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

管理者ガイド

Cisco Webex 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 ドキュメンテーションとソフトウェア

このガイドの対象となる製品

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

ユーザ ドキュメンテーョン

このガイドでは，ビデオ会議デバイスの管理に必要な情報を提供します。

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

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

Cisco ウェブ サイト内のドキュメンテーション

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

► https://www.cisco.com/go/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 クラウド サービスに登録されたデバイスの詳細については，以下のサイトを参照してください。

►https://help.webex.com

Cisco Project Workplace

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

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

ソフトウェア

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

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

ソフトウェア リリース ノート (CE9) を参照することをお勧めします。

► https://www.cisco.com/c/ja_jp/support/collaboration-endpoints/spark-board/tsd-products-support-series-home.html

CE9 の最新情報

この章では, 現行の Cisco Collaboration Endpoint ソフトウェアバージョン 9.x (CE9.x) について, 新規および変更されたデバイス設定 (コンフィギュレーション) の概要と, 新機能および改善点を CE9.8 と比較して説明します。

CE9 では以下の Webex 製品が新しくなっています。

- CE9.0: Room Kit
- CE9.1: Codec Plus, および Room 55
- CE9.2: Room 70
- CE9.4: Codec Pro, Room 70 G2, および Room 55 Dual
- CE9.6: Room Kit Mini
- CE9.8: Board 55/55S, Board 70/70S, および Board 85S

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

► https://www.cisco.com/c/ja_jp/support/collaboration-endpoints/spark-board/tsd-products-support-series-home.html

CE9.9 の新機能および改善点

UI 拡張エディタの更新

(すべての製品)

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

詳細については, 次の場所にある CE9.9 のカスタマイズガイドを参照してください。► https://www.cisco.com/go/in-room-control-docs

Web アプリ *(Boards)*

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

デジタル サイネージ

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

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

ユーザーは, Webex Board でのみサイネージのコンテンツを操作できます。

外部 URL からのブランディング画像とカスタム壁紙の取得 *(すべての製品)*

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

カスタム壁紙は, Webex Board では使用できません。

ネットワーク設定メニューの変更

(すべての製品)

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

超音波設定の変更 *(すべての製品)*

すべての製品で, [オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定に同じデフォルト値が使用されるようになりました。異なる製品間で音量範囲の調整も行われました。製品固有の違いは内部処理され, 値の範囲やデフォルト値に反映されなくなりました。デバイスから再生されるサウンドレベルは変更されません。

TLS 設定の変更 *(すべての製品)*

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

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

ホワイトボードと注釈の更新

(Board)

- ホワイトボード上の付箋や注釈を作成, 編集, および移動できます。
- ホワイトボードと注釈を使用するときに, 3 つの異なるペン サイズから選択できます。
- ホワイトボードと注釈のコピーを作成できます。プレゼンテーションのホワイトボードまたは注釈付きスナップショットは, ホワイトボードメニューに保存されます。他のホワイトボードやスナップショットと同じように, このコピーを選択して作業を続けることができます。

有線タッチリダイレクト *(Board)*

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

タッチリダイレクトは, コール中でないときにのみ機能します。

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

CE9.9 での設定の変更点

新しい設定

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

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

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

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

BYOD TouchForwarding Enabled *(Board)*
CE9.9.0 では使用できません。

HttpFeedback TlsVerify *(すべての製品)*

Logging External TlsVerify *(すべての製品)*

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

Provisioning TlsVerify *(すべての製品)*

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

Standby Signage InteractionMode *(Board)*

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

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

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

UserInterface WebcamOnlyMode *(Room Kit Mini)*

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

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

削除された設定

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

後継の設定:

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

変更された設定

Audio Ultrasound MaxVolume *(すべての製品)*

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

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

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

新しいデフォルト値: 70 *(すべての製品)*

RTP Ports Range Stop *(すべての製品)*

旧: デフォルト: 2486

新: デフォルト: 2487

旧: 整数 (1120 ～ 65535)

旧: 整数 (1121 ～ 65535)

SIP ListenPort *(すべての製品)*

旧: Off/On

新: Auto/Off/On

SIP ListenPort *(Board)*

旧: デフォルト値: On

新: デフォルト: Auto

SIP TlsVerify *(すべての製品)*

旧: デフォルト: Off

新: デフォルト: On

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

旧 : 整数 (-100 ～ 100)

新 : 文字列 (1, 12)

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

旧 : 整数 (-100 ～ 100)

新 : 文字列 (1, 12)

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。

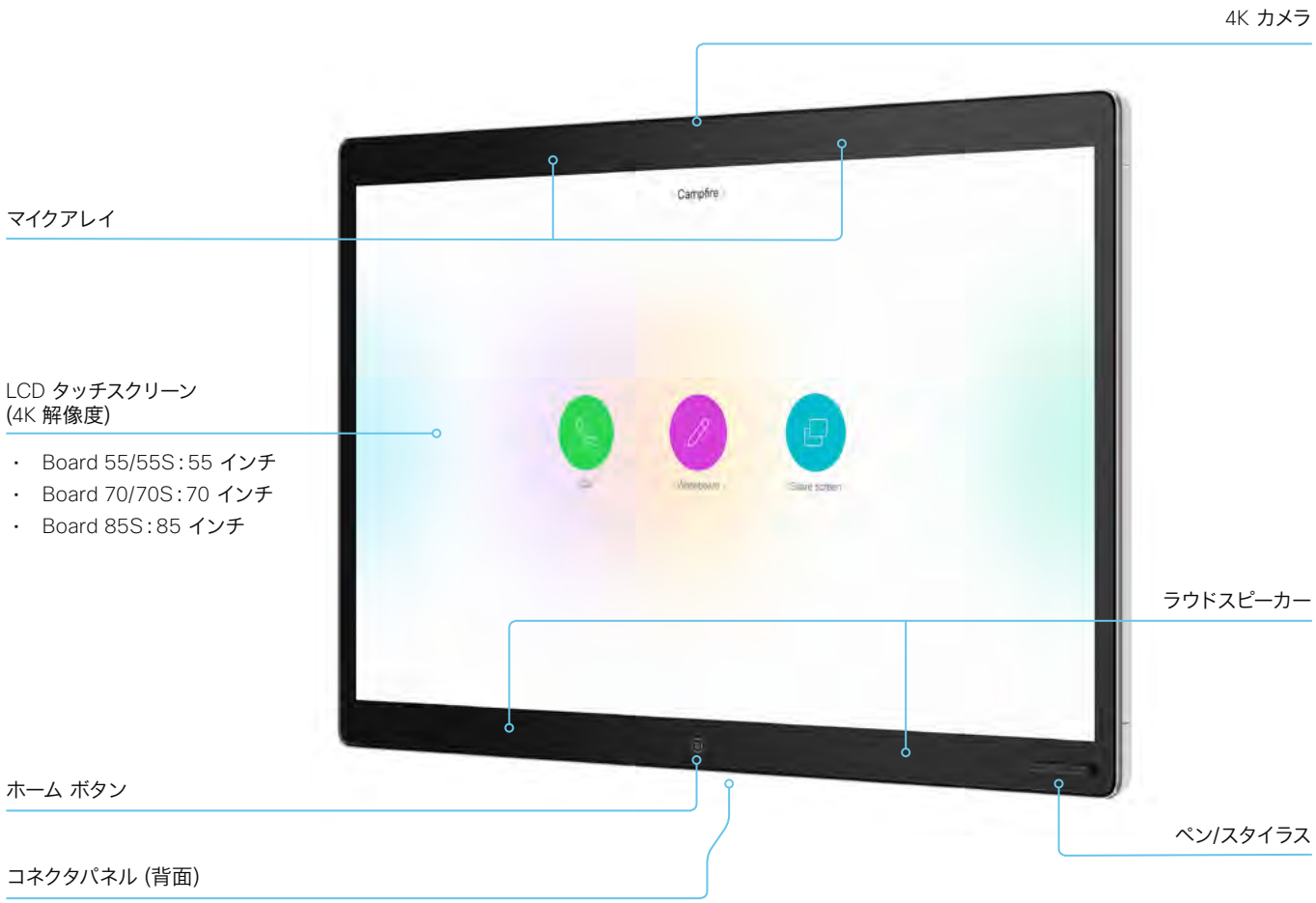
第 2 世代の Webex Board は S シリーズと呼ばれ, ハードウェアプラットフォームにマイナーな最適化が施されています。

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 Cisco Webex Teams 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 Teams 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 (1/2 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. ユーザー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ます。
1. [設定 *(Settings)*], [再起動 *(Restart)*] の順に選択します。
1. [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. ユーザー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

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

デバイスの再起動

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

デバイスが使用可能になるまでに数分かかります。

デバイスの電源オフ

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

デバイスの電源をリモートから再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 (1/4 ページ)

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

それ以外にも次の方法でデバイスの API にアクセスできます。

- HTTP/HTTPS (Web インターフェイスでも使用)
- WebSocket
- 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 ガイドを参照してください。

ヒント

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

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

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

次に例を示します。

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

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

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

アクセス方式	注	方式の有効化/無効化方法
HTTP/HTTPS	・デバイスの Web インターフェイスで使用されます。 ・非セキュア (HTTP) 通信またはセキュア (HTTPS) 通信 ・HTTPS : デフォルトで有効 ・HTTP : 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で, アップグレード後に工場出荷時の設定にリセットされていない場合にのみ, デフォルトで有効になります。	*[ネットワークサービス (NetworkServices)] > [HTTP] > [モード (Mode)]* 変更を有効にするには, デバイスを再起動してください。
WebSocket	・HTTP に関連付けられるため, WebSocket を使用するには HTTP または HTTPS も有効化する必要があります ・暗号化 (wss) または非暗号化 (ws) の通信 ・デフォルトで [無効 (Disabled)]	*[ネットワークサービス (NetworkServices)] > [HTTP] > [モード (Mode)]* *[ネットワークサービス (NetworkServices)] > [WebSocket]* 変更を有効にするには, デバイスを再起動してください。
SSH	・セキュアな TCP/IP 接続 ・*デフォルトで有効*	*[ネットワークサービス (NetworkServices)] > [SSH] > [モード (Mode)]* デバイスを再起動する必要はありません。変更が有効になるまでに少し時間がかかる場合があります。
シリアル接続	・ケーブルを使用してデバイスに接続します。IP アドレス, DNS, ネットワークは不要。 ・*デフォルトで有効* 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。再度有効にする ([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工場出荷時設定にリセットする必要があります。

ビデオ会議デバイスの管理方法 (2/4 ページ)

デバイスの Web インターフェイス

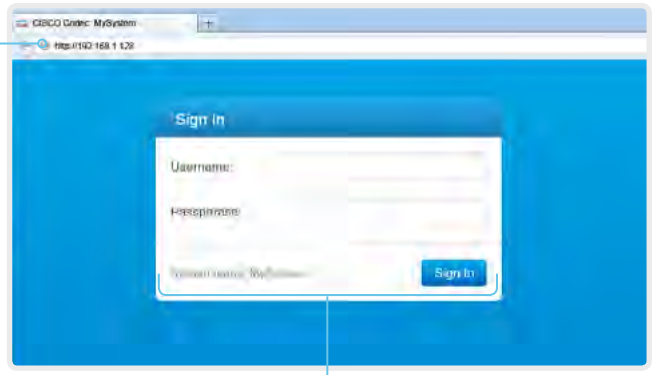
Web インターフェイスは, デバイスの管理ポータルです。コンピュータから接続して, デバイスをリモートで管理できます。フル設定アクセスが提供され, メンテナンス用のツールやメカニズムを利用できます。

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

ウェブ ブラウザは最新版を使用することを推奨します。

デバイスへの接続

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



IP アドレスの確認方法

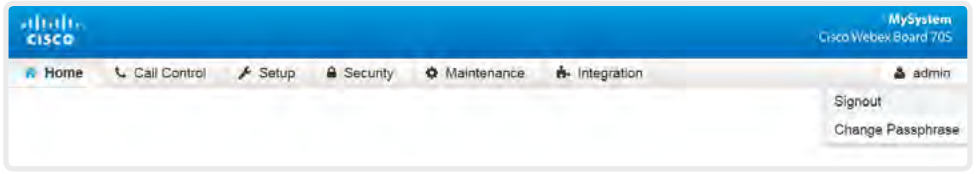
1. ユーザーインターフェイスの上部にあるデバイス名またはアドレスを選択します。
2. *[このデバイスについて (About this device)] に続き, [設定 (Settings)]* を選択します。

サインイン

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

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

admin ユーザのパスワードを設定する必要があります。



サインアウト

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

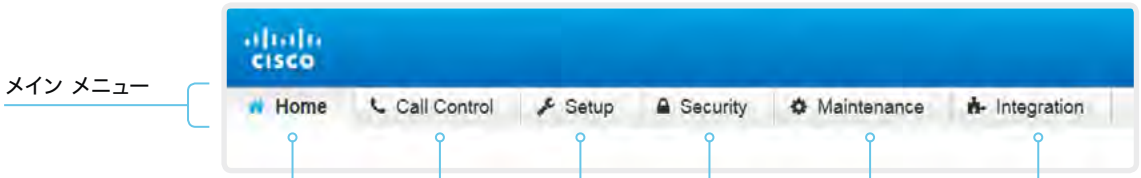
ビデオ会議デバイスの管理方法 (3/4 ページ)

ウェブ インターフェイスの構成

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

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

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



ホーム (Home)

コール制御 (Call Control)

セットアップ (Setup)

- 設定 (Configuration)
- ステータス (Status)
- 周辺機器 (Peripherals)
- パーソナライゼーション (Personalization)
- お気に入り (Favorites)
- 電子メール設定 (Email Settings)

セキュリティ (Security)

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

メンテナンス (Maintenance)

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

統合 (Integration)

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

ビデオ会議デバイスの管理方法 (4/4 ページ)

ユーザー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，デバイスのユーザー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，工場出荷時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」の章を参照してください。

一部の設定とテストは，デバイスの電源を初めて入れたときに起動されるセットアップアシスタントの一部にもなっています。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参照してください。

設定へのアクセス

1. ユーザー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ます。
2. *[設定 (Settings)]* を選択します。

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

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

   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。

第 2 章

設定

ユーザ管理

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

デフォルトのユーザ アカウント

デバイスには，初期状態でデフォルトの管理者ユーザー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」の章を参照してください。

新しいユーザ アカウントの作成

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

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

   認証にクライアント証明書を使用する場合にのみ，*[クライアント証明書 DN (識別名) (Client Certificate DN)]* フィールドに値を入力してください。
4. 適切な *[ロール (Roles)]* チェックボックスをオンにします。

   admin ロールをユーザに割り当てた場合は，*[自分のパスフレーズ (Your passphrase)]* 入力フィールドに自分自身のパスフレーズを確認のために入力します。
5. ユーザをアクティブにするには，*[ステータス (Status)]* を **[アクティブ (Active)]** に設定します。
6. *[Create User]* をクリックします。

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

既存のユーザ アカウントの編集

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

ユーザ特権を変更する

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

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

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

パスフレーズを変更する

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

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

ユーザ アカウントを削除する

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

ユーザ ロール

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

これらは*ユーザ ロール*です。

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

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

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

ROOMCONTROL : このロールを持つユーザーは，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。このユーザーは，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ーは，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。このユーザーは，カスタマイズした UI パネルを作成することもできます。

デバイスパスフレーズの変更

次の操作を行うには，デバイスのパスフレーズを知っている必要があります。

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

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ー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* ユーザー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 ユーザー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

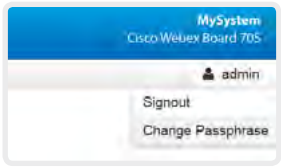
デバイスには複数のユーザーアカウントを作成できます。

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

パスフレーズを変更する

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

   パスフレーズの形式は，0 ～ 64 文字の文字列です。



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

別のユーザのパスフレーズの変更

管理者アクセス権がある場合は，すべてのユーザのパスフレーズを変更できます。

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

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

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

[設定 (Settings)] メニューへのアクセスの制限

デフォルトでは, すべてのユーザーが, ユーザーインターフェイス (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。

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

[設定 (Settings)] メニューのロック

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

   これで, ユーザーインターフェイス (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

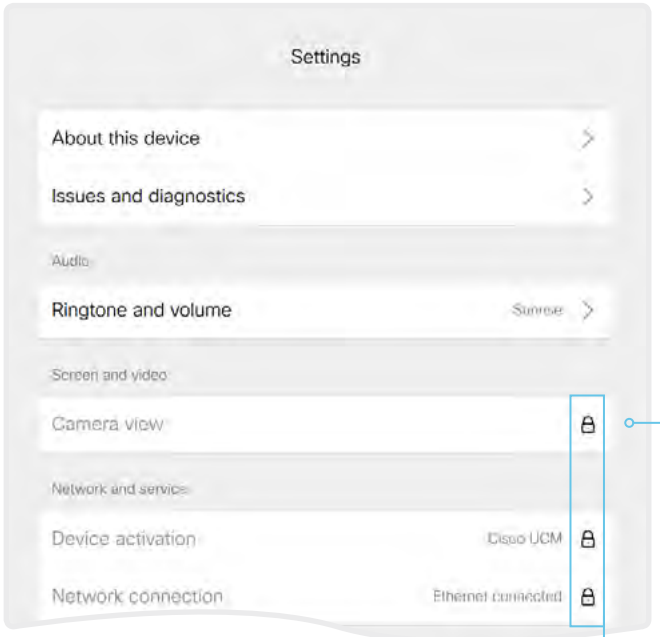
1. ウェブ インターフェイスにサインインして, *[セットアップ (Setup)] > [設定 (Configuration)]* に移動します。
2. *[ユーザインターフェイス (UserInterface)] > [設定メニュー (SettingsMenu)] > [モード (Mode)]* に移動して, [ロックなし (**Unlocked**)] を選択します。
3. [保存 (Save)] をクリックして変更を有効にします。

   これで, 任意のユーザーが, ユーザーインターフェイス (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

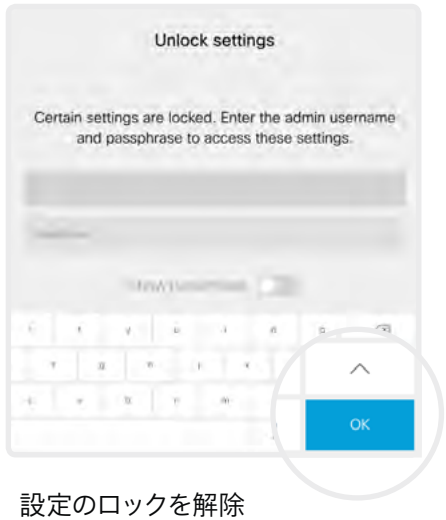
このメニューがロックされている場合は, サインインしないと, デバイスの重要な設定にアクセスできません。

[設定 (Settings)] メニューを開くには, ユーザー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。

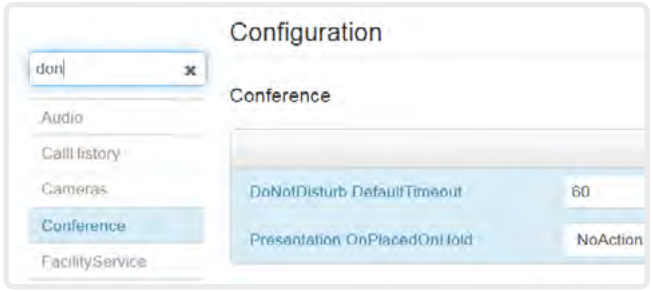
デバイス設定

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

デバイス設定の検索

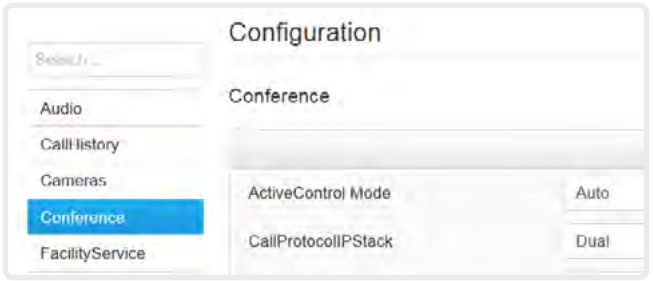
設定を検索する

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



カテゴリを選択して設定に移動する

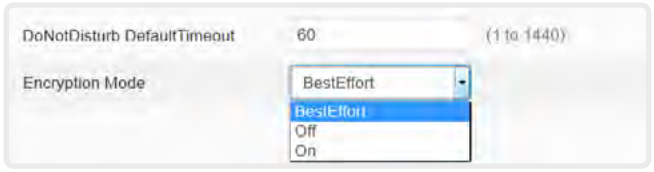
デバイス設定はカテゴリ別にグループ化されています。左側のペインのカテゴリを 1 つ選択して, 関連付けられている設定を表示します。



デバイス設定の変更

値スペースを確認する

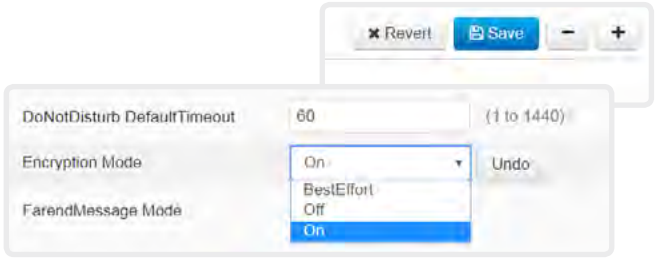
設定の値スペースは, 入力フィールドに続くテキストか, 矢印をクリックすると開くドロップダウン リストで指定します。



値の変更

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

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



変更が保存されていないカテゴリには, 編集記号 (✎) のマークが付きます。

デバイスの設定について

すべてのデバイス設定を Web インターフェイスから変更できます。

個別のデバイス設定については, ▶ 「デバイスの設定」の章を参照してください。

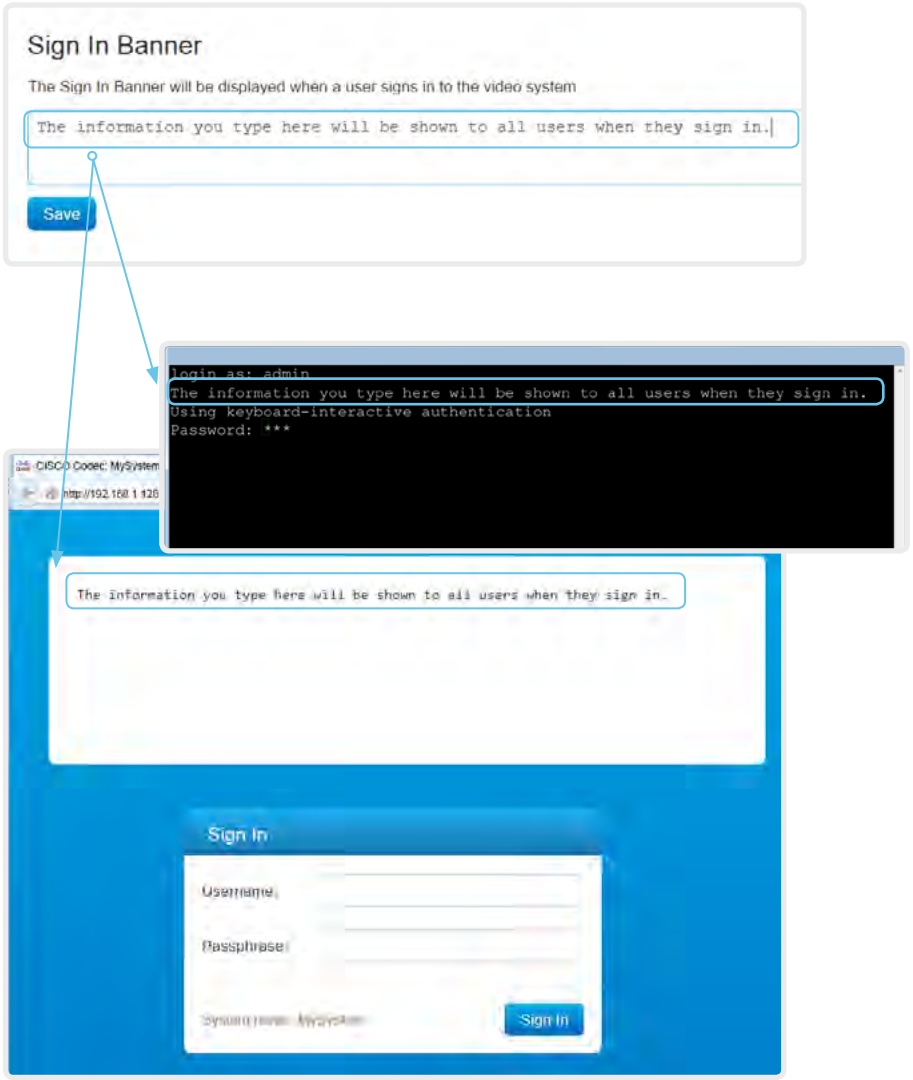
異なる設定には, 異なるユーザ クレデンシャルが必要である場合があります。管理者がすべてのデバイス設定を変更できるように, 管理者にはすべてのユーザーロールを割り当てる必要があります。

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

サインイン バナーの追加

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

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



サインイン バナーについて

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

最大サイズは 4 kByte です。

ウェルカムバナーとサインインバナーの比較

サインインバナー

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

ウェルカムバナー

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

ウェルカムバナーの追加

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

API コマンド

```
xCommand SystemUnit WelcomeBanner Set
```

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

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

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

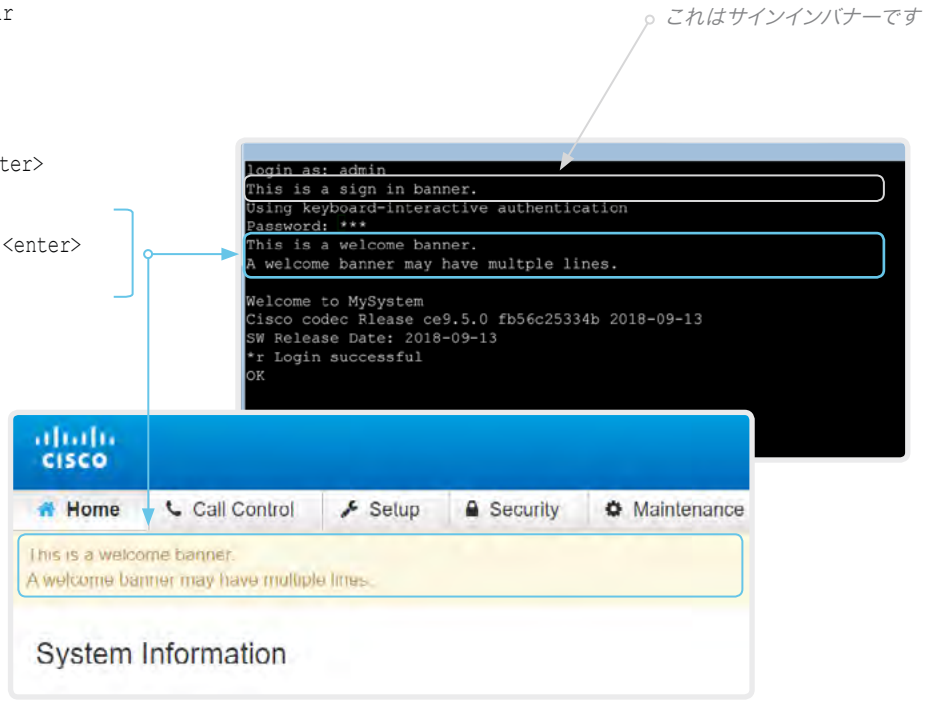
例

```
xCommand SystemUnit WelcomeBanner Set <enter>
```

これはウェルカムバナーです。<enter>

ウェルカムバナーには複数の行を表示することができます。<enter>

. <enter>



ウェルカムバナーについて

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

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

最大サイズは 4 kByte です。

ウェルカムバナーとサインインバナーの比較

サインインバナー

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

ウェルカムバナー

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

デバイスのサービス証明書の管理

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

次のファイルが必要です。

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

証明書と秘密キーは, デバイス上の同じファイル内に保存されます。

証明書を有効/無効にし, 表示, または削除する

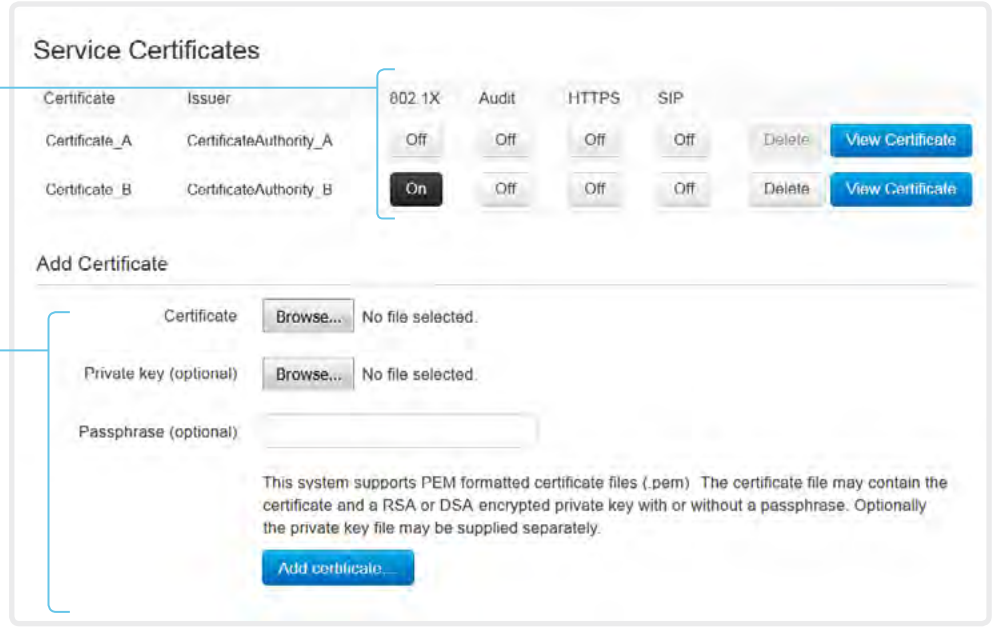
各サービスの証明書を有効または無効にするには, [オン (On)] および [オフ (Off)] ボタンを使用します。

証明書を表示または削除するには, それぞれ対応するボタンを使用します。

証明書の追加

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

   有効期間が 10 年以内の証明書のみが受け付けられます。



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

デバイスのサービス証明書について

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

通信が確立される前に, 有効な証明書をデバイスから提供するようにサーバー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ー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, サーバーまたはクライアントの信頼性を検証します。認証が失敗した場合, 接続は確立されません。

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

CA 証明書リスト

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

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

CA リストは次のとおりです。

- *プレインストール*: デバイスと通信する外部サーバー (HTTPS, syslog, および SMTP) の証明書を検証するために使用される, プレインストールされた CA 証明書。
- *コラボレーションエッジ*: デバイスが Cisco Unified Communications Manager (CUCM) によって Expressway を介してプロビジョニングされている場合に (MRA またはエッジとも呼ばれます) , 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)

外部サーバー用にプレインストールされた CA 証明書の管理

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

証明書の表示または無効化

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

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

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

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

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ー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ー
- 電話帳サーバー
- syslog サーバー (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

デバイスを工場出荷時設定にリセットしても, プレインストールされた証明書のリストは削除されません。

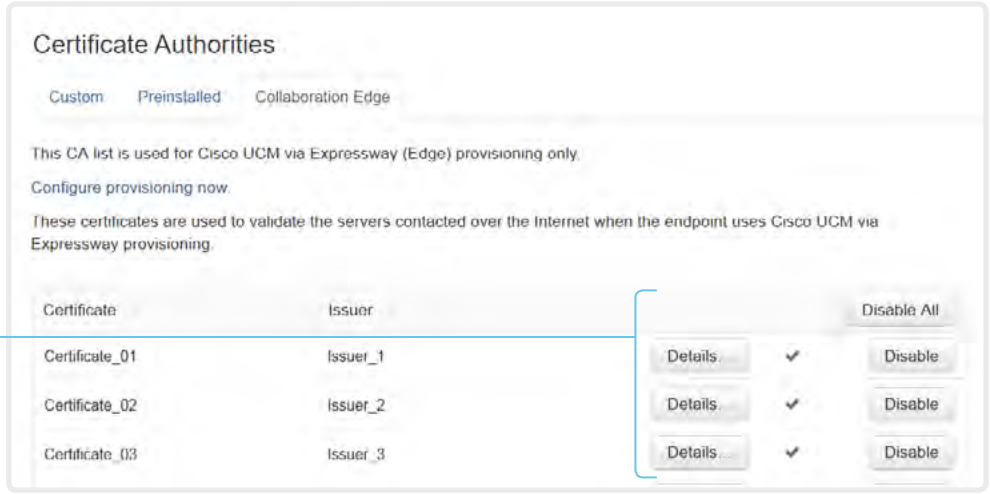
信頼できる認証局 (CA) のリストの管理 (3/4 ページ)

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

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

証明書の表示または無効化

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



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

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

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

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

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

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

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

デバイスを工場出荷時設定にリセットしても, プレインストールされた証明書のリストは削除されません。

信頼できる認証局 (CA) のリストの管理 (4/4 ページ)

デバイスへの CA 証明書のアップロード

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

次のファイルが必要です。

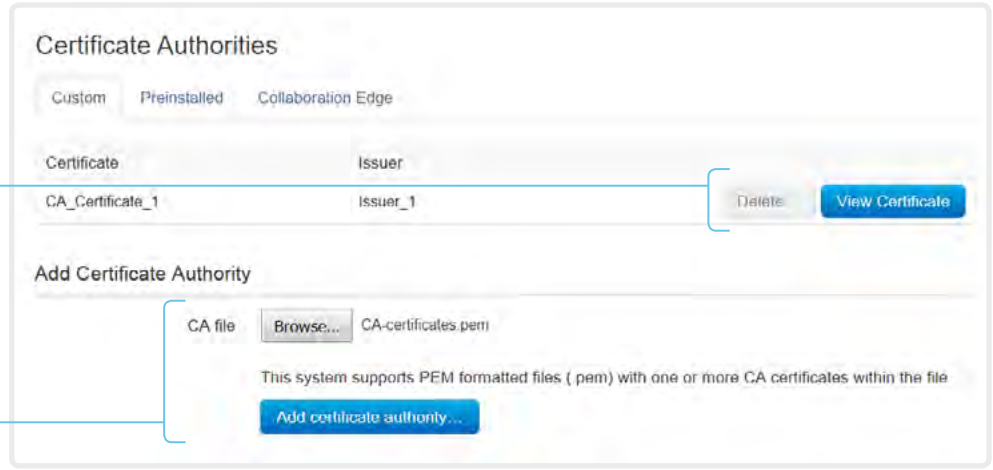
- CA 証明書のリスト (ファイル形式 : .PEM) 。

証明書を表示または削除する

証明書を表示または削除するには, それぞれ対応するボタンを使用します。

CA 証明書のリストのアップロード

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



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

以前に保存した証明書は自動的には削除されません。

CA 証明書を含む新しいファイル内のエントリが既存のリストに付加されます。

信頼できる CA 証明書のカスタムリストについて

このリストには, 自分でデバイスにアップロードした CA 証明書が含まれます。これらの証明書は, クライアント証明書とサーバー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ー
- 電話帳サーバー
- SIP サーバー
- syslog サーバー (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ーおよびサービス

セキュア監査ロギングのセットアップ

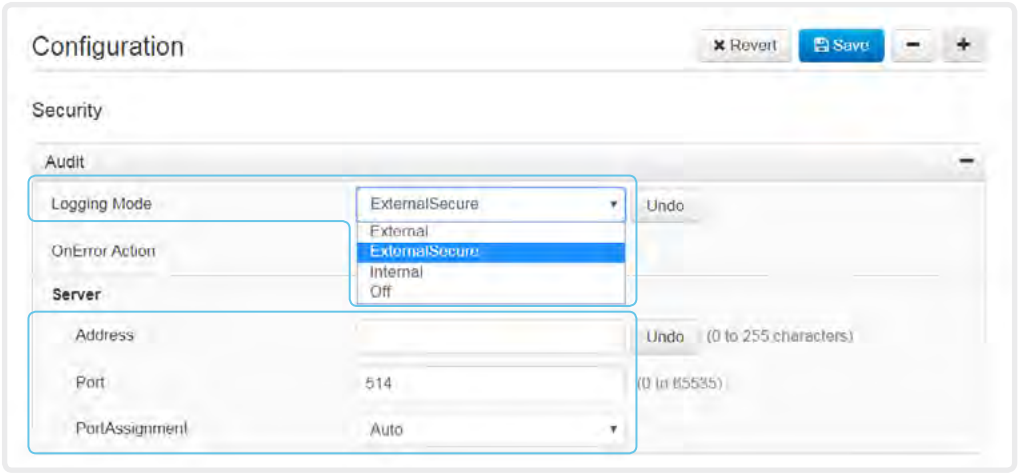
Web インターフェイスにサインインし, *[セットアップ (Setup)] > [設定 (Configuration)]* に移動します。

