [n] Pagination 140
Phonebook Server [n] TlsVerify 140
Phonebook Server [n] Type 141
Phonebook Server [n] URL 141

プロビジョニング設定 142
Provisioning Connectivity 142
Provisioning ExternalManager Address 142
Provisioning ExternalManager AlternateAddress 142
Provisioning ExternalManager Domain 143
Provisioning ExternalManager Path 143
Provisioning ExternalManager Protocol 142
Provisioning LoginName 143
Provisioning Mode 143
Provisioning Password 144
Provisioning TlsVerify 144

プロキシミティの設定 145
Proximity Mode 145
Proximity Services CallControl 145
Proximity Services ContentShare FromClients 145
Proximity Services ContentShare ToClients 145

ルームリセット設定 146
RoomReset Control 146

RTP の設定 147
RTP Ports Range Start 147
RTP Ports Range Stop 147
RTP Video Ports Range Start 147
RTP Video Ports Range Stop 147

セキュリティの設定 148
Security Audit Logging Mode 148
Security Audit OnError Action 148
Security Audit Server Address 148

Security Audit Server Port 148
Security Audit Server PortAssignment 149
Security Session FailedLoginsLockoutTime 149
Security Session InactivityTimeout 149
Security Session MaxFailedLogins 149
Security Session MaxSessionsPerUser 149
Security Session MaxTotalSessions 149
Security Session ShowLastLogon 150

シリアルポート設定 151
SerialPort LoginRequired 151
SerialPort Mode 151

SIP の設定 152
SIP ANAT 152
SIP Authentication Password 152
SIP Authentication UserName 152
SIP DefaultTransport 152
SIP DisplayName 152
SIP Ice DefaultCandidate 153
SIP Ice Mode 153
SIP Line 153
SIP ListenPort 153
SIP Mailbox 153
SIP MinimumTLSVersion 154
SIP PreferredIPSignaling 154
SIP Proxy [n] Address 154
SIP TlsVerify 154
SIP Turn DiscoverMode 154
SIP Turn DropRflx 155
SIP Turn Password 155
SIP Turn Server 155
SIP Turn UserName 155
SIP Type 155
SIP URI 155

スタンバイの設定 156
Standby Control 156
Standby Delay 156
Standby WakeupOnMotionDetection 156

システムユニット設定 157
SystemUnit CrashReporting Advanced 157
SystemUnit CrashReporting Mode 157
SystemUnit CrashReporting Url 157
SystemUnit Name 157

時刻の設定 158
Time DateFormat 158
Time TimeFormat 158
Time Zone 159

ユーザ インターフェイス設定 161
UserInterface Accessibility IncomingCallNotification 161
UserInterface Branding AwakeBranding Colors 161
UserInterface ContactInfo Type 161
UserInterface CustomMessage 161
UserInterface Features Call End 162
UserInterface Features Call MidCallControls 162
UserInterface Features Call Start 162
UserInterface Features HideAll 162
UserInterface Features Share Start 162
UserInterface Features Whiteboard Start 163
UserInterface KeyTones Mode 162
UserInterface Language 163
UserInterface OSD EncryptionIndicator 163
UserInterface OSD HalfwakeMessage 163
UserInterface OSD Output 163
UserInterface Phonebook Mode 164
UserInterface Security Mode 164
UserInterface SettingsMenu Mode 164
UserInterface SettingsMenu Visibility 164
UserInterface SoundEffects Mode 165
UserInterface Wallpaper 165

ユーザ管理設定 166
UserManagement LDAP Admin Filter 166
UserManagement LDAP Admin Group 166
UserManagement LDAP Attribute 166
UserManagement LDAP BaseDN 166
UserManagement LDAP Encryption 166
UserManagement LDAP MinimumTLSVersion 167

UserManagement LDAP Mode 167
UserManagement LDAP Server Address 167
UserManagement LDAP Server Port 167
UserManagement LDAP VerifyServerCertificate 167

ビデオ設定 168
Video ActiveSpeaker DefaultPIPPosition 168
Video DefaultLayoutFamily Local 168
Video DefaultMainSource 168
Video Input Connector [n] CameraControl CameraId 169
Video Input Connector [n] CameraControl Mode 169
Video Input Connector [n] InputSourceType 169
Video Input Connector [n] Name 169
Video Input Connector [n] OptimalDefinition Profile 170
Video Input Connector [n] PresentationSelection 170
Video Input Connector [n] Quality 171
Video Input Connector [n] RGBQuantizationRange 171
Video Input Connector [n] Visibility 171
Video Monitors 171
Video Output Connector [n] Brightness 171
Video Output Connector [n] Resolution 172
Video Output Connector [n] Whitebalance Level 172
Video Presentation DefaultPIPPosition 172
Video Presentation DefaultSource 172
Video Presentation Priority 173
Video Selfview Default FullscreenMode 173
Video Selfview Default Mode 173
Video Selfview Default OnMonitorRole 173
Video Selfview Default PIPPosition 174
Video Selfview Mirrored 174
Video Selfview OnCall Duration 174
Video Selfview OnCall Mode 174

試験的設定 175

音声設定

Audio DefaultVolume

スピーカーのデフォルト音量を定義します。ビデオ会議デバイスのスイッチをオンにするか再起動すると、音量がこの値に設定されます。実行中に音量を変更するには、ユーザ インターフェイスのコントロールを使用します。また、API コマンド (xCommand Audio Volume) を使用して、デバイスの稼働中に音量を変更したり、デフォルト値にリセットしたりすることもできます。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: 50

値スペース: 整数 (0..100)

範囲: 1 ～ 100 の値を選択します。これは、-34.5 dB ～ 15 dB の範囲内の 0.5 dB 単位に相当します。0 に設定すると、音声がオフになります。

Audio Input MicrophoneMode

この設定は DX80 のみに適用されます。

DX80 では両方の脚にマイクが搭載されています。マイク モードを Focused に設定すると、マイクを組み合わせて音声感度が高くなります。その結果、室内のノイズが聞こえなくなり、デバイスの正面に座った人の声がよく聞こえるようになります。デバイスの正面に座っていない人の声は聞こえなくなります。

マイクロフォン モードを Wide に設定すると、デバイスは他のデバイスと同様に動作します。横に座っている人の声が聞こえるようになり、また室内のノイズもより聞こえるようになります。

話者が 1 人のみの場合、Focused モードを使用することをお勧めします。デバイスの前で複数の人が話す場合は Wide モードを使用してください。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Wide

値スペース: Focused/Wide

Focused: 1 点に集中された音の感度。デバイスの真正面にないソースからの音は抑制されます。

Wide: デフォルトのマイク動作で、通常の音声感度です。

Audio Microphones Mute Enabled

デバイスでのマイク ミュートの動作を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: True

値スペース: True/InCallOnly

True: 音声ミュートが使用可能になります。

InCallOnly: 音声ミュートはデバイスがコール中の場合にだけ使用できます。アイドル状態のときは、マイクをミュートにできません。これは、外部の電話サービスまたは音声システムがデバイスを介して接続されており、デバイスがコール中でないときに使用可能にする場合に便利です。InCallOnly に設定されたとき、音声システムが誤ってミュートにされることを防止できます。

Audio SoundsAndAlerts RingTone

着信コールに使用する着信音を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Sunrise

値スペース: Sunrise/Mischief/Ripples/Reflections/Vibes/Delight/Evolve/Playful/Ascent/Calculation/Mellow/Ringer

リストから呼び出し音を選択します。

Audio SoundsAndAlerts RingVolume

着信コールの着信音量を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: 50

値スペース: 整数 (0..100)

範囲: 値は 5 刻みで 0 ～ 100 (-34.5 dB ～ 15 dB) になります。音量 0 = オフです。

Audio Ultrasound Mode

この設定は、インテリジェント プロキシミティ機能に適用されます。設定はデフォルト値のままにしておいてください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : デバイスが超音波ボリュームを動的に調整します。ボリュームは、[オーディオ ウルトラサウンド最大音量 (Audio Ultrasound MaxVolume)] の設定で定義された最大レベルまでさまざまに変化します。

Static : Cisco が助言した場合にのみ使用してください。

Audio Ultrasound MaxVolume

この設定は、Intelligent Proximity 機能に適用されます。超音波のペアリング メッセージの最大音量を設定します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 70

値スペース : 整数 (0..70)

値は指定の範囲内から選択します。0 に設定すると、超音波がオフになります。

Bluetooth 設定

Bluetooth Allowed

デバイスは、組み込みの Bluetooth モジュールを備えています。デフォルトで、ユーザはユーザ インターフェイスを使用してオンとオフを切り替えることができます。この設定を使用すると、管理者は Bluetooth 設定を無効にしてユーザ インターフェイスからセットアップできないようすることができます。

必要なユーザ ロール : ADMIN

デフォルト値 : True

値スペース : False/True

False : 管理者が Bluetooth をオフにし、ユーザーがユーザ インターフェイスからオンにすることはできません。

True : Bluetooth が許可されます。ユーザが ユーザ インターフェイスを使用してオンとオフを切り替えることができます。

Bluetooth Enabled

Bluetooth 接続が許可されている場合 (Bluetooth 許可設定を参照) 、この設定を使用して Bluetooth を有効および無効にすることができます。ビデオ会議デバイスは HFP (ハンズフリー プロファイル) と A2DP (高度なオーディオ配信プロファイル) のプロファイルをサポートします。A2DP だけをサポートするヘッドセットは使用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : False

値スペース : False/True

False : Bluetooth は無効になり、ビデオ会議デバイスと Bluetooth デバイスはペアリングできません。

True : Bluetooth が有効になり、ペアリングを行って Bluetooth ヘッドセットを使用することができます。

CallHistory 設定

CallHistory Mode

不在着信や応答されなかったコールを含めて、発着信コールに関する情報を保存するかどうかを決定します（通話履歴）。これにより、ユーザ インターフェイスの Recents リストにコールが表示されるかどうかが決まります。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値：On

値スペース：Off/On

Off：新しいエントリが通話履歴に追加されません。

On：新しいエントリは通話履歴一覧に保存されます。

カメラ設定

Cameras Camera [n] Backlight DefaultMode

n: 1.. 1

このコンフィギュレーションは、逆光補正をオンまたはオフにします。逆光補正は、部屋の中で人物の背後に強い光がある場合に役立ちます。逆光補正がないと、こちらの画像が相手に非常に暗い状態で見えてしまいます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Off

値スペース : Off/On

Off : カメラの逆光補正をオフにします。

On : カメラの逆光補正をオンにします。

会議設定

Conference ActiveControl Mode

アクティブ コントロールは、会議参加者がビデオ会議デバイスのインターフェイスを使用して Cisco TelePresence Server または Cisco Meeting Server の会議を管理できる機能です。各ユーザは、参加者リストの表示、ビデオ レイアウトの変更、参加者の接続解除などをインターフェイスから行えます。アクティブ コントロール機能は、インフラストラクチャ (Cisco Unified Communications Manager (CUCM) バージョン 9.1.2 以降、Cisco TelePresence Video Communication Server (VCS) バージョン X8.1 以降、Cisco Media Server (CMS) バージョン 2.1 以降) でサポートされている限り、デフォルトでイネーブルです。アクティブ コントロール機能を無効にするには、この設定を変更します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Off

Auto : アクティブ コントロールがインフラストラクチャでサポートされている場合に有効になります。

Off : アクティブ コントロールは無効です。

Conference AutoAnswer Mode

自動応答モードを定義します。デバイスを使用してコールに応答する前に数秒間待機する場合は、Conference AutoAnswer Delay 設定を使用し、コールに応答するときにマイクをミュートする場合は Conference AutoAnswer Mute 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : [応答 (Answer)] をタップして着信コールに応答できます。

On : コール中でなければ、デバイスが自動的に着信コールに応答します。常に手動で、通話中の着信コールの応答や拒否が行えます。

Conference AutoAnswer Mute

着信コールに自動応答する場合にマイクをミュートにするかどうかを定義します。AutoAnswer Mode が有効にされている必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : 着信コールはミュートにされません。

On : 着信コールは自動的に応答されるときミュートにされます。

Conference AutoAnswer Delay

デバイスが自動応答するまで着信コールが待つ必要がある時間 (秒単位) を定義します。[自動応答モード (AutoAnswer Mode)] が有効にされている必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..50)

自動応答遅延 (秒単位) 。

Conference CallProtocolIPStack

デバイスで通信プロトコル (SIP、H323) の IPv4、IPv6、またはデュアル IP スタックを有効にする必要がある場合に選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Dual

値スペース : Dual/IPv4/IPv6

Dual : 通信プロトコルの IPv4 と IPv6 の両方をイネーブルにします。

IPv4 : [IPv4] に設定すると、通信プロトコルは IPv4 を使用します。

IPv6 : [IPv6] に設定すると、通信プロトコルは IPv6 を使用します。

Conference DefaultCall Protocol

デバイスからコールを発信するときに使用するデフォルトのコール プロトコルを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/H320/H323/Sip/Spark

Auto : 使用可能なプロトコルに基づいた通信プロトコルの自動選択をイネーブルにします。複数のプロトコルが使用可能な場合、優先順位は次の通りです : 1) SIP、2) H323、3) H320。デバイスが登録を実行できない場合、自動選択により H323 が選択されます。

H320 : すべてのコールが H.320 コールとしてセットアップされます (Cisco TelePresence ISDN リンクとともに使用している場合のみ) 。

H323 : すべてのコールが H.323 コールとして設定されます。

SIP : すべてのコールが SIP コールとして設定されます。

Spark : Webex 登録済みデバイスのために予約されています。使用しません。

Conference DefaultCall Rate

デバイスからコールを発信するときに使用するデフォルトのコール レートを定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR

Default value: 3072

値スペース : 整数 (64..3072)

デフォルト コール レート (kbps) です。

Conference DoNotDisturb DefaultTimeout

この設定はサイレント セッションのデフォルト期間、つまり着信コールが拒否され、不在履歴として登録される時間を決定します。セッションは、ユーザ インターフェイスを使用して早期に終了できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 60

値スペース : 整数 (1..1440)

DoNotDisturb (着信拒否) セッションが自動的にタイム アウトするまでの分数 (最大 1440 分、つまり 24 時間) 。

Conference Encryption Mode

会議の暗号化モードを定義します。会議が開始されると、数秒間画面に鍵と「Encryption On」または「Encryption Off」という文字が表示されます。

注 : 暗号化オプション キーがデバイスにインストールされていない場合、暗号化モードは常に [オフ (Off)] になります。

必要なユーザ ロール : ADMIN

デフォルト値 : BestEffort

値スペース : Off/On/BestEffort

Off : デバイスは暗号化を使用しません。

On : デバイスは、暗号化されたコールだけを許可します。

BestEffort : デバイスは暗号化を可能な限り使用します。

> ポイントツーポイント コール : 相手先デバイスで暗号化 (AES-128) がサポートされている場合、コールは暗号化されます。そうでない場合は、コールは暗号化なしで送信されます。

> MultiSite コール : 暗号化されたマルチサイト会議を実現するためには、すべてのサイトが暗号化をサポートしている必要があります。そうでない場合は、会議は暗号化されません。

Conference FarEndControl Mode

リモート側 (遠端) にこちら側のビデオ ソースの選択とローカル カメラの制御 (パン、傾斜、ズーム) を許可するかどうか決定できます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 相手先はこちら側のビデオ ソースの選択やローカル カメラの制御 (パン、チルト、ズーム) を許可されません。

On : 遠端にこちら側のビデオ ソースの選択とローカル カメラの制御 (パン、傾斜、ズーム) を許可します。カメラの制御とビデオ ソースの選択は、こちら側でも通常どおり可能です。

Conference FarEndControl SignalCapability

遠端制御 (H.224) 信号機能モードを定義します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : 遠端制御信号機能をディセーブルにします。
On : 遠端制御信号機能をイネーブルにします。

Conference FarEndMessage Mode

制御システムまたはマクロと併用するために、ポイントツーポイント コールにおける 2 台のデバイス間でデータ送信が許可されているかどうかを切り替えます。SIP コールでのみ動作します。この設定は、遠隔メッセージ送信コマンドの xCommand のコール使用を有効化または無効化します。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : 2 台のデバイス間でメッセージを送信できません。
On : ポイントツーポイント コールの 2 台のデバイス間でメッセージ送信を行うことができます。

Conference MaxReceiveCallRate

コールの発信または受信時に使用する最大受信ビット レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには、Conference MaxTotalReceiveCallRate 設定を使用します。

必要なユーザ ロール : ADMIN
Default value: 3072

値スペース : 整数 (64..3072)
最大受信帯域 (kbps) 。

Conference MaxTransmitCallRate

コールの発信または受信時に使用する最大送信ビット レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには、Conference MaxTotalTransmitCallRate 設定を使用します。

必要なユーザ ロール : ADMIN
Default value: 3072

値スペース : 整数 (64..3072)
最大送信帯域 (kbps) 。

Conference MaxTotalReceiveCallRate

受信全体の最大許容ビット レートを定義します。この製品は、同時に複数のコールをサポートしないため、合計送信帯域は 1 つのコールの送信ビット レートと同じになります (参照 : 会議の最大受信コールレート(Conference MaxReceiveCallRate) 設定) 。

必要なユーザ ロール : ADMIN
Default value: 3072

値スペース : 整数 (64..3072)
最大受信帯域 (kbps) 。

Conference MaxTotalTransmitCallRate

送信全体の最大許容ビット レートを定義します。この製品は、同時に複数のコールをサポートしないため、合計送信帯域は 1 つのコールの送信ビット レートと同じになります (参照 : Conference MaxTransmitCallRate 設定) 。

必要なユーザ ロール : ADMIN
Default value: 3072

値スペース : 整数 (64..3072)
最大送信帯域 (kbps) 。

Conference MicUnmuteOnDisconnect Mode

すべてのコールが切断されたときに、マイクを自動的にミュート解除するかどうかを定義します。会議室またはその他の共有リソースでは、次のユーザのためにデバイスを準備するためにこれを実行する場合があります。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : コール中にミュートにされている場合、コールが切断された後もマイクロフォンをミュートにされたままにします。

On : コールが切断された後にマイクロフォンのミュートを解除します。

Conference Multipoint Mode

ポイントツーポイント ビデオ コール (2 者間のコール) から、参加者を追加してマルチポイント会議 (アドホック会議) に拡大する方法を定義します。中央化されたインフラストラクチャ (マルチポイント制御ユニット、MCU) に基づいたさまざまなソリューションを利用できます。

デバイスによる会議への参加者の追加 (直接リモート追加) を許可している MCU をコールする場合、MCU を介してマルチパーティ会議がセットアップされます。

Cisco Unified Communications Manager (CUCM) バージョン 8.6.2 またはそれ以降に登録している場合、デバイスは CUCM 会議ブリッジを使用することもできます (CUCM で設定します) 。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/CUCMMediaResourceGroupList

Auto: 複数のビデオ デバイスを呼び出すことはできません。デバイスによる会議への参加者の追加 (直接リモート追加) を許可している MCU をコールする場合、MCU を介してマルチパーティ会議がセットアップされます。

CUCMMediaResourceGroupList : マルチパーティ会議は、CUCM で設定された会議ブリッジによってホストされます。この設定は、CUCM 環境で CUCM によってプロビジョニングされるため、ユーザが手動で設定すべきではありません。

Conference Presentation OnPlacedOnHold

リモート サイトで保留状態にされた後、プレゼンテーションを共有し続けるかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : NoAction

設定可能な値 : NoAction/Stop

NoAction : 保留しても、デバイスはプレゼンテーションの共有を停止しません。保留されている間はプレゼンテーションは共有されませんが、コールが再開されると自動的に継続されます。

Stop : リモート サイトで保留されると、デバイスはプレゼンテーションの共有を停止します。コールが再開されてもプレゼンテーションは継続されません。

Conference VideoBandwidth Mode

会議ビデオ帯域幅モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : ビデオ チャネルの使用可能な送信帯域幅が現在アクティブなチャネル間で分散されます。プレゼンテーションが存在しない場合は、メイン ビデオ チャネルがプレゼンテーション チャネルの帯域幅を使用します。

Static : 使用可能な送信帯域幅が、アクティブでない場合でも各ビデオ チャネルに割り当てられます。

FacilityService 設定

FacilityService Service [n] Type

n: 1.. 5

最大 5 種類のファシリティ サービスを同時にサポートできます。この設定で、どのようなサービスかを選択できます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Helpdesk

値スペース : Catering/Concierge/Emergency/Helpdesk/Security/Transportation/Other

Catering : ケータリング サービスには、このオプションを選択します。

Concierge : コンシェルジュ サービスには、このオプションを選択します。

Emergency : 緊急サービスには、このオプションを選択します。

Helpdesk : ヘルプ デスク サービスには、このオプションを選択します。

Security : セキュリティ サービスには、このオプションを選択します。

Transportation : 転送サービスには、このオプションを選択します。

Other : その他のオプションでカバーされないサービスには、このオプションを選択します。

FacilityService Service [n] Name

n: 1..5

ファシリティ サービスの名前を定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。名前は、上部バーの疑問符アイコンをタップすると表示されるファシリティ サービス コール ボタンに表示されます。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Service 1 : "Live Support" その他のサービス : ""

値スペース : 文字列 (0, 1024)

ファシリティ サービスの名前。

FacilityService Service [n] Number

n: 1..5

ファシリティ サービスの番号 (URI または電話番号) を定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: ""

値スペース : 文字列 (0, 1024)

ファシリティ サービスの番号 (URI または電話番号) 。

FacilityService Service [n] CallType

n: 1..5

各ファシリティ サービスのコール タイプを定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Video

値スペース : Audio/Video

Audio : オーディオ コールには、このオプションを選択します。

Video : ビデオ コールには、このオプションを選択します。

H323 設定

H323 Authentication Mode

H.323 プロファイルの認証モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : デバイスは H.323 ゲートキーパーに対して自身の認証を試行せず、通常の登録を試行します。

On : 認証が必要なことを H.323 ゲートキーパーから示されると、デバイスはゲートキーパーに対して自身の認証を試みます。デバイスとゲートキーパーの両方で、H323 Authentication LoginName と H323 Authentication Password の設定を定義する必要があります。

H323 Authentication LoginName

デバイスは認証のために、H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はデバイスから H.323 ゲートキーパーへの単方向の認証です。つまり、デバイスはゲートキーパーに認証されます。認証が不要であることを H.323 ゲートキーパーが示している場合でも、デバイスは登録を試行します。H.323 認証モードを有効にする必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

認証ログイン名。

H323 Authentication Password

デバイスは認証のために、H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はデバイスから H.323 ゲートキーパーへの単方向の認証です。つまり、デバイスはゲートキーパーに認証されます。認証が不要であることを H.323 ゲートキーパーが示している場合でも、デバイスは登録を試行します。H.323 認証モードを有効にする必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

認証パスワード。

H323 CallSetup Mode

H.323 コールを確立するときにゲートキーパーとダイレクト コールのどちらを使用するかを定義します。

ダイレクト H.323 コールは、H323 CallSetup Mode が Gatekeeper に設定されている場合も発信できます。

必要なユーザ ロール : ADMIN

デフォルト値 : Gatekeeper

値スペース : Direct/Gatekeeper

Direct : IP アドレスに直接ダイヤルすることによってのみ、H.323 コールを発信できます。

Gatekeeper : デバイスは、H.323 コールを発信するためにゲートキーパーを使用します。このオプションを選択する場合は、H323 Gatekeeper Address も設定する必要があります。

H323 Encryption KeySize

Advanced Encryption Standard (AES) 暗号化キーの確立時に使用する Diffie-Hellman キー交換方式の最小または最大のキー サイズを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Min1024bit

設定可能な値 : Max1024bit/Min1024bit/Min2048bit (最大 1024 ビット/最小 1024 ビット/最小 2048 ビット)

Max1024bit : 最大サイズは 1024 ビットです。

Min1024bit : 最小サイズは 1024 ビットです。

Min2048bit : 最小サイズは 2048 ビットです。

H323 Gatekeeper Address

ゲートキーパーの IP アドレスを定義します。H323 CallSetup Mode を Gatekeeper に設定する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

H323 H323Alias E164

H.323 エイリアス E.164 は、H.323 ゲートキーパーに設定された番号計画に従ってデバイスのアドレスを定義します。E.164 エイリアスは電話番号と同じであり、アクセス コードと結合される場合もあります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 30)

H.323 Alias E.164 のアドレス。使用できる文字は、0 ～ 9、*、# です。

H323 H323Alias ID

H.323 エイリアス ID を定義します。この ID は、H.323 ゲートキーパーでデバイスのアドレス指定に使用され、コール リストに表示されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 49)

H.323 エイリアス ID。例 : "firstname.lastname@company.com", "My H.323 Alias ID"

H323 NAT Mode

ファイアウォール トラバーサル テクノロジーは、ファイアウォール障壁を通過するセキュアなパスを作成し、外部のビデオ会議デバイスに接続されたときの音声またはビデオのデータの正しい交換を可能にします (IP トラフィックが NAT ルータを通過する場合) 。注 : NAT は、ゲートキーパーとの組み合わせでは動作しません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Auto/Off/On

Auto : H323 NAT アドレスと実際の IP アドレスのどちらをシグナリングに使用するかをデバイスが決定します。これにより、LAN 上のデバイス、または WAN のデバイスにコールを発信できるようになります。H323 NAT アドレスが間違っているか設定されていない場合、実際の IP アドレスが使用されます。

