

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 913  
2020 年 6 月



# 管理者ガイド

Cisco Webex Room Kit Mini 用

シスコ製品をお選びいただきありがとうございます。

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

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

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

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

ユーザードキュメントは次の場所から入手できます。

▶ <https://www.cisco.com/go/room-docs>

## 本ガイドの使用方法

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

## 目次

はじめに.....	4
ユーザマニュアルおよびソフトウェア .....	5
CE9 の最新情報 .....	6
Room Kit Mini の概要 .....	22
電源のオンとオフ .....	23
LED インジケータ.....	24
ビデオ会議デバイスの管理方法 .....	25
<b>設定</b> .....	<b>29</b>
ユーザ管理 .....	30
デバイス パスフレーズの変更.....	31
[設定 (Settings) ] メニューへのアクセスの制限 .....	32
デバイス設定 .....	33
サインイン バナーの追加 .....	34
ウェルカムバナーの追加 .....	35
デバイスのサービス証明書の管理 .....	36
信頼できる認証局 (CA) のリストの管理.....	37
セキュア監査ロギングのセットアップ .....	41
CUCM 信頼リストの削除.....	42
永続モードの変更 .....	43
アドホック マルチポイント会議のセットアップ .....	44
コンテンツ共有用のインテリジェントプロキシミティのセットアップ .....	46
ビデオ品質対コールレート比の調整.....	51
画面および Touch 10 ユーザーインターフェイスへの企業ブランディングの追加.....	53
カスタム壁紙の追加.....	55
着信音の選択と着信音量の設定 .....	56
お気に入りリストの管理 .....	57
アクセシビリティ機能のセットアップ .....	58
CUCM からの製品固有の設定のプロビジョニング .....	59
<b>周辺機器</b> .....	<b>61</b>
モニタへの接続 .....	62
入力ソースの接続 .....	63
入力ソース数の拡大.....	65
ディスプレイについて .....	66
4K 解像度について .....	67
HDMI ケーブルについて .....	68
Best Overview 機能のセットアップ .....	69
Touch 10 コントローラの接続 .....	70
ISDN リンクの接続.....	74

メンテナンス.....	75	時刻設定.....	159
新しいソフトウェアのインストール.....	76	ユーザインターフェイス 設定.....	162
オプションキーの追加.....	78	ユーザ管理設定.....	169
デバイスのステータス.....	79	ビデオ設定.....	173
診断の実行.....	80	Web エンジン設定.....	182
ログファイルのダウンロード.....	81	試験的設定.....	183
リモートサポートユーザーの作成.....	82	付録.....	184
設定とカスタム要素のバックアップ/復元.....	83	Touch 10 の使用方法.....	185
カスタム要素の CUCM プロビジョニング.....	84	USB カメラとしての Room Kit Mini の使用.....	186
カスタム要素の TMS プロビジョニング.....	85	リモート モニタリングのセットアップ.....	187
以前に使用していたソフトウェアイメージへの復元.....	86	Web インターフェイスを使用したコール情報へのアクセスとコール応答.....	188
ビデオ会議デバイスの初期設定へのリセット.....	87	Web インターフェイスを使用したコールの発信.....	189
Cisco Touch 10 の初期設定へのリセット.....	90	Web インターフェイスを使用したコンテンツの共有.....	191
Cisco TelePresence Touch 10 の初期設定へのリセット.....	91	ローカル レイアウトの制御.....	192
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.....	92	ローカル カメラの制御.....	193
Device settings.....	93	相手先カメラの制御.....	194
デバイス設定の概要.....	94	ルーム分析.....	195
オーディオ設定.....	100	ビデオ会議デバイスの Touch 10 ユーザインターフェイスのカスタマイズ.....	197
通話履歴設定.....	102	マクロを使用したビデオ会議デバイスの動作のカスタマイズ.....	199
カメラ設定.....	103	ユーザインターフェイスからのデフォルトボタンの削除.....	200
会議設定.....	104	サードパーティ USB 入力デバイスの使用.....	201
ファシリティサービス設定.....	109	HTTP(S) 要求の送信.....	202
H323 設定.....	110	デジタル サイネージ.....	203
HttpClient 設定.....	113	API 駆動型の Web ビュー.....	204
HTTP フィードバック設定.....	114	入力ソースの構成.....	205
ロギングの設定.....	115	プレゼンテーションソースの構成.....	207
マクロ設定.....	117	スタートアップスクリプトの管理.....	209
ネットワーク設定.....	118	デバイスの XML ファイルへのアクセス.....	210
ネットワークサービス設定.....	126	Web インターフェイスからの API コマンドとコンフィギュレーションの実行.....	211
周辺機器の設定.....	135	コネクタ パネル.....	212
電話帳の設定.....	137	イーサネットポートについて.....	213
プロビジョニング設定.....	139	メンテナンス用のシリアル インターフェイス.....	214
プロキシミティの設定.....	142	TCP ポートの開放.....	215
ルーム分析.....	144	TMS からの HTTPFeedback アドレス.....	217
ルームリセットの設定.....	145	オンプレミス登録デバイスの Cisco Webex Edge for Devices へのリンク.....	218
RTP 設定.....	146	Cisco Webex Cloud サービスへのデバイスの登録.....	219
セキュリティ設定.....	147	サポートされている RFC.....	220
シリアルポート 設定.....	150	技術仕様.....	221
SIP 設定.....	151	シスコ Web サイト内のユーザーマニュアル.....	223
スタンバイ設定.....	156	シスコのお問い合わせ先.....	224
システムユニット 設定.....	158		

# 第 1 章 はじめに



## ユーザマニュアルおよびソフトウェア

### このガイドの対象となる製品

- Cisco Webex Room Kit Mini

### ユーザマニュアル

このガイドでは、ビデオ会議デバイスの管理に必要な情報を提供します。

主にオンプレミス登録のデバイス (CUCM、VCS) の機能と設定について説明していますが、その機能と設定の一部は、クラウド サービス (Cisco Webex) に登録されたデバイスにも適用されます。

本製品に関する詳しいガイドは、付録

▶ [シスコ Web サイト内のユーザマニュアル](#)を参照してください。

### シスコ Web サイト内のドキュメンテーション

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

▶ <https://www.cisco.com/go/room-docs>

### クラウドに登録されたデバイスのドキュメンテーション

Cisco Webex Cloud サービスに登録されたデバイスの詳細については、以下のサイトを参照してください。

▶ <https://help.webex.com>

### Cisco Project Workplace

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

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

### ソフトウェア

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

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

ソフトウェア リリース ノート (CE9) を参照することをお勧めします。

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

## CE9 の最新情報

この章では、現行の Cisco Collaboration Endpoint ソフトウェアバージョン 9.x (CE9.x) について、新規および変更されたデバイス設定 (コンフィギュレーション) の概要と、新機能および改善点を CE9.6 と比較して説明します。

CE9 では以下の Webex 製品が新しくなっています。

- CE 9.0: Room Kit
- CE 9.1: Codec Plus、および Room 55
- CE 9.2: Room 70
- CE 9.4: Codec Pro、Room 70 G2、および Room 55 Dual
- CE 9.6: Room Kit Mini
- CE 9.8: Board 55/55S、Board 70/70S、および Board 85S
- CE 9.12: Desk Pro
- CE 9.13: Room Panorama、Room 70 Panorama

詳細については、ソフトウェア リリース ノートを参照することをお勧めします。

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

## CE9.13 の新機能および改善点

### 新商品

- Cisco Webex Room Panorama
- Cisco Webex Room 70 Panorama

### Cisco Webex Control Hub の設定管理のサポート (すべての製品)

Cisco Webex Control Hub が拡張され、Webex Edge for Devices にリンクされたオンプレミス登録デバイスをより詳細に制御できるようになりました。新しい設定管理機能により、多くのデバイス設定への書き込みアクセスが許可されます。この機能はデフォルトで無効になっています。これは Control Hub で有効にすることができます。

### Webex パーソナルミーティングルームに簡単に参加 (すべての製品)

Webex Edge for Devices にリンクされたデバイスから、Webex 組織のユーザーを直接検索できるようになりました。検索結果のユーザー名の横には、パーソナルミーティングルーム (PMR) に参加するボタンが表示されます。

### Webex ミーティングへの参加時のリアルタイムメディアメトリック (すべての製品)

Webex Edge for Devices にリンクされたデバイスは、Webex 登録済みデバイスと同じように、Control Hub のメディアトラブルシューティングセクションに表示されます。これにより、メディア品質の問題のトラブルシューティングが容易になります。

### コール中のタッチ転送 (Board)

コール中にタッチ転送を使用でき、フローティングツールバーを使用してアクティブ化と非アクティブ化を切り替えることができます。

### バーチャル背景のサポート (Desk Pro)

独自のバーチャル背景をアップロードできます。イメージは Web インターフェイス経由でアップロードします。その後、GUI でいずれかのイメージを選択できます。

コンピュータなどの入力デバイスのコンテンツをバーチャル壁紙として使用することもできます。

### CMS ミーティングへのダイヤルイン時の遠端カメラ制御 (すべての製品)

CMS ミーティングへのダイヤルイン時に、アクティブなスピーカーのカメラを制御できます。参加者リストを開くと、カメラを制御するための [リモートカメラ (Remote Camera)] ボタンが表示されます。

注: 参加者間でアクティブなスピーカーが頻繁に変わる場合は、目的の参加者のカメラを制御することが難しくなる可能性があります。FECN に特定の参加者を手動で選択することはできません。現在アクティブなスピーカーが常に対象となります。

### ビデオストリームへのカスタムテキスト

(Codec Plus、Codec Pro、Room 70 G2、Room Kit、Room Kit Mini、Room 55 Dual、Room 70)

時刻や日付、カスタムテキスト文字列をビデオストリームに追加できます (xCommand Video Graphics Text Display)。このテキストは、メインビデオストリーム、プレゼンテーションストリーム、またはローカルビデオ出力に追加できます。

## CE9.12 の新機能および改善点

### 新商品

- Cisco Webex Room USB
- Cisco Webex Desk Pro

### DX シリーズから Desk シリーズへの名称変更

新しい Desk シリーズには、DX70、DX80、および Desk Pro 製品が含まれます。

### Samsung Flip での Room Kit Mini の使用をサポート (Room Kit Mini)

Room Kit Mini は、Samsung Flip デバイスに接続してタッチインターフェイスに対応させることができます。この場合、ホワイトボード機能も使用できます。[Flip] ボタンを押すと、Samsung Flip と Room Kit Mini のユーザーインターフェイスを簡単に切り替えることができます。

### コール中のホワイトボードの一方方向共有 (Board)

コール中にホワイトボードを共有できるようになりました。共有するには、[ホーム (Home)] ボタンをクリックし、[ホワイトボード (Whiteboard)] をクリックします。[編集 (Editing)] モードに入ると、共有が開始されます。ホワイトボードの共有を停止するには、[完了 (Done)] ボタンを押し、[共有を停止 (Stop sharing)] を押します。

ホワイトボードの共有は一方方向であることに注意してください。ホワイトボードに描画できるのは、ホワイトボードを共有しているデバイスのみです。リモート参加者は見ることしかできません。

### パーソナルミーティンググループ ID による Webex への参加のサポート (すべての製品)

[Webexに参加 (Webex Join)] ボタンで、パーソナルミーティンググループ (PMR) ID へのダイヤルがサポートされるようになりました。宛先には、完全な URL または短いパス (ユーザー名やサイト名) を入力するか、ミーティング番号を入力できます。

入力に合わせて、通話履歴リストから PMR の候補が表示されます。

### Webex Edge for Devices での HTTP プロキシのサポート (すべての製品)

HTTP プロキシのサポートが拡張され、*Webex Edge for Devices* にリンクされたデバイスも含まれるようになりました。

*Webex Edge for Devices* では、HttpClient、HttpFeedback、Web エンジンで使用する HTTP プロキシサービスを選択できます。

有効にした場合、Webex クラウドに対するすべての HTTP リクエストで、指定した HTTP プロキシが使用されます。ただし、プロキシのモードに関わらず、デバイスと Cisco Unified Communications Manager (CUCM)、MRA (Expressway 経由の CUCM)、または TMS (電話帳) との通信がプロキシ経由で行われることはありません。

さらに、次の新しい設定によって HTTP プロキシの使用を有効/無効にすることができます。

- HttpClient Http プロキシの使用
- HttpFeedback Http プロキシの使用
- Web エンジン Http プロキシの使用

### プロキシミティの通知の非表示 (すべての製品)

プロキシミティの通知を非表示にできるようになりました。これには、誰かがプロキシミティとペアリングされている場合に画面に表示される [プロキシミティ (Proximity)] アイコンや、ペアリングされたときに表示される通知が含まれます。

この設定は、API またはデバイスの Web インターフェイスを通じて行うことができ、TMS によるプロビジョニングも可能です。

### ミーティングのスケジュールのタイトルを表示しない (すべての製品)

ミーティングのスケジュールのタイトルを表示/非表示にする設定が追加されました。非表示にすると、ミーティング情報の代わりに「ミーティングのスケジュール (Scheduled meeting)」というテキストが表示されます。

### 手動ズーム範囲の拡大

(Room Kit Mini、Room Kit および Room 55)

手動ズームの範囲が、2 倍 (Room Kit Mini) /3 倍 (Room Kit、Room 55) から 5 倍に拡大されました。自動 Best Overview やスピーカートラックのズーム範囲は変わりません。

## デバイスの Web インターフェイスの [通話コントロール (Call Control)] ページを改善 (すべての製品)

- スピーカートラックに対応するデバイスでは、ボタンを使用して現在のスピーカートラックの状態を変更できます。ボタンをクリックすると、スピーカートラックが無効または有効になります。
- [ミュート (Mute)] ボタンには、マイクのミュート状態が正しく反映されます。
- プリセットが選択され、ビデオデバイスに受け入れられると、そのプリセットが青色で強調表示されます。これには、Touch 10 コントローラなどの他のデバイスからの選択も含まれます。ただし、プリセットの強調表示と検出が行われるのは、[カメラの位置 (Camera Positions)] ウィンドウが開いている場合だけです。
- プレゼンタートラックに対応しているデバイスでは、[カメラの位置 (Camera Positions)] ウィンドウからこの機能を有効にできます。
- メインビデオが複数の入力ソースからの合成イメージで構成されている場合は、デフォルトメインビデオのソースが表示されます。これは、デフォルトではメインカメラになります。これにはリモートモニタリングオプションキーが必要です。
- ディレクトリエントリ、通話履歴、お気に入りエントリの表示に関して、一度に表示できる最大数が 50 件から 100 件に増えました。検索フィールドを使用すると、リストを絞り込むことができます。

## CE9.10 の新機能および改善点

### Webex Edge for Devices (すべての製品)

CE9.10 が動作するデバイスでは、*Webex Edge for Devices* を利用できます。Webex Edge for Devices を使用すると、オンプレミスのデバイスを Cisco Webex Cloud サービスにリンクできます。

これにより、登録、デバイス管理、通話、メディアサービスはオンプレミスのままで、特定のクラウド機能にアクセスできるようになります。Webex Control Hub でクラウドサービスを管理したり、サービスからデバイスの診断を受けたりできます。

この機能を使い始めるには、デバイスコネクタツールが必要です。ツールの提供時期については、Webex ヘルプセンターでリリースノートを参照してください。

### Webex ミーティングに簡単に参加 (すべての製品)

ユーザーインターフェイスに [Webexに参加 (Join Webex)] ボタンが追加されました。このボタンはデフォルトで表示されます。

[Webexに参加 (Join Webex)] ボタンでは、ドメインを指定しなくても、ミーティング番号を入力することでミーティングに参加できます。この情報は Webex の招待メールに記載されています。インフラストラクチャでは、\*@webex.com へのコールのルーティングを許可する必要があります。

### パスワードポリシーを定義するための新しい手順

(すべての製品)

以前のソフトウェアバージョンの CE では、パスワードポリシーの定義には `systemtools securitysettings` コマンドを使用していました。現在、このコマンドは設定 (UserManagement PasswordPolicy \*) に置き換えられています。以前にあった制限のいくつかは廃止されました。

以前のソフトウェアバージョンの CE からデバイスをアップグレードする場合、以前に `systemtools securitysettings` コマンドを使用して保存していた値は保持されます。設定に反映されなくなった値は削除されます。以前のデフォルト値はすべて 0 だったため、何も変更していなければ、アップグレード後の新しいデフォルト値もすべて 0 になります。

### SNMP はデフォルトでオフ (すべての製品)

SNMP (簡易ネットワーク管理プロトコル) はデフォルトでオフになります。また、デフォルトのコミュニティ名も提供されなくなりました。

以前のソフトウェアバージョンの CE からデバイスをアップグレードする場合、以前に保存していた値は保持されます。

## CE9.9 の新機能および改善点

### UI 拡張エディタの更新 (すべての製品)

室内制御エディタは、利用可能になった追加機能を反映して *UI 拡張エディタ* という名称に変更されました。エディタを起動するには、Web インターフェイスで [統合 (Integration)] > [UI 拡張エディタ (UI Extension Editor)] に移動します。また、エディタの UI が更新されました。

詳細については、▶ <https://www.cisco.com/go/in-room-control-docs> にある CE9.9 向けのカスタマイズガイドを参照してください。

### Web アプリ (Board)

UI 拡張エディタを使用して Web アプリを作成できます。それにより、Jira、Miro、Office 365、Google ドキュメントなどのアプリに Board からアクセスできます。

### デジタル サイネージ

(Codec Pro、Codec Plus、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、Board)

デジタル サイネージでは、デバイスがハーフ ウェイク モードになっているときに、会社のニュース、ビルの案内図、緊急情報などのカスタム コンテンツを表示することができます。

ユーザは、サイネージ コンテンツを Webex Board だけで操作できます。

### 外部 URL からのブランディング イメージとカスタム壁紙の取得 (すべての製品)

xCommand UserInterface Branding Fetch API コマンドを使用して、外部 URL からブランディングイメージやカスタム壁紙をダウンロードできます。

カスタム壁紙は、Webex Board では使用できません。

### ネットワーク設定メニューの変更

(すべての製品)

デバイスのユーザーインターフェイスの [ネットワーク接続 (Network connection)] ページが変更されました。まず、現在のネットワーク設定が表示され、設定を変更する場合はイーサネットまたは Wi-Fi の設定を開くことができます。以前利用できなかった GUI からの設定がいくつか追加されました。

### 超音波設定の変更 (すべての製品)

すべての製品で、*Audio Ultrasound MaxVolume* 設定に同じデフォルト値が使用されるようになりました。異なる製品間で音量範囲の調整も行われました。製品固有の違いは内部処理され、値の範囲やデフォルト値に反映されなくなりました。デバイスから再生される音声レベルは変更されていません。

### TLS 設定の変更 (すべての製品)

セキュリティ上の理由から、HTTPS クライアント、syslog、および SIP 接続の TLS 設定にいくつかの変更が加えられました。

- 証明書チェックを実行しない場合は、証明書の検証を明示的にオフにする必要があります。デフォルトでは、すべての TLS 接続で証明書がチェックされます。
- TLS の最小バージョンが、バージョン 1.0 から 1.1に上がりました (バージョン 1.0 を許可している CUCM と SIP を除く)。Webex クラウドでは TLS バージョン 1.2 を使用していることに注意してください。
- プロビジョニング、電話帳、およびその他の HTTP サーバについて、証明書の検証を個別に設定できます。これらのすべてのこれらのすべてのサーバータイプをタイプを対象としていた以前の *NetworkServices HTTPS VerifyServerCertificate* 設定は、*Provisioning TLSVerify*、*Phonebook Server [1] TlsVerify*、および *HTTPFeedback TlsVerify* の 3 つの設定に置き換えられました。
- 外部ロギングの証明書の検証 (監査ロギングと通常のロギングの両方) を設定できます。
- SIP の場合、証明書はカスタム CA リストに照らして検証されます。このリストは、Web インターフェイスまたは API を使用して手動でデバイスにアップロードします。その他の接続の場合、証明書は、デバイスにプレインストールされている CA リストまたはカスタム CA リストに照らして検証されます。

### ホワイトボードと注釈の更新 *(Board)*

- ホワイトボードで付箋や注釈を作成、編集、および移動できます。
- ホワイトボードと注釈を使用するときに、3 つの異なるペン サイズから選択できます。
- ホワイトボードと注釈のコピーを作成できます。ホワイトボードメニューには、プレゼンテーションのホワイトボードまたは注釈付きのスナップショットが保存されています。他のホワイトボードやスナップショットの場合と同様に、このコピーに戻って作業を続けることができます。

### 有線タッチリダイレクト *(Board)*

タッチリダイレクトを使用すると、Webex Board の画面からラップトップを制御することができます。ラップトップは、HDMI ケーブル (有線共有) と USB-C ケーブルを使用して Webex Board に接続する必要があります。

タッチリダイレクトは、コール中でないときにのみ機能します。

この機能は、第 2 世代のボード (Webex Board 55S、70S、および 85S) でのみ使用できます。



## CE9.8 の新機能および改善点

### 新商品

以前にはクラウド登録でしか利用できなかった Cisco Webex Board が、オンプレミス登録でも利用できるようになりました。

- Cisco Webex Board 55/55S
- Cisco Webex Board 70/70S
- Cisco Webex Board 85S

### USB ヘッドセットのサポート

*(Room Kit, Room Kit Mini, および Room 55)*

USB ヘッドセット、ハンドセット、または USB Bluetooth Dongle をデバイスの USB-A ポートに接続することができます。これは、DX シリーズと同様です。

### HTTP 要求の拡張サポート *(すべての製品)*

CE9.6 以降、デバイスは任意の HTTP(S) Post および Put 要求を HTTP(S) サーバに送信できるようになりました。この機能が、さらに多くの要求タイプ (Get、Patch、および Delete) をサポートすることになり、サーバから返されるデータ (応答ヘッダおよび本文) の処理機能が拡張されています。

### USB-C エクスペリエンスの改善 *(Room Kit Mini)*

USB-C ポートを介してコンピュータにメディアをストリーミングする場合にのみ、Room Kit Mini は USB カメラ モードとなります。以前のリリースでは、コンピュータに USB-C ポートを接続するだけでこのモードになりました。

### デバイス UI から CMS 会議への参加者の追加

*(すべての製品)*

どのユーザーでも、デバイスのユーザーインターフェイスを使用して、進行中の CMS 会議に別の参加者を追加できます。これには PSTN コールも含まれます。参加者がコールを受け入れると、参加者は同じ CMS 会議に追加されます。

この場合、デバイスが CMS に対し、アクティブ コントロールの仕組みを利用してその参加者にダイヤルするよう指示します。それを受けて CMS は、追加する参加者に直接ダイヤルします。

この機能が動作するためには、デバイス上でアクティブ コントロールが有効であること、コール プロトコルが SIP であること、CMS がバージョン 2.4 以降であることが必要です。マルチポイント モードが CUCMMediaResourceGroupList に設定されている場合、この機能は動作しません。

### API またはローカル Web インターフェイスを使用した Cisco Webex へのデバイスの登録 *(すべての製品)*

デバイスは、Cisco Webex にリモートで登録することができます。その際、デバイスと同じ室内にいる必要はありません。この操作は、API からプログラムによって実行するか、ローカル Web インターフェイス経由で行います。以前のリリースでは、画面上のセットアップ アシスタントを使用する必要がありました。

Web インターフェイスからは、デバイスが現在登録されていない場合のみ、Webex 登録を開始できます。API を使用している場合は、デバイスがオンプレミスのシステム (CUCM または VCS) に現在登録されていても、Webex 登録を開始できます。

### プレインストールされている認証局 (CA) のリスト

*(すべての製品)*

一般に使用される CA 証明書のリストがビデオ会議デバイスに事前にインストールされています。デバイスは、通信している外部サーバからの証明書を検証するときに、このリストを使用します。

- HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバ
- SMTP メール サーバ (Webex Board にのみ該当)

工場出荷時設定へのリセットを行っても、このリストは削除されません。

### WebSocket 経由の xAPI: 認証プロトコルヘッダーを使用した認証 *(すべての製品)*

認証プロトコルヘッダーを使用した認証がサポートされます。これは、HTTP ヘッダー フィールドを使用したベーシック認証に加えて使用されます。

つまり、HTTP ヘッダーを直接制御できないブラウザベースのクライアントでは、Javascript を使用してブラウザから直接デバイスに対して認証を行うことができます。

### Cisco UCM からプロビジョニング可能なデバイス設定の追加 *(すべての製品)*

デバイスが Cisco UCM 12.5(1)SU1 に登録されている場合は、これまでよりも多くの設定とパラメータを UCM からプロビジョニングできます ([デバイス (Device)] > [製品固有の設定レイアウト (Product Specific Configuration Layout)])。また、これらの設定がデバイス上でローカルに変更されている場合は、新しい値を UCM に書き戻すことができます。

これには、公開されているデバイス設定 (xConfiguration) のほとんどが該当します。ネットワーク、プロビジョニング、および SIP 設定については例外が設けられています。

詳細については、▶ [Cisco Unified Communications Manager および IM and Presence Service リリース 12.5\(1\)SU1 のリリースノート](#)の「ビデオエンドポイント管理の概要」の項を参照してください。



## CE9.7 の新機能および改善点

### WebSocket を介した xAPI への接続 (すべての製品)

WebSocket 経由で xAPI に接続できるようになりました。WebSocket 上の通信チャネルは、明示的に閉じられるまで両方向に開かれています。つまり、サーバは新しいデータが利用可能になり次第、クライアントにデータの送信が行えるようになります。また、各要求に対して再認証を行う必要はありません。これは、HTTP と比較してかなり速度が改善されます。

各メッセージには、完全な JSON ドキュメント以外は含まれていません。WebSocket と JSON-RPC では多くのプログラミング言語の優れたライブラリサポートがあります。

WebSocket はデフォルトでは有効ではありません。WebSocket を使用する前に、WebSocket が HTTP に関連付けられていること、および HTTP または HTTPS が有効になっていることに注意してください。

詳細は、▶ [WebSocket 経由の xAPI ガイド](#)を参照してください。

### オーディオコンソールでグラフィックサウンドミキサーを使用可能

(Codec Pro, MX700, MX800, Room 70 G2, Room 70D G2, SX80)

オーディオ コンソールで、グラフィック サウンド ミキサーが利用できるようになりました。これには 8 つのユーザー定義可能なパラメータ化された均等化設定があります。設定は、1 つのフィルタタイプ、ゲイン、中央、クロスオーバー周波数、および Q 値を持つ最大 6 つのセクションで構成されています。各セクションは独自の色で表示され、パラメータのいずれかを変更した結果がすぐにグラフに表示されるようになります。

詳細については、

▶ <https://www.cisco.com/go/in-room-control-docs> にある CE9.7 向けのカスタマイズガイドを参照してください。

### 環境ノイズレポート

(Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Kit, Room Kit Mini)

ルームシリーズデバイスは、室内の固定周囲ノイズを報告するように設定可能です。レポートされた値はA荷重デシベル値 (dBA)で、人間の耳の応答に反響します。レポートされたノイズを元に、施設管理または建物マネージャーは介入して問題をトラブルシューティングできます。

この機能に関連するすべてのシグナリング処理はローカルで、転送されるデータは算出されたノイズレベルだけです。

### マルチ SRG-120DH/PTZ-12 カメラのサポート

(Codec Plus)

HDMI およびイーサネット スイッチを使って最大 3 代の SRG-120DH/PTZ-12 を Codec Plus に接続できるようになりました。

### その他のアップデート

- 1080p は USB カメラとして使用されている場合に Room Kit Mini をサポートします。(Room Kit Mini)
- 通話中にビデオをオフまたはオンにできます。(すべての製品)
- システム管理者は HTTP の使用を防ぎ、HTTPS ポストおよび HTTPS プットリクエストだけを許可できます。(すべての製品)

## CE9.13 での設定の変更点

### 新しい設定

オーディオ マイク AGC (Codec Plus, Room Kit, SX20)

ロギング クラウドアップロード モード (すべての製品)

### 削除された設定

ユーザーインターフェイス ホワイトボード アクティビティインジケータ (MX200 G2, MX300 G2, MX700, MX800, SX10, SX20, SX80)

ユーザーインターフェイス RoomKitTouch 有効 (Board, Room 70 G2, Room Kit Mini, Room Kit, Desk Pro, Room 55, Codec Plus, Room 55 Dual, Room 70, Codec Pro)

### 変更された設定

オーディオ 出力 内蔵スピーカー モード (Codec Plus, MX700/MX800, MX200 G2, MX300 G2, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)

旧: ADMIN

新: ADMIN, INTEGRATOR

カメラ 電源 周波数 (Codec Plus, Codec Pro, Desk Pro, MX200 G2, MX300 G2, MX700, MX800, Room Kit, Room Kit Mini, Room 55, Room 55 Dual, Room 70, Room 70 G2, SX20, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック カメラの位置 パン (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック カメラの位置 チルト (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック カメラの位置 ズーム (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック コネクタ (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック 有効 (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック プレゼンター検出ステータス (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

カメラ プレゼンタートラック トリガーゾーン (Codec Plus, Codec Pro, MX700, MX800, Room 55 Dual, Room 70, Room 70 G2, SX80)

旧: アクセス: public-api-preview

新: アクセス: public-api

会議 アクティブコントロール モード (すべての製品)

旧: アクセス: public-api-preview

新: アクセス: public-web-only

会議 暗号化 モード (すべての製品)

旧: バックエンド: Any

新: バックエンド: On-prem

プロビジョニング CUCM コール管理レコード (すべての製品)

旧: アクセス: public-api-preview

新: アクセス: public-api

旧: デフォルト値: オン

新: デフォルト値: オフ

ユーザーインターフェイス アシスタント モード (Board, Codec Plus, Codec Pro, Desk Pro, Room Kit, Room Kit Mini, Room 55, Room 55 Dual, Room 70, Room 70 G2)

旧: アクセス: public-api-preview

新: アクセス: public-api

ビデオ 入力 コネクタ [n] 最適鮮明度 60fpsのしきい値 (Room Kit, Room 55)

旧: デフォルト: 1920\_1080

新: デフォルト: なし

## CE9.12 での設定の変更点

### 新しい設定

オーディオ 入力 WebView [1] モード (Codec Pro, Room 70 G2)

BYOD タッチ転送 有効 (Board 55S, Board 70S, Board 85S)

カメラ カメラ [n] Flip (Codec Plus, Room 55D, Room 70, Room 70 G2)

カメラ スピーカートラック コネクタ検出 左カメラ (Codec Plus)

カメラ スピーカートラック コネクタ検出 右カメラ (Codec Plus)

カメラ スピーカートラック コネクタ検出 モード (Codec Plus)

カメラ スピーカートラック トラッキングモード (Codec Plus)

HttpClient Httpプロキシの使用 (すべての製品)

HttpFeedback Httpプロキシの使用 (すべての製品)

ネットワークサービス SMTP \* (Room Kit Mini)

プロビジョニング CUCM コール管理レコード (すべての製品)

スタンバイ サイネージ 対話モード (Room Kit Mini)

ユーザインターフェイス 予約 可視性 タイトル (すべての製品)

ユーザインターフェイス 診断 通知 (すべての製品)

ユーザインターフェイス 機能 コール キーパッド (すべての製品)

ユーザインターフェイス プロキシミティ 通知 (すべての製品)

ユーザインターフェイス RoomKitTouch 有効 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

ユーザインターフェイス ホワイトボード アクティビティインジケータ (すべての製品)

音声制御 ウェイクワード モード (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

Webエンジン 機能 WebGL (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

Webエンジン Httpプロキシの使用 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

### 削除された設定

会議 ビデオ帯域幅 モード (すべての製品)

ネットワークサービス SNMP ホスト [1..3] アドレス (すべて製品)

### 変更された設定

マクロ XAPI トランスポート (SX10 を除くすべての製品)

旧: デフォルト: TSH

新: デフォルト: WebSocket

ネットワーク [1] QoS Diffserv オーディオ (すべての製品)

旧: デフォルト: 0

新: デフォルト: 46

ネットワーク [1] QoS Diffserv データ (すべての製品)

旧: デフォルト: 0

新: デフォルト: 34

ネットワーク [1] QoS Diffserv シグナリング (すべての製品)

旧: デフォルト: 0

新: デフォルト: 24

ネットワーク [1] QoS Diffserv ビデオ (すべての製品)

旧: デフォルト: 0

新: デフォルト: 34

ネットワークサービス SMTP ユーザー名 (Board, DX70, DX80)

旧: 文字列 (0, 50)

新: 文字列 (0, 80)

シリアルポート ボーレート (Codec Pro, Room 70 G2)

旧: 115200

新: 9600/19200/38400/57600/115200

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

## CE9.10 での設定の変更点

### 新しい設定

カメラ スピーカートラック クローズアップ (Board)

マクロ 無応答タイムアウト (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2, DX80, DX70)

マクロ XAPI トランスポート (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2, DX80, DX70)

周辺機器 ペアリング Cisco タッチパネル リモートペアリング (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

プロビジョニング WebexEdge (すべての製品)

プロキシミティ 代替ポート 有効 (すべての製品)

セキュリティ Fips モード (すべての製品)

ユーザーインターフェイス アシスタント モード (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

ユーザーインターフェイス アシスタント 会議参加確認 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

ユーザーインターフェイス 機能 コール Webexに参加 (すべての製品)

ユーザ管理 パスワードポリシー 複雑度 数字の最小数 (すべての製品)

ユーザ管理 パスワードポリシー 複雑度 最小文字数 (すべての製品)

ユーザ管理 パスワードポリシー 複雑度 小文字の最小数 (すべての製品)

ユーザ管理 パスワードポリシー 複雑度 特殊文字の最小数 (すべての製品)

ユーザ管理 パスワードポリシー 複雑度 大文字の最小数 (すべての製品)

ユーザ管理 パスワードポリシー 最大有効期間 (すべての製品)

ユーザ管理 パスワードポリシー 再使用制限 (すべての製品)

ビデオ 入力 コネクタ [n] 最適鮮明度 60fpsのしきい値 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

### 削除されたコンフィギュレーション

なし。

### 変更されたコンフィギュレーション

カメラ スピーカートラック クローズアップ (Codec Pro, Codec Plus, Room Kit, Room 55, Room 55D, Room 70, Room 70 G2, SX80, MX700, MX800)

旧: 自動/オフ

新: Auto/Off/On

ネットワークサービス SMTP セキュリティ (Board)

旧: デフォルト: なし

新: デフォルト: StartTls

ネットワークサービス SNMP モード (すべての製品)

旧: デフォルト: 読み取り専用

新: デフォルト値: オフ

スタンバイ サイネージ モード (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

旧: ユーザ ロール: ADMIN

新: ユーザ ロール: ADMIN, INTEGRATOR

ビデオ 入力 コネクタ [n] 最適鮮明度 60fpsのしきい値 (SX80, SX20, MX700, MX800, MX200 G2, MX300 G2)

旧: デフォルト: 1280\_720

新: デフォルト: 1920\_1080

## CE9.9 での設定の変更点

### 新しい設定

オーディオ 入力 ARC [1] モード (Codec Plus)

オーディオ 入力 HDMI [2..3] レベル (Room 55D, Room 70)

オーディオ入力 HDMI [2..3] モード (Room 55D, Room 70)

オーディオ入力 HDMI [2..3] ビデオ関連付けミュート有効非アクティブ ビデオ (Room 55D, Room 70)

BYOD タッチ転送 有効 (Board)

CE9.9.0 では使用できません。

HttpFeedback Tls 検証 (すべての製品)

ログイン 外部 Tls検証 (すべての製品)

電話帳 サーバ [1] Tls 検証 (すべての製品)

プロビジョニング Tls 検証 (すべての製品)

スタンバイ サイネージ オーディオ (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

スタンバイ サイネージ 対話モード (Board)

スタンバイ サイネージ モード (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

スタンバイ サイネージ 更新間隔 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

スタンバイ サイネージ Url (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

ユーザインターフェイス Webcam のみモード (Room Kit Mini)

Web エンジン モード (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

Web エンジン リモートデバッグ (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board)

### 削除された設定

ネットワークサービス HTTPS サーバ証明書検証 (すべての製品)

後継の設定:

- HttpFeedback Tls 検証
- 電話帳 電話帳 サーバ [1] Tls 検証
- プロビジョニング Tls 検証

### 変更された設定

オーディオ 超音波 最大音量 (すべての製品)

多くの製品で値スペースとデフォルト値が変更されました。製品固有の違いは内部処理され、デフォルト値や指定可能な値の範囲に反映されなくなりました。

新: 整数 (0 ~ 90) (Codec Pro, Codec Plus, SX80, SX20)

新: 整数 (0 ~ 70) (Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Board, SX10, MX700, MX800, MX200 G2, MX300 G2, DX70, DX80)

新: デフォルト値: 70 (すべての製品)

RTP ポート範囲終了 (すべての製品)

旧: デフォルト: 70

新: デフォルト: 2487

旧: 整数 (1120 ~ 65535)

旧: 整数 (1121 ~ 65535)

SIP リッスンポート (すべての製品)

旧: オフ/オン

新: Auto/Off/On

SIP リッスンポート (Board)

旧: デフォルト値: オン

新: デフォルト: 自動

SIP Tls検証 (すべての製品)

旧: デフォルト: オフ

新: デフォルト: オン

ビデオ出力コネクタ [n] 位置 水平オフセット (Codec Pro, Codec Plus, Room Kit, Room 55, Room 55D, Room 70, Room 70 G2, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2)

旧: 整数 (-100~100)

新: 文字列 (1, 12)

ビデオ出力コネクタ [n] 位置 垂直オフセット (Codec Pro, Codec Plus, Room Kit, Room 55, Room 55D, Room 70, Room 70 G2, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2)

旧: 整数 (-100~100)

新: 文字列 (1, 12)

## CE9.8 での設定の変更点

### 新しい設定

会議 マルチポイント モード (SX10, DX70, DX80)

ネットワークシステム SMTP 送信元 (Board)

ネットワークサービス SNMP モード (Board)

ネットワークサービス SMTP パスワード (Board)

ネットワークサービス SMTP ポート (Board)

ネットワークサービス SMTP セキュリティ (Board)

ネットワークサービス SMTP サーバ (Board)

ネットワークサービス SMTP ユーザ名 (Board)

シリアルポート ログインが必要 (Codec Pro, Room 70 G2)

ユーザインターフェイス電話帳デフォルト検索フィルタ (すべての製品)

ユーザインターフェイス サウンド エフェクト モード (すべての製品)

### 削除された設定

ビデオ デフォルト レイアウト ファミリ リモート (SX10, DX70, DX80)

### 変更された設定

オーディオ減衰キー クリック検出 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)

旧: デフォルト値: オン

新: デフォルト: True

旧: オフ/オン

新: False/True

オーディオ キー クリック検出の有効化 (Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)

旧: デフォルト: オフ

新: デフォルト: True

旧: オフ/オン

新: False/True

オーディオ 出力 ライン [1..6] 遅延モード (Room 70 G2)

旧: デフォルト: RelativeToHDMI

新: デフォルト: Fixed



## CE9.7 での設定の変更点

### 新しい設定

HttpClient HTTP を許可 (すべての製品)

デバッグ WiFi のロギング (Codec Plus, Codec Pro, DX70, DX80, Room Kit, Room Kit Mini, Room 55, Room 55 D, Room 70, Room 70 G2)

ロギング内部モード (すべての製品)

ネットワークサービス Websocket (すべての製品)

電話帳 サーバ [1] ページネーション (すべての製品)

ルーム分析 環境雑音の予測 モード (Codec Plus, Codec Pro, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)

ユーザインターフェイス機能通話ビデオミュート (Codec Plus, Codec Pro, MX200 G2, MX300 G2, MX700, MX800, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, SX10, SX20, SX80)

ユーザインターフェイス機能 ホワイトボード 開始 (DX70, DX80)

ユーザインターフェイス電話帳モード (すべての製品)

ユーザインターフェイス設定メニュー可視性 (すべての製品)

ユーザインターフェイス Usb プロモーション (Room Kit Mini)

### 削除された設定

ルーム分析 非通話中人数計測 (MX700, MX800)

### 変更された設定

オーディオ入力ライン [1..4] ビデオの関連付け ビデオ入力ソース (MX700, MX800, SX80)

旧: 1/2/3/4/5

新: 1/2/3/4

オーディオ 入力 マイク [1..8] ビデオの関連付け ビデオ入力ソース (Codec Pro, Room 70 G2)

旧: 1/2/3/4/5

新: 1/2/3/4/5/6

オーディオ 入力 マイク [1..8] ビデオの関連付け ビデオ入力ソース (MX700, MX800, SX80)

旧: 1/2/3/4/5

新: 1/2/3/4

ビデオ入力コネクタ [n] カメラ制御モード (Codec Pro, Room 70 G2)

旧: デフォルト値: オン

新: デフォルト値: オフ

旧: オン

新: オン/オフ

ビデオ プレゼンテーション 優先順位 (すべての製品)

旧: Equal/High

新: Equal/High/Low

## Room Kit Mini の概要

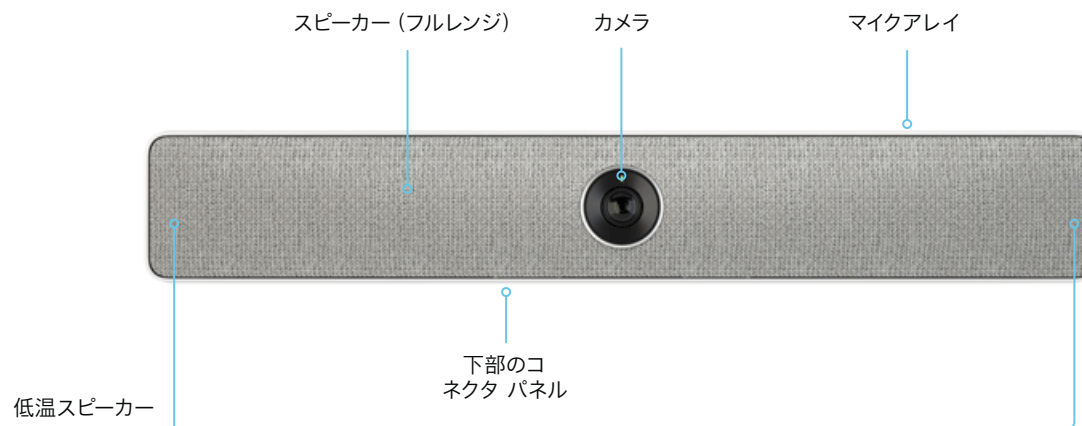
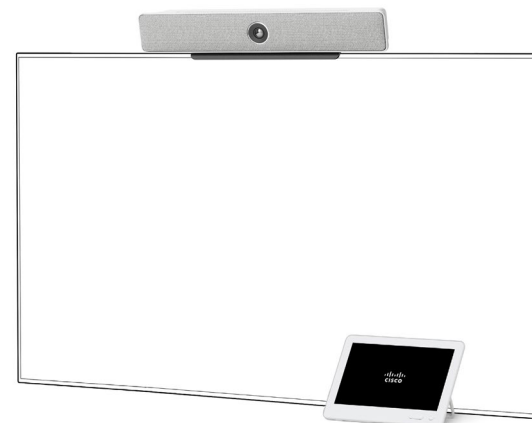
Cisco Webex Room Kit Mini では、カメラ、コーデック、スピーカー、およびマイクが 4K 画面に統合されています。簡単に設置でき、HDMI CEC によってフラット パネル ディスプレイとの優れた統合が実現されます。

Room Kit Mini は、120 度の視野によって 3 ~ 5 人がいるスペース向けに設計されています。以前はハイエンドのビデオ会議室の領域であった洗練された機能が、あらゆる部屋とあらゆるチームに提供されます。

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

### 機能とメリット

- インテリジェントな表示機能を備えた目立たない内蔵カメラ: 会議出席者を検知し、Best Overview を表示します。
- 室内の人数のカウント: 優れたリソース プランニングのための分析を可能にします。
- 内蔵されたマイクとスピーカーによって優れたオーディオ エクスペリエンスが提供されます。
- ノイズ自動抑制機能により、会議室で発生するノイズを低減
- 誰かが会議室に入る時に、モバイル デバイスを介して入室者を認識し、システムがスリープ状態から自動で起動
- Cisco Touch 10 または Cisco Webex Teams アプリケーションで簡単に制御可能
- Cisco Touch 10 による照明やブラインドなどの周辺機器の制御 (室内制御)
- 4K コンテンツ共有 (ローカル会議では 30 fps、遠端では 5 fps)
- 有線またはワイヤレスでのコンテンツ シェアリング
- イーサネットと Wi-Fi
- USB カメラモード (ビデオ会議デバイスのカメラ、マイク、およびスピーカーを含む)
- Cisco Webex Room Kit mini の詳細については、  
▶ <https://www.cisco.com/go/roomkit>を参照してください。



## 電源のオンとオフ

### ユーザインターフェイスを使用した再起動とスタンバイ

#### デバイスの再起動

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [\[設定 \(Settings\)\]](#)、[\[再起動 \(Restart\)\]](#) の順に選択します。
3. [\[再起動 \(Restart\)\]](#) を再度選択して、選択内容を確認します。

#### スタンバイ モードの開始

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [\[スタンバイ \(Standby\)\]](#) を選択します。

#### スタンバイ モードの終了

- ・ Touch コントローラの画面をタップします。

### リモートからのデバイス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 \(Maintenance\)\]](#) > [\[再起動 \(Restart\)\]](#) に移動します。

#### デバイスの再起動

[\[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。

デバイスが使用可能になるまでに数分かかります。

#### デバイスの電源オフ

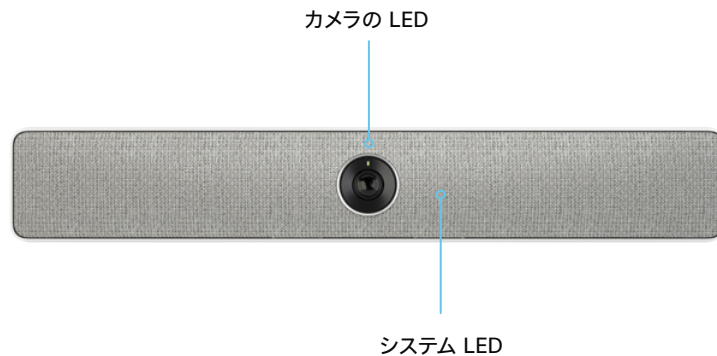
[\[デバイスのシャットダウン... \(Shutdown device...\)\]](#) をクリックして、選択を確定します。



デバイスの電源をリモートから再びオンにすることはできません。

デバイスの電源を入れるには、電源プラグを抜いて再度差し込む必要があります。

## LED インジケータ



### システム LED

アイドル モード時 (スクリーンはアウェイク):

点灯状態になります。

スタンバイ モード時 (スクリーンはオフ):

点灯状態になります。

要注意時 (不在着信がある場合やネットワーク接続がない場合など):

LED が 2 回ずつ、繰り返し点滅します。

スタートアップ (起動) 時:

LED が点滅します。デバイスが使用可能になると点灯状態になります。

### カメラの LED

コールの着信時:

LED が点滅します。

コール中:

点灯状態になります。

セルフビュー オン時:

点灯状態になります。

## ビデオ会議デバイスの管理方法 (1/4 ページ)

一般的には、この管理者ガイドで説明するように、デバイスの管理とメンテナンスに Web インターフェイスを使用することを推奨します。

それ以外にも次の方法でデバイスの API にアクセスできます。

- HTTP/HTTPS (Web インターフェイスでも使用)
- WebSocket
- SSH
- シリアル接続

他のアクセス方法や API の使用方法の詳細については、デバイスの API ガイドをご覧ください。

### ヒント

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

`X > Y > Z` に Value を設定 (Web) することは次と同等です。

`xConfiguration X Y Z: 値 (API)`

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

以下と同じです。

`xStatus X Y Z (API)`

次に例を示します。

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

`xConfiguration SystemUnit Name: MySystem`

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

以下と同じです。

`xStatus SystemUnit Software Version`

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

アクセス方式	注	方式の有効化/無効化方法
HTTP/HTTPS	<ul style="list-style-type: none"> <li>• デバイスの Web インターフェイスで使用されます。</li> <li>• 非セキュア (HTTP) 通信またはセキュア (HTTPS) 通信</li> <li>• HTTPS: デフォルトで [有効 (Enabled)]</li> <li>• HTTP: デバイスを以前のソフトウェア バージョンから CE9.4 以降にアップグレードし、アップグレード後に初期設定にリセットしていない場合のみ、デフォルトで [有効 (Enabled)]</li> </ul>	<p><a href="#">[ネットワークサービス (NetworkServices)] &gt; [HTTP] &gt; [モード (Mode)]</a></p> <p>変更を有効にするには、デバイスを再起動してください。</p>
WebSocket	<ul style="list-style-type: none"> <li>• HTTP に関連付けられるため、WebSocket を使用するには HTTP または HTTPS も有効化する必要があります</li> <li>• 暗号化 (wss) または非暗号化 (ws) の通信</li> <li>• デフォルトで [無効 (Disabled)]</li> </ul>	<p><a href="#">[ネットワークサービス (NetworkServices)] &gt; [HTTP] &gt; [モード (Mode)]</a></p> <p><a href="#">[ネットワークサービス (NetworkServices)] &gt; [WebSocket]</a></p> <p>変更を有効にするには、デバイスを再起動してください。</p>
SSH	<ul style="list-style-type: none"> <li>• セキュアな TCP/IP 接続</li> <li>• デフォルトで [無効 (Disabled)]</li> </ul>	<p><a href="#">[ネットワークサービス (NetworkServices)] &gt; [SSH] &gt; [モード (Mode)]</a></p> <p>デバイスを再起動する必要はありません。変更が有効になるまでに少し時間がかかる場合があります。</p>
シリアル接続	<ul style="list-style-type: none"> <li>• ケーブルを使用してデバイスに接続します。IP アドレス、DNS、ネットワークは不要。</li> <li>• デフォルトで [無効 (Disabled)]</li> <li>• セキュリティ上の理由から、デフォルトではサインインを求められます (<a href="#">[シリアルポート (SerialPort)] &gt; [ログイン必須 (LoginRequired)]</a>)。</li> </ul>	<p><a href="#">[シリアルポート (SerialPort)] &gt; [モード (Mode)]</a></p> <p>変更を有効にするには、デバイスを再起動してください。</p>



すべてのアクセス方式を無効にする ([オフ (Off)] に設定する) と、デバイスを設定できなくなります。再び有効にする ([オン (On)] に設定する) ことはできないため、復元するにはデバイスを初期設定にリセットする必要があります。

ビデオ会議デバイスの管理方法 (2/4 ページ)

## デバイスの Web インターフェイス

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

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

Web ブラウザは最新版を使用することを推奨します。\*

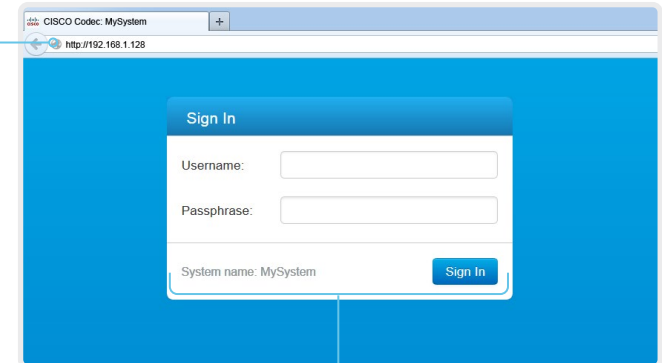
### デバイスへの接続

Web ブラウザを開き、デバイスの IP アドレスをアドレスバーに入力します。



#### IP アドレスの確認方法

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [このデバイスについて (About this device)] に続き、[設定 (Settings)] を選択します。



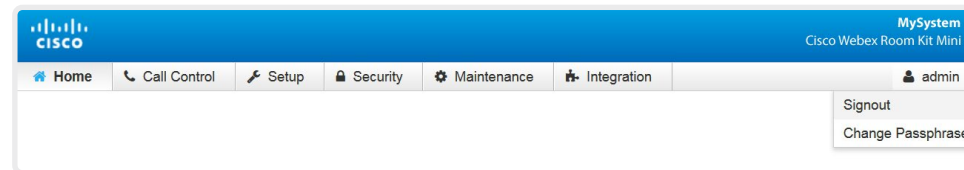
### サインイン

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



デバイスには、*admin* というデフォルト ユーザがパスフレーズなしで用意されています。初めてサインインするときは、[パスフレーズ (Passphrase)] フィールドを空白のままにします。

*admin* ユーザのパスワードを設定する必要があります。



### サインアウト

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

\* Internet Explorer はサポートされなくなりました。

ビデオ会議デバイスの管理方法 (3/4 ページ)

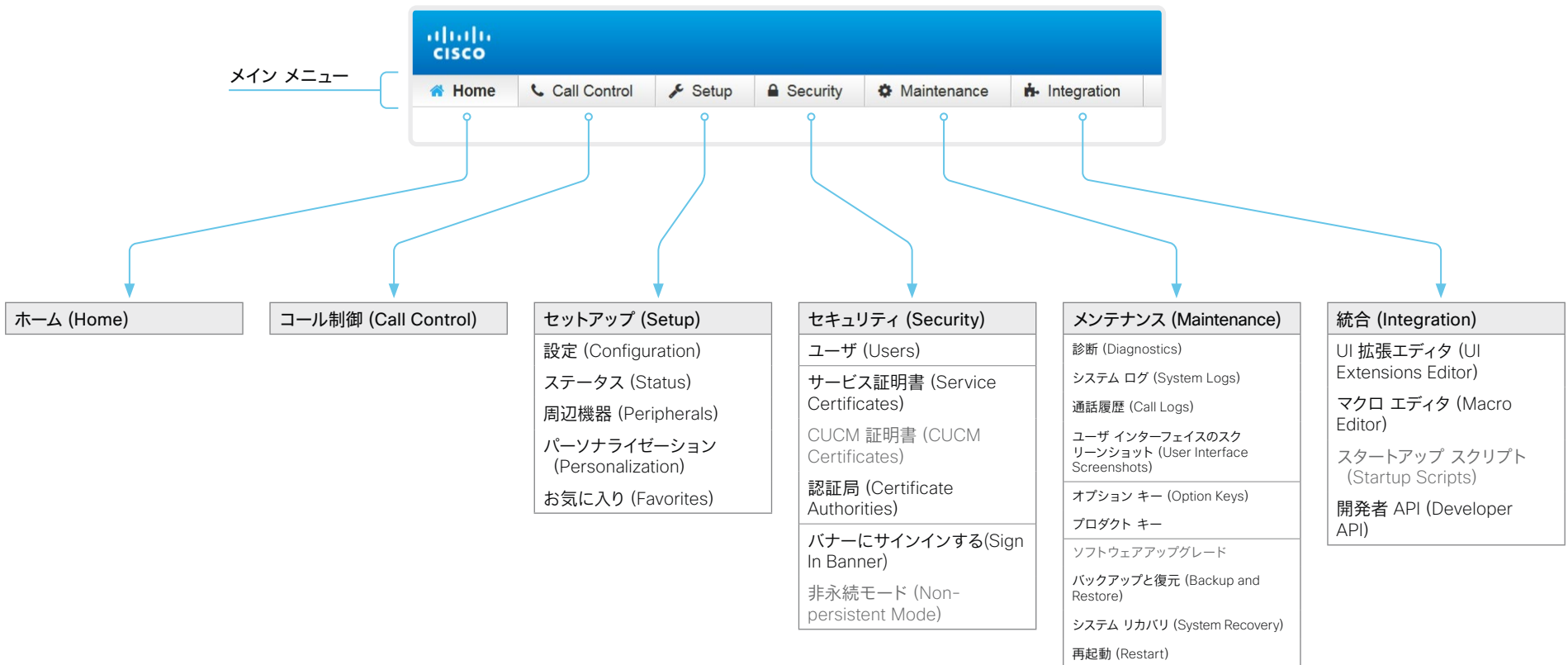
## Web インターフェイスの構成

Web インターフェイスは、各サブページから構成されています。デバイスがオンプレミス サービス (CUCM、VCS) に登録されている場合は、以下のすべてのサブページを使用できます。デバイスがシスコのクラウド サービス (Cisco Webex) に登録されている場合は、灰色で示されているページを使用できません。

