



Webex アプリでのコール（Unified CM） 用導入ガイド

初版：2019年3月28日

最終更新：2024年4月24日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

Webex アプリでのコール (Unified CM) の概要 1

新機能および変更情報 1

Webex アプリでのコール (Unified CM) の概要 25

Webex アプリ の通話機能 26

基本的なコール機能 27

通話中の通話機能 28

追加機能 32

導入機能 43

デスクフォン制御 (DPC) に関する詳細 46

ユーザー向け Webex アプリ の通話エクスペリエンス 47

通話の比較 47

ユーザー体験 48

アーキテクチャ 50

ネットワーク内 50

リモート 51

Webex アプリでのコール (Unified CM) の通話フロー 52

Webex アプリ での Unified CM 通話応答 52

デスクフォンで Unified CM 着信通話に応答する 53

Webex アプリ でディレクトリ番号のないユーザーに発信 53

Webex アプリ から PSTN 番号への Unified CM 通話 54

デスクフォン制御モードでの Unified CM 通話 55

デスクフォン制御モードで会議に参加 55

第 2 章

Webex アプリでのコール (Unified CM) 用環境の準備 57

呼制御環境の要件	57
Unified CM 機能要件	60
接続時のトーンによる自動応答	60
通話パーク	60
コール録音	61
ダイヤルプランのマッピング	61
Dial Via Office Reverse	62
Extend and Connect	63
通話をモバイルに移動	63
マルチライン	64
マルチコールウィンドウ	65
プッシュ構成	66
緊急通報の位置情報報告	66
Survivable Remote Site Telephony (SRST)	68
ボイスメール	68
Wi-Fi から LTE 通話ネットワークのハンドオフ	69
ワイヤレス ロケーション モニタリング サービス	70
Contact Center 機能要件	71
ネットワークの要件	71
ポートとプロトコル	72
サポートされるコーデック	73
証明書の要件	74
Unified CM 証明書 (展開で MRA なし)	74
Unified CM 証明書 (展開で MRA あり)	75
Expressway 証明書 (展開で MRA あり)	75
ヘッドセットの要件	78
ライセンス要件	78
Webex アプリ 要件	79
推奨構成	79
シングルサインオンと IdP の統合	79
SSO リダイレクト URI	80

ディレクトリ同期および連絡先カード	81
Webex アプリの自動プロビジョニングの概要	82
前提条件	83
追加構成	84

第 3 章

Webex アプリでのコール (Unified CM) の導入	85
Webex アプリでのコール (Unified CM) 展開タスクフロー	85
サービスプロファイルの概要	90
デフォルトのサービスプロファイルの作成	90
UC サービスワークフローの構成	91
ボイスメールのパイロット番号の構成	92
UC サービスの構成	93
UC サービスを使用したサービスプロファイルの構成	94
Webex アプリ のボイスメールアイコン インジケータ	94
サービスの発見オプション	95
DNS SRV レコードの構成	95
SRV レコードのテスト	96
認証オプション	97
クライアントの SAML SSO	97
LDAP サーバーによる認証	97
デスクトップクライアントの電話構成でパラメータを設定	97
Webex アプリでのコール (Unified CM) の Unified CM エンドユーザーの構成	98
ソフトフォンワークフローの作成	99
Webex アプリ ソフトフォンデバイスの作成と構成	100
Android デバイスと密度に依存しないピクセル	103
デバイスにディレクトリ番号を追加する	103
ユーザーとデバイスの関連付け	104
暗号化された通話用の電話機セキュリティプロファイルを構成	105
プッシュ通知の構成と推奨設定	106
クライアント構成パラメータの設定 (リリース 12.5 以降)	107
設定パラメータの定義	107

サービスプロファイルへのクライアント設定の割り当て	108
クライアント構成ファイルの作成とホスト (12.5 以前のリリース)	108
XML 構成ファイルの要件	109
共通構成の作成	110
グループ構成の作成	111
構成ファイルのホスト	112
TFTP サーバーの再起動	112
共通構成の作成	113
構成ファイルの要件	114
通話を会議に移動する構成	114
ユーザーワークフロー用通話エクスペリエンス	116
UC マネージャプロファイルの作成	117
Control Hub での通話動作と UC マネージャプロファイルの設定	117
組織レベルで通話動作設定を有効化	118
グループレベルで通話動作設定を有効化	119
ユーザーレベルで通話動作組織設定をオーバーライド	121
ユーザーレベルでの通話動作のグループレベル設定のオーバーライド	121
手動接続設定	122
Webex アプリ での電話サービスの認証	122
展開後に追加機能を構成する	124
既知の問題と Webex アプリでのコール (Unified CM) の制限事項	125

第 4 章

Webex アプリでのコール (Unified CM) の管理とトラブルシュート	129
Jabber コンタクトを移動するためのユーザー設定と Webex アプリ への共通設定	129
Webex アプリでのコール (Unified CM) の通話統計にアクセス	129
UC マネージャプロファイルの編集	130
Webex アプリ での診断	130
Control Hub でのシスコヘッドセットの管理	131
Webex クラウドへの接続が失われる	131
Calling in Webex アプリ (Unified CM) に関する問題のトラブルシュート	132
Webex アプリ のエラーメッセージ	133

付録 A :

付録 135

- ポリシーパラメータ 135
 - 機能パラメータ 135
 - カスタマイズパラメータ 142
 - Jabber to Webex アプリ migration パラメータ 150
- 通話用プロトコルハンドラ 151
 - Windows 用プロトコルハンドラ 151
 - macOS 用プロトコルハンドラ 154
- サービス品質 155
 - Quality of Service オプション 155
 - サポートされるコーデック 155
 - SIP プロファイルでのポート範囲の定義 156
 - DSCP 値の設定 156
 - Unified CM での DSCP 値の設定 157
 - グループポリシーを用いた DSCP 値の設定 157
 - ネットワークで DSCP 値を設定 158
 - Unified CM で信頼できない証明書を許可する 158



第 1 章

Webex アプリでのコール（Unified CM）の概要

- [新機能および変更情報](#)（1 ページ）
- [Webex アプリでのコール（Unified CM）の概要](#)（25 ページ）
- [Webex アプリの通話機能](#)（26 ページ）
- [ユーザー向け Webex アプリの通話エクスペリエンス](#)（47 ページ）
- [アーキテクチャ](#)（50 ページ）
- [Webex アプリでのコール（Unified CM）の通話フロー](#)（52 ページ）

新機能および変更情報

次の表では、新機能に関するコンテンツ更新、既存コンテンツの変更、『Webex アプリでコールイン（Unified CM）に関する導入ガイド』で修正された重大なエラーに関して説明されています。

Webex アプリの更新については、ユーザーに展開するアプリの種類に対応する次の資料を参照してください。

- **スタンドアロンアプリ**：主要な更新に関しては、「[最新情報](#)」ドキュメントを、Webex アプリに関する重要でない更新やバグ修正に関しては「[リリースノート](#)」を参照してください。
- **VDIアプリ**：重要な更新や制限事項に関しては、「[VDI リリースノート](#)」を参照してください。

日付	変更内容
2024 年 4 月 24 日	「Webex アプリで通話を展開する（Unified CM）」の章「会議に通話を移行するように構成する」セクションのステップ 3 へのリンクを追加しました。

日付	変更内容
2024 年 4 月 22 日	新しいパラメータ「ShowSelectiveCallRecordingButton」が [付録 (Appendix)] > [ポリシーパラメータ (Policy Parameters)] > [機能パラメータ (Feature Parameters)] セクションに追加されました。
2023 年 6 月 3 日	新しいパラメータ「EnableSIPURIDialling」が「付録」>「ポリシーパラメータ」>「機能パラメータ」セクションに追加されました。
	新しいパラメータ「LocalPushSSIDList」が「付録」>「ポリシーパラメータ」>「機能パラメータ」セクションに追加されました。
	「展開機能」セクションの「展開機能」の表に、新しい機能名「ローカルプッシュ通知サービス (LPNS)」と「注意」が追加されました。
	「Webex アプリ (Unified CM) での通話概要」>「Webex アプリの通話機能」>「デスクフォン制御 (DPC) の詳細」セクションに注記を追加しました。
2023 年 4 月 29 日	「Control Hub での通話動作と UC マネージャプロファイルを設定」セクションを更新しました。
2023 年 3 月 10 日	「緊急通話のための所在地報告」セクションを変更しました。Redsky は唯一の E911 SP でした。現在、「Intrado」は E911 SP と統合され、「E911 SP Intrado」と呼ばれています。
2022 年 10 月 18 日	「推奨される構成 - SSO リダイレクト URI」セクションの「要件」で、「Unified CM 12.5(x) リリース - 12.5(1) SU4 以降 (Unified CM 14 はサポートされていません)」を「Unified CM 12.5(x) リリース - 12.5(1) SU4 および Unified CM 14.0(x) リリース - 14.0(1) SU1 以降」に置き換えました。

日付	変更内容
2022 年 6 月 7 日	<ul style="list-style-type: none"> • このドキュメントの [概要] > [Webex アプリの通話機能] の追加機能の表に新機能 [複数通話ウィンドウ (Multi call window)] が追加されました。 • [Prepare (準備)] > [Unified CM] 機能の要件に複数通話ウィンドウの要件を追加しました。 • 付録 > ポリシーパラメータ > 機能パラメータ に CucmCallBargeMode パラメータを追加しました。 • 構成ファイルには、新しいパラメータである ShowPhoneNumberInLineSelection があります。これは、ドロップダウンメニューの回線の選択肢で番号を表示または非表示にするこのです。本資料の付録に記載されている カスタマイズパラメータにこのパラメータを追加しました。
2022 年 2 月 15 日	<ul style="list-style-type: none"> • Control Hub でユーザーまたは組織を更新する UI パスを変更しました (「Control Hub で通話動作と UC マネージャプロファイルを設定する」項)。 • Webex アプリの自動プロビジョニングの概要に記載されている「自動プロビジョニングされたデバイスの自動クリーンアップと削除が現在サポートされていないことを説明する注記を削除しました。」
2021 年 12 月 13 日	<ul style="list-style-type: none"> • クラウド接続 UC の自動デバイスプロビジョニング機能の前提条件と構成手順へのリンクを追加しました。 • 「環境の準備」の章に RedSky の緊急位置情報報告を追加しました。 • 通話フローの「デスクフォン制御モードで会議に参加」項に、「ミーティングはスペースから直接行われ、Webex アプリでのみ行われる必要があります。」という説明を追加しました。会議のフル機能はサポートされていません。」 • スタイルガイドラインに従い、項のタイトルをタイトルから文章に変更しました。
2021 年 10 月 5 日	<ul style="list-style-type: none"> • 付録の「Customize パラメータ」表に、EnableADLockPrevention パラメータを追加しました。

日付	変更内容
2021 年 9 月 7 日	<ul style="list-style-type: none">• 付録の「Customize パラメータ」表に、次のパラメータを追加しました。<ul style="list-style-type: none">• 緊急時の免責事項の場合<ul style="list-style-type: none">• E911NotificationFrequency• E911NotificationURL• ビデオ設定の場合<ul style="list-style-type: none">• EnableVideo• StartCallWithVideo• ビデオ設定に次のパラメータを追加しました。• 展開機能表に、次のエントリを追加しました。<ul style="list-style-type: none">• 緊急ダイヤルの免責事項をカスタマイズ• すべての 1 対 1 会議のビデオを無効にする

日付	変更内容
2021 年 8 月 9 日	<ul style="list-style-type: none"> • 追加機能に新しいエントリを追加しました。 <ul style="list-style-type: none"> • ネットワークハンドオフ (Wi-Fi から LTE) • Webex から携帯電話アプリに通話を切り替える • 「環境準備」章の「Unified CM 機能要件」に「Wi-Fi から LTE 会議ネットワークハンドオフ」という新しい項を追加しました。 • 「展開」章に「会議をモバイルに移動する構成」という新しい項を追加しました。 • 「Expressway 証明書 (MRA を使用)」に「Jabber を Webex に移行」と「プライベート CA 証明書の考慮事項」項を追加しました。 • 付録の「機能パラメータ」表に、次のパラメータを追加しました。 <ul style="list-style-type: none"> • EnableRecordingTone • LocalRecordingToneVolume • NearEndRecordingToneVolume • RecordingToneDuration • RecordingToneInterval • 付録の「機能パラメータ」表に、EnableCallPark を追加しました。
2021 年 7 月 7 日	<ul style="list-style-type: none"> • サポートされている最新の機能が一覧されている Webex 用 Contact Center の連携へのリンクを含む「Contact Center 機能要件」という新しい項を追加しました。 • SSO リダイレクト URI について、Unified CM 14.0 がサポートされていないことを明確にしました。 • Webex アプリの新しいブランディングを反映するようにアーキテクチャ図のロゴを更新しました。(詳細については、「新しい Webex Suite とブランディング」を参照してください。)

日付	変更内容
2021 年 6 月 2 日	<ul style="list-style-type: none"> • Webex が Android デバイスが電話かタブレットかを判断する方法を説明するために、「Android デバイスと密度非依存ピクセル」という新しい項を追加しました。 • 「展開」の章に「追加機能の構成」という新しい項を追加しました。 • 付録の「カスタマイズパラメータ」に「EnablePhoneDialerOptionOverMRA」という新しいパラメータを追加しました。 • 機能表に次の項目を追加しました。 <ul style="list-style-type: none"> • デスクトップ用通話中機能表に「「仮想カメラ」」を追加しました。 • 展開機能表に「「仮想カメラ (macOS)」」を追加しました。 • 追加通話機能表に「インドのモバイルアプリユーザー向け PSTN 通話」を追加しました。
2021 年 5 月 11 日	<ul style="list-style-type: none"> • デバイスのディスプレイ dp (電話機は 600 未満、タブレットは 600 以上) を使用して、Webex が Android 機とタブレットを区別する方法に関する情報を追加しました。 • ハイブリッドコール (コールコネクタアーキテクチャ) がサポート終了 (EOL) になるため、「環境の準備」の章から「ユーザ向けハイブリッドコールサービス」を削除しました。

日付	変更内容
2021 年 5 月 5 日	<ul style="list-style-type: none"> • Unified CM で TAB デバイスタ입が使用されている場合に、サポートされるデバイスとして Chromebook が追加されました。 • 同じユーザ用の異なるプラットフォーム上でのソフトウェアデバイスの構成に関する詳細が追加されました。 • 「追加機能」の表に以下を追加しました。 <ul style="list-style-type: none"> • 呼制御環境要件セクションに、MRA フェールオーバー（最低要件（Unified CM 14.0 以降および Expressway X14.0 以降）を追加しました）。 • Webex アプリの診断 • 「通話をミーティングに移動する構成」セクションのエラーを修正しました。この機能を有効にするには、テレフォニーを有効にする必要があります。 • Expressway-C における SSO リダイレクト URI の構成方法に関する詳細を追加しました。
2021 年 4 月 7 日	<ul style="list-style-type: none"> • 「通話をミーティングに移動する構成」という新しいセクションを追加しました（展開の章）。 • 機能テーブルに次のエントリを追加しました。 <ul style="list-style-type: none"> • 通話をミーティングに移動する（通話中の機能：デスクトップおよびモバイル） • 「概要」の章に、Webex が Unified CM とクラウドから構成をプルする方法に関する詳細を追加しました。 • 「アーキテクチャ」セクションを改善しました。
2021 年 3 月 3 日	<ul style="list-style-type: none"> • 中国および非中国展開用の APN の最小リリースを追加しました。 • 通話中の機能の表に「通話録音」を追加しました。 • 「概要」の章に、内部および MRA 導入用のアーキテクチャ図を追加しました。

日付	変更内容
2021 年 2 月 3 日	<ul style="list-style-type: none"> • 索引の「ポリシーパラメータ」の項に次のパラメータを追加しました。 <ul style="list-style-type: none"> • E911EdgeLocationWhiteList • EnableE911EdgeLocationPolicy • EnableE911OnPremLocationPolicy • 「環境の準備」の章に、プッシュ構成、ロケーションモニタリングおよび Cisco Unified Survivable Remote Site Telephony (SRST) に関する新しいセクションを追加しました。 • 追加機能の表に次の変更を行いました。 <ul style="list-style-type: none"> • 追加機能の表の通話履歴のエントリに、コールエントリの削除と 30 日間の 200 コールの制限に関する情報を追加しました。 • 追加機能の表の通知の抑制エントリに、通話中および会議中の通知をミュートに関する詳細を追加しました。 • デスクトップとモバイルのロケーションモニタリングを追加しました。
2021 年 1 月 12 日	<ul style="list-style-type: none"> • 索引の「ポリシーパラメータ」の項に次のパラメータを追加しました。 <ul style="list-style-type: none"> • SoftPhoneModeWindowBehavior • DeskPhoneModeWindowBehavior • 「環境の準備」の章に、コールパーク構成に関する新しいセクションを追加しました。 • 「概要」の章で、機能の表が次のように更新されました。 <ul style="list-style-type: none"> • 通話中の機能の表に次の機能を追加しました。 <ul style="list-style-type: none"> • コールのパークと取得

日付	変更内容
2020年11月24日	<ul style="list-style-type: none">• 索引の「ポリシーパラメータ」の項に次のパラメータを追加しました。<ul style="list-style-type: none">• SelfCareURL• ShowSelfCarePortal• ShowCallAlerts• 「概要」の章で、機能の表が次のように更新されました。<ul style="list-style-type: none">• 「追加機能」の表で、「Webex Teams でのコール」の行に次の注記を追加しました。<p>(注) 有料のコールライセンスを持っているユーザは、ダイヤルパッドにアクセスできます。無料のコールライセンスを使用している場合でも、他の Webex Teams ユーザに発信することができます。</p>• 「通話中の機能」の表で、モバイルの列に「セルフビューのミラー表示」を追加しました。• 「展開機能」の表で、「iPhone および iPad での Apple プッシュ通知 (APNS) と Android での着信コールのプッシュ通知」の行に次の注記を追加しました。<p>(注) 中国の規制により、iPhone および iPad のユーザは、モバイルデバイスがロックされているときに着信コールに応答するためのスライドオプションを利用できなくなりました。代わりにアラート通知が表示されます。着信コールに応答するには、まず画面ロックを解除してから通知をタップする必要があります。</p>• 「展開機能」の表に「セルフケアポータルリンクの設定」(デスクトップおよびモバイル)を追加しました。

日付	変更内容
2020 年 10 月 29 日	<ul style="list-style-type: none">• 追加機能の表に、「ダイヤル文字列への一時停止の追加」がモバイルでサポートされるようになったことを追加しました。• マルチラインおよび Jabber 移行ツールのパラメータに関して、パラメータが Unified CM で選択可能なプリセットではないことを示す注記を追加しました。これらはカスタムパラメータとしてポリシーに追加する必要があります。

日付	変更内容
2020年9月30日	

日付	変更内容
	<ul style="list-style-type: none"> • 機能の概要の表を再構成し、基本的なコール機能、通話中の機能、追加機能、展開機能を説明する4つの表に分けました。各表にはデスクトップとモバイルのサポートを示す列があり、一目でわかりやすくなっています。 • 機能の概要の表に、次のエントリが追加されました。 <ul style="list-style-type: none"> • アプリからのビデオデバイスの制御 (デスクトップ、通話中の機能) • コールオプションの簡略化 (モバイル、追加機能) • Contact Center の統合 (デスクトップ、追加機能) • Jabra ヘッドセットのサポート (デスクトップ、追加機能) • マルチライン (デスクトップ、通話中の機能) • Extend and Connect (デスクトップ、追加機能) • Dial via Office (DVO) (モバイル、追加機能) • バーチャル背景のカスタマイズ (デスクトップの展開機能) • 電話サービスの接続エラーとアクション (追加機能) • コール録音 (追加機能) • ダイアルプランマッピング (追加機能) • 「環境の準備」の章に「Unified CM の機能要件」の項を追加しました。Webex Teams で使用可能にするために事前に設定する必要がある追加機能のサブセクションを追加しました。 • 「管理とトラブルシューティング」の章に、新しい項「Jabber 連絡先と共通設定を Webex Teams に移行するためのユーザの設定」を追加しました。 • 「ポリシーパラメータ」を「付録」に移動し、次の新しいパラメータを追加しました。 <ul style="list-style-type: none"> • RemoteDestinationEditingWithMultipleDevices • RemoteInUsePresencePrimaryLineOnly • SelfCareURL • ShowSelfCarePortal • UserDefinedRemoteDestinations


日付	変更内容
	<ul style="list-style-type: none"> • EnableJabber2TeamsMigration • WebexTeamsDownloadURL <p>• 「展開」の章に「ユーザ用のバーチャル背景の設定」を追加しました。</p>
2020年8月27日	<ul style="list-style-type: none"> • 機能の概要の表に、次のエントリが追加されました。 <ul style="list-style-type: none"> • コールオプションの簡略化（コールオプションの有効化/無効化と整理）：デスクトップの展開機能 • Androidでの着信コールのプッシュ通知（モバイル） • その他のコールオプション：デスクトップ • セルフビューのミラー表示：デスクトップ • 展開の章に、新しい項「プッシュ通知の設定と推奨設定」および「ユーザ用のコールオプションの設定」を追加しました。 • 環境の章の「ボイスメールの要件」で、Unified CM と Unity Connection のリリースを一致させることが推奨され、同じ認証タイプを使用する必要があることを明記しました。 • コールでサポートされるオプションとして、VDI 版 Webex Teams を追加しました。
2020年8月10日	<p>「Webex ソフトフォンデバイスの作成と設定」の項で、モバイルソフトクライアントに緊急電話番号を設定する手順を追加しました。</p>

日付	変更内容
2020年7月30日	<ul style="list-style-type: none"> • XML 設定ファイルの手順のポリシーパラメータに「PreventDeclineOn HuntCall」を追加しました。 • 「UC マネージャプロファイルの作成」の項に、次の注記が追加されました。 <p>「一部の展開では、音声サービスと UDS ドメインの両方が必要になることがあります。ユーザの Webex Teams アカウントが Unified CM と一致しない場合、Webex Teams では、音声サービスのドメインのみからホームクラスタを見つけることはできません。この場合は UDS サーバを設定する必要があります。音声サービスドメインも、モバイルおよびリモートアクセス (MRA) のサポートと Expressway サーバの特定のために引き続き必要です。」</p> • 機能の表に次の情報が追加されました。 <ul style="list-style-type: none"> • 「画面共有は、ユーザがデスクフォンで応答している場合でも使用できます。電話機のユーザは、ビデオがサポートされていれば、電話機から共有画面を見ることができます。サポートされていない場合は、アプリで共有画面を表示します。」 (デスクトップの画面共有) • 「同僚を連絡先リストに追加するときには、そのプロフィールを編集して追加の電話番号を設定できます。これで音声通話やビデオ通話の発信時に新しい電話番号が表示されるようになるため、代替番号をコールすることも簡単です。」 (デスクトップおよびモバイルの連絡先)


日付	変更内容
2020年7月9日	<ul style="list-style-type: none">• 展開の章で、新しい項「Webex Teams でのボイスメールのアイコンインジケータ」を追加しました。• 「Unified CM での信頼されていない証明書の許可」の項に、次の段落が追加されました。「iOS デバイスでは、プライベートなエンタープライズ証明書を使用している場合、デバイス自体にカスタムのルートCAをインストールする必要があります。そうしないと、Webex Teams は SSO 承認 URL への移動に失敗します。」• 「Expressway 証明書 (MRA あり)」の項に、次の注記を追加しました。「MRA のシナリオでは、証明書は Expressway で検証する必要があるだけです。」• 「UC サービスを使用したサービスプロファイルの設定」の項で、SSO を使用しない場合にボイスメールサービスのログイン情報ソースを設定する手順を追加しました。• 「サービス検出オプション」の項で、サポートされるサービス検出方法に関する注記を更新しました。「シスコでは、内部環境と MRA 環境で SRV ルックアップをサポートしています。サービス検出により、クライアントは、エンタープライズネットワークの内部または外部にあるサービスを自動的に検出できます。クライアントは、ドメインネームサーバのクエリーを実行して、サーバの場所を提供するサービス (SRV) レコードを取得します。内部環境および外部環境について、以降の DNS SRV のガイダンスを参照してください。」

日付	変更内容
2020年6月28日	<ul style="list-style-type: none"> • 機能の概要の表に、次のエントリが追加されました。 <ul style="list-style-type: none"> • 連絡先の追加、連絡先の検索、コールする (デスクトップおよびモバイル) • 不在着信 (デスクトップ) • Webex Teams コールのコール制御 (デスクトップ) • コールピックアップ (デスクトップおよびモバイル) • 特定のアプリケーションの共有 (デスクトップ) • ハント グループ (デスクトップおよびモバイル) • セキュリティで保護されたコールのロック記号 (モバイルの展開機能) • ハントグループとコールピックアップを有効にするためのXML設定ファイルの設定方法について説明する新しいセクションを導入の章に追加しました。 <ul style="list-style-type: none"> • クライアント設定パラメータの設定 • クライアント設定ファイルの作成とホスト
2020年5月28日	<ul style="list-style-type: none"> • 機能の概要の表に、次のエントリが追加されました。 <ul style="list-style-type: none"> • 通話履歴コールバック (モバイル) • 通話の統計 (モバイル) • Webex Teams コールのデスクフォン制御 (デスクトップ) • 高解像度 (HD) ビデオ (デスクトップ) • 電話機サービスステータスのヘルスチェッカー (デスクトップ)

日付	変更内容
2020年5月6日	<ul style="list-style-type: none">• 機能概要表に次のエントリが追加されました。<ul style="list-style-type: none">• サービス ドメインの自動検出• 導入の章に、次のセクションを追加または更新しました。<ul style="list-style-type: none">• 「UC マネージャーのプロファイルおよびコール ビヘイビア ワークフロー」 (新規)• 「UC マネージャ プロファイルの作成」 (新規)• 「UC マネージャ プロファイルの編集」 (新規)• 「コール ビヘイビアと UC マネージャ プロファイル 制御ハブの設定」 (更新)
2020年4月30日	<ul style="list-style-type: none">• 機能の概要の表に、次のエントリが追加されました。<ul style="list-style-type: none">• シングル ナンバー リーチ (モバイル)• ボイスメール (モバイル)• 緊急コール (モバイル)• コール転送 (モバイル)• ビデオの共有を使用せずにコールに応答 (モバイル)
2020年3月20日	<ul style="list-style-type: none">• 機能の概要の表に、次のエントリが追加されました。<ul style="list-style-type: none">• オートゲインコントロール (AGC) (デスクトップ およびモバイル)• 会議コール (モバイル)• マージ (モバイル)• ビジュアルボイスメール (デスクトップの追加機能)• 「環境の準備」 および 「導入」 の章に、ビジュアル ボイスメールの設定要件が追加されました。

日付	変更内容
2020 年 2 月 27 日	<ul style="list-style-type: none"> • 機能の概要の表に、次のエントリが追加されました。 <ul style="list-style-type: none"> • コール待機 (モバイル) • 転送 (モバイル) • TEL、SIP、Click To Call のサポート (モバイル) • 制御ハブ ヘッドセットの管理 (追加機能) • Cisco 700 ヘッドセットに関する以下の情報を追加しました。「Cisco 700 Seriesのヘッドセットを使用している場合、ユーザはUSBアダプタを使用してコールに応答、保留、再開するだけでなく、ミュートとミュート解除を行うことができます。」 • 新しいセクション「Webex 制御ハブのシスコヘッドセットの管理」を、「管理およびトラブルシューティング」の章に追加しました。 • 新しいセクション「コール用プロトコルハンドラ」を「概要」の章に追加しました。 • エラーが発生する前に削除された「ネットワーク要件セクション」を再び追加しました。
2020 年 1 月 30 日	<ul style="list-style-type: none"> • 機能概要表に次のエントリが Windows と Mac 用に追加されました。 <ul style="list-style-type: none"> • セキュアなコールのアイコン  をロックします。 • Cisco 700 Series (Bluetooth) ヘッドセットのサポート。 • ポップアウト コール ウィンドウ。 • 一時停止をダイヤル文字列に追加します。 • 「Webex Teams でコールするためのライセンス要件 (ユニファイド CM)」では、有償のサブスクリプションが必要な場合に、ユーザアカウントを組織内で管理する必要があるため、ユーザアカウントは Webex アプリでのコール (Unified CM) を使用する特定のライセンス割り当てを要求しません。

日付	変更内容
2019年12月20日	<ul style="list-style-type: none">• 機能の概要の表に、次のエントリが追加されました。<ul style="list-style-type: none">• モバイルプラットフォームの保留/再開。• デスクトップ、デスクフォン制御モード、およびモバイルのさまざまなデバイスで再開します。• モバイルプラットフォームの通話履歴。• 「ヘッドセットの要件」セクションに、次の注意事項が追加されました。「Webex Teams で Cisco Headset 500 Series または Cisco Headset 700 Series ヘッドセットを使用すると、ヘッドセットファームウェアが自動的に更新されます。ユーザは、更新が利用可能であることを知らせるメッセージをポップアップ表示し、更新後に確認応答することができます。」
2019年12月10日	<ul style="list-style-type: none">• 「環境の準備」の章にネットワーク要件情報が追加されました。• 「組織の SIP アドレスルーティングを設定する」の項で、次の内容を追加しました。「*. example.com は、トップレベルドメインではなくサブドメインのみに一致します。」
2019年11月27日	<ul style="list-style-type: none">• デスクトッププラットフォームの機能概要テーブルに通話履歴が追加されました。• ネットワークの「DSCP 値を設定」すると、AF31 から CS3 にマーキングするシグナリングパケットが変更されます。

日付	変更内容
2019年11月15日	<ul style="list-style-type: none"> • [展開 (Deploy)] の章では、モバイルソフトフォンモードの関連する導入手順と Webex Teams 認証手順を追加しました。 • 機能の概要の表に、次のモバイル機能が追加されました。 <ul style="list-style-type: none"> • 発信 • コールへの応答 • ミュート/ミュート解除 • 通話終了 • コールのプレゼンス: Webex Teams では、同じ組織内のユーザは、アクティブコール中にこのプレゼンスインジケータを表示できます。  • 基本的な共有電話アピランス • コール中の DTMF 入力
2019年11月7日	<ul style="list-style-type: none"> • 機能の概要テーブルに次の機能が追加されました。 <ul style="list-style-type: none"> • Webex Teams コール (Windows または Mac): ユーザは、自分の電話番号を使用して、または Webex Teams コールを使用して発信するかどうかを選択できます。Webex Teams コールは、Webex Teams を使用している他のユーザにコールするための簡単な方法です。ユーザは、通話中に画面とホワイトボードを共有できますが、コールを保留にしたり、コールを転送したり、電話のコールでのみ使用可能な他の機能を使用したりすることはできません。 • SIP (URI) アドレスルーティング: コントロールハブで設定可能です。この設定では、Webex クラウドを介してルーティングされる SIP アドレスを決定できます。デフォルトでは、Webex サービス以外のすべての SIP Uri が、ユニファイド CM を介してルーティングされます。

日付	変更内容
2019年10月9日	<ul style="list-style-type: none">• Unified CM 証明書 (展開で MRA あり) (75 ページ) では、Cisco CallManager 証明書への参照が削除され、次のメモが追加された：「Tomcat証明書は、Webex Teamsが暗号化された呼び出しに対して有効になっている場合のセキュアSIPにも使用される (SIP OuthはMRAのデフォルトポート5091で動作する)。詳細については、このガイドの「暗号化されたコールの電話セキュリティプロファイルの設定」を参照してください。」• Unified CM 証明書 (展開で MRA なし) (74 ページ) に、次の注記が追加されました。「Tomcat 証明書は、Webex Teams が暗号化されたコールに対して有効になっている場合にセキュア SIP にも使用されます (SIP Oauth はデフォルトポート5090で動作します)。詳細については、このガイドの「Configure the Phone Security Profile for Encrypted Calls」を参照してください。」

日付	変更内容
2019年9月26日	<ul style="list-style-type: none"> • Webex アプリでのコール (Unified CM) の概要 (25 ページ) の機能テーブルに次の機能が追加されました。 <ul style="list-style-type: none"> • 表示時またはDNDが有効になっているときにコール通知を抑制します。 • Tel、sip、および clicktocall プロトコルのサポート。 • Outlook からのクリック通話のサポート。 • Cisco 500 Series ヘッドセットのサポート • 新しいセクション「ヘッドセットの要件 (78 ページ)」を追加しました。 • 既知の既知の問題が削除されました。「Webex Teams はセキュアソフトフォンモードではユニファイド CM に登録されません。回避策として非セキュアモードを使用する必要があります。」セキュアモードがサポートされていないその他の不正な情報を削除しました。 • 暗号化された通話用の電話機セキュリティプロファイルを構成 (105 ページ) の SIP Oath 設定の固定手順。暗号化されたコールには、ユニファイド CM 12.5(1) 以降が必要です。 • Webex アプリ での電話サービスの認証 (122 ページ) 追加された注: 「サーバアドレスと UC ドメインの両方が設定されている場合、オンプレミスでのみサーバアドレスがユニファイド CM に接続するために使用されます。DNS SRV による自動検出は無視されます。MRA の場合、サーバアドレスは無視されます。」
2019年8月29日	<ul style="list-style-type: none"> • 新しいセクションとして、暗号化された通話用の電話機セキュリティプロファイルを構成 (105 ページ) を追加。 • ソフトフォンとデスクフォンの両方の制御モードでは、次の機能テーブルに新しいWebex アプリでのコール (Unified CM) の概要 (25 ページ) 通話中機能を追加しました。 <ul style="list-style-type: none"> • 会議 • マージ • 転送

日付	変更内容
2019年7月25日	<ul style="list-style-type: none">自動検出を実行するかどうかを確認するには、[「Webex Teams で認証 (ckm With Webex Teams」)] コンテンツを使用して、ユーザ設定パスを表示します。
2019年7月9日	<ul style="list-style-type: none">Softphone モードの Webex Teams のマージおよび転送機能に関する限定的な利用上の免責事項を削除しました。(これらの機能は現在一般に利用できる)。
2019年6月27日	<ul style="list-style-type: none">プレビューリリースの免責事項が削除されました。(Webex Teams (ユニファイド CM) のコールは公式に使用できません)。Softphone モードの Webex チームに対して、マージおよび転送を限定された可用性機能として追加しました。付録に新しいセクション Unified CM で信頼できない証明書を許可する (158 ページ) が追加されました。証明書の要件と既知の問題に次の情報が追加されました。廃止された「署名アルゴリズム (sha-1 など) で発行された証明書は機能しません。Cisco Unified Communications Manager の『Administration Guide』の「証明書 (Certificates)」の章に記載されているように、サポートされているセキュアシグニチャ256アルゴリズムを使用する必要があります。」

日付	変更内容
2019年6月14日	<ul style="list-style-type: none"> • ユーザー向け Webex アプリの通話エクスペリエンス (47 ページ) で、「Hybrid Call Service ユーザのユーザ体験の変更」セクションに次の情報が追加されました。 「Webex デバイスが Hybrid Call Service に対応した場所として制御ハブで設定されている場合、ユーザは Webex Teams からダイヤルでき、そのコールは、受信側の発信者 ID としてそのデバイスの電話番号を使用して Webex デバイスで開始されます。」 • 証明書の要件 (74 ページ) で、MRA 証明書の要件と再構成を 3 つのサブセクションとして追加しました。これは、ユニファイド CM 証明書 (MRA なし)、ユニファイド CM 証明書 (MRA)、および Expressway 証明書 (MRA) です。 • ネットワークで DSCP 値を設定 (158 ページ) で、QoS ポート範囲情報を修正します。以前は、オーディオストリームの場合は「16384 ~ 24574」、ビデオストリームの場合は「24575 to 32766」を読み取ります。ここでは、「16384 ~ 24575」と「24576 ~ 32676」をそれぞれ読み取ります。
2019 年 4 月 24 日	<ul style="list-style-type: none"> • 再構成の要件セクション: Webex Teams (ユニファイド CM) 要件の各コールには、より簡単に検索できるようにするための独自のサブセクションが用意されています。 • 「導入」の章に新しいセクション (Webex アプリでのコール (Unified CM) の Unified CM エンドユーザーの構成 (98 ページ)) が追加されました。

