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 9.15
2021 年 4 月

管理者ガイド

Cisco Webex Board 用

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。

ユーザードキュメントは次の場所から入手できます。
▶ https://www.cisco.com/go/board-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

第 1 章

はじめに

ユーザマニュアルおよびソフトウェア

このガイドの対象となる製品

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

ユーザマニュアル

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▶ シスコ Web サイト内のユーザマニュアルを参照してください。

シスコ Web サイト内のドキュメンテーション

次のシスコ Web 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/board-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 Cloud 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

次のシスコ Web 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てください。

▶ 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/ja_jp/support/collaboration-endpoints/spark-board/tsd-products-support-series-home.html

最新情報

この章では、新しいデバイス設定および変更されたデバイス設定（構成）の概要と、CE9.15.3、CE9.15.0、CE9.14、および CE9.13 の新機能と改善点を以前のバージョンと比較して示します。

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/ja_jp/support/collaboration-endpoints/spark-board/tsd-products-support-series-home.html

CE9.15.3 の新機能および改善点15.3

ホワイトボードでのシェイプのサポート *(Desk Pro、DX シリーズ、Board)*

ホワイトボード機能を持つデバイスで、描画を開始する前に [図形 (Shapes)] ボタンをタップすると、図形モードが有効になります。次に、ホワイトボードは正方形、円、三角形、四角形などの基本的な形状を認識し、描画時に輪郭を調整できます。

コール中の Web アプリの共有

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

Web エンジンをサポートするデバイスで、コール中に Web ビューを共有できるようになりました。プレゼンターは、対話をサポートするデバイスで、コール中に共有 Web ビューを操作することができます。

共有する前にコール中に Web ビューをプレビューすることはできません。

DX シリーズデバイスでのノイズ除去 *(DX シリーズ)*

Cisco Webex DX70 および DX80 デバイスで、ノイズ除去機能をサポートするようになりました。会議中にこの機能をオンにすると、背景雑音が除去され、音声が鮮明に聞こえます。

会議中の挙手

(DX シリーズ、SX シリーズ、MX シリーズ、Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Desk Pro、Board)

3 人以上での会議中に、デバイス画面の新しい [挙手（Raise Hand)] ボタンをタップして、会議主催者と共同主催者に、自分が実際に手を挙げたことを通知できます。同じボタンをタップすると通知が削除されます。

この機能には、CMS 3.2 以降が必要です。

Webex Edge for Devices - ソフトウェアアップグレードの要件 *(すべての製品)*

Webex Edge for Devices では、Webex の接続を維持するために最新のソフトウェアが必要です。2021 年 3 月以降、Cisco Webex は新しい認証局 IdenTrust Commercial Root CA 1 に移行します。この変更により、デバイスソフトウェアのアップグレードを手動で管理しているお客様は、デバイスが Webex Edge for Devices でサポートされるように、できるだけ早くデバイスを CE9.14.5 以降 (CE9.15 を推奨) にアップグレードする必要があります。

会議室内での予約 *(すべての製品)*

ルームデバイスが Webex Edge for Devices でクラウドにリンクされ、カレンダーサービスを使用している場合は、会議室内での予約機能を使用して現在の会議を延長したり、自発的な会議のために部屋を予約したりすることができるようになりました。

タッチコントローラ、Touch 10 または Room Navigator を使用して、利用可能な部屋を予約できます。Webex Assistant が有効になっている場合、ボイスコマンドを使用して部屋を予約できます。

キーボードレイアウトの拡張言語サポート

(すべての製品)

デバイスが Webex Edge for Devices でクラウドにリンクされている場合は、最大 26 の異なるキーボード言語から選択できるようになりました。ローカライズされた言語の選択は、タッチキーボードおよび TRC-6 リモート制御でサポートされています。

CE9.15.0 の新機能および改善点

コール中の高度な Wi-Fi の詳細を確認する

(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board、DX シリーズ)

Wi-Fi 接続をサポートしているすべてのデバイスで、Wi-Fi 設定にアクセスして、コール中でもネットワークのステータスに関する詳細情報を表示できるようになりました。

Web インターフェイスの更新 *(すべての製品)*

Web インターフェイスが再構成されました。タブ付き垂直メニューが導入され、移動した設定を検索するための検索ボックスがあります。

Web インターフェイスから Room Panorama ディスプレイをアップグレードする *(Room Panorama、Room Panorama 70)*

デバイスの Web インターフェイスから直接、Cisco Webex Room Panorama および Room Panorama 70 の Samsung ディスプレイのファームウェアをアップグレードできます。ディスプレイファームウェアは、cisco.com から入手できます。手順はデバイスの Web インターフェイスの [アップグレードの表示（Display Upgrade）] ページを参照してください。

ログのダウンロードから個人情報を削除する

(すべての製品)

Web インターフェイスからログをダウンロードする際、個人を特定できる情報 (PII) を削除できるようになりました。機密情報は、ダウンロードしたログで「プライバシー保護のために削除されました」というメモに置き換えられます。

サポートケースに匿名化されたログを添付すると、問題の解決に必要な時間が長くなる場合があります。

UI 拡張用のカスタムアイコンをアップロードする

(SX10 を除くすべての製品)

Web インターフェイスのユーザインターフェイス拡張エディタから、パネルまたはアクションボタンのカスタムアイコンをアップロードできるようになりました。

背景雑音の除去

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

新しいノイズ除去機能を使用して、会議中に煩雑なノイズを排除することができます。コール中かどうかにかかわらず、この機能を有効にできます。

ロックされた CMS 会議へのゲストの参加を許可する

(すべての製品)

主催者は、ロックされた CMS 会議へのゲストの参加を許可することができます。

この機能は CE9.15.0.11 でサポートされますが、CMS 3.2 がリリースされるまで利用できません。

浮動ツールバー *(Webex Board、Desk Pro、DX シリーズ)*

タッチスクリーンデバイスで新しい浮動ツールバーを使用できます。共有オプション、注釈、およびタッチリダイレクトにすばやくアクセスできます。ツールバーには、現在のシナリオに該当する異なるオプションが表示されます。また、このツールバーはドッキング可能です。

ホワイトボード上のブラックキャンバス

(Webex Board、Desk Pro、DX シリーズ)

ホワイトボードを使用している場合は、黒白のキャンバスを変更することができます。ホワイトボードを次回開くときのために、設定がデバイスに保存されます。

ホワイトボードの概要 *(Webex Board、Desk Pro、DX シリーズ)*

ホワイトボード全体の概要がより適切に表示されるように、最大 10 倍までズームアウトすることができます。

ブロードキャストモード *(すべての製品)*

クリーンなビデオストリームを出力するようにデバイスを設定できます。このモードでは、インジケータ、通知、およびコントロールが削除されます。ただし、参加者の名前ラベルとミュートインジケータは引き続き表示されます。このモードは、視聴者にビデオを配信したいだけのブロードキャストおよび録音サービスを目的としています。

CUCM コール管理レコード *(すべての製品)*

デフォルトで有効になっている新しい CallDiagnostics 設定では、Cisco Webex Devices がコール統計を CUCM に送信し、コール統計は CUCM のコール管理レコードに追加されます。

Cisco Webex Edge for Devices の更新

（すべての製品）

Cisco Webex Edge for Devices にリンクされたデバイスの拡張機能:

- クラウド管理のソフトウェアアップグレード。有効にすると、Webex Edge for Devices にリンクされたデバイスは、最新の RoomOS ソフトウェアバージョンに自動的にアップグレードされます。

  2021 年 1 月以降、DX、MX、および SX シリーズデバイスは RoomOS 9.15 以降をサポートします。Webex Board、Desk および Room シリーズのデバイスは、RoomOS 10.0 以降をサポートします。
- ネイティブ Webex Meetings エクスペリエンス特定の要件を満たすと、オンプレミスの登録済みデバイスが Webex Meetings に参加すると、クラウドに登録されたデバイスと同じ会議のエクスペリエンスが得られます。
- 参加者リストの一番上に主催者が表示されます。自分が主催していない Webex ミーティングでは、主催者が参加者リストの一番上の自分の名前の下に表示されます。

CE9.14 の新機能および改善点

Web インターフェイスの視覚的更新

（すべての製品）

Web インターフェイスの外観が強化されました。ボタンとテキスト入力フィールドに適用される新しいスタイルにより、同じ機能を維持しながら、小規模/モバイルデバイスの全体的なサポートが向上しています。

通知はページの右下隅に表示されるようになりました。

CMS コールで重要な参加者をピン留めする

（すべての製品）

CMS ミーティングでは、主催者が参加者をピン留めできます。参加者は通話中のスピーカーでなくても、常に他のすべての参加者に表示されます。

音楽モード *（すべての製品）*

音楽モード機能をアクティブにすると、デバイスのエコーキャンセレーションと背景雑音除去の機能を維持しながら、マイクを使用して音楽のパフォーマンスをキャプチャできます。音楽モードは、リモートでの音楽のレッスン、楽器のテスト、および音楽が重要なその他の状況で役立ちます。

音楽モードは、コールが終了すると自動的にオフになります。次回のコールは音声用に最適化されます。

マウスとキーボードのリダイレクト *(Desk Pro)*

Desk Pro USB-C ドッキングステーションの機能が拡張され、USB 転送のサポートが追加されました。つまり、USB キーボードまたはマウスを Desk Pro に接続し、ラップトップで使用することができます。

手動カメラ制御 *(Desk Pro、Board)*

この新機能を使用すると、Desk Pro および Board で、ズームや自動フレーミング機能の無効化など、カメラの位置を手動で調整できます。

タッチボタンの変更

(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、SX80、SX20、SX10、MX700、MX800、MX200 G2、MX300 G2、DX80、DX70)

コール外のシナリオでは、タッチインターフェイスに表示されるボタンがページ上にグループ化されるようになりました。[詳細 (More)]ボタンの代わりに、画面下部の小さな点によって、ボタンのページが追加されていることを示します。左または右にスワイプすると、ページが変更されます。

コール中は、[詳細 (More)] ボタンが表示され、タップすると残りのボタンがスクロール可能なリストに表示されます。

設定可能な Web データとホワイトボードのクリーンアップ

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

設定可能なクリーンアップ機能をオンにした場合、デバイスはデフォルトで毎日午前 0 時に Web データとホワイトボードデータをクリーンアップします。クリーンアップ用に設定された時刻はユーザー定義可能で、変更できます。この機能をオフにすると、クリーンアップは手動の手順に制限されます。

ホワイトボード機能は、Desk Pro および Board でのみ使用できます。

改善された Wi-Fi 設定のユーザインターフェイス

(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、 Room Panorama、Room 70 Panorama、Desk Pro、Board、DX80、DX70)

Wi-Fi 接続をサポートしているすべてのデバイスで、設定を簡単にするために Wi-Fi セットアップインターフェイスが改善されました。

[通話履歴 (Recents)] リストでのコール詳細

（すべての製品）

最近のコール（パケット損失やジッターなど）で収集されたデータが、より簡単に取得できるようになりました。この情報には、[コール (Call)] ボタンをタップし、[通話履歴 (Recents)] を選択することで、デバイスのタッチインターフェイスから直接アクセスできます。

Cisco Webex Edge for Devices の更新

（すべての製品）

Cisco Webex Edge for Devices にリンクされたデバイスの拡張機能:

- デバイスは、Cloud Video Interop (CVI) ゲートウェイ経由で SIP を使用するか、または Microsoft Teams 会議 Web アプリ (WebRTC) を実行することで、Microsoft Teams 会議に参加できます。
- 有効にした場合、デバイスはログをクラウドにアップロードできます。
- クラウドデバイス API が複数回線コマンドをサポートするようになりました。

SpeakerTrack 表示の制限

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

表示の制限機能を使用すると、部屋の一部をビューから除外できます。これにより、スピーカートラッキングで使用される最大のカメラビュー（部屋のオーバービュー）が制限されます。この機能は、手動カメラ制御で使用できるビューには影響しません。

CE9.13 の新機能および改善点

新商品

- Cisco Webex Room Panorama
- Cisco Webex Room 70 Panorama

Cisco Webex Control Hub の設定管理のサポート *(すべての製品)*

Cisco Webex Control Hub が拡張され、Webex Edge for Devices にリンクされたオンプレミス登録デバイスをより詳細に制御できるようになりました。新しい設定管理機能により、多くのデバイス設定への書き込みアクセスが許可されます。この機能はデフォルトで無効になっています。これは Control Hub で有効にすることができます。

Webex パーソナルミーティングルームに簡単に参加

(すべての製品)

Webex Edge for Devices にリンクされたデバイスから、Webex組織のユーザを直接検索できるようになりました。検索結果のユーザ名の横には、パーソナルミーティングルーム（PMR）に参加するボタンが表示されます。

Webex ミーティングへの参加時のリアルタイムメディアメトリック *(すべての製品)*

Webex Edge for Devices にリンクされたデバイスは、Webex登録済みデバイスと同じように、Control Hub のメディアトラブルシューティングセクションに表示されます。これにより、メディア品質の問題のトラブルシューティングが容易になります。

コール中のタッチ転送 *(Board)*

コール中にタッチ転送を使用でき、フローティングツールバーを使用してアクティブ化と非アクティブ化を切り替えることができます。

バーチャル背景のサポート *(Desk Pro)*

独自のバーチャル背景をアップロードできます。イメージは Web インターフェイス経由でアップロードします。その後、GUI でいずれかのイメージを選択できます。

コンピュータなどの入力デバイスのコンテンツをバーチャル壁紙として使用することもできます。

CMS ミーティングへのダイヤルイン時の遠端カメラ制御 *(すべての製品)*

CMS ミーティングへのダイヤルイン時に、アクティブなスピーカーのカメラを制御できます。参加者リストを開くと、カメラを制御するための [リモートカメラ (Remote Camera)] ボタンが表示されます。

注 : 参加者間でアクティブなスピーカーが頻繁に変わる場合は、目的の参加者のカメラを制御することが難しくなる可能性があります。FECC に特定の参加者を手動で選択することはできません。現在アクティブなスピーカーが常に対象となります。

ビデオストリームへのカスタムテキスト

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

時刻や日付、カスタムテキスト文字列をビデオストリームに追加できます（xCommand Video Graphics Text Display）。このテキストは、メインビデオストリーム、プレゼンテーションストリーム、またはローカルビデオ出力に追加できます。

CE9.15.3 での設定の変更点

新しい設定

オーディオ マイク ノイズ除去 モード *(Board、Codec Plus、Codec Pro、Desk Pro、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini、Room Panorama、Room 70 Panorama)*

システムユニット カスタムデバイス ID *(すべての製品)*

ユーザインタラクション 挙手 CMS *(すべての製品)*

ユーザインタラクション Qt 仮想キーボード *(すべての製品)*

削除された設定

予約 プロトコルの優先順位 *(DX70、DX80、MX200 G2、MX300 G2、MX700、MX800、SX10、SX20、SX80)*

変更された設定

なし

CE9.15.0 での設定の変更点

新しい設定

オーディオ 入力 マイク [n] ミュート上書き *(Codec Pro、MX700、MX800、Room 70 G2、Room Panorama、Room 70 Panorama、SX80)*

オーディオ 入力 マイク [n] ファントム電源 *(DX80)*

オーディオ USB モード *(DX70、DX80、Desk Pro、Room 55、Room Kit、Room Kit Mini)*

BYOD HID 転送 有効 *(Desk Pro)*

カメラ 背景 ユーザ画像 許可 *(Desk Pro)*

カメラ カメラの明るさ デフォルトレベル *(Desk Pro、Room 55、Room Kit、Room Kit Mini)*

カメラ カメラの明るさ モード *(Desk Pro、Room 55、Room Kit、Room Kit Mini)*

カメラ カメラ [n] 明るさ アルゴリズム *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、SX80)*

カメラ カメラ 露出補正 レベル *(Desk Pro)*

カメラ カメラ [1] 露出補正 レベルから名前変更

ネットワーク [1] IPv6 インターフェイス ID *(すべての製品)*

ネットワークサービス Wifi A_MPDU *(Board、Codec Plus、Codec Pro、Desk Pro、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini、Room Panorama、Room 70 Panorama)*

ルームスケジューラ 有効 *(すべての製品)*

ユーザインターフェイス OSD モード *(すべての製品)*

ユーザインターフェイス ホワイトボード デフォルトテーマ *(Board、Codec Plus、Codec Pro、DX70、DX80、Desk Pro、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini、Room Panorama、Room 70 Panorama)*

ビデオ デフォルトレイアウトファミリ ローカルコンテンツ *(すべての製品)*

Web エンジン 機能 SIP URI ハンドラ *(Board、Desk Pro、Room Kit Mini)*

Web エンジン最小 TLS バージョン *(Board、Codec Plus、Codec Pro、Desk Pro、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini、Room Panorama、Room 70 Panorama)*

Webex クラウドプロキシミティ ゲスト共有 *(すべての製品)*

Webex クラウド アップグレード モード *(すべての製品)*

Webex Meetings 参加プロトコル *(すべての製品)*

削除された設定

カメラ カメラ [1] 露出補正 レベル *(Desk Pro)*

カメラ カメラ 露出補正 レベルに名前変更

ビデオ レイアウトを記憶 *(すべての製品)*

変更された設定

プロビジョニング CUCM コール管理レコード コール診断 *(すべての製品)*

旧： デフォルト：無効
新： デフォルト：有効

ビデオ デフォルトレイアウトファミリ ローカル *(Codec Plus、Codec Pro、DX70、DX80、MX200 G2、MX300 G2、MX700、MX800、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini、Room Panorama、Room 70 Panorama、SX10、SX20、SX80)*

旧： Auto/Equal/Overlay/Prominent/Single
新： Auto/Equal/Overlay/Prominent/Prominent_L/Single

ビデオ デフォルトレイアウトファミリ ローカル *(Board)*

旧： Auto/Equal/Overlay/Prominent/Single
新： Auto/Equal/Overlay/Prominent/Prominent_L/Single

ビデオ デフォルトレイアウトファミリ ローカル *(Desk Pro)*

旧： Auto/Equal/Modal/Overlay/Prominent/Single
新： Auto/Equal/Overlay/Prominent/Prominent_L/Single

ビデオ デフォルトレイアウトファミリ リモート *(Codec Plus、Codec Pro、MX200 G2、MX300 G2、MX700、MX800、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini、Room Panorama、Room 70 Panorama、SX20、SX80)*

旧： Auto/Equal/Overlay/Prominent/Single
新： Auto/Equal/Overlay/Prominent/Prominent_L/Single

ビデオ デフォルトレイアウトファミリ リモート *(Board)*

旧： Auto/Equal/Overlay/Prominent/Single
新： Auto/Equal/Overlay/Prominent/Prominent_L/Single

ビデオ セルフビュー デフォルト PIP ポジション *(Board)*

旧： デフォルト：LowerRight
新： デフォルト：Current

CE9.14 での設定の変更点

新しい設定

Bluetooth 許可 *(Desk Pro)*

Bluetooth 有効 *(Desk Pro)*

予約 プロトコルの優先順位 *(すべての製品)*

カメラ カメラ [1] 露出補正 レベル *(Desk Pro)*

プロビジョニング CUCM コール管理レコード コール診断 *(すべての製品)*

プロビジョニング CUCM コール管理レコードから名前変更

ルーム分析 環境雑音の予測 間隔 *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board)*

ルームクリーンアップ 自動実行 コンテンツタイプ Web データ *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board)*

ルームクリーンアップ 自動実行 コンテンツタイプ ホワイトボード *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board、DX80、DX70)*

ルームクリーンアップ 自動実行 時間 *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、 Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board、DX80、DX70)*

スタンバイ ブートアクション *(Board)*

スタンバイ ウェイクアップアクション *(Board)*

ユーザインターフェイス 機能 コール 音楽モード *(すべての製品)*

ビデオ デフォルトレイアウトファミリ ローカル *(Board)*

ビデオ レイアウトを記憶 *(すべての製品)*

Webex クラウドプロキシミティ モード *(すべての製品)*

WebRTC コール終了タイムアウト *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board)*

WebRTC 対話モード *(Room Kit Mini、Desk Pro、Board)*

削除された設定

プロビジョニング CUCM コール管理レコード *(すべての製品)*

プロビジョニング CUCM コール管理レコード コール診断に名前変更

変更された設定

オーディオ 出力 ライン [1] 出力タイプ *(Codec Plus、Room Kit、Room 55、Room 55 Dual、Room 70)*

値スペースに追加： Microphone

Bluetooth 可 *(DX70、DX80)*

旧： アクセス : public-api-preview

新： アクセス : public-api

Bluetooth 有効 *(DX70、DX80)*

旧： アクセス : public-api-preview

新： アクセス : public-api

カメラ プレゼンタートラッキング コネクタ *(Codec Pro、Room 70 G2、Room Panorama、Room 70 Panorama)*

旧： 6

新： 1

ロギング クラウドアップロード モード *(すべての製品)*

旧： バックエンド : All

新： バックエンド : On-prem

周辺機器 プロファイル ネットワークスイッチ *(Room 70 Panorama)*

旧： デフォルト : 1

新： デフォルト : NotSet

スタンバイ ブートアクション *(Desk Pro)*

旧： デフォルト : DefaultCameraPosition

新： デフォルト : RestoreCameraPosition

タイムゾーン *（すべての製品）*

Valuespace に追加： America/Nuuk、America/Punta_Arenas、Antarctica/Casey、Antarctica/Davis、Antarctica/DumontDUrville、Antarctica/Macquarie、Antarctica/Mawson、Antarctica/McMurdo、Antarctica/Palmer、Antarctica/Rothera、Antarctica/South_Pole、Antarctica/Syowa、Antarctica/Troll、Antarctica/Vostok、Arctic/Longyearbyen、Asia/Atyrau、Asia/Barnaul、Asia/Famagusta、Asia/Qostanay、Asia/Tomsk、Asia/Yangon、Brazil/Acre、Brazil/DeNoronha、Brazil/East、Brazil/West、CET、CST6CDT、Canada/Atlantic、Canada/Central、Canada/Eastern、Canada/Mountain、Canada/Newfoundland、Canada/Pacific、Canada/Saskatchewan、Canada/Yukon、Chile/Continental、Chile/EasterIsland、Cuba、EET、EST、EST5EDT、Egypt、Eire、Europe/Astrakhan、Europe/Kirov、Europe/Saratov、Europe/Ulyanovsk、GB、GB-Eire、GMT、GMT+0、GMT-0、GMT0、Greenwich、HST、Hongkong、Iceland、Iran、Israel、Jamaica、Japan、Kwajalein、Libya、MET、MST、MST7MDT、Mexico/BajaNorte、Mexico/BajaSur、Mexico/General、NZ、NZ-CHAT、Navajo、PRC、PST8PDT、Poland、Portugal、ROC、ROK、Singapore、Turkey、UCT、US/Alaska、US/Aleutian、US/Arizona、US/Central、US/East-Indiana、US/Eastern、US/Hawaii、US/Indiana-Starke、US/Michigan、US/Mountain、US/Pacific、US/Samoa、UTC、Universal、W-SU、WET、Zulu

ユーザインターフェイス アシスタント 会議参加確認 *(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro、Board)*

旧： デフォルト：False

新： デフォルト：True

ビデオ デフォルトレイアウトファミリ ローカル *(Room Panorama、Room 70 Panorama)*

旧： Auto/Equal/Overlay/Panorama/Prominent/Single

新： Auto/Equal/Overlay/Prominent/Single

ビデオ デフォルトレイアウトファミリ リモート *(Room Panorama、Room 70 Panorama)*

旧： Auto/Equal/Overlay/Panorama/Prominent/Single

新： Auto/Equal/Overlay/Prominent/Single

ビデオ デフォルトレイアウトファミリ リモート *(Desk Pro)*

旧： Auto/Equal/Modal/Overlay/Prominent/Single

新： Auto/Equal/Overlay/Prominent/Single

CE9.13 での設定の変更点

新しい設定

オーディオ マイク AGC *(Codec Plus、Room Kit、SX20)*

ロギング クラウドアップロード モード *(すべての製品)*

削除された設定

ユーザインターフェイス ホワイトボード アクティビティインジケータ *(MX200 G2、MX300 G2、MX700、MX800、SX10、SX20、SX80)*

ユーザインターフェイス RoomKitTouch 有効 *(Board、Room 70 G2、Room Kit Mini、Room Kit、Desk Pro、Room 55、Codec Plus、Room 55 Dual、Room 70、Codec Pro)*

変更された設定

オーディオ 出力 内蔵スピーカー モード *(Codec Plus、MX700/MX800、MX200 G2、MX300 G2、Room Kit、Room 55、Room 55 Dual、Room 70、Room 70 G2)*

旧：ADMIN

新：ADMIN、INTEGRATOR

カメラ 電源 周波数 *(Codec Plus、Codec Pro、Desk Pro、MX200 G2、MX300 G2、MX700、MX800、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、SX20、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック カメラの位置 パン *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック カメラの位置 チルト *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック カメラの位置 ズーム *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック コネクタ *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック 有効 *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック プレゼンター検出ステータス *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

カメラ プレゼンタートラック トリガーゾーン *(Codec Plus、Codec Pro、MX700、MX800、Room 55 Dual、Room 70、Room 70 G2、SX80)*

旧：アクセス：public-api-preview

新：アクセス：public-api

会議 アクティブコントロール モード *(すべての製品)*

旧：アクセス：public-api-preview

新：アクセス：public-web-only

会議 暗号化 モード *(すべての製品)*

旧：バックエンド：Any

新：バックエンド：On-prem

プロビジョニング CUCM コール管理レコード *(すべての製品)*

旧：アクセス：public-api-preview

新：アクセス：public-api

旧：デフォルト値：オン

新：デフォルト値：オフ

ユーザインターフェイス アシスタント モード *(Board、Codec Plus、Codec Pro、Desk Pro、Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2)*

旧：アクセス：public-api-preview

新：アクセス：public-api

ビデオ 入力 コネクタ [n] 最適鮮明度 60fps のしきい値 *(Room Kit、Room 55)*

旧：デフォルト：1920_1080

新：デフォルト：なし

Webex Board の概要 (1/2 ページ)

Webex Board には、4K カメラ、静電容量方式タッチインターフェイス、高解像度 4K 画面に統合されたマイクおよびスピーカーが搭載されています。Webex Board は強力なオーディオおよびビデオ会議デバイスですが、ワイヤレスプレゼンテーション画面やデジタルホワイトボードとして使用することもできます。Webex Board を導入すると、物理的な会議室でのチームの共同作業に役立つだけでなく、仮想的な会議スペースに安全に接続してワークフローを簡単に継続できます。

Webex Board には、次の 3 つの画面サイズがあります。

- **Webex Board 55 および 55S** (55" LED 画面を搭載)。最大 5 人による小さなスペースでの協議向けに設計されています。
- **Webex Board 70 および 70S** (70" LED 画面を搭載)。最大 8 人を収容する大小の会議室向けに設計されています。
- **Webex Board 85S** (85" LED 画面を搭載)。講堂、トレーニングスペース、教室など、大規模なコラボレーションスペース向けに設計されています。

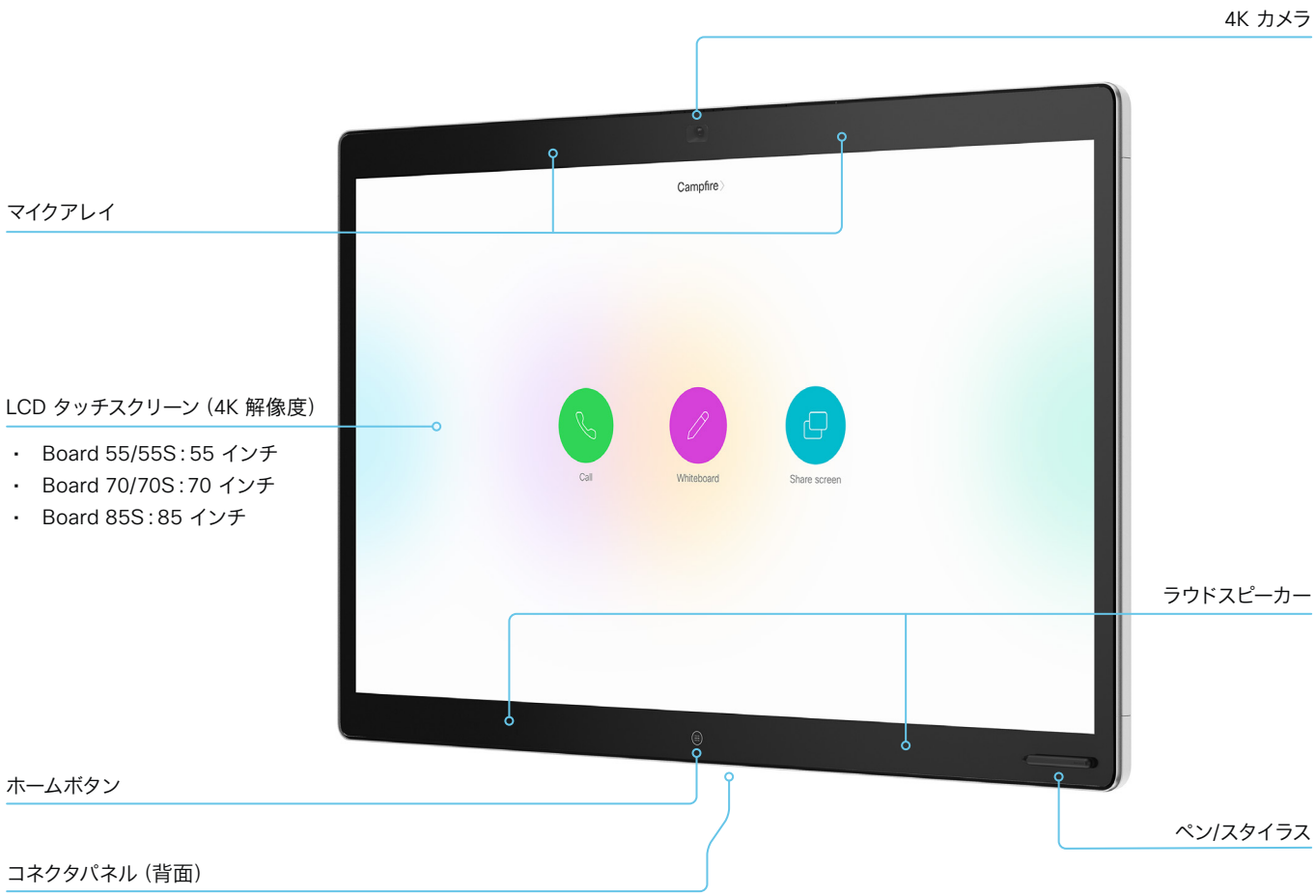
第 2 世代の Webex Board は S シリーズと呼ばれ、ハードウェアプラットフォームにマイナーな最適化が施されています。

Cisco Webex Board の詳細については、► https://www.cisco.com/go/webexboard を参照してください。

機能と利点

- **共有が簡単**：有線またはワイヤレスでのコンテンツ共有。
- **デジタルホワイトボード**：ホワイトボードを自動的に Webex スペースに保存したり、電子メールで送信したりできるホワイトボード機能。画面共有での注釈付けも可能。
- **オーディオ**：インテリジェントな音声トラッキング機能を備えた内蔵マイク。音声に最適化された内蔵スピーカーで高音質のオーディオ会議を提供。
- **ベストオーバービュー**：固定レンズカメラで仮想的にルーム全体をキャプチャ。
- **スピーカートラッキング**：発言中の話者を検出して切り替え、最適にフレーミング。
- **高解像度**：強力な 4K カメラで高解像度イメージをキャプチャ。
- **継続的なワークフロー**：Webex アプリによって別の場所から作業を継続可能。別の Webex Board などのデバイスにも対応。
- **直感的なナビゲーション**：タッチ機能、ワンボタン (OBTP) で簡単に会議に参加。
- **セキュリティ**：エンドツーエンドのセキュリティ。
- **柔軟な登録**：オンプレミス登録にも Cisco Webex 経由でのクラウド登録にも対応。ハードウェアはクラウドプラットフォームでの動作に最適化され、共有のルームやスペースで優れたエクスペリエンスを実現。会議のホストも簡単。

Webex Board の概要 (2/2 ページ)



取り付けオプション

フロアスタンド

壁面スタンド

壁面取り付け

電源のオンとオフ

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

- タッチコントローラの画面またはボードをタップします。

ハーフウェイクモードの開始と次のユーザーに備えたクリーンアップ

- ボードの [ホーム (Home)] ボタンを数秒間押し続けます。

ハーフウェイクモードの終了

- [ホーム (Home)] ボタン、タッチコントローラの画面、またはボード自体をタップします。

リモートからのデバイスの電源オフまたは再起動

Web 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びオンにすることはできません。

デバイスの電源を入れるには、電源プラグを抜いて再度差し込む必要があります。

ビデオ会議デバイスの管理方法 (1/5 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
- 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 に **Value** を設定 (Web) することは次と同等です。
xConfiguration X Y Z: 値 (API)

X > Y > Z ステータス (Web) 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] と設定することは、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

Web 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 (Enabled)]* ・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 (Network Services)] > [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 (Network Services)] > [HTTP] > [モード (Mode)]* *[ネットワークサービス (Network Services)] > [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。
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 (Network Services)] > [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)] > [ログインが必要 (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。

* *[シリアルポート (SerialPort)] > [ログインが必要 (LoginRequired)]* 設定は、Board 55S、70S、および 85S でのみ使用可能です。Board 55 および 70 では常にサインインが必要です。

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 (2/5 ページ)

デバイスの Web インターフェイス

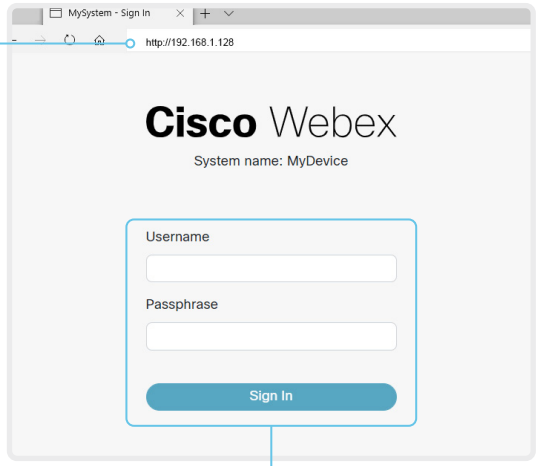
Web インターフェイスは、デバイスの管理ポータルです。コンピュータから接続して、デバイスをリモートで管理できます。フル設定アクセスが提供され、メンテナンス用のツールやメカニズムを利用できます。

注：Web 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）。

Web 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

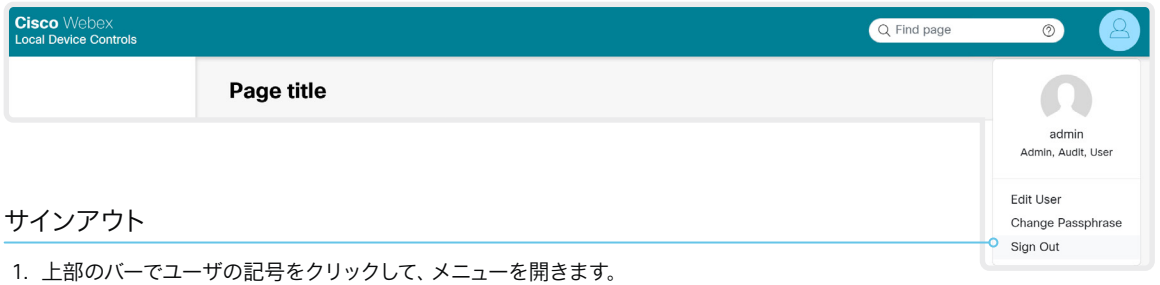
1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. *[このデバイスについて (About this device)]* に続き、*[設定 (Settings)]* を選択します。

サインイン

デバイス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

1. 上部のバーでユーザの記号をクリックして、メニューを開きます。
2. *[サインアウト (Sign Out)]* をクリックします。

* Internet Explorer はサポートされていません。

ビデオ会議デバイスの管理方法 (3/5 ページ)

Web インターフェイスの構成

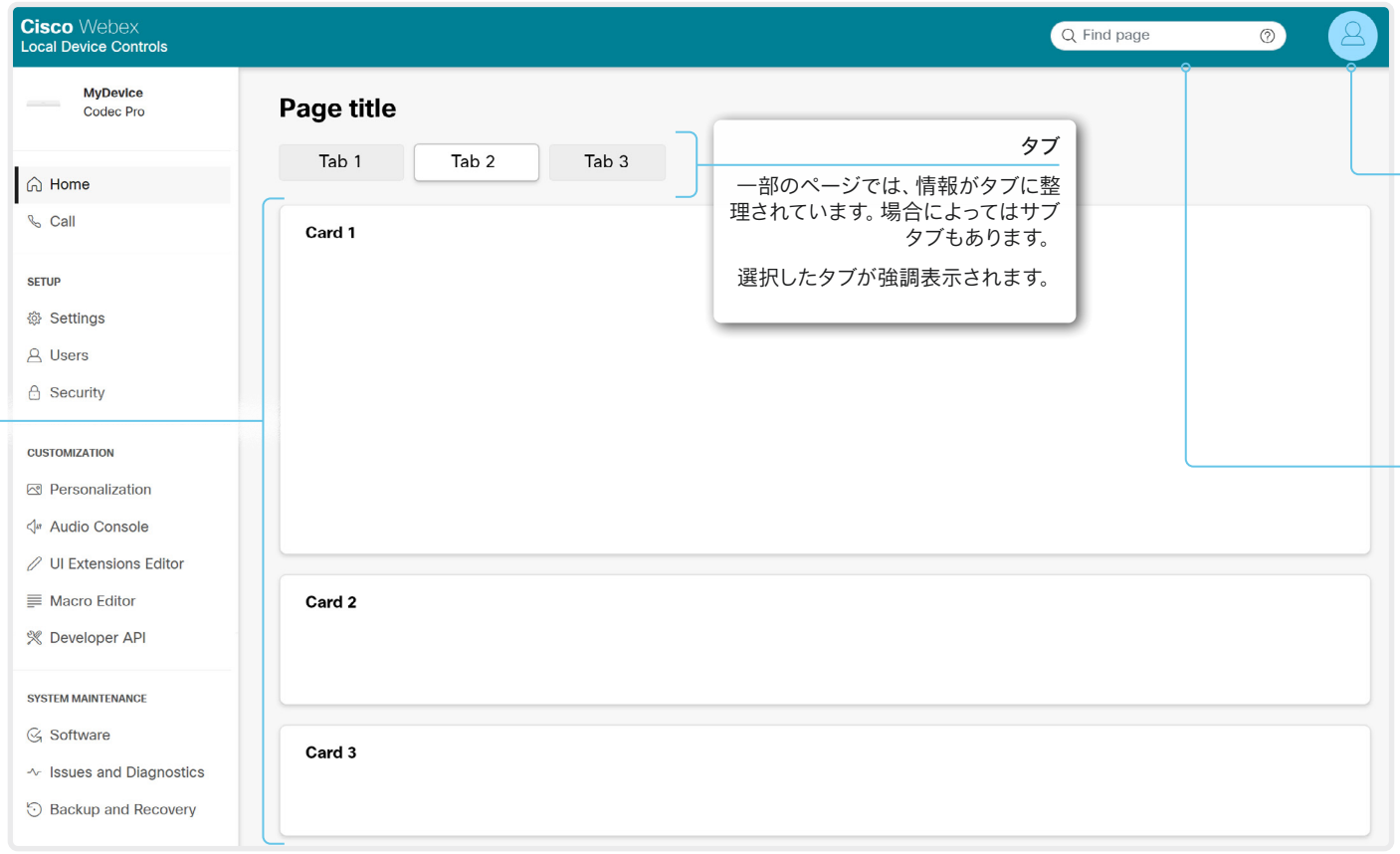
左側のメニューからページまたはトピックを選択します。検索するページを検索するための検索フィールドが上部のバーにあります。

存在するページは、次の条件に依存します。

- デバイスの種類とサービスの登録 (Webex、Cisco UCM、VCS、Webex Edge for Devices)
- 接続された周辺機器と設定
- サインインしているユーザのロールとアクセス権

