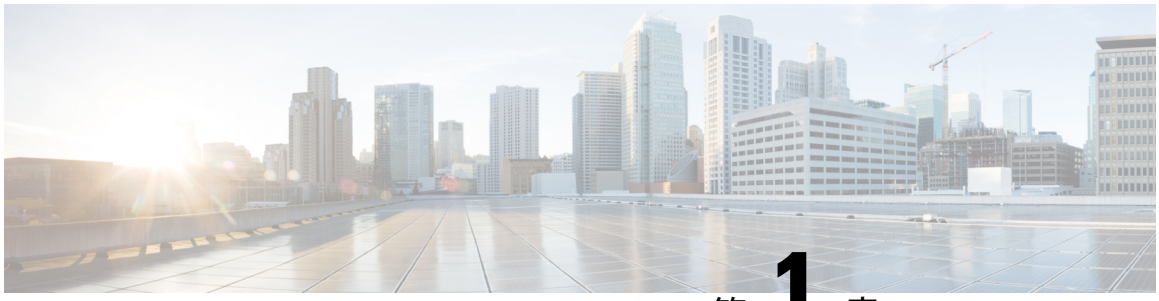
Cisco Unified Communications Manager および IM and Presence Service リリース 12.5（1) のリリース ノート

初版：2019 年 1 月 22 日

最終更新：2020 年 3 月 20 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

このリリースについて

はじめに

これらのリリースでは、Ciscoユニファイド コミュニケーション マネージャ (ユニファイド コミュニケーション マネージャ) および Ciscoユニファイド コミュニケーション マネージャ IM and Presence Service (IM およびプレゼンスサービス) の新機能、制限事項 および注意事項について説明します。このリリース ノートは、メンテナンス リリースごとに毎回更新されていますが、パッチまたはホットフィックス向けには更新されていません。

ユニファイド コミュニケーション マネージャ は、Cisco Unified Communications システムの呼処理コンポーネントであり、企業のテレフォニー機能を拡張して、IP 電話、メディア処理装置、VoIP ゲートウェイ、モバイル デバイス およびマルチメディア アプリケーションを利用可能にします。

IM and Presence Serviceは、ユーザが特定の時間に通信デバイス (電話機など) を使用しているかどうかなど、ユーザのアベイラビリティに関する情報を収集します。また、ウェブ コラボレーションまたはビデオ会議が有効かどうかなど、個々のユーザの通信機能に関する情報も収集できます。Cisco Jabberやユニファイド コミュニケーション マネージャなどのアプリケーションは、この情報を使用して従業員間の生産性を向上させます。従業員が同僚との接続をより効率的にし、コラボレーション通信に最も効果的な方法を決定するのに役立つ。

（注） 過去は、輸出免許、政府規制および輸入の制限により、当社のユニファイドコミュニケーションマネージャとIM and Presence Serviceは世界中で制限されていました。この問題に対処するための無制限の米国輸出分類を取得しました。IM and Presence Serviceは、輸出規制なし(xu)バージョンのみをサポートします。無制限バージョンは、強力な暗号化機能が含まれていないため、IM and Presence Serviceの以前のリリースとは異なります。

無制限バージョンのリリースをインストールすると、制限バージョンにアップグレードできなくなります。無制限バージョンを含むシステムでは、制限バージョンの更新インストールを実行できません。

サポートされるバージョン

次のソフトウェア バージョンは、リリース 12.5(1) でサポートされています。

- Unified Communications Manager 12.5.1.10000-22
- IM and Presence Service 12.5.1.10000-22

このリリースのドキュメント

リリース 12.5 (1) で入手可能なマニュアルの完全なリストについては、このリリースのマニュアルガイド(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.html) を参照してください。

アップグレード手順

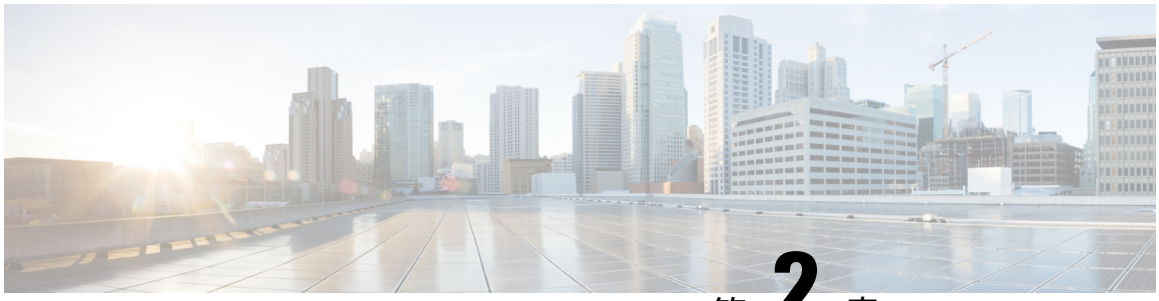
リリース 12.5(1) へのアップグレードについては、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html にある *Cisco Unified Communications Manager* および *IM and Presence Service* のアップグレードおよび移行ガイドをご覧ください。

アップグレード中の Spectre と Meltdown の脆弱性

このリリースのユニファイドコミュニケーション マネージャ、Cisco IM and Presence Service、Cisco Emergency Responder および Cisco Prime Collaboration の導入には、Meltdown および Spectre のマイクロプロセッサの脆弱性に対処するためのソフトウェア パッチが含まれています。

リリース 12.5(1) 以降にアップグレードする前に、Cisco Collaboration Sizing Tool を使用して、現在の展開をアップグレード済みの展開と比較するように、チャネルパートナーまたはアカウ

ントチームと連携させることをお勧めします。必要に応じて、VMリソースを変更して、アップグレードされた導入環境で最適なパフォーマンスが得られるようにします。



第 2 章

新機能および変更された機能

AES 80 ビット認証サポート

Ciscoユニファイド コミュニケーション マネージャ は、128 ビット暗号化キーと 80 ビット認証タグ暗号化アルゴリズムとして使用する Advanced Encryption Standard（AES）をサポートしています。このリリースでは、AES 32 ビット認証タグは、保留音 (MOH)、自動音声応答 (IVR) および警報の暗号化暗号として使用される 80 ビット認証タグに拡張されています。この機能拡張により、80 ビット認証タグを使用して、SIP 回線と SIP トランクを介して Secure Real-Time Transport Protocol (SRTP) コールを行うことができます。

詳細については、『*Cisco Unified Communications Manager の Security Guide*』の「Encrypted Phone Configuration ファイル設定」の章を参照してください。

無効な非アクティブ ユーザ アカウントの監査ログ

このリリースでは、Cisco Database Layer Monitor は非アクティブなユーザを無効にしてから、同じようにログを監査します。

Cisco Database Layer Monitor は、指定日数内に ユニファイド コミュニケーション マネージャ にログインしていない場合、スケジュールされたメンテナンス タスク時にユーザ アカウント ステータスを非アクティブに変更します。無効になっているユーザの詳細は自動的に監査され、監査ログには「<userID> user is inactive」というメッセージが表示されます。

アクティブではないユーザアカウントを無効にする方法の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の「ユーザ アクセスの管理」の章を参照してください。

認証済み Network Time Protocol のサポート

このリリースでは、ユニファイドコミュニケーションマネージャーは Autokey protocol による Network Time Protocol (NTP) 認証をサポートしています。このプロトコルは、公開キーインフラストラクチャ (PKI) ベースの認証と疑似ランダムハッシュシーケンスの組み合わせを使用します。以前は、NTP 認証は対称キーを介してのみ提供されていました。この更新では、いずれかの方法で NTP メッセージを認証できます。

この機能は、ネットワーク上の NTP メッセージに対して暗号化された PKI ベースの保護を提供することにより、システムのセキュリティを強化します。自動キーを使用して認証された NTP は、一般的な基準に準拠するために PKI ベースの認証が必須であるため、システムが一般的な基準のガイドラインを遵守するのに役に立ちます。

この機能を有効にするには Red Hat Package Manager (rpm) バージョン ntp-4.2.6 x86_64 p5-1 以降を使用して NTPv4 を実行している必要があります。

NTP 認証方法を選択します。

展開する NTP 認証方式を選択する場合は、次の点を考慮してください。

- RedHat は自動キーよりも対称キー認証を推奨しています。詳細については、「https://access.redhat.com/support/cases/#/case/list」を参照してください。
- 一般的な基準の遵守では、公開鍵を使用する必要があります。

コンフィギュレーション

パブリッシャノードで NTP を設定するのは、クラスタ内のすべてのサブスクライバの NTP 時間を自動的に同期する Ciscoユニファイド コミュニケーション マネージャ としてのみです。NTP および NTP 認証の設定方法の詳細については、『 *System Configuration Guide for Cisco Unified Communications Manager* 』の「configure NTP」の章を参照してください。

（注） Autokey を使用して NTP 認証を設定するには、まずシステムで共通基準モードを有効にする必要があります。コモンクライテリアモードの詳細については、「*Cisco Unified Communications Manager* のセキュリティガイド」の「FIPS セットアップ」の章を参照してください。

CLI リファレンス ガイドの更新

この機能をサポートするには、**ユーティリティの ntp auth 自動キー {enable | disable | status}**が追加されています。CLI の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

BE6000 ライセンスのサポート

スマートライセンス: BE6000 ライセンスのサポート

新しいコマンド**ユーティリティ BE6000Mode**が、ユニファイドコミュニケーションマネージャと IM and Presence コマンドライン インターフェイスに追加されます。

Business Edition 6000 ソリューションのユニファイドコミュニケーションマネージャ 12.5 (1) では、Business Edition 6000 starter pack ライセンスを使用するために BE6000 モードが必要です。

次のオプションが新しいコマンドで追加されました。

- [ユーティリティ (BE6000Mode)]: このオプションを使用すると、ユニファイドコミュニケーションマネージャで BE6000 モードを有効にすることができます。
- [BE6000Mode disable]: このオプションを使用すると、ユニファイドコミュニケーションマネージャで BE6000 モードを無効にできます。
- [ユーティリティのステータス (BE6000Mode status)]: このオプションを使用すると、ユニファイドコミュニケーションマネージャの BE6000 モードのステータスを表示できます。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「utils BE6000Mode」セクションを参照してください。

SIP トランクのコール管理記録

以前のリリースでは、ユニファイドコミュニケーションマネージャは SIP 電話のコール品質メトリックを含むコール管理レコード (Cmr) を生成しました。このリリースでは、ユニファイドコミュニケーションマネージャが生成した Cmr には、Cisco ユニファイド Border Element (CUBE) または IOS ゲートウェイを介した SIP トランクコールのコール品質メトリックが含まれています。この更新により、SIP トランクコールの音声品質メトリックを評価することができます。

CUBE は、BYE メッセージの P RTP-Stat ヘッダーのコール統計情報、または BYE メッセージへの 200 OK 応答を送信して、ユニファイドコミュニケーションマネージャの Cmr を更新します。コール統計には、送受信されたリアルタイムトランスポートプロトコル (RTP) パケット、送受信された合計バイト数、損失したパケットの総数、遅延ジッター、ラウンドトリップ遅延およびコール時間が含まれます。

SIP トランクの Cmr でのコール統計情報を報告するための前提条件

- Cisco Unified Border Element に Cisco IOS リリース 15.1(3)T 以降のリリースがインストールされて稼働中になっている必要があります。
- Cisco ASR 1000 シリーズ ルータに Cisco IOS XE Release 3.3S 以降のバージョンがインストールされて稼働中になっている必要があります。

詳細については、『*Cisco Unified Communications Manager* の *Call Detail Records Administration Guide*』の「コール管理記録」の章を参照してください。

SIP または TLS 認証済みコールのコール録音

12.5 (1) バージョンより前のバージョンでは、認証された電話機 (デバイスセキュリティモードが認証済みのセキュリティプロファイルを持つ電話機) は、コール録音機能の使用を許可されていませんでした。セキュリティ保護されていない電話機、またはセキュア/暗号化された電話機は、それぞれ非セキュアまたはセキュアなレコーダーでコール録音機能を使用できます。リリース 12.5 (1) では、Cisco Unified CM JTAPI インターフェイスは、新しいサービスパラメータ**認証済み電話録音**の値に基づいて認証された電話機での録音を可能にするように強化されています。

認証された電話機がコール録音機能を使用できるようにすることが期待されています。これは、新しく追加されたサービスパラメータ**認証済み電話機の録音**で設定された値によって異なります。これは次の値に設定できます。

- **録音を許可**する: 認証された電話はコールを録音できます。
- **録音を許可しない**: 認証された電話は、コール録音機能を使用できません。これがサービス パラメータのデフォルト値になります。動作は、現在の動作と同じです。

下位互換性

この機能は下位互換性があります。JTAPI は現在の API をサポートします。

Cisco JTAPI クライアントへのセキュリティアップデート

このリリースでは、Cisco JTAPI Client for Linux (32 および64ビット) プラグインは、RSA セキュリティプロバイダーではなく、シスコのセキュリティプロバイダーを使用します。

Cisco JTAPI パッケージのダウンロードの詳細

このリリースでは、Windows および Linux 用の JTAPI インストールファイルが zip ファイルを通じて提供されます。JTAPI をインストールする前に、Cisco ユニファイド CM Administration の [**アプリケーション**> **プラグイン**] ページでアクセス可能な zip ファイルを解凍する必要があります。

Zip パッケージには次のものが含まれます。

- Linux (32 および64ビット) または Windows (32 および64ビット) 用の JTAPI パッケージ
- マニュアル
- コードの例

Linux (32 および64ビット) の CiscoJ ライブラリは、プラグイン URL からダウンロードできます。

- https://<*IP address*>/plugins/lib_ciscoj_x32 .zip
- https://<*IP address*>/plugins/lib_ciscoj_x64 .zip

Zip ファイル (CiscoJTAPIWindows と .zip) は、次のインストーラに置き換わります。

- CiscoJTAPIClient-linux.bin
- CiscoJTAPIClient.exe
- CiscoJTAPIx64-Windows
- CiscoJTAPIx64-Linux.bin

（注） クラスパスと LD_LIBRARY_PATH の詳細については、zip ファイルの一部である readme ファイルを参照してください。

Cisco JTAPI クライアントのユーザインターフェイスの更新

[**プラグインの検索と一覧表示 (Find And List プラグイン)**] ウィンドウ (**アプリケーション** > **プラグイン**) では、次の変更が行われています。

- **Linux の CISCO jtapi 32 ビットクライアント**と、[**プラグイン名 (Plugin Name)**] 列の**LINUX リンクの Cisco jtapi 64 ビットクライアント**は、**Linux 32 ビットおよび64ビットの cisco jtapi クライアント**に変更されます。
- Windows**用 CISCO jtapi 32 ビットクライアント**および**プラグイン名**列の**windows リンク用 Cisco jtapi 64 ビットクライアント**は、**windows-32 ビットおよび64ビット用の cisco jtapi クライアント**に変更されています。

[**説明 (Description)**] 列の詳細が更新されます。詳細は、[Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスをご覧ください。

インストールの詳細については、『 *Cisco Unified Jtapi* 開発者ガイド』の *Cisco Unified Communications Manager* リリース *12.5 (1)* 』の「 「Cisco Unified jtapi インストール」 」 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.htmlの章を参照してください。

