コラボレーション エンドポイント ソフトウェア バージョン 9.5
SEPTEMBER 2018

管理者ガイド

cisco Webex DX70 **および** DX80

シスコ製品をお選びいただきありがとうございます。

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

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

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

定期的にシスコの Web サイトにアクセスし、このガイドの最新版を入手することを推奨します。

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/dx-docs

本ガイドの使用方法

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

目次

はじめに 4
ユーザ ドキュメンテーションとソフトウェア 5
CE9 の最新情報 6
DX70 および DX80 の概要 21
電源のオンとオフ 22
LED インジケータ 23
ビデオ システムの管理方法 (1/4 ページ) 24

設定 28
ユーザ管理 29
システム パスフレーズを変更する 30
[設定(Settings)] メニューへのアクセスの制限 31
システム設定 32
サインイン バナーの追加 33
ウェルカム バナーの追加 34
ビデオ システムのサービス証明書を管理する 35
信頼できる認証局(CA)のリストを管理する 36
セキュア監査ロギングのセットアップ 37
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 38
CUCM 信頼リストを削除する 39
永続モードを変更する 40
強力なセキュリティ モードの設定 41
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) 42
ビデオ品質の対コール レート比調整 47
画面に企業ブランディングを追加 (1/2 ページ) 48
カスタム壁紙の追加 50
着信音の選択と着信音量の設定 51
お気に入りリストの管理 52
アクセシビリティ機能のセットアップ 53

ペリフェラル 54
コンピュータの接続 55
入力ソース数の拡大 56
Bluetooth ヘッドセット 57
ISDN リンクの接続 58

メンテナンス 59
システム ソフトウェアをアップグレードする (1/2ページ) 60
オプション キーを追加する 62
システム ステータス 63

診断の実行 ... 64
ログ ファイルをダウンロードする ... 65
リモート サポート ユーザを作成する ... 66
設定とカスタム要素のバックアップ/復元 ... 67
カスタム要素の CUCM プロビジョニング ... 68
カスタム要素の TMS プロビジョニング ... 69
以前に使用していたソフトウェア イメージに復元する ... 70
ビデオ システムの工場出荷時設定リセット (1/4 ページ) ... 71
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 ... 75

システム設定 ... 76
システム設定の概要 ... 77
Audio 設定 ... 82
Bluetooth 設定(Bluetooth settings) ... 84
CallHistory 設定 ... 85
Cameras 設定 ... 86
Conference 設定 ... 87
FacilityService 設定 ... 91
H323 設定 ... 92
Logging 設定 ... 95
Macros 設定 ... 96
Network 設定 ... 97
NetworkPort 設定 ... 104
NetworkServices 設定 ... 105
Peripherals 設定 ... 111
Phonebook 設定 ... 112
Provisioning 設定 ... 113
Proximity 設定 ... 116
RoomReset 設定 ... 117
RTP 設定 ... 118
Security 設定 ... 119
SerialPort 設定 ... 122
SIP 設定(SIP settings) ... 123
Standby 設定 ... 127
SystemUnit 設定 ... 128
Time 設定 ... 129
UserInterface 設定 ... 132
UserManagement 設定 ... 135
Video 設定 ... 137
Experimental 設定 ... 144

付録 ... 145
ユーザ インターフェイス ... 146
リモート モニタリングのセットアップ ... 147
Web インターフェイスを使用したコール情報へのアクセスとコール応答 ... 148
Web インターフェイスを使用してコールを発信する (1/2 ページ) ... 149
Web インターフェイスを使用してコンテンツを共有する ... 151
ローカル レイアウトの制御 ... 152
相手先(遠端)カメラの制御 ... 153
パケット損失の復元力:ClearPath ... 154
ビデオ システムの ユーザ インターフェイスをカスタマイズする (1/2 ページ) ... 155
マクロを使用したビデオ システムの動作のカスタマイズ ... 157
スタートアップ スクリプトを管理する ... 158
ビデオ システムの XML ファイルにアクセスする ... 159
Web インターフェイスからの API コマンドとコンフィギュレーションの実行 ... 160
シリアル インターフェイス ... 161
TCP ポートの開放 ... 162
TMS からの新しい HTTPFeedback アドレスの取得 ... 163
技術仕様 (1/2 ページ) ... 164
サポートされている RFC ... 166
シスコ Web サイト内のユーザ ドキュメンテーション ... 167
シスコのお問い合わせ先 ... 168

第 1 章

はじめに

ユーザ ドキュメンテーションとソフトウェア

このガイドの対象となる製品

- Cisco TelePresence DX70
- Cisco TelePresence DX80

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

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

ユーザ ドキュメンテーション

このガイドでは、ビデオ システムの管理に必要な情報を提供します。

主にオンプレミス登録のビデオ システム(CUCM, VCS)の機能と設定について説明していますが、クラウド サービス(Cisco Webex)登録のデバイスにも、その機能と設定の一部が適用されます。

この製品に関する詳しいガイドは、付録 ▶「シスコ Web サイト内のユーザ マニュアル」を参照してください。

シスコ Web サイト内のドキュメンテーション

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

▶ https://www.cisco.com/go/dx-docs

クラウドに登録されたデバイスのドキュメンテーション

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

▶ https://collaborationhelp.cisco.com

Cisco Project Workplace

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

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

ソフトウェア

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

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

ソフトウェア リリース ノート(CE9)を参照することをお勧めします。

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

CE ソフトウェアへの変換

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

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

CE9 の最新情報

この章では、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/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

CE9.5 の新機能および改善点

韓国語キーボードのサポート

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

ウェルカムバナー

ビデオシステムのウェブインターフェイスまたはコマンドラインインターフェイスに、ユーザーがログイン後で表示されるウェルカムバナーを設定できます。開始を取得するために必要な情報がたとえば、バナーに含めることができます。 またはものがあります、システムを設定するときに認識します。

CE9.4 の新機能および改善点

Cisco Spark から Cisco Webex へのリブランディング

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

以下の製品は、新たな名称を得ます。

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

管理設定ロックダウン構成の CUCM プロビジョニング

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

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

ユーザ インターフェイスから逆光補正を有効にします。

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

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

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

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

室内制御の更新

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

CE9.3 の新機能および改善点

設定とカスタム要素のバックアップ/復元

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

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

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

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

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

カスタム要素のプロビジョニング

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

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

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

プロビジョニングの詳細については、リリース ノートを参照してください。

室内制御の更新

室内制御機能には次の機能が追加されています。

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

また、室内制御エディタに次の機能が追加されました。

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

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

ISDN リンクのサポート

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

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

ワンボタン機能(OBTP)のスヌーズ

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

発信前のコール レートの調整

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

カスタム コール レートを選択しない場合は、*[会議のデフォルト コール レート(Conference 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、*[今すぐアップグレード(Upgrade now)]* または*[延期(Postpone)]*を選択することができます。アップグレードを延期した場合には、必要なときに、ユーザ インターフェイスの *[設定(Settings)]* > *[このデバイスについて(About this device)]* メニューからアップグレードを再開できます。以前のように 6 時間待つ必要はなくなりました。

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

システム情報がユーザ インターフェイスに公開されることの防止

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

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

この機能を有効にするには、次の操作が必要です。

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

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

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。

ミラード セルフビュー

他人から見えているように自分の画像を表示したり、鏡に映っているように自分の画像を表示するようにビデオ システムを設定できます。*[ビデオ セルフビュー ミラード(Video Selfview Mirrored)]* 設定を使います。これまで、ミラード セルフビューは、Android ソフトウェアを実行している Cisco DX デバイスでのみ利用できました。

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

1 冊の共通 API ガイド

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

CE9.2 の新機能および改善点

マクロ フレームワーク

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

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

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

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

ブランディングとハーフウェイクのカスタマイズ

独自のテキストと画像をアップロードして、ハーフウェイク状態とアウェイク状態の両方の画面の表示をカスタマイズできます。

ハーフウェイク状態では、次のことができます。

- 画面に背景ブランド イメージを追加します。
- 画面の右下隅に小さなロゴを追加する。

アウェイク状態では、次のことができます。

- 画面の右下隅に小さなロゴを追加する。
- 画面の左下隅にラベルまたはメッセージを追加する。

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

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

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

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

カスタム入力プロンプトの API コマンドAPI

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

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

API 経由での証明書のアップロード

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

ユーザ管理用 API コマンド

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

室内制御のプレビュー モード

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

インテリジェント プロキシミティの変更点

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

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

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

コール サービスを変更する際の初期設定への自動リセット(デバイスの有効化)

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

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

音声とその他のメディアで別個の RTP ポート範囲のサポート

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

CE9.1 の新機能および改善点

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。

Bluetooth ヘッドセットのサポート

Bluetooth ヘッドセットをビデオ システムで使用できます。ヘッドセットは HFP(Hands Free Protocol)をサポートする必要があります。ユーザ インターフェースの Bluetooth ペアリング モードで、Bluetooth を有効化してビデオ システムを設定することができます。

ワイヤレス ネットワーク用の EAP 認証フレームワークのサポート

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

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

ネットワーク ポート 2 を無効化可能

ビデオ システムの 2 番目のネットワーク ポートを介して、コンピュータをネットワークに接続することができます。この場合、ビデオ システムとコンピュータの両方をサポートするために、ネットワーク コンセントは 1 つしか必要ありません。

セキュリティ上の理由から、公共の環境でビデオ システムを使用する場合は、このネットワーク ポートを無効にすることをお勧めします。これにより、第三者がビデオ システムを介してコンピュータをネットワークに接続するのを防ぐことができます。

CE9.0 の新機能および改善点

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。

CE9.5 でのシステム設定の変更点

新しい設定

NetworkServices SSH HostKeyAlgorithm

削除された設定

[なし(None)]

変更された設定

[なし(None)]

CE9.4 でのシステム設定の変更点

新しい設定

Cameras Camera [1] Backlight DefaultMode

Conference FarendMessage Mode

SIP MinimumTLSVersion

削除されたコンフィギュレーション

NetworkServices HTTP Proxy Allowed

Video Output Connector [2] CEC Mode

Video Output Connector [2] Location HorizontalOffset

Video Output Connector [2] Location VerticalOffset

Video Output Connector [2] OverscanLevel

Video Output Connector [2] Resolution

Video Output Connector [2] RGBQuantizationRange

変更されたコンフィギュレーション

Network [1] DNS DNSSEC Mode

旧:**ユーザ ロール**:ADMIN, USER

新:**ユーザ ロール**:ADMIN

Network [1] Speed

旧:**ユーザ ロール**:ADMIN, USER

新:**ユーザ ロール**:ADMIN, INTEGRATOR

NetworkServices HTTP Mode

旧:**デフォルト値**:HTTP+HTTPS

新:**デフォルト値**:HTTPS

NetworkServices SNMP CommunityName

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, INTEGRATOR

NetworkServices SNMP Host [1..3] Address

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, INTEGRATOR

NetworkServices SNMP Mode

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, INTEGRATOR

NetworkServices SNMP SystemContact

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, INTEGRATOR

NetworkServices SNMP SystemLocation

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, INTEGRATOR

UserInterface ContactInfo Type

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

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

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

Video Selfview Mirrored

削除されたコンフィギュレーション

Provisioning HttpMethod

変更されたコンフィギュレーション

NetworkServices HTTP Proxy Allowed

旧:**デフォルト値**:True

新:**デフォルト値**:False

NetworkServices HTTP Proxy Mode

旧:**設定可能な値**:Manual/Off

新:**設定可能な値**:Manual/Off/PACUrl/WPAD

Security Session MaxSessionsPerUser

旧:**設定可能な値**:**整数**(0 ～ 100) **デフォルト値**:0

新:**設定可能な値**:**整数**(1 ～ 20) **デフォルト値**:20

Security Session MaxTotalSessions

旧:**設定可能な値**:**整数**(0 ～ 100) **デフォルト値**:0

新:**設定可能な値**:**整数**(1 ～ 20) **デフォルト値**:20

CE9.2 でのシステム設定の変更点

新しい設定

Audio Ultrasound MaxVolume
Replacing Peripherals Pairing Ultrasound Volume MaxLevel

Audio Ultrasound Mode
Replacing Peripherals Pairing Ultrasound Volume Model

Macros AutoStart

Macros Mode

NetworkServices HTTP Proxy Allowed

NetworkServices HTTP Proxy LoginName

NetworkServices HTTP Proxy Mode

NetworkServices HTTP Proxy Password

NetworkServices HTTP Proxy Url

RTP Video Ports Range Start

RTP Video Ports Range Stop

Security Session FailedLoginsLockoutTime

Security Session MaxFailedLogins

UserInterface CustomMessage

UserInterface OSD HalfwakeMessage

UserInterface SettingsMenu Mode

削除されたコンフィギュレーション

会議マルチ ストリーム モード

Peripherals Pairing Ultrasound Volume MaxLevel
Replaced by Audio Ultrasound MaxVolume

Peripherals Pairing Ultrasound Volume Mode
Replaced by Audio Ultrasound Mode

変更されたコンフィギュレーション

Audio Input MicrophoneMode
旧:**ユーザ ロール**:ADMIN
新:**ユーザ ロール**:ADMIN, INTEGRATOR

Security Audit Logging Mode
旧:**デフォルト値**:Off
新:**デフォルト値**:Internal(**内部**)

UserInterface Language
新: Arabic and Hebrew added to valuespace

Video Output Connector[1] Resolution
旧:**ユーザ ロール**:ADMIN, INTEGRATOR
新:**ユーザ ロール**:ADMIN, INTEGRATOR, USER

CE9.1 でのシステム設定の変更点

新しい設定

Bluetooth Allowed

Bluetooth Enabled

NetworkPort [2] Mode

削除された設定

[なし(None)]

変更された設定

Network[1] IEEE8021X Password

旧:**設定可能な値**: String(0, 32)

新:**設定可能な値**: String(0, 50)

NetworkServices Wifi Enabled

旧:**デフォルト値**:False

新:**デフォルト値**:True

Video Input Connector [n] PresentationSelection

旧:**設定可能な値**:AutoShare/Desktop/Hidden/Manual/OnConnect

新:**設定可能な値**: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

Standby WakeupOnMotionDetection

削除されたコンフィギュレーション

UserInterface UserPreferences

Conference VideoBandwidth PresentationChannel Weight

Standby AudioMotionDetection

Video Layout DisableDisconnectedLocalOutputs

変更されたコンフィギュレーション

NetworkServices Wifi Allowed

Renamed from NetworkServices WIFI Allowed

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, USER

NetworkServices Wifi Enabled

Renamed from NetworkServices WIFI Enabled

旧:**ユーザ ロール**:ADMIN

新:**ユーザ ロール**:ADMIN, USER

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。これは、次の設定に追加されています。**

Audio DefaultVolume

Audio Microphones Mute Enabled

Audio SoundsAndAlerts *

CallHistory Mode

Conference DefaultCall Rate

Conference DoNotDisturb DefaultTimeout

FacilityService *

Peripherals Pairing Ultrasound Volume MaxLevel

Peripherals Pairing Ultrasound Volume Mode

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] Location HorizontalOffset

Video Output Connector [n] Location VerticalOffset

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。**

DX70 および DX80 の概要

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

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

機能とメリット

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

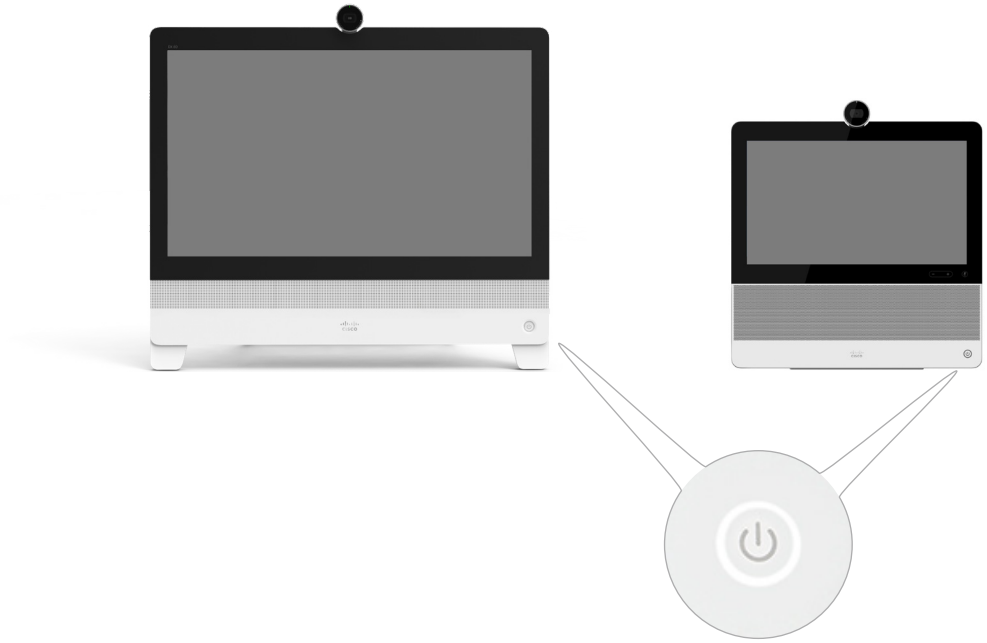
Cisco Webex DX70

Cisco Webex DX80

電源のオンとオフ

電源ボタンによる電源のオン/オフ

LED インジケータ付きの電源ボタンが、図に示すように前面にあります。



電源ボタン(LED が電源ボタンを囲んでいます)

スイッチを入れる

ビデオ システムは自動的には起動しません。電源ボタンを軽く押して数秒間押し続けます。

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。装置がスタンバイ状態になるまでに数秒かかります。

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。

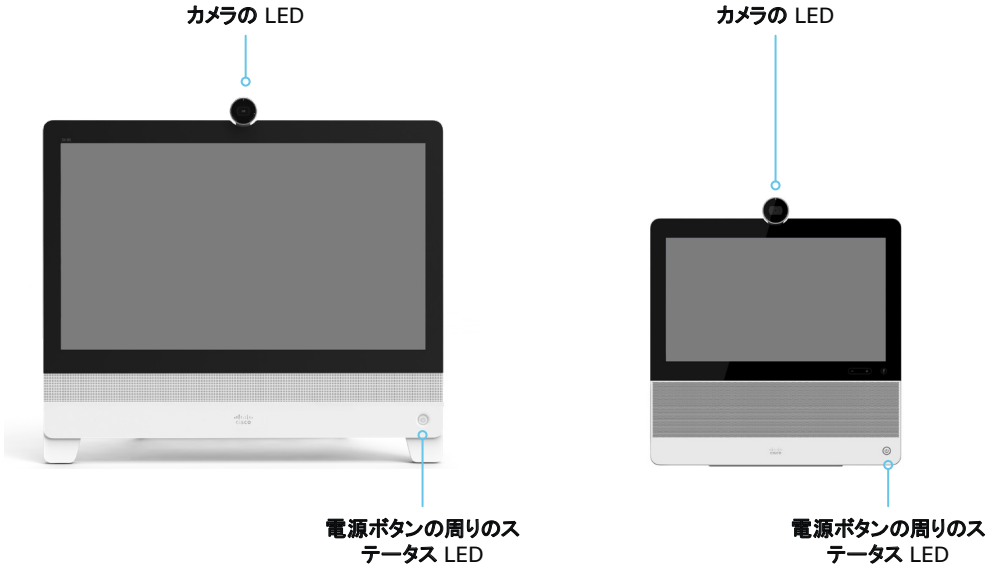
システムが使用可能になるまでに、数分かかります。

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:

点灯状態になります。

ビデオ システムの管理方法 (1/4 ページ)

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

次のような方法でもビデオ システムの API にアクセスできます。

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

Tip

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

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

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

次に例を示します。

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

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

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

アクセス方式	注	方式の有効化/無効化方法
HTTP/HTTPS	・ビデオ システムの Web インターフェイスで使用 ・非セキュア(HTTP)通信またはセキュア(HTTPS)通信 ・HTTPS:デフォルトで*有効* ・HTTP:以前のソフトウェア バージョンから CE9.4(以降)にアップグレードされ、アップグレード後に工場出荷時の設定にリセットされていない状態で提供されるビデオシステムのみ、デフォルトで*有効*となります。	*[ネットワークサービス(NetworkServices)] > [HTTP] > [モード(Mode)]* 変更を有効にするには、ビデオ システムを再起動します。
Telnet	・非セキュア TCP/IP 接続 ・デフォルトで [無効(Disabled)]	*[ネットワークサービス(NetworkServices)] > [Telnet] > [モード(Mode)]* 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	・セキュアな TCP/IP 接続 ・*デフォルトでイネーブルになっている。*	*[ネットワークサービス(NetworkServices)] > [SSH] > [モード(Mode)]* ビデオ システムを再起動する必要はありません。変更が有効になるまでに少し時間がかかる場合があります。
シリアル インターフェイス(RS-232)	・ケーブルを使用してビデオ システムに接続IP アドレス、DNS, ネットワークは不要。 ・*デフォルトでイネーブルになっている。* ・セキュリティ上の理由から、デフォルトではサインインするよう求められます *([シリアル ポート(SerialPort)] > [ログインが必須(LoginRequired)])*	*[シリアルポート(SerialPort)] > [モード(Mode)]* 変更を有効にするには、ビデオ システムを再起動します。

すべてのアクセス方式を無効にする(**[オフ(Off)]**)に設定する)と、ビデオ システムを設定できなくなります。再度有効にする(**[オン(On)]に設定する**)ことはできないため、復元するにはビデオ システムを工場出荷時設定にリセットする必要があります。

ビデオ システムの管理方法（2/4 ページ）

ビデオ システムの Web インターフェイス

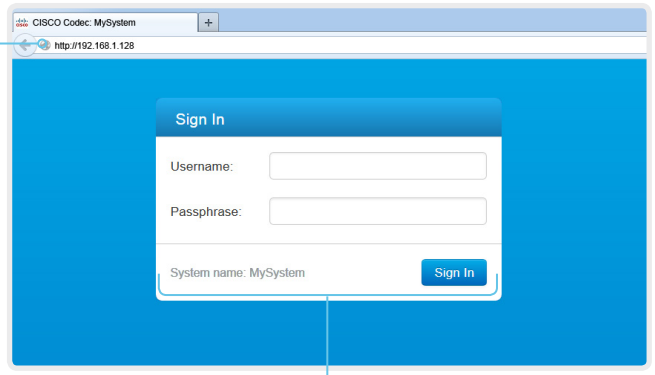
Web インターフェイスは、ビデオ システムの管理ポータルです。コンピュータから接続して、システムをリモートで管理できます。フル設定アクセスが提供され、メンテナンス用のツールやメカニズムを利用できます。

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

Web ブラウザは最新版を使用することを推奨します。

ビデオ システムへの接続

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



IP アドレスの確認方法

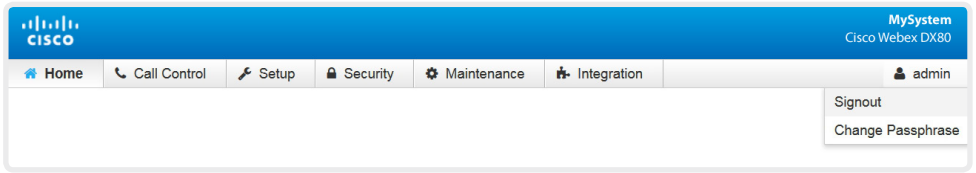
1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[このデバイスについて(About this device)]* に続き、*[設定(Settings)]* を選択します。

サインイン

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

システムには、パスフレーズなしの *admin* というデフォルトのユーザが提供されています。初めてサインインするときは、*[パスフレーズ(Passphrase)]* フィールドを空白のままにします。

admin ユーザのパスワードを設定する必要があります。



サインアウト

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

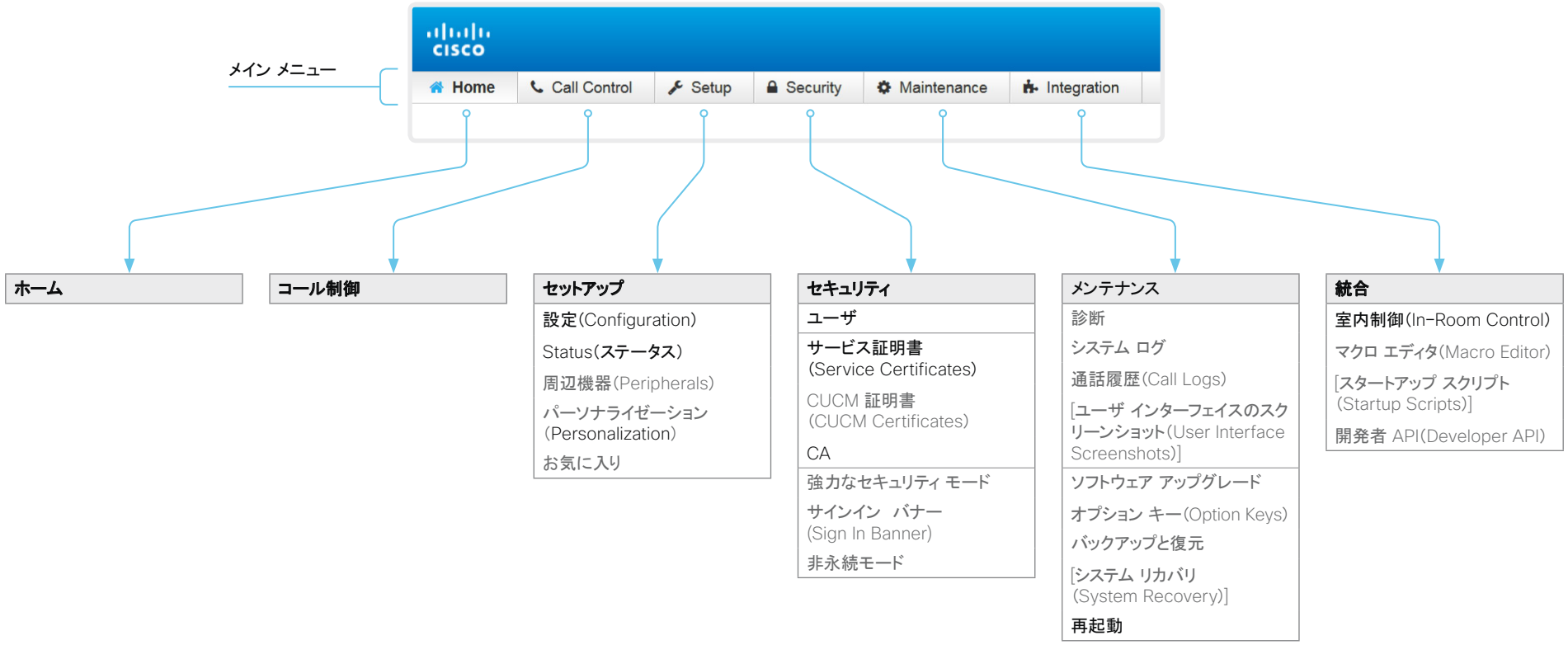
ビデオ システムの管理方法 (3/4 ページ)

Web インターフェイスの構成

Web インターフェイスは、各サブページから構成されています。ビデオ システムがオンプレミス サービス(CUCM, VCS)に登録されているときは下に示すすべてのサブページを使用できます。ビデオ システムがシスコのクラウド サービス(Cisco Webex)に登録されているときは灰色で示されているページを使用できません。

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

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



ビデオ システムの管理方法（4/4 ページ）

ユーザ インターフェイスの設定とシステム情報

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

システムの重要な設定と機能（ネットワーク設定、サービスの有効化、工場出荷時設定へのリセットなど）は、パス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状態では設定されていません。

必ず *admin* ユーザのパスフレーズを設定する必要があります。

パスフレーズの設定方法については、▶「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 アカウントの作成