日付	変更内容
2019年4月10日	<ul style="list-style-type: none"> • デスクフォン制御モードで会議に参加 (55 ページ) がコールフローに追加されました。 • 「要件」のセクションに次の点を追加しました。 <ul style="list-style-type: none"> • Cisco Unified CM Administration > System > Server では、Unified CMサーバ名はFQDNとして定義される必要がある。 • Sso を使用していない MRA の導入モデルと SSO を備えたユニファイドCMはサポートされていません。 • 現時点では、内部のみの自動検出をサポートしています。サービス ディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。クライアントは、ドメイン ネーム サーバのクエリーを実行して、サーバの場所を提供するサービス (SRV) レコードを取得します。 • サーバ情報を使用して、SRV レコードではなく設定として使用している場合は、ユーザの Webex Teams の電子メールアドレスは Unified CMのメールアドレスと一致する必要があり、少なくとも、ドメインが一致する前のユーザID部分と一致している必要がある。
2019年3月28日	<ul style="list-style-type: none"> • ドキュメントの初期バージョン。

Webex アプリでのコール (Unified CM) の概要

Webex アプリでコールイン (Unified CM) ソリューションを使用すると、Webex アプリを Cisco Unified Communications Manager 呼制御環境 (オンプレミス企業、Business Edition 6000/7000、Unified CM Cloud、または HCS パートナーソリューションを介して提供されるもの) に直接登録できます。

ユーザ

このソリューションによってエンドユーザのコールエクスペリエンスが強化され、ユーザは、Unified CM 環境を通じて Webex アプリで直接コールを発信したり、通話中の機能を使用したり、Webex アプリからデスクフォンを制御したりできます。

Webex アプリからダイヤルする場合、ユーザはデスクフォンと同じダイヤル文字列やプレフィックスを使用できます。Webex アプリは、Unified CM に登録されている他のデスクフォンと同じように機能します。Webex アプリで確立された Unified CM コールでは、Unified CM

展開に適用されている設定（場所、帯域幅設定、ポイントツーポイントメディアなど）が使用されます。

管理者

Webex アプリでコールイン (Unified CM) の管理者は、すでに設定済みの既存の Unified CM とモバイルおよびリモートアクセス (MRA) 構成を再利用できます。導入モデルは Jabber に似ています。同じデバイスタイプを使用する：ソフトフォンモードの場合、Webex アプリは SIP デバイスとして登録され、その製品タイプは、デスクトップでは「Cisco Unified クライアント サービス フレームワーク」または CSR、モバイルでは、TCT または BOT、タブレットでは、TAB となります。または、Webex アプリは CTI を使用して Unified CM に接続して、ユーザのエンドポイントを制御できます。

Webex アプリは Webex クラウドへのプライマリ接続を確立し、サービス構成（メッセージング、会議、プレゼンス、連絡先リスト、通話動作など）を取得しますが、ユーザーに特定の通話機能を提供するために Unified CM 環境から次の構成も読み取ります。


- 設定済みの音声サービスドメインを検出する DNS クエリを介した最初の Unified CM Discovery。（マルチクラスタ環境では、クラスタ間ルックアップサービスも活用して、Unified CM ユーザがホームであるクラスタを特定します）。外部ドメイン（MRA の導入）も検出されます。（Webex ドメインが既存の音声サービスドメインと一致しない場合、Control Hub で音声サービスドメインを設定し、特定のユーザに関連付けます。）
- UC サービスパラメータ（Cisco Unity Connection、CTI サービスおよび Jabber 構成サービス プロファイルまたは XML ファイルの対応するパラメータを介した高度な発信機能によるボイスメール向け）
- アイデンティティプロバイダー (IdP) が同号されている場合の、シングルサインオン (SSO) ログイン情報
- 更新および有効期限タイマーを含む Oath トークン。（セッションの有効期限が切れた場合、ユーザは再認証する必要があります）。
- 証明書の検証

Webex アプリの通話機能

この統合により、デスクトップ (Windows および Mac) およびモバイル (Android、iPad、iPhone) 用の Webex アプリで、次の機能セットが提供されます。可能な限り、この表の機能の一覧には、エンドユーザに関連したヘルプ記事へのリンクを含めています。通話発信に関する一般情報は、「[音声およびビデオ通話](#)」を参照してください。エンドユーザー向け機能比較表については、「[サポートされている通話オプション](#)」を参照してください。

基本的なコール機能

表 1: 基本的なコール機能

機能	説明と資料	デスクトップ	モバイル
コールへの応答	—	✓	✓
ビデオを共有せずにコールに応答	すべての着信に対してビデオをオフにするを参照してください。	✓	✓
デスクフォン制御	デスクフォン制御 (Webex アプリでのミーティングやコールなど) : 「デスクフォン電話をかける」を参照してください。	✓	
コール中のDTMF入力	—	✓	✓
通話終了	—	✓	✓
発信	—	✓	✓
ミュート/ミュート解除	—	✓	✓
コールのプレゼンス	Webex アプリでは、アクティブコールの継続中、同じ組織内のユーザにこのプレゼンスが表示されます。 	✓	✓

通話中の通話機能

表 2: 通話中の通話機能

機能名	説明と資料	デスクトップ	モバイル
コール ピックアップ	あるユーザがカスタマーサポートの役割を担当していて、その同僚が電話機への着信コールに回答できない状況になったとします。このとき、両者が同じピックアップグループに属していると、サポートユーザが Webex アプリ で通知を受け取ります。このユーザは、アプリケーションの通知からのコールに回答できます。ユーザは、他のピックアップグループでコールを受信することもできます。「別のユーザーへの着信を取る」を参照してください。	✓	✓
コール録音	コールの録音に関して、ユーザにどの程度の制御を与えるかを決定できます。設定によって、着信コールと発信コールが自動的に録音される場合や、録音するコールをユーザが決定できる場合があります。ユーザによるコール録音を有効にすると、ユーザが自由に録音を開始および停止できるようになります。コールを録音している場合、その録音は、ユーザがコールを別のデバイスに転送したり、別のアクティブコールとマージしたり、会議コールを開始したりしても継続されます。ユーザには、コールが録音中であることを知らせるビジュアルインジケータが表示されます。「通話を録音する」を参照してください。	✓	✓

機能名	説明と資料	デスクトップ	モバイル
コール ウェイティング	すでに通話中のユーザに他の人からのコールが着信した場合、コールを受けたユーザは、その着信をどのように処理するかを選択できます。たとえば、ユーザはアクティブコールを保留にし、2番目のコールに応答することができます。詳細は、「 着信待ち受けに回答する 」を参照してください。	✓	✓
会議通話	ユーザは、通話中に他の人をコールに追加して、その場で会議コールを開始することができます。この方法で開始された会議コールには、他のユーザを8人まで追加できます。「 電話会議を開始する 」を参照してください。	✓	✓
アプリからのビデオデバイスの制御	ユーザは、接続されているビデオデバイスでのビデオの共有を、アプリから直接開始または停止できます。たとえば、Cisco Webex Board に接続しているときにビデオを共有したくない場合、Board のそばまで行ってビデオをオフにする必要はありません。アプリからオフにすることができます。「 Webex Boards、Room、Desk デバイスでの会議中や通話中にビデオをオフにする 」を参照してください。	✓	
保留/復帰	ユーザは、Webex アプリでコールを保留にしたり再開したりできます。 通話を保留にする を参照してください。	✓	✓
ハントグループ	ユーザは、コール設定からハントグループにサインインまたはサインアウトできます。ログインしていて、その所属先のグループにコールが入ると、着信コール通知のハントグループ番号が表示されます。「 ハントグループにサインインする 」を参照してください。	✓	✓

機能名	説明と資料	デスクトップ	モバイル
マージ	ユーザは、2つのアクティブコールを受け取って、Webex アプリで1つの会議コールにマージできます。 2つの通話のマージ を参照してください。	✓	✓
セルフビューのミラー表示	セルフビューのミラー表示：デフォルトでは、ユーザがコール中にビデオを共有すると、自分の姿も鏡に映したように表示されます。背後にテキストがある場合に、逆方向に読む必要なく簡単に読み取れるようにするには、[自分のビデオビューのミラー表示 (Mirror my video view)] 設定をオフにすることができます。この設定は、ミーティングに参加している他のユーザへの表示には影響しません。「 セルフビュービデオのミラービューをオフにする 」を参照してください。に移動します。	✓	✓
通話をミーティングに移動する	通話中のユーザは、文字起こし、リアルタイム翻訳、メモ、アクションアイテム、録音およびホワイトボードなどの高度な会議機能を有効活用できます。そのコールをフル機能の会議に移動します。コールを会議に移行する前に、ユーザは他のユーザを会議に招待できます。	✓	✓
マルチライン	ユーザは、Webex アプリで最大8本の電話回線を使用でき、各回線で通話転送、転送、ハントグループ、共有回線、ボイスメールなどの高度なコール機能を利用できます。回線ごとに異なる呼出音を割り当てることもできます。また、共有回線のプレゼンスを有効にすると、ユーザに回線のステータスが表示されます。「 通話用のアクティブな回線を変更する 」を参照してください。	✓	

機能名	説明と資料	デスクトップ	モバイル
コールのパークと取得	ユーザが、あるデバイスでコールをパークすると、そのユーザまたは他のユーザは別のデバイスからそのコールに応答できます。	✓	✓
別のデバイスからの再開	ユーザは、デスクトップアプリからコールを保留にして、モバイルで再開することができます。または、モバイルコールを保留にして、デスクの電話機で再開します。デスクフォン、モバイル、デスクトップ間の任意の方向に移動します。コールを保留にし、都合のよい場所で再開します。 通話を保留にする を参照してください。	✓	✓
画面共有	<p>画面共有 : Webex アプリでのコール中に、コンピュータ画面のコンテンツを共有できます。ユーザは、画面全体を共有するのではなく、特定のアプリケーションを選択して共有することができます。画面共有は、ユーザがデスクフォンで応答している場合でも使用できます。電話機のユーザは、ビデオがサポートされていれば、電話機から共有画面を見ることができます。サポートされていない場合は、アプリで共有画面を表示します。通話中に画面を共有するを参照してください。</p> <p>(注) ユーザは、呼び出された人物がクラウドに登録されたデバイスを使用しているか、オンプレミスのデバイスを使用しているかにかかわらず、画面を共有できます。画面の共有は、高フレームレート (30 FPS)、高解像度 (1080p)、およびオーディオを使用して送信されます。</p>	✓	

機能名	説明と資料	デスクトップ	モバイル
フロントカメラとバックカメラの切り替え	携帯電話やタブレットでは、フロントカメラとバックカメラを切り替えることができます。「 ビデオ設定を変更する 」のモバイルの項を参照してください。		✓
転送	接続中のコールを Webex アプリ 内でリダイレクトします。ターゲットは、別のユーザがコールを転送する必要があるユーザです。 通話の転送 を参照してください。	✓	✓
仮想カメラ	ユーザーは通話中に、仮想カメラを使用するか選択できます。アプリケーション、ドライバ、ソフトウェアなどの仮想カメラを使用して、ビデオ、画像、またはフィードのオーバーレイを作成できます。	✓	

追加機能

表 3: 追加機能

機能名	説明と資料	デスクトップ	モバイル
ダイヤル文字列への一時停止の追加	ユーザは、入力した電話番号に一時停止を追加できます。これは、会議コールに参加する場合や、自動システムへの応答として番号を入力するときに必要となることがあります。番号にコンマ (,) を追加することで、ダイヤルを 1 秒間遅延させることができます。遅延時間を伸ばすために、複数のコンマを行に追加することができます。例： 95556543123,,,56789。	✓	✓

機能名	説明と資料	デスクトップ	モバイル
連絡先の追加、連絡先の検索、およびコールの発信	<p>ユーザは、同僚を連絡先リストに追加し、自由にグループ化して、チャットやコールが必要なときに相手を見つけやすくすることができます。</p> <p>Outlook の連絡先 (Windows)、ローカルのアドレス帳 (Mac)、ローカルの電話機の連絡先 (iPhone、iPad、および Android) を Webex アプリ から参照することもできるため、簡単に連絡先を見つけて発信できます。</p> <p>同僚を連絡先リストに追加するときには、そのプロフィールを編集して追加の電話番号を設定できます。これで音声通話やビデオ通話の発信時に新しい電話番号が表示されるようになるため、代替番号をコールすることも簡単です。「連絡先リストにユーザーを追加する」を参照してください。</p>	✓	✓
オートゲインコントロール (AGC)	<p>AGC は、着信オーディオレベルをリッスンし、音が大きすぎる場合や小さすぎる場合に録音レベルを調整する独自の回路です。音量が大きすぎると、音量が自動的に小さくなります。音声が強すぎる場合、音は自動的に増幅されます。これによって、OS レベルでの音声の音量が調整されることはありません。</p>	✓	✓


機能名	説明と資料	デスクトップ	モバイル
Webex アプリでのコール	<p>ユーザは、コールの発信時に電話番号を使用するか、Webex アプリでのコールを使用するかを選択できます。Webex アプリでのコールは、Webex アプリを使用している他のユーザにすばやく発信できる手段です。ユーザは、通話中に画面とホワイトボードを共有できますが、コールを保留にしたり、コールを転送したり、電話のコールでのみ使用可能な他の機能を使用したりすることはできません。「Webex アプリ アカウントを持つ任意の相手に発信する」を参照してください。</p> <p>(注) 有料のコールライセンスを持っているユーザは、ダイヤルパッドにアクセスできます。無料のコールライセンスを使用している場合でも、他の Webex アプリ ユーザに発信することができます。</p>	✓	✓
Webex アプリでのコールのコール制御	<p>Cisco 730 ヘッドセットを使用している場合、ユーザは USB アダプタまたは Bluetooth を使用して、コールの応答と終了、コールの保留と再開、コールのミュートとミュート解除を行うことができます。「シスコヘッドセット 730 への通話の発信と応答」を参照してください。</p>	✓	

機能名	説明と資料	デスクトップ	モバイル
コール履歴	<p>ユーザが組織内の他の人にコールを発信すると、コール履歴に電話番号の詳細が表示されます。そのため、誰かをコールバックするために、ユーザは職場または携帯電話のいずれかの番号をコールしているかどうかを確認できます。</p> <p>コール履歴内の名前の横に表示される [コール (Call)] アイコンを選択すると、その履歴の番号に自動的にコールバックします。他のユーザの電話番号を探して選択する必要がなくなりました。不在着信に折り返し電話をした後、通話履歴からその通話を削除できます。通話履歴には、過去 30 日間の 200 件の通話だけが表示されます。詳しくは、「通話履歴の表示」を参照してください。</p>	✓	✓
通話統計	<p>ユーザは、通話中にパケット損失、遅延、解像度レートなどのコールの統計情報を確認できます。「通話の統計情報にアクセスする」を参照してください。</p>		✓
Outlook からのクリックツーコール	<p>Windows または Mac コンピュータでは、Microsoft Outlook や Web ブラウザのリンクなど、アプリ外でクリックした電話番号をコールするためのデフォルトオプションとして Webex アプリを設定できます。クリックして別のアプリからコールするを参照してください。</p>	✓	

機能名	説明と資料	デスクトップ	モバイル
クライアント識別コード (CMC) と Forced Authorization Code (FAC; 強制承認コード)	<p>クライアント識別コード (CMC) と強制承認コード (FAC) により、コールアクセスとアカウントリングを効果的に管理できます。CMCはクライアントのコールアカウントリングおよび請求を支援し、FACは特定のユーザが発信できるコールのタイプを規定します。</p> <p>CMCを使用する場合、ユーザはコードを入力する必要があります。この操作により、コールが特定のクライアント識別に関連していることが指定されます。コールアカウントリングおよび請求を目的として、クライアント識別コードを顧客、学生、またはその他のグループに割り当てることができます。FACを使用する場合、コールが確立する前に、特定のアクセスレベルで割り当てられた有効な認証コードをユーザが入力する必要があります。「環境の準備」の章を参照してください。</p>	✓	✓
Contact Center の連携	<p>Webex アプリは、Cisco Contact Center アプリケーションに統合し、Finesse デスクトップから制御することができます (Unified Contact Center Enterprise または Express)。この統合では、マルチライン、録音、会議などのコンタクトセンター機能がサポートされます。サポートされている最新の機能については、「Contact Center の連携」を参照してください。</p>	✓	
Webex アプリでの診断	<p>接続の問題が発生した場合は、診断ツールを使用すると、構成エラーの特定、ネットワーク診断レポートのエクスポートを実行できます。この情報は、発生した問題のトラブルシュー트에役立ちます。「トラブルシュート」の章を参照してください。</p>	✓	


機能名	説明と資料	デスクトップ	モバイル
Dial-via-Office (DVO)	DVOが設定されたユーザには、携帯電話接続を使用して仕事のコールを発信するオプションが提供されます。これにより、データ接続が利用できない場合でもコールを続行できます。ユーザがどのオプションを選択しても、発信者IDには常に勤務先電話番号が使用されるため、他の人は簡単にユーザを識別することができます。「 携帯電話接続を介して仕事の電話を発信する 」を参照してください。		✓
ダイヤルプランのマッピング	Cisco Unified Communications Managerのダイヤルルールがディレクトリのダイヤルルールと確実に一致するように、ダイヤルプランのマッピングを設定します。「 環境の準備 」の章を参照してください。	✓	✓
緊急コール	ユーザが Webex アプリ で緊急コールを発信した場合、デバイスの電話アプリを使用して発信が行われます。これにより、緊急サービスがネットワークキャリアを介して位置を正確に特定しやすくなります。		✓
Extend and Connect	コールの発信や受信を行うときに、代行用デバイスに接続するようにユーザを設定できます。これらのデバイスは、コール設定を開いたときに [代行用デバイス (Alternate Devices)] に表示されます。ここで、代行用デバイスの電話番号を追加または編集できます。「 代替デバイスから電話をかける 」を参照してください。	✓	


機能名	説明と資料	デスクトップ	モバイル
ファストフェールオーバー (MRA)	Webex はシャットダウン、ノード障害、ネットワーク障害の制御などの障害を迅速に検出し、MRA を介してバックアップパスに対してシームレスにフェールオーバーを実行するため、ユーザの生産性に影響を与えることはありません。「環境の準備」の章を参照してください。	✓	✓
電話サービスステータスのヘルスチェッカー	電話サービスが正常に動作しているかどうか分からない場合は、アプリから電話接続のステータスを検査できます。Windows の場合、プロフィールの写真をクリックしてヘルプ > ヘルス チェッカーに移動します。Mac の場合、ヘルプ > ヘルス チェッカーに移動します。ヘルス チェッカーは、接続をテストし、問題があるかどうかをユーザに通知します。	✓	
高解像度 (HD) ビデオ	ユーザは、HD ビデオを有効または無効にすることができます。そのためには、プロフィール画像をクリックし、[設定 (Settings)] (Windows) または [個人設定 (Preferences)] (Mac) に移動し、[ビデオ (Video)] を選択して、設定を有効または無効にします。コンピュータプロセッサが大きい場合や、通話中または会議中にネットワーク帯域幅を節約する必要がある場合は、HD ビデオを無効にすることをお勧めします。	✓	
ロケーションモニタリング	ロケーションモニタリングをオンにすると、ユーザが Webex から 911 などの緊急サービスに電話をかけた場合、ユーザのロケーションが自動的に緊急時対応要員に共有されます。	✓	✓

機能名	説明と資料	デスクトップ	モバイル
不在履歴	[コール (Calls)]  タブの赤いバッジカウンタで、不在着信の数を確認できます。[コール (Calls)] タブには着信コールと発信コールのリストが表示され、通話履歴から他のユーザにコールバックできます。スケジュールされたミーティングが[ミーティング (Meetings)] タブに表示されるので、この2つのタイプの通信を簡単に識別できます。	✓	
その他のコールオプション	ユーザは、アプリ内で任意のタイプのコールを発信できる場所であればどこからでも (ユーザの検索や、そのユーザと一緒に参加しているスペースなど)、他の人のビデオアドレス (bburke@biotechnia.com など) をコールできます。	✓	
マルチコールウィンドウ	複数の回線を持つ Webex アプリユーザには、デフォルトでこれが表示されます。これは、複数回線または共有回線の管理に役立つ独立したフローティングウィンドウです。「 複数通話ウィンドウで通話を管理する 」を参照してください。	✓ (Windows)	
ネットワークハンドオフ (Wi-Fi から LTE)	アクティブな通話中にネットワークを変更する必要がある一方で、通話を Webex で保持したい場合でも、心配する必要はありません。この変更は、通話品質に影響を与えることなくまた、中断せずに自動的行われます。(「環境の準備」の「Unified CM機能」を参照してください。)	✓	✓
連絡先カードの電話番号	勤務先電話番号と携帯電話番号は Active Directory から同期され、Webex アプリで選択可能な項目として表示されます。(ユーザの電話番号属性を Webex クラウドに同期するには、Cisco Directory Connector が必要です)。	✓	✓

機能名	説明と資料	デスクトップ	モバイル
電話サービスの接続エラーとアクション	電話サービスが切断された場合は、Webex アプリのフッターに、より説明的なエラーメッセージが表示されます。「 エラーメッセージ 」を参照してください。	✓	✓
ポップアウトコールウィンドウ。	ユーザが他のユーザに発信すると、コールウィンドウがポップアウトし、両方のユーザがコール機能にアクセスできるようになります。コール中であっても、ユーザは重要なメッセージに応答できます。	✓	
インドのモバイルアプリユーザー向け PSTN 通話	インドのユーザーは、企業のネットワークに接続できないときにこの電話をかけることができます。Webex モバイルアプリでは、これの代わりにデバイスの Calling アプリを使用するオプションが提供されます。付録の「 customization policy パラメータ 」に記載されている「 EnablePhoneDialerOptionOverMRA 」を参照してください。		✓
パーソナルモードデバイスの PSTN	ハイブリッドコールを利用することで、ユーザのパーソナルモードデバイスに PSTN アクセスを提供できます。（『 Cisco Webex Devices 用ハイブリッドコールに関する導入ガイド 』を参照してください）。	✓	
緊急通報用の RedSky 位置情報報告	Ray Baum の法律に準拠するために、ユーザーがオフィス外にいるときに正確な位置情報の提供を要求できます。	✓	✓
セルフケアポータル：通話転送	ユーザが仕事のコールを別の番号で受ける必要がある場合は、Webex アプリから通話転送を直接設定できます。コール転送番号を入力するだけで、その番号で呼び出し音が鳴ります。「 通話を転送する 」および「 その他の通話設定にアクセスする 」を参照してください。	✓	✓

機能名	説明と資料	デスクトップ	モバイル
セルフケアポータル：シングルナンバーリーチ (SNR)	ユーザは、Webex アプリ からセルフケアポータルにアクセスし、会社のディレクトリ番号と同時に呼出音を鳴らすデバイスの番号を追加できます。「 任意の番号で受信する 」および「 その他の通話設定にアクセスする 」を参照してください。	✓	✓
Cisco 500 Seriesおよび 700 Series (Bluetooth) ヘッドセットのサポート	Cisco 700 Seriesのヘッドセットがある場合、ユーザはUSBアダプタを使用して、コールの応答と終了、コールの保留と再開、コールのミュートとミュート解除を行うことができます。 ユーザが Webex アプリ でシスコヘッドセットを使用しているときは、Webex Control Hub でこれを追跡できます。これにより、インベントリを追跡し、ユーザの問題のトラブルシューティングを行うことができます。(導入の章を参照してください)。	✓	
Jabra ヘッドセットのサポート	サポートされるモデルについては、「 Details%20about%20Headset%20Support 」を参照してください。	✓	
オンライン中で、DND が有効の際、または通話中や会議中の場合、通話通知を非表示できます。	ユーザが着信通話の通知をミュートにすると、着信音が聞こえなくなり、通知も表示されなくなります。ボイスメールを設定した場合、発信者はメッセージを残すことができます。通話はスペースリストと通話履歴に表示されます。	✓	

機能名	説明と資料	デスクトップ	モバイル
Webexから携帯電話アプリに通話を切り替える	Webex でアクティブな通話をしていて、その場で通話に参加したい場合は、通話を Webex から携帯電話アプリに切り替えます。[詳細 (More)]  から素早く切り替えながら、通話を少し中断するだけで、接続と通話品質を維持できます。（「展開」章と「通話を携帯電話アプリに切り替える」を参照してください。）。		✓
tel、sip、および clicktocall プロトコル	この概要の章の該当する項を参照してください。	✓	✓
ボイスメール	Webex アプリでコールを見失うことはもうありません。ユーザは、[コール (Calls)] タブでボイス メールを管理できます。赤いバッジのカウンターを使用すると、ボイスメッセージの数を把握できます。メッセージの詳細をチェックアウトしたり、再生したり、読み取り専用としてマークしたり、そのメッセージを削除したり、送信者にコールバックしたりすることができます。Webex アプリまたはデスクフォンでメッセージを聞くと、赤いバッジカウンタは消去されます。ボイスメールを参照してください。	✓	✓


機能名	説明と資料	デスクトップ	モバイル
ビジュアルボイスメール	ビジュアルボイスメール: Webex アプリでコールを見失うことはもうありません。ユーザは、すべてのボイスメールを管理するための専用ボイスメールタブ  を取得します。赤いバッジのカウンターを使用すると、ボイスメッセージの数を把握できます。メッセージの詳細をチェックアウトしたり、再生したり、読み取り専用としてマークしたり、そのメッセージを削除したり、送信者にコールバックしたりすることができます。Webex アプリ またはデスクフォンのメッセージを聞くと、赤いバッジカウンターは消去されます。ボイスメールを参照してください。	✓	

導入機能

表 4: 導入機能

機能名	説明とマニュアル	デスクトップ	モバイル
Apple および Android のプッシュ構成 (APN)	iPhone、iPad、および Android デバイスでは、プッシュ通知によって Webex アプリの着信コールをユーザに知らせることができます。（「環境の準備」の章を参照してください）。 (注) 中国の規制により、iPhone および iPad のユーザは、モバイルデバイスがロックされているときに着信コールに応答するためのスライドオプションを利用できなくなりました。代わりにアラート通知が表示されます。着信コールに応答するには、まず画面ロックを解除してから通知をタップする必要があります。		✓

機能名	説明とマニュアル	デスクトップ	モバイル
ローカルプッシュ通知サービス (LPNS)	<p>これは、次の動作条件下で、iOS デバイスの Webex ユーザーに VoIP 着信通話を通知するための信頼性が高く安全な方法です。</p> <ul style="list-style-type: none"> • WiFi に制約されたネットワーク。 • インターネットに接続されていないため、Apple プッシュ通知サービス (APN) にアクセスできません。 <p>(注) 1. LPNS 通話通知を取得するには、ユーザーは Webex アプリにローカルネットワーク権限を付与する必要があります。</p> <p>2. LPNS と APN の両方が UCM で設定されている場合、UCM は最初に LPNS チャネルを介して通話を発信し、失敗した場合は、APN がベストエフォートのフォールバックオプションになります。</p> <p>3. ユーザーが複数の iPhone または iPad を使用している場合、LPN 通話通知を適切に機能させるには、Webex アプリが 1 台の iPhone と 1 台の iPad でのみ実行されるようにする必要があります。</p>		<p>✓</p> <p>iOS および iPad OS</p>
サービス ドメインの自動検出	Control Hub を使用して UC マネージャプロフィールを設定すると、Webex アプリ でユーザの [電話サービス (Phone Services)] 設定に自動的にサービスドメインを追加できます。この方法では、手動でドメインを入力する必要がなく、すぐにログインすることもできます。(導入の章を参照してください)。	✓	✓
セルフケアポータルリンクの設定	アプリの [通話設定 (Call Settings)] からユーザがアクセスするポータルリンクを選択できます (ファイルの設定手順については展開の章を、関連するポリシーパラメータについては付録を参照してください)。	✓	✓
バーチャル背景のカスタマイズ	ユーザは、バーチャル背景として使用する独自の画像を最大 3 つ追加できます。「Webex アプリ ユーザー向けに仮想背景を設定する」を参照してください。	✓	

機能名	説明とマニュアル	デスクトップ	モバイル
緊急ダイヤルの免責事項をカスタマイズ	<p>緊急ダイヤルの免責事項の内容は、さまざまな地域や状況の規制やビジネスニーズに合わせてカスタマイズできます。</p> <p>緊急対応インフラストラクチャの準備が整っていない場合、免責事項のポップアップの頻度を変更したり、非表示にできます。(付録の customizable パラメータを参照してください)。</p>	✓	✓
すべての 1 対 1 会議のビデオを無効にする	Control Hub を使用すると、コンプライアンス、プライバシー、またはネットワークの目的で、会議のビデオを無効にするか、デフォルトでビデオを Off に設定できます。	✓	✓
Expressway モバイルリモートアクセス (MRA) Webex アプリ	<p>MRA は、VPN で企業のネットワークに接続せずに Webex アプリ トラフィックのセキュアな接続を提供します。(『Cisco Expressway 経由のモバイルおよびリモートアクセスに関する導入ガイド https://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html』を参照してください)。</p>	✓	✓
セキュアで暗号化されたコール	暗号化されたコールを Unified CM から設定できます。Webex アプリでは、これらのコールにロックアイコン  が表示されます(導入の章を参照してください)。	✓	✓
サービス検出	サービス検出により、クライアントは、エンタープライズ(内部)ネットワークおよび MRA(外部)ネットワークにあるサービスを自動的に検出できます。(導入の章を参照してください)。	✓	✓
コールオプションの簡略化(コールオプションの有効化/無効化と整理)	ニーズに合わせてコールオプションを設定できます。たとえば、同僚の勤務先電話番号、携帯電話番号、または SIP URI アドレスを使用して発信することがあるだけで、Webex アプリ コールを発信する必要はないとします。この場合は、Webex アプリでのコールを無効にして、そのオプションがコールの発信時に表示されないようにできます。「 組織の通話設定を構成する 」を参照してください。	✓	✓

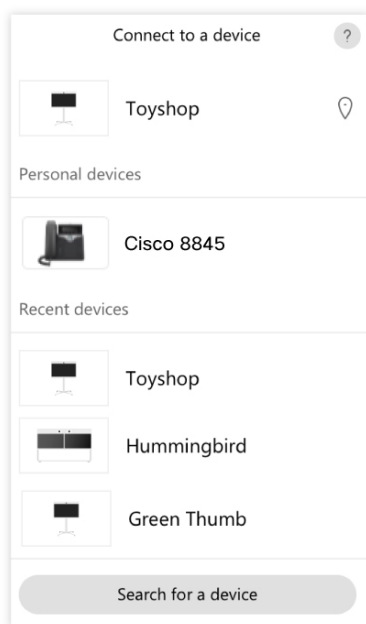
機能名	説明とマニュアル	デスクトップ	モバイル
SIP (URI) アドレスルーティング	Control Hub で設定可能です。この設定では、Webex クラウドを介してルーティングされる SIP アドレスを決定できます。デフォルトでは、Webex サービス以外のすべての SIP Uri が、ユニファイド CM を介してルーティングされます。「 組織の SIP アドレスルーティングを設定する 」を参照してください。	✓	
シングルサインオン (SSO)	IdP およびオンプレミス環境そして Webex クラウド間における SSO の統合により、ユーザは、1つのログイン情報のみでアプリケーション間にサインインできます。（「 環境の準備 」の章を参照してください）。	✓	✓
仮想カメラ (macOS)	Webex Control Hub を使用すると、Webex アプリでの通話や会議で仮想カメラを有効または無効にできます。ユーザーは、アプリケーション、ドライバ、ソフトウェアなどの仮想カメラを使用して、ビデオ、画像、またはフィードのオーバーレイを作成できます。	✓ (macOS のみ)	


デスクフォン制御 (DPC) に関する詳細

ユーザの Unified CM アカウントに関連付けられたデスクフォンまたはエクステンション モビリティプロファイルはすべて、Windows または Mac 用 Webex アプリで、接続可能なデバイスとしてリストされます。デバイスを選択すると、Webex アプリ からダイヤルまたは応答した Unified CM コールではそのデスクフォンが使用されます。ユーザは、コールを開始または停止したり、DTMF 入力(電話機が認識)を入力したり、前の機能テーブルに記載されている通話中の機能を使用したりすることができます。ユーザは、デスクフォン制御モードの Webex アプリ からミーティングに参加することもできます。



(注) Webex アプリは Extension Mobility をサポートしていません。



ユーザは、デスクトップアプリからデスクフォンの説明に直接アクセスし、その説明をカスタマイズできます。電話の説明の上にマウスカーソルを合わせたら、 をクリックして名前を変更できます。ユーザに複数のデスクフォンを割り当てた場合は、それぞれの説明をカスタマイズすると区別しやすくなります。

ユーザー向け Webex アプリ の通話エクスペリエンス

通話の比較

次の表に、Unified CM を経由する Webex アプリ コールのタイプと、Unified CM を経由しない（代わりにクラウドマイクロサービスへのコールとなる）Webex アプリ コールまたはミーティングのタイプを示します。

表 5: Unified CM 経由の通話の比較とクラウド経由の通話と会議

Unified CM 環境経由の通話	Webex クラウド経由の通話と会議
1 対 1 スペースまたは Webex アプリ のコンタクトカードから直接発信された通話	Webex アプリ のグループスペースからのアドホック会議
Webex アプリ でユーザーを検索して通話	Webex アプリ で [参加 (Join)] ボタンを使用して、アドホック会議またはスケジュールされた会議に参加

Unified CM 環境経由の通話	Webex クラウド経由の通話と会議
Webex アプリ の通話 ☎ からディレクトリ番号または PSTN 番号にダイヤル	Webex アプリ の通話 ☎ からプレミスディレクトリ URI にダイヤル (Control Hub の [Unified CM SIP アドレスルーティング (Unified CM SIP Address Routing)] 設定に依存します)。
デスクフォン制御 (DPC) 通話 (発信: Webex アプリ のディレクトリ番号または PSTN 番号に発信、Unified CM デバイスで通話に回答、着信: Webex アプリ で通話に回答、デバイスで通話に回答)。	<p>ルーム、デスク、またはボードデバイスを介してペア化された状態で会議に参加する</p> <p>コンシューマ組織内の無料ユーザー、別の組織内のユーザー、または同じ組織内でディレクトリ番号のないユーザーに対して Webex アプリ で直接発信される 1 対 1 通話。(番号は組織間で共有されないため、連絡先カードには表示されません) これは、Webex アプリ の通話として分類されます。</p>

ユーザー体験

クラウドに登録されたルーム、デスク、またはボードデバイスとペアリングされているユーザーの場合:

- Webex アプリ の Unified CM 登録はアクティブなままです。
- ユーザのディレクトリ番号への着信は Webex アプリ に表示されます。コールを受け入れた場合、応答はデスクトップアプリで行われ、ペアリングされたルーム、デスク、またはボードデバイスは使用されません。
- Webex デバイスがハイブリッドコールに対応するワークスペースとして Control Hub で設定されている場合、ユーザは Webex アプリ からダイヤルできます。ダイヤルすると、コールが Webex デバイスで開始され、そのデバイスのディレクトリ番号を受信側の発信者 ID として使用されます。ユーザは、ペアリングされたデバイスへの着信コールに回答することはできません。
- Webex デバイスがハイブリッド通話に対応するワークスペースにない場合、ディレクトリ番号や PSTN のダイヤリングは失敗し、ユーザーの Webex アプリ にエラーメッセージが表示されます。