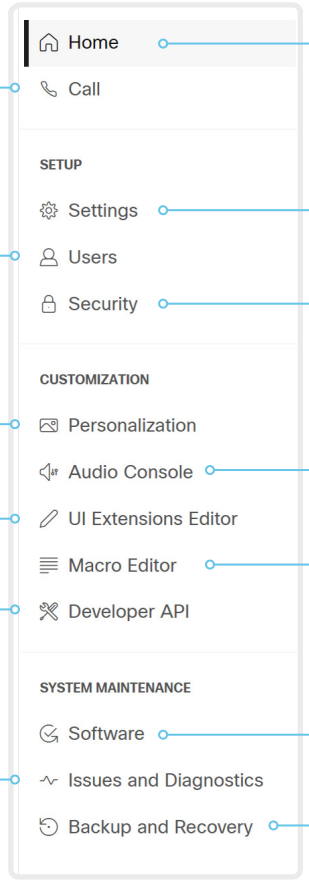
つまり、下の図に示すメニュー項目の一部がデバイスに存在しない可能性があります。

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。



ビデオ会議デバイスの管理方法 (4/5 ページ)

Web インターフェイスのメインメニュー



Home: IP アドレス、MAC アドレス、シリアル番号、アクティブネットワークインターフェイス、ソフトウェアバージョン、問題、登録ステータスなどの一般情報を一覧表示します。

Call: ページを開き、デバイスからコールを設定できます。カメラの位置を変更したり、マイクをミュートしたり、音量を調整したり、レイアウトを変更したり、コールの詳細を確認することができます。

Settings: すべてのデバイスの設定と状態にアクセスできるページを開きます。カメラ、画面、マイク、その他の入力、出力、および周辺機器に関する詳細を確認できます。電子メールでホワイトボードや注釈を共有できるよう SMPT サーバをセットアップすることもできます。

Users: ページを開くと、ユーザの追加、編集、削除、またはユーザのパスフレーズの変更を行うことができます。このページからリモートサポートユーザを作成することもできます。

Security: 異なるサービスおよびバックエンドとの通信に必要な証明書をアップロードおよび表示できるページを開きます。サインインバナーを作成して、デバイスの再起動時に自動的にリセットするシステムコンポーネントを選択することもできます。

Personalization: ブランディング要素の追加、着信音の選択、ローカル連絡先リスト (お気に入り) の作成を行い、デバイスを個人用に設定できるページを開きます。

Audio Console: オーディオ機能の高度なカスタマイズが可能なグラフィカルインターフェイスを提供するオーディオコンソールが開きます。[3]

UI Extensions Editor: カスタム UI パネルとアクションボタンを作成できる、UI 拡張エディタを開きます。

Macro Editor: デバイスの動作を自動化またはカスタマイズするコード (マクロ) のスニペットを作成できるマクロエディタを開きます。

Developer API: デバイスの XML ファイルを表示し、コマンドと構成を実行できるページを開きます。スタートアップスクリプト (廃止) を作成することもできます[1, 2]。

Software: 新しいソフトウェア[1]とオプションキーをインストールできるページを開きます。プロダクトキーも変更できます。プロダクトキーは、シスコのテクニカルサポートの担当者から指示があった場合にのみ変更します。

Issues and Diagnostics: アクティブな診断メッセージを確認し、ログをダウンロードし、ユーザインターフェイスと画面に表示されるメッセージとインジケータのスクリーンショットを作成できるページを開きます。

Backup and Recovery: ブランディング要素、お気に入りリスト、UI 拡張、マクロ、サインインバナー、および設定など、デバイス上の情報をバックアップおよび復元できるページを開きます。以前のソフトウェアイメージへの切り替え、工場出荷時設定へのリセット、デバイスの再起動またはをシャットダウンを行うこともできます。

[1] クラウドに登録されたデバイスでは使用できません。
[2] スタートアップスクリプト機能は廃止され、今後のリリースで削除されます。代わりにマクロを使用することをお勧めします。
[3] オーディオコンソールは、Codec Pro、Room 70 G2、Room Panorama、Room 70 Panorama、SX80、MX700、および MX800 でのみ使用できます。

ビデオ会議デバイスの管理方法 (5/5 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 ログイン情報でサインインする必要があります。

   この場合、ボードとタッチコントローラは別々に動作します。どちらかにサインインして設定をロック解除しても、もう一方には影響しません。

タッチコントローラ

外部インターフェイスユニットによるデバイスの制御

このガイドを通じて、「タッチコントローラ」を参照します。タッチコントローラは、タッチでデバイスを簡単に制御するために、物理的に接続したり、ビデオ会議デバイスにリモートでペアリングしたりする外部インターフェイスユニットです。タッチコントローラでは、会議やコンテンツから、連絡先やディレクトリまで、あらゆるものに瞬時にアクセスできます。

現在、3 つの外部インターフェイスユニットが使用可能です。すべて区別せずに「タッチコントローラ」と呼ばれます。

- Cisco Webex Room Navigator
- Cisco Touch 10
- Cisco TelePresence Touch 10

ビデオ会議デバイスで会議のエクスペリエンスを制御するだけでなく、タッチコントローラを使用して、照明、間仕切り、カーテンなどの部屋の周辺機器を制御することも可能です。Room Navigator は、電波品質や温度などを監視するための環境センサーも備えています。

タッチコントローラは、(PoE) ネットワークに接続した場合、デバイスに直接接続するか、リモートでペアリングできます。ユニットへの電源供給とネットワークアクセスのために必要なケーブルは 1 本だけです。

ビデオ会議デバイスにタッチコントローラを接続する方法については、► 「タッチコントローラの接続」の章を参照してください。

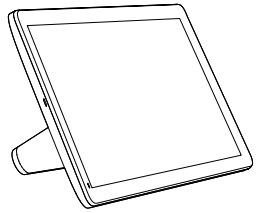
ビデオ会議デバイスとの互換性

Room Navigator は以下をサポートしています。

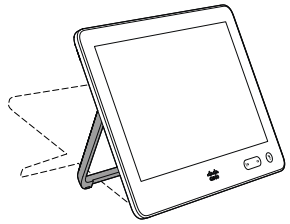
- Room シリーズ
- Board 55S、70S、および 85S

Touch 10 および TelePresence Touch 10 は以下をサポートしています。

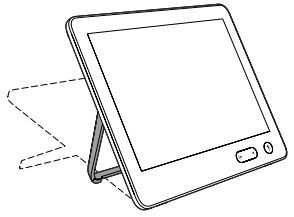
- SX シリーズ
- MX シリーズ
- Room シリーズ
- Board



Cisco Webex Room Navigator
(2021 年初めに発売)



Cisco Touch 10
(2 つ目のバージョン、2017 年後半に発売)



Cisco TelePresence Touch 10
(最初のバージョン)

第 2 章

設定

ユーザ管理

Web 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て、*[ユーザ (Users)]* に移動します。
2. *[ユーザの作成 (Create User)]* をクリックします。
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. *[作成 (Create)]* 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て、*[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. *[保存 (Save)]* 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。

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て、*[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. *[パスフレーズ (Passphrase)]* カードを見つけて、適切な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て、*[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. *[削除 (Delete)]* カードを見つけて、*[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。

*ユーザ ロール*は次の通りです。

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。

- Web 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

パスワードは、*[ユーザ管理 (UserManagement)] > [パスワードポリシー (PasswordPolicy)]* 設定によって設定されたルールに従う必要があります。

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。

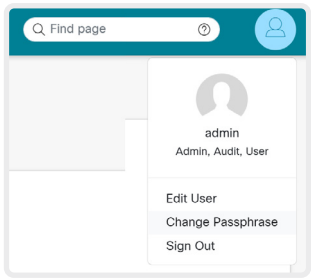
他のユーザ アカウント

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。

自分のパスフレーズの変更

1. Web インターフェイスにサインインして、上部のバーにあるユーザの記号をクリックしてメニューを開きます。
2. *[パスフレーズの変更 (Change Passphrase)]* をクリックします。
3. 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 (Change Passphrase)]* をクリックします。



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て、*[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. *[パスフレーズ (Passphrase)]* カードを見つけて、*[パスフレーズ (Passphrase)]* および *[パスフレーズの確認 (Repeat passphrase)]* 入力フィールドに新しいパスフレーズを入力します。

   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、すべてのユーザーが、ユーザインターフェイス (ボードとタッチコントローラの両方) 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. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
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、ユーザインターフェイス (ボードおよびタッチコントローラ) からデバイスの重要な設定にアクセスするには、ADMIN クレデンシャルでサインインすることが必要になります。

[設定 (Settings)] メニューのロック解除

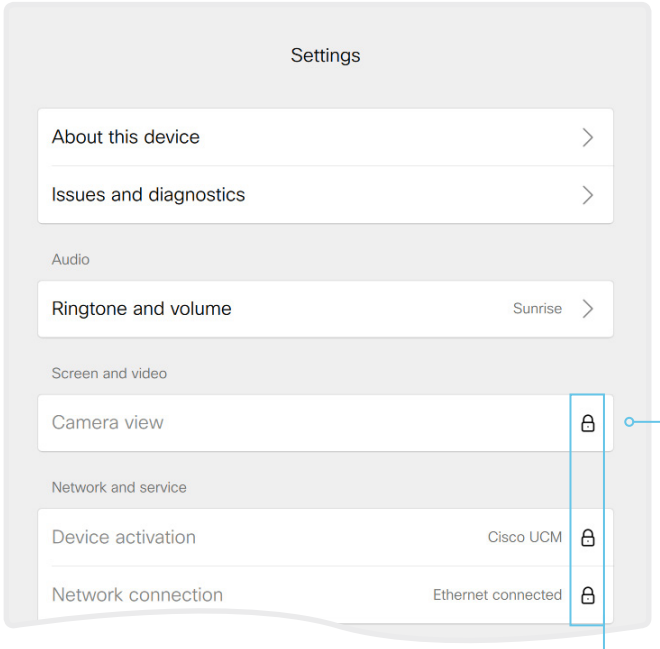
1. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
2. *[ユーザインターフェイス (UserInterface)] > [設定メニュー (SettingsMenu)] > [モード (Mode)]* に移動して、[ロックなし (Unlocked)] を選択します。
3. *[保存 (Save)]* をクリックして変更を有効にします。

   これで、任意のユーザが、ユーザインターフェイス (ボードおよびタッチコントローラ) から [設定 (Settings)] メニューのすべてにアクセスできるようになります。

ユーザインターフェイスの [設定 (Settings)] メニュー

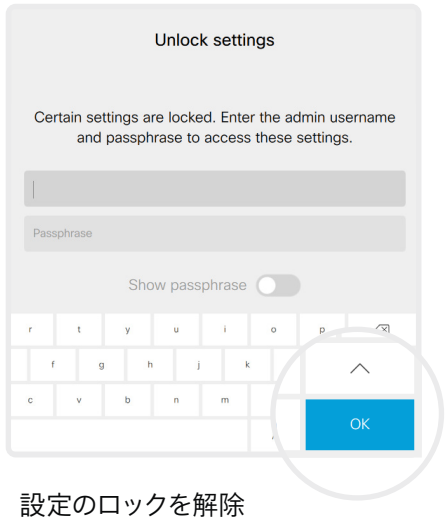
このメニューがロックされている場合は、サインインしないと、デバイスの重要な設定にアクセスできません。

[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。

この場合、ボードとタッチコントローラは別々に動作します。どちらかにサインインして設定をロック解除しても、もう一方には影響しません。

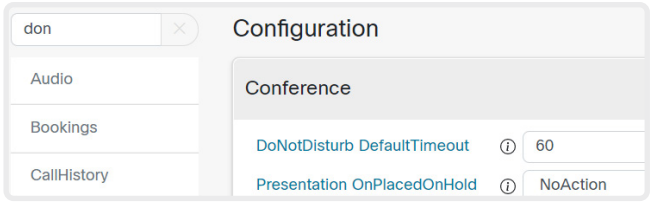
デバイス設定

Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

デバイス設定の検索

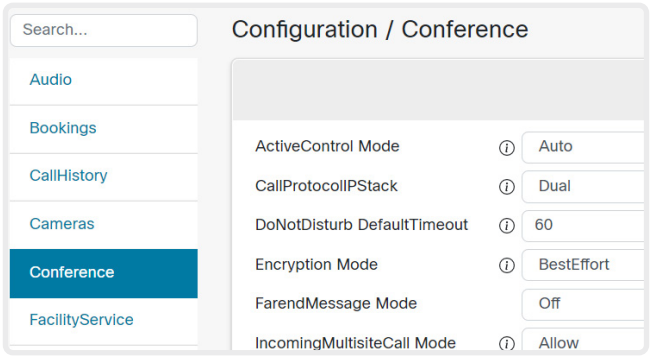
設定を検索する

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

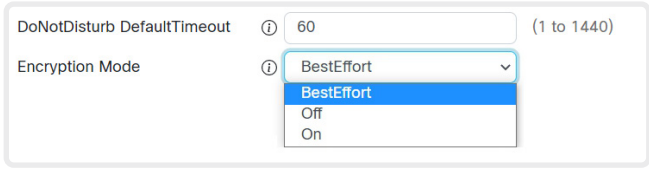
デバイス設定はカテゴリ別にグループ化されています。左側のペインのカテゴリを 1 つ選択して、関連付けられている設定を表示します。



デバイス設定の変更

値スペースを確認する

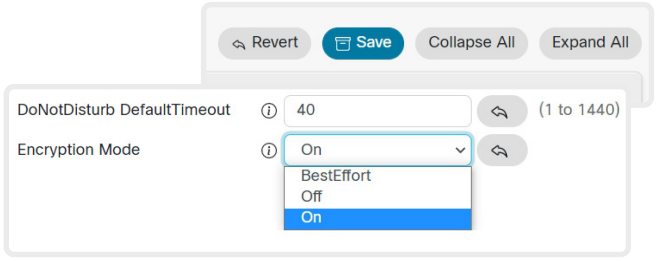
設定の値スペースは、入力フィールドに続くテキストか、矢印をクリックすると開くドロップダウンリストで指定します。



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 (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 ログイン情報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

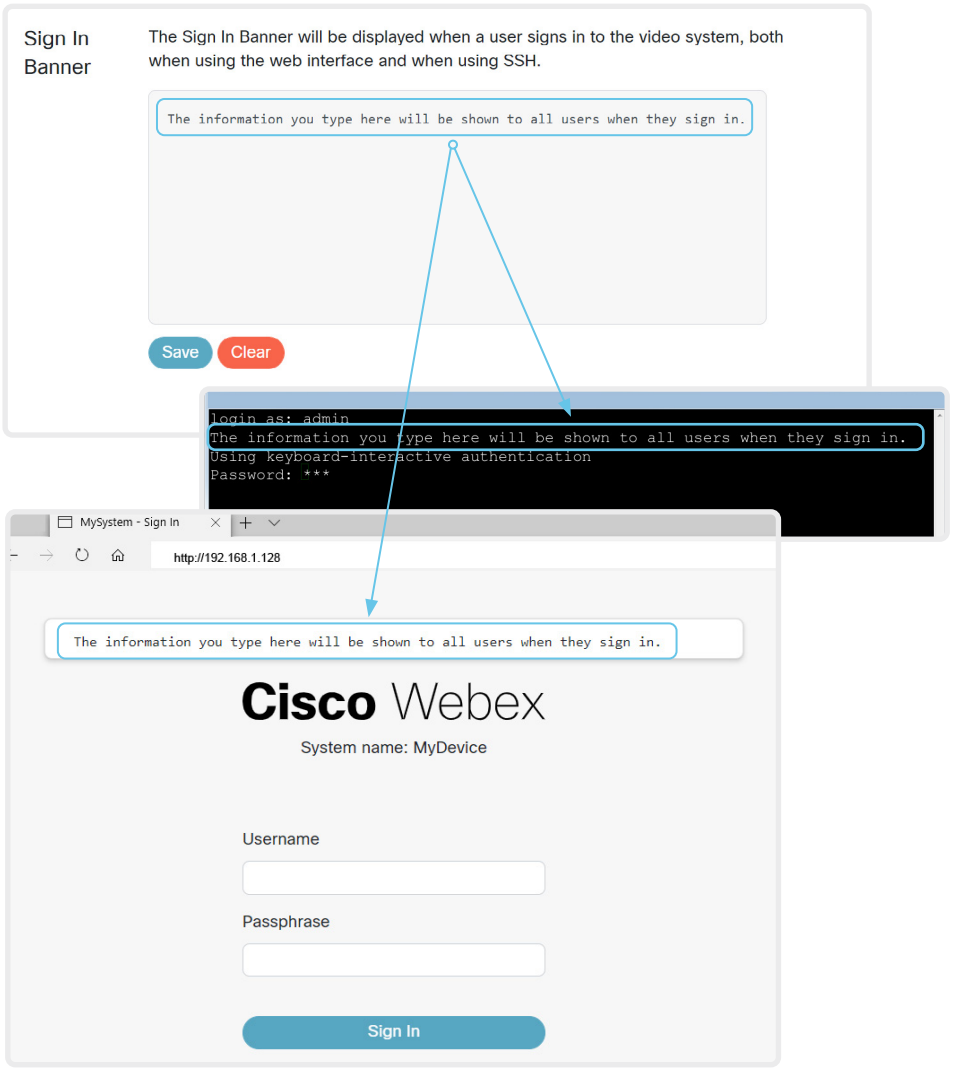
Web インターフェイスにサインインして、*[セキュリティ (Security)]* に移動し、*[サインインバナー (Sign-in Banner)]* を選択します。

サインイン バナーの追加

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。

サインインバナーの削除

- サインインバナーを削除するには、*[クリア (Clear)]* をクリックします。



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 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、ユーザが 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、ユーザが 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

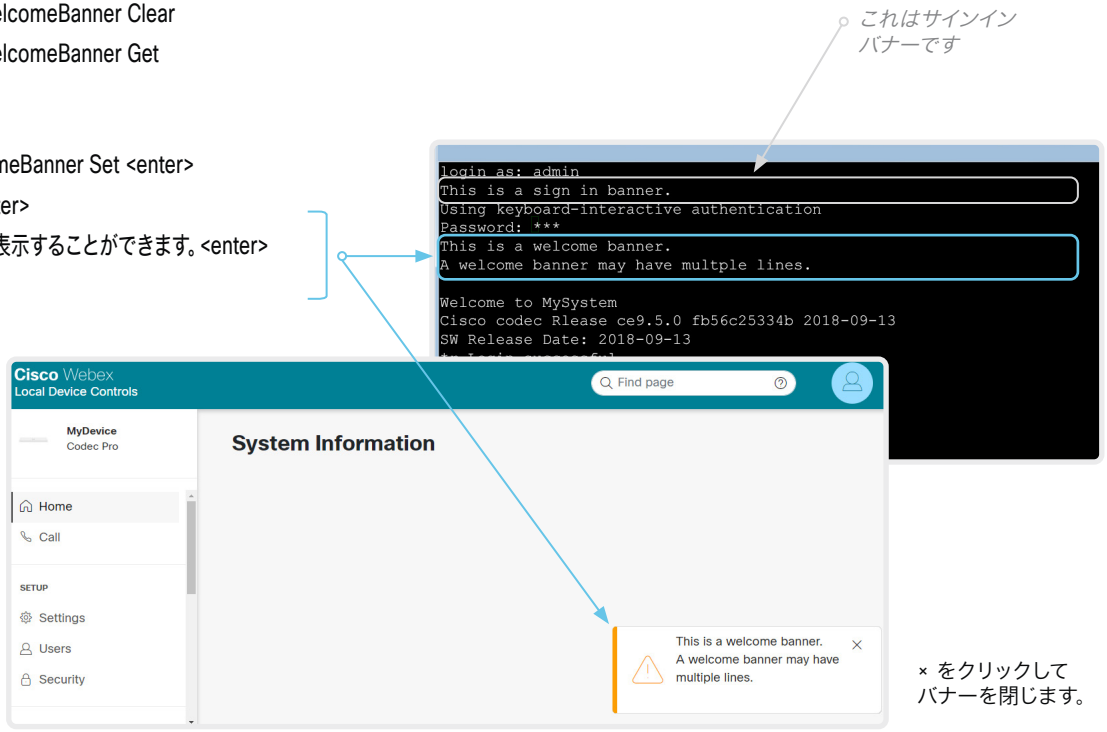
例

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、ユーザが 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、ユーザが 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

Web インターフェイスにサインインして、*[セキュリティ (Security)]* に移動します。*[証明書 (Certificates)]* を選択し、*[サービス (Services)]* サブタブを開きます。

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

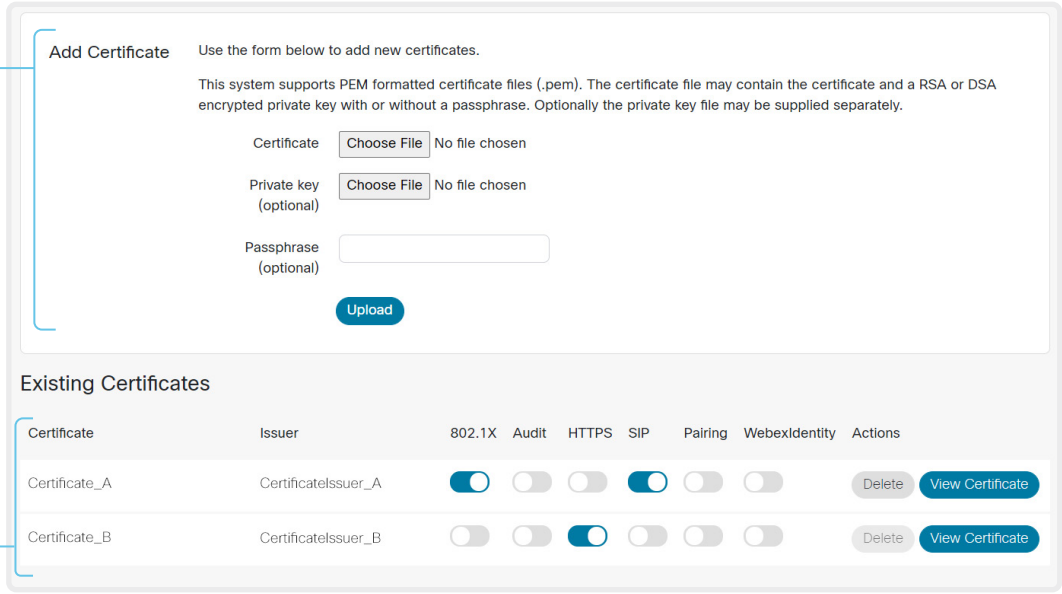
1. [参照 (Browse)] ボタンを押して、コンピュータ上の証明書ファイルと秘密キー ファイル (オプション) を見つけます。
2. 必要な場合には *[パスフレーズ (Passphrase)]* に入力します。
3. *[アップロード (Upload)]* をクリックして、デバイスに証明書を保存します。

   有効期間が 10 年以内の証明書のみが受け付けられます。

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、トグル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。



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 (1/4 ページ)

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て、*[セキュリティ (Security)]* に移動し、*[証明書 (Certificates)]* を選択します。CA リストごとにタブが 1 つ存在します。

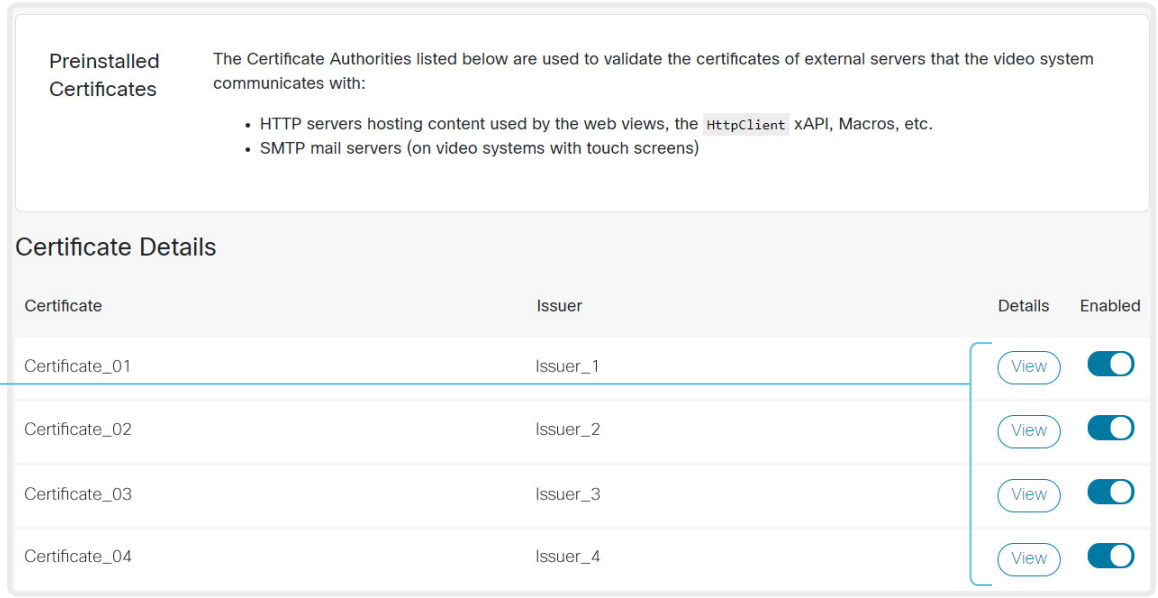
CA リストは次のとおりです。

- *プレインストール*: デバイスと通信する外部サーバー (SMTP、HTTPS、および 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 (Collaboration Edge)*: 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 (MRA とも呼ばれます)、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。
- *カスタム*: 自分でデバイスにアップロードした CA 証明書。ログとその他の接続の証明書を検証するために必要な証明書がプレインストールリストに含まれていない場合は、それらの CA をすべてこのリストに含める必要があります。

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て、*[セキュリティ (Security)]* に移動します。*[証明書 (Certificates)]* を選択し、*[プレインストール (Preinstalled)]* サブタブを開きます。



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。

[表示 (View)]、証明書の有効化または無効化

証明書の詳細を表示するには、*[表示 (View)]* ボタンを使用します。

トグルボタンを使用して、証明書を有効または無効にします。

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。

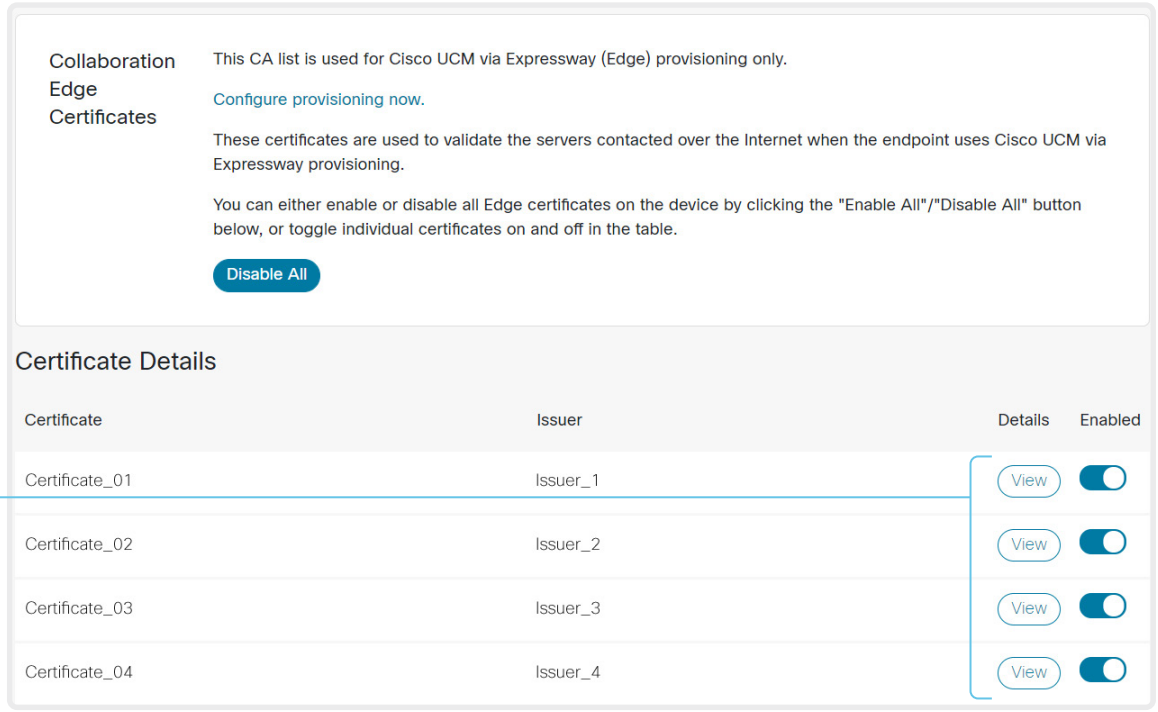
- HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバー
- プロビジョニング サーバ
- 電話帳サーバ
- syslog サーバ (外部ロギング用)
- SMTP メール サーバ
- Cisco Webex クラウドによって使用されるサーバーおよびサービス

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て、*[セキュリティ (Security)]* に移動します。*[証明書 (Certificates)]* を選択し、*[コラボレーションエッジ (Collaboration Edge)]* サブタブを開きます。



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。

[表示 (View)]、証明書の有効化または無効化

証明書の詳細を表示するには、*[表示 (View)]* ボタンを使用します。

トグルボタンを使用して、証明書を有効または無効にします。

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。

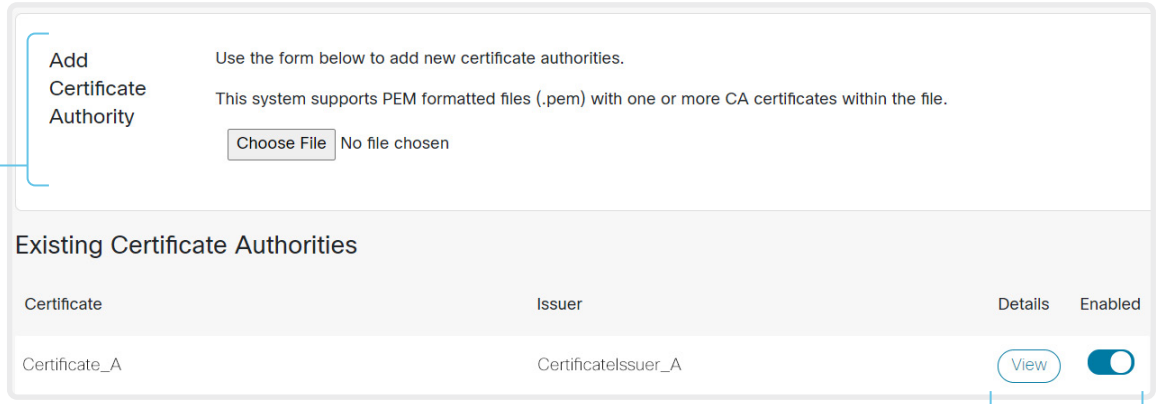
信頼できる認証局 (CA) のリストの管理 (4/4 ページ)

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て、*[セキュリティ (Security)]* に移動します。*[証明書 (Certificates)]* を選択し、*[カスタム (Custom)]* サブタブを開きます。

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) 。



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。

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. *[アップロード (Upload)]* をクリックして、デバイスに新しい CA 証明書を保存します。

   ファイルを選択すると、ボタンが表示されます。

[表示 (View)]、証明書の有効化または無効化

証明書の詳細を表示するには、*[表示 (View)]* ボタンを使用します。

トグルボタンを使用して、証明書を有効または無効にします。

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)
- SMTP メール サーバ
- 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およびサービス

セキュア監査ロギングのセットアップ

Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

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。

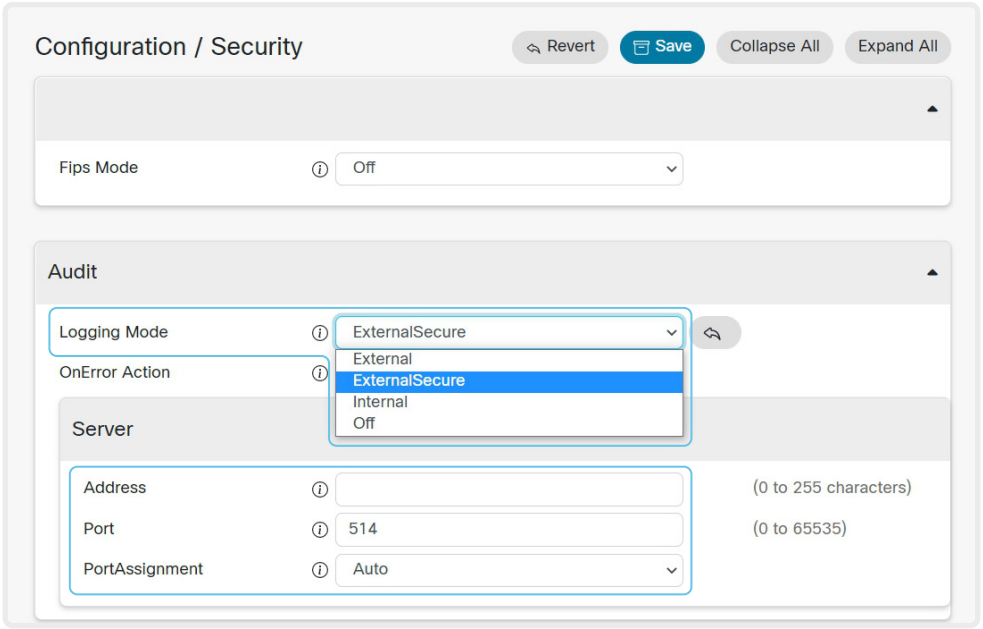
リストの更新方法については、▶ 「デバイスへの CA 証明書のアップロード」の章を参照してください。

1. *[セキュリティ (Security)] > [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。

2. *[セキュリティ (Security)] > [監査 (Audit)] > [ロギング (Logging)] > [モード (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 信頼リストの削除

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て、*[セキュリティ (Security)]* に移動します。*[証明書 (Certificates)]* を選択し、*[Unified CM]* サブタブを開きます。

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、Web 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。

永続モードの変更

Web インターフェイスにサインインして、*[セキュリティ (Security)]* に移動し、*[永続設定 (Persistency Settings)]* を選択します。

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、*[設定 (Settings)]* に移動し、*[ステータス (Statuses)]* を選択し、 *[セキュリティ (Security)] > [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. *[適用 (Apply)]* 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の詳細については、► 「ビデオ会議デバイスの初期設定へのリセット」の章を参照してください。

SMTP 電子メールサーバーのセットアップ

SMTP サーバー接続を設定すると、ビデオ会議デバイスのユーザーが、組織内外の人と電子メールでホワイトボードやコメントを共有できるようになります。

サーバーのセットアップは手動で行うこともできますが、セットアップウィザードを使用することを強くお勧めします。ウィザードを使用すれば、セットアップ中に接続をテストすることや、サーバー証明書のアップロードが必要な場合に、その方法についてガイダンスを得ることができます。

電子メールによる共有の有効化

1. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
2. *[ネットワークサービス (NetworkServices)] > [SMTP] > [モード (Mode)]* に移動します。電子メールによる共有は、[モード (Mode)] が [オン (On)] の場合にのみ可能になります。

ウィザードを使用したサーバーのセットアップ 推奨

1. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[ホワイトボードを電子メールに送信 (Send Whiteboard to Email)]* を選択します。
2. *[ウィザードを開始 (Start Wizard)]* をクリックし、サーバーのアドレス、暗号化方式、およびポート番号を入力します。
3. *[接続のテスト... (Test Connection...)]* をクリックします。.