Off : デバイスは、実際の IP アドレスをシグナリングします。

On : デバイスは、Q.931 および H.245 内にある実際の IP アドレスの代わりに、設定された H323 NAT アドレスをシグナリングします。NAT サーバ アドレスは、スタートアップ メニューに [My IP Address: 10.0.2.1] と表示されます。H323 NAT アドレスが間違っているか設定されていない場合、H.323 コールは設定できません。

H323 NAT Address

NAT 対応ルータの外部/グローバル IP アドレスを定義します。ルータに送信されるパケットは、ビデオ会議デバイスにルーティングされます。ゲートキーパーに登録されている場合は NAT を使用できないことに注意してください。

ルータで、次のポートはビデオ会議デバイスの IP アドレスにルーティングする必要があります。

* ポート 1720

*ポート 5555-6555

*ポート 2326-2487

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

H323 PortAllocation

この設定は、H.323 コール シグナリングに使用される H.245 ポート番号に影響を与えます。

必要なユーザ ロール : ADMIN

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : TCP 接続を開くとき、使用するポートをシステムが割り当てます。このようにする理由は、後続のコールで同じポートを使用しないようにするためです。一部のファイアウォールはこれを攻撃の徴候と見なします。Dynamic を選択した場合、使用される H.323 ポートは 11000 ～ 20999 です。20999 に達すると 11000 から再スタートされます。ポートは、特定の範囲内でシステムによって自動的に選択されます。ファイアウォール管理者は、どのポートがいつ使用されるかを推定しようとしてはなりません。指示された範囲内の割り当てスキーマがより詳細な通知なしで変更されることがあるからです。

Static : スタティックに設定すると、スタティックに事前定義された範囲 [5555-6555] 内でポート指定されます。

HttpClient 設定

HttpClient Mode

HTTP(S) 要求および応答を使用する外部 HTTP(S) サーバとのコミュニケーションを許可または禁止します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : ビデオ会議デバイスは外部 HTTP(S) サーバと通信できません。

On : ビデオ会議デバイスは外部 HTTP(S) サーバと通信できます。

HttpClient AllowHTTP

HttpClient モード の設定は、外部 HTTPs サーバとの通信を許可または禁止するために使用されます。モード設定では HTTP と HTTPS の区別をしていません。HTTP の使用を許可または禁止するには、HttpClient AllowHTTP 設定を使用する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : True

値スペース : False/True

False : ビデオ会議デバイスは、HTTPS のみで通信できます。

True : ビデオ会議デバイスは HTTPS と HTTP の両方で通信できます。

HttpClient AllowInsecureHTTPS

サーバの証明書を最初に確認せずに、HTTPS を使用したサーバとの通信をビデオ会議デバイスに許可するかどうかを選択できます。

デバイスによる証明書検証プロセスのスキップを許可する設定になっていても、自動的にスキップされません。証明書検証なしでデータをサーバで交換するには AllowInsecureHTTPS パラメータを各 xCommand HttpClient コマンドで具体的に設定する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : False

値スペース : False/True

False : デバイスは常に、HTTPS サーバに有効な証明書があるかどうかを確認します。証明書の検証に失敗した場合、サーバとの通信は行われません。

True : デバイスは、サーバと通信する前に証明書検証プロセスをスキップできます。

HTTP フィードバック設定

HttpFeedback TlsVerify

この設定は、ビデオ会議デバイスが任意の HTTPS 通信のために HTTPS サーバに接続するときに適用されます (HTTP クライアントのPOST/PUT/PATCH/GET/DELETE コマンドを参照してください) 。電話帳、プロビジョニング、および外部ロギング サーバについては、Phonebook Server 1 TlsVerify、Provisioning TlsVerify および Logging External TlsVerify の設定を参照してください。

デバイスと HTTPS サーバ間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (プレインストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

一般に、HTTPS 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。このルールには次の 2 つの例外があります。1) 互換性の理由で、CUCM に登録されているデバイスの最小 TLS バージョンは 1.0 です。2) Webex クラウド サービスに登録されているデバイスは、常にバージョン 1.2 を使用します。

注 : アップグレード後にデバイスが初期設定にリセットされておらず、従来の NetworkServices HTTPS VerifyServerCertificate 設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスは HTTPS サーバの証明書を確認しません。

On : デバイスは、HTTPS サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

ロギングの設定

Logging Debug Wifi

このオプションを有効にすると、デバイスは、デバイスとアクセス ポイントの間の Wi-Fi 接続のセットアップやメンテナンスについて詳細な情報を記録します。この機能は、WiFi 接続に問題があった場合のトラブルシューティングに便利です。Wi-Fi 接続が期待通りに動作している場合は、この設定をオフにすることを推奨します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

オフ : 基本 Wi-Fi 情報だけをロギング。

オン : Wi-Fi 接続についての大量の情報をロギング。

Logging External Mode

デバイス ログをリモート syslog サーバに保管するかどうかを決定します。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

リモートサーバのアドレスをロギング外部サーバ アドレス設定に入力する必要があります。ロギング外部サーバ ポートセットに記載されていない限り、標準規格 syslog ポートが使用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : デバイス ログはリモート syslog サーバに保存されません。

On : デバイス ログはリモート syslog サーバに保存されます。

Logging External Protocol

リモート ロギング サーバに対して使用するプロトコルを決定します。syslog プロトコル over TLS (Transport Layer Security) 、またはプレーンテキストの syslog プロトコルのいずれかを使用できます。syslog プロトコルの詳細については、RFC 5424 を参照してください。

必要なユーザ ロール : ADMIN

デフォルト値 : SyslogTLS

値スペース : Syslog/SyslogTLS

Syslog : プレーン テキストの syslog プロトコル。

SyslogTLS : syslog プロトコル over TLS。

Logging External Server Address

リモート syslog サーバの IP アドレス。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Logging External Server Port

リモート syslog サーバがメッセージをリッスンするポート。0 に設定した場合、デバイスは標準の syslog ポートを使用します。syslog の標準 syslog ポートは 514 で、TLS を使用した syslog の標準 syslog ポートは 6514 です。

必要なユーザ ロール : ADMIN

デフォルト値: 514

値スペース : 整数 (0..65535)

リモート syslog サーバが使用しているポート番号。0 は、デバイスが標準 syslog ポートを使用することを意味します。

Logging External TlsVerify

この設定は、ビデオ会議デバイスがリモートの syslog サーバに接続している場合に適用されます。通常のログ作成 (Logging External Mode の設定を参照) と監査ログ (Security Audit Logging Mode の設定を参照) の両方に適用されます。

デバイスと syslog サーバの間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (プレインストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

syslog 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスは syslog サーバの証明書を確認しません。

On : デバイスは、syslog サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

Logging Internal Mode

システム ログをデバイス (ローカル ファイル) に保存するかどうかを決定します。これらは、ログ バンドルをデバイスからダウンロードした際に得られるファイルです。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : システム ログはデバイスに保存されません。

On : システム ログはデバイスに保存されます。

Logging Mode

デバイスのロギング モード (syslog サービス) を定義します。無効にすると、syslog サービスが起動せず、システムログと監査ログのほとんどが生成されません。履歴ログと通話履歴は影響を受けません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : システムのロギング サービスを無効にします。

On : システムのロギング サービスを有効にします。

マクロ設定

Macros Mode

マクロによって、ビデオ会議デバイスの一部を自動化できる JavaScript コードのスニペットを記述できます。これによりカスタム動作を作成します。デフォルトではマクロの使用は無効化されていますが、最初にマクロ エディタを開くときにデバイスでのマクロ使用を有効にするかどうか確認を求められます。デバイスのマクロの使用を手動で有効にする場合や、完全に無効にする場合は、この設定を使用します。マクロ エディタ内でのマクロの使用を無効にすることができます。ただし、デバイスがマクロをリセットするたびにマクロが自動的に再び有効化されるため、マクロの実行は永続的に無効にはなりません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : このデバイス上でのマクロの使用を完全に無効にします。

On : このデバイス上でのマクロの使用を有効にします。

Macros AutoStart

すべてのマクロは、マクロ ランタイムに呼び出され、ビデオ会議デバイスにおいてシングル プロセスで実行します。デフォルトでは実行されている必要がありますが、手動での停止と開始を選択することができます。自動開始が有効化されている場合、デバイスを再起動するときにランタイムは自動的に再び開始されます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスの再起動後、マクロ ランタイムは自動的に開始されません。

On : デバイスの再起動後、マクロ ランタイムは自動的に開始されます。

ネットワーク設定

Network [n] DNS DNSSEC Mode

n: 1..1

ドメイン ネーム システム セキュリティ拡張 (DNSSEC) は、DNS の拡張セットです。署名されたゾーンの DNS の応答を認証するために使用されます。署名されていないゾーンを引き続き許可します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : ドメイン ネーム システム セキュリティ拡張を無効にします。

On : ドメイン ネーム システム セキュリティ拡張を有効にします。

Network [n] DNS Domain Name

n: 1..1

DNS ドメイン名は非修飾名に追加されるデフォルトのドメイン名サフィックスです。

例 : DNS ドメイン名が「company.com」で、ルックアップする名前が「MyVideoSystem」の場合、DNS ルックアップ「MyVideoSystem.company.com」になります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

DNS ドメイン名。

Network [n] DNS Server [m] Address

n: 1..1

m: 1.. 3

DNS サーバのネットワーク アドレスを定義します。最大 3 つまでのアドレスを指定できます。ネットワーク アドレスが不明の場合、管理者またはインターネット サービス プロバイダーに問い合わせます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [n] IEEE8021X Mode

n: 1..1

デバイスは、ポート ベースのネットワーク アクセス コントロールによって、IEEE 802.1X LAN ネットワークに接続できます。このアクセス コントロールは、イーサネット ネットワークに認証済みネットワーク アクセスを提供するために使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : 802.1X 認証が無効になります。

On : 802.1X 認証が有効になります。

Network [n] IEEE8021X TlsVerify

n: 1..1

TLS を使用する場合の、ローカル CA リストの証明書に対する IEEE802.1x 接続のサーバ側証明書の検証です。CA リストをビデオ会議デバイスにアップロードする必要があります。これは、ウェブ インターフェイスから実行できます。

この設定は、Network [1] IEEE8021X Eap Tls が有効 (On) の場合にのみ有効です。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : Off に設定する場合、ローカル CA リストに対するサーバ側 X.509 証明書を確認せずに、TLS 接続が許可されます。これは、デバイスに CA リストがアップロードされていない場合に選択する必要があります。

On : On に設定する場合、すべての TLS 接続のローカル CA リストに対して、サーバ側 X.509 証明書が検証されます。有効な証明書を持つサーバだけが許可されます。

Network [n] IEEE8021X UseClientCertificate

n: 1..1

IEEE802.1x 接続中の、秘密キーと証明書のペアを使用した認証。認証 X.509 証明書がビデオ会議デバイスにアップロードされている必要があります。これは、ウェブ インターフェイスから実行できます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : Off に設定した場合、クライアント側の証明書は使用されません (サーバ側のみ) 。

On : On に設定した場合、クライアント (ビデオ会議デバイス) はサーバと相互認証 TLS ハンドシェイクを実行します。

Network [n] IEEE8021X Identity

n: 1..1

802.1X 認証用のユーザ名を定義します。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

802.1 X 認証用のユーザ名。

Network [n] IEEE8021X Password

n: 1..1

802.1X 認証用のパスワードを定義します。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 50)

802.1X 認証用のパスワード。

Network [n] IEEE8021X AnonymousIdentity

n: 1..1

802.1X 匿名 ID 文字列は、別のトンネリングされた ID をサポートする EAP-PEAP および EAP-TTLS などの EAP (Extensible Authentication Protocol) タイプとともに、非暗号化 ID として使用されます。設定された場合、匿名 ID は最初の (非暗号化) EAP ID 要求に使用されます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

802.1X 匿名 ID 文字列。

Network [n] IEEE8021X Eap Md5

n: 1..1

MD5 (メッセージダイジェスト アルゴリズム 5) モードを定義します。これは、共有秘密に依存するチャレンジ ハンドシェイク認証プロトコルです。MD5 は弱いセキュリティです。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-MD5 プロトコルはディセーブルになります。

On : EAP-MD5 プロトコルが有効になります。

Network [n] IEEE8021X Eap Ttls

n: 1..1

TTLS (トンネル方式トランスポート層セキュリティ) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Funk Software および Certicom によって開発されました。通常 Agere Systems、Proxim および Avaya でサポートされます。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-TTLS プロトコルはディセーブルになります。

On : EAP-TTLS プロトコルが有効になります。

Network [n] IEEE8021X Eap Tls

n: 1..1

IEEE802.1x 接続用の EAP-TLS (トランスポート層セキュリティ) の使用をイネーブルまたはディセーブルにします。RFC5216 で定義された EAP-TLS プロトコルは最もセキュアな EAP 標準の 1 つと見なされています。LAN クライアントは、クライアント証明書を使用して認証されます。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-TLS プロトコルはディセーブルになります。

On : EAP-TLS プロトコルが有効になります。

Network [n] IEEE8021X Eap Peap

n: 1..1

PEAP (Protected Extensible Authentication Protocol) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Microsoft、Cisco と RSA Security により開発されました。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-PEAP プロトコルはディセーブルになります。

On : EAP-PEAP プロトコルが有効になります。

Network [n] IPStack

n: 1..1

デバイスのネットワーク インターフェイスで IPv4、IPv6、またはデュアル IP スタックを使用する必要がある場合に選択します。注 : この設定を変更した後、反映されるまでに 30 秒間待つ必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Dual

値スペース : Dual/IPv4/IPv6

Dual : [デュアル (Dual)] に設定すると、ネットワーク インターフェイスは両方の IP バージョンで同時に動作することができ、また、IPv4 アドレスと IPv6 アドレスの両方を同時に持つことができます。

IPv4 : IPv4 に設定すると、デバイスのネットワーク インターフェイスで IPv4 が使用されます。

IPv6 : IPv6 に設定すると、デバイスのネットワーク インターフェイスで IPv6 が使用されます。

Network [n] IPv4 Assignment

n: 1..1

デバイスが IPv4 アドレス、サブネット マスク、およびゲートウェイ アドレスを取得する方法を定義します。

アドレス割り当てに DHCP を利用する場合は、MAC アドレスによって最後に付加される「01」が、DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : DHCP

値スペース : Static/DHCP

Static : アドレスは、Network IPv4 Address、Network IPv4 Gateway、Network IPv4 SubnetMask の各設定 (静的アドレス) を使用して手動で設定する必要があります。

DHCP : デバイス アドレスは DHCP サーバによって自動的に割り当てられます。

Network [n] IPv4 Address

n: 1..1

デバイスのスタティック IPv4 ネットワーク アドレスを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

Network [n] IPv4 Gateway

n: 1..1

IPv4 ネットワーク ゲートウェイ アドレスを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

Network [n] IPv4 SubnetMask

n: 1..1

IPv4 ネットワークのサブネット マスクを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

Network [n] IPv6 Assignment

n: 1..1

デバイスが IPv6 アドレスおよびデフォルト ゲートウェイ アドレスを取得する方法を定義します。

アドレス割り当てに DHCPv6 を利用する場合は、MAC アドレスによって最後に付加される「01」が、DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : Autoconf

値スペース : Static/DHCPv6/Autoconf

Static : デバイスおよびゲートウェイの IP アドレスは、Network IPv6 Address および Network IPv6 Gateway の設定を使用して手動で設定する必要があります。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。

DHCPv6 : オプションを含むすべての IPv6 アドレスは、DHCPv6 サーバから取得されます。詳細については RFC3315 を参照してください。Network IPv6 DHCPOption 設定は無視されます。

Autoconf : IPv6 ネットワーク インターフェイスの IPv6 ステートレス自動設定をイネーブルにします。詳細については RFC4862 を参照してください。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。

Network [n] IPv6 Address

n: 1..1

デバイスのスタティック IPv6 ネットワーク アドレスを定義します。Network IPv6 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

ネットワーク マスクを含む有効な IPv6 アドレス。例 : 2001:DB8::/48

Network [n] IPv6 Gateway

n: 1..1

IPv6 ネットワーク ゲートウェイ アドレスを定義します。この設定は、Network IPv6 Assignment が Static に設定されている場合にのみ適用されます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv6 アドレス。

Network [n] IPv6 DHCPOptions

n: 1..1

DHCPv6 サーバから一連の DHCP オプション (NTP および DNS サーバ アドレスなど) を取得します。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : DHCPv6 サーバからの DHCP オプションの取得を無効にします。

On : 選択した DHCP オプションのセットの DHCPv6 サーバからの取得をイネーブルにします。

Network [n] MTU

n: 1..1

イーサネット MTU (最大伝送ユニット) サイズを定義します。MTU サイズは、ネットワーク インフラストラクチャでサポートする必要があります。IPv4 の場合、最小サイズは 576 で、IPv6 の場合、最小サイズは 1280 です。

必要なユーザ ロール : admin、user

デフォルト値: 1500

値スペース : 整数 (576..1500)

MTU の値を設定します (バイト単位) 。

Network [n] QoS Mode

n: 1..1

QoS (Quality of Service) は、ネットワーク内のオーディオ、ビデオおよびデータの優先順位を操作するメソッドです。QoS 設定はインフラストラクチャでサポートされている必要があります。DiffServ (ディファレンシエーテッド サービス) は、ネットワーク トラフィックの分類と管理を行い、現代的 IP ネットワークに QoS を提供するためにシンプルかつスケーラブルで粗粒度のメカニズムを指定する、コンピュータ ネットワーキング アーキテクチャです。

必要なユーザ ロール : admin、user

デフォルト値 : Diffserv

値スペース : Off/Diffserv

Off : QoS メソッドは使用されません。

Diffserv : QoS モードを Diffserv に設定すると、Network QoS Diffserv Audio、Network QoS Diffserv Video、Network QoS Diffserv Data、Network QoS Diffserv Signalling、Network QoS Diffserv ICMPv6、および Network QoS Diffserv NTP の各設定を使用してパケットの優先順位が付けられます。

Network [n] QoS Diffserv Audio

n: 1..1

この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。音声に推奨されるクラスは、10 進数値 32 と等しい CS4 です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの音声パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv Video

n: 1..1

この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でビデオ パケットに持たせる優先順位を定義します。プレゼンテーション チャネル (共有コンテンツ) 上のパケットも、ビデオ パケットのカテゴリに属します。パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。ビデオに推奨されるクラスは、10 進数値 32 と等しい CS4 です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでのビデオ パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv Data

n: 1..1

この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。データに対する推奨値は 0 (ベスト エフォート) です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでのデータ パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv Signalling

n: 1..1

この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でリアルタイム処理に不可欠 (時間依存) であると考えられるシグナリング パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。シグナリングに推奨されるクラスは、10 進数値 24 と等しい CS3 です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの信号パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv ICMPv6

n: 1..1

この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で ICMPv6 パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。ICMPv6 に対する推奨値は 0 (ベスト エフォート) です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの ICMPv6 パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv NTP

n: 1..1

この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。NTP に対する推奨値は 0 (ベスト エフォート) です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの NTP パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] RemoteAccess Allow

n: 1..1

リモート アクセスで SSH、Telenet、HTTP、HTTPS からデバイスに許可する IP アドレス (IPv4/IPv6) を定義します。複数の IP アドレスはスペースで区切られます。

ネットワーク マスク (IP 範囲) は <ip address>/N で指定されます。ここで N は IPv4 では 1 ～ 32 の範囲および IPv6 では 1 ～ 128 の範囲を表します。/N は最初の N ビットがセットされたネットワーク マスクの共通インジケータです。たとえば 192.168.0.0/24 は、192.168.0 で開始するどのアドレスとも一致します。これらはアドレスの最初の 24 ビットだからです。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [n] Speed

n: 1..1

イーサネット リンクの速度を定義します。デフォルト値では、ネットワークとネゴシエートして自動的に速度が設定されます。このため、デフォルト値は変更しないことをお勧めします。自動ネゴシエーションを使用しない場合、選択した速度を、ネットワーク インフラストラクチャの最も近いスイッチがサポートしているか確認してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/10half/10full/100half/100full/1000full

Auto : リンク速度を自動でネゴシエートします。

10half : 10 Mbps 半二重に強制リンクします。

10full : 10 Mbps 全二重に強制リンクします。

100half : 100 Mbps 半二重に強制リンクします。

100full : 100 Mbps 全二重に強制リンクします。

1000full : 1 Gbps 全二重に強制リンクします。

Network [n] TrafficControl Mode

n: 1..1

ネットワーク トラフィック制御モードを定義して、ビデオ パケットの伝送速度の制御方法を決定します。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : ビデオ パケットをリンク速度で送信します。

On : ビデオ パケットを最大 20 Mbps で送信します。発信ネットワーク トラフィックのバーストを平滑化するために使用できます。

Network [n] VLAN Voice Mode

n: 1..1

VLAN 音声モードを定義します。Cisco UCM (Cisco Unified Communications Manager) をプロビジョニング インフラストラクチャとして使用している場合、VLAN Voice Mode が Auto に自動的に設定されます。NetworkServices CDP Mode 設定が Off になっている場合は、Auto モードは機能しないことに注意してください。

必要なユーザ ロール : admin、user

デフォルト値 : Auto

値スペース : Auto/Manual/Off

Auto : Cisco Discovery Protocol (CDP) が使用可能な場合は、音声 VLAN に ID を割り当てます。CDP を使用できない場合、VLAN はイネーブルになりません。

Manual : VLAN ID は、Network VLAN Voice VlanId の設定を使用して手動で設定されます。CDP を使用できる場合、手動設定値は、CDP によって割り当てられた値によって却下されます。

Off : VLAN はイネーブルになりません。

Network [n] VLAN Voice VlanId

n: 1..1

VLAN 音声 ID を定義します。この設定は、ネットワーク VLAN 音声モード が Manual に設定されている場合にだけ有効になります。

必要なユーザ ロール : admin、user

デフォルト値: 1

値スペース : 整数 (1..4094)

VLAN 音声 ID を設定します。

NetworkPort 設定

NetworkPort [n] Mode

n: 2.. 2

ビデオ会議デバイスには、2 つのネットワークポートがあります。最初のネットワーク ポートは、デバイスをイーサネット LAN に接続するためのものです。2 番目のネットワーク ポート（コンピュータ ネットワーク ポートとも呼ばれます）では、デバイスを介してイーサネット LAN にコンピュータを接続することができます。このように、ネットワーク コンセントが 1 つあればデバイスとコンピュータの両方をサポートすることができます。

公共の場所でビデオ会議デバイスを使用する場合は、ユーザーがデバイスを介してコンピュータをネットワーク接続することを防ぐため、このネットワーク ポートを無効にすることをお勧めします。

この設定への変更を反映させるには、デバイスを再起動する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : コンピュータ ネットワーク ポートは無効です。

On : コンピュータ ネットワーク ポートは使用可能です。

ネットワークサービス設定

NetworkServices CDP Mode

CDP (Cisco Discovery Protocol) デーモンをイネーブルまたはディセーブルにします。CDP を有効にすると、デバイスは特定の統計情報とデバイス ID を CDP 対応スイッチにレポートします。CDP をディセーブルにする場合、[ネットワーク音声 VLAN モード (Network VLAN Voice Mode)] : [自動 (Auto)] 設定は機能しません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : CDP デーモンは無効です。

On : CDP デーモンはイネーブルです。

NetworkServices H323 Mode

デバイスでの H.323 コールの受発信を可能にするかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : H.323 コールの発信と受信の可能性をディセーブルにします。

On : H.323 コールの発信と受信の可能性を有効にします。

NetworkServices HTTP Mode

HTTP または HTTPS (セキュア HTTP) プロトコルによるデバイスへのアクセスを許可するかどうかを指定します。デバイスの Web インターフェイスは HTTP または HTTPS を使用することに注意してください。この設定を Off にすると、ウェブ インターフェイスを使用できなくなります。

セキュリティの強化 (ウェブ サーバから返されるページと要求の暗号化/暗号化解除) が必要な場合、HTTPS のみを許可します。

注 : 以前のソフトウェア バージョンから CE9.4 以降にアップグレードされたデバイスについては、アップグレード後に初期設定にリセットされていない場合、デフォルト値は HTTP+HTTPS となります。

必要なユーザ ロール : ADMIN

デフォルト値 : HTTPS (CE9.4 では HTTP +]HTTPS から HTTPS に変更)

値スペース : Off/HTTP+HTTPS/HTTPS

Off : HTTP や HTTPS によるデバイスへのアクセスを禁止します。

HTTP+HTTPS : HTTP と HTTPS の両方によるデバイスへのアクセスを許可します。

HTTPS : HTTPS によるデバイスへのアクセスを許可し、HTTP によるアクセスを禁止します。

NetworkServices HTTP Proxy LoginName

これは、HTTP プロキシに対する認証に使用されるクレデンシャルのユーザ名部分です。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が手動に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 80)

認証ログイン名。

NetworkServices HTTP Proxy Password

これは、HTTP プロキシへの認証に使われるクレデンシャルのパスワード部分です。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が手動に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

認証パスワード。

NetworkServices HTTP Proxy Mode

Cisco Webex クラウド サービスに登録されているデバイスを設定して、HTTPS および WebSocket トラフィックにプロキシ サーバを使用することができます。Cisco Webex の HTTP プロキシを手動でセットアップすることができます。自動設定 (PACUrl) 、完全自動 (WPAD) 、またはオフにしておくことができます。

