コラボレーション エンドポイント ソフトウェア バージョン 8.3
2017 年 1 月

アドミニストレータ ガイド

Cisco DX70 および DX80

シスコ製品をお選びいただきありがとうございます。

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

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

このアドミニストレータ ガイドの主な目的は、ユーザの目標とニーズに対応することです。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/dx-docs [英語]

本ガイドの使用方法

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

目次

第 1 章

はじめに

ユーザ ドキュメンテーションとソフトウェア

このガイドの対象となる製品

- Cisco TelePresence DX70
- Cisco TelePresence DX80

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

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

このガイドには、Cisco Spark に登録されているシステムに関する情報は記載されていません。Cisco Spark ルーム システムの詳細については、次の URL にアクセスしてください。

▶ https://help.webex.com/community/cisco-cloud-collab-mgmt [英語]

CE ソフトウェアへのソフトウェアの移行

Cisco DX80 と Cisco DX70 は、元々 *Android ベースのソフトウェアとともに販売されていました。CE ソフトウェア*に移行する前に、変換の要件、および *Android ベースのソフトウェア*と比較した機能の変更点を注意深く確認することが重要です。この確認を行わないと、導入環境が機能せず、再度変換して前に戻すことが必要になる可能性があります。

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

ユーザ ドキュメンテーション

このガイドでは、エンドポイントの管理に必要な情報を提供します。エンドポイントの設置方法については*インストール ガイド*を、必要な初期設定については*スタートアップ ガイド*を参照してください。

このエンドポイントに関する詳しいガイドは、付録
▶「シスコ Web サイト内のユーザ ドキュメンテーション」を参照してください。

ユーザ ドキュメンテーションのダウンロード

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

▶ http://www.cisco.com/go/dx-docs [英語]

Cisco Project Workplace

オフィスや会議室をビデオ会議用に整備する際にインスピレーションを得たり、ガイドラインを確認したりするには、次のシスコ Web サイトをご覧ください。

▶ http://www.cisco.com/go/projectworkplace [英語]

ソフトウェア

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

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

次のサイトから、ソフトウェア リリース ノート（CE8）を参照することを推奨します。

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

CE8.3 の新機能

この章では、新しいシステム設定と変更されたシステム設定の概要、およびシスコ コラボレーション エンドポイント ソフトウェア バージョン 8.3（CE8.3）の新機能と改良点について説明します。

詳細については、ソフトウェアのリリース ノートをご覧になることをお勧めします。

► http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html [英語]

CE8.3 の新機能および改良点

Wi-Fi

組み込みの Wi-Fi アダプタ付きで販売されている DX70 と DX80 のビデオ システムは、イーサネットまたは Wi-Fi のいずれかを通じてネットワークに接続できます。

ビデオ システムでは、次の Wi-Fi の規格がサポートされています。

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

オープン ネットワーク（セキュリティで保護されない）に加えて、次のセキュリティ プロトコルがサポートされています。

- WPA-PSK、TKIP、または AES
- WPA2-PSK、AES

ビデオ システムでは、イーサネットと Wi-Fi の両方に同時に接続することはできません。両方に接続した場合、イーサネットが Wi-Fi よりも優先されるため、Wi-Fi を使用するにはイーサネット ケーブルを取り外す必要があります。

コンテンツ シェアリング用のインテリジェント プロキシミティ

CE ソフトウェアを実行する他のビデオ システムに合わせて、DX70 と DX80 で Cisco Proximity がサポートされるようになりました。Cisco Proximity を使用すると、スマートフォン、タブレット、またはラップトップが受信範囲内に入ったときにそれらをビデオ システムに自動的にペアリングできます。この機能はデフォルトでは無効になっていますか、Web インターフェイスまたは xAPI から有効にすることができます。

DX70 と DX80 では、CE ソフトウェアを使用する他のビデオ システムと同じ次の各サービスがサポートされます。

- モバイル クライアントへのコンテンツ シェアリング（プライバシー侵害の懸念から通話中の場合のみ）
- デスクトップ クライアントからのコンテンツ シェアリング
- モバイル クライアントからの基本的なコール制御

Proximity を有効にしたビデオ システムは、1 部屋につき 1 つだけにすることをお勧めします。2 つ以上のシステムで Proximity を有効にすると、ペアリング状態が不安定になるおそれがあります。Proximity の同時接続の最大数は 3 です。

スマートフォンとタブレット（Android と iOS）向け、およびラップトップ（Windows と OS X）向けの Cisco Proximity クライアントは、► http://proximity.cisco.com [英語] からダウンロードできます。また、Google Play（Android）や Apple App Store（iOS）でスマートフォン/タブレット向けのクライアントを入手することもできます。

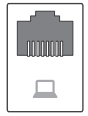
Cisco UCM の機能の追加

CE ソフトウェアを実行する他のビデオ システムですでにサポートされている Cisco UCM の次の複数の機能が有効になります。

- ボイスメール
- 共有回線
- エクステンション モビリティ
- すべてのコールを転送する
- コンサルタティブの追加および転送
  - アクションを完了する前に追加または転送する先の担当者と相談できます。
- 複数のコール（通話）の保留、およびコール（通話）のマージ

コンピュータ ネットワーク ポートに接続されたデバイスの IEEE 802.1x 認証

IEEE 802.1x 認証は、DX70 と DX80 の*コンピュータ ネットワーク* ポートで有効になります。これは、このポートに接続されているデバイスで、このプロトコルを使用して認証できることを意味します。



室内制御

室内制御を使用すると、室内の周辺機器（たとえば照明やブラインドなど）を制御できるように、ビデオ システムのユーザ インターフェイスをカスタマイズできます。室内のビデオ システムと他の周辺機器が同じデバイスから制御されていると、ユーザ エクスペリエンスが一貫したものになります。

最初のリリースでは、グラフィックの解像度が低い場合があります。リリース ノートも参照してください。

室内制御機能のセットアップの詳細については、次のシスコ サイトにあるユーザ ガイドを参照してください。► http://www.cisco.com/go/in-room-control-docs [英語]

追加の入力ソースを持つ外部ビデオ スイッチの制御

シスコのタッチ ユーザ インターフェイスは、サードパーティ製の外部ビデオ スイッチに接続された入力ソースを含めるようにカスタマイズできます。これらの*外部*入力ソースは、ビデオ システムに直接接続されたビデオ ソースのように表示されて動作します。ケーブルを取り替えたり、物理的に入力ソースを手動で変更したりする必要はありません。

作成できる外部入力ソースの数は、ビデオ スイッチで許可されている入力数で決まります。最大で 50 個のソースを推奨します。

ビデオ スイッチは、サードパーティ製の制御システムでサポートされている必要があります。たとえば、Crestron 社製または AMX 社製の制御システムの場合、ビデオ システムの xAPI と通信できます。ビデオ スイッチを制御するのは、ビデオ システムではなく、制御システムです。

ユーザ インターフェイスをカスタマイズする方法、および xAPI を使用してこの機能をセットアップする方法の詳細については、次のシスコ サイトにあるユーザ ガイドを参照してください。► http://www.cisco.com/go/in-room-control-docs [英語]

CMS 2.1 のホストされた会議での ActiveControl

ActiveControl とは、Cisco TelePresence Server のホストされた会議でビデオ システム用にこれまでサポートされてきた SIP のみの機能です。

CE8.3 から、ActiveControl は CMS 2.1 のホストされた会議でもサポートされています。ActiveControl はビデオ システムでデフォルトでは有効になっており、インフラストラクチャでサポートされている限り使用できます（自動ネゴシエーション）。

ActiveControl の新機能

- ビデオ システムがサーバ側からミュートにされると、ミュート インジケータが画面に表示され、マイクのミュート LED が点灯します。
- デフォルトでは、ベスト エフォート型の暗号化が使用されます。
- *自動*レイアウトがデフォルトとして導入されました。*自動*レイアウトに表示されるユーザは、最近の通話中のスピーカーに基づいて決定されます。
- 画面に表示される録音ステータス インジケータ。
- Web インターフェイスの [コール制御（Call Control）] ページから使用できる ActiveControl 機能（たとえば、参加者リスト、参加者のミュート インジケータ、参加者の切断用ボタン）。

xAPI で使用できるメディア チャネルの詳細

メディア チャネルには、進行中の通話の音声、ビデオ、およびデータに関する情報が含まれています。xAPI から、チャネル レート、パケット損失、ジッター、ビデオ フレーム レートなどをモニタできます。

メディア チャネルの詳細を表示するには、xAPI に管理者ユーザとしてログインし、`xStatus MediaChannels` を実行します。また、Web インターフェイスの [ステータス（Status）] ページのメディア チャネルの状態も確認できます。

JSON 形式の HTTP フィードバック

HTTP フィードバックは、XML（eXtensible Markup Language）の代わりに、サードパーティ製のフィードバック インタープリタ用の JSON（JavaScript Object Notation）形式で送信できます。

TMS では、デフォルトでは XML を使用し、JSON でフォーマットされたフィードバックをサポートしません。

設定可能なネットワーク速度

Web インターフェイスまたは xAPI で、イーサネット リンクの速度を設定できます。この速度の設定は、CE ソフトウェアを実行する他のビデオ システムと同じです。

リンク速度の自動ネゴシエーションを行う（デフォルト）か、次の設定を強制するかを選択できます。

- 10 Mbps 半二重
- 10 Mbps 全二重
- 100 Mbps 半二重
- 100 Mbps 全二重
- 1 Gbps 全二重
- ビデオ システムがネットワークとネゴシエートして速度を自動的に設定する場合、通常デフォルト値から変更しないことをお勧めします。

Web インターフェイスで使用できる DTMF トーン用のキーパッド

Web インターフェイスの [コール制御（Call Control）] ページにキーパッドが追加されました。このキーパッドは通話中に使用でき、必要な場合は遠端（相手先）に DTMF トーンを送信するために使用できます。

新しい言語

画面上の表示とユーザ インターフェイスに EnglishUK と SpanishLatin のサポートが追加されました。

CE8.3 でのシステム設定の変更点

新しい構成

Network [1] Speed

NetworkServices WIFI Allowed

NetworkServices WIFI Enabled

Peripherals Profile ControlSystems

Proximity Mode

Proximity Services CallControl

Proximity Services ContentShare FromClients

Proximity Services ContentShare ToClients

Standby AudioMotionDetection

削除された設定

SIP Ice OfferTcpCandidates
試験的設定に移動されました

変更された設定

H323 Encryption KeySize
旧:デフォルト値:Max1024bit
新:デフォルト値:Min1024bit

Logging External Server Port
旧:デフォルト値:0
新:デフォルト値:514

Network [1] *
旧:ユーザ ロール:Admin
新:ユーザ ロール:Admin、User

UserInterface/Language
変更:EnglishUK と SpanishLatin を値スペースに追加

UserInterface OSD Output
旧:1/2/3/Auto
デフォルト値:1
新:Auto
デフォルト値:Auto

Video Monitors
旧:Auto/Dual/DualPresentationOnly/Single
新:Single

Video Selfview Default OnMonitorRole
旧:Current/First/Fourth/Second/Third
デフォルト値:Current
新:First
デフォルト値:First

DX70 および DX80 の概要

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

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

機能とメリット

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

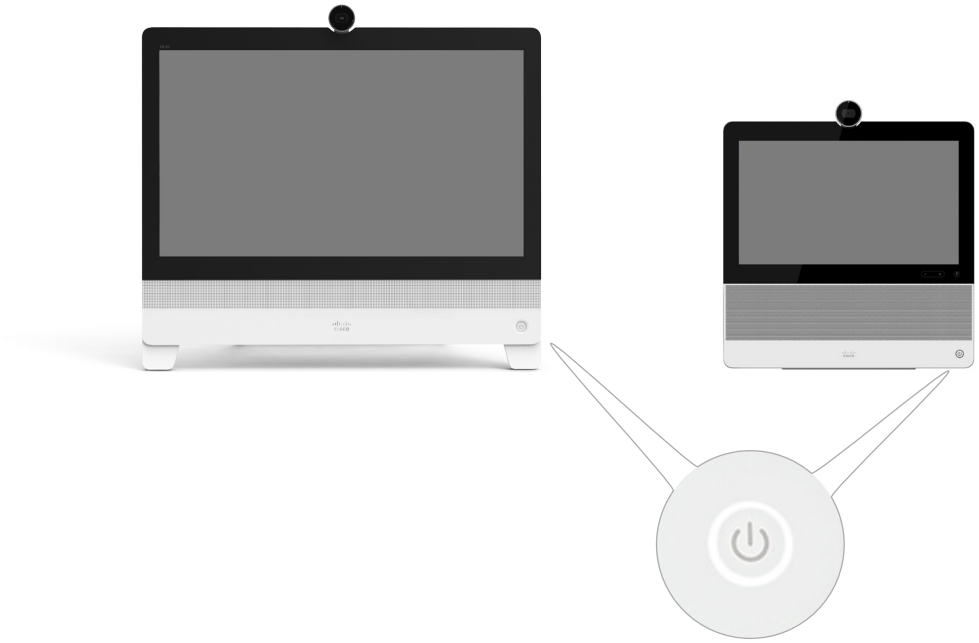
Cisco DX70

Cisco DX80

電源オン/オフ

電源ボタンによる電源のオン/オフ

LED インジケータ付きの電源ボタンが、図に示すように前面にあります。



LED インジケータ付き
電源ボタン

スイッチを入れる

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

ビデオ システムの起動中は LED が点灯しています。

スイッチを切る

電源ボタンを軽く押して消灯するまで押し続けます。

スタンバイ モードの開始/終了

電源ボタンを短く押します。装置がスタンバイ状態になるまでに数秒かかります。

リモートでのシステムの電源オフまたは再起動

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

システムを再起動します。

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

システムが使用可能になるまでに、数分かかります。

システムの電源オフ

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

リモートからシステムの電源を再度オンにすることはできません。

タッチ インターフェイスを使用した再起動とスタンバイ

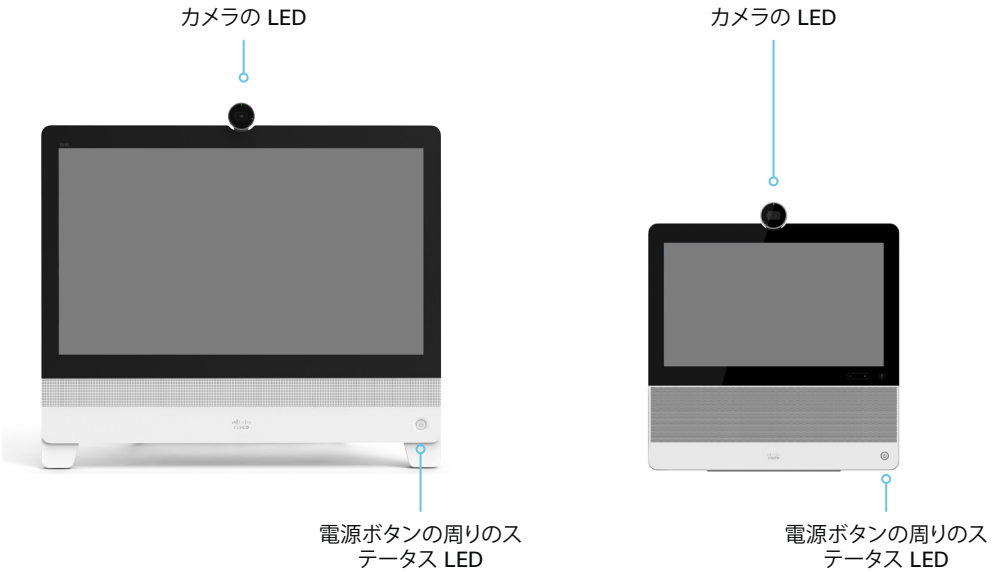
システムを再起動します。

1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [システム情報 (System Information)] > [再起動 (Restart)] を選択します。
3. 再度 [再起動 (Restart)] を選択して、選択を確定します。

スタンバイ モードの開始/終了

1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [スタンバイ (Standby)] を選択します。

LED インジケータ



ステータス LED

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

通常の動作（非スタンバイ状態）：

点灯します。

スタンバイ モード時：

LED がゆっくりと明滅します。

ネットワーク接続なし：

LED が繰り返し 2 回点滅します。

起動（ブート）時：

LED が点滅します。

カメラの LED

カメラの LED はカメラのレンズのすぐ上にあります。

着信コール：

LED が点滅します。

通話中：

点灯します。

ビデオ システムの管理方法 (1/4 ページ)

一般に、ビデオ システムを管理し、保守するには、このアドミニストレータ ガイドに説明されているように、Web インターフェイスを使用することをお勧めします。

または、次のような他の方法により、ビデオ システムの API にアクセスできます。

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

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

ヒント

設定や状態を API で利用できる場合は、Web インターフェイスの設定や状態を、次のように API の設定や状態に変換します。

[X] > [Y] > [Z] を [値 (Value)] (Web) と設定すると、は、以下と同じです。
`xConfiguration X Y Z: Value` (API)

[X] > [Y] > [Z] ステータス (Web) をチェックすると、次の行と同じになります。
`xStatus X Y Z` (API)

次に例を示します。

[SystemUnit] > [名前 (Name)] を [MySystem] と設定すると、
次の行と同じになります。
`xConfiguration SystemUnit Name: MySystem`

[SystemUnit] > [ソフトウェア (Software)] > [バージョン (Version)] ステータスをチェックすると、
次の行と同じになります。
`xStatus SystemUnit Software Version`

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

アクセス方式	注記	アクセス方式を有効または無効にする方法
HTTP/HTTPS	・ビデオ システムの Web インターフェイスで使用されます。 ・非セキュア (HTTP) またはセキュア (HTTPS) 通信 ・HTTP：デフォルトで*有効*です。 HTTPS：デフォルトで*有効*です。	[ネットワーク サービス (NetworkServices)] > [HTTP] > [モード (Mode)] 変更を有効にするには、ビデオ システムを再起動します。
Telnet	・非セキュア TCP/IP 接続 ・デフォルトでは*無効*です。	[ネットワーク サービス (NetworkServices)] > [Telnet] > [モード (Mode)] ビデオ システムを再起動する必要はありません。変更が有効になるまで時間がかかる場合があります。
SSH	・セキュアな TCP/IP 接続 ・デフォルトで [有効 (Enabled)]	[ネットワーク サービス (NetworkServices)] > [SSH] > [モード (Mode)] ビデオ システムを再起動する必要はありません。変更が有効になるまで時間がかかる場合があります。
シリアル インターフェイス (RS-232)	・ケーブルを使ってビデオ システムに接続します。IP アドレス、DNS、またはネットワークは必要ありません。 ・デフォルトで [有効 (Enabled)] ・セキュリティ上の理由から、デフォルトではサインインするよう求められます ([シリアル ポート (SerialPort)] > [ログインが必須 (LoginRequired)])	[シリアル ポート (SerialPort)] > [モード (Mode)] 変更を有効にするには、ビデオ システムを再起動します。

すべてのアクセス方式が無効になっている (Off に設定されている) 場合は、ビデオ システムを設定できません。いずれのアクセス方式も再度有効にする (On に設定する) ことはできないため、復元するにはビデオ システムを工場出荷時設定にリセットする必要があります。

ビデオ システムの管理方法 (2/4 ページ)

ビデオ システムの Web インターフェイス

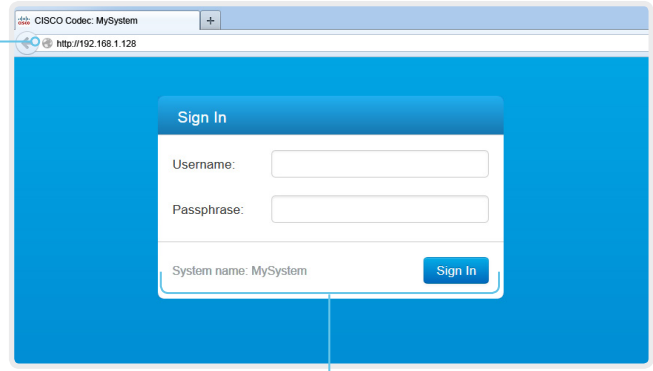
Web インターフェイスは、ビデオ システムの管理ポータルです。コンピュータから接続して、システムをリモートで管理できます。このインターフェイスは、フル設定アクセスを可能にし、メンテナンスのためのツールとメカニズムを提供します。

注:Web インターフェイスでは HTTP または HTTPS が有効である必要があります ([ネットワーク サービス (NetworkServices)] > [HTTP] > [モード (Mode)] の設定を参照)。

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。

ビデオ システムへの接続

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



IP アドレスの確認方法

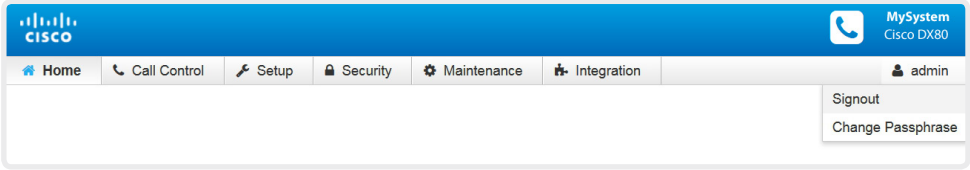
1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [システム情報 (System Information)] を選択します。

サインイン

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

システムには、パスフレーズのない *admin* という名前のデフォルト ユーザが付属しています。初めてサインインする場合は、[パスフレーズ (Passphrase)] フィールドを空白のままにします。

admin ユーザのパスワードを設定する必要があります。



サインアウト

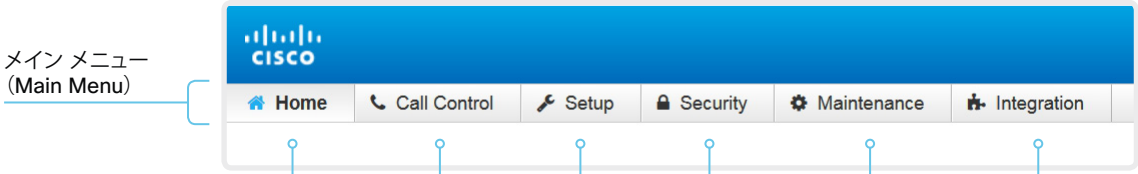
ユーザ名の上にマウスを移動し、ドロップダウン リストから [サインアウト (Sign out)] を選択します。

ビデオ システムの管理方法(3/4 ページ)

Web インターフェイスの編成方法

Web インターフェイスはサブページに分かれています。サインインしているユーザには、そのユーザがアクセス権を持っているページのみが表示されます。

ユーザ管理、ユーザ ロール、およびアクセス権についての詳細は、
▶「ユーザ管理」の章を参照してください。



ホーム(Home)

コール制御(Call Control)

設定(Setup)
- 設定(Configuration)
- ステータス(Status)
- 周辺機器(Peripherals)
- パーソナライゼーション(Personalization)
- ローカル連絡先(Local Contacts)

セキュリティ(Security)
- ユーザ(Users)
- アクセス PIN(暗証番号)(Access PIN)
- サーバ証明書(Server Certificates)
- CUCM 証明書(CUCM Certificates)
- 認証局(Certificate Authorities)
- 強力なセキュリティ モード(Strong Security Mode)
- サインイン バナー(Sign In Banner)
- 非永続モード(Non-persistent Mode)

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

統合(Integration)
- ルーム内コントロール(In-Room Control)
- スタートアップ スクリプト(Startup Scripts)
- 開発者 API(Developer API)

ビデオ システムの管理方法（4/4 ページ）

画面上で使用可能な設定

画面上で次の情報と設定にアクセスできます。

- システム情報
- 警告およびエラー メッセージ
- ビデオ システムの再起動
- 言語、タイム ゾーン、ネットワーク、およびプロビジョニング（サービスのアクティベーション）の基本設定
- 拡張ロギング
- 工場出荷時の状態へのリセット

システム情報および設定へのアクセス

1. ホーム画面で [設定（settings）] アイコン（歯車の形のアイコン）を選択します。
2. [システム情報（System Information）] を選択して、システム情報、潜在的な問題、および [再起動（Restart）] ボタンを見つけます。
3. 次に、システムの調整と基本設定用の [設定（Settings）] を選択します。

   このメニューを開くために、PIN（暗証番号）コードの入力を求められることがあります。詳細については、►「画面上の [設定（Settings）] メニューの PIN（暗証番号）コードの設定」セクションを参照してください。

詳細については、ご使用のビデオ システムのスタートアップ ガイドを参照してください。

第 2 章

設定

ユーザ管理

Web インターフェイスとコマンドライン インターフェイスにアクセスするには、サインインする必要があります。ユーザに各種ロールを割り当てて、ユーザがアクセスできる機能を指定できます。

デフォルトのユーザ アカウント

ビデオ システムには、フル アクセス権を持つデフォルトの管理者ユーザ アカウントが付属しています。ユーザ名は *admin* で、最初はパスフレーズが設定されていません。

admin ユーザのパスフレーズを設定する必要があります。

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

新しいユーザ アカウントを作成する

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

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

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

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

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

既存のユーザ アカウントの編集

Admin ロールを持つユーザに対する変更を行なう場合は常に、確認のために自分のパスフレーズを [自分のパスフレーズ (Your passphrase)] 入力フィールドに入力する必要があります。

ユーザ特権を変更する

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

   [クライアント証明書 DN (識別名) (Client Certificate DN)] フィールドには、HTTPS で証明書ログインを使用する場合にのみ入力してください。
4. [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。

パスフレーズを変更する

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

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

ユーザ アカウントを削除する

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

ユーザ ロールについて

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ことができます。フル アクセス権があるユーザ アカウント (デフォルトの *admin* ユーザなど) は、ADMIN、USER、および AUDIT の各ロールを所有している必要があります。

