

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 9.5
2018 年 9 月



管理者ガイド

Cisco Webex Room Kit用

シスコ製品をお選びいただきありがとうございます。

お使いのシスコ製品は、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 システム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感想があれば、ぜひお伝えください。

定期的にシスコの Web 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。

各種ユーザードキュメントは次の URL から入手できます。

▶ <https://www.cisco.com/go/roomkit-docs> [英語]

本ガイドの使用方法

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

目次

はじめに	4
ユーザドキュメンテーションとソフトウェア	5
CE9 の最新情報	6
Room Kit の概要	18
電源のオンとオフ	19
LED インジケータ	20
ビデオ システムの管理方法	21
設定	25
ユーザ管理	26
システム パスフレーズを変更する	27
[設定 (Settings)] メニューへのアクセスの制限	28
システム設定	29
サインイン バナーの追加	30
ウェルカムバナーの追加	31
ビデオ システムのサービス証明書を管理する	32
信頼できる認証局 (CA) のリストを管理する	33
セキュア監査ログギングのセットアップ	34
Expressway プロビジョニング経由の CUCM 用のブレインストール済み証明書の管理	35
CUCM 信頼リストを削除する	36
永続モードを変更する	37
強力なセキュリティ モードの設定	38
コンテンツ共有のために Intelligent Proximity をセットアップする	39
ビデオ品質の対コール レート比調整	44
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	46
カスタム壁紙の追加	48
着信音の選択と着信音量の設定	49
お気に入りリストの管理	50
アクセシビリティ機能のセットアップ	51
周辺機器	52
モニタの接続	53
入力ソースの接続	55
入力ソース数の拡大	57
ディスプレイについて	58
4K 解像度について	59
HDMI ケーブルについて	60

SpeakerTrack 機能のセットアップ	61	Security 設定	135
ホワイトボードへのスナップ機能の設定	62	SerialPort 設定	138
Touch 10 コントローラの接続	65	SIP 設定	139
ISDN リンクの接続	69	Standby 設定	143
メンテナンス	70	SystemUnit 設定	144
システム ソフトウェアのアップグレード	71	Time 設定	145
オプション キーを追加する	72	UserInterface 設定	148
システム ステータス	73	UserManagement 設定	151
診断の実行	74	Video 設定	153
ログ ファイルをダウンロードする	75	Experimental 設定	163
リモート サポート ユーザを作成する	76	付録	164
設定とカスタム要素のバックアップ/復元	77	Touch 10 の使用方法	165
カスタム要素の CUCM プロビジョニング	78	リモート モニタリングのセットアップ	166
カスタム要素の TMS プロビジョニング	79	Web インターフェイスを使用したコール情報へのアクセスとコール応答	167
以前に使用していたソフトウェア イメージに復元する	80	Web インターフェイスを使用してコールを発信する	168
ビデオ システムの工場出荷時設定リセット	81	Web インターフェイスを使用してコンテンツを共有する	170
Cisco Touch 10 の初期設定へのリセット	84	ローカル レイアウトの制御	171
Cisco TelePresence Touch 10 の初期設定へのリセット	85	ローカル カメラの制御	172
ユーザ インターフェイスのスクリーンショットをキャプチャする	86	相手先カメラの制御	173
システム設定	87	パケット損失の復元力: ClearPath	174
システム設定の概要	88	ルーム分析	175
Audio 設定	93	ビデオ システムの Touch 10 ユーザ インターフェイス	176
CallHistory 設定	97	マクロを使用したビデオ システムの動作のカスタマイズ	178
Cameras 設定	98	入力ソースの構成	179
Conference 設定	100	プレゼンテーションソースの構成	181
FacilityService 設定	105	スタートアップ スクリプトを管理する	183
H323 設定	106	ビデオ システムの XML ファイルにアクセスする	184
Logging 設定	109	Web インターフェイスからの API コマンドとコンフィギュレーションの実行	185
Macros 設定	110	コネクタ パネル	186
Network 設定	111	メンテナンス用のシリアル インターフェイス	187
NetworkServices 設定	118	TCP ポートの開放	188
Peripherals 設定	125	TMS からの新しい HTTPFeedback アドレスの取得	189
Phonebook 設定	127	技術仕様	190
Provisioning 設定	128	サポートされている RFC	192
Proximity 設定	131	シスコ Web サイト内のユーザ ドキュメンテーション	193
RoomAnalytics 設定	132	シスコのお問い合わせ先	194
RoomReset 設定	133		
RTP 設定	134		

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 Room Kit

ユーザドキュメンテーション

このガイドでは、ビデオ システム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ビデオ システム(CUCM、VCS)の機能と設定について説明していますが、クラウド サービス(Cisco Webex)登録のデバイスにも、その機能と設定の一部が適用されます。

この製品に関する詳しいガイドは、付録

▶ 「シスコ Web サイト内のユーザ マニュアル」を参照してください。

シスコ Web サイト内のドキュメンテーション

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

▶ <https://www.cisco.com/go/roomkit-docs> [英語]

クラウド登録デバイスのドキュメンテーション

Cisco Webex Room デバイスの詳細については、次のリンク先を参照してください。

▶ <https://collaborationhelp.cisco.com> [英語]

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 Web サイト [英語] をご覧ください。

▶ <https://www.cisco.com/go/projectworkplace> [英語]

Software

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

▶ <https://software.cisco.com/download/home>

ソフトウェア リリース ノート(CE9)を参照することをお勧めします。

▶ <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html> [英語]

CE9 の最新情報

この章では、CE9.0 と比較した、シスコ 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.x(CE9.x)の新規および変更されたシステム設定の概要と、新機能および改善点を説明しています。

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

▶ <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html> [英語]

CE9.5 の新機能および改善点

プレゼンテーションソースの構成

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

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

ソースの最大利用可能数は、使用するデバイスによって異なります。

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

ケーブル経由で共有されているコンテンツのみ構成に組み込むことができます。

韓国語キーボードのサポート

ユーザーインターフェイス言語が韓国語に設定されている場合、韓国語キーボードでの入力が必要で Touch 10 でサポートされます。

ウェルカムバナー

ビデオシステムの Web インターフェイスまたはコマンドライン インターフェイスに、ユーザーがログイン後に表示されるウェルカムバナーを設定できます。バナーには作業開始に必要な情報や、システムのセットアップ時に注意しなければならないことなどが含まれています。

CE9.4 の新機能および改善点

Cisco Spark から Cisco Webex へのリブランディング

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

以下の製品は、新たな名称を得ます。

- Cisco Spark Room Kit は Cisco Webex Room Kit へ
- Cisco Spark Room Kit Plus は Cisco Webex Room Kit Plus へ
- Cisco Spark Codec Plus は Cisco Webex Codec Plus へ
- Cisco Spark Quad Camera は Cisco Quad Camera へ
- Cisco Spark Room 55 は Cisco Webex Room 55 へ
- Cisco Spark Room 70 は Cisco Webex Room 70 へ
- Cisco DX70 は Cisco Webex DX70 へ
- Cisco DX80 は Cisco Webex DX80 へ

プロキシミティクライアントの最大数が増加しました

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

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

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

特定のケースでのみこれがサポートされます。

- Room Series デバイスと MXP デバイス間の H.323 ダイレクト発信 (IP ダイヤラ)。
- H.323 上の VCS に登録された MXP および SIP または H.323 どちらかで同一の VCS 上に登録された Room Series デバイス。VCS 上において H.323 で SIP 発信を行うには、インターワーキングオプションキーが VCS 上にインストールされている必要があることにご留意ください。

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

管理設定ロックダウン構成の CUCM プロビジョニング

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

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

デフォルトの HTTP モードを HTTP + HTTPS から HTTPS へ変更

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

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

室内制御の更新

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

CE9.3 の新機能および改善点

設定とカスタム要素のバックアップ/復元

バックアップ ファイル バンドル(zip)には、設定とともにカスタム要素を含めることができます。次の要素からバンドルに含めるものを選択できます。

- ・ ブランディング イメージ
- ・ マクロ
- ・ お気に入り
- ・ サインイン バナー
- ・ 室内制御パネル
- ・ 設定(すべてまたは一部)

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

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

バックアップと復元機能は、ビデオ システムの Web インターフェイスの [メンテナンス(Maintenance)] > [バックアップと復元(Backup and Restore)] の下にあります。

カスタム要素のプロビジョニング

前述のように、バックアップ バンドルは、Cisco UCM または TMS を使用して多数のビデオ システムにプロビジョニングできます。複数のビデオ システム用のバックアップ バンドルを作成するときは、デバイス固有の情報を削除することが重要です。そのようなバンドルにデバイス固有の情報が含まれていると、結果的に複数のビデオ システムに到達できなくなる可能性があります。

システム固有ではないバックアップ バンドルをプロビジョニングすることにより、たとえば、ビデオ システムのセットアップをマクロ、ブランディング要素、および室内制御パネルとともに複数のビデオ システムにコピーすることができます。

現時点では、Cisco UCM によるプロビジョニングでは設定は復元されず、その他のカスタム要素のみが復元されます。TMS では、バックアップ バンドルに含まれるすべてのものが復元されます。

プロビジョニングの詳細については、リリース ノートを参照してください。

室内制御の更新

室内制御機能には次の機能が追加されています。

- ・ 合計で最大 20 のパネルにボタンを追加できます。ボタンは、パネルの種類に応じてユーザ インターフェイスのホーム スクリーンまたは通話中スクリーンに表示されます。
- ・ これまでのように、グローバル パネル(常に利用可能)、通話中パネル(通話中にのみ利用可能)、非通話中パネル(通話中でない場合にのみ利用可能)の 3 種類の室内制御パネルがあります。グローバル パネルのエントリ ポイントは、ステータス バー(ユーザ インターフェイスの右上隅)から削除されました。代わりに、グローバル パネルを開くボタンがホーム スクリーンと通話中スクリーンの両方に(それぞれ、非通話中専用パネル用ボタンおよび通話中専用パネル用ボタンとともに)追加されています。
- ・ ユーザ インターフェイスでパネルを開かずにイベントを直接トリガーできるスタンドアロンのトリガー ボタンを作成できます。

また、室内制御エディタに次の機能が追加されました。

- ・ いくつかの新しいアイコンを利用できます。
- ・ 一連の色から室内制御ボタンの色を選択できます。
- ・ テキスト要素をダブルクリックしてテキストを直接編集できます。
- ・ 室内制御 XML ファイルをエディタにドラッグ アンドドロップできます。

室内制御の詳細については、▶ <https://www.cisco.com/go/in-room-control-docs> にある室内制御のガイド/カスタマイズガイド [英語] を参照してください。

ISDN リンクのサポート

ソフトウェアバージョン IL1.1.7 では ISDN リンクが、CE9.3.0 をサポートするすべてのビデオ システムでサポートされます。

これまでのように、自動ペアリング(ビデオ システムによる ISDN リンクの自動検出を可能にする)を使用する場合は、ビデオ システムで IPv6 を有効にする必要があります。

ワンボタン機能(OBTP)のスヌーズ

ワンボタン機能(OBTP)ミーティング アラームで 5 分間のスヌーズが可能です。スヌーズの時間は変更できません。このアラームは、通常、通話中に、スケジュールされた会議が開始間近になると表示されます。会議が終了するまでは、表示されるたびにアラームを 5 分間スヌーズできます。

発信前のコール レートの調整

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

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

着信音の選択と着信音の音量の調整

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

延期されたアップグレードの再開

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

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

システム情報がユーザ インターフェイスに公開されることの防止

重要なシステム情報がユーザ インターフェイスに公開されることを防止できます。たとえば、次の情報の公開を防止できます。

- ・ IP アドレス(ビデオ システム、タッチ コントローラ、UCM/VCS レジストラ)
- ・ MAC アドレス
- ・ Serial number
- ・ ソフトウェア バージョン

この機能を有効にするには、次の操作が必要です。

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

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

アクセシビリティ:着信時のスクリーンの点滅

システムが着信コールを受信するとスクリーンとタッチ コントローラが赤色/薄灰色で点滅するようにビデオ システムを設定できます。これは主に聴覚に障がいのあるユーザ向けの機能で、着信に気付くことが容易になります。

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

1 冊の共通 API ガイド

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

CE9.2 の新機能および改善点

マクロ フレームワーク

マクロ フレームワークにより、ユーザとインテグレータは、JavaScript マクロを作成できます。これにより、シナリオを自動化し、エンドポイントの動作をカスタマイズして、個々のお客様の要件に適合させることができます。

マクロと、イベント/ステータス変更のリスニング、コマンド/設定の実行の自動化、室内制御機能用のローカル制御機能の提供などの強力な機能の組み合わせにより、さまざまなカスタム セットアップが可能になっています。

ビデオ システムを無期限に応答不可にするといったマイナーな動作の変更は、マクロで簡単に実現できます。その他の例としては、設定の自動リセット、特定の時刻の発信、状態の変化に応じたアラート/ヘルプ メッセージの発行などがあります。

複数のサンプル マクロも提供するマクロ エディタは、ビデオ システムの Web インターフェイスから利用できます。

ブランディングとハーフウェイクのカスタマイズ

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

ハーフウェイク状態では、次のことができます。

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

アウェイク状態では、次のことができます。

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

ソース構成

最大 4 つの入力ソース(コーデックで利用できる入力ソースの数によって異なる)で 1 つのイメージを構成できます。このイメージが、メイン ビデオ ストリームでコールの遠端に送信されます。ソース構成は API 経由でのみ有効にできるので、ユーザインターフェイス拡張をマクロと組み合わせて作成し、オンデマンドで構成を制御することをお勧めします。

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

HTTP プロキシのサポート

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

ユーザ インターフェイスの機能

- ・ 設定パネルが再構成されています。
- ・ ビデオ システムの管理者パスワードによって、ユーザ インターフェイス(Touch 10)の設定パネルを保護することができます。パスワードが空白の場合、誰でも設定にアクセスしてシステムを初期設定にリセットすることができます。
- ・ ユーザ インターフェイスでロシア語を選択する場合は、ロシア語のキーボードとラテン文字セットのキーボードを選択できます。
- ・ アラビア語とヘブライ語がユーザ インターフェイスに追加されました。また、ローカライズされたキーボードも含まれます。
- ・ 基本的な IEEE 802.1x 設定がユーザ インターフェイスの設定パネルに追加されています。

「ホワイトボードへのスナップ」機能のサポート

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

ホワイトボードの近くで話している人をビデオ システムが検出すると、カメラのビューがホワイトボード領域に切り替わり、Touch 10 ユーザ インターフェイスの設定パネルのウィザードを使用すると、簡単に機能をセットアップして、ホワイトボード領域の場所を定義できます。

USB -シリアル ポートのサポート

USB(Type-A)-シリアル(D-sub 9)アダプタを接続してビデオ システム API にアクセスすることができます。UC232R-10 USB - RS232(FTDI)アダプタを使用することをお勧めします。

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

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

ソフトウェア バージョン CE9.2 を実行しているビデオ システムでは、ミュートが直接解除されません。そのようなビデオ システムのミュートをリモートで解除しようとすると、音声のミュートをローカルで解除することを求めるメッセージがスクリーンに表示されます。

カスタム入力プロンプトの API コマンドAPI

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

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

API 経由での証明書のアップロード

ASCII PEM 形式の証明書は、複数の API コマンド(`xCommand Security Certificates CA Add` または `xCommand Security Certificates Services Add`)を使用して直接インストールできます。これまでのように、証明書を Web インターフェイスからビデオ システムにアップロードすることもできます。

ユーザ管理用 API コマンド

API コマンド(`xCommand UserManagement User *`)を使用して ユーザ アカウントを直接作成し、管理することができます。これまでのように、これをビデオ システムのユーザ インターフェイスから行うこともできます。

室内制御のプレビュー モード

室内制御エディタには、新しいプレビュー モードがあります。仮想 Touch 10 ユーザ インターフェイスでは、デザインがユーザ インターフェイスでどのように見えるかを確認できます。ユーザ インターフェイスはインタラクティブであるため、機能をテストできます。これにより、サードパーティの制御システムやマクロで作成した機能をトリガーできる実際のイベントがビデオ システムで生成されます。右側のペインのコンソールには、対話操作時のウィジェットの値と、制御システムのフィードバック メッセージが表示されます。

インテリジェント プロキシミティの変更点

Cisco Proximity によって 1 つ以上のクライアントがシステムとペアになっていることを知らせるプロキシミティ インジケータがスクリーン(右中央)に表示されます。プロキシミティが有効になっているときに常に表示されていた古いインジケータ(左上)は削除されました。

プロキシミティ サービスをユーザ インターフェイスから無効にすることはできなくなりました。

超音波設定は [周辺機器ペアリング超音波(Peripherals Pairing Ultrasound)] から [音声超音波(Audio Ultrasound)] に移行されました。

コール サービスを変更する際の初期設定への自動リセット(デバイスの有効化)

ユーザ インターフェイスからデバイス アクティブ化方法が変更されると(たとえば VCS から Cisco UCM への変更)、ビデオ システムは自動的に初期設定にリセットして再起動します。これにより、新しいサービス向けにビデオ システムをプロビジョニングするときに設定の競合が防止されます。

API からプロビジョニングを変更した場合、ビデオ システムの初期設定リセットは自動的に行われません。

音声とその他のメディアで別個の RTP ポート範囲のサポート

音声とその他のメディアでそれぞれ異なる RTP ポート範囲が使用されるように、ビデオ システムを設定できます。この 2 つの範囲を重複させることはできません。デフォルトでは、すべてのメディアが同じ RTP ポート範囲を使用します。

CE9.1 の新機能および改善点

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

デュアル スクリーンのビデオ システムでは、両方のスクリーンを CMS ベースの会議に利用できます。ビデオ システムは、2 つのトランスコードされたビデオ ストリームと 1 つのコンテンツ ストリームを CMS から受信し、両方の画面を使用してこれらのストリームをレンダリングします。

アクティブ コントロールが有効な場合、ミーティング参加者全員と各参加者の現在のアクティビティ ステータス(ミュート、共有、アクティブ スピーカー インジケータなど)を示す参加者リストが得られます。タッチ インターフェイスからレイアウト選択パネルを使用してレイアウトをスムーズに変更できます。

新しいウェイクアップ エクスペリエンス

ウェイクアップエクスペリエンスには、ハーフウェイクとモーション検知スタンバイの 2 つの追加のスタンバイ状態があります。自動ウェイクアップが有効になっている場合、ビデオ システムは、超音波を使用してプレゼンスを検出(モーション検知)するか、Cisco Proximity クライアントとペアになるとプレゼンスを検出します。ビデオ システムは、ハーフウェイク状態になる前(簡単なインタラクティブ操作のガイドがスクリーンに表示されている)はグリーティングによってウェイクアップします。

ワイヤレス ネットワーク用の EAP 認証フレームワークのサポート

WPA-PSK と WPA2-PSK に加えて、ビデオ システムは Wi-Fi 接続用の WPA-EAP 認証フレームワークをサポートするようになりました。サポートされているすべての方式は次のとおりです。

- Open
- WPA-PSK(AES)
- WPA2-PSK(AES)
- EAP-TLS
- EAP-TTLS
- EAP-FAST
- PEAP
- EAP-MSCHAPv2
- EAP-GTC

ルーム分析の追加

室内の人の存在を検知: ビデオ システムは、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。この機能は、超音波に基づいています。室内に誰がいたかは記録として保持されず、部屋が使用中であるかどうかだけを検知します。

人数のカウント: 通話中、およびセルフビュー画像の表示中に、ビデオシステムは室内にいる人の数をカウントします。非通話中の人数を数えるようにビデオ システムを設定することもできますが、ビデオ システムはスタンバイ時には人数を数えることができません。室内にいた人物の記録を保持することではなく、顔の数だけを検知します。

CE9.5 でのシステム設定の変更点

新しい設定

NetworkServices SSH HostKeyAlgorithm

削除された設定

[なし]

変更された設定

なし

CE9.4 でのシステム設定の変更点

新しい設定

Conference FarendMessage Mode

SIP MinimumTLSVersion

削除されたコンフィギュレーション

NetworkServices HTTP Proxy Allowed

変更されたコンフィギュレーション

Audio Output Line [1] OutputType

旧: デフォルト値: LineOut

旧: 設定可能な値: LineOut/Subwoofer

新: デフォルト値: Loudspeaker

新: 設定可能な値: LineOut/Loudspeaker/Recorder/Subwoofer

Network [1] DNS DNSSEC Mode

旧: ユーザ ロール: ADMIN, USER

新: ユーザ ロール: ADMIN

Network [1] Speed

旧: ユーザ ロール: ADMIN, USER

新: ユーザ ロール: ADMIN, INTEGRATOR

NetworkServices HTTP Mode

旧: デフォルト値: HTTP+HTTPS

新: デフォルト値: HTTPS

NetworkServices SNMP CommunityName

旧: ユーザ ロール: ADMIN

新: ユーザ ロール: ADMIN, INTEGRATOR

NetworkServices SNMP Host [1..3] Address

旧: ユーザ ロール: ADMIN

新: ユーザ ロール: ADMIN, INTEGRATOR

NetworkServices SNMP Mode

旧: ユーザ ロール: ADMIN

新: ユーザ ロール: ADMIN, INTEGRATOR

NetworkServices SNMP SystemContact

旧: ユーザ ロール: ADMIN

新: ユーザ ロール: ADMIN, INTEGRATOR

NetworkServices SNMP SystemLocation

旧: ユーザ ロール: ADMIN

新: ユーザ ロール: ADMIN, INTEGRATOR

CE9.3 でのシステム設定の変更点

新しい設定

Audio KeyClickDetector Attenuate
Audio KeyClickDetector Enabled
Network [1] DNS DNSSEC Mode
NetworkServices HTTP Proxy PACUrl
SystemUnit CrashReporting Advanced
SystemUnit CrashReporting Mode
SystemUnit CrashReporting URL
UserInterface Accessibility IncomingCallNotification
UserInterface Security Mode

削除されたコンフィギュレーション

Provisioning HttpMethod

変更されたコンフィギュレーション

NetworkServices HTTP Proxy Allowed
旧: デフォルト値: True
新: デフォルト値: False
NetworkServices HTTP Proxy Mode
旧: 設定可能な値: Manual/Off
新: 設定可能な値: Manual/Off/PACUrl/WPAD
Security Session MaxSessionsPerUser
旧: 設定可能な値: 整数(0 ~ 100) デフォルト値: 0
新: 設定可能な値: 整数(1 ~ 20) デフォルト値: 20
Security Session MaxTotalSessions
旧: 設定可能な値: 整数(0 ~ 100) デフォルト値: 0
新: 設定可能な値: 整数(1 ~ 20) デフォルト値: 20

CE9.2 でのシステム設定の変更点

新しい設定

Audio Input HDMI[n] VideoAssociation MuteOnInactiveVideo
Audio Ultrasound MaxVolume
Replacing Peripherals Pairing Ultrasound Volume MaxLevel
Audio Ultrasound Mode
Replacing Peripherals Pairing Ultrasound Volume Model
Cameras SpeakerTrack Whiteboard Mode
Macros AutoStart
Macros Mode
NetworkServices HTTP Proxy Allowed
NetworkServices HTTP Proxy LoginName
NetworkServices HTTP Proxy Mode
NetworkServices HTTP Proxy Password
NetworkServices HTTP Proxy Url
RTP Video Ports Range Start
RTP Video Ports Range Stop
Security Session FailedLoginsLockoutTime
Security Session MaxFailedLogins
UserInterface CustomMessage
UserInterface OSD HalfwakeMessage
UserInterface SettingsMenu Mode

削除されたコンフィギュレーション

Peripherals Pairing Ultrasound Volume MaxLevel
Replaced by Audio Ultrasound MaxVolume
Peripherals Pairing Ultrasound Volume Mode
Replaced by Audio Ultrasound Mode

変更されたコンフィギュレーション

Audio Input Microphone[n] Level
旧: 値スペース: 0 ~ 36
新: 値スペース: 0 ~ 26
Cameras SpeakerTrack Closeup
旧: ユーザ ロール: Admin、INTEGRATOR
新: ユーザ ロール: ADMIN、INTEGRATOR、USER
Security Audit Logging Mode
旧: デフォルト値: Off
新: デフォルト値: Internal(内部)
UserInterface Language
新: 設定可能な言語にアラビア語とヘブライ語を追加
UserInterface OSD Output
旧: デフォルト値: 1
新: デフォルト値: Auto
Video Selfview OnCall Mode
旧: デフォルト値: Off
新: デフォルト値: On

CE9.1 でのシステム設定の変更点

新しい設定

Cameras Camera Framerate

RoomAnalytics PeopleCountOutOfCall

RoomAnalytics PeoplePresenceDetector

Video Input Connector [n] CEC Mode

削除された設定

[なし]

変更された設定

Conference DefaultCall Rate

旧: デフォルト値: 3072

新: デフォルト値: 6000

Conference MultiStream Mode

旧: 値スペース: Off デフォルト値: Off

新: 値スペース: Auto/Off デフォルト値: Auto

Network[1] IEEE8021X Password

旧: 設定可能な値: String(0, 32)

新: 設定可能な値: String(0, 50)

Peripherals Profile TouchPanels

旧: デフォルト値: NotSet

新: デフォルト値: Minimum1

Standby WakeupOnMotionDetection

旧: デフォルト値: Off

新: デフォルト値: On

Video Input Connector [n] PresentationSelection

旧: 値スペース: AutoShare/Manual/OnConnect

新: 設定可能な値: AutoShare/Desktop/Manual/OnConnect

Video Output Connector [1..2] MonitorRole

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

新: デフォルト値: Auto

Room Kit の概要

Cisco Webex Room Kit では、カメラ、コーデック、スピーカー、およびマイクが単一のデバイスに統合されています。簡単に設置でき、HDMI CEC によってフラット パネル ディスプレイとの優れた統合が実現されます。

この Room Kit は、小規模および中規模のミーティング ルームやチーム コラボレーション ルーム向けに設計されています。以前はハイエンドのビデオ会議室の領域であった洗練された機能が、あらゆる部屋とあらゆるチームに提供されます。

この Room Kit は、クラウド(Cisco Webex)とオンプレミス(CUCM および VCS)の両方で展開できるように構築されています。

機能とメリット

- ・ インテリジェントな表示機能を備えた目立たない内蔵カメラ: 会議出席者を検知し、ベスト オーバービューを表示し、アクティブなスピーカーを検出して切り替えます(スピーカー トラッキング)。
- ・ 内蔵されたマイクとスピーカーによって優れたオーディオ エクスペリエンスが提供されます。
- ・ 自動ウェイクアップ機能: 人が室内に入ると検知します。モバイル デバイスによって人を認識することもできます。
- ・ Cisco Touch 10 または Cisco Webex アプリ対応デバイスによる制御
- ・ ビデオとコンテンツの 2 つのディスプレイのサポート
- ・ ローカル会議での 2 つのコンテンツ ソースのプレゼンテーション
- ・ 4K コンテンツ共有(ローカル会議では 30 fps、遠端では 5 fps)
- ・ 有線またはワイヤレスでのコンテンツ シェアリング
- ・ 室内の人数のカウント: 優れたリソース プランニングのための分析を可能にします。
- ・ イーサネットと Wi-Fi のサポート
- ・ Cisco Touch 10 による照明やブラインドなどの周辺機器の制御(室内制御)

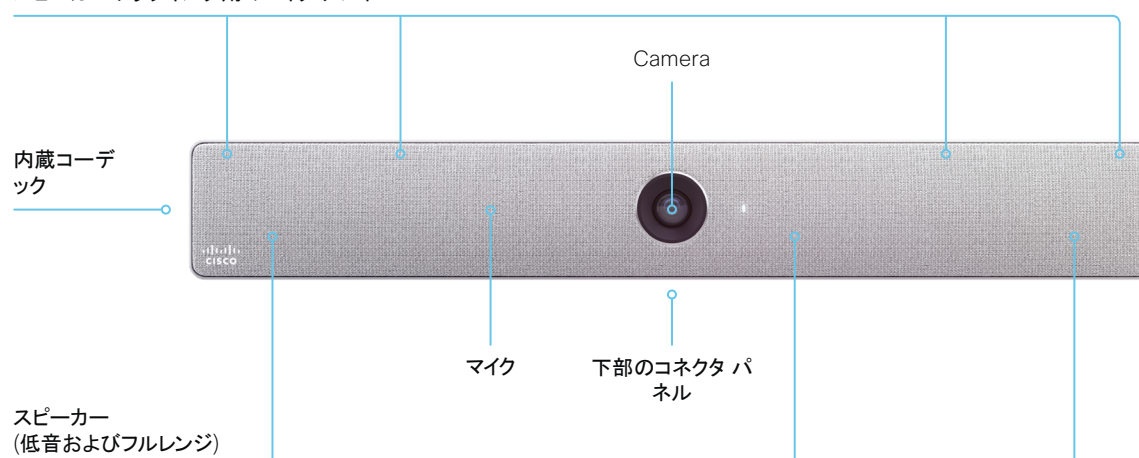
Cisco Webex Room Kit の詳細については、

▶ <https://www.cisco.com/go/roomkit> [英語] を参照してください。



標準フラットパネル ディスプレイの上部に
設置された Room Kit

スピーカー トラッキング用のマイク アレイ



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

システムを再起動します。

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. [\[設定 \(Settings\)\]](#)、[\[再起動 \(Restart\)\]](#) の順に選択します。
3. [\[再起動 \(Restart\)\]](#) を再度選択して、選択内容を確認します。

スタンバイ モードの開始/終了

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. [\[スタンバイ \(Standby\)\]](#) を選択します。

リモートからシステムの電源をオフにするか再起動する

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

システムを再起動します。

[\[デバイスの再起動... \(Restart device...\)\]](#) をクリックします。

システムが使用可能になるまでに、数分かかります。

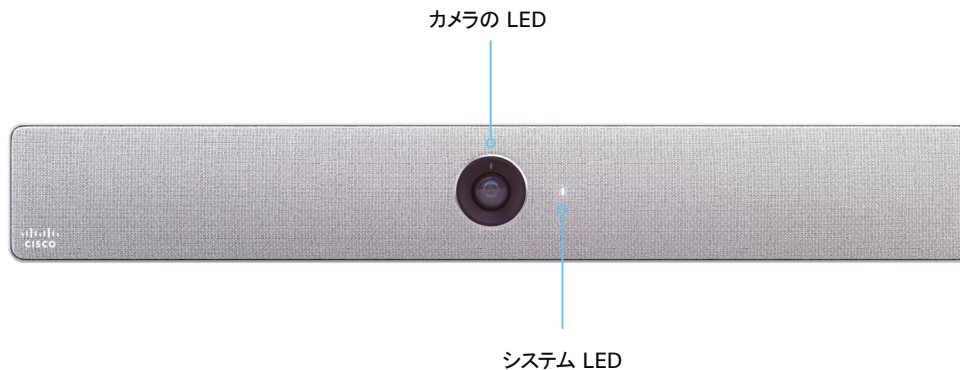
システムの電源をオフにする

[\[デバイスのシャットダウン... \(Shutdown device...\)\]](#) をクリックします。



システムの電源をリモートで再度オンにすることはできません。
システムの電源を入れるには、電源プラグを抜いてから再度接続する必要があります。

LED インジケータ



システム LED

アイドル モード時(スクリーンはアウェイク):

点灯状態になります。

スタンバイ モード時(スクリーンはオフ):

点灯状態になります。

スリープ モード時(低電力モード):

LED がゆっくり点滅します。

要注意時(ネットワーク接続がないなど):

LED が 2 回ずつ、繰り返し点滅します。

スタートアップ(起動)時:

LED が点滅します。システムが使用可能になると点灯状態になります。

カメラの LED

コールの着信時:

LED が点滅します。

コール中:

点灯状態になります。

セルフビュー オン時:

点灯状態になります。

ビデオ システムの管理方法 (1/4 ページ)

一般的には、このアドミニストレータ ガイドに記載されているように、Web インターフェイスを使用してビデオ システムを管理/保守することをお勧めします。

次のような方法でもビデオ システムの API にアクセスできます。

- HTTP または HTTPS(Web インターフェイスでも使用される)
- SSH
- シリアル インターフェイス(RS-232)

別のアクセス方法、および API の使用方法の詳細については、ビデオ システムのAPI ガイドを参照してください。

Tip

設定またはステータスが API で使用可能な場合、Web 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)`

(Web で)`X > Y > Z` ステータスにチェックマークを付けることは

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

は、以下と同じです。

`xStatus SystemUnit Software Version`

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

アクセス方式	注	方式の有効化/無効化方法
HTTP/HTTPS	- ビデオ システムの Web インターフェイスで使用 - 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、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状態で提供されるビデオシステムのみ、デフォルトで有効となります。	[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、ビデオ システムを再起動します。
SSH	- セキュアな TCP/IP 接続 - デフォルトでイネーブルになっている。	[ネットワークサービス(NetworkServices)] > [SSH] > [モード(Mode)] ビデオ システム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 インターフェイス(RS-232)	- ケーブルを使用してビデオ システムに接続IP アドレス、DNS、ネットワークは不要。 - デフォルトでイネーブルになっている。 - セキュリティ上の理由から、デフォルトではサインインするよう求められます([シリアル ポート(SerialPort)] > [ログインが必須(LoginRequired)])	[シリアルポート(SerialPort)] > [モード(Mode)] 変更を有効にするには、ビデオ システムを再起動します。



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、ビデオ システム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、復元するにはビデオ システム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 システムの管理方法 (2/4 ページ)

ビデオ システムの Web インターフェイス

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

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

Web ブラウザは最新版を使用することを推奨します。

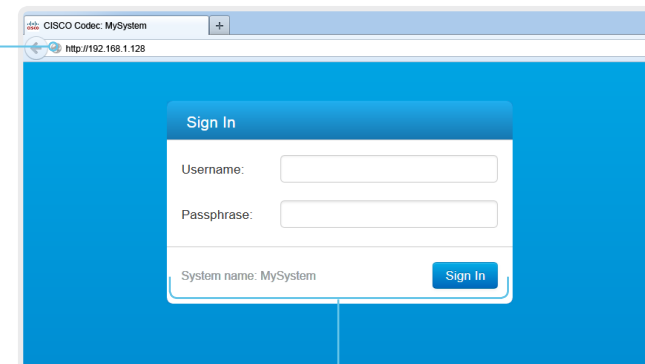
ビデオ システムへの接続

Web ブラウザを開き、ビデオ システムの IP アドレスをアドレス バーに入力します。



IP アドレスの確認方法

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
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。



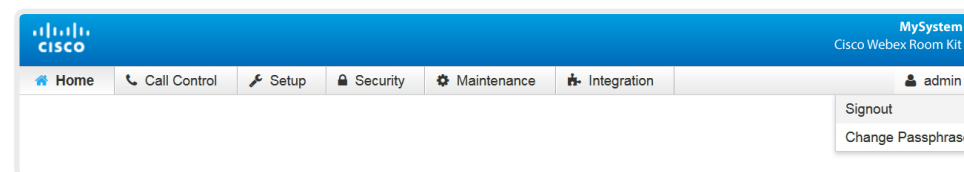
サインイン

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。



システムには、パスフレーズなしの *admin* というデフォルトのユーザが提供されています。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 システムの管理方法 (3/4 ページ)