デバイスが CUCM または VCS などのオンプレミス サービスに登録されている場合は、この設定を [オフ (Off)] のままにしておきます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Manual/Off/PACUrl/WPAD

Manual : ネットワーク サービス HTTP プロキシ URL 設定にプロキシ サーバのアドレスを入力します。必要応じて、ネットワーク サービス HTTP プロキシ ログイン名/パスワード設定に HTTP プロキシのログイン名とパスワードを追加します。

Off : HTTP プロキシ モードがオフになっています。

PACUrl : HTTP プロキシは自動構成です。ネットワーク サービス HTTP プロキシ PACUrl 設定で PAC (プロキシ自動設定) スクリプトの URL を入力する必要があります。

WPAD : WPAD (Web プロキシ自動検出) を使用して、HTTP のプロキシは完全に自動化されかつ自動構成されます。

NetworkServices HTTP Proxy Url

HTTP プロキシ サーバの URL を設定します。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が手動に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

HTTP プロキシ サーバの URL。

NetworkServices HTTP Proxy PACUrl

PAC (プロキシ自動構成) スクリプトの URL を設定します。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が PACUrl に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

PAC (プロキシ自動構成) スクリプトの URL。

NetworkServices HTTPS OCSP Mode

OCSP (Online Certificate Status Protocol) レスポンダ サービスのサポートを定義します。OCSP 機能により、証明書失効リスト (CRL) の代わりに OCSP を有効にして、証明書のステータスをチェックできます。

すべての発信 HTTPS 接続に対して、OCSP レスポンダを介してステータスが照会されます。対応する証明書が失効している場合、HTTPS 接続は使用されません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : OCSP サポートをディセーブルにします。

On : OCSP サポートをイネーブルにします。

NetworkServices HTTPS OCSP URL

証明書のステータスを調べるために使用される OCSP レスポンダ (サーバ) の URL を定義します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な URL。

NetworkServices HTTPS Server MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN
デフォルト値 : TLSv1.1

値スペース : TLSv1.1/TLSv1.2
TLSv1.1 : TLS バージョン 1.1 以降のサポート。
TLSv1.2 : TLS バージョン 1.2 以降のサポート。

NetworkServices HTTPS StrictTransportSecurity

HTTP Strict Transport Security ヘッダーにより、ウェブ サイトからブラウザに対して、サイトを HTTP を使用してロードすることを避け、サイトへの HTTP を使用したアクセスはすべて HTTPS リクエストに自動変換する必要があることを通知します。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : HTTP Strict Transport Security 機能が無効になります。
On : HTTP Strict Transport Security 機能が有効になります。

NetworkServices HTTPS VerifyClientCertificate

ビデオ会議デバイスが HTTPS クライアント (Web ブラウザなど) に接続するときに、クライアントは自身を識別するためにビデオ会議デバイスに証明書を提示するように要求されることがあります。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : クライアント証明書を確認しません。
On : 信頼できる認証局 (CA) によって署名された証明書を提示するようクライアントに要求します。これには、信頼できる CA のリストがデバイスに事前にアップロードされている必要があります。

NetworkServices NTP Mode

ネットワーク タイム プロトコル (NTP) は、リファレンス タイム サーバにデバイスの時刻と日付を同期するために使用されます。時間の更新のために、タイム サーバに定期的に照会します。

必要なユーザ ロール : ADMIN
デフォルト値 : Auto

値スペース : Auto/Manual/Off
Auto : デバイスは時間を参照するために NTP サーバを使用します。デフォルトでは、サーバのアドレスはネットワークの DHCP サーバから取得されます。DHCP サーバを使用しない場合や、DHCP サーバが NTP サーバのアドレスを提供しない場合は、NetworkServices NTP Server [n] Address 設定で指定された NTP サーバ アドレスが使用されます。
Manual : デバイスは、NetworkServices NTP Server [n] Address 設定で指定された NTP サーバを使って時間を参照します。
Off : デバイスは NTP サーバを使用しません。NetworkServices NTP Server [n] Address 設定は無視されます。

NetworkServices NTP Server [n] Address

n: 1..3

NetworkServices NTP Mode が Manual に設定された場合、および NetworkServices NTP Mode が Auto に設定されアドレスが DHCP サーバから提供されない場合に使用される NTP サーバのアドレスです。

必要なユーザ ロール : ADMIN

デフォルト値 : "0.tandberg.pool.ntp.org"

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

NetworkServices NTP Server [n] Key

n: 1..3

NTP 情報が信頼できるソースからのものであることを確かめるためには、ビデオ会議デバイスは NTP ソースが使用する ID またはキー ペアを知っている必要があります。キーおよび ID それぞれの設定には、NetworkServices NTP サーバ [n] キーおよび NetworkServices NTP サーバ [n] KeyId 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 20)

NTP ソースが使用する IDまたはキーペアの一部であるキー。

NetworkServices NTP Server [n] KeyId

n: 1..3

NTP 情報が信頼できるソースからのものであることを確かめるためには、ビデオ会議デバイスは NTP ソースが使用する ID またはキー ペアを知っている必要があります。キーおよび ID それぞれの設定には、NetworkServices NTP サーバ [n] キーおよび NetworkServices NTP サーバ [n] KeyId 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 10)

NTP ソースが使用する ID/キーペアの一部である ID。

NetworkServices NTP Server [n] KeyAlgorithn

n: 1..3

NTP サーバが使用する認証ハッシュ機能を選択します。これは、ビデオ会議デバイスが時間メッセージの認証に使用する必要があるものです。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース: None/SHA1/SHA256

None : NTPサーバはハッシュ機能を使用しません。

SHA1: NTPサーバは SHA-1 ハッシュ機能を使用します。

SHA256: NTP サーバは SHA-256 ハッシュ機能を使用します (ハッシュ機能の SHA-2 群から) 。

NetworkServices SIP Mode

デバイスで SIP コールの発信および受信を可能にするかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : SIP コールの発信と受信の可能性をディセーブルにします。

On : SIP コールの発信と受信の可能性を有効にします。

NetworkServices SNMP Mode

ネットワーク管理システムでは、管理上の対応を補償する条件についてネットワーク接続デバイス（ルータ、サーバ、スイッチ、プロジェクタなど）をモニタするために SNMP（簡易ネットワーク管理プロトコル）が使用されます。保証の管理上の注意使用されます。SNMP は、デバイス設定を表す変数の形式で管理対象デバイス上の管理データを公開します。これらの変数は、その後照会でき（Readonly に設定）、管理アプリケーションによって設定できる場合もあります（ReadWrite に設定）。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値：ReadOnly

値スペース：Off/ReadOnly/ReadWrite

Off：SNMP ネットワーク サービスを無効にします。

ReadOnly：SNMP ネットワーク サービスを照会のみイネーブルにします。

ReadWrite：SNMP ネットワーク サービスの照会とコマンドの両方をイネーブルにします。

NetworkServices SNMP Host [n] Address

n: 1..3

最大 3 つの SNMP マネージャのアドレスを定義します。

デバイスの SNMP エージェント（コーデック内）は、デバイスの位置や連絡先などについて、SNMP マネージャ（PC プログラムなど）からのリクエストに応答します。SNMP トラップはサポートされていません。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

NetworkServices SNMP CommunityName

ネットワーク サービス SNMP コミュニティの名前を定義します。SNMP コミュニティ名は SNMP 要求を認証するために使用されます。SNMP 要求は、デバイスの SNMP エージェントから応答を受け取るため、パスワード（大文字と小文字を区別）を持つ必要があります。デフォルトのパスワードは「public」です。Cisco TelePresence 管理スイート（TMS）がある場合、同じ SNMP コミュニティがそこで設定されていることを確認する必要があります。注：SNMP コミュニティのパスワードは大文字と小文字が区別されます。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0, 50)

SNMP コミュニティ名。

NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システムの連絡先の名前を定義します。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0, 50)

SNMP システム接点の名前。

NetworkServices SNMP SystemLocation

ネットワーク サービス SNMP システム ロケーションの名前を定義します。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0, 50)

SNMP システム ロケーションの名前。

NetworkServices SSH Mode

SSH (Secure Shell) プロトコルは、ビデオ会議デバイスとローカル コンピュータの間でセキュアな暗号化通信を提供できます。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : SSH プロトコルは無効になります。
On : SSH プロトコルはイネーブルになります (デフォルト) 。

NetworkServices SSH HostKeyAlgorithm

SSH ホストキーに使用される暗号化アルゴリズムを選択します。2048 ビットのキーサイズを用いる RSA (リベスト・シャミル・エイドルマンアルゴリズム) 、NIST 曲線の P-384 を用いる ECDSA (楕円曲線デジタル署名アルゴリズム) 、ed25519 署名方式を用いる EdDSA (エドワード曲線デジタル署名アルゴリズム) から選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : RSA

設定可能な値 : ECDSA/RSA/ed25519
ECDSA : ECDSA アルゴリズムを使用します (nist-384p)。
RSA : RSA アルゴリズムを使用します (2048 bits)。
ed25519 : ed25519 アルゴリズムを使用します。

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) 公開キー認証をデバイスへのアクセスに使用できます。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : SSH 公開キーは許可されません。
On : SSH 公開キーが許可されます。

NetworkServices Telnet Mode

Telnet は、インターネットまたはローカル エリア ネットワーク (LAN) 接続で使用されるネットワーク プロトコルです。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : Telnet プロトコルは無効になります。これが出荷時の設定です。
On : Telnet プロトコルはイネーブルになります。

NetworkServices Websocket

非セキュアおよびセキュア バージョン (ws および wss) の両方で、デバイスの API に WebSocket プロトコルから相互作用することができます。WebSocket は HTTP に結びついているので、HTTP または HTTPS を有効にしてから WebSockets を使用する必要があります (NetworkServices HTTP モード設定を参照) 。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : FollowHTTPService/Off
FollowHTTPService: HTTP または HTTTPS が有効な場合、WebSocket プロトコル経由での通信は許可されます。
Off : WebSocket プロトコル経由での通信は許可されません。

NetworkServices WelcomeText

Telnet または SSH 経由でデバイスにログインする際に、ユーザーに表示する情報を選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : ようこそテキストは次のとおりです : ログインに成功しました (Login successfu)
On : ようこそテキストは次のとおりです : <システム名>; ソフトウェア バージョン; ソフトウェアのリリース日; ログインに成功しました (Login successful)

NetworkServices Wifi Allowed

Wi-Fi アダプタが組み込まれているデバイスは、イーサネットまたは Wi-Fi 経由でネットワークに接続できます。イーサネットと Wi-Fi の両方がデフォルトで許可され、ユーザはどちらを使用するかをユーザ インターフェイスから選択できます。この設定を使用して、管理者はユーザ インターフェイスがセットアップできないように Wi-Fi 設定を無効にすることができます。

このDebaisu は次の標準規格をサポートしています : IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、および IEEE 802.11n。デバイスは次のセキュリティ プロトコルをサポートします : WPA-PSK (AES) 、WPA2-PSK (AES) 、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP、EAP-MSCHAPv2 、EAP-GTC、およびオープン ネットワーク (セキュリティ保護なし) 。

デバイスの背面の定格ラベルに記載されている PID (製品 ID) に NR (無線なし) の文字が含まれている場合、デバイスは Wi-Fi をサポートしていません。

必要なユーザ ロール : admin、user

デフォルト値 : True

値スペース : False/True

False : Wi-Fi は使用できません。イーサネット経由でネットワークに接続する必要があります。

True : イーサネットと Wi-Fi の両方を使用できます。

NetworkServices Wifi Enabled

デバイスが Wi-Fi 経由でのネットワーク接続を許可されている場合 (NetworkServices WIFI Allowed 設定を参照) 、この設定を使用して Wi-Fi を有効または無効にすることができます。

イーサネットと Wi-Fi の両方を同時に使用することはできません。Wi-Fi を設定するときにイーサネット ケーブルが接続されている場合、そのイーサネット ケーブルを抜かないと続行できません。Wi-Fi に接続している最中にイーサネット ケーブルを接続すると、イーサネットが優先されます。イーサネット ケーブルを抜いた場合、前回接続した Wi-Fi ネットワークが使用可能であれば、デバイスはそのネットワークに自動的に接続します。

必要なユーザ ロール : admin、user

デフォルト値 : True

値スペース : False/True

False : Wi-Fi は無効になります。

True : Wi-Fi が有効になります。

NetworkServices XMLAPI Mode

デバイスの XML API を有効化または無効化します。セキュリティ上の理由からこれを無効にできます。XML API を無効化にすると、TMS などによるリモート管理機能が制限され、デバイスに接続できなくなります。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : XML API は無効になります。

On : XML API は有効になります。

周辺機器の設定

Peripherals InputDevice Mode

USB キーボードまたはワイヤレスリモート制御などのサードパーティー入力デバイスの、USB ドングルとの使用を許可するかどうかを定義します。入力デバイスはそれ自体を USB キーボードとしてアドバタイズする必要があります。ご自身で、キークリックに対する応答として行うアクションを定義して実装する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : サードパーティー入力デバイスは許可されません。

On : サードパーティ製の USB 入力デバイスを使用して、ビデオ会議デバイスの特定の機能を制御できます。

Peripherals Profile ControlSystems

サードパーティ製コントロール システム (Crestron または AMX など) をビデオ会議デバイスに接続する予定であれば、定義します。この情報はビデオ会議デバイスの診断サービスで使用します。接続された制御システムの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。サードパーティ制御システムは 1 つのみサポートされるので注意してください。

1 に設定する場合、xCommand Peripherals Pair コマンドおよび HeartBeat コマンドを使用して、制御システムからビデオ会議デバイスにハート ビートを送信する必要があります。これに失敗すると、ビデオ会議デバイスは、コントロール システムへの接続が失われたことを示す警告を表示します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : NotSet

値スペース : 1/NotSet

1 : 1 つのサードパーティ製コントロール システムをデバイスに接続する必要があります。

NotSet : サードパーティ製の制御システムの存在に対するチェックは実行されません。

電話帳の設定

Phonebook Server [n] ID

n: 1..1

外部の電話帳の名前を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 64)

外部の電話帳の名前。

Phonebook Server [n] Pagination

n: 1..1

電話帳サーバがページネーション(ウェルカムページ) に対応するかどうかを定義します。ページネーションとはサーバが連続検索に対応しているかどうか、さらにこれらの検索がオフセットに関連付けられるかどうかを意味します。これにより、ユーザインターフェイスは完全な検索結果を得るために必要な可能な限り多くの連続検索を実行できます。

ページネーションが無効の場合、デバイスは検索を 1 度行い、最大 100 エントリを検索結果に返します。それ以上の検索結果をさらにスクロールすることはできません。

必要なユーザ ロール : ADMIN

デフォルト値 : Enabled

値スペース : Disabled/Enabled

Disabled : 電話帳サーバはページネーションに対応しません。デバイスは 1 回の検索を実行します。検索結果の最大エントリ数は 100 です。

Enabled : 電話帳サーバはページネーションに対応しています。

Phonebook Server [n] TlsVerify

この設定は、ビデオ会議デバイスが HTTPS 経由で外部の電話帳サーバに接続するときに適用されます。

デバイスと HTTPS サーバ間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (プレインストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

一般に、HTTPS 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。このルールには次の 2 つの例外があります。1) 互換性の理由で、CUCM に登録されているデバイスの最小 TLS バージョンは 1.0 です。2) Webex クラウド サービスに登録されているデバイスは、常にバージョン 1.2 を使用します。

注 : アップグレード後にデバイスが初期設定にリセットされておらず、従来の NetworkServices HTTPS VerifyServerCertificate 設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスは HTTPS サーバの証明書を確認しません。

On : デバイスは、HTTPS サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

Phonebook Server [n] Type

n: 1..1

電話帳サーバの種類を選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/CUCM/Spark/TMS/VCS
Off : 電話帳を使用しません。
CUCM : 電話帳が Cisco Unified Communications Manager 上に配置されます。
Spark: 電話帳が Cisco Webex クラウドサービス内に配置されます。
TMS : 電話帳が Cisco TelePresence Management Suite サーバ上に配置されます。
VCS : 電話帳が Cisco TelePresence Video Communication Server 上に配置されます。

Phonebook Server [n] URL

n: 1..1

外部電話帳サーバへのアドレス (URL) を定義します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
外部電話帳サーバの有効なアドレス (URL) 。

プロビジョニング設定

Provisioning Connectivity

この設定は、プロビジョニング サーバからの内部または外部のコンフィギュレーションを要求するかどうかを、デバイスがどのように検出するか制御します。

必要なユーザ ロール : admin、user

デフォルト値 : Auto

値スペース : Internal/External/Auto

Internal : 内部コンフィギュレーションを要求します。

External : 外部コンフィギュレーションを要求します。

Auto : 内部または外部のコンフィギュレーションを要求するかどうかを自動的に NAPTR クエリーを使用して検出します。NAPTR の応答に「e」フラグがある場合、外部コンフィギュレーションが要求されます。それ以外の場合、内部コンフィギュレーションが要求されます。

Provisioning ExternalManager Address

外部のマネージャ システムまたはプロビジョニング システムの IP アドレスまたは DNS 名を定義します。

外部マネージャのアドレス (およびパス) が設定されている場合、デバイスは起動時にこのアドレスにメッセージを送信します。このメッセージを受信すると、結果として外部マネージャ/プロビジョニング システムはそのユニットにコンフィギュレーション/コマンドを返すことができます。

CUCM または TMS プロビジョニングを使用する場合、外部マネージャ アドレスを自動的に提供するために DHCP サーバをセットアップできます (TMS には DHCP オプション 242、CUCM には DHCP オプション 150) 。プロビジョニング 外部マネージャーアドレス で設定されたアドレスは、DHCP によって提供されるアドレスを上書きします。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Provisioning ExternalManager AlternateAddress

デバイスが Cisco Unified Communications Manager (CUCM) でプロビジョニングされており、冗長構成として代替の CUCM が利用可能な場合にのみ使用できます。代替 CUCM のアドレスを定義します。メインの CUCM が使用できない場合、デバイスは代替 CUCM でプロビジョニングされます。メインの CUCM が再び使用可能になると、デバイスはこの CUCM によってプロビジョニングされます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Provisioning ExternalManager Protocol

外部のマネージャ システムまたはプロビジョニング システムに要求を送信する際に、HTTP (非セキュアな通信) または HTTPS (セキュアな通信) のどちらのプロトコルを使用するかを定義します。

選択したプロトコルは、NetworkServices HTTP Mode の設定で有効になっている必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : HTTP

値スペース : HTTPS/HTTP

HTTPS : HTTPS を介してリクエストを送信します。

HTTP : HTTP を介してリクエストを送信します。

Provisioning ExternalManager Path

外部のマネージャ システムまたはプロビジョニング システムへのパスを定義します。いくつかの管理サービスが同じサーバに存在する、つまり同じ外部マネージャのアドレスを共有する場合、この設定が必要です。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

外部のマネージャー システムまたはプロビジョニング システムへの有効なパス。

Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを定義します。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効なドメイン名。

Provisioning Mode

プロビジョニング システム (外部マネージャ) を使用してデバイスを設定できます。これにより、ビデオ会議のネットワーク管理者は複数のデバイスを同時に管理することができます。この設定により、使用するプロビジョニング システムの種類を選択します。プロビジョニングは、オフに切り替えることも可能です。詳細については、プロビジョニング システムのプロバイダー/担当者にお問い合わせください。

必要なユーザ ロール : admin、user

デフォルト値 : Auto

値スペース : Off/Auto/CUCM/Edge/Webex/TMS/VCS

Off : デバイスはプロビジョニング システムによって設定されません。

Auto : DHCP サーバでセットアップされる対象としてプロビジョニング サーバが自動的に選択されます。

CUCM : CUCM (Cisco Unified Communications Manager) からデバイスに設定をプッシュします。

Edge : CUCM (Cisco Unified Communications Manager) からデバイスに設定をプッシュします。デバイスは Expressway インフラストラクチャを介して CUCM に接続します。Expressway を経由して登録するには、暗号化オプションキーがデバイスにインストールされている必要があります。

Webex : Cisco Webex クラウド サービスからデバイスに設定をプッシュします。

TMS : TMS (Cisco TelePresence Management System) からデバイスに設定をプッシュします。

VCS : VCS (Cisco TelePresence Video Communication Server) からデバイスに設定をプッシュします。

Provisioning LoginName

これは、プロビジョニング サーバでデバイスを認証するために使用されるクレデンシャルのユーザ名部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 80)

有効なユーザ名。

Provisioning Password

これは、プロビジョニング サーバでデバイスを認証するために使用されるクレデンシャルのパスワード部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効なパスワード。

Provisioning TlsVerify

この設定は、ビデオ会議デバイスが HTTPS 経由でプロビジョニング サーバに接続するときに適用されます。

デバイスと HTTPS サーバ間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (プレインストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

一般に、HTTPS 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。このルールには次の 2 つの例外があります。1) 互換性の理由で、CUCM に登録されているデバイスの最小 TLS バージョンは 1.0 です。2) Webex クラウド サービスに登録されているデバイスは、常にバージョン 1.2 を使用します。

注 : アップグレード後にデバイスが初期設定にリセットされておらず、従来の NetworkServices HTTPS VerifyServerCertificate 設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

デバイスが Expressway 経由で Cisco Webex クラウド サービスや CUCM からプロビジョニングされている場合 (MRA またはエッジとも呼ばれます) 、この設定に関係なく、常に証明書のチェックが実行されます。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : デバイスは HTTPS サーバの証明書を確認しません。

On : デバイスは、HTTPS サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

プロキシミティの設定

Proximity Mode

デバイスが超音波ペアリング メッセージを発信するかどうかを決定します。

デバイスが超音波を発信すると、Proximity クライアントはデバイスが近くにあることを検知できます。クライアントを使用するには、少なくとも 1 つの Proximity サービスをイネーブルにする必要があります (Proximity Services 設定を参照) 。一般的に、すべてのプロキシミティ サービスを有効にすることをお勧めします。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : デバイスは超音波を発信しないため、Proximity サービスを使用できません。

On : デバイスが超音波を発信すると、Proximity クライアントはデバイスが近くにあることを検知できます。有効になっているプロキシミティ サービスを使用できます。

Proximity Services CallControl

Proximity クライアントで基本的なコール制御機能を有効または無効にします。この設定を有効にすると、Proximity クライアントを使用してコールを制御できます (ダイヤル、ミュート、音量、コールの終了など) 。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには、Proximity Mode を On にする必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Disabled

値スペース : Enabled/Disabled

Enabled : Proximity クライアントからのコール制御が有効になります。

Disabled : Proximity クライアントからのコール制御が無効になります。

Proximity Services ContentShare FromClients

クライアントからのコンテンツ共有を有効または無効にします。この設定を有効にするとデバイスで無線によって Proximity クライアントからコンテンツを共有できます (ラップトップ画面の共有など) 。このサービスはラップトップ (OS X および Windows) でサポートされます。この設定が機能するには、Proximity Mode を On にする必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Enabled

値スペース : Enabled/Disabled

Enabled : Proximity クライアントからのコンテンツ共有が有効になります。

Disabled : Proximity クライアントからのコンテンツ共有が無効になります。

Proximity Services ContentShare ToClients

プロキシミティ クライアントに対するコンテンツ共有を有効または無効にします。有効にすると、Proximity クライアントはデバイスからプレゼンテーションを受信します。詳細を拡大して、以前のコンテンツを表示し、スナップショットを作成できます。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには、Proximity Mode を On にする必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Disabled

値スペース : Enabled/Disabled

Enabled : Proximity クライアントに対するコンテンツ共有が有効になります。

Disabled : Proximity クライアントに対するコンテンツ共有が無効になります。

ルームリセットの設定

RoomReset Control

この設定は、コントロールシステムまたはマクロの使用に対するものです。マクロによって、ビデオ会議デバイスの一部を自動化できる JavaScript コードのスニペットを記述できます。これによりカスタム動作を作成します。

ルームが数分に渡って待機状態になると、ビデオ会議デバイスは、ルームがリセット可能な状態であることを示すイベントを送信できます。

この設定が有効である場合に送られるイベントは次の通りです :

*e RoomReset SecondsToReset: 30

** end

*e RoomReset Reset

** end

必要なユーザ ロール : ADMIN

デフォルト値 : On

設定可能な値: CameraPositionsOnly/Off/On

CameraPositionsOnly (カメラポジションのみ) : 適用されません。

Off : ルームリセットイベントは送られません。

On : ルームリセット制御が有効になっており、ルームリセットイベントが送信されます。

RTP 設定

RTP Ports Range Start

RTP ポート範囲の最初のポートを定義します。

デフォルトでは、デバイスは RTP および RTCP メディア データに 2326 ～ 2487 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100、RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 2326

値スペース : 整数 (1024..65438)

RTP ポート範囲内で最初のポートを設定します。この値は偶数にする必要があります。

RTP Ports Range Stop

RTP ポート範囲の最後のポートを定義します。

デフォルトでは、デバイスは RTP および RTCP メディア データに 2326 ～ 2487 の範囲のポートを使用します。RTP ビデオ ポート範囲が有効な場合、デバイスは 1024 ～ 65436 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100、RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値 : 2487

値スペース : 整数 (1121 ～ 65535)