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

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

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

   ww 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、ステータスを **[アクティブ(Acitve)]** または **[非アクティブ(Inactive)]** に設定してから、そのユーザが次回ログインしたときにパスフレーズを変更する必要があるかどうかを決定します。

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

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

パスフレーズを変更する

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

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

ユーザ アカウントを削除する

1. Web インターフェイスにサインインして、*[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 または複数の組み合わせを保持できます。デフォルトの *admin* ユーザなどの、フル アクセス権を持つユーザ アカウントは、ADMIN, USER, AUDIT の各役割も持つ必要があります。

これらはユーザ *ロール*です。

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

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

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

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

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

Cisco Webex 登録済のシステム

ビデオ システムがシスコのクラウド サービス(Cisco Webex)に登録されている場合は、INTEGRATOR ユーザ ロールと ROOMCONTROL ユーザ ロールを持つローカル ユーザだけを利用できます。

システム パスフレーズを変更する

次の操作を行うには、システム パスフレーズを知っている必要があります。

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

デフォルトのユーザ アカウント

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

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

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

他のユーザ アカウント

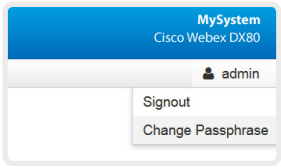
ビデオ システムのユーザ アカウントを複数作成することができます。

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

パスフレーズを変更する

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

   パスフレーズの形式は、0 ～ 64 文字の文字列です。



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

別のユーザのパスフレーズの変更

管理者アクセス権がある場合は、すべてのユーザのパスフレーズを変更できます。

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

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

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

[設定(Settings)] メニューへのアクセスの制限

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

権限のないユーザがビデオ システムの設定を変更できないようにするために、このアクセスを制限することをお勧めします。

[設定(Settings)] メニューをロックする

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

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

[設定(Settings)] メニューのロック解除

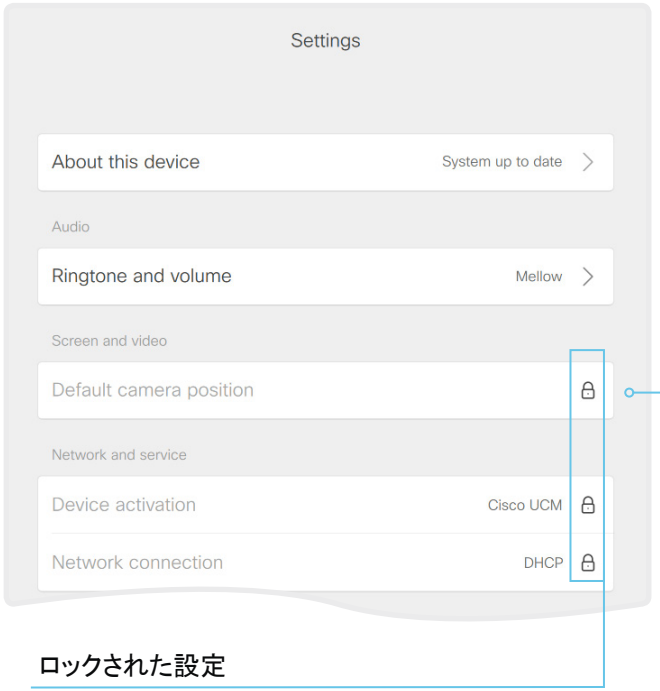
1. Web インターフェイスにサインインして、*[セットアップ(Setup)] > [設定(Configuration)]* に移動します。
2. *[ユーザインターフェイス(UserInterface)] > [設定メニュー(SettingsMenu)] > [モード(Mode)]* に移動して、**[ロックなし(Unlocked)]** を選択します。
3. *[保存(Save)]* をクリックして変更を有効にします。

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

ユーザ インターフェイスの [設定(Settings)] メニュー

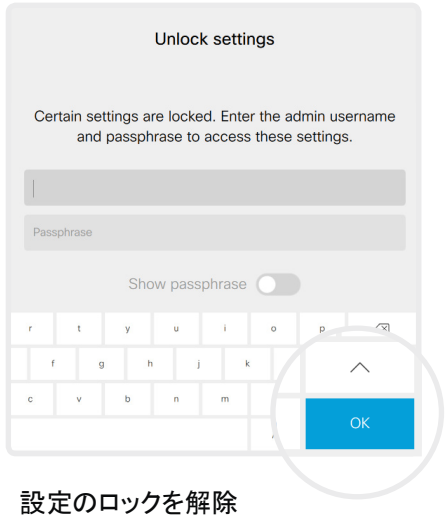
このメニューがロックされている場合は、サインインしないと、システムの重要な設定にアクセスできません。

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



ロックされた設定

ロックされた設定には南京錠のマークが付いています。



設定のロックを解除

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

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

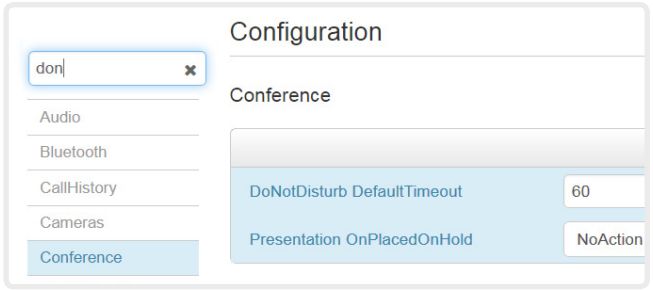
システム設定

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

システム設定を検索する

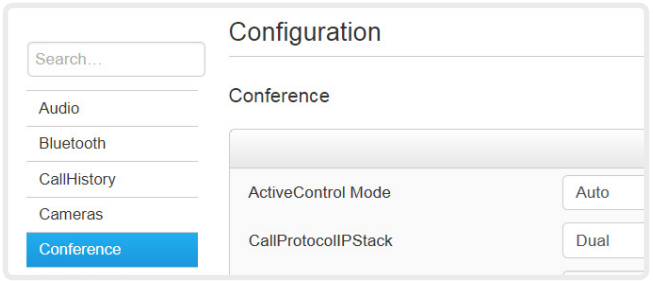
設定を検索する

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



カテゴリを選択して設定に移動する

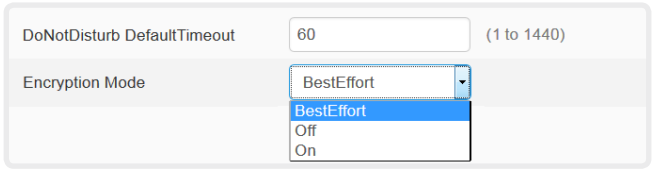
システム設定は各カテゴリにグループ化されています。左側のペインのカテゴリを 1 つ選択して、関連付けられている設定を表示します。



システム設定を変更する

値スペースを確認する

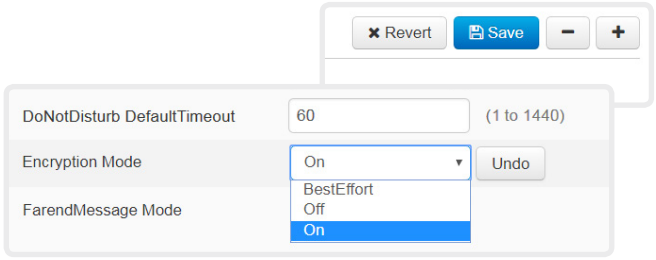
設定の値スペースは、入力フィールドに続くテキストか、矢印をクリックすると開くドロップダウン リストで指定します。



値の変更

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

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



変更が保存されていないカテゴリには、編集記号( )のマークが付きます。

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」の章を参照してください。

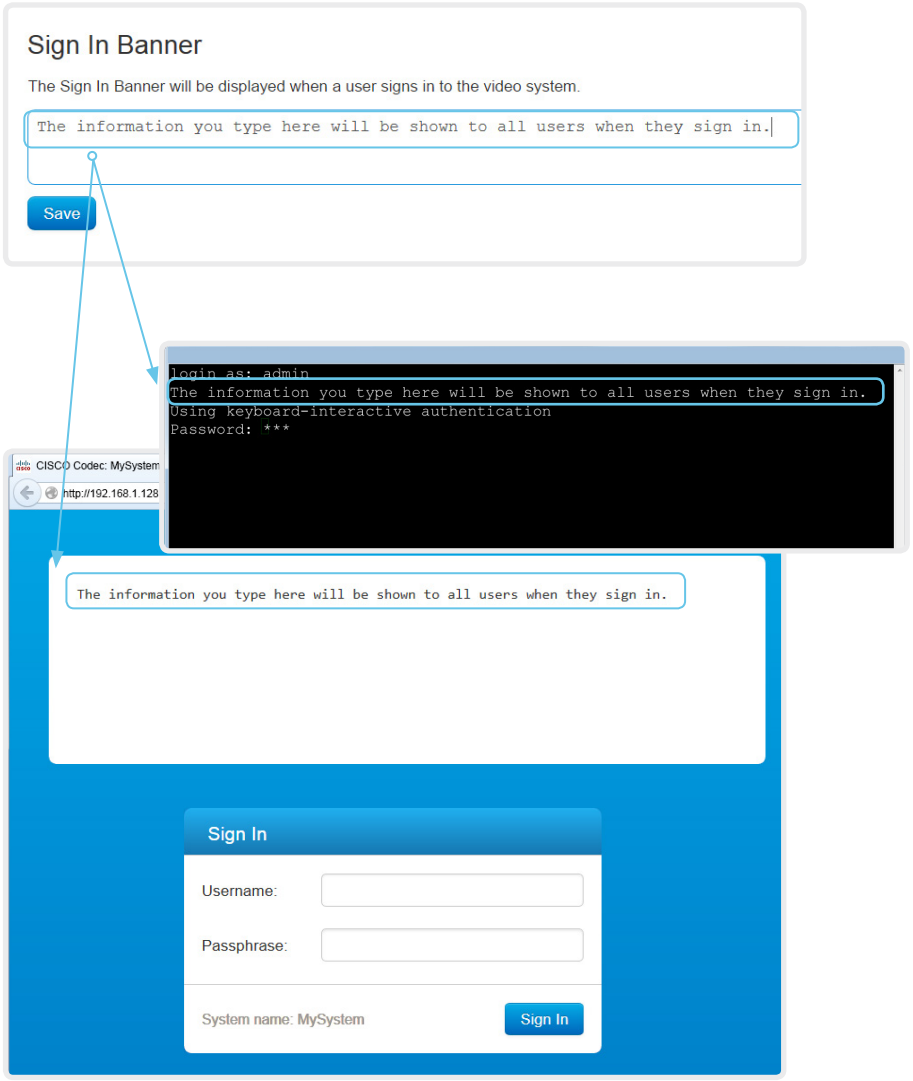
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者はすべてのシステム設定を変更できるように、すべてのユーザ ロールを所有している必要があります。

ユーザ管理およびユーザ ロールに関する詳細情報は、▶「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. サインインしたユーザに表示するメッセージを入力します。
2. *[保存(Save)]* をクリックしてバナーをアクティブにします。



サインイン バナーについて

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

最大サイズは 4 kByte です。

ウェルカムバナーとログインバナーの比較

サインインバナー(Sign In Banner)

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

ウェルカムバナー

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

ウェルカムバナーの追加

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

API コマンド

```
xCommand SystemUnit WelcomeBanner Set
```

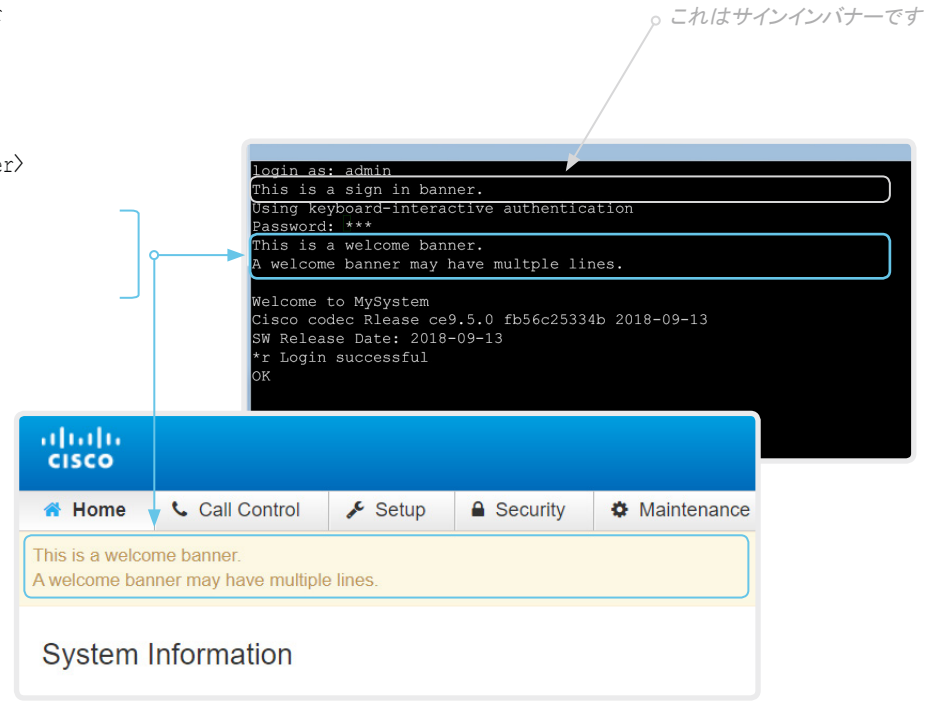
これはマルチライン コマンドです。このコマンド実行後に入力した文字が、コマンドに対する入力となります（改行を含む）。ピリオドを含み改行で終わる別の行を用いて、入力を終了します。

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

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

例

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



ウェルカムバナーについて

ビデオシステムのウェブインターフェイスまたはコマンドラインインターフェイスに、ユーザーがログイン後で表示されるウェルカムバナーを設定できます。バナーには、複数の行を表示することができます。

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

最大サイズは 4 kByte です。

ウェルカムバナーとログインバナーの比較

サインインバナー(Sign In Banner)

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

ウェルカムバナー

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

ビデオ システムのサービス証明書を管理する

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

次のファイルが必要です。

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

証明書と秘密キーは、ビデオ システムの同じファイル内に保存されます。

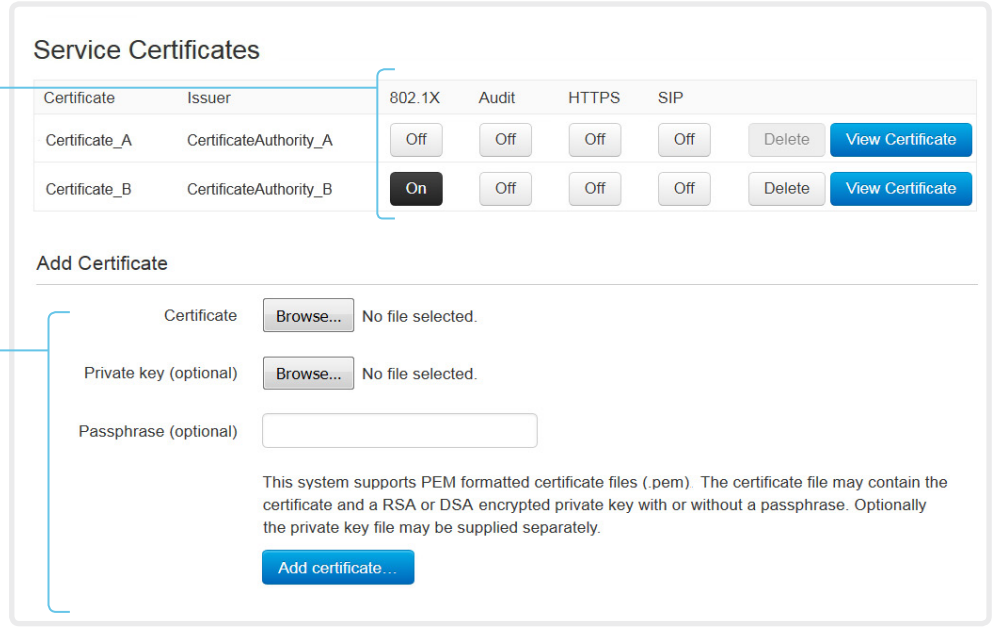
証明書を有効/無効にし、表示、または削除する

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

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

証明書の追加

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



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。

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

複数の証明書をビデオ システムで保存できますが、サービスごとに一度に有効化できる証明書は 1 つだけです。

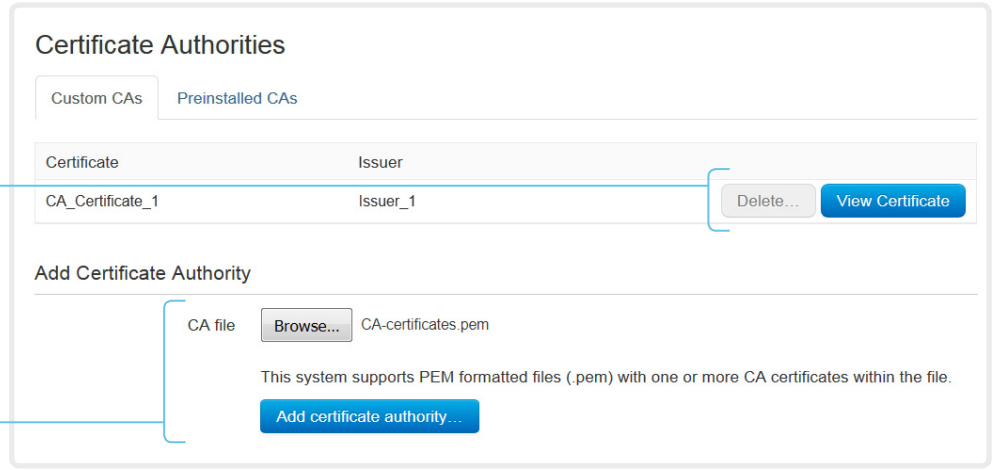
認証が失敗した場合、接続は確立されません。

信頼できる認証局(CA)のリストを管理する

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

次のファイルが必要です。

- CA 証明書のリスト(ファイル形式:.PEM)。



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。

証明書を表示または削除する

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

認証局のリストのアップロード

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

以前に保存した証明書は自動的には削除されません。

CA 証明書を含む新しいファイル内のエントリが既存のリストに付加されます。

信頼できる CA 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 により署名されている必要があります。

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

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

認証が失敗した場合、接続は確立されません。

セキュア監査ロギングのセットアップ

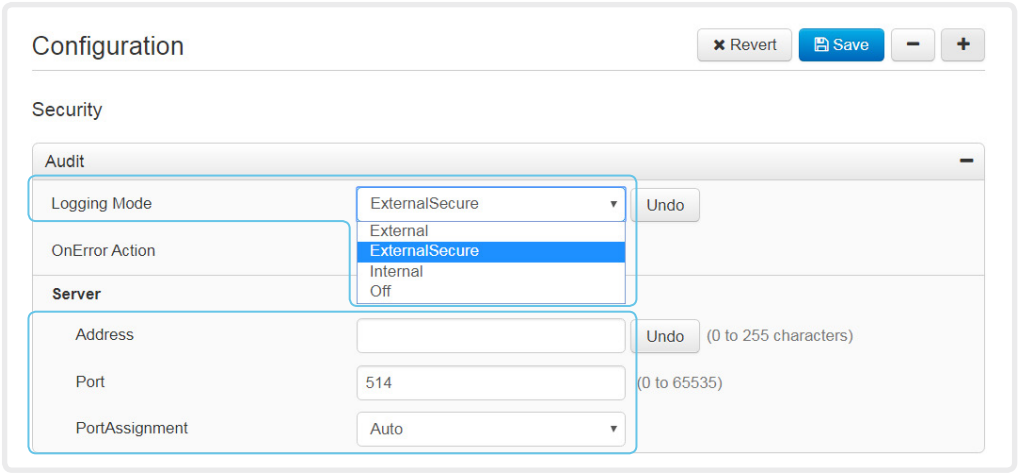
Web インターフェイスにサインインして、*[セットアップ(Setup)] > [設定(Configuration)]* を移動します。

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

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

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

   [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、デフォルトでは無効になっています。

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

監査サーバの署名は、他のサーバ/クライアントと同じ CA リストを使用して検証されます。

監査サーバ認証に失敗した場合は、監査ログが外部サーバに送信されません。

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

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

証明書の表示または無効化

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

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。

プレインストールされた証明書について

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

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

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

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

CUCM 信頼リストを削除する

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

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

CUCM 信頼リストを削除する

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

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

次のようなケースでは、これらのファイルを削除する必要があります。

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

信頼リスト フィンガープリントと証明書の概要

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

この情報は、トラブルシューティングに役立ちます。

信頼リストの詳細

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

永続モードを変更する

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

永続性ステータスの確認

アクティブなラジオ ボタンは、ビデオ システムの現在の永続性ステータスを示しています。

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

永続設定を変更する

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

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

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

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

永続モード

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

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

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

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

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

工場出荷時設定リセットの実行方法については、▶「ビデオ システムの工場出荷時設定リセット」の章を参照してください。

強力なセキュリティ モードの設定

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

強力なセキュリティ モードの設定

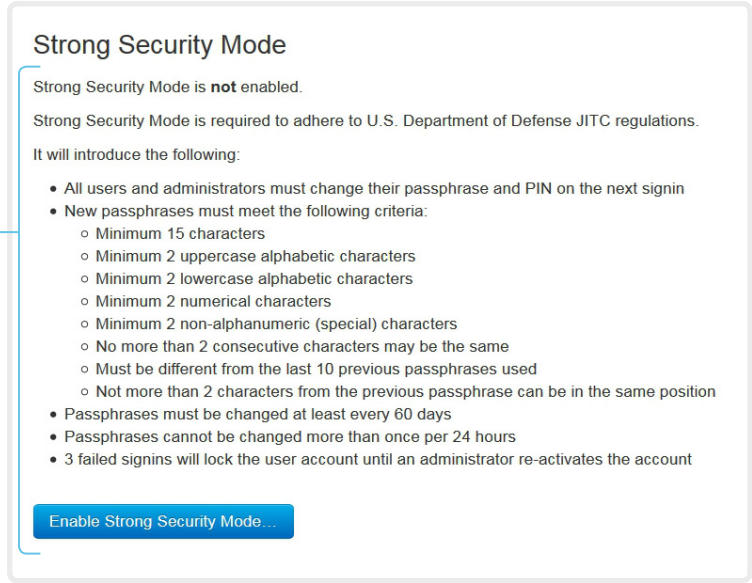
続行する前に、強力なセキュリティ モードの影響について注意してお読みください。

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

   ビデオ システムが自動的に再起動します。

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

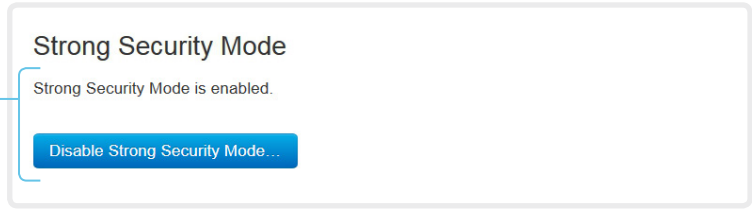
   システム パスフレーズの変更方法については、▶「システム パスフレーズの変更」の章を参照してください。



通常モードに戻る

ビデオ システムを通常モードに戻すには、*「強力なセキュリティモードの無効化…(Disable Strong Security Mode...)」* をクリックします。表示されるダイアログボックスで選択内容を確認します。

ビデオ システムは自動的に再起動します。



強力なセキュリティ モードについて

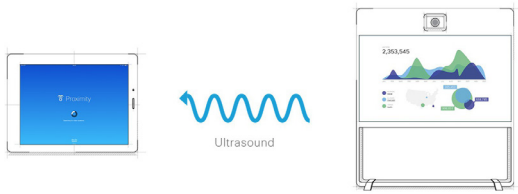
強力なセキュリティ モードは、DoD JITC 規制への準拠が必要な場合にのみ使用します。

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

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。



Proximity の同時接続数は、ビデオ システムのタイプによって異なります。この最大接続数に達すると、新しいユーザはクライアントから警告されます。

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

* *モバイルデバイスのプロキシミティサービスで、共有コンテンツの表示が無効になっている場合は* 接続数 30 です。サービス有効時は接続数 7 です。

プロキシミティ サービス

コールの発信とビデオ システムの制御:

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

モバイル デバイス上での共有コンテンツの表示:

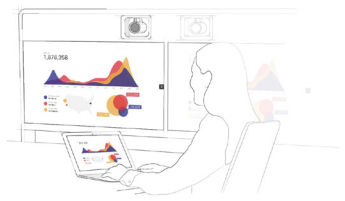
- 共有コンテンツの表示、以前のスライドのレビュー、選択されたスライドの保存
- スマートフォンとタブレット(iOS と Android)で使用可能
- DX70 および DX80 の場合、このサービスは通話時にのみ利用できます。

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の共有
- ラップトップ(OS X と Windows)で使用可能


コールの発信とビデオ 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 クライアントをインストールする

クライアントの入手場所

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

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

エンド ユーザ ライセンス契約書

エンドユーザ ライセンス契約を確認してください。
► https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html [英語]

サポートされるオペレーティング システム

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

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

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

超音波の放出

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

[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、75 dB 未満のレベルで影響が生じることはほとんどありません。

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

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

DX70 および DX80:

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

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

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

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

ヘッドセット

DX70、DX80、および SX10N:

これらのシステムでは、次の理由からヘッドセットを常に使用できます。

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

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

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

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

プロキシミティ サービスを有効にする

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

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

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

   コールの発信とビデオ システムの制御:

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

   モバイル デバイス上での共有コンテンツの表示:

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

   デスクトップ クライアントからのワイヤレス共有:

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

プロキシミティ インジケータ

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

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

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。

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

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

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

プライバシーについて

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ください。
► https://www.cisco.com/web/siteassets/legal/privacy.html
[英語]

ビデオ システムでの通話中には、室内の各モバイル デバイスではコンテンツの受信および表示のみを行えることに注意してください。

基本的なトラブルシューティング

プロキシミティ クライアントを使用するデバイスを検出できない

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

オーディオ アーチファクト

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

ラップトップから内容を共有できない

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

関連リソース

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

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

ビデオ品質の対コール レート比調整

ビデオ入力品質の設定

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

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

最適鮮明度プロファイル

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

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

異なる最適鮮明度プロファイルに使用する標準的な解像度、帯域、および送信フレーム レートの一部を表に示します。解像度とフレーム レートは、発信側と着信側の両方の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 30fps		
	標準	*中*	*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

画面に企業ブランディングを追加 (1/2 ページ)

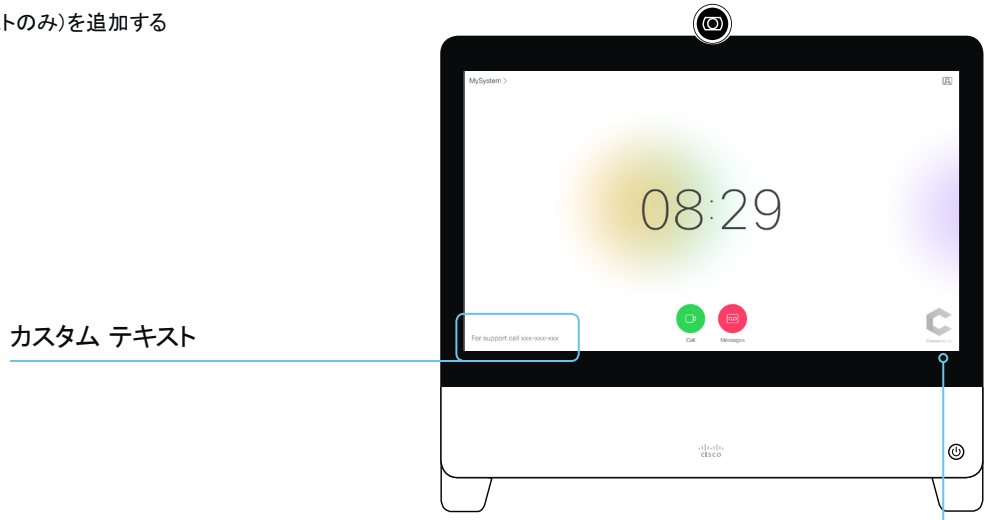
Web インターフェイスにサインインして、*[セットアップ(Setup)] > [パーソナライゼーション(Personalization)]* に移動し、*[ブランディング(Branding)]* タブを開きます。