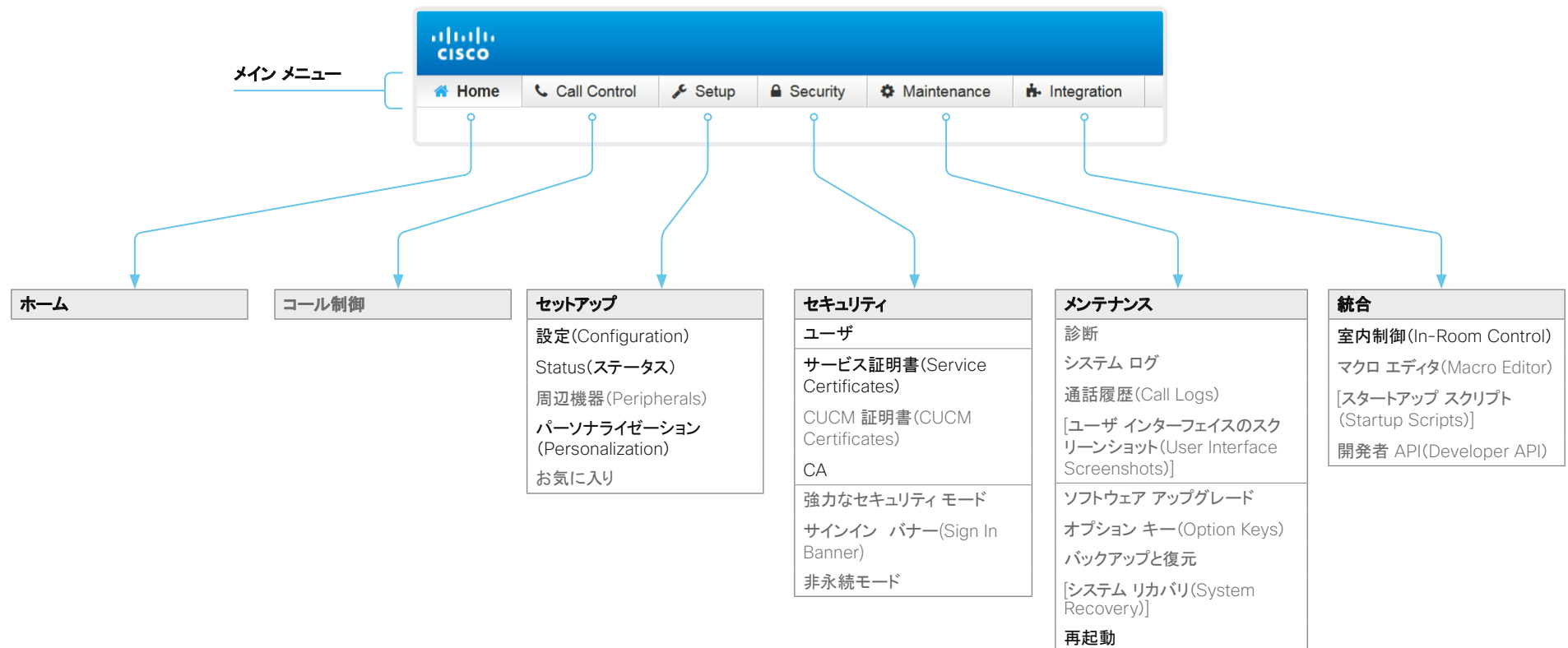
Web インターフェイスの構成

Web 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。ビデオ システムがオンプレミス サービス(CUCM、VCS)に登録されているときは下に示すすべてのサブページを使用できます。ビデオ システムがシスコのクラウド サービス(Cisco Webex)に登録されているとき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。



ビデオ システムの管理方法 (4/4 ページ)

ユーザ インターフェイスの設定とシステム情報

ビデオ システムのユーザ インターフェイスでシステム情報と一部の基本設定およびシステム テストにアクセスできます。

システム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、パスワードで保護できます。▶ [「\[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、ビデオ システム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システムの『スタートアップガイド』を参照してください。

Access Settings

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. [\[設定 \(Settings\)\]](#) を選択します。

南京錠の記号  は、設定が保護されている(ロックされている)ことを示しています。

3. 変更する設定または実行するテストを選択します。

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

第 2 章

設定

ユーザ管理

Web インターフェイスとコマンドライン 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

ビデオ システムには、フル アクセス権が与えられたデフォルトの管理者ユーザ アカウントが付属しています。ユーザ名は *admin* で、パスワードは初期状態では設定されていません。



必ず *admin* ユーザのパスワードを設定する必要があります。

パスワードの設定方法については、▶ [「システム パスワードの変更」](#)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て、[\[セキュリティ\(Security\)\]](#) > [\[ユーザ\(Users\)\]](#) に移動します。
2. [\[新規ユーザを追加\(Add New User\)\]](#) を選択します。

3. [\[ユーザ名\(Username\)\]](#)、[\[パスワード\(Passphrase\)\]](#)、[\[パスワードの確認\(Repeat passphrase\)\]](#) 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ワード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、[\[自分のパスワード\(Your passphrase\)\]](#) 入力フィールドに自分自身のパスワード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、[\[パスワード\(Your passphrase\)\]](#) 入力フィールドに確認のため各自のパスワードを入力する必要があります。

ユーザ特権を変更する

1. Web インターフェイスにサインインして、[\[セキュリティ\(Security\)\]](#) > [\[ユーザ\(Users\)\]](#) に移動します。
2. リスト内の該当ユーザをクリックします。
3. ユーザ ロールを選択し、ステータスを [\[アクティブ\(Acitive\)\]](#) 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ワード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。

パスワードを変更する

1. Web インターフェイスにサインインして、[\[セキュリティ\(Security\)\]](#) > [\[ユーザ\(Users\)\]](#) に移動します。
2. リスト内の該当する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ワードを入力します。
4. [\[パスワードの変更\(Change Passphrase\)\]](#) をクリックして、変更を保存します。
変更を加えないで終了するには、[\[戻る\(Back\)\]](#) ボタンを使用します。

ユーザ アカウントを削除する

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

ユーザ ロール

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

これらはユーザ ロールです。

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

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

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

ROOMCONTROL: このロールを持つユーザは、室内制御を作成できます。ユーザは室内制御エディタおよび対応する開発ツールにアクセスできます。

INTEGRATOR: このロールを持つユーザは、高度な AV シナリオを設定し、ビデオ システムをサードパーティの機器と統合するために必要な設定、コマンド、およびステータスにアクセスできます。このユーザは、室内制御を作成することもできます。

Cisco Webex 登録済のシステム

ビデオ システム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、INTEGRATOR ユーザ ロールと ROOMCONTROL ユーザ ロールを持つローカル ユーザだけを利用できます。

システム パスフレーズを変更する

次の操作を行うには、システム パスフレーズを知っている必要があります。

- Web インターフェイスへのログイン
- コマンドライン インターフェイスへのログインと、その使用

デフォルトのユーザ アカウント

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



システム設定へのアクセスを制限するために、必ず、デフォルトの *admin* ユーザ用のパスフレーズを設定する必要があります。さらに、管理者権限を持つ他のすべてのユーザにもパスフレーズを設定する必要があります。

admin ユーザのパスフレーズが設定されるまでは、システム 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上に表示されます。

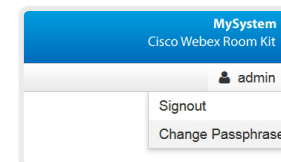
他のユーザ アカウント

ビデオ システムのユーザ アカウントを複数作成することができます。

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. Web 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\(Change Passphrase\)\]](#) 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て、[\[セキュリティ\(Security\)\]](#) > [\[ユーザ\(Users\)\]](#) に移動します。
2. リスト内の該当ユーザをクリックします。
3. 新しいパスフレーズを、[\[パスフレーズ\(Passphrase\)\]](#) および [\[パスフレーズの確認\(Repeat passphrase\)\]](#) 入力フィールドに入力します。
該当ユーザが *admin* ロールを持っている場合は、[\[自分のパスフレーズ\(Your passphrase\)\]](#) 入力フィールドに自分自身のパスフレーズを確認のために入力する必要があります。
4. [\[パスフレーズの変更\(Change Passphrase\)\]](#) をクリックして、変更を保存します。
変更を加えないで終了するには、[\[戻る\(Back\)\]](#) ボタンを使用します。

[設定(Settings)] メニューへのアクセスの制限

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

権限のないユーザがビデオ システム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お勧めします。

[設定(Settings)] メニューをロックする

1. Web 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。

これにより、ユーザは、ADMIN クレデンシャルでサインインしないとユーザ インターフェイス(タッチ コントローラ)でシステムの重要な設定にアクセスできなくなります。

[設定(Settings)] メニューのロック解除

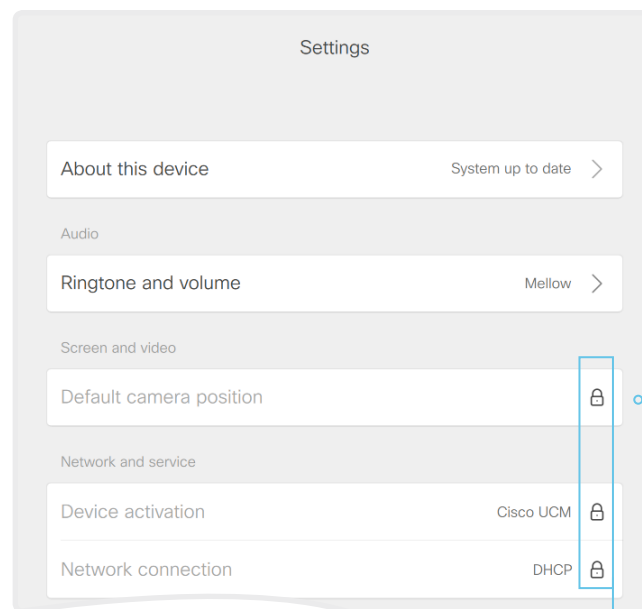
1. Web インターフェイスにサインインして、[セットアップ(Setup)] > [設定(Configuration)] に移動します。
2. [ユーザインターフェイス(UserInterface)] > [設定メニュー(SettingsMenu)] > [モード(Mode)] に移動して、[ロックなし(Unlocked)] を選択します。
3. [保存(Save)] をクリックして変更を有効にします。

これにより、任意のユーザが、ユーザインターフェイス(タッチ コントローラ)ですべての [設定(Settings)] メニュー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

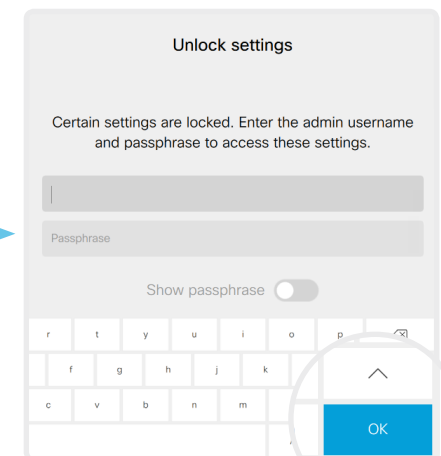
このメニューがロックされている場合は、サインインしないと、システムの重要な設定にアクセスできません。

[設定(Settings)] メニューを開くには、ユーザ インターフェイスの左上隅にある連絡先情報を選択し、[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。

システム設定

Web 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\(Configuration\)\]](#) を移動します。

システム設定を検索する

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

システム設定は各カテゴリ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。

システム設定を変更する

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

- 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。
- [\[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。

システム設定について

Web インターフェイスからすべてのシステム設定を変更できます。

個別のシステム設定については [▶ System settings](#) の章を参照してください。

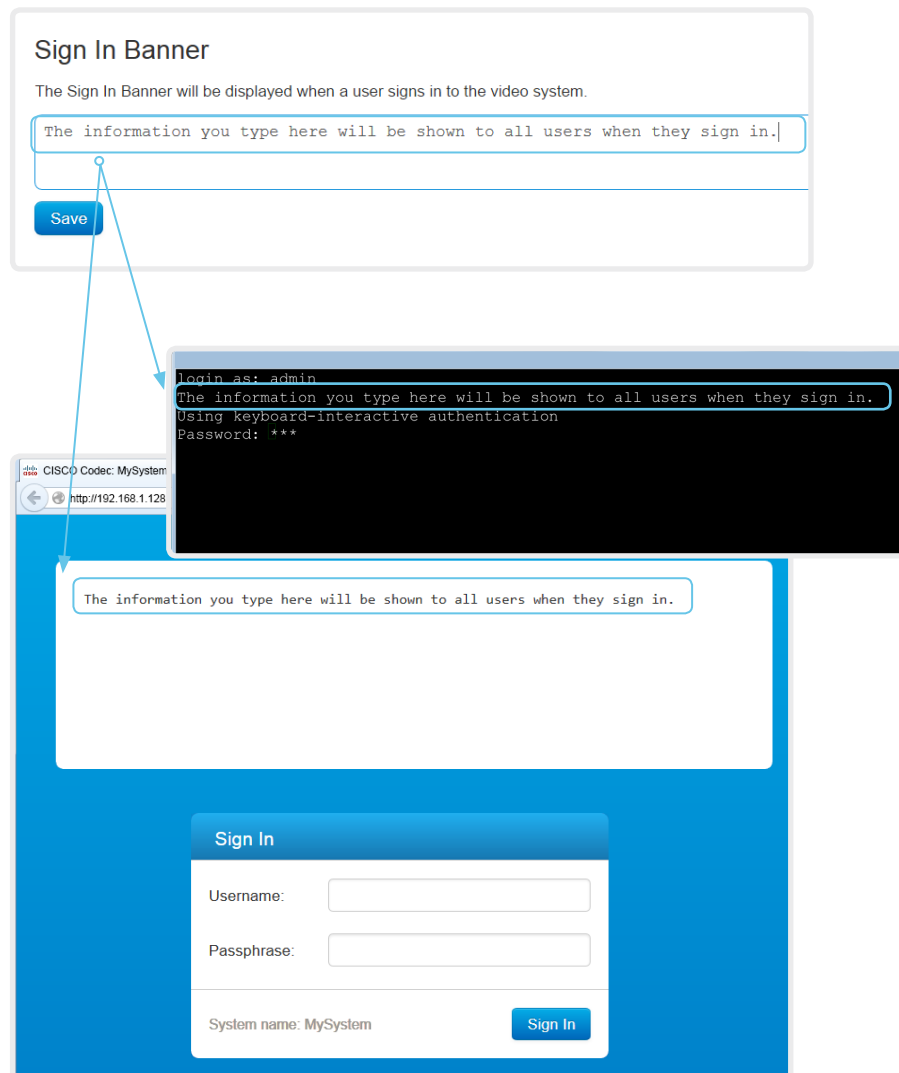
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者はすべてのシステム設定を変更できるように、すべてのユーザ ロールを所有している必要があります。

ユーザ管理およびユーザ ロールに関する詳細情報は、[▶ User administration](#) の章で確認できます。

サインイン バナーの追加

Web インターフェイスにサインインして、[\[設定 \(Configuration\)\]](#) > [\[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

システム管理者がすべてのユーザに初期情報を提供したい場合、サインイン バナーを作成できます。メッセージは、ユーザが Web インターフェイスまたはコマンドライン インターフェイスにサインインすると表示されます。

最大サイズは 4 kByte です。

ウェルカムバナーとサインインバナーの比較

サインインバナー (Sign In Banner)

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

ウェルカムバナー

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

ウェルカムバナーの追加

ウェルカムバナーの追加は API コマンドを使用するのみ利用可能です。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

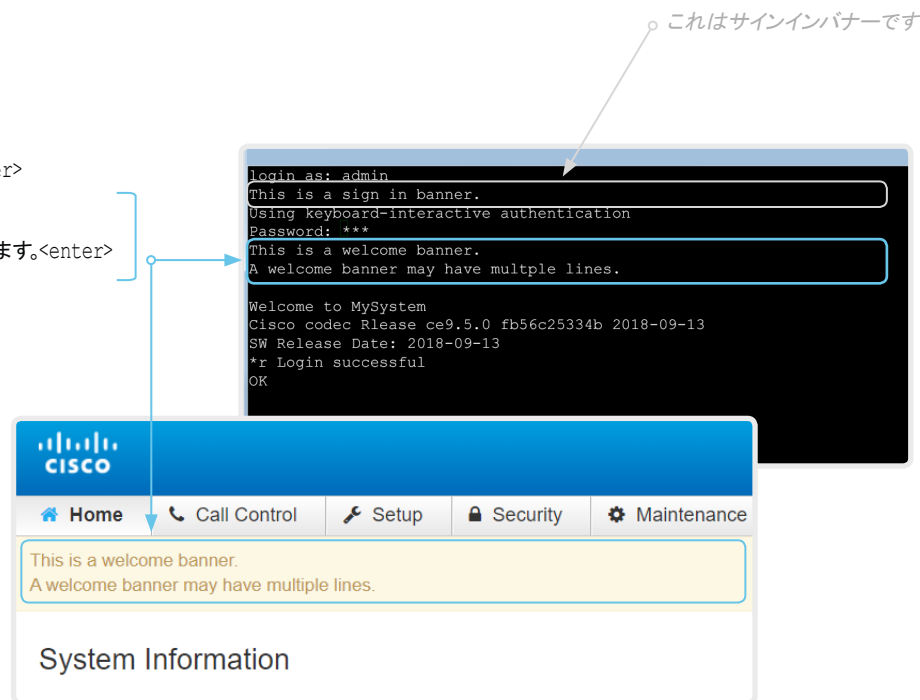
例

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

ビデオシステムの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、ユーザーがログイン後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。

バナーには作業開始に必要な情報や、システムのセットアップ時に注意しなければならないことなどが含まれています。

最大サイズは 4 kByte です。

ウェルカムバナーとログインバナーの比較

サインインバナー (Sign In Banner)

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

ウェルカムバナー

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

ビデオ システムのサービス証明書を管理する

Web 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、ビデオ システム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)を見つけてます。
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、証明書をビデオ システムに保存します。

Service Certificates

Certificate	Issuer	802.1X	Audit	HTTPS	SIP		
Certificate_A	CertificateAuthority_A	Off	Off	Off	Off	Delete	View Certificate
Certificate_B	CertificateAuthority_B	On	Off	Off	Off	Delete	View Certificate

Add Certificate

Certificate

Browse...

No file selected.

Private key (optional)

Browse...

No file selected.

Passphrase (optional)

This system supports PEM formatted certificate files (.pem). The certificate file may contain the certificate and a RSA or DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.

Add certificate...

図に示している証明書および証明書発行者は一例です。お使いのシステムには別の証明書があります。

ビデオ システム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なことがあります。

通信をセットアップする前に、有効な証明書をビデオ システムが提供するように、サーバまたはクライアントが要求することがあります。

ビデオ システムの証明書は、システム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。

複数の証明書をビデオ システムで保存できますが、サービスごとに一度に有効化できる証明書は 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)のリストを管理する

Web インターフェイスにサインインし、[\[セキュリティ\(Security\)\]](#) > [\[証明機関\(Certificate Authorities\)\]](#) に移動して、[\[カスタム CA\(Custom CAs\)\]](#) 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。

認証局のリストのアップロード

1. [\[参照\(Browse\)\]](#) ボタンを押して、CA 証明書のリストを含むファイル(ファイル形式 .PEM)をコンピュータ上で見つけます。
2. [\[認証局の追加...\(Add certificate authority...\)\]](#) をクリックして、新しい CA 証明書をビデオ システムに保存します。

Certificate Authorities

Custom CAs Preinstalled CAs

Certificate	Issuer	
CA_Certificate_1	Issuer_1	Delete... View Certificate

Add Certificate Authority

CA file [Browse...](#) CA-certificates.pem

This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

[Add certificate authority...](#)

図に示している証明書および証明書発行者は一例です。お使いのシステムには別の証明書があります。



以前に保存した証明書は自動的に削除されません。

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 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なことがあります。

通信をセットアップする前に、サーバまたはクライアントからシステムに証明書を提示することを要求するよう、ビデオ システムを設定できます。

証明書は、サーバまたはクライアントの信頼性を確認するテキスト ファイルです。証明書は、信頼できる CA により署名されている必要があります。

証明書の署名を検証するには、信頼できる CA のリストがビデオ システム上に存在する必要があります。

このリストには、監査ロギングとその他の接続の両方の証明書を検証するために必要なすべての CA が含まれている必要があります。

認証が失敗した場合、接続は確立されません。

セキュア監査ロギングのセットアップ

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



監査サーバの証明書を検証する認証局(CA)が、ビデオ システムの信頼できる認証局のリスト内に存在する必要があります。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、▶ [「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。

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。
3. [\[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。
4. [\[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。
5. [\[保存\(Save\)\]](#) をクリックして変更を有効にします。

Configuration

Revert
Save
-
+

Security

Audit

Logging Mode

ExternalSecure

Undo

OnError Action

External

ExternalSecure

Internal

Off

Server

Address

Undo (0 to 255 characters)

Port

514

(0 to 65535)

PortAssignment

Auto

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、ビデオ システム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、ビデオ システムは暗号化された監査ログを外部監査サーバ(syslog サーバ)に送信します。そのサーバの ID は署名された証明書によって検証される必要があります。

監査サーバの署名は、他のサーバ/クライアントと同じ 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。

Expressway プロビジョニング経由の CUCM 用のプレインストール済み証明書の管理

Web インターフェイスにサインインし、[\[設定\(Configuration\)\]](#) > [\[セキュリティ\(Security\)\]](#) に移動して、[\[プレインストール済み CA\(Preinstalled CAs\)\]](#) 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。

Certificate Authorities

Custom CAs
Preinstalled CAs

This CA list is used for Cisco UCM via Expressway (Edge) provisioning only.

[Configure provisioning now.](#)

These certificates are used to validate the servers contacted over the Internet when the endpoint uses Cisco UCM via Expressway provisioning.

Certificate	Issuer			
Certificate_01	Issuer_1	Details...	✓	Disable
Certificate_02	Issuer_2	Details...	✓	Disable
Certificate_03	Issuer_3	Details...	✓	Disable

[Disable All](#)

図に示している証明書および証明書発行者は一例です。お使いのシステムには別の証明書があります。

i プレインストール済み証明書を使用する代わりに、必要な証明書を手動で証明書リストに付加することもできます。

信頼できる証明書のリストの更新方法については、
▶ [「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。

プレインストールされた証明書について

このページ内のプレインストールされた証明書は、ビデオ システムが Cisco Unified Communications Manager(CUCM)によって Expressway(エッジ)経由でプロビジョニングされた場合にのみ使用されます。

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

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

ビデオ システムを初期設定にリセットしても、プレインストールされた証明書のリストは削除されません。

CUCM 信頼リストを削除する

この章内の情報は、Cisco Unified Communications Manager(CUCM)に登録されているビデオ システムにのみ関連します。

Web インターフェイスにサインインして、[\[セキュリティ\(Security\)\] > \[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、Web ページに表示されます。

この情報は、トラブルシューティングに役立ちます。

信頼リストの詳細

CUCM と信頼リストの詳細については、シスコの Web 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

Web 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、ビデオ システム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...\(Save and reboot...\)\]](#) をクリックします。

ビデオ システムが自動的に再起動します。再起動後、新しい永続設定に従って動作が変化します。



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

永続モード

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

- ・ システム設定の変更
- ・ 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、初期設定へのリセットを行う必要があります。

工場出荷時設定リセットの実行方法については、

▶ [「ビデオ システムの工場出荷時設定リセット」](#)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て、[\[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。

ビデオ システム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。

システム パスフレーズの変更方法については、
▶ [「システム 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

ビデオ システム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...」](#) 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。

ビデオ システムは自動的に再起動します。

Strong Security Mode

Strong Security Mode is **not** enabled.

Strong Security Mode is required to adhere to U.S. Department of Defense JITC regulations.

It will introduce the following:

- All users and administrators must change their passphrase and PIN on the next sign in
- New passphrases must meet the following criteria:
 - Minimum 15 characters
 - Minimum 2 uppercase alphabetic characters
 - Minimum 2 lowercase alphabetic characters
 - Minimum 2 numerical characters
 - Minimum 2 non-alphanumeric (special) characters
 - No more than 2 consecutive characters may be the same
 - Must be different from the last 10 previous passphrases used
 - Not more than 2 characters from the previous passphrase can be in the same position
- Passphrases must be changed at least every 60 days
- Passphrases cannot be changed more than once per 24 hours
- 3 failed signins will lock the user account until an administrator re-activates the account

[Enable Strong Security Mode...](#)

Strong Security Mode

Strong Security Mode is enabled.

[Disable Strong Security Mode...](#)

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。

コンテンツ共有のために Intelligent Proximity をセットアップする アップ (1/5 ページ)

Cisco Proximity を使用すると、ユーザは自分のモバイル デバイス(スマートフォン、タブレット、またはラップトップ)がビデオ システム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、キャプチャおよび共有することができます。

モバイル デバイスは、ビデオ システム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 システムとペアリングできます。



Proximity の同時接続数は、ビデオ システム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 システム	最大接続数
Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2	30/7 *
Codec Plus, Codec Pro	30/7 *
SX80	10
SX10, SX20	7
MX700, MX800	10
MX200 G2, MX300 G2	7
DX70, DX80	3

* モバイル デバイスのプロキシミティ サービス上の共有コンテンツの確認が無効化されているときは、接続数は 30 になります。このサービスの有効時、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 システムの制御:

- ・ ダイヤル、ミュート、音量調節、切断
- ・ 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のみ利用できます。

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 [英語]

サポートされるオペレーティング システム

- ・ iOS 7 以降
- ・ Android 4.0 以降
- ・ Mac OS X 10.9 以降
- ・ Windows 7 以降

Windows 8 で導入されたタイル ベースのインターフェイスはサポートされていません。

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

超音波の放出

シスコのビデオ システムは、プロキシミティ機能の一部として超音波を出します。

[\[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 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。

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

- ・ これらのビデオ システムでは、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ル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:

これらのシステムでは、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、Room 55 Dual、Room Kit、Room Kit Plus、Codec Plus、Codec Pro、SX10、SX20、SX80 および MX シリーズ:

- ・ これらのシステムは、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 システムでヘッドセットを使用する場合は、超音波発生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。
- ・ これらのシステム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。

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て、[\[セットアップ\(Setup\)\]](#) > [\[設定\(Configuration\)\]](#)に移動します。

2. [\[プロキシミティ\(Proximity\)\]](#) > [\[モード\(Mode\)\]](#)に移動します。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 システムは超音波ペアリング 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 システムの制御:

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

モバイル デバイス上での共有コンテンツの表示:

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

デスクトップ クライアントからのワイヤレス共有:

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

プロキシミティ インジケータ



1 つ以上の Proximity クライアントがシステムとペアになっている場合、スクリーンにプロキシミティ 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。

プロキシミティがオンになっていると、ビデオ システムは超音波のペアリング メッセージを発信します。

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。

最良のユーザ エクスペリエンスを得るために、プロキシミティを機能常にオンにすることをお勧めします。

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

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

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 Intelligent Proximity のパフォーマンスを確保するために、会議室の音響処理を常に強く推奨します。
- 1 つの部屋の中で Intelligent Proximity を有効にするビデオ システムは 1 つだけにすることを推奨します。複数あると、干渉が発生する可能性があり、デバイス検出とセッション メンテナンスの問題の原因となることがあります。

プライバシーについて

シスコ プライバシー ポリシーと Cisco Proximity 付録には、クライアントにおけるデータ収集とプライバシーの懸念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>

[英語]

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(20 kHz–22 kHz)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、ビデオシステムの Web インターフェイスで[メンテナンス(Maintenance)] > [診断(Diagnostics)]を確認します。超音波に関する問題がリストに記載されていない場合(超音波信号を確認できません[Unable to verify the ultrasound signal])、超音波のベアリングメッセージがビデオシステムから発信されます。クライアントで検出される問題のサポートには、プロキシミティのサポート掲示板を参照してください。

オーディオ アーチファクト

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

ラップトップから内容を共有できない

- コンテンツ シェアリングを機能させるには、ビデオ システム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、プロキシミティ シェアリングは、ビデオ システムが 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、失敗する可能性があります。

関連リソース

Cisco Intelligent Proximity のサイト:

▶ <https://www.cisco.com/go/proximity>

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システムでサポートされている必要があります。

60 fps のビデオの許可

デフォルトとして、カメラは 1 秒あたり 30 フレーム(30 fps)を出力します。これにより、通常の帯域と照明条件であってもクローズアップと広い視野両方の画像の品質が良くなります。条件がさらに良い場合、カメラからの出力が 60 fps となり、全般的に良い品質となる可能性があります。

カメラの出力フレーム レートを設定するには、[カメラのカメラ フレーム レート(Cameras Camera Framerate)] 設定を使用します。

Web 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。
3. [カメラ(Cameras)] > [カメラ(Camera)] > [フレームレート(Framerate)] に進み、60fps のビデオを許可するかどうかを選択します。

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	Medium	大きい	標準	Medium	大きい
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
576	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 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
1536	1280 × 720 @ 30	1280 × 720 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 60	1280 × 720 @ 60
2176	1280 × 720 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 60	1280 × 720 @ 60	1280 × 720 @ 60
3232	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60
4736	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 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	Medium	大きい	標準	Medium	大きい
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
576	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 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
1536	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 60	1280 × 720 @ 60	1920 × 1080 @ 60
2176	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60
3232	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60
4736	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 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て、[\[セットアップ\(Setup\)\]](#) > [\[パーソナライゼーション\(Personalization\)\]](#) に移動し、[\[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、カスタム メッセージ)をビデオ システムに追加できます。

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)。
- ・ 左下隅に短いメッセージ(テキストのみ)を追加します(画面のみで、Touch 10 は不可)。



Logo

推奨事項:

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

ブランディングについて

この章で説明しているように、ブランディング機能により、シスコの全体的なユーザ エクスペリエンスを損なうことなく、スクリーンとタッチ ユーザ インターフェイスの表示をカスタマイズできます。

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

ブランド機能とカスタム壁紙は、同時に使用できません。

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

画面および 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

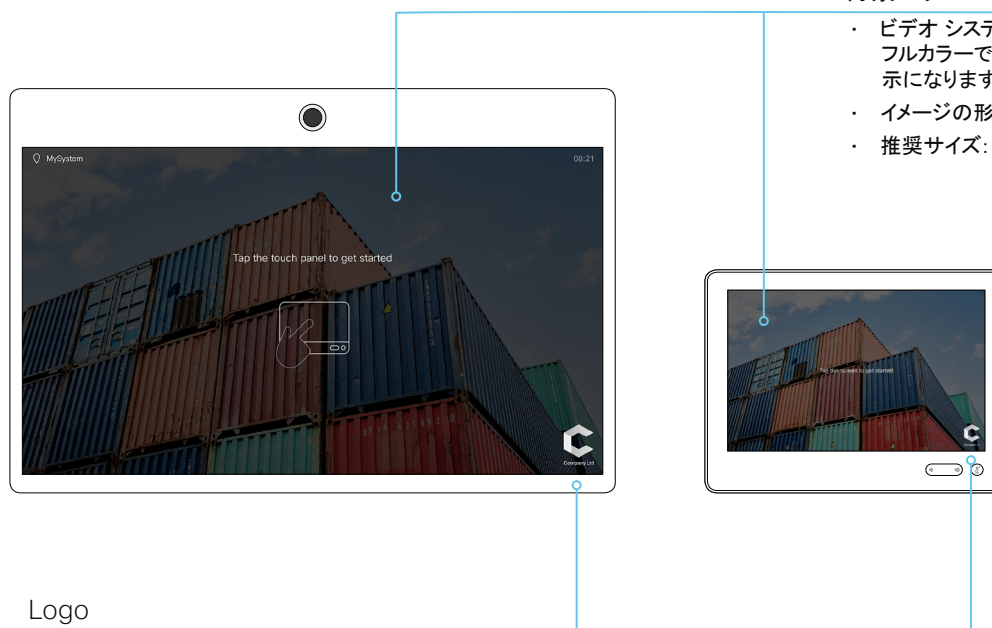
ハーフウェイク状態では、次のことができます。

- ・ 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、ビデオ システム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 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

- ・ ビデオ システムがウェイクアップするとイメージ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



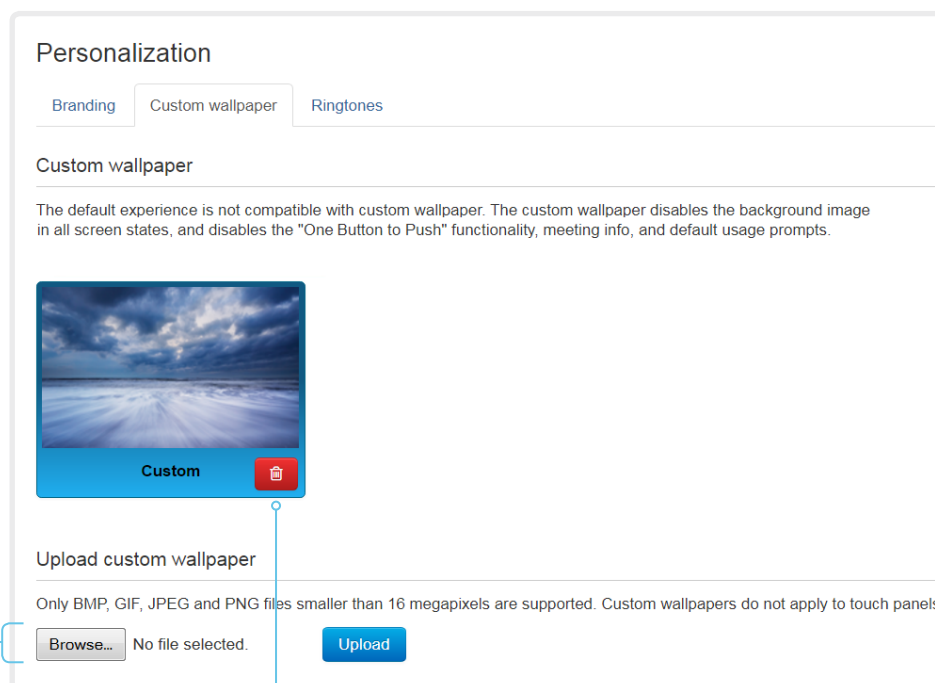
Logo

推奨事項:

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

カスタム壁紙の追加

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



カスタムの壁紙のアップロード

古いカスタム壁紙があれば上書きします。

1. [\[参照\(Browse\)\]](#) ボタンを押して、カスタム壁紙のイメージ ファイルを見つけます。
 2. [\[アップロード\(Upload\)\]](#) をクリックして、ファイルをビデオ システムに保存します。
- サポートされるファイル形式: BMP、GIF、JPEG、PNG

