ソフトウェア バージョン TC7.2
2014 年 8 月

アドミニストレータ ガイド

Cisco TelePresence MX200 G2 および MX300 G2

シスコ製品をお選びいただきありがとうございます。

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

製品マニュアルのこの部分は、ビデオ システムを設定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。このガイドについてのご意見、ご感想をお聞かせください。

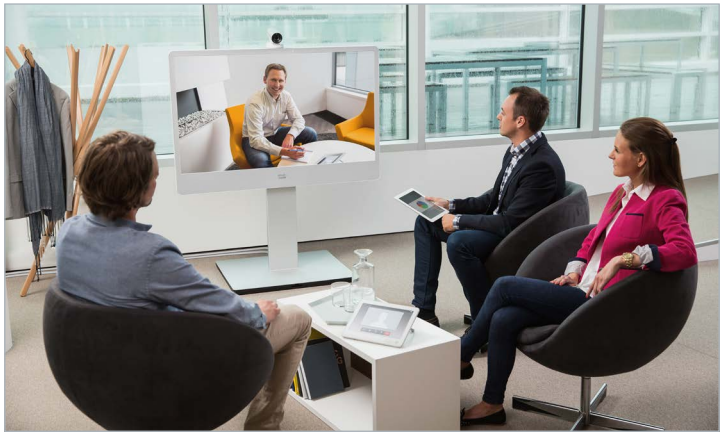
定期的にシスコの Web サイトにアクセスし、このガイドの最新版を入手することを推奨します。

ユーザ ドキュメンテーションは次の URL から入手できます。
http://www.cisco.com/go/telepresence/docs

本ガイドの使用方法

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

目次



第 1 章

はじめに

このマニュアルは、高度なレベルで製品を管理するために必要な情報を示します。

製品のインストール方法および必要な初期設定は、インストール ガイドおよびスタートアップ ガイドでそれぞれ説明しています。

このガイドの対象となる製品

- Cisco TelePresence MX200 G2
- Cisco TelePresence MX300 G2

第 1 世代の MX シリーズ製品（MX300 および MX200）は、別個のガイドで扱われています。

ユーザ ドキュメンテーション

TC ソフトウェアを実行する Cisco TelePresence システムのユーザ ドキュメンテーションには、さまざまなユーザ グループ向けの複数のガイドが含まれています。

- 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
- 『CUCM での TC エンドポイントの管理』：
  製品を 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
- 『管理者ガイド』（このガイド）：
  製品の管理に必要な情報
- クイック リファレンス ガイド：
  製品の使用方法
- ユーザ ガイド：製品の使用方法
- ナレッジ ベースの記事
- 『Video conferencing room primer』：
  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
- 『Video conference room acoustics guidelines』：
  認識される音声の品質を向上させるために行うべきこと
- ソフトウェア リリース ノート
- 法令準拠および安全上の注意ガイド
- 法律およびライセンス情報

ユーザ ドキュメンテーションのダウンロード

ユーザ ドキュメンテーションの更新バージョンがないか、定期的にシスコの Web サイトにアクセスして確認することを推奨します。参照先：

http://www.cisco.com/go/telepresence/docs

シスコの Web サイトにあるドキュメンテーションの検索ガイドラインについては、付録の「シスコ Web サイト内のユーザ ドキュメンテーション」を参照してください。

ソフトウェア

製品のソフトウェアは、シスコの Web サイトからダウンロードできます。参照先：

http://www.cisco.com/cisco/software/navigator.html

次のサイトから、ソフトウェア リリース ノート（TC7）を参照することを推奨します。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

このバージョンの新機能

ここでは TC7.2 ソフトウェア バージョンで追加または変更されたシステム設定および新しい機能の概要について説明します。

ソフトウェア リリース ノート

新機能および変更のすべての概要については、ソフトウェア リリース ノート（TC7）を読むことを推奨します。参照先：

http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

ソフトウェアのダウンロード

ソフトウェアのダウンロードについては、http://www.cisco.com/cisco/software/navigator.html を参照してください。

新機能および改善点

タッチ 10 ネットワーク ペアリングのサポート

タッチ 10 ユーザ インターフェイスのネットワーク ペアリングがサポートされています。

Web スナップショットを Web インターフェイスからリモートで有効にできる

Web スナップショットを Web インターフェイスからリモートで有効にできます。以前のバージョンでは、Web スナップショットはエンドポイントでローカルで有効にする必要がありました。

Collaboration Edge を介して登録したエンドポイントのフェールオーバー サポートの強化

CUCM：CUCM がダウンすると、エンドポイントは別の CUCM に自動的に再登録します。

VCS Control および VCS Expressway：VCS Control または VCS Expressway がダウンすると、エンドポイントは別の VCS Control または VCS Expressway に自動的に再登録します。コール プリザベーションはサポートされていません。

プロビジョニング（HTTPS）：プロビジョニング サービスがダウンすると、エンドポイントは別のプロビジョニング サービスからプロビジョニング データを受信します。

電話帳：電話帳サービスがダウンすると、エンドポイントは自動的に別の電話帳サービスを使用します。

CUCM からプロビジョニングできるパラメータの増加

バージョン固有の設定で次の設定パラメータを CUCM からプロビジョニングできるようになりました。

- SystemUnit Name
- Video OSD TodaysBookings
- Standby StandbyAction
- Audio DefaultVolume
- Conference 1 MaxTotalReceiveCallRate
- Conference 1 MaxTotalTransmitCallRate

タッチ ユーザ インターフェイスとオンスクリーン ディスプレイ（OSD）のスクリーンショットを Web インターフェイスから取得可能

OSD およびタッチパネルのスクリーンショットを取得できる新しい Web 機能が実装されました。この機能は、Web スナップショットが無効な場合でも使用できます。

ビデオ出力ステータスに接続ディスプレイに関する情報を表示

接続しているディスプレイのモデルと優先解像度を示すため、ビデオ出力ステータスで次の値が出力されるようになりました。

- Video Output Connector n Connected
- Video Output Connector n ConnectedDevice Name
- Video Output Connector n ConnectedDevice PreferredFormat

システム設定の変更

新しい構成

H323 Profile [1] Encryption MinKeySize

NetworkServices Medianet Metadata

Peripherals Pairing CiscoTouchPanels RemotePairing

Peripherals Profile TouchPanels

Time OlsonZone

変更された設定

Video Input Connector[n] InputSourceType

旧: <other/camera/PC/DVD/document_camera>

新: <other/camera/PC/DVD/document_camera/whiteboard>

Video Output Connector[n] Resolution

旧: <Auto/1024_768_60/1280_1024_60/1280_720_60/1920_1080_60/1280_768_60/1360_768_60/1366_768_60>

新: <Auto/1024_768_60/1280_1024_60/1280_720_50/1280_720_60/1920_1080_50/1920_1080_60/1280_768_60/1360_768_60/1366_768_60>

Cisco TelePresence MX200 G2 および MX300 G2 の概要

Cisco TelePresence® MX200 G2 および MX300 G2 は、第 2 世代の MX シリーズ多目的エンドポイントです。

MX200 G2 および MX300 G2 は外観、機能性、使いやすさをすべて兼ね備えています。1080p60 の高画質（HD）性能と、デュアル ディスプレイや組み込みの 4 画面分割 MultiSite 会議オプションなどの新機能により、性能と柔軟性が向上しました。Cisco TelePresence Touch 10 ユーザ インターフェイスには、大画面に加えて使いやすいエクスペリエンスも備わっています。

MX200 G2 および MX300 G2 システムは簡単に設置でき、あらゆる会議室をテレプレゼンス対応のチーム ルームにすばやく変えることができます。

MX200 G2 および MX300 G2 は、ビデオ コミュニケーション機能を初めて利用する場合でも、組織全体をビデオ対応にする予定である場合でも、ニーズに対応できます。

MX200 G2

MX300 G2

機能とメリット

- 1 台の端末と、フロア スタンド、ホイール ベース、または壁面取り付けブラケット（VESA マウント）を使用して、容易に設置。
- Cisco Unified Communications Manager（UCM）、Cisco TelePresence Video Communication Server（VCS）、または Cisco WebEx TelePresence プロビジョニングによる自己設定。ユーザが行う必要があるのは、エンドポイントをネットワークに認証させる作業のみです。
- MX200 G2：パン、チルト、5 倍光学ズーム機能を備えた Cisco TelePresence PrecisionHD カメラ。

  MX300 G2：パン、チルト、8 倍光学ズーム機能を備えた Cisco TelePresence PrecisionHD カメラ。
- MX200 G2：高品質 42 インチ LCD ディスプレイ（解像度 1920×1080（1080p60）および縦横比 16:9）。

  MX300 G2：高品質 55 インチ LCD ディスプレイ（解像度 1920×1080（1080p60）および縦横比 16:9）。
- 優れた音声を実現する前面の 2 台のスピーカー。
- 統合マイクと、2 台の外部 Cisco TelePresence Table Microphone 20 のサポート。
- 10 インチ Cisco TelePresence Touch 10 ユーザ インターフェイスにより、シンプルな操作が実現
- 各種の標準規格に準拠。
- 最大 6 Mbps のポイントツーポイント帯域幅で H.323 と Session Initiation Protocol（SIP）をサポート。
- 最大 1080p60 のビデオ解像度をサポート。
- 解像度 1080p30 で高解像度マルチメディアおよびプレゼンテーション共有をサポート。
- コンテンツ共有用に別の画面を追加できるデュアル ディスプレイ機能をサポート。
- スケジュールされている会議を開始するためのワンボタン機能をサポート。
- 最大 3 名までの参加者を追加できる組み込みマルチサイト電話会議オプション。
- システムは Cisco TelePresence Total Solution アプローチ（Cisco TelePresence Multiway 機能、録音/録画およびストリーミング、ファイアウォール トラバーサル サービスなど）を利用します。
- Cisco UCM バージョン 8.6.2 以降ではネイティブでサポートされます。

Cisco TelePresence MX300 G2

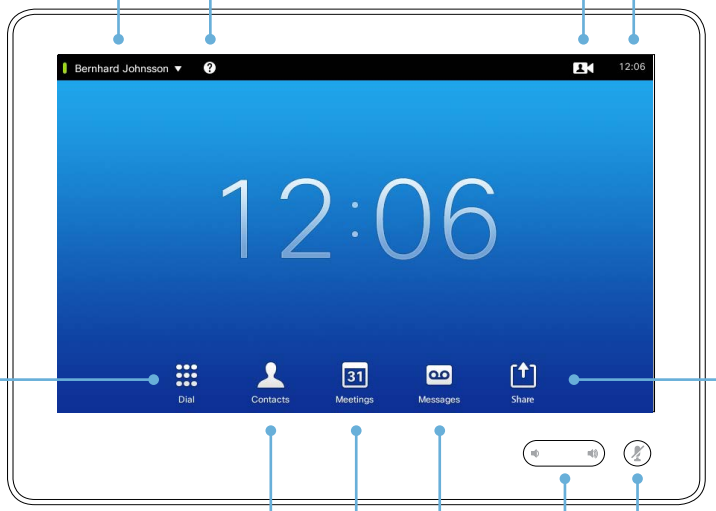
取り付けオプション
（フロアスタンド、ホイール ベース、壁面取り付け）

Cisco TelePresence MX200 G2

取り付けオプション
（フロアスタンド、ホイール ベース、テーブル スタンド、壁面取り付け）

タッチ 10 の使用方法

タッチ 10 ユーザ インターフェイスと使用方法の詳細については、お使いのビデオ システムのユーザ ガイドを参照してください。



? をタップすると、ヘルプ デスクへの連絡またはアクセスが可能です（該当する場合）。

左上隅をタップして、[応答不可（Do not disturb）]機能や [スタンバイ（Standby）] 機能をアクティブ/非アクティブにしたり、[設定（Settings）] にアクセスしたりできます。

カメラアイコンをタップすると、セルフビューとカメラ制御がアクティブになります。

右上隅に時刻が表示されます。

ダイヤル パッドを呼び出すには [ダイヤル（Dial）] をタップします。

[共有（Share）] をタップすると、コンテンツの共有とプレゼンテーションを開始することができます。

[連絡先（Contacts）] をタップすると、[お気に入り（Favorites）]、[ディレクトリ（Directory）]、[履歴（History）] などを含む、連絡先のリストが呼び出されます。

マイク ボタンを押すと、マイクがミュート/ミュート解除されます。

次回予定されている会議のリストを呼び出すには [会議（Meetings）] をタップします。

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

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

第 2 章

Web インターフェイス

Web インターフェイスへのアクセス

Web インターフェイスを使ってビデオ会議システムを詳細に設定できます。

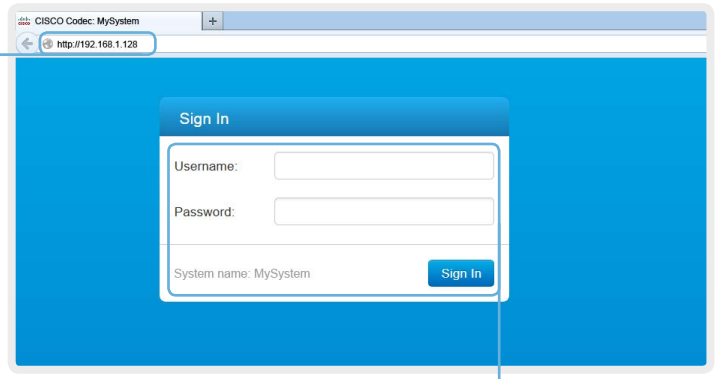
コンピュータから接続して、システムをリモートで管理できます。

この章では、Web インターフェイスを使用してシステム設定とメンテナンスを行う方法について説明します。

主要な Web ブラウザの最新版を使用することを推奨します。

1.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

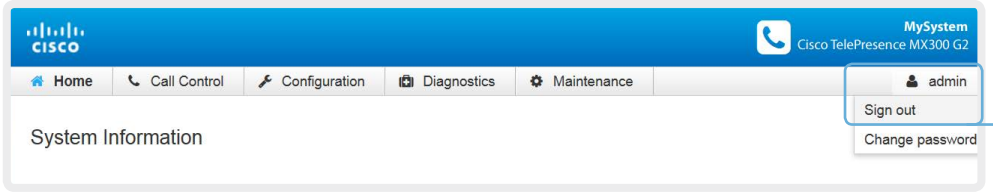
タッチ コントローラ：タッチ コントローラの左上隅にある連絡先情報をタップし、[設定 (Settings)] メニューを開きます。その後、[システム情報 (System Information)] をタップします。

2.サインイン

ビデオ システムのユーザ名とパスワードを入力して、[サインイン (Sign In)] をクリックします。

システムには出荷時にデフォルト ユーザ *admin* (パスワードなし) が設定されています。初めてサインインするときに、[パスワード (Password)] 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。次のページを参照してください。



サイン アウト

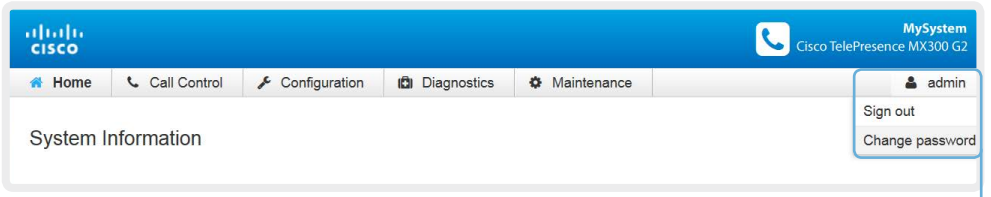
ユーザ名の上にマウスを移動し、ドロップダウン リストから [サインアウト (Sign out)] を選択します。

システム パスワードの変更

システム設定へのアクセスを制限するために、管理者特権を持つユーザのパスワードを設定する必要があります。これにはデフォルトの *admin* ユーザが含まれます。

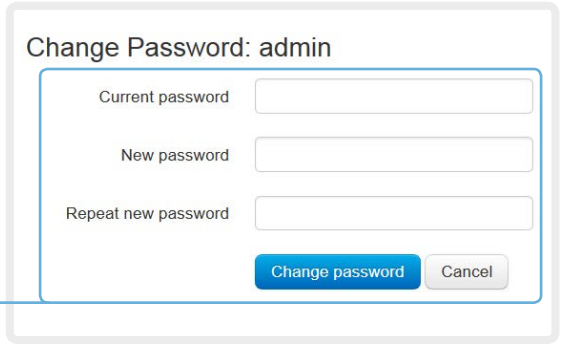
パスワードを設定するまで、システム パスワードが設定されていないという警告が画面に表示されます。

「パスワードの設定」の章で、パスワード保護の詳細を確認できます。



1. [パスワードの変更(Change Password)] ダイアログを開く

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 [パスワードの変更(Change Password)] を選択します。



2.新しいパスワードを設定する

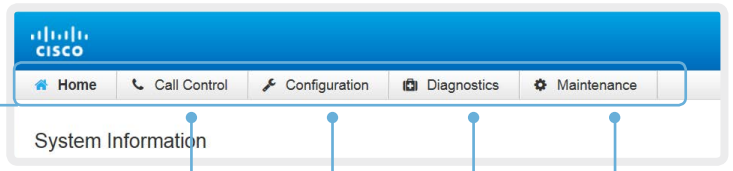
現在のパスワードと新しいパスワードを要求どおりに入力し、[パスワードの変更(Change Password)] をクリックして変更を適用します。

パスワードが現在設定されていない場合は、[現在のパスワード(Current password)] フィールドを空白のままにします。

インタラクティブ メニュー

Web インターフェイスからタスクと設定にアクセスできます。これらはサインインしたときにページの上部に表示されるメイン メニューに表示されます。

メイン メニューの項目の上にマウスを移動すると、関連するサブ メニューに移動できます。



メイン メニュー (Main Menu)

関連するサブページのタイトルを確認するには、メイン メニューの項目の上にマウスを移動します。

サブ ページを開くには、サブ ページのタイトルをクリックします。サブページがない場合はメイン メニューの項目をクリックします。ユーザにアクセス権のあるページのみが表示されます*。

[ホーム (Home)] をクリックすると、[システム設定 (System Settings)] ページに戻ります。

サブページ

コール制御 (Call Control)	設定 (Configuration)	診断	メンテナンス (Maintenance)
	システム設定 (System Configuration)	トラブルシューティング (Troubleshooting)	ソフトウェア アップグレード (Software Upgrade)
	システム ステータス (System Status)	コール履歴 (Call History)	バックアップと復元 (Backup and Restore)
	ローカル コンテンツ管理 (Local Contents Management)	ログ ファイル (Log Files)	システム リカバリ (System Recovery)
	パーソナライゼーション (Personalization)	ユーザ インターフェイスのスクリーンショット (User Interface Screenshots)	再起動 (Restart)
	周辺機器 (Peripherals)		
	ユーザ管理 (User Administration)		
	サインイン バナー (Sign In Banner)		
	スタートアップ スクリプト (Startup Scripts)		
	API		
	セキュリティ (Security)		

* ユーザ管理、ユーザ ロール、およびアクセス権に関する詳細情報は、「ユーザ管理」の項で確認できます。

システム情報

ビデオ システムの [ホーム(Home)] ページには、システムの基本設定およびステータスの概要が表示されます*。

ここにはシステム名や製品タイプ、システムが動作するソフトウェア バージョン、IP アドレスなどの情報が含まれます。また、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。

移動先:[ホーム(Home)]

* 図に示しているシステム情報は一例です。お使いのシステムとは異なる場合があります。

コールの開始

[コール制御(Call Control)] ページを使用してコールを発信できます。

Web インターフェイスを使用してコールを開始する場合でも、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。

発信

[ローカル(Local)]、[ディレクトリ(Directory)] または [新着(Recents)] リストで連絡先の名前を選択するか、[検索またはダイヤル(Search or Dial)] フィールドに完全な URI または番号を入力して、相手を呼び出すことができます。次に、関連する連絡先カードで [コール(Call)] をクリックします。

連絡先リストの検索

[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。入力内容に応じて、[ローカル(Local)]、[ディレクトリ(Directory)] または [新着(Recents)] リストに一致するエントリが表示されます。

リストで正しいエントリを選択し、[コール(Call)] をクリックします。

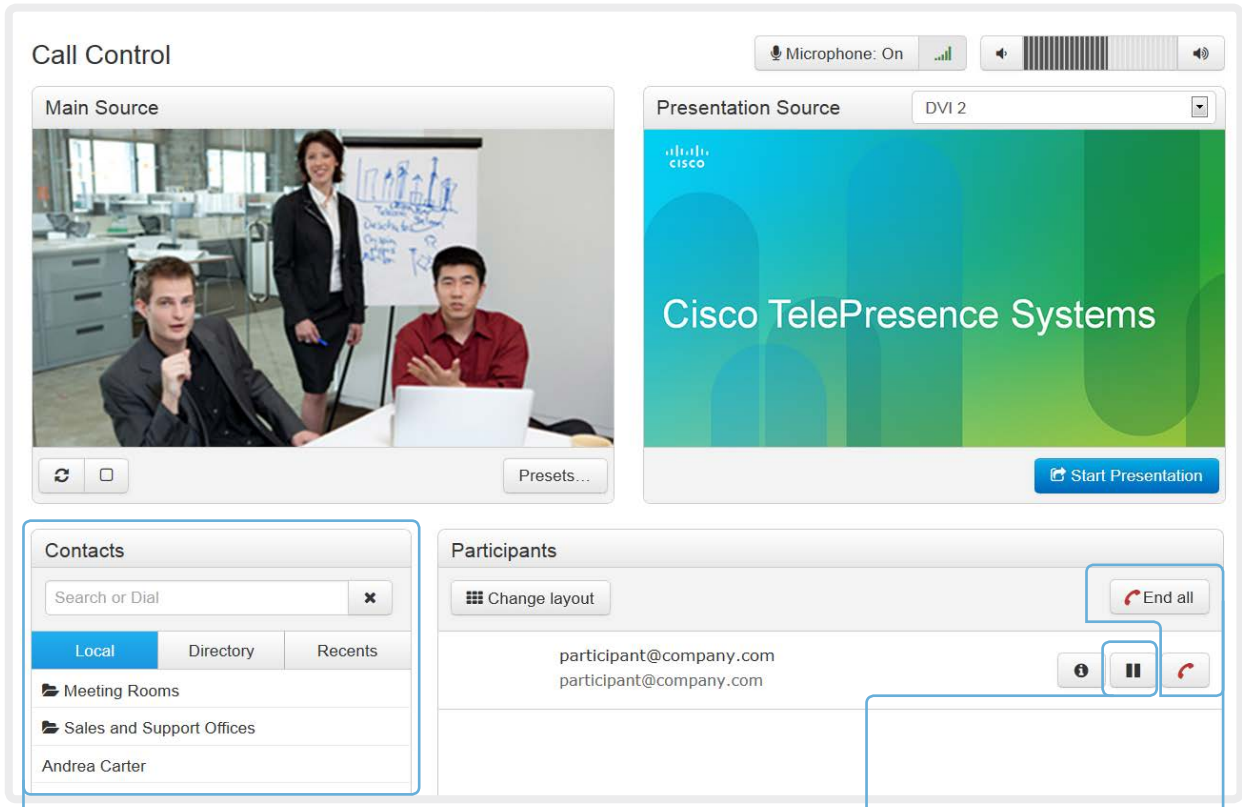
複数の相手に発信

ポイントツーポイント ビデオ コール(2 者限定のコール)を拡張して、参加者を追加することができます。

システムでオプションの組み込み MultiSite 機能がサポートされている場合は、本人も含めて最大 4 名の参加者がビデオ通話(会議)に参加できます。

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

移動先:[コール制御(Call Control)]



相手への発信

[ローカル(Local)]、[ディレクトリ(Directory)] または [新着(Recents)] リストの連絡先名をクリックします。次に、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。

保留と再開

参加者の隣にある ⏸ ボタンを使用すると、その人が保留状態になります。

コールを再開するには、保留中の参加者に表示される ▶ ボタンを使用します。

コールの終了

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

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

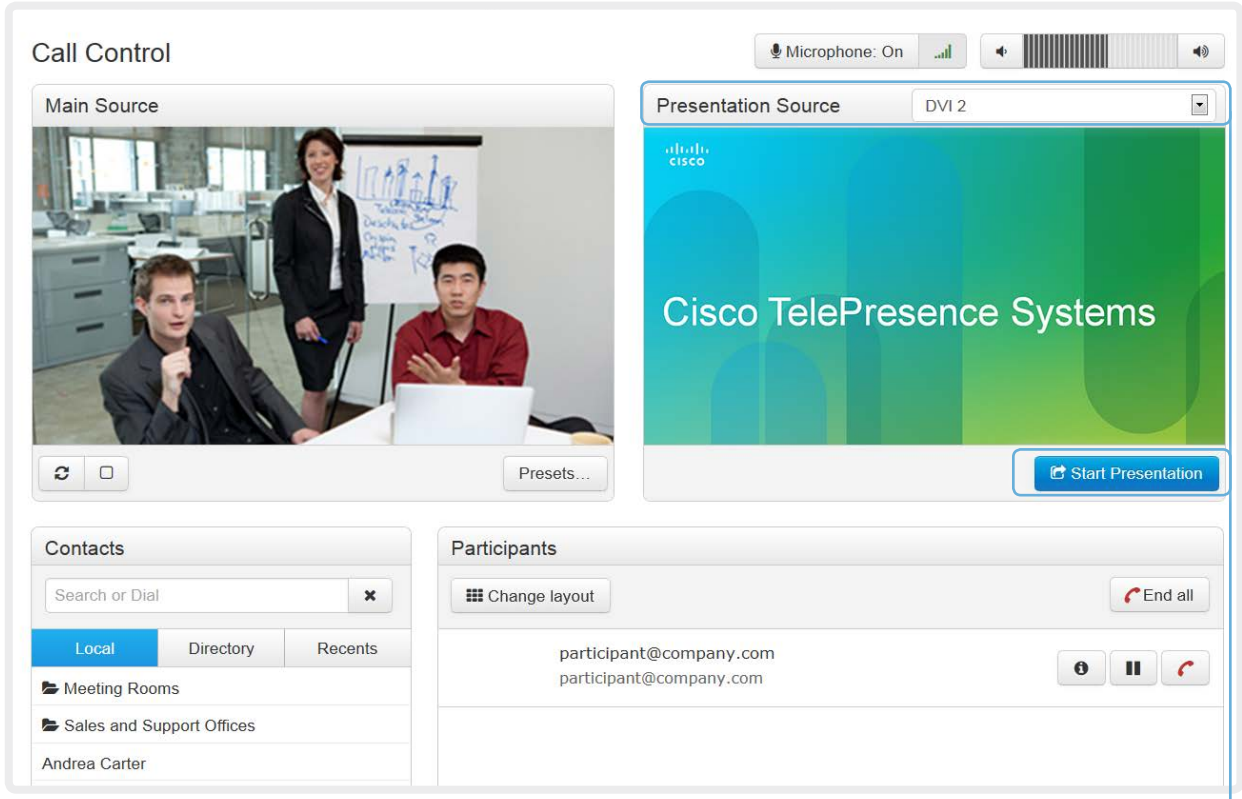
コンテンツの共有

ビデオ システムの外部入力の 1 つにプレゼンテーション ソースを接続できます。プレゼンテーション ソースとして最も多く使用されるのは PC ですが、システムの設定によってはその他のオプションを使用できる場合があります。

コール中、コンテンツを遠端（コールの他の参加者 ）と共有できます。

コールを行っていない場合、コンテンツはディスプレイ上にローカルで共有されます。

移動先：[コール制御（Call Control）]



コンテンツの共有

1. プレゼンテーション ソースをドロップダウン リストから選択します。
2. [プレゼンテーションの開始（Start Presentation）] をクリックします。

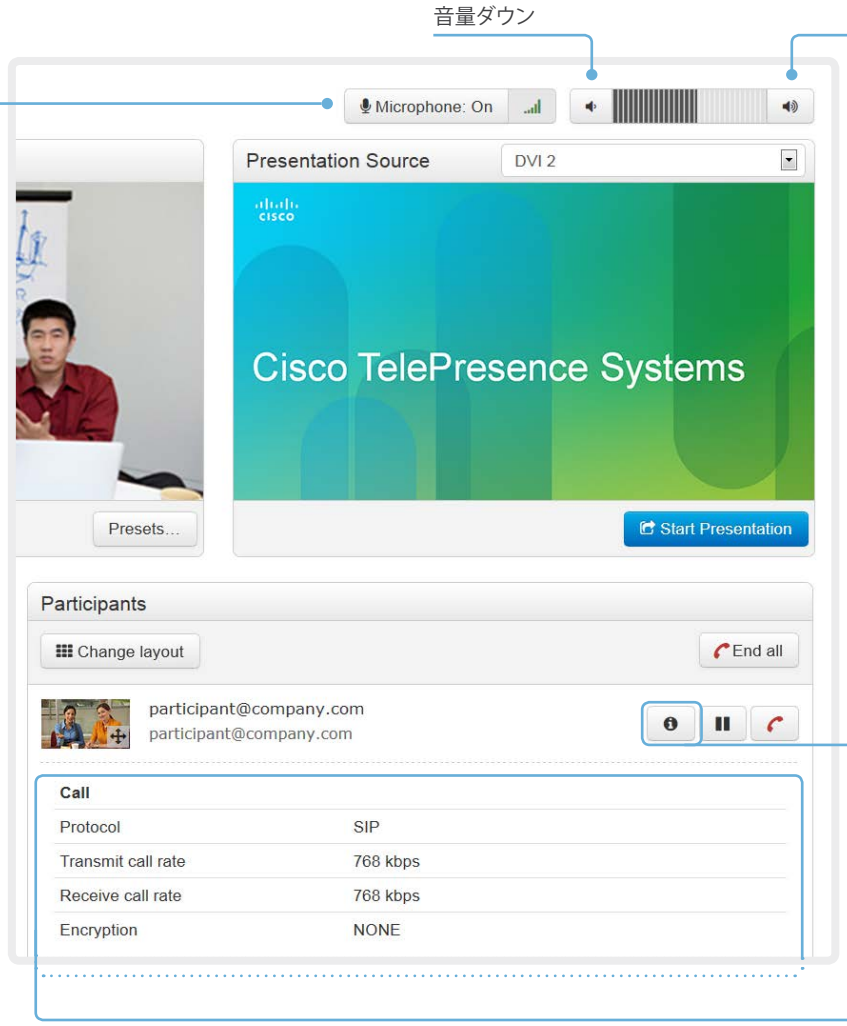
コンテンツ共有の停止：

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。

コールの制御および監視

[コール制御(Call Control)] ページを使用して、複数のコール機能を制御および監視できます。

移動先:[コール制御(Call Control)]



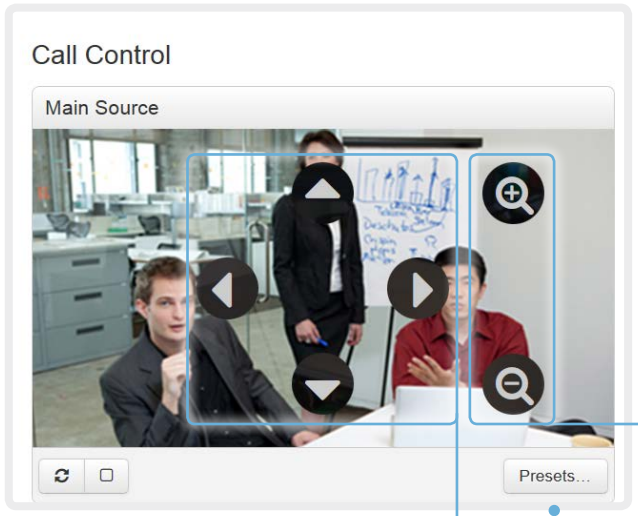
カメラの制御

[コール制御(Call Control)] ページを使用してカメラを制御できます。

カメラ制御(パン、チルト、ズーム)は、カーソルが [メイン ソース(Main Source)] ビデオ領域内にある場合に利用できます。この期間中はライブ スナップショットが自動的に取得されます。

システムがスタンバイ モードの場合、カメラ制御は利用できない点に注意してください。

移動先:[コール制御(Call Control)]

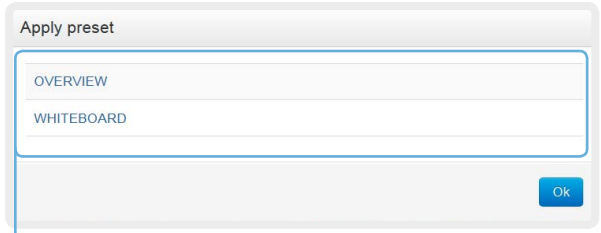


ズーム

ズームインとズームアウトには、+ および - を使用します。

パンとチルト

カメラのパンには左右の矢印キーを使用し、チルトには上下の矢印キーを使用します。



カメラ プリセット

カメラ プリセットが定義されている場合、ここに表示されます。プリセットの名前をクリックして、プリセット位置にカメラを移動します。

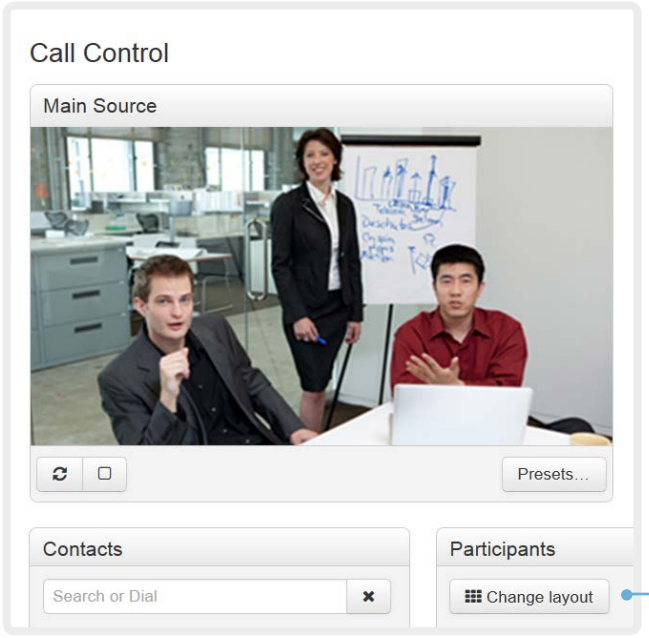
[OK] をクリックしてウィンドウを閉じます。

ローカル レイアウトの制御

[コール制御(Call Control)] ページを使用してローカル レイアウトを選択できます。

ここでいうレイアウトとは、会議参加者のビデオとプレゼンテーション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。

移動先:[コール制御(Call Control)]