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

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

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

   [ポート割り当て (PortAssignment)] を [手動 (Manual)] に設定した場合は, 監査サーバの *[ポート (Port)]* 番号も入力する必要があります。
3. *[監査 (Audit)] > [ロギング モード (Logging Mode)]* を [外部セキュア (ExternalSecure)] に設定します。
4. *[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ー (syslog サーバー) に送信します。そのサーバーの 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。

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

監査サーバ認証に失敗した場合は, 監査ログが外部サーバに送信されません。

CUCM 信頼リストを削除する

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

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

CUCM 信頼リストを削除する

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

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

次のようなケースでは, これらのファイルを削除する必要があります。

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

信頼リスト フィンガープリントと証明書の概要

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

この情報は, トラブルシューティングに役立ちます。

信頼リストの詳細

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

永続モードを変更する

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

永続性ステータスの確認

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

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

永続設定を変更する

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

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

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

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

永続モード

デフォルトでは, 設定, 通話履歴, 内部ログ, ローカル電話帳 (ローカル ディレクトリとお気に入りリスト) , および IP 接続情報が保存されます。すべての永続設定は [永続 **(Persistent)**] に設定されているため, 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。

工場出荷時設定にリセットする方法については, ► 「ビデオ会議デバイスの工場出荷時設定へのリセット」の章を参照してください。

強力なセキュリティ モードの設定

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

強力なセキュリティ モードの設定

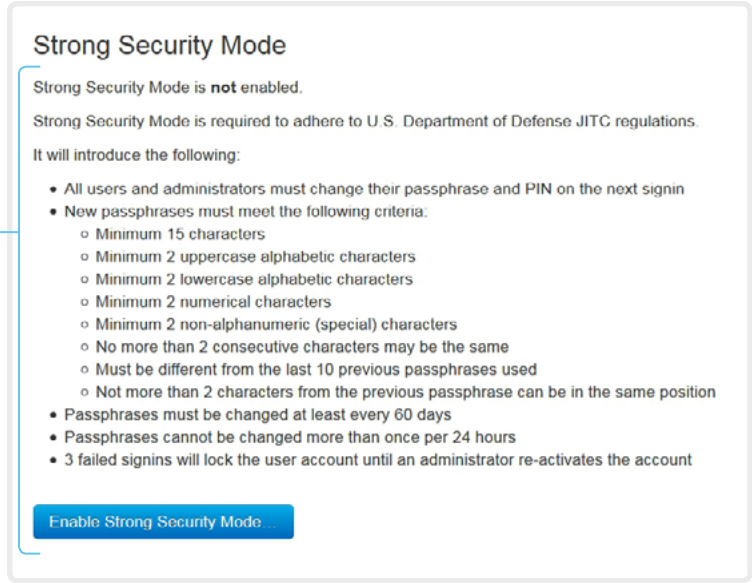
続行する前に, 強力なセキュリティ モードの影響について注意してお読みください。

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

   デバイスが自動的に再起動します。

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

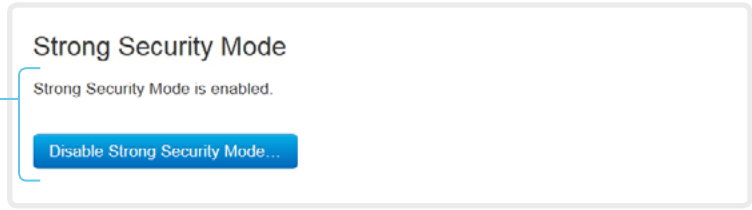
   デバイスパスフレーズの変更方法については, ▶ 「デバイスパスフレーズの変更」の章を参照してください。



通常モードに戻る

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

デバイスが自動的に再起動します。



強力なセキュリティ モードについて

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

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

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，*[セットアップ (Setup)] > [設定 (Configuration)]* に移動します。
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，*[セットアップ (Setup)] > [電子メール設定 (Email Settings)]* に移動します。
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。

   証明書がない場合は，*[アップロード手順に進む (Continue to uploading step)]* をクリックし，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。

手動によるサーバーのセットアップ

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

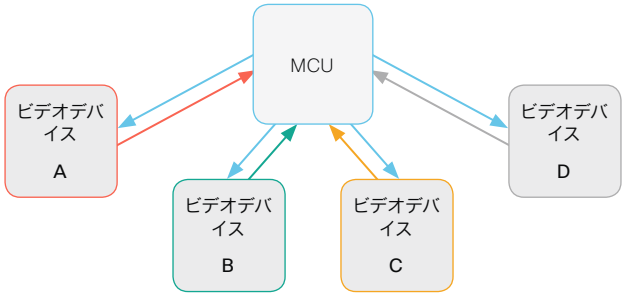
CA リストの詳細については，▶「信頼できる認証局 (CA) のリストの管理」の章を参照してください。

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。



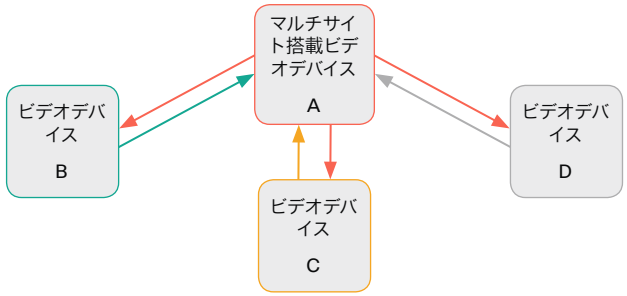
このセットアップでは, ビデオデバイス A, B, C および D が 4 者会議に参加しています。MCU がすべてのデバイスからのメディアストリームを受信し, ストリームを処理して, すべてのメディアを他の参加者に送信します。

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

ローカル会議リソース - マルチサイト

(SX10, DX70, および DX80 では使用不可)

マルチサイトのシナリオでは, 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 が 4 者会議に参加しています。ここではデバイス A でマルチサイト機能を使用し, 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。

マルチサイト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 : マルチサイトサポートなし
- SX80, MX700, および MX800 : 参加者 5 人 (自身を含む) と追加のオーディオコール 1 つ
- Codec Pro, Room 70 G2 : 参加者 5 人 (自身を含む)
- その他の製品 : 参加者 4 人 (自身を含む)

マルチポイント設定

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

- 自動 (Auto)
- CUCMMediaResourceGroupList
- マルチサイト (MultiSite) *(SX10, DX70, DX80 では使用不可)*
- オフ (Off) *(SX10, DX70, DX80 では使用不可)*

次のページの表で, さまざまな会議オプションについて説明しています。

アドホックマルチポイント会議のセットアップ (2/2 ページ)

[会議 マルチポイントモード (Conference Multipoint Mode)] 設定	マルチサイトオプションキー	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	・ オーディオのみの参加者を 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 (SIP Type)] 設定は [シスコ (Cisco)] にする必要があります。 ・ 新しい参加者をコールする間, 会議は保留されます。新しい参加者がコールを受け入れると, その新しいコールを会議にマージできます。 ・ 会議に新しい参加者を最初に追加した参加者だけが, さらに参加者を追加できます。
マルチサイト (MultiSite) [3]	○	該当なし	ローカルマルチサイト [4]	・ 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。 ・ デバイスの上限に達するまで参加者の追加を続けることができます。
	×	該当なし	1 オーディオ追加	・ オーディオのみの参加者を 1 人追加できます。 ・ ビデオでの参加者は追加できません。
自動 (Auto)	○	MCU	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 [4]	・ 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。 ・ 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。 ・ マルチサイトホスト (MCU として機能しているデバイス) のみが参加者を追加できます。これにより, 会議のカスケードを防ぎます。
	×	MCU	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	・ オーディオ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[n] デバイスタイプ (Call [n] DeviceType)] ステータスに表示されます。

[3] SX10, DX70, および DX80 ではサポートされません。

[4] 会議のカスケードを避けるために, [会議 マルチポイント モード (Conference Multipoint Mode)] は [マルチサイト (MultiSite)] ではなく [自動 (Auto)] に設定することをお勧めします。

コンテンツ共有のためにインテリジェント プロキシミティをセットアップする (1/5 ページ)

Cisco Proximity を使用すると, ユーザー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	30/7 *
Room Kit, Room 55 Dual, Room 70, Room 70 G2	30/7 *
Codec Plus, Codec Pro	30/7 *
Board 55/55S, Board 70/70S, Board 85S	30/7 *
SX80	10
SX10, SX20	7
MX700, MX800	10
MX200 G2, MX300 G2	7
DX70, DX80	3

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

プロキシミティ サービス

コールの発信とビデオ会議デバイスの制御:

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

モバイル デバイス上での共有コンテンツの表示:

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

ラップトップからワイヤレスで共有:

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

コールの発信とビデオ会議デバイスの制御

モバイル デバイスでの共有コンテンツの表示

モバイル デバイスからのワイヤレス共有

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

Cisco Proximity クライアントをインストールする

クライアントの入手場所

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

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

エンド ユーザ ライセンス契約書

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

超音波の放出

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

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

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

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

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

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

DX70 および DX80:

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

Board :

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

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

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

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

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

ヘッドセット

DX70, DX80, および SX10N :

これらのデバイスでは, 次の理由からヘッドセットを常に使用できます。

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

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

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

Room 55, Room Kit, Room Kit Mini :

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

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

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

プロキシミティ サービスを有効にする

1. Web インターフェイスにサインインし, *[セットアップ (Setup)] > [設定 (Configuration)]* に移動します。
2. *[プロキシミティ (Proximity)] > [モード (Mode)]* に移動します。プロキシミティが [オン (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 つ以上のプロキシミティ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　ことをお勧めします。

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

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。
- インテリジェントプロキシミティを有効にするビデオ会議デバイスは, 室内で 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

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

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。
- ユーザー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 (「超音波信号を確認できません (Unable to verify the ultrasound signal) 」) がリストに含まれていなければ, 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ています。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

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

その他のリソース

Cisco Proximity のサイト:
► https://proximity.cisco.com

サポート フォーラム:
► https://www.cisco.com/go/proximity-support

ビデオ品質の対コール レート比調整 (1/2 ページ)

ビデオ入力品質の設定

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

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

最適鮮明度プロファイル

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

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

異なる最適鮮明度プロファイルに使用する一般的な解像度, コール レートおよび送信フレーム レートの一部を次のページの表に示します。解像度とフレームレートは, 発信側と着信側の両方のデバイスでサポートされている必要があります。

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

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

ビデオ品質対コール レート比の調整 (2/2 ページ)

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	768 x 448 @ 30	1024 x 576 @ 30	1024 x 576 @ 30	768 x 448 @ 30	1024 x 576 @ 30	1024 x 576 @ 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	1280 x 720 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1280 x 720 @ 30	1280 x 720 @ 60	1280 x 720 @ 60
2560	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1280 x 720 @ 60	1280 x 720 @ 60	1920 x 1080 @ 60
3072	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1280 x 720 @ 60	1280 x 720 @ 60	1920 x 1080 @ 60
4000	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1280 x 720 @ 60	1920 x 1080 @ 60	1920 x 1080 @ 60
6000	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60

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.265, 最大 30fps			H.265, 最大 60fps		
	標準	*中*	*高*	*標準*	*中*	*高*
128	512 × 288 @ 30	512 × 288 @ 30	640 × 360 @ 30	512 × 288 @ 30	512 × 288 @ 30	640 × 360 @ 30
256	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30
384	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30
512	1024 x 576 @ 30	1280 x 720 @ 30	1280 x 720 @ 30	1024 x 576 @ 30	1280 x 720 @ 30	1280 x 720 @ 30
768	1280 × 720 @ 30	1280 × 720 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 60
1152	1280 × 720 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 60	1280 × 720 @ 60
1472	1280 × 720 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 60	1280 × 720 @ 60	1280 × 720 @ 60
1920	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1280 x 720 @ 60	1280 x 720 @ 60	1920 x 1080 @ 60
2560	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1280 x 720 @ 60	1920 x 1080 @ 60	1920 x 1080 @ 60
3072	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 60	1920 x 1080 @ 60	1920 x 1080 @ 60
4000	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 30	1920 x 1080 @ 60	1920 x 1080 @ 60	1920 x 1080 @ 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 Touch 10 ユーザ インターフェイスに企業ブランディングを追加 (1/2 ページ)

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

このページから, 独自のブランディング要素 (背景ブランドイメージ, ロゴ) をビデオ会議デバイスに追加できます。

アウェイク状態のブランディング

アウェイク状態では, 次のことができます。

- 右下隅にロゴを追加します (画面および Touch 10) 。

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ー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ーエクスペリエンスを損なうことなく, 画面とタッチユーザーインターフェイスの表示をカスタマイズできます。

画面および Touch 10 ユーザ インターフェイスに企業ブランディングを追加 (2/2 ページ)

ハーフウェイク状態のブランディング

ハーフウェイク状態では, 次のことができます。

- 背景ブランド イメージを追加します (画面および Touch 10) 。
- 右下隅にロゴを追加します (画面および Touch 10) 。
- スクリーン中央のメッセージをカスタマイズまたは削除します (画面のみ。Touch 10 は不可) 。これは, デバイスの使用開始方法をユーザーに示すメッセージです。

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

背景ブランド イメージ

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

ロゴ

推奨事項 :

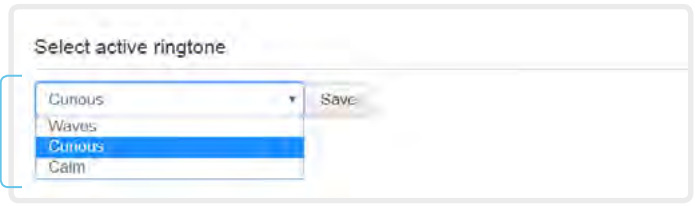
- 白色のロゴ (暗い背景ブランド イメージに適合する)
- 背景が透明な PNG 形式
- 最小 272 × 272 ピクセル

着信音の選択と着信音量の設定

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

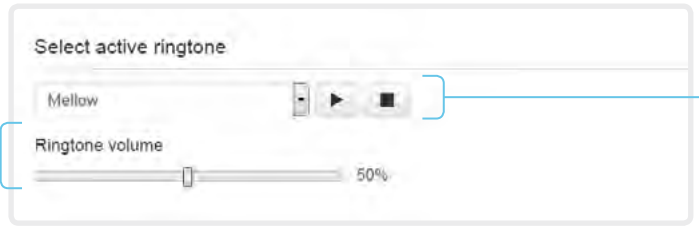
呼び出し音の変更

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



呼び出し音の音量の設定

呼び出し音の音量を調節するにはスライド バーを使用します。



呼び出し音の再生

呼び出し音を再生するには, 再生ボタン (▶) をクリックします。

再生を終了するには, 停止ボタン (■) を使用します。

着信音について

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

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

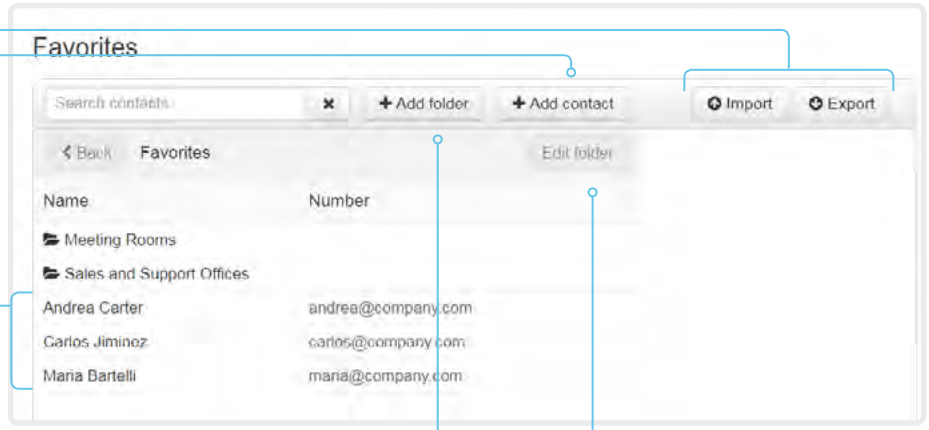
お気に入りリストの管理

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

ファイルから連絡先をインポート/エクスポート

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

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



連絡先を追加または編集する

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

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

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

連絡先を削除する

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

サブフォルダを削除する

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

デバイスのユーザー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 Touch 10 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セットアップできます。

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

CUCM からの製品固有の設定のプロビジョニング (1/2 ページ)

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

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

CUCM リリース 12.5 (1) SU1 以降では, CUCM からプロビジョニングできる設定またはパラメータが増えました。設定のリストは, デバイス上でユーザーに表示される内容 (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「ビデオエンドポイント管理 (Video Endpoints Management) 」の章を参照してください。

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 サーバーに同期されます。
- **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は, 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 のユーザー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。

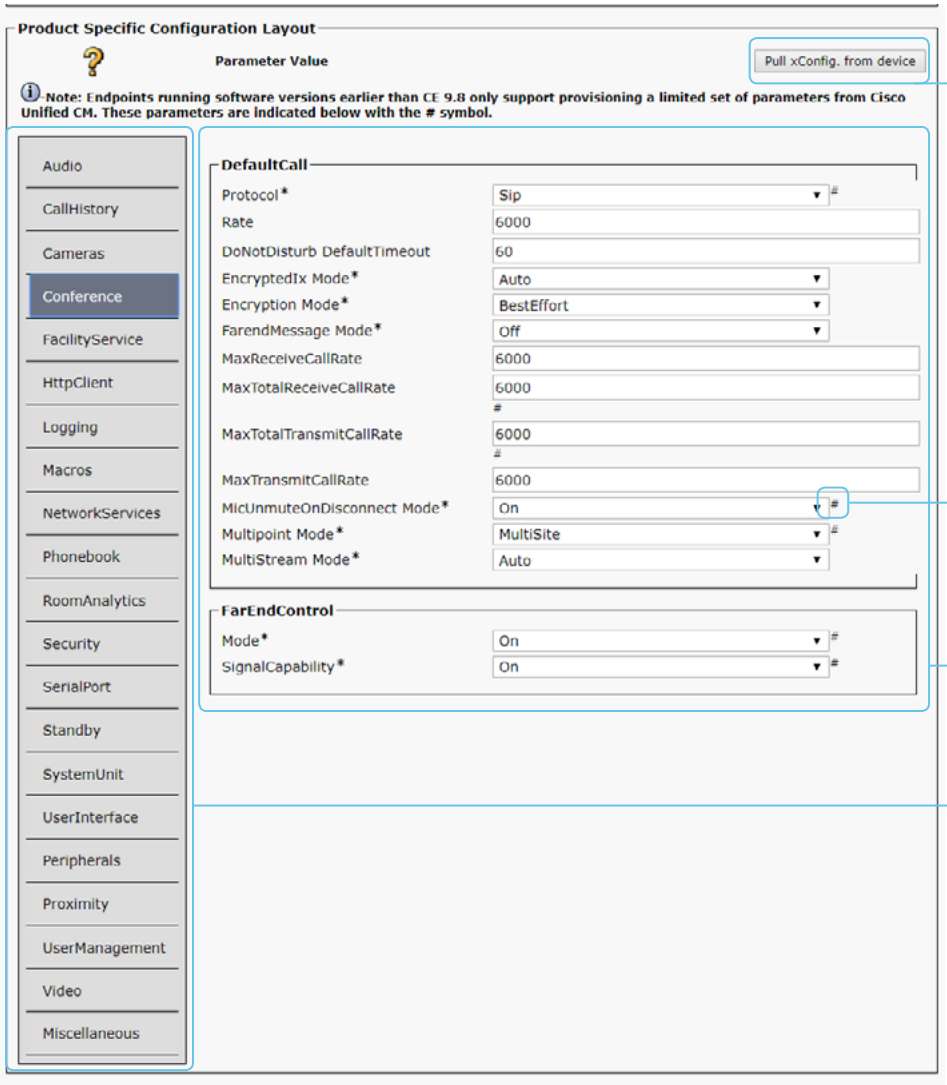
パラメータの完全なセットは, デバイスを CE9.8 以降にアップグレードした場合にのみ機能します。

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。

   使用するモードとして, [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)] を選択します (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

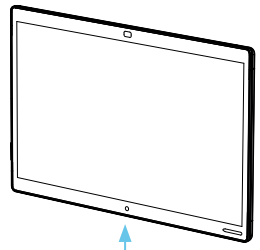
入力ソースの接続 (1/2 ページ)

ウェブ インターフェイスにサインインして, *[セットアップ (Setup)] > [設定 (Configuration)]* に移動すると, 以下に示す設定が見つかります。

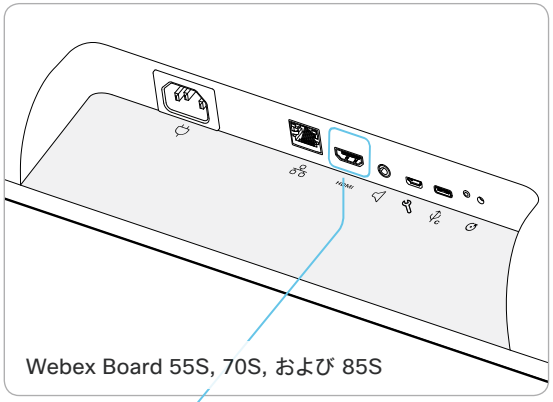
コンピュータまたはその他のコンテンツ ソースの接続

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, 30fps 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。

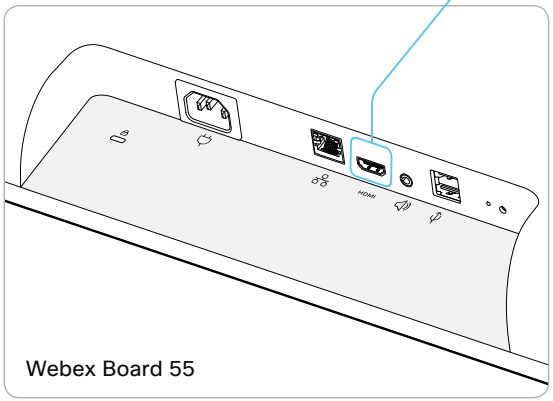


コネクタパネルは下部背面にあります。

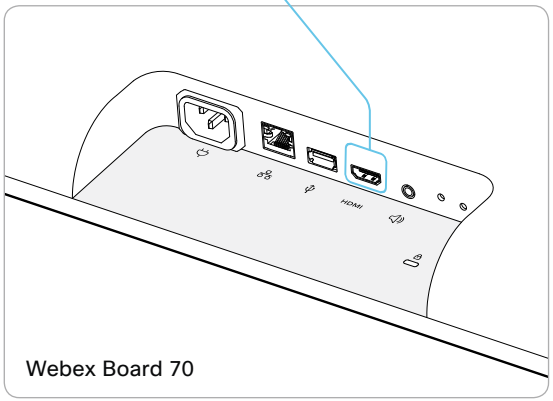


Webex Board 55S, 70S, および 85S

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，スクリーンと Touch 10 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，*[セットアップ (Setup)] > [設定 (Configuration)] > [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，Cisco 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, Cisco 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 Cisco 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

* Room Kit, Room Kit Plus, Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room 70, Room 70 G2, および Board は, シスコの HDMI, ディスプレイポート, およびミニディスプレイポート用プレゼンテーションケーブル (CAB-HDMI-MULT-9M=) をサポートしていません。

最適な概要の機能のセットアップ

ウェブ インターフェイスにサインインして, *[設定 (Configuration)] > [システム設定 (System Configuration)]* に移動すると, ここに示す設定が見つかります。

最適な概要機能は自動カメラ フレーミングを使用し, 室内の人数に基づいて最適な表示を選択します。

カメラは, デジタル顔検出機能を使用して, 室内の個人またはグループを最適に自動表示します。この機能は, 室内での参加者の移動や新たな参加者の入室に合わせて, 画面にすべてのユーザが含まれるように自動的に調整します。

最適な概要の設定

スピーカー トラッキングを設定するには, *[カメラ (Camera)] > [スピーカー トラック (SpeakerTrack)]* の設定を使用します。

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

[自動 (Auto)]: [ベスト概要 (general general)] が有効になります。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。ユーザーは, Board の *[設定 (Settings)] > [詳細設定 (Advanced Settings)]* パネルを使用して, ベストオーバービューを即座にオンまたはオフに切り替えることができます。

[オフ (Off)]: ベストオーバービューはオフになります。ユーザー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。

Touch 10 コントローラの接続 (1/3 ページ)

Touch 10 は，ネットワーク (LAN) 経由で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) を経由した Touch 10 のビデオ会議デバイスへの接続

図のように，Touch 10 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。

Touch 10 の設定

Touch 10 が電源に接続されると，設定手順が始まります。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。

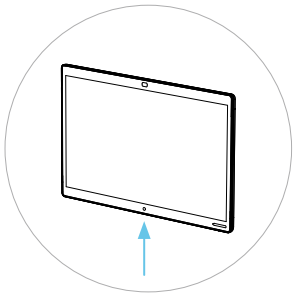
  デバイスがリストに表示されるためには，次の条件を満たす必要があることに注意してください。

  - デバイスと Touch 10 が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。

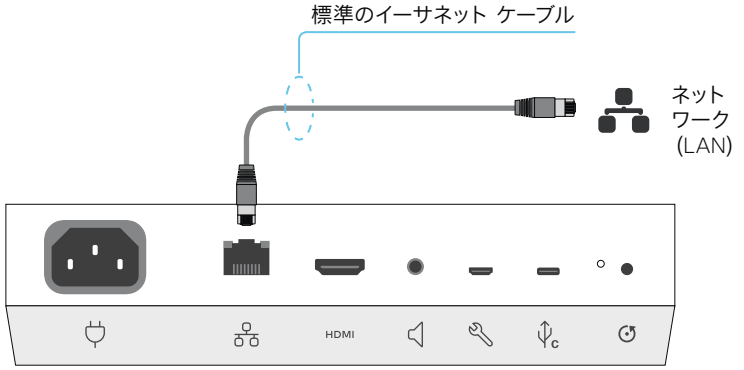
  user ロールを持つユーザであれば十分対応できます。このタスクを実行するために admin ロールは必要ありません。

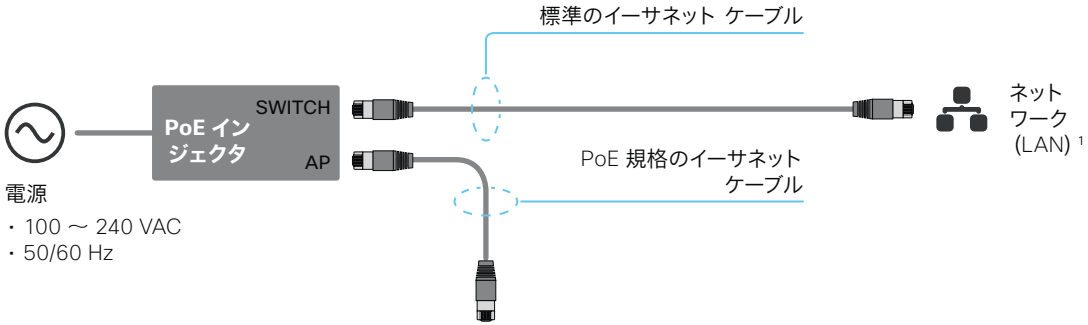
  ユーザ アカウントを作成してそれにロールを割り当てる方法の詳細については，▶「ユーザ管理」の章を参照してください。

Touch 10 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 Touch 10 が再起動します。



コネクタパネルは下部背面にあります。





イーサネット コネクタは，Touch 10 の裏側にあります。

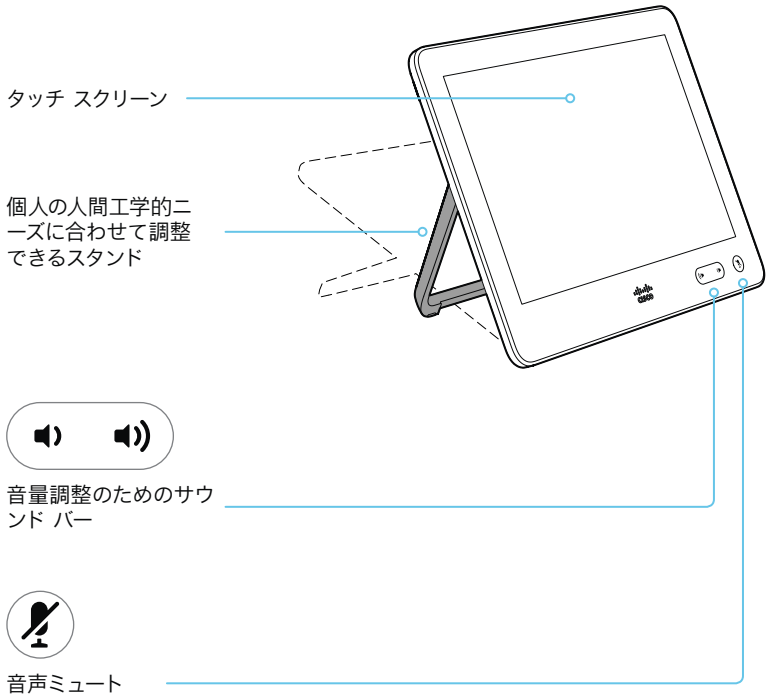
[1] ネットワーク インフラストラクチャが Power over Ethernet (PoE) を提供する場合，PoE インジェクタは必要ありません。タッチ 10 は PoE 規格のイーサネット ケーブルで直接壁面のソケット (イーサネット スイッチ) に接続する必要があります。

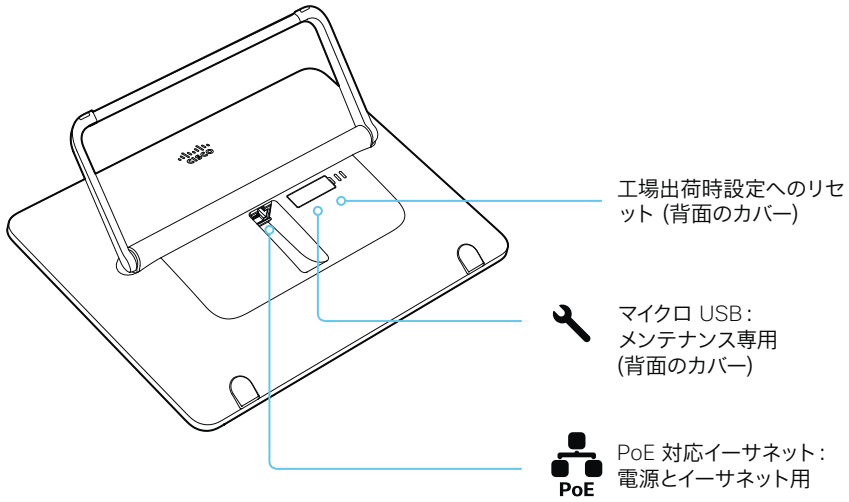
安全のために，PoE 電源はタッチ 10 と同じ建物に存在する必要があります。PoE 規格のイーサネット ケーブルは最大 100m (330 フィート) です。

Touch 10 コントローラの接続 (2/3 ページ)

Cisco Touch 10 の物理インターフェイス

これは, 2017 年後半に提供が開始された Touch 10 コントローラの新しいバージョンです。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。

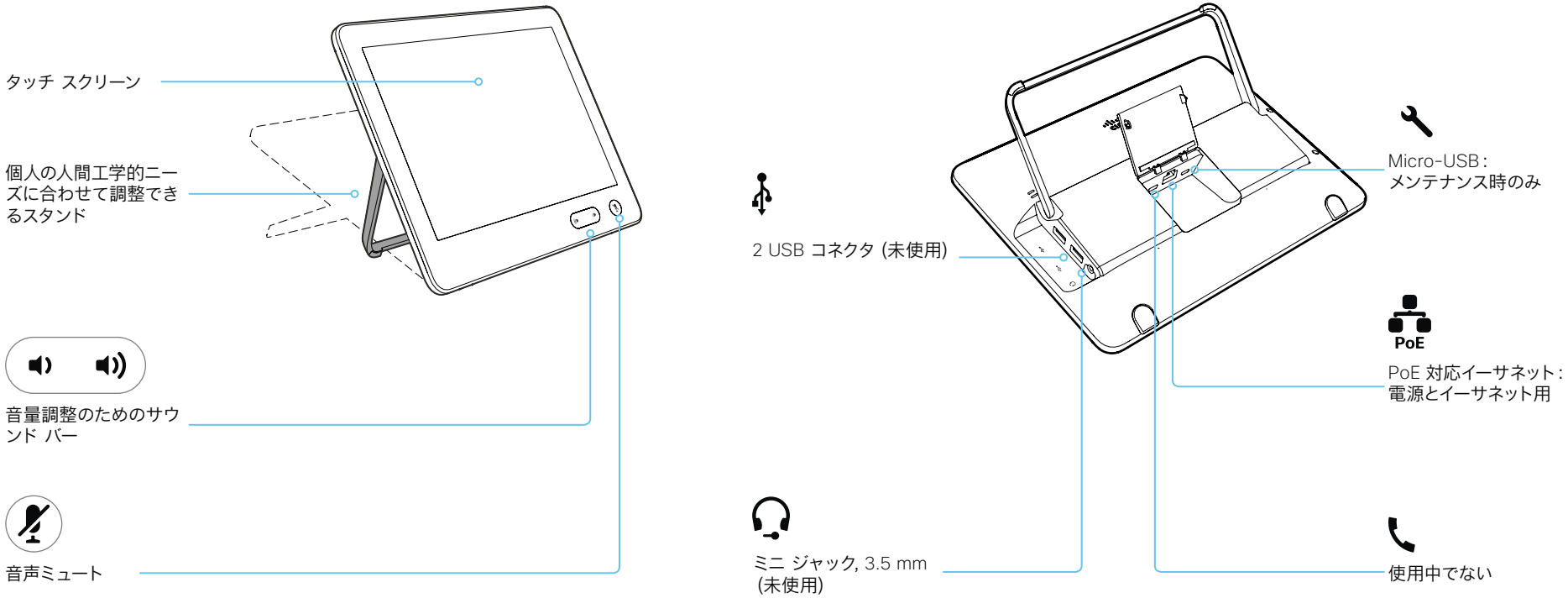




Touch 10 コントローラの接続 (3/3 ページ)

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

Touch 10 コントローラの新し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。



ISDN リンクの接続

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

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

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

要件および制約事項:

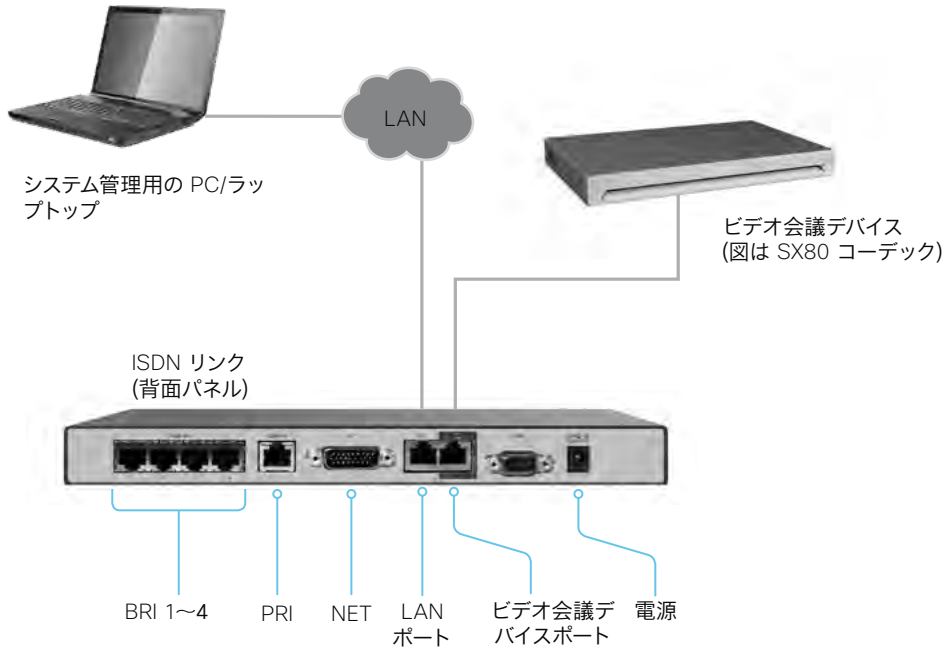
- ビデオ会議システムがタッチコントローラに接続されている必要があります。
- ISDN リンクは, IL1.1.7 以降のソフトウェアを実行している必要があります。
- ISDN リンクと通信するために, ビデオ会議デバイスの Web インターフェイスまたは API で IPv6 を有効にする必要があります。
- 確実にインストールするために, ISDN リンクのインストール ガイドでネットワーク トポロジを確認してください。
- ビデオ会議デバイスと ISDN リンクが同じサブネット上にある必要があります。エンドポイントまたは ISDN リンクに新しい IP アドレスが割り当てられている場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