RFEL 7 への Cisco JTAPI サポート

このリリースでは、Cisco JTAPI は Linux オペレーティングシステムで64ビットの RHEL 7 をサポートしています。以前は、RHEL 6 がサポートされていました。

VMware のサポート

Cisco JTAPI は VMware ESXi バージョン 4.0 で使用されています。アプリケーションでは、VMware バージョンで Windows 2003 および Windows 2008 仮想マシンを使用して、Cisco JJTAPI を実行します。サポート対象の Java 仮想マシンについては、次の表を参照してください。

表 *1*:ユニファイド コミュニケーション マネージャでサポートされている *JVM* バージョン

オペレーティング システム	バージョン	ユニファイド CM 10.0	ユニファイド CM 10.5	ユニファイド CM 11.0	ユニファイド CM 11.5	ユニファイド CM 12.0	ユニファイド CM 12.5
Linux	AS 3.0	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外
Linux	RHEL 7 (64 ビット)	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポートあり
Linux	RHEL 3.7	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外
Linux	RHEL (32 ビット)	RH 5.5 Sun JVM 1.6.0.29	RH 5.5 Oracle JVM 1.7.0.40	RH 5.5 Oracle JVM 1.7.0.76	RH 5.5 Oracle JVM 1.7.0.79	RH 5.5 Oracle JVM 1.7.0.79	RH 5.5 Oracle JVM 1.7.0.79
Linux	RHEL 5.5 (64 ビット)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Linux	RHEL 6 (64 ビット)	Sun JVM 1.7.0.40	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Solaris	6.2 (Sparc および x86)	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外
Windows	Windows XP 2003、2008 サーバ (32 ビット)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	サポート対象外	サポート対象外
Windows	Vista（32 ビット）	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	サポート対象外	サポート対象外
Windows	Windows 7(32 and 64 bit) 2008 Server R2(64 ビット)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows 8(32 and 64 ビット)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79

オペレーティングシステム	バージョン	ユニファイド CM 10.0	ユニファイド CM 10.5	ユニファイド CM 11.0	ユニファイド CM 11.5	ユニファイド CM 12.0	ユニファイド CM 12.5
Windows	Windows サーバ 2012 R1 (32 ビット)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows 8.1(32 および 64 ビット)	サポート対象外	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows サーバ 2012 R2 (64 ビット)	Sun JVM 1.7.40	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows 10(32 および 64 ビット)	サポート対象外	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows サーバ 2016(64 ビット)	サポート対象外	サポート対象外	サポート対象外	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79

Cisco Unified JTAPI の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.htmlの『*Cisco Unified Communications Manager* 向け *Cisco Unified JTAPI* 開発者ガイド』の「「Cisco Unified JTAPI でサポートされている機能」」の章を参照してください。

FIPS モードでの CiscoSSH サポート

Ciscoユニファイド コミュニケーション マネージャ は、OpenSSH の代わりに、CiscoSSH を使用するようになりました。システムで FIPS モードを有効にすると、CiscoSSH も FIPS モードに自動的に切り替わります。

FIPS モードを有効にする方法の詳細については、『*Security Guide for Cisco Unified Communications Manager* 』の「FIPS 140-2 Mode Setup」の章を参照してください。

CiscoSSH サポート

CiscoSSH は、次のキー交換アルゴリズムをサポートします。

- Diffie-Hellman-Group14-SHA1
- Diffie-Hellman-Group-Exchange-SHA256
- Diffie-Hellman-Group-Exchange-SHA1

CiscoSSH は、ユニファイド コミュニケーション マネージャで次の暗号方式をサポートします。

- AES-128-CTR
- AES-192-CTR
- AES-256-CTR
- AES-128-GCM@openssh.com
- AES-256-GCM@openssh.com
- AES-128-CBC（リリース 12.0(1) 以降をサポート）
- AES-192-CBC（リリース 12.0(1) 以降をサポート）
- AES-256-CBC（リリース 12.0(1) 以降をサポート）

CiscoSSH は、クライアントの次の暗号方式をサポートします。

- AES-128-CTR
- AES-192-CTR
- AES-256-CTR
- AES-128-GCM@openssh.com
- AES-256-GCM@openssh.com
- AES-128-CBC
- AES-192-CBC
- AES-256-CBC

暗号管理

暗号管理機能は、Cisco ユニファイド コミュニケーション マネージャIM およびプレゼンス 上のさまざまなセキュアインターフェイスで弱い暗号を無効にすることによって、システムのセキュリティを強化します。Cipher management を使用すると、各 TLS および SSH 接続で許可される一連のセキュリティ暗号を制御することができます。

この機能を使用すると、古いモデルの電話機などの他のコンポーネントとの互換性を損なうことなく、推奨される暗号方式を設定したり、Ciscoユニファイド コミュニケーション マネージャ および IM and Presence に安全に接続されたエンティティを設定したりすることができます。

詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager* セキュリティ ガイド』の「暗号管理」セクションを参照してください。

ユーザ インターフェイスの更新

[**暗号管理 (Cipher Management**)] ウィンドウが、Cisco ユニファイド os 管理、Cisco Unified IM and Presnece OS 管理インターフェイスの [**セキュリティ (Security**)] メニューに追加されます。

詳細については、「 *Cisco* ユニファイドオペレーティングシステムの管理」オンラインヘルプの「暗号管理について」の項を参照してください。

使用している EC 曲線の曲線ネゴシエーションおよびサポートされている暗号方式の詳細については、『 *Security Guide For Cisco Unified Communications Manager, Release 12.5 (1)* 』の「Curve のネゴシエーション」の項を参照してください。

エクステンションモビリティとエクステンションモビリティクロスクラスタの最大ログイン時間を設定します。

このリリースでは、エクステンション モビリティとエクステンション モビリティ クロス クラスタの最大ログイン時間をユーザ レベルで設定できます。ユーザプロファイル設定ページを許可するように設定している場合、ユーザは Cisco Unified Communications セルフケアポータルを使用して最大ログイン時間を設定することもできます。

一括管理を使用して、ユーザのグループの最大ログイン時間を追加または更新することもできます。

エクステンション モビリティ サービス パラメータでは、クラスタ**内最大ログイン時間**の値をゼロに設定できるようになりました。これにより、**クラスタ内**最大ログイン時間の値を False に変更する必要がなくなります。

ユーザ インターフェイスの更新

- Cisco Unified CM の管理では、**ユーザ管理** > **エンドユーザ**の下にある [**エンドユーザの設定 (End User Configuration**)] ページに、**最大ログイン時間 (HHH: MM)**パラメータが追加されます。
- Cisco Unified CM の管理では、[**Allow End User to set The Extension Mobility maximum login time**] チェックボックスが **[ユーザ管理(User Management)]** > **[ユーザー設定(User Settings)]** > **[ユーザプロファイル(User Profiles)**の下の [**User Profile Configuration**] ページに追加されます。
- Cisco Unified Communications セルフケアポータルでは、 **[一般設定 (General Settings)]** > **Extension mobility** の下に次のオプションボタンが追加されます。
  - システムのデフォルトの最大ログイン時間を使用する
  - 最大ログイン時間なし
  - Hours___minutes___ 後に自動的にログアウトする

- Cisco ユニファイド CM の管理では、**[一括管理 (Bulk Administration)]** > **[ユーザ (Users)]** > **[ユーザのテンプレート (User Template)]**の **[ユーザのテンプレート設定 (User Template Configuration)]** ページに**最大ログイン時間 (HHH: MM)**パラメータが追加されます。
- Cisco ユニファイド CM の管理では、**[一括管理 (Bulk Administration)]** > **[ユーザ (Users)]** > **[ユーザの更新 (Update Users)]** > **[クエリ (Query)]**の **[ユーザの更新設定 (Update User Configuration)]** ページに**最大ログイン時間 (HHH: MM)**パラメータが追加されます。
- Cisco ユニファイド CM の管理では、**[一括管理 (Bulk Administration)]** > **[ファイルのアップロード/ダウンロード (Upload/Download Files)]**の BAT スプレッドシートに **EM MAX LOGIN TIME** フィールドが追加されます。
- Cisco ユニファイド CM の管理では、**[一括管理 (Bulk Administration)]** > **[ユーザ (Users)]** > **[ユーザを挿入 (Insert Users)**および**[一括管理 (Bulk Administration)]** > **[ユーザ (Users)]** > **[ユーザの更新 (Update Users)** > **[カスタムファイル (Custom Files)]**ならびに**[一括管理 (Bulk Administration)]** > **[電話とユーザ (Phones & Users)]** > **[電話とユーザを挿入 (Insert Phones with Users)]**の [サンプルファイルを見る (View Sample File)]に **EM MAX LOGIN TIME** フィールドが追加されます。

エクステンションモビリティの最大ログイン時間の設定の詳細については、次を参照してください。

- 詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の「ユーザ プロファイルの設定」を参照してください。
- 『*Cisco Unified Communications* セルフケア ポータル ユーザガイド』の「エクステンション モビリティの最大ログイン時間の設定」セクションhttps://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html を参照してください。

一括ユーザのエクステンション モビリティの最大ログイン時間の設定の詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager* 』を参照してください https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

エクステンション モビリティ サービス パラメータの詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager* 』の「Extension Mobility service parameters」の https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html 項を参照してください。

暗号化された IM コンプライアンスデータベース

IM and Presence Service のこのリリースでは、メッセージ アーカイバ機能の暗号化されたコンプライアンスデータベースをサポートしています。この機能を導入すると、すべてのインスタントメッセージが暗号化されてからコンプライアンスデータベースに送信されます。コンプラ

イアンスデータベース内のデータを調べるユーザは、暗号化キーを使用せずにアーカイブされたメッセージを読み取ることができません。

この機能により、お客様のシステムがコンプライアンス規制に準拠しながら、機密性の高い IM 交換の許可された担当者への読み取りアクセスを制限することで、IM and Presence の導入に対するセキュリティが強化されます。たとえば、会社がインスタントメッセージを使用して顧客と通信し、会社がメッセージアーカイブを必要とする規制された業界でビジネスを行っているとします。暗号化キーへのアクセスを制限することにより、すべてのインスタント メッセージをアーカイブし、データベース管理者などの従業員に、システムの実行を維持するために必要なデータベース アクセスを提供できます。ただし、アーカイブされた IM 交換への読み取りアクセスを本物のビジネスニーズがある従業員にのみ制限することができます。

この機能は、Microsoft SQL サーバが外部コンプライアンス データベースとして展開されている場合にのみサポートされます。

クラスタ間ネットワーク

クラスタ間ネットワークでは、クラスタ間ネットワークの暗号化を1つのクラスタから有効にすることができます。これにより、ネットワークのマスタークラスタになります。マスタークラスタは、クラスタ間ネットワーク内のスレーブ クラスタになるリモートクラスタに暗号キーと暗号化の設定を同期します。リモート クラスタでメッセージ アーカイバ機能が設定されていて、Microsoft SQL サーバ コンプライアンス データベースを使用している場合、暗号化はリモートクラスタに対して自動的に設定されます。

暗号化標準規格

アーカイブされたデータが確実に侵害されないようにするために、この機能では3つのキー(対称暗号化キーと assymetric 公開秘密キーペア) を使用します。

- 暗号化キー: この256ビットの対称キーは、IM and Presence Serviceによって内部的に生成され、保存されます。このキーは、コンプライアンスデータベースにデータをアーカイブする前に、このキーを使用して IM コンプライアンス データを暗号化します。クラスタ間ネットワークの場合、マスター クラスタはその暗号キーをリモート スレーブ クラスタと同期して、クラスタ間ネットワーク全体がマスタークラスタから制御される同じ暗号キーを使用するようにします。

  このキーを IM and Presence Serviceからダウンロードし、データ ビューアとともに使用して、アーカイブされたIMを復号できるようにする必要があります。このキーをダウンロードすると、公開キーと秘密キーのペアから公開キーを使用してキーが暗号化されます。後で秘密キーを使用して暗号キーを復号化できます。

- 公開秘密キーペア: 承認済みのキー生成ツール (OpenSSL など) でこの assymetric キーペアを生成し、それを使用して IM and Presence Service のキーを暗号化してから、データ表示ツールを使用してキーを復号化する必要があります。公開秘密キーのペアは、IM and Presence Serviceからデータ表示ツール (たとえば、分裂) への転送中に暗号化キーを保護します。

暗号化パスワードは、SHA2 でハッシュされ、AES 256 で暗号化されます。インスタント メッセージは、AES 256 アルゴリズムで暗号化されます。

暗号化のプロセス フロー

次の表に、暗号化を有効にし、暗号化されたデータをデータベースから表示するプロセス フローを示します。このフローでは、各ステップと各ステップが完了したインターフェイスが強調表示されます。

表 *2*:暗号化プロセス フロー

	IM and Presence Service マスター クラスタ	**キー生成ツール(OpenSSLなど)**	**データ表示ツール**
ステップ 1	管理者は、クラスタ間ネットワークの暗号化を設定します。マスター クラスタは、クラスタ間ネットワーク全体で暗号化設定を同期します。アーカイブされたデータが暗号化されるようになりました。	—	—
ステップ 2	—	管理者は、暗号キーを保護するための公開キーと秘密キーのペアを生成します。	—
ステップ 3	管理者は、IM and Presence Serviceから暗号キーをダウンロードします。ダウンロード中に、公開キーによって暗号キーが暗号化されます。	—	—
ステップ 4：	—	—	管理者は秘密キーを使用して暗号キーを復号化します。
ステップ 5	—	—	暗号キーは、コンプライアンス データを復号化します。承認された担当者は、アーカイブされたコンプライアンスデータを表示できます。

最小要件

この機能には、次の要件が適用されます。

表 *3:* 暗号化された *IM* コンプライアンス データベースの最小要件

システム	この機能の要件
IM and Presence Service	• 11.x リリースでは、この機能の最小リリースは 11.5 (1) SU5 です。 • 12.x リリースの場合、最小リリースは 12.5 (1) になります。 • この機能は、12.0 (1) または 12.0 (1) SU1 においてもサポートされていません。この機能を 11.5 (1) SU5 に導入し、12.0 (1) または 12.0 (1) SU1 にアップグレードすると、この機能は失われます。
外部データベース	• この機能をサポートするには、すべてのクラスタ ノードでコンプライアンス データベースとして導入された Microsoft SQL サーバが必要です。

コンフィギュレーション

メッセージアーカイバの暗号化データベースを設定する方法の詳細については、*IM and Presence Service* のインスタント メッセージング準拠ガイドの「Message Archiver Configuration」の章を参照してください。

ユーザ インターフェイスの更新

この機能をサポートするために、[**Encryption settings for external database**] セクションが **[コンプライアンス設定の設定]** ウィンドウに追加されました。このフィールドのセットは、**メッセージアーカイバ**を設定し、Microsoft SQL サーバコンプライアンス データベースを選択した場合にのみ表示されます。ここでは、次のフィールドについて説明します。このリリースでは、すべてが追加されています。

