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 9.3
2018 年 4 月

管理者ガイド

Cisco TelePresence SX10 クイック セット

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。

製品マニュアルのこの部分は、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。

この管理者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。このガイドについてのご意見、ご感想をお聞かせください。

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。

ユーザ マニュアルは次の URL から入手できます。
► https://www.cisco.com/go/sx-docs

本ガイドの使用方法

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

目次

はじめに 4
ユーザ ドキュメンテーションとソフトウェア 5
CE9 の最新情報 6
SX10 Quick Set の概要 17
電源のオンとオフ 18
LED インジケータ 19
ビデオ システムの管理方法 20

設定 (Configuration) 24
ユーザ管理 25
システム パスフレーズの変更 26
[設定 (Settings)] メニューへのアクセスの制限 27
システム設定 28
サインイン バナーの追加 29
ビデオ システムのサービス証明書の管理 30
信頼できる認証局 (CA) のリストの管理 31
安全な監査ロギングのセットアップ 32
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 33
CUCM 信頼リストの削除 34
永続モードを変更する 35
強力なセキュリティ モードの設定 36
コンテンツ共有のために Intelligent Proximity をセットアップする 37
ビデオ品質対コール レート比の調整 42
カスタム壁紙の追加 43
着信音の選択と着信音量の設定 44
お気に入りリストの管理 45
アクセシビリティ機能のセットアップ 46

Peripherals 47
入力ソース数の拡大 48
ディスプレイについて 49
Touch 10 コントローラの接続 50
ISDN リンクの接続 53

Maintenance 54
システム ソフトウェアのアップグレード 55
オプション キーの追加 57
システム ステータス 58
診断の実行 59
ログ ファイルのダウンロード 60

リモート サポート ユーザの作成 ... 61
設定とカスタム要素のバックアップ/復元 ... 62
カスタム要素の CUCM プロビジョニング ... 63
カスタム要素の TMS プロビジョニング ... 64
以前使用していたソフトウェア イメージへの復元 ... 65
ビデオ システムの工場出荷時設定リセット ... 66
Cisco Touch 10 の初期設定へのリセット ... 69
Cisco TelePresence Touch 10 の初期設定へのリセット ... 70
ユーザ インターフェイスのスクリーンショットのキャプチャ ... 71

システム設定 ... 72
システム設定の概要 ... 73
Audio settings ... 78
CallHistory settings ... 81
Cameras settings ... 82
Conference settings ... 84
FacilityService settings ... 88
H323 settings ... 89
Logging settings ... 92
Network settings ... 93
NetworkServices settings ... 100
Peripherals settings ... 106
Phonebook settings ... 108
Provisioning settings ... 109
Proximity settings ... 111
RTP settings ... 112
Security settings ... 113
SerialPort settings ... 116
SIP settings ... 117
Standby settings ... 121
SystemUnit settings ... 123
Time settings ... 124
UserInterface settings ... 127
UserManagement settings ... 130
Video settings ... 132
Experimental settings ... 138

付録 ... 139
リモート コントロールと画面上のユーザ インターフェイスの使用方法 ... 140
Touch 10 の使用方法 ... 141
リモート モニタリングのセットアップ ... 142
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 ... 143
Web インターフェイスを使用したコールの発信 ... 144
Web インターフェイスを使用したコンテンツの共有 ... 146
ローカル レイアウトの制御 ... 147
ローカル カメラの制御 ... 148
相手先カメラの制御 ... 149
パケット損失の復元力：ClearPath ... 150
ビデオ システムの Touch 10 ユーザ インターフェイス ... 151
スタートアップ スクリプトの管理 ... 153
ビデオ システムの XML ファイルへのアクセス ... 154
Web インターフェイスからの API コマンドと構成の実行 ... 155
シリアル インターフェイス ... 156
TCP ポートの開放 ... 157
TMS からの新しい HTTPFeedback アドレスの取得 ... 158
技術仕様 ... 159
サポートされている RFC ... 161
シスコ Web サイト内のユーザ ドキュメンテーション ... 162
シスコのお問い合わせ先 ... 163

第 1 章

はじめに

ユーザ ドキュメンテーションとソフトウェア

このガイドの対象となる製品

- Cisco TelePresence SX10 クイック セット

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 Spark）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 ドキュメンテーション」
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/sx-docs

クラウドに登録されたデバイスのドキュメンテーション

Cisco Spark 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]

ソフトウェア

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

▶ https://www.cisco.com/cisco/software/navigator.html [英語]

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/telepresence-quick-set-series/tsd-products-support-series-home.html [英語]

CE ソフトウェアへの変換

TC ソフトウェアから CE ソフトウェア にアップグレードする前に、アップグレード要件を考慮することが重要です。アップグレード要件を満たしていない場合は、CE ソフトウェアをアップグレードしても展開できず、ダウングレードが必要となる可能性があります。

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

CE9 の最新情報

この章では、Cisco Collaboration Endpoint ソフトウェア バージョン 9（CE9）を CE8 と比較した場合の、新規および変更されたシステム設定、新機能および改善点の概要を示します。

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

► https://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/tsd-products-support-series-home.html [英語]

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 / 復元機能には、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）] > [バックアップと復元（Backup and Restore）] の順に選択することにアクセスできます。

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、► http://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 DefaultCall Rate）] 設定で指定されているレートが設定されます。

着信音の選択と着信音の音量の調整

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、すぐにアップグレードするか延期するかを選択できます。アップグレードを延期した場合は、以前のように 6 時間待たなくても、準備ができたときにユーザ インターフェイスのメニューから [設定（Settings）] > [このデバイスについて（About this device）] の順に選択してアップグレードを再開できます。

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スフレーズを設定する
- [ユーザ インターフェイス設定メニュー モード（UserInterface SettingsMenu Mode）] を [ロック（Locked）] に設定する
- [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

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。

画面ステータスのモニタリングと制御

SX10 は、Room シリーズのビデオ システムと同様の CEC（コンシューマ エレクトロニクス制御）の動作をするようになりました。

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

CEC は、デフォルトではビデオ システムで無効になっています。Video Output Connector [1] CEC Mode 設定で有効化する必要があります。

1 冊の共通 API ガイド

すべての API 情報が、すべての製品を対象とする 1 冊の API ガイドに集約されています。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

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 またはオンスクリーン）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ています。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。

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。

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。

ユーザ管理のための 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なので、機能をテストできます。テストでは、ビデオ システムに実際のイベントが生成され、サードパーティ製の制御システムを使用して作成したすべての機能をトリガーすることができます。右側のペインのコンソールには、インタラクティブ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 メッセージの両方が表示されます。

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 インターフェイスを使用してデバイス有効化の方法を変更（VCS から Cisco UCM へ、など）すると、ビデオ システムは初期設定に自動的にリセットされ、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てもビデオ システムは初期設定に自動的にリセットされません。

音声とその他のメディア用の個別 RTP ポート範囲のサポート

音声が他のメディアと異なる RTP ポート範囲を使用するようにビデオ システムを設定できます。この 2 つの範囲を重なら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

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、ハーフウェイクという追加のスタンバイ状態があります。 ハーフウェイク状態では、ビデオ システムが使用されていない場合に画面上に簡単な操作ガイドが表示されます。

CE9.0 の新機能および改善点

更新されたユーザ インターフェイス

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

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

モーション検知ウェイクアップ

モーション検知ウェイクアップでは、会議室に入ってくる人を検出し、ビデオ システムを自動的に起動します。この機能を有効にするには、次の設定を有効にする必要があります。

```
xConfiguration Standby WakeupOnMotionDetection
```

この機能が有効なときに、スタンバイ状態のビデオ システムを手動で設定することはできません。

更新された室内制御エディタ

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

言語サポートの追加

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

その他の変更

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

CE9.3 でのシステム設定の変更点

新しい設定

Network [1] DNS DNSSEC Mode

NetworkServices HTTP Proxy PACUrl

SystemUnit CrashReporting Advanced

SystemUnit CrashReporting Mode

SystemUnit CrashReporting URL

UserInterface Accessibility IncomingCallNotification

UserInterface Security Mode

削除された設定

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：値スペース：Manual/Off

新：値スペース：Manual/Off/PACUrl/WPAD

Security Session MaxSessionsPerUser

旧：値スペース：整数（0..100）
デフォルト値：0

新：値スペース：整数（1..20）
デフォルト値：20

Security Session MaxTotalSessions

旧：値スペース：整数（0..100）
デフォルト値：0

新：値スペース：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 Ultrasound MaxVolume
　周辺機器ペアリング ウルトラサウンド音量最大レベルの置き換え
オーディオ ウルトラサウンド モード
　周辺機器ペアリング ウルトラサウンド音量モデルの置き換え
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

会議マルチ ストリーム モード
Peripherals Pairing Ultrasound Volume MaxLevel
　オーディオ ウルトラサウンド最大音量 に置き換え
周辺機器ペアリング ウルトラサウンド音量モード
　オーディオ ウルトラサウンド モードに置き換え

変更されたコンフィギュレーション

Security Audit Logging Mode
　旧：デフォルト値：Off
　新：デフォルト値：Internal
UserInterface Language
　新：値スペースにアラビア語とヘブライ語を追加

CE9.1 でのシステム設定の変更点

新しい設定

なし。

削除されたコンフィギュレーション

なし。

変更されたコンフィギュレーション

Network[1] IEEE8021X Password
- 旧：値スペース：文字列（0, 32)
- 新：値スペース：文字列（0, 50)

Video Input Connector [n] PresentationSelection
- 旧：値スペース：AutoShare/Manual/OnConnect
- 新：値スペース：AutoShare/Desktop/Manual/OnConnect

CE9.0 でのシステム設定の変更点

新しい設定

NetworkServices HTTPS Server MinimumTLSVersion

NetworkServices HTTPS StrictTransportSecurity

Peripherals Pairing CiscoTouchPanels EmcResilience

モーション検知ウェイクアップのスタンバイ

削除されたコンフィギュレーション

UserInterface UserPreferences

Conference VideoBandwidth PresentationChannel Weight

Standby AudioMotionDetection

変更された設定

Cameras Camera [n] *

旧：ユーザ ロール：ADMIN、USER

新：ユーザ ロール：ADMIN、INTEGRATOR

UserInterface Language

新：ポルトガル語を値スペースに追加

新しい INTEGRATOR ユーザ ロールに関する設定

新しいユーザ ロール INTEGRATOR が、CE9.0 で導入されました。このユーザ ロールは次の設定に追加されました。

Audio DefaultVolume

Audio Input Microphone [n] *

Audio Microphones Mute Enabled

Audio Output Line [n] *

Audio SoundsAndAlerts *

CallHistory Mode

Cameras Camera [n] *

Conference DefaultCall Rate

Conference DoNotDisturb DefaultTimeout

FacilityService *

Peripherals Pairing Ultrasound Volume MaxLevel

Peripherals Pairing Ultrasound Volume Mode

Peripherals Profile *

SerialPort Mode

Standby *

SystemUnit Name

Time Zone

UserInterface OSD Output

UserInterface Wallpaper

Video ActiveSpeaker DefaultPIPPosition

Video Input Connector [n] *

Video Monitors

Video Output Connector [n] CEC Mode

Video Output Connector [n] Resolution

Video Output Connector [n] RGBQuantizationRange

Video Presentation DefaultPIPPosition

Video Selfview Default *

Video Selfview OnCall *

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

SX10 Quick Set の概要

Cisco TelePresence SX10 Quick Set はビデオに対応した小型コラボレーション スペース向けに設計されたオールインワン装置です。

標準フラットパネル ディスプレイに取り付けられたコンパクトなデバイスにカメラとコーデックを統合した高品質の装置です。電源と LAN の両方への単一ケーブルを介して電源とイーサネット（PoE）に接続できます。

カメラには広角視野角があり、狭いスペースでも良好な概観を提供します。高解像度ビデオは 1080p30 解像度に対応しています。

機能とメリット

- 最大 1080p30 の最適解像度による WXGAp5 でのコンテンツ共有。
- 広角 83° 水平視野角 5 倍ズーム（光学およびデジタル）。
- Power over Ethernet（PoE）ですぐに使用できる装置。
- 内蔵マイクとオプションの外部 Cisco TelePresence Table Microphone 20。
- TRC6 リモート コントロール（デフォルト）を使用した操作、または 10 インチのタッチ コントローラ（オプション）を使用した操作。
- 低消費のエネルギー効率（EU クラス B）。
- Cisco Unified Communications Manager（UCM）、Cisco TelePresence Video Communication Server（VCS）、および Cisco Spark に登録。

SX10 Quick Set には TRC6 リモート コントロールが付属しています。Cisco TelePresence Touch 10 コントローラをオプションとして注文できます。

標準フラットパネル ディスプレイの上部にマウントさせた SX10 Quick Set

電源のオンとオフ

電源ボタンによる電源のオン / オフ

LED インジケータ付きの電源ボタンが、図に示すように前面にあります。

電源ボタン（LED が電源ボタンを囲んでいます）

電源をオンにする

ビデオ システムが自動的に起動しない場合は、電源ボタンをやさしく押します。

ビデオ システムの起動中は LED が点灯しています。

スイッチを切る

電源ボタンを軽く押して消灯するまで押し続けます。

スタンバイ モードの開始 / 終了

電源ボタンを短く押します。
数秒後にユニットがスタンバイ状態になります。

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...）] をクリックして、選択を確定します。

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...)] をクリックして、選択を確定します。

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

LED インジケータ

ステータス LED

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

通常の動作（非スタンバイ状態）：
点灯します。

スタンバイ モード時：
LED がゆっくり点滅します。

ネットワーク接続がない場合：
LED が 2 回ずつ、繰り返し点滅します。

スタートアップ（起動）時 :
LED が点滅します。

カメラの LED

カメラの LED はカメラのレンズのすぐ上にあります。

コールの着信時 :
LED が点滅します。

コール中 :
点灯します。

ビデオ システムの管理方法

一般的には、この管理者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。

あるいは、次のような方法でビデオ システムの API にアクセスすることもできます。

- HTTP または HTTPS（Web インターフェイスでも使用されます）
- SSH
- Telnet
- 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。