Webex アプリ でデスクフォン制御モードになっているユーザの場合：

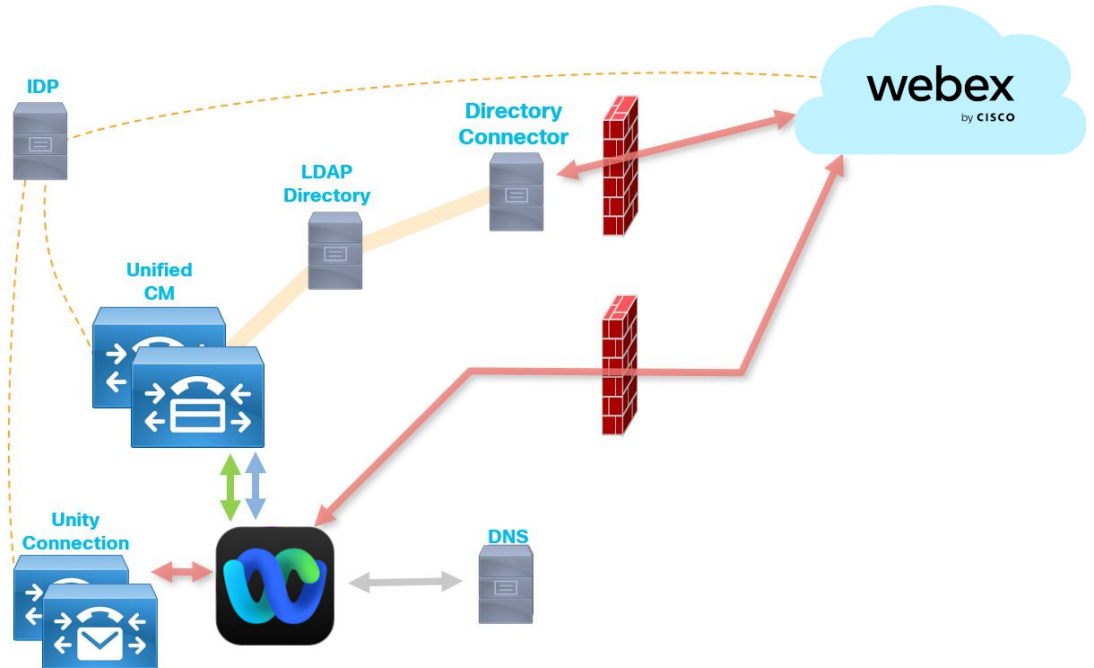
- 連絡先カードを持つユーザへの1:1 コールのメディア (音声およびビデオ) と、検索またはダイヤルビューから開始されたコールはオンプレミスのデスクフォンを経由します。
- グループスペースミーティング、Webex ミーティング (スケジュールまたはアドホック)、および連絡先カードのないユーザへのコールのメディア (オーディオとビデオ) は、オンプレミスのデスクフォンを経由します。

コールがボイスメールに送られるシナリオについては、次のようにします。

- ユニファイド CM を経由しない着信コールでは、ボイスメールにロールバックされず、ユーザが応答または拒否するまで呼出音が鳴ります。
- Unified CM を通過する着信コール (ユーザの社内ディレクトリ番号への着信など) は、ボイスメールにロールオーバーします。

アーキテクチャ


ネットワーク内



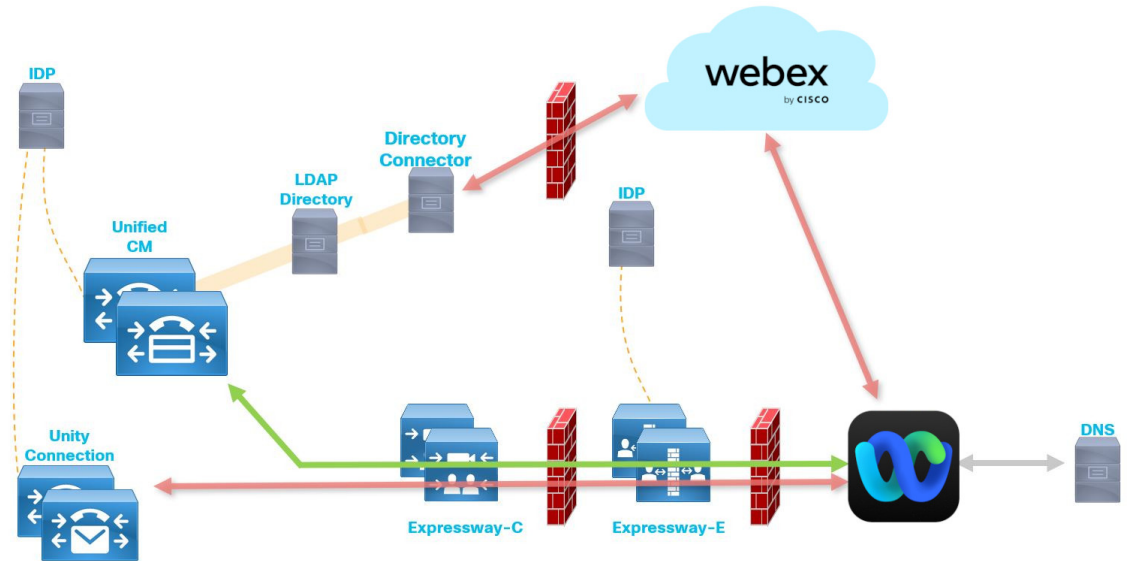
このアーキテクチャ図は、企業のネットワーク内の Unified CM コール環境に統合された Webex を示しています。

表 6: 凡例

アイコン	プロトコル	用途
	HTTPS	Webex クラウドサービス、ビジュアルボイスメール
	SIP	ソフトフォンモード
	CTI/QBE	デスクフォンの制御
	LDAP	ディレクトリ
	DNS	サービス検出






アイコン	プロトコル	用途
	SP 契約	シングルサインオン (SSO) 契約

リモート



このアーキテクチャ図は、Unified CM 発信環境に統合された Webex を表しています。この環境には、リモートユーザ用のモバイルおよびリモートアクセス (MRA) 用に展開された Expressway ペアも含まれています。

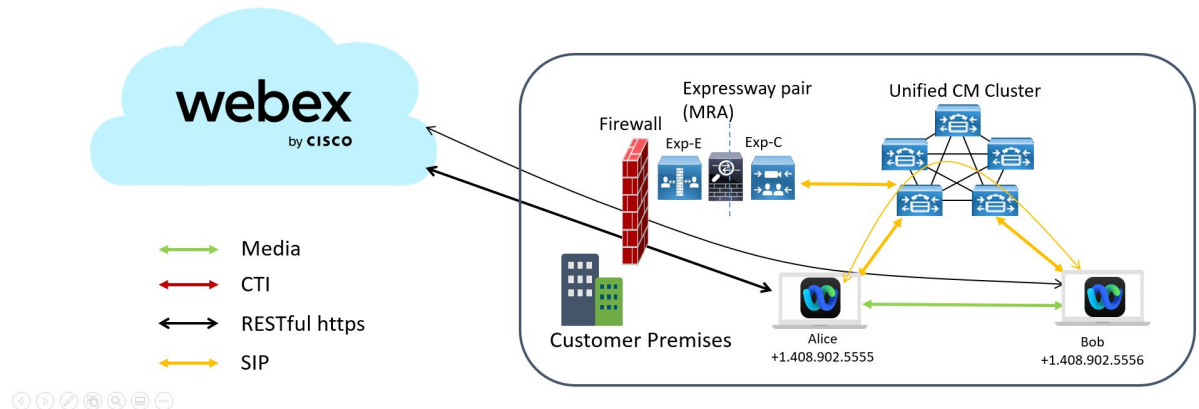
表 7: 凡例

アイコン	プロトコル	用途
	HTTPS	Webex クラウドサービス、ビジュアルボイスメール
	SIP	ソフトフォンモード
	LDAP	ディレクトリ
	DNS	サービス検出
	SP 契約	シングルサインオン (SSO) 契約

Webex アプリでのコール (Unified CM) の通話フロー

Webex アプリでの Unified CM 通話応答

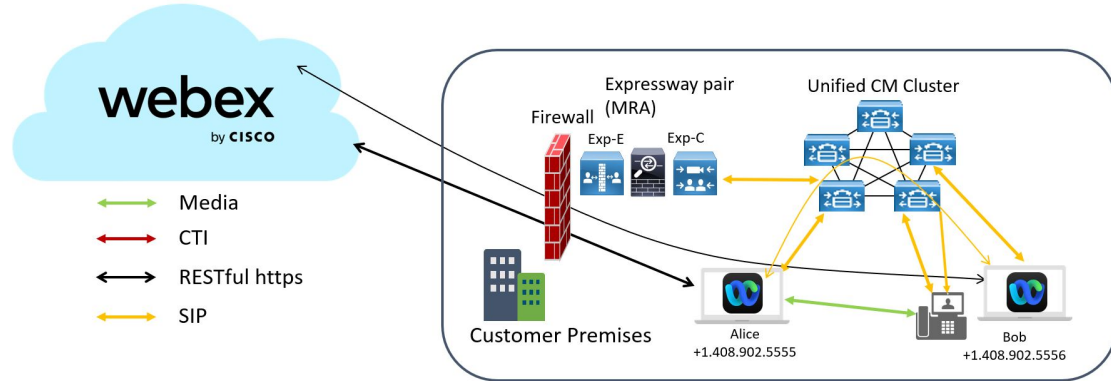
図 1: Unified CM における 2 名のユーザー間の通話、Webex アプリ で応答された通話



1. Webex アプリを使用して、Aliceが 1:1 スペースで連絡先カードから Bob のディレクトリ番号をコールします。
2. Bob の Webex アプリ で電話が鳴りました。
3. Bob は、Webex アプリ で通話に応答しました。呼び出しシグナリングは、Unified CM を介して確立される。
4. 両方のパーティがビデオをオンにしてコンテンツを共有することができる。(カメラが存在する場合、デフォルトでビデオがオンになっています)。

デスクフォンで Unified CM 着信通話に应答する

図 2: Unified CM の 2 名のユーザー間の通話、デスクフォンで通話に应答

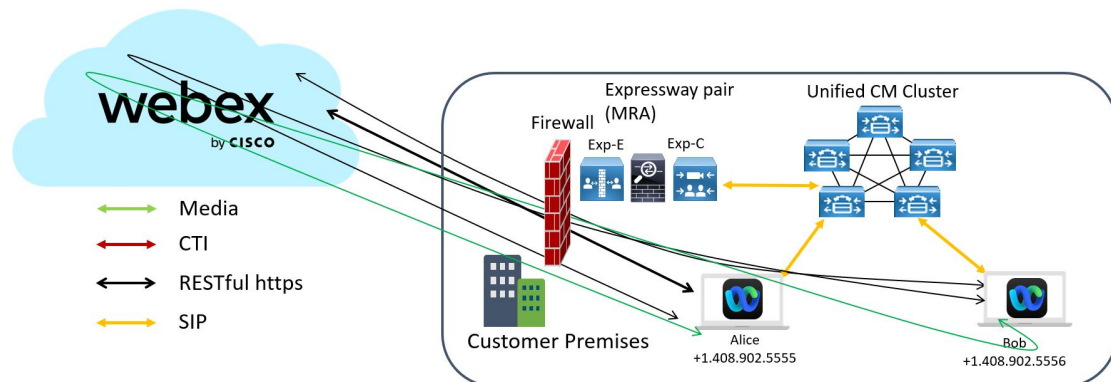


① ② ③ ④ ⑤ ⑥

1. Alice の Webex アプリ から、Alice は、Webex アプリ 1 対 1 スペースで Bob のディレクトリ番号に発信しました。(Bob のディレクトリ番号は、アプリの連絡先カードで入手できる)。
2. 呼び出しシグナリングは、Unified CM を介して確立される。Bob のデスクフォンと彼の Webex アプリ の両方で呼び出し音が鳴ります。
3. Bob は自分のデスクフォンで应答します。メディアは、Alice の Webex アプリ と Bob のデスクフォンの間で直接伝送されます。
4. 両方のパーティがビデオをオンにしてコンテンツを共有することができます。(Webex アプリデスクトップデバイスにカメラが存在すれば、ビデオがデフォルトでオンになります。)

Webex アプリでディレクトリ番号のないユーザーに発信

図 3: Unified CM のユーザーとディレクトリ番号のないユーザー間の通話、Webex アプリで通話应答

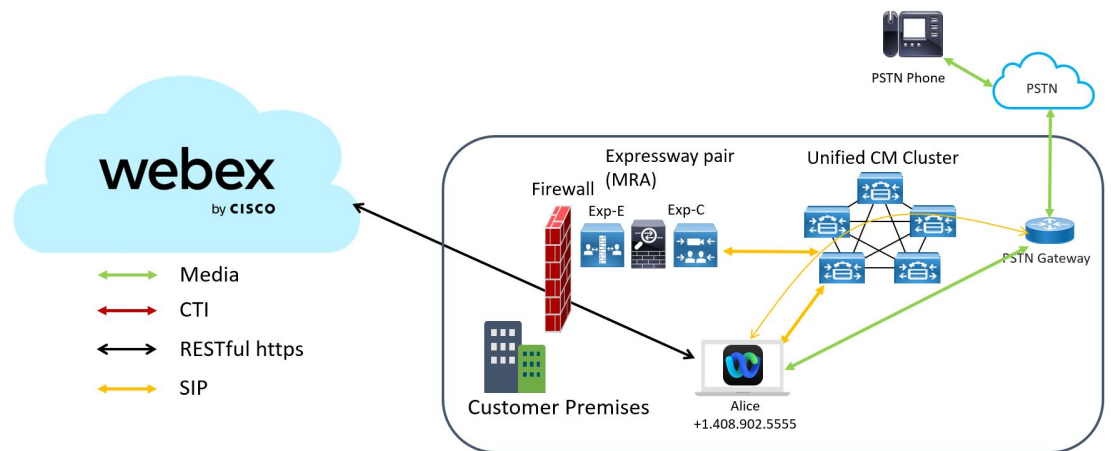


① ② ③ ④ ⑤ ⑥

1. Webex アプリを使用して、Alice は 1 対 1 スペースで Bob の Webex アプリ に発信しました。(Bob の電話番号は、アプリの連絡先カードでは使用できません)。
2. Bob が Webex アプリ でコールに応答します。
3. 通話は、2 名の Webex アプリ ユーザー間で Webex アプリ での通話として確立されます。メディアは、2 つの Webex アプリ インスタンス間でクラウドを介して、または展開されている場合はオンプレミスのビデオメッシュノードを介して伝送されます。

Webex アプリから PSTN 番号への Unified CM 通話

図 4: Unified CM のユーザーから PSTN 番号に発信

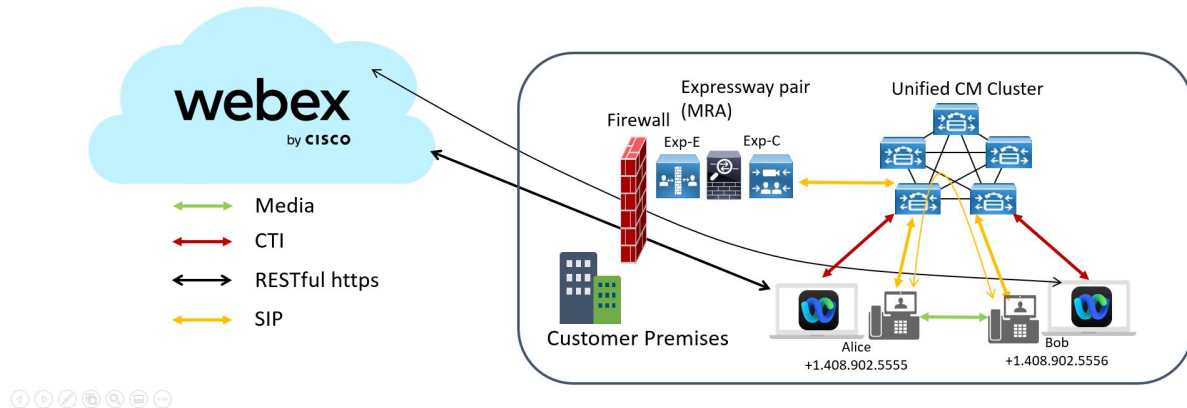


④ ③ ② ①

1. Alice が Webex アプリ から [コール (Call)] タブを使用して、PSTN 番号にコールします。
2. Unified CM を介して PSTN ゲートウェイへのコールシグナリングが確立されます。
3. Webex アプリ と PSTN ゲートウェイ間でメディアが直接伝送されます。

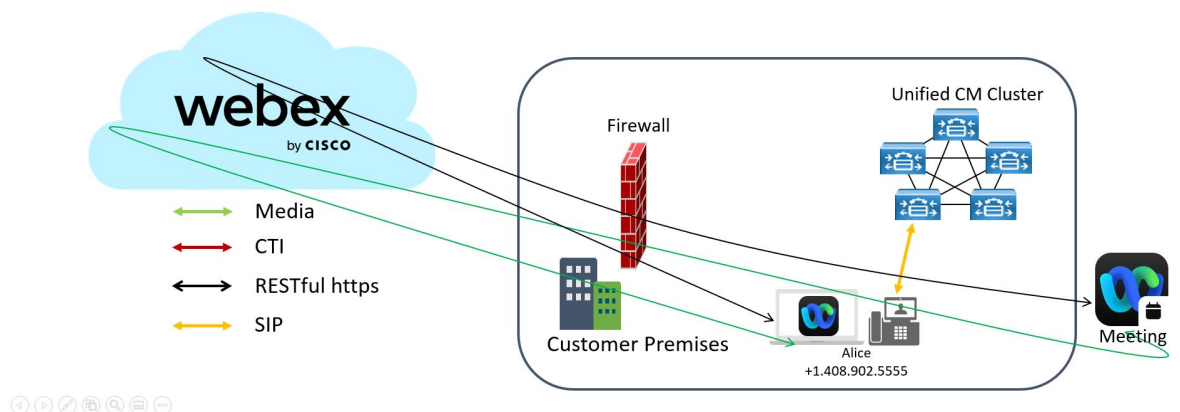
デスクフォン制御モードでの Unified CM 通話

図 5: Unified CM での 2 人のユーザー間の通話。通話は、デスクフォン制御モードで、Webex アプリで応答されます。



1. Webex アプリを使用して、Alice (デスクフォン制御モード) が Webex アプリ 1:1 スペースから Bob のディレクトリ番号をコールします。(Bob の電話番号は、アプリの連絡先カードで使用できます)。
2. コールはデスクの電話機を通過します。コールシグナリングは、ユニファイド CM を介して確立されます。
3. Bob のデスクフォンが鳴り、Webex アプリで通知を受け取ります。
4. Bob は、デスクフォン制御モードで Webex アプリのコールに応答します。メディアは、2 つのデスクフォン間で直接流れます。

デスクフォン制御モードで会議に参加



1. Webex アプリを使用して、Alice は (デスクフォン制御モードで) 会議に参加しました。(会議は、Webex アプリのみで、スペースから直接行う必要があります。会議のフル機能はサポートされていません)。

2. デスクフォン制御モードでは、メディアはユニファイドCMの電話機とクラウド上の会議間で確立されます。クラウド上またはビデオメッシュノードを介して2つの間のメディアフロー (展開されている場合)。



第 2 章

Webex アプリでのコール（Unified CM）用 環境の準備

- 呼制御環境の要件（57 ページ）
- Unified CM 機能要件（60 ページ）
- Contact Center 機能要件（71 ページ）
- ネットワークの要件（71 ページ）
- 証明書の要件（74 ページ）
- ヘッドセットの要件（78 ページ）
- ライセンス要件（78 ページ）
- Webex アプリ 要件（79 ページ）
- 推奨構成（79 ページ）

呼制御環境の要件

Webex アプリでコールイン（Unified CM）を有効にするには、サポートされているいずれかの Unified CM ベースの Cisco Call Control ソリューションを使用する必要があります。このとき、サポートされている最小バージョン以降であることを確認してください。

表 8: サポートされる Unified CM リリース

通話ソリューション	バージョン
Cisco Unified Communications Manager*	最小
	デスクトップおよびモバイル (Android) <ul style="list-style-type: none"> • デスクトップ向け Unified CM Release 11.5 (1) SU3 以降。 • 必須ではありませんが、この最小リリースは Android で Firebase Cloud Messaging (FCM) プッシュ構成をサポートしています。
	デスクトップおよびモバイル (iOS) <ul style="list-style-type: none"> • 11.5 リリースの場合、iOS モバイルデバイスの Apple プッシュ構成 (APN) サービスには、Unified CM Release 11.5(1) SU8 またはそれ以降の SU が必要です。 (このリリースは中国ではサポートされません。次を参照してください)。 • 12.5 リリースの場合、iOS APN には、Unified CM Release 12.5(1) SU3 またはそれ以降の SU が必要です。
安全な通話 (SIP Oauth) <ul style="list-style-type: none"> • Unified CM Release 12.5(1) 以降 <p>(注) CAPF はサポートされていません。</p>	
	推奨

通話ソリューション	バージョン
	<p>デスクトップおよびモバイル</p> <ul style="list-style-type: none"> Unified CM Release 12.5 (1) SU3 以降。 ** この推奨リリースにより、プッシュ構成が環境内のすべてのモバイルプラットフォームで動作し、安全な通話がサポートされるようになります。 <p>詳細については、「プッシュ構成 (66 ページ)」を参照してください。</p> <p>(注) 組織が中国拠点の場合、少なくともこのバージョンを使用する必要があります。</p> <ul style="list-style-type: none"> モバイルおよびリモートアクセス (MRA) を使用して、MRA フェールオーバーを構成する場合、Unified CM Release 14.0 以降が必要です。 <p>SSO リダイレクト URI</p> <p>この機能拡張には、特定の Unified CM と Expressway の要件があります。詳細については、「推奨される構成」の「SSO リダイレクト URI」セクションを参照してください。</p>
Cisco Business Edition	ソリューションでサポートされているバージョンのユニファイド CM が実行されていることを確認するには、 BE6K および BE7K のソフトウェアロードサマリーのドキュメンテーションを確認してください。
Cisco Hosted Collaboration Solution	<p>最低でも 11.5 以降。</p> <p>SIP Oath 暗号化コールのサポートには、12.5 以降をお勧めします。(CAPF はサポートされていません。)</p>
Cisco Unified Communications Manager Cloud	—

* Webex アプリでボイスメールを統合するには、Cisco Unity Connection のバージョンと Unified CM のバージョンを一致させることを推奨します。ただし、両方のサーバで認証方式とログイン情報が同じであることを確認してください。

** Apple による iOS 通知アーキテクチャの変更に合わせて、Cisco Webex アプリには Apple プッシュ通知のサポートが実装されています。できるだけ早い時期に Cisco Unified Communications Manager、Cisco Expressway、および Cisco Webex アプリをアップグレードすることを強く推奨します。アップグレードを適時に行わないと、Cisco Webex アプリ iOS ユーザ用の Unified Communications Manager および IM の通知を使用する Cisco Webex アプリ ユーザで、音声通知が利用できなくなります。アップグレード要件など、iOS 13 でのプッシュ通知に関する最新のサポート情報については、『[Apple プッシュ通知サービスの更新](#)』を参照してください。

必須ではありませんが、モバイルおよびリモートアクセス (MRA) のサポートが必要な場合は (企業ネットワーク外で Webex アプリをソフトフォンモードで使用できるようになりま

す)、Cisco Expressway トラバーサルペアを使用する必要があります。このとき、サポートされている最小バージョン以降であることを確認してください。

表 9: サポートされる Expressway リリース

通話ソリューション	バージョン
Mobile & Remote Access (MRA) の Cisco Expressway E および C トラバーサルペア	<p>Webex アプリでコールイン (Unified CM) には、X8.11.4 以降が必要です。詳細については、『製品のリリースノート』の「重要な情報」セクションを参照してください。このリリース以降では、セキュリティが強化されています。</p> <p>プッシュ通知には X12.6 以降が必要です。</p> <p>モバイルおよびリモートアクセス (MRA) を使用して MRA フェールオーバーを構成する場合は、Expressway Release X14.0 以降が必要です。</p> <p>詳細については、『Cisco Expressway 経由の D モバイルおよびリモートアクセス導入ガイド』を参照してください。</p>

Unified CM 機能要件

多くの Unified CM 機能は、環境の設定後に自動的に Webex アプリで利用可能になります。ただし、一部の機能については、Webex アプリで動作させるために Unified CM での事前設定が必要です。

接続時のトーンによる自動応答

ユーザに割り当てられた電話番号に自動応答を設定できます。自動応用設定に関する詳細は、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> のリリース向け『Cisco Unified Communications Manager システム設定ガイド』および Cisco Unified CM Administration オンラインヘルプを参照してください。

コールが接続される前に Webex 上のエージェントにトーンが聞こえる場合は、Cisco CallManager サービスパラメータの接続時のトーンを [True] に設定します。このパラメータは、メディアストリーミングの開始を示すトーンを再生するかどうかを決定します。このパラメータの有効な値は [True] です。トーンを再生する場合は [True] を、トーンを再生しない場合は、[False] を設定します。デフォルト値は、[False] です。このグローバルパラメータは、クラスタ内のすべてのユーザに影響します。

通話パーク

コールパーク機能を使用すると、別のオフィスの電話機や Webex アプリ内の電話機など Unified Communications Manager システムの別の電話機またはソフトクライアントから取得できるよ

う、コールを保留にできます。通話中の場合は、Webex で [パーク (Park)] をクリックすると、その通話をコールパーク内線番号にパークできます。次に、システム内の別の電話機やソフトウェアクライアントからコールパーク内線番号にダイヤルして、その通話を受けることができます。

コールパーク構成の詳細に関しては、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> のリリースの『Cisco Unified Communications Manager の機能設定ガイド』に記載されている「「コールパークとダイレクトコールパーク」」を参照してください。

コール録音

通話録音を使用すると、録音サーバでエージェントの会話をアーカイブできます。Webex アプリは、Unified CM ベースの展開でこの機能をサポートします。

Unified CM の一部のリリースでは、デバイスパッケージで録音機能を有効にする必要があります。これを確認するには、デバイスの [電話の設定 (Phone Configuration)] ページに [ビルトインブリッジ (Built In Bridge)] フィールドがあるかどうかを調べます。このフィールドが使用できない場合は、最新のデバイスパッケージをダウンロードして適用してください。

コール録音の設定方法の詳細については、『Cisco Unified Communications Manager 機能設定ガイド』の「録音」の章を参照してください。

Jabber Config XML ファイルまたはクライアント設定サービスで構成できる構成パラメータについては、このガイドの付録にある機能パラメータの表を参照してください。

ダイヤルプランのマッピング

Cisco Unified Communications Manager のダイヤルルールがディレクトリのダイヤルルールと確実に一致するように、ダイヤルプランのマッピングを設定します。

アプリケーションダイヤルルール (Application Dial Rules)

アプリケーションダイヤルルールにより、ユーザがダイヤルする電話番号の桁数の追加および削除が自動的に行われます。アプリケーションダイヤルルールは、ユーザがクライアントからダイヤルする番号を操作します。

たとえば、7桁の電話番号の先頭に自動的に9を追加して外線にアクセスするように、ダイヤルルールを設定できます。

ディレクトリ検索ダイヤルルール (Directory Lookup Dial Rules)

ディレクトリ検索ダイヤルルールは、発信者 ID の番号を、クライアントがディレクトリで検索できる番号に変換します。定義する各ディレクトリ検索ルールには、先頭の数字および番号の長さに基づいてどの数字を変換するかを指定します。

たとえば、10桁の電話番号から市外局番と2桁の局番を自動的に削除するディレクトリ検索ルールを作成できます。このタイプのルールでは、たとえば、4089023139を23139に変換します。

Dial Via Office Reverse

Dial Via Office (DvO) 機能を使用すると、ユーザはデバイスのモバイルボイスネットワークを使用して、勤務先電話番号で Webex アプリ 発信コールを開始できます。

Webex アプリ は DvO-R (DvO-リバース) コールをサポートしています。これは次のように動作します。

1. ユーザが DvO-R コールを開始します。
2. クライアントは、Cisco Unified Communications Manager に携帯電話番号にコールするよう通知します。
3. Cisco Unified Communications Manager は携帯電話番号にコールして接続します。
4. Cisco Unified Communications Manager は、ユーザがダイヤルした番号にコールして接続します。
5. Cisco Unified Communications Manager が 2 つのセグメントを接続します。
6. ユーザおよび着信者は、通常のコールと同様に続けます。



(注) 次の状況では、ユーザは Webex アプリ で着信コールを受信しません。

- ユーザが任意のネットワークで [モバイルボイスネットワーク (Mobile Voice Network)] コールオプションを選択した場合、デバイスでシングルナンバーリーチ (SNR) が設定されていないと、ユーザは Webex アプリ で着信コールを受信しません。
- ユーザが任意のネットワークで [モバイルボイスネットワーク (Mobile Voice Network)] コールオプションを選択し、シングルナンバーリーチ (SNR) の設定で [呼び出しスケジュール (Ring Schedule)] が使用されている場合、[呼び出しスケジュール (Ring Schedule)] で設定された時刻を過ぎると、ユーザは Webex アプリ で着信コールを受信しません。

次の表は、着信コールと発信コールに使用されるコールメソッドを示しています。コールメソッド (VoIP、DvO-R、セルラーコール) は、選択されたコールオプションとネットワーク接続によって異なります。

表 10: ネットワーク接続のタイプとコールオプションに応じて使用されるコールメソッド

接続	コールオプション					
	Voice over IP		モバイルボイスネットワーク		自動選択	
Wi-Fi	発信 : VoIP	着信 : VoIP	発信 : DvO-R	着信 : VoIP	発信 : VoIP	着信 : VoIP
モバイルネットワーク (3G、4G、5G)					発信 : DvO-R	着信 : VoIP

DvO-Rを設定するには、「[モバイルおよびリモートアクセスで使用できるようオフィスリバー](#)スを介してダイヤルを設定する」の手順に従ってください。

Extend and Connect

Extend and Connect 機能により、管理者は、あらゆるエンドポイントと相互運用する Unified Communications Manager (UC) コンピュータテレフォニーインテグレーション (CTI) アプリケーションを展開できます。Extend and Connect により、ユーザは、ロケーションを問わずどのデバイスからでも UC アプリケーションにアクセスできます。



- (注) ユーザが番号を追加および編集できるのは、既存のデバイスについてだけです。ユーザ用に少なくとも1つのデバイスを設定する必要があります。デバイスが存在しない場合は、この機能が有効になっていても、Webex アプリにはオプションとして表示されません。

詳細については、「[Extend and Connect の設定](#)」を参照してください。

通話をモバイルに移動

ユーザーは、アクティブな VoIP 通話を Webex アプリ から、モバイルネットワークの自信の携帯電話番号に転送できます。この機能は、通話中のユーザーが、Wi-Fi ネットワークから離れる際や（たとえば、建物から出て、車に乗るなど）、Wi-Fi ネットワークを経由すると音声品質に問題がある場合に便利です。

始める前に

[ユーザーのモバイル ID を設定します。](#)

ステップ 1 Cisco Unified CM Administration で、[\[デバイス \(Devices\)\]](#) > [\[電話機 \(Phone\)\]](#) の順に選択し、ユーザーの Webex アプリ for mobile (TCT または BOT) デバイスを検索します。

ステップ 2 [\[モビリティユーザー ID \(Mobility User ID\)\]](#) の場合、ユーザーの ID（通常は、所有者ユーザー ID と同じ）を選択します。

ステップ 3 構成した [関連モバイル ID](#) を選択します。

ステップ 4 [\[モバイルネットワークに転送 \(Transfer to Mobile Network\)\]](#) の場合、[\[モビリティソフトキーを使用 \(ユーザーが通話を受信\) \(Use Mobility Softkey \(user receives call\)\)\]](#) を選択します。

この設定が構成されていると、Unified CM は、モバイルデバイス用の PSTN モバイル サービス プロバイダーの電話番号に発信します。

ステップ 5 変更を保存したら、[\[ユーザー管理 \(User Management\)\]](#) > [\[エンドユーザー \(End User\)\]](#) の順に選択し、この機能を追加する任意のユーザーアカウントを見つけます。

ステップ 6 次の設定を確認します。

- [\[モビリティの有効化 \(Enable Mobility\)\]](#)

• モバイル音声アクセスの有効化

ステップ7 変更を保存します。

次のタスク

ユーザーはセルフケアポータルで接続先を変更できます。

1. Webex アプリ 設定で、[Calling] > [通話の詳細設定 (Advanced Call Settings)] の順に選択します。
2. セルフケアポータルで、モバイルデバイスを選択します。
3. [シングルナンバーリーチの編集 (Edit Single Number Reach)] をクリックし、[電話番号または URI (Phone Number or URI)] のエントリを変更したら、[保存 (Save)] をクリックします。

マルチライン

ユーザが日常的な Webex アプリ タスクを実行できるように、複数の電話回線を設定できます。ユーザごとに最大 8 本の電話回線を追加できます。デスクトップクライアント向けに、Cisco Services Framework (CSF) デバイスのユーザにマルチラインを設定できます。

マルチラインは、Cisco Unified Communications Manager リリース 11.5 SU3 以降でサポートされています。ただし、Cisco Unified Communications Manager リリース 11.5 SU3 または Cisco Unified Communications Manager リリース 12.0 を使用している場合は、すべてのクラスタノードに [Cisco Options Package \(COP\)](#) ファイルを手動でインストールし、Cisco Unified Communications Manager を再起動して、マルチラインを有効にする必要があります。

マルチラインを設定するには、[デバイスにディレクトリ番号を追加する \(103 ページ\)](#) の手順を使用してデバイスに複数回線を追加し、そのデバイスをユーザに関連付けます。



- (注) マルチラインは、デスクトップ用の Webex アプリ をモバイルおよびリモートアクセス (MRA) モードで使用する場合にもサポートされます。この機能は、トラバーサルペアの Expressway-C で有効にできます (Unified Communication > [設定 (Configuration)] > [SIPパスのヘッダー (SIP Path headers)] を [オン (On)] に設定します)。

共有回線のシナリオでプレゼンスを変更する場合は、RemoteInUsePresencePrimaryLineOnly パラメータを設定することもできます。詳細については、「[ポリシーパラメータ \(135 ページ\)](#)」を参照してください。



- (注) このパラメータは、Unified CM で選択可能なプリセットではありません。ポリシーにカスタムパラメータとして追加する必要があります。

マルチラインのインストールと設定が完了すると、ユーザは次の操作を行えるようになります。

- 発信に使用する優先回線を選択する。
- 不在着信とボイスメールを確認する。
- すべての回線で通話転送、転送、会議コールを使用する。
- 各回線にカスタム着信音を割り当てる。

マルチラインでは、すべての回線で次の機能がサポートされます。

- デスクフォン用 CTI 制御
- ハントグループ
- 共有回線、ダイヤルルール、ディレクタリックアップ
- アクセサリマネージャ

マルチラインが有効になっている場合、次の機能はプライマリラインでのみ使用できます。

- コールピックアップ
- Extend and Connect

マルチコールウィンドウ

複数通話ウィンドウとは、Webex アプリユーザが複数回線または共有回線を管理するために役立つ個別のフローティングウィンドウです。複数回線または共有回線で通話を発信および受信するだけでなく、ユーザはすべての回線のステータスを確認でき、別のウィンドウに移動することなく、保留、転送、割り込みなどの機能に簡単にアクセスできます。

