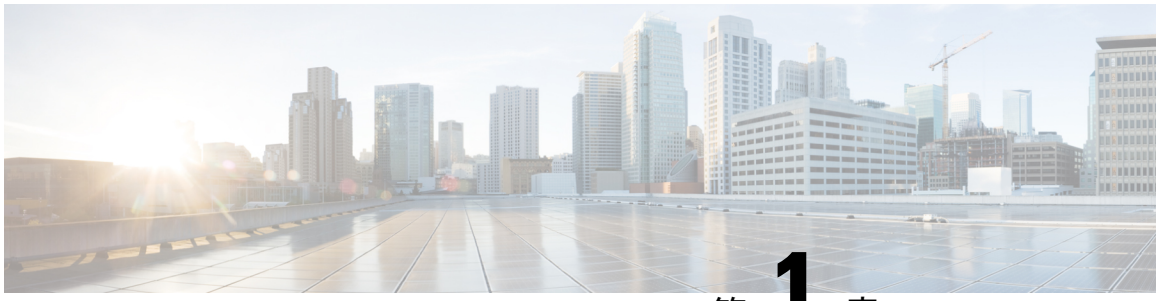
プッシュ通知導入ガイド

最終更新：2024 年 8 月 28 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/

目 次



第 1 章

はじめに

このドキュメントの目的

このドキュメントでは、iOS または Android デバイスで実行される互換性のある Cisco Jabber および Cisco Webex クライアントに対して、Cisco Unified Communications Manager および IM and Presence Service でプッシュ通知を設定する方法について説明します。 プッシュ通知では、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、音声通話、ビデオコール、インスタントメッセージの通知を Cisco Jabber と Cisco Webex for iOS と Android のクライアントにプッシュ することで バックグラウンドで実行されているクライアントに対して通知を送ります。 バックグラウンドで実行されているクライアントとの持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。

このドキュメントでは、以下の展開タイプでプッシュ通知を有効にする方法について説明します。

- プッシュ通知 (オンプレミス展開): Cisco Unified Communications Manager と IM and Presence Service のオンプレミス展開については、第 2 章を参照してプッシュ通知を有効にするためのクラスターの設定方法について説明します。 これには、クライアントが Expressway の Mobile and Remote Access (MRA) 機能経由で登録する展開が含まれます。
- プッシュ通知 (クラウド展開)—Webex Messenger を使ったクラウド展開の場合、第 3 章の展開要件を参照してください。

（注） Webex Messenger クラウドは 2020 年末で廃止されます。詳細については、https://blogs.cisco.com/collaboration/making-the-move-to-modern-messaging を参照してください。

Apple プッシュ通知サービスのアップグレード要件

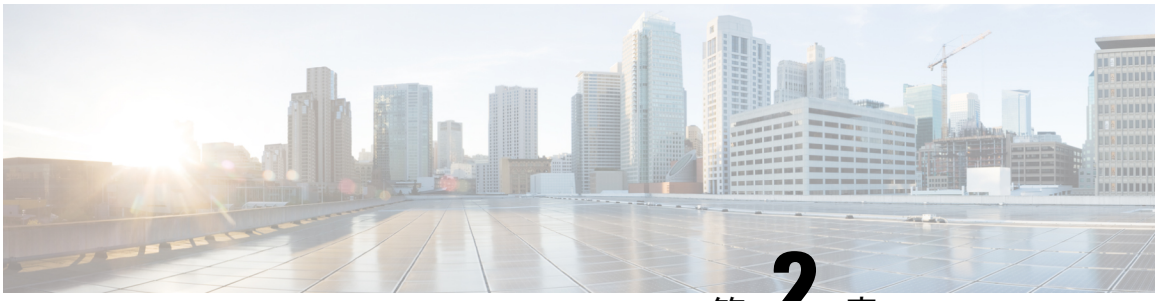
Apple が iOS 通知アーキテクチャに変更したのに合わせ、iOS 上の Cisco Jabber および Cisco Webex クライアントでは、通知用に Apple プッシュ通知サポートが実装されています。Cisco Unified Communications Manager、IM and Presence Service、Cisco Expressway、Cisco Jabber、Cisco Webex を可能な限り早くアップグレードすることを強くお勧めします。アップグレードを適時に行わないと、Cisco Webex iOS ユーザ用の Unified Communications Manager および IM の通知を使用する Cisco Jabber および Cisco Webex iOS ユーザーは、音声通知が利用できなくなります。

重要 Apple Push Notification Service（APNS）が Cisco Unified Communications Manager/IM and Presence クラスタで有効になっていて、Expressway が Push:3 プロトコル対応バージョンにアップグレードされている場合は、まず、すべての Cisco Unified Communications Manager/IM and Presence クラスタを Push:3 プロトコル対応バージョンにアップグレードします。

これは、既存の Cisco Unified Communications Manager/IM and Presence バージョンが、11.5(1)SU8 または 12.5(1)SU3 またはそれ以前（Push:2 対応）でも、Expressway を 12.7（Push:3 対応）にアップグレードされたことを意味します。APNS はこのような展開シナリオでは動作しません。このような場合、Cisco Unified Communications Manager/IM and Presence クラスタを、11.5(1)SU9 などの Push:3 対応バージョンにアップグレードする必要があります。

Apple Push Notification Service には HTTPS が必要であり、制限のないソフトウェアでは機能しません。

アップグレード要件を含む iOS13 以降のバージョンのプッシュ通知関連の最新情報については、「Apple Push Notification Service のアップグレード」を参照してください。



第 2 章

新規および変更情報

新規および変更情報

次の表は、この最新リリースに関するこのガイドでの機能に対する大幅な変更の概要を示したものです。 この表は、ガイドに加えられたすべての変更やこのリリースまでの新機能を網羅したリストではありません。

表 *1 : Unified Communications Manager* と *IM* およびプレゼンスサービスでの新機能と変更された動作

機能または変更	説明	参照先	日付（Date）
リリース 15	「Android プッシュ通知」セクションから、Android デバイスでの VoIP ソケット サポートの廃止を示すメモを削除しました。	Android プッシュ通知 （17 ページ）	2024 年 7 月 10 日
リリース 15	'fos-a.wbx2.com' をファイアウォールの SSL 復号化の除外リストに追加	プッシュ通知の前提条件 （28 ページ）	2024 年 2 月 8 日
リリース 15	このリリースで導入された新しい技術的機能はありません。	—	2023 年 12 月 18 日
リリース 14SU3	このリリースで導入された新しい技術的機能はありません。	—	2023 年 5 月 18 日
「LPNS 相互作用と制限」セクションを更新しました。	Apple の証明書要件を満たすために、LPNS に関する情報が含まれるように証明書要件機能が更新されました。	LPNS 連携動作と制限事項 （54 ページ）	2023 年 7 月 26 日

新規および変更情報

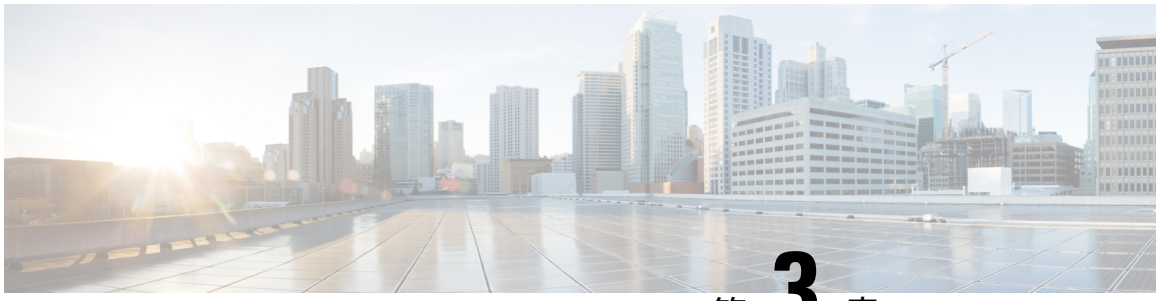
機能または変更	説明	参照先	日付（Date）
Android 版 Cisco Jabber のバージョン更新	「Android プッシュ通知」セクションで、Jabber for Android は Android ターゲット API 34 (Android 14) に更新する必要があることに言及するメモを含めました。	Android プッシュ通知（17 ページ）	2023 年 7 月 21 日
プッシュ通知の最小リリースと機能サポートの表を更新しました。	iOS12 (APNS) の廃止に関する情報を追加しました。	プッシュ通知の最小リリースと機能サポート（25 ページ）	2023 年 7 月 21 日
APNS および LPNS のサポート一覧	APNS および LPNS のサポート マトリックスに関する情報を追加しました。	• プッシュ通知の概要（7 ページ） • プッシュ通知の最小リリースと機能サポート （25 ページ）	2023 年 5 月 25 日

新規および変更情報

機能または変更	説明	参照先	日付（Date）
通話用 iOS ローカルプッシュ接続機能	インターネット接続がなく、Wi-Fi 接続に制限のあるネットワーク環境（病院、クルーズ船、飛行機など）で iOS デバイスを使用する場合、Webex アプリは VoIP の着信通話の通知を受け取りません。インターネットに接続できない場合、Apple プッシュ通知サービス（APNS）にデバイスからアクセスすることができません。 ユーザーは通話を遅延なしで受信したいと思っても、ネットワークの速度が遅い場合は、APNS での通話に数秒の遅延が発生する場合があります。 今回のリリースで、ローカルプッシュ通知サービス（LPNS）が Apple デバイスでの通話用に導入されています。 これにより、永続的接続を使用してクライアントにプッシュメッセージが送信されるため、遅延を最小限に抑えることができます。	• ローカルプッシュ通知サービス （49 ページ） • LPNS 前提条件 （50 ページ） • ローカルプッシュ接続の仕組み （50 ページ） • Wi-Fi SSID の設定 （52 ページ） • Jabber サービス プロファイルをエンドユーザに関連付ける （53 ページ） • Unified Communications Manager のフェイルオーバーがある場合の LPNS の動作 （54 ページ） • リモート LPNS プッシュ通話処理のための LPNS の高可用性 （54 ページ） • LPNS のポートを開く （50 ページ） • LPNS 連携動作と制限事項 （54 ページ） • LPNS アラーム （73 ページ） • LPNS のパフォーマンス カウンター （74 ページ）	2023 年 5 月 18 日
リリース 14SU2	このリリースで導入された技術的機能はありません。	—	2022 年 6 月 16 日

新規および変更情報

機能または変更	説明	参照先	日付（Date）
リリース 14SU1	このリリースで導入された技術的機能はありません。	—	2021 年 10 月 27 日
リリース 14	システムガイドの最初の公開。	—	2021 年 3 月 31 日
リリース 12.5.x	Cisco Jabber サポートの情報が含まれています。	プッシュ通知の概要（7 ページ）	2020 年 8 月
リリース 11.5(1)SU3	iPhone および iPad の Cisco Jabber のプッシュ通知の機能強化に関する情報が含まれています。	プッシュ通知の概要（7 ページ）	2017 年 8 月
リリース 11.5(1)SU2	IM and Presence (高可用性なし) に提供されるプッシュ通知のサポート。	IM および Presence のプッシュ通知の高可用性（23 ページ）	2017 年 1 月



第 3 章

プッシュ通知 (オンプレミス展開)

プッシュ通知の概要

クラスターでプッシュ通知が有効になっている場合、Cisco Unified Communications Manager と IM and Presence Service は Apple または Google クラウドのプッシュ通知サービスを使用して、iOS または Android デバイスで動作する互換性のある Cisco Jabber または Webex クライアントにプッシュ通知を送信します。プッシュ通知により、システムはクライアントと、バックグラウンドモード (一時停止モードとも呼ばれます) になった後でも、クライアントと通信できます。プッシュ通知がないと、システムはバックグラウンドモードになっているクライアントに通話やメッセージを送信できない場合があります。

プッシュ通知の暗号化されたペイロードには、以下の PII 情報が含まれます。

- 表示名
- 表示番号
- ハントパイロットDN

次の表には、Apple プッシュ通知サービス (APNS) とローカル プッシュ通知サービス (LPNS) のサポート マトリックスが詳しく記載されています。

表 *2: APNS* および *LPNS* のサポート一覧

	Unified CM	IM and Presence Service	Cisco Expressway (MRA が展開されている場合)	Cisco Jabber	Webex アプリ	モバイルオペレーティングシステム	注
Apple - APNS メッセージング	11.5(1)SU2	11.5(1)SU2	X8.9.1	11.8.1	該当なし	12	Apple および Cisco クラウドとの接続が必要です。
Apple - APNS 通話	11.5(1)SU3	11.5(1)SU3	X8.10.1	11.9.0	40.6	12	—
Apple—APNS CallKit	11.5(1)SU8 および 12.5(1)SU3 および 14	該当なし	X12.6	12.9	40.6	13	—
Apple—APNS 中国地域	12.5(1)SU3 および 14	12.5(1)SU3	X12.6	12.9 MR	41.4	13	—
Android - FCM	12.5(1)SU3 および 14	12.5(1)SU3	X12.6.2	12.9.1	40.8	8.0	Google および Cisco クラウドとの接続が必要です。
Apple—LPNS	14SU3	該当なし	サポート対象外	14.2	43.6	16.5	Wi-Fi 展開がサポートされています

Unified Communications Manager および IM and Presence Service の展開では、プッシュ通知は次のクライアントにより使用されます。

表 *3:* プッシュ通知を使用する互換性のあるクライアント *(*オンプレミス展開*)*

通信タイプ	プッシュ通知を使用するクライアント	オペレーティングシステム	パートナークラウドサービス	ローカルプッシュ接続
通話	iPhone または iPad の Cisco Jabber iPhone または iPad 版 Cisco Webex	iOS	Apple プッシュ通知サービス (Apple クラウド内)	Unified CM バージョン 14SU3 および Webex アプリ 43.6 以降または Cisco Jabber 14.2 以降でサポートされています。
通話	Android の Cisco Jabber Android 版 Cisco Webex	Android	Android プッシュ通知サービス (Google クラウド内)	サポート対象外
メッセージ*	iPhone または iPad の Cisco Jabber	iOS	Apple プッシュ通知サービス (Apple クラウド内)	サポート対象外
メッセージ*	Android の Cisco Jabber	Android	Android プッシュ通知サービス (Google クラウド内)	サポート対象外

* メッセージングの場合、Webex アプリ クライアントは IIM and Presence Service ではなく Webex アプリ クラウドに登録します。

（注） iOS と Android の特定のプッシュ通知機能の最小リリース情報については、『プッシュ通知の最小リリースと機能サポート （25 ページ）』を参照してください。

プッシュ通知の動作

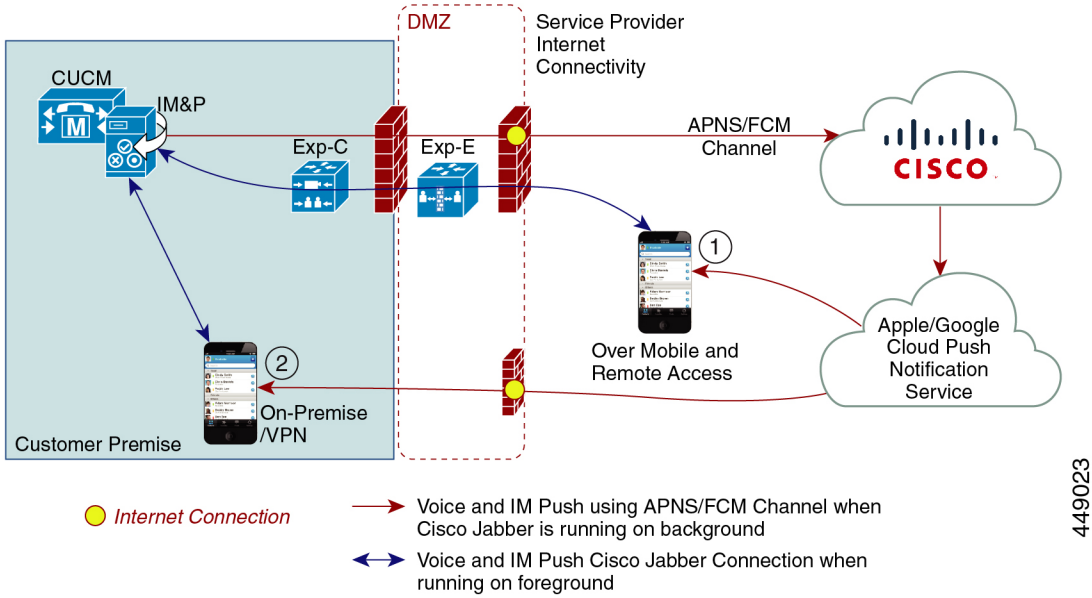
起動時に、Android および iOS プラットフォーム デバイスにインストールされた Cisco Jabber クライアントは Unified Communications Manager と IIM and Presence Service に登録し、Android または iOS で実行される Webex アプリクライアントは通話用に Unified Communications Manager に登録し、メッセージング用には Webex アプリクラウドに登録します。 さらに、Jabber および Webex クライアントは、実行しているプラットフォームに応じて、Google または Apple クラウドにも登録します。クライアントがフォアグラウンドモードである限り、通話やメッセージをクライアントに直接送信できます。

ただし、クライアントがバックグラウンドモードに移行すると (たとえば、バッテリーの寿命を維持するために移行する場合)、標準の通信チャネルが利用できないため、クライアントとの直接通信ができなくなります。プッシュ通知は、パートナークラウド (Apple または Google) を通じてクライアントに到達するための代替チャネルを提供します。

（注） 以下の条件のいずれかに該当する場合、Cisco Jabber および Webex アプリのクライアントは中断モードで実行されていると見なされます。

- Cisco Jabber または Webex アプリがオフスクリーン (バックグラウンド) で実行されている場合。
- Android または iOS デバイスがロックされている場合。
- Android または iOS デバイスの画面がオフになっている場合。