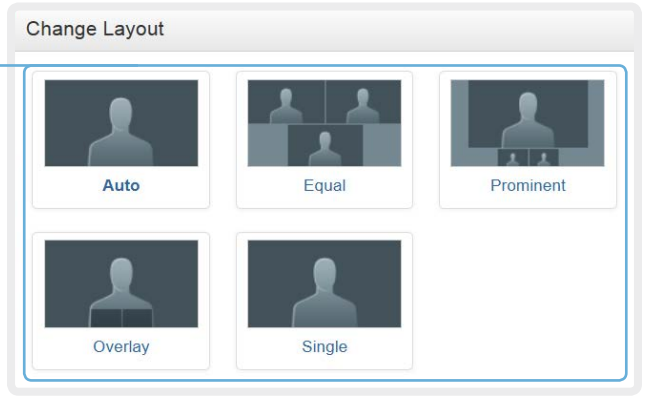


レイアウトの変更

[レイアウトの変更(Change layout)] をクリックし、表示されるウィンドウで優先する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。

コールの間にレイアウトを変更できます。



スナップショットのキャプチャ

スナップショット機能はデフォルトで無効になっていますが、ビデオ システムによりキャプチャされたスナップショットを [コール制御 (Call Control)] ページに表示できます。ビデオ システムのカメラからのキャプチャに加え、プレゼンテーション チャンネルからのキャプチャも表示されます。

この機能は、たとえばカメラのビューをチェックするなど、リモート ロケーションからビデオ システムを管理する際に役立つ場合があります。

Web スナップショットを使用するには、ADMIN クレデンシャルでサイン インする必要があります。

スナップショット機能の有効化

スナップショット機能は、デフォルトでは無効です。この機能は、Web インターフェイスを使用して有効にする必要があります。

Web インターフェイス

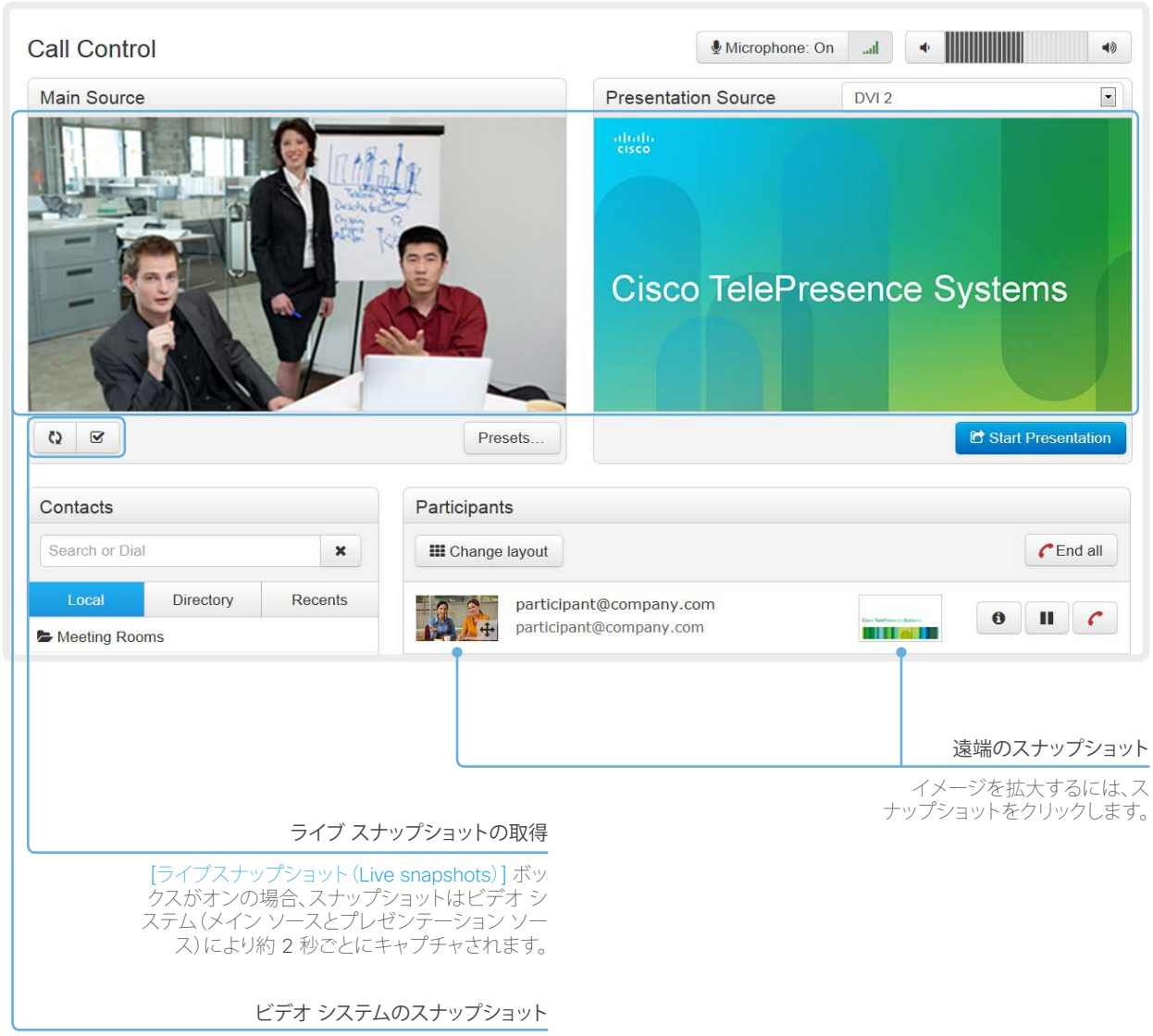
- [設定 (Configuration)] タブに移動し、[システム設定 (System Configuration)] を選択します。
- [ビデオ (Video)] > [Web スナップショットを許可 (AllowWebSnapshots)] に移動し、[オン (On)] を選択します。
- [保存 (Save)] をクリックして変更を有効にします。

コール中の遠端のスナップショット

コール中は、リモート参加者のメイン カメラとプレゼンテーション チャネル (遠端) のスナップショットがキャプチャされ、図のように表示されます。スナップショットはおよそ 30 秒ごとに更新されます。

遠端のビデオ システムで Web スナップショットが無効にされていても、遠端のスナップショットがキャプチャされます。暗号化されたコールの場合にのみ、Web スナップショットが禁止されます。

移動先:[コール制御 (Call Control)]

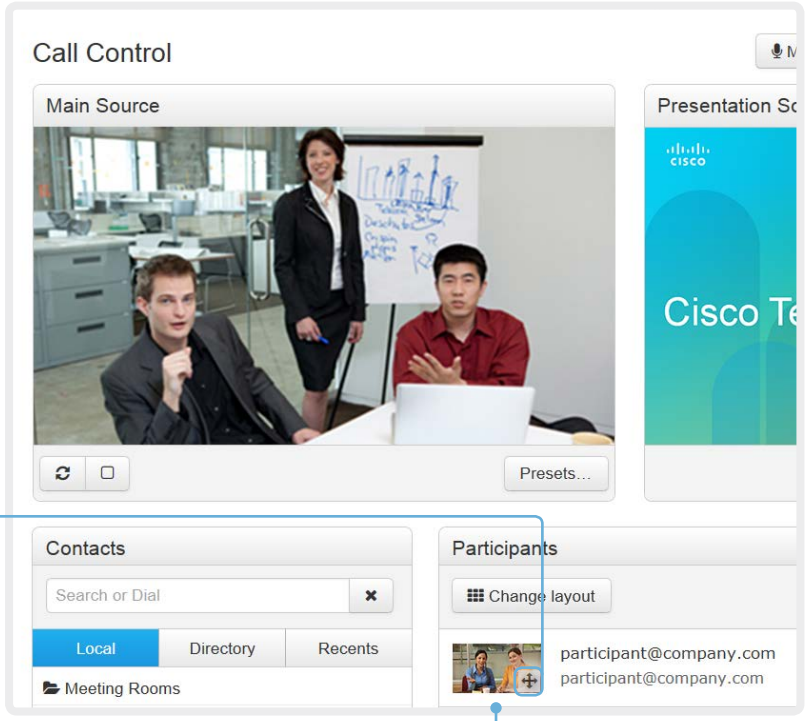


遠端カメラの制御

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。

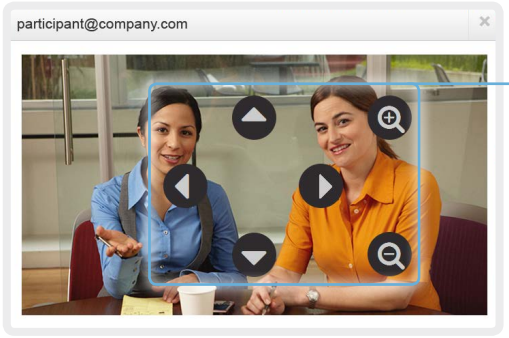
- [会議遠端制御モード（Conference FarEndControl Mode）] 設定が遠端ビデオ システムで [オン（On）] に切り替わっている。
- 遠端カメラにパン、チルト、ズーム機能がある。関連する制御のみ表示される。

移動先：[コール制御（Call Control）]



遠端カメラ制御インジケータ

この記号が表示される場合は、リモート参加者のカメラを制御できます。



リモート参加者のカメラを制御

1. 大きなウィンドウに表示するには、スナップショットをクリックします。
2. コントロールを有効にするイメージにカーソルを置きます。
3. 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。

コール情報へのアクセス

コール状態インジケータは、Web インターフェイス上部のバーで使用できます。システムがコール中であるかどうかや、対応しているコール件数を示します。着信コールについてユーザに通知することもできます。

システム設定

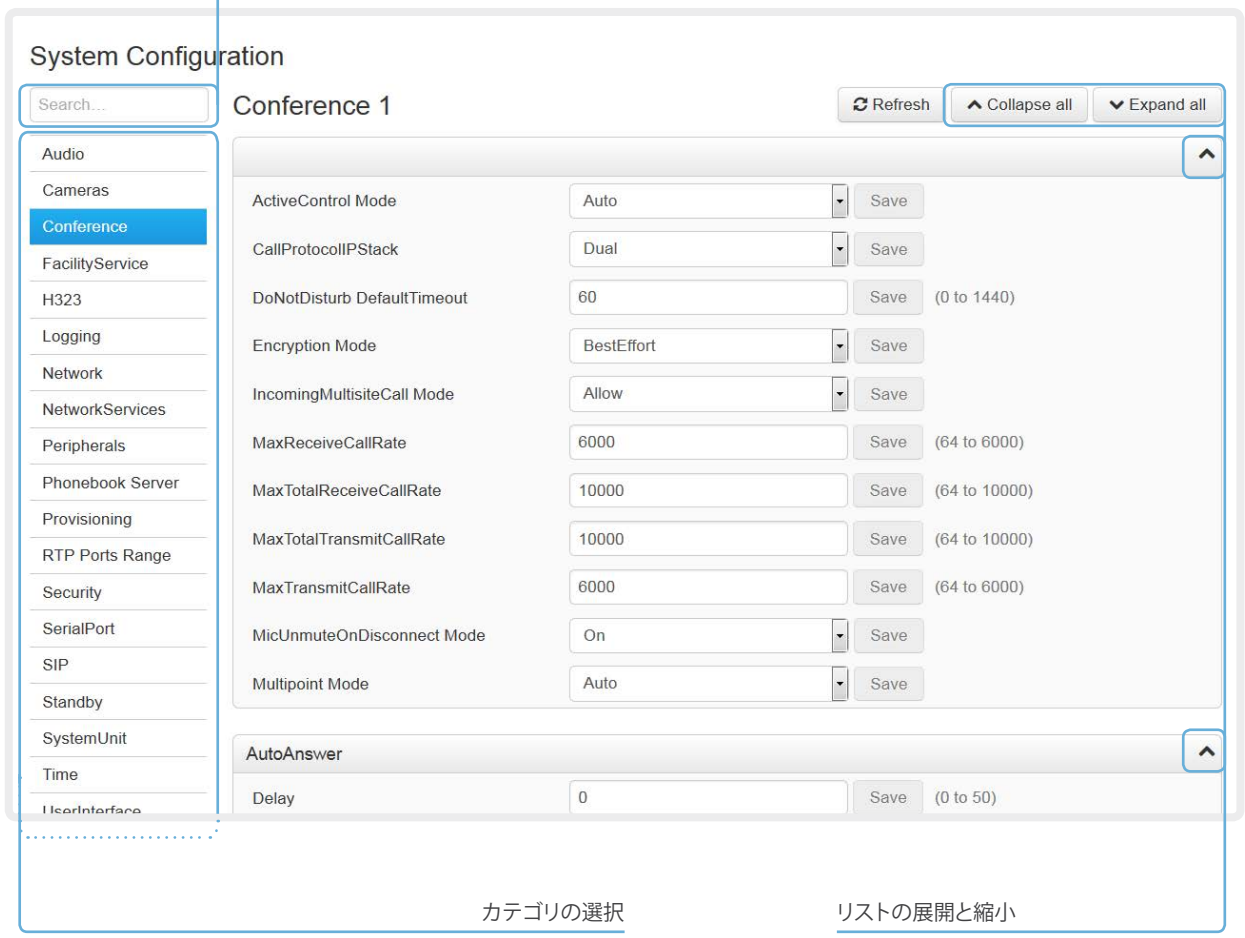
システム設定は複数のカテゴリにグループ化されます。左側のペインでカテゴリを選択すると、関連するすべての設定が右側に表示されます*。

各システム設定については、「システム設定」の章で詳しく説明します。

[設定（Configuration）] > [システム設定（System Configuration）] に移動します。

設定の検索

検索フィールドに必要な数の文字を入力します。
これらの文字を含むすべての設定（値スペースも含め）が強調表示されます。



カテゴリの選択

システム設定はカテゴリ別に構造化されています。
関連する設定を表示するには、カテゴリを選択します。

リストの展開と縮小

ボタンを使用して、すべてのリストに展開するか、個々のリストに縮小します。

* 図に示している設定は一例です。お使いのシステムの設定とは異なる場合があります。

システム設定の変更

すべてのシステム設定は [システム設定(System Configuration)] ページから変更できます*。設定の値スペースは、ドロップダウン リストまたは入力フィールドに続くテキストで指定されます。

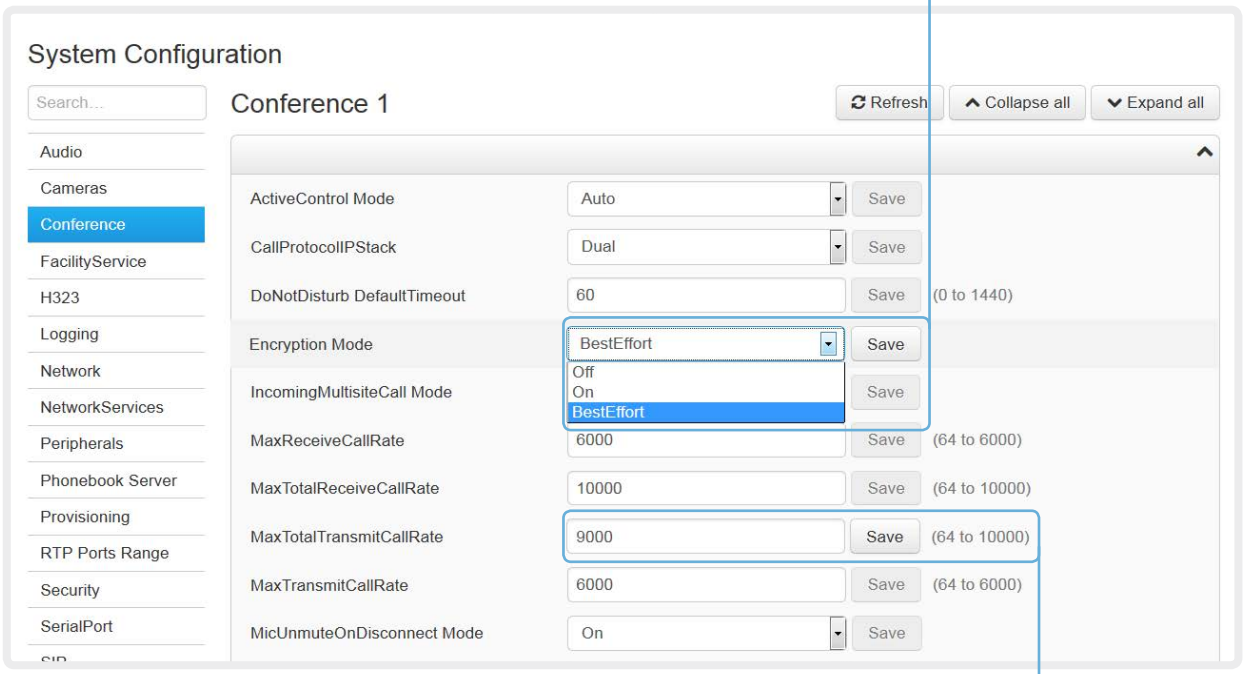
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者はすべてのシステム設定を変更できるように、すべてのユーザ ロールを所有している必要があります。

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

[設定(Configuration)] > [システム設定(System Configuration)] に移動します。

ドロップダウン リスト

矢印をクリックすると、ドロップダウン リストが開きます。優先する値を選択し、[保存(Save)] をクリックして変更を反映します。



テキスト入力フィールド

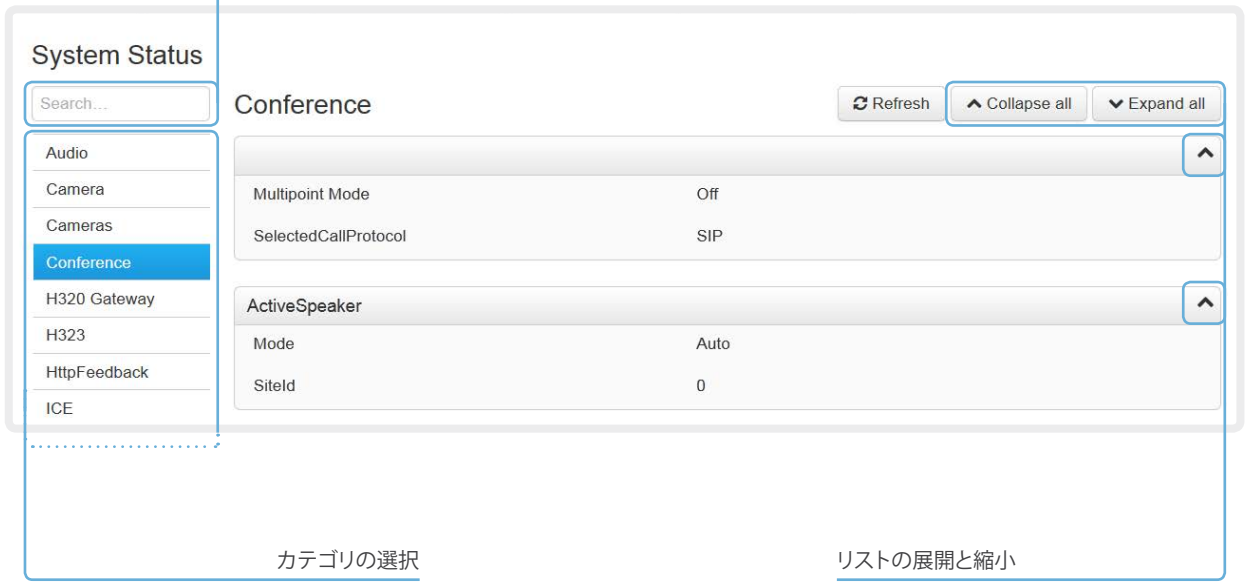
テキストを入力フィールドに入力し、[保存(Save)] をクリックして変更を反映します。

* 図に示している設定は一例です。お使いのシステムの設定とは異なる場合があります。

システム ステータス

システム ステータスは複数のカテゴリにグループ化されます。左側のカラムでカテゴリを選択すると、関連するステータスが右側のウィンドウに表示されます。*

移動先:[設定(Configuration)] > [システム ステータス(System Status)]

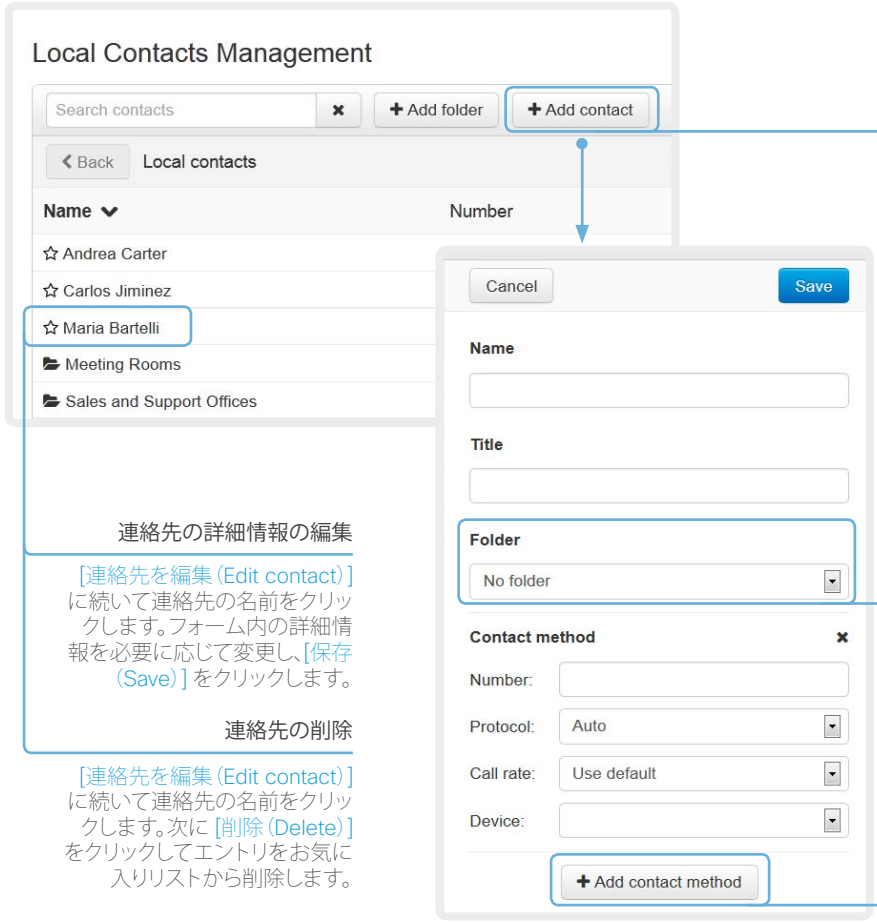


* 図に示しているステータスは一例です。お使いのシステムのステータスとは異なる場合があります。

お気に入りリストの管理

お気に入りリストのエントリはタッチ コントローラおよび Web インターフェイスからアクセスできます。

移動先:[設定(Configuration)] > [ローカルの連絡先管理(Local Contacts Management)]



連絡先の追加

[連絡先の追加(Add Contact)] をクリックし、ポップアップするフォームに入力します。次に [保存(Save)] をクリックして連絡先をお気に入りリストに保存します。

連絡先の詳細情報の編集

[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。フォーム内の詳細情報を必要に応じて変更し、[保存(Save)] をクリックします。

連絡先の削除

[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。次に [削除(Delete)] をクリックしてエントリをお気に入りリストから削除します。

連絡先をフォルダに保存

ドロップダウン リストから適切なフォルダを選択します。

[フォルダーなし(No folder)] は連絡先が最上位レベルに保存されることを意味します。

連絡方法の追加*

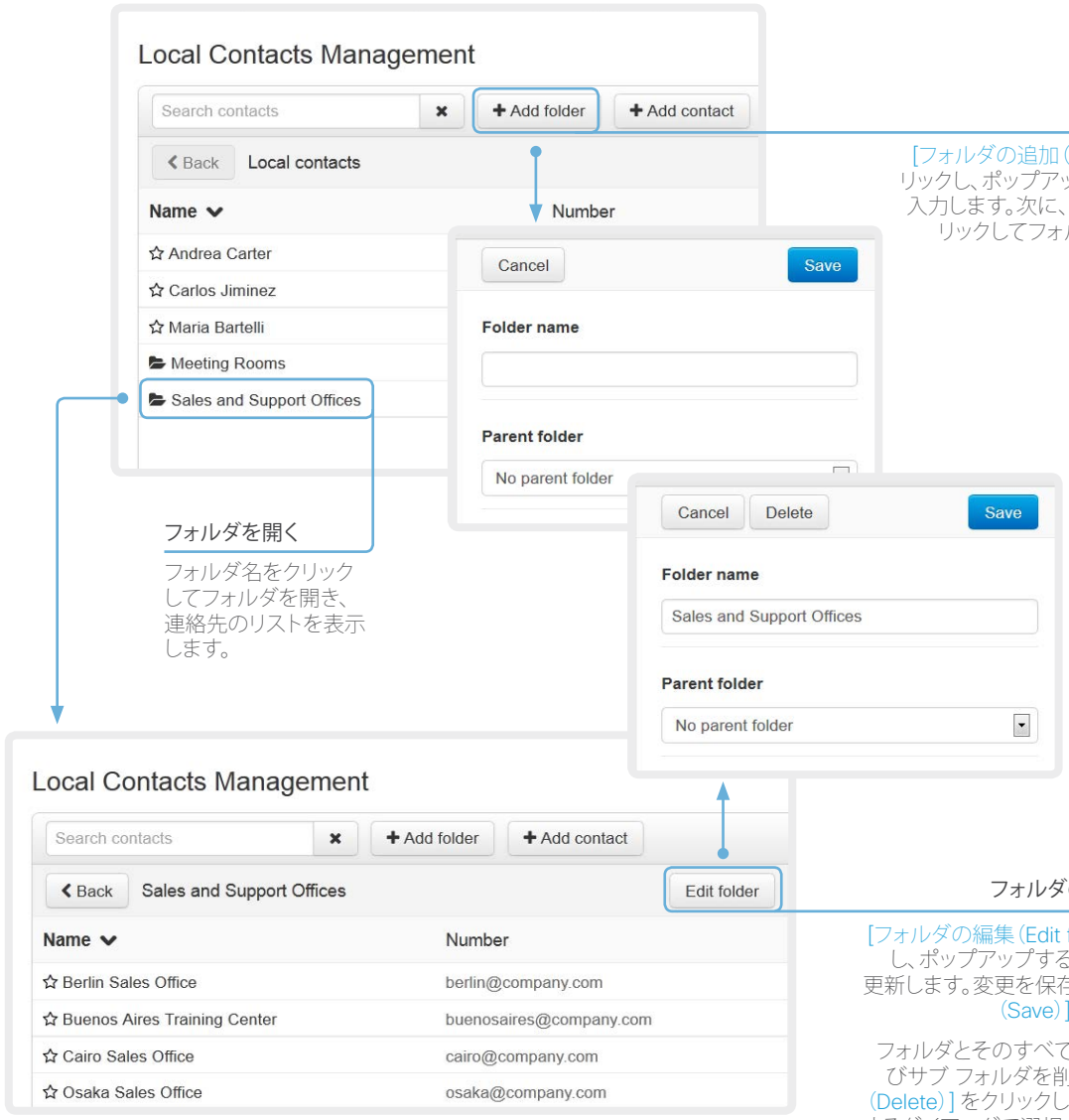
連絡先ごとに、ビデオ、電話、モバイルなど複数の連絡方法を保存できます。

* 最初の連絡方法のみがタッチ コントローラのお気に入りリストに表示されることに注意してください。

お気に入りリストのフォルダ

お気に入りリストのエントリはフォルダに整理できます。

移動先:[設定(Configuration)] > [ローカルの連絡先管理(Local Contacts Management)]



フォルダの追加

[フォルダの追加(Add Folder)] をクリックし、ポップアップするフォームに入力します。次に、[保存(Save)] をクリックしてフォルダを作成します。

フォルダを開く

フォルダ名をクリックしてフォルダを開き、連絡先のリストを表示します。

フォルダの変更または削除

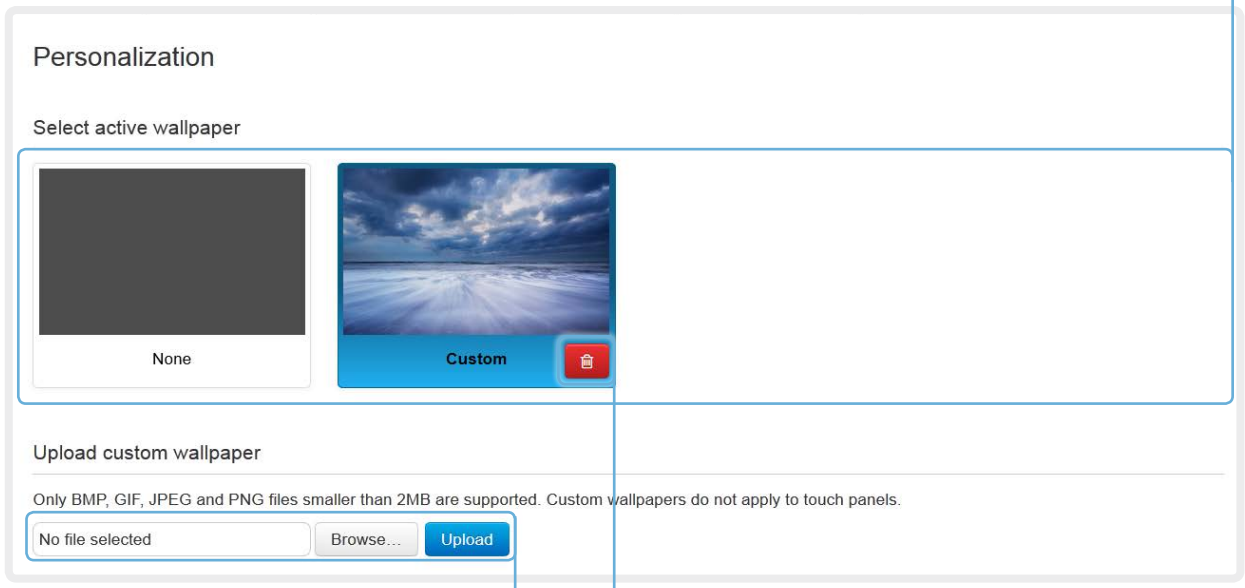
[フォルダの編集(Edit folder)] をクリックし、ポップアップするフォームの情報を更新します。変更を保存する場合は [保存(Save)] をクリックします。

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。

壁紙の選択

企業ロゴまたは別のカスタム画像をビデオ映像の背景に表示したい場合は、カスタムの壁紙をアップロードして、使用できます。

移動先:[設定(Configuration)] > [パーソナライゼーション(Personalization)]



壁紙のアクティブ/非アクティブ化

使用可能な壁紙はミニチュアで表示されます。カスタムの壁紙をアップロードした場合は、リストに表示されます。

ミニチュアをクリックし、対応する壁紙に切り替えます。壁紙を適用しない場合は、[なし(None)] を選択します。

選択したオプションが強調表示されます。

カスタムの壁紙のアップロード

[参照... (Browse…)] をクリックして、カスタム壁紙イメージ ファイルを特定します。

[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	2MByte

カスタムの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

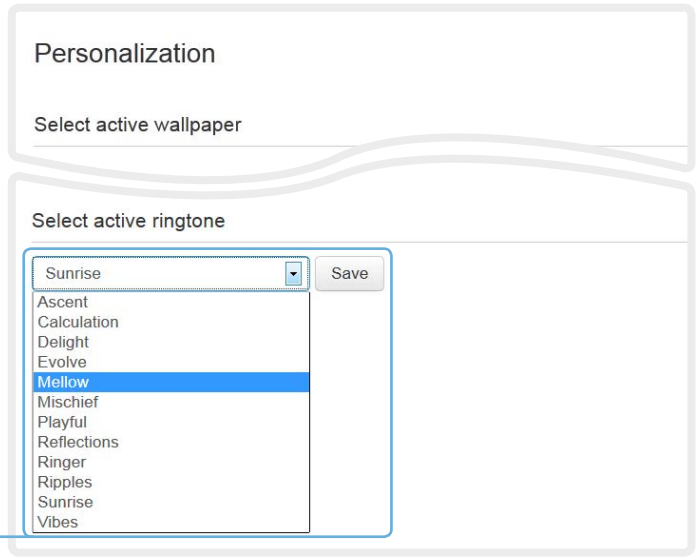
ビデオ システムからカスタムの壁紙を削除するには、削除記号をクリックします。これにより、イメージ ファイルが完全に削除され、再度使用する場合は新しくアップロードしなければならないことに注意してください。

呼び出し音の選択

定義済みの呼び出し音から選択できます。選択された呼び出し音は、このページから再生できます。

呼び出し音を再生するのはビデオ システムであり、Web インターフェイスではありません。

移動先:[設定(Configuration)] > [パーソナライゼーション(Personalization)]



呼び出し音の変更

呼び出し音をドロップダウン リストから選択して [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。

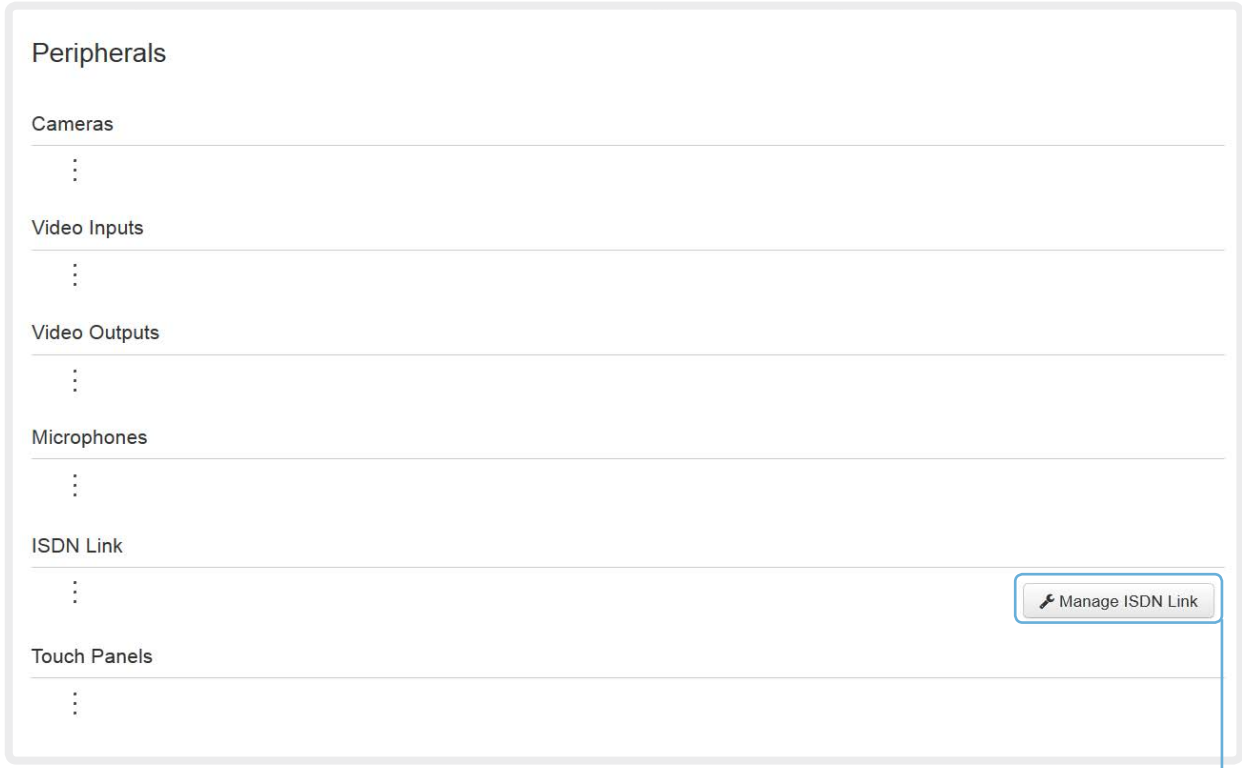
呼び出し音の音量の設定

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。

周辺機器の概要

このページでは、ビデオ入出力、カメラ、マイク、ISDN リンク、タッチ コントローラなどのビデオ システムと接続されたデバイスの概要を表示します。*

移動先:[設定(Configuration)] > [周辺機器(Peripherals)]