ユーザが複数通話ウィンドウを最大限に活用できるように、Unified CM で次の機能を構成します。

- マルチライン
- ボイスメール
- 割り込み
- プライバシー
- メッセージ待機インジケータ (MWI)

これらの項目を読む：

- [Webex アプリ \(Unified CM\) での通話のマルチ通話ウィンドウを設定する](#)
- [Webex アプリ | すべての通話を 1 か所で管理する](#)

プッシュ構成

クラスターでプッシュ構成が有効になっている場合、Cisco Unified Communications Manager は Apple クラウドまたは Google クラウドのプッシュ構成サービスを使用してプッシュ構成を、iOS デバイス (APN; Apple プッシュ構成) または Android (FCM; Firebase Cloud Messaging) デバイスで実行されている互換性のある Webex クライアントに送信します。プッシュ構成を使用すると、システムがバックグラウンドモード (サスペンドモードとも呼ばれる) に入った後も、クライアントと通信できます。プッシュ構成がない場合、バックグラウンドモードに入ったクライアントにコールやメッセージを送信できない場合があります。

Apple と Android のプッシュ構成 (APN) の構成方法に関する詳細は、『プッシュ構成に関する導入ガイド』に記載されている「[プッシュ構成 \(オンプレミス展開\)](#)」を参照してください。

緊急通報の位置情報報告

Ray Baum の法律に準拠するために、米国ではユーザーがオフィス外にいるときに正確な位置情報の提供を要求できます。

ユーザーが新しい場所に居ると Webex アプリ が判断した場合、ユーザーは、住所を更新するように求められます。ユーザーが Webex アプリ から緊急通話を発信した場合、正確な位置情報が National E911 Service Provider を経由して、緊急通話に応答する地域の緊急コールセンターである Public-Safety Answering Point (PSAP) に自動送信されます。このような方法で、ダイヤル元のデバイスや大きな建物内の正確な位置に関係なく、最初の応答者は、「派遣可能な場所」をピンポイントで特定するために必要な情報を入手し、緊急発信者の下に迅速に向かうことができます。



(注) この機能は、Windows、Mac、Linux、VDI、iPad、Android タブレット、Chromebook に限定されています。

セル方式のモバイルソフトフォンデバイスの場合、Webex アプリ は、組み込みの電話アプリをクロス起動して緊急通報を行います。

MacOS Monterey ユーザーは、Webex が BSSID を Redsky に報告できるように、ネットワークへのアクセスを Webex アプリ に許可する必要があります。BSSID を自動報告できない場合、各ユーザーは、Webex アプリ に手動で現在地を追加する必要があります。

お使いの環境が Unified CM 12.5 以前を使用している場合、サポートされているサーバーバージョンにアップグレードする必要があります。

カスタマー タイプ	必要なコンポーネントとサポートされているバージョン
Unified CM オンプレミス	Unified CM 12.5SU6 Cisco Emergency Responder 12.5SU6 Cisco Expressway X14.1

カスタマー タイプ	必要なコンポーネントとサポートされているバージョン
Unified CM Cloud	Unified CM 12.5SU5a Cisco Emergency Responder 12.5SU5a Cisco Expressway X14.0.4

RedSky 関連の構成は、UDS インターフェイスによって強化された Unified CM サービスプロファイルを経由します。

- <EnableEmergencyCalling>(Yes/No)
- <OrganizationId>
- <Secret>
- <LocationUrl>
- <EmergencyNumbers>

[Enable National Emergency Calling](#)
[Organization ID](#)
[Secret](#)
[Location Url](#)
[Emergency Numbers](#)

Unified CM 14 以降を使用している場合、ユーザーは Redsky MyE911 アプリをインストールし、そこから現在地を報告する必要があります。CER を使用してオンプレミスのワイヤレスロケーションを報告している場合は、CER を保持し、RedSky ソリューションを使用してオフプレミスのロケーションのみを追跡できます。



(注) Webex アプリ for Linux は CER をサポートしていません。緊急通報のためにオンプレミスとオフプレミスの両方の場所を報告するには、RedSky を展開する必要があります。

モバイルソフトフォンデバイス (TCT/BOT) の場合、Unified CM サーバーで緊急番号 (911 など) をプロビジョニングして、Webex アプリ が組み込み電話アプリを起動して緊急通話を発信できるようにします。「展開」章の「Webex ソフトフォンデバイスの作成と構成」を参照してください。

その他資料

National E911 Service Provider で Emergency Responder を構成

Cisco Emergency Responder は、RedSky や Intrado などの National E911 Service Provider と統合して、現在地の自動アップデート、ユーザー入力ロケーションの MSAG (Master Street Address Guide) および Call Completion が可能です。Emergency Responder は、企業内を移動するすべてのデバイスの派遣可能な場所を自動的に見つけて追跡するため、E911 規制に準拠できます。

https://www.cisco.com/c/dam/td-xml/en_us/voice-ip-comm/ucm_cloud/WebexCallingDI_Islands/National_E911_for_DedicatedInstance.pdf

Nomadic E911 サポート向け Unified Communications Manager の構成

Nomadic E911 を使用すると、ユーザーが Webex アプリで現在地をネイティブに更新できるようにすることで、管理者は、Ray Baum の法律要件に対処できます。

https://www.cisco.com/c/dam/td-xml/en_us/voice-ip-comm/ucm_cloud/WebexCallingDI_Islands/National_E911_WebexApp_AdminGuide.pdf

Survivable Remote Site Telephony (SRST)

Cisco Unified Survivable Remote Site Telephony (SRST) は、Unified CM に Webex アプリ ユーザーのフォールバックサポートを提供します。Cisco Unified SRST を使用すると、リモートのプライマリ、セカンダリ、または複数の Cisco Unified CM のインストレーションへの接続が失われた場合、または WAN 接続がダウンした場合は、ルータが、Webex アプリ ユーザーの発信処理サポートを提供します。

本機能に関する詳細は、UC Manager リリース向けの『システム設定ガイド』に記載されている「SRST 構成」か、IOS 構成、機能サポートおよび制限事項に関する『Cisco Unified SCCP および SIP SRST 向けシステムアドミニストレーションガイド (全バージョン)』を参照してください。

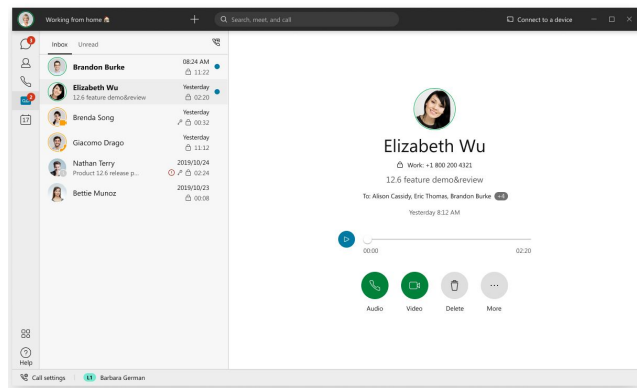
ボイスメール

Webex アプリ でボイスメールを機能させるには、Cisco Unity Connection と Unified CM で使用されている認証方式 (レガシー SSO、oAuth SSO、非 SSO など) が一致することを確認する必要があります。ユニファイド CM を統合すると、Cisco Unity Connection (ボイスメールおよびメッセージングシステム) は、AXL サービスまたは LDAP 統合を使用して手動で設定するユーザーにボイスメッセージ機能を提供します。メールボックスにボイスメッセージを受信すると、ユーザーの電話機および統合されたアプリケーション (この場合は Webex アプリ) でメッセージ受信ライトが点灯します。



(注) サーバのパフォーマンスを考慮する場合、Jabber と Webex アプリ と同時にビジュアルボイスメールを使用しないでください。

Webex アプリ では、ユーザーにビジュアルボイスメール受信ボックスが提供されます。これらのメンバーは、メッセージの再生、削除、既読マーク付け、および音声やビデオコールによる応答を行うことができます。



また、[コールボイスメール (Call Voicemail)] をクリックすると、内部または外部のコールでボイスメールシステムにアクセスできます。これにより、ユーザはメッセージの取得、聞き取り、返信、転送、および削除ができるようになります。ユーザ向けの本機能に関する詳細は、「Webex アプリボイスメール」ドキュメントを参照してください。



- (注) ボイスメールは常にユニファイド CM エンドユーザの資格情報を使用します。これらの資格情報と、Unity Connection でのボイスメールの資格情報は、一貫して、シングルサインオン (SSO) または非 SSO の資格情報のいずれかを設定することによって、ログインのエクスペリエンスを同じにする必要があります。詳細については、[推奨構成 \(79 ページ\)](#) を参照してください。

Cisco Unity Connection の設定とユニファイド CM 環境との統合の詳細については、次のドキュメントを参照してください。

- 『Cisco Unity Connection 版 Cisco Unified Communications Manager SIP 統合ガイド』のリリース：<https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html>
- 『Cisco Unity Connection 版システムアドミニストレーションガイド』にある「Cisco Unity Connection の電話機システム統合管理」のリリース：<https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html>

Wi-Fi から LTE 通話ネットワークのハンドオフ

Wi-Fi から LTE 通話ハンドオフを使用すると、Webex アプリでのコール (Unified CM) ユーザーは、ネットワーク切り替え時にアクティブな通話を切断することなく、Wi-Fi ネットワークと LTE ネットワークを切り替えることができます。

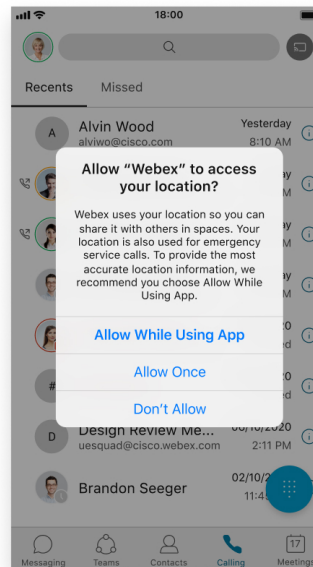
この機能は、デスクトップユーザーとモバイルユーザーに対して自動的に有効になります。通話環境は、Unified CM 14 以降である必要があります。詳細については、「[Unified CM リリースノート](#)」を参照してください。

この機能の既知の問題と制限については、「展開」章の「既知の問題」を参照してください。

ワイヤレス ロケーション モニタリング サービス

Webex アプリは、ワイヤレスアクセスポイント (AP) のロケーションモニタリングに対応しています。ワイヤレス ロケーション モニタリング サービスを使用すると、Webex アプリ ユーザが企業のネットワークに接続する物理的なロケーションを判断します。この情報は、Cisco Unified Communications Manager に格納されます。

この機能は、オンプレミスとモバイルおよびリモートアクセス (MRA) エッジワイヤレス接続でサポートされています。



Webex アプリは、ユーザの位置情報をモニタリングし、サービスセット ID (SSID) と基本サービスセット ID (BSSID) の情報を収集して、この情報を少なくとも 24 時間ごと (デスクトップのみ) にまたは次の時間ごとに、Unified CM に送信します。

- その現在のアクセスポイントは変更されます。
- Webex アプリにサインインします。
- これらは、オンプレミスのネットワークと、MRA 用の Expressway のネットワークを切り替えます。
- Webex アプリがスリープから再開するか、アクティブになります。



(注) モバイル用の Webex アプリが一時停止された場合は、24 時間おきにロケーションを送信できない場合があります。

- オンプレミスの展開の場合は、値が [True] の EnableE911OnPremLocationPolicy パラメータを使用して、ワイヤレス ロケーション モニタリングを構成します。

- **MRA 導入向けの Expressway の場合は**、値が [True] の `EnableE911EdgeLocationPolicy` およびセミコロンで区切られた最大 30 SSID のリストがある `E911EdgeLocationWhiteList` を使用して、ワイヤレス ロケーション モニタリングを構成できます。

これらのパラメータの詳細については、このガイドの付録を参照してください。

Cisco Emergency Responder (CER) の構成方法に関する詳細は、<https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html> のリリースの『*Cisco Emergency Responder* アドミニストレーションガイド』を参照してください。

Contact Center 機能要件

Webex アプリを、Cisco Contact Center ソリューション (Unified Contact Center Enterprise または Express) に統合し、ソフトフォンクライアントとして Finesse デスクトップで制御できるようにします。この統合では、マルチライン、録音、会議などのコンタクトセンター機能がサポートされます。

Webex アプリでサポートされている最新機能を確認するには、「[Webex アプリ向け Contact Center 統合](#)」を参照してください。

Cisco Contact Center ソリューションの構成方法については、該当する製品とリリースに対応する「[機能ガイド資料](#)」を参照してください。

- [Cisco Unified Contact Center Enterprise \(UCCE\)](#)
- [Cisco Unified Contact Center Express \(UCCX\)](#)

ネットワークの要件

社内の Webex アプリでのコール (Unified CM) Wi-Fi ネットワーク上で使用する場合は、次の手順を実行することを推奨します。

- エレベータ、階段、屋外廊下などのエリアを含め、カバレッジのギャップを可能な限り排除するように、Wi-Fi ネットワークを設計します。
- すべてのアクセスポイントで、モバイルデバイスに同じ IP アドレスが割り当てられることを確認します。コール中に IP アドレスが変更されると、コールが切断されます。
- すべてのアクセスポイントの Service Set Identifier (SSID) が同一であることを確認します。SSID が一致しない場合、ハンドオフに時間がかかる場合があります。
- すべてのアクセスポイントで、SSID がブロードキャストされていることを確認します。アクセスポイントで SSID がブロードキャストされていないと、モバイルデバイスはコールを中断して別の Wi-Fi ネットワークに参加することをユーザに求める場合があります。
- NAT (STUN) パケットのセッショントラバーサルユーティリティの通過を許可するように、企業のファイアウォールが設定されていることを確認します。

サイト全体を調査し、音声品質に影響を与えるネットワークの問題を可能な限り解消してください。次のことをお勧めします。

- 重複しないチャンネルの設定、アクセスポイントのカバレッジ、および必要なデータレートとトラフィックレートを確認します。
- 不正なアクセスポイントは排除します。
- 考えられる干渉源の影響を特定して軽減します。

詳細については、次の資料を参照してください。

- 『「Enterprise Mobility Design Guide」』の「VoWLAN Design Recommendations」の項。
- 『Cisco Unified Wireless IP Phone 7925G Deployment Guide』
- 『Capacity Coverage & Deployment Considerations for IEEE 802.11g』ホワイトペーパー。
- ご使用のリリースの Cisco Unified Communications Manager の『Solutions Reference Network Design (SRND)』

ポートとプロトコル

Webex アプリでのコール (Unified CM) では、次の表に示すポートおよびプロトコルを使用します。クライアントとサーバ間にファイアウォールを展開する場合、次のポートおよびプロトコルを許可するようにファイアウォールを設定します。

ポート	アプリケーション層プロトコル	トランスポート層プロトコル	説明
Configuration			
6970	HTTP	TCP	TFTPサーバに接続し、クライアント設定ファイルをダウンロードする。
6972	HTTPS	TCP	TFTPサーバに接続して、Cisco Unified Communications Managerのクライアント設定ファイルを安全にダウンロードする。
8443	HTTPS	TCP	Cisco Unified Communications Managerへのトラフィック。
Communication Manager シグナリング			
2748	CTI	TCP	デスクフォン制御に使用される Computer Telephony Interface (CTI)。
5060	SIP	TCP	Session Initiation Protocol (SIP) コールシグナリングを提供する。

ポート	アプリケーション層プロトコル	トランスポート層プロトコル	説明
5061	SIP over TLS	TCP	SIP over TLS がセキュアな SIP コール シグナリングを提供する。(デバイスの Secure SIP が有効になっている場合に使用)。
5070 ~ 6070	BFCP	UDP	ビデオ画面共有機能の Binary Floor Control Protocol (BFCP)。
音声またはビデオメディアの交換			
16384 ~ 32766	RTP/SRTP	UDP	オーディオ、ビデオ、および BFCP ビデオデスクトップの共有に使用される Cisco Unified Communications Manager メディア ポートの範囲。
33434 ~ 33598	RTP/SRTP	UDP	オーディオおよびビデオに使用される Cisco Webex Hybrid Services のメディアポート範囲。
8000	RTP/SRTP	TCP	ユーザは、クライアントを介してコンピュータ上のデスクフォンデバイスに送信されたビデオを受信できる。

サポートされるコーデック

タイプ	コーデック	コーデックタイプ	Webex アプリ Android の 場合	Webex アプリ iPhone および iPad の場合	Webex アプリ (Mac の 場合)	Webex アプリ (Windows の場合)
音声	G.711	A-law	はい	はい	はい	はい
		μ -law/Mu-law	はい	はい	はい	はい
	G.722		はい	はい	はい	はい
	G.722.1	24 kb/s および 32 kb/s	はい	はい	はい	はい
	G.729		いいえ	いいえ	いいえ	いいえ
	G.729a		はい	はい	はい	はい
	Opus		はい	はい	はい	はい

タイプ	コーデック	コーデックタイプ	Webex アプリ Android の 場合	Webex アプリ iPhone お よび iPad の場合	Webex アプリ (Mac の 場合)	Webex アプリ (Windows の場合)
ビデオ	H.264/AVC	ベースライン プロファイル	はい	はい	はい	はい
		高プロファイル	いいえ	はい	はい	はい

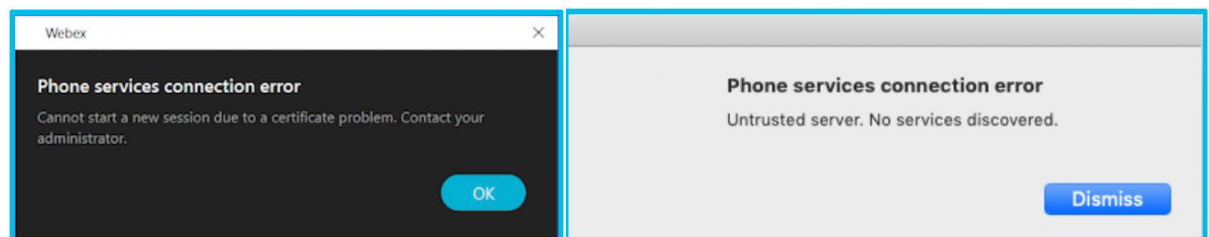
証明書の要件

Unified CM 証明書 (展開で MRA なし)

Unified CM とのセキュアな接続を確立するために、Webex アプリは、接続プロセス中にサーバから提示された証明書を検証します。Jabberとは異なり、Webex アプリでは、信頼されていない証明書を受け入れるオプションがユーザに表示されることはありません。

Unified CM は、Webex アプリが検証できる証明書を使用して設定する必要があります。tomcat 証明書 (Webex アプリが動作しているオペレーティングシステム、デフォルトでは Windows または MacOS にとって既知の証明書) に署名した CA ルートが推奨されますが、信頼された自己署名証明書も使用できます (エンタープライズ管理者が事前に OS に展開する必要があります)。

表 11: 証明書が信頼されていない場合の電話サービスエラー (Windows および Mac 用 Webex アプリ)



- (注) Tomcat 証明書は、Webex アプリで暗号化されたコールが有効になっている場合に、セキュア SIP にも使用されます (SIP Oauth はデフォルトポート 5090 で動作します)。詳細については、このガイドの「暗号化されたコールの電話セキュリティプロファイルの設定」を参照してください。

廃止されたシグニチャアルゴリズム (SHA-1 など) で発行された証明書は機能しません。Cisco Unified Communications Manager については、『*Administration Guide*』の「Certificates」の章に記載されているように、サポートされているセキュアシグニチャアルゴリズム (SHA-256 以降など) を使用する必要があります。



- (注) ユニファイド CM サーバに展開された証明書には、単純なホスト名または IP アドレスではなく、サーバ id として完全修飾ドメイン名 (FQDN) を含める必要があります (たとえば、**cucm** ではなく、**cucm-server-1.example.com**など)。

Cisco ユニファイド Cm Administration > System > server では、ユニファイド CM サーバ名を FQDN として定義する必要があります。

ユニファイド CM での証明書管理に関する情報については、CUCM および [CUCM 証明書の管理および変更通知の証明書と機関のハイレベルレビュー](#) を参照してください。

Unified CM 証明書 (展開で MRA あり)

Unified CM tomcat 証明書は、モバイルおよびリモートアクセス (MRA) にとって重要です。この証明書は、Cisco Unified Communications Manager に自動的にインストールされる。デフォルトでは、これは自己署名され、同じ共通名 (CN) を持ちます。



- (注) Tomcat 証明書は、Webex アプリ で暗号化されたコールが有効になっている場合に、セキュア SIP にも使用されます (MRA では、SIP Oauth はデフォルトポート 5091 で動作します)。詳細については、このガイドの「Configure the Phone Security Profile for Encrypted Calls」を参照してください。

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ2つの自己署名証明書は許可されません。そのため、Expressway の信頼される CA リストで CallManager と tomcat の自己署名証明書の CN が同じ場合、Expressway はそのうちの1つしか信頼できません。つまり、Expressway-C と Cisco Unified Communications Manager 間のセキュア HTTP またはセキュア SIP は失敗します。

Expressway 証明書 (展開で MRA あり)



- (注) MRA のシナリオでは、証明書は Expressway で検証する必要があるだけです。

Expressway の証明書署名要求 (CSR) ツールでは、Expressway でサポートされるユニファイド コミュニケーション機能に適した関連するサブジェクト代替名 (SAN) について確認が求められ、組み込まれます。

次の表は、どのCSR代替名要素がどのユニファイドコミュニケーション機能に適用されるかを示す。

表 12: 証明書署名要求代替名要素とモバイルおよびリモートアクセス (MRA)

Subject Alternative Names (SAN) として次の項目を追加する	MRA の証明書署名要求を生成する場合
Unified CM 登録ドメイン (名前にかかわらず、これらは Unified CM Unified CM SIP 登録ドメインよりもサービス発見ドメインと共通する)	Expressway-E でのみ必要
(クラスタ化されたシステムのみ) Expressway クラスタ名	Expressway-C でのみ必要



(注) 新しくアップロードされたサーバ証明書を有効にするには、Expressway を再起動する必要があります。

Expressway-E のサーバ証明書の要件

Expressway-E のサーバ証明書には、そのサブジェクト代替名 (SAN) のリストに次の要素が含まれる必要がある。

- **Unified CM 登録ドメイン** : Expressway-C で Unified CM 登録用に構成されているすべてのドメイン。エンドポイント デバイスと Expressway-E 間のセキュアな通信に必要です。

Expressway 構成および Expressway-E 証明書で使用される Unified CM 登録ドメインは、Mobile and Remote Access クライアントが、サービス発見中に `_collab-edge` DNS SRV レコードを検索するために使用される。これらは Unified CM での MRA 登録を可能にし、主にサービス発見用である。

これらのサービス検出ドメインは SIP 登録ドメインと一致することもしないこともあります。これは展開方法により異なるため、一致する必要はありません。1つの例は、内部ネットワーク上で Unified CM を使用した `.local` または類似のプライベートドメイン、および Expressway-E FQDN およびサービス発見のパブリックドメイン名を使用する展開である。Expressway-E の証明書にパブリックドメイン名を SAN として含める必要があります。Unified CM で使用されているプライベートドメイン名を含める必要はない。エッジドメインのみを SAN としてリストする必要があります。

DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。代わりに、`CollabEdgeDNS` 形式を選択でき、これは、入力するドメインにプリフィックス `collab-edge` を追加するだけである。この形式は、トップレベルドメインを SAN として含めたくない場合に推奨されます (次のスクリーンショットの例を参照してください)。

Alternative name

Subject alternative names: FQDN of Expressway cluster plus FQDN of this peer

Additional alternative names (comma separated):

Unified CM registrations domains: example.com Format: CollabEdgeDNS

XMPP federation domains: example.com Format: DNS

IM and Presence chat node aliases (federated group chat): chatnode1.example.com, chatnode2.example.com Format: DNS

Alternative name as it will appear: DNS:collab-edge.example.com, DNS:example.com, DNS:chatnode1.example.com, DNS:chatnode2.example.com

Jabber から Webex アプリに移行する際の要件

以降シナリオでは、Expressway-E 証明書の証明書失効リスト (CRL) のデフォルト形式 (ldap:///) でプライベート CA を使用している場合に問題が発生する場合があります。

その展開では、Jabber から Webex アプリに移行した後、iOS デバイスの Webex アプリは、Unified CM 電話サービスに登録されません。iOS クライアントはインターネットから CRL URL にアクセスしようとするため、登録は失敗しますが、CRL 形式の ldap:/// は iOS クライアントではサポートされていません。



ヒント Expressway-E の証明書を発行するためにプライベート CA を使用している場合は、Expressway-E がパブリック CA によって発行され、Jabber から Webex アプリにユーザーを移行することをお勧めします。

Expressway-E セットアップにプライベート CA によって署名された証明書 (特に、ldap:/// 形式の CRL) を使用する必要がある場合は、次の手順に従って、Jabber から Webex アプリへの移行を成功させます。

- ある場合は、private CA テンプレートから CRL パラメータを削除します。
- CRL パラメータなしで Expressway-E サーバー証明書を再発行します。
- プライベート CA が署名する証明書が iOS の次の要件をサポートしていることを確認してください。
 - 最小キーサイズが 2048
 - SHA-2 署名
 - SAN としてのサーバー ドメイン ネーム システム (DNS) 名
 - id-kp-serverAuth OID を含む拡張キー使用延長
 - 有効期間は 398 日以内
- モバイルデバイスにルート CA ファイルをインストールする



- (注) Apple iOS デバイスの場合、[ルート証明書の完全信頼も有効にする](#)必要があります。

ヘッドセットの要件

Webex アプリでの Unified CM コールでは、シスコ Series の次のヘッドセットがサポートされています。各モデルの詳細な情報については、[リンクをクリックしてください](#)。

- [520 Series](#)
- [530 Series](#)
- [560 Series](#)
- [730 Series](#) (Bluetooth)

いくつかの Jabra ヘッドセットもサポートされます。詳細については、「[ヘッドセットサポートに関する詳細](#)」を参照してください。



- (注) Webex アプリでサポートされているヘッドセットを使用すると、ヘッドセットのファームウェアが自動的に更新される場合があります。ユーザは、更新が可能であることを知らせるポップアップメッセージを受け取ります。更新後、確認の通知を受け取ります。

ライセンス要件

有料サブスクリプションのある Cisco Webex 組織 (Control Hub で管理) が必要である。ユーザアカウントは組織内で管理する必要がありますが、特定のライセンス割り当てて Webex アプリでのコール (Unified CM) を使用する必要はありません。

また、ソフトフォン機能では、各 Webex アプリがソフトフォンクライアントとして Unified CM に登録されます。Cisco Jabber と同様に、この登録ではデスクトップ用の Cisco ユニファイドクライアントサービスフレームワーク (CSF) クライアントと、モバイル用のボット、TCT、または TAB デバイスを使用し、ユニファイド CM ライセンスに向けたデバイスとしてカウントします。3つ以上のアプリやデバイスを使用しているユーザは、CUWL 永久ライセンスを必要とし、または、組織が Flex Calling サブスクリプションを利用している必要がある。



- ヒント Webex アプリでのコール (Unified CM) のサブスクリプションチャネルとして、フレックスコールを推奨しています。

Webex アプリ 要件

Webex アプリでのコール (Unified CM) 機能が正しく動作し、最新機能やその他の修正が継続的に配信されるようにするには、ユーザが [デスクトップまたはモバイル](#)、または最新の [VDI シンクライアント](#) 用の最新リリースの Webex アプリ を使用している必要があります。



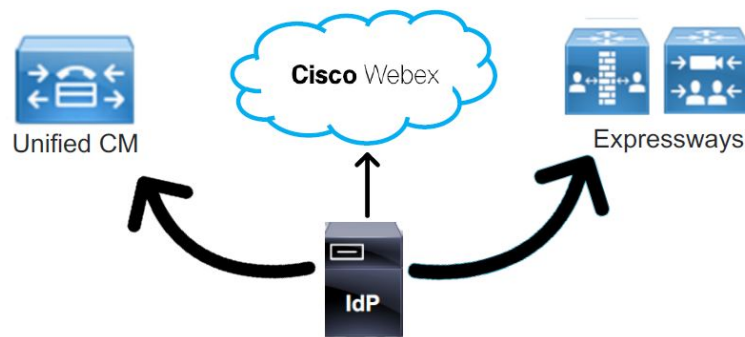
(注) Web アプリ (web.webex.com) では、ユーザが電話番号を呼び出すことはできません。

- インストールとアップグレードの手順については、[「インストールと自動アップグレード」](#) を参照してください。
- 組織のユーザーに対して Webex アプリ の更新頻度を管理する場合は、[「Webex アプリ の製品更新制御」](#) を参照してください。
- ARM および x86 アーキテクチャ両方の Chromebook は、Webex アプリでのコール (Unified CM) でサポートされています。また、Chromebook と Android の両方の電話機で同時に電話機サービスにログインすることができます。
- VDI の導入手順については、[『仮想デスクトップインフラストラクチャ \(VDI\) 導入ガイド』](#) を参照してください。
- リリース情報については、Webex アプリ の [リリースノート](#) および [新機能に関するドキュメント](#) および Webex アプリ の VDI 用 [VDI リリースノート](#) を参照してください。

推奨構成

シングルサインオンと IdP の統合

- Webex アプリでのコール (Unified CM) では、SSO は、ユニファイド CM および Expressway でサポートされています。両方の SSO を有効または無効にする必要があります。SSO による一貫したユーザエクスペリエンスを実現するために、ID プロバイダー (IdP) 統合を Webex アプリ に拡張して、ユーザが同じログイン情報でサインインできるようにすることを推奨します。IdP、宅内環境、および Webex クラウド間のシングルサインオン (SSO) 統合により、ユーザは1つのクレデンシャルセットを使用してアプリケーション間でサインインできます。



- オンプレミスのユニファイド CM 設定については、ご使用のリリースの [Cisco Unified Communications アプリケーションの SAML SSO 導入ガイド](#) を参照してください。導入環境で、ユニファイド CM とすべての Unity Connection ボイスメール サーバにこの設定を適用することを推奨します。
- Expressway の設定については、ご使用のリリースの『[Cisco Expressway 経由の導入ガイド モバイルおよびリモートアクセス](#)』を参照してください。
- クラウド (Webex アプリ) の設定については、「[Webex Control Hub とのシングルサインオン統合 \(https://help.webex.com/article/lfu88u\)](#)」を参照してください。

対応済みの認証タイプについては、次の表を参照してください。

表 13: サポートされている認証タイプ

タイプ	Windows	Mac	iOS	Android
NTLM を使用した IWA 認証	✓	✓	✓ SSO リダイレクト URI の要件を参照してください。	✓
ケルベロスを使用した IWA 認証	✓			
フォームベースの認証	✓	✓	✓	✓
証明書ベースの認証	✓	✓	✓ SSO リダイレクト URI の要件を参照してください。	✓

SSO リダイレクト URI

Webex アプリは、SSP リダイレクト URO をサポートし、アプリの埋め込みブラウザ対応で強化されました。

この機能は次の点で強化されています。

- [RFC7636](#) を使用して、「承認コードの傍受攻撃」から保護します。
- iOS 以外のオペレーティングシステムで実行されている Webex アプリで Android などの埋め込みブラウザを使用できます。
- Webex アプリが Unified Communications Manager (および MRA) OAuth フローの標準搭載ブラウザを使用できるように許可します。SSO が有効になっている場合、このサポートにより二重ログインを回避できます。

要件

この機能には、次の最小バージョンが必要です。

- Unified CM 12.5(x) リリース - 12.5(1) SU4 および Unified CM 14.0(x) リリース - 14.0(1) SU1 以降
- Expressway X14 以降
- Webex アプリ 41.4 以降

詳細については、次の資料を参照してください。

- [Expressway リリースノート](#)
- [Unified CM リリースノート](#)

構成

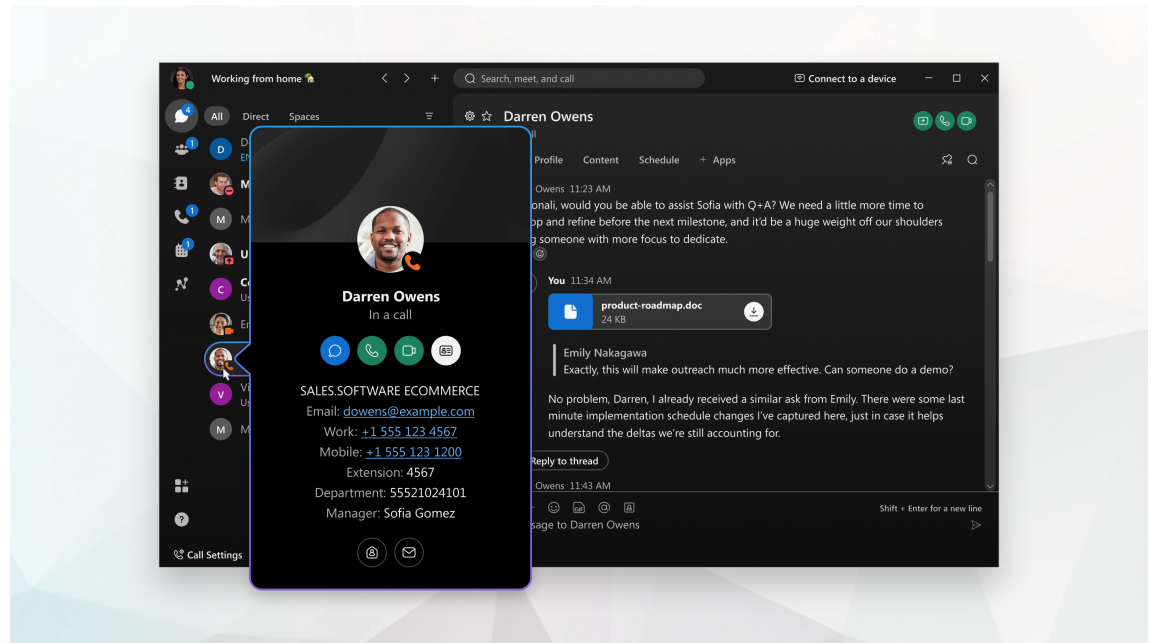
Unified CM の場合：構成は不要です。

Expressway の場合：Expressway-C で、**Webex Client Embedded Browser Support** のパラメータを **[[はい]]** に設定して、この機能を有効化します。詳細については、『*Cisco Expressway* を介したモバイルおよびリモートアクセスに関する導入ガイド (X14.0)』に記載されている「[MRA アクセス制御の構成](#)」を参照してください。

ディレクトリ同期および連絡先カード

Active Directory から Control Hub にユーザー同期をする場合は、Cisco Directory Connector を使用することが推奨されます。

また、ユーザの電話番号を同期することができます。この番号は、Windows および Mac 用の Webex アプリの連絡先カードに表示されます。



- (注) iOS および Android では、ユーザはプロフィールの写真をタップするだけでスペースから連絡先カードにアクセスできます。詳細については、「[連絡しようとしている相手を確認する](#)」を参照してください。

番号が表示されるようにするには、Cisco Directory Connector を展開して、既存の Active Directory 属性からクラウドに番号を同期する必要があります。の属性マッピング情報については、『*Cisco Directory Connector の導入ガイド*』（<https://www.cisco.com/go/hybrid-services-directory>）を参照してください。

Webex アプリの自動プロビジョニングの概要

Control Hub の自動プロビジョニング機能を使用すると、ユーザーはゼロまたは最小限の介入で、Calling in Webex (Unified CM) 用デバイスを自分でプロビジョニングできます。この機能により、Unified CM での複数のデバイスのオーバープロビジョニングが回避され、クラスタの拡張とライセンスの使用への影響を最小限に抑えることができます。Calling in Webex (Unified CM) にプロビジョニングされたユーザーが、登録済み E メールアドレスかユーザー ID で Webex アプリにサインインすると、デバイスが自動で作成されます。