ヒント

API で設定またはステータスを使用できる場合、Web インターフェイスの設定またはステータスが次のように API の設定またはステータスに変換されます。

（Web で）X > Y > Z を **Value** に設定することは次と同等です。
```
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次と同等です。
```
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次と同等です。
```
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	方式を有効 / 無効にする方法
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 ・HTTP：デフォルトで有効 HTTPS：デフォルトで有効	[ネットワークサービス（NetworkServices）] > [HTTP] > [モード（Mode）] 変更を有効にするには、ビデオ システムを再起動します。
Telnet	・非セキュア TCP/IP 接続 ・デフォルトで無効	[ネットワークサービス（NetworkServices）] > [Telnet] > [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。
SSH	・セキュア TCP/IP 接続 ・デフォルトで有効	[ネットワークサービス（NetworkServices）] > [SSH] > [モード（Mode）] 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 有効 ・セキュリティ上の理由から、デフォルトではサインイン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

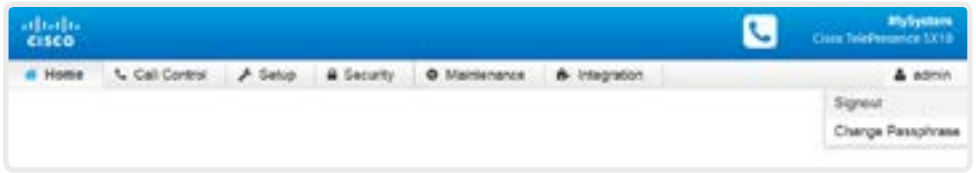
1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. [このデバイスについて（About this device）] に続き、[設定（Settings）] を選択します。

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。

システムには出荷時にデフォルト ユーザ admin（パスフレーズなし）が設定されています。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（Sign out）] を選択します。

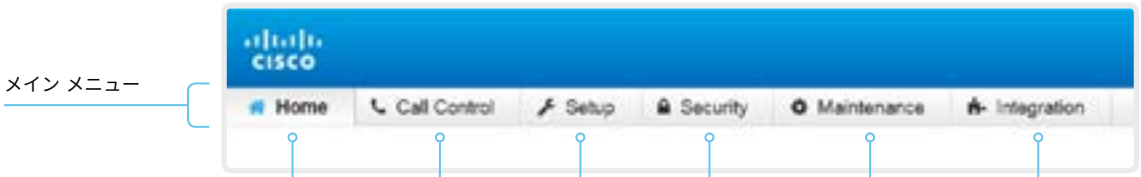
ビデオ システムの管理方法（3/4 ページ）

Web インターフェイスの構成

Web インターフェイスはサブ ページで構成されています。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 Spark）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、およびアクセス権についての詳細は、▶「ユーザ管理」の章を参照してください。



- ホーム
- コール制御
- セットアップ
  - 設定（Configuration）
  - ステータス（Status）
  - 周辺機器（Peripherals）
  - パーソナライゼーション（Personalization）
  - お気に入り（Favorites）
- セキュリティ
  - ユーザ（Users）
  - サービス証明書（Service Certificates）
  - CUCM 証明書（CUCM Certificates）
  - CA（Certificate Authorities）
  - 強力なセキュリティ モード（Strong Security Mode）
  - サインイン バナー（Sign In Banner）
  - 非永続モード（Non-persistent Mode）
- メンテナンス
  - 診断（Diagnostics）
  - システム ログ（System Logs）
  - 通話履歴（Call Logs）
  - ユーザ インターフェイスのスクリーンショット（User Interface Screenshots）
  - ソフトウェア アップグレード（Software Upgrade）
  - オプション キー（Option Keys）
  - バックアップと復元（Backup and Restore）
  - システム リカバリ（System Recovery）
  - 再起動（Restart）
- 統合
  - 室内制御（In-Room Control）
  - スタートアップ スクリプト（Startup Scripts）
  - 開発者 API（Developer API）

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、初期設定へのリセットなど）は、パスフレーズで保護できます。
▶「[設定（Settings）] メニューへのアクセスの制限」の章を参照してください。

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。

アクセス設定

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、パスフレーズは初期設定されていません。

必ず admin ユーザのパスフレーズを設定する必要があります。

パスフレーズの設定方法については、▶「システム パスフレーズの変更」の章を参照してください。

新しいユーザ アカウントを作成する

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. [新規ユーザを追加（Add New User）] を選択します。
3. [ユーザ名（Username）]、[パスフレーズ（Passphrase）]、および [パスフレーズの確認（Repeat passphrase）] の各入力フィールドに入力します。

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

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

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

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

既存のユーザ アカウントの編集

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

ユーザ特権を変更する

1. Web インターフェイスにサインインして、[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 ロールを選択して、ステータスを [アクティブ（Active）] または [非アクティブ（Inactive）] に設定し、ユーザが次回のサインイン時にパスフレーズを変更する必要があるかどうかを決定します。

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

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

パスフレーズの変更

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. 該当する入力フィールドに新しいパスフレーズを入力します。
4. [パスフレーズの変更（Change Passphrase）] をクリックして、変更を保存します。

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

ユーザ アカウントの削除

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、セキュリティ監査設定を変更したり、監査証明書をアップロードしたりすることができます。

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 Spark 登録システム

ビデオ システムがシスコのクラウド サービス（Cisco Spark）に登録されている場合、INTEGRATOR および ROOMCONTROL ユーザ ロールを持つローカル ユーザのみ使用できます。

システム パスフレーズの変更

システム パスフレーズは、以下の操作を行うときに必要となります。

- Web インターフェイスへのサインイン
- コマンドライン インターフェイスへのサインインと使用

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 アクセス権を持つデフォルトのユーザ アカウントが付属しています。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 システムには多くのユーザ アカウントを作成できます。

ユーザ アカウントを作成および管理する方法の詳細については、in the ►「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、[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。

パスフレーズが現在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。

他のユーザのパスフレーズの変更

管理者アクセス権を持っている場合は、任意のユーザのパスワードを変更できます。

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。

   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 コントローラまたはオンスクリーン メニュー）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。

   これで、任意のユーザが、ユーザインターフェイス（タッチ コントローラまたはオンスクリーン メニュー）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。

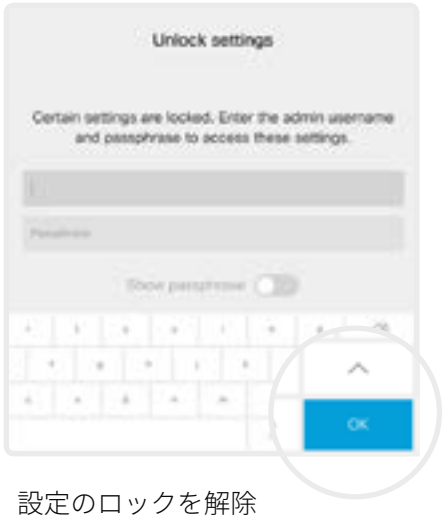
ユーザ インターフェイスの [設定 (Settings)] メニュー

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。

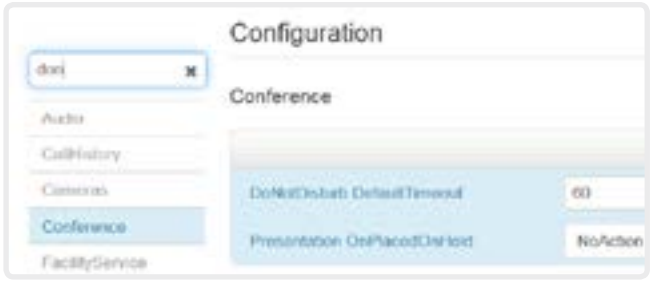
システム設定

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）] に移動します。

システム設定の検索

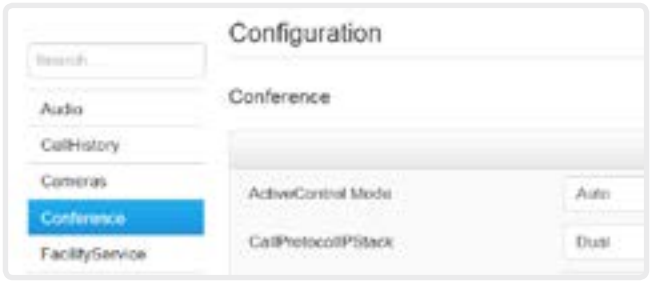
設定の検索

検索フィールドに必要な数の文字を入力します。これらの文字を含む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

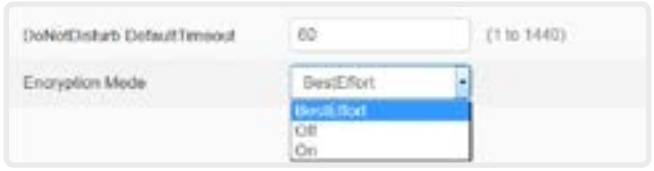
システム設定はカテゴリ別に分類されています。左ペインでカテゴリを選択すると、関連する設定が表示されます。



システム設定を変更する

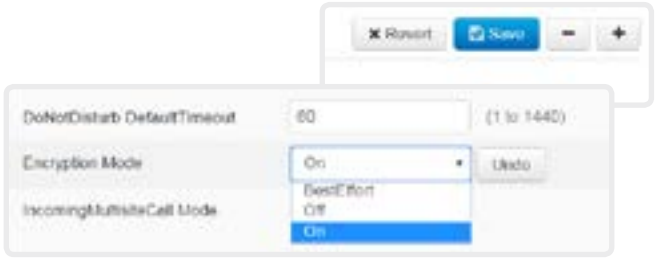
値スペースのチェック

設定の値スペースは、入力フィールドの後のテキストにより、または矢印をクリックして表示されるドロップダウン リストにより指定されます。



値を変更する

1. ドロップダウン リストから適切な値を選択するか、入力フィールドに新しいテキストを入力します。
2. [保存（Save）] をクリックして変更を有効にします。
   変更しない場合は、[元に戻す（Undo）] ボタンまたは [復元（Revert）] ボタンを使用します。



変更が保存されていないカテゴリには、編集記号（）のマークが付きます。

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、▶「システム設定」の章で説明しています。

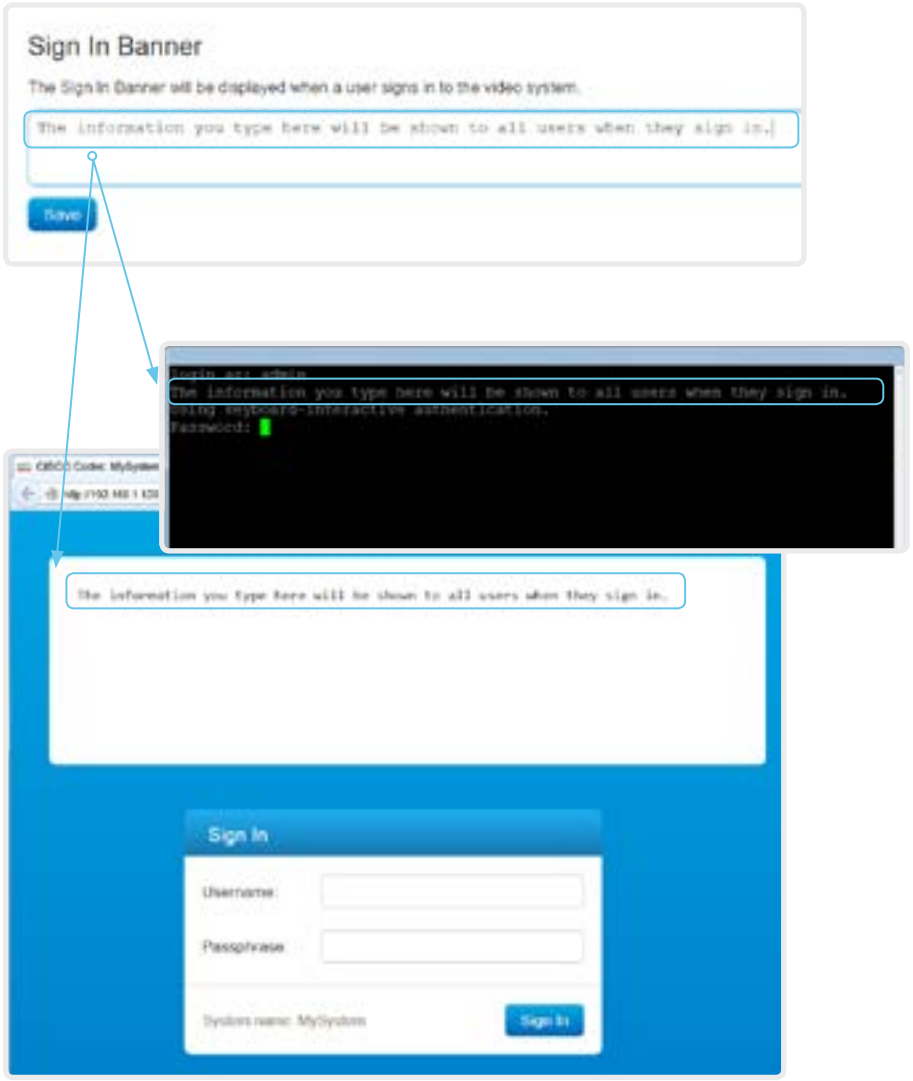
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者はすべてのシステム設定を変更できるように、すべてのユーザ ロールを所有している必要があります。

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

サインイン バナーの追加

Web インターフェイスにサインインして、[設定 (Configuration)] > [サインイン バナー (Sign In Banner)] に移動します。

1. ユーザがサインインしたとき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。

ビデオ システムのサービス証明書の管理

Web インターフェイスにサインインして、[セキュリティ (Security)] > [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。

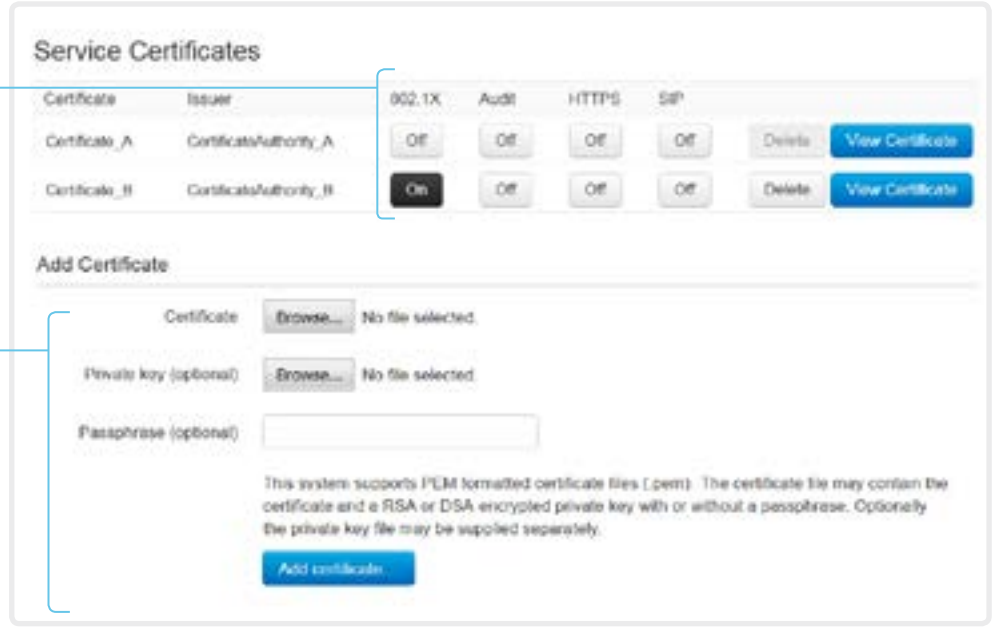
証明書の有効化、無効化、表示、または削除

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、対応するボタンを使用します。

証明書の追加

1. [参照 (Browse)] ボタンを押して、コンピュータ上の証明書ファイルと秘密キー ファイル (オプション) を見つけます。
2. 必要に応じて、[パスフレーズ (Passphrase)] に値を入力します。
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。



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になることがあります。

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、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。

証明書は、HTTPS サーバ、SIP、IEEE 802.1X、および監査ロギング 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。

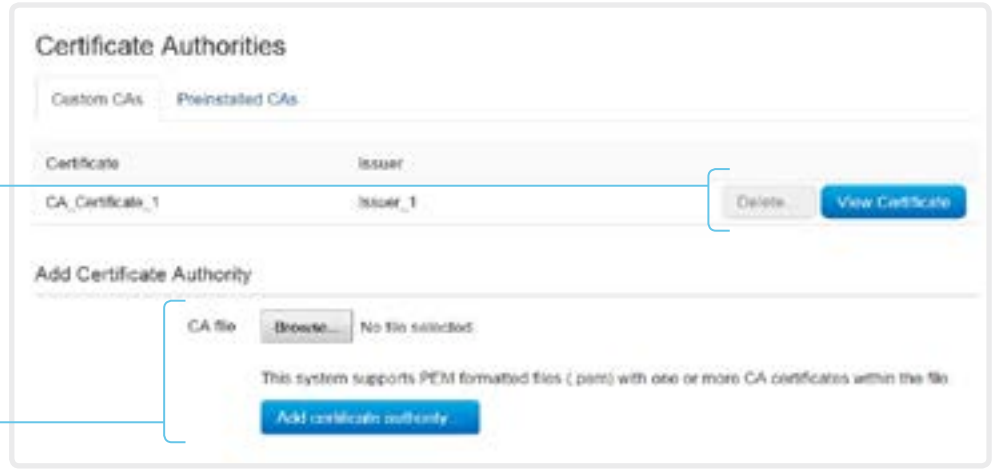
認証が失敗した場合、接続は確立されません。

信頼できる認証局（CA）のリストの管理

Web インターフェイスにサインインし、[セキュリティ（Security）] > [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）。



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。

証明書の表示または削除

証明書を表示または削除するには、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. [証明局の追加 ...（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。

過去に保存した証明書は自動的には削除されません。

CA 証明書を含む新しいファイルのエントリが既存のリストに追加されます。

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になることがあります。

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 によって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、監査ロギング用および他の接続用に証明書を検証するのに必要なすべての CA が含まれる必要があります。

認証が失敗した場合、接続は確立されません。

安全な監査ロギングのセットアップ

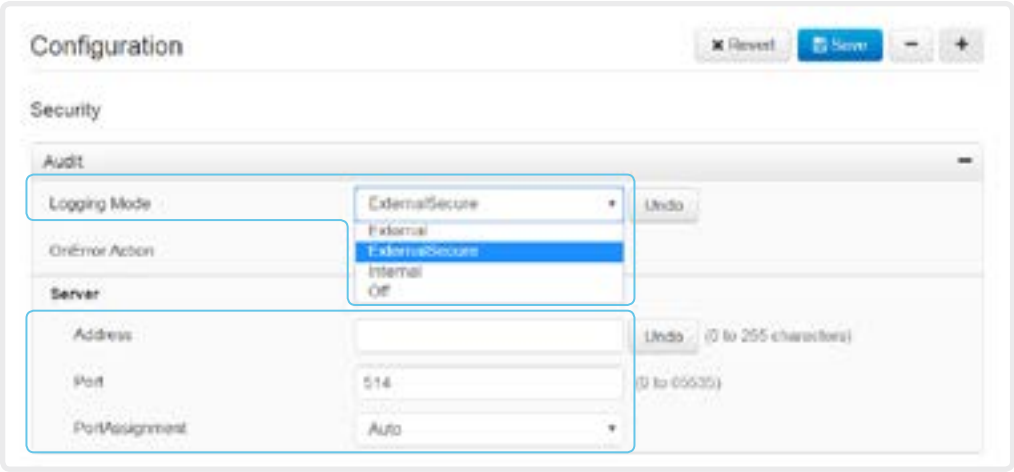
Web インターフェイスにサインインして、[セットアップ（Setup）] > [設定（Configuration）] に移動します。

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

リストの更新方法については、▶「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）] 設定を見つけて、監査サーバの [アドレス（Address）] を入力します。

   [ポート割り当て（PortAssignment）] を [手動（Manual）] に設定した場合は、監査サーバの [ポート（Port）] 番号も入力する必要があります。
3. [監査（Audit）] > [ロギング モード（Logging Mode）] を [外部セキュア（ExternalSecure）] に設定します。
4. [保存（Save）] をクリックして変更を有効にします。



安全な監査ロギングについて

監査ロギングを有効にすると、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 リストを使って検証されます。

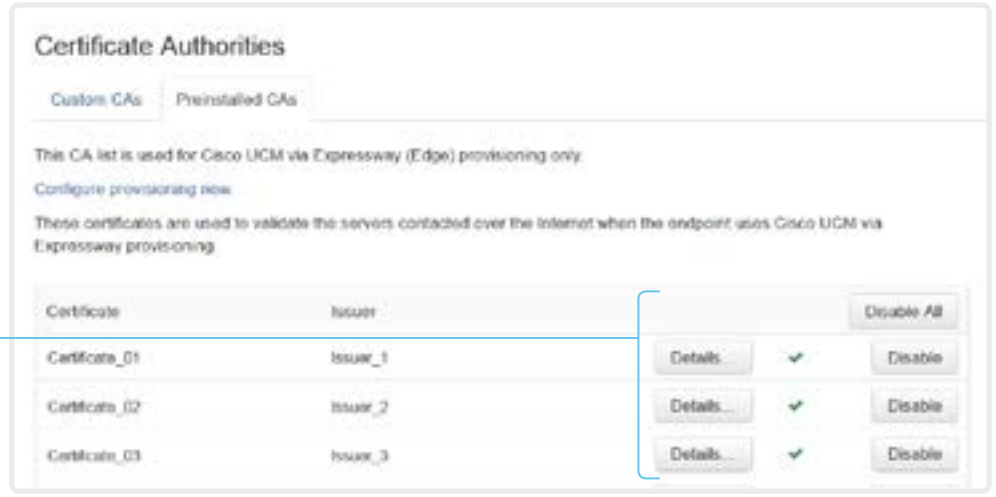
監査サーバの認証に失敗した場合は、監査ログが外部サーバに送信されません。

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。



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。

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。

プレインストール済み証明書について

このリスト内のプレインストール済み証明書は、ビデオ システムが Expressway（Edge）経由で Cisco Unified Communications Manager（CUCM）によって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に照らして検査されます。

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

ビデオ システムを工場出荷時設定にリセットしても、プレインストール済み証明書のリストは削除されません。

CUCM 信頼リストの削除

この章の情報は、Cisco Unified Communications Manager（CUCM）に登録されているビデオ システムにのみ該当します。

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 信頼リストの削除

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。

ただし、次のケースではこれらを削除する必要があります。

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

信頼リストのフィンガープリントと証明書についての概要

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つ可能性があります。

信頼リストについての詳細情報

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

ビデオ システムの現在の永続性ステータスは、アクティブ ラジオ ボタンで示されます。

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

デフォルトでは、すべての永続設定は [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。再起動後に、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）、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。

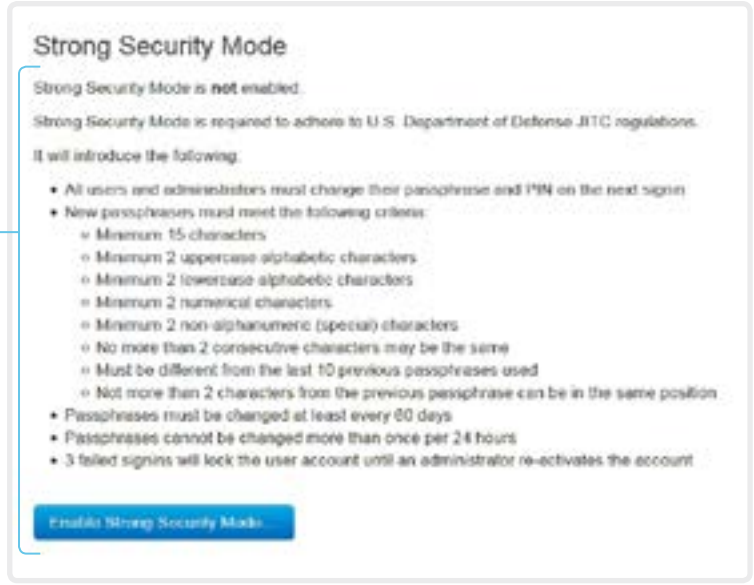
- システム設定の変更
- 通話の発信および受信に関する情報（通話履歴）
- 内部ログ ファイル
- ローカル連絡先またはお気に入りリストの変更内容
- 前回のセッションでのすべての IP 関連情報（DHCP）

[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、その前に [強力なセキュリティ モードの有効化 ... (Enable Strong Security Mode...)] をクリックして、表示されるダイアログボックスで選択を確認します。

   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」の章で説明しています。

通常モードに戻る

[強力なセキュリティ モードの無効化 ...（Disable Strong Security Mode...）] をクリックします。ビデオ システムが通常モードに戻ります。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。

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てください。

強力なセキュリティ モードにより、非常に厳格なパスフレーズ要件が設定され、すべてのユーザは次回のサインイン時にパスフレーズを変更するよう要求されます。

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

Cisco Proximity を使用すると、ユーザは自分のモバイル 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。

同時プロキシミティ接続の数は、ビデオ システムのタイプによって異なります。接続の最大数に達するとクライアントは新しいユーザに警告を出します。

ビデオ システム	最大接続数
Room Kit、Room 55、Room 70	7
Codec Plus	7
SX80	10
SX10、SX20	7
MX700、MX800	10
MX200 G2、MX300 G2	7
DX70、DX80	3

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、音量の調整、通話の切断
- スマートフォンとタブレット（iOS および Android）で使用可能

モバイル デバイスでの共有コンテンツの表示：
- 共有コンテンツの表示、以前のスライドの再表示、選択したスライドの保存
- スマートフォンとタブレット（iOS および Android）で使用可能
- DX70 および DX80 の場合、このサービスは通話時にのみ利用できます。

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共有
- ラップトップ（OS X および Windows）で使用可能

コールの発信とビデオ システムの制御

モバイル デバイスでの共有コンテンツの表示

モバイル デバイスからのワイヤレス共有

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

Cisco Proximity クライアントのインストール

クライアントの入手先

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、► http://proximity.cisco.com から無償でダウンロードできます。

スマートフォンやタブレットのクライアントは、Google Play（Android）および Apple App Store（iOS）から直接、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力します。

[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、75dB 未満のレベルで影響が生じることはほとんどありません。

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

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

DX70 および DX80:

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

Codec Plus、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 コントローラでの音調調節は効果ありません。

ヘッドセット

DX70、DX80、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 55、Room Kit、Room Kit Plus、Codec Plus、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、超音波の放出をオフに切り替える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）。こうするとプロキシミティ機能は使用できません。
- これらのシステムにはヘッドセット専用出力がないため、接続するヘッドセットからの音圧レベルを制御できません。

SX10 と SX10N

Cisco TelePresence SX10 Quick Set は SX10 と SX10N という 2 つのバージョンで提供されます。

SX10N には超音波用の内蔵スピーカーがありますが、SX10 には超音波とその他の音声信号に同じスピーカー（サードパーティ）が使用されます。

使用しているバージョンの確認

SX10 または SX10N が次の文字列に含まれています。

- ビデオ システムの背面にあるレーティング ラベルの PID フィールドを確認します。
- Web インターフェイスで [セットアップ（Setup）] > [ステータス（Status）] に移動し、[システム ユニット（SystemUnit）] > [ハードウェア（Hardware）] > [UDI] ステータスを確認します。

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

プロキシミティ サービスの有効化