*ユーザ ロール*は以下のとおりです。

ADMIN：このロールを持つユーザは、新規ユーザの作成、大部分の設定の変更、コールの発信、および連絡先リストの検索が可能です。このユーザは、監査証明書をアップロードしたり、セキュリティ監査設定を変更したりすることはできません。

USER：このロールを持つユーザは、コールの発信と連絡先リストの検索が可能です。このユーザは、着信音の音量の調整や時刻と日付の形式の設定など、いくつかの設定を変更できます。

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

AUDIT：このロールを持つユーザは、セキュリティ監査設定を変更したり、監査証明書をアップロードしたりすることができます。

システム パスフレーズを変更する

次のアクションを実行するためには、システム パスフレーズを知っている必要があります。

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

デフォルトのユーザ アカウント

ビデオ システムには、フル アクセス権を持つデフォルトのユーザ アカウントが付属しています。ユーザ名は *admin* で、初期状態ではパスフレーズは設定されていません。

システム設定へのアクセスを制限するために、必ず、デフォルトの *admin* ユーザ用のパスフレーズを設定する必要があります。ADMIN 権限を持つ他のユーザ用のパスフレーズも設定する必要があります。

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

他のユーザ アカウント

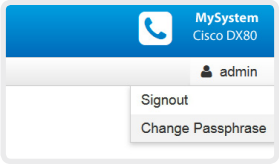
ビデオ システムには多くのユーザ アカウントを作成できます。

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

パスフレーズを変更する

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

   パスフレーズの形式は、0 ～ 64 文字の文字列です。



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

別のユーザのパスフレーズの変更

管理者アクセス権がある場合は、すべてのユーザのパスフレーズを変更できます。

1. Web インターフェイスにサインインして、[セキュリティ (Security)] > [ユーザ (Users)] を選択します。
2. リスト内の該当するユーザをクリックします。
3. 新しいパスフレーズを [パスフレーズ (Passphrase)] と [パスフレーズの再入力 (Repeat passphrase)] の各入力フィールドに入力します。

   そのユーザが Admin ロールを持つ場合、確認のために自分のパスフレーズを [自分のパスフレーズ (Your passphrase)] 入力フィールドに入力する必要があります。
4. [パスフレーズの変更 (Change Passphrase)] をクリックして、変更を保存します。

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

画面上の [設定 (Settings)] メニューの PIN (暗証番号) コードの設定

権限のないユーザがビデオ システムの設定を変更できないようにするために、画面上の [設定 (Settings)] メニューに PIN (暗証番号) コードを設定することを推奨します。

PIN コードの設定

1. Web インターフェイスにサインインして、[セキュリティ (Security)] > [アクセス PIN (暗証番号) (Access PIN)] を選択します。
2. 入力フィールドに PIN コードを入力し、[PIN の設定 (Setup PIN)] をクリックします。

   PIN に使用できる文字は数字のみです。

PIN コードのクリア

1. Web インターフェイスにサインインして、[セキュリティ (Security)] > [アクセス PIN (暗証番号) (Access PIN)] を選択します。
2. [PIN のクリア (Clear PIN)] をクリックします。

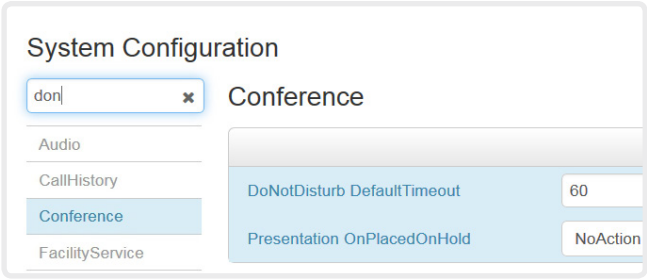
システム設定

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

システム設定を検索する

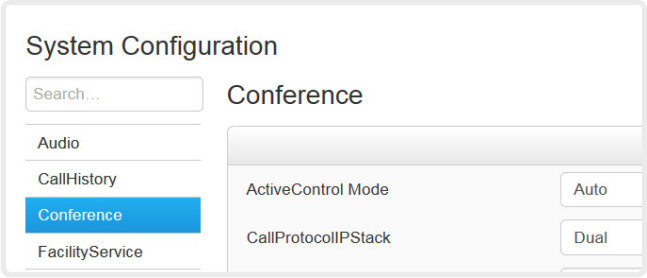
設定を検索する

検索フィールドに必要な数の文字を入力します。これらの文字を含むすべての設定が右ペインに表示されます。値スペースにこれらの文字を含む設定も表示されます。



カテゴリを選択し、設定に移動する

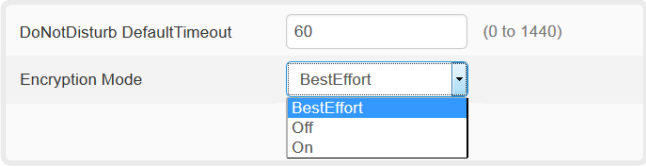
システム設定はカテゴリにグループ分けされています。左ペインでカテゴリを選択すると、関連する設定が表示されます。



システム設定を変更する

値スペースを確認する

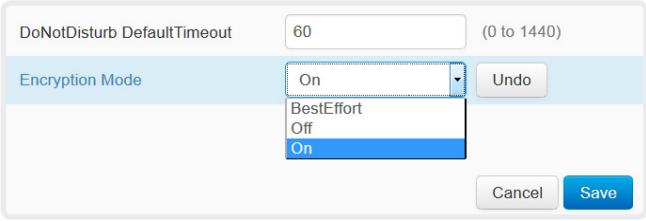
設定値のスペースは、入力フィールドに続くテキスト、または矢印をクリックしたときに開くドロップダウン リストで指定されます。



値を変更する

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

   変更を加えない場合は、[元に戻す (Undo)] または [キャンセル (Cancel)] ボタンを使用します。



保存されていない変更があるカテゴリには編集記号のマークが付きます ( )。

システム設定について

すべてのシステム設定は Web インターフェイスから変更できます。

個別のシステム設定については、▶「システム設定」の章で説明しています。

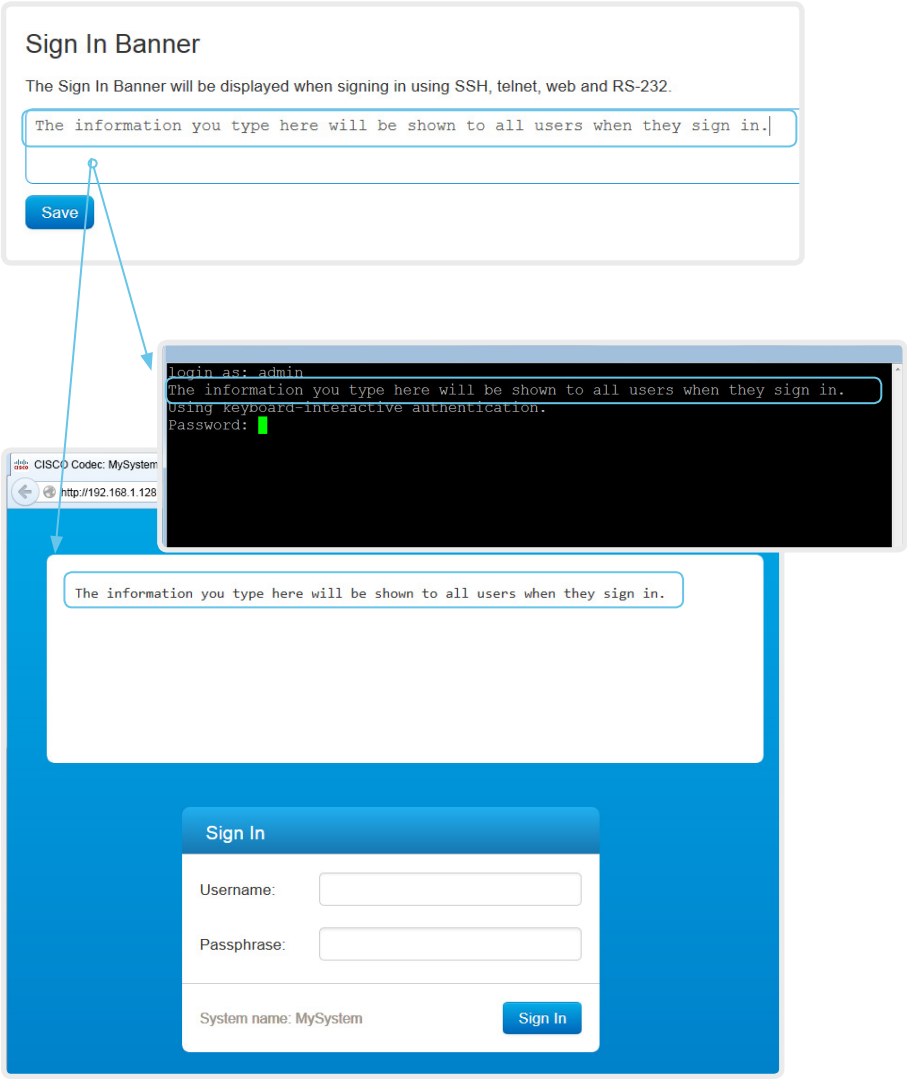
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者はすべてのシステム設定を変更できるように、すべてのユーザ ロールを所有している必要があります。

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

サインイン バナーを追加する

Web インターフェイスにサインインして、[セキュリティ(Security)] > [サインイン バナー(Sign In Banner)] を選択します。

1. ユーザがログインしたときに表示するメッセージを入力します。
2. [保存(Save)] をクリックしてバナーをアクティブにします。



サインイン バナーについて

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

ビデオ システムのサービス証明書の管理

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

次のファイルが必要です。

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

証明書と秘密キーは、ビデオ システムの同じファイル内に保存されます。

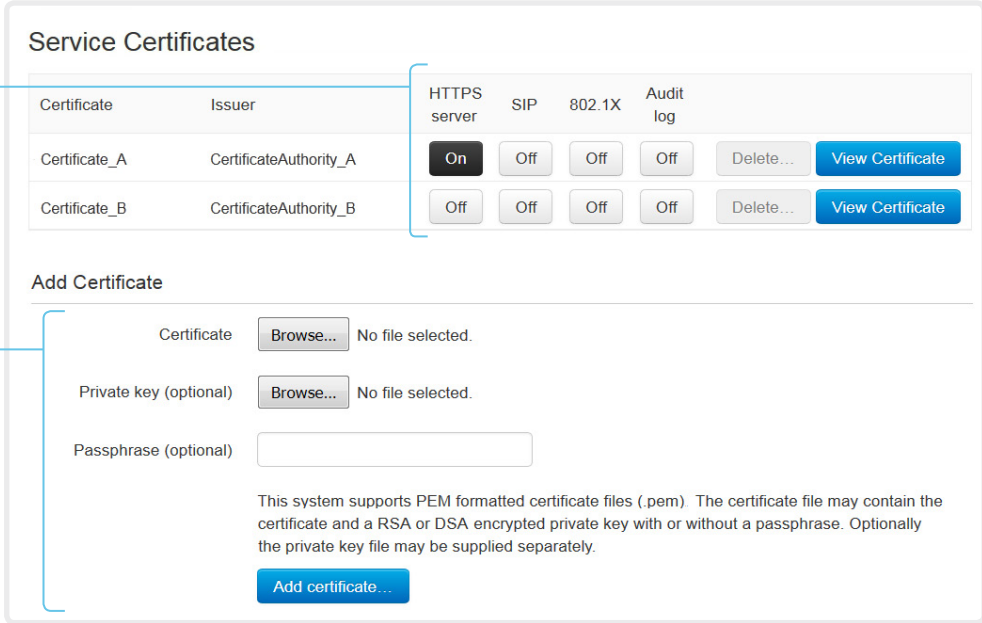
証明書を有効/無効にし、表示、または削除する

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

証明書を表示または削除するには、対応するボタンを使用します。

証明書の追加

1. [参照... (Browse...)] をクリックしてコンピュータ上の証明書ファイルおよび秘密キー ファイル (オプション) を探します。
2. 必要な場合には [パスフレーズ (Passphrase)] に入力します。
3. [証明書の追加... (Add certificate...)] をクリックして、証明書をビデオ システムに保存します。



図内の証明書と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ります。

ビデオ システムのサービス証明書について

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

通信をセットアップする前に、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、HTTPS サーバ、SIP、IEEE 802.1X、および監査ロギングの各サービスに使用されます。

ビデオ 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有効にできる証明書は 1 つだけです。

認証が失敗した場合、接続は確立されません。

信頼できる認証局（CA）のリストを管理する

Web インターフェイスにサインインし、[セキュリティ（Security）] > [認証局（Certificate Authorities）] を選択して、[カスタム CA（Custom CAs）] タブを開きます。

次のファイルが必要です。

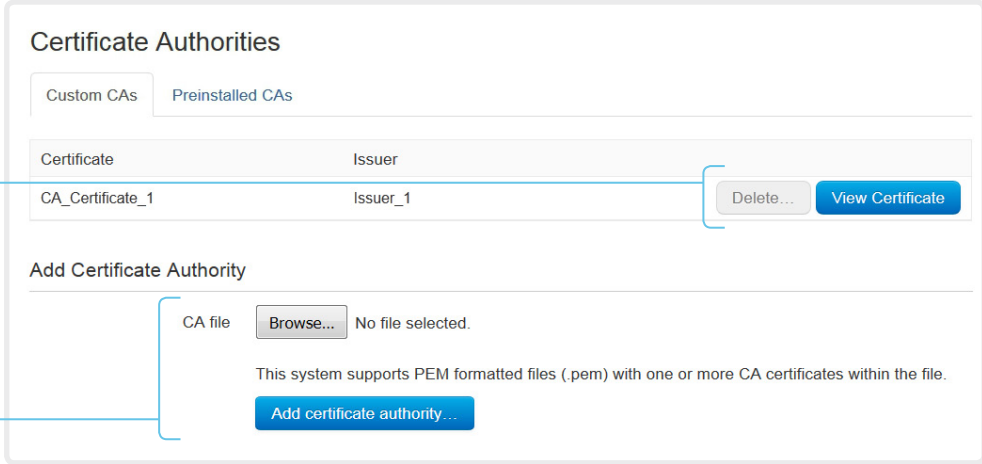
- CA 証明書のリスト（ファイル形式：.PEM）。

証明書を表示または削除する

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

証明局のリストをアップロードする

1. [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。
2. [認証局の追加...（Add certificate authority...）] をクリックして、新しい CA 証明書をビデオ システムに保存します。



図内の証明書と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ります。

以前に保存した証明書は自動的には削除されません。

CA 証明書を持つ新しいファイルのエントリが既存のリストに追加されます。

信頼できる CA について

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

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

リストには、監査ログおよび他の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。

認証が失敗した場合、接続は確立されません。

安全な監査ロギングのセットアップ

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

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

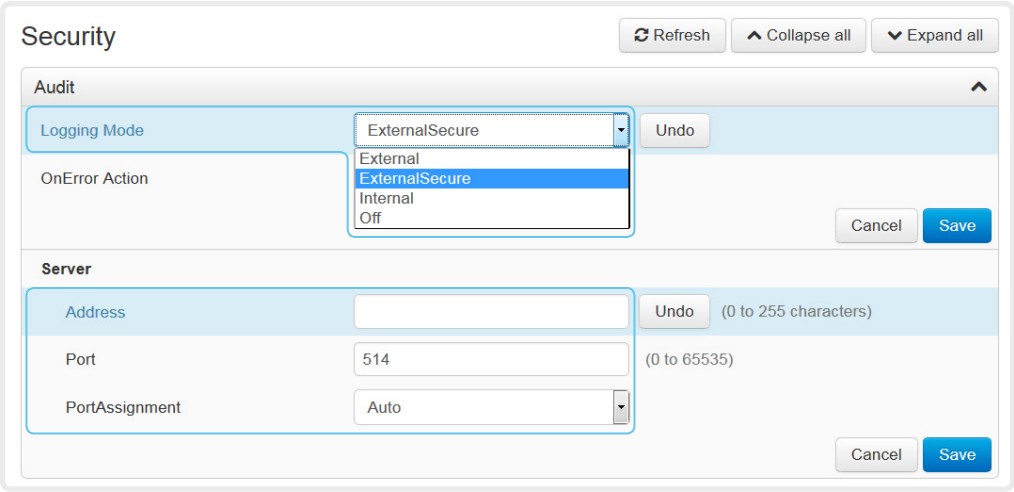
リストの更新方法については、▶「信頼できる認証局(CA)のリストの管理」の章を参照してください。

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

   [ポート割り当て(PortAssignment)] を [手動(Manual)] に設定した場合、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。
3. [監査(Audit)] > [ロギング(Logging)] > [モード(Mode)] を [外部セキュア(ExternalSecure)] に設定します。

   [保存(Save)] をクリックして変更を有効にします。



安全な監査ロギングについて

監査ロギングを有効にすると、ビデオ システム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。

監査ロギングを有効にするには、[セキュリティ(Security)] > [監査(Audit)] > [ロギング(Logging)] > [モード(Mode)] 設定を使用します。監査ロギングはデフォルトで無効になっています。

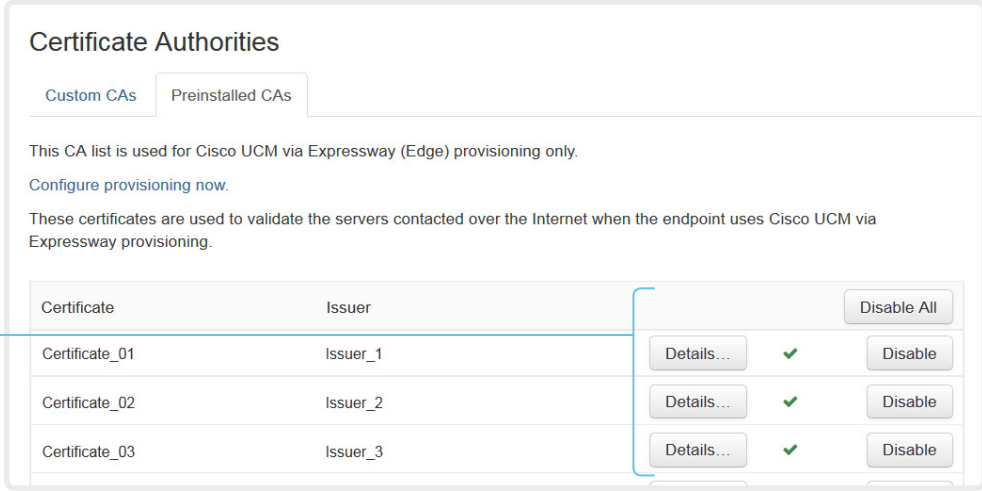
ExternalSecure 監査ログ モードでは、ビデオ システムは暗号化された監査ログを外部監査サーバ(syslog サーバ)に送信します。そのサーバの ID は署名された証明書によって検証される必要があります。

監査サーバの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。

監査サーバの認証が失敗すると、監査ログは外部サーバに送信されません。

Expressway プロビジョニングによる CUCM のプリインストールされた証明書の管理

Web インターフェイスにサインインし、[セキュリティ(Security)] > [認証局(Certificate Authorities)] を選択して、[プリインストールされた CA(Preinstalled CAs)] タブを開きます。



図内の証明書と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ります。

証明書の表示または無効化

詳細を表示または無効化するには、それぞれ、[詳細...(Details...)] ボタンと [無効(Disable)] ボタンを使用します。

プリインストールされた証明書を使用する代わりに、必要な証明書を証明書リストに手動で追加することもできます。

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

プリインストールされた証明書について

このリストにあるプリインストールされた証明書は、ビデオ システムが Expressway(エッジ)を介した Cisco Unified Communications Manager(CUCM)によりプロビジョニングされる場合にのみ使用されます。

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

Cisco Expressway インフラストラクチャ証明書の検証が失敗すると、ビデオ システムはプロビジョニングされず、登録されていません。

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。

CUCM 信頼リストを削除する

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

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

CUCM 信頼リストを削除する

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

一般に、古い CTL（証明書信頼リスト）および ITL（初期信頼リスト）ファイルは削除すべきではありません。

しかし、次のような場合はこれらを削除する必要があります。

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

信頼リストのフィンガープリントと証明書の概要

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

この情報は、トラブルシューティングに役立ちます。

信頼リストについての詳細情報

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 *『Deployment guide for TelePresence endpoints on CUCM』*をお読みください。

永続モードを変更する

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

永続状態を確認する

アクティブなオプション ボタンにより、ビデオ システムの現在の永続状態が示されます。

また、[セットアップ（Setup）] > [ステータス（Status）] > [セキュリティ（Security）] > [永続性（Persistency）] を選択してステータスを確認することもできます。

永続設定を変更する

すべての永続設定は、デフォルトでは [永続（Persistent）] に設定されます。これらの設定の変更は、これらの設定が [非永続（Non-persistent）] になるようにするだけです。

1. 設定、コール履歴、内部ログ、ローカル電話帳（ローカル ディレクトリとお気に入り）、IP 接続情報（DHCP）の永続性を設定するオプション ボタンをクリックします。
2. [保存して再起動...（Save and reboot...）] をクリックします。

   ビデオ システムが自動的に再起動します。再起動後は、新しい永続性設定に従って動作が変更されます。

非永続モードに切り替える前に保存されたログ、設定、およびその他のデータは、消去も削除も行われません。

永続モード

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

通常、永続設定は変更しないことを推奨します。前のセッションでロギングされたすべての情報の表示やトレースをユーザが行えないようにする必要がある場合は、[非永続（Non-persistent）] モードに変更するだけです

非永続モードのときは、システムを再起動するたびに次の情報が削除/消去されます。

- システム設定の変更
- 発信または受信されたコールに関する情報（通話履歴）
- 内部ログ ファイル
- ローカルの連絡先またはお気に入りリストへの変更
- 前回のセッション以降のすべての IP 関連情報（DHCP）

非永続モードに変更する前に保存された情報は、消去も削除も自動的には行われません。このような情報を削除するには、ビデオ システムを工場出荷時設定にリセットする必要があります。

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

強力なセキュリティ モードの設定

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

強力なセキュリティ モードの設定

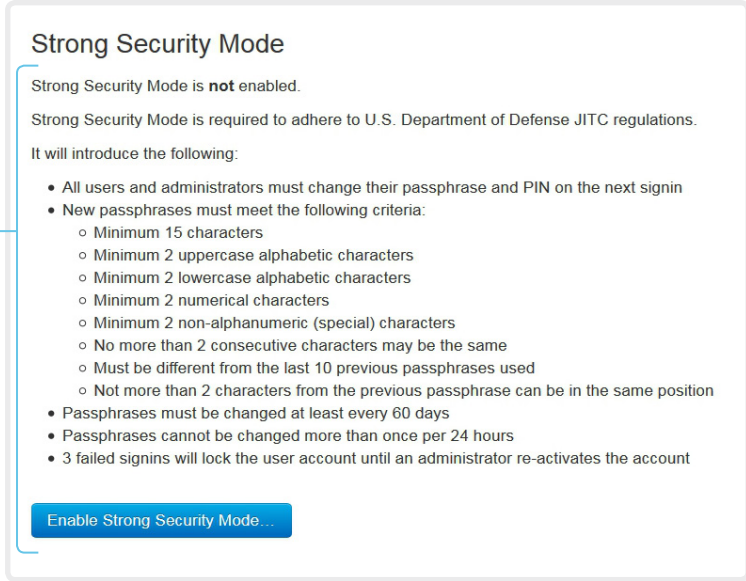
続行する前に、強力なセキュリティ モードによる影響について注意してお読みください。

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...)] をクリックして、表示されるダイアログボックスで選択を確認します。

   ビデオ システムが自動的に再起動します。

2. プロンプトが表示されたら、パスフレーズを変更します。新しいパスフレーズは、記載されている厳密な基準を満たす必要があります。

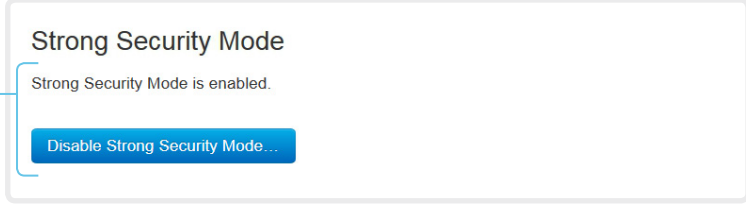
   システム パスフレーズの変更方法については、▶「システム パスフレーズの変更」の章で説明しています。



通常モードに戻る

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

ビデオ システムは自動的に再起動します。



強力なセキュリティ モードについて

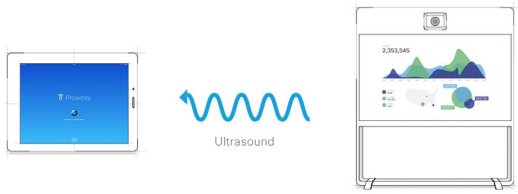
強力なセキュリティ モードは、DoD JITC 規制への準拠が必要な場合にのみ使用します。

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

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

Cisco Proximity により、ユーザは自分のモバイル デバイス(スマートフォン、タブレット、またはラップトップ)がビデオ システムの近くにあるときには、そのデバイスで直接、コンテンツを表示、制御、キャプチャ、および共有することができます。