このページから、独自のブランディング要素(背景ブランド イメージ、ロゴ、カスタム メッセージ)をビデオ システムに追加できます。

アウェイク状態のブランディング

アウェイク状態では、次のことができます。

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



推奨事項:

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

ブランディングについて

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

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

ブランド機能とカスタム壁紙は、同時に使用できません。

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

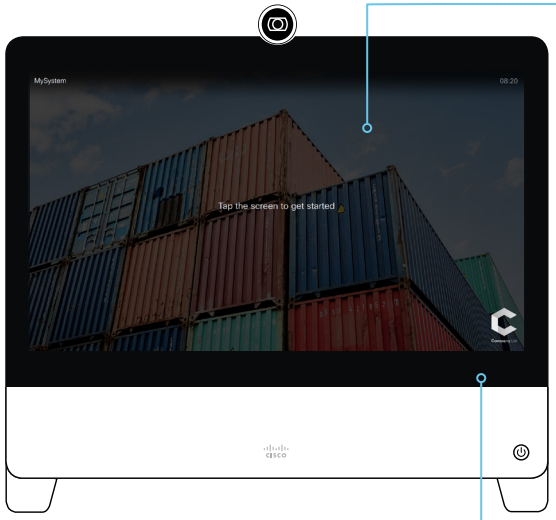
画面に企業ブランディングを追加 (2/2 ページ)

ハーフウェイク状態のブランディング

ハーフウェイク状態では、次のことができます。

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

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



背景ブランド イメージ

- ビデオ システムがウェイクアップするとイメージがフルカラーで表示され、数秒後に自動的に淡色表示になります(透明な黒色のオーバーレイ)
- イメージの形式:PNG または JPEG
- 推奨サイズ: 1920 × 1080 ピクセル

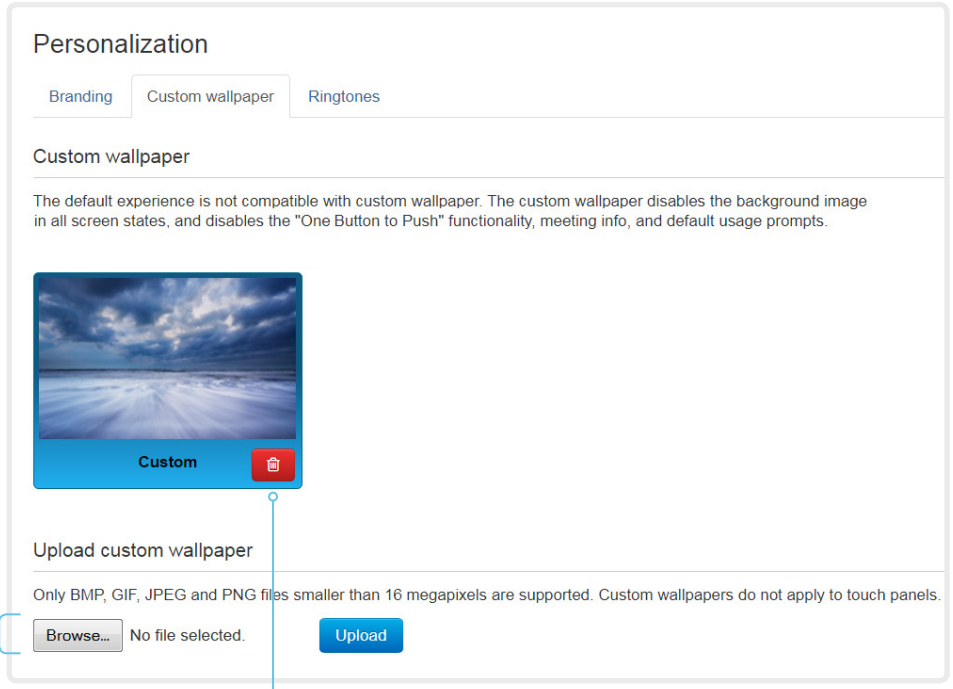
Logo

推奨事項:

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

カスタム壁紙の追加

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



カスタムの壁紙のアップロード

古いカスタム壁紙があれば上書きします。

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

   サポートされるファイル形式:BMP, GIF, JPEG, PNG

   最大ファイル サイズ:16 メガピクセル

カスタム壁紙をアップロードすると、自動的にアクティブになります。

カスタムの壁紙の削除

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

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

カスタム壁紙について

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

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

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

ブランド機能とカスタム壁紙は、同時に使用できません。

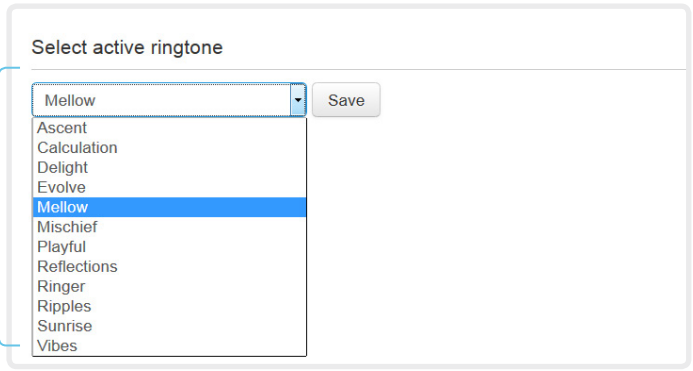
ビデオ システムでブランディング要素がセットアップされている場合は、カスタム壁紙を追加する前に *[ブランディングなしで続行(Continue without branding)]* をクリックする必要があります。

着信音の選択と着信音量の設定

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

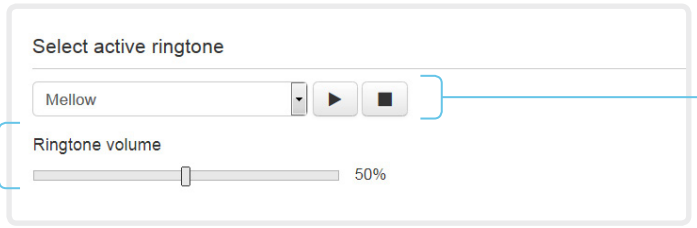
呼び出し音の変更

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



呼び出し音の音量の設定

呼び出し音の音量を調節するにはスライド バーを使用します。



呼び出し音の再生

呼び出し音を再生するには、再生ボタン(▶)をクリックします。

再生を終了するには、停止ボタン(■)を使用します。

着信音について

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

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

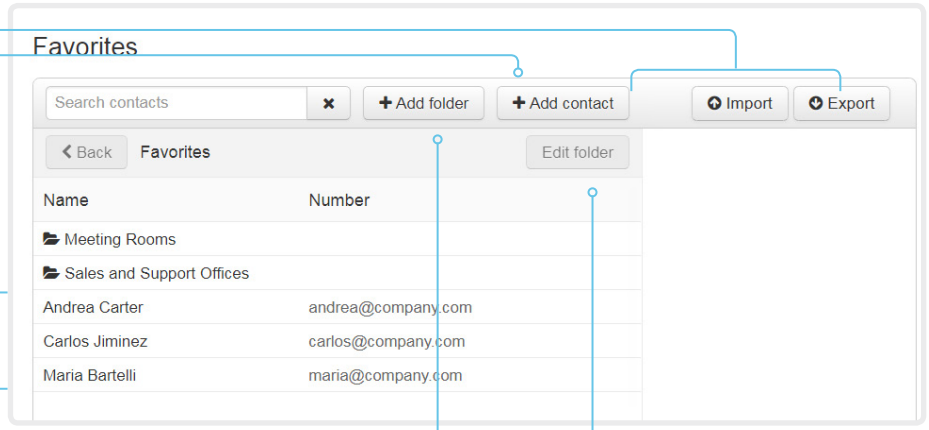
お気に入りリストの管理

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

ファイルから連絡先をインポート/エクスポート

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

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



連絡先を追加または編集する

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

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

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

コンタクトの削除

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

サブフォルダを追加または編集する

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

サブフォルダを削除する

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

ビデオ システムのユーザ インターフェイスによるお気に入りの管理

お気に入りリストへの連絡先の追加

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

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

お気に入りリストからの連絡先の削除

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

アクセシビリティ機能のセットアップ

着信時のスクリーンの点滅

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

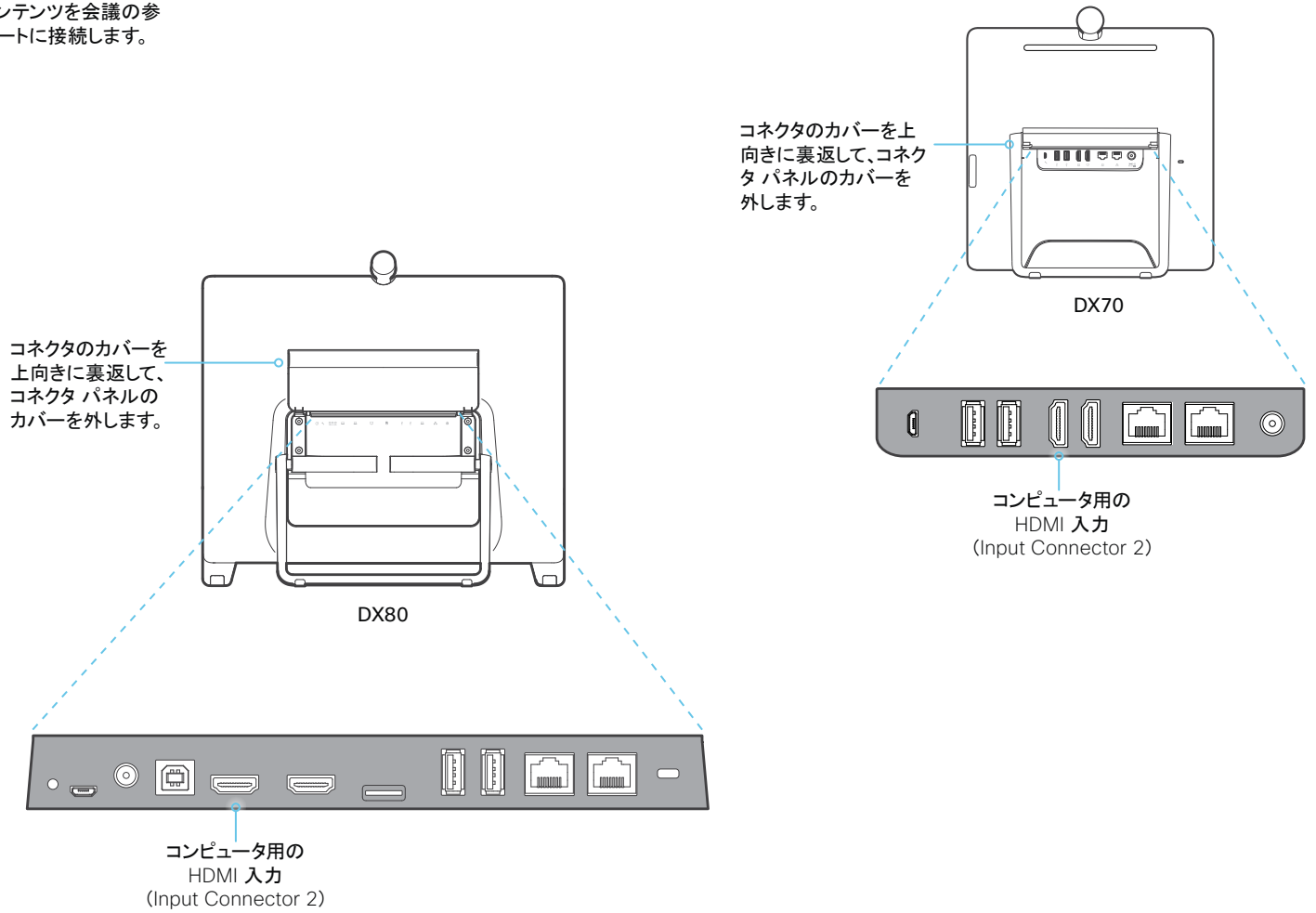
1. Web インターフェイスにサインインして、*[セットアップ(Setup)] > [設定(Configuration)]*に移動します。
2. *[ユーザインターフェイス(UserInterface)] > [アクセシビリティ(Accessibility)] > [着信コール通知(IncomingCallNotification)]* に移動して、[画面表示の強調(AmplifiedVisuals)] を選択します。
3. *[Save(保存)]* をクリックします。

第 3 章

ペリフェラル

コンピュータの接続

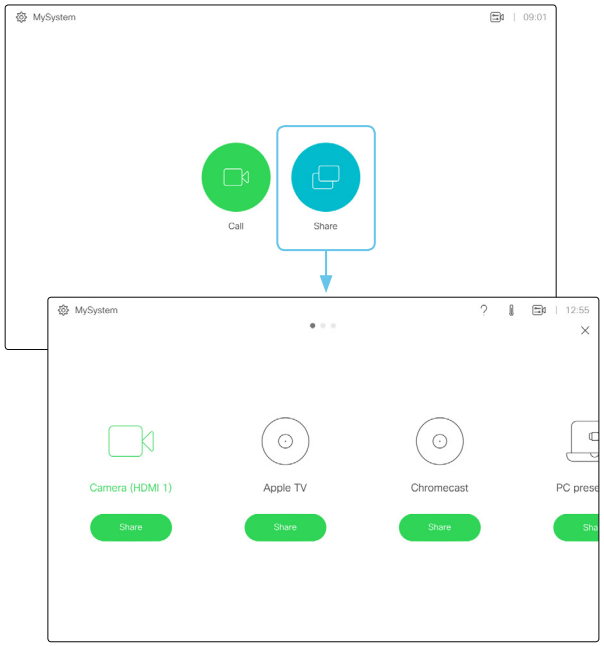
ビデオ システムをコンピュータの画面として使用し、コンテンツを会議の参加者と共有するには、コンピュータを HDMI の入力ポートに接続します。



入力ソース数の拡大

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）

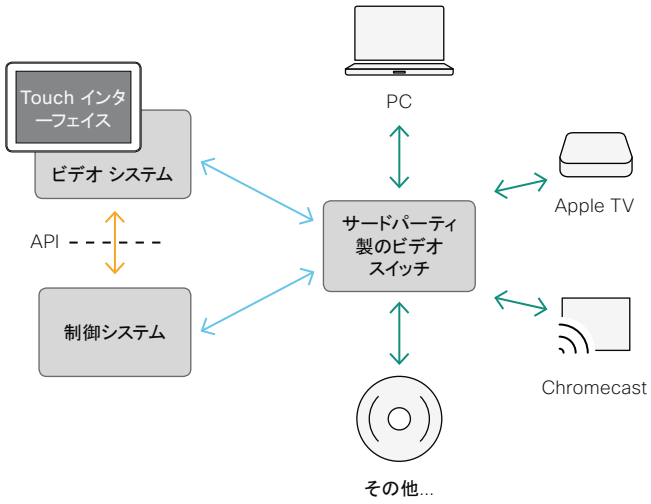
ユーザ インターフェイスを拡張する方法、およびそれをビデオ システムの API を使用してセットアップする方法の詳細については、CE のカスタマイズ ガイド [英語] を参照してください。次のリンクにアクセスします。

▶ 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。ビデオ スイッチを制御するのは、ビデオ システムではなく、制御システムです。

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



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

Bluetooth ヘッドセット

DX70 と DX80 では Bluetooth ヘッドセットがサポートされています。

- サポートされている Bluetooth プロファイル:
  - HFP(ハンズフリー プロファイル)
  - A2DP(高度なオーディオ配信プロファイル)
  - ヘッドセットでは HFP と A2DP の両方、または HFP のみがサポートされている必要があります。A2DP 専用のヘッドセットはサポートされていません。
- Bluetooth ヘッドセットは組み込みの Bluetooth 無線を直接使用してサポートされています。また USB Bluetooth ドングルを介して使用することもできます。
- ビデオ システムに複数のヘッドセットをペアリングすることができますが、一度に接続できるのは 1 つだけです。
- 範囲は最大 10 m(30 フィート)です。通話中にこの範囲の外に出ると、音声がビデオ システムのスピーカーに切り替わります。
- ほとんどのヘッドセットには音量コントロールが組み込まれています。通話中の場合は、ヘッドセットとビデオ システムの音量は同期しています。通話中でない場合は、ヘッドセットとビデオ システムの音量ボタンは独立して動作します。

サポート対象の Bluetooth 機能

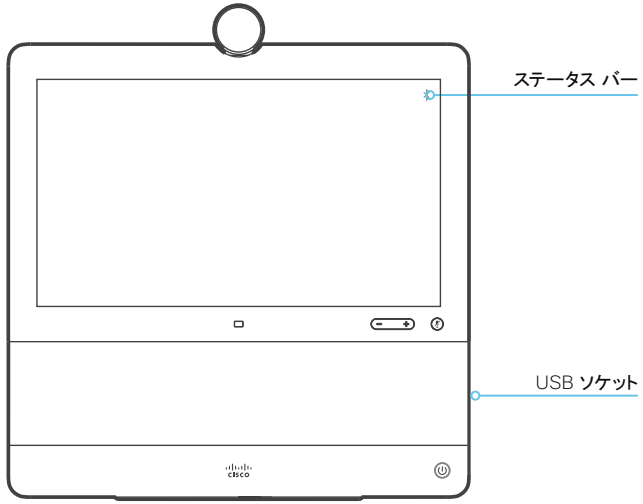
- 着信通話の応答
- 着信コールを拒否する
- 通話の終了
- 音量の増減
- 一部のヘッドセットにはミュート コントロールがあります。これはビデオ システムのミュート コントロールとは独立して動作します。

USB Bluetooth ドングル

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

Bluetooth ヘッドセットのペアリング

1. ヘッドセットで Bluetooth のペアリングをアクティブにします。ご不明な点がある場合は、ヘッドセットのマニュアルを参照してください。
2. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。*[設定(Settings)]*、*[Bluetooth]* の順に選択します。Bluetooth が無効になっている場合は有効にします。Bluetooth はデフォルトで有効になっています。
3. ビデオ システムがデバイスをスキャンします。検出された Bluetooth ヘッドセットがデバイス リストに表示されます。
4. デバイスを選択するとペアリングが開始されます。ペアリングが完了するまで数秒かかることがあります。
5. ペアリングが成功すると、ビデオ システムに接続済みのヘッドセットとしてリストされます。これでペアリングが完了です。

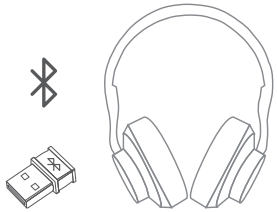


デバイス間の切り替え

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

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

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



Bluetooth のペアリングは、ビデオ システムに対して直接行うことも、USB ドングルを使用して行うこともできます。

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

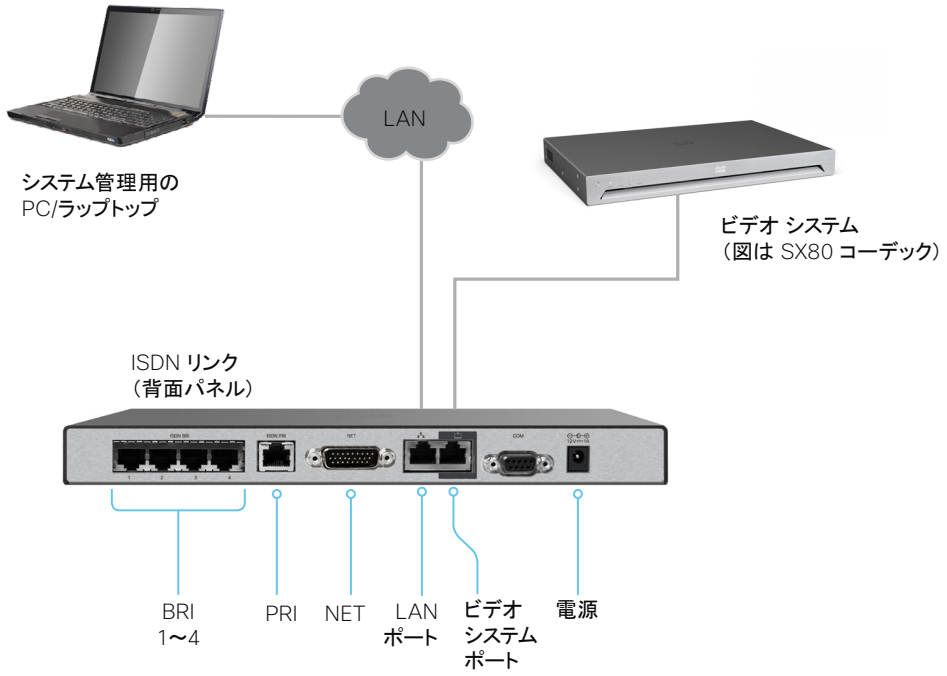
セットアップと構成

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

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

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

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



第 4 章

メンテナンス

システム ソフトウェアをアップグレードする (1/2ページ)

Android ベースのソフトウェアと CE ソフトウェアとの間の変換

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

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

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

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

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

詳細については、ソフトウェア リリース ノートを参照してください。

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

CE8 から CE9 へのアップグレード

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

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

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)

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

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

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

新しいソフトウェアをダウンロードする

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

各ソフトウェア バージョンに固有のファイル名があります。ファイル名の形式は「s52040ce9_5_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。

► https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html にアクセスしてください。

新しいソフトウェアのインストール

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

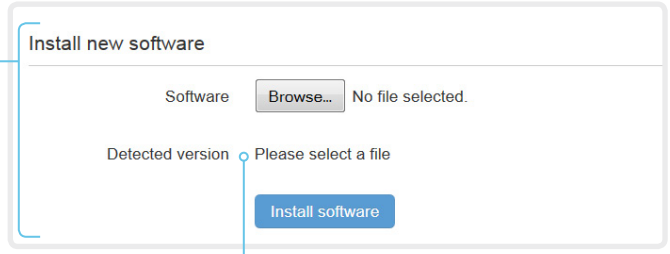
1. *[参照...(Browse...)]* をクリックして、新しいソフトウェアを含む .pkg ファイルを探します。

   ソフトウェアのバージョンが検出され、表示されます。

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

インストールの完了には、通常 15 分以上はかかりません。Web ページから進捗状況を確認できます。インストール後に、ビデオ システムが自動的に再起動します。

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



新しいソフトウェア バージョンの確認

ファイルを選択すると、ここにソフトウェアのバージョンが表示されます。

ソフトウェア バージョンについて

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

オプション キーを追加する

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

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

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

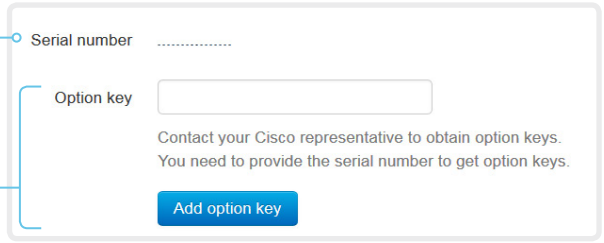
ビデオ システムのシリアル番号。

オプション キーの注文時にはビデオ システムのシリアル番号が必要です。

オプション キーの追加

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

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



オプション キーについて

ビデオ システムには、1 つ以上のソフトウェア オプションがインストールされている場合、またはインストールされていない場合があります。オプションの機能をアクティブするには、対応するオプション キーがビデオ システムに存在する必要があります。

各ビデオ システムには一意のオプション キーがあります。

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

システム ステータス

システム情報の概要

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

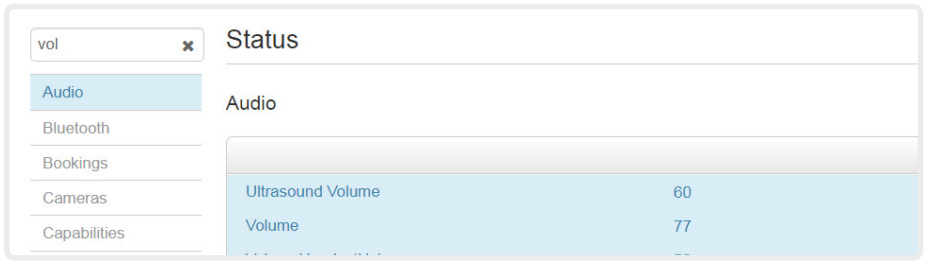
このページには、製品タイプ、システム名、およびハードウェア、ソフトウェア、インストール済みオプション、ネットワーク アドレスに関する基本情報が表示されます。ビデオ ネットワーク(SIP および H.323)の登録ステータスのほか、システムにコールする際に使用する番号および URI も含まれます。

システム ステータスの詳細

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

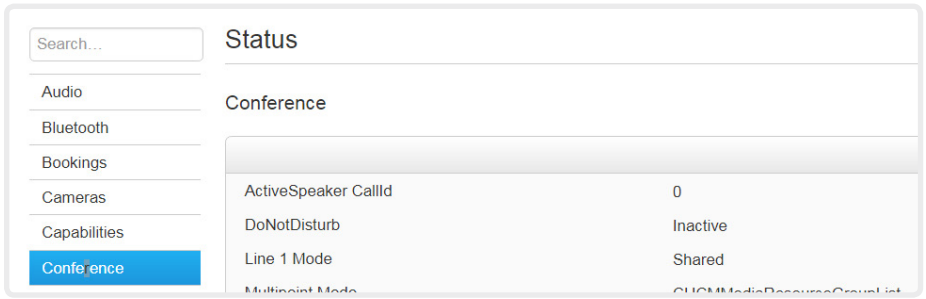
ステータス エントリを検索する

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



カテゴリを選択して適切なステータスに移動する

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



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

診断の実行

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

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

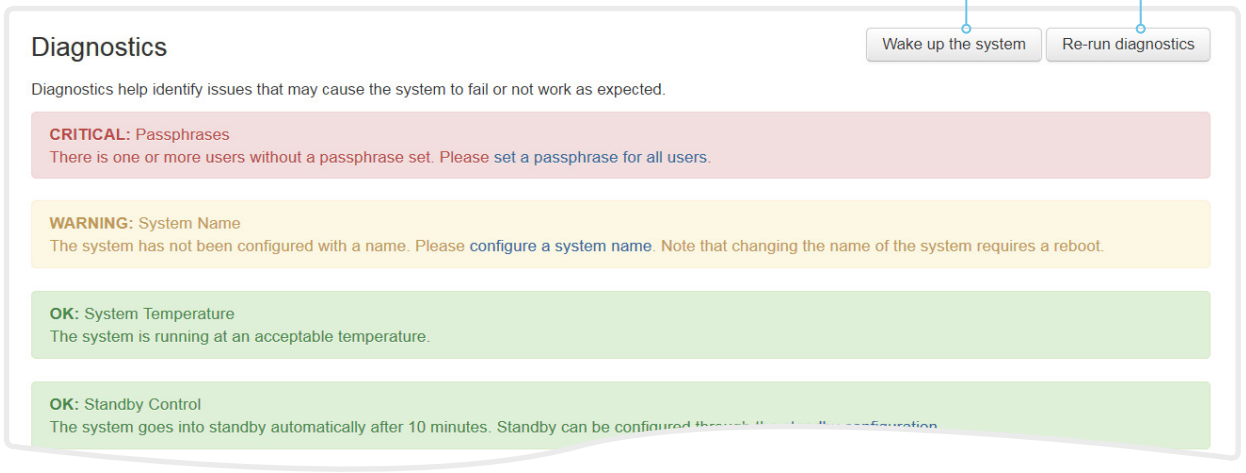
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