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

ユーザ管理、ユーザ ロール、およびアクセス権の詳細については、

▶ 「ユーザ管理」の章をお読みください。



ビデオ会議デバイスの管理方法 (4/4 ページ)

## ユーザ インターフェイス上の設定とデバイス情報


デバイス情報および一部の基本設定とデバイス テストには、デバイスのユーザ インターフェイスからアクセスできます。

デバイスの重要な設定と機能（ネットワーク設定、サービスの有効化、初期設定へのリセットなど）は、パスフレーズで保護できます。▶ [「\[設定 \(Settings\)\] メニューへのアクセスの制限」](#)の章をご覧ください。

一部の設定とテストは、デバイスの電源を初めてオンにしたときに起動するセットアップ アシスタントでも表示されます。セットアップ アシスタントについては、CE ソフトウェアを実行しているデバイスのスタートアップ ガイドをご覧ください。

### 設定へのアクセス

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [\[設定 \(Settings\)\]](#) を選択します。

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

2. 変更する設定または実行するテストを選択します。

設定がロックされている場合は認証ウィンドウが表示され、続行するには ADMIN ログイン情報でサインインする必要があります。



## 第 2 章


# 設定

## ユーザ管理

Web とコマンドライン インターフェイスにアクセスするには、サインインする必要があります。ユーザには、アクセス権を持つ対象を決める、異なるロールを割り当てることができます。

### デフォルトのユーザ アカウント

デバイスには、初期状態でデフォルトの管理者ユーザ アカウントにフル アクセス権が付与されています。ユーザ名は *admin* で、パスワードは初期状態では設定されていません。

 必ず *admin* ユーザのパスワードを設定する必要があります。

パスワードの設定方法については、▶ [「デバイス パスワードの変更」](#)の章をご覧ください。

### 新しいユーザ アカウントの作成

1. Web インターフェイスにサインインし、[\[セキュリティ \(Security\)\] > \[ユーザ \(Users\)\]](#) に移動します。
2. [\[新規ユーザを追加 \(Add New User\)\]](#) を選択します。
3. [ユーザ名 (Username)], [パスワード (Passphrase)], [パスワードの確認 (Repeat passphrase)] の各入力フィールドに入力します。  
デフォルトでは、ユーザが初めてサインインしたときにパスワードを変更する必要があります。  
認証にクライアント証明書を使用する場合にのみ、[クライアント証明書 DN (識別名) (Client Certificate DN)] フィールドに値を入力してください。
4. 適切な [ロール (Roles)] チェックボックスをオンにします。  
admin ロールをユーザに割り当てた場合は、[自分のパスワード (Your passphrase)] 入力フィールドに自分自身のパスワードを確認のために入力します。
5. ユーザをアクティブにするには、[ステータス (Status)] を [アクティブ (Active)] に設定します。
6. [\[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 ロールが割り当てられているユーザを変更する場合は常に、[パスワード (Your passphrase)] 入力フィールドに確認のため各自のパスワードを入力する必要があります。

#### ユーザ特権を変更する

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

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

4. [\[ユーザの編集 \(Edit User\)\]](#) をクリックして変更内容を保存します。  
変更を加えないで終了するには、[\[戻る \(Back\)\]](#) ボタンを使用します。

#### パスワードを変更する

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

#### ユーザ アカウントを削除する

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

### ユーザ ロール

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

ユーザ ロールは次の通りです。

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

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

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

**ROOMCONTROL:** このロールを持つユーザは、カスタマイズされた UI パネル (室内制御など) を作成できます。このユーザは、UI 拡張エディタおよび対応する開発ツールにアクセスできます。

**INTEGRATOR:** このロールを持つユーザは、高度な AV シナリオを設定したり、デバイスをサードパーティの機器と統合したりするために必要な設定、コマンド、およびステータスにアクセスできます。このユーザは、カスタマイズした UI パネルを作成することもできます。

## デバイス パスフレーズの変更

次の操作を行うには、デバイスの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、使用する

### デフォルトのユーザ アカウント

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

**!** デバイス設定へのアクセスを制限するには、デフォルトの *admin* ユーザにパスフレーズを設定する必要があります。さらに、管理者権限を持つ他のすべてのユーザにもパスフレーズを設定する必要があります。

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

### 他のユーザ アカウント

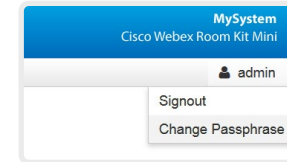
デバイスのユーザ アカウントは複数作成できます。

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。



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

## 別のユーザのパスフレーズの変更

管理者アクセス権がある場合は、すべてのユーザのパスフレーズを変更できます。

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

## [設定 (Settings)] メニューへのアクセスの制限

デフォルトでは、すべてのユーザがユーザインターフェイスから [設定 (Settings)] メニューにアクセスできます。

権限のないユーザがデバイスの設定を変更できないようにするために、このアクセスを制限することを推奨します。

### [設定 (Settings)] メニューのロック

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

これで、ユーザインターフェイス (Touch コントローラ) からデバイスの重要な設定にアクセスするには、ADMIN ログイン情報でサインインする必要があります。

### [設定 (Settings)] メニューのロック解除

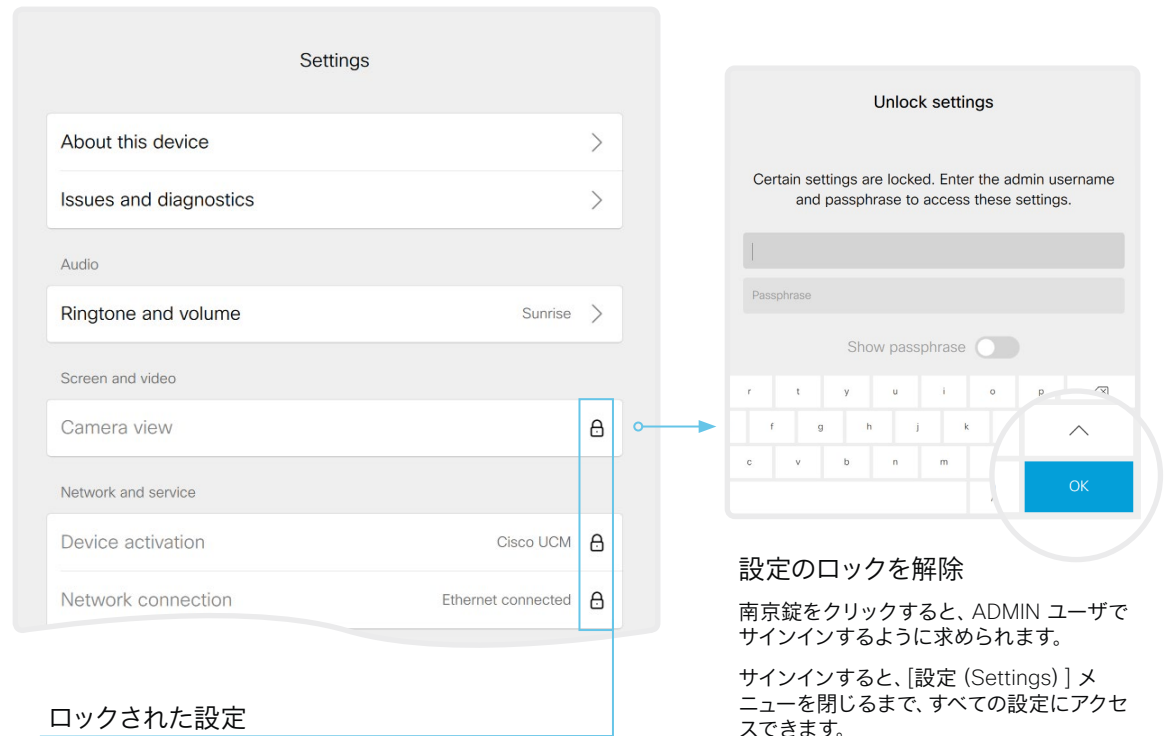
1. Web インターフェイスにサインインして、[セットアップ (Setup)] > [設定 (Configuration)] に移動します。
2. [ユーザインターフェイス (UserInterface)] > [設定メニュー (SettingsMenu)] > [モード (Mode)] に移動して、[ロックなし (Unlocked)] を選択します。
3. をクリックして変更を有効にします。

これで、任意のユーザが、ユーザインターフェイス (Touch コントローラ) から [設定 (Settings)] メニューのすべてにアクセスできるようになります。

### ユーザインターフェイスの [設定 (Settings)] メニュー

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

[設定 (Settings)] メニューを開くには、ユーザインターフェイスの上部にあるデバイス名またはアドレスを選択し、[設定 (Settings)] を選択します。



#### ロックされた設定

ロックされた設定には南京錠のマークが付いています。

#### 設定のロックを解除

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

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

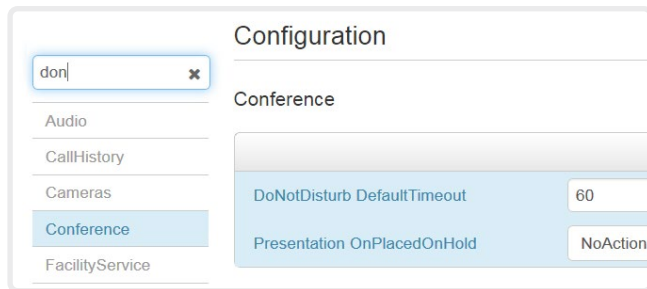
## デバイス設定

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

### デバイス設定の検索

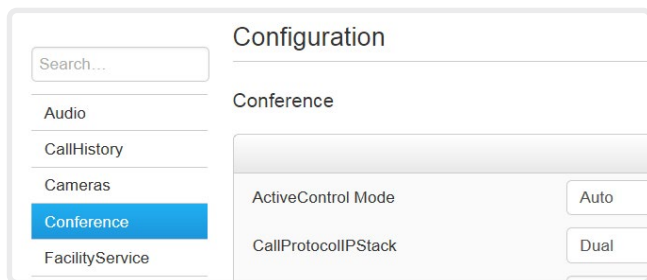
#### 設定を検索する

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



#### カテゴリを選択して設定に移動する

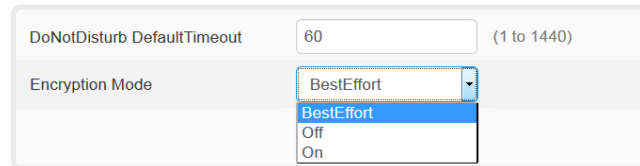
デバイス設定はカテゴリ別にグループ化されています。左側のペインのカテゴリを 1 つ選択して、関連付けられている設定を表示します。



### デバイス設定の変更

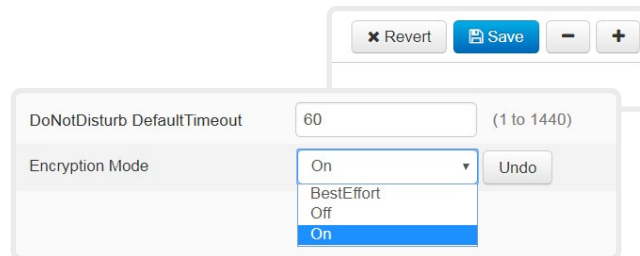
#### 値スペースを確認する

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



#### 値の変更

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



変更が保存されていないカテゴリには、編集記号 (✎) のマークが付きます。

### デバイスの設定について

すべてのデバイス設定を Web インターフェイスから変更できます。

個別のデバイス設定については、[▶ 「デバイス設定」](#) 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 ログイン情報が必要である場合があります。管理者がすべてのデバイス設定を変更できるように、管理者にはすべてのユーザ ロールを割り当てる必要があります。

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

## サインイン バナーの追加

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

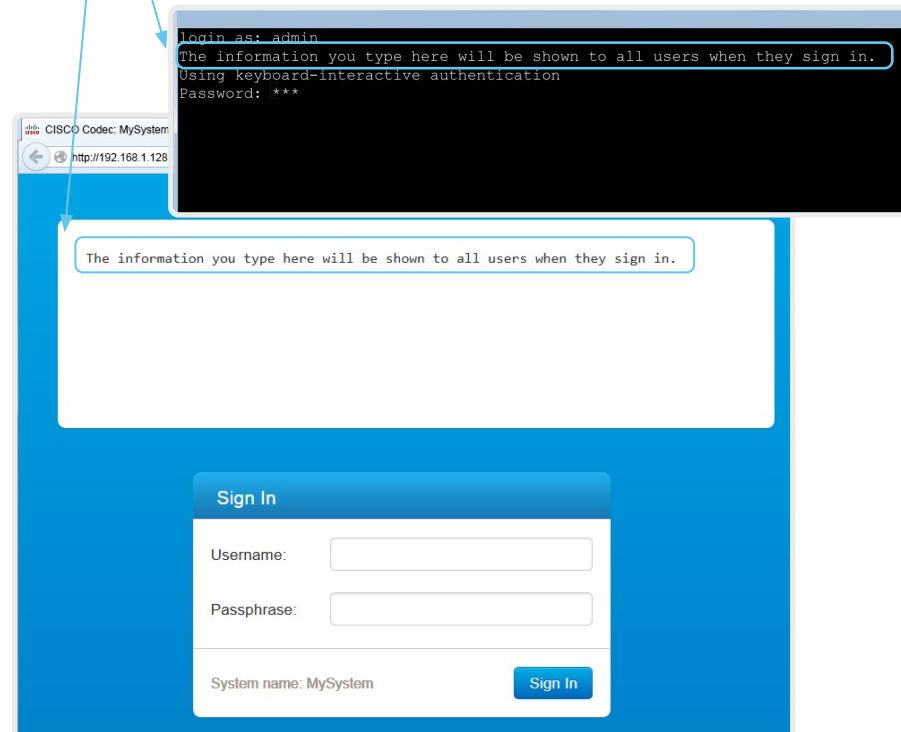
1. サインインしたユーザに表示するメッセージを入力します。
2. [保存 (Save)] をクリックしてバナーをアクティブにします。

### Sign In Banner

The Sign In Banner will be displayed when a user signs in to the video system.

The information you type here will be shown to all users when they sign in.

Save



### サインイン バナーについて

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

最大サイズは 4 kByte です。

### ウェルカムバナーとサインインバナーの比較

#### サインインバナー

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

#### ウェルカムバナー

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

## ウェルカムバナーの追加

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

### API コマンド

```
xCommand SystemUnit WelcomeBanner Set
```

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

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

```
xCommand SystemUnit WelcomeBanner Clear
```

```
xCommand SystemUnit WelcomeBanner Get
```

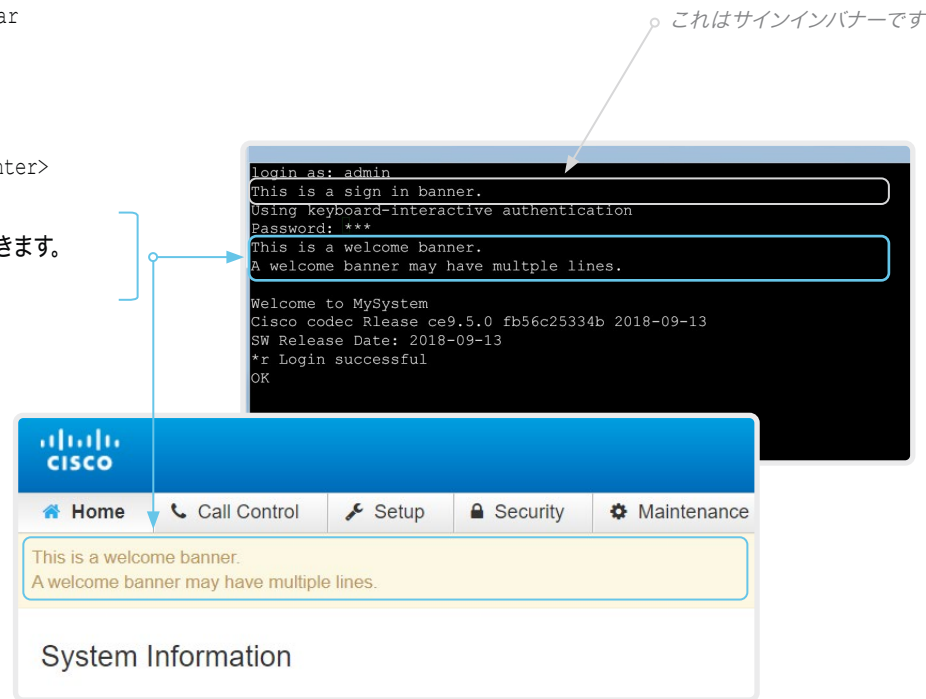
### 例

```
xCommand SystemUnit WelcomeBanner Set <enter>
```

これはウェルカムバナーです。<enter>

ウェルカムバナーには複数の行を表示することができます。<enter>

. <enter>



### ウェルカムバナーについて

デバイスの Web インターフェイスまたはコマンドラインインターフェイスへのサインイン後にユーザーに表示される、ウェルカムバナーを設定できます。バナーには、複数の行を表示することができます。

バナーには、使い始めるうえで必要な情報や、デバイスのセットアップ時に知っておく必要があることなどを記載できます。

最大サイズは 4 kByte です。

### ウェルカムバナーとサインインバナーの比較

#### サインインバナー

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

#### ウェルカムバナー

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



## デバイスのサービス証明書の管理

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

### 証明書を有効/無効にし、表示、または削除する

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

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

### 証明書の追加

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

有効期間が 10 年以内の証明書のみが受け付けられます。

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)
- ・ パズフレーズ (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、デバイス上の同じファイル内に保存されます。

図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

### デバイス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。

通信が確立される前に、有効な証明書をデバイスから提供するようにサーバまたはクライアントから要求されることがあります。

デバイスの証明書は、デバイスの信頼性を確認するテキスト ファイルです。これらの証明書は、認証局 (CA) によって発行されます。

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

複数の証明書をデバイスに保存できませんが、サービスごとに有効化できる証明書は一度に 1 つだけです。

認証が失敗した場合、接続は確立されません。



## 信頼できる認証局 (CA) のリストの管理 (1/4 ページ)

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

通信が確立される前にサーバまたはクライアントに証明書の提供を要求するように、デバイスを設定できます。デバイスは、証明書を使用して、サーバまたはクライアントの信頼性を検証します。認証が失敗した場合、接続は確立されません。

証明書 (テキスト ファイル) は、信頼できる認証局 (CA) によって署名されている必要があります。信頼できる CA からの証明書のリストはデバイス上に保存されています。

### CA 証明書リスト

信頼できる CA のリストの確認とメンテナンスは、デバイスの Web インターフェイスから実行できます。

- 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 \(Certificate Authorities\)\]](#) に移動します。CA リストごとにタブが 1 つ存在します。

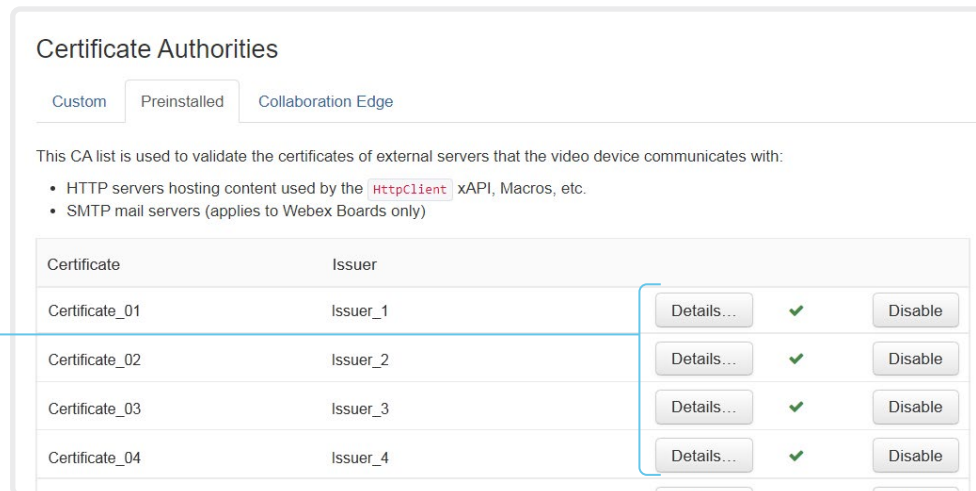
CA リストは次のとおりです。

- **プレインストール**: デバイスと通信する外部サーバ (HTTPS および syslog) の証明書を検証するために使用される、プレインストールされた CA 証明書。
- **コラボレーションエッジ**: デバイスが Cisco Unified Communications Manager (CUCM) によって Expressway を介してプロビジョニングされている場合に、インターネット経由で通信するサーバの証明書を検証するために使用される、プレインストールされた CA 証明書 (MRA またはエッジとも呼ばれます)。
- **カスタム**: 自分でデバイスにアップロードした CA 証明書。ログインおよびその他の接続で証明書を検証するためには、必要な証明書をすべてプレインストール リストに含める必要があります (まだ含まれていない場合)。

信頼できる認証局 (CA) のリストの管理 (2/4 ページ)

## 外部サーバ用にプレインストールされた CA 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 \(Certificate Authorities\)\]](#) に移動して、[\[プレインストール \(Preinstalled\)\]](#) タブを開きます。



図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

**i** プレインストールされた証明書を使用する代わりに、必要な証明書を手動でカスタム証明書リストに追加することもできます。

信頼できる CA 証明書のリストを更新する方法については、  
▶ [「デバイスへの CA 証明書のアップロード」](#)の章をご覧ください。

## プレインストールされた CA 証明書

デバイスには、よく使用される CA 証明書のリストがプレインストールされています。デバイスは、通信している外部サーバからの証明書を検証するときに、このリストを使用します。

- HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバ
- プロビジョニング サーバ
- 電話帳サーバ
- syslog サーバ (外部ロギング用)
- Cisco Webex クラウドによって使用されるサーバおよびサービス

デバイスを初期設定にリセットしても、プレインストールされた証明書のリストは削除されません。

### 証明書の表示または無効化

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

信頼できる認証局 (CA) のリストの管理 (3/4 ページ)

## Expressway プロビジョニングを使用する CUCM 用のプレインストール済み CA 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 \(Certificate Authorities\)\]](#) に移動して、[\[コラボレーションエッジ \(Collaboration Edge\)\]](#) タブを開きます。

**Certificate Authorities**

Custom Preinstalled Collaboration Edge

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

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

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

Disable All

### 証明書の表示または無効化

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

図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。

**i** プレインストールされた証明書を使用する代わりに、必要な証明書を手動でカスタム証明書リストに追加することもできます。

信頼できる CA 証明書のリストを更新する方法については、  
▶ [「デバイスへの CA 証明書のアップロード」](#) の章をご覧ください。

### Expressway を使用する CUCM 用のプレインストール済み CA 証明書

このリストにあるプレインストール CA 証明書は、デバイスを Cisco Unified Communications Manager (CUCM) によって Expressway 経由でプロビジョニングする場合 (エッジ) にのみ使用されます。

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

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

デバイスを初期設定にリセットしても、プレインストールされた証明書のリストは削除されません。

信頼できる認証局 (CA) のリストの管理 (4/4 ページ)

## デバイスへの CA 証明書のアップロード

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 \(Certificate Authorities\)\]](#) に移動して、[\[カスタム \(Customs\)\]](#) 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)。

### 信頼できる CA 証明書のカスタム リストについて

このリストには、自分でデバイスにアップロードした CA 証明書が含まれます。これらの証明書は、クライアント証明書とサーバ証明書の両方について、ロギングおよびその他の接続を検証するために使用できます。

次のものに使用できます。

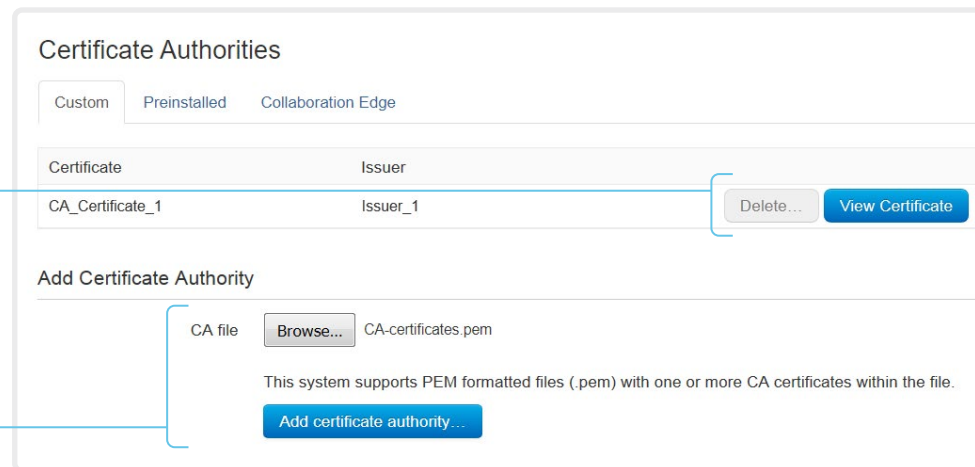
- ・ HttpClient API またはマクロによって使用されるコンテンツをホストしている HTTP サーバ
- ・ プロビジョニング サーバ
- ・ 電話帳サーバ
- ・ SIP サーバ
- ・ syslog サーバ (外部ロギング用)
- ・ Cisco Expressway インフラストラクチャ
- ・ Cisco Webex クラウドによって使用されるサーバおよびサービス

### 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。

### CA 証明書のリストのアップロード

1. [\[参照 \(Browse\)\]](#) ボタンをクリックして、コンピュータから CA 証明書のリストを含むファイル (ファイル形式: .PEM) を見つけます。
2. [\[認証局の追加... \(Add certificate authority...\)\]](#) をクリックして、新しい CA 証明書をデバイスに保存します。



図に示している証明書および証明書発行者は一例です。お使いのデバイスの証明書はこれとは異なります。



以前に保存した証明書は自動的に削除されません。

CA 証明書を含む新しいファイル内のエントリが既存のリストに付加されます。

## セキュア監査ロギングのセットアップ

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



監査サーバの証明書を検証する認証局 (CA) が、デバイス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。含まれていない場合は、外部サーバにログが送信されません。

リストの更新方法については、▶ [「デバイスへの CA 証明書のアップロード」](#)の章を参照してください。

1. [\[セキュリティ \(Security\)\]](#) カテゴリを開きます。
2. [\[監査 \(Audit\)\] > \[サーバ \(Server\)\]](#) 設定を探して、監査サーバの [\[アドレス \(Address\)\]](#) を入力します。  
[\[ポート割り当て \(PortAssignment\)\]](#) を [\[手動 \(Manual\)\]](#) に設定した場合は、監査サーバの [\[ポート \(Port\)\]](#) 番号も入力する必要があります。
3. [\[監査 \(Audit\)\] > \[ロギング モード \(Logging Mode\)\]](#) を [\[外部セキュア \(ExternalSecure\)\]](#) に設定します。
4. [\[保存 \(Save\)\]](#) をクリックして変更を有効にします。

The screenshot shows the 'Configuration' window for 'Security' settings. Under the 'Audit' section, the 'Logging Mode' dropdown menu is open, with 'ExternalSecure' selected. Below it, the 'Server' section contains three fields: 'Address' (empty), 'Port' (514), and 'PortAssignment' (Auto). The 'OnError Action' dropdown is also visible, with 'ExternalSecure' selected. Buttons for 'Revert', 'Save', and 'Undo' are present.

### 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、そのデバイスでのすべてのサインイン アクティビティと設定変更が記録されます。

[\[セキュリティ \(Security\)\] > \[監査 \(Audit\)\] > \[ロギング モード \(Logging Mode\)\]](#) 設定を使用して、監査ロギングを有効にします。監査ロギングは、デフォルトでは無効になっています。

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

監査サーバの署名は、プレインストールされている CA 証明書またはカスタム CA リストを使用して検証されます。

監査サーバ認証に失敗した場合は、監査ログが外部サーバに送信されません。


## CUCM 信頼リストの削除

この章の情報は、Cisco Unified Communications Manager (CUCM) に登録されているデバイスにのみ関連します。

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

### CUCM 信頼リストを削除する

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

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

次のようなケースでは、これらのファイルを削除する必要があります。

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

### 信頼リスト フィンガープリントと証明書の概要

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

この情報は、トラブルシューティングに役立ちます。

### 信頼リストの詳細

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

## 永続モードの変更

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

### 永続性ステータスの確認

アクティブなラジオ ボタンは、デバイスの現在の永続性ステータスを示しています。

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

### 永続設定を変更する

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

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

デバイスが自動的に再起動します。再起動後、新しい永続設定に従って動作が変化します。



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

### 永続モード

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

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

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

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



[\[非永続 \(Non-persistent\)\]](#) モードに変更する前に保存された情報は、自動的にクリアまたは削除されることはありません。そのような情報を削除するには、デバイスを初期設定にリセットする必要があります。

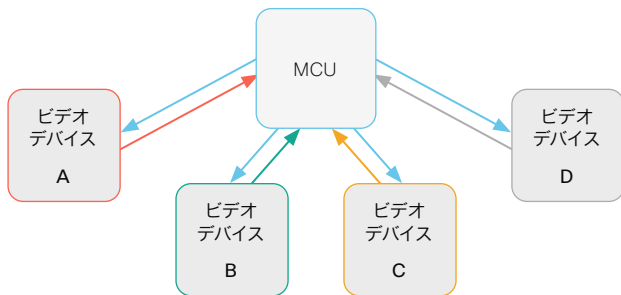
初期設定にリセットする方法の詳細については、[▶ 「ビデオ会議デバイスの初期設定へのリセット」](#) の章を参照してください。

## アドホック マルチポイント会議のセットアップ (1/2 ページ)

ポイントツーポイントのビデオ コール (2 者間のみのコール) を、より多くの参加者とのマルチポイント会議に拡大する方法はいくつかあります。

### 集中型会議インフラストラクチャ

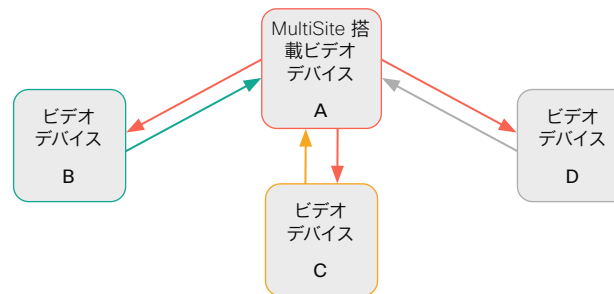
ほとんどのソリューションは、一元化された会議インフラストラクチャである MCU (マルチポイントコントロールユニット)<sup>1</sup> を基盤としています。



このセットアップでは、ビデオ デバイス A、B、C および D は、4 者会議に参加しています。MCU がすべてのデバイスからのメディア ストリームを受信し、ストリームを処理して、すべてのメディアを他の参加者に送信します。

### ローカル会議リソース - マルチサイト (SX10、DX70、および DX80 では使用不可)

MultiSite のシナリオでは、ビデオ デバイスのうち 1 台に MCU 機能を担当させます。



このセットアップでは、ビデオ デバイス A、B、C および D は、4 者会議に参加しています。ここではデバイス A で MultiSite 機能を使用し、MCU として機能させます。このデバイスがすべてのデバイスからのメディア ストリームを受信し、ストリームを処理して、すべてのメディアを他の参加者に送信します。

マルチサイトは標準の製品デリバリーには含まれていません。デバイスにマルチサイトオプションキーをインストールするには、アップグレードオプションの購入が必要です。

MultiSite でサポートされる参加者の最大数は次のとおりです。

- SX10、DX70、および DX80: MultiSite サポートなし
- SX80、MX700、および MX800: 参加者 5 人 (自身を含む) と追加の音声コール 1 つ
- Codec Pro、Room 70 G2、Room Panorama、Room 70 Panorama、Desk Pro: 参加者 5 人 (自身を含む)
- その他の製品: 参加者 4 人 (自身を含む)

### マルチポイント設定

マルチポイント会議の処理方法を決定するには、[\[会議 \(Conference\)\] > \[マルチポイント \(Multipoint\)\] > \[モード \(Mode\)\]](#) 設定を使用します。この設定で使用できる値は次のとおりです。

- Auto
- CUCMMediaResourceGroupList
- MultiSite (SX10、DX70、DX80 では使用不可)
- Off (SX10、DX70、DX80 では使用不可)

次のページの表で、さまざまな会議オプションについて説明しています。

<sup>1</sup> MCU: マルチポイント コントロール ユニットは、ビデオ会議ゲートウェイまたはビデオ会議ブリッジとも呼ばれます。



## アドホック マルチポイント会議のセットアップ (2/2 ページ)

会議マルチポイント モード設定	MultiSite オプション キー	リモート デバイス タイプ <sup>2</sup>	参加者を追加する操作
オフ (Off) <sup>3</sup>	該当なし	MCU	直接リモート追加 <ul style="list-style-type: none"> <li>MCU が [参加者の追加 (Add Participant)] をサポートしている場合、UI に [追加 (Add)] ボタンが表示され、次の参加者を直接コールすることができます。新しい参加者がコールを受け入れるとすぐに会議に追加されます。</li> <li>MCU が [参加者の追加 (Add Participant)] をサポートしていない場合、UI に [追加 (Add)] ボタンは表示されません。</li> </ul>
		ビデオ デバイス	1 オーディオ追加 <ul style="list-style-type: none"> <li>音声のみの参加者を 1 人追加できます。</li> <li>ビデオでの参加者は追加できません。</li> </ul>
CUCM メディア リソースグループ リスト (CUCM-MediaResource-GroupList)	該当なし	ビデオ デバイス	協議追加 <ul style="list-style-type: none"> <li>CUCM に登録されたデバイスでのみ使用でき、[SIP タイプ (SIP Type)] 設定は [シスコ (Cisco)] にする必要があります。</li> <li>新しい参加者をコールする間、会議は保留されます。新しい参加者がコールを受け入れると、その新しいコールを会議にマージできます。</li> <li>会議に新しい参加者を最初に追加した参加者だけが、さらに参加者を追加できます。</li> </ul>
マルチサイト (MultiSite) <sup>3</sup>	はい	該当なし	ローカルマルチサイト <sup>4</sup> <ul style="list-style-type: none"> <li>UI に [追加 (Add)] ボタンが表示され、次の参加者を直接呼び出すことができます。</li> <li>デバイスの上限に達するまで参加者の追加を続けることができます。</li> </ul>
	x	該当なし	1 オーディオ追加 <ul style="list-style-type: none"> <li>音声のみの参加者を 1 人追加できます。</li> <li>ビデオでの参加者は追加できません。</li> </ul>
自動 (Auto)	はい	MCU	直接リモート追加 <ul style="list-style-type: none"> <li>MCU が [参加者の追加 (Add Participant)] をサポートしている場合、UI に [追加 (Add)] ボタンが表示され、次の参加者を直接コールすることができます。新しい参加者がコールを受け入れるとすぐに会議に追加されます。</li> <li>MCU が [参加者の追加 (Add Participant)] をサポートしていない場合、UI に [追加 (Add)] ボタンは表示されません。</li> </ul>
		ビデオ デバイス	カスケードなしのローカルマルチサイト <sup>4</sup> <ul style="list-style-type: none"> <li>UI に [追加 (Add)] ボタンが表示され、次の参加者を直接呼び出すことができます。</li> <li>デバイスの上限に達するまで参加者の追加を続けることができます。</li> <li>MultiSite ホスト (MCU として機能しているデバイス) のみが参加者を追加できます。これにより、会議のカスケードを防ぎます。</li> </ul>
	x	MCU	直接リモート追加 <ul style="list-style-type: none"> <li>MCU が [参加者の追加 (Add Participant)] をサポートしている場合、UI に [追加 (Add)] ボタンが表示され、次の参加者を直接コールすることができます。新しい参加者がコールを受け入れるとすぐに会議に追加されます。</li> <li>MCU が [参加者の追加 (Add Participant)] をサポートしていない場合、UI に [追加 (Add)] ボタンは表示されません。</li> </ul>
		ビデオ デバイス	1 オーディオ追加 <ul style="list-style-type: none"> <li>音声のみの参加者をさらに 1 人追加できます ((SX10、DX70、および DX80 ではサポートされていません)。</li> <li>ビデオでの参加者は追加できません。</li> </ul>

<sup>2</sup> リモート デバイス タイプは、Call [n] DeviceType ステータスに表示されます。

<sup>3</sup> SX10、DX70、および DX80 ではサポートされません。

<sup>4</sup> 会議のカスケードを避けるために、会議 マルチポイント モード を マルチサイト ではなく 自動 に設定することを推奨します。

## コンテンツ共有用のインテリジェントプロキシミティのセットアップ (1/5 ページ)

Cisco Proximity を使用すると、ユーザは自分のモバイル デバイス (スマートフォン、タブレット、またはラップトップ) がビデオ会議デバイスの近くにある場合に、コンテンツをデバイスで直接表示、制御、キャプチャ、共有することができます。

モバイル デバイスがビデオ会議デバイスから送信される超音波の範囲内に入ると、自動的にビデオ会議デバイスとペアリングできます。



プロキシミティの同時接続数は、ビデオ会議デバイスのタイプによって異なります。この最大接続数に達すると、新しいユーザはクライアントから警告されます。

ビデオ会議デバイス	最大接続数
Room Kit, Room Kit Mini, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Panorama, Room 70 Panorama, Codec Plus, Codec Pro	30/7 *
Desk Pro	30/7 *
Board 55/55S, Board 70/70S, Board 85S	30/7 *
SX80, MX700, MX800	10
SX10, SX20, MX200 G2, MX300 G2	7
DX70, DX80	3

\* モバイル デバイス上での共有コンテンツの表示サービスが無効になっている場合、接続数は 30 になります。このサービスが有効になっている場合、接続数は 7 になります。

### プロキシミティ サービス

コールの発信とビデオ会議デバイスの制御:

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

モバイル デバイス上での共有コンテンツの表示:

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

ラップトップからワイヤレスで共有:

- ・ プレゼンテーション ケーブルを接続しないコンテンツの共有
- ・ ラップトップ (OS X と Windows) で使用可能



## コンテンツ共有用のインテリジェントプロキシミティのセットアップ (2/5 ページ)

### Cisco Proximity クライアントをインストールする

#### クライアントの入手場所

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

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

#### エンド ユーザ ライセンス契約書

エンド ユーザ ライセンス契約書をよく確認してください。

▶ [https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN\\_.html](https://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。

## コンテンツ共有用のインテリジェントプロキシミティのセットアップ (3/5 ページ)

### 超音波の放出

シスコのビデオ会議デバイスは、プロキシミティ機能の一部として超音波のペアリングメッセージを発します。

[[プロキシミティ \(Proximity\)](#)] > [[モード \(Mode\)](#)] 設定を使用して、プロキシミティ機能 (および超音波ペアリングメッセージの出力) の [オン (On)] と [オフ (Off)] を切り替えます。

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

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

*Room 70, Room 70 G2, Room Panorama, Room 70 Panorama, Room 55, Room 55 Dual, Room Kit, Room Kit Mini, Room Kit Plus, SX10N および MX シリーズ:*

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

*Desk Pro, DX70, DX80 :*

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

*Board :*

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

Board 50 および 70 (S シリーズ以外) の場合、スピーカーが下向きのため、画面の真下ではレベルが若干高くなる場合があります。

*Codec Plus, Codec Pro, SX10, SX20 および SX80 :*

- これらのビデオ会議デバイスでは、サードパーティのスピーカーで超音波が放出されるため、超音波の音圧レベルを予測できません。スピーカー自体の音量コントロール、および [[音声 \(Audio\)](#)] > [[超音波 \(Ultrasound\)](#)] > [[最大音量 \(MaxVolume\)](#)] での設定は、超音波の音圧レベルに影響を与えません。リモートコントロールまたはタッチコントローラでの音量調節は効果ありません。

### ヘッドセット

*Desk Pro, DX70, DX80, SX10N :*

これらのデバイスでは、次の理由からヘッドセットを常に使用できます。

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

*Room 70, Room 70 G2, Room Panorama, Room 70 Panorama, Room 55 Dual, Room Kit Plus, Codec Plus, Codec Pro, Board, SX10, SX20, SX80, および MX シリーズ:*

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

*Room 55, Room Kit, Room Kit Mini :*

- これらのデバイスでは、USB 出力にいつでもヘッドセットを接続できます。この出力から超音波が送出されることはありません。
- Room 55 および Room Kit のオーディオライン出力 (ミニジャック) は、ヘッドセット向けには設計されていません。これらの出力のいずれかに接続されている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。

ヘッドセットをオーディオライン出力に接続する場合は、超音波の送出手をオフにしておくことを強くお勧めします ([[プロキシミティ \(Proximity\)](#)] > [[モード \(Mode\)](#)] を [[オフ \(Off\)](#)] に設定します)。この場合、[プロキシミティ (Proximity)] 機能を使用することはできません。

## コンテンツ共有用のインテリジェントプロキシミティのセットアップ (4/5 ページ)

### プロキシミティ サービスを有効にする

1. Web インターフェイスにサインインして、[\[セットアップ \(Setup\)\] > \[設定 \(Configuration\)\]](#) に移動します。
2. [\[プロキシミティ \(Proximity\)\] > \[モード \(Mode\)\]](#) に移動します。[プロキシミティ (Proximity)] が On (デフォルト) になっていることを確認します。この場合、ビデオ会議デバイスは超音波のペアリング メッセージを送信します。

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

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

コールの発信とビデオ会議デバイスの制御:

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

モバイル デバイス上での共有コンテンツの表示:

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

デスクトップ クライアントからのワイヤレス共有:

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

### プロキシミティ インジケータ



1 つ以上の Proximity クライアントがデバイスとペアリングされていると、画面にプロキシミティ インジケータが表示されます。

最後のクライアントのペアリングが解除されても、インジケータはすぐには消えません。消えるまで数分かかることがあります。

### プロキシミティについて

プロキシミティ機能はデフォルトでオンに設定されています。

[プロキシミティ (Proximity)] を [オン (On)] にすると、ビデオ会議デバイスから超音波のペアリング メッセージが発信されます。

超音波のペアリング メッセージは、Proximity クライアントがインストールされた近くにあるデバイスによって受信され、デバイスの認証および許可をトリガーします。

プロキシミティが設置環境に適していることを確認した場合は、ユーザーエクスペリエンスを最適化するために、プロキシミティを常に [オン (On)] にしておくことをお勧めします。

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

## コンテンツ共有用のインテリジェントプロキシミティのセットアップ (5/5 ページ)

### 部屋の考慮事項

#### 部屋の音響

- 壁/床/天井の表面が硬い部屋では、音の反響が大きいことが問題になる場合があります。最良の会議環境とインテリジェント プロキシミティのパフォーマンスを確保するために、会議室の音響処理を常に強く推奨します。
- 1 つの部屋の中で Intelligent Proximity を有効にするビデオ会議デバイスは 1 つだけにすることを推奨します。複数あると、干渉が発生する可能性があり、デバイス検出とセッション メンテナンスの問題の原因となることがあります。

### プライバシーについて

シスコのプライバシーポリシー ポリシーと Cisco Proximity 付録には、クライアントにおけるデータ収集とプライバシーの懸念事項が記載されており、この機能を組織に導入する際にはこれを考慮する必要があります。次のページを参照してください。

▶ <https://www.cisco.com/web/siteassets/legal/privacy.html>

### 基本的なトラブルシューティング

プロキシミティ クライアントを使用するデバイスを検出できない

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

#### オーディオ アーチファクト

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

#### ラップトップから内容を共有できない

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

### その他のリソース

Cisco Proximity のサイト:

▶ <https://proximity.cisco.com>

サポートフォーラム:

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

## ビデオ品質対コールレート比の調整 (1/2 ページ)

### ビデオ入力品質の設定

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

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

### 最適鮮明度プロファイル

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

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

異なる最適鮮明度プロファイルに使用する一般的な解像度、コールレートおよび送信フレーム レートの一部を次のページの表に示します。解像度とフレーム レートは、発信側と着信側の両方のデバイスでサポートされている必要があります。

### 60 fps でのビデオ送信のしきい値

60 fps でのビデオ送信を許可する条件を決定するには、[ビデオ 入力 コネクタ n 最適鮮明度 60fpsのしきい値 (Video Input Connector n OptimalDefinition Threshold60fps60fps)] 設定を使用します。

このしきい値より低い解像度では、最大転送フレームレートが 30 fps になります。このしきい値より高い解像度については、使用可能な帯域幅が十分であれば 60 fps になる可能性があります。

### 60 fps のビデオの許可

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

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

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

1. [ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [品質 (Quality)] を選択して、ビデオ品質パラメータを [モーション (Motion)] に設定します (Connector 1 (内蔵カメラ) ではこの手順をスキップします)。
2. [ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [最適鮮明度 (OptimalDefinition)] > [プロファイル (Profile)] に移動して、適切な最適鮮明度プロファイルを選択します。
3. [ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [最適鮮明度 (OptimalDefinition)] > [60fpsのしきい値 (Threshold60fps)] に移動して、その解像度よりも低い場合に最大転送フレームレートを 30 fps にするしきい値を設定します。
4. [カメラ (Cameras)] > [カメラ (Camera)] > [フレームレート (Framerate)] に進み、60fps のビデオを許可するかどうかを選択します。



## ビデオ品質対コール レート比の調整 (2/2 ページ)

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

コール レート (kbps)	H.264、最大 30fps			H.264、最大 60fps		
	標準	中	高	標準	中	高
128	320 × 180 @ 30	320 × 180 @ 30	512 × 288 @ 30	320 × 180 @ 30	512 × 288 @ 20	512 × 288 @ 30
256	512 × 288 @ 30	640 × 360 @ 30	768 × 448 @ 30	512 × 288 @ 30	640 × 360 @ 30	768 × 448 @ 30
384	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30
512	768x448@30	1024x576@30	1024x576@30	768x448@30	1024x576@30	1024x576@30
768	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1024 × 576 @ 30	1280 × 720 @ 30	1280 × 720 @ 30
1152	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 60
1472	1280 × 720 @ 30	1280 × 720 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 60
1920	1280x720@30	1920x1080@30	1920x1080@30	1280x720@30	1280x720@60	1280x720@60
2560	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
3072	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
4000	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1920x1080@60	1920x1080@60
6000	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60

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

コール レート (kbps)	H.265、最大 30fps			H.265、最大 60fps		
	標準	中	高	標準	中	高
128	512 × 288 @ 30	512 × 288 @ 30	640 × 360 @ 30	512 × 288 @ 30	512 × 288 @ 30	640 × 360 @ 30
256	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30	640 × 360 @ 30	768 × 448 @ 30	768 × 448 @ 30
384	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30	768 × 448 @ 30	1024 × 576 @ 30	1280 × 720 @ 30
512	1024x576@30	1280x720@30	1280x720@30	1024x576@30	1280x720@30	1280x720@30
768	1280 × 720 @ 30	1280 × 720 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 30	1280 × 720 @ 60
1152	1280 × 720 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 30	1280 × 720 @ 60	1280 × 720 @ 60
1472	1280 × 720 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1280 × 720 @ 60	1280 × 720 @ 60	1280 × 720 @ 60
1920	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
2560	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1920x1080@60	1920x1080@60
3072	1920x1080@30	1920x1080@30	1920x1080@30	1920x1080@60	1920x1080@60	1920x1080@60
4000	1920x1080@30	1920x1080@30	1920x1080@30	1920x1080@60	1920x1080@60	1920x1080@60
6000	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 30	1920 × 1080 @ 60	1920 × 1080 @ 60	1920 × 1080 @ 60



## 画面および Touch 10 ユーザインターフェイスへの企業ブランディングの追加 (1/2 ページ)

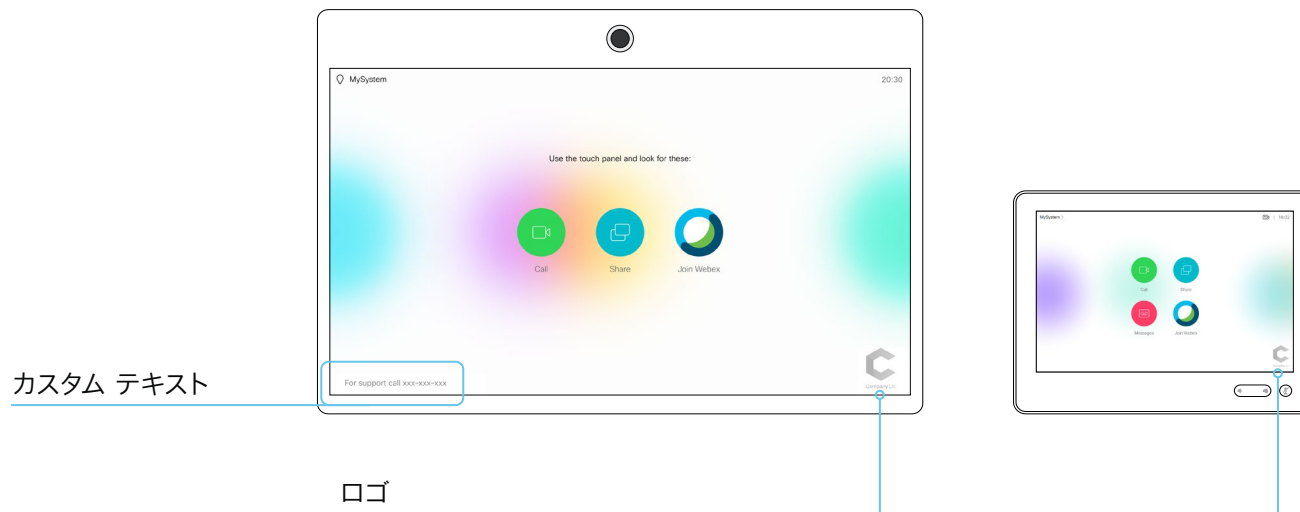
Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[パーソナライゼーション \(Personalization\)\]](#) に移動して、[\[ブランディング \(Branding\)\]](#) タブを開きます。

このページから、独自のブランディング要素 (背景ブランドイメージ、ロゴ、カスタムメッセージ) をビデオ会議デバイスに追加できます。

### アウェイク状態のブランディング

アウェイク状態では、次のことができます。

- ・ 右下隅にロゴを追加します (画面および Touch 10)。
- ・ 左下隅に短いメッセージ (テキストのみ) を追加します (画面のみ、Touch 10 では不可)



### ロゴ

推奨事項:

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

### ブランディングについて

この章で説明するブランディング機能では、シスコの全体的なユーザエクスペリエンスを損なうことなく、画面と Touch ユーザインターフェイスの表示をカスタマイズできます。

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

ブランド機能とカスタム壁紙は、同時に使用できません。

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

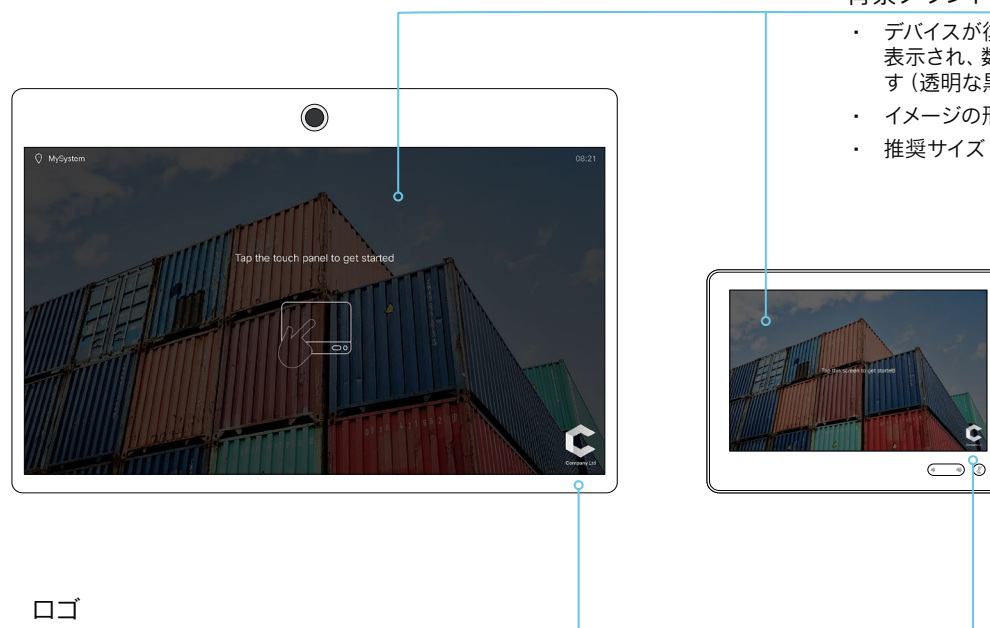
## 画面および Touch 10 ユーザーインターフェイスへの企業ブランディングの追加 (2/2 ページ)

### ハーフウェイク状態のブランディング

ハーフウェイク状態では、次のことができます。

- 背景ブランド イメージを追加します (画面および Touch 10)。
- 右下隅にロゴを追加します (画面および Touch 10)
- スクリーン中央のメッセージをカスタマイズまたは削除します (画面のみ。Touch 10 は不可)。これは、デバイスの使用開始方法をユーザに示すメッセージです。

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



### 背景ブランド イメージ

- デバイスが復帰するときに、画像がフルカラーで表示され、数秒後に自動的に淡色表示になります (透明な黒色のオーバーレイ)
- イメージの形式: PNG または JPEG
- 推奨サイズ: 1920 × 1080 ピクセル