最大ファイル サイズ: 16 メガピクセル

カスタム壁紙をアップロードすると、自動的にアクティブになります。

カスタムの壁紙の削除

[\[削除\(Delete\)\]](#) によって、カスタム壁紙がビデオ システムから完全に削除されます。

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

カスタム壁紙について

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

ビデオ システムでは一度に 1 枚のカスタム壁紙しか保存できません。新しいカスタム壁紙は古いものを上書きします。

この従来のカスタム壁紙機能ではなく、新しいブランディング機能を使用することをお勧めします。それにより、シスコの全体的なユーザーエクスペリエンスが向上し、ワンボタン機能や会議情報などの機能が使用できなくなることを回避できます。▶ [「画面および Touch 10 ユーザー インターフェイスに企業ブランディングを追加」](#)の章を参照してください。

ブランド機能とカスタム壁紙は、同時に使用できません。

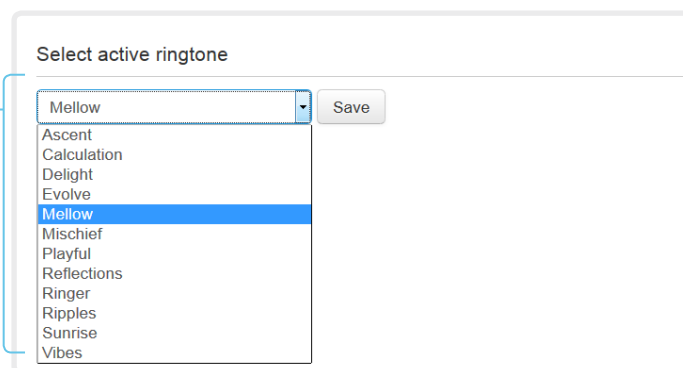
ビデオ システムでブランディング要素がセットアップされている場合は、カスタム壁紙を追加する前に [\[ブランディングなしで続行\(Continue without branding\)\]](#) をクリックする必要があります。

着信音の選択と着信音量の設定

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

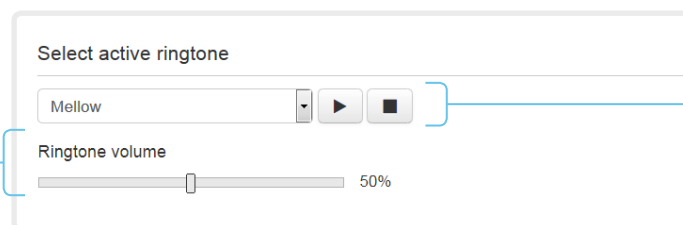
呼び出し音の変更

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

一連の着信音がビデオ システムにインストールされています。着信音を選択して音量を設定するには、Web インターフェイスを使用します。

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

お気に入りリストの管理

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

ファイルから連絡先をインポート/エクスポート

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

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

連絡先を追加または編集する

1. [連絡先の追加 (Add contact)] をクリックして新しいローカル連絡先を作成するか、連絡先の名前をクリックしてから [連絡先を編集 (Edit contact)] をクリックします。

2. ポップアップ表示されたフォームに値を入力するか、そのフォームを更新します。

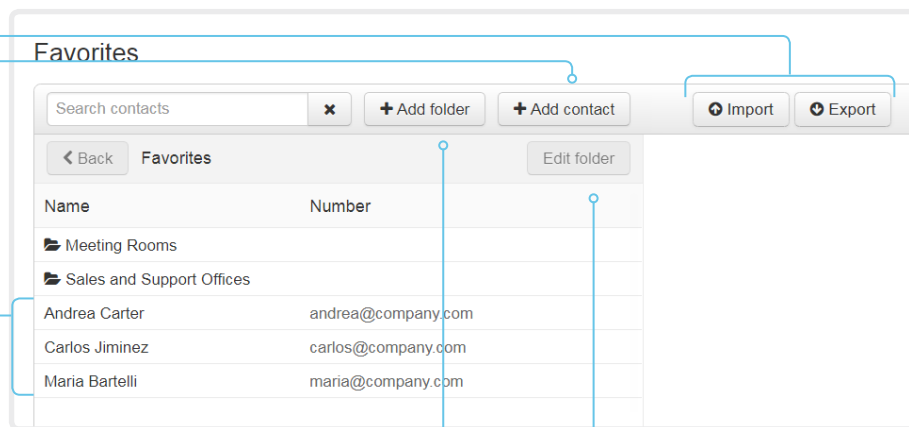
連絡先をサブフォルダに保存するために、フォルダ ドロップダウン リストでフォルダを選択します。

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

3. [保存 (Save)] をクリックしてローカル連絡先を保存します。

コンタクトの削除

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



サブフォルダを追加または編集する

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

サブフォルダを削除する

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

ビデオ システムのユーザー インターフェイスによるお気に入りへの管理

お気に入りリストへの連絡先の追加

1. ホーム画面の [発信 (Call)] を選択します。
2. 追加する連絡先を選択します。
3. [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て、[\[セットアップ\(Setup\)\]](#) > [\[設定\(Configuration\)\]](#)に移動します。
2. [\[ユーザインターフェイス\(UserInterface\)\]](#) > [\[アクセシビリティ\(Accessibility\)\]](#) > [\[着信コール通知\(IncomingCallNotification\)\]](#) に移動して、[\[画面表示の強調\(AmplifiedVisuals\)\]](#) を選択します。
3. [\[Save\(保存\)\]](#) をクリックします。

第 3 章

周辺機器

モニタの接続 (1/2 ページ)

ビデオ システムには 2 つの HDMI ビデオ出力があります。通常、出力はモニタまたはその他のディスプレイに使用されます。ビデオ システムは、使用可能なすべてのモニタにレイアウトを配信します。

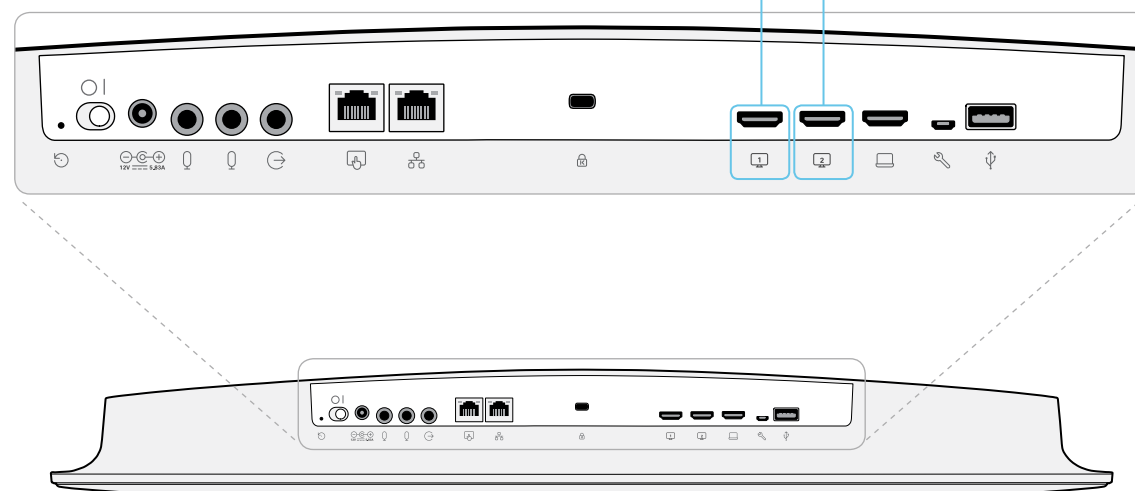
HDMI 出力は、60 fps で最大 3840 × 2160 の解像度をサポートします。高解像度とフレーム レートをサポートするプレミアム HDMI ケーブルが必要です。HDMI 出力には音声はありません。



モニタおよび他の周辺機器の接続時や切断時には、必ず電源を切ってください。

第 2 のモニタ用の HDMI 出力(出力コネクタ 2)

第 1 のモニタ用の HDMI 出力(出力コネクタ 1)



自動セットアップ

デュアル モニタのシナリオをサポートするためにビデオ システム上で特別な設定は不要です。デフォルトでは、モニタの数は自動的に検出され、各モニタのロールは、(第 1 のモニタと第 2 のモニタのどちらとして用意されたものであろうが)物理的な接続に従って自動的に設定されます。

手動設定が必要なとき

1 つ以上の設定を手動で行ってデフォルト動作を上書きできます。次のことを行いたい場合に、手動設定が必要になります。

- ・ モニタをプレゼンテーションの表示専用を使用する場合
- ・ 同じレイアウトを複数のモニタに複製する場合
- ・ 最も低い番号のビデオ出力とは別のモニタに画面表示メッセージとインジケータ(OSD)を表示する。
- ・ 解像度を手動で設定する(ビデオ システムによるモニタのネイティブ解像度および更新間隔の検出に失敗した場合など)。

モニタの接続 (2/2 ページ)

手動セットアップ

一般的なシングルモニタ やデュアルモニタの場合には、自動設定で十分に対応できます。より複雑なシナリオでは、手動セットアップが必要になることがあります。

Web 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。

各モニタのロールの設定

各モニタのロールは、[\[ビデオ\(Video\)\]](#) > [\[出力\(Output\)\]](#) > [\[コネクタ n\(Connector n\)\]](#) > [\[モニタロール\(MonitorRole\)\]](#) 設定を使用して定義します。

モニタ セットアップと一致するモニタ ロールを選択します。

モニタ数の設定

[\[ビデオ\(Video\)\]](#) > [\[モニタ\(Monitors\)\]](#) 設定で、セットアップで使用するレイアウトの異なるモニタ数を設定します。

[自動(Auto)] に設定すると、モニタがコネクタに接続された場合にビデオ システムが自動的に検出するため、セットアップのモニタ数も特定されます。

その他のオプションを使用すれば、シングルモニタ またはデュアルモニタのセットアップの修正や、1 つのモニタをプレゼンテーション専用にするなどができます。

メッセージおよびインジケータを表示するモニタの選択

[\[ユーザインターフェイス\(UserInterface\)\]](#) > [\[OSD\]](#) > [\[出力\(Output\)\]](#) 設定を使用して、画面表示のメッセージおよびインジケータを表示するモニタを定義します。

[自動(Auto)] に設定すると、ビデオ システムがコネクタ数に基づいて使用するモニタを決定します。

モニタ解像度と更新レートを設定します。

ビデオ システムは、モニタのネイティブ解像度を識別し、可能であればこれを出力します。通常は、これによりモニタの最適な画像が提供されます。

解像度や更新間隔の自動検出に失敗した場合、[\[ビデオ\(Video\)\]](#) > [\[出力\(Output\)\]](#) > [\[コネクタ n\(Connector n\)\]](#) > [\[解像度\(Resolution\)\]](#) 設定を使用して手動で解像度を設定する必要があります。

モニタの数と各モニタのロールについて

[\[ビデオ\(Video\)\]](#) > [\[出力\(Output\)\]](#) > [\[コネクタ n\(Connector n\)\]](#) > [\[モニタロール\(MonitorRole\)\]](#) 設定では、出力に接続されたモニタにロールを割り当てます。モニタ ロールによって、モニタ上に表示されるレイアウト (コール参加者とプレゼンテーション) が決まります。

同じモニタ ロールのモニタは同じレイアウトになり、別のモニタ ロールのモニタは異なるレイアウトになります。

[\[ビデオ\(Video\)\]](#) > [\[モニタ\(Monitors\)\]](#) 設定では、部屋のセットアップで使用する異なるレイアウトの数を反映する必要があります。

多くの場合、異なるレイアウトの数は物理モニタの数と同じですが、そうではない場合もあります。正確に同じレイアウトを 2 台のモニタで繰り返す必要がある場合、異なるレイアウトの数は少なくなります。

1 台のモニタをプレゼンテーション用に確保できるように注意してください。

例:

合計 2 台のモニタで、第 2(2 番目の)モニタがプレゼンテーションの表示専用になっています。

- [\[ビデオ\(Video\)\]](#) > [\[モニタ\(Monitors\)\]](#): [デュアルプレゼンテーションのみ(DualPresentationOnly)]
- [\[ビデオ\(Video\)\]](#) > [\[出力\(Output\)\]](#) > [\[コネクタ 1\(Connector 1\)\]](#) > [\[モニタロール\(MonitorRole\)\]](#): [自動(Auto)]
- [\[ビデオ\(Video\)\]](#) > [\[出力\(Output\)\]](#) > [\[コネクタ 2\(Connector 2\)\]](#) > [\[モニタロール\(MonitorRole\)\]](#): [自動(Auto)]
- [\[ユーザインターフェイス\(UserInterface\)\]](#) > [\[OSD\]](#) > [\[出力\(Output\)\]](#): [自動(Auto)]

入力ソースの接続 (1/2 ページ)

Web 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

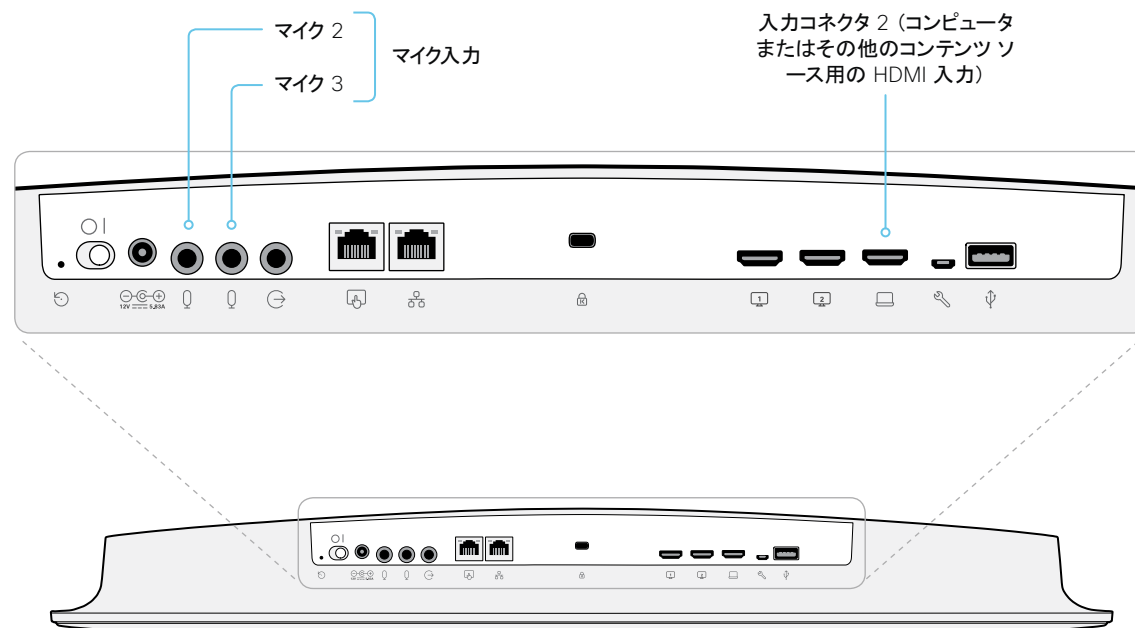
コンテンツをローカルで、または会議参加者と共有するために、1 つの入力ソース(パソコン1 台など)をビデオシステムの HDMI 入力(入力コネクタ 2)に接続できます。

HDMI 入力は、30 fps で最大 3840 × 2160 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。

外部マイクの接続

ビデオ システムにはマイクが内蔵されていますが、1 個または 2 個の外部マイクもサポートしています。Cisco Table Microphone 20 または Cisco TelePresence Ceiling Microphone を使用してください。

マイク 1 はビデオ システムの内蔵マイクですので注意してください。



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。

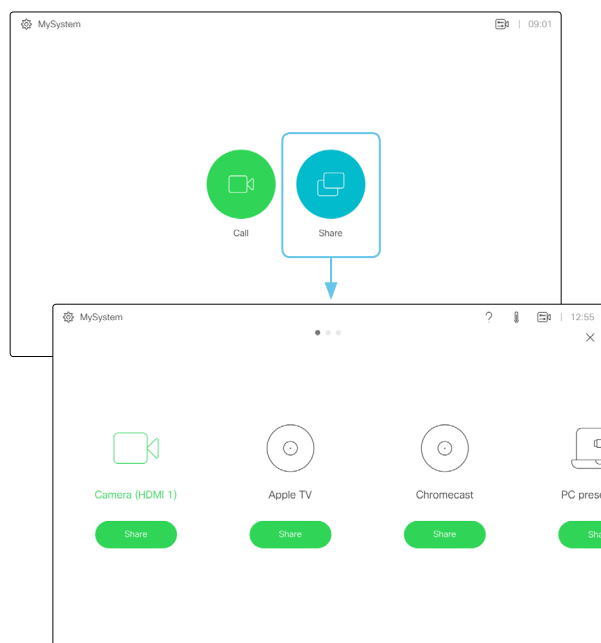
デフォルト値はコネクタ用モーション(Motion)です。

コネクタ 2 のデフォルト値は [\[シャープネス\(Sharpness\)\]](#) です。

入力ソース数の拡大

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

ソースは、ビデオ システムに直接接続されている他のビデオと同じように表示されて動作します。



複数の外部入力ソースがあるユーザ インターフェイス (例)

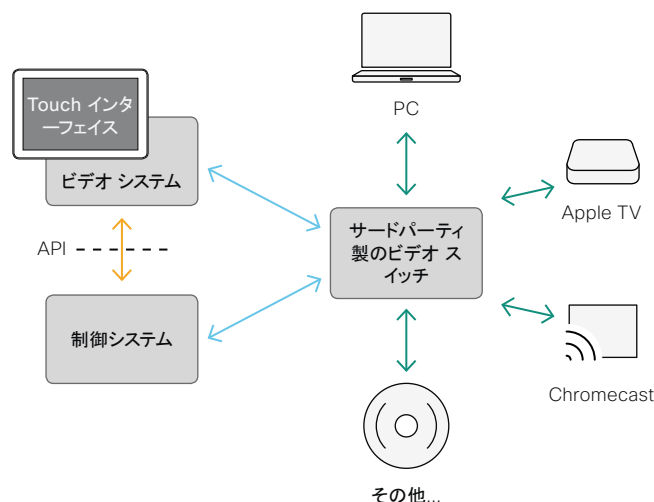
ユーザ インターフェイスを拡張する方法、およびそれをビデオ システムの API を使用してセットアップする方法の詳細については、CE のカスタマイズ ガイド [英語] を参照してください。次のリンクにアクセスします。

▶ <https://www.cisco.com/go/in-room-control-docs> [英語]

アーキテクチャ

タッチ インターフェイスがあるシスコ ビデオ システム、サードパーティ製制御システム (Crestron または AMX など)、およびサードパーティ製ビデオ スイッチが必要です。ビデオ スイッチを制御するのは、ビデオ システムではなく、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には、ビデオ システムの API (イベントとコマンド)* を、ビデオ スイッチや、タッチ インターフェイス上のコントロールと接続するために使用する必要があります。このようにして、ユーザ インターフェイス上に表示されて実行される事柄と、入力ソースの実際の状態とを同期できます。



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

ディスプレイについて

リアルタイム通信の要件

シスコでは、ビデオ システムでのカメラからスクリーンへの遅延を最小限にし、また音声コンポーネントとビデオ コンポーネント間全体の遅延を検出してそれを埋め合わせるために、さまざまな取り組みを行ってきました。

コミュニケーションがより自然な感じになるように低遅延のディスプレイを使用することを推奨します。また、多数のディスプレイを注文する前に、サンプルをテストすることも推奨します。

ほとんどのディスプレイによる遅延は多くの場合非常に高い(100 ms より長い)ため、リアルタイム コミュニケーションの品質を損ないます。

次のディスプレイの設定によって、この遅延が低下する可能性があります。

- ・ [ゲーム(Game)] モード、[PC] モード、あるいは、応答時間(および通常であれば遅延)を低下させるように設計された同様のモードをアクティブにします。
- ・ 遅延を発生させる、動きを円滑化する機能(たとえば、[モーション フロー(Motion Flow)] や [ナチュラル モーション(Natural Motion)] などのビデオ処理)を非アクティブにします。
- ・ 音響エコー キャンセラの誤動作を発生させる [仮想サラウンド (Virtual Surround)] 効果や [ダイナミック コンプレッション (Dynamic Compression)] などの高度な音声処理を非アクティブにします。
- ・ 別の HDMI 入力に変更する。

Consumer Electronics Control (CEC)

ディスプレイのアクティブなビデオ入力がユーザによって変更されることがあります。アクティブなビデオ入力は、製造元のユーザ インターフェイスから設定されます。

発信すると、ビデオシステムはアクティブなビデオ入力が別の入力に切り替えられたかどうかを検出します。すると、ビデオ システムは入力を切り戻すため、ビデオ システムがアクティブなビデオ入力ソースになります。

ビデオシステムがスタンバイ状態に入るときにアクティブな入力ソースでない場合、ディスプレイはスタンバイ状態に移行しません。

シスコが推奨するディスプレイ

最大限のエクスペリエンスと検証済みの互換性のため、次のディスプレイを使用することをお勧めします。このディスプレイの一覧は変更される可能性があるため、CE9 ソフトウェアのリリース ノートで更新を確認してください。

モデル	LG グローバル Web サイト リンク
49インチ UHD(49UH5C)	http://www.lg.com/global/business/information-display/digital-signage/lg-49UH5C
55インチ UHD(55UH5C)	http://www.lg.com/global/business/information-display/digital-signage/lg-55UH5C
65インチ UHD(65UH5C)	http://www.lg.com/global/business/information-display/digital-signage/lg-65UH5C
75インチ UHD (75UH5C)	http://www.lg.com/global/business/information-display/digital-signage/lg-75UH5C
86インチ UHD(86UH5C)	http://www.lg.com/global/business/information-display/digital-signage/lg-86UH5C
98インチ UHD(98UH5C)	http://www.lg.com/global/business/information-display/digital-signage/lg-98LS95D

モデル	LG グローバル Web サイト リンク
QMN シリーズ (43インチ49インチ、55インチ、65インチ、75インチ)	https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N [英語]
QMH シリーズ (49インチ55インチ、65インチ)	https://displaysolutions.samsung.com/digital-signage/detail/1144/QM49H [英語]
QBN シリーズ (43インチ49インチ、55インチ、65インチ、75インチ)	https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N [英語]
QBH シリーズ (65インチ、75インチ)	https://displaysolutions.samsung.com/digital-signage/detail/1205/QB65H [英語]

4K 解像度について

ディスプレイの接続

システムを初めて起動すると、セットアップ アシスタントが自動的に起動します。ここで、ディスプレイをテストして設定を調整します。画面の指示に従います。

後の段階で設定を調整する必要がある場合、Web 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\(Configuration\)\]](#) > [\[ビデオ\(Video\)\]](#) > [\[出力\(Output\)\]](#) > [\[コネクタ n\(Connector n\)\]](#) > [\[解像度\(Resolution\)\]](#) に移動し、画面の解像度を調整します。ディスプレイのサポート内容に応じて解像度を設定してください。

スクリーンが黒くなったりちらつく場合は、解像度を低く設定できます。それでも問題が解決しない場合は、Ultra HD をサポートするディスプレイの HDMI ポートに HDMI ケーブルが接続されていることを確認してください。ディスプレイで HDMI Ultra HD の設定がオンになっていることも確認してください。

シスコでは、テスト済みのディスプレイの一覧を提供しています。
[▶「シスコが推奨するディスプレイ」](#)の章を参照してください。

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\(Preferred Resolution\)\]](#) に移動して、値を調整します。

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

チェックリスト

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

ビデオ システムの入力/出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(TV/ディスプレイ、コンピュータ)が 4K をサポートしており、正しく設定されていることを確認します。

TV/ディスプレイが 4K をサポートしていると製造元が公表していても、TV/ディスプレイをテストして動作を確認する必要があります。

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

HDMI ケーブルは、カメラ、ディスプレイ、およびプレゼンテーション ソースとの接続に必要です。

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

カメラおよびディスプレイ用の HDMI ケーブル

1920X1200@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。動作が保証されている範囲については、3840×2160(60fps)でシスコが事前に選定した HDMI ケーブルを使用するか、またはプレミアム HDMI ケーブル認証プログラムに合格したケーブルを使用します。

プレゼンテーション ソース用の HDMI ケーブル

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

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

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

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

* Room Kit、Room Kit Plus、Codec Plus、Room 55、および Room 70 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。

SpeakerTrack 機能のセットアップ

Web インターフェイスにサインインして、[\[設定\(Configuration\)\]](#) > [\[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。

スピーカートラック機能は自動カメラ 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。

クローズ アップが有効になっている場合、室内の人が話すと、システムがその人を検出し、最適なカメラフレーミングを選択します。クローズ アップには室内の一部の人が含まれない場合があります。室内のすべての人を常に表示しておきたい場合、クローズ アップ機能をオフにできます。

最適な全体表示

カメラは、デジタル顔検出機能を使用して、会議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、会議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。この機能は、スピーカートラックと連動して、最適な会議エクスペリエンスを提供します。

スピーカートラックの設定

スピーカートラックを設定するには、[\[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)]: スピーカートラックは全般に有効になります。システムは室内の人々を検出し自動的に最適なカメラ フレーミングを選択します。スピーカートラックのオン/オフは、タッチ コントローラのカメラ制御パネルを使用してすぐに切り替えることができます。

Off: スピーカートラックがオフになります。スピーカートラックのオン/オフ ボタンがタッチ コントローラに表示されなくなります。クローズ アップ機能は無効になります。

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

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

Auto: システムは、話している人にズームインします。

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

スピーカートラックをサポートしている製品

次のシスコ製品がスピーカートラックをサポートしています。

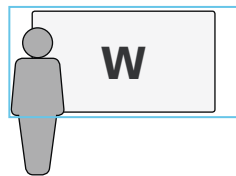
- ・ デュアル カメラが搭載されている MX700 および MX800
- ・ SpeakerTrack 60 カメラまたはクワッド カメラを使用した SX80
- ・ Room Kit
- ・ Room Kit Plus (Codec Plus とクアッド カメラ)
- ・ Room Kit Pro (Codec Pro および Quad Camera)
- ・ Room 55
- ・ Room 55 Dual
- ・ Room 70
- ・ Room 70 G2

ホワイトボードへのスナップ機能の設定 (1/3 ページ)

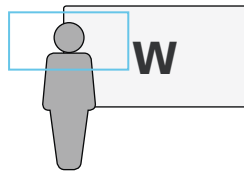
ホワイトボードへのスナップ機能はスピーカートラッキング機能の拡張です。そのため、SpeakerTrack をサポートするカメラが必要になります。

- デュアル カメラが搭載されている MX700 および MX800
- SpeakerTrack 60 カメラまたはクワッド カメラを使用した SX80
- Room Kit
- Room Kit Plus(Codec Plus とクアッド カメラ)
- Room Kit Pro (Codec Pro および Quad Camera)
- Room 55
- Room 55 Dual
- Room 70
- Room 70 G2

Snap to Whiteboard 拡張機能を使用すると、ホワイトボードの横にいる人物が話しているときに、カメラがその人物とホワイトボードの両方をキャプチャできます。

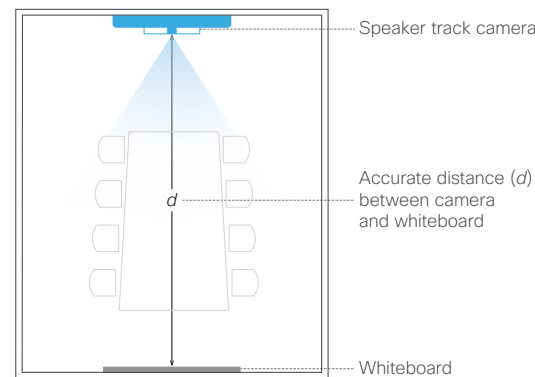


ホワイトボードへのスナップ拡張機能を使用しない場合、カメラは人のみをキャプチャします。



準備

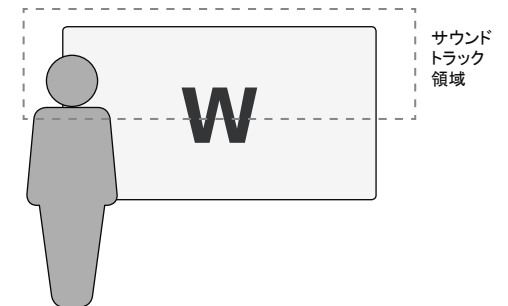
ホワイトボードの位置



図に示すように、ホワイトボードはカメラから部屋の反対側に配置する必要があります。

機能を設定する場合は、カメラとホワイトボード間の正確な距離を知る必要があります。

スピーカーの位置



サウンドトラック領域はホワイトボードの上半分です。

したがって、ホワイトボードでプレゼンテーションを行う人物はホワイトボードの横に直立する必要があります。ユーザは室内を移動できません。

ホワイトボードへのスナップ機能の設定 (2/3 ページ)

ホワイトボードへのスナップのウィザードは、次の場合にのみ使用できます。

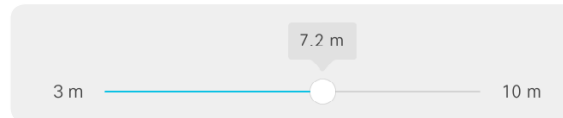
- ・ [\[カメラ\(Camera\)\]](#) > [\[スピーカートラック\(SpeakerTrack\)\]](#) > [\[モード\(Mode\)\]](#) が [\[自動\(Auto\)\]](#)

ホワイトボード領域の定義

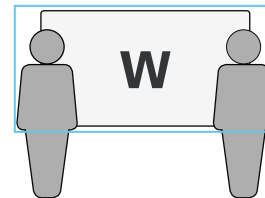
Touch コントローラ上のウィザードを使用して、ホワイトボード領域を定義します。

1. タッチコントローラの左上隅にある連絡先情報をタップし、[\[設定\(Settings\)\]](#)メニューを開きます。
2. [\[ホワイトボードへのスナップ\(Snap to Whiteboard\)\]](#)をタップします。
ビデオ システムで [\[設定\(Settings\)\]](#)メニューがパス フレーズによって保護されている場合は、ADMIN クレデンシャルでサインインします。
3. ウィザードを開始するには、[\[設定\(Configure\)\]](#)または [\[再設定\(Reconfigure\)\]](#)をタップします(この機能の設定が初回かどうかによって異なります)。

4. ウィザードの指示に従います。手順をやり直す場合は戻るボタン  を使用し、次の手順に移動するには次に進むボタン  を使用します。
 - ・ スライダを動かして、カメラとホワイトボードの距離を設定します。距離を正確に測定することが重要です。



- ・ カメラの表示(パン、チルト、ズーム)を調整してホワイトボードがフレームに入るようにします。両側に話し手のためのスペースを残します。



- ・ ホワイトボードの横に立って、話し始めます。
カメラがホワイトボード用に選択したビューにズームする場合は、機能が正しくセットアップされており、使用できる状態になっています。そうでない場合は、右のトラブルシューティングに関する注意事項を参照してください。
- ・ タップ  してウィザードを閉じ、 設定パネルを閉じます。

トラブルシューティング

ホワイトボードの横に話し手がいるときにカメラがホワイトボードの位置に移動しない場合は、次のことを確認してウィザードに必要な手順をやり直してください。

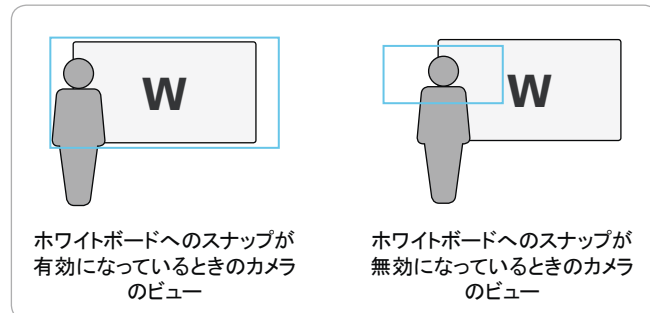
- ・ ホワイトボードがカメラから部屋の反対側に配置されていることを確認します。
- ・ カメラとホワイトボードの距離が正確に測定されていることを確認します。
- ・ 話し手はホワイトボードの近くにいる必要があります。さらに、音声はホワイトボード領域の上半分から発せられるようにまっすぐに立つ必要があります。

ホワイトボードへのスナップ機能の設定 (3/3 ページ)

ホワイトボードへのスナップ機能の有効化および無効化

ホワイトボードへのスナップ機能は、タッチ コントローラの [設定 (Settings)] メニューまたは Web インターフェイスから有効/無効にできます。

i タッチ コントローラで [設定 (Settings)] メニューが開いている (ADMIN パスフレーズで保護されていない) 場合は、会議中または会議と会議の間に任意のユーザがこの機能のオン/オフを切り替えることができます。さらに、任意のユーザが機能を再設定できます。



タッチ コントローラから

1. タッチ コントローラの左上隅にある連絡先情報をタップし、[設定 (Settings)] メニューを開きます。
2. [ホワイトボードへのスナップ (Snap to Whiteboard)] をタップします。

ビデオ システムで [設定 (Settings)] メニューがパス フレーズによって保護されている場合は、ADMIN クレデンシャルでサインインします。

3. トグル スイッチを次のように設定します。

[有効 (Enabled)]: ホワイトボードへのスナップが有効になり、カメラが話し手とその隣りにあるホワイトボードの両方をキャプチャします。

[無効 (Disabled)]: ホワイトボードへのスナップが無効になり、カメラは話し手のみをキャプチャします。

Web インターフェイスから

1. Web 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. [カメラ (Camera)] > [スピーカートラック (SpeakerTrack)] > [ホワイトボード (Whiteboard)] > [モード (Mode)] 設定を見つけます。

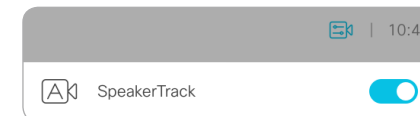
On: ホワイトボードへのスナップが有効になり、カメラが話し手とその隣りにあるホワイトボードの両方をキャプチャします。

Off: ホワイトボードへのスナップが無効になり、カメラは話し手のみをキャプチャします。

スピーカー トラッキングを切り替える方法

ホワイトボードへのスナップ拡張機能が動作するように、いつでもユーザがオン/オフを切り替えることができるスピーカー トラッキングをオンに設定しておく必要があります。

タッチ コントローラのステータス バーにあるカメラ アイコンをタップし、トグル ボタンを使用してスピーカー トラッキングのオン/オフを切り替えます。



Touch 10 コントローラの接続 (1/4 ページ)

Touch 10は、ビデオ システムに直接接続するか(このページの説明を参照)、またはネットワーク(LAN)経由でビデオ システムとペアリングする(次のページの説明を参照)必要があります。後者はリモート ペアリングと呼ばれます。