モバイル デバイスは、ビデオ システムによって送信される超音波の範囲に入ると、ビデオ システムと自動的にペアリングを行うことができます。



同時プロキシミティ接続の数は、ビデオ システムのタイプによって異なります。クライアントは、最大接続数に達したときに新しいユーザに警告します。

ビデオ システム	最大接続数
SX80	10
SX20	7
SX10	7
MX700、MX800	10
MX200 G2、MX300 G2	7
DX70、DX80	3

プロキシミティ サービス

コールの発信とビデオ システムの制御:

- 電話をかける、ミュート、音量調整、コールの終了
- スマートフォンとタブレット(iOS と Android)で使用可能

モバイル デバイス上での共有コンテンツの表示:

- 共有コンテンツの表示、前のスライドのレビュー、選択したスライドの保存
- スマートフォンおよびタブレット(iOS と Android)で利用可能
- DX70 と DX80 の場合、このサービスは通話中の場合のみ利用可能

デスクトップ クライアントからのワイヤレス共有:

- プレゼンテーション ケーブルの接続なしでコンテンツを共有
- ラップトップ(OS X、Windows)で利用可能

コールの発信とビデオ システムの制御

モバイル デバイスでの共有コンテンツの表示

モバイル デバイスからの無線共有

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

Cisco Proximity クライアントをインストールする

クライアントの入手先

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

スマートフォンやタブレットのクライアントは、Google Play (Android) および Apple App Store (iOS) から直接、入手することもできます。

エンド ユーザ ライセンス契約書

次のエンドユーザ ライセンス契約書を慎重に読んでください。
► http://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

サポートされるオペレーティング システム

- iOS 7 以降
- Android 4.0 以降
- Mac OS X 10.9 以降
- Windows 7 以降
  Windows 8 で導入されたタイル ベースのインターフェイスはサポートされていません。

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

超音波の出力

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

プロキシミティ機能の On と Off を切り替える(その結果、超音波の出力も切り替える)には、[プロキシミティ(Proximity)] > [モード(Mode)] 設定を使用します。

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

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

SX10N および MX シリーズ:

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

DX70 および DX80:

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

SX10、SX20、および SX80:

- これらのシステムではサードパーティ製のスピーカーに超音波を出力するため、シスコではこの超音波の音圧レベルを制御することができません。

  超音波の音圧レベルは、スピーカー自体の音量コントロール、および [周辺機器(Peripherals)] > [ペアリング(Pairing)] > [超音波(Ultrasound)] > [音量(Volume)] > [最大レベル(MaxLevel)] の設定から影響を受けます。つまり、リモート コントロールまたはタッチ コントローラの音量コントロールから音圧レベルは調整できません。

ヘッドセット

DX70、DX80、および SX10N:

これらのシステムでは、次の理由からヘッドセットを常に使用できます。

- DX70 と DX80 には、超音波を出力することのない専用のヘッドセット出力が備わっています。
- SX10N には超音波用の組み込みのスピーカーが備わっているため、超音波を HDMI 出力とスピーカー出力に出力することはありません。

SX10、SX20、SX80、または MX シリーズ:

- これらのビデオ システムでヘッドセットを使用する場合、超音波の出力をオフに切り替える([プロキシミティ(Proximity)] > [モード(Mode)] を Off に設定する)ことを強く推奨します。こうすると、プロキシミティ機能を使用できなくなります。

  これらのシステムには専用のヘッドセット出力が備わっていないため、シスコでは接続されたヘッドセットから音圧レベルを制御することはできません。

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

プロキシミティ サービスの有効化

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

   ビデオ システムが超音波ペアリング メッセージの送信を開始します。
3. 許可するサービスを有効にします。[モバイル デバイスからのワイヤレス共有 (Wireless share from a mobile device)] だけが、デフォルトでは有効になっています。

   プロキシミティ機能を完全に利用するためには、すべてのサービスを有効にすることを推奨します。

   コールの発信とビデオ システムの制御:

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

   モバイル デバイスで共有コンテンツを表示:

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

   デスクトップ クライアントからのワイヤレス共有:

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

プロキシミティ サービスの一時的無効化

会議中に室内の各デバイスでコンテンツを受信できないようにしたい場合、ビデオ システムのユーザ インターフェイスを使用してプロキシミティ サービスを一時的に無効にすることができます。

ビデオ システムでは、このような会議中に超音波ペアリング メッセージを送信し続けます。これにより、クライアントが近くにあるビデオ システムを認識することが保証され、ユーザになぜユーザが接続できないかの説明を提供することができます。

1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択して、ドロップダウン パネルを開きます。
2. トグル ボタンを使用してプロキシミティのオン/オフを切り替えます。

プロキシミティ インジケータ

[プロキシミティ (Proximity)] が On になっていて、少なくとも 1 つのプロキシミティ サービスが有効になっている場合、ディスプレイにプロキシミティ インジケータが表示されます。

プロキシミティ インジケータには、次の 2 つの状態があります。

プロキシミティ サービスを使用できます。

プロキシミティ サービスは一時的に無効になっています。プロキシミティ サービスを再度使用できるようにするには、[設定 (settings)] ドロップダウン パネルにあるトグル ボタンを使用します。

プロキシミティについて

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

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

超音波ペアリング メッセージは、プロキシミティ クライアントを使用した近くのデバイスによって受信され、そのデバイスの認証と認可をトリガーします。

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

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

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

プライバシーについて

シスコ プライバシー ポリシーと Cisco Proximity Supplement で、クライアントでのデータ収集と、この機能を組織に導入するときに考慮する必要があるプライバシーの侵害に関する情報を参照できます。参照先:
► http://www.cisco.com/web/siteassets/legal/privacy.html

ビデオ システムのユーザ インターフェイスを使用して、プロキシミティ サービスを一時的に無効にすることができます。これは、会議中に室内の各モバイル デバイスでコンテンツを受信できないようにしたい場合に役立ちます。

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

基本的なトラブルシューティング

プロキシミティ クライアントを持つデバイスを検出できない

- 一部の Windows ラップトップでは、超音波の周波数範囲 (20 ～ 22 kHz) の音を記録できません。これは、特定のデバイスのサウンド カード、サウンド ドライバ、または内蔵マイクに関する周波数の制限が原因である可能性があります。詳細については、サポート フォーラムを参照してください。

音声の問題

- ブーンという音や音割れなど音声の問題がある場合は、最大超音波音量を下げてください ([周辺機器 (Peripherals)] > [ペアリング (Pairing)] > [超音波 (Ultrasound)] > [音量 (Volume)] > [最大レベル (MaxLevel)])。

ラップトップからのコンテンツを共有できない

- コンテンツ シェアリングが機能するためには、ビデオ システムとラップトップが同じネットワーク上にある必要があります。このため、ご使用のビデオ システムが Expressway を通じて会社のネットワークに接続され、ラップトップが VPN (VPN クライアントに依存) を通じて接続されている場合、プロキシミティの共有が失敗することがあります。

関連リソース

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

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

コール レートに合わせてビデオ品質を調整する

最適鮮明度プロファイル

最適鮮明度プロファイルは、ビデオ会議室の照明条件とカメラ（ビデオ入力ソース）の品質を反映している必要があります。照明条件が良く、カメラの品質が高いほど、高いプロファイルを使用する必要があります。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。

一般には、中程度のプロファイルが推奨されています。ただし、照明条件が非常に良い場合は、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お勧めします。特定のコール レートの解像度を上げるために、高いプロファイルを設定することもできます。

ビデオ入力品質の設定

最適鮮明度設定を有効にするには、*Video Input Connector n Quality* 設定を **Motion** に設定する必要があります。ビデオ入力の品質を [シャープさ（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 インターフェイスにサインインして [セットアップ（Setup）] > [設定（Configuration）] を選択します。

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

パケット損失の復元力:ClearPath

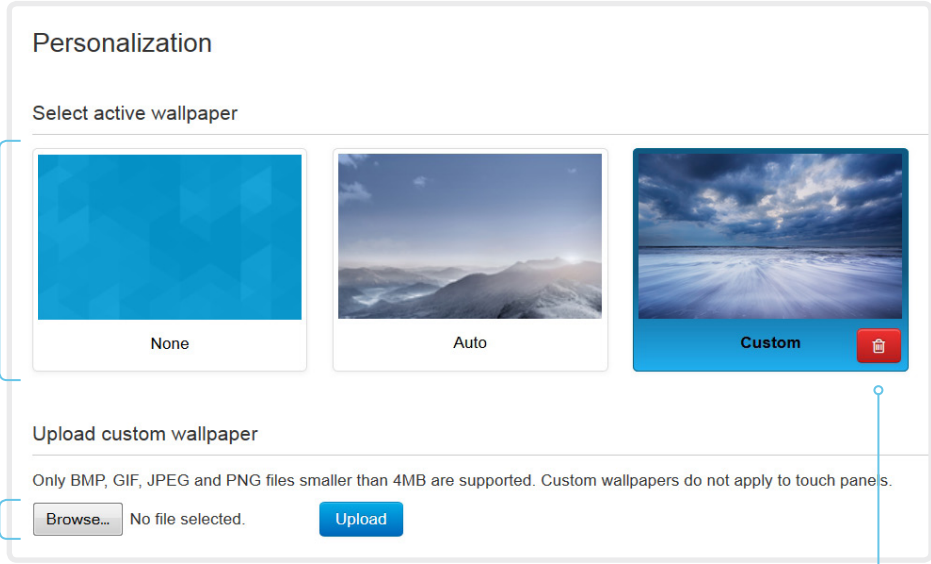
ClearPath により、高度なパケット損失復元メカニズムを導入できます。これらのメカニズムは、エラーを起こしやすい環境でビデオ システムを使用した場合の品質を向上させます。

ClearPath はシスコ独自のプロトコルです。CE ソフトウェアを実行するすべてのエンドポイントが ClearPath に対応しています。

関係するエンドポイントとインフラストラクチャ要素が ClearPath に対応している場合、ポイントツーポイント接続ですべてのパケット損失回復メカニズム(ホスト型会議を含む)が使用されます。

壁紙の選択

Web インターフェイスにサインインして [セットアップ (Setup)] > [パーソナライゼーション (Personalization)] を選択します。



壁紙の選択

リストから壁紙を選択します。

アクティブの壁紙が強調表示されます。

カスタムの壁紙のアップロード

古いカスタムの壁紙を上書きします。

1. [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。
2. [アップロード (Upload)] をクリックして、ファイルをビデオ システムに保存します。

   サポートされるファイル形式：BMP、GIF、JPEG、PNG

   最大ファイル サイズ：4 MByte

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

[削除 (Delete)] を選択すると、ビデオ システムからカスタム壁紙が完全に削除されます。

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

カスタムの壁紙について

企業ロゴまたは別のカスタム画像をメイン ディスプレイ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。

一度にビデオ システムに保存できるカスタムの壁紙は 1 つだけです。つまり、新しいカスタムの壁紙によって古いカスタムの壁紙は上書きされます。

カスタムの壁紙を使用すると、次の項目がメイン ディスプレイから削除されます。

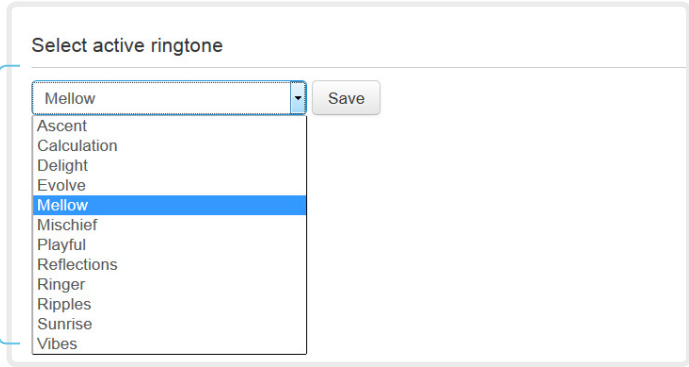
- 大きい時計
- 予定されている会議のリスト

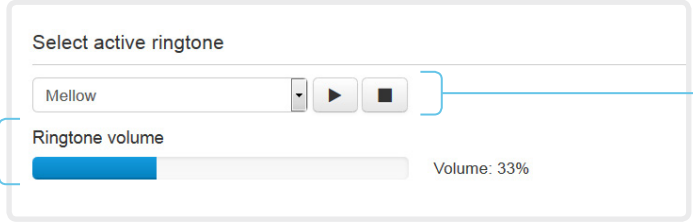
着信音の選択と着信音の音量の設定

Web インターフェイスにサインインして [セットアップ (Setup)] > [パーソナライゼーション (Personalization)] を選択します。

着信音を変更する

1. ドロップダウン リストから着信音を選択します。
2. [保存 (Save)] をクリックすると、選択した着信音がアクティブな着信音になります。





呼び出し音の音量の設定

呼び出し音の音量を調節するにはスライド バーを使用します。

着信音の再生

呼び出し音を再生するには、再生ボタン (▶) をクリックします。

再生を終了するには、停止ボタン (■) を使用します。

着信音について

着信音一式がビデオ システムにインストールされています。着信音を選択して着信音の音量を設定するには、Web インターフェイスを使用します。

Web インターフェイスから選択した着信音を再生することができます。着信音は、Web インターフェイスを実行しているコンピュータではなく、ビデオ システム自体で再生されることに注意してください。

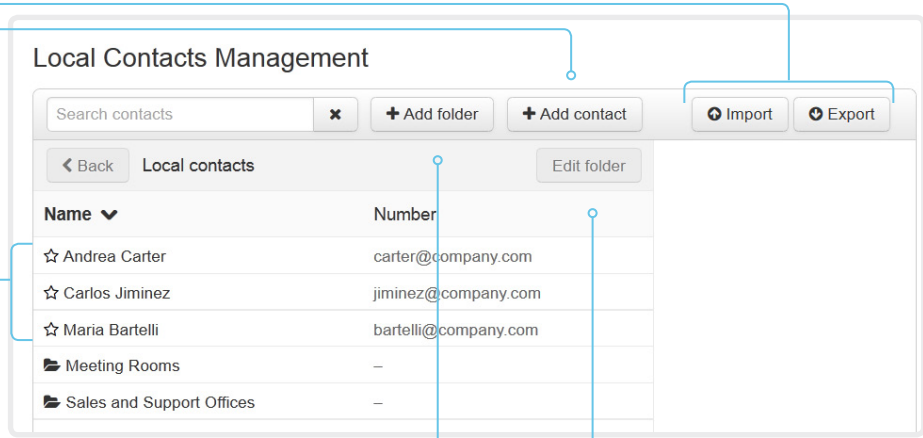
ローカルの連絡先を管理する

Web インターフェイスにサインインして [セットアップ (Setup)] > [ローカルの連絡先 (Local Contacts)] を選択します。

ファイルから連絡先をインポート/エクスポート

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

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



連絡先を追加または編集する

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

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

   連絡先について、複数の連絡方法 (ビデオ アドレス、電話と携帯電話の番号など) を保存する場合は、[連絡方法の追加 (Add contact method)] をクリックし、新しい入力フィールドに入力します。
3. [保存 (Save)] をクリックしてローカル連絡先を保存します。

連絡先を削除する

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

サブフォルダを追加または編集する

1. 新しいサブフォルダを作成するには、[フォルダの追加 (Add folder)] をクリックします。既存のサブフォルダを変更するには、リストされているサブフォルダの 1 つをクリックしてから [フォルダの編集 (Edit folder)] をクリックします。
2. ポップアップしたフォームに入力するか、フォームを更新します。
3. [保存 (Save)] をクリックしてフォルダを作成または更新します。

サブフォルダを削除する

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

ローカル連絡先の場所

画面上:[発信 (Call)] > [ディレクトリ (Directory)] > [ローカルの連絡先 (Local contacts)] を選択します。ローカル連絡先はフォルダ階層にかかわらず、アルファベット順に表示されます。

Web インターフェイス:[コール制御 (Call Control)] をクリックし、[連絡先] セクションの [ローカル (Local)] タブを開きます。

お気に入りリスト

[お気に入り (Favorites)] リストは、画面上でのみ使用できます。[お気に入り (Favorites)] リストは、Web インターフェイスでは使用できません。

このリストを見つけるには、[発信 (Call)] > [お気に入り (Favorites)] を選択します。お気に入りリストには、ローカル連絡先とその他のディレクトリ エントリの両方を追加できます。

また、お気に入りとしてマークされたディレクトリ エントリは、自動的にローカル連絡先フォルダにコピーされます。

お気に入りリストへの連絡先の追加

画面上:連絡先を選択してから、••• を選択します。[お気に入りに設定 (Mark as Favorite)] をクリックします。

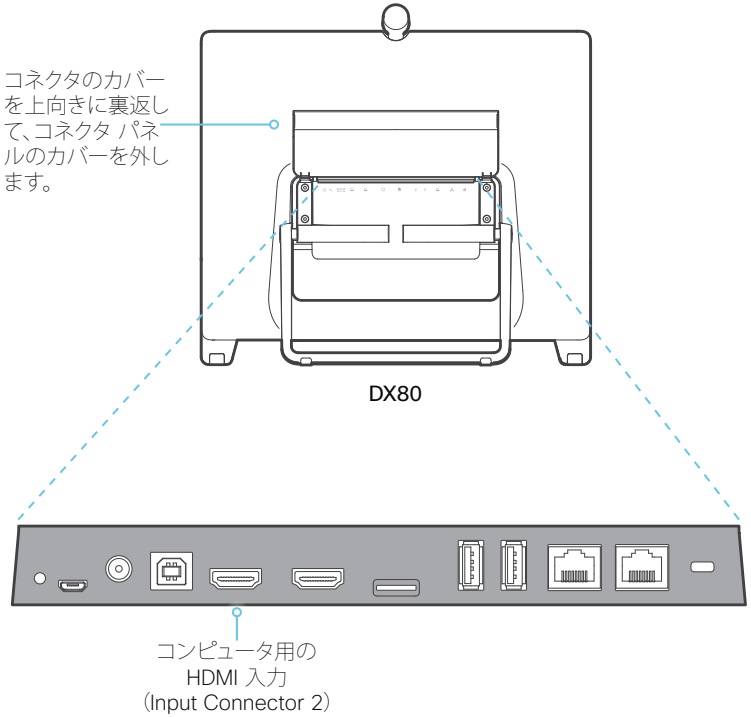
Web インターフェイス:**[セットアップ (Setup)] > [ローカルの連絡先 (Local Contacts)]** を選択します。連絡先の横にある星印をクリックします。

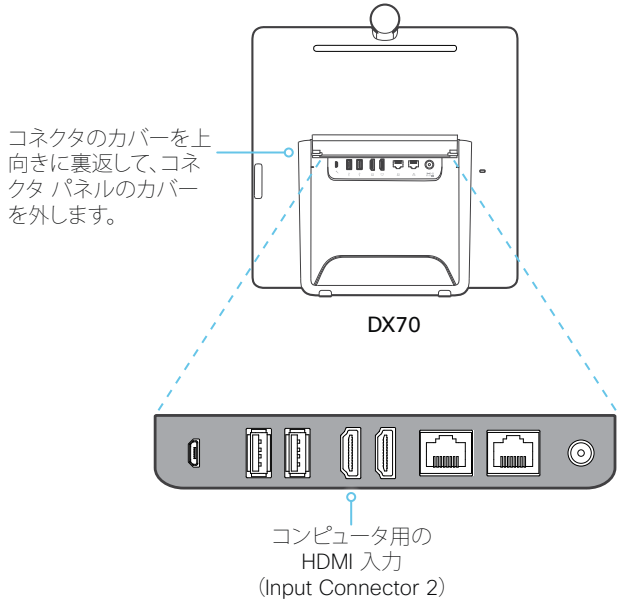
第 3 章

周辺機器

コンピュータの接続

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

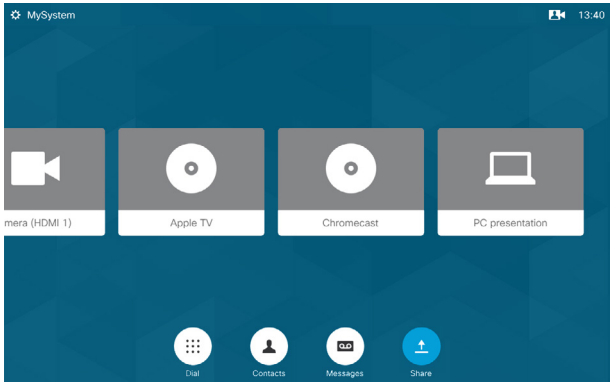




入力ソースの数を拡張する

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

これらのソースは、ビデオ システムに直接接続された他のビデオ ソースのように表示されて動作します。



例の外部入力ソースが表示されたユーザ インターフェイス

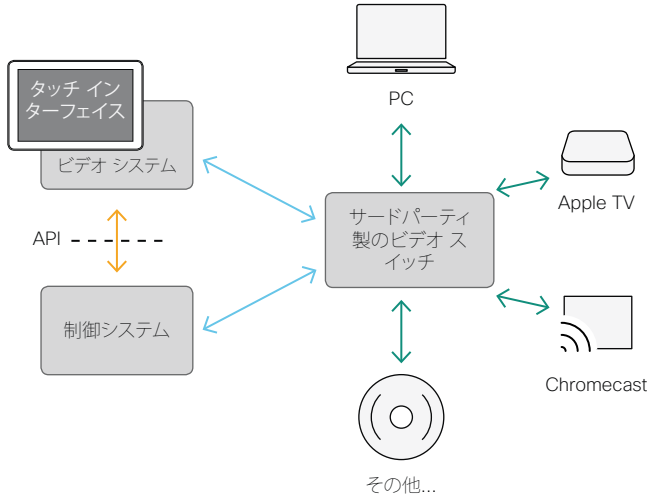
ユーザ インターフェイスを拡張する方法、およびビデオ システムの API を使用してそのユーザ インターフェイスをセットアップする方法の詳細については、*室内制御のガイド*を参照してください。参照先:

► http://www.cisco.com/go/in-room-control-docs [英語]

アーキテクチャ

タッチ インターフェイスを装備した Cisco ビデオ システム、Crestron 社や AMX 社などのサードパーティ製の制御システム、およびサードパーティ製のビデオ スイッチが必要です。ビデオ スイッチを制御するのは、ビデオ システムではなく、制御システムです。

制御システムをプログラミングする場合、ビデオ スイッチと、タッチ インターフェイスのコントロールを接続するために、ビデオ システムの API(イベントとコマンド)*を使用する必要があります。このように、ユーザ インターフェイスで表示されるものと実行されるものを、入力ソースの実際の状態と同期することができます。



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

第 4 章

メンテナンス

システム ソフトウェアをアップグレードする (1/2 ページ)

Android ベースのソフトウェアと CE ソフトウェアとの間の変換

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

Cisco DX80 と Cisco DX70 は、元々 *Android ベースのソフトウェア*とともに販売されていましたが、近く *CE ソフトウェア*とともに出荷される予定です。

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

DX デバイス上の *CE ソフトウェア*では、CE 8.3 の次の機能はサポートされていません。

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

詳細については、ソフトウェア リリース ノートを参照してください。

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

システム ソフトウェアをアップグレードする (2/2ページ)

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

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

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

新しいソフトウェアをダウンロードする

ソフトウェアをダウンロードするには、シスコのソフトウェア ダウンロード Web ページ(► http://www.cisco.com/cisco/software/navigator.html)にアクセスします。次に、お使いの製品に移動します。

ファイル名の形式は「 s52040ce8_3_x.pkg」です。ソフトウェア バージョンごとにファイル名が異なります。

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(CE8)を読むことを推奨します。

参照先:► http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html [英語]

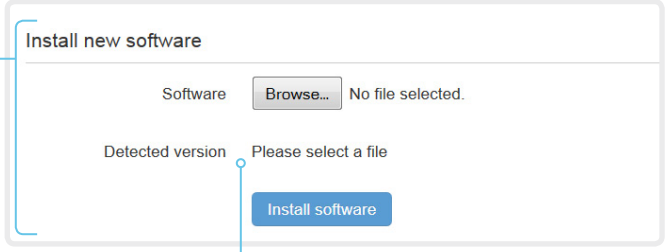
新しいソフトウェアのインストール

該当するソフトウェア パッケージをダウンロードして、お使いのコンピュータに保存します。これは .pkg ファイルです。

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

   ソフトウェア バージョンが検出され、表示されます。

2. [インストール(Install)] をクリックして、インストール プロセスを開始します。



ソフトウェアのバージョンの確認

ファイルを選択すると、ソフトウェアのバージョンが表示されます。

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

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

ソフトウェア バージョンについて

このビデオ会議システムは CE ソフトウェアを使用しています。このドキュメントで説明するバージョンは、CE8.3.x です。

オプション キーを追加する

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

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

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

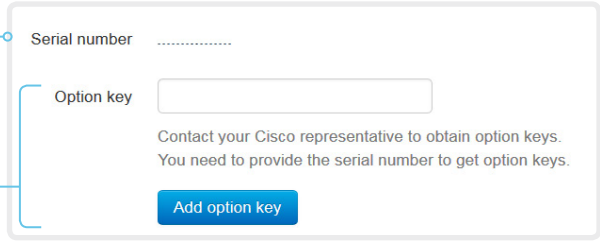
ビデオ システムのシリアル番号

オプション キーを発注する際、ビデオ システムのシリアル番号が必要です。

オプション キーの追加

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

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



オプション キーについて

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

各ビデオ システムには一意のオプション キーがあります。

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

システム ステータス

システム情報の概要

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

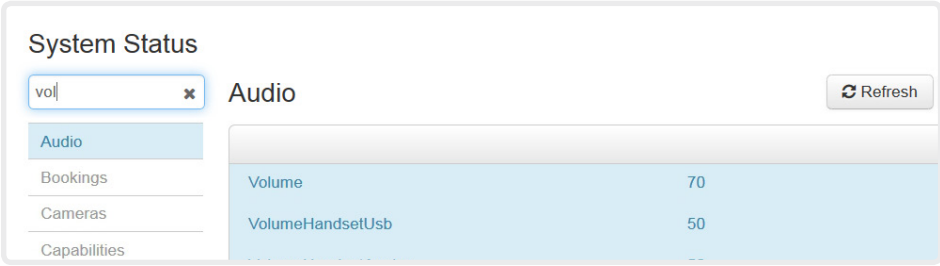
このページには、製品タイプ、システム名、およびハードウェア、ソフトウェア、インストール済みオプション、およびネットワーク アドレスに関する基本情報が表示されます。ビデオ ネットワーク(SIP および H.323)の登録ステータスのほか、システムにコールする際に使用する番号および URI も含まれます。