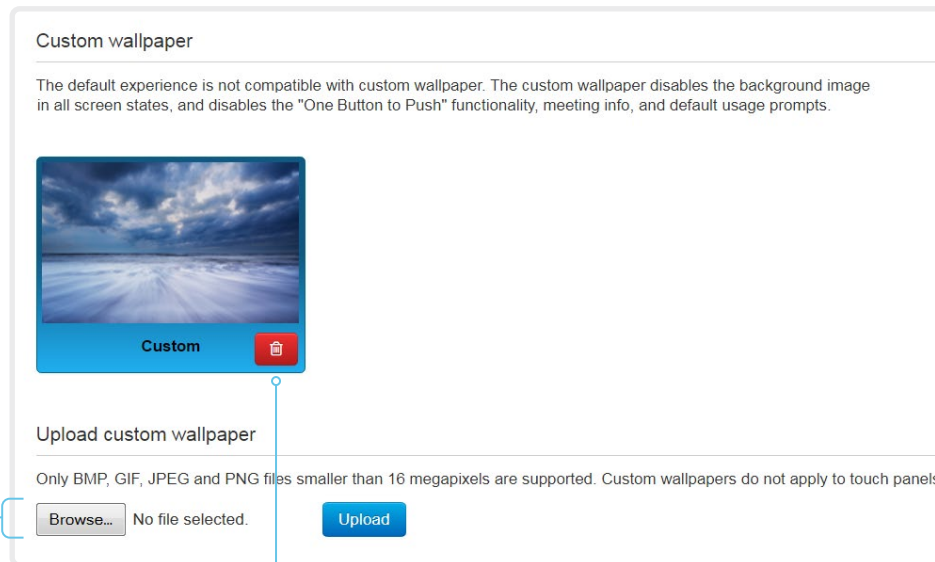
### ロゴ

推奨事項:

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

## カスタム壁紙の追加

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



### カスタムの壁紙のアップロード

古いカスタム壁紙があれば上書きします。

1. [\[参照 \(Browse\)\]](#) ボタンを押して、カスタム壁紙のイメージ ファイルを見つけます。
2. [\[アップロード \(Upload\)\]](#) をクリックして、ファイルをデバイスに保存します。

サポートされるファイル形式: BMP, GIF, JPEG, PNG

最大ファイル サイズ: 16 メガピクセル

カスタム壁紙をアップロードすると、自動的にアクティブになります。

### カスタムの壁紙の削除

[\[削除 \(Delete\)\]](#) をクリックすると、カスタム壁紙がデバイスから完全に削除されます。

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

### カスタム壁紙について

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

デバイスには一度に 1 枚のカスタム壁紙しか保存できません。以前のカスタム壁紙は新しいカスタム壁紙で上書きされます。

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

ブランド機能とカスタム壁紙は、同時に使用できません。

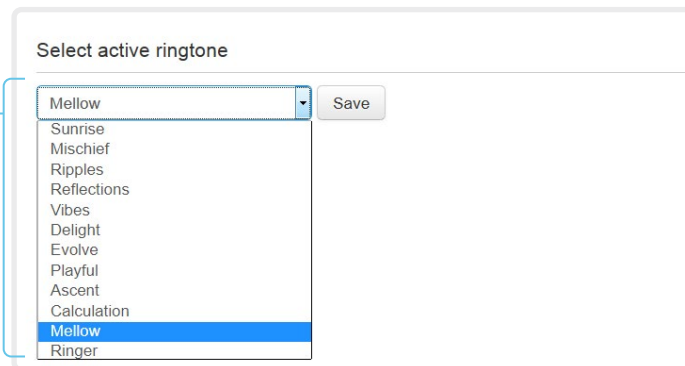
デバイスでブランディング要素がセットアップされている場合は、カスタム壁紙を追加する前に [\[ブランディングなしで続行 \(Continue without branding\)\]](#) をクリックする必要があります。

## 着信音の選択と着信音量の設定

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

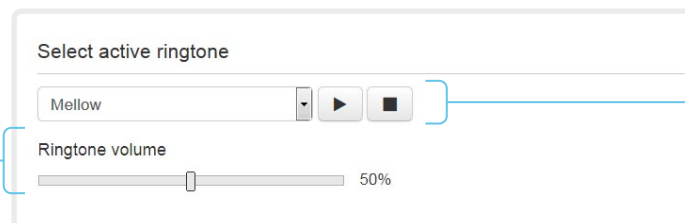
### 呼び出し音の変更

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



### 呼び出し音の音量の設定

呼び出し音の音量を調節するにはスライド バーを使用します。



### 呼び出し音の再生

呼び出し音を再生するには、再生ボタン (▶) をクリックします。

再生を終了するには、停止ボタン (■) を使用します。

### 着信音について

デバイスには着信音一式がインストールされています。着信音を選択して音量を設定するには、Web インターフェイスを使用します。

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

## お気に入りリストの管理

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

### ファイルから連絡先をインポート/エクスポート

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

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

### 連絡先を追加または編集する

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

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

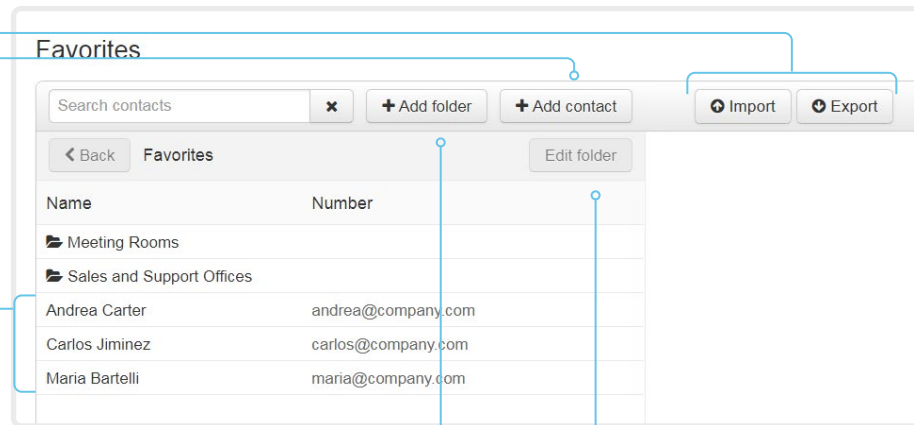
連絡先をサブフォルダに保存するために、フォルダ ドロップダウン リストでフォルダを選択します。

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

3. [\[保存 \(Save\)\]](#) をクリックしてローカル連絡先を保存します。

### コンタクトの削除

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



### サブフォルダを追加または編集する

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

### サブフォルダを削除する

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

## デバイスのユーザ インターフェイスによるお気に入りの管理

### お気に入りリストへの連絡先の追加

1. ホーム画面の [\[発信 \(Call\)\]](#) を選択します。
2. 追加する連絡先を選択します。
3. [\[お気に入りへの追加 \(Add to favorites\)\]](#) を選択します。

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

### お気に入りリストからの連絡先の削除

1. ホーム画面の [\[発信 \(Call\)\]](#) を選択します。
2. [\[お気に入り \(Favorites\)\]](#) タブを選択します。
3. 削除する連絡先を選択します。
4. [\[お気に入りの削除 \(Remove favorite\)\]](#) を選択します。

## アクセシビリティ機能のセットアップ

### 着信時のスクリーンの点滅

聴覚に障がいのあるユーザが着信に気づきやすくするために、着信時にスクリーンが赤色と灰色で点滅するように設定できます。

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

## CUCM からの製品固有の設定のプロビジョニング (1/2 ページ)

この章では、Cisco UCM リリース 12.5(1)SU1 で導入された手法を使用して、設定やパラメータをデバイス（エンドポイント）にプロビジョニングする方法について説明します。

Cisco UCM リリース 12.5(1)SU1 より前のリリースでは、UCM からデバイスにプッシュできるのは製品固有の設定の一部だけに限定されていました。それ以外のすべての設定については、管理者が Cisco TMS またはデバイスの Web インターフェイスを使用する必要がありました。

CUCM リリース 12.5(1)SU1 以降では、CUCM からプロビジョニングできる設定またはパラメータが増えました。設定のリストは、デバイス上でユーザに表示される内容（パブリック xConfiguration）と一致しますが、ネットワーク、プロビジョニング、SIP、および H.323 の設定は例外です。

CUCM の詳細については、▶ 『Cisco Unified Communications Manager リリース 12.5(1)SU1機能設定ガイド』の「ビデオエンドポイント管理」の章を参照してください。

### 設定制御モード

管理者は、導入のニーズに基づいて、CUCM 管理インターフェイスでさまざまな設定制御モードを構成できます。設定を CUCM とデバイスのどちらから制御するか、または両方を使用して制御するかを決定できます。

次のように、さまざまな設定制御モードがあります。

- **Unified CM とエンドポイント (Unified CM and Endpoint) (デフォルト)** : CUCM とデバイスを、デバイス データをプロビジョニングするためのマルチマスター ソースとして動作させる場合は、このモードを使用します。CUCM はデバイスから自動的に xConfiguration データを読み取ります。デバイスでローカルに行われた更新は、即座に CUCM サーバに同期されます。
- **Unified CM** : CUCM が、デバイス データをプロビジョニングするための集中管理型マスター ソースとして動作します。CUCM は、デバイスでローカルに行われた変更をすべて無視します。このような変更は、次回 CUCM が新しい設定をデバイスに適用するときを上書きされます。
- **エンドポイント (Endpoint)** : エンドポイントが設定データのマスター ソースとして動作します。このモードでは、エンドポイントは CUCM からの設定データを無視します。ローカルに行われた変更は同期されません。

このモードは通常、インテグレータがデバイスをインストールし、デバイスからローカルに設定を制御する場合に使用されます。

### オンデマンドによるデバイスからの設定の読み込み

管理者は、CUCM で [\[デバイスからxConfigを読み込む \(Pull xConfig from Device\)\]](#) オプションを使用して、デバイスから設定の変更内容をいつでもオンデマンドで読み込むことができます。

このオプションは、デバイスが登録されている場合にのみ有効になります。

### サポートされる CE ソフトウェアのバージョン

CE9.8 以降をサポートするすべてのデバイスで、CUCM のこの新しいプロビジョニング レイアウトを使用できます。

デバイスのソフトウェア バージョンが CE9.8 より前の場合は、CUCM のユーザ インターフェイスですべてのパラメータを表示できませんが、設定できるのは "#" でマークされているサブセットのみです。"#" は各パラメータ値の右側に表示されます。

パラメータの完全なセットは、デバイスを CE9.8 以降にアップグレードした場合にのみ機能します。



## CUCM からの製品固有の設定のプロビジョニング (2/2 ページ)

### CUCM からのプロビジョニングのセットアップ

1. CUCM にサインインし、[デバイス (Device)] > [電話 (Phone)] に移動して、目的のデバイスを見つけます。
2. [製品固有の設定 (Product Specific Configuration Layout)] セクションを見つけます (図を参照)。
3. [その他 (Miscellaneous)] カテゴリをクリックし、[設定制御モード (Configuration Control Mode)] 設定を見つけます。  
使用するモードを、[Unified CM]、[エンドポイント (Endpoint)]、または [Unified CM とエンドポイント (Unified CM and Endpoint)] から選択します (前のページの説明を参照)。
4. デバイスから現在の設定を読み込む場合は、[デバイスから xConfig を読み込む (Pull xConfig. from Device)] ボタンをクリックします。
5. カテゴリを選択し、変更する設定の値を指定します。
6. 最後に、以前のバージョンの CUCM での手順と同様に、[保存 (Save)] と [設定の適用 (Apply Config)] をクリックします。

### オンデマンドによるデバイスからの設定の読み込み

このボタンをクリックすると、デバイスからすべての構成がオンデマンドで読み込まれます。

### ハッシュ (#) の付いた設定

Cisco UCM リリース 12.5(1)SU1 以前でも使用できていた設定です。

### 設定またはパラメータ

選択中のカテゴリに属している設定です。

### カテゴリ

デバイス設定はカテゴリ別にグループ化されています。これらは、デバイスの Web インターフェイスで表示されるカテゴリと同じです。API コマンド パスにも対応しています。

ただし、[その他 (Miscellaneous)] は例外です。このカテゴリには、CUCM でのみ設定可能な設定が表示されます。これらはデバイスのローカル設定に対応していません。




## 第 3 章

# 周辺機器

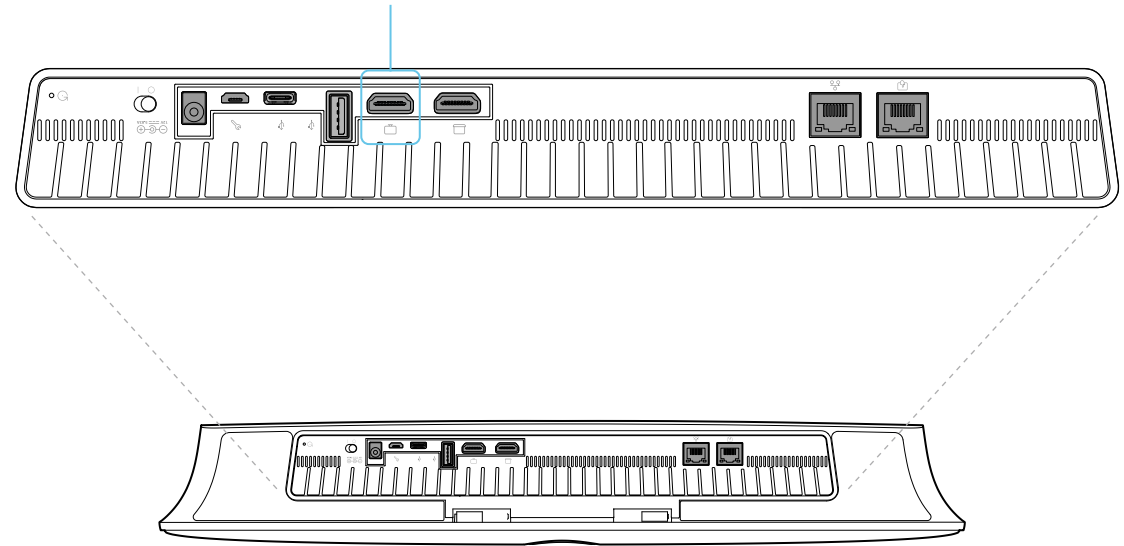
## モニタへの接続

デバイスには HDMI ビデオ出力が 1 つあります。

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

 モニタおよび他の周辺機器の接続時や切断時には、必ず電源を切ってください。

モニタ用の HDMI 出力 (出力コネクタ 1)



## 入力ソースの接続 (1/2 ページ)

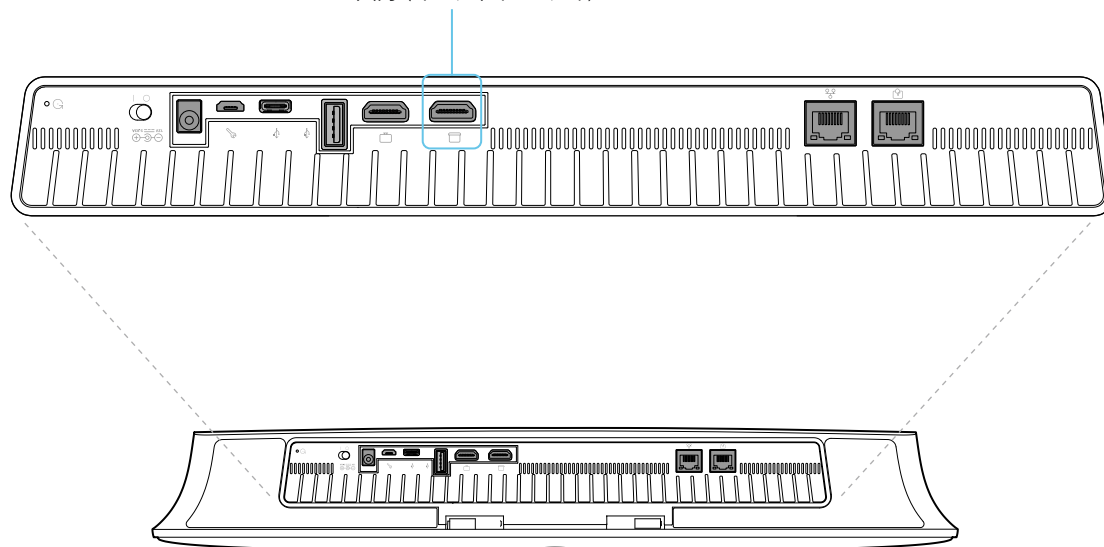
ウェブ インターフェイスにサインインして、[\[セットアップ \(Setup\)\] > \[設定 \(Configuration\)\]](#) に移動すると、以下に示す設定が見つかります。

### コンピュータまたはその他のコンテンツ ソースの接続

入力ソースを 1 つ接続できます。たとえば、1 台のコンピュータをデバイスの HDMI 入力 (入力コネクタ 2) に接続して、コンテンツをローカルで共有したり、会議の参加者と共有したりできます。

HDMI 入力は、30 fps で最大 3840 × 2160 の解像度をサポートしません。高解像度とフレーム レートをサポートするハイスピード HDMI 1.4b ケーブルが必要です。

入力コネクタ 2  
コンピュータまたはその他のコンテンツソース用の  
HDMI 入力 (オーディオとビデオ)



## 入力ソースの接続 (2/2 ページ)

### 入力ソースのタイプと名前の設定

入力ソースのタイプと名前を設定することをお勧めします。

- ・ `[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [入力ソースタイプ (InputSourceType)]`
- ・ `[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [名前 (Name)]`

これらの設定によって、ユーザ インターフェイスに表示される名前とアイコンが決まります。分かりやすい名前とアイコンを設定すると、ソースを簡単に選択できるようになります。

入力コネクタ 1 は内蔵カメラであることに注意してください。

### ビデオとコンテンツの品質について

モーションまたは鮮明度に関する品質を最適化するには、`[ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [品質 (Quality)]` 設定を使用します。

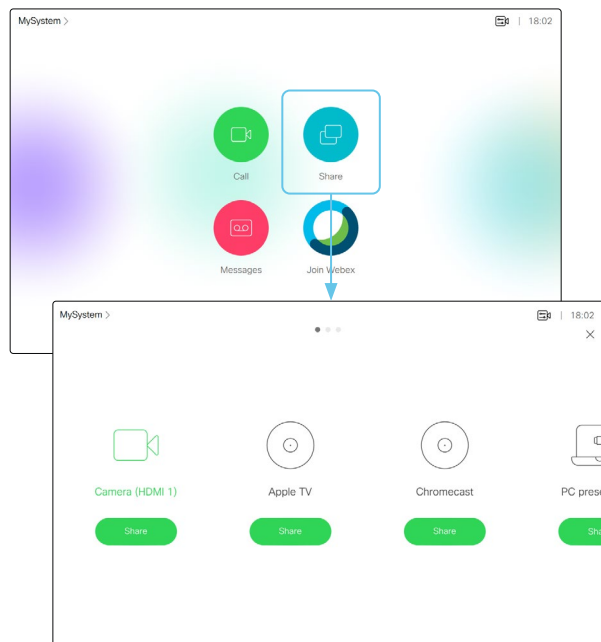
通常、画像の動きが激しい場合は、`[モーション (Motion)]` を選択する必要があります。高品質で詳細な画像とグラフィックが必要なときは、`[シャープネス (Sharpness)]` を選択します。

コネクタ 2 のデフォルト値は シャープネスです。

## 入力ソース数の拡大

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

ソースは、ビデオ会議デバイスに直接接続されている他のビデオと同じように表示されて動作します。



複数の外部入力ソースがあるユーザ インターフェイス (例)

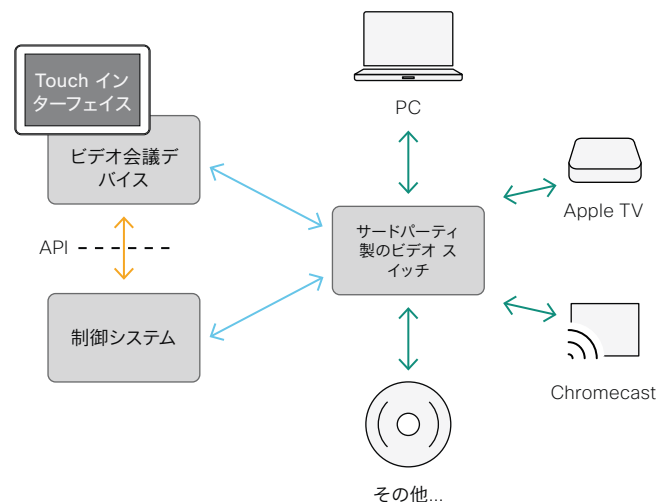
ユーザ インターフェイスを拡張する方法と、それをデバイスの API を使用してセットアップする方法の詳細については、カスタマイズ ガイドをご覧ください。次のリンクにアクセスします。

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

## アーキテクチャ

Touch インターフェイスを搭載したシスコのビデオ会議デバイス、サードパーティ製の制御システム (Crestron または AMX など)、およびサードパーティ製ビデオ スイッチが必要です。ビデオ スイッチを制御するのは、ビデオ会議デバイスではなく、制御システムです。

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



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

## ディスプレイについて

### リアルタイム通信の要件

シスコでは、ビデオ会議デバイスのカメラから画面への遅延を最小限にし、また音声コンポーネントとビデオコンポーネントの間の全体的な遅延を検出してそれを補うために、さまざまな取り組みを行ってきました。

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

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

次のディスプレイの設定によって、この遅延が低下する可能性があります。

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

### Consumer Electronics Control (CEC)

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

コールを開始すると、ビデオ会議デバイスは、アクティブなビデオ入力 が別の入力に切り替えられたかどうかを検出します。そのうえで、ビデオ会議デバイスがアクティブなビデオ入力ソースになるように、ビデオ会議デバイスが入力を切り替えます。

ビデオ会議デバイスがアクティブな入力ソースにならずにスタンバイ状態になった場合、ディスプレイはスタンバイ状態に移行しません。

### Cisco が推奨するディスプレイ

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

#### モデル

49" UHD (49UH5C)

55" UHD (55UH5C)

65" UHD (65UH5C)

75" UHD (75UH5C)

86" UHD (86UH5C)

98" UHD (98UH5C)

#### LG グローバル Web サイト リンク

<http://www.lg.com/global/business/information-display/digital-signage/lg-49UH5C>

<http://www.lg.com/global/business/information-display/digital-signage/lg-55UH5C>

<http://www.lg.com/global/business/information-display/digital-signage/lg-65UH5C>

<http://www.lg.com/global/business/information-display/digital-signage/lg-75UH5C>

<http://www.lg.com/global/business/information-display/digital-signage/lg-86UH5C>

<http://www.lg.com/global/business/information-display/digital-signage/lg-98LS95D>

#### モデル

QMN シリーズ (43"49"、55"、65"、75")

QMH シリーズ (49"55"、65")

QBN シリーズ (43"49"、55"、65"、75")

QBH シリーズ (65"、75")

#### LG グローバル Web サイト リンク

<https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N>

<https://displaysolutions.samsung.com/digital-signage/detail/1144/QM49H>

<https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N>

<https://displaysolutions.samsung.com/digital-signage/detail/1205/QB65H>

## 4K 解像度について

### ディスプレイの接続

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

後で設定の調整が必要になった場合は、Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) > [\[ビデオ \(Video\)\]](#) > [\[出力 \(Output\)\]](#) > [\[コネクタ n \(Connector n\)\]](#) > [\[解像度 \(Resolution\)\]](#) に移動して、画面の解像度を調整します。ディスプレイのサポート内容に応じて解像度を設定してください。

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

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

### コンピュータの接続

コンピュータの接続時にエラーが発生すると、スクリーンと Touch 10 コントローラにメッセージが表示されます。

ビデオ入力コネクタのデフォルトの推奨解像度は 1080p60 (1920\_1080\_60) です。コンピュータで 4K 解像度を使用する場合は、Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) > [\[ビデオ \(Video\)\]](#) > [\[入力 \(Input\)\]](#) > [\[コネクタ n \(Connector n\)\]](#) > [\[推奨解像度 \(Preferred Resolution\)\]](#) に移動して、値を調整します。

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

### チェックリスト

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

ビデオ会議デバイスの入力/出力コネクタが正しく設定されていることを確認してください。

デバイス (TV/ディスプレイ、コンピュータ) が 4K をサポートしており、正しく設定されていることを確認してください。


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

4K の使用では高品質ケーブルの必要性が増します。

- ・ 4kp30 は 1080p60 の約 2 倍のデータレートを 사용합니다。
- ・ 4kp60 は 1080p60 の約 4 倍のデータレートを 사용합니다。

## HDMI ケーブルについて

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

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

### カメラおよびディスプレイ用の HDMI ケーブル

1920X1200@60fps を超える解像度フォーマットには、必ずハイスピード対応の HDMI ケーブルを使用してください。動作が保証されている範囲については、3840×2160 (60fps) でシスコが事前に選定した HDMI ケーブルを使用するか、またはプレミアム HDMI ケーブル認証プログラムに合格したケーブルを使用します。

### プレゼンテーション ソース用の HDMI ケーブル

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

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

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

HDMI ケーブルの詳細については、▶ <http://www.hdmi.org>を参照してください

\* シスコの 4K マルチヘッドケーブル (CAB-HDMI-MUL4K-9M および CAB-HDMI-MUL4K-2M) は、Board および Room シリーズのデバイスと互換性があります。これらのケーブルには、HDMI タイプ A - USB-C、Mini ディスプレイポート、および HDMI タイプ A のコネクタが搭載されています。

1080p マルチヘッドケーブル (CAB-HDMI-MULT-9M) は、SX および MX シリーズのデバイスと互換性があります。1080p のコンテンツに限定するデバイスには、このケーブルを推奨します。このケーブルには、HDMI タイプ A - ディスプレイポート、Mini ディスプレイポート、および HDMI タイプ A のコネクタが搭載されています。



## Best Overview 機能のセットアップ

Web インターフェイスにサインインして、[\[設定 \(Configuration\)\]](#) > [\[システム設定 \(System Configuration\)\]](#) に移動すると、ここに示す設定が見つかります。

最適な概要機能は自動カメラ フレーミングを使用し、室内の人数に基づいて最適な表示を選択します。

カメラは、デジタル顔検出機能を使用して、室内の個人またはグループを最適に自動表示します。この機能は、室内での参加者の移動や新たな参加者の入室に合わせて、画面にすべてのユーザが含まれるように自動的に調整します。

### 最適な概要の設定

スピーカー トラッキングを設定するには、[\[カメラ \(Camera\)\]](#) > [\[スピーカー トラック \(SpeakerTrack\)\]](#) の設定を使用します。

[\[カメラ \(Camera\)\]](#) > [\[スピーカー トラック \(SpeakerTrack\)\]](#) > [\[モード \(Mode\)\]](#)

**自動:** 通常、[Best overview] が有効になっています。デバイスが室内の人々を検出して自動的に最適なカメラフレーミングを選択します。ユーザは、ユーザインターフェイスのカメラ制御パネルから、Best Overview のオンとオフをすぐに切り替えることができます。

**オフ (Off) :** Best Overview はオフになります。ユーザインターフェイスからオンに切り替えることはできません。

## Touch 10 コントローラの接続 (1/4 ページ)

Touch 10 は、このページの説明に従ってビデオ会議デバイスに直接接続するか、次のページの説明に従ってネットワーク (LAN) 経由でデバイスとペアリングする必要があります。後者はリモート ペアリングと呼ばれます。

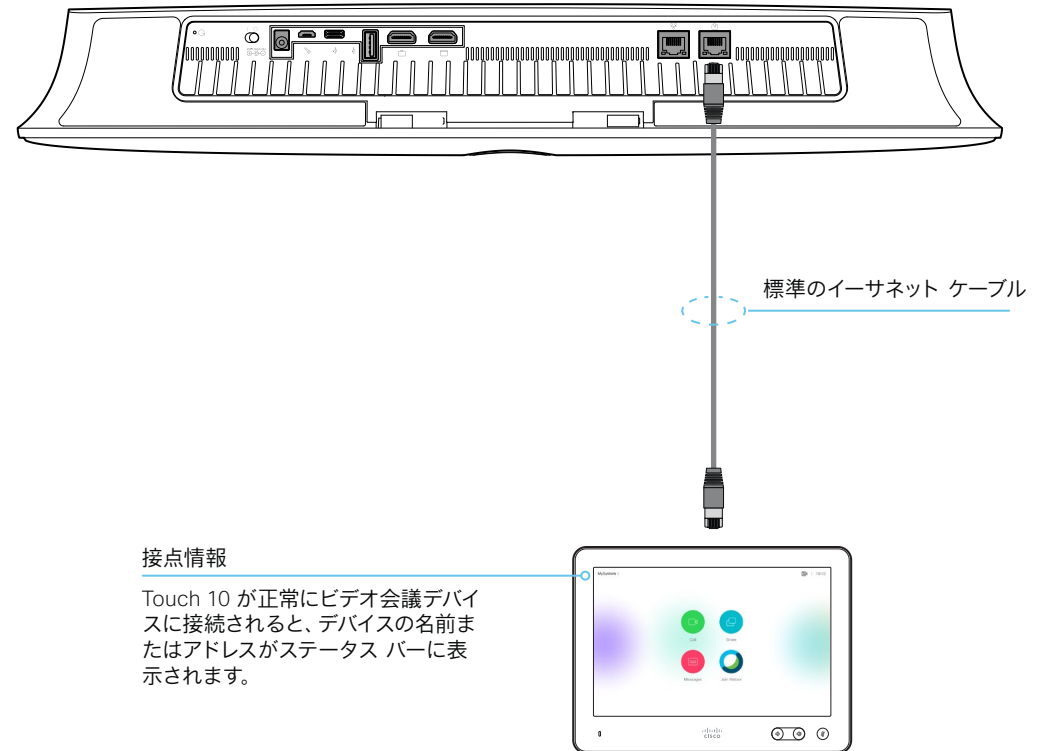
### ビデオ会議デバイスへの Touch 10 の直接接続

図のように、Touch 10 をビデオ会議デバイスの Touch 専用 (RJ-45) ポートに接続します。

### Touch 10 の設定

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

Touch 10 のソフトウェアのアップグレードが必要な場合は、セットアップ手順の一部で新しいソフトウェアがビデオ会議デバイスからダウンロードされ、自動的にユニットにインストールされます。アップグレード後にタッチ 10 が再起動します。



イーサネット コネクタは、Touch 10 の裏側にあります。

## Touch 10 コントローラの接続 (2/4 ページ)

### ネットワーク (LAN) を経由したビデオ会議デバイスへの Touch 10 の接続

図のように、Touch 10 とビデオ会議デバイスを壁面のネットワーク ソケットまたはネットワーク スイッチに接続します。

#### Touch 10 の設定

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

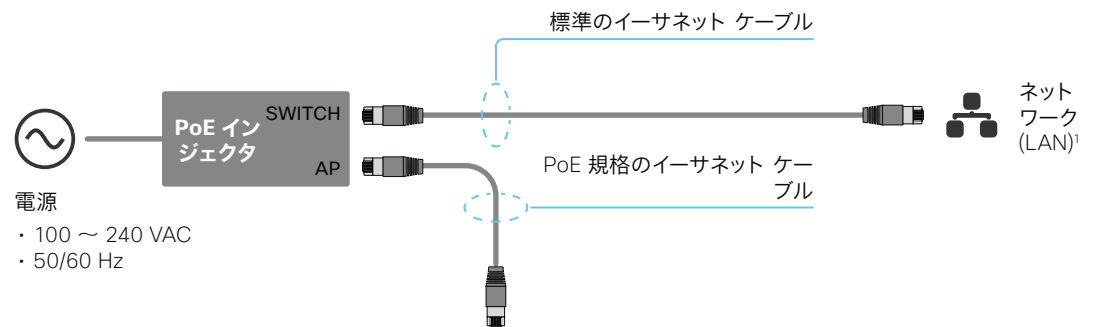
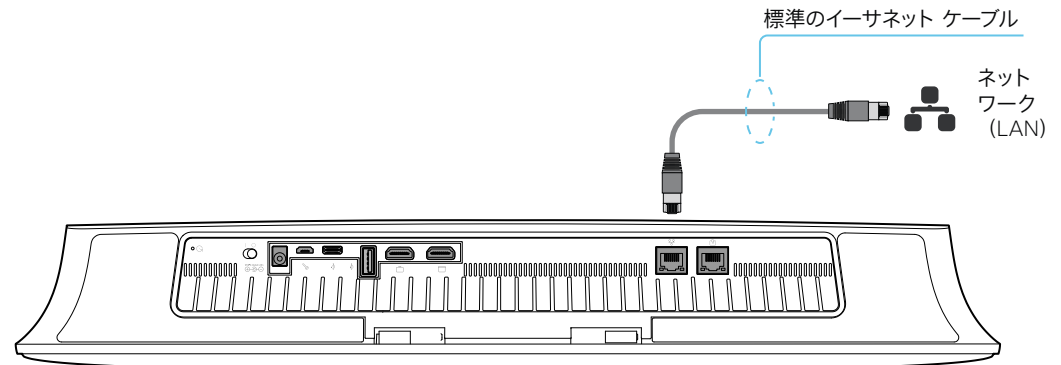
[[ルーム システムの選択 \(Select a room system\)](#)] 画面が表示されたら、以下の点に注意してください。

- ペアリングできることを信号で伝えているデバイスのリストが、画面に表示されます。ペアリングするデバイスの名前をタップします。  
デバイスがリストに表示されるためには、次の条件を満たす必要があることに注意してください。
  - デバイスと Touch 10 が同じサブネット上にある必要があります。
  - デバイスが直近 10 分以内に再起動されている必要があります。デバイスがリストに表示されていない場合は、再起動をお試しください。
- 使用可能なデバイスのリストにデバイスが表示されない場合は、入力フィールドに IP アドレスまたはホスト名を入力します。[\[接続 \(Connect\)\]](#) をタップします。
- ペアリング プロセスを開始するには、ユーザ名とパスワードを使用してログインする必要があります。[\[ログイン \(Login\)\]](#) をタップします。

user ロールを持つユーザであれば十分対応できます。このタスクを実行するために admin ロールは必要ありません。

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

Touch 10 のソフトウェアのアップグレードが必要な場合は、セットアップ手順の一部で新しいソフトウェアがデバイスからダウンロードされ、自動的にユニットにインストールされます。アップグレード後に Touch 10 が再起動します。



#### 接点情報

Touch 10 が正常にビデオ会議デバイスにペアリングされると、デバイスの名前またはアドレスがステータス バーに表示されます。



イーサネット コネクタは、Touch 10 の裏側にあります。

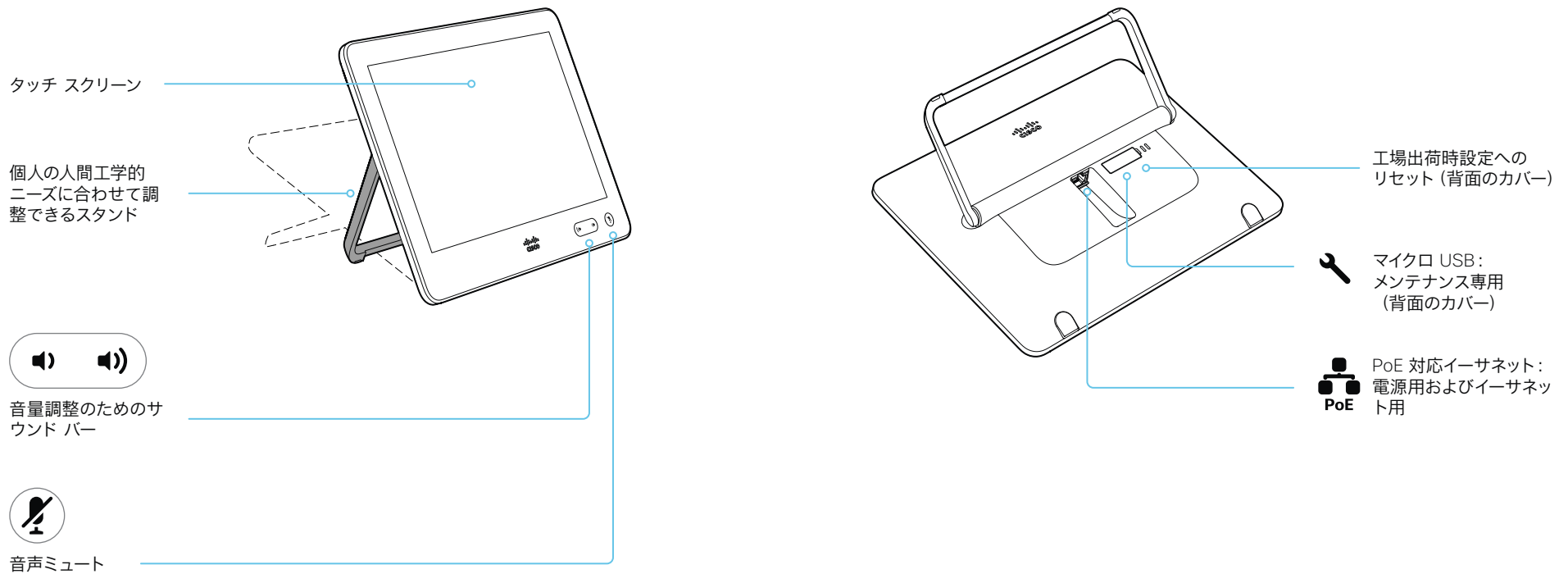
<sup>1</sup> ネットワーク インフラストラクチャが Power over Ethernet (PoE) を提供する場合、PoE インジェクタは必要ありません。タッチ 10 は PoE 規格のイーサネット ケーブルで直接壁面のソケット (イーサネット スイッチ) に接続する必要があります。

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

## Touch 10 コントローラの接続 (3/4 ページ)

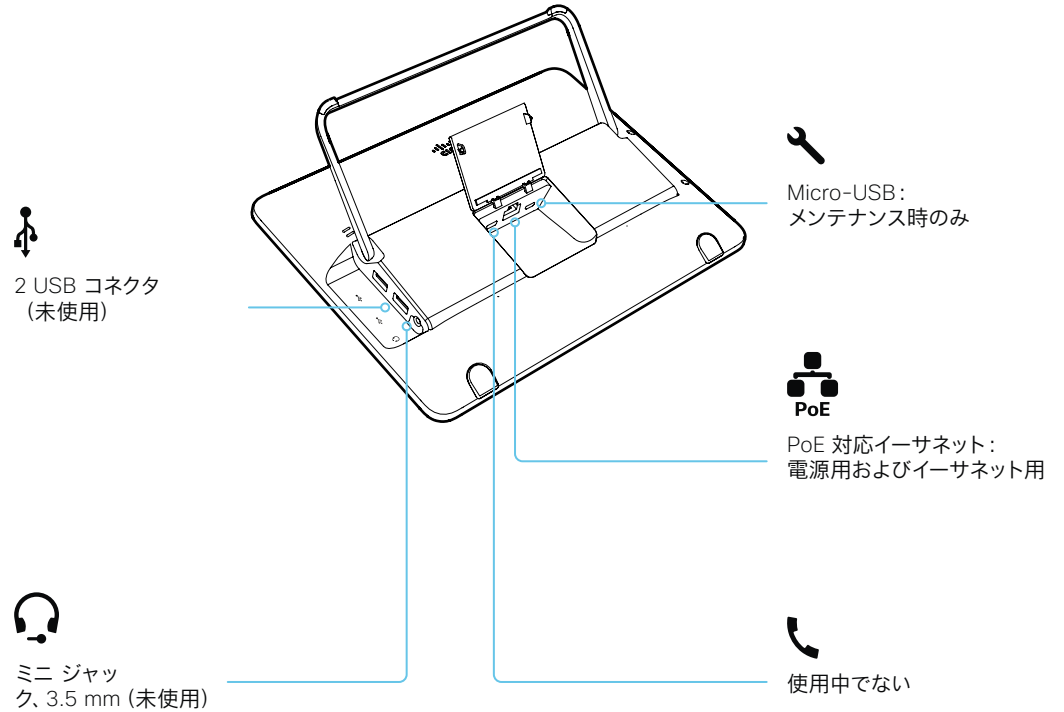
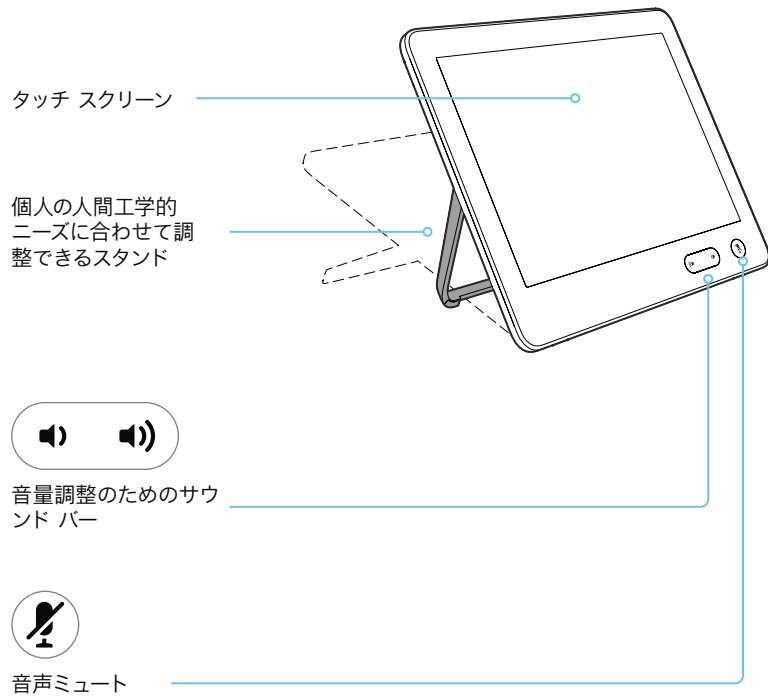
### Cisco Touch 10 の物理インターフェイス

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



## Touch 10 コントローラの接続 (4/4 ページ)

Cisco TelePresence Touch 10 の物理インターフェイス  
新しいバージョンの Touch 10 コントローラについては、前のページを参照してください。



## ISDN リンクの接続

ISDN リンクを設定すると、ビデオ会議デバイスの接続に ISDN 回線を使用することができ、PSTN (公衆電話交換網) 経由でのビデオ コールと電話が可能になります。

ISDN リンクは、ISDN BRI、ISDN PRI、および V.35 をサポートしています。ISDN は、SIP または H.323 コール用の通常の IP 接続に加えて使用できます。また、IP インフラストラクチャなしでも使用できます。

ISDN リンクは、ビデオ会議デバイスの Web インターフェイスから管理します。Web インターフェイスにサインインし、[[セットアップ \(Setup\)](#)] > [[周辺機器 \(Peripherals\)](#)] に移動します。

### 要件および制約事項:

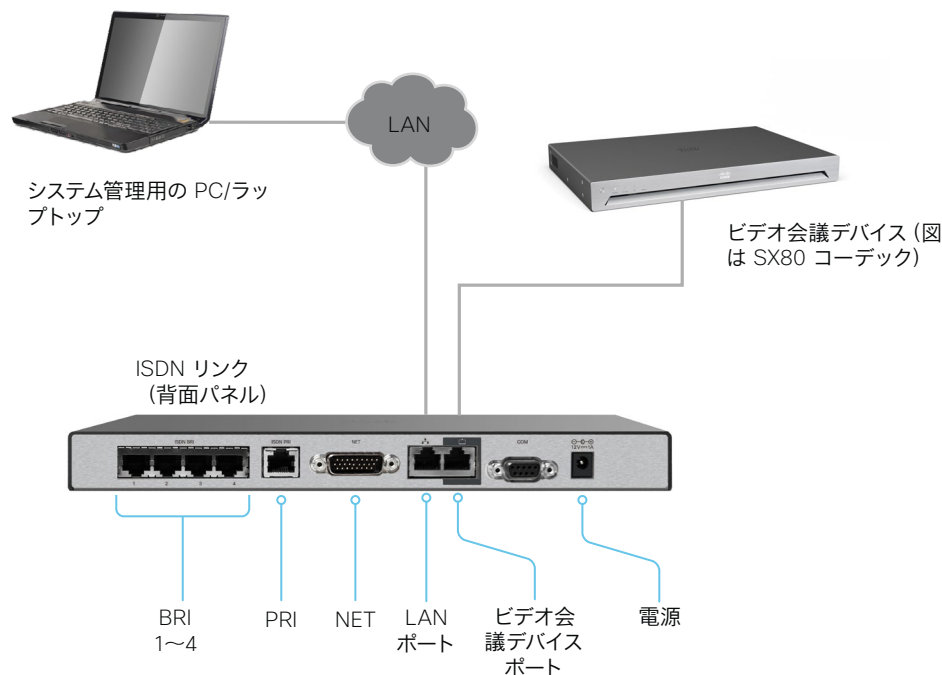
- ISDN リンクは、IL1.1.7 以降のソフトウェアを実行している必要があります。
- ISDN リンクと通信するために、ビデオ会議デバイスの Web インターフェイスまたは API で IPv6 を有効にする必要があります。
- 確実にインストールするために、ISDN リンクのインストール ガイドでネットワーク トポロジを確認してください。
- ビデオ会議デバイスと ISDN リンクが同じサブネット上にある必要があります。エンドポイントまたは ISDN リンクに新しい IP アドレスが割り当てられている場合は、それらが同じサブネットに保持されている間だけペアリングが維持されます。
- Cisco Webex クラウド サービスに登録されているビデオ会議デバイスでは、ISDN リンクを使用できません。

### セットアップと構成

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

### LAN およびビデオ会議デバイスと ISDN リンクの直接接続を使用したセットアップ

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



## 第 4 章

# メンテナンス

## 新しいソフトウェアのインストール (1/2 ページ)

### CE9.13 以降へのアップグレードまたは CE9.13 以降からのダウングレード

アップグレードやダウングレードでは、特定の状況によって設定が失われる可能性があることに注意してください。

CE9.13 以降へのアップグレードまたは CE9.13 以降からのダウングレードを行うと、インストールするバージョンに存在しない設定はすべて削除されます。後で以前のソフトウェアバージョンに戻そうとしても、削除された設定にはデフォルト値が割り当てられます。

### ソフトウェアイメージのファイル形式

#### PKG ファイルと COP ファイルについて

**Boards, Desk Pro, および Room シリーズ:** ビデオデバイスと周辺機器のソフトウェアイメージは別々の PKG ファイルになっています。

そのため、これらのデバイスをアップグレードする場合は COP ファイルを使用する必要があります。COP ファイルには、ビデオデバイスおよび周辺機器に必要な PKG ファイルと、COP ファイルの内容を示す *loads* ファイルが含まれています。

**SX, MX, および DX シリーズ:** ビデオデバイスの PKG ファイルには、デバイス自体のソフトウェアイメージと、関連する周辺機器のソフトウェアイメージの両方が含まれています。

#### CUCM からのアップグレード

デバイスのアップグレードには COP ファイルを使用します。

**Board, Desk Pro, および Room シリーズ:** これらのデバイスをアップグレードする場合は、*loads* ファイルを使用してソフトウェアを指定する必要があります。ビデオデバイスの PKG ファイルでは周辺機器がアップグレードされないため、ビデオデバイスの PKG ファイルだけを使用することはできません。

**SX, MX, および DX シリーズ:** これらのデバイスをアップグレードする場合は、PKG ファイルを使用してソフトウェアを指定できます。これらの PKG ファイルには周辺機器のソフトウェアも含まれています。

#### TMS またはデバイスの Web インターフェイスからのアップグレード:

**Board, Desk Pro, および Room シリーズ:** これらのデバイスをアップグレードする場合は、COP ファイルを使用します。ビデオデバイスの PKG ファイルには周辺機器のソフトウェアイメージが含まれていないため、ビデオデバイスの PKG ファイルだけを使用することはできません。

**SX, MX, および DX シリーズ:** これらのデバイスをアップグレードする場合は、PKG ファイルを使用できます。これらの PKG ファイルには周辺機器のソフトウェアも含まれています。



## 新しいソフトウェアのインストール (2/2 ページ)

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

### 新しいソフトウェアをダウンロードする

各ソフトウェア バージョンに固有のファイル名があります。シスコのソフトウェア ダウンロード Web ページを開き、お使いの製品のページにアクセスします。▶ <https://software.cisco.com/download/home> [英語]

ファイル名フォーマットは:

"cmterm-s53200ce9\_13\_x-yyy.k3.cop.sgn"

"x" はドット内のリリース番号、"yyy" は、ソフトウェアの一意の識別子を表します。

### 新しいソフトウェアのインストール

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

1. [参照... (Browse...)] をクリックして、新しいソフトウェアを含む .cop.sgn ファイルを探します。  
ソフトウェアのバージョンが検出され、表示されます。
2. [ソフトウェアのインストール (Install Software)] をクリックして、インストール プロセスを開始します。

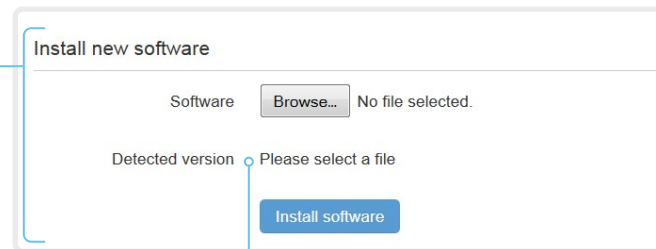
通常、インストールは 15 分以内に完了します。ウェブ ページから進捗状況を確認できます。インストール後、デバイスは自動的に再起動します。

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

### ソフトウェア リリース ノート

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

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



### 新しいソフトウェア バージョンの確認

ファイルを選択すると、ここにソフトウェアのバージョンが表示されます。

## オプションキーの追加

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

すべてのオプション キーのリストと、デバイス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。

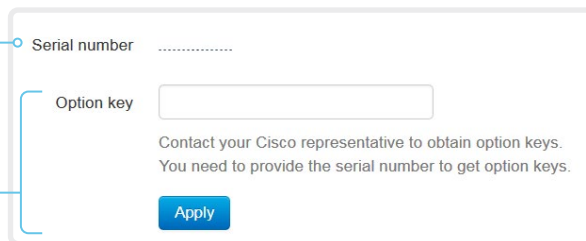
### デバイスのシリアル番号

オプション キーの注文時にはデバイス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. [\[適用 \(Apply\)\]](#) をクリックしてオプション キーを追加します。

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



Serial number .....

Option key

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

Apply

### オプション キーについて

デバイスには、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も、インストールされていない場合もあります。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デバイスに存在している必要があります。

オプション キーは各デバイスに固有のもので、

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。

## デバイスのステータス

### デバイス情報の概要

[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、デバイス名のほか、ハードウェア、ソフトウェア、インストール済みオプション、ネットワーク アドレスに関する基本情報が表示されます。ビデオ ネットワーク (SIP および H.323) の登録ステータスのほか、デバイスにコールする際に使用する番号および URI も含まれます。

### デバイス ステータスの詳細

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

#### ステータス エントリを検索する

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

Status	
Audio	
Ultrasound Volume	70
Volume	48

#### カテゴリを選択して適切なステータスに移動する

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

Status	
Conference	
ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private

\* 図に示しているステータスは一例です。お使いのデバイスのステータスとは異なる場合があります。

## 診断の実行

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

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

エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

### 診断の実行

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

### スタンバイ モードを離れる

スタンバイ モードのデバイスを復帰させるには、[\[システムの復帰 \(Wake up the system\)\]](#) をクリックします。

**Diagnostics** Wake up the system Re-run diagnostics

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

- CRITICAL: Passphrases**  
There is one or more users without a passphrase set. Please [set a passphrase for all users](#).
- WARNING: System Name**  
The system has not been configured with a name. Please [configure a system name](#). Note that changing the name of the system requires a reboot.
- OK: System Temperature**  
The system is running at an acceptable temperature.
- OK: Standby Control**  
The system goes into standby automatically after 10 minutes. Standby can be configured through the [system configuration](#).

\* 図に示しているメッセージは一例ですお使いのデバイスでは表示される情報が異なる場合があります。

## ログファイルのダウンロード

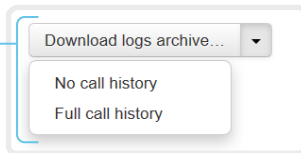
Web インターフェイスにサインインして、[\[メンテナンス \(Maintenance\)\]](#) > [\[システム ログ \(System Logs\)\]](#) を選択します。

### すべてのログ ファイルをダウンロードする

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

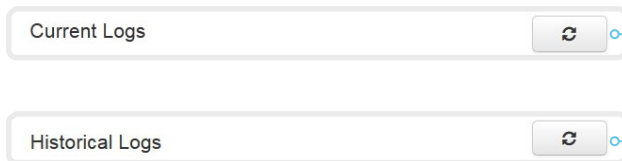
匿名化された通話履歴はログファイルにデフォルトで含まれています。

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



### 1 つのログファイルを開く/保存

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



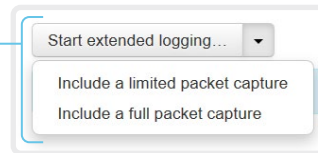
### 拡張ロギングの開始

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

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

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

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



### ログ ファイル リストの表示更新

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

## ログ ファイルについて

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

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

デバイスを再起動するたびに、現在のログファイルはタイムスタンプ付きの履歴ログファイルにすべてアーカイブされます。履歴ログファイルの最大数に到達すると、最も古いファイルは上書きされます。


### 拡張ロギング モード

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

拡張ロギングはデバイスのリソースをより多く使用するため、デバイスの動作が低下する場合があります。拡張ロギング モードは、トラブルシューティングのときにのみ使用してください。

## リモートサポートユーザの作成

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

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

### リモート サポート ユーザの作成

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

リモート サポート ユーザは 7 日間、または削除されるまで有効です。

The system does not have an active Remote Support User.

Create user

Delete user

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

#### Token

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

The system has an active Remote Support User.