Touch 10 とビデオ システムの直接接続

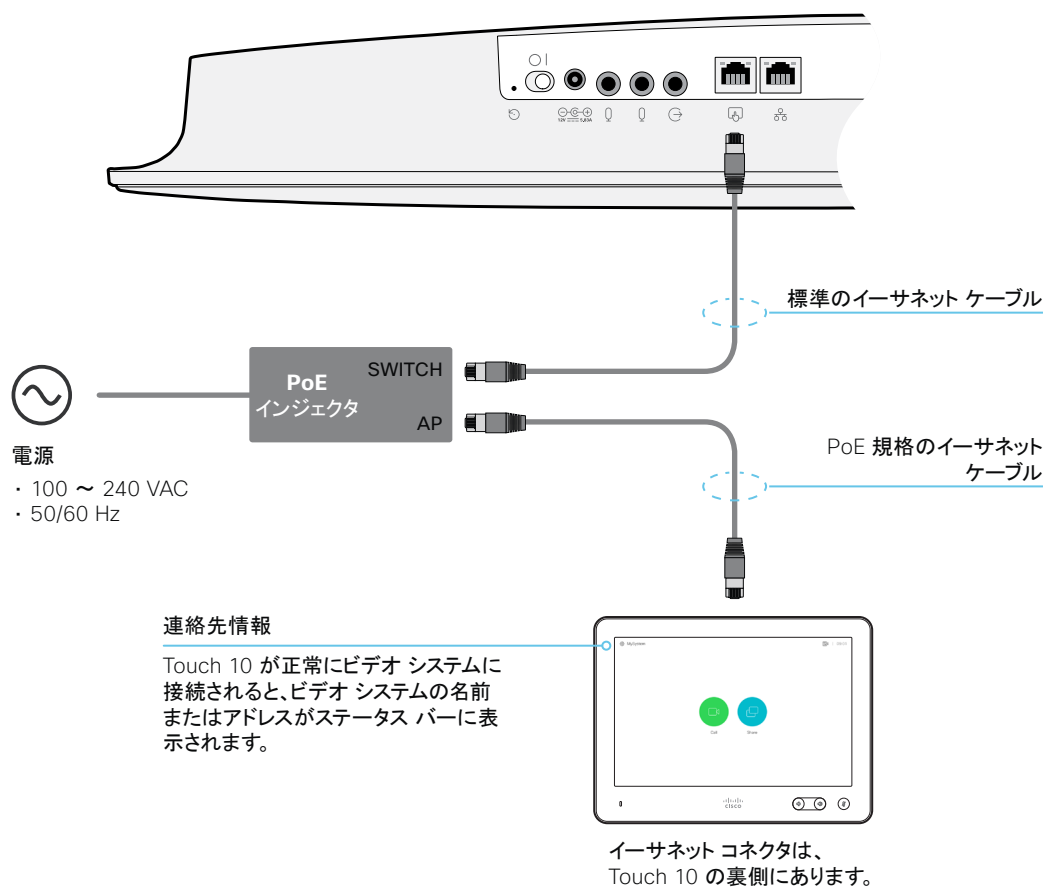
図のように、Touch 10 をビデオシステムの Touch 専用(RJ-45)ポートに接続します。

ビデオ システムは Power over Ethernet(PoE)を提供していないため、Touch 10 に電源を供給するためのミッドスパン PoE インジェクタが必要であることに注意してください。

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。

Touch 10 にソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがビデオ システム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。



Touch 10 コントローラの接続 (2/4 ページ)

ネットワーク(LAN)経由での Touch 10 のビデオ システムへの接続

図のように、Touch 10 とビデオ システムを壁のネットワーク 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。

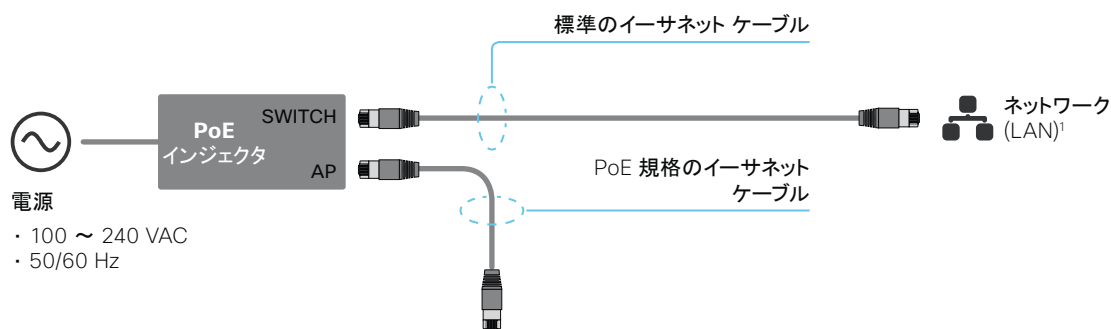
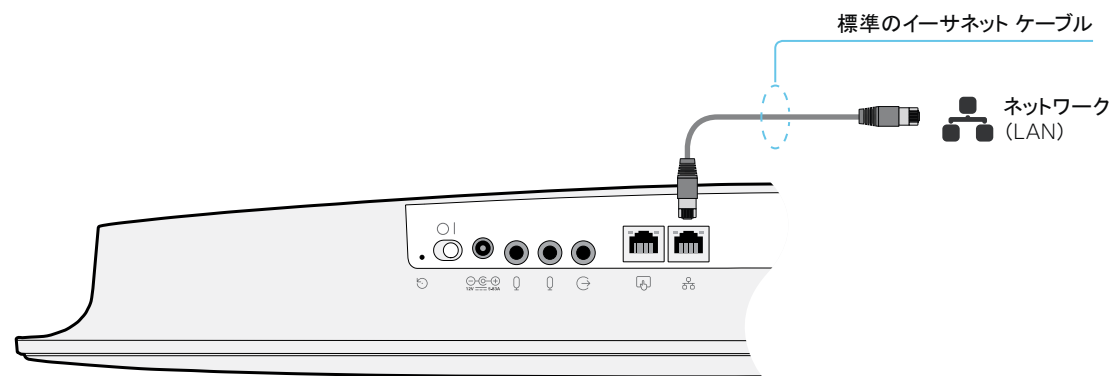
- ペアリング可能なシグナリング中ビデオ システムのリストが、画面に表示されます。ペアリングするビデオ システムの名前をタップします。
ビデオ システムをリストに表示するには、次を満たしている必要があることに注意してください。

- ビデオ システムおよび Touch 10 が同じサブネット上にある必要があります。
- ビデオ システムは、直近の 10 分間に再起動されている必要があります。ビデオ システムがリストに表示されない場合は、再起動してください。
- ビデオ システムが利用可能システムのリストに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。[\[Login\]](#) 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。

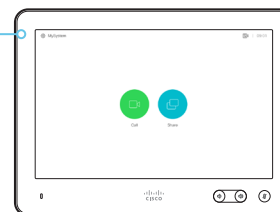
ユーザ アカウントを作成してそれにロールを割り当てる方法の詳細については、[「ユーザ管理」](#)の章を参照してください。

Touch 10 にソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがビデオ システム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。



接点情報

Touch 10 が正常にビデオ システムにペアリングされると、ビデオ システムの名前またはアドレスがステータス バーに表示されます。



イーサネット コネクタは、Touch 10 の裏側にあります。

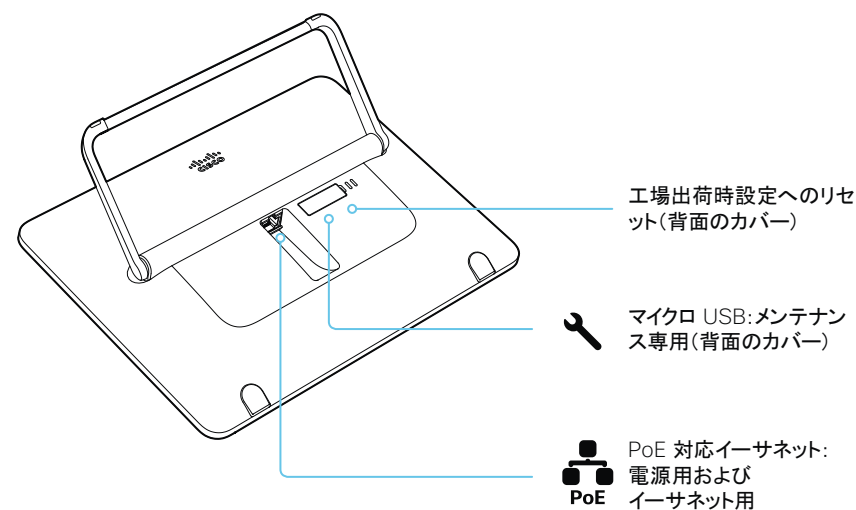
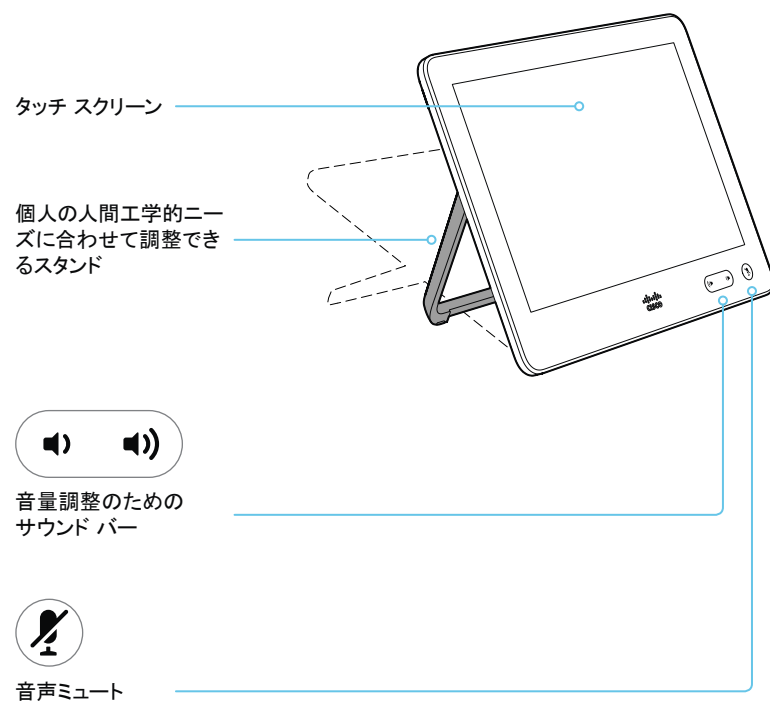
¹ ネットワーク インフラストラクチャが Power over Ethernet (PoE) を提供する場合、PoE インジェクタは必要ありません。タッチ 10 は PoE 規格のイーサネット ケーブルで直接壁面のソケット (イーサネット スイッチ) に接続する必要があります。

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 (4/3 ページ)

Cisco Touch 10 の物理インターフェイス

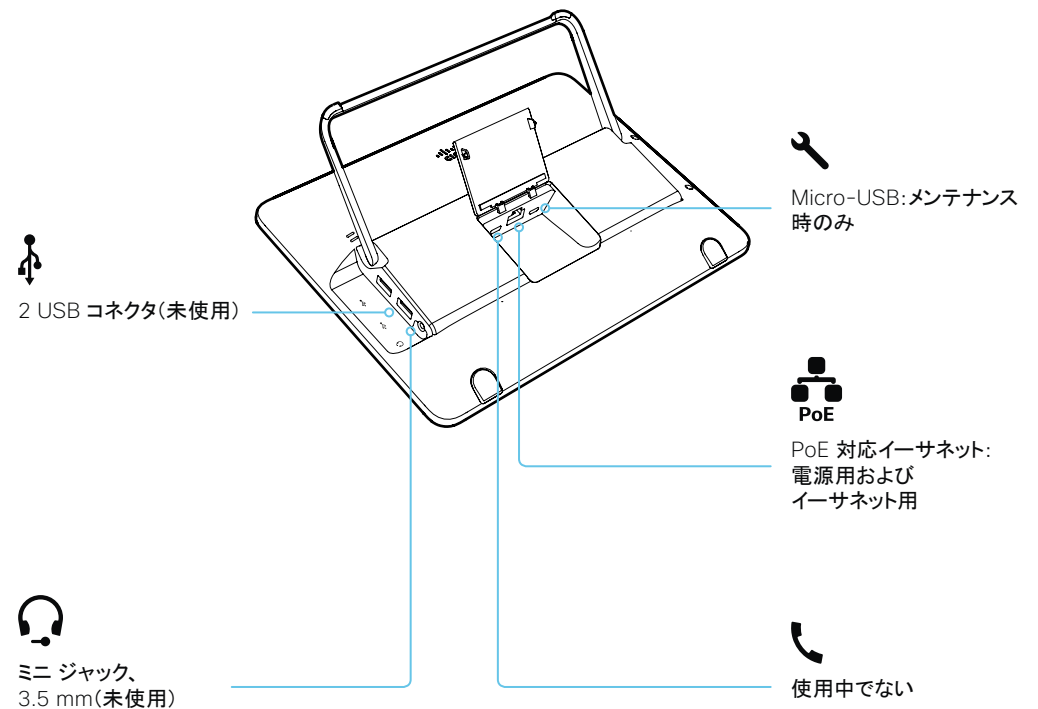
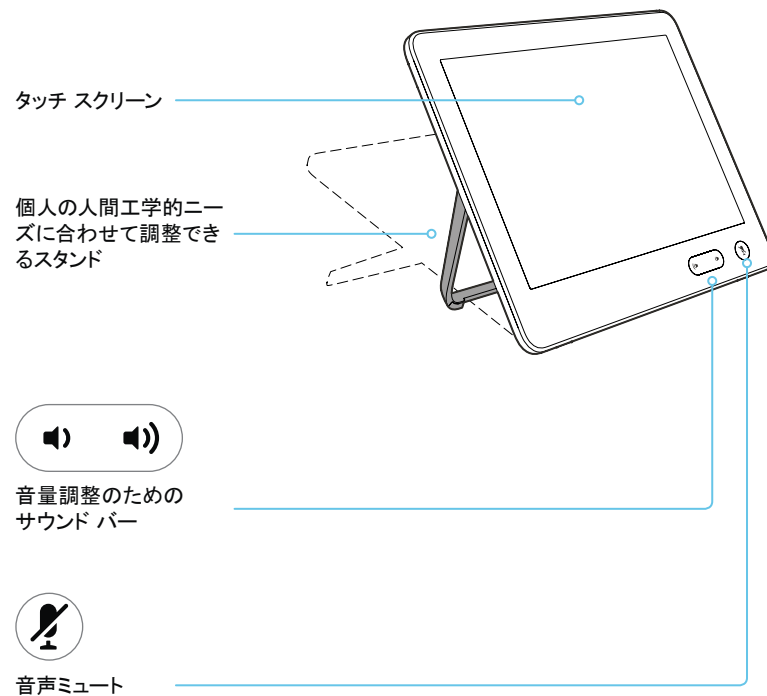
これは、2017 年後半に提供が開始された Touch 10 コントローラの新しいバージョンです。以前のバージョンと同じ機能を備えていますが、物理インターフェイスが多少異なります。新しいデバイスは、前面のロゴと、背面のコネクタが少ないことによって識別できます。



Touch 10 コントローラの接続 (4/4 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 リンクは、ビデオ システムが ISDN 回線を使用して接続することを可能にします。また、PSTN(公衆電話交換網)を介したビデオ コールと電話の両方を可能にします。

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 システムの Web インターフェイスから管理されます。Web インターフェイスにサインインして、[\[セットアップ\(Setup\)\]](#) > [\[周辺機器\(Peripherals\)\]](#) に移動します。

要件:

- ISDN リンクは、IL1.1.7 以降のソフトウェアを実行している必要があります。
- ビデオ システム(コーデック)は、CE9.3 以降のソフトウェアを実行している必要があります。ビデオ システムが TC ソフトウェアから CE ソフトウェアに変換された後に、ISDN リンクをビデオ システムと再ペアリングする必要があります。
- ビデオ エンドポイントは、ISDN リンクと通信するために、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ボロジを確認してください。
- ビデオ システムおよび 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。

制限事項:

- Cisco Webex クラウド サービスに登録されているビデオ システムでは、ISDN リンクを使用できません。

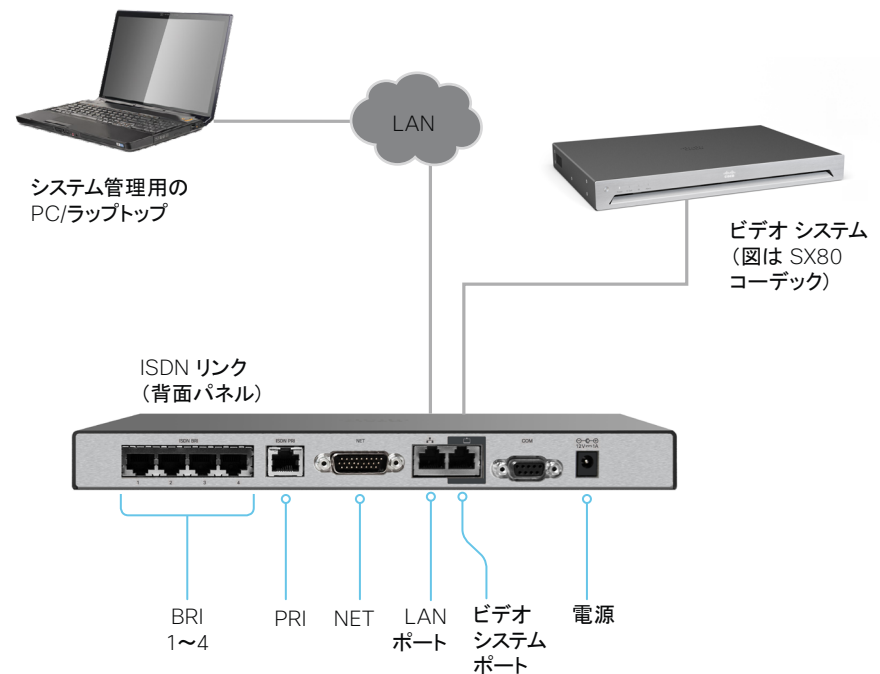
セットアップと構成

ビデオ システムを TC(TC6 以降)から CE ソフトウェア(CE9.3 以降)に変換すると、セキュリティ上の理由により、ISDN リンクのペアリングが自動的に解除されます。

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> [英語] を参照してください。

LAN およびビデオ システムと ISDN リンクの間の直接接続によるセットアップ

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



第 4 章

メンテナンス

システム ソフトウェアのアップグレード

Web 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

ソフトウェアをダウンロードするには、Cisco Download Software Web ページ (<https://software.cisco.com/download/home>) にアクセスし、お使いの製品のページにアクセスします。

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。ファイル名の形式は、「s53200ce9_5_x.cop.sgn」になります。

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。

参照先: <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html> [\[英語\]](#)

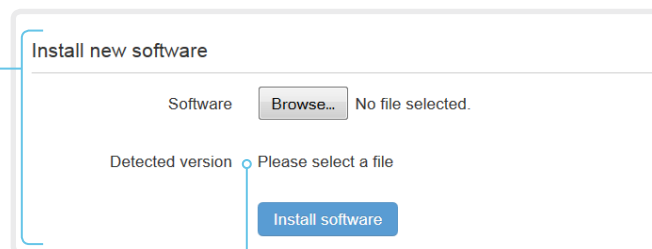
新しいソフトウェアのインストール

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。Web ページから進捗状況を確認できます。インストール後に、ビデオ システムが自動的に再起動します。

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



新しいソフトウェア バージョンの確認

ファイルを選択すると、ここにソフトウェアのバージョンが表示されます。

ソフトウェア バージョンについて

このビデオ会議システムは CE ソフトウェアを使用しています。このドキュメントに記載されているバージョンは、CE9.5.x です。

オプション キーを追加する

Web 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、ビデオ システムにインストールされていないオプション キーのリストが表示されます。

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

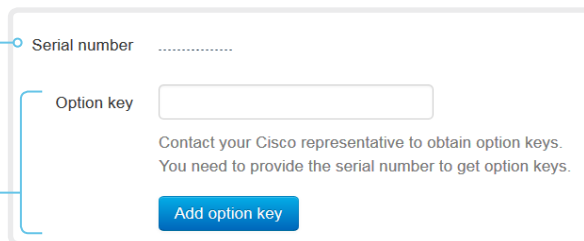
ビデオ システムのシリアル番号。

オプション キーの注文時にはビデオ システム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。



Serial number

Option key

Contact your Cisco representative to obtain option keys.
You need to provide the serial number to get option keys.

[Add option key](#)

オプション キーについて

ビデオ システムには、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、またはインストールされていない場合があります。オプションの機能をアクティブするには、対応するオプション キーがビデオ システムに存在する必要があります。

各ビデオ システムには一意のオプション キーがあります。

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。

システム ステータス

システム情報の概要

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

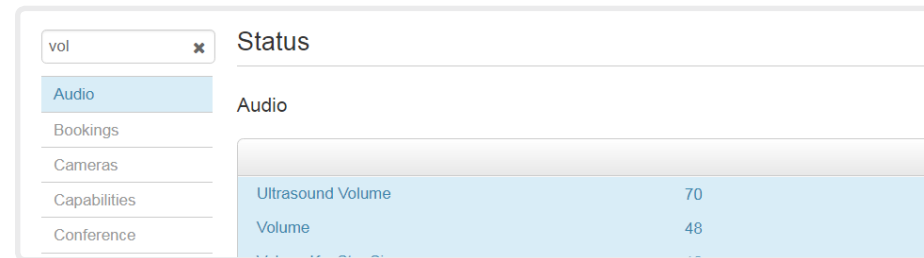
このページには、製品タイプ、システム名、およびハードウェア、ソフトウェア、インストール済みオプション、ネットワーク アドレスに関する基本情報が表示されます。ビデオ ネットワーク(SIP および H.323)の登録ステータスのほか、システムにコールする際に使用する番号および URI も含まれます。

システム ステータスの詳細

Web インターフェイスにサインインして、[セットアップ(Setup)] > [ステータス(Status)] に移動し、より詳細なステータス情報を探します。

ステータス エントリを検索する

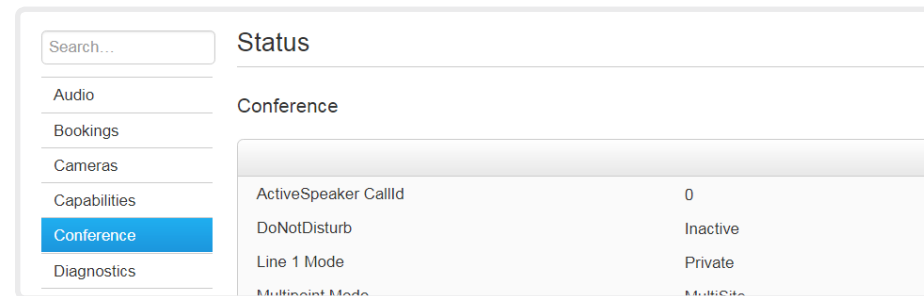
検索フィールドに必要な数の文字を入力します。これらの文字が含まれているすべてのエントリが右側のペインに表示されます。値スペースにこれらの文字が含まれているエントリも表示されます。



Status	
Audio	Audio
Bookings	
Cameras	
Capabilities	
Conference	
Search...	
Ultrasound Volume	70
Volume	48

カテゴリを選択して適切なステータスに移動する

システム ステータスはカテゴリ別にグループ化されます。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。



Status	
Audio	Audio
Bookings	
Cameras	
Capabilities	
Conference	Conference
Diagnostics	
Search...	
ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private
Multicast Mode	MultiSite

* 図に示しているステータスは一例です。お使いのシステムのステータスとは異なる場合があります。

診断の実行

Web インターフェイスにサインインして、[\[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*。

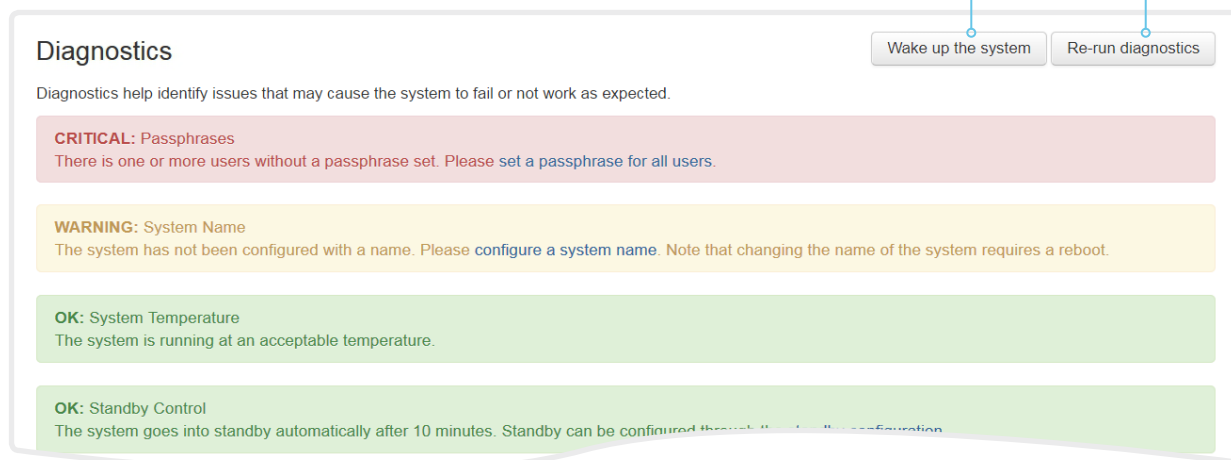
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

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ビデオシステムを復帰させるには、[\[システムの起動 \(Wake up the system\)\]](#) をクリックします。



Diagnostics

Wake up the system Re-run diagnostics

Diagnostics help identify issues that may cause the system to fail or not work as expected.

CRITICAL: Passphrases
There is one or more users without a passphrase set. Please [set a passphrase for all users](#).

WARNING: System Name
The system has not been configured with a name. Please [configure a system name](#). Note that changing the name of the system requires a reboot.

OK: System Temperature
The system is running at an acceptable temperature.

OK: Standby Control
The system goes into standby automatically after 10 minutes. Standby can be configured through the [system configuration](#).

* 図に示しているメッセージは一例ですお使いのシステム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

Web 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

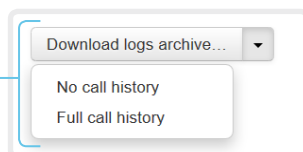
[\[ログ アーカイブのダウンロード... \(Download logs archive...\)\]](#) をクリックして、手順に従います。

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 Web 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。



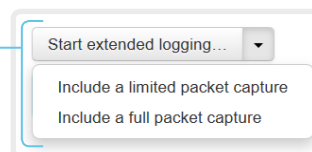
拡張ロギングの開始

[\[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 ファイルについて

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

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

ビデオ システム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。

拡張ロギングはビデオ システムのリソースをより多く使用するため、ビデオ システムの動作が標準を下回る場合があります。拡張ロギングモードは、トラブルシューティングのときにのみ使用してください。



ログ ファイル 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。

リモート サポート ユーザを作成する

Web インターフェイスにログインし、[\[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。

The system does not have an active Remote Support User.

Create user

Delete user

This user is valid until
2018-10-05 16:50:18

Token

```
bgD9FjGyIUNn0TB71KcmT1FPnx6uY0vTFy9kpiUa5z1+b
TQek1PaSpsQJNEMfzThgbvK4J7pgOyt4lmCyvxWPGipJQ
GL0ynjvHBvhfqYEsSWwCSSZxQ1wP6bUPQzOSgztZnkOG7
e9CpAoRNq+mZMqEG1lsswKPZ7HYu1vyVTH/XuPzU7Nues
9pwzLc8BFgBt1xV0fKeoeOmMX+it1Ecamln41nXlScgOt
yPSXiFWLdKAJsQHJQH20PCxxYcnEUYNpAoJiD39edLy4
etY+/SATwBIiohrqF9JLW9FfNEF+IyDlwUmYkPoEirBj7
N3Zvpivlv1Z7+NUalQW9qWTj4Ag==
```

The system has an active Remote Support User.

Create user

Delete user

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

ビデオ システムの問題を診断する場合、リモート サポート ユーザを作成できます。

リモート サポート ユーザにはシステムへの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

Web 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。次の要素からバンドルに含めるものを選択できます。

- ・ ブランディング イメージ
- ・ マクロ
- ・ お気に入り
- ・ サインイン パナー
- ・ 室内制御パネル
- ・ 構成/設定(すべてまたは一部)

バックアップ ファイルは、ビデオ システムの Web インターフェイスから手動で復元できますが、Cisco UCM または TMS などを使用して複数のビデオ システム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(次の章を参照してください)。

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。
現在ビデオ システム上に存在しない要素はグレー表示されます。
3. バックアップ ファイルに含める設定(ある場合)を選択します。次の点に注意してください。
 - ・ デフォルトでは、すべての設定がバックアップ ファイルに含まれます。
 - ・ Web 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。
 - ・ あるビデオ システム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、他のビデオ システムでバックアップ 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、有効にするためにビデオ システム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

ビデオ システムでマクロを含むバックアップ ファイルを復元する場合、以下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

▶ 「構成とカスタム要素のバックアップと復元」の章で説明されているとおり、バックアップ ファイルは、さまざまなビデオシステムのカスタマイズ 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
- ・ HTTP または HTTPS のビデオ システムによって到達可能なカスタム Web サーバ。

ビデオ システムが CUCM(Cisco Unified Communications Manager) からカスタマイズ テンプレートの名前および格納場所に関する情報を取得する際は、ビデオ システムがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。



構成はビデオ システム上では復元されません。これは、構成がカスタマイズ テンプレートとして使用するバックアップ ファイルの一部である場合でも同じです。

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. [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. [Upload File] をクリックします。

各ビデオ システムへのカスタマイズ 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 [構成の適用 (Apply Config)] をクリックし、構成をビデオ システムにプッシュします。

* 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ビデオ システムにファイルを復元することにより、ファイルの SHA512 チェックサムを検索できます。

1. Web 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-manager-callmanager/tsd-products-support-series-home.html> [英語]

カスタム要素の TMS プロビジョニング

► [Backup and restore configurations and custom elements](#) の章で説明されているとおり、バックアップ ファイルは、さまざまなビデオシステムのカスタマイズ 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、HTTP または HTTPS のビデオ システムによって到達可能なカスタム Web サーバ上にホストされる必要があります。

ビデオ システムが TMS (TelePresence Management Suite) からバックアップ ファイルの名前および位置に関する情報を取得する際は、ビデオ システムがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

構成テンプレートの作成と適用

1. 構成テンプレートを作成します。
2. 次の XML 文字列を含むカスタム コマンドを構成テンプレートに追加します。

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

where

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

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

`origin`: Provisioning *

3. 構成テンプレートをプッシュするビデオ システムを選択し、[\[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](#) [英語] 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ビデオシステムにファイルを復元することにより、ファイルの SHA512 チェックサムを検索できます。

1. Web 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、バックアップ ファイルの一部である構成もビデオ システムにプッシュされます。バックアップ ファイルに、特定のビデオ システムに固有の構成 (静的 IP アドレス、システム名、連絡先情報など) が含まれている場合、到達不能なビデオ システムで実行される可能性もあります。

以前に使用していたソフトウェア イメージに復元する

Web 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。

以前使用していたソフトウェア イメージに交換する前に、ビデオ システムのログ ファイル、構成、およびカスタム要素をバックアップすることをお勧めします。

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、シスコ 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。

システムがリセットされるまでお待ちください。終了するとシステムは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

ビデオ システムに重大な問題がある場合は、以前使用していたソフトウェア イメージに切り替えることで、問題の解決に役立つ場合があります。

ソフトウェアを最後にアップグレードしてからシステムを工場出荷時設定にリセットしていない場合は、これまで使用していたソフトウェア イメージがシステムに存在しています。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 システムの工場出荷時設定リセット (1/3 ページ)

ビデオ システムに重大な問題が発生した場合、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。多くの場合これでシステムをリカバリします。ソフトウェアのスワップ(切り替え)については、[▶ Revert to the previously used software image](#) の章を参照してください。

ビデオ システムを初期設定の状態へリセットするには、Web インターフェイスまたはユーザ インターフェイスを使用することを推奨します。これらのインターフェイスが利用できない場合は、pin ホールをリセット(reset pin-hole)使います。

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。
- ・ すべてのシステム パラメータがデフォルト値にリセットされます。
- ・ システムにアップロード済みのファイルが、すべて削除されます。リセットされる内容には、カスタムの壁紙、証明書、およびお気に入りリストが含まれますが、これに限定されません。
- ・ 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。

工場出荷時設定リセット後、ビデオ システム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。

初期設定へのリセットを実行する前に、ビデオ システムのログ 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は、データが消失する場合があります。

ビデオ システムの工場出荷時設定リセット (2/3 ページ)

Web インターフェイスを使用した初期設定へのリセット

初期設定へのリセットを行う前に、ビデオ システムのログ 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。

Web 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 \(Perform a factory reset...\)\]](#) をクリックします。
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. ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了すると、ビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[\[ようこそ \(Welcome\)\]](#) 画面が表示されます。

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進める前に、ビデオ システムのログ 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 インターフェイスの左上隅にある連絡先情報を選択します。
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. [\[はい \(Yes\)\]](#) をクリックして選択を確定するか、[\[戻る \(Back\)\]](#) をクリックして操作を取り止めます。
5. ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了すると、ビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[\[ようこそ \(Welcome\)\]](#) 画面が表示されます。

ログ ファイル、構成、カスタム要素のバックアップ

Web 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。

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。

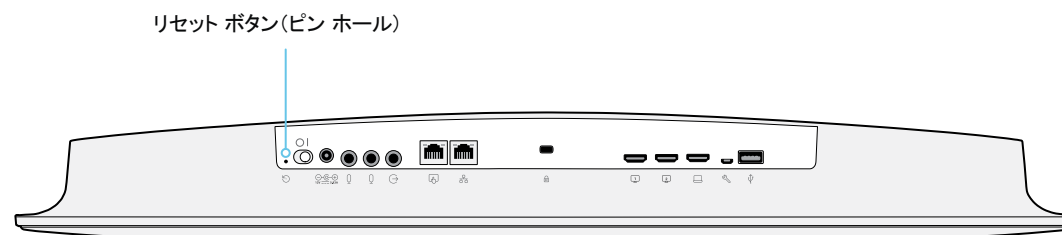
ビデオ システムの工場出荷時設定リセット (3/3 ページ)

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進める前に、ビデオ システムのログ 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. ユニットを前に傾け、リセット ボタン(ピン ホール)が見えるようにします。
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. ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了すると、ビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ(Welcome)] 画面が表示されます。



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な場合があります。その場合は、必ずスコ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 コントローラを工場出荷時設定にリセットすると、ペアリング情報が失われ、(ビデオ システムではなく) タッチ自体が工場出荷時の初期状態に戻されます。