ISDN リンクの管理

ISDN リンクがビデオ システムとペア化されていれば、このページから管理できます。

ISDN リンクの設定および使用の方法は、http://www.cisco.com/go/isdnlink-docs の ISDN リンクのドキュメントに説明されています。

* 図に示している周辺機器は一例です。お使いのシステムでは周辺機器とビデオ入出力の設定が異なる場合があります。

ユーザ管理 (1/4 ページ)

このページからビデオ会議システムのユーザ アカウントを管理できます。

デフォルトのユーザ アカウント

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

admin ユーザのパスワードを設定する必要があります。

パスワードに関する詳細は、「パスワードの設定」の章で確認できます。

ユーザ ロールについて

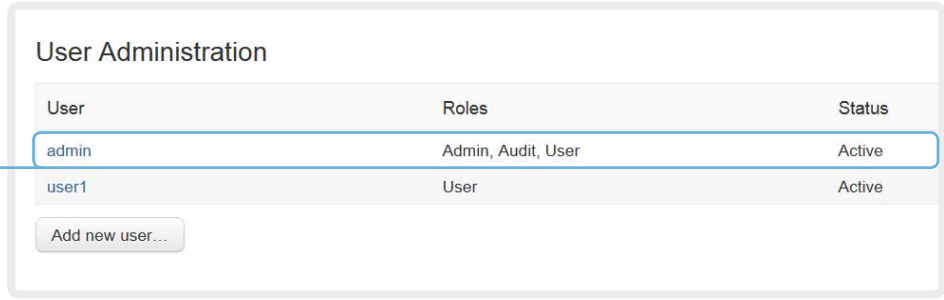
1 つのユーザ アカウントは、1 つのユーザ *ロール*またはその複数の組み合わせを保持する必要があります。

権限がオーバーラップしていない、次の 3 つのユーザ ロールが存在します。

- ADMIN：このロールを持つユーザは、新規ユーザの作成および大部分の設定の変更が可能です。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電話帳の検索が可能です。このユーザは呼び出し音量の調整や時刻と日付の表示形式の変更など、いくつかの設定を変更できます。
- AUDIT：このロールを持つユーザは、セキュリティ監査設定の変更および監査証明書のアップロードが可能です。

フル アクセス権がある管理者ユーザ アカウント（デフォルトの *admin* ユーザなど）には、3 つのロールが付与されている必要があります。

移動先：[設定（Configuration）] > [ユーザ管理（User Administration）]



デフォルトのユーザ アカウント

システムにはデフォルトのユーザ アカウントとして *admin* が登録されています。このユーザにはフル アクセス権があります。

ユーザ管理 (2/4 ページ)

新しいユーザ アカウントの作成

次の手順に従って、新しいユーザ アカウントを作成します。

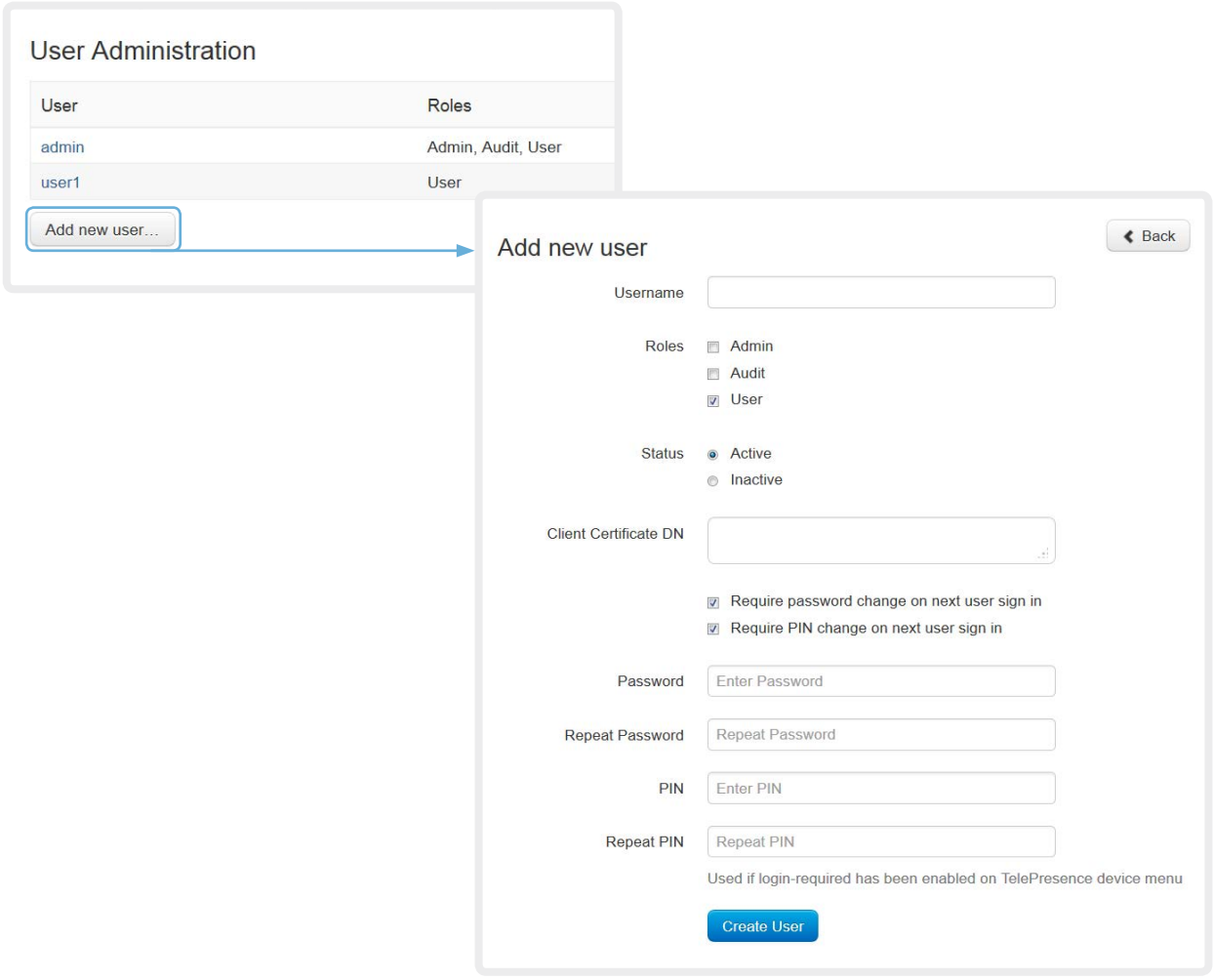
1. [新規ユーザを追加(Add New User)] を選択します。
2. [ユーザ名(Username)] と [パスワード(Password)]* に入力し、該当するユーザ ロールのチェックボックスをオンにします。

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

   HTTPS で証明書ログインを使用したい場合以外は、[クライアント証明書 DN(識別名)(Client Certificate DN)] フィールドには入力しないでください。
3. 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。
4. [ユーザの作成(Create 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。

移動先:[設定(Configuration)] > [ユーザ管理(User Administration)]



* パスワードは Web インターフェイスとコマンドライン インターフェイスで使用されます。

ユーザ管理 (3/4 ページ)

ユーザ権限の変更

次の手順に従って、ユーザ権限を変更します。

1. 既存のユーザ名をクリックすると、[ユーザの編集 (Editing user)] ウィンドウが開きます。
2. 適切なユーザ ロールのチェック ボックスをオンにし、次回サインインするときにユーザがパスワードを変更する必要があるかを指定し、HTTPS で証明書ログインを使用する場合は [クライアント証明書 DN (Client Certificate DN)] フィールドに入力します。
3. [ユーザの更新 (Update User)] をクリックして変更内容を保存します。

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

パスワードの変更

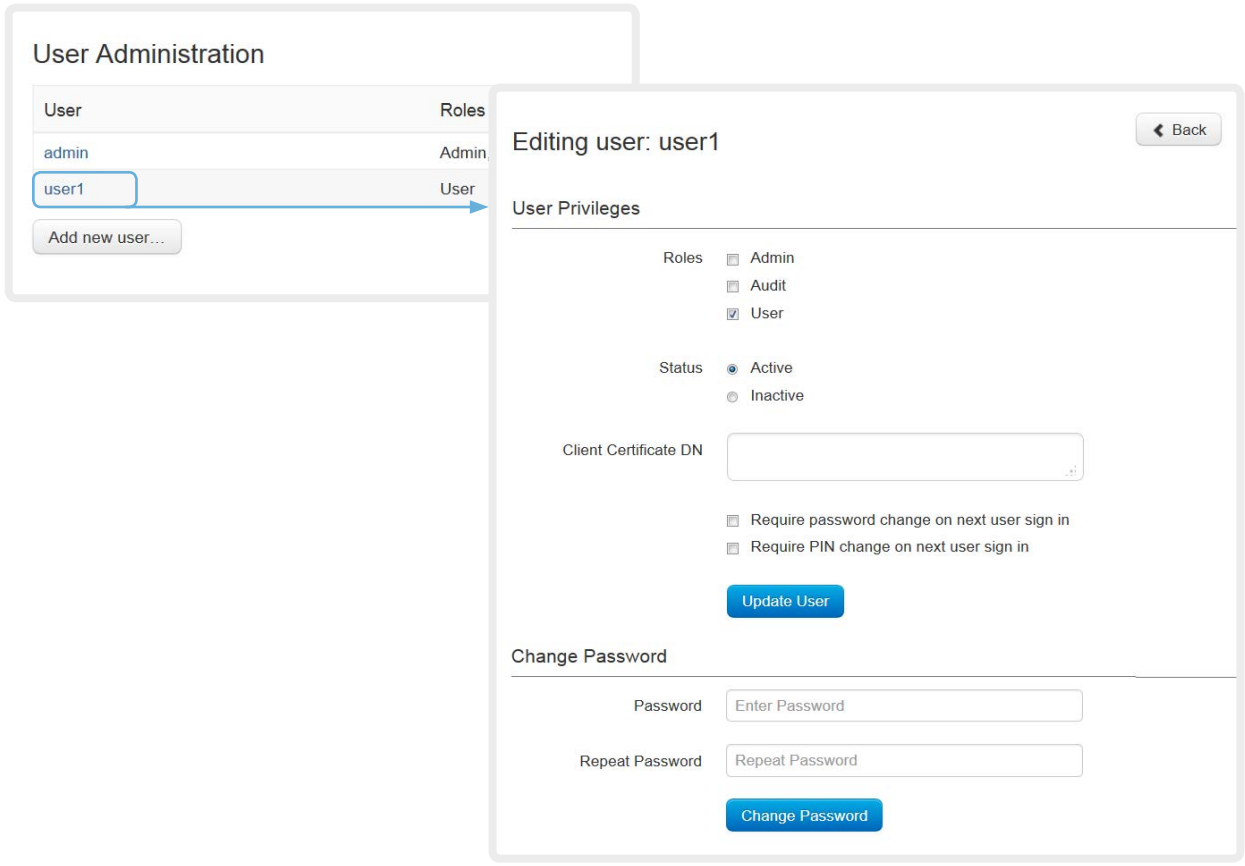
次の手順に従って、パスワードを変更します。*

1. 既存のユーザ名をクリックすると、[ユーザの編集 (Editing user)] ウィンドウが開きます。
2. 該当する入力フィールドに新しいパスワードを入力します。
3. 変更を保存するには、[パスワード変更 (Change Password)] をクリックします。

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

* パスワードは Web インターフェイスとコマンドライン インターフェイスで使用されます。

移動先:[設定 (Configuration)] > [ユーザ管理 (User Administration)]



ユーザ管理 (4/4 ページ)

ユーザ アカウントの非アクティブ化

次の手順に従って、ユーザ アカウントを非アクティブにします。

1. 既存のユーザ名をクリックすると、[ユーザの編集 (Editing user)] ウィンドウが開きます。
2. [ステータス (Status)] を [非アクティブ (Inactive)] に設定します。
3. [ユーザの更新 (Update User)] をクリックして変更内容を保存します。

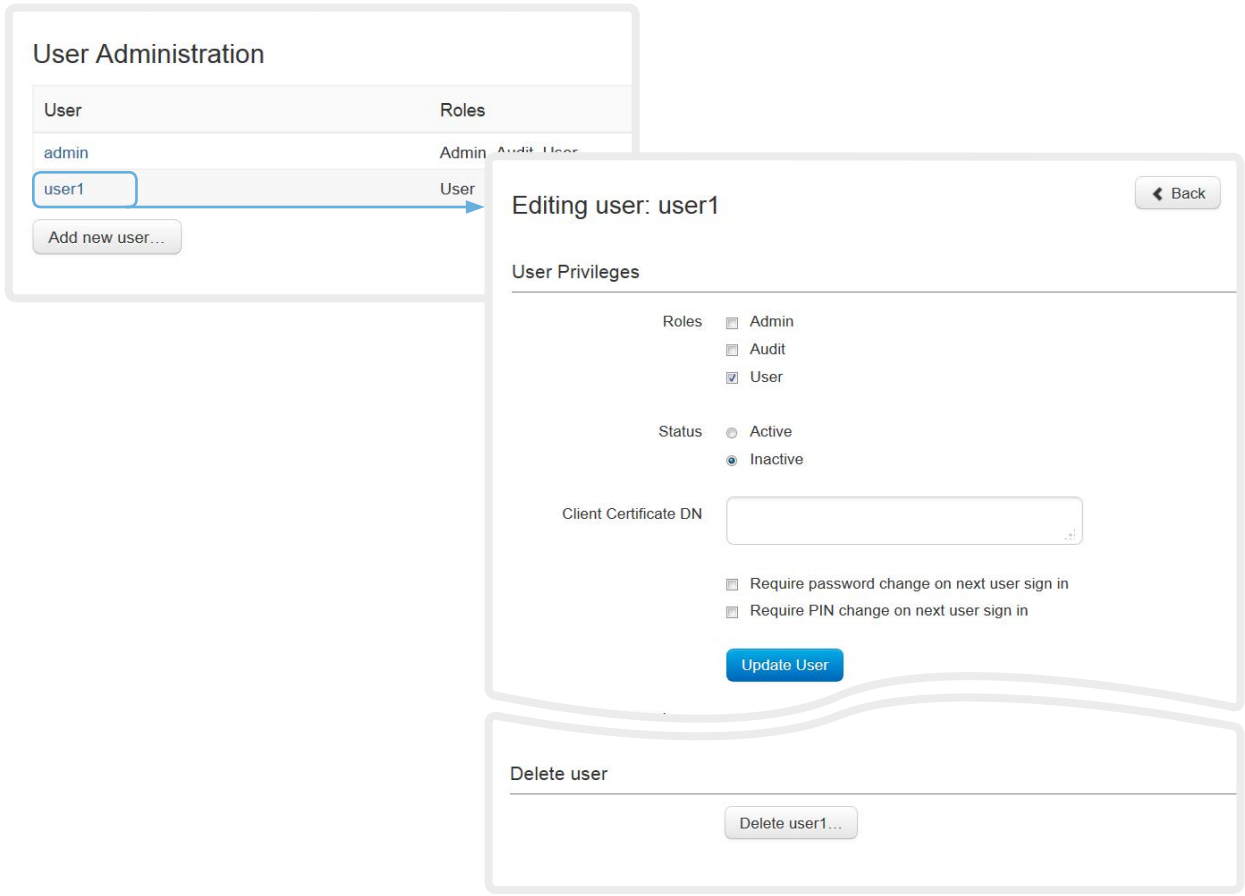
   変更を加えないで終了するには、[戻る (Back)] ボタンを使用します。

ユーザ アカウントの削除

次の手順に従って、ユーザ アカウントを削除します。

1. 既存のユーザ名をクリックすると、[ユーザの編集 (Editing user)] ウィンドウが開きます。
2. [削除 <ユーザ名>... (Delete <user name>...)] をクリックし、プロンプトが表示されたら確定します。

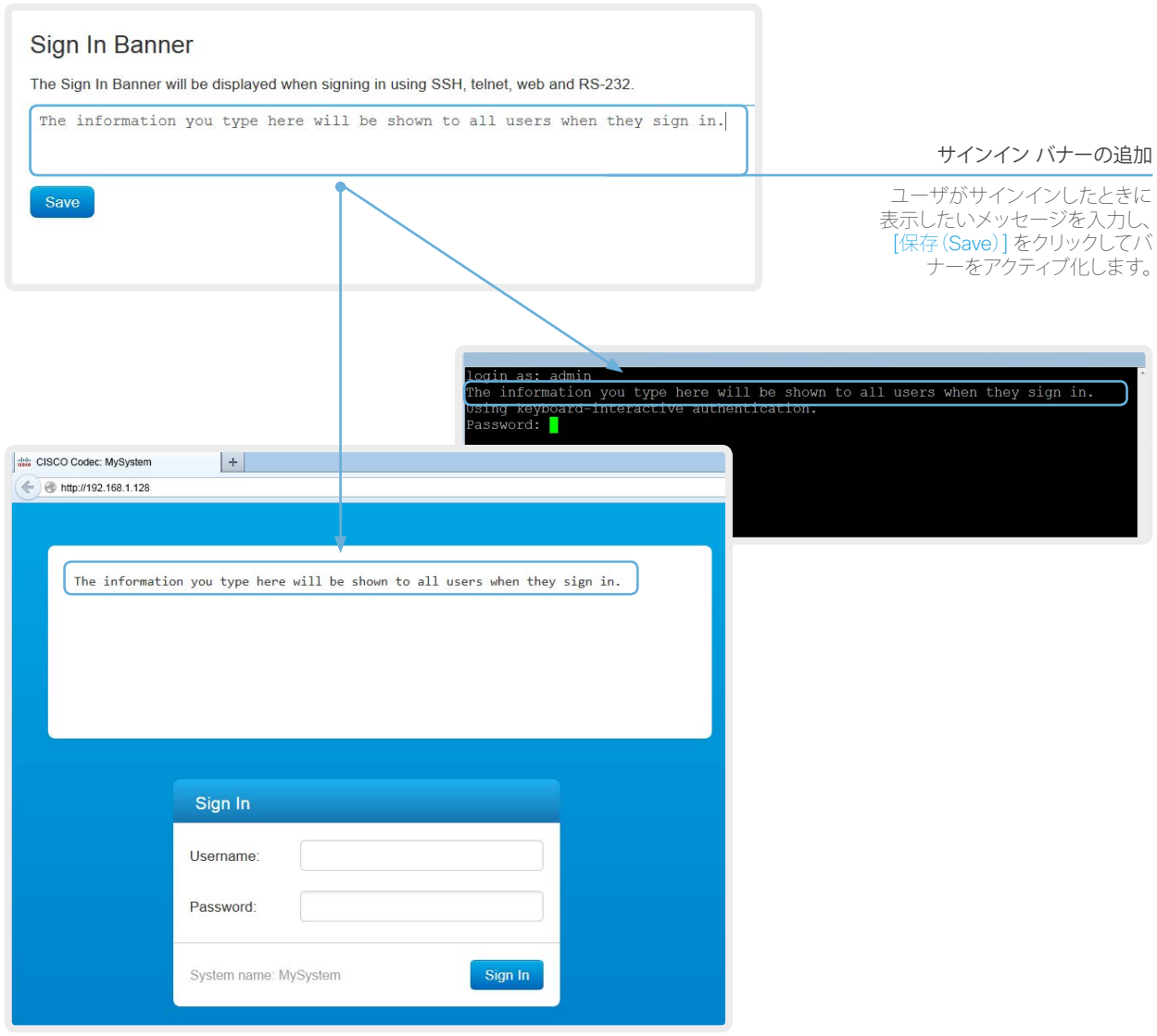
移動先:[設定 (Configuration)] > [ユーザ管理 (User Administration)]



サインイン バナーの追加

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。

移動先:[設定(Configuration)] > [サインイン バナー(Sign In Banner)]



ビデオ システムの証明書の管理

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、ビデオ システムからサーバまたはクライアントに有効な証明書を提示する必要がある場合があります。

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）によって発行される場合があります。

証明書は右の図に示すとおりに一覧表示されます。*これらは HTTPS サーバ、SIP、IEEE 802.1X および監査ログのサービスで使用できます。

システムには複数の証明書を保存できますが、各サービスで一度に使用できる証明書は 1 つだけです。

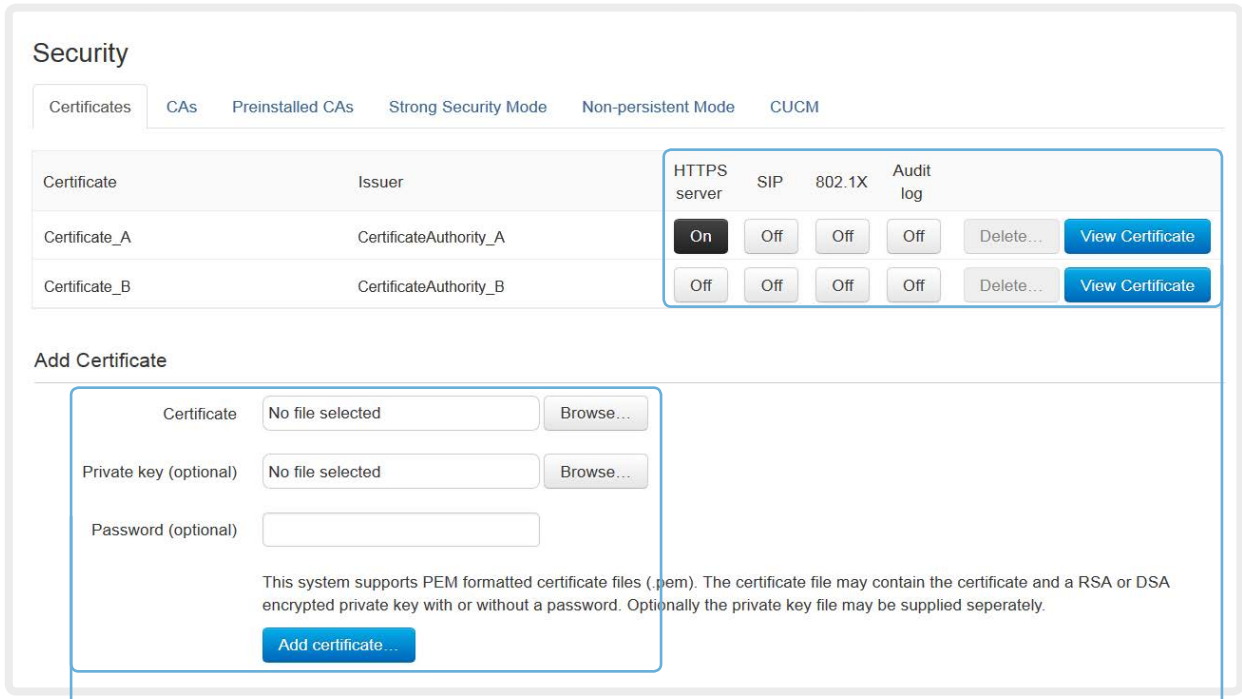
認証が失敗した場合、接続は確立されません。

次のファイルを取得するには、システム管理者に連絡します。

- 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）
- パスワード（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。

移動先：[設定（Configuration）] > [セキュリティ（Security）]：[証明書（Certificates）] タブ



証明書の追加

1. [参照...（Browse...）] をクリックしてコンピュータ上の証明書および秘密キーを探します。
2. 必要な場合には [パスワード（Password）] に入力します。
3. [監査証明書の追加...（Add audit certificate...）] をクリックして、証明書をシステムに保存します。

証明書の有効化と無効化

ボタンを使用して、各種のサービスに対して証明書をオンまたはオフに切り替えます。

また、証明書の表示および証明書の削除には、それぞれ対応するボタンを使用します。

* 図に示している証明書および証明書発行者は一例です。お使いのシステムの証明書とは異なる場合があります。

信頼できる認証局のリストの管理

(1/2 ページ)

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

通信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にビデオ システムを設定できます。

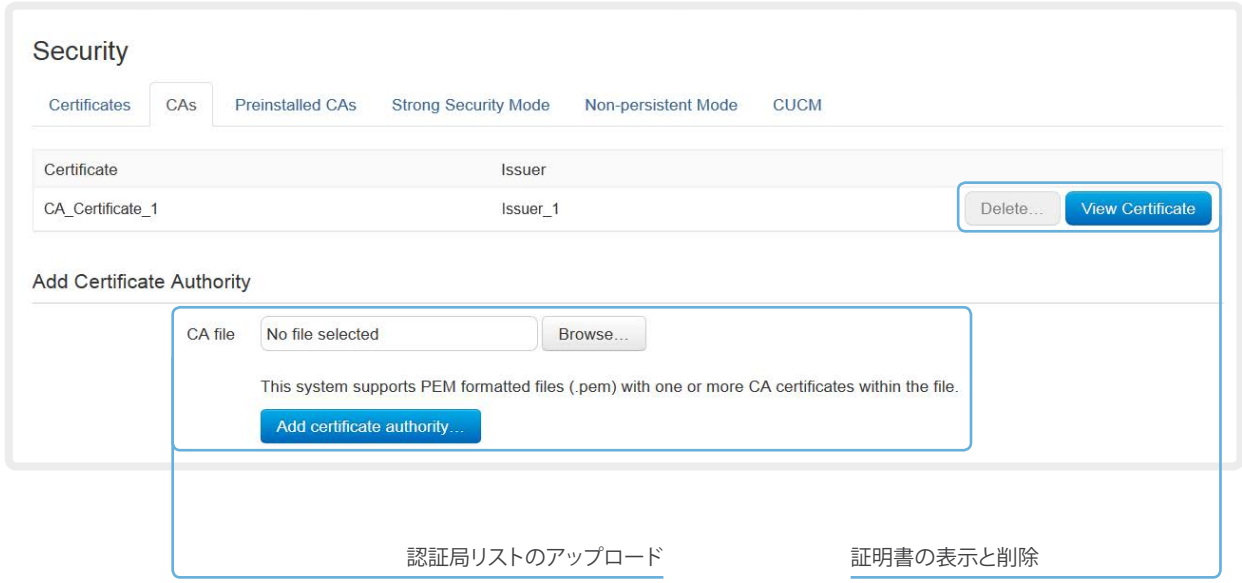
証明書は、サーバまたはクライアントの信頼性を確認するテキストファイルです。証明書は、信頼できる認証局 (CA) によって署名されている必要があります。

証明書の署名を検証するためには、信頼できる CA のリストがビデオ システムに存在する必要があります。CA の証明書は右の図に示すとおりに一覧表示されます。*

リストには、監査ログ、HTTPS、SIP および IEEE 802.1X 接続用の証明書を検証するために必要なすべての CA を含める必要があります。

サーバを認証できない場合、接続は確立されません。

移動先:[設定 (Configuration)] > [セキュリティ (Security)]:[CA] タブ



認証局リストのアップロード

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追加されます。したがって、以前に保存した証明書は削除されません。

i. [参照... (Browse...)] をクリックして、お使いのコンピュータで CA 証明書のリストを含むファイル (ファイル形式:.PEM) を探します。

ii. [証明局の追加... (Add certificate authority...)] をクリックして、新しい CA 証明書をシステムに保存します。

CA 証明書リスト (ファイル形式:.PEM) を取得するには、システム管理者に連絡します。

証明書の表示と削除

証明書の表示および証明書の削除には、それぞれ対応するボタンを使用します。

* 図に示している証明書および証明書発行者は一例です。お使いのシステムの証明書とは異なる場合があります。

信頼できる認証局のリストの管理

(2/2 ページ)

ソフトウェア バージョン TC7.2 より、監査サーバのシグニチャは他のサーバ/クライアントと同じ CA リストを使用して検証されます。

安全な監査ロギングのセットアップ

監査ログには、ビデオ システム上のすべてのサインイン アクティビティと設定の変更が記録されます。

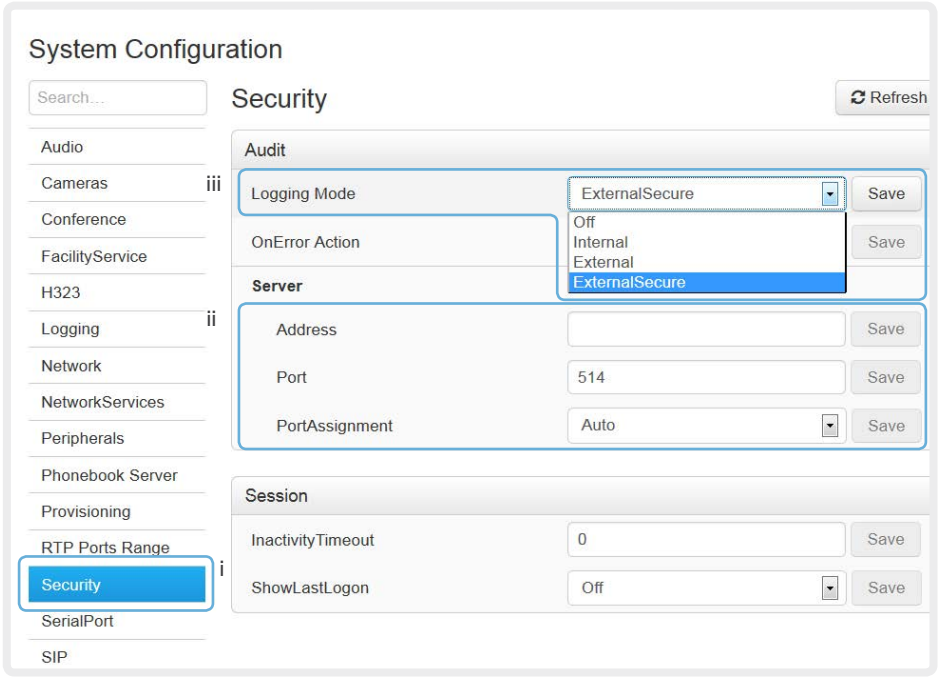
監査ログはデフォルトではディセーブルですが、[セキュリティ (Security)] > [監査 (Audit)] > [ロギング (Logging)] > [モード (Mode)] を使用してイネーブルにできます。

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。

監査サーバを認証できない場合、ログは送信されません。

セキュア監査ログをイネーブルにする前に、常に信頼できる認証局のリストをアップロードしてください。

移動先:[設定 (Configuration)] > [セキュリティ (Security)]:[CA] タブ / [設定 (Configuration)] > [システム設定 (System Configuration)]



セキュア監査ログのイネーブル化

i. [システム設定 (System Configuration)] ページに移動し、[セキュリティ (Security)] カテゴリを選択します。

ii. 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)] で [手動 (Manual)] を選択した場合、監査サーバの [ポート (Port)] 番号も入力する必要があります。[保存 (Save)] をクリックして変更を有効にします。

iii. [ロギング モード (Logging Mode)] ドロップダウン リストから [外部セキュア (ExternalSecure)] を選択します。[保存 (Save)] をクリックして変更を有効にします。

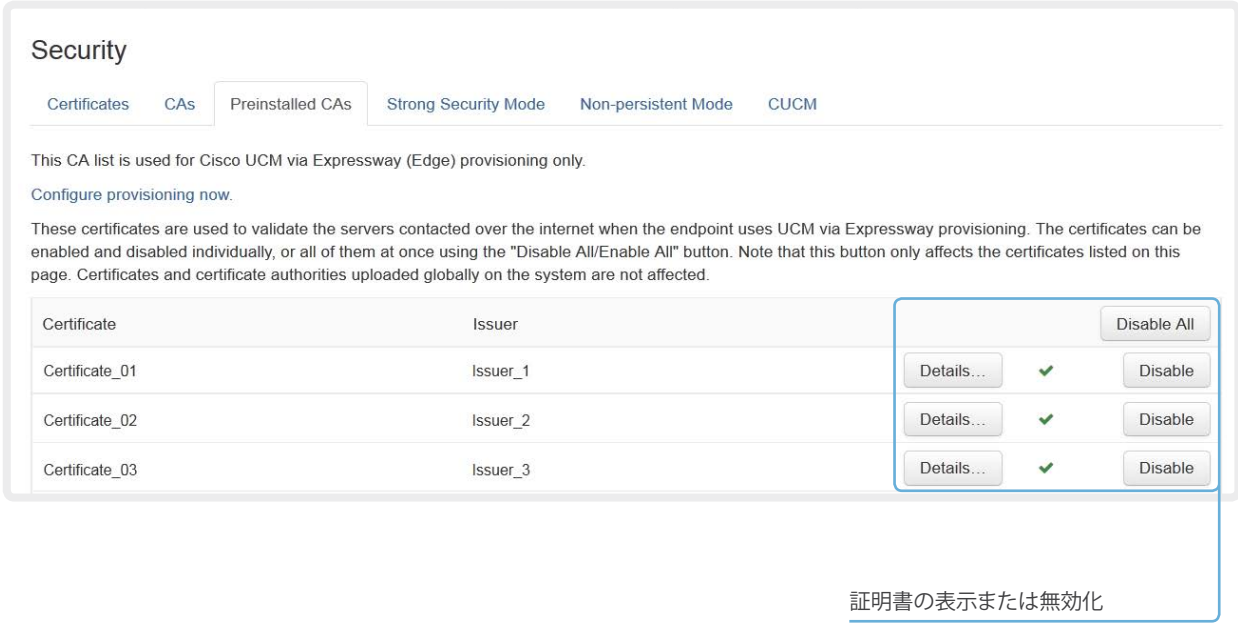
プレインストールされた Edge プロビジョニングの証明書の管理

Web インターフェイスで、このページに表示されるプレインストールされた証明書のリスト* には、Expressway（Edge）経由の Cisco Unified Communications Manager（CUCM）によりビデオ システムがプロビジョニングされる場合に使用する証明書が含まれます。Edge インフラストラクチャの証明書だけがこのリストに対して検証されます。

Edge インフラストラクチャの証明書の検証が失敗すると、ビデオ システムはプロビジョニングを受け取らず、登録されません。

ビデオ システムを出荷時の状態にリセットしても、プリインストールされた証明書のリストは削除されません。

移動先：[設定（Configuration）] > [セキュリティ（Security）]：[プリインストールされた CA（Preinstalled CA）] タブ