Create user

Delete user

### リモート サポート ユーザの削除

[ユーザの削除 (Delete User)] をクリックします。

### リモート サポート ユーザについて

デバイス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 ユーザにはデバイスに対する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) のアシスタントが必要です。

## 設定とカスタム要素のバックアップ/復元

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

バックアップ ファイル (zip 形式) には、設定とともにカスタム要素を含めることができます。以下の要素のいずれをバンドルに含めるかを選択できます。

- ブランディング イメージ
- マクロ
- お気に入り
- サインイン バナー
- UI 拡張
- 構成/設定 (すべてまたは一部)

バックアップ ファイルは、デバイスの Web インターフェイスから手動で復元できます。または、Cisco UCM や TMS などを使用して複数のデバイスにプロビジョニングできるように、バックアップ バンドルを一般化することもできます (これ以降の章を参照)。

### バックアップ ファイルの作成

1. [\[バックアップの作成 \(Create backup\)\]](#) タブを開きます。
2. バックアップ ファイルに含める要素を選択します。  
現在デバイス上に存在しない要素はグレー表示されます。
3. バックアップ ファイルに含める設定 (ある場合) を選択します。次の点に注意してください。
  - デフォルトでは、すべての設定がバックアップ ファイルに含まれます。
  - ウェブ ページの一覧から手動で設定を削除することにより、1 つ以上の設定を手動で削除できます。
  - 特定のデバイスに固有の設定をすべて削除する場合は、[\[システム固有の設定の削除 \(Remove system-specific configurations\)\]](#) をクリックします。  
これは、他のデバイスでバックアップ バンドルを復元する予定がある場合に役立ちます。
4. [\[バックアップのダウンロード \(Download backup\)\]](#) をクリックして、コンピュータ上の zip ファイルに要素を保存します。

### バックアップ ファイルの復元

1. [\[バックアップの復元 \(Restore backup\)\]](#) タブを選択します。
2. [\[参照... \(Browse...\)\]](#) をクリックして、復元するバックアップ ファイルを見つけます。  
バックアップ ファイル内のすべての設定と要素が適用されます。
3. [\[ファイルのアップロード \(Upload File\)\]](#) をクリックして、バックアップを適用します。  
設定によっては、有効にするためにデバイスを再起動する必要があります。

### その他の情報

#### マクロの復元

マクロを含むバックアップ ファイルをデバイスで復元すると、次の処理が適用されます。

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

#### ブランド イメージの復元

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

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

#### バックアップ ファイル

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

## カスタム要素の CUCM プロビジョニング

バックアップ ファイルは、「[▶ 設定とカスタム要素のバックアップ/復元](#)」の章で説明されているとおり、複数のデバイスでカスタマイズ テンプレートとして使用できます。

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

- ・ CUCM TFTP ファイル サービス、または
- ・ デバイスが HTTP または HTTPS で接続可能なカスタム Web サーバ。

デバイスが CUCM (Cisco Unified Communications Manager) からカスタマイズ テンプレートの名前と格納場所に関する情報を取得するときは、デバイスがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

**i** カスタマイズ テンプレートとして使用するバックアップ ファイルに設定が含まれている場合でも、設定はデバイス上に復元されません。

カスタマイズ テンプレートの TFTP ファイル サーバへのアップロード

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

デバイスごとのカスタマイズ プロビジョニング情報の追加

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

これらのフィールドが存在しない場合は、CUCM に新しいデバイス パッケージをインストールする必要があります。

4. [\[保存 \(Save\)\]](#) および [\[設定の適用 \(Apply Config\)\]](#) をクリックして、設定をデバイスにプッシュします。

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

次に例を示します。

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

## SHA512 チェックサム

**ヒント:** Web インターフェイスを使用してデバイスにファイルを復元すると、そのファイルの SHA512 チェックサムを確認できます。

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

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

## CUCM のドキュメンテーション

▶ <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>



## カスタム要素の TMS プロビジョニング

バックアップ ファイルは、「[▶ 設定とカスタム要素のバックアップ/復元](#)」の章で説明されているとおり、複数のデバイスでカスタマイズテンプレートとして使用できます。

バックアップ ファイルは、デバイスが HTTP または HTTPS で接続可能なカスタム Web サーバ上にホストする必要があります。

デバイスが TMS (TelePresence Management Suite) からバックアップ ファイルの名前と位置に関する情報を取得するときは、デバイスがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

### 構成テンプレートの作成と適用

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

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

上記コマンドで、下記のように適用します。

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

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

*Origin*: プロビジョニング\*

3. 設定テンプレートのプッシュ先のデバイスを選択し、[\[システムに設定 \(Set on systems\)\]](#) をクリックします。

TMS 構成テンプレートおよびカスタムコマンドの作成方法の詳細については、[▶ 『Cisco TMS 管理者ガイド』](#) を参照してください。

### SHA512 チェックサム

**ヒント:** Web インターフェイスを使用してデバイスにファイルを復元すると、そのファイルの SHA512 チェックサムを確認できます。

1. Web インターフェイスにサインインして、[\[メンテナンス \(Maintenance\)\]](#) > [\[バックアップと復元 \(Backup and Restore\)\]](#) に移動します。
2. [\[バックアップの復元 \(Restore backup\)\]](#) タブを選択します。
3. [\[参照 \(Browse...\)\]](#) をクリックして、チェックサムを計算したいファイルを検索します。  
ページの下部に SHA512 チェックサムが表示されていることが確認できます。

\* このパラメータを Provisioning に設定しない場合は、バックアップ ファイルに含まれる設定もデバイスにプッシュされます。特定の 1 台のデバイスに固有の構成 (静的 IP アドレス、システム名、連絡先情報など) がバックアップ ファイルに含まれていると、接続できないデバイスができる可能性があります。

## 以前に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。

以前使用していたソフトウェア イメージに切り替える前に、デバイスのログ ファイル、構成、およびカスタム要素をバックアップすることを推奨します。

### ログ ファイル、構成、カスタム要素のバックアップ

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

### 以前に使用していたソフトウェアイメージへの復元

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

1. [\[ソフトウェア回復交換 \(Software Recovery Swap\)\]](#) タブを選択します。
2. [\[ソフトウェア: cex.y.z への切り替え... \(Switch to software: cex.y.z...\)\]](#) をクリックします。ここで x.y.z はソフトウェア バージョンを示します。
3. [\[はい \(Yes\)\]](#) をクリックして選択を確定します。または、操作をやめる場合は [\[キャンセル \(Cancel\)\]](#) をクリックします。

デバイスがリセットされるまでお待ちください。完了するとデバイスが自動的に再起動します。この手順は数分かかることがあります。


### 以前に使用されたソフトウェアイメージについて

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

ソフトウェアを最後にアップグレードしてからデバイスを初期設定にリセットしていない場合は、それまで使用していたソフトウェア イメージがデバイスに存在しています。ソフトウェアをダウンロードする必要はありません。

## ビデオ会議デバイスの初期設定へのリセット (1/3 ページ)

デバイスに重大な問題が発生した場合、最後の手段としてデフォルトの初期設定にリセットすることができます。

 初期設定にリセットすると元に戻すことはできません。

工場出荷時の状態にリセットする前に以前使用したソフトウェア イメージに戻すことを常に検討してください。多くの場合これでデバイスが回復します。ソフトウェアの切り替えについては、[▶ 「以前に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。

デバイスを初期設定にリセットする際は、Web インターフェイスまたはユーザ インターフェイスを使用することを推奨します。上記インターフェイスが利用できない場合は、ピンホールリセットを利用します。

工場出荷時設定リセットにより、次のような影響が発生します。

- 通話履歴が削除されます。
- パスフレーズがデフォルト設定にリセットされます。
- すべてのデバイス パラメータがデフォルト値にリセットされます。
- デバイ스에 アップロード済みのファイルがすべて削除されます。これには、カスタム壁紙、ブランディング要素、証明書、お気に入りリストなどが含まれます。
- 以前の (非アクティブな) ソフトウェア イメージが削除されます。
- オプション キーは影響を受けません。

初期設定にリセットした後は、デバイス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。

初期設定へのリセットを実行する前に、デバイスのログ ファイル、設定、カスタム要素をバックアップすることを推奨します。バックアップしない場合、これらのデータは失われます。

## ビデオ会議デバイスの初期設定へのリセット (2/3 ページ)

### Web インターフェイスを使用した初期設定へのリセット

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

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

1. [\[初期設定へのリセット \(Factory Reset\)\]](#) タブを選択して、表示される情報を注意深く読みます。
2. [\[初期設定へのリセットの実行 \(Perform a factory reset...\)\]](#) をクリックします。
3. [\[はい \(Yes\)\]](#) をクリックして選択を確定するか、[\[キャンセル \(Cancel\)\]](#) をクリックして操作を取り消します。
4. デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。  
デバイスが正常に初期設定にリセットされると、セットアップ アシスタントが起動し、[\[ようこそ \(Welcome\)\]](#) 画面が表示されます。

### ユーザ インターフェイスからの初期設定へのリセット

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [\[設定 \(Settings\)\]](#) を選択します。
3. [\[初期設定へのリセット \(Factory Reset\)\]](#) を選択します。
4. 選択を確定するには[\[リセット \(reset\)\]](#)を選択し、リセットを中止する場合は[\[戻る \(Back\)\]](#)を選択します。
5. デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。  
デバイスが正常に初期設定にリセットされると、セットアップ アシスタントが起動し、[\[ようこそ \(Welcome\)\]](#) 画面が表示されます。

### ログ ファイル、構成、カスタム要素のバックアップ

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

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

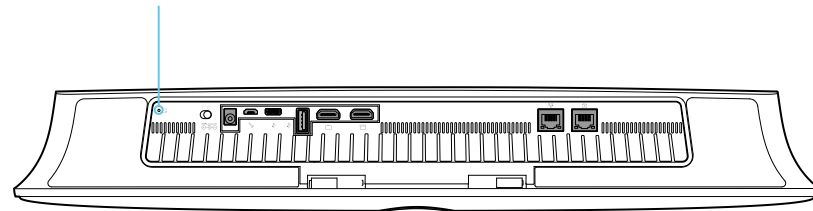
## ビデオ会議デバイスの初期設定へのリセット (3/3 ページ)

### リセット ボタンを使用して工場出荷時設定にリセットする

初期設定へのリセットを続行する前に、デバイスのログ ファイルと設定をバックアップすることを推奨します。

1. ユニットを前に傾け、リセット ボタン (ピン ホール) が見えるようにします。
2. ペーパークリップ (または同等のもの) を使用して、画面が黒くなるまでリセット ボタンを押し続けます (約 10 秒)。その後、ボタンを離します。
3. デバイスがデフォルトの初期設定に戻るまで待ちます。完了するとデバイスが自動的に再起動します。数分かかることがあります。  
デバイスが正常に初期設定にリセットされると、セットアップアシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。

リセット ボタン (ピン ホール)




## Cisco Touch 10 の初期設定へのリセット

この章は、2017 年後半に発売された Touch 10 コントローラ (Cisco Touch 10) に適用されます。このデバイスは、前面の口ゴ、および背面のコネクタが少ないことによって識別されます。

古いバージョンについては、次のページを参照してください。

エラー状態で、接続を再確立するためにタッチ コントローラを工場出荷時設定にリセットすることが必要になる場合があります。その場合は、必ず Cisco のサポート組織に連絡して実行する必要があります。

Touch コントローラを初期設定にリセットすると、ペアリング情報が失われ、(ビデオ会議デバイスではなく) Touch 自体がデフォルトの初期設定に戻ります。

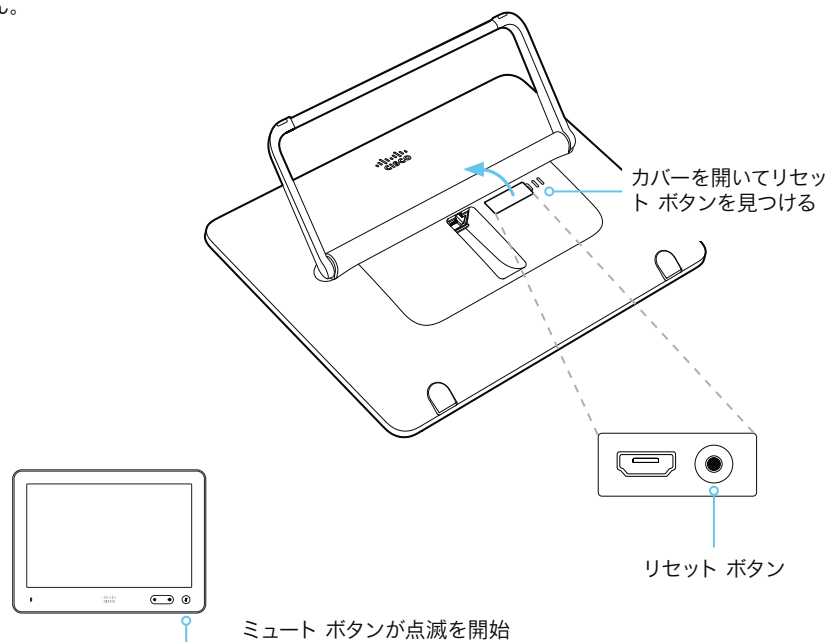
 初期設定にリセットすると元に戻すことはできません。

1. 背面の小さなカバーを開き、リセット ボタンを見つけます。
2. 前面のミュート ボタンが点滅し始めるまでリセット ボタンを押し続けます (約 5 秒間)。その後、ボタンを離します。

Touch 10 が工場出荷時設定へと自動的に戻され、再起動されます。

Touch 10 がビデオ会議デバイスに直接接続されている場合は、デバイスから新しい設定を自動的に受信します。

Touch 10 が LAN 経由で接続されている場合は、改めてビデオ会議デバイスとペアリングする必要があります。ペアリングが成功すると、デバイスから新しい設定を自動的に受信します。



## ペアリングおよびビデオ会議デバイスと Touch 10 の接続方法について

Touch 10 コントローラを使用するには、ビデオ会議デバイスに直接接続するか、LAN 経由でビデオ会議デバイスとペアリングする必要があります。後者はリモート ペアリングと呼ばれます。

ペアリングおよび Touch 10 とビデオ会議デバイスの接続方法については、▶ [「Touch 10 コントローラの接続」](#)の章を参照してください。


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

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

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

エラー状態で、接続を再確立するためにタッチ コントローラを工場出荷時設定にリセットすることが必要な場合があります。その場合は、必ずシスコのサポート組織に連絡して実行する必要があります。

Touch コントローラを初期設定にリセットすると、ペアリング情報が失われ、(ビデオ会議デバイスではなく) Touch 自体がデフォルトの初期設定に戻ります。

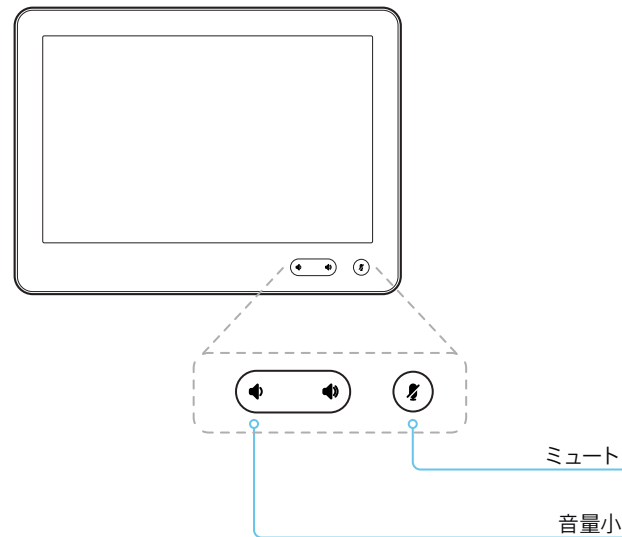
 初期設定にリセットすると元に戻すことはできません。

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

Touch 10 が工場出荷時設定へと自動的に戻され、再起動されます。

Touch 10 がビデオ会議デバイスに直接接続されている場合は、デバイスから新しい設定を自動的に受信します。

Touch 10 が LAN 経由で接続されている場合は、改めてビデオ会議デバイスとペアリングする必要があります。ペアリングが成功すると、デバイスから新しい設定を自動的に受信します。



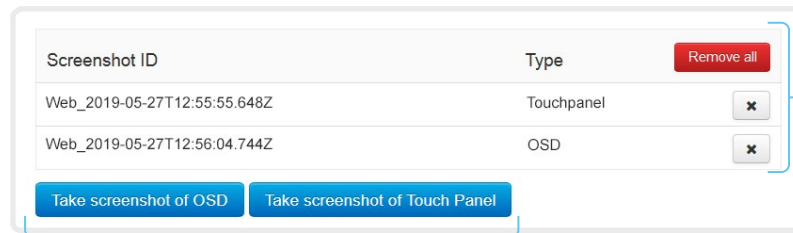
### ペアリングおよびビデオ会議デバイスと Touch 10 の接続方法について

Touch 10 コントローラを使用するには、ビデオ会議デバイスに直接接続するか、LAN 経由でビデオ会議デバイスとペアリングする必要があります。後者はリモート ペアリングと呼ばれます。

ペアリングおよび Touch 10 とビデオ会議デバイスの接続方法については、▶ [「Touch 10 コントローラの接続」](#)の章を参照してください。

## ユーザインターフェイスのスクリーンショットのキャプチャ

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



### スクリーンショットのキャプチャ

Touch コントローラのスクリーンショットをキャプチャするには、[\[タッチパネルのスクリーンショットを撮る \(Take screenshot of Touch Panel\)\]](#) をクリックします。メイン画面 (オンスクリーン ディスプレイ) のスクリーンショットをキャプチャするには、[\[OSDのスクリーンショットを撮る \(Take screenshot of OSD\)\]](#) をクリックします。

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

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

### スクリーンショットを削除する

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

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

### ユーザ インタフェースのスクリーンショットについて

デバイスに接続されている Touch コントローラのスクリーンショットや、メニュー、インジケータ、メッセージを含むメイン画面 (オンスクリーン ディスプレイとも呼ばれる) のスクリーンショットをキャプチャできます。



## 第 5 章

# デバイスの設定

## デバイス設定の概要

これ以降のページでは、Web インターフェイスの [\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) ページで設定する、すべてのデバイス設定のリストを示します。

Web ブラウザを開き、デバイスの IP アドレスを入力して、サインインします。

### IP アドレスの確認方法

1. ユーザ インターフェイスの最上部にあるデバイス名またはアドレスを選択します。
2. [\[このデバイスについて \(About this device\)\]](#) に続き、[\[設定 \(Settings\)\]](#) を選択します。

オーディオ設定	100
オーディオ デフォルト音量	100
オーディオ 入力 HDMI [n] レベル	100
オーディオ 入力 HDMI [n] モード	100
オーディオ 入力 HDMI [n] ビデオの関連付け 非アクティブなビデオでミュート	100
オーディオ キークリック検出 減衰	100
オーディオ キークリック検出 有効	101
オーディオ マイク ミュート 有効	101
オーディオ サウンドとアラート 着信音	101
オーディオ サウンドとアラート 着信音量	101
オーディオ 超音波 最大音量	101
オーディオ 超音波 モード	101
通話履歴設定	102
通話履歴モード	102
カメラ設定	103
カメラ カメラ フレームレート	103
カメラ 電源 周波数	103
カメラ スピーカートラック モード	103
会議設定	104
会議 アクティブコントロール モード	104
会議 自動応答 遅延	104
会議 自動応答 モード	104
会議 自動応答 ミュート	104
会議 通信プロトコルIPスタック	104
会議 デフォルトコール プロトコル	105
会議のデフォルト コール レート	105
会議 応答不可 デフォルトタイムアウト	105
会議 暗号化 モード	105
会議 遠端制御 モード	105
会議 遠端制御 信号機能	106
会議 遠端メッセージ モード	106
会議 着信マルチサイトコール モード	108
会議 最大受信コールレート	106
会議 最大合計受信コールレート	106
会議 最大合計転送コールレート	107

会議 最大転送コールレート .....	106	ロギング 外部 Tls検証 .....	116
会議 切断時のマイクのミュート解除 モード .....	107	ロギング 内部 モード .....	116
会議 マルチポイント モード .....	107	ロギング クラウドアップロード モード .....	115
会議 マルチストリーム モード .....	108	ロギング 外部 Tls 検証 .....	116
会議 プレゼンテーション 保留時の動作 .....	108	マクロ設定 .....	117
会議 プレゼンテーション リレー品質 .....	108	マクロ 自動スタート .....	117
ファシリティサービス設定 .....	109	マクロ モード .....	117
ファシリティサービス サービス [n] コールタイプ .....	109	マクロ XAPI トランスポート .....	117
ファシリティサービス サービス [n] 名前 .....	109	マクロ 無応答タイムアウト .....	117
ファシリティサービス サービス [n] 番号 .....	109	ネットワーク設定 .....	118
ファシリティサービス サービス [n] タイプ .....	109	ネットワーク [n] DNS DNSSEC モード .....	118
H323 設定 .....	110	ネットワーク [n] DNS ドメイン 名前 .....	118
H323 認証ログイン名 .....	110	ネットワーク [n] DNS サーバ [m] アドレス .....	118
H323 認証モード .....	110	ネットワーク [n] IEEE8021X 匿名ID .....	119
H323 認証パスワード .....	110	認証パスワード [n] IEEE8021X Eap Md5 .....	120
H323 コールセットアップモード .....	110	認証パスワード [n] IEEE8021X Eap Peap .....	120
H323 暗号化キーサイズ .....	111	認証パスワード [n] IEEE8021X Eap Tls .....	120
H323 ゲートキーパー アドレス .....	111	認証パスワード [n] IEEE8021X Eap Tls .....	120
H323 エイリアス E164 .....	111	認証パスワード [n] IEEE8021X Identity .....	119
H323 エイリアス ID .....	111	認証パスワード [n] IEEE8021X モード .....	118
H323 NAT アドレス .....	112	認証パスワード [n] IEEE8021X パスワード .....	119
H323 NAT モード .....	111	認証パスワード [n] IEEE8021X Tls検証 .....	119
H323 ポート割り当て .....	112	認証パスワード [n] IEEE8021X クライアント証明書の使用 .....	119
HttpClient 設定 .....	113	認証パスワード [n] IP スタック .....	120
HttpClient HTTPを許可 .....	113	認証パスワード [n] IPv4 アドレス .....	121
HttpClient 安全でないHTTPSを許可 .....	113	認証パスワード [n] IPv4 割り当て .....	121
HttpClient Http プロキシの使用 .....	113	認証パスワード [n] IPv4 ゲートウェイ .....	121
HttpClient モード .....	113	認証パスワード [n] IPv4 サブネットマスク .....	121
HTTP フィードバック設定 .....	114	認証パスワード [n] IPv6 アドレス .....	122
HttpFeedback Http プロキシの使用 .....	114	認証パスワード [n] IPv6 割り当て .....	121
HttpFeedback Tls 検証 .....	114	認証パスワード [n] IPv6 DHCPオプション .....	122
ロギングの設定 .....	115	認証パスワード [n] IPv6 ゲートウェイ .....	122
ロギング デバッグ Wifi .....	115	認証パスワード [n] MTU .....	122
ロギング 外部 モード .....	115	認証パスワード [n] QoS Diffserv オーディオ .....	123
ロギング 外部 プロトコル .....	115	認証パスワード [n] QoS Diffserv データ .....	123
ロギング 外部 サーバ アドレス .....	115	認証パスワード [n] QoS Diffserv ICMPv6 .....	124
ロギング 外部 サーバ ポート .....	116	認証パスワード [n] QoS Diffserv NTP .....	124
		認証パスワード [n] QoS Diffserv シグナリング .....	123
		認証パスワード [n] QoS Diffserv ビデオ .....	123

認証パスワード [n] QoS モード.....	122	ネットワーク サービス WiFi 有効.....	133
認証パスワード [n] リモートアクセス 許可.....	124	ネットワークサービス XMLAPI モード.....	134
認証パスワード [n] 速度.....	124	ネットワークサービス SMTP サーバ.....	130
認証パスワード [n] トラフィック制御 モード.....	125	ネットワークサービス SMTP セキュリティ.....	131
認証パスワード [n] VLAN 音声 モード.....	125	ネットワークサービス SMTP パスワード.....	130
認証パスワード [n] VLAN 音声 VlanId.....	125	ネットワークサービス SMTP ポート.....	130
ネットワークサービス設定.....	126	ネットワークサービス SMTP ユーザー名.....	130
ネットワークサービス CDP モード.....	126	ネットワークシステム SMTP 送信元.....	131
ネットワークサービス H323 モード.....	126	周辺機器の設定.....	135
ネットワークサービス HTTP モード.....	126	周辺機器 入力デバイス モード.....	135
ネットワークサービス HTTP プロキシ ログイン名.....	126	周辺機器 ペアリング Ciscoタッチパネル Emcレジリエンス.....	135
ネットワークサービス HTTP プロキシ モード.....	127	周辺機器 ペアリング Ciscoタッチパネル リモートペアリング.....	135
ネットワークサービス HTTP プロキシ PACUrl.....	127	周辺機器 プロファイル カメラ.....	135
ネットワークサービス HTTP プロキシ パスワード.....	127	周辺機器 プロファイル 制御システム.....	136
ネットワークサービス HTTP プロキシ Url.....	127	周辺機器 プロファイル タッチパネル.....	136
ネットワークサービス HTTPS OCSP モード.....	127	電話帳の設定.....	137
ネットワークサービス HTTPS OCSP URL.....	128	電話帳 サーバ [n] ID.....	137
ネットワークサービス HTTPS サーバ 最小TLSバージョン.....	128	電話帳 サーバ [n] ページネーション.....	137
ネットワークサービス HTTPS StrictTransportSecurity.....	128	電話帳 サーバ [n] タイプ.....	138
ネットワークサービス HTTPS クライアント証明書の検証.....	128	電話帳 サーバ [n] URL.....	138
ネットワークサービス NTP モード.....	128	電話帳 サーバ [n] TLS 検証.....	137
ネットワークサービス NTP サーバ [n] アドレス.....	129	プロビジョニング設定.....	139
ネットワークサービス NTP サーバ [n] キー.....	129	プロビジョニング 接続.....	139
ネットワークサービス NTP サーバ [n] キーアルゴリズム.....	129	プロビジョニング 外部マネージャー アドレス.....	139
ネットワークサービス NTP Server [n] キーID.....	129	プロビジョニング 外部マネージャー 代替アドレス.....	139
ネットワークサービス SIP モード.....	129	プロビジョニング 外部マネージャー ドメイン.....	140
ネットワークサービス SMTP モード.....	130	プロビジョニング 外部マネージャー パス.....	140
ネットワークサービス SNMP コミュニティ名.....	131	プロビジョニング 外部マネージャー プロトコル.....	140
ネットワークサービス SNMP モード.....	131	プロビジョニング ログイン名.....	140
ネットワークサービス SNMP システム管理者.....	131	プロビジョニング モード.....	140
ネットワークサービス SNMP システムロケーション.....	132	プロビジョニング CUCM コール管理レコード.....	139
ネットワークサービス SSH 公開キーの許可.....	132	プロビジョニング パスワード.....	141
ネットワークサービス SSH ホストキーアルゴリズム.....	132	プロビジョニング Tls 検証.....	141
ネットワークサービス SSH モード.....	132	プロビジョニング WebexEdge.....	141
ネットワークサービス UPnP モード.....	132	プロキシミティの設定.....	142
ネットワークサービス UPnP タイムアウト.....	133	プロキシミティ モード.....	142
ネットワークサービス Websocket.....	133	プロキシミティ サービス コール制御.....	142
ネットワークサービス ウェルカムテキスト.....	133		
ネットワークサービス Wifi 許可.....	133		

プロキシミティ サービス コンテンツ共有 クライアントから.....	143	SIP 表示名 .....	151
プロキシミティ サービス コンテンツ共有 クライアントから.....	143	SIP Ice デフォルト候補 .....	152
プロキシミティ 代替ポート 有効.....	142	SIP Ice モード .....	152
ルーム分析設定 .....	144	SIP 回線.....	152
ルーム分析 環境雑音の予測 モード .....	144	SIP リッスンポート .....	152
ルーム分析 非通話中の人をカウント .....	144	SIP メールボックス .....	153
ルーム分析 人の存在の検出.....	144	SIP 最小TLSバージョン .....	153
ルームリセットの設定.....	145	SIP 優先IPシグナリング .....	153
ルームリセット 制御.....	145	SIP プロキシシ [n] アドレス .....	153
RTP 設定 .....	146	SIP Tls検証.....	153
RTP ポート 範囲 開始 .....	146	SIP Turn 検出モード .....	154
RTP ポート 範囲 終了.....	146	SIP Turn ドロップ Rflx.....	154
RTP ビデオ ポート 範囲 開始 .....	146	SIP Turn パスワード .....	154
RTP ビデオ ポート 範囲 終了.....	146	SIP Turn サーバ.....	154
セキュリティ設定 .....	147	SIP Turn ユーザ名 .....	154
セキュリティ 監査 ログイン モード .....	147	SIP タイプ .....	154
セキュリティ 監査 エラー発生時 アクション .....	147	SIP URI .....	155
セキュリティ 監査 サーバ アドレス .....	147	スタンバイ設定 .....	156
セキュリティ 監査 サーバ ポート .....	147	スタンバイ ブートアクション .....	156
セキュリティ 監査 サーバ ポート 割り当て .....	148	スタンバイ 制御.....	156
セキュリティ セッション ログイン失敗時のロックアウト時間 .....	148	スタンバイ 遅延.....	156
セキュリティ セッション 非アクティブタイムアウト .....	148	スタンバイ スタンバイアクション .....	157
セキュリティ セッション ログイン失敗の最大数.....	148	スタンバイ ウェイクアップアクション .....	157
セキュリティ セッション ユーザあたりの最大セッション数 .....	149	スタンバイ モーション検知ウェイクアップ .....	157
セキュリティ セッション 最大総セッション数.....	149	スタンバイ サイネージ Url.....	157
セキュリティ セッション 最後のログオンを表示 .....	149	スタンバイ サイネージ オーディオ .....	156
セキュリティ Fips モード .....	148	スタンバイ サイネージ モード.....	157
シリアルポート設定.....	150	スタンバイ サイネージ 対話モード .....	156
シリアルポート ボーレート .....	150	スタンバイ サイネージ 更新間隔.....	157
シリアルポート ログインが必要.....	150	システムユニット設定.....	158
シリアルポート モード .....	150	高度なシステムユニット クラッシュレポート .....	158
SIP 設定 .....	151	システムユニット クラッシュレポート モード .....	158
SIP ANAT.....	151	システムユニット クラッシュレポート Url .....	158
SIP 認証パスワード .....	151	システムユニット名 .....	158
SIP 認証 ユーザ名.....	151	時刻設定 .....	159
SIP デフォルトトランスポート.....	151	時刻 日付形式 .....	159
		時刻 時刻形式.....	159
		タイムゾーン .....	160

ユーザインターフェイス設定.....	162	ユーザ管理 LDAP モード.....	170
ユーザインターフェイス アクセシビリティ 着信コール通知.....	162	ユーザ管理 LDAP サーバ アドレス.....	170
ユーザインターフェイス ブランディング アウェイク状態のブランディング 色.....	163	ユーザ管理 LDAP サーバ ポート.....	170
ユーザインターフェイス 連絡先情報 タイプ.....	163	ユーザ管理 LDAP サーバ証明書の検証.....	170
ユーザインターフェイス カスタムメッセージ.....	163	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 再使用制限.....	172
ユーザインターフェイス 機能 コール 終了.....	164	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 最大有効期間.....	172
ユーザインターフェイス 機能 コール 通話中のコントロール.....	164	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 複雑度 最小文字数.....	171
ユーザインターフェイス 機能 コール 開始.....	164	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 複雑度 大文字の最小数.....	172
ユーザインターフェイス 機能 コール ビデオミュート.....	164	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 複雑度 小文字の最小数.....	171
ユーザインターフェイス 機能 すべて非表示.....	165	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 複雑度 数字の最小数.....	171
ユーザインターフェイス 機能 共有 開始.....	165	ユーザインターフェイス 連絡先情報 タイプ管理 パスワードポリシー 複雑度 特殊文字の最小数.....	171
ユーザインターフェイス キートーン モード.....	163	ビデオ設定.....	173
ユーザインターフェイス 言語.....	165	ビデオ アクティブスピーカー デフォルトPIPポジション.....	173
ユーザインターフェイス OSD 暗号化インジケータ.....	165	ビデオ デフォルトレイアウトファミリ ローカル.....	173
ユーザインターフェイス OSD ハーフアウェイクメッセージ.....	165	ビデオ デフォルトレイアウトファミリ リモート.....	174
ユーザインターフェイス OSD 出力.....	165	ビデオ デフォルトメインソース.....	174
ユーザインターフェイス 電話帳 モード.....	166	ビデオ 入力 コネクタ [n] カメラ制御 カメラID.....	174
ユーザインターフェイス セキュリティ モード.....	166	ビデオ 入力 コネクタ [n] カメラ制御 モード.....	174
ユーザインターフェイス 設定メニュー モード.....	166	ビデオ 入力 コネクタ [n] CEC モード.....	174
ユーザインターフェイス設定メニュー可視性.....	167	ビデオ 入力 コネクタ [n] 入力ソースタイプ.....	175
ユーザインターフェイス 壁紙.....	167	ビデオ 入力 コネクタ [n] 名前.....	175
ユーザインターフェイス Usbプロモーション.....	167	ビデオ 入力 コネクタ [n] 最適鮮明度 プロファイル.....	175
ユーザインターフェイス Webcamのみモード.....	168	ビデオ 入力 コネクタ [n] 最適鮮明度 60fpsのしきい値.....	176
ユーザインターフェイス アシスタント モード.....	162	ビデオ 入力 コネクタ [n] 推奨解像度.....	176
ユーザインターフェイス アシスタント 会議参加確認.....	162	ビデオ 入力 コネクタ [n] プレゼンテーションの選択.....	176
ユーザインターフェイス サウンドエフェクト モード.....	167	ビデオ 入力 コネクタ [n] 画質.....	177
ユーザインターフェイス プロキシミティ 通知.....	166	ビデオ 入力 コネクタ [n] RGB量子化範囲.....	177
ユーザインターフェイス ホワイトボード アクティビティインジケータ.....	168	ビデオ 入力 コネクタ [n] 可視性.....	177
ユーザインターフェイス 予約 可視性 タイトル.....	162	ビデオ 出力 コネクタ [n] CEC モード.....	178
ユーザインターフェイス 機能 コール Webexに参加.....	164	ビデオ 出力 コネクタ [n] モニタロール.....	178
ユーザインターフェイス 機能 コール キーパッド.....	164	ビデオ 出力 コネクタ [n] 解像度.....	178
ユーザインターフェイス 診断 通知.....	163	ビデオ 出力 コネクタ [n] RGB量子化範囲.....	179
ユーザ管理設定.....	169	ビデオ プレゼンテーション デフォルトPIPポジション.....	179
ユーザ管理 LDAP 管理者 フィルタ.....	169	ビデオプレゼンテーション デフォルトソース.....	179
ユーザ管理 LDAP 管理者 グループ.....	169	ビデオ プレゼンテーション 優先順位.....	179
UserManagement LDAP Attribute.....	169	ビデオセルフビュー デフォルト フルスクリーンモード.....	180
ユーザ管理 LDAP ベースDN.....	169	ビデオ セルフビュー デフォルト モード.....	180
ユーザ管理 LDAP 暗号化.....	169	ビデオ セルフビュー デフォルト 表示先モニタロール.....	180
ユーザ管理 LDAP 最小TLSバージョン.....	170	ビデオ セルフビュー デフォルトPIPポジション.....	180

ビデオ セルフビュー オンコール 時間 .....	181
ビデオ セルフビュー オンコール モード .....	181
<b>Web エンジン設定</b> .....	182
Web エンジン Http プロキシの使用 .....	182
Web エンジン モード .....	182
Web エンジン リモートデバッグ .....	182
Webエンジン 機能 WebGL .....	182
試験的設定 .....	183

## オーディオ設定

### オーディオ デフォルト音量

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

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: 50

値スペース: 整数 (0..100)

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

### オーディオ入力 HDMI [n] レベル

n: 1..1

HDMI 入力コネクタのゲインを設定します。ゲインは、1 db ずつ調整できます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 0

値スペース: 整数 (-24..0)

範囲: デシベル (dB) 単位でゲインを選択します。

### オーディオ 入力 HDMI [n] モード

n: 1..1

HDMI 入力コネクタの音声を有効にするかどうかを定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: HDMI 入力での音声を無効にします。

On: HDMI 入力での音声を有効にします。

### オーディオ 入力 HDMI [n] ビデオの関連付け 非アクティブなビデオでミュート

n: 1..1

この設定を使用して、このプレゼンテーション ソースが現在画面上に表示されていない場合、またはプレゼンテーション ソースが接続されている間常に音声を再生する場合音声再生を停止するかどうかを決定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: 音声は、プレゼンテーション ソースが接続されている間、ローカルおよび相手先に対して常に再生されます。HDMI 入力ソースを指定する必要はありません。

On: 音声は、接続されているプレゼンテーション ソースが画面上に表示されている間、ローカルおよび相手先に対して再生されます。

### オーディオ キークリック検出 減衰

デバイスがキーボードからのクリック ノイズを検出し、マイク信号を自動的に減衰させることができます。キーボードのノイズが他の参加者の邪魔をする可能性があるため、会議出席者がキーボードで入力を開始するときにはこの機能が便利です。参加者がキーボードで入力しながら話す場合、マイクの信号は減衰しません。[オーディオ キー クリック ディテクタ有効化 (Audio KeyClickDetector Enabled) ] 設定が On に設定されている必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: True

値スペース: False/True

False: マイクの信号の減衰は無効です。

True: キーボードのクリック ノイズが検出された場合、デバイスによりマイクの信号が減衰されます。音声または音声とキーボードのクリックが併せて検出された場合、マイクの信号は減衰されません。



## オーディオ キークリック検出 有効

デバイスがキーボードからのクリック ノイズを検出し、マイク信号を自動的に減衰させることができます。キー入力のノイズが他の参加者の邪魔をする可能性があるため、会議出席者がキーボードで入力を開始するときにはこの機能が便利です。マイクの信号の減衰を有効にするには、[オーディオ キークリック ディテクタ減衰 (Audio KeyClickDetector Attenuate)] を On にします。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: True

値スペース: False/True

False: キークリックの検出は無効です。

True: デバイスによりキーボードからクリック ノイズが検出されます。

## オーディオ マイク ミュート 有効

デバイスでのマイク ミュートの動作を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: True

値スペース: True/InCallOnly

True: 音声ミュートが使用可能になります。通常、コール外ではマイクのミュート LED は点灯しませんが、API コマンドを使用するとミュートすることができます。

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または音声システムがデバイスを介して接続されており、デバイスがコール中でないときに使用可能にする場合に便利です。InCallOnly に設定されたとき、音声システムが誤ってミュートにされることを防止できます。

## オーディオ サウンドとアラート 着信音

着信コールに使用する着信音を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Sunrise

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

リストから呼び出し音を選択します。

## オーディオ サウンドとアラート 着信音量

着信コールの着信音量を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: 50

値スペース: 整数 (0..100)

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

## オーディオ 超音波 モード

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。設定はデフォルト値のままにしておいてください。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Dynamic

値スペース: Dynamic/Static

Dynamic: デバイスが超音波ボリュームを動的に調整します。ボリュームは、[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] の設定で定義された最大レベルまでさまざまに変化します。

Static: シスコが助言した場合にのみ使用してください。

## オーディオ 超音波 最大音量

この設定は、Intelligent Proximity 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。

[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定と [プロキシミティ モード (Proximity Mode)] 設定は、超音波ペアリングメッセージにのみ影響します。超音波を使用した人の存在の検出とモーション検知については、[ルーム分析 人の存在の検出 (RoomAnalytics PeoplePresenceDetector)] 設定および [スタンバイ モーション検知ウェイクアップ (Standby WakeupOnMotionDetection)] 設定を参照してください。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 70

値スペース: 整数 (0..70)

値は指定の範囲内から選択します。0 に設定すると、超音波ペアリングメッセージは出力されません。

## 通話履歴設定

### 通話履歴モード

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: 新しいエントリが通話履歴に追加されません。

On: 新しいエントリは通話履歴一覧に保存されます。

## カメラ設定

### カメラのカメラ フレーム レート

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

必要なユーザ ロール: ADMIN

デフォルト値: 30

値スペース: 30/60

30: カメラは、1 秒あたり 30 フレームを出力します。

60: カメラは 1 秒あたり 60 フレームを出力します。

### カメラ電源周波数

カメラが電源周波数フリッカー防止をサポートしている場合、カメラは電源からのすべてのフリッカ ノイズを補うことができます。このカメラ設定はお使いの電源周波数に基づいて設定する必要があります。カメラが電源周波数の自動検出をサポートしている場合、設定で Auto オプションを選択できます。

シスコのカメラは、フリッカ防止と電源周波数の自動検出の両方をサポートしています。Auto はデフォルト値であるため、自動検出をサポートしないカメラの場合、この設定を変更する必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: 50Hz/60Hz/Auto

50Hz: 電線周波数が 50 Hz の場合、この値を使用します。

60Hz: 電線周波数が 60 Hz の場合、この値を使用します。

Auto: カメラが電源周波数を自動検出できるようにします。

### カメラ スピーカー トラック モード

ビデオ会議デバイスは Best Overview 機能をサポートしています。最高の概要は自動カメラ フレーミングを使用し、室内の人数に基づいて最適なカメラ表示を選択します。スピーカートラッキングはサポートされていません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: Auto/Off

自動: Best Overview がオンになっています。デバイスが室内の人々を検出して自動的に最適なカメラフレーミングを選択します。ユーザーは、タッチコントローラのカメラのコントロールパネルで Best Overview のオンとオフを即座に切り替えることができますが、各コールの後は、次のユーザーに備えて機能が再度オンになります。

オフ: Best Overview がオフになっています。

## 会議設定

### 会議 アクティブ コントロール モード

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

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/Off

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

Off: アクティブ コントロールは無効です。

### 会議 自動応答 モード

自動応答モードを定義します。デバイスを使用して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会議自動応答のミュート設定を使用します。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: タッチ コントローラで [応答 (Answer)] をタップし、着信コールに手動で応答できます。

On: コール中でなければ、デバイスが自動的に着信コールに応答します。常に手動で、通話中の着信コールの応答や拒否が行えます。

### 会議自動応答のミュート

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: 着信コールはミュートにされません。

On: 着信コールは自動的に応答されるときミュートにされます。

### 会議 自動応答 遅延

デバイスが自動応答するまで着信コールが待つ必要がある時間 (秒単位) を定義します。[自動応答モード (AutoAnswer Mode)] が有効にされている必要があります。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数 (0..50)

自動応答遅延 (秒単位)。

### 会議 通信プロトコルIPスタック

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

必要なユーザ ロール: ADMIN

デフォルト値: Dual

値スペース: Dual/IPv4/IPv6

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

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

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

## 会議 デフォルト コール プロトコル

デバイスからコールを発信するときに使用するデフォルトのコール プロトコルを定義します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/H320/H323/Sip/Spark

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

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

H323: すべてのコールが H.323 コールとして設定されます。

SIP: すべてのコールが SIP コールとして設定されます。

Spark: Webex 登録済みデバイスのために予約されています。使用しません。

## 会議 デフォルトコール レート

デバイスからコールを発信するときに使用するデフォルトのコール レートを定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 6000

値スペース: 整数 (64..6000)

デフォルト コール レート (kbps) です。

## 会議 応答不可 デフォルトタイムアウト

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 60

値スペース: 整数 (1..1440)

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

## 会議 暗号化 モード

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

注: 暗号化オプション キーがデバイスにインストールされていない場合、暗号化モードは常に [オフ (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: デバイスは暗号化を使用しません。

On: デバイスは、暗号化されたコールだけを許可します。

BestEffort: デバイス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: 相手先デバイスで暗号化 (AES-128) がサポートされている場合、コールは暗号化されます。そうでない場合は、コールは暗号化なしで送信されます。

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

## 会議 遠端制御 モード

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

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

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

## 会議 遠端制御 信号機能

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無効にします。

On: 遠端制御信号機能を有効にします。

## 会議 遠端メッセージ モード

制御システムまたはマクロと併用するために、ポイントツーポイント コールにおける 2 台のデバイス間でデータ送信が許可されているかどうかを切り替えます。SIP コールでのみ動作します。この設定は、遠隔メッセージ送信コマンドの xCommand のコール使用を有効化または無効化します。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: 2 台のデバイス間でメッセージを送信できません。

On: ポイントツーポイント コールの 2 台のデバイス間でメッセージ送信を行うことができます。

## 会議 最大受信コールレート

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

必要なユーザ ロール: ADMIN

デフォルト値: 6000

値スペース: 整数 (64..6000)

最大受信帯域 (kbps)。

## 会議 最大転送コールレート

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

必要なユーザ ロール: ADMIN

デフォルト値: 6000

値スペース: 整数 (64..6000)

最大送信帯域 (kbps)。

## 会議 最大合計受信コールレート

この設定は、デバイスに搭載された MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

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

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

必要なユーザ ロール: ADMIN

デフォルト値: 6000

値スペース: 整数 (64..6000)

最大受信帯域 (kbps)。

## 会議 最大合計転送コールレート

この設定は、デバイスに搭載された MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

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

個々のコールの最大送信ビット レートは、会議 最大転送コールレート設定により定義されます。

必要なユーザ ロール: ADMIN

デフォルト値: 6000

値スペース: 整数 (64..6000)

最大送信帯域 (kbps)。

## 会議 切断時のマイクのミュート解除 モード

すべてのコールが切断されたときに、マイクを自動的にミュート解除するかどうかを定義します。会議室またはその他の共有リソースでは、次のユーザのためにデバイスを準備するためにこれを実行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。

## 会議 マルチポイント モード

ポイントツーポイント ビデオ コール (2 者間のコール) から、参加者を追加してマルチポイント会議 (アドホック会議) に拡大する方法を定義します。ローカルのリソースのみに依存する組み込みの MultiSite 機能と、集中型のインフラストラクチャ (マルチポイント コントロール ユニット: MCU) をベースとする別のソリューションの両方を使用することができます。

MultiSite 機能はアップグレードオプションであり、すべてのデバイスで使用できるとは限りません。デバイスには、MultiSite オプション キーをインストールする必要があります。

Cisco TelePresence Video Communication Server (VCS) に登録されている場合、デバイスは他のビデオデバイスを呼び出す場合に MultiSite を使用できます。Cisco Unified Communications Manager (CUCM) バージョン 8.6.2 以降に登録されている場合、デバイスは、CUCM 会議ブリッジ、またはデバイス内蔵の MultiSite 機能を使用できます。使用するオプションは CUCM によってセットアップされます。

いずれの場合も、デバイスが会議に参加者を追加できるように MCU を呼び出す場合、MCU を介してマルチ パーティ会議がセットアップされます (直接リモート追加)。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/CUCMMediaResourceGroupList/MultiSite/Off

Auto: マルチ ポイント メソッドが自動的に選択されます。

MultiSite オプション キーをデバイスにインストールして、他のビデオ デバイス (MCU 以外) を呼び出す場合、マルチ パーティ会議は、組み込みの MultiSite 機能を使ってセットアップされません。参加者を追加できるのは MultiSite のホストのみです。これにより、カスケード会議ができなくなります。デバイスに MultiSite オプション キーがない場合、複数のビデオ デバイスをビデオで呼び出すことはできません。音声のみの参加者を 1 人追加できます。

MultiSite オプション キーに関係なく、デバイスが会議に参加者を追加する (Direct Remote Add) MCU を呼び出す場合、MCU を介してマルチ パーティ会議をセットアップすることができます。

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

MultiSite: デバイスに MultiSite オプション キーがインストールされている場合は、組み込み MultiSite 機能を使ってマルチ パーティ会議がセットアップします。デバイスに MultiSite オプション キーがない場合、複数のデバイスをビデオでコールすることはできません。音声のみのデバイスを 1 つ追加できます。

Off: 複数のデバイスをビデオでコールすることはできませんが、音声のみのデバイスを追加することができます。デバイスが会議に参加者を追加できるように MCU を呼び出す場合、MCU を介してマルチ パーティ会議がセットアップされます (直接リモート追加)。



## 会議 マルチストリーム モード

デバイスは、会議のマルチストリーム ビデオをサポートします。

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

Off: マルチストリームが無効になります。

## 会議 着信マルチサイトコール モード

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

必要なユーザ ロール: ADMIN

デフォルト値: Allow

値スペース: Allow/Deny

Allow: すでに通話している間に、誰かが電話をかけてきた場合、通知されます。着信コールを受け入れるかどうかは任意です。着信コールに応答している間、進行中のコールを保留しておくこともできますし、それらのコールをマージすることもできます (マルチパーティ ビデオ会議をサポートしている必要があります)。

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

## 会議 プレゼンテーション 保留時の動作

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

必要なユーザ ロール: ADMIN

デフォルト値: NoAction

設定可能な値: NoAction/Stop

NoAction: 保留しても、デバイスはプレゼンテーションの共有を停止しません。保留されている間はプレゼンテーションは共有されませんが、コールが再開されると自動的に継続されます。

Stop: リモート サイトで保留されると、デバイス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。

## 会議プレゼンテーションのリレー品質

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

必要なユーザ ロール: ADMIN

デフォルト値: Sharpness

値スペース: Motion/Sharpness

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

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



## ファシリティサービス設定

### ファシリティサービス サービス [n] タイプ

n: 1..5

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Helpdesk

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

Catering: ケータリング サービスには、このオプションを選択します。

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

Emergency: 緊急サービスには、このオプションを選択します。

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

Security: セキュリティ サービスには、このオプションを選択します。

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

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

### ファシリティサービス サービス [n] 名前

n: 1..5

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

必要なユーザ ロール: ADMIN、INTEGRATOR

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

値スペース: 文字列 (0, 1024)

ファシリティ サービスの名前。

### ファシリティサービス サービス [n] 番号

n: 1..5

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 1024)

ファシリティ サービスの番号 (URI または電話番号)。

### ファシリティサービス サービス [n] コールタイプ

n: 1..5

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Video

値スペース: Audio/Video

Audio: オーディオ コールには、このオプションを選択します。

Video: ビデオ コールには、このオプションを選択します。

## H323 設定

### H323 認証 モード

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: デバイスは H.323 ゲートキーパーに対して自身の認証を試行せず、通常の登録を試行します。

On: 認証が必要なことを H.323 ゲートキーパーから示されると、デバイスはゲートキーパーに対して自身の認証を試みます。デバイスとゲートキーパーの両方で、H323 認証 ログイン名と H323 認証 パスワードの設定を定義する必要があります。

### H323 認証 ログイン名

デバイスは認証のために、H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はデバイスから H.323 ゲートキーパーへの単方向の認証です。つまり、デバイス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、デバイス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 認証パスワード

デバイスは認証のために、H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はデバイスから H.323 ゲートキーパーへの単方向の認証です。つまり、デバイス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、デバイス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 コールセットアップ モード

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

ダイレクト H.323 コールは、H323 コールセットアップ モードが Gatekeeper に設定されている場合も発信できます。

必要なユーザ ロール: ADMIN

デフォルト値: Gatekeeper

値スペース: Direct/Gatekeeper

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

Gatekeeper: デバイスは、H.323 コールを発信するためにゲートキーパーを使用します。このオプションを選択する場合は、H323 ゲートキーパー アドレスも設定する必要があります。

## H323 暗号化 キーサイズ

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

必要なユーザ ロール: ADMIN

デフォルト値: Min1024bit

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

Max1024bit: 最大サイズは 1024 ビットです。

Min1024bit: 最小サイズは 1024 ビットです。

Min2048bit: 最小サイズは 2048 ビットです。

## H323 ゲートキーパー アドレス

ゲートキーパーの IP アドレスを定義します。H323 コールセットアップ モードを 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 H323エイリアス 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デバイス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 Alias E.164 のアドレス。使用できる文字は、0 ~ 9、\*、# です。

## H323 H323エイリアス ID

H.323 エイリアス ID を定義します。この ID は、H.323 ゲートキーパーでデバイスのアドレス指定に使用され、コール リストに表示されます。

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, 49)

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

## H323 NAT モード

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、外部のビデオ会議デバイスに接続されたときの音声またはビデオの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デバイスが決定します。これにより、LAN 上のデバイス、または WAN のデバイス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: デバイスは、実際の IP アドレスをシグナリングします。

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

## H323 NAT アドレス

NAT 対応ルータの外部/グローバル IP アドレスを定義します。ルータに送信されるパケットは、ビデオ会議デバイス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、次のポートはビデオ会議デバイスの 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 ポート割り当て

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

必要なユーザ ロール: ADMIN

デフォルト値: Dynamic

値スペース: Dynamic/Static

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

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

## HttpClient 設定

### HttpClient モード

HTTP(S) 要求および応答を使用する外部 HTTP(S) サーバとのコミュニケーションを許可または禁止します。

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: ビデオ会議デバイスは外部 HTTP(S) サーバと通信できません。

On: ビデオ会議デバイスは外部 HTTP(S) サーバと通信できます。

### HttpClient HTTPを許可

HttpClient モード の設定は、外部 HTTPs サーバとの通信を許可または禁止するために使用されません。モード設定では HTTP と HTTPS の区別をしていません。HTTP の使用を許可または禁止するには、HttpClient HTTPを許可設定を使用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: True

値スペース: False/True

False: ビデオ会議デバイスは、HTTPS のみで通信できます。

True: ビデオ会議デバイスは HTTPS と HTTP の両方で通信できます。

### HttpClient 安全でないHTTPSを許可

サーバの証明書を最初に確認せずに、HTTPS を使用したサーバとの通信をビデオ会議デバイスに許可するかどうかを選択できます。

デバイスによる証明書検証プロセスのスキップを許可する設定になっていても、自動的にスキップされません。証明書検証なしでデータをサーバで交換するには AllowInsecureHTTPS パラメータを各 xCommand HttpClient コマンドで具体的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: False

値スペース: False/True

False: デバイスは常に、HTTPS サーバに有効な証明書があるかどうかを確認します。証明書の検証に失敗した場合、サーバとの通信は行われません。

True: デバイスは、サーバと通信する前に証明書検証プロセスをスキップできます。

### HttpClient Http プロキシの使用

サービスの通信に HTTP プロキシを使用するかどうかを指定できるように、いくつかの [Http プロキシの使用 (UseHttpProxy) ] 設定が用意されています。[HttpClient Httpプロキシの使用 (HttpClient UseHttpProxy) ] 設定は、HttpClient コマンドを使用するマクロおよび任意の HTTP(S) リクエストに適用されます。

この設定を有効にするには、[ネットワークサービス HTTP プロキシ (NetworkServices HTTP Proxy) ] 設定を使用して、HTTP、HTTPS、および WebSocket トラフィック用のプロキシサーバをセットアップする必要があります。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: サーバとの直接通信をセットアップします (プロキシを使用しません)。

On: プロキシ経由の通信をセットアップします。

## HTTP フィードバック設定

### HttpFeedback Tls 検証

この設定は、ビデオ会議デバイスが任意の HTTPS 通信のために HTTPS サーバに接続するときに適用されます (HTTP クライアントの POST/PUT/PATCH/GET/DELETE コマンドを参照してください)。電話帳、プロビジョニング、および外部ロギング サーバについては、電話帳 サーバ [1] Tls 検証、プロビジョニング Tls 検証およびロギング 外部 Tls 検証の設定を参照してください。

デバイスと HTTPS サーバ間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (ブレイクストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

一般に、HTTPS 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。このルールには次の 2 つの例外があります。1) 互換性の理由で、CUCM に登録されているデバイスの最小 TLS バージョンは 1.0 です。2) Webex クラウド サービスに登録されているデバイスは、常にバージョン 1.2 を使用します。

注: アップグレード後にデバイスが初期設定にリセットされておらず、従来のネットワークサービス HTTPS サーバ証明書検証設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

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: デバイスは HTTPS サーバの証明書を確認しません。

On: デバイスは、HTTPS サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

### HttpFeedback Http プロキシの使用

サービスの通信に HTTP プロキシを使用するかどうかを指定できるように、いくつかの [Http プロキシの使用 (UseHttpProxy)] 設定が用意されています。[HttpFeedback Http プロキシの使用 (HttpFeedback UseHttpProxy)] 設定は、ビデオデバイスから送信されたフィードバックに適用されます。

この設定を有効にするには、[ネットワークサービス HTTP プロキシ (NetworkServices HTTP Proxy)] 設定を使用して、HTTP、HTTPS、および WebSocket トラフィック用のプロキシサーバをセットアップする必要があります。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: サーバとの直接通信をセットアップします (プロキシを使用しません)。