   問題がなければ、*[OK]* をクリックしてウィザードを続行します。

   証明書が見つからない場合は、*[再設定 (Reconfigure)]* をクリックし、ウィザードの指示に従って必要な証明書をデバイスにアップロードします。
4. ホワイトボードや注釈の送信元となる電子メールアドレスを入力します。
5. SMTP サーバーが認証を要求し、暗号化方式が TLS または STARTTLS の場合は、ユーザー名とパスワードのフィールドに入力します。
6. *[確認して保存 (Verify and Save)]* を選択して、サーバーのセットアップウィザードを完了します。

   これで、*[ネットワークサービス (NetworkServices)] > [SMTP] > [モード (Mode)]* が **[オン (On)]** になっていれば、デバイスから電子メールでホワイトボードや注釈を送信することができます。

ウィザードを開始するのではなく、*[手動設定 (Manual Configuration)]* を選択した場合は、上記で説明したのと同じフィールドに入力し、*[確認して保存 (Verify and Save)]* を選択します。

設定ページからのサーバの設定

1. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
2. *[ネットワークサービス (NetworkServices)] > [SMTP]* に移動し、*[サーバー (Server)]*、*[セキュリティ (Security)]* (暗号化方式) 、*[ポート (Port)]*、*[送信元 (From)]*、*[ユーザー名 (Username)]*、および *[パスワード (Password)]* を設定します。
3. 必要に応じて、▶「デバイスへの CA 証明書のアップロード」 の章の説明に従って、デバイスに CA 証明書をアップロードします。

暗号化方式と証明書

暗号化方式は、電子メールサーバーでサポートされているものを選択する必要があります。

TLS および STARTTLS 暗号化方式には、サーバー証明書が必要です。SMTP サーバーの証明書を検証できない場合、デバイスは接続を許可しません。証明書チェックを無視することはできません。

ほとんどの場合、サーバー証明書はデバイスにプレインストールされている CA リストを使用して検証できます。そうでない場合は、必要な証明書を自分でデバイスにアップロードする必要があります。自分でアップロードした証明書は、カスタム証明書のリストに追加されます。

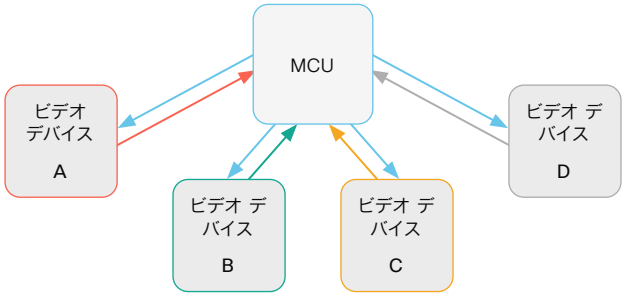
CA リストの詳細については、▶「信頼できる認証局 (CA) のリストの管理」の章を参照してください。

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。

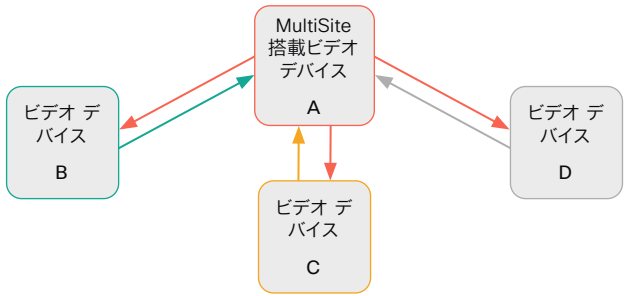


このセットアップでは、ビデオ デバイス A、B、C および D は、4 者会議に参加しています。MCU がすべてのデバイスからのメディア ストリームを受信し、ストリームを処理して、すべてのメディアを他の参加者に送信します。

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、Room Panorama、Room 70 Panorama、Desk Pro : 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。

[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。

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	直接リモート追加	• 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	1 オーディオ追加	• 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	協議追加	• CUCM に登録されたデバイスでのみ使用でき、*[SIP] > [タイプ (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, 4]	はい	該当なし	ローカルマルチサイト[5]	• 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。
	いいえ	該当なし	1 オーディオ追加	• 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)	はい	MCU	直接リモート追加	• 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	カスケードなしのローカルマルチサイト[5]	• 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。
	いいえ	MCU	直接リモート追加	• 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	1 オーディオ追加	• 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、*[コール (Call)] [n] > [デバイスタイプ (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。

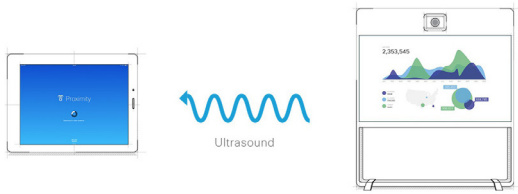
[4] マルチストリームを使用している会議では、マルチサイトは自動的に無効になります。つまり、UI の [追加 (Add)] ボタンを使用して、会議に新しい参加者を追加することはできません (ビデオ参加者も音声のみの参加者も追加できません)。

[5] 会議のカスケードを避けるために、*[会議 (Conference)] > [マルチポイント (Multipoint)] > [モード (Mode)]* を **[マルチサイト (MultiSite)]** ではなく **[自動 (Auto)]** に設定することを推奨します。

コンテンツ共有用のインテリジェントプロキシミティのセットアップ (1/5 ページ)

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。

ビデオ会議デバイス	最大接続数
Room Kit、Room Kit Mini、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Panorama、Room 70 Panorama、Codec Plus、Codec Pro	30/7 *
Desk Pro	30/7 *
Board 55/55S、Board 70/70S、Board 85S	30/7 *
SX80、MX700、MX800	10
SX10、SX20、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

コンテンツ共有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

エンドユーザ ライセンス契約書をよく確認してください。
► https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

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。

コンテンツ共有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のペアリングメッセージを発します。

[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 (および超音波ペアリングメッセージの出力) の **[オン (On)]** と **[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、75dB 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 Panorama、Room 70 Panorama、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 50cm 以上の距離では、超音波の音圧レベルは 75dB 未満になります。

Desk Pro、DX70、DX80 :

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

Board :

- 画面から 20cm 以上の距離では、超音波の音圧レベルは 75dB 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コントロールは効果がありません。

ヘッドセット

Desk Pro、DX70、DX80、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。

- Desk Pro、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 Panorama、Room 70 Panorama、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。

コンテンツ共有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. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
2. *[プロキシミティ (Proximity)] > [モード (Mode)]* に移動します。[プロキシミティ (Proximity)] が On (デフォルト) になっていることを確認します。この場合、ビデオ会議デバイスは超音波のペアリング メッセージを送信します。

   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

プロキシミティ機能はデフォルトで**オン**に設定されています。

[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。

Cisco では、最善のユーザ エクスペリエンスのため、Proximity は常に **[オン (On)]*** に設定することをお勧めしています。

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。

* プロキシミティ (超音波) を**オン**に切り替えた場合は、ヘッドセットを使用*しない*ことをお勧めします。

コンテンツ共有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)

部屋の考慮事項

部屋の音響

- 壁/床/天井の表面が硬い部屋では、音の反響が大きいことが問題になる場合があります。最良の会議環境とインテリジェント プロキシミティのパフォーマンスを確保するために、会議室の音響処理を常に強く推奨します。
- 1 つの部屋の中で Intelligent Proximity を有効にするビデオ会議デバイスは 1 つだけにすることを推奨します。複数あると、干渉が発生する可能性があり、デバイス検出とセッション メンテナンスの問題の原因となることがあります。

プライバシーについて

シスコのプライバシーポリシーと 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

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

ビデオ品質対コールレート比の調整

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、*[ビデオ (Video)　> [入力 (Input)] > [コネクタ n (Connector n)] > [画質 (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。

60 fps でのビデオ送信のしきい値

60 fps でのビデオ送信を許可する条件を決定するには、*[ビデオ (Video)　> [入力 (Input)] > [コネクタ n (Connector n)] > [最適鮮明度 (OptimalDefinition)] > [60fps のしきい値 (Threshold60fps)]* 設定を使用します。

このしきい値より低い解像度では、最大転送フレームレートが 30 fps になります。このしきい値より高い解像度については、使用可能な帯域幅が十分であれば 60 fps になる可能性があります。

Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

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。
3. *[ビデオ (Video)] > [入力 (Input)] > [コネクタn (Connector n)] > [最適鮮明度 (OptimalDefinition)] > [60fpsのしきい値 (Threshold60fps)]* に移動して、その解像度よりも低い場合に最大転送フレームレートを 30 fps にするしきい値を設定します。

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			H.264、最大 60fps		
	標準	*中*	*高*	*標準*	*中*	*高*
128	320 × 180 @ 30	320 × 180 @ 30	512 × 288 @ 30	320 × 180 @ 30	512 × 288 @ 20	512 × 288 @ 30
256	512 × 288 @ 30	640 × 360 @ 30	768 × 448 @ 30	512 × 288 @ 30	640 × 360 @ 30	768 × 448 @ 30
384	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30
512	768x448@30	1024x576@30	1024x576@30	768x448@30	1024x576@30	1024x576@30
768	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30
1152	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 60
1472	1280 × 720 @ 30	1280 × 720 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 60
1920	1280x720@30	1920x1080@30	1920x1080@30	1280x720@30	1280x720@60	1280x720@60
2560	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
3072	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
4000	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1920x1080@60	1920x1080@60
6000	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60

画面およびタッチコントローラへの企業ブランディングの追加 (1/2 ページ)

Web インターフェイスにサインインして、*[パーソナライゼーション (Personalization)]* に移動し、*[ブランディング (Branding)]* を選択します。

このページから、背景ブランドイメージや会社のロゴなど、独自のブランディング要素を追加できます。要素は、デバイスがハーフウェイク状態またはアウェイク状態の場合に表示されます。

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。

- 右下隅にブランドロゴを追加する (画面およびタッチコントローラ)

ロゴ

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

この章で説明するブランディング機能では、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、画面とタッチコントローラの表示をカスタマイズできます。

画面およびタッチコントローラへの企業ブランディングの追加 (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。

- カスタムブランド背景を追加する (画面およびタッチコントローラ)
- 右下隅にブランドロゴを追加する (画面およびタッチコントローラ)

カスタムブランド背景

- 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 : 3840 × 2160 ピクセル

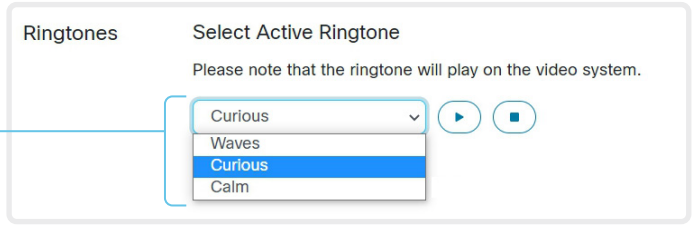
ロゴ

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

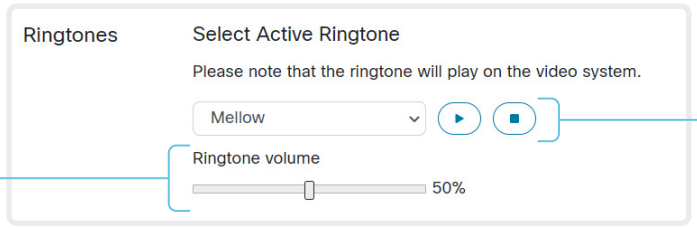
着信音の選択と着信音量の設定

Web インターフェイスにサインインして、*[パーソナライゼーション (Personalization)]* に移動し、*[着信音 (Ringtones)]* を選択します。



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、Web インターフェイスを使用します。

Web 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。

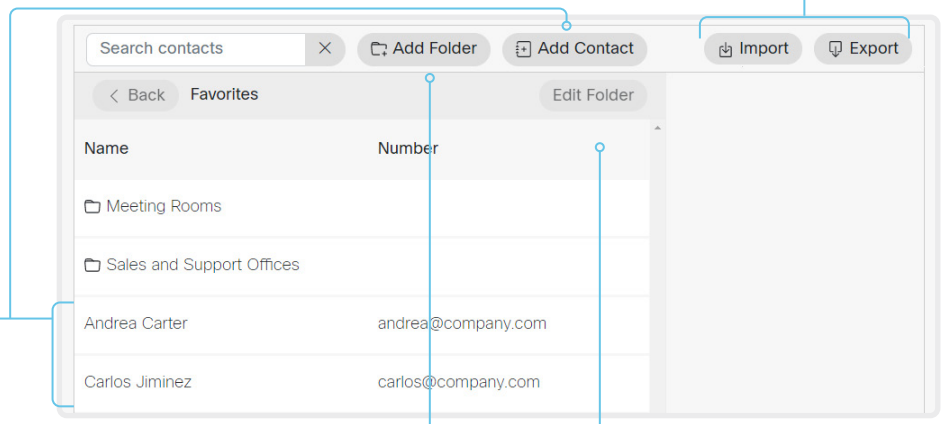
お気に入りリストの管理

Web インターフェイスにサインインして、*[パーソナライゼーション (Personalization)]* に移動し、*[連絡先 (Contacts)]* を選択します。

ファイルからの連絡先のインポートまたはエクスポート

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。

コンタクトを削除する

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、一覧表示されたサブフォルダの 1 つをクリックしてから *[フォルダの編集 (Edit Folder)]* をクリックして既存のサブフォルダを変更します。
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

Board では、これはボード自体ではなくペアリングされたタッチコントローラにのみ適用されます。

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. *[お気に入りへの追加 (Add to favorites)]* 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. *[お気に入りの削除 (Remove 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設定できます。

1. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
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。

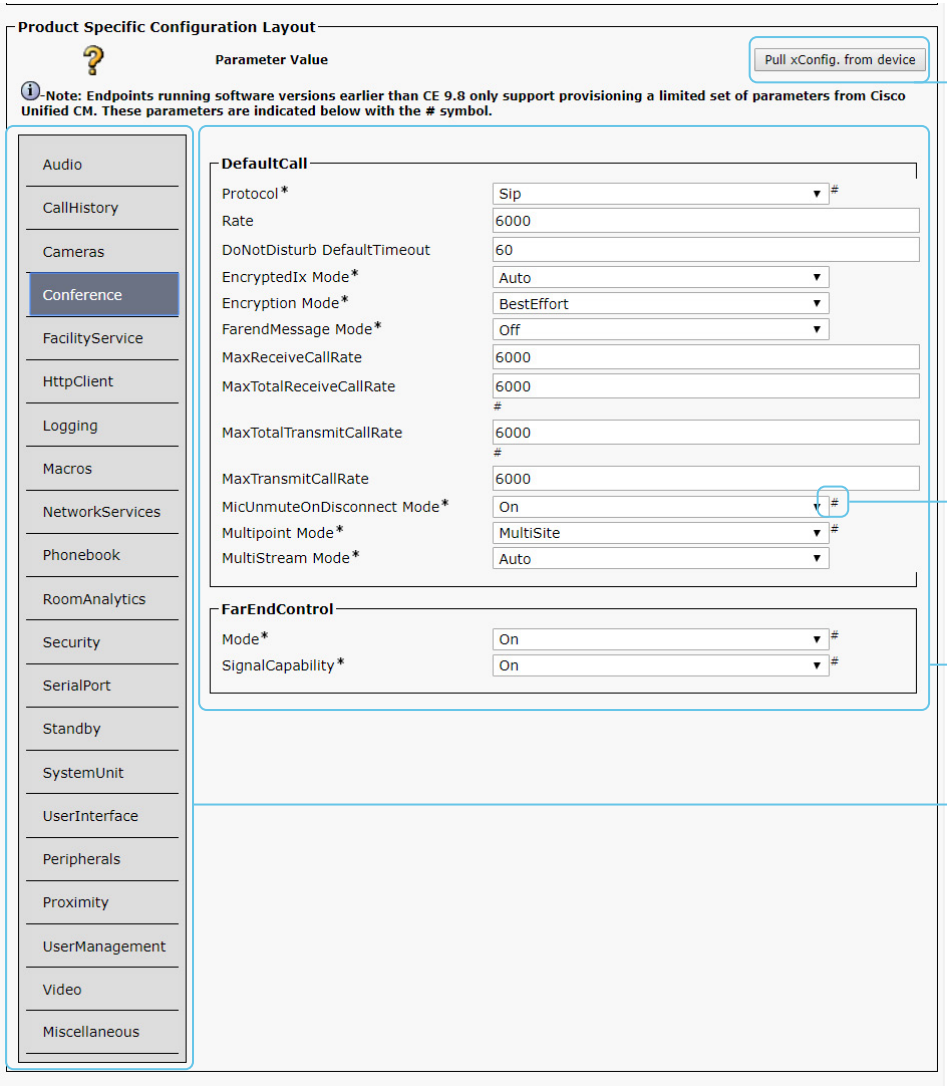
パラメータの完全なセットは、デバイスを CE9.8 以降にアップグレードした場合にのみ機能します。

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

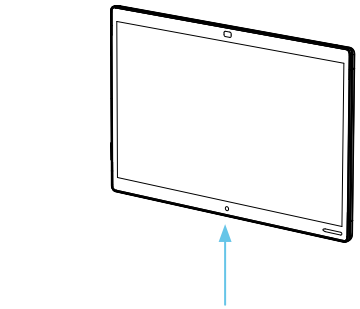
入力ソースの接続

Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択すると、この章に示す設定が見つかります。

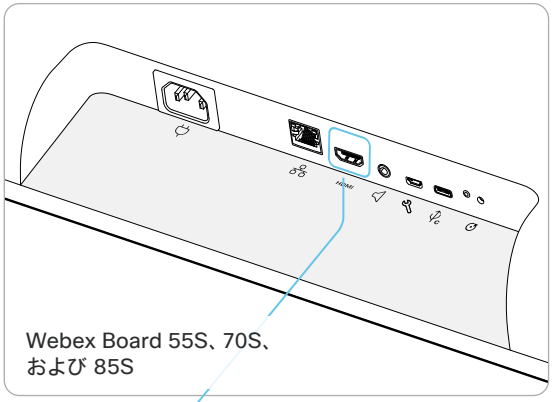
コンピュータまたはその他のコンテンツ ソースの接続

入力ソースを 1 つ接続できます。たとえば、1 台のコンピュータを デバイスの HDMI 入力 (入力コネクタ 2) に接続して、コンテンツをローカルで共有したり、会議の参加者と共有したりできます。

HDMI 入力は、30 fps で最大 3840 × 2160、60 fps で最大 1080p の解像度をサポートします。高解像度とフレーム レートをサポートするハイスピード HDMI 1.4b ケーブルが必要です。

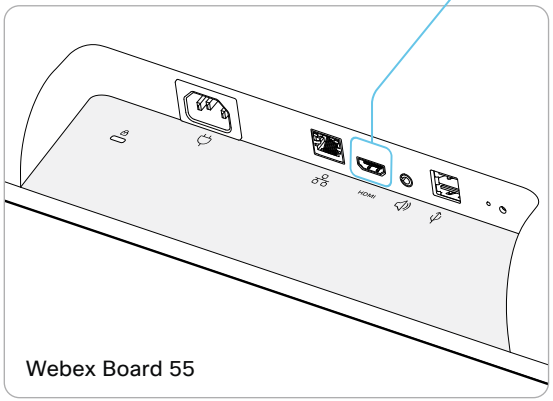


コネクタパネルは下部背面にあります。

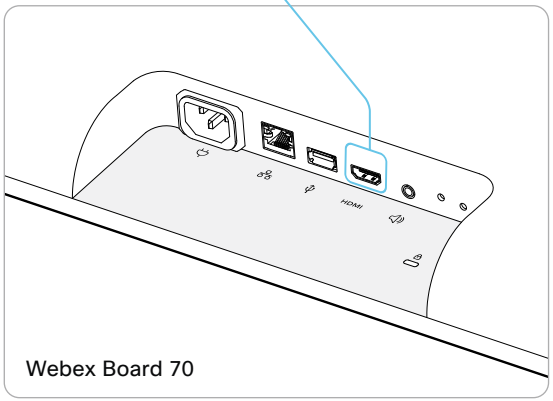


Webex Board 55S、70S、および 85S

入力コネクタ 2
コンピュータまたはその他のコンテンツソース用の HDMI 入力 (オーディオとビデオ)



Webex Board 55



Webex Board 70

入力ソースの接続 (2/2 ページ)

入力ソースのタイプと名前の設定

入力ソースのタイプと名前を設定することをお勧めします。

- *[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [入力ソースタイプ (InputSourceType)]*
- *[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [名前 (Name)]*

これらの設定によって、ユーザ インターフェイスに表示される名前とアイコンが決まります。分かりやすい名前とアイコンを設定すると、ソースを簡単に選択できるようになります。

入力コネクタ 1 は内蔵カメラであることに注意してください。

ビデオとコンテンツの品質について

モーションまたは鮮明度に関する品質を最適化するには、*[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [品質 (Quality)]* 設定を使用します。

通常、画像の動きが激しい場合は、[モーション (Motion)] を選択する必要があります。高品質で詳細な画像とグラフィックが必要なときは、[シャープネス (Sharpness)] を選択します。

コネクタ 2 のデフォルト値は **シャープネス**です。

4K 解像度について

コンピュータの接続

コンピュータの接続時にエラーが発生すると、画面とタッチコントローラにメッセージが表示されます。

ビデオ入力コネクタのデフォルトの推奨解像度は 1080p60（1920_1080_60）です。コンピュータで 4K 解像度を使用する場合は、Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。*[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [推奨解像度 (PreferredResolution)]* に移動して、値を調整します。

また、接続しているコンピュータのオペレーティング システムが提供するディスプレイ/モニタ設定から解像度を上書きすることもできます。

チェックリスト

確実な動作のために、シスコに HDMI ケーブルを注文するか、認定 HDMI ケーブルを使用してください。▶「HDMI ケーブルについて」の章を参照してください。

ビデオ会議デバイスの入力コネクタが正しく設定されていることを確認してください。

デバイス（コンピュータ）が 4K をサポートしていて、正しく設定されていることを確認してください。

4K の使用では高品質ケーブルの必要性が増します。

- 4kp30 は 1080p60 の約 2 倍のデータレートを使用します。
- 4kp60 は 1080p60 の約 4 倍のデータレートを使用します。

HDMI ケーブルについて

プレゼンテーションソースとの接続には HDMI ケーブルが必要です。

確実な動作のために、Cisco に HDMI ケーブルを注文*するか、認定 HDMI ケーブルを使用することをお勧めします。

プレゼンテーション ソース用の HDMI ケーブル

プレゼンテーション ソースには、PC/ラップトップ、ドキュメント カメラ、メディア プレーヤー、ホワイトボード、またはその他のデバイスを使用できます。

1920X1080@60fps を超える解像度フォーマットには、必ずハイスピード対応の HDMI ケーブルを使用してください。確実な動作のために、シスコが提供している HDMI ケーブルを使用するか、高速 HDMI 1.4b カテゴリ 2 仕様準拠のケーブルを使用してください。

HDMI プレゼンテーション ケーブルはシスコに注文 (HDMI 1.4b カテゴリ 2) することをお勧めします。

HDMI ケーブルの詳細については、▶ http://www.hdmi.orgを参照してください

* シスコの 4K マルチヘッドケーブル (CAB-HDMI-MUL4K-9M および CAB-HDMI-MUL4K-2M) は、Board および Room シリーズのデバイスと互換性があります。これらのケーブルには、HDMI タイプ A - USB-C、Mini ディスプレイポート、および HDMI タイプ A のコネクタが搭載されています。

1080p マルチヘッドケーブル (CAB-HDMI-MULT-9M) は、SX および MX シリーズのデバイスと互換性があります。1080p のコンテンツに限定するデバイスには、このケーブルを推奨します。このケーブルには、HDMI タイプ A - ディスプレイポート、Mini ディスプレイポート、および HDMI タイプ A のコネクタが搭載されています。

スピーカートラック機能のセットアップ (1/2 ページ)

スピーカートラッキング機能

スピーカートラッキング機能は、デバイスのカメラによって異なります。

最適な全体表示

デジタル顔検出および自動カメラフレーミングは、状況を評価し、室内のすべての人を含むベストオーバービューを構成するために使用されます。このシステムは、室内で参加者が移動したり、新たな参加者が入室した場合に、フレームにすべての人が含まれるように自動的に調整します。

Desk Pro および Room Kit Mini はベストオーバービューに制限されます。ただし、このページで説明されている他のデバイスはオーディオトラッキングも使用しています。これは、クローズアップとグループフレーミングの作成をサポートするために、室内で通話中のスピーカーの位置を特定するために使用されます。

クローズアップ

Desk Pro または Room Kit Mini ではサポートされていません。

クローズアップが有効になっている場合は、他の参加者を除外して通話中のスピーカーを見つけてズームインするためにオーディオトラッキングが使用されます。室内のすべての人がカメラフレーム内に常に含まれるようにする場合は、クローズアップ機能をオフにします。

スピーカーのみに焦点を合てたい場合は、いくつかの制限があることに注意してください。カメラの最大ズーム係数と、カメラからのスピーカーの距離によっては、スピーカーのフレーミングを単独で作成できない場合があります。

グループフレーミング

SpeakerTrack 60 カメラ、MX700/MX800、Desk Pro または Room Kit Mini ではサポートされていません。

ここでは、通話中のスピーカーだけでなく、通話中のスピーカーのすぐ近くにいる参加者も含むフレームを作成することで、より自然なユーザエクスペリエンスをシステムで作成することを目指しています。

これには、切り替えの総数を減らすという効果的な影響があります。たとえば、フレーム内の別の人が話し始めた場合に、おそらくカメラは再フレームする必要がありません。

表示の制限

SpeakerTrack 60 カメラ、MX700/MX800、SX80、Desk Pro、Room Kit Mini、またはパノラマ表示ビデオシナリオでの Room Panorama / Room 70 Panorama ではサポートされません。

*表示の制限*機能を使用すると、ユーザインターフェイスによって視野角を制限し、部屋の一部を除外することができます。

カメラの仕様

スピーカートラッキングをサポートする内蔵カメラ *(デュアルカメラが搭載されている MX700/MX800、Room Kit、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room 70 Panorama、Room Panorama、Board)*

- カメラはベストオーバービューとクローズアップをサポートしています。
- グループフレーミングは、MX700/MX800 を除くすべての内蔵カメラでサポートされています。

Cisco Quad Camera *(SX80、Codec Plus、および Codec Pro のオプション)*

- カメラは、ベストオーバービュー、クローズアップ、グループフレーミングをサポートします。
- 適切なグループフレーミングを見つけることが、通話中のスピーカーのみのクローズアップを作成することよりも優先されます。
- カメラの最大ズーム係数は SpeakerTrack 60 カメラよりも小さいため、カメラから離れているスピーカーに接近してズームインすることはできません。

Cisco TelePresence SpeakerTrack 60 カメラ *(SX80、Codec Plus、および Codec Pro のオプション)*

- デュアルカメラアセンブリは、ベストオーバービューとクローズアップをサポートする 2 つのカメラで構成されています。
- グループフレーミングはサポートされていません。スピーカーの変更が検出された場合、ビデオ会議デバイスでは、最適なカメラフレームが常に表示されるように、2つのカメラを自動的に切り替えます。

ベストオーバービューに制限されるカメラ *(Room Kit Mini および Desk Pro)*

- ベストオーバービューはサポートされています。
- グループフレーミングとクローズアップはサポートされていません。

スピーカー トラッキングをサポートしている製品

次の Cisco 製品がスピーカー トラッキングをサポートしています。

- デュアル カメラが搭載されている MX700 および MX800
- SpeakerTrack 60 カメラまたは Quad Camera 搭載の SX80
- Room Kit
- Room Kit Mini [1]
- Quad Camera 搭載 Codec Plus (Room Kit Plus) または SpeakerTrack 60 カメラ
- Quad Camera 搭載 Codec Pro （Room Kit Pro) または SpeakerTrack 60 カメラ
- Room 55
- Room 55 Dual
- Room 70
- Room 70 G2
- Room Panorama [2]
- Room 70 Panorama [2]
- Board
- Desk Pro [1]

[1] 完全なスピーカートラッキング機能はサポートされていません。ベストオーバービューのみです。これらの製品については、*[カメラ (Cameras)] > [スピーカートラック (SpeakerTrack)] > [モード (Mode)]* 設定がベストオーバービューのオン/オフの切り替えに該当します。

[2] パノラマ表示ビデオシナリオでは、2 つのカメラのパノラマ表示をオフにすることはできません。この場合、スピーカートラッキングは有効になりません。他のすべてのシナリオでは、スピーカートラッキングは動作し、この章で説明するように設定できます。

スピーカートラック機能のセットアップ (2/2 ページ)

Web インターフェイスにサインインして、[設定 (*Settings*)] に移動し、[設定 (*Configurations*)] を選択すると、ここに示す設定が見つかります。

スピーカー トラッキングの設定

発言者追跡機能

[カメラ (*Camera*)] > [スピーカー トラック (*SpeakerTrack*)] > [モード (*Mode*)]

この設定は、スピーカートラッキングのオン/オフを切り替えるためのものです。[1]

自動 (Auto) : スピーカートラッキングはデフォルトでは有効になっています。ユーザは、ユーザインターフェイスのカメラ制御パネルから、モードのオンとオフをすぐに切り替えることができます。または Board では、 Board 自体の [設定 (Settings)] > [詳細設定 (Advanced Settings)] パネルから切り替えることができます。

オフ (Off) : スピーカートラッキングはオフになります。ユーザインターフェイスからオンに切り替えることはできません。

クローズアップ

[カメラ (*Camera*)] > [スピーカー トラック (*SpeakerTrack*)] > [クローズ アップ (*Closeup*)]

この設定は、*[カメラ (Cameras)] > [スピーカートラック (SpeakerTrack)] > [モード (Mode)]* が [自動 (Auto)] に設定されている場合にのみ適用されます。

クローズアップ機能をオンまたはオフにします。

自動 (Auto) : 動作はデバイスのタイプによって異なります。Board では、室内のすべての人を常にカメラフレーム内に含めることを目指します。その他のデバイスは、話している人にズームインします。

オフ (Off) : デバイスは室内のすべての人を常にカメラフレーム内に含めます。

オン (On) : デバイスは通話中のスピーカーにズームインします。

ホワイトボードモード

[カメラ (*Cameras*)] > [スピーカートラック (*SpeakerTrack*)] > [ホワイトボード (*Whiteboard*)] モード

ホワイトボードへのスナップ機能は、スピーカートラッキングをサポートするデバイスのサブセットでのみサポートされます[2]。.

[1] Desk Pro または Room Kit Mini の場合、この設定はベストオーバービューのオン/オフの切り替えに該当します。

[2] ホワイトボードへのスナップ機能は、SX80、デュアルカメラが搭載されている MX700/MX800、Room Kit、Codec Plus、Codec Pro、Room 55、Room 55 Dual、Room 70、および Room 70 G2 でサポートされています。

タッチコントローラの接続 (1/4 ページ)

タッチコントローラは、ネットワーク (LAN) を経由してビデオ会議デバイスとペアリングする必要があります。これは、リモート ペアリングと呼ばれます。

ネットワーク (LAN) を経由してタッチコントローラをビデオ会議デバイスに接続する

図のように、タッチコントローラ[2] とビデオ会議デバイスを壁面のネットワークソケットまたはネットワークスイッチに接続します。

タッチコントローラの設定

タッチコントローラを電源に接続すると、セットアップ手順が開始します。画面に表示される指示に従います。

[ルーム システムの選択 (Select a room system)] 画面が表示されたら、以下の点に注意してください。

- ペアリングできることを信号で伝えているデバイスのリストが、画面に表示されます。ペアリングするデバイスの名前をタップします。

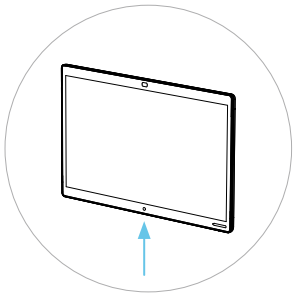
  デバイスがリストに表示されるためには、次の条件を満たす必要があることに注意してください。

  - デバイスとタッチコントローラは同じサブネット上にある必要があります。
  - デバイスが直近 10 分以内に再起動されている必要があります。デバイスがリストに表示されていない場合は、再起動をお試しください。
- 使用可能なデバイスのリストにデバイスが表示されない場合は、入力フィールドに IP アドレスまたはホスト名を入力します。*[接続 (Connect)]* をタップします。
- ペアリング プロセスを開始するには、ユーザ名とパスワードを使用してログインする必要があります。*[ログイン (Login)]* をタップします。

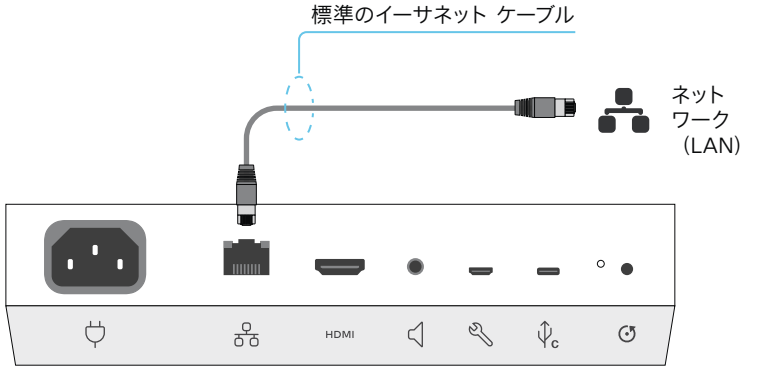
  user ロールを持つユーザであれば十分対応できます。このタスクを実行するために admin ロールは必要ありません。

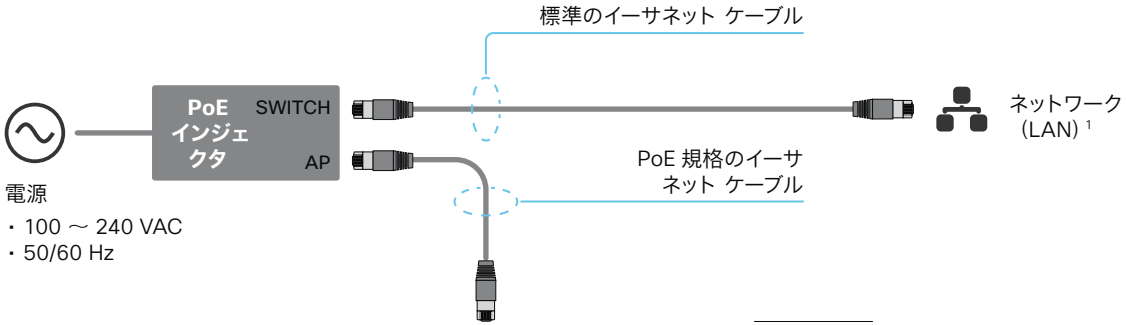
  ユーザ アカウントを作成してそれにロールを割り当てる方法の詳細については、▶「ユーザ管理」の章を参照してください。

タッチコントローラのソフトウェアのアップグレードが必要な場合は、セットアップ手順の一部で新しいソフトウェアがデバイスからダウンロードされ、自動的にユニットにインストールされます。アップグレード後に再起動します。



コネクタパネルは
下部背面にあります。





電源
- 100 ～ 240 VAC
- 50/60 Hz

接点情報

タッチコントローラが正常にビデオ会議デバイスにペアリングされると、デバイスの名前またはアドレスがステータスバーに表示されます。

イーサネットコネクタはタッチコントローラの背面にあります。

[1] ネットワークインフラストラクチャが Power over Ethernet (PoE) を提供する場合、PoE インジェクタは必要ありません。タッチコントローラは PoE 規格のイーサネットケーブルで直接壁面のソケット (イーサネットスイッチ) に接続する必要があります。

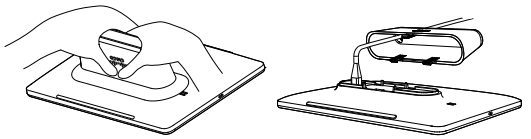
安全のために、PoE 電源はタッチコントローラと同じ建物内にある必要があります。PoE 規格のイーサネット ケーブルは最大 100m (330 フィート) です。

[2] サポートされているタッチコントローラ:Touch 10 (図を参照) と Room Navigator。

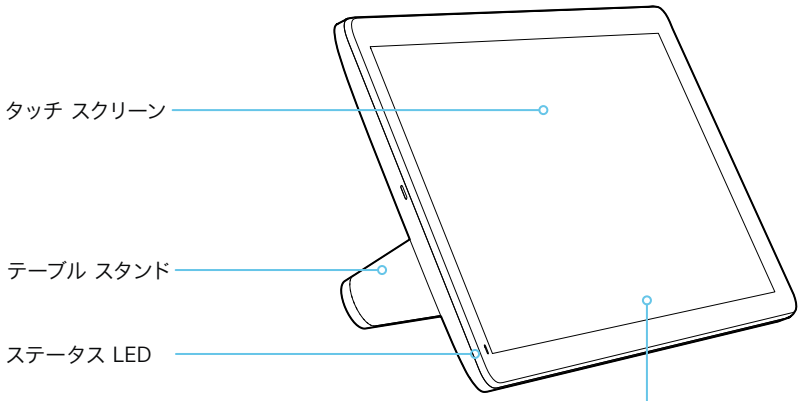
タッチコントローラの接続 (2/4 ページ)

Cisco Webex Room Navigator の物理インターフェイス

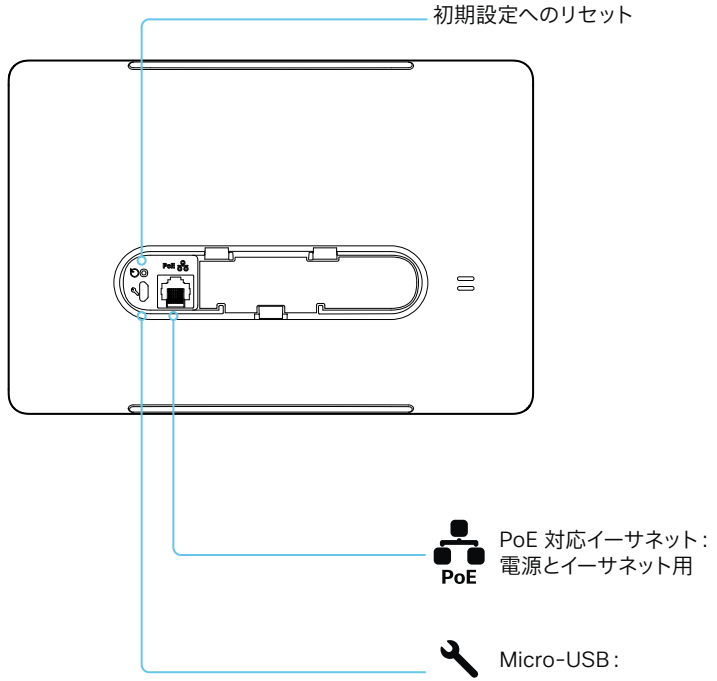
このタッチコントローラは、2021 年初めに発売されました。タッチコントローラは Touch 10 と同じ機能を備えていますが、電波品質や温度などをモニタリングするための環境センサーも提供しています。



コネクタパネルにアクセスするには、テーブルスタンドを取り外します。しっかりと押して回転させます。



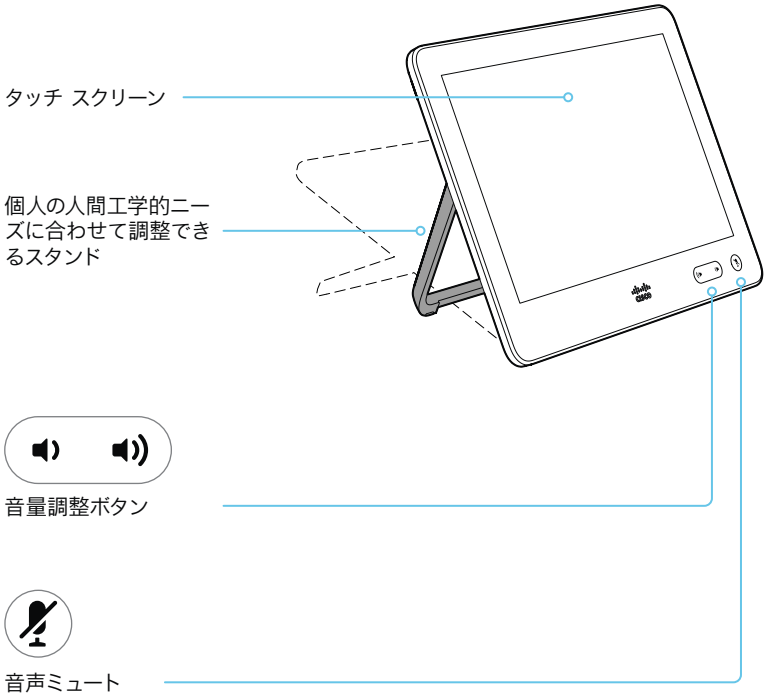
サウンドバーとオーディオミュートには、ユーザインターフェイスからアクセスできます。

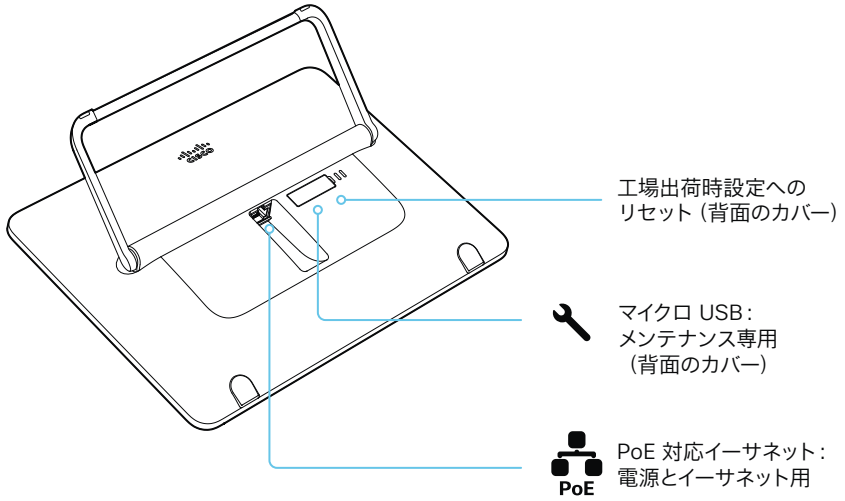


タッチコントローラの接続 (3/4 ページ)

Cisco Touch 10 の物理インターフェイス

これは、2017 年後半に発売されたバージョンの Touch 10 コントローラです。以前のバージョンと同じ機能を備えていますが、物理インターフェイスが多少異なります。新しいデバイスは、前面のロゴと、背面のコネクタが少ないことによって識別できます。

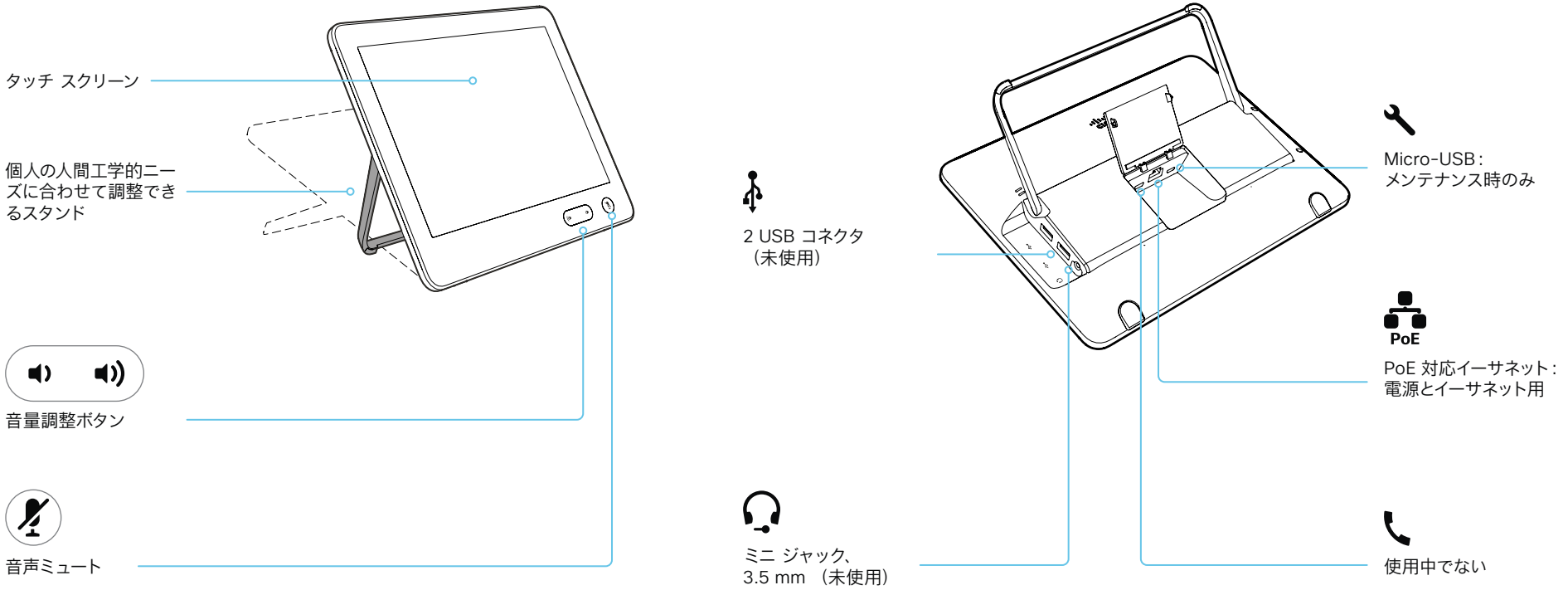




タッチコントローラの接続 (4/4 ページ)