診断の実行

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

スタンバイ モードを離れる

スタンバイモードのビデオシステムを復帰させるには、*[システムの起動(Wake up the system)]* をクリックします。

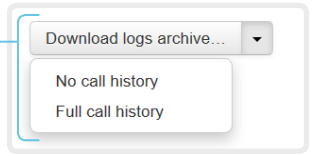


* 図に示しているメッセージは一例ですお使いのシステムでは表示される情報が異なる場合があります。

ログ ファイルをダウンロードする

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

すべてのログ ファイルをダウンロードする



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

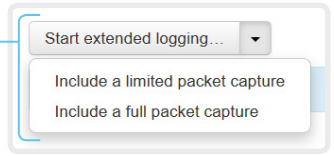
匿名化された通話履歴はログ ファイルにデフォルトで含まれています。

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

1 つのログファイルを開く/保存

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

拡張ロギングの開始



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

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

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

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

ログ ファイル 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

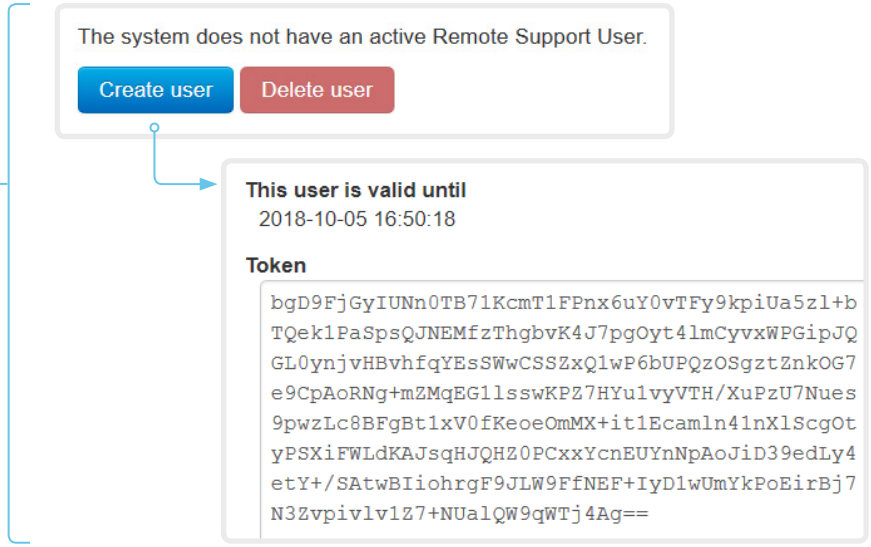
拡張ロギング モードをオンにすると、コールのセットアップ中にネットワークの問題の診断に役立つ場合があります。このモードの間は、より多くの情報がログ ファイルに保存されます。

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 システムの動作が標準を下回る場合があります。拡張ロギング モードは、トラブルシューティングのときにのみ使用してください。

リモート サポート ユーザを作成する

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

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



リモート サポート ユーザの作成

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

リモート サポート ユーザは 7 日間、または削除されるまで有効です。

リモート サポート ユーザの削除

[ユーザの削除(Delete User)] をクリックします。

リモート サポート ユーザについて

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

リモート サポート ユーザにはシステムへの読み取りアクセス権が付与され、トラブルシューティングに役立つ限定された一連のコマンドにアクセスできます。

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

設定とカスタム要素のバックアップ/復元

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

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

- ブランディング イメージ
- マクロ
- お気に入り
- サインイン 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、コンピュータ上に zip ファイル形式で構成要素を保存します。

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 ファイルを選択します。

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

   設定によっては、有効にするためにビデオ システムを再起動する必要があります。

その他の情報

マクロの復元

ビデオ システムでマクロを含むバックアップ ファイルを復元する場合、以下の処理が適用されます。

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

ブランド イメージの復元

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

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

バックアップ ファイル

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

カスタム要素の CUCM プロビジョニング

▶「構成とカスタム要素のバックアップと復元」の章で説明されているとおり、バックアップ ファイルは、さまざまなビデオシステムのカスタマイズ テンプレートとして使用できます。

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

- CUCM TFTP ファイル サービス、または
- HTTP または HTTPS のビデオ システムによって到達可能なカスタム Web サーバ。

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

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

カスタマイズ テンプレートの TFTP ファイル サーバへのアップロード

1. *Cisco Unified OS の管理*にサインインします。
2. *[ソフトウェア アップグレード(Software Upgrades)] > [TFTP ファイル管理(TFTP File Management)]* に移動します。
3. *[Upload File]* をクリックします。入力フィールドにカスタマイズ テンプレートの名前とパスを入力します。
4. *[Upload File]* をクリックします。

各ビデオ システムへのカスタマイズ プロビジョニング情報の追加

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

   これらのフィールドが存在しない場合は、CUCM に新しいデバイス パッケージをインストールする必要があります。
4. *[保存(Save)]* および *[構成の適用(Apply Config)]* をクリックし、構成をビデオ システムに送ります。

* TFTP サービスを使用しない場合は、カスタマイズ テンプレートの完全な URI: `<hostname>:<portnumber>/<path-and-filename>` を入力する必要があります。

次に例を示します。

- http://host:6970/backup.zip または
- https://host:6971/backup.zip

SHA512 チェックサム

ヒントWeb インターフェイスを使用してビデオ システムにファイルを復元することにより、ファイルの SHA512 チェックサムを検索できます。

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

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

CUCM のドキュメンテーション

▶ https://www.cisco.com/c/en/us/support/unified-communications/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

▶「構成とカスタム要素のバックアップと復元」の章で説明されているとおり、バックアップ ファイルは、さまざまなビデオシステムのカスタマイズ テンプレートとして使用できます。

バックアップ ファイルは、HTTP または HTTPS のビデオ システムによって到達可能なカスタム Web サーバ上にホストされる必要があります。

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

構成テンプレートの作成と適用

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

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

   where

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

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

   origin: Provisioning *

3. 構成テンプレートを送るビデオ 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 システムに送られます。バックアップ ファイルに、特定のビデオ システムに固有の構成(静的 IP アドレス、システム名、連絡先情報など)が含まれている場合、到達不能なビデオ システムで実行される可能性もあります。

以前に使用していたソフトウェア イメージに復元する

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

注:以下の手順では、別の CE ソフトウェアのバージョンへの復元(たとえば、CE8.3.y から CE8.2.x)のみを行えます。

Android ベースのソフトウェアに変換して戻す場合は、
▶ 「システム ソフトウェアをアップグレードする」の章を参照してください。

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

ログ ファイル、構成、カスタム要素のバックアップ

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

以前使用していたソフトウェア イメージに復元する

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

1. *[ソフトウェア回復交換(Software Recovery Swap)]* タブを選択します。
2. *[ソフトウェア:cex.y.z への切り替え...(Switch to software: cex.y.z...)]* をクリックします。ここで x.y.z はソフトウェア バージョンを示します。
3. *[はい(Yes)]* をクリックして選択を確定するか、*[キャンセル(Cancel)]* をクリックして操作を取り消します。

システムがリセットされるまでお待ちください。終了するとシステムは自動的に再起動します。この手順は数分かかることがあります。

以前に使用されたソフトウェア イメージについて

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

ソフトウェアを最後にアップグレードしてからシステムを工場出荷時設定にリセットしていない場合は、これまで使用していたソフトウェア イメージがシステムに存在しています。ソフトウェアをダウンロードする必要はありません。

ビデオ システムの工場出荷時設定リセット (1/4 ページ)

ビデオ システムに重大な問題が発生した場合、最後の手段として工場出荷時のデフォルト設定にリセットすることができます。

初期設定にリセットすると元に戻すことはできません。

工場出荷時の状態にリセットする前に以前使用したソフトウェア イメージに戻すことを常に検討してください。多くの場合これでシステムをリカバリします。ソフトウェアのスワップ(切り替え)については、▶「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を使用できない場合は、DX80 ではリセット pin ホールを、DX70 ではミュート ボタンと音量ボタンを使用します。

工場出荷時設定リセットにより、次のような影響が発生します。

- 通話履歴が削除されます。
- パスフレーズがデフォルト設定にリセットされます。
- すべてのシステム パラメータがデフォルト値にリセットされます。
- システムにアップロード済みのファイルが、すべて削除されます。リセットされる内容には、カスタムの壁紙、証明書、およびお気に入りリストが含まれますが、これに限定されません。
- 以前の(非アクティブな)ソフトウェア イメージが削除されます。
- オプション キーは影響を受けません。

工場出荷時設定リセット後、ビデオ システムは自動的に再起動します。これは、以前と同じソフトウェア イメージを使用しています。

初期設定へのリセットを実行する前に、ビデオ システムのログ ファイル、設定、カスタム要素をバックアップすることをお勧めします。バックアップしない場合は、これらのデータが消失します。

ビデオ システムの工場出荷時設定リセット (2/4 ページ)

Web インターフェイスを使用した初期設定へのリセット

初期設定へのリセットを行う前に、ビデオ システムのログ ファイルと設定をバックアップすることをお勧めします。

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

1. *[初期設定へのリセット(Factory Reset)]* タブを選択して、表示される情報を注意深く読みます。
2. *[初期設定へのリセットの実行(Perform a factory reset...)]* 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 (3/4 ページ)

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。

ミュート ボタンと音量ボタンを使用した DX80 の工場出荷時設定へのリセット

次の手順を実行して、起動時に DX80 を工場出荷時設定にリセットします。ビデオ システムの電源がオンになっている場合、先に進む前に電源ボタンを押して、システムがシャットダウンするまで押し続けます。

1. *ミュート* ボタンと *音量アップ* ボタンを探してください。
2. *音量アップ* ボタンを押したままにして、デバイスの電源をオンにします。
3. *ミュート* ボタンが赤色に点灯したら、*音量アップ* ボタンを放し、*ミュート* ボタンを押します。

   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。

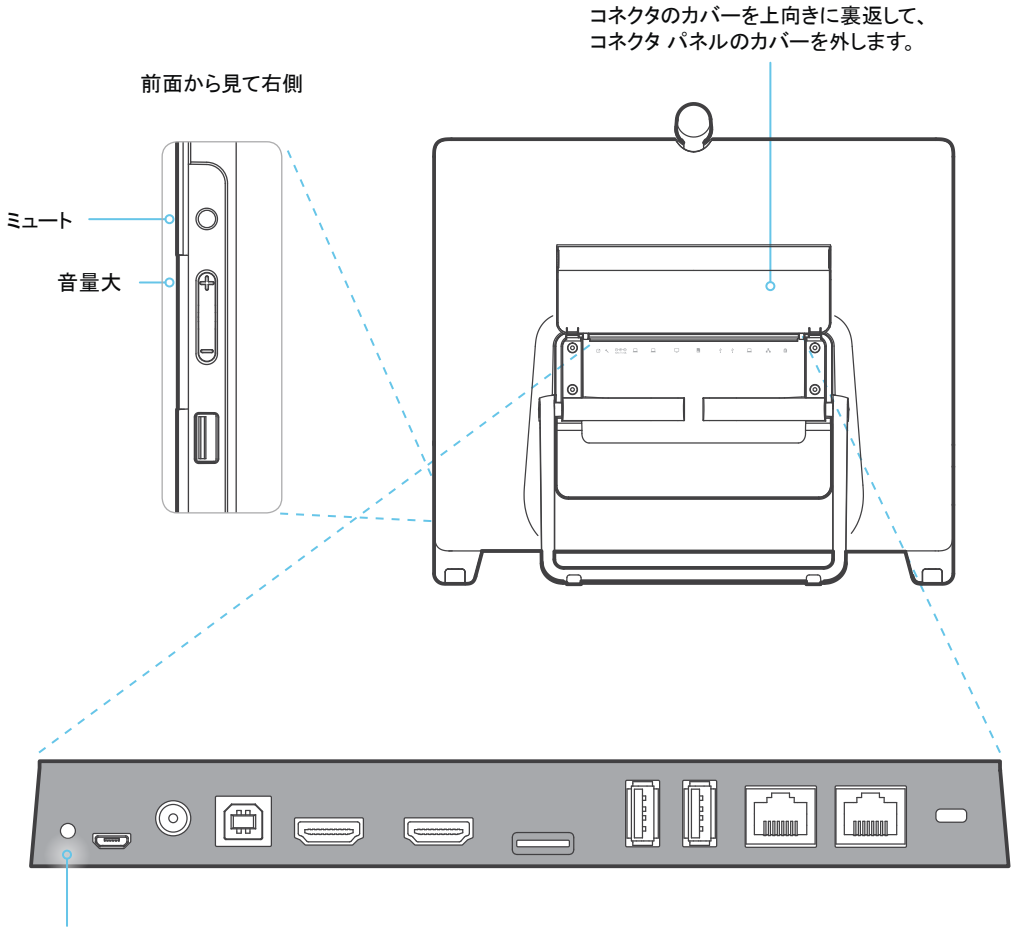
   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、*[ようこそ(Welcome)]* 画面が表示されます。

リセット ボタンを使用した DX80 の工場出荷時設定へのリセット

この方法を使用するには、DX80 が稼動している必要があります。

1. ビデオ システムの背面で、コネクタのカバーを上向きに裏返して、コネクタ パネルのカバーを外します。
2. ペン先(または同等のもの)を使用して、引っ込んでいるリセット ボタンを押して、*[初期設定へのリセットを実行しています(Resetting to factory settings)]* という通知が画面に表示されるまで、このボタンを 1 ～ 2 秒間押し続けます。
3. 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。



リセット ボタン(ピン ホール)

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

ビデオ システムの工場出荷時設定リセット (4/4 ページ)

初期設定へのリセットを行う前に、ビデオ システムのログ ファイルと設定をバックアップすることをお勧めします。

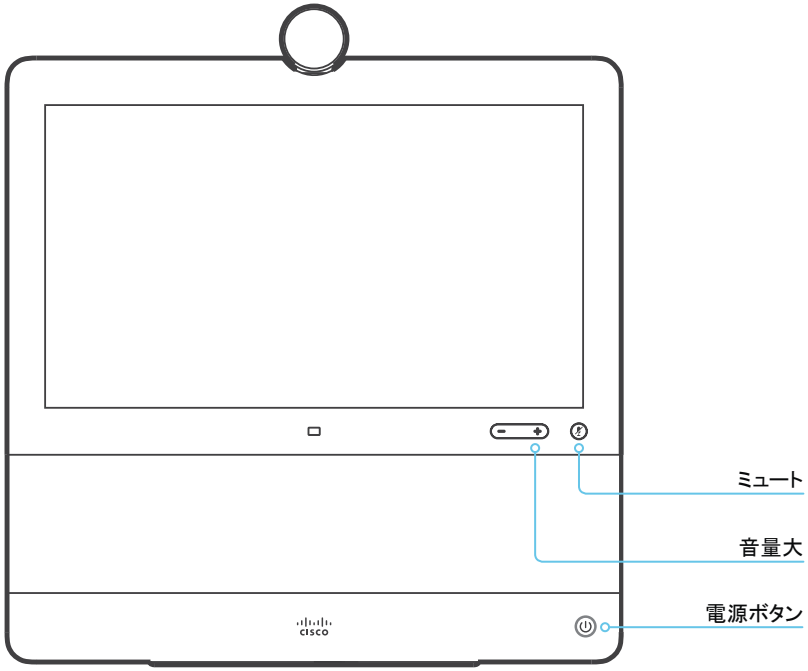
ミュート ボタンと音量ボタンを使用した DX70 の工場出荷時設定へのリセット

次の手順を実行して、起動時に DX70 を工場出荷時設定にリセットします。ビデオ システムの電源がオンになっている場合、先に進む前に電源ボタンを押して、システムがシャットダウンするまで押し続けます。

1. *ミュート* ボタン(LED)と*音量アップ* ボタン(LED)を探してください。
2. 電源ボタンを押して、*ミュート* ボタンに注目してください。
3. *ミュート* ボタンが 2 回点滅したら、*音量アップ* ボタンを押し、そのすぐ後に約 4 秒間*ミュート* ボタンを押し続けます。このプロセス中に、*ミュート* ボタンが数秒間赤になります。

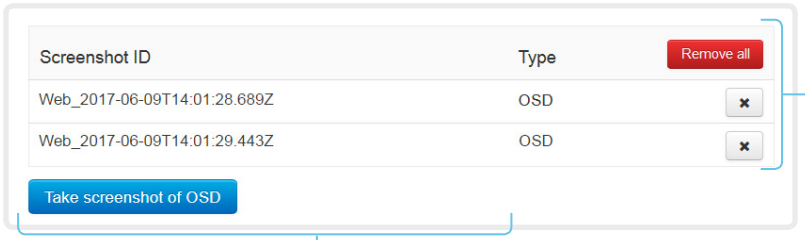
   ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了するとビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

   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

画面上の表示のスクリーンショットをキャプチャするには、*[OSD のスクリーンショットを撮る (Take screenshot of OSD)]* をクリックします。

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

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

スクリーンショットを削除する

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

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

ユーザ インターフェイスのスクリーンショットについて

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、およびメッセージ)のスクリーンショットをキャプチャできます。

第 5 章

システム設定

システム設定の概要

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

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

IP アドレスの確認方法

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

Audio 設定 82
Audio DefaultVolume 82
Audio Input MicrophoneMode 82
Audio Microphones Mute Enabled 82
Audio SoundsAndAlerts RingTone 82
Audio SoundsAndAlerts RingVolume 82
Audio Ultrasound MaxVolume 83
Audio Ultrasound Mode 83

Bluetooth 設定(Bluetooth settings) 84
Bluetooth Allowed 84
Bluetooth Enabled 84

CallHistory 設定 85
CallHistory Mode 85

Cameras 設定 86
Cameras Camera [1..1] Backlight DefaultMode 86

Conference 設定 87
Conference ActiveControl Mode 87
Conference AutoAnswer Delay 87
Conference AutoAnswer Mode 87
Conference AutoAnswer Mute 87
Conference CallProtocolIPStack 87
Conference DefaultCall Protocol 88
Conference DefaultCall Rate 88
Conference DoNotDisturb DefaultTimeout 88
Conference Encryption Mode 88
Conference FarEndControl Mode 88
Conference FarEndControl SignalCapability 89
Conference FarEndMessage Mode 89
Conference MaxReceiveCallRate 89
Conference MaxTotalReceiveCallRate 89
Conference MaxTotalTransmitCallRate 89
Conference MaxTransmitCallRate 89
Conference MicUnmuteOnDisconnect Mode 90
Conference Presentation OnPlacedOnHold 90
Conference VideoBandwidth Mode 90

FacilityService 設定 ... 91
FacilityService Service [1..5] CallType ... 91
FacilityService Service [1..5] Name ... 91
FacilityService Service [1..5] Number ... 91
FacilityService Service [1..5] Type ... 91

H323 設定 ... 92
H323 Authentication LoginName ... 92
H323 Authentication Mode ... 92
H323 Authentication Password ... 92
H323 CallSetup Mode ... 92
H323 Encryption KeySize ... 93
H323 Gatekeeper Address ... 93
H323 H323Alias E164 ... 93
H323 H323Alias ID ... 93
H323 NAT Address ... 94
H323 NAT Mode ... 93
H323 PortAllocation ... 94

Logging 設定 ... 95
Logging External Mode ... 95
Logging External Protocol ... 95
Logging External Server Address ... 95
Logging External Server Port ... 95
Logging Mode ... 95

Macros 設定 ... 96
Macros AutoStart ... 96
Macros Mode ... 96

Network 設定 ... 97
Network [1..1] DNS DNSSEC Mode ... 97
Network [1..1] DNS Domain Name ... 97
Network [1..1] DNS Server [1..3] Address ... 97
Network [1..1] IEEE8021X AnonymousIdentity ... 98
Network [1..1] IEEE8021X Eap Md5 ... 98
Network [1..1] IEEE8021X Eap Peap ... 99
Network [1..1] IEEE8021X Eap Tls ... 99
Network [1..1] IEEE8021X Eap Ttls ... 98
Network [1..1] IEEE8021X Identity ... 98
Network [1..1] IEEE8021X Mode ... 97
Network [1..1] IEEE8021X Password ... 98
Network [1..1] IEEE8021X TlsVerify ... 97
Network [1..1] IEEE8021X UseClientCertificate ... 98
Network [1..1] IPStack ... 99
Network [1..1] IPv4 Address ... 99
Network [1..1] IPv4 Assignment ... 99
Network [1..1] IPv4 Gateway ... 99
Network [1..1] IPv4 SubnetMask ... 100
Network [1..1] IPv6 Address ... 100
Network [1..1] IPv6 Assignment ... 100
Network [1..1] IPv6 DHCPOptions ... 100
Network [1..1] IPv6 Gateway ... 100
Network [1..1] MTU ... 101
Network [1..1] QoS Diffserv Audio ... 101
Network [1..1] QoS Diffserv Data ... 102
Network [1..1] QoS Diffserv ICMPv6 ... 102
Network [1..1] QoS Diffserv NTP ... 102
Network [1..1] QoS Diffserv Signalling ... 102
Network [1..1] QoS Diffserv Video ... 101
Network [1..1] QoS Mode ... 101
Network [1..1] RemoteAccess Allow ... 103
Network [1..1] Speed ... 103
Network [1..1] TrafficControl Mode ... 103
Network [1..1] VLAN Voice Mode ... 103
Network [1..1] VLAN Voice VlanId ... 103

NetworkPort 設定 ... 104
NetworkPort [2..2] Mode ... 104

NetworkServices 設定 ... 105
NetworkServices CDP Mode ... 105
NetworkServices H323 Mode ... 105
NetworkServices HTTP Mode ... 105
NetworkServices HTTP Proxy LoginName ... 105
NetworkServices HTTP Proxy Mode ... 106
NetworkServices HTTP Proxy PACUrl ... 106
NetworkServices HTTP Proxy Password ... 106
NetworkServices HTTP Proxy Url ... 106
NetworkServices HTTPS OCSP Mode ... 106
NetworkServices HTTPS OCSP URL ... 106

NetworkServices HTTPS Server MinimumTLSVersion ... 107
NetworkServices HTTPS StrictTransportSecurity ... 107
NetworkServices HTTPS VerifyClientCertificate ... 107
NetworkServices HTTPS VerifyServerCertificate ... 107
NetworkServices NTP Mode ... 107
NetworkServices NTP Server [1..3] Address ... 108
NetworkServices SIP Mode ... 108
NetworkServices SNMP CommunityName ... 108
NetworkServices SNMP Host [1..3] Address ... 108
NetworkServices SNMP Mode ... 108
NetworkServices SNMP SystemContact ... 108
NetworkServices SNMP SystemLocation ... 109
NetworkServices SSH AllowPublicKey ... 109
NetworkServices SSH HostKeyAlgorithm ... 109
NetworkServices SSH Mode ... 109
NetworkServices Telnet Mode ... 109
NetworkServices WelcomeText ... 109
NetworkServices Wifi Allowed ... 110
NetworkServices Wifi Enabled ... 110
NetworkServices XMLAPI Mode ... 110

Peripherals 設定 ... 111
Peripherals Profile ControlSystems ... 111

Phonebook 設定 ... 112
Phonebook Server [1..1] ID ... 112
Phonebook Server [1..1] Type ... 112
Phonebook Server [1..1] URL ... 112

Provisioning 設定 ... 113
Provisioning Connectivity ... 113
Provisioning ExternalManager Address ... 113
Provisioning ExternalManager AlternateAddress ... 113
Provisioning ExternalManager Domain ... 114
Provisioning ExternalManager Path ... 114
Provisioning ExternalManager Protocol ... 113
Provisioning LoginName ... 114
Provisioning Mode ... 114
Provisioning Password ... 115

Proximity 設定 ... 116
Proximity Mode ... 116
Proximity Services CallControl ... 116
Proximity Services ContentShare FromClients ... 116
Proximity Services ContentShare ToClients ... 116

RoomReset 設定 ... 117
RoomReset Control ... 117

RTP 設定 ... 118
RTP Ports Range Start ... 118
RTP Ports Range Stop ... 118
RTP Video Ports Range Start ... 118
RTP Video Ports Range Stop ... 118

Security 設定 ... 119
Security Audit Logging Mode ... 119
Security Audit OnError Action ... 119
Security Audit Server Address ... 119
Security Audit Server Port ... 120
Security Audit Server PortAssignment ... 120
Security Session FailedLoginsLockoutTime ... 120
Security Session InactivityTimeout ... 120
Security Session MaxFailedLogins ... 120
Security Session MaxSessionsPerUser ... 120
Security Session MaxTotalSessions ... 121
Security Session ShowLastLogon ... 121

SerialPort 設定 ... 122
SerialPort LoginRequired ... 122
SerialPort Mode ... 122

SIP 設定(SIP settings) ... 123
SIP ANAT ... 123
SIP Authentication Password ... 123
SIP Authentication UserName ... 123
SIP DefaultTransport ... 123
SIP DisplayName ... 123
SIP Ice DefaultCandidate ... 124
SIP Ice Mode ... 124
SIP Line ... 124

SIP ListenPort 124
SIP Mailbox 124
SIP MinimumTLSVersion 125
SIP PreferredIPMedia 125
SIP PreferredIPSignaling 125
SIP Proxy [1..4] Address 125
SIP TlsVerify 125
SIP Turn DiscoverMode 125
SIP Turn DropRflx 126
SIP Turn Password 126
SIP Turn Server 126
SIP Turn UserName 126
SIP Type 126
SIP URI 126

Standby 設定 127
Standby Control 127
Standby Delay 127
モーション検知ウェイクアップのスタンバイ 127

SystemUnit 設定 128
SystemUnit CrashReporting Advanced 128
SystemUnit CrashReporting Mode 128
SystemUnit CrashReporting Url 128
SystemUnit Name 128

Time 設定 129
Time DateFormat 129
Time TimeFormat 129
Time Zone 130

UserInterface 設定 132
UserInterface Accessibility IncomingCallNotification 132
UserInterface ContactInfo Type 132
UserInterface CustomMessage 132
UserInterface KeyTones Mode 133
UserInterface Language 133
UserInterface OSD EncryptionIndicator 133
UserInterface OSD HalfwakeMessage 133
UserInterface OSD Output 133
UserInterface Security Mode 134
UserInterface SettingsMenu Mode 134
UserInterface Wallpaper 134

UserManagement 設定 135
UserManagement LDAP Admin Filter 135
UserManagement LDAP Admin Group 135
UserManagement LDAP Attribute 135
UserManagement LDAP BaseDN 135
UserManagement LDAP Encryption 135
UserManagement LDAP MinimumTLSVersion 136
UserManagement LDAP Mode 136
UserManagement LDAP Server Address 136
UserManagement LDAP Server Port 136
UserManagement LDAP VerifyServerCertificate 136

Video 設定 137
Video ActiveSpeaker DefaultPIPPosition 137
Video DefaultLayoutFamily Local 137
Video DefaultLayoutFamily Remote 138
Video DefaultMainSource 138
Video Input Connector [1..2] CameraControl CameraId 138
Video Input Connector [1..2] CameraControl Mode 138
Video Input Connector [1..2] InputSourceType 138
Video Input Connector [1..2] Name 139
Video Input Connector [1..2] OptimalDefinition Profile 139
Video Input Connector [1..2] Visibility 140
Video Input Connector [2..2] PresentationSelection 139
Video Input Connector [2..2] Quality 140
Video Input Connector [2..2] RGBQuantizationRange 140
Video Monitors 140
Video Output Connector [1..1] Brightness 140
Video Output Connector [1..1] Resolution 141
Video Output Connector [1..1] Whitebalance Level 141
Video Presentation DefaultPIPPosition 141
Video Presentation DefaultSource 141
Video Selfview Default FullscreenMode 141
Video Selfview Default Mode 142
Video Selfview Default OnMonitorRole 142