On: プロキシ経由の通信をセットアップします。

## ロギングの設定

### ロギング クラウドアップロード モード

このデバイスからクラウドにログをアップロードできるようにするかどうかを指定します。

有効にした場合、デバイスでは、ビデオデバイスと Control Hub のユーザインターフェイスに [ログのアップロード (Upload Logs)] ボタンが表示されます。

[ログのアップロード (Upload Logs)] ボタンを押すと、デバイスログが収集され、個人を特定できる情報がフィルタ処理されて、クラウドにアップロードされます。管理者は、管理ページからログにアクセスできます。

デバイスは、Webex クラウドサービスに登録されているか、オンプレミスサービスに登録されて Webex Edge for Devices にリンク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: [ログのアップロード (Upload Logs)] ボタンを非表示にします。

On: クラウドに登録されたデバイスに [ログのアップロード (Upload Logs)] ボタンを表示します。

### ロギング デバッグ Wifi

このオプションを有効にすると、デバイスは、デバイスとアクセス ポイントの間の Wi-Fi 接続のセットアップやメンテナンスについて詳細な情報を記録します。この機能は、Wi-Fi 接続に問題があった場合のトラブルシューティングに便利です。Wi-Fi 接続が期待通りに動作している場合は、この設定をオフ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

オフ: 基本 Wi-Fi 情報だけをロギング。

オン: Wi-Fi 接続についての大量の情報をロギング。

### ロギング 外部 モード

デバイスログをリモート syslog サーバに保存するかどうかを指定します。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

リモートサーバのアドレスをロギング外部サーバ アドレス設定に入力する必要があります。ロギング外部サーバ ポートセットに記載されていない限り、標準規格 syslog ポートが使用されます。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: デバイス ログはリモート syslog サーバに保存されません。

On: デバイス ログはリモート syslog サーバに保存されます。

### ロギング 外部 プロトコル

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。syslog プロトコル over TLS (Transport Layer Security)、またはプレーンテキストの syslog プロトコルのいずれかを使用できます。syslog プロトコルの詳細については、RFC 5424 を参照してください。

必要なユーザ ロール: ADMIN

デフォルト値: SyslogTLS

値スペース: Syslog/SyslogTLS

Syslog: プレーン テキストの syslog プロトコル。

SyslogTLS: syslog プロトコル over TLS。

### ロギング 外部 サーバ アドレス

リモート syslog サーバのアドレスを指定します。

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 DNS 名。

## ロギング 外部 サーバ ポート

リモート syslog サーバがメッセージをリッスンするポート。0 に設定した場合、デバイスは標準の syslog ポートを使用します。syslog の標準 syslog ポートは 514 で、TLS を使用した syslog の標準 syslog ポートは 6514 です。

必要なユーザ ロール: ADMIN

デフォルト値: 514

値スペース: 整数 (0..65535)

リモート syslog サーバが使用しているポート番号。0 は、デバイスが標準 syslog ポートを使用することを意味します。

## ロギング 外部 Tls 検証

この設定は、ビデオ会議デバイスがリモートの syslog サーバに接続している場合に適用されません。通常のログ作成 (ロギング外部モードの設定を参照) と監査ログ (セキュリティ監査ロギングモードの設定を参照) の両方に適用されます。

デバイスと syslog サーバの間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (ブレインストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

syslog 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。

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: デバイスは syslog サーバの証明書を確認しません。

On: デバイスは、syslog サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

## ロギング 内部 モード

システムログをデバイス (ローカルファイル) に保存するかどうかを指定します。これらは、ログバンドルをデバイスからダウンロードした際に得られるファイルです。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: システム ログはデバイスに保存されません。

On: システム ログはデバイスに保存されます。

## ロギング モード

デバイスのロギング モード (syslog サービス) を定義します。無効にすると、syslog サービスが起動せず、システムログと監査ログのほとんどが生成されません。履歴ログと通話履歴は影響を受けません。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: システムのロギング サービスを無効にします。

On: システムのロギング サービスを有効にします。



## マクロ設定

### マクロ モード

マクロによって、ビデオ会議デバイスの一部を自動化できる JavaScript コードのスニペットを記述できます。これによりカスタム動作を作成します。デフォルトではマクロの使用は無効化されていますが、最初にマクロ エディタを開くときにデバイスでのマクロ使用を有効にするかどうか確認を求められます。デバイスのマクロの使用を手動で有効にする場合や、完全に無効にする場合は、この設定を使用します。マクロ エディタ内でのマクロの使用を無効にすることができます。ただし、デバイスがマクロをリセットするたびにマクロが自動的に再び有効化されるため、マクロの実行は永続的に無効にはなりません。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: このデバイス上でのマクロの使用を完全に無効にします。

On: このデバイス上でのマクロの使用を有効にします。

### マクロ 自動スタート

すべてのマクロは、マクロ ランタイムに呼び出され、ビデオ会議デバイスにおいてシングル プロセスで実行します。デフォルトでは実行されている必要がありますが、手動での停止と開始を選択することができます。自動開始が有効化されている場合、デバイスを再起動するときにランタイムは自動的に再び開始されます。

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: デバイスの再起動後、マクロ ランタイムは自動的に開始されません。

On: デバイスの再起動後、マクロ ランタイムは自動的に開始されます。

### マクロ 無応答タイムアウト

マクロは、応答しないコードを検出するために継続的に監視されます。マクロが応答しない状況は、通常はプログラムエラーを示唆するものですが、システムリソースが限られているために発生する場合があります。この値を大きくすると、より長い時間にわたってマクロを終了せずに実行できるようになります。一方、値を小さくすると、問題のあるマクロがシステムリソースを消費するのを抑えることができます。

必要なユーザ ロール: ADMIN

デフォルト値: 5

値スペース: 整数 (0..65535)

応答しないマクロを終了するまでの秒数を設定します。値を 0 にすると、チェックが完全に無効になります。

### マクロ XAPI トランスポート

マクロシステムで使用される xAPI 伝送方式を設定します。

必要なユーザ ロール: ADMIN

デフォルト値: WebSocket

値スペース: TSH/WebSocket

TSH: マクロでの xAPI 伝送方式は t-shell です。

WebSocket: マクロでの xAPI 伝送方式は WebSocket です。

## ネットワーク設定

### ネットワーク [n] DNS DNSSEC モード

n: 1..1

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: ドメイン ネーム システム セキュリティ拡張を無効にします。

On: ドメイン ネーム システム セキュリティ拡張を有効にします。

### ネットワーク [n] DNS ドメイン名

n: 1..1

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。

### ネットワーク [n] DNS サーバ [m] アドレス

n: 1..1

m: 1..3

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

必要なユーザ ロール: admin、user

デフォルト値: ""

値スペース: 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

### ネットワーク [n] IEEE8021X モード

n: 1..1

デバイスは、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。このアクセス コントロールは、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ます。

必要なユーザ ロール: admin、user

デフォルト値: Off

値スペース: Off/On

Off: 802.1X 認証が無効になります。

On: 802.1X 認証が有効になります。

## ネットワーク [n] IEEE8021X Tls 検証

n: 1..1

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 リストをビデオ会議デバイスにアップロードする必要があります。これは、ウェブインターフェイスから実行できます。

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

必要なユーザ ロール: admin、user

デフォルト値: Off

値スペース: Off/On

Off: Off に設定する場合、ローカル CA リストに対するサーバ側 X.509 証明書を確認せずに、TLS 接続が許可されます。これは、デバイスに 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: 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。

## ネットワーク [n] IEEE8021X クライアント証明書の使用

n: 1..1

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 証明書がビデオ会議デバイス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 (ビデオ会議デバイス) はサーバと相互認証 TLS ハンドシェイクを実行します。

## ネットワーク [n] IEEE8021X ID

n: 1..1

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。

## ネットワーク [n] IEEE8021X パスワード

n: 1..1

802.1X 認証用のパスワードを定義します。

必要なユーザ ロール: admin、user

デフォルト値: ""

値スペース: 文字列 (0, 50)

802.1X 認証用のパスワード。

## ネットワーク [n] IEEE8021X 匿名ID

n: 1..1

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。

## ネットワーク [n] IEEE8021X Eap Md5

n: 1..1

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 プロトコルは無効になります。

On: EAP-MD5 プロトコルが有効になります。

## ネットワーク [n] IEEE8021X Eap Ttls

n: 1..1

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

必要なユーザ ロール: admin、user

デフォルト値: On

値スペース: Off/On

Off: EAP-TTLS プロトコルは無効になります。

On: EAP-TTLS プロトコルが有効になります。

## ネットワーク [n] IEEE8021X Eap Tls

n: 1..1

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

必要なユーザ ロール: admin、user

デフォルト値: On

値スペース: Off/On

Off: EAP-TLS プロトコルは無効になります。

On: EAP-TLS プロトコルが有効になります。

## ネットワーク [n] IEEE8021X Eap Peap

n: 1..1

PEAP (Protected Extensible Authentication Protocol) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Microsoft、Cisco 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 プロトコルは無効になります。

On: EAP-PEAP プロトコルが有効になります。

## ネットワーク [n] IP スタック

n: 1..1

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

必要なユーザ ロール: admin、user

デフォルト値: Dual

値スペース: Dual/IPv4/IPv6

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

IPv4: IPv4 に設定すると、デバイスのネットワーク 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、デバイスのネットワーク インターフェイスで IPv6 が使用されます。

## ネットワーク [n] IPv4 割り当て

n: 1..1

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

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

必要なユーザ ロール: admin, user

デフォルト値: DHCP

値スペース: Static/DHCP

Static: アドレスは、ネットワーク IPv4 アドレス、ネットワーク IPv4 ゲートウェイ、ネットワーク IPv4 サブネットマスクの各設定 (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: デバイス 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。

## ネットワーク [n] IPv4 アドレス

n: 1..1

デバイスのスタティック IPv4 ネットワーク アドレスを定義します。ネットワーク [n] IPv4 割り当てが Static に設定されている場合にのみ適用できます。

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0, 64)

有効な IPv4 アドレス。

## ネットワーク [n] IPv4 ゲートウェイ

n: 1..1

IPv4 ネットワーク ゲートウェイ アドレスを定義します。ネットワーク [n] IPv4 割り当てが Static に設定されている場合にのみ適用できます。

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0, 64)

有効な IPv4 アドレス。

## ネットワーク [n] IPv4 サブネットマスク

n: 1..1

IPv4 ネットワークのサブネット マスクを定義します。ネットワーク [n] IPv4 割り当てが Static に設定されている場合にのみ適用できます。

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0, 64)

有効な IPv4 アドレス。

## ネットワーク [n] IPv6 割り当て

n: 1..1

デバイスが IPv6 アドレスおよびデフォルト ゲートウェイ アドレスを取得する方法を定義します。

アドレス割り当てに DHCPv6 を利用する場合は、MAC アドレスによって最後に付加される「01」が、DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール: admin, user

デフォルト値: Autoconf

値スペース: Static/DHCPv6/Autoconf

Static: デバイスおよびゲートウェイの IP アドレスは、ネットワーク IPv6 アドレスおよびネットワーク IPv6 ゲートウェイの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。ネットワーク [n] IPv6 DHCP オプション設定は、どの方法を使用するかを決定します。

DHCPv6: オプションを含むすべての IPv6 アドレスは、DHCPv6 サーバから取得されます。詳細については RFC3315 を参照してください。ネットワーク [n] IPv6 DHCP オプション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 ステータス自動設定を有効にします。詳細については RFC4862 を参照してください。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。ネットワーク [n] IPv6 DHCP オプション設定は、どの方法を使用するかを決定します。

## ネットワーク [n] IPv6 アドレス

n: 1..1

デバイスのスタティック IPv6 ネットワーク アドレスを定義します。ネットワーク IPv6 割り当てが Static に設定されている場合にのみ適用できます。

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0, 64)

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

## ネットワーク [n] IPv6 ゲートウェイ

n: 1..1

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、ネットワーク IPv6 割り当てが 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。

## ネットワーク [n] IPv6 DHCPオプション

n: 1..1

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

必要なユーザ ロール: admin, user

デフォルト値: On

値スペース: Off/On

Off: DHCPv6 サーバからの DHCP オプションの取得を無効にします。

On: 選択した DHCP オプションのセットの DHCPv6 サーバからの取得を有効にします。

## ネットワーク [n] MTU

n: 1..1

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

必要なユーザ ロール: admin, user

デフォルト値: 1500

値スペース: 整数 (576..1500)

MTU の値を設定します (バイト単位)。

## ネットワーク [n] QoS モード

n: 1..1

QoS (Quality of Service) は、ネットワーク内のオーディオ、ビデオ、その他のデータの優先順位を処理する手法です。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 (差別化サービス) は、ネットワークトラフィックを分類して管理するための、シンプルかつスケラブルで粗いメカニズムを指定するネットワーキングアーキテクチャです。これにより、IP ネットワークに QoS 優先順位が割り当てられます。

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: [ネットワーク QoS Diffserv オーディオ (Network QoS Diffserv Audio) ], [ネットワーク QoS Diffserv ビデオ (Network QoS Diffserv Video) ], [ネットワーク QoS Diffserv データ (Network QoS Diffserv Data) ], [ネットワーク QoS Diffserv シグナリング (Network QoS Diffserv Signalling) ], [ネットワーク QoS Diffserv ICMPv6 (Network QoS Diffserv ICMPv6) ], および [ネットワーク QoS Diffserv NTP (Network QoS Diffserv NTP) ] の各設定を使用して、パケットに優先順位が付けられます。

## ネットワーク [n] QoS Diffserv オーディオ

n: 1..1

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

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。DiffServ RFC で推奨されているトラフィッククラスは、0 ~ 63 の 10 進数値にマップされます。オーディオには EF を使用することをお勧めします。EF は 10 進数値 46 で表されます。

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: 46

値スペース: 整数 (0..63)

IP ネットワーク内でのオーディオパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

## ネットワーク [n] QoS Diffserv ビデオ

n: 1..1

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

IP ネットワーク内でビデオ パケットに持たせる優先順位を定義します。プレゼンテーションチャンネル (共有コンテンツ) のパケットも、ビデオパケットのカテゴリに属します。DiffServ RFC で推奨されているトラフィッククラスは、0 ~ 63 の 10 進数値にマップされます。ビデオには AF41 を使用することをお勧めします。AF41 は 10 進数値 34 で表されます。

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: 34

値スペース: 整数 (0..63)

IP ネットワーク内でのビデオパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

## ネットワーク [n] QoS Diffserv データ

n: 1..1

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

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。DiffServ RFC で推奨されているトラフィッククラスは、0 ~ 63 の 10 進数値にマップされます。データには AF41 を使用することをお勧めします。AF41 は 10 進数値 34 で表されます。

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: 34

値スペース: 整数 (0..63)

IP ネットワーク内でのデータパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

## ネットワーク [n] QoS Diffserv シグナリング

n: 1..1

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

IP ネットワーク内でリアルタイム処理に不可欠 (時間依存) であると考えられるシグナリング パケットに持たせる優先順位を定義します。DiffServ RFC で推奨されているトラフィッククラスは、0 ~ 63 の 10 進数値にマップされます。シグナリングには CS3 を使用することをお勧めします。CS3 は 10 進数値の 24 で表されます。

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: 24

値スペース: 整数 (0..63)

IP ネットワーク内でのシグナリングパケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

## ネットワーク [n] QoS Diffserv ICMPv6

n: 1..1

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

IP ネットワーク内で ICMPv6 パケットに持たせる優先順位を定義します。DiffServ RFC で推奨されているトラフィッククラスは、0 ~ 63 の 10 進数値にマップされます。ICMPv6 には 0 を使用することをお勧めします。

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 ネットワーク内での ICMPv6 パケットの優先順位を設定します。0 は「ベスト エフォート」を意味します。

## ネットワーク [n] QoS Diffserv NTP

n: 1..1

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

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。DiffServ RFC で推奨されているトラフィッククラスは、0 ~ 63 の 10 進数値にマップされます。NTP には 0 を使用することをお勧めします。

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 ネットワーク内での NTP パケットの優先順位を設定します。0 は「ベストエフォート」を意味します。

## ネットワーク [n] リモートアクセス 許可

n: 1..1

リモート アクセスで SSH/HTTP/HTTPS からデバイスに許可する IP アドレス (IPv4/IPv6) を定義します。複数の IP アドレスはスペースで区切られます。

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

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0..255)

有効な IPv4 アドレスまたは IPv6 アドレス。

## ネットワーク [n] 速度

n: 1..1

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

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: Auto

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

Auto: リンク速度を自動でネゴシエートします。

10half: 10 Mbps 半二重に強制リンクします。

10full: 10 Mbps 全二重に強制リンクします。

100half: 100 Mbps 半二重に強制リンクします。

100full: 100 Mbps 全二重に強制リンクします。

1000full: 1 Gbps 全二重に強制リンクします。



## ネットワーク [n] トラフィック制御 モード

n: 1..1

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

必要なユーザ ロール: admin、user

デフォルト値: On

値スペース: Off/On

Off: ビデオ パケットをリンク速度で送信します。

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

## ネットワーク [n] VLAN 音声 モード

n: 1..1

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 音声モードが Auto に自動的に設定されます。ネットワークサービス CDP モード設定が 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 は有効になりません。

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

Off: VLAN は有効になりません。

## ネットワーク [n] VLAN 音声

n: 1..1

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

必要なユーザ ロール: admin、user

デフォルト値: 1

値スペース: 整数 (1..4094)

VLAN 音声 ID を設定します。

## ネットワークサービス設定

### ネットワークサービス CDP モード

CDP (Cisco Discovery Protocol) デーモンを有効または無効にします。CDP を有効にすると、デバイス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 を無効にすると、[ネットワーク音声 VLAN モード (Network VLAN Voice Mode) ]:[自動 (Auto) ] 設定は機能しません。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: CDP デーモンは無効です。

On: CDP デーモンは有効です。

### ネットワークサービス H323 モード

デバイスでの H.323 コールの発信を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無効にします。

On: H.323 コールの発信と受信の可能性を有効にします。

### ネットワークサービス HTTP モード

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

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

注: 以前のソフトウェア バージョンから CE9.4 以降にアップグレードされたデバイスについては、アップグレード後に初期設定にリセットされていない場合、デフォルト値は HTTP+HTTPS となります。

必要なユーザ ロール: ADMIN

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

値スペース: Off/HTTP+HTTPS/HTTPS

Off: HTTP や HTTPS によるデバイスへのアクセスを禁止します。

HTTP+HTTPS: HTTP と HTTPS の両方によるデバイスへのアクセスを許可します。

HTTPS: HTTPS によるデバイスへのアクセスを許可し、HTTP によるアクセスを禁止します。

### ネットワーク サービス HTTP プロキシ ログイン名

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

必要なユーザ ロール: admin、user

デフォルト値: ""

値スペース: 文字列 (0, 80)

認証ログイン名。

## ネットワークサービス HTTP プロキシ パスワード

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

必要なユーザ ロール: admin、user

デフォルト値: ""

値スペース: 文字列 (0, 64)

認証パスワード。

## ネットワーク サービス HTTP プロキシ モード

HTTP、HTTPS、および WebSocket トラフィックに対してプロキシサーバを使用するように設定できます。HTTP プロキシは手動でセットアップするか、自動設定 (PACUrl) または完全な自動化 (WPAD) を使用するか、オフにすることができます。

[ネットワークサービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が [オフ (Off)] でない場合は、どのサービスでプロキシを使用するかを、[HttpClient Httpプロキシの使用 (HttpClient UseHttpProxy)]、[HttpFeedback Httpプロキシの使用 (HttpFeedback UseHttpProxy)]、および [Webエンジン Httpプロキシの使用 (WebEngine UseHttpProxy)] の各設定で指定できます。

Cisco Webex Cloud との通信は、[ネットワークサービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode)] が [オフ (Off)] でない限り、常にプロキシ経由で行われます。

プロキシのモードにかかわらず、デバイスと CUCM、MRA (Expressway 経由の CUCM)、TMS との通信にはプロキシは使用されません。

必要なユーザ ロール: admin、user

デフォルト値: Off

値スペース: Manual/Off/PACUrl/WPAD

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

Off: HTTP プロキシ モードがオフになっています。

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

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

## ネットワーク サービス HTTP プロキシ Url

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

必要なユーザ ロール: admin、user

デフォルト値: ""

値スペース: 文字列 (0..255)

HTTP プロキシ サーバの URL。

## ネットワーク サービス HTTP プロキシ PACUrl

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

必要なユーザ ロール: admin、user

デフォルト値: ""

値スペース: 文字列 (0..255)

PAC (プロキシ自動構成) スクリプトの URL。

## ネットワークサービス HTTPS OCSP モード

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

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: OCSP サポートを無効にします。

On: OCSP サポートを有効にします。

## ネットワークサービス 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。

## ネットワークサービス HTTPS サーバ 最小TLSバージョン

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

必要なユーザ ロール: ADMIN

デフォルト値: TLSv1.1

値スペース: TLSv1.1/TLSv1.2

TLSv1.1: TLS バージョン 1.1 以降のサポート。

TLSv1.2: TLS バージョン 1.2 以降のサポート。

## ネットワークサービス HTTPS StrictTransportSecurity

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

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

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

## ネットワークサービス HTTPS クライアント証明書の検証

ビデオ会議デバイスが HTTPS クライアント (Web ブラウザなど) に接続するときに、クライアントは自身を識別するためにビデオ会議デバイス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 のリストがデバイスに事前にアップロードされている必要があります。

## ネットワークサービス NTP モード

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 サーバにデバイスの時刻と日付を同期するために使用されます。時間の更新のために、タイム サーバに定期的に照会します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/Manual/Off

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

Manual: デバイスは、ネットワークサービス NTP サーバ [n] アドレス設定で指定された NTP サーバを使って時間を参照します。

Off: デバイスは NTP サーバを使用しません。ネットワークサービス NTP サーバ [n] アドレス設定は無視されます。

## ネットワークサービス NTP サーバ [n] アドレス

n: 1..3

ネットワークサービス NTP モード Manual に設定された場合、およびネットワークサービス NTP モードが 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。

## ネットワークサービス NTP サーバ [n] キー

n: 1..3

NTP 情報が信頼できるソースからのものであることを確かめるためには、ビデオ会議デバイスは NTP ソースが使用する ID またはキー ペアを知っている必要があります。キーおよび ID それぞれの設定には、ネットワークサービス NTP サーバ [n] キーおよび ネットワークサービス NTP サーバ [n] キーID 設定を使用します。

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, 2045)

NTP ソースが使用する ID またはキーペアの一部であるキー。

## ネットワークサービス NTP サーバ [n] キーID

n: 1..3

NTP 情報が信頼できるソースからのものであることを確かめるためには、ビデオ会議デバイスは NTP ソースが使用する ID またはキー ペアを知っている必要があります。キーおよび ID それぞれの設定には、ネットワークサービス NTP サーバ [n] キー および ネットワークサービス NTP サーバ [n] キーID 設定 設定を使用します。

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, 10)

NTP ソースが使用する ID/キーペアの一部である ID。

## ネットワークサービス NTP サーバ [n] キーアルゴリズム

n: 1..3

NTP サーバが使用する認証ハッシュ機能を選択します。これは、ビデオ会議デバイスが時間メッセージの認証に使用する必要があるものです。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: None/SHA1/SHA256

None: NTPサーバはハッシュ機能を使用しません。

SHA1: NTPサーバは SHA-1 ハッシュ機能を使用します。

SHA256: NTP サーバは SHA-256 ハッシュ機能を使用します (ハッシュ機能の SHA-2 群から)。

## ネットワークサービス SIP モード

デバイスで 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無効にします。

On: SIP コールの発信と受信の可能性を有効にします。

## ネットワークサービス SMTP モード

SMTP (簡易メール転送プロトコル) を使用するようにデバイスを設定して、デバイスから中継用のメールサーバーに電子メールを送信することができます。これは、ユーザーが組織内外の人に電子メールでホワイトボードやプレゼンテーションを送信する場合に必要です。

暗号化通信を使用するように設定されているデバイスでは ([ネットワークサービス SMTP セキュリティ (NetworkServices SMTP Security) ] 設定を参照)、SMTP サーバの証明書が検証された場合にのみ接続が許可されます。証明書チェックを無視することはできません。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

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: SMTP (および電子メール) サポートを無効にします。

On: 電子メールの送信用に SMTP サポートを有効にします。

## ネットワークサービス SMTP サーバ

これは SMTP サーバのアドレスです。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

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。

## ネットワークサービス SMTP ポート

このポートは、デバイスから SMTP サーバへの送信メールに使用されます。

暗号化の設定 (NetworkServices SMTP Security) と SMTP サーバの要件に基づいてポート番号を設定します。デフォルト値は使用しないでください。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

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..65535)

デバイスからの送信電子メールに使用されるポート。

## ネットワークサービス SMTP ユーザー名

これは、SMTP サーバでデバイスを認証するために使用されるクレデンシャルのユーザー名の部分です。この設定は、SMTP サーバによって要求される場合があります。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

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, 80)

有効なユーザ名。

## ネットワークサービス SMTP パスワード

これは、SMTP サーバでデバイスを認証するため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、SMTP サーバによって要求される場合があります。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

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, 64)

有効なパスワード。

## ネットワークシステム SMTP 送信元

このデバイスから電子メールメッセージを送信するときに使用する、メッセージの送信元メールアドレスの名前を指定します。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

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)

SMTP サーバの要件を満たす電子メールアドレス。

## ネットワークサービス SMTP セキュリティ

デバイスと SMTP サーバ間の通信を保護するかどうかと、その方法を選択します。

この設定は、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

必要なユーザ ロール: ADMIN

デフォルト値: StartTls

値スペース: なし (None) /StartTls/Tls

None: 暗号化なしで SMTP サーバに接続します。

StartTls: 最初に暗号化なしで SMTP サーバに接続してから、STARTTLS コマンドを送信して暗号化接続 (TLS) にアップグレードします。

Tls: TLS (トランスポート層セキュリティ) 経由で SMTP に接続します。

## ネットワークサービス SNMP モード

SNMP (簡易ネットワーク管理プロトコル) は、IP ネットワークに接続されているルーター、サーバ、スイッチなどのデバイスの監視と管理を行うために、ネットワーク管理システムによって使用されます。SNMP は、管理対象デバイスの管理データを変数の形で公開します。これにより、デバイスのステータスと設定が表示されます。これらの変数は、管理アプリケーションでリモートから照会したり、場合によっては設定したりできます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Off

値スペース: Off/ReadOnly/ReadWrite

Off: SNMP ネットワーク サービスを無効にします。

ReadOnly: SNMP ネットワーク サービスを照会のみ有効にします。

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。

## ネットワーク サービス SNMP コミュニティ名

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。管理システムからの SNMP 要求に、一致するコミュニティ名 (大文字と小文字の区別あり) が含まれていない場合、そのメッセージは破棄され、ビデオデバイスの SNMP エージェントは応答送信しません。

Cisco TelePresence Management Suite (TMS) を使用している場合は、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。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 50)

SNMP コミュニティ名。

## ネットワークサービス SNMP システム管理者

SNMP サーバで使用できる連絡先情報を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 50)

ビデオデバイスの連絡先情報を表す文字列。



## ネットワークサービス SNMP システムロケーション

SNMP サーバで使用できるロケーション情報を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 50)

ビデオデバイスのロケーション情報を表す文字列。

## ネットワークサービス SNMP モード

SSH (Secure Shell) プロトコルは、ビデオ会議デバイスとローカル コンピュータの間で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 プロトコルは無効になります。

On: SSH プロトコルは有効になります (デフォルト)。

## ネットワークサービス SSH ホストキーアルゴリズム

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

必要なユーザ ロール: ADMIN

デフォルト値: RSA

設定可能な値: ECDSA/RSA/ed25519

ECDSA: ECDSA アルゴリズムを使用します (nist-384p)。

RSA: RSA アルゴリズムを使用します (2048 bits)。

ed25519: ed25519 アルゴリズムを使用します。

## ネットワークサービス SSH 公開キーの許可

Secure Shell (SSH) 公開キー認証をデバイス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。

## ネットワークサービス UPnP モード

UPnP (ユニバーサル プラグ アンド プレイ) を完全に無効にするか、ビデオ会議デバイスがオンになった後または再起動した後に、短時間だけ UPnP を有効にします。

デフォルトでは、ビデオ会議デバイスをオンにするか再起動すると、UPnP が有効になります。その後、ネットワークサービス UPnP タイムアウトの設定で定義されたタイムアウト時間が経過すると、UPnP は自動的に無効になります。

UPnP が有効になると、デバイスはネットワーク上での自身のプレゼンスをアダプタイズします。このアダプタイズによって、タッチ コントローラはビデオ会議デバイスを自動的に検出できるようになります。タッチ コントローラとペアリングするために、手動でデバイスの IP アドレスを入力する必要はありません。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: UPnP は無効になります。ビデオ会議デバイスは自身のプレゼンスをアダプタイズしないため、タッチ コントローラをデバイスとペアリングするためにはデバイスの IP アドレスを手動で入力する必要があります。

On: UPnP は有効になります。ビデオ会議デバイスはタイムアウト期間が経過するまで、自身のプレゼンスをアダプタイズします。



## ネットワークサービス UPnP タイムアウト

デバイスの電源をオンにした後または再起動した後に、UPnP を有効のままにしておく秒数を定義します。この設定を有効にするには、ネットワークサービス UPnP モードを On 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: 600

値スペース: 整数 (0..3600)

範囲: 0 ~ 3600 秒の値を選択します。

## ネットワークサービス UPnP モードを WebSocket

非セキュアおよびセキュアバージョン (ws および wss) の両方で、デバイスの API に WebSocket プロトコルから相互作用することができます。WebSocket は HTTP に結びついているので、HTTP または HTTPS を有効にしてから WebSockets を使用する必要があります (ネットワークサービス HTTP モード設定を参照)。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: FollowHTTPService/Off

FollowHTTPService: HTTP または HTTPS が有効な場合、WebSocket プロトコル経由での通信は許可されます。

Off: WebSocket プロトコル経由での通信は許可されません。

## ネットワークサービス ウェルカムテキスト

SSH でデバイスにログインする際に、ユーザに表示する情報を選択します。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

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

On: ようこそテキストは次のとおりです: &lt;システム名&gt;; 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)

## ネットワークサービス Wifi 許可a

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

このデバイスは次の標準をサポートします: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac。デバイスは次のセキュリティ プロトコルをサポートします: WPA-PSK (AES)、WPA2-PSK (AES)、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP、EAP-MSCHAPv2、EAP-GTC、およびオープン ネットワーク (セキュリティ保護なし)。

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

必要なユーザ ロール: admin, user

デフォルト値: True

値スペース: False/True

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

True: イーサネットと Wi-Fi の両方を使用できます。

## ネットワーク サービス WiFi 有効

デバイスが Wi-Fi 経由でのネットワーク接続を許可されている場合 (NetworkServices WIFI Allowed 設定を参照)、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 の両方を同時に使用することはできません。Wi-Fi を設定するときにイーサネット ケーブルが接続されている場合、そのイーサネット ケーブルを抜かないと続行できません。Wi-Fi に接続している最中にイーサネット ケーブルを接続すると、イーサネットが優先されます。イーサネット ケーブルを抜いた場合、前回接続した Wi-Fi ネットワークが使用可能であれば、デバイスはそのネットワークに自動的に接続します。

必要なユーザ ロール: admin, user

デフォルト値: True

値スペース: False/True

False: Wi-Fi は無効になります。

True: Wi-Fi が有効になります。

## ネットワークサービス XMLAPI モード

デバイスの XML API を有効化または無効化します。セキュリティ上の理由からこれを無効にできません。XML API を無効化にすると、TMS などによるリモート管理機能が制限され、デバイスに接続できなくなります。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: XML API は無効になります。

On: XML API は有効になります。

## 周辺機器の設定

### 周辺機器 入力デバイス モード

USB キーボードまたはワイヤレスリモート制御などのサードパーティ入力デバイスの、USB ドングルとの使用を許可するかどうかを定義します。入力デバイスはそれ自体を USB キーボードとしてアダプタサイズする必要があります。ご自身で、キークリックに対する応答として行うアクションを定義して実装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: Off

値スペース: Off/On

Off: サードパーティ入力デバイスは許可されません。

On: サードパーティ製の USB 入力デバイスを使用して、ビデオ会議デバイスの特定の機能を制御できます。

### 周辺機器 ペアリング Ciscoタッチパネル Emcレジリエンス

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: EMC レジリエンスモードは無効になります。

On: EMC レジリエンスモードは有効になります。

### 周辺機器 ペアリング Ciscoタッチパネル リモートペアリング

ビデオ会議デバイスのユーザインターフェイスとして Cisco Touch 10 (タッチパネル) を使用するには、Touch 10 をデバイスに直接接続するか、LAN 経由でデバイスとペアリングする必要があります。後者はリモート ペアリングと呼ばれます。

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

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

[オフ (Off)]: Touch 10 のリモート ペアリングは許可されません。

On: タッチ 10 リモート ペアリングは許可されます。

### 周辺機器 プロファイル カメラ

ビデオ会議デバイスに接続されることが予想されるタッチ パネルの数を定義します。この情報はデバイスの診断サービスで使用します。接続されたカメラの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Minimum1

値スペース: NotSet/Minimum1/0/1/2/3/4/5/6/7

NotSet: カメラの確認は実行されません。

Minimum1: 少なくとも 1 台のカメラがデバイスに接続されている必要があります。

0 ~ 7: デバイスへの接続が予想されるカメラの数を選択します。

## 周辺機器 プロファイル 制御システム

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

1 に設定する場合、xCommand Peripherals Pair コマンドおよび HeartBeat コマンドを使用して、制御システムからビデオ会議デバイスにハート ビートを送信する必要があります。これに失敗すると、ビデオ会議デバイスは、コントロール システムへの接続が失われたことを示す警告を表示します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: NotSet

値スペース: 1/NotSet

1: 1 つのサードパーティ製コントロール システムをデバイスに接続する必要があります。

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

## 周辺機器 プロファイル タッチパネル

デバイスに接続する予定の Cisco Touch コントローラの数 を定義します。この情報はデバイスの診断サービスで使用します。接続されたタッチ コントローラの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Minimum1

値スペース: NotSet/Minimum1/0/1/2/3/4/5

NotSet: タッチ パネル チェックは実行されません。

Minimum1: 少なくとも 1 台の Cisco Touch コントローラがデバイスに接続されている必要があります。

0 ~ 5: デバイスへの接続が予想される Touch コントローラの数を選択します。公式にサポートされるシスコ タッチ コントローラは、1 台のみであることに注意してください。

## 電話帳の設定

### Phonebook サーバ [n] ID

n: 1..1

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。

### 電話帳 サーバ [n] ページネーション

n: 1..1

電話帳サーバがページネーション(ウェルカムページ)に対応するかどうかを定義します。ページネーションとはサーバが連続検索に対応しているかどうか、さらにこれらの検索がオフセットに関連付けられるかどうかを意味します。これにより、ユーザインターフェイスは完全な検索結果を得るために必要な可能な限り多くの連続検索を実行できます。

ページネーションが無効の場合、デバイスは検索を 1 度行い、最大 100 エントリを検索結果に返します。それ以上の検索結果をさらにスクロールすることはできません。

必要なユーザ ロール: ADMIN

デフォルト値: Enabled

値スペース: Disabled/Enabled

Disabled: 電話帳サーバはページネーションに対応しません。デバイスは 1 回の検索を実行します。検索結果の最大エントリ数は 100 です。

Enabled: 電話帳サーバはページネーションに対応しています。

### 電話帳 サーバ [n] TLS 検証

この設定は、ビデオ会議デバイスが HTTPS 経由で外部の電話帳サーバに接続するときに適用されます。

デバイスと HTTPS サーバ間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (ブレインストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

一般に、HTTPS 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。このルールには次の 2 つの例外があります。1) 互換性の理由で、CUCM に登録されているデバイスの最小 TLS バージョンは 1.0 です。2) Webex クラウド サービスに登録されているデバイスは、常にバージョン 1.2 を使用します。

注: アップグレード後にデバイスが初期設定にリセットされておらず、従来のネットワークサービス HTTPS サーバ証明書検証設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

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: デバイスは HTTPS サーバの証明書を確認しません。

On: デバイスは、HTTPS サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

## 電話帳 サーバ [n] タイプ

n: 1..1

電話帳サーバの種類を選択します。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/CUCM/Spark/TMS/VCS

Off: 電話帳を使用しません。

CUCM: 電話帳が Cisco Unified Communications Manager 上に配置されます。

Spark: 電話帳が Cisco Webex クラウドサービス内に配置されます。

TMS: 電話帳が Cisco TelePresence Management Suite サーバ上に配置されます。

VCS: 電話帳が Cisco TelePresence Video Communication Server 上に配置されます。

## 電話帳サーバ [n] URL

n: 1..1

外部電話帳サーバへのアドレス (URL) を定義します。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0..255)

外部電話帳サーバの有効なアドレス (URL)。

## プロビジョニング設定

### プロビジョニング 接続

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

必要なユーザ ロール: admin, user

デフォルト値: Auto

値スペース: Internal/External/Auto

Internal: 内部コンフィギュレーションを要求します。

External: 外部コンフィギュレーションを要求します。

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

### プロビジョニング CUCM コール管理レコード

CUCM コール管理レコードのサポート。このソフトウェアバージョンでは、この機能は実験的なものです。

必要なユーザ ロール: admin, user

デフォルト値: Off

値スペース: Off/On

On: CUCM コール管理レコードのサポートを有効にします。

Off: CUCM コール管理レコードのサポートを無効にします。

### プロビジョニング 外部マネージャ アドレス

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

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

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

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

### プロビジョニング 外部マネージャ 代替アドレス

デバイスが Cisco Unified Communications Manager (CUCM) でプロビジョニングされており、冗長構成として代替の CUCM が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。メインの CUCM が使用できない場合、デバイスは代替 CUCM でプロビジョニングされます。メインの CUCM が再び使用可能になると、デバイスはこの 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。

## プロビジョニング 外部マネージャ プロトコル

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

選択したプロトコルは、ネットワークサービス HTTP モードの設定で有効になっている必要があります。

必要なユーザ ロール: admin, user

デフォルト値: HTTP

値スペース: HTTPS/HTTP

HTTPS: HTTPS を介してリクエストを送信します。

HTTP: HTTP を介してリクエストを送信します。

## プロビジョニング 外部マネージャ パス

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

必要なユーザ ロール: admin, user

デフォルト値: ""

値スペース: 文字列 (0..255)

外部のマネージャ システムまたはプロビジョニング システムへの有効なパス。

## プロビジョニング 外部マネージャ ドメイン

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。

## プロビジョニング モード

プロビジョニング システム (外部マネージャ) を使用してデバイスを設定できます。これにより、ビデオ会議のネットワーク管理者は複数のデバイス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/Webex/TMS/VCS

Off: デバイスはプロビジョニング システムによって設定されません。

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

CUCM: CUCM (Cisco Unified Communications Manager) からデバイスに設定をプッシュします。

Edge: CUCM (Cisco Unified Communications Manager) からデバイスに設定をプッシュします。デバイスは Expressway インフラストラクチャを介して CUCM に接続します。Expressway を経由して登録するには、暗号化オプションキーがデバイスにインストールされている必要があります。

Webex: Cisco Webex クラウド サービスからデバイスに設定をプッシュします。Webex クラウドサービスに登録するには、暗号化オプションキーがデバイスにインストールされている必要があります。

TMS: TMS (Cisco TelePresence Management System) からデバイスに設定をプッシュします。

VCS: VCS (Cisco TelePresence Video Communication Server) からデバイスに設定をプッシュします。

## プロビジョニング ログイン名

これは、プロビジョニング サーバでデバイスを認証するために使用されるログイン情報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。



## プロビジョニング パスワード

これは、プロビジョニング サーバでデバイスを認証するため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。

## プロビジョニング TLS 検証

この設定は、ビデオ会議デバイスが HTTPS 経由でプロビジョニング サーバに接続するときに適用されます。

デバイスと HTTPS サーバ間の接続を確立する前に、デバイスは、サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうかを確認します。CA 証明書は、デバイスの CA リスト (ブレイクストールされているリストまたは Web インターフェイスか API を使用して手動でアップロードするリスト) に含める必要があります。

一般に、HTTPS 接続の最小 TLS (Transport Layer Security) のバージョンは 1.1 です。このルールには次の 2 つの例外があります。1) 互換性の理由で、CUCM に登録されているデバイスの最小 TLS バージョンは 1.0 です。2) Webex クラウド サービスに登録されているデバイスは、常にバージョン 1.2 を使用します。

注: アップグレード後にデバイスが初期設定にリセットされておらず、従来のネットワークサービス HTTPS サーバ証明書検証設定が明示的に On に設定されていなかった場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

デバイスが Expressway 経由で Cisco Webex クラウド サービスや CUCM からプロビジョニングされている場合 (MRA またはエッジとも呼ばれます)、この設定に関係なく、常に証明書のチェックが実行されます。

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: デバイスは HTTPS サーバの証明書を確認しません。

On: デバイスは、HTTPS サーバの証明書が信頼できるかどうかを確認します。信頼できない証明書の場合、デバイスとサーバの間の接続は確立されません。

## プロビジョニング WebexEdge

デバイスを Webex Edge for Devices にリンクするかどうかを定義します。リンクしたデバイスには、特定の Webex クラウドサービスへのアクセスが提供されます。

この設定は、オンプレミスサービスに登録されているデバイス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: デバイスは Webex Edge for Devices にリンクされません。

On: デバイスは Webex Edge for Devices にリンクされます。

## プロキシミティの設定

### プロキシミティ 代替ポート 有効

この設定は、[ネットワークサービス HTTP モード (NetworkServices HTTP Mode)] が [HTTP+HTTPS] または [HTTPS.] に設定されている場合にのみ適用されます。

デフォルトでは、プロキシミティ接続は TCP ポート 443 を使用します。この設定を使用すると、ポート 65533 でもプロキシミティ接続が許可されます。

必要なユーザ ロール: ADMIN

デフォルト値: False

値スペース: False/True

False: プロキシミティ接続は常に TCP ポート 443 を使用します。

True: プロキシミティ接続は TCP ポート 443 または 65533 を使用できます。使用されるポートはクライアントによって変わります。

### プロキシミティ モード

[プロキシミティ モード (Proximity Mode)] 設定は、Webex クラウドサービスに登録されているデバイスには効果がありません。クラウド登録デバイスから超音波ペアリングメッセージが送信されないようにするには、[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] を 0 に設定する必要があります。

オンプレミス登録デバイスの場合は、[プロキシミティ モード (Proximity Mode)] 設定により、超音波ペアリングメッセージを出力するかどうかを決定します。デバイスから超音波ペアリングメッセージを出力すると、デバイスが近くにあることをシスココラボレーションクライアントで検知できます。

クライアントを使用するには、少なくとも 1 つのプロキシミティサービスを有効にする必要もあります ([プロキシミティ サービス (Proximity Services)] 設定を参照)。一般的に、すべてのプロキシミティ サービスを有効にすることをお勧めします。

[プロキシミティ モード (Proximity Mode)] 設定と [オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定は、超音波ペアリングメッセージにのみ影響します。超音波の出力をすべて停止するには、[ルーム分析 人の存在の検出 (RoomAnalytics PeoplePresenceDetector)] 設定と [スタンバイ モーション検知ウェイクアップ (Standby WakeupOnMotionDetection)] 設定も [オフ (Off)] 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: On

値スペース: Off/On

Off: シスココラボレーションクライアントはデバイスが近くにあることを検知できません。このため、プロキシミティサービスは使用できません。

On: シスココラボレーションクライアントはデバイスが近くにあることを検知できます。有効になっているプロキシミティサービスを使用できます。

### プロキシミティ サービス コール制御

シスココラボレーション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、シスココラボレーション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、音量調節、コールの終了など)。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには、プロキシミティ モードを 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: シスココラボレーションクライアントからのコール制御が有効になります。

Disabled: シスココラボレーションクライアントからのコール制御が無効になります。

## プロキシミティ サービス コンテンツ共有 クライアントから

シスココラボレーションクライアントからのコンテンツ共有を有効または無効にします。この設定を有効にすると、シスココラボレーションクライアントからのコンテンツをデバイスにワイヤレスで共有できます (ラップトップ画面の共有など)。このサービスはラップトップ (OS X および Windows) でサポートされます。この設定が機能するには、プロキシミティ モードを On にする必要があります。

必要なユーザ ロール: admin、user

デフォルト値: Enabled

値スペース: Enabled/Disabled

Enabled: シスココラボレーションクライアントからのコンテンツ共有が有効になります。

Disabled: シスココラボレーションクライアントからのコンテンツ共有が無効になります。

## プロキシミティ サービス コンテンツ共有 クライアントへ

シスココラボレーションクライアントへのコンテンツ共有を有効または無効にします。有効にすると、シスココラボレーションクライアントはデバイスからプレゼンテーションを受け取ります。詳細を拡大して、以前のコンテンツを表示し、スナップショットを作成できます。このサービスはモバイルデバイス (iOS および Android) でサポートされます。この設定が機能するには、プロキシミティ モードを 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: シスココラボレーションクライアントへのコンテンツ共有が有効になります。

Disabled: シスココラボレーションクライアントへのコンテンツ共有が無効になります。

## ルーム分析設定

### ルーム分析 環境雑音の予測 モード

デバイスは室内の固定周囲ノイズ レベル (背景雑音レベル) を算出することができます。結果は RoomAnalytics AmbientNoise レベル dBA ステータスにレポートされます。新しい周囲ノイズレベルが検出されるとステータスが更新されます。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: Off

値スペース: Off/On

- On: デバイスは固定周囲ノイズ レベルを定期的に予測します。
- Off: デバイスは固定周囲ノイズ レベルを定期的に予測しません。

顔検出を使用して、デバイスが室内にいる人の人数を特定できます。デフォルトでは、デバイスは通話中のときまたはセルフ ビューに画像を表示したときのみ人数を数えます。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: Off

値スペース: Off/On

- Off: デバイスは、デバイスが通話中のときまたはセルフ ビューがオンのときのみ、人数を数えます。
- On: デバイスは、デバイスがスタンバイ モードでない限り、人数を数えます。セルフ ビューがオフであっても、これは非通話中の人数を含みます。

### ルーム分析 人の存在の検出

デバイスは、人が室内に存在しているかどうかを確認し、その結果を [ルーム分析 人の存在 (RoomAnalytics PeoplePresence)] のステータスにレポートすることができます。この機能は、超音波に基づいています。詳細については、ステータスの説明を参照してください。

この設定と [スタンバイ モーション検知ウェイクアップ (Standby WakeupOnMotionDetection)] 設定の両方が [オフ (Off)] になっている場合、人の存在を検出するための超音波信号は出力されません。[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定と [プロキシミティ モード (Proximity Mode)] 設定は、人の存在の検出には影響しません。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: Off

値スペース: Off/On

- Off: ユーザの存在に関する情報は、デバイスのステータスで報告されません。
- On: ユーザの存在に関する情報は、デバイスのステータスで報告されます。

## ルームリセットの設定

### RoomReset control

この設定は、コントロールシステムまたはマクロの使用に対するものです。マクロによって、ビデオ会議デバイスの一部を自動化できる JavaScript コードのスニペットを記述できます。これによりカスタム動作を作成します。

ルームが数分に渡って待機状態になると、ビデオ会議デバイスは、ルームがリセット可能な状態であることを示すイベントを送信できます。

この設定が有効である場合に送られるイベントは次の通りです：

```
*e RoomReset SecondsToReset: 30
** end
*e RoomReset Reset
** end
```

必要なユーザ ロール: ADMIN

デフォルト値: On

設定可能な値: CameraPositionsOnly/Off/On

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

Off: ルームリセットイベントは送信されません。

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

## RTP 設定

### RTP ポート 範囲 開始

RTP ポート範囲の最初のポートを定義します。

デフォルトでは、デバイスは RTP および RTCP メディア データに 2326 ~ 2487 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100、RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

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

設定の変更内容は、次の発信から有効になります。

必要なユーザ ロール: ADMIN

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。この値は偶数にする必要があります。

### RTP ポート 範囲 終了

RTP ポート範囲の最後のポートを定義します。

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

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

設定の変更内容は、次の発信から有効になります。

必要なユーザ ロール: ADMIN

デフォルト値: 2487

値スペース: 整数 (1121 ~ 65535)

RTP ポート範囲内で最後のポートを設定します。この値は奇数にする必要があります。偶数値を入力すると、自動的に 1 が加算されます。

### RTP ビデオ ポート 範囲 開始

RTP ビデオ ポート範囲の最初のポートを定義します。

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

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

設定の変更内容は、次の発信から有効になります。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数 (0, 1024..65454)

RTP ビデオ ポート範囲の最初のポートを設定します。

### RTP ビデオ ポート 範囲 終了

RTP ビデオ ポート範囲の最後のポートを定義します。

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

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

設定の変更内容は、次の発信から有効になります。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数 (0, 1024..65535)

RTP ビデオ ポート範囲の最後のポートを設定します。

## セキュリティ設定

### セキュリティ 監査 ログイン モード

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。ログインモード設定がオフに設定されている場合、この設定には効果がありません。

External モードまたは ExternalSecure モードを使用する場合は、セキュリティ監査サーバアドレス設定に監査サーバのアドレスを入力する必要があります。

必要なユーザ ロール: AUDIT

デフォルト値: Internal

設定可能な値: External/ExternalSecure/Internal/Off

External: デバイスは外部監査 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: デバイスは、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 ファイルが Web インターフェイスからデバイスにアップロードされている必要があります。CA のリストの証明書の common\_name パラメータは syslog サーバの IP アドレスまたは DNS 名と一致する必要があり、セキュア TCP サーバでセキュア (TLS) TCP syslog メッセージをリッスンするように設定される必要があります。

Internal: デバイスは内部ログに監査ログを記録し、満杯になるとログをローテーションします。

Off: 監査ログインは実行されません。

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、セキュリティ監査ログインモードが 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、デバイスはリポートし、停止期間が経過するまでは監査役だけが装置の操作を許可されます。停止状態が過ぎ去ると、監査ログは syslog サーバに再スプールされます。ネットワークの違反 (物理リンクなし)、動作中の外 Syslog サーバが存在しない (または syslog への間違ったアドレスまたはポート)、TLS 認証が失敗した (使用中の場合)、ローカル バックアップ (再スプール) ログがいっぱいになった、などの停止状態があります。

Ignore: デバイスは通常の動作を続行し、満杯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。

### セキュリティ 監査 サーバ アドレス

監査ログの送信先である syslog サーバの IP アドレスまたは DNS 名を設定します。この設定は、セキュリティ監査ログインモードが 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、IPv6 アドレス、または DNS 名。

### セキュリティ 監査 サーバ ポート

監査ログは syslog サーバに送信されます。デバイス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、セキュリティ 監査 サーバ ポート割り当てがマニュアル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: 514

値スペース: 整数 (0..65535)

監査サーバのポートを設定します。



## セキュリティ 監査 サーバ ポート割り当て

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、セキュリティ監査ロギング モードが External または ExternalSecure に設定されている場合のみ関連します。使用しているポート番号を確認するために、セキュリティ 監査 サーバ ポート状態をチェックできます。Web インターフェイスで [セットアップ (Setup)] &gt; [ステータス (Status)] に移動するか、コマンドライン インターフェイスの場合はコマンド xStatus Security Audit Server Port を実行します。

必要なユーザ ロール: AUDIT

デフォルト値: Auto

値スペース: Auto/Manual

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

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

## セキュリティ Fips モード

必要に応じて、デバイスを FIPS モードに設定することができます (連邦情報処理標準 (FIPS) 140-3、「暗号化モジュールのセキュリティ要件」)。FIPS モードでは、リモートサポート ユーザは利用できません。また、デバイスと HTTP プロキシ間のダイジェストアクセス認証はサポートされません。これは、ダイジェストアクセス認証で使用される MD5 暗号化ハッシュが FIPS で許可されていないためです。この最後の制限は、Webex 登録デバイスにのみ影響します。これは HTTP プロキシが Webex ソリューションにのみ使用されるためです。

FIPS モードでは、HTTPS のみを許可し、SNMP や IEEE8021X に切り替えないようにする (デフォルト値を保持する) 必要があります。

この設定に対する変更を完全に反映させるには、デバイスを再起動する必要があります。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: デバイスは FIPS モードではありません。

On: デバイスが FIPS モードになります。

## セキュリティ セッション ログイン失敗時のロックアウト時間

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

この設定に対する変更を反映するには、デバイスを再起動します。

必要なユーザ ロール: ADMIN

デフォルト値: 60

値スペース: 整数 (0..10000)

ロックアウト時間 (分) を設定します。

## セキュリティ セッション非アクティブタイムアウト

ユーザが Web または SSH セッションから自動的にログアウトされるまでに、デバイスがユーザの非アクティブ状態をどれくらいの時間受け入れるかを定義します。

この設定に対する変更を反映するには、デバイスを再起動します。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数 (0..10000)

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

## セキュリティ セッション ログイン失敗の最大数

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

この設定に対する変更を反映するには、デバイスを再起動します。

必要なユーザ ロール: ADMIN

デフォルト値: 0

値スペース: 整数 (0..10)

ユーザ 1 人あたりの失敗できるログイン試行の最高回数を設定します。



## セキュリティ セッション ユーザあたりの最大セッション数

ユーザ 1 人あたりの最大同時セッション数は 20 セッションです。

必要なユーザ ロール: ADMIN

デフォルト値: 20

値スペース: 整数 (1..20)

ユーザ 1 人あたりの最大同時セッション数を設定します。

## セキュリティ セッション 最大総セッション数

同時セッションの合計最大数は 20 セッションです。

必要なユーザ ロール: ADMIN

デフォルト値: 20

値スペース: 整数 (1..20)

同時セッションの合計最大数を設定します。

## セキュリティ セッション 最後のログオンを表示

SSH を使用してデバイスにログインすると、前回ログインに成功したセッションのユーザ ID、時刻および日付が表示されます。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

On: 最後のセッションに関する情報を表示します。

Off: 最後のセッションに関する情報を表示しません。

## シリアルポート設定

### シリアルポート モード

シリアル ポートを有効/無効にします。この設定はすべてのシリアルポートに適用されます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: シリアル通信が無効になります。

On: シリアル通信が有効になります。

### シリアルポート ボーレート

シリアルポートのボーレート (データ転送速度) を設定します。

シリアル ポートの他の接続パラメータは次の通りです。データ ビット: 8。パリティ: なし。ストップ ビット: 1。フロー制御: なし。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 115200

値スペース: 115200

リストからボーレートを選択します (ビット/秒)。

### シリアルポート ログインが必要

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。デバイスに複数のシリアルポートがある場合、この設定はすべてのシリアルポートに適用されます。

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: ユーザはログインせずに、シリアル ポート経由でデバイスにアクセスできます。