RTP ポート範囲内で最後のポートを設定します。この値は奇数にする必要があります。偶数値を入力すると、自動的に 1 が加算されます。

RTP Video Ports Range Start

RTP ビデオ ポート範囲の最初のポートを定義します。

開始と終了の値の両方が 0 に設定されている場合、RTP ビデオ ポートの範囲は無効です。有効にするには、最初のポートを 1024 から 65454 までの値に設定し、最後のポートを 1024 から 65535 までの値に設定します。最小範囲は 80 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0、1024..65454)

RTP ビデオ ポート範囲の最初のポートを設定します。

RTP Video Ports Range Stop

RTP ビデオ ポート範囲の最後のポートを定義します。

開始と終了の値の両方が 0 に設定されている場合、RTP ビデオ ポートの範囲は無効です。有効にするには、最初のポートを 1024 から 65454 までの値に設定し、最後のポートを 1024 から 65535 までの値に設定します。最小範囲は 80 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0、1024..65535)

RTP ビデオ ポート範囲の最後のポートを設定します。

セキュリティ設定

Security Audit Logging Mode

監査ログを記録または送信する場所を定義します。監査ログは syslog サーバに送信されます。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

External モードまたは ExternalSecure モードを使用する場合は、セキュリティ監査サーバアドレス設定に監査サーバのアドレスを入力する必要があります。

必要なユーザ ロール : AUDIT

デフォルト値 : Internal

設定可能な値 : External/ExternalSecure/Internal/Off

External : デバイスは外部監査 syslog サーバに監査ログを送信します。syslog サーバでは UDP をサポートする必要があります。

ExternalSecure : デバイスは、監査 CA リストの証明書で検証された外部 syslog サーバに暗号化された監査ログを送信します。監査 CA リスト ファイルが Web インターフェイスからデバイスにアップロードされている必要があります。CA のリストの証明書の common_name パラメータは syslog サーバの IP アドレスまたは DNS 名と一致する必要があり、セキュア TCP サーバでセキュア (TLS) TCP syslog メッセージをリッスンするように設定される必要があります。

Internal : デバイスは内部ログに監査ログを記録し、満杯になるとログをローテーションします。

Off : 監査ロギングは実行されません。

Security Audit OnError Action

syslog サーバへの接続が失われた場合の動作を定義します。この設定は、Security Audit Logging Mode が ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値 : Ignore

値スペース : Halt/Ignore

Halt : 停止状態が検出された場合、デバイスはリブートし、停止期間が経過するまでは監査役だけが装置の操作を許可されます。停止状態が過ぎ去ると、監査ログは syslog サーバに再スプールされます。ネットワークの違反 (物理リンクなし) 、動作中の外 Syslog サーバが存在しない (または syslog への間違ったアドレスまたはポート) 、TLS 認証が失敗した (使用中の場合) 、ローカル バックアップ (再スプール) ログがいっぱいになった、などの停止状態があります。

Ignore : デバイスは通常の動作を続行し、満杯になった場合は内部ログをローテーションします。接続が復元されると syslog サーバに再度監査ログを送信します。

Security Audit Server Address

監査ログの送信先である syslog サーバの IP アドレスまたは DNS 名を設定します。この設定は、Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Security Audit Server Port

監査ログは syslog サーバに送信されます。デバイスが監査ログを送信する syslog サーバのポートを定義します。この設定は、Security Audit PortAssignment がマニュアルに設定されている場合にのみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値: 514

値スペース : 整数 (0..65535)

監査サーバのポートを設定します。

Security Audit Server PortAssignment

監査ログは syslog サーバに送信されます。外部 syslog サーバのポート番号の割り当て方法を定義できます。この設定は、Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。使用しているポート番号を確認するために、Security Audit Server Port 状態をチェックできます。ウェブ インターフェイスで [セットアップ (Setup)] > [ステータス (Status)] に移動するか、コマンドライン インターフェイスの場合はコマンド xStatus Security Audit Server Port を実行します。

必要なユーザ ロール : AUDIT

デフォルト値 : Auto

値スペース : Auto/Manual

Auto : [セキュリティ監査ロギング モード (Security Audit Logging Mode)] が [外部 (External)] にセットされている場合、UDP ポート番号 514 を使用します。Security Audit Logging Mode が ExternalSecure にセットされている場合、TCP ポート番号 6514 を使用します。
Manual : [セキュリティ監査サーバのポート (Security Audit Server Port)] 設定で定義されたポート値を使用します。

Security Session FailedLoginsLockoutTime

ユーザが Web または SSH セッションのログインに失敗したあと、デバイスがユーザをロックアウトする時間を定義します。

この設定に対する変更を反映するには、デバイスを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 60

値スペース : 整数 (0..10000)
ロックアウト時間 (分) を設定します。

Security Session InactivityTimeout

ユーザが Web、Telnet または SSH セッションから自動的にログ アウトする前に、デバイスがユーザの非アクティブ状態をどれくらいの時間受け入れるかを定義します。

この設定に対する変更を反映するには、デバイスを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..10000)
非アクティブ タイムアウト (分単位) を設定します。非アクティブな状態でも強制的に自動ログアウトしない場合は、0 を選択します。

Security Session MaxFailedLogins

ウェブまたは SSH セッションにログイン試行を失敗できるユーザ 1 人あたりの最大数を定義します。ユーザが試行の最大数を超えた場合、ユーザはロックアウトされます。0 は、失敗できるログインの回数に制限がないことを意味します。

この設定に対する変更を反映するには、デバイスを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..10)
ユーザ 1 人あたりの失敗できるログイン試行の最高回数を設定します。

Security Session MaxSessionsPerUser

ユーザ 1 人あたりの最大同時セッション数は 20 セッションです。

必要なユーザ ロール : ADMIN

デフォルト値: 20

値スペース : 整数 (1..20)
ユーザ 1 人あたりの最大同時セッション数を設定します。

Security Session MaxTotalSessions

同時セッションの合計最大数は 20 セッションです。

必要なユーザ ロール : ADMIN

デフォルト値: 20

値スペース : 整数 (1..20)
同時セッションの合計最大数を設定します。

Security Session ShowLastLogon

SSH または Telnet を使用してデバイスにログインしたとき、前回ログインに成功したセッションの UserId、時刻および日付が表示されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

On : 最後のセッションに関する情報を表示します。

Off : 最後のセッションに関する情報を表示しません。

SerialPort 設定

SerialPort Mode

シリアル ポートを有効/無効にします。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : On

値スペース : Off/On
Off : シリアル ポートを無効にします。
On : シリアル ポートをイネーブルにします。

SerialPort LoginRequired

シリアル ポートに接続するときにログインが必要かどうかを定義します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : ユーザはログインせずに、シリアル ポート経由でデバイスにアクセスできます。
On : シリアル ポート経由でデバイスに接続するときに、ログインが必要です。

SIP 設定

SIP ANAT

ANAT (Alternative Network Address Types) は RFC 4091 で規定されている複数のアドレスとアドレス タイプのメディア ネゴシエーションを有効にします。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : ANAT を無効にします。
On : ANAT を有効にします。

SIP Authentication UserName

これは、SIP プロキシへの認証に使用されるクレデンシャルのユーザ名部分です。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 128)
有効なユーザ名。

SIP Authentication Password

これは、SIP プロキシへの認証に使用されるクレデンシャルのパスワード部分です。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 128)
有効なパスワード。

SIP DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : Auto

値スペース : Auto/TCP/Tls/UDP
TCP : デバイスはデフォルトの転送方法として常に TCP を使用します。
UDP : デバイスはデフォルトの転送方法として常に UDP を使用します。
Tls : デバイスはデフォルトの転送方法として常に TLS を使用します。TLS 接続の場合、SIP CA リストをデバイスにアップロードできます。該当する CA リストがデバイスにない場合は、ディフィー ヘルマン匿名認証が使用されます。
Auto : デバイスは、TLS、TCP、UDP の順序でトランスポート プロトコルを使用して接続を試みます。

SIP DisplayName

設定されたとき、着信コールは SIP URI ではなく、表示名を報告します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 550)
SIP URI の代わりに表示する名前。

SIP Ice DefaultCandidate

ICE プロトコルには、使用するメディア ルートを決定するまでの時間（最大で通話開始から 5 秒間）が必要となります。この時間内に、この設定に従って、デバイスのメディアがデフォルトの候補に送信されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Host

値スペース : Host/Rflx/Relay

Host : メディアをデバイスのプライベート IP アドレスに送信します。

Rflx : TURN サーバが認識しているデバイスのパブリック IP アドレスにメディアを送信します。

Relay : TURN サーバで割り当てられた IP アドレスおよびポートにメディアを送信します。

SIP Ice Mode

ICE (Interactive Connectivity Establishment、RFC 5245) は、最適化されたメディア パスの検出にデバイスで使用できる NAT トラバーサル ソリューションです。このため、音声とビデオの最短ルートがデバイス間で常に確保されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Off/On

Auto : TURN サーバが提供されている場合は ICE が有効になり、提供されていない場合は ICE が無効になります。

Off : ICE が無効になります。

On : ICE が有効になります。

SIP Line

Cisco Unified Communications Manager (CUCM) に登録すると、デバイスを共有電話の一部にできます。これは、複数のデバイスが同じディレクトリ番号を共有することを意味します。RFC 4235 で規定されているように、同じ番号を共有する各デバイスは、ライン上のもう一方のアピアランスからステータスを受け取ります。

共有回線はデバイスではなく CUCM によって設定されることに注意してください。そのため、手動でこの設定を変更しないでください。CUCM は必要に応じてこの情報をデバイスにプッシュします。

必要なユーザ ロール : ADMIN

デフォルト値 : Private

値スペース : Private/Shared

Shared : デバイスは共有電話の一部であるため、ディレクトリ番号を他のデバイスと共有します。

Private : このデバイスは共有電話の一部ではありません。

SIP ListenPort

SIP TCP/UDP ポートでの着信接続のリッスンをオンまたはオフにします。オフにした場合、デバイスは SIP プロキシ (CUCM または VCS) を介してのみ到達可能になります。セキュリティ対策として、デバイスが SIP プロキシに設定されている場合は SIP ListenPort をオフにすべきです。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Auto/Off/On

Auto : デバイスが SIP プロキシに登録されている場合、SIP TCP/UDP ポートでの着信接続に対するリスニングは自動的にオフになります。それ以外の場合は、オンになります。

Off : SIP TCP/UDP ポートでの着信接続のリッスンをオフにします。

On : SIP TCP/UDP ポートでの着信接続のリッスンをオンにします。

SIP Mailbox

Cisco Unified Communications Manager (CUCM) に登録すると、個人用ボイス メールボックスを所有するオプションが与えられます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な番号またはアドレス。ボイス メールボックスがない場合は、文字列を空のままにしておきます。

SIP MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN

デフォルト値 : TLSv1.0

値スペース : TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0 : TLS バージョン 1.0 以上をサポートします。

TLSv1.1 : TLS バージョン 1.1 以上をサポートします。

TLSv1.2 : TLS バージョン 1.2 以上をサポートします。

SIP PreferredIPSignaling

シグナリングの優先 IP バージョンを定義します (音声、ビデオ、データ) 。Network IPStack および Conference CallProtocolIPStack の両方が Dual に設定されていて、ネットワークに優先 IP バージョンを選択するメカニズムがない場合にのみ使用可能です。また、優先 IP バージョンが登録に使用されるように、DNS で A/AAAA ルックアップのプライオリティを指定します。

必要なユーザ ロール : ADMIN

デフォルト値 : IPv4

値スペース : IPv4/IPv6

IPv4 : シグナリングの優先 IP バージョンは IPv4 です。

IPv6 : シグナリングの優先 IP バージョンは IPv6 です。

SIP Proxy [n] Address

n: 1.. 4

プロキシ アドレスは発信プロキシに手動で設定されたアドレスです。完全修飾ドメイン名、または IP アドレスを使用することが可能です。デフォルト ポートは、TCP および UDP の場合は 5060 ですが、もう 1 ポート準備できます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

SIP TlsVerify

SIP TLS 経由の接続を確立する前に、デバイスは、信頼できる認証局 (CA) がピアの証明書に署名しているかどうかを確認します。CA が CA リストに含まれており、Web インターフェイスまたは API を使用して手動でデバイスにアップロードされている必要があります。プレインストールされている証明書リストは、SIP TLS 接続の証明書の検証には使用されません。

注 : アップグレード後にデバイスが初期設定にリセットされておらず、この設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

どの TLS バージョンを許可するかを指定するには、SIP MinimumTLSVersion 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスはピアの証明書を確認しません。いずれにしても SIP TLS 接続が確立されます。

On : デバイスは、ピアの証明書が信頼できるかどうかを確認します。信頼できない場合、SIP TLS 接続は確立されません。

SIP Turn DiscoverMode

検出モードを定義し、DNS で利用可能な TURN サーバの検索に対してアプリケーションを有効/無効にします。コールを発信する前に、デバイスはポート割り当てが可能かどうかを確認します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 検出モードを無効にします。

On : On に設定すると、デバイスは DNS で利用可能な TURN サーバを検索し、コールを発信する前にポート割り当てが可能かどうかをテストします。

SIP Turn DropRflx

DropRflx は、リモート デバイスが同じネットワークにない場合に限り、TURN リレー経由でデバイスにメディアを強制させます。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : DropRflx を無効にします。

On : リモート デバイスが別のネットワークにある場合、デバイスは TURN リレー経由でメディアを強制します。

SIP Turn Server

TURN (Traversal Using Relay NAT) サーバのアドレスを定義します。これはメディア リレー フォールバックとして使用され、また、デバイス固有のパブリック IP アドレスを検出するためにも使用されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

推奨する形式は DNS SRV レコード (例 : _turn._udp.<ドメイン>) ですが、有効な IPv4 または IPv6 アドレスも指定できます。

SIP Turn UserName

TURN サーバへのアクセスに必要なユーザ名を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

有効なユーザ名。

SIP Turn Password

TURN サーバへのアクセスに必要なパスワードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

有効なパスワード。

SIP Type

ベンダーまたはプロバイダーに対する SIP 拡張および特別な動作を有効にします。

必要なユーザ ロール : ADMIN

デフォルト値 : Standard

値スペース : Standard/Cisco

Standard : 標準 SIP プロキシに登録する場合はこれを使用します (Cisco TelePresence VCS でテスト済み) 。

Cisco : Cisco Unified Communications Manager に登録する場合はこれを使用します。

SIP URI

SIP URI (Uniform Resource Identifier) は、デバイスの識別に使用されるアドレスです。URI が登録され、SIP サービスによりデバイスへの着信コールのルーティングに使用されます。SIP URI 構文は RFC 3261 で定義されています。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

SIP URI 構文に準拠したアドレス (URI) 。

スタンバイ設定

Standby Control

デバイスがスタンバイ モードに移行するかどうかを定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : On

値スペース : Off/On
Off : デバイスはスタンバイ モードを開始しません。
On : Standby Delay がタイム アウトすると、デバイスはスタンバイ モードを開始します。

Standby Delay

スタンバイ モードに入るまでにデバイスがアイドル モードのまま経過する時間の長さ (分単位) を定義します。[スタンバイ制御 (Standby Control)] が有効である必要があります。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値: 10

値スペース : 整数 (1..480)
スタンバイ遅延 (分) を設定します。

Standby WakeupOnMotionDetection

モーション検出時の自動復帰は、ユーザがルームに入室したときに検出する機能です。この機能は、超音波検出に基づいています。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Off

値スペース : Off/On
Off : 動体検知ウェイクアップは無効です。
On : 人が部屋に入ってくると、デバイスが自動的にスタンバイからウェイクアップします (DX80 にのみ適用) 。

SystemUnit 設定

SystemUnit Name

デバイス名を定義します。デバイスが SNMP エージェントとして機能している場合に、デバイス名は DHCP リクエストでホスト名として送信されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

デバイス名を定義します。

SystemUnit CrashReporting Advanced

デバイスがクラッシュすると、デバイスは解析のためにシスコ自動クラッシュ レポート ツール（ACR）にログを自動送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : ACR ツールは標準的なログ解析を実行します。

On : ACR ツールは高度なログ解析を実行します。

SystemUnit CrashReporting Mode

デバイスがクラッシュすると、デバイスは解析のためにシスコ自動クラッシュ レポート ツール（ACR）にログを自動送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : ACR ツールにログは送信されません。

On : ACR ツールにログは自動的に送信されます。

SystemUnit CrashReporting Url

デバイスがクラッシュすると、デバイスは解析のためにシスコ自動クラッシュ レポート ツール（ACR）にログを自動送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

[Cisco Automatic Crash Report ツール (Cisco Automatic Crash Report tool)] の URL。

時刻設定

Time TimeFormat

時刻形式を定義します。

必要なユーザ ロール : admin、user
デフォルト値 : 24H

値スペース : 24H/12H
24H : 24 時間の時間フォーマットを設定します。
12H : 12 時間 (AM/PM) の時間フォーマットを設定します。

Time DateFormat

日付形式を定義します。

必要なユーザ ロール : admin、user
デフォルト値 : DD_MM_YY

値スペース : DD_MM_YY/MM_DD_YY/YY_MM_DD
DD_MM_YY : 2010 年 1 月 30 日は「30.01.10」と表示されます。
MM_DD_YY : 2010 年 1 月 30 日は「01.30.10」と表示されます。
YY_MM_DD : 2010 年 1 月 30 日は「10.01.30」と表示されます。

Time Zone

デバイスが物理的に存在する地域のタイム ゾーンを設定します。値スペースの情報は、tz データベース（別名：IANA タイムゾーン データベース）から取得しています。

必要なユーザ ロール： ADMIN、INTEGRATOR、USER

デフォルト値：Etc/UTC

設定可能な値：アフリカ/アビジャン、アフリカ/アクラ、アフリカ/アディスアベバ、アフリカ/アルジェ、アフリカ/アスマラ、アフリカ/アスメラ、アフリカ/バマコ、アフリカ/バンギ、アフリカ/バンジュール、アフリカ/ビサウ、アフリカ/ブランタイア、アフリカ/ブラザビル、アフリカ/ブジュンブラ、アフリカ/カイロ、アフリカ/カサブランカ、アフリカ/セウタ、アフリカ/コナクリ、アフリカ/ダカール、アフリカ/ダルエスサラーム、アフリカ/ジブチ、アフリカ/ドゥアラ、アフリカ/アイウン、アフリカ/フリータウン、アフリカ/ガボローネ、アフリカ/ハラーレ、アフリカ/ヨハネスブルク、アフリカ/ジュバ、アフリカ/カンパラ、アフリカ/ハルツーム、アフリカ/キガリ、アフリカ/キンシャサ、アフリカ/ラゴス、アフリカ/リーブルビル、アフリカ/ロメ、アフリカ/ルアンダ、アフリカ/ルブンバシ、アフリカ/ルサカ、アフリカ/マラボ、アフリカ/マプト、アフリカ/マセール、アフリカ/ムババーネ、アフリカ/モガディシュ、アフリカ/モンロヴィア、アフリカ/ナイロビ、アフリカ/ンジャメナ、アフリカ/ニアメイ、アフリカ/ヌアクショット、アフリカ/ワガドゥグ、アフリカ/ポルトノボ、アフリカ/サントメ・プリンシペ、アフリカ/ティンブクトゥ、アフリカ/トリポリ、アフリカ/チュニス、アフリカ/ウィントフック、アメリカ/アダック、アメリカ/アンカレッジ、アメリカ/アンギラ、アメリカ/アンティグア、アメリカ/アラグァイーナ、アメリカ/アルゼンチン/ブエノスアイレス、アメリカ/アルゼンチン/カタマルカ、アメリカ/アルゼンチン/コモドーロ・リバダビア、アメリカ/アルゼンチン/コルドバ、アメリカ/アルゼンチン/フフイ、アメリカ/アルゼンチン/ラ・リオージャ、アメリカ/アルゼンチン/メンドーサ、アメリカ/アルゼンチン/リオ・ガレゴス、アメリカ/アルゼンチン/サルタ、アメリカ/アルゼンチン/サンファン、アメリカ/アルゼンチン/サンルイス、アメリカ/アルゼンチン/トゥクマン、アメリカ/アルゼンチン/ウシュアイア、アメリカ/アルバ、アメリカ/アスンシオン、アメリカ/アティコーカン、アメリカ/アトーチャ、アメリカ/バヒア、アメリカ/バヒア・バンデラス、アメリカ/バルバドス、アメリカ/ベレン、アメリカ/ベリーズ、アメリカ/ブランサルトン、アメリカ/ボア・ビスタ、アメリカ/ボゴタ、アメリカ/ボイシ、アメリカ/ブエノスアイレス、アメリカ/ケンブリッジベイ、アメリカ/カンポグランデ、アメリカ/カンクーン、アメリカ/カラカス、アメリカ/カタマルカ、アメリカ/カイエン、アメリカ/ケイマン、アメリカ/シカゴ、アメリカ/チワワ、アメリカ/コーラル・ハーバー、アメリカ/コルドバ、アメリカ/コスタリカ、アメリカ/クレストン、アメリカ/クイアバ、アメリカ/キュラソー、アメリカ/デンマルクション、アメリカ/ドーソン、アメリカ/ドーソンクリーク、アメリカ/デンバー、アメリカ/デトロイト、アメリカ/ドミニカ、アメリカ/エドモントン、アメリカ/エイルネペ、アメリカ/エルサルバドル、アメリカ/エンセナダ、アメリカ/フォート・ネルソン、アメリカ/フォート・ウェイン、アメリカ/フォルタレザ、アメリカ/グレース・米、アメリカ/ゴットホープ、アメリカ/グース・ベイ、アメリカ/グランドターク、アメリカ/グレナダ、アメリカ/グアダルーペ、アメリカ/グアテマラ、アメリカ/グアヤキル、アメリカ/ガイアナ、アメリカ/ハリファクス、アメリカ/ハバナ、アメリカ/エルモシージョ、アメリカ/インディアナ/インディアナポリス、アメリカ/インディアナ/ノックス、アメリカ/インディアナ/マレンゴ、アメリカ/インディアナ/ピータースバーグ、アメリカ/インディアナ/テルシティ、アメリカ/インディアナ/ヴィベイ、アメリカ/インディアナ/ヴァンセンヌ、アメリカ/インディアナ/ウィナマク、アメリカ/インディアナポリス、アメリカ/イヌヴィック、アメリカ/イカルイト、アメリカ/ジャマイカ、アメリカ/フフイ、アメリカ/ジュノー、アメリカ/ケンタッキー/ルイビル、アメリカ/ケンタッキー/モンティチェロ、アメリカ/ノックス、アメリカ/クラレンダイク、アメリカ/ラパス、アメリカ/リマ、アメリカ/ロサンゼルス、アメリカ/ルイビル、アメリカ/ローワー・プリンシズ、アメリカ/マセイオ、アメリカ/マナグア、アメリカ/マナウス、アメリカ/マリゴ、アメリカ/マルティニーク、アメリカ/マタモロス、アメリカ/マサトラン、アメリカ/メンドーサ、アメリカ/メノミニー、アメリカ/メリダ、アメリカ/メトラカトラ、アメリカ/メキシコシティ、アメリカ/ミクロン島、アメリカ/モンクトン、アメリカ/モントレー、アメリカ/モンテビデオ、アメリカ/モントリオール、アメリカ/モンセラート、アメリカ/ナッソー、アメリカ/ニューヨーク、アメリカ/ニピゴン、アメリカ/ノーム、アメリカ/ノローニャ、アメリカ/ノースダコタ/ビューラ、アメリカ/ノースダコタ/センター、アメリカ/ノースダコタ/ニュー・セーラム、アメリカ/オジナガ、アメリカ/パナマ、アメリカ/パングナータング、アメリカ/パラマリボ、アメリカ/フェニックス、アメリカ/ポルトープランス、アメリカ/ポートオブスペイン、アメリカ/ポルト・アクレ、アメリカ/ポルト・ヴェーリョ、アメリカ/プエルトリコ、アメリカ/レイニーリバー、アメリカ/ランキン・インレット、アメリカ/レシフェ、アメリカ/レジーナ、アメリカ/レゾリュート、アメリカ/リオ・ブランコ、アメリカ/ロサリオ、アメリカ/サンタイザベル、アメリカ/サンタレム、アメリカ/サンチアゴ、アメリカ/サントドミンゴ、アメリカ/サンパウロ、アメリカ/スコールスビーサンド、アメリカ/シップロック、アメリカ/シトカアメリカ/サン・バルテルミー島、アメリカ/セント・ジョーンズ、アメリカ/セントクリストファー・ネイビス、アメリカ/セントルシア、アメリカ/セント・トーマス、アメリカ/サン・ヴィンセント、アメリカ/スウィフトカレント、アメリカ/テグシガルパ、アメリカ/スーリー、アメリカ/サンダーベイ、アメリカ/ティファナ、アメリカ/トロント、アメリカ/トルトラ、アメリカ/バンクーバー、アメリカ/バージン、アメリカ/ホワイトハウス、アメリカ/ウィニペグ、アメリカ/ヤクタート、アメリカ/イエローナイフ、南極/ケーシー、南極/デービス、南極/デュモン・デュルヴィル、南極/マックォーリー、南極/モーソン、南極/マクマルド、南極/パーマー、南極/ロゼラ、南極/南極点、南極/昭和、南極/トロール、南極/ボストーク、北極/ロングイェールビーン、アジア/アデン、アジア/アルマトイ、アジア/アンマン、アジア/アナディル、アジア/アクタウ、アジア/アクトベ、アジア/アシガバート、アジア/アシガバート、アジア/バグダッド、アジア/バーレーン、アジア/バクー、アジア/バンコク、アジア/バルナウル、アジア/ベイルート、アジア/ビシュケク、アジア/ブルネイ、アジア/カルカッタ、アジア/チタ、アジア/チョイバルサン、アジア/重慶、アジア/重慶、アジア/コロンボ、アジア/ダッカ、アジア/ダマスカス、アジア/ダッカ、アジア/ディリ、アジア/ドバイ、アジア/ドゥシャンベ、アジア/ガザ、アジア/ハルビン、アジア/ヘブロン、アジア/ホーチミンシティ、アジア/香港、アジア/ホブド、アジア/イルクーツク、アジア/イスタンブール、アジア/ジャカルタ、アジア/ジャヤプラ、アジア/エルサレム、アジア/カブール、アジア/カムチャッカ、アジア/カラチ、アジア/カシュガル、アジア/カトマンズ、アジア/カトマンズ、アジア/ハンドゥイガ、アジア/コルカタ、アジア/クラスノヤルスク、アジア/クアラルンプール、アジア/クチン、アジア/クウェート、アジア/マカオ、アジア/マカオ、アジア/マガダン、アジア/マカッサル、アジア/マニラ、アジア/マスカット、アジア/ニコシア、アジア/ノヴォクズネツク、アジア/ノヴォシビルスク、アジア/オムスク、アジア/オラル、アジア/プノンペン、アジア/ポンティアナック、アジア/平壌、アジア/カタール、アジア/クズロルダ、アジア/ラングーン、アジア/リャド、アジア/サイゴン、アジア/サハリン、アジア/サマルカンド、アジア/ソウル、アジア/上海、アジア/シンガポール、アジア/スレドネコリムスク、アジア/台北、アジア/タシケント、アジア/トビリシ、アジア/テヘラン、アジア/テルアビブ、アジア/ティンプー、アジア/ティンプー、アジア/東京、アジア/トムスク、アジア/ウジュンパンダン、アジア/ウランバートル、アジア/ウランバートル、アジア/ウルムチ、アジア/ウスチ＝ネラ、アジア/ヴィエンチャン、アジア/ウラジオストク、アジア/ヤクーツク、アジア/エカテリンブルク、アジア/エレバン、大西洋/アゾレス諸島、大西洋/バミューダ諸島、大西洋/カナリア諸島、大西洋/カーボベルデ、大西洋/フェロー諸島、大西洋/フェロー諸島、大西洋/ヤンマイエン島、大西洋/マデイラ島、大西洋/レイキャビク、大西洋/南ジョージア、大西洋/セントヘレナ、大西洋/スタンレー、オーストラリア/ACT、オーストラリア/アデレード、オーストラリア/ブリスベン、オーストラリア/ブロークンヒル、オーストラリア/キャンベラ、オーストラリア/カリー、オーストラリア/ダーウィン、オーストラリア/ユークラ、オーストラリア/ホバート、オーストラリア/LHI、オーストラリア/リンデマン、オーストラリア/ロード・ハウ、オーストラリア/メルボルン、オーストラリア/NSW、オーストラリア/ノース、オーストラリア/パース、オーストラリア/クイーンズランド、オーストラリア/サウス、オーストラリア/シドニー、オースト