組織内のユーザーは Webex アプリデバイスに事前にプロビジョニングされるため、管理者は Unified CM に行く必要はありません。ユーザーが任意のデバイスを使用して Webex アプリに初回サインインした際に、デバイスがまだ Unified CM サーバーで使用できない場合、ユーザーの新しいデバイスタイプが自動的に作成されます。

この機能により、ユーザーがさまざまなデバイスプラットフォームから Webex アプリにサインインするときに、Unified CM で次のデバイスタイプの自動プロビジョニングが可能になります。

- Android デバイス (BOT)
- Chromebook/iPad デバイス (TAB)
- Windows/MAC デバイス (CSF)
- iPhone デバイス (TCT)



Note デバイスを削除した後、同じタイプのデバイスを自動プロビジョニングするまで、5分～10分待つことをお勧めします。また、デバイスを再度自動プロビジョニングする前に、Webex アプリからデバイスをリセットすることもできます ([ヘルプ (Help)] > [正常性チェック (Health Checker)] の順に選択し、[リセット (Reset)] ボタンをクリック)。

前提条件

ユーザーに Webex アプリの自動プロビジョニングを許可する前に、次の要件を満たしていることを確認してください。

- クラウド接続 UC をアクティブ化し、組織内のオンプレミスデバイスを設定して、Control Hub と通信します。詳細については、「[オンプレミスデバイス用のクラウド接続 UC のセットアップ](#)」を参照してください。
- Control Hub のユーザーアカウントには、Basic または Professional Webex Calling ライセンスのいずれかを追加します。
- Cisco Unified Communications Manager クラスタは、バージョン 11.5 以上である必要があります。Calling in Webex (Unified CM) でサポートされている Unified CM のバージョンについては、「[Calling in Webex \(Unified CM\) 用導入ガイド](#)」を参照してください。
- サポートされている Webex アプリの最小バージョンは 41.12 以降です。
- サポートされる Cisco Expressway リリースの最小バージョンは X14.0.2 です。Expressway のバージョンが推奨バージョンよりも低い場合、Expressway は次の URL を許可リストに手動で追加して、外部クライアント (Cisco Jabber または Webex アプリ) が MRA 構成で検出された Unified Communications ノードにアクセスできるようにする必要があります。
 - **POST** : <https://{{cucmip}}:8443/devicemanagement/v1/clientAutoProv/createDevice>
 - **GET** : <https://{{cucmip}}:8443/ucmservices/v1/supportedServices>
- Unified CM ユーザーのユーザー ID または E メールアドレスが、Webex Identity Service のユーザーレコードエンティティのユーザー ID と一致することを確認します。また、Unified CM サーバーで構成されたユーザーは、組織の Webex Identity Service で使用できる必要があります。

追加構成

Webex アプリでのコール (Unified CM) 展開の利点をさらに高めるために、次の追加設定を推奨します。

- Quality of Service (QoS) については [付録 \(135 ページ\)](#)、このガイドの中で説明しています。QoS を使用すると、ネットワークインフラストラクチャのパケット損失、遅延、ジッターを管理できます。
- 『システム構成ガイド』で説明されている、[Cisco Unified Communications Manager のためのコールアドミッション制御 \(CAC\)](#)。CAC を使用すると、そのリンクで同時に許可されるコールの数を制限することによって、ワイドエリア (IP WAN) リンクを介したコールの音声品質とビデオ品質を制御できます。



第 3 章

Webex アプリでのコール（Unified CM）の導入

- [Webex アプリでのコール（Unified CM） 展開タスクフロー（85 ページ）](#)
- [サービスプロファイルの概要（90 ページ）](#)
- [UC サービスワークフローの構成（91 ページ）](#)
- [サービスの発見オプション（95 ページ）](#)
- [認証オプション（97 ページ）](#)
- [デスクトップクライアントの電話構成でパラメータを設定（97 ページ）](#)
- [Webex アプリでのコール（Unified CM）の Unified CM エンドユーザーの構成（98 ページ）](#)
- [ソフトフォンワークフローの作成（99 ページ）](#)
- [プッシュ通知の構成と推奨設定（106 ページ）](#)
- [クライアント構成パラメータの設定（リリース 12.5 以降）（107 ページ）](#)
- [クライアント構成ファイルの作成とホスト（12.5 以前のリリース）（108 ページ）](#)
- [共通構成の作成（113 ページ）](#)
- [通話を会議に移動する構成（114 ページ）](#)
- [ユーザーワークフロー用通話エクスペリエンス（116 ページ）](#)
- [Webex アプリでの電話サービスの認証（122 ページ）](#)
- [展開後に追加機能を構成する（124 ページ）](#)
- [既知の問題と Webex アプリでのコール（Unified CM）の制限事項（125 ページ）](#)

Webex アプリでのコール（Unified CM） 展開タスクフロー

これらの手順では、に使用される一般的な電話機 Webex アプリでのコール（Unified CM）のみの導入を順を追って説明します。この展開では、Webex アプリは Cisco Jabber と同様に、ソフトフォンクライアントとして Unified CM に登録されます。

始める前に

[Webex アプリでのコール（Unified CM） 用環境の準備（57 ページ）](#)

手順

	コマンドまたはアクション	目的
ステップ 1	<p>UC サービスワークフローの構成 (91 ページ)</p> <ul style="list-style-type: none"> ボイスメールのパイロット番号の構成 (92 ページ) UC サービスの構成 (93 ページ) UC サービスを使用したサービスプロファイルの構成 (94 ページ) 	<p>サービス プロファイルに UC サービスをまとめてバンドルします。ユーザに関連付けられたデバイスを Webex アプリ に提供する CTI サービスを作成する必要があります。ユーザが Webex アプリ でボイスメールにアクセスできるようにする場合は、ボイスメールサービスを作成します。最後に、サービス プロファイルを作成して、後でエンドユーザアカウントに適用される UC サービスを追加します。</p>
ステップ 2	<p>サービスの発見オプション (95 ページ) から選択する。</p> <ul style="list-style-type: none"> DNS SRV レコードの構成 (95 ページ) 手動接続設定 (122 ページ) 	<p>サービス ディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。次のいずれかのオプションを使用してサービスディスカバリを設定できます。</p> <ul style="list-style-type: none"> DNS SRV レコード: クライアント (Webex アプリ) が自動的にサービスを見つけて接続します。これは推奨オプションです。 手動接続設定: 手動接続設定はサービス発見が使用されていない場合にフォールバックメカニズムを提供する。管理者の指示により、ユーザは、タスクフローの最後に記載されているように、サーバアドレスまたは UC ドメインの後に、SSO または非 SSO クレデンシャルを手動で入力する必要があります。
ステップ 3	<p>認証オプション (97 ページ) から選択する。</p> <ul style="list-style-type: none"> クライアントの SAML SSO (97 ページ) LDAP サーバーによる認証 (97 ページ) 	<p>これらのオプションは、で Webex アプリユーザが電話サービスにサインインするときに使用される認証メカニズムを決定します。</p> <ul style="list-style-type: none"> SAML シングルサインオン (SSO): エンドユーザのパスワードは、SSO に使用される id プロバイダーに存在するパスワードに対して認証されます。 LDAP サーバ: エンドユーザパスワードは、会社の LDAP ディレクトリに割り当てられているパスワードに対して認証される。
ステップ 4	<p>デスクトップクライアントの電話構成でパラメータを設定 (97 ページ)</p>	<p>クライアントは、Cisco Unified Communications Manager 上の特定の場所から電話の各種設定を取得できる。</p>

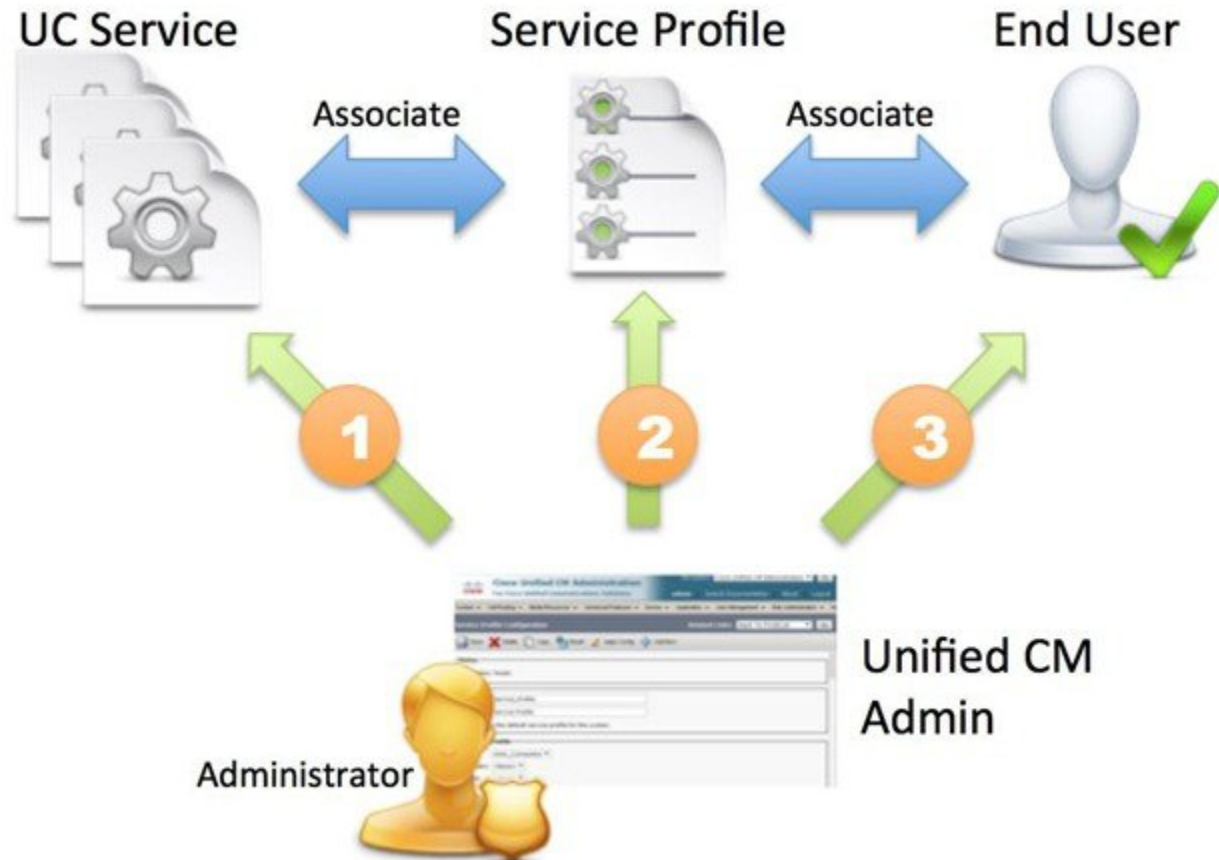
	コマンドまたはアクション	目的
ステップ 5	Webex アプリでのコール (Unified CM) の Unified CM エンドユーザーの構成 (98 ページ)	Webex アプリでのコール (Unified CM) を機能させるには、新しいユーザを作成するか、次の設定で Unified CM の既存のユーザを設定する必要がある。
ステップ 6	<p>ソフトフォンワークフローの作成 (99 ページ) の手順に従う。</p> <ul style="list-style-type: none"> • デバイスにディレクトリ番号を追加する (103 ページ) • ユーザーとデバイスの関連付け (104 ページ) • 暗号化された通話用の電話機セキュリティプロファイルを構成 (105 ページ) 	これらの手順に従って、ソフトフォンデバイスを手動または自動で作成し、構成し (ソフトフォン使用の場合、各 Webex アプリ に対応)、ソフトフォンデバイスにディレクトリ番号を追加したら、デバイスをエンドユーザーアカウントに関連付けます。必要に応じて、安全かつ暗号化された通話を実現するためにデバイスと Webex アプリ インスタンスを構成します。
ステップ 7	<p>ソフトフォンワークフローの作成 (99 ページ) の手順に従う。</p> <ul style="list-style-type: none"> • 次のいずれかのオプションを使用してソフトフォンを作成して構成します。 <ul style="list-style-type: none"> • Automatic (クラウド接続 UC (CCUC) を経由した Control Hub) — デバイスの自動プロビジョニング。 <p>(注) このプロセスでは、ユーザーのデバイスを自動作成し、ユーザーを電話サービスに接続するまでに最大 5 分かかる場合があります。ユーザーが自動プロビジョニングをサポートしていないバージョンのアプリを使用していた場合、アプリをアップグレードするために再起動する必要があります。その後、指定された時間枠でソフトフォンデバイスが自動作成されます。</p> • Manual (Unified CM) — Webex アプリ ソフトフォンデバイスの作成と構成 (100 ページ) • デバイスにディレクトリ番号を追加する (103 ページ) • ユーザーとデバイスの関連付け (104 ページ) • 暗号化された通話用の電話機セキュリティプロファイルを構成 (105 ページ) 	これらの手順に従って、ソフトフォンデバイスを手動または自動で作成し、構成し (ソフトフォン使用の場合、各 Webex アプリ に対応)、ソフトフォンデバイスにディレクトリ番号を追加したら、デバイスをエンドユーザーアカウントに関連付けます。必要に応じて、安全かつ暗号化された通話を実現するためにデバイスと Webex アプリ インスタンスを構成します。

	コマンドまたはアクション	目的
ステップ 8	プッシュ通知の構成と推奨設定 (106 ページ)	プッシュ通知に対応する展開では、Google または Apple のクラウドベースのプッシュ通知サービスを使用して、バックグラウンドで動作している iOS および Android 用 Webex アプリ クライアントに音声通話、ビデオ通話、インスタントメッセージの通知をプッシュします。iOS および Android 用 Webex アプリ との永続的な通信を維持するには、プッシュ通知を有効にする必要があります。
ステップ 9	次のオプションを選択します。 <ul style="list-style-type: none"> クライアント構成パラメータの設定 (リリース 12.5 以降) (107 ページ) (最優先) クライアント構成ファイルの作成とホスト (12.5 以前のリリース) (108 ページ) 	次のいずれかの方法を使用してユーザがログインしたときに適用されるクライアント設定パラメータを設定できます。 <ul style="list-style-type: none"> Unified CM でクライアント設定パラメータを設定します。 設定パラメータを含む XML エディタを使って XML ファイルを作成します。次に、TFTP サーバで XML ファイルをホストします。Webex アプリでのコール (Unified CM) で、既存の Jabber の構成 XML ファイル機能を利用します。このファイルを使用すると、組織内の Webex アプリ ユーザに対して、特定のコール機能 (ハントグループやコールピックアップなど) やその他のサポートされている機能を有効にすることができます。
ステップ 10	通話を会議に移動する構成 (114 ページ)	通話中のユーザは、高度な会議機能を利用しながら、他の同僚を会議に招待できます。ユーザは、そのコールを会議に移動できます。そこから、何か重要なことを共有したいときに手を挙げたり、誰かの発言に対して視覚的に同意を示すために絵文字を追加したり、ブレイクアウトルームを使用することができます。
ステップ 11	次のユーザーワークフロー用通話エクスペリエンス (116 ページ) の手順に従ってください。 <ul style="list-style-type: none"> UC マネージャプロファイルの作成 (117 ページ) UC マネージャプロファイルの編集 (130 ページ) Control Hub での通話動作と UC マネージャプロファイルの設定 	Control Hub を使用して、ユーザのコールエクスペリエンスをカスタマイズできます。音声サービスドメイン、UCS サーバ、またはその両方を使用して UC マネージャプロファイルを設定します。一部のユーザ (推奨) または組織全体 (サービスを展開する準備ができていない場合) のコール動作を設定します。Webex アプリでのコール (Unified CM) では、ユーザが発信機能セットを使用できるように、この設定を設定します。アプリに表示されるコールオペ

	コマンドまたはアクション	目的
		ションと、シングルクリックツーコールを実行できるようにするかどうかを設定します。
ステップ 12	Webex アプリでの電話サービスの認証 (122 ページ)	DNS SRV を導入している場合、ユーザーは、Webex アプリの電話サービスで自動検出されます。これを行わない場合は、前に設定した UC マネージャプロファイルでサインインプロセスを簡略化できます。これには、電話機の UDS サーバまたは UC ドメイン (FQDN または IP アドレス) が含まれています。これらのすべての設定が行われていない場合、ユーザーは、UDS サーバまたは UC ドメイン (FQDN または IP アドレス) のサーバアドレスを手動で入力する必要があります。
ステップ 13	展開後に追加機能を構成する (124 ページ)	これらのタスクはオプションであり、Webex アプリでのコール (Unified CM) の展開には必須ではありません。ただし、これらの機能は、自分とユーザーに対してより多くのカスタマイズを提供します。追加のガイダンスについては、各ステップリンクされている資料を参照してください。

サービスプロファイルの概要

図 6: サービスプロファイルのワークフロー



1. UC サービスの作成します。
2. UC サービスをサービス プロファイルに関連付けます。
3. ユーザをサービスプロファイルに関連付けます。

デフォルトのサービスプロファイルの作成

UC サービスを追加するためのサービスプロファイルを作成します。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ 2 [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービス プロファイル (Service Profile)] の順に選択します。

[サービス プロファイルの検索と一覧表示 (Find and List Service Profiles)] ウィンドウが開きます。

ステップ3 [新規追加] を選択します。

[サービス プロファイルの設定 (Service Profile Configuration)] ウィンドウが開きます。

ステップ4 [名前 (Name)] フィールドにサービス プロファイルの名前を入力します。

ステップ5 サービス プロファイルをクラスタのデフォルトにする場合は、[システム デフォルトのサービス プロファイルに設定 (Make this the default service profile for the system)] を選択します。

(注) Cisco Unified Communications Manager リリース 9.x のみ、IM 専用ユーザはデフォルト サービス プロファイルを使用する必要があります。このため、[デフォルトを使用 (Use Default)] を選択します。

ステップ6 [保存] を選択します。

次のタスク

展開用の UC サービスを作成します。

UC サービスワークフローの構成

Webex アプリでのコール (Unified CM) 展開用のサービス プロファイルに、関連する UC サービスを設定します。CTI サービスは必須です。

Unity Connection を導入しており、ボイスメールアクセスを Webex アプリ に統合する必要がある場合に、ボイスメール サービスをセットアップします。

始める前に

[ボイスメール \(68 ページ\)](#)

手順

	コマンドまたはアクション	目的
ステップ1	ボイスメールのパイロット番号の構成 (92 ページ)	ボイスメールのアクセスを Webex アプリ ユーザに対して設定する場合は、ユニファイド CM の展開時にボイスメール システムへのアクセスに使用するディレクトリ番号を必ず確認してください。
ステップ2	UC サービスの構成 (93 ページ)	CTI UC サービスは、そのユーザに関連付けられているデバイスのリストを取得する CTI サービスの場所を Webex アプリ に提供します。ボイスメール サービスは、既存の Unity Connection の展開に結び付け、対応するサービス プロファイルに関連付けられている場合は、ユーザにボイスメールを取得させます。
ステップ3	UC サービスを使用したサービスプロファイルの構成 (94 ページ)	Cisco Unified Communications Manager サービスを追加して設定したら、それらをサービスプロファイル

	コマンドまたはアクション	目的
		に追加します。サービスプロファイルで追加の設定を適用できます。

次のタスク

サービス プロファイルをエンド ユーザ アカウントに関連付けます。

ボイスメールのパイロット番号の構成

ボイスメールパイロット番号は、ユーザが自分のボイス メッセージにアクセスする場合に使用する電話番号を指定するものです。ユーザが電話機の [メッセージ (Message)] ボタンを押すか、Webex アプリ からボイスメールにアクセスすると、Cisco Unified Communications Manager が自動的にボイスメッセージ番号をダイヤルします。パイロット番号はそれぞれ異なるボイスメッセージ システムに所属させることができます。

ステップ 1 Cisco Unified CM の管理から、**詳細機能 > ボイスメール > ボイスメールパイロット**に移動します。

ステップ 2 次の設定を行います。

- **ボイスメールパイロット番号** : ボイスメールパイロット番号を識別する番号を入力します。使用できる文字は、数字 (0 ~ 9)、プラス (+)、アスタリスク (*)、およびポンド (#) です。
 (注) [ボイスメールパイロット番号 (Voice Mail Pilot Number)] と [コーリングサーチスペース (Calling Search Space)] の両方のフィールドが空白の場合、設定を保存できません。この 2 つのフィールドのいずれかに値を入力する必要があります。
- **コール検索スペース** : 適切なコール検索スペースを選択します。コーリングサーチスペースは、このパイロット番号からコールを発信できる番号を検索するための、パーティションのコレクションで構成されます。
- **説明** : パイロット番号の説明を記述します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符 (")、パーセント記号 (%)、アンパサンド (&)、山カッコ (<>) は使用できません。
- **これをシステムのデフォルトのボイスメールパイロットにします**。この設定をオンにすると、このパイロット番号を使用して、システム用のデフォルトボイスメールパイロット番号にすることができます。
 (注) [デフォルト (Default)] ボックスをオンにすると、現在のデフォルトパイロット番号がこのボイスメールパイロット番号に変更されます。

ステップ 3 変更を保存します。

UC サービスの構成

Cisco Unified Communications Manager サービスを追加して、アドレスおよびサービスのその他設定を指定します。

CTI UC サービスは、そのユーザに関連付けられているデバイスのリストを取得する CTI サービスの場所を Webex アプリに提供します。ボイスメールサービスは、既存の Unity Connection の展開に結び付け、対応するサービスプロファイルに関連付けられている場合は、ユーザにボイスメールを取得させます。

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。
- [UC サービスの検索と一覧表示 (Find and List UC Services)] ウィンドウが開きます。
- ステップ 3** [新規追加] を選択します。
- [UC サービスの設定 (UC Service Configuration)] ウィンドウが開きます。
- ステップ 4** [UC サービスの追加 (Add a UC Service)] セクションで、[UC サービス タイプ (UC Service Type)] ドロップダウン リストから [CTI] を選択します。
- ステップ 5** [Next] を選択します。
- ステップ 6** 次の手順に従って、CTI サービスの詳細情報を提供する。
- [名前 (Name)] フィールドにサービスの名前を入力します。
入力した名前は、プロファイルにサービスを追加する際に表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。
 - [ホスト名/IP アドレス (Host Name/IP Address)] フィールドに、CTI サービスのアドレスを入力します。
ホスト名、IPアドレス、または完全修飾ドメイン名 (FQDN) の形式でアドレスを入力する。この値は、CTI Manager サービスを実行しているユニファイド CM パブリッシャに対応します。サブスクライバに対して2番目のサービスを作成します。
 - [ポート (Port)] フィールドに、CTI サービスに使用するポート番号を入力します。
- ステップ 7** 変更内容を保存し、[ユーザの管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] に戻り、[新規追加 (Add New)] をクリックします。
- ステップ 8** [ボイスメール (Voicemail)] を選択して [次へ (Next)] をクリックします。
- ステップ 9** 次の手順に従って、ボイスメール サービスの詳細情報を設定します。
- [名前 (Name)] フィールドにサービスの名前を入力します。
入力した名前は、プロファイルにサービスを追加する際に表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。
 - [ホスト名/IP アドレス (Host Name/IP Address)] フィールドでボイスメール アドレスを指定します。

完全修飾ドメイン名 (FQDN) の形式でアドレスを入力します。そうしないと、証明書の検証手順は失敗します。

(注) デフォルトでは、クライアントは常にポート 443 と HTTPS プロトコルを使用してボイスメールサーバに接続しています。そのため、ユーザが指定する値は有効になりません。

ステップ 10 変更を保存します。

次のタスク

UC サービスをサービスプロファイルに追加します。

UC サービスを使用したサービスプロファイルの構成

Cisco Unified Communications Manager サービスを追加して設定したら、それらをサービスプロファイルに追加します。サービスプロファイルで追加の設定を適用できます。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ 2 [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービスプロファイル (Service Profile)] の順に選択します。

ステップ 3 [名前 (Name)] フィールドにサービスプロファイルの名前を入力します。

ステップ 4 サービスプロファイルをクラスタのデフォルトにする場合は、[システムデフォルトのサービスプロファイルに設定 (Make this the default service profile for the system)] を選択します。

ステップ 5 [ボイスメールプロファイル (Voicemail Profile)] および [CTIプロファイル (CTI Profile)] に UC サービスを追加します。

ステップ 6 [ボイスメールサービスのログイン情報ソース (Credential source for voicemail service)] を [Unified CM - IM and Presence] に設定します。




ステップ 7 必要に応じて追加設定を完了し、[保存 (Save)] をクリックします。

次のタスク

Unified CM で構成されているサービスプロファイルをエンドユーザアカウントに割り当てる必要があります。

Webex アプリのボイスメールアイコンインジケータ

Unity Connection サーバのビジュアルボイスメールの Web バージョンでは、ボイスメールの作成時に、以下の属性を示すチェックボックスが提供されます。Webex アプリでは、ユーザのビジュアルボイスメールの一覧に含まれるボイスメッセージエントリの横に、対応するアイコンが表示されます。

-  感嘆符：緊急で重要なボイスメッセージを示します。
-  ロック：セキュアなボイスメッセージを示します。メッセージは再生のたびにダウンロードされ、終了するとローカルファイルが削除されます。
-  キー：プライベートなボイスメッセージを示します。プライベートメッセージを他の人に転送することはできません。

サービスの発見オプション

サービス検出により、クライアントは、エンタープライズ（内部）ネットワークおよび MRA（外部）ネットワークにあるサービスを自動的に検出できます。次のいずれかのオプションを使用してサービスディスカバリを設定できます。

オプション	説明
DNS SRV レコードの構成 (95 ページ)	クライアントはサービスを自動的に検出して接続します。 これは推奨オプションです。
手動接続設定 (122 ページ)	手動接続設定は、サービス ディスカバリが使用されていない場合にフォールバック メカニズムを提供します。



- (注) シスコでは、内部環境と MRA 環境で SRV ルックアップをサポートしています。サービス検出により、クライアントは、エンタープライズネットワークの内部または外部にあるサービスを自動的に検出できます。クライアントは、ドメインネームサーバのクエリーを実行して、サーバの場所を提供するサービス (SRV) レコードを取得します。内部環境および外部環境について、以降の DNS SRV のガイダンスを参照してください。

DNS SRV レコードの構成

始める前に

『*Planning Guide For Cisco Jabber*』の「*Service Discovery*」の章に記載されている SRV レコードの要件を確認します。

展開用の SRV レコードを作成します。

オプション	説明
_cisco-uds	Cisco Unified Communications Managerの場所を提供する。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。
_collab-edge	Cisco VCS の提供先または Cisco Expressway-E の場所を指定します。クライアントは、Cisco Unified Communications Manager からサービスプロファイルを取得してオーセンティケータを決定できます。

SRV レコードの例

```
_cisco-uds._tcp.DOMAIN service location:
priority = 0
weight = 0
port = 8443
svr hostname=_cisco-uds._tcp.example.com
```

次のタスク

[SRV レコードのテスト \(96 ページ\)](#)

SRV レコードのテスト

SRV レコードを作成した後、それらがアクセス可能かどうかを確認します。



ヒント Webベースのオプションが必要な場合は、[コラボレーションソリューションアナライザ](#)サイトの SRV チェックツールを使用することもできます。

ステップ 1 コマンドプロンプトを開きます。

ステップ 2 **Nslookup**を入力します。

デフォルトの DNS サーバとアドレスが表示されます。これが想定されている DNS サーバであることを確認します。

ステップ 3 **set type=SRV** と入力します。

ステップ 4 各 SRV レコードの名前を入力します。

たとえば、_cisco uds _tcp。例ドメイン

- サーバとアドレスの表示: SRV レコードにアクセスできます。

- `_Cisco uds_tcp` を表示します。例ドメイン: 存在しないドメイン:SRV レコードに問題があります。

認証オプション

クライアントの SAML SSO

SSO を Unified CM と統合して、Webex アプリ ユーザが単一のログイン情報セットを使用してサインインできるようにする方法の詳細については、『Cisco Unified Communications アプリケーション SAML SSO 導入ガイド』を参照してください。Cloud (Webex Control Hub) の設定については、「シングルサインオンと Webex コントロールハブの統合」を参照してください。

LDAP サーバーによる認証

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンドユーザのパスワードが認証されるようにするには、この手順を実行します。LDAP 認証により、システム管理者は会社のすべてのアプリケーションに対してエンドユーザの1つのパスワードを割り当てることができます。ユーザがクライアントにサインインすると、Webex アプリ がその認証を Cisco Unified Communications Manager にルーティングする。その後、Cisco Unified Communications Manager がその認証をディレクトリ サーバに送信します。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ 2 [システム (System)] > [LDAP] > [LDAP 認証 (LDAP Authentication)] を選択します。

ステップ 3 [エンドユーザ用 LDAP 認証の使用 (Use LDAP Authentication for End Users)] を選択します。

ステップ 4 必要に応じて、LDAP クレデンシャルとユーザ検索ベースを指定します。

[LDAP認証 (LDAP Authentication)] ウィンドウ上のフィールドの詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。

ステップ 5 [保存 (Save)] を選択します。

デスクトップクライアントの電話構成でパラメータを設定

クライアントは、Cisco Unified Communications Manager 上の次の場所から電話の各種設定を取得できます。

エンタープライズ電話の設定 (Enterprise Phone Configuration)

クラスタ全体に適用されます。



- (注) IM and Presence サービス機能のみを使用しているユーザ (IM 専用) の場合は、[エンタープライズ電話の設定 (Enterprise Phone Configuration)] ウィンドウで電話の設定パラメータを設定する必要があります。

Common Phone Profile Configuration

デバイスのグループに適用され、クラスタの設定よりも優先されます。

[Cisco Unified Client Services Framework (CSF) 電話機の設定 (Cisco Unified Client Services Framework (CSF) Phone Configuration)]

個別の CSF デスクトップデバイスに適用され、グループの設定よりも優先される。

Webex アプリでのコール (Unified CM) の Unified CM エンドユーザーの構成

Webex アプリでのコール (Unified CM) を有効にするには、次の設定を使用して新しいユーザを作成するか、またはユニファイド CM で既存のユーザを設定する必要があります。



- (注) LDAP 同期を使用する場合は、これらの設定がすでに行われている可能性があります。新しい LDAP 同期を設定する場合は、で『Cisco Jabber のオンプレミス展開』ドキュメント (<https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>) の「ldap 同期の概要」を参照してください。

ステップ 1 [Cisco Unified CM Administration] から、**User Management > End Users** に移動して任意の条件を選択し、**Find** をクリックした後、設定するユーザアカウントを開く。

ステップ 2 ユーザの電子メールアドレスに**メール ID** が含まれていることを確認します。

- (注) SRV レコードではなく [サーバ情報 (Server Information)] を設定に使用している場合は、ユーザの Webex アプリ 電子メールアドレスが Unified CM 電子メールアドレスと一致する必要があります。少なくとも、ドメインの前のユーザ ID 部分が一致しなければなりません。

ステップ 3 ユーザの [サービス設定 (Service Settings)] で、[ホームクラスタ (Home Cluster)] チェックボックスをオンにします。

各ユーザがホームとしている Cisco Unified Communications Manager にこの設定を設定し、デバイスが登録されている場所を指定します。

ステップ 4 (任意) ユーザ レベルのオーバーライドが必要な場合は、[UC サービスプロファイル] ドロップダウンリストから、(CTI サービスとボイスメールを使用して) 作成したサービス プロファイルを選択します。

ステップ 5 変更を保存してから、該当するロールをユーザに割り当てます。

ステップ 6 [アクセス コントロール グループに追加 (Add to Access Control Group)] をクリックします。

ステップ 7 エンドユーザに割り当てる各アクセス制御グループの対応するチェックボックスをクリックする。

ユーザを、少なくとも次のアクセス コントロール グループに割り当てる必要があります。

- **標準 CCM エンド ユーザ**
- **STANDARD CTI Enabled:** このオプションは、デスクフォン制御に使用されます。

電話機のモデルによっては、次のコントロール グループが追加が必要となります。

- Cisco Unified IP Phone 9900、8900、8800 Series、または DX Series では、[標準 CTI による接続時の転送 および会議をサポートする電話の制御 (Standard CTI Allow Control of Phones supporting Connected Xfer and conf)] を選択します。
- Cisco Unified IP Phone 6900 Series では、[標準 CTI によるロールオーバー モードをサポートする電話の制御 (Standard CTI Allow Control of Phones supporting Rollover Mode)] を選択します。

次のタスク

ユーザをデバイスに関連付ける。

ソフトフォンワークフローの作成

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかのオプションを使用して、ユーザーのソフトフォンを作成します。 <ul style="list-style-type: none"> • Control Hub through Cloud Connected UC (CCUC) —デバイスの自動プロビジョニング。 	ヒント Control Hub の自動プロビジョニング機能を使用することをお勧めします。この機能により、ユーザーはゼロまたは最小限の介入で、Calling in Webex (Unified CM) 用デバイスを自分でプロビジョニングできます。この機能により、Unified CM での複数のデバイスのオーバープロビジョニングが回避され、クラスタの拡張とライセンスの使用への影響を最小限に抑えることができます。Calling in Webex (Unified CM) にプロビジョニングされたユーザーが、登録済み E メールアドレスかユーザー ID で Webex アプリにサインインすると、デバイスが自動で作成されます。

	コマンドまたはアクション	目的
	<p>(注) このプロセスでは、ユーザーのデバイスを自動作成し、ユーザーを電話サービスに接続するまでに最大5分かかる場合があります。ユーザーが自動プロビジョニングをサポートしていないバージョンのアプリを使用していた場合、アプリをアップグレードするために再起動する必要があります。その後、指定された時間枠でソフトフォンデバイスが自動作成されます。</p> <p>• Unified CM—Webex アプリ ソフトフォンデバイスの作成と構成 (100 ページ)</p>	<p>ソフトフォンモードで Webex アプリ を使用するユーザーごとに、少なくとも 1 つのデバイスを作成します。</p> <p>適切なデバイスタイプのデスクトップ、モバイル、タブレットなど、ユーザが使用している任意のサポート対象の Webex アプリ プラットフォーム用に、1 つのソフトフォンデバイスを追加できます。</p>
ステップ 2	デバイスにディレクトリ番号を追加する (103 ページ)	作成する各デバイスに対して、電話番号を追加します。
ステップ 3	ユーザーとデバイスの関連付け (104 ページ)	ユーザとデバイスを関連付けます。
ステップ 4	暗号化された通話用の電話機セキュリティプロファイルを構成 (105 ページ)	この作業は、すべてのデバイスと Webex アプリ でセキュアな電話機能をセットアップするために実行します。

Webex アプリ ソフトフォンデバイスの作成と構成

Webex アプリ をソフトフォンクライアントにするには、Webex アプリでのコール (Unified CM) 用に設定している各ユーザーに 1 つ以上のデバイスを作成します。デスクトップおよびモバイル用の Webex アプリ は、Cisco Jabber と同じデバイスタイプを使用して Unified CM に登録します。



(注) ユーザにデスクフォン制御だけを提供してソフトフォン機能を提供しない場合は、そのユーザにデスクトップ CSF デバイスを作成する必要はありません。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスにログインします。

ステップ 2 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

[電話の検索/一覧表示 (Find and List Phones)] ウィンドウが開きます。

ステップ 3 [新規追加] を選択します。

ステップ 4 [電話のタイプ (Phone Type)] ドロップダウンリストで、設定しているデバイス タイプに適したオプションを選択してから、[次へ (Next)] を選択します。