On: シリアル ポート経由でデバイスに接続するときに、ログインが必要です。

## SIP 設定

### SIP ANAT

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

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: ANAT を無効にします。

On: ANAT を有効にします。

### SIP 認証ユーザ名

これは、SIP プロキシへの認証に使用されるログイン情報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 認証パスワード

これは、SIP プロキシへの認証に使用されるログイン情報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 デフォルトトランスポート

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/TCP/Tls/UDP

TCP: デバイスはデフォルトの転送方法として常に TCP を使用します。

UDP: デバイスはデフォルトの転送方法として常に UDP を使用します。

Tls: デバイス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 リストをデバイスにアップロードできます。該当する CA リストがデバイスにない場合は、ディフィーヘルマン匿名認証が使用されます。

Auto: デバイスは、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 表示名

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

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0, 550)

SIP URI の代わりに表示する名前。

## SIP Ice デフォルト候補

ICE プロトコルには、使用するメディア ルートを決定するまでの時間（最大で通話開始から 5 秒間）が必要となります。この時間内に、この設定に従って、デバイスのメディアがデフォルトの候補に送信されます。

必要なユーザ ロール: ADMIN

デフォルト値: Host

値スペース: Host/Rfx/Relay

Host: メディアをデバイスのプライベート IP アドレスに送信します。

Rfx: TURN サーバが認識しているデバイスのパブリック IP アドレスにメディアを送信します。

Relay: TURN サーバで割り当てられた IP アドレスおよびポートにメディアを送信します。

## SIP Ice モード

ICE (Interactive Connectivity Establishment, RFC 5245) は、最適化されたメディア パスの検出にデバイスで使用できる 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デバイス間で常に確保されます。メディアパスを設定すると、最初に STUN (Session Traversal Utilities for NAT) メッセージが交換されます。

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 サーバが提供されている場合は ICE が有効になり、提供されていない場合は ICE が無効になります。

Off: ICE が無効になります。

On: ICE が有効になります。

## SIP 回線

Cisco Unified Communications Manager (CUCM) に登録すると、デバイスを共有電話の一部にできます。これは、複数のデバイスが同じディレクトリ番号を共有することを意味します。RFC 4235 で規定されているように、同じ番号を共有する各デバイスは、ライン上のもう一方のアピアランスからステータスを受け取ります。

共有回線はデバイスではなく 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デバイスにプッシュします。

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: デバイスは共有電話の一部であるため、ディレクトリ番号を他のデバイスと共有します。

Private: このデバイスは共有電話の一部ではありません。

## SIP リッスンポート

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、デバイスは SIP プロキシ (CUCM または VCS) を介してのみ到達可能になります。セキュリティ対策として、デバイスが SIP プロキシに設定されている場合は SIP ListenPort をオフにすべきです。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Auto/Off/On

Auto: デバイスが SIP プロキシに登録されている場合、SIP TCP/UDP ポートでの着信接続に対するリスニングは自動的にオフになります。それ以外の場合は、オンになります。

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 メールボックス

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 最小 TLS バージョン

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

必要なユーザ ロール: ADMIN

デフォルト値: TLSv1.0

値スペース: TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0: TLS バージョン 1.0 以上をサポートします。

TLSv1.1: TLS バージョン 1.1 以上をサポートします。

TLSv1.2: TLS バージョン 1.2 以上をサポートします。

## SIP 優先IPシグナリング

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)。ネットワーク IP スタックおよび会議 通信プロトコルIPスタックの両方が 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 プロキシ [n] アドレス

n: 1..4

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 TLS検証

SIP TLS 経由の接続を確認する前に、デバイスは、信頼できる認証局 (CA) がピアの証明書に署名しているかどうかを確認します。CA が CA リストに含まれており、Web インターフェイスまたは API を使用して手動でデバイスにアップロードされている必要があります。プレインストールされている証明書リストは、SIP TLS 接続の証明書の検証には使用されません。

注: アップグレード後にデバイスが初期設定にリセットされておらず、この設定が明示的に On に設定されていない場合、CE 9.8 以前のソフトウェア バージョンから CE 9.9 以降にアップグレードされたデバイスではこの値が Off に設定されます。

どの TLS バージョンを許可するかを指定するには、SIP 最小 TLS バージョン設定を使用します。

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: デバイスはピアの証明書を確認しません。いずれにしても SIP TLS 接続が確立されます。

On: デバイスは、ピアの証明書が信頼できるかどうかを確認します。信頼できない場合、SIP TLS 接続は確立されません。

## SIP Turn 検出モード

検出モードを定義し、DNS で利用可能な TURN サーバの検索に対してアプリケーションを有効/無効にします。コールを発信する前に、デバイスはポート割り当てが可能かどうかを確認します。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: 検出モードを無効にします。

On: On に設定すると、デバイスは 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 DropRfIx

DropRfIx は、リモート デバイスが同じネットワークにない場合に限り、TURN リレー経由でデバイス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: DropRfIx を無効にします。

On: リモート デバイスが別のネットワークにある場合、デバイスは TURN リレー経由でメディアを強制します。

## SIP Turn サーバ

TURN (Traversal Using Relay NAT) サーバのアドレスを定義します。これはメディア リレー フォールバックとして使用され、また、デバイス固有のパブリック 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 ユーザ名

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 パスワード

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 タイプ

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

必要なユーザ ロール: ADMIN

デフォルト値: Standard

値スペース: Standard/Cisco

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

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

## SIP URI

SIP URI (Uniform Resource Identifier) は、デバイスの識別に使用されるアドレスです。URI が登録され、SIP サービスによりデバイス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)。

## スタンバイ設定

### スタンバイ ブートアクション

ビデオ会議デバイスの再起動後のカメラの位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: DefaultCameraPosition

値スペース: None/DefaultCameraPosition/RestoreCameraPosition

None: アクションはありません。

RestoreCameraPosition: ビデオ会議デバイスを再起動すると、カメラは再起動前の位置に戻ります。

DefaultCameraPosition: ビデオ会議デバイスを再起動すると、カメラは工場出荷時のデフォルトの位置に移動します。

### スタンバイ制御

デバイスがスタンバイ 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、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: デバイスはスタンバイ モードを開始しません。

On: Standby Delay がタイムアウトすると、デバイスはスタンバイ モードを開始します。

### スタンバイ遅延

スタンバイ モードに入るまでにデバイスがアイドル モードのまま経過する時間の長さ (分単位) を定義します。[スタンバイ制御 (Standby Control)] が有効である必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 10

値スペース: 整数 (1..480)

スタンバイ遅延 (分) を設定します。

### スタンバイ サイネージ オーディオ

デフォルトでは、デバイスは、Web ページに音声がある場合でも、デジタル信号モードで音声を再生しません。この設定を使用して、デフォルトの動作を上書きすることができます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Off

値スペース: Off/On

Off: デバイスは、Web ページで音声を再生しません。

On: Web ページに音声が含まれている場合、デバイスは音声を再生します。音量は、デバイスの音量設定に従います。

### スタンバイ サイネージ 対話モード

デフォルトでは、ユーザーがデジタル サイネージの Web ページを操作することはできません。この設定を使用すると、Web ページとの対話機能を有効にすることができます。

対話モードは、Room Kit Mini では通常は使用できず、Room Kit Mini を Samsung Flip (Webex on Flip) と共に使っている場合にのみ使用できます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 非インタラクティブ (NonInteractive)

値スペース: インタラクティブ (Interactive) /非インタラクティブ (NonInteractive)

Interactive: Web ページを操作することができます。

NonInteractive: Web ページを操作することはできません。



## スタンバイ サイネージ モード

URL (Web ページ) からのコンテンツは、従来のハーフ ウェイク バックグラウンド イメージおよび情報を置き換えることができます。この機能は、「デジタル サイネージ」と呼ばれます。

デジタル サイネージを使用すると、デバイスが通常の方法でスタンバイ状態に入ることを防止できません。そのため、スタンバイ遅延の設定は、デバイスがスタンバイ状態になるまでのデジタルサイネージの表示時間を決定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Off

値スペース: Off/On

Off: デバイスでデジタル サイネージが有効になっていません。

On: Web エンジン モード設定がオンになっている場合、デジタル サイネージが有効化され、デバイスのハーフ ウェイク モードに置き換えられます。

## スタンバイ サイネージ 更新間隔

この設定を使用して、Web ページを定期的に更新することができます。これは、Web ページ自体を更新できない場合に便利です。更新間隔をインタラクティブ モードで設定することは推奨されません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 0

値スペース: 整数 (0 ~ 1440)

各 Web ページの更新間隔を秒数で表示します。値が 0 の場合、Web ページは強制的に更新されなくなります。

## スタンバイ サイネージ Url

画面 (デジタル サイネージ) に表示する Web ページの URL を設定します。URL の長さが 0 の場合、デバイスに通常のハーフ ウェイク モードが保持されます。URL が機能していない場合、デバイスは通常のハーフ ウェイク モードを保持し、診断メッセージが発行されます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 2000)

Web ページの URL。

## スタンバイ スタンバイアクション

スタンバイ モードに入るときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: PrivacyPosition

値スペース: None/PrivacyPosition

None: アクションはありません。

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

## スタンバイ ウェイクアップアクション

スタンバイ モードを抜けるときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: RestoreCameraPosition

値スペース: None/RestoreCameraPosition/DefaultCameraPosition

None: アクションはありません。

RestoreCameraPosition: ビデオ会議デバイスがスタンバイ状態から復帰すると、カメラはスタンバイ前の位置に戻ります。

DefaultCameraPosition: ビデオ会議デバイスがスタンバイ状態になると、カメラは工場出荷時のデフォルトの位置に移動します。

## スタンバイ モーション検知ウェイクアップ

モーション検知時の自動ウェイクアップは、人が入室したことをデバイスで検出できるようにする機能です。この機能は、超音波検出に基づいています。

この設定と [ルーム分析 人の存在の検出 (RoomAnalytics PeoplePresenceDetector)] 設定の両方が [オフ (Off)] になっている場合、モーション検知用の超音波信号は出力されません。[オーディオ 超音波 最大音量 (Audio Ultrasound MaxVolume)] 設定と [プロキシミティ モード (Proximity Mode)] 設定は、モーション検知には影響しません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: モーション検知ウェイクアップが無効になります。

On: 人が部屋に入ると、デバイスが自動的にスタンバイから復帰します。

## システムユニット設定

### システムユニット名

デバイス名を定義します。デバイスが SNMP エージェントとして機能している場合に、デバイス名は DHCP リクエストでホスト名として送信されます。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0, 50)

デバイス名を定義します。

### 高度なシステムユニット クラッシュレポート

デバイスがクラッシュすると、デバイスは解析のためにシスコ自動クラッシュ レポート ツール (ACR) にログを自動送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: ACR ツールは標準的なログ解析を実行します。

On: ACR ツールは高度なログ解析を実行します。

### システムユニット クラッシュレポート モード

デバイスがクラッシュすると、デバイスは解析のためにシスコ自動クラッシュ レポート ツール (ACR) にログを自動送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: ACR ツールにログは送信されません。

On: ACR ツールにログは自動的に送信されます。

### システムユニット クラッシュレポート Url

デバイスがクラッシュすると、デバイスは解析のためにシスコ自動クラッシュ レポート ツール (ACR) にログを自動送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール: ADMIN

デフォルト値: "acr.cisco.com"

値スペース: 文字列 (0..255)

[Cisco Automatic Crash Report ツール (Cisco Automatic Crash Report tool) ] の URL。

## 時刻設定

### 時刻 時刻形式

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。

### 時刻 日付形式

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

デバイスが物理的に存在する地域のタイムゾーンを設定します。値スペースの情報は、tz データベース (別名: IANA タイムゾーン データベース) から取得しています。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: Etc/UTC

設定可能な値: アフリカ/アビジャン、アフリカ/アクラ、アフリカ/アディスアベバ、アフリカ/アルジェ、アフリカ/アスマラ、アフリカ/アスマラ、アフリカ/バマコ、アフリカ/バンギ、アフリカ/バンジュール、アフリカ/ビサウ、アフリカ/ブランタイア、アフリカ/ブラザビル、アフリカ/ブジュンブラ、アフリカ/カイロ、アフリカ/カサブランカ、アフリカ/セウタ、アフリカ/コナクリ、アフリカ/ダカール、アフリカ/ダルエスサラーム、アフリカ/ジブチ、アフリカ/ドゥアラ、アフリカ/アイウン、アフリカ/フリータウン、アフリカ/ガボローネ、アフリカ/ハラール、アフリカ/ヨハネスブルク、アフリカ/ジュバ、アフリカ/カンバラ、アフリカ/ハルツーム、アフリカ/キガリ、アフリカ/キンシャサ、アフリカ/ラゴス、アフリカ/リールビル、アフリカ/ロメ、アフリカ/ルアンダ、アフリカ/ルブンバシ、アフリカ/ルサカ、アフリカ/マラボ、アフリカ/マプト、アフリカ/マセール、アフリカ/ムババーネ、アフリカ/モガディシユ、アフリカ/モンロヴィア、アフリカ/ナイロビ、アフリカ/ンジャメナ、アフリカ/ニアメイ、アフリカ/ヌアクショット、アフリカ/ワガドゥグ、アフリカ/ポルトノボ、アフリカ/サントメ・プリンシペ、アフリカ/ティンブクトゥ、アフリカ/トリポリ、アフリカ/チュニス、アフリカ/ウイントフック、アメリカ/アダック、アメリカ/アンカレッジ、アメリカ/アンギラ、アメリカ/アンティグア、アメリカ/アラグアイーナ、アメリカ/アルゼンチン/ブエノスアイレス、アメリカ/アルゼンチン/カタマルカ、アメリカ/アルゼンチン/コモドーロ・リバダビア、アメリカ/アルゼンチン/コルドバ、アメリカ/アルゼンチン/ファイ、アメリカ/アルゼンチン/ラ・リオージャ、アメリカ/アルゼンチン/メンドーサ、アメリカ/アルゼンチン/リオ・ガレゴス、アメリカ/アルゼンチン/サルタ、アメリカ/アルゼンチン/サンファン、アメリカ/アルゼンチン/サンルイス、アメリカ/アルゼンチン/トゥクマン、アメリカ/アルゼンチン/ウシュアイア、アメリカ/アルバ、アメリカ/アスンシオン、アメリカ/アティコーカン、アメリカ/アトーチヤ、アメリカ/バヒア、アメリカ/バヒア・バンデラス、アメリカ/バルバドス、アメリカ/ベレン、アメリカ/ベリーズ、アメリカ/ブランサルトン、アメリカ/ボア・ピスタ、アメリカ/ボゴタ、アメリカ/ボイシ、アメリカ/ブエノスアイレス、アメリカ/ケンブリッジベイ、アメリカ/カンボグランデ、アメリカ/カンクーン、アメリカ/カラカス、アメリカ/カタマルカ、アメリカ/カイエン、アメリカ/ケイマン、アメリカ/シカゴ、アメリカ/チワワ、アメリカ/コーラル・ハーバー、アメリカ/コルドバ、アメリカ/コスタリカ、アメリカ/クレストン、アメリカ/クワイアバ、アメリカ/キュラソー、アメリカ/デンマルクシオン、アメリカ/ドーンソン、アメリカ/ドーンソークリーク、アメリカ/デンバー、アメリカ/デトロイト、アメリカ/ドミニカ、アメリカ/エドモントン、アメリカ/エイルネペ、アメリカ/エルサルバドル、アメリカ/エンセナダ、アメリカ/フォート・ネルソン、アメリカ/フォート・ウェイン、アメリカ/フォルタレザ、アメリカ/グレース・米、アメリカ/ゴットホープ、アメリカ/グース・ベイ、アメリカ/グランドターク、アメリカ/グレナダ、アメリカ/グアダルーペ、アメリカ/グアテマラ、アメリカ/グアヤキル、アメリカ/ガイアナ、アメリカ/ハリファクス、アメリカ/ハバナ、アメリカ/エルモシーゾ、アメリカ/インディアナ/インディアナポリス、アメリカ/インディアナ/ノックス、アメリカ/インディアナ/マレンゴ、アメリカ/インディアナ/ピーターズバーグ、アメリカ/インディアナ/テルシエティ、アメリカ/インディアナ/ヴィベイ、アメリカ/インディアナ/ヴァンセンヌ、アメリカ/インディアナ/ウィナマク、アメリカ/インディアナポリス、アメリカ/イヌヴィック、アメリカ/イカルイト、アメリカ/ジャマイカ、アメリカ/フワイ、アメリカ/ジュノー、アメリカ/ケンタッキー/ルイビル、アメリカ/ケンタッキー/モンティチェロ、アメリカ/ノックス、アメリカ/クラレンダイク、アメリカ/ラバス、アメリカ/リマ、アメリカ/ロサンゼルス、アメリカ/ルイビル、アメリカ/ローワー・プリンシズ、アメリカ/マセイオ、アメリカ/マナグア、アメリカ/マナウス、アメリカ/マ

リゴ、アメリカ/マルチニーク、アメリカ/マタモロス、アメリカ/マストラノ、アメリカ/メンドーサ、アメリカ/メノミニ、アメリカ/メリダ、アメリカ/メトラカトラ、アメリカ/メキシコシティ、アメリカ/ミクロン島、アメリカ/モンクトン、アメリカ/モントレイ、アメリカ/モンテビデオ、アメリカ/モントリオール、アメリカ/モンセラート、アメリカ/ナツソー、アメリカ/ニューヨーク、アメリカ/ニビゴン、アメリカ/ノーム、アメリカ/ノローニヤ、アメリカ/ノースダコタ/ビューラ、アメリカ/ノースダコタ/センター、アメリカ/ノースダコタ/ニュー・セララム、アメリカ/オジナガ、アメリカ/パナマ、アメリカ/バングナータング、アメリカ/パラマリボ、アメリカ/フェニックス、アメリカ/ポルトープランス、アメリカ/ポートオブスペイン、アメリカ/ポルト・アクレ、アメリカ/ポルト・ヴェーリヨ、アメリカ/プエルトリコ、アメリカ/レイニールバー、アメリカ/ランキン・インレット、アメリカ/レシフェ、アメリカ/レジーナ、アメリカ/レゾリュート、アメリカ/リオ・ブランコ、アメリカ/ロサリオ、アメリカ/サンタイザベル、アメリカ/サンタレム、アメリカ/サンチアゴ、アメリカ/サントドミンゴ、アメリカ/サンパウロ、アメリカ/ス・コールスピーサンド、アメリカ/シップロック、アメリカ/氏とか、アメリカ/サン・バルテルミー島、アメリカ/セント・ジョーンズ、アメリカ/セントクリストファー・ネイビス、アメリカ/セントルシア、アメリカ/セント・トーマス、アメリカ/サン・ヴィンセント、アメリカ/スウィフトカレント、アメリカ/テグシガルバ、アメリカ/スーリー、アメリカ/サンダーベイ、アメリカ/ティファナ、アメリカ/トロント、アメリカ/トルトラ、アメリカ/バンクーバー、アメリカ/バージン、アメリカ/ホワイトハウス、アメリカ/ウィニベグ、アメリカ/ヤクタート、アメリカ/イエローナイフ、南極/ケーシー、南極/デービス、南極/デューモン・デュルヴィル、南極/マックオーリー、南極/モーソン、南極/マクマルド、南極/バーマー、南極/ロゼラ、南極/南極点、南極/昭和、南極/トロール、南極/ポストーク、北極/ロングイェールピーン、アジア/アデン、アジア/アルマトイ、アジア/あんまん、アジア/アナディル、アジア/アクトウ、アジア/アクトベ、アジア/アシガバート、アジア/アシガバート、アジア/バグダッド、アジア/バーレーン、アジア/バクー、アジア/バンコク、アジア/バルナウル、アジア/ベイルート、アジア/ビシュケク、アジア/ブルネイ、アジア/カルカタ、アジア/チタ、アジア/チョイバルサン、アジア/重慶、アジア/重慶、アジア/コロombo、アジア/ダッカ、アジア/ダマスカス、アジア/ダッカ、アジア/ディリ、アジア/ドバイ、アジア/ドゥシャンベ、アジア/ガザ、アジア/ハルビン、アジア/ヘブロン、アジア/ホーチミンシティ、アジア/香港、アジア/ホブド、アジア/イルクーツク、アジア/イスタンブール、アジア/ジャカルタ、アジア/ジャヤブラ、アジア/エルサレム、アジア/カプール、アジア/カムチャッカ、アジア/カラチ、アジア/カシュガル、アジア/カトマンズ、アジア/カトマンズ、アジア/ハンドゥイガ、アジア/コルカタ、アジア/クラスノヤルスク、アジア/アラランブール、アジア/クチン、アジア/クウェート、アジア/マカオ、アジア/マカオ、アジア/マカオ、アジア/マカッサル、アジア/マニラ、アジア/マスカット、アジア/ニコシア、アジア/ノヴォクズネット、アジア/ノヴォシビルスク、アジア/オムスク、アジア/オラル、アジア/ブノベン、アジア/ボンティアナック、アジア/平壤、アジア/カタール、アジア/クズロルダ、アジア/ラングーン、アジア/リヤド、アジア/サイゴン、アジア/サハリン、アジア/サマルカンド、アジア/ソウル、アジア/上海、アジア/シンガポール、アジア/スレドネコリムスク、アジア/台北、アジア/タシケント、アジア/トビリシ、アジア/テヘラン、アジア/テルアビブ、アジア/ティンブー、アジア/ティンブー、アジア/東京、アジア/トムスク、アジア/ウジュンバダタン、アジア/ウランバートル、アジア/ウランバートル、アジア/ウルムチ、アジア/ウスチ=ネラ、アジア/ヴィエンチャン、アジア/ウラジオストク、アジア/ヤクーツク、アジア/エカテリンブルク、アジア/エレバン、大西洋/アゾレス諸島、大西洋/バミューダ諸島、大西洋/カナリア諸島、大西洋/カーボベルデ、大西洋/フェロー諸島、大西洋/フェロー諸島、大西洋/ヤンマイエン島、大西洋/マディラ島、大西洋/レイキャビク、大西洋/南ジョージア、大西洋/セントヘレナ、大西洋/スタンレー、オーストラリア/ACT、オーストラリア/アデレード、オーストラリア/ブリスベン、オーストラリア/ブローケンヒル、オーストラリア/キャンベラ、オーストラリア/カリー、オーストラリア/ダーウィン、オーストラリア/ユークラ、オーストラリア/ホバート、オーストラリア/LHI、オーストラリア/リンデマン、オーストラリア/ロード・ハウ、オーストラリア/メルボルン、オーストラリア/NSW、オーストラリア/ノース、オーストラリア/パース、オーストラリア/クイーンズランド、オーストラリア/サウス、

オーストラリア/シドニー、オーストラリア/タスマニア、オーストラリア/ヴィクトリア、オーストラリア/ウエスト、オーストラリア/ヤンコウイナ、ブラジル/アクレ、ブラジル/デ・ノローニヤ、ブラジル/イースト、CET、CST6CDT、カナダ/アトランティック、カナダ/セントラル、カナダ/イーストサスカチュワン、カナダ/イースタン、カナダ/マウンテン、カナダ/ニューファンドランド、カナダ/パシフィック、カナダ/サスカチュワン、カナダ/ユーコン、チリ/コンチネンタル、チリ/イースター島、キューバ、EET、EST、EST5EDT、エジプト、Eire、その他/GMT、その他/GMT+0、その他/GMT+1、その他/GMT+10、その他/GMT+11、その他/GMT+12、その他/GMT+2、その他/GMT+3、その他/GMT+4、その他/GMT+5、その他/GMT+6、その他/GMT+7、その他/GMT+8、その他/GMT+9、その他/GMT-0、その他/GMT-1、その他/GMT-10、その他/GMT-11、その他/GMT-12、その他/GMT-13、その他/GMT-14、その他/GMT-2、その他/GMT-3、その他/GMT-4、その他/GMT-5、その他/GMT-6、その他/GMT-7、その他/GMT-8、その他/GMT-9、その他/GMT0、その他/グリニッジ、その他/UCT、その他/UTC、その他/ユニバーサル、その他/ズールー、ヨーロッパ/アムステルダム、ヨーロッパ/アンドラ、ヨーロッパ/アストラハン、ヨーロッパ/アテナ、ヨーロッパ/ベルファスト、ヨーロッパ/ベルグラード、ヨーロッパ/ベルリン、ヨーロッパ/ブラティスラヴァ、ヨーロッパ/ブリュッセル、ヨーロッパ/ブカレスト、ヨーロッパ/ブダペスト、ヨーロッパ/ビュージゲン、ヨーロッパ/キシノウ、ヨーロッパ/コペンハーゲン、ヨーロッパ/ダブリン、ヨーロッパ/ジブラルタル、ヨーロッパ/ガンジー、ヨーロッパ/ヘルシンキ、ヨーロッパ/マン島、ヨーロッパ/イスタンブール、ヨーロッパ/ジャージー、ヨーロッパ/カリニングラード、ヨーロッパ/キエフ、ヨーロッパ/キロフ、ヨーロッパ/リスボン、ヨーロッパ/リュブリャナ、ヨーロッパ/ロンドン、ヨーロッパ/ルクセンブルク、ヨーロッパ/マドリッド、ヨーロッパ/マルタ、ヨーロッパ/マリエハムン、ヨーロッパ/ミンスク、ヨーロッパ/モナコ、ヨーロッパ/モスクワ、ヨーロッパ/ニコシア、ヨーロッパ/おスロー、ヨーロッパ/パリ、ヨーロッパ/ポドゴリツァ、ヨーロッパ/ブラハ、ヨーロッパ/リガ、ヨーロッパ/ローマ、ヨーロッパ/サマラ、ヨーロッパ/サンマリノ、ヨーロッパ/サラエボ、ヨーロッパ/シンフェオポリ、ヨーロッパ/スコピエ、ヨーロッパ/ソフィア、ヨーロッパ/ストックホルム、ヨーロッパ/タリン、ヨーロッパ/ティラーナ、ヨーロッパ/ティラスポリ、ヨーロッパ/ウリヤノフスク、ヨーロッパ/ウージュホロド、ヨーロッパ/ファドゥーツ、ヨーロッパ/パチカン、ヨーロッパ/ウィーン、ヨーロッパ/ヴィリニウス、ヨーロッパ/ヴォルゴグラード、ヨーロッパ/ワルシャワ、ヨーロッパ/ザグレブ、ヨーロッパ/ザボリージャ、ヨーロッパ/チューリッヒ、英国、英国エア、GMT、GMT+0、GMT-0、GMT0、グリニッジ、HST、香港、アイスランド、インド洋/アンタナナリボ、インド洋/チャゴス、インド洋/クリスマス諸島、インド洋/ココス、インド洋/コモロ諸島、インド洋/ケルゲレン諸島、インド洋/マヘ島、インド洋/モルディブ、インド洋/モーリシャス諸島、インド洋/マヨット、インド洋/レユニオン、イラン、イスラエル、ジャマイカ、日本、クェゼリン、リビア、MET、MST、MST7MDT、メキシコ/バハノルテ、メキシコ/バハスル、メキシコ/一般、NZ、NZ-CHAT、ナバホ、PRC、PST8PDT、太平洋/アピア、太平洋/オークランド、太平洋/ブーゲンビル、太平洋/チャタム、太平洋/チューク諸島、太平洋/イースター島、太平洋/エファテ島、太平洋/エンターベリー島、太平洋/ファカオフォ島、太平洋/フィジー、太平洋/フナフティ島、太平洋/ガラパゴス諸島、太平洋/ガンビア、太平洋/ガダルカナル、太平洋/グアム、太平洋/ホノルル、太平洋/ジョンストン、太平洋/クリスマスイ、太平洋/コスラエ、太平洋/クェゼリン、太平洋/マジロ、太平洋/マルキーズ諸島、太平洋/ミッドウェー島、太平洋/ナウル、太平洋/ニウエ、太平洋/ノーフォーク、太平洋/ヌメア、太平洋/パゴパゴ、太平洋/パラオ、太平洋/ピトケアン、太平洋/ボンベイ、太平洋/ボナベ、太平洋/ポートモレスビー、太平洋/ラロトンガ、太平洋/サイパン、太平洋/サモア、太平洋/タヒチ、太平洋/タラワ、太平洋/トンガタプ、太平洋/トラック、太平洋/ウェーキ、太平洋/ウォリス、太平洋/ヤップ、ポーランド、ポルトガル、ROC、ROK、シンガポール、トルコ、UCT、米国/アラスカ、米国/アリゾナ、米国/アリゾナ、米国/セントラル、米国/東インドアナ、米国/イースタン、米国/ハワイ、米国/インドアナスターク、米国/ミシガン、米国/マウンテン、米国/パシフィック、米国/パシフィックニュー、米国/サモア、UTC、ユニバーサル、W-SU、WET、ズールー

リストからタイムゾーンを選択します。

## ユーザインターフェイス設定

### ユーザインターフェイス アクセシビリティ 着信コール通知

画面表示を強調した着信コールの通知を利用できます。画面とタッチ 10 は約 1 秒ごと (1.75 Hz) に赤と白に点滅し、聴覚が不自由なユーザが着信コールに気づきやすくするようにしています。デバイスがコール中の場合、進行中のコールの妨げになるため画面は点滅しません、その代わりに、通常の通知が画面とタッチ パネルに表示されます。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: Default

値スペース: AmplifiedVisuals/Default

AmplifiedVisuals: デバイスがコールを受け入れたときに、画面とタッチパネル上での画面表示の強調を有効にします。

Default: スクリーンとタッチパネル上での通知を使用したデフォルトの動作を有効にします。

### ユーザーインターフェイス アシスタント モード

Webex Assistant を使用すると、音声コマンドを使用してデバイスを制御できます。Webex Assistant はクラウドサービスなので、デバイスが Webex クラウドサービスに登録されているか、オンプレミスサービスに登録されて Webex Edge for Devices にリンクされている必要があります。

デバイスで Webex Assistant を有効または無効にするには、この設定を使用します。

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: Webex Assistant がオフになります。

On: インフラストラクチャでサポートされている場合、Webex Assistant を使用できます。

### ユーザインターフェイス アシスタント 会議参加確認

参加確認は Webex Assistant によって提供される機能です。参加確認が有効になっている場合、OBTP ミーティングの開始直前にミーティングルームに人がいることが検出されると、デバイスはその人にこれから始まるミーティングに参加するかどうかを確認します。

デバイスで参加確認機能を有効または無効にするには、この設定を使用します。

必要なユーザ ロール: ADMIN

デフォルト値: False

値スペース: False/True

False: 参加確認機能はオフになります。

True: Webex Assistant がアクティブになっていれば、参加確認機能を使用できます。

### ユーザインターフェイス 予約 可視性 タイトル

ミーティングの詳細をプライベートに変更します。「ミーティングのスケジュール (Scheduled meeting)」というテキストがミーティングのタイトルとして表示されます。

必要なユーザ ロール: ADMIN, INTEGRATOR, USER

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: ミーティングのタイトルが公開され、ユーザインターフェイスに表示されます。

Hidden: ミーティングのタイトルが非表示になり、ユーザインターフェイスには「ミーティングのスケジュール (Scheduled meeting)」と表示されます。

## ユーザインターフェイス ブランディング アウェイク状態のブランディング 色

ブランディングのカスタマイズを使用してデバイスがセットアップされている場合、この設定は、デバイスが起動している時に表示されるロゴの色に影響します。ロゴをフルカラーで表示するか、またはロゴの不透明度を下げるかによって、画面上の背景や他の要素とより自然にブレンドするように設定することができます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: Auto/Native

Auto: ロゴの不透明度は低減されます。

Native: ロゴはフルカラーです。

## ユーザインターフェイス 連絡先情報 タイプ

ユーザ インターフェイスで表示する連絡先の種類を選択します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

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

Auto: 他のデバイスがこのビデオ会議デバイスに接続するためにダイヤルする必要があるアドレスを表示します。アドレスは、デフォルトのコール プロトコルおよびデバイス登録によって異なります。

None: どのようなコンタクト情報も表示しません。

IPv4: デバイスの IPv4 アドレスを示します。

IPv6: デバイスの IPv6 アドレスを示します。

H323Id: デバイスの H.323 ID を表示します (H323 H323Alias ID 設定を参照)。

H320Number: 連絡先情報としてデバイスの H.320 番号を表示します (Cisco TelePresence ISDN リンクを使用している場合のみサポートされます)。

E164Alias: 連絡先情報としてデバイスの H.323 E164 エイリアスを表示します (H323 H323Alias E164 設定を参照)。

SipUri: デバイスの SIP URI を表示します (SIP URI 設定を参照)。

SystemName: デバイス名を表示します (SystemUnit Name 設定を参照)。

DisplayName: デバイスの表示名を表示します (SIP DisplayName 設定を参照)。

## ユーザインターフェイス カスタムメッセージ

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 128)

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

## ユーザインターフェイス 診断 通知

ユーザインターフェイスに診断の通知を表示するかどうかを設定します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: 診断の通知がユーザインターフェイスに表示されます。

Hidden: 診断の通知はユーザインターフェイスに表示されません。

## ユーザインターフェイス キートーン モード

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) が鳴るようにデバイスを設定できます。

必要なユーザ ロール: admin、user

デフォルト値: On

値スペース: Off/On

Off: キー トーンは再生されません。

On: キー トーンがオンになります。



## ユーザインターフェイス 機能 コール 終了

ユーザインターフェイスからデフォルトの通話終了ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden: デフォルトボタンをユーザ インターフェイスから削除します。

## ユーザインターフェイス 機能 コール キーパッド

ユーザインターフェイスから、デフォルトの通話中の [キーパッド (Keypad)] ボタンを削除するかどうかを選択します。このボタンは、DTMF 入力などに使用できるキーパッドを開きます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden: デフォルトボタンをユーザ インターフェイスから削除します。

## ユーザインターフェイス 機能 コール 通話中制御

ユーザインターフェイスからデフォルトの保留、転送、および通話再開ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden: ユーザ インターフェイスからデフォルトボタンを削除します。

## ユーザインターフェイス 機能 コール Webexに参加

ユーザインターフェイスからデフォルトの [Webexに参加 (Join Webex)] ボタンを削除するかどうかを選択します。

このボタンを使用すると、ユーザは Webex ミーティング番号で Webex ミーティングにダイヤルインできます。ドメインは必要ありません。ただし、この機能を動作させるには、インフラストラクチャの設定で \*@webex.com へのコールのルーティングを許可する必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden: デフォルトボタンをユーザ インターフェイスから削除します。

## ユーザインターフェイス 機能 コール 開始

ユーザインターフェイスから、デフォルトの通話ボタン (ディレクトリ、お気に入り、および直近の通話リスト)、さらにデフォルトの着信追加参加者ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: デフォルトボタンをユーザ インターフェイスに表示します。

Hidden: ユーザ インターフェイスからデフォルトボタンを削除する

## ユーザインターフェイス機能通話ビデオミュート

ユーザインターフェイスにデフォルトの[ビデオをオフにする]ボタンを表示するかどうかを選択します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

自動: この機能が継続的な通話でサポートされている場合、ユーザインターフェイスに[ビデオをオフにする]ボタンが表示されます。

非表示: [ビデオをオフにする]ボタンはユーザインターフェイスに表示されません。



## ユーザインターフェイス 機能 すべて非表示

ユーザインターフェイスからデフォルトボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: False

値スペース: False/True

- False: すべてのデフォルトボタンをユーザインターフェイスで表示します。
- True: すべてのデフォルトボタンをユーザインターフェイスで表示しません。

## ユーザインターフェイス 機能 共有 開始

ユーザインターフェイスから、コンテンツの共有とコール発信の両方で、コンテンツを共有およびプレビューするためのデフォルトボタンやその他の UI 要素を削除するかどうかを選択します。設定はボタンと UI 要素だけを削除し、機能などは削除しません。Proximity または Cisco Webex Teams アプリを使ってコンテンツの共有は可能です。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値のスペース: Auto/Hidden

- Auto: デフォルトボタンと UI 要素をユーザ インターフェイスに表示します。
- Hidden: デフォルトボタンと UI 要素をユーザ インターフェイスから削除します。

## ユーザインターフェイス 言語

ユーザ インターフェイスで使用される言語を選択します。該当する言語がサポートされていない場合、デフォルトの言語 (Medium) が使用されます。

必要なユーザ ロール: admin、user

デフォルト値: English

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

リストから言語を選択します。

## ユーザインターフェイス OSD 暗号化インジケータ

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

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/AlwaysOn/AlwaysOff

- Auto: コールが暗号化されている場合は、「コールは暗号化されています (Call is encrypted)」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。
- コールが暗号化されていない場合は、「コールは暗号化されていません (Call is not encrypted)」という通知が 5 秒間表示されます。暗号化インジケータ アイコンは表示されません。
- AlwaysOn: 「コールは暗号化されています (Call is encrypted)」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。
- AlwaysOff: 暗号化インジケータは画面上に表示されません。

## ユーザインターフェイス OSD ハーフウェイクメッセージ

カスタム メッセージは、デバイスがハーフウェイク状態のときに、メイン スクリーンの中央に表示できます。カスタム メッセージは、デバイスの使用開始方法について指示するデフォルトのメッセージを置き換えます。カスタム メッセージを追加せずにデフォルト メッセージを削除することもできます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ""

値スペース: 文字列 (0, 128)

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

## ユーザインターフェイス OSD 出力

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: Auto

Auto: オンスクリーン情報とインジケータをデバイスの画面に送信します。

## ユーザインターフェイス 電話帳 モード

この設定は、ユーザがデバイスのユーザ インターフェイスから、ディレクトリとお気に入りリストに連絡先を追加または変更することを許可するかどうかを決定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: ReadWrite

値スペース: ReadOnly/ReadWrite

ReadOnly: 連絡先をお気に入りリストに追加したり、お気に入りリストの連絡先を編集したりはできません。また、通話前にディレクトリやお気に入りリストから連絡先を編集することはできません。

ReadWrite: 連絡先をお気に入りリストに追加したり、お気に入りリストの連絡先を編集したりできます。また、通話前にディレクトリやお気に入りリストから連絡先を編集することができます。

## ユーザインターフェイス プロキシミティ 通知

ユーザインターフェイスにプロキシミティの通知を表示するかどうかを設定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: Auto/Off/On

Auto: プロキシミティの通知を表示するタイミングをシステムが自動的に決定できるようにします。

Off: プロキシミティの通知はユーザインターフェイスに表示されません。

On: すべてのプロキシミティの通知がユーザインターフェイスに表示されます。

## ユーザインターフェイス セキュリティ モード

この設定では、重要なデバイス情報 (例: ビデオ会議デバイスの連絡先情報や IP アドレス、Touch コントローラ、および UCM/VCS レジストラ) がユーザ インターフェイス (ドロップダウン メニューと設定パネル) で公開されるのを防ぐことができます。設定パネルに移動するとこのような情報は非表示になっていないので注意してください。

管理者権限を持たない人に連絡先情報、IP アドレス、MAC アドレス、シリアル番号およびソフトウェアのバージョンを絶対に公開しない場合は、[ユーザ インターフェイス設定メニュー モード (UserInterface SettingsMenu Mode)] を [ロック (Locked)] に設定します。また、管理者権限を持つすべてのユーザ アカウントにパスフレーズを設定することも必要です。

必要なユーザ ロール: ADMIN

デフォルト値: Normal

値スペース: Normal/Strong

Normal: IP アドレスやその他のデバイス情報がユーザ インターフェイスに表示されます。

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

## ユーザインターフェイス 設定メニュー モード

ユーザ インターフェイス (Touch 10 または画面上) の設定パネルは、そのデバイスの管理者パスワードで保護できます。このパスワードが空白の場合、誰でも設定パネルの設定にアクセスし、たとえばデバイスを初期設定にリセットすることができます。認証を有効にすると、認証を必要とするすべての設定に南京錠のアイコンが表示されます。設定を選択するときに、管理者のユーザ名とパスフレーズを入力するよう求められます。認証が必須でない設定には、南京錠のアイコンが表示されません。

必要なユーザ ロール: ADMIN

デフォルト値: Unlocked

値スペース: Locked/Unlocked

Locked: 管理者のユーザ名とパスフレーズによる認証が必要です。

Unlocked: 認証は必要ありません。

## ユーザインターフェイス 設定メニュー 可視性

デバイス名 (または連絡先情報) および関連するドロップ ダウン メニューと [設定 (Settings)] パネルを、ユーザ インタフェースに表示するかどうかを選択します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値のスペース: Auto/Hidden

Auto: デバイス名とドロップ ダウン メニュー、[設定 (Settings)] パネルをユーザ インタフェースに表示します。

Hidden: デバイス名とドロップ ダウン メニュー、[設定 (Settings)] パネルを、ユーザ インタフェースに表示しません。

## ユーザインターフェイス サウンドエフェクト モード

他のユーザが Proximity でラップトップやモバイルに接続したときなどにサウンド エフェクトを鳴らすように、デバイスを設定できます。

テキスト入力時のキーボード クリックのサウンド エフェクトは、この設定の影響を受けません (ユーザインターフェイス キートーン モード 設定を参照してください)。

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: サウンド エフェクトを鳴らしません。

On: サウンド エフェクトをオンにします。

## ユーザインターフェイス壁紙

アイドル状態のときのビデオ画面の背景画像 (壁紙) を選択します。

Web インタフェースを使用してデバイスにカスタム壁紙をアップロードできます。サポートされるファイル形式は BMP、GIF、JPEG、PNG です。最大ファイル サイズは 4 MByte です。カスタム壁紙を使用すると、予定されている会議のクロックおよび一覧がメイン ディスプレイから削除されます。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Auto

値スペース: Auto/Custom/None

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。デバイスにカスタム壁紙がアップロードされていない場合、この設定はデフォルト値に戻ります。

## ユーザインターフェイス Usbプロモーション

ハーフウェイク画面に、このデバイスを USB カメラとして使用できることを知らせるテキストを表示するかどうかを選択します。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

オフ: USB カメラの情報テキストは表示されません。

オン: USB カメラの情報テキストが表示されます。

## ユーザインターフェイス Webcamのみモード

このデバイスは、Web カメラとして使用することも、通常のビデオ会議デバイスとして使用することもできます。オンプレミスまたはクラウドコールサービス (CUCM、VCS、Webex など) に登録されていない場合でも、web カメラとして使用できます。

この設定は、ビデオ会議デバイスが登録されていない場合に、ユーザ インターフェイスを Web カメラのみのシナリオに適応させるかどうかを決定します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/Off

Auto: デバイスがコール サービスに登録されている場合は、ユーザ インターフェイス全体が表示されます。デバイスが登録されていない場合はコールに使用できないため、関係のないユーザ インターフェイス要素は削除されます。

Off: 常にユーザ インターフェイス全体がデバイスに表示されます。

## ユーザインターフェイス ホワイトボード アクティビティインジケータ

アクティビティインジケータを使用すると、コール中に誰が描画し、注釈を付けているかを確認できます。

参加者がホワイトボードと対話しているときは、その参加者のアバターまたはデバイスの頭文字が表示されるため、誰が描画や注釈付けを行っているかを把握できます。

クラウド登録デバイス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: On

値スペース: Off/On

On: アクティビティインジケータを有効にします。

Off: アクティビティインジケータを無効にします。

## ユーザー管理設定

### ユーザ管理 LDAP 管理者 フィルタ

どのユーザに管理者権限を付与する必要があるか決定するために LDAP フィルタが使用されます。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタが優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても、ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0, 1024)

この文字列の構文については、LDAP の仕様を参照してください。例:  
 "(| (memberof=CN=admin group, OU=company groups, DC=company, DC=com)  
 (sAMAccountName=username))"

### ユーザ管理 LDAP 管理者 グループ

この AD (Active Directory) グループのメンバーには、管理者権限が付与されます。この設定は、memberOf:1.2.840.113556.1.4.1941:=&lt;group name&gt; の短縮形です。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。LDAP 管理者フィルタが優先されるため、ユーザ管理 LDAP 管理者フィルタが設定されている場合であっても、ユーザ管理 LDAP 管理者グループ設定は無視されます。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0..255)

AD グループの識別名。例: "CN=admin group, OU=company groups, DC=company, DC=com"

### ユーザ管理 LDAP 属性

指定のユーザ名にマップするために使用する属性。設定しない場合、sAMAccountName が使用されます。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0..255)

属性名。

### UserManagement LDAP BaseDN

検索を開始するエントリの識別名 (ベース)。

必要なユーザ ロール: ADMIN

デフォルト値: ""

値スペース: 文字列 (0..255)

ベースの識別名。例: "DC=company, DC=com"

### ユーザ管理 LDAP 暗号化

デバイスと LDAP サーバの間の通信を保護する方法を定義します。ポート番号は、ユーザ管理 LDAP サーバ ポート設定を使用してポート番号をオーバーライドできます。

必要なユーザ ロール: ADMIN

デフォルト値: LDAPS

値スペース: LDAPS/None/STARTTLS

LDAPS: ポート 636 over TLS (Transport Layer Security) 上の LDAP サーバに接続します。

None: ポート 389 で LDAP サーバに接続します (暗号化なし)。

STARTTLS: ポート 389 で LDAP サーバに接続し、暗号化された接続 (TLS) にアップグレードするための STARTTLS コマンドを送信します。

## ユーザ管理 LDAP 最小TLSバージョン

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

必要なユーザ ロール: ADMIN

デフォルト値: TLSv1.2

値スペース: TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0: TLS バージョン 1.0 以上をサポートします。

TLSv1.1: TLS バージョン 1.1 以上をサポートします。

TLSv1.2: TLS バージョン 1.2 以上をサポートします。

## ユーザ管理 LDAP モード

このデバイスでは、ユーザ名とパスワードを一元的に保存、検証する場所として、LDAP (Lightweight Directory Access Protocol) サーバの使用をサポートします。この設定を使用して、LDAP 認証を使用するかどうか設定します。実装は、Microsoft Active Directory (AD) サービスでテスト済みです。

LDAP モードをオンにする場合、設定に合わせたユーザ管理 LDAP 設定の構成を確認してください。いくつかの例を示します。

例 1:

- ユーザ管理 LDAP モード: On
- ユーザ管理 LDAP アドレス: "192.0.2.20"
- ユーザ管理 LDAP ベース DN: "DC=company, DC=com"
- ユーザ管理 LDAP 管理グループ: "CN=admin group, OU=company group, DC=company, DC=com"

例 2:

- ユーザ管理 LDAP モード: On
- ユーザ管理 LDAP アドレス: "192.0.2.20"
- ユーザ管理 LDAP ベース DN: "DC=company, DC=com"
- ユーザ管理 LDAP 管理フィルタ: "(|(memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

Off: LDAP 認証は使用不可です。

On: LDAP 認証は許可されます。

## ユーザ管理 LDAP サーバ アドレス

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。

## ユーザ管理 LDAP サーバ ポート

LDAP サーバに接続するポートをオンに設定します。0 に設定した場合は、選択したプロトコルのデフォルトを使用します (「ユーザ管理 LDAP 暗号化設定」を参照する)。

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。

## ユーザ管理 LDAP サーバ証明書の検証

デバイスを LDAP サーバに接続すると、サーバはデバイスに証明書を提示して自身を識別します。この設定は、デバイスがサーバの証明書を確認するかどうかを決定するために使用します。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: デバイスは LDAP サーバの証明書を検証しません。

On: デバイスは、LDAP サーバの証明書が信頼できる認証局 (CA) によって署名されているかどうか検証する必要があります。該当する CA が、デバイスに事前にアップロードされている信頼できる CA のリストに含まれている必要があります。デバイスの Web インターフェイスを使用して、信頼できる CA のリストを管理します (詳細については『管理者ガイド』を参照してください)。

## ユーザ管理 パスワードポリシー 複雑度 数字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある数字 (0 ~ 9) の最小文字数を指定します。

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 ~ 4)

数字の最小文字数。0 は制限がないことを意味します。

## ユーザ管理 パスワードポリシー 複雑度 最小文字数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、パスワードの最小文字数を指定します。

必要なユーザ ロール: ADMIN

デフォルト値: 8

値スペース: 整数 (0 ~ 256)

文字の最小数。0 は制限がないことを意味します。

## ユーザ管理 パスワードポリシー 複雑度 小文字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある小文字の最小文字数を指定します。

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 ~ 4)

小文字の最小文字数。0 は制限がないことを意味します。

## ユーザ管理 パスワードポリシー 複雑度 特殊文字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy)] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある特殊文字の最小文字数を指定します。

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 ~ 4)

特殊文字の最小文字数。0 は制限がないことを意味します。



## ユーザ管理 パスワードポリシー 複雑度 大文字の最小数

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy) ] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、パスワードに含める必要のある大文字の最小文字数を指定します。

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 ~ 4)

大文字の最小文字数。0 は制限がないことを意味します。

## ユーザ管理 パスワードポリシー 最大有効期間

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy) ] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、パスワードが無効になるまでの最大日数を指定します。

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 ~ 7300)

最小日数。0 は制限がないことを意味します。

## ユーザ管理 パスワードポリシー 再使用制限

デバイスにローカルユーザとしてサインインする場合、パスワードは [ユーザインターフェイス パスワードポリシー (UserManagement PasswordPolicy) ] 設定で設定されたルールに従う必要があります。これらの設定は、CE9.10 より前のソフトウェアバージョンに用意されていた「systemtools securitysetting」コマンドを置き換えるものです。

新しいパスワードルールは既存のパスワードには適用されませんが、次のパスワードの変更時に有効になります。

この設定は、再使用の制限 (n) を指定します。つまり、ユーザは、直前の n 個のパスワードを再使用することはできません。

必要なユーザ ロール: ADMIN

デフォルト値: 12

値スペース: 整数 (0..24)

パスワードの最小数。0 は制限がないことを意味します。



## ビデオ設定

### ビデオ アクティブスピーカー デフォルトPIPポジション

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

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: Current

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

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

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。

### ビデオ デフォルトレイアウトファミリー ローカル

ローカルで使用するビデオ レイアウト ファミリーを選択します。

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: デバイスによって提供されるローカル レイアウト データベースの指定に従って、デフォルトのレイアウト ファミリーがローカル レイアウトとして使用されます。

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

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

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

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

## ビデオ デフォルトレイアウトファミリ リモート

リモート参加者（遠く）に送信されるストリーミングで使用するビデオレイアウトファミリを選択します。この設定は、デバイスに搭載された MultiSite 機能（オプション）を使用してマルチポイントのビデオ会議をホストする場合にのみ適用されます。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

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

Auto: デバイスによって提供されるローカル レイアウト データベースの指定に従って、デフォルトのレイアウト ファミリがローカル レイアウトとして使用されます。

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

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

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

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、音声は切り替えられます。

## ビデオ デフォルトメインソース

コールのメインビデオのデフォルト入力ソースを定義します。ビデオ会議デバイスのスイッチをオンにするか再起動すると、メインビデオがこのソースで再生されます。デバイスの実行中に別のソースに変更するには、Video Input SetMainVideoSource コマンドを使用します。

必要なユーザ ロール: admin, user

デフォルト値: 1

値スペース: 1

メインビデオのデフォルトソース。

## ビデオ 入力 コネクタ [n] カメラ制御 カメラID

n: 1..2

カメラ ID は、このビデオ入力に接続されているカメラの一意の ID です。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: 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。

## ビデオ 入力 コネクタ [n] カメラ制御 モード

n: 1..2

このビデオ入力コネクタに接続されているカメラを制御するかどうかを定義します。カメラ制御はコネクタ 2 (HDMI) では使用できないことに注意してください。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: Connector 1: On Connector 2: Off

値スペース: Connector 1: Off/On Connector 2: Off

Off: カメラ制御を無効にします。

On: カメラ制御を有効にします。

## ビデオ 入力 コネクタ [n] CEC モード

n: 2..2

ビデオ入力 (HDMI) は、Consumer Electronics Control (CEC) をサポートします。この設定を有効にすると、接続デバイスの情報（デバイスの種類やデバイス名）がビデオ会議デバイスのステータスで使用可能になります (Video Input Connector[n] ConnectedDevice CEC [n])。ただし、接続デバイスは CEC もサポートすることが条件となります。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: CEC が無効です。

On: CEC が有効になります。

## ビデオ 入力 コネクタ [n] 入力ソースタイプ

n: 1..2

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 はデバイスの内蔵カメラであることに注意してください。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Connector 1: camera Connector 2: PC

値スペース: Connector 1: camera Connector 2: PC/camera/document\_camera/mediaplayer/  
whiteboard/other

PC: コンピュータがビデオ入力に接続されている場合に使用します。

camera: カメラがビデオ入力に接続されている場合に使用します。

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

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

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

other: 他のオプションが当てはまらない場合に使用します。

## ビデオ 入力 コネクタ [n] 名前

n: 1..2

ビデオ入力コネクタの名前を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Connector 1: "Camera" Connector 2: "PC"

値スペース: 文字列 (0, 50)

ビデオ入力コネクタの名前。

## ビデオ 入力 コネクタ [n] 最適鮮明度 プロファイル

n: 1..2

この設定は、対応するビデオ入力コネクタ [n] 画質設定が Sharpness に設定されている場合には無効です。

最適鮮明度プロファイルは、ビデオ会議室の照明状態とカメラと品質を反映します。光の条件およびカメラの品質が優れているほど、プロファイルが高くなります。通常、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。解像度が発信側と着信側の両方のデバイスでサポートされている必要があります。

ビデオ 入力 コネクタ [n] 最適鮮明度 しきい値 60 fps 設定を使用し、60 fps が許可される最小解像度を設定します。このしきい値を下回ると、30 fps が最大フレームレートになります。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Medium

値スペース: Normal/Medium/High

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

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

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

## ビデオ 入力 コネクタ [n] 最適鮮明度 しきい値 60 fps

n: 1..2

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

必要なユーザ ロール: ADMIN

デフォルト値: 1920\_1080

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

512\_288: 512x288 にしきい値を設定します。

768\_448: 768x448 にしきい値を設定します。

1024\_576: 1024x576 にしきい値を設定します。

1280\_720: 1280x720 にしきい値を設定します。

1920\_1080: 1920 X 1080 にしきい値を設定します。

Never: 60 fps を送信するしきい値を設定しません。

## ビデオ 入力 コネクタ [n] 推奨解像度

n: 2..2

ビデオ会議デバイスに HDMI 経由でシステムに接続した入力ソース (例: ラップトップ) の解像度として通知されている推奨の画面解像度と更新間隔を定義します。ソース デバイス (例、ラップトップのディスプレイ構成ソフトウェア) によって手動でオーバーライドされない限り、ソース側の解像度の選択するためのロジックは、自動的にこの解像度とリフレッシュ レートを選択します。

1920\_1080\_60 より大きい形式では特に大量のデータが使用されるため、少なくとも HDMI 1.4b データレートに対応したプレゼンテーションケーブル (またはアダプタ) が必要です。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: 1920\_1080\_60