- **[Enable encryption on this cluster]**: ローカル クラスタで暗号化を有効にするには、このチェックボックスをオンにします。
- **[Enable Encryption On Remote**cluster]: クラスタ間ネットワーク内のクラスタ間ピアで暗号化を有効にするには、このチェックボックスをオンにします。ローカル クラスタはマスター クラスタになります。これにより、その暗号キーがスレーブ クラスタであるリモート クラスタに同期されます。
- **パスワード/パスワードの確認**—暗号化 パスワードを入力します。暗号キーをダウンロードする場合、暗号化を無効にする場合、または暗号化パスワードを変更する場合は、このパスワードを再入力する必要があります。
- **このクラスタのステータス テーブル**: この読み取り専用ステータス テーブルには、クラスタ間同期のステータスが表示されます。また、どのクラスタがマスタークラスタであるかも表示されます。テーブルには、次のステータス列が表示されます。

- [変更に成功した日]:暗号化パスワードと暗号化ステータスの両方で最後に成功した設定変更の結果。
- [変更に失敗した日]:暗号化パスワードまたは暗号化ステータスを変更しようとしたときに失敗した場合、結果はここに表示されます。
- マスタークラスタ ID: このフィールドは、クラスタ間ピアの設定でマスター クラスタであるクラスタを識別します。

- **パスワードの変更**: 暗号化が設定されている場合は、このボタンをクリックしてパスワードを変更します。マスター クラスタ上のパスワードのみを変更できます。
- [**暗号キーのダウンロード**]: 暗号キーをダウンロードするには、このボタンをクリックします。キーをダウンロードするには、外部 Windows ツールで生成した公開キーと同様に、暗号化パスワードを入力する必要があります。
- **暗号化の無効化**—このチェック ボックスにチェックを入れて暗号化を無効化します。

アラームの更新

Cisco XCP Message Archiver サービスに、メッセージ アーカイバの暗号化に関する問題を示すために、**MAencryptionMultiMaster**アラームが追加されました。このアラームは、複数のクラスタがメッセージ アーカイバ暗号化のマスター クラスタとして設定されているクラスタ間ピア ネットワークがある場合に発生します。

オンプレミス コールの楕円曲線暗号化

サポートされている Cisco IP 電話 間のポイントツーポイントコールの楕円曲線暗号化をサポート Ciscoユニファイド コミュニケーション マネージャ。

楕円曲線暗号化は、より小さいキーを使用しながら、3072ビット RSA 公開キーに対して同等のセキュリティを提供します。これにより、高レベルのシステムセキュリティを維持しながら、データストレージとデータ転送の要件が容易になります。

この機能はオンプレミス コールだけでサポートされていて、Mobile & Remote Access の展開ではサポートされていません。楕円曲線暗号化を使用するには、システムとデバイスが楕円曲線をサポートしている必要があります。

コンフィギュレーション

楕円曲線を使用するようにシステムを設定するには、暗号管理インターフェイスで楕円曲線を使用する暗号が許可されていることを確認する必要があります。暗号管理ウィンドウを使用してシステム暗号方式を設定する方法の詳細については、『 *Security Guide for Cisco Unified Communications Manager, Release 12.5 (1)* 』を参照してください。

汎用デバイスまたは回線テンプレートの強化

このリリースでは、デバイスのプロビジョニングを容易にするために、ユニバーサルデバイステンプレートとユニバーサル回線テンプレート機能が強化されています。

この機能は次の点で強化されています。

- ユーザの有無にかかわらず新しい電話機を追加します。ユーザに関連付けられていない、または使用せずに、ユニバーサルデバイステンプレートを使用して新しい電話機を追加できます。たとえば、会議室の電話やロビーの電話などです。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Administration Guide FOR Cisco Unified Communications Manager and IM and Presence Service*』の「Add New Phone from Template With or no End User」の項を参照してください。
- ユニバーサルデバイステンプレートまたはユニバーサル回線テンプレートのコピー: 既存のテンプレートをコピーし、必要なマイナー変更を行うことによって、新しいユニバーサルデバイステンプレートまたはユニバーサル回線テンプレートを作成できます。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の「Configure Universal Line template」および「Configure Universal Device template」の項を参照してください。
- ユニバーサルデバイステンプレートとユニバーサル回線テンプレートのインポートまたはエクスポート: 一括管理ツール (BAT) は、ユニバーサルデバイステンプレートとユニバーサル回線テンプレートのインポートまたはエクスポートをサポートします。既存のユニバーサルデバイステンプレートまたはユニバーサル回線テンプレートをエクスポートし、小規模なサイト固有の変更とインポートを行うことができます。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『*Bulk Administration Guide for Cisco Unified Communications Manager*』の「設定データのエクスポート オプション」を参照してください。
- 非サイズセーフ電話ボタンレイアウト:個々の電話ボタンテンプレートを作成することも、デバイスのデフォルトの電話ボタンテンプレートを使用することもできます。これには、[**エンタープライズパラメータの設定 (Enterprise Parameters Configuration)**] ページの [非サイズセーフ電話および自動登録レガシーモードエンタープライズパラメータの電話テンプレートの選択] を設定します。この機能により、不要な電話ボタンテンプレートの作成が削減されます。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Administration Guide FOR Cisco Unified Communications Manager and IM and Presence Service*』の「電話のボタンのテンプレート」の項を参照してください。
- [タグ (TAG)] または [トークン (Token)]: ユニバーサルデバイステンプレートのタグまたはトークンとしてより多くのパラメータを設定できます。

ユーザ インターフェイス

- ユーザの有無にかかわらず新しい電話機を追加するには、[**テンプレートから新規追加(Add New From Template)**] ボタンが Cisco ユニファイド CM 管理インターフェイスの [**端末(Device) > 電話 (Phone) > 電話の検索と一覧表示 (Find and List Phones)**] メニューに追加されます。
- ユニバーサルデバイステンプレートとユニバーサル回線テンプレートをインポートまたはエクスポートするために、ユニバーサルデバイステンプレートとユニバーサル回線テンプレートパラメータが**一括管理 > インポート/エクスポート > エクスポート > ユーザデータ**の下に追加されます。
- 非サイズの安全な電話ボタンレイアウトでは、[**エンタープライズパラメータ設定(Enterprise Parameters Configuration)**] ページに、**非サイズセーフ電話の電話テンプレート選択**が追加されます。
- ユニバーサルデバイステンプレートとユニバーサル回線テンプレートをコピーするには、[ユニバーサルデバイステンプレートの**検索と一覧表示**]ページ、[**ユニバーサルデバイステンプレートの設定**] ページ、[**ユニバーサル回線テンプレートの検索と一覧表示**] ページおよび [**ユニバーサル回線テンプレートの設定**] ページの下に [**コピー**] ボタンが追加されています。
- デバイス名 #DEV #、Product Type #PDT #、Protocol Type #PROTO # および Extension #EXT # タグは、[**ユニバーサルデバイステンプレートの設定 (Universal Device Template Configuration)**] ページの [**デバイスの説明の作成 (Build Input For Device Description)**] ポップアップに追加されます。
- 拡張 # EXT # および Line Index #LI # タグは、[**ユニバーサルデバイステンプレートの設定 (Universal Device Template Configuration)**] ページの [**回線ラベルの作成 (Build Input For line label)**] ポップアップに追加されます。

スマート ライセンシングの CLI 更新の強化

次の CLI コマンドを使用して、スマートソフトウェアライセンシングサービスに接続するユニファイドコミュニケーションマネージャを選択できるようになりました。製品を Cisco ライセンシング サーバに直接接続させる場合は、直接 オプションがデフォルトで選択されます。

- smart transport direct のライセンス
- license smart transport gateway < URL >
- license smart transport proxy < プロキシサーバ > < プロキシポート >

CLI コマンドの詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『Command Line Interface Reference Guide for Cisco Unified Communications Solutions』のライセンス コマンドを参照してください。

FIPS モードでは SHA256 ハッシュ アルゴリズムが必須です

このリリースでは、システムが FIPS モードで実行されている場合、SHA256 ハッシュ アルゴリズムを使用して証明書を暗号化する必要があります。FIPSモードを有効にした後に、自己署名証明書または証明書署名要求（CSR）を生成すると、システムは、ハッシュアルゴリズムとしてSHA256を使用するオプションのみを提供します。[SHA1]を選択することはできません。この機能強化により、Ciscoユニファイド コミュニケーション マネージャ は FIPS に準拠しています。

FIPSモードが有効になっている以前のリリースからアップグレードすると、既存のSHA1またはSHA256 ハッシュ アルゴリズムで暗号化された証明書は保持されます。

FIPSモードを有効にする方法の詳細については、『*Security Guide for Cisco Unified Communications Manager*』の「「FIPS Mode Setup」」の章を参照してください。

ユーザ インターフェイスの更新

FIPS モードが有効になっている場合、[**Generate New Self Signed certificate** And **Generate Certificate signed Request**] ダイアログボックスに表示される [**Hash Algorithm**] ドロップダウンでは、**SHA256**のみを選択できます。ただし、FIPS モードが無効になっている場合でも、**SHA1**または**SHA256**を選択できます。

オンライン ヘルプの更新

「自己署名証明書フィールド」と「証明書署名要求フィールド」の表に、SHA256 が自己署名証明書および証明書署名要求のハッシュアルゴリズムとしてデフォルトで表示されるようになりました。

フィールドの詳細なヘルプコンテンツについては、『 *Cisco* ユニファイドアドミニストレーション *CM Administration Online help*』を参照してください。

きめ細かいアクセス制御

[きめ細かいアクセス制御]は、システムへのアクセスを許可する際に、以下に示すようなタスクへのアクセスを制限できます。

- ユーザの追加
- パスワードの編集
- ユーザ ランクの編集
- アクセス コントロール グループの編集

詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/admin/cucm_b_administration-guide-1251/cucm_b_administration-guide-1251_chapter_010.htmlを参照してください。

Intercluster Peer Sync Enhancements

IM and プレゼンスサービスのこのリリースには、クラスタ間ピアが同期できない場合の同期の問題を容易に解決できるようにするための Cisco クラスタ間 Sync Agent の機能拡張が含まれています。デフォルトでは、システムはクラスタ間ピア同期ステータスをモニタするようになりました。問題を同期しているピアクラスタが見つかった場合、Cisco Intercluster SyncAgent は自動的に再起動して問題を解決します。これにより、クラスタ間ネットワーク接続が稼働し続けるようになります。

この機能拡張の一部として、次の更新が導入されました。

- インターフェイスには、最後に成功した同期の時刻を示す新しいフィールドが追加されました。
- 同期障害が発生するたびに、新しいアラームが生成されます。システムは自動的に再同期を試行します。
- 新しいサービスパラメータにより、Cisco Intercluster Sync Agent の自動再起動が有効になり、以前のリリースとの下位互換性も可能になります。

ユーザ インターフェイスの更新

[**クラスタ間ピアの設定 (クラスタ間 peer Configuration**)] ウィンドウに、最後に成功したクラスタ間ピア同期を表示する新しい**最後の同期時刻**ステータスが表示されるようになりました。

アラームの更新

新しいアラームが導入されました。**Interclustersyncagentpeerperiodicsyncfailure**。このアラームは、Cisco クラスタ間 sync Agent サービスがクラスタ間ピアとの定期的な同期障害を検出するたびに生成されます。Cisco Intercluster Sync Agent サービスは障害発生時にただちに再同期を試行するため、処置は必要ありません。

サービス パラメータの更新

Cisco Intercluster Sync Agent の新しいサービス パラメータが導入されました。**クラスタ間ピア間の定期的な同期の失敗に対して自動リカバリを有効に**します。このサービスパラメータが有効になっている場合、クラスタ間ピア同期の問題が検出されると、Cisco クラスタ間 Sync Agent サービスが自動的に再起動します。サービス パラメータはデフォルトで有効になっていますが、この機能が含まれていない以前のリリースとの下位互換性を維持するために無効にすることができます。

Jabber 設定ファイルの管理

リリース 12.5 (1) 以降では、Cisco ユニファイド CM Administration インターフェイスを使用して、Jabber クライアント設定パラメータを一元的に管理できます。この機能を使用すると、導入環境内のサイトごと、またはユーザグループごとなど、さまざまな導入シナリオに対して複数の Jabber クライアント設定テンプレートを作成することができます。この機能により、次のものを排除することで Jabber の導入が簡素化されます。

- Jabber-config.xml ファイルを手動で設定する必要があります。
- TFTP サーバにコンフィギュレーションファイルをアップロードする必要があります。
- Cisco TFTP サービスの再起動

（注） この機能には、Cisco Jabber 12.5 リリースバージョン以降が必要です。

ユーザ インターフェイスの更新

この機能をサポートするには、UC サービスの設定 [**ユーザ管理（User Management）** > **ユーザ設定（User Settings）** > **UCサービス（UC Service）**] ウィンドウを使用して、次の新しいサービスを含むように更新されました。

- Jabberクライアント設定(jabber-config.xml)

新しいサービスを使用して、導入のニーズに応じて複数の Jabber クライアント設定テンプレートを作成できます。各テンプレートでは、シングル、マルチパートおよびカスタムパラメータを設定できます。テンプレートが作成されたら、[**User Settings] [> Service Profiles**] に移動して、それらを共通、デスクトップ およびモバイル Jabber のクライアントタイプに関連付けます。

パラメータの詳細については、*Cisco Jabber* のパラメータ リファレンス ガイドを参照してください。

認証局プロキシ機能（CAPF）のオンライン CA

このリリースでは、Certificate Authority Proxy Function (CAPF) サービスにはオンライン CA オプションが含まれています。Online CA オプションを使用すると、CSR プロセスはユニファイドコミュニケーションマネージャに組み込まれます。そのため、CA 署名付き LSC 証明書は、サードパーティの CA から自動的に要求および受信できます (秒単位)。

以前のリリースでは、オフライン CA オプションでは、CA 署名付き LSC 証明書の発行を要求することができましたが、これは時間がかかり、手動プロセスでした。この機能により、サードパーティの CA によって署名された電話機の LSC 証明書を簡単に管理できるようになりま

す。オンライン CA 機能は、CA 署名付き LSC 証明書の取得に必要な作業の量を大幅に削減します。

リリース 12.5 (1) では Microsoft CA のみが CAPF を使用したオンライン CA としてサポートされています。

コンフィギュレーション

オンライン CA を使用するように認証局プロキシ機能を設定する方法の詳細については、*Cisco Unified Communications Manager* のセキュリティガイドの「Certificate Authority proxy function」の章を参照してください。

ユーザ インターフェイスの更新

次の Cisco Certificate Authority Proxy Function サービスパラメータが更新されます。

- エンドポイントへの証明書発行元: オンライン CA 機能をサポートするために、このサービスパラメータには**オンライン ca**オプションが含まれるようになりました。このオプションは、オンライン CA を使用する場合に選択する必要があります。

さらに、次の新しいサービスパラメータを使用して、CA への接続を設定することができます。

- オンライン CA ホスト名
- オンライン CA ポート
- オンライン CA テンプレート
- オンライン CA タイプ: 現在**MICROSOFT ca**のみが使用可能なサードパーティ ca です。
- オンライン CA ユーザ名
- オンライン CA パスワード

有用性の更新

Cisco 証明書登録サービスは、[**セキュリティ設定 (Security Settings)**] 見出しの下に機能サービスとして追加されます。オンライン CA を使用するには、このサービスが動作している必要があります。