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



第 4 章

メンテナンス

デバイスソフトウェアのアップグレード

ウェブ インターフェイスにサインインし, *[メンテナンス (Maintenance)] > [ソフトウェアのアップグレード (Software Upgrade)]* に移動します。

新しいソフトウェアをダウンロードする

各ソフトウェア バージョンに固有のファイル名があります。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_9_x-yyy.k3.cop.sgn”

"x" はドット内のリリース番号, "yyy" は, ソフトウェアの一意の識別子を表します。

ソフトウェア リリース ノート

新着情報および変更の概要について, ソフトウェア リリース ノート (CE9) を読むことを推奨します。

▶ https://www.cisco.com/c/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。

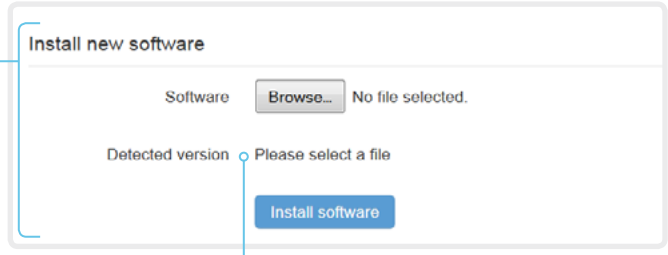
1. *[参照... (Browse...)]* をクリックして, 新しいソフトウェアを含む .cop.sgn ファイルを探します。

   ソフトウェアのバージョンが検出され, 表示されます。

2. *[ソフトウェアのインストール (Install Software)]* をクリックして, インストール プロセスを開始します。

インストールの完了には, 通常 15 分以上はかかりません。ウェブ ページから進捗状況を確認できます。インストール後, デバイスは自動的に再起動します。

再起動後にウェブ インターフェイスで作業を再開するには, 再度サインインする必要があります。



新しいソフトウェア バージョンの確認

ファイルを選択すると, ここにソフトウェアのバージョンが表示されます。

ソフトウェアのダウンロード

Cisco Download Software ウェブ ページを開き, 使用する製品のページにアクセスします。▶https://software.cisco.com/download/home

Webex Board および Room シリーズは, COP ファイルを使用して Web インターフェイスからアップグレードできます。

SX, MX, および DX シリーズは, PKG ファイルを使用して Web インターフェイスからアップグレードできます。

オプション キーを追加する

ウェブ インターフェイスにログインし, *[メンテナンス (Maintenance)] > [オプション キー (Option Keys)]* に移動します。

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

アンインストールされたオプションのオプション キーを取得する方法については, Cisco の担当者にお問い合わせください。

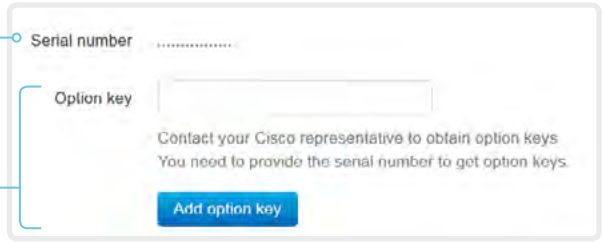
デバイスのシリアル番号

オプションキーの注文時にはデバイスのシリアル番号が必要です。

オプション キーの追加

1. テキストの入力フィールドに*オプション キー*を入力します。
2. *[オプション キーの追加* (Add option key) *]* をクリックします。

オプション キーを複数追加する場合は, すべてのキーに対してこの手順を繰り返してください。



オプション キーについて

デバイスには, 1 つ以上のソフトウェアオプションがインストールされている場合も, インストールされていない場合もあります。オプションの機能をアクティブにするには, 対応する*オプションキー*がデバイスに存在している必要があります。

オプションキーは各デバイスに固有のものです。

オプション キーは, ソフトウェアのアップグレードまたは出荷時の状態にリセットしても削除されないため, 一度追加するだけで済みます。

デバイスのステータス

デバイス情報の概要

[システム情報 (System Information)] ページを表示するには，ウェブインターフェイスにログインします。

このページには，製品タイプ，デバイス名のほか，ハードウェア，ソフトウェア，インストール済みオプション，ネットワークアドレスに関する基本情報が表示されます。ビデオネットワーク (SIP および H.323) の登録ステータスのほか，デバイスにコールする際に使用する番号および URI も含まれます。

デバイスステータスの詳細

より詳細なステータス情報を確認するには，Web インターフェイスにサインインし，*[セットアップ (Setup)]* > *[ステータス (Status)]* に移動します*。

ステータス エントリを検索する

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

カテゴリを選択して適切なステータスに移動する

デバイスステータスはカテゴリ別にグループ化されています。左側のペインでカテゴリを選択すると，関連するステータスが右側に表示されます。

* 図に示しているステータスは一例です。お使いのデバイスのステータスとは異なる場合があります。

診断の実行

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

[診断 (Diagnostics)] ページには, エラーの一般的な原因に関するステータスが示されます*。

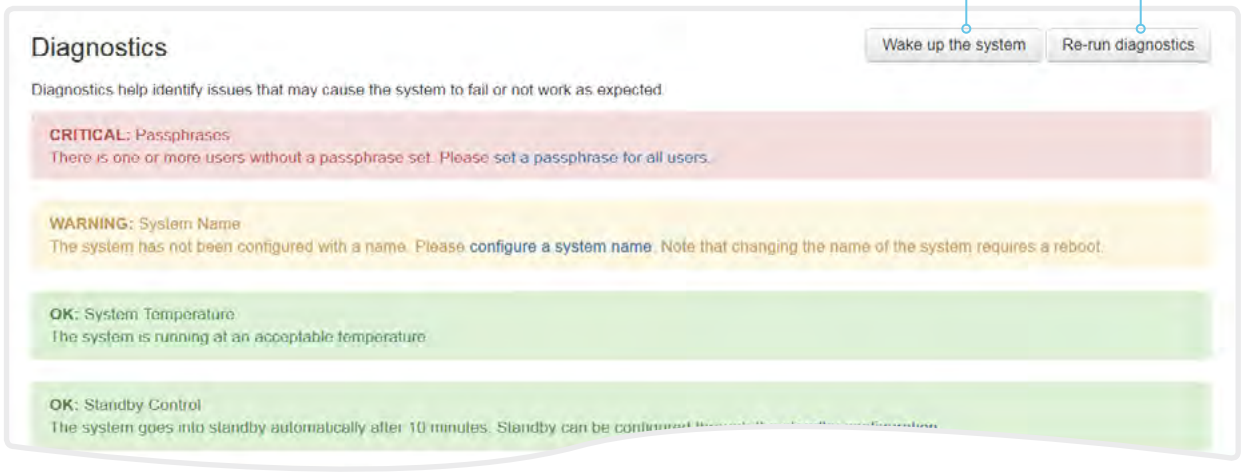
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

診断の実行

[診断の再実行 (Re-run diagnostics)] をクリックして, リストを最新の状態にします。

スタンバイ モードを離れる

スタンバイモードのデバイスを復帰させるには, *[システムの起動 (Wake up the system)]* をクリックします。

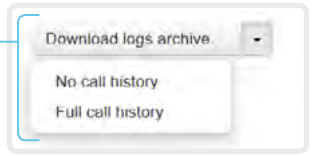


* 図に示しているメッセージは一例ですお使いのデバイスでは表示される情報が異なる場合があります。

ログ ファイルをダウンロードする

ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [システム ログ (System Logs)]* を選択します。

すべてのログ ファイルをダウンロードする



[ログ アーカイブのダウンロード... (Download logs archive...)] をクリックして, 手順に従います。

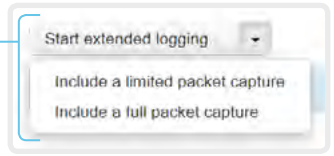
匿名化された通話履歴はログ ファイルにデフォルトで含まれています。

ログ ファイルから通話履歴を除外する場合や, 完全な通話履歴 (匿名以外の発信側/着信側) を含める場合は, ドロップダウン リストを使用します。

1 つのログファイルを開く/保存

ログ ファイルを開くにはウェブ ブラウザでファイル名をクリックし, ファイルをコンピュータに保存するにはファイル名を右クリックします。

拡張ロギングの開始



[拡張ロギングの開始... (Start extended logging...)] をクリックします。

拡張ロギングは, ネットワーク トラフィックの完全キャプチャが含まれているかどうかによって 3 分から 10 分かかります。

タイムアウトになる前に拡張ロギングを停止するには, *[拡張ロギングの停止 (Stop extended logging)]* をクリックします。

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

ログ ファイル リストの表示更新

[現在のログ (Current logs)] または *[履歴ログ (Historical logs)]* の更新ボタンをクリックすると, 対応するリストの表示が更新されます。

ログ ファイルについて

ログファイルは, テクニカル サポートが必要な場合に, Cisco のサポートから要求されることがある Cisco 固有のデバッグ ファイルです。

Current log ファイルはタイムスタンプ付きのイベント ログ ファイルです。

デバイスを再起動するたびに, 現在のログファイルはタイムスタンプ付きの履歴ログファイルにすべてアーカイブされます。履歴ログファイルの最大数に到達すると, 最も古いファイルは上書きされます。

拡張ロギング モード

拡張ロギング モードをオンにすると, コールのセットアップ中にネットワークの問題の診断に役立つ場合があります。このモードの間は, より多くの情報がログ ファイルに保存されます。

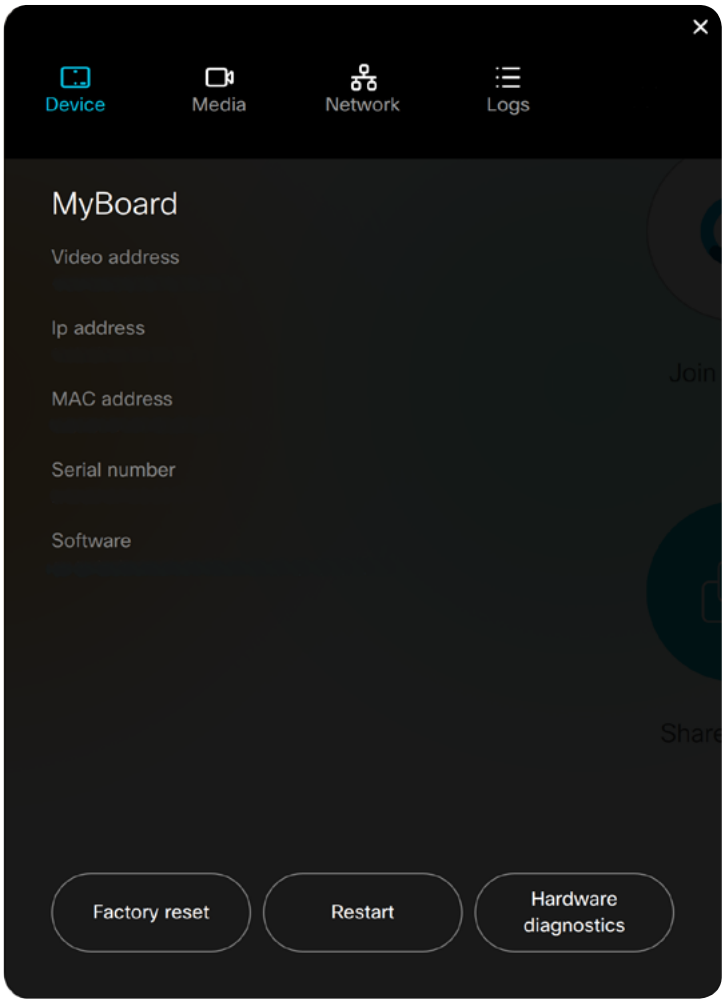
拡張ロギングはデバイスのリソースをより多く使用するため, デバイスの動作が低下する場合があります。拡張ロギング モードは, トラブルシューティングのときにのみ使用してください。

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 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

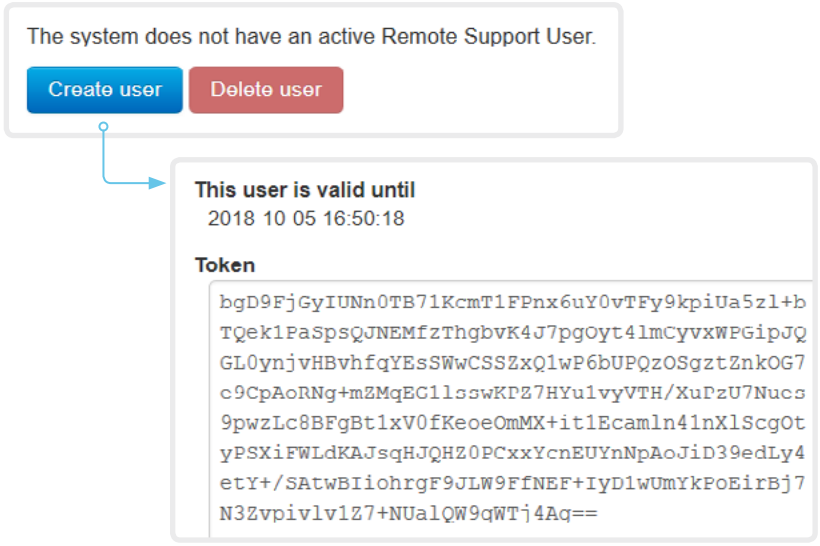
ウェブ インターフェイスにログインし, *[メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)]* に移動して, *[リモート サポート ユーザ (Remote Support User)]* タブを選択します。

リモート サポート ユーザは, Cisco TAC から指示されたトラブルシューティングを行うためだけに有効にする必要があります。

リモート サポート ユーザの作成

1. *[ユーザの作成 (Create User)]* をクリックします。
2. Cisco TAC で案件を開きます。
3. *[トークン (Token)]* フィールドのテキストをコピーして, Cisco TAC に送信します。
4. Cisco TAC はパスワードを生成します。

リモート サポート ユーザは 7 日間, または削除されるまで有効です。



リモート サポート ユーザの削除

[ユーザの削除 (Delete User)] をクリックします。

リモート サポート ユーザについて

デバイスに診断の問題がある場合は, リモートサポートユーザーを作成できます。

リモートサポートユーザーにはデバイスに対する読み取りアクセス権が付与され, トラブルシューティングに役立つ限定された一連のコマンドにアクセスできます。

リモート サポート ユーザのパスワードを取得するには, Cisco Technical Assistance Center (TAC) アシスタントが必要です。

設定とカスタム要素のバックアップ/復元

ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)]* に移動します。

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

- ブランディング イメージ
- マクロ
- お気に入り
- サインイン バナー
- UI 拡張
- 構成/設定 (すべてまたは一部)

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

バックアップ ファイルの作成

1. *[バックアップの作成 (Create backup)]* タブを開きます。
2. バックアップ ファイルに含める要素を選択します。

   現在デバイスに存在しない要素はグレー表示されます。
3. バックアップ ファイルに含める設定 (ある場合) を選択します。次の点に注意してください。
   - デフォルトでは, すべての設定がバックアップ ファイルに含まれます。
   - ウェブ ページの一覧から手動で設定を削除することにより, 1 つ以上の設定を手動で削除できます。
   - 特定のデバイスに固有の設定をすべて削除する場合は, *[システム固有の設定の削除 (Remove system-specific configurations)]* をクリックします。

     これは, 他のデバイスでバックアップバンドルを復元する予定がある場合に役立ちます。
4. *[バックアップのダウンロード (Download backup)]* をクリックして, コンピュータ上の zip ファイルに要素を保存します。

バックアップ ファイルの復元

1. *[バックアップの復元 (Restore backup)]* タブを選択します。
2. *[参照... (Browse...)]* をクリックして, 復元するバックアップ ファイルを見つけます。

   バックアップ ファイル内のすべての設定と要素が適用されます。
3. *[ファイルのアップロード (Upload File)]* をクリックして, バックアップを適用します。

   設定によっては, 有効にするためにデバイスを再起動する必要があります。

その他の情報

マクロの復元

マクロを含むバックアップファイルをデバイスで復元すると, 次の処理が適用されます。

- マクロのランタイムを起動または再起動します。
- マクロは自動的に有効化 (開始) されます。

ブランド イメージの復元

バックアップバンドルにブランドイメージが含まれている場合, *[ユーザインターフェイス壁紙 (UserInterface Wallpaper)]* 設定は自動的に **[自動 (Auto)]** に設定されます。

したがって, ブランド イメージは自動的に表示されます。カスタム壁紙より優先される場合もあります。

バックアップ ファイル

バックアップ ファイルは, いくつかのファイルを含む zip 形式のファイルです。それらのファイルは zip ファイル内の最上位にあり, フォルダに含まれていないことが重要です。

カスタム要素の CUCM プロビジョニング

バックアップファイルは, ▶ 「設定とカスタム要素のバックアップおよび復元」の章で説明されているとおり, 複数のデバイスで*カスタマイズテンプレート*として使用できます。

カスタマイズ テンプレート (バックアップ ファイル) は, 次のいずれかによってホストされています。

- CUCM TFTP ファイル サービス, または
- デバイスから HTTP または HTTPS で接続可能なカスタム Web サーバー。

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, デバイスがサーバー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。

設定は, 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含まれている場合でも, デバイス上には復元されません。

カスタマイズ テンプレートの TFTP ファイル サーバへのアップロード

1. *Cisco Unified OS の管理*にサインインします。
2. *[ソフトウェア アップグレード (Software Upgrades)] > [TFTP ファイル管理 (TFTP File Management)]* に移動します。
3. *[ファイルをアップロード (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. *[ファイルをアップロード (Upload File)]* をクリックします。

各デバイスへのカスタマイズプロビジョニング情報の追加

1. *Cisco Unified CM の管理*にサインインします。
2. *[デバイス (Device)] > [電話 (Phone)]* に移動します。
3. 関連するデバイスの製品固有の構成セクション内で, [カスタマイズ プロビジョニング (Customization Provisioning)] フィールドに以下を入力します。
   - *カスタマイズ ファイル*:カスタマイズ テンプレートのファイル名 (backup.zip など) *
   - *カスタマイズ ハッシュの型*:**SHA512**
   - *カスタマイズ ハッシュ*:カスタマイズ テンプレートの SHA512 チェックサム。

   これらのフィールドが存在しない場合は, CUCM に新しいデバイス パッケージをインストールする必要があります。
4. *[保存 (Save)]* および *[設定の適用 (Apply Config)]* をクリックして, 設定をデバイスにプッシュします。

* TFTP サービスを使用しない場合は, カスタマイズ テンプレートの完全な URI : `<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. ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)]* に移動します。
2. *[バックアップの復元 (Restore backup)]* タブを選択します。
3. *[参照 (Browse...)]* をクリックして, チェックサムを計算したいファイルを検索します。

   ページの下部に SHA512 チェックサムが表示されていることが確認できます。

CUCM のドキュメンテーション

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

カスタム要素の TMS プロビジョニング

バックアップファイルは，▶ 「設定とカスタム要素のバックアップおよび復元」の章で説明されているとおり，複数のデバイスで*カスタマイズテンプレート*として使用できます。