Video Selfview Default PIPPosition....142
Video Selfview Mirrored....142
Video Selfview OnCall Duration....143
Video Selfview OnCall Mode....143

Experimental 設定....144

Audio 設定

Audio DefaultVolume

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

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: 50

値スペース:整数(0..100)

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

Audio Input MicrophoneMode

この設定は DX80 にだけ適用されます。

DX80 では両方の脚にマイクが搭載されています。マイク モードを Focused に設定すると、マイクを組み合わせて音声感度が高くなります。その結果、室内のノイズが聞こえなくなり、ビデオ システムの正面に座った人の声がよく聞こえるようになります。システムの正面に座っていない人の声は聞こえなくなります。

マイクロフォン モードを Wide に設定すると、システムは他のシステムと同様に動作します。横に座っている人の声が聞こえるようになり、また室内のノイズもより聞こえるようになります。

話者が 1 人のみの場合、Focused モードを使用することをお勧めします。システムの前で複数の人が話す場合は Wide モードを使用してください。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Wide

値スペース:Focused/Wide

Focused:1 点に集中された音の感度。ビデオ システムの真正面にないソースからの音は抑制されます。

Wide:デフォルトのマイク動作で、通常の音声感度です。

Audio Microphones Mute Enabled

ビデオ システムでのマイク ミュートの動作を決定します。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:True

値スペース:True/InCallOnly

True:音声ミュートが使用可能になります。

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

Audio SoundsAndAlerts RingTone

着信コールに使用する着信音を定義します。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値:Sunrise

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

リストから呼び出し音を選択します。

Audio SoundsAndAlerts RingVolume

着信コールの着信音量を定義します。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: 50

値スペース:整数(0..100)

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

Audio Ultrasound Mode

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Dynamic

値スペース:Dynamic/Static

Dynamic:ビデオ システムによって超音波ボリュームを動的に調整します。ボリュームは、[オーディオ ウルトラサウンド最大音量(Audio Ultrasound MaxVolume)] の設定で定義された最大レベルまでさまざまに変化します。

Static:シスコが助言した場合にのみ使用してください。

Audio Ultrasound MaxVolume

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:DX80:70 DX70:60

設定可能な値: DX80: 整数 (0 ～ 90) DX70: 整数 (0 ～ 60)

値は指定の範囲内から選択します。0 に設定すると、超音波がオフになります。

Bluetooth 設定(Bluetooth settings)

Bluetooth Allowed

ビデオ システムは、組み込みの Bluetooth モジュールを備えています。デフォルトで、ユーザはユーザ インターフェイスを使用してオンとオフを切り替えることができます。この設定を使用すると、管理者は Bluetooth 設定を無効にしてユーザ インターフェイスからセットアップできないようすることができます。

必要なユーザ ロール:ADMIN

デフォルト値:True

値スペース:False/True

False:管理者が Bluetooth をオフにし、ユーザーがユーザ インターフェイスからオンにすることはできません。

[はい(True)]:Bluetooth が許可されます。ユーザが ユーザ インターフェイスを使用してオンとオフを切り替えることができます。

Bluetooth Enabled

Bluetooth 接続が許可されている場合(Bluetooth 許可設定を参照)、この設定を使用して Bluetooth を有効および無効にすることができます。ビデオ システム は HFP(ハンズフリー プロファイル)と A2DP(高度なオーディオ配信プロファイル)のプロファイルをサポートします。A2DP だけをサポートするヘッドセットは使用できません。

必要なユーザ ロール:ADMIN

デフォルト値:False

値スペース:False/True

False:Bluetooth は無効になり、ビデオ システムと Bluetooth デバイスはペアリングできません。

[はい(True)]:Bluetooth が有効になり、ペアリングを行って Bluetooth ヘッドセットを使用することができます。

CallHistory 設定

CallHistory Mode

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:On

値スペース:Off/On

Off:新しいエントリが通話履歴に追加されません。

On:新しいエントリは通話履歴一覧に保存されます。

Cameras 設定

Cameras Camera [1..1] Backlight DefaultMode

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Off

値スペース:Off/On

Off:カメラの逆光補正をオフにします。

On:カメラの逆光補正をオンにします。

Conference 設定

Conference ActiveControl Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/Off

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

Off:アクティブ コントロールは無効です。

Conference AutoAnswer Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:[応答(Answer)] をタップして着信コールに応答できます。

On:通話中でない限り、システムが自動的に着信コールに応答します。常に手動で、通話中の着信コールの応答や拒否が行えます。

Conference AutoAnswer Mute

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:着信コールはミュートにされません。

On:着信コールは自動的に応答されるときミュートにされます。

Conference AutoAnswer Delay

システムによって自動的に応答される前に着信コールがどれくらい待つ必要があるかを定義します(秒単位)。[自動応答モード(AutoAnswer Mode)] が有効にされている必要があります。

必要なユーザ ロール:ADMIN

デフォルト値: 0

値スペース:整数(0..50)

自動応答遅延(秒単位)。

Conference CallProtocolIPStack

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

必要なユーザ ロール:ADMIN

デフォルト値:Dual

値スペース:Dual/IPv4/IPv6

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

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

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

Conference DefaultCall Protocol

システムからコールを発信するときに使用されるデフォルトの通信プロトコルを定義します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/H320/H323/Sip/Spark

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

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

H323:すべてのコールが H.323 コールとして設定されます。

SIP:すべてのコールが SIP コールとして設定されます。

Spark:Webex 登録済みシステムのために予約されています。使用しません。

Conference DefaultCall Rate

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: 3072

値スペース:整数(64..3072)

デフォルトのコール レート(帯域)(kbps)。

Conference DoNotDisturb DefaultTimeout

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: 60

値スペース:整数(1..1440)

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

Conference Encryption Mode

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

注:暗号化オプション キーがビデオ システムにインストールされていない場合、暗号化モードは常に Off になります。

必要なユーザ ロール:ADMIN

デフォルト値:BestEffort

値スペース:Off/On/BestEffort

Off:システムは、暗号化を使用しません。

On:システムは、暗号化されたコールだけを許可します。

BestEffort:システムは暗号化を可能な限り使用します。

> ポイント ツー ポイント コール:遠端システムで暗号化(AES-128)がサポートされている場合、コールは暗号化されます。そうでない場合は、コールは暗号化なしで送信されます。

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

Conference FarEndControl Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:遠端はこちら側のビデオ ソースの選択やローカル カメラの制御(パン、傾斜、ズーム)を許可されません。

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

Conference FarEndControl SignalCapability

遠端制御(H.224)信号機能モードを定義します。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:遠端制御信号機能をディセーブルにします。

On:遠端制御信号機能をイネーブルにします。

Conference FarEndMessage Mode

制御システムまたはマクロと併用するための、ポイントツーポイント通話における 2 種のコーデック間のデータ送信の許可状況を切り替えます。SIP コールでのみ動作します。この設定は、遠隔メッセージ送信コマンドの xCommand のコール使用を有効化または無効化します。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:2 つのコーデック間でメッセージ送信を行うことはできません。

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

Conference MaxReceiveCallRate

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

必要なユーザ ロール:ADMIN

デフォルト値: 3072

値スペース:整数(64..3072)

最大受信コール レート(帯域)(kbps)。

Conference MaxTransmitCallRate

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

必要なユーザ ロール:ADMIN

デフォルト値: 3072

値スペース:整数(64..3072)

最大送信コール レート(帯域)(kbps)。

Conference MaxTotalReceiveCallRate

受信全体の最大許容ビット レートを定義します。この製品は、同時に複数のコールをサポートしないため、合計送信帯域は 1 つのコールの送信ビット レートと同じになります(参照:会議の最大受信コール レート(Conference MaxReceiveCallRate) 設定)。

必要なユーザ ロール:ADMIN

デフォルト値: 3072

値スペース:整数(64..3072)

最大受信コール レート(帯域)(kbps)。

Conference MaxTotalTransmitCallRate

送信全体の最大許容ビット レートを定義します。この製品は、同時に複数のコールをサポートしないため、合計送信帯域は 1 つのコールの送信ビット レートと同じになります(参照:Conference MaxTransmitCallRate 設定)。

必要なユーザ ロール:ADMIN

デフォルト値: 3072

値スペース:整数(64..3072)

最大送信コール レート(帯域)(kbps)。

Conference MicUnmuteOnDisconnect Mode

すべてのコールが切断されたときに、マイクを自動的にミュート解除するかどうかを定義します。会議室またはその他の共有リソースでは、このようにして次のユーザのためにシステムを準備する場合があります。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

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

On:コールが切断された後にマイクロフォンのミュートを解除します。

Conference Presentation OnPlacedOnHold

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

必要なユーザ ロール:ADMIN

デフォルト値:NoAction

設定可能な値:NoAction/Stop

NoAction:保留にされてもビデオ システムはプレゼンテーションの共有を停止しません。保留されている間はプレゼンテーションは共有されませんが、コールが再開されると自動的に継続されます。

Stop:リモート サイトで保留状態にされた後、ビデオ システムはプレゼンテーションの共有を停止します。コールが再開されてもプレゼンテーションは継続されません。

Conference VideoBandwidth Mode

会議ビデオ帯域幅モードを定義します。

必要なユーザ ロール:ADMIN

デフォルト値:Dynamic

値スペース:Dynamic/Static

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

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

FacilityService 設定

FacilityService Service [1..5] Type

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Helpdesk

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

Catering:ケータリング サービスには、このオプションを選択します。

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

Emergency:緊急サービスには、このオプションを選択します。

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

Security:セキュリティ サービスには、このオプションを選択します。

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

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

FacilityService Service [1..5] Name

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

必要なユーザ ロール:ADMIN, INTEGRATOR

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

値スペース:文字列(0, 1024)

ファシリティ サービスの名前。

FacilityService Service [1..5] Number

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: ""

値スペース:文字列(0, 1024)

ファシリティ サービスの番号(URI または電話番号)。

FacilityService Service [1..5] CallType

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Video

値スペース:Audio/Video

Audio:オーディオ コールには、このオプションを選択します。

Video:ビデオ コールには、このオプションを選択します。

H323 設定

H323 Authentication Mode

H.323 プロファイルの認証モードを定義します。

必要なユーザ ロール:ADMIN
デフォルト値:Off

値スペース:Off/On

Off:システムは H.323 ゲートキーパーに対して自身の認証を試行せず、通常の登録を試行します。

On:認証が必要なことを H.323 ゲートキーパーから示されると、システムはゲートキーパーに対して自身の認証を試みます。コーデックとゲートキーパーの両方で、H323 Authentication LoginName と H323 Authentication Password の設定を定義する必要があります。

H323 Authentication LoginName

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

必要なユーザ ロール:ADMIN
デフォルト値: ""

値スペース:文字列(0, 50)

認証ログイン名。

H323 Authentication Password

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

必要なユーザ ロール:ADMIN
デフォルト値: ""

値スペース:文字列(0, 50)

認証パスワード。

H323 CallSetup Mode

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

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

必要なユーザ ロール:ADMIN
デフォルト値:Gatekeeper

値スペース:Direct/Gatekeeper

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

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

H323 Encryption KeySize

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

必要なユーザ ロール:ADMIN

デフォルト値:Min1024bit

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

Max1024bit:最大サイズは 1024 ビットです。

Min1024bit:最小サイズは 1024 ビットです。

Min2048bit:最小サイズは 2048 ビットです。

H323 Gatekeeper Address

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

H323 H323Alias E164

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 30)

H.323 エイリアス E.164 アドレス。使用できる文字は、0 ～ 9, *, # です。

H323 H323Alias ID

H.323 ゲートキーパー上のシステムのアドレス指定に使用され、コール リストに表示される H.323 エイリアス ID を定義します。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 49)

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

H323 NAT Mode

ファイアウォール トラバーサル テクノロジーは、ファイアウォール障壁を通過するセキュアなパスを作成し、外部のビデオ会議システムに接続されたときの音声/ビデオ データの正しい交換を可能にします(IP トラフィックが NAT ルータを通過する場合)。注:NAT は、ゲートキーパーとの組み合わせでは動作しません。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Auto/Off/On

Auto:H323 NAT アドレスと実際の IP アドレスのどちらをシグナリングに使用するかをシステムが決定します。これにより、LAN 上のエンドポイント、または WAN のエンドポイントにコールを発信できるようになります。H323 NAT アドレスが間違っているか設定されていない場合、実際の IP アドレスが使用されます。

Off:システムは、実際の IP アドレスをシグナリングします。

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

H323 NAT Address

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

ルータで、次のポートはシステムの IP アドレスにルーティングする必要があります。

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

H323 PortAllocation

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

必要なユーザ ロール:ADMIN

デフォルト値:Dynamic

値スペース:Dynamic/Static

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

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

Logging 設定

Logging External Mode

ロギングにリモート syslog サーバを使用するかどうかを決定します。

必要なユーザ ロール:ADMIN
デフォルト値:Off

値スペース:Off/On
Off:リモート syslog サーバのロギングを無効にします。
On:リモート syslog サーバのロギングを有効にします。

Logging External Protocol

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

必要なユーザ ロール:ADMIN
デフォルト値:SyslogTLS

値スペース:Syslog/SyslogTLS
Syslog:プレーン テキストの syslog プロトコル。
SyslogTLS:syslog プロトコル over TLS。

Logging External Server Address

リモート syslog サーバの IP アドレス。

必要なユーザ ロール:ADMIN
デフォルト値: ""

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

Logging External Server Port

リモート syslog サーバがメッセージをリッスンするポート。0 に設定されている場合、ビデオ システムで標準の syslog ポートが使用されます。syslog の標準 syslog ポートは 514 で、TLS を使用した syslog の標準 syslog ポートは 6514 です。

必要なユーザ ロール:ADMIN
デフォルト値: 514

値スペース:整数(0..65535)
リモート syslog サーバが使用しているポート番号。0 は、ビデオ システムが標準 syslog ポートを使用することを意味します。

Logging Mode

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

必要なユーザ ロール:ADMIN
デフォルト値:On

値スペース:Off/On
Off:システムのロギング サービスを無効にします。
On:システムのロギング サービスを有効にします。

Macros 設定

Macros Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:このビデオ システム上でのマクロの使用を完全に無効にします。

On:このビデオ システム上でのマクロの使用を有効にします。

Macros AutoStart

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:ビデオ システムの再起動後、マクロ ランタイムは自動的に開始しません。

On:ビデオ システムの再起動後、マクロ ランタイムが自動的に開始します。

Network 設定

Network [1..1] DNS DNSSEC Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:ドメイン ネーム システム セキュリティ拡張を無効にします。

On:ドメイン ネーム システム セキュリティ拡張を有効にします。

Network [1..1] DNS Domain Name

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

DNS ドメイン名。

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [1..1] IEEE8021X Mode

システムは、イーサネット ネットワークに認証済みネットワーク アクセスを提供するために使用される、ポート ベースのネットワーク アクセス コントロールによって、IEEE 802.1X LAN ネットワークに接続できます。

必要なユーザ ロール:ADMIN, USER

デフォルト値:Off

値スペース:Off/On

Off:802.1X 認証が無効になります。

On:802.1X 認証がイネーブルになります。

Network [1..1] IEEE8021X TlsVerify

TLS を使用する場合の、ローカル CA リストの証明書に対する IEEE802.1x 接続のサーバ側証明書の検証です。CA リストはビデオ システムにアップロードする必要があります。これは、Web インターフェイスから実行できます。

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Off

値スペース:Off/On

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

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

Network [1..1] IEEE8021X UseClientCertificate

IEEE802.1x 接続中の、秘密キーと証明書のペアを使用した認証。認証 X.509 証明書は、ビデオ システムにアップロードされている必要があります。これは、Web インターフェイスから実行できます。

必要なユーザ ロール:ADMIN, USER

デフォルト値:Off

値スペース:Off/On

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

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

Network [1..1] IEEE8021X Identity

802.1X 認証用のユーザ名を定義します。

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

802.1 X 認証用のユーザ名。

Network [1..1] IEEE8021X Password

802.1X 認証用のパスワードを定義します。

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 50)

802.1X 認証用のパスワード。

Network [1..1] IEEE8021X AnonymousIdentity

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

802.1X 匿名 ID 文字列。

Network [1..1] IEEE8021X Eap Md5

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:On

値スペース:Off/On

Off:EAP-MD5 プロトコルはディセーブルになります。

On:EAP-MD5 プロトコルが有効になります。

Network [1..1] IEEE8021X Eap Ttls

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:On

値スペース:Off/On

Off:EAP-TTLS プロトコルはディセーブルになります。

On:EAP-TTLS プロトコルが有効になります。

Network [1..1] IEEE8021X Eap Tls

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:On

値スペース:Off/On

Off:EAP-TLS プロトコルはディセーブルになります。

On:EAP-TLS プロトコルが有効になります。

Network [1..1] IEEE8021X Eap Peap

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:On

値スペース:Off/On

Off:EAP-PEAP プロトコルはディセーブルになります。

On:EAP-PEAP プロトコルが有効になります。

Network [1..1] IPStack

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Dual

値スペース:Dual/IPv4/IPv6

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

IPv4:[IPv4] に設定すると、システムのネットワーク インターフェイスで IPv4 が使用されます。

IPv6:[IPv6] に設定すると、システムのネットワーク インターフェイスで IPv6 が使用されます。

Network [1..1] IPv4 Assignment

システムが IPv4 アドレス、サブネット マスク、およびゲートウェイ アドレスを取得する方法を定義します。

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:DHCP

値スペース:Static/DHCP

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

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

Network [1..1] IPv4 Address

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効な IPv4 アドレス。

Network [1..1] IPv4 Gateway

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効な IPv4 アドレス。

Network [1..1] IPv4 SubnetMask

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

必要なユーザ ロール:ADMIN, USER
デフォルト値: ""

値スペース:文字列(0, 64)
有効な IPv4 アドレス。

Network [1..1] IPv6 Assignment

システムが IPv6 アドレスおよびデフォルト ゲートウェイ アドレスを取得する方法を定義します。
アドレス割り当てに DHCPv6 を利用する場合は、MAC アドレスによって最後に付加される「01」が、DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール:ADMIN, USER
デフォルト値:Autoconf

値スペース:Static/DHCPv6/Autoconf
Static:コーデックおよびゲートウェイの IP アドレスは、Network IPv6 Address および Network IPv6 Gateway の各設定を使用して手動で設定する必要があります。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。
DHCPv6:オプションを含むすべての IPv6 アドレスは、DHCPv6 サーバから取得されます。詳細については RFC3315 を参照してください。Network IPv6 DHCPOption 設定は無視されます。
Autoconf:IPv6 ネットワーク インターフェイスの IPv6 ステートレス自動設定をイネーブルにします。詳細については RFC4862 を参照してください。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。

Network [1..1] IPv6 Address

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

必要なユーザ ロール:ADMIN, USER
デフォルト値: ""

値スペース:文字列(0, 64)
ネットワーク マスクを含む有効な IPv6 アドレス。例:2001:DB8::/48

Network [1..1] IPv6 Gateway

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

必要なユーザ ロール:ADMIN, USER
デフォルト値: ""

値スペース:文字列(0, 64)
有効な IPv6 アドレス。

Network [1..1] IPv6 DHCPOptions

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

必要なユーザ ロール:ADMIN, USER
デフォルト値:On

値スペース:Off/On
Off:DHCPv6 サーバからの DHCP オプションの取得を無効にします。
On:選択した DHCP オプションのセットの DHCPv6 サーバからの取得をイネーブルにします。

Network [1..1] MTU

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 1500

値スペース:整数(576..1500)

MTU の値を設定します(バイト単位)。

Network [1..1] QoS Mode

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Diffserv

値スペース:Off/Diffserv

Off:QoS メソッドは使用されません。

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

Network [1..1] QoS Diffserv Audio

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

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 0

値スペース:整数(0..63)

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

Network [1..1] QoS Diffserv Video

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

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 0

値スペース:整数(0..63)

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

Network [1..1] QoS Diffserv Data

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

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 0

値スペース:整数(0..63)

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

Network [1..1] QoS Diffserv Signalling

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

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

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 0

値スペース:整数(0..63)

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

Network [1..1] QoS Diffserv ICMPv6

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

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

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 0

値スペース:整数(0..63)

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

Network [1..1] QoS Diffserv NTP

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

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 0

値スペース:整数(0..63)

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

Network [1..1] RemoteAccess Allow

リモート アクセスで SSH/Telnet/HTTP/HTTPS からコーデックに許可する IP アドレス(IPv4/IPv6)を定義します。複数の IP アドレスはスペースで区切られます。

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0..255)

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [1..1] Speed

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Auto

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

Auto:リンク速度を自動でネゴシエートします。

10half:10 Mbps 半二重に強制リンクします。

10full:10 Mbps 全二重に強制リンクします。

100half:100 Mbps 半二重に強制リンクします。

100full:100 Mbps 全二重に強制リンクします。

1000full:1 Gbps 全二重に強制リンクします。

Network [1..1] TrafficControl Mode

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:On

値スペース:Off/On

Off:ビデオ パケットをリンク速度で送信します。

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

Network [1..1] VLAN Voice Mode

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Auto

値スペース:Auto/Manual/Off

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

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

Off:VLAN はイネーブルになりません。

Network [1..1] VLAN Voice VlanId

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: 1

値スペース:整数(1..4094)

VLAN 音声 ID を設定します。

NetworkPort 設定

NetworkPort [2..2] Mode

ビデオ システムには、2 つのネットワーク ポートがあります。最初のネットワーク ポートは、ビデオ システムをイーサネット LAN に接続するためのものです。2 番目のネットワーク ポート(コンピュータ ネットワーク ポートとも呼ばれます)では、ビデオ システムを介してイーサネット LAN にコンピュータを接続することができます。このように、ネットワーク コンセントが 1 つあればビデオ システムとコンピュータの両方をサポートすることができます。

公共の場所でビデオ システムを使用する場合は、ユーザがビデオ システムを介してコンピュータをネットワーク接続することを防ぐため、このネットワーク ポートを無効にすることをお勧めします。

この設定への変更を反映させるには、ビデオ システムを再起動する必要があります。

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:コンピュータ ネットワーク ポートが無効です。

On:コンピュータ ネットワーク ポートは使用可能です。

NetworkServices 設定

NetworkServices CDP Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:CDP デーモンは無効です。

On:CDP デーモンは有効です。

NetworkServices H323 Mode

システムで H.323 コールの発信および受信を可能にするかどうかを定義します。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:H.323 コールの発信と受信の可能性をディセーブルにします。

On:H.323 コールの発信と受信の可能性を有効にします。

NetworkServices HTTP Mode

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

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

注:以前のソフトウェア バージョンから CE9.4(以降)にアップグレードされ、アップグレード後に工場出荷時の設定にリセットされていない状態で提供されるビデオシステムについて、デフォルト値は HTTP + HTTPS となります。

必要なユーザ ロール:ADMIN

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

値スペース:Off/HTTP+HTTPS/HTTPS

Off:HTTP や HTTPS によるビデオ システムへのアクセスを禁止します。

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

HTTPS:HTTPS によるビデオ システムへのアクセスを許可し、HTTP によるアクセスを禁止します。

NetworkServices HTTP Proxy LoginName

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 80)

認証ログイン名。

NetworkServices HTTP Proxy Password

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

認証パスワード。

NetworkServices HTTP Proxy Mode

Cisco Webex の HTTP プロキシを手動でセットアップすることができます。自動設定(PACUrl), 完全自動(WPAD), またはオフにしておくことができます。

必要なユーザ ロール:ADMIN, USER

デフォルト値:Off

値スペース:Manual/Off/PACUrl/WPAD

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

Off:HTTP プロキシ モードがオフになっています。

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

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

NetworkServices HTTP Proxy Url

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0..255)

HTTP プロキシ サーバの URL。

NetworkServices HTTP Proxy PACUrl

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0..255)

PAC (プロキシ自動構成) スクリプトの URL。

NetworkServices HTTPS OCSP Mode

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

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:OCSP サポートをディセーブルにします。

On:OCSP サポートをイネーブルにします。

NetworkServices HTTPS OCSP URL

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

有効な URL。

NetworkServices HTTPS Server MinimumTLSVersion

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

必要なユーザ ロール:ADMIN

デフォルト値:TLSv1.1

値スペース:TLSv1.1/TLSv1.2

TLSv1.1:TLS バージョン 1.1 以降のサポート

TLSv1.2:TLS バージョン 1.2 以降のサポート

NetworkServices HTTPS StrictTransportSecurity

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

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

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

NetworkServices HTTPS VerifyServerCertificate

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:サーバ証明書を確認しません。

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

NetworkServices HTTPS VerifyClientCertificate

ビデオ システムが HTTPS クライアント(Web ブラウザなど)に接続すると、クライアントは自分自身を識別するためにビデオ システムに証明書を提示するように要求されることがあります。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:クライアント証明書を確認しません。

On:信頼できる認証局(CA)によって署名された証明書を提示するようクライアントに要求します。これには、信頼できる CA のリストがシステムに事前にアップロードされている必要があります。

NetworkServices NTP Mode

ネットワーク タイム プロトコル(NTP)は、リファレンス タイム サーバにシステムの時刻と日付を同期するために使用されます。時間の更新のために、タイム サーバに定期的に照会します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/Manual/Off

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

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

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

NetworkServices NTP Server [1..3] Address

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

必要なユーザ ロール:ADMIN

デフォルト値:"0.tandberg.pool.ntp.org"

値スペース:文字列(0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

NetworkServices SIP Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:SIP コールの発信と受信の可能性をディセーブルにします。

On:SIP コールの発信と受信の可能性を有効にします。

NetworkServices SNMP Mode

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:ReadOnly

値スペース:Off/ReadOnly/ReadWrite

Off:SNMP ネットワーク サービスをディセーブルにします。

ReadOnly:SNMP ネットワーク サービスを照会のみイネーブルにします。

ReadWrite:SNMP ネットワーク サービスの照会とコマンドの両方をイネーブルにします。

NetworkServices SNMP Host [1..3] Address

最大 3 つの SNMP マネージャのアドレスを定義します。

システムの SNMP エージェント(コーデック内)は、システム ロケーションやシステム接点についてなど、SNMP マネージャ(PC プログラムなど)からのリクエストに応答します。SNMP トラップはサポートされていません。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: ""

値スペース:文字列(0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

NetworkServices SNMP CommunityName

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: ""

値スペース:文字列(0, 50)

SNMP コミュニティ名。

NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システムの連絡先の名前を定義します。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: ""

値スペース:文字列(0, 50)

SNMP システム接点の名前。

NetworkServices SNMP SystemLocation

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

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

値スペース:文字列(0, 50)
SNMP システム ロケーションの名前。

NetworkServices SSH Mode

SSH(または Secure Shell)プロトコルは、コーデックとローカル コンピュータ間でのセキュアな暗号化通信を提供できます。

必要なユーザ ロール:ADMIN
デフォルト値:On

値スペース:Off/On
Off:SSH プロトコルはディセーブルになります。
On:SSH プロトコルはイネーブルになります(デフォルト)。

NetworkServices SSH HostKeyAlgorithm

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

必要なユーザ ロール:ADMIN
デフォルト値:RSA

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

NetworkServices SSH AllowPublicKey

Secure Shell(SSH)公開キー認証をコーデックへのアクセスに使用できます。

必要なユーザ ロール:ADMIN
デフォルト値:On

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

NetworkServices Telnet Mode

Telnet は、インターネットまたはローカル エリア ネットワーク(LAN)接続で使用されるネットワーク プロトコルです。

必要なユーザ ロール:ADMIN
デフォルト値:Off

値スペース:Off/On
Off:Telnet プロトコルはディセーブルになります。これが出荷時の設定です。
On:Telnet プロトコルはイネーブルになります。