Cisco Unified レポートの更新

新しいレポート、**古い lscs**がシスコのユニファイドレポーティングユーザインターフェイスに追加されました。このレポートには、電話機によって拒否されたローカルで有効な証明書(LSCs)が一覧表示されます。

コマンドライン インターフェイスの更新

次の CLI コマンドがシステムに追加されました。これらのコマンドは、3つの CAPF モードすべてに対して機能します。

- **ユーティリティ capf stale-lsc delete all**: すべての古い lsc 証明書をシステムから削除します。
- **ユーティリティ capf stale-lsc ビュー**: すべての古い lsc 証明書のリストを提供します。
- [**ユーティリティ (capf csr)] リスト**: 保留中の csr ファイルのタイムスタンプリストをシステムから取得します。**List**パラメータは、既存のユーティリティ capf csr コマンドに追加されます。
- [**monitorcapf set keep_alive**]: キープアライブタイマーを設定して、電話機から capf への接続 (デフォルトではポート 3804) がファイアウォールによってタイムアウトにならないようにすることができます。デフォルト値は、15 分です。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*、リリース *12.5(1)*』の 「Utils コマンド」の章を参照してください。

更新のトラブルシューティング

利用できるログは次のとおりです。

- CAPF ログファイルは、「`/var/log/active/cm/trace/capf/sdi`」にあります。これらのログを取得するには、CAPF サービスのトレースを有効にする必要があります。
- Cisco RA ログファイルは、「`/var/log/active/cm/trace/capf/sdi/nginx < number >`」にあります。これらのログを取得するためにトレースを有効にする必要はありません。
- CLI ログは次の場所にあります: `"/var/log/active/platform/log/cli * .log"`

デフォルト CA 証明書の管理

このリリースでは、CLI を使用して、ユニファイドコミュニケーションマネージャと IM and プレゼンスサービスにバンドルされているデフォルトの CA 証明書を簡単に管理できます。デフォルトの CA 証明書を個別に、または同時に有効または無効にするオプションがあります。さらに、これらの各証明書の目的を表示することもできます。

12.5 (1) リリース以降では、Cisco ユニファイド OS Administration を使用して1つのノードから CAPF 信頼証明書を削除すると、その証明書はクラスタ内のすべてのサーバから削除されます。

CLI 更新

この機能をサポートするために、このリリースでは次の CLI コマンドが新しく追加されました。

show cert default-ca list
このコマンドは、すべてのデフォルト CA 証明書を表示します。これは、Cisco Unified Communications Manager IM and Presence Service にバンドルされています。

set cert default-ca list enable {all | common-name}
このコマンドは、クラスタ内のすべてのサーバで、すべてまたは特定のデフォルト CA 証明書を有効にします。
set cert default-ca list enable {all | common-name}
このコマンドは、クラスタ内のすべてのサーバで、すべてまたは特定のデフォルト CA 証明書を無効にします。

CLI コマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*（Cisco Unified Communications ソリューションのコマンド ライン インターフェイス ガイド）』を参照してください。

信頼証明書の削除の詳細については、*Cisco Unified Communications Manager* のセキュリティガイドの「証明書の概要」の章を参照してください。

CUBE メディア プロキシ サーバを使用するマルチフォーク記録

Ciscoユニファイド コミュニケーション マネージャ リリース 12.5 (1) 以前では、ユニファイドコミュニケーションマネージャは1つのコールに対して1つのレコーダーのみをサポートしていました。Ciscoユニファイド コミュニケーション マネージャ リリース 12.5 (1) では、ユニファイドコミュニケーションマネージャはコール録音機能のマルチ分岐をサポートしています。

ユニファイドコミュニケーションマネージャは、複数のレコーダーに接続されている CUBE メディアプロキシサーバに接続されています。JTAPI インターフェイスは、CUBE メディアプロキシサーバを介したマルチ分岐録音の場合、複数のレコーダーの詳細を取得するように拡張されています。

下位互換性

この機能は下位互換性があります。JTAPI は現在の API をサポートしています。

エクステンションモビリティとクラスタ間のエクステンション モビリティの複数ログイン動作

このリリースでは、クラスタ間のエクステンション モビリティ機能が更新されました。これで、クラスタ間のエクステンション モビリティの複数ログイン動作は、エクステンション モビリティの複数ログイン動作と一貫するようになりました。[**サービスパラメータ設定 (Service Parameter Configuration)**] ページでは、次のいずれかとして**複数のログイン動作**を設定できます。

- 複数のログインは許可されます
- 複数のログインは許可されません
- Auto Logout

ユーザ インターフェイスの更新

[**サービスパラメータの設定 (Service Parameter Configuration)**] ウィンドウで、**クラスタ内マルチログイン動作**サービスパラメータの名前が**複数のログイン動作**に変更されます。このパラメータは、クラスタ間ログインのエクステンションモビリティとエクステンションモビリティの両方に適用されます。

詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある *Cisco Unified Communications Manager* の機能設定ガイドの「エクステンション モビリティ」章、または「エクステンション モビリティ クロス クラスタ」章をご覧ください。

複数のセキュア SIP トランクを同じ宛先に接続する

このリリースは、同じ**宛先 IP アドレス**と**宛先ポート番号**に対する複数のセキュア SIP トランクの設定をサポートします。

機能には次の利点があります。

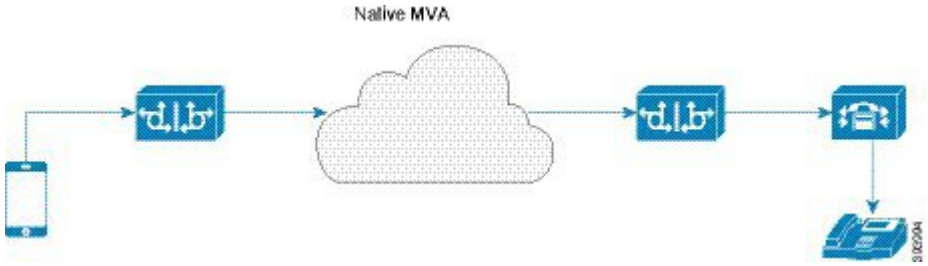
- 帯域幅の最適化: 緊急コール用のルートを提供し、帯域幅に制限がありません。
- 特定の地域または CCS 設定に基づいたルーティングの選択。

ネイティブ モバイル音声アクセス

このリリースでは、モバイルボイスアクセスのネイティブサポートが導入されています。この更新により、モバイルボイスアクセス IVR をホストする ISR G2 ルータを展開して設定する必要がなくなったため、モビリティの導入が簡素化されます。Ciscoユニファイド コミュニケーション マネージャ は、IVR サービスをネイティブにホストできます。

モバイルボイスアクセスが設定されている場合、エンドユーザは、任意の電話機 (携帯電話やリモート PSTN 電話など) からシステム IVR にコールし、認証後に、そのユーザの会社の番号からルーティングされるコールを発信できます。着信側には、発信者が自分のデスクフォンからダイヤルしていたかのようにコールが表示されます。さらに、モバイルボイスアクセスコールは企業に固定されており、集中型課金、CDR レコード および携帯電話ネットワークではなく企業ネットワークを介したコールのルーティングからの潜在的なコスト削減などの追加の利点を提供します。

次の図は、携帯電話を使用したネイティブモバイルボイスアクセスのセットアップを強調表示しています。この設定には、2つのセッション境界コントローラ、Ciscoユニファイドコミュニケーション マネージャ およびエンタープライズデスクフォンが含まれます。携帯電話のユーザが IVR 番号にダイヤルインすると、Ciscoユニファイド コミュニケーション マネージャ はユーザを認証し、企業の電話機とユーザを関連付けます。これにより、発信コールは企業のデスクフォンからダイヤルされたかのように配置できます。



コンフィギュレーション

従来のモバイルボイスアクセスと比較した場合のネイティブモバイルボイスアクセスのサポートの設定の主な違いは次のとおりです。

- 音声プロンプトを処理するためにISR G2ゲートウェイを導入する必要がなくなりました。
- Mobile Voice Access Number サービスパラメータは、モバイルボイスアクセスプロンプトにアクセスするためにお客様がダイヤルする必要がある電話番号を表します。この番号は、モバイルボイスアクセスのみを対象としており、ユーザの電話回線に電話番号として割り当てることはできません。
- システムでモバイル音声アクセス機能を設定した後は、**Cisco CallManager** サービスを再起動します。

モバイルボイスアクセスの設定方法の詳細については、『 Feature Configuration Guide for Cisco ユニファイド コミュニケーション マネージャ 』の「Configure Cisco Unified Mobility」の章の「Mobile Voice Access configuration」のトピックを参照してください。

ネイティブおよびレガシーモバイルボイスアクセスの統合オプション

ISR G2 ルータを導入している場合でも、IVR への要求が VXML サポートを使用して ISR G2 ルータに送信される従来のモバイルボイスアクセスを展開するオプションがあります。単一システム内でモバイルボイスアクセスの両方の方法を統合できます。これは、Ciscoユニファイド コミュニケーション マネージャ で設定されている Mobile Voice Access Number サービスパラメータが、ルータのダイヤルピアで定義されている外線番号の値と一致する必要がないためです。

クラスタ内のネイティブとレガシーの両方の MVA を統合するためのオプションがいくつかあります。次に例を示します。

- ネイティブおよびレガシーサポートのために、さまざまなモバイルボイスアクセス(MVA)番号を設定します。ユーザは、ダイヤルする番号に対応する MVA サービスを使用します。ルータで設定されている従来の MVA 番号をダイヤルすると、ISR G2 ルータからレガシー MVA サービスが使用されます。[Mobile Voice Access Number] サービスパラメータで設定されている番号をダイヤルすると、Ciscoユニファイドコミュニケーションマネージャのネイティブ MVA サポートによってルーティングされます。
- 同じ番号の複数のセッションボーダーコントローラを展開します。ユーザは、システムがどのようにルートをルーティングするかに応じて、いずれかの MVA 方式を使用できます。

Jabber モバイルでの永続的なチャットのサポート

このリリースでは、iPhone、iPad および Android の Cisco Jabber の永続的なチャットルームがサポートされています。この更新により、Cisco Jabber モバイル クライアントは、Windows または Mac 上の Cisco Jabber などのデスクトップク ライアントとまったく同じ永続的なチャット機能を利用できます。

この機能には、IM and Presence Serviceで永続的なチャットルームを設定する方法の変更は含まれていません。ただし、この機能には、iPhone、iPad および Android での Cisco Jabber の次の更新が含まれています。

- Cisco Jabber モバイルクライアントは、永続的なチャットルームに入ることができるようになりました。
- Jabberがサイレントモードのときに永続的なチャット通知を無効にするために使用できるミュート機能。ミュート機能は、Cisco Jabber クライアント内の Cisco Jabber ユーザが有効にする必要があります。
- この機能は、ミュート設定を上書きします。Jabberユーザが記載されている場合、ミュート機能がアクティブになっているかどうかに関係なく、通知が送信されます。
- 他の Jabber アプリケーションへのシーン通知の背後では、1つのデバイスでチャット メッセージを読むと、すべてのJabberアプリケーションでの読み取りメッセージとして表示されます。

サポートされている最小リリース

この機能には、次の最小リリースサポート情報が適用されます。

製品	サポート情報
IM and Presence Service	• 一連の 11. x リリースでは、この機能は 11.5 (1) SU5 で導入されました。一連の 12.x リリースでは、この機能は 12.5 (1) で導入されています。 • この機能が 11.5 (1) SU5 に導入されていて、12.x リリースにアップグレードする場合は、この機能のサポートを維持するために 12.5 (1) にアップグレードする必要があります。Jabber モバイル クライアントの永続的なチャットは、リリース 12.0 (1) または 12.0 (1) SU1 ではサポートされていません。
Cisco Jabber	• Cisco Jabber の最小リリースは 12.1 (0) です。 • Cisco Jabber の機能の詳細については、Cisco Jabber のマニュアルを参照してください。

コンフィギュレーション

永続的なチャットの設定方法の詳細については、*IM and Presence Service* の設定および管理ガイドの「チャットルームの設定」の章を参照してください。

リモート アカウント セキュリティ強化

リモートアカウント機能は、パスフレーズの公開キーと秘密キーのペアを使用して非対称ベースの暗号化モデルを使用するように拡張されています。この更新により、システムがリモートアカウントを介して侵入者によってアクセスされないようにすることによって、システムのセキュリティが強化されます。Cisco TAC 担当者のみがパスフレーズを復号化して、リモートアカウントを介してシステムにアクセスできるようにすることができます。

（注） この機能は、ユニファイドコミュニケーションマネージャーリリース 10.5 (2) SU7、11.5 (1) および 11.5 (1) SU4 でもサポートされています。

リモート アカウントの設定

TAC でケースをオープンしており、システムへのリモートアクセスを許可する必要がある場合は、Cisco ユニファイドオペレーティングシステムの管理インターフェイスの [**Remote Access Configuration**] ウィンドウからリモートアカウント情報を取得するか、または、ユーティリティの `remote_account status` CLI コマンドを実行します。

リモートアカウントの設定方法の詳細については、*Cisco Unified Communications Manager* のトラブルシューティングガイドの「TAC を使用したケースのオープン」の章にある「リモートアカウントのセットアップ」の手順を参照してください。または、コマンドラインインターフェイスを使用してリモートアカウントを設定することもできます。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions* 』の「`utils remote_account *`」コマンドを参照してください。

トラブルシューティング ログ

この機能では、次のトラブルシューティングログを使用できます。

- リモートサポート UI ログは、次の場所にあります。`/usr/local/thirdparty/jakarta-tomcat/logs/cmplatform/log4j/cmplatform * .log`
- リモートサポートの CLI ログは、次の場所にあります。`"/var/log/active/platform/log/cli * .log"`
- リモートサポート作成アカウントログは、「`/var/log/active/platform/log/createaccount * .log`」にあります。

ISR ゲートウェイベースの SCCP 会議ブリッジでの RFC 2833 DTMF サポート

リリース 12.5 (1) では、ユニファイドコミュニケーションマネージャは、ISR ゲートウェイベースの Skinny Client Control Protocol (SCCP) 会議ブリッジでインバンド RFC 2833 デュアルトーン多重周波数 (DTMF) をサポートしています。この更新により、SCCP 会議ブリッジは、インバンド DTMF とアウトオブバンド DTMF のシームレスなサポートを提供できます。

この機能により、DTMF インターワーキング用のメディアターミネーションポイント (MTP) を挿入する必要がなくなります。以前のリリースでは、アウトオブバンド DTMF のみがサポートされていた場合、会議参加者がインバンド RFC 2833 DTMF のみをサポートしているシナリオでは、ユニファイドコミュニケーションマネージャーが MTP を割り当てました。MTP の割り当てには、追加のメディアリソースとセキュリティ侵害が必要です。この機能の更新により、この問題に対処します。

RFC 2833 は、Cisco 4000 シリーズ ISR ゲートウェイベースの SCCP 会議ブリッジでのみサポートされています。Cisco 4000 シリーズ ISR ゲートウェイでは、最小リリースの16.7.1 が実行されている必要があります。アウトオブバンド DTMF のみをサポートする古い会議ブリッジの場合、ユニファイドコミュニケーションマネージャはインバンドサポートをアドバタイズしません。