Webex アプリ ユーザの場合、ユーザごとに複数のデバイスを作成できますが、ユーザごとに作成できるデバイスのタイプは1つだけです。たとえば、1つのデュアルモードモバイルデバイスと1つのCSF デバイスを作成できますが、2つのCSF デバイスを作成することはできません。

- [Cisco Unified Client Services Framework] : Mac 用 Webex アプリ または Windows 用 Webex アプリ の CSF デバイスを作成するには、このオプションを選択します。
- [Cisco Dual Mode for iPhone] : iPhone 用 Webex アプリ ユーザに TCT デバイスを作成するには、このオプションを選択します。
- **Cisco Jabber for Tablet**— iPad、Android タブレットまたは Google Chromebook で Webex アプリ 用 TAB デバイスを作成するには、このオプションを選択します。Android の場合、Webex アプリ は、600 密度非依存ピクセル (dp) 以上のディスプレイを備えたデバイスをタブレットとして識別します。
- **Cisco Dual Mode for Android** : Android 機ユーザ向けの Webex アプリ の BOT デバイスを作成するには、このオプションを選択します。Webex アプリ は、タブレットとして 600dp 以上のディスプレイを持つデバイスを識別します。

(注) Webex アプリ が Android デバイスを識別する方法の詳細については、「[Android デバイスと密度に依存しないピクセル \(103 ページ\)](#)」を参照してください。

Windows デバイスの場合は Webex アプリ iPhone の場合は Webex アプリ など、プラットフォームごとに1つのデバイスタイプで電話サービスにサインインできます。ユーザーは、同じプラットフォーム上の1つ以上のデバイスタイプの電話サービスにはサインインできません (例: iPad 用 Webex アプリ や Android タブレット用 Webex アプリ)。

(注) Chromebook ユーザは Webex アプリでのコール (Unified CM) を使用するために TAB デバイスが必要ですが、電話サービスは Chromebook と Android 機に同時にサインインしているユーザに対して機能します。

ステップ 5 [オーナーのユーザ ID (Owner User ID)] ドロップダウンリストで、デバイスを作成するユーザを選択します。

ステップ 6 [デバイス名 (Device Name)] フィールドで、適切な形式を使用してデバイスの名前を指定します。

次を選択する場合:	必要なフォーマット
Cisco Unified Client Services Framework	<ul style="list-style-type: none"> • 有効な文字: a~z、A~Z、0~9。 • 15文字の制限。
Cisco Dual Mode for iPhone	<ul style="list-style-type: none"> • デバイス名は、Tctで始まる必要があります。 たとえば、ユーザ名が tadams であるユーザ Tanya Adams の TCT デバイスを作成する場合は、「TCTTADAMS」と入力します。 • すべて大文字でなければなりません。 • 有効な文字: A~Z、0~9、ピリオド(.)、アンダースコア(_)、ハイフン(-)。 • 文字数の上限は 15 文字です。

次を選択する場合:	必要なフォーマット
Cisco Jabber for Tablet	<ul style="list-style-type: none"> • デバイス名は、TABで始める必要があります。 たとえば、ユーザ名が tadams であるユーザ Tanya Adams の TAB デバイスを作成する場合は、「TABTADAMS」と入力します。 • すべて大文字でなければなりません。 • 有効な文字: A~Z、0~9、ピリオド(.)、アンダースコア(_)、ハイフン(-)。 • 文字数の上限は 15 文字です。 • Android の場合、Webex アプリ は、600 密度非依存ピクセル (dp) 以上のディスプレイを備えたデバイスをタブレットとして識別します。詳細については、Android デバイスと密度に依存しないピクセル (103 ページ) を参照してください。
Cisco Dual Mode for Android	<ul style="list-style-type: none"> • デバイス名はボットで始まる必要があります。 たとえば、ユーザ名が tadams であるユーザ Tanya Adams の BOT デバイスを作成する場合は、「BOTTADAMS」と入力します。 • すべて大文字でなければなりません。 • 有効な文字: A~Z、0~9、ピリオド(.)、アンダースコア(_)、ハイフン(-)。 • 文字数の上限は 15 文字です。 • Android の場合、Webex アプリ は、600 密度非依存ピクセル (dp) 未満のディスプレイを備えたデバイスを電話機として識別します。詳細については、Android デバイスと密度に依存しないピクセル (103 ページ) を参照してください。

(注) Webex アプリ ユーザが企業のネットワークの外部に接続する必要がある場合は、Expressway にモバイルおよびリモートアクセス (MRA) を展開する必要があります。

ステップ 7 モバイルデバイス (TCT、BOT、および TAB) の場合、ユーザのモバイルプロバイダー経由で緊急コールをルーティングするには、[プロダクト固有の設定 (Product Specific Configuration Layout)] セクションの [緊急電話番号 (Emergency Numbers)] に、指定の緊急電話番号を入力します。

ユーザが直接ダイヤルできる追加の緊急電話番号を、コンマ区切りのリストにして入力できます。これらの番号には数字だけで構成されている必要があります。スペース、ダッシュ、その他の文字は使用できません。

デバイスに定義された緊急電話番号は常に、エンタープライズ環境ではなくモバイルネットワークを使用して直接ダイヤルされます。緊急電話番号が場所によって異なる場合、または組織が専用のセキュリティ番号を使用している場合、モバイルネットワークプロバイダーの国の外へ頻繁に出張するユーザには、直通ダイヤル番号を使用してください。

ステップ 8 [保存] を選択します。

ステップ 9 [設定の適用 (Apply Config)] をクリックします。

次のタスク

1つ以上のディレクトリ番号 (回線) をソフトフォンデバイスに追加します。

Android デバイスと密度に依存しないピクセル

Webex アプリは、密度非依存ピクセル (dp) を使用して Android デバイスを識別します。dp は画面サイズの長さの単位で、通常、モバイルソフトウェアでアプリの表示をさまざまな画面サイズに拡大縮小するために使用されます。ディスプレイが 600dp 以上のデバイスはタブレットとして識別されます。600dp 未満の場合は、電話機として認識されます。

- **タブレット (600dp 以上)** — デバイスにタブレット UI が表示され (左右のレイアウト、右側のパネルにスペースチャットコンテンツまたはプロファイルの詳細ページが表示されます)、Unified CM で TAB ソフトフォンデバイスタイプを選択します。
- **電話機 (600 dp 未満)** — デバイスには電話 UI (垂直レイアウト) が表示され、Unified CM で BOT ソフトフォンデバイスタイプを選択します。

詳細については、「[Android デベロッパー資料](#)」を参照してください。

デバイスにディレクトリ番号を追加する

各デバイスを作成して設定したら、そのデバイスに電話番号を追加する必要があります。ここでは、[デバイス (Device)] > [電話機 (Phone)] メニュー オプションを使用して、電話番号を追加する手順について説明します。

始める前に

デバイスを作成します。

ステップ 1 [電話の設定 (Phone Configuration)] ウィンドウの [割り当て情報 (Association Information)] セクションに移動します。

ステップ 2 [新規DNを追加 (Add a new DN)] をクリックします。

ステップ 3 [電話番号 (Directory Number)] フィールドで、電話番号を指定します。

ステップ 4 [回線に関連付けられているユーザ (Users Associated with Line)] セクションで、[エンドユーザの関連付け (Associate End Users)] をクリックします。

- ステップ 5** [ユーザの検索 (Find User where)] フィールドで、適切なフィルタを指定してから、[検索 (Find)] をクリックします。
- ステップ 6** 表示されたリストから、該当するユーザを選択して、[選択項目の追加 (Add Selected)] をクリックします。
- ステップ 7** その他に必要な設定があれば、それらをすべて指定します。
- ステップ 8** [設定の適用 (Apply Config)] を選択します。
- ステップ 9** [保存 (Save)] を選択します。

ユーザーとデバイスの関連付け

始める前に



(注) ユーザごとに別々のサービスプロファイルを使用する場合は、Webex アプリ のソフトフォンデバイスを複数のユーザに関連付けしないでください。

- ステップ 1** ユーザとデバイスを関連付けます。
- [Unified CM の管理 (Unified CM Administration)] インターフェイスを開きます。
 - [ユーザ管理 (User Management)] > [エンド ユーザ (End User)] を選択します。
 - 適切なユーザを探して選択します。
[エンド ユーザの設定 (End User Configuration)] ウィンドウが表示されます。
 - [デバイス情報 (Device Information)] セクションで [デバイスの割り当て (Device Association)] を選択します。
 - 必要に応じて、ユーザとデバイスを関連付けます。
 - [エンド ユーザの設定 (End User Configuration)] ウィンドウに戻り、[保存 (Save)] を選択します。
- ステップ 2** デバイス構成で [ユーザのオーナー ID (User Owner ID)] フィールドを設定します。
- [デバイス (Device)] > [電話 (Phone)] の順に選択します。
 - 適切なデバイスを探して選択します。
[電話の設定 (Phone Configuration)] ウィンドウが開きます。
 - [デバイス情報 (Device Information)] セクションを探します。
 - [ユーザ (User)] を [オーナー (Owner)] フィールドの値として選択します。
 - [オーナーのユーザ ID (Owner User ID)] フィールドから適切なユーザ ID を選択します。
 - [保存 (Save)] を選択します。

暗号化された通話用の電話機セキュリティプロファイルを構成

任意で、すべてのデバイスと Webex アプリ インスタンス用に電話機能を設定できます。セキュアな電話機能では、セキュアな SIP シグナリングおよびセキュア メディア ストリームが提供されます。

ユーザのセキュアな電話機能を有効にした場合は、Cisco Unified Communications Manager へのデバイス接続がセキュアになります。ただし、他のデバイスとのコールは、両方のデバイスがセキュアな接続を備えている場合にのみセキュアになります。セキュアコールサポートには、ユニファイド CM 12.5 以降が必要です。

始める前に

- Unified CM リリース 12.5 以降を使用する必要があります。また、Webex アプリ でサポートされるのは SIP OAuth だけです。CAPF はサポートされていません。詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> にある *Feature Configuration Guide for Cisco Unified Communications Manager* の SIP OAuth に関する章を参照してください。
- 電話会議の場合は、会議ブリッジがセキュアな電話機能をサポートしていることを確認します。会議ブリッジがセキュアな電話機能をサポートしていない場合、そのブリッジへのコールは安全ではありません。同様に、クライアントが電話会議でメディアを暗号化できるようにするために、すべての参加者が共通の暗号化アルゴリズムをサポートする必要があります。

ステップ 1 Cisco Unified Communications Manager で、[システム (System)] > [セキュリティ (Security)] > [電話セキュリティプロファイル (Phone Security Profile)] の順に選択します。

ステップ 2 [新規追加] を選択します。

ステップ 3 [電話のタイプ (Phone Type)] ドロップダウン リストで、設定しているデバイス タイプに適したオプションを選択してから、[次へ (Next)] を選択します。

- [Cisco Unified Client Services Framework] : Mac または Windows 用の Webex アプリ の CSF デバイスを作成するには、このオプションを選択します。
- [Cisco Dual Mode for iPhone] : このオプションは、iPhone 用の TFT デバイスを作成する場合に選択します。
- [Cisco Jabber for Tablet] : このオプションは、iPad または Android タブレット用の TAB デバイスを作成する場合に選択します。
- [Cisco Dual Mode for Android] : このオプションは、Android デバイス用の BOT デバイスを作成する場合に選択します。
- [CTI リモートデバイス (CTI Remote Device)] : このオプションは、CTI リモート デバイスを作成する場合に選択します。

CTI リモート デバイスは、ユーザのリモート接続先をモニタリングし、通話を制御する仮想デバイスです。

ステップ 4 [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] ウィンドウの [名前 (Name)] フィールドで、電話セキュリティプロファイルの名前を指定します。


ステップ 5 **Device Security Mode** (デバイスセキュリティモード) の場合に、**Encrypted** (暗号化) を選択する。

SIP接続は、AES 128 / SHA暗号化を使用したTLS経由である。クライアントは、Secure Real-time Transport Protocol (SRTP) を使用して、暗号化されたメディア ストリームを提供します。

ステップ 6 **Enable Oath Authentication** をチェックする。

ステップ 7 [Save (保存)] をクリックします。

次のタスク

Windows または Mac 用の Webex アプリ を使用してコールを発信し、セキュアコールの設定を確認できます。通話中に、通話ウィンドウの右上に錠前のアイコン  が表示されるので、通話が安全であることがわかります。

プッシュ通知の構成と推奨設定

プッシュ通知に対応する展開では、Google または Apple のクラウドベースのプッシュ通知サービスを使用して、バックグラウンドで動作している iOS および Android 用 Cisco Webex アプリクライアントに音声通話、ビデオ通話、インスタントメッセージの通知をプッシュします。

コール環境でボイス環境とシングルナンバーリーチ (SNR) を使用している場合は、タイマーを変更して設定全体を最適化することを推奨します。

始める前に

Unified CM と Expressway が、プッシュ通知でサポートされる最小バージョンを満たしていることを確認してください。 [呼制御環境の要件 \(57 ページ\)](#) を参照してください。

ステップ 1 Cisco Unified CM の管理から、[**詳細機能 (Advanced Features)**] > [**シスコクラウドオンボーディング (Cisco Cloud Onboarding)**] に移動します。

ステップ 2 [プッシュ通知を有効化 (Enable Push Notifications)] をオンにします。

詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/push_notifications/cucm_b_push-notifications-deployment-guide.html にある『プッシュ通知導入ガイド』を参照してください。

ステップ 3 ボイスメールが設定されている場合は、[**コールルーティング (Call Routing)**] > [**ボイスメール (Voicemail)**] に移動して、[無応答時の呼び出し時間 (秒) (No Answer Ring Duration (seconds))] を 25 秒以上に変更することを推奨します。

ボイスメールサーバが設定されている場合、無応答時にボイスメールに転送するまでのタイマーは 12 秒です。プッシュ通知は約 8 秒で送信されるため、この時間値を変更しないと、通知後の呼び出しは 4 秒しか行われないうこととなります。

ステップ 4 SNR が設定されている場合は、[デバイス (Device)] > [リモート接続先 (Remote Destination)] に移動し、任意のエントリを開いて、[ビジネス回線にダイヤルされたときに、X秒経過してからこの電話の呼出音を鳴らす (Wait seconds before ringing this phone when my business line is dialed)] を **13** 秒以上に変更することを推奨します。

着信通知を受信したとき、Webex アプリ では、この待ち時間がタイムアウトする前にすばやく Unified CM に登録しなければなりません。タイムアウトすると、Webex アプリ ではなく電話機自体の呼出音が鳴ります。

クライアント構成パラメータの設定 (リリース 12.5 以降)

クライアントの設定パラメータを設定し、Unified CM でサービス プロファイルに割り当てます。

始める前に

サポートされている機能について、必要な Unified CM 設定が適切であることを確認する必要があります。手順については、次のマニュアルを参照してください。

- **ハントグループ**については『Cisco Unified Communications Manager のシステム構成ガイド』を参照してください。
- **コールピックアップ**については『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。

ステップ 1 設定パラメータの定義 (107 ページ)

ユニファイド CM を使用すると、クライアントの設定を含む UC サービスに関する情報の追加、検索、表示、および保守を行うことができます。

ステップ 2 サービスプロファイルへのクライアント設定の割り当て (108 ページ)

ユニファイド CM を使用すると、サービスプロファイルを使用してクライアント設定をユーザに割り当てることができます。

設定パラメータの定義

Unified CM (リリース 12.5 以降) では、Webex アプリ クライアント設定など、jabber-config.xml ファイルで提供される UC サービスに関する情報を追加、検索、表示、および保守できます。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

サービスプロファイルへのクライアント設定の割り当て

ステップ2 [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。

ステップ3 次のいずれかを選択します。

- 新しい設定の場合は、[新規追加 (Add New)] を選択し、[UCサービスタイプ (UC Service Type)] として [Jabberクライアント設定 (Jabber Client Configuration (jabber-config.xml))] を選択します。
- 既存の設定の場合は、[UCサービスタイプ (UC Service Type)] を [Jabberクライアント設定 (Jabber Client Configuration (jabber-config.xml))] として設定した UC サービスを選択します。

ステップ4 [Next] を選択します。

ステップ5 [UC サービス情報(UC Service Information)] セクションで名前を入力します。詳細な要件については、Unified CM ヘルプを参照してください。

ステップ6 [Jabber設定パラメータ (Jabber Configuration Parameters)] セクションにパラメータを入力します。詳細については、[ポリシーパラメータ \(135 ページ\)](#) を参照してください。

ステップ7 [保存 (Save)] を選択します。

サービスプロファイルへのクライアント設定の割り当て

ユニファイドCMを使用すると、サービスプロファイルを使用してクライアント設定をユーザに割り当てることができます。

ステップ1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ2 [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービス プロファイル (Service Profile)] の順に選択します。

ステップ3 [新規追加 (Add New)] を選択するか、または Webex アプリ クライアントの設定を割り当てる既存のサービスプロファイルを選択します。

ステップ4 [Jabberクライアント設定 (jabber-config)] セクションで、プロファイルに適用する設定の名前を選択します。

ステップ5 [保存 (Save)] を選択します。

クライアント構成ファイルの作成とホスト (12.5 以前のリリース)

クライアント設定ファイルを作成して、それらを Cisco Unified Communications Manager TFTP サービス上でホストします。

始める前に

設定ファイルがサポートする機能について、必要な Unified CM の設定が適切であることを確認する必要があります。手順については、次のマニュアルを参照してください。

- **ハントグループ**については『Cisco Unified Communications Manager のシステム構成ガイド』を参照してください。
- **コールピックアップ**については『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	XML 構成ファイルの要件 (109 ページ)	XML 設定ファイルの適切な形式とその他の要件を理解します。
ステップ 2	ポリシーパラメータ (135 ページ)	ユーザに対して特定の機能を有効にするために使用できるポリシーパラメータの表を参照します。
ステップ 3	共通構成の作成 (110 ページ)	展開でユーザ用のクライアントを設定します。
ステップ 4	グループ構成の作成 (111 ページ)	ユーザのセットごとに異なる設定を適用します。
ステップ 5	構成ファイルのホスト (112 ページ)	TFTP サーバ上でコンフィギュレーション ファイルをホストします。
ステップ 6	TFTP サーバの再起動 (112 ページ)	TFTP サーバを再起動して、クライアントが設定ファイルにアクセスできるようにします。

XML 構成ファイルの要件

次の設定ファイル要件に注意してください。

- 設定ファイル名は、大文字と小文字を区別します。エラーを回避し、クライアントが TFTP サーバからファイルを取得できるよう、ファイル名には小文字を使用してください。
- 設定ファイルには、utf-8 エンコーディングを使用してください。
- クライアントは、有効な XML 構造のない設定ファイルは読み込めません。設定ファイルの構造で終了要素をチェックし、その要素が正しくネストされていることを確認します。
- 設定ファイルでは、有効な XML 文字エンティティ参照のみが許可されます。たとえば、& を & の代わりに使用します。XML に無効な文字が含まれている場合は、クライアントは設定ファイルを解析できません。

設定ファイルを検証するには、Microsoft Internet Explorer でそのファイルを開きます。

- Internet Explorer に XML 構造全体が表示された場合、設定ファイルは有効です。

- Internet Explorer に XML 構造の一部しか表示されない場合は、設定ファイルに無効な文字またはエンティティが含まれている可能性があります。

共通構成の作成

Webex アプリでのコール (Unified CM) は、既存の Jabber のコンフィギュレーション XML ファイルの機能を利用します。このファイルを使用して、組織内の Webex アプリ ユーザに対して特定のコール機能 (ハントグループとコールピックアップ) を有効にすることができます。

始める前に

過去に Jabber を既に展開している場合は、jabber-config.xml ファイルがユニファイド CM TFTP サーバ上に存在することになります。ブラウザで

`http://tftp_server_address:6970/jabber-config.xml` を開くことで (`tftp_server_address` がパブリッシャのサーバ FQDN または IP アドレスになっている)、ファイルがダウンロードされたかどうかを確認できます。

必要なポリシーパラメータがすでに指定されている場合は、設定ファイルでこれ以上の操作を行う必要はありません。



- (注) Webex アプリ と Jabber は、同じ jabber-config.xml ファイルを共有します。このガイドで説明しているように、Webex アプリ では、ファイル内の Jabber パラメータのサブセットだけが使用されます。

ステップ 1 任意のテキスト エディタを使用して jabber-config.xml という名前のファイルを作成するか、ダウンロードしたファイルを開きます。

- ファイル名には小文字を使用してください。
- UTF-8 エンコーディングを使用してください。

(注) Unified CM 12.5 以降では、管理インターフェイスでこのファイルを作成できます。

ステップ 2 <policies></policies> にある jabber-config.xml に必要な設定パラメータを定義します。

- コール ピックアップの場合 :

```
<EnableCallPickup>true</EnableCallPickup>
<EnableGroupCallPickup>true</EnableGroupCallPickup>
<EnableOtherGroupPickup>true</EnableOtherGroupPickup>
```

- ハント グループの場合 :

```
<EnableHuntGroup>true</enableHuntGroup>
```

ハントグループの着信コールに対する拒否ボタンを非表示にするには、次のように記述します。

```
<PreventDeclineOnHuntCall>true</PreventDeclineOnHuntCall>
```

グループ構成の作成

グループ構成ファイルは、ユーザのサブセットに適用され、デスクトップ (CSF デバイス) の場合は、Webex アプリ で、モバイルデバイスの場合は、Webex アプリ でサポートされます。グループ設定ファイルは、グローバル設定ファイルよりも優先されます。

CSF デバイスでユーザをプロビジョニングする場合は、デバイス設定の[シスコ サポート フィールド (Cisco Support Field)] フィールドでグループの設定ファイル名を指定します。ユーザが CSF デバイスを所有していない場合は、インストール中に TFTP_FILE_NAME 引数を使用してグループごとに一意の設定ファイル名を設定します。

始める前に

設定ファイルの構造が有効でない場合、クライアントは設定した値を読み取ることができません。詳細については、この章の XML サンプルを確認してください。

ステップ 1 任意のテキスト エディタを使用して XML グループ設定ファイルを作成します。

グループ設定ファイルには、適切な名前を指定できます (例: webexteams-groupa-config.xml)。

ステップ 2 グループ設定ファイルで必須の設定パラメータを定義します。

ステップ 3 該当する CSF デバイスにグループの設定ファイルを追加します。

- a) Cisco ユニファイド CM 管理インターフェイスを開き、[デバイス (Device)] > [電話 (Phone)] を選択します。
- b) グループ設定ファイルを適用する適切な CSF デバイスを検索して選択します。
- c) [電話の設定 (Phone Configuration)] ウィンドウで、[プロダクト固有の設定レイアウト (Product Specific Configuration Layout)] > [デスクトップクライアント設定 (Desktop Client Settings)] に移動します。
- d) [シスコサポートフィールド (Cisco Support Field)] フィールドに、
configurationfile=group_configuration_file_name.xml と入力します。たとえば、
configurationfile=webexteams-groupa-config.xml と入力します。

TFTP サーバ上でデフォルト ディレクトリ以外の場所にあるグループ設定ファイルをホストする場合は、パスとファイル名を指定する必要があります (例:

configurationfile=/customFolder/webexteams-groupa-config.xml)。複数のグループの設定ファイルを追加しないでください。クライアントは [シスコ サポート フィールド (Cisco Support Field)] フィールドの最初のグループ設定のみを使用します。

- e) [Save (保存)] をクリックします。

ステップ 4 TFTP サーバ上でグループ設定ファイルをホストします。

構成ファイルのホスト

デバイス設定ファイルが存在する Cisco Unified Communications Manager TFTP サーバで設定ファイルをホストすることをお勧めします。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified OS の管理から、ソフトウェア アップグレード (Software Upgrades) > TFTP ファイル マネジメント (TFTP File Management) に移動して、[ファイルのアップロード (Upload file)] をクリックします。	環境内に複数の TFTP サーバが存在する場合は、すべての TFTP サーバの設定ファイルが同じであることを確認します。
ステップ 2	[参照 (Browse)] をクリックして、ローカルシステムから jabber-config.xml ファイルを選択し、[ディレクトリ (directory)] フィールドを空白のままにして、[ファイルのアップロード (Upload file)] をクリックします。	設定ファイルが TFTP サーバのデフォルトディレクトリに格納されるように、[ディレクトリ (Directory)] テキスト ボックスの値は空のままにします。

TFTP サーバーの再起動

クライアントが設定ファイルにアクセスできるようにするには、その前に TFTP サーバを再起動する必要があります。

- ステップ 1 右上のドロップダウンから、[Cisco ユニファイドサービスアビリティ (Cisco Unified Serviceability)] をクリックしてログインします。
- ステップ 2 [ツール (Tools)] > [コントロールセンター：機能サービス (Control Center - Feature Services)] の順にクリックして、[サーバ (Server)] から Unified CM Publisher を選択します。
- ステップ 3 [移動 (Go)] をクリックして、[CM サービス (CM Services)] にスクロールし、[Cisco Tftp] をクリックします。
- ステップ 4 一番上までスクロールし、[再起動 (Restart)] をクリックして、[OK] をクリックします。

サービスが正常に再起動したことを示すメッセージが表示されます。

環境内に複数の TFTP サーバが存在する場合は、すべての TFTP サーバの設定ファイルが同じであることを確認します。

次のタスク

設定ファイルが TFTP サーバで使用できることを確認するには、任意のブラウザで設定ファイルを開きます。通常、http://tftp_server_address:6970/jabber-config.xml の URL にあるグローバル設定ファイルにアクセスできます。

共通構成の作成

Webex アプリでのコール (Unified CM) は、既存の Jabber のコンフィギュレーション XML ファイルの機能を利用します。このファイルを使用して、組織内の Webex アプリ ユーザに対して特定のコール機能 (ハントグループとコールピックアップ) を有効にすることができます。

始める前に

過去に Jabber を既に展開している場合は、jabber-config.xml ファイルがユニファイド CM TFTP サーバ上に存在することになります。ブラウザで

`http://tftp_server_address:6970/jabber-config.xml` を開くことで (`tftp_server_address` がパブリッシャのサーバ FQDN または IP アドレスになっている)、ファイルがダウンロードされたかどうかを確認できます。

必要なポリシーパラメータがすでに指定されている場合は、設定ファイルでこれ以上の操作を行う必要はありません。



(注) Webex アプリ と Jabber は、同じ jabber-config.xml ファイルを共有します。このガイドで説明しているように、Webex アプリ では、ファイル内の Jabber パラメータのサブセットだけが使用されます。

ステップ 1 任意のテキスト エディタを使用して jabber-config.xml という名前のファイルを作成するか、ダウンロードしたファイルを開きます。

- ファイル名には小文字を使用してください。
- UTF-8 エンコーディングを使用してください。

(注) Unified CM 12.5 以降では、管理インターフェイスでこのファイルを作成できます。

ステップ 2 `<policies></policies>` にある jabber-config.xml に必要な設定パラメータを定義します。

- コール ピックアップの場合 :

```
<EnableCallPickup>true</EnableCallPickup>  
<EnableGroupCallPickup>true</EnableGroupCallPickup>  
<EnableOtherGroupPickup>true</EnableOtherGroupPickup>
```

- ハント グループの場合 :

```
<EnableHuntGroup>true</enableHuntGroup>
```

ハントグループの着信コールに対する拒否ボタンを非表示にするには、次のように記述します。

```
<PreventDeclineOnHuntCall>true</PreventDeclineOnHuntCall>
```

構成ファイルの要件

- 設定ファイル名は、大文字と小文字を区別します。エラーを回避し、クライアントが TFTP サーバからファイルを取得できるよう、ファイル名には小文字を使用してください。
- 設定ファイルには、utf-8 エンコーディングを使用する必要があります。
- クライアントは、有効な XML 構造のない設定ファイルは読み込めません。設定ファイルの構造で終了要素をチェックし、要素が正しく入れ子になっていることを確認します。
- XML には、有効な XML 文字エンティティ参照しか含めることができません。たとえば、& を & の代わりに使用します。XML に無効な文字が含まれている場合は、クライアントは設定ファイルを解析できません。



ヒント Microsoft Internet Explorer で設定ファイルを開き、無効な文字やエンティティがないことを確認します。

Internet Explorer に XML 構造の全体が表示される場合は、設定ファイルには無効な文字やエンティティは含まれていません。

Internet Explorer に XML 構造の一部しか表示されない場合は、設定ファイルには無効な文字やエンティティが含まれている可能性があります。

通話を会議に移動する構成

通話中のユーザは、高度な会議機能を利用しながら、他の同僚を会議に招待できます。ユーザは、そのコールを会議に移動できます。そこから、何か重要なことを共有したいときに手を挙げたり、誰かの発言に対して視覚的に同意を示すために絵文字を追加したり、ブレイクアートルームを使用することができます。

この機能には、次の手順で示す特定の Unified CM、Expressway および Webex アプリ サイト構成が必要です。

始める前に



(注) 会議へのコールの移動は、次の Webex Meetings サイトの構成では機能しません。

- 暗号化はエンドツーエンドまたは PKI に設定されます。
- テレフォニーは無効になります。
- ビデオメッシュが展開され、メディアの暗号化が有効になります。
- サイトはスローリリースチャンネルにあります。詳細については、「[ソフトウェア リリース チャンネルの管理](#)」を参照してください。

ステップ 1 Unified CM で SIP URI ダイアルを構成します。

のリリースに関する詳細は、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>にある『システム設定ガイド』の「URIダイアルの構成」を参照してください。『システム設定ガイド』の「URIダイアルの構成」を参照してください。

Unified CM で SIP ルートパターンを構成し、example.webex.com などの Webex アプリ サイトにコールをルーティングします。

ステップ 2 パーティションとコーリングサーチスペース (CSS) を構成したら、CCS を再ルーティング コーリングサーチスペース (CSS) として設定します。これにより、パーティションが評価され、再ルート接続先が許可されているかどうかを確認します。

この構成は、コールを行った後、リモート参加者を会議に参加させるユーザに必要です。

- パーティションと CCS の手順に関しては、[このドキュメント](#)を参照してください。
- ソフトフォンデバイスを使用するユーザの再ルート CSS の場合は、[デバイス (Device)] > [電話 (Phone)] の順に選択し、csf<userid> など修正するデバイスを検索します。次に、[再ルーティング コーリング検索スペース (Rerouting Calling Search Space)] 設定で作成した CSS を選択し、変更を保存します。

再ルート CSS を使用すると、ユーザは別のパスに沿ってコールを転送し、コールを会議に移動できます。再ルート CSS は、最初の手順で構成した SIP ルートパターンにアクセスできる必要があります。

ステップ 3 Expressway ペアを構成して、Unified CM から Webex アプリ にコールをルーティングします。

詳細については、『[シスコ Expressway 管理者ガイド](#)』の「ゾーンおよびネイバー」を参照してください。

Expressway-C では、2つのネイバージーン (1つは Unified CM 用、もう1つは Webex アプリ に到達可能な Expressway-E 用) を構成します。

詳細に関しては、「[相互 TLS 認証用の Expressway の設定](#)」を参照してください。

ステップ 4 Webex Meetings サイトが最小 41.3 以降で、テレフォニーが有効になっていることを確認してください。

会議のバージョンを確認するには、「[Cisco Webex Control Hub の Webex サイトのバージョンを確認](#)」の手順に従います。

ステップ 5 通話をミーティングに移動するユーザに対しては、フル機能の会議エクスペリエンスを有効化できます。

- お客様に対しては、このエクスペリエンスは自動的に有効になります。問題が発生した場合は、パートナーまたは CSM に問い合わせ、指示に従ってください。
- エスカレーションされた会議に追加されるリモートユーザは、この機能は不要です。

ステップ 6 ユーザは、[次の手順](#)を使用してデフォルトの Webex アプリ サイトを設定する必要があります。

ステップ 7 jabber-config.xml file (12.5 以前の Unified CM) または Jabber クライアント構成プロファイル (Unified CM 12.5 以降) では、EnableMeetingPowerUp パラメータを [True] に設定します。

パラメータ構成に関しては、本章の関連セクションを参照してください。パラメータとその値の詳細については、「[ポリシーパラメータ \(135 ページ\)](#)」の付録を参照してください。

ユーザは、Webex アプリ の会議に対してコールを移動できるようになります。変更はすぐに有効になりますが、現在通話中のユーザは、次の通話まで会議に移動できません。

本機能の使用方法に関するエンドユーザ向け詳細については、「[通話をミーティングに移動する](#)」を参照してください。

ユーザーワークフロー用通話エクスペリエンス

これらタスクを使用すると、ログイン動作の設定 (例: オンネットと MRA) や通話動作などのユーザー向けの通話エクスペリエンスをさまざまな面でカスタマイズできます。



(注) 仮想バックグラウンド設定や通話オプションの優先付けなどの追加カスタム機能については、「[展開後に追加機能を構成する \(124 ページ\)](#)」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UC マネージャプロファイルの作成 (117 ページ)	UC マネージャプロファイルは、デフォルトで組織のドメインに設定されています。このため、ユーザが Webex アプリ の電話サービスにサインインするときに、手動でドメインを指定することが必要になる場合があります。デフォルトを上書きしてドメインを指定する場合は、組織全体またはユーザレベルのオーバーライドのための UC マネージャプロファイルを設定できます。別のドメインの Webex アプリ 電話サービスにユーザがサインインできるようにす

	コマンドまたはアクション	目的
		るには、組織のデフォルトオプションを選択するか、または新しいプロフィールを手動で作成します。
ステップ 2	UC マネージャプロフィールの編集 (130 ページ)	制御ハブの UC マネージャプロフィールはいつでも編集できます。
ステップ 3	Control Hub での通話動作と UC マネージャプロフィールの設定 (117 ページ)	UC マネージャプロフィールは、制御ハブ内の通話動作設定 (組織全体またはユーザーレベル) で関連付けられます。コールビヘイビアを設定する場合は、UC マネージャプロフィールのデフォルト オプションまたは手動オプションを選択することもできます。

UC マネージャプロフィールの作成

ステップ 1 <https://admin.webex.com> のお客様のビューで、[管理 (Management)] > [組織設定 (Organization Settings)] の順に選択し、[UC マネージャプロフィール (UC Manager Profiles)] の [プロフィールを追加 (Add Profile)] を選択します。

ステップ 2 プロファイル名を追加し、必要な設定を選択してから [保存 (Save)] を選択します。

SRV レコードはあっても、ログイン電子メールアドレスがサービス検出に使用されていない場合は、音声サービスドメインを入力します。これはモバイルリモートアクセス (MRA) にも必要です。Webex アプリアカウントのユーザ ID が Unified CM のユーザ ID と一致しない場合や、複数の Unified CM クラスタ展開で ILS が有効になっていない場合は、UDS サーバを入力することもできます。両方の値を入力した場合、Webex アプリは、まず UDS をオンプレミスに使用し、音声サービスを MRA に使用します。

Control Hub での通話動作と UC マネージャプロフィールの設定

コントロールハブを使用して、組織内の特定のユーザまたは組織全体に対する発信動作を設定できます。通話動作の場合、ユーザーに対してこの設定を構成することで、通話機能を使用できるようになります。Webex アプリはまず、クラウドサービスに接続し、その構成を取得します。これには、通話動作設定も含まれます。

デフォルトで、Webex アプリは、Webex 組織ドメイン (ユーザーの E メールドメイン) に基づき、DNS SRV クエリを送信します。Webex ドメインが既存の音声サービスドメインと一致しない場合、またはそれぞれに DNS SRV レコードがない複数のドメインがある場合、組織のデフォルトまたは UC Manager プロファイルに割り当てられたユーザに対して別のドメインを指定する場合に手動で構成した UC Manager プロファイルをオーバーライド設定として指定できます。