証明書の表示または無効化

証明書の表示および証明書の無効化には、それぞれ対応するボタンを使用します。

プレインストールされたすべての証明書を無効化にして、代わりに手動でアップロードした証明書のリストを検証に使用できます。信頼できる証明書を手動でビデオ システムにアップロードする方法は、[設定（Configuration）] > [セキュリティ（Security）]：[CA] ページで確認できます。

* 図に示している証明書および証明書発行者は一例です。お使いのシステムの証明書とは異なる場合があります。

強力なセキュリティ モードの設定

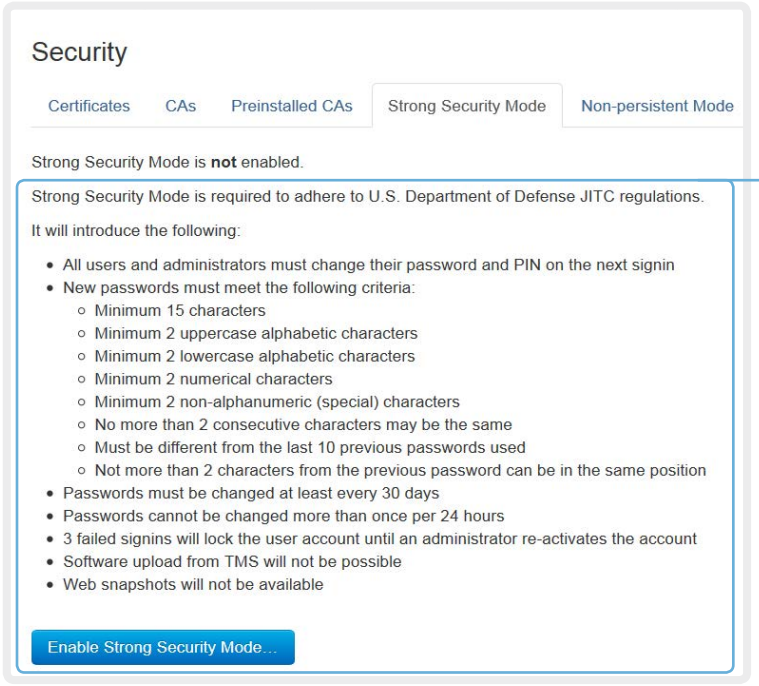
強力なセキュリティ モードは、DoD JITC への準拠が必要な場合にのみ使用する必要があります。

強力なセキュリティ モードを設定する前に、表示される情報をよく確認してください。

強力なセキュリティ モードでは非常に厳格なパスワード要件が設定され、すべてのユーザが次回のサインイン時にパスワードを変更することを要求します。

TMS からのソフトウェアのアップロード、Web スナップショット、および Web インターフェイスからの発信は、強力なセキュリティ モードでは禁止されます。

移動先:[設定(Configuration)] > [セキュリティ(Security)]:[強力なセキュリティ モード(Strong Security Mode)]タブ



強力なセキュリティ モードの設定

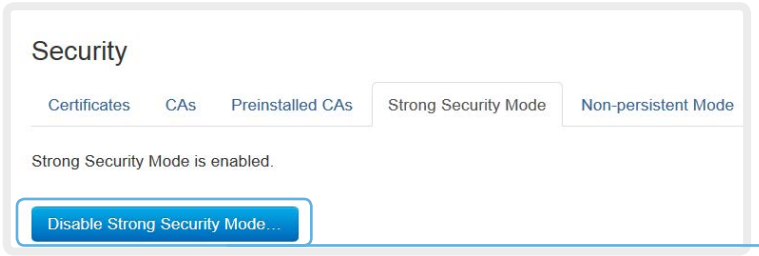
続行する前に、強力なセキュリティ モードによる影響について注意してお読みください。

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。

   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、パスワードを変更します。新しいパスワードは説明にしたがって厳格な基準を満たす必要があります。

   システム パスワードの変更方法については、「パスワードの設定」の項で説明します。



通常モードに戻る

強力なセキュリティ モードのときは、[強力なセキュリティ モードの無効化... (Disable strong security mode...)] をクリックすることにより、システムを通常モードに復元できます。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。

システムが自動的に再起動します。

永続モードの変更

デフォルトでは、すべての永続設定は [永続 (Persistent)] に設定されます。つまり、設定、コール履歴、内部ログ、ローカル電話帳/お気に入りリスト、IP 接続情報が通常どおり保存されます。システムを再起動しても情報は削除されません。

原則として、永続のデフォルト設定を変更しないことを推奨します。ただし、以前のセッションでロギングされたすべての情報の表示またはトレースをユーザに許可しない場合は、[非永続 (Non-persistent)] モードを使用する必要があります。

[非永続 (Non-persistent)] モードに変更する前に保存された情報を消去/削除するには、ビデオ システムを出荷時の状態にリセットすることを検討する必要があります。

工場出荷時設定へのリセットに関する詳細情報は、付録の「工場出荷時設定へのリセット」に記述してあります。

[非永続 (Non-persistent)] モードのときは、システムを起動するたびに次の情報は削除/消去されます。

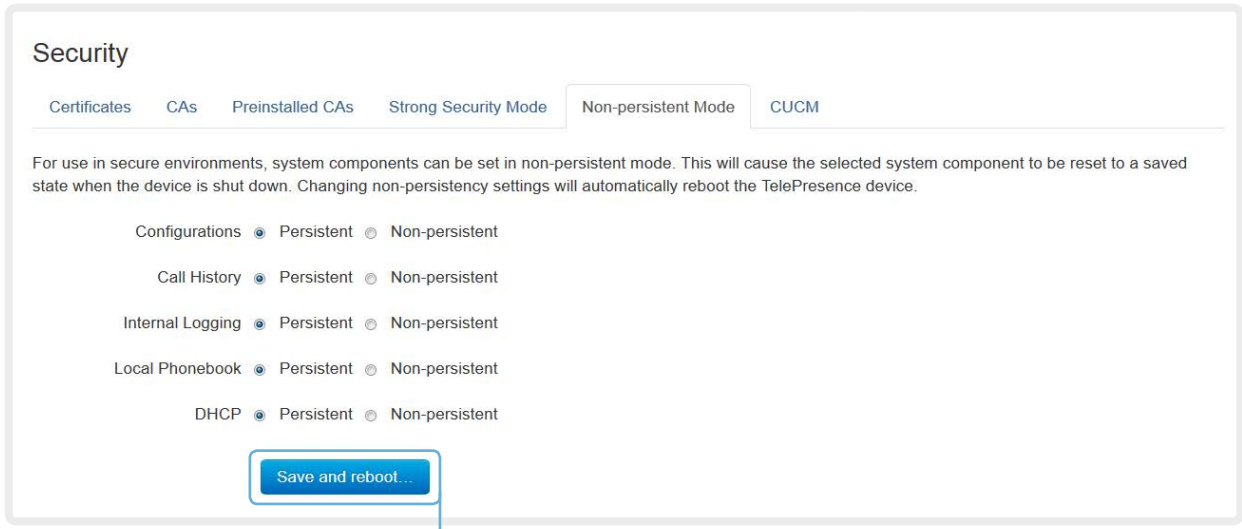
- 最後の再起動以降に行ったシステム設定の変更。
- 最後の再起動以降に行った発信または受信コールに関する情報 (通話履歴)。
- 最後の再起動以降に作成された内部ログ ファイル システム。
- 最後の再起動以降に行ったローカルの連絡先/お気に入りリストの変更。
- 前回のセッション以降のすべての IP 関連情報 (DHCP)。

永続状態の確認

[セキュリティ (Security)] ページを開き、[非永続モード (Non-persistent Mode)] タブに移動すると、アクティブなオプション ボタンにビデオ システムの現在の永続状態が示されます。

また、[設定 (Configuration)] > [システム ステータス (System Status)] ページで [セキュリティ (Security)] > [永続 (Persistency)] を表示し、状態を確認することもできます。

移動先:[設定 (Configuration)] > [セキュリティ (Security)]:[非永続モード (Non-persistent Mode)]タブ



永続設定の変更

1. 必要に応じて 5 つのカテゴリで永続設定を設定します。
2. [保存して再起動... (Save and reboot...)] をクリックします。

   システムが再起動します。再起動後に、新しい永続設定に従った動作が開始されます。

   非永続モードに切り替える前に保存されたログや構成などは、消去または削除されないことに注意してください。

信頼リストの削除（CUCM のみ）

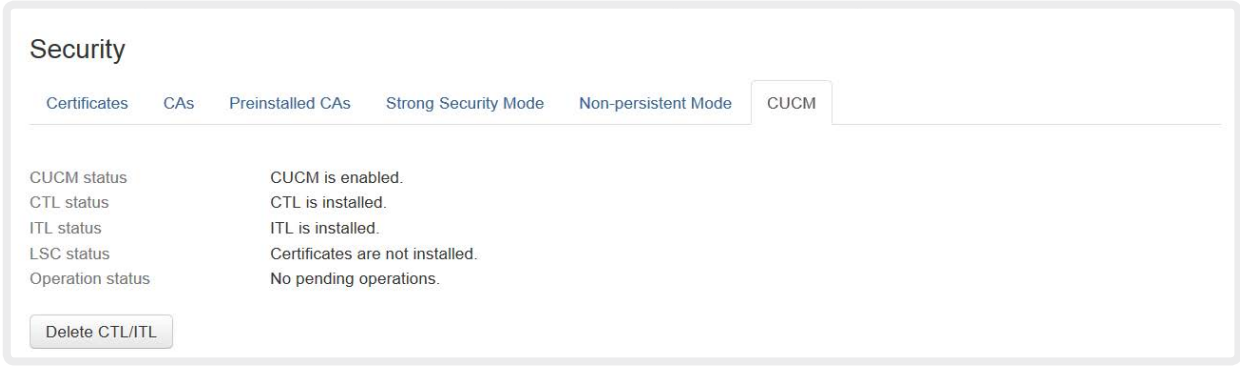
このページの情報は、Cisco Unified Communications Manager（CUCM）に登録されているビデオ システムにのみ関連します。

Web インターフェイスはビデオ システムに保存された既存の信頼リスト（CTL および ITL）を削除するために使用できます。通常、古い CTL および ITL ファイルは削除しませんが、いくつかの場合に削除する必要があります。

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。

CUCM および信頼リストに関する詳細情報は、シスコの Web サイトにある『*Administering TC Endpoints on CUCM*』ガイドをお読みください。

移動先：[設定（Configuration）] > [セキュリティ（Security）]：[CUCM] タブ



トラブルシューティング

[トラブルシューティング（Troubleshooting）] 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。このリストは製品およびインストールによって異なる場合があります。*

重大な問題やエラーは赤、警告は黄色で明確に示されていることに注意してください。

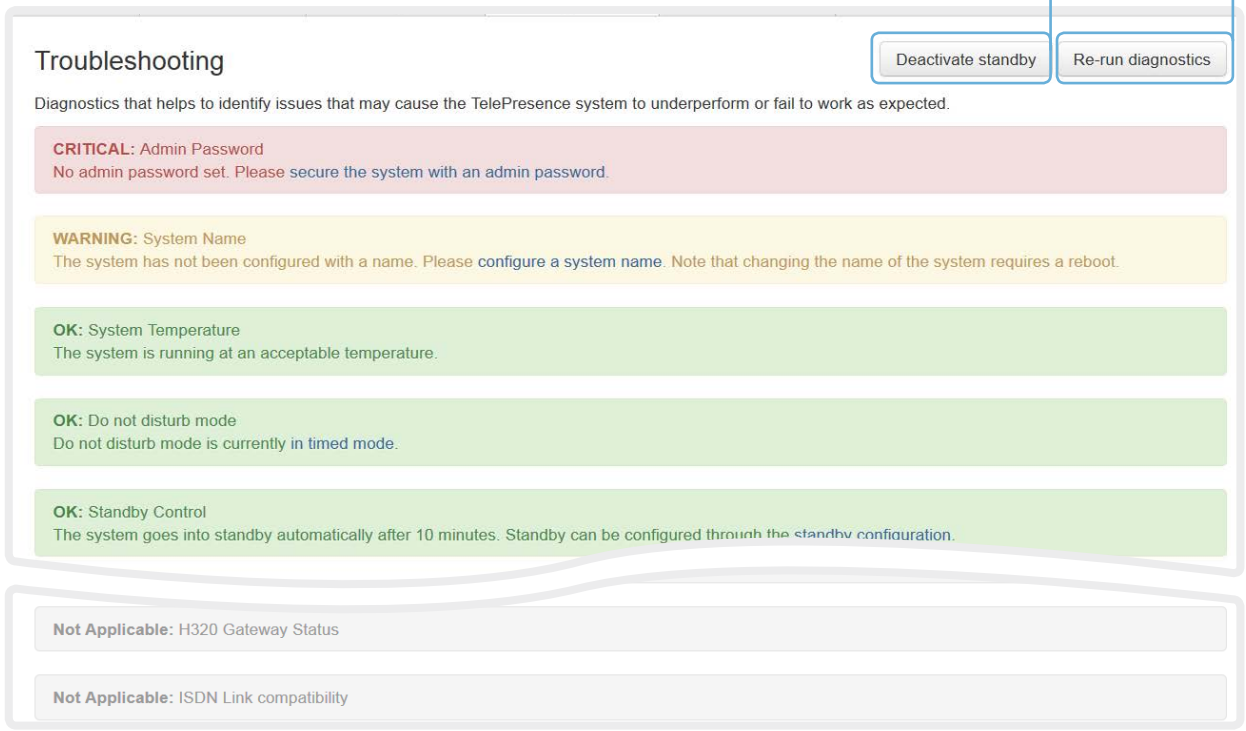
移動先：[診断（Diagnostics）] > [トラブルシューティング（Troubleshooting）]

診断の実行

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

スタンバイ モードを離れる

このボタンは、システムがスタンバイ モードのときにだけ表示されます。スタンバイ モードで [スタンドバイの非アクティブ化（Deactivate standby）] をクリックして、システムを復帰させます。



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

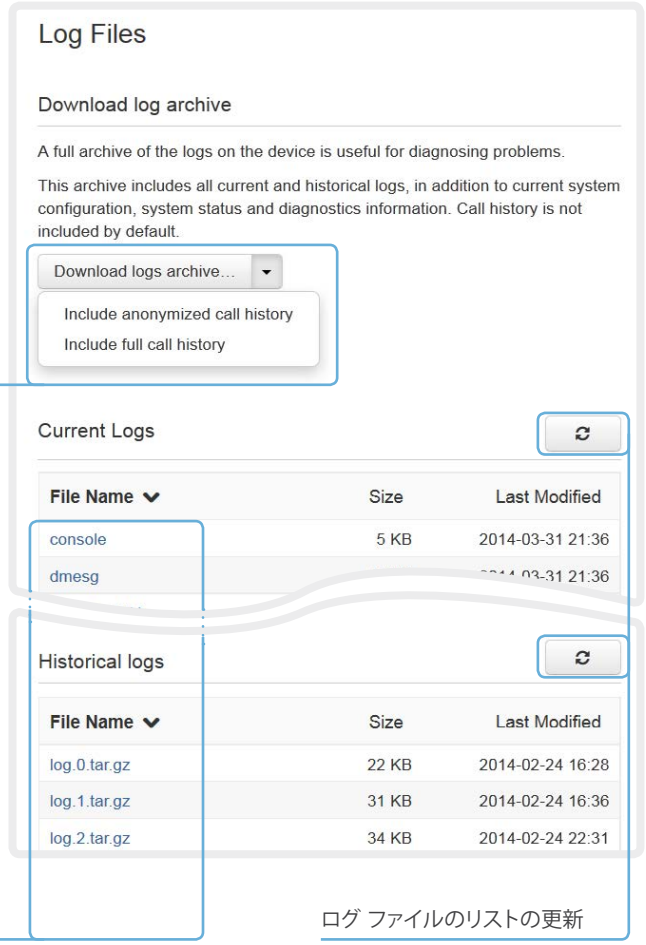
ログ ファイルのダウンロード

ログ ファイル* は、技術サポートが必要な場合にシスコのサポート組織によって要求される可能性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。

すべての Current log ファイルは、システムを再起動するたびにタイムスタンプ付きの *Historical log* ファイルに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。

移動先:[診断(Diagnostics)] > [ログ ファイル(Log Files)]



すべてのログファイルのダウンロード

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

アーカイブに通話履歴を含める場合はドロップダウン リストを使用します。全通話履歴を含めるか、発信者/受信者を匿名にするかを選択できます。

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。

ログ ファイルのリストの更新

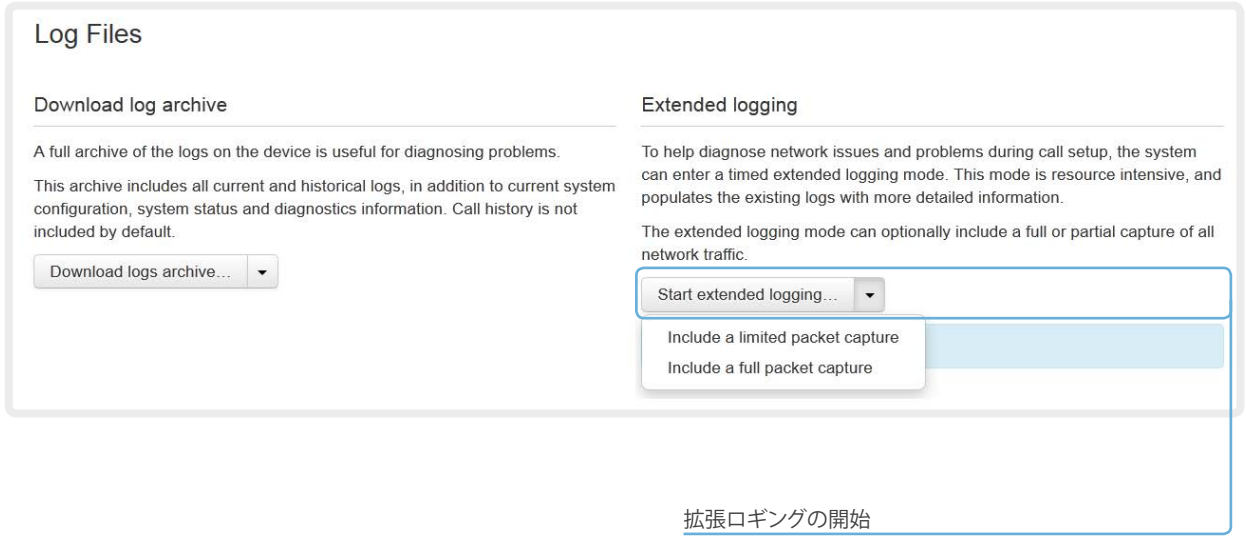
* 図に示しているログ ファイルは一例です。お使いのシステムには他のファイルがある場合があります。

拡張ロギングの開始

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ることに注意してください。拡張ロギング モードは問題のトラブルシューティング時のみに使用すべきです。

移動先:[診断(Diagnostics)] > [ログ ファイル(Log Files)]



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。

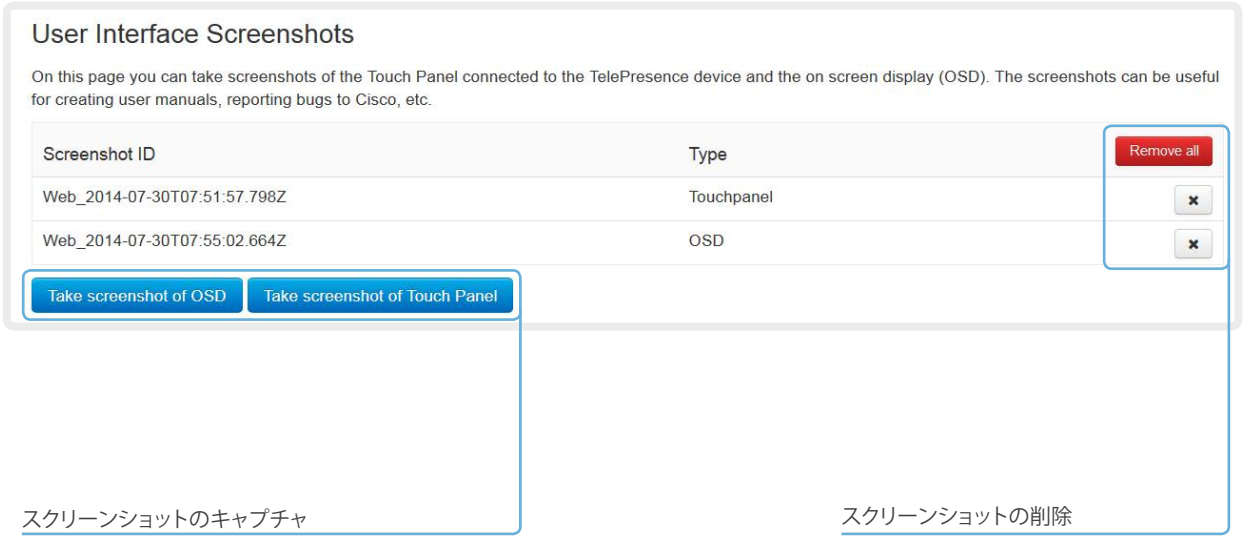
拡張ロギングは 10 分間継続します。タイムアウトする前に、拡張ロギングがオンのときに表示される [拡張ロギングの停止(Stop extended logging)] ボタンをクリックして拡張ロギングを停止する必要があります。

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 トラフィックの全部または一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。

スクリーンショットのキャプチャ

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

移動先：[診断（Diagnostics）] > [ユーザ インターフェイスのスクリーンショット（User Interface Screenshots）]



スクリーンショットのキャプチャ

[タッチ パネルのスクリーンショットを撮る（Take screenshot of Touch Panel）] をクリックし、タッチ コントローラのスクリーンショットをキャプチャするか、[OSD のスクリーンショットを撮る（Take screenshot of OSD）] をクリックして画面上の表示のスクリーンショットをキャプチャします。

スクリーンショットはボタンの下の領域に表示されます。スクリーンショットの準備ができるまで 30 秒かかることに注意してください。

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

スクリーンショットの削除

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

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

システム ソフトウェアのアップグレード

このビデオ会議システムは TC 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、TC7.2 です。

ソフトウェアのバージョンに関する質問はシステム管理者に問い合わせてください。

ソフトウェア リリース ノート

新情報および変更のすべての概要については、ソフトウェア リリース ノート（TC7）を読むことを推奨します。

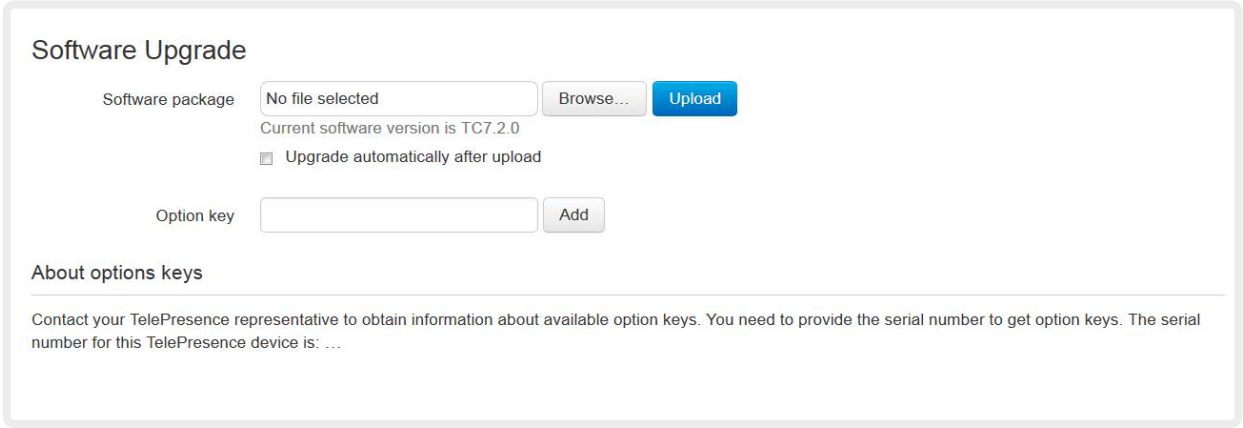
URL：http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

新しいソフトウェア

ソフトウェアをダウンロードするには、Cisco Download Software Web ページ（http://www.cisco.com/cisco/software/navigator.html）に移動します。次に、お使いの製品に移動します。

ファイル名の形式は「s52010tc7_2_0.pkg」です（各ソフトウェア バージョンに一意のファイル名があります）。

移動先：[メンテナンス（Maintenance）] > [ソフトウェア アップグレード（Software Upgrade）]



オプション キーの追加

*オプション キー*はオプション機能をアクティブにするために必要です。システムには複数のオプション キーがある場合があります。すでにキーがインストールされている場合は、この項目をスキップしてソフトウェア インストールに進むことができます。

必要なキーがない場合は、シスコの営業担当者に連絡し、キーを取得してください。

i. *オプション キー*を適切なテキスト入力フィールドに入力し、[追加（Add）] をクリックします。

   オプション キーが複数ある場合は、すべてのキーに対してこの手順を繰り返してください。

各ビデオ システムには次のような一意のオプション キーがあります。

- 1R000-1-AA7A4A09

新しいソフトウェアのインストール

Cisco Download Software Web ページ（左のリンク参照）から適切なソフトウェア パッケージをダウンロードして、ローカル コンピュータに格納します。これは .pkg ファイルです。

i. [参照...（Browse...）] をクリックして、新しいソフトウェアを含むダウンロードされた .pkg ファイルを探します。

ii. [アップロード後に自動アップグレード（Upgrade automatically after upload）] チェックボックスをオンにして [アップロード（Upload）] をクリックすると、インストール プロセスがすぐに開始されます。

   ソフトウェアを今すぐアップロードし、後でインストールを行う場合は、チェックボックスをオフにしたままにします。

インストールの完了には最長で 30 分ほどかかる場合があります。Web ページから進捗状況を確認できます。インストール後、システムは自動的に再起動します。

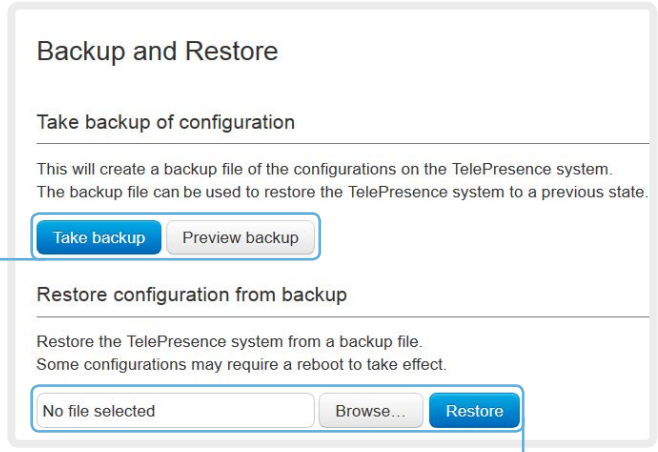
再起動後に Web インターフェイスで作業を再開するには、再度サインインする必要があります。

バックアップと復元

[システム設定(System configuration)] ページで使用可能なすべてのシステム設定は、画面上に一覧表示するか、テキスト ファイルとして保存できます。

テキスト ファイルをシステムに再度ロードして設定を復元することができます。

移動先:[メンテナンス(Maintenance)] > [バックアップと復元(Backup and Restore)]



現在の設定のバックアップまたは表示

現在の設定を画面上に表示するには、[バックアップのプレビュー(Preview backup)] をクリックします。

設定をテキスト ファイルとして保存するには、[バックアップを取る(Take backup)] をクリックします。

以前の設定の復元

[参照... (Browse…)] をクリックし、復元したい設定を含むファイルを探します。

システムをファイルで定義されているとおりに再設定するには、[復元(Restore)] をクリックします。

以前に使用していたソフトウェア バージョンへの復元

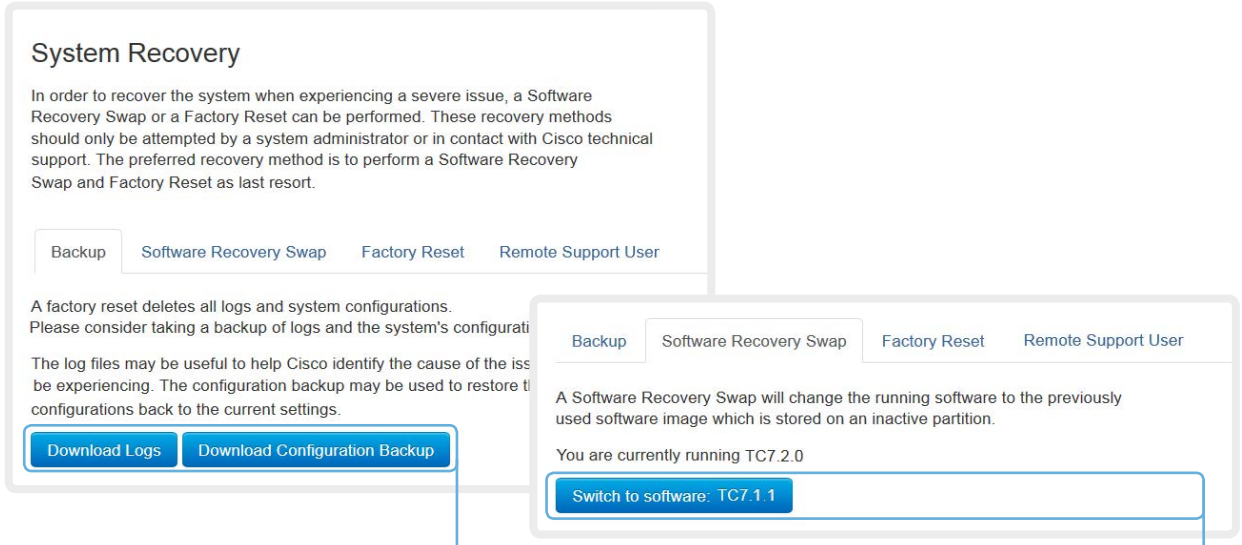
ビデオ システムに重大な問題がある場合は、これまで使用していたソフトウェア バージョンに切り替えることにより問題の解決に役立つ場合があります。

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出荷時の状態にリセットしていない場合は、これまで使用したソフトウェア イメージは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。

以前使用していたソフトウェア バージョンへの復元は、システム管理者が行うか、シスコのテクニカル サポートにお問い合わせいただくことによってのみ行われます。

他のソフトウェア イメージにスワップする前に、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強く推奨します。

移動先:[メンテナンス(Maintenance)] > [システム リカバリ(System Recovery)]:[バックアップ(Backup)] タブおよび [ソフトウェア リカバリのスワップ(Software Recovery Swap)] タブ



1. ログ ファイルとシステム設定のバックアップ

他のソフトウェア イメージにスワップする前に、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推奨します。

[ログのダウンロード(Download Logs)] と [設定のバックアップをダウンロード(Download Configuration Backup)] をクリックし、手順に従ってファイルをコンピュータに保存します。

2. 以前に使用していたソフトウェア バージョンへの復元

1. [ソフトウェア TCx.y.z... への切り替え(Switch to software TCx.y.z...)] をクリックして以前使用していたソフトウェア バージョンに戻します。x.y.z はソフトウェアのバージョンを示します。
2. [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止めます。

   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。

工場出荷時の状態へのリセット

ビデオ システムに重大な問題が発生した場合、最後の手段として工場出荷時のデフォルト設定にリセットすることができます。工場出荷時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、これによりシステムがリカバリされます。*

工場出荷時の状態へのリセットは、システム管理者が行うか、シスコのテクニカル サポートにお問い合わせいただくことによってのみ行われます。

ビデオ システムを出荷時の状態にリセットすると、以下のことが行われます。

- 通話履歴が削除されます。
- パスワードがデフォルト値にリセットされます。
- すべてのシステム パラメータがデフォルト値にリセットされます。
- システムにアップロードされていたファイルは、すべて削除されます。これには、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、また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。**

システムはリセット後に自動的に再起動されます。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。

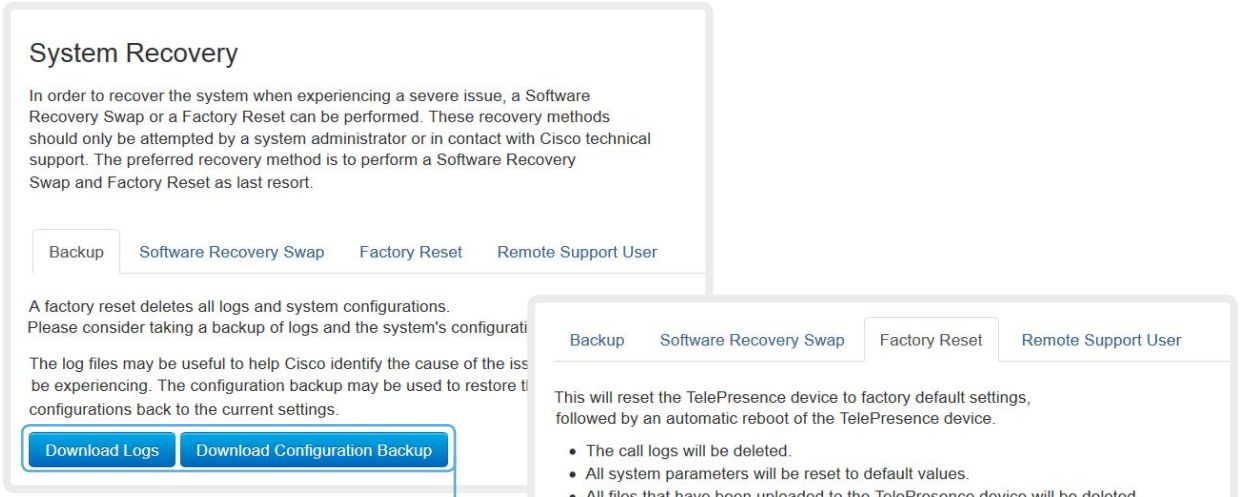
出荷時の状態にリセットする前にシステムのログ ファイルおよび設定をバックアップすることをお勧めします。

工場出荷時設定にリセットすると、元に戻すことはできません。

工場出荷時設定へのリセットに関する詳細情報は、付録の「工場出荷時設定へのリセット」に記述してあります。

* ソフトウェアの交換については、「以前に使用していたソフトウェア バージョンへの復元」の項を参照してください。

移動先:[メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)]:[バックアップ (Backup)] タブおよび [工場出荷時状態へのリセット (Factory Reset)] タブ



1. ログ ファイルとシステム設定のバックアップ

出荷時の状態にリセットする前にシステムのログ ファイルおよび設定をバックアップすることをお勧めします。そうしないと、データが失われます。

[ログのダウンロード (Download Logs)] と [設定のバックアップをダウンロード (Download Configuration Backup)] をクリックし、手順に従ってファイルをコンピュータに保存します。