システム ステータスの詳細

Web インターフェイスにサインインして、[設定(Setup)] > [ステータス(Status)] を選択し、より詳細なステータス情報を確認します*。

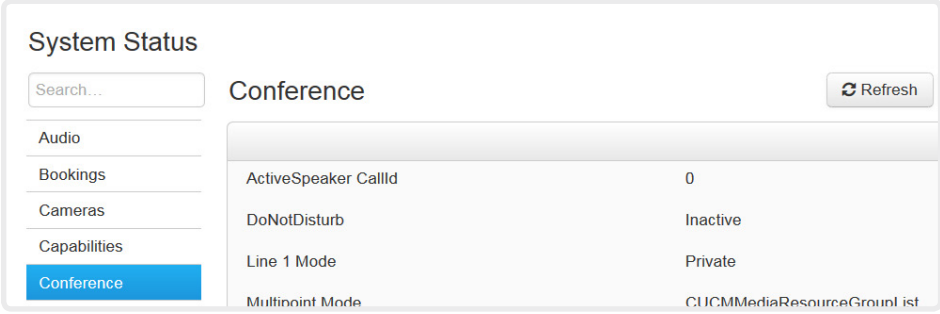
ステータス エントリを検索する

検索フィールドに必要な数の文字を入力します。これらの文字を含むすべてのエントリが右ペインに表示されます。値スペースにこれらの文字を含むエントリも表示されます。



カテゴリを選択し、正しいステータスに移動する

システム ステータスはカテゴリにグループ分けされています。左ペインでカテゴリを選択すると、関連するステータスが右側に表示されます。



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

診断の実行

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

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

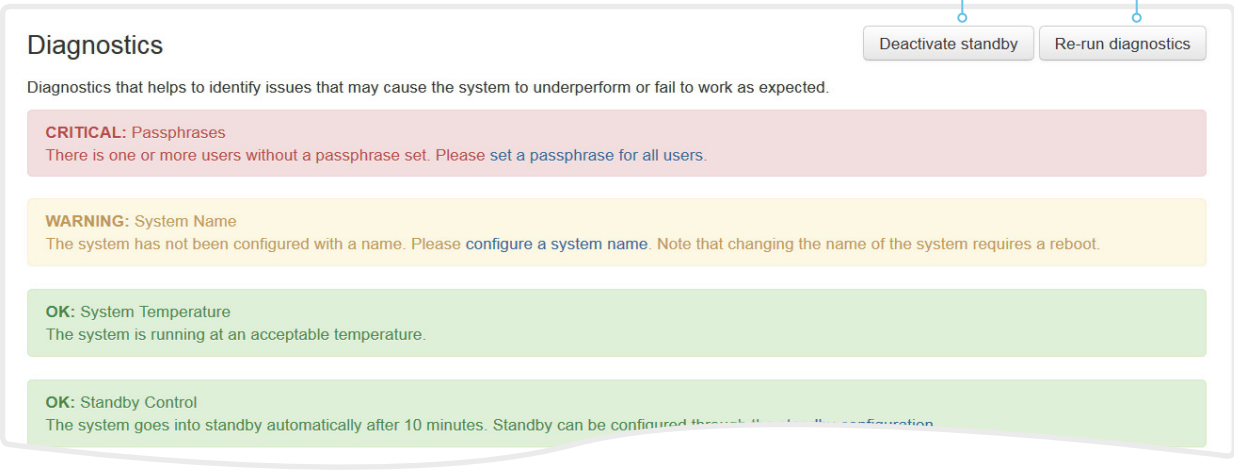
エラーおよび重大な問題は赤、警告は黄色で明確に表示されます。

診断の実行

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

スタンバイ モードを離れる

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

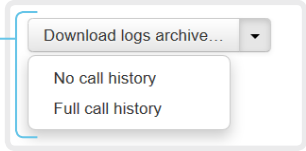


* 図に示しているメッセージは一例です。お使いのシステムでは表示される情報が異なる場合があります。

ログ ファイルをダウンロードする

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

すべてのログ ファイルをダウンロードする



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

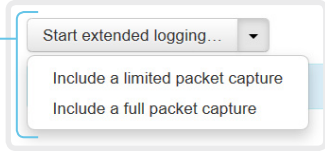
匿名化された通話履歴はログ ファイルにデフォルトで含まれています。

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

1 つのログファイルを開く/保存

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

拡張ロギングの開始



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

ネットワーク トラフィック全部のキャプチャを含めるかどうかによって、拡張ロギングには 3 分または 10 分かかります。

タイムアウトが発生する前に拡張ロギングを中止する場合は、[拡張ロギングの停止 (Stop extended logging)] をクリックします。

デフォルトとして、ネットワーク トラフィックはキャプチャされません。ネットワーク トラフィックの部分キャプチャまたは完全キャプチャを含める場合は、ドロップダウン メニューを使用します。

ログ ファイルのリストを更新する

*現在のログ*または*履歴ログ*のリストを更新するには、[現在のログ (Current logs)] または [履歴ログ (Historical logs)] の更新ボタンをクリックします。

ログ ファイルについて

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

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

現在のログ ファイルはすべて、ビデオ 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。

拡張ロギング モード

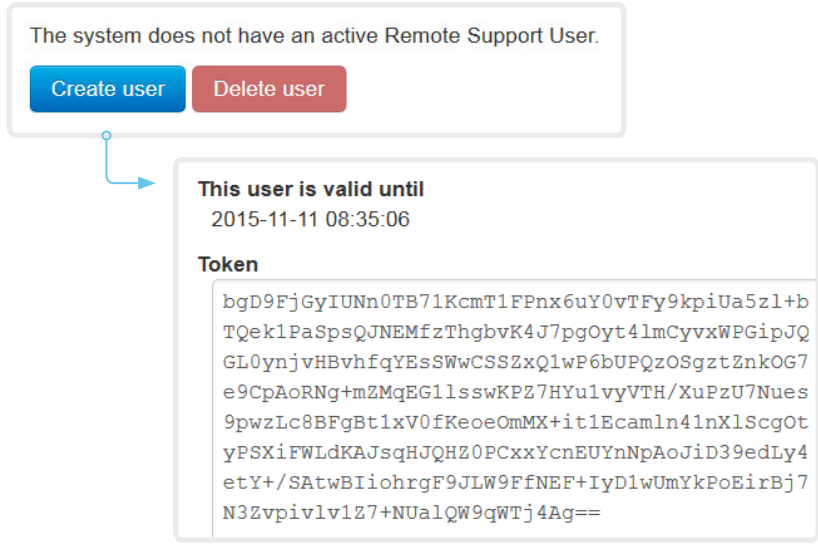
拡張ロギング モードをオンにすると、コールのセットアップ中にネットワークの問題の診断に役立つ場合があります。このモードの間は、より多くの情報がログ ファイルに保存されます。

拡張ロギングはビデオ システムのリソースをより多く使用するため、ビデオ システムのパフォーマンスが低下する可能性があることに注意してください。拡張ロギング モードは問題をトラブルシューティングするときにだけ使用してください。

リモート サポート ユーザを作成する

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

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



リモート サポート ユーザの作成

1. [ユーザの作成 (Create User)] をクリックします。
2. Cisco TAC でケースをオープンします。
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。

リモート サポート ユーザについて

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。

設定をバックアップ、または復元する

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

現在の設定を表示する

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。

現在の設定をバックアップする

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。

バックアップから設定を復元する

1. [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。
2. 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。

   一部の設定では、設定を有効にするためにビデオ システムを再起動する必要があります。

設定のバックアップについて

[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、バックアップ テキスト ファイルとして保存できます。

バックアップ 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。

以前使用していたソフトウェア イメージへの復元

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

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

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

以前に使っていたソフトウェア イメージと交換する前に、ビデオ システムのログ ファイルと設定をバックアップすることを推奨します。

ログ ファイルとシステム設定のバックアップ

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

以前に使用していたソフトウェア イメージに復元する

この手順は管理者のみ、またはシスコ テクニカルサポートに連絡した場合にのみ、実行する必要があります。

1. [ソフトウェア リカバリのスワップ（Software Recovery Swap）] タブを選択します。
2. [ソフトウェア cex.y.z... への切り替え（Switch to software cex.y.z...）] をクリックします（x.y.z はソフトウェアのバージョンを示します）。
3. [はい（Yes）] をクリックして選択を確定するか、[キャンセル（Cancel）] をクリックして操作を取り止めます。

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が自動的に再起動します。この手順には数分かかることがあります。

以前に使用されたソフトウェア イメージについて

ビデオ システムに重大な問題がある場合は、これまで使用していたソフトウェア イメージ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初期設定にリセットしていない場合は、これまで使用していたソフトウェア イメージが、まだ、システム上に存在しています。ソフトウェアを再度ダウンロードする必要はありません。

ビデオ システムを工場出荷時設定にリセットする (1/3 ページ)

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

初期設定にリセットしたら元に戻すことはできません。

工場出荷時の状態にリセットする前に以前使用したソフトウェア イメージに戻すことを常に検討してください。多くの場合これでシステムをリカバリします。ソフトウェアの交換については、►「以前使用していたソフトウェア イメージへの復元」の章を参照してください。

Web インターフェイスを使用して、システムを初期設定にリセットすることをお勧めします。Web インターフェイスを使用できない場合は、DX80 ではリセット ボタンを、DX70 ではミュート ボタンと音量ボタンを使用します。

工場出荷時設定にリセットすると、以下のことが行われます。

- 通話履歴が削除されます。
- パスフレーズがデフォルト設定にリセットされます。
- すべてのシステム パラメータがデフォルト値にリセットされます。
- システムにアップロードされたすべてのファイルが削除されます。これには、カスタム壁紙、証明書、ローカル連絡先、およびお気に入りリストが含まれますが、これらに限定されません。
- 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。

初期設定へのリセット後は、ビデオ システムが自動的に再起動します。これは、以前と同じソフトウェア イメージを使用しています。

工場出荷時の状態にリセットする前にビデオ 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 ファイルとシステム設定をバックアップする

Web インターフェイスにログインし、[メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)] に移動します。

ログ ファイルとシステム設定をバックアップする

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

Web インターフェイスを使用して工場出荷時設定にリセットする

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

Web インターフェイスにログインし、[メンテナンス (Maintenance)] > [システム リカバリ (System Recovery)] に移動します。

1. [初期設定へのリセット (Factory Reset)] タブを選択して、表示される情報を注意深く読みます。
2. [工場出荷時設定へのリセット... (Perform a factory reset...)] をクリックします。
3. [はい (Yes)] をクリックして選択を確定するか、[キャンセル (Cancel)] をクリックして操作を取り止めます。
4. ビデオ システムがデフォルトの初期設定に戻るまで待機します。終了するとビデオ システムが自動的に再起動します。数分かかることがあります。

   ビデオ システムは、メイン画面に通知を表示して、初期設定にリセットされたことを示します。通知は約 10 秒後に非表示になります。

ビデオ システムの工場出荷時設定リセット (2/3 ページ)

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

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

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

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

   ビデオ システムがデフォルトの初期設定に戻るまで待機します。終了するとビデオ システムが自動的に再起動します。数分かかることがあります。

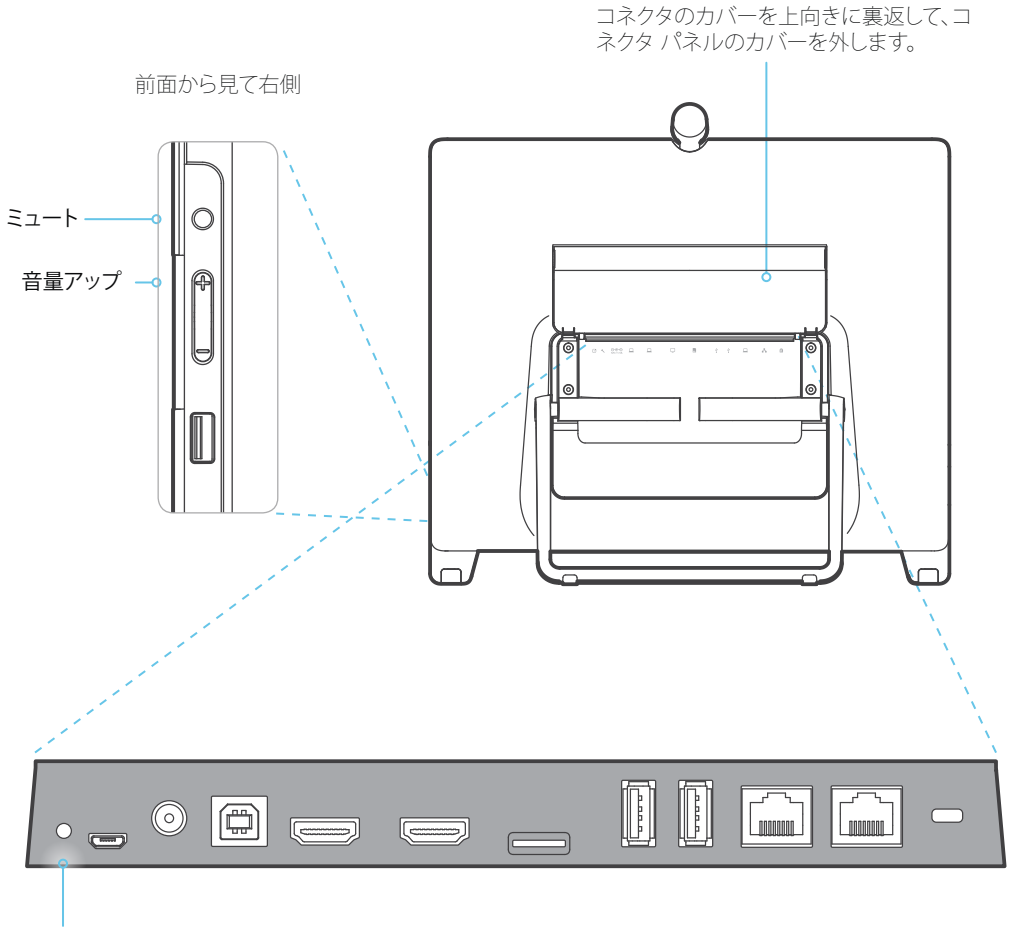
   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。詳細については、*DX80 のスタートアップ ガイド*を参照してください。

リセット ボタンを使用した DX80 の工場出荷時設定へのリセット

この方法を使用するには、DX80 が稼動している必要があります。

1. ビデオ システムの背面で、コネクタのカバーを上向きに裏返して、コネクタ パネルのカバーを外します。
2. ペン先 (または同等のもの) を使用して、引っ込んでいるリセット ボタンを押して、[初期設定へのリセットを実行しています (Resetting to factory settings)] という通知が画面に表示されるまで、1 ～ 2 秒間押し続けます。
3. ビデオ システムがデフォルトの初期設定に戻るまで待機します。終了するとビデオ システムが自動的に再起動します。数分かかることがあります。

   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。詳細については、*DX80 のスタートアップ ガイド*を参照してください。



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

ビデオ システムの工場出荷時設定リセット (3/3 ページ)

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

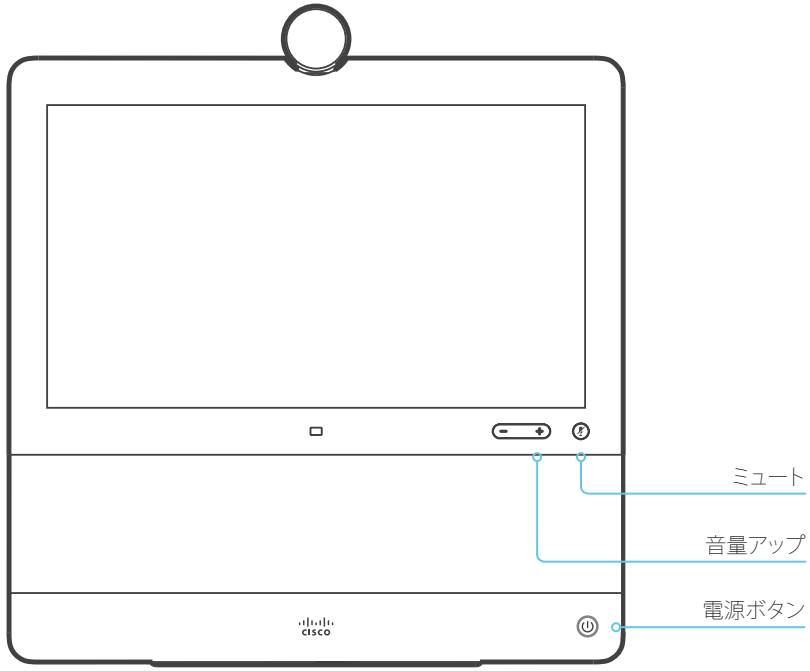
ミュート ボタンと音量ボタンを使用した DX70 の工場出荷時設定へのリセット

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

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

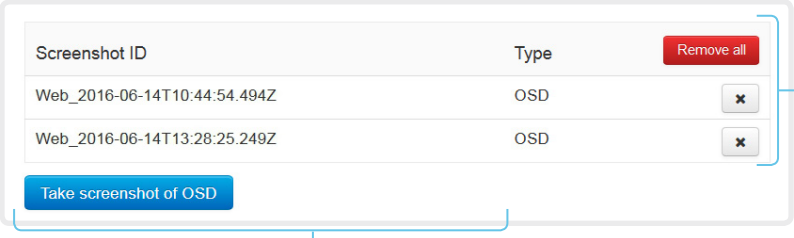
   ビデオ システムがデフォルトの初期設定に戻るまで待機します。終了するとビデオ システムが自動的に再起動します。数分かかることがあります。

   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。詳細については、*DX70 のスタートアップ ガイド*を参照してください。



ユーザ インターフェイスのスクリーンショットのキャプチャ

Web インターフェイスにサインインして、[メンテナンス（Maintenance）] > [ユーザ インターフェイスのスクリーンショット（User Interface Screenshots）] を選択します。



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 X ボタンをクリックします。

スクリーンショットのキャプチャ

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

スクリーンショットはボタンの下の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最大で 30 秒かかる場合があります。

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

ユーザ インターフェイスのスクリーンショットについて

画面上の表示（メイン ディスプレイのメニュー、インジケータ、およびメッセージ）のスクリーンショットをキャプチャできます。

第 5 章

システム設定

システム設定の概要

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

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

IP アドレスの検索方法

1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [システム情報 (System Information)] を選択します。

音声設定

Audio DefaultVolume

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：50

値スペース：整数（0 ～ 100）

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

Audio Microphones Mute Enabled

ビデオ システムでのマイク ミュートの動作を定義します。

必要なユーザ ロール：ADMIN

デフォルト値：True

値スペース：True/InCallOnly

True：音声ミュートが使用可能になります。

InCallOnly：音声ミュートはデバイスがコール中の場合にだけ使用できます。アイドル状態のときは、マイク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。

Audio SoundsAndAlerts RingTone

着信コールに使用する呼び出し音を定義します。

必要なユーザ ロール：ADMIN、USER

デフォルト値：Sunrise

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

リストから呼び出し音を選択します。

Audio SoundsAndAlerts RingVolume

着信コールの着信音量を定義します。

必要なユーザ ロール：ADMIN、USER

デフォルト値：50

値スペース：整数（0 ～ 100）

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

Audio Input MicrophoneMode

この設定は DX80 にのみ適用されます。

DX80 の両方の脚にマイクが搭載されています。マイク モードを Focused に設定すると、両方のマイクを組み合わせて指向性を上げることができます。これにより、室内から拾うノイズが抑制されます。この状態でビデオ システムの正面に座ると、マイクが拾う音質が改善します。システムの真正面に座っていない人たちの声は抑制されます。

マイクロフォン モードを [ワイド (Wide)] に設定すると、システムは他のシステムと同様に動作します。横に座っている人の声は聞こえますが、室内から拾う雑音も大きくなります。

自分だけで話す場合は、Focused モードを使用することをお勧めします。システムの前で複数人が話す場合は、Wide モードを使用してください。

必要なユーザ ロール: ADMIN

デフォルト値: Wide

値スペース: Focused/Wide

Focused:指向性を上げます。ビデオ システムの正面にない音源からの音は抑制されます。

Wide:通常の音の感度によるデフォルトのマイク動作。

CallHistory 設定

CallHistory Mode

発信または受信されたコールに関する情報を保存するかどうかを決定します（通話履歴）。これには、不在着信と応答されなかったコールが含まれます。これにより、ユーザ インターフェイスの Recents リストにコールが表示されるかどうかが決まります。

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：新しいエントリは通話履歴に追加されません。

On：新しいエントリが通話履歴リストに保存されます。

会議 設定

Conference ActiveControl Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：Auto

値スペース：Auto/Off

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

Off：アクティブ コントロールはディセーブルです。

Conference AutoAnswer Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

Off：着信コールに応答するには、[応答（Answer）] をタップする必要があります。

On：通話中でない限り、システムが自動的に着信コールに応答します。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。

Conference AutoAnswer Mute

着信コールへの自動応答時にマイクをミュートするかどうかを定義します。AutoAnswer Modeが有効にされている必要があります。

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

Off：着信コールはミュートにされません。

On：着信コールは自動的に応答されるときミュートにされます。

Conference AutoAnswer Delay

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）。AutoAnswer Mode が有効にされている必要があります。

必要なユーザ ロール：ADMIN

デフォルト値：0

値スペース：整数（0 ～ 50）

自動応答遅延（秒単位）。

Conference CallProtocolIPStack

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

必要なユーザ ロール：ADMIN

デフォルト値：Dual

値スペース：Dual/IPv4/IPv6

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

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

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

Conference DefaultCall 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 コール レートを定義します。

必要なユーザ ロール: ADMIN

デフォルト値: 3072

値スペース: 整数(64 ～ 3072)

デフォルトのコール レート(帯域)(kbps)。

Conference DoNotDisturb DefaultTimeout

この設定はサイレント セッションのデフォルト期間、つまり着信コールが拒否され、不在履歴として登録される時間を決定します。セッションは、ユーザ インターフェイスを使用して早期に終了できます。デフォルト値は 60 分です。

必要なユーザ ロール: ADMIN

デフォルト値: 60

値スペース: 整数(1 ～ 1440)

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(最大 1440 分(24 時間))。

Conference Encryption Mode

会議の暗号化モードを定義します。会議が開始されると、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 キーがビデオ システムにインストールされていない場合、暗号化モードは常に Off になります。

必要なユーザ ロール: ADMIN

デフォルト値: BestEffort

値スペース: Off/On/BestEffort

Off:システムは、暗号化を使用しません。

On:システムは、暗号化されたコールだけを許可します。

BestEffort:システムは暗号化を可能な限り使用します。

>ポイント ツー ポイント コール:遠端(相手先)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 MultiSite 会議を実現するためには、すべてのサイトで暗号化をサポートしている必要があります。そうでない場合は、会議は暗号化されません。

Conference FarEndControl Mode

リモート側(遠端)にこちら側のビデオ ソースの選択とローカル カメラの制御(パン、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

デフォルト値: On

値スペース: Off/On

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

On: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。

Conference FarEndControl SignalCapability

遠端制御(H.224)信号機能モードを定義します。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off:遠端制御信号機能をディセーブルにします。

On:遠端制御信号機能をイネーブルにします。

Conference 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 レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには、Conference MaxTotalReceiveCallRate 設定を使用します。

必要なユーザ ロール: ADMIN

デフォルト値: 3072

値スペース: 整数(64 ～ 3072)

最大受信コール レート(帯域)(kbps)。

Conference MaxTransmitCallRate

コール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 レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには、Conference MaxTotalTransmitCallRate 設定を使用します。

必要なユーザ ロール: ADMIN

デフォルト値: 3072

値スペース: 整数 (64 ～ 3072)

最大送信コール レート (帯域) (kbps)。

Conference MaxTotalReceiveCallRate

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

必要なユーザ ロール: ADMIN

デフォルト値: 3072

値スペース: 整数 (64 ～ 3072)

最大受信コール レート (帯域) (kbps)。

Conference MaxTotalTransmitCallRate

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

必要なユーザ ロール: ADMIN

デフォルト値: 3072

値スペース: 整数 (64 ～ 3072)

最大送信コール レート (帯域) (kbps)。

Conference MicUnmuteOnDisconnect Mode

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

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

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

On: コールが切断された後にマイクロフォンのミュートを解除します。

Conference Presentation OnPlacedOnHold

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

必要なユーザ ロール: ADMIN

デフォルト値: NoAction

値スペース: Stop/NoAction

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。

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。

Conference VideoBandwidth Mode

会議ビデオ帯域幅モードを定義します。

必要なユーザ ロール: ADMIN

デフォルト値: Dynamic

値スペース: Dynamic/Static

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

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

Conference 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

デフォルト値: 5

値スペース: 整数(1 ～ 9)