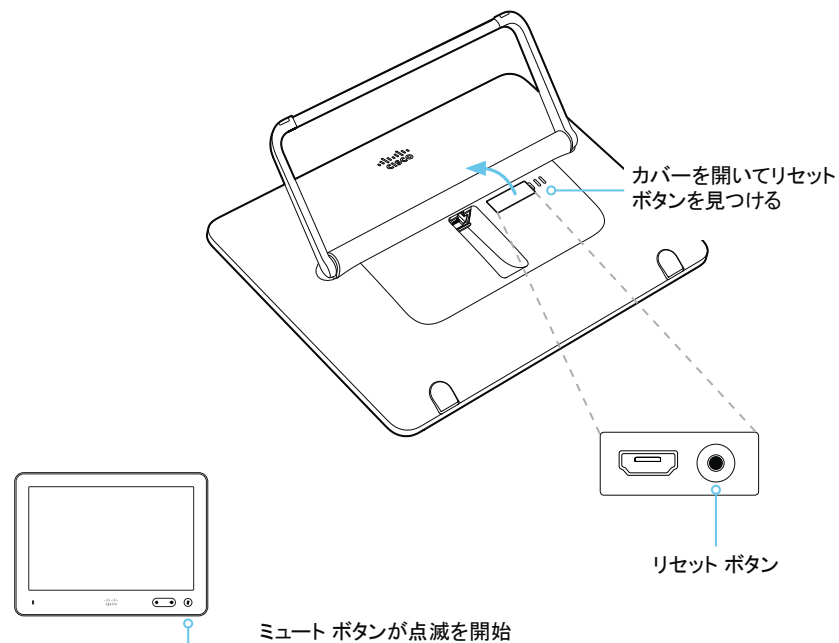
初期設定にリセットすると元に戻すことはできません。

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 がビデオ システムに直接接続されている場合は、新しい設定がビデオ システムから自動的に受信されます。

Touch 10 が LAN 経由で接続されている場合は、新たにデバイスをビデオ システムに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、新しい設定がビデオ システムから自動的に受信されます。



ペアリングについて、およびビデオ システムに Touch 10 を接続する方法について

Touch 10 コントローラを使用するには、Touch 10 をコードブックに直接接続するか、LAN 経由でコードブックにペアリング (リモート ペアリング) する必要があります。後者はリモート ペアリングと呼ばれます。

ペアリング、および Touch 10 とビデオ システムの接続方法については、▶ [「Touch 10 コントローラの接続」](#)「Touch 10 コントローラの接続」

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な場合があります。その場合は、必ずシスコ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 コントローラを工場出荷時設定にリセットすると、ペアリング情報が失われ、(ビデオ システムではなく) タッチ自体が工場出荷時の初期状態に戻されます。



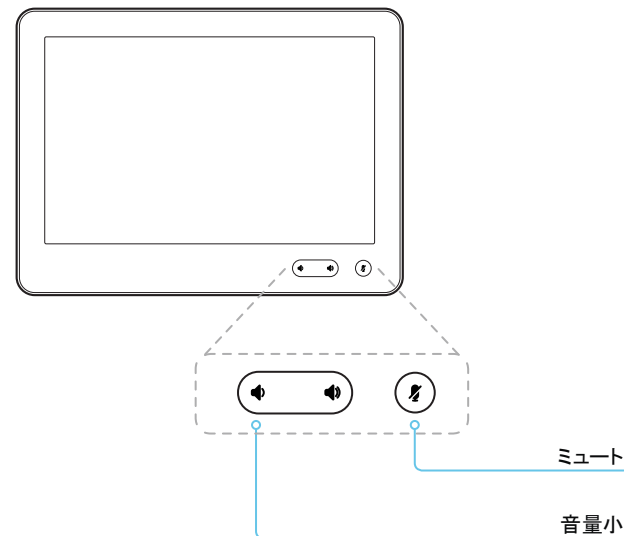
初期設定にリセットすると元に戻すことはできません。

1. **Mute** および **Volume down** ボタンを見つけます。
2. (赤と緑が) 点滅しはじめるまで、**Mute** ボタンを押します。約 10 秒かかります。
3. **Volume down** 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 がビデオ システムに直接接続されている場合は、新しい設定がビデオ システムから自動的に受信されます。

Touch 10 が LAN 経由で接続されている場合は、新たにデバイスをビデオ システムに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、新しい設定がビデオ システムから自動的に受信されます。



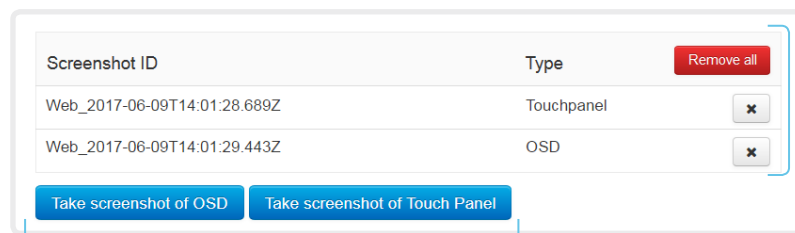
ペアリングについて、およびビデオ システムに Touch 10 を接続する方法について

Touch 10 コントローラを使用するには、Touch 10 をコードブックに直接接続するか、LAN 経由でコードブックにペアリング (リモート ペアリング) する必要があります。後者はリモート ペアリングと呼ばれます。

ペアリング、および Touch 10 とビデオ システムの接続方法については、▶ [「Touch 10 コントローラの接続」](#)

ユーザ インターフェイスのスクリーンショットをキャプチャする

Web インターフェイスにサインインして、[\[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 パネルのスクリーンショットを撮る \(Take screenshot of Touch Panel\)\]](#) をクリックしてタッチ コントローラのスクリーンショットをキャプチャするか、[\[OSD のスクリーンショットを撮る \(Take screenshot of OSD\)\]](#) をクリックして画面上の表示のスクリーンショットをキャプチャします。

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 **x** ボタンをクリックします。

ユーザ インターフェイスのスクリーンショットについて

ビデオ システムに接続された タッチ コントローラと、画面上の表示(メイン ディスプレイのメニュー、インジケータ、メッセージ)の両方のスクリーンショットをキャプチャできます。

第 5 章

システム設定

システム設定の概要

これ以降のページでは、Web インターフェイス上の [\[セットアップ\(Setup\)\]](#) > [\[設定\(Configuration\)\]](#) ページで設定されるすべてのシステム設定をリストします。

Web ブラウザを開き、ビデオ システムの IP アドレスを入力して、サインインします。



IP アドレスの確認方法

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
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。

Audio 設定	93
Audio DefaultVolume.....	93
Audio Input Microphone [1..3] Mode.....	94
Audio Input Microphone [2..3] EchoControl Mode.....	93
Audio Input Microphone [2..3] EchoControl Dereverberation	93
Audio Input Microphone [2..3] EchoControl NoiseReduction.....	93
Audio Input Microphone [2..3] Level.....	94
Audio Output InternalSpeaker Mode.....	95
Audio Output Line [1..1] Mode	95
Audio Output Line [1..1] OutputType.....	95
Audio SoundsAndAlerts RingTone.....	95
Audio SoundsAndAlerts RingVolume.....	95
Audio Ultrasound MaxVolume.....	96
Audio Ultrasound Mode	96
Audio KeyClickDetector Enabled	94
Audio Microphones Mute Enabled.....	95
Audio KeyClickDetector Attenuate.....	94
CallHistory 設定	97
CallHistory Mode.....	97
Cameras settings	98
Cameras SpeakerTrack Closeup.....	98
Cameras SpeakerTrack Whiteboard Mode	99
Cameras SpeakerTrack Mode.....	98
Cameras Camera Framerate.....	98
Cameras PowerLine Frequency.....	98
Conference settings	100
Conference ActiveControl Mode.....	100
Conference AutoAnswer Delay.....	100
Conference AutoAnswer Mode	100
Conference AutoAnswer Mute	100
Conference CallProtocolIPStack.....	100
Conference DefaultCall Protocol	101
Conference DefaultCall Rate.....	101
Conference DoNotDisturb DefaultTimeout	101
Conference Encryption Mode.....	101

Conference FarEndControl Mode	101	Macros settings	110
Conference FarEndControl SignalCapability	102	Macros AutoStart	110
Conference MaxReceiveCallRate	102	Macros Mode	110
Conference MaxTotalReceiveCallRate	102	Network settings	111
Conference MaxTotalTransmitCallRate	103	Network [1..1] DNS DNSSEC Mode	111
Conference MaxTransmitCallRate	102	Network [1..1] IEEE8021X Eap Md5	112
Conference MicUnmuteOnDisconnect Mode	103	Network [1..1] IEEE8021X Password	112
Conference Multipoint Mode	103	Network [1..1] IPv4 Gateway	113
Conference Presentation OnPlacedOnHold	104	Network [1..1] IPv6 Address	114
Conference Presentation RelayQuality	104	Network [1..1] MTU	115
Conference VideoBandwidth Mode	104	Network [1..1] RemoteAccess Allow	117
Conference MultiStream Mode	103	Network [1..1] Speed	117
Conference IncomingMultisiteCall Mode	104	Network [1..1] VLAN Voice Mode	117
Conference FarEndMessage Mode	102	Network [1..1] VLAN Voice VlanId	117
FacilityService 設定	105	Network [1..1] DNS DNS Server [1..3] Address	111
FacilityService Service [1..5] CallType	105	Network [1..1] DNS Domain Name	111
FacilityService Service [1..5] Name	105	Network [1..1] IEEE8021X Eap Peap	113
FacilityService Service [1..5] Number	105	Network [1..1] IEEE8021X Eap Tls	113
FacilityService Service [1..5] Type	105	Network [1..1] IEEE8021X Eap Ttls	112
H323 設定	106	Network [1..1] IEEE8021X TlsVerify	111
H323 Authentication LoginName	106	Network [1..1] IEEE8021X Identity	112
H323 Authentication Mode	106	Network [1..1] IEEE8021X UseClientCertificate	112
H323 Authentication Password	106	Network [1..1] IEEE8021X Mode	111
H323 CallSetup Mode	106	Network [1..1] IEEE8021X AnonymousIdentity	112
H323 Encryption KeySize	107	Network [1..1] IPv4 Address	113
H323 Gatekeeper Address	107	Network [1..1] IPv4 SubnetMask	114
H323 H323Alias E164	107	Network [1..1] IPv4 Assignment	113
H323 H323Alias ID	107	Network [1..1] IPv6 DHCP Options	114
H323 NAT Address	108	Network [1..1] IPv6 Gateway	114
H323 NAT Mode	107	Network [1..1] IPv6 Assignment	114
H323 PortAllocation	108	Network [1..1] IP Stack	113
Logging settings	109	Network [1..1] QoS Diffserv ICMPv6	116
Logging External Mode	109	Network [1..1] QoS Diffserv NTP	116
Logging External Protocol	109	Network [1..1] QoS Diffserv Audio	115
Logging External Server Address	109	Network [1..1] QoS Diffserv Signalling	116
Logging External Server Port	109	Network [1..1] QoS Diffserv Data	116
Logging Mode	109	Network [1..1] QoS Diffserv Video	115
		Network [1..1] QoS Mode	115
		Network [1..1] TrafficControl Mode	117

NetworkServices settings	118	Phonebook settings	127
NetworkServices CDP Mode.....	118	Phonebook Server [1..1] ID.....	127
NetworkServices H323 Mode.....	118	Phonebook Server [1..1] URL.....	127
NetworkServices HTTP Mode.....	118	Phonebook Server [1..1] Type.....	127
NetworkServices HTTP Proxy LoginName.....	118		
NetworkServices HTTP Proxy Mode.....	119	Provisioning 設定	128
NetworkServices HTTP Proxy PACUrl.....	119	Provisioning Connectivity.....	128
NetworkServices HTTP Proxy Password.....	119	Provisioning ExternalManager Address.....	128
NetworkServices HTTP Proxy Url.....	119	Provisioning ExternalManager AlternateAddress.....	128
NetworkServices HTTPS OCSP Mode.....	119	Provisioning ExternalManager Domain.....	129
NetworkServices HTTPS OCSP URL.....	119	Provisioning ExternalManager Path.....	129
NetworkServices HTTPS Server MinimumTLSVersion.....	120	Provisioning ExternalManager Protocol.....	128
NetworkServices HTTPS StrictTransportSecurity.....	120	Provisioning LoginName.....	129
NetworkServices HTTPS VerifyClientCertificate.....	120	Provisioning Mode.....	129
NetworkServices HTTPS VerifyServerCertificate.....	120	Provisioning Password.....	130
NetworkServices NTP Mode.....	120		
NetworkServices NTP Server [1..3] Address.....	121	Proximity 設定	131
NetworkServices SIP Mode.....	121	Proximity Mode.....	131
NetworkServices SNMP CommunityName.....	121	Proximity Services CallControl.....	131
NetworkServices SNMP Host [1..3] Address.....	121	Proximity Services ContentShare FromClients.....	131
NetworkServices SNMP Mode.....	121	Proximity Services ContentShare ToClients.....	131
NetworkServices SNMP SystemContact.....	121		
NetworkServices SNMP SystemLocation.....	122	RoomAnalytics 設定	132
NetworkServices SSH AllowPublicKey.....	122	RoomAnalytics PeopleCountOutOfCall.....	132
NetworkServices SSH Mode.....	122	RoomAnalytics PeoplePresenceDetector.....	132
NetworkServices SSH HostKeyAlgorithm.....	122		
NetworkServices UPnP Mode.....	122	RoomReset 設定	133
NetworkServices UPnP Timeout.....	123	RoomReset Control.....	133
NetworkServices WelcomeText.....	123		
NetworkServices Wifi Allowed.....	123	RTP 設定	134
NetworkServices Wifi Enabled.....	123	RTP Ports Range Start.....	134
NetworkServices XMLAPI Mode.....	124	RTP Ports Range Stop.....	134
		RTP Video Ports Range Start.....	134
		RTP Video Ports Range Stop.....	134
Peripherals settings	125	Security 設定	135
Peripherals Pairing CiscoTouchPanels EmcResilience.....	125	Security Audit Logging Mode.....	135
Peripherals Profile Cameras.....	125	Security Audit OnError Action.....	135
Peripherals Profile ControlSystems.....	125	Security Audit Server Address.....	135
Peripherals Profile TouchPanels.....	126	Security Audit Server PortAssignment.....	136
Peripherals InputDevice Mode.....	125	Security Session InactivityTimeout.....	136
		Security Session MaxSessionsPerUser.....	136

Security Session MaxTotalSessions	137	Standby StandbyAction	143
Security Session ShowLastLogin	137	Standby WakeupAction	143
Security Session FailedLoginsLockoutTime	136	Standby WakeupOnMotionDetection	143
Security Session MaxFailedLogins	136	SystemUnit 設定	144
Security Audit Server Port	136	SystemUnit CrashReporting Advanced	144
SerialPort 設定	138	SystemUnit CrashReporting Mode	144
SerialPort BaudRate	138	SystemUnit CrashReporting Url	144
SerialPort LoginRequired	138	SystemUnit Name	144
SerialPort Mode	138	Time 設定	145
SIP 設定(SIP settings)	139	Time DateFormat	145
SIP ANAT	139	Time TimeFormat	145
SIP Authentication Password	139	Time Zone	146
SIP Authentication UserName	139	UserInterface 設定	148
SIP DefaultTransport	139	UserInterface Accessibility IncomingCallNotification	148
SIP DisplayName	139	UserInterface CustomMessage	148
SIP Ice DefaultCandidate	140	UserInterface KeyTones Mode	149
SIP Ice Mode	140	UserInterface Language	149
SIP ListenPort	140	UserInterface OSD EncryptionIndicator	149
SIP Mailbox	140	UserInterface OSD HalfwakeMessage	149
SIP PreferredIPMedia	141	UserInterface OSD Output	150
SIP PreferredIPSignaling	141	UserInterface SettingsMenu Mode	150
SIP Proxy [1..4] Address	141	UserInterface Wallpaper	150
SIP TlsVerify	141	UserInterface ContactInfo Type	148
SIP Turn DiscoverMode	141	UserInterface Security Mode	150
SIP Turn DropRflx	142	UserManagement の設定	151
SIP Turn Password	142	UserManagement LDAP Admin Filter	151
SIP Turn Server	142	UserManagement LDAP Admin Group	151
SIP Turn UserName	142	UserManagement LDAP Attribute	151
SIP Type	142	UserManagement LDAP BaseDN	151
SIP URI	142	UserManagement LDAP Encryption	151
SIP MinimumTLSVersion	141	UserManagement LDAP MinimumTLSVersion	152
SIP Line	140	UserManagement LDAP Mode	152
Standby 設定	143	UserManagement LDAP Server Address	152
Standby BootAction	143	UserManagement LDAP Server Port	152
Standby Control	143	UserManagement LDAP VerifyServerCertificate	152
Standby Delay	143		

Video 設定	153
Video ActiveSpeaker DefaultPIPPosition	153
Video DefaultLayoutFamily Local	153
Video DefaultLayoutFamily Remote	154
Video DefaultMainSource	154
Video Input Connector [1..2] CameraControl Mode	154
Video Input Connector [1..2] OptimalDefinition Profile	155
Video Input Connector [2..2] CEC Mode	154
Video Input Connector [2..2] PreferredResolution	155
Video Input Connector [2..2] PresentationSelection	156
Video Input Connector [2..2] Quality	156
Video Input Connector [2..2] RGBQuantizationRange	156
Video Output Connector [1..2] CEC Mode	157
Video Output Connector [1..2] Location HorizontalOffset	158
Video Output Connector [1..2] Location VerticalOffset	158
Video Output Connector [1..2] MonitorRole	159
Video Output Connector [1..2] Resolution	159
Video Output Connector [1..2] RGBQuantizationRange	160
Video Presentation DefaultPIPPosition	160
Video Presentation DefaultSource	160
Video Selfview Default FullscreenMode	160
Video Selfview Default Mode	161
Video Selfview Default OnMonitorRole	161
Video Selfview Default PIPPosition	161
Video Selfview OnCall Duration	162
Video Selfview OnCall Mode	161
Video Monitors	157
Video Input Connector[1..2] CameraControl CameraID	154
Video Input Connector [1..2] InputSourceType	155
Video Input Connector [1..2] Name	155
Video Input Connector [1..2] Visibility	157
Experimental settings	163

Audio 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 システム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、ビデオ システム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

Default value: 50

値スペース: 整数(0..100)

範囲: 1 ~ 100 の値を選択します。これは、-34.5 dB ~ 15 dB の範囲内の 0.5 dB 単位に相当します。0 に設定すると、音声が入力になります。

Audio Input Microphone [2..3] EchoControl Mode

エコー キャンセラは、音声環境で検出された変更があると、室内の音声特性に合わせて継続的に自己調整を行います。音声条件に大幅な変更を加えた場合は、エコー キャンセラの再調整に 1 ~ 2 秒かかることがあります。

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: エコー制御をオフにします。外部のエコー キャンセラもしくは再生機器が使われている場合に推奨します。

On: エコー コントロールをオンにします。一般的には相手先で自らの音声が入力にならないようにするために、オンに設定することが推奨されます。選択すると、エコー キャンセレーションは常にアクティブになります。

Audio Input Microphone [2..3] EchoControl Dereverberation

システムには室内の残響を減らす組み込みの信号処理が備わっています。残響除去を使用するには、Audio Input Microphone [n] EchoControl Mode を有効に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: Off

値スペース: Off/On

Off: 残響をオフにします。

On: 残響除去をオンにします。

Audio Input Microphone [2..3] EchoControl NoiseReduction

システムにはノイズ リダクションが組み込まれており、これにより、定常的なバックグラウンド ノイズ(空調システム、冷却ファンなどのノイズ)が軽減されます。さらに、ハイ パス フィルタ(ハムフィルタ)により、非常に低い周波数のノイズが軽減されます。ノイズ リダクションを使用するには、Audio Input Microphone [n] EchoControl Mode を有効に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: On

値スペース: Off/On

Off: ノイズ リダクションをオフにします。

On: ノイズ リダクションをオンにします。低周波ノイズがある場合、推奨されます。

Audio Input Microphone [2..3] Level

マイクの入力コネクタのゲインを設定します。接続しているオーディオ送信元の出力レベルに合わせて、ゲインを調整する必要があります。ゲインは、1 db ずつ調整できます。

ゲインの設定が高すぎる場合、オーディオ信号がクリップされます。ゲインの設定が低すぎる場合、オーディオの信号対雑音比が低下します。ただし、通常はクリッピングよりも望ましい結果が得られます。

通常、未処理の音声信号は信号レベルが大幅に変動するため、十分な信号のヘッドルームを取れるようにすることが非常に重要だということに注意してください。

0 dB のゲインの最大入力レベルは、-18 dBu です。

例:マイクの最大出力レベルが -40 dBu の場合、ゲインの設定は $-18 \text{ dBu} - (-40 \text{ dBu}) = 22 \text{ dB}$ にしてください。

必要なユーザ ロール:ADMIN, INTEGRATOR

Default value: 14

値スペース:整数(0..26)

範囲:デシベル(dB)単位でゲインを選択します。

Audio Input Microphone [1..3] Mode

マイク コネクタで音声を無効または有効にします。Microphone [1] はビデオ システムの内部マイクです。ので注意してください。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:On

値スペース:Off/On

[オフ(Off)]: 音声入力マイクのコネクタを無効にします。

[オン(On)]: 音声入力マイクのコネクタを有効にします。

Audio KeyClickDetector Attenuate

ビデオ システム(コーデック)は、キーボードのクリック ノイズを検出し、自動的にマイクの信号を減衰することができます。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 クリック検出 有効設定が 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:On

値スペース:Off/On

Off:マイクの信号の減衰は無効です。

On:キーボードのクリック ノイズが検出された場合、システム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

ビデオ システム(コーデック)は、キーボードのクリック ノイズを検出し、自動的にマイクの信号を減衰することができます。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 減衰キー クリック検出(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:Off

値スペース:Off/On

Off:キー クリックの検出は無効です。

On:システム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 Microphones Mute Enabled

ビデオ システムでのマイク ミュートの動作を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: True

値スペース: True/InCallOnly

True: 音声ミュートが使用可能になります。

InCallOnly: 音声ミュートはデバイスがコール中の場合にだけ使用できます。アイドル状態のときは、マイクロフォンをミュートにできません。これは、外部の電話サービス/音声システムがコーデックで接続され、コーデックがコール中でないときに使用可能にする場合に便利です。InCallOnly に設定されたとき、音声システムが誤ってミュートにされることを防止できます。

Audio Output InternalSpeaker Mode

ビデオ システムの内蔵スピーカーを使用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: ビデオ システムの統合スピーカーを無効にします。

On: ビデオ システムの統合スピーカーを有効にします。

Audio Output Line [1..1] モード

音声ライン出力の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: On

値スペース: Off/On

Off: 音声ライン出力を無効にします。

On: 音声ライン出力を有効にします。

Audio Output Line [1..1] OutputType

出力タイプは、接続デバイスに一致するよう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: Loudspeaker (スピーカー)

設定可能な値: LineOut/Loudspeaker/Recorder/Subwoofer (ライン出力/スピーカー/レコーダー/サブウーハー)

Loudspeaker: スピーカーがライン出力に接続されている場合、スピーカーを使用します。このモードでのコネクタ出力レベルは、音量のマスターコントロールと、システムサウンドすべて（着信音、webex アシスタントなど）を含めた出力信号に従って設定されます。

録画機能が回線の出力に接続されている場合は、よく: 使用記録します。このモードでは出力レベルは固定され、システム音は含まれません。音声にはローカルでのプレゼンテーション ソース、ローカルのマイク、およびあらゆる遠隔ソースが含まれます。

Subwoofer: サブウーファーがライン出力に接続されている場合、サブウーファーを使用します。このモードでは、低音はライン出力に送信され、それ以外のオーディオ信号は内蔵スピーカーで再生されます。

LineOut: 他のデバイスのライン出力を使用します。このモードでは、内蔵スピーカーはフルレンジのオーディオを再生します。出力レベルは固定され、システム音声は含まれません。音声にはローカルでのプレゼンテーション ソースおよびあらゆる遠隔ソースが含まれます。

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: Sunrise

値スペース: Sunrise/Mischief/Ripples/Reflections/Vibes/Delight/Evolve/Playful/Ascent/Calculation/Mellow/Ringer

リストから呼び出し音を選択します。

Audio SoundsAndAlerts RingVolume

着信コールの着信音量を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

Default value: 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、Intelligent Proximity 機能に適用されます。設定はデフォルト値のままにしておいてください。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: Dynamic

値スペース: Dynamic/Static

Dynamic: ビデオ システムによって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: シスコ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

Default value: 70

値スペース: 整数 (0..70)

指定されている範囲内の値を選択します。0 に設定すると、超音波がオフになります。

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。

Cameras 設定

Cameras Camera Framerate

デフォルトとして、カメラは 1 秒あたり 30 フレームを出力します。これにより、通常の帯域と照明条件であってもクローズアップと広い視野両方の画像の品質が良くなります。条件がさらに良い場合、カメラから 1 秒あたり 60 フレームの出力となり、全般的に良い品質となる可能性があります。

必要なユーザ ロール: ADMIN

デフォルト値: 30

値スペース: 30/60

30: カメラは、1 秒あたり 30 フレームを出力します。

60: カメラは、1 秒あたり 60 フレームを出力します。

Cameras PowerLine Frequency

カメラが電源周波数フリッカー防止をサポートしている場合、カメラは電源からのすべてのフリッカノイズを補うことができます。このカメラ設定はお使いの電源周波数に基づいて設定する必要があります。カメラが電源周波数の自動検出をサポートしている場合、設定で Auto オプションを選択できます。すべての Cisco Precision カメラはフリッカー防止および電源周波数の自動検出の両方をサポートしています。Auto はデフォルト値であるため、自動検出をサポートしないカメラの場合、この設定を変更する必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: 50Hz/60Hz/Auto

50Hz: 電線周波数が 50 Hz の場合、この値を使用します。

60Hz: 電線周波数が 60 Hz の場合、この値を使用します。

Auto: カメラが電源周波数を自動検出できるようにします。

Cameras SpeakerTrack Mode

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: Auto/Off

Auto: スピーカーのトラッキングはオンです。システムは室内の人々を検出し自動的に最適なカメラ フレーミングを選択します。スピーカー トラッキングのオン/オフは、タッチ コントローラのカメラ コントロール パネルですぐに切り替えることができます。

Off: スピーカー トラッキングがオフになります。

Cameras SpeakerTrack Closeup

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

ルーム内の人が話すと、システムがその人を発見し、最善のカメラ フレーミングを選択します。これはクローズアップと呼ばれ、ルーム内の一部の人は含まれない場合があります。室内のすべての人を常に表示しておきたい場合、クローズ アップ機能をオフにできます。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Auto

値スペース: Auto/Off

Auto: システムは、話している人にズームインします。

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

Cameras SpeakerTrack Whiteboard Mode

[ホワイトボードへのスナップ(Snap to Whiteboard)] 機能はスピーカー トラッキング機能の拡張です。そのため、スピーカー トラッキングをサポートするカメラが必要になります。プレゼンタがホワイトボードの横に立っている場合、Snap to Whiteboard が有効になっていると、カメラはプレゼンタとホワイトボードの両方をキャプチャします。この機能が無効の場合、プレゼンタのみがキャプチャされます。[ホワイトボードへのスナップ(Snap to Whiteboard)] 機能はタッチ コントローラまたは Web インターフェイスで設定されます。

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

Off: Snap to Whiteboard 機能は無効です。

On: Snap to Whiteboard 機能は有効です。

Conference 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 システム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。コールに回答する前に数秒間待機する場合は Conference AutoAnswer Delay 設定を使用し、コールに回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: 通話中でない限り、システムが自動的に着信コールに回答します。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。[自動応答モード (AutoAnswer Mode)] が有効にされている必要があります。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

- Off: 着信コールはミュートにされません。
- On: 着信コールは自動的に応答されるときミュートにされます。

Conference AutoAnswer Delay

システムによって自動的に応答される前に着信コールがどれくらい待つ必要があるかを定義します (秒単位)。[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

Default value: 0

値スペース: 整数 (0..50)

自動応答遅延 (秒単位)。

Conference CallProtocolIPStack

システムで通信プロトコル (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

システムからコールを発信するときに使用されるデフォルトの通信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有効にします。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。システム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 登録済みシステムのために予約されています。使用しません。

Conference DefaultCall Rate

システムからコールを発信するときに使用するデフォルトのコール レートを定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

Default value: 6000

値スペース: 整数 (64..6000)

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

Default value: 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 キーがビデオ システムにインストールされていない場合、暗号化モードは常に 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: システムは、暗号化を使用しません。

On: システムは、暗号化されたコールだけを許可します。

BestEffort: システム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: 遠端システムで暗号化 (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: 遠端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、傾斜、ズーム) を許可されません。

On: 遠端はこちら側のビデオ 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の、ポイントツーポイント通話における 2 種のコーデック間のデータ送信の許可状況を切り替えます。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 つのコーデック間でメッセージ送信を行うことはできません

On:ポイントツーポイント通話で 2 つのコーデック間のメッセージ送信を行うことができます。

Conference MaxReceiveCallRate

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

必要なユーザ ロール:ADMIN

Default value: 6000

値スペース:整数(64..6000)

最大受信帯域(kbps)。

Conference MaxTransmitCallRate

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

必要なユーザ ロール:ADMIN

Default value: 6000

値スペース:整数(64..6000)

最大送信帯域(kbps)。

Conference MaxTotalReceiveCallRate

この設定は、ビデオ システム内蔵の MultiSite 機能(オプション)を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

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

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

必要なユーザ ロール:ADMIN

Default value: 6000

値スペース:整数(64..6000)

最大受信帯域(kbps)。

Conference MaxTotalTransmitCallRate

この設定は、ビデオ システム内蔵の MultiSite 機能(オプション)を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

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

個々のコールの最大送信ビット レートは、Conference MaxTransmitCallRate 設定により定義されます。

必要なユーザ ロール:ADMIN

Default value: 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、このようにして次のユーザのためにシステムを準備する場合があります。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

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

On:コールが切断された後にマイクロフォンのミュートを解除します。

Conference Multipoint Mode

ビデオ システムでマルチパーティビデオ会議(アドホック会議)を処理する方法を定義します。

Cisco TelePresence Video Communication Server(VCS)に登録すると、ビデオ システムで組み込み MultiSite 機能を使用できるようになります。Cisco Unified Communications Manager(CUCM)バージョン 8.6.2 以降にすると、ビデオ システムは、CUCM 会議ブリッジ、または内蔵 MultiSite 機能を使用できます。使用するオプションは CUCM によってセットアップされます。

CUCM 会議ブリッジを使用すれば、多くの参加者との会議をセットアップできます。組み込み MultiSite では、最大 4 人の参加者(自分自身を含む)が許可されます。

組み込みの MultiSite 機能はオプションであり、すべてのビデオ システムで使用できるわけではありません。

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。マルチポイント方式が使用できない場合は、マルチポイント モードがオフに設定されます。

[CUCMMediaResourceGroupList]:マルチパーティ会議は、CUCM で設定された会議ブリッジによってホストされます。この設定は、CUCM 環境で CUCM によってプロビジョニングされるため、ユーザが手動で設定すべきではありません。

[多地点接続(MultiSite)]:組み込み MultiSite 機能を使用してマルチパーティ会議が設定されます。MultiSite 機能を使用できないときに [多地点接続(MultiSite)] が選択された場合、[マルチポイント モード(Multipoint Mode)] は自動的に [オフ(Off)] に設定されます。

Off:マルチパーティ会議は許可されません。

Conference MultiStream Mode

ビデオ システムでは、電話会議のマルチ ストリーム ビデオをサポートしています。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/Off

Auto:電話会議インフラストラクチャがマルチストリーム機能をサポートしている場合は、マルチストリームが使用されます。必要な最低バージョン:CMS 2.2、CUCM 11.5、VCS X8.7。

Off:マルチストリームが無効になります。

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:保留にされてもビデオ システム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 サイトで保留状態にされた後、ビデオ システム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、内蔵 MultiSite 機能(オプション)を使用してマルチポイント ビデオ会議をホストするときに応用されます。リモート ユーザがプレゼンテーションを共有している場合、ビデオ システムは、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ン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せん。

FacilityService 設定

FacilityService Service [1..5] Type

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 [1..5] Name

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 [1..5] Number

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 [1..5] CallType

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:システムは 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、システムはゲートキーパーに対して自身の認証を試みます。コーデック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

システムは認証のために、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。認証はコーデックから H.323 ゲートキーパーへの単方向の認証です。つまり、システム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、システム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

システムは認証のために、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。認証はコーデックから H.323 ゲートキーパーへの単方向の認証です。つまり、システム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、システム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。

[ゲートキーパー (Gatekeeper)]:システムは、H.323 コールを発信するためにゲートキーパーを使用します。このオプションを選択する場合は、H323 Gatekeeper Address も設定する必要があります。

H323 Encryption KeySize

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

必要なユーザ ロール:ADMIN

デフォルト値:Min1024bit

設定可能な値:Max1024bit/Min1024bit/Min2048bit(最大 1024 ビット/最小 1024 ビット/最小 2048 ビット)

Max1024bit:最大サイズは 1024 ビットです。

Min1024bit:最小サイズは 1024 ビットです。

Min2048bit:最小サイズは 2048 ビットです。

H323 Gatekeeper Address

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

H323 H323Alias E164

H.323 エイリアス E.164 は、H.323 ゲートキーパーに設定された番号計画に従ってシステム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 エイリアス E.164 アドレス。使用できる文字は、0 ~ 9、*、# です。

H323 H323Alias ID

H.323 ゲートキーパー上のシステムのアドレス指定に使用され、コール リストに表示される H.323 エイリアス ID 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, 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、外部のビデオ会議システムに接続されたときの音声/ビデオ 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システムが決定します。これにより、LAN 上のエンドポイント、または WAN のエンドポイント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:システムは、実際の IP アドレスをシグナリングします。

On:システムは、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、システム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、次のポートはシステムの 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

* Port 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。

Logging 設定

Logging External Mode

ロギングにリモート syslog サーバを使用するかどうかを決定します。

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:リモート syslog サーバのロギングを無効にします。

On:リモート syslog サーバのロギングを有効にします。

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 に設定されている場合、ビデオ システムで標準の syslog ポートが使用されます。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

Default value: 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、ビデオ システムが標準 syslog ポートを使用することを意味します。

Logging Mode

ビデオ システムのロギング モードを定義します(syslog サービス)。無効にすると、syslog サービスが起動せず、イベント ログの大部分が生成されません。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。