図 *1*: プッシュ通知のアーキテクチャ



上の図は、Android および iOS 用 Cisco Jabber クライアントがバックグラウンドで実行中または停止した場合に何が起こるかを示しています。標準チャネルが利用できないため、プッシュ通知は Cisco クラウドの Push REST サービスに送信され、Cisco クラウドは通知を適切なパートナー クラウド (Apple または Google) に転送し、パートナー クラウドはプッシュ通知をクライアントに転送します。クライアントは、通話またはメッセージを受け入れるために、オンプレミス展開に再登録します。

この図には、（1）Cisco Jabber クライアントが Expressway 経由でオンプレミスの Cisco Unified Communications Manager および IM and Presence Service の展開に接続している MRA 展開と、（2）エンタープライズ ネットワーク内からオンプレミス展開に直接接続する Cisco Jabber for Android または iOS のクライアントが示されています。

（注） Windows と iOS デバイスに同時にログインしている Jabber ユーザの場合:

- 2 人のユーザがアクティブな通話を行っており、別のユーザがメッセージを送信すると、プッシュ通知が iOS デバイスに送信されます。
- ユーザがアクティブな通話中でない場合、別のユーザがメッセージを送信しても、iOS デバイスにプッシュ通知は送信されません。

プッシュ通知の動作

次の表は、Unified Communications Manager および IM and Presence Service のオンプレミス展開でのプッシュ通知クライアントの動作を示します。

（注） Webex アプリ クライアントは、メッセージングにオンプレミスの IM およびプレゼンス サービスではなく、Webex アプリ クラウドを使用します。

（注） IOS 上の Webex アプリと Cisco Jabber は、Apple IOS CallKit の制限により、常にビデオ コールとして表示されます。

表 *4 : iOS* または *Android* の *Cisco Jabber* または *Webex* クライアントのプッシュ通知の動作

Cisco Jabber または **Webex** クライアントは次の状態にあります...	**iOS12** を実行中	**iOS13** 以上のバージョンまたは **Android** を実行中
フォアグラウンドモード	**音声通話とビデオ コール** Unified CM は、SIP チャネルを使用して、通話を Cisco Jabber または Webex クライアントに直接送信します。 さらに、Unified CM はフォアグラウンド モードのクライアントにプッシュ通知を送信します。 ただし、プッシュ通知は通話を確立するために使用されません。代わりに、標準 SIP チャネルが使用されます。 **メッセージ (Jabber のみ)** IM and Presence Service は、標準の通信チャネルを使用して、Cisco Jabber にメッセージを直接送信します。 IM およびプレゼンス サービスは、フォアグラウンドモードのクライアントにプッシュ通知を送信しません。	**音声通話とビデオ コール** Unified CM は、SIP チャネルを使用して、通話を Cisco Jabber または Webex クライアントに直接送信します。 さらに、Unified CM はフォアグラウンド モードのクライアントにプッシュ通知を送信します。 ただし、プッシュ通知は通話を確立するために使用されません。代わりに、標準 SIP チャネルが使用されます。 **メッセージ (Jabber のみ)** IM and Presence Service は、標準の通信チャネルを使用して、直接 Cisco Jabber にメッセージを送信します。 IM and Presence Service は、フォアグラウンド モードのクライアントにプッシュ通知を送信しません。

Cisco Jabber または Webex クライアントは次の状態にあります...	iOS12 を実行中	iOS13 以上のバージョンまたは Android を実行中
バックグラウンドモード	**音声通話とビデオ コール** SIP チャネルは利用できません。Unified CM はプッシュ通知チャネルを使用します。プッシュ通知を受信すると、クライアントは Unified CM に再登録し、SIP チャネル経由で SIP INVITE を受信します。 **メッセージ (Jabber のみ)** 標準チャンネルは利用できません。IM およびプレゼンス サービスはプッシュ通知チャネルを使用して、IM 通知を Jabber に送信します。 ユーザが通知をクリックすると、クライアントはフォアグラウンドモードに移行し、IM およびプレゼンス サービスとのセッションを再開し、メッセージをダウンロードします。 （注） クライアントがバックグラウンドモードの場合、プレゼンス状況は **退席中**。	**音声通話とビデオ コール** SIP チャネルは通話には利用できません。 Unified CM はプッシュ通知の「VoIP」チャネルを使用します。プッシュ通知を受信すると、クライアントは発信者 ID で CallKit を起動し、Unified CM に再登録し、SIP チャネル経由で SIP INVITE を受信します。 ユーザは着信に応答できます。 **メッセージ (Jabber のみ)** 標準チャンネルは利用できません。IM およびプレゼンス サービスはプッシュ通知の「メッセージ」チャネルを使用して、IM 通知を Jabber に送信します。ユーザが通知をクリックすると、クライアントはフォアグラウンド モードに移行し、IM およびプレゼンス サービスとのセッションを再開し、メッセージをダウンロードします。 （注） クライアントがバックグラウンドモードの間、プレゼンス状況は **[退席中（Away）]** になります。

Apple プッシュ通知

Cisco Jabber および iOS で実行される Cisco Webex クライアント (例えば、iPhone および iPad 上の Cisco Jabber) は、Apple クラウドで実行される Apple プッシュ通知サービスからプッシュ通知を受け取ります。

Cisco Jabber 12.9 リリースから、すべての新しい iOS アプリケーションと更新は iOS 13 以降のバージョンを使用して構築されます。 iOS 13 では、Apple は、中断されたアプリケーションのプッシュ通知を iOS 12 の場合とは異なる方法で処理します。

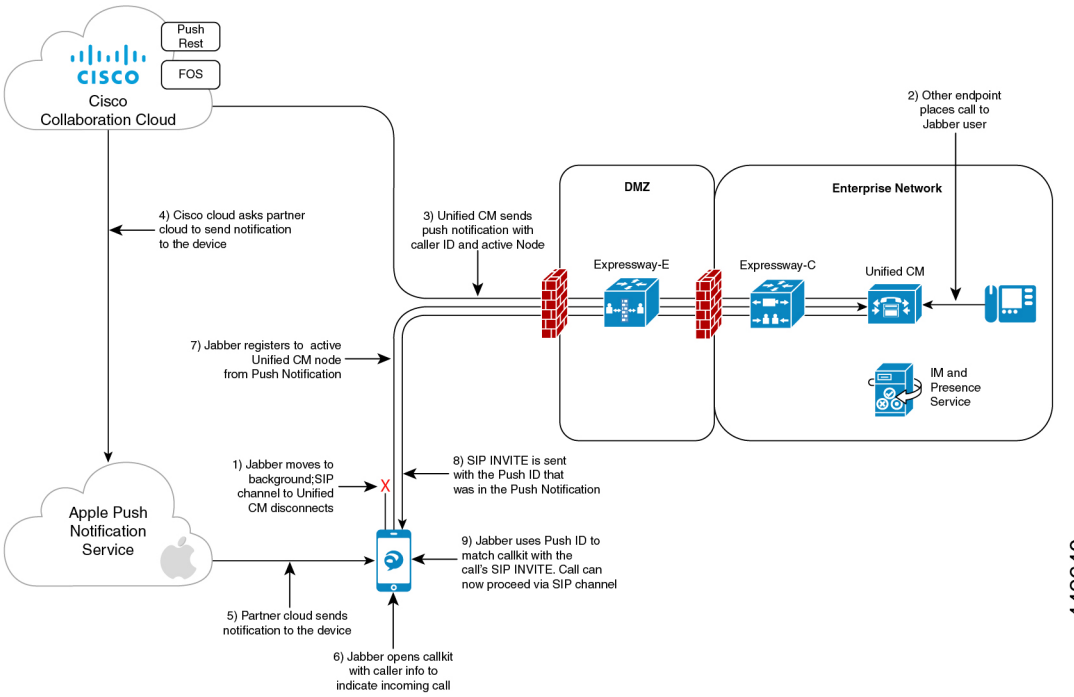
- iOS 13 でのプッシュ通知は、通話用の「VoIP」チャネルとメッセージング用に別の「メッセージ」チャネルを使用して配信されます。 iOS 12 とは対照的です、すべてのプッシュ通知トラフィックが同じチャネルを使用して配信されます。

- 2020 年 8 月の時点で、Apple iOS クライアントではプッシュ通知が必須です。
- iOS クライアントは通知を受け取るとすぐに CallKit を起動し、着信を知らせます。
- プッシュ通知の「VoIP」トラフィックには、発信者 ID 情報 (表示名、番号) が含まれます。クライアントは、この情報を使用して、CallKit の CallerID フィールドに入力します。外部プレゼンテーションの名前と番号が構成されている場合、プッシュ通知はサポートされているデバイスでカスタマイズされた識別名と番号を表示します。そうでない場合は、発信者の元の名前と番号が着信側のデバイスに表示されます。
- **不在着信通知**: 発信者が進行中の発信通話を切断すると、2 回目のプッシュ通知が Push 対応デバイスに送信されます。 プッシュ通知は、プッシュ対応デバイスが 13 秒以内に着信を登録しない場合にも送信されます。
- **共有回線**: 他のデバイスとの共有回線を持つプッシュ通知対応デバイスがコールを受け取り、共有デバイスがコールに応答すると、プッシュ通知対応デバイスは、他のデバイスからの応答があったことを示す 2 番目のプッシュ通知を受信します。
- タイプが「VoIP」のプッシュ通知は高優先度と見なされ、遅延なく配信されます。

（注） Unified CM リリースでどのプッシュ通知機能がサポートされるかについての詳細は、プッシュ通知の最小リリースと機能サポート （25 ページ） を参照してください。

以下の画像は、iOS13 以降のバージョンで VoIP プッシュ通知が送信されたときに何が起こるかの内訳を示しています。

図 *2 : iOS13* 以上のバージョンで送信された場合の *VoIP* プッシュ通知の動作



iOS13 以上のバージョンと APNS の変更を含む Cisco Jabber または Webex アプリ クライアントのプッシュ通知の通話エクスペリエンスの比較

以下の表は、クライアントがアップグレードされ、サーバがアップグレードされない場合、またはクライアントがアップグレードされず、サーバがアップグレードされる場合のユーザエクスペリエンスのビヘイビアを示しています。

	ロックされた画面	ロック解除された画面
Cisco Jabber 12.9	• クライアントはプッシュ通知を受け取ります。 • CallKit ビューと発信者の CallerID が画面に表示されます。 • ユーザは、デバイスのロックを解除することなく、CallKit からの通話に応答したり、拒否したりできます。	• クライアントはプッシュ通知を受け取ります。 • CallKit ビューと発信者の CallerID が着信通知に表示されます。 • Cisco Jabber アプリは、ユーザが通話に応答し、発信者の詳細情報 (発信者名と発信者番号) とともに起動します。

	ロックされた画面	ロック解除された画面
Cisco Jabber 12.8 以前	• クライアントはプッシュ通知を受け取ります。 • この通知により、Cisco Jabber アプリが起動します、ユーザにはその中の通話情報が表示されます。 • ユーザはロックされたデバイスから着信に応答できます。	• クライアントはプッシュ通知を受け取ります。 • この通知により、Cisco Jabber アプリが起動します、ユーザにはその中の通話情報が表示されます。 • ユーザはアプリから直接着信に応答できます。

（注） メッセージ プッシュ通知のユーザ エクスペリエンスの動作に変更はありません。

プッシュ通知のクラウド セキュリティ

セキュリティは、Cisco Jabber および Cisco Webex アーキテクチャへの取り組みの中心にあります。 すべてのプッシュ通知コンテンツは、ユーザのサインイン時に Cisco Jabber および Cisco Webex によって定義された 256 ビットの高度暗号化標準 (AES) キーを使用して暗号化されます。クライアントがキーを定期的に更新することもできます。プッシュ通知の一部として送信されるすべてのコンテンツは暗号化されます。

Cisco のクラウドプッシュ サービスは暗号化されたペイロードを必要とし、Apple または Google クラウドに送信する前に暗号化されていないものをすべて拒否します。 Cisco のクラウドプッシュ サービスとのすべての通信は、Transport Layer Security (TLS) を使用して保護されています。 これにより、APNS を通じてプッシュされるコンテンツが暗号化されます。

PushRest サービスは、オンプレミス サーバから取得したペイロードをキャッシュしません。PushRest サービスはプロキシであり、情報を Apple または Google クラウドに渡します。

すべての個人識別情報 (PII) は暗号化されます。 サービスの詳細以外で暗号化されたペイロードには含まれないが、安全な TLS 接続で送信される情報は次のとおりです。

- プッシュ ターゲットは、特定のプッシュ セッション デバイス用にクライアント (APNS または場合によっては FCM) が生成したトークンで、不定期に更新されるか、以降のサインインで変更されます。
- トラッキング ID (問題が発生した場合のデバッグに使用される、クライアントが各メッセージに対して生成した ID)

iOS13 プッシュ通知 (中国地域)

Unified Communications Manager は、iOS13 以降のバージョンのデバイスで実行されている Cisco Jabber または Webex クライアントの VoIP 通話プッシュ通知をサポートしています。 さらに、IM およびプレゼンス サービスは、iOS13 以降のバージョンのデバイスで実行される Cisco Jabber

クライアントのメッセージ プッシュ通知をサポートします。 中国本土地域にあるプッシュ通知対応デバイスへの着信通話を取得すると、規制要件により、iOS デバイスで実行されているクライアントはCallKit ビューを表示できません。 代わりに、名前や番号などの発信者 ID の詳細を含むメッセージ通知が表示されます。

中国本土地域の iOS13 以降のバージョンの Cisco Jabber および Cisco Webex クライアント:

- VoIP 通話のプッシュ通知メッセージを受け取ると、CallKit ビューを表示できません。
- VoIP 通話プッシュ通知メッセージにより、アプリケーションは着信通話と発信者 ID に関する情報を含むメッセージ トーストを表示します。

これにより、エンドユーザは、呼び出しに応答する前に、発信者を確実に確認できます。 アプリケーションのメッセージ通知をタップして、Unified Communications Manager で登録を開始します。 登録が完了すると、 Unified Communications Manager は着信をアプリケーションにルーティングします。

（注） ユーザは Cisco Jabber および Cisco Webex クライアントのメッセージ通知をすばやくタップ Unified Communications Managerすることで、通話をユーザにルーティングすることをお勧めします。 ユーザが設定された時間 (13 秒) 内にメッセージ通知をタップしなかった場合、着信は CallKit で受信者にアラートすることはなく、不在着信メッセージ通知がユーザに送信されます。

中国地域のプッシュ通知は iOS デバイスのみが対象で、最小リリースは 12.5(1)SU3 です。 Android デバイスではサポートされていません。

Cisco Jabber 12.9 MR が必要です。 IM and Presence Serviceのプッシュ通知はこの規制の影響を受けません。

Android プッシュ通知

12.5(1)SU3 Unified Communications Manager では、Android デバイスで実行される Cisco Jabber または Webex クライアントの VoIP プッシュ通知をサポートしています。 さらに、IM and Presence Service は Android クライアントの Cisco Jabber のメッセージングプッシュ通知をサポートします。

電話がかかってくると、 Unified Communications Manager プッシュ通知サービス (CPNS) は Google クラウドを介して、中断モードまたはバックグラウンドモードで実行中の Android クライアントにプッシュ通知を送信します。 通知の受信後、Cisco Jabber または Webex クライアントは通話を受信するために Unified Communications Manager に登録し直します。

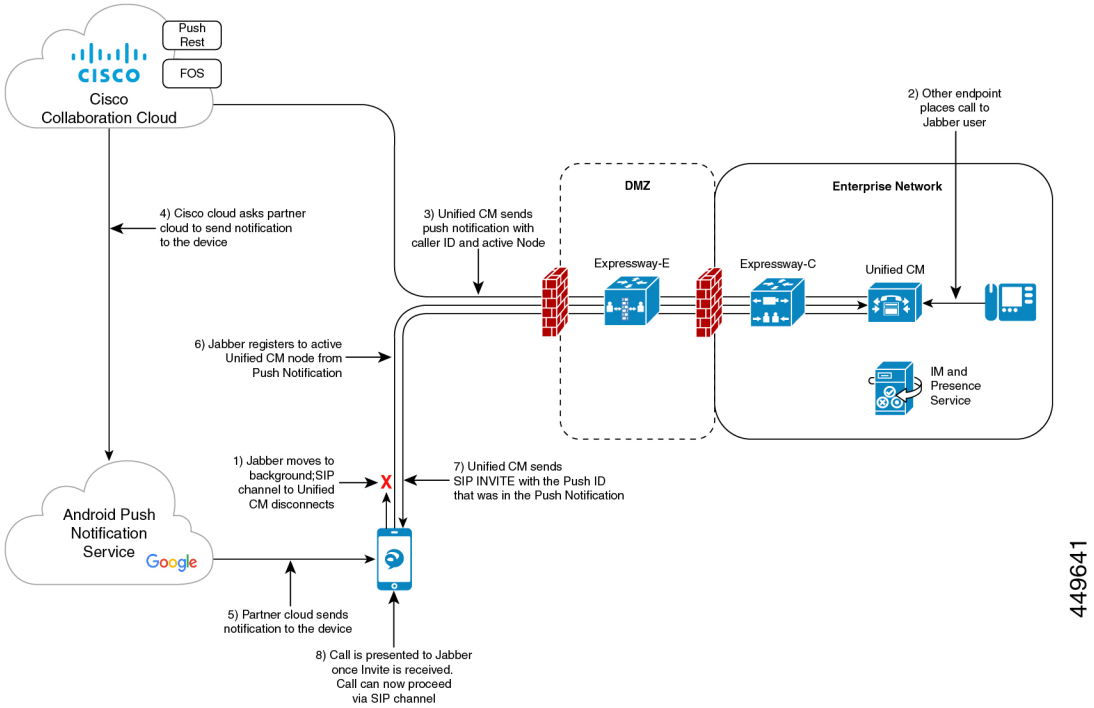
（注）

- Cisco Webex の Android プッシュ通知は音声通話の通知専用です。 メッセージングでは、Cisco Webex はオンプレミスの IM and Presence Service サーバを使用しません。