プレゼンテーション チャネルの帯域幅の重みを設定します。

FacilityService 設定

FacilityService Service [1..5] Type

このソフトウェアのバージョンでは適用されません。

FacilityService Service [1..5] Name

このソフトウェアのバージョンでは適用されません。

FacilityService Service [1..5] Number

このソフトウェアのバージョンでは適用されません。

FacilityService Service [1..5] CallType

このソフトウェアのバージョンでは適用されません。

H323 設定

H323 Authentication Mode

H.323 プロファイルの認証モードを定義します。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off:システムは H.323 ゲートキーパーに対して自身の認証を試みませんが、通常の登録を試みます。

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

H323 Authentication LoginName

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

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、50)

認証ログイン名。

H323 Authentication Password

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

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、50)

認証パスワード。

H323 CallSetup Mode

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

H323 CallSetup Mode を Gatekeeper に設定した場合も、ダイレクト H.323 コールを発信できます。

必要なユーザ ロール: ADMIN

デフォルト値: Gatekeeper

値スペース: Direct/Gatekeeper

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

Gatekeeper: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 Gatekeeper Address も設定する必要があります。

H323 Encryption KeySize

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

必要なユーザ ロール：ADMIN

デフォルト値：Min1024bit

値スペース：Min1024bit/Max1024bit/Min2048bit

Min1024bit：最小サイズは 1024 ビットです。

Max1024bit：最大サイズは 1024 ビットです。

Min2048bit：最小サイズは 2048 ビットです。

H323 Gatekeeper Address

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

必要なユーザ ロール：ADMIN

デフォルト値：" "

値スペース：文字列（0、255）

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

H323 H323Alias E164

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

必要なユーザ ロール：ADMIN

デフォルト値：" "

値スペース：文字列（0、30）

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

H323 H323Alias ID

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

必要なユーザ ロール：ADMIN

デフォルト値：" "

値スペース：文字列（0、49）

H.323 エイリアス ID。例：「firstname.lastname@company.com」、「My H.323 Alias ID」

H323 NAT Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Auto/Off/On

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

Off：システムは、実際の IP アドレスをシグナリングします。

On：システムは、Q.931 および H.245 内にある実際の IP アドレスの代わりに、設定された H323 NAT アドレスをシグナリングします。NAT サーバ アドレスは、スタートアップ メニューで「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。

H323 NAT Address

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

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

*ポート 1720

*ポート 5555-6555

*ポート 2326-2487

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、64)

有効な IPv4 アドレスまたは IPv6 アドレス。

H323 PortAllocation

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

必要なユーザ ロール: ADMIN

デフォルト値: Dynamic

値スペース: Dynamic/Static

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

Static: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。

ログ 設定

Logging External Mode

ロギングでリモート syslog サーバ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
デフォルト値: Off

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

Logging External Protocol

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

必要なユーザ ロール: ADMIN
デフォルト値: SyslogTLS

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

Logging External Server Address

リモート syslog サーバのアドレス。

必要なユーザ ロール: ADMIN
デフォルト値: " "

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

Logging External Server Port

リモート syslog サーバがメッセージをリッスンするポート。0 (デフォルト) に設定すると、ビデオ システムでは標準の syslog ポートが使用されます。標準の syslog ポートは、syslog の場合は 514、TLS を介した syslog の場合は 6514 です。

必要なユーザ ロール: ADMIN
デフォルト値: 514

値スペース: 整数 (0 ～ 65535)
リモート syslog サーバで使用するポートの番号。0 は、ビデオ システムで標準の syslog ポートを使用することを意味します。

Logging Mode

ビデオ システムのロギング モード (syslog サービス) を定義します。無効にした場合は、syslog サービスが開始せず、イベント ログのほとんどが生成されません。履歴ログとコール ログは影響を受けません。

必要なユーザ ロール: ADMIN
デフォルト値: On

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

ネットワーク 設定

Network [1] DNS Domain Name

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、64）

DNS ドメイン名。

Network [1] 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、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [1] IEEE8021X Mode

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：Off

値スペース：Off/On

Off：802.1X 認証がディセーブルになります（デフォルト）。

On：802.1X 認証がイネーブルになります。

Network [1] IEEE8021X TlsVerify

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

この設定は、Network [1] IEEE8021X Eap Tls が有効（On）の場合にのみ適用されます。

必要なユーザ ロール：ADMIN、USER

デフォルト値：Off

値スペース：Off/On

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

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

Network [1] IEEE8021X UseClientCertificate

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：Off

値スペース：Off/On

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

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

Network [1] IEEE8021X Identity

802.1X 認証用のユーザ名を定義します。

必要なユーザ ロール：ADMIN、USER
デフォルト値：" "

値スペース：文字列（0、64）
802.1X 認証用のユーザ名。

Network [1] IEEE8021X Password

802.1X 認証用のパスワードを定義します。

必要なユーザ ロール：ADMIN、USER
デフォルト値：" "

値スペース：文字列（0、32）
802.1X 認証用のパスワード。

Network [1] IEEE8021X AnonymousIdentity

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

必要なユーザ ロール：ADMIN、USER
デフォルト値：" "

値スペース：文字列（0、64）
802.1X 匿名 ID 文字列。

Network [1] IEEE8021X Eap Md5

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

必要なユーザ ロール：ADMIN、USER
デフォルト値：On

値スペース：Off/On
Off：EAP-MD5 プロトコルはディセーブルになります。
On：EAP-MD5 プロトコルはイネーブルになります（デフォルト）。

Network [1] IEEE8021X Eap Ttls

TTLS（Tunneled Transport Layer Security）モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Funk Software および Certicom によって開発されました。通常 Agere Systems、Proxim および Avaya でサポートされます。

必要なユーザ ロール：ADMIN、USER
デフォルト値：On

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

Network [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、USER
デフォルト値：On

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

Network [1] IEEE8021X Eap Peap

Peap（保護拡張認証プロトコル）モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Microsoft、シスコと RSA Security により開発されました。

必要なユーザ ロール：ADMIN、USER

デフォルト値：On

値スペース：Off/On

Off：EAP-PEAP プロトコルはディセーブルになります。

On：EAP-PEAP プロトコルはイネーブルになります（デフォルト）。

Network [1] IPStack

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：Dual

値スペース：Dual/IPv4/IPv6

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

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

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

Network [1] 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、USER

デフォルト値：DHCP

値スペース：Static/DHCP

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

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

Network [1] IPv4 Address

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効な IPv4 アドレス。

Network [1] IPv4 Gateway

IPv4 ネットワーク ゲートウェイ アドレスを定義します。Network IPv4 Assignment が Static に設定されている場合に限り適用されます。

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効な IPv4 アドレス。

Network [1] IPv4 SubnetMask

IPv4 ネットワークのサブネット マスクを定義します。Network IPv4 Assignment が Static に設定されている場合に限り適用されます。

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効な IPv4 アドレス。

Network [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、USER

デフォルト値: Autoconf

値スペース: Static/DHCPv6/Autoconf

Static:コーデックおよびゲートウェイの IP アドレスは、Network IPv6 Address および Network IPv6 Gateway の各設定を使用して手動で設定する必要があります。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。

DHCPv6:オプションを含むすべての IPv6 アドレスは、DHCPv6 サーバから取得されます。詳細については 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。

Network [1] IPv6 Address

システムのスタティック IPv6 ネットワーク アドレスを定義します。Network IPv6 Assignment が Static に設定されている場合に限り適用されます。

必要なユーザ ロール: ADMIN、USER

デフォルト値: " "

値スペース: 文字列(0、64)

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

Network [1] IPv6 Gateway

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

必要なユーザ ロール: ADMIN、USER

デフォルト値: " "

値スペース: 文字列(0、64)

有効な IPv6 アドレス。

Network [1] IPv6 DHCPOptions

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

必要なユーザ ロール: ADMIN、USER

デフォルト値: On

値スペース: Off/On

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

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

Network [1] MTU

イーサネット MTU(最大伝送ユニット)サイズを定義します。MTU サイズがネットワーク 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。最小サイズは、IPv4 の場合が 576、IPv6 の場合が 1280 です。

必要なユーザ ロール: ADMIN、USER

デフォルト値: 1500

値スペース: 整数(576 ～ 1500)

MTU の値(バイト)を設定します。

Network [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、USER

デフォルト値: Diffserv

値スペース: Off/Diffserv

Off:QoS メソッドは使用されません。

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

Network [1] QoS Diffserv Audio

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

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：0

値スペース：整数（0 ～ 63）

IP ネットワーク内の音声パケットの優先順位を設定します。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。

Network [1] QoS Diffserv Video

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

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：0

値スペース：整数（0 ～ 63）

IP ネットワーク内のビデオ パケットの優先順位を設定します。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。

Network [1] QoS Diffserv Data

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

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：0

値スペース：整数（0 ～ 63）

IP ネットワーク内のデータ パケットの優先順位を設定します。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。

Network [1] QoS Diffserv Signalling

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

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

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：0

値スペース：整数（0 ～ 63）

IP ネットワーク内のシグナリング パケットの優先順位を設定します。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。

Network [1] QoS Diffserv ICMPv6

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

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

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：0

値スペース：整数（0 ～ 63）

IP ネットワーク内の ICMPv6 パケットの優先順位を設定します。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。

Network [1] QoS Diffserv NTP

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

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：0

値スペース：整数（0 ～ 63）

IP ネットワーク内の NTP パケットの優先順位を設定します。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。

Network [1] RemoteAccess Allow

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

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、255）

有効な IPv4 アドレスまたは IPv6 アドレス。

Network [1] Speed

イーサネット リンク速度を定義します。デフォルト値から変更しないことをお勧めします。デフォルト値では、ネットワークとネゴシエートして速度を自動的に設定します。自動ネゴシエーションを使用しない場合、選択する速度がご使用のネットワーク インフラストラクチャの最も近いスイッチでサポートされていることを確認してください。

必要なユーザ ロール：ADMIN、USER

デフォルト値：Auto

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

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。

Network [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定義します。

必要なユーザ ロール: ADMIN、USER

デフォルト値: On

値スペース: Off/On

Off:ビデオ パケットをリンク速度で送信します。

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

Network [1] VLAN Voice Mode

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

必要なユーザ ロール: ADMIN、USER

デフォルト値: Auto

値スペース: Auto/Manual/Off

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

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

Off:VLAN はイネーブルになりません。

Network [1] VLAN Voice VlanId

VLAN 音声 ID を定義します。この設定は、Network VLAN Voice Mode が [手動(Manual)] に設定されている場合にだけ有効になります。

必要なユーザ ロール: ADMIN、USER

デフォルト値: [1]

値スペース: 整数(1 ～ 4094)

VLAN 音声 ID を設定します。

NetworkServices 設定

NetworkServices CDP Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：CDP デーモンはディセーブルです。

On：CDP デーモンはイネーブルです。

NetworkServices H323 Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

Off：H.323 コールの発信と受信の可能性をディセーブルにします。

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

NetworkServices HTTP Mode

HTTP または HTTPS（HTTP Secure）プロトコルを使用したビデオ システムへのアクセスを許可するかどうかを定義します。ビデオ システムの Web インターフェイスでは HTTP または HTTPS が使用されることに注意してください。この設定が Off になっている場合は、Web インターフェイスを使用できません。

セキュリティを強化する（要求および Web サーバから返されるページの暗号化と復号化）には、HTTPS のみを許可します。

必要なユーザ ロール：ADMIN

デフォルト値：HTTP+HTTPS

値スペース：Off/HTTP+HTTPS/HTTPS

Off：HTTP または HTTPS を介したビデオ システムへのアクセスは許可されません。

HTTP+HTTPS：HTTP および HTTPS を介したビデオ システムへのアクセスは、両方とも許可されます。

HTTPS：HTTPS を介したビデオ システムへのアクセスは許可されますが、HTTP を介したアクセスは許可されません。

NetworkServices HTTPS VerifyServerCertificate

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

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

Off：サーバ証明書を確認しません。

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

NetworkServices HTTPS VerifyClientCertificate

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

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

Off：クライアント証明書を確認しません。

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

NetworkServices 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（CRLs）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

デフォルト値：Off

値スペース：Off/On

Off：OCSP サポートをディセーブルにします。

On：OCSP サポートをイネーブルにします。

NetworkServices HTTPS OCSP URL

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

必要なユーザ ロール：ADMIN

デフォルト値：" "

値スペース：文字列（0、255）

有効な URL。

NetworkServices NTP Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：Auto

値スペース：Auto/Manual/Off

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

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

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

NetworkServices NTP Server [1..3] Address

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

必要なユーザ ロール：ADMIN

デフォルト値：0.tandberg.pool.ntp.org

値スペース：文字列（0、255）

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

NetworkServices SIP Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：SIP コールの発信と受信の可能性をディセーブルにします。

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

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

デフォルト値: ReadOnly

値スペース: Off/ReadOnly/ReadWrite

Off:SNMP ネットワーク サービスをディセーブルにします。

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

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

NetworkServices SNMP Host [1..3] Address

最大 3 つの SNMP マネージャのアドレスを定義します。

システムの SNMP エージェント(コーデック内)は、システム ロケーションやシステム接点についてなど、SNMP マネージャ(PC プログラムなど)からの要求に応答します。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

デフォルト値: " "

値スペース: 文字列(0、255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

NetworkServices SNMP CommunityName

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

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、50)

SNMP コミュニティ名。

NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システム接点の名前を定義します。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、50)

SNMP システム接点の名前。

NetworkServices SNMP SystemLocation

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

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、50)

SNMP システム ロケーションの名前。

NetworkServices SSH Mode

SSH（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

デフォルト値：On

値スペース：Off/On

Off：SSH プロトコルはディセーブルになります。

On：SSH プロトコルはイネーブルになります（デフォルト）。

NetworkServices SSH 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

デフォルト値：On

値スペース：Off/On

Off：SSH 公開キーは許可されません。

On：SSH 公開キーが許可されます。

NetworkServices Telnet Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

Off：Telnet プロトコルはディセーブルになります。これが出荷時の設定です。

On：Telnet プロトコルはイネーブルになります。

NetworkServices WelcomeText

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

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

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

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

NetworkServices WIFI Allowed

組み込みの Wi-Fi アダプタが装備されている DX ビデオ システムは、イーサネットまたは Wi-Fi のいずれかを通じてネットワークに接続できます。これらのシステムは、イーサネットと Wi-Fi の両方に同時に接続することはできません。これらのシステムでは、標準規格の IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、および IEEE 802.11n がサポートされます。セキュリティのタイプは、WPA-PSK TKIP、WPA2-PSK AES、およびオープン（セキュリティで保護されない）がサポートされます。

デフォルトではイーサネットと Wi-Fi の両方が許可されます。この設定は、Wi-Fi の使用を禁止する場合に使用します。

一部の DX のビデオ システムは、組み込みの Wi-Fi アダプタ（ビデオ システムの背面の定格ラベルにある PID は、これらの装置の場合 CP-DX80-NR-K9= または CP-DX70-W-NR-K9= です）なしで販売されています。これらのシステムでは、Wi-Fi を設定するためのオプションを何も取得しません。

必要なユーザ ロール：ADMIN

デフォルト値：True

値スペース：False/True

False：Wi-Fi は使用できません。イーサネットを通じてネットワークに接続する必要があります。

True：イーサネットと Wi-Fi の両方が許可されます。

NetworkServices WIFI Enabled

ビデオ システムが Wi-Fi を通じてネットワークに接続することが許可されている（NetworkServices WIFI Allowed を参照）限り、この設定を使用して Wi-Fi を有効または無効にすることができます。

イーサネットと Wi-Fi を同時に使用することはできません。イーサネット ケーブルが接続されているときに Wi-Fi の設定を試みる場合は、イーサネット ケーブルのプラグを外す必要があります。Wi-Fi に接続されているときにイーサネット ケーブルを接続した場合、イーサネットが優先されます。イーサネット ケーブルのプラグを外した場合、ビデオ システムは最後に接続された Wi-Fi ネットワークに自動的に接続されます（可能な場合）。

必要なユーザ ロール：ADMIN

デフォルト値：いいえ（False）

値スペース：False/True

False：Wi-Fi は無効になります。

True：Wi-Fi は有効になります。

NetworkServices XMLAPI Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：XML API はディセーブルになります。

On：XML API はイネーブルになります（デフォルト）。

周辺機器 設定

Peripherals Pairing Ultrasound Volume Mode

この設定はインテリジェント プロキシミティ機能に適用されます。設定をデフォルト値で維持します。

必要なユーザ ロール: ADMIN

デフォルト値: Dynamic

値スペース: Dynamic/Static

Dynamic:ビデオ システムは超音波の音量を動的に調整します。音量は Peripherals Pairing Ultrasound Volume MaxLevel 設定で定義された最大レベルまで変化します。

Static:シスコから推奨された場合にのみ使用してください。

Peripherals Pairing Ultrasound Volume MaxLevel

この設定はインテリジェント プロキシミティ機能に適用されます。超音波ペアリング メッセージの最大音量を設定します。Peripherals Pairing Ultrasound Volume Mode 設定を参照してください。

必要なユーザ ロール: ADMIN

デフォルト値: DX80:70 DX70:60

値スペース: DX80:整数(0 ～ 90) DX70:整数(0 ～ 60)

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

Peripherals Profile ControlSystems

サードパーティ(Crestron 社や AMX 社など)製の制御システムがビデオ システムに接続されていると想定されるかどうかを定義します。この情報はビデオ システムの診断サービスで使用されます。接続されている制御システムの数がこの設定に一致しない場合、診断サービスによって設定が不一致と報告されます。サポートされるサードパーティ製の制御システムは、1 台のみであることに注意してください。

1 に設定すると、xCommand の Peripherals Pair コマンドと HeartBeat コマンドを使用して、制御システムでビデオ システムにハート ビートを送信する必要があります。この送信を行わないと、ビデオ システムが制御システムへの接続を失ったという警告が室内制御拡張機能によって表示されます。

必要なユーザ ロール: ADMIN

デフォルト値: NotSet

値スペース: 1/NotSet

1:1 台のサードパーティ製制御システムがビデオ システムに接続されている必要があります。

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

Phonebook 設定

Phonebook Server [1] ID

外部の電話帳の名前を定義します。

必要なユーザ ロール: ADMIN
デフォルト値: " "

値スペース: 文字列(0、64)
外部の電話帳の名前。

Phonebook Server [1] Type

電話帳サーバの種類を選択します。

必要なユーザ ロール: ADMIN
デフォルト値: Off

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

Phonebook Server [1] URL

外部電話帳サーバのアドレス(URL)を定義します。

必要なユーザ ロール: ADMIN
デフォルト値: " "

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

プロビジョニング 設定

Provisioning Connectivity

この設定は、プロビジョニング サーバからの内部または外部の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、USER

デフォルト値: Auto

値スペース: Internal/External/Auto

Internal:内部コンフィギュレーションを要求します。

External:外部コンフィギュレーションを要求します。

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

Provisioning Mode

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

必要なユーザ ロール: ADMIN、USER

デフォルト値: Auto

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

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

Auto:プロビジョニング サーバを自動的に選択します。

CUCM:CUCM(Cisco Unified Communications Manager)からビデオ システムに設定をプッシュします。

Edge:CUCM(Cisco Unified Communications Manager)からビデオ システムに設定をプッシュします。システムは Collaboration Edge インフラストラクチャを経由して CUCM に接続します。

Spark:Spark からビデオ システムに設定をプッシュします。

TMS:TMS(Cisco TelePresence Management System)からビデオ システムに設定をプッシュします。

VCS:VCS(Cisco TelePresence Video Communication Server)からビデオ システムに設定をプッシュします。

Provisioning LoginName

これは、プロビジョニング サーバとの間でビデオ システム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。

必要なユーザ ロール: ADMIN、USER

デフォルト値: " "

値スペース: 文字列(0、80)

有効なユーザ名。

Provisioning Password

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効なパスワード。

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、USER

デフォルト値：POST

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。

Provisioning ExternalManager Address

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

外部マネージャのアドレス（およびパス）が設定されている場合、システムはスタートアップ時にこのアドレスにメッセージを送信します。このメッセージを受信すると、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、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Provisioning ExternalManager AlternateAddress

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、64）

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

Provisioning ExternalManager Protocol

要求を外部マネージャ/プロビジョニング システムに送信するときに HTTP（非セキュア通信）プロトコルを使用するか、HTTPS（セキュア通信）プロトコルを使用するかを定義します。

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：HTTP

値スペース：HTTPS/HTTP

HTTPS：HTTPS を介して要求を送信します。

HTTP：HTTP を介して要求を送信します。

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定義します。いくつかの管理サービスが同じサーバに存在する、つまり同じ外部マネージャのアドレスを共有する場合、この設定が必要です。

必要なユーザ ロール：ADMIN、USER

デフォルト値：" "

値スペース：文字列（0、255）

外部マネージャ/プロビジョニング システムへの有効なパス。

Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを定義します。

必要なユーザ ロール: ADMIN、USER
デフォルト値: " "

値スペース: 文字列 (0、64)
有効なドメイン名。

プロキシミティ 設定

Proximity Mode

ビデオ システムが超音波ペアリング メッセージを発するかどうかを決定します。

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：Off

値スペース：Off/On

Off：ビデオ システムは超音波を発しないため、プロキシミティ サービスを使用できません。

On：ビデオ システムが超音波を発し、プロキシミティ クライアントはビデオ システムが近くにあることを検出できます。有効化されたプロキシミティ サービスを使用できます。

Proximity Services CallControl

プロキシミティ クライアントの基本的なコール制御機能を有効または無効にします。この設定を有効にすると、プロキシミティ クライアントを使用してコールを制御できます（ダイヤル、ミュート、音量の調整、通話の切断など）。このサービスは、モバイル デバイス（iOS および Android）でサポートされます。この設定を有効にするには、Proximity Mode を On にする必要があります。

必要なユーザ ロール：ADMIN、USER

デフォルト値：Disabled

値スペース：Enabled/Disabled

Enabled：プロキシミティ クライアントからのコール制御が有効になります。

Disabled：プロキシミティ クライアントからのコール制御が無効になります。

Proximity Services ContentShare FromClients

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：Enabled

値スペース：Enabled/Disabled

Enabled：Proximity クライアントからのコンテンツ共有がイネーブルになります。

Disabled：Proximity クライアントからのコンテンツ共有がディセーブルになります。

Proximity Services ContentShare ToClients

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

必要なユーザ ロール：ADMIN、USER

デフォルト値：Disabled

値スペース：Enabled/Disabled

Enabled：Proximity クライアントに対するコンテンツ共有がイネーブルになります。

Disabled：Proximity クライアントに対するコンテンツ共有がディセーブルになります。

RoomReset 設定

RoomReset Control

適用なし

RTP 設定

RTP Ports Range Start

RTP ポート範囲の最初のポートを定義します。

デフォルトで、RTP および RTCP メディア データに 2326 ～ 2487 の範囲の UDP ポートを使用します。各メディア チャネルは RTP および RTCP に 2 つの隣接ポートを使用します。UDP ポート範囲に必要なポートの数は、エンドポイントで対応できる同時コールの数に基づいています。

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

デフォルト値：2326

値スペース：整数（1024 ～ 65438）

RTP ポート範囲内で最初のポートを設定します。

RTP Ports Range Stop

RTP ポート範囲の最後のポートを定義します。

デフォルトで、RTP および RTCP メディア データに 2326 ～ 2487 の範囲の UDP ポートを使用します。各メディア チャネルは RTP および RTCP に 2 つの隣接ポートを使用します。UDP ポート範囲に必要なポートの数は、エンドポイントで対応できる同時コールの数に基づいています。

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

デフォルト値：2486

値スペース：整数（1120 ～ 65535）

RTP ポート範囲内で最後のポートを設定します。

セキュリティ 設定

Security Audit Logging Mode

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

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

必要なユーザ ロール: AUDIT

デフォルト値: Off

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

Off:監査ロギングは実行されません。

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。

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

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

Security Audit OnError Action

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

必要なユーザ ロール: AUDIT

デフォルト値: Ignore

値スペース: Halt/Ignore

Halt:停止状態が検出された場合、システム コーデックはリブートし、停止状態が過ぎ去るまではオーディタだけが装置の操作を許可されます。停止状態が過ぎ去ると、監査ログは syslog サーバに再スプールされます。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。

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

Security Audit Server Address

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

必要なユーザ ロール: AUDIT

デフォルト値: " "

値スペース: 文字列 (0、255)

有効な IPv4 アドレスまたは IPv6 アドレス。

Security Audit Server Port

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

デフォルト値: 514

値スペース: 整数(0 ～ 65535)

監査サーバ ポートを設定します。

Security Audit Server PortAssignment

監査ログは syslog サーバに送信されます。外部 syslog サーバのポート番号の割り当て方法を定義できます。この設定は、Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。使用しているポート番号を確認するために、Security Audit Server Port 状態をチェックできます。Web インターフェイスで [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

デフォルト値: Auto

値スペース: Auto/Manual

Auto:Security Audit Logging Mode が 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。

Manual:Security Audit Server Port)] 設定で定義されたポート値を使用します。

Security Session InactivityTimeout

ユーザが Web、Telnet、または SSH セッションから自動的にログ アウトされるまでに、システムでユーザの非アクティブ状態を受け入れる時間の長さを定義します。

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数(0 ～ 10000)

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

Security Session MaxSessionsPerUser

ユーザ 1 人あたりの最大同時セッション数。デフォルト値の 0 は、ハード リミットがないことを意味します。セッションではリソースを消費するため一定の制限がありますが、この制限はさまざまな基準に応じて異なることがあります。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数(0 ～ 100)