2.工場出荷時の状態へのリセット

表示された情報をよく確認してから、[初期設定へのリセット (Perform a factory reset...)] をクリックします。

[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止めます。

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。

リモート サポート ユーザ

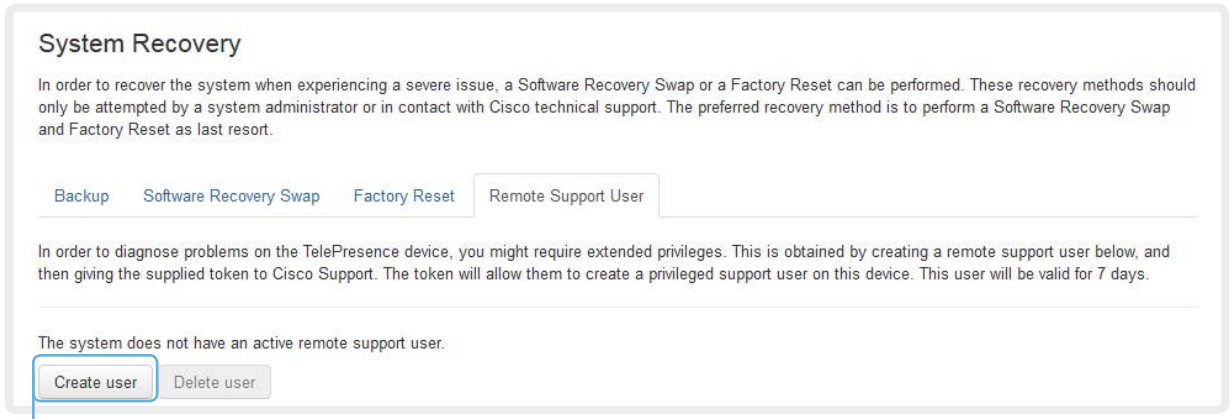
ビデオ システムに診断の問題がある場合は、リモート サポート ユーザを作成できます。

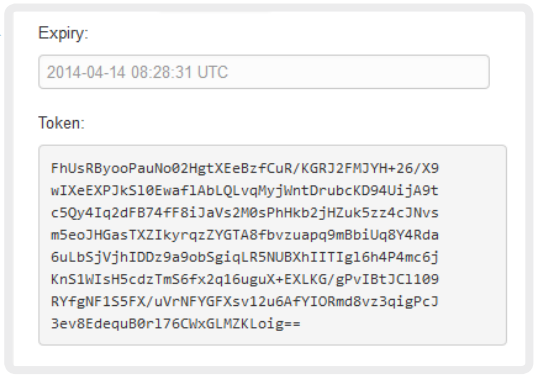
リモート サポート ユーザにはシステムへの読み取りアクセス権が付与され、トラブルシューティングに役立つ限定された一連のコマンドにアクセスできます。

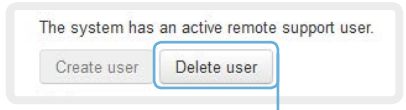
リモート サポート ユーザのパスワードを取得するには、Cisco Technical Assistance Center（TAC）アシスタントが必要です。

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

移動先：[メンテナンス（Maintenance）] > [システム リカバリ（System Recovery）]：[リモート サポートユーザ（Remote Support User）]タブ







リモート サポート ユーザの作成

1. Cisco TAC でケースをオープンします。
2. [ユーザの作成（Create User）] をクリックします。
3. [トークン（Token）] フィールドのテキストをコピーし、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。

システムの再起動

システムは、Web インターフェイスを使用して、リモートでシャットダウンまたは再起動が可能です。

移動先:[メンテナンス(Maintenance)] > [再起動(Restart)]

システムの再起動

システムを再起動するには、[TelePresence デバイスの再起動...(Restart TelePresence device...)] をクリックします。

システムが使用可能になるまでに、数分かかります。

システムのシャットダウン

[TelePresence デバイスのシャットダウン...(Shutdown TelePresence device...)] をクリックしてシステムをシャットダウンします。

システムはリモートで再びオンにすることはできません。電源ボタンを物理的に押して、電源をオンにします。

第 3 章

システム設定

システム設定の概要

続くページに、Web インターフェイスの [システム設定 (System Configuration)] ページで設定されるシステム設定の完全なリストを示します。例では、デフォルト値または値の例のいずれかを示します。

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 (IPv4 または IPv6) を確認するには、タッチ ユーザ インターフェイスの [設定 (Settings)]* メニューを開き、[システム情報 (System Information)] をタップします。

* [設定 (Settings)] メニューは、タッチ ユーザ インターフェイスの左上隅の連絡先情報をタップすると表示されるドロップ ダウン ウィンドウからアクセスできます。

音声設定

Audio Input Microphone [1]

音声入力マイク モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（Off）]：マイクのコネクタをディセーブルにします。

[オン（On）]：マイクのコネクタをイネーブルにします。

例：`Audio Input Microphone 1 Mode: On`

Audio Microphones Mute Enabled

音声ミュートが許可されるかどうかを決定します。デフォルト値は true です。

必要なユーザ ロール：ADMIN

値スペース：<True/InCallOnly>

[真（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 に設定すると、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。

例：`Audio Microphones Mute Enabled: True`

Audio SoundsAndAlerts KeyTones Mode

システムはタッチ コントローラでテキストまたは数値を入力しているときに、キーボード クリック音（キー トーン）が再生されるように設定できます。

必要なユーザ ロール：USER

値スペース：<Off/On>

[オフ（Off）]：入力時にキー トーンは再生されません。

[オン（On）]：入力時にキー トーンが再生されます。

例：`Audio SoundsAndAlerts KeyTones Mode: Off`

Audio SoundsAndAlerts RingTone

この設定は着信コールに使用する呼び出し音を定義します。呼び出し音の正確な名前を入力する必要があります。次の方法で使用可能な呼び出し音を検索できます。

Web インターフェイス：[設定（Configuration）] > [パーソナライゼーション（Personalization）] ページ

タッチ コントローラ：[設定（Settings）] メニューの呼び出し音およびサウンド パネル。このパネルは、[設定（Settings）] メニューの開いている部分、またはパスワード保護された管理メニューに含まれています。UserInterface UserPreference 設定は、パスワード保護された領域に入れるパネルを定義します。

必要なユーザ ロール：USER

値スペース：<S: 1, 100>

フォーマット：最大 100 文字の文字列。

例：`Audio SoundsAndAlerts RingTone: "Sunrise"`

Audio SoundsAndAlerts RingVolume

着信コールの呼び出し音の音量を設定します。

必要なユーザ ロール：USER

値スペース：<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。

例：`Audio SoundsAndAlerts RingVolume: 40`

Audio DefaultVolume

デフォルトのスピーカーの音量を設定します。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、音量はこの値を返します。ビデオ システムの稼働中に音量を変更するには、タッチ コントローラを使用します。

必要なユーザ ロール：USER

値スペース：<0..100>

範囲：値は 0 ～ 100 である必要があります。1 ～ 100 の値は -34.5 dB ～ 15 dB（0.5 dB 刻み）の範囲に対応します。値 0 は、音声がオフになっていることを意味します。

例：`Audio DefaultVolume: 50`

カメラ 設定

Cameras PowerLine Frequency

ビデオ システムのカメラは、電源からのすべてのフリッカ ノイズを補うことができます（電源周波数フリッカ防止）。カメラは電源周波数の自動検出もサポートしています。Auto オプション（デフォルト）を選択するか、お使いの電源周波数に基づいてこのカメラ設定を設定してください。

必要なユーザ ロール：ADMIN

値スペース：<Auto/50Hz/60Hz>

[自動（Auto）]：カメラが電源周波数を自動検出できるようにします。

[50Hz]：電線周波数が 50 Hz の場合、この値を使用します。

[60Hz]：電線周波数が 60 Hz の場合、この値を使用します。

例：`Cameras PowerLine Frequency: Auto`

Cameras Camera [1] Backlight

この設定は、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

値スペース：<Off/On>

[オフ（Off）]：カメラの逆光補正をオフにします。

[オン（On）]：カメラの逆光補正をオンにします。

例：`Cameras Camera 1 Backlight: Off`

Cameras Camera [1] Brightness Mode

カメラの明るさモードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

[自動（Auto）]：カメラの明るさはシステムによって自動的に設定されます。

[手動（Manual）]：カメラの明るさの手動設定をイネーブルにします。明るさのレベルは Cameras Camera Brightness Level 設定を使用して設定されます。

例：`Cameras Camera 1 Brightness Mode: Auto`

Cameras Camera [1] Brightness Level

明るさレベルを設定します。カメラの明るさモードを [手動（Manual）] に設定する必要があります。

必要なユーザ ロール：ADMIN

値スペース：<1..31>

範囲：1 ～ 31 の値を選択します。

例：`Cameras Camera 1 Brightness Level: 20`

Cameras Camera [1] Focus Mode

カメラの焦点モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

[自動（Auto）]：コールが接続されると、カメラはオートフォーカスになります。カメラの移動（パン、チルト、ズーム）後も同様です。システムは、オートフォーカスを数秒間だけ使用して正しい焦点に設定します。その後、オートフォーカスはカメラが焦点調整し続けることを防ぐためオフになります。

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

例：`Cameras Camera 1 Focus Mode: Auto`

Cameras Camera [1] Gamma Mode

この設定は、ガンマ補正をイネーブルにします。ガンマは、画像ピクセルとモニタの明るさとの間の非線形関係を表します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

[自動（Auto）]：自動がデフォルトであり、推奨設定です。

[手動（Manual）]：手動モードではガンマ値はガンマ レベル設定、リファレンスと変更されます。参照：Cameras Camera [1..n] Gamma Level

例：`Cameras Camera 1 Gamma Mode: Auto`

Cameras Camera [1] Gamma Level

ガンマ レベルを設定して、使用するガンマ補正テーブルを選択できます。この設定は、明るさの設定を変更しても十分な結果が得られない困難な光条件に役立つことがあります。[ガンマ モード(Gamma Mode)] を [手動(Manual)] に設定する必要があります。

必要なユーザ ロール: ADMIN

値スペース: <0..7>

範囲: 0 ～ 7 の値を選択します。

例: `Cameras Camera 1 Gamma Level: 0`

Cameras Camera [1] Mirror

ミラー モード(水平反転)を使用して画面の画像を反転できます。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(Off)]: セルフビューを通常モードで表示します。つまり、セルフビューは他の人から自分を見るような感覚になります。

[オン(On)]: セルフビューをミラー モードで表示します。つまり、セルフビューは反転され、セルフビューは鏡の中の自分を見るような感覚になります。

例: `Cameras Camera 1 Mirror: Auto`

Cameras Camera [1] Whitebalance Mode

カメラのホワイトバランス モードを設定します。

必要なユーザ ロール: ADMIN

値スペース: <Auto/Manual>

[自動(Auto)]: カメラはカメラのビューに合わせて常にホワイト バランスを調整します。

[手動(Manual)]: カメラのホワイトバランスの手動設定をイネーブルにします。ホワイトバランスのレベルは Cameras Camera Whitebalance Level 設定を使用して設定します。

例: `Cameras Camera 1 Whitebalance Mode: Auto`

Cameras Camera [1] Whitebalance Level

ホワイトバランス レベルを設定します。カメラの [ホワイトバランス モード(Camera Whitebalance Mode)] を [手動(Manual)] に設定する必要があります。

必要なユーザ ロール: ADMIN

値スペース: <1..16>

範囲: 1 ～ 16 の値を選択します。

例: `Cameras Camera 1 Whitebalance Level: 1`

会議 設定

Conference [1..1] 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 での会議を管理できるようにする機能です（TRC5 リモート コントロールおよび画面上の表示からは利用できません）。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）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

値スペース：<Auto/Off>

[自動（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イネーブルになります。

[オフ（Off）]：アクティブ コントロールはディセーブルです。

例：`Conference ActiveControl Mode: Auto`

Conference [1..1] 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

値スペース：<Dual/IPv4/IPv6>

[デュアル（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。

例：`Conference 1 CallProtocolIPStack: Dual`

Conference [1..1] AutoAnswer Mode

自動応答モードを設定します。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

値スペース：<Off/On>

[オフ（Off）]：着信コールに応答するには、タッチ コントローラで [応答（Answer）] をタップする必要があります。

[オン（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。通話中の着信コールに対しては、常に手動で応答または拒否する必要があります。

例：`Conference 1 AutoAnswer Mode: Off`

Conference [1..1] AutoAnswer Mute

着信コールが自動的に応答する場合にマイクをミュートするかどうか決定します。[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

値スペース：<Off/On>

[オフ（Off）]：着信コールはミュートにされません。

[オン（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。

例：`Conference 1 AutoAnswer Mute: Off`

Conference [1..1] 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

値スペース：<0..50>

範囲：0 ～ 50 秒の値を選択します。

例：`Conference 1 AutoAnswer Delay: 0`

Conference [1..1] MicUnmuteOnDisconnect Mode

すべてのコールが切断されたとき、マイクが自動的にミュート解除されるかどうかを決定します。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

値スペース：<Off/On>

[オフ（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。

[オン（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。

例：`Conference 1 MicUnmuteOnDisconnect Mode: On`

Conference [1..1] 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（タッチ コントローラ）を使用して早期に終了できます。デフォルト値は 60 分です。

必要なユーザ ロール：ADMIN

値スペース：<0..1440>

*範囲：*サイレント セッションが自動的にタイム アウトするまでの分数を 0 ～ 1440（24 時間）の間で選択します。

例：`Conference 1 DoNotDisturb DefaultTimeOut: 60`

Conference [1..1] 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、チルト、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

値スペース：<Off/On>

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

[オン（On）]：相手先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、チルト、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、こちら側では通常どおり可能です。

例：`Conference 1 FarEndControl Mode: On`

Conference [1..1] FarEndControl SignalCapability

遠端制御（H.224）信号機能モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（Off）]：遠端制御信号機能をディセーブルにします。

[オン（On）]：遠端制御信号機能をイネーブルにします。

例：`Conference 1 FarEndControl SignalCapability: On`

Conference [1..1] Encryption Mode

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

注：暗号化オプション キーをインストールする必要があります。暗号化オプション キーがインストールされていない場合は、暗号化モードは [オフ（Off）] に設定されます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On/BestEffort>

[オフ（Off）]：システムは、暗号化を使用しません。

[オン（On）]：システムは、暗号化されたコールだけを許可します。

[ベストエフォート（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。

例：`Conference 1 Encryption Mode: BestEffort`

Conference [1..1] 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コール プロトコルを設定します。

必要なユーザ ロール: ADMIN

値スペース: <Auto/H323/Sip/H320>

[自動(Auto)]:使用可能なプロトコルに基づいた通信プロトコルの自動選択をイネーブルにします。複数のプロトコルが使用可能な場合、優先順位は次のとおりです:1)SIP、2)H323、3)H320。システムで登録できない場合や、通信プロトコルがイネーブルになっていない場合、自動選択で H323 が選択されます。

[H.323]:[H.323] を選択するとコールは H.323 コールとして設定されます。

[Sip]:[Sip] を選択するとコールは SIP コールとして設定されます。

[H320]:[H320] を選択するとコールは H.320 コールとして設定されます(Cisco TelePresence ISDN リンク ゲートウェイに接続されている場合のみ)。

例: `Conference 1 DefaultCall Protocol: H323`

Conference [1..1] DefaultCall Rate

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コール レートを設定します。

必要なユーザ ロール: ADMIN

値スペース: <64..6000>

*範囲:*64 ～ 6000 kbps の値を選択します。

例: `Conference 1 DefaultCall Rate: 1920`

Conference [1..1] MaxTransmitCallRate

コールを発信または受信するときに使用される最大送信ビット レートを指定します。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

値スペース: <64..6000>

*範囲:*64 ～ 6000 kbps の値を選択します。

例: `Conference 1 MaxTransmitCallRate: 6000`

Conference [1..1] MaxReceiveCallRate

コールを発信または受信するときに使用される最大受信ビット レートを指定します。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

値スペース: <64..6000>

*範囲:*64 ～ 6000 kbps の値を選択します。

例: `Conference 1 MaxReceiveCallRate: 6000`

Conference [1..1] MaxTotalTransmitCallRate

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

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

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

必要なユーザ ロール: ADMIN

値スペース: <64..10000>

*範囲:*64 ～ 10000 の値を選択します。

例: `Conference 1 MaxTotalTransmitCallRate: 10000`

Conference [1..1] MaxTotalReceiveCallRate

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

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

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

必要なユーザ ロール： ADMIN

値スペース： <64..10000>

*範囲：*64 ～ 10000 の値を選択します。

例： `Conference 1 MaxTotalReceiveCallRate: 10000`

Conference [1..1] VideoBandwidth Mode

会議のビデオ帯域幅モードを設定します。

必要なユーザ ロール： ADMIN

値スペース： <Dynamic/Static>

[動的（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。

[静的（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。

例： `Conference 1 VideoBandwidth Mode: Dynamic`

Conference [1..1] VideoBandwidth MainChannel Weight

使用可能な送信ビデオ帯域幅が「MainChannel Weight」および「PresentationChannel Weight」に従ってメイン チャネルおよびプレゼンテーション チャネルに分配されます。メイン チャネルの重みが 2 で、プレゼンテーション チャネルの重みが 1 の場合、メイン チャネルはプレゼンテーション チャネルの 2 倍の帯域幅を使用します。

必要なユーザ ロール： ADMIN

値スペース： <1..10>

*範囲：*1 ～ 10。

例： `Conference 1 VideoBandwidth MainChannel Weight: 5`

Conference [1..1] VideoBandwidth PresentationChannel Weight

使用可能な送信ビデオ帯域幅が「MainChannel Weight」および「PresentationChannel Weight」に従ってメイン チャネルおよびプレゼンテーション チャネルに分配されます。メイン チャネルの重みが 2 で、プレゼンテーション チャネルの重みが 1 の場合、メイン チャネルはプレゼンテーション チャネルの 2 倍の帯域幅を使用します。

必要なユーザ ロール： ADMIN

値スペース： <1..10>

*範囲：*1 ～ 10。

例： `Conference 1 VideoBandwidth PresentationChannel Weight: 5`

Conference [1..1] Presentation RelayQuality

この設定は、内蔵 MultiSite 機能（オプション）を使用してマルチポイント ビデオ会議をホストするときに適用されます。リモート ユーザがプレゼンテーションを共有している場合、ビデオ システム（コーデック）は、プレゼンテーションのトランスコーディングを行い、それをマルチポイント会議の他の参加者に送信します。[リレー品質（RelayQuality）] 設定は、プレゼンテーション ソースに対して、高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール： ADMIN

値スペース： <Motion/Sharpness>

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

[シャープさ（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。

例： `Conference 1 Presentation RelayQuality: Sharpness`

Conference [1..1] 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

値スペース： <Stop/NoAction>

[停止（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。

[アクションなし（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。

例： `Conference 1 Presentation OnPlacedOnHold: NoAction`

Conference [1..1] Multipoint Mode

ビデオ システムがマルチパーティ ビデオ会議を処理する方法を定義します。

Cisco TelePresence Video Communication Server（VCS）に登録すると、ビデオ システムは独自の組み込み MultiSite 機能または MultiWay ネットワーク ソリューションを使用できます。MultiWay では、マルチポイント コントロール ユニット（MCU）がビデオ ネットワークに含まれていることが必要です。

Cisco Unified Communications Manager（CUCM）バージョン 8.6.2 以降に登録すると、ビデオ システムは、CUCM 会議ブリッジ、または内蔵 MultiSite 機能を使用できます。どれを使用するかは CUCM によって設定されます。

Multiway および CUCM 会議ブリッジの両方を使用すれば、多くの参加者との会議を設定できます。組み込み MultiSite では、最大 4 人の参加者（自分自身を含む）が許可されます。

必要なユーザ ロール： ADMIN

値スペース： <Auto/Off/MultiSite/MultiWay/CUCMMediaResourceGroupList>

[自動（Auto）]：利用可能なマルチポイント メソッドが自動的に選択されます。利用可能なマルチポイントがない場合、[マルチポイント モード（Multipoint Mode）] は自動的に [オフ（Off）] に設定されます。MultiWay および MultiSite の両方が利用可能な場合、MultiWay サービスは組み込み MultiSite よりも優先されます。

[オフ（Off）]：マルチパーティ会議は許可されません。

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

[MultiWay]：マルチパーティ会議は MultiWay サービスを使用して設定されます。MultiWay サービスを使用できない場合に [MultiWay] が選択された場合、[マルチポイント モード（Multipoint Mode）] は自動的に [オフ（Off）] に設定されます。これは、NetworkServices MultiWay Address 設定が空か、正しく設定されていない場合に発生する可能性があります。

[CUCMMediaResourceGroupList]：マルチパーティ会議（アドホック会議）は、CUCM で設定された会議ブリッジによってホストされます。この設定は、CUCM 環境で CUCM によりプロビジョニングされるものであり、ユーザが手動で設定すべきではありません。

例： `Conference 1 Multipoint Mode: Auto`

Conference [1..1] IncomingMultisiteCall Mode

すでにコール中または会議中の場合に着信コールを許可するかどうかを選択します。

必要なユーザ ロール： ADMIN

値スペース： <Allow/Deny>

[許可（Allow）]：すでに通話している間に、誰かが電話をかけてきた場合、通知されます。着信コールを受け入れるかどうかは任意です。進行中のコールは、着信コールに応答するときに保留になる場合があります。またはコールをマージすることができます（MultiSite または MultiWay のサポートが必要です）。

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

例： `Conference 1 IncomingMultisiteCall Mode: Allow`

ファシリティ サービス設定

FacilityService Service [1..5] Type

タッチ コントローラを使用するには [ヘルプ デスク(Helpdesk)] に設定します。API(アプリケーション プログラミング インターフェイス)コマンド セットを使用するシステム インテグレータの場合はその他のオプションを利用できます。

必要なユーザ ロール: ADMIN

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

[ヘルプ デスク(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。

例: `FacilityService Service 1 Type:Helpdesk`

FacilityService Service [1..5] Name

ファシリティ サービス名を入力します。この名前は、ファシリティ サービス コール ボタンに表示されます。タッチ コントローラでは、FacilityService Service 1 だけを使用できます。ファシリティ サービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。コール ボタンを表示するには、タッチ コントローラの右上隅のシステム名の右側にある疑問符がついている小さいボタンをタップします。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 255>

*フォーマット:*最大 255 文字の文字列。

例: `FacilityService Service 1 Name:""`

FacilityService Service [1..5] Number

ファシリティ サービス番号(URI または電話番号)を入力します。タッチ コントローラでは、FacilityService Service 1 だけを使用できます。ファシリティ サービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。コール ボタンを表示するには、タッチ コントローラの右上隅のシステム名の右側にある疑問符がついている小さいボタンをタップします。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 255>

*フォーマット:*最大 255 文字の文字列。

例: `FacilityService Service 1 Number:""`

FacilityService Service [1..5] CallType

ファシリティ サービスにコール タイプを設定します。

必要なユーザ ロール: ADMIN

値スペース: <Video/Audio>

[ビデオ(Video)]:ビデオ コールには、このオプションを選択します。

[音声(Audio)]:オーディオ コールには、このオプションを選択します。

例: `FacilityService Service 1 CallType:Video`

H323 設定

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

値スペース： <Auto/Off/On>

[自動（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。

[オフ（Off）]：システムは、実際の IP アドレスをシグナリングします。

[オン（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 メニューで「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。

例： `H323 NAT Mode: Off`

H323 NAT Address

NAT サポートのルータに外部/グローバル IP アドレスを入力します。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

*ポート 2326-2487

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 64>

*フォーマット：*有効な IPv4 アドレスまたは IPv6 アドレス。

例： `H323 NAT Address: ""`

H323 Profile [1..1] Authentication Mode

H.323 プロファイルの認証モードを設定します。

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（Off）]：H.323 Gatekeeper Authentication Mode が Off に設定されている場合、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。

[オン（On）]：H.323 Gatekeeper Authentication Mode が On に設定され、認証が必要なことを .323 ゲートキーパーがに示している場合、システムはゲートキーパーに対して自身の認証を試行します。コーデックとゲートキーパーの両方で認証ログイン名と認証パスワードが定義される必要があります。

例： `H323 Profile 1 Authentication Mode: Off`

H323 Profile [1..1] Authentication LoginName

システムは、H.323 ゲートキーパーに認証ログイン名と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 ゲートキーパー認証モード（H.323 Gatekeeper Authentication Mode）] がイネーブルになっている必要があります。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 50>

*フォーマット：*最大 50 文字の文字列。

例： `H323 Profile 1 Authentication LoginName: ""`

H323 Profile [1..1] Authentication Password

システムは、H.323 ゲートキーパーに認証ログイン名と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 ゲートキーパー認証モード (H.323 Gatekeeper Authentication Mode)] がイネーブルになっている必要があります。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 50>

フォーマット:最大 50 文字の文字列。

例: `H323 Profile 1 Authentication Password: ""`

H323 Profile [1..1] CallSetup Mode

H.323 コール セットアップ モードは、H323 コールを確立するときにゲートキーパーまたはダイレクトコールを使用するかどうかを定義します。

注:ダイレクト H.323 コールは、H.323 コール コンフィギュレーション モードがゲートキーパーに設定されていても行うことができます。

必要なユーザ ロール: ADMIN

値スペース: <Direct/Gatekeeper>

[直接 (Direct)]:H323 コール発信のためダイヤリングするときに IP アドレスを使用する必要があります。

[ゲートキーパー (Gatekeeper)]:システムはゲートキーパーを使用して、H.323 コールを発信します。このオプションを選択する場合は H323 Profile Gatekeeper Address および H323 Profile Gatekeeper Discovery 設定も行う必要があります。

例: `H323 Profile 1 CallSetup Mode: Gatekeeper`

H323 Profile [1..1] Encryption MinKeySize

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キー サイズを定義します。

必要なユーザ ロール: ADMIN

値スペース: <1024bit/2048bit>

[1024bit]:最小サイズは 1024 ビットです。

[2048bit]:最小サイズは 2048 ビットです。

例: `H323 Profile 1 Encryption MinKeySize: 1024bit`

H323 Profile [1..1] Gatekeeper Discovery

システムが H.323 ゲートキーパーに登録する方法を決定します。

必要なユーザ ロール: ADMIN

値スペース: <Manual/Auto>

[手動 (Manual)]:システムは、ゲートキーパーの IP アドレスで指定された特定のゲートキーパーを使用します。

[自動 (Auto)]:システムは自動的に使用可能なゲートキーパーに登録しようとします。あるゲートキーパーが 30 秒以内にコーデックから送信された要求に応答すると、この特定のゲートキーパーが使用されます。これには、ゲートキーパーが自動検出モードにあることも必要です。ゲートキーパーが応答しなかった場合は、H.323 コールにゲートキーパーを使用しないため、IP アドレスを手動で指定する必要があります。

例: `H323 Profile 1 Gatekeeper Discovery: Manual`

H323 Profile [1..1] Gatekeeper Address

ゲートキーパーの IP アドレスを入力します。[H.323 コール セットアップ モード (H.323 Call Setup Mode)] を [ゲートキーパー (Gatekeeper)] に設定し、[ゲートキーパーの検出 (Gatekeeper Discovery)] を [手動 (Manual)] に設定する必要があります。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 255>

フォーマット:有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例: `H323 Profile 1 Gatekeeper Address: "192.0.2.0"`

H323 Profile [1..1] 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

値スペース: <S: 0, 30>

フォーマット:最大 30 文字のコンパクト文字列。使用できる文字は、0 ～ 9、*、# です。

例: `H323 Profile 1 H323Alias E164: "90550092"`

H323 Profile [1..1] H323Alias ID

H.323 ゲートキーパー 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 を指定します。例:「firstname.lastname@company.com」、「My H.323 Alias ID」

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 49>

*フォーマット:*最大 49 文字の文字列。

例: `H323 Profile 1 H323Alias ID: "firstname.lastname@company.com"`

H323 Profile [1..1] PortAllocation

H.323 ポート割り当ての設定は、H.323 コール シグナリングに使用する H.245 ポート番号に影響します。

必要なユーザ ロール: ADMIN

値スペース: <Dynamic/Static>

[動的(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。[動的(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。RTP および RTCP メディア データの場合、システムは範囲 2326 ～ 2487 の UDP ポートを使用しています。各メディア チャネルは 2 つの隣接ポートを使用しています。つまり RTP と RTCP がそれぞれ 2330 と 2331 を使用しています。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。

[静的(Static)]:静的に設定すると、静的に事前定義された範囲 [5555-6555] 内でポート指定されます。

例: `H323 Profile 1 PortAllocation: Dynamic`

ログ 設定

ロギング モード

このバージョンでは適用されません。

ネットワーク設定

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

値スペース： <Dual/IPv4/IPv6>

[デュアル(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。

例： `Network 1 IPStack: Dual`

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。この設定は IPv4 ネットワーク上のシステムにのみ適用されます。

必要なユーザ ロール： ADMIN

値スペース： <Static/DHCP>

[静的(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。

例： `Network 1 IPv4 Assignment: DHCP`

Network [1..1] IPv4 Address

システムのスタティック IPv4 ネットワーク アドレスを入力します。この設定は、Network 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

値スペース： <S: 0, 64>

*フォーマット：*有効な IPv4 アドレス。

例： `Network 1 IPv4 Address: "192.0.2.2"`

Network [1..1] IPv4 Gateway

IPv4 ネットワーク ゲートウェイを定義します。この設定は、Network 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

値スペース： <S: 0, 64>

*フォーマット：*有効な IPv4 アドレス。

例： `Network 1 IPv4 Gateway: "192.0.2.1"`

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。この設定は、Network 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

値スペース： <S: 0, 64>

*フォーマット：*有効な IPv4 アドレス形式。

例： `Network 1 IPv4 SubnetMask: "255.255.255.0"`

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。この設定は IPv6 ネットワーク上のシステムにのみ適用されます。

必要なユーザ ロール： ADMIN

値スペース： <Static/DHCPv6/Autoconf>

[静的(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 RFC 3315 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 RFC 4862 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。

例： `Network 1 IPv6 Assignment: Autoconf`

Network [1..1] IPv6 Address

システムのスタティック IPv6 ネットワーク アドレスを入力します。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

値スペース: <S: 0, 64>

*フォーマット:*有効な IPv6 アドレス。

例: `Network 1 IPv6 Address: "2001:0DB8:0000:0000:0000:0000:0000:0002"`

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

値スペース: <S: 0, 64>

*フォーマット:*有効な IPv6 アドレス。

例: `Network 1 IPv6 Gateway: "2001:0DB8:0000:0000:0000:0000:0000:0001"`

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

値スペース: <Off/On>

[オフ(Off)]:DHCPv6 サーバからの DHCP オプションの取得をディセーブルにします。

[オン(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。

例: `Network 1 IPv6 DHCPOptions: On`

Network [1..1] DHCP RequestTFTPServerAddress

この設定は、Cisco Unified Communications Manager(CUCM)に登録されたビデオ システムにのみ使用されます。

この設定は、TFTP サーバ(プロビジョニング サーバ)のアドレスを自動的に検出できるように、エンドポイントが DHCP サーバに DHCP オプション 150 を要求するかを決定します。

この設定が Off になっている場合、または DHCP サーバがオプション 150 をサポートしていない場合は、Provisioning ExternalManager Address 設定を使用して TFTP サーバ アドレスを手動で設定する必要があります。

[ネットワーク VLAN 音声モード(Network VLAN Voice Mode)] 設定が [自動(Auto)] であり、Cisco Discovery Protocol(CDP)により ID が音声 VLAN に割り当てられている場合、オプション 150 のリクエストは必ず送信されます。つまり、Network DHCP RequestTFTPServerAddress の設定は無視されます。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(Off)]:ビデオ システムは DHCP オプション 150 のリクエストを送信しません。TFTP サーバのアドレスを手動で設定する必要があります。この規則の例外については、上記の注を参照してください。

[オン(On)]:ビデオ システムは自動的に TFTP サーバのアドレスを検出できるように、オプション 150 のリクエストを DHCP に送信します。

例: `Network 1 DHCP RequestTFTPServerAddress: On`

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

値スペース: <S: 0, 64>

*フォーマット:*最大 64 文字の文字列。

例: `Network 1 DNS Domain Name: ""`

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。最大で 3 つ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

値スペース: <S: 0, 64>

*フォーマット:*有効な IPv4 アドレスまたは IPv6 アドレス。

例: `Network 1 DNS Server 1 Address: ""`

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 優先順位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

値スペース： <Off/Diffserv>

[オフ（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。

例： `Network 1 QoS Mode: Diffserv`

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

値スペース： <0..63>

*範囲：*0～63 の値を選択します。数字が大きいほど、優先順位が高くなります。デフォルト値は 0（ベスト エフォート）です。

例： `Network 1 QoS Diffserv Audio: 0`

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

値スペース： <0..63>

*範囲：*0～63 の値を選択します。数字が大きいほど、優先順位が高くなります。デフォルト値は 0（ベスト エフォート）です。

例： `Network 1 QoS Diffserv Video: 0`

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

値スペース： <0..63>

*範囲：*0～63 の値を選択します。数字が大きいほど、優先順位が高くなります。デフォルト値は 0（ベスト エフォート）です。

例： `Network 1 QoS Diffserv Data: 0`

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

値スペース: <0..63>

*範囲:*0～63 の値を選択します。数字が大きいほど、優先順位が高くなります。デフォルト値は 0(ベスト エフォート)です。

例: `Network 1 QoS Diffserv Signalling: 0`

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

値スペース: <0..63>

*範囲:*0～63 の値を選択します。数字が大きいほど、優先順位が高くなります。デフォルト値は 0(ベスト エフォート)です。

例: `Network 1 QoS Diffserv ICMPv6: 0`

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

値スペース: <0..63>

*範囲:*0～63 の値を選択します。数字が大きいほど、優先順位が高くなります。デフォルト値は 0(ベスト エフォート)です。

例: `Network 1 QoS Diffserv NTP: 0`

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

値スペース: <Off/On>

[オフ(Off)]:802.1X 認証がディセーブルになります(デフォルト)。

[オン(On)]:802.1X 認証がイネーブルになります。

例: `Network 1 IEEE8021X Mode: Off`

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..1] IEEE8021X Eap Tls がイネーブル（On）の場合にだけ有効です。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（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。

[オン（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。

例：`Network 1 IEEE8021X TlsVerify: Off`

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

値スペース：<Off/On>

[オフ（Off）]：[オフ（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）。

[オン（On）]：[オン（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。

例：`Network 1 IEEE8021X UseClientCertificate: Off`

Network [1..1] IEEE8021X Identity

802.1X ID は 802.1X 認証に必要なユーザ名です。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

*フォーマット：*最大 64 文字の文字列。

例：`Network 1 IEEE8021X Identity: ""`

Network [1..1] IEEE8021X Password

802.1X パスワードは 802.1X 認証に必要なパスワードです。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 32>

*フォーマット：*最大 32 文字の文字列。

例：`Network 1 IEEE8021X Password: ""`

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

値スペース：<S: 0, 64>

*フォーマット：*最大 64 文字の文字列。

例：`Network 1 IEEE8021X AnonymousIdentity: ""`

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）モードを設定します。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