ラリア/タスマニア、オーストラリア/ヴィクトリア、オーストラリア/ウエスト、オーストラリア/ヤンコウィナ、ブラジル/アクレ、ブラジル/デ・ノローニャ、ブラジル/イースト、CET、CST6CDT、カナダ/アトランティック、カナダ/セントラル、カナダ/イーストサスカチュワン、カナダ/イースタン、カナダ/マウンテン、カナダ/ニューファンドランド、カナダ/パシフィック、カナダ/サスカチュワン、カナダ/ユーコン、チリ/コンチネンタル、チリ/イースター島、キューバ、EET、EST、EST5EDT、エジプト、Eire、その他/GMT、その他/GMT+0、その他/GMT+1、その他/GMT+10、その他/GMT+11、その他/GMT+12、その他/GMT+2、その他/GMT+3、その他/GMT+4、その他/GMT+5、その他/GMT+6、その他/GMT+7、その他/GMT+8、その他/GMT+9、その他/GMT-0、その他/GMT-1、その他/GMT-10、その他/GMT-11、その他/GMT-12、その他/GMT-13、その他/GMT-14、その他/GMT-2、その他/GMT-3、その他/GMT-4、その他/GMT-5、その他/GMT-6、その他/GMT-7、その他/GMT-8、その他/GMT-9、その他/GMT0、その他/グリニッジ、その他/UCT、その他/UTC、その他/ユニバーサル、その他/ズールー、ヨーロッパ/アムステルダム、ヨーロッパ/アンドラ、ヨーロッパ/アストラハン、ヨーロッパ/アテナ、ヨーロッパ/ベルファスト、ヨーロッパ/ベルグラード、ヨーロッパ/ベルリン、ヨーロッパ/ブラティスラヴァ、ヨーロッパ/ブリュッセル、ヨーロッパ/ブカレスト、ヨーロッパ/ブダペスト、ヨーロッパ/ビュージンゲン、ヨーロッパ/キシナウ、ヨーロッパ/コペンハーゲン、ヨーロッパ/ダブリン、ヨーロッパ/ジブラルタル、ヨーロッパ/ガーンジー、ヨーロッパ/ヘルシンキ、ヨーロッパ/マン島、ヨーロッパ/イスタンブール、ヨーロッパ/ジャージー、ヨーロッパ/カリーニングラード、ヨーロッパ/キエフ、ヨーロッパ/キロフ、ヨーロッパ/リスボン、ヨーロッパ/リュブリャナ、ヨーロッパ/ロンドン、ヨーロッパ/ルクセンブルク、ヨーロッパ/マドリード、ヨーロッパ/マルタ、ヨーロッパ/マリエハムン、ヨーロッパ/ミンスク、ヨーロッパ/モナコ、ヨーロッパ/モスクワ、ヨーロッパ/ニコシア、ヨーロッパ/オスローヨーロッパ/パリ、ヨーロッパ/ポドゴリツァ、ヨーロッパ/プラハ、ヨーロッパ/リガ、ヨーロッパ/ローマ、ヨーロッパ/サマラ、ヨーロッパ/サンマリノ、ヨーロッパ/サラエボ、ヨーロッパ/シンフェロポリ、ヨーロッパ/スコピエ、ヨーロッパ/ソフィア、ヨーロッパ/ストックホルム、ヨーロッパ/タリン、ヨーロッパ/ティラーナ、ヨーロッパ/ティラスポリ、ヨーロッパ/ウリヤノフスク、ヨーロッパ/ウージュホロド、ヨーロッパ/ファドゥーツ、ヨーロッパ/バチカン、ヨーロッパ/ウィーン、ヨーロッパ/ヴィリニュス、ヨーロッパ/ヴォルゴグラード、ヨーロッパ/ワルシャワ、ヨーロッパ/ザグレブ、ヨーロッパ/ザポリージャ、ヨーロッパ/チューリッヒ、英国、英国エア、GMT、GMT+0、GMT-0、GMT0、グリニッジ、HST、香港、アイスランド、インド洋/アンタナナリボ、インド洋/チャゴス、インド洋/クリスマス諸島、インド洋/ココス、インド洋/コモロ諸島、インド洋/ケルゲレン諸島、インド洋/マヘ島、インド洋/モルディブ、インド洋/モーリシャス諸島、インド洋/マヨット、インド洋/レユニオン、イラン、イスラエル、ジャマイカ、日本、クェゼリン、リビア、MET、MST、MST7MDT、メキシコ/バハノルテ、メキシコ/バハスル、メキシコ/一般、NZ、NZ-CHAT、ナバホ、PRC、PST8PDT、太平洋/アピア、太平洋/オークランド、太平洋/ブーゲンビル、太平洋/チャタム、太平洋/チューク諸島、太平洋/イースター島、太平洋/エファテ島、太平洋/エンダーベリー島、太平洋/ファカオフォ島、太平洋/フィジー、太平洋/フナフティ島、太平洋/ガラパゴス諸島、太平洋/ガンビア、太平洋/ガダルカナル、太平洋/グアム、太平洋/ホノルル、太平洋/ジョンストン、太平洋/キリスィマスィ、太平洋/コスラエ、太平洋/クェゼリン、太平洋/マジュロ、太平洋/マルキーズ諸島、太平洋/ミッドウェー島、太平洋/ナウル、太平洋/ニウエ、太平洋/ノーフォーク、太平洋/ヌメア、太平洋/パゴパゴ、太平洋/パラオ、太平洋/ピトケアン、太平洋/ポンペイ、太平洋/ポナペ、太平洋/ポートモレスビー、太平洋/ラロトンガ、太平洋/サイパン、太平洋/サモア、太平洋/タヒチ、太平洋/タラワ、太平洋/トンガタプ、太平洋/トラック、太平洋/ウェーキ、太平洋/ウォリス、太平洋/ヤップ、ポーランド、ポルトガル、ROC、ROK、シンガポール、トルコ、UCT、米国/アラスカ、米国/アリューシャン、米国/アリゾナ、米国/セントラル、米国/東インディアナ、米国/イースタン、米国/ハワイ、米国/インディアナスターク、米国/ミシガン、米国/マウンテン、米国/パシフィック、米国/パシフィックニュー、米国/サモア、UTC、ユニバーサル、W-SU、WET、ズールー

リストからタイム ゾーンを選択します。

UserInterface 設定

UserInterface Accessibility IncomingCallNotification

画面表示を強調した着信コールの通知を利用できます。画面とタッチ 10 は約 1 秒ごと (1.75 Hz) に赤と白に点滅し、聴覚が不自由なユーザが着信コールに気づきやすくするようにしています。デバイスがコール中の場合、進行中のコールの妨げになるため画面は点滅しません、その代わり、通常の通知が画面とタッチ パネルに表示されます。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Default

値スペース : AmplifiedVisuals/Default

AmplifiedVisuals : デバイスがコールを受け入れたときに、画面とタッチパネル上での画面表示の強調を有効にします。

Default : スクリーンとタッチパネル上での通知を使用したデフォルトの動作を有効にします。

UserInterface Branding AwakeBranding Colors

ブランディングのカスタマイズを使用してデバイスがセットアップされている場合、この設定は、デバイスが起動している時に表示されるロゴの色に影響します。ロゴをフルカラーで表示するか、またはロゴの不透明度を下げるかによって、画面上の背景や他の要素とより自然にブレンドするように設定することができます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Native

Auto : ロゴの不透明度は低減されます。

Native : ロゴはフルカラーです。

UserInterface ContactInfo Type

ユーザ インターフェイスで表示する連絡先の種類を選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/DisplayName/E164Alias/H320Number/H323Id/IPv4/IPv6/None/SipUri/SystemName

Auto : 他のデバイスがこのビデオ会議デバイスに接続するためにダイヤルする必要があるアドレスを表示します。アドレスは、デフォルトのコール プロトコルおよびデバイス登録によって異なります。

None : どのようなコンタクト情報も表示しません。

IPv4 : デバイスの IPv4 アドレスを示します。

IPv6 : デバイスの IPv6 アドレスを示します。

H323Id : デバイスの H.323 ID を表示します (H323 H323Alias ID 設定を参照) 。

H320Number : 連絡先情報としてデバイスの H.320 番号を表示します (Cisco TelePresence ISDN リンクを使用している場合のみサポートされます) 。

E164Alias : 連絡先情報としてデバイスの H.323 E164 エイリアスを表示します (H323 H323Alias E164 設定を参照) 。

SipUri : デバイスの SIP URI を表示します (SIP URI 設定を参照) 。

SystemName : デバイス名を表示します (SystemUnit Name 設定を参照) 。

DisplayName : デバイスの表示名を表示します (SIP DisplayName 設定を参照) 。

UserInterface CustomMessage

アウェイク モードのとき、スクリーンの下部左側にカスタム メッセージを表示することができます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: ""

値スペース : 文字列 (0, 128)

カスタム メッセージを追加します。カスタム メッセージを削除するには空の文字列を追加します。

UserInterface KeyTones Mode

テキストまたは数値を入力する際に、キーボード クリック効果音 (キー トーン) が鳴るようにデバイスを設定できます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : キー トーンは再生されません。

On : キー トーンがオンになります。

UserInterface Features Call End

ユーザインターフェイスからデフォルトの通話終了ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : デフォルトボタンをユーザ インターフェイスから削除します。

UserInterface Features Call MidCallControls

ユーザインターフェイスからデフォルトの保留、転送、および通話再開ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : ユーザ インターフェイスからデフォルトボタンを削除する

UserInterface Features Call Start

ユーザーインターフェイスから、デフォルトの通話ボタン (ディレクトリ、お気に入り、および直近の通話リスト) 、さらにデフォルトの着信追加参加者ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース:Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : ユーザ インターフェイスからデフォルトボタンを削除する

UserInterface Features HideAll

ユーザインターフェイスからデフォルトボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : False

値スペース : False/True

False : すべてのデフォルトボタンをユーザインターフェイスで表示します。

Trues : すべてのデフォルトボタンをユーザインターフェイスで表示しません。

UserInterface Features Share Start

ユーザインターフェイスから、コンテンツの共有とコール発信の両方で、コンテンツを共有およびプレビューするためのデフォルトボタンやその他の UI 要素を削除するかどうかを選択します。設定はボタンと UI 要素だけを削除し、機能などは削除しません。Proximity または Cisco Webex Teams アプリを使ってコンテンツの共有は可能です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンと UI 要素をユーザ インターフェイスに表示します。

Hidden: デフォルトボタンと UI 要素をユーザ インターフェイスから削除します。

UserInterface Features Whiteboard Start

ユーザ インターフェイスからデフォルトの [ホワイトボード (Whiteboard)] ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。この設定は、Cisco Webex に登録されているデバイスにのみ適用されます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : デフォルトボタンをユーザ インターフェイスから削除します。

UserInterface Language

ユーザ インターフェイスで使用される言語を選択します。該当する言語がサポートされていない場合、デフォルトの言語 (Medium) が使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : English

値スペース : Arabic/Catalan/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/English/EnglishUK/Finnish/French/FrenchCanadian/German/Hebrew/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/Portuguese/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish

リストから言語を選択します。

UserInterface OSD EncryptionIndicator

暗号化インジケータが画面に表示される時間の長さを定義します。暗号化された通話のアイコンは、ロックされた南京錠です。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/AlwaysOn/AlwaysOff

Auto : コールが暗号化されている場合は、「コールは暗号化されています (Call is encrypted) 」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。

コールが暗号化されていない場合は、「コールは暗号化されていません (Call is not encrypted) 」という通知が 5 秒間表示されます。暗号化インジケータ アイコンは表示されません。

AlwaysOn : 「コールは暗号化されています (Call is encrypted) 」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。

AlwaysOff : 暗号化インジケータは画面上に表示されません。

UserInterface OSD HalfwakeMessage

カスタム メッセージは、デバイスがハーフウェイク状態のときに、メイン スクリーンの中央に表示できます。カスタム メッセージは、デバイスの使用開始方法について指示するデフォルトのメッセージを置き換えます。カスタム メッセージを追加せずにデフォルト メッセージを削除することもできます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

カスタム メッセージ。空の文字列 : デフォルト メッセージを復元します。空白のみ : メッセージは一切表示されません。

UserInterface OSD Output

オンスクリーン用の情報とインジケータ (OSD) を表示するモニタを定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto

Auto : オンスクリーン情報とインジケータをデバイスの画面に送信します。

UserInterface Phonebook Mode

この設定は、ユーザがデバイスのユーザ インターフェイスから、ディレクトリとお気に入りリストに連絡先を追加または変更することを許可するかどうかを決定します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : ReadWrite

値スペース : ReadOnly/ReadWrite

ReadOnly : 連絡先をお気に入りリストに追加したり、お気に入りリストの連絡先を編集したりはできません。また、通話前にディレクトリやお気に入りリストから連絡先を編集することはできません。

ReadWrite : 連絡先をお気に入りリストに追加したり、お気に入りリストの連絡先を編集したりできます。また、通話前にディレクトリやお気に入りリストから連絡先を編集することができます。

UserInterface Security Mode

この設定では、重要なデバイス情報 (例 : ビデオ会議デバイスの連絡先情報や IP アドレス、Touch コントローラ、および UCM/VCS レジストラ) がユーザ インターフェイス (ドロップダウン メニューと設定パネル) で公開されるのを防ぐことができます。設定パネルに移動するとこのような情報は非表示になっていないので注意してください。

管理者権限を持たない人に連絡先情報、IP アドレス、MAC アドレス、シリアル番号およびソフトウェアのバージョンを絶対に公開しない場合は、[ユーザ インターフェイス設定メニュー モード (UserInterface SettingsMenu Mode)] を [ロック (Locked)] に設定します。また、管理者権限を持つすべてのユーザ アカウントにパスフレーズを設定することも必要です。

必要なユーザ ロール : ADMIN

デフォルト値 : Normal

値スペース : Normal/Strong

Normal : IP アドレスやその他のデバイス情報がユーザ インターフェイスに表示されます。

Strong : 連絡先情報および IP アドレスは、ユーザ インターフェイス (ドロップ ダウン メニューと設定パネル) に表示されません。

UserInterface SettingsMenu Mode

ユーザ インターフェイス (Touch 10 または画面上) の設定パネルは、そのデバイスの管理者パスワードで保護できます。このパスワードが空白の場合、誰でも設定パネルの設定にアクセスし、たとえばデバイスを初期設定にリセットすることができます。認証を有効にすると、認証を必要とするすべての設定に南京錠のアイコンが表示されます。設定を選択するときに、管理者のユーザ名とパスフレーズを入力するよう求められます。認証が必須でない設定には、南京錠のアイコンが表示されません。

必要なユーザ ロール : ADMIN

デフォルト値 : Unlocked

値スペース : Locked/Unlocked

Locked : 管理者のユーザ名とパスフレーズによる認証が必要です。

Unlocked : 認証は必要ありません。

UserInterface SettingsMenu Visibility

デバイス名 (または連絡先情報) および関連するドロップ ダウン メニューと [設定 (Settings)] パネルを、ユーザ インタフェースに表示するかどうかを選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto : デバイス名とドロップ ダウン メニュー、[設定 (Settings)] パネルをユーザ インターフェイスに表示します。

Hidden : デバイス名とドロップ ダウン メニュー、[設定 (Settings)] パネルを、ユーザ インタフェースに表示しません。

UserInterface SoundEffects Mode

他のユーザが Proximity でラップトップやモバイルに接続したときなどにサウンド エフェクトを鳴らすように、デバイスを設定できます。

テキスト入力時のキーボード クリックのサウンド エフェクトは、この設定の影響を受けません（UserInterface Keytones Mode 設定を参照してください）。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : サウンド エフェクトを鳴らしません。

On : サウンド エフェクトをオンにします。

UserInterface Wallpaper

アイドル状態のときのビデオ画面の背景画像（壁紙）を選択します。

Web インターフェイスを使用してデバイスにカスタム壁紙をアップロードできます。サポートされるファイル形式は BMP、GIF、JPEG、PNG です。最大ファイル サイズは 4 MByte です。カスタム壁紙を使用すると、予定されている会議のクロックおよび一覧がメイン ディスプレイから削除されます。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Auto

値スペース : Auto/Custom/None

Auto : デフォルトの壁紙を使用します。

None : 画面に背景イメージはありません。

Custom : 画面の背景画像としてカスタムの壁紙を使用します。デバイスにカスタム壁紙がアップロードされていない場合、この設定はデフォルト値に戻ります。

UserManagement の設定

UserManagement LDAP Admin Filter

どのユーザに管理者権限を付与する必要があるか決定するために LDAP フィルタが使用されます。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタが優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても、ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 1024)

この文字列の構文については、LDAP の仕様を参照してください。例 : "(|(memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

UserManagement LDAP Admin Group

この AD (Active Directory) グループのメンバーには、管理者権限が付与されます。この設定は、memberOf:1.2.840.113556.1.4.1941:=<group name> の短縮形です。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタが優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても、ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

AD グループの識別名。例 : "CN=admin group, OU=company groups, DC=company, DC=com"

UserManagement LDAP Attribute

指定のユーザ名にマップするために使用する属性。設定しない場合、sAMAccountName が使用されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

属性名。

UserManagement LDAP BaseDN

検索を開始するエントリの識別名 (ベース) 。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

ベースの識別名。例 : "DC=company, DC=com"

UserManagement LDAP Encryption

デバイスと LDAP サーバの間の通信を保護する方法を定義します。ポート番号は、UserManagement LDAP Server Port 設定を使用してポート番号をオーバーライドできます。

必要なユーザ ロール : ADMIN

デフォルト値 : LDAPS

値スペース : LDAPS/None/STARTTLS

LDAPS : ポート 636 over TLS (Transport Layer Security) 上の LDAP サーバに接続します。

None : ポート 389 で LDAP サーバに接続します (暗号化なし) 。

STARTTLS : ポート 389 で LDAP サーバに接続し、暗号化された接続 (TLS) にアップグレードするための STARTTLS コマンドを送信します。

UserManagement LDAP MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN
デフォルト値 : TLSv1.2

値スペース : TLSv1.0/TLSv1.1/TLSv1.2
TLSv1.0 : TLS バージョン 1.0 以上をサポートします。
TLSv1.1 : TLS バージョン 1.1 以上をサポートします。
TLSv1.2 : TLS バージョン 1.2 以上をサポートします。

UserManagement LDAP Mode

このデバイスでは、ユーザ名とパスワードを一元的に保存、検証する場所として、LDAP (Lightweight Directory Access Protocol) サーバの使用をサポートします。この設定を使用して、LDAP 認証を使用するかどうか設定します。実装は、Microsoft Active Directory (AD) サービスでテスト済みです。

LDAP モードをオンにする場合、設定に合わせたユーザ管理 LDAP 設定の構成を確認してください。いくつかの例を示します。

例 1 :

- ユーザ管理 LDAP モード : On
- ユーザ管理 LDAP アドレス : "192.0.2.20"
- ユーザ管理 LDAP ベース DN : "DC=company, DC=com"
- ユーザ管理 LDAP 管理グループ : "CN=admin group, OU=company group, DC=company, DC=com"

例 2 :

- ユーザ管理 LDAP モード : On
- ユーザ管理 LDAP アドレス : "192.0.2.20"
- ユーザ管理 LDAP ベース DN : "DC=company, DC=com"
- ユーザ管理 LDAP 管理フィルタ : "(| (memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : LDAP 認証は使用不可です。
On: LDAP 認証は許可されます。

UserManagement LDAP Server Address

LDAP サーバの IP アドレスまたはホスト名を設定します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な IPv4 アドレス、IPv6 アドレス、またはホスト名。

UserManagement LDAP Server Port

LDAP サーバに接続するポートをオンに設定します。0 に設定した場合は、選択したプロトコルのデフォルトを使用します (「UserManagement LDAP Encryption 設定」を参照する) 。

必要なユーザ ロール : ADMIN
デフォルト値: 0

値スペース : 整数 (0..65535)
LDAP サーバのポート番号。

UserManagement LDAP VerifyServerCertificate

デバイスを LDAP サーバに接続すると、サーバはデバイスに証明書を提示して自身を識別します。この設定は、デバイスがサーバの証明書を確認するかどうかを決定するために使用します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : デバイスは LDAP サーバの証明書を検証しません。
On : デバイスは、LDAP サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうか検証する必要があります。該当する CA が、デバイスに事前にアップロードされている信頼できる CA のリストに含まれている必要があります。デバイスの Web インターフェイスを使用して、信頼できる CA のリストを管理します (詳細については管理者ガイドを参照してください) 。

ビデオ設定

Video ActiveSpeaker DefaultPIPPosition

通話中のスピーカーを示すピクチャインピクチャ (PiP) の画面上の位置を定義します。この設定は、通話中のスピーカーを PiP 表示するビデオ レイアウト (オーバーレイ レイアウト) を使用している場合にのみ有効です。また、場合によっては、カスタム レイアウトでも有効です (「Video DefaultLayoutFamily Local の設定」を参照) 。この設定は、次回以降のコールで有効になります。コール中に変更された場合、現在のコールへの影響はありません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : 通話中のスピーカーの PiP の位置はコール終了後にも変更されません。

UpperLeft : 通話中のスピーカーの PiP が画面の左上隅に表示されます。

UpperCenter : 通話中のスピーカーの PiP が画面の上部中央に表示されます。

UpperRight : 通話中のスピーカーの PiP が画面の右上隅に表示されます。

CenterLeft : 通話中のスピーカーの PiP が画面の左中央に表示されます。

CenterRight : 通話中のスピーカーの PiP が画面の右中央に表示されます。

LowerLeft : 通話中のスピーカーの PiP が画面の左下隅に表示されます。

LowerRight : 通話中のスピーカーの PiP が画面の右下隅に表示されます。

Video DefaultLayoutFamily Local

ローカルで使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Equal/Prominent/Overlay/Single

Auto : デバイスによって提供されるローカル レイアウト データベースの指定に従って、デフォルトのレイアウト ファミリがローカル レイアウトとして使用されます。

Equal : Equal レイアウト ファミリがローカル レイアウトとして使用されます。画面上に十分なスペースがある限り、すべてのビデオのサイズは等しくなります。

Prominent : [対象拡大表示 (Prominent)] レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは大きい画像となり、他の参加者は小さい画像となります。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Overlay : [オーバーレイ (Overlay)] レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となり、他の参加者は小さいピクチャ イン ピクチャ (PiP) となります。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Single : 通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Video DefaultMainSource