組織内のユーザに対しハイブリッドコールがまだ有効になっている場合、このオプションは使用できません。通話動作を割り当てる前に、ユーザーからハイブリッドコールを削除する必要があります。詳細については、「環境の準備」の章を参照してください。



Note 組織のニーズに応じてこの設定を構成することを推奨します (たとえば、組織内の特定のユーザを有効にして、サービスを試し、組織全体のサービスを設定する必要がある場合)。

詳細情報

ユーザーが Webex アプリから通話を発信したときに開く通話アプリケーションを制御します。クライアントの通話設定を構成できます。これには、Unified CM、Webex Calling、およびシスコからの有料通話サービスがないユーザーがいる組織の混合モード展開が含まれます。

ユーザーの通話ライセンスに応じて、通話動作のオプションを設定できます。

- Unified CM ライセンスが付与されているユーザーの場合、Cisco Jabber から直接、または Webex アプリを介して通話を発信するように設定し、ユーザーに適用されるドメイン (組織ドメインまたは UC Manager プロファイル) を選択できます。組織レベル、グループレベル、およびユーザーレベルで設定を構成できます。
- シスコの有料通話サービスを利用していないユーザーは、サードパーティアプリケーションを設定して通話を発信できます。デフォルトでは、Webex アプリを介したすべての通話は [Webex で通話 (Call on Webex)] オプションを使用します。組織レベルで設定を構成できます。
- Webex Calling のライセンスが付与されているユーザーの場合、Webex アプリが通話を行うためのデフォルトの通話アプリケーションになります。したがって、特定の通話動作の構成は必要ありません。

組織レベルで通話動作設定を有効化

組織レベルで構成された設定は、組織下のすべてのユーザーに自動的に適用されます。

ステップ 1 <https://admin.webex.com> で Control Hub にログインします。

ステップ 2 [サービス (Services)] > [Calling] > [クライアント設定 (Client Settings)] の順に選択します。

ステップ 3 [通話動作 (Calling Behavior)] セクションに移動し、Unified CM ユーザーおよびシスコからの有料通話サービスを持たないユーザー向けの通話動作オプションを設定します。

Unified CM ユーザーの場合

- [ユーザーの E メールドメインを使用する (Use the email domain of the user)] を選択して、組織のドメイン (デフォルトオプション) を Webex アプリのすべての Unified CM ユーザーに適用するか、[通話用 UC マネージャプロファイルを使用する (Use UC Manager Profile for calling)] を選択して、ドロップダウンリストで、作成した [UC マネージャプロファイル (UC Manager profile)] を選択します。

- 組織が通話に対して Jabber アプリを使用している場合は、**[Webex アプリから Cisco Jabber を開く (Open Cisco Jabber from the Webex app)]** チェックボックスをオンにします。Unified CM ユーザーは、Cisco Jabber で直接、または Webex を介して通話を発信できます。ユーザーが Webex アプリで電話をかけると、Cisco Jabber アプリが起動し、発信用に向けて使用します。

シスコからの有料通話サービスを利用していないユーザーの場合

- **[Webex からサードパーティアプリを開く (Open third-party app from Webex)]** チェックボックスをオンにすると、Webex での通話を有効にしていない場合でも、すべてのユーザーがサードパーティアプリを介して通話を発信できるようにします。ユーザーが Webex アプリで電話をかけると、サードパーティアプリが起動し、発信用に向けて使用します。

グループレベルで通話動作設定を有効化

Calling テンプレートを使用してユーザーグループの Unified CM 通話動作の組織設定を有効にできます。テンプレートを作成してユーザーグループに割り当てることができます。テンプレートの構成は、グループ内のすべてのユーザーに適用されます。

テンプレートを作成する

Before you begin

ユーザーに Unified CM ライセンスが付与されているかを確認してください。詳細については、「[各ユーザーのサービスライセンスの編集](#)」を参照してください。

ステップ 1 <https://admin.webex.com> で Control Hub にログインします。

ステップ 2 [サービス (Services)] > [Calling] > [クライアント設定 (Client Settings)] > [テンプレート (Templates)] の順に選択します。

ステップ 3 [テンプレートを作成 (Create template)] をクリックします。

ステップ 4 [全般 (General)] セクションで、テンプレート名と説明を入力します。

ステップ 5 [通話動作 (Calling behavior)] セクションで次の設定を更新します。

- **[ユーザーの E メールドメインを使用する (Use the email domain of the user)]** を選択して、組織のドメイン (デフォルトオプション) をユーザーグループに適用するか、**[通話用 UC マネージャプロフィールを使用する (Use UC Manager Profile for calling)]** を選択して、ドロップダウンリストで、作成した **[UC マネージャプロフィール (UC Manager profile)]** を選択します。
- **[Webex アプリから Cisco Jabber を開く (Open Cisco Jabber from the Webex app)]** チェックボックスをオンにすると、Unified CM ユーザーは、Cisco Jabber または Webex で直接発信できるようになります。ユーザーが Webex アプリで電話をかけると、Cisco Jabber アプリが起動し、発信用に向けて使用します。

ステップ 6 [テンプレートを作成して次へ (Create template and next)] をクリックします。

ステップ 7 検索ボックスでこのテンプレート用のグループを検索して選択します。

■ ユーザーグループに既存のテンプレートを適用する

ステップ 8 [完了 (Done)] をクリックします。

テンプレートを削除するには、テンプレートをクリックし、[アクション (Actions)] ドロップダウンリストで [削除 (Delete)] を選択します。[テンプレートを削除 (Delete template)] ページで、テンプレートを完全に削除することを通知するチェックボックスをオンにし、[削除 (Delete)] をクリックします。

テンプレートを変更するには、テンプレートを選択し、トグルを変更して、[保存 (Save)] をクリックします。

ユーザーグループに既存のテンプレートを適用する

Calling テンプレートの適用検討時の考慮事項

- ユーザーが組織に入ると、ユーザーは組織レベルからの設定を継承します。
- ユーザーがユーザーグループに追加された場合、Calling テンプレートの設定が適用されません。
- ユーザーが複数のユーザーグループに属している場合、最も高いランク (ランク 1) のテンプレートが最も優先され、そのテンプレート設定が適用されます。
- ユーザーに個別のユーザー設定がある場合、これらの設定はユーザーグループまたは組織レベルの設定よりも優先されます。

テンプレートの管理の詳細については、「[設定テンプレートの構成](#)」を参照してください。

既存のテンプレートは、[グループ (Group)] セクションまたは、[Calling] セクションから適用できます。

[グループ (Group)] セクションからテンプレートを適用する場合は、「[設定テンプレートの構成](#)」を参照してください。

[Calling] セクションから適用するには、次の手順を実行します。

ステップ 1 <https://admin.webex.com> のお客様ビューにある左側のナビゲーションバーで [サービス (Services)] を選択し、[Calling] > [クライアント設定 (Client Settings)] > [テンプレート (Templates)] の順に選択します。

ステップ 2 既存のテンプレートの横にある [...] アイコンをクリックし、[テンプレートの適用 (Apply template)] をクリックします。

ステップ 3 テンプレートを適用するグループ名を入力し、グループを選択します。

ステップ 4 [Done] をクリックします。

ユーザーレベルで通話動作組織設定をオーバーライド

Before you begin

ユーザーに Unified CM ライセンスが付与されているかを確認してください。詳細については、「[各ユーザーのサービスライセンスの編集](#)」を参照してください。

ステップ 1 <https://admin.webex.com> で Control Hub にログインします。

ステップ 2 [管理 (Management)] > [ユーザー (Users)] の順に選択し、変更するユーザーを選択します。

ステップ 3 [Calling] > [通話動作 (Calling Behavior)] の順に選択します。

ステップ 4 [組織レベルの設定を使用する (Use organization level settings)] のトグルを Off にし、ユーザー設定で組織のデフォルト設定をオーバーライドします。

組織のデフォルト設定に戻すには、[組織レベルの設定を使用する (Use organization level settings)] トグルをオンにします。

Note トグルは、ユーザーがグループにも属しておらず、組織レベルの設定をオーバーライドしたときのみ表示されます。

ステップ 5 次の通話動作設定を更新します。

- [ユーザーの E メールドメインを使用する (Use the email domain of the user)] を選択して、組織のドメイン (デフォルトオプション) をユーザーに適用するか、[通話用 UC マネージャプロファイルを使用する (Use UC Manager Profile for calling)] を選択して、ドロップダウンリストで、作成した [UC マネージャプロファイル (UC Manager profile)] を選択します。
- [Webex アプリから Cisco Jabber を開く (Open Cisco Jabber from the Webex app)] チェックボックスをオンにすると、Unified CM ユーザーは、Cisco Jabber または Webex で直接発信できるようになります。ユーザーが Webex アプリで電話をかけると、Cisco Jabber アプリが起動し、発信用に向けて使用します。

ステップ 6 [保存 (Save)] > [はい (Yes)] の順に選択します。

ユーザーレベルでの通話動作のグループレベル設定のオーバーライド

Before you begin

- ユーザーに Unified CM ライセンスが付与されているかを確認してください。詳細については、「[各ユーザーのサービスライセンスの編集](#)」を参照してください。
- ユーザーが、Calling テンプレートが割り当てられているユーザーグループの一部であることを確認してください。

ステップ 1 <https://admin.webex.com> で Control Hub にログインします。

ステップ2 [管理 (Management)] > [ユーザー (Users)] の順に選択し、変更するユーザーを選択します。

ステップ3 [Calling] > [通話動作 (Calling Behavior)] の順に選択します。

ステップ4 次の通話動作設定を更新します。

- [ユーザーの E メールドメインを使用する (Use the email domain of the user)] を選択して、組織のドメイン (デフォルトオプション) を適用するか、[通話用 UC マネージャプロファイルを使用する (Use UC Manager Profile for calling)] を選択して、ドロップダウンリストで、作成した [UC マネージャプロファイル (UC Manager profile)] を選択します。
- [Webex アプリから Cisco Jabber を開く (Open Cisco Jabber from the Webex app)] チェックボックスをオンにすると、Unified CM ユーザーは、Cisco Jabber または Webex で直接発信できるようになります。ユーザーが Webex アプリで電話をかけると、Cisco Jabber アプリが起動し、発信用に向けて使用します。

ステップ5 [保存 (Save)] をクリックし、[オーバーライド設定 (Override setting)] を確認します。

更新されたフィールドの横に、オーバーライドのマークが表示されます。グループテンプレート設定に戻るには、[アクション (Actions)] > [リセット (Reset)] の順に選択します。ユーザーが継承した Calling テンプレートの詳細を確認するには、[アクション (Actions)] > [継承の確認 (View inheritance)] の順に選択します。



Note [リセット (Reset)] オプションは、継承された設定がユーザーに対してオーバーライドされた場合にのみ使用できます。

手動接続設定

手動接続設定は、サービス ディスカバリが使用されていない場合にフォールバック メカニズムを提供します。

Webex アプリの起動時には、[電話サービス (Phone Services)] ウィンドウでオーセンティケータとサーバアドレスを指定できます。アプリは、以降の起動時に読み込まれるローカルアプリケーション設定にサーバアドレスをキャッシュします。アプリがサービスプロファイルからオーセンティケータおよびサーバアドレスを取得できない場合、Webex アプリは、最初の起動時にユーザに詳細設定を入力するように求めます。

Webex アプリでの電話サービスの認証

DNS SRV が実装されている場合は、Webex アプリの電話サービスでユーザーが自動検出され、SSOまたは手動のログイン情報を使用してサインインできます。導入されていない場合でも、UC マネージャプロファイルを設定すると、サインインプロセスを簡単にすることができます (このガイドですでに説明しています)。これらのすべての設定が行われていない場合、ユーザは、UDS サーバまたは UC ドメイン (FQDN または IP アドレス) のサーバアドレスを手動で入力する必要があります。

手順

- DNS SRV による自動検出または UC マネージャプロファイルが設定されている場合は、ユーザが Webex アプリ を開くだけで、SSO か手動のログイン情報を求めるプロンプトが表示されます。これ以上の手順は必要ありません。

一致するログインおよび UC ドメインでサービスディスカバリを使用している場合、サーバアドレスまたは UC ドメインを入力するオプションは表示されません。このオプションは、電話サービス用の特定のドメインに対して UC マネージャプロファイルを指定した場合、表示されません。

- DNS SRV を使用して自動検出を行わない場合は、次の手順に従ってユーザを支援してください。
 - a) 該当する Webex アプリ プラットフォームを使用して、電話サービスの設定にアクセスします。
 - Windows の場合は、プロファイルの写真をクリックし、[設定 (Settings)] を選択し、[電話サービス (Phone Services)] をクリックします。
 - Mac の場合は、プロファイルの写真をクリックして、[Preferences] を選択し、[Phone Services] をクリックします。
 - Android には、プロファイルの写真をタップし、[設定 (Settings)] を選択し、[電話サービス (Phone Services)] を選択します。
 - iPhone および iPad の場合は、プロファイルの写真をタップし、[電話サービス (Phone Services)] を選択します。

- b) 認証のタイプとプラットフォームに応じて、次のオプションを入力します。

Windows または Mac の場合は、次のいずれかを入力します。

- [サーバアドレス (Server address)]: SRV レコードが設定されていない場合は、ユーザデータサービス (UDS) サーバを入力します。通常、これはユニファイド CM パブリッシュャです。
- [UC ドメイン (UC Domain)]: サービス検出に使用されるユニファイド CM のドメイン名を入力します。

Android、iPhone、または iPad の場合、**Server Address or UC Domain**(サーバアドレスまたは UC ドメイン)フィールドに UDS サーバまたはドメイン名を入力し、**Apply**(適用) 又は **Apply Changes** (変更の適用) をタップする。



- (注) サーバアドレス/UDS サーバと UC ドメイン/音声サービスの両方を設定した場合は、サーバアドレスによってホームクラスタが決定され (DNS SRV による自動検出は無視されます)、UC ドメインによって、クライアントがオンプレミスかオフプレミス (MRA) かが決定されます。

- c) アプリケーションにプロンプトが表示されたら、ユーザ名とパスワードを入力するようにユーザに指示してから、サインインすることができます。



(注) サインイン画面は、既存の SSO の設定によって異なります。

ユーザは電話サービスで認証され、Webex アプリでのコール (Unified CM) 機能を使用できます。

次のタスク

- **Train Your Users** : 「サポートされている通話オプション」の記事を読むようにユーザーに指示するか、この記事トレーニング教材として使用して、Webex アプリでのコール (Unified CM) の機能セットの使用法 (Webex アプリで通話を保留する方法、デスクトップ制御の使用法など) をユーザーが習得できるように支援します。
- **問題のトラブルシューティング**: 登録時にエラーが発生した場合は、このガイドのトラブルシューティングの資料を参照してください。
- **サーバ情報のリセット** : 電話サービスの情報が変更された場合、または Webex アプリユーザが Unified CM のサーバ情報を再入力する必要がある場合は (ラボから実稼働サーバに移行する場合など)、データベースをリセットする必要があります (デスクトップでは [設定 (Settings)] > [ヘルスチェッカー (Health Checker)] > [データベースのリセット (Reset Database)])。モバイルアプリでサーバ情報をリセットするには、ユーザがデバイスでアンインストールと再インストールを実行する必要があります。

展開後に追加機能を構成する

これらの追加機能は、Webex アプリでのコール (Unified CM) の初回展開には必須ではありません。ただし、最初の展開手順を完了した後、これらの機能を構成して、自分やユーザーをさらにカスタマイズすることができます。追加のガイダンスについては、各機能にリンクされている資料を参照してください。

これらの追加機能を構成する方法については、項目のリンクにアクセスしてください。

表 14: 追加機能に関する資料

ヘルプセンター項目	機能説明と利点
Control Hub で組織の通話設定を構成する	Control Hub のこれらの通話設定機能を使用して、さまざまな通話展開を管理する際に、管理者として完全な制御と柔軟性を得ることができます。さまざまな通話オプション (勤務先番号または内線番号、SIP アドレスなど) を有効にして優先順位を付け、ユーザーのシングルクリック ツー コールを設定します。

ヘルプセンター項目	機能説明と利点
組織の SIP アドレスルーティングを設定する	Control Hub でこの設定を構成し、デフォルトオプションを変更すると、Webex の SIP 通話を、入力したドメインの Unified CM 環境を通じてルーティングできます。この設定により、通話トラフィックがクラウドに直接行き来することが減ります。
Webex アプリユーザー向けに仮想背景を設定する	背景をぼかすと、周囲の焦点がぼやけて見え、背後で何が起きているのかが見えなくなります。 管理者は、Control Hub を使用して、Webex での会議や通話に仮想背景を適用するためのオプションを構成できます。ユーザには、プリセット背景や独自のカスタム背景の使用を許可することができます。
Control Hub で通話とミーティング用に仮想カメラを設定する (MacOS のみ)	Control Hub を使用すると、Webex アプリでの通話や会議で仮想カメラを有効または無効にできます。ユーザーは、アプリケーション、ドライバ、ソフトウェアなどの仮想カメラを使用して、ビデオ、画像、またはフィードのオーバーレイを作成できます。
Webex アプリで通話のビデオを有効または無効にする (Webex での通話のみ)	Webex アプリで、通話やその他の Webex サービスのビデオを無効にすることができます。ビデオオプションの有効化および無効化は、すべての Calling ライセンスで利用でき、Control Hub の組織レベルおよびユーザーレベルで構成できます。 (注) Control Hub 設定は、Call on Webex のみに影響します。Webex アプリでのコール (Unified CM) のビデオを構成する場合、構成ファイルの EnableVideo パラメータまたは Unified CM の関連するサービスプロファイルを使用します。詳細については、付録のカスタマイズパラメータを参照してください。
Calling in Webex App に対してリモートデスクトップ制御を有効または無効にする (Call on Webex のみ)	Webex アプリで、通話およびその他の Webex サービスのリモートデスクトップ制御 (RDC) を無効にすることができます。RDC の有効化および無効化は、すべての Calling ライセンスで利用でき、Control Hub の組織レベルおよびユーザーレベルで構成できます。

既知の問題と Webex アプリでのコール (Unified CM) の制限事項

Webex アプリ 固有の情報については、「[既知の問題](#)」項目も参照してください。

モバイル

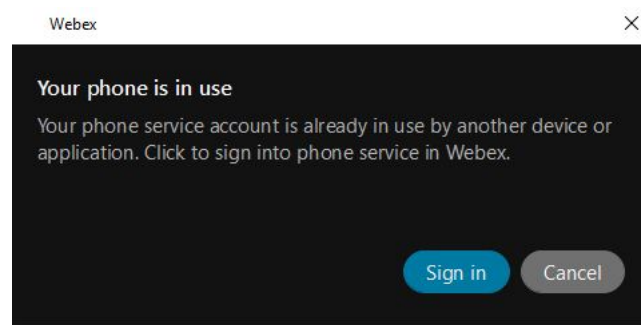
- これらの制限は、モバイル用 Webex (41.8) の Wi-Fi から LTE 通話ハンドオフに適用されます。

- この機能は、1つの通話のアクティブな通話引き継ぎのみをサポートしています。
Webex モバイルアプリでの複数の同時通話の場合、すべての通話は、ネットワークに切り替えた後に終了します。
- ネットワークの切り替え後は共有機能が失われるため、呼び出し元のユーザーはその通話中に共有を開始または受信できません。
- ネットワークが 20 秒以内に回復しない場合、アクティブな通話は終了します。
- 通話録音がアクティブな場合、録音は停止し、引き継ぎ後も再開しません。
- ネットワーク引き継ぎは、通話中の機能（保留や転送）、画面共有引き継ぎ、会議通話引き継ぎ、Contact Center 機能はサポートしません。
- Webex アプリでのコール (Unified CM) モバイルと近接のペアリングの場合は、連携しません。
- モバイルプラットフォームでアプリケーションの2つのインスタンスを実行している場合は、別のアクティブな接続に関するメッセージが表示されます。
- モバイルアプリの連絡先カードの番号については、ユーザは緑色のビデオアイコンをタップして他のユーザの番号を表示する必要があります。
- Webex アプリ ログインおよび電話サービスの場合、Web セッションは分かれます。たとえば、通話環境と Webex クラウドのコンポーネント用に同じ IdP (SSO) が構成されている場合でも、認証のために2回のプロンプトが表示されることがあります。この問題を解決するには、Unified CM および Expressway 環境をアップグレードして、SSO リダイレクト URI の拡張機能をサポートします。推奨構成に関する詳細は、「環境の準備」の章を参照してください。

全般

- Webex アプリでのコール (Unified CM) ハイブリッドコールまたはとは Webex Calling 連動しません。ユーザに対して Webex アプリでのコール (Unified CM) を有効化する前に、ハイブリッドコールまたは Webex Calling ユーザを無効化してください。ユーザを無効ハイブリッドコールにする方法の詳細については、「環境の準備」の章を参照してください。
- 非推奨の署名アルゴリズム (SHA-1 など) で発行された証明書は機能しない。 *Administration Guide for Cisco Unified Communications Manager* の証明書の章に記載されているように、SHA-256 以降などのサポートされているセキュアな署名アルゴリズムを使用する必要があります。
- 通話中のアプリケーション機能を相互 Webex アプリでのコール (Unified CM) 起動し、1人のユーザに対して設定することはできません。Control Hub を使うと、個人ユーザの発信動作のオーバーライドや設定ができます。たとえば、Webex アプリでのコール (Unified CM) に数名のユーザが、Cisco Jabber アプリ相互起動に数名のユーザが必要になる場合があります。
- 電話サービスおよび Jabber との共存：

- 電話サービスを使用できるデバイスは、各タイプ (デスクトップおよびモバイル) で 1 台だけです。Jabber と Webex アプリ で同時に電話サービスにサインインすることはできません。
- Jabber と Webex アプリ はそれぞれ、Unified CM で同じソフトフォンデバイスとしての登録を試行します。登録ポップアップでは、発信に使用するクライアントを選択できます。



ユーザーがすでに1つのクライアントに登録されており、別のクライアントが登録を強制した場合、元々登録しているクライアントでダイアログは表示されません。

- コールWebex アプリでのコール (Unified CM) は、Webex ビデオメッシュノードを利用しません。



第 4 章

Webex アプリでのコール（Unified CM）の管理とトラブルシューティング

- [Jabber コンタクトを移動するためのユーザー設定と Webex アプリ への共通設定（129 ページ）](#)
- [Webex アプリでのコール（Unified CM）の通話統計にアクセス（129 ページ）](#)
- [UC マネージャプロファイルの編集（130 ページ）](#)
- [Webex アプリ での診断（130 ページ）](#)
- [Control Hub でのシスコヘッドセットの管理（131 ページ）](#)
- [Webex クラウドへの接続が失われる（131 ページ）](#)
- [Calling in Webex アプリ（Unified CM）に関する問題のトラブルシューティング（132 ページ）](#)
- [Webex アプリ のエラーメッセージ（133 ページ）](#)

Jabber コンタクトを移動するためのユーザー設定と Webex アプリ への共通設定

この機能には、Cisco Jabber に組み込まれており、バディリストの連絡先とその他の共通ユーザー設定を、Jabber から Webex に移行する手段を提供します。データが暗号化されている場合このオプションが Jabber で自動的にユーザにポップアップ表示されるようにするには、事前にいくつかの設定を構成する必要があります。

[Webex アプリ に移動する Jabber ユーザーの構成方法について確認します。](#)

Webex アプリでのコール（Unified CM）の通話統計にアクセス

コール中には、ビデオのフレームレート、オーディオコーデック、パケット損失、ジッター、帯域幅の使用状況などのコール統計にアクセスできます。また、使用しているコール環境を示

サインジケータも表示されます（この情報は、管理者やサポートチームがトラブルシューティングの目的で必要とする場合があります）。

デスクトップまたはモバイルで Webex アプリ の通話統計にアクセスするには、「[通話の統計情報にアクセスする](#)」の手順に従います。

UC マネージャプロフィールの編集

ステップ1 <https://admin.webex.com> のお客様のビューで、[管理 (Management)] > [組織設定 (Organization Settings)] の順に選択し、[UC マネージャプロフィール (UC Manager Profiles)] で [...] を選択します。

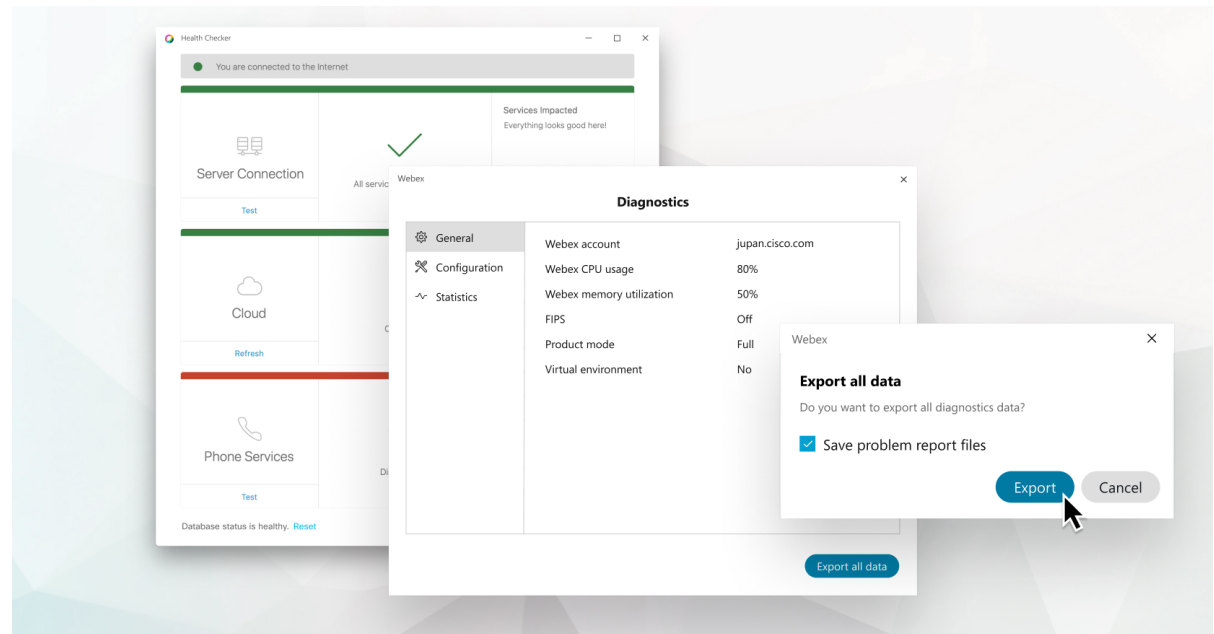
ステップ2 [編集 (Edit)] を選択します。

ステップ3 必要な編集を行い、[保存 (Save)] を選択します。

Webex アプリ での診断

Webex アプリ (デスクトップおよびVDI) で利用可能な診断は、接続の問題を解決し、メディアの品質を確認し、重要なトラブルシューティング情報を収集するのに役立ちます。

図 7: Webex アプリ での診断



Webex アプリでのコール (Unified CM) のセットアップ中に、音声ドメインや UC サービスなどの接続に関連する問題や必要な設定が発生する場合があります。このツールを使用すると、どのサービスが正しく設定されているのか、何が足りないのかを診断できます。この機能は、

Webex アプリでのコール (Unified CM) への移行の場合でも、新規ユーザを設定する場合でも、シナリオのトラブルシュートおよびサポートケースの削減に役立ちます。

ユーザエクスペリエンスに問題がある場合は、[診断ビューとデータのエクスポートにアクセス](#)し、自分やサポートと共有できます。

- **Unified CM 設定**：以下など、電話サービスが正しく機能するための重要な設定 (Jabber 移行や新規ユーザ設定など)
 - Unified CM のバージョン
 - UC サービスドメイン
 - SSO
 - ボイスメールなどの UC サービス
 - MRA の Expressway
- **メディア品質**：ビデオ、オーディオの品質および両方向での共有
- **デバイス**：ユーザがデバイスに接続した際のデバイス情報

診断ウィンドウを表示するショートカットキーについては、「[キーボードとナビゲーションショートカット](#)」を参照してください。

Control Hub でのシスコヘッドセットの管理

Control Hub デバイスビューでは、組織に登録されているすべてのシスコヘッドセットのリストを取得して、追跡することができます。各ヘッドセットエントリの詳細オプションと管理オプションを確認できます。この情報は、ヘッドセットを交換する必要があるか、または修理するかを決定するのに役立ちます。

詳細については、「[Control Hub のヘッドセット管理](#)」を参照してください。

Webex クラウドへの接続が失われる

<https://status.webex.com> または [正常性チェッカー](#) が、Webex アプリ クラウドの完全な機能停止または部分的な機能停止を検出した場合、通話タイプが Unified CM 通話で、Unified CM インフラストラクチャを介する限り、Calling in Webex アプリ (Unified CM) は、すでにサインインしているユーザーに対して機能します。

サインインがブロックされた場合、Unified CM コールは次のシナリオでは無効です。

- ユーザの初回サインイン
- Webex アプリ からログアウトし、再度サインイン

Unified CM コールは、アプリがサインインした状態が続く次のシナリオで発生します。

- Webex アプリ を終了してから再起動：連絡先、通話履歴、メッセージなどキャッシュされたデータが残ります。Unified CM 登録とコールは、影響を受けませんが、通話中に他のユーザにプレゼンスが送信されません。
- Webex アプリ が実行中のデバイスをリブート：連絡先、通話履歴、メッセージなどキャッシュされたデータが残ります。Unified CM 登録とコールは、影響を受けませんが、通話中に他のユーザにプレゼンスが送信されません。

シングルナンバーリーチ (SNR) の回避策

Webex アプリ から Unified CM に到達できない場合は、セルフケアポータルを使用して（リンクは Webex アプリ にあります）、コールが PSTN 経由でモバイルにルーティングされるようにシングルナンバーリーチ (SNR) を設定できます。管理手順については、[Feature Configuration Guide for Cisco Unified Communications Manager](#)のCisco Unified Mobility Featuresの章を参照してください。ユーザセルフケア設定については、[セルフケアポータルユーザガイド](#)を参照してください。

Calling in Webex アプリ (Unified CM) に関する問題のトラブルシューティング

Webex アプリ でコールイン (Unified CM) の使用を試行する際に、登録の問題が発生した場合は、チケットを送信する前にチェックリストの項目を確認してください。

-
- ステップ 1** ユーザのために、CTI RD または Cisco Spark RD がユニファイド CM から削除されたことを確認します。それ以外の場合は、余分なリモートデバイスを削除します。
 - ステップ 2** 別の通話アプリに相互起動するなど、Control Hub で組織が異なる通話動作を有効にする場合、この機能を無効化し、[Webex アプリ でコールイン (Unified CM) (Calling in Unified CM)] を再度選択します。これは、Unified CM 登録と相互起動を同時に有効化できないためです。
 - ステップ 3** 同じマシンに Jabber がインストールされている場合は、Jabber を終了します。これは、Jabber と Webex アプリ の両方をソフトフォンモードで同時に Unified CM に登録することはできないためです。
 - ステップ 4** Unified CM 上の他の設定を確認してください。いくつかの一般的な原因は次のとおりである。
 - ユニファイド CM エンドユーザアカウントに制御されたデバイスはありません。ソフトフォンデバイスが制御対象デバイスに追加されていることを確認します。
 - エクステンションモビリティユーザのSUBSCRIBE コーリングサーチスペースがありません。この設定に対して値が選択されていることを確認します。
 - エンドユーザアカウントのアクセスコントロールグループ権限がありません: **STANDARD CTI** は、**Connected Xfer** および **conf** をサポートする電話機の制御を許可します。このボックスがチェックされていることを確認してください。
-

次のタスク

これらの手順のすべてに対処しても問題が解決しない場合は、Webex アプリ を再起動し、[ヘルプ (Help)] > [フィードバックを送信 (Send Feedback)] を選択してログを送信し、ケースを開いてサポートチームに調査を依頼します。

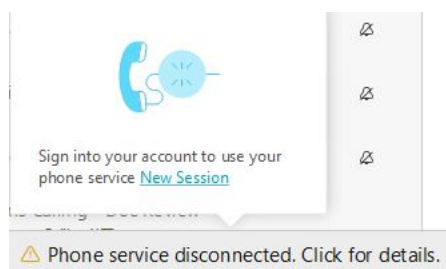
Webex アプリのエラーメッセージ

サインインの失敗またはその他の理由によって Webex アプリ が Unified CM に登録できなかった場合、アプリに警告アイコンが表示されます。このアイコンの横に理由の要約が表示されます。

△ Phone service disconnected. Click for details.