バックアップファイルは，デバイスから HTTP または HTTPS で接続可能なカスタム Web サーバー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，デバイスがサーバー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>
```

   where

   web-server-address：バックアップ ファイルへの URI (例：http://host/backup.zip) 。

   checksum：バックアップ ファイルの SHA512 チェックサム。

   起源：**プロビジョニング** *

3. 設定テンプレートのプッシュ先のデバイスを選択し，*[システムのセット (Set on systems)]* をクリックします。

TMS 構成テンプレートおよびカスタムコマンドの作成方法の詳細については，▶ Cisco TMS 管理者ガイド を参照してください。

SHA512 チェックサム

ヒント：Web インターフェイスを使用してデバイスにファイルを復元すると，そのファイルの SHA512 チェックサムを確認できます。

1. ウェブ インターフェイスにサインインして，*[メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)]* に移動します。
2. *[バックアップの復元 (Restore backup)]* タブを選択します。
3. *[参照 (Browse...)]* をクリックして，チェックサムを計算したいファイルを検索します。

   ページの下部に SHA512 チェックサムが表示されていることが確認できます。

* 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てい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。

以前に使用していたソフトウェア イメージに復元する

ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [システム回復 (System Recovery)]* に移動します。

以前に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, 設定, およびカスタム要素をバックアップすることをお勧めします。

ログ ファイル, 構成, カスタム要素のバックアップ

1. *[バックアップ (Backup)]* タブを選択します。
2. *[ログのダウンロード (Download logs)]* をクリックし, 指示に従ってログ ファイルをコンピュータに保存します。
3. *[バックアップのダウンロード (Download Backup)]* をクリックし, 指示に従ってバックアップ バンドルをコンピュータに保存します。

以前使用していたソフトウェア イメージに復元する

管理者以外, または, Cisco テクニカル サポートの指示のもとで行う場合以外はこの手順を実行しないでください。

1. *[ソフトウェア回復交換 (Software Recovery Swap)]* タブを選択します。
2. *[ソフトウェア: cex.y.z への切り替え... (Switch to software: cex.y.z...)]* をクリックします。ここで x.y.z はソフトウェア バージョンを示します。
3. *[はい (Yes)]* をクリックして選択を確定します。または, 操作をやめる場合は *[キャンセル (Cancel)]* をクリックします。

デバイスがリセットされるまでお待ちください。完了するとデバイスが自動的に再起動します。この手順は数分かかることがあります。

以前に使用されたソフトウェア イメージについて

デバイスに重大な問題がある場合は, 以前に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工場出荷時設定へのリセット (1/3 ページ)

デバイスに重大な問題が発生した場合は, 最後の手段として工場出荷時のデフォルト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。ソフトウェアの交換については, ▶ 「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。

デバイスを工場出荷時設定にリセットするには, Web インターフェイスまたはユーザー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。

工場出荷時設定へのリセット後, デバイスは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。

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, 設定, カスタム要素をバックアップすることをお勧めします。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工場出荷時設定へのリセット (2/3 ページ)

ウェブ インターフェイスを使用した初期設定へのリセット

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。

ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [システム回復 (System Recovery)]* に移動します。

1. *[初期設定へのリセット (Factory Reset)]* タブを選択して, 表示される情報を注意深く読みます。
2. *[初期設定へのリセットの実行 (Perform a factory reset...)]* クリックします。
3. *[はい (Yes)]* をクリックして選択を確定するか, *[キャンセル (Cancel)]* をクリックして操作を取り消します。
4. デバイスが工場出荷時のデフォルト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。

   デバイスが正常に工場出荷時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. デバイスが工場出荷時のデフォルト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。

   デバイスが正常に工場出荷時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

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. ユーザー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ます。
2. *[設定 (Settings)]* を選択します。
3. *[初期設定へのリセット (Factory Reset)]* を選択します。
4. 選択を確認するには *[リセット (reset)]* を選択し, 気が変わったら *[戻る (Back)]* を選択します。
5. デバイスが工場出荷時のデフォルト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。

   デバイスが正常に工場出荷時設定にリセットされると, セットアップアシスタントが起動し, *[ようこそ (Welcome)]* 画面が表示されます。

ログ ファイル, 構成, カスタム要素のバックアップ

ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)]* に移動します。

1. *[バックアップ (Backup)]* タブを選択します。
2. *[ログのダウンロード (Download logs)]* をクリックし, 指示に従ってログ ファイルをコンピュータに保存します。
3. *[バックアップのダウンロード (Download Backup)]* をクリックし, 指示に従ってバックアップ バンドルをコンピュータに保存します。

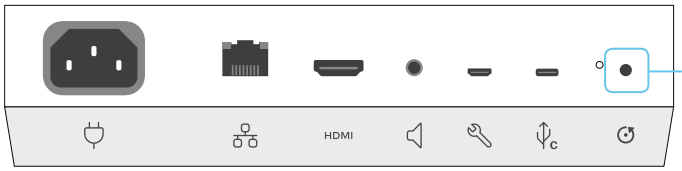
ビデオ会議デバイスの工場出荷時設定へのリセット (3/3 ページ)

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

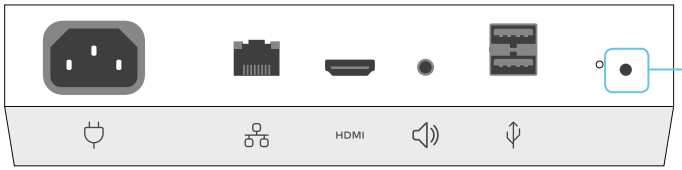
工場出荷時設定へのリセットを実行する前に, デバイスのログファイルと設定をバックアップすることをお勧めします。

1. 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. デバイスが工場出荷時のデフォルト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。

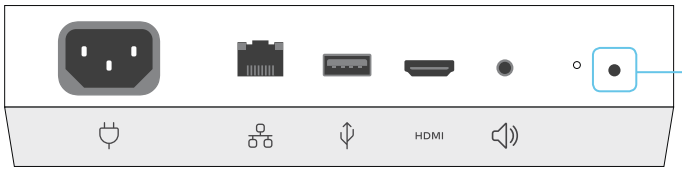
   デバイスが正常に工場出荷時設定にリセットされると, セットアップアシスタントが起動し, *[ようこそ (Welcome)]* 画面が表示されます。



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 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新しい 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。その場合は, 必ず Cisco のサポート組織に連絡して実行する必要があります。

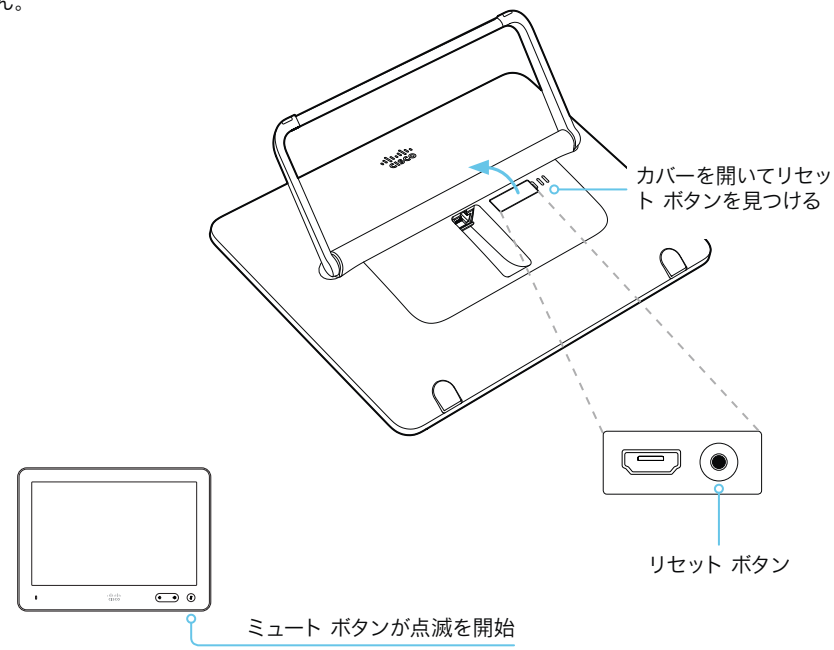
タッチコントローラを初期設定にリセットすると, ペアリング情報が失われ, (ビデオ会議デバイスではなく) タッチ自体がデフォルトの初期設定に戻ります。

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。

ペアリングおよび Touch 10 とビデオ会議デバイスの接続方法については, ► 「Touch 10 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。その場合は，必ず Cisco のサポート組織に連絡して実行する必要があります。

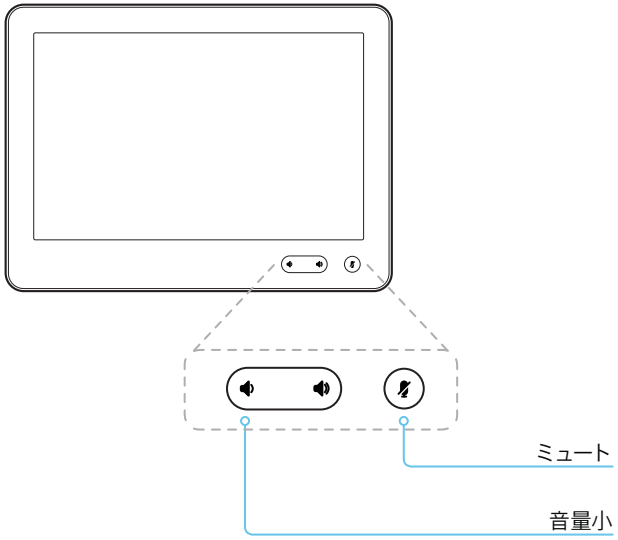
タッチコントローラを初期設定にリセットすると，ペアリング情報が失われ，(ビデオ会議デバイスではなく) タッチ自体がデフォルトの初期設定に戻ります。

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。

ペアリングおよび Touch 10 とビデオ会議デバイスの接続方法については，► 「Touch 10 コントローラの接続」の章を参照してください。

ユーザ インターイスのスクリーンショットをキャプチャする

ウェブ インターフェイスにサインインして, *[メンテナンス (Maintenance)] > [ユーザ インターフェイスのスクリーンショット (User Interface Screenshots)]* に移動します。

スクリーンショットのキャプチャ

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を撮る (Take screenshot of Touch Panel)]* 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を撮る (Take screenshot of OSD)]* をクリックします。

スクリーンショットはボタンの下のエリアに表示されます。スクリーンショットの準備ができるまで最大 30 秒かかる場合があります。

キャプチャされたすべてのスナップショットはボタンの上のリストに含まれています。イメージを表示するには, スクリーンショット ID をクリックします。

スクリーンショットを削除する

すべてのスクリーンショットを削除する場合は, *[すべて削除 (Remove all)]* をクリックします。

1 つのスクリーンショットのみを削除するには, そのスクリーンショットの ✖ ボタンをクリックします。

ユーザ インタフェースのスクリーンショットについて

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) のスクリーンショットをキャプチャすることができます。

第 5 章

デバイスの設定

デバイスの設定の概要

以降のページでは, Web インターフェイスの *[セットアップ (Setup)]* > *[設定 (Configuration)]* ページで設定されるすべてのデバイス設定のリストを示します。

Web ブラウザを開き, デバイスの IP アドレスを入力して, サインインします。

IP アドレスの確認方法

1. ユーザー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。

オーディオの設定

Audio DefaultVolume

スピーカーのデフォルト音量を定義します。ビデオ会議デバイスのスイッチをオンにするか再起動すると，音量がこの値に設定されます。実行中に音量を変更するには，ユーザ インターフェイスのコントロールを使用します。また，API コマンド (xCommand Audio Volume) を使用して，デバイスの稼働中に音量を変更したり，デフォルト値にリセットしたりすることもできます。

必要なユーザ ロール : ADMIN, INTEGRATOR, USER

デフォルト値: 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。

Audio KeyClickDetector Attenuate

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。

Audio KeyClickDetector Enabled

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。

Audio SoundsAndAlerts RingTone

着信コールに使用する着信音を定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR, USER

デフォルト値 : 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。

Audio SoundsAndAlerts RingVolume

着信コールの着信音量を定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR, USER

デフォルト値: 50

値スペース : 整数 (0..100)

範囲 : 値は 5 刻みで 0 ～ 100 (-34.5 dB ～ 15 dB) になります。音量 0 = オフです。

Audio Ultrasound Mode

この設定は, インテリジェント プロキシミティ機能に適用されます。設定はデフォルト値のままにしておいてください。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : 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 ウルトラサウンド最大音量 (Audio Ultrasound MaxVolume)] の設定で定義された最大レベルまでさまざまに変化します。

Static : Cisco が助言した場合にのみ使用してください。

Audio Ultrasound MaxVolume

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

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値: 70

値スペース : 整数 (0..70)

値は指定の範囲内から選択します。0 に設定すると, 超音波がオフになります。

BYOD 設定

BYOD TouchForwarding Enabled

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。

タッチリダイレクトは, コール中でないときにのみ機能します。

ソフトウェアバージョン CE9.9.0 では, タッチリダイレクトが常に有効になり, この設定は使用できません。また, 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

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。

CallHistory 設定

CallHistory Mode

不在着信や応答されなかったコールを含めて, 発着信コールに関する情報を保存するかどうかを決定します (通話履歴) 。これにより, ユーザ インターフェイスの Recents リストにコールが表示されるかどうかが決まります。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : 新しいエントリが通話履歴に追加されません。

On : 新しいエントリは通話履歴一覧に保存されます。

カメラ設定

Cameras Camera [n] Backlight DefaultMode

n: 1.. 1

このコンフィギュレーションは, 逆光補正をオンまたはオフにします。逆光補正は, 部屋の中で人物の背後に強い光がある場合に役立ちます。逆光補正がないと, こちらの画像が相手に非常に暗い状態で見えてしまいます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Off

値スペース : Off/On

Off : カメラの逆光補正をオフにします。

On : カメラの逆光補正をオンにします。

Cameras Camera [n] Brightness Mode

n: 1.. 1

カメラの明るさモードを定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Manual

Auto : カメラの明るさはデバイスによって自動的に設定されます。

Manual : カメラの明るさの手動設定を有効にします。明るさのレベルは, Cameras Camera [n] Brightness DefaultLevel 設定を使用して設定します。

Cameras Camera [n] Brightness DefaultLevel

n: 1.. 1

明るさのレベルを定義します。カメラの明るさモード Cameras Camera [n] Brightness Mode を [手動 (Manual)] に設定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: 20

値スペース : 整数 (1..31)

明るさレベル。

Cameras Camera [n] Focus Mode

n: 1.. 1

カメラのフォーカス モードを定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Manual

Auto : 通話がつながった時点, およびビューが変更された後にカメラがシングル ショット オートフォーカスを行います。

Manual : オートフォーカスをオフにし, カメラの焦点を手動で調整します。

Cameras Camera [n] Gamma Mode

n: 1.. 1

この設定は, ガンマ補正を有効にします。ガンマは, 画像ピクセルとモニタの明るさとの間の関係を表します。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Manual

Auto : 自動がデフォルトであり, 推奨設定です。

Manual : 手動モードではガンマ値はガンマ レベル設定で変更されます。Cameras Camera [n] Gamma Level を参照してください。

Cameras Camera [n] Gamma Level

n: 1.. 1

ガンマ レベルを設定して, 使用するガンマ修正テーブルを選択できます。この設定は, 明るさの設定を変更しても十分な結果が得られない困難な光条件に役立つことがあります。カメラのガンマ モード Cameras Camera [n] Gamma Mode を [手動 (Manual)] に設定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: 0

値スペース : 整数 (0..7)

ガンマ レベルを定義します。

Cameras SpeakerTrack Mode

ビデオ会議デバイスはベストオーバービュー機能をサポートしています。最高の概要は自動カメラ 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。スピーカートラッキングはサポートされていません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Off

自動: ベスト概要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。ユーザーは, 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, 次のユーザーに備えて機能が再度オンになります。

オフ: ベスト概要がオフになっています。

会議設定

Conference ActiveControl Mode

アクティブコントロールは, 会議参加者がビデオ会議デバイスのインターフェイスを使用して Cisco TelePresence Server または Cisco Meeting Server の会議を管理できるようにする機能です。各ユーザは, 参加者リストの表示, ビデオ レイアウトの変更, 参加者の接続解除などをインターフェイスから行えます。アクティブ コントロール機能は, インフラストラクチャ (Cisco Unified Communications Manager (CUCM) バージョン 9.1.2 以降, Cisco TelePresence Video Communication Server (VCS) バージョン X8.1 以降, Cisco Media Server (CMS) バージョン 2.1 以降) でサポートされている限り, デフォルトでイネーブルです。アクティブ コントロール機能を無効にするには, この設定を変更します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Off

Auto : アクティブ コントロールがインフラストラクチャでサポートされている場合に有効になります。

Off : アクティブ コントロールは無効です。

Conference AutoAnswer Mode

自動応答モードを定義します。デバイスを使用してコールに応答する前に数秒間待機する場合は, Conference AutoAnswer Delay 設定を使用し, コールに応答するときにマイクをミュートする場合は Conference AutoAnswer Mute 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : 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。

Conference AutoAnswer Mute

着信コールに自動応答する場合にマイクをミュートにするかどうかを定義します。AutoAnswer Mode が有効にされている必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : 着信コールはミュートにされません。

On : 着信コールは自動的に応答されるときミュートにされます。

Conference AutoAnswer Delay

デバイスが自動応答するまで着信コールが待つ必要がある時間 (秒単位) を定義します。[自動応答モード (AutoAnswer Mode)] が有効にされている必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..50)

自動応答遅延 (秒単位) 。

Conference CallProtocolIPStack

デバイスで通信プロトコル (SIP, H323) の IPv4, IPv6, またはデュアル IP スタックを有効にする必要がある場合に選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Dual

値スペース : Dual/IPv4/IPv6

Dual : 通信プロトコルの IPv4 と IPv6 の両方をイネーブルにします。

IPv4 : [IPv4] に設定すると, 通信プロトコルは IPv4 を使用します。

IPv6 : [IPv6] に設定すると, 通信プロトコルは IPv6 を使用します。

Conference DefaultCall Protocol

デバイスからコールを発信するときに使用するデフォルトのコールプロトコルを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/H320/H323/Sip/Spark

Auto : 使用可能なプロトコルに基づいた通信プロトコルの自動選択をイネーブルにします。複数のプロトコルが使用可能な場合, 優先順位は次の通りです : 1) SIP, 2) H323, 3) H320。デバイスが登録を実行できない場合, 自動選択により H323 が選択されます。

H320 : すべてのコールが H.320 コールとしてセットアップされます (Cisco TelePresence ISDN リンクとともに使用している場合のみ) 。

H323 : すべてのコールが H.323 コールとして設定されます。

SIP : すべてのコールが SIP コールとして設定されます。

Spark : Webex 登録済みデバイスのために予約されています。使用しません。

Conference DefaultCall Rate

デバイスからコールを発信するときに使用するデフォルトのコールレートを定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR

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。

Conference DoNotDisturb DefaultTimeout

この設定はサイレント セッションのデフォルト期間, つまり着信コールが拒否され, 不在履歴として登録される時間を決定します。セッションは, ユーザ インターフェイスを使用して早期に終了できます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値: 60

値スペース : 整数 (1..1440)

DoNotDisturb (着信拒否) セッションが自動的にタイム アウトするまでの分数 (最大 1440 分, つまり 24 時間) 。

Conference Encryption Mode

会議の暗号化モードを定義します。会議が開始されると, 数秒間画面に鍵と「Encryption On」または「Encryption Off」という文字が表示されます。

注 : 暗号化オプションキーがデバイスにインストールされていない場合, 暗号化モードは常に [オフ (Off)] になります。

必要なユーザ ロール : ADMIN

デフォルト値 : BestEffort

値スペース : Off/On/BestEffort

Off : デバイスは暗号化を使用しません。

On : デバイスは, 暗号化されたコールだけを許可します。

BestEffort : デバイスは暗号化を可能な限り使用します。

> ポイントツーポイントコール : 相手先デバイスで暗号化 (AES-128) がサポートされている場合, コールは暗号化されます。そうでない場合は, コールは暗号化なしで送信されます。

> MultiSite コール : 暗号化されたマルチサイト会議を実現するためには, すべてのサイトが暗号化をサポートしている必要があります。そうでない場合は, 会議は暗号化されません。

Conference FarEndControl Mode

リモート側 (遠端) にこちら側のビデオ ソースの選択とローカル カメラの制御 (パン, 傾斜, ズーム) を許可するかどうか決定できます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 相手先はこちら側のビデオ ソースの選択やローカル カメラの制御 (パン, チルト, ズーム) を許可されません。

On : 遠端にこちら側のビデオ ソースの選択とローカル カメラの制御 (パン, 傾斜, ズーム) を許可します。カメラの制御とビデオ ソースの選択は, こちら側でも通常どおり可能です。

Conference FarEndControl SignalCapability

遠端制御 (H.224) 信号機能モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 遠端制御信号機能をディセーブルにします。

On : 遠端制御信号機能をイネーブルにします。

Conference FarEndMessage Mode

制御システムまたはマクロと併用するために, ポイントツーポイントコールにおける 2 台のデバイス間でデータ送信が許可されているかどうかを切り替えます。SIP コールでのみ動作します。この設定は, 遠隔メッセージ送信コマンドの xCommand のコール使用を有効化または無効化します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : 2 台のデバイス間でメッセージを送信できません。

On : ポイントツーポイントコールの 2 台のデバイス間でメッセージ送信を行うことができます。

Conference MaxReceiveCallRate

コールの発信または受信時に使用する最大受信ビット レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには, Conference MaxTotalReceiveCallRate 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : 10000

値スペース : 整数 (64 ～ 10000)

最大受信帯域 (kbps) 。

Conference MaxTransmitCallRate

コールの発信または受信時に使用する最大送信ビット レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには, Conference MaxTotalTransmitCallRate 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大送信帯域 (kbps) 。

Conference MaxTotalReceiveCallRate

この設定は, デバイスに搭載されたマルチサイト機能 (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, Conference MaxReceiveCallRate 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) 。

Conference MaxTotalTransmitCallRate

この設定は, デバイスに搭載されたマルチサイト機能 (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, Conference MaxTransmitCallRate 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) 。

Conference MicUnmuteOnDisconnect Mode

すべてのコールが切断されたときに, マイクを自動的にミュート解除するかどうかを定義します。会議室またはその他の共有リソースでは, 次のユーザーに向けてデバイスを準備するためにこれが実行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 : On

値スペース : Off/On

Off : コール中にミュートにされている場合, コールが切断された後もマイクロフォンをミュートにされたままにします。

On : コールが切断された後にマイクロフォンのミュートを解除します。

Conference Multipoint Mode

ポイントツーポイントビデオコール (2 者間のコール) から, 参加者を追加してマルチポイント会議 (アドホック会議) に拡大する方法を定義します。ローカルのリソースのみに依存する組み込みのマルチサイト機能と, 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。

マルチサイト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。デバイスにマルチサイト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ときにマルチサイトを使用できます。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, またはデバイスに搭載されたマルチサイト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, デバイスによる会議への参加者の追加 (直接リモート追加) を許可している MCU をコールすると, 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。

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 : マルチポイント方式が自動的に選択されます。

マルチサイトオプションキーがデバイスにインストールされており, (MCU ではない) 他のビデオデバイスをコールする場合は, 搭載されたマルチサイト機能を使用してマルチパーティ会議がセットアップされます。参加者を追加できるのはマルチサイトホストのみです。これにより, 会議のカスケードを防ぎます。デバイスにマルチサイト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コールすることはできません。音声のみの参加者を 1 人追加できます。

マルチサイトオプションキーに関係なく, デバイスによる会議への参加者の追加 (直接リモート追加) を許可している MCU をコールする場合, MCU を介してマルチパーティ会議をセットアップできます。

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 : デバイスにマルチサイトオプションキーがインストールされている場合は, 搭載されたマルチサイト機能を使ってマルチパーティ会議がセットアップされます。デバイスにマルチサイト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。オーディオのみのデバイスを 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, オーディオのみのデバイスを追加できます。デバイスによる会議への参加者の追加 (直接リモート追加) を許可している MCU をコールする場合, MCU を介してマルチパーティ会議がセットアップされます。

Conference IncomingMultisiteCall Mode

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。

Conference Presentation OnPlacedOnHold

リモート サイトで保留状態にされた後, プレゼンテーションを共有し続けるかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : NoAction

設定可能な値 : NoAction/Stop

NoAction : 保留しても, デバイスはプレゼンテーションの共有を停止しません。保留されている間はプレゼンテーションは共有されませんが, コールが再開されると自動的に継続されます。

Stop : リモートサイトで保留されると, デバイスはプレゼンテーションの共有を停止します。コールが再開されてもプレゼンテーションは継続されません。

Conference Presentation RelayQuality

この設定は, 搭載されたマルチサイト機能 (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。リモートユーザー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。

Conference VideoBandwidth Mode

会議ビデオ帯域幅モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : ビデオ チャネルの使用可能な送信帯域幅が現在アクティブなチャネル間で分散されます。プレゼンテーションが存在しない場合は, メイン ビデオ チャネルがプレゼンテーション チャネルの帯域幅を使用します。

Static : 使用可能な送信帯域幅が, アクティブでない場合でも各ビデオ チャネルに割り当てられます。

FacilityService 設定

FacilityService Service [n] Type

n: 1..5

最大 5 種類のファシリティ サービスを同時にサポートできます。この設定で, どのようなサービスかを選択できます。ファシリティ サービスは, FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは, ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Helpdesk

値スペース : Catering/Concierge/Emergency/Helpdesk/Security/Transportation/Other

Catering : ケータリング サービスには, このオプションを選択します。

Concierge : コンシェルジュ サービスには, このオプションを選択します。

Emergency : 緊急サービスには, このオプションを選択します。

Helpdesk : ヘルプ デスク サービスには, このオプションを選択します。

Security : セキュリティ サービスには, このオプションを選択します。

Transportation : 転送サービスには, このオプションを選択します。

Other : その他のオプションでカバーされないサービスには, このオプションを選択します。

FacilityService Service [n] Name

n: 1..5

ファシリティ サービスの名前を定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは, FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。名前は, 上部バーの疑問符アイコンをタップすると表示されるファシリティ サービス コール ボタンに表示されます。施設サービスは, ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Service 1 : "Live Support" その他のサービス : ""

値スペース : 文字列 (0, 1024)

ファシリティ サービスの名前。

FacilityService Service [n] Number

n: 1..5

ファシリティ サービスの番号 (URI または電話番号) を定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは, FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは, ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値: ""

値スペース : 文字列 (0, 1024)

ファシリティ サービスの番号 (URI または電話番号) 。

FacilityService Service [n] CallType

n: 1..5

各ファシリティ サービスのコール タイプを定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは, FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは, ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Video

値スペース : Audio/Video

Audio : オーディオ コールには, このオプションを選択します。

Video : ビデオ コールには, このオプションを選択します。

H323 設定

H323 Authentication Mode

H.323 プロファイルの認証モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : デバイスは H.323 ゲートキーパーに対して自身の認証を試行せず, 通常の登録を試行します。

On : 認証が必要なことを H.323 ゲートキーパーから示されると, デバイスはゲートキーパーに対して自身の認証を試みます。デバイスとゲートキーパーの両方で, H323 Authentication LoginName と H323 Authentication Password の設定を定義する必要があります。

H323 Authentication LoginName

デバイスは認証のために, H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はデバイスから H.323 ゲートキーパーへの単方向の認証です。つまり, デバイスはゲートキーパーに認証されます。認証が不要であることを H.323 ゲートキーパーが示している場合でも, デバイスは登録を試行します。H.323 認証モードを有効にする必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

認証ログイン名。

H323 Authentication Password

デバイスは認証のために, H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はデバイスから H.323 ゲートキーパーへの単方向の認証です。つまり, デバイスはゲートキーパーに認証されます。認証が不要であることを H.323 ゲートキーパーが示している場合でも, デバイスは登録を試行します。H.323 認証モードを有効にする必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

認証パスワード。

H323 CallSetup Mode

H.323 コールを確立するときにゲートキーパーとダイレクト コールのどちらを使用するかを定義します。

ダイレクト H.323 コールは, H323 CallSetup Mode が Gatekeeper に設定されている場合も発信できます。

必要なユーザ ロール : ADMIN

デフォルト値 : Gatekeeper

値スペース : Direct/Gatekeeper

Direct : IP アドレスに直接ダイヤルすることによってのみ, H.323 コールを発信できます。

Gatekeeper : デバイスは, H.323 コールを発信するためにゲートキーパーを使用します。このオプションを選択する場合は, H323 Gatekeeper Address も設定する必要があります。

H323 Encryption KeySize

Advanced Encryption Standard (AES) 暗号化キーの確立時に使用する Diffie-Hellman キー交換方式の最小または最大のキー サイズを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Min1024bit

設定可能な値 : Max1024bit/Min1024bit/Min2048bit

Max1024bit : 最大サイズは 1024 ビットです。

Min1024bit : 最小サイズは 1024 ビットです。

Min2048bit : 最小サイズは 2048 ビットです。

H323 Gatekeeper Address

ゲートキーパーの IP アドレスを定義します。H323 CallSetup Mode を Gatekeeper に設定する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

H323 H323Alias E164

H.323 エイリアス E.164 は, H.323 ゲートキーパーに設定された番号計画に従ってデバイスのアドレスを定義します。E.164 エイリアスは電話番号と同じであり, アクセス コードと結合される場合もあります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 30)

H.323 Alias E.164 のアドレス。使用できる文字は, 0 ～ 9, *, # です。

H323 H323Alias ID

H.323 エイリアス ID を定義します。この ID は, H.323 ゲートキーパーでデバイスのアドレス指定に使用され, コールリストに表示されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 49)

H.323 エイリアス ID。例 : "firstname.lastname@company.com", "My H.323 Alias ID"

H323 NAT Mode

ファイアウォールトラバーサルテクノロジーは, ファイアウォール障壁を通過するセキュアなパスを作成し, 外部のビデオ会議デバイスに接続されたときのオーディオまたはビデオのデータの正しい交換を可能にします (IP トラフィックが NAT ルータを通過する場合) 。注 : NAT は, ゲートキーパーとの組み合わせでは動作しません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Auto/Off/On

Auto : H323 NAT アドレスと実際の IP アドレスのどちらをシグナリングに使用するかをデバイスが決定します。これにより, LAN 上のデバイス, または WAN のデバイスにコールを発信できるようになります。H323 NAT アドレスが間違っているか設定されていない場合, 実際の IP アドレスが使用されます。

Off : デバイスは, 実際の IP アドレスをシグナリングします。

On : デバイスは, Q.931 および H.245 内にある実際の IP アドレスの代わりに, 設定された H323 NAT アドレスをシグナリングします。NAT サーバ アドレスは, スタートアップ メニューに [My IP Address: 10.0.2.1] と表示されます。H323 NAT アドレスが間違っているか設定されていない場合, H.323 コールは設定できません。

H323 NAT Address

NAT 対応ルータの外部/グローバル IP アドレスを定義します。ルータに送信されるパケットは, ビデオ会議デバイスにルーティングされます。ゲートキーパーに登録されている場合は NAT を使用できないことに注意してください。

ルータで, 次のポートはビデオ会議デバイスの IP アドレスにルーティングする必要があります。

* ポート 1720

*ポート 5555-6555

*ポート 2326-2487

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

H323 PortAllocation

この設定は, H.323 コール シグナリングに使用される H.245 ポート番号に影響を与えます。

必要なユーザ ロール : ADMIN

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : TCP 接続を開くとき, 使用するポートをシステムが割り当てます。このようにする理由は, 後続のコールで同じポートを使用しないようにするためです。一部のファイアウォールはこれを攻撃の徴候と見なします。Dynamic を選択した場合, 使用される H.323 ポートは 11000 ～ 20999 です。20999 に達すると 11000 から再スタートされます。ポートは, 特定の範囲内でシステムによって自動的に選択されます。ファイアウォール管理者は, どのポートがいつ使用されるかを推定しようとしてはなりません。指示された範囲内の割り当てスキーマがより詳細な通知なしで変更されることがあるからです。

Static : スタティックに設定すると, スタティックに事前定義された範囲 [5555-6555] 内でポート指定されます。

HttpClient 設定

HttpClient 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) サーバーと通信できません。

On : ビデオ会議デバイスは外部 HTTP (S) サーバーと通信できます。

HttpClient AllowHTTP

HttpClient モード の設定は, 外部 HTTPs サーバとの通信を許可または禁止するために使用されます。モード設定では HTTP と HTTPS の区別をしていません。HTTP の使用を許可または禁止するには, HttpClient AllowHTTP 設定を使用する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : True

値スペース : False/True

False : ビデオ会議デバイスは, HTTPS のみで通信できます。

True : ビデオ会議デバイスは HTTPS と HTTP の両方で通信できます。

HttpClient AllowInsecureHTTPS

サーバーの証明書を最初に確認せずに, HTTPS を使用したサーバー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 サーバー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, サーバー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。

HttpFeedback の設定

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 サーバー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ーについては, [電話帳 サーバー1 Tls 検証 (Phonebook Server 1 TlsVerify)], [プロビジョニング Tls検証 (Provisioning TlsVerify)], および [ロギング 外部 Tls検証 (Logging External TlsVerify)] の設定を参照してください。

デバイスと HTTPS サーバー間の接続を確立する前に, デバイスは, サーバー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 : 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, アップグレード後にデバイスが工場出荷時設定にリセットされておらず, 以前の [ネットワーク HTTPS サーバー証明書検証 (NetworkServices HTTPS VerifyServerCertificate)] 設定が明示的に [オン (On)] に設定されていなかった場合, この値は [オフ (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 サーバーの証明書を確認しません。

On : デバイスは, HTTPS サーバー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, デバイスとサーバーの間の接続は確立されません。

ロギングの設定

Logging Debug Wifi

このオプションを有効にすると, デバイスは, デバイスとアクセスポイントの間の Wi-Fi 接続のセットアップやメンテナンスについて詳細な情報を記録します。この機能は, WiFi 接続に問題があった場合のトラブルシューティングに便利です。Wi-Fi 接続が期待通りに動作している場合は, この設定をオフにすることを推奨します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 基本 Wi-Fi 情報だけをロギング。

On : Wi-Fi 接続についての大量の情報をロギング。

Logging External Mode

デバイスログをリモート syslog サーバーに保管するかどうかを決定します。ロギングモード設定がオフに設定されている場合, この設定には効果がありません。

リモートサーバのアドレスをロギング外部サーバ アドレス設定に入力する必要があります。ロギング外部サーバ ポートセットに記載されていない限り, 標準規格 syslog ポートが使用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : デバイスログはリモート syslog サーバーに保存されません。

On : デバイスログはリモート syslog サーバーに保存されます。

Logging External Protocol

リモート ロギング サーバに対して使用するプロトコルを決定します。syslog プロトコル over TLS (Transport Layer Security) , またはプレーンテキストの syslog プロトコルのいずれかを使用できます。syslog プロトコルの詳細については, RFC 5424 を参照してください。

必要なユーザ ロール : ADMIN

デフォルト値 : SyslogTLS

値スペース : Syslog/SyslogTLS

Syslog : プレーン テキストの syslog プロトコル。

SyslogTLS : syslog プロトコル over TLS。

Logging External Server Address

リモート syslog サーバの IP アドレス。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

Logging External Server Port

リモート syslog サーバがメッセージをリッスンするポート。0 に設定した場合, デバイスは標準の syslog ポートを使用します。syslog の標準 syslog ポートは 514 で, TLS を使用した syslog の標準 syslog ポートは 6514 です。

必要なユーザ ロール : ADMIN

デフォルト値: 514

値スペース : 整数 (0..65535)

リモート syslog サーバが使用しているポート番号。0 は, デバイスが標準 syslog ポートを使用することを意味します。

Logging External TlsVerify

この設定は, ビデオ会議デバイスがリモートの syslog サーバーに接続している場合に適用されます。通常のログ作成 (Logging External Mode の設定を参照) と監査ログ (Security Audit Logging Mode の設定を参照) の両方に適用されます。

デバイスと syslog サーバーの間の接続を確立する前に, デバイスは, サーバー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 サーバーの証明書を確認しません。

On : デバイスは, syslog サーバー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, デバイスとサーバーの間の接続は確立されません。

Logging Internal Mode

システムログをデバイス (ローカルファイル) に保存するかどうかを決定します。これらは, ログバンドルをデバイスからダウンロードした際に得られるファイルです。ロギングモード設定がオフに設定されている場合, この設定には効果がありません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : システムログはデバイスに保存されません。

On : システムログはデバイスに保存されます。

Logging Mode

デバイスのロギングモード (syslog サービス) を定義します。無効にすると, syslog サービスが起動せず, システムログと監査ログのほとんどが生成されません。履歴ログと通話履歴は影響を受けません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : システムのロギング サービスを無効にします。

On : システムのロギング サービスを有効にします。

マクロ設定

Macros Mode

マクロによって，ビデオ会議デバイスの一部を自動化できる JavaScript コードのスニペットを記述できます。これによりカスタム動作を作成します。デフォルトではマクロの使用は無効化されていますが，最初にマクロエディタを開くときにデバイスでのマクロ使用を有効にするかどうか確認を求められます。デバイスのマクロの使用を手動で有効にする場合や，完全に無効にする場合は，この設定を使用します。マクロ エディタ内でのマクロの使用を無効にすることができます。ただし，デバイスがマクロをリセットするたびにマクロが自動的に再び有効化されるため，マクロの実行は永続的に無効にはなりません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : このデバイス上でのマクロの使用を完全に無効にします。

On : このデバイス上でのマクロの使用を有効にします。

Macros AutoStart

すべてのマクロは，マクロランタイムに呼び出され，ビデオ会議デバイスにおいてシングルプロセスで実行されます。デフォルトでは実行されている必要がありますが，手動での停止と開始を選択することができます。自動開始が有効化されている場合，デバイスを再起動するときにランタイムは自動的に再び開始されます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスの再起動後，マクロランタイムは自動的に開始されません。

On : デバイスの再起動後，マクロランタイムは自動的に開始されます。

ネットワーク設定

Network [n] DNS DNSSEC Mode

n: 1..1

ドメイン ネーム システム セキュリティ拡張 (DNSSEC) は, DNS の拡張セットです。署名されたゾーンの DNS の応答を認証するために使用されます。署名されていないゾーンを引き続き許可します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : ドメイン ネーム システム セキュリティ拡張を無効にします。

On : ドメイン ネーム システム セキュリティ拡張を有効にします。

Network [n] DNS Domain Name

n: 1..1

DNS ドメイン名は非修飾名に追加されるデフォルトのドメイン名サフィックスです。

例 : DNS ドメイン名が「company.com」で, ルックアップする名前が「MyVideoSystem」の場合, DNS ルックアップ「MyVideoSystem.company.com」になります。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

DNS ドメイン名。

Network [n] DNS Server [m] Address

n: 1..1

m: 1..3

DNS サーバのネットワーク アドレスを定義します。最大 3 つまでのアドレスを指定できます。ネットワーク アドレスが不明の場合, 管理者またはインターネット サービス プロバイダーに問い合わせます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [n] IEEE8021X Mode

n: 1..1

デバイスは, ポートベースのネットワークアクセスコントロールによって, IEEE 802.1X LAN ネットワークに接続できます。このアクセスコントロールは, イーサネットネットワークに認証済みネットワークアクセスを提供するために使用されます。

必要なユーザ ロール : admin, user

デフォルト値 : Off

値スペース : Off/On

Off : 802.1X 認証が無効になります。

On : 802.1X 認証が有効になります。