LDAP の UDS プロキシ経由で会議室を検索する

このリリースの一部として、UDS プロキシ機能は、OpenLDAP サーバでのルームオブジェクト検索として表される会議室をサポートするように拡張されています。フィルタが設定されておらず、ディレクトリ サーバ タイプが OpenLDAP の場合、ユニファイドコミュニケーションマネージャーは、デフォルトのフィルタ文字列 (objectclass = inetOrgPerson) のみを使用してユーザを検索します。会議室を検索するには、フィルタ文字列を使用してカスタムフィルタを設定します (| (objectClass = intOrgPerson) (objectClass = room)) を使用し、LDAP 検索設定でこのカスタムフィルタを使用します。

これにより、Cisco Jabber クライアントは部屋に関連付けられた名前およびダイヤル番号で会議室を検索できます。会議室は、ルーム オブジェクトの OpenLDAP サーバに、givenName、sn(lastName)、または telephonenumber の属性が設定されていると検索可能です。

この機能は、スペースを含む複数の単語を含む検索文字列を使用して、**名前**検索の既存のトークン化ルールを拡張します。たとえば、3つのスペースを含む文字列 A B C D を検索する場合は、次のようになります。

1. 最初の名前として文字列全体 (A B C D) を検索します。
2. 最後の名前として文字列全体 (A B C D) を検索します。
3. 最初の単語 (A) を最初の名前、残りの単語 (B C D) を姓として検索します。
4. 最初の単語 (A) を姓、残りの単語 (B C D) を最初の名前として検索します。

アクティベーションコードを使用したデバイスオンボーディング

アクティベーションコードにより、新しくプロビジョニングされた電話機が簡単にプロビジョニングされます。アクティベーションコードは、電話機の登録時にユーザが入力する必要がある、シングル使用の16桁の値です。アクティベーションコードは、管理者が各電話機の MAC アドレスを収集して入力することなく、電話機のプロビジョニングとオンボードを行うための方法を提供します。

アクティベーション コードには次の利点があります。

- 実際の MAC アドレスを手動で入力する必要はありません。管理者はダミーの MAC アドレスを使用することができ、電話機は登録時に実際の MAC アドレスを使用して設定を自動的に更新します。
- 電話名を BAT から SEP に変換するために、タップなどの IVR を導入する必要はありません。

電話ユーザは、セルフケアポータルを使用してアクティベーションコードを取得できます。[**Show Phones Ready To Activate]**エンタープライズパラメータが [**True**] に設定されている場合に備えています。それ以外の場合は、管理者が電話機のユーザにコードを提供する必要があります。

（注） ダミー MAC アドレスを使用してプロビジョニングすると、アクティベーションコードは電話機モデルに接続されます。電話機をアクティブ化するには、電話機のモデルに一致するアクティベーションコードを入力する必要があります。

セキュリティを強化するために、電話機の実際の MAC アドレスを使用して電話機をプロビジョニングできます。管理者はプロビジョニング時に各電話機の MAC アドレスを収集して入力する必要があるため、このオプションにはより多くの設定が含まれますが、ユーザは電話機の実際の MAC アドレスに一致するアクティベーションコードを入力する必要があるため、セキュリティが向上します。

電話モデルのサポート

リリース 12.5 (1) では、アクティベーションコードは次の Cisco IP 電話 モデルでサポートされています。7811、7821、7832、7841、7861、8811、8841、8845、8851、8851NR、8861、8865および8865NR。

コンフィギュレーション

この機能を設定して使用する方法の詳細については、*Cisco Unified Communications Manager* の『 *System Configuration Guide* 』の「Device Onboarding with Activation code」の章を参照してください。

ユーザ インターフェイスの更新

この機能をサポートするために、次の更新が行われています。

- [**オンボード方式**] フィールドが [**デバイスのデフォルト**] ウィンドウに追加されました。アクティベーション コードを使用するには、このフィールドを**アクティベーション コード**に設定する必要があります。これが設定されている場合、これらの電話モデルでは、自動登録の代わりにアクティベーション コードがオンボードに使用されます。
- [**電話の設定（Phone Configuration）**] ウィンドウは次のコンフィギュレーション フィールドで更新されています。
  - [**アクティベーション コードが必要**]: このチェック ボックスをオンにすると、電話機ではアクティベーション コードをオンボードにする必要があります。
  - [**詳細の表示 (View Details)**]: アカウントの詳細を表示するには、このボタンをクリックします。
  - **新しいアクティベーション コードの生成**: アクティブなアクティベーション コードがあり、新しいアクティベーション コードを生成する場合は、このボタンをクリックします。
  - **リリース アクティベーションコード**: アクティベーションコードを削除するには、このボタンをクリックします。
- [**電話の検索/一覧表示 (Find And List phone)**] ウィンドウから [**アクティベーション コードのエクスポート (Export Activation code)**] オプションが**関連リンク**に追加されました。このオプションを使用して、アクティブなアクティベーション コードのリストを CSV ファイルに出力できます。
- 一括管理ツールの BAT テンプレートに、**オンボードオプションのアクティベーション コード**が追加されました。

セルフケア ポータルの更新

セルフケア ポータルに表示される電話機には、[**Ready To activate**] オプションが含まれています。これにより、電話ユーザはセルフケア ポータルを使用して電話機をアクティブ化できます。このオプションは、電話機がアクティブになっていない場合に表示され、アクティベーション用のアクティベーション コードが必要です。ユーザがこのオプションをクリックすると、電話機に関連付けられているアクティベーション コードが表示されます。電話機にコードを入力するか、電話機のカメラを使用してアクティベーション コード バーコードをスキャンすることで、電話機をアクティブ化できます。

この方法を使用するには、[**Show Phone Ready To Activate**]エンタープライズ パラメータを [**True**] に設定する必要があります。

有用性の更新

この機能をサポートするために、**シスコ デバイス アクティベーション サービス**が追加されました。この機能サービスは、デフォルトでイネーブルにされています。

アラームおよびカウンタの更新

このリリースでは、新しいアラーム**DevActApplicationOnboardIssue**が追加されています。このアラームは、デバイスのアクティブ化が失敗するたびにトリガーされます。このアラームには、モデルの不一致またはホスト名の不一致という2つの原因が考えられます。デバイスのオンボードを再試行する前に、新しいアクティベーション コードを生成することをお勧めします。

シスコデバイスアクティベーションサービスの下に、次の新しいカウンタが追加されました。

- **ActivationCodeAttempts**: アクティベーション コード作成要求の数を表します。
- **ActivationCodeFails**: 失敗したアクティベーション コード作成要求の数を表します。障害の理由には、電話機レコードごとに1つのコードなどの DB エラーが含まれます。API はレート制限されています。
- **Invokeattempts**: これは、呼び出し要求の数を表します。電話機が SRP ハンドシェイクをオンボードに開始しました。
- **呼び出し失敗 (invokefails)**: 失敗した呼び出し要求の数を表します。障害の理由には、サーバがビジー状態、APIがレート制限されている、または不正なアクティベーション コードを受信したなどがあります
- **Registerattempts**: これは register 要求の数を表します。電話機が SRP ハンドシェイクを完了し、オンボードになっています。
- **Registerfails**: これは、失敗した register 要求の数を表します。失敗の理由としては、サーバがビジー状態、APIがレート制限されている、モデルの不一致、デバイス名の不一致、または不正な MIC などがあります。
- **Releaseattempts**: アクティベーションコードのリリース要求の数を表します。アクティベーションコードのリリースが試行されます。
- **Releasefails**: これは、失敗したアクティベーションコードのリリース要求の数を表します。失敗などの API はレート制限されており、アクティベーションコードは存在しません。
- **ThrottleCount**: レート制限が原因で API が失敗した回数をカウントします。これは、スロットリングが発生したときを確認するために、1分ごとにゼロに戻ります。

セキュアエンドユーザログイン資格情報

以前のリリースでは、Ciscoユニファイド コミュニケーション マネージャ ではローカル エンド ユーザのログイン クレデンシャルは [sha1] を使用してハッシュされました。12.5(1) からのリリース以降、すべてのローカルエンドユーザのログイン クレデンシャルは強化されたセキュリティを提供するためにSHA2を使用してがハッシュされます。すべてのローカルエンドユーザのパスワードまたはPINは、最初の成功したログイン時に自動的に新しいSHA2標準を使用してに移行されます。

このリリースでは、ユニファイド コミュニケーション マネージャには、「**古いクレデンシャルのアルゴリズムを持つUCSユーザ**」 レポートが含まれます。このレポートは、Cisco Unified Reporting ページからアクセスでき、管理者が [SHA1] を使ってハッシュされたパスワードまたは PIN を持つすべてのユーザをリストするのに役立ちます。

User Interface Updates

「「**UCM Users with The Date Credential Algorithm**」 」というタイトルの新しいレポートが、シスコのユニファイドレポーティングインターフェイスの [**システムレポート (System report)**] メニューに追加されました。

オンライン ヘルプの更新

次の表に、セキュアエンドユーザのログインクレデンシャル機能のオンラインヘルプの更新を示します。The レポートはユニファイド コミュニケーション マネージャと IM and Presence Service では同じです。

表 *4:* エンドユーザの期限切れクレデンシャルレポート

レポート	説明
期限切れのクレデンシャルアルゴリズムを使用したユーザの UCM	では、SHA1 を使用してパスワードまたは Pin が保存され、ハッシュされているローカルエンドユーザのリストを提供しています。

安全なエンド ユーザーのログイン情報の詳細については、『*Security Guidefor Cisco Unified Communications Manager*』を参照してください。

外部プレゼンテーションの名前と番号

リリース 12.5 (1) では、個別の発信者番号とプレゼンテーション番号を含めるように Cisco ユニファイド CM の管理を設定できます。この機能により、ユーザはアウトバウンド PSTN コールを匿名化して、robocalls を削減するためのダイヤルイン方式 (DID) 番号ではなく、外部プレゼンテーションの名前と番号を表示することができます。

請求に外線番号を使用することはできません。匿名化名と番号は、個々のユーザまたはユーザのグループに対して実行できます。以前のリリースでは、ユニファイドコミュニケーションマネージャを回線単位で設定して、ダイヤルイン方式 (DID) 番号とは異なる番号を送信することはできませんでした。この機能は、PSTN コールにのみ適用されます。このリリースのユニファイドコミュニケーション マネージャでは、既存の ID 番号や名前とは異なる外部プレゼンテーション名と番号がサポートされています。設定されるプレゼンテーション名と番号は、次のデバイスで表示されます。

- SIP
- SCCP
- SNRD

ユーザ インターフェイスの更新

外部プレゼンテーションの名前と番号をサポートするために、次のユーザインターフェイスの更新が実装されています。

- [SIPプロファイルの設定（SIP Profile Configuration）] で、**[設定済み回線デバイス発信者情報のパススルーを許可（Allow Passthrough of Configured Line Device Caller Information）]** フィールドの名前を **[外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]** に変更します。
- 新しいサービス パラメータ**[外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]** が**[サービス パラメータ設定値]**のクラスタ パラメータの下に追加されました。
- 新しいセクション **[外部プレゼンテーション情報（External Presentation Information）]**が**[ディレクトリ番号設定]**ページに次の 3 つのフィールドと共に追加されました。
  - 名前非表示の外部プレゼンテーション
  - 外部プレゼンテーション番号
  - 外部プレゼンテーション名
- 次の表は、[**SIP プロファイルの設定 (SIP Profile Configuration)**] ページの既存および名前が変更されたフィールドを示しています。

表 *5 : SIP* プロファイル設定 *UI* 更新

既存のフィールド	名前変更したフィールド
[URI からの着信要求の設定（Incoming Requests FROM URI Settings）]	外部プレゼンテーション情報
Caller ID DN	外部プレゼンテーション番号
Caller Name	外部プレゼンテーション名

前の変更では、新しいチェックボックスの [**Anonymous External Presentation**] が追加されています。

- 次の表は、[**トランクの設定 (Trunk Configuration)**] ページの既存および名前が変更されたフィールドを示しています。

表 *6 :* トランク設定ページの *UI* 更新

既存のフィールド	名前変更したフィールド
発信者情報	プレゼンテーション情報
Caller ID DN	プレゼンテーション番号
Caller Name	プレゼンテーション名

既存のフィールド	名前変更したフィールド
[Maintain Original Caller ID DN and Caller Name in Identity Headers]	プレゼンテーション名と番号はFROMヘッダー チェックボックスでのみ送信し、他のアイデンティティヘッダーでは送信しないでください。

管理者が匿名プレゼンテーションidを設定できるようにするために、新しいチェックボックスの [**Anonymous presentation**] が表示されます。

セッション管理

ユーザの同時 ウェブ アプリケーションセッションの最大数を制限するには、**set webapp session maxlimit**コマンドを使用します。また、[**Session Management**] ウィンドウでユーザの詳細を入力することによって、各ノードに固有のユーザのアクティブなサインインセッションを終了することもできます。

現在のセッションの制限

このリリースでは、ユニファイドコミュニケーションマネージャは、ユーザの同時 ウェブ アプリケーションセッションの最大数を制限します。

これは、次のインターフェイスに適用されます。

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications セルフケア ポータル
- Ciscoユニファイド コミュニケーション マネージャ IM and Presence アドミニストレーション
- Cisco Unified IM and Presence Serviceアビリティ
- Cisco Unified IM and Presence のレポート

CLI 更新

セッション制限をサポートするために、**set webapp session maxlimit**という名前の新しいコマンドが導入されました。このコマンドを実行するには、コマンド特権レベル4のアクセス権を持っている必要があります。

set webapp sesshon maxlimitコマンドの詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Command Line Interface Reference Guide for Cisco Unified*

Communications Solutions、リリース *12.5(1)*』の「「コマンドの設定」」の章を参照してください。

セッションの終了

このリリースでは、ユニファイドコミュニケーションマネージャは、各ノードに固有のユーザのアクティブなサインインセッションを終了できます。

これは、次のインターフェイスに適用されます。

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications セルフケア ポータル
- Ciscoユニファイド コミュニケーション マネージャ IM and Presence アドミニストレーション
- Cisco Unified IM and Presence Serviceアビリティ
- Cisco Unified IM and Presence のレポート

ユーザ インターフェイスの更新

[**セッション管理 (Session Management)**] ウィンドウが、Cisco ユニファイド os 管理、Cisco Unified IM and Presnece OS 管理インターフェイスの [**セキュリティ (Security)**] メニューに追加されます。

セッション管理の設定

次の表に、[**セッション管理 (Session Management)**] ウィンドウのフィールドの詳細を示します。

フィールド	説明
Status（ステータス）	選択したユーザIDのセッション終了ステータスメッセージが表示されます。
セッションの終了	
ユーザ ID	アクティブなサインイン ユーザのユーザ ID を入力します。これは必須フィールドです。
セッションの終了	[**セッションの終了 (Terminate session)**] ボタンをクリックすると、サインインしているアクティブなユーザのセッションが終了します。

セッション終了方法の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の「セキュリティの管理」の章を参照してください。