発信を開始する際にデフォルトのメイン ビデオ ソースとして使用されるビデオ入力ソースを定義します。

必要なユーザ ロール : admin、user

デフォルト値: 1

値スペース : 1

デフォルトのメインビデオソースとして使用されるソース。

Video Input Connector [n] CameraControl CameraId

n: 1.. 2

カメラ ID は、このビデオ入力に接続されているカメラの一意の ID です。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Connector n:

設定可能な値: Connector n:
カメラ ID は固定されており、変更できません。

Video Input Connector [n] CameraControl Mode

n: 1..2

カメラを制御可能にするかどうかを定義します。この値は、コネクタ 1 (内蔵カメラ) とコネクタ 2 (HDMI) の両方について固定であり、変更することはできません。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Connector n: Off

設定可能な値 : Connector n: Off
Off : カメラ制御をディセーブルにします。

Video Input Connector [n] InputSourceType

n: 1..2

ビデオ入力に接続された入力ソースのタイプを選択します。
コネクタ 1 はデバイスの内蔵カメラであることに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Connector 1 : camera Connector 2 : PC

値スペース : Connector 1 : camera Connector 2 : PC/camera/document_camera/mediaplayer/whiteboard/other
PC : コンピュータがビデオ入力に接続されている場合に使用します。
camera : カメラがビデオ入力に接続されている場合に使用します。
document_camera : ドキュメント カメラがビデオ入力に接続されている場合に使用します。
mediaplayer : メディア プレーヤーがビデオ入力に接続されている場合に使用します。
whiteboard : ホワイトボード カメラがビデオ入力に接続されている場合に使用します。
other : 他のオプションが当てはまらない場合に使用します。

Video Input Connector [n] Name

n: 1..2

ビデオ入力コネクタの名前を定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Connector n: ""

値スペース : 文字列 (0, 50)
ビデオ入力コネクタの名前。

Video Input Connector [n] OptimalDefinition Profile

n: 1..2

この設定は、対応する Video Input Connector [n] Quality 設定が Sharpness に設定されている場合には無効です。

最適鮮明度プロファイルは、ビデオ会議室の照明状態とカメラと品質を反映します。光の条件およびカメラの品質が優れているほど、プロファイルが高くなります。通常、Normal または Medium プロファイルが推奨されます。ただし、光の条件が良い場合、特定のコール率の解像度を大きくするために、High プロファイルを設定できます。解像度が発信側と着信側の両方のデバイスでサポートされている必要があります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Medium

値スペース : Normal/Medium/High

Normal : 照明が通常から不良の環境には、このプロファイルを使用します。解像度は控えめに設定されます。

Medium : 安定した光条件および高品質なビデオ入力が必要です。一部のコール レートの場合、これは高解像度へ移動できます。

High : 優れた全体的なエクスペリエンスを実現するには、理想に近いビデオ会議の光の状態および高品質なビデオ入力が必要です。相当高い解像度が使用されます。

Video Input Connector [n] PresentationSelection

n: 2..2

プレゼンテーション ソースをビデオ入力に接続したときの、ビデオ会議デバイスの動作を定義します。

デバイスがスタンバイ モードの場合、プレゼンテーション ソースを接続すると起動します。遠端とプレゼンテーションを共有するには、この設定が AutoShare に設定されていなければ、追加操作 (ユーザ インターフェイスで [共有 (Share)] を選択) が必要です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Connector n: Desktop

設定可能な値: Connector n: AutoShare/Desktop/Manual/OnConnect

AutoShare : 通話時に、ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) 、自動的に遠端とローカル画面に表示されます。ユーザ インターフェイス上で [共有 (Share)] を選択する必要はありません。コールの発信時または応答時にプレゼンテーション ソースがすでに接続されている場合は、ユーザ インターフェイス上で [共有 (Share)] を手動で選択する必要があります。

Desktop : ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) 、画面に表示されます。これは、アイドル状態のときと通話中のときの両方に適用されます。また、ビデオ入力のコンテンツは、通話の終了時にアクティブ入力であれば、画面に表示されたままとなります。

Manual : ユーザ インターフェイスで [共有 (Share)] を選択するまでビデオ入力の内容は画面に表示されません。

OnConnect : ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが起動すると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) 、画面に表示されます。それ以外の場合は、Manual モードと同じ動作です。

Video Input Connector [n] Quality

n: 2..2

ビデオのエンコーディングと送信のときには、高解像度と高フレーム レートとの間にトレード オフが存在します。一部のビデオ ソースでは、高フレーム レートが高解像度より重要である場合や、逆の場合もあります。この設定で、高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: Connector n: Sharpness

設定可能な値: Connector n: Motion/Sharpness

Motion : できるだけ高いフレーム レートにします。通常、多数の参加者がいる場合や画像の動きが激しい場合など、高フレーム レートが必要なときに使用されます。

Sharpness : できるだけ高い解像度にします。詳細なイメージやグラフィックに高い品質が必要な場合に使用されます。

Video Input Connector [n] RGBQuantizationRange

n: 2..2

ビデオ入力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していません。その場合、ソースの完全なイメージを取得するために、この設定を使用して設定を上書きできます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Full/Limited

Auto : RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて自動的に選択されます。CE ビデオ形式は、限定された量子化範囲レベルを使用します。IT ビデオ形式は、完全な量子化範囲レベルを使用します。

Full : 完全な量子化の範囲。R、G、B の量子化範囲にはすべてのコード値 (0 ～ 255) が含まれます。これは CEA-861-E で規定されています。

Limited : 限定された量子化の範囲。極端なコード値を除いた R、G、B の量子化範囲 (16 ～ 235) 。これは CEA-861-E で規定されています。

Video Input Connector [n] Visibility

n: 1..2

ユーザ インターフェイスのメニューにあるビデオ入力コネクタの表示を定義します。

コネクタ 1 はデバイスの内蔵カメラであり、プレゼンテーション ソースとして使用できないことに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Connector 1: Never Connector 2: IfSignal

値スペース : Connector 1: Never Connector 2: Always/IfSignal/Never

Always : ビデオ入力コネクタ用メニュー選択は、ユーザ インターフェイスに常に表示されます。

IfSignal : ビデオ入力コネクタ用メニュー選択は、ビデオ入力に何か接続されている場合のみ表示されます。

Never : 入力の送信元はプレゼンテーション ソースとして使用されないため、ユーザ インターフェイスに表示されません。

Video Monitors

モニタ レイアウト モードを定義します。デバイスがサポートするスクリーンは 1 台のみのため、この値は固定で変更できないことに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Single

値スペース : Single

Single : レイアウトは、デバイスの画面に表示されます。

Video Output Connector [n] Brightness

n: 1.. 1

デバイスの内蔵画面の明るさレベルを定義します。

必要なユーザ ロール : admin、user

デフォルト値: 80

値スペース : 整数 (0..100)

範囲 : 値は 0 ～ 100 である必要があります。

Video Output Connector [n] Resolution

n: 1.. 1

内蔵画面の解像度と更新間隔。この値は固定されており、変更できません。

デフォルト値 : 1920_1080_60

値スペース : 1920_1080_60

1920_1080_60 : 解像度は 1920 X 1080、リフレッシュ レートは 60 Hz です。

Video Output Connector [n] Whitebalance Level

n: 1.. 1

内蔵スクリーンの色温度 (ホワイト バランス) を、4000 K (暖色) ～ 9000 K (寒色) の間で調整します。

必要なユーザ ロール : admin、user

デフォルト値: 6500

値スペース : 整数 (4000..9000)

ケルビン単位の色温度。

Video Presentation DefaultPIPPosition

プレゼンテーションのピクチャインピクチャ (PiP) の画面上の位置を定義します。この設定は、たとえばユーザ インターフェイスを使用して、プレゼンテーションが明示的に PiP に縮小された場合にのみ有効です。この設定は、次回以降のコールで有効になります。コール中に変更された場合、現在のコールへの影響はありません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : プレゼンテーション PiP の位置はコール終了後にも変更されません。

UpperLeft : プレゼンテーション PiP が画面の左上隅に表示されます。

UpperCenter : プレゼンテーション PiP が画面の上部中央に表示されます。

UpperRight : プレゼンテーション PiP が画面の右上隅に表示されます。

CenterLeft : プレゼンテーション PiP が画面の左中央に表示されます。

CenterRight : プレゼンテーション PiP が画面の右中央に表示されます。

LowerLeft : プレゼンテーション PiP が画面の左下隅に表示されます。

LowerRight : プレゼンテーション PiP が画面の右下隅に表示されます。

Video Presentation DefaultSource

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソースを定義します。この設定は、API およびサードパーティのユーザ インターフェイスで使用できます。Cisco が提供するユーザ インターフェイスの使用時には関係ありません。

必要なユーザ ロール : admin、user

デフォルト値 : 2

値スペース : 2

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソース。

Video Presentation Priority

帯域幅がメインビデオチャネルとプレゼンテーションチャネル間で分散される方法を決定します。

必要なユーザ ロール : ADMIN

デフォルト値: Equal

値スペース: Equal/High/Low

利用可能なビデオ伝送帯域幅がメインチャネルとプレゼンテーションチャネルの間で分散されます。

High : プレゼンテーションチャネルは、メインビデオチャネルを犠牲にして、利用可能な帯域の大部分に割り当てられます。

Low : メインビデオチャネルは、プレゼンテーションチャネルを犠牲にして、利用可能な帯域の大部分に割り当てられます。

Video Selfview Default FullscreenMode

コール終了後に、メイン ビデオ ソース (セルフビュー) を全画面表示するか、小さいピクチャインピクチャ (PiP) として表示するかを定義します。この設定はセルフビューがオンになっている場合にのみ有効です (Video Selfview Default Mode の設定を参照) 。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Off/Current/On

Off : セルフビューは PiP として表示されます。

Current : セルフビューの画像のサイズはコール終了時に未変更の状態に保たれます。つまりコール中に PiP であった場合はコール終了後にも PiP のままであり、コール中に全画面であった場合はコール終了後にも全画面のままです。

On : セルフビューの画像は全画面表示されます。

Video Selfview Default Mode

コール終了後にメイン ビデオ ソース (セルフビュー) を画面に表示するかどうかを定義します。セルフビュー ウィンドウの位置とサイズはそれぞれ、Video Selfview Default PIPPosition と Video Selfview Default FullscreenMode の設定によって決まります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Off/Current/On

Off : セルフビューはコール退出時にオフにされます。

Current : セルフビューはそのままの状態で残ります。つまりコール中にオンであった場合はコール終了後にもオンのままであり、コール中にオフであった場合はコール終了後にもオフのままです。

On : セルフビューはコール退出時にオンにされます。

Video Selfview Default OnMonitorRole

コールの後にメイン ビデオ ソース (セルフビュー) を表示するスクリーンを決定します。デバイスにはスクリーンが 1 台のみ搭載されているため、この値は固定で変更できないことに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : First

値スペース : First

First : セルフビューの画像は内蔵スクリーンに表示されます。

Video Selfview Default PIPPosition

コール終了後に小さいセルフビュー ピクチャインピクチャ (PiP) を表示する画面上の位置を定義します。この設定は、セルフビューがオンになっており (Video Selfview Default Mode 設定を参照) 、全画面表示がオフになっている場合 (Video Selfview Default FullscreenMode 設定を参照) にのみ有効です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : セルフビュー PiP の位置はコール終了後にも変更されません。

UpperLeft : セルフビュー PiP が画面の左上隅に表示されます。

UpperCenter : セルフビュー PiP が画面の上部中央に表示されます。

UpperRight : セルフビュー PiP が画面の右上隅に表示されます。

CenterLeft : セルフビュー PiP が画面の左中央に表示されます。

CenterRight : セルフビュー PiP が画面の右中央に表示されます。

LowerLeft : セルフビュー PiP が画面の左下隅に表示されます。

LowerRight : セルフビュー PiP が画面の右下隅に表示されます。

Video Selfview Mirrored

自身を鏡映しにしたときのような、相手に見える状態のセルフビュー イメージを表示するようにデバイスを設定できます。

この設定は、遠方に送信されるビデオに影響を与えません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : 他人から見えている自分のようにセルフビューを表示します。

On : 鏡に映っている自分のようにセルフビューを表示します。

Video Selfview OnCall Mode

コールをセットアップする短い間、この設定を使用してセルフ ビューがオンにされます。セルフビューをオンのままにしておく時間の長さは、Video Selfview OnCall Duration 設定で定義します。これは一般にセルフ ビューがオフの場合に適用されます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : セルフ ビューはコール セットアップ中に自動的に表示されません。

On : セルフ ビューはコール セットアップ中に自動的に表示されます。

Video Selfview OnCall Duration

この設定は Video Selfview OnCall Mode 設定がオンになっている場合にのみ有効です。この場合、ここで設定された秒数により、自動的にオフにされる前にセルフ ビューが表示される期間が決まります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 10

値スペース : 整数 (1..60)

範囲 : セルフ ビューをオンにする期間を選択します。有効な範囲は、1 ～ 60 秒です。

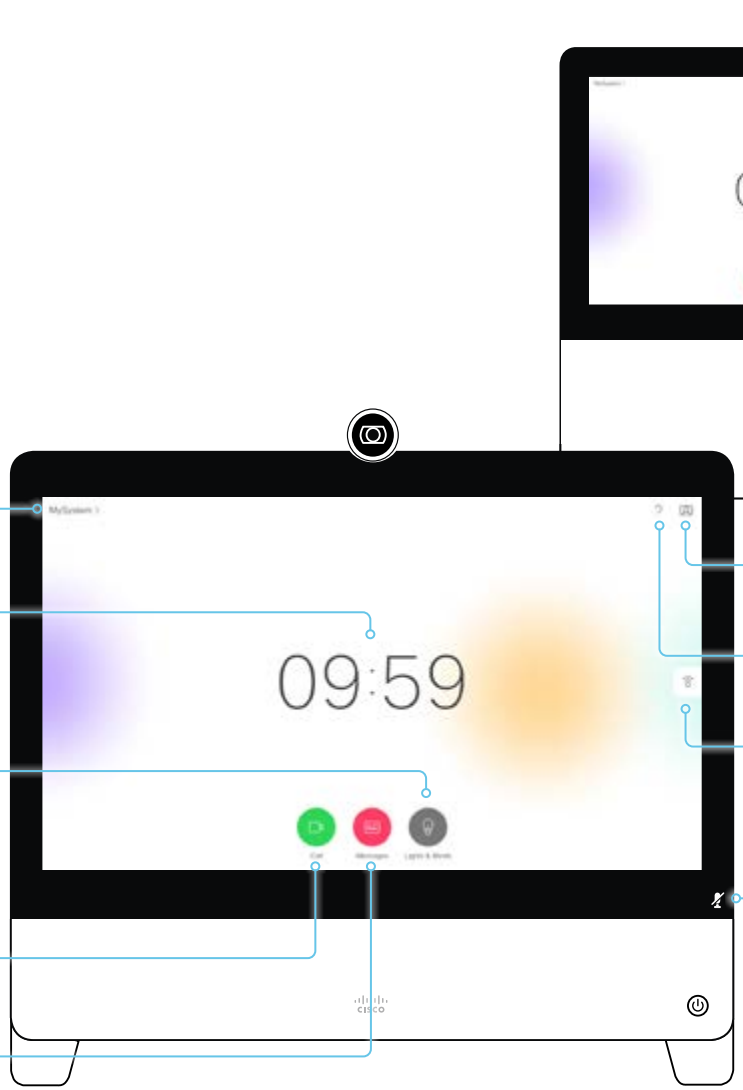
試験的設定

試験的設定は、テストのためだけのもので、Cisco と同意したのでない限り使用できません。これらの設定は記載されておらず、以降のリリースで変更されます。

付録

ユーザ インターフェイス

ユーザ インターフェイスとその使用方法の詳細については、ビデオ会議デバイスのユーザ ガイドをご覧ください。



装置の右側：
- ヘッドセット用の USB ソケットとミニジャック ソケット

マイク：ミュート/ミュート解除。

スピーカーの音量コントロール。

セルフビュー：オン/オフ

? をタップして、ヘルプ デスクまたはその他のファシリティ サービスに問い合わせます（有効な場合）。

Proximity を使用して 1 つ以上のクライアントがデバイスとペアになっていることを示します。

マイクのミュート インジケータ。

装置の右側：
- マイクのミュート ボタン
- スピーカーの音量コントロール
- ヘッドセット用の USB ソケット

デバイス名またはアドレスをタップすると、[システム情報 (*System Information*)]、[設定 (*Settings*)]、[再起動 (*Restart*)] および [初期設定へのリセット (*Factory Reset*)] にアクセスできます。画面の明るさを調整し、コール転送モード、スタンバイ モード、応答不可モードをアクティブにすることもできます。

時刻を指定します。

ユーザ インターフェイス拡張機能のエントリ ポイント（お使いのデバイスでは、これと異なる色、テキスト、アイコンのボタンがある場合があります）。

[発信 (*Call*)] をタップすると、[お気に入り (Favorites)] リスト、[ディレクトリ (Directory)] リスト、[発着信履歴 (Recents)] リストなどの連絡先を呼び出したり、[検索またはダイヤル (Search or Dial)] フィールドを開いたりできます。

該当する場合、[メッセージ (*Messages*)] をタップして、ボイス メール システムを呼び出します。

リモート モニタリングのセットアップ

要件:

- RemoteMonitoring オプション

リモート モニタリングは別の場所からデバイスを制御する場合に便利です。

入力ソースからのスナップショットが ウェブ インターフェイスに表示されるため、部屋にいなくてもカメラ ビューをチェックしてカメラを制御できます。

有効にすると、スナップショットは約 5 秒おきに自動的に更新されます。

デバイスでリモート モニタリング オプションを設定するかどうかの確認

1. ウェブ インターフェイスにログインします。
2. [ホーム (Home)] ページで、インストールされているオプションのリストに *RemoteMonitoring* が含まれているかどうかを確認します。

   リストにない場合、リモート モニタリングは使用できません。

リモート モニタリングを有効にする

RemoteMonitoring オプション キーをインストールします。オプション キーのインストール方法については、►「オプション キーを追加する」の章で説明しています。

リモート モニタリング オプションを有効にする場合は、プライバシーに関する地域の法律および規制を遵守する必要があります。また、システム管理者がカメラや画面を監視および制御する場合があることを、デバイスのユーザに適切な方法で通知してください。デバイスの使用時にプライバシー規制を遵守するのはお客様の責任であり、シスコはこの機能の違法な使用について一切の責任を追わないものとします。

スナップショットについて

ローカル入力ソース

デバイスのローカル入力ソースのスナップショットは [コール制御 (Call Control)] ページに表示されます。

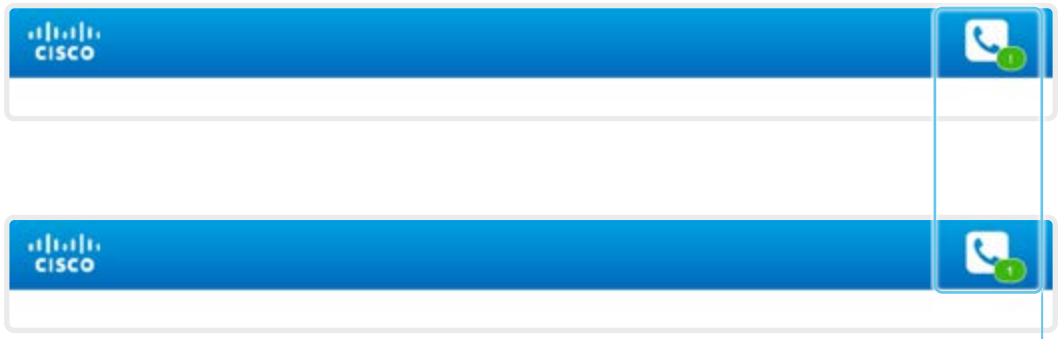
スナップショットは、デバイスがアイドル状態のときおよびコール中に表示されます。

遠端のスナップショット

通話中の場合、遠端カメラからのスナップショットも表示できます。これは、相手先デバイスでリモート モニタリング オプションが設定されているかどうかとは関係がありません。

遠端スナップショットは、コールが暗号化されていると表示されません。

ウェブ インターフェイスを使用したコール情報へのアクセスとコール応答



着信通知

[コールインジケーター (*Call indicator*)] をクリックし、コールの応答と拒否を行う [コール操作 (*Call Control*)]ページを開きます。

デバイスがコール中

コールインジケーター

コール インジケータは、着信コールについて通知するため、およびデバイスがコール中であるときを表示するために用意されています。

デバイスがアイドル状態の場合、コール インジケータは表示されません。

コールの操作

[コール操作 (Call Control)]ページでは、コール操作に関係する操作ボタンが表示されます。各ボタンを使用して次のことを実行します。

- コールの詳細を表示する
- コールを保留にする
- 通話に応答する
- コールを切断する

ウェブ インターフェイスを使用してコールをかける (1/2 ページ)

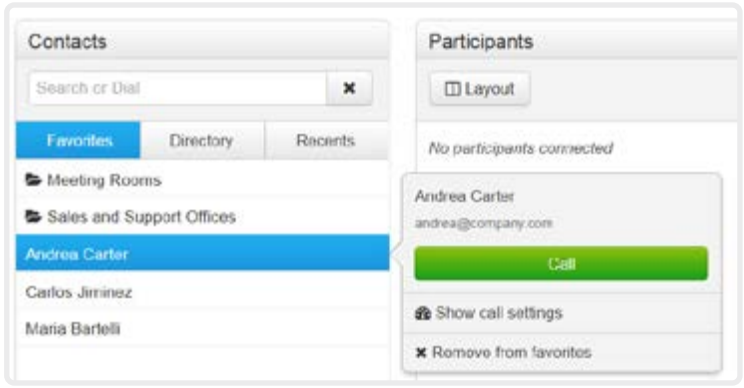
ウェブ インターフェイスにログインし、[コール制御 (*Call Control*)] に移動します。

コールの発信

Web インターフェイスを使ってコールを開始した場合でも、コールに使用されるのはビデオ会議デバイス (ディスプレイ、マイク、およびスピーカー) であり、Web インターフェイスを実行している PC ではありません。

1. 正しいエントリを見つけるには、[お気に入り (*Favorites*)] リスト、[ディレクトリ (*Directory*)] リスト、または [発着信履歴 (*Recents*)] リストに移動するか、あるいは [検索またはダイヤル (*Search or Dial*)] フィールドに 1 文字以上を入力します*。該当する連絡先名をクリックします。
2. 連絡先カードで [コール (*Call*)] をクリックします。

または、[検索して発信 (Search and Dial)] フィールドに完全な URI または番号を入力します。次に、URI または番号の横に表示される [コール (*Call*)] ボタンをクリックします。



DTMF トーンの送信

アプリケーションが DTMF (デュアルトーン多重周波数) シグナリングを必要とする場合は、クリックしてキー パッドを開きます。

コールの詳細の表示/非表示

情報ボタンをクリックすると、コールの詳細情報が表示されます。

もう一度ボタンをクリックすると情報が非表示になります。

コールの保留および復帰

参加者を保留にするには、その名前の横にある ボタンを使用します。

コールを再開するには、保留中の参加者に表示される ボタンを使用します。

コールの終了

コールを終了するには、[全通話切断 (*Disconnect all*)] または ボタンをクリックします。

* 検索時には、入力内容に応じて、[お気に入り (*Favorites*)]、[ディレクトリ (*Directory*)]、および [履歴 (*Recents*)] リストの一致するエントリが表示されます。

ウェブ インターフェイスを使用したコールの発信 (2/2 ページ)

ウェブ インターフェイスにログインし、[コール制御 (*Call Control*)] に移動します。

複数の相手に発信

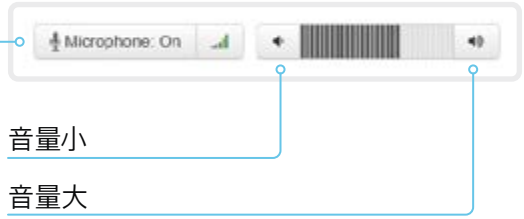
会議ブリッジを使用した複数の相手に対するコール (CUCM アドホック会議) は、ビデオ会議デバイス自身でサポートされていても Web インターフェイスではサポートされません。

音量の調整

マイクをミュートにする

[マイク: オン (*Microphone: On*)] をクリックして、マイクをミュートにします。すると、テキストが [マイク: オフ (*Microphone: Off*)] に変わります。

ミュートを解除するには、[マイク: オフ (*Microphone: Off*)] をクリックします。



ウェブインターフェイスを使用してコンテンツを共有する

ウェブ インターフェイスにログインし、[コール制御 (*Call Control*)] に移動します。

コンテンツの共有

1. [プレゼンテーションの開始 (*Start Presentation*)] をクリックします。すると、テキストが [プレゼンテーションの停止 (*Stop Presentation*)] に変わります。

コンテンツ共有の停止 :