Network [n] IEEE8021X TlsVerify

n: 1..1

TLS を使用する場合の, ローカル CA リストの証明書に対する IEEE802.1x 接続のサーバ側証明書の検証です。CA リストがビデオ会議デバイスにアップロードされている必要があります。これは, ウェブ インターフェイスから実行できます。

この設定は, Network [1] IEEE8021X Eap Tls が有効 (On) の場合にのみ有効です。

必要なユーザ ロール : admin, user

デフォルト値 : Off

値スペース : Off/On

Off : Off に設定する場合, ローカル CA リストに対するサーバ側 X.509 証明書を確認せずに, TLS 接続が許可されます。これは, デバイスに CA リストがアップロードされていない場合に選択する必要があります。

On : On に設定する場合, すべての TLS 接続のローカル CA リストに対して, サーバ側 X.509 証明書が検証されます。有効な証明書を持つサーバだけが許可されます。

Network [n] IEEE8021X UseClientCertificate

n: 1..1

IEEE802.1x 接続中の, 秘密キーと証明書のペアを使用した認証。認証 X.509 証明書がビデオ会議デバイスにアップロードされている必要があります。これは, ウェブ インターフェイスから実行できます。

必要なユーザ ロール : admin, user

デフォルト値 : Off

値スペース : Off/On

Off : Off に設定した場合, クライアント側の証明書は使用されません (サーバ側のみ) 。

On : On に設定した場合, クライアント (ビデオ会議デバイス) はサーバーと相互認証 TLS ハンドシェイクを実行します。

Network [n] IEEE8021X Identity

n: 1..1

802.1X 認証用のユーザー名を定義します。

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 認証用のユーザー名。

Network [n] IEEE8021X Password

n: 1..1

802.1X 認証用のパスワードを定義します。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 50)

802.1X 認証用のパスワード。

Network [n] IEEE8021X AnonymousIdentity

n: 1..1

802.1X 匿名 ID 文字列は, 別のトンネリングされた ID をサポートする EAP-PEAP および EAP-TTLS などの EAP (Extensible Authentication Protocol) タイプとともに, 非暗号化 ID として使用されます。設定された場合, 匿名 ID は最初の (非暗号化) EAP ID 要求に使用されます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

802.1X 匿名 ID 文字列。

Network [n] IEEE8021X Eap Md5

n: 1..1

MD5 (メッセージダイジェスト アルゴリズム 5) モードを定義します。これは, 共有秘密に依存するチャレンジ ハンドシェイク認証プロトコルです。MD5 は弱いセキュリティです。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : EAP-MD5 プロトコルが無効になります。

On : EAP-MD5 プロトコルが有効になります。

Network [n] IEEE8021X Eap Ttls

n: 1..1

TTLS (トンネル方式トランスポート層セキュリティ) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Funk Software および Certicom によって開発されました。通常 Agere Systems, Proxim および Avaya でサポートされます。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : EAP-TTLS プロトコルが無効になります。

On : EAP-TTLS プロトコルが有効になります。

Network [n] IEEE8021X Eap Tls

n: 1..1

IEEE802.1x 接続用の EAP-TLS (トランスポート層セキュリティ) の使用をイネーブルまたはディセーブルにします。RFC5216 で定義された EAP-TLS プロトコルは最もセキュアな EAP 標準の 1 つと見なされています。LAN クライアントは, クライアント証明書を使用して認証されます。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : EAP-TLS プロトコルが無効になります。

On : EAP-TLS プロトコルが有効になります。

Network [n] IEEE8021X Eap Peap

n: 1..1

PEAP (Protected Extensible Authentication Protocol) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Microsoft, Cisco と RSA Security により開発されました。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : EAP-PEAP プロトコルが無効になります。

On : EAP-PEAP プロトコルが有効になります。

Network [n] IPStack

n: 1..1

デバイスのネットワークインターフェイスで IPv4, IPv6, またはデュアル IP スタックを使用する必要がある場合に選択します。注 : この設定を変更した後, 反映されるまでに 30 秒間待つ必要があります。

必要なユーザ ロール : admin, user

デフォルト値 : Dual

値スペース : Dual/IPv4/IPv6

Dual : [デュアル (Dual)] に設定すると, ネットワーク インターフェイスは両方の IP バージョンで同時に動作することができ, また, IPv4 アドレスと IPv6 アドレスの両方を同時に持つことができます。

IPv4 : IPv4 に設定すると, デバイスのネットワークインターフェイスで IPv4 が使用されます。

IPv6 : IPv6 に設定すると, デバイスのネットワークインターフェイスで IPv6 が使用されます。

Network [n] IPv4 Assignment

n: 1..1

デバイスが IPv4 アドレス, サブネットマスク, およびゲートウェイアドレスを取得する方法を定義します。

アドレス割り当てに DHCP を利用する場合は, MAC アドレスによって最後に付加される「01」が, DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール : admin, user

デフォルト値 : DHCP

値スペース : Static/DHCP

Static : アドレスは, Network IPv4 Address, Network IPv4 Gateway, Network IPv4 SubnetMask の各設定 (静的アドレス) を使用して手動で設定する必要があります。

DHCP : デバイスアドレスは DHCP サーバーによって自動的に割り当てられます。

Network [n] IPv4 Address

n: 1..1

デバイスのスタティック IPv4 ネットワークアドレスを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

Network [n] IPv4 Gateway

n: 1..1

IPv4 ネットワーク ゲートウェイ アドレスを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

Network [n] IPv4 SubnetMask

n: 1..1

IPv4 ネットワークのサブネット マスクを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

Network [n] IPv6 Assignment

n: 1..1

デバイスが IPv6 アドレスおよびデフォルトゲートウェイアドレスを取得する方法を定義します。

アドレス割り当てに DHCPv6 を利用する場合は, MAC アドレスによって最後に付加される「01」が, DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール : admin, user

デフォルト値 : Autoconf

値スペース : Static/DHCPv6/Autoconf

Static : デバイスおよびゲートウェイの IP アドレスは, [ネットワーク IPv6 アドレス (Network IPv6 Address)] および [ネットワーク IPv6 ゲートウェイ (Network IPv6 Gateway)] の設定を使用して手動で設定する必要があります。NTP アドレスや DNS サーバ アドレスなどのオプションは, 手動で設定するか, または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は, どの方法を使用するかを決定します。

DHCPv6 : オプションを含むすべての IPv6 アドレスは, DHCPv6 サーバから取得されます。詳細については RFC3315 を参照してください。Network IPv6 DHCPOption 設定は無視されます。

Autoconf : IPv6 ネットワーク インターフェイスの IPv6 ステートレス自動設定をイネーブルにします。詳細については RFC4862 を参照してください。NTP アドレスや DNS サーバ アドレスなどのオプションは, 手動で設定するか, または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は, どの方法を使用するかを決定します。

Network [n] IPv6 Address

n: 1..1

デバイスのスタティック IPv6 ネットワークアドレスを定義します。Network IPv6 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

ネットワーク マスクを含む有効な IPv6 アドレス。例 : 2001:DB8::/48

Network [n] IPv6 Gateway

n: 1..1

IPv6 ネットワーク ゲートウェイ アドレスを定義します。この設定は, Network IPv6 Assignment が Static に設定されている場合にのみ適用されます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv6 アドレス。

Network [n] IPv6 DHCPOptions

n: 1..1

DHCPv6 サーバから一連の DHCP オプション (NTP および DNS サーバ アドレスなど) を取得します。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : DHCPv6 サーバからの DHCP オプションの取得を無効にします。

On : 選択した DHCP オプションのセットの DHCPv6 サーバからの取得をイネーブルにします。

Network [n] MTU

n: 1..1

イーサネット MTU (最大伝送ユニット) サイズを定義します。MTU サイズは, ネットワーク インフラストラクチャでサポートする必要があります。IPv4 の場合, 最小サイズは 576 で, IPv6 の場合, 最小サイズは 1280 です。

必要なユーザ ロール : admin, user

デフォルト値: 1500

値スペース : 整数 (576..1500)

MTU の値を設定します (バイト単位) 。

Network [n] QoS Mode

n: 1..1

QoS (Quality of Service) は, ネットワーク内のオーディオ, ビデオおよびデータの優先順位を操作するメソッドです。QoS 設定はインフラストラクチャでサポートされている必要があります。DiffServ (ディファレンシエーテッド サービス) は, ネットワーク トラフィックの分類と管理を行い, 現代的 IP ネットワークに QoS を提供するためにシンプルかつスケーラブルで粗粒度のメカニズムを指定する, コンピュータ ネットワーキング アーキテクチャです。

必要なユーザ ロール : admin, user

デフォルト値 : Diffserv

値スペース : Off/Diffserv

Off : QoS メソッドは使用されません。

Diffserv : QoS モードを Diffserv に設定すると, Network QoS Diffserv Audio, Network QoS Diffserv Video, Network QoS Diffserv Data, Network QoS Diffserv Signalling, Network QoS Diffserv ICMPv6, および Network QoS Diffserv NTP の各設定を使用してパケットの優先順位が付けられます。

Network [n] QoS Diffserv Audio

n: 1..1

この設定は, Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

パケットのプライオリティは, 0 ～ 63 です。数字が大きいほど, 優先順位が高くなります。音声に推奨されるクラスは, 10 進数値 32 と等しい CS4 です。これを確認するには, ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は, パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin, user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの音声パケットの優先順位を設定します。数値が大きいほど, 優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv Video

n: 1..1

この設定は, Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でビデオ パケットに持たせる優先順位を定義します。プレゼンテーション チャネル (共有コンテンツ) 上のパケットも, ビデオ パケットのカテゴリに属します。パケットのプライオリティは, 0 ～ 63 です。数字が大きいほど, 優先順位が高くなります。ビデオに推奨されるクラスは, 10 進数値 32 と等しい CS4 です。これを確認するには, ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は, パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin, user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでのビデオ パケットの優先順位を設定します。数値が大きいほど, 優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv Data

n: 1..1

この設定は, Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

パケットのプライオリティは, 0 ～ 63 です。数字が大きいほど, 優先順位が高くなります。データに対する推奨値は 0 (ベスト エフォート) です。これを確認するには, ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は, パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin, user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでのデータ パケットの優先順位を設定します。数値が大きいほど, 優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv Signalling

n: 1..1

この設定は, Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でリアルタイム処理に不可欠 (時間依存) であると考えられるシグナリング パケットに持たせる優先順位を定義します。

パケットのプライオリティは, 0 ～ 63 です。数字が大きいほど, 優先順位が高くなります。シグナリングに推奨されるクラスは, 10 進数値 24 と等しい CS3 です。これを確認するには, ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は, パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin, user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの信号パケットの優先順位を設定します。数値が大きいほど, 優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv ICMPv6

n: 1..1

この設定は, Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で ICMPv6 パケットに持たせる優先順位を定義します。

パケットのプライオリティは, 0 ～ 63 です。数字が大きいほど, 優先順位が高くなります。ICMPv6 に対する推奨値は 0 (ベスト エフォート) です。これを確認するには, ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は, パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin, user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの ICMPv6 パケットの優先順位を設定します。数値が大きいほど, 優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] QoS Diffserv NTP

n: 1..1

この設定は, Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

パケットのプライオリティは, 0 ～ 63 です。数字が大きいほど, 優先順位が高くなります。NTP に対する推奨値は 0 (ベスト エフォート) です。これを確認するには, ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は, パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin, user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの NTP パケットの優先順位を設定します。数値が大きいほど, 優先順位が高くなります。0 は「ベスト エフォート」を意味します。

Network [n] RemoteAccess Allow

n: 1..1

リモートアクセスで SSH/HTTP/HTTPS からデバイスに許可する IP アドレス (IPv4/IPv6) を定義します。複数の IP アドレスはスペースで区切られます。

ネットワーク マスク (IP 範囲) は <ip address>/N で指定されます。ここで N は IPv4 では 1 ～ 32 の範囲および IPv6 では 1 ～ 128 の範囲を表します。/N は最初の N ビットがセットされたネットワーク マスクの共通インジケータです。たとえば 192.168.0.0/24 は, 192.168.0 で開始するどのアドレスとも一致します。これらはアドレスの最初の 24 ビットだからです。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [n] Speed

n: 1..1

イーサネット リンクの速度を定義します。デフォルト値では, ネットワークとネゴシエートして自動的に速度が設定されます。このため, デフォルト値は変更しないことをお勧めします。自動ネゴシエーションを使用しない場合, 選択した速度を, ネットワーク インフラストラクチャの最も近いスイッチがサポートしているか確認してください。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/10half/10full/100half/100full/1000full

Auto : リンク速度を自動でネゴシエートします。

10half : 10 Mbps 半二重に強制リンクします。

10full : 10 Mbps 全二重に強制リンクします。

100half : 100 Mbps 半二重に強制リンクします。

100full : 100 Mbps 全二重に強制リンクします。

1000full : 1 Gbps 全二重に強制リンクします。

Network [n] TrafficControl Mode

n: 1..1

ネットワーク トラフィック制御モードを定義して, ビデオ パケットの伝送速度の制御方法を決定します。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : ビデオ パケットをリンク速度で送信します。

On : ビデオ パケットを最大 20 Mbps で送信します。発信ネットワーク トラフィックのバーストを平滑化するために使用できます。

Network [n] VLAN Voice Mode

n: 1..1

VLAN 音声モードを定義します。Cisco UCM (Cisco Unified Communications Manager) をプロビジョニング インフラストラクチャとして使用している場合, VLAN Voice Mode が Auto に自動的に設定されます。NetworkServices CDP Mode 設定が Off になっている場合は, Auto モードは機能しないことに注意してください。

必要なユーザ ロール : admin, user

デフォルト値 : Auto

値スペース : Auto/Manual/Off

Auto : Cisco Discovery Protocol (CDP) が使用可能な場合は, 音声 VLAN に ID を割り当てます。CDP を使用できない場合, VLAN はイネーブルになりません。

Manual : VLAN ID は, Network VLAN Voice VlanId の設定を使用して手動で設定されます。CDP を使用できる場合, 手動設定値は, CDP によって割り当てられた値によって却下されます。

Off : VLAN はイネーブルになりません。

Network [n] VLAN Voice VlanId

n: 1..1

VLAN 音声 ID を定義します。この設定は, ネットワーク VLAN 音声モード が Manual に設定されている場合にだけ有効になります。

必要なユーザ ロール : admin, user

デフォルト値: 1

値スペース : 整数 (1..4094)

VLAN 音声 ID を設定します。

ネットワークサービス設定

NetworkServices CDP Mode

CDP (Cisco Discovery Protocol) デーモンをイネーブルまたはディセーブルにします。CDP を有効にすると, デバイスは特定の統計情報とデバイス ID を CDP 対応スイッチにレポートします。CDP をディセーブルにする場合, [ネットワーク音声 VLAN モード (Network VLAN Voice Mode)] : [自動 (Auto)] 設定は機能しません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : CDP デーモンは無効です。

On : CDP デーモンはイネーブルです。

NetworkServices H323 Mode

デバイスでの H.323 コールの受発信を可能にするかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : H.323 コールの発信と受信の可能性をディセーブルにします。

On : H.323 コールの発信と受信の可能性を有効にします。

NetworkServices HTTP Mode

HTTP または HTTPS (セキュア HTTP) プロトコルによるデバイスへのアクセスを許可するかどうかを指定します。デバイスの Web インターフェイスは HTTP または HTTPS を使用することに注意してください。この設定を Off にすると, ウェブ インターフェイスを使用できなくなります。

セキュリティの強化 (ウェブ サーバから返されるページと要求の暗号化/暗号化解除) が必要な場合, HTTPS のみを許可します。

注 : 以前のソフトウェアバージョンから CE9.4 以降にアップグレードされたデバイスについては, アップグレード後に初期設定にリセットされていない場合, デフォルト値は HTTP+HTTPS となります。

必要なユーザ ロール : ADMIN

デフォルト値 : HTTPS (CE9.4 では HTTP +]HTTPS から HTTPS に変更)

値スペース : Off/HTTP+HTTPS/HTTPS

Off : HTTP や HTTPS によるデバイスへのアクセスを禁止します。

HTTP+HTTPS : HTTP と HTTPS の両方によるデバイスへのアクセスを許可します。

HTTPS : HTTPS によるデバイスへのアクセスを許可し, HTTP によるアクセスを禁止します。

NetworkServices HTTP Proxy LoginName

これは, HTTP プロキシへの認証に使用されるクレデンシャルのユーザー名部分です。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が手動に設定されている必要があります。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 80)

認証ログイン名。

NetworkServices HTTP Proxy Password

これは, HTTP プロキシへの認証に使われるクレデンシャルのパスワード部分です。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が手動に設定されている必要があります。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

認証パスワード。

NetworkServices HTTP Proxy Mode

Cisco Webex クラウドサービスに登録されているデバイスを設定して, HTTPS および WebSocket トラフィックにプロキシサーバーを使用することができます。Cisco Webex の HTTP プロキシを手動でセットアップすることができます。自動設定 (PACUrl) , 完全自動 (WPAD) , またはオフにしておくことができます。

デバイスが CUCM または VCS などのオンプレミスサービスに登録されている場合は, この設定を [オフ (Off)] のままにしておきます。

必要なユーザ ロール : admin, user

デフォルト値 : Off

値スペース : Manual/Off/PACUrl/WPAD

Manual : ネットワーク サービス HTTP プロキシ URL 設定にプロキシ サーバのアドレスを入力します。必要応じて, ネットワーク サービス HTTP プロキシ ログイン名/パスワード設定に HTTP プロキシのログイン名とパスワードを追加します。

Off : HTTP プロキシ モードがオフになっています。

PACUrl : HTTP プロキシは自動構成です。ネットワーク サービス HTTP プロキシ PACUrl 設定で PAC (プロキシ自動設定) スクリプトの URL を入力する必要があります。

WPAD : WPAD (Web プロキシ自動検出) を使用して, HTTP のプロキシは完全に自動化されかつ自動構成されます。

NetworkServices HTTP Proxy Url

HTTP プロキシ サーバの URL を設定します。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が手動に設定されている必要があります。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0..255)

HTTP プロキシ サーバの URL。

NetworkServices HTTP Proxy PACUrl

PAC (プロキシ自動構成) スクリプトの URL を設定します。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が PACUrl に設定されている必要があります。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0..255)

PAC (プロキシ自動構成) スクリプトの URL。

NetworkServices HTTPS OCSP Mode

OCSP (Online Certificate Status Protocol) レスポンダ サービスのサポートを定義します。OCSP 機能により, 証明書失効リスト (CRL) の代わりに OCSP を有効にして, 証明書のステータスをチェックできます。

すべての発信 HTTPS 接続に対して, OCSP レスポンダを介してステータスが照会されます。対応する証明書が失効している場合, HTTPS 接続は使用されません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : OCSP サポートを無効にします。

On : OCSP サポートを有効にします。

NetworkServices HTTPS OCSP URL

証明書のステータスを調べるために使用される OCSP レスポンダ (サーバ) の URL を定義します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な URL。

NetworkServices HTTPS Server MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN
デフォルト値 : TLSv1.1

値スペース : TLSv1.1/TLSv1.2
TLSv1.1 : TLS バージョン 1.1 以降のサポート。
TLSv1.2 : TLS バージョン 1.2 以降のサポート。

NetworkServices HTTPS StrictTransportSecurity

HTTP Strict Transport Security ヘッダーにより, ウェブ サイトからブラウザに対して, サイトを HTTP を使用してロードすることを避け, サイトへの HTTP を使用したアクセスはすべて HTTPS リクエストに自動変換する必要があることを通知します。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : HTTP Strict Transport Security 機能が無効になります。
On : HTTP Strict Transport Security 機能が有効になります。

NetworkServices HTTPS VerifyClientCertificate

ビデオ会議デバイスが HTTPS クライアント (Web ブラウザなど) に接続するときに, クライアントは自身を識別するためにビデオ会議デバイスに証明書を提示するように要求されることがあります。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : クライアント証明書を確認しません。
On : 信頼できる認証局 (CA) によって署名された証明書を提示するようクライアントに要求します。これには, 信頼できる CA のリストがデバイスに事前にアップロードされている必要があります。

NetworkServices NTP Mode

ネットワークタイムプロトコル (NTP) は, リファレンスタイムサーバー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 サーバーを使用します。デフォルトでは, サーバのアドレスはネットワークの DHCP サーバから取得されます。DHCP サーバを使用しない場合や, DHCP サーバが NTP サーバのアドレスを提供しない場合は, NetworkServices NTP Server [n] Address 設定で指定された NTP サーバ アドレスが使用されます。
Manual : デバイスは, [ネットワークサービス NTP サーバー[n] アドレス (NetworkServices NTP Server[n] Address)] 設定で指定された NTP サーバーを使って時間を参照します。
Off : デバイスは NTP サーバーを使用しません。NetworkServices NTP Server [n] Address 設定は無視されます。

NetworkServices NTP Server [n] Address

n: 1..3

NetworkServices NTP Mode が Manual に設定された場合, および NetworkServices NTP Mode が Auto に設定されアドレスが DHCP サーバから提供されない場合に使用される NTP サーバのアドレスです。

必要なユーザ ロール : ADMIN

デフォルト値 : "0.tandberg.pool.ntp.org"

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

NetworkServices NTP Server [n] Key

n: 1..3

NTP 情報が信頼できるソースからのものであることを確かめるためには, ビデオ会議デバイスは NTP ソースが使用する ID またはキーペアを知っている必要があります。キーおよび ID それぞれの設定には, NetworkServices NTP サーバ [n] キーおよび NetworkServices NTP サーバ [n] KeyId 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 20)

NTP ソースが使用する IDまたはキーペアの一部であるキー。

NetworkServices NTP Server [n] KeyId

n: 1..3

NTP 情報が信頼できるソースからのものであることを確かめるためには, ビデオ会議デバイスは NTP ソースが使用する ID またはキーペアを知っている必要があります。キーおよび ID それぞれの設定には, NetworkServices NTP サーバ [n] キーおよび NetworkServices NTP サーバ [n] KeyId 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 10)

NTP ソースが使用する ID/キーペアの一部である ID。

NetworkServices NTP Server [n] KeyAlgorithn

n: 1..3

NTP サーバーが使用する認証ハッシュ機能を選択します。これは, ビデオ会議デバイスが時間メッセージの認証に使用する必要があるものです。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース: None/SHA1/SHA256

None : NTPサーバはハッシュ機能を使用しません。

SHA1: NTPサーバは SHA-1 ハッシュ機能を使用します。

SHA256: NTP サーバは SHA-256 ハッシュ機能を使用します (ハッシュ機能の SHA-2 群から) 。

NetworkServices SIP Mode

デバイスで SIP コールの発信および受信を可能にするかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : SIP コールの発信と受信の可能性をディセーブルにします。

On : SIP コールの発信と受信の可能性を有効にします。

NetworkServices SMTP Mode

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ーに電子メールを送信することができます。これは, ユーザー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できるように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 サーバー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。

NetworkServices SMTP Server

これは SMTP サーバーのアドレスです。

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。

NetworkServices SMTP Port

このポートは, デバイスから SMTP サーバーへの送信電子メールに使用されます。

暗号化の設定 ([ネットワークサービス SMTP セキュリティ (NetworkServices SMTP Security)] と SMTP サーバー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。

NetworkServices SMTP Username

これは, SMTP サーバー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ー名部分です。この設定は SMTP サーバー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, 50)

有効なユーザ名。

NetworkServices SMTP Password

これは, SMTP サーバー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 サーバー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。

NetworkServices SMTP From

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 サーバーの要件を満たす電子メールアドレス。

NetworkServices SMTP Security

デバイスと SMTP サーバー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 : None

値スペース : None /StartTls/Tls
None : 暗号化なしで SMTP サーバーに接続します。
StartTls : 最初に暗号化なしで SMTP サーバーに接続してから, 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。

NetworkServices SNMP Mode

ネットワーク管理システムでは, 管理上の対応を補償する条件についてネットワーク接続デバイス (ルータ, サーバ, スイッチ, プロジェクタなど) をモニタするために SNMP (簡易ネットワーク管理プロトコル) が使用されます。保証の管理上の注意使用されます。SNMP は, デバイス設定を表す変数の形式で管理対象デバイス上の管理データを公開します。これらの変数は, その後照会でき (Readonly に設定) , 管理アプリケーションによって設定できる場合もあります (ReadWrite に設定) 。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値 : ReadOnly

値スペース : Off/ReadOnly/ReadWrite
Off : SNMP ネットワーク サービスを無効にします。
ReadOnly : SNMP ネットワーク サービスを照会のみイネーブルにします。
ReadWrite : SNMP ネットワーク サービスの照会とコマンドの両方をイネーブルにします。

NetworkServices SNMP Host [n] Address

n: 1..3

最大 3 つの SNMP マネージャのアドレスを定義します。
デバイスの SNMP エージェント (コーデック内) は, デバイスの位置や連絡先などについて, SNMP マネージャ (PC プログラムなど) からのリクエストに応答します。SNMP トラップはサポートされていません。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

NetworkServices SNMP CommunityName

ネットワーク サービス SNMP コミュニティの名前を定義します。SNMP コミュニティ名は SNMP 要求を認証するために使用されます。SNMP 要求は, デバイスの SNMP エージェントから応答を受け取るため, パスワード (大文字と小文字を区別) を持つ必要があります。デフォルトのパスワードは「public」です。Cisco TelePresence 管理スイート (TMS) がある場合, 同じ SNMP コミュニティがそこで設定されていることを確認する必要があります。注 : SNMP コミュニティのパスワードは大文字と小文字が区別されます。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値: ""

値スペース : 文字列 (0, 50)
SNMP コミュニティ名。

NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システムの連絡先の名前を定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値: ""

値スペース : 文字列 (0, 50)
SNMP システム接点の名前。

NetworkServices SNMP SystemLocation

ネットワーク サービス SNMP システム ロケーションの名前を定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値: ""

値スペース : 文字列 (0, 50)
SNMP システム ロケーションの名前。

NetworkServices SSH Mode

SSH (Secure Shell) プロトコルは, ビデオ会議デバイスとローカルコンピュータの間でセキュアな暗号化通信を提供できます。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : SSH プロトコルは無効になります。
On : SSH プロトコルは有効になります (デフォルト)。

NetworkServices SSH HostKeyAlgorithm

SSH ホストキーに使用される暗号化アルゴリズムを選択します。2048 ビットのキーサイズを用いる RSA (リベスト・シャミル・エイドルマンアルゴリズム) , NIST 曲線の P-384 を用いる ECDSA (楕円曲線デジタル署名アルゴリズム) , ed25519 署名方式を用いる EdDSA (エドワード曲線デジタル署名アルゴリズム) から選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : RSA

設定可能な値 : ECDSA/RSA/ed25519
ECDSA : ECDSA アルゴリズムを使用します (nist-384p) 。
RSA : RSA アルゴリズムを使用します (2048 bits) 。
ed25519 : ed25519 アルゴリズムを使用します。

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) 公開キー認証をデバイスへのアクセスに使用できます。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : SSH 公開キーは許可されません。
On : SSH 公開キーが許可されます。

NetworkServices UPnP Mode

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, NetworkServices UPnP Timeout 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。

NetworkServices UPnP Timeout

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, NetworkServices UPnP Mode 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。

NetworkServices Websocket

非セキュアおよびセキュアバージョン (ws および wss) の両方で, デバイスの API に WebSocket プロトコルからやり取りできます。WebSocket は HTTP に結びついているので, HTTP または HTTPS を有効にしてから WebSockets を使用する必要があります (NetworkServices HTTP モード設定を参照) 。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : FollowHTTPService/Off

FollowHTTPService: HTTP または HTTTPS が有効な場合, WebSocket プロトコル経由での通信は許可されます。

Off : WebSocket プロトコル経由での通信は許可されません。

NetworkServices WelcomeText

SSH 経由でデバイスにログインするときに, ユーザーに表示する情報を選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : ようこそテキストは次のとおりです : ログインに成功しました (Login successfu)

On : ようこそテキストは次のとおりです : <システム名>; ソフトウェア バージョン; ソフトウェアのリリース日; ログインに成功しました (Login successful)

NetworkServices Wifi Allowed

Wi-Fi アダプタが組み込まれているデバイスは, イーサネットまたは Wi-Fi 経由でネットワークに接続できます。イーサネットと Wi-Fi の両方がデフォルトで許可され, ユーザはどちらを使用するかをユーザ インターフェイスから選択できます。この設定を使用して, 管理者はユーザ インターフェイスがセットアップできないように Wi-Fi 設定を無効にすることができます。

この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。このデバイスは次のセキュリティプロトコルをサポートします : WPA-PSK (AES) , WPA2-PSK (AES) , EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, EAP-MSCHAPv2, EAP-GTC, およびオープンネットワーク (セキュリティ保護なし) 。

デバイスの背面の定格ラベルに記載されている PID (製品 ID) に NR (無線なし) の文字が含まれている場合, デバイスは Wi-Fi をサポートしていません。

必要なユーザ ロール : admin, user

デフォルト値 : True

値スペース : False/True

False : Wi-Fi は使用できません。イーサネット経由でネットワークに接続する必要があります。

True : イーサネットと Wi-Fi の両方を使用できます。

NetworkServices Wifi Enabled

デバイスが Wi-Fi 経由でのネットワーク接続を許可されている場合 (NetworkServices WIFI Allowed 設定を参照) , この設定を使用して Wi-Fi を有効または無効にすることができます。

イーサネットと Wi-Fi の両方を同時に使用することはできません。Wi-Fi を設定するときにイーサネット ケーブルが接続されている場合, そのイーサネット ケーブルを抜かないと続行できません。Wi-Fi に接続している最中にイーサネット ケーブルを接続すると, イーサネットが優先されます。イーサネットケーブルを抜いた場合, 前回接続した Wi-Fi ネットワークが使用可能であれば, デバイスはそのネットワークに自動的に接続します。

必要なユーザ ロール : admin, user

デフォルト値 : True

値スペース : False/True

False : Wi-Fi は無効になります。

True : Wi-Fi が有効になります。

NetworkServices XMLAPI Mode

デバイスの XML API を有効化または無効化します。セキュリティ上の理由からこれを無効にできます。XML API を無効化にすると, TMS などによるリモート管理機能が制限され, デバイスに接続できなくなります。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : XML API は無効になります。

On : XML API は有効になります。

周辺機器の設定

Peripherals Profile Cameras

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。

Peripherals Profile ControlSystems

サードパーティ製の制御システム (Crestron や AMX など) をビデオ会議デバイスに接続しているかどうかを定義します。この情報は, ビデオ会議デバイスの診断サービスで使用されます。接続された制御システムの数がこの設定に一致しない場合, 診断サービスによって不一致がレポートされます。

現在, 本製品ではこのような情報は利用できません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : NotSet

値スペース : 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

Phonebook Server [n] ID

n: 1..1

外部の電話帳の名前を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 64)

外部の電話帳の名前。

Phonebook Server [n] Pagination

n: 1..1

電話帳サーバがページネーション (ウェルカムページ) に対応するかどうかを定義します。ページネーションとはサーバが連続検索に対応しているかどうか, さらにこれらの検索がオフセットに関連付けられるかどうかを意味します。これにより, ユーザインターフェイスは完全な検索結果を得るために必要な可能な限り多くの連続検索を実行できます。

ページネーションが無効の場合, デバイスは 1 回の検索を実行し, 最大 100 エントリを検索結果に返します。それ以上の検索結果をさらにスクロールすることはできません。

必要なユーザ ロール : ADMIN

デフォルト値 : Enabled

値スペース : Disabled/Enabled

Disabled : 電話帳サーバはページネーションに対応しません。デバイスは 1 回の検索を実行します。検索結果の最大エントリ数は 100 です。

Enabled : 電話帳サーバはページネーションに対応しています。

Phonebook Server [n] TlsVerify

この設定は, ビデオ会議デバイスが HTTPS 経由で外部の電話帳サーバーに接続するときに適用されます。

デバイスと HTTPS サーバー間の接続を確立する前に, デバイスは, サーバー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 : 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, アップグレード後にデバイスが工場出荷時設定にリセットされておらず, 以前の [ネットワーク HTTPS サーバー証明書検証 (NetworkServices HTTPS VerifyServerCertificate)] 設定が明示的に [オン (On)] に設定されていなかった場合, この値は [オフ (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 サーバーの証明書を確認しません。

On : デバイスは, HTTPS サーバー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, デバイスとサーバーの間の接続は確立されません。

Phonebook Server [n] Type

n: 1..1

電話帳サーバの種類を選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/CUCM/Spark/TMS/VCS
Off : 電話帳を使用しません。
CUCM : 電話帳が Cisco Unified Communications Manager 上に配置されます。
Spark: 電話帳が Cisco Webex クラウドサービス内に配置されます。
TMS : 電話帳が Cisco TelePresence Management Suite サーバ上に配置されます。
VCS : 電話帳が Cisco TelePresence Video Communication Server 上に配置されます。

Phonebook Server [n] URL

n: 1..1

外部電話帳サーバへのアドレス (URL) を定義します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
外部電話帳サーバの有効なアドレス (URL) 。

プロビジョニング設定

Provisioning Connectivity

この設定は, プロビジョニング サーバからの内部または外部のコンフィギュレーションを要求するかどうかを, デバイスがどのように検出するか制御します。

必要なユーザ ロール : admin, user

デフォルト値 : Auto

値スペース : Internal/External/Auto

Internal : 内部コンフィギュレーションを要求します。

External : 外部コンフィギュレーションを要求します。

Auto : 内部または外部のコンフィギュレーションを要求するかどうかを自動的に NAPTR クエリーを使用して検出します。NAPTR の応答に「e」フラグがある場合, 外部コンフィギュレーションが要求されます。それ以外の場合, 内部コンフィギュレーションが要求されます。

Provisioning ExternalManager Address

外部のマネージャ システムまたはプロビジョニング システムの IP アドレスまたは DNS 名を定義します。

外部マネージャのアドレス (およびパス) が設定されている場合, デバイスは起動時にこのアドレスにメッセージを送信します。このメッセージを受信すると, 結果として外部マネージャ/プロビジョニング システムはそのユニットにコンフィギュレーション/コマンドを返すことができます。

CUCM または TMS プロビジョニングを使用する場合, 外部マネージャ アドレスを自動的に提供するために DHCP サーバをセットアップできます (TMS には DHCP オプション 242, CUCM には DHCP オプション 150) 。プロビジョニング 外部マネージャーアドレス で設定されたアドレスは, DHCP によって提供されるアドレスを上書きします。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

Provisioning ExternalManager AlternateAddress

デバイスが Cisco Unified Communications Manager (CUCM) でプロビジョニングされており, 冗長構成として代替の CUCM が利用可能な場合にのみ使用できます。代替 CUCM のアドレスを定義します。メインの CUCM が使用できない場合, デバイスは代替の CUCM でプロビジョニングされます。メインの CUCM が再び使用可能になると, デバイスはこの CUCM によってプロビジョニングされます。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

Provisioning ExternalManager Protocol

外部のマネージャ システムまたはプロビジョニング システムに要求を送信する際に, HTTP (非セキュアな通信) または HTTPS (セキュアな通信) のどちらのプロトコルを使用するかを定義します。

選択したプロトコルは, NetworkServices HTTP Mode の設定で有効になっている必要があります。

必要なユーザ ロール : admin, user

デフォルト値 : HTTP

値スペース : HTTPS/HTTP

HTTPS : HTTPS を介してリクエストを送信します。

HTTP : HTTP を介してリクエストを送信します。

Provisioning ExternalManager Path

外部のマネージャ システムまたはプロビジョニング システムへのパスを定義します。いくつかの管理サービスが同じサーバに存在する，つまり同じ外部マネージャのアドレスを共有する場合，この設定が必要です。

必要なユーザ ロール：admin, user

デフォルト値: ""

値スペース：文字列 (0..255)

外部のマネージャー システムまたはプロビジョニング システムへの有効なパス。

Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを定義します。

必要なユーザ ロール：admin, user

デフォルト値: ""

値スペース：文字列 (0, 64)

有効なドメイン名。

Provisioning Mode

プロビジョニングシステム (外部マネージャ) を使用してデバイスを設定できます。これにより，ビデオ会議のネットワーク管理者は複数のデバイスを同時に管理することができます。この設定により，使用するプロビジョニング システムの種類を選択します。プロビジョニングは，オフに切り替えることも可能です。詳細については，プロビジョニング システムのプロバイダー/担当者にお問い合わせください。

必要なユーザ ロール：admin, user

デフォルト値：Auto

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

Off：デバイスはプロビジョニングシステムによって設定されません。

Auto：DHCP サーバでセットアップされる対象としてプロビジョニング サーバが自動的に選択されます。

CUCM：CUCM (Cisco Unified Communications Manager) からデバイスに設定をプッシュします。

Edge：CUCM (Cisco Unified Communications Manager) からデバイスに設定をプッシュします。デバイスは Expressway インフラストラクチャを介して CUCM に接続します。Expressway を経由して登録するには，暗号化オプションキーがデバイスにインストールされている必要があります。

Webex：Cisco Webex クラウドサービスからデバイスに設定をプッシュします。

TMS：TMS (Cisco TelePresence Management System) からデバイスに設定をプッシュします。

VCS：VCS (Cisco TelePresence Video Communication Server) からデバイスに設定をプッシュします。

Provisioning LoginName

これは，プロビジョニングサーバー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ー名部分です。この設定は，プロビジョニング サーバが要求する場合，使用する必要があります。

必要なユーザ ロール：admin, user

デフォルト値: ""

値スペース：文字列 (0, 80)

有効なユーザ名。

Provisioning Password