  IM and Presence Service 12.5 SU3 が Expressway X12.6 および Cisco Jabber 12.9 バージョンで展開される場合、バグ ID CSCvv12541 は適用されず、Android の Cisco Jabber ユーザは問題はありません。

- Android では、Cisco Jabber または Webex クライアントと Unified CM サーバ間のキープアライブ接続が常に機能しているという保証はありません。 そのため、Cisco Jabber または Webex クライアントがバックグラウンドにある間に、FCM (Firebase Cloud Messaging) を使用する Cisco Cloud Onboarding で、確実にチャットメッセージ (Cisco Jabber のみ) と通話を受信できるようにすることをお勧めします。

図 *3:* バックグラウンド モードでの *Android* プッシュ通知の呼び出し処理



（注）

Google クラウドからの Android プッシュ通知サービスを使用した Cisco Jabber および Cisco Webex クライアント ユーザのサインインの一部として、サブスクライバー サービス FCM (Firebase Cloud Messaging) および FCM: dev がサポートされています。

Unified Communications Manager フェイルオーバー時のプッシュ通知

Unified Communications Manager グループは、デバイスを登録できる最大 3 つの冗長サーバの優先順位リストです。 各グループには、1 個のプライマリ ノードと最大 2 個のバックアップ ノードが含まれます。 一覧表示するノードの順序によって優先順位が決まります。最初のノードがプライマリノード、2 番目がバックアップノード、3 番目がターシャリノードになります。

Unified Communication Manager では、デバイスプールはデバイスのグループに共通の設定セットを提供し、特定のロケーション情報に従ってデバイスを設定できるようにします。 [デバイスプールの設定] を通じて、デバイスを Cisco Unified Communications Manager グループに指定することができます。

Cisco Jabber または Cisco Webex クライアントがバックグラウンドまたは一時停止状態に移行し、クライアントが登録されているプライマリノードがネットワークから外れる、またはクラッシュした場合、Cisco Jabber または Cisco Webex へのすべての通話が Unified CM からプッシュ通知をトリガーします。

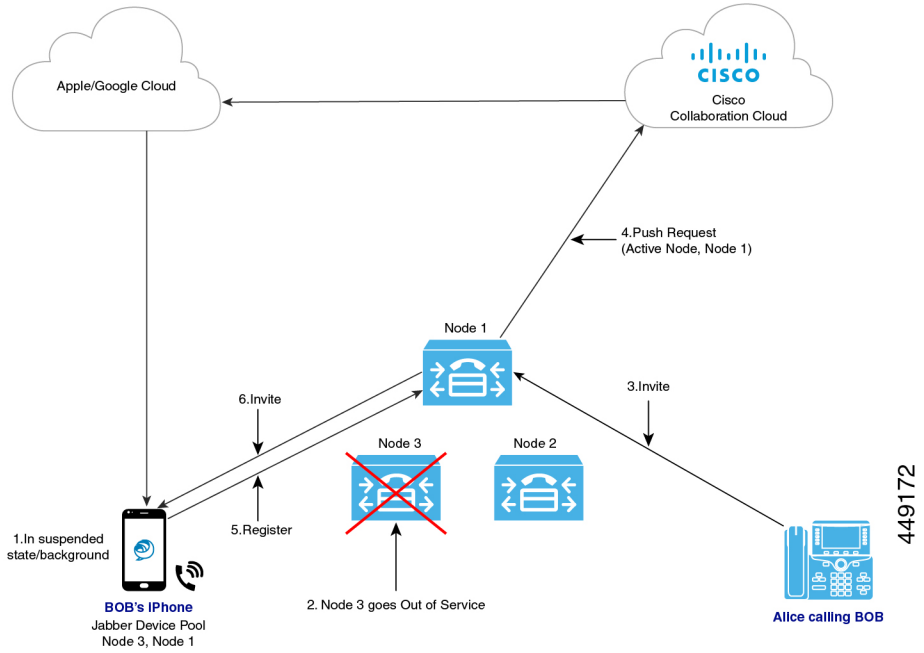
以前、Cisco Jabber または Cisco Webex は以前に登録したノードへの登録を試みましたが、登録に失敗しました。 現在は、その後正常に登録し直すために、デバイス プール内のアクティブノードに接続しようとします。 Cisco Jabber または Cisco Webex クライアントが登録する必要がある現在のアクティブノードを検出するこのプロセスは時間の損失につながります。

Unified Communications Manager プッシュ通知サービス (CPNS) は、プッシュ通知が送信されるたびに、Cisco Jabber または Cisco Webex を正しいアクティブノードに登録できるようにすることで、損失や遅延を回避することを目的としています。 このプッシュ通知リクエストには現在のアクティブノード情報が含まれているため、クライアントは同じノードまたは現在のアクティブノードにすばやく登録し直すことができます。

（注） 12.5(1)SU3 リリース以降、アクティブ ノードはプッシュ通知にのみ含まれます。

図 *4 :* 着信のプッシュ通知

次の画像は、 Unified Communications Manager のフェイルオーバーの例を示しています。この例では、クライアントがバックグラウンドモードまたはサスペンド状態の間、プライマリノードがアウトオブサービスになります。 クライアントの着信コールを受信すると、 統合通信マネージャーは、アクティブノードとしてバックアップノードをハイライト表示したプッシュ通知を送信します。プライマリ登録ノードがダウンしているからです。 プッシュ通知を受信したクライアントは、バックアップノードに登録します。

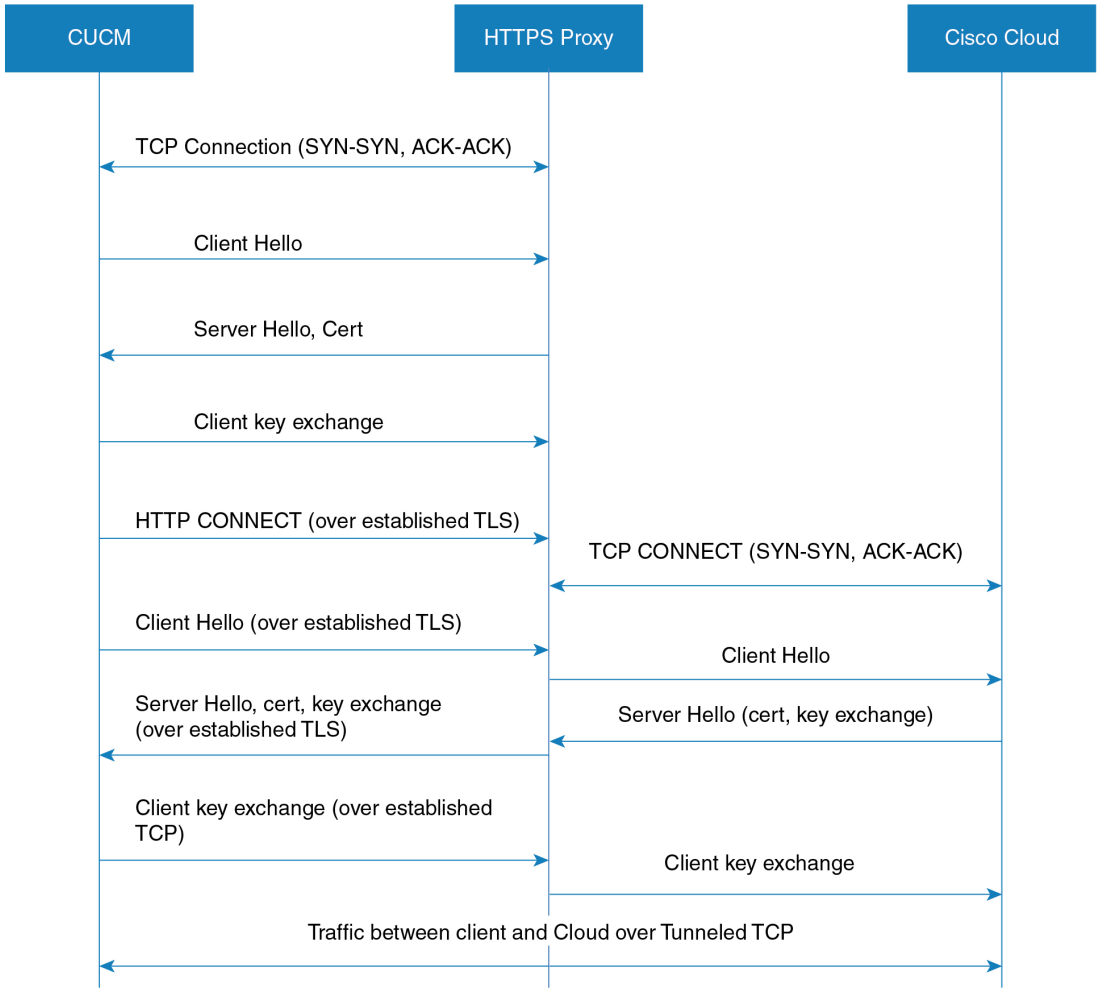


クラウド接続のプロキシサポート

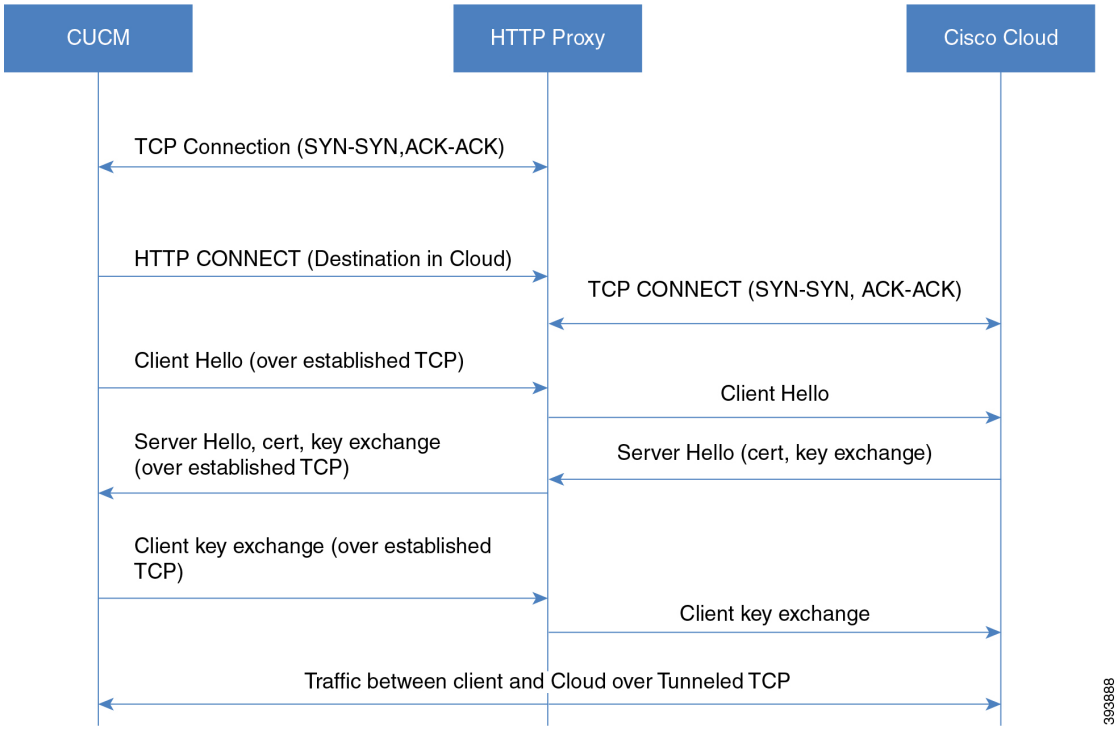
一部の導入では、プロキシサーバーを使用して Cisco Cloud に接続する必要がある場合があります。これは、オンプレミスの展開が企業のファイアウォールの背後にあり、クラウドへの直接アクセスを許可しない場合に特に当てはまります。

Unified Communications Manager は、Cisco Web セキュリティアプライアンスを HTTPS プロキシサーバとしてサポートしています。ただし、以下のいずれかのコールフローをサポートする HTTP または HTTPS プロキシサーバーを使用することができます。認証を有効にして HTTP プロキシを使用する場合は、ログイン情報のセキュリティのためにプロキシサーバーのダイジェスト認証を設定することを推奨します。

HTTPS プロキシのサポートされているコールフロー



HTTPS プロキシのサポートされているコールフロー



プロキシサーバーのキャパシティの要件

プッシュ通知用の Proxy Server Capacity Calculator を使用して、プロキシサーバーが処理できるキャパシティを推定します。導入に適用される情報を入力すると、この計算ツールはHTTP プロキシサーバーがプッシュ通知の展開で処理できる必要があるトランザクション数を出力します。

プロキシサーバーの DNS 要件

- Unified Communications Manager でプロキシサーバ接続を設定する場合、プロキシサーバーの FQDN アドレスを使用すると、DNS がプロキシサーバへの接続に使用されます。プロキシサーバーの FQDN が複数の IP アドレスに解決される場合、Unified Communications Manager は最初の IP アドレスを試行して 2 秒待機してから、2 番目のアドレスに進みます。
- プッシュ通知を送信した後、Unified Communications Manager は確認を 5 秒待機してから、2 番目のアドレスを試行します。
- Cisco cloud 接続用のプロキシサーバーでは、接続の失敗に対するフェールオーバープロセスを高速化するために、プロキシサーバーを低いフェールオーバーレートで設定することを推奨しています。
- Cisco Web Security アプライアンスを導入している場合、FQDN は WSA の仮想 IP アドレスにマップする必要があります。

（注） プロキシ IP アドレスのデフォルトの有効期限 (TTL) は、1 時間になります。そのため、IP アドレスが変更された場合、その変更が DNS 要求に対して利用可能になるまでに最大 1 時間かかることがあります。

IM および Presence のプッシュ通知の高可用性

プッシュ通知高可用性は、Cisco Jabber Android および iOS クライアントのプッシュ通知が有効な IM および Presence セッションのフェイルオーバーと冗長性を提供します。 この機能により、IM およびプレゼンス サービスは IM セッションをローカルのメモリ内データベース (IMDB) に保存し、これはバックアップサブクラスタノードのメモリ内データベースに自動的に複製されます。 これにより、バックアップ ノードがセッション情報を持ち、ユーザによるアクションなしでセッションを引き継ぐことができます。

IM 履歴

プッシュ通知の高可用性が設定されている場合、フェールオーバーが発生しても Cisco Jabber ユーザはチャット履歴を失いません。

Jabber が一時停止モードの場合の未読メッセージキュー

プッシュ通知対応 IM セッションで、Cisco Jabber for Android および iOS クライアントが一時停止モードに移行すると、IM and Presence Service はクライアントにプッシュ通知を送信しますが、未読のインスタントメッセージ、プレゼンスの更新、その他の XMPP スタンザ（チャットルームの招待など）の送信を停止します。代わりに、これらのメッセージは、クライアントがプッシュ通知をクリックするか、フォアグラウンドモードに戻るまで、ローカルサーバのキューに入れられます。

Cisco Jabber が一時停止モードの場合、プッシュ通知が有効な IM セッションの未読メッセージキューに関する制限があります。一部のフェイルオーバーの使用例では、未読メッセージキューは失われます。 これが発生するときの説明については、「冗長性とフェイルオーバーの使用例」を参照してください。

冗長性とフェイルオーバーの使用例

この機能は、次の使用例に対応します。

- ノード障害 (自動フェイルオーバー) - ノードに突然障害が発生すると、バックアップ ノードが IM セッションを引き継ぎ、Cisco Jabber ユーザへのプッシュ通知は引き続きバックアップ ノードから送信されます。 ユーザは操作を実行したり、IM 履歴を失うことなく、作業を続けることができます。 しかし、クライアントが中断モードの間、障害が発生したサーバでまだクライアントに送信されていない未読メッセージは失われます。
- ノードのシャットダウン (手動フェールオーバー): ノードが正常にシャットダウンされると、バックアップ ノードが IM セッションを引き継ぎ、プッシュ通知は引き続き送信されます。今回はバックアップ ノードから送信されます。 ユーザは、IM 履歴を失うことな

く、作業を続けることができます。 元のノードでキューに入れられ、Jabber クライアントに送信されるのを待っていた未読メッセージは、バックアップ ノードが引き継ぐときに一時的に失われます。 しかし、元のノードが復帰し、ユーザが元のノードに戻った後、メッセージキューが取得され、ユーザに送信されます。

- Cisco XCP Router のクラッシュ—Cisco XCP Router が突然クラッシュした場合、ルーターが復帰すると、ノードはセッションを再開し、プッシュ通知を送信し続けます。 IM 履歴は保持され、Cisco Jabber ユーザはアクションなしで作業を続行できます。 ただし、ルーターがクラッシュする前にサーバのキューにあった未読メッセージで、まだクライアントに送信されていなかったものは、失われます。
- Cisco XCP Router の再起動—管理者が Cisco XCP Router を再起動する場合 (設定の更新後などに発生する可能性があります)、IM 履歴と未読メッセージキューの両方が保持されます。 ルーターが再起動すると、IM およびプレゼンス サービスはプッシュ通知の送信を再開します。 未読メッセージ キューは、Jabber クライアントが再度ログインすると送信されます。

（注） 音声およびビデオ コールの場合、冗長性とフェイルオーバーは Cisco Unified Communications Manager グループによって処理されます。