値スペース：<Off/On>

[オフ（Off）]：EAP-MD5 プロトコルはディセーブルになります。

[オン（On）]：EAP-MD5 プロトコルはイネーブルになります（デフォルト）。

例：`Network 1 IEEE8021X Eap Md5: On`

Network [1..1] IEEE8021X Eap Ttls

TTLS（トンネリングされたトランスポート層セキュリティ）モードを設定します。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

値スペース：<Off/On>

[オフ（Off）]：EAP-TTLS プロトコルはディセーブルになります。

[オン（On）]：EAP-TTLS プロトコルはイネーブルになります（デフォルト）。

例：`Network 1 IEEE8021X Eap Ttls: On`

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。RFC 5216 で規定された 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

値スペース：<Off/On>

[オフ（Off）]：EAP-TLS プロトコルはディセーブルになります。

[オン（On）]：EAP-TLS プロトコルはイネーブルになります（デフォルト）。

例：`Network 1 IEEE8021X Eap Tls: On`

Network [1..1] IEEE8021X Eap Peap

Peap（保護拡張認証プロトコル）モードを設定します。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

値スペース：<Off/On>

[オフ（Off）]：EAP-PEAP プロトコルはディセーブルになります。

[オン（On）]：EAP-PEAP プロトコルはイネーブルになります（デフォルト）。

例：`Network 1 IEEE8021X Eap Peap: On`

Network [1..1] MTU

イーサネット MTU（最大伝送単位）を設定します。

必要なユーザ ロール：ADMIN

値スペース：<576..1500>

範囲：576 ～ 1500 バイトの値を選択します。

例：`Network 1 MTU: 1500`

Network [1..1] Speed

イーサネット リンクの速度を設定します。

必要なユーザ ロール：ADMIN

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

[自動（Auto）]：リンク速度を自動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。

例：`Network 1 Speed: Auto`

Network [1..1] TrafficControl Mode

ネットワーク トラフィック制御モードを設定してビデオ パケットの送信レートの制御方法を決定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（Off）]：ビデオ パケットをリンク速度で送信します。

[オン（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。

例：`Network 1 TrafficControl: On`

Network [1..1] RemoteAccess Allow

ssh/telnet/HTTP/HTTPS へのアクセスのため IP アドレスをフィルタします。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 255>

*フォーマット:*最大 255 文字の文字列、カンマ区切りの IP アドレスまたは IP 範囲。

例: `Network 1 RemoteAccess Allow: "192.168.1.231, 192.168.1.182"`

Network [1..1] VLAN Voice Mode

VLAN 音声モードを設定します。Cisco UCM(Cisco Unified Communications Manager)をプロビジョニング インフラストラクチャとして使用している場合、[VLAN 音声モード(VLAN Voice Mode)] が [自動(Auto)] に自動的に設定されます。

必要なユーザ ロール: ADMIN

値スペース: <Auto/Manual/Off>

[自動(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。

[手動(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置き換えられます。

[オフ(Off)]:VLAN はイネーブルになりません。

例: `Network 1 VLAN Voice Mode: Auto`

Network [1..1] VLAN Voice VlanId

VLAN 音声 ID を設定します。この設定は、VLAN Voice Mode 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

値スペース: <1..4094>

*範囲:*1 ～ 4094 の値を選択します。

例: `Network 1 VLAN Voice VlanId: 1`

ネットワーク サービス設定

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決定します。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(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。

[オン(On)]:H.323 コールの発信と受信の可能性をイネーブルにします(デフォルト)。

例: `NetworkServices H323 Mode: On`

NetworkServices HTTP Mode

Web ブラウザを使用したシステムへのアクセスを有効または無効にする HTTP モードを設定します。Web インターフェイスは、システム管理、コール転送などのコール管理、診断、およびソフトウェア アップロードに使用されます。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(Off)]:HTTP プロトコルはディセーブルになります。

[オン(On)]:HTTP プロトコルはイネーブルになります。

例: `NetworkServices HTTP Mode: On`

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決定します。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(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。

[オン(On)]:SIP コールの発信と受信の可能性をイネーブルにします(デフォルト)。

例: `NetworkServices SIP Mode: On`

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

値スペース: <Off/On>

[オフ(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。

[オン(On)]:Telnet プロトコルはイネーブルになります。

例: `NetworkServices Telnet Mode: Off`

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

値スペース: <Off/On>

[オフ(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)

[オン(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)

例: `NetworkServices WelcomeText: On`

NetworkServices XMLAPI Mode

このバージョンでは適用されません。

NetworkServices MultiWay Address

MultiWay アドレスは Video Communication Server に設定された Conference Factory Alias と等しい必要があります。Multiway 会議では、ビデオ エンドポイントのユーザは既存のコールにサード パーティを追加できます。

Multiway は次の場合に使用できます。

1) 既存のコールに他のユーザを追加する必要がある場合。

2) 通話中に第三者からのコールがあり、既存のコールにその人を含める必要がある場合。

要件：MX300 G2 はソフトウェア バージョン TC7.0 以降、Video Communication Server (VCS) バージョン X5 以降および Codian MCU バージョン 3.1 以降を実行する必要があります。Multiway 会議に参加するよう招待されるビデオ システムは、H.323 コールの場合 H.323 routeToMC ファシリティ メッセージ、SIP コールの場合 SIP REFER メッセージをサポートする必要があります。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 255>

フォーマット：最大 255 文字の文字列 (有効なダイヤル URI)。

例： `NetworkServices MultiWay Address: "h323:multiway@company.com"`

NetworkServices MultiWay Protocol

MultiWay コールに使用するプロトコルを決定します。

必要なユーザ ロール： ADMIN

値スペース： <Auto/H323/Sip>

[自動 (Auto)]：システムが MultiWay コールのプロトコルを選択します。

[H323]：H323 プロトコルが MultiWay コールに使用されます。

[Sip]：SIP プロトコルが MultiWay コールに使用されます。

例： `NetworkServices MultiWay Protocol: Auto`

NetworkServices HTTPS Mode

HTTPS は、ユーザのページ要求と Web サーバから返されるページの暗号化と復号化を実行する Web プロトコルです。

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ (Off)]：HTTPS プロトコルはディセーブルになります。

[オン (On)]：HTTPS プロトコルはイネーブルになります (デフォルト)。

例： `NetworkServices HTTPS Mode: On`

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

値スペース： <Off/On>

[オフ (Off)]：サーバ証明書を確認しません。

[オン (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。

例： `NetworkServices HTTPS VerifyServerCertificate: Off`

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

値スペース： <Off/On>

[オフ (Off)]：クライアント証明書を確認しません。

[オン (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。

例： `NetworkServices HTTPS VerifyClientCertificate: Off`

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 をイネーブルにして、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

値スペース： <Off/On>

[オフ (Off)]：OCSP サポートをディセーブルにします。

[オン (On)]：OCSP サポートをイネーブルにします。

例： `NetworkServices HTTPS OCSP Mode: Off`

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 を指定します。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 255>

フォーマット：最大 255 文字の文字列。

例： `NetworkServices HTTPS OCSP URL: "http://ocspserver.company.com:81"`

NetworkServices Medianet Metadata

Cisco Medianet 展開に関連するメタデータでメディア フローのタグ付け機能をオン/オフに切り替えます。

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（Off）]：メディア フローはそのメタデータではタグ付けされません。

[オン（On）]：メディア フローはそのメタデータでタグ付けされます。

例： `NetworkServices Medianet Metadata: Off`

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を同期するために使用されます。その後、時間の更新のためにこのタイム サーバが 24 時間ごとに照会されます。時間は画面上部に表示されます。システムは、H.235 認証を必要とするゲートキーパーまたはボーダー コントローラに送信されるメッセージのタイムスタンプに、この時間を使用します。システムは、H.235 認証を必要とするゲートキーパーまたはボーダー コントローラに送信されるメッセージのタイムスタンプに、この時間を使用します。また、発信履歴、不在着信、および受信コールのタイムスタンプにも使用されます。

必要なユーザ ロール： ADMIN

値スペース： <Auto/Off/Manual>

[自動（Auto）]：システムは、ネットワーク上の DHCP サーバから指定されたアドレスによって NTP サーバを使用します。DHCP サーバが使用されない場合、または DHCP サーバが NTP サーバ アドレスをシステムに提供しない場合、システムはユーザが指定した、スタティックに定義された NTP サーバ アドレスを使用します。

[オフ（Off）]：システムは NTP サーバを使用しません。

[手動（Manual）]：システムは、ユーザが指定によって静的に定義された NTP サーバ アドレスを常に使用します。

例： `NetworkServices NTP Mode: Auto`

NetworkServices NTP Address

ネットワーク タイム プロトコル サーバのアドレスを定義するために、NTP のアドレスを入力します。このアドレスは、NTP Mode が Manual に設定された場合、または 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ます。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 64>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例： `NetworkServices NTP Address: "0.tandberg.pool.ntp.org"`

NetworkServices SNMP Mode

ネットワーク管理システムでは、管理上の対応を保証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）を監視するために SNMP（Simple Network Management Protocol）が使用されます。SNMP は、システム設定を説明する管理システム上の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

値スペース： <Off/ReadOnly/ReadWrite>

[オフ（Off）]：SNMP ネットワーク サービスをディセーブルにします。

[読み取り専用（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。

[読み書き（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。

例： `NetworkServices SNMP Mode: ReadOnly`

NetworkServices SNMP Host [1..3] Address

最大 3 個の SNMP マネージャのアドレスを入力します。

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）からの要求に応答します。SNMP トラップはサポートされません。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 64>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例： `NetworkServices SNMP Host 1 Address: ""`

NetworkServices SNMP CommunityName

ネットワーク サービス SNMP コミュニティ名を入力します。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

値スペース: <S: 0, 50>

フォーマット:最大 50 文字の文字列。

例: `NetworkServices SNMP CommunityName: "public"`

NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システム接点の名前を入力します。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 50>

フォーマット:最大 50 文字の文字列。

例: `NetworkServices SNMP SystemContact: ""`

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入力します。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 50>

フォーマット:最大 50 文字の文字列。

例: `NetworkServices SNMP SystemLocation: ""`

NetworkServices SSH Mode

SSH(セキュア シェル)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

値スペース: <Off/On>

[オフ(Off)]:SSH プロトコルはディセーブルになります。

[オン(On)]:SSH プロトコルはイネーブルになります(デフォルト)。

例: `NetworkServices SSH Mode: On`

NetworkServices SSH AllowPublicKey

セキュア シェル(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

値スペース: <Off/On>

[オフ(Off)]:SSH 公開キーは許可されません。

[オン(On)]:SSH 公開キーが許可されます。

例: `NetworkServices SSH AllowPublicKey: On`

NetworkServices CTMS Mode

この設定は Cisco TelePresence Multipoint Switch(CTMS)によって制御されるマルチパーティ会議を許可するかどうかを決定します。

ビデオ システムは CTMS バージョン 1.8 以降で制御される暗号化されていないマルチパーティ会議を開始または参加できます。暗号化された会議は、ソフトウェア バージョン CTMS 1.9.1 以降でサポートされます。暗号化は NetworkServices CTMS Encryption 設定により指定されます。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(Off)]:CTMS によるマルチパーティ会議は禁止されます。

[オン(On)]:CTMS によるマルチパーティ会議は許可されます。

例: `NetworkServices CTMS Mode: On`

NetworkServices CTMS Encryption

この設定は Cisco TelePresence Multipoint Switch（CTMS）によって制御されるマルチパーティ会議に参加する場合に、ビデオ システムが暗号化をサポートするかどうかを示します。

CTMS は会議に次の 3 種類のセキュリティ設定を割り当てます。非セキュア（暗号化しない）、ベスト エフォート（すべての参加者が暗号化をサポートしている場合は暗号化し、それ以外の場合は暗号化しない）、セキュア（常に暗号化）。

必要なユーザ ロール： ADMIN

値スペース： <Off/BestEffort>

[オフ（Off）]：ビデオ システムは暗号化を許可しないため、セキュアな CTMS 会議（暗号化）に参加できません。ベスト エフォートの CTMS 会議に参加する場合、その会議は非セキュアにダウングレードされます（暗号化しない）。

[ベストエフォート（BestEffort）]：ビデオ システムは、CTMS と暗号化パラメータをネゴシエートし、セキュアな CTMS 会議（暗号化）に参加できます。CTMS のバージョンが 1.9.1 より古い場合には、この値を使用しないでください。

例： `NetworkServices CTMS Encryption: Off`

周辺機器設定

Peripherals Pairing CiscoTouchPanels RemotePairing

ビデオ システムのユーザ インターフェイスとしてシスコのタッチ 10（タッチ パネル）を使用するには、タッチ 10 をビデオ システムに直接接続するか、LAN 経由でビデオ システムとペアリングする必要があります。後者はリモート ペアリングと呼ばれます。

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

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（Off）]：タッチ 10 のリモート ペアリングは許可されません。

[オン（On）]：タッチ 10 リモート ペアリングは許可されます。

例：

```
Peripherals Pairing CiscoTouchPanels RemotePairing: On
```

Peripherals Profile TouchPanels

ビデオ システムに接続されることが予想されるタッチ パネルの数を設定します。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。接続されたタッチ パネル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。このバージョンでサポートされるシスコ タッチ コントローラは、1 台のみであることに注意してください。

必要なユーザ ロール： ADMIN

値スペース： <NotSet/Minimum1/0/1/2/3/4/5>

[設定されていない（NotSet）]：タッチ パネル チェックは実行されません。

[最小 1（Minimum1）]：少なくとも 1 台のタッチ パネルがビデオ システムに接続されている必要があります。

0-5：この数のタッチ コントローラがビデオ システムに接続されている必要があります。

例：

```
Peripherals Profile TouchPanels: Minimum1
```

電話帳設定

Phonebook Server [1..1] ID

外部の電話帳の名前を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：`Phonebook Server 1 ID: ""`

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

値スペース：<VCS/TMS/Callway/CUCM>

[VCS]：電話帳が Cisco TelePresence ビデオ コミュニケーション サーバにある場合は、VCS を選択します。

[TMS]：電話帳が Cisco TelePresence 管理スイート サーバにある場合は、TMS を選択します。

[Callway]：電話帳が WebEx TelePresence サブスクリプション サービス（旧称：CallWay）によって提供される場合は、Callway を選択します。詳細については WebEx TelePresence のプロバイダーにお問い合わせください。

[CUCM]：電話帳が Cisco Unified Communications Manager にある場合は、CUCM を選択します。

例：`Phonebook Server 1 Type: TMS`

Phonebook Server [1..1] URL

外部電話帳のサーバ アドレス（URL）を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：`Phonebook Server 1 URL: "http://tms.company.com/tms/public/external/phonebook/phonebookservice.asmx"`

プロビジョニング 設定

Provisioning Connectivity

この設定は、プロビジョニング サーバからの内部または外部の設定を要求するかどうかを、デバイスが検出する方法を制御します。

必要なユーザ ロール：ADMIN

値スペース：<Internal/External/Auto>

[内部（Internal）]：内部コンフィギュレーションを要求します。

[外部（External）]：外部コンフィギュレーションを要求します。

[自動（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、外部設定が要求されます。それ以外の場合、内部設定が要求されます。

例：`Provisioning Connectivity: Auto`

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

値スペース：<Off/TMS/VCS/CallWay/CUCM/Auto/Edge>

[オフ（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。

[自動（Auto）]：プロビジョニング サーバはビデオ システムによって自動的に選択されます。

[TMS]：ビデオ システムは TMS（Cisco TelePresence 管理システム）を使用して設定されます。

[VCS]：ビデオ システムは VCS（Cisco TelePresence Video Communication Server）を使用して設定されます。

[Callway]：ビデオ システムは WebEx TelePresence サブスクリプション サービス（旧称：CallWay）を使用して設定します。

[CUCM]：ビデオ システムは CUCM（Cisco Unified Communications Manager）を使用して設定されます。

[Edge]：システムは Collaboration Edge インフラストラクチャを経由して CUCM に接続します。

例：`Provisioning Mode: Auto`

Provisioning LoginName

これは、プロビジョニング 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。Provisioning Mode が Callway（WebEx TelePresence）の場合、ビデオ番号を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 80>

フォーマット：最大 80 文字の文字列。

例：`Provisioning LoginName: ""`

Provisioning Password

これは、プロビジョニング 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。Provisioning Mode が Callway（WebEx TelePresence）の場合、アクティベーション コードを入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：`Provisioning Password: ""`

Provisioning HttpMethod

プロビジョニングに使用する HTTP 方式を選択します。

必要なユーザ ロール：ADMIN

値スペース：<GET/POST>

[GET]：プロビジョニング サーバが GET をサポートする場合、GET を選択します。

[POST]：プロビジョニング サーバが POST をサポートする場合、POST を選択します。

例：`Provisioning HttpMethod: POST`

Provisioning ExternalManager Address

外部マネージャやプロビジョニング システムの IP アドレスまたは DNS 名を入力します。

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、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設定/コマンドを結果として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)。Provisioning ExternalManager Address 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

値スペース: <S: 0, 64>

*フォーマット:*有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例: `Provisioning ExternalManager Address: ""`

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 のアドレスを入力します。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

値スペース: <S: 0, 64>

*フォーマット:*有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例: `Provisioning ExternalManager AlternateAddress: ""`

Provisioning ExternalManager Protocol

セキュア管理を使用するかどうかを指定します。

必要なユーザ ロール: ADMIN

値スペース: <HTTP/HTTPS>

[HTTP]:HTTP に設定してセキュアな管理をディセーブルにします。HTTP は NetworkServices HTTP Mode の設定でイネーブルにする必要があります。

[HTTPS]:HTTPS に設定してセキュアな管理をイネーブルにします。HTTPS は NetworkServices HTTPS Mode の設定でイネーブルにする必要があります。

例: `Provisioning ExternalManager Protocol: HTTP`

Provisioning ExternalManager Path

外部マネージャ/プロビジョニング システムへのパスを設定します。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

値スペース: <S: 0, 255>

*フォーマット:*最大 255 文字の文字列。

例: `Provisioning ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを入力します。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 64>

*フォーマット:*最大 64 文字の文字列。

例: `Provisioning ExternalManager Domain: "any.domain.com"`

RTP 設定

RTP Ports Range Start

RTP ポート範囲の最初のポートを指定します。「H323 Profile [1..1] PortAllocation」設定も参照してください。

注: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

値スペース: <1024..65438>

範囲: 1024 ～ 65438 の値を選択します。

例: `RTP Ports Range Start: 2326`

RTP Ports Range Stop

RTP ポート範囲の最後のポートを指定します。「H323 Profile [1..1] PortAllocation」設定も参照してください。

注: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

値スペース: <1120..65535>

範囲: 1120 ～ 65535 の値を選択します。

例: `RTP Ports Range Stop: 2486`

セキュリティ 設定

Security Audit Logging Mode

監査ログを記録または送信する場所を設定します。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

値スペース: <Off/Internal/External/ExternalSecure>

[オフ (Off)]: 監査ロギングは実行されません。

[内部 (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。

[外部 (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。

[外部保護 (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。

例: `Security Audit Logging Mode: Off`

Security Audit OnError Action

syslog サーバへの接続が失われた場合の動作を指定します。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

値スペース: <Halt/Ignore>

[停止 (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。次のような停止状態があります。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。

[無視 (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。

例: `Security Audit OnError Action: Ignore`

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 アドレスを入力します。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

値スペース: <S: 0, 64>

フォーマット: 有効な IPv4 アドレスまたは IPv6 アドレス

例: `Security Audit Server Address: ""`

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 サーバのポートを入力します。この設定は、[セキュリティ監査ポートの割当て (Security Audit PortAssignment)] が [手動 (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

値スペース: <0..65535>

範囲: 0 ～ 65535 の値を選択します。

例: `Security Audit Server Port: 514`

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、[セキュリティ監査サーバのポート (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 [設定 (Configuration)] > [システム ステータス (System 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

値スペース: <Auto/Manual>

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

[手動 (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。

例: `Security Audit Server PortAssignment: Auto`

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

値スペース：<Off/On>

[オン（On）]：最後のセッションに関する情報を表示します。

[オフ（Off）]：最後のセッションに関する情報を表示しません。

例：`Security Session ShowLastLogon: Off`

Security Session InactivityTimeout

ユーザが自動的にログ 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決定します。

必要なユーザ ロール：ADMIN

値スペース：<0..10000>

*範囲：*1 ～ 10000 秒の値を選択します。または、非アクティブ状態により自動ログアウトを強制しない場合は、0 を選択します。

例：`Security Session InactivityTimeout: 0`

SerialPort 設定

SerialPort Mode

シリアル ポート（Micro USB から USB ケーブルへの接続を介して）をイネーブルまたはディセーブルにします。シリアル ポートは 115200 bps、8 データ ビット、パリティなし、1 ストップ ビットを使用します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（Off）]：シリアル ポートをディセーブルにします。

[オン（On）]：シリアル ポートをイネーブルにします。

例：`SerialPort Mode: On`

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決定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（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。

[オン（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。

例：`SerialPort LoginRequired: On`

SIP 設定

SIP ANAT

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

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（Off）]：ANAT をディセーブルにします。

[オン（On）]：ANAT をイネーブルにします。

例： `SIP ANAT: Off`

SIP AuthenticateTransferror

このバージョンでは適用されません。

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。この設定はデフォルト値のままにすることを推奨します。

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（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。

[オン（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。

例： `SIP ListenPort: On`

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

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。

例： `SIP PreferredIPMedia: IPv4`

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 [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。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

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。

例： `SIP PreferredIPSignaling: IPv4`

SIP OCSP Mode

このバージョンでは適用されません。

SIP OCSP DefaultResponder

このバージョンでは適用されません。

SIP Profile [1..1] Ice Mode

ICE（Interactive Connectivity Establishment、RFC 5245）は、最適化されたメディア パスの検出にエンドポイントで使用できる NAT トラバーサル ソリューションです。このため、音声とビデオの最短ルートがエンドポイント間で常に確保されます。注：ICE は CUCM（Cisco Unified Communication Manager）に登録された場合はサポートされません。

必要なユーザ ロール： ADMIN

値スペース： <Auto/Off/On>

[自動（Auto）]：[自動（Auto）] に設定すると、TURN サーバを指定した場合に ICE がイネーブルになります。そうでない場合 ICE はディセーブルです。

[オフ（Off）]：ICE をディセーブルにします。

[オン（On）]：ICE をイネーブルにします。

例： `SIP Profile 1 Ice Mode: Auto`

SIP Profile [1..1] Ice DefaultCandidate

これは、ICE が使用するメディア ルートを決定するまで（コールの最初の 5 秒まで）エンドポイントがメディアを受け取るデフォルトの IP アドレスです。

必要なユーザ ロール： ADMIN

値スペース： <Host/Rflx/Relay>

[ホスト（Host）]：エンドポイントは固有の IP アドレスでメディアを受信します。

[Rflx]：エンドポイントは TURN サーバで認識されるパブリック IP アドレスでメディアを受信します。

[リレー（Relay）]：エンドポイントは TURN サーバで割り当てられた IP アドレスとポートでメディアを受信し、ICE が完了するまでフォールバックとして使用されます。

例： `SIP Profile 1 Ice DefaultCandidate: Host`

SIP Profile [1..1] Turn DiscoverMode

アプリケーションで DNS で利用可能な TURN サーバの検索を有効または無効にするには、検出モードを設定します。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

値スペース： <Off/On>

[オフ（Off）]：検出モードをディセーブルにします。

[オン（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。

例： `SIP Profile Turn DiscoverMode: On`

SIP Profile [1..1] Turn BandwidthProbe

このバージョンでは適用されません。

SIP Profile [1..1] 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

値スペース： <Off/On>

[オフ（Off）]：DropRflx をディセーブルにします。

[オン（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。

例： `SIP Profile Turn DropRflx: Off`

SIP Profile [1..1] Turn Server

これはエンドポイントで使用される TURN（Traversal Using Relay NAT）サーバのアドレスです。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

値スペース： <S: 0, 255>

*フォーマット：*優先されるフォーマットは DNS SRV レコード（例：_turn._udp.<domain>）、または有効な IPv4 アドレスまたは IPv6 アドレスを指定できます。

例： `SIP Profile 1 Turn Server: "_turn._udp.example.com"`

SIP Profile [1..1] Turn UserName

TURN サーバへのアクセスに必要なユーザ名です。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 128>

*フォーマット：*最大 128 文字の文字列。

例： `SIP Profile 1 Turn UserName: ""`

SIP Profile [1..1] Turn Password

TURN サーバへのアクセスに必要なパスワードです。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 128>

*フォーマット:*最大 128 文字の文字列。

例: `SIP Profile 1 Turn Password: ""`

SIP Profile [1..1] 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

値スペース: <S: 0, 255>

*フォーマット:*最大で 255 文字で SIP URI 構文に準拠します。

例: `SIP Profile 1 URI: "sip:firstname.lastname@company.com"`

SIP Profile [1..1] DisplayName

設定されたとき、着信コールは SIP URI ではなく、DisplayName を報告します。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 255>

*フォーマット:*最大 255 文字の文字列。

例: `SIP Profile 1 DisplayName: ""`

SIP Profile [1..1] Authentication [1..1] LoginName

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

値スペース: <S: 0, 128>

*フォーマット:*最大 128 文字の文字列。

例: `SIP Profile 1 Authentication 1 LoginName: ""`

SIP Profile [1..1] Authentication [1..1] 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

値スペース: <S: 0, 128>

*フォーマット:*最大 128 文字の文字列。

例: `SIP Profile 1 Authentication 1 Password: ""`

SIP Profile [1..1] 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

値スペース: <TCP/UDP/Tls/Auto>

[TCP]:システムはデフォルトの転送方法として常に TCP を使用します。

[UDP]:システムはデフォルトの転送方法として常に UDP を使用します。

[Tls]:システムはデフォルトの転送方法として常に TLS を使用します。TLS 接続の場合、SIP CA リストをビデオ システムにアップロードできます。このような CA リストがシステムにない場合は匿名の Diffie Hellman が使用されます。

[自動(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。

例: `SIP Profile 1 DefaultTransport: Auto`

SIP Profile [1..1] 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

値スペース: <Off/On>

[オフ(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、SIP CA リストがアップロードされていない場合に選択する必要があります。

[オン(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。

例: `SIP Profile 1 TlsVerify: Off`

SIP Profile [1..1] Outbound

ファイアウォール トラバーサル、接続の再利用および冗長性のための、クライアント開始接続メカニズムをオンまたはオフにします。現在のバージョンは RFC 5626 をサポートします。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（Off）]：プロキシ アドレス リストに最初に設定されている単一プロキシに接続します。

[オン（On）]：プロキシ アドレス リストのサーバへの複数のアウトバウンド接続をセットアップします。

例：`SIP Profile 1 Outbound: Off`

SIP Profile [1..1] 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 アドレスを使用できます。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。SIP プロファイル発信がイネーブルの場合、複数のプロキシをアドレス指定できます。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

*フォーマット：*有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例：`SIP Profile 1 Proxy 1 Address: ""`

SIP Profile [1..1] Proxy [1..4] Discovery

SIP プロキシ アドレスを手動とダイナミック ホスト コンフィギュレーション プロトコル（DHCP）のどちらを使用して取得するかを選択します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

[自動（Auto）]：Auto が選択されると、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を使用して SIP プロキシ アドレスを取得します。

[手動（Manual）：[手動（Manual）] が選択されると、手動で設定された SIP プロキシ アドレスが使用されます。

例：`SIP Profile 1 Proxy 1 Discovery: Manual`

SIP Profile [1..1] 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イネーブルにします。

必要なユーザ ロール：ADMIN

値スペース：<Standard/Cisco>

[標準（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 および Broadsoft 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。

例：`SIP Profile 1 Type: Standard`

SIP Profile [1..1] 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。メールボックスの番号（アドレス）をこの設定に入力するか、またはボイス メールボックスがない場合は文字列を空のままにしてください。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>>

*フォーマット：*最大 255 文字の文字列。

例：`SIP Profile 1 Mailbox: "12345678"`

SIP Profile [1..1] 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することができます。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

値スペース：<Private/Shared>

[共有（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。

[プライベート（Private）]：このシステムは共有回線の一部ではありません（デフォルト）。

例：`SIP Profile 1 Line: Private`

スタンバイ設定

Standby Control

システムがスタンバイ モードに移行するかどうかを決定します。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(Off)]:システムはスタンバイ モードを開始しません。

[オン(On)]:Standby Delay がタイム アウトになったときにスタンバイ モードを開始します。[スタンバイ遅延(Standby Delay)] を適切な値に設定する必要があります。

例: `Standby Control: On`

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)] がイネーブルである必要があります。

必要なユーザ ロール: ADMIN

値スペース: <1..480>

*範囲:*1 ～ 480 分の値を選択します。

例: `Standby Delay: 10`

Standby BootAction

コーデックの再起動後のカメラの位置を定義します。

必要なユーザ ロール: ADMIN

値スペース: <None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

[なし(None)]:アクションはありません。

[プリセット 1 ～ 15(Preset1 ～ Preset15)]:再起動後、カメラ位置は選択したプリセットによって定義された位置にセットされます。

[RestoreCameraPosition]:再起動後、カメラ位置は前回のブート前の位置にセットされます。

[DefaultCameraPosition]:再起動後、カメラ位置は工場出荷時のデフォルトの位置にセットされます。

例: `Standby BootAction: DefaultCameraPosition`

Standby StandbyAction

スタンバイ モードに入るときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN

値スペース: <None/PrivacyPosition>

[なし(None)]:アクションはありません。

[PrivacyPosition]:プライバシーのためカメラを横向き位置に向けます。

例: `Standby StandbyAction: PrivacyPosition`

Standby WakeupAction

スタンバイ モードを抜けるときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN

値スペース: <None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

[なし(None)]:アクションはありません。

[プリセット 1 ～ 15(Preset1 ～ Preset15)]:スタンバイを抜けるとき、カメラ位置は選択したプリセットによって定義された位置にセットされます。

[RestoreCameraPosition]:スタンバイを抜けるとき、カメラ位置はスタンバイに入る前の位置にセットされます。

[DefaultCameraPosition]:スタンバイを抜けるとき、カメラ位置は工場出荷時のデフォルトの位置にセットされます。

例: `Standby WakeupAction: RestoreCameraPosition`

システム ユニット設定

SystemUnit Name

システム装置の名前を定義するシステム名を入力します。システムで H.323 エイリアス ID が設定されている場合、この ID がシステム名の代わりに使用されます。次の場合にシステム名が表示されます。

1）コーデックが SNMP エージェントとして機能している場合。

2）DHCP サーバ向け。

必要なユーザ ロール： ADMIN

値スペース： <S: 0, 50>

フォーマット：最大 50 文字の文字列。

例： `SystemUnit Name: "Meeting Room"`

SystemUnit MenuLanguage

これは、UserInterface Language 設定で置き換えられました。

SystemUnit CallLogging Mode

システムが受信または送信するコールのコール ロギング モードを設定します。コール ログは、Web インターフェイスを介して表示できます。

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（Off）]：ロギングをディセーブルにします。

[オン（On）]：ロギングをイネーブルにします。

例： `SystemUnit CallLogging Mode: On`

SystemUnit ContactInfo Type

タッチ コントローラの左上隅にあるステータス フィールドに表示される連絡先情報のタイプを選択します。

必要なユーザ ロール： ADMIN

値スペース： <Auto/None/IPv4/IPv6/H323Id/E164Alias/H320Number/SipUri/SystemName/DisplayName>

[自動（Auto）]：このシステムに到達するために別のシステムがダイヤルできるアドレスを示します。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。

[なし（None）]：ステータス フィールドに連絡先情報を表示しません。

[IPv4]：連絡先情報として IPv4 アドレスを表示します。

[IPv6]：連絡先情報として IPv6 アドレスを表示します。

[H323Id]：連絡先情報として H.323 ID を表示します（H323 Profile [1..1] H323Alias ID 設定を参照）。

[E164Alias]：連絡先情報として H.323 E164 エイリアスを表示します（H323 Profile [1..1] H323Alias E164 設定を参照）。

[H320Number]：連絡先情報として H.320 番号を表示します（Cisco TelePresence ISDN リンク ゲートウェイに接続されている場合のみ）。

[SipUri]：連絡先情報として SIP URI を表示します（SIP Profile [1..1] URI 設定を参照）。

[システム名（SystemName）]：連絡先情報としてシステム名を表示します（SystemUnit Name 設定を参照）。

[表示名（DisplayName）]：連絡先情報として表示名を表示します（SIP Profile [1..1] DisplayName 設定を参照）。

例： `SystemUnit ContactInfo Type: Auto`

時刻設定

Time TimeFormat

時間のフォーマットを設定します。

必要なユーザ ロール：USER

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。

例：`Time TimeFormat: 24H`

Time DateFormat

日付のフォーマットを設定します。

必要なユーザ ロール：USER

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。

例：`Time DateFormat: DD_MM_YY`

タイム ゾーン

これは、ソフトウェア バージョン TC7.2 以降、Time OlsonZone 設定で置き換えられました。

Time OlsonZone

ビデオ システムの地理的な場所のタイム 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：USER

値スペース：<Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Ensenada, America/Fort_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/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/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, 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/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, 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/Easterlsland, 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/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/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/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/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>

*範囲:*リストからタイム ゾーンを選択します。

例: 範囲:リストのタイム ゾーンからタイム ゾーンを選択します。

ユーザ インターフェイス設定

UserInterface Language

画面およびタッチ コントローラでメニューやメッセージで使用される言語を選択します。デフォルトの言語は英語です。

必要なユーザ ロール: USER

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

*範囲:*リストから言語を選択します。

例: `UserInterface Language: English`

UserInterface OSD EncryptionIndicator

暗号化インジケータ(鍵)が画面に表示される時間の長さを定義します。この設定は、暗号化されたコールと暗号化されていないコール、つまりセキュアな会議と非セキュアな会議の両方に適用されます。暗号化されたコールはロックされた鍵のアイコンで示され、暗号化されていないコールはバツ印の付いたロックされた鍵のアイコンで示されます。

必要なユーザ ロール: ADMIN

値スペース: <Auto/AlwaysOn/AlwaysOff>

[自動(Auto)]:Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されている場合、暗号化インジケータがコールの最初の数秒間に表示されます。Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されていない場合、バツ印の付いた暗号化インジケータがコール全体にわたり表示されます。Conference Encryption Mode 設定が BestEffort に設定されていない場合、暗号化インジケータはまったく表示されません。

[常時オン(AlwaysOn)]:暗号化インジケータはコール全体にわたり画面上に表示されます。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用されます。

[常時オフ(AlwaysOff)]:暗号化インジケータは画面上に表示されません。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用されます。

例: `UserInterface OSD EncryptionIndicator: Auto`

UserInterface OSD LanguageSelection

ユーザが、[設定(Settings)]メニューから簡単に言語設定を変更しないようにするには、[管理者設定(Administrator Settings)]メニューから言語設定を使用できます。管理者設定はパスワードで保護することができます。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ(Off)]:言語は、[管理者設定(Administrator Settings)]メニューから設定されます。