Cisco TelePresence Touch 10 の物理インターフェイス

新しいバージョンの Touch 10 コントローラについては、前のページを参照してください。



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て、*[設定 (Settings)]* に移動します。*[音声とビデオ (Audio and Video)]* を選択し、*[すべての周辺機器 (All Peripherals)]* サブタブを開きます。

要件および制約事項:

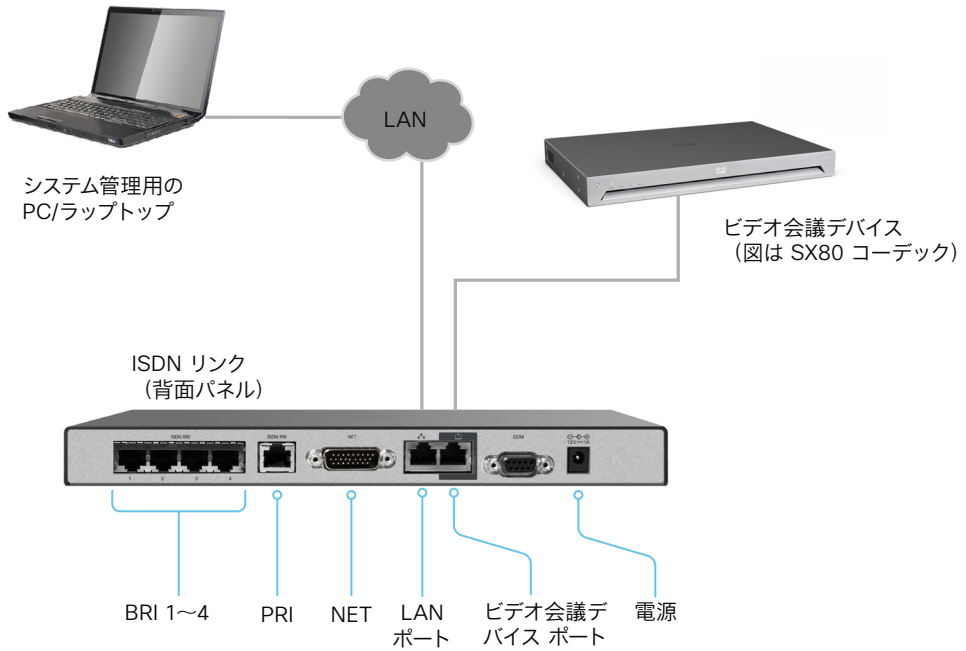
- ビデオ会議システムがタッチコントローラに接続されている必要があります
- ISDN リンクは、IL1.1.7 以降のソフトウェアを実行している必要があります。
- ISDN リンクと通信するために、ビデオ会議デバイスの Web インターフェイスまたは API で IPv6 を有効にする必要があります。
- 確実にインストールするために、ISDN リンクのインストール ガイドでネットワーク トポロジを確認してください。
- ビデオ会議デバイスと ISDN リンクが同じサブネット上にある必要があります。エンドポイントまたは ISDN リンクに新しい IP アドレスが割り当てられている場合は、そ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 Web 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



第 4 章

メンテナンス

新しいソフトウェアのインストール

CE9.13 以降へのアップグレードまたは CE9.13 以降からのダウングレード

アップグレードやダウングレードでは、特定の状況によって設定が失われる可能性があることに注意してください。

CE9.13 以降へのアップグレードまたは CE9.13 以降からのダウングレードを行うと、インストールするバージョンに存在しない設定はすべて削除されます。後で以前のソフトウェアバージョンに戻そうとしても、削除された設定にはデフォルト値が割り当てられます。

ソフトウェアイメージのファイル形式

PKG ファイルと COP ファイルについて

Boards、Desk Pro、および Room シリーズ：ビデオデバイスと周辺機器のソフトウェアイメージは別々の PKG ファイルになっています。

そのため、これらのデバイスをアップグレードする場合は COP ファイルを使用する必要があります。COP ファイルには、ビデオデバイスおよび周辺機器に必要な PKG ファイルと、COP ファイルの内容を示す *loads* ファイルが含まれています。

SX シリーズ、MX シリーズ、および DX：ビデオデバイスの PKG ファイルには、デバイス自体のソフトウェアイメージと、関連する周辺機器のソフトウェアイメージの両方が含まれています。

CUCM からのアップグレード

デバイスのアップグレードには COP ファイルを使用します。

Board、Desk Pro、および Room シリーズ：これらのデバイスをアップグレードする場合は、*loads* ファイルを使用してソフトウェアを指定する必要があります。ビデオデバイスの PKG ファイルでは周辺機器がアップグレードされないため、ビデオデバイスの PKG ファイルだけを使用することはできません。

SX シリーズ、MX シリーズ、および DX：これらのデバイスをアップグレードする場合は、PKG ファイルを使用してソフトウェアを指定できます。これらの PKG ファイルには周辺機器のソフトウェアも含まれています。

TMS またはデバイスの Web インターフェイスからのアップグレード：

Board、Desk Pro、および Room シリーズ：これらのデバイスをアップグレードする場合は、COP ファイルを使用します。ビデオデバイスの PKG ファイルには周辺機器のソフトウェアイメージが含まれていないため、ビデオデバイスの PKG ファイルだけを使用することはできません。

SX シリーズ、MX シリーズ、および DX：これらのデバイスをアップグレードする場合は、PKG ファイルを使用できます。これらの PKG ファイルには周辺機器のソフトウェアも含まれています。

新しいソフトウェアのインストール (2/2 ページ)

Web インターフェイスにサインインして、*[ソフトウェア (Software)]* に移動し、*[ソフトウェアアップグレード (Software Upgrade)]* を選択します。

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。Cisco Download Software ウェブ ページにアクセスし、お使いの製品のページにアクセスします。 ▶https://software.cisco.com/download/home

ファイル名フォーマットは：
“cmterm-s53200ce9_15_x_z.k3.cop.sgn”

ここで、「x」はマイナーリリース番号、「z」はビルド番号です。

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/ja_jp/support/collaboration-endpoints/spark-board/tsd-products-support-series-home.html

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 .cop.sgn ファイルです。ファイル名は変更しないでください。

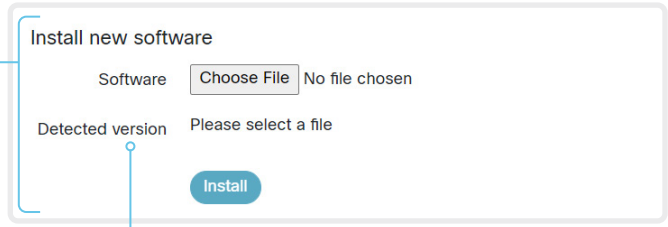
1. *[ファイルの選択 (Choose File)]* をクリックし、新しいソフトウェアを含む .cop.sgn ファイルを見つけます。

   ソフトウェアのバージョンが検出され、表示されます。

2. [インストール (Install)] 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。

クラウド管理ソフトウェアのアップグレード

お使いのデバイスが Webex Edge for Devices にリンクされている場合、Webex クラウドサービスからソフトウェアをアップグレードできます。次に、クラウドから新しい RoomOS ソフトウェアバージョンが利用可能になるとすぐに、デバイスが自動的にアップグレードされます。

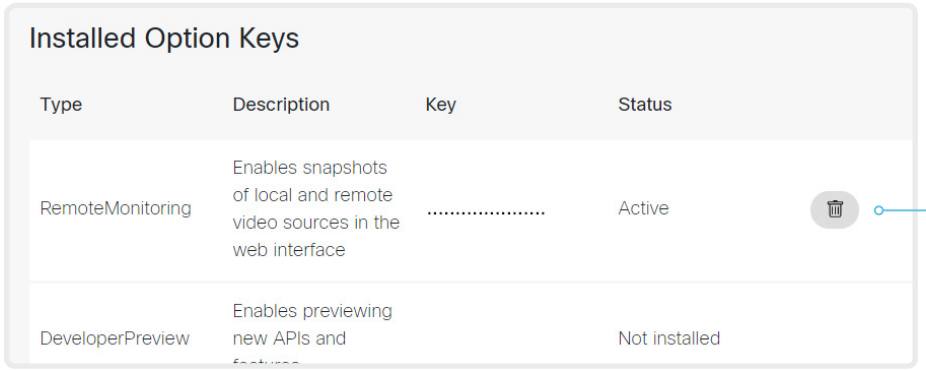
詳細については、Webex ヘルプセンターの ▶Webex Edge for Devices のクラウド管理ソフトウェアアップグレード (https://help.webex.com/naspqfz/) に関する記事を参照してください。

オプションキーの追加

Web インターフェイスにサインインして、*[ソフトウェア (Software)]* に移動し、*[オプションキー (Option Keys)]* を選択します。

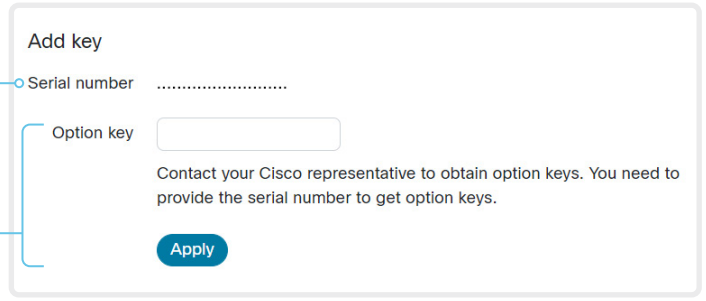
すべてのオプション キーのリストと、デバイスにインストールされていないオプション キーのリストが表示されます。

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、シスコの担当者にお問い合わせください。



オプションキーのアンインストール

削除ボタンをクリックして、オプションキーをアンインストールします。



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. [適用 (Apply)] をクリックしてオプションキーを追加します。

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

Web インターフェイスにサインインして、*[ホーム (Home)]* を選択します。

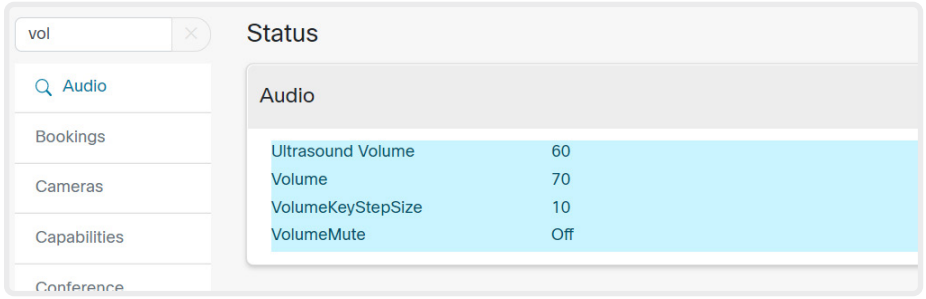
これは、IP アドレス、MAC アドレス、シリアル番号、アクティブネットワークインターフェイス、ソフトウェアバージョン、問題、登録ステータスなどの一般的な情報を示す *[システム情報 (System Information)]* ページです。

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て、*[設定 (Settings)]* に移動し、*[ステータス (Statuses)]* を選択します*。

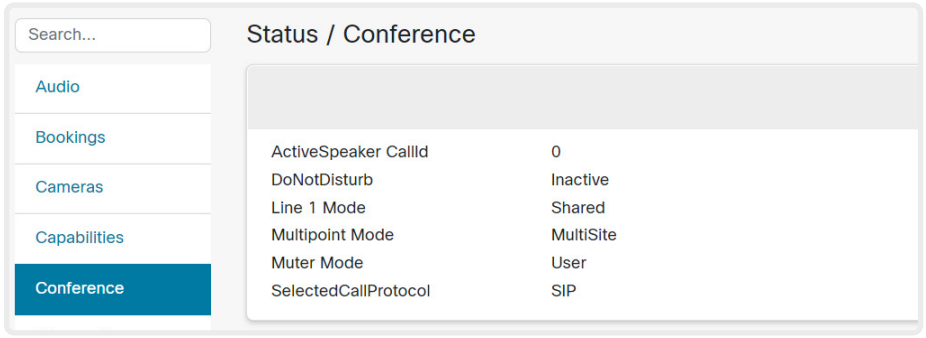
ステータス エントリを検索する

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

Web インターフェイスにサインインして、*[問題と診断 (Issues and Diagnostics)]* に移動し、*[問題 (Issues)]* を選択します。

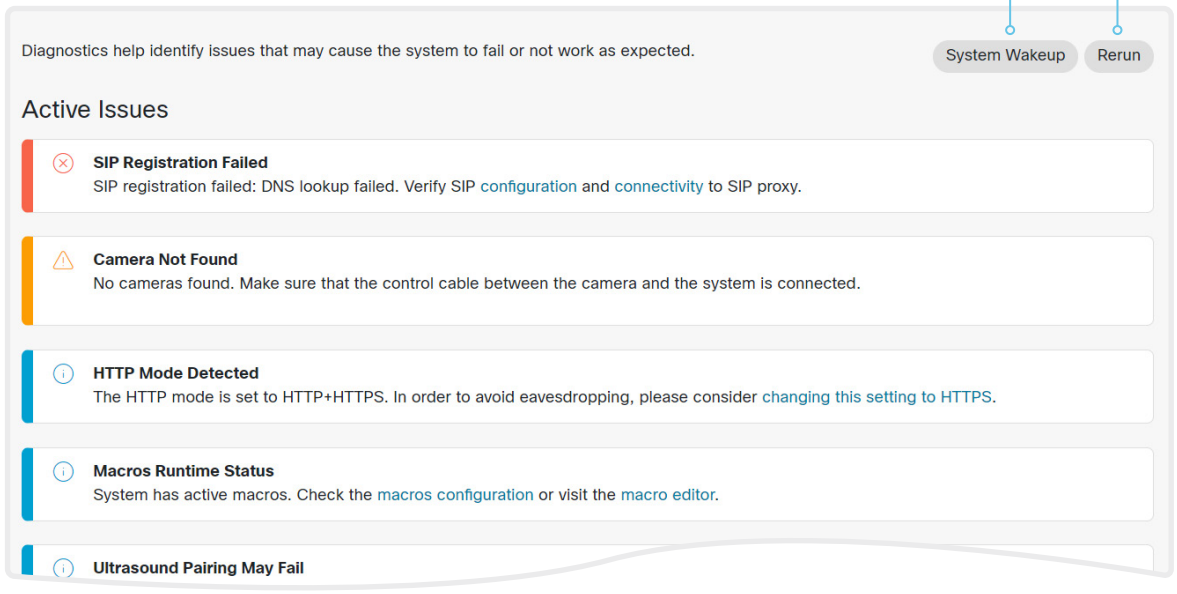
アクティブな問題のリスト*が表示されます。エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

診断の実行

[再実行 (Rerun)] をクリックして、リストが最新であることを確認します。

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 (System Wakeup)]* をクリックします。

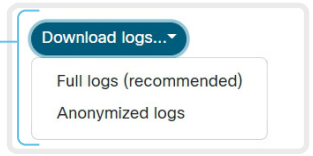


* 図に示している問題は一例です。お使いのデバイスでは表示される情報が異なります。

ログファイルのダウンロード

Web インターフェイスにサインインして、*[問題と診断 (Issues and Diagnostics)]* に移動し、*[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



[システムログ (System Logs)] カードを見つけて、*[ログのダウンロード... (Download logs...)]* をクリックします。。

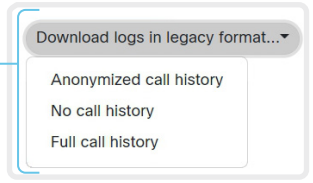
[完全なログ (Full logs)] をダウンロードするか、または *[匿名化されたログ (Anonymized logs)]* をダウンロードするかを選択します。

指示に従ってファイルを保存します。

個人を特定できる情報 (PII) は、匿名化されたログで「*プライバシー保護のために削除されました*」というメモに置き換えられます。サポートケースに匿名化されたログを添付すると、問題の解決に必要な時間が長くなる場合があります。

すべてのログファイルをダウンロードする (従来の形式)

非推奨

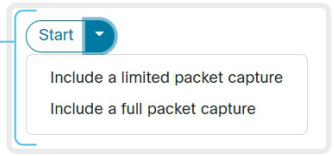


[システムログ (System Logs)] カードを見つけて、*[従来の形式でログをダウンロード... (Download logs in legacy format...)]* をクリックします。。

ログファイルに完全な通話履歴 (匿名以外の発信側/着信側) 、匿名化された通話履歴を含めるかどうか、または通話履歴をまったく含めないかを選択します。

指示に従ってファイルを保存します。

拡張ロギングを開始する



[拡張ロギング (Extended Logging)] カードを見つけて、*[開始 (Start)]* 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、*[停止 (Stop)]* をクリックします。

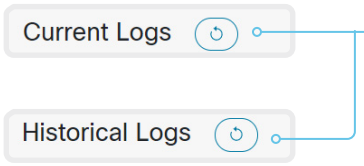
デフォルトとして、ネットワーク トラフィックはキャプチャされません。ネットワーク トラフィックの一部または全部のキャプチャを含めるには、ドロップダウン メニューを使用します。

ログファイルを開くまたは保存する

*現在のログファイル*をクリックして、ログファイルを Web ブラウザで開き、右クリックしてファイルをコンピュータに保存します。

*履歴ログファイル*をクリックし、指示に従ってファイルをコンピュータに保存します。

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、シスコのサポートから要求されることがあるシスコ固有のデバッグ 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。

ログファイルの形式

CE9.15.0 では、クラウドに登録されたデバイスに使用される形式に合った新しいログファイル形式が導入されました。

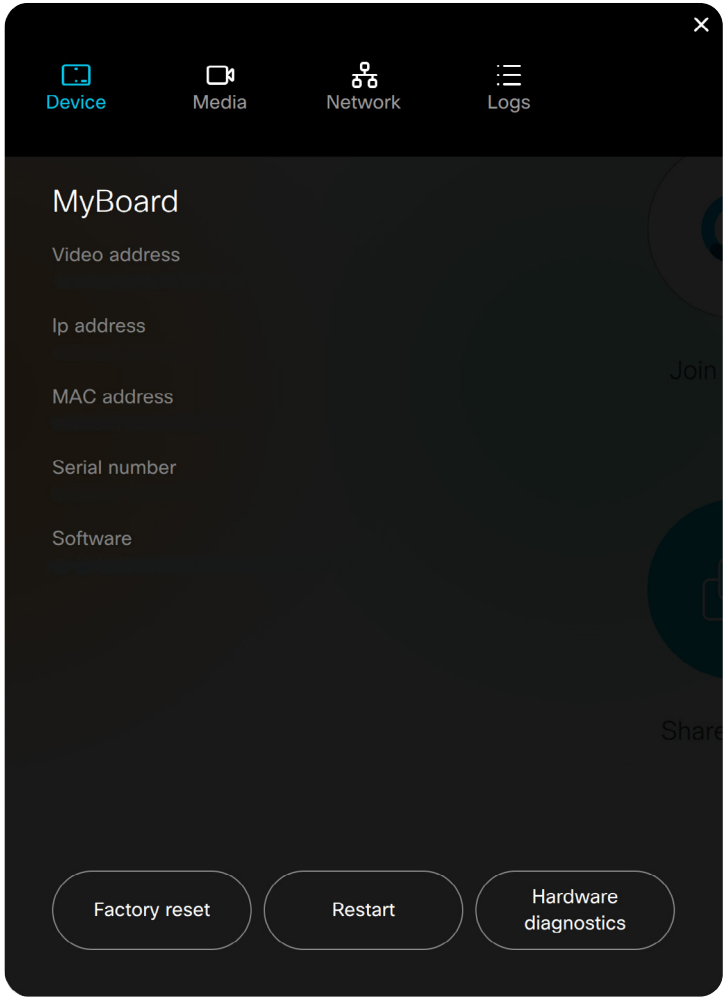
従来の形式ではなく、新しいファイル形式を使用してログをダウンロードすることをお勧めします。

テクニカルサポート画面へのアクセス

テクニカルサポート画面にアクセスするには、画面に 1 本の指を置いたまま [ホーム (Home)] ボタンを 3 回タップします。

テクニカルサポート画面から次の情報にアクセスできます。

- 機器情報
- メディア統計情報
- ネットワーク情報および診断
- ハードウェア診断 (マイクのレベル、タッチスクリーン、ベストオーバービュー、およびカメラ)
- ログ
- ボードの再起動
- 工場出荷時の状態へのリセット



リモート サポート ユーザを作成する

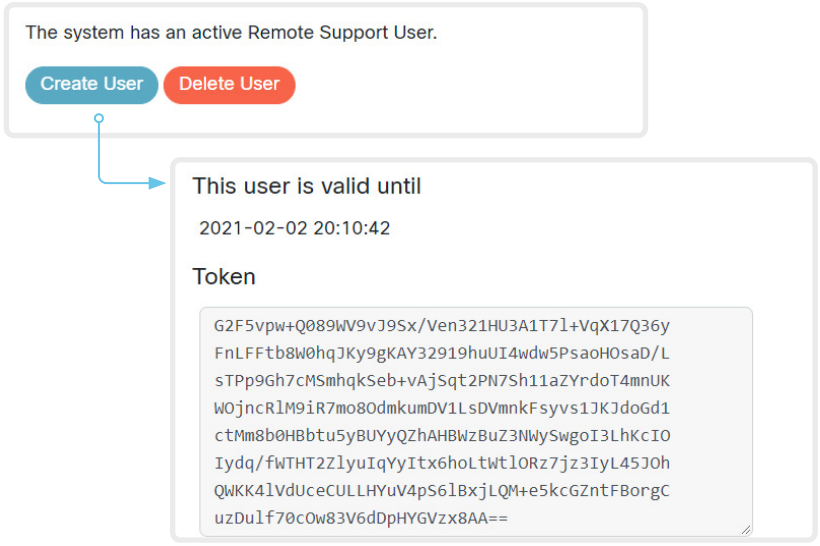
Web インターフェイスにサインインして、*[ユーザ (Users)] に移動します*。

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. *[リモートサポートユーザ (Remote Support User)]* カードを見つけて、*[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] 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) の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

Web インターフェイスにサインインして、*[バックアップとリカバリ (Backup and Recovery)]* 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 (Backup)]* を選択します。
2. バックアップ ファイルに含める要素を選択します。
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. *[ダウンロード (Download)]* 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. *[復元 (Restore)]* を選択します。
2. *[ファイルの選択 (Choose File)]* 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. *[アップロード (Upload)]* 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/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 Administration* 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 Administration* 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 : <hostname>:<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. Web インターフェイスにサインインして、*[バックアップとリカバリ (Backup and Recovery)]* に移動し、*[復元 (Restore)]* を選択します。
2. *[ファイルの選択 (Choose File)]* をクリックし、チェックサムを計算するファイルを見つけます。

   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/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。

```
<コマンド>
 <プロビジョニング>
    <サービス>
     <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
     </Fetch>
    </サービス>
 </プロビジョニング>
</コマンド>
```

   上記コマンドで、下記のように適用します。

   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、*[システムに設定 (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. Web インターフェイスにサインインして、*[バックアップとリカバリ (Backup and Recovery)]* に移動し、*[復元 (Restore)]* を選択します。
2. *[ファイルの選択 (Choose File)]* をクリックし、チェックサムを計算するファイルを見つけます。

   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への復元

Web インターフェイスにサインインして、*[バックアップとリカバリ (Backup and Recovery)]* に移動し、*[システムリカバリ (System Recovery)]* を選択します。

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。

ログファイルのバックアップ

1. *[問題と診断 (Issues and Diagnostics)]* に移動し、*[システムログ (System Logs)]* 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。

設定とカスタム要素のバックアップ

1. *[バックアップとリカバリ (Backup and Recovery)]* に移動し、*[バックアップ (Backup)]* を選択します。
2. *[ダウンロード (Download)]* 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。

以前に使用していたソフトウェアイメージへの復元

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. *[システムリカバリ (System Recovery)]* を選択します。
2. *[ソフトウェア回復交換 (Software Recovery Swap)]* カードを見つけて、*[ソフトウェアの交換 (Swap software)]* をクリックします。
3. *[Confirm (確認)]* をクリックして続行します。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

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。上記インターフェイスが利用できない場合は、 ピンホールリセットを利用します。

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、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 (2/3 ページ)

Web 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。

Web インターフェイスにサインインして、*[バックアップとリカバリ (Backup and Recovery)]* に移動し、*[システムリカバリ (System Recovery)]* を選択します。

1. *[初期設定へのリセット (Factory Reset)]* カードを見つけて、表示される情報を注意深く読みます。
2. *[工場出荷時の初期状態へのリセット (Reset to Factory Defaults)]* をクリックします。
3. *[初期設定へのリセット (Factory Reset)]* をクリックして選択内容を確認します。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。
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。

テクニカルサポート画面からの工場出荷時設定へのリセット

工場出荷時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と設定をバックアップすることをお勧めします。

1. テクニカルサポート画面にアクセスするには、ボードの画面に 1 本の指を置いたままホームボタンを 3 回押します。
2. *[工場出荷時設定へのリセット (Factory reset)]* を選択します。
3. *[リセット (Reset)]* を選択して確定します。または、操作をやめる場合は *[キャンセル (Cancel)]* を選択します。
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. 選択を確定するには*[リセット (reset)]*を選択し、リセットを中止する場合は *[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。

ログファイルのバックアップ

1. *[問題と診断 (Issues and Diagnostics)]* に移動し、*[システムログ (System Logs)]* 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。

設定とカスタム要素のバックアップ

1. *[バックアップとリカバリ (Backup and Recovery)]* に移動し、*[バックアップ (Backup)]* を選択します。
2. *[ダウンロード (Download)]*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。

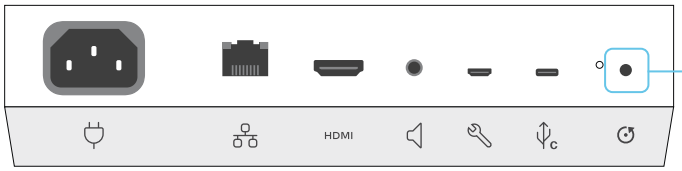
ビデオ会議デバイスの初期設定へのリセット (3/3 ページ)

リセット ボタンを使用して工場出荷時設定にリセットする

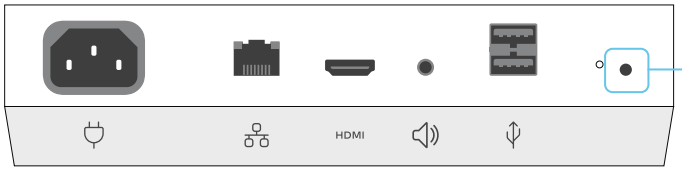
初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

1. コネクタパネルにあるリセットボタン (ピンホール) の位置を確認します。
2. ペーパークリップ (または同等のもの) を使用して、画面が黒くなるまでリセット ボタンを押し続けます (約 10 秒) 。その後、ボタンを離します。
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。

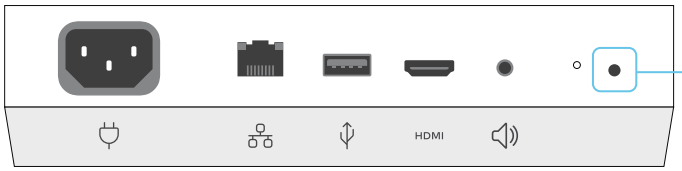
   デバイスが正常に初期設定にリセットされると、セットアップアシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。



Webex Board 55S、70S、および 85S



Webex Board 55



Webex Board 70

リセット ボタン

ボタンは引っ込めて取り付けられているため、使用がかなり難しい場合があります。ボタンを押すと、ボタンが下がる感覚がわかります。

Cisco Webex Room Navigator の初期設定へのリセット

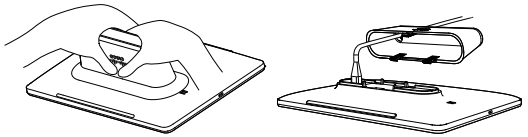
エラー状態で、接続を再確立するためにタッチコントローラを工場出荷時設定にリセットすることが必要になる場合があります。

タッチコントローラを初期設定にリセットすると、ペアリング情報が失われ、（ビデオ会議デバイスではなく）タッチコントローラ自体がデフォルトの初期設定に戻ります。

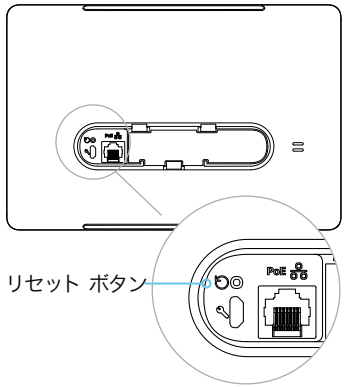
初期設定にリセットすると元に戻すことはできません。

1. 脚を取り外して、コネクタパネルのリセットボタン（ピンホール）を見つけます。
2. ペーパークリップ（または同等のもの）を使用して、画面が黒くなるまでリセット ボタンを押し続けます（約 10 秒）。その後、ボタンを離します。
3. Room Navigator 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、Room Navigator が自動的に再起動します。数分かかることがあります。

   Room Navigator を改めてビデオ会議デバイスとペアリングする必要があります。ペアリングが成功すると、デバイスから新しい設定を自動的に受信します。



しっかりと押して回転させ、テーブルスタンドを取り外します。



Room Navigator のビデオ会議デバイスへの接続方法およびペアリングについて

Room Navigator を使用するには、LAN を経由してビデオ会議デバイスにペアリングする必要があります（リモートペアリング）。

Room Navigator のビデオ会議デバイスへの接続方法およびペアリングについては、▶「タッチコントローラの接続」の章を参照してください。

Cisco Touch 10 の初期設定へのリセット

この章は、2017 年後半に発売された Touch 10 コントローラ (Cisco Touch 10) に適用されます。 このデバイスは、前面のロゴ、および背面のコネクタが少ないことによって識別されます。

古いバージョンについては、次のページを参照してください。

エラー状態で、接続を再確立するためにタッチコントローラを工場出荷時設定にリセットすることが必要になる場合があります。

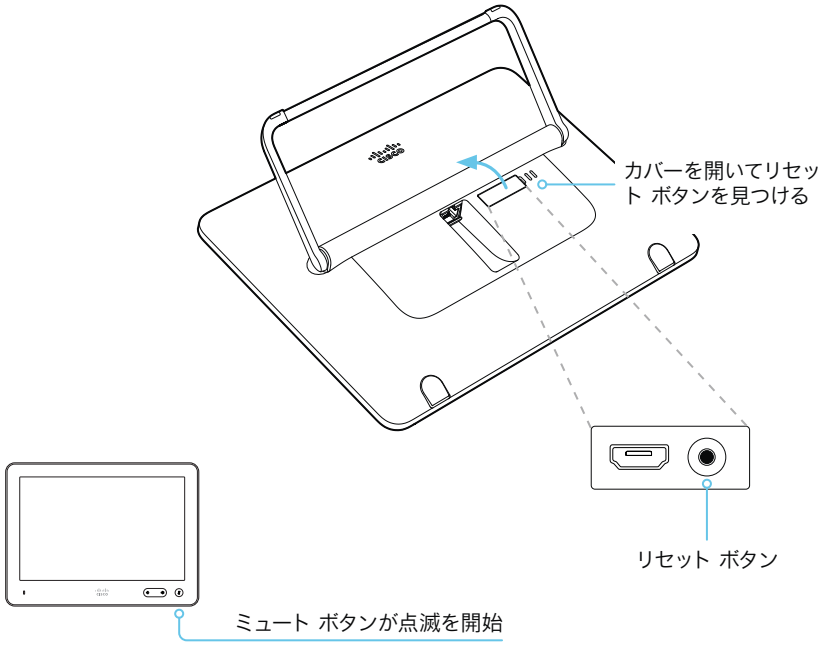
タッチコントローラを初期設定にリセットすると、ペアリング情報が失われ、(ビデオ会議デバイスではなく) タッチコントローラ自体がデフォルトの初期設定に戻ります。

初期設定にリセットすると元に戻すことはできません。

1. 背面の小さなカバーを開き、リセット ボタンを見つけます。
2. 前面のミュート ボタンが点滅し始めるまでリセット ボタンを押し続けます (約 5 秒間)。その後、ボタンを離します。

   Touch 10 が工場出荷時設定へと自動的に戻され、再起動されます。

   Touch 10 は改めてビデオ会議デバイスとペアリングする必要があります。ペアリングが成功すると、デバイスから新しい設定を自動的に受信します。



ペアリングおよびビデオ会議デバイスと Touch 10 の接続方法について

Touch 10 コントローラを使用するには、LAN 経由でビデオ会議デバイスとペアリング (リモートペアリング) する必要があります。

Touch 10 とビデオ会議デバイスの接続方法およびペアリングについては、▶ 「タッチコントローラの接続」の章を参照してください。

Cisco TelePresence Touch 10 の初期設定へのリセット

この章は、最初の Touch 10 コントローラ (Cisco TelePresence Touch 10) に適用されます。 このデバイスには前面のロゴはありません。

2017 年後半に発売された新しいバージョンについては、前のページを参照してください。

エラー状態で、接続を再確立するためにタッチコントローラを工場出荷時設定にリセットすることが必要になる場合があります。

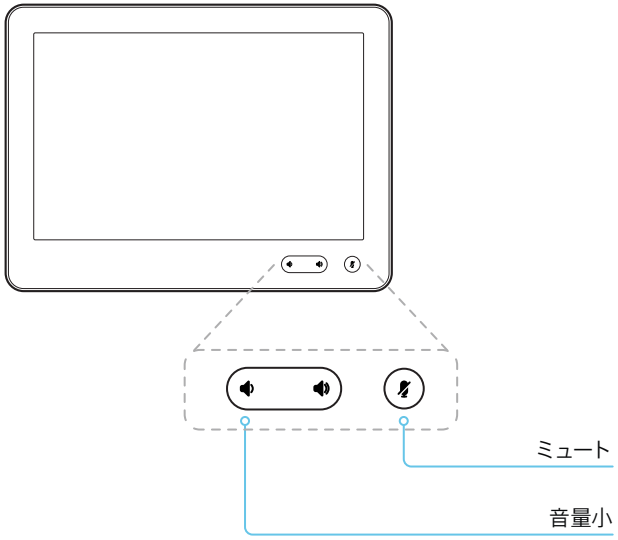
タッチコントローラを初期設定にリセットすると、ペアリング情報が失われ、(ビデオ会議デバイスではなく) タッチコントローラ自体がデフォルトの初期設定に戻ります。

初期設定にリセットすると元に戻すことはできません。

1. *ミュート*および*音量小*ボタンを見つけます。
2. (赤と緑が) 点滅しはじめるまで、*ミュート* ボタンを押します。約 10 秒かかります。
3. 音量小ボタンを 2 回押します。

   Touch 10 が工場出荷時設定へと自動的に戻され、再起動されます。

   Touch 10 は改めてビデオ会議デバイスとペアリングする必要があります。ペアリングが成功すると、デバイスから新しい設定を自動的に受信します。



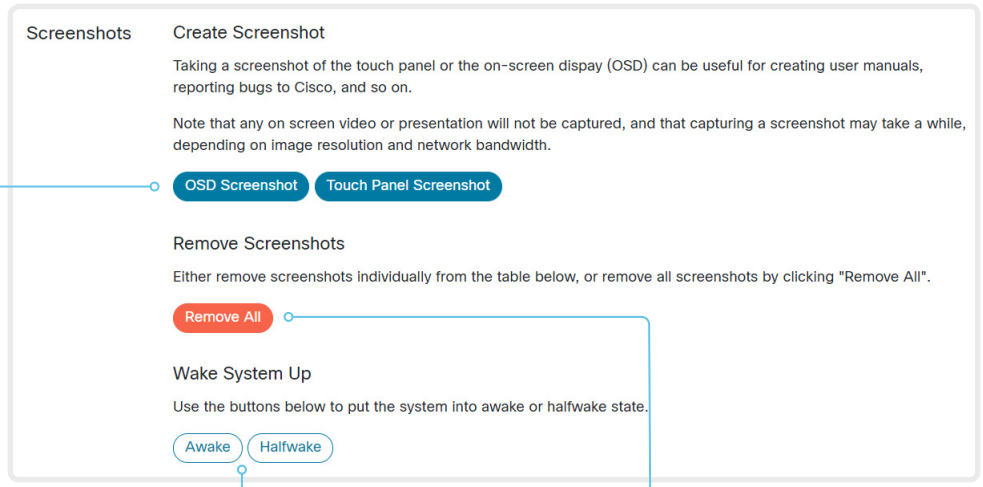
ペアリングおよびビデオ会議デバイスと Touch 10 の接続方法について

Touch 10 コントローラを使用するには、LAN 経由でビデオ会議デバイスとペアリング (リモートペアリング) する必要があります。

Touch 10 とビデオ会議デバイスの接続方法およびペアリングについては、▶ 「タッチコントローラの接続」の章を参照してください。

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

Web インターフェイスにサインインして、*[問題と診断 (Issues and Diagnostics)]* に移動し、*[ユーザインターフェイスのスクリーンショット (User Interface Screenshots)]* を選択します。



スクリーンショットのキャプチャ

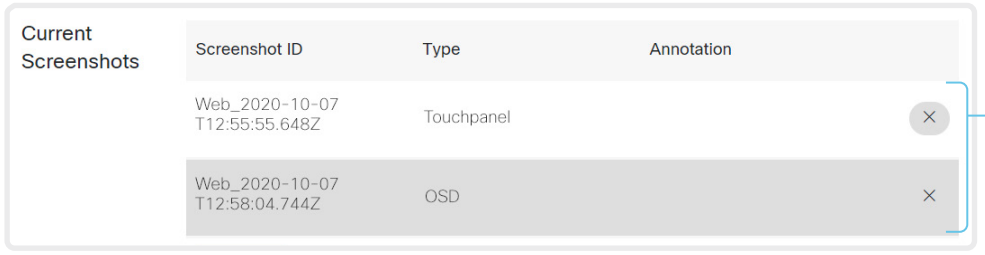
タッチコントローラのスクリーンショットをキャプチャするには、*[タッチパネルのスクリーンショット (Touch Panel Screenshot)]* をクリックします。メイン画面 (オンスクリーンディスプレイ) のスクリーンショットをキャプチャするには、*[OSD のスクリーンショット (OSD screenshot)]* をクリックします。

スクリーンショットは *[現在のスクリーンショット (Current Screenshots)]* カードの下に表示されます。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。

キャプチャされたスクリーンショットはすべて、*[現在のスクリーンショット (Current Screenshots)]* カードに一覧表示されます。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。

デバイスの復帰

スタンバイからデバイスを復帰するには、次のボタンを使用します。



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

デバイスに接続されているタッチコントローラのスクリーンショットや、メニュー、インジケータ、メッセージを含むメイン画面 (*オンスクリーンディスプレイ*とも呼ばれる) のスクリーンショットを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

次のページでは、デバイス設定の完全なリストを確認できます。これらは Web インターフェイスから設定できます。

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。*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

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。

ソフトウェアバージョン : CE9.15.3　　製品 : Board

オーディオ設定

オーディオ デフォルト音量

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: 70

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。

オーディオ キークリック検出 減衰

デバイスがキーボードからのクリック ノイズを検出し、マイク信号を自動的に減衰させることができます。キー入力のノイズが他の参加者の邪魔をする可能性があるため、会議出席者がキーボードで入力を開始するときにはこの機能が便利です。参加者がキーボードで入力しながら話す場合、マイクの信号は減衰しません。[オーディオ キー クリック ディテクタ有効化 (Audio KeyClickDetector Enabled)] 設定が On 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、INTEGRATOR、USER

デフォルト値 : True

値スペース : False/True

False : マイクの信号の減衰は無効です。

True : キーボードのクリック ノイズが検出された場合、デバイスによりマイクの信号が減衰されます。音声または音声とキーボードのクリックが併せて検出された場合、マイクの信号は減衰されません。

オーディオ キークリック検出 有効

デバイスがキーボードからのクリック ノイズを検出し、マイク信号を自動的に減衰させることができます。キー入力のノイズが他の参加者の邪魔をする可能性があるため、会議出席者がキーボードで入力を開始するときにはこの機能が便利です。マイクの信号の減衰を有効にするには、[オーディオ キー クリック ディテクタ減衰 (Audio KeyClickDetector Attenuate)]を On にします。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : True

値スペース : False/True

False : キー クリックの検出は無効です。

True : デバイスによりキーボードからクリック ノイズが検出されます。

オーディオ マイク ノイズ除去 モード

この設定は、デバイスのノイズ除去機能をオン/オフにするために使用されます。

これが無効になっていると、オプションはユーザインターフェイスに表示されません。また、xAPI を介して設定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 : Manual

値スペース : Disabled/Manual

オーディオ サウンドとアラート 着信音

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 : 波 (Waves)

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。

オーディオ サウンドとアラート 着信音量

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。

オーディオ 超音波 モード

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 : スタティック (Static)

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 超音波 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 : シスコが助言した場合にのみ使用してください。

オーディオ 超音波 最大音量

この設定は、Intelligent Proximity 機能に適用されます。超音波ペアリングメッセージの最大音量を設定します。

[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定と [プロキシミティ モード (Proximity Mode)] 設定は、超音波ペアリングメッセージにのみ影響します。超音波を使用した人の存在の検出とモーション検知については、[ルーム分析 人の存在の検出 (RoomAnalytics PeoplePresenceDetector)] 設定および [スタンバイ モーション検知ウェイクアップ (Standby WakeupOnMotionDetection)] 設定を参照してください。

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、超音波ペアリングメッセージは出力されません。

BYOD 設定

BYOD タッチ転送 有効

この設定を使用すると、タッチリダイレクト機能を有効または無効にすることができます。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 ケーブルによって Board に接続する必要があります。ボードからラップトップへの接続には、USB-C - USB-C ケーブルまたは USB-C - USB-A ケーブルを使用できます。

この機能は第 1 世代のボード（Webex Board 55 および 70、S シリーズ以外）では使用できないことにも注意してください。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値：True

値スペース：False/True

False：タッチ リダイレクトが無効になります。

True：タッチ リダイレクトが有効になります。

通話履歴設定

通話履歴モード

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指定します（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

カメラ スピーカートラック モード

スピーカートラックは自動カメラ フレーミングを使用し、室内の人数に基づいて最適なカメラ表示を選択します。カメラは、通話中のスピーカーのクローズアップを検索してキャプチャするオーディオ トラッキング技術を使用します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Off

自動: Best Overview がオンになっています。デバイスが室内の人々を検出して自動的に最適なカメラフレーミングを選択します。ユーザは、タッチコントローラのカメラのコントロールパネルでベストオーバービューのオンとオフを即座に切り替えることができますが、各コールの後は、次のユーザに備えて機能が再度オンになります。

オフ: Best Overview がオフになっています。

カメラ スピーカートラック クローズアップ

カメラの SpeakerTrack モードが [自動 (Auto)] に設定されている場合のみ、この設定が適用されます。

クローズアップ機能をオンにすると、人が話していることがデバイスによって検出され、その人が映るように最適なフレーミングが選択されます。これはクローズ アップといい、室内のすべての人を含まない場合があります。室内のすべての人を常に表示しておきたい場合、クローズ アップ機能をオフにできます。

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/Off/On

Auto : デバイスは、室内のすべての人を常にカメラのフレーム内に含めます。

Off : デバイスは、室内のすべての人が常にカメラのフレームに入るように維持されます。

On : デバイスは、話している人にズームインします。

会議設定

会議 アクティブ コントロール モード

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。

会議 自動応答 モード

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、会議 自動応答 遅延設定を使用し、コールに応答するときにマイクをミュートする場合は会議自動応答のミュート設定を使用します。

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 : タッチコントローラで [応答 (Answer)] をタップし、着信コールに手動で応答できます。

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。

会議自動応答のミュート

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。[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 : 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。

会議 自動応答 遅延

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) 。

会議 通信プロトコルIPスタック

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。

会議 デフォルト コール プロトコル

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。

会議 デフォルトコール レート

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

デフォルト値 : 10000

値スペース : 整数 (64 ～ 10000)

デフォルト コール レート (kbps) です。

会議 応答不可 デフォルトタイムアウト

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) 。

会議 暗号化 モード

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。

会議 遠端制御 モード

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。

会議 遠端制御 信号機能

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無効にします。

On : 遠端制御信号機能を有効にします。

会議 遠端メッセージ モード

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。

会議 最大受信コールレート

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、会議 最大合計受信コールレート設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : 10000

値スペース : 整数 (64 ～ 10000)

最大受信帯域 (kbps) 。

会議 最大転送コールレート

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、会議 最大合計転送コールレート設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大送信帯域 (kbps) 。

会議 最大合計受信コールレート

この設定は、デバイスに搭載された MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

受信全体の最大許容ビット レートを定義します。ビット レートは任意の時点におけるすべてのアクティブ コール間で均等に分割されます。これは、誰かがマルチポイント会議に参加または退出するとき、またはコールが保留 (中断) されるか再開されるときに個々のコールが適切に高速化または低速化されることを意味します。

個々のコールの最大受信ビット レートは、会議 最大受信コールレート設定により定義されます。

必要なユーザ ロール : ADMIN

デフォルト値 : 10000

値スペース : 整数 (64 ～ 10000)

最大受信帯域 (kbps) 。

会議 最大合計転送コールレート

この設定は、デバイスに搭載された MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

送信全体の最大許容ビット レートを定義します。ビット レートは任意の時点におけるすべてのアクティブ コール間で均等に分割されます。これは、誰かがマルチポイント会議に参加または退出するとき、またはコールが保留 (中断) されるか再開されるときに個々のコールが適切に高速化または低速化されることを意味します。

個々のコールの最大送信ビット レートは、会議 最大転送コールレート設定により定義されます。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大送信帯域 (kbps) 。

会議 切断時のマイクのミュート解除 モード

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。

会議 マルチポイント モード

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。ローカルのリソースのみに依存する組み込みの MultiSite 機能と、集中型のインフラストラクチャ (マルチポイント コントロール ユニット : MCU) をベースとする別のソリューションの両方を使用することができます。

MultiSite 機能はアップグレードオプションであり、すべてのデバイスで使用できるとは限りません。デバイスには、MultiSite オプション キーをインストールする必要があります。

Cisco TelePresence Video Communication Server (VCS) に登録されている場合、デバイスは他のビデオデバイスを呼び出す場合に MultiSite を使用できます。Cisco Unified Communications Manager (CUCM) バージョン 8.6.2 以降に登録されている場合、デバイスは、CUCM 会議ブリッジ、またはデバイス内蔵の MultiSite 機能を使用できます。使用するオプションは CUCM によってセットアップされます。

いずれの場合も、デバイスが会議に参加者を追加できるように MCU を呼び出す場合、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 (直接リモート追加) 。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/CUCMMediaResourceGroupList/MultiSite/Off

Auto : マルチ ポイント メソッドが自動的に選択されます。

MultiSite オプション キーをデバイスにインストールして、他のビデオ デバイス (MCU 以外) を呼び出す場合、マルチ パーティ会議は、組み込みの MultiSite 機能を使ってセットアップされます。参加者を追加できるのは MultiSite のホストのみです。これにより、カスケード会議ができなくなります。デバイスに MultiSite オプション キーがない場合、複数のビデオ デバイスをビデオで呼び出すことはできません。音声のみの参加者を 1 人追加できます。

MultiSite オプション キーに関係なく、デバイスが会議に参加者を追加する (Direct Remote Add) MCU を呼び出す場合、MCU を介してマルチ パーティ会議をセットアップすることができます。

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。

MultiSite : デバイスに MultiSite オプション キーがインストールされている場合は、組み込み MultiSite 機能を使ってマルチ パーティ会議がセットアップします。デバイスに MultiSite オプション キーがない場合、複数のデバイスをビデオでコールすることはできません。音声のみのデバイスを 1 つ追加できます。

Off : 複数のデバイスをビデオでコールすることはできませんが、音声のみのデバイスを追加することができます。デバイスが会議に参加者を追加できるように MCU を呼び出す場合、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 (直接リモート追加) 。

会議 着信マルチサイトコール モード

すでにコール中または会議中の場合に着信コールを許可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：Allow

値スペース：Allow/Deny

Allow：すでに通話している間に、誰かが電話をかけてきた場合、通知されます。着信コールを受け入れるかどうかは任意です。着信コールに応答している間、進行中のコールを保留しておくこともできますし、それらのコールをマージすることもできます（マルチパーティ ビデオ会議をサポートしている必要があります）。

Deny：すでに通話中の場合、着信コールは拒否されます。着信コールについては通知されません。ただし、コール履歴リストの不在履歴として表示されます。

会議 プレゼンテーション 保留時の動作

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。

会議プレゼンテーションのリレー品質

この設定は、搭載された MultiSite 機能（オプション）を使用してマルチポイント ビデオ会議をホストするデバイスに適用されます。リモート ユーザがプレゼンテーションを共有している場合、デバイスがプレゼンテーションのトランスコーディングを行い、それをマルチポイント会議の他の参加者に送信します。[リレー品質（RelayQuality）] 設定は、プレゼンテーション ソースに対して、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

デフォルト値：Sharpness

値スペース：Motion/Sharpness

Motion：できるだけ高いフレーム レートにします。高いフレーム レートが必要な場合に使用します（通常、画像の動きが激しい場合）。

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。

ファシリティサービス設定

ファシリティサービス サービス [n] タイプ

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、ファシリティサービス サービス [n] 名前とファシリティサービス サービス [n] 番号の両方の設定が正しく設定されていないと使用できません。ファシリティ 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。

ファシリティサービス サービス [n] 名前

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、ファシリティサービス サービス [n] 名前とファシリティサービス サービス [n] 番号の両方の設定が正しく設定されていないと使用できません。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。ファシリティ 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。

ファシリティサービス サービス [n] 番号

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、ファシリティサービス サービス [n] 名前とファシリティサービス サービス [n] 番号の両方の設定が正しく設定されていないと使用できません。ファシリティ 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) 。

ファシリティサービス サービス [n] コールタイプ

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、ファシリティサービス サービス [n] 名前とファシリティサービス サービス [n] 番号の両方の設定が正しく設定されていないと使用できません。ファシリティ 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 認証 モード

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 認証 ログイン名とH323 認証 パスワードの設定を定義する必要があります。

H323 認証 ログイン名

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 認証パスワード

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 コールセットアップ モード

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 コールセットアップ モードが 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 ゲートキーパー アドレスも設定する必要があります。

H323 暗号化 キーサイズ

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 ゲートキーパー アドレス

ゲートキーパーの IP アドレスを定義します。H323 コールセットアップ モードを 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 H323エイリアス 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 H323エイリアス 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 モード

H323 NAT モードは、デバイスがプライベートネットワーク上にあり、ゲートキーパーに登録されていない場合に使用することを目的としています。H323 NAT モードを使用すると、パブリックネットワーク上のデバイスにアクセスできます。

NAT は IPv6 ではサポートされません。

注 : ビデオ会議デバイスがゲートウェイに登録されている場合、H323 NAT モードと H323 NAT アドレス設定は無視されます。H323 NAT モードではなく、ファイアウォールトラバーサル機能を持つゲートキーパーを使用することをお勧めします。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Auto/Off/On

Auto : Auto モードは、H323 NAT アドレス設定で NAT アドレスを指定している場合にのみ動作します。

デバイスがゲートキーパーに登録されていない場合、デバイスのローカルアドレスがプライベートである場合、発信先のアドレス (リモート) がパブリックである場合、ローカルアドレスとリモートアドレスの両方が IPv4 の場合、NAT がオンになります。それ以外の場合は、NAT がオフになります。

つまり、プライベートネットワーク上にあるデバイスだけでなく、(プライベートネットワークの外部の) 外部デバイスにも発信することができます。プライベートネットワーク上のコールの場合、H323 NAT アドレスは使用されません (ただし、存在する必要があります) 。パブリックネットワークへのコールでは、H323 NAT アドレスが使用されます。

Off : NAT がオフになっている場合、H323 NAT アドレス設定は無視されます。この場合、ゲートキーパーを使用しない限り、プライベートネットワーク外のデバイスへのコールを設定することはできません。

On : NAT は常にオンになります。H323 NAT アドレス設定で NAT アドレスを指定する必要があります。デバイスは、Q.931 および H.245 内にあるプライベート IP アドレスの代わりに、H323 NAT アドレスをシグナリングします。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 アドレス

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。プライベートネットワーク外のデバイスへのコールを設定する場合は、このアドレスが公開されます。NAT アドレスを使用する場合の詳細については、H323 NAT モード設定を参照してください。

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)

IPv4 アドレス。ほとんどの場合、パブリック IP アドレスで、RFC 1918 を参照しますが、別のプライベートアドレス (より大きな企業ネットワークなど) にすることもできます。

H323 ポート割り当て

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 モード

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 HTTPを許可

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 HTTPを許可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 安全でないHTTPSを許可

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。

HttpClient Http プロキシの使用

サービスの通信に HTTP プロキシを使用するかどうかを指定できるように、いくつかの [Http プロキシの使用 (UseHttpProxy)] 設定が用意されています。[HttpClient Httpプロキシの使用 (HttpClient UseHttpProxy)] 設定は、HttpClient コマンドを使用するマクロおよび任意の HTTP(S) リクエストに適用されます。

この設定を有効にするには、[ネットワークサービス HTTP プロキシ (NetworkServices HTTP Proxy)] 設定を使用して、HTTP、HTTPS、および WebSocket トラフィック用のプロキシサーバをセットアップ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 : サーバとの直接通信をセットアップします (プロキシを使用しません) 。

On : プロキシ経由の通信をセットアップします。

HTTP フィードバック設定

HttpFeedback Tls 検証

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、電話帳 サーバ [1] Tls 検証、プロビジョニング Tls 検証およびロギング 外部 Tls 検証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、従来のネットワークサービス HTTPS サーバ証明書検証設定が明示的に 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。

HttpFeedback Http プロキシの使用

サービスの通信に HTTP プロキシを使用するかどうかを指定できるように、いくつかの [Httpプロキシの使用 (UseHttpProxy)] 設定が用意されています。[HttpFeedback Httpプロキシの使用 (HttpFeedback UseHttpProxy)] 設定は、ビデオデバイスから送信されたフィードバックに適用されます。

この設定を有効にするには、[ネットワークサービス HTTP プロキシ (NetworkServices HTTP Proxy)] 設定を使用して、HTTP、HTTPS、および WebSocket トラフィック用のプロキシサーバをセットアップ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 : サーバとの直接通信をセットアップします (プロキシを使用しません) 。

On : プロキシ経由の通信をセットアップします。

ロギングの設定

ロギング クラウドアップロード モード

デバイスからのログを Webex クラウドサービスにアップロードできるかどうかを指定します。デバイスログは、個人を特定できる情報でフィルタリングされた後、クラウドに送信されます。

有効にすると、デバイス自体または Control Hub からログのアップロードを開始できます。デバイスにはユーザインターフェイスに [ログの送信 (Send logs)] ボタンが表示され、Control Hub の [デバイス (Devices)] ページに [ログの管理 (Manage Logs)] セクションが表示されます。

デバイスは、Webex クラウドサービスに登録されているか、オンプレミスサービスに登録されて Webex Edge for Devices にリンク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 : デバイスからのログを Webex クラウドにアップロードすることはできません。

On : デバイスからのログを Webex クラウドにアップロードできます。

ロギング デバッグ 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。

ロギング 外部 モード

デバイスログをリモート syslog サーバに保存するかどうかを指定します。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。

ロギング 外部 プロトコル

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指定します。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。

ロギング 外部 サーバ アドレス

リモート syslog サーバのアドレスを指定します。

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 DNS 名。

ロギング 外部 サーバ ポート

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。

ロギング 外部 Tls 検証

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 (ロギング外部モードの設定を参照) と監査ログ (セキュリティ監査ロギング モードの設定を参照) 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。

ロギング 内部 モード

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指定します。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。

ロギング モード

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

マクロ モード

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。

マクロ 自動スタート

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。

マクロ 無応答タイムアウト

マクロは、応答しないコードを検出するために継続的に監視されます。マクロが応答しない状況は、通常はプログラムエラーを示唆するものですが、システムリソースが限られているために発生する場合もあります。この値を大きくすると、より長い時間にわたってマクロを終了せずに実行できるようになります。一方、値を小さくすると、問題のあるマクロがシステムリソースを消費するのを抑えることができます。

必要なユーザ ロール : ADMIN

デフォルト値: 5

値スペース : 整数 (0..65535)

応答しないマクロを終了するまでの秒数を設定します。値を 0 にすると、チェックが完全に無効になります。

マクロ XAPI トランスポート

マクロシステムで使用される xAPI 伝送方式を設定します。

必要なユーザ ロール : ADMIN

デフォルト値 : WebSocket

値スペース : TSH/WebSocket

TSH : マクロでの xAPI 伝送方式は t-shell です。

WebSocket : マクロでの xAPI 伝送方式は WebSocket です。

ネットワーク設定

ネットワーク [n] DNS DNSSEC モード

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。

ネットワーク [n] DNS ドメイン名

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。

ネットワーク [n] DNS サーバ [m] アドレス

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。

ネットワーク [n] IEEE8021X モード

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。

ネットワーク [n] IEEE8021X TIs 検証

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 TIs 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。

ネットワーク [n] IEEE8021X クライアント証明書の使用

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、Web 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。

ネットワーク [n] IEEE8021X ID

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。

ネットワーク [n] IEEE8021X パスワード

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。

ネットワーク [n] IEEE8021X 匿名ID

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。

ネットワーク [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 プロトコルは無効になります。

On : EAP-MD5 プロトコルが有効になります。

ネットワーク [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 プロトコルは無効になります。

On : EAP-TTLS プロトコルが有効になります。

ネットワーク [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 プロトコルは無効になります。

On : EAP-TLS プロトコルが有効になります。

ネットワーク [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 プロトコルは無効になります。

On : EAP-PEAP プロトコルが有効になります。

ネットワーク [n] IP スタック

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。

ネットワーク [n] IPv4 割り当て

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。

DHCP を使用する場合、DHCP 要求で使用されるクライアント ID は「01」の後に MAC アドレスが続きます。

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、ネットワーク IPv4 アドレス、ネットワーク IPv4 ゲートウェイ、ネットワーク IPv4 サブネットマスクの各設定 (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。

ネットワーク [n] IPv4 アドレス

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。ネットワーク [n] IPv4 割り当てが 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。

ネットワーク [n] IPv4 ゲートウェイ

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。ネットワーク [n] IPv4 割り当てが 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。

ネットワーク [n] IPv4 サブネットマスク

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。ネットワーク [n] IPv4 割り当てが 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。

ネットワーク [n] IPv6 割り当て

n: 1..1

デバイスが IPv6 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。

DHCPv6 を使用する場合、DHCP 要求で使用されるクライアント ID は「01」の後に MAC アドレスが続きます。

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、ネットワーク IPv6 アドレスおよびネットワーク IPv6 ゲートウェイ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。ネットワーク [n] IPv6 DHCPオプション設定は、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。ネットワーク [n] IPv6 DHCPオプション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有効にします。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。ネットワーク [n] IPv6 DHCPオプション設定は、どの方法を使用するかを決定します。

ネットワーク [n] IPv6 アドレス

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。ネットワーク IPv6 割り当てが 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

ネットワーク [n] IPv6 ゲートウェイ

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、ネットワーク IPv6 割り当てが 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。

ネットワーク [n] IPv6 DHCPオプション

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有効にします。

ネットワーク [n] IPv6 インターフェイス ID

n: 1.. 1

デバイスの IPv6 インターフェイス ID を定義します。選択したインターフェイス ID (MAC または Opaque) によって、IPv6 アドレスの一部を生成するために使用されるメソッドが決定します。これは、リンクローカル IPv6 アドレスとステートレスアドレス自動構成 (SLAAC) アドレスの両方に該当します。

アドレスには、デバイスによって生成された 64 ビットのプレフィックスと 64 ビットインターフェイス ID が含まれます。MAC では、RFC-2373 で説明するように、EUI-64 ベースのインターフェイス ID が生成されます。

Opaque では、デバイスの最初のブート時に RFC-7217 で説明するようにランダムな 64 ビットのインターフェイス ID が生成され、永遠に、または工場出荷時の状態にリセットされるまで使用されます。

必要なユーザ ロール : admin、user

デフォルト値: MAC

値スペース : MAC/Opaque

MAC : インターフェイス識別方法として MAC を選択します。

Opaque : インターフェイス識別方法として Opaque を選択します。

ネットワーク [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) 。

ネットワーク [n] QoS モード

n: 1..1

QoS (Quality of Service) は、ネットワーク内のオーディオ、ビデオ、その他のデータの優先順位を処理する手法です。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 (差別化サービス) は、ネットワークトラフィックを分類して管理するための、シンプルかつスケーラブルで粗いメカニズムを指定するネットワーキングアーキテクチャです。これにより、IP ネットワークに QoS 優先順位が割り当てられます。

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 : [ネットワーク QoS Diffserv オーディオ (Network QoS Diffserv Audio)]、[ネットワーク QoS Diffserv ビデオ (Network QoS Diffserv Video)]、[ネットワーク QoS Diffserv データ (Network QoS Diffserv Data)]、[ネットワーク QoS Diffserv シグナリング (Network QoS Diffserv Signalling)]、[ネットワーク QoS Diffserv ICMPv6 (Network QoS Diffserv ICMPv6)]、および [ネットワーク QoS Diffserv NTP (Network QoS Diffserv NTP)] の各設定を使用して、パケットに優先順位が付けられます。

ネットワーク [n] QoS Diffserv オーディオ

n: 1..1

この設定は、[ネットワーク QoS モード (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。DiffServ RFC で推奨されているトラフィッククラスは、0 ～ 63 の 10 進数値にマップされます。オーディオには EF を使用することをお勧めします。EF は 10 進数値 46 で表されます。

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 : 46

値スペース : 整数 (0..63)

IP ネットワーク内でのオーディオパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

ネットワーク [n] QoS Diffserv ビデオ

n: 1..1

この設定は、[ネットワーク QoS モード (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) のパケットも、ビデオパケットのカテゴリに属します。DiffServ RFC で推奨されているトラフィッククラスは、0 ～ 63 の 10 進数値にマップされます。ビデオには AF41 を使用することをお勧めします。AF41 は 10 進数値 34 で表されます。

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 : 34

値スペース : 整数 (0..63)

IP ネットワーク内でのビデオパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

ネットワーク [n] QoS Diffserv データ

n: 1..1

この設定は、[ネットワーク QoS モード (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。DiffServ RFC で推奨されているトラフィッククラスは、0 ～ 63 の 10 進数値にマップされます。データには AF41 を使用することをお勧めします。AF41 は 10 進数値 34 で表されます。

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 : 34

値スペース : 整数 (0..63)

IP ネットワーク内でのデータパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

ネットワーク [n] QoS Diffserv シグナリング

n: 1..1

この設定は、[ネットワーク QoS モード (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。DiffServ RFC で推奨されているトラフィッククラスは、0 ～ 63 の 10 進数値にマップされます。シグナリングには CS3 を使用することをお勧めします。CS3 は 10 進数値の 24 で表されます。

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 : 24

値スペース : 整数 (0..63)

IP ネットワーク内でのシグナリングパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

ネットワーク [n] QoS Diffserv ICMPv6

n: 1..1

この設定は、[ネットワーク QoS モード (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。DiffServ RFC で推奨されているトラフィッククラスは、0 ～ 63 の 10 進数値にマップされます。ICMPv6 には 0 を使用することをお勧めします。

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 ネットワーク内での ICMPv6 パケットの優先順位を設定します。0 は「ベスト エフォート」を意味します。

ネットワーク [n] QoS Diffserv NTP

n: 1..1

この設定は、[ネットワーク QoS モード (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。DiffServ RFC で推奨されているトラフィッククラスは、0 ～ 63 の 10 進数値にマップされます。NTP には 0 を使用することをお勧めします。

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 ネットワーク内での NTP パケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

ネットワーク [n] リモートアクセス 許可

n: 1..1

リモート アクセスで SSH/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。

ネットワーク [n] 速度

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。

ネットワーク [n] トラフィック制御 モード

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。

ネットワーク [n] VLAN 音声 モード

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 音声モードが Auto に自動的に設定されます。ネットワークサービス CDP モード設定が 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 は有効になりません。

Manual : VLAN ID は、ネットワーク [n] VLAN 音声 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 は有効になりません。

ネットワーク [n] VLAN 音声 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。

ネットワークサービス設定

ネットワークサービス CDP モード

CDP (Cisco Discovery Protocol) デーモンを有効または無効にします。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 を無効にすると、[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 デーモンは有効です。

ネットワークサービス H323 モード

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無効にします。

On : H.323 コールの発信と受信の可能性を有効にします。

ネットワークサービス HTTP モード

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、Web 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 (Web 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。

ネットワーク サービス HTTP プロキシ ログイン名

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。

ネットワークサービス HTTP プロキシ パスワード

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。

ネットワーク サービス HTTP プロキシ モード

HTTP、HTTPS、および WebSocket トラフィックに対してプロキシサーバを使用するように設定できます。HTTP プロキシは手動でセットアップするか、自動設定 (PACUrl) または完全な自動化 (WPAD) を使用するか、オフにすることができます。

[ネットワークサービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が [オフ (Off)] でない場合は、どのサービスでプロキシを使用するかを、[HttpClient Httpプロキシの使用 (HttpClient UseHttpProxy)]、[HttpFeedback Httpプロキシの使用 (HttpFeedback UseHttpProxy)]、および [Webエンジン Httpプロキシの使用 (WebEngine UseHttpProxy)] の各設定で指定できます。

Cisco Webex Cloud との通信は、[ネットワークサービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が [オフ (Off)] でない限り、常にプロキシ経由で行われます。

プロキシのモードにかかわらず、デバイスと CUCM、MRA (Expressway 経由の CUCM) 、TMS との通信にはプロキシは使用されません。

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。

ネットワーク サービス HTTP プロキシ 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。

ネットワーク サービス HTTP プロキシ 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。

ネットワークサービス HTTPS OCSP モード

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 サポートを無効にします。

On : OCSP サポートを有効にします。

ネットワークサービス 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。

ネットワークサービス HTTPS サーバ 最小TLSバージョン

HTTPS で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。

ネットワークサービス HTTPS StrictTransportSecurity

HTTP Strict Transport Security ヘッダーにより、Web 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。

ネットワークサービス HTTPS クライアント証明書の検証

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。

ネットワークサービス NTP モード

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、ネットワークサービス NTP サーバ [n] アドレス設定で指定された NTP サーバ アドレスが使用されます。

Manual：デバイスは、ネットワークサービス NTP サーバ [n] アドレス設定で指定された 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。ネットワークサービス NTP サーバ [n] アドレス設定は無視されます。

ネットワークサービス NTP サーバ [n] アドレス

n: 1..3

ネットワークサービス NTP モードが Manual に設定された場合、およびネットワークサービス NTP モードが 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。

ネットワークサービス NTP サーバ [n] キー

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。ネットワークサービス NTP サーバー [n] キー設定を使用してキーを指定します。キーの先頭に「HEX:」を付けます。

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。

ネットワークサービス NTP サーバ [n] キーID

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。ID にはネットワークサービス NTP サーバー [n] キー ID 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。

ネットワークサービス NTP サーバ [n] キーアルゴリズム

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) 。

ネットワークサービス SIP モード

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無効にします。

On : SIP コールの発信と受信の可能性を有効にします。

ネットワークサービス SMTP モード

SMTP (簡易メール転送プロトコル) を使用するようにデバイスを設定して、デバイスから中継用のメール サーバに電子メールを送信することができます。これは、ユーザが組織内外の人に電子メールでホワイトボードやプレゼンテーションを送信する場合に必要です。

暗号化通信を使用するように設定されているデバイスでは ([ネットワークサービス SMTP セキュリティ (NetworkServices SMTP Security)] 設定を参照) 、SMTP サーバの証明書が検証された場合にのみ接続が許可されます。証明書チェックを無視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 : Off

値スペース : Off/On

Off : SMTP (および電子メール) サポートを無効にします。

On : 電子メールの送信用に SMTP サポートを有効にします。

ネットワークサービス SMTP サーバ

これは SMTP 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: ""

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。

ネットワークサービス SMTP ポート

このポートは、デバイスから SMTP サーバへの送信メールに使用されます。

暗号化の設定 (NetworkServices SMTP Security) と SMTP サーバの要件に基づいてポート番号を設定します。デフォルト値は使用しないでください。

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)

デバイスからの送信電子メールに使用されるポート。

ネットワークサービス SMTP ユーザ名

これは、SMTP 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の部分です。この設定は、SMTP サーバによって要求される場合があります。

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, 80)

有効なユーザ名。

ネットワークサービス SMTP パスワード

これは、SMTP 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、SMTP サーバによって要求される場合があります。

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, 64)

有効なパスワード。

ネットワークシステム SMTP 送信元

このデバイスから電子メールメッセージを送信するときに使用する、メッセージの送信元メールボックスの名前を指定します。

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)

SMTP サーバの要件を満たす電子メールアドレス。

ネットワークサービス SMTP セキュリティ

デバイスと SMTP サーバ間の通信を保護するかどうかと、その方法を選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : StartTls

値スペース : なし (None) /StartTls/Tls
None : 暗号化なしで SMTP サーバに接続します。
StartTls : 最初に暗号化なしで SMTP サーバに接続してから、STARTTLS コマンドを送信して暗号化接続 (TLS) にアップグレードします。
Tls : TLS (トランスポート層セキュリティ) 経由で SMTP に接続します。

ネットワークサービス SNMP モード

SNMP (簡易ネットワーク管理プロトコル) は、IP ネットワークに接続されているルーター、サーバ、スイッチなどのデバイスの監視と管理を行うために、ネットワーク管理システムによって使用されます。SNMP は、管理対象デバイスの管理データを変数の形で公開します。これにより、デバイスのステータスと設定が表されます。これらの変数は、管理アプリケーションでリモートから照会したり、場合によっては設定したりできます。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Off

値スペース : Off/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有効にします。
ReadWrite : SNMP ネットワーク サービスの照会とコマンドの両方を有効にします。

ネットワーク サービス SNMP コミュニティ名

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。管理システムからの SNMP 要求に、一致するコミュニティ名 (大文字と小文字の区別あり) が含まれていない場合、そのメッセージは破棄され、ビデオデバイスの SNMP エージェントは応答送信しません。

Cisco TelePresence Management Suite (TMS) を使用している場合は、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。

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。

ネットワークサービス SNMP システム管理者

SNMP サーバで使用できる連絡先情報を定義します。

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)
ビデオデバイスの連絡先情報を表す文字列。

ネットワークサービス SNMP システムロケーション

SNMP サーバで使用できるロケーション情報を定義します。

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)
ビデオデバイスのロケーション情報を表す文字列。

ネットワークサービス SNMP モード

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 プロトコルは有効になります (デフォルト) 。

ネットワークサービス SSH ホストキーアルゴリズム

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。

ネットワークサービス SSH 公開キーの許可

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。

ネットワークサービス UPnP モード

UPnP (ユニバーサル プラグ アンド プレイ) を完全に無効にするか、ビデオ会議デバイスがオンになった後または再起動した後に、短時間だけ UPnP を有効にします。

デフォルトでは、ビデオ会議デバイスをオンにするか再起動すると、UPnP が有効になります。その後、ネットワークサービス UPnP タイムアウトの設定で定義されたタイムアウト時間が経過すると、UPnP は自動的に無効になります。

UPnP が有効になると、デバイスはネットワーク上での自身のプレゼンスをアドバタイズします。このアドバタイズによって、タッチコントローラはビデオ会議デバイスを自動的に検出できるようになります。タッチコントローラとペアリングするために、手動でデバイスの IP アドレスを入力する必要はありません。

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 : UPnP は無効になります。ビデオ会議デバイスは自身のプレゼンスをアドバタイズしないため、タッチコントローラをデバイスとペアリングするためにはデバイスの IP アドレスを手動で入力する必要があります。

On : UPnP は有効になります。ビデオ会議デバイスはタイムアウト期間が経過するまで、自身のプレゼンスをアドバタイズします。

ネットワークサービス UPnP タイムアウト

デバイスの電源をオンにした後または再起動した後に、UPnP を有効のままにしておく秒数を定義します。この設定を有効にするには、ネットワークサービス UPnP モードを On 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: 600

値スペース : 整数 (0..3600)

範囲 : 0 ～ 3600 秒の値を選択します。

ネットワークサービス 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。

ネットワークサービス ウェルカムテキスト

SSH でデバイスにログインする際に、ユーザ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)

ネットワークサービス Wifi 許可

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。

このデバイスは次の標準をサポートします : IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n、and IEEE 802.11ac。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。

ネットワークサービス Wifi A_MPDU

この設定は、リアルタイムのメディアパフォーマンスを向上させることを目的としています。集合的 MAC プロトコルデータユニット (A-MPDU) がオンの場合、MAC プロトコルデータフレームはグループ化され、まとめて送信されます。受信者は、個々のフレームごとに確認するのではなく、グループの受信を確認します。これにより帯域幅が最適化されますが、データ配信が遅延する可能性があります。これは、ビデオコールデータなど、リアルタイム配信の優先順位が必要なデータには不適切です。

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 : A-MPDU を無効にし、データがグループ化されてまとめて送信されるのではなく、リアルタイム配信の優先順位を維持するためにすぐに送信されるようにします。

On : A-MPDU を有効にし、MAC プロトコルデータフレームがグループ化され、まとめて送信されるようにします。

ネットワーク サービス WiFi 有効

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。

ネットワークサービス XMLAPI モード

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

周辺機器 ペアリング Ciscoタッチパネル リモートペアリング

ビデオ会議デバイスのユーザインターフェイスとしてタッチコントローラ (Cisco Webex Room Navigator または Cisco Touch 10) を使用するには、タッチコントローラをデバイスに直接接続するか、LAN 経由でデバイスにペアリングする必要があります。後者はリモート ペアリングと呼ばれます。

リモート ペアリングはデフォルトで許可されています。リモート ペアリングを回避する場合は、この設定をオフに切り替えてください。

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 : タッチコントローラのリモートペアリングは許可されません。

On : タッチコントローラのリモートペアリングは許可されます。

周辺機器 プロファイル カメラ

デバイスに接続されることが予想されるカメラの数を定義します。この情報はデバイスの診断サービスで使用します。接続されたカメラ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。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 0

値スペース : 0

0 : デバイスに接続されることが予想されるカメラの数。

周辺機器 プロファイル 制御システム

サードパーティ製の制御システム (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。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : NotSet

値スペース : 未設定 (NotSet)

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

電話帳 サーバ [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。

電話帳 サーバ [n] ページネーション

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。

電話帳 サーバ [n] TLS 検証

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、従来のネットワークサービス HTTPS サーバ証明書検証設定が明示的に 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。

電話帳 サーバ [n] タイプ

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。

電話帳サーバ [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

プロビジョニング 接続

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。

プロビジョニング CUCM コール管理レコード コール診断

デバイスがコール統計を CUCM に送信できるようにし、コール統計は CUCM のコール管理レコードに追加されます。コール統計は、コールの終了時に CUCM に送信されます。

必要なユーザ ロール : admin、user

デフォルト値 : Enabled

値スペース : Disabled/Enabled

Enabled : CUCM コール管理レコードのサポートを有効にします。

Disabled : CUCM コール管理レコードのサポートを無効にします。

プロビジョニング 外部マネージャ アドレス

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。

プロビジョニング 外部マネージャ 代替アドレス

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。

プロビジョニング 外部マネージャ プロトコル

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、ネットワークサービス HTTP モード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。

プロビジョニング 外部マネージャ パス

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。

プロビジョニング 外部マネージャ ドメイン

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。

プロビジョニング モード

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。Webex クラウドサービスに登録するには、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。

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。

プロビジョニング ログイン名

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ログイン情報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。

プロビジョニング パスワード

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ログイン情報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。

プロビジョニング Tls 検証

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、従来のネットワークサービス HTTPS サーバ証明書検証設定が明示的に 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。

プロビジョニング WebexEdge

デバイスを Webex Edge for Devices にリンクするかどうかを定義します。リンクしたデバイスには、特定の Webex クラウドサービスへのアクセスが提供されます。

この設定は、オンプレミスサービス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、user

デフォルト値 : Off

値スペース : Off/On

Off : デバイスは Webex Edge for Devices にリンクされません。

On : デバイスは Webex Edge for Devices にリンクされます。

プロキシミティの設定

プロキシミティ 代替ポート 有効

この設定は、[ネットワークサービス HTTP モード (NetworkServices HTTP Mode)] が [HTTP+HTTPS] または [HTTPS.] に設定されている場合にのみ適用されます。

デフォルトでは、プロキシミティ接続は TCP ポート 443 を使用します。この設定を使用すると、ポート 65533 でもプロキシミティ接続が許可されます。

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 : プロキシミティ接続は常に TCP ポート 443 を使用します。

True : プロキシミティ接続は TCP ポート 443 または 65533 を使用できます。使用されるポートはクライアントによって変わります。

プロキシミティ モード

[プロキシミティ モード (Proximity Mode)] 設定は、Webex クラウドサービスに登録されているデバイスには効果がありません。クラウド登録デバイスから超音波ペアリングメッセージが送信されないようにするには、[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] を 0 に設定する必要があります。

オンプレミス登録デバイスの場合は、[プロキシミティ モード (Proximity Mode)] 設定により、超音波ペアリングメッセージを出力するかどうかを決定します。デバイスから超音波ペアリングメッセージを出力すると、デバイスが近くにあることをシスココラボレーションクライアントで検知できます。

クライアントを使用するには、少なくとも 1 つのプロキシミティサービスを有効にする必要もあります ([プロキシミティ サービス (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。

[プロキシミティ モード (Proximity Mode)] 設定と [オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定は、超音波ペアリングメッセージにのみ影響します。超音波の出力をすべて停止するには、[ルーム分析 人の存在の検出 (RoomAnalytics PeoplePresenceDetector)] 設定と [スタンバイ モーション検知ウェイクアップ (Standby WakeupOnMotionDetection)] 設定も [オフ (Off)] 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 : On

値スペース : Off/On

Off : シスココラボレーション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せん。このため、プロキシミティサービスは使用できません。

On : シスココラボレーション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。

プロキシミティ サービス コール制御

シスココラボレーションクライアントの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、シスココラボレーション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、音量調節、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、プロキシミティ モードを 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 : シスココラボレーションクライアントからのコール制御が有効になります。

Disabled : シスココラボレーションクライアントからのコール制御が無効になります。

プロキシミティ サービス コンテンツ共有 クライアントから

シスココラボレーション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、シスココラボレーションクライアントからのコンテンツをデバイスにワイヤレスで共有できます (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、プロキシミティ モードを 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 : シスココラボレーション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 : シスココラボレーションクライアントからのコンテンツ共有が無効になります。

プロキシミティ サービス コンテンツ共有 クライアントへ

シスココラボレーションクライアントへの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、シスココラボレーションクライアントはデバイスからプレゼンテーションを受け取ります。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、プロキシミティ モードを 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 : シスココラボレーションクライアントへのコンテンツ共有が有効になります。

Disabled : シスココラボレーションクライアントへのコンテンツ共有が無効になります。

ルーム分析設定

ルーム分析 環境雑音の予測 間隔

環境雑音の予測を実行する間隔を設定します (有効化されている場合) 。xConfiguration ルーム分析 環境雑音の予測 モードを使用して、環境雑音の予測を有効または無効にすることができます。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値: 10

値スペース : 整数 (10..60)

環境雑音の予測を実行する頻度の間隔 (秒) を設定します。

ルーム分析 環境雑音の予測 モード

デバイスは室内の固定周囲ノイズ レベル (背景雑音レベル) を算出することができます。結果は RoomAnalytics AmbientNoise レベル dBA ステータスにレポートされます。新しい周囲ノイズレベルが検出されるとステータスが更新されます。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Off

値スペース : Off/On

On : デバイスは固定周囲ノイズ レベルを定期的に予測します。

Off : デバイスは固定周囲ノイズ レベルを定期的に予測しません。

ルーム分析 非通話中人数計測

顔検出を使用して、デバイスが室内にいる人の人数を特定できます。デフォルトでは、デバイスは通話中のときまたはセルフ ビューに画像を表示したときにのみ人数を数えます。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Off

値スペース : Off/On

Off : デバイスは、デバイスが通話中のときまたはセルフ ビューがオンのときのみ、人数を数えます。

On : デバイスは、デバイスがスタンバイ モードでない限り、人数を数えます。セルフ ビューがオフであっても、これは非通話中の人数を含みます。

ルーム分析 人の存在の検出

デバイスは、人が室内に存在しているかどうかを確認し、その結果を [ルーム分析 人の存在 (RoomAnalytics PeoplePresence)] のステータスにレポートすることができます。この機能は、超音波に基づいています。詳細については、ステータスの説明を参照してください。

この設定と [スタンバイ モーション検知ウェイクアップ (Standby WakeupOnMotionDetection)] 設定の両方が [オフ (Off)] になっている場合、人の存在を検出するための超音波信号は出力されません。[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定と [プロキシミティ モード (Proximity Mode)] 設定は、人の存在の検出には影響しません。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Off

値スペース : Off/On

Off : ユーザの存在に関する情報は、デバイスのステータスで報告されません。

On : ユーザの存在に関する情報は、デバイスのステータスで報告されます。

ルームクリーンアップの設定

ルームクリーンアップ 自動実行 コンテンツタイプ Web データ

Web データの毎日のルームクリーンアップを有効または無効にします。xConfiguration ルームクリーンアップ 自動実行 時間を使用して時刻を設定します。

必要なユーザ ロール : ADMIN

デフォルト値 : Daily

値スペース : Daily/Off

Daily : Web データの毎日のクリーンアップを有効にします。

Off : Web データの毎日のクリーンアップを無効にします。

ルームクリーンアップ 自動実行 コンテンツタイプ ホワイトボード

ホワイトボードの毎日のルームクリーンアップを有効または無効にします。xConfiguration ルームクリーンアップ 自動実行 時間を使用して時刻を設定します。

必要なユーザ ロール : ADMIN

デフォルト値 : Daily

値スペース : Daily/Off

Daily : ホワイトボードの毎日のクリーンアップを有効にします。

Off : ホワイトボードの毎日のクリーンアップを無効にします。

ルームクリーンアップ 自動実行 時間

ルームクリーンアップを実行する毎日の時刻を設定します。

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..23)

ルームクリーンアップが行われる時刻。

ルームリセットの設定

ルームリセット 制御

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信されません。

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。

ルームスケジューラの設定

ルームスケジューラ 有効

ルームスケジューリング機能を使用すると、会議室にあるタッチコントローラから部屋を直接予約できます。部屋が使用可能な場合は、進行中の会議を延長することもできます。Webex Assistant（音声駆動型の仮想アシスタント）を使用して会議を予約または延長することもできます。

ルームスケジューリング機能では、デバイスが Webex クラウドサービスに登録されているか、または Webex Edge for Devices にリンクされている必要があります。また、予約を許可するカレンダーサービスをルームに設定する必要があります。

ルームスケジューリング機能はパーソナルモードデバイスではサポートされていません。

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 : ルームスケジューリング機能は使用できません。

True : 上記の前提条件を満たす場合、ルームスケジューリング機能を使用できます。

RTP 設定

RTP ポート 範囲 開始

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 ポート 範囲 終了

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 ビデオ ポート 範囲 開始

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 ビデオ ポート 範囲 終了

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

セキュリティ 監査 ロギング モード

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。

セキュリティ 監査 エラー発生時 アクション

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、セキュリティ監査ロギング モードが 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。

セキュリティ 監査 サーバ アドレス

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、セキュリティ監査ロギング モードが 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。

セキュリティ 監査 サーバ ポート

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、セキュリティ 監査 サーバ ポート割り当て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。

セキュリティ 監査 サーバ ポート割り当て

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、セキュリティ監査ロギング モードが 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、セキュリティ 監査 サーバ ポート状態をチェックできます。Web 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。セキュリティ監査ロギング モードが 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。

セキュリティ Fips モード

必要に応じて、デバイスを FIPS モードに設定することができます (連邦情報処理標準 (FIPS) 140-3、「暗号化モジュールのセキュリティ要件」) 。FIPS モードでは、リモートサポートユーザは利用できません。また、デバイスと HTTP プロキシ間のダイジェストアクセス認証はサポートされません。これは、ダイジェストアクセス認証で使用される MD5 暗号化ハッシュが FIPS で許可されていないためです。この最後の制限は、Webex 登録デバイスにのみ影響します。これは HTTP プロキシが Webex ソリューションにのみ使用されるためです。

FIPS モードでは、HTTPS のみを許可し、SNMP や IEEE8021X に切り替えないようにする (デフォルト値を保持する) 必要があります。

この設定に対する変更を完全に反映させるには、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 : Off

値スペース : Off/On

Off : デバイスは FIPS モードではありません。

On : デバイスが FIPS モードになります。

セキュリティ セッション ログイン失敗時のロックアウト時間

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。

セキュリティ セッション非アクティブタイムアウト

ユーザが Web または SSH セッションから自動的にログアウトされるまでに、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) を設定します。0 を指定すると、1 時間のタイムアウトになります。最大タイムアウト長は 12 時間です。

セキュリティ セッション ログイン失敗の最大数

Web 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。

セキュリティ セッション ユーザあたりの最大セッション数

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。

セキュリティ セッション 最大総セッション数

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。

セキュリティ セッション 最後のログオンを表示

SSH を使用してデバイスにログインすると、前回ログインに成功したセッションのユーザ ID、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。

シリアルポート設定

シリアルポート モード

シリアル ポートを有効/無効にします。

この設定は、第 1 世代の Board (Webex Board 55 および Webex Board 70) では使用できません。

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 : シリアル通信が無効になります。

On : シリアル通信が有効になります。

シリアルポート ボーレート

シリアルポートのボーレート (データ転送速度) を設定します。

シリアル ポートの他の接続パラメータは次の通りです。データ ビット : 8。パリティ : なし。ストップ ビット : 1。フロー制御 : なし。

この設定は、第 1 世代の Board (Webex Board 55 および Webex Board 70) では使用できません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 115200

値スペース : 115200

リストからボーレートを選択します (ビット/秒) 。

シリアルポート ログインが必要

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。

この設定は、第 1 世代のボード (Webex Board 55 および Webex Board 70) では使用できません。

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 : 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 認証ユーザ名

これは、SIP プロキシへの認証に使用されるログイン情報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 認証パスワード

これは、SIP プロキシへの認証に使用されるログイン情報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 デフォルトトランスポート

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 表示名

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 デフォルト候補

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 モード

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。メディアパスを設定すると、最初に STUN（Session Traversal Utilities for NAT）メッセージが交換されます。

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 回線

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 リッスンポート

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 をオフにする必要があります。

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：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 メールボックス

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 最小 TLS バージョン

SIP で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 優先IPシグナリング

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) 。ネットワーク IP スタックおよび会議 通信プロトコルIPスタックの両方が 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 プロキシ [n] アドレス

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 Tls検証

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 最小 TLS バージョン設定を使用します。

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 検出モード

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 サーバ

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 ユーザ名

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 パスワード

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 タイプ

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

スタンバイ ブートアクション

ビデオ会議デバイスの再起動後のカメラの位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: RestoreCameraPosition

値スペース: None/DefaultCameraPosition/RestoreCameraPosition

None: アクションはありません。

RestoreCameraPosition: ビデオ会議デバイスを再起動すると、カメラは再起動前の位置に戻ります。

DefaultCameraPosition: ビデオ会議デバイスを再起動すると、カメラは工場出荷時のデフォルトの位置に移動します。

スタンバイ制御

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。

スタンバイ遅延

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: 4

値スペース: 整数 (1..480)

スタンバイ遅延 (分) を設定します。

スタンバイ サイネージ オーディオ

デフォルトでは、デバイスは、Web ページに音声がある場合でも、デジタル信号モードで音声を再生しません。この設定を使用して、デフォルトの動作を上書き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: Off

値スペース: Off/On

Off: デバイスは、Web ページで音声を再生しません。

On: Web ページに音声が含まれている場合、デバイスは音声を再生します。音量は、デバイスの音量設定に従います。

スタンバイ サイネージ 対話モード

デフォルトでは、ユーザがデジタル サイネージの Web ページを操作することはできません。この設定を使用すると、Web ページとの対話機能を有効に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: 非インタラクティブ (NonInteractive)

値スペース: インタラクティブ (Interactive) /非インタラクティブ (NonInteractive)

Interactive: Web ページを操作することができます。

NonInteractive: Web ページを操作することはできません。

スタンバイ サイネージ モード

URL (Web ページ) からのコンテンツは、従来のハーフ ウェイク バックグラウンド イメージおよび情報を置き換えることができます。この機能は、「デジタル サイネージ」と呼ばれます。ユーザーは、リンクのクリックやフォームへのテキスト入力など、Web ページの操作を行うことができます。

デジタル サイネージを使用すると、デバイスが通常の方法でスタンバイ状態に入ることを防止できません。そのため、スタンバイ遅延の設定は、デバイスがスタンバイ状態になるまでのデジタル サイネージの表示時間を決定します。

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 : デバイスでデジタル サイネージが有効になっていません。

On : Web エンジン モード設定がオンになっている場合、デジタル サイネージが有効化され、デバイスのハーフ ウェイク モードに置き換えられます。

スタンバイ サイネージ 更新間隔

この設定を使用して、Web ページを定期的に更新することができます。これは、Web ページ自体を更新できない場合に便利です。更新間隔をインタラクティブ モードで設定することは推奨されません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 0

値スペース : 整数 (0 ～ 1440)

各 Web ページの更新間隔を秒数で表示します。値が 0 の場合、Web ページは強制的に更新されなくなります。

スタンバイ サイネージ Url

画面 (デジタル サイネージ) に表示する Web ページの URLを設定します。URL の長さが 0 の場合、デバイスに通常のハーフ ウェイク モードが保持されます。URL が機能していない場合、デバイスは通常のハーフ ウェイク モードを保持し、診断メッセージが発行されます。

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, 2000)

Web ページの URL。

スタンバイ ウェイクアップアクション

スタンバイ モードを抜けるときのカメラ位置を定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : RestoreCameraPosition

値スペース : None/RestoreCameraPosition/DefaultCameraPosition

None : アクションはありません。

RestoreCameraPosition : ビデオ会議デバイスがスタンバイ状態から復帰すると、カメラはスタンバイ前の位置に戻ります。

DefaultCameraPosition : ビデオ会議デバイスがスタンバイ状態になると、カメラは工場出荷時のデフォルトの位置に移動します。

スタンバイ モーション検知ウェイクアップ

モーション検知時の自動ウェイクアップは、人が入室したことをデバイスで検出できるようにする機能です。この機能は、超音波検出に基づいています。

この設定と [ルーム分析 人の存在の検出 (RoomAnalytics PeoplePresenceDetector)] 設定の両方が [オフ (Off)] になっている場合、モーション検知用の超音波信号は出力されません。[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定と [プロキシミティ モード (Proximity Mode)] 設定は、モーション検知には影響しません。

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 : モーション検知ウェイクアップが無効になります。

On : 人が部屋に入ると、デバイスが自動的にスタンバイから復帰します。

システムユニット設定

システムユニット名

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。

高度なシステムユニット クラッシュレポート

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 : On

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。

システムユニット クラッシュレポート モード

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 : On

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。

システムユニット クラッシュレポート 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 : "acr.cisco.com"

値スペース : 文字列 (0..255)

[Cisco Automatic Crash Report ツール（Cisco Automatic Crash Report tool）] の URL。

システムユニット カスタムデバイス ID

システムユニット カスタムデバイス ID は、ユニットに関するカスタム情報を保存する場所になります。これは、たとえば、プロビジョニング設定でデバイスを追跡する上で役立ちます。

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..255)

時刻設定

時刻 時刻形式

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。

時刻 日付形式

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。

タイムゾーン

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

値スペース：Africa/Abidjan、Africa/Accra、Africa/Addis_Ababa、Africa/Algiers、Africa/Asmara、Africa/Asmera、Africa/Bamako、Africa/Bangui、Africa/Banjul、Africa/Bissau、Africa/Blantyre、Africa/Brazzaville、Africa/Bujumbura、Africa/Cairo、Africa/Casablanca、Africa/Ceuta、Africa/Conakry、Africa/Dakar、Africa/Dar_es_Salaam、Africa/Djibouti、Africa/Douala、Africa/El_Aaiun、Africa/Freetown、Africa/Gaborone、Africa/Harare、Africa/Johannesburg、Africa/Juba、Africa/Kampala、Africa/Khartoum、Africa/Kigali、Africa/Kinshasa、Africa/Lagos、Africa/Libreville、Africa/Lome、Africa/Luanda、Africa/Lubumbashi、Africa/Lusaka、Africa/Malabo、Africa/Maputo、Africa/Maseru、Africa/Mbabane、Africa/Mogadishu、Africa/Monrovia、Africa/Nairobi、Africa/Ndjamena、Africa/Niamey、Africa/Nouakchott、Africa/Ouagadougou、Africa/Porto-Novo、Africa/Sao_Tome、Africa/Timbuktu、Africa/Tripoli、Africa/Tunis、Africa/Windhoek、America/Adak、America/Anchorage、America/Anguilla、America/Antigua、America/Araguaina、America/Argentina/Buenos_Aires、America/Argentina/Catamarca、America/Argentina/ComodRivadavia、America/Argentina/Cordoba、America/Argentina/Jujuy、America/Argentina/La_Rioja、America/Argentina/Mendoza、America/Argentina/Rio_Gallegos、America/Argentina/Salta、America/Argentina/San_Juan、America/Argentina/San_Luis、America/Argentina/Tucuman、America/Argentina/Ushuaia、America/Aruba、America/Asuncion、America/Atikokan、America/Atka、America/Bahia、America/Bahia_Banderas、America/Barbados、America/Belem、America/Belize、America/Blanc-Sablon、America/Boa_Vista、America/Bogota、America/Boise、America/Buenos_Aires、America/Cambridge_Bay、America/Campo_Grande、America/Cancun、America/Caracas、America/Catamarca、America/Cayenne、America/Cayman、America/Chicago、America/Chihuahua、America/Coral_Harbour、America/Cordoba、America/Costa_Rica、America/Creston、America/Cuiaba、America/Curacao、America/Danmarkshavn、America/Dawson、America/Dawson_Creek、America/Denver、America/Detroit、America/Dominica、America/Edmonton、America/Eirunepe、America/El_Salvador、America/Ensenada、America/Fort_Nelson、America/Fort_Wayne、America/Fortaleza、America/Glace_Bay、America/Godthab、America/Goose_Bay、America/Grand_Turk、America/Grenada、America/Guadeloupe、America/Guatemala、America/Guayaquil、America/Guyana、America/Halifax、America/Havana、America/Hermosillo、America/Indiana/Indianapolis、America/Indiana/Knox、America/Indiana/Marengo、America/Indiana/Petersburg、America/Indiana/Tell_City、America/Indiana/Vevay、America/Indiana/Vincennes、America/Indiana/Winamac、America/Indianapolis、America/Inuvik、America/Iqaluit、America/Jamaica、America/Jujuy、America/Juneau、America/Kentucky/Louisville、America/Kentucky/Monticello、America/Knox_IN、America/Kralendijk、America/La_Paz、America/Lima、America/Los_Angeles、America/Louisville、America/Lower_Princes、America/Maceio、America/Managua、America/Manaus、America/Marigot、America/Martinique、America/Matamoros、America/Mazatlan、America/Mendoza、America/Menominee、America/Merida、America/Metlakatla、America/Mexico_City、America/Miquelon、America/Moncton、America/Monterrey、America/Montevideo、America/Montreal、America/Montserrat、America/Nassau、America/New_York、America/Nipigon、America/Nome、America/Noronha、America/North_Dakota/Beulah、America/North_Dakota/Center、America/North_Dakota/New_Salem、America/Nuuk、America/Ojinaga、America/Panama、America/Pangnirtung、America/Paramaribo、America/Phoenix、America/Port-au-Prince、America/Port_of_Spain、America/Porto_Acre、America/Porto_Velho、America/Puerto_Rico、America/Punta_Arenas、America/Rainy_River、America/Rankin_Inlet、America/Recife、America/Regina、America/Resolute、America/Rio_Branco、America/Rosario、America/Santa_Isabel、America/Santarem、America/Santiago、America/Santo_Domingo、America/Sao_Paulo、America/Scoresbysund、America/Shiprock、America/Sitka、America/St_Barthelemy、America/St_Johns、America/St_Kitts、America/St_Lucia、America/St_Thomas、America/St_Vincent、America/Swift_Current、America/Tegucigalpa、America/Thule、America/Thunder_Bay、America/Tijuana、America/Toronto、America/Tortola、America/Vancouver、America/Virgin、America/Whitehorse、America/Winnipeg、America/Yakutat、America/Yellowknife、Antarctica/Casey、Antarctica/Davis、Antarctica/DumontDUrville、Antarctica/Macquarie、Antarctica/Mawson、Antarctica/McMurdo、Antarctica/Palmer、Antarctica/Rothera、Antarctica/South_Pole、Antarctica/Syowa、Antarctica/Troll、Antarctica/Vostok、Arctic/Longyearbyen、Asia/Aden、Asia/Almaty、Asia/Amman、Asia/Anadyr、Asia/Aqtau、Asia/Aqtobe、Asia/Ashgabat、Asia/Ashkhabad、Asia/Atyrau、Asia/Baghdad、Asia/Bahrain、Asia/Baku、Asia/Bangkok、Asia/Barnaul、Asia/Beirut、Asia/Bishkek、Asia/Brunei、Asia/Calcutta、Asia/Chita、Asia/Choibalsan、Asia/Chongqing、Asia/Chungking、Asia/Colombo、Asia/Dacca、Asia/Damascus、Asia/Dhaka、Asia/Dili、Asia/Dubai、Asia/Dushanbe、Asia/Famagusta、Asia/Gaza、Asia/Harbin、Asia/Hebron、Asia/Ho_Chi_Minh、Asia/Hong_Kong、Asia/Hovd、Asia/Irkutsk、Asia/Istanbul、Asia/Jakarta、Asia/Jayapura、Asia/Jerusalem、Asia/Kabul、Asia/Kamchatka、Asia/Karachi、Asia/Kashgar、Asia/Kathmandu、Asia/Katmandu、Asia/Khandyga、Asia/Kolkata、Asia/Krasnoyarsk、Asia/Kuala_Lumpur、Asia/Kuching、Asia/Kuwait、Asia/Macao、Asia/Macau、Asia/Magadan、Asia/Makassar、Asia/Manila、Asia/Muscat、Asia/Nicosia、Asia/Novokuznetsk、Asia/Novosibirsk、Asia/Omsk、Asia/Oral、Asia/Phnom_Penh、Asia/Pontianak、Asia/Pyongyang、Asia/Qatar、Asia/Qostanay、Asia/Qyzylorda、Asia/Rangoon、Asia/Riyadh、Asia/Saigon、Asia/Sakhalin、Asia/Samarkand、Asia/Seoul、Asia/Shanghai、Asia/Singapore、Asia/Srednekolymsk、Asia/Taipei、Asia/Tashkent、Asia/Tbilisi、Asia/Tehran、Asia/Tel_Aviv、Asia/Thimbu、Asia/Thimphu、Asia/Tokyo、Asia/Tomsk、Asia/Ujung_Pandang、Asia/Ulaanbaatar、Asia/Ulan_Bator、Asia/Urumqi、Asia/Ust-Nera、Asia/Vientiane、Asia/Vladivostok、Asia/Yakutsk、Asia/Yangon、Asia/Yekaterinburg、Asia/Yerevan、Atlantic/Azores、Atlantic/Bermuda、Atlantic/Canary、Atlantic/Cape_Verde、Atlantic/Faeroe、Atlantic/Faroe、Atlantic/Jan_Mayen、Atlantic/Madeira、Atlantic/Reykjavik、Atlantic/South_Georgia、Atlantic/St_Helena、Atlantic/Stanley、Australia/ACT、Australia/Adelaide、Australia/Brisbane、Australia/Broken_Hill、Australia/Canberra、Australia/Currie、Australia/Darwin、Australia/Eucla、Australia/Hobart、Australia/LHI、Australia/Lindeman、Australia/

Lord_Howe、Australia/Melbourne、Australia/NSW、Australia/North、Australia/Perth、Australia/Queensland、Australia/South、Australia/Sydney、Australia/Tasmania、Australia/Victoria、Australia/West、Australia/Yancowinna、Brazil/Acre、Brazil/DeNoronha、Brazil/East、Brazil/West、CET、CST6CDT、Canada/Atlantic、Canada/Central、Canada/Eastern、Canada/Mountain、Canada/Newfoundland、Canada/Pacific、Canada/Saskatchewan、Canada/Yukon、Chile/Continental、Chile/EasterIsland、Cuba、EET、EST、EST5EDT、Egypt、Eire、Etc/GMT、Etc/GMT+0、Etc/GMT+1、Etc/GMT+10、Etc/GMT+11、Etc/GMT+12、Etc/GMT+2、Etc/GMT+3、Etc/GMT+4、Etc/GMT+5、Etc/GMT+6、Etc/GMT+7、Etc/GMT+8、Etc/GMT+9、Etc/GMT-0、Etc/GMT-1、Etc/GMT-10、Etc/GMT-11、Etc/GMT-12、Etc/GMT-13、Etc/GMT-14、Etc/GMT-2、Etc/GMT-3、Etc/GMT-4、Etc/GMT-5、Etc/GMT-6、Etc/GMT-7、Etc/GMT-8、Etc/GMT-9、Etc/GMT0、Etc/Greenwich、Etc/UCT、Etc/UTC、Etc/Universal、Etc/Zulu、Europe/Amsterdam、Europe/Andorra、Europe/Astrakhan、Europe/Athens、Europe/Belfast、Europe/Belgrade、Europe/Berlin、Europe/Bratislava、Europe/Brussels、Europe/Bucharest、Europe/Budapest、Europe/Busingen、Europe/Chisinau、Europe/Copenhagen、Europe/Dublin、Europe/Gibraltar、Europe/Guernsey、Europe/Helsinki、Europe/Isle_of_Man、Europe/Istanbul、Europe/Jersey、Europe/Kaliningrad、Europe/Kiev、Europe/Kirov、Europe/Lisbon、Europe/Ljubljana、Europe/London、Europe/Luxembourg、Europe/Madrid、Europe/Malta、Europe/Mariehamn、Europe/Minsk、Europe/Monaco、Europe/Moscow、Europe/Nicosia、Europe/Oslo、Europe/Paris、Europe/Podgorica、Europe/Prague、Europe/Riga、Europe/Rome、Europe/Samara、Europe/San_Marino、Europe/Sarajevo、Europe/Saratov、Europe/Simferopol、Europe/Skopje、Europe/Sofia、Europe/Stockholm、Europe/Tallinn、Europe/Tirane、Europe/Tiraspol、Europe/Ulyanovsk、Europe/Uzhgorod、Europe/Vaduz、Europe/Vatican、Europe/Vienna、Europe/Vilnius、Europe/Volgograd、Europe/Warsaw、Europe/Zagreb、Europe/Zaporozhye、Europe/Zurich、GB、GB-Eire、GMT、GMT+0、GMT-0、GMT0、Greenwich、HST、Hongkong、Iceland、Indian/Antananarivo、Indian/Chagos、Indian/Christmas、Indian/Cocos、Indian/Comoro、Indian/Kerguelen、Indian/Mahe、Indian/Maldives、Indian/Mauritius、Indian/Mayotte、Indian/Reunion、Iran、Israel、Jamaica、Japan、Kwajalein、Libya、MET、MST、MST7MDT、Mexico/BajaNorte、Mexico/BajaSur、Mexico/General、NZ、NZ-CHAT、Navajo、PRC、PST8PDT、Pacific/Apia、Pacific/Auckland、Pacific/Bougainville、Pacific/Chatham、Pacific/Chuuk、Pacific/Easter、Pacific/Efate、Pacific/Enderbury、Pacific/Fakaofo、Pacific/Fiji、Pacific/Funafuti、Pacific/Galapagos、Pacific/Gambier、Pacific/Guadalcanal、Pacific/Guam、Pacific/Honolulu、Pacific/Johnston、Pacific/Kiritimati、Pacific/Kosrae、Pacific/Kwajalein、Pacific/Majuro、Pacific/Marquesas、Pacific/Midway、Pacific/Nauru、Pacific/Niue、Pacific/Norfolk、Pacific/Noumea、Pacific/Pago_Pago、Pacific/Palau、Pacific/Pitcairn、Pacific/Pohnpei、Pacific/Ponape、Pacific/Port_Moresby、Pacific/Rarotonga、Pacific/Saipan、Pacific/Samoa、Pacific/Tahiti、Pacific/Tarawa、Pacific/Tongatapu、Pacific/Truk、Pacific/Wake、Pacific/Wallis、Pacific/Yap、Poland、Portugal、ROC、ROK、Singapore、Turkey、UCT、US/Alaska、US/Aleutian、US/Arizona、US/Central、US/East-Indiana、US/Eastern、US/Hawaii、US/Indiana-Starke、US/Michigan、US/Mountain、US/Pacific、US/Samoa、UTC、Universal、W-SU、WET、Zulu

リストからタイムゾーンを選択します。

ユーザインタラクション設定

ユーザインタラクション 挙手 CMS

この設定は、CMS 会議の挙手機能の可用性を制御します。CMS が挙手機能をサポートし、この設定が True に設定されている場合、挙手ボタンがデバイスのユーザインターフェイスに表示されます。

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

ユーザインターフェイス設定

ユーザインターフェイス アクセシビリティ 着信コール通知

画面表示を強調した着信コールの通知を利用できます。画面とタッチコントローラ 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。

ユーザインターフェイス アシスタント モード

Webex Assistant を使用すると、音声コマンドを使用してデバイスを制御できます。Webex Assistant はクラウドサービスなので、デバイスが Webex クラウドサービスに登録されているか、オンプレミスサービスに登録されて Webex Edge for Devices にリンクされている必要があります。

デバイスで Webex Assistant を有効または無効にするには、この設定を使用します。

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 : Webex Assistant がオフになります。

On : インフラストラクチャでサポートされていれば、Webex Assistant を使用できます。

ユーザインターフェイス アシスタント 会議参加確認

参加確認は Webex Assistant によって提供される機能です。参加確認が有効になっている場合、OBTP ミーティングの開始直前にミーティングルームに人がいることが検出されると、デバイスはその人にこれから始まるミーティングに参加するかどうかを確認します。

デバイスで参加確認機能を有効または無効にするには、この設定を使用します。

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 : 参加確認機能はオフになります。

True : Webex Assistant がアクティブになっていれば、参加確認機能を使用できます。

ユーザインターフェイス 予約 可視性 タイトル

ミーティングの詳細をプライベートに変更します。「ミーティングのスケジュール（Scheduled meeting）」というテキストがミーティングのタイトルとして表示されます。

必要なユーザ ロール： ADMIN、INTEGRATOR、USER

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto : ミーティングのタイトルが公開され、ユーザインターフェイスに表示されます。

Hidden : ミーティングのタイトルが非表示になり、ユーザインターフェイスには「ミーティングのスケジュール（Scheduled meeting）」と表示されます。

ユーザインターフェイス ブランディング アウェイク状態のブランディング 色

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。

ユーザインターフェイス 連絡先情報 タイプ

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)。

ユーザインターフェイス 診断 通知

ユーザインターフェイスに診断の通知を表示するかどうかを設定します。

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 : 診断の通知がユーザインターフェイスに表示されます。

Hidden : 診断の通知はユーザインターフェイスに表示されません。

ユーザインターフェイス キートーン モード

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。

ユーザインターフェイス 機能 コール 終了

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。

ユーザインターフェイス 機能 コール キーパッド

ユーザインターフェイスから、デフォルトの通話中の [キーパッド (Keypad)] ボタンを削除するかどうかを選択します。このボタンは、DTMF 入力などに使用できるキーパッドを開きます。

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。

ユーザインターフェイス 機能 コール Webexに参加

ユーザインターフェイスからデフォルトの [Webexに参加 (Join Webex)] ボタンを削除するかどうかを選択します。

このボタンを使用すると、ユーザは Webex ミーティング番号で Webex ミーティングにダイヤルインできます。ドメインは必要ありません。ただし、この機能を動作させるには、インフラストラクチャの設定で *@webex.com へのコールのルーティングを許可する必要があります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : 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。

ユーザインターフェイス 機能 コール 通話中制御

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

ユーザインターフェイス 機能 コール 音楽モード

ユーザインターフェイスで音楽モードのトグルボタンを表示するかどうかを選択します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Hidden

値のスペース: Auto/Hidden

Auto : この機能が対応中のコールでサポートされている場合、ユーザインターフェイスで音楽モードのトグルボタンを表示します。

Hidden : 音楽モードのトグルボタンは、ユーザインターフェイスに表示されません。

ユーザインターフェイス 機能 コール 開始

ユーザ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

ユーザインターフェイス機能通話ビデオミュート

ユーザインターフェイスにデフォルトの[ビデオをオフにする]ボタンを表示するかどうかを選択します。

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

自動 : この機能が継続的な通話でサポートされている場合、ユーザインターフェイスに[ビデオをオフにする]ボタンが表示されます。

非表示 : [ビデオをオフにする]ボタンはユーザインターフェイスに表示されません。

ユーザインターフェイス 機能 すべて非表示

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。

True : 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。

ユーザインターフェイス 機能 共有 開始

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。Cisco Proximity または Cisco Webex アプリを使用してコンテンツを共有することもできます。

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。

ユーザーインターフェイス ホワイトボード 開始

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。

ユーザインターフェイス 言語

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。

ユーザインターフェイス OSD 暗号化インジケータ

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。

ユーザインターフェイス OSD モード

クリーンなビデオストリームを出力するようにデバイスを設定できます。これはブロードキャストモードと呼ばれます。このモードでは、インジケータ、通知、およびコントロールが削除されます。このモードは、視聴者にビデオを配信したいだけのブロードキャストおよび録音サービスを目的としています。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Unobstructed

Auto : インジケータ、通知、およびコントロールがビデオストリーム（通常モード）に含まれます。

Unobstructed : インジケータ、通知、およびコントロールがビデオストリーム（ブロードキャストモード）から削除されます。名前ラベルは削除されません。

ユーザインターフェイス OSD 出力

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: 1

値スペース : 1

1 : 画面上の情報とインジケータをデバイスの内蔵画面に送信します。

ユーザインターフェイス 電話帳 モード

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。

ユーザインターフェイス プロキシミティ 通知

ユーザインターフェイスにプロキシミティの通知を表示するかどうかを設定します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Off/On

Auto : プロキシミティの通知を表示するタイミングをシステムが自動的に決定できるようにします。

Off : プロキシミティの通知はユーザインターフェイスに表示されません。

On : すべてのプロキシミティの通知がユーザインターフェイスに表示されます。

ユーザインターフェイス Qt 仮想キーボード

これは仮想キーボードのプレビュー機能です。今後のリリースでは、この xconfig が削除され、この機能が永続的に有効になります。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : False

値スペース : False/True

ユーザインターフェイス セキュリティ モード

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。

ユーザインターフェイス 設定メニュー モード

ユーザインターフェイス (タッチコントローラまたは画面上) 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。

ユーザインターフェイス 設定メニュー 可視性

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。

ユーザインターフェイス サウンドエフェクト モード

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 (ユーザインターフェイス キートーン モード 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。

ユーザインターフェイス壁紙

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。

ユーザインターフェイス ホワイトボード アクティビティインジケータ

アクティビティインジケータを使用すると、コール中に誰が描画し、注釈を付けているかを確認できます。

参加者がホワイトボードと対話しているときは、その参加者のアバターまたはデバイスの頭文字が表示されるため、誰が描画や注釈付けを行っているかを把握できます。

クラウド登録デバイスにのみ適用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

On : アクティビティインジケータを有効にします。

Off : アクティビティインジケータを無効にします。

ユーザインターフェイス ホワイトボード デフォルトテーマ

ホワイトボードのデフォルトのテーマを黒または白に変更します。

必要なユーザ ロール : ADMIN

デフォルト値 : Light

値スペース : Dark/Light

Dark : ホワイトボードのデフォルトの外観は黒です。誰かが自分とホワイトボードを共有している場合も黒です。

Light : ホワイトボードのデフォルトの外観は白です。誰かが自分とホワイトボードを共有している場合も白です。

ユーザ管理設定

ユーザ管理 LDAP 管理者 フィルタ

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))"

ユーザ管理 LDAP 管理者 グループ

この AD (Active Directory) グループのメンバーには、管理者権限が付与されます。この設定は、memberOf:1.2.840.113556.1.4.1941:=<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"

ユーザ管理 LDAP 属性

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。

ユーザ管理 LDAP ベースDN

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"

ユーザ管理 LDAP 暗号化

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、ユーザ管理 LDAP サーバ ポート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。

ユーザ管理 LDAP 最小TLSバージョン

LDAP で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。

ユーザ管理 LDAP モード

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。

ユーザ管理 LDAP サーバ アドレス

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。

ユーザ管理 LDAP サーバ ポート

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 (「ユーザ管理 LDAP 暗号化設定」を参照) 。

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。

ユーザ管理 LDAP サーバ証明書の検証

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) 。

ユーザ管理 パスワードポリシー 複雑度 数字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある数字 (0 ～ 9) の最小文字数を指定します。

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 ～ 4)

数字の最小文字数。0 は制限がないことを意味します。

ユーザ管理 パスワードポリシー 複雑度 最小文字数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、パスワードの最小文字数を指定します。

必要なユーザ ロール : ADMIN

デフォルト値 : 8

値スペース : 整数 (0 ～ 256)

文字の最小数。0 は制限がないことを意味します。

ユーザ管理 パスワードポリシー 複雑度 小文字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある小文字の最小文字数を指定します。

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 ～ 4)

小文字の最小文字数。0 は制限がないことを意味します。

ユーザ管理 パスワードポリシー 複雑度 特殊文字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある特殊文字の最小文字数を指定します。

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 ～ 4)

特殊文字の最小文字数。0 は制限がないことを意味します。

ユーザ管理 パスワードポリシー 複雑度 大文字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある大文字の最小文字数を指定します。

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 ～ 4)

大文字の最小文字数。0 は制限がないことを意味します。

ユーザ管理 パスワードポリシー 最大有効期間

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、パスワードが無効になるまでの最大日数を指定します。

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 ～ 7300)

最小日数。0 は制限がないことを意味します。

ユーザ管理 パスワードポリシー 再使用制限

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次回のパスワードの変更時に有効になります。

この設定は、再使用の制限 (n) を指定します。つまり、ユーザは、直前の n 個のパスワードを再使用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 : 12

値スペース : 整数 (0..24)

パスワードの最小数。0 は制限がないことを意味します。

ビデオ設定

ビデオ アクティブスピーカー デフォルトPIPポジション

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。

ビデオ デフォルトレイアウトファミリ ローカル

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。この設定は、デバイスに搭載された MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合にのみ適用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Equal/Overlay/Prominent/Prominent_L/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 : Grid 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。参加者は同じサイズのビデオのグリッド内に表示されます。共有コンテンツがある場合、それはグリッドの横に表示されます。

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が全画面で表示され、他の参加者はサムネイルで下部にオーバーレイ表示されます。コンテンツがある場合は、通話中のスピーカーがサムネイルで上部にオーバーレイされた状態でコンテンツが全画面表示で表示されます。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。

Prominent : [スタック (Stack)] 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共有コンテンツは大きい画像となり、他の参加者は小さい画像として上部に表示されます。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。

Prominent_L : [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が画面の左上部分に表示され、他の参加者は下部および右側の横に表示されます。

Single : Focus 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。

ビデオ デフォルトレイアウトファミリ ローカルコンテンツ

コンテンツ共有の開始時に、デフォルトでローカルで切り替えるビデオレイアウトファミリを選択します。この設定は、デバイスに搭載された MultiSite 機能（オプション）を使用してマルチポイントのビデオ会議をホストする場合にのみ適用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Equal/Overlay/Prominent/Prominent_L/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 : Grid 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。参加者は同じサイズのビデオのグリッド内に表示されます。共有コンテンツが、グリッドの横に表示されます。

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。共有コンテンツは、全画面表示で通話中のスピーカーがサムネイルで上部にオーバーレイされた状態で表示されます。

Prominent : [スタック（Stack）] 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。共有コンテンツは大きい画像となり、参加者は小さい画像として上部に表示されます。

Prominent_L : [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。コンテンツが画面の左上部分に表示され、参加者は下部および右側の横に表示されます。

Single : Focus 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。共有コンテンツは全画面表示で表示されます。参加者は表示されません。

ビデオ デフォルトレイアウトファミリ リモート

リモート参加者（遠く）に送信されるストリーミングで使用するビデオレイアウトファミリを選択します。この設定は、デバイスに搭載された MultiSite 機能（オプション）を使用してマルチポイントのビデオ会議をホストする場合にのみ適用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Equal/Prominent/Prominent_L/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 : Grid 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。参加者は同じサイズのビデオのグリッド内に表示されます。共有コンテンツがある場合、それはグリッドの横に表示されます。

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が全画面で表示され、他の参加者はサムネイルで下部にオーバーレイ表示されます。コンテンツがある場合は、通話中のスピーカーがサムネイルで上部にオーバーレイされた状態でコンテンツが全画面表示で表示されます。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。

Prominent : [スタック（Stack）] 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共有コンテンツは大きい画像となり、他の参加者は小さい画像として上部に表示されます。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。

Prominent_L : [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が画面の左上部分に表示され、他の参加者は下部および右側の横に表示されます。

Single : Focus 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。

ビデオ デフォルトメインソース

コールのメインビデオのデフォルト入力ソースを定義します。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、メインビデオがこのソースで再生されます。デバイスの実行中に別のソースに変更するには、Video Input SetMainVideoSource コマンドを使用します。

必要なユーザ ロール : admin、user

デフォルト値: 1

値スペース : 1

メインビデオのデフォルトソース。

ビデオ 入力 コネクタ [n] カメラ制御 カメラID

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: 1

値スペース : 1
カメラ ID は固定されており、変更できません。

ビデオ 入力 コネクタ [n] カメラ制御 モード

n: 1..2

このビデオ入力コネクタに接続されているカメラを制御するかどうかを定義します。
カメラ制御はコネクタ 2 （HDMI）では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 : On Connector 2 : Off

値スペース : Connector 1 : Off/On Connector 2 : Off
Off : カメラ制御を無効にします。
On : カメラ制御を有効にします。

ビデオ 入力 コネクタ [n] CEC モード

n: 2.. 2

ビデオ入力 (HDMI) は、Consumer Electronics Control (CEC) をサポートします。この設定を有効にすると、接続デバイスの情報 (デバイスの種類やデバイス名) がビデオ会議デバイスのステータスで使用可能になります (Video Input Connector[n] ConnectedDevice CEC [n]) 。ただし、接続デバイスは CEC もサポートすることが条件となります。

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 : CEC が無効です。
On : CEC が有効になります。

ビデオ 入力 コネクタ [n] 入力ソースタイプ

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。

ビデオ 入力 コネクタ [n] 名前

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 1 : "Camera" Connector 2 : PC

値スペース : 文字列 (0, 50)
ビデオ入力コネクタの名前。

ビデオ 入力 コネクタ [n] 最適鮮明度 プロファイル

n: 1..2

この設定は、対応するビデオ入力コネクタ [n] 画質設定が 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。

ビデオ 入力 コネクタ [n] 最適鮮明度 しきい値 60 fps 設定を使用し、60 fps が許可される最小解像度を設定します。このしきい値を下回ると、30 fps が最大フレームレートになります。

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。

ビデオ 入力 コネクタ [n] 最適鮮明度 しきい値 60 fps

n: 1..2

各ビデオ入力について、この設定は 60 fps で送信できる最低解像度をデバイスに通知します。これより低い解像度すべてについて、最大送信フレーム レートは 30 fps となります。使用可能な帯域幅が適切であれば、これより高い解像度で 60 fps も可能です。

必要なユーザ ロール : ADMIN

デフォルト値 : 1920_1080

値スペース : 512_288/768_448/1024_576/1280_720/1920_1080/Never

512_288 : 512x288 にしきい値を設定します。

768_448 : 768x448 にしきい値を設定します。

1024_576 : 1024x576 にしきい値を設定します。

1280_720 : 1280x720 にしきい値を設定します。

1920_1080 : 1920 X 1080 にしきい値を設定します。

Never : 60 fps を送信するしきい値を設定しません。

ビデオ 入力 コネクタ [n] 推奨解像度

n: 2..2

ビデオ会議デバイスに HDMI 経由でシステムに接続した入力ソース (例 : ラップトップ) の解像度として通知されている推奨の画面解像度と更新間隔を定義します。ソース デバイス (例、ラップトップのディスプレイ構成ソフトウェア) によって手動でオーバーライドされない限り、ソース側の解像度の選択するためのロジックは、自動的にこの解像度とリフレッシュ レートを選択します。

1920_1080_60 より大きい形式では特に大量のデータが使用されるため、少なくとも HDMI 1.4b データレートに対応したプレゼンテーションケーブル (またはアダプタ) が必要です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : 1920_1080_60

値スペース : 1920_1080_60/2560_1440_60/3840_2160_30

1920_1080_60 : 解像度は 1920 X 1080、リフレッシュ レートは 60 Hz です。

2560_1440_60 : 解像度は 2560 X 1440、リフレッシュ レートは 60 Hz です。

3840_2160_30 : 解像度は 3840 X 2160、リフレッシュ レートは 30 Hz です。

ビデオ 入力 コネクタ [n] プレゼンテーションの選択

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 : AutoShare

値スペース : 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。

ビデオ 入力 コネクタ [n] 画質

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 : Sharpness

値スペース : Motion/Sharpness

Motion : できるだけ高いフレーム レートにします。高いフレームレートが必要な場合に使用します (通常、画像の動きがある場合) 。

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。

ビデオ入力コネクタ [n] RGB 量子化範囲

n: 2..2

ビデオ入力に接続されたデバイスは CTA-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 CTA-861-F 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 CTA-861-F 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 CTA-861-F で規定されています。

ビデオ 入力 コネクタ [n] 可視性

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 （コネクタ 1 : 表示しない コネクタ2 : 入力信号がある場合）

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。

ビデオ出力コネクタ [n] 解像度

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。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : 3840_2160_60

値スペース : 3840_2160_60

3840_2160_60 : 解像度は 3840 x 2160、リフレッシュ レートは 60 Hz です。

ビデオ プレゼンテーション デフォルトPIPポジション

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。

ビデオ プレゼンテーション デフォルトソース

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 : 1/2

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。

ビデオ プレゼンテーション 優先順位

プレゼンテーションチャネルとビデオチャネル間でどのように帯域幅を分配するかを指定します。

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。

ビデオ セルフビュー デフォルト フルスクリーンモード

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 (ビデオ セルフビュー デフォルト モードの設定を参照) 。

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。

ビデオ セルフビュー デフォルト モード

コール後、およびコール中にビデオがオフになって再度オンになった後に、メインビデオソース (セルフビュー) を画面に表示する必要があ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、ビデオ セルフビュー デフォルト PIP ポジションとビデオ セルフビュー デフォルト フルスクリーンモード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 : コール退出時や、コール中にビデオをオンにした後も、セルフビューがオフになります。

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。コール中にビデオをオンにした後も同様です。

On : コール退出時や、コール中にビデオをオンにした後も、セルフビューがオンになります。

ビデオ セルフビュー デフォルト 表示先モニタロール

コールの後にメイン ビデオ ソース (セルフビュー) を表示する画面/出力を設定します。この値は、異なる出力用に設定されたビデオ出力 コネクタ [n] モニタロール設定のモニタ ロールを反映します。

この設定は、セルフ ビューが全画面で表示されたとき、およびセルフビューがピクチャインピクチャ (PiP) で表示されたときの両方に適用されます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/First/Second

Current : コールを中止すると、セルフビュー画像がコール中と同じ出力上に維持されます。

First : セルフビュー画像は、ビデオ出力 コネクタ [n] モニタロールが First に設定された出力上に表示されます。

Second : セルフビュー画像は、ビデオ出力 コネクタ [n] モニタロールが Second に設定された出力上に表示されます。

ビデオ セルフビュー デフォルト PIP ポジション

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 (ビデオ セルフビュー デフォルト モード設定を参照) 、全画面表示がオフになっている場合 (ビデオ セルフビュー デフォルト フルスクリーン モード設定を参照) 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。

ビデオ セルフビュー オンコール モード

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、ビデオ セルフビュー オンコール 期間設定で定義します。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 : Off

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。

ビデオ セルフビュー オンコール 期間

この設定はビデオ セルフビュー オンコール モード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。

音声制御の設定

音声制御 ウェイクワード モード

この設定を使用して、Webex Assistant で使用されるウェイクワード（「OK Webex」など）を有効または無効にします。Webex Assistant では、デバイスのハンズフリーを使用できます。ウェイクワードを使用すると、コールの発信やプレゼンテーションの開始などのタスクを開始できます。

ユーザインターフェイス アシスタント モード設定を使用して Webex Assistant をオンにします。

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：ウェイクワードの使用を無効にします。

On：ウェイクワードの使用を有効にします。

Web エンジン設定

Webエンジン 機能 WebGL

WebGL (Web Graphics Library) は、Web ブラウザでプラグインを使用せずにインタラクティブな 2D グラフィックや 3D グラフィックをレンダリングするための Javascript API です。

WebGL は試験的な機能であり、将来変更される可能性があります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

On : WebGL が有効になります。

Off : WebGL が無効になります。

Web エンジン 機能 SIP URL ハンドラ

この設定により、Web ビューベースの機能 (Web アプリ、デジタルサイネージなど) から直接 SIP コールを開始できます。ユーザは SIP:yourSipUrl というラベルの付いたボタンを選択してコールを開始し、そのコールはデバイスによって発信されます。

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 : Web ビューからの SIP コールの開始は無効になります。

On : Web ビューからの SIP コールの開始は有効になります。

Web エンジン 最小 TLS バージョン

Web エンジンで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 : TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0 : TLS バージョン 1.0 以降のサポート。

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。

Web エンジン モード

Web エンジンは、デジタルサイネージや Web アプリなど、デバイスの Web ビューを使用する機能が動作するための前提条件です。

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 : Web エンジンが無効になります。

On : Web エンジンが有効になります。

Web エンジン リモートデバッグ

Web ページに問題が発生した場合は、リモート デバッグをオンにすることを推奨します。リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

使用後は、必ずリモート デバッグをオフにしてください。

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 : リモート デバッグがオフに切り替わります。

On : リモート デバッグがオンに切り替わります。

Web エンジン Http プロキシの使用

サービスの通信に HTTP プロキシを使用するかどうかを指定できるように、いくつかの [Httpプロキシの使用 (UseHttpProxy)] 設定が用意されています。[Webエンジン Httpプロキシの使用 (WebEngine UseHttpProxy)] 設定は、デジタルサイネージ、API 駆動型 Web ビュー、Web アプリなど、Web ビューベースのすべての機能に適用されます。

この設定を有効にするには、[ネットワークサービス HTTP プロキシ (NetworkServices HTTP Proxy)] 設定を使用して、HTTP、HTTPS、および WebSocket トラフィック用のプロキシサーバをセットアップ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 : サーバとの直接通信をセットアップします (プロキシを使用しません) 。

On : プロキシ経由の通信をセットアップします。

Webex の設定

Webex クラウドプロキシミティ ゲスト共有

この設定では、devices.webex.com 経由でゲスト共有機能をオフに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 : Auto

値スペース : Auto/Off

Auto : ゲストの共有を許可するかどうかをシステムが自動的に判断できるようにします。これは、現在デフォルトでは有効になっています。

Off : ゲスト共有機能をオフにします。

Webex クラウドプロキシミティ モード

オンプレミスのコールマネージャに登録され、Webex Edge for Devices にリンクされたデバイスは、超音波、Wi-Fi 検出、ゲスト共有のようなペアリングメカニズムを処理するためにオンプレミスとクラウド両方のプロキシミティモードをサポートします。この設定では、使用する 2 つのプロキシミティモードを定義できます。

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 : リンクされたデバイスは、オンプレミスのプロキシミティモードを使用します。

On : リンクされたデバイスはクラウドのプロキシミティモードを使用します。

Webex クラウドアップグレード モード

オンプレミスサービスに登録され、Webex Edge for Devices にリンクされているデバイスでは、オンプレミスのプロビジョニングサービスまたは Webex クラウドサービス (クラウド管理のソフトウェアのアップグレード) からソフトウェアをアップグレードするかどうかを選択できます。

クラウド管理のソフトウェアのアップグレードでは、新しい RoomOS ソフトウェアバージョンが利用可能になると、デバイスは自動的にアップグレードされます。これは、クラウドに登録されたデバイスのアップグレードと同時です。デバイスを手動でアップグレードする必要なく、最新の更新とバグ修正をより速く取得できます。

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 : デバイスソフトウェアはクラウドからアップグレードされません。CUCM などのオンプレミスのプロビジョニングサービスを使用するか、または手動アップグレードを使用する必要があります。

On : クラウドで新しいソフトウェアバージョンが利用可能になると、デバイスソフトウェアは自動的にアップグレードされます。

Webex Meetings 参加プロトコル

オンプレミスのサービスに登録され、Webex Edge for Devices にリンクされているデバイスは、Webex Meetings へのコールに Webex クラウドサービスを使用する場合があります。Webex を介したコールでは、高度なミュート、共同ホスト、転送ホスト、顔認識など、一連のネイティブ Webex Meetings インコール機能を利用できます。

Webex Meetings のコールルーティングが使用される場合は次のとおりです。[Webex に参加 (Join Webex)] ボタンを使用する場合、Webex Assistant を使用してパーソナルルームミーティング (PMR) に参加する場合、および @webex.com、@*.webex.com、および @meet.ciscospark.com のいずれかのドメインを含む URI で [コール (Call)] ボタンまたはダイヤル API コマンドを使用する場合。他のコールは、デフォルトプロトコルに使用します。

また、ネイティブの Webex Meetings コールルーティングでは、デバイスがクラウド管理のソフトウェアのアップグレードに対して有効で、Control Hub からの設定が有効で、会議マルチポイントモードが Auto に設定されている必要があります。

CE 9.15.0 では Room Panorama と Room 70 Panorama はサポートされていません。

必要なユーザ ロール : ADMIN

デフォルト値: SIP

値スペース : SIP/Webex

SIP : コールプロトコルは SIP です。

Webex : 上記の要件を満たしている場合、コールプロトコルは Webex です。それ以外の場合は、SIP です。

WebRTC の設定

WebRTC コール終了タイムアウト

これは CE9.15.3 ではサポートされません。WebRTC ミーティングで [コールの終了 (End Call)] を押して Web ビューを閉じるまでの時間を延長できます。通常動作では、この設定を変更する必要はありませんが、トラブルシューティングに役立つ場合があります。

WebRTC は、Microsoft Teams ミーティング Web アプリで Microsoft Teams ミーティングに参加する場合に使用されます。WebRTC は、オンプレミスのサービスに登録され、Webex Edge for Devices にリンクされているデバイス、および Webex クラウドサービスに登録されているデバイスでのみ使用できます。

必要なユーザ ロール : ADMIN

デフォルト値 : 2

値スペース : 整数 (0..600)

秒単位の時間。

WebRTC 対話モード

これは CE9.15.3 ではサポートされません。WebRTC ミーティングでは、デバイスのコール制御または WebRTC アプリのネイティブコントロールを使用できます。

WebRTC は、Microsoft Teams ミーティング Web アプリで Microsoft Teams ミーティングに参加する場合に使用されます。WebRTC は、オンプレミスのサービスに登録され、Webex Edge for Devices にリンクされているデバイス、および Webex クラウドサービスに登録されているデバイスでのみ使用できます。

必要なユーザ ロール : ADMIN

デフォルト値 : 非インタラクティブ (NonInteractive)

値スペース : インタラクティブ (Interactive) /非インタラクティブ (NonInteractive)

Interactive : WebRTC アプリのネイティブコントロールをデバイスのタッチスクリーンから直接使用できます。これにより、ネイティブの WebRTC 機能にアクセスできます。

NonInteractive : WebRTC アプリのネイティブコントロールは利用できません。デバイスの通常のコール制御のみ使用できます。

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

Webex Board の使用方法

Webex Board とその使用方法の詳細については、*ユーザガイド*を参照してください。

通話中やビデオプレゼンテーションの音量は変えることができます。画面の下部をタップし、スライダーを使用して音量を調節します。

ボードにタッチコントローラが接続されている場合は、タッチコントローラで追加機能が利用できます。

デバイス名またはアドレスをタップすると、[設定 (Settings)] にアクセスできます。ここには、[デバイス情報 (Device Information)]、[詳細設定 (Advanced Settings)]、[ネットワーク設定 (Network settings)]、[デバイスのアクティベーション (Device activation)]、[着信音 (Ringtone)]、[再起動 (Restart)]、および [工場出荷時設定へのリセット (Factory reset)] の設定があります。

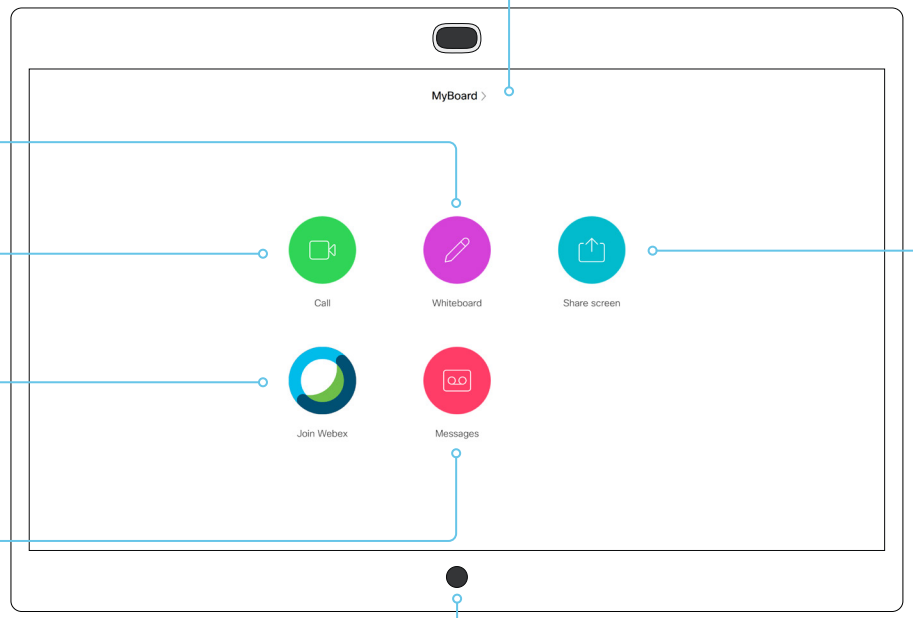
[ホワイトボード (Whiteboard)] をタップすると、新しいホワイトボードを開始するか、既存のホワイトボードのリストにアクセスすることができます。

[コール (Call)] をタップすると、コールを発信できます。

[Webexに参加 (Join Webex)] をタップして、Webex ミーティングに参加します。

[メッセージ (Messages)] をタップしてボイスメールを呼び出します (該当する場合) 。

[ホーム (Home)] ボタンをタップすると、ホーム画面に戻ります。ボタンを押し続けると、ボードがスタンバイモードになります。

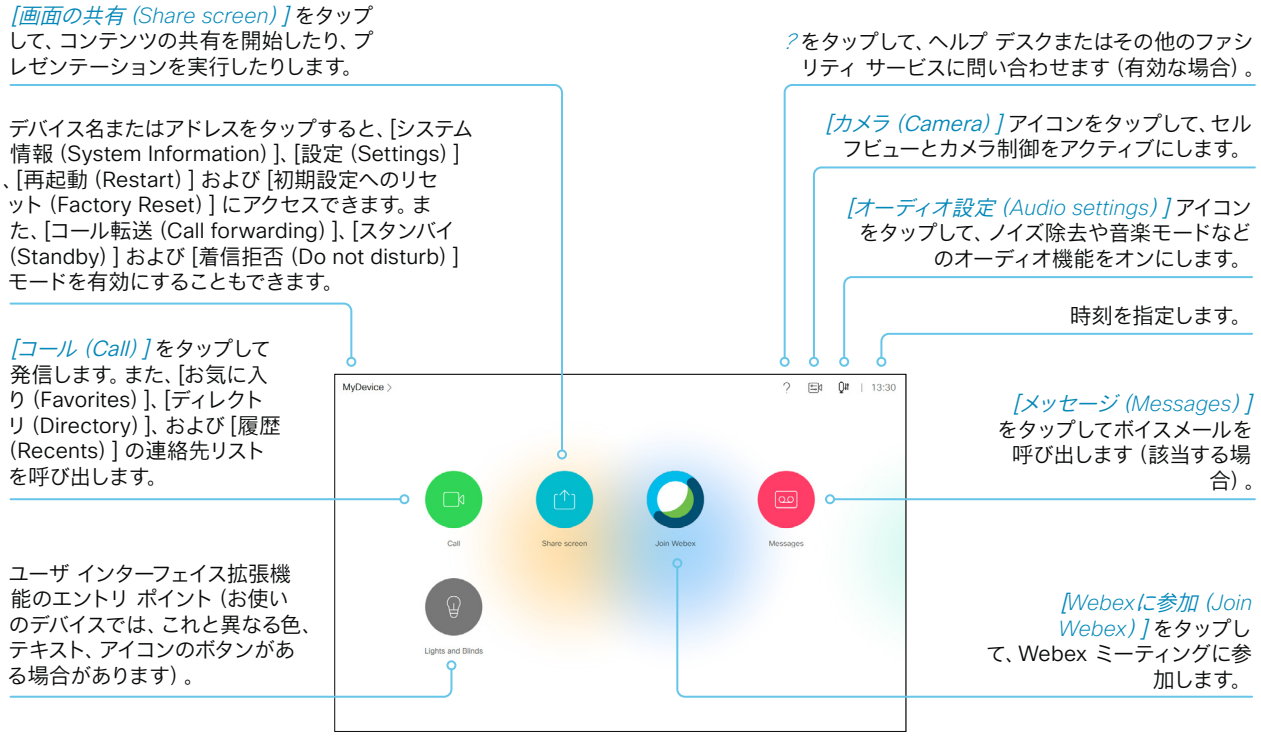


[画面の共有 (Share screen)] をタップすると、共有オプションが表示されます。

タッチコントローラの使用方法

タッチコントローラ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ーガイドを参照してください。

すべての機能がすべての製品で利用できるとは限りません。そのため、ここに示されているタッチボタンは、お使いのデバイスでは表示されない場合があります。



音量コントロール *およびミュート*

スピーカーの音量を下げるには音量ボタンの左側を押し続け、音量を上げるには右側を押し続けます。

[ミュート (Mute)] ボタンを押して、マイクをミュート/ミュート解除します。

Room Navigator :

- 音量コントロールはタッチスクリーンにあります。
- ミュートボタンはコール中にのみ表示されます。

Touch 10 :

- 音量コントロールとミュートボタンはタッチスクリーンの下にあります

リモート モニタリングのセットアップ

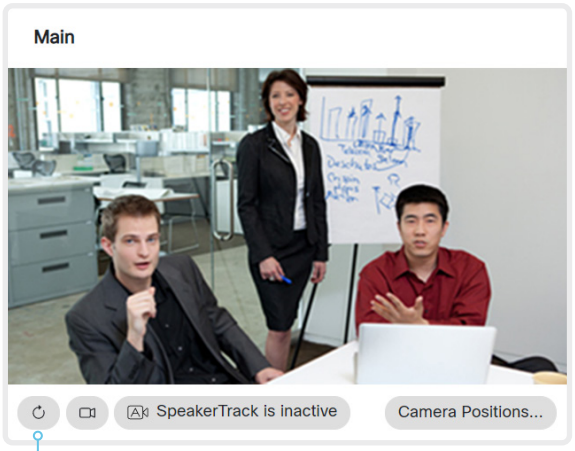
要件:

- *[リモート モニタリング (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 Web 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. Web インターフェイスにサインインして、*[ソフトウェア (Software)]* に移動し、*[オプションキー (Option Keys)]* を選択します。
2. *[RemoteMonitoring] が [インストールされたオプションキー (Installed Option Keys)]* のリストにあ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、►「オプションキーの追加」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

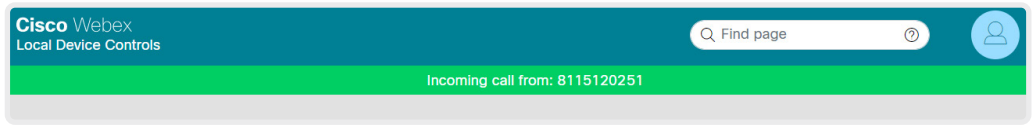
通話中の場合、遠端カメラからのスナップショットも表示できます。これは、相手先デバイスでリモート モニタリング オプションが設定されているかどうかとは関係がありません。

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。

Web 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

Web ページの上部にある緑のバナーは、着信コールについて通知するため、またデバイスがコール中であることを表示するためにあります。

デバイスがアイドル状態の場合、緑のバナーはありません。



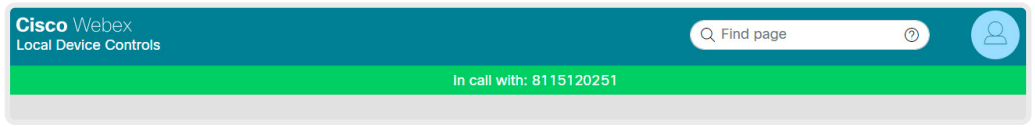
着信通知

緑のバナーをクリックして *[コール (Call)]* ページを開きます。ここで、コールの応答または拒否を行うことができます。

コールの操作

[コール (Call)] 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



デバイスがコール中

デバイスがコール中である場合は緑のバナーが表示されます。 また、デバイスに複数のアクティブコールがある場合にも表示されます。

Web インターフェイスを使用したコールの発信 (1/2 ページ)

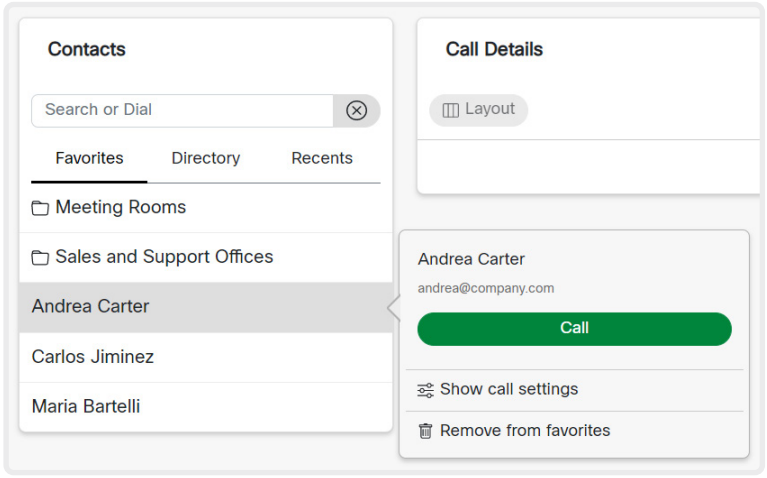
Web インターフェイスにサインインして、*[コール (Call)]* に移動します。

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。

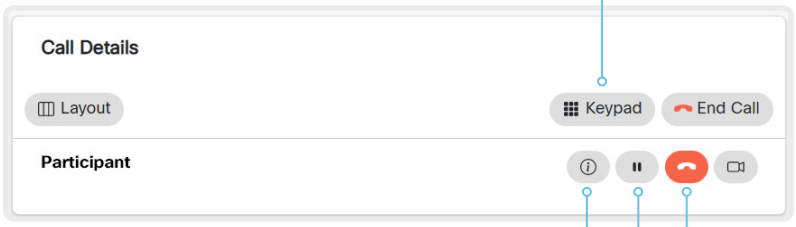
または、*[検索して発信 (Search and Dial)]* フィールドに完全な URI または番号を入力します。次に、URI または番号の横に表示される *[コール (Call)]* ボタンをクリックします。



* 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。

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

コールまたは会議を終了する場合は、*[コールの終了 (End Call)]* をクリックします。表示されるダイアログで選択内容を確認します。

1 人の参加者のみコールを終了するには、その参加者の 📞 ボタン をクリックします。

Web インターフェイスを使用したコールの発信 (2/2 ページ)

Web インターフェイスにサインインして、*[コール (Call)]* に移動します。

複数の相手に発信

ポイントツーポイントのビデオ コール (2 者間限定のコール) を拡張して、音声専用でもう 1 人の参加者を増やすことができます。

オプションで搭載される MultiSite 機能をデバイスで使用している場合は、自身を含めて最大 4 人までビデオ コール (会議) に参加できます。

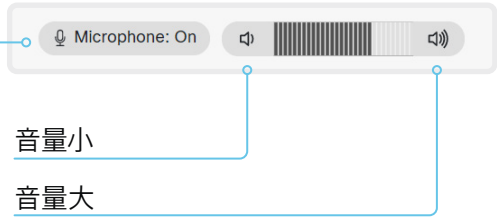
最初の参加者を呼び出したときと同じ手順で、次の会議参加者を呼び出してください。

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。



Web インターフェイスを使用したコンテンツの共有

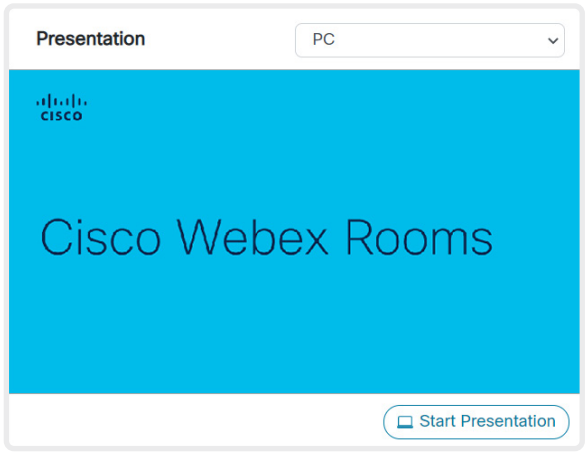
Web インターフェイスにサインインして、*[コール (Call)]* に移動します。

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の停止 (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

デバイスのビデオ入力にプレゼンテーションソースを接続できます。ほとんどの場合は PC がプレゼンテーションソースとして使用されますが、デバイスの設定によっては他のオプションを使用できる場合があります。

通話中に、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。

相手先カメラの制御

Web インターフェイスにサインインして、*[コール (Call)]* 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)] > [遠端制御 (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。
- 相手先カメラでスピーカートラッキングが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。

ルーム分析 (ページ 1 / 2)

ルーム分析機能は、会議室からのいくつかの変数を使用します。また、それらの変数を再利用して、時間経過やコールのたびに部屋の使用率を分析します。

以下に示す設定を見つけるには、Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

ステータスを確認するには、*[設定 (Settings)]* に移動し、*[ステータス (Statuses)]* を選択します。

人の存在の検出

このデバイスは、人が室内にいるかどうかを見つける機能を備えています。室内に人がいるかどうかを検知するには最低 2 分かかります。部屋が空室になった後、ステータスを変更するまで最大 2 分かかることがあります。

この機能は、超音波に基づいています。室内にいた人物の記録を保持することはなく、人が部屋にいたかどうかだけを検知します。

Web インターフェイスから人の存在の検出をオンまたはオフにできます。*[ルーム分析 (RoomAnalytics)] > [人の存在の検出 (PeoplePresenceDetector)]* 設定を使用します。

人数のカウント

顔検出を使用して、デバイスで室内の人数を特定できます。室内にいた人物の記録を保持することはなく、顔の平均数だけを検知します。カメラに顔を向けていない人はカウントされません。室内に物体や写真がある場合、これらも顔として検知され、カウントされる可能性があります。

信頼性の高い平均数を得るために、コール時間の長さは最低 2 分必要です。2 分未満のコールと人数のカウントが無効にされたコールでは、通話履歴を取得すると「N/A」が表示されます。

デフォルトでは、デバイスはコール中またはセルフビュー画像を表示しているときにのみ人数をカウントします。

非通話中の人をカウントするように選択できます。オンにすると、デバイスは、デバイスがスタンバイ モードでない場合に人数をカウントします。セルフ ビューがオフであっても、これは非通話中の人数を含みます。

[ルーム分析 (RoomAnalytics)] > [非通話中の人をカウント (PeopleCountOutOfCall)] 設定を使用します。

ステータス

人の存在および人のカウントに関する特定の瞬間のステータスを確認することができます。*[ルーム分析 (RoomAnalytics)]* のステータスを確認します。

診断

タッチコントローラから SpeakerTrack 診断モードを有効にすると、画面上で実況される人数のカウンタを見ることができます。セルフビューをオンにし、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タップして、*[設定 (Settings)]* メニューを開きます。*[問題と診断 (Issues & diagnostics)]* をタップし、*[SpeakerTrack の診断 (SpeakerTrack diagnostics)]* をオンにします。

別の方法として、ボードのテクニカルサポート画面を開くこともできます (ボードの画面に 1 本の指を置いたままホームボタンを 3 回押します) 。次に、[デバイス (Device)] タブの *[ハードウェア診断 (Hardware diagnostics)]* をクリックし、*[ベストオーバービューのデバッグ (BestOverview debug)]* をオンにします。

通話履歴コマンド

コール後に、通話履歴コマンドから人々の平均数の値を抽出できます。

- xCommand CallHistory Get DetailLevel: Full

通話履歴コマンドは、API (Application Programming Interface) から使用できます。詳細については、お使いの製品の API リファレンス ガイドを参照してください。

▶ https://www.cisco.com/go/board-docs

ルーム分析 (ページ 2 / 2)

環境ノイズ レポート

このデバイスでは、室内の定常環境雑音レベルをレポートできます。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。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。

この値はノイズレベルの異常な変化の検出に使用できます。このような変化は、室内で仕事をしている人にとっては不快なノイズを引き起こす場合があります。施設管理はこの問題をトラブルシューティングするために迅速に介入できます。

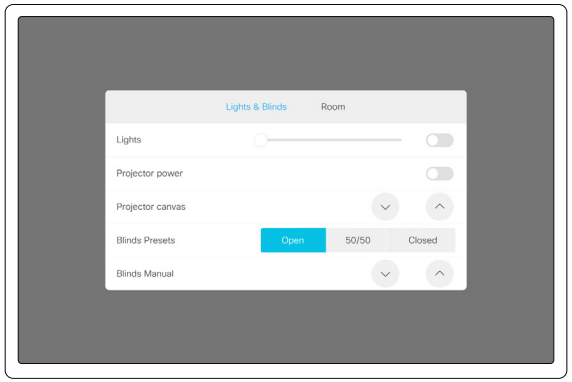
Web インターフェイスから周囲ノイズの検出をオンまたはオフにできます。*[ルーム分析 (RoomAnalytics)] > [環境雑音の予測 (AmbientNoiseEstimation)] > [モード (Mode)]* 設定を使用します。

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タッチ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

ボードにタッチコントローラが接続されている場合、カスタムパネルとアクションボタンは、ボード自体ではなくタッチコントローラに表示されます。Web アプリは常にボードに表示されます。

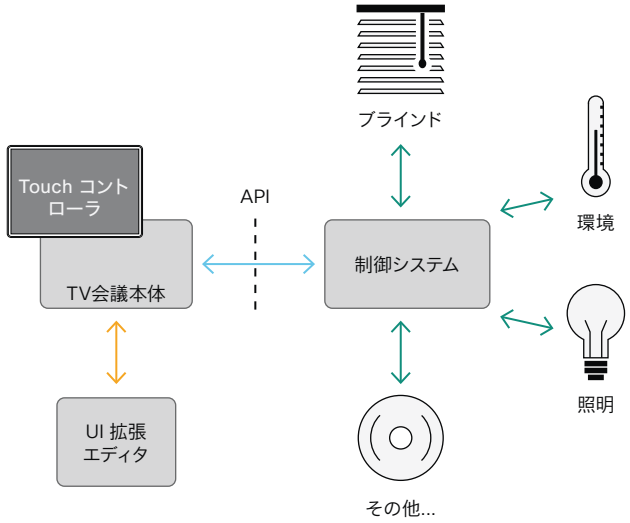
UI 拡張エディタ (以前の室内制御エディタ) を使用してカスタムユーザーインターフェイスパネル、アクションボタン、および Web アプリを設計する方法、およびビデオ会議デバイスの API を使用してコントロールとアクションをプログラミングする方法の詳細については、カスタマイズガイドを参照してください。次のリンクからアクセスできます。

► 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。カスタムユーザーインターフェイス拡張機能 (アクションボタン、Web アプリ、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*して、*[UI拡張エディタ (UI Extensions Editor)]* に移動します。

- デバイスの Web インターフェイスでエディタが直接開きます。

  新しいパネル、アクションボタン、または Web アプリ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ーインターフェイスで確認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。

-  をクリックしてプレビューを開始します。

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、アロー関数、promise および class 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。次のリンクからアクセスできます。

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

デバイスでのマクロの使用許可

Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

- [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*して、*[マクロエディタ (Macro Editor)]* に移動します。

これにより、デバイスの Web インターフェイスに組み込まれているマクロエディタが開きます。スタンドアロンのエディタは提供していません。

* 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。

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。

カスタマイゼーション

ユーザインターフェイスからのデフォルトボタンの削除

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ボタンを削除するには、次の設定を使用します (ボード自体とタッチコントローラの両方に適用されます) 。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。

- [ユーザーインターフェイス (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。コール中に表示される、参加者の *[追加 (Add)]* ボタンもタッチコントローラから削除されます。
- *[ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [Webexに参加 (JoinWebex)]*: Webex ミーティングに参加するためのデフォルトのボタンを削除します。
- *[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。
- *[ユーザーインターフェイス (UserInterface)] > [機能 (Features)] > [ホワイトボード (Whiteboard)] > [開始 (Start)]*: デフォルトの [コール (Call」)] 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)] > [ビデオミュート (VideoMute)]*: デフォルトの *[ビデオをオフにする (Turn video off)]* ボタンを削除します。
- *[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)] > [通話中のコントロール (MidCallControls)]*: 通話中の *[保留 (Hold)]*、*[保留解除 (Resume)]*、および *[転送 (Transfer)]* ボタンをタッチコントローラから削除します。
- *[ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [音楽モード (MusicMode)]*: デバイスの音楽モードを有効にするトグルボタンを削除します。音楽モードは、マイクが音楽をキャプチャする必要がある場合に便利です。
- *[ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [キーパッド (Keypad)]*: 通話中の [キーパッド (Keypad)] ボタンを削除します。このボタンは、DTMF 入力に使用できるキーパッドを開きます。
- *[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。

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。

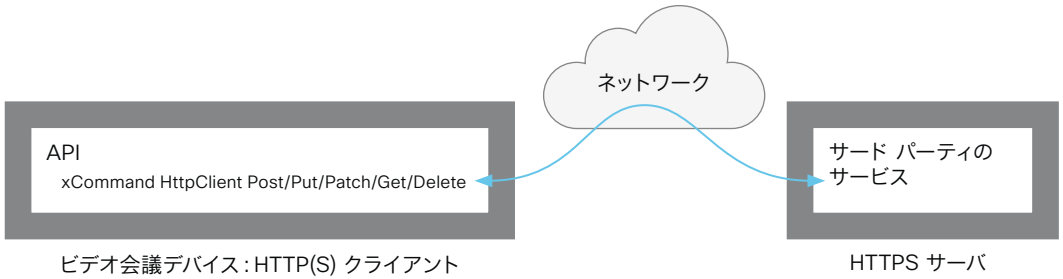
解説場所

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。 次のリンクからアクセスできます。

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

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 はホスト名追加表現を許容します : <HTTP(S) サーバのホスト名または IP アドレスに一致する正規表現>**
- **xCommand HttpClient Allow Hostname Clear**
- **xCommand HttpClient Allow Hostname List**
- **xCommand HttpClient Allow Hostname Remove Id: <リスト内のエントリーの ID>**

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 <メソッド>
 [AllowInsecureHTTPS: <True/False>]
 [Header: <ヘッダーテキスト>]
 [ResponseSizeLimit: <最大応答サイズ>]
 [ResultBody: <None/PlainText/Base64>]
 [Timeout: <タイムアウト時間>]
 Url: <要求の送信先 URL>
```

<メソッド> 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。 次のリンクからアクセスできます。

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

Web ビュー ベースの機能

デジタル サイネージ

デジタル サイネージを使用すると、デバイスがハーフウェイク状態のときにカスタム コンテンツ (Web ページ) を表示できます。デジタル サイネージは、広告コンテンツを表示してブランドを宣伝するだけでなく、訪問者や社内の従業員情報、ダッシュボード、またはカレンダーを表示するのに最適な方法です。

ユーザーは、リンクのクリックやフォームへのテキスト入力など、画面上のコンテンツの操作を行うことができます。

カスタムコンテンツは、ハーフウェイク状態の従来の背景画像と情報を置き換え、常にフルスクリーンで表示されます。Web ウィンドウまたはタブ 1 つのみがサポートされます。Web ページが新しいウィンドウまたはタブでページを開こうとすると、現在のページは置き換えられます。

キャッシュ、Cookie、ローカル ストレージなどのデータは、デバイスの再起動時に自動的に消去されることはありません。データを削除するには、ストレージ削コマンドを使用する必要があります。

- xCommand WebEngine DeleteStorage [Type: Webengine]

Web ページがサポートされていない場合、デバイスはすぐに通常のハーフウェイク モードになります。

デジタル サイネージのセットアップ

1. Web インターフェイスにサインインして、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
2. *[Webエンジン (WebEngine)] > [モード (Mode)]* を [オン (On)] に設定して、Web エンジンを有効にします。
3. *[スタンバイ (Standby)] > [サイネージ (Signage)] > [モード (Mode)]* を [オン (On)] に設定して、デジタル サイネージを有効にします。
4. *[スタンバイ (Standby)] > [サイネージ (Signage)] > [URL (Url)]* に、表示する Web ページの URL を入力します。
5. Web ページは、デバイスがスタンバイ モードになる前に表示されます。Web ページの表示時間を決定するには、次の設定を使用します。

   [スタンバイ (Standby)] > [モード (Mode)]: Off に設定すると、デバイスはスタンバイ モードになりません (非推奨) 。On に設定すると、[スタンバイ (Standby)] > [遅延 (Delay)] がタイム アウトしたときにデバイスがスタンバイ モードになります。

   [スタンバイ (Standby)] > [遅延 (Delay)]: デバイスがスタンバイ モードになるまでに Web ページを表示する時間 (分単位) を定義します。

   [スタンバイ (Standby)] > [モーション検知復帰 (WakeUpOnMotion Detection)]: On に設定すると、人が室内に入ったときにデバイスが自動的にスタンバイから復帰して Web ページを表示します。Off に設定すると、人が室内に入ってもデバイスは影響を受けません。

その他のデジタル サイネージ設定 :

- 音声が含まれる Web ページで音声を再生するかどうかを決定します。

  [スタンバイ (Standby)] > [サイネージ (Signage)] > [音声 (Audio)]
- Web ページとの対話を許可するかどうかを決定する。

  [スタンバイ (Standby)] > [サイネージ (Signage)] > [対話モード (InteractiveMode)]
- Web ページを一定の間隔で強制的に更新する。これは、Web ページが自動更新されない場合に便利です。

  [スタンバイ (Standby)] > [サイネージ (Signage)] > [更新間隔 (RefreshInterval)]

Web エンジン

Web ビュー ベースの機能はすべて、Web エンジンを使用しています。このため、Web ビュー ベースの機能を使用するには、Web エンジンが有効になっている必要があります。

Web エンジンは、V8 JavaScript を使用した Chromium/Qt WebEngine に基づいています。Chromium バージョンは定期的に更新されますが、Chrome ラップトップ バージョンよりも古いバージョンである可能性があります。

次の機能はサポートされていません。PDF、WebGL WebRTC、パスワード マネージャー、プラグイン、ファイルのダウンロードとアップロード、通知。

リモート デバッグ

Web ページに問題が発生した場合は、リモート デバッグをオンにすることができます。

[Webエンジン (WebEngine)] > [リモートデバッグ (RemoteDebugging)]

リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

プロキシの使用

Web ビューベースの機能で HTTP プロキシを使用するようにデバイスを設定できます。

[ネットワークサービス (NetworkServices)] > [HTTP] > [プロキシ (Proxy)]

さらに、次の設定をオンにする必要があります。

[Webエンジン (WebEngine)] > [Httpプロキシの使用 (UseHttpProxy)]

Web ビュー ベースの機能

Web アプリ

Web アプリは、ユーザーがデバイスのホーム画面からアクセスできる Web ページまたはアプリケーションです。Web アプリは通話中でない場合にのみ使用できます。

Web アプリはフルスクリーンで起動し、15 分間使用されないとタイムアウトします。Web アプリは対話型にすることもできます。

キャッシュ、Cookie、ローカルストレージなどのデータは、セッションが終了すると自動的に消去されます。

Web アプリを作成するには、デバイスの Web インターフェイスから利用できる *UI 拡張エディタ*を使用する必要があります。エディタでは、ホーム画面で使用されるラベルとアイコンも設定できます。デフォルトでは Web ページのアイコンが使用されますが、代わりに別のアイコンを選択することもできます。

アイコンの詳細：

- 形式： .ico、.png、.jpg、svg、または .gif
- アイコンサイズ：最小 60 × 60 ピクセル、最大 1200 × 1200 ピクセル

代表的なアプリとして、Office 365、Trello、Wikipedia、YouTube のほか、社内の Web ページやツールがあります。

解説場所

Web アプリの作成方法の詳細については、カスタマイズガイドを参照してください。 次のリンクからアクセスできます。

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

Web アプリの作成

1. Web インターフェイスにサインイン* して、*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。
2. [Webエンジン (WebEngine)] > [モード (Mode)] を **[オン (On)]** に設定して、Web エンジンを有効にします。
3. *[UI 拡張エディタ (UI Extensions Editor)]* に移動します。デバイスの Web インターフェイス上で直接エディタが開きます。
4. *[新規 (New)]* をクリックし、Web アプリの *[追加 (Add)]* ボタンを選択します。
5. 右側のバーに Web アプリのプロパティを入力します。
   - Id：アプリの一意識別子。
   - 名前 (Name) ：ホーム画面に表示されるボタンのラベル。
   - Web アプリの URL：Web アプリの URL。
   - Web アプリアイコンの URL (オプション) ：ホーム画面のボタンのアイコンです。
6. 上部のバーにあるエクスポートボタン をクリックして、設定をデバイスにアップロードします。

   これで、新しい Web アプリのボタンがホーム画面に表示されます。

ラベルとアイコンを持つ Web アプリボタン

* 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 ユーザーロールを持つユーザーが必要です。

Web エンジン

Web ビュー ベースの機能はすべて、Web エンジンを使用しています。このため、Web ビューベースの機能を使用するには、Web エンジンが有効になっている必要があります。

Web エンジンは、V8 JavaScript を使用した Chromium/Qt WebEngine に基づいています。Chromium バージョンは定期的に更新されますが、Chrome ラップトップ バージョンよりも古いバージョンである可能性があります。

次の機能はサポートされていません。PDF、WebGL WebRTC、パスワード マネージャー、プラグイン、ファイルのダウンロードとアップロード、通知。

リモート デバッグ

Web ページに問題が発生した場合は、リモートデバッグをオンにすることができます。

[Webエンジン (WebEngine)] > [リモートデバッグ (RemoteDebugging)]

リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

プロキシの使用

Web ビューベースの機能で HTTP プロキシを使用するようにデバイスを設定できます。

[ネットワークサービス (NetworkServices)] > [HTTP] > [プロキシ (Proxy)]

さらに、次の設定をオンにする必要があります。

[Webエンジン (WebEngine)] > [Httpプロキシの使用 (UseHttpProxy)]

Web ビュー ベースの機能

API 駆動型の Web ビュー

Web ビューは、API コマンドを使用して開いたり閉じたりすることができます。インテグレータは、サードパーティ統合またはマクロを作成するときに、これらのコマンドを使用できます。インテグレータは、外部イベントに基づいて読み込む URL を決定します。たとえば、企業の重要な通知を表示できます。

Web ビューは全画面表示になっており、15 分後にタイムアウトになるか、または API コマンドをコールしてビューを閉じます。

Web ビューを開く：

- xCommand UserInterface WebView Display Url: <url>

Web ビューを閉じる：

- xCommand UserInterface WebView Clear

キャッシュ、Cookie、ローカル ストレージなどのデータは、セッションが終了すると自動的に消去されます。

インテグレータは、API 駆動型 Web ビュー、マクロ、およびタッチコントローラのカスタムボタンを組み合わせることで、タッチスクリーンのないデバイス向けにも対話型のソリューションを作成できます。タッチコントローラのボタンをタップすると、メイン画面にさまざまな Web ビューが表示されます。たとえば、基本的なヘルプ ページを開いて参照したり、説明ビデオを表示したりできます。

Web エンジン

Web ビュー ベースの機能はすべて、Web エンジンを使用しています。このため、Web ビュー ベースの機能を使用するには、Web エンジンが有効になっている必要があります。

Web エンジンは、V8 JavaScript を使用した Chromium/Qt WebEngine に基づいています。Chromium バージョンは定期的に更新されますが、Chrome ラップトップ バージョンよりも古いバージョンである可能性があります。

次の機能はサポートされていません。PDF、WebGL WebRTC、パスワード マネージャー、プラグイン、ファイルのダウンロードとアップロード、通知。

リモート デバッグ

Web ページに問題が発生した場合は、リモート デバッグをオンにすることができます。

[Webエンジン (WebEngine)] > [リモートデバッグ (RemoteDebugging)]

リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

プロキシの使用

Web ビューベースの機能で HTTP プロキシを使用するようにデバイスを設定できます。

[ネットワークサービス (NetworkServices)] > [HTTP] > [プロキシ (Proxy)]

さらに、次の設定をオンにする必要があります。

[Webエンジン (WebEngine)] > [Httpプロキシの使用 (UseHttpProxy)]

プレゼンテーションソースの構成 (1/2 ページ)

デバイスの API を使用して、単一のビデオ ストリームに最大 4 つのプレゼンテーション ソースを結合できます。*

組み合わせることのできるプレゼンテーション ソースの最大数はデバイスによって異なります。

ビデオ会議デバイス	組み合わすことができる異なる入力ソースの最大数
Room Kit、Room Kit Mini、SX20、MX200 G2、MX300 G2、Board	2
Codec Plus、Room 55、Room 55 Dual、Room 70、Desk Pro	3
SX80、MX700、MX800、Codec Pro、Room 70 G2、Room Panorama*、Room 70 Panorama*	4
SX10、DX70、DX80	利用不可

ケーブル (デバイスに応じて DVI、VGA、HDMIなど) 経由で共有されているソースのみを共有できます。

ソース構成

構成レイアウト

2 つのレイアウトから選択できます。

- 同等 (Equal)
- プロミネント (Prominent)

ソースの数は、コール時と非コール時どちらであっても、いつでも変更できます。画像サイズは修正できません。

ソースが画面に表示される順序は、コマンド内の順番に従います。表示は左上から始まり、右下が最後になります。

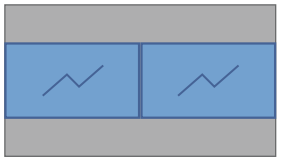
オン デマンドによる構成およびレイアウトの変更

プレゼンテーションソース構成は API コマンドを使用してのみ利用可能です。専用のユーザ インターフェイスは提供されません。

構成とレイアウトをオン デマンドで簡単に変更できるようにするには、マクロを使用してカスタムのユーザ インターフェイス パネル (UI 拡張機能) を作成することを推奨します。

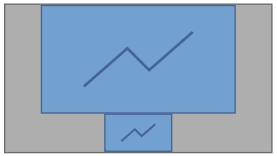
レイアウト

同等 (Equal)



ソースの数 : 2

プロミネント (Prominent)



ソースの数 : 2

* Panorama デバイスでは、メインカメラに 2 つの入力ソースを使用します。

プレゼンテーションソースの構成 (2/2 ページ)

API コマンド

xCommand Presentation Start ConnectorId: <1..n>
PresentationSource: <1..n>
Instance: <New, 1..n>
Layout: <Equal, Prominent>
SendingMode: <LocalRemote, LocalOnly>

値は次のとおりです。

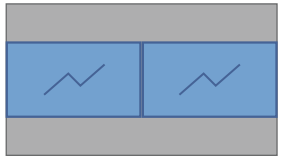
入力ソースは、接続されている物理コネクタ（ConnectorId）、または論理ソース識別子（PresentationSource）のどちらかによって識別可能です。同じコマンド内で異なる識別子を使うことはできません。ConnectorId または PresentationSource のうち片方のみを使用してください。

これらの識別子は、[ビデオ入力コネクタ（Video Input Connector）] および [ビデオ入力ソース（Video Input Source）] のステータスで見つけることができます。

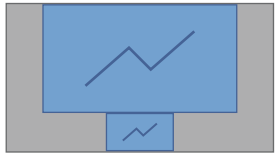
詳細については、API ガイドを参照してください。

例

xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal



xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent



スタートアップスクリプトの管理

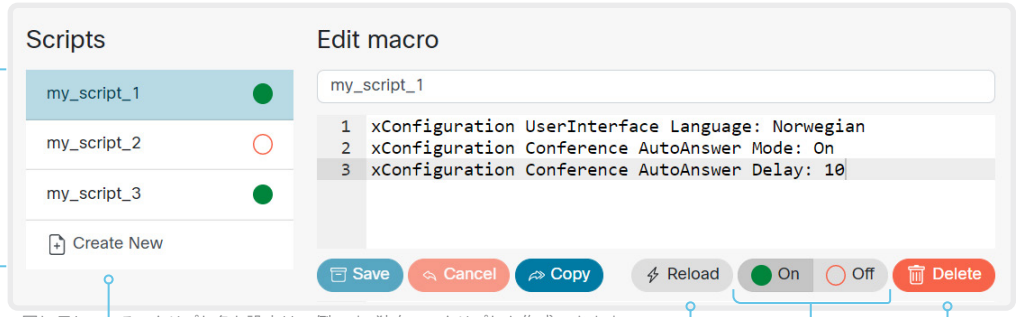
Web インターフェイスにサインインして、*[開発者 API (Developer API)]* に移動します。*[スタートアップスクリプト (Startup Scripts)]* カードを見つけて、*[エディタの起動 (Launch Editor)]* をクリックします。

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。



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。

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. *[再ロード (Reload)]* 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

注：この機能は廃止され、今後のリリースで削除されます。代わりにマクロを使用することをお勧めします。

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

Web インターフェイスにサインインして、*[開発者 API (Developer API)]* に移動します。

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、Web 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、Web 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。

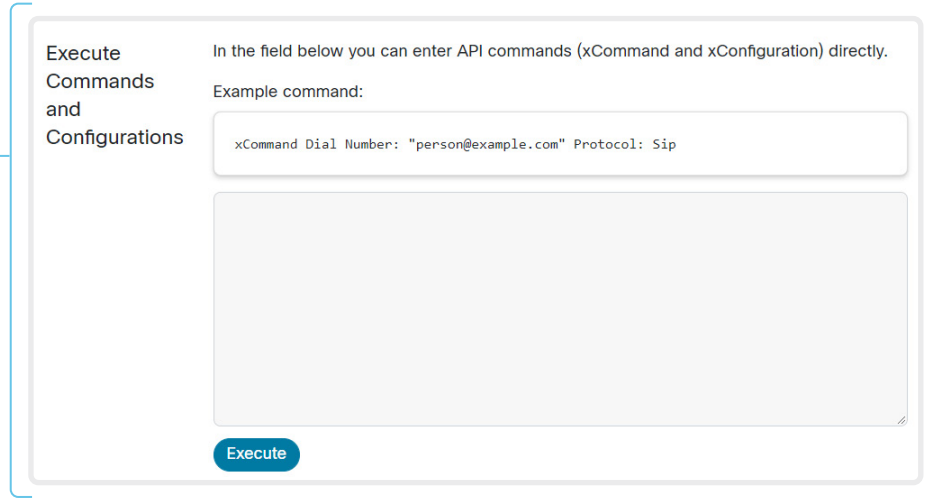
Web インターフェイスからの API コマンドとコンフィギュレーションの実行

Web インターフェイスにサインインして、*[開発者 API (Developer API)]* に移動します。

コマンド (xCommand) および設定 (xConfiguration) は、Web 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

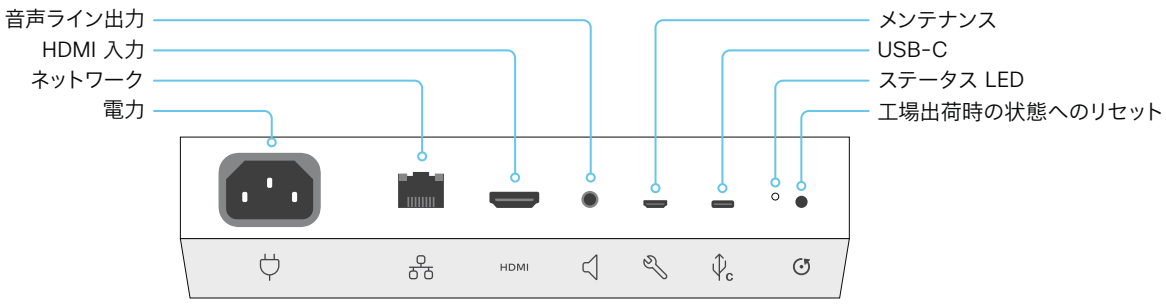
1. テキスト領域に、コマンド (xCommand または xConfiguration) またはコマンド シーケンスを入力します。
2. [実行 (Execute)] をクリックしてコマンドを発行します。



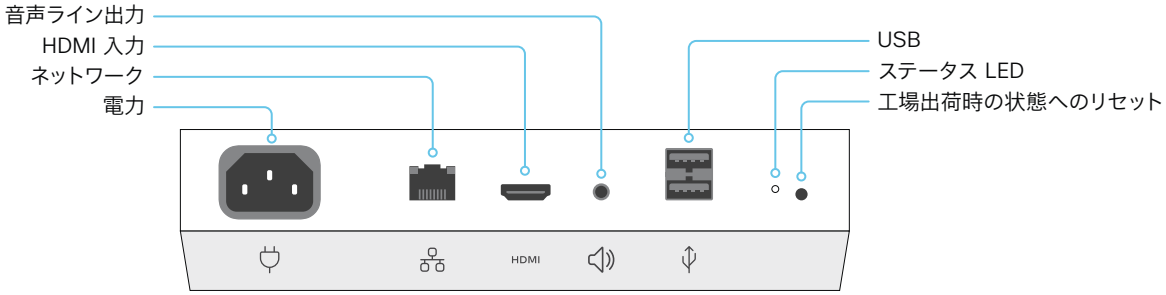
API について

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。

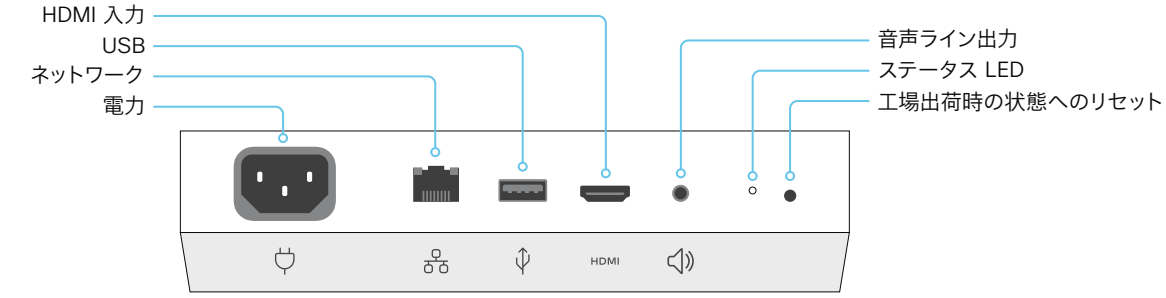
コネクタ パネル



Webex Board 55S、70S、および 85S [1]



Webex Board 55



Webex Board 70

電源

- Board 55S：100 ～ 240 VAC、3.0 ～ 1.5 A、50/60 Hz
- Board 70S：100 ～ 240 VAC、3.5 ～ 2.0 A、50/60 Hz
- Board 85S：100 ～ 240 VAC、4.6 ～ 2.0 A、50/60 Hz
- Board 55、70：100 ～ 240 VAC、最大 3.5 A、50/60 Hz

ネットワーク

- イーサネット インターフェイス、10 Mb/100 Mb/1 Gb のイーサネット LAN インターフェイス (RJ45) 。[2]

HDMI 入力

- HDMI バージョン 1.4b、最大解像度は 30 fps で 3840 × 2160。コンピュータまたは外部再生デバイス用。高解像度とフレーム レートをサポートするハイスピード HDMI 1.4b ケーブルが必要です。Cisco 認定プレゼンテーション ケーブルをお勧めします。

音声ライン出力

- 3.5 mm ミニジャック、3 ピンコネクタ。

USB

- Board 55：メンテナンス用 USB 2.0 タイプ A X 2
- Board 70：メンテナンス用 USB 2.0 タイプ A X 1
- Board 55S、70S、および 85S：メンテナンス用マイクロUSB
- Board 55S、70S、および 85S：USB-C

工場出荷時の状態へのリセット

- 工場出荷時設定へのリセット用ピンホール。工場出荷時設定へのリセットは、可能であればタッチユーザーインターフェイスまたは Web インターフェイスから行うことをお勧めします。

[1] 第 2 世代の Webex Board ファミリ (*S シリーズ*) では、ハードウェアプラットフォームにマイナーな最適化が施されています。

[2] すべてのモデルで Wi-Fi もサポートされます。

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、タッチコントローラ、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。これらのポートはタッチ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[1] / Room 55 Dual[1]	2	1 ( )
Room 70 G2[1]	4	2 (、PoE)
Room 70 Panorama[1] / Room Panorama[1]	4	2 (、PoE)
Codec Plus	2	1 ( )
Codec Pro	4	2 (、PoE)
Board	0	0
Desk Pro[2]	1	0
SX10	0	0
SX20	0	0
SX80	2	0
MX200 G2 / MX300 G2	2	0
MX700[1, 3] / MX800[1, 3]	2	0
DX70[2] / DX80[2]	1	0

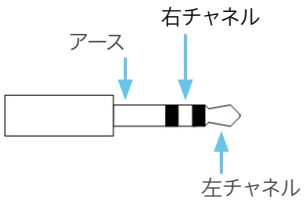
[1] この製品の 1 つ以上の補助ポートは、内部使用のために予約されています。

[2] この製品の補助ポートはネットワーク拡張ポートです。コンピュータやその他のデバイスをこのポートに接続して、ビデオ会議デバイスと同じネットワーク/LAN にアクセスできます。このポートは周辺機器には使用されず、コーデックからローカル IP アドレスが割り当てられることはありません。

[3] この製品には個別の 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 インジェクタはタッチコントローラに使用されます。

ミニ端子コネクタのピン配列方法

3.5 mm ミニ端子、3 極 （ライン出力）



オーディオコネクタ（ミニジャック）	
	出力回線
コネクタのピン配列	チップ = 左チャネル リング = 右チャネル シールド = GND
信号タイプ	アンバランス
コネクタ（コーデック）	ミニ端子 3.5 mm、 3 コンダクタ
入力インピーダンス	なし
出力インピーダンス	470 Ohm
最大入力レベル	なし
最大出力レベル	8.2 dBu ±2 dB
ファントム電源	なし
ファントム電源抵抗のピン「tip」	なし
ファントム電源抵抗のピン「ring 1」	なし
周波数応答	20 Hz ～ 20 kHz ±1 dB
信号対雑音比	-100 dB

Webex Board 55S、70S、および 85S のメンテナンス用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[1]。

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。

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

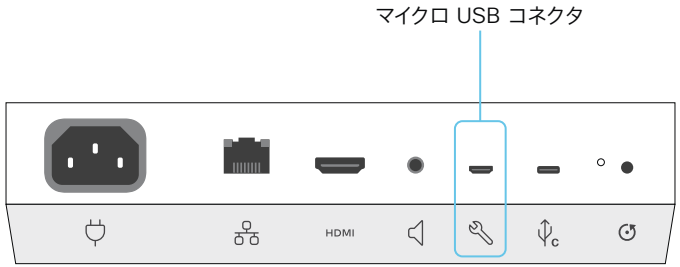
シリアル通信はデフォルトでイネーブルになっています。動作を変更するには、次の設定を使用します。

[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。



Webex Board 55S、70S、および 85S

1. USB ケーブルをコンピュータからボードのマイクロ USB ポートに接続します。

   コンピュータに USB - シリアルポートデバイスが 2 つ表示されます。名前はコンピュータのオペレーティングシステムによって異なります。Linux では通常、カメラが /dev/ttyUSB0、メインが /dev/ttyUSB1 になります。

   これらのポートは、2 つの CPU のネイティブシリアルインターフェイス (UART) に接続されています。ブートローダからのログを含む、システムからこのポートに印刷されたすべてのものを表示します。

2. 起動完了後にサインインプロンプトが表示されたら、管理者の資格情報でログインします。カメラ CPU ではなく、メイン CPU にしかログインできません。

   サインイン後、ボードの API にアクセスすることができます。

   ボードが工場出荷時設定にリセットされている場合は、admin と空のパスワードでサインインします。

[1] CP210x USB - UART ブリッジ仮想 COM ポート (VCP) ドライバが必要です。▶ http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers を参照してください

Webex Board 55 および 70 のメンテナンス用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[1]。

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。

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

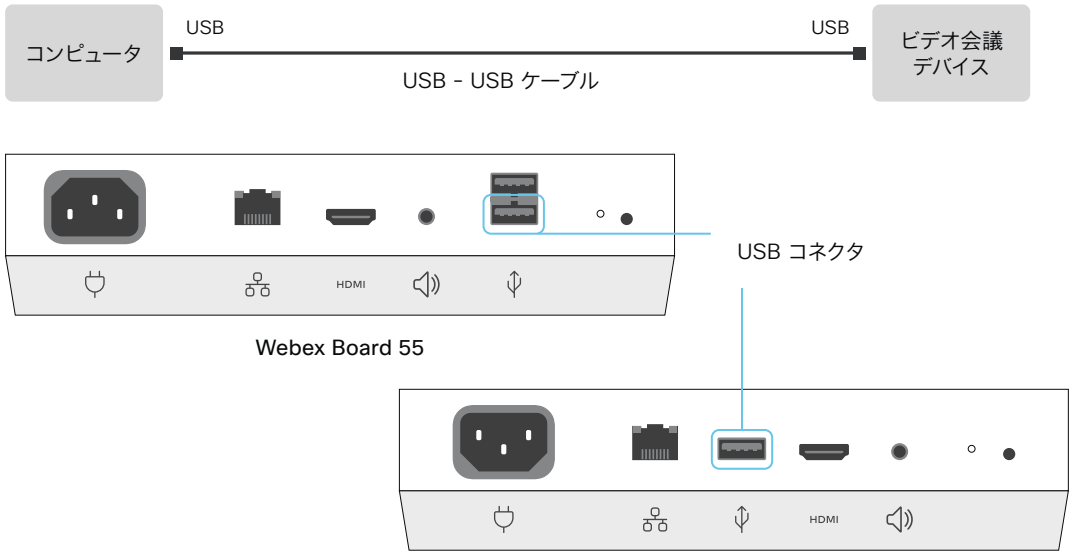
シリアル通信はデフォルトでイネーブルになっています。動作を変更するには、次の設定を使用します。

[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。



1. USB ケーブルをコンピュータからボードの USB-A ポートに接続します。Webex Board 55 では、パネルに最も近い USB ポートを使用してください。
2. ボードの電源を入れます。コンピュータに仮想シリアルポートが表示されます。名前はコンピュータのオペレーティングシステムによって異なります。Linux では、通常は /dev/ttyACM0 になります。

   注: コンピュータを接続する前にボードの電源を入れた場合、コンピュータでボードを認識することはできません。
3. サインインプロンプトが表示されたら、管理者の資格情報を使用してログインします。サインイン後、ボードの API にアクセスすることができます。

   ボードが工場出荷時設定にリセットされている場合は、admin と空のパスワードでサインインします。

[1] CP210x USB - UART ブリッジ仮想 COM ポート (VCP) ドライバが必要です。▶ http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers を参照してください

TCP ポートの開放

コーデック内の Web 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ます。

デバイスの Web インターフェイスからデバイスの設定を構成できます。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。*[設定 (Settings)]* に移動し、*[設定 (Configurations)]* を選択します。

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 4043 : リモート ペアリング ソフトウェアのダウンロード

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

TCP 4045 : リモート ペアリング バージョン情報

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

TCP 4047 : リモート ペアリング セッション接続

このポートは、Touch パネルがビデオ会議デバイスとリモート ペアリングされている場合にのみ使用可能 (オープン) です。Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

TCP 4051 : リモートペアリングポート (廃止)

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

TCP 4053 : リモート ペアリング ポート

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

TCP 4062 : リモートペアリングポート

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

TCP 4190 : UPnP ポート

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。

NetworkServices UPnP Mode: Off

TCP 5060/5061 : SIP リッスン ポート

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

TCP 65533 : プロキシミティ接続用代替ポート

このポートはデフォルトで閉じられています。プロキシミティで代替ポートを有効にする設定を True にすると、このポートがプロキシミティ接続用に開放されます。

Proximity AlternatePort Enabled: False/True

エフェメラル IP ポート

エフェメラル IP ポート範囲 : 32768 ～ 60999

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 ステータスには失敗したことが示され、障害のタイプを示す診断メッセージが表示されます。

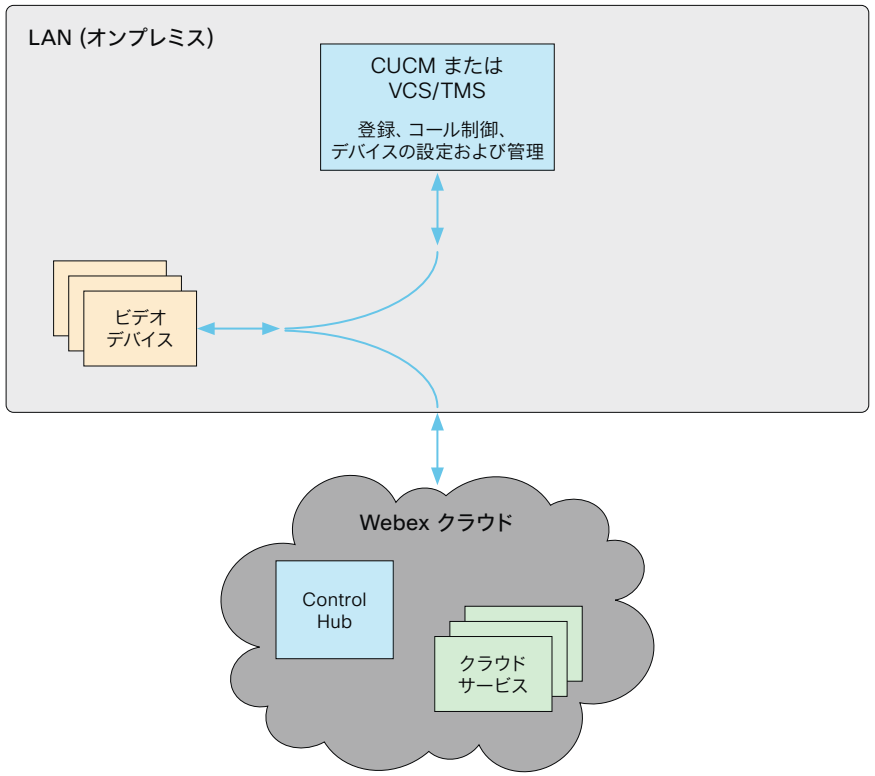
メッセージの再送を試みる際、TMS での通話詳細記録 (CDR) の紛失が生じます。

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。

オンプレミス登録デバイスの Cisco Webex Edge for Devices へのリンク

Webex Edge for Devices を使用すると、オンプレミス登録のデバイスを Webex クラウドサービスにリンクできます。これにより、登録、デバイスの設定管理、通話[1]、メディアサービスはオンプレミスのままで、特定のクラウド機能にアクセスできるようになります。Webex Control Hub でクラウドサービスを管理したり、デバイスの診断を受けたりできます。



設定

最初にデバイスをオンプレミスサービスに登録してから、Webex Edge にリンクすることをお勧めします。デバイスを *Webex Edge for Devices* にリンクする方法については、Webex ヘルプセンターで▶Webex Edge for Devices (https://help.webex.com/cy2l2z/) に関する記事を参照してください。

機能

Webex Edge for Devices には次の機能があります。

- Control Hub でのオンライン/オフライン接続ステータス
- 管理者アラートの設定に対応したデバイス診断
- デバイスの履歴分析を Control Hub で直接使用可能
- Control Hub からのデバイス設定へのアクセス
- クラウド xAPI アクセス
- Webex コールに参加する場合のリアルタイムメディアメトリック
- Control Hub からのログの管理
- Control Hub によるハイブリッド予定表[2]
- Webex Assistant (音声駆動型の仮想アシスタント)

前述の *Webex Edge for Devices* の記事には、使用できる機能と制限事項の最新の一覧が含まれています。

前提条件

- CE ソフトウェアの暗号化されたバージョン
- CUCM バージョン 12.5su1、または最新のデバイスパックを適用した 11.5.x
- Control Hub の管理者アクセス権
- Cisco Webex Device Connector (Webex Egde へのリンクを設定するため)
- クラウド サービス ライセンス(シスコ コラボレーション フレックス プラン)

[1] Webex Meetings へのコールに Webex クラウドサービスを使用するようにデバイスを設定できます。詳細については、Webex ヘルプセンターで ▶Webex Edge for Devices 用のネイティブ Webex Meetings (https://help.webex.com/c31fqg/) に関する記事を参照してください。

[2] TMS ベースの予約は無視されます。

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。

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。

アクティベーションコードの作成

Cisco Webex にデバイスを登録するには、アクティベーションコードが必要です。

共有モードのデバイス :

管理者は Control Hub 上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。

共有モードのデバイス用のアクティベーションコードを作成する方法については、▶Cisco Webex ルームデバイスまたは Cisco Webex Board 用のワークスペースの作成とサービスの追加（https://help.webex.com/1mqb9cb/）に関する記事を参照してください。

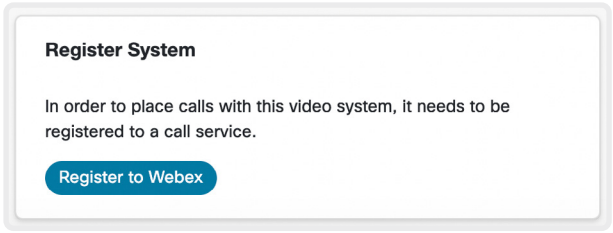
パーソナルモードのデバイス :

Cisco Webex Settings (https://settings.webex.com) から、管理者でなくてもアクティベーションコードを取得できます。

パーソナルモードでデバイス用のアクティベーションコードを作成する方法については、▶Webex Board、Room または Desk Device のパーソナルデバイスとしての設定（https://help.webex.com/n3alqtv/）に関する記事を参照してください。

1. Web インターフェイスにサインインして、*[ホーム (Home)]* に移動します。*[システムの登録 (Register System)]* カードを見つけます。

   このカードは、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. *[Webex に登録 (Register to Webex)]* をクリックします。
3. ポップアップが表示され、アクティベーションコードを入力できます。

   形式:

   - *xxxx-xxxx-xxxx-xxxx*、または
   - *xxxxxxxxxxxxxxx*

4. 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 5321 Simple Mail Transfer Protocol
- 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』

最小帯域幅の計算

最小帯域幅の要件は、技術仕様で指定されています。デュアルストリームを使用する場合、使用可能な帯域幅は 2 つのストリームに分割されます。

デュアルストリームで希望の解像度の最小帯域幅を計算するには、その解像度の最小ビットレート (bps) を 2 倍します (720p30 など)。

たとえば、解像度 720p30 に対して最低 768 kbps の帯域幅がある場合、デュアルストリームの最小帯域幅は 768 × 2、または 1536 kbps になります。

技術仕様 (1/2 ページ)

ソフトウェアの互換性
- Cisco Collaboration Endpoint Software Version 9.8 以降
- RoomOS

コンポーネント
すべてユニットに組み込み:
- マルチタッチ LED ディスプレイ
  - **Webex Board 55/55S: 55 インチ**
  - **Webex Board 70/70S: 70 インチ**
  - **Webex Board 85S: 85 インチ**
- 4K カメラ
- 12 のマイクロフォンアレイ
- スピーカー
- ホワイトボードペン

取り付けオプション:
- フロアスタンド (自立型または壁面固定型)
- 壁面取り付け

オプションのハードウェアコンポーネント:
- HDMI プレゼンテーションケーブル 8 m/26.2 フィート
- ペンキット (ペン 2 本のと交換用ペン先 6 個)

ディスプレイ
Webex Board 55/55S:
- エッジ LED LCD、55 インチ、4K、350 ニット、16:9
- 視野角: +/- 89 度 (全方向)
- 色数: 10 億 7 千万 (10 ビット)
- コントラスト: 1:4000
- 応答時間: 8 ミリ秒

Webex Board 70/70S:
- エッジ LED LCD、70 インチ、4K、300 ニット、16:9
- 視野角: +/- 88 度 (全方向)
- 色数: 10 億 7 千万 (10 ビット)
- コントラスト: 1:4000
- 応答時間: 6 ミリ秒

Webex Board 85S:
- ダイレクト LED LCD、85 インチ、4K、300 ニット、16:9
- 視野角: +/- 89 度 (全方向)
- 色数: 10 億 7 千万 (10 ビット)
- コントラスト: 1:4000
- 応答時間: 6.5 ミリ秒

ユーザーインターフェイス
- 静電容量方式タッチ
- オプティカルボンディングの保護ガラス
- マルチタッチ

カメラの概要
- 固定焦点レンズ
- 4Kp60
- F 値: 2.8
- 水平視野角 83°
- 垂直視野角 55°
- カメラの取り付け傾斜: -25 度

オーディオシステム
- 12 素子マイクアレイ (インテリジェントな音声トラッキング機能付き)
- 統合型音声最適化スピーカー

音声機能
- 高品質 20-kHz 音声
- アコースティック エコー キャンセレーション
- オートゲインコントロール (AGC)
- オートノイズリダクション
- アクティブリップシンク
- インテリジェントな音声トラッキング機能付きマイクロフォンアレイ

帯域幅要件
- 最小帯域幅:
  - **720p30、768 kbps ~**
  - **1080p30、1.72 Mbps ~**
- 最大帯域幅:
  - **送信: 4.3 Mbps**
  - **受信: 10 Mbps**

プレゼンテーション機能
- 最大 4K のローカルプレゼンテーション
- HDMI 音声

ライブビデオ解像度 (エンコード/デコード)
- メインビデオ:
  - **最大 1920 × 1080@30 (HD1080p)**
- プレゼンテーションの共有
  - **最大 1920 × 1080@30 (HD1080p)**

入力と出力
- HDMI 入力 X 1:
  - **最大 4K (3840 × 2160) までのフォーマットに対応**
  - **フレームレート: 1080p まで 60 fps、2160p では 30 fps**
  - **Extended Display Identification Data (EDID)**
- 3.5 mm ミニジャック音声出力 (ライン出力)
- 初期設定リセット ピンホール
- イーサネット

Webex Board 55:
- USB 3.0 X 2 (サービス)

Webex Board 70:
- USB 3.0 X 1 (サービス)

Webex Board 55S/70S/85S:
- USB-C (今後の使用)
- USB micro (保守用)

ネットワーク インターフェイス
- イーサネット (RJ-45) 100/1000 Mbps X 1
- Wi-Fi: 802.11a/b/g/n、802.11ac (2.4 および 5 GHz)
- Bluetooth® 対応
- IPv4 DHCP/スタティック
- 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)
- Network Time Protocol (NTP)
- HTTP プロキシサポート (メディアでなくシグナリング用)
- サポートされる TLS プロキシの検査
- Cisco Discovery Protocol (CDP)
- 802.1X ネットワーク認証 (パスフレーズまたは X.509 クライアント証明書)
- 802.1Q 仮想 LAN
- 802.1p (QoS およびサービスクラス (CoS))

ユーザーコントロール
- Cisco Webex Board をタッチスクリーンから直接制御する、Webex アプリを使用する、または Cisco Webex Room Navigator (Webex Board 55/70 ではサポートされない) または Cisco Touch 10 コントローラを使用する

言語サポート
- CE9.8 では、英語、スペイン語、ドイツ語、フランス語、フランス語 (カナダ) 、ポルトガル語、日本語、チェコ語、デンマーク語、オランダ語、スウェーデン語、スペイン語 (南米) 、イタリア語、フィンランド語、ポーランド語、トルコ語
- 今後のソフトウェアリリースで追加言語がサポートされる可能性あり

サポートされるインフラストラクチャ
- Cisco Unified Communications Manager 10.5.2 以降
- Cisco TelePresence Video Communication Server (Cisco VCS)
- Cisco Webex クラウドサービス (Control Hub で管理)

暗号化
- リアルタイムメディア (音声、ビデオ、画面共有) は Secure Real-Time Transport Protocol (SRTP) で暗号化
- エンドツーエンドの暗号化には Advanced Encryption Standard (AES) 128、AES 256、SHA1、SHA256、および RSA を使用

動作温度および湿度
- 周囲温度: 0 ～ 35 °C (32 ～ 95°F)
- 相対湿度 (RH) : 10 ～ 90%

技術仕様 (2/2 ページ)

電源
- 電源自動検知
- 100 ～ 240 VAC、50/60Hz

Webex Board 55:
- 電力消費:
  - スタンバイ:45 W
  - アイドル状態または使用中:185 W

Webex Board 55S:
- 電力消費 (最大 4.6 A):
  - スタンバイ:33 W
  - アイドル状態または使用中:170 W

Webex Board 70:
- 電力消費:
  - スタンバイ:55 W
  - アイドル状態または使用中:240 W

Webex Board 70S:
- 電力消費 (最大 4.6 A):
  - スタンバイ:33 W
  - アイドル状態または使用中:222 W

Webex Board 85S:
- 電力消費 (最大 4.6 A):
  - スタンバイ:41 W
  - アイドル状態または使用中:352 W

寸法

Webex Board 55/55S:
- 幅:1283 mm (50.5 インチ)
- 高さ:814 mm (32.1 インチ)
- 奥行き:48.3 mm (1.9 インチ)
- 重量:39.8 kg (87.7 ポンド)

Webex Board 70/70S:
- 幅:1627 mm (64.1 インチ)
- 高さ:1034 mm (40.7 インチ)
- 深さ:61 mm/2.4 in
- 重量:64.3 kg (141.8 ポンド)

Webex Board 85S:
- 幅:1966 mm (77.4 インチ)
- 高さ:1221 mm (48.1 インチ)
- 深さ:76 mm/3 in
- 重量:100 kg (220 ポンド)

認定および適合規格

Webex Board 55、70:
- 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 A
- FCC 規格 (無線機器)

Webex Board 55S、70S、85S:
- 法規制の遵守
  - 指令 2014/30/EU (EMC 指令)
  - 指令 2014/53/EU (無線機器指令)
  - 指令 2011/65/EU (RoHS)
  - 指令 2002/96/EU (WEEE)
  - NRTL 認定 (製品の安全性)
  - FCC 規格 (無線機器)
- 標準規格
  - 無線: EN 300 328、EN 301 893、EN 300 440
  - EMC:EN 301 489-1 および -17、EN 55032 - クラス A、EN 55024
  - 安全性:EN 60950-1、EN 62479、EN 62311 (無線バージョン)
  - FCC CFR 47 Part 15B (EMC):クラス A
  - FCC CFR 47 Part 15C (RF)
  - FCC CFR 47 Part 15E (RF)

各国の認定書類については、製品認定ステータスデータベース https://pas.cisco.com/pdtcnc/ を参照してください。

2020 年 10 月 12 日

シスコ Web サイト内のユーザマニュアル

次の短縮リンクを使用して、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

Desk シリーズ:

► https://www.cisco.com/go/desk-docs

Board:

► https://www.cisco.com/go/board-docs [英語]

通常、すべてのシスココラボレーションエンドポイントのユーザマニュアルは ► https://www.cisco.com/c/en/us/support/collaboration-endpoints で参照できます。

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などのカスタマイズ。機能によっては、一部のタイプの製品で使用できない場合があります。

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*

シスコのお問い合わせ先

シスコの Web サイトでは、シスコ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

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

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本書に組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。全著作権所有。著作権©1981、カリフォルニア大学理事会。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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

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

印刷版と複製ソフトは公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト (https://www.cisco.com/c/ja_jp/about/contact-cisco.html) をご覧ください。

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)。

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。