共有している間に表示される [プレゼンテーションを中止 (*Stop Presentation*)] ボタンをクリックします。

スナップショット領域

選択されたプレゼンテーション ソースのスナップショットが表示されます。

リモート モニタリングオプションが設定されているデバイスでのみ利用できます。

コンテンツ シェアリング (共有) について

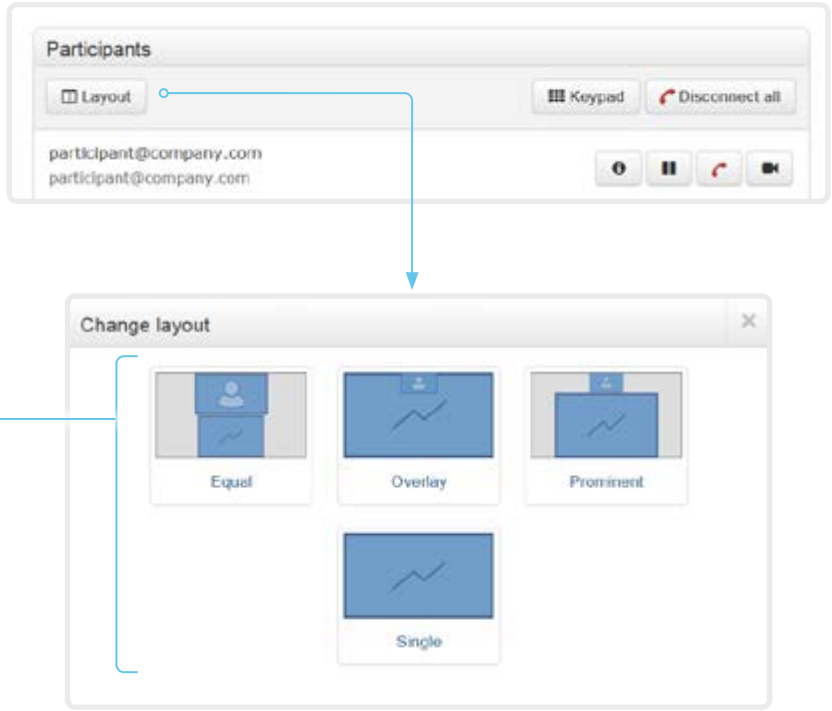
プレゼンテーション ソース (最も多いのは PC) は、デバイスの背面にあるコンピュータ用の HDMI 入力コネクタに接続できます。

コールの間、コールの他の参加者 (相手先) とコンテンツを共有できます。

コール (通話) 中でない場合は、コンテンツはローカルに表示されます。

ローカル レイアウトの制御

ウェブ インターフェイスにログインし、[コール制御 (*Call Control*)] に移動します。



レイアウトの変更

[レイアウト (*Layout*)] をクリックし、表示されるウィンドウで望ましいレイアウトを選択します。

選択するレイアウトのセットは、デバイスの設定によって異なります。

レイアウトは、アイドル中でも通話中でも変更可能です。

レイアウトについて

ここでいうレイアウトとは、プレゼンテーションとビデオを画面に表示するさまざまな方法のことです。会議の種類によって、レイアウトを変える必要があります。

相手先カメラの制御

ウェブ インターフェイスにログインし、[コール制御 (*Call Control*)] に移動します。

前提条件

以下の条件において、通話中にリモート参加者のカメラ (相手先) を制御できます。

- 相手先デバイスで [会議 (*Conference*)] > [相手先制御 (*FarEndControl*)] > [モード (*Mode*)] 設定が [オン (On)] になっている。
- 遠端カメラにパン、チルト、ズーム機能がある。関連する制御のみ表示される。
- 遠端カメラではスピーカーのトラッキングはオンになっていない。
- ローカル デバイスでリモート モニタリング オプションが設定されている。

リモート参加者のカメラを制御

1. リモート カメラ制御ウィンドウを開くには、カメラのアイコンをクリックします。
2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および - を使用します。

   遠端カメラの制御が許可されていない場合は、画面にコントロールが表示されません。

   コールが暗号化されている場合、制御の背後の遠端スナップショットは表示されません。

パケット損失の復元力：ClearPath

ClearPath により、高度なパケット損失復元メカニズムを導入できます。これらのメカニズムは、エラーを起こしやすい環境でデバイスを使用する場合の品質を向上させます。

ClearPath は Cisco 独自のプロトコルです。CE ソフトウェアが実行されているすべてのエンドポイントが ClearPath に対応しています。

関係するエンドポイントとインフラストラクチャ要素が ClearPath に対応している場合、ポイントツーポイント接続（ホストされた会議を含む）ですべてのパケット損失復元メカニズムが使用されます。

カスタマイゼーション

ビデオ会議デバイスのユーザーインターフェイスのカスタマイズ (ページ 1/2)

ユーザ インターフェイスをカスタマイズして、照明やブラインドなど、会議室内の周辺機器を制御したり、マクロをトリガーしてビデオ会議デバイスの動作を変更したりできます。

これにより、制御システムの機能と、ビデオ会議デバイスの使いやすいユーザ インターフェイスを強力に組み合わせることができます。

室内制御パネルの例

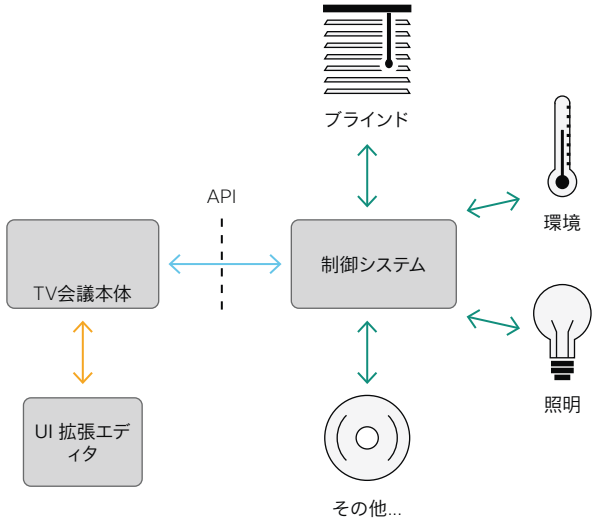
UI 拡張エディタ (以前の室内制御エディタ) を使用してカスタムのユーザ インターフェイス パネルとアクション ボタンを設計する方法、およびビデオ会議デバイスの API を使用してコントロールとアクションをプログラミングする方法の詳細については、カスタマイズ ガイドをご覧ください。次のリンクにアクセスします。

▶ https://www.cisco.com/go/in-room-control-docs

室内制御アーキテクチャ

タッチインターフェイスを搭載したシスコのビデオ会議デバイスと、制御システムが必要です。制御システムは、ハードウェア ドライブや周辺機器を備えた Crestron や AMX などの他社製システムである場合もあります。これはビデオ会議デバイスではなく、周辺機器を制御するコントロール システムです。

コントロール システムをプログラミングするときは、ビデオ会議デバイスのユーザ インターフェイス上のコントロールに接続するために、ビデオ会議デバイスの API (イベントとコマンド) を使用する必要があります。



室内制御の概略図

ビデオ会議デバイスのマクロ フレームワークは、コントロール システムとしても使用できます。この場合、コントロール システムはデバイスの API を使用して、短縮ダイヤル、言語の選択、カスタマイズされたシステムのリセットなど、あらゆる種類のローカル機能をトリガーすることができます。

カスタマイゼーション

ビデオ会議デバイスのユーザーインターフェイスのカスタマイズ (ページ 2/2)

UI 拡張エディタ

無料のエディタ

ビデオ会議デバイスのソフトウェアには、ドラッグアンドドロップ方式の使いやすいエディタが無償で付属しています。カスタムのユーザ インターフェイス拡張機能 (アクション ボタン、および室内制御などのカスタム パネル) を作成するには、このエディタを使用します。

Web インターフェイスにサインイン*し、[統合 (*Integration*)] > [UI拡張エディタ (*UI Extensions Editor*)] に移動します。

- エディターがデバイスの Web インターフェイスで直接開きます。

  新しいパネルまたはアクション ボタンを作成してデバイスにプッシュし、その結果をすぐにユーザ インターフェイスで確認することができます。

- [エディタ (Editor)] メニュー ☰ をクリックし、[エディタをダウンロード (*Download the Editor*)] を選択すると、ハード ドライブからローカルにブラウザで実行できるスタンドアロン バージョンを入手できます。

  これにより、デバイスに接続しなくてもカスタム ユーザ インターフェイスを作成できます。後でファイルをエクスポートおよびインポートして、ローカル バージョンとデバイスの間で作業を移動することができます。

プレビュー機能

エディタは、カスタム インターフェイスがどのようにユーザ インターフェイスに表示されるか確認するためのプレビュー機能も提供します。

プレビュー機能ではカスタム パネルがソフトウェア的に完全に再現されるため、コントロールをクリックすると、実際のユーザ インターフェイスでコントロールを選択した場合と同じアクションが実行されます。

したがって、実際の ユーザ インターフェイスを有効にすることなく、プレビュー機能を使用してお使いの統合をテストできます。リモートの場所からデバイスのカスタム パネルを使用することもできます。

* UI 拡張エディタおよびプログラミングに必要な API コマンドにアクセスするには、ROOMCONTROL、INTEGRATOR、または ADMIN ユーザ ロールを持つユーザが必要です。

カスタマイゼーション

マクロを使用したビデオ会議デバイスの動作のカスタマイズ

マクロにより、デバイスで実行するコードの独自のスニペットを作成できます。言語は、arrow functions、promises および classes などの機能をサポートする JavaScript/ECMAScript 6 です。

インテグレータは、マクロ フレームワークを利用して、個別の顧客要件に応じてデバイスの動作を調整するスクリプトを作成できます。インテグレータが行える作業には、独自の機能または機能のバリエーションの実装、特定の設定または再設定の自動化、機能のカスタム テストやモニタリングの作成などがあります。

マクロの使用とカスタム ユーザ インターフェイス パネル (UI 拡張機能) の作成を組み合わせることで、カスタマイズされたローカル機能をトリガーするようにユーザ インターフェイスを変更できます。以下に例を示します。

- 短縮ダイヤル ボタンの追加
- すべての設定を好みのデフォルト セットアップに戻すためのルーム リセットボタンの追加

マクロの詳細およびデバイスに搭載されているマクロ エディタの使用方法については、カスタマイズ ガイドをご覧ください。次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

デバイスでのマクロの使用許可

ウェブ インターフェイスにサインインして、[セットアップ (*Setup*)] > [設定 (*Configuration*)] に移動します。

- [マクロ (Macros)] > [モード (Mode)] を [オン (**On**)] に設定します。

  この設定が [オフ (**Off**)] の場合にマクロ エディタを起動しようとすると、ポップアップ メッセージが表示されます。[マクロの有効化 (*Enable Macros*)] をタップして応答した場合は [マクロ (*Macros*)] > [モード (*Mode*)] 設定が自動的に [オン (**On**)] に変更され 、エディタが起動します。

マクロ エディタの起動

Web インターフェイスにサインインし*、[統合 (*Integration*)] > [マクロエディタ (*Macro Editor*)] に移動します。

オフラインで使用可能なエディタのスタンドアロン バージョンは提供されていません。

マクロ エディタ

マクロ エディタは、以下のことができる強力なツールです。

- 変更したり、そのまま使用したり、または自身のマクロを記述する際のヒントとして使用したりするコードの例をロードできます。
- 詳細なマクロ記述チュートリアルを用意しているので、参照してください。コードの例についても、より詳しく説明しています。
- 独自のマクロを記述して、デバイスにアップロードできます。
- マクロは、個別に有効または無効にできます。
- マクロを実行したときの動作は、組み込みのログ コンソールで確認できます。

* マクロ エディタにアクセスするには、ADMIN ユーザ ロールを保持しているユーザが必要です。

カスタマイゼーション

ユーザ インターフェイスからデフォルトボタンを削除する

通話 または 共有などのデフォルトボタンを使用しない使用例もあります。このような使用しないボタンは混乱を引き起こす場合があります。このような場合、使用しないボタンをユーザインターフェイスから削除できます。その場合もカスタム UI ボタンは表示できます。カスタムボタンの追加中にデフォルトボタンを削除すると、ユーザインターフェイスを完全にカスタマイズできるようになります。

たとえば、誰もこのデバイスからコンテンツや通話を共有しない場合は、[通話 (Call)] ボタンと [共有 (Share)] ボタンを削除できます。代わりに、実行する予定のタスク用のカスタム ボタンとパネルを追加します。

構成

ユーザ インターフェイスからデフォルトのボタンを削除するには、次の設定を使用します。設定は、デバイスの Web インターフェイスと API の両方から利用できます。

- [ユーザインターフェイス (*UserInterface*)] > [機能 (*Features*)] > [コール (*Call*)] > [開始 (*Start*)] : デフォルトの [コール (*Call*)] ボタンを削除します (ディレクトリ、お気に入り、コール履歴リストも含まれます) 。コール中に表示される、参加者の [追加 (Add)] ボタンも削除されます。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [共有 (Share)] > [開始 (Start)]: 通話中および通話中以外の両方で、コンテンツの共有およびプレビュー用のデフォルトユーザ インターフェイスを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [通話 (Call)] > [ビデオミュート (VideoMute)]: デフォルト ビデオをオフにする ボタンを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [すべて非表示 (HideAll)]: すべてのデフォルトボタンを削除します。カスタム ボタンは削除されません。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [通話 (Call)] > [終了 (End)]: 通話終了 ボタンを削除します。
- [ユーザインターフェイス (*UserInterface*)] > [機能 (*Features*)] > [コール (*Call*)] > [コール中制御 (*MidCallControls*)] : コール中の [保留 (Hold)]、[保留解除 (Resume)]、および [転送 (Transfer)] ボタンを削除します。

設定はボタンだけを削除し、機能などは削除しません。共有 ボタンをユーザーインターフェイスから削除しても、Proximity を使用してコンテンツを共有できます。

解説場所

ボタンの削除方法およびユーザインターフェイスのカスタマイズ方法については カスタマイズガイドを参照してください。 次のリンクにアクセスします。

▶ https://www.cisco.com/go/in-room-control-docs

カスタマイゼーション

サードパーティ USB 入力デバイスの使用

サードパーティ製の USB 入力デバイスを使用して、ビデオ会議デバイスの特定の機能を制御できます。USB ドングルや USB キーボードでの Bluetooth リモート制御はこのような入力デバイスの一例です。

この機能は、Touch 10 または DX ユーザ インターフェイス、いずれか便利な方の機能の補正を意味しています。Touch 10 および DXのユーザ インターフェイスを置き換えるという意味ではありません。

アプリケーションの例

- クラスルームや講義で、小型のリモコンを使用してビデオ会議デバイスをスタンバイ モードから復帰させることができます。また、表示する入力ソースを選択するためにリモート制御を使用するのも便利です。
- Touch 10 を使用できない状況でのカメラビュー（パン、チルト、ズーム）の制御例えば、病院の手術室。

機能の概要

USB 入力デバイスのボタンを押すと、API でイベントが生成されます。マクロまたはサードパーティーの制御デバイスは、こういったイベントをリッスンして応答することが可能です。この動作は、カスタム UI ボタン（UI 拡張機能）の動作と似ています。ウェブフックを使って、直接SSH セッションでイベントをリッスンすることも可能です。

アクション選択からすぐに利用できるアクションのライブラリはありません。ご自身で、イベントに対する応答として行うアクションを定義して実装する必要があります。次に例を示します。

- [音量アップ（Volume Up）] キーが押されたら、ビデオ会議デバイスの音量を上げます。
- [スリープ（Sleep）] キーが押されたら、ビデオ会議デバイスをスタンバイモードにします。

設定、イベント、およびステータス

USB 入力デバイスのサポートはデフォルトで無効になっています。周辺機器 > InputDevice > モード を オンに設定することで明示的に有効にします。

ボタンを押してから離すと、押されたおよびリリースされたイベントが作成されます：

```
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Pressed
** end
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Released
** end
```

イベントをリッスンするには、InputDevice イベントからのフィードバックを登録する必要があります。

```
xFeedback Register /event/UserInterface/InputDevice
** end
```

ビデオ会議デバイスでサードパーティの入力デバイスが検出されると、その入力デバイスがビデオ会議デバイスの [ユーザインターフェイス（*UserInterface*）] > [周辺機器（*Peripherals*）] > [接続されているデバイス（*ConnectedDevice*）] ステータスに表示されます。入力デバイスは複数のデバイスとして報告される場合があります。

必要な工具

- Cisco Webex Room シリーズまたは DX シリーズのデバイス。
- 自体を USB キーボードとしてアドバタイズするサードパーティー入力デバイス。例えば、USB ドングル付きの Bluetooth リモート制御。

解説場所

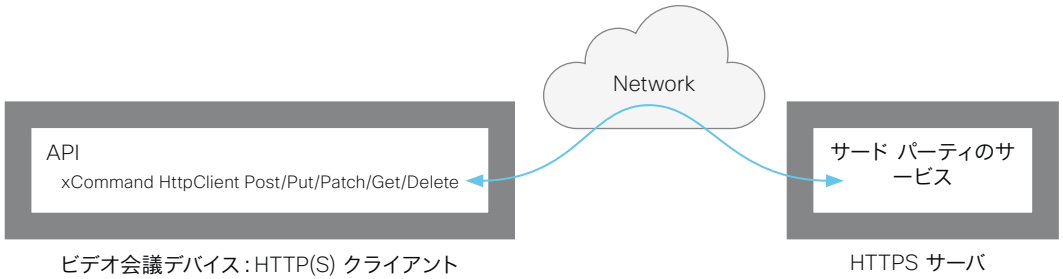
サードパーティー入力デバイスの利用についての詳細は、 カスタマイズガイドをご覧ください。 次のリンクにアクセスします。

▶ https://www.cisco.com/go/in-room-control-docs

Cisco support (TAC) はマクロを含む、サードパーティーコードのデバッグに対応していません。マクロやサードパーティーコードについてのヘルプは、▶Cisco Collaboration Developer コミュニティ を確認してください。

カスタマイゼーション

HTTP(S) 要求の送信



HTTP(S) 要求機能を使用すると、ビデオ会議デバイスから HTTP(S) サーバに任意の HTTP(S) 要求を送信できます。さらに、デバイスはサーバから送信された応答を受信します。このデバイスは、**POST**、**PUT**、**PATCH**、**GET**、および **DELETE** メソッドをサポートします。

マクロを使用することで、いつでもデータを HTTP(S) サーバに送信できます。送信するデータを選択して、必要に応じて構造化することができます。それにより、すでに確立されているサービスにデータを適合させることができます。

セキュリティ対策：

- HTTP(S) 要求機能は、デフォルトでは無効になっています。システム管理者は *HttpClient > モード* を オンに設定することでこの機能を明示的に有効にする必要があります。
- システム管理者は *HttpClient > AllowHTTP* を 偽に設定することで HTTP の使用を防ぐことができます。
- システム管理者は、デバイスがデータを送信可能な先であるHTTP(S) サーバのリストを指定することができます。
- 同時 HTTP(S) 要求の数は制限されています。

許可されている HTTP(S) サーバのリスト

システム管理者はコマンドを使用して最大 10 の許容されている HTTP(S) サーバ (ホスト)のリストを設定し維持できます：

- `xCommand HttpClient Allow Hostname Add Expression: <Regular expression that matches the host name or IP address of the HTTP(S) server>`
- `xCommand HttpClient Allow Hostname Clear`
- `xCommand HttpClient Allow Hostname List`
- `xCommand HttpClient Allow Hostname Remove Id: <id of an entry in the list>`

リストが空でない場合、HTTP(S) リクエストをリスト内のサーバにだけ送信できます。リストが空の場合、リクエストを任意の HTTP(S) サーバに送信できます。

許容されているサーバのリストに対するチェックは、非セキュア (HTTP) およびセキュア (HTTPS) なデータ転送の両方で実行されます。

証明書の検証なしの HTTPS の使用

HTTPS 経由で要求を送信する場合、ビデオ会議デバイスはデフォルトで HTTPS サーバの証明書を確認します。HTTPS サーバ証明書が有効でない場合、 エラーメッセージが表示されます。デバイスはそのサーバにデータを送信しません。

証明書が検証される HTTPs の使用を推奨します。証明書の検証が不可能な場合、システム管理者は [HTTPクライアント (*HttpClient*)] > [セキュアでないHTTPSを許可 (*AllowInsecureHTTPS*)] を [オン (On)] に設定できます。これにより、サーバの証明書を検証せずに HTTPS を使用することができます。

HTTP(S) 要求の送信

HTTP(S) 要求機能が有効になったら、次のコマンドを使用して要求を HTTP(S) サーバに送信できます。

```
xCommand HttpClient <Method>
  [AllowInsecureHTTPS: <True/False>]
  [Header: <Header text>]
  [ResponseSizeLimit: <Maximum response size>]
  [ResultBody: <None/PlainText/Base64>]
  [Timeout: <Timeout period>]
  Url: <URL to send the request to>
```

`<Method>` は、`POST`、`PUT`、`PATCH`、`GET`、`DELETE` のいずれかです。

`Post`、`Put`、および `Patch` コマンドは複数行コマンドです。複数行コマンドの使用方法と、コマンド パラメータの詳細な説明については、API ガイドをお読みください。

解説場所

HTTP(S) Post リクエストについての詳細情報は カスタマイズガイドにあります。 次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

スタートアップ スクリプトを管理する

Web インターフェイスにサインインし、[統合 (*Integration*)] > [スタートアップスクリプト (*Startup Scripts*)] に移動します。

図に示しているスクリプト名と設定は一例です。独自のスクリプトを作成できます。

スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます。*

緑色のドットがアクティブなスタートアップ スクリプトの横に、赤色の丸が非アクティブなスタートアップ スクリプトの横に表示されます。

複数のスタートアップ スクリプトがある場合は、リストの上から下に順番に実行されます。

スタートアップ スクリプトを作成する

1. [新規作成 (*Create new...*)] をクリックします。.
2. タイトル入力フィールドにスタートアップ スクリプトの名前を入力します。
3. コマンド入力エリアにコマンド（xConfiguration または xCommand) を入力します。新しい行で各コマンドを開始します。
4. [*Save* (保存)] をクリックします。
5. [オン (*On*)] をクリックして、スタートアップ スクリプトをアクティブにします。
6. 既存のスクリプトを編集の開始点として使用する場合は、そのスクリプトを選択して [コピー (*Copy*)] をクリックします。

起動スクリプトをすぐに実行する

1. リストからスタートアップ スクリプトを選択します。
2. [実行 (*Run*)] をクリックします。

   アクティブなスタートアップ スクリプトと非アクティブなスタートアップ スクリプトの両方をすぐに実行できます。

スタートアップ スクリプトをアクティブ化または非アクティブ化する

1. リストからスタートアップ スクリプトを選択します。
2. スクリプトをアクティブにする場合は [オン (*On*)] を、非アクティブにする場合は [オフ (*Off*)] をクリックします。

   アクティブなスタートアップ スクリプトは、デバイスが起動するたびに実行されます。

スタートアップ スクリプトを削除する

1. リストからスタートアップ スクリプトを選択します。
2. [削除 (*Delete*)　をクリックします。

スタートアップ スクリプトについて

スタートアップ スクリプトには起動手順の一部として実行されるコマンド (xCommand) および構成 (xConfiguration) が含まれます。

`xCommand SystemUnit Boot` など、いくつかのコマンドとコンフィギュレーションはスタートアップ スクリプトに含めることができません。不正なコマンドや設定が含まれたスクリプトは保存できません。

xCommand および xConfiguration の構文とセマンティックは、製品の API ガイドに説明されています。

デバイスの XML ファイルへのアクセス

ウェブ インターフェイスにサインインして、[統合 (*Integration*)] > [開発者 API (*Developer API*)] を選択します。

XML ファイルはデバイスの API の一部です。デバイスに関する情報が階層で構成されています。

- Configuration.xml には現在のデバイス設定 (構成) が含まれます。これらの設定は、ウェブ インターフェイスまたは API (アプリケーション プログラミング インターフェイス) から制御されます。
- status.xml 内の情報は、デバイスによって常に更新され、システムおよびプロセスの変更が反映されます。ステータス情報は、ウェブ インターフェイスまたは API からモニタします。
- Command.xml には、デバイスにアクションの実行を指示するために使用できるコマンドの概要が含まれています。コマンドは、API から発行されます。
- Valuespace.xml には、デバイス設定、ステータス情報、およびコマンドのすべての値スペースの概要が含まれています。

XML ファイルを開く

XML ファイルを開くにはファイル名をクリックします。

API について

アプリケーション プログラミング インターフェイス (API) は、デバイスを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、デバイスの API ガイドで説明されています。

ウェブ インターフェイスからの API コマンドとコンフィギュレーションの実行

ウェブ インターフェイスにサインインして、[統合 (*Integration*)] > [開発者 API (*Developer API*)] を選択します。

コマンド (xCommand) および設定 (xConfiguration) は、ウェブ インターフェイスから実行できます。構文とセマンティックの説明については、デバイスの API ガイドをご覧ください。

API コマンドとコンフィギュレーションの実行

1. テキスト領域に、コマンド (xCommand または xConfiguration) またはコマンド シーケンスを入力します。
2. [実行 (*Execute*)] をクリックしてコマンドを発行します。

API について

アプリケーション プログラミング インターフェイス (API) は、デバイスを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、デバイスの API ガイドで説明されています。

イーサネットポートについて

メインネットワークポート

メイン ネットワーク ポート - ネットワーク ポート 1 - は常に LAN 接続用に予約されています。これは、すべてのビデオ会議デバイスに適用されます。

ネットワーク ポート 1 は、デバイスに応じて、番号 1、ネットワーク記号（⁂）、またはその両方でマークされます。

補助ポート

ビデオ会議デバイスによっては、ネットワーク ポートが複数あります。追加のポートは、カメラ、Touch 10、サードパーティー製制御システムなどの周辺機器に使用できます。