値スペース: 1920\_1080\_60/2560\_1440\_60/3840\_2160\_30

1920\_1080\_60: 解像度は 1920 X 1080、リフレッシュ レートは 60 Hz です。

2560\_1440\_60: 解像度は 2560 X 1440、リフレッシュ レートは 60 Hz です。

3840\_2160\_30: 解像度は 3840 X 2160、リフレッシュ レートは 30 Hz です。

## ビデオ 入力 コネクタ [n] プレゼンテーションの選択

n: 2..2

プレゼンテーション ソースをビデオ入力に接続したときの、ビデオ会議デバイスの動作を定義します。

デバイスがスタンバイ モードの場合、プレゼンテーション ソースを接続すると起動します。遠端とプレゼンテーションを共有するには、この設定が AutoShare に設定されていなければ、追加操作 (ユーザ インターフェイスで [共有 (Share)] を選択) が必要です。

必要なユーザ ロール: ADMIN, INTEGRATOR

デフォルト値: OnConnect

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

AutoShare: 通話時に、ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど)、自動的に遠端とローカル画面に表示されます。ユーザ インターフェイス上で [共有 (Share)] を選択する必要はありません。コールの発信時または応答時にプレゼンテーション ソースがすでに接続されている場合は、ユーザ インターフェイス上で [共有 (Share)] を手動で選択する必要があります。

Desktop: ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど)、画面に表示されます。これは、アイドル状態のときと通話中のときの両方に適用されます。また、ビデオ入力のコンテンツは、通話の終了時にアクティブ入力であれば、画面に表示されたままとなります。

Manual: ユーザ インターフェイスで [共有 (Share)] を選択するまでビデオ入力の内容は画面に表示されません。

OnConnect: ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが起動すると (たとえば接続されているコンピュータがスリープ モードから復帰するなど)、画面に表示されます。それ以外の場合は、Manual モードと同じ動作です。

## ビデオ 入力 コネクタ [n] 画質

n: 2..2

ビデオのエンコーディングと送信のときには、高解像度と高フレーム レートとの間にトレード オフが存在します。一部のビデオ ソースでは、高フレーム レートが高解像度より重要である場合や、逆の場合もあります。この設定で、高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 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。

## ビデオ入力コネクタ [n] RGB 量子化範囲

n: 2..2

ビデオ入力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していません。その場合、ソースの完全なイメージを取得するために、この設定を使用して設定を上書きできます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Auto

値スペース: Auto/Full/Limited

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

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

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

## ビデオ 入力 コネクタ [n] 可視性

n: 1..2

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 はデバイスの内蔵カメラであり、プレゼンテーション ソースとして使用できないことに注意してください。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Connector 1: Never Connector 2: Always

値スペース: Connector 1: Never Connector 2: Always/IfSignal/Never

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

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

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

## ビデオ 出力 コネクタ [n] CEC モード

n: 1..1

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

この設定が [オン (On)] の場合、ビデオ会議デバイス自身がスタンバイになるときに、CEC を使用して画面をスタンバイ状態にセットします。同様に、デバイスがスタンバイから復帰するときに、デバイス自身が画面を起動します。

画面のアクティブなビデオ入力ユーザによって変更されることがあります。コールが開始されると、デバイスはアクティブなビデオ入力画面の別の入力に切り替えられたかどうかを検出します。切り替えられている場合、デバイスは入力を切り替え直し、デバイスがアクティブなビデオ入力ソースになります。デバイスがスタンバイ状態になるときに、デバイスがアクティブな入力ソースでない場合は、画面はスタンバイ状態にセットされません。

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

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: CEC が無効です。

On: CEC が有効になります。

## ビデオ出力コネクタ [n] モニタロール

n: 1..1

適用なし

## ビデオ出力コネクタ [n] 解像度

n: 1..1

接続している画面の解像度とリフレッシュ レートを定義します。

1920\_1200\_60 より大きなフォーマットには、高品質なディスプレイ ケーブルを使用する必要があります。動作が保証されている範囲については、3840\_2160\_60 でシスコが事前に選定したディスプレイ ケーブルを使用するか、または「プレミアム HDMI 認証」プログラムに合格したケーブルを使用します。

UHD テレビおよび画面には、3840\_2160\_30 (30 Hz) のみしか使用できないものもありますが、3840\_2160\_60 (60 Hz) はデフォルト設定ではありません。このような場合、テレビと画面の関連設定で、デバイスが接続されている HDMI 入力として 3840\_2160\_60 を許可するように再設定する必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Connector n: Auto

値スペース: Auto/1920\_1080\_50/1920\_1080\_60/1920\_1200\_50/1920\_1200\_60/  
2560\_1440\_60/3840\_2160\_30/3840\_2160\_60

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

1920\_1080\_50: 解像度は 1920 X 1080、リフレッシュ レートは 50 Hz です。

1920\_1080\_60: 解像度は 1920 X 1080、リフレッシュ レートは 60 Hz です。

1920\_1200\_50: 解像度は 1920 X 1200、リフレッシュ レートは 50 Hz です。

1920\_1200\_60: 解像度は 1920 X 1200、リフレッシュ レートは 60 Hz です。

2560\_1440\_60: 解像度は 2560 X 1440、リフレッシュ レートは 60 Hz です。

3840\_2160\_30: 解像度は 3840 X 2160、リフレッシュ レートは 30 Hz です。

3840\_2160\_60: 解像度は 3840 x 2160、リフレッシュ レートは 60 Hz です。



## ビデオ入力コネクタ [n] RGB 量子化範囲

n: 1..1

HDMI 出力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していません。その場合、ディスプレイの完全なイメージを取得するために、この設定を使用して設定を上書きできます。ほとんどの HDMI ディスプレイはフルの量子化範囲を想定しています。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Full

値スペース: Auto/Full/Limited

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

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

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

## ビデオ プレゼンテーション デフォルトPIPポジション

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Current

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

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

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

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

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

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

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

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

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

## ビデオ プレゼンテーション デフォルトソース

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソースを定義します。この設定は、API およびサードパーティのユーザ インターフェイスで使用できます。Cisco が提供するユーザ インターフェイスの使用時には関係ありません。

必要なユーザ ロール: admin、user

デフォルト値: 2

値スペース: 1/2

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソース。

## ビデオ プレゼンテーション 優先順位

プレゼンテーションチャンネルとビデオチャンネル間でどのように帯域幅を分配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: Equal

値スペース: Equal/High/Low

利用可能なビデオ伝送帯域幅がメインチャンネルとプレゼンテーションチャンネルの間で分散されます。

High: プレゼンテーションチャンネルは、メインビデオチャンネルを犠牲にして、利用可能な帯域の大部分に割り当てられます。

Low: メインビデオチャンネルは、プレゼンテーションチャンネルを犠牲にして、利用可能な帯域の大部分に割り当てられます。

## ビデオ セルフビュー デフォルト フルスクリーンモード

コール終了後に、メイン ビデオ ソース (セルフビュー) を全画面表示するか、小さいピクチャインピクチャ (PiP) として表示するかを定義します。この設定はセルフビューがオンになっている場合にのみ有効です (ビデオ セルフビュー デフォルト モードの設定を参照)。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Current

値スペース: Off/Current/On

Off: セルフビューは PiP として表示されます。

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

On: セルフビューの画像は全画面表示されます。

## ビデオ セルフビュー デフォルト モード

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、ビデオ セルフビュー デフォルト PIP ポジションとビデオ セルフビュー デフォルト フルスクリーンモードの設定によって決まります。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Current

値スペース: Off/Current/On

Off: セルフビューはコール退出時にオフにされます。

Current: セルフビューはそのままの状態が残ります。つまりコール中にオンであった場合はコール終了後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。

## ビデオ セルフビュー デフォルト 表示先モニタロール

コールの後にメイン ビデオ ソース (セルフビュー) を表示する画面/出力を設定します。この値は、異なる出力用に設定されたビデオ出力 コネクタ [n] モニタロール設定のモニタ ロールを反映しません。

この設定は、セルフ ビューが全画面で表示されたとき、およびセルフビューがピクチャインピクチャ (PiP) で表示されたときの両方に適用されます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Current

値スペース: Current/First/Second

Current: コールを中止すると、セルフビュー画像がコール中と同じ出力上に維持されます。

First: セルフビュー画像は、ビデオ出力 コネクタ [n] モニタロールが First に設定された出力上に表示されます。

Second: セルフビュー画像は、ビデオ出力 コネクタ [n] モニタロールが Second に設定された出力上に表示されます。

## ビデオ セルフビュー デフォルト PIP ポジション

コール終了後に小さいセルフビュー ピクチャインピクチャ (PiP) を表示する画面上の位置を定義します。この設定は、セルフビューがオンになっており (ビデオ セルフビュー デフォルト モード設定を参照)、全画面表示がオフになっている場合 (ビデオ セルフビュー デフォルト フルスクリーン モード設定を参照) にのみ有効です。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Current

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

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

UpperLeft: セルフビュー PiP が画面の左上隅に表示されます。

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

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

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

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

LowerLeft: セルフビュー PiP が画面の左下隅に表示されます。

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



## ビデオ セルフビュー オンコール モード

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、ビデオ セルフビュー オンコール 期間設定で定義します。これは一般にセルフ ビューがオフの場合に適用されます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: セルフ ビューはコール セットアップ中に自動的に表示されません。

On: セルフ ビューはコール セットアップ中に自動的に表示されます。

## ビデオ セルフビュー オンコール 期間

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

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 10

値スペース: 整数 (1..60)

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

## Web エンジン設定

### Webエンジン 機能 WebGL

WebGL (Web Graphics Library) は、Web ブラウザでプラグインを使用せずにインタラクティブな 2D グラフィックや 3D グラフィックをレンダリングするための Javascript API です。

WebGL は試験的な機能であり、将来変更される可能性があります。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off/On

On: WebGL が有効になります。

Off: WebGL が無効になります。

### Web エンジン モード

Web エンジンは、デジタル サイネージなど、デバイスの Web ビューを使用する機能が動作するための前提条件です。

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: Web エンジンが無効になります。

On: Web エンジンが有効になります。

### Web エンジン リモートデバッグ

Web ページに問題が発生した場合は、リモート デバッグをオンにすることを推奨します。リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

使用後は、必ず RemoteDebugging をオフにしてください。

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 デバッグがオフに切り替わります。

On: リモート デバッグがオンに切り替わります。

### Web エンジン Http プロキシの使用

サービスの通信に HTTP プロキシを使用するかどうかを指定できるように、いくつかの [Http プロキシの使用 (UseHttpProxy)] 設定が用意されています。[Webエンジン Httpプロキシの使用 (WebEngine UseHttpProxy)] 設定は、デジタルサイネージ、API 駆動型 Web ビュー、Web アプリなど、Web ビューベースのすべての機能に適用されます。

この設定を有効にするには、[ネットワークサービス HTTP プロキシ (NetworkServices HTTP Proxy)] 設定を使用して、HTTP、HTTPS、および WebSocket トラフィック用のプロキシサーバーをセットアップする必要があります。

必要なユーザ ロール: ADMIN

デフォルト値: On

値スペース: Off/On

Off: サーバーとの直接通信をセットアップします (プロキシを使用しません)。

On: プロキシ経由の通信をセットアップします。

## 試験的設定

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

# 付録

## Touch 10 の使用方法

Touch 10 とその使用方法の詳細については、ビデオ会議デバイスのユーザーガイドを参照してください。

すべての機能がすべての製品で利用できるとは限りません。そのため、ここに示されているタッチボタンは、お使いのデバイスでは表示されない場合があります。

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

デバイス名またはアドレスをタップすると、[システム情報 (System Information)]、[設定 (Settings)]、[再起動 (Restart)] および [初期設定へのリセット (Factory Reset)] にアクセスできます。また、[コール転送 (Call forwarding)]、[スタンバイ (Standby)] および [着信拒否 (Do not disturb)] モードを有効にすることもできます。

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

[Webexに参加 (Join Webex)] をタップして、Webex ミーティングに参加します。

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

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

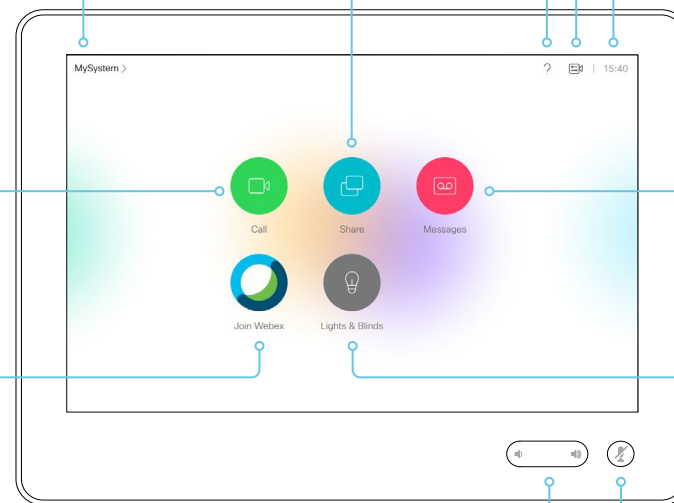
[カメラ (Camera)] アイコンをタップして、セルフビューとカメラ制御をアクティブにします。

時刻を指定します。

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

ユーザ インターフェイス拡張機能のエントリ ポイント (お使いのデバイスでは、これと異なる色、テキスト、アイコンのボタンがある場合があります)。

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



## USB カメラとしての Room Kit Mini の使用

このデバイスは USB カメラとして使用することができます。このモードでは次のコンポーネントが使用されます。

- ・ デバイスのカメラ
- ・ デバイスのマイク
- ・ デバイスのスピーカー
- ・ デバイスに接続された画面 (あれば)
- ・ サードパーティクライアント\*を使用しているコンピュータ

デバイスがコールサービス (クラウドまたはオンプレミス) に登録されている場合は、デバイスを通常のビデオ会議デバイスとして使用することも、USB カメラとして使用することもできます。どちらのモードになるかはデバイス自体が決定します。デバイスは、USB-C ポートに接続されたコンピュータにメディアをストリーミングしている場合のみ USB カメラモードになります。

デバイスがコールサービスに登録されていない場合でも、デバイスを USB カメラとして使用できます。

### セットアップと構成

管理者は、特別な設定を行ってデバイスを USB カメラとしてセットアップする必要はありません。

ただし、次のように一部のカスタマイズと USB カメラのみのセットアップに対する適用を行うことができます。

- ・ 初回のセットアップウィザードには、デバイスを USB デバイスとしてのみ使用するオプションが用意されています。このオプションを選択するときは、コールサービス (クラウドまたはオンプレミス) の登録を省略します。
- ・ デバイスがコールサービスに登録されていない場合は、[\[ユーザインターフェイス \(UserInterface\)\] > \[Webcam のみモード \(WebcamOnlyMode\)\]](#) 設定を使用して、ユーザインターフェイスを USB カメラのみのシナリオに適応させることができます。

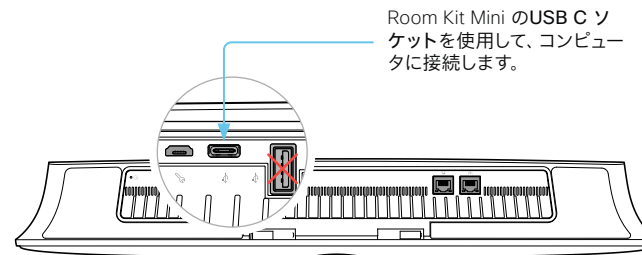
Touch 10 に対して完全なユーザインターフェイスを保持するか、またはコールサービスに登録されていない場合に不適切な要素を削除するかを選択できます。

\* たとえば、Microsoft Teams、Skype for Business、Slack、Zoom などがあります。Cisco は製品の発売前にこれらのクライアントを正常にテストしています。異なるソフトウェアバージョン間の互換性は、定期的にはテストされません。

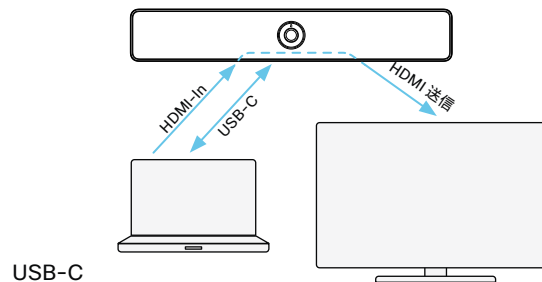
### USB-C に接続する

USB カメラとして使用するには、次に示すようにデバイスがコンピュータに接続されていて、接続がアクティブになっている必要があります (コンピュータがスリープモードになっていないことが必要です)。

Touch 10 からカメラと音量を制御できます。その他の機能は、使用しているコンピュータ上のサードパーティクライアントによって制御されます。



### デバイスに接続された画面の使用



#### USB-C

- ・ ビデオ会議デバイスのカメラおよびマイクからのビデオとオーディオを、コンピュータクライアントに出力
- ・ コンピュータクライアントからのオーディオを、ビデオ会議デバイスのスピーカーに出力

#### HDMI インおよび HDMI 送信:

- ・ コンピュータクライアント (相手先) からのビデオを、ビデオ会議デバイスを通じて画面に出力

### ビデオ解像度

サポートされるビデオ解像度

- ・ 720p
- ・ 1080p

### 最小要件

最小 USB バージョン:

- ・ USB 2.0

最小のコンピュータオペレーティングシステム:

- ・ Windows 7
- ・ OS X 10.6

## リモート モニタリングのセットアップ

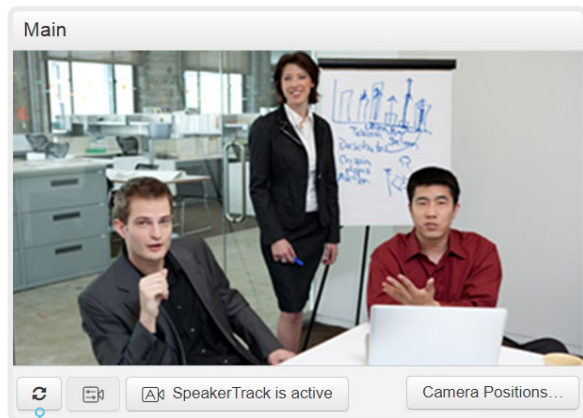
要件:

- ・ [リモート モニタリング (RemoteMonitoring)] オプション

リモート モニタリングは別の場所からデバイスを制御する場合に便利です。

入力ソースからのスナップショットが Web インターフェイスに表示されるため、部屋にいなくてもカメラ ビューをチェックしてカメラを制御できます。

有効にすると、スナップショットは約 5 秒おきに自動的に更新されます。



スナップショットを自動更新する

デバイスでリモート モニタリング オプションを設定するかどうかの確認

1. Web インターフェイスにログインします。
2. [ホーム (Home)] ページで、インストールされているオプションのリストに *RemoteMonitoring* が含まれているかどうかを確認します。  
リストにない場合、リモート モニタリングは使用できません。

リモート モニタリングを有効にする

*RemoteMonitoring* オプション キーをインストールします。オプション キーのインストール方法については、▶「[オプションキーの追加](#)」の章で説明しています。

リモート モニタリング オプションを有効にする場合は、プライバシーに関する地域の法律および規制を遵守する必要があります。また、システム管理者がカメラや画面を監視および制御する可能性があることを、デバイスのユーザーに適切な方法で通知してください。デバイス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追わないものとします。

スナップショットについて

ローカル入力ソース

デバイスのローカル入力ソースのスナップショットは [コール制御 (Call Control)] ページに表示されます。

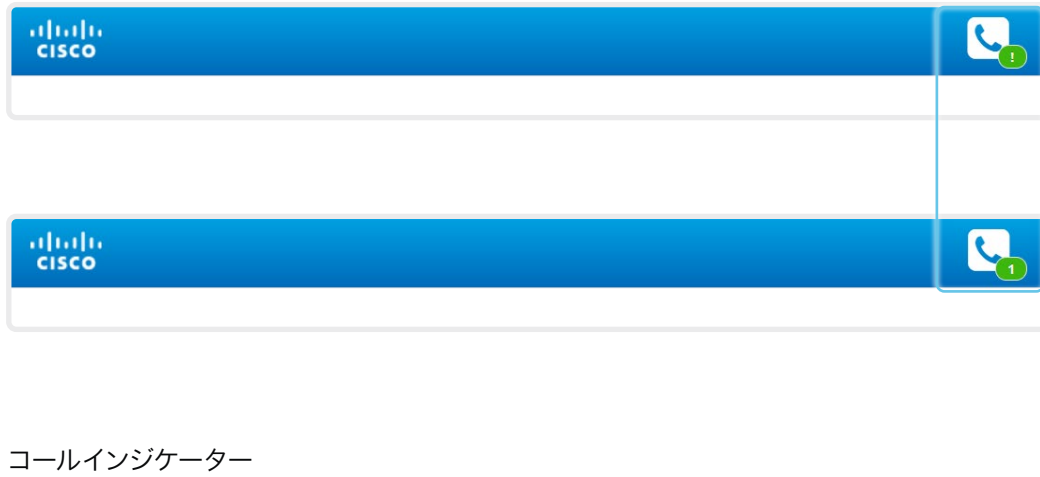
スナップショットは、デバイスがアイドル状態のときおよびコール中に表示されます。

遠端のスナップショット

通話中の場合、遠端カメラからのスナップショットも表示できます。これは、相手先デバイスでリモート モニタリング オプションが設定されているかどうかとは関係がありません。

遠端スナップショットは、コールが暗号化されていると表示されません。

## Web インターフェイスを使用したコール情報へのアクセスとコール応答



### 着信通知

[コールインジケータ (Call indicator)] をクリックし、コールの応答と拒否を行う [コール操作 (Call Control)] ページを開きます。

### デバイスがコール中

バッジはアクティブ コール数を示します。





### コールインジケータ

コール インジケータは、着信コールについて通知するため、およびデバイスがコール中であることを表示するために用意されています。

デバイスがアイドル状態の場合、コール インジケータは表示されません。

### コールの操作

[コール操作 (Call Control)] ページでは、コール操作に関する操作ボタンが表示されます。各ボタンを使用して次のことを実行します。

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



## 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)

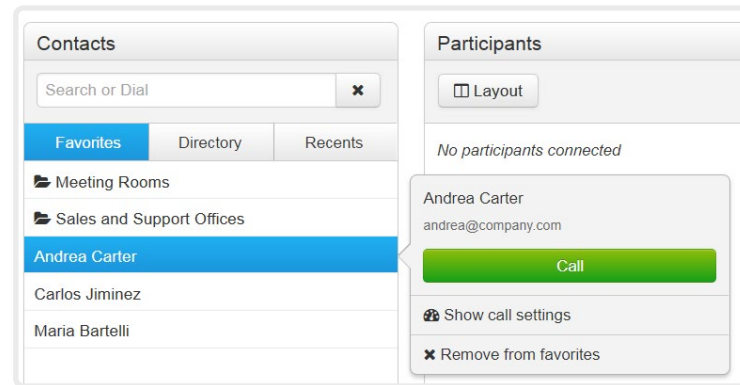
Web インターフェイスにログインし、[コール制御 (Call Control)] に移動します。

### コールの発信

**i** Web インターフェイスを使ってコールを開始した場合でも、コールに使用されるのはビデオ会議デバイス (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している PC ではありません。

- 正しいエントリを見つけるには、[お気に入り (Favorites)] リスト、[ディレクトリ (Directory)] リスト、または [発信履歴 (Recents)] リストに移動するか、あるいは [検索またはダイヤル (Search or Dial)] フィールドに 1 文字以上を入力します。該当する連絡先名をクリックします。
- 連絡先カードで [コール (Call)] をクリックします。

または、[検索して発信 (Search and Dial)] フィールドに完全な URI または番号を入力します。次に、URI または番号の横に表示される [コール (Call)] ボタンをクリックします。



\* 検索時には、入力内容に応じて、[お気に入り (Favorites)]、[ディレクトリ (Directory)]、および [履歴 (Recents)] リストの一致するエントリが表示されます。

### DTMF トーンの送信

アプリケーションが DTMF (デュアルトーン多重周波数) シグナリングを必要とする場合は、クリックしてキーパッドを開きます。



### コールの詳細の表示/非表示

情報ボタンをクリックすると、コールの詳細情報が表示されます。

もう一度ボタンをクリックすると情報が非表示になります。

### コールの保留および復帰

参加者を保留にするには、その名前の横にある [ ] ボタンを使用します。

コールを再開するには、保留中の参加者に表示される [ ] ボタンを使用します。

### コールの終了

コールまたは会議を終了するには、[全通話切断 (Disconnect all)] をクリックします。表示されるダイアログで選択内容を確認します。

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

## Web インターフェイスを使用したコールの発信 (2/2 ページ)

Web インターフェイスにログインし、[\[コール制御 \(Call Control\)\]](#) に移動します。

### 複数の相手に発信

ポイントツーポイントのビデオ コール (2 者間限定のコール) を拡張して、音声専用でもう 1 人の参加者を増やすことができます。

オプションで搭載される MultiSite 機能をデバイスで使用している場合は、自身を含めて最大 4 人までビデオ コール (会議) に参加できます。最初の参加者を呼び出したときと同じ手順で、次の会議参加者を呼び出してください。

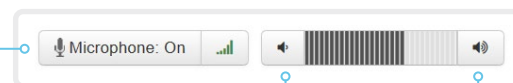
会議ブリッジを使用した複数のコールは、ビデオ会議デバイスでサポートされていても、Web インターフェイスではサポートされません。

### 音量の調整

#### マイクをミュートにする

[\[マイク: オン \(Microphone: On\)\]](#) をクリックして、マイクをミュートにします。すると、テキストが [\[マイク: オン \(Microphone: On\)\]](#) に変わります。

ミュートを解除するには、[\[マイク: オン \(Microphone: Off\)\]](#) をクリックします。



音量小

音量大

## Web インターフェイスを使用したコンテンツの共有

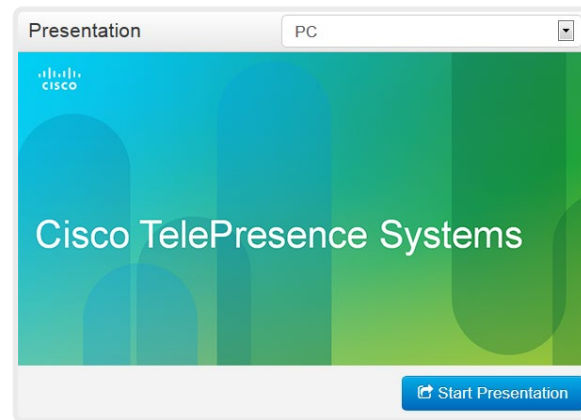
Web インターフェイスにログインし、[コール制御 (Call Control)] に移動します。

### コンテンツの共有

1. [プレゼンテーションの開始 (Start Presentation)] をクリックします。すると、テキストが [プレゼンテーションの停止 (Stop Presentation)] に変わります。

#### コンテンツ共有の停止:

共有している間に表示される [プレゼンテーションの停止 (Stop Presentation)] ボタンをクリックします。



#### スナップショット領域

選択されたプレゼンテーションソースのスナップショットが表示されます。

リモート モニタリングオプションが設定されているデバイス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

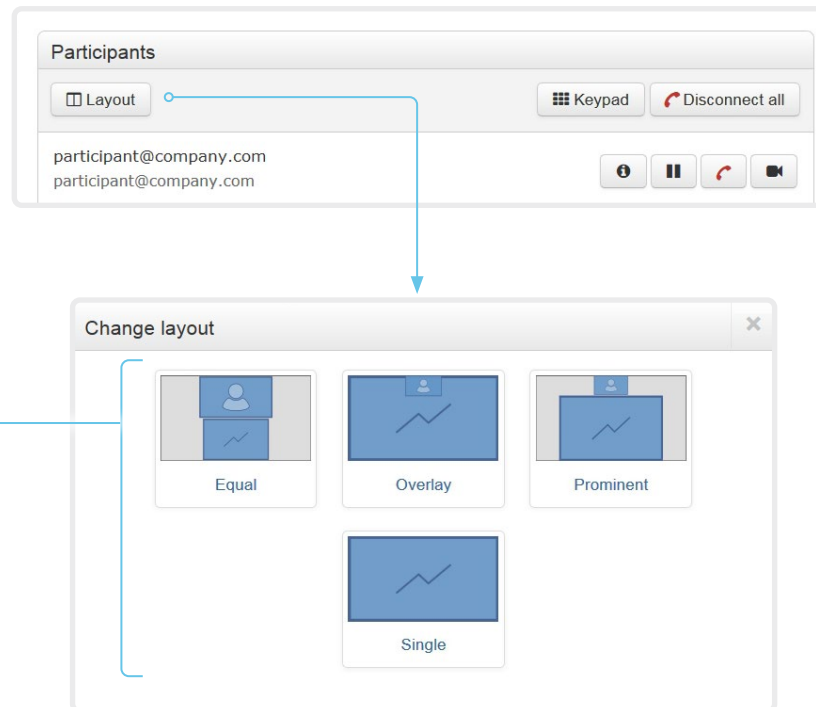
デバイスのビデオ入力にプレゼンテーションソースを接続できます。ほとんどの場合は PC がプレゼンテーションソースとして使用されますが、デバイスの設定によっては他のオプションを使用できる場合があります。

通話中に、他の参加者 (相手先) とコンテンツを共有できます。

コール (通話) 中でない場合は、コンテンツはローカルに表示されます。

## ローカル レイアウトの制御

Web インターフェイスにログインし、[コール制御 (Call Control)] に移動します。



### レイアウトの変更

[レイアウト (Layout)] をクリックし、表示されるウィンドウで望ましいレイアウトを選択します。\*

選択するレイアウトのセットは、デバイスの設定によって異なります。

レイアウトは、アイドル中でも通話中でも変更可能です。

### レイアウトについて

ここでいうレイアウトとは、プレゼンテーションとビデオを画面に表示するさまざまな方法のことです。会議の種類によって、レイアウトを変える必要があります。

通話や会議の参加者の数は、選択肢に反映されます。

\* 会議ブリッジにコールしている場合、参加者レイアウトの変更は、ビデオ会議デバイス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。

## ローカル カメラの制御

Web インターフェイスにログインし、[\[コール制御 \(Call Control\)\]](#) に移動します。

### 手動カメラ制御の前提条件

- [\[ビデオ \(Video\)\]](#) > [\[入力 \(Input\)\]](#) > [\[コネクタ n \(Connector n\)\]](#) > [\[カメラ制御 \(CameraControl\)\]](#) > [\[モード \(Mode\)\]](#) 設定が [オン (On)] になっている。
- カメラにパン、チルト、またはズーム機能が付いている。
- Best Overview がオフになっている。

### スナップショット領域

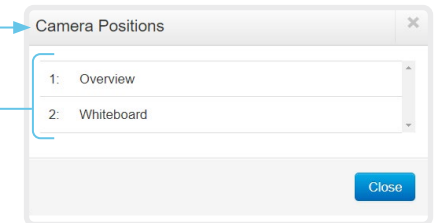
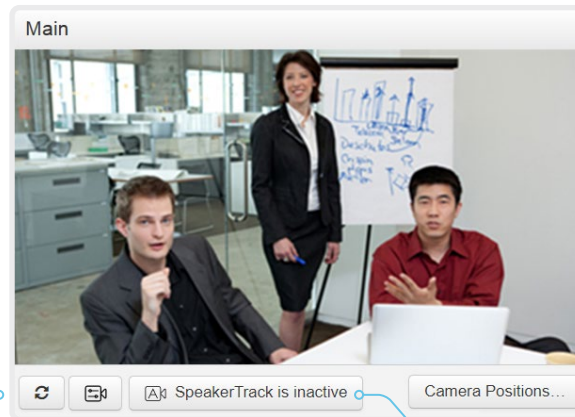
メイン入力ソースのスナップショットが表示されます。  
リモート モニタリングオプションが設定されているデバイスでのみ利用できます。

### スナップショットを自動更新する

### パン/チルト/ズーム コントロールを使用したカメラの移動

最高概要をオンにすると、カメラ制御は使用できません。

1. カメラ アイコンをクリックして、カメラ制御ウィンドウを開きます。  
室内からのビデオ スナップショットは、リモート モニタリング オプションが設定されているデバイスにのみ表示されます。
2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および - を使用します。  
関連するコントロールのみがウィンドウに表示されます。
3. [\[閉じる \(Close\)\]](#) をクリックして、ウィンドウを閉じます。

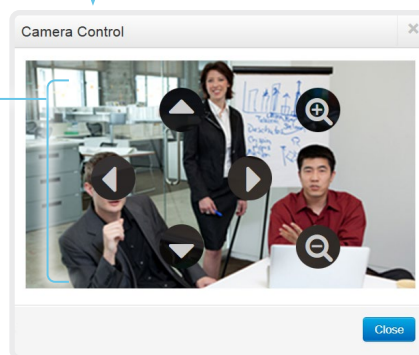


### カメラのプリセット位置への移動

1. [\[カメラの位置... \(Camera Positions...\)\]](#) をクリックして、使用可能なプリセットのリストを開きます。  
プリセットが定義されていない場合は、ボタンが無効になり、[\[プリセットなし \(No presets\)\]](#) と表記されます。
2. プリセットの名前をクリックすると、カメラがそのプリセット位置に移動します。
3. [\[閉じる \(Close\)\]](#) をクリックして、ウィンドウを閉じます。

### 最適な全体表示

クリックして Best Overview のオンとオフを切り替えます。



**i** Web インターフェイスを使用してプリセットを定義することはできません。デバイスのユーザーインターフェイスを使用する必要があります。

プリセットを選択すると、最高概要は自動的にオフになります。

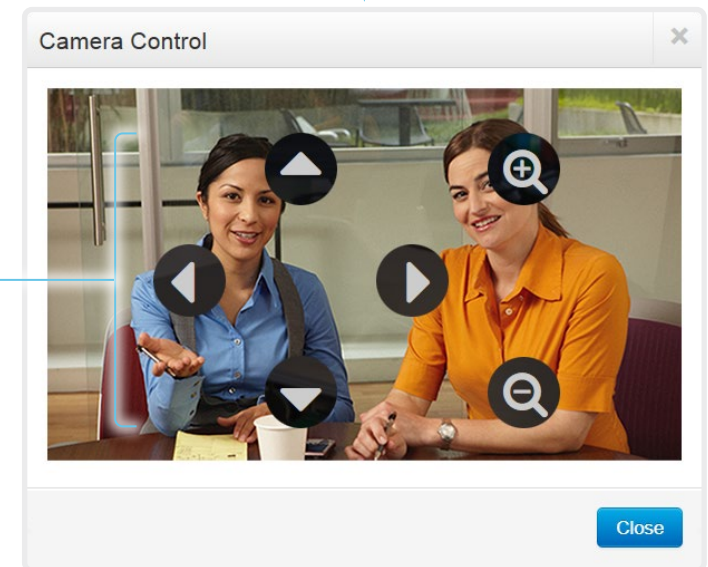
## 相手先カメラの制御

Web インターフェイスにログインし、[[コール制御 (Call Control)]] に移動します。

### 前提条件

以下の条件において、通話中にリモート参加者のカメラ（相手先）を制御できます。

- 相手先デバイスで [会議 (Conference)] > [相手先制御 (FarEndControl)] > [モード (Mode)] 設定が [オン (On)] になっている。
- 遠端カメラにパン、チルト、ズーム機能がある。関連する制御のみ表示される。
- 遠端カメラではスピーカーのトラッキングはオンになっていない。
- ローカル デバイスでリモート モニタリング オプションが設定されている。



### リモート参加者のカメラを制御

1. リモート カメラ制御ウィンドウを開くには、カメラのアイコンをクリックします。
2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および - を使用します。

遠端カメラの制御が許可されていない場合は、画面にコントロールが表示されません。

コールが暗号化されている場合、制御の背後の遠端スナップショットは表示されません。

## ルーム分析 (ページ 1 / 2)

ルーム分析機能は、会議室からのいくつかの変数を使用します。また、それらの変数を再利用して、時間経過やコールのたびに部屋の使用率を分析します。

### 人の存在の検出

このデバイスは、人が室内にいるかどうかを見つける機能を備えています。室内に人がいるかどうかを検知するには最低 2 分かかります。部屋が空室になった後、ステータスを変更するまで最大 2 分かかることがあります。

この機能は、超音波に基づいています。室内にいた人物の記録を保持することはなく、人が部屋にいたかどうかだけを検知します。

Web インターフェイスから人の存在の検出をオンまたはオフにできません。Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) > [\[ルーム分析 \(RoomAnalytics\)\]](#) > [\[人の存在の検出 \(PeoplePresenceDetector\)\]](#) に移動します。

### 人数のカウント

顔検出を使用して、デバイスで室内の人数を特定できます。室内にいた人物の記録を保持することはなく、顔の平均数だけを検知します。カメラに顔を向けていない人はカウントされません。室内に物体や写真がある場合、これらも顔として検知され、カウントされる可能性があります。

信頼性の高い平均数を得るために、コール時間の長さは最低 2 分必要です。2 分未満のコールと人数のカウントが無効にされたコールでは、通話履歴を取得すると「N/A」が表示されます。

デフォルトでは、デバイスはコール中またはセルフビュー画像を表示しているときにのみ人数をカウントします。

非通話中の人をカウントするように選択できます。オンにすると、デバイスは、デバイスがスタンバイ モードでない場合に人数をカウントします。セルフ ビューがオフであっても、これは非通話中の人数を含みます。Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) > [\[ルーム分析 \(RoomAnalytics\)\]](#) > [\[非通話中人数カウント \(PeopleCountOutOfCall\)\]](#) に移動します。

### ステータス

人の存在および人のカウントに関する特定の瞬間のステータスを確認することができます。Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[ステータス \(Status\)\]](#) > [\[ルーム分析 \(RoomAnalytics\)\]](#) に移動します。

### 診断

ユーザーインターフェイスコントローラからスピーカートラックの診断モードを有効にすると、リアルタイムの人数のカウントが画面上に表示されます。セルフビューをオンにし、ユーザー インターフェイスの最上部にあるデバイス名またはアドレスをタップして、[\[設定 \(Settings\)\]](#) メニューを開きます。[\[問題と診断 \(Issues & diagnostics\)\]](#) をタップし、[\[SpeakerTrack の診断 \(SpeakerTrack diagnostics\)\]](#) をオンにします。

### 通話履歴コマンド

コール後に、通話履歴コマンドから人々の平均数の値を抽出できます。

- `xCommand CallHistory Get DetailLevel: Full`

通話履歴コマンドは、API (Application Programming Interface) から使用できます。詳細については、お使いの製品の API リファレンス ガイドを参照してください。

リンク: [▶ https://www.cisco.com/go/room-docs](https://www.cisco.com/go/room-docs) [英語]

## ルーム分析 (ページ 2 / 2)

### 環境ノイズ レポート

このデバイスでは、室内の定常環境雑音レベルをレポートできます。レポートされた値はA荷重デシベル値(dBA)で、人間の耳の応答に反響します。この機能に関連するすべてのシグナリング処理はローカルで、転送されるデータは算出されたノイズレベルだけです。

この値はノイズレベルの異常な変化の検出に使用できます。このような変化は、室内で仕事をしている人にとっては不快なノイズを引き起こす場合があります。施設管理はこの問題をトラブルシューティングするために迅速に介入できます。

Web インターフェイスから周囲ノイズの検出をオンまたはオフにできます。Web インターフェイスにサインインし、[\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) > [\[ルーム分析 \(RoomAnalytics\)\]](#) > [\[環境雑音の予測 \(AmbientNoiseEstimation\)\]](#) > [\[モード \(Mode\)\]](#) に移動します。

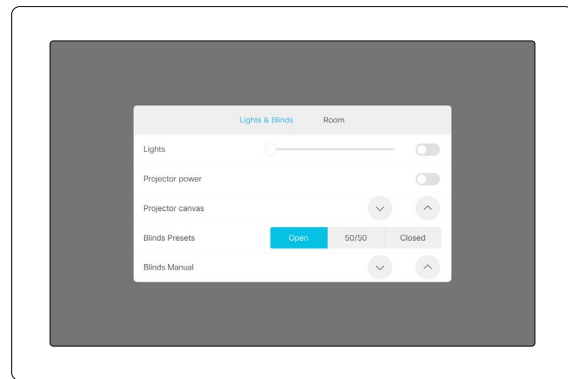


カスタマイゼーション

## ビデオ会議デバイスの Touch 10 ユーザーインターフェイスのカスタマイズ (ページ 1 / 2)

ユーザ インターフェイスをカスタマイズして、照明やブラインドなど、会議室内の周辺機器を制御したり、マクロをトリガーしてビデオ会議デバイスの動作を変更したりできます。

これにより、制御システムの機能と、ビデオ会議デバイスの使いやすいユーザ インターフェイス (Touch 10) を強力に組み合わせることができます。



室内制御パネルの例

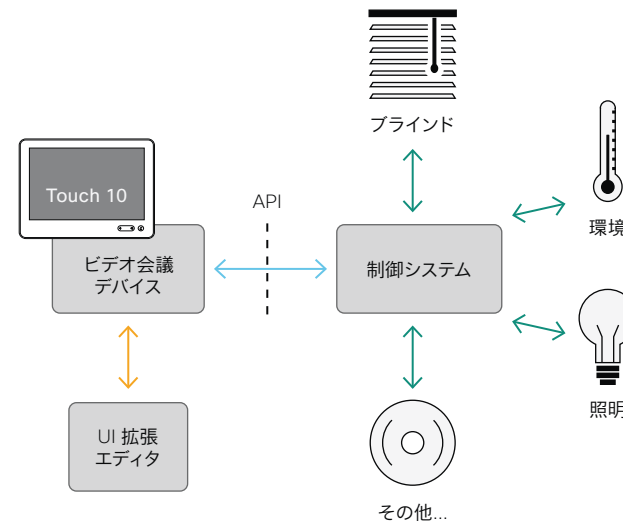
UI 拡張エディタ (以前の室内制御エディタ) を使用してカスタムのユーザ インターフェイス パネルとアクション ボタンを設計する方法、およびビデオ会議デバイスの API を使用してコントロールとアクションをプログラミングする方法の詳細については、カスタマイズ ガイドをご覧ください。次のリンクからアクセスできます。

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

### 室内制御アーキテクチャ

Touch 10 コントローラが付属するシスコのビデオ会議デバイスと、コントロール システムが必要です。制御システムは、ハードウェア ドライブや周辺機器を備えた Crestron や AMX などの他社製システムである場合もあります。これはビデオ会議デバイスではなく、周辺機器を制御するコントロール システムです。

コントロール システムをプログラミングするときは、ビデオ会議デバイスのユーザ インターフェイス上のコントロールに接続するために、ビデオ会議デバイスの API (イベントとコマンド) を使用する必要があります。



室内制御の概略図

ビデオ会議デバイスのマクロ フレームワークは、コントロール システムとしても使用できます。この場合、コントロール システムはデバイスの API を使用して、短縮ダイヤル、言語の選択、カスタマイズされたシステムのリセットなど、あらゆる種類のローカル機能をトリガーすることができます。

カスタマイゼーション

## ビデオ会議デバイスの Touch 10 ユーザインターフェイスのカスタマイズ (ページ 2/2)

### UI 拡張エディタ

#### 無料のエディタ

ビデオ会議デバイスのソフトウェアには、ドラッグアンドドロップ方式の使いやすいエディタが無償で付属しています。カスタムのユーザ インターフェイス拡張機能 (アクション ボタン、および室内制御などのカスタム パネル) を作成するには、このエディタを使用します。

Web インターフェイスにサインインし、[\[統合 \(Integration\)\]](#) > [\[UI 拡張エディタ \(UI Extensions Editor\)\]](#) に移動します。

- エディターがデバイスの Web インターフェイスで直接開きます。  
新しいパネルまたはアクション ボタンを作成してデバイスにプッシュし、その結果をすぐにユーザ インターフェイスで確認することができます。
- [\[エディタ \(Editor\)\]](#) メニュー (☰) をクリックし、[\[エディタをダウンロード \(Download the Editor\)\]](#) を選択すると、ハード ドライブからローカルにブラウザで実行できるスタンドアロン バージョンを入手できます。  
これにより、デバイスに接続しなくてもカスタム ユーザ インターフェイスを作成できます。後でファイルをエクスポートおよびインポートして、ローカル バージョンとデバイスの間で作業を移動することができます。

#### プレビュー機能

エディタは、カスタム インターフェイスがどのようにユーザ インターフェイスに表示されるか確認するためのプレビュー機能も提供します。

プレビュー機能ではカスタム パネルがソフトウェア的に完全に再現されるため、コントロールをクリックすると、実際の Touch 10 ユーザ インターフェイスでコントロールを選択した場合と同じアクションが実行されます。

したがって、実際の Touch 10 ユーザ インターフェイスで有効にすることなく、プレビュー機能を使用してお使いの統合をテストできます。リモートの場所からデバイスのカスタム パネルを使用することもできます。

\* UI 拡張エディタおよびプログラミングに必要な API コマンドにアクセスするには、ROOMCONTROL、INTEGRATOR、または ADMIN ユーザ ロールを持つユーザが必要です。

カスタマイゼーション

## マクロを使用したビデオ会議デバイスの動作のカスタマイズ

マクロにより、デバイスで実行するコードの独自のスニペットを作成できます。言語は、アロー関数、promise および class などの機能をサポートする JavaScript/ECMAScript 6 です。

インテグレータは、マクロ フレームワークを利用して、個別の顧客要件に応じてデバイスの動作を調整するスクリプトを作成できます。インテグレータが行える作業には、独自の機能または機能のバリエーションの実装、特定の設定または再設定の自動化、機能のカスタム テストやモニタリングの作成などがあります。

マクロの使用とカスタム ユーザ インターフェイス パネル (UI 拡張機能) の作成を組み合わせることで、カスタマイズされたローカル機能をトリガーするようにユーザ インターフェイス (Touch 10) を変更できます。以下に例を示します。

- ・ 短縮ダイヤル ボタンの追加
- ・ すべての設定を好みのデフォルト セットアップに戻すためのルームリセットボタンの追加

マクロの詳細およびデバイスに搭載されているマクロ エディタの使用法については、*カスタマイズ ガイド*をご覧ください。次のリンクからアクセスできます。

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

### デバイスでのマクロの使用許可

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

- ・ [\[マクロ \(Macros\)\] > \[モード \(Mode\)\]](#) を [オン (On)] に設定します。

この設定が [オフ (Off)] の場合にマクロ エディタを起動しようとすると、ポップアップ メッセージが表示されます。[\[マクロの有効化 \(Enable Macros\)\]](#) をタップして応答した場合は [\[マクロ \(Macros\)\] > \[モード \(Mode\)\]](#) 設定が自動的に [オン (On)] に変更され、エディタが起動します。

### マクロ エディタの起動

Web インターフェイスにサインインし、[\[統合 \(Integration\)\] > \[マクロ エディタ \(Macro Editor\)\]](#) に移動します。

オフラインで使用可能なエディタのスタンドアロン バージョンは提供されていません。

### マクロ エディタ

マクロ エディタは、以下のことができる強力なツールです。

- ・ 変更したり、そのまま使用したり、または自身のマクロを記述する際のヒントとして使用したりするコードの例をロードできます。
- ・ 詳細なマクロ記述チュートリアルを用意しているので、参照してください。コードの例についても、より詳しく説明しています。
- ・ 独自のマクロを記述して、デバイスにアップロードできます。
- ・ マクロは、個別に有効または無効にできます。
- ・ マクロを実行したときの動作は、組み込みのログ コンソールで確認できます。

\* マクロ エディタにアクセスするには、ADMIN ユーザ ロールを保持しているユーザが必要です。

カスタマイゼーション

## ユーザインターフェイスからのデフォルトボタンの削除

通話 または 共有などのデフォルトボタンを使用しない使用例もあります。このような使用しないボタンは混乱を引き起こす場合があります。このような場合、使用しないボタンをユーザインターフェイスから削除できます。その場合もカスタム UI ボタンは表示できます。カスタムボタンの追加中にデフォルトボタンを削除すると、ユーザインターフェイスを完全にカスタマイズできるようになります。

たとえば、誰もこのデバイスからコンテンツや通話を共有しない場合は、[通話 (Call)] ボタンと [共有 (Share)] ボタンを削除できます。代わりに、実行する予定のタスク用のカスタム ボタンとパネルを追加します。

### 構成

ユーザ インターフェイスからデフォルトのボタンを削除するには、次の設定を使用します。設定は、デバイスの Web インターフェイスと API の両方から利用できます。

- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [開始 (Start)]: デフォルトの [コール (Call)] ボタンを削除します (ディレクトリ、お気に入り、コール履歴リストも含まれます)。コール中に表示される、参加者の [追加 (Add)] ボタンも削除されます。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [Webexに参加 (JoinWebex)]: Webex ミーティングに参加するためのデフォルトのボタンを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [共有 (Share)] > [開始 (Start)]: 通話中および通話中以外の両方で、コンテンツの共有およびプレビュー用のデフォルトユーザ インターフェイスを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [ビデオミュート (VideoMute)]: デフォルトの [ビデオをオフにする (Turn video off)] ボタンを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [通話 (Call)] > [終了 (End)]: 通話終了 ボタンを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [コール中制御 (MidCallControls)]: コール中の [保留 (Hold)]、[保留解除 (Resume)]、および [転送 (Transfer)] ボタンを削除します。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [コール (Call)] > [キーパッド (Keypad)]: 通話中の [キーパッド (Keypad)] ボタンを削除します。このボタンは、DTMF 入力に使用できるキーパッドを開きます。
- [ユーザインターフェイス (UserInterface)] > [機能 (Features)] > [すべて非表示 (HideAll)]: すべてのデフォルトボタンを削除します。カスタム ボタンは削除されません。



設定はボタンだけを削除し、機能などは削除しません。共有 ボタンをユーザインターフェイスから削除しても、Proximity を使用してコンテンツを共有できます。

### 解説場所

ボタンの削除方法およびユーザインターフェイスのカスタマイズ方法については [カスタマイズガイド](#)を参照してください。次のリンクからアクセスできます。

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

カスタマイゼーション

## サードパーティ USB 入力デバイスの使用

サードパーティ製の USB 入力デバイスを使用して、ビデオ会議デバイスの特定の機能を制御できます。USB ドングルや USB キーボードでの Bluetooth リモート制御はこのような入力デバイスの一例です。

この機能は、利便性を高めるために、ビデオ会議デバイスのユーザインターフェイスの機能を補完することを目的としています。ユーザインターフェイスを置き換えるものではありません。

アプリケーションの例

- ・ クラスルームや講義で、小型のリモコンを使用してビデオ会議デバイスをスタンバイ モードから復帰させることができます。また、表示する入力ソースを選択するためにリモート制御を使用するのも便利です。
- ・ タッチインターフェイスを使用できない状況で、カメラビュー（パン、チルト、ズーム）を制御します。例えば、病院の手術室。

### 機能の概要

USB 入力デバイスのボタンを押すと、API でイベントが生成されます。マクロまたはサードパーティの制御デバイスは、こういったイベントをリッスンして応答することが可能です。この動作は、カスタム UI ボタン (UI 拡張機能) の動作と似ています。ウェブフックを使って、直接SSH セッションでイベントをリッスンすることも可能です。

アクション選択からすぐに利用できるアクションのライブラリはありません。ご自身で、イベントに対する応答として行うアクションを定義して実装する必要があります。次に例を示します。

- ・ [音量アップ (Volume Up)] キーが押されたら、ビデオ会議デバイスの音量を上げる。
- ・ [スリープ (Sleep)] キーが押されたら、ビデオ会議デバイスをスタンバイモードにする。

### 設定、イベント、およびステータス

USB 入力デバイスのサポートはデフォルトで無効になっています。[周辺機器 > InputDevice > モード](#) を オンに設定することで明示的に有効にします。

ボタンを押してから離すと、押されたおよびリリースされたイベントが作成されます：

```
*e UserInterface InputDevice Key アクションキー: &lt;キーの名前>
*e UserInterface InputDevice Key アクションコード: &lt;キーの ID>
*e UserInterface InputDevice Key Action Type: 押された
** end
*e UserInterface InputDevice Key アクションキー: &lt;キーの名前>
*e UserInterface InputDevice Key アクションコード: &lt;キーの ID>
*e UserInterface InputDevice Key Action Type: リリースされた
** 終了
```

イベントをリッスンするには、InputDevice イベントからのフィードバックを登録する必要があります。

```
xFeedback Register /event/UserInterface/InputDevice
** end
```

ビデオ会議デバイスでサードパーティの入力デバイスが検出されると、その入力デバイスがビデオ会議デバイスの [\[ユーザインターフェイス \(UserInterface\)\] > \[周辺機器 \(Peripherals\)\] > \[接続されているデバイス \(ConnectedDevice\)\]](#) ステータスに表示されます。入力デバイスは複数のデバイスとして報告される場合があります。

### 必要な工具

- ・ Cisco Webex Room、Desk、または DX シリーズのデバイス。
- ・ デバイス自体を USB キーボードとしてアダプタ化するサードパーティ入力デバイス。例えば、USB ドングル付きの Bluetooth リモート制御。

### 解説場所

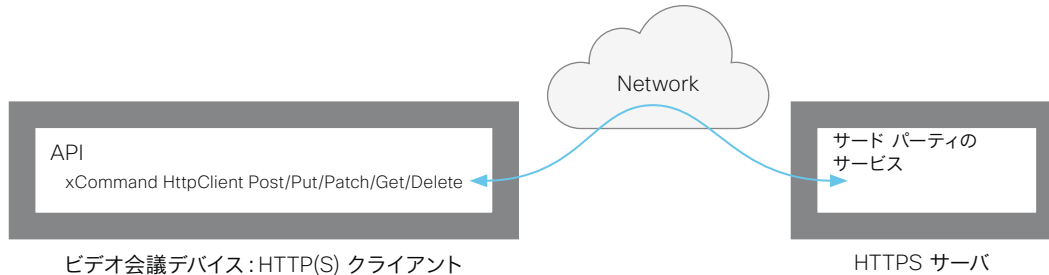
サードパーティ入力デバイスの利用についての詳細は、[カスタマイズガイド](#)をご覧ください。次のリンクからアクセスできます。

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

Cisco support (TAC) はマクロを含む、サードパーティコードのデバッグに対応していません。マクロやサードパーティコードについてのヘルプが必要な場合は、▶ [シスコ コラボレーション開発者コミュニティ](#)を確認してください。

カスタマイゼーション

## HTTP(S) 要求の送信



HTTP(S) 要求機能を使用すると、ビデオ会議デバイスから HTTP(S) サーバに任意の HTTP(S) 要求を送信できます。さらに、デバイスはサーバから送信された応答を受信します。このデバイスは、POST、PUT、PATCH、GET、および DELETE メソッドをサポートします。

マクロを使用することで、いつでもデータを HTTP(S) サーバに送信できます。送信するデータを選択して、必要に応じて構造化することができます。それにより、すでに確立されているサーバにデータを適合させることができます。

セキュリティ対策:

- HTTP(S) 要求機能は、デフォルトでは無効になっています。システム管理者は `HttpClient > モード` を オンに設定することでこの機能を明示的に有効にする必要があります。
- システム管理者は `HttpClient > AllowHTTP` を 偽に設定することで HTTP の使用を防ぐことができます。
- システム管理者は、デバイスがデータを送信可能な先である HTTP(S) サーバのリストを指定することができます。
- 同時 HTTP(S) 要求の数は制限されています。