NetworkServices WelcomeText

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

必要なユーザ ロール:ADMIN
デフォルト値:On

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

NetworkServices Wifi Allowed

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

このシステムは次の標準規格をサポートしています:IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, および IEEE 802.11n。システムは次のセキュリティ プロトコルをサポートしています:WPA-EAP-PEAP, WPA-EAP-TLS, WPA-EAP-TTLS, WPA-EAP-FAST, WPA-EAP-MSCHAPv2, WPA-EAP-GTC, WPA-PSK(AES), WPA2-PSK(AES)およびオープン ネットワーク(セキュリティが保護されていない)。

ビデオ システムの背面の定格ラベルに記載されている PID (製品 ID)に NR (無線なし)の文字が含まれている場合、システムは Wi-Fi をサポートしていません。

必要なユーザ ロール:ADMIN, USER

デフォルト値:True

値スペース:False/True

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

True:イーサネットと Wi-Fi の両方を使用できます。

NetworkServices Wifi Enabled

ビデオ システムが Wi-Fi 経由でのネットワーク接続を許可されていれば(NetworkServices WIFI Allowed 設定を参照)、この設定を使用して Wi-Fi を有効および無効にすることができます。

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:True

値スペース:False/True

False:Wi-Fi は無効になります。

True:Wi-Fi が有効になります。

NetworkServices XMLAPI Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:XML API は無効になります。

On:XML API は有効になります。

Peripherals 設定

Peripherals Profile ControlSystems

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

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:NotSet

値スペース:1/NotSet

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

NotSet:サードパーティ製の制御システムの存在に対するチェックは実行されません。

Phonebook 設定

Phonebook Server [1..1] ID

外部の電話帳の名前を定義します。

必要なユーザ ロール:ADMIN
デフォルト値:""

値スペース:文字列(0, 64)
外部の電話帳の名前。

Phonebook Server [1..1] Type

電話帳サーバの種類を選択します。

必要なユーザ ロール:ADMIN
デフォルト値:Off

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

Phonebook Server [1..1] URL

外部電話帳サーバへのアドレス(URL)を定義します。

必要なユーザ ロール:ADMIN
デフォルト値:""

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

Provisioning 設定

Provisioning Connectivity

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Auto

値スペース:Internal/External/Auto

Internal:内部コンフィギュレーションを要求します。

External:外部コンフィギュレーションを要求します。

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

Provisioning ExternalManager Address

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

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Provisioning ExternalManager AlternateAddress

エンドポイントが Cisco Unified Communications Manager(CUCM)でプロビジョニングされており、代替 CUCM が冗長性に利用可能な場合にのみ使用できます。代替 CUCM のアドレスを定義します。主な CUCM が使用できない場合、エンドポイントは代替 CUCM でプロビジョニングされます。主な CUCM が再び使用可能になると、エンドポイントはこの CUCM によってプロビジョニングされます。

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Provisioning ExternalManager Protocol

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:HTTP

値スペース:HTTPS/HTTP

HTTPS:HTTPS を介してリクエストを送信します。

HTTP:HTTP を介してリクエストを送信します。

Provisioning ExternalManager Path

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0..255)

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

Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを定義します。

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効なドメイン名。

Provisioning Mode

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Auto

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

Off:ビデオ システムはプロビジョニング システムによって設定されません。

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

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

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

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

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

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

Provisioning LoginName

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

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 80)

有効なユーザ名。

Provisioning Password

これは、指定サーバとのビデオ システムの認証に使用されるクレデンシャルのパスワード部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。

必要なユーザ ロール:ADMIN, USER

デフォルト値: ""

値スペース:文字列(0, 64)

有効なパスワード。

Proximity 設定

Proximity Mode

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

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Off

値スペース:Off/On

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

[オン(On)]:ビデオ システムが超音波を発し、Proximity クライアントはビデオ システムに近接していることを検出できます。有効になっているプロキシミティ サービスを使用できます。

Proximity Services CallControl

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Disabled

値スペース:Enabled/Disabled

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

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

Proximity Services ContentShare FromClients

クライアントからのコンテンツ共有を有効または無効にします。この設定を有効にすると、ビデオ システムで無線によって Proximity クライアントからコンテンツを共有できます(ラップトップ画面の共有など)。このサービスはラップトップ(OS X および Windows)でサポートされます。この設定が機能するには、Proximity Mode を On にする必要があります。

必要なユーザ ロール:ADMIN, USER

デフォルト値:Enabled

値スペース:Enabled/Disabled

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

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

Proximity Services ContentShare ToClients

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Disabled

値スペース:Enabled/Disabled

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

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

RoomReset 設定

RoomReset Control

この設定は、コントロールシステムまたはマクロの使用に対するものです。マクロを使用して、ビデオ エンドポイントの一部を自動化できる JavaScript コードの一部を記述することができます。このようにしてカスタム動作を作成します。

ルームが数分に渡って待機状態になると、システムからルームがリセット準備完了状態であると伝えるイベントを送ることができます。

この設定が有効である場合に送られるイベントは次の通りです:

* e RoomReset SecondsToReset: 30

** end

* e RoomReset Reset

** end

必要なユーザ ロール:ADMIN

デフォルト値:On

設定可能な値:CameraPositionsOnly/Off/On(カメラポジションのみ/オフ/オン)

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

Off:ルームリセットイベントは送られません。

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

RTP 設定

RTP Ports Range Start

RTP ポート範囲の最初のポートを定義します。

デフォルトで、RTP および RTCP メディア データに 2326 ～ 2486 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100, RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP Video Ports Range が有効な場合、オーディオは RTP Ports Range 設定で定義された範囲を使用し、他のメディア データは RTP Video Ports Range 設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール:ADMIN

デフォルト値: 2326

値スペース:整数(1024..65438)

RTP ポート範囲内で最初のポートを設定します。

RTP Ports Range Stop

RTP ポート範囲の最後のポートを定義します。

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

RTP Video Ports Range が有効な場合、オーディオは RTP Ports Range 設定で定義された範囲を使用し、他のメディア データは RTP Video Ports Range 設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール:ADMIN

デフォルト値: 2486

値スペース:整数(1120..65535)

RTP ポート範囲内で最後のポートを設定します。

RTP Video Ports Range Start

RTP ビデオ ポート範囲の最初のポートを定義します。

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

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

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール:ADMIN

デフォルト値: 0

値スペース:整数(0, 1024..65454)

RTP ビデオ ポート範囲の最初のポートを設定します。

RTP Video Ports Range Stop

RTP ビデオ ポート範囲の最後のポートを定義します。

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

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

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール:ADMIN

デフォルト値: 0

値スペース:整数(0, 1024..65535)

RTP ビデオ ポート範囲の最後のポートを設定します。

Security 設定

Security Audit Logging Mode

監査ログを記録または送信する場所を定義します。監査ログは syslog サーバに送信されます。

External/ExternalSecure モードを使用し、[セキュリティ監査サーバ ポート割り当て(Security Audit Server PortAssignment)] 設定でポート割り当てを [手動(Manual)] に設定する場合は、[セキュリティ監査サーバ アドレス(Security Audit Server Address)] と [セキュリティ監査サーバのポート(Security Audit Server Port)] の設定で監査サーバのアドレスとポート番号も入力する必要があります。

必要なユーザ ロール:AUDIT

デフォルト値:Internal

設定可能な値:External/ExternalSecure/Internal/Off (外部/安全な外部/内部/オフ)

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

ExternalSecure:システムは監査 CA リストの証明書で検証された外部 syslog サーバに暗号化された監査ログを送信します。監査 CA リスト ファイルは、Web インターフェイスを使用してコーデックにアップロードする必要があります。CA のリストの証明書の common_name パラメータは syslog サーバの IP アドレスと一致する必要があり、セキュア TCP サーバでセキュア(TLS)TCP syslog メッセージをリッスンするように設定される必要があります。

Internal:システムは内部ログに監査ログを記録し、いっぱいになった場合はログをローテーションします。

Off:監査ロギングは実行されません。

Security Audit OnError Action

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

必要なユーザ ロール:AUDIT

デフォルト値:Ignore

値スペース:Halt/Ignore

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

Ignore:システムは、通常の動作を続行し、いっぱいになった場合は内部ログをローテーションします。接続が復元されると syslog サーバに再度監査ログを送信します。

Security Audit Server Address

監査ログは syslog サーバに送信されます。syslog サーバの IP アドレスを定義します。有効な IPv4 または IPv6 のアドレス形式のみが受け入れられます。ホスト名はサポートされていません。この設定は、Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール:AUDIT

デフォルト値: ""

値スペース:文字列(0..255)

有効な IPv4 アドレスまたは IPv6 アドレス。

Security Audit Server Port

監査ログは syslog サーバに送信されます。システムが監査ログを送信する syslog サーバのポートを定義します。この設定は、Security Audit PortAssignment が Manual に設定されている場合にのみ関連します。

必要なユーザ ロール:AUDIT

デフォルト値: 514

値スペース:整数(0..65535)

監査サーバのポートを設定します。

Security Audit Server PortAssignment

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

必要なユーザ ロール:AUDIT

デフォルト値:Auto

値スペース:Auto/Manual

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

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

Security Session FailedLoginsLockoutTime

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

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール:ADMIN

デフォルト値: 60

値スペース:整数(0..10000)

ロックアウト時間(分)を設定します。

Security Session InactivityTimeout

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

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール:ADMIN

デフォルト値: 0

値スペース:整数(0..10000)

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

Security Session MaxFailedLogins

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

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール:ADMIN

デフォルト値: 0

値スペース:整数(0..10)

ユーザ 1 人あたりの失敗できるログイン試行の最高回数を設定します。

Security Session MaxSessionsPerUser

ユーザ 1 人あたりの最大同時セッション数は 20 セッションです。

必要なユーザ ロール:ADMIN

デフォルト値: 20

値スペース:整数(1..20)

ユーザ 1 人あたりの最大同時セッション数を設定します。

Security Session MaxTotalSessions

同時セッションの合計最大数は 20 セッションです。

必要なユーザ ロール:ADMIN
デフォルト値: 20

値スペース:整数(1..20)
同時セッションの合計最大数を設定します。

Security Session ShowLastLogon

SSH または Telnet を使用してシステムにログインしたとき、前回ログインに成功したセッションの UserId、時刻および日付が表示されます。

必要なユーザ ロール:ADMIN
デフォルト値:Off

値スペース:Off/On
On:最後のセッションに関する情報を表示します。
Off:最後のセッションに関する情報を表示しません。

SerialPort 設定

SerialPort Mode

シリアル ポートを有効/無効にします。

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

値スペース:Off/On
Off:シリアル ポートをディセーブルにします。
On:シリアル ポートをイネーブルにします。

SerialPort LoginRequired

シリアル ポートに接続するときにログインが必要かどうかを定義します。

必要なユーザ ロール:ADMIN
デフォルト値:On

値スペース:Off/On
Off:ユーザはログインせずに、シリアル ポート経由でコーデックにアクセスできます。
On:シリアル ポート経由でコーデックに接続するときに、ログインが必要です。

SIP 設定(SIP settings)

SIP ANAT

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

必要なユーザ ロール:ADMIN
デフォルト値:Off

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

SIP Authentication UserName

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

必要なユーザ ロール:ADMIN
デフォルト値: ""

値スペース:文字列(0, 128)
有効なユーザ名。

SIP Authentication Password

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

必要なユーザ ロール:ADMIN
デフォルト値: ""

値スペース:文字列(0, 128)
有効なパスワード。

SIP DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール:ADMIN
デフォルト値:Auto

値スペース:Auto/TCP/TIs/UDP
TCP:システムはデフォルトの転送方法として常に TCP を使用します。
UDP:システムはデフォルトの転送方法として常に UDP を使用します。
TIs:システムはデフォルトの転送方法として常に TLS を使用します。TLS 接続の場合、SIP CA リストをビデオ システムにアップロードできます。このような CA リストがシステムにない場合は匿名の Diffie Hellman が使用されます。
Auto:システムは、TLS, TCP, UDP の順序でトランスポート プロトコルを使用して接続を試みます。

SIP DisplayName

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

必要なユーザ ロール:ADMIN
デフォルト値: ""

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

SIP Ice DefaultCandidate

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

必要なユーザ ロール：ADMIN

デフォルト値：Host

値スペース：Host/Rflx/Relay

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

Rflx：TURN サーバから見えるビデオ システムのパブリック IP アドレスにメディアを送信します。

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

SIP Ice Mode

ICE（Interactive Connectivity Establishment、RFC 5245）は、最適化されたメディア パスの検出にビデオ システムで使用できる NAT トラバーサル ソリューションです。そのため、音声とビデオの最短ルートがビデオ システム間で常に確保されます。

必要なユーザ ロール：ADMIN

デフォルト値：Auto

値スペース：Auto/Off/On

Auto：TURN サーバを指定した場合は、ICE が有効になります。それ以外の場合は、ICE が無効になります。

Off：ICE が無効になります。

On：ICE が有効になります。

SIP Line

Cisco Unified Communications Manager（CUCM）に登録すると、エンドポイントを共有回線の一部にできます。これは、複数のデバイスが同じディレクトリ番号を共有することを意味します。RFC 4235 で規定されているように、同じ番号を共有する各デバイスは、ライン上のもう一方のアピアランスからステータスを受け取ります。

共有回線はエンドポイントではなく CUCM によって設定されることに注意してください。そのため、手動でこの設定を変更しないでください。CUCM は必要に応じてこの情報をエンドポイントにプッシュします。

必要なユーザ ロール：ADMIN

デフォルト値：Private

値スペース：Private/Shared

Shared：システムは共有回線の一部であるため、ディレクトリ番号を他のデバイスと共有します。

Private：このシステムは共有回線の一部ではありません。

SIP ListenPort

SIP TCP/UDP ポートでの着信接続のリッスンをオンまたはオフにします。オフにした場合、エンドポイントは SIP レジストラ（CUCM または VCS）を介してのみ到達可能になります。

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：SIP TCP/UDP ポートでの着信接続のリッスンをオフにします。

On：SIP TCP/UDP ポートでの着信接続のリッスンをオンにします。

SIP Mailbox

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

必要なユーザ ロール：ADMIN

デフォルト値：""

値スペース：文字列（0, 255）

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

SIP MinimumTLSVersion

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

必要なユーザ ロール:ADMIN

デフォルト値:TLSv1.0

値スペース:TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0:TLS バージョン 1.0 以上をサポートします。

TLSv1.1:TLS バージョン 1.1 以上をサポートします。

TLSv1.2:TLS バージョン 1.2 以上をサポートします。

SIP PreferredIPMedia

メディア(音声、ビデオ、データ)を送受信するための優先 IP バージョンを定義します。[Network IPStack] および [Conference CallProtocolIPStack] の両方が [デュアル(Dual)] に設定されていて、ネットワークに優先 IP バージョンを選択するメカニズムがない場合にのみ使用可能です。

必要なユーザ ロール:ADMIN

デフォルト値:IPv4

値スペース:IPv4/IPv6

IPv4:メディアの優先 IP バージョンは IPv4 です。

IPv6:メディアの優先 IP バージョンは IPv6 です。

SIP PreferredIPSignaling

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

必要なユーザ ロール:ADMIN

デフォルト値:IPv4

値スペース:IPv4/IPv6

IPv4:シグナリングの優先 IP バージョンは IPv4 です。

IPv6:シグナリングの優先 IP バージョンは IPv6 です。

SIP Proxy [1..4] Address

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

SIP TlsVerify

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

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

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

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

SIP Turn DiscoverMode

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:検出モードを無効にします。

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

SIP Turn DropRflx

DropRflx は、リモート エンドポイントが同じネットワークにない場合に限り、TURN リレー経由でエンドポイントにメディアを強制させます。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:DropRflx を無効にします。

On:リモート エンドポイントが別のネットワークにある場合、TURN リレー経由でメディアを強制します。

SIP Turn Server

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

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

SIP Turn UserName

TURN サーバへのアクセスに必要なユーザ名を定義します。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 128)

有効なユーザ名。

SIP Turn Password

TURN サーバへのアクセスに必要なパスワードを定義します。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 128)

有効なパスワード。

SIP Type

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

必要なユーザ ロール:ADMIN

デフォルト値:Standard

値スペース:Standard/Cisco

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

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

SIP URI

SIP URI(Uniform Resource Identifier)は、ビデオ システムの識別に使用されるアドレスです。URI が登録され、SIP サービスによりシステムへの着信コールのルーティングに使用されます。SIP URI 構文は RFC 3261 で定義されています。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

SIP URI 構文に準拠したアドレス(URI)。

Standby 設定

Standby Control

システムがスタンバイ モードに移行するか否かを定義します。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:On

値スペース:Off/On

Off:システムはスタンバイ モードを開始しません。

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

Standby Delay

スタンバイ モードに入る前に、システムがアイドル モードのまま経過する時間の長さ(分単位)を定義します。[スタンバイ制御(Standby Control)] が有効である必要があります。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: 10

値スペース:整数(1..480)

スタンバイ遅延(分)を設定します。

モーション検知ウェイクアップのスタンバイ

動体検知自動ウェイク アップは、人が室内に入ってきたときに検知する機能です。この機能は、超音波での検知に基づいており、この機能を動作させるには [近接モード設定(Proximity Mode setting)] がオンである必要があります。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Off

値スペース:Off/On

Off:動体検知ウェイクアップは無効です。

On:人が部屋に入ってくると、システムが自動的にスタンバイからウェイクアップします(DX80にのみ適用)。

SystemUnit 設定

SystemUnit Name

システム名を定義します。コーデックが SNMP エージェントとして機能している場合に、システム名は DHCP リクエストでホスト名として送信されます。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 50)

システム名を定義します。

SystemUnit CrashReporting Advanced

ビデオ システム (コーデック) がクラッシュすると、システムは解析のために [シスコ自動クラッシュレポートツール(Cisco Automatic Crash Report tool)] (ACR)へログを自動的に送信できます。
ACR ツールは、シスコの内部使用のみであり、お客様は利用できません。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:ACR ツールは標準的なログ解析を実行します。

On:ACR ツールは高度なログ解析を実行します。

SystemUnit CrashReporting Mode

ビデオ システム (コーデック) がクラッシュすると、システムは解析のために [シスコ自動クラッシュレポートツール(Cisco Automatic Crash Report tool)] (ACR)へログを自動的に送信できます。
ACR ツールは、シスコの内部使用のみであり、お客様は利用できません。

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:ACR ツールにログは送信されません。

On:ACR ツールにログは自動的に送信されます。

SystemUnit CrashReporting Url

ビデオ システム (コーデック) がクラッシュすると、システムは解析のために [シスコ自動クラッシュレポートツール(Cisco Automatic Crash Report tool)] (ACR)へログを自動的に送信できます。
ACR ツールは、シスコの内部使用のみであり、お客様は利用できません。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

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

Time 設定

Time TimeFormat

時刻形式を定義します。

必要なユーザ ロール:ADMIN, USER
デフォルト値:24H

値スペース:24H/12H
24H:24 時間の時間フォーマットを設定します。
12H:12 時間(AM/PM)の時間フォーマットを設定します。

Time DateFormat

日付形式を定義します。

必要なユーザ ロール:ADMIN, USER
デフォルト値:DD_MM_YY

値スペース:DD_MM_YY/MM_DD_YY/YY_MM_DD
DD_MM_YY:2010 年 1 月 30 日は「30.01.10」と表示されます。
MM_DD_YY:2010 年 1 月 30 日は「01.30.10」と表示されます。
YY_MM_DD:2010 年 1 月 30 日は「10.01.30」と表示されます。

Time Zone

ビデオ システムが物理的に存在する地域のタイム ゾーンを設定します。値スペースの情報は、tz データベース（別名:IANA タイムゾーン データベース）から取得しています。

必要なユーザ ロール:ADMIN, INTEGRATOR, USER

デフォルト値:Etc/UTC

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

リストからタイム ゾーンを選択します。

UserInterface 設定

UserInterface Accessibility IncomingCallNotification

画面表示を強調した着信コールの通知を利用できます。画面と Touch 10 は約 1 秒ごと(1.75 Hz)に赤と白に点滅し、聴覚が不自由なユーザが着信コールに気づきやすくするようにしています。システムが通話中の場合、進行中の通話の妨げになるため画面は点滅しません、その代わり、通常の通知が画面とタッチパネルに表示されます。

必要なユーザ ロール:ADMIN, INTEGRATOR, USER

デフォルト値:Default

値スペース:AmplifiedVisuals/Default

AmplifiedVisuals:ビデオ システムが着信したときに画面とタッチパネル上での画面表示の強調を有効にします。

Default:スクリーンとタッチパネル上での通知を使用したデフォルトの動作を有効にします。

UserInterface ContactInfo Type

ユーザ インターフェイスで表示する連絡先の種類を選択します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/DisplayName/E164Alias/H320Number/H323Id/IPv4/IPv6/None/SipUri/SystemName

Auto:他のシステムがこのシステムに到達するためにダイヤルする必要があるアドレスを表示します。アドレスはデフォルトのコール プロトコルおよびシステム登録によって異なります。

None:どのようなコンタクト情報も表示しません。

IPv4:システムの IPv4 アドレスを示します。

IPv6:システムの IPv6 アドレスを示します。

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

H320Number:連絡先情報としてシステムの H.320 番号を表示します(Cisco TelePresence ISDN リンクを使用している場合のみサポート)。

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

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

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

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

UserInterface CustomMessage

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: ""

値スペース:文字列(0, 128)

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

UserInterface KeyTones Mode

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:Off

値スペース:Off/On

Off:キー トーンは再生されません。

On:キー トーンがオンになります。

UserInterface Language

ユーザ インターフェイスで使用される言語を選択します。該当する言語がサポートされていない場合、デフォルトの言語(英語)が使用されます。

必要なユーザ ロール:ADMIN, USER

デフォルト値:English

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

リストから言語を選択します。

UserInterface OSD EncryptionIndicator

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

必要なユーザ ロール:ADMIN

デフォルト値:Auto

値スペース:Auto/AlwaysOn/AlwaysOff

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

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

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

AlwaysOff:暗号化インジケータは画面上に表示されません。

UserInterface OSD HalfwakeMessage

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

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 128)

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

UserInterface OSD Output

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

必要なユーザ ロール:ADMIN、INTEGRATOR

デフォルト値:Auto

値スペース:Auto

Auto:オンスクリーン用の情報とインジケータをシステムの内蔵画面に送信します。

UserInterface Security Mode

この設定では、重要なシステム情報(例、ビデオ システムの連絡先情報や IP アドレス、タッチ コントローラ、および UCM/VCS レジストラ)がユーザ インターフェイス(ドロップダウン メニューと設定パネル)で公開されるのを防ぐことができます。設定パネルに移動するとこのような情報は非表示になっていないので注意してください。

管理者権限を持たない人に連絡先情報、IP アドレス、MAC アドレス、シリアル番号およびソフトウェアのバージョンを絶対に公開しない場合は、[ユーザ インターフェイス設定メニュー モード (UserInterface SettingsMenu Mode)] を [ロック(Locked)] に設定します。また、管理者権限を持つすべてのユーザ アカウントにパスフレーズを設定することも必要です。

必要なユーザ ロール:ADMIN

デフォルト値:Normal

値スペース:Normal/Strong

Normal:IP アドレスやその他のシステムの情報がユーザ インターフェイスに表示されます。

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

UserInterface SettingsMenu Mode

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

必要なユーザ ロール:ADMIN

デフォルト値:Unlocked

値スペース:Locked/Unlocked

Locked:管理者のユーザ名とパスフレーズによる認証が必要です。

Unlocked:認証は必要ありません。

UserInterface Wallpaper

アイドル状態のときのビデオ画面の背景画像(壁紙)を選択します。

Web インターフェイスを使用してビデオシステムにカスタムの壁紙をアップロードできます。サポートされるファイル形式は BMP, GIF, JPEG, PNG です。最大ファイル サイズは 4 MByte です。カスタム壁紙を使用すると、予定されている会議のクロックおよび一覧がメイン ディスプレイから削除されます。

必要なユーザ ロール:ADMIN, INTEGRATOR, USER

デフォルト値:Auto

値スペース:Auto/Custom/None

[自動(Auto)]:デフォルトの壁紙を使用します。

None:画面に背景イメージはありません。

Custom:画面の背景画像としてカスタムの壁紙を使用します。カスタム壁紙がシステムにアップロードされていない場合、設定がデフォルト値に戻ります。

UserManagement 設定

UserManagement LDAP Admin Filter

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

LDAP 管理者グループまたは LDAP 管理者フィルタを常に設定する必要があります。LDAP 管理者フィルタが優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても、ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0, 1024)

この文字列の構文については、LDAP の仕様を参照してください。例:"(| (memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

UserManagement LDAP Admin Group

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

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタは優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合、ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

AD グループの識別名。例:"CN=admin group, OU=company groups, DC=company, DC=com"

UserManagement LDAP Attribute

提供されるユーザ名へのマッピングに使用される属性。設定しない場合は、sAMAccountName が使用されます。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

属性名。

UserManagement LDAP BaseDN

検索を開始するエントリの識別名(ベース)。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

ベースの識別名。例:"DC=company, DC=com"

UserManagement LDAP Encryption

ビデオ システムと LDAP サーバとの間の通信を保護する方法を定義します。ポート番号は、UserManagement LDAP Server Port 設定を使用してポート番号をオーバーライドできます。

必要なユーザ ロール:ADMIN

デフォルト値:LDAPS

値スペース:LDAPS/None/STARTTLS

LDAPS:ポート 636 over TLS(Transport Layer Security)上の LDAP サーバに接続します。

None:ポート 389 上の LDAP サーバに接続します(暗号化なし)。

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

UserManagement LDAP MinimumTLSVersion

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

必要なユーザ ロール:ADMIN

デフォルト値:TLSv1.2

値スペース:TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0:TLS バージョン 1.0 以上をサポートします。

TLSv1.1:TLS バージョン 1.1 以上をサポートします。

TLSv1.2:TLS バージョン 1.2 以上をサポートします。

UserManagement LDAP Mode

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

LDAP モードをオンにする場合、設定に合わせたユーザ管理 LDAP 設定の構成を確認してください。いくつかの例を示します。

例 1:

- ユーザ管理 LDAP モード:On
- ユーザ管理 LDAP アドレス:"192.0.2.20"
- ユーザ管理 LDAP ベース DN:"DC=company, DC=com"
- ユーザ管理 LDAP 管理グループ:"CN=admin group, OU=company group, DC=company, DC=com"

例 2:

- ユーザ管理 LDAP モード:On
- ユーザ管理 LDAP アドレス:"192.0.2.20"
- ユーザ管理 LDAP ベース DN:"DC=company, DC=com"
- ユーザ管理 LDAP 管理フィルタ:"(| (memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

必要なユーザ ロール:ADMIN

デフォルト値:Off

値スペース:Off/On

Off:LDAP 認証は許可されません。

On: LDAP 認証は許可されます。

UserManagement LDAP Server Address

LDAP サーバの IP アドレスまたはホスト名を設定します。

必要なユーザ ロール:ADMIN

デフォルト値: ""

値スペース:文字列(0..255)

有効な IPv4 アドレス、IPv6 アドレス、またはホスト名。

UserManagement LDAP Server Port

LDAP サーバに接続するポートをオンに設定します。0 に設定した場合は、選択したプロトコルのデフォルトを使用します(「UserManagement LDAP Encryption 設定」を参照)。

必要なユーザ ロール:ADMIN

デフォルト値: 0

値スペース:整数(0..65535)