Push v3 対応デバイスの HA イベント中のサポートされている再ログイン率

このセクションでは、展開のニーズに応じて、PUSH v3 対応デバイスの HA イベント中のクライアント再ログイン レートを計算する方法に関する情報を提供します。

この手順は、15,000 OVA があり、以下の順序で配布されていることを前提としています。

- IM and Presence パブリッシャーノードに登録されている 2,000 人のユーザが Push v3 を有効にしており、
- IM and Presence パブリッシャーノードに直接登録されている 5,500 人のユーザでプッシュが有効になっていません。
- IM and Presence サブスクライバノードに直接登録されている 7,500 人のユーザーでプッシュが有効になっていません。

高可用性イベントの場合、サポート対象のフェイルオーバー率は 4 ユーザ/秒、またはそれ以下でなければなりません。 次の測定を使用して、このレートを達成できます。

クライアントの再ログインの下限が 200 に設定されている場合、クライアントの再ログインの上限は 2075 に設定され、再ログイン率は次のように計算されます。

7500/(2075-200)= 4 ユーザ/秒

（注）
- 上記の結果は UCS-C220-M4S Intel Xeon CPU E5-2660 v4@2.00GHz プラットフォームで測定されました。
- この計算は、IM and Presence リリース 11.5 の展開にのみ適用できます。

プッシュ通知の最小リリースと機能サポート

最小リリーズ

次の表に、基本的なプッシュ通知をサポートするための最小リリースを示します。

（注） 特定のプッシュ通知機能に必要な最小リリースについては、「プッシュ通知の機能サポート」の表を参照してください。

オペレーティング システム	プッシュ通知の最小リリース
iOS16.5 以降（LPNS）	• Unified Communications Manager 14SU3 • Cisco Jabber 14.2 • Cisco Webex アプリ 43.6 • IM and Presence Service メッセージングではサポートされていません • Android ではサポートされていません
iOS12（APNS） （注） 未サポート。詳細については、https://www.cisco.com/c/en/us/support/docs/field-notices/705/fn70555.htmlを参照してください。	• Unified Communications Manager 11.5(1)SU4 以上（推奨：11.5(1)SU7 または 12.5(1)SU2） • IM and Presence Service 11.5(1)SU4 以上（推奨：11.5(1)SU7 または 12.5(1)SU2） • Cisco Jabber 11.9（推奨：12.8） • Cisco Expressway X8.10.1：MRA が展開されている場合（推奨：X12.6）

オペレーティング システム	プッシュ通知の最小リリース
iOS13 以降（APNS）	• Unified Communications Manager 11.5(1)SU8（11.x リリースの場合）、12.5(1)SU3（12.x リリースの場合） • IM and Presence Service 11.5(1)SU8（11.x リリースの場合）、12.5(1)SU3（12.x リリースの場合） • Cisco Jabber 12.9 • Cisco Expressway X12.6（MRA が展開されている場合） （注） 最小リリースへのアップグレードとプッシュ通知機能がすでに有効になっている場合は、Expressway をアップグレードする前に、最初にすべての IM and Presence Service クラスタをアップグレードする必要があります。 Expressway をバージョン X12.7 以降にアップグレードし、IM and Presence Service を 11.5(1)SU8 または 12.5(1)SU3 以降のバージョンにアップグレードし、プッシュ通知機能がすでに有効になっている場合、Expressway をアップグレードする前に、少なくとも 1 つの IM and Presence Service クラスタをアップグレードする必要があります。

オペレーティング システム	プッシュ通知の最小リリース
Android	• Unified Communications Manager 12.5(1)SU3 以上のリリース • IM and Presence Service 12.5(1)SU3 以上のリリース • Cisco Jabber 12.9.1 • Cisco Expressway X12.6.2（MRA が展開されている場合） 詳細については、最新の X12.6.2 Expressway リリースノートを参照してください。 （注） 最小リリースへのアップグレードとプッシュ通知機能がすでに有効になっている場合は、Expressway をアップグレードする前に、最初にすべての IM and Presence Service クラスタをアップグレードする必要があります。 Expressway をバージョン X12.7 以降にアップグレードし、IM and Presence Service を 11.5(1)SU8 または 12.5(1)SU3 以降のバージョンにアップグレードし、プッシュ通知機能がすでに有効になっている場合、Expressway をアップグレードする前に、少なくとも 1 つの IM and Presence Service クラスタをアップグレードする必要があります。

機能サポート

次の表に、特定の Unified Communications Manager リリースでサポートされるプッシュ通知機能の概要を示します。

Unified CM リリース	iOS12	iOS13 以降のバージョン	Android	iOS16.5
11.5(1)SU4 - SU7	基本的なプッシュ通知のサポート 単一プッシュ通知チャネル	基本的なプッシュ通知のサポート 単一プッシュ通知チャネル	サポートなし	基本的なクラウドプッシュ通知のサポート
11.5(1)SU8	基本的なプッシュ通知のサポート 単一プッシュ通知チャネル	基本的なプッシュ通知のサポート プッシュ通知の発信者ID コールとメッセージ用の個別チャネル	サポートなし	基本的なクラウドプッシュ通知のサポート

Unified CM リリース	iOS12	iOS13 以降のバージョン	Android	iOS16.5
12.5(x) SU2 まで	基本的なプッシュ通知のサポート 単一プッシュ通知チャネル	基本的なプッシュ通知のサポート 単一プッシュ通知チャネル	サポートなし	基本的なクラウドプッシュ通知のサポート
12.5(1) SU3	基本的なプッシュ通知のサポート 単一プッシュ通知チャネル	基本的なプッシュ通知のサポート プッシュ通知の発信者ID CallerID が外部プレゼンテーション名と番号をサポート プッシュ通知の登録ノード コールとメッセージ用の個別チャネル	基本的なプッシュ通知のサポート プッシュ通知の登録ノード コールとメッセージ用の個別チャネル	基本的なクラウドプッシュ通知のサポート
14SU3	サポートなし	サポートなし	基本的なプッシュ通知のサポート プッシュ通知の登録ノード コールとメッセージ用の個別チャネル ローカルプッシュはサポートされていません	コールのローカルプッシュ通知のサポート。メッセージングはサポートされません 基本的なプッシュ通知のサポート プッシュ通知の発信者 ID CallerID が外部プレゼンテーション名と番号をサポート プッシュ通知の登録ノード

プッシュ通知の前提条件

以下は、オンプレミス展開用オンボードプッシュ通知に対する前提条件です。

- Domain Name System は、Unified Communications Manager と IM and Presence Service の両方で必ず構成し、外部ルーティング可能なアドレスを解決できる必要があります。
- Unified Communications Manager プッシュ通知サービス（CPNS）はすべてのノードで実行する必要があり、CallManager はローカル CPNS にのみに接続する必要があります。機能的なプッシュ通知を確保するには、ローカルノードで CPNS を有効にすることが必須です。
- 次の Cisco Cloud への接続については、Unified Communications Manager および IM and Presence Service からポート 443 を介して接続を有効にする必要があります。
  - `fos-a.wbx2.com`—Unified Communications Manager でのフュージョン オンボーディング サービス：プッシュ通知サブスクリプション要求の場合にこのサービスに接続します。Unified CM を Fusion Onboarding Service（FOS）と通信して、共通アイデンティティ（CI）マシンアカウントをプロビジョニングします。
  - `push.webexconnect.com` でのプッシュ REST サービス：Unified Communications Manager および IM and Presence Service は、このサービスに接続してプッシュ通知を送信します。
  - `idbroker.webex.com` の共通アイデンティティサービス ー Unified Communications Manager および IM and Presence Service は、プッシュ通知送信前にこのサービスを認証します。

（注） ファイアウォールの暗号解読除外リストに `push.webexconnect.com` と `idbroker.webex.com` を追加します。

- Cisco Jabber へのメッセージングプッシュ通知の場合は、インスタントメッセージを有効化し、[マルチ デバイス メッセージング（Multiple Device Messaging）] 機能と [ストリーム管理（Stream Management）] 機能を IM and Presence Service に構成する必要があります。詳細については、「IM and Presence Service の設定と管理」を参照してください。
- プッシュ通知は、リリース 11.5(1)SU3 で導入された次のネットワークサービスに依存します。Cisco Unified Serviceability の **[コントロールセンター-ネットワークサービス（Control Center - Network Services）]** ウィンドウで、これらのサービスが実行されていることを確認できます。両方のサービスはデフォルトで有効になっています。
  - **シスコ プッシュ通知サービス**：音声コールとビデオ コールのプッシュ通知を処理します。
  - **シスコ管理エージェントサービス**：プッシュ通知に関連するトラブルシューティング情報の送信を処理します。
- iOS または Android デバイスは、Cisco Jabber アプリケーションからの通知を許可するように設定する必要があります。

- クラウド接続用にプロキシサーバーが必要な場合は、「クラウド接続のプロキシサポート（20 ページ）」の HTTP(S) プロキシサポートに関する情報を確認してください。
- iPhone または iPad クライアントに Cisco Jabber を導入する場合、音声プッシュ通知が動作するには、**[EnableVoipSocket]** パラメータ設定が **[false]** である必要があります。Cisco Unified CM Administration の **[UC サービスの設定（UC Service Configuration）]** ウィンドウでこのパラメータを設定できます（サービスタイプとして **[Jabberクライアント設定（Jabber Client Configuration）]** を選択し、**[オプション（Options）]** セクションでパラメータを設定します）。

  XML エディタでこのパラメータを編集することもできます。パラメータの 詳細については、『Parameters Reference Guide for Cisco Jabber』を参照してください。

ライセンスに関する要件

- 11.5(x) リリースの場合、Unified Communications Manager はライセンスに Cisco Prime License Manager を使用します。プッシュ通知のオンボードプロセスの一環として、Prime License Manager でライセンスを同期する必要があります。
- 12.x 以降のリリースの場合、Unified Communications Manager はライセンスにスマートライセンシングを使用します。プル通知の場合は、クラスタをオンにする前にスマートライセンスを設定する必要があります。スマートライセンシングに Unified Communications Manager を設定する方法については、『Cisco Unified Communications Manager システム設定ガイド』の「スマート ソフトウェア ライセンシング」章を参照してください。
- リリース 12.5 (x) 以降では、スマートライセンスが特定のライセンス予約で設定されている場合、プッシュ通知はサポートされません。プッシュ通知を動作させるには、特定のライセンス予約機能を無効にする必要があります。

証明書の前提条件

- MRA を設定している場合は、Unified Communications Manager、IM and Presence Service、および Cisco Expressway-C の間で証明書を交換する必要があります。各システムで同じ CA による CA 署名付き証明書を使用することを推奨します。その場合、次のようになります。
  - 各システムに CA ルート証明書チェーンをインストールします（Unified Communications Manager および IM and Presence Service の場合は tomcat 信頼ストアに証明書チェーンをインストールします）。
  - Unified Communications Manager の場合は、CSR を発行して CA 署名付き Cisco Tomcat および Cisco CallManager 証明書を要求します。
  - IM and Presence Service の場合は、CSR を発行して CA 署名付き Cisco Tomcat 証明書を要求します。

（注） 別の CA を使用する場合は、各 CA のルート証明書チェーンを Unified Communications Manager 、IM and Presence Service、および Expressway-C にインストールする必要があります。

（注） また、Unified Communications Manager と IM and Presence Service の両方に自己署名証明書を使用することができます。この場合は、Unified Communications Manager 用の Cisco Tomcat 証明書と Cisco CallManager 証明書、IM and Presence Service 用の Cisco Tomcat 証明書を Expressway-C にアップロードする必要があります。

プッシュ通知の設定タスク フロー

次のタスクを実行して、Cisco Unified Communications Manager および IM and Presence Service クラスタでプッシュ通知を設定します。

始める前に

プッシュ通知の前提条件 （28 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	ライセンスの同期 （32 ページ）	リリース 11.5 (1) SUx のみ。Cisco プライムライセンスマネージャのシステムライセンスを同期します。これは、新しいライセンスを追加したかどうかに関係なく、必須のタスクです。 （注） Prime License Manager がスマートライセンスに置き換わるため、このタスクは、Cisco Unified Communications Manager リリース 12.0(1) 以降で省略できます。
ステップ 2	プッシュ通知用のポートを開く （33 ページ）	プッシュ通知に必要なポートを開きます。
ステップ 3	プッシュ通知を有効化する （34 ページ）	プッシュ通知用の Cisco Unified Communications Manager および IM and Presence Service をオンボードします。

	コマンドまたはアクション	目的
ステップ 4	プッシュ通知の高可用性を有効にする（36 ページ）	IM およびプレゼンスの展開では、プッシュ通知を有効にすると高可用性が確保されます。
ステップ 5	OAuth 更新ログインを設定する （37 ページ）	これらの一連のタスクを完了して、より迅速な Cisco Jabber の OAuth 更新ログインを展開します。
ステップ 6	Expressway からの設定の更新 （40 ページ）	Expressway-C では、Authz 証明書を再同期できるように Unified Communications Manager サーバーを更新します。作業が終了したら、お使いのユーザーを再起動します。
ステップ 7	Expressway-E を再起動する （41 ページ）	IM and Presence Service を導入している場合は、Expressway-E を再起動する必要があります。
ステップ 8	トラブルシューティング オプションの設定 （41 ページ）	Cisco Unified Communications Manager のプッシュ通知アラームを Cisco Cloud に送信する頻度およびアラームシビラティ（重大度）を決定するトラブルシューティング パラメータを設定します。

（注） Cisco Expressway を使用したモバイルおよびリモートアクセス（MRA）の導入については、Expressway の使用によるプッシュ通知についての『Cisco Expressway 経由の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。

ライセンスの同期

11.5 (1) SU システムの場合は、Cisco プライムライセンスマネージャで次の手順を使用して、システムライセンスを同期します。これは、ライセンスを更新したかどうかに関係なく、オンプレミス展開のプッシュ通知を有効にするための必須タスクです。

（注） このタスクは、Cisco Unified Communications Manager 11.5 (1) SU リリースのみに必要です。このタスクは、リリース 12.0 (1) 以降では省略できます。これは、スマートライセンシングがプライムライセンスマネージャを置き換えるためです。

始める前に

ライセンスの追加手順や製品インスタンスを含むライセンス許諾の詳細については、『Cisco Prime License Manager ユーザガイド』を参照してください。

手順

ステップ 1 Cisco Prime License Manager で、[**製品インスタンス（Product Instance**）] タブを選択します。

ステップ 2 **ライセンスの同期**をクリックします。

プッシュ通知用のポートを開く

次のポートが、Cisco Unified Communications Manager および IM and Presence Service からのプッシュ通知サポート用に開かれていることを確認してください。

表 *5:* プッシュ通知のポート要件

送信元	宛先	ポートとプロトコル	説明
Unified CM および IM and Presence Service	Cisco cloud	443/TLS	プッシュ通知用の HTTPS ベースの通信： • Unified CM パブリッシャノードから `fos-a.wbx2.com` のフュージョン オンボーディング サービスへのサブスクリプション要求 • `idbroker.webex.com` での共通アイデンティティサービスへの認証要求 • `push.webexconnect.com` でのプッシュ REST サービスへのプッシュ通知 このポートは、すべてのクラスタノードに対して開いている必要があります。

（注）

- Apple デバイスについては、「エンタープライズ ネットワークでの Apple 製品の使用 - Apple サポート」を参照してください。

  Android デバイスについては、「Android エンタープライズ ネットワーク要件 - Android エンタープライズヘルプ」（google.com）を参照してください。

（注） さらに、ポート 9966 は、Ccisco プッシュ通知サービスによって内部的に使用され、すべての Unified Communications Manager クラスタノード上の Cisco CallManager サービスと通信します。クラスタ内のノード間の通信がファイアウォールを通過する場合は、このポートをファイアウォールで開く必要があります (たとえば、ノードが別のサブネットに配置されている場合、例のように WAN に接続されています)。この場合は、このポートをファイアウォールで開いて、これらのサービスが通信できるようにする必要があります。

プッシュ通知を有効化する

この手順を使用して、Cisco Unified Communications Manager および IM and Presence Service クラスタ内でプッシュ通知を有効にします。

始める前に

次の点を確認してください。

- ポート 443 Unified Communications Manager はパブリッシャーノードからのアウトバウンド HTTPS リクエスト用に開放されている必要があります。
- **Cisco プッシュ通知サービス** と **Cisco 管理エージェントサービス** の両方のネットワークサービスが Cisco Unified Serviceability で実行されている必要があります。 両方のサービスがデフォルトで有効になっています。

手順

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**高度な機能** > **Cisco Cloud Onboarding**。
Unified Communications Manager Cisco クラウドが到達可能かどうか、また証明書が存在するかどうかを確認するため、ページの読み込みに 1 分ほどかかる場合があります。

ステップ 3 [**バウチャーの生成**] ボタンをクリックして、システムのライセンスを同期します。

ステップ 4 **プッシュ通知を有効にする** チェックボックスを選択してください。

ステップ 5 [**CiscoにCisco Cloud ServiceのCA証明書をこの信頼に必要なものとして管理させたい**] チェックボックスをオンにして、システムが自動的に証明書を更新するようにします。

（注） このチェックボックスをオンにすると、Cisco はクラウド証明書の要件を自動的にインストールします。 しかし、システムのインストールに使用したファイルに含まれていない新しい証明書要件が追加された場合、クラウド証明書を手動で取得する必要があるかもしれません。 証明書を手動でアップロードする方法については、クラウド接続の証明書 （59 ページ） を参照してください。

ステップ 6 Ciscoクラウドに到達するためにHTTP(S)プロキシが必要な場合、[**HTTP(S)プロキシを有効にする**] チェックボックスにチェックを入れ、サーバの詳細を入力します。