ユーザ 1 人あたりの最大セッション数。0 は、ハード リミットがないことを意味します。

Security Session MaxTotalSessions

合計の同時セッションの最大数。デフォルト値の 0 は、ハード リミットがないことを意味します。セッションではリソースを消費するため一定の制限がありますが、この制限はさまざまな基準に応じて異なることがあります。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数(0 ～ 100)

合計のセッションの最大数。0 は、ハード リミットがないことを意味します。

Security Session ShowLastLogon

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

On:最後のセッションに関する情報を表示します。

Off:最後のセッションに関する情報を表示しません。

SerialPort 設定

SerialPort Mode

シリアル ポート（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
デフォルト値：On

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

SerialPort LoginRequired

シリアル ポートに接続するときにログインが必要かどうかを定義します。

必要なユーザ ロール：ADMIN
デフォルト値：On

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

SIP 設定

SIP 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
デフォルト値：Off

値スペース：Off/On
Off：ANAT をディセーブルにします。
On：ANAT をイネーブルにします。

SIP Authentication UserName

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

必要なユーザ ロール：ADMIN
デフォルト値：" "

値スペース：文字列（0、128）
有効なユーザ名。

SIP Authentication Password

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

必要なユーザ ロール：ADMIN
デフォルト値：" "

値スペース：文字列（0、128）
有効なパスワード。

SIP DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール：ADMIN
デフォルト値：Auto

値スペース：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。
Auto：システムは、TLS、TCP、UDP の順序でトランスポート プロトコルを使用して接続を試みます。

SIP DisplayName

これが設定される場合、着信コールは SIP URI ではなく、表示名を報告します。

必要なユーザ ロール：ADMIN
デフォルト値：" "

値スペース：文字列（0、550）
SIP URI の代わりに表示される名前。

SIP Ice Mode

ICE (Interactive Connectivity Establishment、RFC 5245) は、最適化されたメディア パスの検出にビデオ システムで使用できる NAT トラバーサル ソリューションです。このため、音声とビデオの最短ルートがビデオ システム間で常に確保されます。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/Off/On

Auto:TURN サーバを指定した場合に ICE が有効になります。指定しない場合 ICE は無効になります。

Off:ICE は無効になります。

On:ICE は有効になります。

SIP Ice DefaultCandidate

ICE プロトコルでは、使用するメディア ルートを決定するための時間が必要です (最大でコールの最初の 5 秒)。この間、ビデオ システムのメディアは、この設定で定義されたデフォルトの宛先に送信されます。

必要なユーザ ロール: ADMIN

デフォルト値: Host

値スペース: Host/Rflx/Relay

Host:ビデオ システムのプライベート IP アドレスにメディアを送信します。

Rflx: TURN サーバで認識される、ビデオ システムのパブリック IP アドレスにメディアを送信します。

Relay:TURN サーバに割り当てられている IP アドレスとポートにメディアを送信します。

SIP Line

Cisco Unified Communications Manager (CUCM) に登録すると、エンドポイントを共有回線の一部に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

デフォルト値: Private

値スペース: Private/Shared

Shared:システムは共有回線の一部であるため、ディレクトリ番号を他のデバイスと共有します。

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

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

デフォルト値: On

値スペース: Off/On

Off:SIP TCP/UDP ポートでの着信接続のリッスンをオフにします。

On:SIP TCP/UDP ポートでの着信接続のリッスンをオンにします。

SIP Mailbox

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

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列 (0、255>)

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

SIP 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 Dual に設定されていて、ネットワークに優先 IP バージョンを選択するメカニズムがない場合にのみ使用可能です。

必要なユーザ ロール: ADMIN

デフォルト値: IPv4

値スペース: IPv4/IPv6

IPv4:メディアの優先 IP バージョンは IPv4 です。

IPv6:メディアの優先 IP バージョンは IPv6 です。

SIP PreferredIPSignaling

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

必要なユーザ ロール: ADMIN

デフォルト値: IPv4

値スペース: IPv4/IPv6

IPv4:シグナリングの優先 IP バージョンは IPv4 です。

IPv6:シグナリングの優先 IP バージョンは IPv6 です。

SIP Proxy [1..4] Address

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

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

SIP TlsVerify

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off:検証せずに TLS 接続を許可するには、Off に設定します。TLS 接続は、サーバから受信した x.509 証明書をローカル CA リストと確認せずにセットアップできます。これは通常、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。

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

SIP Turn DiscoverMode

検出モードを定義し、DNS で利用可能な TURN サーバの検索に対してアプリケーションをイネーブル/ディセーブルにします。コールを発信する前に、システムはポート割り当てが可能かどうかを確認します。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off:検出モードをディセーブルにします。

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

SIP Turn DropRflx

DropRflx は、リモート エンドポイントが同じネットワークにない場合に限り、TURN リレー経由でエンドポイントにメディアを強制させます。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off:DropRflx をディセーブルにします。

On:リモート エンドポイントが別のネットワークにある場合、TURN リレー経由でメディアを強制します。

SIP Turn Server

TURN (Traversal Using Relay NAT) サーバのアドレスを定義します。これはメディア リレー フォールバックとして使用されるほか、エンドポイント固有のパブリック IP アドレスを検出するためにも使用されます。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列 (0、255)

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

SIP Turn UserName

TURN サーバへのアクセスに必要なユーザ名を定義します。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列 (0、128)

有効なユーザ名。

SIP Turn Password

TURN サーバへのアクセスに必要なパスワードを定義します。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列 (0、128)

有効なパスワード。

SIP Type

ベンダーまたはプロバイダーに対する SIP 拡張および特別な動作をイネーブルにします。

必要なユーザ ロール: ADMIN

デフォルト値: Standard

値スペース: Standard/Cisco

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

SIP URI

SIP URI (Uniform Resource Identifier) は、ビデオ システムの識別に使用されるアドレスです。URI が登録され、SIP サービスによりシステムへの着信コールのルーティングに使用されます。SIP URI 構文は RFC 3261 で定義されています。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列 (0、255)

SIP URI 構文に準拠したアドレス (URI)。

Standby 設定

Standby AudioMotionDetection

ビデオ システムで、人がその近くにいることを自動的に検出できます。この機能がオンになっている場合、誰かが検出されるとビデオ システムはスタンバイ状態から動作状態に復帰します。

必要なユーザ ロール: ADMIN
デフォルト値: Off

値スペース: Off/On
Off:ビデオ システムの近くに人がいることの検出がオフになります。
On:ビデオ システムの近くに人がいることの検出がオンになります。

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定義します。

必要なユーザ ロール: ADMIN
デフォルト値: On

値スペース: Off/On
Off:システムはスタンバイ モードを開始しません。
On:Standby Delay がタイム アウトになると、システムはスタンバイ モードになります。Standby Delay を適切な値に設定する必要があります。

Standby Delay

スタンバイ モードに入る前に、システムがアイドル モードのまま経過する時間の長さ(分単位)を定義します。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
デフォルト値: 10

値スペース: 整数(1 ～ 480)
スタンバイ遅延(分)を設定します。

SystemUnit 設定

SystemUnit Name

システム名を定義します。コーデックが SNMP エージェントとして機能している場合に、システム名は DHCP 要求でホスト名として送信されます。

必要なユーザ ロール: ADMIN
デフォルト値: " "

値スペース: 文字列(0、50)
システム名を定義します。

時刻設定

Time TimeFormat

時刻形式を定義します。

必要なユーザ ロール: ADMIN、USER
デフォルト値: 24H

値スペース: 24H/12H
24H:24 時間の時間フォーマットを設定します。
12H:12 時間(AM/PM)の時間フォーマットを設定します。

Time DateFormat

日付形式を定義します。

必要なユーザ ロール: ADMIN、USER
デフォルト値: DD_MM_YY

値スペース: DD_MM_YY/MM_DD_YY/YY_MM_DD
DD_MM_YY:2010 年 1 月 30 日は「30.01.10」と表示されます。
MM_DD_YY:2010 年 1 月 30 日は「01.30.10」と表示されます。
YY_MM_DD:2010 年 1 月 30 日は「10.01.30」と表示されます。

タイム ゾーン

ビデオ システムの地理的な場所のタイム ゾーンを定義します。値スペースの情報は、tz データベース（別名：IANA タイムゾーン データベース）から取得しています。

必要なユーザ ロール：ADMIN、USER

デフォルト値：Etc/UTC

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_Nelson、America/Fort_Wayne、America/Fortaleza、America/Glace_Bay、America/Godthab、America/Goose_Bay、America/Grand_Turk、America/Grenada、America/Guadeloupe、America/Guatemala、America/Guayaquil、America/Guyana、America/Halifax、America/Havana、America/Hermosillo、America/Indiana/Indianapolis、America/Indiana/Knox、America/Indiana/Marengo、America/Indiana/Petersburg、America/Indiana/Tell_City、America/Indiana/Vevay、America/Indiana/Vincennes、America/Indiana/Winamac、America/Indianapolis、America/Inuvik、America/Iqaluit、America/Jamaica、America/Jujuy、America/Juneau、America/Kentucky/Louisville、America/Kentucky/Monticello、America/Knox_IN、America/Kralendijk、America/La_Paz、America/Lima、America/Los_Angeles、America/Louisville、America/Lower_Princes、America/Maceio、America/Managua、America/Manaus、America/Marigot、America/Martinique、America/Matamoros、America/Mazatlan、America/Mendoza、America/Menominee、America/Merida、America/Metlakatla、America/Mexico_City、America/Miquelon、America/Moncton、America/Monterrey、America/Montevideo、America/Montreal、America/Montserrat、America/Nassau、America/New_York、America/Nipigon、America/Nome、America/Noronha、America/North_Dakota/Beulah、America/North_Dakota/Center、America/North_Dakota/New_Salem、America/Ojinaga、America/Panama、America/Pangnirtung、America/Paramaribo、America/Phoenix、America/Port-au-Prince、America/Port_of_Spain、America/Porto_Acre、America/Porto_Velho、America/Puerto_Rico、America/Rainy_River、America/Rankin_Inlet、America/Recife、America/Regina、America/Resolute、America/Rio_Branco、America/Rosario、America/Santa_Isabel、America/Santarem、America/Santiago、America/Santo_Domingo、America/Sao_Paulo、America/Scoresbysund、America/Shiprock、America/Sitka、America/St_Barthelemy、America/St_Johns、America/St_Kitts、America/St_Lucia、America/St_Thomas、America/St_Vincent、America/Swift_Current、America/Tegucigalpa、America/Thule、America/Thunder_Bay、America/Tijuana、America/Toronto、America/Tortola、America/Vancouver、America/Virgin、America/Whitehorse、America/Winnipeg、America/Yakutat、America/Yellowknife、Antarctica/Casey、Antarctica/Davis、Antarctica/DumontDUrville、Antarctica/Macquarie、Antarctica/Mawson、Antarctica/McMurdo、Antarctica/Palmer、Antarctica/Rothera、Antarctica/South_Pole、Antarctica/Syowa、Antarctica/Troll、Antarctica/Vostok、Arctic/Longyearbyen、Asia/Aden、Asia/Almaty、Asia/Amman、Asia/Anadyr、Asia/Aqtau、Asia/Aqtobe、Asia/Ashgabat、Asia/Ashkhabad、Asia/Baghdad、Asia/Bahrain、Asia/Baku、Asia/Bangkok、Asia/Barnaul、Asia/Beirut、Asia/Bishkek、Asia/Brunei、Asia/Calcutta、Asia/Chita、Asia/Choibalsan、Asia/Chongqing、Asia/Chungking、Asia/Colombo、Asia/Dacca、Asia/Damascus、Asia/Dhaka、Asia/Dili、Asia/Dubai、Asia/Dushanbe、Asia/Gaza、Asia/Harbin、Asia/Hebron、Asia/Ho_Chi_Minh、Asia/Hong_Kong、Asia/Hovd、Asia/Irkutsk、Asia/Istanbul、Asia/Jakarta、Asia/Jayapura、Asia/Jerusalem、Asia/Kabul、Asia/Kamchatka、Asia/Karachi、Asia/Kashgar、Asia/Kathmandu、Asia/Katmandu、Asia/Khandyga、Asia/Kolkata、Asia/Krasnoyarsk、Asia/Kuala_Lumpur、Asia/Kuching、Asia/Kuwait、Asia/Macao、Asia/Macau、Asia/Magadan、Asia/Makassar、Asia/Manila、Asia/Muscat、Asia/Nicosia、Asia/Novokuznetsk、Asia/Novosibirsk、Asia/Omsk、Asia/Oral、Asia/Phnom_Penh、Asia/Pontianak、Asia/Pyongyang、Asia/Qatar、Asia/Qyzylorda、Asia/Rangoon、Asia/Riyadh、Asia/Saigon、Asia/Sakhalin、Asia/Samarkand、Asia/Seoul、Asia/Shanghai、Asia/Singapore、Asia/Srednekolymsk、Asia/Taipei、Asia/Tashkent、Asia/Tbilisi、Asia/Tehran、Asia/Tel_Aviv、Asia/Thimbu、Asia/Thimphu、Asia/Tokyo、Asia/Tomsk、Asia/Ujung_Pandang、Asia/Ulaanbaatar、Asia/Ulan_Bator、Asia/Urumqi、Asia/Ust-Nera、Asia/Vientiane、Asia/Vladivostok、Asia/Yakutsk、Asia/Yekaterinburg、Asia/Yerevan、Atlantic/Azores、Atlantic/Bermuda、Atlantic/Canary、Atlantic/Cape_Verde、Atlantic/Faeroe、Atlantic/Faroe、Atlantic/Jan_Mayen、Atlantic/Madeira、Atlantic/Reykjavik、Atlantic/South_Georgia、Atlantic/St_Helena、Atlantic/Stanley、Australia/ACT、Australia/Adelaide、Australia/Brisbane、Australia/Broken_Hill、Australia/Canberra、Australia/Currie、Australia/Darwin、Australia/Eucla、Australia/Hobart、Australia/LHI、Australia/Lindeman、Australia/Lord_Howe、Australia/Melbourne、Australia/NSW、Australia/North、Australia/Perth、Australia/Queensland、Australia/South、Australia/Sydney、Australia/Tasmania、Australia/Victoria、Australia/West、Australia/Yancowinna、Brazil/Acre、Brazil/DeNoronha、Brazil/East、Brazil/West、CET、CST6CDT、Canada/Atlantic、Canada/Central、Canada/East-Saskatchewan、Canada/Eastern、Canada/Mountain、Canada/Newfoundland、Canada/Pacific、Canada/Saskatchewan、Canada/Yukon、Chile/Continental、Chile/EasterIsland、Cuba、EET、EST、EST5EDT、Egypt、Eire、Etc/GMT、Etc/GMT+0、Etc/GMT+1、Etc/GMT+10、Etc/GMT+11、Etc/GMT+12、Etc/GMT+2、Etc/GMT+3、Etc/GMT+4、Etc/GMT+5、Etc/GMT+6、Etc/GMT+7、Etc/GMT+8、Etc/GMT+9、Etc/GMT-0、Etc/GMT-1、Etc/GMT-10、Etc/GMT-11、Etc/GMT-12、Etc/GMT-13、Etc/GMT-14、Etc/GMT-2、Etc/GMT-3、Etc/GMT-4、Etc/GMT-5、Etc/

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

リストからタイム ゾーンを選択します。

UserInterface 設定

UserInterface ContactInfo Type

ホーム画面に表示される連絡先情報のタイプと、[設定(Settings)] アイコンをタップしたとき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

デフォルト値: Auto

値スペース: Auto/None/IPv4/IPv6/SipUri/SystemName/DisplayName

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、システム登録によって異なります。

None:連絡先情報を一切表示しません。

IPv4:システムの IPv4 アドレスを表示します。

IPv6:システムの IPv6 アドレスを表示します。

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

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

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

UserInterface KeyTones Mode

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

必要なユーザ ロール: ADMIN、USER

デフォルト値: Off

値スペース: Off/On

Off:キー トーンによる効果音はありません。

On:キー トーンによる効果音がオンになります。

UserInterface Language

画面のメニューとメッセージで使用する言語を選択します。

必要なユーザ ロール: ADMIN、USER

デフォルト値: English

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

リストから言語を選択します。

UserInterface OSD EncryptionIndicator

暗号化インジケータ(鍵)が画面に表示される時間の長さを定義します。暗号化された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

デフォルト値: Auto

値スペース: Auto/AlwaysOn/AlwaysOff

Auto:コールが暗号化されている場合は、「コールは暗号化されています(Call is encrypted)」という通知が 5 秒間表示され、コール中は暗号化インジケータ アイコンが表示されます。

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

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。

AlwaysOff:暗号化インジケータは画面上に表示されません。

UserInterface OSD Output

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

必要なユーザ ロール: ADMIN
デフォルト値: Auto

値スペース: Auto
Auto:オンスクリーン用の情報とインジケータをシステムの内蔵ディスプレイに送信します。

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 4 MByte です。カスタムの壁紙を使用した場合、予定されている会議のリストと時計がメイン ディスプレイから削除されます。

必要なユーザ ロール: ADMIN、USER
デフォルト値: Auto

値スペース: Auto/Custom/None
Auto:デフォルトの壁紙を使用します。
None:画面に背景イメージはありません。
Custom:画面の背景画像としてカスタムの壁紙を使用します。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。

UserInterface UserPreferences

適用なし

UserManagement 設定

UserManagement LDAP Mode

ビデオ システムでは、ユーザ名とパスワードの保存と検証を行う中心的な場所としての LDAP (Lightweight Directory Access Protocol) サーバの使用がサポートされます。この設定は、LDAP 認証を使用するかどうかを設定する場合に使用します。シスコの実装は、Microsoft Active Directory (AD) サービスで機能するかテストされています。

必要なユーザ ロール: ADMIN
デフォルト値: Off

値スペース: Off/On
Off:LDAP 認証は許可されません。
On:LDAP 認証を使用します。

UserManagement LDAP Server Address

LDAP サーバの IP アドレスまたはホスト名を設定します。

必要なユーザ ロール: ADMIN
デフォルト値: " "

値スペース: 文字列 (0、255)
有効な IPv4 アドレス、IPv6 アドレス、またはホスト名。

UserManagement LDAP Server Port

LDAP サーバに接続するためのポートを設定します。0 に設定した場合、選択したプロトコルのデフォルトを使用します (UserManagement LDAP Encryption 設定を参照)。

必要なユーザ ロール: ADMIN
デフォルト値: [0]

値スペース: 整数 (0 ～ 65535)
LDAP サーバのポート番号。

UserManagement LDAP Encryption

ビデオ システムと LDAP サーバ間の通信を保護する方法を定義します。ポート番号は、UserManagement LDAP Server Port 設定を使用してオーバーライドできます。

必要なユーザ ロール: ADMIN
デフォルト値: LDAPS

値スペース: LDAPS/None/STARTTLS
LDAPS:TLS (Transport Layer Security) を介してポート 636 で LDAP サーバに接続します。
None:暗号化なしでポート 389 で LDAP サーバに接続します。
STARTTLS:ポート 389 で LDAP サーバに接続してから、STARTTLS を送信して TLS 暗号化を有効にします。

UserManagement LDAP MinimumTLSVersion

許可される TLS (Transport Layer Security) プロトコルの最も低いバージョンを設定します。

必要なユーザ ロール: ADMIN
デフォルト値: TLSv1.2

値スペース: TLSv1.0/TLSv1.1/TLSv1.2
TLSv1.0:TLS バージョン 1.0 以上をサポートします。
TLSv1.1:TLS バージョン 1.1 以上をサポートします。
TLSv1.2:TLS バージョン 1.2 以上をサポートします。

UserManagement LDAP VerifyServerCertificate

ビデオ システムが LDAP サーバに接続すると、LDAP サーバはそれ自体の証明書を提示することによって、このビデオ システムに対してそれ自体を証明します。この設定は、ビデオ システムがサーバの証明書を確認するかどうかを指定する場合に使用します。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off:ビデオ システムは LDAP サーバの証明書を確認しません。

On:ビデオ システムは、LDAP サーバの証明書が信頼できる認証局(CA)によって署名されていることを確認する必要があります。CA は、事前にシステムにアップロードされた信頼できる CA のリストに登録されている必要があります。信頼できる CA のリストを管理するには、ビデオ システムの Web インターフェイスを使用します(アドミニストレータ ガイドで詳細を参照してください)。

UserManagement LDAP Admin Filter

LDAP フィルタを使用して管理者権限を付与するユーザを指定します。この設定を行うと、この設定が UserManagement LDAP Admin Group 設定よりも優先されます。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、1024)

この文字列の構文については LDAP の仕様を参照してください。例:" (CN=adminuser)"

UserManagement LDAP Admin Group

この AD(Active Directory)グループのメンバーには、管理者アクセス権が付与されます。この設定は、(memberOf:1.2.840.113556.1.4.1941:=<group name>)という指定の省略表現です。UserManagement LDAP Admin Filter が設定されている場合、この設定は無視されます。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、255)

AD グループの識別名。例:" CN=admin_group、OU=company groups、DC=company、DC=com"

UserManagement LDAP Attribute

指定されたユーザ名にマッピングするために使用する属性。設定しなかった場合は、sAMAccountName が使用されます。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、255)

属性名。

ビデオ設定

Video ActiveSpeaker DefaultPIPPosition

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

必要なユーザ ロール：ADMIN

デフォルト値：Current

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

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

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

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

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

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

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

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

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

Video DefaultLayoutFamily Local

ローカルで使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール：ADMIN

デフォルト値：Auto

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

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

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

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

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

Single：通話中のスピーカー、または（存在する場合）プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Video DefaultLayoutFamily Remote

リモート参加者が使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール: ADMIN
デフォルト値: Auto

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

Auto:ローカル レイアウト データベースによって指定される、デフォルト レイアウト ファミリが、リモート レイアウトとして使用されます。

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

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

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

Single:通話中のスピーカー、または(存在する場合)プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Video DefaultMainSource

メイン ビデオ ソースとして使用されるビデオ入力ソースを定義します。

必要なユーザ ロール: ADMIN、USER
デフォルト値: 1

値スペース: 1

メイン ビデオ ソースとして使用されるソースを設定します。

Video Input Connector [1..2] CameraControl Mode

カメラを制御できるかどうかを定義します。この値は、Connector 1(内蔵カメラ)と Connector 2(HDMI)の両方で固定されており、変更できません。

必要なユーザ ロール: ADMIN
デフォルト値: Off

値スペース: Off

Off:カメラ制御をディセーブルにします。

Video Input Connector [1..2] CameraControl CameraId

カメラ ID は、ビデオ入力に接続されているカメラの一意の ID です。

必要なユーザ ロール: ADMIN
デフォルト値: 1

値スペース: 1

カメラ ID は固定されており、変更できません。

Video Input Connector [1..2] 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
デフォルト値: Connector 1:camera　Connector 2:desktop

値スペース: Connector 1:camera　Connector 2:camera/desktop/document_camera/mediaplayer/PC/whiteboard/other

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。

desktop:この値は、ビデオ システムのモニタがこの入力に接続された PC またはラップトップのメイン画面の場合に使用します。この値を設定した場合、Video Input Connector [n] PresentationSelection 設定も desktop に設定する必要があります。

document_camera:ドキュメント カメラがビデオ入力に接続されている場合に使用します。

mediaplayer:メディア プレーヤーがビデオ入力に接続されている場合に使用します。

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。

whiteboard:ホワイトボード カメラがビデオ入力に接続されている場合に使用します。

other:他のオプションに該当しない場合に使用します。

Video Input Connector [1..2] Name

ビデオ入力コネクタの名前を定義します。

必要なユーザ ロール: ADMIN

デフォルト値: " "

値スペース: 文字列(0、50)

ビデオ入力コネクタの名前。

Video Input Connector [2] Quality

ビデオをエンコードして送信する場合は、高解像度と高フレーム レートとの間でトレード オフが生じます。一部のビデオ ソースでは、高フレーム レートが高解像度より重要である場合や、逆の場合もあります。この設定は、高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール: ADMIN

デフォルト値: Sharpness

値スペース: Motion/Sharpness

Motion:できるだけ高いフレーム レートにします。通常、多数の参加者がいる場合や画像の動きが激しい場合など、高フレーム レートが必要なときに使用されます。

Sharpness:できるだけ高い解像度にします。詳細なイメージやグラフィックに高い品質が必要な場合に使用されます。

Video Input Connector [1..2] OptimalDefinition Profile

この設定は、対応する Video Input Connector [n] Quality が 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、Normal または Medium プロファイルが推奨されます。ただし、光の条件が良い場合、特定のコール率の解像度を大きくするために、High プロファイルを設定できます。解像度は、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。

必要なユーザ ロール: ADMIN

デフォルト値: Medium

値スペース: Normal/Medium/High

Normal:照明が通常から不良の環境には、このプロファイルを使用します。解像度は控えめに設定されます。

Medium:安定した光条件および高品質なビデオ入力が必要です一部のコール レートの場合、これは高解像度へ移動できます。

High:優れた全体的なエクスペリエンスを実現するには、理想に近いビデオ会議の光の状態および高品質なビデオ入力が必要です。高い解像度が使用されます。

Video Input Connector [2] PresentationSelection

ビデオ入力にプレゼンテーション ソースを接続するときの、ビデオ システムの動作を定義します。

ビデオ システムがスタンバイ モードである場合、プレゼンテーション ソースを接続すると起動します。遠端（相手先）とプレゼンテーションを共有するには、この設定が AutoShare に設定されている場合を除き、追加のアクション（ユーザ インターフェイスで [共有（Share）] を選択する）が必要になります。