LDAP サーバのポート番号。

UserManagement LDAP VerifyServerCertificate

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

必要なユーザ ロール:ADMIN

デフォルト値:On

値スペース:Off/On

Off:ビデオ システムは LDAP サーバの証明書を検証しません。

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

Video 設定

Video ActiveSpeaker DefaultPIPPosition

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Current

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

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

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

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

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

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

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

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

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

Video DefaultLayoutFamily Local

ローカルで使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール:ADMIN

デフォルト値:Auto

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

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

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

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

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

Single:通話中のスピーカー、または(存在する場合)プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Video DefaultLayoutFamily Remote

リモート参加者が使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール:ADMIN
デフォルト値:Auto

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

Auto:ローカル レイアウト データベースによって指定される、デフォルト レイアウト ファミリが、リモート レイアウトとして使用されます。

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

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

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

Single:通話中のスピーカー、または(存在する場合)プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Video DefaultMainSource

発信を開始する際にデフォルトのメイン ビデオ ソースとして使用されるビデオ入力ソースを定義します。

必要なユーザ ロール:ADMIN, USER
デフォルト値: 1

値スペース:1

デフォルトのメイン ビデオ ソースとして使用されるソースを設定します。

Video Input Connector [1..2] CameraControl CameraId

カメラ ID は、ビデオ入力に接続されているカメラの一意の ID です。

必要なユーザ ロール:ADMIN, INTEGRATOR
デフォルト値:Connector n: 1(コネクタ n:1)

設定可能な値: Connector n: 1

カメラ ID は固定されており、変更できません。

Video Input Connector [1..2] CameraControl Mode

カメラを制御できるかどうかを定義します。この値は、コネクタ 1(内蔵カメラ)とコネクタ 2(HDMI)の両方について固定であり、変更することはできません。

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

設定可能な値:Connector n: Off

Off:カメラ制御をディセーブルにします。

Video Input Connector [1..2] InputSourceType

ビデオ入力に接続された入力ソースのタイプを選択します。
コネクタ 1 はシステムの内蔵カメラであることに注意してください。

必要なユーザ ロール:ADMIN, INTEGRATOR
デフォルト値:Connector 1:camera Connector 2:PC

設定可能な値:Connector 1:camera Connector 2:PC/camera/document_camera/mediaplayer/whiteboard/other(コネクタ 1:カメラ コネクタ2:パソコン/カメラ/ドキュメントカメラ/メディアプレーヤー/ホワイトボード/その他)

PC:コンピュータがビデオ入力に接続されている場合に使用します。

camera:カメラがビデオ入力に接続されている場合に使用します。

document_camera:ドキュメント カメラがビデオ入力に接続されている場合に使用します。

mediaplayer:メディア プレーヤーがビデオ入力に接続されている場合に使用します。

whiteboard:ホワイトボード カメラがビデオ入力に接続されている場合に使用します。

other:他のオプションが当てはまらない場合に使用します。

Video Input Connector [1..2] Name

ビデオ入力コネクタの名前を定義します。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Connector n: ""

値スペース:文字列(0, 50)

ビデオ入力コネクタの名前。

Video Input Connector [1..2] OptimalDefinition Profile

この設定は、対応する Video Input Connector [n] Quality 設定が Sharpness に設定されている場合には無効です。

最適鮮明度プロファイルは、ビデオ会議室の照明状態とカメラと品質を反映します。光の条件およびカメラの品質が優れているほど、プロファイルが高くなります。通常、Norma] または Medium プロファイルが推奨されます。ただし、光の条件が良い場合、特定のコール率の解像度を大きくするために、High プロファイルを設定できます。解像度は、発呼側と着信側の両方のシステムでサポートされている必要があります。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Medium

値スペース:Normal/Medium/High

Normal:照明が通常から不良の環境には、このプロファイルを使用します。解像度は控えめに設定されます。

Medium:安定した光条件および高品質なビデオ入力が必要です。一部のコール レートの場合、これは高解像度へ移動できます。

High:優れた全体的なエクスペリエンスを実現するには、理想に近いビデオ会議の光の状態および高品質なビデオ入力が必要です。相当高い解像度が使用されます。

Video Input Connector [2..2] PresentationSelection

ビデオ入力にプレゼンテーション ソースを接続するときの、ビデオ システムの動作を定義します。

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Connector n: Desktop

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

AutoShare:通話時に、ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると(たとえば接続されているコンピュータがスリープ モードから復帰するなど)、自動的に遠端とローカル画面に表示されます。ユーザ インターフェイス上で [共有(Share)] を選択する必要はありません。コールの発信時または応答時にプレゼンテーション ソースがすでに接続されている場合は、ユーザ インターフェイス上で [共有(Share)] を手動で選択する必要があります。

Desktop:ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると(たとえば接続されているコンピュータがスリープ モードから復帰するなど)、画面に表示されます。これは、アイドル状態のときと通話中のときの両方に適用されます。また、ビデオ入力のコンテンツは、通話の終了時にアクティブ入力であれば、画面に表示されたままとなります。

Manual:ユーザ インターフェイスで [共有(Share)] を選択するまでビデオ入力の内容は画面に表示されません。

OnConnect:ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが起動すると(たとえば接続されているコンピュータがスリープ モードから復帰するなど)、画面に表示されます。それ以外の場合は、Manual モードと同じ動作です。

Video Input Connector [2..2] Quality

ビデオのエンコーディングと送信のときには、高解像度と高フレーム レートとの間にトレード オフが存在します。一部のビデオ ソースでは、高フレーム レートが高解像度より重要である場合や、逆の場合もあります。この設定で、高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Connector n: Sharpness

設定可能な値:Connector n: Motion/Sharpness

Motion:できるだけ高いフレーム レートにします。通常、多数の参加者がいる場合や画像の動きが激しい場合など、高フレーム レートが必要なときに使用されます。

Sharpness:できるだけ高い解像度にします。詳細なイメージやグラフィックに高い品質が必要な場合に使用されます。

Video Input Connector [2..2] RGBQuantizationRange

ビデオ入力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していません。その場合、ソースの完全なイメージを取得するために、この設定を使用して設定を上書きできます。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Auto

値スペース:Auto/Full/Limited

Auto:RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて自動的に選択されます。CE ビデオ形式は、限定された量子化範囲レベルを使用します。IT ビデオ形式は、完全な量子化範囲レベルを使用します。

Full:完全な量子化の範囲。R, G, B の量子化範囲にはすべてのコード値(0 ～ 255)が含まれます。これは CEA-861-E で規定されています。

Limited:限定された量子化の範囲。極端なコード値を除いた R, G, B の量子化範囲(16 ～ 235)。これは CEA-861-E で規定されています。

Video Input Connector [1..2] Visibility

ユーザ インターフェイスのメニューにあるビデオ入力コネクタの表示を定義します。

コネクタ 1 はシステムの内蔵カメラであり、プレゼンテーション ソースとして使用できないことに注意してください。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Connector 1: Never Connector 2: IfSignal (コネクタ 1:表示しない コネクタ2:入力信号がある場合)

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

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

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

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

Video Monitors

モニタ レイアウト モードを定義します。ビデオ システムがサポートするスクリーンは 1 台のみのため、この値は固定で変更できないことに注意してください。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Single

値スペース:Single

Single:レイアウトは、ビデオ システムの画面に表示されます。

Video Output Connector [1..1] Brightness

ビデオ システムの内蔵スクリーンの明るさレベルを定義します。

必要なユーザ ロール:ADMIN, USER

デフォルト値: 80

値スペース:整数(0..100)

範囲:値は 0 ～ 100 である必要があります。

Video Output Connector [1..1] Resolution

内蔵画面の解像度と更新間隔。この値は固定されており、変更できません。

デフォルト値:Connector 1:1920_1080_60

値スペース:Connector 1:1920_1080_60

1920_1080_60:解像度は 1920 x 1080, 更新間隔は 60 Hz です。

Video Output Connector [1..1] Whitebalance Level

内蔵スクリーンの色温度(ホワイト バランス)を、4000 K(暖色)～ 9000 K(寒色)の間で調整します。

必要なユーザ ロール:ADMIN, USER

デフォルト値: 6500

値スペース:整数(4000..9000)

ケルビン単位の色温度。

Video Presentation DefaultPIPPosition

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Current

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

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

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

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

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

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

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

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

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

Video Presentation DefaultSource

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

必要なユーザ ロール:ADMIN, USER

デフォルト値:2

値スペース:2

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソース。

Video Selfview Default FullscreenMode

コール終了後に、メイン ビデオ ソース(セルフビュー)を全画面表示するか、小さいピクチャインピクチャ(PiP)として表示するかを定義します。この設定はセルフビューがオンになっている場合にのみ有効です(Video Selfview Default Mode の設定を参照)。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Current

値スペース:Off/Current/On

Off:セルフビューは PiP として表示されます。

Current:セルフビューの画像のサイズはコール終了時に未変更の状態に保たれます。つまりコール中に PiP であった場合はコール終了後にも PiP のままであり、コール中に全画面であった場合はコール終了後にも全画面のままです。

On:セルフビューの画像は全画面表示されます。

Video Selfview Default Mode

コール終了後にメイン ビデオ ソース(セルフビュー)を画面に表示するかどうかを定義します。セルフビュー ウィンドウの位置とサイズはそれぞれ、Video Selfview Default PIPPosition と Video Selfview Default FullscreenMode の設定によって決まります。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Current

値スペース:Off/Current/On

Off:セルフビューはコール退出時にオフにされます。

Current:セルフビューはそのままの状態で残ります。つまりコール中にオンであった場合はコール終了後にもオンのままであり、コール中にオフであった場合はコール終了後にもオフのままです。

On:セルフビューはコール退出時にオンにされます。

Video Selfview Default OnMonitorRole

コールの後にメイン ビデオ ソース(セルフビュー)を表示するスクリーンを決定します。ビデオ システムにはスクリーンが 1 台しかないため、この値は固定で変更できないことに注意してください。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:First

値スペース:First

First:セルフビューの画像は内蔵スクリーンに表示されます。

Video Selfview Default PIPPosition

コール終了後に小さいセルフビュー ピクチャインピクチャ(PiP)を表示する画面上の位置を定義します。この設定は、セルフビューがオンになっており(Video Selfview Default Mode 設定を参照)、全画面表示がオフになっている場合(Video Selfview Default FullscreenMode 設定を参照)にのみ有効です。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:Current

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

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

UpperLeft:セルフビュー PiP が画面の左上隅に表示されます。

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

UpperRight:セルフビュー PiP が画面の右上隅に表示されます。

CenterLeft:セルフビュー PiP が画面の左中央に表示されます。

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

LowerLeft:セルフビュー PiP が画面の左下隅に表示されます。

LowerRight:セルフビュー PiP が画面の右下隅に表示されます。

Video Selfview Mirrored

他人から見えているように自分の画像を表示したり、鏡に映っているように自分の画像を表示するようにビデオ システムを設定できます。

この設定は、遠方に送信されるビデオに影響を与えません。

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:On

値スペース:Off/On

Off:他人から見えている自分のようにセルフビュー画像を表示します。

On:鏡に映っている自分のようにセルフビュー画像を表示します。

Video Selfview OnCall Mode

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値:On

値スペース:Off/On

Off:セルフ ビューはコール セットアップ中に自動的に表示されません。

On:セルフ ビューはコール セットアップ中に自動的に表示されます。

Video Selfview OnCall Duration

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

必要なユーザ ロール:ADMIN, INTEGRATOR

デフォルト値: 10

値スペース:整数(1..60)

範囲:セルフ ビューをオンにする期間を選択します。有効な範囲は、1 ～ 60 秒です。

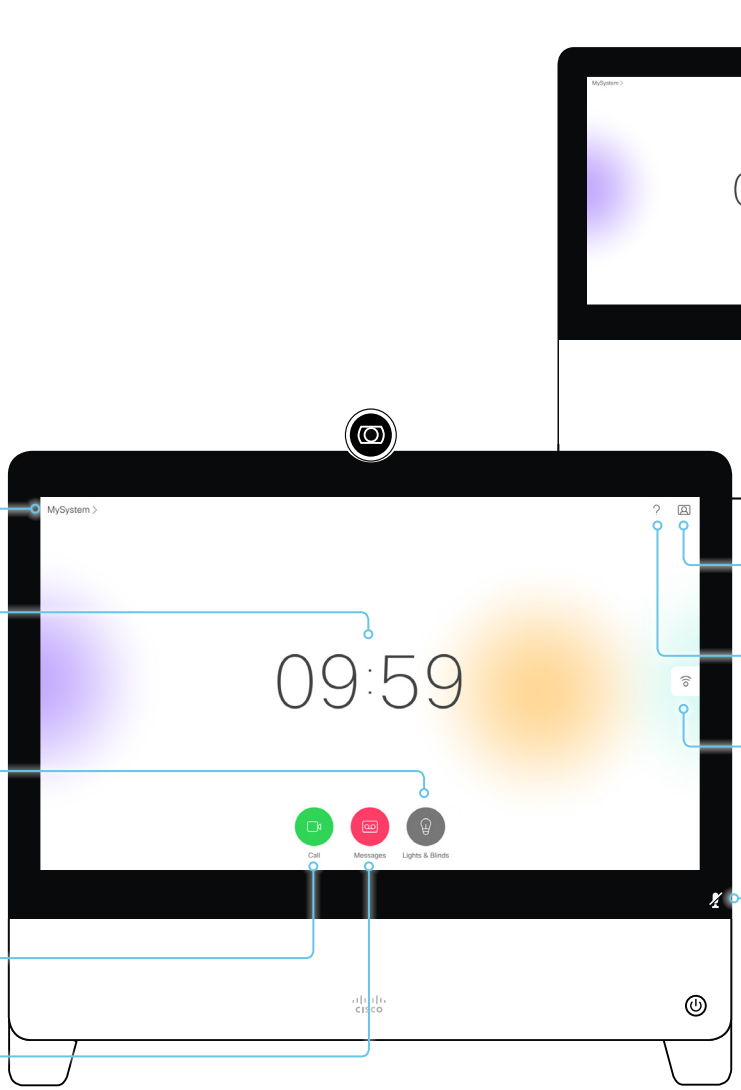
Experimental 設定

試験的設定は、テストのためだけのもので、シスコと同意したのでない限り使用できません。これらの設定は記載されておらず、以降のリリースで変更されます。

付録

ユーザ インターフェイス

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



システム名または連絡先情報をタップして、*[システム情報(System Information)]*、*[設定(Settings)]*、*[再起動(Restart)]* および *[初期設定へのリセット(Factory Reset)]* にアクセスします。画面の明るさを調整し、*コール転送モード*、*スタンバイ モード*、*応答不可モード*をアクティブにすることもできます。

時刻を指定します。

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

[発信(Call)] をタップすると、*[お気に入り(Favorites)]* リスト、*[ディレクトリ(Directory)]* リスト、*[発着信履歴(Recents)]* リストなどの連絡先を呼び出したり、*[検索またはダイヤル(Search or Dial)]* フィールドを開いたりできます。

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

装置の右側:
- ヘッドセット用の USB ソケットとミニジャック ソケット

マイク:
ミュート/ミュート解除。

スピーカーの音量コントロール。

セルフビュー:オン/オフ

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

Proximity を使用して 1 つ以上のクライアントがシステムとペアになっていることを示します。

マイクのミュート インジケータ。

装置の右側:
- マイクのミュート ボタン
- スピーカーの音量コントロール
- ヘッドセット用の USB ソケット

リモート モニタリングのセットアップ

要件:

- *RemoteMonitoring* オプション

リモート モニタリングは別の場所からビデオ システムを制御する場合に便利です。

入力ソースからのスナップショットが Web インターフェイスに表示されるため、部屋にいなくてもカメラ ビューをチェックしてカメラを制御できます。

有効にすると、スナップショットは約 5 秒おきに自動的に更新されます。

ビデオ システムに *RemoteMonitoring* オプションがあるかどうかを確認する

1. Web インターフェイスにログインします。
2. [ホーム(Home)] ページで、インストールされているオプションのリストに *RemoteMonitoring* が含まれているかどうかを確認します。

   リストにない場合、リモート モニタリングは使用できません。

リモート モニタリングを有効にする

RemoteMonitoring オプション キーをインストールします。オプション キーのインストール方法については、▶「オプション キーを追加する」の章で説明しています。

リモート モニタリング オプションを有効にする場合は、プライバシーに関する地域の法律および規制を遵守する必要があります。また、システム管理者がカメラや画面を監視および制御する場合があることを、システムのユーザに適切な方法で通知してください。システムの使用時にプライバシー規制を遵守するのはお客様の責任であり、シスコはこの機能の違法な使用について一切の責任を否認します。

スナップショットについて

ローカル入力ソース

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は [コール制御(Call Control)] ページに表示されます。

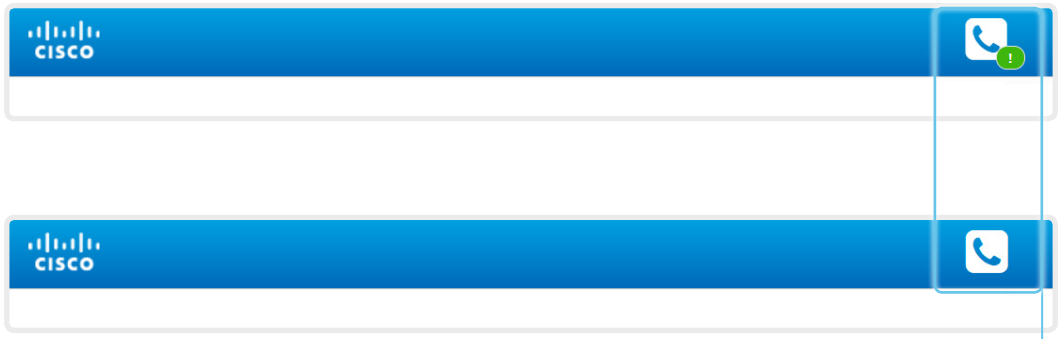
スナップショットは、ビデオ システムがアイドル状態のときにも、通話中にも表示されます。

遠端のスナップショット

通話中の場合、遠端カメラからのスナップショットも表示できます。遠端ビデオ システムに *[リモート モニタリング(RemoteMonitoring)]* オプションがあるかどうかは問題ではありません。

遠端スナップショットは、コールが暗号化されていると表示されません。

Web インターフェイスを使用したコール情報へのアクセスとコール応答



着信通知

*[コールインジケーター(Call indicator)]*をクリックし、コールの応答と拒否を行う*[コール操作(Call Control)]*ページを開きます。

システムが通話中

コールインジケーター

コールインジケーターでは着信の通知表示と、システムが通話中になる時を表示します。

システムが待機状態の場合、コールインジケーターは表示されません。

コールの操作

*[コール操作(Call Control)]*ページでは、コール操作に関係するボタンが表示されます。各ボタンを使用して次のことを実行します。

- コールの詳細を表示する
- コールを保留にする
- 通話に応答します。
- コールを切断する

Web インターフェイスを使用してコールを発信する (1/2 ページ)

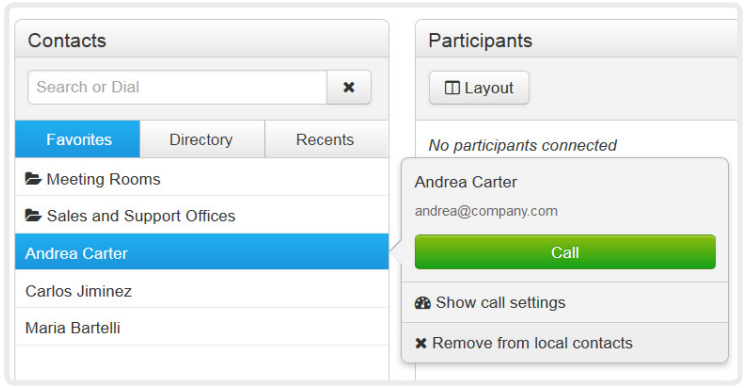
Web インターフェイスにログインし、*[コール制御(Call Control)]* に移動します。

コールの発信

Web インターフェイスを使ってコールを開始した場合でも、コールに使用されるのはビデオ システム(ディスプレイ、マイクおよびスピーカー)であり、Web インターフェイスを実行する PC ではありません。

1. 正しいエントリを見つけるには、*[お気に入り(Favorites)]* リスト、*[ディレクトリ(Directory)]* リスト、または *[発着信履歴(Recents)]* リストに移動するか、あるいは *[検索またはダイヤル(Search or Dial)]* フィールドに 1 文字以上入力します*。該当する連絡先名をクリックします。
2. 連絡先カードで *[コール(Call)]* をクリックします。

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



* 検索時には、入力内容に応じて、*[お気に入り(Favorites)]*、*[ディレクトリ(Directory)]*、および *[履歴(Recents)]* リストの一致するエントリが表示されます。

DTMF トーンの送信

アプリケーションが DTMF(デュアルトーン多重周波数)シグナリングを必要とする場合は、クリックしてキー パッドを開きます。

コールの詳細の表示/非表示

情報ボタンをクリックすると、コールの詳細情報が表示されます。

もう一度ボタンをクリックすると情報が非表示になります。

コールの保留および復帰

参加者を保留にするには、その名前の横にある ⏸ ボタンを使用します。

コールを再開するには、保留中の参加者に表示される ▶ ボタンを使用します。

コールの終了

コールを終了するには、*[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ログインし、*[コール制御(Call Control)]* に移動します。

複数の相手に発信

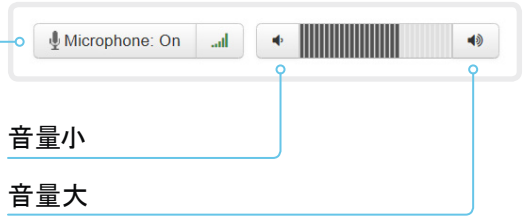
会議ブリッジを使用した複数のコール(CUCM のアドホック会議)は、ビデオ システムでサポートされていても Web インターフェイスではサポートされません。

音量の調整

マイクをミュートにする

[マイク: オン(Microphone: On)] をクリックして、マイクをミュートにします。すると、テキストが *[マイク: オフ(Microphone: Off)]* に変わります。

ミュートを解除するには、*[マイク: オフ (Microphone: Off)]* をクリックします。



Web インターフェイスを使用してコンテンツを共有する

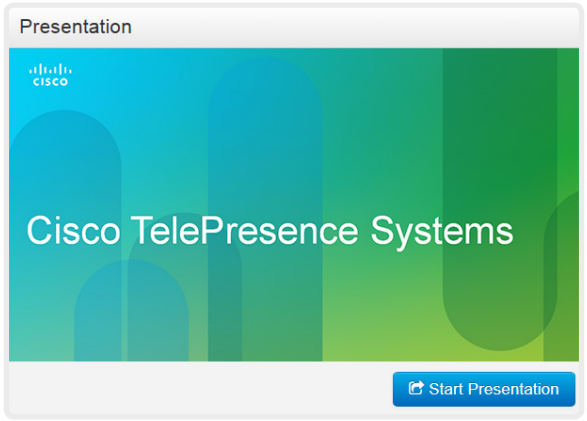
Web インターフェイスにログインし、*[コール制御 (Call Control)]* に移動します。

コンテンツの共有

1. *[プレゼンテーションの開始 (Start Presentation)]* をクリックします。すると、テキストが *[プレゼンテーションの停止 (Stop Presentation)]* に変わります。

コンテンツ共有の停止:

共有している間に表示される *[プレゼンテーションを中止 (Stop Presentation)]* ボタンをクリックします。



スナップショット領域

選択されたプレゼンテーション ソースのスナップショットが表示されます。

リモート モニタリング オプションがあるビデオシステムでのみ利用できます。

コンテンツ シェアリング(共有)について

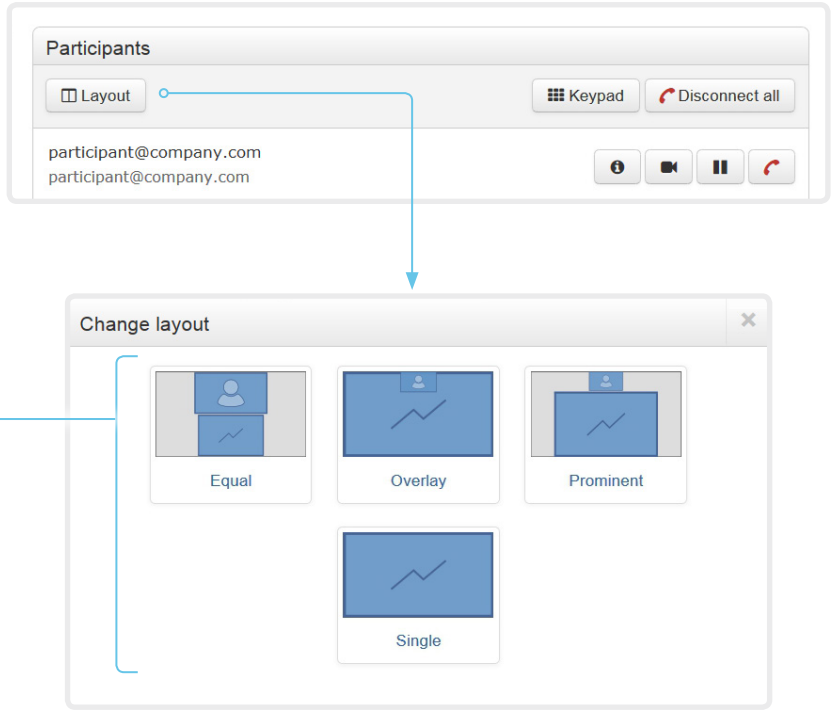
プレゼンテーション ソース(最も多いのは PC)は、ビデオ システムの背面にあるコンピュータ用の HDMI コネクタに接続できます。

コールの間、コールの他の参加者(相手先)とコンテンツを共有できます。

コール(通話)中でない場合は、コンテンツはローカルに表示されます。

ローカル レイアウトの制御

Web インターフェイスにログインし、*[コール制御(Call Control)]* に移動します。



レイアウトの変更

[レイアウト(Layout)] をクリックし、表示されるウィンドウで望ましいレイアウトを選択します。

選択するレイアウトのセットは、システム設定によって異なります。

レイアウトは、アイドル中でも通話中でも変更可能です。

レイアウトについて

ここでいうレイアウトとは、プレゼンテーションとビデオを画面に表示するさまざまな方法のことです。会議の種類によって、レイアウトを変える必要があります。

相手先(遠端)カメラの制御

Web インターフェイスにログインし、*[コール制御(Call Control)]* に移動します。

前提条件

以下の条件において、通話中にリモート参加者のカメラ(相手先)を制御できます。

- 遠端ビデオ システムで *[会議(Conference)] > [遠端制御(FarEndControl)] > [モード(Mode)]* 設定が **[オン(On)]** になっている。
- 遠端カメラにパン、チルト、ズーム機能がある。関連する制御のみ表示される。
- 遠端カメラではスピーカーのトラッキングはオンになっていない。
- ローカル ビデオ システムにリモート モニタリング オプションがある。

リモート参加者のカメラを制御

1. リモート カメラ制御ウィンドウを開くには、カメラのアイコンをクリックします。
2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および − を使用します。

   遠端カメラの制御が許可されていない場合は、画面にコントロールが表示されません。

   コールが暗号化されている場合、制御の背後の遠端スナップショットは表示されません。

パケット損失の復元力:ClearPath

ClearPath により、高度なパケット損失復元メカニズムを導入できます。これらのメカニズムは、エラーを起こしやすい環境でビデオ システムを使用した場合の品質を向上させます。