（注） Cisco はプロキシ サーバの基本認証とダイジェスト認証をサポートしています。 推奨する認証方法はダイジェスト認証です。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 クラスタ内のすべてのノードで Cisco Tomcat サービスを再起動し、Cisco が管理する証明書をインストールします。

a) コマンドライン インターフェイスにログインします。

b) `utils service restart Cisco Tomcat` コマンドを実行します。
Cisco Tomcat サービスの再起動後、 **Cisco Cloud Onboarding 構成** ウィンドウの [状況] に、「Cisco Cloud Onboarding Pending」というメッセージが表示されます。

ステップ 9 [**Cisco Cloud Onboarding Configuration**] ウィンドウで、[**プッシュ通知を有効にする**] および [**Ciscoにこの信頼関係に必要なCisco Cloud Service CA証明書の管理を任せたい**] のチェックボックスがまだチェックされていることを確認します。 再確認が必要な場合があります。

ステップ 10 （任意） トラブルシューティングの設定を構成して、システムの問題を迅速に解決できるようにします。 フィールドの説明については、オンライン ヘルプを参照してください。

a) [**トラブルシューティング情報を Cisco クラウドに送信する**] チェックボックスを選択します。

b) [**トラブルシューティングのために暗号化された PII を Cisco クラウドに送信する**] チェックボックスを選択します。

ステップ 11 **[保存（Save）]** をクリックします。
クラスターはプッシュ通知サブスクリプション リクエストを開始します。 リクエストが完了し、プッシュ通知が有効になると、**[ステータス（Status）]** フィールドに「Cloud Onboarding Completed」というメッセージが表示されます。

（注） Unified Communications Manager プッシュ通知サービス (CPNS) を再起動します。

ステップ 12 IM and Presence Service を展開に含める場合、すべての IM and Presence Service クラスタ ノードで **[Cisco XCP Config Manager]** と **[Cisco XCP Router]** サービスを再起動します。

a) **[Cisco Cloud オンボーディング（Cisco Cloud Onboarding）]** ウィンドウの **[ステータス（Status）]** エリアに表示される **[Control Center - ネットワークサービス（Network Services）]** リンクをクリックします。 リンクが表示されない場合は、Cisco Unified Serviceability のインタフェースにログインして、**[ツール]**>**[コントロールセンター]**-**[ネットワークサービス]**の順に選択します。

b) **[サーバー（Server）]** ドロップダウン リスト ボックスから、IM and Presence データベース パブリッシャ ノードを選択し、**[移動（Go）]** をクリックします。

c) **Cisco XCP Config Manager** サービスを選択して、[**再起動] をクリックします**。

d) **[Cisco XCP Router]** サービスを選択し、**[リスタート（Restart）]** をクリックします。

e) すべての IM and Presence クラスター ノードに対してこの手順を繰り返します。

（注） 「デバイスデフォルトページでActivation Codeオンボーディングを使用するために有効化されている電話はありません」というメッセージが表示された場合、オンボーディングが失敗したということではありませんが、これは、デバイスデフォルト **ウィンドウ内のどのデバイスもオンプレミスオンボーディング方法のアクティベーションコードを使用するように構成されていないことを示します。**

（注） Unified CM オンボーディング ページが更新されるたびに、Unified Communications Manager プッシュ通知サービス (CPNS) を再起動する必要があります。

（注） **Cisco XCP Router** を再起動しても、 **Cisco Cloud オンボーディング構成** ウィンドウの **ステータス** メッセージは更新されません。すべてのノードに対して上記の手順を完了してから **Cisco Cloud Onboarding Configuration** ウィンドウに戻ると、 **[ステータス]** Cisco XCP ルーターを再起動する必要があるというメッセージが引き続き表示されます。 しかし、各 IM and Presence クラスタ ノードで 1 回だけ再起動する必要があります。

（注） プッシュ通知を無効にするには、[**プッシュ通知を有効にする**] チェックボックスを解除し、[**保存**] をクリックします。 保存後、すべての IM and Presence Service クラスタ ノードで **[Cisco XCP Router]** を再起動します。

プッシュ通知の高可用性を有効にする

この手順を使用して、プッシュ通知の高可用性が IM and Presence Service で有効になっていることを確認します。 この機能は、中断モードの Android または iOS クライアント上の Cisco Jabber に冗長性とフェイルオーバーを提供するために必要です。

（注） Cisco Webex クライアントは、メッセージングに IM およびプレゼンスサービスではなく、Cisco Webex クラウドを使用します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] から、以下を選択します。**[システム（System）]** > **[サービスパラメータ（Service Parameters）]**。

ステップ 2 **サーバ** ドロップダウンから、IMとプレゼンスノードを選択します。

ステップ 3 **サービス** ドロップダウンから **Cisco XCP Router (アクティブ) を選択します。**

ステップ 4 **[プッシュ通知 (クラスター全体)]**で、 **プッシュ通知高可用性** サービスパラメータを **有効に設定します。**

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 このサービスパラメータの設定を編集した場合、すべての IM and Presence ノードで **Cisco XCP Router** を再起動してください。 それ以外の場合は、次のタスクに進むことができます:

a) Cisco Unified Serviceability から、**[ツール（Tools）]** > **[コントロールセンター-ネットワークサービス（Control Center - Network Services）]** の順に選択します。

b) **[サーバ（Server）]** ドロップダウンから、IM and Presence クラスタ ノードを選択し、**[移動（Go）]** をクリックします。

c) [Cisco XCP Router]を選択し、[リスタート（Restart）]をクリックします。

d) すべての IM and Presence クラスタ ノードでこの手順を繰り返します。

OAuth 更新ログインを設定する

これらのタスクを完了して Oauth 更新ログインをセットアップします。これは、Cisco Jabber および Cisco Webex クライアントにより迅速なログインを提供するオプション機能です。

（注） OAuth 更新ログインは、Cisco Expressway ではデフォルトで有効になっていますが、Unified Communications Manager ではデフォルトで無効になっています。 両方のシステムにデフォルト設定を使用すると、構成の不一致が発生します。

手順

	コマンドまたはアクション	目的
ステップ 1	Unified Communications Manager で OAuth 更新ログインを設定する （38 ページ）	OAuth アクセス トークンを使用してログインの更新を設定し、Unified Communications Manager でトークンを更新します。 （注） Oauth 更新ログインは Unified Communications Manager でオプションとして展開可能です。
ステップ 2	Expressway で Oauth 構成を確認する （39 ページ）	Cisco Expressway を展開している場合、Expressway の Oauth 更新ログインの構成が Unified Communications Manager の構成と一致していることを確認してください。

	コマンドまたはアクション	目的
ステップ 3	Unity Connection で Oauth を有効にする（40 ページ）	Cisco Unity Connection で、OAuth リフレッシュログインを有効にし、 Unified Communications Manager パブリッシャーノードを Authz サーバとして指定します。

Unified Communications Manager で OAuth 更新ログインを設定する

Unified Communications Manager でこの手順を使用して、Cisco Jabber クライアントと Cisco Webex クライアンOAuthアクセストークンとリフレッシュトークンを使用してリフレッシュログインを設定します。 Oauth 更新ログインは、ネットワークが変更された後にユーザが再ログインする必要がない合理化されたログイン フローを提供します。

（注） 互換性を確保するために、展開のさまざまな Unified Communications コンポーネントがすべて更新ログインをサポートしていることを確認してください。 Oauth 更新ログインが有効になったら、この機能を無効にすると、すべての Jabber および Webex クライアントをリセットする必要があります。

注意 デフォルトでは Unified Communications Manager で無効になっているが、Cisco Expressway ではデフォルトで有効になっている OAuth 更新ログインを有効にすることを推奨します。 両方のシステムが展開され、デフォルト設定を使用している場合、 Unified Communications Manager で[ログインの更新]を有効にするか、Cisco Expresswayでそれらを無効にする必要があります。そうしないと、構成の不一致が発生します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**システム** > **エンタープライズパラメータ**。

ステップ 2 [**SSO 設定**] で、次のいずれかを実行します:

- **OAuth ログインフロー更新** エンタープライズパラメータを選択し、それを **有効** に設定してOAuth 更新ログインを有効にします。
- **[OAuth ログインフロー更新（OAuth with Refresh Login Flow）]** エンタープライズパラメータを選択し、それを **[無効（Disabled）]** に設定してOAuth 更新ログインを無効にします。 これがデフォルト設定です。

ステップ 3 [OAuth ログイン更新] を有効にした場合、次のエンタープライズパラメーターを構成することにより、アクセス トークンと更新トークンの有効期限タイマーを構成します。

- **Oauth アクセストークン有効期限タイマー (分)**—このパラメータは、個々の OAuth アクセストークンの有効期限タイマーを分で指定します。 タイマーの期限が切れた後、OAuth アクセス トークンは無効になりますが、Jabber クライアントは、更新トークンが有効である限り、ユーザを再認証することなく、新しいアクセストークンを要求して取得できます。 有効な範囲は 1 から 1440 分で、デフォルトは 60 分です。
- **OAuth 更新トークン有効期限タイマー (日)**—このパラメータは OAuth 更新トークンの有効期限タイマーを日単位で指定します。 タイマーが期限切れになった後、更新トークンは無効になり、Jabber クライアントは新しい更新トークンを取得するために再認証する必要があります。 有効な範囲は 1 から 365 日で、デフォルトは 60 日です。

ステップ 4 **[保存（Save）]** をクリックします。

（注） 構成を保存したら、すべての Cisco Jabber および Webex クライアントをリセットします。

次のタスク

Cisco Expressway の OAuth 更新ログインの構成が Unified Communications Manager の設定と一致していることを確認してください。 詳細は、Expressway で Oauth 構成を確認する （39 ページ）を参照してください。

Expressway で Oauth 構成を確認する

Cisco Expressway を展開している場合、Expressway の OAuth 更新ログインの構成が Unified Communications Manager の構成と一致していることを確認してください。

（注） OAuth 更新ログインは、Cisco Expressway ではデフォルトで有効になっていますが、Unified Communications Manager ではデフォルトで無効になっています。 両方のシステムにデフォルト設定を使用すると、構成の不一致が発生します。 Unified Communications Managerでは、OAuth 更新ログインは **OAuthと更新ログインフロー** エンタープライズパラメータ経由で設定されます。

手順

ステップ 1 Cisco Expressway-C にログインします。

ステップ 2 **[設定（Configuration）]** > **[Unified Communications]** > **[MRA アクセス制御（MRA Access Control）]** を選択します。

- Unified Communications Managerに OAuth 更新ログインが有効になっている場合、[**更新を伴う Oauth トークンによる認証**] 設定を [**オン**] に設定します。 これがデフォルト設定です。

- Cisco Unified Communications Manager で OAuth 更新ログインが無効になっている場合は、[**更新を伴う OAuth トークンによる認証**] 設定を [**オフ**] に設定します。

ステップ 3 **[保存（Save）]** をクリックします。

Unity Connection で Oauth を有効にする

Jabber に Oauth 更新ログインを展開する場合、この手順を使用して Unity Connection で機能を有効にします。 設定の一部として、 Unified Communications Manager パブリッシャーノードを Authz サーバとして指定する必要があります。

手順

ステップ 1 Cisco Unity Connection で Oauth 更新ログインを有効にする:

a) Cisco Unity Connection の管理から **[システム設定]** > **[エンタープライズパラメータ] を選択します。**
b) [**SSO および OAuth の構成] で設定を構成します。**
c) **エンタープライズパラメータのOAuth ログインの更新** を **有効に設定してください。**
d) **[保存（Save）]** をクリックします。

ステップ 2 Unified Communications Manager パブリッシャーノードを Cisco Unity Connection の認証サーバとして追加します。

a) Cisco Unity Connection の管理から、 **[システム設定]** > **Authz サーバ** を選択します。
b) 次のいずれかを実行します。
   - サーバを選択して既存の認証サーバ構成を編集します。
   - 新しい認証サーバーを追加するには、**[新規追加（Add New）]** をクリックします。
c) ページのフィールドを設定します。
d) **[保存（Save）]** をクリックします。

Expressway からの設定の更新

次の手順を使用して、プッシュ通知用の Cisco Expressway の設定を更新します。これにより、その設定と証明書を、Unified Communications Manager と同期させることができます。

（注） Cisco Expressway 設定の詳細については、「*Expressway* メンテナンスおよび運用ガイド」ページにある『Cisco Expressway 管理者ガイド』を参照してください。

手順

ステップ 1 Expressway-C にログインします。

ステップ 2 Cisco Unified Communications Manager Administration サーバーを更新 します。

a) Expressway-C で、**[設定（Configuration）]** > **[Unified Communications]** > **[Unified CM サーバー（Unified CM servers）]**に移動します。

b) **[サーバーの更新 (Refresh server)]** をクリックする
Expressway は、Authz 証明書を Unified Communications Manager と同期します。

ステップ 3 サーバーの更新後、Expressway-C を再起動します。再起動が完了するまで、Expressway-C は IM and Presence Service のプッシュ機能を認識せず、PUSH メッセージを Cisco Jabber クライアントに送信しません。

a) **[メンテナンス（Maintenance）]** > **[再起動オプション（Restart options）]**を選択します。

b) **[再起動（Restart）]** をクリックします。

Expressway-E を再起動する

インスタントメッセージによるプッシュ通知には Expressway-E の再起動が必要です。 IM およびプレゼンス サービスでプッシュ通知を有効にした後、Expressway-E を再起動する必要があります。 再起動するまで、Expressway-E は IM and Presence Service のプッシュ機能を認識できず、PUSH メッセージを Jabber クライアントに送信しません。

（注） 展開に IM and Presence Service が含まれない場合、このタスクをスキップできます。

手順

ステップ 1 Expressway-E にログインします。

ステップ 2 **[メンテナンス（Maintenance）]** > **[再起動のオプション（Restart options）]** を選択します。

ステップ 3 **再起動（Restart）**をクリックします。

トラブルシューティング オプションの設定

Unified Communications Manager パブリッシャーノードでこの手順を使用して、プッシュ通知アラームを Cisco クラウドに送信する頻度と重大度を決定するパラメータを設定します。

始める前に

Cisco 管理エージェントサービス ネットワークサービスは、 Unified Communications Manager が Cisco Cloud にプッシュ通知アラームを送信するために稼働している必要があります。 Cisco Unified Serviceability の [**コントロールセンター - ネットワークサービス**] ウィンドウで、サービスが実行中であることを確認できます。 このサービスはデフォルトで有効になっています。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 プッシュ通知アラームをクラウドに送信する頻度を設定するには、 `utils managementAgent alarms pushfrequency <minutes >` コマンドを実行します。ここで、 `<minutes>` は5から90分の間の整数を表します。 デフォルト値は 30 分です。

ステップ 3 Cisco Cloud にプッシュ通知アラームを送信するための最小重大度を設定するには、 `utils managementAgent alarms minpushlevel <alarm_level>` コマンドを実行します。 `<alarm_level>` は最小重大度を示します。 この重大度を下回るプッシュ通知アラームは Cisco クラウドに送信されません。

プッシュ通知の `<alarm_level>` オプションは、最も重要から最も軽度まで、次のとおりです:

- `クリティカル（Critical）`
- エラー (デフォルト値)
- 警告
- 通知
- 情報

ステップ 4 プッシュ通知のアラームを Cisco Cloud にすぐに送信する必要があり、スケジュールされたアップロードを待つことができない場合は、 `utils managementAgent alarms pushnow` コマンドを実行します。

リリース 12.0 以降の APNS バウチャー生成

リリース 11.5 では、Prime License Manager (PLM) が APNS に必要なバウチャーを生成します。 12.0 で PLM が廃止されると、この機能は Cisco Smart Software Manager (CSSM) および CSSM サテライトによって提供されます。

フレッシュ インストールまたはプッシュ通知機能のない 11.5(1)SU2 より前のバージョンからのアップグレード

リリース 12.0 では、PLM の代わりにスマート ライセンシングが使用されます。 Unified CM を Smart License Manager (SLM) に登録し、Cisco Cloud Onboarding UI の [バウチャーの生成] をク

リックして、Unified CM にバウチャーを同期します。 その後、11.5(1)SU2 のプロセスとはわずかに異なるオンボーディング プロセスに進みます。

11.5(1)SU2 から 12.0 以降のリリースへのアップグレード

このシナリオでは、Unified CM は評価モードに切り替わります。 評価モードが期限切れになる前に、Unified CM を SLM に登録します。

- PLM から同期されたバウチャーコードは、アップグレード中にデータベースから削除されます。
- アップグレード前に Unified CM がオンボーディングだった場合、プロビジョニングが許可されるまでプッシュ通知が機能し続けます。 スマート ライセンスによってプロビジョニングが無効になっている場合、プッシュ通知は機能しません。ただし、評価モード中にプッシュ通知が無効になっている場合、再オンボーディングは、新しいクーポンが SLM から同期され、新しいオンボーディング プロセスを通じてオンボーディングが実行された後にのみ可能になります。
- アップグレード前に Unified CM がオンボーディングされていない場合、Unified CM を CSSM または CSSM サテライトに登録する必要があります。 Cisco Cloud Onboarding UI で [クーポンの生成] をクリックして、クーポンを Unified CM と同期する必要があります。また、新しいオンボーディング プロセスを使用してオンボーディングを実行する必要があります。
- アップグレード前にプッシュ通知を無効にして、アップグレード後に新しいオンボーディング フローを使用して再度オンボードすることを推奨します。

プッシュ通知のトラブルシューティング

プッシュ通知はさまざまなコンポーネントに影響し、その一部はローカルにホストされていて、一部がクラウドにあります。プッシュ通知のトラブルシューティングを設定して、システムの問題を事前にトラブルシューティングするために必要な情報を Cisco TAC に説明することが重要です。

Cisco Cloud にトラブルシューティング情報を送信する

デフォルトでは、Unified Communications Manager はプッシュ通知のトラブルシューティング情報を一定の間隔で Cisco Cloud に送信します。シスコはこの情報を使用してプッシュ通知とシステム コンポーネントのデバッグを積極的に行っていきます。Cisco TAC がプッシュ通知のアラームにすばやくアクセスできるようにすることによって、システムのトラブルシューティングを迅速に行います。

このオプションは、プッシュ通知が有効化された後、デフォルトで有効になっていますが、管理者は、**[Cisco Cloud オンボード設定]** ウィンドウで無効にすることができます。このオプションが有効になっている場合、Cisco Unified Communications Manager は、**顧客のクラスタ ID** を生成し、その ID を顧客のホーム Unified Communications Manager クラスタに保存します。プッ

シュ通知に関する Cisco TAC をコールするユーザーは、TAC のスタッフがお客様のプッシュ通知アラームを特定できるように、ID を提供する必要があります。

個人識別情報（PII）暗号化

また、プッシュ通知アラームに保存されている個人を識別できる情報（PII）を暗号化するように、Unified Communications Manager を設定することもできます。PII データには、ユーザー名、ホスト名、デバイス名など、特定のユーザーを識別するためのデータが含まれます。**トラブルシューティングのために暗号化された PII を Cisco Cloud に送信する**オプションを選択してこの機能を有効にします。

セキュリティを強化するために、PII データを復号化するための **Cisco Support トークン**は、顧客の Unified Communications Manager サーバーの **[Cisco Cloud オンボーディング設定（Cisco Cloud Onboarding Configuration）]** ウィンドウでのみ提供されています。Cisco は、お客様がトークンを提供しない限り、このデータを復号化することはできません。プッシュ通知の問題について Cisco TAC をコールしている場合は、TAC がプッシュ通知アラームで暗号化された情報を読み取ることができるように、そのトークンを提供する必要があります(PII暗号化が設定されていることが前提です)。

このオプションを選択しない場合、Cisco Cloud に個人を特定できる情報は送信されません。

プッシュ通知のトラブルシューティング用の CLI コマンド

プッシュ通知では、次の CLI コマンドを使用できます。これは、Unified Communications Manager パブリッシャーノード上で実行して、トラブルシューティングを行うことができます。

- **utils managementAgent alarms pushfrequency** — このコマンドを実行すると、Cisco Unified Communications Manager が Cisco Cloud にプッシュ通知アラームを送信する間隔を構成できます。デフォルト値は 30 分です。
- **utils managementAgent alarms pushlevel** — このコマンドを実行すると、Cisco Unified Communications Manager が Cisco Cloud にプッシュ通知アラームを送信する最低重大度レベルを構成できます。デフォルトの重大度は「エラー (Error)」です。
- **utils managementAgent alarms pushnow**：次のコマンドを実行して、通知間隔の期限が切れるのを待たずに、プッシュ通知アラームを直ちに Cisco Cloud にアップロードします。

トレース

Cisco Management エージェントサービスおよび Cisco Push Notification Service でトレースを実行することもできます。デフォルトでは、トレースは情報レベルに設定され、次の場所に保存されます。

- Cisco Management Agent Service：`/var/log/active/cm/trace/cmas/log4j/`
- Cisco Push Notification Service：`/var/log/active/cm/trace/ccmpns/log4j/`

トレースを設定する方法の詳細については、『Cisco Unified Serviceability 管理ガイド』の「トレース」の章を参照してください。

クラウドサービスの到達可能性

Unified CM クラスタのすべてのノードで、`push.webexconnect.com` および `idbroker.webex.com` との接続を確立できることを確認します。また、ブロックされている IP アドレス一覧で、任意の IP アドレスが一覧されているかを確認します。お使いの IP アドレス がブロック済み IP アドレス一覧に入っていないかを確認するには、「https://help.webex.com/en-us/article/WBX1831/Unable-to-Reach-or-Access-Webex-Site」を参照してください。

プッシュ通知が有効になっている 11.5(1)SU2 からのアップグレード

11.5(1)SU2 リリースからアップグレードしていて、古いリリースでプッシュ通知を有効にした場合、現在のリリースでプッシュ通知を無効にしてから、オンボーディングプロセスに従ってプッシュ通知を再度有効にする必要があります。 これは、11.5(1)SU2 リリースの一部ではなかったこのリリースでの API の変更により必要になります。 プッシュ通知を無効にし、このリリースのオンボーディングプロセスに従わない限り、アップグレードしたシステムは Cisco Cloud にトラブルシューティングログを送信できません。

システムを新しいリリースにアップグレードした後、次のことを行ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	プッシュ通知を無効にする	手順は以下のとおりです。 **1.** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**高度な機能** > **Cisco Cloud Onboarding** **2.** 次のチェックボックスをオフにします。 • **プッシュ通知を有効化する** • **トラブルシューティング情報を Cisco Cloud に送信する** • **トラブルシューティングのために暗号化された PII を Cisco Cloud に送信する** **3.** **[保存（Save）]** をクリックします。
ステップ 2	このリリースのプッシュ通知を有効にします。	オンボーディング プロセスの詳細は、プッシュ通知の設定タスク フロー （31 ページ） を参照してください。

リフレッシュトークンを手動で更新する

400 不正リクエストメッセージを受け取った場合は、プッシュ通知サービスへのアクセストークンの有効期限が切れているため、アクセストークンを手動で更新する必要があります。このプロセスに従って、アクセストークンを手動で更新します。

	ステップ	詳細
ステップ 1	影響を受けるマシンと同じバージョンを使用して、新しい Cisco Unified Communications Manager サーバをインストールします。Unified Communications Manager	インストールの手順については、『Cisco Unified Communications Manager および IM and Presence Service のインストールガイド』を参照してください。
ステップ 2	新しいノードのライセンスを取得する	「Smart Software Manager」の章を参照してください。 Cisco Unified Communications Manager システム設定ガイド
ステップ 3	必要な証明書チェーンを tomcat-trust にアップロードし、プッシュ通知の新しいノードをオンボードしてください	このドキュメントのオンボーディングの手順に従ってください。
ステップ 4	オンボーディングが成功したことを確認する	`utils service restart Cisco Push Notification service` コマンドを実行して、Cisco プッシュ通知サービスを再起動してください。 ログを表示し、トークンが正常に取得されたことを確認します。
ステップ 5	新しいマシンから更新トークンを取得する	期限切れのトークンを持つ元のノードで、`run sql select * from machine account details` CLI コマンドを実行してマシンの詳細を取得します。
ステップ 6	元のノードからマシンの詳細を取得する	`run sql * from machineaccountdetails` CLI コマンドを実行します。
ステップ 7	顧客のリフレッシュトークンを更新する	`run sql update machineaccountdetails set refreshtoken=<actual_token_text>` CLI コマンドを実行します
ステップ 8	クラスター全体でリフレッシュトークンを更新する	Unified Communications Manager および IM and Presence Service クラスタのすべてのノードで次の CLI コマンドを実行します: `run sql select refreshtoken from machineaccountdetails`

プッシュ通知の相互作用と制限

プッシュ通知では、次の機能間の相互作用と制約が確認されています。

表 *6:* プッシュ通知の機能間の相互作用と制約

機能	連携動作と制限事項
NAT およびファイアウォール接続	Push REST サービスへのアイドル状態の TCP 接続を少なくとも 30 分間開いておくように、NAT およびファイアウォールデバイスを設定することを推奨します。 既存の接続でエラーが発生した場合、新しい TCP 接続ではプッシュ通知が再試行されません。 既存の接続を開いたままにしておくことで、NAT およびファイアウォール デバイスによる時期尚早の終了が原因で発生するエラーを防ぐことができます。
ボイスコール	クライアントが一時停止モードの音声通話とビデオ コールの場合、プッシュ通知チャネルが確立するまでの間、通話の接続に遅延が生じる場合があります。 5 秒後に、Unified CM が iOS デバイスから返される呼び出し音を受信しない場合、Unified CM は発信側デバイスで呼び出し音を鳴らします。 プッシュ通知プロセスの遅延が Unified CM が IOS デバイスにコールを提供するのを防ぐ場合、Unified CM は 13 秒後にコールをドロップします。

機能	連携動作と制限事項
プッシュ通知の高可用性	高可用性は、11.5(1)SU3 の時点で、プッシュ通知展開の IM およびプレゼンス サービスでサポートされています。プッシュ通知が有効で、ノードがフェイルオーバーした場合、Android および iOS クライアント用の Cisco Jabber で以下が発生します。 • フォアグラウンドモードの Cisco Jabber クライアントの場合、クライアントはバックアップノードに自動的にログインします。メインノードが復旧するまで、バックアップは引き継ぎます。バックアップノードが引き継ぐときも、メインノードが回復するときも、サービスに中断はありません。 • バックグラウンド モードの Cisco Jabber クライアントの場合、バックアップ ノードが引き継ぎますが、プッシュ通知が送信される前に遅延が発生します。 Jabber クライアントはバックグラウンド モードであるため、ネットワークへのアクティブな接続がないため、バックアップ ノードに自動的にログインしません。バックアップノードは、プッシュ通知を送信する前に、バックグラウンドモードにあるすべてのフェイルオーバーユーザに対して JSM セッションを再作成する必要があります。 遅延の長さはシステム負荷によって異なります。 テストによると、高可用性ペアでユーザが均等に分散された 15,000 ユーザの OVA の場合、フェイルオーバー後にプッシュ通知が送信されるまでに 10ー20 分かかります。 この遅延は、バックアップノードが引き継ぐとき、およびメインノードが回復した後にも発生します。 （注） ノード障害または予期しない Cisco XCP Router のクラッシュの場合、IM 履歴を含むユーザの IM セッションは、ユーザ アクションを必要とすることなく維持されます。 ただし、Cisco Jabber for Android および iOS クライアントが一時停止モードの場合、クラッシュ時にサーバのキューにあった未読メッセージを取得することはできません。
プッシュ通知を停止する	プッシュ通知がデバイスに配信されないようにするには、Cisco Jabber または Webex アプリケーションからログアウトします。

機能	連携動作と制限事項
複数デバイス メッセージング (MDM)	ユーザがデスクトップ版 Cisco Jabber クライアントをモバイル版 Cisco Jabber クライアントと共に使用する場合、プッシュ通知は [**最後のアクティブセッション**] に従います。 これは、次のいずれかの条件が満たされた場合にのみ、プッシュ通知がモバイル用 Cisco Jabber クライアントに送信されることを意味します。 • モバイル用の Cisco Jabber クライアントは、ユーザが最後に対話したクライアントでした。 • デスクトップ版 Cisco Jabber クライアントが 300 秒以上非アクティブでした。 • デスクトップ用 Cisco Jabber クライアントがサインアウトされました。

ローカル プッシュ通知サービス

重要 このセクションは、リリース 14SU3 以降に適用されます。

（注）
- Webex アプリ 43.6 以降または Cisco Jabber 14.2 以降を搭載した iOS 16.5 以降で実行されている iOS デバイスはこの機能をサポートしています。 iOS デバイスがオンプレミス モードで接続されていることを確認してください。
- このリリースでは、ローカル プッシュ通知サービス (LPNS) は音声コールの通知のみをサポートしています。
- LPNS は Android デバイスおよび MRA ユーザではサポートされていません。

（注） MRA ユーザは、引き続き APNs チャネルを通じてプッシュ通知を受け取ります。 LPNS を設定することは、この状況を排除しません。

現在、Webex アプリは、iOS デバイスがインターネットに接続されていない Wi-Fi の制限されたネットワークで動作している場合、VoIP 通話の着信通知を受け取りません。 たとえば、病院、クルージング船、飛行機などです。 インターネット接続がないため、デバイスは APNS にアクセスできません。ユーザーは通話を遅延なしで受信したいと思っても、しかし、APNS

ではネットワーク遅延による数秒の遅れで呼び出しが受信されます。 LPNS はこの問題を解決します。

Webex アプリが Unified Communications Manager に登録され、LPNS を提供するプロビジョンされた Wi-Fi ネットワークに参加すると、Webex アプリは着信と不在着信に関する通知の受信を開始します。 通知には発信側の名前と電話番号が表示されます。

設定済みの Wi-Fi ネットワーク内にクライアントがある場合、クライアントは Unified Communications Manager サーバへのローカル接続を確立します。 iOS デバイスがプッシュ通知を受信すると、まずローカルサーバに送信しようとします。それが失敗すると、Apple Push サーバ経由で送信します。

LPNS 前提条件

オンプレミス展開でローカル プッシュ通知を有効にするには、APNS の Unified CM クラスタをオンボードします。 詳細については、プッシュ通知を有効化する （34 ページ） を参照してください。

（注） 参照されているセクションの手順 12 を実行する必要はありません。

LPNS が起動しているかどうかは、Cisco Unified Serviceability の [Control Center - ネットワークサービス] **ウィンドウの** CM サービス **エリアで確認できます。** 利用可能な場合、 **Cisco ローカルプッシュ通知サービスとして表示されます**。既定では、このサービスは有効になっています。

LPNS のポートを開く

からの LPNS サポートのために次のポートが開いていることを確認してください Unified Communications Manager。

表 *7: LPNS* のポート要件

送信元（From）	移行後	ポートおよびプロトコル	説明
Webex アプリ	Unified Communications Manager	9560/安全なウェブソケット	（注） クラスターの LPNS は 9560 ポートを使用して、高可用性のメッシュを有効にします。

ローカル プッシュ接続の仕組み

起動時に、iOS プラットフォームにインストールされている Webex アプリ クライアントは、発信するために Unified CM に登録します。 クライアントがフォアグラウンド モードにある間、Unified CM はコールをクライアントに直接送信します。 クライアントが設定済みの Wi-Fi

ネットワークにある場合、Unified CM サーバへのローカル接続を確立します。 Webex アプリはプッシュ通知を受信すると、まずローカル サーバに送信しようとします。 それが失敗した場合、Apple プッシュ サーバ経由でプッシュ通知を送信します。

デバイスが Wi-Fi ネットワークに接続されている場合、Webex アプリは Unified CM とのセキュアな持続的な接続を維持します。 Unified CM は、この接続を介して Webex アプリへの着信通知を配信します。 WebSocket接続は、デバイスが指定されたネットワークに接続されている限り維持されます。 Webex アプリが強制終了されるか、電話が再起動されると、デバイスが指定された Wi-Fi ネットワークに接続されている限り、Unified CM サーバへの LPNS WebSocket 接続が再確立されます。

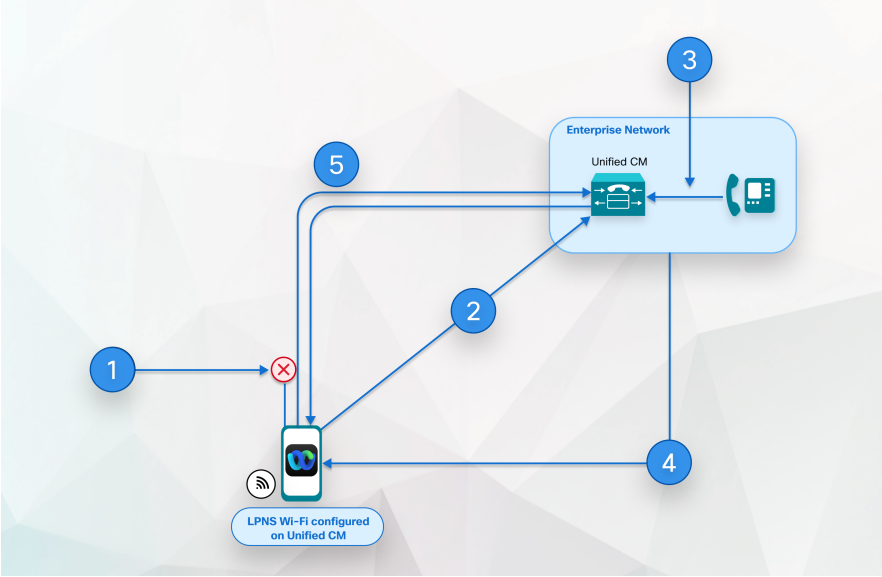
リソースを効率的に使用できるように、LPNS サーバは OAuth トークンの有効期限が切れたとき、または Webex アプリ クライアントが指定された Wi-Fi ネットワークから移動したときに、それを知る必要があります。 これはキープアライブ メッセージを使用して行われます。 クライアントは 120 秒ごとにキープアライブメッセージを LPNS サーバに送信します。 LPNS サーバはこのメッセージを確認し、WebSocket 接続を維持します。 LPNS サーバが 120 秒以内にキープアライブ メッセージを受信しない場合（トークンの期限切れ、または Webex アプリ クライアントが Wi-Fi ネットワークから切断している場合）、クライアントへの接続を閉じ、401 エラー メッセージを送信します。

（注） 以下の場合に、特定の iOS デバイスの LPNS セッションが閉じられます。

- ユーザのログオフ時。
- サインイン済みユーザが削除されたとき。
- デバイスが削除されたとき。
- ユーザがプロビジョニングされた Wi-Fi からプロビジョニングされていない Wi-Fi に移動したとき

以下の画像は、VoIP ローカルプッシュ通知がプライベートネットワークで iOS デバイスに送信される際に行われるプロセスの内訳を示しています。

図 *5 : iOS* デバイスに送信される際のプライベート ネットワークでの *VoIP* ローカル プッシュ通知の動作



1. Webex アプリがバックグラウンドにあり、Unified CM への SIP チャネルが切断されます。
2. Webex アプリは、デバイスが Wi-Fi に接続され、ユーザがログインするまで、WebSocket 経由で接続されたままになります。
3. Webex アプリが着信を受信します。
4. Unified CM は招待をバッファし、WebSocket を通じて Webex アプリにローカル プッシュ通知を送信します。
5. Webex アプリがウェイクアップされ、Unified CM に登録され、SIP チャネルが確立されます。

Wi-Fi SSID の設定

LPNS 通知を有効にするには、まず Wi-Fi SSID を設定する必要があります。

始める前に

ログインフロー更新による OAuth エンタープライズパラメータが有効になっていることを確認してください。『Cisco Unified Communications Manager システム設定ガイド』の「共通のエンタープライズパラメータ」の項を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザーの管理（User Management）] > [ユーザー設定（User Settings）] > [UCサービス（UC Service）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **UC サービスタイプ** ドロップダウンから **[Jabber クライアントの設定 (jabber-config.xml)**] を選択し、 **次へ**をクリックします。

ステップ 4 Wi-Fi SSID の **名前** と **説明** を入力します。

ステップ 5 **Jabber 設定パラメータ** エリア内:

a) **[セクション（Section）]** ドロップダウンから **[電話機（Phone）]** を選択します。
b) **パラメータ** ドロップダウンから **LocalPushSSIDList**を選択します。
c) **値**に、Wi-Fi アドレス ID を入力します。 有効な文字は英数字です。

最大 10 個の ID をセミコロンで区切って入力できます。

ステップ 6 **[保存（Save）]** をクリックします。

Jabber サービス プロファイルをエンド ユーザに関連付ける

Wi-Fi SSID を設定したら、サービス プロファイルを作成してエンドユーザに関連付ける必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザー管理（User Management）]** > **[ユーザー設定（User Settings）]** > **[サービスプロファイル（Service Profile）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 Jabber サービスプロファイルの **名前** と **説明** を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 **Jabber クライアント設定 (jabber-config.xml)** エリアで、 **モバイル** ドロップダウンから前のステップで作成した UC サービスプロファイルを選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 Cisco Unified CM の管理から、**[ユーザ管理]** > **[エンドユーザ]** を選択し、 **[検索]** をクリックします。

エンドユーザの一覧が表示されます。

ステップ 8 選択したユーザの **ユーザ ID** をクリックします。

ステップ 9 **サービス設定** エリアで、 **UC サービスプロファイル** ドロップダウンメニューから **手順 3 - 4 で作成した Jabber サービスプロファイル** を選択し、[**保存**] をクリックします。

選択したエンド ユーザに関連付けられているデバイスに、選択した Jabber サービス プロファイルが設定されます。 選択した構成を含む `jabber-config.xml` ファイルが Webex アプリにダウンロードされます。

Unified Communications Manager のフェイルオーバーがある場合の LPNS の動作

Unified Communications Manager グループは、デバイスを登録できる最大 3 つの冗長サーバの優先順位リストです。 各グループには、1 個のプライマリ ノードと最大 2 個のバックアップ ノードが含まれます。 一覧表示するノードの順序によって優先順位が決まります。最初のノードがプライマリノード、2 番目がバックアップノード、3 番目がターシャリノードになります。

Unified CM では、デバイス プールはデバイスのグループに共通の設定セットを提供し、特定のロケーション情報に従ってデバイスを設定できるようにします。[デバイスプールの設定] を通じて、デバイスを Cisco Unified Communications Manager グループに指定することができます。

プライマリ ノードの LPNS サービスがダウンすると、Webex アプリ クライアントがそれを検出し、デバイス プール内の次の優先順位のノードに接続します。

プライマリ ノードの LPNS サービスが起動しているとき、Webex アプリ クライアントは、以前に WebSocket セッションを確立したノードに接続されたままになります。 現在アクティブなセッションが閉じられているか、または壊れた場合、クライアントはより高い優先順位のノードへのフォールバックを試みません。

クライアントは、フェイルオーバーを行う前に、より優先順位の高いノードが使用可能かどうかを確認します。 セッションを確立する前に、最も高い優先順位のノードをハントすると、セッションが確立されるまで遅延が発生します。 LPNS は、クライアントが利用可能な LPNS サーバの 1 つに接続しなおすまで、プッシュ通知を配信できません。

リモート LPNS プッシュ通話処理のための LPNS の高可用性

LPNS の高可用性は、iOS Webex アプリ クライアントの LPNS セッションにフェールオーバーと冗長性を提供します。 これにより、すべてのクライアントのアクティブなセッション情報が、LPNS が実行されているすべてのノードに知られていることが保証されます。 これにより、デバイスの現在アクティブな呼処理ノードの場所に関係なく、クライアントにプッシュ通知がシームレスに配信されます。

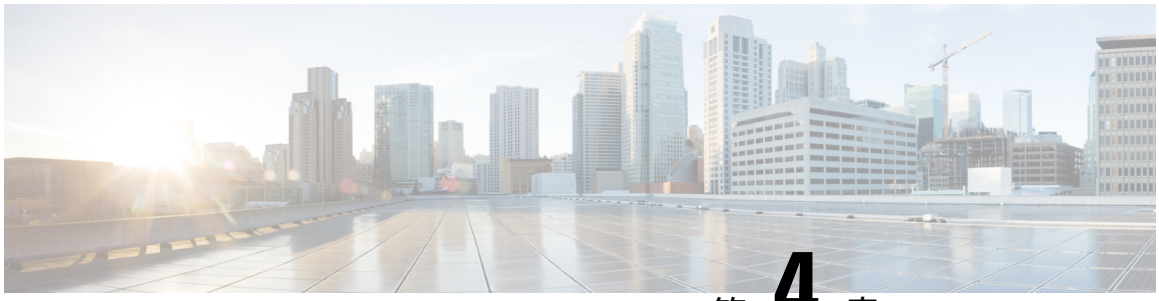
LPNS 連携動作と制限事項

LPNS では、次の機能の連携動作と制限事項が確認されています。

表 *8 : LPNS* の機能の連携動作と制限事項

機能	連携動作と制限事項
ネットワークアドレス変換（NAT）およびファイアウォール接続	LPNS へのクライアント WebSocket 接続を維持するように NAT およびファイアウォールデバイスを構成することをお勧めします。

機能	連携動作と制限事項
LPNS 高可用性	高可用性は、Webex アプリがその CallManager グループで構成されている次の利用可能な Unified Communications Manager にフェールオーバーしようとする場合に Unified Communications Manager で保証されます。クライアントの WebSocket フェールオーバーが発生すると、Webex アプリがフォアグラウンドに移動するたびに、iOS デバイスが Unified Communications Manager に登録されます。その後、Unified Communications Manager は確立された WebSocket を介して音声通話通知を配信します。
証明書の要件	• iOS 証明書の要件により、LPNS 機能に自己署名証明書は推奨されません。詳細については、「https://support.apple.com/en-us/HT211025」を参照してください。 • LPNS を使用する場合は、iOS 証明書の要件（証明書の有効期間が 397 日未満）を確認するパブリック CA 署名付き証明書をお勧めします。 • iOS 証明書を確認するプライベート CA 署名付き証明書を使用している場合は、証明書を iOS 信頼ストアにインポートしてください。 • LPNS の展開は、Apple の証明書要件を満たす必要があります。



第 4 章

プッシュ通知 (クラウド展開)

Webex Messenger を使用したクラウドの導入

スタートアップ時に、Android および iOS 版 Cisco Jabber または Cisco Webex クライアントは、Cisco WebEx Messenge と Apple クラウドの両方に登録します。Android および iOS 版の Cisco Jabber クライアントまたは Cisco Webex クライアントがバックグラウンドに移行した場合、Webex Messenger から Cisco Jabber または Cisco Webex への標準の通信チャネルは利用できなくなります。プッシュ通知は、Jabber クライアントに到達するための代替チャネルを提供します。

インスタントメッセージの場合、IM 通知が Apple クラウド経由で Cisco Jabber または Cisco Webex クライアントに送信されます。ユーザーが IM 通知をクリックすると、Cisco Jabber または Cisco Webex クライアントがフォアグラウンドに戻って、Webex Messenger とのセッションを再開して、インスタントメッセージをダウンロードします。

音声コールとビデオコールの場合、コールは Apple クラウド経由で Cisco Jabber または Cisco Webex クライアントに送信されます。Cisco Jabber または Cisco Webex クライアントがプッシュ通知を受信すると、クライアントはフォアグラウンドに戻ってクライアントが呼出音を鳴らします。

プッシュ通知の設定

IM のみのクラウドを導入している場合は、プッシュ通知を有効にするための設定は必要ありません。Webex Messenger は、デフォルトで Android および iOS 版 Cisco Jabber または Cisco Webex クライアントのプッシュ通知をサポートしています。

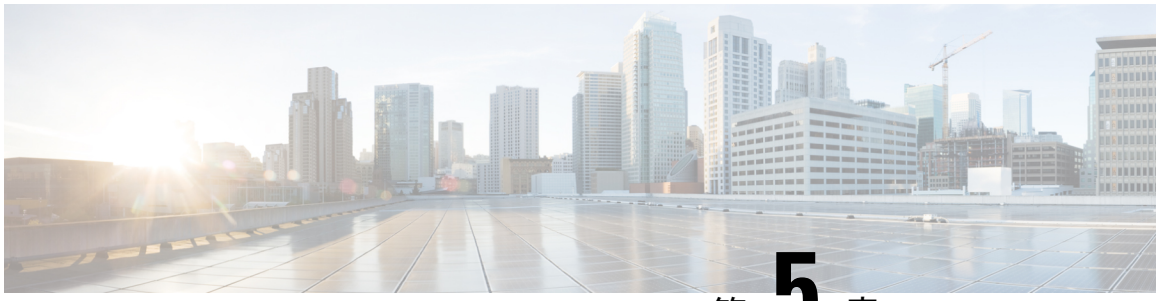
音声コールとビデオコールのサポートを追加するには、オンプレミスの Unified Communications Manager をプッシュ通知用に設置する必要があります。詳細については、「プッシュ通知 (オンプレミス展開) （7 ページ）」章の前提条件と設定タスクを参照してください。

一般的な Cisco Webex Messenger の設定については、『Cisco Webex Messenger 管理ガイド』を参照してください。

クラウド展開の終了済みプッシュ通知

Webex Messenger が正常にシャットダウンされた場合、終了したプッシュ通知が Android および iOS 版 Cisco Jabber または Cisco Webex クライアントに送信されます。終了したプッシュ通知は、サーバーのシャットダウンをユーザーに通知し、すべての queud インスタントメッセージ、プレゼンスの更新、およびその他の XMPP スタンザ (チャットルーム invite など) が失われたことをユーザーに通知します。ユーザーは、Cisco Jabber または Cisco Webex をフォアグラウンドに移行させて、新しいセッションに対してプッシュ通知が有効になっている新しいセッションを開始する必要があります。

Webex Messenger サーバーに障害が発生した場合、終了していないプッシュ通知は送信されません。サーバーでキューに入れられ、クライアントへの配信を待機している、キューに入れられたインスタントメッセージ、プレゼンス更新、および XMPP スタンザはすべて失われます。ユーザーは、Cisco Jabber または Cisco Webex をフォアグラウンドに戻して、新しいセッションに対してプッシュ通知が有効になっている新しいセッションを開始する必要があります。



第 5 章

証明書とパフォーマンスの監視

クラウド接続の証明書

オンプレミスの展開で、Cisco によるクラウド証明書の自動管理を行わないことを選択した場合、またはシステムのインストールファイルに含まれていない新しい証明書要件が追加された場合、証明書を手動で取得してアップロードする必要があります。 このような場合、CA サイトから手動で証明書をダウンロードし、 Unified Communications Manager と IM and Presence Service にアップロードする必要があります。 このオプションを選択するには、Unified Communications Manager の **[Cloud オンボーディング設定（Cloud Onboarding Configuration）]** ウィンドウの **[この信頼に必要なシスコクラウドサービス CA 証明書をシスコが管理する（I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust）]** チェックボックスをオフにします。

クラウド接続のルート証明書

証明書を手動でアップロードする場合に取得する必要があるルート証明書については、下の表を参照してください。 Unified Communications Manager および IM and Presence Service に証明書をアップロードする方法については、『Cisco Unified Communications Manager セキュリティガイド』の「証明書」の項を参照してください。 **「証明書の目的」** として **tomcat-trust** を選択してください。

表 *9*: クラウド接続のルート証明書

この **CA** により署名されたクラウドホスト	以下により信頼される必要がある	この目的のために	発行 **CA**	**SHA256** の指紋 **(Thumbprint)**
Common Identity (CI) サービス	Unified Communications ManagerIM and Presence Service	1. Cisco Unified Communications Manager は Cisco Push REST サービスで認証するための CI マシントークンを要求します。 2. Unified Communications Manager、IM and Presence Service、および Cisco Push REST サービス間の https 通信をセキュアにします。	O = IdenTrust CN = IdenTrust 商用ルート CA 1	5D 56 49 9B E4 D2 E0 8B CF CA D0 8A 3E 38 72 3D 50 50 3B DE 70 69 48 E4 2F 55 60 30 19 E5 28 AE
Cisco Webex	Cisco Unified Communications Manager および IM and Presence Service	Unified Communications Manager は、Fusion Onboarding Service (FOS) と通信して CI マシンアカウントをプロビジョニングします。	O = Go Daddy Group, Inc. OU = Go Daddy クラス 2 認証局	C3 84 6B F2 4B 9E 93 CA 64 27 4C 0E C6 7C 1E CC 5E 02 4F FC AC D2 D7 40 19 35 0E 81 FE 54 6A E4

クラウド証明書を自動的にアップロードできるシナリオ

次の表は、 **Cisco Cloud Onboarding Configuration** ウィンドウで **この信頼に必要なCisco Cloud Service CA証明書をCiscoに管理させたい** チェックボックスが選択されている場合、オンボーディングが成功するか、または証明書を手動でアップロードする必要があるかどうかを示しています。

表 *10 :* クラウド証明書を自動的にアップロードできるシナリオ

シナリオ	インストール iso ファイルには必要な証明書が含まれています。	Cisco に証明書の要件を管理させることを選択しました	オンボーディングは成功しました。
初回オンボーディング	可	可	可
初回オンボーディング	いいえ。証明書の要件は、インストール iso が作成された後に変更されました	可	いいえ。新しい証明書は手動で入手してアップロードする必要があります。 前の表「クラウド接続のルート証明書」を参照してください。
オンボーディング済みですが、新しい証明書の要件が生じました。	ご利用のシステムには必要な証明書が含まれません	可	はい。 システムは新しい証明書を自動的に取得し、インストールすることができます。

プッシュ通知のアラーム

次の表では、リリース 11.5(1)SU3 の Unified Communications Manager および IM and Presence Service でプッシュ通知通話サポートに追加されたアラームを示します。

表 *11 :* プッシュ通知のアラーム

アラーム	説明
Cisco CallManager のアラーム	
PushNotificationServiceUnavailable	**詳細**: Cisco プッシュ通知サービスに接続できません。 CallManager サービスは、Cisco Cloud にプッシュ通知を送信するための接続を必要とします。 **重大度**: ALERT_ALARM **アクション**:Cisco Unified Serviceability で、Cisco プッシュ通知サービスの状況が実行中であることを確認してください。 サービスが停止している場合は、開始してください。 サービスが実行している場合、再起動します。

アラーム	説明
PushNotificationInvalidDeviceTokenResponse	**説明** : 無効なデバイストークンのため、CallManager Serviceから送信されたプッシュ通知に対して、クラウドがエラーコード 410 を返しました。 この iOS Cisco Jabber または Cisco Webex デバイスのプッシュ通知は、iOS Cisco Jabber および Webex デバイスにより有効なデバイストークンが設定されるまで停止されます。 **重大度**: ERROR_ALARM **アクション**:ユーザは、iOS デバイス上の Cisco Jabber または Webex クライアントからいったんログアウトし、ログインし直してください。
PushNotificationServiceAccessTokenUnavailable	**詳細:**Cisco プッシュ通知サービス (CPNS) は有効なアクセストークンを持っていません。Unified Communications Manager はクラウドにプッシュ通知を送信するために有効なアクセストークンが必要です。認証エラーまたはネットワークエラーのため、このアクセストークンはクラウドからは入手できません。 **重大度:** ALERT_ALARM **アクション:Cisco Cloud Onboarding Configuration** ウィンドウをチェックして、オンボーディングプロセスが正常に完了したことを確認してください。 問題が解決しない場合は、Cisco TAC に連絡して支援を求めてください。
Cisco プッシュ通知サービスのアラーム	
StartFailed	**詳細:** このアラームは、内部障害により Cisco プッシュ通知サービスが開始できなかったことを示します。 **重大度:** CRITICAL_ALARM **アクション:** Cisco プッシュ通知サービスを再起動してください。 問題が解決しない場合は、Cisco プッシュ通知サービスのアプリケーション ログを確認し、Cisco TAC に連絡してサポートを受けてください。

アラーム	説明
AccessTokenInvalid	**説明:** このアラームは現在のアクセストークンの有効期限が切れ、無効になり、新しいアクセストークンが利用できないことを示します。 **重大度:** ALERT_ALARM **アクション:Cisco Cloud Onboarding Configuration** ウィンドウで、オンボーディングプロセスが正常に完了したことを確認してください。 問題が引き続き発生する場合は、Cisco TAC に連絡して支援を求めてください。
HttpClientPoolCreationError	**詳細:** HTTP クライアント接続プール作成時のエラーを示します。 **重大度:** ALERT_ALARM **アクション:Cisco Cloud Onboarding Configuration** ウィンドウを確認して、HTTP プロキシの設定が正しいことを確認してください。 さらに、オンボーディング プロセスが完了していることを確認してください。
Cisco XCP Config Manager	
PushNotificationFailed	**詳細:** Cisco XCP Config Manager はプッシュ通知を送信できませんでした。 **重大度:** CRITICAL_ALARM **アクション:** エラーコードを確認し、指示されたエラーアクションに従ってください。
PushNotificationFailedInvalidDeviceToken	**詳細:** Cisco Cloud へのプッシュ通知の送信に失敗しました。デバイストークンが無効なためです。 **重大度:** CRITICAL_ALARM **アクション:** ユーザは Jabber に再ログインする必要があります。