### 許可されている HTTP(S) サーバのリスト

システム管理者はコマンドを使用して最大 10 の許可されている HTTP(S) サーバ (ホスト) のリストを設定し維持できます:

- `xCommand HttpClient` はホスト名追加表現を許可します: `<HTTP(S) サーバのホスト名または IP アドレスに一致する正規表現>`
- `xCommand HttpClient Allow Hostname Clear`
- `xCommand HttpClient Allow Hostname List`
- `xCommand HttpClient Allow Hostname Remove Id:` `<リスト内のエントリーの ID>`

リストが空でない場合、HTTP(S) リクエストをリスト内のサーバにだけ送信できます。リストが空の場合、リクエストを任意の HTTP(S) サーバに送信できます。

許可されているサーバのリストに対するチェックは、非セキュア (HTTP) およびセキュア (HTTPS) なデータ転送の両方で実行されます。

### 証明書の検証なしの HTTPS の使用

HTTPS 経由で要求を送信する場合、ビデオ会議デバイスはデフォルトで HTTPS サーバの証明書を確認します。HTTPS サーバ証明書が有効でない場合、エラーメッセージが表示されます。デバイスはそのサーバにデータを送信しません。

証明書が検証される HTTPS の使用を推奨します。証明書の検証が不可能な場合、システム管理者は `[HTTP クライアント (HttpClient)] > [セキュアでない HTTPS を許可 (AllowInsecureHTTPS)]` を [オン (On)] に設定できます。これにより、サーバの証明書を検証せずに HTTPS を使用することができます。

### HTTP(S) 要求の送信

HTTP(S) 要求機能が有効になったら、次のコマンドを使用して要求を HTTP(S) サーバに送信できます。

```
xCommand HttpClient <メソッド>
[AllowInsecureHTTPS: <true/false>]
[Header: <ヘッダー テキスト>]
[ResponseSizeLimit: <最大応答サイズ>]
[ResponseBody: <None/PlainText/Base64>]
[Timeout: <タイムアウト時間>]
Url: <要求の送信先 URL>
```

<メソッド> は、Post、Put、Patch、Get、Delete のいずれかです。

Post、Put、および Patch コマンドは複数行コマンドです。複数行コマンドの使用方法和、コマンド パラメータの詳細な説明については、API ガイドをお読みください。

### 解説場所

HTTP(S) Post リクエストについての詳細情報は [カスタマイズガイド](#)にあります。次のリンクにアクセスします。

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



Web ビュー ベースの機能

## デジタル サイネージ

デジタル サイネージを使用すると、デバイスがハーフウェイク状態のときにカスタム コンテンツ (Web ページ) を表示できます。デジタル サイネージは、広告コンテンツを表示してブランドを宣伝するだけでなく、訪問者や社内の従業員情報、ダッシュボード、またはカレンダーを表示するのに最適な方法です。

カスタム コンテンツは、ハーフウェイク状態の従来の背景画像と情報を置き換え、常にフル スクリーンで表示されます。Web ウィンドウまたはタブ 1 つのみがサポートされます。Web ページが新しいウィンドウまたはタブでページを開こうとすると、現在のページは置き換えられます。

キャッシュ、Cookie、ローカル ストレージなどのデータは、デバイスの再起動時に自動的に消去されることはありません。データを削除するには、ストレージ削除コマンドを使用する必要があります。

- xCommand WebEngine DeleteStorage [Type: Webengine]

Web ページがサポートされていない場合、デバイスはすぐに通常のハーフウェイク モードになります。詳細情報は、デバイスの Web インターフェイスの [\[メンテナンス \(Maintenance\)\]](#) > [\[診断 \(Diagnostics\)\]](#) ページで確認できます。

## デジタル サイネージのセットアップ

1. Web インターフェイスにサインインして、[\[セットアップ \(Setup\)\]](#) > [\[設定 \(Configuration\)\]](#) に移動します。
2. [\[Webエンジン \(WebEngine\)\]](#) > [\[モード \(Mode\)\]](#) を [オン (On)] に設定して、Web エンジンを有効にします。
3. [\[スタンバイ \(Standby\)\]](#) > [\[サイネージ \(Signage\)\]](#) > [\[モード \(Mode\)\]](#) を [オン (On)] に設定して、デジタル サイネージを有効にします。
4. [\[スタンバイ \(Standby\)\]](#) > [\[サイネージ \(Signage\)\]](#) > [\[Url\]](#) に、表示する Web ページの URL を入力します。
5. Web ページは、デバイスがスタンバイ モードになる前に表示されます。Web ページの表示時間を決定するには、次の設定を使用します。

[\[スタンバイ \(Standby\)\]](#) > [\[モード \(Mode\)\]](#): Off に設定すると、デバイスはスタンバイ モードになりません (非推奨)。On に設定すると、[\[スタンバイ \(Standby\)\]](#) > [\[遅延 \(Delay\)\]](#) がタイムアウトしたときにデバイスがスタンバイ モードになります。

[\[スタンバイ \(Standby\)\]](#) > [\[遅延 \(Delay\)\]](#): デバイスがスタンバイ モードになるまでに Web ページを表示する時間 (分単位) を定義します。

[\[スタンバイ \(Standby\)\]](#) > [\[モーション検知復帰 \(WakeUpOnMotionDetection\)\]](#): On に設定すると、人が室内に入ったときにデバイスが自動的にスタンバイから復帰して Web ページを表示します。Off に設定すると、人が室内に入ってもデバイスは影響を受けません。

その他のデジタル サイネージ設定:

- 音声が含まれる Web ページで音声を再生するかどうかを決定します。  
[\[スタンバイ \(Standby\)\]](#) > [\[サイネージ \(Signage\)\]](#) > [\[音声 \(Audio\)\]](#)
- Web ページを一定の間隔で強制的に更新します。これは、Web ページが自動更新されない場合に便利です。  
[\[スタンバイ \(Standby\)\]](#) > [\[サイネージ \(Signage\)\]](#) > [\[更新間隔 \(RefreshInterval\)\]](#)

## Web エンジン

Web ビュー ベースの機能はすべて、Web エンジンを使用しています。このため、Web ビュー ベースの機能を使用するには、Web エンジンが有効になっている必要があります。

Web エンジンは、V8 JavaScript を使用した Chromium/Qt WebEngine に基づいています。Chromium バージョンは定期的に更新されますが、Chrome ラップトップ バージョンよりも古いバージョンである可能性があります。

次の機能はサポートされていません。PDF、WebGL WebRTC、パスワード マネージャー、プラグイン、ファイルのダウンロードとアップロード、通知。

## リモート デバッグ

Web ページに問題が発生した場合は、リモート デバッグをオンにすることができます。

[\[Webエンジン \(WebEngine\)\]](#) > [\[リモート デバッグ \(RemoteDebugging\)\]](#)

リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

## プロキシの使用

Web ビューベースの機能で HTTP プロキシを使用するようにデバイスを設定できます。

[\[ネットワークサービス \(NetworkServices\)\]](#) > [\[HTTP\]](#) > [\[プロキシ \(Proxy\)\]](#)

さらに、次の設定をオンにする必要があります。

[\[Webエンジン \(WebEngine\)\]](#) > [\[Httpプロキシの使用 \(UseHttpProxy\)\]](#)

Web ビュー ベースの機能

## API 駆動型の Web ビュー

Web ビューは、API コマンドを使用して開いたり閉じたりすることができます。インテグレータは、サードパーティ統合またはマクロを作成するときに、これらのコマンドを使用できます。インテグレータは、外部イベントに基づいて読み込む URL を決定します。たとえば、企業の重要な通知を表示できます。

Web ビューは全画面表示になっており、15 分後にタイムアウトになるか、または API コマンドをコールしてビューを閉じます。

Web ビューを開く:

- `xCommand UserInterface WebView Display Url: &lt;url>`

Web ビューを閉じる:

- `xCommand UserInterface WebView Clear`

キャッシュ、Cookie、ローカル ストレージなどのデータは、セッションが終了すると自動的に消去されます。

インテグレータは、API 駆動型 Web ビュー、マクロ、およびカスタム ボタンを組み合わせることで、タッチ スクリーンのないデバイス向けにも対話型のソリューションを作成できます。Touch コントローラのボタンをタップすると、メイン画面にさまざまな Web ビューが表示されます。たとえば、基本的なヘルプ ページを開いて参照したり、説明ビデオを表示したりできます。

## Web エンジン

Web ビュー ベースの機能はすべて、Web エンジンを使用しています。このため、Web ビュー ベースの機能を使用するには、Web エンジンが有効になっている必要があります。

Web エンジンは、V8 JavaScript を使用した Chromium/Qt WebEngine に基づいています。Chromium バージョンは定期的に更新されますが、Chrome ラップトップ バージョンよりも古いバージョンである可能性があります。

次の機能はサポートされていません。PDF、WebGL WebRTC、パスワード マネージャー、プラグイン、ファイルのダウンロードとアップロード、通知。

### リモート デバッグ

Web ページに問題が発生した場合は、リモート デバッグをオンにすることができます。

```
[Webエンジン (WebEngine)] > [リモート
デバッグ (RemoteDebugging)]
```

リモート デバッグを使用すると、Chrome 開発者コンソールにアクセスして、Web ページの潜在的な問題を識別することができます。有効にすると、画面の下部にバナーが表示され、モニタされる可能性があることをユーザに警告します。ヘッダには、開発者コンソールを開くためにローカルの Chrome ブラウザに入力可能な URL も表示されます。

### プロキシの使用

Web ビューベースの機能で HTTP プロキシを使用するようにデバイスを設定できます。

```
[ネットワークサービス
(NetworkServices)] > [HTTP] >
[プロキシ (Proxy)]
```

さらに、次の設定をオンにする必要があります。

```
[Webエンジン (WebEngine)] >
[Httpプロキシの使用 (UseHttpProxy)]
```



## 入力ソースの構成 (1/2 ページ)

デバイスの API を使用して、単一のメインのビデオ ストリームに最大 4 つの入力ソースを結合できます。

組み合わせることのできる入力ソースの最大数はデバイスによって異なります。

ビデオ会議デバイス	組み合わせることができる異なる入力ソースの最大数
Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2	2
Codec Plus, Room 55, Room 55 Dual, Room 70, Desk Pro	3
SX80, MX700, MX800, Codec Pro, Room 70 G2	4
SX10, DX70, DX80	利用不可

## ソース構成

### 構成レイアウト

3 つのレイアウトから選択できます。

- ・ 同等 (Equal)
- ・ プロミネント (Prominent)
- ・ PIP (2 つの入力ソースを構成するときのみ使用可能)

PIP 位置をコーナーの一つに変更できます。PIP のサイズは通常でも大型でも可能です。

構成とレイアウトは、コールとコール外の両方でいつでも変更できます。

### 自画面

自画面は、遠端に送信されるのと同じ構成イメージを示します。

### 個別カメラ制御

API コマンド (xCommand Camera \*) を使用して、個々のカメラを制御することができますが、ユーザ インターフェイス上の制御は使用できません。

ユーザ インターフェイスでカメラを選択すると、メインのビデオ ストリームが構成されたビデオ ストリームから、選択されたカメラからの単一のストリームに切り替えられます。

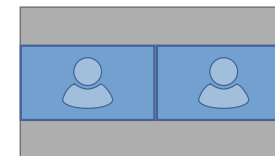
### オン デマンドによる構成およびレイアウトの変更

入力ソース構成は API コマンドを使用してのみ利用可能です。専用のユーザ インターフェイスは提供されません。

構成とレイアウトをオン デマンドで簡単に変更できるようにするには、マクロを使用してカスタムのユーザ インターフェイス パネル (UI 拡張機能) を作成することを推奨します。

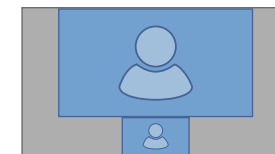
## レイアウト

### 同等 (Equal)



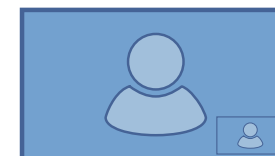
ソースの数: 2

### プロミネント (Prominent)



ソースの数: 2

### ピクチャインピクチャ (PIP)



右下隅



右下隅、大型 PIP

## 入力ソースの構成 (2/2 ページ)

### API コマンド

```
xCommand Video Input SetMainVideoSource
ConnectorId: &lt;1..n> SourceId:
&lt;1..m> Layout: &lt;Equal, PIP,
Prominent> PIPPosition &lt;LowerLeft,
LowerRight, UpperLeft, UpperRight>
PIPSize &lt;Auto, Large>
```

値は次のとおりです。

入力ソースは、(ConnectorId) に接続されている物理コネクタか、論理ソース識別子 (SourceId) のいずれかによって識別できます。同じコマンド内で異なる識別子を混合することはできません。ConnectorId または SourceId のいずれかを使用してください。これらの識別子は、[ビデオ入力コネクタ (Video Input Connector)] および [ビデオ入力ソース (Video Input Source)] のステータスで見つけることができます。

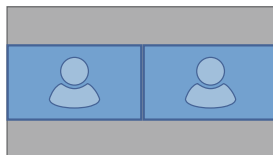
Equal と PIP、さらにプロミネント (レイアウト) の違いは、サイドバーに表示されます。

PIP 位置をコーナーの一つに変更できます。PIP のサイズは通常 (自動) でも大型でも可能です。

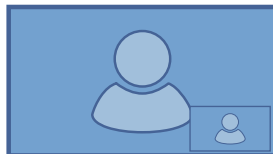
詳細については、API ガイドを参照してください。

### 例

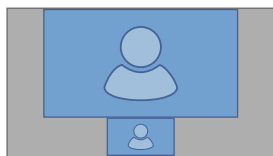
```
xCommand Video Input SetMainVideoSource ConnectorId: 1 ConnectorId: 2 Layout: Equal
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: PIP PIPPosition: LowerRight PIPSize: Large
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: Prominent
```



## プレゼンテーションソースの構成 (1/2 ページ)

デバイスの API を使用して、単一のビデオ ストリームに最大 4 つのプレゼンテーション ソースを結合できます。

組み合わせることのできるプレゼンテーション ソースの最大数はデバイスによって異なります。

ビデオ会議デバイス	プレゼンテーションソースの最大組み合わせ可能数
Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2, Board	2
Codec Plus, Room 55, Room 55 Dual, Room 70, Desk Pro	3
SX80, MX700, MX800, Codec Pro, Room 70 G2	4
SX10, DX70, DX80	利用不可

ケーブル (デバイスに応じて DVI, VGA, HDMI など) 経由で共有されているソースのみを共有できます。

### ソース構成

#### 構成レイアウト

2 つのレイアウトから選択できます。

- ・ 同等 (Equal)
- ・ プロミネント (Prominent)

ソースの数は、コール時と非コール時どちらであっても、いつでも変更できます。画像サイズは修正できません。

ソースが画面に表示される順序は、コマンド内の順番に従います。表示は左上から始まり、右下が最後になります。

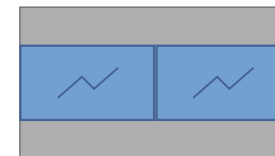
#### オン デマンドによる構成およびレイアウトの変更

プレゼンテーションソース構成は API コマンドを使用してのみ利用可能です。専用のユーザ インターフェイスは提供されません。

構成とレイアウトをオン デマンドで簡単に変更できるようにするには、マクロを使用してカスタムのユーザ インターフェイス パネル (UI 拡張機能) を作成することを推奨します。

### レイアウト

#### 同等 (Equal)



ソースの数: 2

#### プロミネント (Prominent)



ソースの数: 2

## プレゼンテーションソースの構成 (2/2 ページ)

### API コマンド

```
xCommand Presentation Start ConnectorId:
  <1..n>
  PresentationSource: <None, 1..n>
  Instance: <New, 1..n> Layout:
  <Equal, Prominent> SendingMode:
  <LocalRemote, LocalOnly>
```

値は次のとおりです。

入力ソースは、接続されている物理コネクタ (ConnectorId)、または論理ソース識別子 (PresentationSource) のどちらかによって識別可能です。同じコマンド内で異なる識別子を使うことはできません。ConnectorId または PresentationSource のうち片方のみを使用してください。

これらの識別子は、[ビデオ入力コネクタ (Video Input Connector)] および [ビデオ入力ソース (Video Input Source)] のステータスで見つけることができます。

PresentationSource:None を選択すると、空のフレームが挿入されます。

詳細については、API ガイドを参照してください。

### 例

```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal
```



```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent
```



## スタートアップスクリプトの管理

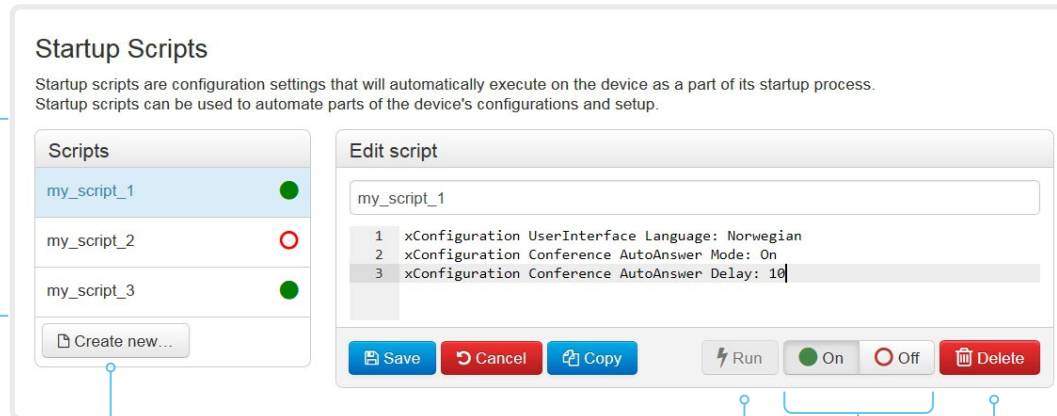
Web インターフェイスにサインインし、[\[統合 \(Integration\)\]](#) > [\[スタートアップスクリプト \(Startup Scripts\)\]](#) に移動します。

### スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます\*

緑色のドットがアクティブなスタートアップ スクリプトの横に、赤色の丸が非アクティブなスタートアップ スクリプトの横に表示されます。

複数のスタートアップ スクリプトがある場合は、リストの上から下に順番に実行されます。



図に示しているスクリプト名と設定は一例です。独自のスクリプトを作成できます。

### スタートアップ スクリプトを作成する

1. [\[新規作成 \(Create new...\)\]](#) をクリックします。
2. タイトル入力フィールドにスタートアップ スクリプトの名前を入力します。
3. コマンド入力エリアにコマンド (xConfiguration または xCommand) を入力します。新しい行で各コマンドを開始します。
4. [\[Save \(保存\)\]](#) をクリックします。
5. [\[オン \(On\)\]](#) をクリックして、スタートアップ スクリプトをアクティブにします。

既存のスクリプトを編集の開始点として使用する場合は、そのスクリプトを選択して [\[コピー \(Copy\)\]](#) をクリックします。

### 起動スクリプトをすぐに実行する

1. リストからスタートアップ スクリプトを選択します。
2. [\[実行 \(Run\)\]](#) をクリックします。

アクティブなスタートアップ スクリプトと非アクティブなスタートアップ スクリプトの両方をすぐに実行できます。

### スタートアップ スクリプトをアクティブ化または非アクティブ化する

1. リストからスタートアップ スクリプトを選択します。
2. スクリプトをアクティブにする場合は [\[オン \(On\)\]](#) を、非アクティブにする場合は [\[オフ \(Off\)\]](#) をクリックします。  
アクティブなスタートアップ スクリプトは、デバイスが起動するたびに実行されます。

### スタートアップ スクリプトを削除する

1. リストからスタートアップ スクリプトを選択します。
2. [\[削除 \(Delete\)\]](#) をクリックします。

### スタートアップ スクリプトについて

スタートアップ スクリプトには起動手順の一部として実行されるコマンド (xCommand) および構成 (xConfiguration) が含まれます。

xCommand SystemUnit Boot など、いくつかのコマンドとコンフィギュレーションはスタートアップ スクリプトに含めることができません。不正なコマンドや設定が含まれたスクリプトは保存できません。

xCommand および xConfiguration の構文とセマンティックは、製品の API ガイドに説明されています。

## デバイスの 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 ファイルはデバイスの API の一部です。デバイスに関する情報が階層で構成されています。

- *Configuration.xml* には現在のデバイス設定 (構成) 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、デバイスによって常に更新され、システムおよびプロセスの変更が反映されます。ステータス情報は、Web インターフェイスまたは API からモニタします。
- *Command.xml* には、デバイスにアクションの実行を指示するために使用できるコマンドの概要が含まれています。コマンドは、API から発行されます。
- *Valuespace.xml* には、デバイス設定、ステータス情報、およびコマンドのすべての値スペースの概要が含まれています。

### XML ファイルを開く

XML ファイルを開くにはファイル名をクリックします。

### API について

アプリケーション プログラミング インターフェイス (API) は、デバイス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、デバイスの API ガイドで説明されています。

## Web インターフェイスからの API コマンドとコンフィギュレーションの実行

Web インターフェイスにサインインして、[\[統合 \(Integration\)\]](#) > [\[開発者 API \(Developer API\)\]](#) を選択します。

コマンド (xCommand) および設定 (xConfiguration) は、Web インターフェイスから実行できます。構文とセマンティックの説明については、デバイスの API ガイドをご覧ください。

### API コマンドとコンフィギュレーションの実行

1. テキスト領域に、コマンド (xCommand または xConfiguration) またはコマンド シーケンスを入力します。
2. [\[実行 \(Execute\)\]](#) をクリックしてコマンドを発行します。

Execute API commands and configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

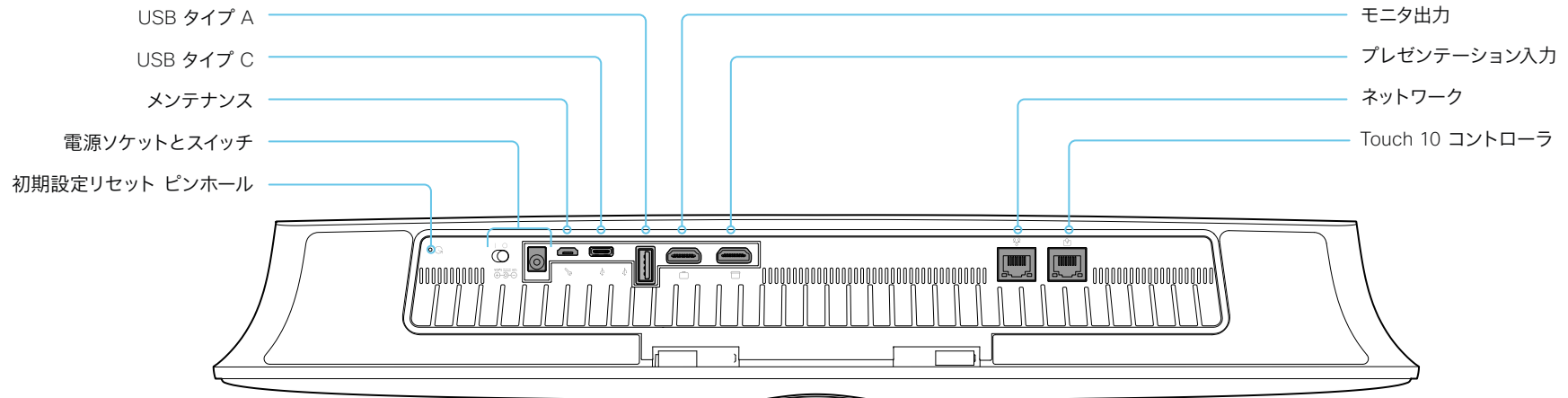
Enter commands...

Execute

### API について

アプリケーション プログラミング インターフェイス (API) は、デバイス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、デバイスの API ガイドで説明されています。

## コネクタ パネル



### 初期設定リセット ピンホール

ピンホールは最後の手段として使用してください。初期設定へのリセットは、Touch ユーザ インターフェイスまたはウェブ インターフェイスから実行することをお勧めします。

### 電源

必ず付属の電源を使用してください。電源スイッチがオンの位置にある場合、デバイスは自動的に電源が入ります。

### メンテナンス

デバイスとのシリアル通信には、マイクロ USB コネクタを使用します。

### USB

- ・ USB: 2.0 タイプ A
- ・ USB 2.0 タイプ C

### モニタ出力

HDMI バージョン 2.0、最大解像度は 60fps で 3840 × 2160。これらの出力には音声がありません。高解像度とフレーム レートをサポートするプレミアム HDMI ケーブルが必要です。Cisco 認定ディスプレイ ケーブルをお勧めします。

### プレゼンテーション入力

HDMI バージョン 1.4b、最大解像度はコンピューターでは 30fps で 3840 × 2160。高解像度とフレーム レートをサポートするハイスピード HDMI 1.4b ケーブルが必要です。Cisco 認定プレゼンテーション ケーブルをお勧めします。

### ネットワーク

イーサネット インターフェイス、10 Mb/100 Mb/1 Gb のイーサネット LAN インターフェイス (RJ45)。

### Touch 10 コントローラ

Touch 10 は、このソケットでは提供されていないイーサネット経由で電源供給されています。



## イーサネットポートについて

### メインネットワークポート

メイン ネットワーク ポート - ネットワーク ポート 1 - は常に LAN 接続用に予約されています。これは、すべてのビデオ会議デバイスに適用されます。

ネットワーク ポート 1 は、デバイスに応じて、番号 1、ネットワーク記号 (%)、またはその両方でマークされます。

### 補助ポート

ビデオ会議デバイスによっては、ネットワーク ポートが複数あります。追加のポートは、カメラ、Touch 10、サードパーティー製制御システムなどの周辺機器に使用できます。

このようなネットワークポートに接続されているデバイスはコーデックからローカル IP アドレスを取得するため、企業ネットワークには接続されていません。パケットは、メインネットワークポート (LAN) と補助ネットワークポート (リンク-ローカル) の間の移動はできません。

- Cisco の周辺機器には、169.254.1.41 から 169.254.1.240 の範囲 (DHCP) での動的 IP アドレスが割り当てられます。
- Cisco 以外のデバイスには、動的 IP アドレス (DHCP) : 169.254.1.30 を割り当てることができます。

**注:** Cisco 以外のデバイスで動的 IP アドレスを取得できるのは、一度に 1 つだけです。

- さらに、Cisco 以外のデバイスには、169.254.1.241 ~ 169.254.1.254 の範囲の静的 IP アドレスを割り当てることができます。

この方法は、SSH を使用してコーデックに接続する場合にも使用できます。このケースでは、IP アドレス 169.254.1.1 を使用できます。

### パワーオーバーイーサネット (PoE)

補助ネットワークポートには Power over Ethernet (PoE) を提供するものもあります。これらのポートは Touch 10 コントローラなどの周辺機器に電源を供給します。

製品	補助ネットワークポートの数	PoE 付きの補助ネットワークポートの数
Room Kit	1	0
Room Kit Mini	1	1 (🖱)
Room 55	1	1 (🖱)
Room 70 / Room 55 Dual	2	1 (🖱)
Room 70 G2	4	2 (🖱, PoE)
Codec Plus	2	1 (🖱)
Codec Pro	4	2 (🖱, PoE)
Board	0	0
Desk Pro	1	0 <sup>1</sup>
SX10	0	0
SX20	0	0
SX80	2	0
MX200 G2 / MX300 G2	2	0
MX700 / MX800	2	0 <sup>2</sup>
DX70 / DX80	1	0 <sup>1</sup>

<sup>1</sup> これらの製品の補助ポートはネットワーク拡張ポートです。コンピュータやその他のデバイスをこのポートに接続して、ビデオ会議デバイスと同じネットワーク/LAN にアクセスできます。このポートは周辺機器には使用されず、コーデックからローカル IP アドレスが割り当てられることはありません。

<sup>2</sup> これらの製品には個別の PoE インジェクタがあり、補助ネットワークポートの 1 つに接続されます。PoE インジェクタは Touch 10 コントローラに使用されます。

## メンテナンス用のシリアル インターフェイス

デバイスとの直接通信には、micro USB コネクタを使用します<sup>1</sup>。マイクロ USB to USB ケーブルが必要です。コンピュータにシリアル 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、手動でシリアル ポート ドライバをインストールする必要があります<sup>2</sup>。

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を使用します。最も一般的なコンピュータ タイプ (PC、MAC) およびオペレーティング システムでは、PuTTY または Tera Term は機能します。

パラメータ:

- ・ ボー レート: 115200 bps
- ・ データ ビット: 8
- ・ パリティ: なし
- ・ ストップ ビット: 1
- ・ ハードウェア フロー制御: オフ

### デバイスの設定

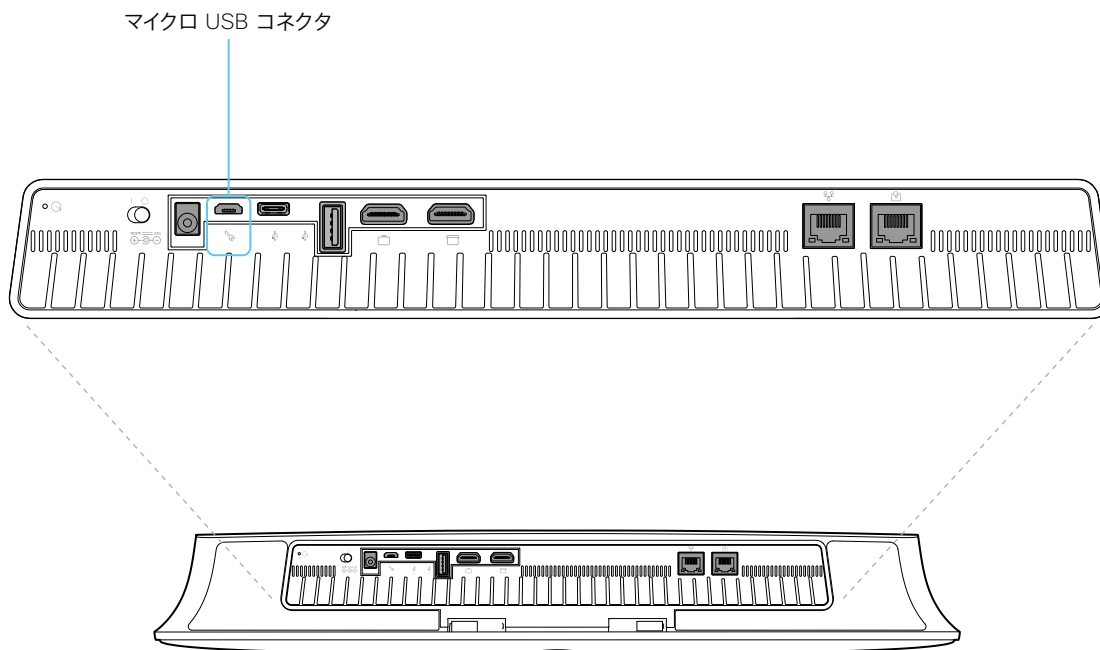
シリアル通信はデフォルトでイネーブルになっています。動作を変更するには、次の設定を使用します。

[シリアルポート (SerialPort)] > [モード (Mode)]

セキュリティ上の理由から、シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには、次の設定を使用します。

[シリアルポート (SerialPort)] > [ログインが必須 (LoginRequired)]

デバイスが CUCM によって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は CUCM から行う必要があります。



<sup>1</sup> マイクロ USB ポートはメンテナンス用です。シリアル接続経由でビデオ システムの API にアクセスする場合は、USB ポート (Type-A) に接続します。詳細については、API ガイドを参照してください。

<sup>2</sup> CP210x USB - UART ブリッジ仮想 COM ポート (VCP) ドライバが必要です。  
<http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers> を参照してください。

## TCP ポートの開放 (1/2 ページ)

コーデック内の Web サーバでは、非セキュアまたは不必要なポート、プロトコル、モジュール、またはサービスの使用が禁止または制限されています。いくつかのポートはデフォルトで開放されています。

### TCP 22: SSH

SSH モード設定を [オフ (Off)] にすることで、ポートを閉じることができます。

NetworkServices SSH Mode: Off/On

### TCP 80: HTTP

HTTP モードを [オフ (Off)] にするか、[HTTPS (HTTPS)] にすることで、ポートを閉じることができます。

NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off

### TCP 443: HTTP

HTTP モード設定を [オフ (Off)] にすることで、ポートを閉じることができます。

NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off

### TCP 4043: リモート ペアリング ソフトウェアのダウンロード

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

### TCP 4045: リモート ペアリング バージョン情報

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

### TCP 4047: リモート ペアリング セッション接続

このポートは、Touch パネルがビデオ会議デバイスとリモート ペアリングされている場合にのみ使用可能 (オープン) です。Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

### TCP 4053: リモート ペアリング ポート

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On

### TCP 5060/5061: SIP リッスン ポート

SIP リッスンポートはデフォルトで開放されています。SIP リッスン ポートは、Cisco UCM (Unified Communication Manager) によって無効にされています。SIP リッスン ポートを [オフ (Off)] にすることで、ポートを閉じることができます。

SIP ListenPort: Off/On

### TCP 65533: プロキシミティ接続用代替ポート

このポートはデフォルトで閉じられています。プロキシミティで代替ポートを有効にする設定を True にすると、このポートがプロキシミティ接続用に開放されます。

Proximity AlternatePort Enabled: False/True

デバイスの設定は、Web インターフェイスの [\[セットアップ \(Setup\)\] >](#) [\[設定 \(Configuration\)\]](#) ページから行います。Web ブラウザを開き、デバイスの IP アドレスを入力して、サインインします。

## TCP ポートの開放 (2/2 ページ)

### TCP 4051: リモートペアリングポート (廃止)

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing:  
Off/On
```

### TCP 4062: リモートペアリングポート

Touch パネルとのリモート ペアリングを [オフ (Off)] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing:  
Off/On
```

### TCP 4190: UPnP ポート

SIP リッスン ポートを [オフ (Off)] にすることで、ポートを閉じることができます。

```
NetworkServices UPnP Mode: Off
```

## TMS からの HTTPFeedback アドレス

デバイスが Cisco TelePresence Management Suite (TMS) に追加されると、TMS に情報 (イベント) を送り返すように自動的に設定されます。デバイスは、TMS からそれらのイベントに送信されるアドレス (HTTPFeedback アドレス) を受けとります。このアドレスが存在しないか、または正しく設定されていない場合、デバイスは TMS にイベントを送信できません。

### 失われたイベントへの応答

イベントへの応答がデバイスで受信されない場合、デバイスは最大 6 回、間隔を増やしながら HTTPFeedback アドレスに送信を再試行します。

再試行してもデバイスで応答が受信されない場合、エンドポイントは 10 分ごとに HTTPFeedback アドレスにメッセージの送信を試行します。HTTPFeedback ステータスには失敗したことが示され、障害のタイプを示す診断メッセージが表示されます。

メッセージの再送を試みる際、TMS での通話詳細記録 (CDR) の紛失が生じます。

### TMS からの新しい HTTPFeedback アドレスの取得

イベントを送信するための新しいアドレスを取得するには、デバイスを再起動して、TMS から (スケジュール設定または TMS 管理者によるトリガーで) 次の管理アドレスがプッシュされるのを待つ必要があります。

## オンプレミス登録デバイスの Cisco Webex Edge for Devices へのリンク

Webex Edge for Devices を使用すると、オンプレミス登録のデバイスを Webex クラウドサービスにリンクできます。これにより、登録、デバイスの設定管理、通話、メディアサービスはオンプレミスのままで、特定のクラウド機能にアクセスできるようになります。Webex Control Hub でクラウドサービスを管理したり、デバイスの診断を受けたりできます。

### 設定

最初にデバイスをオンプレミスサービスに登録してから、Webex Edge にリンクすることをお勧めします。デバイスを Webex Edge for Devices にリンクする方法については、Webex ヘルプセンターで [▶ Webex Edge for Devices](#) の記事を参照してください。

### 機能

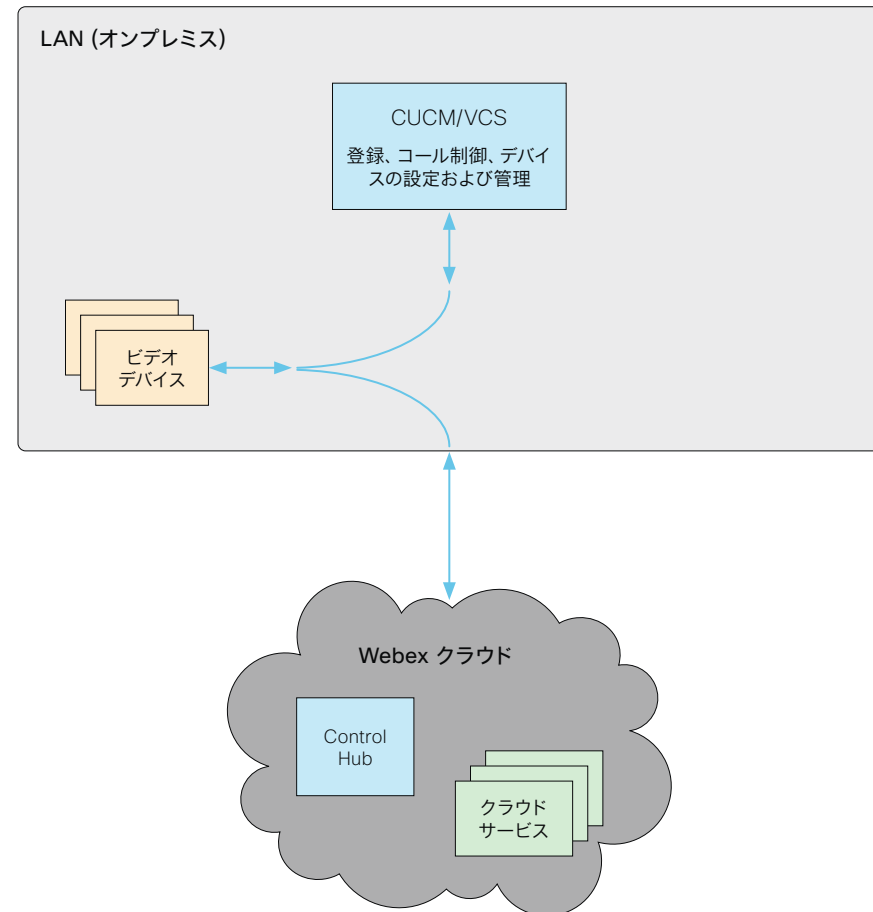
Webex Edge for Devices には次の機能があります。

- Control Hub でのオンライン/オフライン接続ステータス
- 管理者アラートの設定に対応したデバイス診断
- デバイスの履歴分析を Control Hub で直接使用可能
- Control Hub でデバイス設定にアクセス (高度な設定)
- クラウド xAPI アクセス
- Control Hub によるハイブリッド予定表
- Webex Assistant (音声駆動型の仮想アシスタント)

前述の Webex Edge for Devices の記事には、使用できる機能と制限事項の最新の一覧が含まれています。

### 前提条件

- ソフトウェアバージョン CE 9.10 以降
- CUCM バージョン 12.5su1、または最新のデバイスパックを適用した 11.5.x
- Control Hub の管理者アクセス権
- デバイスコネクタツール (Webex Edge へのリンクを設定するため)
- クラウド サービス ライセンス(シスコ コラボレーション フレックス プラン)



## Cisco Webex Cloud サービスへのデバイスの登録

画面上のセットアップ アシスタントを使用する代わりに、Web インターフェイスからリモートで Cisco Webex にデバイスを登録できます。

デバイスを登録するには、まず、コントロール ハブで、アクティベーション コードを作成する必要があります。アクティベーションコードの作成方法については、▶ [Cisco Webex Room デバイス](#)または [Cisco Webex Board に Workspace を作成するか、サービスを追加する](#)を参照してください。

Web インターフェイスから登録できるのは、現在サービスに登録されていないデバイスのみです。

**注:** このデバイス用に作成されたローカル ユーザとカスタマイズは、すべて非アクティブ化されます。

1. Web インターフェイスにサインインし、ホーム画面で [\[ここをクリックして Webex に登録 \(Click here to register to Webex\)\]](#) をクリックします。  
このリンクは、デバイスがサービスにまだ登録されていない場合にのみ使用できます。
2. ポップアップが表示され、コントロール ハブで作成したアクティベーション コードを入力することができます。  
形式:
  - XXXX-XXXX-XXXX-XXXX、または
  - XXXXXXXXXXXXXXXXX
3. 登録後に、画面上のセットアップ アシスタントからタイム ゾーンと言語を設定する必要があります。ウィザードがタイム アウトした場合は、デフォルトの設定が適用されます。

### 制限

利用可能な設定の一部は、オンプレミスの登録済みデバイスにのみ適用されます。これらは、Webex に登録されているデバイスには適用されません。API ガイドの「サポートされているコマンド マトリックス」では、これらの項目は「オンプレミスのみ」とマークされています。

適用されない設定はすべて、H.323、H.320、SIP、NTP、CUCM、LDAP、Proximity、および相手先カメラ制御に関連するものです。

### System Information

General		H323	
Product:	Cisco ...	Status	Inactive
System time:	12:30	Gatekeeper	-
Browser time:	12:30	Number	-
Last boot:	yesterday at 15:00	ID	-
Serial number:		<b>SIP</b>	
Software version:	ce...	Status	Inactive
Installed options:	Encryption RemoteMonitoring	Proxy	-
System name:	MySystem	This video system is not registered  In order to place calls with this video system, it needs to be registered to a call service.  <a href="#">Click here to register to Webex</a>	
IPv4:			
IPv6:			
MAC address:			
Temperature:	65.7°C / 150.3°F		

## サポートされている RFC

RFC (Request For Comments) シリーズには、Internet Engineering Task Force (IETF) によって作成される技術仕様およびポリシー文書など、インターネットに関する技術および組織のドキュメントが含まれます。

CE ソフトウェアは、以下を含む RFC の範囲をサポートしています。

- RFC 2782 『DNS RR for specifying the location of services (DNS SRV)』
- RFC 3261 SIP 『Session Initiation Protocol』
- RFC 3263 『Locating SIP Servers』
- RFC 3361 『DHCP Option for SIP Servers』
- RFC 3550 RTP 『RTP: A Transport Protocol for Real-Time Applications』
- RFC 3711 『The Secure Real-time Transport Protocol (SRTP)』
- RFC 4091 『The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework』
- RFC 4092 『Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)』
- RFC 4582 『The Binary Floor Control Protocol』  
draft-ietf-bfcpbis-rfc4582bis-00 『Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport』
- RFC 4733 『RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals』
- RFC 5245 『Interactive Connectivity Establishment (ICE)』 : A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5589 『SIP Call Control Transfer』
- RFC 5766 『Traversal Using Relays around NAT (TURN)』 : Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905 『Network Time Protocol Version 4: Protocol and Algorithms Specification』



## 技術仕様 (1/2 ページ)

### ソフトウェアの互換性

- ・ Cisco Collaboration Endpoint Software Version 9.6 以降
- ・ RoomOS

### 帯域幅

ポイントツーポイントで最大 6 Mbps

### ファイアウォール トラバース

- ・ Cisco TelePresence Expressway テクノロジー
- ・ H.460.18 および H.460.19 ファイアウォール トラバース

### ビデオ規格

- ・ H.264
- ・ H.265 (SIP)

### ビデオ入力

- ・ 1 つの HDMI 入力により、HD1080p60 を含め最大 4K (3840 X 2160/30 fps) のフォーマットをサポート
- ・ Consumer Electronics Control (CEC) 2.0

### ビデオ出力

- ・ 60 fps で最大 3840 × 2160 (4Kp60) のフォーマットをサポートする 1 つの HDMI 出力\*
- ・ 30 fps または 60 fps で最大 1920 × 1080 (HD1080p) のライブ ビデオ解像度 (エンコードおよびデコード)
- ・ Consumer Electronics Control (CEC) 2.0

### USB パススルー

- ・ 接続されたコンピュータで、1 つの USB ケーブルでビデオ、マイク、およびスピーカーを使用可能
- ・ ビデオ解像度 720p

### 音声規格

- ・ AAC-LD
- ・ G.722
- ・ G.722.1
- ・ G.711
- ・ G.729
- ・ Opus

### 音声機能

- ・ ハイクオリティ 20kHz オーディオ
- ・ オートゲイン コントロール (AGC)
- ・ オートノイズリダクション
- ・ アクティブリップシンク

### 音声入力

- ・ HDMI からのオーディオ入力 1 個
- ・ 内部マイクروفोन

### スピーカー (統合)

- ・ 平衡型構成の高品質スピーカー 3 個
- ・ 周波数特性: 70Hz ~ 20kHz
- ・ 増幅器用電源: 24W
- ・ 最大出力レベル: 85dB SPL

### MULTISITE

- ・ H.239 デュアル ストリーム (H.323)
- ・ BFCP デュアル ストリーム (SIP)
- ・ 5fps で最大 3840 × 2160 の解像度のサポート

### DUAL ストリーム

- ・ 1 つの HDMI 入力により、HD1080p60 を含め最大 4K (3840 × 2160/30 fps) のフォーマットをサポート
- ・ Consumer Electronics Control (CEC) 2.0

### ワイヤレス共有

- ・ Cisco Webex Teams アプリ (最大 3840 × 2160、5 fps)
- ・ Cisco Webex Meetings アプリケーション (最大 3840 X 2160/5 fps)
- ・ Cisco Intelligent Proximity クライアント (5 fps で 最大 1920 × 1080)

### マルチポイント サポート

- ・ マルチサイト オプションで組み込み 4-way SIP/H.323 会議機能

### マルチサイト機能 (組み込みマルチポイント)、オプションのアップグレード

- ・ 対応型 SIP/H.323 マルチサイト:
  - 3 ウェイ: コンテンツのない 1080p30 までの解像度。解像度は最大 720 p 30 で、1080p15 までのコンテンツ
  - 4 ウェイ: 最大 720p30 まで、最大 1080p15 までの解像度。
- ・ 音声および映像の個別トランスコーディング
- ・ 同じ電話会議で H.323、SIP、VoIP が混在可能
- ・ 5 fps で最大 3840 × 2160 の解像度で、任意の参加者からのプレゼンテーション (H.239/BFCP) をサポート
- ・ ベスト インプレッション機能 (自動連続表示レイアウト)
- ・ 任意の拠点からの暗号化およびデュアル ストリーム

### プロトコル

- ・ H.323
- ・ SIP
- ・ Cisco Webex

### 内蔵暗号化機能

- ・ H.323 および SIP ポイントツーポイント
- ・ 規格準拠: H.235 v3 および Advanced Encryption Standard (AES)
- ・ 暗号化キーの自動生成と自動交換

### IP ネットワーク機能

- ・ DNS ルックアップによるサービス構成
- ・ 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
- ・ 動的のブレイクアウトおよびリップシンク バッファリング
- ・ H.323 の H.245 DTMF トーン
- ・ SIP の RFC 4733 DTMF トーン
- ・ NTP による日時のサポート
- ・ メディア適合およびレジリエンス
- ・ URI ダイアル
- ・ DHCP (ダイナミック ホスト コンフィギュレーション プロトコル)
- ・ IEEE 802.1x ネットワーク認証
- ・ IEEE 802.1q VLAN
- ・ IEEE 802.1p QoS および Class of Service (CoS)

### IPv6 ネットワーク サポート

- ・ 単一のコール スタックで H.323 と SIP の両方をサポート
- ・ DHCP、SSH、HTTP、HTTPS、DNS、および DiffServ に対するデュアル スタックの IPv4 および IPv6
- ・ スタティックと自動 IP 設定 (ステートレス アドレス自動設定) の両方をサポート

### CISCO UNIFIED COMMUNICATIONS MANAGER

- ・ Cisco Unified Communications Manager (CUCM) のネイティブ登録
- ・ CUCM バージョン 9.1.2 以降と Cisco Webex Room Kit Mini のデバイス パックが必要

### セキュリティ機能

- ・ HTTPS および SSH を使用した管理
- ・ IP 管理用パスワード
- ・ 管理メニューのパスワード
- ・ IP サービスの停止可能
- ・ ネットワーク設定の保護
- ・ プライバシー カバー

### ネットワーク インターフェイス

- ・ LAN 用イーサネット (RJ-45) X 1、10/100/1000 Mbps
- ・ Cisco Touch 10 用イーサネット (RJ-45) X 1
- ・ Wi-Fi: IEEE 802.11a/b/g/n/ac 2.4GHz、5GHz、2x2 MIMO

### その他のインターフェイス

- ・ USB 2.0 ポート Type-A X 1
- ・ USB 2.0 ポート Type-C X 1
- ・ 1 つのマイクロ USB ポート
- ・ 初期設定リセット ピンホール

### オプションのハードウェア コンポーネント

- ・ HDMI プレゼンテーションケーブル 8 m/26.2 フィート
- ・ USB パススルー機能用 4 m/13 フィート USB ケーブル
- ・ 画面取り付けキット

## 技術仕様 (2/2 ページ)

### カメラの概要

- ・ 4K Ultra HD カメラ
- ・ 最大 60 fps をサポート (Best Overview 適用時には最大 30 fps)
- ・ 8 メガピクセルイメージセンサー
- ・ 1/1.4 CMOS
- ・ 5 倍ズーム
- ・ 絞り  $f/1.4$
- ・ 水平視野角 120°
- ・ 自動フレーミング (顔検出)
- ・ 自動フォーカス、輝度およびホワイト バランス
- ・ 焦点距離: 1 m ~ 無限遠

### 電源

- ・ 100-240 VAC、50/60 Hz、12 V<sub>DC</sub>入力
- ・ 平均 20 W、ピーク時 70 W
- ・ 電源 FSP FSP070-AHAN2 または AcBel ADF019 を使用する必要あり

### 動作温度および湿度

- ・ 周囲温度: 0 ~ 40 °C (32 ~ 104°F)
- ・ 相対湿度 (RH): 10 ~ 90%

### 保管および輸送の温度

- ・ RH 10 ~ 90% では -20 ~ 60°C (-4 ~ 140°F) (結露しないこと)

### 寸法

- ・ 幅: 500 mm/19.7
- ・ 高さ: 81 mm (3.2 インチ)
- ・ 深さ: 77 mm/3 インチ
- ・ 重量: 18+ kg (40 ポンド)

### 認定および適合規格

- ・ 指令 2014/35/EU (低電圧指令)
- ・ 指令 2014/30/EU (EMC 指令): クラス A
- ・ 指令 2014/53/EU (無線機器指令)
- ・ 指令 2011/65/EU (RoHS)
- ・ 指令 2002/96/EC (WEEE)
- ・ NRTL 認定 (製品の安全性)
- ・ FCC CFR 47 Part 15B (EMC): クラス A
- ・ FCC CFR 47 Part 15C (RF)
- ・ FCC CFR 47 Part 15E (RF)
- ・ 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.cisconfax.com](http://www.cisconfax.com) を参照してください。

すべての仕様は予告なしに変更される場合があります。システム仕様は異なる場合があります。

これらのドキュメントの画像はすべて説明目的でのみ使用され、実際の製品とは異なる場合があります。

Cisco および Cisco ロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標のリストは、[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks) に記載されています。Third party trademarks mentioned are the property of their respective owners. 「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。

2020 年 3 月

## シスコ Web サイト内のユーザマニュアル

次の短縮リンクを使用して、CE ソフトウェアを実行する製品シリーズのマニュアルを検索します。

### Room シリーズ:

▶ <https://www.cisco.com/go/room-docs>

### MX シリーズ:

▶ <https://www.cisco.com/go/mx-docs>

### SX シリーズ:

▶ <https://www.cisco.com/go/sx-docs>

### Desk シリーズ/DX シリーズ:

▶ <https://www.cisco.com/go/desk-docs>

### Board:

▶ <https://www.cisco.com/go/board-docs> [\[英語\]](#)

通常、すべてのシスココラボレーションエンドポイントのユーザーマニュアルは ▶ <https://www.cisco.com/c/en/us/support/collaboration-endpoints> で参照できます。

マニュアルは以下のカテゴリに整理されています。一部のマニュアルはすべての製品で利用できません。

### インストールとアップグレード > インストールとアップグレード ガイド

- ・ *インストレーション ガイド*: 製品のインストール方法
- ・ *スタートアップ ガイド*: デバイスを動作させるために必要な初期設定
- ・ *RCSI ガイド*: 法規制の遵守および安全に関する情報

### 保守と運用 > メンテナンスとオペレーション ガイド

- ・ *スタートアップ ガイド*: デバイスを動作させるために必要な初期設定
- ・ *管理者ガイド*: 製品の管理に必要な情報
- ・ *CUCM での TelePresence エンドポイントの導入ガイド*: Cisco Unified Communications Manager (CUCM) と組み合わせてデバイスを使用開始する際に実行するタスク
- ・ *スペア部品の概要*、*スペア部品の交換ガイド*、*ケーブル スキーマ*: スペア部品を交換するときに役立つ情報

### 保守と運用 > エンドユーザ ガイド

- ・ *ユーザ ガイド*: 製品の使用方法
- ・ *クイック リファレンス ガイド*: 製品の使用方法
- ・ *物理インターフェイス ガイド*: コネクタのパネルと LED など、コーデックの物理インターフェイスに関する詳細

### リファレンス ガイド > コマンド リファレンス

- ・ *API リファレンス ガイド*: Application Programmer Interface (API) のリファレンス ガイド

### リファレンス ガイド > テクニカル リファレンス

- ・ *CAD 図面*: 測定値付き 2D CAD 図面

### 設定 > 設定ガイド

- ・ *カスタマイズ ガイド*: ユーザ インターフェイスのカスタマイズ方法、デバイスの API を使用した室内制御のプログラミング方法、マクロの作成方法、オーディオ コンソールを使用した高度な音声セットアップの設定方法

### 設計 > 設計ガイド

- ・ *ビデオ会議室に関するガイドライン*: 会議室の設計とベストプラクティスに関する一般的なガイドライン
- ・ *ビデオ会議室のガイドライン*: 音質を向上させるための対策

### ソフトウェア ダウンロード、リリースと一般情報 > ライセンス情報

- ・ *オープン ソースの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と通知

### ソフトウェア ダウンロード、リリースと一般情報 > リリース ノート

- ・ *ソフトウェア リリース ノート*

## シスコのお問い合わせ先

シスコの Web サイトでは、Cisco の世界各地のお問い合わせ先を確認できます。

参照先: ▶ <https://www.cisco.com/go/offices>

本社  
Cisco Systems, Inc.  
170 West Tasman  
Dr.San Jose, CA 95134 USA

### 知的財産

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとし、このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または黙示のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとし、

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

印刷版と複製ソフトは公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開業しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト ([www.cisco.com/go/offices/](http://www.cisco.com/go/offices/) [英語]) をご覧ください。

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。Cisco の商標の一覧については、[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks) をご覧ください。Third-party trademarks mentioned are the property of their respective owners。「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1110R)。

### Cisco 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、およびユーザーは、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したものとみなされます。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。