Macros 設定

Macros Mode

マクロを使用して、ビデオ エンドポイントの一部を自動化できる JavaScript コードの一部を記述することができます。このようにしてカスタム動作を作成します。デフォルトではマクロを使用できませんが、初めてマクロ エディタを開くと、コーデックでマクロの使用を有効化するかどうかを尋ねられます。コーデックでのマクロの使用を手動で有効化するか完全に無効化する場合、この設定を使用します。マクロの使用は、マクロ エディター内で無効化できます。ただし、コーデックがマクロをリセットするたびにマクロが自動的に再度有効化されるため、マクロの実行は常時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: このビデオ システム上でのマクロの使用を完全に無効にします。

On: このビデオ システム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 エンドポイントにおいてシングル プロセスで実行します。ランタイムは、デフォルトでは実行されているはずですが、手動での停止や開始を選択できます。自動開始が有効化されている場合、ビデオ システムを再起動するときにランタイムは自動的に再度開始します。

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: ビデオ システムの再起動後、マクロ ランタイムは自動的に開始しません。

On: ビデオ システムの再起動後、マクロ ランタイムが自動的に開始します。

Network 設定

Network [1..1] DNS DNSSEC Mode

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 [1..1] DNS Domain Name

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 [1..1] DNS Server [1..3] Address

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 [1..1] IEEE8021X モード

システムは、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る、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。

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 認証がイネーブルになります。

Network [1..1] IEEE8021X TlsVerify

TLS を使用する場合は、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 リストはビデオ システムにアップロードする必要があります。これは、Web インターフェイスから実行できます。

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、コーデックに CA リストがアップロードされていない場合、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 [1..1] IEEE8021X UseClientCertificate

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 証明書は、ビデオ システムにアップロードされている必要があります。これは、Web インターフェイスから実行できます。

必要なユーザ ロール: ADMIN, USER

デフォルト値: Off

値スペース: Off/On

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

On: On に設定した場合、クライアント(ビデオ システム)はサーバと相互認証 TLS ハンドシェイクを実行します。

Network [1..1] IEEE8021X Identity

802.1X 認証用のユーザ名を定義します。

必要なユーザ ロール: ADMIN, USER

デフォルト値: ""

値スペース: 文字列(0, 64)

802.1 X 認証用のユーザ名。

Network [1..1] IEEE8021X Password

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 [1..1] IEEE8021X AnonymousIdentity

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 として使用されません。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 [1..1] IEEE8021X Eap Md5

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

必要なユーザ ロール: ADMIN, USER

デフォルト値: On

値スペース: Off/On

Off: EAP-MD5 プロトコルはディセーブルになります。

On: EAP-MD5 プロトコルが有効になります。

Network [1..1] IEEE8021X Eap Ttls

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

必要なユーザ ロール: ADMIN, USER

デフォルト値: On

値スペース: Off/On

Off: EAP-TTLS プロトコルはディセーブルになります。

On: EAP-TTLS プロトコルが有効になります。

Network [1..1] IEEE8021X Eap Tls

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

必要なユーザ ロール:ADMIN,USER

デフォルト値:On

値スペース:Off/On

Off:EAP-TLS プロトコルはディセーブルになります。

On: EAP-TLS プロトコルが有効になります。

Network [1..1] IEEE8021X Eap Peap

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、シスコと RSA Security により開発されました。

必要なユーザ ロール:ADMIN,USER

デフォルト値:On

値スペース:Off/On

Off:EAP-PEAP プロトコルはディセーブルになります。

On: EAP-PEAP プロトコルが有効になります。

Network [1..1] IP Stack

システムのネットワーク 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、システムのネットワーク 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、システムのネットワーク インターフェイスで IPv6 が使用されます。

Network [1..1] IPv4 Assignment

システムが 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:システム アドレスは DHCP サーバによって自動的に割り当てられます。

Network [1..1] IPv4 Address

システムのスタティック 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 [1..1] IPv4 Gateway

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 [1..1] IPv4 SubnetMask

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 [1..1] IPv6 Assignment

システムが 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:コードブックおよびゲートウェイの IP アドレスは、Network IPv6 Address および Network IPv6 Gateway の各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 [1..1] IPv6 Address

システムのスタティック 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 [1..1] IPv6 Gateway

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 [1..1] IPv6 DHCPOptions

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 [1..1] MTU

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。最小サイズは、IPv4 の場合は 576、IPv6 の場合は 1280 です。

必要なユーザ ロール:ADMIN,USER

Default value: 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 [1..1] QoS Mode

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 [1..1] QoS Diffserv Audio

この設定は、[ネットワーク QoS モード(Network QoS Mode)] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ~ 63 です。数字が大きいくほど、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

Default value: 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。数値が大きいくほど、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 [1..1] QoS Diffserv Video

この設定は、[ネットワーク QoS モード(Network QoS Mode)] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内でビデオ パケットに持たせる優先順位を定義します。プレゼンテーション チャネル(共有コンテンツ)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。数字が大きいくほど、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

Default value: 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。数値が大きいくほど、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 [1..1] QoS Diffserv Data

この設定は、[ネットワーク QoS モード(Network QoS Mode)] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

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

Default value: 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 [1..1] QoS Diffserv Signalling

この設定は、[ネットワーク QoS モード(Network QoS Mode)] が [Diffserv] に設定されている場合にのみ有効になります。

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

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

Default value: 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 [1..1] QoS Diffserv ICMPv6

この設定は、[ネットワーク QoS モード(Network QoS Mode)] が [Diffserv] に設定されている場合にのみ有効になります。

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

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

Default value: 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 [1..1] QoS Diffserv NTP

この設定は、[ネットワーク QoS モード(Network QoS Mode)] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

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

Default value: 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 [1..1] RemoteAccess Allow

リモート アクセスで SSH/HTTP/HTTPS からコーデックに許可する 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 [1..1] Speed

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 [1..1] TrafficControl Mode

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 [1..1] VLAN Voice Mode

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 [1..1] VLAN Voice VlanId

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

Default value: 1

値スペース:整数(1..4094)

VLAN 音声 ID を設定します。

NetworkServices 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、エンドポイント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 デーモンは有効です。

NetworkServices H323 Mode

システムで H.323 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: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)プロトコルによるビデオ システムへのアクセスを許可するか否かを指定します。ビデオ システムの Web インターフェイスは HTTP または HTTPS を使用することに注意してください。この設定を Off にすると、Web インターフェイスを使用できなくなります。

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

注:以前のソフトウェア バージョンから CE9.4(以降)にアップグレードされ、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状態で提供されるビデオシステムについて、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 によるビデオ システムへのアクセスを禁止します。

HTTP+HTTPS:HTTP と HTTPS の両方によるビデオ システムへのアクセスを許可します。

HTTPS:HTTPS によるビデオ システム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用さ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 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。

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。必要に応じて、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)レスポンス 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 レスポンスを介してステータスが照会されます。対応する証明書が失効している場合、HTTPS 接続は使用されません。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:OCSP サポートをディセーブルにします。

On:OCSP サポートをイネーブルにします。

NetworkServices HTTPS OCSP URL

証明書のステータスを調べるために使用される OCSP レスポンス(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、Web サイトからブラウザに対して、サイトを HTTP を使用してロードすることを避け、サイトへの HTTP を使用したアクセスはすべて HTTPS リクエストに自動変換する必要があることを通知します。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off: HTTP Strict Transport Security 機能が無効になります。

On: HTTP Strict Transport Security 機能が有効になります。

NetworkServices HTTPS VerifyServerCertificate

ビデオ システムが外部 HTTPS サーバ(電話帳サーバや外部マネージャなど)に接続すると、このサーバはビデオ システムに対して自身を識別する証明書を示します。

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:サーバ証明書を確認しません。

On:サーバ証明書が信頼できる認証局(CA)によって署名されていることを確認するようシステムに要求します。これには、信頼できる CA のリストがシステムに事前にアップロードされている必要があります。

NetworkServices HTTPS VerifyClientCertificate

ビデオ システムが HTTPS クライアント(Web ブラウザなど)に接続すると、クライアントは自分自身を識別するためにビデオ システム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 のリストがシステムに事前にアップロードされている必要があります。

NetworkServices NTP Mode

ネットワーク タイム プロトコル(NTP)は、リファレンス タイム サーバにシステム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:システムは時間を参照するために NTP サーバを使用します。デフォルトでは、サーバのアドレスはネットワークの DHCP サーバから取得されます。DHCP サーバを使用しない場合や、DHCP サーバが NTP サーバのアドレスを提供しない場合は、NetworkServices NTP Server [n] Address 設定で指定された NTP サーバアドレスが使用されます。

Manual:システムは、NetworkServices NTP Server [n] Address 設定で指定された NTP サーバを使って時間を参照します。

Off:システムは NTP サーバを使用しません。NetworkServices NTP Server [n] Address 設定は無視されます。

NetworkServices NTP Server [1..3] Address

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 SIP Mode

システムで SIP コールの発信および受信を可能にするかどうかを定義します。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:SIP コールの発信と受信の可能性をディセーブルにします。

On: SIP コールの発信と受信の可能性を有効にします。

NetworkServices SNMP Mode

ネットワーク管理システムでは、管理上の対応を補償する条件についてネットワーク接続デバイス(ルータ、サーバ、スイッチ、プロジェクトなど)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、システム コンフィギュレーションを説明する管理対象システム変数の形式で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 サービスをディセーブルにします。

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 [1..3] Address

最大 3 つの SNMP マネージャのアドレスを定義します。

システムの SNMP エージェント(コーデック内)は、システム ロケーションやシステム接点についてなど、SNMP マネージャ(PC プログラムなど)からのリクエストに回答します。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、コーデックの 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(または Secure Shell)プロトコルは、コーデックとローカル コンピュータ間での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 プロトコルはディセーブルになります。

On:SSH プロトコルはイネーブルになります(デフォルト)。

NetworkServices SSH HostKeyAlgorithm

SSH ホストキーに使用される暗号化アルゴリズムを選択します。2048 ビットのキーサイズを用いる RSA(リベスト・シャミール・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) 公開キー認証をコーデック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 システム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 システム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。タイムアウトを設定するには、ビデオ システムの Web インターフェイスを使用します。

UPnP が有効になると、ビデオ システムはネットワーク上での自身のプレゼンスをアダプタイズします。このアダプタイズによって、タッチ コントローラはビデオ システム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、手動でビデオ システムの 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 システムは自身のプレゼンスをアダプタイズしないため、タッチ コントローラをビデオ システムとペアリングするためにはビデオ システムの 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 システム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ダプタイズします。

NetworkServices UPnP Timeout

ビデオ システムがオンになった後または再起動した後、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

Default value: 600

値スペース:整数(0..3600)

範囲:0 ~ 3600 秒の値を選択します。

NetworkServices WelcomeText

SSH 経由でコーデックにログインする際に、ユーザに表示する情報を選択します。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

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

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ビデオ システムは、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。

このシステム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。システム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)。

ビデオ システム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、システムは 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

ビデオ システムが Wi-Fi 経由でのネットワーク接続を許可されていれば(NetworkServices WIFI Allowed 設定を参照)、この設定を使用して Wi-Fi を有効および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 ケーブルを抜くと、ビデオ システムは、前回接続した Wi-Fi ネットワークが使用可能であれば、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

ビデオ システムの XML API をイネーブルまたはディセーブルにします。セキュリティ上の理由からこれを無効にできます。XML API をディセーブルにすると、TMS などとのリモート管理機能が制限され、ビデオ システム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。

Peripherals 設定

Peripherals InputDevice Mode

ビデオシステムの操作に、サードパーティ製 USB キーボードまたはリモコンの使用を許可するかどうかを設定します。

これは、CE9.5 にプレビュー機能として含まれています。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off: サードパーティ製 USB キーボードまたはリモコンの使用は許可されません。

On: サードパーティ製 USB キーボードまたはリモコンを使ってビデオシステムを操作できます。

Peripherals Pairing CiscoTouchPanels EmcResilience

多量の電磁雑音が存在する環境でタッチ コントローラを使用すると、誤信号が生じる(例、誰もタップしていないのに、タッチ コントローラがタップされた状態になる)ことがあります。この問題に対処するには、[EMC レジリエンスモード(EMC Resilience Mode)] 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:EMC レジリエンスモードは無効になります。

On:EMC レジリエンスモードは有効になります。

Peripherals Profile Cameras

ビデオ システムに接続されることが予想されるタッチ パネルの数を定義します。この情報はビデオ システム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: Minimum1

値スペース:NotSet/Minimum1/0/1/2/3/4/5/6/7

NotSet:カメラ チェックは実行されません。

Minimum1:1 台のカメラがビデオ システムに接続されている必要があります。

0 ~ 5:ビデオ システムへの接続が予想されるカメラの数を選択します。

Peripherals Profile ControlSystems

サードパーティ製制御システム(Crestron または AMX など)をビデオ システムに接続する予定であれば、定義します。この情報はビデオ システムの診断サービスで使用します。接続された制御システムの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。サードパーティ制御システムは 1 つのみサポートされるので注意してください。

1 に設定する場合、xCommand Peripherals Pair コマンドおよび HeartBeat コマンドを使用して、制御システムからビデオ システムにハートビートを送信する必要があります。これが失敗すると、室内制御拡張により、ビデオ システムが制御システムへの接続を失ったことを示す警告が表示されます。

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値:NotSet

値スペース:1/NotSet

1:1 つのサードパーティ製制御システムをビデオ システムに接続する必要があります。

NotSet: サードパーティ製制御システムの検査は実行されません。

Peripherals Profile TouchPanels

ビデオ システムに接続する予定のシスコ タッチ コントローラの数を実験します。この情報はビデオ システムの診断サービスで使われます。接続されたタッチ コントロー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: Minimum1

値スペース:NotSet/Minimum1/0/1/2/3/4/5

NotSet:タッチ パネル チェックは実行されません。

Minimum1:少なくとも 1 台のシスコ タッチ コントローラがビデオ システムに接続されている必要があります。

0 ~ 5:ビデオ システムへの接続が予想されるタッチ コントローラの数を選択します。公式にサポートされるシスコ タッチ コントローラは、1 台のみであることを注意してください。

Phonebook 設定

Phonebook Server [1..1] ID

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 [1..1] Type

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 [1..1] URL

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)。

Provisioning 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、システムはスタートアップ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

エンドポイントが Cisco Unified Communications Manager(CUCM)でプロビジョニングされており、代替 CUCM が冗長性に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。主な CUCM が使用できない場合、エンドポイントは代替 CUCM でプロビジョニングされます。主な CUCM が再び使用可能になると、エンドポイントはこの 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 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)を使用してビデオ システムを設定できます。これにより、ビデオ会議のネットワーク管理者は複数のビデオ システム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/Spark/TMS/VCS

Off: ビデオ システム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)からビデオ システムにコンフィギュレーションをプッシュします。

Edge: CUCM(Cisco Unified Communications Manager)からビデオ システムにコンフィギュレーションをプッシュします。システムは Collaboration Edge インフラストラクチャを介して CUCM に接続します。Edge を越えて登録するには、暗号化オプションキーがビデオ システムにインストールされている必要があります。

Spark: Cisco Webex クラウド サービスからビデオ システムに設定をプッシュします。

TMS: TMS(Cisco TelePresence Management System)からビデオ システムにコンフィギュレーションをプッシュします。

VCS: VCS(Cisco TelePresence Video Communication Server)からビデオ システムにコンフィギュレーションをプッシュします。

Provisioning LoginName

これは、プロビジョニング サーバによるビデオ システムの認証で使用するクレデンシャルのユーザ名部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。

必要なユーザ ロール: ADMIN、USER

デフォルト値: ""

値スペース: 文字列(0, 80)

有効なユーザ名。

Provisioning Password

これは、指定サーバとのビデオ システム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。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。

Proximity 設定

Proximity Mode

ビデオ システムが超音波ベアリング メッセージを発信するか否かを決定します。

ビデオ システムが超音波を発信すると、Proximity クライアントはビデオ システム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

[オフ(Off)]: ビデオ システムは超音波を発しないため、Proximity サービスを使用できません。

[オン(On)]: ビデオ システムが超音波を発し、Proximity クライアントはビデオ システムに近接していることを検出できます。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、ビデオ システムで無線によって Proximity クライアントからコンテンツを共有できます (ラップトップ画面の共有など)。このサービスはラップトップ (OS X および Windows) でサポートされます。この設定が機能するには、Proximity Mode を On にする必要があります。

必要なユーザ ロール: ADMIN, USER

デフォルト値: Enabled

値スペース: Enabled/Disabled

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

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

Proximity Services ContentShare ToClients

Proximity 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 クライアントはビデオ システムからプレゼンテーションを受け取ります。詳細を拡大して、以前のコンテンツを表示し、スナップショットを作成できます。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには、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 PeopleCountOutOfCall

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

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Off

値スペース: Off/On

Off: ビデオ システムは、システムが通話中のときまたはセルフ ビューがオンのときのみ、人数を数えます。

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

RoomAnalytics PeoplePresenceDetector

ビデオ システムは、人が室内に存在しているかどうかを確認し、その結果を [室内在室分析 (RoomAnalytics PeoplePresence)] のステータスにレポートすることができます。この機能は、超音波に基づいています。室内に人が存在しているかどうかを検出するには最短で 2 分かかり、空室になったあとにステータスを変更するには最長 2 分かかる可能性があります。

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: ビデオ システムのステータスに、室内に人が存在しているかどうかは表示されません。

On: ビデオ システムのステータスに、室内に人が存在しているかどうかが表示されます。

RoomReset 設定

RoomReset 設定

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。マクロを使用して、ビデオ エンドポイントの一部を自動化できる JavaScript コードの一部を記述することができます。このようにして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、システムからルームがリセット準備完了状態であると伝えるイベントを送ることができます。

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(カメラポジションのみ/オフ/オン)

CameraPositionsOnly(カメラポジションのみ): 適用されません。

Off(オフ): ルームリセットイベントは送られません。

On(オン): ルームリセット操作が有効となり、ルームリセットイベントが送られます。

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、RTP および RTCP メディア データに 2326 ~ 2486 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 Video Ports Range が有効な場合、オーディオは RTP Ports Range 設定で定義された範囲を使用し、他のメディア データは RTP Video Ports Range 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、次の発信から有効になります。

必要なユーザ ロール:ADMIN

Default value: 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。

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、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、システムは 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 Video Ports Range が有効な場合、オーディオは RTP Ports Range 設定で定義された範囲を使用し、他のメディア データは RTP Video Ports Range 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、次の発信から有効になります。

必要なユーザ ロール:ADMIN

Default value: 2486

値スペース:整数(1120..65535)

RTP ポート範囲内で最後のポートを設定します。

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。

開始と終了の両方の値が 0 に設定されている場合、RTP Video Ports Range 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、次の発信から有効になります。

必要なユーザ ロール:ADMIN

Default value: 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、次の発信から有効になります。

必要なユーザ ロール:ADMIN

Default value: 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。

Security 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。

External/ExternalSecure モードを使用し、[セキュリティ監査サーバ ポート割り当て (Security Audit Server Port Assignment)] 設定でポート割り当てを [手動 (Manual)] に設定する場合は、[セキュリティ監査サーバ アドレス (Security Audit Server Address)] と [セキュリティ監査サーバのポート (Security Audit Server Port)] の設定で監査サーバのアドレスとポート番号も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 (外部/安全な外部/内部/オフ)

External: システムは外部監査 syslog サーバに監査ログを送信します。syslog サーバでは UDP をサポートする必要があります。

ExternalSecure: システムは監査 CA リストの証明書で検証された外部 syslog サーバに暗号化された監査ログを送信します。監査 CA リスト ファイルは、Web インターフェイスを使用してコーデックにアップロードする必要があります。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: システムは内部ログに監査ログを記録し、いっぱいになった場合は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、システム コーデックはリブートし、停止状態が過ぎ去るまではオーディオ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: システムは、通常の動作を続行し、いっぱいになった場合は内部ログをローテーションします。接続が復元されると syslog サーバに再度監査ログを送信します。

Security Audit Server Address

監査ログは syslog サーバに送信されます。syslog サーバの IP アドレスを定義します。有効な IPv4 または IPv6 のアドレス形式のみが受け入れられます。ホスト名はサポートされていません。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 アドレスまたは IPv6 アドレス。

Security Audit Server Port

監査ログは syslog サーバに送信されます。システムが監査ログを送信する syslog サーバのポートを定義します。この設定は、Security Audit PortAssignment が Manual 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

Default value: 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。Web インターフェイスで [セットアップ(Setup)] > [ステータス(Status)] に移動するか、コマンドライン インターフェイスの場合はコマンド `xStatus Security Audit Server Port` を実行します。

必要なユーザ ロール: AUDIT

デフォルト値: Auto

値スペース: Auto/Manual

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

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

Security Session FailedLoginsLockoutTime

ユーザが Web または SSH セッションのログインに失敗したあと、システムがユーザをロックアウトする時間を定義します。

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール: ADMIN

Default value: 60

値スペース: 整数(0..10000)

ロックアウト時間(分)を設定します。

Security Session InactivityTimeout

ユーザが Web または SSH セッションから自動的にログアウトする前に、システムがユーザの非アクティブ状態をどれくらいの時間受け入れるかを定義します。

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール: ADMIN

Default value: 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

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

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール: ADMIN

Default value: 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

Default value: 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

Default value: 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 を使用してシステムにログインしたとき、前回ログインに成功したセッションのユーザ ID、時刻および日付が表示されます。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

On:最後のセッションに関する情報を表示します。

Off:最後のセッションに関する情報を表示しません。

SerialPort 設定

SerialPort Mode

シリアル ポートを有効/無効にします。

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値:On

値スペース:Off/On

Off:シリアル ポートをディセーブルにします。

On:シリアル ポートをイネーブルにします。

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とおりです。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。

必要なユーザ ロール:ADMIN、INTEGRATOR

Default value: 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。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:ユーザはログインせずに、シリアル ポート経由でコーデックにアクセスできます。

On:シリアル ポート経由でコーデックに接続するときに、ログインが必要です。

SIP 設定

SIP ANAT

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:ANAT を無効にします。

On:ANAT を有効にします。

SIP Authentication UserName

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 128)

有効なユーザ名。

SIP Authentication Password

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 128)

有効なパスワード。

SIP DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/TCP/Tls/UDP

TCP:システムはデフォルトの転送方法として常に TCP を使用します。

UDP:システムはデフォルトの転送方法として常に UDP を使用します。

Tls:システム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 リストをビデオ システムにアップロードできます。このような CA リストがシステムにない場合は匿名の Diffie Hellman が使用されます。

Auto:システムは、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、ビデオ システムのメディアが、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:メディアをビデオ システムのプライベート IP アドレスへ送信します。

Rflx:TURN サーバから見えるビデオ システムのパブリック 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 パスの検出にビデオ システムで利用できる NAT トラバーサル ソリューションです。そのため、音声とビデオの最短ルートがビデオ システム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 サーバを指定した場合は、ICE が有効になります。それ以外の場合は、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、エンドポイント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。

共有回線はエンドポイントではなく 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エンドポイントにプッシュします。

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:システム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:このシステム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、エンドポイントは SIP レジストラ(CUCM または VCS)を介してのみ到達可能になります。

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: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 PreferredIPMedia

メディア(音声、ビデオ、データ)を送受信するための優先 IP バージョンを定義します。[Network IPStack] および [Conference CallProtocolIPStack] の両方が [デュアル(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。

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:メディアの優先 IP バージョンは IPv4 です。

IPv6:メディアの優先 IP バージョンは IPv6 です。

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 [1..4] Address

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

TLS 接続の場合、SIP CA リストをビデオ システムにアップロードできます。これは、Web インターフェイスから実行できます。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:検証せずに TLS 接続を許可するには、Off に設定します。TLS 接続は、サーバから受信した x.509 証明書をローカル CA リストと確認せずにセットアップできます。これは通常、コーデックに SIP CA リストがアップロードされていない場合、選択する必要があります。

On:TLS 接続を確認するには、On に設定します。x.509 証明書が CA リストで検証された、サーバへの TLS 接続だけが許可されます。

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、システム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:DNS で利用可能な TURN サーバを検索し、コールを発信する前にポート割り当てが可能かどうかをテストします。

SIP Turn DropRflx

DropRflx は、リモート エンドポイントが同じネットワークにない場合に限り、TURN リレー経由でエンドポイント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 エンドポイントが別のネットワークにある場合、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、エンドポイント固有のパブリック IP アドレスを検出するためにも使用されます。

必要なユーザ ロール:ADMIN

デフォルト値:""

値スペース:文字列(0..255)

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

SIP Turn UserName

TURN サーバへのアクセスに必要なユーザ名を定義します。

必要なユーザ ロール:ADMIN

デフォルト値:""

値スペース:文字列(0, 128)

有効なユーザ名。

SIP Turn Password

TURN サーバへのアクセスに必要なパスワードを定義します。

必要なユーザ ロール:ADMIN

デフォルト値:""

値スペース:文字列(0, 128)

有効なパスワード。

SIP Type

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

必要なユーザ ロール:ADMIN

デフォルト値:Standard

値スペース:Standard/Cisco

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

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

SIP URI

SIP URI(Uniform Resource Identifier)は、ビデオ システムの識別に使用されるアドレスです。URI が登録され、SIP サービスによりシステム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)。

Standby 設定

Standby BootAction

コーデックの再起動後のカメラの位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: DefaultCameraPosition

値スペース: None/DefaultCameraPosition/RestoreCameraPosition

None: アクションはありません。

RestoreCameraPosition: ビデオ システムを再起動すると、カメラは再起動前の位置に戻ります。

DefaultCameraPosition: ビデオ システムを再起動すると、カメラは工場出荷時のデフォルトの位置に移動します。

Standby Control

システムがスタンバイ モードに移行するか否かを定義します。

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: システムはスタンバイ モードを開始しません。

On: Standby Delay がタイムアウトになると、システムはスタンバイ モードになります。Standby Delay を適切な値に設定する必要があります。

Standby Delay

スタンバイ モードに入る前に、システムがアイドル 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

Default value: 10

値スペース: 整数(1..480)

スタンバイ遅延(分)を設定します。

Standby StandbyAction

スタンバイ モードに入るときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: PrivacyPosition

値スペース: None/PrivacyPosition

None: アクションはありません。

PrivacyPosition: ビデオ システムがスタンバイになると、プライバシー保護のためカメラは横向きになります。

Standby WakeupAction

スタンバイ モードを抜けるときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: RestoreCameraPosition

値スペース: None/RestoreCameraPosition/DefaultCameraPosition

None: アクションはありません。

RestoreCameraPosition: ビデオ システムがスタンバイではなくなると、カメラはスタンバイ前の位置に戻ります。

DefaultCameraPosition: ビデオ システムがスタンバイではなくなると、カメラは工場出荷時のデフォルトの位置に移動します。

Standby WakeupOnMotionDetection

動体検知自動ウェイクアップは、人が室内に入ってきたときに検知する機能です。この機能は、超音波での検知に基づいており、この機能を動作させるには [近接モード設定(Proximity Mode setting)] がオン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: 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: 人が部屋に入ってくると、システムが自動的にスタンバイからウェイクアップします。

SystemUnit 設定

SystemUnit Name

システム名を定義します。コーデックが SNMP エージェントとして機能している場合に、システム名は 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)

システム名を定義します。

SystemUnit CrashReporting Advanced

ビデオ システム (コーデック) がクラッシュすると、システムは解析のために [シスコ自動クラッシュレポートツール (Cisco Automatic Crash Report tool)] (ACR) ヘログを自動的に送信できます。ACR ツールは、シスコ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

ビデオ システム (コーデック) がクラッシュすると、システムは解析のために [シスコ自動クラッシュレポートツール (Cisco Automatic Crash Report tool)] (ACR) ヘログを自動的に送信できます。ACR ツールは、シスコ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

ビデオ システム (コーデック) がクラッシュすると、システムは解析のために [シスコ自動クラッシュレポートツール (Cisco Automatic Crash Report tool)] (ACR) ヘログを自動的に送信できます。ACR ツールは、シスコ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)

[シスコ自動クラッシュレポートツール (Cisco Automatic Crash Report tool)] の URL。

Time 設定

Time TimeFormat

時刻形式を定義します。

必要なユーザ ロール:admin、user

デフォルト値:24H

値スペース:24H/12H

24H:24 時間の時間フォーマットを設定します。

12H:12 時間(AM/PM)の時間フォーマットを設定します。

Time DateFormat

日付形式を定義します。

必要なユーザ ロール:admin、user

デフォルト値:DD_MM_YY

値スペース:DD_MM_YY/MM_DD_YY/YY_MM_DD

DD_MM_YY:2010 年 1 月 30 日は「30.01.10」と表示されます。

MM_DD_YY:2010 年 1 月 30 日は「01.30.10」と表示されます。

YY_MM_DD:2010 年 1 月 30 日は「10.01.30」と表示されます。

Time Zone

ビデオ システム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:Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Ensenada, America/Fort_Nelson, America/Fort_Wayne, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox_IN, America/Kralendijk, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Lower_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico_City, America/

Miquelon, America/Moncton, America/Monterrey, America/Montevidео, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Beulah, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Porto_Velho, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio_Branco, America/Rosario, America/Santa_Isabel, America/Santarem, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St_Barthelemy, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDURville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Choibalsan, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho_Chi_Minh, Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung_Pandang, Asia/Ulaanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/

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

リストからタイムゾーンを選択します。

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 Touch 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。システムが通話中の場合、進行中の通話の妨げになるため画面は点滅しません、その代わりに、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:ビデオ システムが着信し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 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:他のシステムがこのシステムに到達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 プロトコルおよびシステム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:システムの IPv4 アドレスを示します。

IPv6:システムの IPv6 アドレスを示します。

H323Id:システムの H.323 ID を表示します(H323 H323Alias ID の設定を参照)。

H320Number :連絡先情報としてシステムの 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)。

E164Alias:連絡先情報としてシステムの H.323 E164 エイリアスを表示します(H323 H323Alias E164 の設定を参照)。

SipUri:システムの SIP URI を表示します(SIP URI の設定を参照)。

SystemName:システム名を表示します(SystemUnit Name の設定を参照)。

DisplayName:システムの表示名を表示します(SIP DisplayName の設定を参照)。

UserInterface CustomMessage

アウェイク モードのとき、スクリーンの下部左側にカスタム メッセージを表示することができます。

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値:""

値スペース:文字列(0, 128)

カスタム メッセージを追加します。カスタム メッセージを削除するには空の文字列を追加します。

UserInterface KeyTones Mode

テキストまたは数値を入力する際に、キーボード クリック効果音(キー トーン)が鳴るようにシステムを設定できます。

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: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 Language

ユーザ インターフェイスで使用す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(英語)が使用されます。

必要なユーザ ロール:ADMIN、USER

デフォルト値:English

値スペース:Arabic/Catalan/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/English/EnglishUK/Finnish/French/FrenchCanadian/German/Hebrew/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/Portuguese/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish

リストから言語を選択します。

UserInterface OSD EncryptionIndicator

暗号化インジケータが画面に表示される時間の長さを定義します。暗号化された通話のアイコンは、ロックされた南京錠です。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/AlwaysOn/AlwaysOff

Auto:コールが暗号化されている場合は、「コールは暗号化されています(Call is encrypted)」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。

コールが暗号化されていない場合は、「コールは暗号化されていません(Call is not encrypted)」という通知が 5 秒間表示されます。暗号化インジケータ アイコンは表示されません。

AlwaysOn:「コールは暗号化されています(Call is encrypted)」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。

AlwaysOff:暗号化インジケータは画面上に表示されません。

UserInterface OSD HalfwakeMessage

カスタム メッセージは、システムが起動中の状態のとき、メインスクリーンの中央に表示できます。カスタム メッセージは、ビデオ システムの使用開始方法の指示を与えるデフォルト メッセージに置き換えられます。カスタム メッセージを追加せずにデフォルト メッセージを削除することもできます。

必要なユーザ ロール:ADMIN

デフォルト値:""

値スペース:文字列(0, 128)

カスタム メッセージ。空の文字列:デフォルト メッセージを復元します。空白のみ:メッセージは一切表示されません。

UserInterface OSD Output

オンスクリーン用の情報とインジケータ(OSD)を表示するモニタを定義します。

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値:Auto

値スペース:Auto/1/2

Auto:システムはモニタがビデオ出力に接続されたことを検出し、接続した最初のモニタにオンスクリーン情報とインジケータを送信します。複数のモニタが設定されている場合、システムをオンにする前にすべてのモニタが接続されていると、オンスクリーン情報およびインジケータは出力コネクタ 1(HDMI 1)から開始して最も低い番号のビデオ出力に送信されます。

1-2 :システムは画面に表示される情報とインジケータを、指定した出力に送信します。システムの出力コネクタ n にオンスクリーン用の情報とインジケータを送信するには、n を選択します。

UserInterface Security Mode

この設定では、重要なシステム情報(例、ビデオ システムの連絡先情報や 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 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システムの情報がユーザ インターフェイスに表示されます。

Strong:連絡先情報および IP アドレスは、ユーザ インターフェイス(ドロップ ダウン メニューと設定パネル)に表示されません。

UserInterface SettingsMenu Mode

ビデオ システムの管理者パスワードによって、ユーザ インターフェイス(Touch 10 または画面)の設定パネルを保護することができます。このパスワードが空白の場合、誰でも設定メニューの設定にアクセスできます(例、システムを初期設定へリセット)。認証を有効にすると、認証を必要とするすべての設定に南京錠のアイコンが表示されます。設定を選択するときに、管理者のユーザ名とパスフレーズを入力するように求められます。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 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ビデオシステムにカスタムの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

[自動(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。カスタム壁紙がシステムにアップロードされていない場合、設定がデフォルト値に戻ります。

UserManagement の設定

UserManagement LDAP Admin Filter

LDAP フィルタは、管理者権限が付与されるユーザを判別するために使用します。

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 管理者フィルタは優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合、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 管理者フィルタは優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合、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

提供されるユーザ名へのマッピングに使用される属性。設定しない場合は、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

ビデオ システムと LDAP サーバと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 上の LDAP サーバに接続します (暗号化なし)。

STARTTLS: ポート 389 上の LDAP サーバに接続し、次に STARTTLS を送信して TLS 暗号化を有効にします。

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

ビデオ システムは、LDAP(Lightweight Directory Access Protocol)サーバを、ユーザ名とパスワードを一元的に保存および検証する場所として使用することをサポートします。この設定を使用して、LDAP 認証を使用するかどうかを設定します。実装は、Microsoft Active Directory (AD)サービスでテスト済みです。

LDAP モードでスイッチする場合、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 groups, 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 認証は許可されません。

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)。

必要なユーザ ロール:ADMIN

Default value: 0

値スペース:整数(0..65535)

LDAP サーバのポート番号。

UserManagement LDAP VerifyServerCertificate

ビデオ システムを LDAP サーバに接続すると、サーバはビデオ システムに証明書を提示して身元を示します。この設定は、ビデオ システムがサーバの証明書を確認するかどうかを決定するために使用します。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:ビデオ システムは LDAP サーバの証明書を検証しません。

On:ビデオ システムは、LDAP サーバの証明書が信頼できる認証局(CA)によって署名されているか必ず検証します。システムにアップロードする信頼できる CA の一覧に、その CA を事前に追加する必要があります。ビデオ システムの Web インターフェイスを使用して、信頼できる CA の一覧を管理します(詳細については、管理者ガイドを参照)。

Video 設定

Video ActiveSpeaker DefaultPiPPosition

通話中のスピーカーを示すピクチャインピクチャ(PiP)の画面上の位置を定義します。この設定は、通話中のスピーカーを PiP 表示するビデオ レイアウト(オーバーレイ レイアウト)を使用している場合にのみ有効です。また、場合によっては、カスタム レイアウトでも有効です(「Video DefaultLayoutFamily Local の設定」を参照)。この設定は、次回以降のコールで有効になります。コール中に変更された場合、現在のコールへの影響はありません。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Current

値スペース:Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current:通話中のスピーカーの PiP の位置はコール終了後にも変更されません。

UpperLeft:通話中のスピーカーの PiP が画面の左上隅に表示されます。

UpperCenter:通話中のスピーカーの PiP が画面の上部中央に表示されます。

UpperRight:通話中のスピーカーの PiP が画面の右上隅に表示されます。

CenterLeft:通話中のスピーカーの PiP が画面の左中央に表示されます。

CenterRight:通話中のスピーカーの PiP が画面の右中央に表示されます。

LowerLeft:通話中のスピーカーの PiP が画面の左下隅に表示されます。

LowerRight:通話中のスピーカーの PiP が画面の右下隅に表示されます。

Video DefaultLayoutFamily Local

ローカルで使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/Equal/Prominent/Overlay/Single

Auto:システムによって提供されるローカル レイアウト データベースに指定されたデフォルト レイアウト ファミリがローカル レイアウトとして使用されます。

Equal:Equal レイアウト ファミリがローカル レイアウトとして使用されます。画面上に十分なスペースがある限り、すべてのビデオのサイズは等しくなります。

Prominent:[対象拡大表示(Prominent)] レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または(存在する場合)プレゼンテーションは大きい画像となり、他の参加者は小さい画像となります。通話中のスピーカーが遷移するとき、音声切り替えられます。

Overlay:[オーバーレイ(Overlay)] レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または(存在する場合)プレゼンテーションは全画面表示となり、他の参加者は小さいピクチャ イン ピクチャ(PiP)となります。通話中のスピーカーが遷移するとき、音声切り替えられます。

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、音声切り替えられます。

Video DefaultLayoutFamily Remote

リモート参加者が使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/Equal/Prominent/Overlay/Single

Auto: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

Default value: 1

値スペース:1/2/3

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を設定します。

Video Input Connector [1..2] CameraControl CameraID

カメラ ID は、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(コネクタ n:1)

設定可能な値: Connector n: 1(コネクタ n:1)

カメラ ID は固定されており、変更できません。

Video Input Connector [1..2] CameraControl Mode

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

設定可能な値: 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 [2..2] CEC Mode

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 システム ステータスで使用可能になります(ビデオ入力コネクタ [n] 接続デバイス CEC [n])。ただし、接続デバイスは CEC もサポートすることが条件となります。

必要なユーザ ロール:ADMIN,INTEGRATOR

デフォルト値:On

設定可能な値: Connector n: Off/On

Off:CEC が無効になります。

On:CEC が有効になります。

Video Input Connector [1..2] InputSourceType

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 はシステム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

設定可能な値: Connector 1: camera Connector 2: PC/camera/document_camera/mediaplayer/whiteboard/other (コネクタ 1: カメラ コネクタ 2: パソコン/カメラ/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/その他)

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 [1..2] Name

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 [1..2] OptimalDefinition Profile

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、Norma] 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。解像度は、発呼側と着信側の両方のシステム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 [2..2] PreferredResolution

ビデオ システムに HDMI 経由でシステムに接続したソース デバイス (例: ラップトップ) の推奨解像度として通知されている画面の解像度とリフレッシュ レートを定義します。送信元デバイス (ラップトップのディスプレイ設定ソフトウェア) によって手動で上書きされない限り、解像度とリフレッシュ レートはソース側の解像度の選択に関するロジックによって自動的に選択されます。

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、更新間隔は 30 Hz です。

Video Input Connector [2..2] PresentationSelection

ビデオ入力にプレゼンテーション ソースを接続するときの、ビデオ システムの動作を定義します。ビデオ システムがスタンバイ モードである場合、プレゼンテーション ソースを接続すると起動します。遠端とプレゼンテーションを共有するには、この設定が AutoShare に設定されていなければ、追加操作(ユーザ インターフェイスで [共有(Share)] を選択)が必要です。

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値: Connector n: OnConnect

設定可能な値: Connector n: AutoShare/Desktop/Manual/OnConnect (自動共有/デスクトップ/手動/接続上)

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 [2..2] Quality

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 [2..2] RGBQuantizationRange

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 [1..2] Visibility

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 はシステム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: Always (コネクタ 1: 表示しない コネクタ2: 常に表示)

設定可能な値: Connector 1: Never Connector 2: Always/IfSignal/Never (コネクタ 1: 表示しない コネクタ2: 常に表示/入力信号がある場合/表示しない)

Always: ビデオ入力コネクタ用メニュー選択は、ユーザ インターフェイスに常に表示されます。

IfSignal: ビデオ入力コネクタ用メニュー選択は、ビデオ入力に何か接続されている場合のみ表示されます。

Never: 入力の送信元はプレゼンテーション ソースとして使用されないため、ユーザ インターフェイスに表示されません。

Video Monitors

Video Output Connector [n] MonitorRole 設定を使用する各画面にロールを割り当てます。モニタロールは、この出力に接続されている画面上のどのレイアウト(コール参加者とプレゼンテーション)に表示するかを決定します。同じモニタ ロールの画面は同じレイアウトになり、別のモニタ ロールの画面は異なるレイアウトになります。

Video Monitors で設定するモニタ レイアウト モードには、部屋のセットアップで利用する各レイアウト数を反映させてください。いくつかの画面がプレゼンテーション用に確保でき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: Auto

値スペース: Auto/Single/Dual/DualPresentationOnly

Auto: ビデオ システムに接続された画面数は自動的に検出され、レイアウトはモニタ ロールの設定に従って画面に割り振られます。

Single: すべての画面に同じレイアウトが表示されます。

Dual: レイアウトはモニタ ロール [第 1 (First)] および [第 2 (Second)] の画面に配信されます。プレゼンテーションがレイアウトの一部である場合、コールの参加者はすべてモニタ ロール [第 1 (First)] の画面に表示され、プレゼンテーションはモニタ ロール [第 2 (Second)] の画面に表示されます。

DualPresentationOnly: コールのすべての参加者がモニタ ロール [第 1 (First)] の画面に表示されます。プレゼンテーションがレイアウトの一部である場合、プレゼンテーションはモニタ ロール [第 2 (Second)] の画面に表示されます。

Video Output Connector [1..2] CEC Mode

ビデオ出力(HDMI)は、Consumer Electronics Control(CEC)をサポートします。

この設定が [オン(On)] の場合、システムはシステム自体がスタンバイに移行する際、画面をスタンバイ状態に設定するために CEC を使用します。同様に、システムがスタンバイから復帰するとき、システム自身が画面を起動します。

画面のアクティブなビデオ入力がユーザによって変更されることがあります。発信が開始されると、ビデオ システムはアクティブなビデオ入力が画面の別の入力に切り替えられたかどうかを検出します。すると、ビデオ システムは入力を切り戻すため、ビデオ システムがアクティブなビデオ入力ソースになります。ビデオ システムがスタンバイ状態に入るときにビデオ システムがアクティブな入力ソースでない場合、画面はスタンバイに設定されません。

出力に接続した画面に CEC 互換性があること、および CEC が画面上で有効であることが必須条件です。

CEC については、製造業者によって異なるマーケティング名称が使用されていることに注意してください。例: Anynet+ (Samsung)、Aquos Link (シャープ)、BRAVIA Sync (Sony)、HDMI-CEC (日立)、Kuro Link (パイオニア)、CE-Link および Regza Link (東芝)、RIHD (オンキヨー)、HDAVI Control、EZ-Sync、VIERA Link (Panasonic)、EasyLink (Philips)、NetCommand for HDMI (三菱)。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: CEC が無効になります。

On: CEC が有効になります。

Video Output Connector [1..2] Location HorizontalOffset

HorizontalOffset 設定および VerticalOffset 設定は、各ビデオ出力に関連付けられています。これらの設定は、これらの出力に接続されているディスプレイの相対的な位置を信号で送信するために使用されます。

HorizontalOffset = 0 および VerticalOffset = 0 はディスプレイが水平および垂直の両方で中央に位置することを示します。負の水平オフセットは、モニタが中心の左にあり、正の水平オフセットはモニタが中心の右にあることを示します。負の垂直オフセットは、モニタが中心の下にあり、正の垂直オフセットはモニタが中心の上にあることを示します。オフセットの大きさはディスプレイが(他のディスプレイと比較して)どれくらい中央から離れているかを示します。

例:隣り合った 2 つの画面があります。左はコネクタ 1 の画面、右はコネクタ 2 の画面です。ここでは次の設定が適用されます。

Video Output Connector 1 Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Connector 2 Location: HorizontalOffset = 1, VerticalOffset = 0

例:下のように 2 つの画面があります。上側はコネクタ 1 の画面、下側はコネクタ 2 の画面です。ここでは次の設定が適用されます。

Video Output Connector 1 Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Connector 2 Location: HorizontalOffset = 0, VerticalOffset = -1

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Connector 1:0 Connector 2:1

値スペース:整数(-100..100)

範囲:値は -100 ~ 100 である必要があります。

Video Output Connector [1..2] Location VerticalOffset

HorizontalOffset 設定および VerticalOffset 設定は、各ビデオ出力に関連付けられています。これらの設定は、これらの出力に接続されているディスプレイの相対的な位置を信号で送信するために使用されます。

HorizontalOffset = 0 および VerticalOffset = 0 はディスプレイが水平および垂直の両方で中央に位置することを示します。負の水平オフセットは、モニタが中心の左にあり、正の水平オフセットはモニタが中心の右にあることを示します。負の垂直オフセットは、モニタが中心の下にあり、正の垂直オフセットはモニタが中心の上にあることを示します。オフセットの大きさはディスプレイが(他のディスプレイと比較して)どれくらい中央から離れているかを示します。

例:隣り合った 2 つの画面があります。左はコネクタ 1 の画面、右はコネクタ 2 の画面です。ここでは次の設定が適用されます。

Video Output Connector 1 Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Connector 2 Location: HorizontalOffset = 1, VerticalOffset = 0

例:下のように 2 つの画面があります。上側はコネクタ 1 の画面、下側はコネクタ 2 の画面です。ここでは次の設定が適用されます。

Video Output Connector 1 Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Connector 2 Location: HorizontalOffset = 0, VerticalOffset = -1

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: Connector n: 0

値スペース:整数(-100..100)

範囲:値は -100 ~ 100 である必要があります。

Video Output Connector [1..2] MonitorRole

モニタ ロールは、ビデオ出力に接続された画面にどのビデオ ストリームを表示するかを示します。すべての出力用の Video Monitors 設定および MonitorRole 設定とともに、各画面に表示されるレイアウト(ビデオ ストリーム)を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Connector n: Auto

値スペース: Auto/First/Second/PresentationOnly

Auto: 画面が接続されたときにシステムが検知し、Video Monitors 設定に対応するモニタ ロール

([第 1 (First)], [第 2 (Second)])を自動的に割り当てます。

First/Second: マルチ画面設定での画面の役割を定義します。シングル画面設定では、[第 1 (First)]

と [第 2 (Second)] の間に違いはありません。

PresentationOnly: アクティブな場合プレゼンテーション ビデオ ストリームを表示し、他のものは表示しません。このモニタ ロールの画面および出力は Video Monitors 設定によって無視されます。

Video Output Connector [1..2] Resolution

接続している画面の解像度とリフレッシュ レートを定義します。

1920_1200_60 より大きなフォーマットには、高品質なディスプレイ ケーブルを使用する必要があります。動作を保証するには、3840_2160_60 で使用するように Cisco によってあらかじめ認定されたディスプレイ ケーブルを使用するか、「プレミアム HDMI 認定」プログラムに合格したケーブルをご使用ください。

UHD テレビおよび画面には、3840_2160_30 (30 Hz)のみしか使用できないものもありますが、3840_2160_60 (60 Hz)はデフォルト設定ではありません。このような場合、テレビと画面の関連設定で、ビデオ システムが接続されている HDMI 入力として 3840_2160_60 を許可するように再設定する必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Connector n: Auto

値スペース: Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30/3840_2160_60

Auto: システムは接続されたモニタのネゴシエーションに基づいて自動的に最適な解像度の設定を試行します。

1920_1080_50: 解像度は 1920 X 1080、リフレッシュ レートは 50 Hz です。

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

1920_1200_50: 解像度は 1920 X 1200、リフレッシュ レートは 50 Hz です。

1920_1200_60: 解像度は 1920 X 1200、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。

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 Output Connector [1..2] RGBQuantizationRange

HDMI 出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、ディスプレイ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。ほとんどの HDMI ディスプレイはフルの量子化範囲を想定しています。

必要なユーザ ロール:ADMIN,INTEGRATOR

デフォルト値:Full

値スペース:Auto/Full/Limited

Auto:RGB の量子化の範囲は、AVI インフォフレームの RGB 量子化範囲ビット(Q0,Q1)に基づいて自動的に選択されます。AVI インフォフレームが使用できない場合、RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて選択されます。

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 Presentation DefaultPiPPosition

プレゼンテーションのピクチャインピクチャ(PiP)の画面上の位置を定義します。この設定は、たとえばユーザ インターフェイスを使用して、プレゼンテーションが明示的に PiP に縮小された場合にのみ有効です。この設定は、次回以降のコールで有効になります。コール中に変更された場合、現在のコールへの影響はありません。

必要なユーザ ロール:ADMIN,INTEGRATOR

デフォルト値:Current

値スペース:Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current:プレゼンテーション PiP の位置はコール終了後にも変更されません。

UpperLeft:プレゼンテーション PiP が画面の左上隅に表示されます。

UpperCenter:プレゼンテーション PiP が画面の上部中央に表示されます。

UpperRight:プレゼンテーション PiP が画面の右上隅に表示されます。

CenterLeft:プレゼンテーション PiP が画面の左中央に表示されます。

CenterRight:プレゼンテーション PiP が画面の右中央に表示されます。

LowerLeft:プレゼンテーション PiP が画面の左下隅に表示されます。

LowerRight:プレゼンテーション PiP が画面の右下隅に表示されます。

Video Presentation DefaultSource

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソースを定義します。この設定は、API およびサード パーティのユーザ インターフェイスで使用できます。シスコが提供するユーザ 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 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が残ります。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:Current

値スペース:Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current:セルフビュー PiP の位置はコール終了後にも変更されません。

UpperLeft:セルフビュー PiP が画面の左上隅に表示されます。

UpperCenter:セルフビュー PiP が画面の上部中央に表示されます。

UpperRight:セルフビュー PiP が画面の右上隅に表示されます。

CenterLeft:セルフビュー PiP が画面の左中央に表示されます。

CenterRight:セルフビュー PiP が画面の右中央に表示されます。

LowerLeft:セルフビュー PiP が画面の左下隅に表示されます。

LowerRight:セルフビュー PiP が画面の右下隅に表示されます。

Video Selfview OnCall Mode

コールをセットアップする短い間、この設定を使用してセルフ ビューがオンにされます。セルフビューをオンのままにしておく時間の長さは、Video Selfview OnCall Duration 設定で定義します。これは一般にセルフ ビューがオフの場合に適用されます。

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値:On

値スペース:Off/On

Off:セルフ ビューはコール セットアップ中に自動的に表示されません。

On:セルフ ビューはコール セットアップ中に自動的に表示されます。

Video Selfview OnCall Duration

この設定は Video Selfview OnCall Mode 設定がオンになっている場合にのみ有効です。この場合、ここで設定された秒数により、自動的にオフにされる前にセルフ ビューが表示される期間が決まります。

必要なユーザ ロール:ADMIN、INTEGRATOR

Default value: 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。

Experimental 設定

試験的設定は、テストのためだけのもので、シスコ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

Touch 10 の使用方法

Touch 10 ユーザ インターフェイスとその使用方法の詳細については、ビデオ システムのユーザ ガイドを参照してください。

システム名または連絡先情報をタップして、**[システム情報 (System Information)]**、**[設定 (Settings)]**、**[再起動 (Restart)]** および **[初期設定へのリセット (Factory Reset)]** にアクセスします。また、**[コール転送 (Call forwarding)]**、**[スタンバイ (Standby)]** および **[着信拒否 (Do not disturb)]** モードを有効にすることもできます。

[コール (Call)] をタップして発信します。また、**[お気に入り (Favorites)]**、**[ディレクトリ (Directory)]**、および **[履歴 (Recents)]** の連絡先リストを呼び出します。

該当する場合、**[メッセージ (Messages)]** をタップして、ボイス メール システムを呼び出します。

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

? をタップして、ヘルプ デスクまたはその他のファシリティ サービスに問い合わせます (有効な場合)。

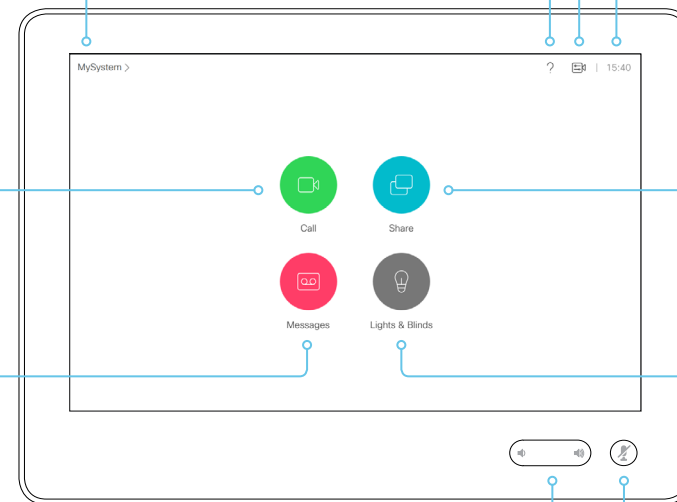
[カメラ (Camera)] アイコンをタップして、セルフビューとカメラ制御をアクティブにします。

時刻を指定します。

[共有 (Share)] をタップして、コンテンツの共有を開始したり、プレゼンテーションを実行したりします。

ユーザーインターフェイス拡張のエントリーポイント (システム上に、様々な色、テキスト、アイコンのボタンが存在する場合があります)。

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



リモート モニタリングのセットアップ

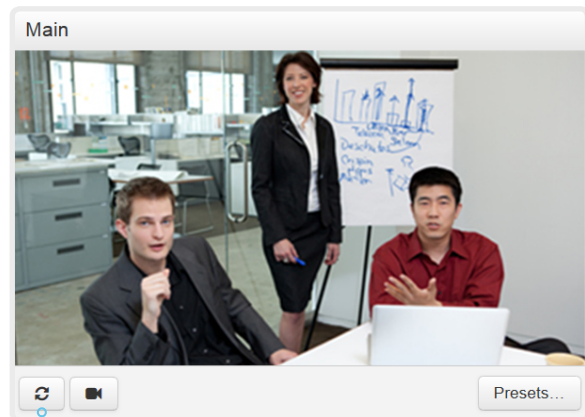
要件:

- RemoteMonitoring オプション

リモート モニタリングは別の場所からビデオ システムを制御する場合に便利です。

入カソースからのスナップショットが Web インターフェイスに表示されるため、部屋にいなくてもカメラ ビューをチェックしてカメラを制御できます。

有効にすると、スナップショットは約 5 秒おきに自動的に更新されます。



スナップショットを自動更新する

ビデオ システムに *RemoteMonitoring* オプションがあるかどうかを確認する

1. Web 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、システムのユーザに適切な方法で通知してください。システム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否認します。

スナップショットについて

ローカル入カソース

ビデオ システムのローカル入カ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。

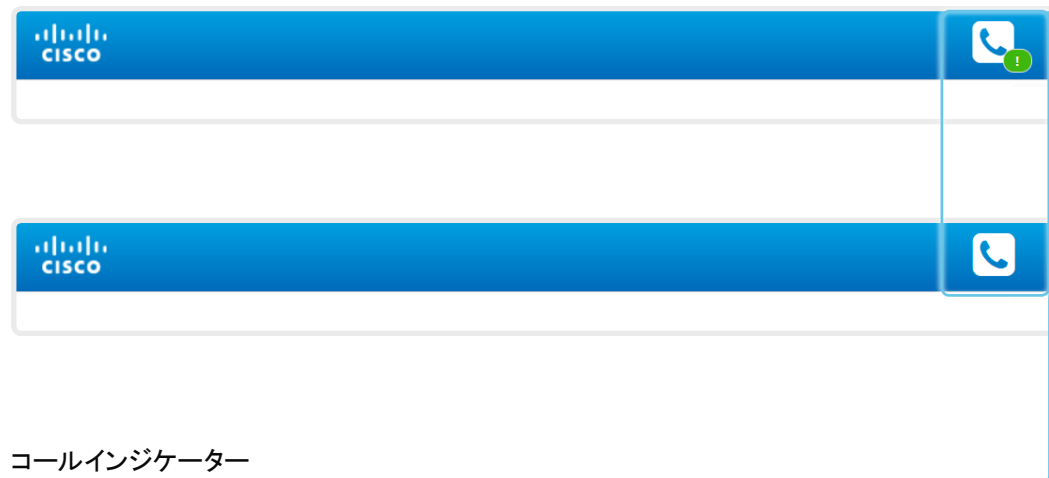
スナップショットは、ビデオ システムがアイドル状態のときにも、通話中にも表示されます。

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。遠端ビデオ システムに [リモート モニタリング(*RemoteMonitoring*)] オプションがあるかどうかは問題ではありません。

遠端スナップショットは、コールが暗号化されていると表示されません。

Web インターフェイスを使用したコール情報へのアクセスとコール応答



コールインジケーター

コールインジケーターでは着信の通知表示と、システムが通話中になる時を表示します。

システムが待機状態の場合、コールインジケーターは表示されません。

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。

システムが通話中

[*コールインジケーター (call indicator)*] にマウスカーソルを乗せると、アクティブコールの数が表示されます。

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
-  通話に応答します。
-  コールを切断する

Web インターフェイスを使用してコールを発信する (1/2 ページ)

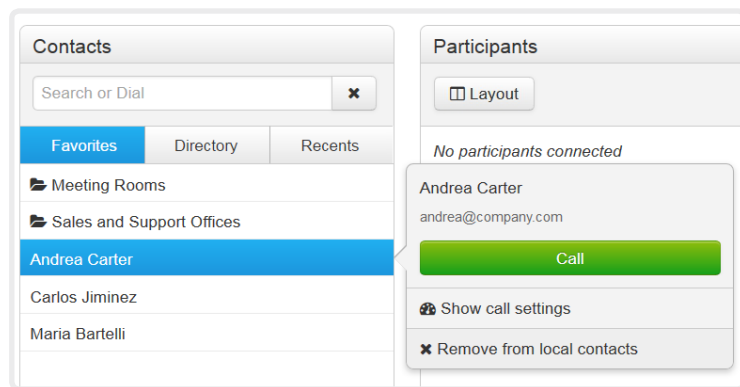
Web インターフェイスにログインし、[\[コール制御\(Call Control\)\]](#) に移動します。

コールの発信

i 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 システム(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する 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。

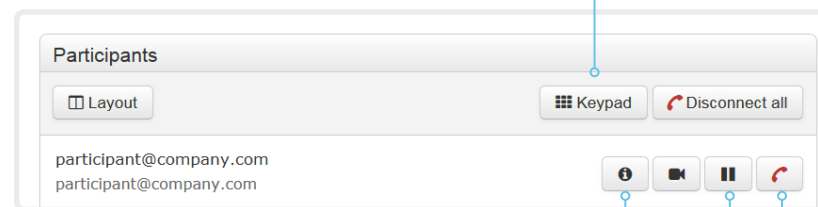
または、[\[検索して発信\(Search and Dial\)\]](#) フィールドに完全な URI または番号を入力します。次に、URI または番号の横に表示される [\[コール\(Call\)\]](#) ボタンをクリックします。



* 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。

Web インターフェイスを使用したコールの発信 (2/2 ページ)

Web インターフェイスにログインし、[\[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。

オプションの組み込み MultiSite 機能をシステムで使用している場合は、本人も含めて最大 4 人までがビデオ 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。

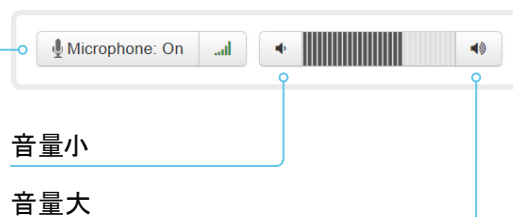
会議ブリッジを使用した複数のコール(CUCM のアドホック会議)は、ビデオ システムでサポートされていても Web インターフェイスではサポートされません。

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。



Web インターフェイスを使用してコンテンツを共有する

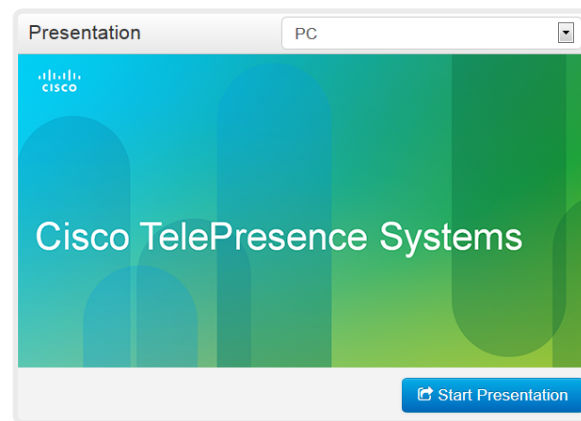
Web インターフェイスにログインし、[\[コール制御\(Call Control\)\]](#)に移動します。

コンテンツの共有

1. プレゼンテーション ソース ドロップダウンリストで、共有するコンテンツ ソースを選択します。
2. [\[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。



プレゼンテーション ソース ドロップダウンリスト

ドロップダウン リストから、共有する入力ソースを選択します。

スナップショット領域

選択されたプレゼンテーション ソースのスナップショットが表示されます。

リモート モニタリング オプションがあるビデオシステムでのみ利用できます。

コンテンツ シェアリング(共有)について

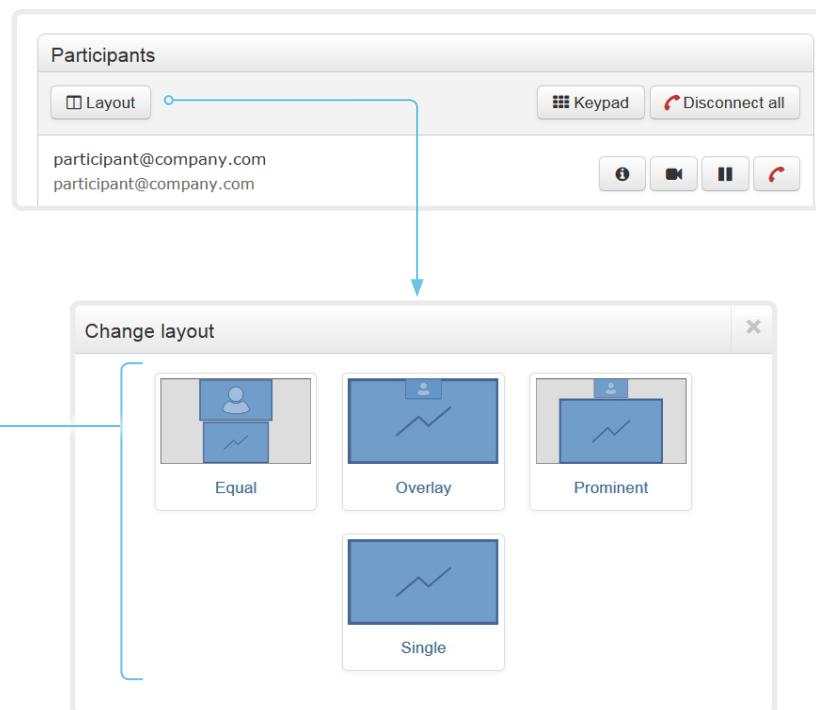
プレゼンテーション ソースは、ビデオ入力またはお使いのビデオ システムに接続することができます。プレゼンテーション ソースとして最も多く使用されるのは PC ですが、システムの設定によってはその他のオプションを使用できる場合があります。

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。

ローカル レイアウトの制御

Web インターフェイスにログインし、[\[コール制御\(Call Control\)\]](#)に移動します。



レイアウトの変更

[\[レイアウト\(Layout\)\]](#)をクリックし、表示されるウィンドウで望ましいレイアウトを選択します。

選択するレイアウトのセットは、システム設定によって異なります。

レイアウトは、アイドル中でも通話中でも変更可能です。

レイアウトについて

ここでいうレイアウトとは、プレゼンテーションとビデオを画面に表示するさまざまな方法のことです。会議の種類によって、レイアウトを変える必要があります。

通話や会議の参加者の数は、選択肢に反映されます。

ローカル カメラの制御

Web 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

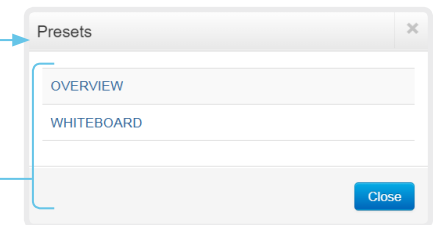
- [\[ビデオ\(Video\)\]](#) > [\[入力\(Input\)\]](#) > [\[コネクタ n\(Connector n\)\]](#) > [\[カメラ制御\(CameraControl\)\]](#) > [\[モード\(Mode\)\]](#) 設定が [\[オン\(On\)\]](#) になっている。
- カメラにパン、チルト、またはズーム機能が付いている。
- スピーカーのトラッキングはオフです。

スナップショット領域

メイン入力ソースのスナップショットが表示されます。

リモート モニタリング オプションがあるビデオ システムでのみ利用できます。

スナップショットを自動更新する



カメラのプリセット位置への移動

1. [\[プリセット...\(Presets...\)\]](#) をクリックして、使用可能なプリセットのリストを開きます。
プリセットが定義されていない場合は、ボタンが無効になり、[\[プリセットなし\(No presets\)\]](#) と表記されます。
2. プリセットの名前をクリックすると、カメラがそのプリセット位置に移動します。
3. [\[Close\]](#) をクリックして、ウィンドウを閉じます。



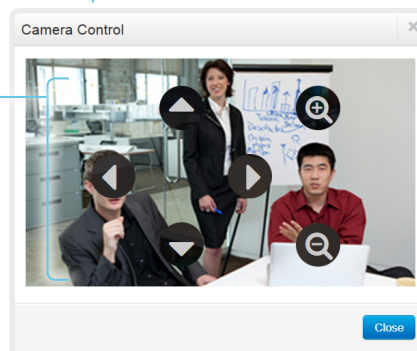
Web インターフェイスを使用してプリセットは定義できません。タッチ コントローラを使用する必要があります。

プリセットを選択すると、スピーカーのトラッキングは自動的にオフになります。

パン/チルト/ズーム コントロールを使用したカメラの移動

スピーカーのトラッキングをオンにすると、カメラ制御は使用できません。

1. カメラ アイコンをクリックして、カメラ制御ウィンドウを開きます。
部屋からのビデオ スナップショットは、リモート モニタリング オプションがあるビデオシステムにのみ表示されます。
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。
関連するコントロールのみがウィンドウに表示されます。
3. [\[Close\]](#) をクリックして、ウィンドウを閉じます。



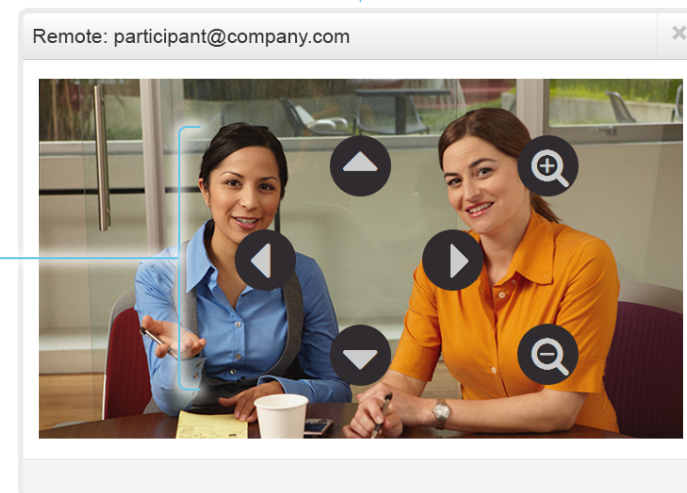
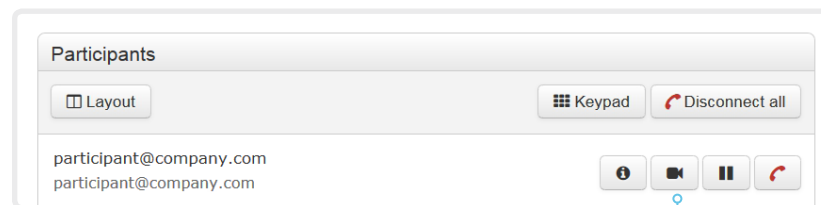
相手先カメラの制御

Web 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。

- ・ 遠端ビデオ システムで [\[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 ビデオ システムにリモート 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ビデオ システムを使用した場合の品質を向上させます。

ClearPath はシスコ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

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

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

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

Web インターフェイスから人の存在の検出をオンまたはオフにできます。Web 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\(Configuration\)\]](#) > [\[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、ビデオ システムが室内にいる人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、ビデオ システムは通話中のときまたはセルフ ビューに画像を表示したときにのみ人数をカウントします。

非通話中の人をカウントするように選択できます。有効にすると、ビデオ システムはビデオ システムがスタンバイ モードでない限り、人数を数えます。セルフ ビューがオフであっても、これは非通話中の人数を含みます。Web 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\(Configuration\)\]](#) > [\[ルーム分析\(RoomAnalytics\)\]](#) > [\[非通話中の人をカウント\(PeopleCountOutOfCall\)\]](#) に移動します。

Status(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て、[\[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トを見ることができます。セルフ ビューをオンにしてタッチ コントローラの左上隅にある連絡先情報をタップし、[\[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。

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

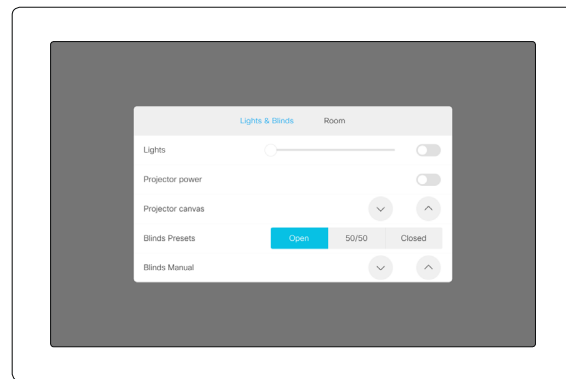
通話履歴コマンドは、API(Application Programming Interface)から使用できます。詳細については、お使いの製品の API リファレンス ガイドを参照してください。

参照先: ► <https://www.cisco.com/go/roomkit-docs> [英語]

ビデオ システムの Touch 10 ユーザ インターフェイスをカスタマイズ (1/2 ページ)

照明やブラインドなど、会議室内の周辺機器の制御を許可するようにユーザ インターフェイスをカスタマイズすることができます。また、マクロをトリガーすることによってビデオ システムの動作を変更します。

これにより、制御システムの機能とビデオ システムのユーザ フレンドリーなユーザ インターフェイスとの強力な組み合わせが可能になります (Touch 10)。



室内制御パネルの例

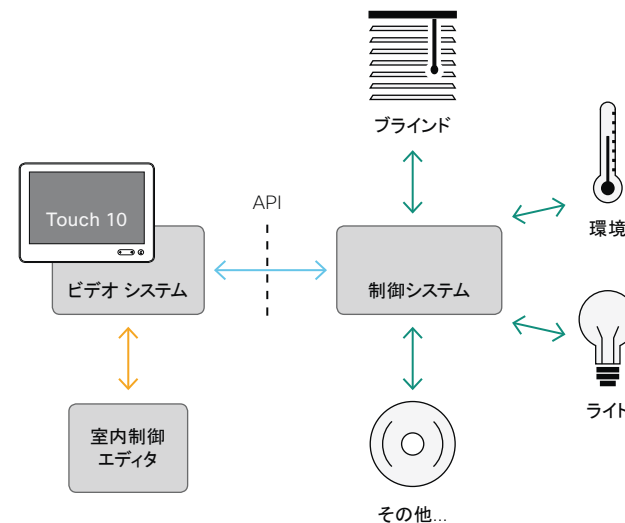
室内制御エディタを使用してカスタム ユーザ インターフェイス パネル (室内制御パネル) を設計する方法、およびビデオ システムの API を使用して室内制御をプログラミングする方法の詳細については、『CE カスタマイズガイド』[英語] を参照してください。次のリンクにアクセスします。

▶ <https://www.cisco.com/go/in-room-control-docs> [英語]

室内制御アーキテクチャ

Touch 10 コントローラおよび制御システムでは、シスコのビデオ 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があります。これはビデオ システムではなく、周辺機器を制御する制御システムです。

制御システムをプログラミングする場合、ビデオ システムのユーザ インターフェイス上のコントロールを接続するために、ビデオ システムの 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 システムのマクロ フレームワークは、制御システムとしても役立つことがあります。この場合、制御システムはビデオ システムの 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。

ビデオ システムの Touch 10 ユーザ インターフェイスをカスタマイズ (2/2 ページ)

室内制御エディタ

無料のエディタ

ビデオ システムのソフトウェアには、無料の使いやすいドラッグ アンドドロップ エディタが付属しています。カスタム ユーザ インターフェイス パネル(室内制御パネル)の構成にはこれを使用してください。

Web インターフェイスにサインインして、[\[統合\(Integration\)\] > \[室内制御\(In-Room Control\)\]](#)に移動します。

- ・ [\[エディタの起動\(Launch Editor\)\]](#) をクリックして、エディタをビデオ システムの Web インターフェイスから直接起動します。

新しい室内制御パネルをビデオ システムにプッシュすることができます。結果はタッチ コントローラ上に即座に表示されます。

- ・ [\[エディタをダウンロード\(Download Editor\)\]](#) をクリックして、お使いのハード ドライブからブラウザでローカルに実行できるスタンドアロン バージョンをダウンロードします。

これにより、ビデオ システムに接続せずにカスタム インターフェイスを構成できます。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 バージョンとビデオ システム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。

プレビュー機能はお使いのカスタム(室内制御)パネルの完全なソフトウェア バージョンでもあるため、制御をクリックすると、実際の Touch 10 ユーザ インターフェイスで選択されるのと同じ動作が発生します。

したがって、実際の Touch 10 ユーザ インターフェイスで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。離れた場所からビデオ システムの室内制御を使用することもできます。

ルーム シミュレータ

ルーム シミュレータを使用して、Touch 10 ユーザ インターフェイスの室内制御により、室内の状態がどのように変更されたかを可視化することができます。



ビデオ システムのシミュレータ設定をエクスポートする前に、すべての既存の室内の設定をバックアップします。シミュレータ設定は、ビデオ システム上の既存の設定を置き換えます。

Web インターフェイスにサインインして、[\[統合\(Integration\)\] > \[室内制御\(In-Room Control\)\]](#)に移動します。

- ・ [\[シミュレータの起動\(Launch Simulator\)\]](#) をクリックして、ルーム シミュレータをブラウザで開きます。

ルーム シミュレータには、ビデオ システムにエクスポート可能な定義済みの室内制御設定が含まれます。つまり、実際の Touch 10 ユーザ インターフェイスから、シミュレータの仮想会議室を制御することができます。

- ・ [\[シミュレータ設定のロード\(Load simulator config\)\]](#) をクリックして、ビデオ システムのシミュレータ設定をエクスポートします。

* 制御システムをプログラミングするときに必要な室内制御エディタおよび API コマンドにアクセスするには、ROOMCONTROL、INTEGRATOR、または ADMIN ユーザ ロールを持つユーザが必要です。

マクロを使用したビデオ システムの動作のカスタマイズ

マクロにより、ビデオ システム上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。

マクロ フレームワークを利用して、インテグレータはビデオ システムの動作を個別の顧客要件に応じて調整するスクリプトを作成することができます。インテグレータが行える作業には、独自の機能または機能のバリエーションの実装、特定の設定または再設定の自動化、機能のカスタム テストやモニタリングの作成などがあります。

マクロの使用とカスタム ユーザ インターフェイス(以前は室内制御パネルと呼ばれた)の作成を組み合わせることで、ユーザ インターフェイス(Touch 10)を修正して、カスタマイズされたローカル機能をトリガーできます。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

マクロについての詳細およびビデオ システムの組み込みマクロエディタの使用方法については、[CE カスタマイズ ガイド \[英語\]](#) 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> [\[英語\]](#)

ビデオ システムでのマクロの使用の許可

Web 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、ポップアップ メッセージが表示されます。[\[マクロの有効化\(Enable Macros\)\]](#) をタップして応答した場合は [\[マクロ\(Macros\)\]](#) > [\[モード\(Mode\)\]](#) 設定が自動的に [オン(On)] に変更され、エディタが起動します。

マクロ エディタの起動

Web インターフェイスにサインイン * して、[\[統合\(Integration\)\]](#) > [\[マクロ エディタ\(Macro Editor\)\]](#) に移動します。

オフラインで使用可能なエディタのスタンドアロン バージョンは提供されていません。

マクロ エディタ

マクロ エディタは、以下のことができる強力なツールです。

- ・ 変更したり、そのまま使用したり、または自身のマクロを記述する際のヒントとして使用したりするコードの例をロードできます。
- ・ 詳細なマクロ記述チュートリアルを用意しているので、参照してください。コードの例についても、より詳しく説明しています。
- ・ 独自のマクロを記述し、ビデオ システムにアップロードできます。
- ・ マクロは、個別に有効または無効にできます。
- ・ マクロを実行したときの動作は、組み込みのログ コンソールで確認できます。

* マクロ エディタにアクセスするには、ADMIN ユーザ ロールを保持しているユーザが必要です。

入力ソースの構成 (1/2 ページ)

ビデオ システムの API を使用すると、単一の主要なビデオ ストリームで最大 4 つの入力ソースを結合できます。

入力ソースの最大数は、ビデオ システムによって異なります。

ビデオ システム	組み合わせることができる異なる 入力ソースの最大数
Room Kit, SX20, MX200 G2, MX300 G2	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

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。

- ・ 等しい
- ・ PIP (2 つの入力ソースを構成するときのみ使用可能)

レイアウトは固定されるため、画像サイズの変更や、PIP の移動はできません。

構成とレイアウトは、コールとコール外の両方でいつでも変更できます。

自画面

自画面は、遠端に送信されるのと同じ構成イメージを示します。

個別カメラ制御

API コマンド(xCommand Camera *)を使用して、個々のカメラを制御することができますが、ユーザ インターフェイス上の制御は使用できません。

ユーザ インターフェイスでカメラを選択すると、メインのビデオ ストリームが構成されたビデオ ストリームから、選択されたカメラからの単一のストリームに切り替えられます。

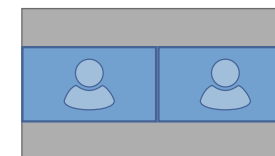
オン デマンドによる構成およびレイアウトの変更

入力ソース構成は 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。

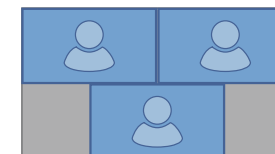
構成とレイアウトをオン デマンドで簡単に変更できるようにするには、マクロを使用してカスタム ユーザ インターフェイス パネル(室内制御パネル)を作成することをお勧めします。

レイアウト

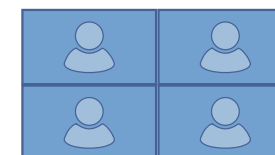
等しい



ソースの数:2

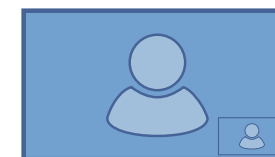


ソースの数:3



ソースの数:4

ピクチャインピクチャ(PIP)



ソースの数:2

入力ソースの構成 (2/2 ページ)

API コマンド

```
xCommand Video Input SetMainVideoSource
ConnectorId: <1..n> SourceId: <1..m>
Layout: <Equal, PIP>
```

値は次のとおりです。

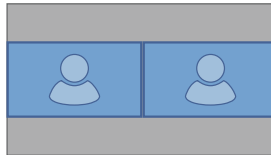
入力ソースは、(ConnectorId)に接続されている物理コネクタか、論理ソース識別子(SourceId)のいずれかによって識別できます。同じコマンド内で異なる識別子を混合することはできません。ConnectorId または SourceId のいずれかを使用してください。これらの識別子は、*[ビデオ入力コネクタ(Video Input Connector)]* および *[ビデオ入力ソース(Video Input Source)]* のステータスで見つけることができます。

Equal レイアウトと PIP レイアウト(Layout)の違いは、サイドバーに表示されます。

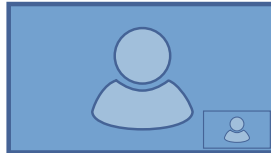
詳細については、API ガイドを参照してください。

例

```
xCommand Video Input SetMainVideoSource ConnectorId: 1 ConnectorId: 2 Layout: Equal
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: PIP
```



プレゼンテーションソースの構成 (ページ 1)

ビデオ システムの API を使用すると、単一のビデオ ストリームで最大 4 つのプレゼンテーションソースを組み合わせることができます。

プレゼンテーションソースの最大数は、ビデオ システムによって異なります。

ビデオ システム	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, SX20, MX200 G2, MX300 G2	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 (DVI, VGA, HDMI など) 経由で共有されているソースのみ共有できます。

ソース構成

構成レイアウト

プレゼンテーションのソースは等間隔のレイアウトで組み合わせられます。イメージのサイズを変更することはできません。

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。

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。

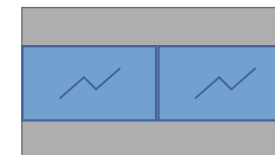
オン デマンドによる構成およびレイアウトの変更

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 ユーザ インターフェイス パネル (室内制御パネル) を作成することをお勧めします。

レイアウト

等しい



ソースの数:2



ソースの数:3



ソースの数:4

プレゼンテーションソースの構成 (ページ 2)

API コマンド

```
xCommand Presentation Start
  ConnectorId: <1..n>
  PresentationSource: <1..m>
  Instance: <1..p>
  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。

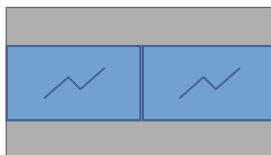
詳細については、API ガイドを参照してください。

例

```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2
```



```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2
```



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て、[統合 \(Integration\)](#) > [スタートアップ スクリプト \(Startup Scripts\)](#) を選択します。

スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます*

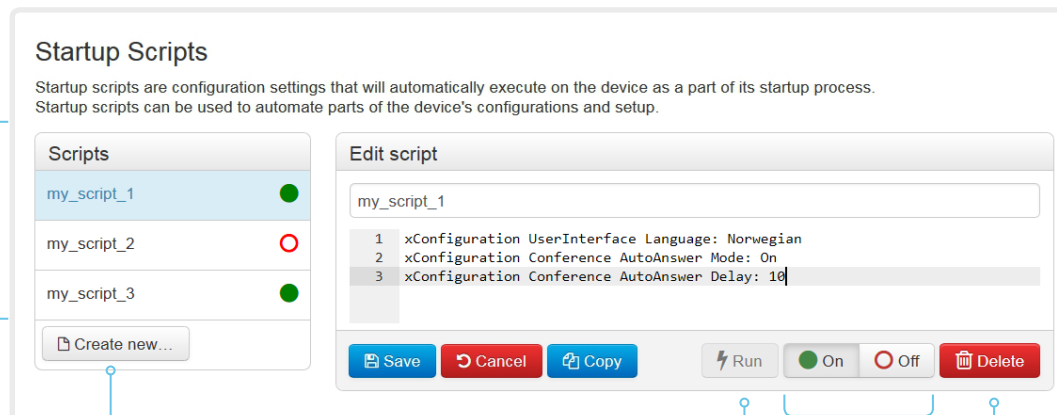
緑色のドットがアクティブなスタートアップ スクリプトの横に、赤色の丸が非アクティブなスタートアップ スクリプトの横に表示されます。

複数のスタートアップ スクリプトがある場合は、リストの上から下に順番に実行されます。

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。



図に示しているスクリプト名と設定は一例です。独自のスクリプトを作成できます。

スタートアップ スクリプトをすぐに実行する

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、ビデオ システムが起動するたびに呼び出されます。

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。

ビデオ システムの XML ファイルにアクセスする

Web 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 ファイルはビデオ システムの API の一部です。システムに関する情報が階層で構成されています。

- *Configuration.xml* には現在のシステム設定 (コンフィギュレーション) が含まれます。これらの設定は、Web インターフェイスまたは API (アプリケーション プログラミング インターフェイス) から制御されます。
- *status.xml* 内の情報は常にビデオ システムによって更新され、システムおよびプロセスの変更が反映されます。ステータス情報は、Web インターフェイスまたは API からモニタします。
- *Command.xml* にはアクションの実行をシステムに指示するために使用できるコマンドの概要が含まれます。コマンドは、API から発行されます。
- *Valuespace.xml* には、システム設定、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、ビデオ システム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、ビデオ システムの API ガイドで説明されています。

Web インターフェイスからの API コマンドとコンフィギュレーションの実行

Web インターフェイスにサインインして、[\[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、Web インターフェイスから実行できます。構文とセマンティックについては、ビデオ システムの API ガイドで説明されています。

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。

Execute API commands and configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

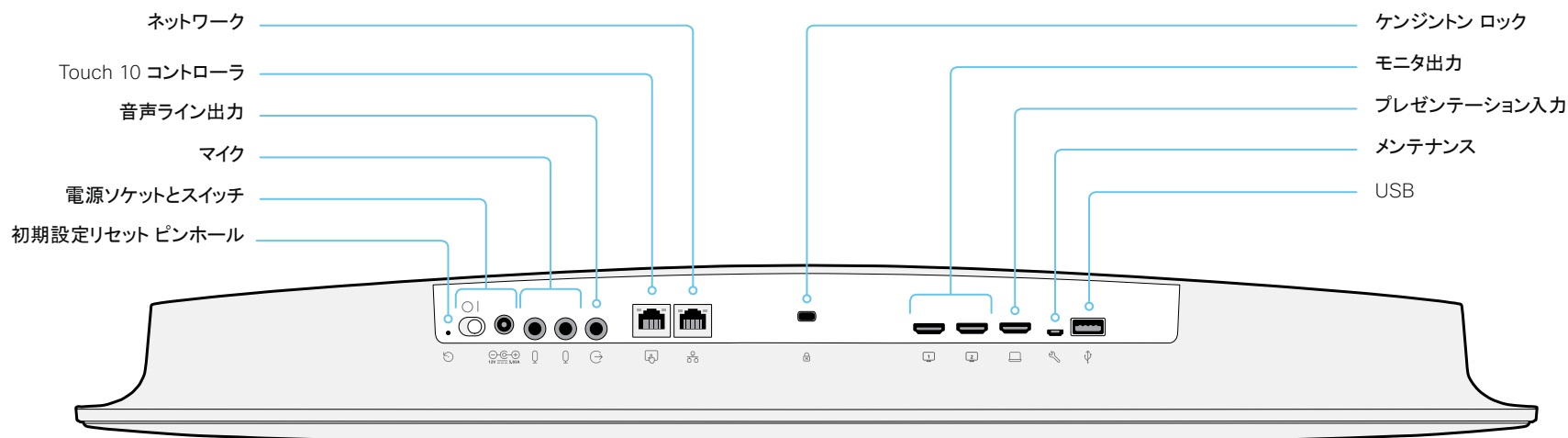
Enter commands...

Execute

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、ビデオ システム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、ビデオ システムの API ガイドで説明されています。

コネクタ パネル



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)。

Touch 10 コントローラ

Touch 10 は、このソケットでは提供されていないイーサネット経由で電源供給されています。したがって、Touch 10 とビデオ システム間にはミッドスパン パワー インジェクタが必要です。▶「[Touch 10 コントローラの接続](#)」の章を参照してください。

音声ライン出力

3.5 mm ミニジャック、3 ピン コネクタ。アクティブ スピーカー(増幅器内蔵)またはセルフパワー型サブウーファーと共に使用します (Audio Output Line OutputType の設定を参照)。

マイク

2 つの 3.5 mm ミニジャック、外部マイク用の 4 ピン コネクタ: Cisco Table Microphone 20 または Cisco TelePresence Ceiling Microphone。

電源

必ず付属の電源を使用してください。

- ・ DC 出力: 5.83 A、12 V
- ・ AC 入力: 100 ~ 240 V、50 ~ 60 Hz、最大 1.2 A

電源スイッチがオンの位置にある場合、システムは自動的に電源が入ります。

初期設定リセット ピンホール

ピンホールは最後の手段として使用してください。初期設定へのリセットは、Touch ユーザ インターフェイスまたは Web インターフェイスから実行することをお勧めします。

モニタ出力

HDMI バージョン 2.0、最大解像度は 60 fps で 3840 × 2160。メイン モニタには出力 1 を使用し、出力 2 はオプションの 2 番目のモニタに使用します。これらの出力には音声がありません。高解像度とフレーム レートをサポートするプレミアム HDMI ケーブルが必要です。シスコ認定ディスプレイ ケーブルをお勧めします。

プレゼンテーション入力

HDMI バージョン 1.4b、最大解像度は 30 fps で 3840 × 2160。コンピュータや外部再生デバイス(オーディオおよびビデオ)など、異なるタイプの入力ソースに使用されます。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。シスコ認定プレゼンテーション ケーブルをお勧めします。

メンテナンス

ビデオ システムとのシリアル通信には、マイクロ USB コネクタを使用します。

USB

USB 2.0(将来的に使用)。

ケンジントン ロック

ビデオ システムの移動または盗難を防止するために、ケンジントン ロックを使用できます。

メンテナンス用のシリアル インターフェイス

ビデオ システムとの直接通信には、マイクロ USB コネクタを使用します¹。マイクロ USB to USB ケーブルが必要です。コンピュータがシリアル ポートドライバを自動インストールしない場合には、手動でコンピュータにインストールする必要があります。²

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も使用できます。

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

ビデオ システムの設定値

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。

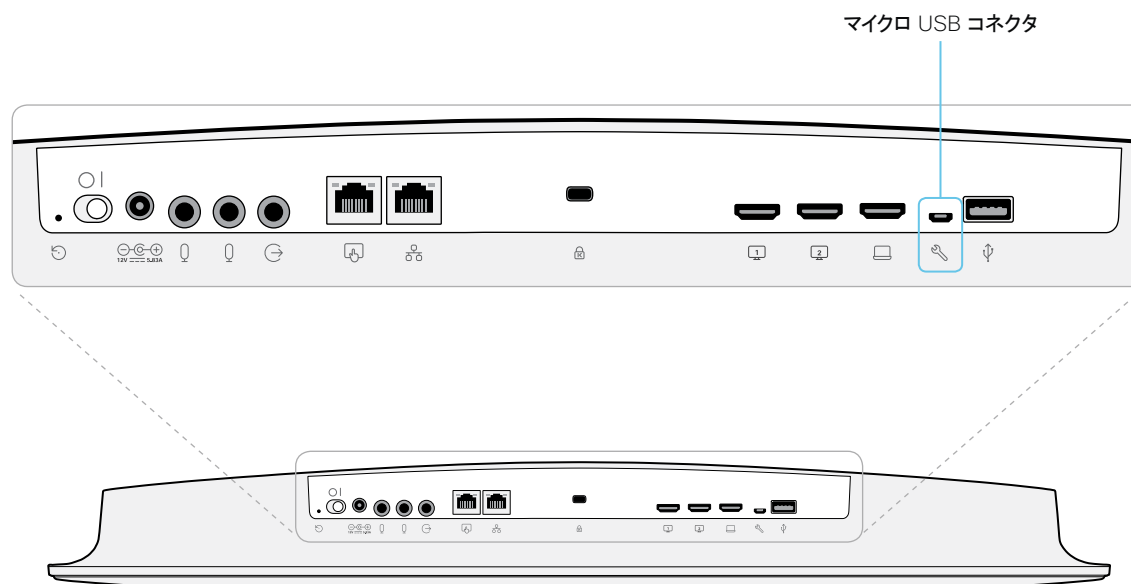
[シリアルポート (SerialPort)] > [モード (Mode)]

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)]

シリアル ポートの設定を変更した後、ビデオ システムを再起動します。

ビデオ システムが CUCM によりプロビジョニングされる場合、シリアル ポート設定は CUCM から設定する必要があります。



¹ マイクロ USB ポートはメンテナンス用途で使います。シリアル接続経由でビデオ システムの API にアクセスする場合は、USB ポート (タイプ A) に接続します。詳細については、API ガイドを参照してください。

² UART ブリッジ仮想 COM ポート (VCP) ドライバには、CP210x USB が必要です。次の内容を参照してください。▶ <http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

TCP ポートの開放

コーデック内の Web サーバでは、非セキュアまたは不必要なポート、プロトコル、モジュール、またはサービスの使用が禁止または制限されています。いくつかのポートは、デフォルトで開放されているか、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 4051:リモート ペアリング セッション接続

このポートは、Touch パネルがビデオ システムとリモート 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 4052:リモート ペアリングおよび転送

このポートは、Touch パネルがビデオ システムとリモート 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

システム設定は、Web インターフェイスの [\[セットアップ\(Setup\)\]](#) > [\[構成\(Configuration\)\]](#) ページから設定します。Web ブラウザを開き、ビデオ システムの IP アドレスを入力して、サインインします。

TMS からの新しい HTTPFeedback アドレスの取得

ビデオ システムが 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。ビデオ システムは、これらのイベントが TMS から送信されるようにアドレスを受信します (HTTPFeedback address)。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、ビデオ システムは 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

ビデオ システムがイベントへの応答を受信しない場合、1 秒間隔で最大 10 回、HTTPFeedback アドレスに送信を再試行します。

ビデオ システムが再試行でも応答を受信しない場合、エンドポイントは HTTPFeedback アドレスを削除し、TMS にイベントを送信できなくなります。

これは TMS の通話詳細記録 (CDR) が失われる原因になります。

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、ビデオ システムを再起動して、TMS から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 (予定されているか、TMS 管理者によってトリガーされる)。

技術仕様 (1/2 ページ)

ソフトウェアの互換性

- ・ シスコ コラボレーション エンドポイント ソフトウェア パー
ジョン 9.0 以降
- ・ RoomOS

帯域幅

ポイントツーポイントで最大 6 Mbps

ファイアウォール トラバース

- ・ Cisco TelePresence Expressway テクノロジー
- ・ H.460.18 および H.460.19 ファイアウォール トラバ
ース

ビデオ標準

- ・ H.264
- ・ H.265(SIP)

ビデオ入力

- ・ 30 fps で最大 3840 × 2160(60 fps で 1920 × 1080
を含む)をサポートする 1 つの HDMI 入力 *
- ・ Consumer Electronics Control (CEC) 2.0

ビデオ出力

- ・ 60 fps で最大 3840 × 2160 をサポートする 2 つの
HDMI 出力 *
- ・ ライブ ビデオ解像度(エンコードおよびデコード)30fps ま
たは 60fps で最大 1920 × 1080
- ・ Consumer Electronics Control (CEC) 2.0

音声標準

- ・ AAC-LD
- ・ G.722
- ・ G.722.1
- ・ G.711
- ・ G.729
- ・ Opus

音声機能

- ・ ハイクオリティ 20kHz オーディオ
- ・ サブウーファー用の予備(ライン出力)
- ・ 誘導ループ用の予備(ライン出力)
- ・ 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

音声入力

- ・ 2 つのマイク、4 ポール ミニジャック
- ・ HDMI からのオーディオ入力 1 個
- ・ 統合マイク

オーディオ出力(外部)

- ・ ライン出力 1 個、ミニジャック(ステレオ)

スピーカー(統合)

- ・ 平衡型構成の高品質スピーカー 5 個
- ・ 周波数特性:70Hz ~ 20kHz
- ・ 増幅器用電源:24W
- ・ 最大出力レベル:86dB SPL

スピーカー トラッキング

- ・ スピーカー トラッキング用の 6 要素マイク アレイ

デュアル ストリーム

- ・ H.239 デュアル ストリーム(H.323)
- ・ BFCP デュアル ストリーム(SIP)
- ・ 解像度のサポート:8 fps で最大 3840 × 2160、30 fps
で最大 1920 × 1080

ワイヤレス共有

- ・ Cisco Webex クライアント(最大解像度 3840 ×
2160 - 5 fps)
- ・ Cisco Intelligent Proximity クライアント(5 fps で 最大
1920 × 1080)

マルチポイント サポート

- ・ マルチサイト オプションで組み込み 4-way SIP/H.323
会議機能

マルチサイト機能(組み込みマルチポイント)、オプションのア ップグレード

- ・ 適応型 SIP/H.323 マルチサイト:
 - 3-way 解像度は 30 fps で最大 1920 × 1080、コンテ
ンツは 5 fps で最大 3840 × 2160
 - 4-way 解像度は 30 fps で最大 1920 × 1080、コンテ
ンツは 5 fps で最大 3840 × 2160
- ・ 完全個別音声および映像トランスコーディング
- ・ 同一会議で H.323、SIP、VoIP が混在可能
- ・ 5 fps で最大 3840 × 2160 の解像度で、任意の参加者
からのプレゼンテーション(H.239/BFCP)をサポート
- ・ ベスト インプレッション機能(自動連続表示レイアウト)
- ・ 任意のサイトからの暗号化およびデュアル ストリーム

プロトコル

- ・ H.323
- ・ SIP
- ・ Cisco WebEx

組み込み暗号化

- ・ H.323 および SIP ポイントツーポイント
- ・ 規格標準:H.235 v3 および Advanced Encryption
Standard(AES)
- ・ キーの自動生成と交換

IP ネットワーク機能

- ・ サービス設定での DNS ルックアップ
- ・ 差別化サービス(QoS)
- ・ IP 帯域幅最適化コントロール(フロー制御を含む)
- ・ 自動ゲートキーパー検出
- ・ ダイナミック再生およびリップシンクのバッファリング
- ・ H.323 の H.245 DTMF トーン
- ・ SIP の RFC 4733 DTMF トーン
- ・ NTP による日時のサポート
- ・ パケット損失時のダウンスピード機能
- ・ URI ダイアル
- ・ DHCP(ダイナミック ホスト コンフィギュレーション プロト
コル)
- ・ IEEE 802.1x ネットワーク認証
- ・ IEEE 802.1q VLAN
- ・ IEEE 802.1p QoS および Class of Service(CoS)9
- ・ ClearPath

IPv6 ネットワークのサポート

- ・ H.323 および SIP に対する単一コール スタックのサポ
ート
- ・ DHCP、SSH、HTTP、HTTPS、DNS、および DiffServ に
対するデュアル スタックの IPv4 および IPv6
- ・ ステティック IP アドレスの割り当て、ステートレス自動設定
および DHCPv6 をサポート

CISCO UNIFIED COMMUNICATIONS MANAGER

- ・ Cisco Unified Communications Manager(CUCM)の
ネイティブ登録
- ・ CUCM バージョン 9.1.2 以降と Cisco Webex Room
Kit のデバイス パックが必要

セキュリティ機能

- ・ HTTPS および SSH を使用して管理
- ・ IP 管理パスワード
- ・ 管理メニューのパスワード
- ・ IP サービスの無効
- ・ ネットワーク設定の保護

* 入力用:HDMI パーバージョン 1.4b、出力用:HDMI パーバージョン 2.0

技術仕様 (2/2 ページ)

ネットワーク インターフェイス

- ・ LAN 用イーサネット(RJ-45)X 1、10/100/1000 Mbps
- ・ Cisco Touch 10 用イーサネット(RJ-45)X 1
- ・ Wi-Fi: IEEE 802.11a/b/g/n/ac 2.4 GHz、5 GHz、2x2 MIMO

その他のインターフェイス

- ・ USB 2.0 ポート
- ・ マイクロ USB
- ・ 初期設定リセット ピンホール

カメラの概要

- ・ 5K Ultra HD カメラ
- ・ 最大 60 fps のサポート(スピーカー トラッキングでは 30 fps および最適な全体表示が有効)
- ・ 15.1 メガピクセル イメージ センサー(5184 × 2916 ピクセル)
- ・ 1/1.7 CMOS
- ・ 3 倍ズーム
- ・ 絞り f/2.0
- ・ 水平視野 83 °、垂直視野 51.5 °
- ・ 自動フレーミング(オーディオと顔検出)
- ・ 自動フォーカス、輝度およびホワイト バランス
- ・ 焦点距離: 1 m ~ 無限遠

電源

- ・ 100-240 VAC、50/60 Hz、12 V DC 入力
- ・ 平均 20 W、ピーク時 70 W

動作温度および湿度

- ・ 周囲温度: 0 ~ 40 ° C(32 ~ 104 ° F)
- ・ 相対湿度(RH): 10 ~ 90%

保管および輸送の温度

- ・ RH 10 ~ 90% では -20 ~ 60 ° C(-4 ~ 60 ° F)(結露しないこと)

ロック機構

- ・ ケンジントン セキュリティ ロック

寸法

- ・ 幅: 700 mm(27.5 インチ)
- ・ 高さ: 106 mm(3.5 インチ)
- ・ 奥行: 88 mm(2.9 インチ)
- ・ 重量: 最大 3.2 kg(7 ポンド)

認定および適合規格

- ・ 指令 2014/35/EU(低電圧指令)
- ・ 指令 2014/30/EU(EMC 指令): クラス A
- ・ 指令 2014/53/EU(無線機器指令)
- ・ 指令 2011/65/EU(RoHS)
- ・ 指令 2002/96/EC(WEEE)

- ・ NRTL 認定(製品の安全性)
- ・ FCC CFR 47 Part 15B(EMC): クラス A
- ・ FCC Listed(無線機器)

各国の認定書類については、Product Approval Status Database(製品認定ステータス データベース) www.cisco.com/go/productapproval 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。

Cisco および Cisco ロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。Cisco の商標の一覧については、www.cisco.com/go/trademarks/ をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。

2018 年 4 月

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)』: オファ
ーまたはアンサー プロトコル用のネットワーク アドレス変換(NAT)通
過のためのプロトコル
- RFC 5589『SIP Call Control Transfer』
- RFC 5766『Traversal Using Relays around NAT (TURN)』
:Session Traversal Utilities for NAT(STUN)のためのリレー拡張
- RFC 5905『Network Time Protocol Version 4: Protocol and Algorithms Specification』

シスコ Web 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/roomkit-docs> [英語]

MX シリーズ:

▶ <https://www.cisco.com/go/mx-docs> [英語]

SX シリーズ:

▶ <https://www.cisco.com/go/sx-docs> [英語]

DX シリーズ:

▶ <https://www.cisco.com/go/dx-docs> [英語]

通常、すべてのシスコ コラボレーション エンドポイントのユーザ マニュアルはこちらから検索できます。▶ <https://www.cisco.com/go/telepresence/docs> [英語]

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

- ・ *インストール ガイド*: 製品のインストール方法
- ・ *スタートアップ ガイド*: システムを稼働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*: システムを稼働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
- ・ 『*Deployment guide for TelePresence endpoints on CUCM*』: ビデオ システムを Cisco Unified Communications Manager (CUCM) とともに使用開始するために実行するタスク
- ・ *スベア部品の概要、スベア部品の交換ガイド、ケーブル スキーマ*: スベア部品を交換するときに役立つ情報

保守と運用 > エンドユーザ ガイド

- ・ *ユーザ ガイド*: 製品の使用方法
- ・ *クイック リファレンス ガイド*: 製品の使用方法
- ・ *物理インターフェイス ガイド*: コネクタのパネルと LED など、コーデックの物理インターフェイスに関する詳細

リファレンス ガイド > コマンド リファレンス

- ・ 『*API リファレンス ガイド*』: Application Programmer Interface (API) のリファレンス ガイド

リファレンス ガイド > テクニカル リファレンス

- ・ *CAD 図面*: 測定値付き 2D CAD 図面

設定 > 設定ガイド

- ・ *CE 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、ビデオシステムの API を用いた室内操作のプログラミングの方法、マクロの作成方法、ビデオスイッチの使い方、オーディオコンソールを用いた上級者向けの音声セットアップと設定方法。

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 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および通知

[ソフトウェア ダウンロード、リリースと一般情報 (Software Downloads, Release and General Information)] > [リリースノート (Release Notes)]

- ・ *ソフトウェア リリース ノート*

シスコのお問い合わせ先

シスコの Web サイトでは、シスコの世界各地のお問い合わせ先を確認できます。

参照先: ▶ <https://www.cisco.com/go/offices> [英語]

本社
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

Intellectual property rights

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

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

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティング システムの UCB パブリックドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号については、シスコの Web サイトをご覧ください (www.cisco.com/go/offices)。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

シスコ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。By using this product you agree to comply with applicable laws and regulations. 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。