アラーム	説明
PushNotificationFailedInvalidAccessToken	**詳細:** Cisco Cloud へのプッシュ通知の送信に失敗しました。アクセストークンが無効なためです。 **重大度:** CRITICAL_ALARM **アクション**：IM and Presence Service の Cisco XCP Config Manager サービスのログを確認し、AccessToken が適切なタイミングで取得および更新されたかどうかを確認します。AccessToken が取得され、タイムリーに更新された場合は、Cisco Cloud でさらなるデバッグを詳しく調査してください。
AccessTokenFetchFailed	**詳細:** Cisco XCP Config Manager はアクセストークンを取得できませんでした。 **重大度:** CRITICAL_ALARM **アクション:** エラーコードを確認し、指示されたエラーアクションに従ってください
XCPConfigMgrAccessTokenIsNull	**詳細:** Cisco XCP Config Manager はアクセストークンを取得できませんでした。 **重大度:** **アクション:** IM およびプレゼンス サービス ノードは Cisco クラウドに接続してアクセストークンを取得する必要があります。 次のことを確認してください。 • アクセストークン URL と更新トークンが有効であることを確認してください。 • [**Cisco Cloud Onboarding**] ウィンドウで、プロキシの詳細が正しいことを確認してください。 • Cisco クラウドへの接続を確認してください。
Cisco Jabber のアラーム	
APNSAlarm	**詳細:** iOS Jabber クライアントはプッシュ通知を処理できませんでした。 **重大度:** ALERT_ALARM **アクション:** Cisco TACに連絡してください。

アラーム	説明
未読メッセージの警告 （注） このアラートは、12.5 (1) より前のリリースでのみ表示されます。この問題は 12.5 (1) に修正されています。	**説明** : iOS Jabber クライアントが次のメッセージを受け取ります: タイムアウトにより、未読メッセージがサーバーから削除される可能性があります。 Jabber にログインして未読メッセージを確認してください。 **重大度:** ALERT_ALARM **条件:** Cisco Jabber for iPhone がバックグラウンドで動作しています。ユーザはアプリケーションを閉じる前に Cisco Jabber からサインアウトしませんでした。

プッシュ通知のパフォーマンス カウンター

Apple プッシュ通知のパフォーマンス カウンタ

次の表では、Cisco Unified Real Time Monitoring ToolにIM and Presence Serviceのオンプレミス展開のプッシュ通知をサポートするために追加されたカウンターを示します。 Unified Communications Manager カウンターは特定の APNS サブスクライバー サービス (たとえば、APNS、APNS:beta、APNS:dev、APNS:test、APNS:load) に対してのみ増加することに注意してください。 例えば、サブスクライバーサービスが「APNS:beta」の場合、APNS:beta カウンターのみが増加し、APNS:dev カウンターは増加しません。 Cisco Jabber および Cisco Webex のサービスタイプにより、どの購読者サービスが使用されるかが決まります。

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
Cisco CallManager カウンタ		
NumberOfPushReqSent	Cisco CallManager サービスにより送信されたプッシュ通知要求の総数。	すべての APNS 購読者サービス。
受信プッシュ応答数	Cisco CallManager サービスが受信したプッシュ通知応答の総数。	任意の APNS 利用者サービス

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
NumberOfPushErrorResReceived	Cisco CallManager サービスが受信し、200 OK 以外の応答コードを持つプッシュ通知応答の総数。 Cisco Push Notification Service (CPNS) と Cloud PushRest の間の TLS ハンドシェイクが失敗した場合、このカウンターは、TLS ハンドシェイクの失敗が原因で送信できなかったプッシュ要求に対して増分されます。	すべての APNS 購読者サービス。
CustomRegionNumofMsgPushReqSent	CallKit が無効になっているカスタム地域デバイスへの呼び出しが行われたときに、CallManager サービスから送信されたメッセージ プッシュ通知要求の合計数。	すべての APNS 購読者サービス。
CustomRegionNumofMissedCallMsgPushReqSent	CallKit が無効になっている、CallManager サービスからカスタム地域デバイスに送信された不在着信メッセージ プッシュ通知要求の合計数。	任意の APNS 利用者サービス
CustomRegionNumofSharedCancelMsgPushReqSent	共有回線シナリオで、CallKit が無効になっているカスタム地域デバイスに、CallManager サービスから送信された通話キャンセル メッセージ プッシュ通知リクエストの総数。	任意の APNS 利用者サービス
Cisco Mobility Manager カウンター		
MobilityPushNotificationCallsExtendedToMIDueToTimeout	これは Cisco Jabber または Cisco Webex がプッシュ通知を受信してから「Cisco Jabber デュアルモード (iPhone) 着信通話プッシュ通知待機タイマー」が切れるまでに、モビリティ ID の宛先に送信された、Cisco Jabber または Cisco Webex が登録しなかった通話の合計数を表します。	任意の APNS 利用者サービス
MobilityPushNotificationCallsExtended ToJabber	これは、「Jabber デュアルモード (iPhone) 着信プッシュ通知待機タイマー」が切れる前にプッシュ通知を受け取ってから Cisco Jabber に正常に登録された通話の合計数を表します。	任意の APNS 利用者サービス
Cisco XCP Config Manager カウンター		

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
NumberOfPushSuccess	正常に送信されたプッシュ通知の数。	すべての APNS 購読者サービス。
プッシュ失敗数	プッシュ通知の送信に失敗した回数。	すべての APNS 購読者サービス。
ターゲットが無効です	無効なターゲットが原因で失敗したプッシュ通知の合計数。	すべての APNS 購読者サービス。
ターゲットの期限切れ	期限切れのターゲットが原因で失敗したプッシュ通知の合計数。	任意の APNS 利用者サービス
Cisco XCP プッシュカウンタ		
PushEnabledSessionsApns	APNSを利用者サービスとして持つAPNSクライアントのプッシュ有効セッション数。 このカウンターは、プッシュ通知が有効になると増加し、プッシュ通知が無効になるか、セッションが終了すると減少します。	APNS
PushEnableReqRcvdAPNs	60秒の間隔で、APNSを購読サービスとしているクライアント向けに受信したプッシュ通知の有効化リクエストの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS
PushErrorsApns	60 秒間隔中に受信したプッシュ エラーの数。このカウンターは 60 秒ごとに 0 にリセットされます。	APNS
PushSentSilentApns	60 秒間隔中にサイレントモードのセッションに送信されたメッセージの数。このカウンターは 60 秒ごとに 0 にリセットされます。	APNS
PushSentDisconnApns	中断状態のセッションに送信されたメッセージの数、60秒の間隔で。 このカウンターは60秒ごとに 0 にリセットされます。	APNS
PushEnabledSessionsApnsBeta	APNS:betaをサブスクライバーサービスとして使用するクライアントのプッシュが有効なセッションの数。 このカウンターは、プッシュ通知が有効になると増加し、プッシュ通知が無効になるか、セッションが終了すると減少します。	APNS:beta

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
PushEnableReqRcvdApnsBeta	60 秒間隔で、APNS:beta をサブスクライバーサービスとして使用するクライアントについて受信したプッシュ有効化リクエストの数。このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:beta
PushErrorsApnsBeta	サブスクライバーサービスが APNS:beta の場合、60 秒間隔中に受信したプッシュエラーの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:beta
PushSentSilentApnsBeta	サブスクライバーサービスが APNS:beta である場合に、60秒の間にサイレントモードのセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:beta
PushSentDisconnApnsBeta	サブスクライバーサービスが APNS:beta である場合に、60秒の間に一時停止状態のセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:beta
PushEnabledSessionsApnsDev	APNS:dev をサブスクライバーサービスとして使用するクライアントのプッシュが有効なセッションの数。 このカウンターは、プッシュ通知が有効になると増加し、プッシュ通知が無効になるか、セッションが終了すると減少します。	APNS:開発
PushEnableReqRcvdApnsDev	60 秒の間隔で、APNS:dev をサブスクライバーサービスとして使用するクライアントについて受信したプッシュ有効化リクエストの数。このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:dev
PushErrorsApnsDev	サブスクライバーサービスが APNS:dev の場合、60 秒間隔中に受信したプッシュエラーの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:dev

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
PushSentSilentApnsDev	サブスクライバーサービスが APNS:dev である場合に、60 秒の間にサイレントモードのセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:dev
PushSentDisconnApnsDev	サブスクライバーサービスが APNS:dev である場合に、60 秒の間に一時停止状態のセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:dev
PushEnabledSessionsApnsLoad	APNS:load をサブスクライバーサービスとして使用するクライアントのプッシュが有効なセッションの数。 カウンターはプッシュ通知が有効になると増加し、プッシュ通知が無効になるかセッションが終了すると減少します。	APNS:load
PushEnableReqRcvdApnsLoad	60 秒間隔で、APNS:load をサブスクライバーサービスとして使用するクライアントについて受信したプッシュ有効化リクエストの数です。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:load
PushErrorsApnsLoad	サブスクライバーサービスが APNS:load の場合、60 秒間隔中に受信したプッシュエラーの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:load
PushSentSilentApnsLoad	サブスクライバーサービスが APNS:load である場合に、60秒の間にサイレントモードのセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:load
PushSentDisconnAPNsLoad	サブスクライバーサービスが APNS:load である場合に、60秒の間に一時停止状態のセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:load

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
PushEnabledSessionsApnsTest	APNS:test をサブスクライバサービスとして使用するクライアントのプッシュが有効なセッションの数。 このカウンターは、プッシュ通知が有効になると増加し、プッシュ通知が無効になるか、セッションが終了すると減少します。	APNS:テスト
PushEnableReqRcvdApnsTest	60 秒間隔で、APNS:test をサブスクライバーサービスとして使用するクライアントについて受信したプッシュ有効化リクエストの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:テスト
PushErrorsApnsTest	登録者サービスが APNS:test の場合、60 秒間隔中に受信したプッシュ エラーの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:test
PushSentSilentApnsTest	登録者サービスが APNS:test の場合、60 秒の間にサイレントモードのセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:テスト
PushSentDisconnApnsTest	サブスクライバーサービスが APNS:test である場合に、60 秒の間に一時停止状態のセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	APNS:テスト

Android プッシュ通知のパフォーマンス カウンター

次の表は、リリース 12.5(1)SU3 以降の Unified Communications Manager と IM and Presence Service の Android プッシュ通知をサポートするために Cisco Unified Real Time Monitoring Tool に追加されたカウンターを示しています。

（注） メッセージング カウンターは Cisco Jabber にのみ適用されます。 Cisco Webex クライアントは、メッセージングに IM and Presence Service ではなく、Cisco Webex クラウドを使用します。

（注） プッシュが有効なCisco JabberまたはCisco Webexクライアントのユーザが FCM または FCM:dev をサブスクライバーサービスとして使用して Android デバイスからログインすると、FCM (Firebase Cloud Messaging) および FCM:dev カウンターが増分します。

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
Cisco XCP プッシュカウンタ		
PushEnabledSessionsFcm	登録者サービスとしてFCMを持つクライアントのプッシュが有効なセッションの数。 このカウンターは、プッシュが有効な Cisco Jabber または Cisco Webex ユーザが FCM を使用してサブスクライバーサービスとして Android デバイスにログインすると増分し、プッシュ通知が無効になるか、クライアントセッションが終了すると減ります。	FCM
PushEnableReqRcvdFcm	60 秒の間隔で、FCM をサブスクライバー サービスとして使用するクライアントの IM and Presence サーバーが受信したプッシュ有効化リクエストの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	FCM
PushErrorsFcm	登録者サービスが FCM の場合に、60 秒間に受信したプッシュ エラーの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	FCM
PushSentSilentFcm	サブスクライバーサービスが FCM である場合に、60 秒の間にサイレントモードのセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。 Android デバイスの Cisco Jabber または Cisco Webex アプリケーションがバックグラウンドになると、プッシュが有効なクライアントセッションがサイレントモードに切り替わります。	FCM

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
PushSentDisconnFcm	サブスクライバーサービスが FCM である場合に、60 秒の間に一時停止状態のセッションに送信されたメッセージの数。 このカウンターは 60 秒ごとに 0 にリセットされます。 Android デバイス上の Cisco Jabber または Cisco Webex アプリケーションがバックグラウンドになり、ネットワーク接続が終了すると、プッシュが有効なクライアントセッションは一時停止状態に移行します。	FCM
PushEnabledSessionsFcmDev	FCM:dev をサブスクライバサービスとして持つクライアントのプッシュ有効セッション数。 このカウンターは、プッシュが有効な Cisco Jabber または Cisco Webex ユーザが FCM:dev を使用して Android デバイスにサブスクライバーサービスとしてログインすると増分し、プッシュ通知が無効になるか、クライアントセッションが終了すると減ります。	FCM:dev
PushEnableReqRcvdFcmDev	60 秒の間隔で、FCM:dev をサブスクライバーサービスとして使用するクライアントの IM and Presence サーバーが受信したプッシュ有効化リクエストの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	FCM:dev
PushErrorFcmDev	サブスクライバーサービスが FCM:dev の場合、60 秒の間に受信したプッシュ エラーの数。 このカウンターは 60 秒ごとに 0 にリセットされます。	FCM:dev

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
PushSentSilentFcmDev	サブスクライバーサービスが FCM:dev である場合に、60 秒の間にサイレントモードのセッションに送信されたメッセージの数。このカウンターは 60 秒ごとに 0 にリセットされます。 Android デバイスの Cisco Jabber または Cisco Webex アプリケーションがバックグラウンドになると、プッシュが有効なクライアントセッションがサイレントモードに切り替わります。	FCM:dev
PushSentDisconnFcmDev	登録者サービスが FCM:dev の場合、60 秒間に中断状態のセッションに送信されたメッセージ数。 このカウンターは 60 秒ごとに 0 にリセットされます。 Android デバイスの Jabber アプリケーションがバックグラウンドになり、ネットワーク接続が終了すると、プッシュが有効なクライアントセッションは中断状態に移行します。	FCM:dev

LPNS アラーム

重要 このセクションは、リリース 14SU3 以降に適用されます。

次の表では、LPNS をサポートするために追加されたアラームの詳細を示します Unified Communications Manager。

表 *12 : LPNS* のアラーム

Cisco LPNS アラーム	説明
LocalPushNotificationInvalidOAuthToken	**詳細:** Webex クライアントが無効/期限切れの oAuth トークンを返しました。 CallManager は接続を削除し、このクライアントへのローカル プッシュ通知の以降の送信を停止します。 **重大度:** ALERT_ALARM **アクション:** 更新/アクセストークンを更新するために、モバイル上の Webex アプリと Cisco Unified CM の接続を確認してください。
ローカルプッシュ通知サービスが利用できません	**詳細:** Cisco ローカルプッシュ通知サービスに接続できません。 CallManager サービスは、モバイルの Webex アプリにローカル プッシュ通知を送信するために接続を必要とします。 **重大度:** CRITICAL_ALARM **アクション:** Cisco プッシュ通知サービスおよび Cisco ローカル プッシュ通知サービスを再起動してください。 問題が引き続き発生する場合、アプリケーション ログで Cisco ローカルプッシュ通知サービスを確認し、Cisco TAC に連絡してサポートを受けてください。
ローカルプッシュ開始に失敗しました	**説明:** このアラームは、内部障害が原因で Cisco ローカルプッシュ通知サービスを開始できなかったことを示します。 **重大度:** ALERT_ALARM **アクション:** Cisco ローカルプッシュ通知サービスを再起動してください。 問題が引き続き発生する場合、ローカル プッシュ通知サービスのアプリケーション ログを確認し、Cisco TAC に連絡してサポートを受けてください。

LPNS のパフォーマンス カウンター

重要 このセクションは、リリース 14SU3 以降に適用されます。

次の表は、Unified Communications Manager のオンプレミス展開の LPNS をサポートするために Cisco Unified リアルタイム監視ツールに追加されたカウンターの詳細を示します。

表 *13 : LPNS* のパフォーマンス カウンター

RTMT カウンタ	カウンタの説明	サブスクライバーサービスが次のように設定されている場合、カウンターが増加します...
Cisco CallManager カウンタ		
NumberOfLocalPushReqSent	Cisco CallManager サービスが送信したローカル プッシュ通知要求の合計数。このカウンターはローカル プッシュ要求が送信されるノードから更新されます。	任意の LPNS 購読者サービス。
NumberOfLocalPushResReceived	Cisco CallManager サービスが受信したローカル プッシュ通知応答の合計数。このカウンターはローカル プッシュ応答が受信されるノードから更新されます。	任意の LPNS 購読者サービス。
NumberOfLocalPushTimout	タイムアウトになったローカルプッシュ通知リクエストの合計数。	任意の LPNS 購読者サービス。
NumberOfLocalPushErrorResReceived	Cisco CallManager サービスが受信した、エラー レスポンス コードのローカル プッシュ通知レスポンスの合計数。	任意の LPNS 購読者サービス。
NumberofMissedCallLocalPushReqSent	CallManager サービスからデバイスに送信された不在着信のローカル プッシュ通知要求の合計数。	任意の LPNS 購読者サービス。
NumberofSharedCancelLocalPushReqSent	共有回線シナリオで、CallManager サービスからデバイスに送信されたコール ローカル プッシュ通知キャンセル要求の合計数。	すべての LPNS 購読者サービス。

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。