アップグレードの簡易化

この機能により、ユニファイドコミュニケーションマネージャとインスタントメッセージング & プレゼンスサービスのネイティブアップグレードの操作性が向上します。

これにより、アップグレードプロセスがシンプルになります。

- アップグレード期間
- サービスの影響
- シーケンス処理の複雑さ
- 手動によるタッチポイント

データベースレプリケーションは再起動前の段階に移行され、変更管理を簡素化し、再起動後の更新によるユーザ/デバイスの影響を軽減します。

クラスタ全体のアップグレードを実行できます。ユニファイドコミュニケーションマネージャパブリッシャによって制御されるワンタッチクラスタ全体のアップグレードおよびリブートによって、手動のタッチポイントが90%削減され、メンテナンス時間の計画が簡素化され、全体的な期間 (大規模システムの場合は50%) がさらに短縮されます。

アップグレード前およびアップグレード後のCOPファイルを自動化することで、アップグレードの失敗を引き起こす可能性のある問題を早期に検出できます。

プライムコラボレーション導入バッチ COP インストールとタスクチェーンにより、マルチステージ操作のための手動のタッチポイントが削減されます。

コマンドラインインターフェイスとユーザインターフェイスの更新:

次の新しいオプションが、コマンドラインインターフェイスで、ユニファイドコミュニケーションマネージャ、IM and Presence ユーザ インターフェイス および**ユーティリティシステムの upgrade initiate**コマンドに追加されています。

- [**Install/Upgrade Cluster**] メニューが**ソフトウェアアップグレード**の下に追加されます。このオプションを使用すると、クラスタ内の選択されたすべてのノードでアップグレードファイルのダウンロードが完了した後にのみ、クラスタ全体のアップグレードを実行できます。
- **ユーティリティシステムアップグレードクラスタ**: この新しい cli コマンドを使用すると、cli を使用してクラスタ全体のアップグレードを実行できます。
- [**Reboot Cluster**] メニューが**ソフトウェアアップグレード**の下に追加されます。このオプションを使用すると、クラスタ全体の再起動またはスイッチバージョン操作を実行できま

す。スイッチのバージョンを実行するか、またはスライダーを使用してクラスタノードを順番に順番に配置して再起動することができます。

- [**Install/Upgrade Cluster** and **install/upgrade**] ページの [**Source**] ドロップダウンリストに [**Local Filesystem**] オプションが追加されました。

  ローカルイメージオプションは、CLI の**ユーティリティの system upgrade initiate**コマンドに表示されます。

  このローカルイメージまたはローカルファイルシステムソースオプションを使用すると、アップグレード中に以前にダウンロードした ISO または COP ファイルを使用できます。ダウンロードした ISO または COP ファイルがない場合、ソースにはローカルイメージ < none > が表示されます。ISO または COP ファイルがある場合は、.iso または COP でダウンロードしたファイルを含むローカルイメージオプションが表示されます。

- [**Use download credentials From パブリッシャ**] オプションは、ユニファイドコミュニケーションマネージャ、IM and Presence ユーザ インターフェイスの [**Software Installation/upgrade**] ページ および[**utils system upgrade initiate**] CLI コマンドに追加されます。このオプションを使用すると、パブリッシャのソース設定を使用できます。このオプションは、クラスタ内のユニファイドコミュニケーションマネージャサブスクライバ、IM and Presence パブリッシャ、またはサブスクライバノードで使用できます。このオプションは、クラスタ全体のアップグレードには適用されません。

- [**ダウンロード後にアップグレードを続行**] オプションは、ユニファイドコミュニケーションマネージャ、IM and Presence ユーザ インターフェイスの [**Software Installation/upgrade**] ページ および[**utils system upgrade initiate**] CLI コマンドに追加されます。このオプションを使用すると、ファイルのダウンロード後にアップグレードが自動的に開始されます。ユーザの確認を待たず、インストールを開始します。

- [**アップグレード後にバージョン サーバをスイッチ**] オプションは、ユニファイドコミュニケーションマネージャ、IM and Presence ユーザ インターフェイスの [**Software Installation/upgrade**] ページ および[**utils system upgrade initiate**] CLI コマンドに追加されます。このオプションを使用すると、アップグレードが正常に完了した後にシステムが自動的に再起動します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「utils system upgrade」セクションを参照してください。

詳細は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html にある *Cisco Unified Communications Manager* および *IM and Presence Service* のアップグレードおよび移行ガイドの「アプリケーションのアップグレード」セクションをご覧ください。

有用性の更新

プラットフォーム通信 ウェブ サービス はプラットフォーム サービスとして追加されました。このサービスは、Unified Communications Manager、IM and Presence Service および Cisco Unity Connection システム上で実行される、Representational State Transfer Protocol（REST）API です。

詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Serviceability Administration Guide*』の「プラットフォーム サービス」を参照してください。

アップグレード前および後の COP ファイル

このリリースでは、システムの健全性とアップグレードの準備状況を確認するために使用できる2つの COP ファイル(アップグレード前とアップグレード後) が提供されています。アップグレード前の COP で障害が発生した場合は、アップグレードを実行する前に修正する必要があります。

COP ファイルは一連のテストを実行し、アップグレードの失敗を引き起こす可能性のある問題を特定し、アップグレードの前後に情報を比較するために使用されるステータスと値のデータも収集します。この情報を使用して、必要に応じて是正措置を講じることができます。

詳細は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html にある *Cisco Unified Communications Manager* および *IM and Presence Service* のアップグレードおよび移行ガイドの「アップグレード前のタスク フロー」と「アップグレード後のタスク フロー」セクションをご覧ください。

ユニファイド コミュニケーション マネージャでの SIP OAuth サポート

Unified Communications Manager へのセキュア登録では、CTL ファイルの更新、共通証明書信頼ストアの設定などが行われます。Jabber デバイスがオンプレミスとオフプレミスの間で切り替わる場合、セキュア登録のたびに LSC を更新して CAPF 登録を更新する処理は複雑です。

Unified Communications Manager の SIP 回線で OAuth をサポートすることで、CAPF なしでセキュア シグナリングとセキュア メディアが可能になります。Unified Communication Manager クラスタと Jabber エンドポイントで OAuth ベースの認証を有効にすると、SIP 登録時に OAuth トークンの検証が行われます。

スマート ソフトウェア ライセンシング

11.5.1 では、プライム ライセンス マネージャは、オンボード APNS クラスタのバウチャーを提供します。12.x 以降、Cisco Smart Software Manager または Cisco Smart Software Manager サテ

ライトは、apn クラスタを Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する前に、オンボード APN クラスタのバウチャーを提供します。

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/cucm_b_push-notifications-deployment-guide_chapter_01.html#reference_CE836F3E3283BCF699F2AFC21426B783の「ライセンスの前提条件」の章を参照してください。

特定のライセンスの予約

これは Cisco Smart software manager または Cisco Smart Software manager サテライトへの接続にいつでも機能しない、安全性の高い環境の機能です。

特定のライセンスの予約では、ユニファイドコミュニケーションマネージャ製品インスタンス用に、権限付与、永久、または期間を予約できます。Cisco Smart Software Manager から生成された承認コードは、ユニファイド コミュニケーション マネージャ製品にインストールできます。また、指定されたライセンス消費内で製品を実行している場合、定期的な同期は必要ありません。

Cisco Smart Software Manager でライセンスを予約する機能は、スマートアカウントプロファイルを介して実行されます。スマートアカウントで特定のライセンスの予約を有効にするには、sa-adoption-support@external.cisco.comに電子メールを送信します。

シスコ特定ライセンス予約方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.htmlにある『*System Configuration Guide for Cisco Unified Communications Manager*』の「「Specific License Reservation」」の章を参照してください。

CLI 更新

この機能をサポートするために、次の新しい CLI コマンドが導入されました。

- ライセンスのスマート予約の有効化
- ライセンスのスマート予約の無効化
- スマート許可証予約要求
- license smart reservation cancel
- ライセンススマート予約インストール "< 認証-コード >"
- ライセンススマート予約インストールファイル < url >
- license smart reservation return
- ライセンススマート予約の戻り値承認「<authorization-code>」

CLI コマンドの詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『*Command*

Line Interface Reference Guide for Cisco Unified Communications Solutions』の「ライセンス コマンド」および「コマンドの表示」の章を参照してください。

アラームおよびアラートの更新

[Alert]

この機能をサポートするために、次の新しいアラートが導入されました。

- SmartLicense_SLR_InEval
- SmartLicense_SLR_NoProvision_EvalExpired
- SmartLicense_SLR_InOverage_NotAuthorized
- SmartLicense_SLR_NoProvision_NotAuthorized
- SmartLicense_SLR_ExportControlNotAllowed

これらのアラートの詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『「Cisco Unified リアルタイム モニタリング ツール アドミニストレーション ガイド』」の「パフォーマンスカウンタとアラート」の章を参照してください。

特定のライセンスの予約で制御されている機能のエクスポート

混合モードを有効にするかまたは CTL ファイルを更新するには、エクスポート制御機能設定を許可する、Cisco Smart ソフトウェア マネージャ (CSSM) のSmart アカウントから受信した認証コードを使用することにより、ユニファイドコミュニケーションマネージャで特定ライセンス予約が完了していることを確認します。

輸送設定の強化

このリリースでは、スマート アカウント管理者はチェック ボックスをオンにすると、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトへの登録中に交換されるユニファイド コミュニケーション マネージャの IP アドレスとホスト名を制限できます。

VMware ツールの更新

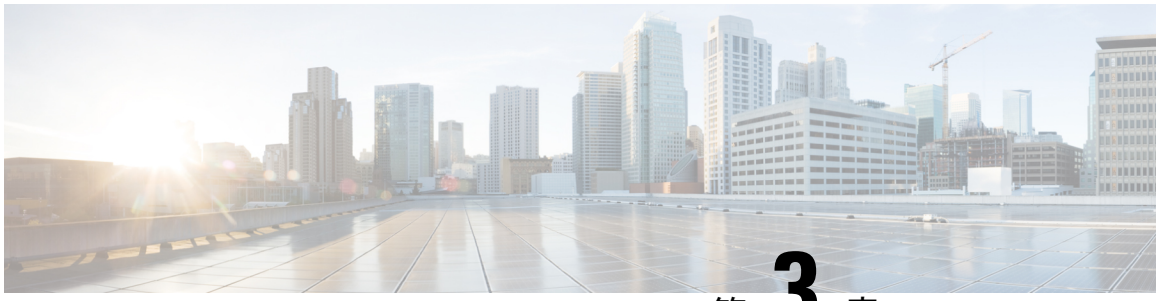
このリリースでは、ユニファイドコミュニケーションマネージャは次のいずれかで VMware ツールの更新をサポートしています。

- ネイティブ VMware ツール (VMware によって提供されます)
- オープン VMware ツール (シスコが提供)
- リリース 12.5 (1) よりも前のバージョンからユニファイドコミュニケーションマネージャをアップグレードするには、[ネイティブ (native VMware tools)] オプションを使用する必要があります。アップグレード後に VMware ツールを開くように変更できます。

- ユニファイドコミュニケーションマネージャリリース 12.5 (1) 以降 (たとえば、より高い SU)からアップグレードする場合は、システムでネイティブVMwareを使用するか、VMware ツールを開くかを選択できます。
- ユニファイドコミュニケーションマネージャリリース 12.5 (1) 以降からの新規インストールおよび PCD 移行については、デフォルトでインストールされている VMware ツールを開きます。

VMware ツールの更新方法の詳細については、*Cisco Unified Communications Manager* および *IM and Presence Service* のアップグレードおよび移行ガイドの「*VMware* ツールの更新」の章を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html。



第 3 章

特記事項

Unified CM 更新アップグレードでブルー スクリーンが表示される

特定のリリースへの Cisco Unified Communications Manager の更新アップグレードには、問題があります。タイムゾーン データの入力後 30 分以上の間、青色の移行画面が表示されることがあります。

このブルー スクリーンが表示された場合は、アップグレードを中止しないでください。また、カーネル パニックが発生します。ブルー スクリーンが表示されていても、アップグレードは引き続き実行されます。ブルー スクリーンは、約 30 分後には表示されなくなります。

影響を受けるアップグレードのバージョン

この問題は、アップグレードするバージョンが以下の表の範囲内にある場合に、Unified Communications Manager の更新アップグレードに影響します。この範囲には、範囲内にある SU と ES バージョンが含まれています。この問題は、該当範囲よりも古いバージョンまたは新しいバージョンへのアップグレードや、IM and Presence Service のアップグレードでは発生しません。

表 7: 更新アップグレードのブルー スクリーンの問題の影響を受けるアップグレード先バージョン

リリース カテゴリ	影響を受けるアップグレードのバージョンの範囲
10.5(x)	10.5.2.21170-1 ～ 10.5.2.22188-1（10.5(2)SU9 を含む）
11.5(x)	11.5.1.16099 ～ 11.5.1.17118-1（11.5(1)SU6 を含む）
12.0(x)	12.0.1.23036-1 ～ 12.0.1.24053-1（12.0(1)SU3 を含む）
12.5(x)	12.5.1.11001-1 — 12.5.1.12018-1（12.5(1)SU1 を含む）

詳細については、CSCvs28202 を参照してください。

無効なデフォルト 証明書 バックアップの失敗

ディザスタリカバリシステム (DRS) を使用してバックアップを実行する場合、**set cert default-cal-list disable {all | common-name}**を使用してすべてまたは特定のデフォルト証明書が無効になっている場合、バックアップに無効な証明書が含まれていません。新規にインストールされたサーバでバックアップを復元すると、それらの無効な証明書が再度表示されます。

新規インストールおよびアップグレード時のデフォルト CA 証明書

ユニファイドコミュニケーションマネージャリリース 12.5 (1) 以降をインストールすると、CAP_RTP_001 と CAP_RTP_002 証明書を除くすべてのデフォルト CA 証明書が存在します。これらの証明書を有効にするには、**set cert default-ca list enable {all | common-name}**コマンドを使用します。

Unified Communications Manager リリース 12.5 (1) 以降にアップグレードする場合は、アップグレード後に古いバージョンに存在していたデフォルトの証明書のみが表示されます。

Okta 経由の RTMT への SAML SSO ログインの Java 要件

Okta が id プロバイダーとして設定されている SAML SSO があり、SSO を使用して Cisco ユニファイドリアルタイムモニタリングツールにログインする場合は、最小 Java バージョン8.221 を実行している必要があります。この要件は Ciscoユニファイド コミュニケーション マネージャ および IM and Presence Service の 12.5(x) リリースに適用されます。

同じコールでサポートされていない複数のクロック レート

このリリースでは Cisco TelePresence エンドポイントと Cisco Jabber クライアントは、提供されたコーデックに一致するさまざまなクロックレートの複数の「電話イベント」 SDP 属性をサポートしていません。この機能は、VoLTE/IMS エンドポイントを完全にインターワーキングするために必要です。この更新のため、これらのエンドポイントタイプと VoLTE または IMS エンドポイント間の相互運用性の問題が、8 kHz の異なるクロックレートがネゴシエートされる通話中の再招待で発生する可能性があります。

これらのエンドポイント クラス間のコールの場合:

- 最初のコール セットアップは問題なく実行されます。
- 通話中の再招待では、INVITE がユニファイド コミュニケーション マネージャによって開始された場合、問題は発生しません。
- エンドポイントによって開始された再招待では、8 kHz とは異なるクロックレートを使用すると、相互運用性の問題が発生する可能性があります。