必要なユーザ ロール：ADMIN

デフォルト値：Desktop

値スペース：AutoShare/Desktop/Manual/OnConnect

AutoShare：通話中に、ビデオ入力のコンテンツは、ケーブルを接続したとき、またはソースが別の方法でアクティブにされたとき（たとえば、接続されたコンピュータがスリープ モードから動作状態に復帰したとき）に、ローカル画面とともに遠端（相手先）に自動的に表示されます。ユーザ インターフェイスで [共有（Share）] を選択する必要はありません。コールを発信またはコールに応答したときに、プレゼンテーション ソースがすでに接続されている場合は、ユーザ インターフェイスで [共有（Share）] を手動で選択する必要があります。

Desktop：ケーブルを接続したとき、またはソースが別の方法でアクティブにされたとき（たとえば、接続されたコンピュータがスリープ モードから動作状態に復帰したとき）に、ビデオ入力のコンテンツが画面に表示されます。この設定は、アイドル状態のときと通話中のときの両方に適用されます。また、ビデオ入力のコンテンツは、コールを終了しても、終了時にその入力がアクティブの入力であった場合は画面に残ります。

Manual：ビデオ入力のコンテンツは、ユーザ インターフェイスで [共有（Share）] を選択するまで画面に表示されません。

OnConnect：ビデオ入力のコンテンツは、ケーブルを接続したとき、またはソースが別の方法でアクティブにされたとき（たとえば、接続されたコンピュータがスリープ モードから動作状態に復帰したとき）に画面に表示されます。それ以外の場合は、Manual モードと同じ動作です。

Video Input Connector [2] 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。

必要なユーザ ロール：ADMIN

デフォルト値：Auto

値スペース：Auto/Full/Limited

Auto：RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて自動的に選択されます。CE ビデオ形式は、限定された量子化範囲レベルを使用します。IT ビデオ形式は、完全な量子化範囲レベルを使用します。

Full：完全な量子化の範囲。R、G、B の量子化範囲にはすべてのコード値（0 ～ 255）が含まれます。これは CEA-861-E で規定されています。

Limited：限定された量子化の範囲。極端なコード値を除いた R、G、B の量子化範囲（16 ～ 235）。これは CEA-861-E で規定されています。

Video Input Connector [1..2] Visibility

ユーザ インターフェイスのメニューにあるビデオ入力コネクタの表示を定義します。

コネクタ 1 はシステムの内蔵カメラであり、プレゼンテーション ソースとして使用できないことに注意してください。

Video Input Connector 2 Visibility（HDMI コネクタ）のデフォルト値は IfSignal です。

必要なユーザ ロール：ADMIN

デフォルト値：コネクタ 1：Never　コネクタ 2：Always　コネクタ 3：OnConnect

値スペース：コネクタ 1：Never　コネクタ 2、3：Never/Always/IfSignal

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、Never に設定します。

Always：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。

IfSignal：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。

Video Layout DisableDisconnectedLocalOutputs

この設定は、On に固定されています。
デフォルト値: On

値スペース: On
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。

Video Monitors

モニタ レイアウト モードを定義します。ビデオ システムがサポートするモニタは 1 台のみのため、この値は固定で変更できないことに注意してください。

必要なユーザ ロール: ADMIN
デフォルト値: Single

値スペース: Single
Single:レイアウトは、ビデオ システムのモニタに表示されます。

Video Output Connector [1] Brightness

ビデオ システムの内蔵ディスプレイの明るさレベルを定義します。

必要なユーザ ロール: ADMIN、USER
デフォルト値: 80

値スペース: 整数(0 ～ 100)
範囲:値は 0 ～ 100 である必要があります。

Video Output Connector [2] CEC Mode

HDMI 出力(Output Connector 2)は将来の使用に備えるものです。

Video Output Connector [2] Location HorizontalOffset

HDMI 出力(Output Connector 2)は将来の使用に備えるものです。

Video Output Connector [2] Location VerticalOffset

HDMI 出力(Output Connector 2)は将来の使用に備えるものです。

Video Output Connector [2] OverscanLevel

HDMI 出力(Output Connector 2)は将来の使用に備えるものです。

Video Output Connector [1..2] Resolution

Connector 1:内蔵ディスプレイの解像度と更新間隔。この値は固定されており、変更できません。
Connector 2:HDMI 出力(Output Connector 2)は将来の使用に備えるものです。
デフォルト値: Connector 1:1920_1080_60

値スペース: Connector 1:1920_1080_60
1920_1080_60:解像度は 1920 x 1080、更新間隔は 60 Hz です。

Video Output Connector [2] RGBQuantizatonRange

HDMI 出力(Output Connector 2)は将来の使用に備えるものです。

Video Output Connector [1] Whitebalance Level

内蔵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。

必要なユーザ ロール: ADMIN、USER
デフォルト値: 6500

値スペース: 整数(4000 ～ 9000)
ケルビン単位の色温度。

Video Presentation DefaultPIPPosition

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

必要なユーザ ロール: ADMIN

デフォルト値: Current

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

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

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

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

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

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

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

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

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

Video Presentation DefaultSource

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソースを定義します。この設定は、API およびサード パーティ製ユーザ インターフェイスで使用できます。シスコから提供されるユーザ インターフェイスを使用している場合は該当しません。

必要なユーザ ロール: ADMIN、USER

デフォルト値: 2

値スペース: 2

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソース。

Video Selfview Default Mode

コール終了後にメイン ビデオ ソース(セルフビュー)を画面に表示するかどうかを定義します。セルフ ビュー ウィンドウの位置とサイズはそれぞれ、Video Selfview Default PIPPosition 設定と Video Selfview Default FullscreenMode 設定によって決定されます。

必要なユーザ ロール: ADMIN

デフォルト値: Current

値スペース: Off/Current/On

Off:セルフビューはコール退出時にオフにされます。

Current:セルフビューはそのままの状態で残ります。つまりコール中にオンであった場合はコール終了後にもオンのままであり、コール中にオフであった場合はコール終了後にもオフのままです。

On:セルフビューはコール退出時にオンにされます。

Video Selfview Default FullscreenMode

コール終了後に、メイン ビデオ ソース(セルフビュー)を全画面表示するか、小さいピクチャインピクチャ(PiP)として表示するかを定義します。この設定はセルフビューがオンである場合にのみ適用されます(Video Selfview Default Mode 設定を参照)。

必要なユーザ ロール: ADMIN

デフォルト値: Current

値スペース: Off/Current/On

Off:セルフビューは PiP として表示されます。

Current:セルフビューの画像のサイズはコール終了時に未変更の状態に保たれます。つまりコール中に PiP であった場合はコール終了後にも PiP のままであり、コール中に全画面であった場合はコール終了後にも全画面のままです。

On:セルフビューの画像は全画面表示されます。

Video Selfview Default OnMonitorRole

コール終了後にメイン ビデオ ソース(セルフビュー)を表示するモニタを定義します。このビデオシステムにはモニタが 1 つしかないため、この値は固定で変更できないことに注意してください。

必要なユーザ ロール: ADMIN

デフォルト値: First

値スペース: First

First:セルフビューの画像は内蔵スクリーンに表示されます。

Video Selfview Default PIPPosition

コール終了後に小さいセルフビュー ピクチャインピクチャ（PiP）を表示する画面上の位置を定義します。この設定は、セルフビューがオンで（Video Selfview Default Mode 設定を参照）、しかもフルスクリーン ビューがオフである場合（Video Selfview Default FullscreenMode 設定を参照）にのみ適用されます。

必要なユーザ ロール：ADMIN

デフォルト値：Current

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

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

UpperLeft：セルフビュー PiP が画面の左上隅に表示されます。

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

UpperRight：セルフビュー PiP が画面の右上隅に表示されます。

CenterLeft：セルフビュー PiP が画面の左中央に表示されます。

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

LowerLeft：セルフビュー PiP が画面の左下隅に表示されます。

LowerRight：セルフビュー PiP が画面の右下隅に表示されます。

Video Selfview OnCall Mode

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

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：セルフ ビューはコール セットアップ中に自動的に表示されません。

On：セルフ ビューはコール セットアップ中に自動的に表示されます。

Video Selfview OnCall Duration

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

必要なユーザ ロール：ADMIN

デフォルト値：10

値スペース：整数（1 ～ 60）

範囲：セルフ ビューをオンにする期間を選択します。有効な範囲は、1 ～ 60 秒です。

Experimental 設定

試験的設定は、テストのためだけのもので、シスコと同意したのでない限り使用できません。これらの設定は記載されておらず、以降のリリースで変更されます。

付録

ユーザ インターフェイス

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

[システム情報(System information)] と [設定(Settings)] メニューへのアクセス、ビデオ システムの [再起動(Restart)]、[スタンバイ(Standby)] モードと [応答不可(Do not disturb)] モードのアクティブ化と非アクティブ化、画面の明るさの調節

*プロキシミティ*機能が使用可能かどうかを示します。

システム名または連絡先情報

[発信（Call）] をタップすると、[お気に入り（Favorites）] リスト、[ディレクトリ（Directory）] リスト、[発着信履歴（Recents）] リストなどの連絡先を呼び出したり、[検索またはダイヤル（Search or Dial）] フィールドを開いたりできます

[メッセージ(Messages)] をタップすると、ボイス メール システムを呼び出すことができます(使用可能な場合)

装置の右側:
- ヘッドセット用の USB ソケットとミニジャック ソケット

マイク:ミュート/ミュート解除

スピーカーの音量コントロール

セルフビュー:オン/オフ

室内制御のエントリ アイコン(使用可能な場合)(システムによってはエントリ アイコンが異なる場合があります)

時刻

マイクのミュート インジケータ

装置の右側:
- マイクのミュート ボタン
- スピーカーの音量コントロール
- ヘッドセット用の USB ソケット

リモート モニタリングのセットアップ

要件:

- *RemoteMonitoring* オプション

リモート モニタリングは、別の場所からビデオ システムを制御する場合に役立ちます。

入力ソースからのスナップショットが Web インターフェイスに表示されるため、部屋にいなくても、カメラ ビューを確認したり、カメラを制御したりできます。

有効になっている場合、スナップショットは約 5 秒ごとに自動的に更新されます。

ビデオ システムに *RemoteMonitoring* オプションがあるかどうかの確認

1. Web インターフェイスにサインインします。
2. [ホーム(Home)] ページで、インストールされているオプションのリストで *RemoteMonitoring* がオンになっているかどうかを確認します。

   リストでそのように示されていない場合、リモート モニタリングは使用不可です。

リモート モニタリングを有効にする

RemoteMonitoring オプション キーをインストールします。オプション キーのインストール方法については、▶「オプション キーを追加する」の章で説明しています。

リモート モニタリング オプションをイネーブルにする場合は、プライバシーに関する地域の法律および規制を遵守する必要があります。また、システム管理者がカメラや画面を監視および制御する場合があることを、システムのユーザに適切な方法で通知してください。システムの使用時にプライバシー規制を遵守するのはお客様の責任であり、シスコはこの機能の違法な使用について一切の責任を否認します。

スナップショットについて

ローカル入力ソース

ビデオ システムのローカル入力ソースのスナップショットが [コール制御(Call Control)] ページに表示されます。

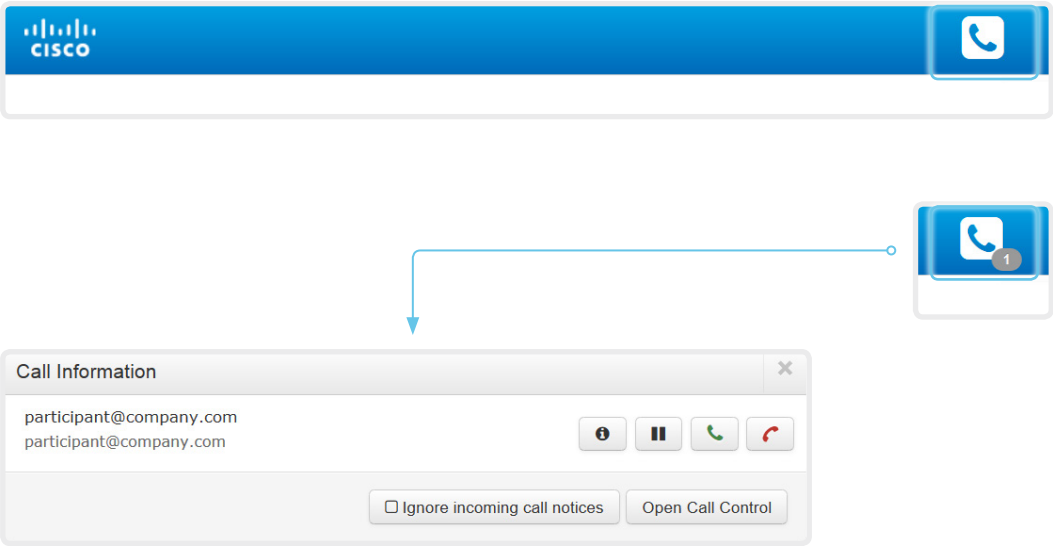
スナップショットは、ビデオ システムがアイドル中でも通話中でも表示されます。

遠端のスナップショット

通話中に、遠端カメラからのスナップショットを表示することもできます。遠端ビデオ システムに *RemoteMonitoring* オプションがあるかどうかは問題ではありません。

コールが暗号化されると遠端スナップショットは表示されません。

Web インターフェイス使用中のコール情報へのアクセス



コール状態インジケータ

バッジはアクティブ コール数を示します。システムがアイドル状態の場合、バッジはありません。

インジケータをクリックし、接続されているコールの詳細情報を表示します。

[コール情報 (Call Information)] ウィンドウの表示

[コール情報 (Call Information)] ウィンドウを手動で開くには、*コール状態インジケータ*をクリックします。

デフォルトでは、ビデオ システムがコールを受信すると [コール情報 (Call Information)] ウィンドウが自動的に表示されます。

着信コール通知のオン/オフの切り替え

[着信コール通知を無視する (Ignore incoming call notices)] をクリックすると、ビデオ システムがコールを受信したときに [コール情報 (Call Information)] ウィンドウを自動的に表示するかどうか決定できます。

このチェックボックスをオンにした場合は、[コール情報 (Call Information)] ウィンドウが自動的に開きません。

[コール制御 (Call Control)] ページの表示

[コール制御 (Call Control)] ページに直接移動するには、[コール制御を開く (Open Call Control)] をクリックします。

コールを制御する

関連するコントロール ボタンが [コール情報 (Call Information)] ウィンドウに表示されます。これらのボタンを使用して次の操作を行うことができます。

- コールの詳細を表示する
- コールを保留にする
- コールに応答する
- コールを切断する

コール状態インジケータについて

コール状態インジケータは、システムが通話中であるかどうかを示します。着信コールについてユーザに通知することもできます。

コール状態インジケータは [コール制御 (Call Control)] ページ以外のすべてのページで使用できます。

Web インターフェイスを使用したコールの発信 (1/2 ページ)

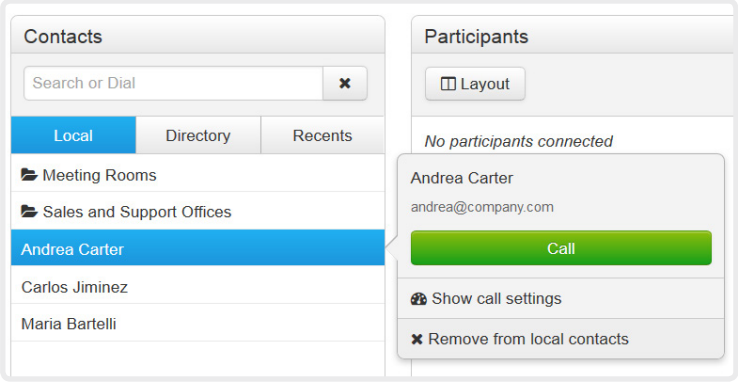
Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。

コールの発信

Web インターフェイスを使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。

1. [ローカル (Local)]、[ディレクトリ (Directory)]、または [新着 (Recents)] リストを参照して正しいエントリを見つけるか、[検索またはダイヤル (Search or Dial)] フィールドに 1 つ以上の文字列を入力します*。正しい連絡先名をクリックします。
2. 連絡先カードで [コール (Call)] をクリックします。

または、[検索して発信 (Search and Dial)] フィールドに完全な URI または番号を入力します。次に、URI または番号の横に表示される [コール (Call)] ボタンをクリックします。



DTMF トーンの送信

クリックすると、アプリケーションで DTMF (デュアルトーン多重周波数) シグナリングが必要な場合に使用できるキー パッドが表示されます。

コールの詳細の表示/非表示

[情報ボタン (information button)] をクリックすると、コールの詳細情報が表示されます。

もう一度ボタンをクリックすると情報が非表示になります。

コールの保留と再開

参加者を保留にするには、その参加者の名前の横にある ⏸ ボタンを使用します。

コールを再開するには、保留中の参加者に表示される ▶ ボタンを使用します。

コールの終了

コールを終了するには、[全通話切断 (Disconnect all)] または ☎ ボタンをクリックします。

*検索時には、入力内容に応じて、[ローカル (Local)]、[ディレクトリ (Directory)]、および [履歴 (Recents)] リストの一致するエントリが表示されます。

Web インターフェイスを使用したコールの発信 (2/2 ページ)

Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。

複数の相手に発信

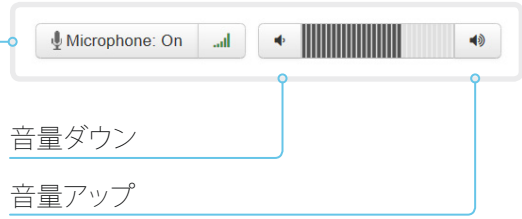
会議ブリッジを使用した複数のコール (CUCM のアドホック会議) は、ビデオ システムでサポートされていても Web インターフェイスではサポートされません。

ボリュームを調整する

マイクをミュートにする

[マイク:オン (Microphone: On)] をクリックすると、マイクがミュートされます。すると、テキストが [マイク: オフ (Microphone: Off)] に変わります。

[マイク:オフ (Microphone: Off)] をクリックすると、ミュートが解除されます。



Web インターフェイスを使用したコンテンツの共有

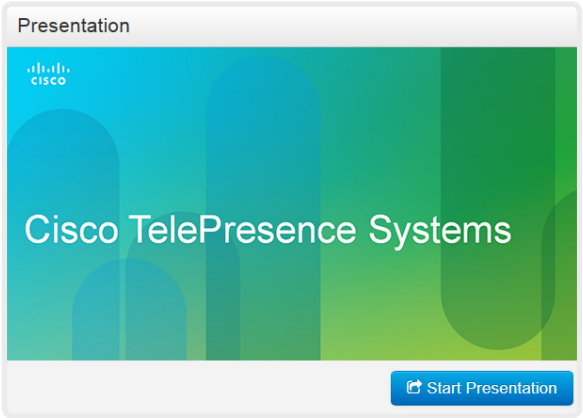
Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。

コンテンツの共有

1. [プレゼンテーションの開始 (Start Presentation)] をクリックします。そうすると、テキストが [プレゼンテーションの停止 (Stop Presentation)] に変わります。

コンテンツ共有の停止:

共有している間に表示される [プレゼンテーションを中止 (Stop Presentation)] ボタンをクリックします。



[スナップショット (Snapshot)] 領域

選択したプレゼンテーション ソースのスナップショットが表示されます。

リモート モニタリング オプションがあるビデオ システムでのみ利用できます。

コンテンツ シェアリング (共有) について

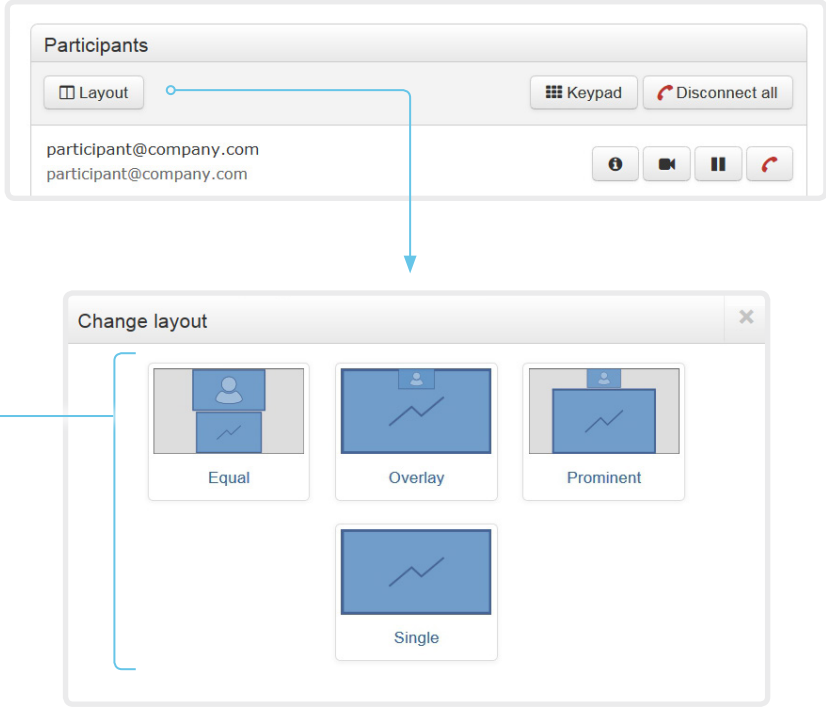
プレゼンテーション ソース (最も多いのは PC) は、ビデオ システムの背面にあるコンピュータ用の HDMI コネクタに接続できます。

コールの間、コールの他の参加者 (相手先) とコンテンツを共有できます。

コール (通話) 中でない場合は、コンテンツはローカルに表示されます。

ローカル レイアウトの制御

Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。



レイアウトの変更

[レイアウト (Layout)] をクリックし、表示されたウィンドウで好みのレイアウトを選択します。

選択するレイアウトのセットは、システム設定によって異なります。

レイアウトは、アイドル中でも通話中でも変更可能です。

レイアウトについて

ここでいうレイアウトとは、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。

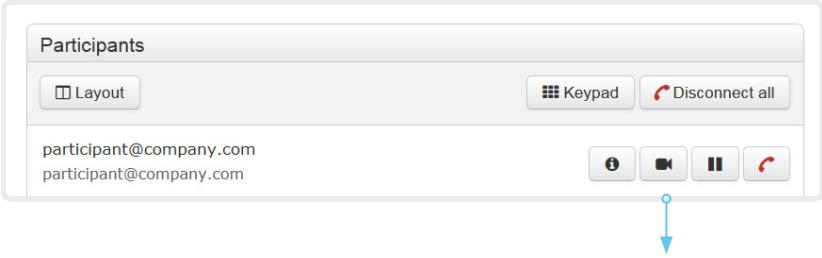
相手先（遠端）カメラの制御

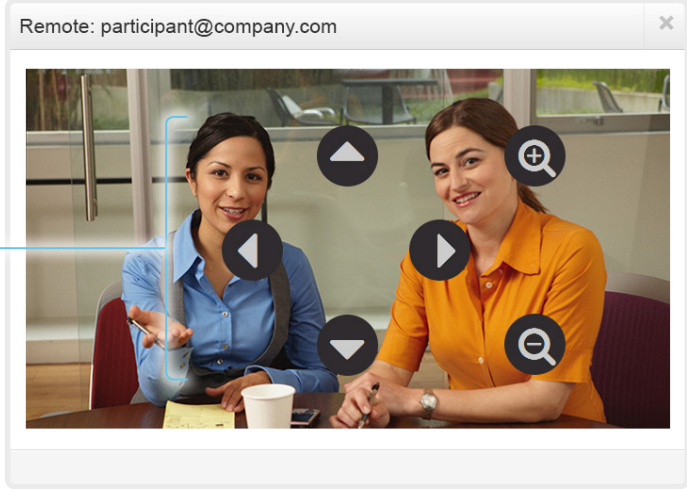
Web インターフェイスにサインインして、[コール制御（Call Control）] に移動します。

前提条件

以下の条件において、通話中にリモート参加者のカメラ（相手先）を制御できます。

- [会議（Conference）] > [遠端制御（FarEndControl）] > [モード（Mode）] 設定が遠端ビデオ システムで 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。
- ローカル ビデオ システムにリモート モニタリング オプションがある。





リモート参加者のカメラを制御

1. リモート カメラ制御ウィンドウを開くには、カメラのアイコンをクリックします。
2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および - を使用します。

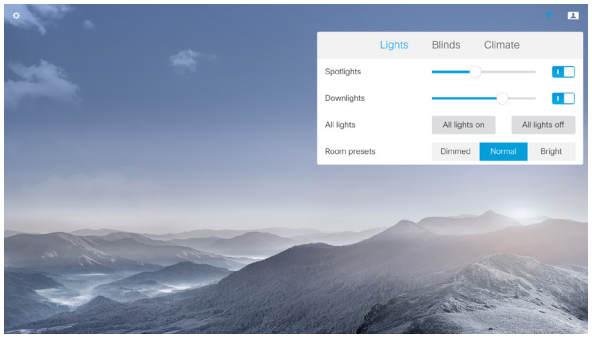
   相手先カメラの制御が許可されていない場合は、画面にコントロールが表示されません。

   コールが暗号化されている場合、コントロールの背後の相手先（遠端）のスナップショットは表示されません。

ユーザ インターフェイスへの室内制御の追加

ユーザ インターフェイスは、会議室にある周辺機器（たとえば、照明やブラインド）を制御できるようにカスタマイズできます。

これにより、制御システムの機能とビデオ システムのユーザ フレンドリーなユーザ インターフェイスとの強力な組み合わせが可能になります。



例の室内制御パネル

室内制御エディタを使用して室内制御パネルを設計する方法、およびビデオ システムの API を使用して室内制御をプログラミングする方法の詳細については、*室内制御のガイド*を参照してください。参照先：