このようなネットワークポートに接続されているデバイスはコーデックからローカル IP アドレスを取得するため、企業ネットワークには接続されていません。パケットは、メインネットワークポート (LAN) と補助ネットワークポート (リンク-ローカル) の間の移動はできません。

- Cisco の周辺機器には、169.254.1.41 から 169.254.1.240 の範囲 (DHCP) でのダイナミック IP アドレスが割り当てられます。
- Cisco 以外のデバイスには、ダイナミック IP アドレス (DHCP) :169.254.1.30 を割り当てることができます。

  注 : Cisco 以外のデバイスでダイナミック IP アドレスを取得できるのは、一度に 1 つだけです。
- さらに、Cisco 以外のデバイスには、169.254.1.241 ～ 169.254.1.254 の範囲の静的 IP アドレスを割り当てることもできます。

この方法は、SSH を使用してコーデックに接続する場合にも使用できます。このケースでは、IP アドレス 169.254.1.1 を使用できます。

パワーオーバーイーサネット (PoE)

補助ネットワークポートには Power over Ethernet (PoE) を提供するものもあります。これらのポートは Touch 10 コントローラなどの周辺機器に電源を供給します。

製品	補助ネットワークポートの数	PoE 付きの補助ネットワークポートの数
Room Kit	1	0
Room Kit Mini	1	1 ( )
Room 55	1	1 ( )
Room 70 / Room 55 Dual	2	1 ( )
Room 70 G2	4	2 (、PoE)
Codec Plus	2	1 ( )
Codec Pro	4	2 (、PoE)
Board	0	0
SX10	0	0
SX20	0	0
SX80	2	0
MX200 G2 / MX300 G2	2	0
MX700 / MX800	2	0*
DX70 / DX80	1	0

* これらの製品には個別の PoE インジェクタがあり、補助ネットワークポートの 1 つに接続されます。PoE インジェクタは Touch 10 コントローラに使用されます。

シリアル インターフェイス

デバイスとの直接通信には、micro USB コネクタを使用します。マイクロ USB to USB ケーブルが必要です。コンピュータにシリアル ポート ドライバが自動的にインストールされない場合は、手動でシリアル ポート ドライバをインストールする必要があります。

シリアル インターフェイスに接続するには、ターミナル エミュレータ（SSH クライアント）を使用します。最も一般的なコンピュータ タイプ (PC、MAC) およびオペレーティング システムでは、PuTTY または Tera Term は機能します。

シリアル接続は、IP アドレス、DNS、またはネットワークなしで使用できます。

パラメータ :

- ボー レート : 115200 bps
- データ ビット : 8
- パリティ : なし
- ストップ ビット : 1
- ハードウェア フロー制御 : オフ

デバイスの設定

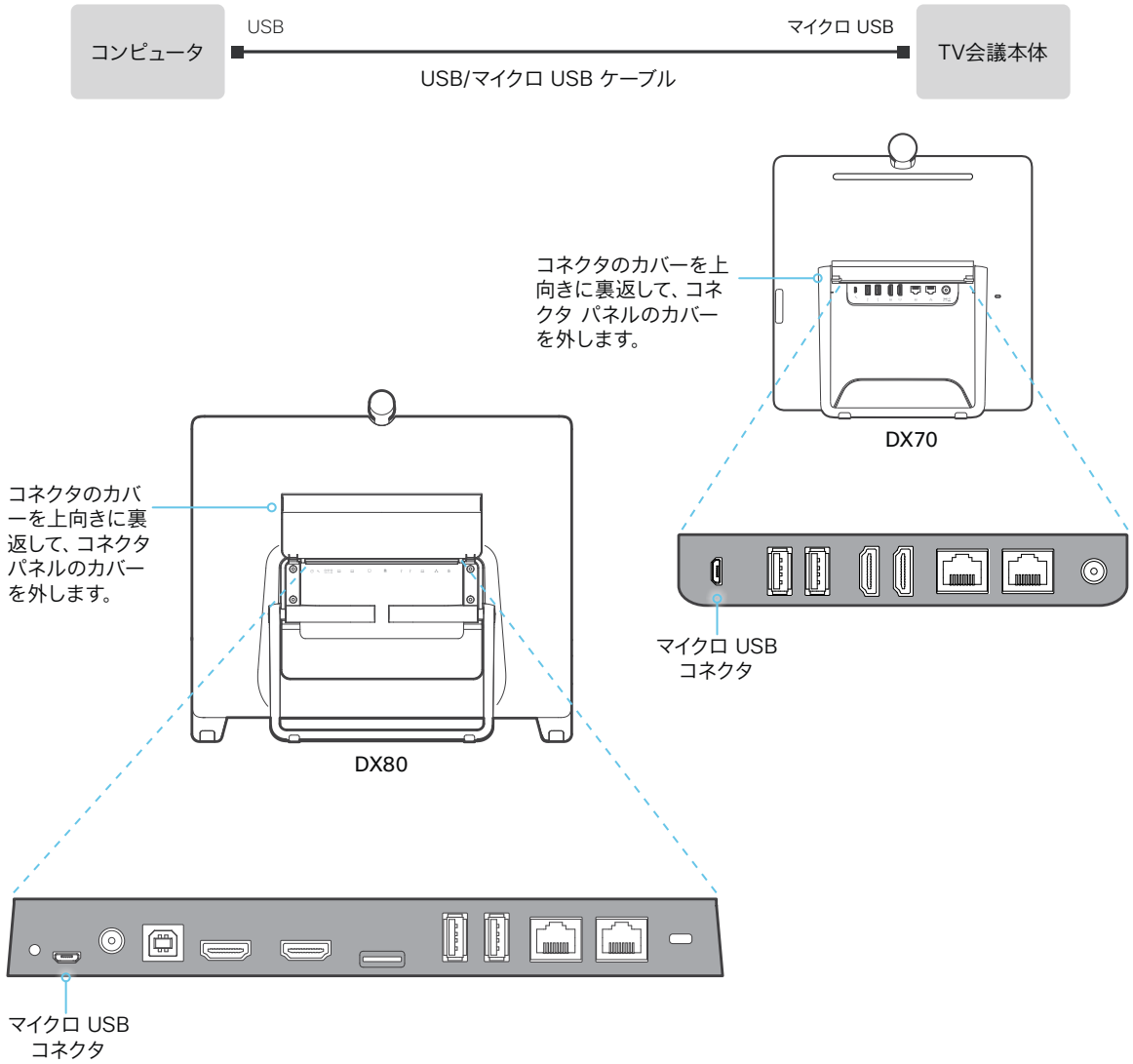
シリアル通信はデフォルトでイネーブルになっています。動作を変更するには、次の設定を使用します。

[シリアルポート（*SerialPort*）] > [モード（*Mode*）]

セキュリティ上の理由から、シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには、次の設定を使用します。

[シリアルポート（*SerialPort*）] > [ログインが必須（*LoginRequired*）]

デバイスが CUCM によってプロビジョニングされている場合、シリアル ポートの設定は CUCM から行う必要があります。



TCP ポートの開放

コーデック内のウェブ サーバでは、非セキュアまたは不必要なポート、プロトコル、モジュール、またはサービスの使用が禁止または制限されています。いくつかのポートは、デフォルトで開放されているか、閉じられています。

TCP 22 : SSH

SSH モード設定を [オフ (Off)] にすることで、ポートを閉じることができます。

```
NetworkServices SSH Mode: Off/On
```

TCP 80 : HTTP

HTTP モードを [オフ (Off)] にするか、[HTTPS (HTTPS)] にすることで、ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

TCP 443 : HTTP

HTTP モード設定を [オフ (Off)] にすることで、ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

TCP 5060/5061 : SIP listen ports

SIP リッスン ポートはデフォルトで開放されています。SIP リッスン ポートは、Cisco UCM (Unified Communication Manager) によって無効にされています。SIP リッスン ポートを [オフ (Off)] にすることで、ポートを閉じることができます。

```
SIP ListenPort: Off/On
```

デバイスの設定は、Web インターフェイスの [セットアップ (*Setup*)] > [設定 (*Configuration*)] ページから行います。Web ブラウザを開き、デバイスの IP アドレスを入力して、サインインします。

TMS からの HTTPFeedback アドレス

デバイスが Cisco TelePresence Management Suite (TMS) に追加されると、TMS に情報 (イベント) を送り返すように自動的に設定されます。デバイスは、TMS からそれらのイベントに送信されるアドレス (HTTPFeedback アドレス) を受けとります。このアドレスが存在しないか、または正しく設定されていない場合、デバイスは TMS にイベントを送信できません。

失われたイベントへの応答

イベントへの応答がデバイスで受信されない場合、デバイスは最大 6 回、間隔を増やしながら HTTPFeedback アドレスに送信を再試行します。

再試行してもデバイスで応答が受信されない場合、エンドポイントは 10 分ごとに HTTPFeedback アドレスにメッセージの送信を試行します。HTTPFeedback ステータスは、失敗したことを示します。障害のタイプを示す診断メッセージがあります。

メッセージの再送を試みる際、TMS での通話詳細記録 (CDR) の紛失が生じます。

TMS からの新しい HTTPFeedback アドレスの取得

イベントを送信するための新しいアドレスを取得するには、デバイスを再起動して、TMS から (スケジュール設定または TMS 管理者によるトリガーで) 次の管理アドレスがプッシュされるのを待つ必要があります。

Cisco Webex Cloud サービスへのデバイスの登録

画面上のセットアップ アシスタントを使用する代わりに、Web インターフェイスからリモートで Cisco Webex にデバイスを登録できます。

デバイスを登録するには、まず、コントロール ハブで、アクティベーション コードを作成する必要があります。アクティベーション コードの作成方法については、► 「場所の作成および Cisco Webex Room デバイスまたは Cisco Webex Board のサービスの追加」をご覧ください。

Web インターフェイスから登録できるのは、現在サービスに登録されていないデバイスのみです。

注 : このデバイス用に作成されたローカル ユーザとカスタマイズは、すべて非アクティブ化されます。

1. Web インターフェイスにサインインし、ホーム画面で [ここをクリックして Webex に登録 (*Click here to register to Webex*)] をクリックします。

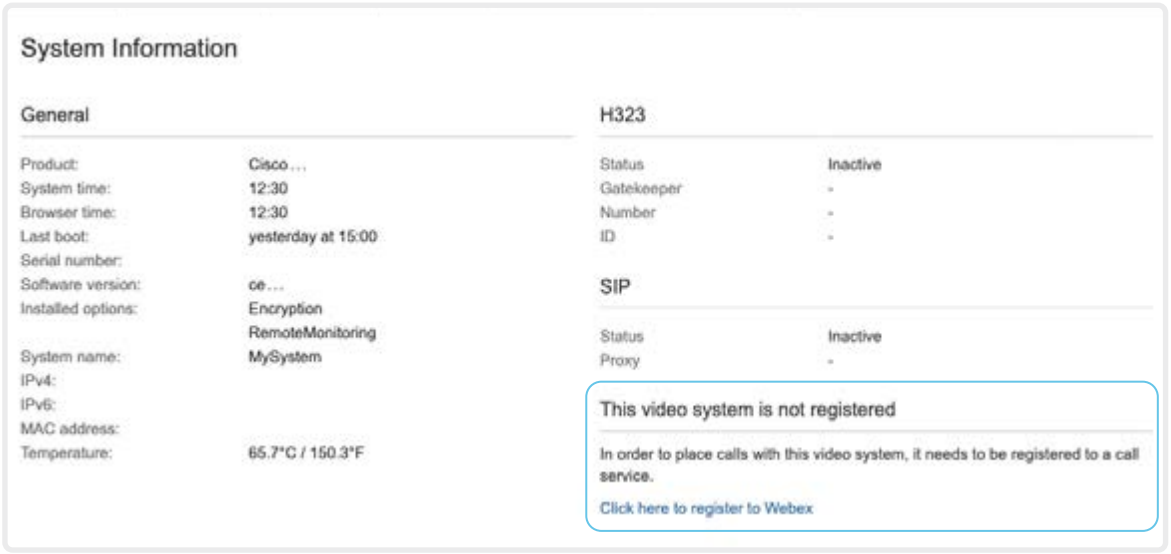
   このリンクは、デバイスがサービスにまだ登録されていない場合にのみ使用できます。

2. ポップアップが表示され、コントロール ハブで作成したアクティベーション コードを入力することができます。

   形式:

   - xxxx-xxxx-xxxx-xxxx、または
   - xxxxxxxxxxxxxxx

3. 登録後に、画面上のセットアップ アシスタントからタイム ゾーンと言語を設定する必要があります。ウィザードがタイム アウトした場合は、デフォルトの設定が適用されます。



制限

利用可能な設定の一部は、オンプレミスの登録済みデバイスにのみ適用されます。これらは、Webex に登録されているデバイスには適用されません。API ガイドの「サポートされているコマンド マトリックス」では、これらの項目は「オンプレミスのみ」とマークされています。

適用されない設定はすべて、H.323、H.320、SIP、NTP、CUCM、LDAP、Proximity、および相手先カメラ制御に関連するものです。

サポートされている RFC

RFC (Request For Comments) シリーズには、Internet Engineering Task Force (IETF) によって作成される技術仕様およびポリシー文書など、インターネットに関する技術および組織のドキュメントが含まれます。

CE ソフトウェアは、以下を含む RFC の範囲をサポートしています。

- RFC 2782『DNS RR for specifying the location of services (DNS SRV)』
- RFC 3261 SIP『Session Initiation Protocol』
- RFC 3263『Locating SIP Servers』
- RFC 3361『DHCP Option for SIP Servers』
- RFC 3550 RTP『RTP: A Transport Protocol for Real-Time Applications』
- RFC 3711『The Secure Real-time Transport Protocol (SRTP)』
- RFC 4091『The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework』
- RFC 4092『Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)』
- RFC 4582『The Binary Floor Control Protocol』
- draft-ietf-bfcpbis-rfc4582bis-00『Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport』
- RFC 4733『RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals』
- RFC 5245『Interactive Connectivity Establishment (ICE)』: A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5589『SIP Call Control Transfer』
- RFC 5766『Traversal Using Relays around NAT (TURN)』: Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905『Network Time Protocol Version 4: Protocol and Algorithms Specification』

技術仕様 (1/2 ページ)

ソフトウェアの互換性

- コラボレーション エンドポイント ソフトウェア バージョン 8.2 以降

製品の同梱物:

- 内蔵の HD カメラとマイクを備えた DX80 システムまたは DX70 システム
- ネットワーク ケーブル
- HDMI/USB ケーブル (DX80 のみ)
- 電源アダプタおよび使用地域向けの電源コード

統合型の HD カメラ

- ディスプレイから -5°～ 70°
- 水平視野角 63°
- 垂直視野角 38°
- 解像度 : 1080p30
- F 2.2
- 顔認識に基づくインスタント フォーカス
- プライバシー シャッター

ユーザ インターフェイス

- 画面上のグラフィカル ユーザ インターフェイス

言語のサポート
(ソフトウェアのバージョンによって異なる)

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

システム管理

- 組み込みの SNMP、Telnet、SSH、XML、および SOAP による総合的管理
- Web サーバ、HTTP、および HTTPS を使用したリモート ソフトウェア アップロード
- 画面上のメニュー システム

ディレクトリ サービス

- ローカル ディレクトリ (お気に入り) のサポート
- 社内ディレクトリ (Cisco Unified Communications Manager リリースおよび Cisco TelePresence Management Suite 利用)
- LDAP および H.350 をサポートするサーバ ディレクトリ (Cisco TelePresence Managment Suite が必要)
- 日時を含む着信、発信、および不在着信のコール履歴

電源

- 定格 : 最大 60 W
- 省電力スタンバイ モード

動作温度および湿度

- 周囲温度 : 0 ～ 40 °C (32 ～ 95°F)
- 相対湿度 (RH) : 10 ～ 90%

保管および輸送の温度

- RH 10 ～ 90% では -20 ～ 60° (-4 ～ 140°F) (結露しないこと)

DX80 システムの寸法

- 幅 : 56.5 cm (22.2 インチ)
- 高さ : 51.2 cm (20.2 インチ)
- 奥行 : 8.9 cm (3.5 インチ)
- 重量 : 7.1 kg (15.65 ポンド)

DX70 システムの寸法

- 幅 : 35.31 cm (13.91 インチ)
- 高さ : 37.71 cm (14.84 インチ)
- 奥行 : 6.23 cm (2.45 インチ)
- 重量 : 3.4 kg (7.5 ポンド)

帯域幅

- 最大 3 Mbps

解像度とフレーム レートの最小帯域幅

- 768 kbps から 720p30
- 1472 kbps から 1080p30

ファイアウォール トラバーサル

- Cisco TelePresence Expressway テクノロジー

ビデオ標準

- H.263
- H.263+
- H.264
- AVC (H.264/MPEG-4 Part 10 Advanced Video Coding)

ビデオ入力

HDMI ビデオ入力 X 1。最大 1920 X 1080@60 fps (HD1080p60) までのフォーマット (以下を含む) をサポートします。

- 640 X 480
- 720 X 480
- 800 X 600
- 1024 X 768
- 1280 X 720
- 1366 X 768
- 1920 X 1080

Extended Display Identification Data (EDID)

ビデオ出力

HDMI 出力 (1 個) * (将来の使用に備えて予約済み) 。以下のフォーマットをサポートします。

- 1920 X 1080@60 fps (1080p60)

VESA モニタ電源管理

Extended Display Identification Data (EDID)

ライブ ビデオ解像度 (エンコード/デコード)

最大 1920 X 1080@30 fps (HD1080p30) までのエンコードまたはデコード ビデオ フォーマット (以下を含む) をサポートします。

- 176 X 144 @ 30 fps (QCIF) (デコードのみ)
- 352 X 288 @ 30 fps (CIF)
- 512 X 288 @ 30 fps (w288p)
- 576 X 448 @ 30 fps (448p)
- 640 X 480 @ 30 fps (VGA)
- 704 X 576 @ 30 fps (4CIF)
- 768 X 448 @ 30 fps (w448p)
- 800 X 600 @ 30 fps (SVGA)
- 1024 X 576 @ 30 fps (w576p)
- 1024 X 768 @ 30 fps (XGA)
- 1280 X 720 @ 30 fps (HD720p)
- 1280 X 768 @ 30 fps (WXGA)
- 1280 × 1024 @ 30 fps (SXGA)
- 1440 × 900 @ 30 fps (WXGA+)
- 1680 x 1050@30 fps (WSXGA+)
- 1920 X 1080 @ 30 fps (HD1080p)

音声標準

- 64 kbps AAC-LD
- OPUS
- G.722
- G.722.1
- G.711mu
- G.711a
- G.729AB

音声機能

- 最大 48 kHz のサンプリング レート
- ハイクオリティ 20 kHz オーディオ
- 音響エコー キャンセラ
- オート ゲイン コントロール
- オートノイズリダクション
- アクティブリップシンク

音声入力

- 内蔵マイク アレイ
- HDMI 音声 1

* HDMI バージョン 1.3

技術仕様 (2/2 ページ)

音声出力
- ライン出力 1 個、ミニジャック (DX70)
- 1 HDMI (デジタル メイン音声)

デュアル ストリーム
- H.239 デュアル ストリーム (H.323)
- BFCP デュアル ストリーム (SIP)
- 15 fps で最大 1920 × 1080 の解像度のサポート

マルチポイント サポート
- シスコ アドホック会議 (Cisco Unified Communications Manager (CUCM) と、Cisco Meeting Server (CMS) または Cisco TelePresence Server および Cisco TelePresence Conductor が必要)

プロトコル
- SIP および H.323

組み込み暗号化
- SIP および H.323 のポイントツーポイント
- 規格準拠 : H.235v3 および Advanced Encryption Standard (AES)
- キーの自動生成と交換
- デュアル ストリームでサポート

IP ネットワーク機能
- DNS ルックアップによるサービス構成
- 差別化サービス (QoS)
- IP 帯域幅最適化コントロール (フロー制御を含む)
- 自動ゲートキーパー検出
- 動的プレイアウトおよびリップシンク バッファリング
- H.245 Dual Tone MultiFrequency (DTMF) トーン (H.323)
- NTP による日時のサポート
- パケット損失時のダウンスピード機能
- URI ダイヤル
- TCP/IP
- DHCP
- IEEE 802.1x ネットワーク認証
- IEEE 802.1Q 仮想 LAN
- IEEE 802.1p QoS およびサービス クラス
- Cisco ClearPath

IPV6 ネットワークのサポート
- H.323 および SIP に対するデュアル スタックの IPv4 および IPv6
- DHCP、SSH、HTTP、HTTPS、DNS、DiffServ に対するデュアル スタックの IPv4 および IPv6
- スタティック IP アドレスの割り当て、ステートレス自動設定および DHCPv6 をサポート

サポートされるインフラストラクチャ
- Cisco Unified Communications Manager 8.6.2 以降
- Cisco TelePresence Video Communication Server (Cisco VCS)

セキュリティ機能
- Web インターフェイス (HTTPS/HTTP) および SSH を使用した管理
- パスワードで保護された IP 管理
- パスワードで保護された管理メニュー
- IP サービスの停止可能
- ネットワーク設定の保護

ネットワーク インターフェイス
- 内部 2 ポートの Cisco イーサネット スイッチ (RJ-45) 10/100/1000BASE-T (自動ネゴシエーションのみ)
- Wi-Fi : IEEE 802.11a/b/g/n、2.4 GHz、5 GHz
- Bluetooth 4.0 LE

その他のインターフェイス
- USB ポート 3 個
- MicroSD カード スロット 1 個 (将来の使用に備えて)
- メンテナンス目的の Micro-USB ポート 1 個

認定および適合規格
- 指令 2014/35/EU (低電圧指令)
- 指令 2014/30/EU (EMC 指令) : クラス A
- 指令 2014/53/EU (無線機器指令)
- 指令 2011/65/EU (RoHS)
- 指令 2002/96/EC (WEEE)
- NRTL 認定 (製品の安全性)
- FCC CFR 47 Part 15B (EMC) : クラス B
- FCC Listed (無線機器)

各国の認定書類については、Product Approval Status Database (製品認定ステータス データベース) www.ciscofax.com を参照してください。

Cisco ウェブ サイト内のユーザ ドキュメンテーション

次の短いリンクを使用して、CE ソフトウェアを実行する製品シリーズのマニュアルを検索します。

Room シリーズ:

▶ https://www.cisco.com/go/room-docs

MX シリーズ:

▶ https://www.cisco.com/go/mx-docs

SX シリーズ:

▶ https://www.cisco.com/go/sx-docs

DX シリーズ:

▶ https://www.cisco.com/go/dx-docs

Board:

▶ https://www.cisco.com/go/board-docs [英語]

通常、すべての Cisco Collaboration エンドポイントのユーザ マニュアルはこちらから検索できます。 ▶ https://www.cisco.com/go/telepresence/docs

マニュアルは以下のカテゴリに整理されています。一部のマニュアルはすべての製品で利用できません。

インストールとアップグレード > インストールとアップグレード ガイド

- インストレーション ガイド: 製品のインストール方法
- スタートアップ ガイド: デバイスを動作させるために必要な初期設定
- RCSI ガイド: 法規制の遵守および安全に関する情報

保守と運用 > メンテナンスとオペレーション ガイド

- スタートアップ ガイド: デバイスを動作させるために必要な初期設定
- 管理者ガイド: 製品の管理に必要な情報
- CUCM での TelePresence エンドポイントの導入ガイド: Cisco Unified Communications Manager (CUCM) と組み合わせてデバイスを使用開始する際に実行するタスク
- スペア部品の概要、スペア部品の交換ガイド、ケーブル スキーマ: スペア部品を交換するときに役立つ情報

保守と運用 > エンドユーザ ガイド

- ユーザ ガイド: 製品の使用方法
- クイック リファレンス ガイド: 製品の使用方法
- 物理インターフェイス ガイド: コネクタのパネルと LED など、コーデックの物理インターフェイスに関する詳細

リファレンス ガイド > コマンド リファレンス

- 『API リファレンス ガイド』: Application Programmer Interface (API) のリファレンス ガイド

リファレンス ガイド > テクニカル リファレンス

- CAD 図面: 測定値付き 2D CAD 図面

設定 > 設定ガイド

- カスタマイズ ガイド: ユーザ インターフェイスのカスタマイズ方法、デバイスの API を使用した室内制御のプログラミング方法、マクロの作成方法、オーディオ コンソールを使用した高度な音声セットアップの設定方法

設計 > 設計ガイド

- ビデオ会議室に関するガイドライン: 会議室の設計とベストプラクティスに関する一般的なガイドライン
- ビデオ会議室のガイドライン: 音質を向上させるための対策

ソフトウェア ダウンロード、リリースと一般情報 > ライセンス情報

- オープン ソースのドキュメンテーション: この製品で使用されるオープン ソース ソフトウェアのライセンスと通知

ソフトウェア ダウンロード、リリースと一般情報 > リリース ノート

- ソフトウェア リリース ノート

Cisco のお問い合わせ先

Cisco のウェブサイトでは、Cisco の世界各地のお問い合わせ先を確認できます。

参照先：► https://www.cisco.com/go/offices

本社
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

知的財産

Cisco 製品のセキュリティの概要

この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。シスコ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みなされます。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、
http://www.bis.doc.gov/policiesandregulations/ear/index.htm で参照できます。