これは, プロビジョニングサーバーでデバイスを認証するために使用されるクレデンシャルのパスワード部分です。この設定は, プロビジョニング サーバが要求する場合, 使用する必要があります。

必要なユーザ ロール : admin, user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効なパスワード。

Provisioning TlsVerify

この設定は, ビデオ会議デバイスが HTTPS 経由でプロビジョニングサーバーに接続するときに適用されます。

デバイスと HTTPS サーバー間の接続を確立する前に, デバイスは, サーバー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 : 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, アップグレード後にデバイスが工場出荷時設定にリセットされておらず, 以前の [ネットワーク HTTPS サーバー証明書検証 (NetworkServices HTTPS VerifyServerCertificate)] 設定が明示的に [オン (On)] に設定されていなかった場合, この値は [オフ (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 サーバーの証明書を確認しません。

On : デバイスは, HTTPS サーバー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, デバイスとサーバーの間の接続は確立されません。

プロキシミティの設定

Proximity Mode

デバイスが超音波のペアリングメッセージを発信するかどうかを決定します。

デバイスが超音波を発信すると, Proximity クライアントはデバイスが近くにあることを検知できます。クライアントを使用するには, 少なくとも 1 つの Proximity サービスをイネーブルにする必要があります (Proximity Services 設定を参照) 。一般的に, すべてのプロキシミティ サービスを有効にすることをお勧めします。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : デバイスは超音波を発信しないため, Proximity サービスを使用できません。

On : デバイスが超音波を発信すると, Proximity クライアントはデバイスが近くにあることを検知できます。有効になっているプロキシミティ サービスを使用できます。

Proximity Services CallControl

Proximity クライアントで基本的なコール制御機能を有効または無効にします。この設定を有効にすると, Proximity クライアントを使用してコールを制御できます (ダイヤル, ミュート, 音量, コールの終了など) 。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには, Proximity Mode を On にする必要があります。

必要なユーザ ロール : admin, user

デフォルト値 : Disabled

値スペース : Enabled/Disabled

Enabled : Proximity クライアントからのコール制御が有効になります。

Disabled : Proximity クライアントからのコール制御が無効になります。

Proximity Services ContentShare FromClients

クライアントからのコンテンツ共有を有効または無効にします。この設定を有効にすると, デバイス上で Proximity クライアントからワイヤレスでコンテンツ (ラップトップ画面の共有など) を共有できます。このサービスはラップトップ (OS X および Windows) でサポートされます。この設定が機能するには, Proximity Mode を On にする必要があります。

必要なユーザ ロール : admin, user

デフォルト値 : Enabled

値スペース : Enabled/Disabled

Enabled : Proximity クライアントからのコンテンツ共有が有効になります。

Disabled : Proximity クライアントからのコンテンツ共有が無効になります。

Proximity Services ContentShare ToClients

プロキシミティ クライアントに対するコンテンツ共有を有効または無効にします。有効にすると, Proximity クライアントはデバイスからプレゼンテーションを受信します。詳細を拡大して, 以前のコンテンツを表示し, スナップショットを作成できます。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには, Proximity Mode を On にする必要があります。

必要なユーザ ロール : admin, user

デフォルト値 : Disabled

値スペース : Enabled/Disabled

Enabled : Proximity クライアントに対するコンテンツ共有が有効になります。

Disabled : Proximity クライアントに対するコンテンツ共有が無効になります。

RoomAnalytics 設定

RoomAnalytics AmbientNoiseEstimation モード

デバイスは, 室内の定常環境雑音レベル (背景雑音レベル) を評価できます。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, 定常環境雑音レベルを定期的に評価します。

Off: デバイスは, 定常環境雑音レベルを定期的に評価しません。

RoomAnalytics PeopleCountOutOfCall

顔検出を使用すると, 室内にいる人の人数をデバイスが特定できるようになります。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。

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, コール中またはセルフビューがオンになっているときにのみ人数をカウントします。

On: 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。

RoomAnalytics PeoplePresenceDetector

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 RoomAnalytics PeoplePresence 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。

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: 人が存在するかどうかの情報は, デバイスのステータスで報告されません。

On: 人が存在するかどうかの情報が, デバイスのステータスで報告されます。

ルームリセットの設定

RoomReset Control

この設定は，コントロールシステムまたはマクロの使用に対するものです。マクロによって，ビデオ会議デバイスの一部を自動化できる JavaScript コードのスニペットを記述できます。これによりカスタム動作を作成します。

ルームが数分に渡って待機状態になると，ビデオ会議デバイスは，ルームがリセット可能な状態であることを示すイベントを送信できます。

この設定が有効である場合に送られるイベントは次の通りです：

*e RoomReset SecondsToReset: 30

** end

*e RoomReset Reset

** end

必要なユーザ ロール：ADMIN

デフォルト値：On

設定可能な値: CameraPositionsOnly/Off/On

CameraPositionsOnly: 適用されません。

Off：ルームリセットイベントは送られません。

On：ルームリセット制御が有効になっており，ルームリセットイベントが送信されます。

RTP 設定

RTP Ports Range Start

RTP ポート範囲の最初のポートを定義します。

デフォルトでは, デバイスは RTP および RTCP メディアデータに 2326 ～ 2487 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100, RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP ビデオ ポート範囲が有効な場合, オーディオは RTP ポート範囲設定で定義された範囲を使用し, その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は, 次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 2326

値スペース : 整数 (1024..65438)

RTP ポート範囲内で最初のポートを設定します。この値は偶数にする必要があります。

RTP Ports Range Stop

RTP ポート範囲の最後のポートを定義します。

デフォルトでは, デバイスは RTP および RTCP メディアデータに 2326 ～ 2487 の範囲のポートを使用します。RTP ビデオポート範囲が有効な場合, デバイスは 1024 ～ 65436 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100, RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP ビデオ ポート範囲が有効な場合, オーディオは RTP ポート範囲設定で定義された範囲を使用し, その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は, 次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値 : 2487

値スペース : 整数 (1121 ～ 65535)

RTP ポート範囲内で最後のポートを設定します。この値は奇数にする必要があります。偶数値を入力すると, 自動的に 1 が加算されます。

RTP Video Ports Range Start

RTP ビデオ ポート範囲の最初のポートを定義します。

開始と終了の値の両方が 0 に設定されている場合, RTP ビデオ ポートの範囲は無効です。有効にするには, 最初のポートを 1024 から 65454 までの値に設定し, 最後のポートを 1024 から 65535 までの値に設定します。最小範囲は 80 です。

RTP ビデオ ポート範囲が有効な場合, オーディオは RTP ポート範囲設定で定義された範囲を使用し, その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は, 次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0, 1024..65454)

RTP ビデオ ポート範囲の最初のポートを設定します。

RTP Video Ports Range Stop

RTP ビデオ ポート範囲の最後のポートを定義します。

開始と終了の値の両方が 0 に設定されている場合, RTP ビデオ ポートの範囲は無効です。有効にするには, 最初のポートを 1024 から 65454 までの値に設定し, 最後のポートを 1024 から 65535 までの値に設定します。最小範囲は 80 です。

RTP ビデオ ポート範囲が有効な場合, オーディオは RTP ポート範囲設定で定義された範囲を使用し, その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は, 次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0, 1024..65535)

RTP ビデオ ポート範囲の最後のポートを設定します。

セキュリティ設定

Security Audit Logging Mode

監査ログを記録または送信する場所を定義します。監査ログは syslog サーバに送信されます。ロギングモード設定がオフに設定されている場合, この設定には効果がありません。

External モードまたは ExternalSecure モードを使用する場合は, セキュリティ監査サーバアドレス設定に監査サーバのアドレスを入力する必要があります。

必要なユーザ ロール : AUDIT

デフォルト値 : Internal

設定可能な値 : External/ExternalSecure/Internal/Off

External : デバイスは外部監査 syslog サーバー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 サーバーに, 暗号化された監査ログを送信します。監査 CA リストファイルが Web インターフェイスからデバイスにアップロードされている必要があります。CA のリストの証明書の common_name パラメータは syslog サーバの IP アドレスまたは DNS 名と一致する必要があり, セキュア TCP サーバでセキュア (TLS) TCP syslog メッセージをリッスンするように設定される必要があります。

Internal : デバイスは内部ログに監査ログを記録し, 満杯になるとログをローテーションします。

Off : 監査ロギングは実行されません。

Security Audit OnError Action

syslog サーバへの接続が失われた場合の動作を定義します。この設定は, Security Audit Logging Mode が ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値 : Ignore

値スペース : Halt/Ignore

Halt : 停止状態が検出された場合, デバイスはリブートし, 停止期間が経過するまでは監査役だけが装置の操作を許可されます。停止状態が過ぎ去ると, 監査ログは syslog サーバに再スプールされます。ネットワークの違反 (物理リンクなし) , 動作中の外 Syslog サーバが存在しない (または syslog への間違ったアドレスまたはポート) , TLS 認証が失敗した (使用中の場合) , ローカル バックアップ (再スプール) ログがいっぱいになった, などの停止状態があります。

Ignore : デバイスは通常の動作を続行し, 満杯になると内部ログをローテーションします。接続が復元されると syslog サーバに再度監査ログを送信します。

Security Audit Server Address

監査ログの送信先である syslog サーバの IP アドレスまたは DNS 名を設定します。この設定は, Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

Security Audit Server Port

監査ログは syslog サーバに送信されます。デバイスが監査ログを送信する syslog サーバーのポートを定義します。この設定は, Security Audit PortAssignment がマニュアルに設定されている場合にのみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値: 514

値スペース : 整数 (0..65535)

監査サーバのポートを設定します。

Security Audit Server PortAssignment

監査ログは syslog サーバに送信されます。外部 syslog サーバのポート番号の割り当て方法を定義できます。この設定は, Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。使用しているポート番号を確認するために, Security Audit Server Port 状態をチェックできます。ウェブ インターフェイスで [セットアップ (Setup)] > [ステータス (Status)] に移動するか, コマンドライン インターフェイスの場合はコマンド xStatus Security Audit Server Port を実行します。

必要なユーザ ロール : AUDIT

デフォルト値 : Auto

値スペース : Auto/Manual

Auto : [セキュリティ監査ロギング モード (Security Audit Logging Mode)] が [外部 (External)] にセットされている場合, UDP ポート番号 514 を使用します。Security Audit Logging Mode が ExternalSecure にセットされている場合, TCP ポート番号 6514 を使用します。

Manual : [セキュリティ監査サーバのポート (Security Audit Server Port)] 設定で定義されたポート値を使用します。

Security Session FailedLoginsLockoutTime

ユーザーが Web または SSH セッションのログインに失敗した後, デバイスがユーザーをロックアウトする時間を定義します。

この設定に対する変更を反映するには, デバイスを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 60

値スペース : 整数 (0..10000)

ロックアウト時間 (分) を設定します。

Security Session InactivityTimeout

ユーザーが 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, デバイスがユーザーの非アクティブ状態をどれくらいの時間受け入れるかを定義します。

この設定に対する変更を反映するには, デバイスを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..10000)

非アクティブ タイムアウト (分単位) を設定します。非アクティブな状態でも強制的に自動ログアウトしない場合は, 0 を選択します。

Security Session MaxFailedLogins

ウェブまたは SSH セッションにログイン試行を失敗できるユーザ 1 人あたりの最大数を定義します。ユーザが試行の最大数を超えた場合, ユーザはロックアウトされます。0 は, 失敗できるログインの回数に制限がないことを意味します。

この設定に対する変更を反映するには, デバイスを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..10)

ユーザ 1 人あたりの失敗できるログイン試行の最高回数を設定します。

Security Session MaxSessionsPerUser

ユーザ 1 人あたりの最大同時セッション数は 20 セッションです。

必要なユーザ ロール : ADMIN

デフォルト値: 20

値スペース : 整数 (1..20)

ユーザ 1 人あたりの最大同時セッション数を設定します。

Security Session MaxTotalSessions

同時セッションの合計最大数は 20 セッションです。

必要なユーザ ロール : ADMIN

デフォルト値: 20

値スペース : 整数 (1..20)

同時セッションの合計最大数を設定します。

Security Session ShowLastLogon

SSH 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ー 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。

SerialPort 設定

SerialPort Mode

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, INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : シリアル ポートを無効にします。

On : シリアル ポートを有効にします。

SerialPort BaudRate

シリアル ポートに, ボー レート (データ送信レート, ビット/秒) 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, INTEGRATOR

デフォルト値: 115200

値スペース : 115200

リストされているボー レート (bps) からボー レートを選択します。

SerialPort LoginRequired

シリアル ポートに接続するときにログインが必要かどうかを定義します。

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 : ユーザーはログインせずに, シリアルポート経由でデバイスにアクセスできます。

On : シリアルポート経由でデバイスに接続するときに, ログインが必要です。

SIP 設定

SIP ANAT

ANAT (Alternative Network Address Types) は RFC 4091 で規定されている複数のアドレスとアドレス タイプのメディア ネゴシエーションを有効にします。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : ANAT を無効にします。
On : ANAT を有効にします。

SIP Authentication UserName

これは, SIP プロキシへの認証に使用されるクレデンシャルのユーザー名部分です。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 128)
有効なユーザ名。

SIP Authentication Password

これは, SIP プロキシへの認証に使用されるクレデンシャルのパスワード部分です。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 128)
有効なパスワード。

SIP DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : Auto

値スペース : Auto/TCP/TIs/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。
TIs : デバイスはデフォルトの転送方法として常に TLS を使用します。TLS 接続の場合, SIP CA リストをデバイスにアップロードできます。該当する CA リストがデバイスにない場合は, ディフィーヘルマン匿名認証が使用されます。
Auto : デバイスは, TLS, TCP, UDP の順序でトランスポートプロトコルを使用して接続を試みます。

SIP DisplayName

設定されたとき, 着信コールは SIP URI ではなく, 表示名を報告します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 550)
SIP URI の代わりに表示する名前。

SIP Ice DefaultCandidate

ICE プロトコルには, 使用するメディア ルートを決定するまでの時間 (最大で通話開始から 5 秒間) が必要となります。この時間内に, この設定に従って, デバイスのメディアがデフォルトの候補に送信されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Host

値スペース : Host/Rflx/Relay

Host : メディアをデバイスのプライベート IP アドレスに送信します。

Rflx : TURN サーバーが認識しているデバイスのパブリック IP アドレスにメディアを送信します。

Relay : TURN サーバで割り当てられた IP アドレスおよびポートにメディアを送信します。

SIP Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) は, 最適化されたメディアパスの検出にデバイスで使用できる NAT トラバーサルソリューションです。このため, オーディオとビデオの最短ルートがデバイス間で常に確保されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Off/On

Auto : TURN サーバが提供されている場合は ICE が有効になり, 提供されていない場合は ICE が無効になります。

Off : ICE が無効になります。

On : ICE が有効になります。

SIP Line

Cisco Unified Communications Manager (CUCM) に登録すると, デバイスを共有回線の一部にできます。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 : デバイスは共有回線の一部であるため, 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回線の一部ではありません。

SIP ListenPort

SIP TCP/UDP ポートでの着信接続のリッスンをオンまたはオフにします。オフにした場合, デバイスは SIP プロキシ (CUCM または VCS) を介してのみ到達可能になります。セキュリティ対策として, デバイスが SIP プロキシに設定されている場合は SIP ListenPort をオフにすべきです。

必要なユーザ ロール : ADMIN

デフォルト値 : 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 Mailbox

Cisco Unified Communications Manager (CUCM) に登録すると, 個人用ボイス メールボックスを所有するオプションが与えられます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な番号またはアドレス。ボイス メールボックスがない場合は, 文字列を空のままにしておきます。

SIP MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN

デフォルト値 : TLSv1.0

値スペース : TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0 : TLS バージョン 1.0 以上をサポートします。

TLSv1.1 : TLS バージョン 1.1 以上をサポートします。

TLSv1.2 : TLS バージョン 1.2 以上をサポートします。

SIP PreferredIPSignaling

シグナリングの優先 IP バージョンを定義します (音声, ビデオ, データ) 。Network IPStack および Conference CallProtocolIPStack の両方が Dual に設定されていて, ネットワークに優先 IP バージョンを選択するメカニズムがない場合にのみ使用可能です。また, 優先 IP バージョンが登録に使用されるように, DNS で A/AAAA ルックアップのプライオリティを指定します。

必要なユーザ ロール : ADMIN

デフォルト値 : IPv4

値スペース : IPv4/IPv6

IPv4 : シグナリングの優先 IP バージョンは IPv4 です。

IPv6 : シグナリングの優先 IP バージョンは IPv6 です。

SIP Proxy [n] Address

n: 1..4

プロキシ アドレスは発信プロキシに手動で設定されたアドレスです。完全修飾ドメイン名, または IP アドレスを使用することが可能です。デフォルト ポートは, TCP および UDP の場合は 5060 ですが, もう 1 ポート準備できます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレス, IPv6 アドレス, または DNS 名。

SIP TlsVerify

SIP TLS 経由の接続を確立する前に, デバイスは, 信頼できる認証局 (CA) がピアの証明書に署名しているかどうかを確認します。CA が CA リストに含まれており, Web インターフェイスまたは API を使用して手動でデバイスにアップロードされている必要があります。プレインストールされている証明書リストは, SIP TLS 接続の証明書の検証には使用されません。

注 : 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, アップグレード後にデバイスが工場出荷時設定にリセットされておらず, この設定が明示的に [オン (On)] に設定されていなかった場合, この値は [オフ (Off)] に設定されます。

どの TLS バージョンを許可するかを指定するには, SIP MinimumTLSVersion 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : デバイスはピアの証明書を確認しません。いずれにしても SIP TLS 接続が確立されます。

On : デバイスは, ピアの証明書が信頼できるかどうかを確認します。信頼できない場合, SIP TLS 接続は確立されません。

SIP Turn DiscoverMode

検出モードを定義し, DNS で利用可能な TURN サーバの検索に対してアプリケーションを有効/無効にします。コールを発信する前に, デバイスはポート割り当てが可能かどうかを確認します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 検出モードを無効にします。

On : On に設定すると, デバイスは DNS で利用可能な TURN サーバーを検索し, コールを発信する前にポート割り当てが可能かどうかをテストします。

SIP Turn DropRflx

DropRflx は, リモートデバイスが同じネットワークにない場合に限り, TURN リレー経由でデバイスにメディアを強制させます。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : DropRflx を無効にします。

On : リモートデバイスが別のネットワークにある場合, デバイスは TURN リレー経由でメディアを強制します。

SIP Turn Server

TURN (Traversal Using Relay NAT) サーバのアドレスを定義します。これはメディアリレーフォールバックとして使用され, また, デバイス固有のパブリック IP アドレスを検出するためにも使用されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

推奨する形式は DNS SRV レコード (例 : _turn._udp.<ドメイン>) ですが, 有効な IPv4 または IPv6 アドレスも指定できます。

SIP Turn UserName

TURN サーバーへのアクセスに必要なユーザー名を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

有効なユーザ名。

SIP Turn Password

TURN サーバへのアクセスに必要なパスワードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

有効なパスワード。

SIP Type

ベンダーまたはプロバイダーに対する SIP 拡張および特別な動作を有効にします。

必要なユーザ ロール : ADMIN

デフォルト値 : Standard

値スペース : Standard/Cisco

Standard : 標準 SIP プロキシに登録する場合はこれを使用します (Cisco TelePresence VCS でテスト済み) 。

Cisco : Cisco Unified Communications Manager に登録する場合はこれを使用します。

SIP URI

SIP URI (Uniform Resource Identifier) は, デバイスの識別に使用されるアドレスです。URI が登録され, SIP サービスによりデバイスへの着信コールのルーティングに使用されます。SIP URI 構文は RFC 3261 で定義されています。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

SIP URI 構文に準拠したアドレス (URI) 。

スタンバイ設定

Standby Control

デバイスをスタンバイモードに移行するかどうかを定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値 : On

値スペース : Off/On
Off : デバイスはスタンバイモードを開始しません。
On : Standby Delay がタイムアウトすると, デバイスはスタンバイモードを開始します。

Standby Delay

スタンバイモードに入るまでにデバイスがアイドルモードのまま経過する時間の長さ (分単位) を定義します。[スタンバイ制御 (Standby Control)] が有効である必要があります。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値: 4

値スペース : 整数 (1..480)
スタンバイ遅延 (分) を設定します。

Standby Signage Audio

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オーバーライドできます。

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 ページでオーディオを再生しません。
On : Web ページにオーディオが含まれている場合, デバイスはオーディオを再生します。音量は, デバイスの音量設定に従います。

Standby Signage InteractionMode

デフォルトでは, ユーザーがデジタルサイネージ 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 : NonInteractive

値スペース : Interactive/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。

Standby Signage Mode

URL (Web ページ) からのコンテンツで, 従来のハーフウェイク背景画像と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しても, デバイスが通常どおりスタンバイ状態に入ることは防げません。そのため, [スタンバイ 遅延 (Standby Delay)] 設定で, 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
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化されていません。
On : WebEngine Mode 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を置き換えます。

Standby Signage RefreshInterval

この設定を使用して, Web ページを定期的な間隔で強制的に更新できます。これは, Web ページ自体を更新できない場合に便利です。インタラクティブモードで更新間隔を設定することは推奨しません。

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 (秒数) 。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。

Standby Signage Url

画面に表示する Web ページ (デジタルサイネージ) の URLを設定します。URL の長さが 0 の場合, デバイスは通常のハーフウェイクモードを維持します。URL が機能しない場合, デバイスは通常のハーフウェイクモードを維持し, 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。

Standby WakeupOnMotionDetection

モーション検知自動ウェイクアップは, ユーザーが入室したことを検出する機能です。この機能は, 超音波検出に基づいています。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : 動体検知ウェイクアップは無効です。

On : 人が部屋に入ると, デバイスが自動的にスタンバイから復帰します。

SystemUnit 設定

SystemUnit Name

デバイス名を定義します。デバイスが SNMP エージェントとして機能している場合に, デバイス名は DHCP リクエストでホスト名として送信されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

デバイス名を定義します。

SystemUnit CrashReporting Advanced

デバイスがクラッシュすると, デバイスは解析のためにシスコ自動クラッシュレポートツール (ACR) にログを自動送信できます。ACR ツールは, Cisco の内部使用のみであり, お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : 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。

SystemUnit CrashReporting Mode

デバイスがクラッシュすると, デバイスは解析のためにシスコ自動クラッシュレポートツール (ACR) にログを自動送信できます。ACR ツールは, Cisco の内部使用のみであり, お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : 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。

SystemUnit CrashReporting Url

デバイスがクラッシュすると, デバイスは解析のためにシスコ自動クラッシュレポートツール (ACR) にログを自動送信できます。ACR ツールは, Cisco の内部使用のみであり, お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : "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。

時刻設定

Time TimeFormat

時刻形式を定義します。

必要なユーザ ロール : admin, user
デフォルト値 : 24H

値スペース : 24H/12H
24H : 24 時間の時間フォーマットを設定します。
12H : 12 時間 (AM/PM) の時間フォーマットを設定します。

Time DateFormat

日付形式を定義します。

必要なユーザ ロール : admin, user
デフォルト値 : DD_MM_YY

値スペース : DD_MM_YY/MM_DD_YY/YY_MM_DD
DD_MM_YY : 2010 年 1 月 30 日は「30.01.10」と表示されます。
MM_DD_YY : 2010 年 1 月 30 日は「01.30.10」と表示されます。
YY_MM_DD : 2010 年 1 月 30 日は「10.01.30」と表示されます。

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

設定可能な値 : アフリカ/アビジャン, アフリカ/アクラ, アフリカ/アディスアベバ, アフリカ/アルジェ, アフリカ/アスマラ, アフリカ/アスメラ, アフリカ/バマコ, アフリカ/バンギ, アフリカ/バンジュール, アフリカ/ビサウ, アフリカ/ブランタイア, アフリカ/ブラザビル, アフリカ/ブジュンブラ, アフリカ/カイロ, アフリカ/カサブランカ, アフリカ/セウタ, アフリカ/コナクリ, アフリカ/ダカール, アフリカ/ダルエスサラーム, アフリカ/ジブチ, アフリカ/ドゥアラ, アフリカ/アイウン, アフリカ/フリータウン, アフリカ/ガボローネ, アフリカ/ハラーレ, アフリカ/ヨハネスブルク, アフリカ/ジュバ, アフリカ/カンパラ, アフリカ/ハルツーム, アフリカ/キガリ, アフリカ/キンシャサ, アフリカ/ラゴス, アフリカ/リーブルビル, アフリカ/ロメ, アフリカ/ルアンダ, アフリカ/ルブンバシ, アフリカ/ルサカ, アフリカ/マラボ, アフリカ/マプト, アフリカ/マセール, アフリカ/ムババーネ, アフリカ/モガディシュ, アフリカ/モンロヴィア, アフリカ/ナイロビ, アフリカ/ンジャメナ, アフリカ/ニアメイ, アフリカ/ヌアクショット, アフリカ/ワガドゥグ, アフリカ/ポルトノボ, アフリカ/サントメ・プリンシペ, アフリカ/ティンブクトゥ, アフリカ/トリポリ, アフリカ/チュニス, アフリカ/ウィントフック, アメリカ/アダック, アメリカ/アンカレッジ, アメリカ/アンギラ, アメリカ/アンティグア, アメリカ/アラグァイーナ, アメリカ/アルゼンチン/ブエノスアイレス, アメリカ/アルゼンチン/カタマルカ, アメリカ/アルゼンチン/コモドーロ・リバダビア, アメリカ/アルゼンチン/コルドバ, アメリカ/アルゼンチン/フフイ, アメリカ/アルゼンチン/ラ・リオージャ, アメリカ/アルゼンチン/メンドーサ, アメリカ/アルゼンチン/リオ・ガレゴス, アメリカ/アルゼンチン/サルタ, アメリカ/アルゼンチン/サンファン, アメリカ/アルゼンチン/サンルイス, アメリカ/アルゼンチン/トゥクマン, アメリカ/アルゼンチン/ウシュアイア, アメリカ/アルバ, アメリカ/アスンシオン, アメリカ/アティコーカン, アメリカ/アトーチャ, アメリカ/バヒア, アメリカ/バヒア・バンデラス, アメリカ/バルバドス, アメリカ/ベレン, アメリカ/ベリーズ, アメリカ/ブランサルトン, アメリカ/ボア・ビスタ, アメリカ/ボゴタ, アメリカ/ボイシ, アメリカ/ブエノスアイレス, アメリカ/ケンブリッジベイ, アメリカ/カンポグランデ, アメリカ/カンクーン, アメリカ/カラカス, アメリカ/カタマルカ, アメリカ/カイエン, アメリカ/ケイマン, アメリカ/シカゴ, アメリカ/チワワ, アメリカ/コーラル・ハーバー, アメリカ/コルドバ, アメリカ/コスタリカ, アメリカ/クレストン, アメリカ/クイアバ, アメリカ/キュラソー, アメリカ/デンマルクション, アメリカ/ドーソン, アメリカ/ドーソンクリーク, アメリカ/デンバー, アメリカ/デトロイト, アメリカ/ドミニカ, アメリカ/エドモントン, アメリカ/エイルネペ, アメリカ/エルサルバドル, アメリカ/エンセナダ, アメリカ/フォート・ネルソン, アメリカ/フォート・ウェイン, アメリカ/フォルタレザ, アメリカ/グレース・ベイ, アメリカ/ゴットホープ, アメリカ/グース・ベイ, アメリカ/グランドターク, アメリカ/グレナダ, アメリカ/グアダルーペ, アメリカ/グアテマラ, アメリカ/グアヤキル, アメリカ/ガイアナ, アメリカ/ハリファクス, アメリカ/ハバナ, アメリカ/エルモシージョ, アメリカ/インディアナ/インディアナポリス, アメリカ/インディアナ/ノックス, アメリカ/インディアナ/マレンゴ, アメリカ/インディアナ/ピータースバーグ, アメリカ/インディアナ/テルシティ, アメリカ/インディアナ/ヴィベイ, アメリカ/インディアナ/ヴァンセンヌ, アメリカ/インディアナ/ウィナマク, アメリカ/インディアナポリス, アメリカ/イヌヴィック, アメリカ/イカルイト, アメリカ/ジャマイカ, アメリカ/フフイ, アメリカ/ジュノー, アメリカ/ケンタッキー/ルイビル, アメリカ/ケンタッキー/モンティチェロ, アメリカ/ノックス, アメリカ/クラレンダイク, アメリカ/ラパス, アメリカ/リマ, アメリカ/ロサンゼルス, アメリカ/ルイビル, アメリカ/ローワー・プリンシズ, アメリカ/マセイオ, アメリカ/マナグア, アメリカ/マナウス, アメリカ/マリゴ, アメリカ/マルティニーク, アメリカ/マタモロス, アメリカ/マサトラン, アメリカ/メンドーサ, アメリカ/メノミニー, アメリカ/メリダ, アメリカ/メトラカトラ, アメリカ/メキシコシティ, アメリカ/ミクロン島, アメリカ/モンクトン, アメリカ/モントレー, アメリカ/モンテビデオ, アメリカ/モントリオール, アメリカ/モンセラート, アメリカ/ナッソー, アメリカ/ニューヨーク, アメリカ/ニピゴン, アメリカ/ノーム, アメリカ/ノローニャ, アメリカ/ノースダコタ/ビューラ, アメリカ/ノースダコタ/センター, アメリカ/ノースダコタ/ニュー・セーラム, アメリカ/オジナガ, アメリカ/パナマ, アメリカ/パンゲナータング, アメリカ/パラマリボ, アメリカ/フェニックス, アメリカ/ポルトープランス, アメリカ/ポートオブスペイン, アメリカ/ポルト・アクレ, アメリカ/ポルト・ヴェーリョ, アメリカ/プエルトリコ, アメリカ/レイニーリバー, アメリカ/ランキン・インレット, アメリカ/レシフェ, アメリカ/レジーナ, アメリカ/レゾリュート, アメリカ/リオ・ブランコ, アメリカ/ロサリオ, アメリカ/サンタイザベル, アメリカ/サンタレム, アメリカ/サンチアゴ, アメリカ/サントドミンゴ, アメリカ/サンパウロ, アメリカ/スコールスビーサンド, アメリカ/シップロック, アメリカ/シトカ, アメリカ/サン・バルテルミー島, アメリカ/セント・ジョーンズ, アメリカ/セントクリストファー・ネイビス, アメリカ/セントルシア, アメリカ/セント・トーマス, アメリカ/サン・ヴィンセント, アメリカ/スウィフトカレント, アメリカ/テグシガルパ, アメリカ/スーリー, アメリカ/サンダーベイ, アメリカ/ティファナ, アメリカ/トロント, アメリカ/トルトラ, アメリカ/バンクーバー, アメリカ/バージン, アメリカ/ホワイトハウス, アメリカ/ウィニペグ, アメリカ/ヤクタート, アメリカ/イエローナイフ, 南極/ケーシー, 南極/デービス, 南極/デュモン・デュルヴィル, 南極/マックォーリー, 南極/モーソン, 南極/マクマルド, 南極/パーマー, 南極/ロゼラ, 南極/南極点, 南極/昭和, 南極/トロール, 南極/ボストーク, 北極/ロングイェールビーン, アジア/アデン, アジア/アルマトイ, アジア/アンマン, アジア/アナディル, アジア/アクタウ, アジア/アクトベ, アジア/アシガバート, アジア/アシガバート, アジア/バグダッド, アジア/バーレーン, アジア/バクー, アジア/バンコク, アジア/バルナウル, アジア/ベイルート, アジア/ビシュケク, アジア/ブルネイ, アジア/カルカッタ, アジア/チタ, アジア/チョイバルサン, アジア/重慶, アジア/重慶, アジア/コロンボ, アジア/ダッカ, アジア/ダマスカス, アジア/ダッカ, アジア/ディリ, アジア/ドバイ, アジア/ドゥシャンベ, アジア/ガザ, アジア/ハルビン, アジア/ヘブロン, アジア/ホーチミンシティ, アジア/香港, アジア/ホブド, アジア/イルクーツク, アジア/イスタンブール, アジア/ジャカルタ, アジア/ジャヤプラ, アジア/エルサレム, アジア/カブール, アジア/カムチャッカ, アジア/カラチ, アジア/カシュガル, アジア/カトマンズ, アジア/カトマンズ, アジア/ハンドゥイガ, アジア/コルカタ, アジア/クラスノヤルスク, アジア/クアラルンプール, アジア/クチン, アジア/クウェート, アジア/マカオ, アジア/マカオ, アジア/マガダン, アジア/マカッサル, アジア/マニラ, アジア/マスカット, アジア/ニコシア, アジア/ノヴォクズネツク, アジア/ノヴォシビルスク, アジア/オムスク, アジア/オラル, アジア/プノンペン, アジア/ポンティアナック, アジア/平壌, アジア/カタール, アジア/クズロルダ, アジア/ラングーン, アジア/リャド, アジア/サイゴン, アジア/サハリン, アジア/サマルカンド, アジア/ソウル, アジア/上海, アジア/シンガポール, アジア/スレドネコリムスク, アジア/台北, アジア/タシケント, アジア/トビリシ, アジア/テヘラン, アジア/テルアビブ, アジア/ティンプー, アジア/ティンプー, アジア/東京, アジア/トムスク, アジア/ウジュンパンダン, アジア/ウランバートル, アジア/ウランバートル, アジア/ウルムチ, アジア/ウスチ＝ネラ, アジア/ヴィエンチャン, アジア/ウラジオストク, アジア/ヤクーツク, アジア/エカテリンブルク, アジア/エレバン, 大西洋/アゾレス諸島, 大西洋/バミューダ諸島, 大西洋/カナリア諸島, 大西洋/カーボベルデ, 大西洋/フェロー諸島, 大西洋/フェロー諸島, 大西洋/ヤンマイエン島, 大西洋/マデイラ島, 大西洋/レイキャビク, 大西洋/南ジョージア, 大西洋/セントヘレナ, 大西洋/スタンレー, オーストラリア/ACT, オーストラリア/アデレード, オーストラリア/ブリスベン, オーストラリア/ブロークンヒル, オーストラリア/キャンベラ, オーストラリア/カリー, オーストラリア/ダーウィン, オーストラリア/ユークラ, オーストラリア/ホバート, オーストラリア/LHI, オーストラリア/リンデマン, オーストラリア/ロード・ハウ, オーストラリア/メルボルン, オーストラリア/NSW, オーストラリア/ノース, オーストラリア/パース, オーストラリア/クイーンズランド, オーストラリア/サウス, オーストラリア/シドニー, オーストラリア/タスマニア, オーストラリア/ヴィクトリア, オーストラリア/ウエスト, オーストラリア/ヤ

ンコウィナ, ブラジル/アクレ, ブラジル/デ・ノローニャ, ブラジル/イースト, CET, CST6CDT, カナダ/アトランティック, カナダ/セントラル, カナダ/イーストサスカチュワン, カナダ/イースタン, カナダ/マウンテン, カナダ/ニューファンドランド, カナダ/パシフィック, カナダ/サスカチュワン, カナダ/ユーコン, チリ/コンチネンタル, チリ/イースター島, キューバ, EET, EST, EST5EDT, エジプト, Eire, その他/GMT, その他/GMT+0, その他/GMT+1, その他/GMT+10, その他/GMT+11, その他/GMT+12, その他/GMT+2, その他/GMT+3, その他/GMT+4, その他/GMT+5, その他/GMT+6, その他/GMT+7, その他/GMT+8, その他/GMT+9, その他/GMT-0, その他/GMT-1, その他/GMT-10, その他/GMT-11, その他/GMT-12, その他/GMT-13, その他/GMT-14, その他/GMT-2, その他/GMT-3, その他/GMT-4, その他/GMT-5, その他/GMT-6, その他/GMT-7, その他/GMT-8, その他/GMT-9, その他/GMT0, その他/グリニッジ, その他/UCT, その他/UTC, その他/ユニバーサル, その他/ズールー, ヨーロッパ/アムステルダム, ヨーロッパ/アンドラ, ヨーロッパ/アストラハン, ヨーロッパ/アテナ, ヨーロッパ/ベルファスト, ヨーロッパ/ベルグラード, ヨーロッパ/ベルリン, ヨーロッパ/ブラティスラヴァ, ヨーロッパ/ブリュッセル, ヨーロッパ/ブカレスト, ヨーロッパ/ブダペスト, ヨーロッパ/ビュージンゲン, ヨーロッパ/キシナウ, ヨーロッパ/コペンハーゲン, ヨーロッパ/ダブリン, ヨーロッパ/ジブラルタル, ヨーロッパ/ガーンジー, ヨーロッパ/ヘルシンキ, ヨーロッパ/マン島, ヨーロッパ/イスタンブール, ヨーロッパ/ジャージー, ヨーロッパ/カリーニングラード, ヨーロッパ/キエフ, ヨーロッパ/キロフ, ヨーロッパ/リスボン, ヨーロッパ/リュブリャナ, ヨーロッパ/ロンドン, ヨーロッパ/ルクセンブルク, ヨーロッパ/マドリード, ヨーロッパ/マルタ, ヨーロッパ/マリエハムン, ヨーロッパ/ミンスク, ヨーロッパ/モナコ, ヨーロッパ/モスクワ, ヨーロッパ/ニコシア, ヨーロッパ/オスロー ヨーロッパ/パリ, ヨーロッパ/ポドゴリツァ, ヨーロッパ/プラハ, ヨーロッパ/リガ, ヨーロッパ/ローマ, ヨーロッパ/サマラ, ヨーロッパ/サンマリノ, ヨーロッパ/サラエボ, ヨーロッパ/シンフェロポリ, ヨーロッパ/スコピエ, ヨーロッパ/ソフィア, ヨーロッパ/ストックホルム, ヨーロッパ/タリン, ヨーロッパ/ティラーナ, ヨーロッパ/ティラスポリ, ヨーロッパ/ウリヤノフスク, ヨーロッパ/ウージュホロド, ヨーロッパ/ファドゥーツ, ヨーロッパ/バチカン, ヨーロッパ/ウィーン, ヨーロッパ/ヴィリニュス, ヨーロッパ/ヴォルゴグラード, ヨーロッパ/ワルシャワ, ヨーロッパ/ザグレブ, ヨーロッパ/ザポリージャ, ヨーロッパ/チューリッヒ, 英国, 英国エア, GMT, GMT+0, GMT-0, GMT0, グリニッジ, HST, 香港, アイスランド, インド洋/アンタナナリボ, インド洋/チャゴス, インド洋/クリスマス諸島, インド洋/ココス, インド洋/コモロ諸島, インド洋/ケルゲレン諸島, インド洋/マヘ島, インド洋/モルディブ, インド洋/モーリシャス諸島, インド洋/マヨット, インド洋/レユニオン, イラン, イスラエル, ジャマイカ, 日本, クェゼリン, リビア, MET, MST, MST7MDT, メキシコ/バハノルテ, メキシコ/バハスル, メキシコ/一般, NZ, NZ-CHAT, ナバホ, PRC, PST8PDT, 太平洋/アピア, 太平洋/オークランド, 太平洋/ブーゲンビル, 太平洋/チャタム, 太平洋/チューク諸島, 太平洋/イースター島, 太平洋/エファテ島, 太平洋/エンダーベリー島, 太平洋/ファカオフォ島, 太平洋/フィジー, 太平洋/フナフティ島, 太平洋/ガラパゴス諸島, 太平洋/ガンビア, 太平洋/ガダルカナル, 太平洋/グアム, 太平洋/ホノルル, 太平洋/ジョンストン, 太平洋/キリスィマスィ, 太平洋/コスラエ, 太平洋/クェゼリン, 太平洋/マジュロ, 太平洋/マルキーズ諸島, 太平洋/ミッドウェー島, 太平洋/ナウル, 太平洋/ニウエ, 太平洋/ノーフォーク, 太平洋/ヌメア, 太平洋/パゴパゴ, 太平洋/パラオ, 太平洋/ピトケアン, 太平洋/ポンペイ, 太平洋/ポナペ, 太平洋/ポートモレスビー, 太平洋/ラロトンガ, 太平洋/サイパン, 太平洋/サモア, 太平洋/タヒチ, 太平洋/タラワ, 太平洋/トンガタプ, 太平洋/トラック, 太平洋/ウェーキ, 太平洋/ウォリス, 太平洋/ヤップ, ポーランド, ポルトガル, ROC, ROK, シンガポール, トルコ, UCT, 米国/アラスカ, 米国/アリューシャン, 米国/アリゾナ, 米国/セントラル, 米国/東インディアナ, 米国/イースタン, 米国/ハワイ, 米国/インディアナスターク, 米国/ミシガン, 米国/マウンテン, 米国/パシフィック, 米国/パシフィックニュー, 米国/サモア, UTC, ユニバーサル, W-SU, WET, ズールー

リストからタイム ゾーンを選択します。

UserInterface 設定

UserInterface Accessibility IncomingCallNotification

画面表示を強調した着信コールの通知を利用できます。画面とタッチ 10 は約 1 秒ごと (1.75 Hz) に赤と白に点滅し，聴覚が不自由なユーザが着信コールに気づきやすくするようにしています。デバイスが既に通話中の場合は，進行中の通話の妨げにならないように画面は点滅しません。代わりに，通常の通知が画面とタッチパネルに表示されます。

必要なユーザ ロール： ADMIN, INTEGRATOR, USER

デフォルト値 : Default

値スペース : AmplifiedVisuals/Default

AmplifiedVisuals : デバイスがコールを受け入れたときに，画面とタッチパネル上での画面表示の強調を有効にします。

Default : スクリーンとタッチパネル上での通知を使用したデフォルトの動作を有効にします。

UserInterface Branding AwakeBranding Colors

ブランディングのカスタマイズを使用してデバイスがセットアップされている場合，この設定は，デバイスが起動している時に表示されるロゴの色に影響します。ロゴをフルカラーで表示するか，またはロゴの不透明度を下げるかによって，画面上の背景や他の要素とより自然にブレンドするように設定することができます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Native

Auto : ロゴの不透明度は低減されます。

Native : ロゴはフルカラーです。

UserInterface ContactInfo Type

ユーザ インターフェイスで表示する連絡先の種類を選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/DisplayName/E164Alias/H320Number/H323Id/IPv4/IPv6/None/SipUri/SystemName

Auto : 他のデバイスがこのビデオ会議デバイスに接続するためにダイヤルする必要があるアドレスを表示します。アドレスは，デフォルトのコールプロトコルおよびデバイス登録によって異なります。

None : どのようなコンタクト情報も表示しません。

IPv4 : デバイスの IPv4 アドレスを示します。

IPv6 : デバイスの IPv6 アドレスを示します。

H323Id : デバイスの H.323 ID を表示します (H323 H323Alias ID 設定を参照) 。

H320Number : 連絡先情報としてデバイスの H.320 番号を表示します (Cisco TelePresence ISDN リンクを使用している場合のみサポートされます) 。

E164Alias : 連絡先情報としてデバイスの H.323 E164 エイリアスを表示します (H323 H323Alias E164 設定を参照) 。

SipUri : デバイスの SIP URI を表示します (SIP URI 設定を参照) 。

SystemName : デバイス名を表示します (SystemUnit Name 設定を参照) 。

DisplayName : デバイスの表示名を表示します (SIP DisplayName 設定を参照) 。

UserInterface KeyTones Mode

テキストまたは数値を入力する際に，キーボードクリック効果音 (キートーン) が鳴るようにデバイスを設定できます。

必要なユーザ ロール : admin, user

デフォルト値 : Off

値スペース : Off/On

Off : キー トーンは再生されません。

On : キー トーンがオンになります。

UserInterface Features Call End

ユーザインターフェイスからデフォルトの通話終了ボタンを削除するかどうかを選択します。設定はボタンだけを削除し, 機能などは削除しません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : デフォルトボタンをユーザ インターフェイスから削除します。

UserInterface Features Call MidCallControls

ユーザインターフェイスからデフォルトの保留, 転送, および通話再開ボタンを削除するかどうかを選択します。設定はボタンだけを削除し, 機能などは削除しません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : ユーザ インターフェイスからデフォルトボタンを削除します。

UserInterface Features Call Start

ユーザーインターフェイスから, デフォルトの通話ボタン (ディレクトリ, お気に入り, および直近の通話リスト) , さらにデフォルトの着信追加参加者ボタンを削除するかどうかを選択します。設定はボタンだけを削除し, 機能などは削除しません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : ユーザ インターフェイスからデフォルトボタンを削除します。

UserInterface Features Call VideoMute

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

Auto : 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。

Hidden : [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。

UserInterface Features HideAll

ユーザインターフェイスからデフォルトボタンを削除するかどうかを選択します。設定はボタンだけを削除し, 機能などは削除しません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : False

値スペース : False/True

False : すべてのデフォルトボタンをユーザインターフェイスで表示します。

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。

UserInterface Features Share Start

ユーザインターフェイスから, コンテンツの共有とコール発信の両方で, コンテンツを共有およびプレビューするためのデフォルトボタンやその他の UI 要素を削除するかどうかを選択します。設定はボタンと UI 要素だけを削除し, 機能などは削除しません。Proximity または Cisco Webex Teams アプリを使ってコンテンツの共有は可能です。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンと UI 要素をユーザ インターフェイスに表示します。

Hidden: デフォルトボタンと UI 要素をユーザ インターフェイスから削除します。

UserInterface Features Whiteboard Start

ユーザーインターフェイスからデフォルトの [ホワイトボード (Whiteboard)] ボタンを削除するかどうかを選択します。設定はボタンだけを削除し, 機能などは削除しません。この設定は, Cisco Webex に登録されているデバイスにのみ適用されます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden : デフォルトボタンをユーザ インターフェイスから削除します。

UserInterface Language

ユーザ インターフェイスで使用される言語を選択します。該当する言語がサポートされていない場合, デフォルトの言語 (Medium) が使用されます。

必要なユーザ ロール : admin, user

デフォルト値 : English

値スペース : Arabic/Catalan/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/English/EnglishUK/Finnish/French/FrenchCanadian/German/Hebrew/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/Portuguese/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish

リストから言語を選択します。

UserInterface OSD EncryptionIndicator

暗号化インジケータが画面に表示される時間の長さを定義します。暗号化された通話のアイコンは, ロックされた南京錠です。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/AlwaysOn/AlwaysOff

Auto : コールが暗号化されている場合は, 「コールは暗号化されています (Call is encrypted) 」という通知が 5 秒間表示されます。その後, 通話の残りの部分では暗号化インジケータ アイコンが表示されます。

コールが暗号化されていない場合は, 「コールは暗号化されていません (Call is not encrypted) 」という通知が 5 秒間表示されます。暗号化インジケータ アイコンは表示されません。

AlwaysOn : 「コールは暗号化されています (Call is encrypted) 」という通知が 5 秒間表示されます。その後, 通話の残りの部分では暗号化インジケータ アイコンが表示されます。

AlwaysOff : 暗号化インジケータは画面上に表示されません。

UserInterface OSD Output

オンスクリーン用の情報とインジケータ (OSD) を表示するモニタを定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値: 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。

UserInterface Phonebook Mode

この設定は, ユーザーがデバイスのユーザーインターフェイスから, ディレクトリおよびお気に入りリストに連絡先を追加または変更することを許可するかどうかを決定します。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : ReadWrite

値スペース : ReadOnly/ReadWrite

ReadOnly : 連絡先をお気に入りリストに追加したり, お気に入りリストの連絡先を編集したりはできません。また, 通話前にディレクトリやお気に入りリストから連絡先を編集することはできません。

ReadWrite : 連絡先をお気に入りリストに追加したり, お気に入りリストの連絡先を編集したりできます。また, 通話前にディレクトリやお気に入りリストから連絡先を編集することができます。

UserInterface Security Mode

この設定では, 重要なデバイス情報 (例 : ビデオ会議デバイスの連絡先情報や IP アドレス, タッチコントローラ, および UCM/VCS レジストラ) がユーザーインターフェイス (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ーインターフェイスに表示されます。

Strong : 連絡先情報および IP アドレスは, ユーザ インターフェイス (ドロップ ダウン メニューと設定パネル) に表示されません。

UserInterface SettingsMenu Mode

ユーザーインターフェイス (Touch 10 または画面上) の設定パネルは, そのデバイスの管理者パスワードで保護できます。このパスワードが空白の場合, 誰でも設定パネルの設定にアクセスし, たとえばデバイスを初期設定にリセットすることができます。認証を有効にすると, 認証を必要とするすべての設定に南京錠のアイコンが表示されます。設定を選択するときに, 管理者のユーザー名とパスフレーズを入力するよう求められます。認証が必須でない設定には, 南京錠のアイコンが表示されません。

必要なユーザ ロール : ADMIN

デフォルト値 : Unlocked

値スペース : Locked/Unlocked

Locked : 管理者のユーザ名とパスフレーズによる認証が必要です。

Unlocked : 認証は必要ありません。

UserInterface SettingsMenu Visibility

デバイス名 (または連絡先情報) および関連するドロップダウンメニューと [設定 (Settings)] パネルを, ユーザー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)] パネルをユーザー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, ユーザーインタフェースに表示しません。

UserInterface SoundEffects Mode

他のユーザーがプロキシミティ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 ([ユーザーインターフェイス キーボード モード (UserInterface Keytones Mode)] 設定を参照してください) 。

必要なユーザ ロール : admin, user

デフォルト値 : On

値スペース : Off/On

Off : サウンドエフェクトを鳴らしません。

On : サウンドエフェクトをオンにします。

UserInterface Wallpaper

アイドル状態のときのビデオ画面の背景画像 (壁紙) を選択します。

Web インターフェイスを使用してデバイスにカスタム壁紙をアップロードできます。サポートされるファイル形式は BMP, GIF, JPEG, PNG です。最大ファイル サイズは 4 MByte です。カスタム壁紙を使用すると，予定されている会議のクロックおよび一覧がメイン ディスプレイから削除されます。

必要なユーザ ロール : ADMIN, INTEGRATOR, USER

デフォルト値 : Auto

値スペース : Auto/Custom/None

Auto : デフォルトの壁紙を使用します。

None : 画面に背景イメージはありません。

Custom : 画面の背景画像としてカスタムの壁紙を使用します。デバイスにカスタム壁紙がアップロードされていない場合，この設定はデフォルト値に戻ります。

UserManagement の設定

UserManagement LDAP Admin Filter

どのユーザに管理者権限を付与する必要があるか決定するために LDAP フィルタが使用されます。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタが優先されるため, ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても, ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 1024)

この文字列の構文については, LDAP の仕様を参照してください。例 : " (| (memberof=CN=admin group, OU=company groups, DC=company, DC=com) (sAMAccountName=username)) "

UserManagement LDAP Admin Group

この AD (Active Directory) グループのメンバーには, 管理者権限が付与されます。この設定は, memberOf:1.2.840.113556.1.4.1941:=<group name> の短縮形です。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタが優先されるため, ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても, ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

AD グループの識別名。例 : "CN=admin group, OU=company groups, DC=company, DC=com"

UserManagement LDAP Attribute

指定のユーザ名にマップするために使用する属性。設定しない場合, sAMAccountName が使用されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

属性名。

UserManagement LDAP BaseDN

検索を開始するエントリの識別名 (ベース) 。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

ベースの識別名。例 : "DC=company, DC=com"

UserManagement LDAP Encryption

デバイスと LDAP サーバーの間の通信を保護する方法を定義します。ポート番号は, UserManagement LDAP Server Port 設定を使用してポート番号をオーバーライドできます。

必要なユーザ ロール : ADMIN

デフォルト値 : LDAPS

値スペース : LDAPS/None/STARTTLS

LDAPS : ポート 636 over TLS (Transport Layer Security) 上の LDAP サーバに接続します。

None : ポート 389 で LDAP サーバーに接続します (暗号化なし) 。

STARTTLS : ポート 389 で LDAP サーバーに接続し, 暗号化された接続 (TLS) にアップグレードするための STARTTLS コマンドを送信します。

UserManagement LDAP MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN
デフォルト値 : TLSv1.2

値スペース : TLSv1.0/TLSv1.1/TLSv1.2
TLSv1.0 : TLS バージョン 1.0 以上をサポートします。
TLSv1.1 : TLS バージョン 1.1 以上をサポートします。
TLSv1.2 : TLS バージョン 1.2 以上をサポートします。

UserManagement LDAP Mode

このデバイスでは, ユーザー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) サーバーの使用をサポートします。この設定を使用して, LDAP 認証を使用するかどうか設定します。実装は, Microsoft Active Directory (AD) サービスでテスト済みです。

LDAP モードをオンにする場合, 設定に合わせたユーザ管理 LDAP 設定の構成を確認してください。いくつかの例を示します。

例 1 :

- ユーザ管理 LDAP モード : On
- ユーザ管理 LDAP アドレス : "192.0.2.20"
- ユーザ管理 LDAP ベース DN : "DC=company, DC=com"
- ユーザ管理 LDAP 管理グループ : "CN=admin group, OU=company group, DC=company, DC=com"

例 2 :

- ユーザ管理 LDAP モード : On
- ユーザ管理 LDAP アドレス : "192.0.2.20"
- ユーザ管理 LDAP ベース DN : "DC=company, DC=com"
- ユーザ管理 LDAP 管理フィルタ : "(| (memberof=CN=admin group, OU=company groups, DC=company, DC=com) (sAMAccountName=username)) "

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : LDAP 認証は使用不可です。
On: LDAP 認証は許可されます。

UserManagement LDAP Server Address

LDAP サーバの IP アドレスまたはホスト名を設定します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な IPv4 アドレス, IPv6 アドレス, またはホスト名。

UserManagement LDAP Server Port

LDAP サーバに接続するポートをオンに設定します。0 に設定した場合は, 選択したプロトコルのデフォルトを使用します (「UserManagement LDAP Encryption 設定」を参照する) 。

必要なユーザ ロール : ADMIN
デフォルト値: 0

値スペース : 整数 (0..65535)
LDAP サーバのポート番号。

UserManagement LDAP VerifyServerCertificate

デバイスを LDAP サーバーに接続すると, サーバー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, デバイスがサーバー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 サーバーの証明書を検証しません。
On : デバイスは, LDAP サーバーの証明書が信頼できる認証局 (CA) によって署名されているかどうか検証する必要があります。該当する CA が, デバイスに事前にアップロードされている信頼できる CA のリストに含まれている必要があります。デバイスの Web インターフェイスを使用して, 信頼できる CA のリストを管理します (詳細については管理者ガイドを参照してください) 。

ビデオ設定

Video ActiveSpeaker DefaultPIPPosition

通話中のスピーカーを示すピクチャインピクチャ (PiP) の画面上の位置を定義します。この設定は, 通話中のスピーカーを PiP 表示するビデオ レイアウト (オーバーレイ レイアウト) を使用している場合にのみ有効です。また, 場合によっては, カスタム レイアウトでも有効です (「Video DefaultLayoutFamily Local の設定」を参照) 。この設定は, 次回以降のコールで有効になります。コール中に変更された場合, 現在のコールへの影響はありません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : 通話中のスピーカーの PiP の位置はコール終了後にも変更されません。

UpperLeft : 通話中のスピーカーの PiP が画面の左上隅に表示されます。

UpperCenter : 通話中のスピーカーの PiP が画面の上部中央に表示されます。

UpperRight : 通話中のスピーカーの PiP が画面の右上隅に表示されます。

CenterLeft : 通話中のスピーカーの PiP が画面の左中央に表示されます。

CenterRight : 通話中のスピーカーの PiP が画面の右中央に表示されます。

LowerLeft : 通話中のスピーカーの PiP が画面の左下隅に表示されます。

LowerRight : 通話中のスピーカーの PiP が画面の右下隅に表示されます。

Video DefaultLayoutFamily Remote

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マルチサイト機能 (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/Overlay/Single

Auto : ローカル レイアウト データベースによって指定される, デフォルト レイアウト ファミリが, リモート レイアウトとして使用されます。

Equal : Equal レイアウト ファミリがリモート レイアウトとして使用されます。画面上に十分なスペースがある限り, すべてのビデオのサイズは等しくなります。

Prominent : Prominent レイアウト ファミリがリモート レイアウトとして使用されます。通話中のスピーカー, または (存在する場合) プレゼンテーションは大きい画像となり, 他の参加者は小さい画像となります。通話中のスピーカーが遷移するとき, 音声が切り替えられます。

Overlay : [オーバーレイ (Overlay)] レイアウト ファミリがリモート レイアウトとして使用されます。通話中のスピーカー, または (存在する場合) プレゼンテーションは全画面表示となり, 他の参加者は小さいピクチャ イン ピクチャ (PiP) となります。通話中のスピーカーが遷移するとき, 音声が切り替えられます。

Single : 通話中のスピーカー, または (存在する場合) プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき, 音声が切り替えられます。

Video DefaultMainSource

発信を開始する際にデフォルトのメイン ビデオ ソースとして使用されるビデオ入力ソースを定義します。

必要なユーザ ロール : admin, user

デフォルト値: 1

値スペース : 1

デフォルトのメインビデオソースとして使用されるソース。

Video Input Connector [n] CameraControl CameraId

n: 1..2

カメラ ID は, このビデオ入力に接続されているカメラの一意の ID です。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値 : Connector n: 1

設定可能な値: Connector n: 1
カメラ ID は固定されており, 変更できません。

Video Input Connector [n] CameraControl Mode

n: 1..2

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 : カメラ制御をディセーブルにします。
On : カメラ制御をイネーブルにします。

Video Input Connector [n] CEC Mode

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 [ビデオ 入力 コネクタ[n] 接続されているデバイス CEC [n] (Video Input Connector[n] ConnectedDevice CEC [n])] ステータスで参照できるようになります。ただし, 接続デバイスも CEC をサポートしてい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

設定可能な値: Connector n: Off/On
Off : CEC が無効です。
On : CEC が有効になります。

Video Input Connector [n] InputSourceType

n: 1..2

ビデオ入力に接続された入力ソースのタイプを選択します。
コネクタ 1 はデバイスの内蔵カメラであることに注意してください。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値 : Connector 1 : camera Connector 2 : PC

値スペース : Connector 1 : camera Connector 2 : PC/camera/document_camera/mediaplayer/whiteboard/other
PC : コンピュータがビデオ入力に接続されている場合に使用します。
camera : カメラがビデオ入力に接続されている場合に使用します。
document_camera : ドキュメント カメラがビデオ入力に接続されている場合に使用します。
mediaplayer : メディア プレーヤーがビデオ入力に接続されている場合に使用します。
whiteboard : ホワイトボード カメラがビデオ入力に接続されている場合に使用します。
other : 他のオプションが当てはまらない場合に使用します。

Video Input Connector [n] Name

n: 1..2

ビデオ入力コネクタの名前を定義します。

必要なユーザ ロール : ADMIN, INTEGRATOR
デフォルト値 : Connector 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。

Video Input Connector [n] OptimalDefinition Profile

n: 1..2

この設定は, 対応する Video Input Connector [n] Quality 設定が Sharpness に設定されている場合には無効です。

最適鮮明度プロファイルは, ビデオ会議室の照明状態とカメラと品質を反映します。光の条件およびカメラの品質が優れているほど, プロファイルが高くなります。通常, Normal または Medium プロファイルが推奨されます。ただし, 光の条件が良い場合, 特定のコール率の解像度を大きくするために, High プロファイルを設定できます。解像度が発信側と着信側の両方のデバイスでサポートされている必要があります。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Medium

値スペース : Normal/Medium/High

Normal : 照明が通常から不良の環境には, このプロファイルを使用します。解像度は控えめに設定されます。

Medium : 安定した光条件および高品質なビデオ入力が必要です。一部のコール レートの場合, これは高解像度へ移動できます。

High : 優れた全体的なエクスペリエンスを実現するには, 理想に近いビデオ会議の光の状態および高品質なビデオ入力が必要です。相当高い解像度が使用されます。

Video Input Connector [n] PreferredResolution

n: 2..2

推奨する画面解像度とリフレッシュレートを定義します。これらは, HDMI 経由でシステムに接続されている入力ソース (例 : ラップトップ) に対してビデオ会議デバイスがアドバタイズします。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。

2560_1440_60 と 3840_2160_30 のフォーマットは, 1920_1080_60 フォーマットと比較すると約 2 倍の量のデータを使用し, HDMI 1.4b データレート以上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) を必要とします。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Connector n : 1920_1080_60

設定可能な値: Connector n: 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。

Video Input Connector [n] PresentationSelection

n: 2..2

プレゼンテーションソースをビデオ入力に接続したときの, ビデオ会議デバイスの動作を定義します。

デバイスがスタンバイモードの場合, プレゼンテーションソースを接続すると復帰します。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 : コネクタ n : AutoShare

設定可能な値: Connector n: AutoShare/Desktop/Manual/OnConnect

AutoShare : 通話時に, ビデオ入力のコンテンツは, ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) , 自動的に遠端とローカル画面に表示されます。ユーザ インターフェイス上で [共有 (Share)] を選択する必要はありません。コールの発信時または応答時にプレゼンテーション ソースがすでに接続されている場合は, ユーザ インターフェイス上で [共有 (Share)] を手動で選択する必要があります。

Desktop : ビデオ入力のコンテンツは, ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) , 画面に表示されます。これは, アイドル状態のときと通話中のときの両方に適用されます。また, ビデオ入力のコンテンツは, 通話の終了時にアクティブ入力であれば, 画面に表示されたままとなります。

Manual : ユーザ インターフェイスで [共有 (Share)] を選択するまでビデオ入力の内容は画面に表示されません。

OnConnect : ビデオ入力のコンテンツは, ケーブルを接続するかまたはソースが起動すると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) , 画面に表示されます。それ以外の場合は, Manual モードと同じ動作です。

Video Input Connector [n] Quality

n: 2..2

ビデオのエンコーディングと送信のときには, 高解像度と高フレーム レートとの間にトレード オフが存在します。一部のビデオ ソースでは, 高フレーム レートが高解像度より重要である場合や, 逆の場合もあります。この設定で, 高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値: Connector n: Sharpness

設定可能な値: Connector n: Motion/Sharpness

Motion : できるだけ高いフレーム レートにします。通常, 多数の参加者がいる場合や画像の動きが激しい場合など, 高フレーム レートが必要なときに使用されます。

Sharpness : できるだけ高い解像度にします。詳細なイメージやグラフィックに高い品質が必要な場合に使用されます。

Video Input Connector [n] RGBQuantizationRange

n: 2..2

ビデオ入力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら, 一部のデバイスは規格に準拠していません。その場合, ソースの完全なイメージを取得するために, この設定を使用して設定を上書きできます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Full/Limited

Auto : RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて自動的に選択されます。CE ビデオ形式は, 限定された量子化範囲レベルを使用します。IT ビデオ形式は, 完全な量子化範囲レベルを使用します。

Full : 完全な量子化の範囲。R, G, B の量子化範囲にはすべてのコード値 (0 ～ 255) が含まれます。これは CEA-861-E で規定されています。

Limited : 限定された量子化の範囲。極端なコード値を除いた R, G, B の量子化範囲 (16 ～ 235) 。これは CEA-861-E で規定されています。

Video Input Connector [n] Visibility

n: 1..2

ユーザ インターフェイスのメニューにあるビデオ入力コネクタの表示を定義します。

コネクタ 1 はデバイスの内蔵カメラであり, プレゼンテーションソースとして使用できないことに注意してください。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Connector 1: Never Connector 2: IfSignal

値スペース : Connector 1: Never Connector 2: Always/IfSignal/Never

Always : ビデオ入力コネクタ用メニュー選択は, ユーザ インターフェイスに常に表示されます。

IfSignal : ビデオ入力コネクタ用メニュー選択は, ビデオ入力に何か接続されている場合のみ表示されます。

Never : 入力の送信元はプレゼンテーション ソースとして使用されないため, ユーザ インターフェイスに表示されません。

Video Output Connector [n] Resolution

n: 1.. 1

内蔵画面の解像度と更新間隔。この値は固定されており, 変更できません。

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。

Video Presentation DefaultPIPPosition

プレゼンテーションのピクチャインピクチャ (PiP) の画面上の位置を定義します。この設定は, たとえばユーザ インターフェイスを使用して, プレゼンテーションが明示的に PiP に縮小された場合にのみ有効です。この設定は, 次回以降のコールで有効になります。コール中に変更された場合, 現在のコールへの影響はありません。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : プレゼンテーション PiP の位置はコール終了後にも変更されません。

UpperLeft : プレゼンテーション PiP が画面の左上隅に表示されます。

UpperCenter : プレゼンテーション PiP が画面の上部中央に表示されます。

UpperRight : プレゼンテーション PiP が画面の右上隅に表示されます。

CenterLeft : プレゼンテーション PiP が画面の左中央に表示されます。

CenterRight : プレゼンテーション PiP が画面の右中央に表示されます。

LowerLeft : プレゼンテーション PiP が画面の左下隅に表示されます。

LowerRight : プレゼンテーション PiP が画面の右下隅に表示されます。

Video Presentation DefaultSource

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソースを定義します。この設定は, API およびサードパーティのユーザー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。

Video Presentation Priority

帯域幅がメインビデオチャネルとプレゼンテーションチャネル間で分散される方法を決定します。

必要なユーザ ロール : ADMIN

デフォルト値: Equal

値スペース: Equal/High/Low

Equal : 利用可能なビデオ伝送帯域幅がメインチャネルとプレゼンテーションチャネルの間で分散されます。

High : プレゼンテーションチャネルは, メインビデオチャネルを犠牲にして, 利用可能な帯域の大部分に割り当てられます。

Low : メインビデオチャネルは, プレゼンテーションチャネルを犠牲にして, 利用可能な帯域の大部分に割り当てられます。

Video Selfview Default FullscreenMode

コール終了後に, メイン ビデオ ソース (セルフビュー) を全画面表示するか, 小さいピクチャインピクチャ (PiP) として表示するかを定義します。この設定はセルフビューがオンになっている場合にのみ有効です (Video Selfview Default Mode の設定を参照) 。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Current

値スペース : Off/Current/On

Off : セルフビューは PiP として表示されます。

Current : セルフビューの画像のサイズはコール終了時に未変更の状態に保たれます。つまりコール中に PiP であった場合はコール終了後にも PiP のままであり, コール中に全画面であった場合はコール終了後にも全画面のままです。

On : セルフビューの画像は全画面表示されます。

Video Selfview Default Mode

コール終了後にメイン ビデオ ソース (セルフビュー) を画面に表示するかどうかを定義します。セルフビュー ウィンドウの位置とサイズはそれぞれ, Video Selfview Default PIPPosition と Video Selfview Default FullscreenMode の設定によって決まります。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : Current

値スペース : Off/Current/On

Off : セルフビューはコール退出時にオフにされます。

Current : セルフビューはそのままの状態で残ります。つまりコール中にオンであった場合はコール終了後にもオンのままであり, コール中にオフであった場合はコール終了後にもオフのままです。

On : セルフビューはコール退出時にオンにされます。

Video Selfview Default OnMonitorRole

コールの後にメイン ビデオ ソース (セルフビュー) を表示する画面/出力を設定します。この値は, 異なる出力用に設定された Video Output Connector [n] MonitorRole 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, Video Output Connector [n] MonitorRole 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, Video Output Connector [n] MonitorRole が Second に設定された出力上に表示されます。

Video Selfview Default PIPPosition

コール終了後に小さいセルフビュー ピクチャインピクチャ (PiP) を表示する画面上の位置を定義します。この設定は, セルフビューがオンになっており (Video Selfview Default Mode 設定を参照) , 全画面表示がオフになっている場合 (Video Selfview Default FullscreenMode 設定を参照) にのみ有効です。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : 右下 (LowerRight)

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : セルフビュー PiP の位置はコール終了後にも変更されません。

UpperLeft : セルフビュー PiP が画面の左上隅に表示されます。

UpperCenter : セルフビュー PiP が画面の上部中央に表示されます。

UpperRight : セルフビュー PiP が画面の右上隅に表示されます。

CenterLeft : セルフビュー PiP が画面の左中央に表示されます。

CenterRight : セルフビュー PiP が画面の右中央に表示されます。

LowerLeft : セルフビュー PiP が画面の左下隅に表示されます。

LowerRight : セルフビュー PiP が画面の右下隅に表示されます。

Video Selfview OnCall Mode

コールをセットアップする短い間, この設定を使用してセルフ ビューがオンにされます。セルフビューをオンのままにしておく時間の長さは, Video Selfview OnCall Duration 設定で定義します。これは一般にセルフ ビューがオフの場合に適用されます。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値 : 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。

Video Selfview OnCall Duration

この設定は Video Selfview OnCall Mode 設定がオンになっている場合にのみ有効です。この場合, ここで設定された秒数により, 自動的にオフにされる前にセルフ ビューが表示される期間が決まります。

必要なユーザ ロール : ADMIN, INTEGRATOR

デフォルト値: 10

値スペース : 整数 (1..60)

範囲 : セルフ ビューをオンにする期間を選択します。有効な範囲は, 1 ～ 60 秒です。

Web エンジンの設定

WebEngine Mode

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。

WebEngine RemoteDebugging

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ーに警告します。ヘッダーには, 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 : リモートデバッグをオフにします。

On : リモートデバッグをオンにします。

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

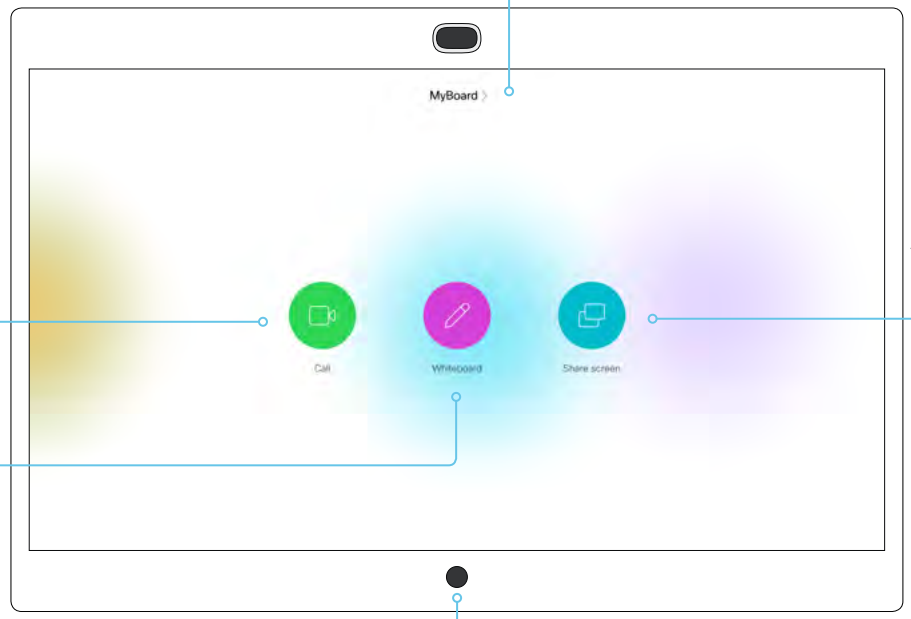
Webex Board の使用方法

Webex Board のユーザーインターフェイスとボードの使用方法については，ユーザーガイドに詳しく記載されています。

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設定を行うことができます。

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。



[コール (Call)] をタップすると，コールを発信できます。

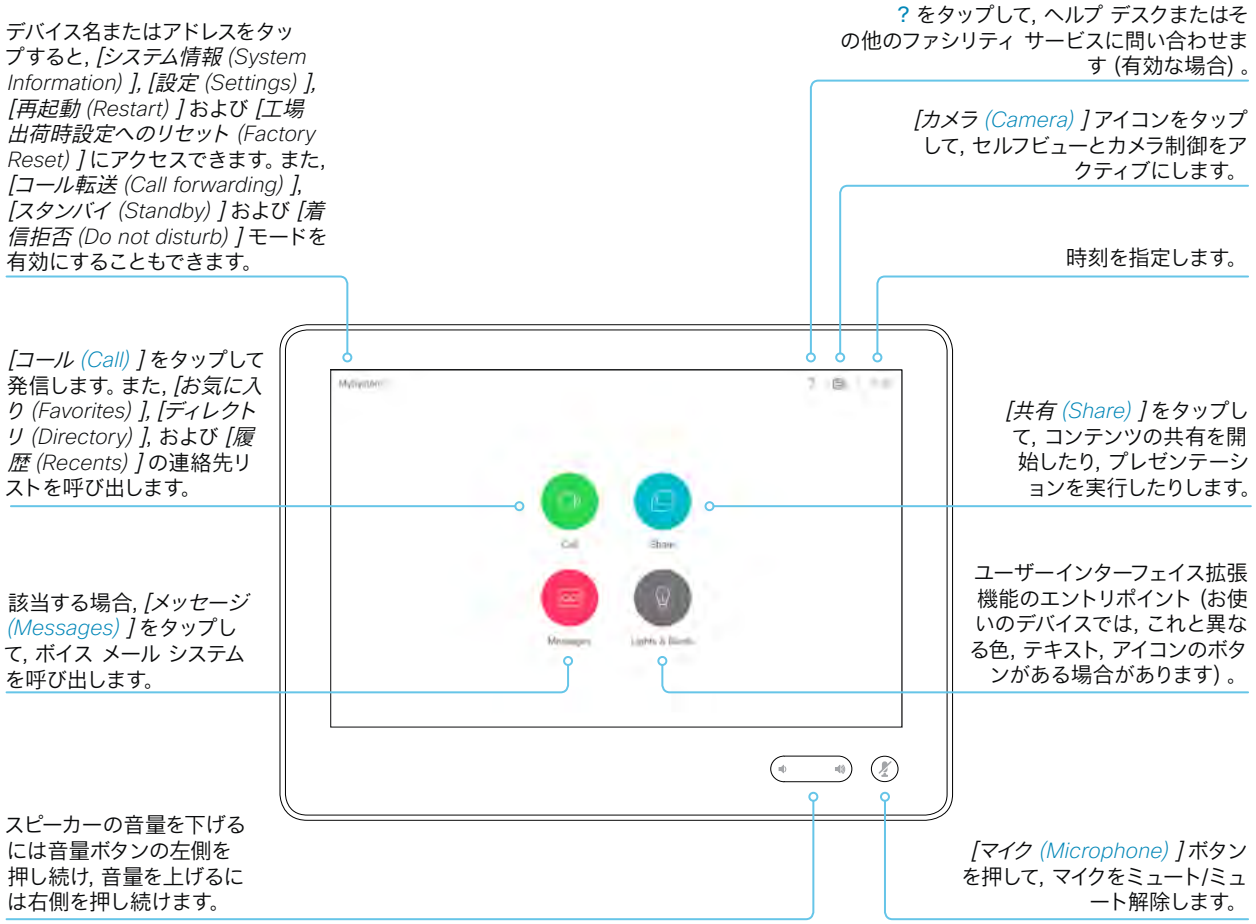
[ホワイトボード (Whiteboard)] をタップすると，新しいホワイトボードを開始するか，既存のホワイトボードのリストにアクセスすることができます。

[共有 (Share)] をタップすると，共有オプションが表示されます。

*ホーム 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。

Touch 10 の使用方法

Touch 10 ユーザーインターフェイスとその使用方法の詳細については，ビデオ会議デバイスのユーザーガイドを参照してください。



リモート モニタリングのセットアップ

要件:

- *RemoteMonitoring* オプション

リモートモニタリングは別の場所からデバイスを制御する場合に便利です。

入力ソースからのスナップショットが ウェブ インターフェイスに表示されるため, 部屋にいなくてもカメラ ビューをチェックしてカメラを制御できます。

有効にすると, スナップショットは約 5 秒おきに自動的に更新されます。

デバイスにリモートモニタリングオプションがあるかどうかの確認

1. ウェブ インターフェイスにログインします。
2. [ホーム (Home)] ページで, インストールされているオプションのリストに *RemoteMonitoring* が含まれているかどうかを確認します。

   リストにない場合, リモート モニタリングは使用できません。

リモート モニタリングを有効にする

RemoteMonitoring オプション キーをインストールします。オプション キーのインストール方法については, ►「オプション キーを追加する」の章で説明しています。

リモートモニタリングオプションを有効にする場合は, プライバシーに関する地域の法律および規制を遵守する必要があります。また, システム管理者がカメラや画面を監視および制御する場合があることを, デバイスのユーザー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。

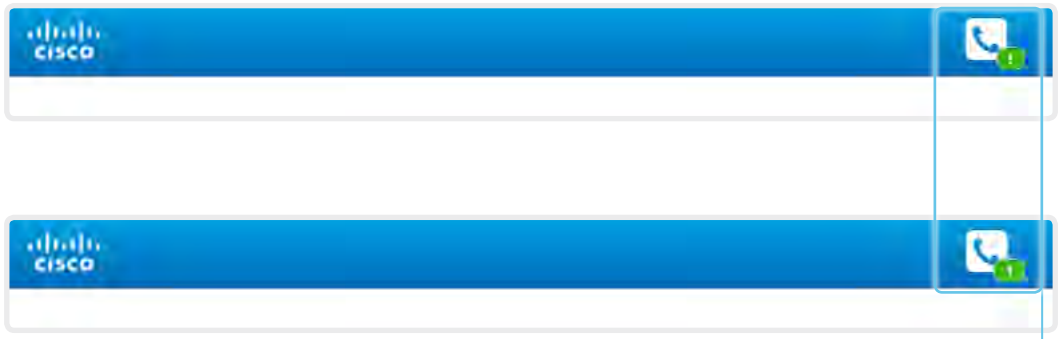
スナップショットは, デバイスがアイドル状態のときおよびコール中に表示されます。

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, 遠端デバイスにリモートモニタリングオプションがあるかどうかとは関係がありません。

遠端スナップショットは, コールが暗号化されていると表示されません。

ウェブ インターフェイスを使用したコール情報へのアクセスとコール応答



着信通知

[コールインジケーター (Call indicator)] をクリックし，コールの応答と拒否を行う *[コール操作 (Call Control)]* ページを開きます。

デバイスがコール中

バッジはアクティブ コール数を示します。

コールインジケーター

コールインジケータは，着信コールについて通知するため，およびデバイスがコール中であるときを表示するために用意されています。

デバイスがアイドル状態の場合，コールインジケータは表示されません。

コールの操作

[コール操作 (Call Control)] ページでは，コール操作に関係する操作ボタンが表示されます。各ボタンを使用して次のことを実行します。

- コールの詳細を表示する
- コールを保留にする
- 通話に応答する
- コールを切断する

ウェブ インターフェイスを使用してコールをかける (1/2 ページ)

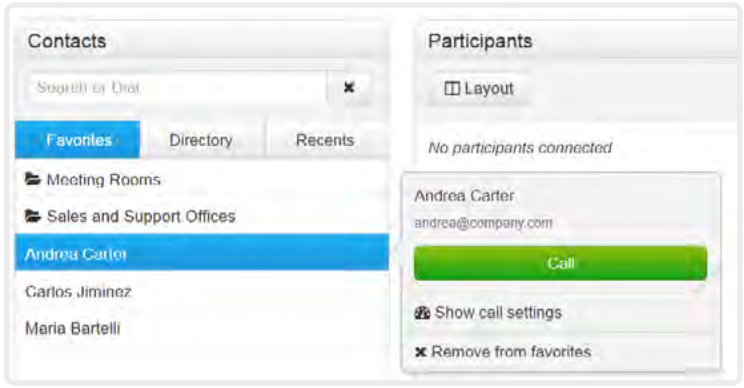
ウェブ インターフェイスにログインし, *[コール制御 (Call Control)]* に移動します。

コールの発信

Web インターフェイスを使ってコールを開始した場合でも, コールに使用されるのはビデオ会議デバイス (ディスプレイ, マイク, およびスピーカー) であり, Web インターフェイスを実行している PC ではありません。

1. 正しいエントリを見つけるには, *[お気に入り (Favorites)]* リスト, *[ディレクトリ (Directory)]* リスト, または *[発着信履歴 (Recents)]* リストに移動するか, あるいは *[検索またはダイヤル (Search or Dial)]* フィールドに 1 文字以上を入力します*。該当する連絡先名をクリックします。
2. 連絡先カードで *[コール (Call)]* をクリックします。

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



* 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には, *[全通話切断 (Disconnect all)]* 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。

ウェブ インターフェイスを使用したコールの発信 (2/2 ページ)

ウェブ インターフェイスにログインし, *[コール制御 (Call Control)]* に移動します。

複数の相手に発信

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マルチサイト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。

会議ブリッジを使用した複数の相手に対するコール (CUCM アドホック会議) は, ビデオ会議デバイス自身でサポートされていても Web インターフェイスではサポートされません。

音量の調整

マイクをミュートにする

[マイク: オン (Microphone: On)] をクリックして, マイクをミュートにします。すると, テキストが *[マイク: オフ (Microphone: Off)]* に変わります。

ミュートを解除するには, *[マイク: オフ (Microphone: Off)]* をクリックします。

ウェブインターフェイスを使用してコンテンツを共有する

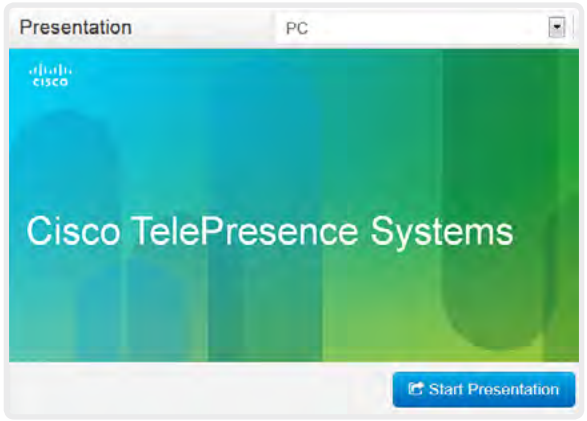
ウェブ インターフェイスにログインし, *[コール制御 (Call Control)]* に移動します。

コンテンツの共有

[プレゼンテーションの開始 (Start Presentation)] をクリックします。すると, テキストが *[プレゼンテーションの停止 (Stop Presentation)]* に変わります。

コンテンツ共有の停止 :

共有している間に表示される *[プレゼンテーションを中止 (Stop Presentation)]* ボタンをクリックします。



スナップショット領域

選択されたプレゼンテーション ソースのスナップショットが表示されます。

リモートモニタリングオプションのあ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

ウェブ インターフェイスにログインし, *[コール制御 (Call Control)]* に移動します。

前提条件

以下の条件において, 通話中にリモート参加者のカメラ (相手先) を制御できます。

- 遠端デバイスで *[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。
- 遠端カメラではスピーカーのトラッキングはオンになっていない。
- ローカルデバイスにリモートモニタリングオプションがある。

リモート参加者のカメラを制御

1. リモート カメラ制御ウィンドウを開くには, カメラのアイコンをクリックします。
2. カメラのパンには左右の矢印キー, チルトには上下の矢印キー, ズームインとズームアウトには + および - を使用します。

   遠端カメラの制御が許可されていない場合は, 画面にコントロールが表示されません。

   コールが暗号化されている場合, 制御の背後の遠端スナップショットは表示されません。

パケット損失の復元力：ClearPath

ClearPath により，高度なパケット損失復元メカニズムを導入できます。これらのメカニズムは，エラーを起こしやすい環境でデバイスを使用する場合の品質を向上させます。

ClearPath は Cisco 独自のプロトコルです。CE ソフトウェアが実行されているすべてのエンドポイントが ClearPath に対応しています。

関係するエンドポイントとインフラストラクチャ要素が ClearPath に対応している場合，ポイントツーポイント接続 (ホストされた会議を含む) ですべてのパケット損失復元メカニズムが使用されます。MultiSite 会議でサポートされるのは，これらのメカニズムの一部だけです。

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。

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。

ウェブ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。Web インターフェイスにサインインし，*[セットアップ (Setup)] > [設定 (Configuration)] > [ルーム分析 (RoomAnalytics)] > [人の存在の検出 (PeoplePresenceDetector)]* に移動します。

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。Web インターフェイスにサインインし，[セットアップ (Setup)] > [設定 (Configuration)] > [ルーム分析 (RoomAnalytics)] > [非通話中の人をカウント (PeopleCountOutOfCall)] に移動します。

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。Web インターフェイスにサインインし，*[セットアップ (Setup)] > [ステータス (Status)] > [ルーム分析 (RoomAnalytics)]* に移動します。

診断

Touch 10 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，ユーザー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

Room 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, 室内で作業している人にとってはじゃあmである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。

ウェブ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。Web インターフェイスにサインインし, *[セットアップ (Setup)] > [設定 (Configuration)] > [ルーム分析 (RoomAnalytics)] > [環境雑音の予測 (AmbientNoiseEstimation)] > [モード (Mode)]* に移動します。

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 (1/2 ページ)

ユーザーインターフェイスをカスタマイズすると，照明やブラインドなど，会議室内の周辺機器を制御したり，マクロをトリガーしてビデオ会議デバイスの動作を変更したりできます。

これにより，制御システムの機能と，ビデオ会議デバイスの使いやすいユーザーインターフェイス (Touch 10) 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。

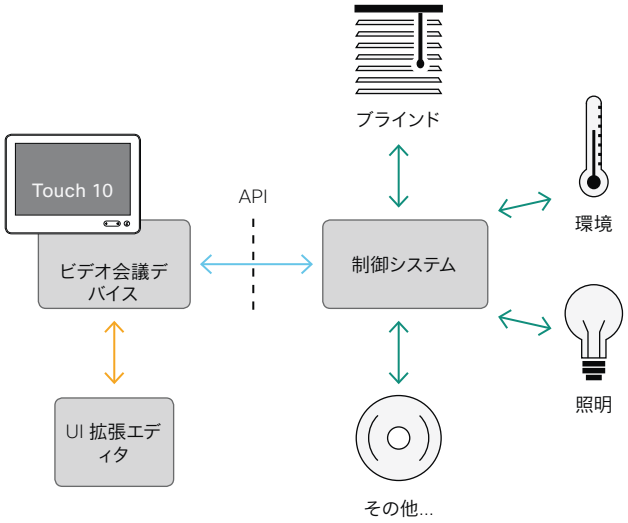
UI 拡張エディタ (以前の室内制御エディタ) を使用してカスタムユーザーインターフェイスパネル，アクションボタン，および Web アプリを設計する方法，およびビデオ会議デバイスの API を使用してコントロールとアクションをプログラミングする方法の詳細については，カスタマイズガイドを参照してください。次のリンクにアクセスします。

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

室内制御アーキテクチャ

タッチインターフェイス*を搭載したシスコのビデオ会議デバイスと，制御システムが必要です。制御システムは，ハードウェア ドライブや周辺機器を備えた Crestron や AMX などの他社製システムである場合もあります。周辺機器を制御するのは，ビデオ会議デバイスではなく制御システムです。

制御システムをプログラミングするとき，ビデオ会議デバイスのユーザーインターフェイス上のコントロールに接続するには，ビデオ会議デバイスの API (イベントとコマンド) を使用する必要があります。



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，制御システムとしても使用できます。この場合，制御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 (2/2 ページ)

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*，*[統合 (Integration)] > [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。

- [エディタ (Editor)] メニュー ≡ をクリックし，*[エディタをダウンロード (Download the Editor)]* を選択すると，ハードドライブからローカルにブラウザで実行できるスタンドアロンバージョンを入手できます。

  これにより，デバイスに接続しなくてもカスタムユーザーインターフェイスや Web アプリを作成できます。後でファイルをエクスポートおよびインポートして，ローカルバージョンとデバイスの間で作業を移動することができます。

プレビュー機能

エディタは，カスタム インターフェイスがどのようにユーザ インターフェイスに表示されるか確認するためのプレビュー機能も提供します。

プレビュー機能ではカスタムパネルがソフトウェア的に完全に再現されるため，コントロールをクリックすると，実際のユーザー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 ユーザーロールを持つユーザーが必要です。

カスタマイゼーション

マクロを使用したビデオ会議デバイスの動作のカスタマイズ

マクロにより, デバイスで実行するコードの独自のスニペットを作成できます。言語は, arrow functions, promises および classes などの機能をサポートする JavaScript/ECMAScript 6 です。

インテグレータは, マクロフレームワークを利用して, 個別の顧客要件に応じてデバイスの動作を調整するスクリプトを作成できます。インテグレータが行える作業には, 独自の機能または機能のバリエーションの実装, 特定の設定または再設定の自動化, 機能のカスタム テストやモニタリングの作成などがあります。

マクロの使用とカスタムユーザー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ー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組み込みの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参照してください。次のリンクにアクセスします。

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

デバイスでのマクロの使用許可

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

- *[マクロ (Macros)] > [モード (Mode)]* を [オン (On)] に設定します。

  この設定が [オフ (Off)] の場合にマクロ エディタを起動しようとすると, ポップアップ メッセージが表示されます。*[マクロの有効化 (Enable Macros)]* をタップして応答した場合は *[マクロ (Macros)] > [モード (Mode)]* 設定が自動的に [オン (On)] に変更され, エディタが起動します。

マクロ エディタの起動

Web インターフェイスにサインインし*, *[統合 (Integration)] > [マクロエディタ (Macro Editor)]* に移動します。

オフラインで使用可能なエディタのスタンドアロン バージョンは提供されていません。

* マクロ エディタ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デフォルトボタンを削除する

通話 または *共有*などのデフォルトボタンを使用しない使用例もあります。このような使用しないボタンは混乱を引き起こす場合があります。このような場合, 使用しないボタンをユーザインターフェイスから削除できます。その場合もカスタム UI ボタンは表示できます。カスタムボタンの追加中にデフォルトボタンを削除すると, ユーザインターフェイスを完全にカスタマイズできるようになります。

たとえば, 誰もこのデバイスからコンテンツや通話を共有しない場合は, *[通話 (Call)]* ボタンと *[共有 (Share)]* ボタンを削除できます。代わりに, 実行する予定のタスク用のカスタムボタンとパネルを追加します。

構成

ユーザー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。通話中に表示される, 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)] > [Share (共有)] > [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)] > [Call (通話)] > [VideoMute (ビデオミュート)]*: デフォルト *ビデオをオフにする* ボタンを削除します。
- *[ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [HideAll (すべて非表示)]*: すべてのデフォルトボタンを削除します。カスタムボタンは削除されません。
- *[ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [Call (通話)] > [End (終了)]*: *通話終了* ボタンを削除します。
- *[ユーザーインターフェイス (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。

設定はボタンだけを削除し, 機能などは削除しません。*共有* ボタンをユーザーインターフェイスから削除しても, Proximity を使用してコンテンツを共有できます。

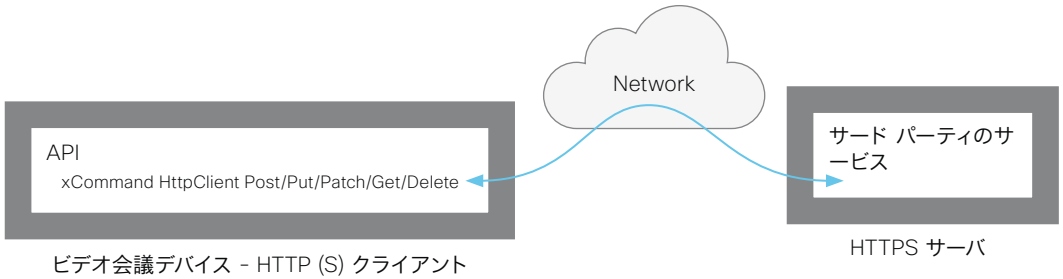
解説場所

ボタンの削除方法およびユーザインターフェイスのカスタマイズ方法については *カスタマイズガイド*を参照してください。 次のリンクにアクセスします。

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

カスタマイゼーション

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) サーバーに任意の HTTP (S) 要求を送信できます。さらに, デバイスはサーバーから送信された応答を受信します。デバイスは, **Post**, **Put**, **Patch**, **Get**, および **Delete** メソッドをサポートしています。

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 **False** 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) サーバーのリスト

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` はホスト名の消去を許容します
- `xCommand HttpClient` はホスト名リストを許容します
- `xCommand HttpClient` はホスト名削除 `ID` を許容します: `<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。

証明書検証なしの HTTPS

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 サーバー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ー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 *[HttpClient]* > [安全でない HTTPS を許可 *(AllowInsecureHTTPS)*] を [オン (On)] to に設定することができます。これにより, サーバー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) サーバーに送信できます。