新しい Cisco ゲートウェイのサポート

Cisco Unified Communications Manager の新リリースでは、次の Cisco ゲートウェイに対するサポートが導入されています。

- Cisco VG400 アナログ音声ゲートウェイ
- Cisco VG450 アナログ音声ゲートウェイ
- Cisco 4461 サービス統合型ルータ

次の表に、サポートが導入されたゲートウェイ モデルと、リリース カテゴリ別の最初のリリースを示します。各リリースカテゴリ（たとえば、10.5(2)、11.5(x)）内では、ゲートウェイモデルのサポートは、そのカテゴリの後のリリースとともに、指定されたリリースとともに追加されます。これらのリリースでは、Cisco Unified Communications Manager の [**ゲートウェイの設定（Gateway Configuration**）]ウィンドウでゲートウェイを選択できます。

表 *8 :* リリース カテゴリ別の最初のリリースを使用する *Cisco* ゲートウェイ

ゲートウェイ モデル	10.5(2) リリース	11.5(x) リリース	12.0 （x） リリース	12.5 （x） リリース
Cisco VG 202、202 XM、204、204 XM、310、320、350 アナログ音声ゲートウェイ	10.5(2) 以降	11.5(1) 以降	12.0(1) 以降	12.5(1) 以降
Cisco VG400 アナログ音声ゲートウェイ	サポート対象外	11.5（1）SU7 以降	12.0（1）SU2 以降	12.5(1) 以降
Cisco VG450 アナログ音声ゲートウェイ	10.5（2）SU8 以降	11.5（1）SU6 以降	12.0（1）SU2 以降	12.5(1) 以降
Cisco 4321、4331 4351、4431、4451 サービス統合型ルータ	10.5(2) 以降	11.5(1) 以降	12.0（1）SU2 以降	12.5(1) 以降
Cisco 4461 サービス統合型ルータ	10.5（2）SU8 以降	11.5（1）SU6 以降	12.0（1）SU2 以降	12.5(1) 以降

Cisco アナログ電話アダプタ

Cisco アナログ電話アダプタは、アナログ電話機、またはファックスなどのアナログ デバイスをネットワークに接続します。これらのデバイスは、[**電話の設定（Phone Configuration**）] ウィンドウを使用して設定できます。次の表では、ATA シリーズのモデル サポートを取り上げています。

表 *9 : Cisco* アナログ電話アダプタ

ATA アダプタ	10.5(2)x リリース	11.5(x) リリース	12.0 （x） リリース	12.5 （x） リリース
Cisco ATA 190 アナログ電話アダプタ **	10.5(2) 以降	11.5(1) 以降	12.0(1) 以降	12.5(1) 以降
Cisco ATA 191 アナログ電話アダプタ **	10.5(2)SU7 以降	11.5(1)SU4 以降	12.0（1）SU2 以降	12.5(1) 以降

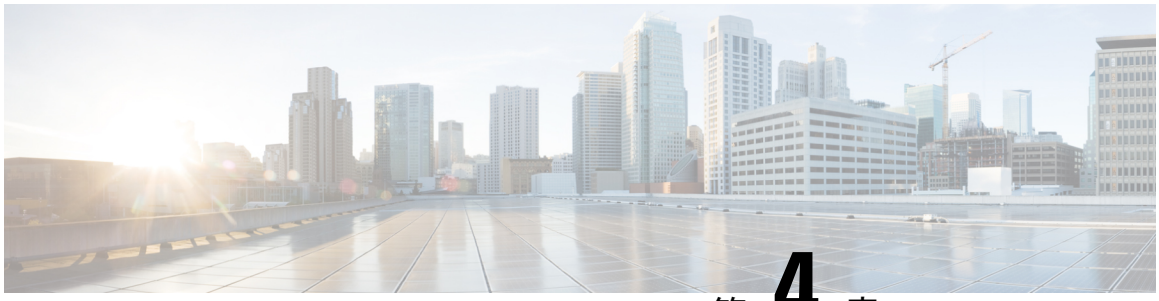
SDL リスニングポートの更新には、すべてのノードで CTIManager を再起動する必要がある

SDL リスニング ポートサービス パラメータの設定を編集する場合、サービスが実行されているすべてのクラスタ ノードで**Cisco CTIManager**サービスを再起動する必要があります。現在、ヘルプテキストにはサービスを再起動するように指示されていますが、サービスが実行されているすべてのノードでサービスを再起動する必要があるとは指示されていません。このサービスパラメータにアクセスするには、**システム**>**サービスパラメータ**に進み、**Cisco CTIManager**をサービスとして選択し、**[詳細(Advanced)]** をクリックして CTIManager サービスパラメータの完全なリストを表示します。

この更新は CSCvp56764 の一部です。

ビデオ エンドポイントの移行要件

Cisco TelePresence エンドポイントを任意の Cisco Unified Communications Manager 12.x リリースに移行する場合は、移行前に、ファームウェアを CE 9.8 以降にアップグレードすることを強く推奨します。それ以外の場合は、デバイスを登録するときに、既存のエンドポイントの設定がデフォルト設定で上書きされます。この問題は、CE9.7およびそれ以前のバージョンには、既存の設定を Unified CM (Communications Manager) に通信する方法がないために発生します。エンドポイントが CE 9.8 以降で実行されている場合、エンドポイントは移行時に既存の設定を維持します。



第 4 章

不具合

バグ検索ツール

システムは、重大度に従って既知の問題（バグ）を格付けします。これらのリリース ノートには、次のバグ レベルの説明があります。

- 重大度レベル 1 または 2 のすべてのバグ
- 重要な重大度レベル 3 のバグ。
- お客様から報告されたすべてのバグ

任意のリリースの任意の重大度のオープンな警告および解決済の警告は、お客様が必要に応じて障害情報を検索できるオンライン ツールである Cisco バグ検索ツールを使用して検索できます。

Cisco バグ検索ツールにアクセスするには、次のアイテムが必要です。

- インターネット接続
- ウェブ ブラウザ
- Cisco .com のユーザ ID とパスワード

Cisco バグ検索ツールを使用するには、以下のステップに従います。

1. Cisco バグ検索ツールにアクセスします: https://tools.cisco.com/bugsearch/。
2. 自分の Cisco.com のユーザ ID とパスワードでログインします。
3. 特定の問題に関する情報を検索する場合は、**[検索（Search for）]** フィールドにバグ ID 番号を入力し、**[移動(Go)]** をクリックします。

ヒント　バグの検索、保存された検索の作成、バググループの作成などの方法については、[バグ検索] ページの **[ヘルプ (help)]** をクリックしてください。

未解決の注意事項

次の表は、このリリースで開いている注意事項のリストです。https://bst.cloudapps.cisco.com/bugsearch/ のバグ検索ツールで障害を検索できます。

表 *10 :* ユニファイド コミュニケーション マネージャおよび *IM and Presence Service* 、リリース *12.5(1)* の未解決の注意事項

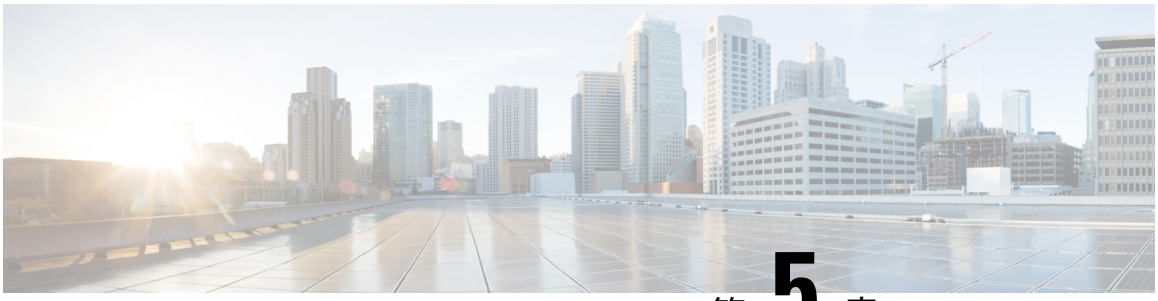
不具合	説明
Unified Communications Manager	
CSCvn02095	CUCM は、491への応答として、一時ポートで ACK を送信します。
CSCvn17505	CUCM が通話中 INVITE への応答として連絡先ヘッダーポートを変更する
CSCvn30046	CUCM 12.x クラスタに接続すると、EMCC SIP トランクコールが失敗する
CSCvn32181	拡張トラフィック負荷の下で、メモリの破損によって ccm プロセスのコアダンプが発生しました。
CSCvn36226	CVP は、CUCM に保留中の491要求を送信し、ユーザは5秒タイマーの前に切断しました。
CSCvn41358	早期参照転送のシナリオで、SRTP が偽の応答でリセットされる
CSCvn43882	SIPInterface は waitForAnswerorOfferorMXCap 状態でスタックしているため、空の invite を処理しません。
CSCvn57934	CUCM 10. x 以降では、メモリスロットリング仮想メモリパラメータは引き続き 2.9 GB に設定されています
CSCvn77411	RecordingGatewayRegistrationTimeout の後、SIPvBIB は IN_SERVICE 通知を受信しません。
CSCvn78081	SIP エンドポイントから転送が開始された場合、FAX コールが機能しない
CSCvn79777	複数の QueueControl Pid が原因でコールキューイング接続先 HuntPilot が失敗する
CSCvn80227	お客様は、予約済み文字を含むディレクトリ URI とパターンを挿入できません
CSCvn75533	SIP INVITE Call Info huntpiloturi パラメータを認識できない電話

不具合	説明
CSCvn78228	デュアルモード電話機から呼び出されたときにコールピックアップ機能が機能しない
CSCvn85800	ANAT が使用されている場合、CUCM が SDP から dtmf パラメータを失う
CSCvn85549	CUCM (着呼側) が SRST GW 結果から SIPStationCdfc リークに受信した場合、その値は1になります。
CSCvn85077	2つの MTP 挿入により、SNR から SNR へのコールが音声なしで失敗する
CSCvm95380	2018g による DST/TZ の更新
CSCvn26492	「パスワードユーザセキュリティの設定」 CLI メッセージの変更
CSCvn55141	アップグレードの実行中の経過時間の詳細
CSCvn73875	スマートライセンスのステータスが評価期限切れ/認証期限切れ/OOC (猶予期限切れ) の場合のアップグレードの失敗
CSCvn78796	クラスタアップグレード: UCM Pub に障害が発生した場合、UCM Sub と IM & P Pub はアップグレードを続行できません
CSCvn80652	IP アドレスが変更された CUCM パブリッシャセットのネットワークホスト名がサブスクライバに伝達されない
CSCvn81764	アップグレードの簡素化: CLI にクラスタステータスが表示されているときの混乱メッセージ
CSCvn91735	クリーンアップのインストールが何らかの状況で発生している
CSCvn82784	RTMT は、パブリッシャで AMC サービスをダウンしていることを示します。
CSCvm78768	CallManager マルチ San 証明書は、新しい証明書のアップロード中に古いものに切り替わります
CSCvm70018	複数の San CallManager 証明書をアップロードしている間に、TFTP サービスが自己再起動を早期に開始する
CSCvm86354	MultiSAN 証明書のアップロードは、pushCertificate の遅延により、false の負のステータスまたはタイムアウトを返します
CSCvn48876	CUCM が HTTP 要求に対して 200 OK を応答する (Oauth トークンの期限切れ)
CSCvn65166	SSO の有効化が正常にアップグレードされた後でも、SAML SSO ログインが失敗することがあります。
CSCvn90535	CTI コアを軽減する getAuthHeader 関数の検証チェック

不具合	説明
CSCvk22709	Export Phone 固有の詳細オプションを使用した BAT エクスポート ファイルの短縮ダイヤルの順序が正しくない
CSCvm93248	CCD 要求サービスをインポートできません
CSCvn01402	一括インターコム電話番号を追加できません
CSCvn40041	電話テンプレートの設定ページでボタンが機能しない
CSCvn51683	RTMT トレースログの収集: NAT セットアップでの SFTP サーバの RSA キーの UC アプリへの追加に失敗しました
CSCvn57671	Ldap 同期による LDAP アカウントのロックアウト
CSCvn20235	初めてオンボードしようとしている間に、クラウドのオンボードが失敗する
CSCvn49234	タグ routePartitionName の値は、addPhone axl api 要求中に追加されません。
CSCvn51603	複数のアナライザ-DNA が HTTP 500 エラーで失敗する
CSCvn57645	[全言語 (ALL-LANG)]: セルフケア: ステータスバーの文字列がロケールで英語で表示される
CSCvn57656	ALL-LANG: ccmadmin: EMCC クラスタ間サービスプロファイルの破損した文字
CSCvn64792	Axl を使用して 12.5.1.10000-15 に IPV6 Imp を挿入できない
CSCvn72342	デバイスの説明にアラビア語の言語がある場合、PCA で電話機が不明と表示される
CSCvn79005	[権限情報 (Permissions Information)] セクションで、ACG (アクセスコントロールグループ) & ロールがありません
CSCvn85656	カッコ付きの CUCM インポートパターンが UI に正しく表示されない
CSCvj07705	ワイヤレス アクセス ポイント コントローラが CUCM の「保留中」状態でスタックする
CSCvn15735	フィールド完了前にオペレーション「完了者」 検証をトリガー
CSCvn40028	インターコム電話番号の設定ページでインターコム DNs を更新できない
CSCvn46045	クライアントとサーバの JRE タイムゾーンバージョンが一致しない場合、RTMT はポップアップアラートを表示しません。
CSCvn47595	セルフケア: 8832 のアイコンがありません

不具合	説明
CSCvm76719	CMUI ログインでは、ログインが成功するまで数回 j_security_check エラーをクリアする必要があります
CSCvn26756	RTMT のコールフロー図に、最初の Invite CCM 12.0 が表示されない
CSCvn01600	AXL 要求 Addphone Buttontemplate を使用して追加されたコールパーク BLF ボタンは、CUCM DB では適切ではありません
IM and Presence Service	
CSCvn49679	IM & P パブリッシャ同期エージェントがホスト名の変更後に動作しない
CSCvn65321	<プレゼンス>パケットに特定の特殊文字が含まれている場合の XCP ルータコア
CSCvh72114	ICSA 定期同期の失敗」カーソルはすでにリリースされており、使用できません。
CSCvm40610	PushEnabledSessionsApns カウンタに誤った値が表示される
CSCvn12220	応答を受信する前にコールレッグが終了した場合、XCP SIP CM は発信要求をブロックしません。
CSCvn36404	ICSA は、xcpsecret 値が変更されていない場合でも、ICSA 同期中に R2Rconfig を同期する必要があります。
CSCvn40022	Cisco XCP Connection Manager サービスが、ドメインタイムアウトに対する disco # info 要求が発生した場合にクラッシュする
CSCvn46096	PEIDSQueryError の直後の IM & P PE コアダンプ
CSCvn62075	XCP ルータは、他のノードから受信したすべてのエッジ情報を無効にする必要があります。
CSCvn68387	Proxydomain にヌル値がある場合の XCP Auth コア
CSCvh63600	高負荷によるフェールオーバー後のプレゼンスの遅延更新
CSCvn73687	「バージョンスイッチング」セクションのアップグレードおよび移行ガイドに誤りのあるデータが含まれています
CSCvk44869	CAXL updateContact または addContact make 名簿サブスクリプションの両方
CSCvh72096	CUCM BAT 経由でプレゼンスを無効または有効にする場合の変更通知の遅延
CSCvk09795	アイドル状態の jabber d でのメモリリーク