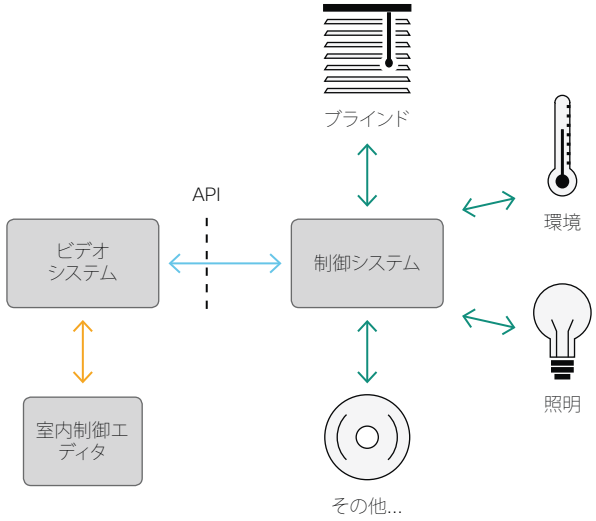
► http://www.cisco.com/go/in-room-control-docs [英語]

アーキテクチャ

タッチ インターフェイスを装備した Cisco ビデオ システム、および周辺機器用のハードウェア ドライバ付きの、Crestron 社や AMX 社などのサードパーティ製の制御システムが必要です。周辺機器を制御するのは、ビデオ システムではなく、制御システムです。

制御システムをプログラミングする場合、ビデオ システムのユーザ インターフェイス上のコントロールを接続するために、ビデオ システムの API（イベントとコマンド）を使用する必要があります。

カスタムの室内制御パネルを作成するために使用する必要がある、使いやすいドラッグアンドドロップ式のエディタが、ビデオ システムのソフトウェアに無償で付属しています。



室内制御の概略図

室内制御エディタ

室内制御エディタは、ビデオ システムのユーザ インターフェイス用のカスタムの室内制御パネルを作成する場合に使用できます。

Web インターフェイスにサインイン*して、[統合（Integration）] > [室内制御（In-Room Control）] を選択します。

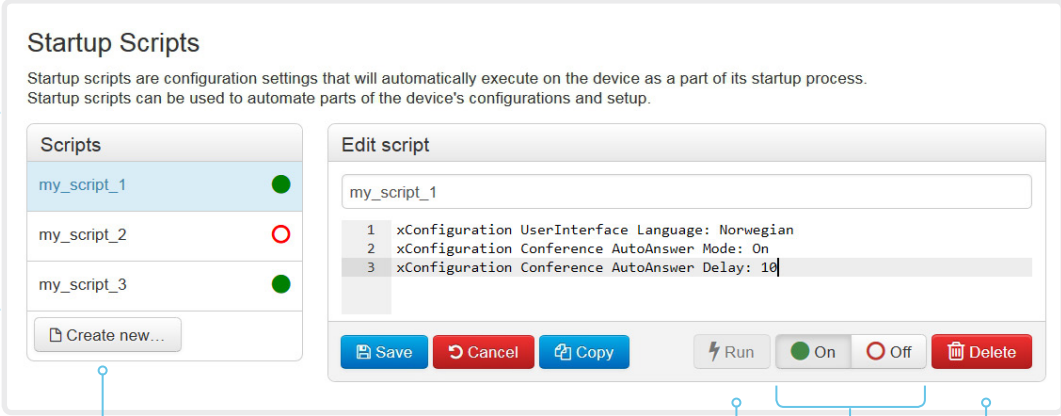
- ビデオ システムの Web インターフェイスから直接このエディタを起動するには、[エディタの起動（Launch Editor）] をクリックします。

  ビデオ システムに新しい室内制御パネルをプッシュすると、結果がタッチ コントローラにすぐに表示されます。
- オフラインで作業するために使用できるスタンドアロン バージョンをダウンロードするには、[エディタのダウンロード（Download Editor）] をクリックします。

* 制御システムをプログラミングする場合に必要な室内制御エディタと API コマンドにアクセスするには、ROOMCONTROL または ADMIN のユーザ ロールを持つユーザが必要です。

スタートアップ スクリプトの管理

Web インターフェイスにサインインして、[統合 (Integration)] > [スタートアップ スクリプト (Startup Scripts)] を選択します。



図に示すスクリプト名と設定は一例です。独自のスクリプトを作成できます。

スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます*。

アクティブなスタートアップ スクリプトの横には緑色のドットが表示され、非アクティブ スタートアップ スクリプトの横には赤色のリングが表示されます。

複数のスタートアップ スクリプトがある場合は、リストの上から下に順番に実行されます。

スタートアップ スクリプトの作成

1. [Create new... (新規作成...)] をクリックします。
2. タイトル入力フィールドにスタートアップ スクリプトの名前を入力します。
3. コマンド入力領域に、コマンド (xConfiguration または xCommand) を入力します。新しい行で各コマンドを開始します。
4. [保存 (Save)] をクリックします。
5. On をクリックすると、スタートアップ スクリプトがアクティブになります。

既存のスクリプトを編集の開始点として使用する場合は、そのスクリプトを選択して、[コピー (Copy)] をクリックします。

スタートアップ スクリプトをすぐに実行する

1. リストからスタートアップ スクリプトを選択します。
2. [実行 (Run)] をクリックします。

   アクティブ スタートアップ スクリプトと非アクティブ スタートアップ スクリプトの両方を、即時に実行できます。

スタートアップ スクリプトのアクティブ化または非アクティブ化

1. リストからスタートアップ スクリプトを選択します。
2. On をクリックしてスクリプトをアクティブにするか、Off をクリックしてスクリプトを非アクティブにします。

   アクティブ スタートアップ スクリプトは、ビデオ システムが起動するたびに実行されます。

スタートアップ スクリプトの削除

1. リストからスタートアップ スクリプトを選択します。
2. [削除 (Delete)] をクリックします。

スタートアップ スクリプトについて

スタートアップ スクリプトには起動手順の一部として実行されるコマンド (xCommand) および構成 (xConfiguration) が含まれます。

`xCommand SystemUnit Boot` などのいくつかのコマンドと設定はスタートアップ スクリプトに配置することができません。不正なコマンドや設定が含まれるスクリプトは保存できません。

xCommand および xConfiguration の構文とセマンティックは、製品の API ガイドに説明されています。

ビデオ システムの XML ファイルへのアクセス

Web インターフェイスにサインインして、[統合（Integration）] > [開発者 API（Developer API）] を選択します。

XML ファイルはビデオ システムの API の一部です。このファイルには、システムに関する情報が階層構造で保存されています。

- *Configuration.xml* には現在のシステム設定（コンフィギュレーション）が含まれます。これらの設定は、Web インターフェイスまたは API（アプリケーション プログラミング インターフェイス）から制御されます。
- *status.xml* 内の情報は常にビデオ システムによって更新され、システムおよびプロセスの変更が反映されます。ステータス情報は、Web インターフェイスまたは API からモニタされます。
- *Command.xml* にはアクションの実行をシステムに指示するために使用できるコマンドの概要が含まれます。コマンドは、API から発行されます。
- *Valuespace.xml* にはシステム設定、ステータス情報、およびコマンドのすべての値スペースの概要が含まれます。

XML ファイルを開く

ファイル名をクリックして、XML ファイルを開きます。

API について

アプリケーション プログラミング インターフェイス（API）は、ビデオ システムを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、ビデオ システムの API ガイドを参照してください。

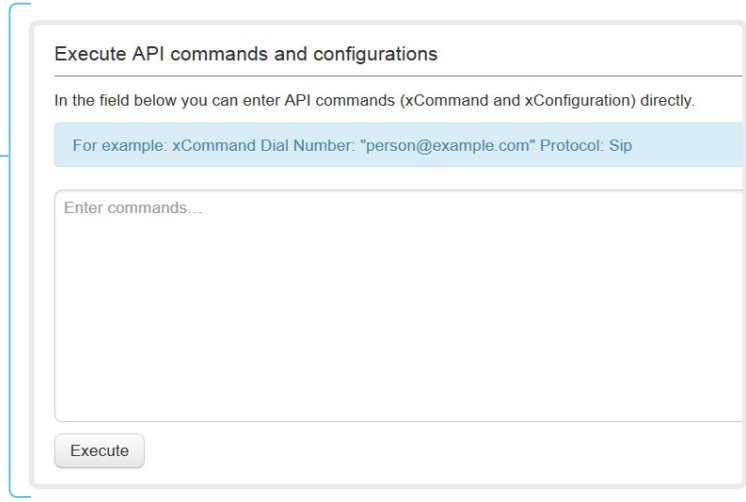
Web インターフェイスからの API コマンドと設定の実行

Web インターフェイスにサインインして、[統合 (Integration)] > [開発者 API (Developer API)] を選択します。

コマンド (xCommand) と設定 (xConfiguration) は Web インターフェイスから実行できます。構文とセマンティクスについては、ビデオ システムの API ガイドを参照してください。

API コマンドと構成を実行する

1. テキスト領域で、1 つのコマンド (xCommand または xConfiguration) またはコマンドのシーケンスを入力します。
2. [実行 (Execute)] をクリックして、コマンドを発行します。



API について

アプリケーション プログラミング インターフェイス (API) は、ビデオ システムを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、ビデオ システムの API ガイドを参照してください。

シリアル インターフェイス

ビデオ システムとの直接通信には、マイクロ USB コネクタを使用します。マイクロ USB と USB を接続するケーブルが必要です。コンピュータでシリアル ポート ドライバが自動的にインストールされない場合は、シリアル ポート ドライバをコンピュータに手動でインストールする必要があります。

シリアル インターフェイスに接続するには、ターミナル エミュレータ（SSH クライアント）を使用します。最も一般的なコンピュータのタイプ（PC、Mac）とオペレーティング システムの場合、PuTTY または Tera Term が動作します。

シリアル接続は、IP アドレス、DNS、ネットワークなしでも使用できます。

パラメータ：

- ボー レート：115200 bps
- データ ビット：8
- パリティ：なし
- ストップ ビット：1

ビデオ システムの設定

シリアル通信はデフォルトで有効になっています。次の設定を使用して動作を変更します。

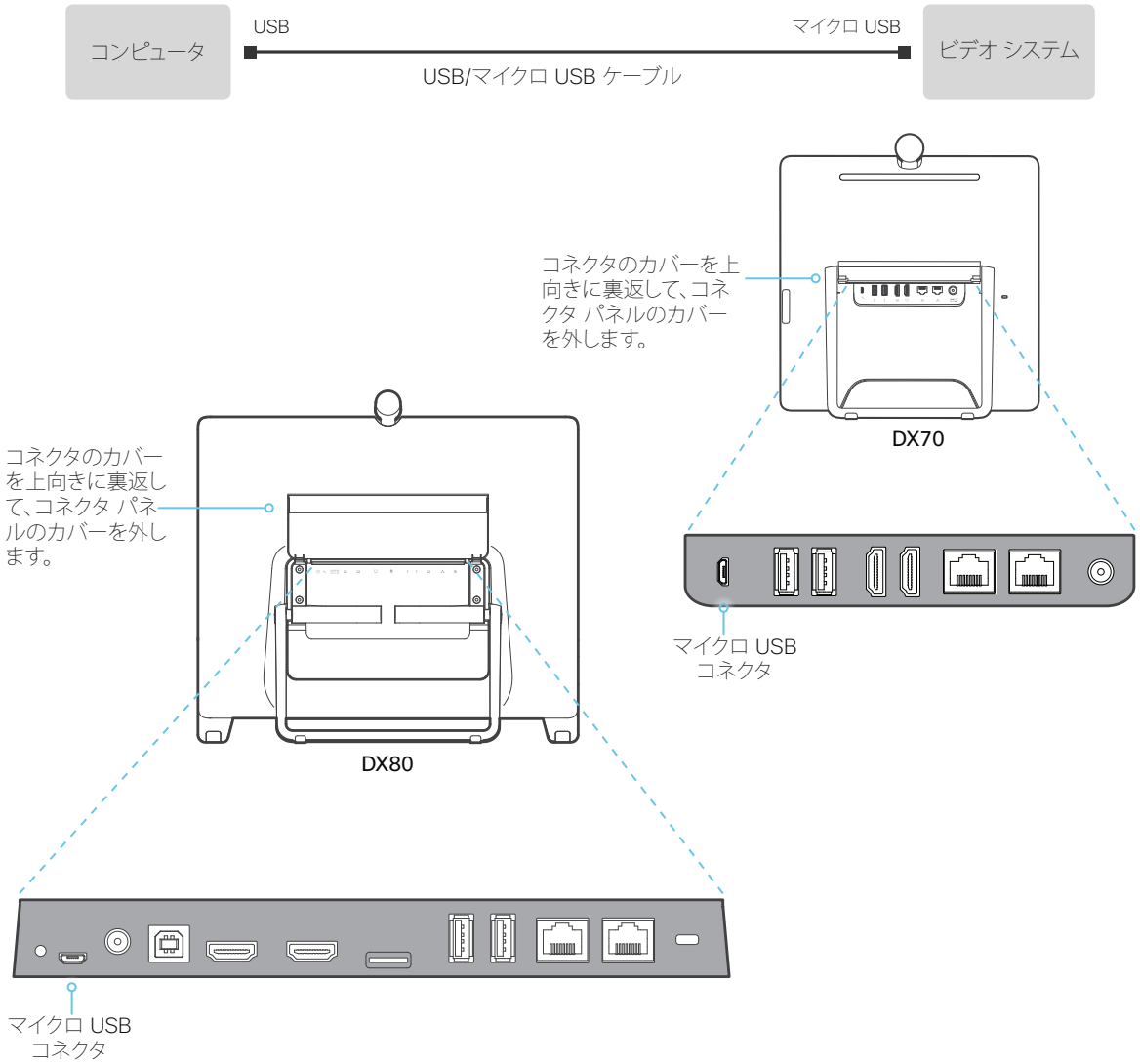
[シリアル ポート（SerialPort）] > [モード（Mode）]

セキュリティ上の理由から、シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには、次の設定を使用します。

[SerialPort] > [LoginRequired]

シリアル ポートの設定を変更した後、ビデオ システムを再起動します。

ビデオ システムが CUCM からプロビジョニングされている場合、シリアル ポートの設定を CUCM から設定する必要があります。



技術仕様(1/2 ページ)

ソフトウェアの互換性

- コラボレーション エンドポイント ソフトウェア バージョン 8.2 以降

製品の同梱物:

- 内蔵の HD カメラとマイクを備えた DX80 システムまたは DX70 システム
- ネットワーク ケーブル
- HDMI/USB ケーブル(DX80 のみ)
- 電源アダプタおよび使用地域向けの電源コード

統合型の HD カメラ

- ディスプレイから -5°~ 70°
- 水平視野角 63°
- 垂直視野角 38°
- 解像度:1080p30
- F 2.2
- 顔認識に基づくインスタント フォーカス
- プライバシー シャッター

ユーザ インターフェイス

- 画面上のグラフィカル ユーザ インターフェイス

言語のサポート

(ソフトウェアのバージョンによって異なる)

- アラビア語、カタロニア語、中国語(簡体字)、中国語(繁体字)、チェコ語、デンマーク語、オランダ語、英語、英語(英国)、フィンランド語、フランス語、フランス語(カナダ)、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、ノルウェイ語、ポーランド語、ブラジル ポルトガル語、ロシア語、スペイン語、スペイン語(ラテン)、スウェーデン語、トルコ語

システム管理

- 組み込みの SNMP、Telnet、SSH、XML、および SOAP による総合的管理
- Web サーバ、HTTP、および HTTPS を使用したリモート ソフトウェア アップロード
- 画面上のメニュー システム

ディレクトリ サービス

- ローカル ディレクトリ(お気に入り)のサポート
- 社内ディレクトリ(Cisco Unified Communications Manager リリースおよび Cisco TelePresence Management Suite 利用)
- LDAP および H.350 をサポートするサーバ ディレクトリ(Cisco TelePresence Managment Suite が必要)
- 日時を含む着信、発信、および不在着信のコール履歴

電源

- 定格:最大 60 W
- 省電力スタンバイ モード

動作温度および湿度

- 周囲温度:0 ~ 40 °C(32 ~ 95 °F)
- 相対湿度(RH):10 ~ 90%

保管および輸送の温度

- RH 10 ~ 90% では -20 ~ 60°(-4 ~ 140°F)(結露しないこと)

DX80 システムの寸法

- 幅:56.5 cm(22.2 インチ)
- 高さ:51.2 cm(20.2 インチ)
- 奥行:8.9 cm(3.5 インチ)
- 重量:7.1 kg(15.65 ポンド)

DX70 システムの寸法

- 幅:35.31 cm(13.91 インチ)
- 高さ:37.71 cm(14.84 インチ)
- 奥行:6.23 cm(2.45 インチ)
- 重量:3.4 kg(7.5 ポンド)

認定および適合規格

- 指令 2014/35/EU(低電圧指令)
- 指令 2014/30/EU(EMC 指令):クラス A
- 指令 2014/53/EU(無線機器指令)
- 指令 2011/65/EU(RoHS)
- 指令 2002/96/EC(WEEE)

- NRTL 認定(製品の安全性)
- FCC CFR 47 Part 15B(EMC):クラス B
- FCC Listed(無線機器)

各国の認定書類については、Product Approval Status Database(製品認定ステータス データベース)www.ciscofax.com を参照してください。

BANDWIDTH

- 最大 3 Mbps

解像度とフレーム レートの最小帯域幅

- 768 kbps から 720p30
- 1472 kbps から 1080p30

ファイアウォール トラバーサル

- Cisco TelePresence Expressway テクノロジー

ビデオ標準

- H.263
- H.263+
- H.264
- AVC(H.264/MPEG-4 Part 10 Advanced Video Coding)

ビデオ入力

HDMI ビデオ入力 X 1。最大 1920 X 1080@60 fps(HD1080p60)までのフォーマット(以下を含む)をサポートします。

- 640 X 480
- 720 X 480
- 800 X 600
- 1024 X 768
- 1280 X 720
- 1366 X 768
- 1920 X 1080

Extended Display Identification Data(EDID)

ビデオ出力

HDMI 出力(1 個)*(将来の使用に備えて予約済み)。以下のフォーマットをサポートします。

- 1920 X 1080@60 fps(1080p60)

VESA モニタ電源管理

Extended Display Identification Data(EDID)

* HDMI バージョン 1.3

技術仕様(2/2 ページ)

ライブ ビデオ解像度(エンコード/デコード)

最大 1920 X 1080@30 fps(HD1080p30)までのエンコードまたはデコード ビデオ フォーマット(以下を含む)をサポートします。

- 176 X 144 @ 30 fps(QCIF)(デコードのみ)
- 352 X 288 @ 30 fps(CIF)
- 512 X 288 @ 30 fps(w288p)
- 576 X 448 @ 30 fps(448p)
- 640 X 480 @ 30 fps(VGA)
- 704 X 576 @ 30 fps(4CIF)
- 768 X 448 @ 30 fps(w448p)
- 800 X 600 @ 30 fps(SVGA)
- 1024 X 576 @ 30 fps(w576p)
- 1024 X 768 @ 30 fps(XGA)
- 1280 X 720 @ 30 fps(HD720p)
- 1280 X 768 @ 30 fps(WXGA)
- 1280 X 1024 @ 30 fps(SXGA)
- 1440 X 900 @ 30 fps(WXGA+)
- 1680 X 1050 @ 30 fps(WSXGA+)
- 1920 X 1080 @ 30 fps(HD1080p)

音声標準

- 64 kbps AAC-LD
- OPUS
- G.722
- G.722.1
- G.711mu
- G.711a
- G.729AB

音声機能

- 最大 48 kHz のサンプリング レート
- ハイクオリティ 20 kHz オーディオ
- 音響エコー キャンセラ
- オート ゲイン コントロール
- オート ノイズ リダクション
- アクティブ リップ シンク

音声入力

- 内蔵マイク アレイ
- HDMI 音声 1

音声出力

- ライン出力 1 個、ミニジャック(DX70)
- 1 HDMI(デジタル メイン音声)

デュアル ストリーム

- H.239(H.323)デュアル ストリーム
- BFCP(SIP)デュアル ストリーム
- 最大 1080p(1920 X 1080)の解像度をサポート

マルチポイント サポート

- Cisco Ad-Hoc Conferencing(Cisco Unified Communications Manager、Cisco TelePresence Server および Cisco TelePresence Conductor が必要)

プロトコル

- SIP および H.323

組み込み暗号化

- SIP および H.323 のポイントツーポイント
- 規格準拠:H.235v3 および Advanced Encryption Standard(AES)
- キーの自動生成と交換
- デュアル ストリームでサポート

IP ネットワーク機能

- サービス設定での DNS ルックアップ
- 差別化サービス(QoS)
- IP 帯域幅最適化コントロール(フロー制御を含む)
- 自動ゲートキーパー検出
- ダイナミック再生およびリップシンクのバッファリング
- H.323 で H.245 デュアルトーン多重周波数(DTMF)トーン
- NTP による日時のサポート
- パケット損失時のダウンスピード機能
- URI ダイヤル
- TCP/IP
- DHCP
- IEEE 802.1x ネットワーク認証
- IEEE 802.1Q 仮想 LAN
- IEEE 802.1p QoS およびサービス クラス
- Cisco ClearPath

IPV6 ネットワークのサポート

- H.323 および SIP に対するデュアル スタックの IPv4 および IPv6
- DHCP、SSH、HTTP、HTTPS、DNS、DiffServ に対するデュアル スタックの IPv4 および IPv6
- スタティック IP アドレスの割り当て、ステートレス自動設定および DHCPv6 をサポート

サポートされるインフラストラクチャ

- Cisco Unified Communications Manager 8.6.2 以降
- Cisco TelePresence Video Communication Server (Cisco VCS)

セキュリティ機能

- Web インターフェイス(HTTPS/HTTP)および SSH を使用した管理
- パスワードで保護された IP 管理
- パスワードで保護された管理メニュー
- IP サービスのディセーブル
- ネットワーク設定の保護

ネットワーク インターフェイス

- 内部 2 ポートの Cisco イーサネット スイッチ(RJ-45)10/100/1000BASE-T(自動ネゴシエーションのみ)

その他のインターフェイス

- USB ポート 3 個
- MicroSD カード スロット 1 個(将来の使用に備えて)
- メンテナンス目的の Micro-USB ポート 1 個

すべての仕様は予告なしに変更される場合があります。システム仕様は異なる場合があります。

これらのドキュメントの画像はすべて説明目的でのみ使用され、実際の製品とは異なる場合があります。

2016 年 12 月

サポートされている RFC

RFC（Request For Comments）シリーズには、Internet Engineering Task Force（IETF）によって作成される技術仕様およびポリシー文書など、インターネットに関する技術および組織のドキュメントが含まれます。

- 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: Session Initiation Protocol』
- 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 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』

シスコ Web サイト内のユーザ ドキュメンテーション

Cisco TelePresence 製品のユーザ ドキュメンテーションは、► http://www.cisco.com/go/telepresence/docs で入手できます。

該当する製品が見つかるまで、右ペインの製品カテゴリを選択します。以下の順にパスをたどってください。

[コラボレーション デスク エンドポイント (Collaboration Desk Endpoints)] >

[DX シリーズ (DX Series)] >

[DX シリーズ (DX Series)]

または、次のショートリンクを使用してドキュメンテーションを検索します。► http://www.cisco.com/go/dx-docs [英語]

ドキュメントは、次のカテゴリに編成されます。

[インストールとアップグレード (Install and Upgrade)] > [インストールとアップグレード (Install and Upgrade Guides)]

- *インストレーション ガイド*:製品のインストール方法
- *スタートアップ ガイド*:システムを稼働させるために必要な初期設定
- *RCSI ガイド*:法規制の遵守および安全に関する情報

[保守と運用 (Maintain and Operate)] > [メンテナンスとオペレーション ガイド (Maintain and Operate Guides)]

- *アドミニストレータ ガイド*:製品の管理に必要な情報
- *『Deployment guide for TelePresence endpoints on CUCM』*:ビデオ システムを Cisco Unified Communications Manager (CUCM) とともに使用開始するために実行するタスク

[保守と運用 (Maintain and Operate)] > [エンドユーザ ガイド (End-User Guides)]'

- *ユーザ ガイド*:製品の使用方法

[リファレンス ガイド (Reference Guides)] > [コマンド リファレンス (Command references)]

- *API リファレンス ガイド*:アプリケーション プログラミング インターフェイス (API) のリファレンス ガイド

[ソフトウェア ダウンロード、リリースと一般情報 (Software Downloads, Release and General Information)] > [ライセンス情報 (Licensing Information)]

- *オープン ソース ドキュメンテーション*:この製品で使用されるオープン ソース ソフトウェアのライセンスおよび通知

[ソフトウェア ダウンロード、リリースと一般情報 (Software Downloads, Release and General Information)] > [リリース ノート報 (Release Notes)]

- *ソフトウェア リリース ノート*

シスコのお問い合わせ先

シスコの Web サイトでは、シスコの世界各地のお問い合わせ先を確認できます。

参照先：► http://www.cisco.com/go/offices

Corporate Headquarters:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

シスコ製品のセキュリティの概要

この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.bis.doc.gov/policiesandregulations/ear/index.htm で参照できます。