```
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 ガイドを参照してください。

解説場所

HTTP (S) Post リクエストについての詳細情報は カスタマイズガイドにあります。 次のリンクにアクセスします。

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

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: WebApps]`

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。詳細情報はデバイスの Web インターフェイスの *[メンテナンス (Maintenance)] > [診断 (Diagnostics)]* ページで確認できます。

デジタルサイネージのセットアップ

1. ウェブ インターフェイスにサインインして, *[セットアップ (Setup)] > [設定 (Configuration)]* に移動します。
2. *[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]* 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入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)]: [オフ (Off)] に設定すると, デバイスはスタンバイモードに入りません (非推奨) 。[オン (On)] に設定すると, デバイスは *[スタンバイ (Standby)] > [遅延 (Delay)]* がタイムアウトになったときにスタンバイモードに入ります。

   [スタンバイ (Standby)] > [遅延 (Delay)]: デバイスがスタンバイモードに入るまでに 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)] > [モーション検知ウェイクアップ (WakeUpOnMotionDetection)]: [オン (On)] に設定すると, 誰か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。[オフ (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:

- オーディオが含まれる Web ページでオーディオを再生するかどうかを決定する。

  [スタンバイ (Standby)] > [サイネージ (Signage)] > [オーディオ (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ーに警告します。ヘッダーには, 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。

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* 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。 次のリンクにアクセスします。

► 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*, *[セットアップ (Setup)] > [設定 (Configuration)]* に移動します。
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. [統合 *(Integration)*] > [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. 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。
   - URL : Web アプリの URL。
   - アイコン URL (Icon URL) (オプション) : ホーム画面ボタンのアイコン。
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ーに警告します。ヘッダーには, 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。

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 ページを閉じる :

- `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ーに警告します。ヘッダーには, 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	プレゼンテーションソースの最大組み合わせ可能数
Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2, Board	2
Codec Plus, Room 55, Room 55 Dual, Room 70	3
SX80, MX700, MX800, Codec Pro, Room 70 G2	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。

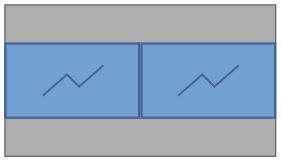
オン デマンドによる構成およびレイアウトの変更

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ー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。

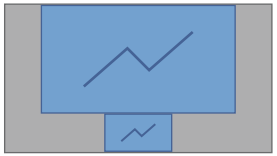
レイアウト

同等 (Equal)



ソースの数 : 2

プロミネント (Prominent)



ソースの数 : 2

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>
```

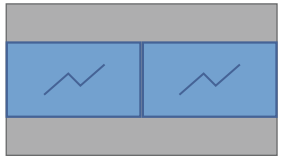
値は次のとおりです。

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。

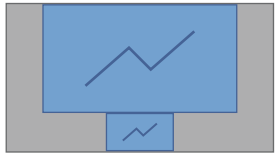
詳細については, API ガイドを参照してください。

例

```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal
```

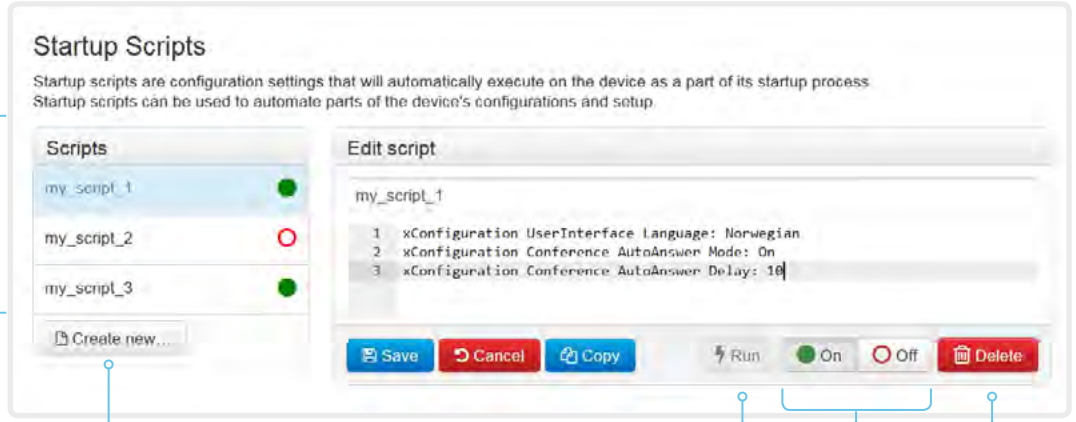


```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent
```



スタートアップ スクリプトを管理する

Web インターフェイスにサインインし, *[統合 (Integration)] > [スタートアップスクリプト (Startup Scripts)]* に移動します。



図に示しているスクリプト名と設定は一例です。独自のスクリプトを作成できます。

スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます。*

緑色のドットがアクティブなスタートアップ スクリプトの横に, 赤色の丸が非アクティブなスタートアップ スクリプトの横に表示されます。

複数のスタートアップ スクリプトがある場合は, リストの上から下に順番に実行されます。

スタートアップ スクリプトを作成する

1. *[新規作成 (Create new...)]* をクリックします。
2. タイトル入力フィールドにスタートアップ スクリプトの名前を入力します。
3. コマンド入力エリアにコマンド (xConfiguration または xCommand) を入力します。新しい行で各コマンドを開始します。
4. *[Save (保存)]* をクリックします。
5. [オン (On)] をクリックして, スタートアップ スクリプトをアクティブにします。

既存のスクリプトを編集の開始点として使用する場合は, そのスクリプトを選択して *[コピー (Copy)]* をクリックします。

起動スクリプトをすぐに実行する

1. リストからスタートアップ スクリプトを選択します。
2. *[実行 (Run)]* をクリックします。
   アクティブなスタートアップ スクリプトと非アクティブなスタートアップ スクリプトの両方をすぐに実行できます。

スタートアップ スクリプトをアクティブ化または非アクティブ化する

1. リストからスタートアップ スクリプトを選択します。
2. スクリプトをアクティブにする場合は *[オン (On)]* を, 非アクティブにする場合は *[オフ (Off)]* をクリックします。
   アクティブなスタートアップスクリプトは, デバイスが起動するたびに実行されます。

スタートアップ スクリプトを削除する

1. リストからスタートアップ スクリプトを選択します。
2. *[削除 (Delete)* をクリックします。

スタートアップ スクリプトについて

スタートアップ スクリプトには起動手順の一部として実行されるコマンド (xCommand) および構成 (xConfiguration) が含まれます。

`xCommand SystemUnit Boot` など, いくつかのコマンドとコンフィギュレーションはスタートアップ スクリプトに含めることができません。不正なコマンドや設定が含まれたスクリプトは保存できません。

xCommand および xConfiguration の構文とセマンティックは, 製品の API ガイドに説明されています。

デバイスの XML ファイルへのアクセス

ウェブ インターフェイスにサインインして, *[統合 (Integration)] > [開発者 API (Developer API)]* を選択します。

XML ファイルはデバイスの API の一部です。デバイスに関する情報が階層で構成されています。

- *Configuration.xml* には現在のデバイス設定 (コンフィギュレーション) が含まれます。これらの設定は, ウェブ インターフェイスまたは API (アプリケーション プログラミング インターフェイス) から制御されます。
- *status.xml* 内の情報は, デバイスによって常に更新され, システムおよびプロセスの変更が反映されます。ステータス情報は, ウェブ インターフェイスまたは API からモニタします。
- *Command.xml* には, デバイスにアクションの実行を指示するために使用できるコマンドの概要が含まれています。コマンドは, API から発行されます。
- *Valuespace.xml* には, デバイス設定, ステータス情報, およびコマンドのすべての値スペースの概要が含まれています。

XML ファイルを開く

XML ファイルを開くにはファイル名をクリックします。

API について

アプリケーションプログラミングインターフェイス (API) は, デバイスを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は, デバイスの API ガイドで説明されています。

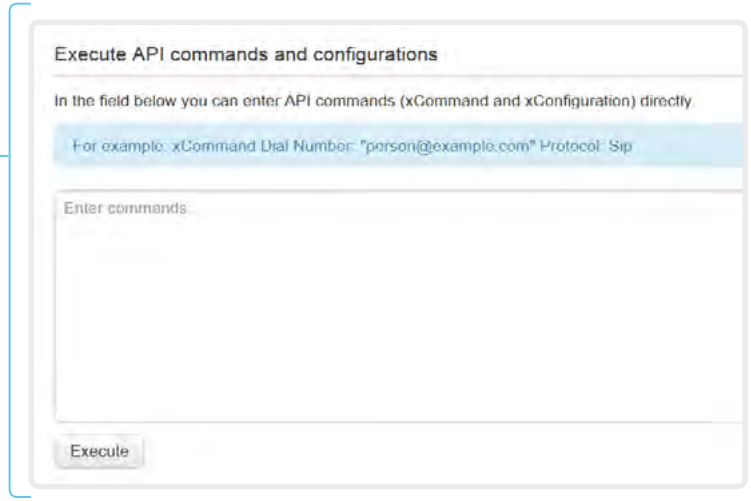
ウェブ インターフェイスからの API コマンドとコンフィギュレーションの実行

ウェブ インターフェイスにサインインして, *[統合 (Integration)] > [開発者 API (Developer API)]* を選択します。

コマンド (xCommand) および設定 (xConfiguration) は, ウェブ インターフェイスから実行できます。構文とセマンティックの説明については, デバイスの API ガイドを参照してください。

API コマンドとコンフィギュレーションの実行

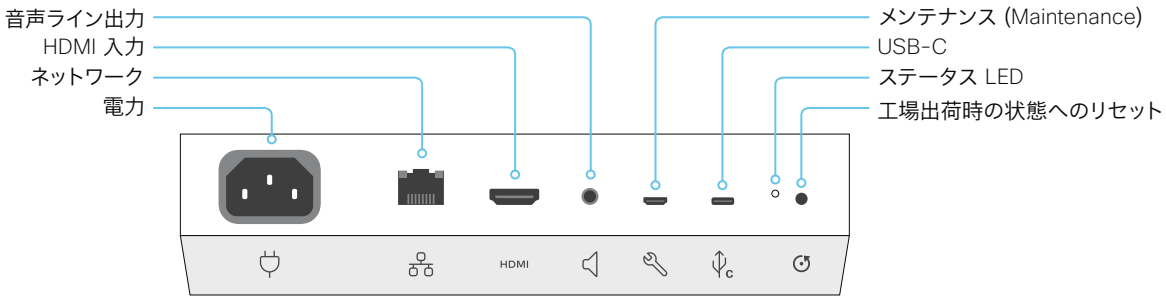
1. テキスト領域に, コマンド (xCommand または xConfiguration) またはコマンド シーケンスを入力します。
2. *[実行 (Execute)]* をクリックしてコマンドを発行します。



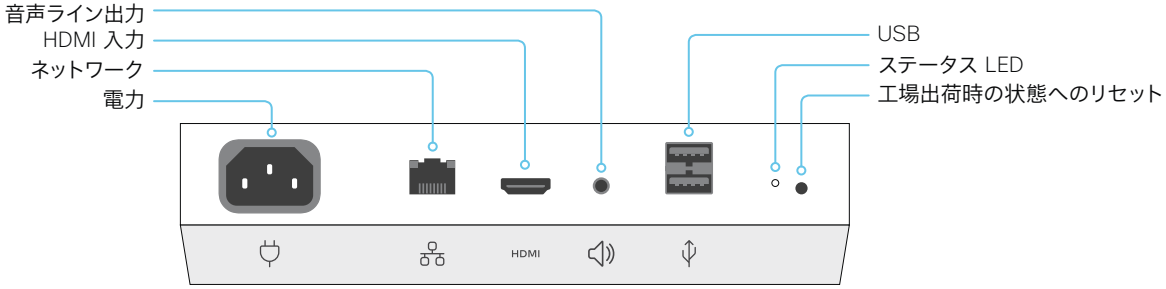
API について

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。

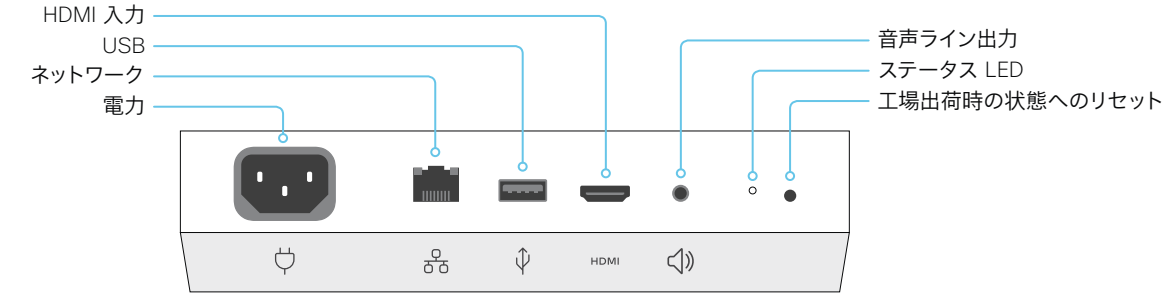
コネクタ パネル



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) 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 には, デバイスによって番号 1, ネットワーク記号 (品) , またはその両方が付いています。

補助ポート

ビデオ会議デバイスによっては, ネットワークポートが複数あります。追加のポートは, カメラ, Touch 10, サードパーティー製制御システムなどの周辺機器に使用できます。

このようなネットワークポートに接続されているデバイスはコーデックからローカル IP アドレスを取得するため, 企業ネットワークには接続されていません。パケットは, メインネットワークポート (LAN) と補助ネットワークポート (リンク-ローカル) の間の移動はできません。

- Cisco の周辺機器には, 169.254.1.41 から 169.254.1.240 の範囲 (DHCP) でのダイナミック IP アドレスが割り当てられます。
- Cisco 以外のデバイスには, ダイナミック IP アドレス (DHCP) :169.254.1.30 を割り当てることができます。

  注 : Cisco 以外のデバイスでダイナミック IP アドレスを取得できるのは, 一度に 1 つだけです。
- さらに, Cisco 以外のデバイスには, 169.254.1.241 ～ 169.254.1.254 の範囲の静的 IP アドレスを割り当てることもできます。

この方法は, SSH を使用してコーデックに接続する場合にも使用できます。このケースでは, IP アドレス 169.254.1.1 を使用できます。

パワーオーバーイーサネット (PoE)

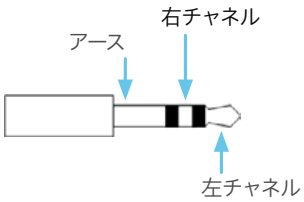
補助ネットワークポートには Power over Ethernet (PoE) を提供するものもあります。これらのポートは Touch 10 コントローラなどの周辺機器に電源を供給します。

製品	補助ネットワークポートの数	PoE 付きの補助ネットワークポートの数
Room Kit	1	0
Room Kit Mini	1	1 ( )
Room 55	1	1 ( )
Room 70 / Room 55 Dual	2	1 ( )
Room 70 G2	4	2 (, PoE)
Codec Plus	2	1 ( )
Codec Pro	4	2 (, PoE)
Board	0	0
SX10	0	0
SX20	0	0
SX80	2	0
MX200 G2 / MX300 G2	2	0
MX700 / MX800	2	0*
DX70 / DX80	1	0

* これらの製品には個別の PoE インジェクタがあり, 補助ネットワークポートの 1 つに接続されます。PoE インジェクタは Touch 10 コントローラに使用されます。

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)	
	ライン出力
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, マイクロ 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 (SSH クライアント) を使用します。最も一般的なコンピュータ タイプ (PC, MAC) およびオペレーティング システムでは, PuTTY または Tera Term は機能します。

シリアル接続は, IP アドレス, DNS, またはネットワークなしで使用できます。

パラメータ :

- ボー レート : 115200 bps
- データ ビット : 8
- パリティ : なし
- ストップ ビット : 1
- ハードウェア フロー制御 : オフ

デバイスの設定

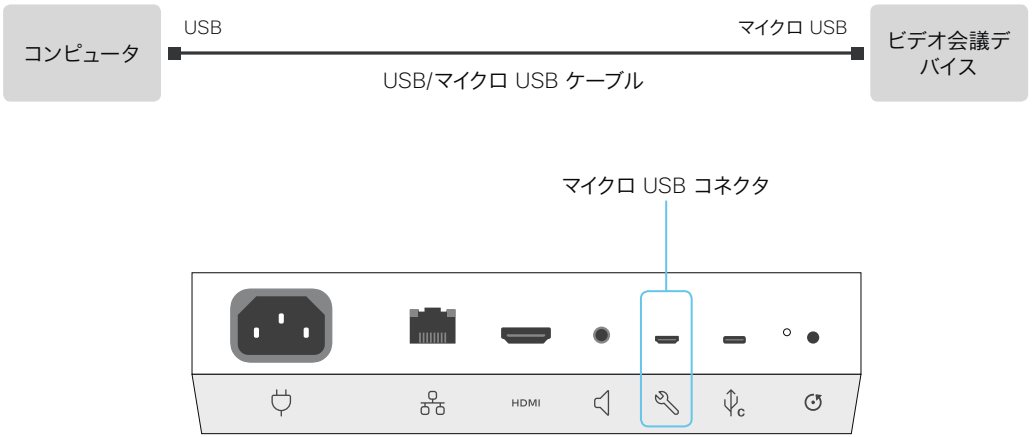
シリアル通信はデフォルトでイネーブルになっています。動作を変更するには, 次の設定を使用します。

[シリアルポート (SerialPort)] > [モード (Mode)]

セキュリティ上の理由から, シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには, 次の設定を使用します。

[シリアルポート (SerialPort)] > [ログインが必須 (LoginRequired)]

デバイスが CUCM によってプロビジョニングされている場合, シリアルポートの設定は CUCM から構成する必要があります。



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。▶ https://jp.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

Board 55 および 70 には，メンテナンス機能を提供する USB-A ポートが搭載されています。これらのデバイスにはメイン CPU へのシリアル接続はありません。USB の他に利用できるのは仮想シリアルインターフェイスだけです。つまり，デバイスがほぼ完全に機能していない限り，コンピュータからボードを認識することはできません。

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 (SSH クライアント) を使用します。最も一般的なコンピュータ タイプ (PC, MAC) およびオペレーティング システムでは，PuTTY または Tera Term は機能します。

シリアル接続は，IP アドレス，DNS，またはネットワークなしで使用できます。

パラメータ：

- ボー レート：115200 bps
- データ ビット：8
- パリティ：なし
- ストップ ビット：1
- ハードウェア フロー制御：オフ

デバイスの設定

シリアル通信はデフォルトでイネーブルになっています。動作を変更するには，次の設定を使用します。

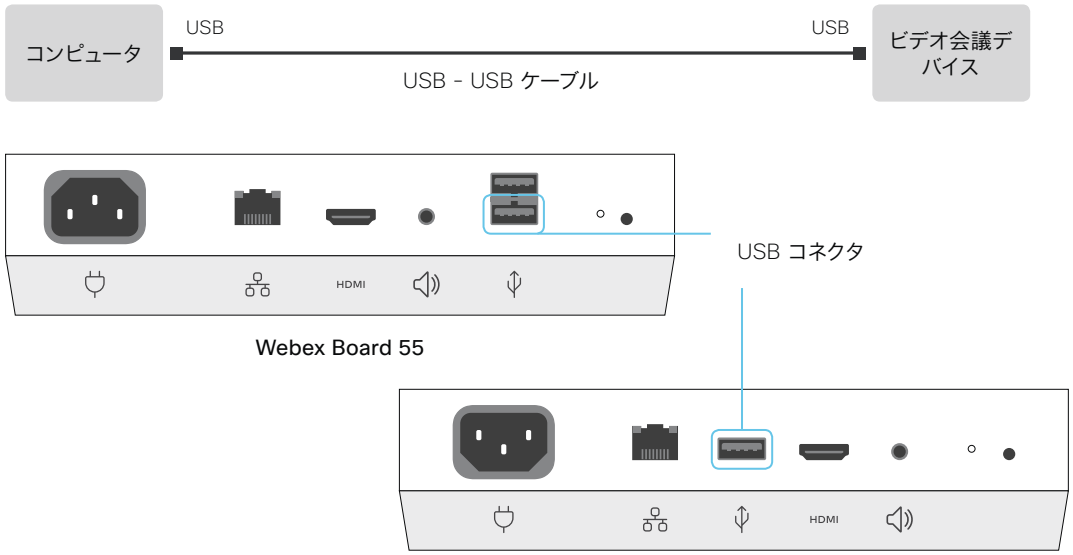
[シリアルポート (SerialPort)] > [モード (Mode)]

セキュリティ上の理由から，シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには，次の設定を使用します。

[シリアルポート (SerialPort)] > [ログインが必須 (LoginRequired)]

デバイスが CUCM によってプロビジョニングされている場合，シリアルポートの設定は CUCM から構成する必要があります。

[1] CP210x USB - UART ブリッジ仮想 COM ポート (VCP) ドライバが必要です。▶ https://jp.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers を参照してください。



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。

TCP ポートの開放

コーデック内のウェブ サーバでは, 非セキュアまたは不必要なポート, プロトコル, モジュール, またはサービスの使用が禁止または制限されています。いくつかのポートは, デフォルトで開放されているか, 閉じられています。

TCP 22 : SSH

SSH モード設定を [オフ (Off)] にすることで, ポートを閉じることができます。

```
NetworkServices SSH Mode: Off/On
```

TCP 80 : HTTP

HTTP モードを [オフ (Off)] にするか, [HTTPS (HTTPS)] にすることで, ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

TCP 443 : HTTP

HTTP モード設定を [オフ (Off)] にすることで, ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

TCP 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, タッチ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 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 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
```

デバイスの設定は, Web インターフェイスの [セットアップ (Setup)] > [設定 (Configuration)] ページから構成します。Web ブラウザを開き, デバイスの IP アドレスを入力して, サインインします。

TMS からの HTTPFeedback アドレス

デバイスが Cisco TelePresence Management Suite (TMS) に追加されると, TMS に情報 (イベント) を送り返すように自動的に設定されます。デバイスは, TMS からそれらのイベントに送信されるアドレス (HTTPFeedback アドレス) を受けとります。このアドレスが存在しないか, または正しく設定されていない場合, デバイスは TMS にイベントを送信できません。

失われたイベントへの応答

イベントへの応答がデバイスで受信されない場合, デバイスは最大 6 回, 間隔を増やしながら HTTPFeedback アドレスに送信を再試行します。

再試行してもデバイスで応答が受信されない場合, エンドポイントは 10 分ごとに HTTPFeedback アドレスにメッセージの送信を試行します。HTTPFeedback ステータスは, 失敗したことを示します。障害のタイプを示す診断メッセージがあります。

メッセージの再送を試みる際, TMS での通話詳細記録 (CDR) の紛失が生じます。

TMS からの新しい HTTPFeedback アドレスの取得

イベントを送信するための新しいアドレスを取得するには, デバイスを再起動して, TMS から (スケジュール設定または TMS 管理者によるトリガーで) 次の管理アドレスがプッシュされるのを待つ必要があります。

Cisco Webex クラウドサービスへのデバイスの登録

画面上のセットアップアシスタントを使用する代わりに, Web インターフェイスからリモートで Cisco Webex にデバイスを登録できます。

デバイスを登録するには, まずコントロールハブでアクティベーションコードを作成する必要があります。アクティベーションコードの作成方法については, ► 「場所の作成および Cisco Webex Room デバイスまたは Cisco Webex Board のサービスの追加」を参照してください。

Web インターフェイスから登録できるのは, 現在サービスに登録されていないデバイスのみです。

注 : このデバイスに作成したローカルユーザーとカスタマイズは, すべて非アクティブ化されます。

1. Web インターフェイスにサインインし, ホーム画面で [ここをクリックして Webex に登録 (Click here to register to Webex)] をクリックします。

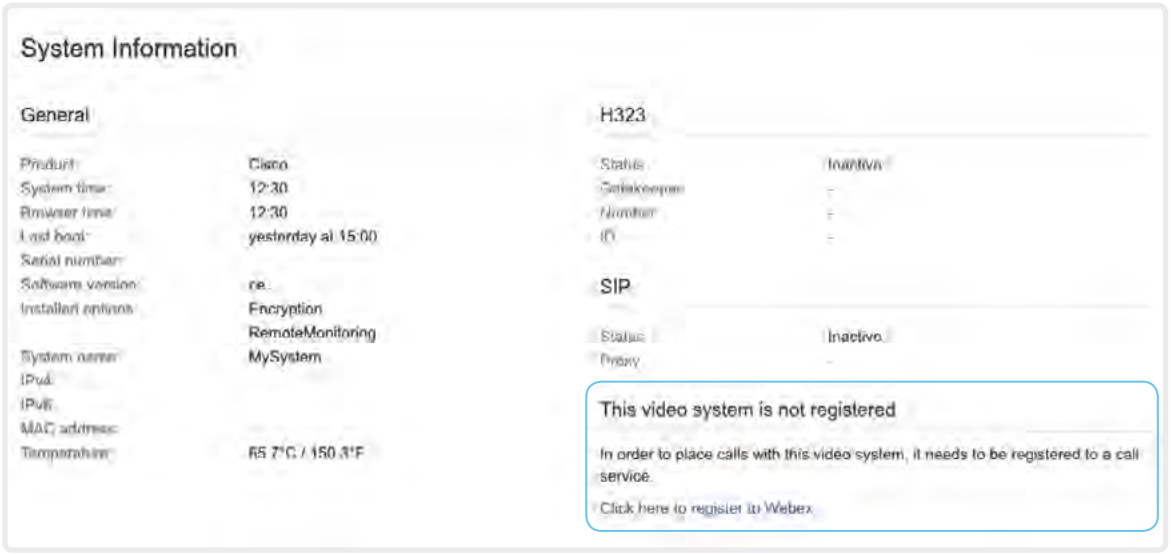
   このリンクは, デバイスがサービスにまだ登録されていない場合にのみ使用できます。

2. ポップアップが表示され, コントロールハブで作成したアクティベーションコードを入力することができます。

   形式:

   - *xxxx-xxxx-xxxx-xxxx*, または
   - *xxxxxxxxxxxxxxx*

3. 登録後に, 画面上のセットアップアシスタントからタイムゾーンと言語設定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』

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 X 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
- タッチスクリーンから Cisco Webex Board を直接制御, Cisco Webex Teams アプリを使用, または Cisco Touch 10 コントローラの使用

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, 50/60 Hz

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 Listed (無線機器)

Webex Board 55S, 70S, 85S :
- 適合規格 :
  - 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 (R)

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 http://www.ciscofax.com を参照してください。

すべての仕様は予告なしに変更される場合があります。システム仕様は異なる場合があります。

これらのドキュメントの画像はすべて説明目的でのみ使用され, 実際の製品とは異なる場合があります。

2019 年 6 月

Cisco ウェブ サイト内のユーザ ドキュメンテーション

次の短いリンクを使用して, CE ソフトウェアを実行する製品シリーズのマニュアルを検索します。

Room シリーズ:

► https://www.cisco.com/go/room-docs

MX シリーズ:

► https://www.cisco.com/go/mx-docs

SX シリーズ:

► https://www.cisco.com/go/sx-docs

DX シリーズ:

► https://www.cisco.com/go/dx-docs

Board:

► https://www.cisco.com/go/board-docs

通常, すべての Cisco Collaboration エンドポイントのユーザ マニュアルはこちらから検索できます。► https://www.cisco.com/go/telepresence/docs

マニュアルは以下のカテゴリに整理されています。一部のマニュアルはすべての製品で利用できません。

インストールとアップグレード > インストールとアップグレード ガイド

- *インストレーション ガイド:* 製品のインストール方法
- *スタートアップガイド:* デバイスを動作させるために必要な初期設定
- *RCSI ガイド:* 法規制の遵守および安全に関する情報

保守と運用 > メンテナンスとオペレーション ガイド

- *スタートアップガイド:* デバイスを動作させるために必要な初期設定
- *管理者ガイド:* 製品の管理に必要な情報
- *CUCM での TelePresence エンドポイントの導入ガイド:* Cisco Unified Communications Manager (CUCM) と組み合わせてデバイスの使用を開始する場合に実行するタスク
- *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

設計 > 設計ガイド

- *カスタマイズガイド:* ユーザー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オーディオセットアップの設定方法

設計 > 設計ガイド

- *ビデオ会議室に関するガイドライン:* 会議室の設計とベストプラクティスに関する一般的なガイドライン
- *ビデオ会議室のガイドライン:* 音質を向上させるための対策

ソフトウェア ダウンロード, リリースと一般情報 > ライセンス情報

- *オープン ソースのドキュメンテーション:* この製品で使用されるオープン ソース ソフトウェアのライセンスと通知

ソフトウェア ダウンロード、リリースと一般情報 > リリース ノート

- *ソフトウェア リリース ノート*

Cisco のお問い合わせ先

Cisco のウェブサイトでは, Cisco の世界各地のお問い合わせ先を確認できます。

参照先 : ► https://www.cisco.com/go/offices

本社
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

知的財産

Cisco 製品のセキュリティの概要

この製品には, 輸入, 輸出, 譲渡, 使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。シスコの暗号化製品を譲渡された第三者は, その暗号化技術の輸入, 輸出, 配布, および使用を許可されたわけではありません。輸入業者, 輸出業者, 販売業者, およびユーザは, 米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては, 関係法令の順守に同意したものとみなされます。米国および他の国の法律を順守できない場合は, 本製品を至急送り返してください。

米国の輸出規制の詳細については,
http://www.bis.doc.gov/policiesandregulations/ear/index.htm で参照できます。