ヒント アイコンの上にカーソルを合わせると、トラブルシューティングの方法に関する手がかりが表示されるエラーメッセージが表示されます。アイコンをクリックして、問題を解決するために実行すべき次の手順（電話サービスへのサインイン、新しいセッションの開始など）がないかどうかを確認することもできます。



Webex アプリ で表示される場合があるエラーの詳細と問題の解決方法については、「[エラーメッセージ](#)」資料を参照してください。



付録 **A**

付録

- [ポリシーパラメータ \(135 ページ\)](#)
- [通話用プロトコルハンドラ \(151 ページ\)](#)
- [サービス品質 \(155 ページ\)](#)
- [Unified CM で信頼できない証明書を許可する \(158 ページ\)](#)

ポリシーパラメータ

ポリシーパラメータについては、次の表を参照してください。これらのパラメータによって、Webex アプリ の特定のクライアント機能を制御できます。

機能パラメータ

パラメータ	説明と値	サポートされるプラットフォーム
CucmCallBargeMode	<p>パラメータ : CucmCallBargeMode</p> <ul style="list-style-type: none">• OFF (デフォルト) — [割り込み (barge)] ボタンは Webex アプリ に表示されます。• BARGE — 割り込みの開始者は割り込みの招待を送信し、割り込み先は会議サーバーとして機能します。 <p>例 :</p> <pre><CucmCallBargeMode>BARGE</CucmCallBargeMode></pre>	

パラメータ	説明と値	サポートされるプラットフォーム
E911EdgeLocationWhiteList	<p>パラメータ : E911EdgeLocationWhiteList</p> <p>セミコロンで区切られた最大 30 のサービスセット ID (SSID) のホワイトリストを指定します。</p> <p>E911EdgeLocationPolicy パラメータが [True] に設定されている場合は、このパラメータをかならず構成してください。その後クライアントは、モバイルおよびリモートアクセスネットワーク向けの Expressway を介して企業のネットワークに接続するユーザを監視します。</p> <p>例 :</p> <pre><EnableE911EdgeLocationPolicy>true</EnableE911EdgeLocationPolicy> <E911EdgeLocationWhiteList>SSID1;SSID2</E911EdgeLocationWhiteList></pre>	デスクトップおよびモバイル
EnableCallPark	<p>パラメータ : EnableCallPark</p> <p>クライアントでコールパーク機能を使用できるかどうかを指定します。</p> <p>[コールパーク (call park)]機能にアクセスするには、[通話 (Call)] ウィンドウで [詳細 (More)] オプションを選択します。</p> <ul style="list-style-type: none"> • true (デフォルト) — コールパークが有効です。 • false — コールパークが無効です。コールパーク オプションが [詳細 (More)] ボタンの下に表示されません。 	デスクトップ
EnableCallPickup	<p>パラメータ : EnableCallPickup</p> <p>ユーザが自分のコールピックアップグループ内のコールをピックアップできるかどうか指定します。</p> <ul style="list-style-type: none"> • true : コールピックアップを有効にします。 • false : コールピックアップを無効にします (デフォルト)。 	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
EnableE911EdgeLocationPolicy	<p>パラメータ : EnableE911EdgeLocationPolicy</p> <p>ユーザがモバイルおよびリモートアクセス向け Expressway を介して企業のネットワークに接続するときに、クライアントがワイヤレスロケーションモニタリングを使用することを指定します。</p> <ul style="list-style-type: none"> • true : Webex アプリ が MRA を介してワイヤレスロケーションを監視します。また、サービスセット ID (SSID) を使用して、E911EdgeLocationWhiteList パラメータを構成する必要があります。セミコロンで区切られた最大 30 の SSID のリストを構成できます。 • false : Webex アプリ は、ワイヤレスロケーションを監視しません (デフォルト)。 <p>例 :</p> <pre><EnableE911EdgeLocationPolicy>true</EnableE911EdgeLocationPolicy> <E911EdgeLocationWhiteList>SSID1;SSID2</E911EdgeLocationWhiteList></pre>	デスクトップおよびモバイル
EnableE911OnPremLocationPolicy	<p>パラメータ : EnableE911OnPremLocationPolicy</p> <p>クライアントがオンプレミス展開でワイヤレスロケーションモニタリングサービスを使用することを指定します。</p> <ul style="list-style-type: none"> • true : オンプレミスに接続されている場合、Webex アプリ は常にワイヤレスロケーションを監視します。 • false : Webex アプリ オンプレミスに接続されていても、ワイヤレスロケーションを監視しません (デフォルト)。 	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
EnableGroupCallPickup	<p>パラメータ : EnableGroupCallPickup</p> <p>コールピックアップグループ番号を入力して、ユーザが別のコールピックアップグループの着信コールをピックアップできるかどうか指定します。</p> <ul style="list-style-type: none"> • true : グループコールピックアップを有効にします。 • false : グループコールピックアップを無効化します (デフォルト)。 	デスクトップおよびモバイル
EnableHuntGroup	<p>パラメータ : EnableHuntGroup</p> <p>ユーザがハントグループにログインできるかどうか指定します。</p> <ul style="list-style-type: none"> • true : ユーザはハントグループにログインできます。 • false : ユーザは、ハントグループにログインできません (デフォルト)。 	デスクトップおよびモバイル
EnableMeetingPowerUp	<p>パラメータ : EnableMeetingPowerUp</p> <p>ユーザがアクティブ通話をミーティングに移動するよう指定します。</p> <ul style="list-style-type: none"> • true : コールを会議に移動できるようにします。 • false : コールを会議に移動できないようにします (デフォルト)。 	デスクトップ
EnableOtherGroupPickup	<p>パラメータ : EnableOtherGroupPickup</p> <p>ユーザが、自分のコールピックアップグループに関連付けられたグループ内の着信コールをピックアップできるかどうか指定します。</p> <ul style="list-style-type: none"> • true : 他のグループのコールピックアップを有効にします。 • false : 別のグループコールピックアップを無効化します (デフォルト)。 	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
EnableRecordingTone	<p>パラメータ : EnableRecordingTone</p> <p>ユーザの録音トーンを有効します。このパラメータは、LocalRecordingToneVolume、NearEndRecordingToneVolume、RecordingToneDuration、RecordingToneIntervalの他のパラメータと連携します。</p> <p>(注) rrecording tone パラメータを追加する前に、Unified CM service パラメータで録音通知トーンを再生できるようにしてください。</p> <p>詳細については、『Cisco Unified Communications Manager の機能とサービスガイド』にある「モニタリングと録音」章を参照してください。</p> <ul style="list-style-type: none"> • true — 録音トーンを有効にします。(デフォルト) • false — 録音トーンを無効にします。 	デスクトップおよびモバイル
EnableSIPURIDialling	<p>パラメータ : EnableSIPURIDialling</p> <p>Webex で URI ダイアルを有効にして、ユーザが URI を使用して通話できるようにします。</p> <ul style="list-style-type: none"> • true ユーザが URI を使用して通話できるようになります。(デフォルト) • false— URI を使用してもユーザは通話できません。 <p>例 :</p> <pre><EnableSIPURIDialling>>false</EnableSIPURIDialling></pre>	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
LocalPushSSIDList	<p>パラメータ : LocalPushSSIDList</p> <p>管理者は、Jabber-config.xml ファイルでサポートされている WiFi リストを指定する必要があります。</p> <p>セミコロンで区切られた最大 10 のサービスセット ID (SSID) のホワイトリストを指定します。</p> <p>ローカルプッシュ通知接続機能が CUCM で有効になっている場合は、このパラメータを設定する必要があります。</p> <p>例 :</p> <pre><LocalPushSSIDList>SSID1;SSID2</LocalPushSSIDList></pre>	モバイル : iOS および iPad OS
LocalRecordingToneVolume	<p>パラメータ : LocalRecordingToneVolume</p> <p>クライアントが録音トーンをローカルで再生する音量を指定します。</p> <p>範囲は 0 ~ 100% で、デフォルトは 10 です。</p> <p>例 :</p> <pre><LocalRecordingToneVolume>25</LocalRecordingToneVolume></pre> <p>録音トーンを適切に構成する方法の詳細については、「EnableRecordingTone」を参照してください。</p>	デスクトップおよびモバイル
NearEndRecordingToneVolume	<p>パラメータ : NearEndRecordingToneVolume</p> <p>Webex がリモートデバイスおよび近端録音サーバーに送信する録音トーンの音量を指定します。</p> <p>範囲は 0 ~ 100% で、デフォルトは 10 です。</p> <p>例 :</p> <pre><NearEndRecordingToneVolume>25</NearEndRecordingToneVolume></pre> <p>録音トーンを適切に設定する方法の詳細については、EnableRecordingTone を参照してください。</p>	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
PreventDeclineOnHuntCall	<p>パラメータ : PreventDeclineOnHuntCall</p> <p>ハンティンググループに着信コールがあった場合に、[拒否] ボタンを表示するかどうかを指定します。</p> <ul style="list-style-type: none"> • true : ハンティンググループの着信コールに対して [拒否 (Decline)] ボタンは表示されません。 • false : ハンティンググループの着信通話で [拒否 (Decline)] ボタンが表示されます (デフォルト) 。 	デスクトップおよびモバイル
RecordingToneDuration	<p>パラメータ : RecordingToneDuration</p> <p>シングルトーンのミリ秒を指定します。</p> <p>範囲は 100 ~ 2000 で、デフォルトは 500 です。</p> <p>例 :</p> <pre><RecordingToneDuration>500</RecordingToneDuration></pre> <p>録音トーンを適切に構成する方法の詳細については、「EnableRecordingTone」を参照してください。</p>	デスクトップおよびモバイル
RecordingToneInterval	<p>パラメータ : RecordingToneInterval</p> <p>連続トーン間のミリ秒を指定します。</p> <p>範囲は 8000 ~ 32000 で、デフォルトは 11500 です。</p> <p>例 :</p> <pre><RecordingToneInterval>11500</RecordingToneInterval></pre> <p>録音トーンを適切に構成する方法の詳細については、「EnableRecordingTone」を参照してください。</p>	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
ShowSelectiveCallRecordingButton	<p>パラメータ : ShowSelectiveCallRecordingButton</p> <ul style="list-style-type: none"> • true (デフォルト) : Webex アプリに録音ボタンが表示されます。 • false : 録音ボタンは Webex アプリで非表示になるため、ユーザーは録音を開始または停止できませんが、サードパーティの CTI を使用して録音することはできます。 <p>例 :</p> <pre><ShowSelectiveCallRecordingButton>false</ShowSelectiveCallRecordingButton></pre> <p>(注) このパラメータは、ユーザーの回線の [Cisco Unified CM 管理ポータル] の [録音オプション (Recording Option)] フィールドが [選択的通話録音有効 (Selective Call Recording Enabled)] に設定されている場合にのみ有効です。</p>	デスクトップおよびモバイル

カスタマイズパラメータ

パラメータ	説明と値	サポートされるプラットフォーム
DeskPhoneModeWindowBehavior	<p>デスクフォン制御モードで呼制御ウィンドウを表示するかどうかを制御します。</p> <ul style="list-style-type: none"> • OnCall (デフォルト) : コールへの応答時に常に [会話 (Conversation)] ウィンドウが表示されます。 • Never : コールへの応答時に [会話 (Conversation)] ウィンドウは表示されません。 • NotOnHold : コールが共有回線デバイスで保留されている場合、[会話 (Conversation)] ウィンドウは表示されません。その他のシナリオではウィンドウが表示されます。 	デスクトップ (Windows のみ)

パラメータ	説明と値	サポートされるプラットフォーム
E911NotificationFrequency	<p>緊急通話の免責事項の頻度を制御します。</p> <ul style="list-style-type: none"> • FirstSignIn (デフォルト) — 初回サインインした時のみ免責事項を表示します。 • EverySignIn — ユーザーがサインアウトし、サインインするごとに免責事項を表示します。 • Never — 免責事項は表示されません。 <p>初回サインインのみに免責事項を表示する例 <code><E911NotificationFrequency>FirstSignIn</E911NotificationFrequency></code></p>	デスクトップおよびモバイル
E911NotificationURL	<p>サインインするたびに、カスタマイズ可能な免責事項に関するメッセージまたは通知がユーザーに表示されます。テレフォニー機能を有効にする前にユーザーはこれに同意する必要があります。このプロンプトにより、ユーザーは免責事項または通知を確認できます。</p> <p>このパラメータの値を、通知メッセージをホストしている有効な HTML Web ページの URL に設定します。</p> <p>例 :</p> <p><code><E911NotificationURL>http://www.example.com/e911.html</E911NotificationURL></code></p> <p>企業のネットワークの外部で稼働するすべてのアプリで Web ページが正しく表示されるようにするには、スクリプトおよびリンク タグが E911NotificationURL パラメータでサポートされていないため、Web ページに静的な HTML ページを指定する必要があります。</p>	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
EnableADLockPrevention	<p>サインイン試行の失敗の最大数に対して Active Directory サーバーを構成できます。この設定により、一部の Webex 展開で誤ったアカウントロックアウトが発生する可能性があります。たとえば、SSO 認証のない展開では、すべての Webex サービスが同じ不正なログイン情報を AD サーバーに送信し、失敗カウンタを急速に引き上げる可能性があります。</p> <p>この問題が発生した場合は、EnableADLockPrevention を使用して、サービスが同じ不正なログイン情報を AD サーバーに送信しないようにすることができます。使用できる値は次のとおりです。</p> <ul style="list-style-type: none"> • true —1 つのサービスが無効なログイン情報エラーを受け取った後、Webex は同じログイン情報を持つすべてのサービスを停止します。 • false (デフォルト) — Webex は無効なログイン情報エラーを無視し、サインインの試行を続行します。 <p>例 :</p> <pre><EnableADLockPrevention>true</EnableADLockPrevention></pre>	デスクトップおよびモバイル
EnablePhoneDataOptionOverMRA	<p>インドの規制により、ユーザーは企業のネットワークに接続していない場合、VoIP アプリを使用して PSTN 通話を発信できません。</p> <p>Webex モバイルユーザーが外にいて、Webex の連絡先電話番号に電話をかけたい場合、アプリは組み込みの電話アプリを使用して電話をかけるオプションを提供します。</p> <ul style="list-style-type: none"> • true —MRA 環境からのすべての通話は、電話オプションダイアログに表示されます。 • false (デフォルト) — ユーザーが接続しているネットワークに関係なく、電話オプションダイアログは表示されません。 	モバイル

パラメータ	説明と値	サポートされるプラットフォーム
EnableVideo	<p>ユーザーが発信通話と着信通話でビデオを使用できるかどうかを指定します。</p> <ul style="list-style-type: none"> • true (デフォルト) ユーザーは、発信通話と着信通話でビデオを使用できます。 • false ユーザーは、発信通話と着信通話でビデオを使用できません。すべての通話は、音声のみの通話となります。 <p>重要 このキーが構成されている場合、キーの設定は常に Control Hub の設定 よりも優先されます。キーに値が構成されていない場合、Control Hub の設定が有効となり、ビデオを有効にするか無効にするかを決定します。</p>	デスクトップおよびモバイル
RemoteControlEditingMultipleDevices	<p>複数のデバイスを使用するユーザが、リモート接続先を編集または追加できるかどうかを決定できます。</p> <ul style="list-style-type: none"> • true (デフォルト) : 複数のデバイスを使用するユーザは、リモートの接続先を編集または追加できます。(デフォルト) • false : 複数のデバイスを使用するユーザは、リモート接続先を編集または追加できません。 	デスクトップ

パラメータ	説明と値	サポートされるプラットフォーム
RemotePresencePrimaryLineOnly	<p>複数回線を持つユーザがコールに参加している場合のプレゼンスの動作を指定します。</p> <ul style="list-style-type: none"> • true : ユーザがプライマリラインを使用している場合にのみ、RemoteInUse プレゼンスが表示されます。たとえば、ユーザの 2 番目の回線がデスクフォンと同じ番号を共有している場合、デスクフォンからコールを行っても、ユーザのステータスは「通話中」とは表示されません。 • false (デフォルト) : ユーザが使用する回線に関わらず、すべての回線で RemoteInUse プレゼンスが表示されます。たとえば、ユーザの 2 番目の回線がデスクフォンと同じ番号を共有している場合、デスクフォンからコールを行うと、ユーザのステータスは「通話中」として表示されます。 <p>(注) このパラメータは、Unified CM で選択可能なプリセットではありません。ポリシーにカスタムパラメータとして追加する必要があります。</p>	デスクトップ
SelfCareURL	<p>Cisco Unified Communications Manager サービスの完全修飾ドメイン名 (FQDN) を指定します。</p> <p>Cisco Unified Communications Manager でデフォルトのサービスプロファイルが選択されていない場合のセルフケアポータル URL を定義します。</p> <p>例 :</p> <pre><SelfCareURL>https://selfcare.example.com</SelfCareURL></pre>	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
ShowSelfCarePortal	<p>[オプション (Options)]ダイアログに[セルフケアポータル (Self Care Portal)]タブを表示するか指定します。</p> <ul style="list-style-type: none"> • true (デフォルト) : [オプション (Options)]ダイアログに[セルフケアポータル (Self Care Portal)]タブが表示されます。 • false : [オプション (Options)]ダイアログに[セルフケアポータル (Self Care Portal)]タブを表示しません。 	デスクトップおよびモバイル
ShowCallAlerts	<p>着信コールアラートを表示するかどうかを指定します。</p> <ul style="list-style-type: none"> • true (デフォルト) : 着信電話アラートが常に表示されます。 • false : 着信コールアラートは表示されません。 	デスクトップ (Windows のみ)
ShowPhoneNumbersInLineSelection	<p>回線選択ドロップダウンに電話番号を表示するかどうかを制御します。</p> <ul style="list-style-type: none"> • true (デフォルト) — 回線選択ドロップダウンメニューで回線の電話番号 (DID または内線番号) が表示されます。回線にテキストラベルが構成されている場合は、番号とラベルが表示されます。 • false — 回線選択ドロップダウンメニューで回線の電話番号 (DID または内線番号) が表示されません。回線のテキストラベルのみが表示されます。 	デスクトップ (Windows のみ)

パラメータ	説明と値	サポートされるプラットフォーム
SoftPhoneModeWindowBehavior	<p>ソフトフォンモードで呼制御ウィンドウを表示するかどうかを制御します。</p> <ul style="list-style-type: none"> • OnCall (デフォルト) : コールへの応答時に常に[会話 (Conversation)]ウィンドウが表示されます。 • Never : コールへの応答時に [会話 (Conversation)]ウィンドウは表示されません。 • NotOnHold : コールが共有回線デバイスで保留されている場合、[会話 (Conversation)]ウィンドウは表示されません。その他のシナリオではウィンドウが表示されます。 	デスクトップ (Windows のみ)
StartCallWithVideo	<p>ユーザーが着信通話のビデオを開始できるかどうかを指定します。</p> <ul style="list-style-type: none"> • true (デフォルト) — 着信通話でビデオを送信します。 • false — 着信通話でビデオを送信しませんが、ビデオは受信できます。 	デスクトップおよびモバイル

パラメータ	説明と値	サポートされるプラットフォーム
UserDefinedRemoteDestinations	<p>ユーザは、クライアント インターフェイスを使用してリモート接続先を追加、編集、および削除できます。拡張機能と接続機能をプロビジョニングしてデフォルトの動作を変更するには、このパラメータを使用します。</p> <p>デフォルトでは、ユーザのデバイス リストに CTI リモート デバイスだけが含まれる場合、クライアントはユーザがリモート接続先を追加、編集、または削除できないようにします。これは、割り当てられた専用のリモート デバイスをユーザが変更できないようにするためです。ただし、ユーザのデバイス リストに ソフトフォン デバイス または デスクフォン デバイスが含まれる場合、クライアントはユーザがリモート接続先を追加、編集、および削除できるようにします。</p> <ul style="list-style-type: none"> • true : ユーザはリモート接続先を追加、編集、および削除できます。 • false (デフォルト) : ユーザはリモート接続先を追加、編集、および削除できません。 	デスクトップ

Jabber to Webex アプリ migration パラメータ

パラメータ	説明と値	サポートされるプラットフォーム
EnableJabber2TeamsMigration	<p>Jabber から Webex アプリ にデータを移行する候補としてユーザをタグ付けします。このプロセスにより、ユーザの連絡先（バディ）リストおよび共通の設定が Webex アプリ に渡されます。</p> <ul style="list-style-type: none"> • true : ユーザは、両方のアプリケーションで電子メールアドレスが一致していれば、Jabber から Webex アプリ にデータを移行できます。データの移行は、ユーザが Jabber にサインインしてから 5 分～3 時間以内に開始されます。または、ヘルプメニューから手動で移行を開始することもできます。 • false : Jabber から Webex アプリ へのデータの移行はユーザに表示されません。（デフォルト） <p>(注) このパラメータは、Unified CM で選択可能なプリセットではありません。ポリシーにカスタムパラメータとして追加する必要があります。</p>	デスクトップ
WebexTeamsDownloadURL	<p>アップグレード中にユーザが Webex アプリ をダウンロードしなかった場合のために、ダウンロードできる場所を指定します。この URL の値を追加しないと、ユーザは管理者に連絡してヘルプを求めるように指示されます。</p> <p>例（公式のダウンロードページを使用）：</p> <pre><WebexTeamsDownloadURL>https://www.webex.com/downloads.html</WebexTeamsDownloadURL></pre> <p>(注) このパラメータは、Unified CM で選択可能なプリセットではありません。ポリシーにカスタムパラメータとして追加する必要があります。</p>	デスクトップ

通話用プロトコルハンドラ

Webex アプリでのコール (Unified CM) は、オペレーティング システムで次のプロトコルハンドラを登録して、Web ブラウザまたはその他のアプリケーションからの click-to-call 機能を有効にします。次のプロトコルは、Webex アプリが Mac または Windows でデフォルトの通話アプリケーションになっていると、音声通話またはビデオ通話を開始します。

- CLICKTOCALL: または CLICKTOCALL://
- SIP: または SIP://
- TEL: または TEL://
- WEBEXTEL: または WEBEXTEL://

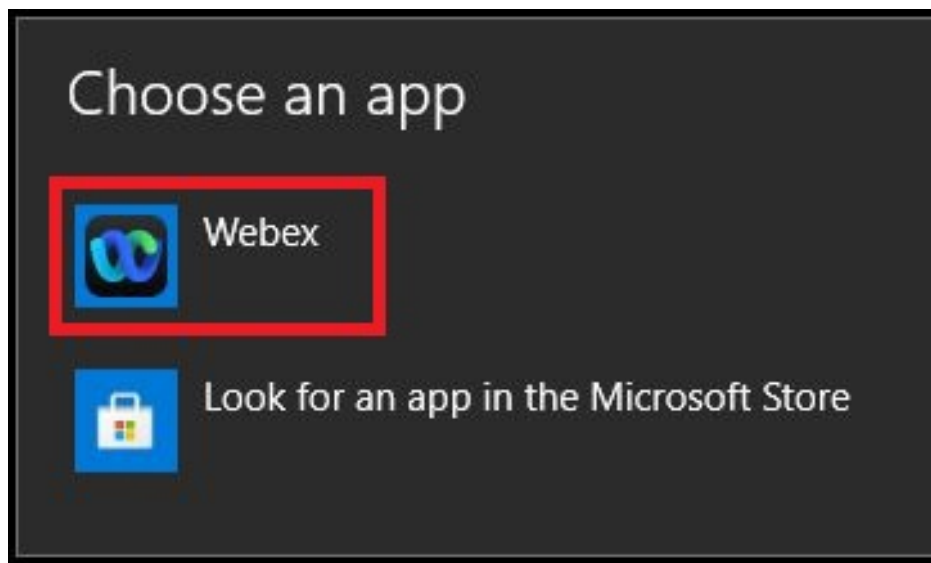
```
sip://12345  
sip:12345  
sip://test@example.com  
sip:test@example.com  
tel://12345  
tel:12345  
tel://test@example.com  
tel:test@example.com  
clicktocall://12345  
clicktocall:12345  
clicktocall://test@example.com  
clicktocall:test@example.com
```



- (注) これらのプロトコルに対してアプリが起動されたときに Unified CM が未接続の場合、Webex アプリは Unified CM が接続するまで 3 分間待機します。接続されていない状態が 3 分経過すると、コール要求は停止します。SIP アドレスを使用してコールを開始する場合 (例: sip:test@example.com)、コールは、制御ハブにある組織の SIP アドレスルーティング設定に応じて、クラウドまたはユニファイド CM を経由する場合があります。

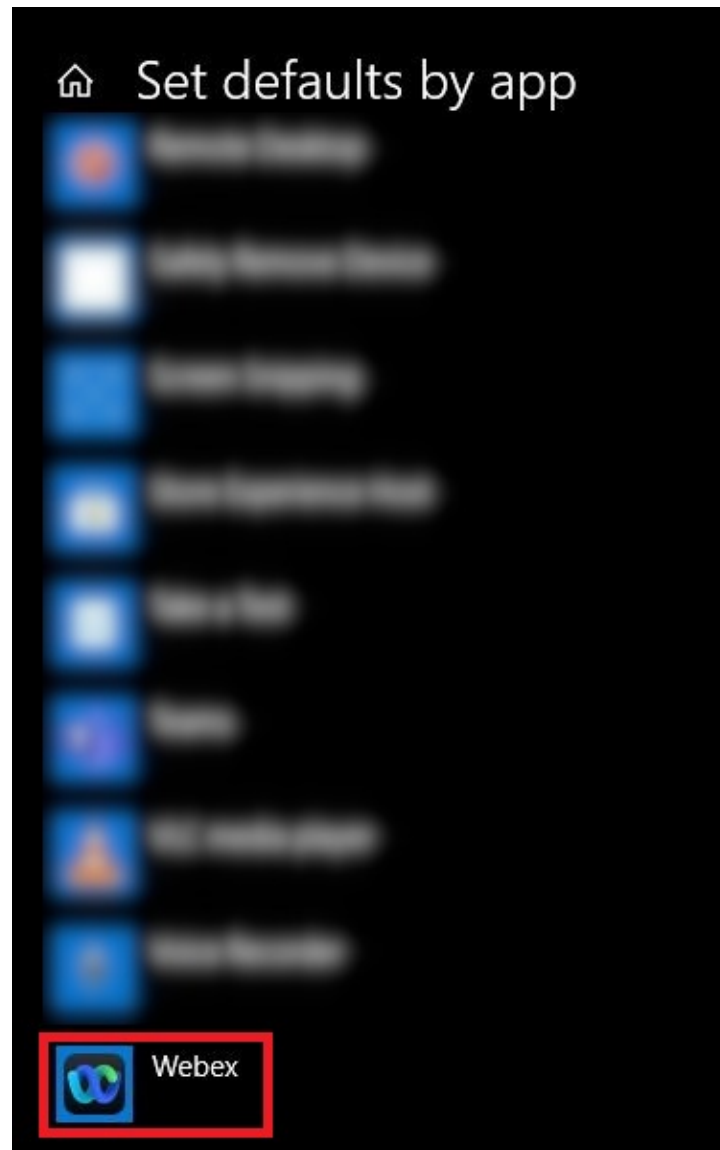
Windows 用プロトコルハンドラ

他のアプリは、Webex アプリの前にプロトコルハンドラに登録できます。Windows 10 では、コールの起動に使用するアプリを選択するように、システム ウィンドウがユーザーに要求します。ユーザーが常にこのアプリを使用するをオンにすると、ユーザー設定を記憶できます。

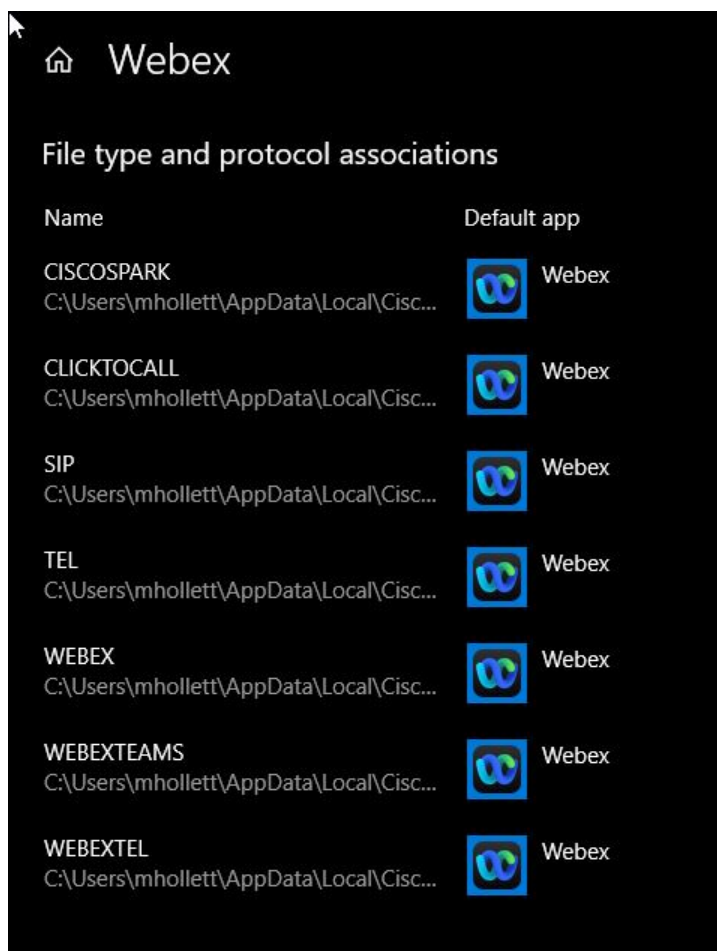


Webex アプリ を選択できるようにするために、ユーザがデフォルトの通話アプリの設定をリセットする必要がある場合は、Windows 10 で Webex アプリ のプロトコルの関連付けを変更するように指示できます。

1. システム設定で[既定のアプリ (Default app)]の設定を開き、[アプリごとに既定値を設定する (Set defaults by app)]をクリックして、[Webex アプリ]を選択します。



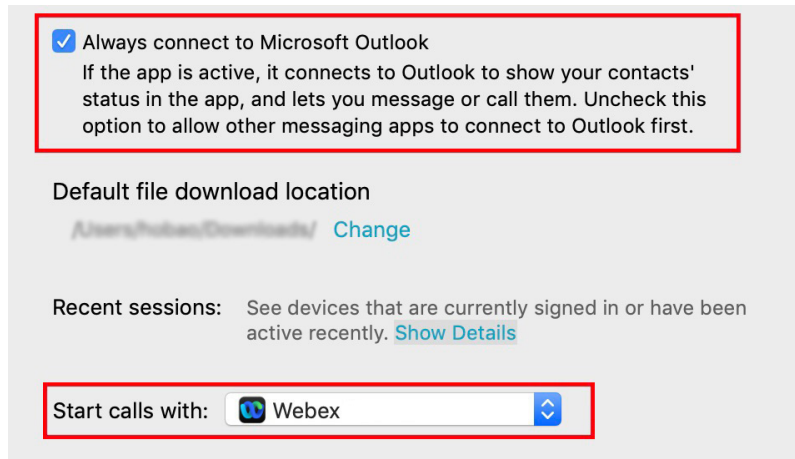
2. 各プロトコルに対して **Webex アプリ** を選択します。



macOS 用プロトコルハンドラ

Mac OS では、他のアプリが Webex アプリよりも先に通話プロトコルに登録されている場合、ユーザーは Webex アプリをデフォルトの通話オプションとして設定する必要があります。

Mac 用 Webex アプリでは、一般設定の [通話の開始 (Start calls with)] 設定で **Webex アプリ** が選択されていることを確認します。また、[常に Microsoft Outlook に接続 (Always connect to Microsoft Outlook)] をオンにすると、Outlook 連絡先の番号をクリックしたときに Webex アプリでコールを発信できます。



サービス品質

Quality of Service オプション

Webex アプリの Quality of Service (QoS) を構成するには、次のオプションを使用します。

- サポートされるコーデック (155 ページ)
- SIP プロファイルでのポート範囲の定義 (156 ページ)
- DSCP 値の設定 (156 ページ)

サポートされるコーデック

タイプ	コーデック	コーデックタイプ	Webex アプリ (Mac の場合)	Webex アプリ (Windows の場合)
音声	G.711	A-law	はい	はい
		μ-law/Mu-law	はい	はい
	G.722		はい	はい
	G.722.1	24 kb/s および 32 kb/s	はい	はい
	G.729		いいえ	いいえ
	G.729a		はい	はい
	Opus		はい	はい

タイプ	コーデック	コーデックタイプ	Webex アプリ (Mac の場合)	Webex アプリ (Windows の場合)
ビデオ	H.264/AVC		はい	はい

SIP プロファイルでのポート範囲の定義

クライアントは、ポート範囲を使用して、ネットワークに RTP トラフィックを送信します。また、クライアントは、ポート範囲を均等に分割して、下半分を音声コール用に、上半分をビデオコール用に使用します。オーディオメディアおよびビデオメディアのポート範囲を分割する結果として、クライアントにより識別可能なメディアストリームが作成されます。IP パケットのヘッダー内の DSCP 値を設定することで、それらのメディアストリームを分類し、優先させることができます。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ 2 [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [SIP プロファイル (SIP Profile)] の順に選択します。

ステップ 3 適切な SIP プロファイルを検索するか、新しい SIP プロファイルを作成します。

[SIP プロファイルの設定 (SIP Profile Configuration)] ウィンドウが開きます。

ステップ 4 オーディオとビデオに共通または個別のポート範囲を設定するかどうかを指定します。音声とビデオのポート範囲を分離している場合は、音声ポートとビデオポートを提供します。次のフィールドにポート範囲を指定してください。

- [開始メディアポート (Start Media Port)] : メディアストリームの開始ポートを定義します。このフィールドは、範囲の最小ポートを設定します。
- [終了メディアポート (Stop Media Port)] : メディアストリームの終了ポートを定義します。このフィールドは、範囲の最大ポートを設定します。

ステップ 5 [設定の適用 (Apply Config)] を選択し、[OK] をクリックします。

DSCP 値の設定

RTP メディアパケットヘッダーで Differentiated Services Code Point (DSCP; DiffServ コードポイント) の値を設定し、ネットワークを通過する Webex アプリトラフィックに優先順位をつけます。

Unified CM での DSCP 値の設定

Unified CM で、オーディオメディアとビデオメディアの DSCP 値を設定できます。Webex アプリは、デバイス構成から DSCP 値を取得し、RTP メディアパケットの IP ヘッダーに直接適用します。



制約事項 Microsoft Windows 10 などのオペレーティングシステムには、アプリケーションが IP パケットヘッダーに DSCP 値を設定できないようにするセキュリティ機能があります。そのため、Microsoft グループポリシーなどの DSCP 値をマーキングするための代替方式を使用する必要があります。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ 2 [システム(System)] > [サービスパラメータ(Service Parameters)] を選択します。

[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウが開きます。

ステップ 3 適切なサーバを選択してから、[Cisco CallManager (Cisco CallManager)] サービスを選択します。

ステップ 4 [クラスタ全体のパラメータ (システム : QOS) (Clusterwide Parameters (System - QOS))] セクションを見つけます。

ステップ 5 適切な DSCP 値を設定し、[保存 (Save)] を選択します。

グループポリシーを用いた DSCP 値の設定

Windows 用 Webex アプリを Microsoft Windows 7 以降などのオペレーティングシステムに展開する場合は、Microsoft グループポリシーを使用して DSCP 値を適用できます。

グループポリシーを作成するには、Microsoft サポートの記事 (<http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx>) の手順を実行します。

次の属性を用いて音声メディアとビデオメディアに別々のポリシーを作成する必要があります。

これらの指示は、Webex アプリを経由する Unified CM コールに適用されます。Webex アプリのみのコールについては、Webex アプリの「[ネットワーク要件](#)」のドキュメントに記載されているガイドラインを使用してください。

属性	音声ポリシー	ビデオポリシー	シグナリングポリシー
アプリケーション名	CiscoCollabHost.exe	CiscoCollabHost.exe	CiscoCollabHost.exe
プロトコル	UDP	UDP	TCP

属性	音声ポリシー	ビデオ ポリシー	シグナリング ポリシー
ポート番号または範囲	Cisco Unified Communications Manager 上の SIP プロファイルからの対応するポート番号または範囲。	Cisco Unified Communications Manager 上の SIP プロファイルからの対応するポート番号または範囲。	SIP は 5060
DSCP の値	46	34	24

ネットワークで DSCP 値を設定

スイッチおよびルータを設定し、RTP メディアの IP ヘッダーで DSCP 値をマーキングします。

ネットワーク内の DSCP 値を設定するには、クライアントアプリケーションからの異なるストリームを識別する必要があります。

- **メディア ストリーム**：クライアントは音声ストリームとビデオストリームに別々のポート範囲を使用するため、それらのポート範囲に基づいて音声メディアとビデオメディアを区別できます。SIP プロファイルのデフォルトのポート範囲を使用して、次のようにメディア パケットをマーキングする必要があります。

- 音声メディアは、EF として、16384 ~ 24575 のポートでストリーミングする
- ビデオメディアは、AF41 として、24575 ~ 32767 のポートでストリーミングする

- **シグナリングストリーム**：SIP、CTIQBE、および XMPP に必要なさまざまなポートに基づいて、クライアントとサーバ間のシグナリングを識別できる。たとえば、Webex アプリと Cisco Unified Communications Manager 間の SIP シグナリングはポート 5060 を介して行われます。

シグナリングパケットを CS3 としてマークする必要がある。

- Webex アプリ のみのコールのポート範囲については、Webex アプリ の [ネットワーク要件](#) に関するドキュメントに記載されているガイドラインを使用してください。

Unified CM で信頼できない証明書を許可する

必要に応じて、コントロールハブを使用して、ユニファイド CM からの信頼できない証明書を許可できます。これらは自己署名されているか、または証明書が接続に使用されているアドレスと一致しないため、信頼できない可能性があります。



注意 この設定により、導入のセキュリティがダウングレードされます。証明書の信頼には、より安全な方法を使用することを強く推奨します。この方法は、ラボテスト環境などの限定的な導入のための最後の手段として使用してください。

始める前に

- このオプションを使用する前に、証明書の要件とベストプラクティスについて理解しておいてください：[証明書の要件（74 ページ）](#)。
- iOS デバイスでは、プライベートなエンタープライズ証明書を使用している場合、デバイス自体にカスタムのルート CA をインストールする必要があります。そうしないと、Webex アプリは SSO 承認 URL への移動に失敗します。

ステップ 1 <https://admin.webex.com> のお客様ビューで、[サービス (Services)] > [Calling] の順に選択し、[クライアント設定 (Client Settings)] を選択します。

ステップ 2 Unified CM 設定で、**信頼されていない証明書を使用せずに CM 登録を許可する** をオンに切り替える。

このトグルをオンにすると、使用されている証明書の種類に関係なく、Webex アプリが Unified CM 環境に登録されます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。