不具合	説明
CSCvm63696	プレゼンススロットリングメカニズムで空のタグによって発生した Cisco XCP ルータサービスのクラッシュ
CSCvn05142	AD 同期機能の無効化とグループメンバーのプレゼンスのオフラインへの変更
CSCvn31799	External DB full による TC サービスメモリ リーク
CSCvn35499	前回の同期時刻が正しく更新されていません
CSCvn47142	12.5 tt5 の Jabberd コア
CSCvn50468	APNS クラスタオンボードがありませんが、証明書が見つからないため、IMP xcpconfigmgr がトークンを取得することが失敗しました
CSCvc98070	IM & P ノードは、別のノードのグループ チャット エイリアスを認識していません
CSCve61037	PChat、データベース MSSQL、CC モードを有効にした後、TC を開始できません
CSCvk22395	会議室からのプレゼンススタンザのステータスコードが、quiet/silent セッションに対して配信されない
CSCvn75705	L2 システムをアップグレードした直後の jabber d プロセスコアダンプ
CSCvn78563	EWS 経由で Microsoft Exchange サーバに接続すると Cisco Presence エンジンがクラッシュする
CSCvn90001	ICSA 用のポート37239の予約
CSCvo01877	起動結果の jabberd のデッドロックが最終的なコアです



第 5 章

Cisco エンドポイント

Cisco IP 電話およびゲートウェイ

電話機とゲートウェイのファームウェア バージョン

次の表に、Ciscoユニファイド コミュニケーション マネージャ 12.5 (1) でサポートされている最新の Cisco IP 電話 ファームウェアバージョンを示します。

表 *11* : 電話機ファームウェアのバージョン

電話ファミリ	ファームウェア リリース番号
Cisco Unified SIP 電話 3905	9.4(1)SR3
Cisco Unified IP 電話 6901 および 6911	9.3 (1) SR2
Cisco Unified IP 電話 6921、6941、6945 および 6961	9.4(1)SR3
Cisco IP 電話 7800 シリーズ	12.5(1)
Cisco IP 会議用電話 7832	12.5(1)
Cisco Unified IP 電話 7900 シリーズ	9.4 (2) SR3
Cisco Unified ワイヤレス IP 電話 7925G、7925G-EX および 7926G	1.4 (8) SR1
Cisco IP 電話 8800 シリーズ	12.5(1)
Cisco ワイヤレス IP 電話 8821	11.0(4)SR1 11.0 (5)

電話ファミリ	ファームウェア リリース番号
Cisco Unified IP 会議用電話 8831	10.3 (1) SR4b
Cisco IP 会議用電話 8832	12.5(1)
Cisco Unified IP 電話 8941/8945	9.4 (2) SR3
Cisco Unified IP 電話 8961、9951 および 9971	9.4 (2) SR4

次の表に、Ciscoユニファイド コミュニケーション マネージャ 12.5 でサポートされている最新のゲートウェイファームウェアバージョンを示します。

表 *12*：ゲートウェイのファームウェア バージョン

電話ファミリ	ファームウェア リリース番号
Cisco ATA 190 アナログ電話アダプタ	1.2.2
Cisco ATA 191 アナログ電話アダプタ	12.0 (1) SR1

Ciscoユニファイド コミュニケーション マネージャ での電話機ファームウェアリリース

各 Ciscoユニファイド コミュニケーション マネージャ リリースには、電話機のファームウェアのバージョンが1つ含まれています。ただし、このバージョンは電話機のファームウェアの最新バージョンではない可能性があります。

電話機のファームウェアの最新バージョンは、ソフトウェア ダウンロード サイトから入手できます。

Ciscoユニファイド コミュニケーション マネージャ セルフケアポータル

Ciscoユニファイド コミュニケーション マネージャ セルフケアポータルは、PDF 形式の IP 電話 のユーザガイドへのリンクを提供します。これらのユーザ ガイドはポータルに保存され、Ciscoユニファイド コミュニケーション マネージャ リリースに付属の電話機のファームウェアバージョンと一致します。

Cisco Unified Communications Manager リリース後、ユーザガイドの後続の更新は、Cisco Web サイトにのみ表示されます。電話ファームウェアのリリース ノートには、該当するドキュメントの URL が含まれています。Web ページで、更新されたドキュメントのドキュメントリンクの横には「更新済」と表示されます。

（注） Cisco Unified Communications Manager デバイスパッケージおよびユニファイド コミュニケーション マネージャ エンドポイント ロケール インストーラは、Cisco Unified Communications Manager の英語のユーザガイドを更新しません。

管理者およびユーザは、シスコのウェブサイトで更新されたユーザガイドを確認し、PDFファイルをダウンロードする必要があります。管理者は、会社のウェブサイトでユーザがファイルを使用できるようにすることもできます。

ヒント　管理者は、会社に導入されている電話機モデルの ウェブ ページをブックマークして、それらの Url をユーザに送信することができます。

Ciscoユニファイド コミュニケーション マネージャ で廃止された電話機モデル

Ciscoユニファイド コミュニケーション マネージャ のファームウェア リリース 12.0 以降、次の電話機はサポートされません。

- Cisco Unified IP 電話 7970G
- Cisco Unified IP 電話 7971G-GE
- Cisco Unified ワイヤレス IP 電話 7921G

Ciscoユニファイド コミュニケーション マネージャ のファームウェア リリース 11.5 以降、次の電話機はサポートされません。

- Cisco IP 電話 12 SP+ および関連モデル
- Cisco IP 電話 30 VIP および関連モデル
- Cisco Unified IP 電話 7902
- Cisco Unified IP 電話 7905
- Cisco Unified IP 電話 7910
- Cisco Unified IP 電話 7910SW
- Cisco Unified IP 電話 7912
- Cisco Unified ワイヤレス IP 電話 7920
- Cisco Unified IP Conference Station 7935

IPv6-Only は SCCP ファームウェアを搭載している Cisco IP 電話に影響する

Ciscoユニファイドコミュニケーションマネージャ リリース12.0では、IPv6を使用してSession開始プロトコル (SIP) ファームウェアを実行している電話と通信できます。

一部のCisco IP 電話は、Skinny Client Control Protocol（SCCP）ファームウェアで実行できます。SCCP ファームウェアはIPv6 をサポートしていません。次のデスクフォンは、SIP またはSCCP ファームウェアで実行できます。

- Cisco Unified IP 電話 6901、6911、6921、6941、6945 および 6961
- Cisco Unified IP 電話 7906G、7911G、7931G、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7965G、7962G、7970G、7971G-GE and 7975G
- Cisco Unified IP 電話 8941 および 8945

IPv6のみで通信するようにCiscoユニファイド コミュニケーション マネージャをセットアップした場合、SCCPファームウェアがインストールされている上記の電話のいずれかをSIPファームウェアにアップグレードする必要があります。SCCP ファームウェアは、IPv6 を使用してCiscoユニファイド コミュニケーション マネージャ と通信できません。

Cisco ワイヤレス IP 電話 の 7925G、7925G-EXおよび 7926G は、SCCP 電話機でもあります。SIP ファームウェアを備えておらず、IPv4 のみをサポートしています。

CiscoユニファイドコミュニケーションマネージャでのIPv6の設定方法の詳細は、*Cisco Unified Communications Manager* システム設定ガイド の 「IPv6 の設定」 を参照してください。

Cisco Unified SIP 電話 3905 の機能

ファームウェア リリース 9.4(1)SR3 では、Cisco Unified SIP 電話 3905 の新機能は導入されていません。

Cisco Unified IP 電話 6900 シリーズの機能

Cisco Unified IP 電話 6900 シリーズに導入された新機能はありません。

Cisco IP 電話 7800 シリーズの機能

次の表に、ファームウェア リリース 12.0(1)、12.1(1)、12.1(1) SR1 および 12.5(1) 用に Cisco IP 電話 7800 シリーズに追加された機能を示します。詳細は、次の場所にあるリリース ノートを参照してください：http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html

機能名	ファームウェア リリース
IPv6 機能サポート	12.0(1)
Expressway 経由でのモバイルおよびリモート アクセスとドメイン名の処理	12.0(1)
Cisco ヘッドセット 531 および Cisco ヘッドセット 532	12.1(1)

機能名	ファームウェア リリース
G g722.2 ANR-WB のサポート	12.1(1)
トランスポート層セキュリティ強化	12.1(1)
一括ダイヤル	12.1 (1) SR1
アクティベーションコードのオンボーディング	12.5(1)
Cisco ヘッドセット 561 および 562	12.5(1)
ヘッドセット ユーザのハンドセットを無効にする	12.5(1)
Transport Layer Support 暗号方式の無効化	12.5(1)
楕円曲線のサポート	12.5(1)
対話型接続の確立およびメディアパス	12.5(1)
ヘッドセット パラメータのリモート設定	12.5(1)
ウィスパー ページ and Ciscoユニファイド コミュニケーション マネージャ Express	12.5(1)

Cisco IP 会議用電話 7832 の機能

次の表に、ファームウェアリリース 12.0 (1)、12.1 (1) および 12.5 (1) 用に Cisco IP 会議用電話 7832 に追加された機能を示します。詳細は、次の場所にあるリリース ノートを参照してください：http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html

機能名	ファームウェア リリース
クライアント関連コードと強制承認コード	12.1(1)
Expressway 経由でのモバイルおよびリモートアクセス	12.1(1)
トランスポート層セキュリティ強化	12.1(1)
Transport Layer Support 暗号方式の無効化	12.5(1)
楕円曲線のサポート	12.5(1)
ウィスパー ページ and Ciscoユニファイド コミュニケーション マネージャ Express	12.5(1)

Cisco Unified IP 電話 7900 シリーズの機能

Cisco Unified IP 電話 7900 シリーズに導入された新機能はありません。

Cisco Unified ワイヤレス IP 電話 7920 シリーズ機能

Cisco Unified ワイヤレス IP 電話 792x シリーズには新機能が導入されていません。

Cisco IP 電話 8800 シリーズの機能

次の表に、ファームウェアリリース 12.0 (1)、12.0 (1) SR1、12.1 (1)、12.1 (1) SR1 および 12.5 (1) 用に Cisco IP 電話 8800 シリーズに追加された機能を示します。詳細は、次の場所にあるリリース ノートを参照してください：http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

機能名	ファームウェア リリース
拡張回線モード向け新機能サポート	12.0(1)
IPv6 機能サポート	12.0(1)
Expressway 経由でのモバイルおよびリモートアクセスとドメイン名の処理	12.0(1)
Cisco IP 電話 8851、8851NR、8861、8865 および 8865NR のキー拡張モジュール	12.0(1)
Cisco ヘッドセット 531 および Cisco ヘッドセット 532	12.1(1)
音声フィードバック	12.1(1)
コール履歴拡張	12.1(1)
着信コールと拡張回線モード	12.1(1)
スピードダイヤルとナビゲーションの機能拡張	12.1(1)
G g722.2 ANR-WB のサポート	12.1(1)
トランスポート層セキュリティ強化	12.1(1)
着信コールの拡張回線モードと簡易回線表示	12.1(1)SR1
壁紙とキー拡張モジュール	12.1(1)SR1
一括ダイヤル	12.1 (1) SR1

機能名	ファームウェア リリース
アクティベーションコードのオンボーディング	12.5(1)
中国語のサポート	12.5(1)
Cisco ヘッドセット 561 および 562	12.5(1)
ヘッドセット ユーザのハンドセットを無効にする	12.5(1)
Transport Layer Support 暗号方式の無効化	12.5(1)
楕円曲線のサポート	12.5(1)
拡張回線モードとコール履歴	12.5(1)
対話型接続の確立およびメディアパス	12.5(1)
ヘッドセット パラメータのリモート設定	12.5(1)
Transport Layer Security 1.2 およびワイヤレス認証	12.5(1)
ウィスパー ページ and Ciscoユニファイド コミュニケーション マネージャ Express	12.5(1)

Cisco ワイヤレス IP 電話 8821 の機能

次の表に、ファームウェアリリース 11.0 (3) SR4、11.0 (3) SR5、11.0 (3) SR6、11.0 (4)、11.0 (4) SR1 および 11.0 (4) SR2 の Cisco ワイヤレス IP 電話 882x シリーズに追加された機能を示します。詳細は、次の場所にあるリリース ノートを参照してください：http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

機能名	ファームウェア リリース
Opus コーデック サポート	11.0 (3) SR4
一括配置ユーティリティ	11.0 (3) SR4
設定可能なホーム画面	11.0(4)
ローカル連絡先（Local Contacts）	11.0(4)
問題レポート ツール	11.0(4)
呼出音の機能拡張	11.0(4)

機能名	ファームウェア リリース
ファームウェア リリース 11.0 (4) のユーザ インターフェイスの機能拡張	11.0(4)
壁紙のサイズ変更	11.0(4)

Cisco Unified IP 会議用電話 8831 の機能

Cisco Unified IP 会議用電話 8831 に導入された新機能はありません。

Cisco IP 会議用電話 8832 の機能

次の表に、ファームウェアリリース 12.0 (1) SR2、12.0 (1) SR3、12.1 (1)、12.5(1)SR2 および 12.5 (1)SR3 用に Cisco 会議 IP 電話 8832 に追加された機能を示します。詳細は、次の場所にあるリリース ノートを参照してください：http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

機能名	ファームウェア リリース
Cisco IP 会議用電話 8832 PoE インジェクタ	12.0 (1) SR2
オーディオ クロック周波数	12.0 (1) SR3
クライアント関連コードと強制承認コード	12.1(1)
デイジーチェーンのサポート	12.1(1)
G g722.2 ANR-WB のサポート	12.1(1)
ワイヤレスマイクのサポート	12.1(1)
Expressway 経由でのモバイルおよびリモート アクセス	12.1(1)
トランスポート層セキュリティ強化	12.1(1)
Wi-Fi サポートおよびワイヤレス LAN プロファイル	12.1(1)
Transport Layer Support 暗号方式の無効化	
楕円曲線のサポート	12.5 (1) SR2
Transport Layer Security 1.2 およびワイヤレス認証	12.5 (1) SR2
ウィスパー ページ and Ciscoユニファイド コミュニケーション マネージャ Express	12.5 (1) SR2

Cisco Unified IP 電話 8941 および 8845 の機能

Cisco Unified IP 電話 8941 および 8945 に対して導入された新機能はありません。

Cisco Unified IP 電話 8961、9951 および 9971 の機能

Cisco Unified IP 電話 8961、9951 および 9971 に対して導入された新機能はありません。

Cisco ATA 190 シリーズの機能

Cisco ATA 190 アナログ電話アダプタには新しい機能が追加されていません。

Cisco ATA 191 アナログ電話アダプタは、Ciscoユニファイド コミュニケーション マネージャ 12.1 がリリースされた後にリリースされました。このデバイスでは、アナログ電話または fax 装置を IP フォンに変えることができます。初期リリース後に新しい機能は導入されていません。