[オン(On)]:言語は、[設定(Settings)]メニューから設定されます。

例: `UserInterface OSD LanguageSelection: On`

UserInterface OSD LoginRequired

このバージョンでは適用されません。

UserInterface OSD Output

画面情報およびインジケータを表示するモニタを定義します。

必要なユーザ ロール: ADMIN

値スペース: <Auto/1/2>

[自動(Auto)]:システムは情報とインジケータをシステムの内蔵 LCD ディスプレイに送信します。

範囲:1 ～ 2:システムは情報とインジケータを指定した出力に送信します。情報とインジケータを内蔵 LCD ディスプレイに送信するには 1 を選択してください。OSD をシステムの HDMI 出力に接続されたディスプレイに送信するには 2 を選択してください。

例: `UserInterface OSD Output: Auto`

UserInterface Wallpaper

アイドル状態のときのビデオ画面の背景イメージ（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次の BMP、JPEG、GIF、PNG です。最大ファイル サイズは 2 MByte です。

必要なユーザ ロール： USER

値スペース： <None/Custom>

[なし（None）]：画面に背景イメージはありません。

[カスタム（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。

例： `UserInterface Wallpaper: None`

UserInterface TouchPanel DefaultPanel

タッチ コントローラが復帰時に表示する内容（連絡先リスト、会議リスト、またはダイヤル パッド）を定義します。

必要なユーザ ロール： USER

値スペース： <None/LastUsed/ContactList/MeetingList/Dialpad>

[なし（None）]：次のオプションはいずれもデフォルトでタッチ コントローラに表示されません。

[前回使用（LastUsed）]：前回使用した内容（連絡先リスト、会議リスト、またはダイヤル パッド）がデフォルトでタッチ コントローラに表示されます。

[連絡先リスト（ContactList）]：連絡先リスト（お気に入り, ディレクトリおよび履歴）がタッチ コントローラのデフォルトとして表示されます。

[会議リスト（MeetingList）]：スケジュールされた会議のリストがタッチ コントローラのデフォルトとして表示されます。

[ダイヤル パッド（Dialpad）]：ダイヤル パッドがタッチ コントローラのデフォルトとして表示されます。

例： `UserInterface TouchPanel DefaultPanel: None`

UserInterface UserPreferences

一部のユーザ設定（呼び出し音、音量、言語、日時など）は、タッチ コントローラの [設定（Settings）] メニュー、または [設定（Settings）] > [管理者（Administrator）] メニューから利用できるように設定できます。[管理者（Administrator）] メニューにアクセスする場合は、ユーザは管理者権限を持っている必要があります。

必要なユーザ ロール： ADMIN

値スペース： <Off/On>

[オフ（Off）]：ユーザ設定は、管理者権限を持つユーザに対して、タッチ コントローラの [設定（Settings）] > [管理者（Administrator）] メニューから選択できます。

[オン（On）]：ユーザ設定は、タッチ コントローラの [設定（Settings）] メニューから選択できます。

例： `UserInterface UserPreferences: Off`

ビデオ設定

Video AllowWebSnapshots

ローカル入力ソース、リモート サイトおよびプレゼンテーション チャネルで取得されるスナップショットを許可または拒否します。スナップショットが許可されている場合、Web インターフェイスの [コール制御 (Call Control)] ページに、アイドル状態または通話中の両方でスナップショットが表示されます。

デフォルトではスナップショットは許可されていません。スナップショットを取得できるようにするには、この設定を [オン (On)] に切り替える必要があります。

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ (Off)]: Web スナップショットのキャプチャは許可されません。

[オン (On)]: Web スナップショットをキャプチャし、Web インターフェイスに表示できます。

例: `Video AllowWebSnapshots: Off`

Video CamCtrlPip CallSetup 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。Video CamCtrlPip CallSetup Duration 設定は、それが維持される時間の長さを指定します。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

値スペース: <Off/On>

[オフ (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。

[オン (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。

例: `Video CamCtrlPip CallSetup Mode: On`

Video CamCtrlPip CallSetup Duration

この設定は Video CamCtrlPip CallSetup Mode 設定がオンである場合のみ有効です。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

値スペース: <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。

例: `Video CamCtrlPip CallSetup Duration: 10`

Video Input Connector [1..4] Name

ビデオ入力コネクタの名前を入力します。

必要なユーザ ロール: ADMIN

値スペース: <S: 0, 50>

フォーマット: 最大 50 文字の文字列。

例: `Video Input Connector 1 Name: ""`

Video Input Connector [1..4] 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

値スペース: コネクタ 1: <camera> 他のコネクタ: <other/camera/PC/DVD/document_camera/whiteboard>

[その他 (other)]: 下記のオプションのいずれにも一致しない場合に使用します。

[カメラ (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。

[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。

[DVD]: DVD 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。

[ドキュメント カメラ (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。

[ホワイトボード (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。

例: `Video Input Connector 2 InputSourceType: PC`

Video Input Connector [1..4] 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。

> Video Input Connector 2 Visibility（DVI コネクタ）のデフォルト値は [常時（Always）] です。

> Video Input Connector 3,4 Visibility のデフォルト値は [IfSignal] です。

必要なユーザ ロール： ADMIN

値スペース： コネクタ 1：<Never>　他のコネクタ：<Never/Always/IfSignal>

[なし（Never）]：入力ソースがプレゼンテーション ソースとして使用される見込みがない場合、[なし（Never）] に設定します。

[常時（Always）]：[常時（Always）] に設定すると、ビデオ入力コネクタ用メニュー選択はグラフィカル ユーザ インターフェイスに常に表示されます。

[シグナルがある場合（IfSignal）]：[シグナルがある場合（IfSignal）] に設定すると、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。

例：
```
Video Input Connector 2 Visibility: Always
```

Video Input Connector [1..4] CameraControl Mode

このビデオ入力コネクタに接続されているカメラを制御するかどうかを定義します。

カメラ制御はコネクタ 2（HDMI）、コネクタ 3（HDMI）、およびコネクタ 4（DVI-I）では使用できないことに注意してください。

必要なユーザ ロール： ADMIN

値スペース： コネクタ 1：<Off/On>　コネクタ 2、3、4：<Off>

[オフ（Off）]：カメラ制御をディセーブルにします。

[オン（On）]：カメラ制御をイネーブルにします。

例：
```
Video Input Connector 1 CameraControl Mode: On
```

Video Input Connector [1..4] CameraControl CameraId

カメラ ID を定義します。この値は固定されており、変更できません。

必要なユーザ ロール： ADMIN

値スペース： <1>

*範囲：*この値は固定されており、変更できません。

例：
```
Video Input Connector 1 CameraControl CameraId: 1
```

Video Input Connector [2..4] Quality

ビデオのエンコードと送信のときには、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。

必要なユーザ ロール： ADMIN

値スペース： <Motion/Sharpness>

[モーション（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。

[シャープさ（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。

例：
```
Video Input Connector 3 Quality: Sharpness
```

Video Input Connector [1..4] OptimalDefinition Profile

この設定は、対応する Video Input Connector Quality 設定が [モーション (Motion)] に設定されている場合のみ有効になります。

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。良い光の条件では、ビデオ エンコーダは指定のコール レートに一層優れた品質 (高解像度またはフレーム レート) を提供します。通常、[標準 (Normal)] または [中 (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、[高 (High)] プロファイルを設定できます。

異なる最適鮮明度プロファイルに使用する一般的な解像度、コール レートおよび送信フレーム レートの一部を次の表に示します。解像度は、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。Video Input Source OptimalDefinition Threshold60fps 設定を使用し、60 fps のフレーム レートをいつ使用するか決定します。

さまざまな最適鮮明度プロファイル、コール レート、フレーム レートで使用される一般的な解像度

フレーム レート	最適鮮明度プロファイル	コール レート						
		256 kbps	*768 kbps*	*1152 kbps*	*1472 kbps*	*2560 kbps*	*4 Mbps*	*6 Mbps*
30 fps	*標準*	512X288	1024X576	1280X720	1280X720	1920X1080	1920X1080	1920X1080
	中型	640X360	1280X720	1280X720	1280X720	1920X1080	1920X1080	1920X1080
	大 (High)	768X448	1280X720	1280X720	1920X1080	1920X1080	1920X1080	1920X1080
60 fps	*標準*	256X144	512X288	768X448	1024X576	1280X720	1280X720	1920X1080
	中型	256X144	768X448	1024X576	1024X576	1280X720	1920X1080	1920X1080
	大 (High)	512X288	1024X576	1280X720	1280X720	1920X1080	1920X1080	1920X1080

必要なユーザ ロール: ADMIN

値スペース: <Normal/Medium/High>

[標準 (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。

[中 (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。

[高 (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。高い解像度が使用されます。

例: `Video Input Connector 1 OptimalDefinition Profile: Medium`

Video Input Connector [1..4] OptimalDefinition Threshold60fp

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

必要なユーザ ロール: ADMIN

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

[512_288]: 512x288 にしきい値を設定します。

[768_448]: 768x448 にしきい値を設定します。

[1024_576]: 1024x576 にしきい値を設定します。

[1280_720]: 1280x720 にしきい値を設定します。

[1920_1080]: 1920x1080 にしきい値を設定します。

[なし (Never)]: 60 fps を送信するしきい値を設定しません。

例: `Video Input Connector 1 OptimalDefinition Threshold60fps: 1280_720`

Video Input Connector [2..4] 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。相手先とプレゼンテーションを共有すると、常に追加アクションが必要となることに注意してください (ユーザ インターフェイスで [共有 (Share)] を押します)。

必要なユーザ ロール: ADMIN

値スペース: <Manual/Automatic/OnConnect>

[手動 (Manual)]: 手動モードでは、ビデオ入力の内容をユーザ インターフェイスから選択するまで画面に表示されません。

[自動 (Automatic)]: 自動モードでは、ビデオ入力の内容が画面に自動的に表示されます。複数のソースが [自動 (Automatic)] に設定されている場合、最後に接続されたソースが使用されます。コールが切断されたときにすべてのコンテンツがアクティブな (表示される) 場合、コンテンツはローカルに表示されたままの状態になります。

[接続中 (OnConnect)]: [接続中 (OnConnect)] モードでは、ケーブルが接続されている場合はビデオ入力の内容が画面に表示されます。それ以外の場合は、[手動 (Manual)] モードと同じ動作です。

例: `Video Input Connector 2 PresentationSelection: OnConnect`

Video Input Connector [2..4] 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ないため、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することができます。ほとんどのソースは完全な量子化範囲を想定するため、デフォルト値は [フル (Full)] に設定されます。

必要なユーザ ロール： ADMIN

値スペース： <Auto/Full/Limited>

[自動 (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。

[フル (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。

[制限 (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。

例： `Video Input Connector 2 RGBQuantizationRange: Full`

Video Input Connector [2] DviType

公式 DVI 規格は、デジタル信号とアナログ信号の両方をサポートします。ほとんどの場合、デフォルトの AutoDetect 設定で信号がアナログ RGB かデジタルかを検出できます。ただし DVI-I ケーブルを使用した場合 (これらのケーブルはアナログとデジタル両方の信号を伝送できます)、まれに自動検出に失敗することがあります。この設定により、AutoDetect を上書きし、正しい DVI ビデオ入力を選択できます。

必要なユーザ ロール： ADMIN

値スペース： <AutoDetect/Digital/AnalogRGB/AnalogYPbPr>

[自動検出 (AutoDetect)]：信号がアナログ RGB かデジタルかを自動的に検出するには、[自動検出 (AutoDetect)] に設定します。

[デジタル (Digital)]：アナログとデジタルの両方のピンを持つ DVI-I ケーブルを使用し、AutoDetect が失敗する場合、Digital に設定すると DVI ビデオ入力を強制的に [デジタル (Digital)] にします。

[アナログ RGB (AnalogRGB)]：アナログとデジタルの両方のピンを持つ DVI-I ケーブルを使用し、[自動検出 (AutoDetect)] が失敗する場合、[アナログ RGB (AnalogRGB)] に設定すると DVI ビデオ入力を強制的にアナログ RGB にします。

[アナログ YPbPr (AnalogYPbPr)]：コンポーネント (YPbPr) の信号を自動検出できないため、[アナログ YPbPr (AnalogYPbPr)] に設定して DVI ビデオ入力を強制的にアナログ YPbPr にします。

例： `Video Input Connector 2 DviType: AutoDetect`

Video Layout DisableDisconnectedLocalOutputs

この設定は、On に固定されています。

必要なユーザ ロール： ADMIN

値スペース： <On>

[オン (On)]：組み込みのレイアウト エンジンはモニタを接続するローカル出力のみレイアウトを設定します。

例： `Video Layout DisableDisconnectedLocalOutputs: On`

Video Layout LocalLayoutFamily

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

値スペース： <Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker/Prominent/Overlay/Single>

[自動 (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。

[全画面 (FullScreen)]：この値は使用しないでください。

[等しい (Equal)]：[等しい (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。

[プレゼンテーション スモール スピーカ (PresentationSmallSpeaker)]：この値は使用しないでください。

[プレゼンテーション ラージ スピーカ (PresentationLargeSpeaker)]：この値は使用しないでください。

[対象拡大表示 (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。

[オーバーレイ (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。

[一画面表示 (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。

例： `Video Layout LocalLayoutFamily: Auto`

Video Layout PresentationDefault View

プレゼンテーションの共有を開始する際に、プレゼンテーションが画面にどのように表示されるかを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Default/Minimized/Maximized>

[デフォルト（Default）]：プレゼンテーションは、レイアウトの一部です。

[最小化（Minimized）]：プレゼンテーションは PIP モードで開始されます。

[最大化（Maximized）]：プレゼンテーションは、全画面モードで開始されます。

例：`Video Layout PresentationDefault View: Default`

Video Layout RemoteLayoutFamily

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

値スペース：<Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker/Prominent/Overlay/Single>

[自動（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。

[全画面（FullScreen）]：この値は使用しないでください。

[等しい（Equal）]：[等しい（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。

[プレゼンテーション スモール スピーカ（PresentationSmallSpeaker）]：この値は使用しないでください。

[プレゼンテーション ラージ スピーカ（PresentationLargeSpeaker）]：この値は使用しないでください。

[対象拡大表示（Prominent）]：[対象拡大表示（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。

[オーバーレイ（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。

[一画面表示（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。

例：`Video Layout RemoteLayoutFamily: Auto`

Video Layout Scaling

イメージとそれを配置するフレームとの間に違いがある場合、システムがイメージまたはフレームのアスペクト比をどのように調整するかを定義します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

[オフ（Off）]：アスペクト比の調整はありません

[オン（On）]：システムがアスペクト比を自動的に調整できるようにします。

例：`Video Layout Scaling: On`

Video Layout ScaleToFrame

ビデオ入力ソースのアスペクト比がコンポジション内の対応するイメージ フレーム アスペクト比と一致しない場合の対処方法を定義します。たとえば、4:3 入力（XGA など）を 16:9 出力（HD720 など）に表示する場合です。

必要なユーザ ロール：ADMIN

値スペース：<Manual/MaintainAspectRatio/StretchToFit>

[手動（Manual）]：ビデオ入力ソースとターゲット イメージ フレーム間のアスペクト比の違いが Video Layout ScaleToFrameThreshold 設定（パーセンテージ）よりも小さい場合、イメージはフィットするよう拡大されます。そうでない場合は、元のアスペクト比が維持されます。

[アスペクト比の維持（MaintainAspectRatio）]：入力ソースのアスペクト比を維持し、フレームの残りの部分（文字のボクシングや柱のボクシング）は黒で埋めます。

[フレームに合わせる（StretchToFit）]：イメージのフレームにフィットするよう入力ソースを（水平または垂直に）拡張します。注：一般的な制限として、1 方向を拡大しながら別の方向を縮小することはできません。このような状況で、コーデックは letterboxing を適用します。

例：`Video Layout ScaleToFrame: MaintainAspectRatio`

Video Layout ScaleToFrameThreshold

Video Layout ScaleToFrame が [手動（Manual）] に設定されている場合に限り適用できます。ビデオ入力ソースとターゲット イメージ フレーム間のアスペクト比の違いが ScaleToFrameThreshold 設定（パーセンテージ）よりも小さい場合、イメージはフィットするよう拡大されます。そうでない場合は、元のアスペクト比が維持されます。

必要なユーザ ロール：ADMIN

値スペース：<0..100>

*範囲:*0 ～ 100 % の値を選択します。

例：`Video Layout ScaleToFrameThreshold: 5`

Video PIP ActiveSpeaker DefaultValue Position

通話中のスピーカーのピクチャ イン ピクチャ(PiP)画面の位置を設定します。この設定は通話中のスピーカーが PiP に表示されるビデオ レイアウトを使用する場合、つまりオーバーレイ レイアウト、またはカスタム レイアウト(Video Layout LocalLayoutFamily 設定を参照)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

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

[現在(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。
[左上隅(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。
[上部中央(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。
[右上隅(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。
[左中央(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。
[右中央(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。
[左下隅(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。
[右下隅(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。

例:
```
Video PIP ActiveSpeaker DefaultValue Position: Current
```

Video PIP Presentation DefaultValue Position

プレゼンテーションのピクチャ イン ピクチャ(PiP)画面の位置を設定します。この設定は、たとえばタッチ コントローラを使用して、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

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

[現在(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。
[左上隅(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。
[上部中央(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。
[右上隅(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。
[左中央(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。
[右中央(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。
[左下隅(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。
[右下隅(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。

例:
```
Video PIP Presentation DefaultValue Position: Current
```

Video SelfviewPosition

画面上で小さいセルフビューの PiP(Picture in Picture)を表示する位置を選択します。
この設定は Video SelfviewDefault PIPPosition 設定によって廃止されました。

必要なユーザ ロール: ADMIN

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

[左上隅(UpperLeft)]:セルフビュー PiP が画面の左上隅に表示されます。
[上部中央(UpperCenter)]:セルフビュー PiP が画面の上部中央に表示されます。
[右上隅(UpperRight)]:セルフビュー PiP が画面の右上隅に表示されます。
[左中央(CenterLeft)]:セルフビュー PiP が画面の左中央に表示されます。
[右中央(CenterRight)]:セルフビュー PiP が画面の右中央に表示されます
[左下隅(LowerLeft)]:セルフビュー PiP が画面の左下隅に表示されます。
[右下隅(LowerRight)]:セルフビュー PiP が画面の右下隅に表示されます。

例:
```
Video SelfviewPosition: CenterRight
```

Video SelfviewDefault Mode

メイン ビデオ ソース(セルフビュー)をコールの後に画面に表示するかどうかを指定します。セルフビュー ウィンドウの位置とサイズはそれぞれ、Video SelfviewDefault PIPPosition 設定および Video SelfviewDefault FullscreenMode 設定によって決定されます。

必要なユーザ ロール: ADMIN

値スペース: <Off/Current/On>

[オフ(Off)]:セルフビューはコール退出時にオフにされます。
[現在(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。
[オン(On)]:セルフビューはコール退出時にオンにされます。

例:
```
Video SelfviewDefault Mode: Current
```

Video SelfviewDefault 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)画面で表示するかを設定します。この設定はセルフビューがオンである場合にのみ有効です(Video SelfviewDefault Mode 設定を参照)。

必要なユーザ ロール: ADMIN

値スペース: <Off/Current/On>

[オフ(Off)]: セルフビューは PiP として表示されます。

[現在(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。

[オン(On)]: セルフビューの画像は全画面表示されます。

例: `Video SelfviewDefault FullscreenMode: Current`

Video SelfviewDefault PIPPosition

コール終了後のセルフビューの小さいピクチャ イン ピクチャ(PiP)画面の位置を設定します。この設定はセルフビューがオンであり(Video SelfviewDefault Mode 設定を参照)、フルスクリーン ビューがオフである場合(Video SelfviewDefault FullscreenMode 設定を参照)にのみ有効です。

必要なユーザ ロール: ADMIN

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

[現在(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。

[左上隅(UpperLeft)]: セルフビュー PiP が画面の左上隅に表示されます。

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

[右上隅(UpperRight)]: セルフビュー PiP が画面の右上隅に表示されます。

[左中央(CenterLeft)]: セルフビュー PiP が画面の左中央に表示されます。

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

[左下隅(LowerLeft)]: セルフビュー PiP が画面の左下隅に表示されます。

[右下隅(LowerRight)]: セルフビュー PiP が画面の右下隅に表示されます。

例: `Video SelfviewDefault PIPPosition: Current`

Video SelfviewDefault OnMonitorRole

コール終了後にメイン ビデオ ソース(セルフビュー)に表示するモニタ/出力を設定します。

必要なユーザ ロール: ADMIN

値スペース: <First/Second/Current>

[第 1(First)]: セルフビューの画像はメイン画面に表示されます。

[第 2(Second)]: セルフビューの画像はセカンダリ画面に表示されます。

[現在(Current)]: コールを中止すると、セルフビュー画像がコール中と同じ画面上に保持されます。

例: `Video SelfviewDefault OnMonitorRole: Current`

Video Monitors

モニタ レイアウト モードを設定します。

必要なユーザ ロール: ADMIN

値スペース: <Auto/DualPresentationOnly>

[自動(Auto)]: 2 番目のモニタが接続されている場合には、レイアウトは 2 台のモニタに分散されます。それ以外の場合は、すべてがメイン モニタに表示されます。

[デュアル プレゼンテーションのみ(DualPresentationOnly)]: 最初のモニタにはコールのすべての参加者が、2 番目のモニタにはプレゼンテーション(存在する場合)が表示されます。

例: `Video Monitors: Auto`

Video OSD LanguageSelection

これは、UserInterface OSD LanguageSelection 設定に変更されました。

Video OSD EncryptionIndicator

これは、UserInterface OSD EncryptionIndicator 設定に変更されました。

Video OSD Output

これは UserInterface OSD Output 設定に変更されました。

Video OSD LoginRequired

これは、UserInterface OSD LoginRequired 設定に変更されました。

Video Output Connector [1] Brightness

ビデオ システムの LCD 画面の明るさレベルを設定します。デフォルト値は 50 です。

必要なユーザ ロール: USER

値スペース: <0..100>

範囲: 値は 0 ～ 100 である必要があります。

例: `Video Output Connector 1 Brightness: 80`

Video Output Connector [1] Whitebalance Level

LCD ディスプレイの色温度（ホワイト バランス）は、4000 K（暖色）～ 9000 K（寒色）で調整できます。デフォルト値は 6500 K です。

必要なユーザ ロール: USER

値スペース: <4000..9000>

範囲: 値は 4000 ～ 9000 である必要があります。

例: `Video Output Connector 1 Whitebalance Level: 6500`

Video Output Connector [2] CEC Mode

ビデオ出力（HDMI）は、Consumer Electronics Control（CEC）をサポートします。この設定が [オン（On）] の場合（デフォルトは [オフ（Off）]）、システムはシステム自体がスタンバイに移行する際にモニタをスタンバイ状態に設定するために CEC を使用します。同様に、システムがスタンバイから復帰するとき、システム自身がモニタを起動します。HDMI 出力に接続されているモニタには CEC との互換性があり、このように動作するためにはモニタで CEC が設定されている必要があります。

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

必要なユーザ ロール: ADMIN

値スペース: <Off/On>

[オフ（Off）]：CEC 制御をディセーブルにします。

[オン（On）]：CEC 制御をイネーブルにします。

例: `Video Output Connector 2 CEC Mode: Off`

Video Output Connector [2] OverscanLevel

モニタによっては、受信する画像全体を表示できない可能性があります。これはモニタに表示したときに、システム ビデオ出力から送信される画像の外側部分がカットされることを意味します。

ビデオ システムに使用可能なフレームの外側部分を使用しないこと、つまりモニタに表示されない可能性がある部分は使用しないことを指示するには、この設定を使用します。この場合、画面上のビデオとメッセージの両方が拡大縮小されます。

必要なユーザ ロール: ADMIN

値スペース: <None/Medium/High>

[なし（None）]：システムは出力解像度すべてを使用します。

[中（Medium）]：システムは出力解像度の外側 3 % を使用しません。

[高（High）]：システムは出力解像度の外側 6 % を使用しません。

例: `Video Output Connector 2 OverscanLevel: None`

Video Output Connector [2] Location HorizontalOffset

HorizontalOffset 設定および VerticalOffset 設定は、各ビデオ出力に関連付けられています。これらの設定は、これらの出力に接続されているディスプレイの相対的な位置を信号で送信するために使用されます。内蔵 LCD ディスプレイは HorizontalOffset = 0 および VerticalOffset = 0 です（暗黙の設定であり、設定不可能です）。

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

例：一つは中央、もうひとつはその左にある 2 台のディスプレイがあるとします。ここでは次の設定が適用されます。中央のディスプレイは HorizontalOffset = 0、左側のディスプレイは HorizontalOffset = -1 となります。

例：一つは中央、もうひとつはその下にある 2 台のディスプレイがあるとします。ここでは次の設定が適用されます。中央のディスプレイは VerticalOffset = 0、下側のディスプレイは Vertical Offset = -1 となります。

各出力のデフォルト値は次の通りです。

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

必要なユーザ ロール: ADMIN

値スペース: <-100..100>

範囲: 値は -100 ～ 100 である必要があります。

例: `Video Output Connector 2 Location HorizontalOffset: 1`

Video Output Connector [2] Location VerticalOffset

HorizontalOffset 設定および VerticalOffset 設定は、各ビデオ出力に関連付けられています。これらの設定は、これらの出力に接続されているディスプレイの相対的な位置を信号で送信するために使用されます。内蔵 LCD ディスプレイは HorizontalOffset = 0 および VerticalOffset = 0 です（暗黙の設定であり、設定不可能です）。

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

例：一つは中央、もうひとつはその左にある 2 台のディスプレイがあるとします。ここでは次の設定が適用されます。中央のディスプレイは HorizontalOffset = 0、左側のディスプレイは HorizontalOffset = -1 となります。

例：一つは中央、もうひとつはその下にある 2 台のディスプレイがあるとします。ここでは次の設定が適用されます。中央のディスプレイは VerticalOffset = 0、下側のディスプレイは Vertical Offset = -1 となります。

各出力のデフォルト値は次の通りです。

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

必要なユーザ ロール： ADMIN

値スペース： <-100..100>

範囲: 値は -100 ～ 100 である必要があります。

例：
```
Video Output Connector 2 Location Vertical Offset: 0
```

Video Output Connector [2] RGBQuantizatonRange

HDMI 出力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していないため、ディスプレイの完全なイメージを取得するためにこの設定を使用して設定を上書きすることができます。ほとんどの HDMI ディスプレイは完全な量子化範囲を予期するため、デフォルト値は [フル（Full）] に設定されます。

必要なユーザ ロール： ADMIN

値スペース： <Auto/Full/Limited>

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

[フル（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。

[制限（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。

例：
```
Video Output Connector 2 RGBQuantizatonRange: Full
```

Video Output Connector [1..2] Resolution

[コネクタ 1（Connector 1）]（統合型LCDディスプレイ）：この値は固定されており、変更できません。

[コネクタ 2（Connector 2）]：ビデオ システムの HDMI 出力に接続されたモニタの解像度とリフレッシュレートを設定します。

必要なユーザ ロール： ADMIN

値スペース： コネクタ 1：<1920_1080_60> コネクタ 2：<Auto/1024_768_60/1280_1024_60/1280_720_50/1280_720_60/1920_1080_50/1920_1080_60/1280_768_60/1360_768_60/1366_768_60>

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

1024_768_60: 解像度は 1024 x 768、更新間隔は 60 Hz です。

1280_1024_60: 解像度は 1280 x 1024、更新間隔は 60 Hz です。

1280_720_50: 解像度は 1280 x 720、更新間隔は 50 Hz です。

1280_720_60: 解像度は 1280 x 720、更新間隔は 60 Hz です。

1920_1080_50: 解像度は 1920 x 1080、更新間隔は 50 Hz です。

1920_1080_60: 解像度は 1920 x 1080、更新間隔は 60 Hz です。

1280_768_60: 解像度は 1280 x 768、更新間隔は 60 Hz です。

1360_768_60: 解像度は 1360 x 768、更新間隔は 60 Hz です。

1366_768_60: 解像度は 1366 x 768、更新間隔は 60 Hz です。

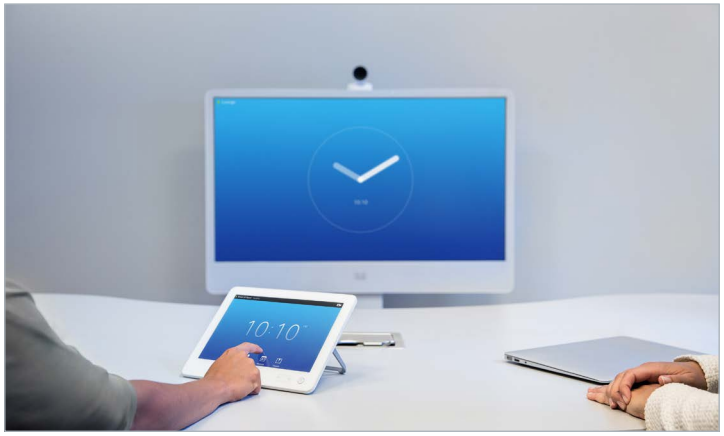
例：
```
Video Output Connector 2 Resolution: Auto
```

Video WallPaper

これは、UserInterface Wallpaper に変更されました。

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。



第 4 章

パスワードの設定

システム パスワードの設定

システム パスワードは、ビデオ システムを保護します。Web インターフェイスを利用する場合や、タッチ 10 ユーザ インターフェイスから [管理者 (Administrator)] 設定へアクセスする場合は、サインインする必要があります。

admin ユーザ

ビデオ システムは完全な資格情報を持つデフォルトのユーザ アカウントに提供されます。ユーザ名は *admin* であり、初期状態ではデフォルト ユーザにパスワード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、*admin* ユーザにパスワードを設定する必要があります。同様の認証情報持つ他のユーザ用のパスワードも設定します。

パスワードをメモし、安全な場所に保管してください。パスワードを忘れた場合は、ユニットを工場出荷時設定にリセットする必要があります。

admin ユーザのパスワードが設定されるまで、システム パスワードが設定されていないことを示す警告が表示されます。

他のユーザ アカウント

ビデオ システムに任意の数のユーザ アカウントを作成できます。

ユーザ アカウントの作成と管理の方法に関する詳細情報は、「ユーザ管理」の項で確認できます。

システム パスワードの変更

システム パスワードを変更するには、次の手順に従います。

パスワードが現在設定されていない場合は、[現在のパスワード (Current password)] を空白の状態で使用します。パスワードを削除するには、[新しいパスワード (New password)] フィールドを空白のままにします。

1. ユーザ名と現在のパスワードを使用して Web インターフェイスにサインインします。
2. 右上隅のユーザ名をクリックして、ドロップダウン メニューの [パスワード変更 (Change password)] を選択します。
3. [現在のパスワード (Current password)] と [新しいパスワード (New password)] の入力フィールドにそれぞれパスワードを入力後、新しいパスワードを再入力します。

   パスワードの形式は、0 ～ 64 文字の文字列です。
4. [パスワード変更 (Change Password)] をクリックします。

他のユーザのシステム パスワードの変更

管理者権限を持っている場合は、次の手順を実行して、すべてのユーザのパスワードを変更することができます。

1. ユーザ名とパスワードを使用して Web インターフェイスにサインインします。
2. [設定 (Configuration)] タブに移動し、[ユーザ管理 (User Administration)] を選択します。
3. 対象のユーザをリストから選択します。
4. 新しいパスワードと PIN コードを入力します。
5. [保存 (Save)] をクリックします。

付録

タッチ 10 ユーザ インターフェイスの接続 (1/2 ページ)

タッチ 10 ユーザ インターフェイスは、MX200 G2 または MX300 G2 ビデオ システムに直接接続するか (このページの説明を参照)、またはネットワーク (LAN) 経由でビデオ システムとペアリングします (次のページの説明を参照)。後者はリモート ペアリングと呼ばれます。

この章の手順は、すべての MX200 G2 および MX300 G2 ビデオ システムに適用されます。

ビデオ システムへのタッチ 10 の直接接続

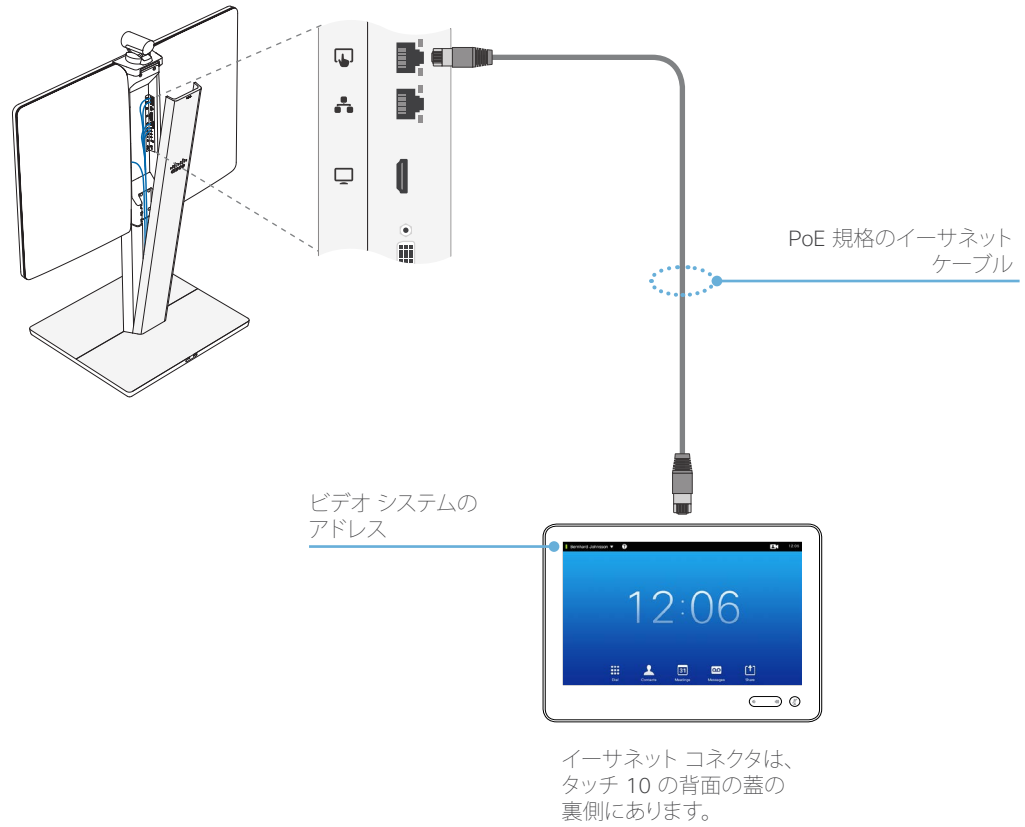
図のように、タッチ 10 をビデオ システムの PoE インジェクタに接続します。