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）] に移動して、Proximity を [オン（On）] にします。

   ビデオ システムで超音波のペアリング メッセージの送信が開始されます。
3. 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完全に利用するためには、すべてのサービスを有効にすることを推奨します。

   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れば、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

サードパーティ製スピーカーの使用時にプロキシミティが期待どおりに動作するように追加テストが必要な可能性があるため、プロキシミティ機能はデフォルトで [オフ（Off）] になっています。超音波によってまれにオーディオ アーチファクトが生じることがあります。このアーチファクトが生じた場合、[音声（Audio）] > [超音波（Ultrasound）] > [最大レベル（MaxLevel）] の設定を使用して超音波の最大音量を下げることを検討してください。

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。

セットアップ , セットアップでプロキシミティが適切であることを確認した場合は、ユーザ エクスペリエンスを最適化するために、プロキシミティを常に**オン** * にしておく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。

* SX10：プロキシミティ（超音波）を**オン**に切り替えた場合は、、ヘッドセットを使用しないことをお勧めします。SX10N：ヘッドセットを常に使用できます。

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)

部屋についての考慮事項

部屋の音響

- 壁 / 床 / 天井の表面が硬い部屋では、音の反響が大きいために問題になる場合があります。会議のエクスペリエンスとインテリジェント プロキシミティのパフォーマンスを最適化するために、会議室の音響処理を常に考慮することを強くお勧めします。
- インテリジェント プロキシミティを有効にしたビデオ システムは、1 部屋で 1 つのみ使用することをお勧めします。複数使用すると電波障害が発生して、デバイスの検出とセッション メンテナンスで問題が生じる可能性があります。

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案事項が記載されており、この機能を組織に導入する際にはこれを考慮する必要があります。次のページを参照して下さい。
► 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

- ビデオ システムがスタンバイ モードかどうかを確認します。スピーカーがオフになっている（たとえば、スタンバイ モードの TV）場合、超音波は送信されません。SX10 に適用されます。SX10N には適用されません。
- スピーカーの音量を確認します。超音波の音量を制御するのは、スピーカー自体の音量コントロールです（リモート コントロールまたは Touch 10 を使用してコントロールされる音量ではありません）。音量が低すぎると、受信デバイスで超音波のペアリング メッセージを検出できません。SX10 に適用されます。SX10N には適用されません。
- 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。

オーディオ アーチファクト

- うなりやクリッピング ノイズなどのオーディオ アーチファクトが聞こえる場合は、最大超音波音量を下げます（[オーディオ (Audio)] > [超音波 (Ultrasound)] > [最大音量 (MaxVolume)]）。

ラップトップからコンテンツを共有できない

- 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

ビデオ品質対コール レート比の調整

ビデオ入力品質の設定

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

最適鮮明度設定を有効にするには、Video Input Connector n Quality 設定を **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、ビデオ会議室の照明状態とカメラ（ビデオ入力ソース）の品質を反映します。照明の状態およびカメラの品質が優れているほど、使用するプロファイルは高度になります。

通常は、[中（Medium）] プロファイルをお勧めします。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。特定のコール レートに対する解像度を上げるには、[高（High）] プロファイルを設定できます。

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

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）] に移動します。

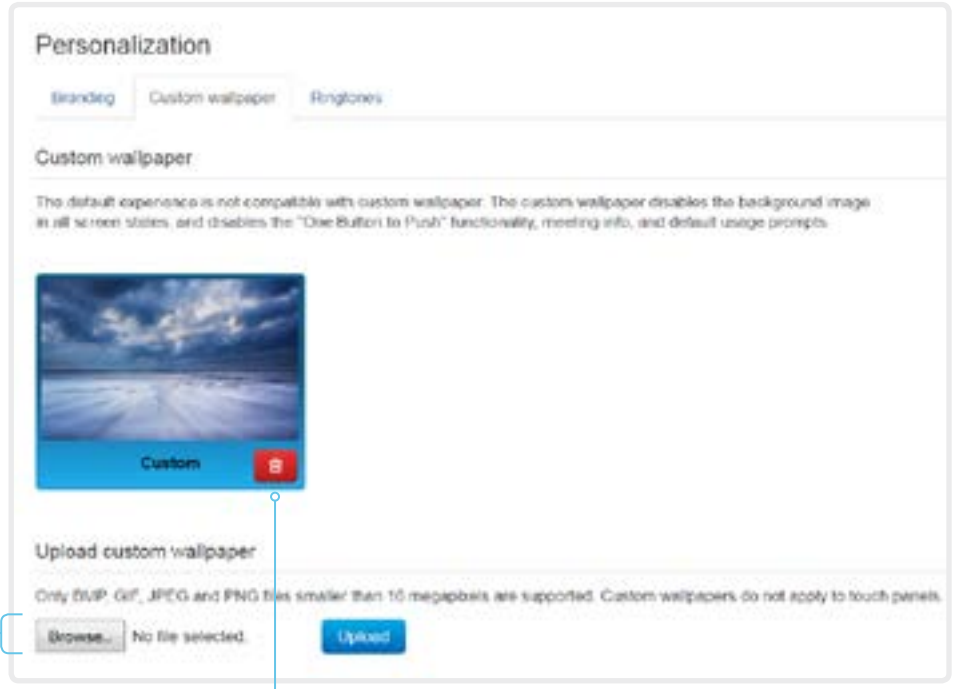
1. [ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [品質（Quality）] を選択して、ビデオ品質パラメータを [モーション（Motion）] に設定します（Connector 1（内蔵カメラ）ではこの手順をスキップします）。
2. [ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [最適鮮明度（OptimalDefinition）] > [プロファイル（Profile）] に移動して、適切な最適鮮明度プロファイルを選択します。

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

コール レート (kbps)	H.264、最大 30 fps		
	標準	Medium	大きい
128	320 × 180 @ 30	512 × 288 @ 20	512 × 288 @ 30
160	512 × 288 @ 20	512 × 288 @ 30	640 × 360 @ 30
224	512 × 288 @ 30	640 × 360 @ 30	768 × 448 @ 30
352	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30
448	768 × 448 @ 30	768 × 448 @ 30	1024 × 576 @ 30
576	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30
768	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30
1088	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30
1312	1280 × 720 @ 30	1280 × 720 @ 30	1920 × 1080 @ 30
1696	1280 × 720 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30
2464	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30
3072	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30

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。

もう一度使用するには、新たに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。

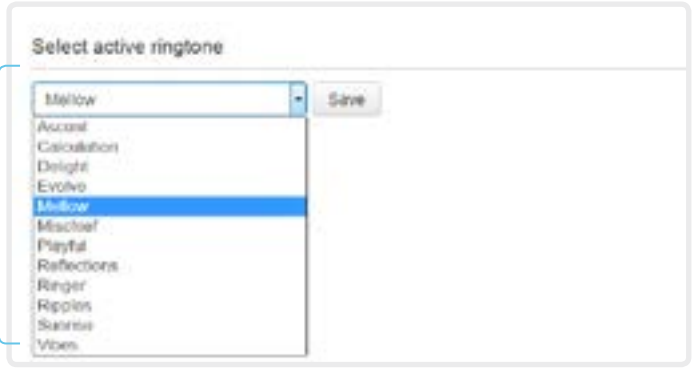
カスタムの壁紙を使用するときには、ワンボタン機能や会議情報の表示など、いくつかの機能が失われます。

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。呼び出し音は、Web インターフェイスを実行しているコンピュータではなく、ビデオ システム自体で再生されることに注意してください。

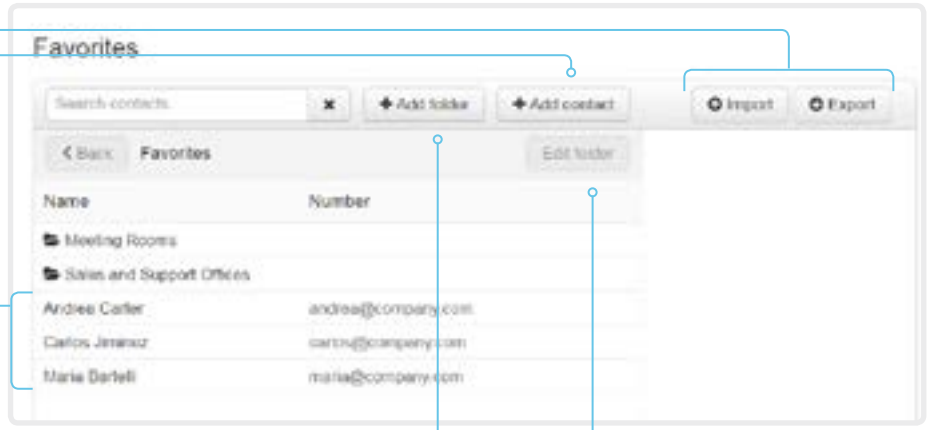
お気に入りリストの管理

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り入れるには [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. 表示されたフォームに値を入力するか、更新します。

   連絡先をサブフォルダに保存するには、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）を保存するには、[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。

サブフォルダの追加または編集

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、列挙されたサブフォルダのいずれかをクリックして [フォルダの編集（Edit folder）] をクリックし、既存のサブフォルダを変更します。
2. 表示されたフォームに値を入力するか、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。

サブフォルダの削除

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 インターフェイスによるお気に入りの管理

お気に入りリストへの連絡先の追加

1. ホーム画面の [発信（Call）] を選択します。
2. 追加する連絡先を選択します。
3. 連絡先カードの [発信（Call）] ボタンの下に表示されている 3 つの点を選択します（リモート コントロールを使用する場合のみ必須）。
4. [お気に入りに追加（Add to favorites）] または [お気に入りに設定（Mark as Favorite）] を選択します。

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

お気に入りリストからの連絡先の削除

1. ホーム画面の [発信（Call）] を選択します。
2. [お気に入り（Favorites）] タブを選択します。
3. 削除する連絡先を選択します。
4. 連絡先カードの [発信（Call）] ボタンの下に表示されている 3 つの点を選択します（リモート コントロールを使用する場合のみ必須）。
5. [お気に入りの削除（Remove favorite）] または [お気に入り設定を解除（Unmark as favorite）] を選択します。

アクセシビリティ機能のセットアップ

着信時のスクリーンの点滅

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

1. 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。

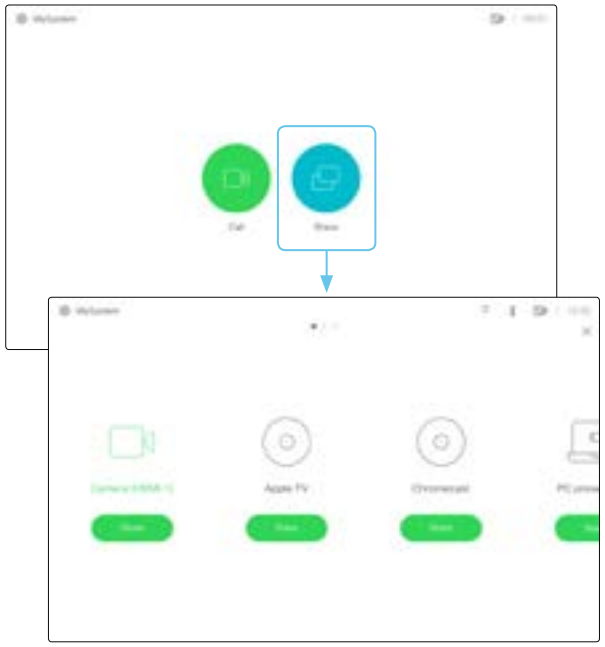
第 3 章

周辺機器

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）

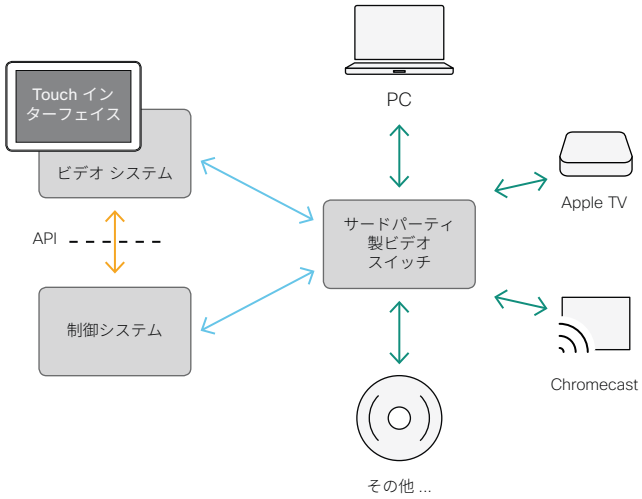
ユーザ インターフェイスを拡張する方法、およびそれをビデオ システムの API を使用してセットアップする方法の詳細については、CE のカスタマイズ ガイド [英語] を参照してください。次のリンクにアクセスします。

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

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。これはビデオ システムではなく、ビデオ スイッチ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ディスプレイ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、ディスプレイはスタンバイに設定されません。

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に、次の LG 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” UHD（49UH5C）	http://www.lg.com/global/business/information-display/digital-signage/lg-49UH5C
55” UHD（55UH5C）	http://www.lg.com/global/business/information-display/digital-signage/lg-55UH5C
65” UHD（65UH5C）	http://www.lg.com/global/business/information-display/digital-signage/lg-65UH5C
75” UHD（75UH5C）	http://www.lg.com/global/business/information-display/digital-signage/lg-75UH5C
86” UHD（86UH5C）	http://www.lg.com/global/business/information-display/digital-signage/lg-86UH5C

Touch 10 コントローラの接続 (1/3 ページ)

Touch 10 は、ネットワーク (LAN) 経由でビデオ システムにペアリングする必要があります。これは、リモート ペアリングと呼ばれます。

ネットワーク（LAN）経由で Touch 10 をビデオ システムへ接続する

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。

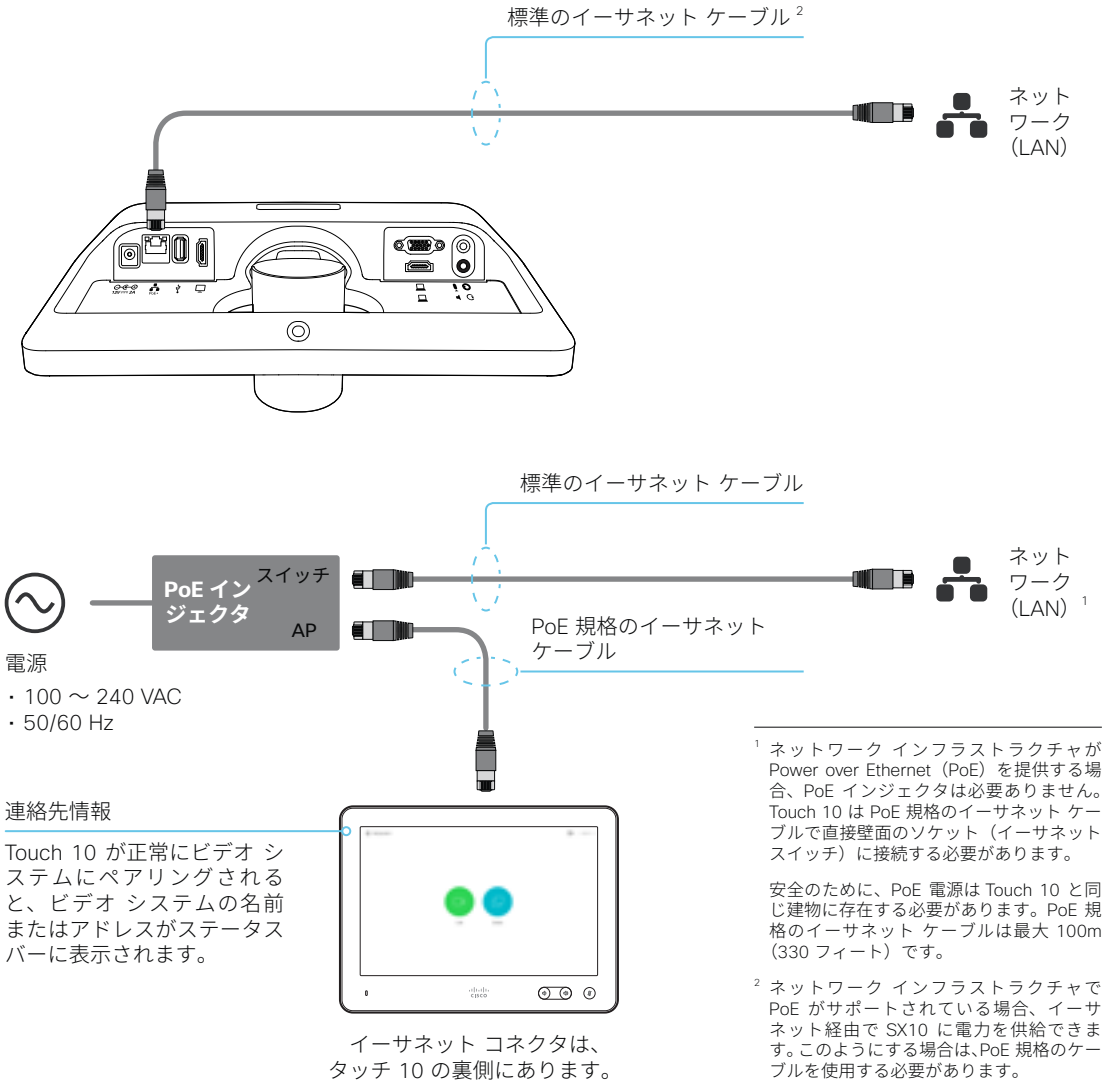
  ビデオ システムをリストに表示するには、次を満たしている必要があることに注意してください。

  - 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。



[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。Touch 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。

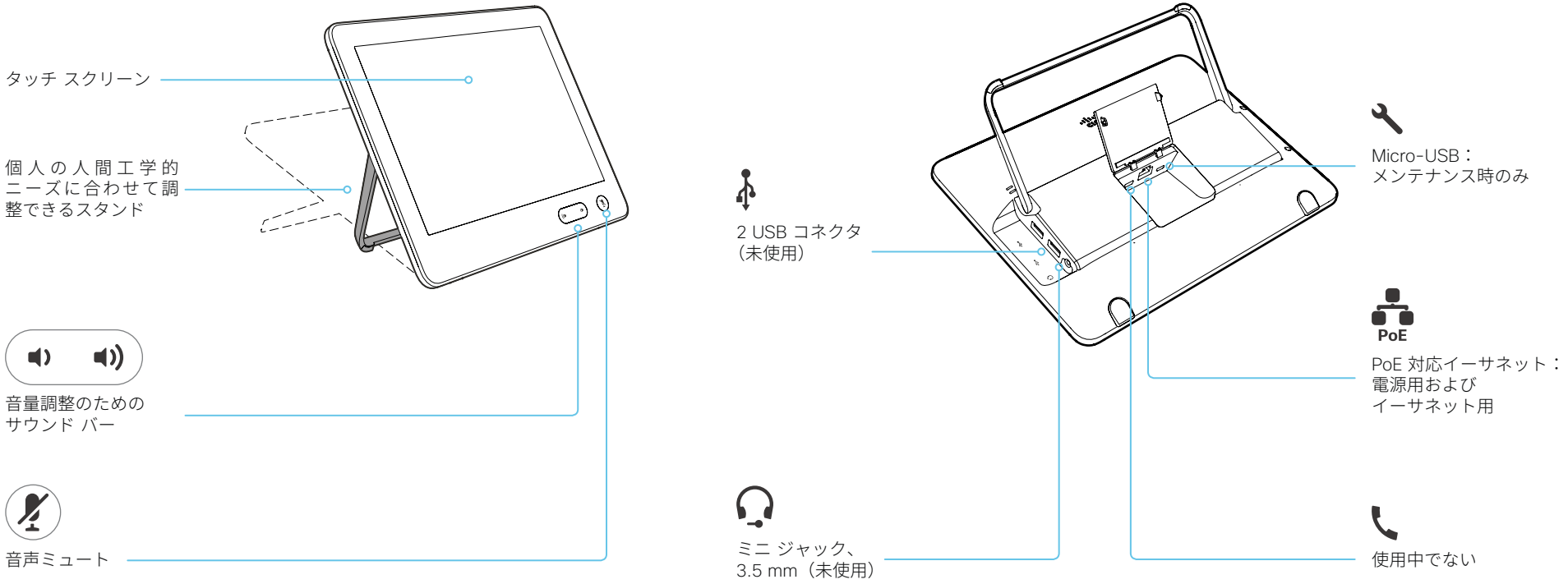
安全のために、PoE 電源は Touch 10 と同じ建物に存在する必要があります。PoE 規格のイーサネット ケーブルは最大 100m（330 フィート）です。

[2] ネットワーク インフラストラクチャで PoE がサポートされている場合、イーサネット経由で SX10 に電力を供給できます。このようにする場合は、PoE 規格のケーブルを使用する必要があります。

Touch 10 コントローラの接続 (2/3 ページ)

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

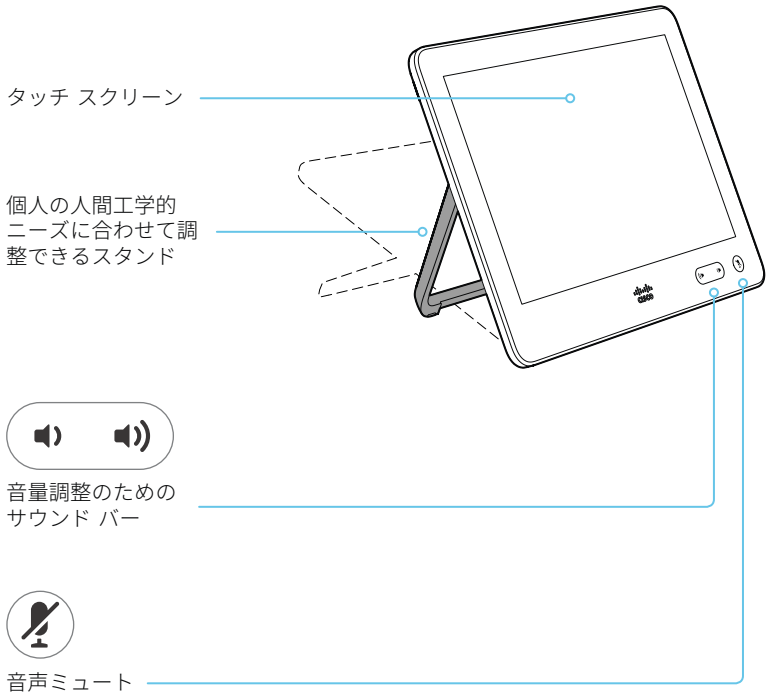
Touch 10 コントローラの新しいバージョンについては、次のページを参照してください。

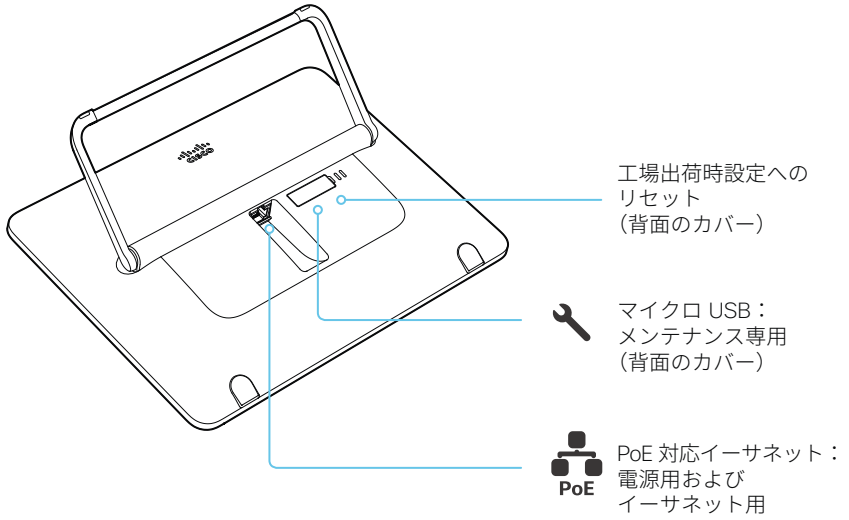


Touch 10 コントローラの接続 (3/3 ページ)

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。





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 トポ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 Spark 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。

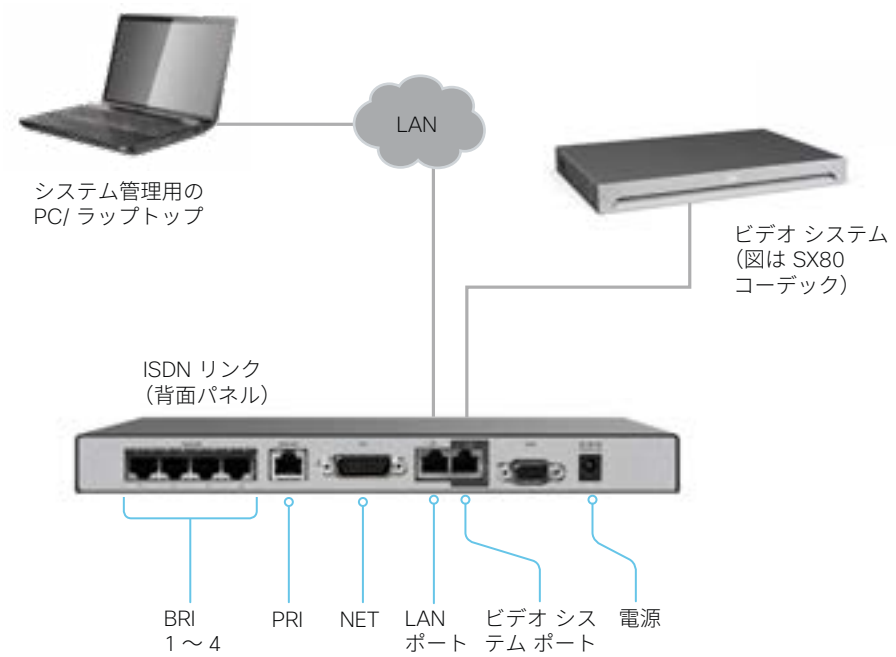
セットアップと構成

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、次を参照してください。► https://www.cisco.com/go/isdnlink-docs [英語]

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]



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（1/2 ページ）

TC ソフトウェアから CE ソフトウェアへのアップグレード

CE ソフトウェアは、TC ソフトウェアの進化形です。CE ソフトウェアにアップグレードする前に、TC7.3.6 以降にアップグレードしておくことをお勧めします。

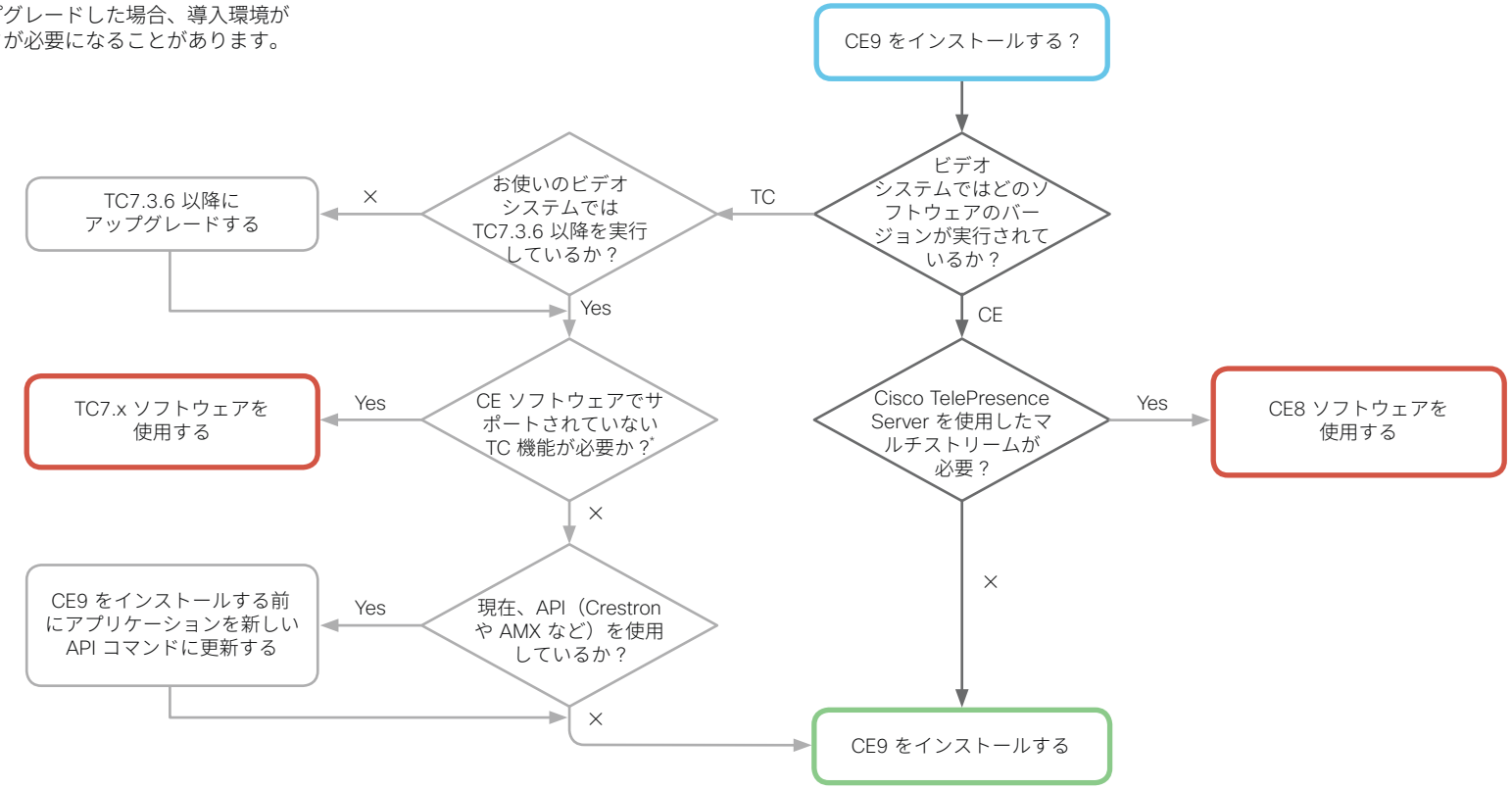
CE ソフトウェアにアップグレードする前に、アップグレード要件および機能の変更について読んでおくことは重要です。また、ご使用の環境で変更がサポートされていることを確認します。ソフトウェア リリース ノートを注意深く読むことを推奨します。

これらの点を考慮せずに CE にアップグレードした場合、導入環境が正常に機能しないためダウングレードが必要になることがあります。

CE8 から CE9 へのアップグレード

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

また、CE8 で Touch コントローラから使用できたいくつかの機能は、最初の CE9 リリースでは使用できません。アップグレードを実行する前に、詳細な点についてソフトウェアのリリース ノートを参照してください。



* CE ソフトウェアは次の製品と機能をサポートしません：
- CTMS 会議
- MediaNet
- 16:9 の解像度をサポートしないディスプレイ

システム ソフトウェアをアップグレードする (2/2 ページ)

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のダウンロード

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://www.cisco.com/cisco/software/navigator.html）に移動します。次に、ご使用の製品のページに移動します。

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「s52030ce9_3_x.pkg」です。

ソフトウェア リリース ノート

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

参照先：► https://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-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

該当するソフトウェア パッケージをダウンロードしてコンピュータに保存します。これは .pkg ファイルです。ファイル名は変更しないでください。

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

通常、インストールは 15 分以内に完了します。Web ページから進捗状況を確認できます。インストール後、ビデオ システムは自動的に再起動します。

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

新しいソフトウェア バージョンの確認

ファイルを選択すると、ここにソフトウェアのバージョンが表示されます。

ソフトウェア 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、CE9.3.x です。

オプション キーの追加

Web インターフェイスにサインインして、[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. テキスト入力フィールドにオプション キーを入力します。
2. [オプション キーの追加 (Add option key)] をクリックします。

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

オプション キーについて

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にするには、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。

ビデオ システムごとに一意のオプション キーが割り当てられます。

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

Web インターフェイスにサインインして、[システム情報（System Information）] ページを表示します。

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 エントリの検索

検索フィールドに必要な数の文字を入力します。これらの文字を含む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るエントリも表示されます。

カテゴリを選択して適切なステータスに移動する

システム ステータスはカテゴリ別に分類されています。左ペインでカテゴリを選択すると、右側に関連ステータスが表示されます。

[*] 図に示しているステータスは一例です。お使いの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 *。

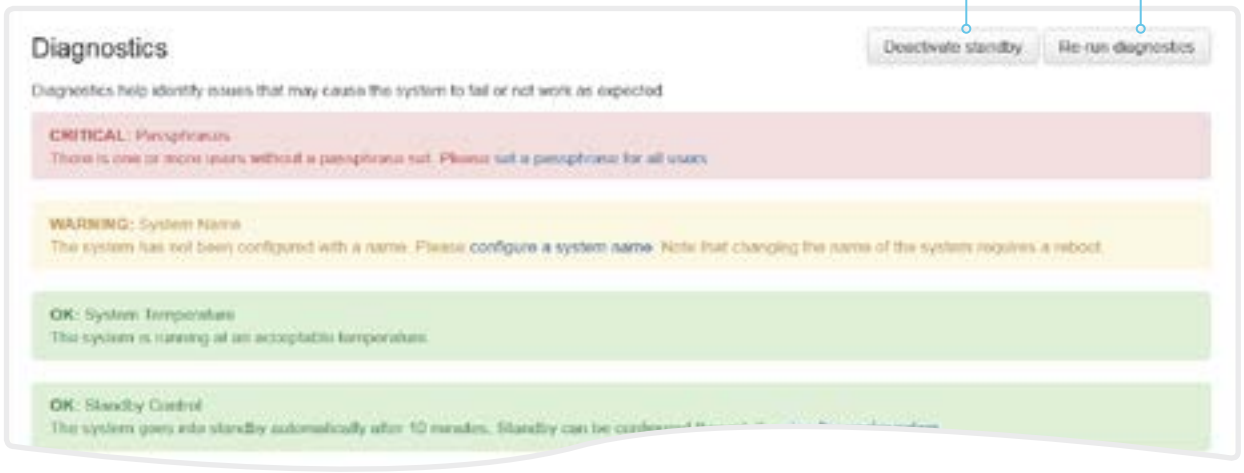
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

診断の実行

[診断の再実行（Re-run diagnostics）] をクリックして、リストが最新であることを確認します。

スタンバイ モードを離れる

スタンバイ モードのビデオ システムを復帰させるには、[スタンバイの非アクティブ化（Deactivate standby）] をクリックします。

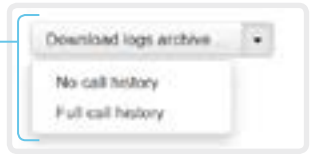


* 図に示しているメッセージは一例です。お使いのシステムでは表示される情報が異なる場合があります。

ログ ファイルのダウンロード

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）] に移動します。

すべてのログ ファイルのダウンロード



[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）を含める場合には、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 リストの表示更新

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

ログ ファイルについて

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

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

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 システムのパフォーマンスが低下する可能性があります。拡張ロギング モードは、トラブルシューティングのときにのみ使用してください。

リモート サポート ユーザの作成

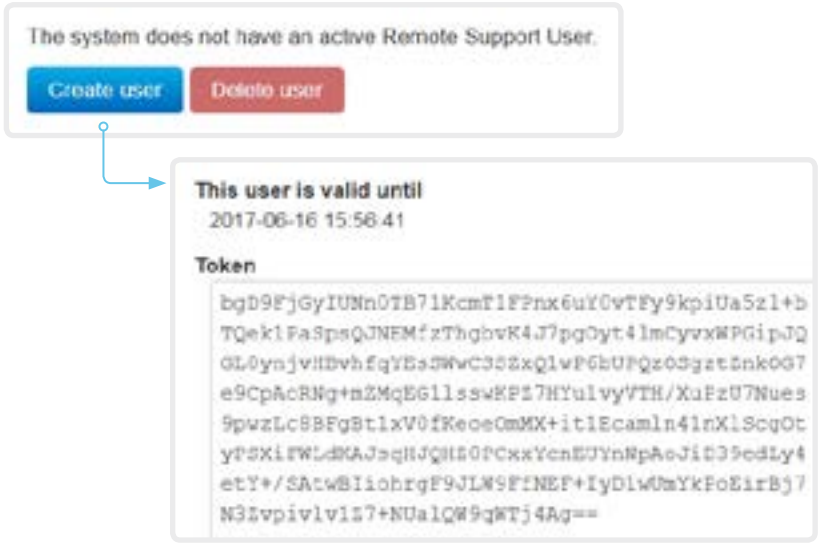
Web インターフェイスにログインし、[メンテナンス（Maintenance）] > [システム リカバリ（System Recovery）] に移動して、[リモート サポート ユーザ（Remote Support User）] タブを選択します。

リモート サポート ユーザは、Cisco TAC によって指示されたトラブルシューティングを行う場合にのみ有効にする必要があります。

リモート サポート ユーザの作成

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

リモート サポート ユーザは 7 日間、または削除されるまで有効です。



リモート サポート ユーザの削除

[ユーザの削除（Delete User）] をクリックします。

リモート サポート ユーザについて

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いくつかの限定的な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
- [お気に入り]
- サインイン バナー
- 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

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）] **に設定されています。**

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

バックアップ ファイル

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

カスタム要素の CUCM プロビジョニング

▶「バックアップと復元の構成とカスタム要素」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 テンプレートに完全な 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/unified-communications-manager-callmanager/tsd-products-support-series-home.html

カスタム要素の TMS プロビジョニング

▶「バックアップと復元の構成とカスタム要素」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。

```
<Command>
  <Provisioning>
    <Service>
      <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
      </Fetch>
    </Service>
  </Provisioning>
</Command>
```

   値は次のとおりです。

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

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

   origin: **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。

以前使用していたソフトウェア イメージへの復元

Web インターフェイスにサインインして、[メンテナンス（Maintenance）] > [システム リカバリ（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

この手順は管理者のみが実行するか、またはシスコ テクニカル サポートと連絡を取っている場合にのみ実行してください。

1. [ソフトウェア リカバリのスワップ（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。この手順には数分かかることがあります。

以前使用していたソフトウェア 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以降、システムをまだ工場出荷時設定にリセットしていない場合は、以前に使用したソフトウェア イメージがシステム上に残っています。ソフトウェアを再度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。

工場出荷時設定リセットは元に戻すことができません。

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。ソフトウェアの交換については、►「以前使用していたソフトウェア イメージへの復元」の章を参照してください。

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使用できない場合は、リセット ボタンを使用してください。

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。

- コール ログが削除されます。
- パスフレーズがデフォルト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されていたファイルは、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 システムの初期設定へのリセット (2/3 ページ)

Web インターフェイスを使用した工場出荷時設定リセット

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。

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 リカバリ（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 リカバリ（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。

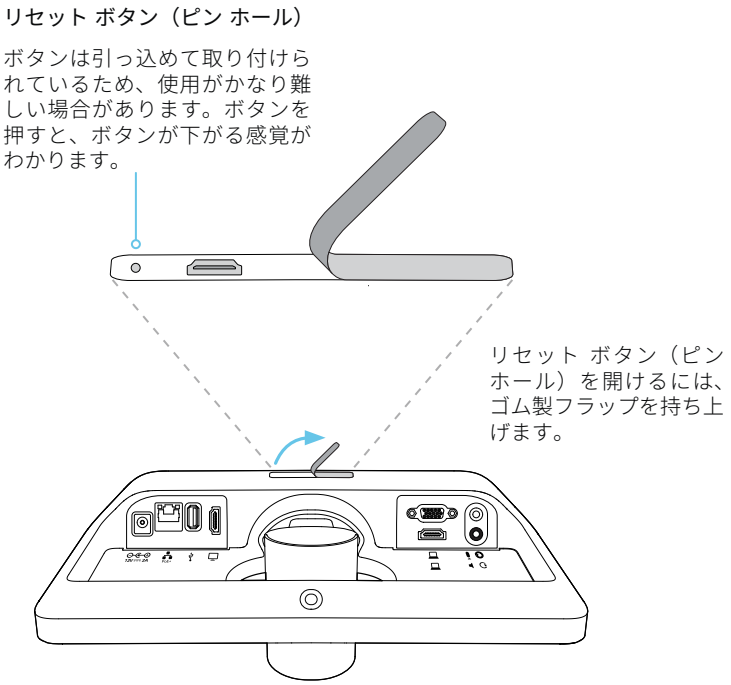
ビデオ システムの工場出荷時設定リセット（3/3 ページ）

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. リセット ボタン（ピン ホール）を開けるには、ユニット背面のゴム製フラップを持ち上げます。
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。

エラーが発生した状況では、接続を回復するためにタッチ コントローラを工場出荷時設定にリセットする必要が生じることがあります。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。

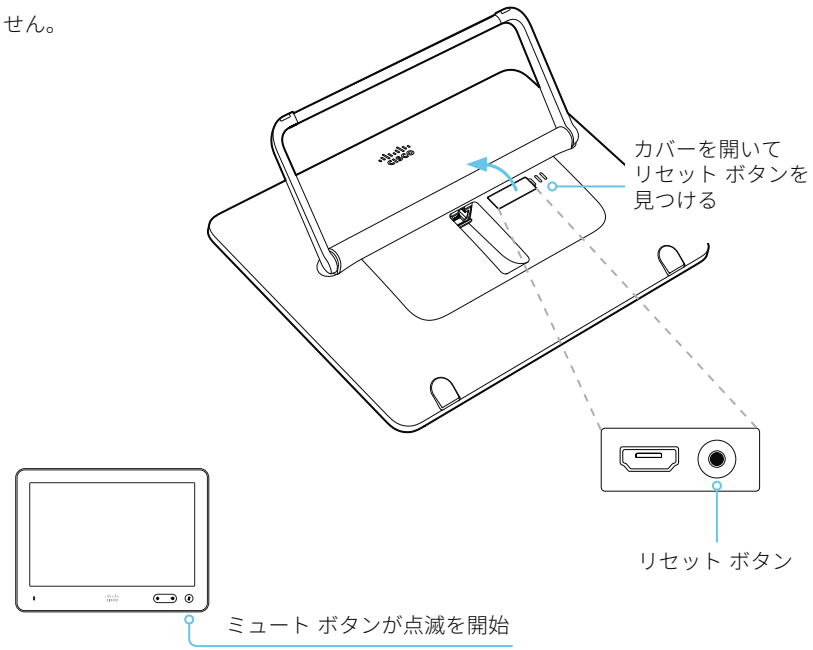
タッチ コントローラを工場出荷時設定にリセットすると、ペアリング情報が失われ、（ビデオ システムではなく）タッチ自体が工場出荷時の初期状態に戻されます。

工場出荷時設定リセットは元に戻すことができません。

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。

   タッチ 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。

   タッチ 10 は、ビデオ システムと改めて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

タッチ 10 コントローラを使用するには、LAN 経由でタッチ 10 をコーデックとペアリング（リモート ペアリング）する必要があります。

ペアリング、および Touch 10 とビデオ 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」の章を参照してください。

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

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

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

エラーが発生した状況では、接続を回復するためにタッチ コントローラを工場出荷時設定にリセットする必要が生じることがあります。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。

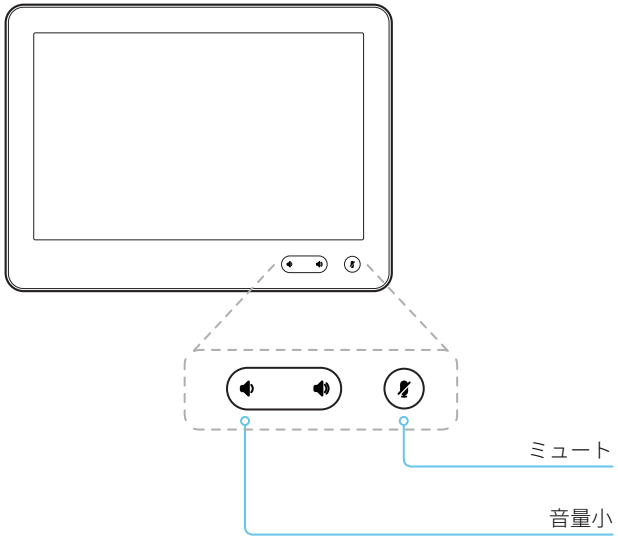
タッチ コントローラを工場出荷時設定にリセットすると、ペアリング情報が失われ、（ビデオ システムではなく）タッチ自体が工場出荷時の初期状態に戻されます。

工場出荷時設定リセットは元に戻すことができません。

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

   タッチ 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。

   タッチ 10 は、ビデオ システムと改めて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

タッチ 10 コントローラを使用するには、LAN 経由でタッチ 10 をコーデックとペアリング（リモート ペアリング）する必要があります。

ペアリング、および Touch 10 とビデオ 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」の章を参照してください。

ユーザ インターフェイスのスクリーンショットのキャプチャ

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、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領域に表示されます。スクリーンショットの準備ができるまでに最大 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。スクリーンショット ID をクリックするとイメージが表示されます。

スクリーンショットの削除

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

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

ユーザ インタ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 settings 78
Audio DefaultVolume 78
Audio Input Microphone [1..2] Mode 79
Audio Input Microphone [2..2] EchoControl Dereverberation 79
Audio Input Microphone [2..2] EchoControl Mode 78
Audio Input Microphone [2..2] EchoControl NoiseReduction 79
Audio Input Microphone [2..2] Level 79
Audio Microphones Mute Enabled 78
Audio Output Line [1..1] Delay DelayMs 80
Audio Output Line [1..1] Delay Mode 80
Audio SoundsAndAlerts RingTone 78
Audio SoundsAndAlerts RingVolume 78
Audio Ultrasound MaxVolume 80
Audio Ultrasound Mode 80

CallHistory settings 81
CallHistory Mode 81

Cameras settings 82
Cameras Camera [1..1] Backlight DefaultMode 82
Cameras Camera [1..1] Brightness DefaultLevel 82
Cameras Camera [1..1] Brightness Mode 82
Cameras Camera [1..1] Flip 82
Cameras Camera [1..1] Focus Mode 82
Cameras Camera [1..1] Mirror 83
Cameras Camera [1..1] Whitebalance Level 83
Cameras Camera [1..1] Whitebalance Mode 83

Conference settings 84
Conference ActiveControl Mode 84
Conference AutoAnswer Delay 84
Conference AutoAnswer Mode 84
Conference AutoAnswer Mute 84
Conference CallProtocolIPStack 84
Conference DefaultCall Protocol 85
Conference DefaultCall Rate 85
Conference DoNotDisturb DefaultTimeout 85
Conference Encryption Mode 85

Conference FarEndControl Mode 85
Conference FarEndControl SignalCapability 86
Conference MaxReceiveCallRate 86
Conference MaxTotalReceiveCallRate 86
Conference MaxTotalTransmitCallRate 86
Conference MaxTransmitCallRate 86
Conference MicUnmuteOnDisconnect Mode 86
Conference Presentation OnPlacedOnHold 87
Conference VideoBandwidth Mode 87

FacilityService settings 88
FacilityService Service [1..5] CallType 88
FacilityService Service [1..5] Name 88
FacilityService Service [1..5] Number 88
FacilityService Service [1..5] Type 88

H323 settings 89
H323 Authentication LoginName 89
H323 Authentication Mode 89
H323 Authentication Password 89
H323 CallSetup Mode 89
H323 Encryption KeySize 90
H323 Gatekeeper Address 90
H323 H323Alias E164 90
H323 H323Alias ID 90
H323 NAT Address 91
H323 NAT Mode 90
H323 PortAllocation 91

Logging settings 92
Logging External Mode 92
Logging External Protocol 92
Logging External Server Address 92
Logging External Server Port 92
Logging Mode 92

Network settings 93
Network [1..1] DNS DNSSEC Mode 93
Network [1..1] DNS Domain Name 93
Network [1..1] DNS Server [1..3] Address 93
Network [1..1] IEEE8021X AnonymousIdentity 94
Network [1..1] IEEE8021X Eap Md5 94
Network [1..1] IEEE8021X Eap Peap 95
Network [1..1] IEEE8021X Eap Tls 95
Network [1..1] IEEE8021X Eap Ttls 94
Network [1..1] IEEE8021X Identity 94
Network [1..1] IEEE8021X Mode 93
Network [1..1] IEEE8021X Password 94
Network [1..1] IEEE8021X TlsVerify 93
Network [1..1] IEEE8021X UseClientCertificate 94
Network [1..1] IPStack 95
Network [1..1] IPv4 Address 95
Network [1..1] IPv4 Assignment 95
Network [1..1] IPv4 Gateway 95
Network [1..1] IPv4 SubnetMask 96
Network [1..1] IPv6 Address 96
Network [1..1] IPv6 Assignment 96
Network [1..1] IPv6 DHCPOptions 96
Network [1..1] IPv6 Gateway 96
Network [1..1] MTU 96
Network [1..1] QoS Diffserv Audio 97
Network [1..1] QoS Diffserv Data 97
Network [1..1] QoS Diffserv ICMPv6 98
Network [1..1] QoS Diffserv NTP 98
Network [1..1] QoS Diffserv Signalling 98
Network [1..1] QoS Diffserv Video 97
Network [1..1] QoS Mode 97
Network [1..1] RemoteAccess Allow 98
Network [1..1] Speed 99
Network [1..1] TrafficControl Mode 99
Network [1..1] VLAN Voice Mode 99
Network [1..1] VLAN Voice VlanId 99

NetworkServices settings 100
NetworkServices CDP Mode 100
NetworkServices H323 Mode 100
NetworkServices HTTP Mode 100
NetworkServices HTTP Proxy Allowed 100
NetworkServices HTTP Proxy LoginName 101
NetworkServices HTTP Proxy Mode 101
NetworkServices HTTP Proxy PACUrl 101

NetworkServices HTTP Proxy Password ... 101
NetworkServices HTTP Proxy Url ... 101
NetworkServices HTTPS OCSP Mode ... 102
NetworkServices HTTPS OCSP URL ... 102
NetworkServices HTTPS Server MinimumTLSVersion ... 101
NetworkServices HTTPS StrictTransportSecurity ... 102
NetworkServices HTTPS VerifyClientCertificate ... 102
NetworkServices HTTPS VerifyServerCertificate ... 102
NetworkServices NTP Mode ... 103
NetworkServices NTP Server [1..3] Address ... 103
NetworkServices SIP Mode ... 103
NetworkServices SNMP CommunityName ... 104
NetworkServices SNMP Host [1..3] Address ... 103
NetworkServices SNMP Mode ... 103
NetworkServices SNMP SystemContact ... 104
NetworkServices SNMP SystemLocation ... 104
NetworkServices SSH AllowPublicKey ... 104
NetworkServices SSH Mode ... 104
NetworkServices Telnet Mode ... 104
NetworkServices UPnP Mode ... 105
NetworkServices UPnP Timeout ... 105
NetworkServices WelcomeText ... 105
NetworkServices XMLAPI Mode ... 105

Peripherals settings ... 106
Peripherals Pairing CiscoTouchPanels EmcResilience ... 106
Peripherals Pairing CiscoTouchPanels RemotePairing ... 106
Peripherals Profile Cameras ... 106
Peripherals Profile ControlSystems ... 106
Peripherals Profile TouchPanels ... 107

Phonebook settings ... 108
Phonebook Server [1..1] ID ... 108
Phonebook Server [1..1] Type ... 108
Phonebook Server [1..1] URL ... 108

Provisioning settings ... 109
Provisioning Connectivity ... 109
Provisioning ExternalManager Address ... 110
Provisioning ExternalManager AlternateAddress ... 110
Provisioning ExternalManager Domain ... 110
Provisioning ExternalManager Path ... 110
Provisioning ExternalManager Protocol ... 110
Provisioning LoginName ... 109
Provisioning Mode ... 109
Provisioning Password ... 110

Proximity settings ... 111
Proximity Mode ... 111
Proximity Services CallControl ... 111
Proximity Services ContentShare FromClients ... 111
Proximity Services ContentShare ToClients ... 111

RTP settings ... 112
RTP Ports Range Start ... 112
RTP Ports Range Stop ... 112
RTP Video Ports Range Start ... 112
RTP Video Ports Range Stop ... 112

Security settings ... 113
Security Audit Logging Mode ... 113
Security Audit OnError Action ... 113
Security Audit Server Address ... 113
Security Audit Server Port ... 114
Security Audit Server PortAssignment ... 114
Security Session FailedLoginsLockoutTime ... 114
Security Session InactivityTimeout ... 114
Security Session MaxFailedLogins ... 114
Security Session MaxSessionsPerUser ... 114
Security Session MaxTotalSessions ... 115
Security Session ShowLastLogon ... 115

SerialPort settings ... 116
SerialPort LoginRequired ... 116
SerialPort Mode ... 116

SIP settings ... 117
SIP ANAT ... 117
SIP Authentication Password ... 117
SIP Authentication UserName ... 117
SIP DefaultTransport ... 117
SIP DisplayName ... 117
SIP Ice DefaultCandidate ... 118

SIP Ice Mode 118
SIP Line 118
SIP ListenPort 118
SIP Mailbox 118
SIP PreferredIPMedia 119
SIP PreferredIPSignaling 119
SIP Proxy [1..4] Address 119
SIP TlsVerify 119
SIP Turn DiscoverMode 119
SIP Turn DropRflx 119
SIP Turn Password 120
SIP Turn Server 120
SIP Turn UserName 120
SIP Type 120
SIP URI 120

Standby settings 121
Standby BootAction 121
Standby Control 121
Standby Delay 121
Standby StandbyAction 121
Standby WakeupAction 121
Standby WakeupOnMotionDetection 121

SystemUnit settings 122
SystemUnit CrashReporting Advanced 122
SystemUnit CrashReporting Mode 122
SystemUnit CrashReporting Url 122
SystemUnit Name 122

Time settings 123
Time DateFormat 123
Time TimeFormat 123
Time Zone 124

UserInterface settings 126
UserInterface Accessibility IncomingCallNotification 126
UserInterface ContactInfo Type 126
UserInterface CustomMessage 126
UserInterface KeyTones Mode 126
UserInterface Language 126
UserInterface OSD EncryptionIndicator 127
UserInterface OSD HalfwakeMessage 127
UserInterface OSD Output 127
UserInterface Security Mode 127
UserInterface SettingsMenu Mode 127
UserInterface Wallpaper 128

UserManagement settings 129
UserManagement LDAP Admin Filter 130
UserManagement LDAP Admin Group 130
UserManagement LDAP Attribute 130
UserManagement LDAP BaseDN 130
UserManagement LDAP Encryption 129
UserManagement LDAP MinimumTLSVersion 129
UserManagement LDAP Mode 129
UserManagement LDAP Server Address 129
UserManagement LDAP Server Port 129
UserManagement LDAP VerifyServerCertificate 130

Video settings 131
Video ActiveSpeaker DefaultPIPPosition 131
Video DefaultLayoutFamily Local 131
Video DefaultLayoutFamily Remote 132
Video DefaultMainSource 132
Video Input Connector [1..3] CameraControl CameraId 132
Video Input Connector [1..3] CameraControl Mode 132
Video Input Connector [1..3] InputSourceType 132
Video Input Connector [1..3] Name 133
Video Input Connector [1..3] OptimalDefinition Profile 133
Video Input Connector [1..3] Visibility 134
Video Input Connector [2..2] RGBQuantizationRange 134
Video Input Connector [2..3] PresentationSelection 133
Video Input Connector [2..3] Quality 134
Video Monitors 134
Video Output Connector [1..1] CEC Mode 135
Video Output Connector [1..1] OverscanLevel 135
Video Output Connector [1..1] Resolution 135
Video Output Connector [1..1] RGBQuantizationRange 135
Video Presentation DefaultPIPPosition 136
Video Presentation DefaultSource 136

Video Selfview Default FullscreenMode 136
Video Selfview Default Mode 136
Video Selfview Default PIPPosition 137
Video Selfview OnCall Duration 137
Video Selfview OnCall Mode 137

Experimental settings 138

Audio settings

Audio DefaultVolume

Define the default volume for the speakers. The volume is set to this value when you switch on or restart the video system. Use the controls on the user interface to change the volume while it is running. You may also use API commands (xCommand Audio Volume) to change the volume while the video system is running, and to reset to default value.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

Range: Select a value between 1 and 100. This corresponds to the dB range from -34.5 dB to 15 dB, in steps of 0.5 dB. If set to 0 the audio is switched off.

Audio Microphones Mute Enabled

Define the microphone mute behaviour on the video system.

Requires user role: ADMIN, INTEGRATOR

Default value: True

Value space: True/InCallOnly

True: Muting of audio is always available.

InCallOnly: Muting of audio is only available when the device is in a call. When Idle it is not possible to mute the microphone. This is useful when an external telephone service/audio system is connected via the codec and is to be available when the codec is not in a call. When set to InCallOnly this will prevent the audio-system from being muted by mistake.

Audio SoundsAndAlerts RingTone

Define which ringtone to use for incoming calls.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Sunrise

Value space: Sunrise/Mischief/Ripples/Reflections/Vibes/Delight/Evolve/Playful/Ascent/Calculation/Mellow/Ringer

Select a ringtone from the list.

Audio SoundsAndAlerts RingVolume

Define the ring volume for incoming calls.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

Range: The value goes in steps of 5 from 0 to 100 (from -34.5 dB to 15 dB). Volume 0 = Off.

Audio Input Microphone [2..2] EchoControl Mode

The echo canceller continuously adjusts itself to the audio characteristics of the room, and compensates for any changes it detects in the audio environment. If the changes in the audio conditions are significant, the echo canceller may take a second or two to re-adjust.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Turn off the echo control. Recommended if external echo cancellation or playback equipment is used.

On: Turn on the echo control. Recommended, in general, to prevent the far end from hearing their own audio. Once selected, echo cancellation is active at all times.

Audio Input Microphone [2..2] EchoControl NoiseReduction

The system has built-in noise reduction, which reduces stationary background noise, for example noise from air-conditioning systems, cooling fans etc. In addition, a high pass filter (Humfilter) reduces very low frequency noise. Noise reduction requires that Audio Input Microphone [n] EchoControl Mode is enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Turn off the noise reduction.

On: Turn on the noise reduction. Recommended in the presence of low frequency noise.

Audio Input Microphone [2..2] EchoControl Dereverberation

The system has built-in signal processing to reduce the effect of room reverberation. Dereverberation requires that Audio Input Microphone [n] EchoControl Mode is enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Turn off the dereverberation.

On: Turn on the dereverberation.

Audio Input Microphone [2..2] Level

Set the gain on the Microphone input connector. The gain should be adjusted to suit the output level of the connected audio source. The gain can be tuned in steps of 1 dB.

If the gain is set too high, the audio signal will be clipped. If the gain is set too low, the audio signal-to-noise ratio will be degraded; however, this is usually preferable to clipping.

Note that unprocessed speech signals typically contain significant level variations, making it very important to allow for sufficient signal headroom.

The maximum input level with 0 dB gain is -18 dBu.

Example: If your microphone has a maximum output level of -40 dBu, then you should set the gain to -18 dBu - (-40 dBu) = 22 dB.

Requires user role: ADMIN, INTEGRATOR

Default value: 17

Value space: Integer (0..24)

Range: Select the gain in decibel (dB).

Audio Input Microphone [1..2] Mode

Disable or enable audio on the microphone connector. Note that Microphone [1] is the video system's internal microphone.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the audio input microphone connector.

On: Enable the audio input microphone connector.

Audio Output Line [1..1] Delay DelayMs

To obtain lip-synchronization, you can configure each audio line output with an extra delay that compensates for delay in other connected devices, for example TVs and external loudspeakers. The delay that you set here is either fixed or relative to the delay on the HDMI output, as defined in the Audio Output Line [n] Delay Mode setting.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (0..290)

The delay in milliseconds.

Audio Output Line [1..1] Delay Mode

You may add extra delay to an audio line output with the Audio Output Line [n] Delay DelayMs setting. The extra delay added is either a fixed number of milliseconds, or a number of milliseconds relative to the detected delay on the HDMI output (typically introduced by the connected TV).

Requires user role: ADMIN, INTEGRATOR

Default value: RelativeToHDMI

Value space: Fixed/RelativeToHDMI

Fixed: Any extra delay (DelayMs) added to the output, will be a fixed number of millisecond.

RelativeToHDMI: Any extra delay (DelayMs) added to the output, will be relative to the detected delay on the HDMI output. The actual delay is HDMI-delay + DelayMs. The Audio Output Connectors Line [n] DelayMs status reports the actual delay.

Audio Ultrasound Mode

This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Requires user role: ADMIN, INTEGRATOR

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The video system adjusts the ultrasound volume dynamically. The volume may vary up to the maximum level as defined in the Audio Ultrasound Volume MaxVolume setting.

Static: Use only if advised by Cisco.

Audio Ultrasound MaxVolume

This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing message.

Requires user role: ADMIN, INTEGRATOR

Default value: 70

Value space: Integer (0..70)

Select a value in the specified range. If set to 0, the ultrasound is switched off.

CallHistory settings

CallHistory Mode

Determine whether or not information about calls that are placed or received are stored, including missed calls and calls that are not answered (call history). This determines whether or not the calls appear in the Recents list in the user interfaces.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: New entries are not added to the call history.

On: New entries are stored in the call history list.

Cameras settings

Cameras Camera [1..1] Backlight DefaultMode

This configuration turns backlight compensation on or off. Backlight compensation is useful when there is much light behind the persons in the room. Without compensation the persons will easily appear very dark to the far end.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

Cameras Camera [1..1] Brightness Mode

Define the camera brightness mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: The camera brightness is automatically set by the system.

Manual: Enable manual control of the camera brightness. The brightness level is set using the Cameras Camera [n] Brightness DefaultLevel setting.

Cameras Camera [1..1] Brightness DefaultLevel

Define the brightness level. Requires the Cameras Camera [n] Brightness Mode to be set to Manual.

Requires user role: ADMIN, INTEGRATOR

Default value: 20

Value space: Integer (1..31)

The brightness level.

Cameras Camera [1..1] Flip

With Flip mode (vertical flip) you can flip the image upside down. Flipping applies both to the self-view and the video that is transmitted to the far end.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto

Auto: If the camera detects that it is mounted upside down, the image is automatically flipped.

Cameras Camera [1..1] Focus Mode

Define the camera focus mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/AutoLimited/Manual

Auto: The camera will do single shot auto focusing once a call is connected, as well as after pan, tilt, zoom have changed.

AutoLimited: Not applicable.

Manual: Turn the autofocus off and adjust the camera focus manually.

Cameras Camera [1..1] Mirror

With Mirror mode (horizontal flip) you can mirror the image on screen. Mirroring applies both to the self-view and the video that is transmitted to the far end.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Off/On

Auto: If the camera detects that it is mounted upside down, the image is automatically mirrored. If the camera cannot auto-detect whether it is mounted upside down or not, the image is not changed.

Off: Display the image as other people see you.

On: Display the image as you see yourself in a mirror.

Cameras Camera [1..1] Whitebalance Mode

Define the camera white balance mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: The camera will continuously adjust the white balance depending on the camera view.

Manual: Enables manual control of the camera white balance. The white balance level is set using the Cameras Camera [n] Whitebalance Level setting.

Cameras Camera [1..1] Whitebalance Level

Define the white balance level. Requires the Cameras Camera [n] Whitebalance Mode to be set to manual.

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: Integer (1..16)

The white balance level.

Conference settings

Conference ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server or Cisco Meeting Server using the video system's interfaces. Each user can see the participant list, change video layout, disconnect participants, etc. from the interface. The active control feature is enabled by default, provided that it is supported by the infrastructure (Cisco Unified Communications Manager (CUCM) version 9.1.2 or newer, Cisco TelePresence Video Communication Server (VCS) version X8.1 or newer, Cisco Media Server (CMS) version 2.1 or newer). Change this setting if you want to disable the active control features.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off

Auto: Active control is enabled when supported by the infrastructure.

Off: Active control is disabled.

Conference AutoAnswer Mode

Define the auto answer mode. Use the Conference AutoAnswer Delay setting if you want the system to wait a number of seconds before answering the call, and use the Conference AutoAnswer Mute setting if you want your microphone to be muted when the call is answered.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: You must answer incoming calls manually by pressing the OK key or the green Call key on the remote control, or by tapping Answer on the Touch controller.

On: The system automatically answers incoming calls, except if you are already in a call. You must always answer or decline incoming calls manually when you are already engaged in a call.

Conference AutoAnswer Mute

Define if the microphone shall be muted when an incoming call is automatically answered. Requires that AutoAnswer Mode is switched on.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The incoming call will not be muted.

On: The incoming call will be muted when automatically answered.

Conference AutoAnswer Delay

Define how long (in seconds) an incoming call has to wait before it is answered automatically by the system. Requires that AutoAnswer Mode is switched on.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..50)

The auto answer delay (seconds).

Conference CallProtocolIPStack

Select if the system should enable IPv4, IPv6, or dual IP stack on the call protocol (SIP, H323).

Requires user role: ADMIN

Default value: Dual

Value space: Dual/IPv4/IPv6

Dual: Enables both IPv4 and IPv6 for the call protocol.

IPv4: When set to IPv4, the call protocol will use IPv4.

IPv6: When set to IPv6, the call protocol will use IPv6.

Conference DefaultCall Protocol

Define the Default Call Protocol to be used when placing calls from the system.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/H320/H323/Sip/Spark

Auto: Enables auto-selection of the call protocol based on which protocols are available. If multiple protocols are available, the order of priority is: 1) SIP; 2) H323; 3) H320. If the system cannot register, the auto-selection chooses H323.

H320: All calls are set up as H.320 calls (only applicable if used with Cisco TelePresence ISDN Link).

H323: All calls are set up as H.323 calls.

Sip: All calls are set up as SIP calls.

Spark: Reserved for Spark registered systems. Do not use.

Conference DefaultCall Rate

Define the Default Call Rate to be used when placing calls from the system.

Requires user role: ADMIN, INTEGRATOR

Default value: 3072

Value space: Integer (64..3072)

The default call rate (kbps).

Conference DoNotDisturb DefaultTimeout

This setting determines the default duration of a Do Not Disturb session, i.e. the period when incoming calls are rejected and registered as missed calls. The session can be terminated earlier by using the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: 60

Value space: Integer (1..1440)

The number of minutes (maximum 1440 minutes = 24 hours) before the Do Not Disturb session times out automatically.

Conference Encryption Mode

Define the conference encryption mode. A padlock with the text "Encryption On" or "Encryption Off" displays on screen for a few seconds when the conference starts.

NOTE: If the Encryption Option Key is not installed on the video system, the encryption mode is always Off.

Requires user role: ADMIN

Default value: BestEffort

Value space: Off/On/BestEffort

Off: The system will not use encryption.

On: The system will only allow calls that are encrypted.

BestEffort: The system will use encryption whenever possible.

> In Point to point calls: If the far end system supports encryption (AES-128), the call will be encrypted. If not, the call will proceed without encryption.

> In MultiSite calls: In order to have encrypted MultiSite conferences, all sites must support encryption. If not, the conference will be unencrypted.

Conference FarEndControl Mode

Lets you decide if the remote side (far end) should be allowed to select your video sources and control your local camera (pan, tilt, zoom).

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The far end is not allowed to select your video sources or to control your local camera (pan, tilt, zoom).

On: Allows the far end to be able to select your video sources and control your local camera (pan, tilt, zoom). You will still be able to control your camera and select your video sources as normal.

Conference FarEndControl SignalCapability

Define the far end control (H.224) signal capability mode.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the far end control signal capability.

On: Enable the far end control signal capability.

Conference MaxReceiveCallRate

Define the maximum receive bit rate to be used when placing or receiving calls. Note that this is the maximum bit rate for each individual call; use the Conference MaxTotalReceiveCallRate setting to set the aggregated maximum for all simultaneous active calls.

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

The maximum receive call rate (kbps).

Conference MaxTransmitCallRate

Define the maximum transmit bit rate to be used when placing or receiving calls. Note that this is the maximum bit rate for each individual call; use the Conference MaxTotalTransmitCallRate setting to set the aggregated maximum for all simultaneous active calls.

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

The maximum transmitt call rate (kbps).

Conference MaxTotalReceiveCallRate

Define the maximum overall receive bit rate allowed. This product does not support multiple simultaneous calls, so the total receive call rate will be the same as the receive bit rate for one call (ref. Conference MaxReceiveCallRate setting).

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

The maximum receive call rate (kbps).

Conference MaxTotalTransmitCallRate

Define the maximum overall transmit bit rate allowed. This product does not support multiple simultaneous calls, so the total transmit call rate will be the same as the transmit bit rate for one call (ref. Conference MaxTransmitCallRate setting).

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

The maximum transmit call rate (kbps).

Conference MicUnmuteOnDisconnect Mode

Define if the microphones shall be unmuted automatically when all calls are disconnected. In a meeting room or other shared resources this may be done to prepare the system for the next user.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: If muted during a call, let the microphones remain muted after the call is disconnected.

On: Unmute the microphones after the call is disconnected.

Conference Presentation OnPlacedOnHold

Define whether or not to continue sharing a presentation after the remote site has put you on hold.

Requires user role: ADMIN

Default value: NoAction

Value space: Stop/NoAction

Stop: The video system stops the presentation sharing when the remote site puts you on hold. The presentation will not continue when the call is resumed.

NoAction: The video system will not stop the presentation sharing when put on hold. The presentation will not be shared while you are on hold, but it will continue automatically when the call is resumed.

Conference VideoBandwidth Mode

Define the conference video bandwidth mode.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The available transmit bandwidth for the video channels are distributed among the currently active channels. If there is no presentation, the main video channels will use the bandwidth of the presentation channel.

Static: The available transmit bandwidth is assigned to each video channel, even if it is not active.

FacilityService settings

FacilityService Service [1..5] Type

Up to five different facility services can be supported simultaneously. With this setting you can select what kind of services they are. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the Touch user interface. They are not available for systems that use a remote control.

Requires user role: ADMIN, INTEGRATOR

Default value: Helpdesk

Value space: Catering/Concierge/Emergency/Helpdesk/Security/Transportation/Other

Catering: Select this option for catering services.

Concierge: Select this option for concierge services.

Emergency: Select this option for emergency services.

Helpdesk: Select this option for helpdesk services.

Security: Select this option for security services.

Transportation: Select this option for transportation services.

Other: Select this option for services not covered by the other options.

FacilityService Service [1..5] Name

Define the name of the facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. The name will show on the facility service call button, which appears when you tap the question mark icon in the top bar. Facility services are available from the Touch user interface. They are not available for systems that use a remote control.

Requires user role: ADMIN, INTEGRATOR

Default value: Service 1: " Live Support" Other services: " "

Value space: String (0, 1024)

The name of the facility service.

FacilityService Service [1..5] Number

Define the number (URI or phone number) of the facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the Touch user interface. They are not available for systems that use a remote control.

Requires user role: ADMIN, INTEGRATOR

Default value: " "

Value space: String (0, 1024)

The number (URI or phone number) of the facility service.

FacilityService Service [1..5] CallType

Define the call type for each facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the Touch user interface. They are not available for systems that use a remote control.

Requires user role: ADMIN, INTEGRATOR

Default value: Video

Value space: Audio/Video

Audio: Select this option for audio calls.

Video: Select this option for video calls.

H323 settings

H323 Authentication Mode

Define the authenticatin mode for the H.323 profile.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.

On: If an H.323 Gatekeeper indicates that it requires authentication, the system will try to authenticate itself to the gatekeeper. Requires the H323 Authentication LoginName and H323 Authentication Password settings to be defined on both the codec and the Gatekeeper.

H323 Authentication LoginName

The system sends the H323 Authentication Login Name and the H323 Authentication Password to an H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. Requires the H.323 Authentication Mode to be enabled.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 50)

The authentication login name.

H323 Authentication Password

The system sends the H323 Authentication Login Name and the H323 Authentication Password to an H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. Requires the H.323 Authentication Mode to be enabled.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 50)

The authentication password.

H323 CallSetup Mode

Defines whether to use a Gatekeeper or Direct calling when establishing H.323 calls.

Direct H.323 calls can be made also when H323 CallSetup Mode is set to Gatekeeper.

Requires user role: ADMIN

Default value: Gatekeeper

Value space: Direct/Gatekeeper

Direct: You can only make an H.323 call by dialing an IP address directly.

Gatekeeper: The system uses a Gatekeeper to make an H.323 call. When choosing this option, the H323 Gatekeeper Address must also be configured.

H323 Encryption KeySize

Define the minimum or maximum key size for the Diffie-Hellman key exchange method, which is used when establishing the Advanced Encryption Standard (AES) encryption key.

Requires user role: ADMIN

Default value: Min1024bit

Value space: Min1024bit/Max1024bit/Min2048bit

Min1024bit: The minimum size is 1024 bit.

Max1024bit: The maximum size is 1024 bit.

Min2048bit: The minimum size is 2048 bit.

H323 Gatekeeper Address

Define the IP address of the Gatekeeper. Requires H323 CallSetup Mode to be set to Gatekeeper.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

H323 H323Alias E164

The H.323 Alias E.164 defines the address of the system, according to the numbering plan implemented in the H.323 Gatekeeper. The E.164 alias is equivalent to a telephone number, sometimes combined with access codes.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 30)

The H.323 Alias E.164 address. Valid characters are 0-9, * and #.

H323 H323Alias ID

Define the H.323 Alias ID, which is used to address the system on a H.323 Gatekeeper and will be displayed in the call lists.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 49)

The H.323 Alias ID. Example: " firstname.lastname@company.com", " My H.323 Alias ID"

H323 NAT Mode

The firewall traversal technology creates a secure path through the firewall barrier, and enables proper exchange of audio/video data when connected to an external video conferencing system (when the IP traffic goes through a NAT router). NOTE: NAT does not work in conjunction with gatekeepers.

Requires user role: ADMIN

Default value: Off

Value space: Auto/Off/On

Auto: The system will determine if the H323 NAT Address or the real IP address should be used in signaling. This makes it possible to place calls to endpoints on the LAN as well as endpoints on the WAN. If the H323 NAT Address is wrong or not set, the real IP address will be used.

Off: The system will signal the real IP address.

On: The system will signal the configured H323 NAT Address instead of its real IP address in Q.931 and H.245. The NAT server address will be shown in the startup-menu as: " My IP Address: 10.0.2.1". If the H323 NAT Address is wrong or not set, H.323 calls cannot be set up.

H323 NAT Address

Define the external/global IP address to the router with NAT support. Packets sent to the router will then be routed to the system. Note that NAT cannot be used when registered to a gatekeeper.

In the router, the following ports must be routed to the system's IP address:

* Port 1720
* Port 5555-6555
* Port 2326-2487

Requires user role: ADMIN

Default value: " "

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

H323 PortAllocation

This setting affects the H.245 port numbers used for H.323 call signaling.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.

Static: When set to Static the ports are given within a static predefined range [5555-6555].

Logging settings

Logging External Mode

Determine whether or not to use a remote syslog server for logging.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable logging to a remote syslog server.

On: Enable logging to a remote syslog server.

Logging External Protocol

Determine which protocol to use toward the remote logging server. You can use either the syslog protocol over TLS (Transport Layer Security), or the syslog protocol in plaintext. For details about the syslog protocol, see RFC 5424.

Requires user role: ADMIN

Default value: SyslogTLS

Value space: Syslog/SyslogTLS

Syslog: Syslog protocol in plain text.

SyslogTLS: Syslog protocol over TLS.

Logging External Server Address

The address of the remote syslog server.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

Logging External Server Port

The port that the remote syslog server listens for messages on. If set to 0, the video system will use the standard syslog port. The standard syslog port is 514 for syslog, and 6514 for syslog over TLS.

Requires user role: ADMIN

Default value: 514

Value space: Integer (0..65535)

The number of the port that the remote syslog server is using. 0 means that the video system uses the standard syslog port.

Logging Mode

Define the logging mode for the video system (syslog service). When disabled, the syslog service does not start, and most of the event logs are not generated. The Historical Logs and Call Logs are not affected.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the system logging service.

On: Enable the system logging service.

Network settings

Network [1..1] DNS DNSSEC Mode

Domain Name System Security extensions (DNSSEC) is a set of extensions to DNS. It is used to authenticate DNS replies for zones that are signed. It will still allow unsigned zones.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: Disable Domain Name System Security Extensions.

On: Enable Domain Name System Security Extensions.

Network [1..1] DNS Domain Name

The DNS Domain Name is the default domain name suffix which is added to unqualified names.

Example: If the DNS Domain Name is "company.com" and the name to lookup is "MyVideoSystem", this will result in the DNS lookup "MyVideoSystem.company.com".

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The DNS domain name.

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

Define the network addresses for DNS servers. Up to three addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

Network [1..1] IEEE8021X Mode

The system can be connected to an IEEE 802.1X LAN network, with a port-based network access control that is used to provide authenticated network access for Ethernet networks.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: The 802.1X authentication is disabled.

On: The 802.1X authentication is enabled.

Network [1..1] IEEE8021X TlsVerify

Verification of the server-side certificate of an IEEE802.1x connection against the certificates in the local CA-list when TLS is used. The CA-list must be uploaded to the video system. This can be done from the web interface.

This setting takes effect only when Network [1] IEEE8021X Eap Tls is enabled (On).

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: When set to Off, TLS connections are allowed without verifying the server-side X.509 certificate against the local CA-list. This should typically be selected if no CA-list has been uploaded to the codec.

On: When set to On, the server-side X.509 certificate will be validated against the local CA-list for all TLS connections. Only servers with a valid certificate will be allowed.

Network [1..1] IEEE8021X UseClientCertificate

Authentication using a private key/certificate pair during an IEEE802.1x connection. The authentication X.509 certificate must be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: When set to Off client-side authentication is not used (only server-side).

On: When set to On the client (video system) will perform a mutual authentication TLS handshake with the server.

Network [1..1] IEEE8021X Identity

Define the user name for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

The user name for 802.1X authentication.

Network [1..1] IEEE8021X Password

Define the password for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 50)

The password for 802.1X authentication.

Network [1..1] IEEE8021X AnonymousIdentity

The 802.1X Anonymous ID string is to be used as unencrypted identity with EAP (Extensible Authentication Protocol) types that support different tunneled identity, like EAP-PEAP and EAP-TTLS. If set, the anonymous ID will be used for the initial (unencrypted) EAP Identity Request.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

The 802.1X Anonymous ID string.

Network [1..1] IEEE8021X Eap Md5

Define the Md5 (Message-Digest Algorithm 5) mode. This is a Challenge Handshake Authentication Protocol that relies on a shared secret. Md5 is a Weak security.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled.

Network [1..1] IEEE8021X Eap Ttls

Define the TTLS (Tunneled Transport Layer Security) mode. Authenticates LAN clients without the need for client certificates. Developed by Funk Software and Certicom. Usually supported by Agere Systems, Proxim and Avaya.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled.

Network [1..1] IEEE8021X Eap Tls

Enable or disable the use of EAP-TLS (Transport Layer Security) for IEEE802.1x connections. The EAP-TLS protocol, defined in RFC 5216, is considered one of the most secure EAP standards. LAN clients are authenticated using client certificates.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled.

Network [1..1] IEEE8021X Eap Peap

Define the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled.

Network [1..1] IPStack

Select if the system should use IPv4, IPv6, or dual IP stack, on the network interface. NOTE: After changing this setting you may have to wait up to 30 seconds before it takes effect.

Requires user role: ADMIN, USER

Default value: Dual

Value space: Dual/IPv4/IPv6

Dual: When set to Dual, the network interface can operate on both IP versions at the same time, and can have both an IPv4 and an IPv6 address at the same time.

IPv4: When set to IPv4, the system will use IPv4 on the network interface.

IPv6: When set to IPv6, the system will use IPv6 on the network interface.

Network [1..1] IPv4 Assignment

Define how the system will obtain its IPv4 address, subnet mask and gateway address. This setting applies only to systems on IPv4 networks.

Requires user role: ADMIN, USER

Default value: DHCP

Value space: Static/DHCP

Static: The addresses must be configured manually using the Network IPv4 Address, Network IPv4 Gateway and Network IPv4 SubnetMask settings (static addresses).

DHCP: The system addresses are automatically assigned by the DHCP server.

Network [1..1] IPv4 Address

Define the static IPv4 network address for the system. Applicable only when Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv4 address.

Network [1..1] IPv4 Gateway

Define the IPv4 network gateway address. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv4 address.

Network [1..1] IPv4 SubnetMask

Define the IPv4 network subnet mask. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv4 address.

Network [1..1] IPv6 Assignment

Define how the system will obtain its IPv6 address and the default gateway address. This setting applies only to systems on IPv6 networks.

Requires user role: ADMIN, USER

Default value: Autoconf

Value space: Static/DHCPv6/Autoconf

Static: The codec and gateway IP addresses must be configured manually using the Network IPv6 Address and Network IPv6 Gateway settings. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

DHCPv6: All IPv6 addresses, including options, will be obtained from a DHCPv6 server. See RFC 3315 for a detailed description. The Network IPv6 DHCPOptions setting will be ignored.

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC 4862 for a detailed description. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

Network [1..1] IPv6 Address

Define the static IPv6 network address for the system. Applicable only when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv6 address including a network mask. Example: 2001:DB8::/48

Network [1..1] IPv6 Gateway

Define the IPv6 network gateway address. This setting is only applicable when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv6 address.

Network [1..1] IPv6 DHCPOptions

Retrieve a set of DHCP options, for example NTP and DNS server addresses, from a DHCPv6 server.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: Disable the retrieval of DHCP options from a DHCPv6 server.

On: Enable the retrieval of a selected set of DHCP options from a DHCPv6 server.

Network [1..1] MTU

Define the Ethernet MTU (Maximum Transmission Unit) size. The MTU size must be supported by your network infrastructure. The minimum size is 576 for IPv4 and 1280 for IPv6.

Requires user role: ADMIN, USER

Default value: 1500

Value space: Integer (576..1500)

Set a value for the MTU (bytes).

Network [1..1] QoS Mode

The QoS (Quality of Service) is a method which handles the priority of audio, video and data in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS priorities on modern IP networks.

Requires user role: ADMIN, USER

Default value: Diffserv

Value space: Off/Diffserv

Off: No QoS method is used.

Diffserv: When you set the QoS Mode to Diffserv, the Network QoS Diffserv Audio, Network QoS Diffserv Video, Network QoS Diffserv Data, Network QoS Diffserv Signalling, Network QoS Diffserv ICMPv6 and Network QoS Diffserv NTP settings are used to prioritize packets.

Network [1..1] QoS Diffserv Audio

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Audio packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Audio is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the audio packets in the IP network - the higher the number, the higher the priority. 0 means " best effort".

Network [1..1] QoS Diffserv Video

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Video packets should have in the IP network. The packets on the presentation channel (shared content) are also in the Video packet category. The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Video is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the video packets in the IP network - the higher the number, the higher the priority. 0 means " best effort".

Network [1..1] QoS Diffserv Data

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Data packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for Data is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the data packets in the IP network - the higher the number, the higher the priority. 0 means " best effort".

Network [1..1] QoS Diffserv Signalling

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Signalling packets that are deemed critical (time-sensitive) for the real-time operation should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Signalling is CS3, which equals the decimal value 24. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the signalling packets in the IP network - the higher the number, the higher the priority. 0 means " best effort".

Network [1..1] QoS Diffserv ICMPv6

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority ICMPv6 packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for ICMPv6 is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the ICMPv6 packets in the IP network - the higher the number, the higher the priority. 0 means " best effort".

Network [1..1] QoS Diffserv NTP

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority NTP packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for NTP is 0, which means " best effort". If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the NTP packets in the IP network - the higher the number, the higher the priority. 0 means " best effort".

Network [1..1] RemoteAccess Allow

Define which IP addresses (IPv4/IPv6) are allowed for remote access to the codec from SSH/Telnet/HTTP/HTTPS. Multiple IP addresses are separated by a white space.

A network mask (IP range) is specified by <ip address>/N, where N is 1-32 for IPv4, and N is 1-128 for IPv6. The /N is a common indication of a network mask where the first N bits are set. Thus 192.168.0.0/24 would match any address starting with 192.168.0, since these are the first 24 bits in the address.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0..255)

A valid IPv4 address or IPv6 address.

Network [1..1] Speed

Define the Ethernet link speed. We recommend not to change from the default value, which negotiates with the network to set the speed automatically. If you do not use auto-negotiation, make sure that the speed you choose is supported by the closest switch in your network infrastructure.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Auto/10half/10full/100half/100full

Auto: Auto-negotiate link speed.

10half: Force link to 10 Mbps half-duplex.

10full: Force link to 10 Mbps full-duplex.

100half: Force link to 100 Mbps half-duplex.

100full: Force link to 100 Mbps full-duplex.

Network [1..1] TrafficControl Mode

Define the network traffic control mode to decide how to control the video packets transmission speed.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: Transmit video packets at link speed.

On: Transmit video packets at maximum 20 Mbps. Can be used to smooth out bursts in the outgoing network traffic.

Network [1..1] VLAN Voice Mode

Define the VLAN voice mode. The VLAN Voice Mode will be set to Auto automatically if you have Cisco UCM (Cisco Unified Communications Manager) as provisioning infrastructure. Note that Auto mode will NOT work if the NetworkServices CDP Mode setting is Off.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Auto/Manual/Off

Auto: The Cisco Discovery Protocol (CDP), if available, assigns an id to the voice VLAN. If CDP is not available, VLAN is not enabled.

Manual: The VLAN ID is set manually using the Network VLAN Voice VlanId setting. If CDP is available, the manually set value will be overruled by the value assigned by CDP.

Off: VLAN is not enabled.

Network [1..1] VLAN Voice VlanId

Define the VLAN voice ID. This setting will only take effect if Network VLAN Voice Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: 1

Value space: Integer (1..4094)

Set the VLAN voice ID.

NetworkServices settings

NetworkServices CDP Mode

Enable or disable the CDP (Cisco Discovery Protocol) daemon. Enabling CDP will make the endpoint report certain statistics and device identifiers to a CDP-enabled switch. If CDP is disabled, the Network VLAN Voice Mode: Auto setting will not work.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

NetworkServices H323 Mode

Define whether the system should be able to place and receive H.323 calls or not.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable the possibility to place and receive H.323 calls.

On: Enable the possibility to place and receive H.323 calls.

NetworkServices HTTP Mode

Define whether or not to allow access to the video system using the HTTP or HTTPS (HTTP Secure) protocols. Note that the video system's web interface use HTTP or HTTPS. If this setting is switched Off, you cannot use the web interface.

If you need extra security (encryption and decryption of requests, and pages that are returned by the web server), allow only HTTPS.

Requires user role: ADMIN

Default value: HTTP+HTTPS

Value space: Off/HTTP+HTTPS/HTTPS

Off: Access to the video system not allowed via HTTP or HTTPS.

HTTP+HTTPS: Access to the video system allowed via both HTTP and HTTPS.

HTTPS: Access to the video system allowed via HTTPS, but not via HTTP.

NetworkServices HTTP Proxy Allowed

The HTTP Proxy Settings are available from the user interface when the system is provisioned to Cisco Spark. The HTTP proxy settings makes it possible to onboard a video system behind a HTTP proxy to Spark.

Requires user role: ADMIN, USER

Default value: False

Value space: False/True

False: The HTTP proxy settings are not available from the Cisco Spark setup wizard.

True: The HTTP proxy settings are available from the Cisco Spark setup wizard.

NetworkServices HTTP Proxy LoginName

This is the user name part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 80)

The authentication login name.

NetworkServices HTTP Proxy Password

This is the password part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

The authentication password.

NetworkServices HTTP Proxy Mode

The HTTP proxy for Cisco Spark can be set up manually, it can be auto-configured (PACUrl), fully automated (WPAD), or it can be turned off.

Requires user role: ADMIN, USER

Default value: Off

Value space: Manual/Off/PACUrl/WPAD

Manual: Enter the address of the proxy server in the NetworkServices HTTP Proxy URL setting. Optionally, also add the HTTP proxy login name and password in the NetworkServices HTTP Proxy LoginName/Password settings.

Off: The HTTP proxy mode is turned off.

PACUrl: The HTTP proxy is auto-configured. You must enter the URL for the PAC (Proxy Auto Configuration) script in the NetworkServices HTTP Proxy PACUrl setting.

WPAD: With WPAD (Web Proxy Auto Discovery) the HTTP proxy is fully automated and auto-configured.

NetworkServices HTTP Proxy Url

Set the URL of the HTTP proxy server. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0..255)

The URL of the HTTP proxy server.

NetworkServices HTTP Proxy PACUrl

Set the URL of the PAC (Proxy Auto Configuration) script. Requires that the NetworkServices HTTP Proxy Mode is set to PACUrl.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0..255)

The URL of the PAC (Proxy Auto Configuration) script.

NetworkServices HTTPS Server MinimumTLSVersion

Set the lowest version of the TLS (Transport Layer Security) protocol that is allowed.

Requires user role: ADMIN

Default value: TLSv1.1

Value space: TLSv1.1/TLSv1.2

TLSv1.1: Support of TLS version 1.1 or higher.

TLSv1.2: Support of TLS version 1.2 or higher.

NetworkServices HTTPS StrictTransportSecurity

The HTTP Strict Transport Security header lets a web site inform the browser that it should never load the site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The HTTP strict transport security feature is disabled.

On: The HTTP strict transport security feature is enabled.

NetworkServices HTTPS VerifyServerCertificate

When the video system connects to an external HTTPS server (like a phone book server or an external manager), this server will present a certificate to the video system to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify server certificates.

On: Requires the system to verify that the server certificate is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS VerifyClientCertificate

When the video system connects to a HTTPS client (like a web browser), the client can be asked to present a certificate to the video system to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify client certificates.

On: Requires the client to present a certificate that is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS OCSP Mode

Define the support for OCSP (Online Certificate Status Protocol) responder services. The OCSP feature allows users to enable OCSP instead of certificate revocation lists (CRLs) to check the certificate status.

For any outgoing HTTPS connection, the OCSP responder is queried of the status. If the corresponding certificate has been revoked, then the HTTPS connection will not be used.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable OCSP support.

On: Enable OCSP support.

NetworkServices HTTPS OCSP URL

Define the URL of the OCSP responder (server) that will be used to check the certificate status.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

A valid URL.

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the system's time and date to a reference time server. The time server will be queried regularly for time updates.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Manual/Off

Auto: The system will use an NTP server for time reference. As default, the server address will be obtained from the network's DHCP server. If a DHCP server is not used, or if the DHCP server does not provide an NTP server address, the NTP server address that is specified in the NetworkServices NTP Server [n] Address setting will be used.

Manual: The system will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.

Off: The system will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

NetworkServices NTP Server [1..3] Address

The address of the NTP server that will be used when NetworkServices NTP Mode is set to Manual, and when NetworkServices NTP Mode is set to Auto and no address is supplied by a DHCP server.

Requires user role: ADMIN

Default value: " 0.tandberg.pool.ntp.org"

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SIP Mode

Define whether the system should be able to place and receive SIP calls or not.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the possibility to place and receive SIP calls.

On: Enable the possibility to place and receive SIP calls.

NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices (routers, servers, switches, projectors, etc) for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

Requires user role: ADMIN

Default value: ReadOnly

Value space: Off/ReadOnly/ReadWrite

Off: Disable the SNMP network service.

ReadOnly: Enable the SNMP network service for queries only.

ReadWrite: Enable the SNMP network service for both queries and commands.

NetworkServices SNMP Host [1..3] Address

Define the address of up to three SNMP Managers.

The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.), for example about system location and system contact. SNMP traps are not supported.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SNMP CommunityName

Define the name of the Network Services SNMP Community. SNMP Community names are used to authenticate SNMP requests. SNMP requests must have a password (case sensitive) in order to receive a response from the SNMP Agent in the codec. The default password is " public". If you have the Cisco TelePresence Management Suite (TMS) you must make sure the same SNMP Community is configured there too. NOTE: The SNMP Community password is case sensitive.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 50)

The SNMP community name.

NetworkServices SNMP SystemContact

Define the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 50)

The name of the SNMP system contact.

NetworkServices SNMP SystemLocation

Define the name of the Network Services SNMP System Location.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 50)

The name of the SNMP system location.

NetworkServices SSH Mode

SSH (or Secure Shell) protocol can provide secure encrypted communication between the codec and your local computer.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) public key authentication can be used to access the codec.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH public key is not allowed.

On: The SSH public key is allowed.

NetworkServices Telnet Mode

Telnet is a network protocol used on the Internet or Local Area Network (LAN) connections.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The Telnet protocol is disabled. This is the factory setting.

On: The Telnet protocol is enabled.

NetworkServices UPnP Mode

Fully disable UPnP (Universal Plug and Play), or enable UPnP for a short time period after the video system has been switched on or restarted.

The default operation is that UPnP is enabled when you switch on or restart the video system. Then UPnP is automatically disabled after the timeout period that is defined in the NetworkServices UPnP Timeout setting. Use the video system's web interface to set the timeout.

When UPnP is enabled, the video system advertises its presence on the network. The advertisement permits a Touch controller to discover video systems automatically, and you do not need to manually enter the video system's IP address in order to pair the Touch controller.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: UPnP is disabled. The video system does not advertise its presence, and you have to enter the video system's IP address manually in order to pair a Touch controller to the video system.

On: UPnP is enabled. The video system advertises its presence until the timeout period expires.

NetworkServices UPnP Timeout

Define for how many seconds UPnP shall stay enabled after the video system is switched on or restarted. The NetworkServices UPnP Mode setting must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: 600

Value space: Integer (0..3600)

Range: Select a value between 0 and 3600 seconds.

NetworkServices WelcomeText

Choose which information the user should see when logging on to the codec through Telnet/SSH.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The welcome text is: Login successful

On: The welcome text is: Welcome to <system name>; Software version; Software release date; Login successful.

NetworkServices XMLAPI Mode

Enable or disable the video system's XML API. For security reasons this may be disabled. Disabling the XML API will limit the remote manageability with for example TMS, which no longer will be able to connect to the video system.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The XML API is disabled.

On: The XML API is enabled.

Peripherals settings

Peripherals Pairing CiscoTouchPanels EmcResilience

If the Touch controller is used in environments with considerable amounts of electromagnetic noise present, you may experience an appearance of false signals–for example as if someone tapped the Touch controller when obviously nobody did so. To cope with this you may enable the EMC Resilience Mode.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The EMC resilience is disabled.

On: The EMC resilience is enabled.

Peripherals Pairing CiscoTouchPanels RemotePairing

In order to use Cisco Touch 10 (touch controller) as user interface for the video system, Touch 10 must be paired to the video system via the network (LAN). This is referred to as remote pairing.

Remote pairing is allowed by default; you must switch this setting Off if you want to prevent remote pairing.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Remote pairing of Touch 10 is not allowed.

On: Remote pairing of Touch 10 is allowed.

Peripherals Profile Cameras

Define the number of cameras that are expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected cameras does not match this setting, the diagnostics service will report it as an inconsistency.

Requires user role: ADMIN, INTEGRATOR

Default value: Minimum1

Value space: NotSet/Minimum1/0/1/2/3/4/5/6/7

NotSet: No camera check is performed.

Minimum1: At least one camera should be connected to the video system.

0-7: Select the number of cameras that are expected to be connected to the video system.

Peripherals Profile ControlSystems

Define if a third-party control system, for example Crestron or AMX, is expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected control systems does not match this setting, the diagnostics service will report it as an inconsistency. Note that only one third-party control system is supported.

If set to 1, the control system must send heart beats to the video system using xCommand Peripherals Pair and HeartBeat commands. Failing to do so will cause the in-room control extensions to show a warning that the video system has lost connectivity to the control system.

Requires user role: ADMIN, INTEGRATOR

Default value: NotSet

Value space: 1/NotSet

1: One third-party control system should be connected to the video system.

NotSet: No check for a third-party control system is performed.

Peripherals Profile TouchPanels

Define the number of Cisco Touch controllers that are expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected Touch controllers does not match this setting, the diagnostics service will report it as an inconsistency.

Requires user role: ADMIN, INTEGRATOR

Default value: NotSet

Value space: NotSet/Minimum1/0/1/2/3/4/5

NotSet: No touch panel check is performed.

Minimum1: At least one Cisco Touch controller should be connected to the video system.

0-5: Select the number of Touch controllers that are expected to be connected to the video system. Note that only one Cisco Touch controller is officially supported.

Phonebook settings

Phonebook Server [1..1] ID

Define a name for the external phone book.

Requires user role: ADMIN
Default value: " "

Value space: String (0, 64)
The name for the external phone book.

Phonebook Server [1..1] Type

Select the phonebook server type.

Requires user role: ADMIN
Default value: Off

Value space: Off/CUCM/Spark/TMS/VCS
Off: Do not use a phonebook.
CUCM: The phonebook is located on the Cisco Unified Communications Manager.
Spark: The phonebook is located on Spark.
TMS: The phonebook is located on the Cisco TelePresence Management Suite server.
VCS: The phonebook is located on the Cisco TelePresence Video Communication Server.

Phonebook Server [1..1] URL

Define the address (URL) to the external phone book server.

Requires user role: ADMIN
Default value: " "

Value space: String (0..255)
A valid address (URL) to the phone book server.

Provisioning settings

Provisioning Connectivity

This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Internal/External/Auto

Internal: Request internal configuration.

External: Request external configuration.

Auto: Automatically discover using NAPTR queries whether internal or external configurations should be requested. If the NAPTR responses have the "e" flag, external configurations will be requested. Otherwise internal configurations will be requested.

Provisioning Mode

It is possible to configure a video system using a provisioning system (external manager). This allows video conferencing network administrators to manage many video systems simultaneously. With this setting you choose which type of provisioning system to use. Provisioning can also be switched off. Contact your provisioning system provider/representative for more information.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Off/Auto/CUCM/Edge/Spark/TMS/VCS

Off: The video system is not configured by a provisioning system.

Auto: The provisioning server is automatically selected as set up in the DHCP server.

CUCM: Push configurations to the video system from CUCM (Cisco Unified Communications Manager).

Edge: Push configurations to the video system from CUCM (Cisco Unified Communications Manager). The system connects to CUCM via the Collaboration Edge infrastructure. In order to register over Edge the encryption option key must be installed on the video system.

Spark: Push configurations to the video system from Spark.

TMS: Push configurations to the video system from TMS (Cisco TelePresence Management System).

VCS: Push configurations to the video system from VCS (Cisco TelePresence Video Communication Server).

Provisioning LoginName

This is the username part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 80)

A valid username.

Provisioning Password

This is the password part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid password.

Provisioning ExternalManager Address

Define the IP Address or DNS name of the external manager / provisioning system.

If an External Manager Address (and Path) is configured, the system will send a message to this address when starting up. When receiving this message the external manager / provisioning system can return configurations/commands to the unit as a result.

When using CUCM or TMS provisioning, the DHCP server can be set up to provide the external manager address automatically (DHCP Option 242 for TMS, and DHCP Option 150 for CUCM). An address set in the Provisioning ExternalManager Address setting will override the address provided by DHCP.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager AlternateAddress

Only applicable when the endpoint is provisioned by Cisco Unified Communication Manager (CUCM) and an alternate CUCM is available for redundancy. Define the address of the alternate CUCM. If the main CUCM is not available, the endpoint will be provisioned by the alternate CUCM. When the main CUCM is available again, the endpoint will be provisioned by this CUCM.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager Protocol

Define whether to use the HTTP (unsecure communication) or HTTPS (secure communication) protocol when sending requests to the external manager / provisioning system.

The selected protocol must be enabled in the NetworkServices HTTP Mode setting.

Requires user role: ADMIN, USER

Default value: HTTP

Value space: HTTPS/HTTP

HTTPS: Send requests via HTTPS.

HTTP: Send requests via HTTP.

Provisioning ExternalManager Path

Define the Path to the external manager / provisioning system. This setting is required when several management services reside on the same server, i.e. share the same External Manager address.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0..255)

A valid path to the external manager or provisioning system.

Provisioning ExternalManager Domain

Define the SIP domain for the VCS provisioning server.

Requires user role: ADMIN, USER

Default value: " "

Value space: String (0, 64)

A valid domain name.

Proximity settings

Proximity Mode

Determine whether the video system will emit ultrasound pairing messages or not.

When the video system emits ultrasound, Proximity clients can detect that they are close to the video system. In order to use a client, at least one of the Proximity services must be enabled (refer to the Proximity Services settings). In general, Cisco recommends enabling all the Proximity services.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: The video system does not emit ultrasound, and Proximity services cannot be used.

On: The video system emits ultrasound, and Proximity clients can detect that they are close to the video system. Enabled Proximity services can be used.

Proximity Services CallControl

Enable or disable basic call control features on Proximity clients. When this setting is enabled, you are able to control a call using a Proximity client (for example dial, mute, adjust volume and hang up). This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Call control from a Proximity client is enabled.

Disabled: Call control from a Proximity client is disabled.

Proximity Services ContentShare FromClients

Enable or disable content sharing from Proximity clients. When this setting is enabled, you can share content from a Proximity client wirelessly on the video system, e.g. share your laptop screen. This service is supported by laptops (OS X and Windows). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Enabled

Value space: Enabled/Disabled

Enabled: Content sharing from a Proximity client is enabled.

Disabled: Content sharing from a Proximity client is disabled.

Proximity Services ContentShare ToClients

Enable or disable content sharing to Proximity clients. When enabled, Proximity clients will receive the presentation from the video system. You can zoom in on details, view previous content and take snapshots. This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Content sharing to a Proximity client is enabled.

Disabled: Content sharing to a Proximity client is disabled.

RTP settings

RTP Ports Range Start

Define the first port in the range of RTP ports.

As default, the system is using the ports in the range 2326 to 2486 for RTP and RTCP media data. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2326

Value space: Integer (1024..65438)

Set the first port in the range of RTP ports.

RTP Ports Range Stop

Define the last port in the range of RTP ports.

As default, the system is using the ports in the range 2326 to 2487 for RTP and RTCP media data. If the RTP Video Ports Range is enabled the system is using the ports in the range 1024 to 65436. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2486

Value space: Integer (1120..65535)

Set the last port in the range of RTP ports.

RTP Video Ports Range Start

Define the first port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65454)

Set the first port in the range of RTP video ports.

RTP Video Ports Range Stop

Define the last port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65535)

Set the last port in the range of RTP video ports.

Security settings

Security Audit Logging Mode

Define where to record or transmit the audit logs. The audit logs are sent to a syslog server.

When using the External/ExternalSecure modes and setting the port assignment to manual in the Security Audit Server PortAssignment setting, you must also enter the address and port number for the audit server in the Security Audit Server Address and Security Audit Server Port settings.

Requires user role: AUDIT

Default value: Internal

Value space: Off/Internal/External/ExternalSecure

Off: No audit logging is performed.

Internal: The system records the audit logs to internal logs, and rotates logs when they are full.

External: The system sends the audit logs to an external syslog server. The syslog server must support UDP.

ExternalSecure: The system sends encrypted audit logs to an external syslog server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the codec using the web interface. The common_name parameter of a certificate in the CA list must match the IP address of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

Security Audit OnError Action

Define what happens when the connection to the syslog server is lost. This setting is only relevant when Security Audit Logging Mode is set to ExternalSecure.

Requires user role: AUDIT

Default value: Ignore

Value space: Halt/Ignore

Halt: If a halt condition is detected the system codec is rebooted and only the auditor is allowed to operate the unit until the halt condition has passed. When the halt condition has passed the audit logs are re-spooled to the syslog server. Halt conditions are: A network breach (no physical link), no syslog server running (or incorrect address or port to the syslog server), TLS authentication failed (if in use), local backup (re-spooling) log full.

Ignore: The system will continue its normal operation, and rotate internal logs when full. When the connection is restored it will again send its audit logs to the syslog server.

Security Audit Server Address

The audit logs are sent to a syslog server. Define the IP address of the syslog server. Only valid IPv4 or IPv6 address formats are accepted. Host names are not supported. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure.

Requires user role: AUDIT

Default value: " "

Value space: String (0..255)

A valid IPv4 address or IPv6 address

Security Audit Server Port

The audit logs are sent to a syslog server. Define the port of the syslog server that the system shall send its audit logs to. This setting is only relevant when Security Audit Server PortAssignment is set to Manual.

Requires user role: AUDIT

Default value: 514

Value space: Integer (0..65535)

Set the audit server port.

Security Audit Server PortAssignment

The audit logs are sent to a syslog server. You can define how the port number of the external syslog server will be assigned. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure. To see which port number is used you can check the Security Audit Server Port status. Navigate to Setup > Status on the web interface or; if on a command line interface, run the command xStatus Security Audit Server Port.

Requires user role: AUDIT

Default value: Auto

Value space: Auto/Manual

Auto: Will use UDP port number 514 when the Security Audit Logging Mode is set to External. Will use TCP port number 6514 when the Security Audit Logging Mode is set to ExternalSecure.

Manual: Will use the port value defined in the Security Audit Server Port setting.

Security Session FailedLoginsLockoutTime

Define how long the system will lock out a user after failed login to a web or SSH session.

Restart the system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 60

Value space: Integer (0..10000)

Set the lockout time (minutes).

Security Session InactivityTimeout

Define how long the system will accept inactivity from the user before he is automatically logged out from a web, Telnet, or SSH session.

Restart the system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10000)

Set the inactivity timeout (minutes); or select 0 when inactivity should not enforce automatic logout.

Security Session MaxFailedLogins

Define the maximum number of failed login attempts per user for a web or SSH session. If the user exceeded the maximum number of attempts the user will be locked out. 0 means that there is no limit for failed logins.

Restart the system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10)

Set the maximum number of failed login attempts per user.

Security Session MaxSessionsPerUser

The maximum number of simultaneous sessions per user is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions per user.

Security Session MaxTotalSessions

The maximum number of simultaneous sessions in total is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions in total.

Security Session ShowLastLogon

When logging in to the system using SSH or Telnet you will see the UserId, time and date of the last session that did a successful login.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

On: Show information about the last session.

Off: Do not show information about the last session.

SerialPort settings

SerialPort Mode

Enable/disable the serial port.

Requires user role: ADMIN, INTEGRATOR
Default value: On

Value space: Off/On
Off: Disable the serial port.
On: Enable the serial port.

SerialPort LoginRequired

Define if login shall be required when connecting to the serial port.

Requires user role: ADMIN
Default value: On

Value space: Off/On
Off: The user can access the codec via the serial port without any login.
On: Login is required when connecting to the codec via the serial port.

SIP settings

SIP ANAT

ANAT (Alternative Network Address Types) enables media negotiation for multiple addresses and address types, as specified in RFC 4091.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable ANAT.

On: Enable ANAT.

SIP Authentication UserName

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 128)

A valid username.

SIP Authentication Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 128)

A valid password.

SIP DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/TCP/Tls/UDP

TCP: The system will always use TCP as the default transport method.

UDP: The system will always use UDP as the default transport method.

Tls: The system will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the video system. If no such CA-list is available on the system then anonymous Diffie Hellman will be used.

Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

SIP DisplayName

When configured the incoming call will report the display name instead of the SIP URI.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 550)

The name to be displayed instead of the SIP URI.

SIP Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the video systems can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the video systems.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

Auto: ICE is enabled if a TURN server is provided, otherwise ICE is disabled.

Off: ICE is disabled.

On: ICE is enabled.

SIP Ice DefaultCandidate

The ICE protocol needs some time to reach a conclusion about which media route to use (up to the first 5 seconds of a call). During this period media for the video system will be sent to the Default Candidate as defined in this setting.

Requires user role: ADMIN

Default value: Host

Value space: Host/Rflx/Relay

Host: Send media to the video system's private IP address.

Rflx: Send media to the video system's public IP address, as seen by the TURN server.

Relay: Send media to the IP address and port allocated on the TURN server.

SIP Line

When registered to a Cisco Unified Communications Manager (CUCM) the endpoint may be part of a shared line. This means that several devices share the same directory number. The different devices sharing the same number receive status from the other appearances on the line as defined in RFC 4235.

Note that shared lines are set up by CUCM, not by the endpoint. Therefore do not change this setting manually; CUCM pushes this information to the endpoint when required.

Requires user role: ADMIN

Default value: Private

Value space: Private/Shared

Shared: The system is part of a shared line and is therefore sharing its directory number with other devices.

Private: This system is not part of a shared line.

SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the endpoint will only be reachable through the SIP registrar (CUCM or VCS).

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Listening for incoming connections on the SIP TCP/UDP ports is turned off.

On: Listening for incoming connections on the SIP TCP/UDP ports is turned on.

SIP Mailbox

When registered to a Cisco Unified Communications Manager (CUCM) you may be offered the option of having a private voice mailbox.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 255)

A valid number or address. Leave the string empty if you do not have a voice mailbox.

SIP PreferredIPMedia

Define the preferred IP version for sending and receiving media (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for media is IPv4.

IPv6: The preferred IP version for media is IPv6.

SIP PreferredIPSignaling

Define the preferred IP version for signaling (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version. It also determines the priority of the A/AAAA lookups in DNS, so that the preferred IP version is used for registration.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for signaling is IPv4.

IPv6: The preferred IP version for signaling is IPv6.

SIP Proxy [1..4] Address

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

SIP TlsVerify

For TLS connections a SIP CA-list can be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Set to Off to allow TLS connections without verifying them. The TLS connections are allowed to be set up without verifying the x.509 certificate received from the server against the local CA-list. This should typically be selected if no SIP CA-list has been uploaded.

On: Set to On to verify TLS connections. Only TLS connections to servers, whose x.509 certificate is validated against the CA-list, will be allowed.

SIP Turn DiscoverMode

Define the discover mode to enable/disable the application to search for available Turn servers in DNS. Before making calls, the system will test if port allocation is possible.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Set to Off to disable discovery mode.

On: When set to On, the system will search for available Turn servers in DNS, and before making calls the system will test if port allocation is possible.

SIP Turn DropRflx

DropRflx will make the endpoint force media through the Turn relay, unless the remote endpoint is on the same network.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable DropRflx.

On: The system will force media through the Turn relay when the remote endpoint is on another network.

SIP Turn Server

Define the address of the TURN (Traversal Using Relay NAT) server. It is used as a media relay fallback and it is also used to discover the endpoint's own public IP address.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

The preferred format is DNS SRV record (e.g. _turn._udp.<domain>), or it can be a valid IPv4 or IPv6 address.

SIP Turn UserName

Define the user name needed for accessing the TURN server.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 128)

A valid user name.

SIP Turn Password

Define the password needed for accessing the TURN server.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 128)

A valid password.

SIP Type

Enables SIP extensions and special behavior for a vendor or provider.

Requires user role: ADMIN

Default value: Standard

Value space: Standard/Cisco

Standard: Use this when registering to standard SIP Proxy (tested with Cisco TelePresence VCS).

Cisco: Use this when registering to Cisco Unified Communication Manager.

SIP URI

The SIP URI (Uniform Resource Identifier) is the address that is used to identify the video system. The URI is registered and used by the SIP services to route inbound calls to the system. The SIP URI syntax is defined in RFC 3261.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

An address (URI) that is compliant with the SIP URI syntax.

Standby settings

Standby Control

Define whether the system should go into standby mode or not.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: The system will not enter standby mode.

On: The system will enter standby mode when the Standby Delay has timed out. Requires the Standby Delay to be set to an appropriate value.

Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. Requires the Standby Control to be enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: 10

Value space: Integer (1..480)

Set the standby delay (minutes).

Standby BootAction

Define the camera position after a restart of the codec.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: RestoreCameraPosition

Value space: None/DefaultCameraPosition/RestoreCameraPosition

None: No action.

RestoreCameraPosition: When the video system restarts, the camera returns to the position that it had before the restart.

DefaultCameraPosition: When the video system restarts, the camera moves to the factory default position.

Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN, INTEGRATOR

Default value: PrivacyPosition

Value space: None/PrivacyPosition

None: No action.

PrivacyPosition: When the video system enters standby, the camera turns to a sideways position for privacy.

Standby WakeupAction

Define the camera position when leaving standby mode.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: RestoreCameraPosition

Value space: None/RestoreCameraPosition/DefaultCameraPosition

None: No action.

RestoreCameraPosition: When the video system leaves standby, the camera returns to the position that it had before entering standby.

DefaultCameraPosition: When the video system leaves standby, the camera moves to the factory default position.

Standby WakeupOnMotionDetection

Automatic wake up on motion detection is a feature that will sense when a person walks into the room. The feature is based on ultrasound detection, and the Proximity Mode setting must be On to make the feature work.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: The wake up on motion detection is disabled.

On: Not applicable in this version.

SystemUnit settings

SystemUnit Name

Define the system name. The system name will be sent as the hostname in a DHCP request and when the codec is acting as an SNMP Agent.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 50)

Define the system name.

SystemUnit CrashReporting Advanced

If the video system (codec) crashes, the system can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The ACR tool will perform standard log analyses.

On: The ACR tool will perform advanced log analyses.

SystemUnit CrashReporting Mode

If the video system (codec) crashes, the system can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: No logs will be sent to ACR tool.

On: The logs will automatically be sent to ACR tool.

SystemUnit CrashReporting Url

If the video system (codec) crashes, the system can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

The URL to the Cisco Automatic Crash Report tool (ACR).

Time settings

Time TimeFormat

Define the time format.

Requires user role: ADMIN, USER
Default value: 24H

Value space: 24H/12H
24H: Set the time format to 24 hours.
12H: Set the time format to 12 hours (AM/PM).

Time DateFormat

Define the date format.

Requires user role: ADMIN, USER
Default value: DD_MM_YY

Value space: DD_MM_YY/MM_DD_YY/YY_MM_DD
DD_MM_YY: The date January 30th 2010 will be displayed: 30.01.10
MM_DD_YY: The date January 30th 2010 will be displayed: 01.30.10
YY_MM_DD: The date January 30th 2010 will be displayed: 10.01.30

Time Zone

Define the time zone for the geographical location of the video system. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Etc/UTC

Value space: Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Ensenada, America/Fort_Nelson, America/Fort_Wayne, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox_IN, America/Kralendijk, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Lower_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Beulah, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/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/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Pacific-New, US/Samoa, UTC, Universal, W-SU, WET, Zulu

Select a time zone from the list.

UserInterface settings

UserInterface Accessibility IncomingCallNotification

You can enable an incoming call notification with amplified visuals. The screen and Touch 10 will flash red/white approximately once every second (1.75 Hz) to make it easier for hearing impaired users to notice an incoming call. If the system is already in a call the screen will not flash as this will disturb the on-going call, instead you will get a normal notification on screen and touch panel.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Default

Value space: AmplifiedVisuals/Default

AmplifiedVisuals: Enable the amplified visuals on screen and touch panel when the video system receives a call.

Default: Enable the default behavior with a notification on screen and touch panel.

UserInterface ContactInfo Type

Choose which type of contact information to show in the status field in the upper left corner of the display and Touch controller.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/None/IPv4/IPv6/SipUri/SystemName/DisplayName

Auto: Show the address which another system can dial to reach this system. The address depends on the system registration.

None: Do not show any contact information.

IPv4: Show the system's IPv4 address.

IPv6: Show the system's IPv6 address.

SipUri: Show the system's SIP URI (refer to the SIP URI setting).

SystemName: Show the system's name (refer to the SystemUnit Name setting).

DisplayName: Show the system's display name (refer to the SIP DisplayName setting).

UserInterface CustomMessage

A custom message can be displayed, in the lower left side of the screen, in awake mode.

Requires user role: ADMIN, INTEGRATOR

Default value: " "

Value space: String (0, 128)

Add a custom message. Add an empty string to remove a custom message.

UserInterface KeyTones Mode

You can configure the system to make a keyboard click sound effect (key tone) when pressing a key on the remote control, or when typing text or numbers on the Touch controller.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: There is no key tone sound effect.

On: The key tone sound effect is turned on.

UserInterface Language

Select the language to be used in the user interface. If the language is not supported, the default language (English) will be used.

Requires user role: ADMIN, USER

Default value: English

Value space: 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

Select a language from the list.

UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator is shown on screen. The icon for encrypted calls is a locked padlock.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/AlwaysOn/AlwaysOff

Auto: If the call is encrypted, a "Call is encrypted" notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

If the call is not encrypted, a "Call is not encrypted" notification is shown for 5 seconds. No encryption indicator icon is shown.

AlwaysOn: The “Call is encrypted” notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

AlwaysOff: The encryption indicator is never displayed on screen.

UserInterface OSD HalfwakeMessage

A custom message can be displayed in the middle of the main screen when the system is in the half wake state. The custom message will replace the default message, which gives instructions how to start using the video system. You can also delete the default message, without adding a custom message.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 128)

The custom message. An empty string: Restore the default message. A space only: There will be no message at all.

UserInterface OSD Output

Define on which monitor on-screen information and indicators (OSD) should be displayed. If the video system is controlled with a remote control also the on-screen menus appear on this monitor.

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: 1

1: The system sends the on-screen information to the connected monitor.

UserInterface Security Mode

This setting allows you to prevent important system information from being exposed in the user interface (drop down menu and Settings panel), for example the contact information and IP addresses of the video system, touch controller, and UCM/VCS registrars. It is important to note that such information is not hidden when navigating further into the Settings panel.

If you want to fully prevent that people without administrator rights can see the contact information, IP addresses, MAC address, serial number, and software version, you must also set the UserInterface SettingsMenu Mode to Locked, and of course have a passphrase for all user accounts with administrator rights.

Requires user role: ADMIN

Default value: Normal

Value space: Normal/Strong

Normal: IP addresses and other system information are shown on the user interface.

Strong: Contact information and IP addresses are not displayed on the user interface (drop down menu and Settings panel).

UserInterface SettingsMenu Mode

The Settings panel in the user interface (Touch 10 or on-screen) can be protected by the video system's admin password. If this password is blank, anyone can access the settings in the Settings menu, and for example factory reset the system. If authentication is enabled, all settings that require authentication have a padlock icon. You will be prompted to enter the administrator's user name and passphrase when you select the setting. Some settings do not require authentication, they do not have a padlock icon.

Requires user role: ADMIN

Default value: Unlocked

Value space: Locked/Unlocked

Locked: Authentication with administrator's username and passphrase is required.

Unlocked: No authentication is required.

UserInterface Wallpaper

Select a background image (wallpaper) for the video screen when idle.

You may upload a custom wallpaper to the video system using the web interface. The following file formats are supported: BMP, GIF, JPEG, PNG. The maximum file size is 4 MByte. When you use a custom wallpaper, the clock and the list of upcoming meetings are removed from the main display

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Auto

Value space: Auto/Custom/None

Auto: Use the default wallpaper.

None: There is no background image on the screen.

Custom: Use the custom wallpaper as background image on the screen. If no custom wallpaper is uploaded to the system, the setting will revert to the default value.

UserManagement settings

UserManagement LDAP Mode

The video system supports the use of an LDAP (Lightweight Directory Access Protocol) server as a central place to store and validate user names and passwords. Use this setting to configure whether or not to use LDAP authentication. Our implementation is tested for the Microsoft Active Directory (AD) service.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: LDAP authentication is not allowed.

On: For client certificate verification to work when LDAP authentication is enabled, the codec requires a CA (Certificate Authority) certificate, and the user must have a Client Certificate that matches their user distinguishing name (DN) in the active directory (AD).

UserManagement LDAP Server Address

Set the IP address or hostname of the LDAP server.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

A valid IPv4 address, IPv6 address or hostname.

UserManagement LDAP Server Port

Set the port to connect to the LDAP server on. If set to 0, use the default for the selected protocol (see the UserManagement LDAP Encryption setting).

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..65535)

The LDAP server port number.

UserManagement LDAP Encryption

Define how to secure the communication between the video system and the LDAP server. You can override the port number by using the UserManagement LDAP Server Port setting.

Requires user role: ADMIN

Default value: LDAPS

Value space: LDAPS/None/STARTTLS

LDAPS: Connect to the LDAP server on port 636 over TLS (Transport Layer Security).

None: Connect to LDAP server on port 389 with no encryption.

STARTTLS: Connect to LDAP server on port 389, then send STARTTLS to enable TLS encryption.

UserManagement LDAP MinimumTLSVersion

Set the lowest version of the TLS (Transport Layer Security) protocol that is allowed.

Requires user role: ADMIN

Default value: TLSv1.2

Value space: TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0: Support TLS version 1.0 or higher.

TLSv1.1: Support TLS version 1.1 or higher.

TLSv1.2: Support TLS version 1.2 or higher.

UserManagement LDAP VerifyServerCertificate

When the video system connects to an LDAP server, the server will identify itself to the video system by presenting its certificate. Use this setting to determine whether or not the video system will verify the server certificate.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The video system will not verify the LDAP server's certificate.

On: The video system must verify that the LDAP server's certificate is signed by a trusted Certificate Authority (CA). The CA must be on the list of trusted CAs that are uploaded to the system in advance. Use the video system's web interface to manage the list of trusted CAs (see more details in the administrator guide).

UserManagement LDAP Admin Filter

The LDAP filter is used to determine which users should be granted administrator privileges. If set, this setting takes precedence over the UserManagement LDAP Admin Group setting.

Requires user role: ADMIN

Default value: " "

Value space: String (0, 1024)

Refer to the LDAP specification for the syntax of this string. Example: " (CN=adminuser)"

UserManagement LDAP Admin Group

Members of this AD (Active Directory) group will be given administrator access. This setting is a shorthand for saying (memberOf:1.2.840.113556.1.4.1941:=<group name>). If UserManagement LDAP Admin Filter is set, this setting is ignored.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

The distinguished name of the AD group. Example: " CN=admin_group, OU=company groups, DC=company, DC=com"

UserManagement LDAP Attribute

The attribute used to map to the provided username. If not set, sAMAccountName is used.

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

The attribute name.

UserManagement LDAP BaseDN

The distinguishing name of the entry at which to start a search (base).

Requires user role: ADMIN

Default value: " "

Value space: String (0..255)

The distinguishing name of the base. Example: " DC=company, DC=com"

Video settings

Video ActiveSpeaker DefaultPIPPosition

Define the position on screen of the active speaker picture-in-picture (PiP). The setting only takes effect when using a video layout where the active speaker is a PiP, i.e. the Overlay layout, or possibly a Custom layout (refer to the Video DefaultLayoutFamily Local setting). The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the active speaker PiP will be kept unchanged when leaving a call.

UpperLeft: The active speaker PiP will appear in the upper left corner of the screen.

UpperCenter: The active speaker PiP will appear in the upper center position.

UpperRight: The active speaker PiP will appear in the upper right corner of the screen.

CenterLeft: The active speaker PiP will appear in the center left position.

CentreRight: The active speaker PiP will appear in the center right position.

LowerLeft: The active speaker PiP will appear in the lower left corner of the screen.

LowerRight: The active speaker PiP will appear in the lower right corner of the screen.

Video DefaultLayoutFamily Local

Select which video layout family to use locally.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single

Auto: The default layout family, as given in the layout database provided by the system, will be used as the local layout.

Equal: The Equal layout family will be used as the local layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the local layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the local layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

Video DefaultLayoutFamily Remote

Select which video layout family to be used for the remote participants.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single

Auto: The default layout family, as given by the local layout database, will be used as the remote layout.

Equal: The Equal layout family will be used as the remote layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the remote layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the remote layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

Video DefaultMainSource

Define which video input source to be used as the default main video source when you start a call.

Requires user role: ADMIN, USER

Default value: 1

Value space: 1

Set the source to be used as the default main video source.

Video Input Connector [1..3] CameraControl Mode

Define whether the camera that is connected to this video input connector can be controlled or not.

Note that camera control is not available for Connector 2 (HDMI) and Connector 3 (VGA).

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: On Connector 2,3: Off

Value space: Connector 1: Off/On Connector 2,3: Off

Off: Disable camera control.

On: Enable camera control.

Video Input Connector [1..3] CameraControl CameraId

The camera ID is a unique identifier of the cameras that are connected to the video input.

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: 1

The camera ID is fixed and cannot be changed.

Video Input Connector [1..3] InputSourceType

Select which type of input source is connected to the video input.

Note that Connector 1 is the system's integrated camera.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: camera Other connectors: PC

Value space: Connector 1: camera Other connectors: PC/camera/document_camera/mediaplayer/whiteboard/other

PC: Use this when a computer is connected to the video input.

camera: Use this when a camera is connected to the video input.

document_camera: Use this when a document camera is connected to the video input.

mediaplayer: Use this when a media player is connected to the video input.

whiteboard: Use this when a whiteboard camera is connected to the video input.

other: Use this when the other options do not match.

Video Input Connector [1..3] Name

Define a name for the video input connector.

Requires user role: ADMIN, INTEGRATOR

Default value: " "

Value space: String (0, 50)

Name for the video input connector.

Video Input Connector [1..3] OptimalDefinition Profile

This setting will not take effect if the corresponding Video Input Connector [n] Quality setting is set to Sharpness.

The optimal definition profile reflects the lighting conditions in the video conferencing room and the quality of the camera. The better lighting conditions and the better quality of the camera, the higher the profile. Generally, the Normal or Medium profiles are recommended. However, when the lighting conditions are very good, the High profile can be set in order to increase the resolution for a given call rate. The resolution must be supported by both the calling and called systems.

Requires user role: ADMIN, INTEGRATOR

Default value: Medium

Value space: Normal/Medium/High

Normal: Use this profile for a normally to poorly lit environment. Resolutions will be set rather conservative.

Medium: Requires good and stable lighting conditions and a good quality video input. For some call rates this leads to higher resolution.

High: Requires nearly optimal video conferencing lighting conditions and a good quality video input in order to achieve a good overall experience. Rather high resolutions will be used.

Video Input Connector [2..3] PresentationSelection

Define how the video system will behave when you connect a presentation source to the video input.

If the video system is in standby mode, it will wake up when you connect a presentation source. Sharing the presentation with the far end requires additional action (select Share on the user interface) except when this setting is set to AutoShare.

Requires user role: ADMIN, INTEGRATOR

Default value: OnConnect

Value space: AutoShare/Desktop/Manual/OnConnect

AutoShare: While in a call, the content on the video input will automatically be presented to the far end as well as on the local screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). You do not have to select Share on the user interface. If a presentation source is already connected when you make or answer a call, you have to manually select Share on the user interface.

Desktop: The content on the video input will be presented on the screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). This applies both when idle and in a call. Also, the content on the video input will stay on the screen when you leave the call, provided that it was the active input at the time of leaving.

Manual: The content on the video input will not be presented on the screen until you select Share from the user interface.

OnConnect: The content on the video input will be presented on screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). Otherwise, the behavior is the same as in manual mode.

Video Input Connector [2..3] Quality

When encoding and transmitting video there is a trade-off between high resolution and high frame rate. For some video sources it is more important to transmit high frame rate than high resolution and vice versa. This setting specifies whether to give priority to high frame rate or to high resolution.

Requires user role: ADMIN, INTEGRATOR

Default value: Sharpness

Value space: Motion/Sharpness

Motion: Gives the highest possible frame rate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.

Sharpness: Gives the highest possible resolution. Used when you want the highest quality of detailed images and graphics.

Video Input Connector [2..2] RGBQuantizationRange

The devices connected to the video input should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any source.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on video format according to CEA-861-E. CE video formats will use limited quantization range levels. IT video formats will use full quantization range levels.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

Video Input Connector [1..3] Visibility

Define the visibility of the video input connector in the menus on the user interface.

Note that Connector 1 is the system's integrated camera, which is not available as a presentation source.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Never Connector 2: Always Connector 3: OnConnect

Value space: Connector 1: Never Connector 2, 3: Always/IfSignal/Never

Always: The menu selection for the video input connector will always be visible on the user interface.

IfSignal: Yhe menu selection for the video input connector will only be visible when something is connected to the video input.

Never: The input source is not expected to be used as a presentation source, and will not show up on the user interface.

Video Monitors

Define the monitor layout mode. Note that this video system supports only one screen, so this value is fixed and cannot be changed.

Requires user role: ADMIN, INTEGRATOR

Default value: Single

Value space: Single

Single: The layout is shown on the video system's screen.

Video Output Connector [1..1] CEC Mode

This video output (HDMI) supports Consumer Electronics Control (CEC).

When this setting is On, the system will use CEC to set the screen in standby when the system itself enters standby. Likewise the system will wake up the screen when the system itself wakes up from standby.

Note that the different manufacturers uses different marketing names for CEC, for example Anynet+ (Samsung); Aquos Link (Sharp); BRAVIA Sync (Sony); HDMI-CEC (Hitachi); Kuro Link (Pioneer); CE-Link and Regza Link (Toshiba); RIHD (Onkyo); HDAVI Control, EZ-Sync, VIERA Link (Panasonic); EasyLink (Philips); and NetCommand for HDMI (Mitsubishi).

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: CEC is disabled.

On: CEC is enabled.

Video Output Connector [1..1] OverscanLevel

Some monitors may not present the entire image that they receive. This means that the outer parts of the image that is sent from the video system may be cut off when displayed on the monitor.

Use this setting to instruct the video system not to use the outer part of the available frame. This part might be cut off by the monitor. Both the video and messages on screen will be scaled in this case.

Requires user role: ADMIN

Default value: None

Value space: None/Medium/High

None: The video system will use all of the output resolution.

Medium: The video system will not use the outer 3% of the output resolution.

High: The video system will not use the outer 6% of the output resolution.

Video Output Connector [1..1] Resolution

Define the resolution and refresh rate for the connected screen. This value is fixed and cannot be changed.

Default value: Connector n: Auto

Value space: Auto

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.

Video Output Connector [1..1] RGBQuantizationRange

Devices connected to an HDMI output should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any display. Most HDMI displays expects full quantization range.

Requires user role: ADMIN, INTEGRATOR

Default value: Full

Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on the RGB Quantization Range bits (Q0, Q1) in the AVI infoframe. If no AVI infoframe is available, RGB quantization range is selected based on video format according to CEA-861-E.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

Video Presentation DefaultPIPPosition

Define the position on screen of the presentation picture-in-picture (PiP). The setting only takes effect when the presentation is explicitly minimized to a PiP, for example using the user interface. The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the presentation PiP will be kept unchanged when leaving a call.

UpperLeft: The presentation PiP will appear in the upper left corner of the screen.

UpperCenter: The presentation PiP will appear in the upper center position.

UpperRight: The presentation PiP will appear in the upper right corner of the screen.

CenterLeft: The presentation PiP will appear in the center left position.

CenterRight: The presentation PiP will appear in the center right position.

LowerLeft: The presentation PiP will appear in the lower left corner of the screen.

LowerRight: The presentation PiP will appear in the lower right corner of the screen.

Video Presentation DefaultSource

Define which video input source to use as a default presentation source. This setting may be used by the API and 3rd party user interfaces. It is not relevant when using the user interfaces provided by Cisco.

Requires user role: ADMIN, USER

Default value: 2

Value space: 2

The video input source to use as default presentation source.

Video Selfview Default Mode

Define if the main video source (self-view) shall be displayed on screen after a call. The position and size of the self-view window is determined by the Video Selfview Default PIPPosition and the Video Selfview Default FullscreenMode settings respectively.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Off/Current/On

Off: Self-view is switched off when leaving a call.

Current: Self-view is left as is, i.e. if it was on during the call, it remains on after the call; if it was off during the call, it remains off after the call.

On: Self-view is switched on when leaving a call.

Video Selfview Default FullscreenMode

Define if the main video source (self-view) shall be shown in full screen or as a small picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting).

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Off/Current/On

Off: Self-view will be shown as a PiP.

Current: The size of the self-view picture will be kept unchanged when leaving a call, i.e. if it was a PiP during the call, it remains a PiP after the call; if it was fullscreen during the call, it remains fullscreen after the call.

On: The self-view picture will be shown in fullscreen.

Video Selfview Default PIPPosition

Define the position on screen of the small self-view picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting) and fullscreen view is switched off (see the Video Selfview Default FullscreenMode setting).

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the self-view PiP will be kept unchanged when leaving a call.

UpperLeft: The self-view PiP will appear in the upper left corner of the screen.

UpperCenter: The self-view PiP will appear in the upper center position.

UpperRight: The self-view PiP will appear in the upper right corner of the screen.

CenterLeft: The self-view PiP will appear in the center left position.

CentreRight: The self-view PiP will appear in the center right position.

LowerLeft: The self-view PiP will appear in the lower left corner of the screen.

LowerRight: The self-view PiP will appear in the lower right corner of the screen.

Video Selfview OnCall Mode

This setting is used to switch on self-view for a short while when setting up a call. The Video Selfview OnCall Duration setting determines for how long it remains on. This applies when self-view in general is switched off.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Self-view is not shown automatically during call setup.

On: Self-view is shown automatically during call setup.

Video Selfview OnCall Duration

This setting only has an effect when the Video Selfview OnCall Mode setting is switched On. In this case, the number of seconds set here determines for how long self-view is shown before it is automatically switched off.

Requires user role: ADMIN, INTEGRATOR

Default value: 10

Value space: Integer (1..60)

Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.

Experimental settings

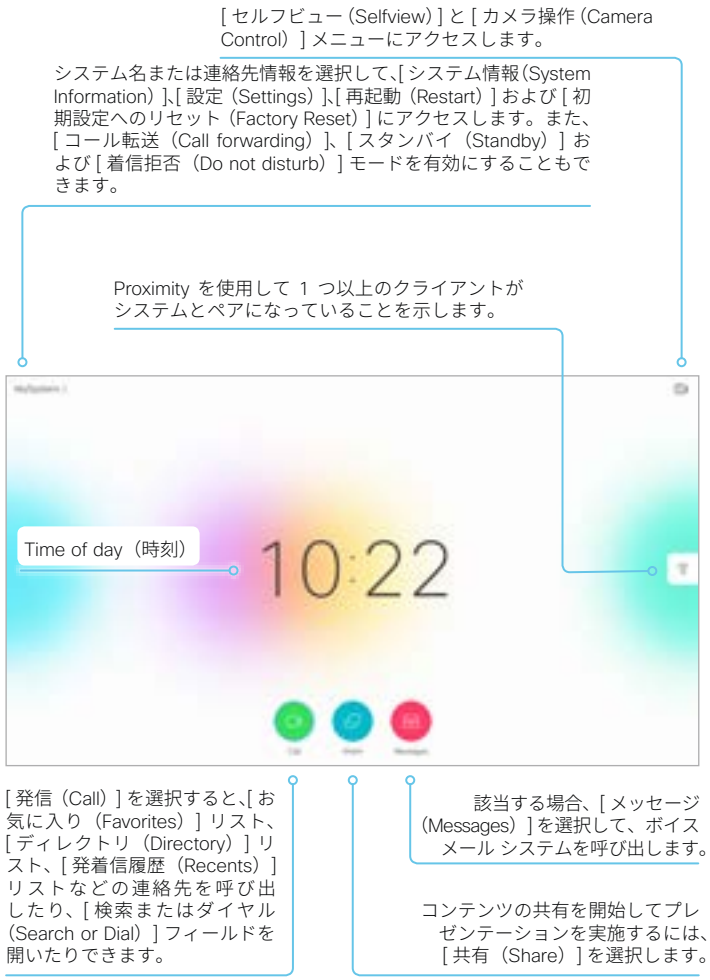
The Experimental settings are for testing only and should not be used unless agreed with Cisco. These settings are not documented and WILL change in later releases.

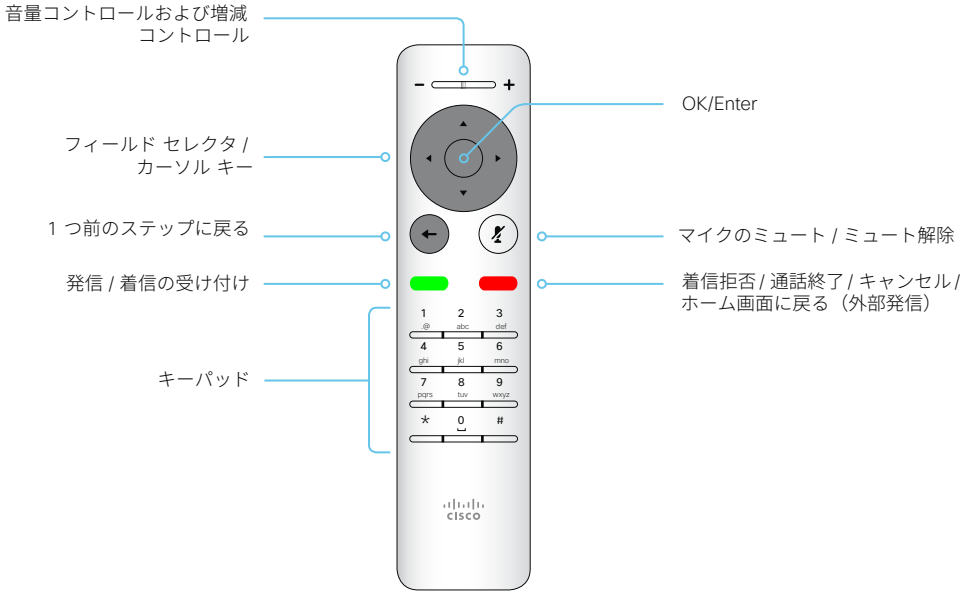
付録

リモート コントロールと画面上のユーザ インターフェイスの使用方法

TRC6 リモート コントロールを使用してビデオ システムを操作する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。

TRC5 リモート コントロールはサポートされません。





TRC6 リモコン

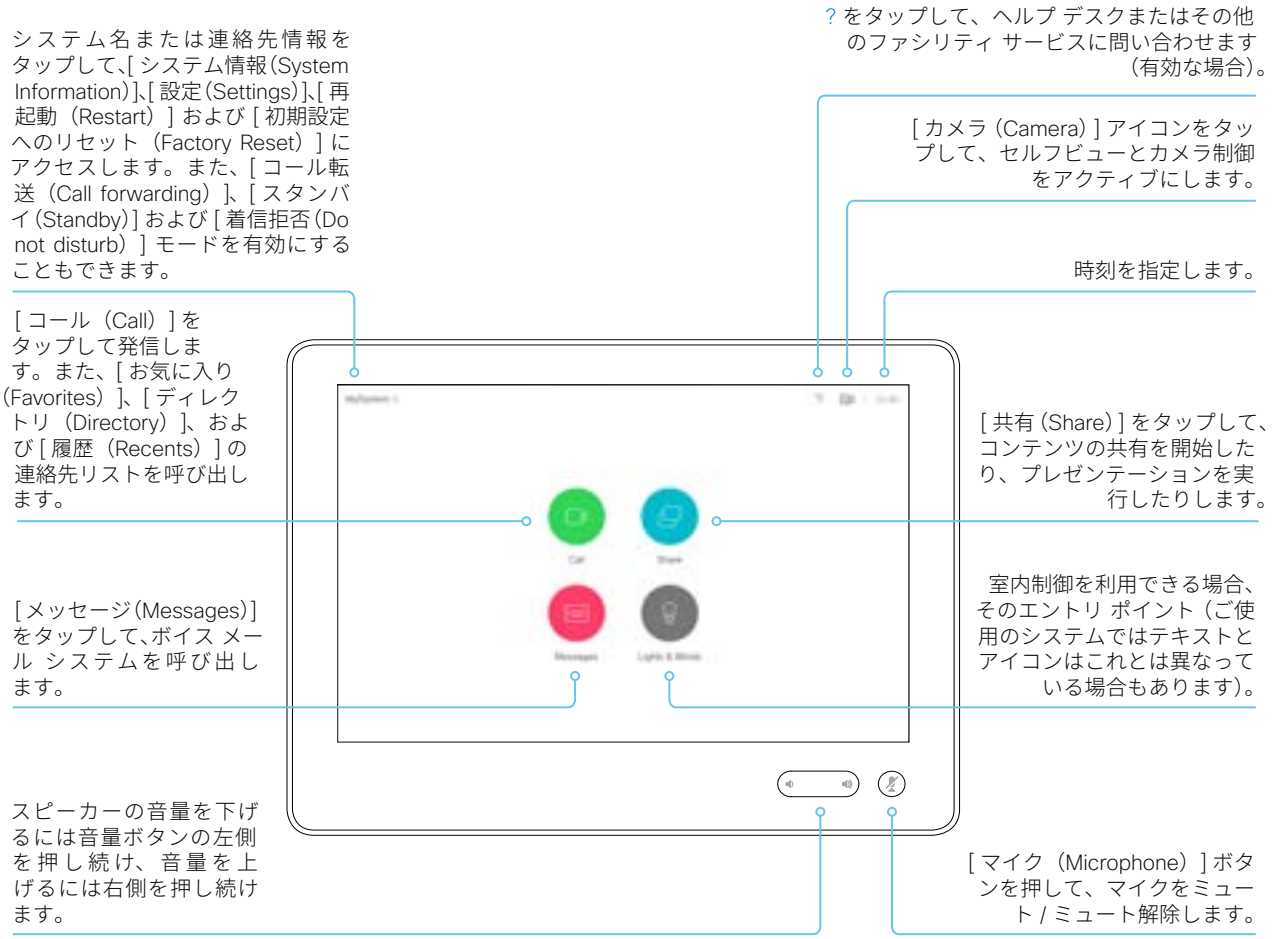
操作のヒント

画面の中を移動するには、方向キーを使用します。**OK/Enter** キーを押し、選択したメニュー フィールドを開きます。

キャンセル キーを使用してメニューを終了し (ホーム画面に戻ります)、変更内容を取り消します。戻るキーを使用して 1 つ前のステップに戻ります。

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。



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役立ちます。

入力ソースからのスナップショットが Web インターフェイスに表示されるため、部屋にいなくても、カメラ ビューを確認したり、カメラを制御したりできます。

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。

ビデオ システムに RemoteMonitoring オプションがあるかどうかの確認

1. Web インターフェイスにサインインします。
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 モニタリングの有効化

RemoteMonitoring オプション キーをインストールします。オプション キーのインストール方法については、▶「オプション キーの追加」の章で説明しています。

リモート モニタリング オプションを有効にする場合は、プライバシーに関する地域の法律および規制を遵守する必要があります。また、システム管理者がカメラや画面を監視および制御する場合があることを、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

ローカル入力ソース

ビデオ システムのローカル入力ソースのスナップショットが [コール制御（Call Control）] ページに表示されます。

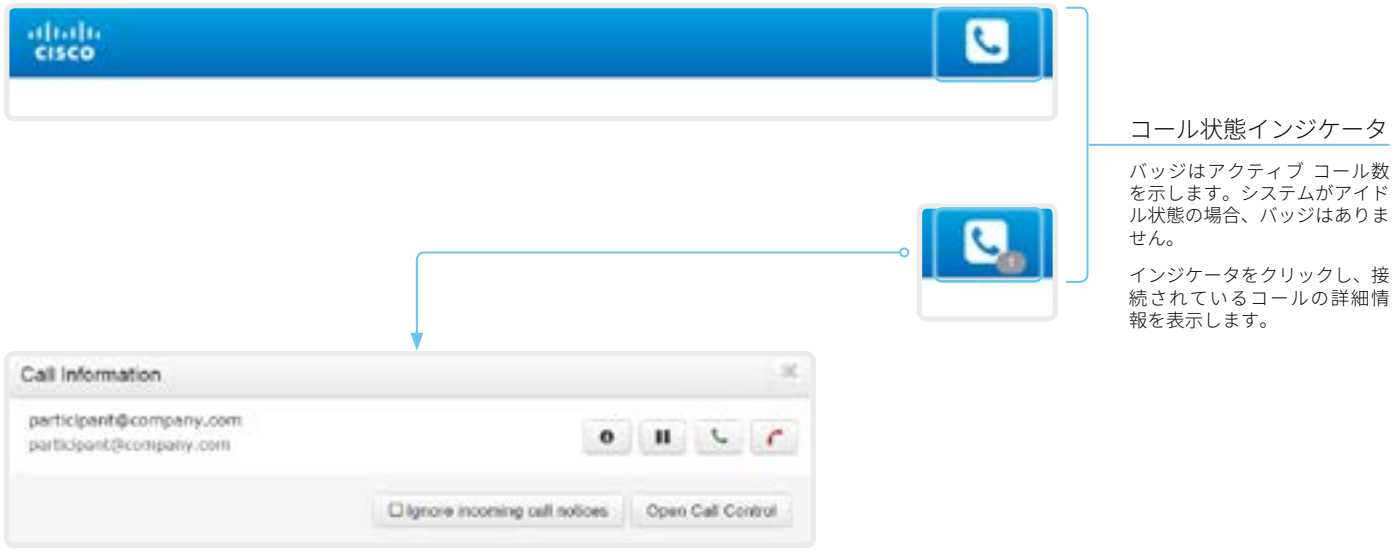
スナップショットは、ビデオ システムがアイドル中でも通話中でも表示されます。

遠端のスナップショット

通話中に、遠端カメラからのスナップショットを表示することもできます。この場合、遠端ビデオ システムに RemoteMonitoring オプションがあるかどうかは関係ありません。

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



コール状態インジケータ

バッジはアクティブ コール数を示します。システムがアイドル状態の場合、バッジはありません。

インジケータをクリックし、接続されているコールの詳細情報を表示します。

[コール情報（Call Information）] ウィンドウの表示

[コール情報（Call Information）] ウィンドウを手動で開くには、コール状態インジケータをクリックします。

デフォルトでは、ビデオ システムがコールを受信すると [コール情報（Call Information）] ウィンドウが自動的に表示されます。

着信コール通知のオン / オフの切り替え

[着信コール通知を無視する（Ignore incoming call notices）] をクリックすると、ビデオ システムがコールを受信したときに [コール情報（Call Information）] ウィンドウを自動的に表示するかどうかを決定できます。

このチェックボックスをオンにした場合は、[コール情報（Call Information）] ウィンドウが自動的に開きません。

[コール制御（Call Control）] ページの表示

[コール制御（Call Control）] ページに直接移動するには、[コール制御を開く（Open Call Control）] をクリックします。

コールの制御

関連する制御ボタンが [コール情報（Call Information）] ウィンドウに表示されます。ボタンの用途は次のとおりです。

- コールの詳細を表示する
- コールを保留にする
- コールに応答する
- コールを切断する

コール状態インジケータについて

コール状態インジケータは、システムが通話中であるかどうかを示します。着信コールについてユーザに通知することもできます。

コール状態インジケータは [コール制御（Call Control）] ページ以外のすべてのページで使用できます。

Web インターフェイスを使用したコールの発信 (1/2 ページ)

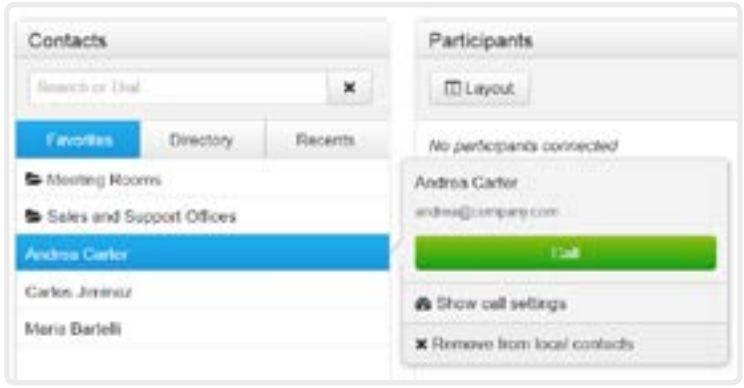
Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。

コールの発信

Web インターフェイスを使ってコールを開始した場合でも、コールに使用されるのはビデオ 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. [お気に入り (Favorites)]、[ディレクトリ (Directory)]、または [履歴 (Recents)] リストに移動して該当するエントリを探すか、[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 (information button)] 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、その参加者の名前の横にある ⏸ ボタンを使用します。

コールを再開するには、保留中の参加者に表示される ▶ ボタンを使用します。

コールの終了

コールを終了するには、[全通話切断 (Disconnect all)] または ⏹ ボタンをクリックします。

Web インターフェイスを使用したコールの発信 (2/2 ページ)

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

複数の相手に発信

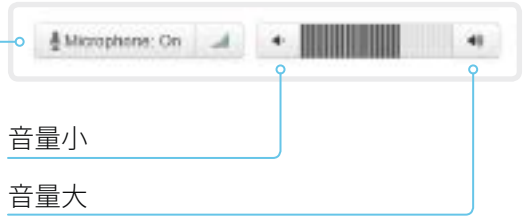
会議ブリッジを使用した複数のコール（CUCM のアドホック会議）は、ビデオ システムでサポートされていても Web インターフェイスではサポートされません。

音量の調整

マイクのミュート

[マイク：オン（Microphone: On）] をクリックすると、マイクがミュートになります。すると、テキストが [マイク：オフ（Microphone: Off）] に変わります。

ミュートを解除するには、[マイク：オフ（Microphone: Off）] をクリックします。



Web インターフェイスを使用したコンテンツの共有

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

コンテンツを共有する

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。これにより、テキストが [プレゼンテーションを中止（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

このドロップダウン 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

選択し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

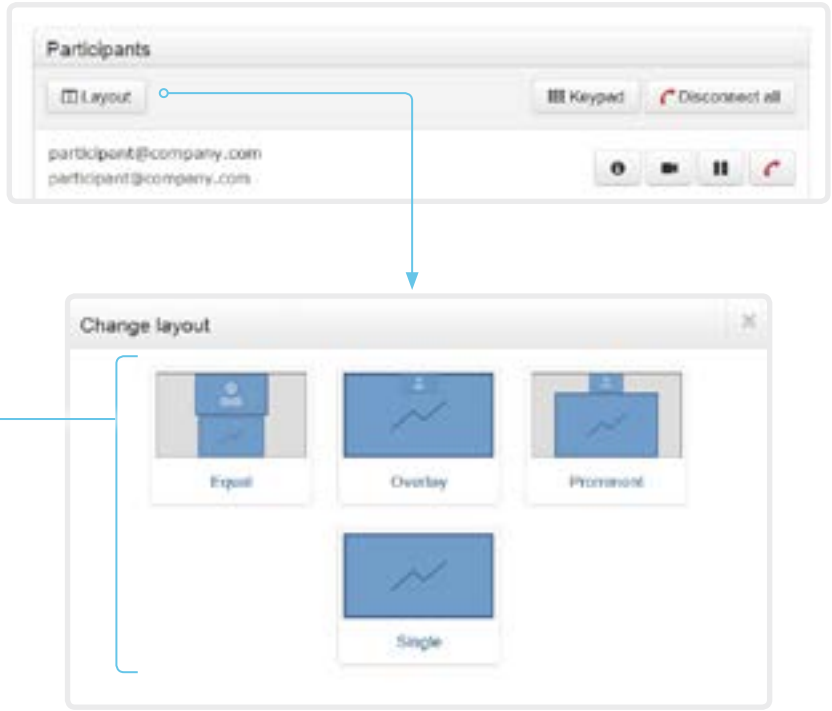
ビデオ システムのビデオ入力の 1 つに プレゼンテーション ソースを接続できます。プレゼンテーション ソースとして最も多く使用されるのは PC ですが、システムの設定によってはその他のオプションを使用できる場合があります。

コールの間、コールの他の参加者（遠端）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サインインして、[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。

ローカル カメラの制御

Web インターフェイスにサインインして、[コール制御（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）] > [カメラ操作（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。

スナップショットの自動更新

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

1. 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。

   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。

   ウィンドウには、該当するコントロールのみが表示されます。

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して、カメラをプリセット位置に移動します。

3. [OK] 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。

相手先カメラの制御

Web インターフェイスにサインインして、[コール制御（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 ソフトウェアを実行す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ですべてのパケット損失回復メカニズム（ホスト型会議を含む）が使用されます。

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（1/2 ページ）

ユーザ インターフェイスは、会議室にある周辺機器（たとえば、照明やブラインド）を制御できるようにカスタマイズできます。

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

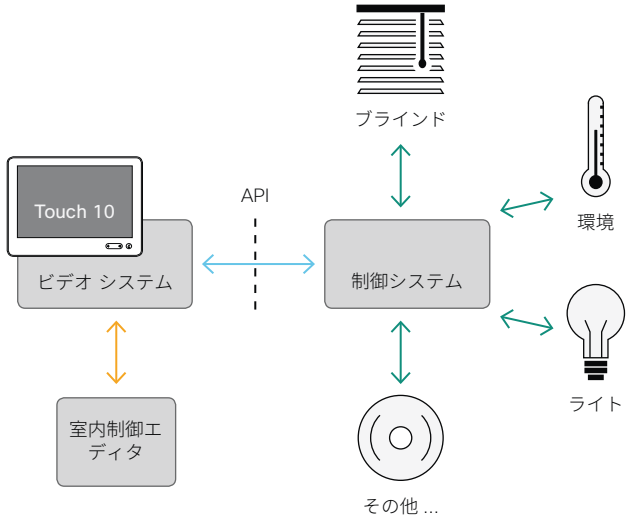
室内制御エディタを使用してカスタム ユーザ インターフェイス パネル（室内制御パネル）を設計する方法、およびビデオ システムの API を使用して室内制御をプログラミングする方法の詳細については、『CE カスタマイズ ガイド』[英語] を参照してください。次のリンクにアクセスします。

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

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もあります。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 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。

スタートアップ スクリプトの管理

Web インターフェイスにサインインして、[統合（Integration）] > [スタートアップ スクリプト（Startup Scripts）] に移動します。

図に示しているスクリプト名とコンフィギュレーションは一例です。独自のスクリプトを作成できます。

スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます*。

アクティブなスタートアップ スクリプトの横には緑色のドットが表示され、非アクティブ スタートアップ スクリプトの横には赤色のリングが表示されます。

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 スクリプトの作成

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. コマンド入力領域に、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）] をクリックすると、スタートアップ スクリプトがアクティブになります。

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。

スタートアップ スクリプトの即時実行

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 スタートアップ スクリプトと非アクティブ スタートアップ スクリプトの両方を、即時に実行できます。

スタートアップ スクリプトのアクティブ化または非アクティブ化

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. [オン（On）] をクリックしてスクリプトをアクティブにするか、[オフ（Off）] をクリックしてスクリプトを非アクティブにします。

   アクティブ 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実行されます。

スタートアップ スクリプトの削除

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。不正なコマンドやコンフィギュレーションが含まれる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 ファイルへのアクセス

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）] に移動します。

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

ファイル名をクリックして、XML ファイルを開きます。

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 コマンドと構成の実行

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）] に移動します。

コマンド (xCommand) とコンフィギュレーション (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。

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。

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。コンピュータによりシリアル ポート ドライバが自動インストールされない場合には、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有効になっています。動作を変更するには、次の設定を使用します。

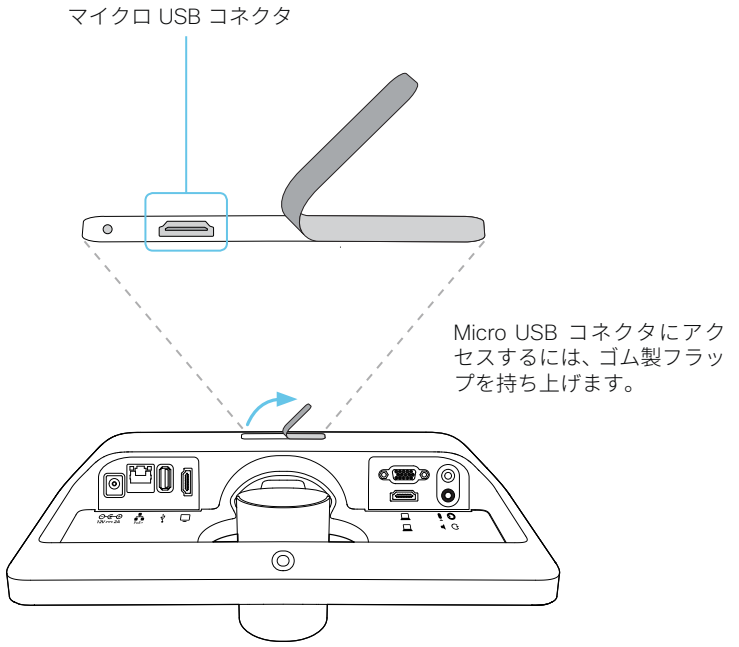
[シリアルポート（SerialPort）] > [モード（Mode）]

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 からプロビジョニングされている場合、シリアル ポートの設定を CUCM から設定する必要があります。



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。

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。

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 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 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 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。

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

- Cisco TelePresence ソフトウェア バージョン TC7.1 以降
- コラボレーション エンドポイント ソフトウェア バージョン 8.0 以降

製品の同梱物 :

- HD カメラとマイクを備えた SX10 コーデック
- 壁面取り付け
- TRC6 リモコン
- ネットワーク ケーブルおよび HDMI ケーブル

統合型の HD カメラ

- 合計のズーム 5x
- +5° /-25° チルト、± 30° パン
- 垂直視野角 51.5°
- 水平視野角 83°
- F 値 2.1 以上
- 1920 X 1080 ピクセル プログレッシブ @ 30 fps
- 自動または手動フォーカス、輝度およびホワイト バランス
- 上下が反対になったときに画像を自動反転

ユーザ インターフェイス

- TRC6 リモコンおよび画面に表示されるグラフィカル ユーザ インターフェイス
- Cisco TelePresence Touch 10（オプション）

言語のサポート [げんごのさぽーと]

(ソフトウェア バージョンによって異なります)

- アラビア語、カタロニア語、中国語（繁体字）、中国語（簡体字）、チェコ語、デンマーク語、オランダ語、英語、英国英語、フィンランド語、フランス語、カナダ フランス語、ドイツ語、ヘブライ語、ハンガリー語、イタリア語、日本語、韓国語、ノルウェー語、ポーランド語、ブラジル ポルトガル語、ロシア語、スペイン語、ラテン スペイン語、スウェーデン語、トルコ語

システム管理

- 埋め込み Telnet、SSH、XML、および SOAP によるトータル管理
- Web サーバ、SCP、HTTP、および HTTPS を使用したリモート ソフトウェアのアップロード
- リモート コントロールと画面メニューのシステム

ディレクトリ サービス

- ローカル ディレクトリ（お気に入り）のサポート
- 社内ディレクトリ（Cisco Unified Communications Manager リリース および Cisco TelePresence Management Suite 利用）
- LDAP および H.350 をサポートするサーバ ディレクトリ（Cisco TelePresence Managment Suite が必要）
- 日時を含む着信、発信、および不在着信のコール履歴

電源

- PoE 対応：37 ～ 57 V、最大 0.35 A
- 電源モジュール
  - **AC 入力：1 A、100-240 V、50-60 Hz**
  - **DC 出力：12 V、最大 2 A**
- 通常の動作で最大 12 W

動作温度および湿度

- 周囲温度：0 ～ 40°C（32 ～ 95°F）
- 相対湿度（RH）：10 ～ 90%

保管および輸送の温度

- RH 10 ～ 90% では -20 ～ 60°（-4 ～ 140°F）（結露しないこと）

SX10 コーデックの寸法

- 幅：27.5 cm（10.8 インチ）
- 高さ：11.7 cm（4.6 インチ）
- 奥行：9.1 cm（3.6 インチ）（下方向の最大カメラ チルトを含む）
- 重量：0.9 kg（2.0 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 B
- 指令 2011/65/EU（RoHS）
- 指令 2002/96/EC（WEEE）
- NRTL 認定（製品の安全性）
- FCC CFR 47 Part 15B（EMC）：クラス B

各国の認定書類については、Product Approval Status Database（製品認定ステータス データベース）www.ciscofax.com を参照してください。

帯域幅

- 最大 3 Mbps

解像度とフレーム レートの最小帯域幅

- 768 kbps から 720p30
- 1472 kbps から 1080p30

ファイアウォール トラバーサル

- Cisco TelePresence Expressway テクノロジー

ビデオ標準

- H.263
- H.263+
- H.264

ビデオ入力

2 つのビデオ入力（ユーザ インターフェイスで HDMI* または VGA を選択可能）。次のような最大の 1280 × 768@30fps までのフォーマットをサポート

- 640 × 480（VGA）
- 720 × 480
- 704 × 576（4CIF）
- 800 × 600（SVGA）
- 848 × 480
- 1024 × 768（VGA）
- 1152 × 864（XGA+）
- 1280 × 720（720p）
- 1280 × 768（WXGA）

Extended Display Identification Data（EDID）

ビデオ出力

HDMI 出力（1 個）* サポート フォーマット：

- 1920 × 1080 @ 60 fps（1080p60）

VESA モニタ電源管理

Extended Display Identification Data（EDID）

* HDMI バージョン 1.3

技術仕様 (2/2 ページ)

ライブ ビデオ解像度（エンコード / デコード）

次のような最大 1920 × 1080@30 fps（HD1080p30）までのエンコードまたはデコード ビデオ フォーマットをサポート：

- 176 × 144 @ 30 fps（QCIF）（デコードのみ）
- 352 × 288 @ 30 fps（CIF）
- 512 × 288 @ 30 fps（w288p）
- 576 × 448 @ 30 fps（448p）
- 640 × 480 @ 30 fps（VGA）
- 704 × 576 @ 30 fps（4CIF）
- 768 × 448 @ 30 fps（w448p）
- 800 × 600 @ 30 fps（SVGA）
- 1024 × 576 @ 30 fps（w576p）
- 1024 × 768 @ 30 fps（XGA）
- 1280 × 720 @ 30 fps（HD720p）
- 1280 × 768 @ 30 fps（WXGA）
- 1920 × 1080 @ 30 fps（HD1080p）

音声標準

- 64 kbps AAC-LD
- OPUS
- G.722
- G.722.1
- G.711mu
- G.711a
- G.729AB
- G.729

音声機能

- ハイクオリティ 20kHz オーディオ
- 音響エコー キャンセラ 2
- オート ゲイン コントロール
- オート ノイズ リダクション
- アクティブ リップ シンク

音声入力

- 内蔵マイク 1
- 外部マイク 1、4 極ミニジャック（Cisco TelePresence Table Microphone 20）
- HDMI 音声 1

音声出力

- 出力回線 1、ミニジャック
- 1 HDMI（デジタル メイン音声）

デュアル ストリーム

- H.239 デュアル ストリーム（H.323）
- BFCP デュアル ストリーム（SIP）
- 15fps で最大 1920 × 1080 の解像度のサポート

マルチポイント サポート

- シスコ アドホック会議（Cisco Unified Communications Manager（CUCM）と、Cisco Meeting Server（CMS）または Cisco TelePresence Server および Cisco TelePresence Conductor が必要）

プロトコル

- SIP および H.323

組み込み暗号化

- SIP および H.323 ポイントツーポイント
- 標準ベース：Advanced Encryption Standard（AES）
- キーの自動生成と交換
- デュアル ストリームでサポート

IP ネットワーク機能

- 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）
- 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
- NTP による日時のサポート
- パケット損失時のダウンスピード機能
- URI ダイヤル
- TCP/IP
- DHCP
- IEEE 802.1x ネットワーク認証
- IEEE 802.1Q 仮想 LAN
- IEEE 802.1p QoS およびサービス クラス
- Cisco ClearPath

IPV6 ネットワークのサポート

- DHCP、SSH、HTTP、HTTPS、DNS、DiffServ に対するデュアル スタックの IPv4 および IPv6
- スタティック IP アドレスの割り当て、ステートレス自動設定および DHCPv6 をサポート

サポートされるインフラストラクチャ

- Cisco Unified Communications Manager 8.6.2 以降
- Cisco TelePresence Video Communication Server（Cisco VCS）

セキュリティ機能

- Web インターフェイス（HTTPS/HTTP）および SSH を使用した管理
- パスワードで保護された IP 管理
- パスワードで保護された管理メニュー
- IP サービスのディセーブル
- ネットワーク設定の保護

ネットワーク インターフェイス

- PoE 対応 LAN コネクタ（RJ-45）10/100 Mbps 1 個（自動ネゴシエーションのみ）

その他のインターフェイス

- 将来的に使用する USB ポート 1 個
- メンテナンス目的の Micro-USB ポート 1 個

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。

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

MX シリーズ：

► https://www.cisco.com/go/mx-docs

SX シリーズ：

► https://www.cisco.com/go/sx-docs

DX シリーズ：

► https://www.cisco.com/go/dx-docs

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

マニュアルは以下のカテゴリに整理されています。一部のマニュアルはすべての製品で利用できません。

インストールとアップグレード > インストールとアップグレード ガイド

- インストレーション ガイド：製品のインストール方法
- スタートアップ ガイド：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
- CUCM での TelePresence エンドポイントの導入ガイド：Cisco Unified Communications Manager（CUCM）でビデオ システムの使用を開始するために実行するタスク
- スペア部品の概要、スペア部品の交換ガイド、ケーブル スキーマ：スペア部品を交換するときに役立つ情報

保守と運用 > エンドユーザ ガイド

- ユーザ ガイド：製品の使用方法
- クイック リファレンス ガイド：製品の使用方法
- 物理インターフェイス ガイド：コネクタのパネルと LED など、コーデックの物理インターフェイスに関する詳細

リファレンス ガイド > コマンド リファレンス

- API リファレンス ガイド：アプリケーション プログラミング インターフェイス（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：寸法付きの 2D CAD 図面

設定 > 設定ガイド

- CE カスタマイズ ガイド：室内制御パネルをデザインする方法と、室内コントロールをプログラミングするためにビデオ システムの API を使用する方法。
- CE Console ユーザ ガイド：ビデオ システムの高度なカスタマイズが可能な機能にグラフィカル インターフェイスを提供する CE コンソール アプリケーションの使用方法

設計 > 設計ガイド

- ビデオ会議室のガイドライン：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：聴き取られる音声の品質を向上させるために行うべきこと

ソフトウェア ダウンロード、リリースと一般情報 > ライセンス情報

- オープン ソースのドキュメント：この製品で使用されているオープン 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 > リリース ノート

- ソフトウェア リリース ノート

シスコのお問い合わせ先

シスコの Web サイトでは、シスコの世界各地のお問い合わせ先を確認できます。

参照先：► https://www.cisco.com/go/offices

本社
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

知的財産権

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. 米国および現地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。