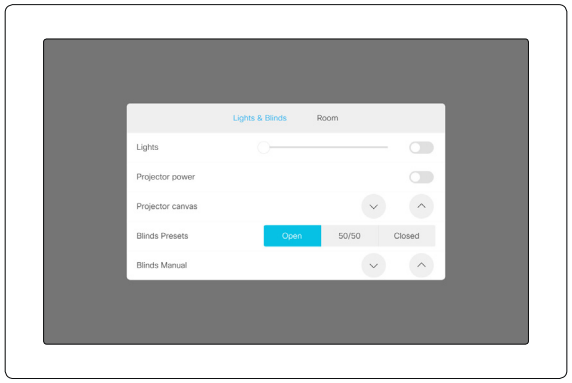
ClearPath はシスコ独自のプロトコルです。CE ソフトウェアが実行されているすべてのエンドポイントが ClearPath に対応しています。

関係するエンドポイントとインフラストラクチャ要素が ClearPath に対応している場合、ポイントツーポイント接続(ホストされた会議を含む)ですべてのパケット損失復元メカニズムが使用されます。

ビデオ システムの ユーザ インターフェイスをカスタマイズする (1/2 ページ)

照明やブラインドなど、会議室内の周辺機器の制御を許可するようにユーザ インターフェイスをカスタマイズすることができます。また、マクロを実行することによってビデオ システムの動作を変更します。

これにより、制御システムの機能とビデオ システムのユーザ フレンドリーなユーザ インターフェイスとの強力な組み合わせが可能になります。



室内制御パネルの例

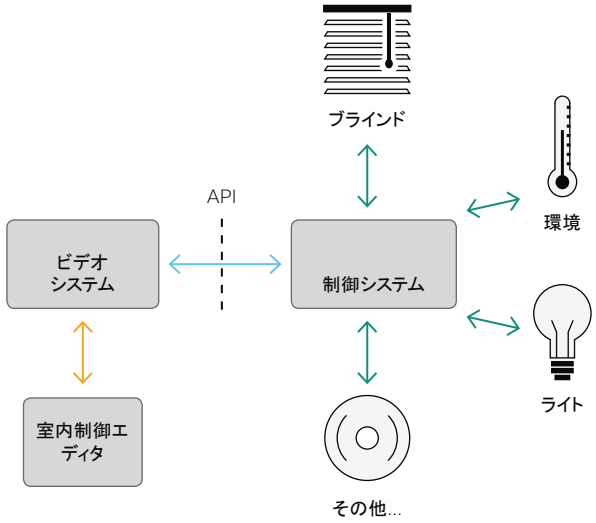
室内制御エディタを使用してカスタム ユーザ インターフェイス パネル（室内制御パネル）を設計する方法、およびビデオ システムの API を使用して室内制御をプログラミングする方法の詳細については、*『CE カスタマイズ ガイド』*[英語] を参照してください。次のリンクにアクセスします。

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

室内制御アーキテクチャ

タッチ インターフェイス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 システムのマクロ フレームワークは、制御システムとしても役立つことがあります。この場合、制御システムはビデオ システムの API を使用して、短縮ダイヤル、言語の選択、カスタマイズされたシステムのリセットなど、あらゆる種類のローカル機能をトリガーすることができます。

ビデオ システムの ユーザ インターフェイスをカスタマイズする (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 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 ユーザ インターフェイスを有効にすることなく、プレビュー機能を使用してお使いの統合をテストできます。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、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る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 ユーザ インターフェイスから、シミュレータの仮想会議室を制御することができます。
- *[シミュレータ設定のロード(Load simulator config)]* をクリックして、ビデオ システムのシミュレータ設定をエクスポートします。

* 制御システムをプログラミングするときに必要な室内制御エディタおよび API コマンドにアクセスするには、ROOMCONTROL, INTEGRATOR, または ADMIN ユーザ ロールを持つユーザが必要です。

マクロを使用したビデオ システムの動作のカスタマイズ

マクロにより、ビデオ システム上で実行するコードの独自のスニペットを作成できます。言語は、arrow functions, promises および classes などの機能をサポートする JavaScript/ECMAScript 6 です。

マクロ フレームワークを利用して、インテグレータはビデオ システムの動作を個別の顧客要件に応じて調整するスクリプトを作成することができます。インテグレータが行える作業には、独自の機能または機能のバリエーションの実装、特定の設定または再設定の自動化、機能のカスタム テストやモニタリングの作成などがあります。

マクロの使用とカスタム ユーザ インターフェイス パネル（以前は室内制御パネルと呼ばれた）の作成を組み合わせることで、ユーザ インターフェイス を修正して、カスタマイズされたローカル機能をトリガーできます。以下に例を示します。

- 短縮ダイヤルボタンの追加
- すべての設定を好みのデフォルト セットアップに戻すためのルーム リセットボタンの追加

マクロについての詳細およびビデオ システムの組み込みマクロエディタの使用方法については、*CE カスタマイズ ガイド* [英語] を参照してください。次のリンクにアクセスします。

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

ビデオ システムでのマクロの使用の許可

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

- *[マクロ(Macros)] > [モード(Mode)]* を **[オン(On)]** に設定します。

  この設定が **[オフ(Off)]** の場合にマクロ エディタを起動しようとすると、ポップアップ メッセージが表示されます。*[マクロの有効化(Enable Macros)]* をタップして応答した場合は *[マクロ(Macros)] > [モード(Mode)]* 設定が自動的に **[オン(On)]** に変更され 、エディタが起動します。

マクロ エディタの起動

Web インターフェイスにサインイン * して、*[統合(Integration)] > [マクロ エディタ(Macro Editor)]* に移動します。

オフラインで使用可能なエディタのスタンドアロン バージョンは提供されていません。

* マクロ エディタにアクセスするには、ADMIN ユーザ ロールを保持しているユーザが必要です。

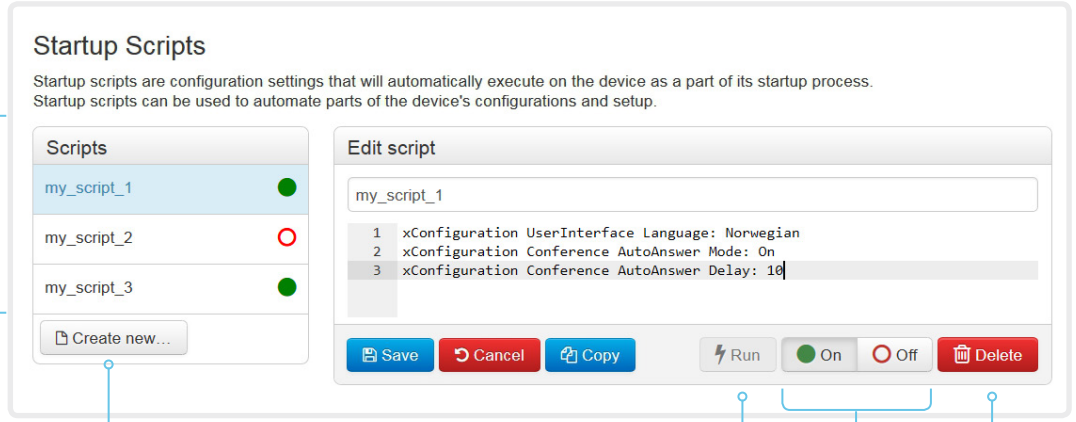
マクロ エディタ

マクロ エディタは、以下のことができる強力なツールです。

- 変更したり、そのまま使用したり、または自身のマクロを記述する際のヒントとして使用したりするコードの例をロードできます。
- 詳細なマクロ記述チュートリアルを用意しているので、参照してください。コードの例についても、より詳しく説明しています。
- 独自のマクロを記述し、ビデオ システムにアップロードできます。
- マクロは、個別に有効または無効にできます。
- マクロを実行したときの動作は、組み込みのログ コンソールで確認できます。

スタートアップ スクリプトを管理する

Web インターフェイスにサインインして、*[統合(Integration)]* > *[スタートアップ スクリプト(Startup Scripts)]* を選択します。



図に示しているスクリプト名と設定は一例です。独自のスクリプトを作成できます。

スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます。

緑色のドットがアクティブなスタートアップ スクリプトの横に、赤色の丸が非アクティブなスタートアップ スクリプトの横に表示されます。

複数のスタートアップ スクリプトがある場合は、リストの上から下に順番に実行されます。

スタートアップ スクリプトを作成する

1. *[新規作成(Create new...)]* をクリックします。
2. タイトル入力フィールドにスタートアップ スクリプトの名前を入力します。
3. コマンド入力エリアにコマンド(xConfiguration または xCommand)を入力します。新しい行で各コマンドを開始します。
4. *[Save(保存)]* をクリックします。
5. *[オン(On)]* をクリックして、スタートアップ スクリプトをアクティブにします。

既存のスクリプトを編集の開始点として使用する場合は、そのスクリプトを選択して *[コピー(Copy)]* をクリックします。

スタートアップ スクリプトをすぐに実行する

1. リストからスタートアップ スクリプトを選択します。
2. *[実行(Run)]* をクリックします。

   アクティブなスタートアップ スクリプトと非アクティブなスタートアップ スクリプトの両方をすぐに実行できます。

スタートアップ スクリプトをアクティブ化または非アクティブ化する

1. リストからスタートアップ スクリプトを選択します。
2. スクリプトをアクティブにする場合は *[オン(On)]* を、非アクティブにする場合は *[オフ(Off)]* をクリックします。

   アクティブなスタートアップ スクリプトは、ビデオ システムが起動するたびに呼び出されます。

スタートアップ スクリプトを削除する

1. リストからスタートアップ スクリプトを選択します。
2. *[削除(Delete)]* をクリックします。

スタートアップ スクリプトについて

スタートアップ スクリプトには起動手順の一部として実行されるコマンド(xCommand)および構成(xConfiguration)が含まれます。

`xCommand SystemUnit Boot` など、いくつかのコマンドとコンフィギュレーションはスタートアップ スクリプトに含めることができません。不正なコマンドや設定が含まれたスクリプトは保存できません。

xCommand および xConfiguration の構文とセマンティックは、製品の API ガイドに説明されています。

ビデオ システムの XML ファイルにアクセスする

Web インターフェイスにサインインして、*[統合(Integration)] > [開発者 API(Developer API)]* を選択します。

XML ファイルはビデオ システムの API の一部です。システムに関する情報が階層で構成されています。

- *Configuration.xml* には現在のシステム設定(コンフィギュレーション)が含まれます。これらの設定は、Web インターフェイスまたは API(アプリケーション プログラミング インターフェイス)から制御されます。
- *status.xml* 内の情報は常にビデオ システムによって更新され、システムおよびプロセスの変更が反映されます。ステータス情報は、Web インターフェイスまたは API からモニタします。
- *Command.xml* にはアクションの実行をシステムに指示するために使用できるコマンドの概要が含まれます。コマンドは、API から発行されます。
- *Valuespace.xml* には、システム設定、ステータス情報、およびコマンドのすべての値スペースの概要が含まれています。

XML ファイルを開く

XML ファイルを開くにはファイル名をクリックします。

API について

アプリケーション プログラミング インターフェイス(API)は、ビデオ システムを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、ビデオ システムの API ガイドで説明されています。

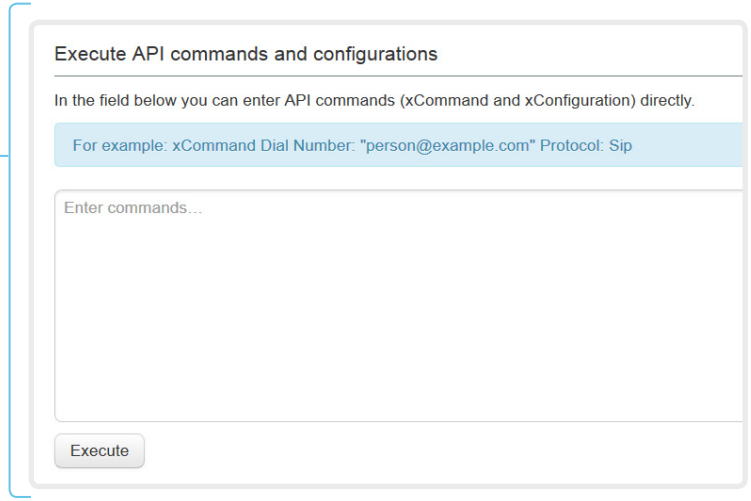
Web インターフェイスからの API コマンドとコンフィギュレーションの実行

Web インターフェイスにサインインして、*[統合(Integration)]* > *[開発者 API(Developer API)]* を選択します。

コマンド(xCommand)および設定(xConfiguration)は、Web インターフェイスから実行できます。構文とセマンティックについては、ビデオ システムの API ガイドで説明されています。

API コマンドとコンフィギュレーションの実行

1. テキスト領域に、コマンド(xCommand または xConfiguration)またはコマンド シーケンスを入力します。
2. *[実行(Execute)]* をクリックしてコマンドを発行します。



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。コンピュータがシリアル ポート ドライバを自動インストールしない場合には、手動でコンピュータにインストールする必要があります。[2]

シリアル インターフェイスに接続するには、ターミナル エミュレータ(SSH クライアント)を使用します。最も一般的なコンピュータ タイプ(PC, MAC)およびオペレーティング システムでは、PuTTY または Tera Term は機能します。

シリアル接続は、IP アドレス、DNS、またはネットワークなしでも使用できます。

パラメータ:

- ボー レート:115200 bps
- データ ビット:8
- パリティ:なし
- ストップ ビット:1
- ハードウェア フロー制御:オフ

ビデオ システムの設定値

シリアル通信はデフォルトでイネーブルになっています。動作を変更するには、次の設定を使用します。

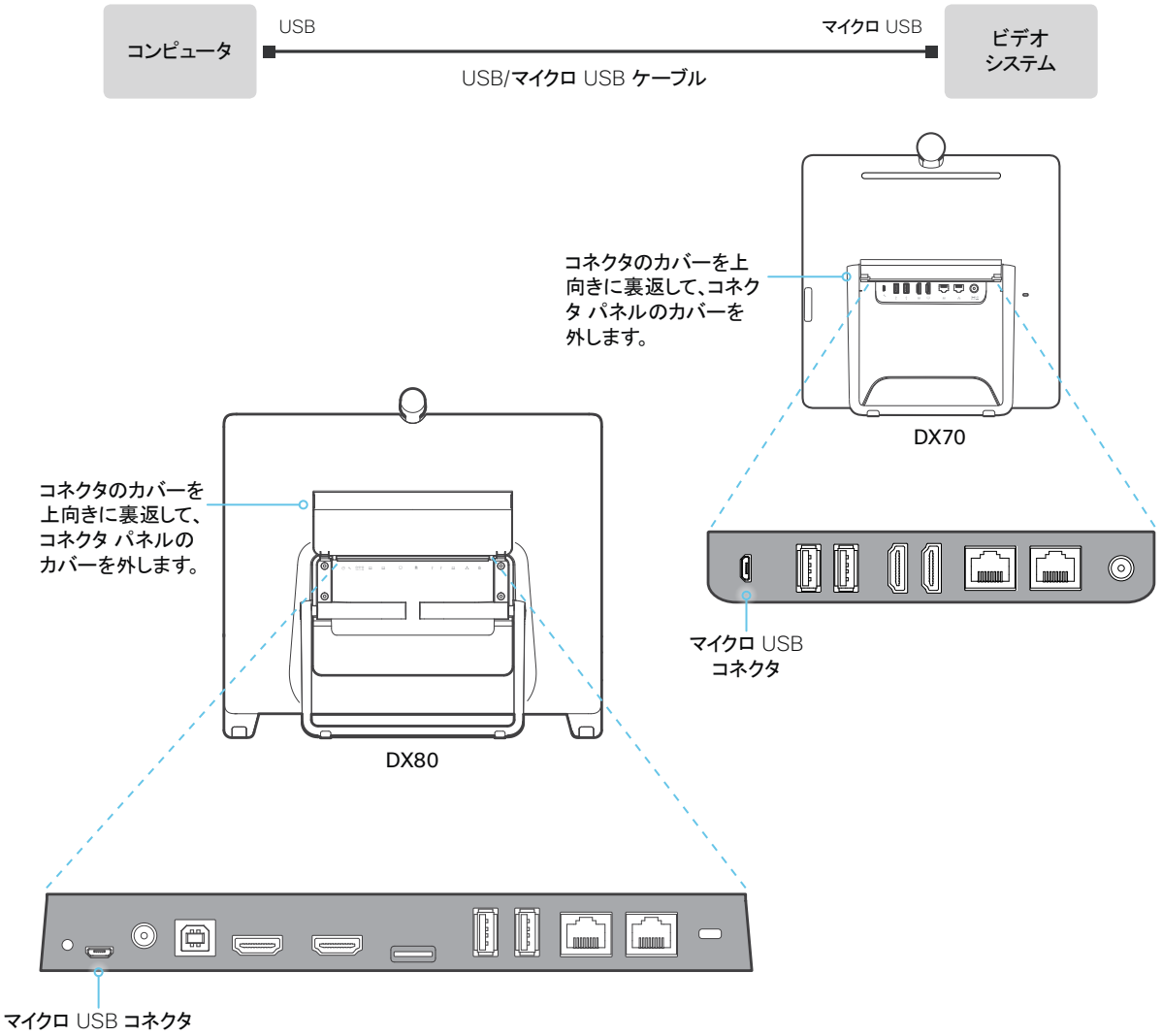
[シリアルポート(SerialPort)] > [モード(Mode)]

セキュリティ上の理由から、シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには、次の設定を使用します。

[シリアルポート(SerialPort)] > [ログインが必須(LoginRequired)]

シリアル ポートの設定を変更した後、ビデオ システムを再起動します。

ビデオ システムが CUCM によりプロビジョニングされる場合、シリアル ポート設定は CUCM から設定する必要があります。



TCP ポートの開放

コーデック内の Web サーバでは、非セキュアまたは不必要なポート、プロトコル、モジュール、またはサービスの使用が禁止または制限されています。いくつかのポートは、デフォルトで開放されているか、閉じられています。

TCP 22:SSH

SSH モード設定を **[オフ(Off)]** にすることで、ポートを閉じることができます。

```
NetworkServices SSH Mode: Off / On
```

TCP 80:HTTP

HTTP モードを **[オフ(Off)]** にするか、**[HTTPS(HTTPS)]** にすることで、ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS / HTTPS / Off
```

TCP 443:HTTP

HTTP モード設定を **[オフ(Off)]** にすることで、ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS / HTTPS / Off
```

TCP 5060/5061:SIP listen ports

SIP リッスン ポートはデフォルトで開放されています。SIP リッスン ポートは、Cisco UCM(Unified Communication Manager)によって無効にされています。SIP リッスン ポートを **[オフ(Off)]** にすることで、ポートを閉じることができます。

```
SIP ListenPort: Off / On
```

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

- コラボレーション エンドポイント ソフトウェア バージョン 8.2 以降

製品の同梱物:

- 内蔵の HD カメラとマイクを備えた DX80 システムまたは DX70 システム
- ネットワーク ケーブル
- HDMI/USB ケーブル(DX80 のみ)
- 電源アダプタおよび使用地域向けの電源コード

統合型の HD カメラ

- ディスプレイから −5° ～ 70°
- 水平視野角 63°
- 垂直視野角 38°
- 解像度:1080p30
- F 2.2
- 顔認識に基づくインスタント フォーカス
- プライバシー シャッター

ユーザ インターフェイス

- 画面上のグラフィカル ユーザ インターフェイス

言語サポート

(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

- 組み込みの SNMP、Telnet、SSH、XML、および SOAP による総合的管理
- Web サーバ、HTTP、および HTTPS を使用したリモート ソフトウェア アップロード
- 画面上のメニュー システム

ディレクトリ サービス

- ローカル ディレクトリ(お気に入り)のサポート
- 社内ディレクトリ(Cisco Unified Communications Manager リリースおよび Cisco TelePresence Management Suite 利用)
- LDAP および H.350 をサポートするサーバ ディレクトリ(Cisco TelePresence Managment Suite が必要)
- 日時を含む着信、発信、および不在着信のコール履歴

電源

- 定格:最大 60 W
- 省電力スタンバイ モード

動作温度および湿度

- 周囲温度:0 ～ 40 ° C(32 ～ 95° F)
- 相対湿度(RH):10 ～ 90%

保管および輸送の温度

- RH 10 ～ 90% では −20 ～ 60° (−4 ～ 140° F)(結露しないこと)

DX80 システムの寸法

- 幅:56.5 cm(22.2 インチ)
- 高さ:51.2 cm(20.2 インチ)
- 奥行:8.9 cm(3.5 インチ)
- 重量:7.1 kg(15.65 ポンド)

DX70 システムの寸法

- 幅:35.31 cm(13.91 インチ)
- 高さ:37.71 cm(14.84 インチ)
- 奥行:6.23 cm(2.45 インチ)
- 重量:3.4 kg(7.5 ポンド)

帯域幅

- 最大 3 Mbps

解像度とフレーム レートの最小帯域幅

- 768 kbps から 720p30
- 1472 kbps から 1080p30

ファイアウォール トラバーサル

- Cisco TelePresence Expressway テクノロジー

ビデオ標準

- H.263
- H.263+
- H.264
- AVC(H.264/MPEG−4 Part 10 Advanced Video Coding)

ビデオ入力

HDMI ビデオ入力 X 1。最大 1920 X 1080 @60 fps(HD1080p60)までのフォーマット(以下を含む)をサポートします。

- 640 X 480
- 720 X 480
- 800 X 600
- 1024 X 768
- 1280 X 720
- 1366 X 768
- 1920 X 1080

Extended Display Identification Data(EDID)

ビデオ出力

HDMI 出力(1 個)* (将来使用に備えて予約済み)。以下のフォーマットをサポートします。

- 1920 X 1080@60 fps(1080p60)

VESA モニタ電源管理

Extended Display Identification Data(EDID)

ライブ ビデオ解像度(エンコード/デコード)

最大 1920 X 1080@30 fps(HD1080p30)までのエンコードまたはデコード ビデオ フォーマット(以下を含む)をサポートします。

- 176 × 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)
- 1280 × 1024 @ 30 fps(SXGA)
- 1440 × 900 @ 30 fps(WXGA+)
- 1680 × 1050 @ 30 fps(WSXGA+)
- 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

音声機能

- 最大 48 kHz のサンプリング レート
- ハイクオリティ 20 kHz オーディオ
- 音響エコー キャンセラ
- オート ゲイン コントロール
- オート ノイズ リダクション
- アクティブ リップ シンク

音声入力

- 内蔵マイク アレイ
- HDMI 音声 1

* HDMI バージョン 1.3

技術仕様 (2/2 ページ)

音声出力
- ライン出力 1 個、ミニジャック(DX70)
- 1 HDMI(デジタル メイン音声)

デュアル ストリーム
- H.239 デュアル ストリーム(H.323)
- BFCP デュアル ストリーム(SIP)
- 15 fps で最大 1920 × 1080 の解像度のサポート

マルチポイント サポート
- シスコ アドホック会議(Cisco Unified Communications Manager(CUCM)と、Cisco Meeting Server(CMS) または Cisco TelePresence Server および Cisco TelePresence Conductor が必要)

プロトコル
- SIP および H.323

組み込み暗号化
- SIP および H.323 のポイントツーポイント
- 規格準拠:H.235v3 および Advanced Encryption Standard(AES)
- キーの自動生成と交換
- デュアル ストリームでサポート

IP ネットワーク機能
- サービス設定での DNS ルックアップ
- 差別化サービス(QoS)
- IP 帯域幅最適化コントロール(フロー制御を含む)
- 自動ゲートキーパー検出
- ダイナミック再生およびリップシンクのバッファリング
- H.323 で H.245 デュアルトーン多重周波数(DTMF) トーン
- NTP による日時のサポート
- パケット損失時のダウンスピード機能
- URI ダイヤル
- TCP/IP
- DHCP
- IEEE 802.1x ネットワーク認証
- IEEE 802.1Q 仮想 LAN
- IEEE 802.1p QoS およびサービス クラス
- Cisco ClearPath

IPV6 ネットワークのサポート
- H.323 および SIP に対するデュアル スタックの IPv4 および IPv6
- DHCP、SSH、HTTP、HTTPS、DNS、DiffServ に対するデュアル スタックの IPv4 および IPv6
- スタティック IP アドレスの割り当て、ステートレス自動設定および DHCPv6 をサポート

サポートされるインフラストラクチャ
- Cisco Unified Communications Manager 8.6.2 以降
- Cisco TelePresence Video Communication Server(Cisco VCS)

セキュリティ機能
- Web インターフェイス(HTTPS/HTTP)および SSH を使用した管理
- パスワードで保護された IP 管理
- パスワードで保護された管理メニュー
- IP サービスのディセーブル
- 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
- 内部 2 ポートの Cisco イーサネット スイッチ(RJ-45) 10/100/1000BASE-T(自動ネゴシエーションのみ)
- Wi-Fi:IEEE 802.11a/b/g/n、2.4 GHz、5 GHz
- Bluetooth 4.0 LE

その他のインターフェイス
- USB ポート 3 個
- MicroSD カード スロット 1 個(将来の使用に備えて)
- メンテナンス目的の Micro-USB ポート 1 個

認定および適合規格
- 指令 2014/35/EU(低電圧指令)
- 指令 2014/30/EU(EMC 指令):クラス A
- 指令 2014/53/EU(無線機器指令)
- 指令 2011/65/EU(RoHS)
- 指令 2002/96/EC(WEEE)
- NRTL 認定(製品の安全性)
- FCC CFR 47 Part 15B(EMC):クラス B
- FCC Listed(無線機器)

各国の認定書類については、Product Approval Status Database(製品認定ステータス データベース)www.ciscofax.com を参照してください。

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 [英語]

マニュアルは以下のカテゴリに整理されています。一部のマニュアルはすべての製品で利用できません。

インストールとアップグレード > インストールとアップグレード ガイド

- *インストレーション 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
- *『Deployment guide for TelePresence endpoints on CUCM』*:ビデオ システムを Cisco Unified Communications Manager(CUCM)とともに使用開始するために実行するタスク
- *スペア部品の概要、スペア部品の交換ガイド、ケーブル スキーマ*:スペア部品を交換するときに役立つ情報

保守と運用 > エンドユーザ ガイド

- *ユーザ ガイド*:製品の使用方法
- *クイック リファレンス ガイド*:製品の使用方法
- *物理インターフェイス ガイド*:コネクタのパネルと LED など、コーデックの物理インターフェイスに関する詳細

リファレンス ガイド > コマンド リファレンス

- *『API リファレンス ガイド』*:Application Programmer Interface(API)のリファレンス ガイド

リファレンス ガイド > テクニカル リファレンス

- *CAD 図面*:測定値付き 2D CAD 図面

設定 > 設定ガイド

- *CE カスタマイズガイド*: ユーザーインターフェイスのカスタマイズ方法、ビデオシステムの API を用いた室内操作のプログラミングの方法、マクロの作成方法、ビデオスイッチの使い方、オーディオコンソールを用いた上級者向けの音声セットアップと設定方法。

設計 > 設計ガイド

- *ビデオ会議室に関するガイドライン*:会議室の設計とベスト プラクティスに関する一般的なガイドライン
- *ビデオ会議室のガイドライン*:音質を向上させるための対策

ソフトウェア ダウンロード、リリースと一般情報 > ライセンス情報

- *オープン ソース ドキュメンテーション*:この製品で使用されるオープン ソース ソフトウェアのライセンスおよび通知

[ソフトウェア ダウンロード、リリースと一般情報(Software Downloads, Release and General Information)] > [リリース ノート(Release Notes)]

- *ソフトウェア リリース ノート*

シスコのお問い合わせ先

シスコの Web サイトでは、シスコの世界各地のお問い合わせ先を確認できます。

参照先:▶ https://www.cisco.com/go/offices [英語]

本社
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

Intellectual property rights

シスコ製品のセキュリティの概要