タッチ 10 の設定

タッチ 10 が接続されると、設定手順が始まります。画面に表示される指示に従います。

タッチ 10 にソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがビデオ システムからダウンロードされ、自動的にユニットにインストールされます。アップグレード後にタッチ 10 が再起動します。

ビデオ システムのアドレスが上部バナーに表示されているかチェックすれば、タッチ 10 がビデオ システムに正常に接続されていることを確認できます。



タッチ 10 ユーザ インターフェイスの接続 (2/2 ページ)

ネットワーク(LAN)経由でのタッチ 10 のビデオ システムへの接続

図のように、タッチ 10 とビデオ システムを壁のネットワーク ソケットまたはネットワーク スイッチに接続します。

タッチ 10 の設定

タッチ 10 が電源に接続されると、設定手順が始まります。画面に表示される指示に従います。

[ペアリング対象のコーデックを選択 (Select codec to pair with)] ダイアログが表示されたら、以下に注意してください。

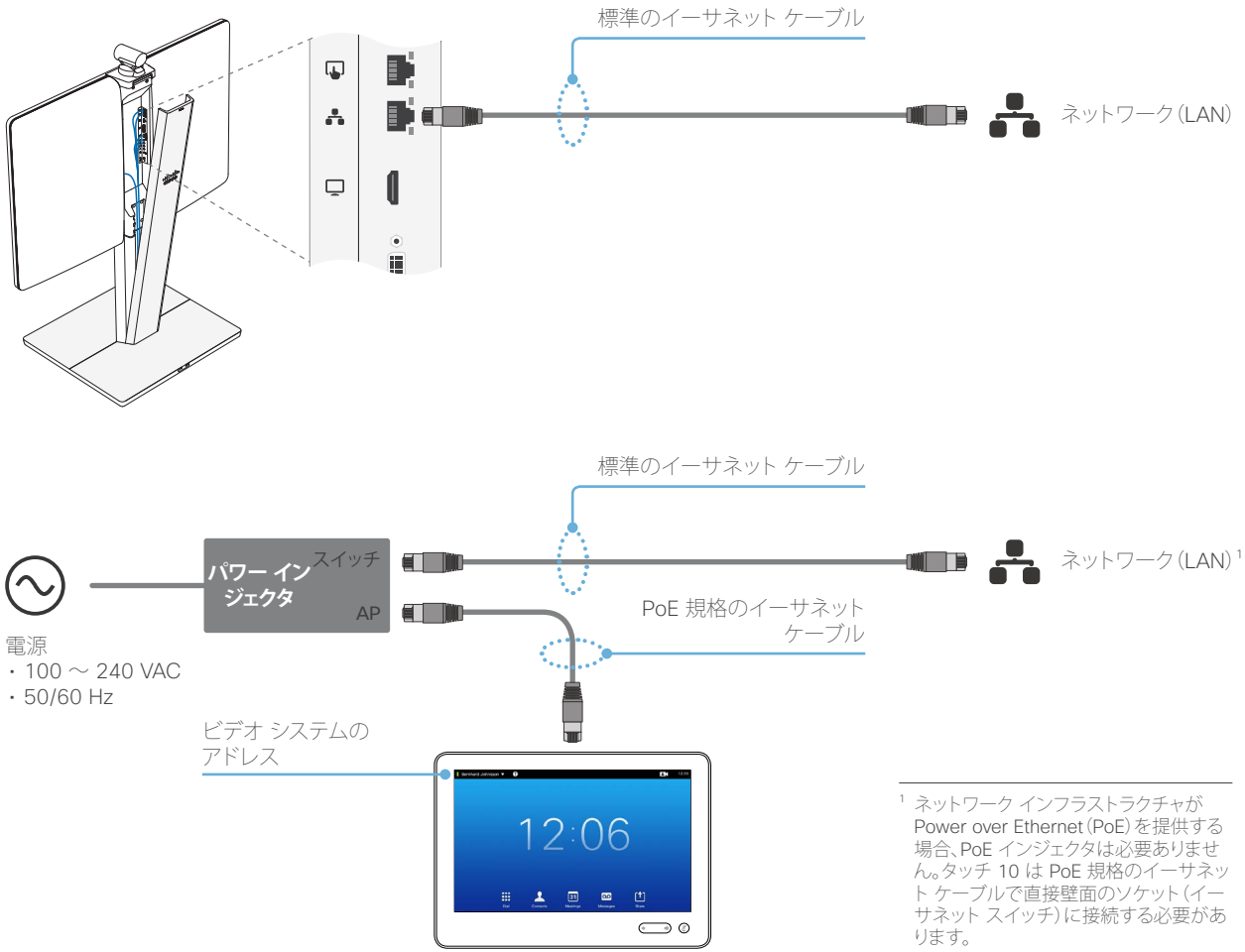
- ペアリング可能なシグナリング中ビデオ システムのリストが、ダイアログに表示されます。ペアリングするシステム名をタップして、続いて[ペアリング開始 (Start Pairing)]をタップします。

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

  - ビデオ システムおよびタッチ 10 が同じサブネット上にある必要があります。
  - ビデオ システムは、直近の 10 分間に再起動されている必要があります。システムがリストに表示されない場合は、再起動してください。
- ビデオ システムが使用可能なコーデックのリストに表示されない場合は、デバイスを手動でペアリングすることができます。[コーデックを手動で選択... (Select codec manually...)] をクリックして、ビデオ システムの IP アドレスまたはホスト名を入力し、[ペアリング開始 (Start Pairing)] をタップします。
- ペアリングを開始するために、ビデオ システムの管理者のユーザ名およびパスワードを入力する必要があります。

タッチ 10 にソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがビデオ システムからダウンロードされ、自動的にユニットにインストールされます。アップグレード後にタッチ 10 が再起動します。

ビデオ システムのアドレスが上部バナーに表示されているかチェックすれば、タッチ 10 がビデオ システムに正常に接続されていることを確認できます。



イーサネット コネクタは、タッチ 10 の背面の蓋の裏側にあります。

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

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

Cisco VCS プロビジョニング

Cisco VCS（Video Communication Server）プロビジョニングを使用する場合、Cisco TMS（TelePresence Management System）に、プロビジョニング可能なすべての設定が含まれているテンプレートをアップロードする必要があります。これは *Cisco TMS プロビジョニング設定テンプレート*と呼ばれます。

このテンプレートには、ビデオ システムの詳細設定がすべて含まれています。[システムユニット名（SystemUnit Name）] と [SIPプロファイル[1..1]URI（SIP Profile [1..1] URI）] を除すべての設定をビデオ システムに自動的にプロビジョニングできます。

設定は、このマニュアルの「システム設定」の章で説明しています。デフォルト値またはサンプル値による例が含まれています。

プロビジョニング設定テンプレートのダウンロード

次の URL からテンプレートをダウンロードできます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/products-release-notes-list.html

各ソフトウェア リリースに、ビデオ システム モデルごとに 1 つのプロビジョニング設定テンプレート ファイル（XML ファイル）があります。該当するファイルをご確認の上、使用してください。

Cisco TMS へのファイルのアップロード方法や、プロビジョニングするパラメータの希望値の設定方法については、『*Cisco TMS Provisioning Deployment Guide*』を参照してください。Cisco TMS で設定しない場合は、デフォルト値が使用されます。

最適鮮明度プロファイル

理想的な光の条件下で、帯域幅（コール レート）の要件を大幅に減らすことができます。

最適鮮明度プロファイルは、会議室の光の状態とビデオ入力（カメラ）の品質に合わせる必要があります。光の状態とビデオ入力が優れていれば、プロファイルも向上します。このとき、良い光の条件で、ビデオ エンコーダは指定のコール レートに一層優れた品質（高解像度またはフレーム レート）を提供します。

一般に、最適鮮明度プロファイルを [標準（Normal）] に設定することが推奨されます。ただし、光の条件が良い場合は、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推奨します。

Web インターフェイスの [システム設定（System Configuration）] に進み、[ビデオ（Video）] > [入力（Input）] > [ソース [1..n]（Source [1..n]）] > [最適化定義（OptimalDefinition）] > [プロファイル（Profile）] に移動して、優先する最適鮮明度プロファイルを選択します。

解像度のしきい値を設定して、60 fps でのビデオ送信を可能にするタイミングを指定できます。このしきい値より低いすべての解像度では、最大送信フレーム レートは 30 fps とします。それより高い解像度では、使用可能な帯域幅が十分であれば 60 fps にすることが可能です。

Web インターフェイスの [システム設定（System Configuration）] に進み、[ビデオ（Video）] > [入力（Input）] > [ソース [1..n]（Source [1..n]）] > [最適化定義（OptimalDefinition）] > [しきい値 60fps（Threshold60fps）] に移動して、しきい値を設定します。

最適鮮明度設定を有効にするには、ビデオ入力の品質設定を [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 [シャープさ（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。

Web インターフェイスの [システム設定（System Configuration）] に進み、[ビデオ（Video）] > [入力（Input）] > [ソース [1..n]（Source [1..n]）] > [品質（Quality）] に移動して、ビデオ品質パラメータを [モーション（Motion）] に設定します。

ビデオ設定についての詳細は、「システム設定」の章を参照してください。

大（High）

通常、ビデオ会議専用の部屋で使用されます。優れた全体的なエクスペリエンスを実現するには、非常に良い光の条件と高品質のビデオ入力が必要です。

理想的な条件下では、帯域幅要件が [標準（Normal）] と比べて最大 50% 削減できます。

中型

通常は、安定した良い光の条件と高品質のビデオ入力を備えた会場で使用されます。

帯域幅要件は [標準（Normal）] と比べて最大 25% 削減できます。

標準

この設定は、室内の光が中程度か不十分であるオフィス環境でよく使用されます。

さまざまな最適鮮明度プロファイル、コール レート、フレーム レートで使用される一般的な解像度

フレーム レート	最適鮮明度プロファイル	コール レート						
		256 kbps	*768 kbps*	*1152 kbps*	*1472 kbps*	*2560 kbps*	*4 Mbps*	*6 Mbps*
30 fps	*標準*	512X288	1024X576	1280X720	1280X720	1920X1080	1920X1080	1920X1080
	中型	640X360	1280X720	1280X720	1280X720	1920X1080	1920X1080	1920X1080
	大（High）	768X448	1280X720	1280X720	1920X1080	1920X1080	1920X1080	1920X1080
60 fps	*標準*	256X144	512X288	768X448	1024X576	1280X720	1280X720	1920X1080
	中型	256X144	768X448	1024X576	1024X576	1280X720	1920X1080	1920X1080
	大（High）	512X288	1024X576	1280X720	1280X720	1920X1080	1920X1080	1920X1080

ClearPath — パケット損失からの復元

ClearPath により、エラーを起こしやすい環境でビデオ システムを使用する場合の経験品質を向上させる、高度なパケット損失復元メカニズムが導入されます。

お使いのビデオ システムで ClearPath を有効にしておくことを推奨します。

(Web インターフェイスで)[システム設定(System Configuration)] に移動します。

- [会議1(Conference 1)] > [パケット損失の復元(PacketLossResilience)] > [モード(Mode)] を選択します。

  ClearPath を無効にするには [オフ(Off)] を選択し、ClearPath を有効にするには [オン(On)] を選択します。

ビデオ システムの初期設定へのリセット

> 工場出荷時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、必ずログ ファイルおよび現在の設定のバックアップを実行してください。Web インターフェイスを開いてログインし、次の手順に従ってください。
>
> - [メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)] に移動し、[バックアップ (Backup)] タブを選択します。
> - [ログのダウンロード (Download Logs)] と [設定のバックアップのダウンロード (Download configuration backup)] をクリックし、手順に従ってファイルをコンピュータに保存します。

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

工場出荷時の状態にリセットする前に、以前に使用していたソフトウェア バージョンに戻すことを必ず検討してください。多くの場合これでシステムをリカバリします。現在および以前のソフトウェア イメージの両方がシステムに存在することに注意してください。ソフトウェアの交換については、「以前に使用していたソフトウェア バージョンへの復元」の項を参照してください。

システムを工場出荷時の状態へリセットするには、タッチ ユーザ インターフェイスまたは Web インターフェイスを使用することを推奨します。これらのインターフェイスが使用できない場合、ビデオ システムのリセット ボタンを使用できます。

ビデオ システムを出荷時の状態にリセットすると、以下のことが行われます。

- 通話履歴が削除されます。
- パスワードがデフォルト値にリセットされます。
- すべてのシステム パラメータがデフォルト値にリセットされます。
- システムにアップロードされていたファイルは、すべて削除されます。これには、カスタム背景、証明書、お気に入りリストを (個人アドレス帳) などがあります。
- 以前の (非アクティブな) ソフトウェア イメージが削除されます。
- オプション キーは影響を**受けません。**

システムはリセット後に自動的に再起動されます。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。

ユーザ インターフェイス:タッチ

1. ユニットがスリープ モードの場合、タッチ スクリーンを静かにタップします。
2. [設定 (Settings)]* メニューを開き、[管理者 (Administrator)] > [(リセット) Reset] に移動します。[管理者 (Administrator)] メニューにアクセスするには、管理者のユーザ名とパスワードでログインしなければなりません。
3. [初期設定へのリセット (Factory Reset)] ボタンをタップします。

   システムが工場出荷時設定へと戻され、自動的に再起動されます。これには数分かかることがあります。

   システムは再起動後、メイン画面に通知を表示して、工場出荷時設定にリセットされたことを確認します。通知は約 10 秒後に非表示になります。

ユーザ インターフェイス:Web

> タッチ ユーザ インターフェイスで [設定 (Settings)]* メニューを開き [システム情報 (System Information)] をタップして、システムの IP アドレス (IPv4 または IPv6) を確認します。

1. 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。
2. [メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)] に移動し、[工場出荷時状態へのリセット (Factory Reset)] タブを選択します。
3. 表示された情報をよく確認してから、[初期設定へのリセット (Perform a factory reset...)] をクリックします。
4. 工場出荷時の状態へのリセットを実行することを確認するために赤い [はい (Yes)] ボタンをクリックします。

   システムが工場出荷時設定へと戻され、自動的に再起動されます。これには数分かかることがあります。

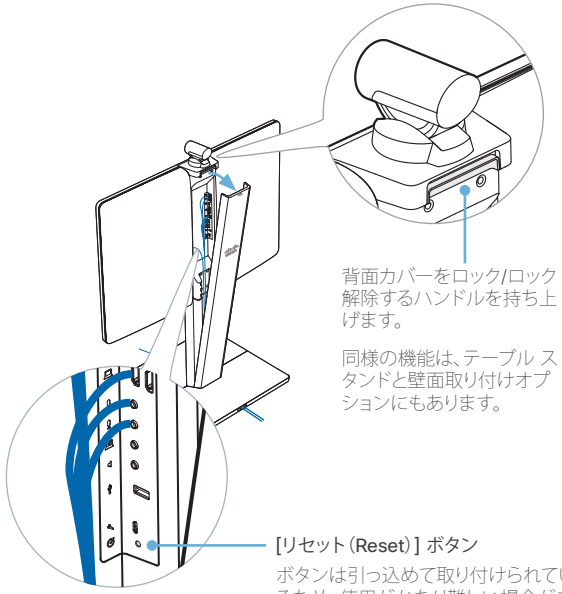
   システムは再起動後、メイン画面に通知を表示して、工場出荷時設定にリセットされたことを確認します。通知は約 10 秒後に非表示になります。

リセット ボタンの使用

1. ビデオ システムのカバーを取り外します。
2. ペン先 (または同等のもの) を使用して、画面が黒くなるまでリセット ボタンを押し続けます (約 10 秒)。その後、ボタンを離します。

   システムが工場出荷時設定へと戻され、自動的に再起動されます。これには数分かかることがあります。

   システムは再起動後、メイン画面に通知を表示して、工場出荷時設定にリセットされたことを確認します。通知は約 10 秒後に非表示になります。



* [設定 (Settings)] メニューは、タッチ ユーザ インターフェイスの左上隅の連絡先情報をタップすると表示されるドロップ ダウン ウィンドウからアクセスできます。

タッチ 10 ユーザ インターフェイスの初期設定へのリセット

エラー状態で、接続を再確立するためにタッチ 10 ユーザ インターフェイスを工場出荷時の状態にリセットする必要がある場合があります。その場合は、必ずシスコのサポート組織に連絡して実行する必要があります。

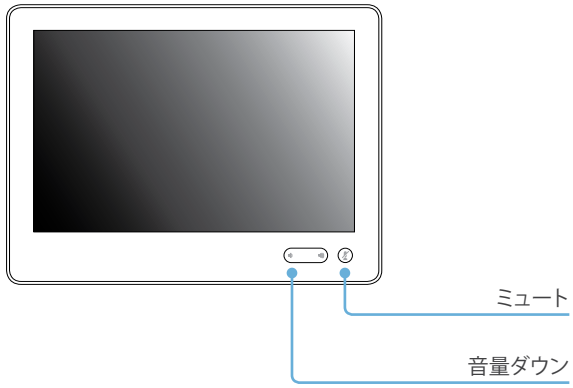
タッチ 10 を工場出荷時にリセットしてペアリング情報が失われると、(ビデオ システムではなく) タッチ自体が工場出荷時のデフォルトに戻されます。

タッチ 10 はリセット後に再起動し、ビデオ システムから新しい設定を自動的に受信します。

工場出荷時設定にリセットすると、元に戻すことはできません。

タッチ 10 の初期設定へのリセット

1. *ミュート*および*音量小*ボタンを見つけます。



2. (赤と緑が) 点滅しはじめるまで、*ミュート* ボタンを押します。約 10 ～ 15 秒かかります。
3. *音量小*ボタンを 2 回押します。

   タッチ 10 が工場出荷時設定へと自動的に戻され、再起動されます。

技術仕様

製品仕様

製品互換性

標準準拠テレプレゼンスおよびビデオ システムとの完全互換性

ソフトウェアの互換性

MX200 G2:

- Cisco TelePresence ソフトウェア バージョン TC7.1 以降

MX300 G2:

- Cisco TelePresence ソフトウェア バージョン TC7.0 以降

コンポーネント

以下を含む完全統合装置:

- コーデック
- Display
- カメラ
- 統合マイクおよびスピーカー

Cisco TelePresence Table Microphone 20
(システムには 2 つのマイクが付属)

ケーブル:DVI-to-VGA ケーブル、ミニ ジャック(3.5 mm) オーディオ ケーブル、LAN ケーブル、電源ケーブル

Display

MX200 G2:

- LCD モニタ:42"
- 解像度:1920 X 1080(16:9)
- コントラスト比:通常 1300:1
- 視野角:±178°
- 応答時間:通常 8 ミリ秒
- 輝度:通常 450 cd/m^2

MX300 G2:

- LCD モニタ:55"
- 解像度:1920 X 1080(16:9)
- コントラスト比:通常 4000:1
- 視野角:±178°
- 応答時間:通常 8 ミリ秒
- 輝度:通常 450 cd/m^2

PC および 2 番目のソース ビデオ入力

DVI-I

HDMI X 2

対応 PC 入力解像度

SVGA(800 X 600)～ 1080p(1920 X 1080)

カメラの概要

MX200 G2:

- 2.5 倍光学ズーム(デジタル ズームを含めると 5 倍)
- 電動式チルト +5°/-25°、パン ±30°
- 水平視野角 83°
- 垂直視野角 51.5°
- 解像度:1080p60 および 720p60
- F 2.0
- 自動または手動フォーカス、輝度およびホワイト バランス
- 遠端カメラ制御
- 焦点距離:0.3 m(0.98 ft)～無限遠

MX300 G2:

- 4 倍光学ズーム(デジタル ズームを含めると 8 倍)
- 電動式チルト +15°/-25°、パン ±90°
- 水平視野角 72°
- 垂直視野角 43.5°
- 解像度:1080p60 および 720p60
- F 1.7
- 自動または手動フォーカス、輝度およびホワイト バランス
- 遠端カメラ制御
- 焦点距離:0.3 m(0.98 ft)～無限遠

オーディオ システム

- 内蔵フルレンジ スピーカーおよびベース スピーカー
- 内蔵フルレンジ マイクロフォン
- 2 台の Cisco TelePresence Table Microphone 20 のサポート
- ミニ ジャック オーディオ入力(例:PC 用)
- ミニ ジャック オーディオ出力

ユーザ インターフェイス

Cisco TelePresence Touch 10

- 10 インチ投影型タッチ スクリーン
- 解像度:1280 x 800

言語サポート

- 英語、アラビア語、カタロニア語、チェコ語、デンマーク語、オランダ語、フィンランド語、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、ポルトガル語(ブラジル)、中国語(簡体字)、スペイン語、ロシア語、スウェーデン語、中国語(繁体字)、トルコ語、ロシア語(ソフトウェア バージョンによって異なります)

電源

- 自動検知電源
- 100 ～ 240 VAC、50 ～ 60 Hz
- 定格:最大 300 W
- 消費電力:最大標準構成で 235 W

温度範囲

動作温度および湿度:

- 周囲温度:0 ～ 35°C(32 ～ 95°F)
- 相対湿度(RH):10 ～ 90%
- RH 10 ～ 90 %(結露しないこと)時の保管および輸送温度:-20 ～ 60 °C(-4 ～ 140 °F)

物理寸法

フロア スタンド付き MX200:
高さ:1397 mm(55 インチ)
幅:995 mm(39.2 インチ)
奥行:602 mm(23.7 インチ)
重量:37 kg(109 ポンド)

テーブル スタンド付き MX200:
高さ:781 mm(30.7 インチ)
幅:995 mm(39.2 インチ)
奥行:259 mm(10.2 インチ)
重量:26 kg(57 ポンド)

壁面取り付けの MX200:
高さ:671 mm(26.4 インチ)
幅:995 mm(39.2 インチ)
奥行:146 mm(5.7 インチ)
重量:26 kg(57 ポンド)

ホイール ベース付き MX200:
高さ:1480 mm(58.3 インチ)
幅:995 mm(39.2 インチ)
奥行:711 mm(28.0 インチ)
重量:34 kg(73 ポンド)

フロア スタンド付き MX300:
高さ:1521 mm(59.9 インチ)
幅:1278 mm(50.4 インチ)
奥行:671 mm(26.5 インチ)
重量:53 kg(117 ポンド)

壁面取り付けの MX300:
高さ:948 mm(37.4 インチ)
幅:1278 mm(50.4 インチ)
奥行:200 mm(7.9 インチ)
重量:40 kg(88 ポンド)

ホイール ベース付き MX300:
高さ:1606 mm(63.3 インチ)
幅:1278 mm(50.4 インチ)
奥行:755 mm(29.8 インチ)
重量:47 kg(104 ポンド)

認定および適合規格

EU/EEC

- 指令 2006/95/EC（低電圧指令）
  - **規格 EN 60950-1**
- 指令 2004/108/EC（EMC 指令）
  - **規格 EN 55022、クラス A**
  - **規格 EN 55024**
  - **規格 EN 61000-3-2/-3-3**
- 指令 2011/65/EU（RoHS）

警告：本製品はクラス A 製品です。国内環境で本製品を使用すると、電波障害を引き起こす可能性があります。その場合には、ユーザが十分な対策を講じるように求められることがあります。

USA

- UL 60950-1 認証取得
- FCC15B クラス A に準拠

注：この機器は、FCC 規定の Part 15 に基づくクラス A デジタル デバイスの制限に準拠していることがテストによって確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

カナダ

- CAN/CSA C22.2 No. 60950-1-07 認証取得
- このクラス A デジタル装置は、カナダの ICES-003 に準拠
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

ビデオおよび音声の仕様

Bandwidth

- 最大 6 Mbps ポイントツーポイントの H.323 および SIP

解像度とフレーム レートの最小帯域幅

- 768 kbps から 720p30
- 1152 kbps から 720p60
- 1472 kbps から 1080p30
- 2560 kbps から 1080p60

ビデオ標準

- H.263
- H.263+
- H.264

ビデオ機能

- ワイドスクリーン：16:9
- 高度な画面レイアウト
- インテリジェント ビデオ管理
- ローカル自動レイアウト

ビデオ入力（3 系統）

HDMI × 2、DVI-I × 1（アナログおよびデジタル）入力。

サポート対象の形式：最大 1920X1080@60fps（HD1080p60）、以下を含む

- 640 × 480
- 720 × 480
- 720 × 576
- 800 × 600
- 848 × 480
- 1024 × 768
- 1152 × 864
- 1280 × 720
- 1280 × 768
- 1280 × 800
- 1280 × 960
- 1280 × 1024
- 1360 × 768
- 1366 × 768
- 1400 × 1050
- 1440 × 900
- 1680 × 1050
- 1920 × 1080

Extended Display Identification Data（EDID）

ビデオ出力（1 系統）

HDMI 1 出力。

サポート対象の形式：最大 1920 × 1080@60fps（1080p60）、以下を含む

- 1280 × 720（720p）
- 1280 × 768（WXGA）
- 1360 × 768（WXGA）
- 1366 × 768（WXGA）
- 1920 × 1080（(1080p）

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）

次のような最大 1920× 1080@60fps（HD1080p60）までのエンコードまたはデコード ビデオ フォーマットをサポート

- 176 × 144 @ 30 fps（QCIF）（デコードのみ）
- 352 × 288 @ 30 fps（CIF）
- 512 × 288 @ 30 fps（w288p）
- 576 × 448 @ 30 fps（448p）
- 640 × 480 @ 30 fps（VGA）
- 704 × 576 @ 30 fps（4CIF）
- 768 × 448 @ 30 fps（w448p）
- 800 × 600 @ 30 fps（SVGA）
- 1024 × 576 @ 30 fps (w576p)
- 1024 × 768 @ 30 fps (XGA)
- 1280 × 720 @ 30 fps (720p30)
- 1280 × 768 @ 30 fps (WXGA)
- 1280 × 1024 @ 30 fps (SXGA)
- 1440 × 900 @ 30 fps (WXGA+)*
- 1600 × 1200 @ 30 fps (UXGA)*
- 1680 × 1050 @ 30 fps (WSXGA+)*
- 1920 × 1080 @ 30 fps (1080p30)*
- 512 × 288 @ 60 fps (w288p60)*
- 768 × 448@60 fps（w448p60）
- 1024 × 576@60 fps（w576p60）
- 1280 × 720@60 fps (720p60)
- 1920 × 1080 @ 60 fps（HD1080p）

* プレミアム解像度オプションが必要

音声機能

- ハイクオリティ 20 kHz オーディオ
- 音響エコー キャンセラ × 3
- 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

音声標準

- 64 および 128 kbps AAC-LD
- G.722
- G.722.1
- G.711
- G.728
- G.729AB

デュアル ストリーム

- H.239（H.323）デュアル ストリーム
- Binary Floor Control Protocol（BFCP）デュアル ストリーム（SIP）
- 最大 1080p（1920 × 1080）解像度をサポート

マルチポイント サポート

- 4 画面分割の内蔵 SIP/H.323 マルチポイント サポート、MultiSite を参照してください
- Cisco TelePresence Multiway のサポート（Cisco TelePresence Video Communication Server [Cisco VCS] および Cisco TelePresence Multipoint Control Unit（MCU）が必要）
- Cisco TelePresence Multipoint Switch（CTMS）でホストされたマルチポイント会議にネイティブで参加する機能

MultiSite 機能（内蔵マルチポイント）

- 適応型 SIP/H-323 MultiSite
- 3 方向解像度（最大 720p30）
- 4 方向解像度（最大 576p30）
- 完全個別音声および映像トランスコーディング
- マルチサイト連続表示での個別レイアウト
- 同一会議で H.323、SIP、Voice over IP (VoIP) の混在可能
- 最大 1080p30/SXGA の解像度で、任意の参加者からのプレゼンテーション（H.239/BFCP）をサポート
- ベスト インプレッション機能（自動連続表示レイアウト）
- 任意のサイトからの H.264、暗号化、およびデュアル ストリーム
- IP ダウンスピード機能
- ダイヤル インとダイヤル アウト
- 会議レート最大 6 Mbps

ネットワーク、セキュリティ、管理仕様

プロトコル

- H.323
- SIP

ネットワーク インターフェイス

- LAN 用：LAN/イーサネット（RJ-45）X 1、10/100/1000 Mbps

その他のインターフェイス

- メンテナンス用 Micro USB

IP ネットワーク機能

- サービス設定を行うためのドメイン ネーム システム（DNS）のルックアップ
- ディファレンシエーテッド サービス（Quality of Service（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
- ネットワーク タイム プロトコル（NTP）による日付および時刻のサポート
- パケット損失時のダウンスピード機能
- DNS ベースの URI ダイヤリング
- TCP/IP
- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
- IEEE 802.1x ネットワーク認証
- IEEE 802.1Q VLAN
- IEEE 802.1p QoS およびサービス クラス
- シスコ ClearPath
- Medianet：Mediatrace とメタデータ

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（IPv4 および IPv6）
- DHCP、SSH、HTTP、HTTPS、DNS、DiffServ に対するデュアル スタック（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

ファイアウォール トラバーサル

- Cisco TelePresence Expressway テクノロジー
- H.460.18 および H.460.19 ファイアウォール トラバーサル
- SIP ICE（Interactive Connectivity Establishment）

組み込み暗号化

- H.323 および SIP ポイントツーポイント
- 規格準拠：H.235v3 および Advanced Encryption Standard（AES）
- キーの自動生成と交換
- デュアル ストリームのサポート

セキュリティ機能

- セキュア HTTP（HTTPS）およびセキュア シェル（SSH）プロトコルによる管理
- 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

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）
- Cisco WebEx TelePresence

システム管理

- Cisco TelePresence Management Suite（Cisco TMS）のサポート
- 内蔵 Simple Network Management Protocol（SNMP）、Telnet、SSH、XML、および Simple Object Access Protocol（SOAP）によるトータル管理
- リモート ソフトウェア アップロード：Web サーバ、HTTP、および HTTPS を使用

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
- Lightweight Directory Access Protocol（LDAP）および H.350 をサポートするサーバ ディレクトリのエントリ無制限
- 社内ディレクトリ数無制限（Cisco TelePresence Management Suite で使用可能）
- ローカル ディレクトリ：200 件の番号
- 受信コールの日付と時刻
- 発信コールの日付と時刻
- 不在着信の日付と時刻

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。

サポートされる最新の RFC および草案

- RFC 2190『RTP Payload Format for H.263 Video Streams』
- RFC 2460『Internet protocol, version 6 (IPv6) specification』
- RFC 2617『Digest Authentication』
- RFC 2782『DNS RR for specifying the location of services (DNS SRV)』
- RFC 2976『The SIP INFO Method』
- RFC 3016『RTP Payload Format for MPEG-4 Audio/Visual Streams』
- RFC 3261 SIP：セッション開始プロトコル
- RFC 3262『Reliability of Provisional Responses in SIP』
- RFC 3263『Locating SIP Servers』
- RFC 3264『An Offer/Answer Model with SDP』
- RFC 3311『UPDATE method』
- RFC 3361『DHCP Option for SIP Servers』
- RFC 3388『Grouping of Media Lines in the Session Description Protocol (SDP)』
- RFC 3420『Internet Media Type message/sipfrag』
- RFC 3515『Refer method』
- RFC 3550『RTP: A Transport Protocol for Real-Time Applications』
- RFC 3551『RTP Profile for Audio and Video Conferences with Minimal Control』
- RFC 3581『Symmetric Response Routing』
- RFC 3605『RTCP attribute in SDP』
- RFC 3711『The Secure Real-time Transport Protocol (SRTP)』
- RFC 3840『Indicating User Agent Capabilities in SIP』
- RFC 3890『A Transport Independent Bandwidth Modifier for SDP』
- RFC 3891『The SIP "Replaces" Header』
- RFC 3892『Referred-By Mechanism』
- RFC 3960『Early Media』
- RFC 3986『Uniform Resource Identifier (URI): Generic Syntax』
- RFC 4028『Session Timers in SIP』
- 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 4145『TCP-Based Media Transport in the SDP』
- RFC 4235『An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)』
- RFC 4566『SDP: Session Description Protocol』
- RFC 4568『SDP:Security Descriptions for Media Streams』
- RFC 4574『The Session Description Protocol (SDP) Label Attribute』
- 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 4583『Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams』

  draft-ietf-bfcpbis-rfc4583bis-00『Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams』
- RFC 4585『Extended RTP Profile for RTCP-Based Feedback』
- RFC 4587『RTP Payload Format for H.261 Video Streams』
- RFC 4629『RTP Payload Format for ITU-T Rec.H.263 Video』
- RFC 4733『RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals』
- RFC 4796『The SDP Content Attribute』
- RFC 4862『IPv6 stateless address autoconfiguration』
- RFC 5104『Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)』
- RFC 5168『XML Schema for Media Control』
- 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 5389『Session Traversal Utilities for NAT (STUN)』
- RFC 5577『RTP Payload Format for ITU-T Recommendation G.722.1』
- RFC 5589『SIP Call Control Transfer』
- RFC 5626『Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)』
- RFC 5766『Traversal Using Relays around NAT (TURN)』：Session Traversal Utilities for NAT（STUN）のためのリレー拡張
- RFC 5768『Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)』
- RFC 5905『Network Time Protocol Version 4: Protocol and Algorithms Specification』
- RFC 6156『Traversal Using Relays around NAT (TURN) Extension for IPv6』
- RFC 6184『RTP Payload Format for H.264 Video』
- RFC 6185『RTP Payload Format for H.264 Reduced-Complexity Decoding Operation (RCDO)』

シスコ Web サイト内のユーザ ドキュメンテーション

一般に、Cisco TelePresence 製品のユーザ マニュアルはこのサイトから入手できます。

http://www.cisco.com/go/telepresence/docs

お使いの製品が見つかるまで、右ペインの製品カテゴリを選択する必要があります。以下の順にパスをたどってください。

[コラボレーション ルーム エンドポイント（Collaboration Room Endpoints）] >

Cisco TelePresence MX シリーズ

また、マニュアルを検索するために次の短いリンクを使用できます。

http://www.cisco.com/go/mx-docs

ドキュメントは、次のカテゴリに編成されます。

インストール ガイド：

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

スタートアップ ガイド：

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

保守と運用 > メンテナンスとオペレーション ガイド

管理者ガイド：

保守と運用 > メンテナンスとオペレーション ガイド

ユーザ ガイドとクイック リファレンス ガイド：

保守と運用 > エンドユーザ ガイド

ナレッジ ベースの記事とよく寄せられる質問（FAQ）：

トラブルシューティングとアラート > トラブルシューティング ガイド

CAD 図面：

リファレンス ガイド > テクニカル リファレンス

ビデオ会議室ガイドライン：

設計 > 設計ガイド

ソフトウェア ライセンス情報：

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

法令準拠および安全上の注意：

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

ソフトウェア リリース ノート：

ソフトウェア ダウンロード、リリースと一般情報 > リリース ノート

知的財産権

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。

URL：http://www.cisco.com/web/siteassets/contacts

Corporate Headquarters:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA