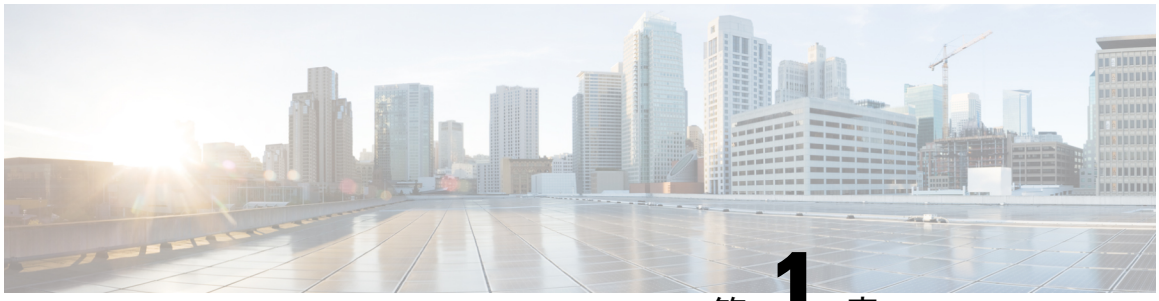
Cisco Unified Communications Manager および IM and Presence Service リリース 11.5（1）SU1 のリリース ノート

初版：2016 年 8 月 22 日

最終更新：2019 年 8 月 27 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

マニュアルの変更履歴

日付	リビジョン
2017 年 10 月 6 日	ドキュメンテーションの不具合 CSCvg10775 に関する情報を更新する
2017 年 10 月 23 日	88xx 電話の帯域幅割り当てに関する重要な注意事項が追加された。
2017年11月2日	ルートフィルタと関連付けられたルートパターンに関する重要な注意事項が追加された。
2017年12月13日	CSCvd71818 および CSCvg70867 の欠落している ENUM 値に関するトピックが追加された。

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。

リリース 11.5(1)SU1 のドキュメント

このリリースのマニュアルとして、11.5(1) リリースの既存のドキュメントを使用できます。ただし、11.5(1) SU1 バージョンが存在する場合は、11.5(1) SU1 バージョンを使用する必要があります。

次のドキュメントは、11.5(1) SU1 固有のバージョンで更新および公開されました。

- Cisco Unified Communications Manager and IM & Presence Service リリース 11.5(1)SU1 アドミニストレーション ガイド
- Cisco Unified Serviceability アドミニストレーション ガイド、リリース 11.5(1)SU1
- Cisco Unified Communications Manager リリース 11.5(1)SU1 セキュリティガイド
- Cisco Unified Communications Manager リリース 11.5(1)SU1 システム設定ガイド

また、11.5(1) SU1 リリースに関連する警告、バグ修正 および重要な注意については、次のドキュメントを参照してください。

- Cisco Unified Communications Manager、リリース 11.5(1)SU1 の Readme ファイル
- Cisco Unified CM IM and Presence サービス、リリース 11.5(1) SU1 の Readme ファイル

リリース 11.5(1) の既存のドキュメンテーション

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 サービスのリリース 11.5(1) で使用可能なドキュメントセットの詳細については、次のドキュメントを参照してください。11.5(1)SU1 バージョンが存在する場合を除き、11.5(1) ドキュメントは 11.5(1)SU1 で再利用できます。

- Cisco Unified Communications Manager and IM and Presence Service リリース 11.5(1) ドキュメンテーション ガイド

ソフトウェア バージョン

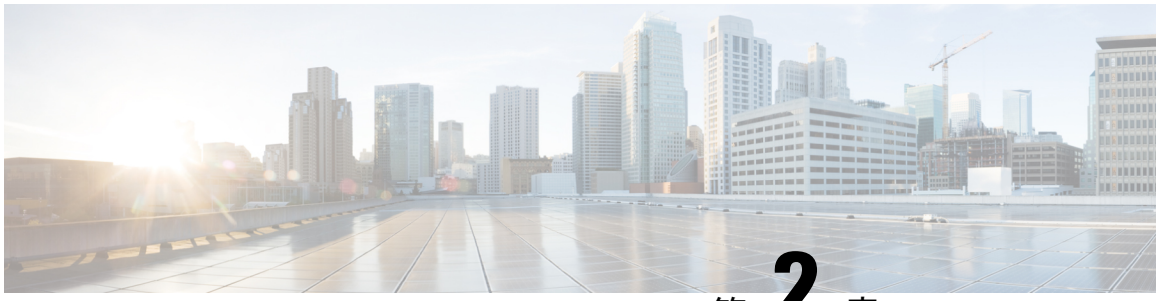
このリリースでは、次のソフトウェア バージョンがサポートされています。

- Ciscoユニファイド コミュニケーション マネージャ 11.5.1.11900-22
- IM and Presence Service 11.5.1.11900-21

サポートされるプラットフォーム

このリリースの Ciscoユニファイド コミュニケーション マネージャ は、次のオペレーティングシステムでテストされていてサポートしています。

- Microsoft Windows
- Linux



第 2 章

アップグレード

バージョン要件

11.5 (1) SU1 までのバージョン 11.x の場合

IM and Presence ノードをインストールする場合は、最初にアップグレードする IM and Presence ノード（IM and Presence データベース パブリッシャ ノード）のソフトウェア バージョンが、Unified Communications Manager パブリッシャ ノードにインストールされているソフトウェア バージョンの先頭の 3 つの番号と一致している必要があります。たとえば、 IM and Presence Service のソフトウェア バージョン 11.0.1.10000-1 は、Unified Communications Manager のソフトウェア バージョン 11.0.1.30000-2 と互換性があります。サンプルの Unified Communications Manager のバージョンと、互換性のある IM and Presence Service のバージョンについては、次のテーブルを参照してください。太字の番号が一致する必要があります。

表 *1 :* 互換性のある *Unified Communications Manager* および *IM and Presence Service* のバージョンの例

サンプルの Unified Communications Manager バージョン	互換性のある IM and Presence Service バージョンの例
11.0.1 .30000-2	**11.0.1** .10000-1
11.5.1.10000-6	**11.5.1**.10000-4

最初の IM and Presence ノードをインストールした後にインストールする IM and Presence サブスクライバ ノードのソフトウェア バージョンは、最初の IM and Presence ノードの 5 つのバージョン番号と一致している必要があります。たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合は、すべての IM and Presence のサブスクライバ ノードも 11.5.1.10000-1 である必要があります。

リリース 11.5(1) SU2

リリース 11.5(1)SU2 の場合、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 サービス の両方で、公式の 11.5(1)SU2 バージョンを実行している必要があります。以前のバージョンの IM and Presence Service と一緒に Ciscoユニファイド コミュニケーション マネージャ の 11.5(1)SU2 バージョンを実行することはサポートされません。同様に、以前のバージョンの Unified Communications Manager と一緒に IM and Presence Service の 11.5(1)SU2 バージョンを実行することはサポートされません。

次のソフトウェアバージョンは、Release 11.5(1)SU2 でサポートされています。

- Unified Communications Manager 11.5.1.12900-21
- IM and Presence Service 11.5.1.12900-25

リリース 11.5(1) SU3

リリース 11.5(1)SU3 の場合、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 サービス の両方で、公式の 11.5(1)SU3 バージョンを実行している必要があります。以前のバージョンの IM and Presence Service と一緒に Ciscoユニファイド コミュニケーション マネージャ の 11.5(1)SU3 バージョンを実行することはサポートされません。同様に、以前のバージョンの Unified Communications Manager と一緒に IM and Presence Service の 11.5(1)SU3 バージョンを実行することはサポートされません。

次のソフトウェアバージョンは、Release 11.5(1)SU3 でサポートされています。

- Unified Communications Manager 11.5.1.13900-52
- ユニファイド コミュニケーション マネージャ 11.5.1.13901-3
- ユニファイド コミュニケーション マネージャ 11.5.1.13902-2
- IM and Presence Service 11.5.1.13900-57
- IM and Presence Service 11.5.1.13901-1

リリース 11.5(1)SU4

サポートされているバージョンは次のとおりです。

- Ciscoユニファイド コミュニケーション マネージャ 11.5.1.14900-11
- IM and Presence Service 11.5.1.14900-32

このリリースでは、IM and Presence サービスの次の 2 つの主要な導入オプションが提供されています。

- 標準展開（分散化）：この展開では、展開をサポートするには、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 サービスの両方で上記の 11.5(1)SU4 バージョンを実行している必要があります。バージョンの不一致はサポートされていません。
- IM and Presence サービスの集中展開：IM and Presence 集中クラスタ内の、Ciscoユニファイド コミュニケーション マネージャ インスタンス（これは主にデータベースとプロビジョニング インスタンスであり、テレフォニーは処理しません）と IM and Presence サービスの両方で 11.5(1)SU4 バージョンを実行している必要があります。ただし、IM and Presence サービスが接続されているリモートテレフォニークラスタは、11.5 (1) SU4 バージョンを実行している必要はありません。

リリース 11.5(1)SU5

サポートされているバージョンは次のとおりです。

- Ciscoユニファイド コミュニケーション マネージャ 11.5.1.15900-18
- IM and Presence Service 11.5.1.15900-33

このリリースでは、IM and Presence サービスの次の 2 つの主要な導入オプションが提供されています。

- 標準展開（分散化）：この展開では、展開をサポートするには、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 サービスの両方で上記の 11.5(1)SU5 バージョンを実行している必要があります。バージョンの不一致はサポートされていません。
- IM and Presence サービスの集中展開：IM and Presence 集中クラスタ内の、Ciscoユニファイド コミュニケーション マネージャ インスタンス（これは主にデータベースとプロビジョニング インスタンスであり、テレフォニーは処理しません）と IM and Presence サービスの両方で 11.5(1)SU4 バージョンを実行している必要があります。ただし、IM and Presence サービスが接続されているリモートテレフォニークラスタは、11.5 (1) SU5 バージョンを実行している必要はありません。

リリース 11.5(1)SU6

サポートされているバージョンは次のとおりです。

- Ciscoユニファイド コミュニケーション マネージャ 11.5.1.16900-16
- IM and Presence Service 11.5.1.16910-12

このリリースでは、IM and Presence サービスの次の 2 つの主要な導入オプションが提供されています。

- 標準展開（分散化）：この展開では、展開をサポートするには、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 サービスの両方で上記の 11.5(1)SU6 バージョンを実行している必要があります。バージョンの不一致はサポートされていません。
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster、both the IM and Presence Service and the Ciscoユニファイド コミュニケーション マ

ネージャ instance (this is primarily a database and provisioning instance、and does not handle telephony) must be running an 11.5(1)SU5 version. ただし、IM and Presence サービスが接続されているリモートテレフォニークラスタは、11.5 (1) SU6 バージョンを実行している必要はありません。

Ciscoユニファイドコミュニケーションマネージャのアップグレード パス

次の表に、サポートUnified Communications Managerされているアップグレードパスの範囲を示します。サポートされるアップグレードパスの詳細については、『*Cisco Unified Communications Manager Software Compatibility Matrix*』を参照してください（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html）。

表 *2 : Unified Communications Manager* アップグレード パス、リリース *11.5(1)*

遷移元	目的	アップグレード タイプ
8.5(x) 以前のリリース	11.5 (1) SU1	更新アップグレード。必須 COP ファイル： • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn オプションの COP ファイル： • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn • ciscocm.free_common_space_v<latest_version>.cop.sgn
8.6(x)	11.5 (1) SU1	更新アップグレード。必須 COP ファイル： • ciscocm.version3-keys.cop.sgn オプションの COP ファイル： • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn • ciscocm.free_common_space_v<latest_version>.cop.sgn
9.1(x)	11.5 (1) SU1	更新アップグレード。必須 COP ファイル： • ciscocm.version3-keys.cop.sgn オプションの COP ファイル： • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn • ciscocm.free_common_space_v<latest_version>.cop.sgn

遷移元	目的	アップグレード タイプ
10.5(x)	11.5 (1) SU1	標準アップグレード：COP ファイルは不要。
11.0(x)	11.5 (1) SU1	標準アップグレード：COP ファイルは不要。
11.5(1)	11.5 (1) SU1	標準アップグレード：COP ファイルは不要。

ここに記載されていないリリースからのアップグレード、または MCS ハードウェアにインストールされているリリースからのアップグレードを行うには、Prime Collaboration Deployment を使用してアップグレードを実行する必要があります。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」を参照してください。

IM and Presence サービスのアップグレード パス

次の表に、IM and Presence サービスに対してサポートされるアップグレードパスの範囲を示します。サポートされるアップグレード パスの詳細については、『*Cisco Unified Communications Manager Software Compatibility Matrix*』を参照してください（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html）。

表 *3 : Cisco Unified Presence* リリースからのアップグレード パス

元の Cisco Unified Presence リリース	アップグレード先の IM and Presence リリース	アップグレード タイプ
8.5(4) ～ 8.6(1)	11.5 (1) SU1	更新アップグレード。以下の COP ファイルが必要： • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

表 *4 : IM and Presence Service* 各リリースからのアップグレード パス

元の IM and Presence リリース	アップグレード先の IM and Presence Release	アップグレード タイプ
9.1(x)	11.5 (1) SU1	更新アップグレード。以下の COP ファイルが必要： • ciscocm.version3-keys.cop.sgn
10.5(x)	11.5 (1) SU1	標準アップグレード：COP ファイルは不要。
11.0(x)	11.5 (1) SU1	標準アップグレード：COP ファイルは不要。
11.5(1)	11.5 (1) SU1	標準アップグレード：COP ファイルは不要。

ここに記載されていないリリースからのアップグレード、または MCS ハードウェアにインストールされているリリースからのアップグレードを行うには、Prime Collaboration Deployment を使用してアップグレードを実行する必要があります。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」を参照してください。

FIPS Mode を有効にした状態でのアップグレード

リリース 11.5(x) では、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 は、FIPS モードが有効になっている場合、2048 ビット未満のキーサイズの RSA 証明書をサポートしていません。これは、サーバ証明書と LSCs に影響します。

FIPS モードが有効になっているリリース 11.5 (x) にアップグレードしており、現在のバージョンで2048 ビット未満の RSA キーサイズを使用している場合は、次のいずれかの項目を実行して問題を解決できます。

次のいずれかの操作を実行できます。

- 現在のバージョンが 2048 ビットのキーサイズをサポートしている場合は、アップグレードする前に影響を受ける証明書を再生成します。または、
- リリース 11.5(x) にアップグレードした後、影響を受ける証明書を再生成します。

（注） このオプションを選択すると、セキュアな接続では、RSA キーサイズが 2048 ビット以上になるまで、影響を受ける証明書の使用は許可されません。

非推奨の電話のモデル

非推奨の電話機を含むアップグレード

以前のリリースのこれらの電話機のいずれかを使用していて、このリリースにアップグレードする場合は、次の操作を実行します。

1. ネットワーク内の電話機が、リリース 11.5 でサポートされているかどうかを確認します。
2. サポートされていない電話機を確認します。
3. サポートされていない電話機の場合は、電話の電源を切り、ネットワークから電話を切断します。
4. この電話機のユーザに、サポートされる電話機をプロビジョニングします。移行 FX ツールを使用して、古いモデルから新しいモデルの電話機に移行することができます。詳細に

ついては、http://refreshcollab.cisco.com/webportal/46/CUCM%20Readiness%20Assessment#endpoint_refresh_tool を参照してください。

5. ネットワーク内のすべての電話機がリリース 11.5 でサポートされたら、システムをアップグレードします。

（注） 非推奨の電話機は、アップグレード後に削除することもできます。管理者がアップグレードの完了後に、Ciscoユニファイド コミュニケーション マネージャ にログインすると、システムに非推奨の電話機の管理者に通知する警告メッセージが表示されます。

ライセンシング

非推奨の電話機とサポートされている電話機を交換するために、新しいデバイス ライセンスを購入する必要はありません。システムから非推奨の電話機を削除するか、新しいCiscoユニファイド コミュニケーション マネージャ バージョンに切り替えて、非推奨の電話機が登録できなくなると、新しい電話機のデバイス ライセンスが使用可能になります。

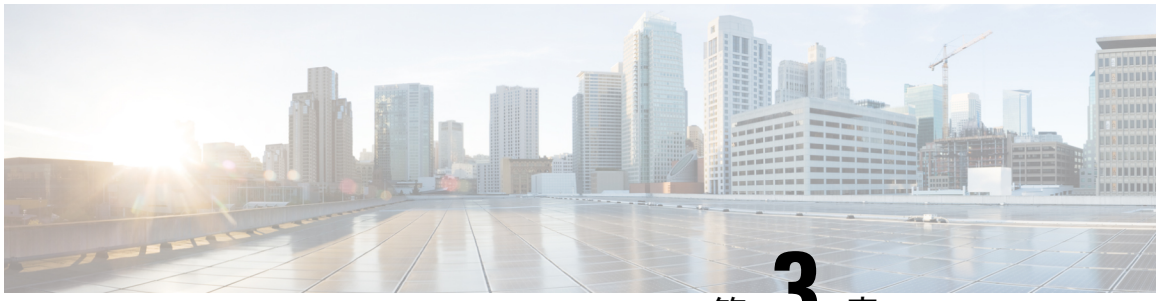
CLI によって開始される IM and Presence のアップグレードに必要な OS 管理者アカウント

utils system upgrade CLI コマンドを使用して、IM and Presence Service ノードをアップグレードする場合は、管理者権限を持つユーザではなく、デフォルト OS 管理者アカウントを使用する必要があります。デフォルト OS 管理者アカウントを使用しないと、必須のサービスをインストールするためにアップグレードに必要な特権レベルがなくなり、アップグレードが失敗する可能性があります。**show myself** CLI コマンドを実行すると、アカウントの特権レベルを確認できます。アカウントには特権レベル 4 が必要です。

この制限は、IM and Presence Service の CLI によって開始されるアップグレードにのみ適用され、ユニファイドコミュニケーションマネージャには適用されないことに注意してください。また、この制限は、新しい ISO ファイルでは修正される可能性があることに注意してください。特定の ISO ファイルの詳細については、ISO Readme ファイルを参照してください。この制限に関する最新情報については、https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb14399の CSCvb14399 を参照してください。

アップグレード時の Cisco Jabber

IM and Presence Service をアップグレードするときに、すべてのユーザが Cisco Jabber からログアウトする必要はありません。ただし、ベストプラクティスとしては、ユーザはアップグレード中に Cisco Jabber からログアウトします。



第 3 章

新機能および変更された機能

（注） この章では、このリリースの新機能および更新された機能について概要を説明します。次の機能は、リリース 11.5 (1) SU1 専用に新規または更新されています。

- APIC-EM コントローラ
- ダウンロード ファイル整合性チェックのチェックサム
- IM and Presence の一般的な基準
- 強化されたセキュリティ モード
- 最大セッション制限 CLI 更新
- ランク ベースのアクセス コントロール
- FileBeat を使用したプラットフォームログおよびリモートサポートログのリモート監査ロギング

この章に記載されているその他の機能は、リリース 11.5 (1) で追加されましたが、ここでも説明しています。

AXL 読み取りアクセス ロールのユーザへの追加

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 11.5 (1) 以降では、管理者は AXL (管理 XML 層) ユーザに読み取り専用アクセスロールを割り当てることができます。読み取り専用アクセス権を持つAXLユーザは、読み取り専用アプリケーションプログラミングインター

フェイス (API) のみを実行でき、システム更新に使用される Api を実行するためのアクセス権はありません。

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 11.5 (1) で導入された新しい標準アクセスロールを次に示します。

- 標準 AXL API ユーザ
- 標準 AXL 読み取り専用 API アクセス

アドミニストレーション ガイドの更新

ユーザ機能への AXL 読み取りアクセス権限の追加については、『*Cisco Unified Communications Manager* のアドミニストレーション ガイド』の次のトピックが更新されています。

標準権限とアクセス コントロール グループ

次のテーブルには、AXL ユーザの新しいフィールドが含まれています。

表 *5*:標準権限、特権 およびアクセス コントロール グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準AXL APIユーザ	AXL API を実行するログイン権限を付与します。	
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API（API の一覧表示、API の取得、SQL Query API の実行）の実行をデフォルトで許可します。	

APIC-EM コントローラ QoS サポート

APIC EM コントローラを使用して、SIP メディアフローのプライオリティ設定を管理することで、輻輳しているネットワークを軽減します。

このリリースでは、SIP プロファイル内の APIC EM コントローラのサポートを設定できるようになりました。この機能拡張により、ユーザグループの APIC EM コントローラ統合を有効または無効にできるため、ネットワーク QoS の管理が容易になります。たとえば、すべての Cisco Jabber エンドポイントが APIC EM を使用して SIP メディアフローを管理する一方で、すべての Cisco ユニファイド IP 電話 は Ciscoユニファイド コミュニケーション マネージャ 内部 QoS メカニズムを使用するように SIP プロファイルを設定できます。

SIP メディア フローの管理

APIC-EM を使用する SIP コールの場合、Cisco Unified Communications Manger はコールの始めに APIC-EM コントローラにポリシー要求を送信して、メディア フローの APIC-EM がセットアップ中であることを通知します。ポリシー要求にはコールに関する情報（送信元デバイスと宛先デバイスの IP アドレスとポート、フローのメディア タイプ、プロトコルなど）が含まれています。

APIC-EM は、関連付けられているメディア フローの DSCP 値をコール フローの先頭でスイッチに通知します。スイッチは、それらの DSCP 値を個別のメディア パケットに挿入して、エンドポイントで挿入される値を上書きします。コールフロー内のゲートウェイで輻輳が発生すると、そのゲートウェイでは DSCP 値が高い方のパケットが先に送信されます。そのため、優先順位が高い音声ストリームやビデオ ストリームが、電子メール、印刷ジョブ、ソフトウェア ダウンロードなどの優先順位の低いネットワーク トラフィックによってブロックされません。コールが終了すると、Ciscoユニファイド コミュニケーション マネージャ は APIC-EM に通知し、APIC-EM はフローの削除をスイッチに通知します。

コンフィギュレーション

APIC EM 統合の設定方法の詳細については、『 *System Configuration Guide for Cisco Unified Communications Manager, Release 11.5 (1) SU1* 』の「configure QOS with APIC-em Controller」を参照してください。

APIC-EM でのユーザ インターフェイスの更新

[**SIP プロファイルの設定 (SIP Profile Configuration)**] ウィンドウに次のチェックボックスが追加されました。

- **外部 QoS の有効化**—外部 QoS をサポートするために SIP プロファイルを使用するデバイスを設定するには、このチェックボックスをオンにします。この機能を有効にすると、APIC-EM コントローラを使用して、このデバイスからの SIP メディア フローの QoS を管理できます。

（注） このチェックボックスは、**[外部 QoS の有効化（Enable External QoS）]** サービス パラメータが **[はい（True）]** に設定されている場合にのみ表示されます。

[**HTTP プロファイル (HTTP Profile)**] ウィンドウには、次の4つのフィールドが追加されています。

- **ユーザ名**—HTTP サーバへのこの接続にユーザ名を割り当てます。このユーザ名は、対象の HTTP サーバで設定されているユーザ名と一致している必要があります。ユーザ名に関する制限については、対象の HTTP サーバのマニュアルを参照してください。

- **パスワード** - この接続にパスワードを割り当てます。HTTP サーバで設定されているパスワードと同じものを設定する必要があります。許容される文字などのパスワードに関する制限については、対象の HTTP サーバのマニュアルを参照してください。
- **タイムアウトのリクエスト** - このタイマーは、Ciscoユニファイド コミュニケーション マネージャ が要求を HTTP サーバに送信した後に Ciscoユニファイド コミュニケーション マネージャ が応答を待機する最大時間をミリ秒単位で指定します。
- **[最大要求再試行回数（Maximum Request Retries）]** - [要求タイムアウト（Request Timeout）] タイマーが時間切れになった場合に Ciscoユニファイド コミュニケーション マネージャ が要求を再送信する最大回数を指定します。

（注） [**HTTP Profile**] フィールドは 11.5 (1) ユーザインターフェイスに表示されますが、使用するには、少なくとも 11.5 (1) SU1 がインストールされている必要があります。

APIC-EM コントローラの新しいアラーム

11.5 (1) SU1 リリースでは、次のアラームが APIC EM コントローラのサポートに追加されました。

- **ExternalQoSTokenUnavailable**: このエラーアラームは、Ciscoユニファイド コミュニケーション マネージャ が APIC EM コントローラとの接続に失敗したときに生成されます。これは、認証やネットワークエラーが発生した場合など、アクセストークンが APIC EM コントローラから使用できない場合に発生する可能性があります。

  エラーを解決するには、[**HTTP プロファイル (HTTP Profile**)] ウィンドウのユーザ名とパスワードが、APIC EM で設定されているポリシー管理クレデンシャルと一致することを修正します。問題が修正されたら、[**External QoS Enabled**] サービスパラメータを [**False**] に切り替えてから [**True**] に戻すことによって、新しい接続試行を開始します。

- [**ExternalQoSTokenAvailable**]: この情報アラームは、Ciscoユニファイド コミュニケーション マネージャ が APIC EM コントローラから有効なアクセストークンを取得できたことを確認するために生成されます。アラームは、 **ExternalQoSTokenUnavailable**アラームが最初に生成された場合にのみ生成されます。

  このアラームにはアクションは必要ありません。

APIC EM の通信の更新

起動時に、またはサービスパラメータを設定すると、Ciscoユニファイド コミュニケーション マネージャ はサービスチケット要求を送信して、APIC EM からアクセストークンを取得します。APIC EM から新しいトークンを受信した後、Ciscoユニファイド コミュニケーション マネージャ はすべてのノースバウンド REST API を使用してトークンを送信し、要求が承認されたユーザからのものであることを検証します。ユーザ名またはパスワードが変更された場合、

またはサービスパラメータが**False**に切り替えられて**True**になった場合、Ciscoユニファイド コミュニケーション マネージャ は新しいトークンを要求します。

APIC EM の開発者マニュアルについては、https://developer.cisco.com/site/apic-em/を参照してください。

アプリケーション向けの認証セキュリティ

リリース 11.5(1) 以降では、管理者は、ウェブブラウザを使用して AXL などの API サービスに接続するときに、フォームベースの認証を使用するようにシステムを設定できるようになりました。この更新により、より安全な認証方式を提供することによって、アプリケーションのセキュリティが向上します。以前は、ブラウザがユーザのログイン情報をキャッシュできるようにする**基本認証**が、ブラウザを介してアクセス可能なすべての API サービスに使用されていました。この更新を処理するために、管理者が認証方式を設定できるように、新しいエンタープライズパラメータである、**API ブラウザアクセス用の認証方式**が追加されました。管理者は、次のオプションから選択できます。

- 基本: アプリケーションにサインインするユーザは、ブラウザのサインインプロンプトで自身を認証する必要があります。これがデフォルトのオプションです。
- フォームベース: アプリケーションにサインインするユーザは、フォームベースのサインインページにリダイレクトされます。フォームベースの認証は、基本認証よりも安全性が高くなります。

（注） この変更は、フォームベースの認証を使用してすでに動作しているウェブベースのアプリケーションには影響しません。

コール保持期間の管理

[クラスタ全体のパラメータ (デバイス-SIP) (Clusterwide Parameters (Device-SIP))] サービスエリアの下の [**サービスパラメータ設定 (Service Parameter Configuration)**] ウィンドウに、**SIP コール保持期限タイマー**と呼ばれる新しいサービスパラメータが追加されました。このパラメータは、コールの保持状態でコールがアクティブな状態でいる秒数を指定します。デフォルト値は 0 です。この機能を有効にするには、1-86400 の範囲内でこのサービスパラメータを設定する必要があります。デフォルト値を保持することを選択した場合は、電話が切断されるまで、またはデバイスがメディア接続が解放されたと判断するまで、コールは保持されます。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

この機能の使用例を次に示します。

- 回線間コール: コールマネージャがピアエンドとの通信を失った場合、SIP レイヤは存続中のレッグの保持タイマーを開始し、期限が切れた時点でレッグを切断します。

- SIP トランク経由のコール: sip トランクが宛先との通信を失った場合、SIP レイヤは存続中のレッグの保持タイマーを開始し、期限が切れた時点でレッグを切断します。
- 電話ベースの録音を有効にしたコール:録音レッグが保存に移行すると、SIP レイヤは録音レッグの保持タイマーを開始し、期限が切れるとレッグを切断します。
- ゲートウェイ録音を有効にしたコール:録音レッグが保存に移行すると、SIP レイヤは録音レッグの保持タイマーを開始し、期限切れになるとレッグを切断します。

（注） コールのコール処理を処理する Ciscoユニファイド コミュニケーション マネージャ ノードがコールの両方のデバイス/レッグとの接続を失った場合、SIP コール保持期限切れタイマーは効果がありません。

Cisco エンドポイント

Cisco IP 電話

電話機ファームウェアのバージョン

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 11.5 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 *6*: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) SR2
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)SR2
Cisco IP 電話 7800 シリーズ	11.5(1)
Cisco Unified IP 電話 7900 シリーズ	9.4 (2) SR1
Cisco Unified ワイヤレス IP 電話 7925G、7925G-EX および 7926G	1.4 (8)
Cisco IP 電話 8800 シリーズ	11.5(1)
Cisco Unified IP 会議用電話 8831	10.3 (1) SR2
Cisco Unified IP 電話 8941/8945	9.4 (2) SR2

電話ファミリ	ファームウェア リリース番号
Cisco Unified IP 電話 8961、9951 および 9971	9.4(2)SR2

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の電話ドキュメンテーション

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ユニファイド コミュニケーション マネージャ 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。ウェブ 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ユニファイド コミュニケーション マネージャ 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ユニファイド コミュニケーション マネージャ 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 Web 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 web 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。

非推奨のエンドポイント

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

Ciscoユニファイドコミュニケーションマネージャ の過去のリリースで、これらの電話機モデルのいずれかを使用しており、リリース 11.5 にアップグレードした場合、使用していた電話機は、アップグレード完了後に機能しなくなります。

Cisco Unified SIP 電話 3905

次の表に、ファームウェア リリース 9.4 (1) SR2 用に Cisco Unified SIP 電話 3905 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-sip-phone-3900-series/products-release-notes-list.html

機能名	ファームウェア リリース
回線テキスト ラベル	9.4(1)SR2

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 11.0 (1) および 11.5 (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

電話機のファームウェアリリース11.5 は、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11.5 には組み込まれていません。電話機のファームウェアは、Cisco.com からダウンロードして個別にインストールする必要があります。

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には、ファームウェアリリース11.0 の*CISCO IP* 電話 *7800* シリーズユーザガイドが含まれています。ファームウェアリリース11.5 のユーザガイドについては、 http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-user-guide-list.htmlを参照してください。

機能名	ファームウェア リリース
割り込み拡張	11.5(1)
遅延アップグレード	11.5(1)
[発着信履歴（Recents）] の無効化ソフトキー	11.5(1)
強化されたデバッグオプション	11.0(1)
外部ダイヤルトーン	11.5(1)

機能名	ファームウェア リリース
FIPS 140-2 レベル 1 のサポート	11.5(1)
Expressway 経由でのモバイルおよびRemote Access	11.0(1)
Opus オーディオコーデック	11.5(1)
問題レポート ツール	11.0(1)

Cisco Unified IP 電話 7900 シリーズの機能

次の表に、ファームウェアリリース 9.4 (2) SR1 のCisco Unified IP 電話 7900 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-7900-series/products-release-notes-list.html

機能名	ファームウェア リリース
設定可能なデフォルトのオーディオパス	9.4 (2) SR1

Cisco Unified ワイヤレス IP 電話 7925G、7925G-EX および 7926G の機能

次の表に、ファームウェアリリース 1.4 (8) の Cisco Unified ワイヤレス IP 電話 7925G、7925G-EX および 7926G 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-7900-series/products-release-notes-list.html

機能名	ファームウェア リリース
ワイヤレス チャネルの更新	1.4 (8)

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 10.3 (2)、11.0 (1) および 11.5 (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

電話機のファームウェアリリース11.5 は、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11.5 には組み込まれていません。電話機のファームウェアは、Cisco.com からダウンロードして個別にインストールする必要があります。

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には、ファームウェア リリース11.0 の*CISCO IP 電話 8800 シリーズ ユーザ ガイド*が含まれています。ファームウェア リリース11.5 のユーザガイドについては、 http://www.cisco.com/c/en/us/support/

collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.htmlを参照してください。

機能名	ファームウェア リリース
アプリケーション ダイヤル ルール	11.0(1)
Visual Voicemail からのボイスメール サービスへのアクセス	11.0(1)
Cisco IP 電話 8800 シリーズの割り込みの機能拡張	11.0(1)
Cisco IP Phone 8845 および 8865	10.3 (2)
遅延アップグレード	11.5(1)
強化されたデバッグオプション	11.0(1)
応答不可の強化	11.5(1)
[拡張回線モード（Enhanced Line Mode）]	11.5(1)
外部ダイヤルトーン	11.5(1)
FIPS 140-2 レベル 1 のサポート	11.5(1)
Expressway 経由でのモバイルおよびRemote Access	11.0(1)
Opus オーディオコーデック	11.5(1)
問題レポート ツール	11.0(1)
ユーザ インターフェイスの強化。	11.0(1)
Wi-Fi セキュリティの強化	11.5(1)
Cisco IP 電話 8861 および 8865 用の WLAN プロファイル	11.5(1)
EAP-TLS、SCEP、PEAP-GTC の X.509 デジタル 証明書サポート	11.0(1)

Cisco Unified IP Conference Station 8831 の機能

次の表に、ファームウェアリリース 10.3 (1) SR2 の Cisco Unified IP Conference Station 8831 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
ダウングレードが無効	10.3 (1) SR2
HTTPS サポート	10.3 (1) SR2

Cisco Unified IP 電話 8941 および 8945 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 Desktop Collaboration シリーズ

Cisco DX650、DX70 および DX80 ファームウェア

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 11.5 でサポートされている最新の Cisco DX シリーズファームウェアバージョンを示します。

デバイス	ファームウェア
Cisco DX650	10.2 (5) SR2
Cisco DX70	10.2(5)SR2
Cisco DX80	10.2(5)SR2

Cisco DX650、DX70 および DX80 の機能

次の表に、ファームウェアリリース 10.2 (5) の Cisco DX 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/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

機能名	ファームウェア リリース
[コールの統計（Call Statistics）] へのアクセス	10.2 (5)
代替電話帳サーバ	10.2 (5)
問題レポートの自動アップロード	10.2 (5)
信頼リストの更新	10.2 (5)
連絡先検索	10.2 (5)
デフォルトの壁紙 (DX650 のみ)	10.2 (5)

機能名	ファームウェア リリース
FIPS Mode	10.2 (5)
HDMI オーディオ	10.2 (5)
設定のパスワード保護	10.2(5)
SIP URI	10.2(5)
PC モードのまま	10.2 (5)
No Radio Hardware (CP-DX70-K9 = および CP-DX80-NR-K9 =) のサポート	10.2 (5)
発信コールの呼び出し中にシステムを使用する	10.2 (5)

CLI 権限レベル

Ciscoユニファイド コミュニケーション マネージャ のインストール中に、権限レベル 4 の管理者がプラットフォーム レベルで作成されます。この管理者は、すべてのコマンド ライン インターフェイス（CLI）コマンドを実行する権限を持ちます。権限レベル 4 の管理者は、CLI コマンドを使用して次の管理者を作成します。

- 権限レベル 0 の管理者：この管理者はインターフェイス上で読み取り専用のアクセス権限を持ちます。
- 権限レベル 1 の管理者：この管理者はインターフェイス上で読み取りおよび書き込み両方のアクセス権限を持ちます。

（注） 管理者はそれぞれに対して定義された権限に基づいて CLI コマンドを実行できます。

CLI リファレンス ガイドの更新

Cisco Unified Communications ソリューションの *CLI* リファレンスガイドでは、次の CLI コマンドの特権レベルが変更されています。

- **show accountlocking**
- **show session maxlimit**
- **show csr own name**
- **show csr list type**
- **show password change-at-loginuserid**

- **show cli session timeout**
- **show process using-most memory**
- **show tech all**
- **show open files all**
- **show open files process**
- **show open files regexp**
- **show open ports all**
- **show open ports regexp**
- **set account name**
- **set account enable**
- **set accountlocking count**
- **set logging enable**
- **set logging disable**
- **set workingdir activelog**
- **set workingdir inactivelog**
- **set password inactivity enable**
- **set password inactivity disable**
- **set password inactivity period**
- **set network max_ip_conntrack**
- **set network cluster publisher hostname**
- **set network cluster publisher ip**
- **delete account**
- **delete dscp**
- **file list activelog**
- **file list inactivelog**
- **file list install**
- **file list salog**
- **file list partBsalog**
- **file list tftp**
- **file view system-management-log**
- **file dump sftpdetails**
- **file dump activelog**

- **file dump inactivelog**
- **file dump tftp**
- **utils ldap config ipaddr**
- **utils ldap config fqdn**
- **utils ldap config status**
- **utils diagnose version**
- **utils diagnose list**
- **utils diagnose test**
- **utils diagnose fix**
- **utils diagnose module**
- **utils firewall ipv6 enable**
- **utils firewall ipv6 disable**
- **utils iothrottle enable**
- **utils iothrottle disable**
- **utils iothrottle status**
- **utils service list**
- **utils system upgrade status**

上記の 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『*Cisco Unified Communications Solutions* の *CLI* 参照ガイド』を参照してください。

SHA1_80 での会議の暗号化

このリリースでは、Ciscoユニファイドコミュニケーションマネージャが会議メディアのSRTP暗号化のAES_CM_128_HMAC_SHA1_80暗号をサポートするようになりました。暗号化はSIP電話でサポートされており、次のような場合に自動的にネゴシエートされます。

- **Cisco IOS Enhanced 会議ブリッジ**の会議ブリッジタイプが Ciscoユニファイド コミュニケーション マネージャ に割り当てられます。
- SIP 電話は暗号をサポートしています。
- ISR4000シリーズゲートウェイは、暗号をサポートする負荷とともに導入されます。最新のロードの詳細については、ゲートウェイのマニュアルを参照してください。

会議のすべてのデバイスが AES_CM_128_HMAC_SHA1_80 をサポートしている場合は、信頼されたリレーポイントがメディアパスに割り当てられているかどうかに関係なく、すべての電話に対して暗号が自動的にネゴシエートされます。コールにSCCP電話機またはサポートされ

ていない SIP 電話機も含まれている場合、サポートされていない電話機のコールレッグは AES_CM_128_HMAC_SHA1_32 にフォールバックします。

エンドツーエンド セッション ID 用 CTI サポート

Cisco Unified Communications Managerのリリース 11.5 (1) では、コールのエンドツーエンドセッション ID に CTI サポートが追加されています。エンドツーエンドセッション ID を使用すると、 Cisco Unified Communications Managerは、1つの一意の識別子でコールのエンドツーエンドを追跡できます。以前は、この機能は SIP でのみサポートされていました。この CTI アップデートでは、CTI および SIP には、コールの共通セッション ID があります。

コールのエンドツーエンドセッション ID の CTI 実装の詳細については、『 「Cisco Unified Communications Manager 向け Cisco Unified JTAPI 開発者ガイド』」の「新機能および変更された情報」の章を参照してください。

Cisco Mobile およびRemote Access クライアントとエンドポイントのディレクトリ サーバ ユーザ検索

以前のリリースでは、Cisco Mobile とRemote Access クライアント（たとえば、Cisco Jabber）またはエンドポイント（たとえば、Cisco DX 80 電話）を使用しているユーザが企業ファイアウォールの外部でユーザ検索を実行した場合、結果は Ciscoユニファイド コミュニケーション マネージャ に保存されたユーザ アカウントに基づいていました。データベースには、ローカルで設定されたか、または社内ディレクトリから同期されたユーザアカウントも含まれています。

このリリースでは、Cisco MobileおよびRemote Access クライアントとエンドポイントは、企業ファイアウォールの外部で動作している場合でも、社内ディレクトリ サーバを検索できます。この機能を有効にすると、ユーザ データ サービス（UDS）がプロキシとして機能し、Ciscoユニファイド コミュニケーション マネージャ データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

この機能を使用して、次の結果を実現できます。

- 地理的な場所に関係なく、同じユーザ検索結果を提供する：モバイルおよびRemote Access クライアントとエンドポイントは、社内ディレクトリを使用してユーザ検索を実行できます。企業ファイアウォールの外部で接続されている場合でも実行可能です。
- Ciscoユニファイドコミュニケーションマネージャ データベースに設定されるユーザアカウントの数を削減する：モバイルクライアントは、社内ディレクトリ内のユーザを検索できます。以前のリリースでは、ユーザ検索結果はデータベースに設定されているユーザに基づいていました。今回のリリースでは、ユーザ検索のためだけにユーザ アカウントをデータベースに設定または同期する必要がなくなりました。管理者は、クラスタによって管理されているユーザアカウントを設定すれば作業が完了します。データベース内のユー

ザアカウントの合計数が削減すると、データベース全体のパフォーマンスが改善される一方、ソフトウェア アップグレードの時間枠が短縮されます。

この機能を設定するには、[LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで [企業ディレクトリ サーバでのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] オプションを有効にし、LDAP ディレクトリ サーバの詳細を設定する必要があります。詳細については、エンタープライズ ディレクトリ ユーザ検索の設定 （29 ページ）の手順を参照してください。

システム設定の更新

『 *System Configuration Guide for Cisco Unified Communications Manager* 』は、次の新しいトピックで更新され、Cisco モバイルおよびリモートアクセス クライアントおよびエンドポイントのディレクトリサーバのユーザ検索機能について説明しています。

- [Configure Enterprise Directory Server User Search]: エンタープライズ ディレクトリ サーバのユーザ検索用にシステムを設定する方法について説明します。
- [LDAP 属性 for UDS Search of Directory Server]: ユーザがエンタープライズ ディレクトリ サーバに対して検索するための UDS と LDAP 属性のマッピングを表示します。このようなタイプの検索要求の場合、UDS はプロキシとして機能して、社内ディレクトリ サーバに LDAP 要求をリレーします。

エンタープライズ ディレクトリ ユーザ検索の設定

データベースではなくエンタープライズ ディレクトリ サーバに対してユーザ検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

始める前に

- LDAP ユーザ検索に選択するプライマリ、セカンダリ および第 3 サーバが Unified Communications Manager のサブスクライバ ノードに到達可能なネットワークにあることを確認します。
- **システム > LDAP > LDAP システム**から、**LDAP システム設定** ウィンドウを開き、**LDAP サーバ タイプ** ドロップダウン リスト から LDAP のタイプを設定します。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [LDAP] > [LDAP 検索（LDAP Search）]** を選択します。

ステップ 2 エンタープライズLDAPディレクトリ サーバを使用してユーザ検索を実行するには、[エンタープライズディレクトリ サーバのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] チェックボックスをオンにします。

ステップ 3 [LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

ディレクトリ サーバの UDS 検索用の LDAP 属性

次の表に、[エンタープライズ ディレクトリ サーバに対するユーザ検索を有効化（Enable user search to Enterprise Directory Server）] オプションが有効になっている場合に、UDS ユーザ検索要求で使用される LDAP 属性の一覧を示します。このようなタイプのディレクトリ要求の場合、UDS はプロキシとして機能して、社内ディレクトリ サーバに検索要求をリレーします。

（注） UDS ユーザの応答タグは、いずれかの LDAP 属性にマッピングされることがあります。属性のマッピングは、[LDAP サーバ タイプ（LDAP Server Type）] ドロップダウン リストから選択するオプションによって決まります。このドロップダウン リストには、**[システム（System）]** > **[LDAP]** > **[LDAP システムの設定（LDAP System Configuration）]** ウィンドウからアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	メール アドレス
directoryUri	• msRTCSIP-primaryuseraddress • mail

UDS ユーザの応答タグ	LDAP 属性
部署	• 部署 • departmentNumber
manager	manager
タイトル	タイトル
ポケットベル	ポケットベル

LDAP 検索用のユーザ インタフェースの更新

このリリースでは、[**LDAP 検索設定 (LDAP Search Configuration)**] ウィンドウが追加されました。このウィンドウにアクセスするには、[Cisco Unified CM Administration] から [**システム (System)** > **LDAP** > **LDAP 検索 (LDAP Search)**] を選択します。

[**LDAP 検索設定 (LDAP Search Configuration)**] ウィンドウを使用して、企業内のすべてのエンドポイントと Cisco モバイルおよびリモートアクセス クライアントを設定し、エンタープライ イズディレクトリ サーバに対してユーザ検索を実行します (企業のファイアウォールの外部で動作している場合でも)。

この設定ウィンドウで使用可能なフィールドオプションについて説明するために、*Cisco Unified CM Administration* オンラインヘルプに次のトピックが追加されています。

LDAP 検索の設定項目

表 *7 : LDAP* 検索の設定項目

フィールド	説明
UDS 経由のエンタープライズ ユーザ用 LDAP 検索	
エンタープライズ ディレクトリ サーバのユーザ検索を有効化(Enable user search to Enterprise Directory Server)	LDAP 検索を有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[LDAP 検索設定（LDAP Search Configuration）]** ウィンドウのすべてのフィールドがアクティブになります。 既存の LDAP 検索を無効にするには、このチェックボックスをオフにして、**[保存（Save）]** をクリックします。 （注） このチェックボックスをオフにすると、**[LDAP 検索設定（LDAP Search Configuration）]** ウィンドウのすべてのフィールドが編集不可になります。

フィールド	説明
LDAP マネージャ識別名（LDAP Manager Distinguished Name）	ディレクトリ サービスのエントリに一意の名前を入力します。
LDAP パスワード（LDAP Password）	LDAP サーバにアクセスするためのパスワードを入力します。
Confirm Password	**[LDAP パスワード（LDAP Password）]** フィールドに入力したのと同じパスワードを入力します。
LDAP ユーザ検索ベース 1(LDAP User Search Base 1)	最初の検索ベースに LDAP ユーザ検索の値を入力します。たとえば、**cn=users,dc=citglab,dc=india,dc=com** のような検索ベース値を入力します。 （注） このフィールドは必須です。
LDAP ユーザ検索ベース 2(LDAP User Search Base 2)	（オプション）2 番目の検索ベースに LDAP ユーザ検索の値を入力します。 （注） 最初の検索ベースでユーザ情報が見つからなかった場合は、この検索ベースに値を入力できます。
LDAP ユーザ検索ベース 3	（オプション）3 番目の検索ベースに LDAP ユーザ検索の値を入力します。 （注） 1 番目と 2 番目の検索ベースでユーザ情報が見つからなかった場合は、この検索ベースに値を入力できます。
ユーザの LDAP カスタム フィルタ	このドロップダウン リストから、ユーザの検索条件としてフィルタ オプションの 1 つを選択します。ドロップダウンリストに表示されるオプションは、**[LDAP カスタム検索フィルタ（LDAP Custom Search Filter）]** ウィンドウで定義します。
Recursive Search on All Search Bases	このチェックボックスをオンにして、2 番目と 3 番目の検索ベースからもユーザ情報を検索するように指定します。デフォルトでは、最初の検索ベースのみで情報が検索されます。**[すべての検索ベースで再帰検索を実行する（Recursive Search on All Search Bases）]** チェックボックスをオンにすると、最初の検索ベースでユーザ情報が見つからなかった場合に、引き続き 2 番目と 3 番目の検索ベースでもユーザ情報が検索されます。

フィールド	説明
UDS Tagを LDAP に属性マッピング 次の UDS タグの LDAP 属性を表示または選択します。	
userName	属性名が **sAMAccountName** として表示されます。
firstName	属性名が **givenName** として表示されます。
middleName	次のいずれかの属性を選択します。 • **middleName** • **initials**
lastName	属性名が **sn** として表示されます。
manager	属性名が **manager** として表示されます。
部門	次のいずれかの属性を選択します。 • **部門** • **departmentNumber**
phoneNumber	次のいずれかの属性を選択します。 • **telephone** • **ipPhone**
電子メール	属性名が **mail** として表示されます。
title	属性名が **title** として表示されます。
homeNumber	属性名が **homephone** として表示されます。
mobileNumber	属性名が **mobile** として表示されます。
pager	属性名が **pager** として表示されます。
directoryUri	次のいずれかの属性を選択します。 • **msRTCSIP-primaryuseraddress** • **メール アドレス** • **none**
displayName	属性名が **displayName** として表示されます。
UC サービス ディレクトリ情報	

フィールド	説明
Primary Server	ドロップダウンリストから、LDAP検索用の既存のユニファイドコミュニケーション（UC）サービスの1つを選択します。ドロップダウン リストからUCサービスを選択すると、**[サーバのホスト名またはIPアドレス（Host Name or IP address of Server）]**、**[ポート番号（Port Number）]** および **[プロトコル（Protocol）]** 列にIPアドレスの詳細が表示されます。さらに **[詳細の表示（View Details）]** リンクが表示されます。このリンクをクリックすると、選択したUCサービスの設定の詳細が表示されます。 選択しようとしているUCサービスがドロップダウンリストにリストされていない場合は、新しいUCサービスを作成できます。新しいUCサービスを追加するには、**[UCサービスの追加（Add UC Service）]** ボタンをクリックします。新しく追加したUC サービスが **[プライマリ サーバ（Primary Server）]** ドロップダウン リストに表示されます。 （注） このフィールドは必須です。
Secondary Server	（オプション）ドロップダウンリストから、LDAP検索用の既存のUC サービスの1つを選択します。ドロップダウンリストからUCサービスを選択すると、**[サーバのホスト名またはIPアドレス（Host Name or IP address of Server）]**、**[ポート番号（Port Number）]** および **[プロトコル（Protocol）]** 列にIPアドレスの詳細が表示されます。さらに **[詳細の表示（View Details）]** リンクが表示されます。このリンクをクリックすると、選択したUCサービスの設定の詳細が表示されます。 選択しようとしているUCサービスがドロップダウンリストにリストされていない場合は、新しいUCサービスを作成できます。新しいUCサービスを追加するには、**[UCサービスの追加（Add UC Service）]** ボタンをクリックします。新しく追加したUC サービスが **[セカンダリ サーバ（Secondary Server）]** ドロップダウン リストに表示されます。

フィールド	説明
ターシャリ サーバ（Tertiary Server）	（オプション）ドロップダウン リストから、LDAP 検索用の既存の UC サービスの 1 つを選択します。ドロップダウン リストから UC サービスを選択すると、**[サーバのホスト名またはIPアドレス（Host Name or IP address of Server）]**、**[ポート番号（Port Number）]** および **[プロトコル（Protocol）]** 列に IP アドレスの詳細が表示されます。さらに **[詳細の表示（View Details）]** リンクが表示されます。このリンクをクリックすると、選択した UC サービスの設定の詳細が表示されます。 選択しようとしている UC サービスがドロップダウン リストにリストされていない場合は、新しい UC サービスを作成できます。新しい UC サービスを追加するには、**[UCサービスの追加（Add UC Service）]** ボタンをクリックします。新しく追加した UC サービスが **[ターシャリ サーバ（Tertiary Server）]** ドロップダウン リストに表示されます。
UC サービスの追加	プライマリ、セカンダリ およびターシャリ ディレクトリ サーバを設定するには、このボタンをクリックします。**[UC サービスの設定（UC Service Configuration）]** ウィンドウで必須フィールドに値を入力します。このウィンドウで入力した値は、**[プライマリ サーバ（Primary Server）]**、**[セカンダリ サーバ（Secondary Server）]** および **[ターシャリ サーバ（Tertiary Server）]** フィールドに UC サービスとして表示されます。 UC サービスの設定フィールドの詳細については、オンライン ヘルプの「*UC* サービスの設定」セクションを参照してください。

（注） LDAP ユーザ検索用に選択したプライマリ、セカンダリ およびターシャリ サーバが Ciscoユニファイド コミュニケーション マネージャ サブスクライバー ノードにネットワーク経由で接続されていない場合は、**[LDAP 検索設定（LDAP Search Configuration）]** ウィンドウで値を保存した後、各サーバの接続ステータスとして「失敗（failed）」が表示されます。Ciscoユニファイド コミュニケーション マネージャ サブスクライバー ノードにネットワーク経由で接続されたサーバの IP アドレスが設定されている UC サービスを選択すると、この設定のステータスが「成功（successful）」になります。

ディレクトリ サーバ サポート

このリリースでは、Ciscoユニファイド コミュニケーション マネージャ を次の LDAP ディレクトリと統合できます。これらのディレクトリはユーザ アカウントの同期と認証をサポートされています。

- Microsoft Active Directory 2008 R1/R2
- Microsoft Active Directory 2012 R1/R2
- Microsoft Lightweight Directory Services 2008 R1/R2
- Microsoft Lightweight Directory Services 2012 R1/R2
- Oracle ディレクトリ サービス企業版 11gR1 (11.1.1.7.x 以降)
- Oracle Unified ディレクトリ 11gR2 (11.1.2.2.0 または 11.1.2.3.0)
- OpenLDAP 2.4.40 以降

ユニファイド コミュニケーション セルフケア ポータルを使用した名前設定の表示

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11.5 のユニファイド コミュニケーション セルフケアポータルを使用して、ユーザ ID ではなく他のユーザに表示される表示名を変更します。

この機能は、ユニファイド コミュニケーション セルフケ アポータルに表示される **[表示名 (Display Name)]** フィールドによって処理されます。このフィールドは、次のユーザとしてログインすると動作が変化します。

- ローカル ユーザ：Lightweight Directory Access Protocol（LDAP）で同期していないローカル ユーザとしてログインした場合、[表示名（Display Name）] フィールドで表示名を変更できます。
- LDAP 同期ユーザ：LDAP 同期ユーザとしてログインすると、[表示名（Display Name）] フィールドは、編集不能になります。

表示名の表示と変更

Lightweight Directory Access Protocol（LDAP）で同期していないローカル ユーザとしてログインした場合、次の手順を使用して、表示名を表示したり変更したりできます。

（注） ユニファイド コミュニケーション セルフ ケア ポータルにログインすると、アプリケーションからログアウトするためのリンクに、表示名が表示されます（すでに構成されている場合）。構成されていない場合は、ログアウトのリンクにはユーザ ID が表示されます。

手順

ステップ 1 ユニファイド コミュニケーション セルフ ケア ポータルから、[一般設定（General Settings）] タブをクリックします。

ステップ 2 [表示名（Display Name）] をクリックします。
[表示名（Display Name）] テキスト ボックスが表示されます。

ステップ 3 [表示名（Display Name）] テキスト ボックスには、他のユーザに対して自分のユーザ ID 以外の名前を表示する場合に、その表示名前を入力します。

（注）
- 以前に表示名を構成していた場合、このフィールドには構成されているその名前が自動的に表示されます。
- LDAP 同期ユーザとしてログインする場合、表示名は編集不能となるため、このフィールドのための [保存（Save）] と [キャンセル（Cancel）] ボタンは表示されません。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 （オプション）以前に構成されていた表示名に戻すには、[キャンセル（Cancel）] をクリックします。

CTI でハント ログ ステータスを有効にする

Ciscoユニファイド コミュニケーション マネージャ のリリース 11.5(1) では、アプリケーションを介して、サインインしたり、ハントグループからサインアウトしたりできるようになりました。以前は、この機能は Cisco Unified CM の管理インターフェイスからのみ使用できました。この機能の使用例を次に示します。

- アプリケーションを使用して、ハントグループから電話機にサインインしてサインアウトすることができます。
- ハントグループのログオンステータスが変更されるたびに、通知が表示されます。

ハントログのステータスを有効にする方法の詳細については、Ciscoユニファイド コミュニケーション マネージャ の『 *Cisco Unified JTAPI AND TAPI* 開発者ガイド』の「新機能および変更された情報」の章を参照してください 。

tomcat インターフェイスでの EC 暗号

Tomcatインターフェイスの楕円曲線（EC）暗号はデフォルトで無効になっています。Ciscoユニファイド コミュニケーション マネージャ または IM and Presence Service で [HTTPS 暗号（HTTPS Ciphers）] のエンタープライズパラメータを使用して、これらを有効にできます。このパラメータを変更すると、すべてのノードで Cisco Tomcat サービスを再起動する必要があります。

ILS 証明書管理の強化

リリース 11.5(1) では、管理者は TLS 認証とパスワードベースの認証を同時に使用して ILS ネットワークをセットアップすることが可能です。このとき、クラスタ間の自己署名証明書を交換するのではなく、共通の認証局（CA）の署名がある証明書を使用します。クラスタ間で Transport Layer Security（TLS）認証とパスワード認証を使用するには、認証局のルート証明書を tomcat-trust にアップロードして、認証局のルート証明書の署名がある Tomcat 証明書をすべてのクラスタに対して取得する必要があります。その証明書は同じクラスタにインポートされます。証明書がすべてのクラスタに同じパスワードでアップロードされると、クラスタは、クラスタ間検索サービス（ILS）ネットワークに接続できます。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_0_1/sysConfig/CUCM_BK_C733E983_00_cucm-system-configuration-guide.html）の「「Configure Intercluster Lookup Service」」の章を参照してください。

強化されたセキュリティの更新

次の拡張セキュリティアップデートが追加されました。

- 強化されたセキュリティ モード （39 ページ）: より厳格なクレデンシャルポリシーなどの一連のリスク管理制御をシステムで有効にする新しいシステム実行モード。
- 連絡先検索認証。 （40 ページ）: この機能を有効にすると、ユーザは会社のディレクトリを使用するために認証を受ける必要があります。
- 監査ログの更新 （40 ページ）: 監査ログフレームワークは、リモート監査ログの転送プロトコルオプションとして TCP を含むように更新されました。以前は、UDP だけが提供されていました。詳細な監査ロギングオプションを使用して、設定の変更をデータベースに記録することができるようになりました。さらに、プラットフォーム監査ログ、リモートサポートログ および一括管理 csv ファイルに対して、FileBeat を使用したリモートロギングが提供されるようになりました。
- SHA-512 デジタル署名サポート （42 ページ）: システムは、デジタル署名のために SHA-512 をサポートするようになりました。

- ランク ベースのアクセス コントロール（43 ページ）:既存のアクセスコントロールグループフレームワークをオーバーレイする、新しいユーザランクベースのアクセス制御セット。
- ファイル整合性チェックの SHA-512 チェックサム （44 ページ）: すべてのファイルダウンロードに SHA512 チェックサムを使用できます。
- 最大セッション制限 CLI 更新 （44 ページ）—すべてのインターフェイスに適用します。

強化されたセキュリティモードを設定するには、強化されたセキュリティ設定のタスク フロー（44 ページ）に進みます。

強化されたセキュリティ モード

強化されたセキュリティ モードは FIPS 対応システムで稼働します。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 サービス の両方を、強化されたセキュリティ モードで動作するようにすることができます。これにより、次のセキュリティおよびリスク管理制御機能をシステムで実現できます。

- ユーザのパスワードとパスワードの変更に関して厳格化されたクレデンシャル ポリシーが適用されます。
- デフォルトでは、連絡先検索の認証機能が有効です。
-

クレデンシャル ポリシーの更新

強化されたセキュリティ モードを有効にすると、新しいユーザ パスワードとパスワード変更に関してより厳格なクレデンシャル ポリシーが有効になります。強化されたセキュリティ モードを有効にした後で、管理者は一連の CLI コマンド **set password ***** を使用して、次の要件のいずれかを変更できます。

- パスワードの長さは 14 ～ 127 文字です。
- パスワードには少なくとも 1 つの小文字、1 つの大文字、1 つの数字 および 1 つの特殊文字が含まれている必要があります。
- 過去 24 回以内に使用したパスワードを再使用することはできません。
- パスワードの最短有効期間は 1 日、最長有効期間は 60 日です。
- 新たに生成されるパスワードの文字列では、古いパスワードの文字列と少なくとも 4 文字が異なる必要があります。

CLI コマンドの更新

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 Presemce サービスの拡張セキュリティモードを設定するには、次の CLI コマンドを追加します。

- **utils EnhancedSecurityMode enable**—このコマンドを実行して強化されたセキュリティ モードのクラスタ ノードを有効にします。このコマンドをすべてのノードで同時に実行しないでください。
- **utils EnhancedSecurityMode enable**—このコマンドを実行して強化されたセキュリティ モードのクラスタ ノードを無効にします。このコマンドをすべてのノードで同時に実行しないでください。
- **utils EnhancedSecurityMode status**ーこのコマンドを実行し、強化されたセキュリティ モードが有効であるかどうかを確認します。

連絡先検索認証。

このリリースでは、連絡先検索認証機能がCiscoユニファイド コミュニケーション マネージャに追加されています。この機能は、ユーザが会社のディレクトリを検索する前に自身を認証するように要求することにより、ディレクトリ セキュリティを強化します。この機能は コマンド ライン インターフェイスを使用して設定できます。

CLI コマンドの更新

この機能を Ciscoユニファイド コミュニケーション マネージャ で設定するには、次の新しい CLI コマンドを追加します。

- **utils contactsearchauthentication enable**—このコマンドを実行して UDS を使用する連絡先検索の認証を有効にします。
- **utils contactsearchauthentication disable**—このコマンドを実行して UDS を使用する連絡先検索の認証を無効にします。
- **utils contactsearchauthentication status**—このコマンドを実行して連絡先検索認証が有効であることを検証します。

ユーザ インターフェイスの更新

[**Secure Contact SEARCH URL**] エンタープライズパラメータが追加され、UDS を使用するセキュアな連絡先検索要求が転送されるディレクトリサーバのURLを指定します。このパラメータは、連絡先検索認証が有効になっている場合にのみ使用されます。

監査ログの更新

監査ログフレームワークは、次のものを含むように拡張されました。

- TCP を使用したリモートロギング: ログの配信を保証するために、TCP がリモート監査ロギングの転送プロトコルとして提供されるようになりました。この機能は、CLI コマンドを使用して設定できます。
- 詳細な監査ロギング: 詳細な監査ログは、監査ログに追加の設定情報を保存するオプションの監査ログ機能です。標準監査ログに保存されるすべての情報に加えて、詳細監査ロギ

ングには、変更された値も含め、追加、更新、または削除された設定項目も保存されます。詳細監査ロギングはデフォルトで無効になっていますが、[監査ログ設定（Audit Log Configuration）] ウィンドウで有効にすることができます。

- プラットフォーム ログのリモート処理およびFileBeat—リリース 11.5(1)SU1 を使用しているリモート サポート ログはリモート監査ログサポートを、プラットフォーム監査ログ (`/var/log/active/audit/vos-audit.logx` にローカルで保存)、リモートサポート ログ (例えば、 `remote_activity.log_<timestamp>`) でリアルタイムでサポートします。以前は、これらの監査ログはローカルにのみ保存可能でした。

  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 サービスは、FileBeat クライアントを使用して、これらのログを外部 logstash サーバにアップロードします。この機能は、一括管理ツールが使用する csv ファイルのアップロードにも使用されます。

CLI コマンドの更新

リモート監査ロギングの転送プロトコルを設定するために、次のCLI コマンドが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 サービスで使用できるようになりました。

- **utils remotesyslog set protocol tcp**: リモート監査ログの伝送プロトコルとして、このコマンドを実行して TCP を設定します。
- **utils remotesyslog set protocol udp**: リモート監査ログの伝送プロトコルとして、このコマンドを実行して UDP を設定します。
- **remotesyslog show protocol**: リモート監査ログに使用される伝送プロトコルを確認するには、このコマンドを実行します。

プラットフォーム監査ログおよびリモートサポート監査ログをアップロードするようにFileBeat クライアントを設定するには、次のCLI コマンドを使用する必要があります。すべてのコマンドは、特権レベル4管理者ユーザが使用できます。

- [**Fleatbeat の設定**]: 外部 logstash サーバ情報を使用して Filebeat クライアントを設定するには、このコマンドを使用します。
- **Utils FileBeat の有効化**: 外部 logstash サーバへのアップロードを有効にするには、このコマンドを使用します。このコマンドをすべてのノードで同時に実行しないでください。
- **Utils FileBeat の無効化**: 外部 logstash サーバへのアップロードを有効にするには、このコマンドを使用します。このコマンドをすべてのノードで同時に実行しないでください。
- **utils File Beat ステータス]**: このコマンドを使用して、Flebeat アップロードに対してシステムが有効か無効かを確認します

ユーザ インターフェイスの更新

監査ロギング向けの、次のユーザインターフェイスの更新が行われました。

- Cisco Unified Serviceability ウィンドウに **[Overflow Warning Threshold]** テキストボックスが追加されました。システムは、**監査ログ**が上書きされるレベルに近づいている場合にアラートを出すことができます。このフィールドを使用して、監査ログが上書きされるレベルに近づくと、警告が送信されてくる、しきい値を設定します。有効な値は1-99%です。デフォルト値は 80% です。
- **[Audit Log Configuration]** ウィンドウに **[Detailed audit Logging]** チェックボックスが追加されました。このチェックボックスをオンにすると、詳細な監査ログが有効になります。

監査ログ フィールドの更新

新しい監査ロギングの要件により、監査ログ自体に新しい**CorrelationID**パラメータが追加されます。1つのログメッセージが最大サイズを超えると、システムはそのメッセージを小さなメッセージに分割し、共通の**CorrelationID**値を割り当ててメッセージをリンクします。ログメッセージが最大しきい値を超えると、1つのログメッセージが監査ログに書き込まれ、[**CorrelationID**] フィールドが空になります。

次の 2 つの監査ログメッセージは、1つの大きなメッセージを形成します。次の例では、共通の**CorrelationID**値によってメッセージがリンクされます。

```
09:45:38.800
|LogMessage   UserID : admin  ClientAddress : 10.10.10.10  Severity : 6  EventType :
GeneralConfigurationUpdate  ResourceAccessed: CUCMServiceability  EventStatus : Success
  CompulsoryEvent : No  AuditCategory : AdministrativeEvent  ComponentID : Cisco CCM
Servicability  CorrelationID: 123456789 AuditDetails : <first part of the message> App
ID: Cisco Tomcat Cluster ID
```

```
09:45:38.800
|LogMessage   UserID : admin  ClientAddress : 10.10.10.10  Severity : 6  EventType :
GeneralConfigurationUpdate  ResourceAccessed: CUCMServiceability  EventStatus : Success
  CompulsoryEvent : No  AuditCategory : AdministrativeEvent  ComponentID : Cisco CCM
Servicability  CorrelationID: 123456789 AuditDetails : <remainder of the message> App
ID: Cisco Tomcat Cluster ID:  Node ID: sampleNodeHostname
```

新規アラームと新規アラート

TCPRemoteSyslogDeliveryFailedアラームとアラートは、両方ともシスコ ユニファイド リアルタイム モニタリング ツールに追加されています。TCP がリモート監査ログ転送プロトコルとして設定されていて、TCP伝送障害が発生すると、アラームがトリガーされます。さらに、一致するアラートが管理者に電子メールで送信されます。

アラート通知は、シスコ ユニファイドリアルタイム モニタリング ツールで設定する必要があります。

SHA-512 デジタル署名サポート

このリリースでは、デジタル署名に SHA-512 を使用するようにシステムを設定するオプションが用意されています。SHA-512 が設定されている場合、SHA-512 をサポートしていないレガシー電話は機能しません。

ユーザ インターフェイスの更新

[**TFTP ファイル署名アルゴリズム**] エンタープライズ パラメータが追加され、CTL、ITL および TFTP コンフィギュレーションファイルの生成時に使用されるダイジェストアルゴリズムのタイプが speciying に追加されました。**SHA-1** (デフォルト) または**SHA-512**を選択できます。

ランク ベースのアクセス コントロール

ユーザ ランクのアクセス コントロールでは、管理者がエンド ユーザやアプリケーション ユーザに提供できるアクセス レベルに対する一連の制御を行います。

エンド ユーザやアプリケーション ユーザをプロビジョニングする場合、管理者は各ユーザのユーザ ランクを割り当てる必要があります。管理者は、各アクセス コントロール グループにもユーザ ランクを割り当てる必要があります。Conttrol グループにアクセスするユーザを追加する場合、管理者は、ユーザのユーザのランク要件がグループのランク要件を満たしているグループにのみユーザを割り当てることができます。たとえば、あるエンド ユーザのユーザ ランクが 3 の場合、3 ～ 10 のユーザ ランクが設定されているアクセス コントロール グループに割り当てることができます。ただし、管理者は、そのユーザを 1 または 2 のユーザランク要件を持つアクセス制御グループに割り当てることはできません。

管理者は、[ユーザ順位の**設定**] ウィンドウ内に独自のユーザランク階層を作成し、ユーザをプロビジョニングし、アクセス制御グループを使用して、その階層を使用することができます。ユーザランクの階層を設定しない場合や、ユーザをプロビジョニングするとき、または conrol グループにアクセスするときにユーザランクの設定を指定しない場合は、すべてのユーザとアクセス制御グループにはデフォルトのユーザランク 1 (可能な限り高いランク) が割り当てられます。

ユーザアクセスのセットアップ方法については、*Cisco Unified Communications Manager* システム設定ガイド、リリース *11.5(1)SU1* の「ユーザアクセスの設定」を参照してください。

ユーザ インターフェイスの更新

このリリースでは、[**ユーザランクの設定 (User Rank Configuration)**] ウィンドウが新しくなっています。このウィンドウには、ユーザ**管理**>**ユーザ設定**>のユーザランクでアクセスできます。このウィンドウでは、エンドユーザとアプリケーションユーザに割り当てることができるユーザランクを設定できます。次のフィールドがあります。

- ユーザ ランク
- ユーザ ランク名
- 説明

[**ユーザランク (User Rank)**] フィールドは、次の設定ウィンドウに追加されています。このフィールドでは、エンドユーザまたはアプリケーションユーザのユーザランクを割り当てることができます。

- End User Configuration
- アプリケーション ユーザの設定

- ユーザ/電話のクイック追加
- LDAP ディレクトリ
- BAT ユーザ テンプレート

[**Access Control Group Configuration**] ウィンドウで、[new **Available for users Rank as**] ドロップダウンメニューが追加されました。このフィールドでは、ユーザがそのグループに割り当てられるために満たす必要がある最小ランクを割り当てることができます。

ファイル整合性チェックの SHA-512 チェックサム

ダウンロードのファイル整合性を確認するために、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 サービスは、すべてのダウンロードファイルに SHA-512 チェックサム値を提供するようになりました。たとえば、Cisco AXL ツールキットまたは Cisco ユニファイドリアルタイムモニタリングツールなどのアプリケーションプラグインダウンロードの SHA-512 チェックサムは、[**アプリケーションの検索と一覧表示 (Find And List Application Pugins**)] ウィンドウの [**説明 (Description**)] 列に表示されます。

ダウンロードにエラーが含まれていないことを確認するために、管理者は外部プログラムを使用して、ポストされたチェックサムとダウンロードしたファイルのチェックサムを比較することができます。チェックサムが一致した場合、ダウンロードにエラーはありませんでした。

最大セッション制限 CLI 更新

このリリースでは、既存の**set session maxlimit < value >** CLI コマンドが更新されました。このリリースでは、このコマンドにより、Cisco ユニファイド OS 管理ユーザインターフェイス、ディザスタリカバリシステムのユーザインターフェイス および SSH クライアントセッションの同時セッションの最大数が設定されるようになりました。

強化されたセキュリティ設定のタスク フロー

システムの 11.5 (1) リリースの一部であるセキュリティ強化を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	強化されたセキュリティ モードの設定（45 ページ）	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 サービスで強化されたセキュリティ モードを有効にします。
ステップ 2	システム クレデンシャル ポリシーが新しいガイドラインを満たしていることを確認する	クレデンシャルポリシーの更新の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/

	コマンドまたはアクション	目的
		unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『*Administration Guide for Cisco Unified Communications Manager AND IM And プレゼンス Service*』の「Manage credential policies」の章を参照してください。
ステップ 3	連絡先検索の認証の有効化 （46 ページ）	Cisco ユニファイド コミュニケーション マネージャ で連絡先検索の認証を有効にします。この機能が有効である場合、ユーザはディレクトリで他のユーザを検索する前にユーザ自身を認証する必要があります。
ステップ 4	リモート監査ログを設定する （48 ページ）	Cisco ユニファイド コミュニケーション マネージャ for IM and Presence Service のリモート監査ログの設定。これには、すべての監査ログおよびアラームに対するリモート syslog サーバの設定が含まれます。必要に応じて、監査ログに設定の更新に関する詳細を含める場合は、詳細な監査ロギングを有効にすることもできます。
ステップ 5	システムを SHA-512 デジタル署名暗号化を使用するように更新する （52 ページ）	デジタル署名に SHA-512 を使用するようにシステムをアップグレードします。
ステップ 6	電話のリセット （55 ページ）	変更を有効にするには、電話をリセットする必要があります。

強化されたセキュリティ モードの設定

強化されたセキュリティ モードを設定するには、すべての Unified Communications Manager または IM and Presence Service クラスタ ノードで次の手順に従います。

始める前に

強化されたセキュリティ モードを有効にする前に、FIPS を有効にしてください。

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 **utils EnhancedSecurityMode status** コマンドを実行し、強化されたセキュリティ モードが有効であるかどうかを確認します。

ステップ 3 クラスタ ノードで次のいずれかのコマンドを実行します。

- 強化されたセキュリティ モードを有効にするには、**utils EnhancedSecurityMode enable** コマンドを実行します。
- 強化されたセキュリティ モードを無効にするには、**utils EnhancedSecurityMode disable** コマンドを実行します。

ステップ 4 ノードが更新されたら、次のノードでこの手順を繰り返します。Unified Communications Manager および IM and Presence Service クラスタ ノードごとに繰り返します。

（注） **utils EnhancedSecurityMode enable** CLI コマンドまたは **utils EnhancedSecurityMode disable** CLI コマンドをすべてのノードで同時に実行しないでください。

連絡先検索の認証の有効化

Unified Communications Manager で連絡先検索の認証をセットアップするには、次のタスクを実行します。この機能が設定されている場合、ユーザはディレクトリで他のユーザを検索する前にユーザ自身を認証する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	連絡先検索の認証の電話サポートの確認（46 ページ）	電話でこの機能がサポートされていることを確認します。Cisco Unified Reporting で [Unified CM Phone Feature List] レポートを実行し、この機能をサポートしている電話モデルのリストを確認します。
ステップ 2	連絡先検索の認証の設定 （47 ページ）	Unified Communications Manager で連絡先検索の認証を設定します。
ステップ 3	連絡先検索用のセキュアなディレクトリ サーバの設定 （47 ページ）	電話のユーザがディレクトリで他のユーザを検索したときに示される URL を Unified Communications Manager で設定するには、次の手順を実行します。

連絡先検索の認証の電話サポートの確認

導入環境内の電話が連絡先検索の認証をサポートしていることを確認します。[Phone Feature List] レポートを実行して、この機能をサポートしているすべての電話モデルのリストを取得します。

手順

ステップ 1 Cisco Unified Reporting から [システム レポート(System Reports)] をクリックします。
ステップ 2 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] を選択します。
ステップ 3 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] レポートをクリックします。
ステップ 4 [製品 (Product)] フィールドはデフォルト値のままにします。
ステップ 5 [機能 (Feature)] ドロップダウンから [Authenticated Contact Search] を選択します。
ステップ 6 [送信（Submit）] をクリックします。`

次のタスク

連絡先検索の認証の設定 （47 ページ）

連絡先検索の認証の設定

電話ユーザの連絡先検索の認証を設定するには、Unified Communications Manager でこの手順に従います。

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 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。
ステップ 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

ステップ 4 すべての Unified Communications Manager クラスタ ノードでこの手順を繰り返します。

（注） 変更を有効にするには、電話をリセットする必要があります。

次のタスク

連絡先検索用のセキュアなディレクトリ サーバの設定 （47 ページ）

連絡先検索用のセキュアなディレクトリ サーバの設定

UDS がユーザ検索リクエストを送信するディレクトリ サーバ URL を Unified Communications Manager に設定するには、次の手順を使用します。デフォルトの値は `https://<cucm-fqdn-or-ip>:port/cucm-uds/users` です。

（注） デフォルトの UDS ポートは 8443 です。連絡先検索の認証が有効になると、デフォルトの UDS ポートは 9443 に切り替わります。その後、連絡先検索の認証を無効にした場合は、UDS ポートを手動で 8443 に戻す必要があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム(System)]** > **[Enterprise Parameters]** の順に選択します。

ステップ 2 [Secure Contact Search URL] テキスト ボックスに、セキュアな UDS ディレクトリ要求の URL を入力します。

（注） URL には、Cisco TFTP サービスを実行していないノードを選択することを推奨します。Cisco TFTP と UDS サービスのいずれかのサービスが再起動すると、互いに悪影響が及ぶ可能性があります。

ステップ 3 **[保存（Save）]** をクリックします。

リモート監査ログを設定する

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 で上記のタスクを完了して、リモート監査ログを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	リモート監査ログを設定する （49 ページ）	リモート監査ログの監査ログ設定を行います。設定の変更をログに記録する場合は、詳細な監査ロギングを有効にします。
ステップ 2	リモート監査ログの転送プロトコルの設定 （50 ページ）	オプション。リモート監査ログの転送プロトコルを設定します。通常動作モードのシステム デフォルトは UDP ですが、TCP を設定することもできます。
ステップ 3	アラート通知用の電子メール サーバの設定 （50 ページ）	RTMT で、電子メール アラート用の電子メールサーバをセットアップします。
ステップ 4	電子メール アラートの有効化 （51 ページ）	**TCPRemoteSyslogDeliveryFailed** アラートの電子メール通知を設定します。

	コマンドまたはアクション	目的
ステップ 5	Logstash サーバ情報の設定 （51 ページ）	IP アドレス、ポート番号、ダウンロード可能なファイル タイプなどの外部 Logstash サーバ情報で FileBeat クライアントを設定します。
ステップ 6	FileBeat クライアントの設定 （52 ページ）	プラットフォーム監査ログ、リモート サポート ログおよび一括管理 CSV ファイルのアップロード用の FileBeat クライアントを有効または無効にするには、次の手順を使用します。

リモート監査ログを設定する

この手順を使用して、リモート監査ログを Ciscoユニファイド コミュニケーション マネージャと IM and Presence サービスに設定します。

始める前に

- リモート syslog サーバをすでにセットアップしている必要があります。
- また、各クラスタ ノードとリモート syslog サーバ（中間のゲートウェイを含む）間で、間にあるゲートウェイへの接続を含み、IPSec を設定している必要があります。IPSec 設定については、『*Cisco IOS Security Configuration Guide*』を参照してください。

手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[監査ログ設定（Audit Log Configuration）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン メニューから、クラスタ内のサーバを選択し、[実行（Go）] をクリックします。

ステップ 3 [すべてのノードに適用（Apply to All Nodes）] チェックボックスをオンにします。

ステップ 4 [サーバ名（Server Name）] フィールドに、リモート syslog サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 これはオプションです。変更された項目と変更された値も含め、設定更新を記録するには、[詳細監査ロギング（Detailed Audit Logging）] チェックボックスをオンにします。

ステップ 6 [監査ログ設定（Audit Log Configuration）] ウィンドウの残りのフィールドに値を入力します。フィールドとその説明を含むヘルプについては、オンライン ヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

リモート監査ログの転送プロトコルの設定 （50 ページ）

リモート監査ログの転送プロトコルの設定

リモート監査ログ用の転送プロトコルを変更するには、次の手順を使用します。システム デフォルトは UDP ですが、TCP に設定し直すこともできます。

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 **utils remotesyslog show protocol** コマンドを実行して、どのプロトコルが設定されているかを確認します。

ステップ 3 このノード上でプロトコルを変更する必要がある場合は、次の手順を実行します。

- TCP を設定するには、**utils remotesyslog set protocol tcp** コマンドを実行します。
- UDP を設定するには、**utils remotesyslog set protocol udp** コマンドを実行します。

ステップ 4 プロトコルを変更した場合は、ノードを再起動します。

ステップ 5 すべての 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 サービスのクラスタ ノードでこの手順を繰り返します。

次のタスク

アラート通知用の電子メール サーバの設定 （50 ページ）

アラート通知用の電子メール サーバの設定

アラート通知用の電子メール サーバをセットアップするには、次の手順を使用します。

手順

ステップ 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル（Alert Central）] をクリックします。

ステップ 2 **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メール サーバの設定（Config Email Server）]** の順に選択します。

ステップ 3 [メール サーバ設定（Mail Server Configuration）] ポップアップで、メール サーバの詳細を入力します。

ステップ 4 [OK] をクリックします。

次のタスク

電子メール アラートの有効化 （51 ページ）

電子メール アラートの有効化

リモート監査ロギングを TCP で設定した場合は、次の手順を使用して、送信障害を通知する電子メール アラートを設定します。

手順

ステップ 1 Real-Time Monitoring Tool の [システム（System）] 領域で、[アラート セントラル（Alert Central）] をクリックします。

ステップ 2 **Alert Central** ウィンドウで、**TCPRemoteSyslogDeliveryFailed** を選択します

ステップ 3 **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [アラート アクションの設定（Config Alert Action）]** の順に選択します。

ステップ 4 [アラート アクション（Alert Action）] ポップアップで、[デフォルト（Default）] を選択して、[編集（Edit）] をクリックします。

ステップ 5 [アラート アクション（Alert Action）] ポップアップで、受信者を追加します。

ステップ 6 ポップアップ ウィンドウで、電子メール アラートを送信するアドレスを入力して、[OK] をクリックします。

ステップ 7 [アラート アクション（Alert Action）] ポップアップで、アドレスが [受信者（Recipients）] に表示されていることと、[有効（Enable）] チェックボックスがオンになっていることを確認します。

ステップ 8 [OK] をクリックします。

Logstash サーバ情報の設定

次の手順を使用して、IP アドレス、ポート番号、ダウンロード可能なファイル タイプなどの外部 Logstash サーバ情報で FileBeat クライアントを設定します。

始める前に

外部 Logstash サーバがセットアップされていることを確認します。

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 **utils FileBeat configure** コマンドを実行します。

ステップ 3 画面上の指示に従って、Logstash サーバの詳細を設定します。

FileBeat クライアントの設定

プラットフォーム監査ログ、リモート サポート ログ および一括管理 CSV ファイルのアップロード用の FileBeat クライアントを有効または無効にするには、次の手順を使用します。

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 **utils FileBeat status** コマンドを実行し、Filebeat クライアントが有効になっているかどうかを確認します。

ステップ 3 次のコマンドの 1 つを実行します。

- クライアントを有効にするには、**utils FileBeat enable** コマンドを実行します。
- クライアントを無効にするには、**utils FileBeat disable** コマンドを実行します。

ステップ 4 各ノードでこの手順を繰り返します。

これらのコマンドをすべてのノードで同時に実行しないでください。

システムを SHA-512 デジタル署名暗号化を使用するように更新する

次のタスクを完了して、Ciscoユニファイド コミュニケーション マネージャ がデジタル署名に SHA-512 を使用するようにアップグレードします。

始める前に

デジタル署名を使用するには、クラスタ セキュリティを混合モードに設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	お使いの電話が SHA-512 をサポートしていることを確認します。	特定の電話機モデルの電話サポートを確認するには、電話機のマニュアルを参照してください。
ステップ 2	デバイスのファームウェアのアップグレード （53 ページ）	オプション。いずれかの電話機のデバイス ファームウェアをアップグレードする必要がある場合は、次の手順を使用して新しいファームウェアをインストールします。
ステップ 3	サポートされていない電話機の対処方法を計画します。	オプション。SHA-512 をサポートしていないレガシー電話は、システムをアップグレードすると機能しません。新しい

	コマンドまたはアクション	目的
		電話機モデルにアップグレードしたり、サポートされていない電話機をシステムから削除したりする必要がある場合があります。
ステップ 4	SHA-512 の有効化 （54 ページ）	デジタル署名のために SHA-512 のクラスタ全体の使用を有効にします。
ステップ 5	CTL ファイルの更新 （54 ページ）	クラスタ セキュリティが混合モードに設定されている場合は、CTL セキュリティ ファイルを再生成します。
ステップ 6	サービスの再起動 （55 ページ）	Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。

デバイスのファームウェアのアップグレード

デバイス ファームウェアをアップグレードするには、次の手順を実行します。これは、SHA-512 をサポートするように電話機をアップグレードするために必要になる場合があります。

（注） SHA-512 をサポートしていないレガシー電話機がある場合は、それらの電話機を新しい電話機モデルにアップグレードする必要がある場合があります。

手順

ステップ 1 Cisco Unified OS の管理から、**[ソフトウェア アップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** の順に選択します。

ステップ 2 ソフトウェアの場所セクションに適切な値を入力し、[次へ（Next）] をクリックします。

ステップ 3 [使用可能なソフトウェア（Available Software）] ドロップダウン リストで、デバイス パッケージ ファイルを選択して、[次へ（Next）] をクリックします。

ステップ 4 MD5 の値が正しいことを確認し、[次へ（Next）] をクリックします。

ステップ 5 警告ボックスで、正しいファームウェアを選択したことを確認し、[インストール（Install）] をクリックします。

ステップ 6 成功メッセージを受信したことを確認します。

（注） クラスタを再起動している場合は、ステップ 8 に進みます。

ステップ 7 サービスを実行しているすべてのノードで [Cisco TFTP] サービスを再起動します。

ステップ 8 新しいロードにデバイスをアップグレードするには、影響を受けたデバイスをリセットします。

ステップ 9 Cisco Unified CM の管理から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）]** の順に選択し、新しいロードに（特定のデバイスに対して）ロード ファイルの名前を手動で変更します。

ステップ 10 [保存（Save）] をクリックし、デバイスをリセットします。

ステップ 11 すべてのクラスタ ノードで **Cisco Tomcat** サービスを再起動します。

ステップ 12 この場合、パブリッシャ ノード上で **Cisco CallManager** サービスを再起動します。

（注） ただし、サブスクライバ ノードでのみ **Cisco CallManager** サービスを実行している場合は、このステップをスキップできます。

次のタスク

すべての電話機が SHA-512 をサポートしていることを確認したら、SHA-512 の有効化 （54 ページ）

SHA-512 の有効化

電話に SHA-512 デジタル署名を要求するよう Ciscoユニファイド コミュニケーション マネージャ を設定するには、次の手順を使用します。

（注） この手順を完了すると、SHA-512 をサポートしていない旧型の電話は機能しません。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム(System)] > [Entエンタープライズ パラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 [TFTP File Signature Algorithm] エンタープライズ パラメータを [SHA-512] に設定します。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

クラスタ セキュリティが混合モードに設定されている場合、CTL ファイルの更新 （54 ページ）

クラスタ セキュリティが非セキュアモードに設定されている場合、サービスの再起動 （55 ページ）

CTL ファイルの更新

クラスタ セキュリティが混合モードに設定されている場合、SHA-512 使用のためのシステム アップグレード後に、この手順を実行して CTL ファイルを再生成します。

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 パブリッシャ ノードで **utils ctl update CTLfile** コマンドを実行します。

次のタスク

サービスの再起動 （55 ページ）

サービスの再起動

Cisco TFTP サービスおよび Cisco CallManager サービスを再起動するには、次の手順を実行します。クラスタで SHA-512 を有効にした後、サービスを再起動する必要があります。

手順

ステップ 1 Cisco Unified Serviceability で **[ツール(Tools)]** > **[コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 以下の 2 つのサービスをそれぞれ選択し、[停止（Stop）] をクリックします。

- Cisco CallManager
- Cisco TFTP

ステップ 3 両方のサービスが停止したら、両方を再度選択し、[開始（Start）] をクリックします。

次のタスク

電話のリセット （55 ページ）

電話のリセット

電話をリセットするには、次の手順を実行します。[Contact Search Authentication] で行った設定の変更と SHA-2 デジタル署名の変更を有効にするため、電話のリセットが必要です。

手順

ステップ 1 [Cisco Unified CM Administration] から、**[デバイス（Device）]** > **[電話（Phones）]** を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [すべて選択（Select All）] をクリックします。

ステップ 4 [選択をリセットする（Reset selected）] をクリックします。

強化された TLS 暗号化

Cisco ユニファイドコミュニケーションマネージャIM およびプレゼンスサービス Release 11.5(1) では、TLS バージョン 1.2 接続で Tomcat、SIP プロキシ および XMPP インターフェイスに関して楕円曲線デジタル署名アルゴリズム（ECDSA）がサポートされます。

証明書を作成する際は、RSA ベースの証明書と ECDSA ベースの証明書の両方を設定することを推奨します。たとえば、Tomcat 証明書を設定する場合、Tomcat-ECDSA 証明書も設定する必要があります（その逆も同様）。

（注） IM and Presence Service ピアが TLS バージョン 1.2 をサポートしない場合は、接続が TLS バージョン 1.0 にフォールバックされ、既存の動作が保持されます。

このサポートの一部として、Tomcat、SIP プロキシおよびXMPP インターフェイスをサポートする TLS 接続で使用するために 4 つの新しい暗号方式が導入されました。これらの新しい暗号方式のうちの 2 つは RSA ベースで、残りの 2 つは ECDSA ベースです。

ECDSA ベース暗号方式のサポートの詳細については、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 Release 11.0(1) のリリース ノートの「ECDSA Support for Common Criteria for Certified Solutions」を参照してください。

導入された新しい暗号方式は次のとおりです。

- ECDHE ECDSA 暗号方式
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- ECDHE RSA 暗号方式
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**

RSA ベースの暗号方式については、既存のセキュリティ証明書が使用されます。ただし、ECDSA ベースの暗号方式には次の追加のセキュリティ証明書が必要です。

- `cup-ECDSA`
- `cup-xmpp-ECDSA`
- `cup-xmpp-s2s-ECDSA`
- `tomcat-ECDSA`

証明書名が `-ECDSA` で終わる場合、その **証明書/キー** タイプは楕円曲線（EC）です。それ以外の場合は、RSA です。EC 証明書の共通名（CN）はホスト名に `-EC` が追加されます。また、EC 証明書の SAN フィールドにはサーバの FQDN またはホスト名が含まれます。

（注） RSA ベースの証明書（Tomcat、XMPP、XMPP-s2s および CUP）の共通名（CN）フィールドには EC を使用しないことを推奨します。使用すると、既存の EC ベースの証明書が上書きされます。

IM and Presence Service でのセキュリティ証明書の設定の詳細については、「IM and Presence Service の証明書タイプ」、「IM and Presence Service へのマルチサーバ CA 署名付き証明書のアップロード」 および「IM and Presence Service への単一サーバ CA 署名付き証明書のアップロード」を参照してください。

TLS 暗号の設定については、「TLS 暗号のマッピングの設定」を参照してください。

エンタープライズ グループの更新

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 サービスのこのリリースでは、エンタープライズ グループ機能に次の更新が導入されました。

- LDAP 同期でのセキュリティグループのサポート
- エンタープライズ グループ LDAP 設定パラメータ

LDAP 同期でのセキュリティグループのサポート

エンタープライズグループ機能は、外部LDAPディレクトリからのセキュリティグループの同期をサポートするように更新されました。Cisco Jabberユーザは、セキュリティ グループのディレクトリを検索して、グループ メンバーを自分の連絡先リストに追加できます。

この機能の設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』の「エンタープライズ グループ」の章を参照してください。

エンタープライズ グループ LDAP 設定パラメータ

IM and Presence サービス リリース 11.5 (1) では、**エンタープライズ グループ LDAP 設定**パラメータがクラスタ間ピアテーブルに追加されています。このパラメータを使用して、IM と Preseence サービスピアの間に設定エラーがないことを確認できます。クラスタ間ピアテーブルを表示するには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [クラスタ間設定（Inter-Clustering）]** を選択します。

競合がある場合は、[エンタープライズグループ競合 (Enterprise Group Conflicts)] リンクをクリックします。表示される [**Details**] ボタンをクリックして、詳細レポートを表示します。

この更新の一環として、[**プレゼンス情報を許可する最大エンタープライズグループサイズ**]の許容範囲は 1 ~ 200 ユーザです。デフォルト値は 100 ユーザです。

デバイス パックのヒットの少ないインストール

Cisco Unified Communications Managerリリース 11.5(1) 以降では、既存のファームウェアまたは設定を更新したり、新しいデバイスサポートを有効にしたりするために、デバイスパックを適用するためにクラスタ全体のリブートは必要なくなりました。キャッシュされた情報は、新しいデバイスのインストール中に実行時に更新されます。この更新により、サービスを中断せずにデバイスのファームウェアをアップグレードしたり、新しい電話機モデルをテストしたりできます。

アドミニストレーション ガイドの更新

『*Cisco Unified Communications Manager* のアドミニストレーションガイド』の「Install a Device Pack Or Cisco Options Package File」の手順を更新しました。クラスタ全体のリブートが削除されたことを示す注意事項があります。デバイスファームウェアのアップグレードの詳細については、『Ciscoユニファイド コミュニケーション マネージャ のアドミニストレーション ガイド』の「デバイス ファームウェアの管理」の章を参照してください。

H.265 ビデオ コーデックのサポート

11.5 リリースでは、 Cisco Unified Communications Managerは SIP-SIP ビデオコール用の H.265 ビデオコーデックをサポートしています。H.265 は、MTP/TRP/RSVP エージェント パススルーの場合にサポートされます。H.265 パススルーを使用するには、MTP パススルーを設定する必要があります。

このリリースでサポートされているビデオコーデックの完全なリストについては、ビデオ コーデック 設定の更新 （130 ページ） を参照してください。

IM and Presence Service での持続チャットの高可用性

持続チャットにおける高可用性の概要

現在のリリースから、持続チャット機能は高可用性に対応しています。IM and Presence Service ノードの障害またはテキスト会議（TC）サービスの障害時は、サービスによりホストされているすべての持続チャット ルームが自動的にバックアップ ノードの TC サービスによってホストされます。フェールオーバー後、Jabber クライアントはシームレスに持続チャットルームを使用し続けることができます。

高可用性の詳細については、Ciscoユニファイドコミュニケーション マネージャ のシステム設定ガイドから、プレゼンス冗長グループの設定に関する章を参照してください。

この例では、3 人のユーザ（A、B、C）と 3 つの IM and Presence Service ノード（1A、2A、1B）があります。ノード 1A と 1B は同じプレゼンス冗長グループの一部で、高可用性（HA）ペアを形成します。ユーザは、次のノードに割り当てられます。

- ユーザ A = ノード 1A
- ユーザ B = ノード 2A
- ユーザ C = ノード 1B

1. ユーザ A、B、C はノード 1A にホストされているチャット ルームにいます。
2. テキスト会議（TC）サービスがノード 1A で失敗します。
3. IM and Presence Service 管理者は、手動フォールバックを開始します。
4. ノード 1B は、HA の状態 [バックアップモードで実行中（Running in Backup Mode）] に遷移する前に、HA の状態 [フェールオーバー済み(重要なサービスは非実行)（Failed Over with Critical Services not Running）] に遷移します。
5. HA フェールオーバー モデルに沿ってユーザ A が自動的にサインアウトし、バックアップ ノード 1B にサインインします。
6. ユーザ B および C に変更はありませんが、ノード 2A でホストされているチャット ルームに引き続きメッセージを送信できます。
7. ノード 1A は**テイクバック中**に移行して、ノード 2A は**フォールバック中**に移行します。
8. ユーザ A はノード 1B からサインアウトします。ユーザ B および C は持続チャット ルームを使用し、フォールバックが発生したらルームはノード 1A に戻ります。
9. ノード 1B は、HA の状態 [テイクバック中（Taking Back）] から [正常（Normal）] に遷移し、そのピア ノード ルームをアンロードします。
10. ノード 1A は、HA の状態 [フェールオーバー中（Failing Over）] から [正常（Normal）] に遷移し、pubalias.cisco.com に関連付けられているルームをリロードします。
11. ユーザ A はノード 1A に再度サインインし、持続チャット ルームに入り、引き続きメッセージを読んだりルームに送信したりできます。

表 *8:* グループ チャットと持続チャットの制限

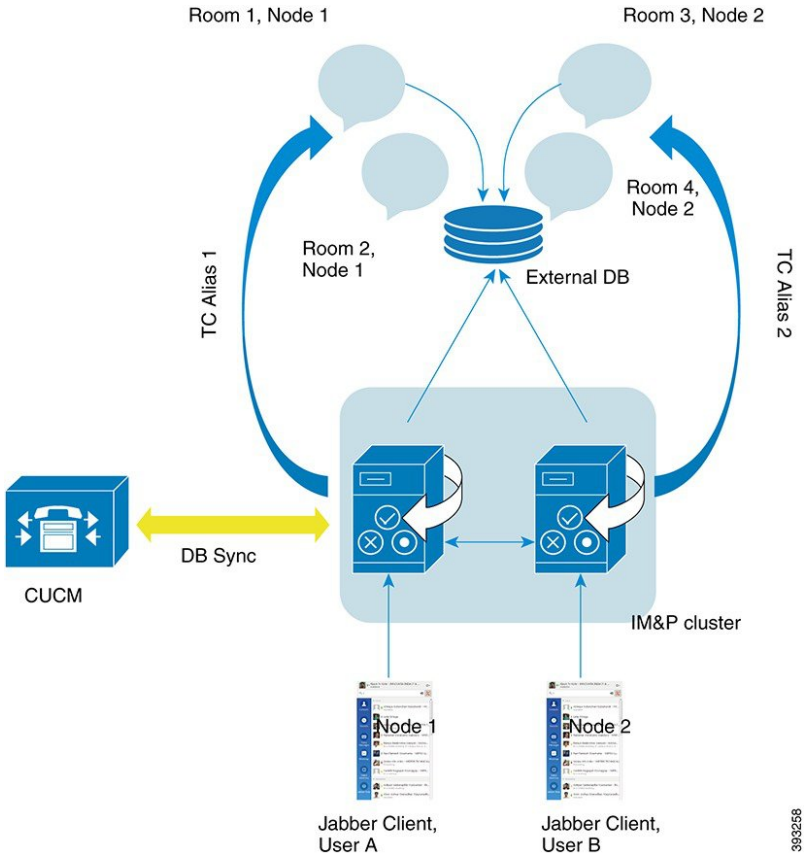
機能	制限事項
匿名ルームでのチャット	Cisco Jabber 経由でチャットを展開する場合（グループ チャットまたは持続チャットのいずれか）は、[グループチャットとパーシステントチャットの設定（Group Chat and Persistent Chat Settings）] ウィンドウで [デフォルトで、ルームは匿名です（Rooms are anonymous by default）] および [ルームのオーナーは、ルームを匿名にするかどうかを変更できます（Room owners can change whether or not rooms are anonymous）] オプションが選択されていないことを確認してください。いずれかのチェックボックスをオンにすると、チャットは失敗します。

持続チャットにおける高可用性のフロー

次に、フェールオーバーとフェールバックにおける持続チャットの高可用性フローを示します。

（注） この機能強化のために、テキスト会議（TC）サービスは不可欠なサービスとして位置付けられています。その結果、TC の高可用性のフェールオーバーのフローは、ノードの別の重要なサービス（Cisco XCP ルータ サービスなど）の障害によりフェールオーバーが引き起こされたとしても同様になります。

図 *1:* 持続チャットにおける高可用性の構造



持続チャットにおける高可用性のフェールオーバー フロー

この例では、4 人のユーザが、2 つのハイ アベイラビリティ（HA）ペアあるいはサブクラスタを持つ 4 つの IM and Presence Service ノードを持っています。ユーザは以下のように割り当てられます。

サブクラスタ 1	サブクラスタ 2
• 山田 はノード 1A 存在：ノード 1A はチャット ルームをホストしています。 • 髙橋 はノード 1B 上に	• 斎藤はノード 2A 上に存在する • 小川はノード 2B 上に存在する

1. 4 人のユーザすべてが、ノード 1A でホストされる同一のチャット ルーム内でチャットを行っています。
2. テキスト会議（TC）サービスがノード 1A で失敗します。
3. 90 秒後に、Server Recovery Manager（SRM）は TC の重要なサービスの障害を特定し、自動フェールオーバーを開始します。
4. ノード 1B は、1A からユーザを引き継ぎ、**フェールオーバー済み（重要なサービスは非実行）**の状態に移行させてから、**バックアップモードで実行中** のHAの状態に移行させます。
5. HA フェールオーバー モデルに沿って、山田が自動的にログアウトし、バックアップ ノード 1B にサインインします。
6. 他のユーザは影響を受けません。ノード 1B でホストされるチャット ルームへのメッセージは引き続き投稿されます。
7. ユーザ A は持続チャット ルームに入り、引き続きメッセージを読んだりルームに送信したりできます。

持続チャット ルームの高可用性フォールバック フロー

この例では、4 人のユーザが、2 つのハイ アベイラビリティ（HA） ペアあるいはサブクラスタのある 4 つのIM and Presence Service ノードを持っています。ユーザは以下のように割り当てられます。

サブクラスタ 1	サブクラスタ 2
• 山田 はノード 1A 存在：ノード 1A はチャット ルームをホストしています。 • 髙橋 はノード 1B 上に	• 斎藤はノード 2A 上に存在する • 小川はノード 2B 上に存在する

1. 4 人のユーザすべてが、ノード 1A でホストされる同一のチャット ルーム内でチャットを行っています。
2. テキスト会議（TC）サービスがノード 1A で失敗します。
3. ノード 1B は、1A からユーザを引き継ぎ、**フェールオーバー済み（重要なサービスは非実行）**に移行させてから、**バックアップモードで実行中** のHAの状態に移行させます。
4. HA フェールオーバー モデルに沿って、山田が自動的にログアウトし、バックアップ ノード 1B にサインインします。

5. 髙橋、斎藤および小川は影響を受けません。ノード1Bでホストされるチャットルームへのメッセージは引き続き投稿されます。
6. IM and Presence Service管理者は、手動フォールバックを開始します。
7. ノード1Aは**テイクバック中**に移行して、ノード2Aは**フォールバック中**に移行します。
8. 山田はノード1Bからログアウトします。髙橋、斎藤、小川は、常設チャットルームの使用を継続し、**フォールバック**が起こると、ルームはノード1Aに戻ります。
9. ノード1Bは、HAの状態から、**正常**に**フォールバック**し、ピアノードルームをアンロードします。
10. ノード1Bは、**テイクバック中**のHAの状態から**正常**に移行し、ピアノードルームをリロードします。
11. ユーザAは持続チャットルームに入り、引き続きメッセージを読んだりルームに送信したりできます。

持続チャットにおける高可用性の有効化と確認

持続チャットの高可用性を有効にし、正しく動作していることを確認するには、次の手順を実行します。

手順

ステップ1 高可用性がプレゼンス冗長グループで有効なことを確認するには、以下を実行します。

a) [Cisco Unified CM管理（Cisco Unified CM Administration）]から、**[システム（System）]** > **[プレゼンス冗長グループ（Presence Redundancy Groups）]**を選択します。
b) [プレゼンス冗長グループの検索/一覧表示(Find and List Presence Redundancy Groups)]ウィンドウで[検索（Find）]をクリックして、オンにするプレゼンス冗長グループを選択します。
c) [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）]ウィンドウで、[高可用性の有効化（Enable High Availability）]チェックボックスがオンになっていることを確認します。

ステップ2 持続チャットがプレゼンス冗長グループで有効なことを確認するには、以下を実行します。

a) [Cisco Unified CM IM and Presenceの管理UI（Cisco Unified CM IM and Presence Administration UI）]で、**[メッセージング（Messaging）]** > **[グループチャットと持続チャット（Group Chat and Persistent Chat）]**を選択します。
b) [グループチャットと持続チャット（Group Chat and Persistent Chat）]ウィンドウで、[持続チャットの有効化（Enable Persistent Chat）]チェックボックスがオンになっていることを確認します。

ステップ3 プレゼンス冗長グループノードがどちらも同じ外部データベースに割り当てられていることを確認します。画像を参照してください。

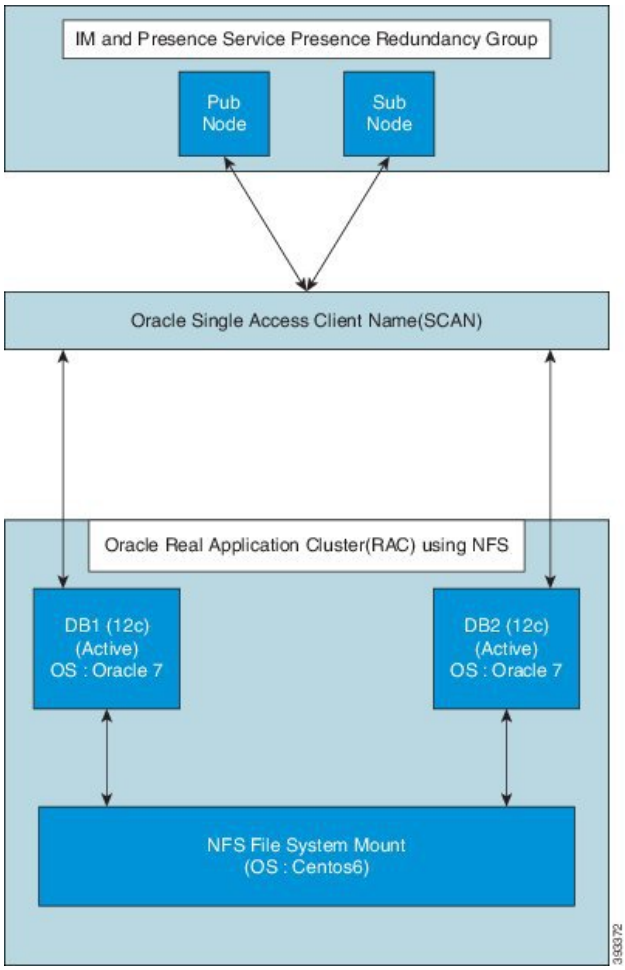
ステップ 4 持続チャットの高可用性が有効であることを確認するには、**[システム（System）]>[プレゼンストポロジ（Presence Topology）]** ウィンドウを確認します。[ノードの詳細(Node Detail)] ペインの [ノードのステータス（Node Status）] セクションの [サービス列（Service Column）] で、[Cisco XCP Text Conference Manager] エントリの [モニタ対象（Monitored）] 列が [Yes] であることを確認します。

これがモニタ対象サービスである場合は、これが重要なサービスであり、高可用性が正常に有効にされていることを意味します。モニタ対象サービスでない場合は、プレゼンス冗長グループが正しく設定されていることを確認します。

持続チャットの高可用性のための外部データベース

サポートされているバージョンについては、『*Database Setup Guide for IM and Presence Service*』の「External Database Setup Requirements」の項を参照してください。

図 *2 : Oracle* 高可用性設定



外部データベースのテーブルのマージ

外部データベースのマージ ツールでは、複数の外部データベース パーティションに保存されている持続チャット データを 1 つのデータベースにマージできます。

以前のバージョンでは、プレゼンス冗長グループの各 IM and Presence Service ノードに固有の外部データベースが割り当てられていました。現在のリリースからは、持続チャットの高可用性を有効にする際はプレゼンス冗長グループのノードを 1 つの外部データベースにのみ割り当てる必要があります。外部データベースのマージ ツールにより、これらの 2 つのデータベースをすばやく連結することができます。

外部データベースのマージ ツールは、Oracle と Postgres データベースで使用できます。

（注） Oracle データベースで外部データベース マージ ツールを使用するには、[Oracle SID] フィールドに [データベース名（Database Name）] フィールドと同じ値を設定する必要があります。そうしないと、マージは失敗します。詳細については、CSCva08935 を参照してください。

外部データベースのマージ ツール

IM and Presence Service のプレゼンス冗長グループで 2 つのデータベースをマージするには、次の手順を使用します。

始める前に

- 2 つのソースおよび対象データベースが、プレゼンス冗長グループの各 IM and Presence Service ノードに正しく割り当てられていることを確認します。これにより両方のスキーマが有効であることが確認されます。
- 対象データベースのテーブルスペースをバックアップします。
- 対象データベース上に、新しくマージされたデータベースが十分に収まる領域があることを確認します。
- ソース データベースと対象データベース用に作成されたデータベース ユーザに、次のコマンドを実行する権限があることを確認します。
  - `CREATE TABLE`
  - `CREATE PUBLIC DATABASE LINK`

  データベース ユーザにこれらの権限がない場合は、次のコマンドを使用して付与することができます。
  - `GRANT CREATE TABLE TO <user_name>;`
  - `GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;`

手順

ステップ 1 IM and Presence Service パブリッシャ ノード上の [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] にサインインします。

ステップ 2 プレゼンス冗長グループの各 IM and Presence Service ノードの **[システム（System）] > [サービス（Services）]** ウィンドウで Cisco XCP Text Conference Service を停止します。

ステップ 3 **[メッセージング（Messaging）] > [外部データベースの設定（External Server Setup）] > [外部データベース ジョブ（External Database Jobs）]** をクリックします。

ステップ 4 マージ ジョブのリストを表示するには、[検索（Search）] をクリックします。新しいジョブを追加するには、[マージ ジョブの追加（Add Merge Job）] を選択します。

ステップ 5 [外部データベースのマージ（Merging External Databases）] ウィンドウで、次の情報を入力します。

- [データベース タイプ（Database Type）] ドロップダウン リストから [Oracle] または [Postgres] を選択します。
- マージされたデータを含む 2 つのソース データベースと対象データベースの IP アドレスとホスト名を選択します。

[データベース タイプ（Database Type）] に [Oracle] を選択した場合、テーブルスペース名とデータベース名を入力します。[データベースタイプ（Database Type）] に [Postgres] を選択した場合、データベース名を指定します。

ステップ 6 [Feature テーブル（Feature Tables）] ペインで、[Text Conference（TC）] チェックボックスがデフォルトでオンになっています。現在のリリースでは、その他の選択肢はありません。

ステップ 7 [選択したテーブルの検証（Validate Selected Tables）] をクリックします。

（注） Cisco XCP Text Conference サービスが停止していなければ、エラー メッセージが表示されます。サービスが停止していれば、検証は完了します。

ステップ 8 [検証の詳細（Validation Details）] ペインにエラーがなければ、[選択したテーブルをマージ（Merge Selected Tables）] をクリックします。

ステップ 9 マージが正常に完了したら、[外部データベースの検索と一覧表示（Find And List External Database Jobs）] ウィンドウがロードされます。ウィンドウを更新し、新しいジョブを表示するには、[検索（Find）] をクリックします。

詳細を表示するには、ジョブの [ID] をクリックします。

ステップ 10 Cisco XCP Router サービスを再起動します。

ステップ 11 両方の IM and Presence Service ノードで Cisco XCP Text Conference Service を開始します。

ステップ 12 新しくマージされた外部データベース（対象データベース）をプレゼンス冗長グループに再割り当てする必要があります。

データベース複製で

このリリースでは、`utils imdb_replication replication status`コマンドが導入されました。このコマンドは、導入における各サブクラスタのノード ペア間のイン メモリ データベース（IMDB）レプリケーションが正しく動作することを検証します。

このコマンドはまた、IM and Presence サービス ノードの発信からのユーティリティを使用して、それぞれの関連するデータストアのIMDBテーブルで読み取りおよび書き込みを実行します。

（注） このコマンドを使用して管理 CLI 診断ユーティリティを実行するには、ポート 6603、6604 および 6605 がクラスタの IM and Presence Service ノード間で設定されているすべてのファイアウォールでオープンである必要があります。このセットアップは、通常の運用では必要ありません。

外部マルチキャスト MOH からユニキャスト MOH へのインターワーキング

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9.x 以前は、Cisco Media コンバージェンスサーバ (MCS) または仮想マシンで実行されていました。MCS を使用して、コンパクトディスクやジュークボックスなどの Universal Serial bus (USB) ケーブルプラグを保留音 (MOH) デバイスに使用することができます。デバイスは固定オーディオソースと呼ばれ、ユニキャストとマルチキャストの両方の保留音を再生するために使用されます。

Ciscoユニファイド コミュニケーション マネージャ リリース 10. x 以降は、仮想マシンでのみ実行されます。したがって、USB MOH デバイスはサポートされなくなりました。これにより、ローカルでアップロードされた wav ファイルを MOH として再生するようにCiscoユニファイド コミュニケーション マネージャ を制限します。この制限を打開するため、このリリースでは、Cisco Unified Survivable Remote Site Telephony（SRST）ルータをオーディオ ソースとして設定できます。このルータは、マルチキャスト受信が可能なデバイスに対してマルチキャスト MOH オーディオを提供します。この方法では、Ciscoユニファイド コミュニケーション マネージャ がマルチキャスト MOH オーディオを送信している場合と同様にデバイスが機能します。ただし、ユニキャスト受信だけが可能なデバイスでは、外部 MOH ソース（Cisco Unified SRST ルータなど）から送信される MOH オーディオは聞こえません。ユニキャスト受信のみが可能なデバイスの例としては、公衆電話交換網（PSTN）電話機、セッション ボーダー コントローラ（SBC）の接続先 および Session Initiation Protocol（SIP）トランクなどがあります。

In Ciscoユニファイド コミュニケーション マネージャ Release 11.5、this feature is an enhancement to receive multicast MOH audio from an external audio source and send it as unicast MOH audio. Cisco ユニファイド コミュニケーション マネージャ はこの機能を使用して、ユニキャスト MOH の受信のみが可能なデバイスに対し、マルチキャスト MOH オーディオをユニキャスト MOH と

して再生します。外部 MOH オーディオ ソースの例としては、Cisco Unified SRST ルータや、マルチキャスト MOH オーディオを送信できるソフトウェアなどがあります。

管理者は [Cisco Unified CM の管理（Cisco Unified CM Administration）] の [保留音オーディオ ソースの設定（Music On Hold Audio Source Configuration）] ウィンドウでこの機能に関するフィールドを設定できます。

（注）

- この機能は、マルチキャスト受信可能なデバイスに対して外部オーディオ ソースを使用してマルチキャスト MOH オーディオを再生できる既存の機能には影響しません。
- ユニキャストメディア接続の場合、外部マルチキャスト ソースを使用したMOHオーディオ ソースを設定していても、Ciscoユニファイド コミュニケーション マネージャ MOH サーバは初回アナウンスと定期的なアナウンスを再生します。

コーデック固有の着信オーディオ ストリームに関する設定のヒント

必要なオーディオ フィードをストリーミングするため、MOH サーバに対し、外部マルチキャスト オーディオ ソース（Cisco Unified SRST ルータなど）を設定します。

Cisco Unified SRST ルータなどの外部マルチキャスト オーディオ ソースを設定するには、**[MOH オーディオ ソースの設定（MOH Audio Source Configuration）]** ウィンドウで **[ソースの IPv4 マルチキャスト アドレス（Source IPv4 Multicast Address）]** フィールドと **[ソースのポート番号（Source Port Number）]** フィールドを設定します。

- Ciscoユニファイド コミュニケーション マネージャ は、[MOHオーディオソースの設定（MOH Audio Source Configuration）] ウィンドウで設定した外部マルチキャスト IP アドレスとポートで、マルチキャスト G.711 μ-law ストリームをリッスンします。MOH サーバは G.711 μ-law または A-law、あるいは L16 256K ワイドバンド MOH コーデック間の変換を実行できます。外部マルチキャスト RTP ストリームは、G.711 μ-law または A-law、あるいは L16 256K ワイドバンド MOH コーデックのソースとして、MOH に G.711 μ-law コーデックを使用します。G.711 A-law およびワイドバンド コールの場合、Ciscoユニファイド コミュニケーション マネージャ MOH サーバは、着信 G.711 μ-law ストリームを発信 G.711 A-law またはワイドバンド ストリームに変換してから、デバイスに送信します。
- Ciscoユニファイド コミュニケーション マネージャ は、[MOH オーディオ ソースの設定（MOH Audio Source Configuration）] ウィンドウで設定した外部マルチキャスト IP アドレスおよびポートの値に 4 を加算したアドレスで、マルチキャスト G.729 μ-law ストリームをリッスンします。たとえば、239.1.1.1:16384 を使用して MOH オーディオ ソースを設定した場合、Ciscoユニファイド コミュニケーション マネージャ は 239.1.1.1:16384 で G.711 μ-law ストリームをリッスンし、239.1.1.1:16388（ポート値に 4 を加算した値）で G.729 をリッスンします。MOH サーバは、G.729 コーデックの変換は実行できません。MOH G.729 コーデックを使用する発信者には、G.729 または G.729a コーデックを使用する外部マルチキャスト RTP ストリームが必要です。

保留音のオーディオ ソース フィールド

（注）

- Ciscoユニファイドコミュニケーションマネージャ MOH サーバは、MOH 音源で設定されたマルチキャスト MOH オーディオを外部ソースから受信し、それをユニキャストとしてユニキャスト受信のみに対応したデバイスへ送信します。
- 管理者は、外部マルチキャスト ソースで設定されたのと同じ MOH 音源を使用して、マルチキャスト受信対応デバイス向けにマルチキャスト MOH を再生できます。これには、MOH サーバで設定したベース マルチキャスト IP アドレスおよびベース マルチキャスト ポート番号と同じソース IPv4 マルチキャスト アドレスおよびポートを使用して、MOH 音源を設定します。
- 管理者はさらに、ソース IPv4 アドレスから受信したマルチキャスト MOH オーディオを別のマルチキャスト IPv4 アドレスから送信するように MOH サーバを設定することもできます。管理者は、**[保留音オーディオ設定（Music On Hold Audio Configuration）]** ウィンドウで、MOH 音源に複数のマルチキャスト IPv4 アドレスを設定し、MOH サーバにベース マルチキャスト IP アドレスを設定できます。

フィールド	説明
保留音のオーディオ ソース情報	
[MOH オーディオ ストリーム番号（MOH Audio Stream Number）]	この MOH オーディオ ソースのストリーム番号を選択するには、このフィールドを使用します。ドロップダウン矢印をクリックし、リストから値を選択します。既存の MOH オーディオ ソースの場合、値は MOH オーディオ ソースのタイトルで表示されます。
[MOH オーディオ ソース ファイル（MOH Audio Source File）]	この MOH オーディオ ソースのファイルを選択するには、このフィールドを使用します。ドロップダウン矢印をクリックし、リストから値を選択します。
[MOH オーディオ ソース名（MOH Audio Source Name）]	MOH オーディオ ソースの一意の名前を、このフィールドに入力します。この名前には、文字、数字、スペース、ダッシュ、ドット（ピリオド）およびアンダースコアを含み、最大で 50 の有効な文字を使用できます。
マルチキャストを許可（Allow Multi-casting）	選択した MOH オーディオ ソースのマルチキャストを許可するには、このチェックボックスをオンにします。

フィールド	説明
[MOH WAV ファイル ソースを使用する（Use MOH WAV file source）]	MOH音源を選択するには、このオプションをクリックします。マルチキャスト ソースがない場合は、このフィールドを使用します。 （注） • このオプションを選択すると、**[MOH 音源ファイル（MOH Audio Source File）]** フィールドが有効になります。 • **[外部のマルチキャストソースを再映像配信する（Rebroadcast External Multicast Source）]** フィールドをクリックする場合は、**[MOH音源ファイル（MOH Audio Source File）]** フィールドを選択しないでください。
外部マルチキャスト ソースの再ブロードキャスト	外部マルチキャスト ソースから送信されるMOHオーディオを再ブロードキャストするには、このオプションを選択します。マルチキャスト ソースがある場合は、このフィールドを使用します。
[IPv4 マルチキャスト アドレスのソース（Source IPv4 Multicast Address）]	ソースのIPv4マルチキャストアドレスを入力します。外部ソース（たとえば、Cisco Unified SRST ルータ）は、このマルチキャスト アドレスおよびポートの宛先へオーディオ RTP ストリームを送信するように設定されます。 （注） SRST ルータは IPv6 アドレスをサポートしません。
送信元ポート番号	外部ソースがマルチキャスト MOH オーディオを送信するために使用するマルチキャスト ソースのポート番号を入力します。

フィールド	説明
[MOH オーディオ ソース ファイル ステータス（MOH Audio Source File Status）]	このペインには、選択した MOH オーディオ ソースのファイルに関する次の情報が表示されます。 • [InputFileName] • [ErrorCode] • [ErrorText] • [DurationSeconds] • [DiskSpaceKB] • [LowDateTime] • [HighDateTime] • [OutputFileList] • [MOH オーディオ変換の完了日（MOH Audio Translation completion date）] （注） [OutputFileList] には ULAW、ALAW、G.729 およびワイドバンド WAV ファイルと、ステータス オプションについての情報が含まれます。
アナウンスの設定	

フィールド	説明
[最初のアナウンス（Initial Announcement）]	ドロップダウン リストから最初のアナウンスを選択します。 （注） 最初のアナウンスを持たない MOH を選択するには、[選択なし（Not Selected）] オプションを選択します。 [詳細表示（View Details）] リンクをクリックすると、次のような最初のアナウンス情報を参照できます。 • [アナウンス ID（Announcement Identifier）] • 説明（Description） • [デフォルトのアナウンス（Default Announcement）] （注） • オーディオ ソースの [マルチキャストを許可（Allow Multi-casting）]「」のチェックがオフで、[再生される最初のアナウンス（Initial Announcement Played）]「」が [キューされたコールのみ（Only for queued calls）] に設定されている場合だけ、MOH サーバによって再生されます。 • [マルチキャストを許可（Allow Multi-casting）]「」のチェックがオンか、[再生される最初のアナウンス（Initial Announcement Played）]「」が [常時（Always）] に設定されている場合、ANN によって再生されます。

フィールド	説明
[再生される最初のアナウンス（Initial Announcement Played）]	次のうち 1 つを選択して、最初のアナウンスを再生するタイミングを決定します。 • [ハント メンバーへのルーティング前にアナウンスを再生（Play announcement before routing to Hunt Member）] • [コールがキューに入る場合アナウンスを再生（Play announcement if call is queued）]
[定期アナウンス（Periodic Announcement）]	定期アナウンスをドロップダウン リストから選択します。 （注） 定期アナウンスを持たない MOH を選択するには、[選択なし（Not Selected）] オプションを選択します。 [詳細表示（View Details）] リンクをクリックすると、次のような定期アナウンスの情報を参照できます。 • [アナウンス ID（Announcement Identifier）] • 説明（Description） • [デフォルトのアナウンス（Default Announcement）] （注） • MOH サーバは、他の設定に関係なく常に定期アナウンスを再生します。 • 外部マルチキャストソースを使用する場合は、MOH サーバからのユニキャストまたはマルチキャストストリームのみが定期的なアナウンスを含みます。外部のブロードキャストソースからの外部マルチキャストストリームには、定期的なアナウンスはありません。
[定期アナウンスの間隔（Periodic Announcement Interval）]	定期アナウンスの間隔を指定する値（秒単位）を入力します。有効な値は 10 ～ 300 です。デフォルト値は 30 です。

フィールド	説明
[アナウンスのロケール（Locale Announcement）]	[アナウンスのロケール（Locale Announcement）] は、インストールされたロケールインストールパッケージによって異なります。 （注） • MOH が再生する音声ガイダンスは、[アナウンスのロケール（Locale Announcement）] の設定を使用します。 • ANN が再生する音声ガイダンスは、発信者のユーザ ロケールを使用します。
MOH オーディオ ソース	
（MOH オーディオ ソースのリスト）	このリストボックスには、追加する MOH オーディオ ソースが表示されます。MOH オーディオ ソースを設定するには、その MOH オーディオ ソースのオーディオ ストリーム番号を選択します。 オーディオ ソース ID は、保留音サーバ内のオーディオ ソースを示す ID です。このオーディオソースには、ディスク上のファイルか、ソース ストリーム保留音サーバがストリーミング データを取得する固定デバイスのどちらかを含めることができます。MOH サーバは、最大で 51 のオーディオ ソース ID をサポートします。オーディオ ソース ID が示す各オーディオ ソースは、必要に応じてユニキャストおよびマルチキャスト モードでストリームできます。 （注） [<なし>（<None>）] を選択すると、MOH オーディオ ソースにはシステムのデフォルトである MOH オーディオ ソース サービス パラメータ（[デフォルトのネットワーク保留 MoHオーディオソースID（Default Network Hold MoH Audio Source ID）]）が使用されます。

フィールド	説明
ファイルのアップロード（Upload File）	ドロップダウン リストに表示されていない MOH オーディオ ソース ファイルをアップロードするには、[ファイルのアップロード（Upload file）] をクリックします。[ファイルのアップロード（Upload File）] ウィンドウで、オーディオ ソース ファイルのパスを入力するか、[参照（Browse）] をクリックしてファイルを指定します。オーディオ ソース ファイルを指定した後、[ファイルのアップロード（Upload File）] をクリックしてアップロードを完了します。オーディオ ファイルがアップロードされた後、[アップロード結果（Upload Result）] ウィンドウにアップロードの結果が表示されます。[閉じる（Close）] をクリックして、このウィンドウを閉じます。 （注） ファイルをアップロードする際、ファイルは Cisco Unified Communications Manager サーバにアップロードされ、オーディオ変換が実行されて、MOH のための指定コーデックのオーディオ ファイルが作成されます。元のファイル サイズによっては、処理が完了するまで数分かかることがあります。 （注） MOH サーバにオーディオ ソース ファイルをアップロードする場合、ファイルは 1 つの MOH サーバのみにアップロードされます。各サーバの Cisco Unified Communications Manager の管理を使用して、クラスタ内の各 MOH サーバにオーディオ ソース ファイルをアップロードする必要があります。MOH オーディオ ソース ファイルは、クラスタ内の他の MOH サーバには自動で反映されません。

iX Transport 暗号化

Cisco Unified Communications Manager リリース11.5 以降では、dlts を使用して既存の iX チャネルサポートの上に暗号化が新しく追加されています。この機能は、ビデオ会議でiXアプリケーションメディアチャネルを暗号化するためのサポートを提供します。これにより、会議参加者の id など、このチャネルで送信される情報のプライバシーが保護されます。

コール暗号化ステータスの考慮に iX メディア回線の暗号化を含めるには、[**サービスパラメータ設定 (service parameter configuration**)] ウィンドウの [クラスタ**全体のパラメータ (Feature-Call Secure status Policy)**] セクションで、[**Secure call Icon Display policy**] ドロップダウンリストから [**bfcp transport] を暗号化する必要があり**ます。

ロケーション認識

ロケーション認識は、リリース 11.5 (1) の新機能です。この機能により、管理者はネットワークインフラストラクチャデバイスを Ciscoユニファイド コミュニケーション マネージャ データベースにインポートできます。Ciscoユニファイドコミュニケーション マネージャ は、この情報を使用して、特定のスイッチまたはワイヤレスアクセスポイントに電話をマッピングします。

ロケーション認識には、次の利点があります。

- Ciscoユニファイドコミュニケーション マネージャ によって、企業ネットワーク内でコールを発信するユーザの物理的な場所を判断できます。ローミングの状況では、モビリティコールをワイヤレスアクセスポイントに追跡することもできます。
- 緊急通報の場合、Cisco Emergency Responder はロケーション認識を使用して緊急サービスを緊急通報者の物理的な場所に誘導します。
- 管理者は、Cisco Unified CM 管理インターフェイス内からアクセスポイントやスイッチなどのネットワークインフラストラクチャデバイスを表示および管理できます。

ロケーション認識の概要

ロケーション認識によって、管理者は企業ネットワークに接続している電話の接続元となる物理的な場所を決定できます。ワイヤレス ネットワークでは、ワイヤレス アクセスポイント インフラストラクチャを表示し、どのモバイルデバイスが現在それらのアクセスポイントに関連付けられているかを確認できます。有線ネットワークでは、イーサネット スイッチ インフラストラクチャを表示し、どのデバイスが現在それらのスイッチに接続しているかを確認できます。これによって、コールが発信されたビル、フロア およびキューブを判別できます。

Ciscoユニファイド コミュニケーション マネージャ の [スイッチとアクセス ポイントの検索と一覧表示（Find and List Switches and Access Points）] ウィンドウでネットワーク インフラストラクチャを表示できます。

この機能では、ユニファイドコミュニケーションマネージャーデータベースを次の情報を使用して動的に更新します。

- 各インフラストラクチャ デバイスの IP アドレス、ホスト名、BSSID 情報（適用可能な場合）を含み、スイッチやワイヤレス アクセスポイントなどのネットワーク インフラストラクチャ デバイス。
- 次を含み、各インフラストラクチャ デバイスに関連付けられたエンドポイント。
  - ワイヤレス ネットワークでは、現在ワイヤレス アクセスポイントに関連付けられているデバイスのリスト。
  - 有線ネットワークでは、現在イーサネット スイッチに接続されているデバイスとデバイス タイプのリスト。

Cisco Emergency Responder の統合

ロケーション認識は、緊急通報を発信するユーザの物理的な場所を判別する Cisco Emergency Responderなどの統合アプリケーションで役立ちます。ロケーション認識を有効にすると、Cisco Emergency Responder は、モバイル デバイスが新しいワイヤレス アクセスポイントに関連付けられた後、またはデスクトップ電話が新しいイーサネット スイッチに接続された後、数分以内にデバイスとインフラストラクチャの新しい関連付けを学習します。

Cisco Emergency Responder 起動すると、まず、現在のデバイスに対するユニファイドコミュニケーションマネージャーデータベースに対して、ネットワークインフラストラクチャの関連付けが照会されます。以降 2 分ごとに、Cisco Emergency Responder は既存の関連付けへの更新をチェックします。その結果、モバイル発信者がローミング状態で緊急通報を発信した場合でも、Cisco Emergency Responder はすぐに発信者の物理的な場所を判別し、適切なビル、フロア、またはキューブに緊急サービスを手配します。

ワイヤレス ネットワークの更新

ワイヤレスインフラストラクチャの位置認識を有効にするには、ユニファイドコミュニケーションマネージャーで、Cisco Wireless LAN コントローラと同期するように設定します。ユニファイドコミュニケーションマネージャーと最大 50 のコントローラを同期できます。同期プロセス中に、ユニファイドコミュニケーションマネージャーは、そのコントローラが管理しているアクセスポイントインフラストラクチャでデータベースを更新します。Cisco Unified CM Manager の管理では、各アクセス ポイントに関連付けられているモバイル クライアントのリストを含み、ワイヤレス アクセス ポイントのステータスを表示できます。

モバイルクライアントがアクセスポイント間を移動すると、モバイルクライアントはエンドポイントからの SIP および SCCP シグナリングマネージャーが、新しいデバイスとアクセスポイントの関連付けを、そのデータベースを更新するユニファイドコミュニケーションマネージャーに伝達します。また、Cisco Emergency Responder は、新しいエンドポイントが関連付けを変更したときに数分ごとにユニファイドコミュニケーションマネージャーデータベースに照会することによって、新しい関連付けについて学習します。その結果、モバイルクライアントが緊急通報の電話をかけると、Cisco Emergency Responder に、電話をかけたユーザがいる物理的な場所の正確な情報が残ります。

ワイヤレスアクセスポイントコントローラの定期的な同期スケジュールがある場合、ユニファイド コミュニケーション マネージャーは、各同期の後にデータベースからのアクセスポイントを動的に追加または更新します。

一括管理を使用したアクセス ポイントの挿入

サードパーティ製のワイヤレスアクセスポイントコントローラを使用している場合、またはCisco の主要インフラストラクチャからアクセスポイントをエクスポートする場合は、バルク管理ツールを使用して、CSV ファイルからのワイヤレスアクセスポイントインフラストラクチャをユニファイドコミュニケーションマネージャデータベースに一括挿入することができます。一括挿入の後に発生するモバイル デバイスの場所の更新により、アクセス ポイントの現在の関連付けでデータベースが更新されます。

ただし、一括管理では、新しいアクセス ポイントがワイヤレス ネットワークに追加される際に、アクセス ポイント インフラストラクチャを動的に更新することはできません。モバイルコールが、一括挿入後に追加されたアクセスポイントを使用して配置された場合、そのアクセスポイントはデータベース内のレコードを持たないため、ユニファイドコミュニケーションマネージャーは新しいアクセスポイントの BSSID と一致しなくても、インフラストラクチャをマークすることになります。、ワイヤレス デバイスの場合は、未識別 AP として使用されます。

一括管理ツールの詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』の「Manage Infrastructure Devices」の章を参照してください。

有線ネットワークの更新

有線インフラストラクチャについて場所の認識を有効にするために何も設定する必要はありません。機能は自動的に有効になります。

有線電話を登録する際、電話機と Ciscoユニファイド コミュニケーション マネージャ の間のシグナリングによって、スイッチ インフラストラクチャでデータベースが動的に更新されます。Cisco Unified CM Administration での会社のスイッチ インフラストラクチャに関する詳細を、特定のスイッチに接続されている電話機のリストも含め表示できます。

モバイルデバイスと異なり、有線デバイスは、通常、1 つのスイッチから別のスイッチにローミングしません。会社内で従業員が席を替わったときなどに起こり得る、電話機が移動しない場合は、電話機が新しい場所から再登録されると、新しいスイッチ情報でデータベースが更新されます。Ciscoユニファイドコミュニケーション マネージャ で、新しいスイッチは移動された電話を接続されたエンドポイントとして表示されます。

スイッチが廃止され、ネットワーク インフラストラクチャから削除される場合、そのスイッチは、Ciscoユニファイドコミュニケーション マネージャ 内で見えたままです。インフラストラクチャのビューから古いスイッチを削除するには、[アクセスポイントとスイッチの設定（Access Point and Switch Configuration）] ウィンドウで非アクティブ化する必要があります。

場所の認識の前提条件

この機能を使用すると、Ciscoユニファイド コミュニケーション マネージャ を複数のシスコ ワイヤレス LAN コントローラと同期できます。また、シスコ ワイヤレス LAN コントローラ

のハードウェアとアクセスポイントのインフラストラクチャをセットアップする必要があります。詳細については、コントローラのドキュメンテーションを参照してください。

Location Awareness の設定タスク フロー

Ciscoユニファイド コミュニケーション マネージャ で Location Awareness をセットアップするには、次のタスクを実行します。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	無線インフラストラクチャ同期のサービスの開始 （79 ページ）	Cisco Unified Serviceability で、Location Awareness 機能をサポートするサービスを開始します。
ステップ 2	ワイヤレス アクセス ポイント コントローラの設定 （79 ページ）	データベースとワイヤレス アクセス ポイント コントローラを同期します。同期すると、無線インフラストラクチャがデータベースにインポートされます。 ヒント 自動更新の同期スケジュールをセットアップします。
ステップ 3	インフラストラクチャ デバイスの挿入 （80 ページ）	これはオプションです。Cisco Prime Infrastructure の無線インフラストラクチャを追加するか、またはサードパーティのワイヤレス LAN コントローラを使用している場合は、一括管理を使用して、CSV ファイルでデータベースを更新します。 （注） このメソッドを使用して、自動更新をセットアップすることはできません。
ステップ 4	インフラストラクチャ デバイス トラッキングの非アクティブ化 （81 ページ）	これはオプションです。同期内容に追跡を望まないアクセス ポイントが含まれている場合（たとえば、同期することでラボのアクセスポイントが制御される場合）は、アクセスポイントを非アクティブにできるため、[Cisco Unified CM の管理（Ciscoユニファイド コミュニケーション マネージャ Administration）] でアクセス ポイントの更新が追跡されることはありません。

無線インフラストラクチャ同期のサービスの開始

場所認識機能に対応するシスコ ワイヤレス LAN コントローラとの同期をサポートするサービスを開始するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）] > [サービスの開始（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択します。

ステップ 3 次のサービスがオンになっていることを確認します。

- **Cisco CallManager**
- **Cisco AXL Web サービス**
- **Cisco Wireless Controller Synchronization サービス**

ステップ 4 これはオプションです。一括管理を使用して CSV ファイルからネットワーク インフラストラクチャをインポートする場合、[一括プロビジョニング サービス（Bulk Provisioning Service）] がオンになっていることを確認します。

ステップ 5 **[保存（Save）]** をクリックします。

ワイヤレス アクセス ポイント コントローラの設定

シスコのワイヤレス アクセス ポイント コントローラとデータベースを同期するには、次の手順を使用します。同期プロセス中に、ユニファイド コミュニケーション マネージャーは、そのコントローラが管理しているアクセスポイントインフラストラクチャでデータベースを更新します。最大 50 のワイヤレス アクセスポイント コントローラを追加できます。

手順

ステップ 1 Cisco Unified CM の管理で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [ワイヤレス アクセスポイント]** を選択します。

ステップ 2 設定するコントローラを選択します。

- **[検索（Find）]** をクリックして、既存のコントローラを編集するコントローラを選択します。
- 新しいコントローラを設定するには、**[新規追加（Add New）]** をクリックします。

ステップ 3 [名前（Name）] フィールドに、コントローラの IP アドレスまたはホスト名を入力します。

ステップ 4 コントローラの [説明（Description）] を入力します。

ステップ 5 コントローラに SNMP メッセージを送信するために使用する SNMP 設定を行います。

a) [SNMP バージョン（SNMP Version）] ドロップダウン リスト ボックスから、コントローラで使用する SNMP バージョン プロトコルを選択します。

b) その他のSNMP認証フィールドを入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。
c) [SNMP 設定のテスト（Test SNMP Settings）] ボタンをクリックし、入力した SNMP 設定が有効であることを確認します。

ステップ 6 スケジュール同期を設定して、データベースを定期的に更新する場合：

a) [インフラストラクチャデバイスを検出するためにスケジュール同期を有効にする（Enable scheduled synchronization to discover Infrastructure Devices）] チェックボックスをオンにします。
b) [再同期の実行間隔（Perform a Re-sync Every）] フィールドで、同期スケジュールを作成します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 （任意） データベースを今すぐ更新するには、[同期（Synchronize）] をクリックします。

オプション同期内容に、追跡を行わないアクセス ポイント（たとえば、研究室用の機器または使用していないアクセス ポイント）が含まれる場合は、アクセス ポイントを追跡の対象から外すことができます。

インフラストラクチャ デバイスの挿入

CSV ファイルから Ciscoユニファイド コミュニケーション マネージャ データベースへのワイヤレス アクセス ポイント インフラストラクチャの一括インポートを行うには、次の手順を実行します。この手順を使用して、Cisco Prime Infrastructure からエクスポートされた CSV ファイルをインポートすることや、サードパーティのワイヤレス アクセス ポイント コントローラからアクセス ポイントをインポートすることも可能です。

始める前に

データ ファイルは、次のように区別された列を含み、カンマ区切り値（CSV）形式にしてしておく必要があります。

- アクセス ポイントまたはスイッチの名前
- IPv4 アドレス（IPv4 Address）
- IPv6 アドレス（IPv6 Address）
- BSSID：ワイヤレス アクセス プロトコル（WAP）のインフラストラクチャ デバイスに必須
- 説明：場所の識別子、スイッチ タイプと場所の組み合わせ、または別の有効な識別子

（注） IPv4 アドレスと IPv6 アドレスの両方を定義することも、そのいずれかを定義することもできます。

（注） BSSID 値には、アクセス ポイントの個別のチャネルの BSSID とは異なり、アクセス ポイントを一意に識別する、0 で終わる BSSID マスクを入力します。

手順

ステップ 1 **[一括管理（Bulk Administration）] > [インフラストラクチャ デバイス（Infrastructure Device）] > [インフラストラクチャ デバイスの挿入（Insert Infrastructure Device）]**.を選択します。
[インフラストラクチャ デバイスの挿入の設定（Insert Infrastructure Device Configuration）] ウィンドウが表示されます。

ステップ 2 [ファイル名（File Name）] フィールドで、このトランザクション用に作成した CSV データ ファイルを選択します。

ステップ 3 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

デフォルトの説明は、[インフラストラクチャ デバイスの挿入（Insert Infrastructure Device）] です。

ステップ 4 ジョブを実行するタイミングを選択します。

- すぐにジョブを実行する場合は、**[今すぐ実行（Run Immediately）]** ラジオ ボタンを選択します。
- 後でジョブを実行する場合は、**[後で実行（Run Later）]** ラジオ ボタンを選択します。

ステップ 5 [送信（Submit）] をクリックします。
ジョブをただちに実行することを選択した場合は、ジョブが実行されます。

ステップ 6 ジョブを後で実行することを選択した場合は、ジョブを実行するスケジュールを設定します。

a) **[一括管理（Bulk Administration）] > [ジョブ スケジューラ（Job Scheduler）]** を選択します。
b) [検索（Find）] をクリックし、作成したジョブを選択します。
c) [ジョブ スケジューラ（Job Scheduler）] ウィンドウで、ジョブを実行するスケジュールを設定します。
d) [保存（Save）] をクリックします。
スケジュールされた時間にジョブが実行されます。

インフラストラクチャ デバイス トラッキングの非アクティブ化

同期の対象に、トラッキングを避けたいスイッチまたはアクセスポイント（たとえば、ラボの機器や使用されていないアクセス ポイントなど）が含まれている場合、そのアクセス ポイントまたはスイッチへのトラッキングを非アクティブ化できます。このアクセスポイントまたはスイッチのステータスは、ユニファイドコミュニケーションマネージャーによって更新されません。

手順

ステップ 1 Cisco Unified CM の管理で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [スイッチとアクセス ポイント（Switches and Access Points）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、追跡を停止するスイッチまたはアクセスポイント選択します。

ステップ 3 [選択項目の非アクティブ化（Deactivate Selected）] をクリックします。

Location Awareness でインフラストラクチャを管理

ロケーション対応機能の一部として、スイッチとワイヤレス アクセスポイントなどのネットワーク インフラストラクチャ デバイスを管理できます。ロケーション対応を有効にすると、Ciscoユニファイド コミュニケーション マネージャ データベースには、各スイッチまたはアクセスポイントに現在関連付けられているエンドポイントのリストを含め、ネットワークのスイッチとアクセスポイントのステータス情報が保存されます。

エンドポイントからインフラストラクチャ デバイスへのマッピングは、Ciscoユニファイド コミュニケーション マネージャ と Cisco Emergency Responder が発信者の物理的な場所を特定するのに役立ちます。たとえば、モバイルクライアントがローミング中に緊急通報を行っている場合、Cisco Emergency Responder はこのマッピングを使用して緊急サービスを送る場所を判断します。

データベースに保存されるインフラストラクチャ情報は、インフラストラクチャの使用状況をモニタするのに役立ちます。Ciscoユニファイド コミュニケーション マネージャ インターフェイスから、スイッチとワイヤレスアクセスポイントなどのネットワーク インフラストラクチャのデバイスを確認できます。現時点で特定のアクセスポイントまたはスイッチに関連付けられているエンドポイントのリストを表示することもできます。インフラストラクチャ デバイスが使用されていない場合は、インフラストラクチャ デバイスをアクティブ化するか非アクティブ化して追跡されないようにできます。

インフラストラクチャの管理の前提条件

Ciscoユニファイド コミュニケーション マネージャ インターフェイス内でワイヤレス インフラストラクチャを管理するには、その前に、ロケーション認識機能を設定する必要があります。有線インフラストラクチャの場合、この機能はデフォルトで有効になっています。設定の詳細については、以下の章を参照してください。

『System Configuration Guide for Cisco Unified Communications Manager』の「Location Awareness」。

また、ネットワーク インフラストラクチャをインストールする必要もあります。詳細については、ワイヤレス LAN コントローラ、アクセス ポイント、スイッチなどのインフラストラクチャ デバイスに付属しているハードウェア ドキュメントを参照してください。

インフラストラクチャの管理のタスク フロー

次のタスクを実行して、ネットワーク インフラストラクチャ デバイスを監視および管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	インフラストラクチャデバイスのステータスの表示 （83 ページ）	ワイヤレス アクセス ポイントまたはイーサネット スイッチの現在のステータスを、関連付けられているエンドポイントの一覧とともに取得します。
ステップ 2	インフラストラクチャ デバイス トラッキングの非アクティブ化 （84 ページ）	使用されていないスイッチまたはアクセス ポイントがある場合は、そのデバイスに非アクティブのマークを付けます。そのインフラストラクチャ デバイスのステータスまたは関連付けられているエンドポイントの一覧が更新されなくなります。
ステップ 3	非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化 （84 ページ）	非アクティブなインフラストラクチャ デバイスのトラッキングを開始します。Ciscoユニファイド コミュニケーション マネージャ が、インフラストラクチャ デバイスのステータスおよび関連付けられているエンドポイントの一覧により、データベースの更新を開始します。

インフラストラクチャ デバイスのステータスの表示

この手順を使用して、ワイヤレス アクセス ポイントやイーサネット スイッチなどのインフラストラクチャ デバイスの現在のステータスを取得します。Ciscoユニファイド コミュニケーション マネージャ インターフェイス内で、アクセス ポイントまたはスイッチのステータスおよび現在関連付けられているエンドポイントの一覧を表示できます。

手順

ステップ 1 Cisco Unified CM の管理で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [スイッチとアクセス ポイント（Switches and Access Points）]** を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 ステータスを表示するスイッチまたはアクセス ポイントをクリックします。

[スイッチおよびアクセス ポイントの設定（Switches and Access Point Configuration）] ウィンドウに、そのアクセスポイントまたはスイッチに現在関連付けられているエンドポイントの一覧を含み、現在のステータスが表示されます。

インフラストラクチャ デバイス トラッキングの非アクティブ化

スイッチやアクセス ポイントなどの特定のインフラストラクチャ デバイスのトラッキングを削除するには、次の手順を使用します。使用されていないスイッチまたはアクセス ポイントで、この手順を実行できます。

（注） インフラストラクチャデバイスのトラッキングを削除すると、デバイスはデータベースに残ったまま、非アクティブになります。Ciscoユニファイドコミュニケーション マネージャは、その後、そのインフラストラクチャデバイスに関連するエンドポイントの一覧も含めて、そのデバイスのステータスを更新しません。[スイッチとアクセス ポイント（Switches and Access Points）] ウィンドウの [関連リンク（Related Links）] ドロップダウンで、非アクティブなスイッチとアクセスポイントを表示できます。

手順

ステップ 1 Cisco Unified CM の管理で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [スイッチとアクセス ポイント（Switches and Access Points）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、追跡を停止するスイッチまたはアクセスポイント選択します。

ステップ 3 [選択項目の非アクティブ化（Deactivate Selected）] をクリックします。

非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化

この手順を使用して、非アクティブ化されたインフラストラクチャデバイスのトラッキングを開始します。スイッチまたはアクセス ポイントがアクティブになると、Ciscoユニファイドコミュニケーション マネージャ では、スイッチまたはアクセス ポイントに関連付けられているエンドポイントの一覧を含むステータスを動的にトラッキングし始めます。

始める前に

Location Awareness を設定する必要があります。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Location Awareness」の章を参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [スイッチとアクセス ポイント（Switches and Access Points）]** を選択します。

ステップ 2 [関連リンク（Related Links）]から、[非アクティブなスイッチおよびアクセス ポイント（Inactive Switches and Access Points）] を選択し、[移動（Go）] をクリックします。
[非アクティブなスイッチおよびアクセス ポイントの検索および表示（Find and List Inactive Switches and Access Points）] ウィンドウに、トラッキングされていないインフラストラクチャ デバイスが表示されます。

ステップ 3 トラッキングを開始するスイッチまたはアクセス ポイントを選択します。

ステップ 4 [選択項目の再アクティブ化（Reactivate Selected）] をクリックします。

IM and Presence サービスでの外部データベース サポートの Microsoft SQL

IM and Presence サービスリリース 11.5 (1) では、Microsoft SQL の外部データベースのサポートが導入されました。

Microsoft SQL Server のインストールと設定

始める前に

- Microsoft SQL データベースのセキュリティの推奨事項については、「セキュリティの推奨事項について」の項を確認してください。
- サポートされているバージョンについては、「外部データベースの設定の要件」を参照してください。
- MS SQL Server をインストールするには、Microsoft のマニュアルを参照してください。

（注） XMPP 仕様に従って、IM and Presence Service ノードでは UTF8 の文字符号を使用します。これにより、ノードは動作時に多数の言語を同時に使用することができ、クライアント インターフェイスで言語の特殊別文字を正しく表示できるようになります。ノードで Microsoft SQL を使用する場合は、UTF8 をサポートするように設定する必要があります。

Microsoft SQL Server Management Studio を使用して MS SQL Server に接続します。

新しい Microsoft SQL Server データベースの作成

新しい Microsoft SQL Server データベースを作成するには、次の手順を使用します。

手順

ステップ 1 SQL サーバと Windows 認証を有効にします。

a) 左側のナビゲーション ウィンドウで、Microsoft SQL Server の名前を右クリックし、[プロパティ（properties）] をクリックします。

b) [SQL ServerとWindows認証モードを有効にする（Enable SQL Server and Windows Authentication mode）] をクリックします。

ステップ 2 左側のナビゲーション ウィンドウで、[データベース（Databases）] を右クリックし、[新しいデータベース（New Database）] をクリックします。

ステップ 3 [データベース名（Database name）] フィールドに適切な名前を入力します。

ステップ 4 [OK] をクリックします。新しい名前が、データベースの下にネストされた左側のナビゲーション ウィンドウに表示されます。

新しいログインとデータベース ユーザの作成

この手順を使用して、新しいログインおよび Microsoft SQL データベース ユーザを作成します。

手順

ステップ 1 左側のナビゲーション ウィンドウで、**[セキュリティ（Security）]** > **[ログイン（Login）]** を右クリックし、[新しいログイン（New Login）] をクリックします。

ステップ 2 [ログイン名（Login name）] フィールドに適切な名前を入力します。

ステップ 3 [SQL Server認証（SQL Server authentication）] チェックボックスをオンにします。

ステップ 4 [パスワード（Password）]フィールドに新しいパスワードを入力し、[パスワードの確認（Confirm password）] フィールドでパスワードを確認します。

ステップ 5 [パスワードポリシーの適用（Enforce password policy）] チェックボックスをオンにします。

（注） [パスワード有効期限ポリシーの適用（Enforce password expiration policy）] が選択されていないことを確認します。このパスワードは、IM and Presence サービスがデータベースに接続するために使用するもので、期限切れであってはなりません。

ステップ 6 [デフォルトのデータベース（Default database）] ドロップダウンリストから、この新しいユーザを適用するデータベースを選択します。

ステップ 7 [ログイン-新規（Login - New）] ウィンドウの左側のナビゲーション ウィンドウで、[ユーザマッピング（User Mapping）] をクリックします。

ステップ 8 [このログインにマップされたユーザ（Users mapped to this login）] リストで、このユーザを追加するデータベースを確認します。

ステップ 9 [ユーザマッピング（User Mapping）] をクリックし、[このペインにマップされたユーザ（Users mapped to this pane）] ペインの [マップ（Map）] 列で、すでに作成したデータベースのチェックボックスをオンにします。

ステップ 10 [サーバロール（Server Roles）] で、[パブリック（public）] ロールのチェックボックスのみがオンになっていることを確認します。

ステップ 11 [OK] をクリックします。**[セキュリティ（Security）] > [ログイン（Logins）]** で、新しいユーザが作成されます。

データベース ユーザ所有者権限の付与

この手順を使用して、Microsoft SQL データベースの所有権をデータベース ユーザに付与します。

手順

ステップ 1 左側のナビゲーション ウィンドウで、[データベース（Databases）] をクリックし、作成したデータベースの名前をクリックして、**[セキュリティ（Security）]**>**[ユーザ（Users）]** をクリックします。

ステップ 2 所有者権限を追加するデータベース ユーザの名前を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 3 [データベースユーザ（Database User）] ペインで、[メンバーシップ（Membership）] をクリックします。

ステップ 4 [ロールメンバー（Role Members）] リストで、[db_owner] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

（オプション）データベース ユーザ アクセスの制限

データベース所有者としてのデータベース ユーザを削除し、Microsoft SQL Server 外部データベースのデータベースユーザにさらにオプション制限を適用する場合は、この手順を使用します。

⚠

注意 IM and Presence サービスのアップグレード中に、データベース スキーマのアップグレードが行われる場合は、データベース ユーザにデータベースの所有者権限が必要です。

手順

ステップ 1 ストアド プロシージャを実行するための新しいデータベース ロールを作成します。

a) 左側のナビゲーション ウィンドウで、[データベース（Databases）] をクリックし、新しいデータベース ロールを追加するデータベースの名前をクリックします。
b) [役割（Roles）] を右クリックし、[新しいデータベースロール（New Database Role）] をクリックします。
c) [データベースロール（Database Role）] ウィンドウで、[全般（General）] をクリックします。
d) [ロール名（Role name）] フィールドに適切な名前を入力します。
e) [セキュリティ設定可能（Securables）] をクリックし、次に [検索（Search）] をクリックして [オブジェクトの追加（Add Objects）] ウィンドウを開きます。
f) [特定のオブジェクト（Specific Objects）] オプション ボタンを選択し、[OK] をクリックします。
g) [オブジェクトタイプ（Object Types）] をクリックして、[オブジェクトタイプの選択（Select Object Types）] ウィンドウを開きます。
h) [オブジェクトタイプの選択（Select Object Types）] ウィンドウで、[ストアドプロシージャ（Stored procedures）] チェックボックスをオンにして、[OK] をクリックします。ストアド プロシージャが [これらのオブジェクトタイプを選択（Select these object types）] ペインに追加されます。
i) [参照（Browse）] をクリックします。
j) [オブジェクトの参照（Browse for Objects）] ウィンドウで、次のチェックボックスをオンします。
   - [dbo][jabber_store_presence]
   - [dbo][ud_register]
   - [dbo][ps_get_affiliation]
   - [dbo][tc_add_message_clear_old]
   - [dbo][wlc_waitlist_update]
k) [OK] をクリックします。新しい名前が [選択するオブジェクト名を入力（Enter the object names to select）] ペインに表示されます。
l) [オブジェクトの選択（Select Objects）] ウィンドウで、[OK] をクリックします。
m) [データベースロール（Database Role）] ウィンドウで、[セキュリティ設定可能（Securables）] リスト内のオブジェクト リストの最初のエントリをクリックします。
n) [明示的（Explicit）] リストで、[実行（Execute）] 権限の [付与（Grant）] チェックボックスをオンにします。
o) [セキュリティ設定可能（Securables）] リストのすべてのオブジェクトに対してステップ 13 と 14 を繰り返します。
p) [OK] をクリックします。

   新しいデータベース ロールが **[セキュリティ（Security）] > [役割（Roles）] > [データベースロール（Database Roles）]** で作成されます。

ステップ 2 データベース ユーザのデータベース ロールのメンバーシップを更新するには、次の手順を実行します。

a) **[セキュリティ（Security）] > [ユーザ（Users）]** で、作成したデータベース ユーザを右クリックし、[プロパティ（Properties）] をクリックします。
b) [データベースユーザ（Database User）] ウィンドウで、左側のナビゲーション ウィンドウにある [メンバーシップ（Membership）] をクリックします。
c) [ロールメンバー（Role Members）] ペインで、[db_owner] チェックボックスをオフにします。
d) [db_datareader]、[db_datawriter] およびステップ 1 で作成したデータベース ロールのチェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

Multiple Device Messaging の概要

Multiple Device Messaging（MDM）により、現在サインインしているすべてのデバイス間で追跡される、1 対 1 のインスタント メッセージ（IM）交換が実現します。デスクトップ クライアントとモバイルデバイスを使用し、どちらも MDM が有効な場合、メッセージは両方のデバイスに送信されるか、または CC で送信されます。既読通知は、会話の参加中に両方のデバイスで継続的に同期されます。

たとえばデスクトップ コンピュータから IM 交換を開始しても、デスクから移動した後はモバイル デバイスで交換を続けることができます。Multiple Device Messaging のフロー （90 ページ）を参照してください。

MDM は、モバイル デバイスのバッテリを節約できる静音モードをサポートします。Jabber クライアントは、モバイル クライアントが使用されていないときは自動的に静音モードに切り替わります。静音モードはクライアントが再びアクティブになるとオフになります。

MDM は、Cisco XCP Message Archiver サービスなどの、MDM をサポートしていないサードパーティ クライアントとの互換性があります。

MDM はバージョン 11.7 以降のすべての Jabber クライアントによりサポートされます。

次の制限が適用されます。

- クライアントはサインインしている必要があります。サインアウトしたクライアントには、送受信された IM および通知は表示されません。
- ファイル転送は、ファイルを送受信したアクティブ デバイスでのみ使用できます。
- グループ チャットはチャット ルームに参加したデバイスでのみ使用できます。
- MDM は、バージョン X8.8 以前の Cisco Expressway 経由でクラウドから IM and Presence Service に接続するクライアントではサポートされません。

MDM の操作方法の詳細については、次の 2 つのフローを参照してください。

Multiple Device Messaging のフロー

このフローでは、ユーザ（Alice）がラップトップとモバイル デバイスで MDM を有効化した際にメッセージと通知がどのように処理されるかについて説明しています。

1. Alice はラップトップ上で Jabber クライアントを開いており、モバイル デバイスでも Jabber を使用しています。
2. Alice は Bob からインスタント メッセージ（IM）を受け取ります。

   Alice のラップトップが通知を受信すると、新しいメッセージ インジケータが表示されます。モバイル デバイスには通知ではなく、新しいメッセージとして表示されます。

（注） IM は必ずすべての MDM 対応クライアントに一斉送信されます。通知はアクティブな Jabber クライアントにのみ表示されます。アクティブな Jabber クライアントがない場合は、すべての Jabber クライアントに通知が送信されます。

3. Alice は 20 分間 Bob とチャットしました。

   ラップトップでチャットする一方、モバイル デバイスでは新しいメッセージを受信し、既読として処理されます。モバイル デバイスには通知が送信されません。
4. Alice は 3 人目のユーザ（Colin）から 3 通のチャット メッセージを受信します。この際も Alice のデバイスはステップ 2 と同じように動作します。
5. Colin からのメッセージには応答せず、ラップトップを閉じます。帰路で Alice は Bob から別のメッセージを受信します。

   この状況では、ラップトップとモバイル デバイスの両方で新しいメッセージを受信し、通知を表示します。
6. Alice はモバイル デバイスを開き、Bob と Colin から送信された新しいメッセージを見つけます。これらのメッセージはラップトップにも送済みです。
7. Alice がモバイル デバイスでメッセージを読むと、メッセージはラップトップとモバイル デバイスの両方で既読になります。

Multiple Device Messaging における静音モードのフロー

このフローでは、モバイル デバイス上で Multiple Device Messaging が静音モードを有効にする手順について説明します。

1. Alice は、ラップトップとモバイル デバイスで Jabber を使用しています。Bob からのメッセージを読み、ラップトップ上の Jabber から返信します。
2. モバイル デバイスで別のアプリケーションを使い始めます。ここで Jabber はバックグラウンドで動作し続けます。
3. Jabber がバックグラウンドで実行している間、静音モードは自動的に有効になります。

4. Bob が Alice に別のメッセージを送信します。Alice のモバイル デバイスでは Jabber が静音モードにあるため、メッセージは配信されません。Alice から Bob への応答メッセージはバッファとして保存されます。
5. メッセージのバッファリングは、次のトリガーイベントのいずれかが発生するまで続きます。
   - <iq> スタンザが受信される。
   - 他の Alice のデバイスでアクティブなクライアントがない場合に、<message> スタンザが受信される。

   （注） アクティブなクライアントとは、過去 5 分間に、使用可能なプレゼンス ステータスまたはインスタント メッセージのいずれかを送信した最後のクライアントのことです。

   - バッファの制限に達した。
6. Alice がモバイル デバイスの Jabber に戻ると、再びアクティブになります。バッファとして保存された Bob のメッセージが配信され、Alice から閲覧可能になります。

Multiple Device Messaging の有効化

Multiple Device Messaging はデフォルトで有効になっています。次の手順を使用して、この機能を有効または無効にすることができます。

手順

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

ステップ 2 [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス パブリッシャ（IM and Presence Service Publisher）] ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco XCP ルータ（アクティブ）（Cisco XCP Router (Active)）] を選択します。

ステップ 4 [マルチデバイス メッセージングの有効化（Enable Multi-Device Messaging）] ドロップダウン リストから [有効（Enabled）] または [無効（Disabled）] を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 Cisco XCP Router サービスを再起動します。

複数のデバイスのメッセージングのカウンタ

Multiple Device Messaging（MDM）は、Cisco XCP MDM カウンタ グループから次のカウンタを使用します。

表 *9:* カウンタ グループ：***Cisco XCP MDM*** カウンタ

カウンタ名	説明
MDMSessions	MDM が有効な現在のセッション数。
MDMSilentModeSessions	サイレント モードにおける現在のセッション数。
MDMQuietModeSessions	静音モードにおける現在のセッション数。
MDMBufferFlushes	MDM バッファ フラッシュの合計数。
MDMBufferFlushesLimitReached	バッファ サイズ全体の上限に到達したことで発生したMDMバッファ フラッシュの合計数。
MDMBufferFlushPacketCount	最後のタイムスライスでフラッシュされたパケットの数。
MDMBufferAvgQueuedTime	MDMバッファがフラッシュされるまでの平均時間（秒）。

ロケーション認識の有用性の更新

新しい機能サービスである**シスコ ワイヤレス コントローラの同期サービス**は、**ロケーションベースのトラッキングサービス**の見出しの下にある Cisco Unified Serviceability に追加されました。このサービスは、ネットワークのワイヤレス アクセス ポイントと関連モバイル デバイスのステータスを提供するロケーション認識機能をサポートします。

シスコ ワイヤレス コントローラ 同期 サービス は Ciscoユニファイド コミュニケーション マネージャ と シスコ ワイヤレス アクセス ポイント コントローラを同期するためにも実行する必要があります。サービスが動作し、同期が設定されると、Ciscoユニファイド コミュニケーション マネージャ は、データベースとシスコのワイヤレス アクセス ポイント コントローラを同期し、コントローラが管理するワイヤレス アクセス ポイントのステータス情報を保存します。最新の情報となるように、一定の間隔で同期が実行されるようにスケジュール設定できます。

ロケーション認識のためのユーザ インターフェイスの更新

ロケーション認識機能のために、2つの新しいユーザインターフェイスウィンドウが追加されました。ユーザインターフェイスのマニュアルは、オンラインヘルプシステムから入手できます。

- **スイッチおよびアクセス ポイントの設定** ウィンドウは Cisco Unified CM 管理から、**詳細機能** > **デバイス ロケーション追跡サービス** > **スイッチおよびアクセス ポイント**を選択することで、アクセス可能です。この設定ウィンドウでは、ロケーション認識機能の一部としてインポートされた特定のスイッチまたはアクセスポイントの詳細を表示できます。
- **スイッチおよびアクセス ポイントの設定** ウィンドウは Cisco Unified CM 管理から、**詳細機能** > **デバイス ロケーション追跡サービス** > **スイッチおよびアクセス ポイント**を選択することで、アクセス可能です。この設定ウィンドウでは、ワイヤレス アクセス ポイントのリストをシスコ ワイヤレス LAN コントローラと同期するように Cisco Unified Communication Manager を設定できます。

スイッチとアクセス ポイントの設定

[スイッチとアクセス ポイントの設定（Switches and Access Point Configuration）] ウィンドウで、スイッチまたはワイヤレス アクセス ポイントのネットワーク設定を表示できます。ここでは、次の 2 つのタイプの情報を表示できます。

- **[インフラストラクチャの詳細（Infrastructure Details）]** セクションでは、特定のスイッチまたはアクセス ポイントに対する IP アドレス、ホスト名、BSSID（該当する場合）などのネットワーク設定を表示します。
- **[関連するエンドポイント（Associated Endpoints）]** セクションでは、スイッチに接続しているエンドポイント、またはワイヤレス アクセス ポイントに関連付けられているエンドポイントを表示します。

Ciscoユニファイド コミュニケーション マネージャ が追跡しているデバイスのリストからスイッチまたはアクセス ポイントを削除するには、**[無効にする（Deactivate）]** ボタンをクリックします。Ciscoユニファイドコミュニケーションマネージャ はこのスイッチまたはアクセスポイントに対する更新を追跡しません。また、このスイッチまたはアクセスポイントについては、エンドポイント情報は追跡されません。

ワイヤレス アクセス ポイント コントローラの設定

次の表に、[ワイヤレスアクセスポイントコントローラの設定（Wireless Access Point Controller Configuration）] ウィンドウのフィールド設定を示します。

表 *10*：ワイヤレス アクセス ポイント コントローラの設定

フィールド	定義
Controller Name	ワイヤレス アクセス ポイント コントローラのホスト名または IP アドレスを入力します。
説明	（オプション）サーバの説明を入力します。 説明には、任意の言語で最大50文字まで入力できます。説明には、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

フィールド	定義
SNMP Version	ドロップダウン リスト ボックスから、ワイヤレス アクセス ポイント コントローラと通信するために Ciscoユニファイド コミュニケーション マネージャ が使用する SNMP バージョンを選択します。可能なバージョンは **1**、**2c** および **3**。 （注） 残りの SNMP の構成時の設定は、選択した SNMP バージョンによって異なります。
SNMP Community String	SNMP 要求に使用されるコミュニティ ストリング値を入力します。このフィールドは、SNMP バージョン 1 または 2c を設定している場合にのみ表示されます。
SNMP User Id	SNMP 通信に使用されるユーザ ID を入力します。このフィールドは、SNMP バージョン 3 の場合にのみ表示されます。
SNMP Authentication Protocol	ドロップダウンから、SNMP メッセージを認証するために使用されるプロトコルを選択します。利用可能なオプションは、**SHA** または **MD5** です。このフィールドは、SNMP バージョン 3 の場合にのみ表示されます。
SNMP Authentication Password	テキストボックスに、Ciscoユニファイドコミュニケーション マネージャ によって SNMP メッセージの認証時に使用される SNMP ユーザ ID とパスワードを入力します。このフィールドは、SNMP バージョン 3 の場合にのみ表示されます。
SNMP Privacy Protocol	ドロップダウン メニューから、SNMP メッセージを暗号化するために使用されるプロトコルを選択します。利用可能なオプションは、**AES-128** または **DES** です。このフィールドは、SNMP バージョン 3 の場合にのみ表示されます。
SNMP Privacy Password	ドロップダウン リスト ボックスから、SNMP メッセージを暗号化するために使用されるパスワードを入力します。このフィールドは、SNMP バージョン 3 の場合にのみ表示されます。
[SNMP設定のテスト（Test SNMP Settings）]	このボタンをクリックすると、設定した SNMP 設定で Cisco ユニファイド コミュニケーション マネージャ がコントローラと通信できるか確認できます。Refer to the **Status** section for the test results.
[ワイヤレスアクセスポイントコントローラ同期スケジュール（Wireless Access Point Controller Synchronization Schedule）]	

フィールド	定義
[スケジュール同期を有効にしてインフラストラクチャ デバイスを検出する（Enable scheduled synchronization to discover Infrastructure Devices）]	ワイヤレス アクセス ポイント コントローラと同期するように Ciscoユニファイド コミュニケーション マネージャ の同期スケジュールをセットアップするには、このチェックボックスをオンにします。時間、日、週、または月の単位で発生するように同期を設定できます。 （注） ワイヤレス アクセス ポイント コントローラと同期するには、その前に **Cisco Wireless Controller Synchronization Service** と **Cisco AXL Web Service** が実行されている必要があります。
[再同期の実行間隔（Perform a Re-sync Every)]	同期スケジュールを設定します。たとえば、テキストボックスに「**2**」と入力し、ドロップダウン メニューから [毎週（Weekly）] を選択すると、同期は隔週で実行されます。
次の再同期時刻（YYYY-MM-DD hh:mm）（Next Re-sync Time (YYYY-MM-DD hh:mm)）	このフィールドには、このワイヤレス アクセス ポイント コントローラと Ciscoユニファイド コミュニケーション マネージャ の間で同期がスケジュールされている次回の時間が表示されます。

ロケーション認識の新しいアラーム

ロケーション認識機能のために、次の新しいリアルタイムモニタリングツールアラームが追加されました。Cisco Unified Serviceabilityで、**アラーム** > **定義** に進みアラーム定義を表示します。

- SwitchesAndAccessPointReached75PercentCapacity
- SwitchesAndAccessPointReached90PercentCapacity
- SwitchesAndAccessPointReached95PercentCapacity
- CiscoWLCSyncServiceDown
- CiscoWLCSyncStarted
- CiscoWLCSyncStartFailure
- CiscoWLCSyncDBAccessFailure
- CiscoWLCSyncDBInsertFailure
- CiscoWLCSyncProcessStarted
- CiscoWLCSyncProcessFailToStart
- CiscoWLCSyncProcessCompleted
- CiscoWLCSyncProcessStoppedManually
- CiscoWLCSyncNoSchedulesFound
- CiscoWLCSyncInvalidScheduleFound

- CiscoWLCSyncSNMPResponseTimeout
- CiscoWLCSyncSNMPv2CommunityStringError
- CiscoWLCSyncSNMPv3AuthenticationError

LSC レポート、一括更新 およびモニタリング強化

リリース 11.5 (1) 以降、 Cisco Unified Communications Managerはデータベース内のエンドポイントのローカルで有効な証明書 (lsc) 情報を保存します。管理者は、 Cisco Unified Communications Managerインターフェイス内から、レポートをモニタし、レポートを生成し、lsc 有効期限情報を一括更新することができます。

この機能には次の更新が行われます。

- **管理者は、一括管理とデバイス電話**の [**電話の検索と一覧表示 (Find and List phone to Update**)] ウィンドウで lsc の有効期限のステータスをモニタできます。管理者は一括管理ツール (BAT) を使用して、電話機の LSCs の一括更新を行うことができます。
- 管理者は、Cisco Unified CM Administration で、LSC の有効期限、lsc 発行者名 および LSC 発行者の有効期限の検索フィルタを使用して、「ファイル内の CAPF レポート」を表示して生成することができます。
- これで、管理者は LSC の有効期限のステータスをモニタし、証明書が期限切れになるという警告を電子メールで送信するようにシステムを設定できるようになりました。証明書モニタリングの電子メールオプションの設定方法についての詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある*Cisco Unified Communications Manager* および *IM and Presence* サービス アドミニストレーション ガイドの「「証明書の管理」」の章を参照してください。
- 管理者は、 **Cisco Certificate Authority Proxy Function (Active)**のサービスパラメータで、問題の日付から 1 ~ 1825 日までの有効期間を設定できるようになりました。以前は、有効期間は 1825 日に設定されており、再設定するオプションはありませんでした。

（注） 上記の機能は、LSCs がCisco Unified Communication Manager 11.5 (1) で生成された場合にのみ使用できます。11.5 (1) へのアップグレード前に LSCs が割り当てられていた場合は、LSCs のレポーティングとモニタリングにこの機能を使用するように LSCs を更新する必要があります。更新されていない以前に使用可能な LSC 機能への影響はありません。

ユーザ インターフェイスの更新

Cisco Unified CM の管理で、[**デバイス** > **の電話 (Device Phone)**] メニューと [**一括管理電話 (Bulk Administration** > **phone**)] メニューの両方を開きます。

[**ユーザの検索/一覧表示 (Find And List Users)**] ウィンドウには、次のフィルタが追加されます。管理者はこれらのフィルタを使用して、Cisco Unified Communications Managerインターフェイス内から lsc の有効期限情報をモニタできます。

- [LSC 有効期日（LSC Expires）]：電話の LSC 有効期日を表示します。
- [LSC 発行元（LSC Issued By）]：発行元の名前を表示します。これは、CAPF またはサードパーティのいずれかです。
- [LSC 発行元の有効期日（LSC Issuer Expires By）]：発行元の有効期日を表示します。

Cisco Unified OS の管理では、[**Certificate Monitor Configuration**] ウィンドウに次のボタンが追加されます。

- **Enable LSC Monitoring**—チェック ボックスはデフォルトでオンになっています。LSC の有効期限のステータスに関する電子メールを受信するには、このチェックボックスをオンにします。LSCの有効期限のステータスをモニタするには、このチェックボックスを有効または無効にします。

アドミニストレーション ガイドの更新

『 Administration Guide 』の次のトピックは、 「LSC レポート、一括更新 およびモニタリング拡張」機能向けに更新されています。この手順を使用して、LSCs が間もなく期限切れになる電話機を特定します。

電話の LSC ステータスの表示および CAPF レポートの生成

この手順を使用して、Cisco Unified Communications Manager インタフェース内からローカルで有効な証明書（LSC）の有効期限情報を監視します。次の検索フィルタは、LSC情報を表示します。

- [LSC 有効期日（LSC Expires）]：電話の LSC 有効期日を表示します。
- [LSC 発行元（LSC Issued By）]：発行元の名前を表示します。これは、CAPF またはサードパーティのいずれかです。
- [LSC 発行元の有効期日（LSC Issuer Expires By）]：発行元の有効期日を表示します。

（注） 新しいデバイスに LSC が発行されていない場合、[LSC 有効期日（LSC Expires）] および [LSC 発行元の有効期日（LSC Issuer Expires by）] フィールドのステータスは [該当なし（NA）]「」に設定されます。

Cisco Unified Communications Manager 11.5(1) へのアップグレード前に LSC がデバイスに発行された場合は、[LSC 有効期日（LSC Expires）] および [LSC 発行元の有効期日（LSC Issuer Expires by）] フィールドのステータスは [不明（Unknown）]「」に設定されます。

手順

ステップ 1 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索条件（Find Phone where）] の最初のドロップダウン リストから、次の基準の 1 つを選択します。

- LSC 有効期日（LSC Expires）
- LSC 発行元（LSC Issued By）
- LSC 発行元の有効期日（LSC Issuer Expires by）

[電話の検索条件（Find Phone where）] の 2 番目のドロップダウン リストから、次の基準の 1 つを選択します。

- が次の日付より前（is before）
- が次の文字列と等しい（is exactly）
- が次の日付より後（is after）
- が次の文字列で始まる（begins with）
- が次の文字列を含む（contains）
- が次の文字列で終わる（ends with）
- が次の文字列と等しい（is exactly）
- が空である（is empty）
- が空ではない（is not empty）

ステップ 3 [検索（Find）] をクリックします。
検出された電話の一覧が表示されます。

ステップ 4 [関連リンク（Related Links）] ドロップダウン リストから [ファイルでの CAPF レポート（CAPF Report in File）] を選択し、[移動（Go）] をクリックします。
レポートがダウンロードされます。

一括管理の更新

クエリトピックを使用した電話の更新は、「LSC レポート、一括更新 およびモニタリング拡張」機能向けに更新されています。この手順を使用して、LSCs が間もなく期限切れになる電話機を特定します。

更新する電話機を決定したら、*Cisco Unified Communications Manager* の一括管理ガイドの「電話機の更新」の章にある既存の手順を使用して、電話機の lscs を更新できます。

ネイティブ キュー アナウンスの強化

Cisco Unified Communications Manager Release 11.5(1) 以降、着信コールが、キューイングが有効なハント パイロットのハント メンバーに接続されている間、キューイング アナウンスを再生する前に、そのコールの状態を接続済みに変更するように設定できます。

新しい **[Connect Inbound Call before Playing Queuing Announcement]** チェックボックスが、以下のトランクおよびゲートウェイ設定ウィンドウに追加されました。

- H.225 トランク（ゲートキーパー制御）
- クラスタ間トランク（非ゲートキーパー制御）
- クラスタ間トランク（ゲートキーパー制御）
- H.323 ゲートウェイ（ゲートウェイ タイプ）
- SIP プロファイル（トランク固有設定）
- MGCP（E1 PRI、T1 PRI、T1 CAS および BRI）

ネイティブキューイングアナウンス拡張機能の一部として、次の制限が追加されています。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』のコール キューイング セクションを参照してください。

- H323 から SIP へのインターワーキング シナリオでは、インターワーキング遅延のために、ネイティブ コール キューイング フローで初期アナウンスメント、MoH、定期アナウンスを聞いたり、コール失敗を見ることがないことがあります。このようなシナリオでは、SIP プロトコルだけを使用します。

iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプトイン制御

このリリースの Ciscoユニファイド コミュニケーション マネージャ には、iOS での Cisco Jabber の SSO ログイン動作を ID プロバイダー（IdP）によって制御するためのオプトイン設定オプションが導入されています。このオプションを使用すると、制御されたモバイル デバイス管理（MDM）環境内で、Cisco Jabber が IdP による証明書ベースの認証を実行できるようになります。

オプトイン制御を設定するには、Ciscoユニファイド コミュニケーション マネージャ で [iOS の SSO ログイン動作（SSO Login Behavior for iOS）] エンタープライズ パラメータを使用します。

（注） このパラメータのデフォルト値を変更する前に、http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html で Cisco Jabber 機能のサポートおよびドキュメントを参照して、SSO ログイン動作と証明書ベースの認証に対する iOS 上での Cisco Jabber のサポートを確認してください。

この機能を有効にするには、iOS Cisco Jabber の SSO ログインの動作設定 （100 ページ）の手順を参照してください。

iOS Cisco Jabber の SSO ログインの動作設定

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 オプトイン制御を設定するには、[SSO の設定（SSO Configuration）] セクションで、[iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータで、[ネイティブ ブラウザの使用（Use Native Browser）] オプションを選択します。

（注） [iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータには次のオプションが含まれます。

- [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。このオプションは、デフォルトで有効です。
- [ネイティブ ブラウザの使用（Use Native Browser）]：このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー（IdP）を利用する証明書ベースの認証を実行します。

  （注） ネイティブブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 **[保存（Save）]** をクリックします。

PIN 同期

PIN 同期機能は、リリース 11.5 (1) の新機能です。これにより、同じエンドユーザ PIN クレデンシャルを使用して、エクステンション モビリティ、会議の現在、モバイルコネクト、Cisco Unity Connection ボイスメールにサインインできます。

機能を有効にするには、以下の手順に従います。

- **Cisco Unified Communications Manager の [Application Server Configuration]** ウィンドウの [**End User PIN Synchronization**] チェックボックスをオンにして、Cisco Unity Connection サーバへの接続を確認する必要があります。

PIN 同期の有効化

PIN 同期を有効にし、 ユーザが、エクステンション モビリティ、開催中の会議、モバイル コネクト および Cisco Unity Connection ボイスメールに同じ PIN を使用してサイン インできるようにするには、次の手順を実行します。

（注） Cisco Unified Communications Manager パブリッシュ データベース サーバが稼働し、そのデータベースのレプリケーションが完了した場合のみ、Cisco Unity Connection と Cisco Unified Communications Manager 間の PIN の同期に成功します。Cisco Unity Connection で PIN の同期に失敗すると、次のエラー メッセージが表示されます。`Failed to update PIN on CUCM. Reason: Error getting the pin.`

（注） PIN の同期が有効で、エンド ユーザが PIN を変更した場合は、Cisco Unified Communications Manager で PIN が更新されます。これは、設定済みの Unity Connection アプリケーション サーバの 1 台以上で PIN の更新に成功した場合のみです。

始める前に

この手順は、アプリケーション サーバを Cisco Unity Connection の設定にすでに接続していることを前提としています。それ以外の場合は、新しいアプリケーションサーバを追加する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 の『 *System Configuration Guide for Cisco Unified Communications Manager* 』の「「Integrate Applications, Configure application Servers 」」 の章を参照してください。

PIN 同期の機能を有効にするには、最初に、Cisco Unity Server に接続するための有効な証明書を Cisco Unified OS の管理ページから Ciscoユニファイド コミュニケーション マネージャ の tomcat-trust にアップロードする必要があります。証明書をアップロードする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-maintenance-guides-list.html の『*Cisco Unified*

Communications Manager アドミニストレーション ガイド』の「「Manage Security Certificates」」の章を参照してください。

Cisco Unity Connection サーバのユーザ ID は、Cisco Unified Communications Manager のユーザ ID と一致する必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [アプリケーション サーバ（Application Servers）]** の順に選択します。

ステップ 2 Cisco Unity Connection の設定を行うアプリケーション サーバを選択します。

ステップ 3 [エンド ユーザの PIN 同期（Enable End User PIN Synchronization）] チェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

セルフケア ユーザ ガイドの更新

共通 PIN 機能については、セルフケア ユーザ ガイドの次のトピックが更新されています。

電話サービスの暗証番号の設定

電話サービス暗証番号は、エクステンション モビリティ、電話会議、モバイル コネクトなどのさまざまなサービスのため、また新しい電話の自己プロビジョニングのために使用されます。入力する PIN は、ユニファイドコミュニケーションマネージャで定義されたクレデンシャルポリシーを満たしている必要があります。たとえば、クレデンシャルポリシーで 7 桁以上の PIN が指定されている場合、入力する PIN は 7 桁以上の長さで、128 桁を超えることはできません。詳細については、システム管理者にお問い合わせください。

手順

ステップ 1 ユニファイド コミュニケーション セルフ ケア ポータルから、**[一般設定（General Settings）]** を選択し、**電話サービス PIN** をクリックします。

ステップ 2 [**新しい電話の PIN**] テキストボックスに pin を入力し、[**新しい電話の PIN の確認**] テキストボックスに PIN を再入力して確認します。

ステップ 3 [保存（Save）] をクリックします。

（注） ネットワーク管理者により暗証番号の同期が有効になっている場合は、エクステンション モビリティ、Conference Now、モバイル コネクト および Cisco Unity Connection ボイスメール ボックスにログインする際に、同じ暗証番号を使用することができます。

一括管理の更新

共通 PIN 機能については、一括管理ガイドの次のトピックが更新されています。

クエリを使用したパスワードおよび PIN のリセット

クエリを使用してユーザを特定し、パスワードと PIN をデフォルト値にリセットすることができます。

手順

ステップ 1 **[一括管理（Bulk Administration）] > [ユーザ（Users）] > [パスワード/暗証番号のリセット（Reset Password/PIN）] > [クエリ（Query）]** の順に選択します。

[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。

ステップ 2 リセットするユーザを特定するには、クエリ フィルタを定義します。

ステップ 3 最初の [ユーザの検索（Find User where）] ドロップダウン リストから、次の条件のいずれかを選択します。

- ユーザ ID（User ID）
- 名
- ミドル ネーム（Middle Name）
- 姓
- マネージャ（Manager）
- 部署名（Department）

2 番目の **[ユーザの検索（Find User where）]** ドロップダウン リスト ボックスから、次の条件のいずれかを選択します。

- が次の文字列で始まる（begins with）
- が次の文字列を含む（contains）
- が次の文字列と等しい（is exactly）
- が次の文字列で終わる（ends with）
- が空である（is empty）
- が空ではない（is not empty）

ステップ 4 必要に応じて適切な検索テキストを指定し、[検索（Find）] をクリックします。

（注） 複数の部署からユーザを選択するには、複数の部署をカンマで区切ってこのフィールドに入力します。たとえば、部署 12 と部署 14 からユーザを選択するには、3 番目のボックスに「12、14」と入力します。操作を別々に行う必要はありません。

ヒント データベースに登録されているすべてのユーザを検索するには、検索テキストを何も入力せずに **[検索（Find）]** をクリックします。

ステップ 5 さらにクエリを定義するには、[AND] または [OR] を選択して複数のフィルタを追加し、ステップ 3 （103 ページ） と ステップ 4 （103 ページ） を繰り返します。

ステップ 6 [検索（Find）] をクリックします。

検出されたユーザのリストが次の分類で表示されます。

- ユーザ ID（User ID）
- 名
- ミドル ネーム（Middle Name）
- 姓
- マネージャ（Manager）
- Department Name
- LDAP 同期ステータス

ステップ 7 [次へ（Next)] をクリックします。

ステップ 8 クエリで定義したすべてのレコードを対象として更新する値を入力します。

- [パスワード（Password）]：ユーザが Cisco Unified IP Phone の [セルフ ケア ポータル（Self Care Portal）] ウィンドウにログオンする際に使用するデフォルト パスワードを入力します。
- [Confirm Password]：パスワードを再入力します。
- [暗証番号（PIN）]：ユーザが Cisco Unified IP Phone にログインするときに使用するエクステンション モビリティ機能用のデフォルト PIN を入力します。
- [暗証番号の確認（Confirm PIN）]：PIN を再入力します。

（注） この PIN を使用してエンド ユーザが Cisco Unity Connection ボイスメールにアクセスできるようにするには、Cisco Unity Connection サーバへの接続用に [アプリケーション サーバの設定（Application Server Configuration）] ウィンドウの [エンドユーザPIN 同期の有効化（Enable End User PIN Synchronization）] チェックボックスをオンにする必要があります。Cisco Unity Connection 内の PIN が正常に更新された場合にのみ、Cisco Unified Communications Manager の PIN が更新されます。

ステップ 9 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

ステップ 10 パスワードまたは PIN の変更方法を選択します。次のいずれかを実行します。

a) すぐにパスワードまたは PIN を変更する場合は、[今すぐ実行（Run Immediately）] をクリックします。

b) 後で変更する場合は、[後で実行（Run Later）] をクリックします。

ステップ 11 パスワードまたは PIN をリセットするためのジョブを作成するには、**[送信（Submit）]** をクリックします。

ステップ 12 このジョブをスケジュールしてアクティブ化するには、[一括管理（Bulk Administration）] メイン メニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

このジョブをスケジュールするか、アクティブ化するには、**[一括管理（Bulk Administration）]** メイン メニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

ヒント　更新されたユーザ数と、エラー コードを含む失敗したレコード数がログ ファイルに表示されます。

カスタム ファイルを使用したパスワードおよび PIN のリセット

ユーザを特定してパスワードと PIN をデフォルト値にリセットするには、テキスト エディタを使用して、ユーザ ID のカスタム ファイルを作成できます。

始める前に

1. パスワードまたは PIN をリセットするユーザ ID を行単位で列挙したテキスト ファイルを作成します。
2. カスタム ファイルを Cisco Unified Communications Manager の最初のノードにアップロードします。

（注）　bat.xlt を使って作成した挿入トランザクション ファイルまたはエクスポート トランザクション ファイルを、リセット トランザクションに使用しないでください。代わりに、リセット対象のユーザ レコードの詳細を含むカスタム ファイルを作成する必要があります。リセット トランザクションには、このファイルだけを使用してください。このカスタム リセット ファイルでは見出しが不要で、ユーザ ID の値を入力できます。

手順

ステップ 1　**[一括管理（Bulk Administration）] > [ユーザ（Users）] > [パスワード/暗証番号のリセット（Reset Password/PIN）] > [カスタムファイル（Custom File）]** の順に選択します。

[ユーザの検索/一覧表示（Find and List Users）] ウィンドウが表示されます。

ステップ 2　**[ユーザの検索/一覧表示（Find and List Users）]** ウィンドウで、次のオプションの中からカスタム ファイルで使用したフィールドを選択します。

- ユーザ ID（User ID）
- 名
- ミドル ネーム（Middle Name）
- 姓
- 部署名（Department）

ステップ 3　**[カスタムファイル（In Custom File）]** ドロップダウン リスト ボックスで、カスタム ファイルのファイル名を選択します。

ステップ 4　[Next] をクリックします。

ステップ 5　**[ユーザパスワード/暗証番号のリセット（Reset Password/PIN for Users）]** ウィンドウで、すべてのレコードに関して更新する値を入力します。

- [パスワード（Password）]：ユーザが **Cisco Unified IP Phone の [セルフ ケア ポータル（Self Care Portal）]** ウィンドウにログオンする際に使用するデフォルト パスワードを入力します。
- [Confirm Password]：パスワードを再入力します。
- [暗証番号（PIN）]：ユーザが Cisco Unified IP Phone にログインするときに使用するエクステンション モビリティ機能用のデフォルト PIN を入力します。
- [暗証番号の確認（Confirm PIN）]：PIN を再入力します。

（注） この PIN を使用してエンド ユーザが Cisco Unity Connection ボイスメールにアクセスできるようにするには、Cisco Unity Connection サーバへの接続用に [アプリケーション サーバの設定（Application Server Configuration）] ウィンドウの [エンドユーザPIN同期の有効化（Enable End User PIN Synchronization）] チェックボックスをオンにする必要があります。Cisco Unity Connection 内の PIN が正常に更新された場合にのみ、Cisco Unified Communications Manager の PIN が更新されます。

ステップ 6 **[ジョブ情報（Job Information）]** 領域に、ジョブの説明を入力します。

ステップ 7 パスワードまたは PIN の変更方法を選択します。次のいずれかを実行します。

a) すぐにパスワードまたは PIN を変更する場合は、[今すぐ実行（Run Immediately）] をクリックします。
b) 後で変更する場合は、[後で実行（Run Later）] をクリックします。

ステップ 8 パスワードまたは PIN をリセットするためのジョブを作成するには、**[送信（Submit）]** をクリックします。

ステップ 9 このジョブをスケジュールしてアクティブ化するには、[一括管理（Bulk Administration）] メイン メニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

このジョブをスケジュールするか、アクティブ化するには、**[一括管理（Bulk Administration）]** メイン メニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

ヒント 更新されたユーザ数と、エラー コードを含む失敗したレコード数がログ ファイルに表示されます。

ユーザ インターフェイス フィールドの説明の更新 Description Updates

次のアプリケーション サーバのフィールドの説明が更新されました。

アプリケーション サーバの設定

次の表では、[アプリケーション サーバ（Application Server）] ウィンドウで利用可能なすべての設定について説明します。各サーバは異なる設定を必要とするので、次の表のすべての設定が各サーバに当てはまるわけではありません。

表 *11* : アプリケーション サーバの設定

フィールド	説明
アプリケーション サーバの情報	
アプリケーション サーバ タイプ	接続先のアプリケーション タイプに対してアプリケーション サーバを選択します。
名前	設定するアプリケーション サーバを特定するための名前を入力します。
IP Address	設定するサーバの IP アドレスを入力します。 （注） IP アドレスが、1 ～ 255 の数字パターンで構成される数値（10.255.172.57 など）であることを確認します。 ヒント Cisco Unity および Cisco Unity Connection では、Cisco Unity および Cisco Unity Connection Administration で定義したのと同じ管理者ユーザ名とパスワードを使用する必要があります。このユーザ ID は、Cisco Unity または Cisco Unity Connection と Cisco Unified Communications Manager Administration との間の認証を提供します。
URL	アプリケーション サーバの URL を入力します。
エンド ユーザ URL	このアプリケーション サーバに関連付けられているエンド ユーザの URL を入力します。
利用可能なアプリケーション ユーザ	このペインは、このアプリケーション サーバに関連付けることのできるアプリケーション ユーザが表示されます。 アプリケーションユーザをこのアプリケーション サーバに関連付けるには、アプリケーション ユーザ（例、CCMAdministrator、CCMSysUser、UnityConnection など）を選択し、このペインの下にある下矢印をクリックします。

フィールド	説明
選択されたアプリケーション ユーザ	このペインには、アプリケーション サーバに関連付けられたアプリケーション ユーザが表示されます。アプリケーション ユーザを削除するには、アプリケーションユーザを選択し、このペインの上にある上矢印をクリックします。アプリケーションユーザを追加するには、[利用可能なアプリケーション ユーザ（Available Application Users）] ペインでアプリケーションユーザを選択し、下矢印をクリックします。 （注） Cisco Unified Communications Manager を **Cisco Unity Connection** と統合するように設定する場合、接続に単一のアプリケーションユーザを選択する必要があります。複数を選択することはできません。
エンド ユーザ PIN 同期を有効化	Cisco Unified Communications Manager と Cisco Unity Connection との間のエンドユーザ PIN 同期を有効化するには、このチェックボックスをオンにします。エンド ユーザは、同じ PIN を使用して、エクステンション モビリティにログインし、自分のボイスメールにアクセスできます。 このチェックボックスを有効化するには、Cisco Unity Server 接続の有効な証明書を、Cisco Unified OS Administration ページから Cisco Unified Communications Manager の [tomcat-trust] にアップロードする必要があります。証明書をアップロードする方法の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の「Manage Security Certificates」の章を参照してください。

ビジネス クライアント向けに更新された Skype を使用するリモート通話制御

このリリースでは、IM and Presence サービスのリモートコール制御機能は、Lync 2013 クライアントからアップグレードされ、Lync 2013 サーバに登録されている Skype for Business 2015 ク

ライアントをサポートしています。この機能により、ユーザはアップグレードされた Skype for Business クライアントを使用して Cisco Unified IP 電話を制御できます。

（注） Skype for Business 2015 クライアントは Lync 2013 クライアントからアップグレード済みでなければならず、Lync 2013 サーバに登録されている必要があります。

Remote Call Control の設定の詳細は、次の URL の *Microsoft Lync* サーバを使用した、*IM and Presence Service on Cisco Unified Communications Manager* のリモート通話コントロール を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html

RSA セキュリティ証明書による、拡張されたキー長のサポート

Ciscoユニファイド コミュニケーション マネージャ および IM and Presence Service 以降では、RSA 証明書/キー タイプの自己署名証明書および CSR 証明書に関して、3072 ビットおよび 4096 ビットの新しいキー長サイズが導入されています。

RTMT に対する SAML ベースのシングル サインオン (SSO)

このリリースでは、RTMT の Windows 版がセキュリティ アサーション マークアップ言語（SAML）SSO をサポートしています。SAML SSO が有効になっている場合、ID プロバイダ（IdP）でシングル サインインした後、RTMT アプリケーションや、サポートされる他のアプリケーション（Ciscoユニファイド コミュニケーション マネージャ など）を起動できます。各アプリケーションに個別にサインインしたり、アプリケーションごとに個別のクレデンシャルを保持する必要はなくなりました。

SAML SSO モードでは、RTMT は最初に Ciscoユニファイド コミュニケーション マネージャ の証明書を追加します。次に、RTMT が IdP サーバにアクセスしようとすると、証明書の受け入れウィンドウがポップアップ表示されます。IdP サーバの詳細を表示するには、このウィンドウの [**表示 (view)**] ボタンをクリックします。証明書を受け入れると、RTMT は IdP サインインページを表示します。

（注） [Certificate 受諾] ウィンドウは、初めてサインインしたときにのみポップアップ表示され、後続のサインインでは表示されません。

この機能の目的は次のとおりです。

- RTMT は、Ciscoユニファイド コミュニケーション マネージャ が SSO モードまたは非 SSO モードのいずれであるかを自動的に検出します。
- SSO 対応 RTMT クライアントは、互換性を確保するために SSO が有効になっていない Ciscoユニファイド コミュニケーション マネージャ でも動作します。

環境に SAML SSO を導入する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-maintenance-guides-list.htmlの『*SAML Sso Deployment Guide for Cisco Unified Communications Applications*』を参照してください。

（注）
- RTMT では、[**Analysis Manager**] タブへのアクセスと [**System** > **Trace] & LOG Central**オプションは、SAML SSO モードではサポートされていません。そのため、これらのオプションにアクセスしようとすると、認証ウィンドウがポップアップ表示され、クレデンシャルを入力するよう要求されます。[認証 (authentication)] ウィンドウで、IdP クレデンシャルの代わりにCiscoユニファイドコミュニケーションマネージャに保存されるクレデンシャルを入力します。

（注） [**Analysis Manager**] タブと [**System** > **Trace & Log Central**] オプションの両方にアクセスするには、[authentication] ウィンドウでいずれかでクレデンシャルを入力します。

- SAML SSO は、RTMT の Windows バージョンでサポートされています。ただし、RTMT の Linux バージョンは SAML SSO をサポートしていません。

RTMT の SAML SSO を設定するには、Ciscoユニファイド コミュニケーション マネージャ で **RTMT に SSO を使用** エンタープライズ パラメータを使用します。この機能を有効にするには、RTMT への SSO の設定 （110 ページ）の手順を参照してください。

RTMT への SSO の設定

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 RTMT に SSO を設定するには、[SSO の設定（SSO Configuration）] セクションで、[RTMT での SSO の使用（Use SSO for RTMT）] パラメータに [True] を選択します。

（注） [RTMT での SSO の使用（Use SSO for RTMT）] パラメータには、次のオプションが含まれます。

- [True]：このオプションを選択すると、RTMT は、SAML SSO ベースの IdP ログイン ウィンドウを表示します。

  （注） 新規インストール時には、[RTMT での SSO の使用（Use SSO for RTMT）] パラメータのデフォルト値は [True] になっています。

- [False]：このオプションを選択すると、RTMT は、基本認証のログイン ウィンドウを表示します。

  （注） [RTMT での SSO の使用（Use SSO for RTMT）] パラメータがない Cisco ユニファイド コミュニケーション マネージャ のバージョンからアップグレードする場合、新しいバージョンに表示されるこのパラメータのデフォルト値は [False] です。

ステップ 3 **[保存（Save）]** をクリックします。

シングル サインオン単一サービス プロバイダー合意

シングル サインオンを使用すると、いずれか 1 つのシスコ コラボレーション アプリケーションにログオンした後、複数のコラボレーション アプリケーションにアクセスできます。Unified Communications Manager リリース 11.5 より前のリリースでは、管理者が SSO を有効にすると、各クラスタ ノードが URL と証明書を使って独自のサービス プロバイダ メタデータ（SP メタデータ）ファイルを作成しました。作成された各ファイルを ID プロバイダ（IDP）サーバに個別にアップロードする必要がありました。IDP サーバがそれぞれの IDP/SAML 交換を個別の合意と見なしたので、クラスタ内のノード数と等しい数の合意が作成されました。

ユーザエクスペリエンスを改善し、大規模な導入でのソリューション全体のコストを削減するために、このリリースでは機能強化されました。現在では、Unified Communications Manager クラスタ（Unified Communications Manager とインスタント メッセージングおよびプレゼンス（IM and Presence））で単一の SAML 合意がサポートされます。

（注） クラスタ全体にわたる単一 SSO 合意の導入では、マルチ サーバ CA 署名付き tomcat 証明書が必要です。したがって、この機能を使用する前に、この Tomcat 証明書を Unified Communications Manager クラスタに必ずインストールしてください。SAML SSO 設定ウィザードは、SSO 有効化の際に Tomcat マルチ サーバ証明書を検査します。

SAML SSO 導入ガイドの更新

『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』からの次のトピックは「Single Sign On Single Service Provider Agreement」機能について更新されています。

SAMLSSOをアクティブにするためのCiscoユニファイドコミュニケーションマネージャの設定

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

ステップ 2 [SAML シングル サインオンの設定（SAML Single Sign-On Configuration）] ウィンドウで、次の [SSOモード（SSO Mode）] フィールドのオプションのいずれかをクリックします。

- [ノードごと（Per Node）]：シングル ノードのサーバ メタデータをアップロードします。
- [クラスタ全体（Cluster wide）]：クラスタの複数のノードのサーバ メタデータをアップロードします。

ステップ 3 [Enable SSO] をクリックします。

ステップ 4 [続行（Continue）] をクリックします。
[SAML シングル サインオンの設定（SAML Single Sign-On Configuration）] ウィンドウに、ステータスおよび tomcat マルチサーバ証明書の詳細が表示されます。

ステップ 5 [クラスタ全体（Cluster wide）] の SSO モードを選択した場合、次の手順を実行します。

a) [マルチサーバ Tomcat 証明書のテスト（Test for Multi-Server Tomcat Certificate）] をクリックします。

b) Tomcat 証明書が有効であれば、[次へ（Next）] ボタンが有効になります。[次へ（Next）] をクリックします。

（注） Tomcat 証明書が無効の場合、[次へ（Next）] ボタンは無効で、それ以上進めません。

IdP メタデータ信頼ファイルをダウンロードするメッセージと手順が表示されます。

ステップ 6 [メタデータのエクスポート（Export Metadata）] をクリックします。
選択する SSO モードによって、ノードまたはクラスタに対する `single agreement.xml` ファイルがダウンロードされます。

次のタスク

信頼の輪をまだ作成していない場合は、この時点で作成するか、または IdP 設定時にタスクをシフトできます。SAML SSO に対して IdP を設定する前に信頼の輪を作成します。

オンライン ヘルプの更新

シングル サインオン シングル サービス プロバイダー契約機能については、 *Cisco Unified CM Administration* のオンラインヘルプの次のトピックが更新されています。

SAML シングル サインオン フィールド

設定	説明
SSO モード	次のオプションのいずれかを選択します。 **クラスタ全体** クラスタモードごとに1つの契約を選択するには、このオプションをクリックします **ノードごと** ノードごとの SSO モードを選択するには、このオプションをクリックします。
Server Name	クラスタ内のすべてのサーバの名前を指定します。
SSO ステータス	次のステータスのいずれかが表示されます。 **SAML** サーバ上で SAML SSO が有効になっていることを示します。 **ディセーブル** サーバ上で SAML SSO が無効になっていることを示します。 Ciscoユニファイド コミュニケーション マネージャ：**[Cisco Unified OS の管理（Cisco Unified OS Administration）] > [セキュリティ（Security）] > [シングル サイン オン（Single Sign On）]** IM and Presence サービス：**[Cisco Unified CM IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] > [セキュリティ（Security）] > [シングル サイン オン（Single Sign On）]**
メタデータの再インポート	**[メタデータの再インポート（Re-Import Metadata）]** アイコンをクリックすると、IdP メタデータ ファイルがパブリッシャからサブスクライバにインポートされます。 （注） このオプションは、パブリッシャ ノードでは [N/A]（該当なし）と表示されます。

設定	説明
前回のメタデータ インポート（Last Metadata Import）	サーバで IdP メタデータが最後にインポートされた時間を示します。SAML SSO セットアップを初めて実行するときには、このフィールドに 「[なし（Never）]」 と表示されます。
Export Metadata	選択した SSO モードに基づいて、[**メタデータのエクスポート (Export metadata**)] をクリックしてメタデータ ファイルをダウンロードします。**クラスタ全体**の SSO モードを選択すると、クラスタ メタデータ ファイルがダウンロードされます。**ノードごと**の SSO モードを選択すると、サーバ メタデータ ファイルがダウンロードされます。 （注） エクスポート メタデータ モードが SSO を有効にするために選択した SSO モードと同期していることを確認します。 指定したサーバの SAML メタデータ ファイルを生成し、ブラウザを使ってダウンロードする必要があります。次に、このメタデータ ファイルを IdP サーバにインポートする必要があります。 **重要** ノードのホスト名またはドメインを変更する場合は、必ずそのノードからメタデータ ファイルをダウンロードし、IdP サーバにファイルを再度アップロードしてください。 **[すべてのメタデータのエクスポート（Export All Metadata）]** ボタンは、SAML SSO 状態がアクティブに設定されているかどうかに関係なく、デフォルトで有効になります。
前回のメタデータ エクスポート（Last Metadata Export）	指定したサーバの SAML メタデータ ファイルが最後にエクスポートされた時間を示します。SAML SSO セットアップを初めて実行するときには、このフィールドに 「[なし（Never）]」 と表示されます。

設定	説明
SSO テスト（SSO Test）	IdP を使用した SAML 設定のテスト結果が表示されます。このテストでは、指定したサーバが IdP を信頼していること および指定したサーバが IdP によって信頼されていることを確認します。サーバと IdP の間の信頼関係は、SAML メタデータ ファイルのエクスポートとインポートが成功したかどうかによって異なります。 次のいずれかの値が表示されます。 **Never** このサーバでテストがまだ実行されていないことを示します。 **Passed** このサーバでテストが成功に実行されたこと およびサーバと IdP が相互に信頼していることを示します。 **不合格** 指定したサーバのテストを試みたが、サーバが IdP を信頼していないか、IdP がサーバを信頼していないか、他の何らかのネットワーク/IdP の問題が原因でテストが成功しなかったことを示します。
テストの実行	**[テストの実行（Run Test）]** をクリックすると、SSO テストが実行されます。SAML SSO を有効化する前に、このテストを実行する必要があります。このテストが成功するまでは、SAML SSO のセットアップを完了できません。このテストを実行するには、管理者権限を持つ LDAP 同期済みユーザが少なくとも 1 人必要です。また、そのユーザ ID のパスワードを知っておく必要もあります。 （注） IdP メタデータ ファイルがサーバにインポートされ、サーバ メタデータ ファイルが IdP サーバにエクスポートされるまでは、このテストを実行することができません。
SAML SSO の有効化（Enable SAML SSO）	**[SAML SSO の有効化（Enable SAML SSO）]** をクリックすると、SAML SSO の設定が開始されます。
IdP メタデータファイルの更新（Update IdP Metadata File）	**[IdP メタデータ ファイルの更新（Update IdP Metadata File）]** をクリックすると、クラスタ内のすべてのサーバの IdP メタデータが更新されます。

設定	説明
すべてのメタデータのエクスポート（Export All Metadata）	**ノードごと**として SSO モードを選択し、[**すべてのメタデータのエクスポート (Export All Metadata)**] をクリックすると、各サーバからの SAML メタデータファイルがエクスポートされます。これらのファイルは、ダウンロードしやすいように圧縮ファイル（.zip）に変換されます。ファイルを解凍してから、各ファイルを IdP にインポートする必要があります。 SSO モードを**クラスタ全体**として選択し、[**すべてのメタデータのエクスポート (Export All Metadata)**] をクリックすると、クラスタの単一の SAML メタデータファイルがエクスポートされます。
すべての無効なサーバの修正（Fix All Disabled Servers）	**[すべての無効なサーバの修正（Fix All Disabled Servers）]** をクリックすると、SAML SSO が無効になっている各サーバでこれが有効になります。
IdP 信頼メタデータ ファイルを表示（View IdP Trust Metadata File）	**[IdP 信頼メタデータ ファイルを表示（View IdP Trust Metadata File）]** をクリックすると、IdP メタデータ ファイルのコピーがダウンロードされます。

セキュアクラスタでのセルフプロビジョニングと自動登録

このリリース以前は、自動登録機能とセルフプロビジョニング機能は、クラスタセキュリティが非セキュアモードに設定されている場合にのみサポートされていました。このリリースでは、クラスタ セキュリティモードが非セキュアまたは混合モードのいずれであるかに関係なく、これらの機能を使用できます。この機能拡張により、管理者は自動登録とセルフプロビジョニングのメリットを失うことなく、UCM クラスタを保護できます。

管理者は、自動登録を使用して、多数の新しい電話機がネットワークに接続されているときにプロビジョニングすることができます。自動登録プロセス中に、 Cisco Unified Communications Managerは事前設定された範囲から電話番号を割り当てます。また、ユニバーサルデバイスと回線テンプレートを適用することにより、 Cisco Unified Communications Managerは電話番号と電話番号の両方にデフォルト設定を割り当てます。

セルフプロビジョニングを使用すると、電話機のユーザは管理者を使用せずに自分の電話機をプロビジョニングできます。新しい電話機がネットワークに接続されると、電話機のユーザが認証できる IVR にダイヤルする機能を使用して、システムに自動登録します。認証に成功すると、電話機はそのユーザのシステムに自動的に設定されます。

自動登録とセルフプロビジョニングの設定の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の *Cisco Unified Communications Manager* の

システム構成ガイドの「自動登録の設定」および「セルフプロビジョニングの設定」の章を参照してください。

セルフプロビジョニングおよび自動登録のためのユーザインターフェイスの更新

この機能の更新をサポートするには、『 *Cisco Unified Communications Manager Administration Online Help Guide* 』で次のユーザインターフェイスの更新が行われました。

- [**Cisco Unified CM**] および [**Cisco Unified CM グループの設定**] ウィンドウの GUI フィールドの動作は、混合モードまたは非セキュアモードのどちらであるかにかかわらず、まったく同じです。
- [Universal Device Template Configuration] ウィンドウの [**Certificate Authority Proxy Function (CAPF) Settings**] セクションに、[**certificate Operation**] ドロップダウンメニューが表示されるようになりました。自動登録またはセルフプロビジョニング中に電話機で LSC をインストールする場合は、[Certificate Operation] フィールドで [Install/Upgrade] を選択する必要があります。

（注） このフィールドを [インストール/アップグレード (Install/Upgrade)] に設定した状態で**Cisco ユニファイド CM**に自動登録する電話の場合、Capf操作の有効期限は既存のエンタープライズパラメータ「capf 操作の有効期限 (日数)」によって制御されます。

コマンドライン インターフェイスの更新

コマンドライン インターフェイス ガイドでは、次のアップデートがユーティリティ ctl に対して行われています。

set-cluster mixed-mode	CTL ファイルを更新し、クラスタを混合モードに設定します。 クラスタ設定を非セキュアモードから混合モードに変更し、自動登録がクラスタですでに有効になっている場合は、次の警告メッセージが表示されます。 "この操作によりクラスタは混合モードに設定されます。少なくとも1つの CM ノードで自動登録が有効になっています。Do you want to continue? (Y/N)"

v.150 コーデックに対するサポート

Cisco Unified Communications Managerリリース 11.5 (1) 以降では、セキュアなコール接続を確立するために、SIP トランク、MLPP および MTP ゲートウェイポートの設定で、V の IOS を設定しますCiscoユニファイド コミュニケーション マネージャ での IOS 設定についての詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの *Cisco Unified Communications Manager* のセキュリティガイド をご覧ください。

V.150 の概要

V.150 Minimum Essential Requirements 機能により、IP ネットワーク経由でモデムから安全なコール発信が可能になります。この機能は、モデムとテレフォニーデバイスが従来の公衆電話交換網（PSTN）で稼働している大規模なインストール ベースに対しダイヤルアップ モデムを使用します。V.150.1 勧告では、PSTN 上のモデムおよびテレフォニー デバイスと IP ネットワーク間でのモデム経由でのデータのリレー方法について、具体的に定義されています。V.150.1 は、ダイヤルアップ モデム コールをサポートしている IP ネットワークでのモデムの使用に関する ITU-T 勧告です。

Cisco V.150.1 Minimum Essential Requirements 機能は、国家安全保障局（NSA）の SCIP-216 Minimum Essential Requirements（MER）for V.150.1 勧告の要件に準拠しています。SCIP-216 勧告により既存の V.150.1 要件が簡素化されました。

Cisco V.150.1 MER 機能は次のインターフェイスをサポートしています。

- Media Gateway Control Protocol（MGCP）T1（PRI と CAS）および E1（PRI）トランク
- Session Initiation Protocol（SIP）トランク
- アナログ ゲートウェイ ポイント向けの Skinny Client Control Protocol（SCCP）
- Secure Communication Interoperability Protocol-End Instruments（SCIP-EI）

Cisco V.150.1 MER の前提条件

システムですでに基本的なコール制御機能がセットアップされている必要があります。コール制御システムをセットアップする手順については、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_0_1/sysConfig/CUCM_BK_C733E983_00_cucm-system-configuration-guide.html にある『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

Unified Communications Manager の次のいずれかのリリースがインストールされている必要があります。

- 最小バージョンはリリース 10.5(2) SU3 です。
- 11.0 の最小バージョンは 11.0(1) SU2 です（2016 年春に公開）。
- 11.5(1) 以降のすべてのリリースではこの機能がサポートされています。
- Cisco IOS リリース 15.6(2)T 以降が必要です。

V.150 は、メディア ターミネーション ポイント（MTP）ではサポートされていません。V.150 コールを処理するデバイス、トランク およびゲートウェイから MTP を削除することが推奨されます。

V.150 設定のタスク フロー

Unified Communications Manager で V.150 のサポートを追加するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループ設定のタスク フロー（120ページ）を行うには、次のサブタスクを実行します。 • 非 V.150 エンドポイントのメディア リソース グループの設定（120ページ） • 非 V.150 エンドポイントのメディア リソース グループ リストの設定（121 ページ） • V.150 エンドポイントのメディア リソース グループの設定（121 ページ） • V.150 エンドポイントのメディア リソース グループ リストの設定（122 ページ）	V.150 デバイスおよび非 V.150 デバイスのメディア リソース グループおよびメディア リソース グループ リストを追加します。
ステップ 2	Cisco V.150（MER）に対応したゲートウェイの設定（122 ページ）	ゲートウェイに V.150 機能を追加します。
ステップ 3	#unique_173	MGCP ゲートウェイ全体で V.150 サポートを使用するには、ポートインターフェイスに V.150 サポートを追加します。
ステップ 4	#unique_174	SCCP ゲートウェイ全体で V.150 サポートを使用するには、ポートインターフェイスに V.150 サポートを追加します。
ステップ 5	電話での V.150 サポートの設定（123 ページ）	V.150 コールを発信する電話に V.150 サポートを追加します。
ステップ 6	SIP トランク設定のタスク フロー（124 ページ）を行うには、次のサブタスクのいずれかまたは両方を実行します。 • クラスタ全体の V.150 フィルタの設定（125 ページ） • SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加（126 ページ）	V.150 コールに使用する SIP トランクに V.150 サポートを追加します。

メディア リソース グループ設定のタスク フロー

2 つのメディア リソース グループ セット（非 V.150 コール用の MTP リソースからなるメディア リソース グループと、V.150 コール用の MTP リソースが含まれないメディア リソース グループ）を設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	非 V.150 エンドポイントのメディア リソース グループの設定 （120 ページ）	非 V.150 エンドポイントで使用する MTP を含むメディア リソース グループを設定します。
ステップ 2	非 V.150 エンドポイントのメディア リソース グループ リストの設定 （121 ページ）	非 V.150 エンドポイントの MTP メディア リソースが含まれているメディア リソース グループ リストを設定します。
ステップ 3	V.150 エンドポイントのメディア リソース グループの設定 （121 ページ）	セキュア V.150 コール用の MTP リソースが含まれていないメディア リソース グループを設定します。
ステップ 4	V.150 エンドポイントのメディア リソース グループ リストの設定 （122 ページ）	メディア リソース グループに必要なリソースを追加した後で、MTP のない非 V.150 エンドポイント用のメディア リソース グループ リストを設定します。

非 V.150 エンドポイントのメディア リソース グループの設定

非 V.150 エンドポイントの MTP リソースのメディア リソース グループを新たに追加するには、次の手順に従います。

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource Group]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[名前(Name)]** フィールドに、メディア リソース グループ名として「「Do not use with V.150 devices」」と入力します。

ステップ 4 [Available Media Resources] フィールドで MTP デバイスだけを選択し、下矢印キーをクリックします。
選択されたデバイスが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

非 V.150 エンドポイントのメディア リソース グループ リストの設定 （121 ページ）

非 V.150 エンドポイントのメディア リソース グループ リストの設定

非 V.150 エンドポイントの MTP リソースのメディア リソース グループ リストを新たに追加するには、次の手順に従います。

始める前に

非 V.150 エンドポイントのメディア リソース グループの設定 （120 ページ）

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource Group List]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[名前(Name)]** フィールドに、メディア リソース グループ リストの名前として「「Non-V.150」」と入力します。

ステップ 4 **[Available Media Resources]** フィールドで、「「Do not use with V.150 Devices」」という名前の V.150 MER リソース グループを選択し、下矢印キーをクリックします。
選択されたデバイスが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

V.150 エンドポイントのメディア リソース グループの設定

V.150 デバイスに対し、MTP リソースのない新しいメディア リソース グループを追加するには、次の手順に従います。

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource Group]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[名前(Name)]** フィールドに、メディア リソース グループ名として「「For use with V.150 devices」」と入力します。

ステップ 4 [Available Media Resources] フィールドで MTP リソースを除く複数のデバイスを選択し、下矢印キーをクリックします。
選択されたデバイスが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

V.150 エンドポイントのメディア リソース グループ リストの設定 （122 ページ）

V.150 エンドポイントのメディア リソース グループ リストの設定

V.150 デバイスの MTP リソースのメディア リソース グループ リストを追加するには、次の手順に従います。

始める前に

V.150 エンドポイントのメディア リソース グループの設定 （121 ページ）

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource Group List]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[名前(Name)]** フィールドに、メディア リソース グループ リストの名前として「「V.150」」と入力します。

ステップ 4 **[Available Media Resources]** フィールドで、「「For V.150 Devices」」という名前の V.150 MER リソース グループを選択し、下矢印キーをクリックします。
選択されたメディア リソース グループが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

Cisco V.150（MER）に対応したゲートウェイの設定

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ (Gateway)]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ゲートウェイタイプ (Gateway Type)] ドロップダウン リストからゲートウェイを選択します。

ステップ 4 [次へ（Next)] をクリックします。

ステップ 5 [Protocol] ドロップダウン リストから、プロトコルを選択します。

ステップ 6 ゲートウェイに対して選択するプロトコルに応じて、次のいずれかを実行します。

- MGCP の場合は、[Domain Name] フィールドに、ゲートウェイで設定されているドメイン名を入力します。
- SCCP の場合は、[MAC Address (Last 10 Characters)] フィールドにゲートウェイ MAC アドレスを入力します。

ステップ 7 **[Unified Communications Manager Group]** ドロップダウン リストから **[Default]** を選択します。

ステップ 8 [Configured Slots、VICs and Endpoints] 領域で次の手順を実行します。

a) 各 [Module] ドロップダウン リストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュール ハードウェアに対応するスロットを選択します。

b) 各 [Subunit] ドロップダウン リストで、ゲートウェイにインストールされている VIC を選択します。

c) **[保存（Save）]** をクリックします。
ポートのアイコンが表示されます。各ポートのアイコンは、ゲートウェイで使用可能なポート インターフェイスに対応します。ポート インターフェイスを設定するには、該当するポートのアイコンをクリックします。

ステップ 9 [VPN Gateway Configuration] ウィンドウでその他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

次のいずれかを実行します。

- #unique_173または
- #unique_174

電話での V.150 サポートの設定

電話に V.150 のサポートを追加するには、次の手順を使用します。V.150 をサポートする電話のタイプは次のとおりです。

- Cisco 7962：Cisco 7962 として登録されているサード パーティ SCCP エンドポイント
- 7961G-GE：Cisco 7961G-GE として登録されているサード パーティ SCCP エンドポイント
- サード パーティ AS-SIP エンドポイント

始める前に

必ず目的の電話番号と同じユーザ ID を使用してエンド ユーザを作成してください。

サードパーティ AS-SIP SIP エンドポイントの [エンド ユーザ設定（End User Configuration）] ウィンドウの [ダイジェスト クレデンシャル（Digest Credentials）] フィールドを必ず設定してください。

新しいエンド ユーザの設定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「「Provision End Users Manually」」の章を参照してください。

手順

ステップ 1 [Cisco Unified Communications Manager Administration] から、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 既存の電話で V.150 を設定するには、[検索（Find）] をクリックして電話を選択します。
- 新しい電話で V.150 を設定するには、[新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウンリストから、V.150 をサポートする電話のタイプを選択し、[次へ（Next)] をクリックします。

ステップ 4 Cisco 7962 として登録されているサードパーティ SCCP エンドポイントの場合：[Device Protocol] ドロップダウン リストから [SCCP] を選択し、[次へ（Next)] をクリックします。

ステップ 5 [Media Resource Group List] ドロップダウン メニューから [V.150] を選択します。

ステップ 6 サード パーティ AS-SIP SIP エンドポイントのみ。次のフィールドを設定します。

- [Digest User] ドロップダウンからこの電話のエンドユーザを選択します。このエンドユーザがダイジェスト認証に使用されます。
- [メディア ターミネーション ポイント必須（Media Termination Point Required）] チェックボックスはオフのままにします。
- [音声とビデオ コールの Early Offer サポート（Early Offer support for voice and video calls）] チェックボックスをオンにします。

ステップ 7 **[保存（Save）]** をクリックします。
[Apply Config] のメッセージ ウィンドウが表示されます。

ステップ 8 [設定の適用（Apply Config）] をクリックします。

ステップ 9 [OK] をクリックします。

SIP トランク設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	V.150 の SIP プロファイルの設定 （125 ページ）	SIP プロファイルで SIP トランクの SIP Best Effort Early Offer サポートを設定します。
ステップ 2	クラスタ全体の V.150 フィルタの設定（125 ページ）	オプション。クラスタ全体での SIP V.150 SDP オファー フィルタリングのデフォルト設定を行います。

	コマンドまたはアクション	目的
ステップ 3	SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （126 ページ）	特定の SIP トランクに割り当て可能な SIP トランク セキュリティ プロファイル内で V.150 フィルタを設定します。
ステップ 4	V.150 の SIP トランクの設定 （127 ページ）	V.150 コールを処理する SIP トランクで V.150 サポートを設定します。

V.150 の SIP プロファイルの設定

SIP プロファイルで SIP トランクの SIP Best Effort Early Offer サポートを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。
- 既存のプロファイルを選択するには、[検索（Find）] をクリックして SIP プロファイルを選択します。

ステップ 3 [名前(Name)] フィールドに、V.150 の SIP 名を入力します。

ステップ 4 [説明（Description)] フィールドに、V.150 の説明を入力します。

ステップ 5 [Early Offer Support for Voice and video class] ドロップダウンリストから [Select Best Effort (no MTP inserted)] を選択します。

ステップ 6 必要なその他の設定値を入力します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

クラスタ全体の V.150 フィルタの設定

クラスタ全体での SIP V.150 SDP オファー フィルタリングのデフォルト設定には、次の手順を使用します。

（注） SIP トランク セキュリティ プロファイル内の [SIP V.150 SDP Offer Filtering] 値に、クラスタ全体のサービス パラメータ設定とは異なる値を設定すると、このセキュリティ プロファイル設定により、そのセキュリティ プロファイルを使用するトランクのクラスタ全体のサービス パラメータ設定がオーバーライドされます。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム(System)]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからアクティブなサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 [Clusterwide Parameters (Device- SIP)] セクションで [SIP V.150 SDP Offer Filtering] サービス パラメータの値を設定します。

ステップ 5 ドロップダウン リストから [SIP V.150 SDP Offer Filtering] を選択します。

ステップ 6 目的のフィルタリング アクションを指定します。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （126 ページ）

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加

SIP トランク セキュリティ プロファイル内で V.150 フィルタを割り当てるには、次の手順を実行します。

（注） SIP トランク セキュリティ プロファイルの [SIP V.150 SDP Offer Filtering] に、クラスタ全体のサービス パラメータとは異なる値を設定すると、このセキュリティ プロファイル設定は、そのセキュリティ プロファイルを使用するトランクのクラスタ全体のサービス パラメータ設定をオーバーライドします。

始める前に

クラスタ全体の V.150 フィルタの設定 （125 ページ）

手順

ステップ 1 [Cisco Unified CM Administration] から **[システム(System)]** > **[セキュリティ（Security）]** > **[SIP Trunk Security Profile]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の SIP トランク セキュリティ プロファイルの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、リストから既存のプロファイルを選択します。
- 新しい SIP トランク セキュリティ プロファイルを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [SIP V.150 SDP Offer Filtering] ドロップダウン リストの値を設定します。

（注） デフォルト設定では、クラスタ全体のサービス パラメータ [SIP V.150 Outbound SDP Offer Filtering] の値が使用されます。

ステップ 4 [SIP Trunk Security Profile Configuration] ウィンドウのその他のフィールドをすべて設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

V.150 の SIP トランクの設定 （127 ページ）

V.150 の SIP トランクの設定

SIP トランクの設定を行うには、次の手順に従います。

始める前に

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （126 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[Add New] をクリックします。
- 既存のトランクを選択するには、[Find] をクリックして SIP トランクを選択します。

ステップ 3 新しいトランクの場合は次の手順に従います。

- [Trunk Type] ドロップダウンリストから [SIP Trunk] を選択します。
- [Protocol Type] ドロップダウンリストから、[SIP] を選択します。
- [Trunk Service Type] ドロップダウン リストから [None(Default)] を選択します。
- [次へ（Next)] をクリックします。

ステップ 4 [名前(Name] フィールドに SIP トランク名を入力します。

ステップ 5 [説明(Description)] フィールドに SIP トランクの説明を入力します。

ステップ 6 **[Media Resource Group List]** ドロップダウンリストから、「「V.150」」という名前のメディア リソース グループ リストを選択します。

ステップ 7 SIP トランクの宛先アドレスを設定します。

a) [Destination Address] テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv4 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

b) 宛先が DNS SRV レコードの場合は [Destination Address is an SRV] チェック ボックスをオンにします。
c) 宛先を追加するには、[+] ボタンをクリックします。SIP トランクには最大 16 個の宛先を追加できます。

ステップ 8 [SIP Trunk Security Profile] ドロップダウンリストから、このトランクに設定した SIP トランク セキュリティプロファイルを割り当てます。

ステップ 9 [SIP Profile] ドロップダウンリストから、[Best Effort Early Offer] 設定でセットアップした SIP プロファイルを割り当てます。

ステップ 10 [Media Termination Point Required] チェックボックスはオフのままにします。

ステップ 11 [Trunk Configuration] ウィンドウのその他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 12 **[保存（Save）]** をクリックします。

Unified Communications Manager のアップグレード

オーディオストリームの不均一なレベル保護転送エラー修正 (ULPFEC)

以前のリリースの Ciscoユニファイド コミュニケーション マネージャ では、ビデオストリームの前方誤り訂正 (FEC) のみがサポートされていました。このリリースでは、Ciscoユニファイド コミュニケーション マネージャ はオーディオストリームの X ULPFECUC もサポートしています。このサポートにより、エンドポイントとインフラストラクチャ アプリケーションは、メディアパケット損失の復元力が向上し、ユーザに高品質な音声品質を提供します。この機能は、パブリックインターネット、ビジネスツービジネス (B2B)、モバイルおよびリモートアクセス (MRA) ソリューションを通過する会議中の音声品質を向上させます。

Expressway 経由での SIP 登録用ユーザ認証

リリース 11.5 (1) では、Ciscoユニファイド コミュニケーション マネージャ は、Expressway 経由でCiscoユニファイドコミュニケーションマネージャに登録しているモバイルおよびリモートアクセスユーザの、ユーザ認証をサポートしています。SIPインターフェイスには、Expressway から受信した着信 SIP REGISTER 要求の Contact ヘッダーに userid フィールドが含まれるようになりました。

Expressway がモバイルまたはリモートアクセス電話から SIP 登録メッセージを受信すると、ユーザ id フィールドが連絡先ヘッダーに追加され、REGISTER メッセージが Ciscoユニファイド コミュニケーション マネージャ にリレーされます。Ciscoユニファイド コミュニケーショ

ン マネージャ は、データベース内の次の値に対して着信登録要求のユーザを承認し、登録要求を承認または拒否します。

- **電話の設定** ウィンドウで設定されている電話の**所有者ユーザ ID**。
- **エンドユーザ設定**でデバイスコントローラとして関連付けられているすべてのユーザの**ユーザ ID** 。

SIP Registration Authorization Enabledサービスパラメータを使用して、ユーザ認証を有効または無効にすることができます。これは、このリリースで新規です。デフォルトでは、ユーザ認証は有効になっています。

許可の例

Ciscoユニファイド コミュニケーション マネージャ は、次のシナリオで、Expressway から到着する SIP REGISTER メッセージの登録を受け入れます。

- 着信 SIP REGISTER メッセージには、userid フィールドは表示されません。
- SIP REGISTER メッセージの userid は、[***Phone Configuration***] ウィンドウの [**owner User ID**] フィールドに割り当てられている電話の所有者、または [**End User Configuration**] ウィンドウでそのデバイスが制御対象デバイスとしてリストされているユーザの**ユーザ ID**の**いずれか**に一致します。

  （注） 電話の**所有者のユーザ ID**設定がデバイスを制御するユーザの**ユーザ ID**と異なる場合でも、1つの一致がある限り、登録は成功します。

  複数のユーザがデバイスコントローラとして電話機に関連付けられている場合、登録要求は、登録を成功させるために、デバイスコントローラまたは電話の所有者と1つの一致だけを必要とします。

- Ciscoユニファイド コミュニケーション マネージャ では、デバイスを所有または制御するようにユーザが設定されていません。たとえば、デバイスには [**電話の設定 (Phone Configuration**)] ウィンドウで**オーナーユーザ ID**が割り当てられておらず、そのデバイスが**エンドユーザ設定**の制御対象デバイスとしてリストされているユーザはありません。

Ciscoユニファイド コミュニケーション マネージャ は、次のシナリオで401の不正な応答で登録要求を拒否します。

- REGISTER メッセージの userid フィールドが、[**電話の設定 (Phone Configuration**)] ウィンドウで設定されている**オーナーユーザ id**またはデバイスコントローラとして設定されているエンドユーザの**ユーザ id**のいずれとも一致しません。
- SIP REGISTER メッセージには、連絡先ヘッダーに複数の userid が含まれています。

- SIP REGISTER メッセージ内の userid＝"」。デバイスエントリに**オーナーユーザ ID**が設定されている Ciscoユニファイドコミュニケーション マネージャ、またはユーザがデバイスコントローラとして電話機に関連付けられている場合。

SIP 登録拒否の新しいアラーム

新しい重大度4警告アラーム (**Authorizationerror)** がリアルタイムモニタリングツールに追加されました。このアラームは、ユーザ認証の失敗が原因で、Ciscoユニファイドコミュニケーション マネージャ が Expressway から受信した登録試行を拒否するインスタンスをカバーします。新しいアラームは、アラームの**Endpointtransientconnection**セットの理由コード**35**として追加されました。

表 *12 :* アラームの *EndpointTransientConnection* セットの認証アラーム

Alarm Value	定義
35	**認証エラー**：（SIP デバイスのみ）次のいずれかの理由によりデバイス登録が失敗しました。1）SIP REGISTER メッセージの連絡先ヘッダーにある userID が、Unified CM に設定されている値と一致しない（[電話の設定（phone configuration）] ページの所有者ユーザ ID および [エンドユーザ（End User）] ページのデバイスに関連付けられたユーザ ID）。または 2）SIP REGISTER メッセージの連絡先ヘッダーに複数の userID が存在する場合。どちらの状況もセキュリティ リスクです。 上記のように Unified CM の設定を確認して、認可されたユーザがこの特定のデバイスを登録しようとしているかどうかを確認します。

EndpointTransientConnection アラームの完全なリストについては、 *Cisco Unified Communications Manager* のマネージド サービス ガイドを参照してください。

ビデオ コーデック 設定の更新

Cisco Unified Communications Managerリリース 11.5 (1) では、ビデオコーデックのネゴシエーション順序の設定が更新されました。次の表に、このリリースと以前のリリースの順序の設定を示します。

表 *13 : 11.5 (1)* のビデオコーデック設定の更新

11.5 (1) の新しい優先順序	以前のリリースの優先順序
• H.265 • H.264 AVC • H.264 SVC • H.264 UC • H.264 1998 • H.323 • H.261	• H.265 • H.264 SVC • H.264 UC • H.264 AVC • H.264 1998 • H.323 • H.261

この更新の一環として、h.264 AVC コーデックは優先順位の順になっています(以前は4番目)。これらのコーデックよりも優れた相互運用性を提供するため、h.264 SVC または h.264 UC よりも前にネゴシエートされます。

（注） 以前のリリースでは、H.265 ビデオコーデックは「ベストエフォート」ベースでのみサポートされていました。このリリースでは、バージョン H.265 が完全にサポートされています。

ウェブ ブラウザのサポート

この機能は、各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 11.5 ウェブアプリケーションへのシームレスなアクセスをサポートする ウェブブラウザを提供します。たとえば、Cisco ユニファイド CM の管理、Cisco Unified Serviceability および Cisco Unified オペレーティングシステムの管理などです。このリリース以降、次の Web ブラウザがサポートされています。

- Windows 10 (64 ビット) での Firefox: 最新のブラウザ バージョンのみ
- Windows 10 (64 ビット) の Chrome: 最新のブラウザ バージョンのみ
- Windows 10 (64 ビット) を使用した Internet Explorer 11
- Windows 8.1 (64 ビット) を使用した Internet Explorer 11
- Windows 7 (64 ビット) を使用した Internet Explorer 11
- Windows 10 を使用した Edge ブラウザ (32 ビット/64 ビット)
- MacOS (10. x) を使用した Safari: 最新のブラウザ バージョンのみ

Ciscoユニファイド コミュニケーション マネージャ クライアントの Windows 10 サポート

このリリースの Ciscoユニファイド コミュニケーション マネージャ では、Microsoft Windows 7 と Microsoft Windows 10 (32 ビットおよび64ビット) の両方のオペレーティングシステムでのインストール、操作 およびアンインストールがサポートされています。次の Unified CM クライアントに対するこれらの操作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 セキュリティトークンアドバイザリ (CTL クライアント)
- Windows 向け Cisco Unified Real-Time Monitoring Tool（RTMT）
- Cisco Unified CM Assistant Console (IPMA)

マネージャ アシスタント ユーザ ガイドおよびオンラインヘルプの更新

『*Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager*』からの次のトピックがCiscoユニファイド コミュニケーション マネージャ クライアント向け Windows 10 のサポート機能に追加されました。

サポートされるプラットフォーム

IP Manager Assistant（IPMA）プラグインは、次のオペレーティング システムでテスト済みで、サポートされています。

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10

（注） IPMA プラグインは、Linux オペレーティング システムではサポートされていません。

RTMT ガイドの更新

『*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』の次のトピックは、Ciscoユニファイド コミュニケーション マネージャ クライアント機能の Windows 10 サポート用に更新されています。

さらに、Windows 98 および XP のインスタンスはサポートされなくなったため、削除されています。

Cisco Unified Real-Time Monitoring Tool のインストールとセット アップ

ここでは、KDE または GNOME クライアントで Windows 8.1、Windows 10、Windows 2000、Windows Vista、7、または Linux を実行するコンピュータで解像度 800*600 以上に対して動作する Cisco Unified Real-Time Monitoring Tool のインストールとセットアップの詳細について説明します。

Unified RTMT の起動

始める前に

Windows Vista、Windows 7、Windows 8.1 または Windows 10 のシングル サインオンのため、Unified RTMT を管理者として実行します。

（注） ルートまたは中間 CA 証明書が RSASSA-PSS シグニチャアルゴリズムを使用している場合は、この CA を使用して tomcat 証明書に署名しないでください。それ以外の場合、RTMT は起動しません。これは、1.2 を介した TLS バージョンが RSASSA-PSS シグニチャアルゴリズムをサポートしておらず、今後の TLS バージョンでこのサポートを追加するために Java に対してバグが開かれているためです。

手順

ステップ 1 プラグインをインストールしたら、Unified RTMT を開きます。

Windows Vista、Windows 7、Windows 8.1 または Windows 10 クライアントがあり、シングル サインオン機能を使用する場合は、デスクトップまたはスタート メニューの Unified RTMT のショートカットを右クリックして[管理者として実行]をクリックします。タイムゾーンを同期するように選択した場合は、アプリケーションがロードされて再起動するまで少し時間を置いてください。

重要 Windows 7 または Vista で RTMT を起動する前に、ユーザ アカウント制御（UAC）機能が無効になっていることを確認します。UAC 機能の詳細については、https://docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uacを参照してください。

ステップ 2 [ホスト IP アドレス（Host IP Address）] フィールドに、ノードまたはクラスタ内のノード（該当する場合）の IP アドレスまたはホスト名を入力します。

ステップ 3 [OK] をクリックします。

- シングル サインオン機能が有効になっている場合、Unified RTMT はユーザ名とパスワードを要求しないため、ステップ 8 に進みます。
- シングル サインオンが有効になっていない場合、Unified RTMT はユーザ名とパスワードを求める別のウィンドウを表示します。以下のステップに示すように詳細を入力します。

ステップ 4 [ユーザ名（User Name）] フィールドに、アプリケーションの管理者ユーザ名を入力します。

ステップ 5 [パスワード（Password）]フィールドに、ユーザ名に対して設定した管理者ユーザパスワードを入力します。

（注） 認証が失敗した場合、またはノードにアクセスできない場合、ノードおよび認証の詳細を再入力するよう要求するプロンプトがツールで表示されます。[キャンセル（Cancel）] ボタンをクリックしてアプリケーションを終了することもできます。認証に成功すると、Unified RTMT はローカル キャッシュから、またはバックエンドのバージョンに一致するモニタリング モジュールがローカル キャッシュに含まれていない場合にはリモート ノードから、モニタリング モジュールを起動します。

ステップ 6 プロンプトが表示されたら、[はい（Yes）] をクリックして証明書ストアを追加します。

Unified RTMT が起動します。

（注） シングル サイン オン機能を使用してサインインした場合、次のメニューのいずれかをクリックすると、Unified RTMT は一度だけユーザ名とパスワードの入力を要求します。

- **[システム（System）] > [パフォーマンス（Performance）] > [パフォーマンス ログ ビューア（Performance log viewer）]**
- **[システム（System）] > [ツール（Tools）] > [トレースおよびログ中央]**
- **[システム（System）] > [ツール（Tools）] > [ジョブのステータス（Job status）]**
- **[システム（System）] > [ツール（Tools）] > [Syslog ビューア（Syslog Viewer）]**
- **[音声/ビデオ（Voice/Video）] > [CallProcess] > [セッション トレース（Session Trace）]**
- **[音声/ビデオ（Voice/Video）] > [CallProcess] > [着信側トレース（Called Party Tracing）]**
- **[音声/ビデオ（Voice/Video）] > [レポート（Report）] > [学習パターン（Learned Pattern）]**
- **[音声/ビデオ（Voice/Video）] > [レポート（Report）] > [SAF フォワーダ（SAF forwarders）]**
- **Analysis Manager**

次のタスク

Unified RTMT の使用だけに限定されたプロファイルを持つユーザを作成できます。ユーザは Unified RTMT にフル アクセスできますが、ノードを管理する権限がありません。

管理インターフェイスに追加し、RealtimeAndTraceCollection の定義済み標準グループにユーザを追加しても Unified RTMT ユーザを新しいアプリケーションのユーザを作成できます。

ユーザとユーザ グループの追加方法の詳細な手順については、『*Administration Guide for Cisco Unified Communications Manager*』および『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified Analysis Manager のインストールとセットアップ

ここでは、KDE または GNOME クライアントで Windows 8.1、Windows 10、Windows 2000、Windows Vista、または Linux を実行するコンピュータで解像度 800*600 以上に対して動作する Cisco Unified Real-Time Monitoring Tool のインストールの詳細について説明します。

（注） Windows オペレーティング システム プラットフォームで RTMT を 実行するには、少なくとも 128 MB のメモリが必要です。

セキュリティ ガイドの更新

Cisco Unified Communications Manager のセキュリティガイドの次のトピックは、Ciscoユニファイド コミュニケーション マネージャ クライアント機能の Windows 10 サポートについて更新されています。

Cisco CTL クライアントの設定について

デバイス認証、ファイル認証およびシグナリング認証は、証明書信頼リスト（CTL）ファイルの作成に依存します。このファイルは、シスコの証明書信頼リスト(CTL)をインストールして設定すると作成されます。

CTL ファイルには、次のサーバまたはセキュリティ トークンのエントリが含まれています。

- System Administrator Security Token（SAST）
- 同じサーバ上で実行されている Cisco CallManager サービスと Cisco TFTP サービス
- Certificate Authority Proxy Function（CAPF）
- TFTP サーバ（複数の場合あり）
- ASA ファイアウォール
- ITLRecovery

CTLファイルには、サーバごとのサーバ証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名 および IP アドレスが含まれています。

CTL ファイルを作成したら、Cisco CallManager サービスと Cisco TFTP サービスが実行されているすべてのノード上の [Cisco Unified Serviceability] でこれらのサービスを再起動する必要があります。電話が次回初期化されたときに、その電話ではこのCTL ファイルをTFTP サーバからダウンロードします。CTL ファイルに自己署名証明書が含まれた TFTP サーバのエントリがある場合、電話では .sgn 形式の署名付き設定ファイルを要求します。TFTP サーバに証明書が含まれていない場合、電話では署名なしのファイルを要求します。

Cisco CTL クライアントが CTL ファイルにサーバ証明書を追加した後、次の CLI コマンドを実行して CTL ファイルを更新できます。

utils ctl set-cluster mixed-mode
CTL ファイルを更新し、クラスタを混合モードに設定します。
utils ctl set-cluster non-secure-mode
CTL ファイルを更新し、クラスタを非セキュア モードに設定します。
utils ctl update CTLFile
クラスタ内の各ノードの CTL ファイルを更新します。

CTL ファイルにファイアウォールを設定すると、セキュアな Unified Communications Manager システムの一部として Cisco ASA ファイアウォールを保護できます。ファイアウォール証明書が「「CCM」」証明書として表示されます。

（注）
- パブリッシャ ノードで CLI コマンドを実行する必要があります。
- CallManager 証明書を再生成すると、ファイルの署名者が変更されることに注意してください。デフォルトのセキュリティをサポートしていない電話は、電話から CTL ファイルが手動で削除されない限り、新しい CTL ファイルを受け入れません。電話機の CTL ファイルの削除の詳細については、お使いの電話機モデルの『Cisco IP 電話 Administration Guide』を参照してください。

Windows 用の Cisco CTL クライアントのインストール

Windows Vista、Windows 7、Windows 8.1、Windows 10 へ Cisco CTL クライアントをインストールするには、次の手順を実行します。

手順

ステップ 1 クライアントをインストールする Windows ワークステーションまたはサーバから、『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って [Unified Communications Manager Administration] を参照します。

ステップ 2 [Unified Communications Manager Administration] で、**[アプリケーション（Application）]** > **[プラグイン(Plugin）]** を選択します。

[Find and List Plugins] ウィンドウが表示されます。

ステップ 3 [Plugin Type equals] ドロップダウン リスト ボックスから [Installation] を選択し、[検索（Find）] をクリックします。

ステップ 4 Cisco CTL クライアントを探します。

ステップ 5 ファイルをダウンロードするには、ウィンドウ左側、Cisco CTL クライアント プラグイン名の反対にある [ダウンロード（Download）] をクリックします。

ステップ 6 [保存 (Save)] をクリックして、ファイルを適切な場所に保存します。ファイルの場所を控えておいてください。

ステップ 7 インストールを開始するには、[Cisco CTL Client]（ファイルの保存場所によりアイコンまたは実行ファイル）をダブルクリックします。

（注） または、[Download Complete] ボックスで [オープン（Open）] をクリックします。

ステップ 8 Cisco CTL クライアントのバージョンが表示されたら、[次へ（Next)] をクリックします。

ステップ 9 インストール ウィザードが表示されます。[次へ（Next)] をクリックします。

ステップ 10 使用許諾契約に同意して、[次へ（Next)] をクリックします。

ステップ 11 クライアントをインストールするフォルダを選択します。デフォルトの場所を変更する場合は、[Browse] をクリックし、場所を選択して [次へ（Next)] をクリックします。

ステップ 12 インストールを開始するには、[次へ（Next)] をクリックします。

ステップ 13 インストールが完了したら、[完了（Finish）] をクリックします。

Windows での eToken パスワードの変更

重要 この情報は CTL クライアント暗号化オプションに適用されます。セキュリティ トークンが不要な **utils ctl**utils ctl **utils ctl**CLI コマンド セットを使用して暗号化を設定することもできます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

Windows Vista、Windows 7、Windows 8.1、Windows 10 のサーバまたはワークステーションでセキュリティ トークンのパスワードを変更するには、次の手順を実行します。

手順

ステップ 1 Windows サーバまたはワークステーションに Cisco CTL クライアントがインストールされていることを確認します。

ステップ 2 インストールされていない場合は、Cisco CTL クライアントをインストールしてある別の Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンを挿入します。

ステップ 3 インストールされていない場合は、Cisco CTL クライアントをインストールしてある別の Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンを挿入します。

ステップ 4 **[Start]** > **[Programs]** > **[etoken]** > **[Etoken Properties]** を選択し、**[etoken]** を右クリックして **[Change etoken password]** を選択します。

ステップ 5 [Current Password] フィールドに、このトークン用に最初に作成したパスワードを入力します。

ステップ 6 新しいパスワードを入力します。

ステップ 7 確認のためもう一度新しいパスワードを入力します。

ステップ 8 [OK] をクリックします。

TAPI および JTAPI クライアント向け Windoes 10 サポート

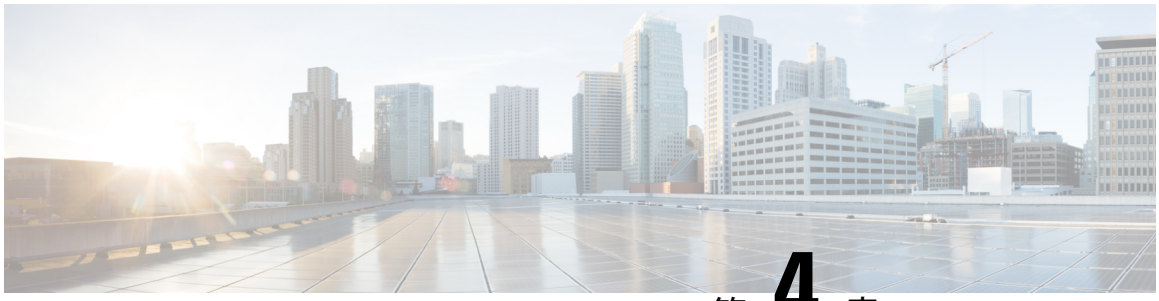
Ciscoユニファイドコミュニケーションマネージャ のこのリリースでは、次のクライアントの Microsoft Windows 10 (32 ビットおよび 64 ビット) オペレーティングシステムでのインストール、操作 およびアンインストールがサポートされています。

- Cisco Unified TAPI クライアント (32 ビットおよび x64 クライアント)
- Windows 用 Cisco Unified JTAPI クライアント (32 ビットおよび x64 クライアント)

[Cisco Spark リモート デバイス（Cisco Spark Remote Device）]

ライセンスや MTP の挿入が不要であり、詳細なバグ修正が含まれているため、ハイブリッド導入には Cisco Spark リモート デバイス（Spark-RD）を強くお勧めします。このオプションを使用するには、Unified CM 10.5(2)SU5、11.0(1a)SU3、または 11.5(1)SU3 を使用する必要があります。サポート対象外のリリースについては、代わりに CTI-RD を使用しますが、これにはライセンスや MTP の挿入が必要です。サポート対象のリリースでの手動作成と自動作成については、新規のアクティブ化に Cisco Spark-RD を使用する必要があります。以前のリリースで作成した CTI-RD は、Cisco Spark-RD に移行するまでは、引き続き機能します。

Hybrid Call Services の Cisco Spark リモートデバイスとサポートされている設定の詳細については、を参照してください。 http://www.cisco.com/go/hybrid-services-call



第 4 章

特記事項

機能とサービス

Media Sense は Selective Recording でコンサルト コールを記録しない

選択的な録音が設定されている場合、Media Sense サーバでは転送中のコンサルト コールは録音されません。たとえば、エージェントと顧客間のコールが録音中であり、エージェントが次のエージェントにコールの転送を開始した場合、コールが転送される前にこの別のエージェント間で発生するコンサルト コールは録音されません。

コンサルト コールが必ず録音されるようにするには、エージェントはコンサルト コールの開始時に [録音（Record）] ソフトキーを押す必要があります。

OVA 要件およびユーザ キャパシティ

導入のサイジングを行う際は、OVA 要件を考慮して、以下のガイドラインに従ってください。

- マルチ クラスタ環境では、最小限の OVA を 15,000 ユーザに導入することを推奨します。
- 常設チャットの展開には、少なくとも15,000 ユーザ OVA を導入することを推奨します。
- 中央集中型の導入の場合は、最小 OVA 25,000 ユーザでが推奨されます。

（注） Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

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

Note that if you edit the setting of the **SDL Listening Port** service parameter、you must restart the **Cisco CTIManager** service on all cluster nodes where the service is running. 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。

相互運用性

Unified CM ノードへの AXL リクエスト

スケジュール用に Cisco TelePresence Management Suite (TMS) を実行している場合は、それを追加したノードで、エンドポイント情報を取得するために複数の AXL クエリを送信します。TMS が生成する負荷のため、AXL を使用する他のアプリケーション (Cisco Emergency Responder または Cisco Unified Attendant Console など) を設定して、これらのノードに AXL 要求を送信することを推奨します。

Cisco Unified Attendant Console サポート

この情報はCSCva12833に適用されます。

Cisco Unified Attendant Console リリース 11.x 以前は、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 11.5 (1) と互換性がありません。Cisco Unified Attendant Console Advanced リリース 11.0.1 にインストールまたはアップグレードする必要があります。

詳細については、ここを参照してください。

Expressway-C との IM and Presence サービスの相互運用性

Cisco Unified IM and Presence サービスリリース 11.5(1) および Expressway-C を相互運用するには、最小バージョンの Expressway-C X8.8 を実行している必要があります。IM and Presence サービス 11.5(1) では、旧バージョンの Expressway-C はサポートされていません。

すでに使用されている以前のリリースからアップグレードする場合は、お使いのシステムを X8.8 にアップグレードしてください。Expressway-C をアップグレードした後、IM and Presence サービスをアップグレードできます。

SAML SSO 展開での Tomcat 証明書の再生成

SAML SSO 展開内で Tomcat 証明書を再生成する場合は、Ciscoユニファイド コミュニケーション マネージャ で新しいメタデータファイルを生成し、そのメタデータファイルを IdP にアップロードする必要もあります。

IM and Presence Service

Cisco Unified Presence 8.6 でサポートされていないクラスタ間ピアリング

Cisco Unified Presence 8.6 は、Cisco Unified IM and Presence サービス 11.x のクラスタ間ピアとしてはサポートされていません。サポートされているクラスタ間ピア設定については、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/11_x/cucm_b_cucm-imp-compatibility-matrix-11x.html#CUP0_RF_I0092C6B_00の*Cisco Unified Communications Manager*と *IM and Presence* サービスの互換性マトリックスを参照してください。

IM and Presence Service ノードの使用不可後に高可用性をリセットする

このドキュメントの更新については、CSCuz86028 を参照してください。

IM and Presence Service ノードの停止中に、たとえばノードのリブートやノードのネットワーク停止などによって発生します。その結果、高可用性フェールオーバーが発生した場合は、高可用性 (HA) をリセットしたフォールバックが発生したことを確認してください。

これを行うには、まず HA を無効にしてから、Ciscoユニファイド コミュニケーション マネージャ の**プレゼンス冗長性グループの設定**ウィンドウで HA を有効にします。

Jabber への IM and Presnce サーバの Ping は設定できない

IM and Presence サーバは、2 回の 1 分間の ping の後にクライアントからキープアライブを受信しない場合に、ユーザのプレゼンスステータスを使用不可として更新します。

これらの ping のタイミングは、サーバ側でハードコードされており、設定できません。

IM and Presence サブスクライバ ノードの再起動

UCS サーバのクラッシュで発生する可能性がある 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 サービスパブリッシャノードが両方とも使用できない場合は、サブスクライバノードが回復しない可能性があるため、IM and Presence サービス サブスクライバ ノードを再起動しないでください。Jabberユーザがログインできない可能性があり、それにより、IM and Presence クラスタを再構築する必要が生じる場合があります。

IM and Presence サブスクライバ ノードを再起動する前に、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 サービスパブリッシャノードが稼働していることを確認してください。

その他

88xx SIP 電話への帯域幅割り当て

SIP プロトコルを使用して 88 xx 電話機を導入する場合は、これらの電話機が Ciscoユニファイド コミュニケーション マネージャ に登録する際に推奨される 32 kbps よりも多くの帯域幅を使用することに注意してください。APIC EM コント ローラーで QoS 帯域幅の割り当てを設定するときは、登録に際してのこの高い帯域幅の要件を必ず考慮してください。

Dialed Number Analyzer はシングル サインオンをサポートしていない

Dialed Number Analyzer はシングル サインオンをサポートしていない

Ciscoユニファイド コミュニケーション マネージャ にサービス機能としてインストールされた Dialed Number Analyzer (DNA) はシングル サインオン (SSO) をサポートしていません。非 SSO モードを使用して、アプリケーションにログインします。非 SSO モードを使用してログインした後は、SSO ログインせずに Ciscoユニファイド コミュニケーション マネージャ Administration にアクセスできます。

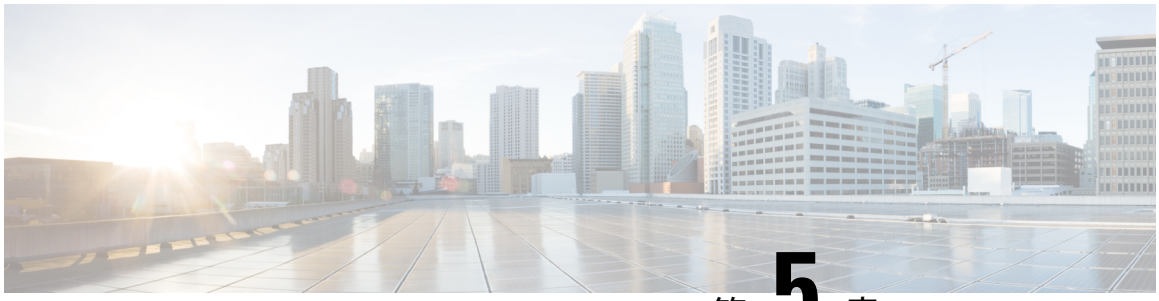
DNA にアクセスするには、ブラウザで次の URL を入力します。

https://<cm-machine>/dna、ここでこの <cm-machine> には、Dialed Number Analyzer をインストールするノード名または IP アドレスを指定します。

ルート フィルタとコールのルーティング

コールルーティングを設定するときは、1 つのルートフィルターを多数のコールのルーティングに割り当てないようにします。ルートフィルタを使用するすべてのコールのルーティングのコール ルーティングを更新するために必要な追加のシステム処理が原因で、数百の関連するコールのルーティングがあるルートフィルタを編集すると、システムコアが発生する可能性が

あります。発生しないようにするには、重複するルートフィルタを作成します。詳細については、CSCup04938 を参照してください。



第 5 章

欠陥についてのマニュアルの更新

アドミニストレーション ガイド

発信側または着信側トランスフォーメーションは、発信側または着信側トランスフォーメーション CSS を使用してヒットできる

このドキュメントの更新により、CSCvc90159 が解決されます。

次のトランスフォームパターンに関する情報は、『 *Administration Guide* 』の「 *Configure transformation patterns* 」の章では省略されています Ciscoユニファイド コミュニケーション マネージャ。

次のことが可能です。

- 着信側トランスフォーメーション CSS が指定された発信側トランスフォーメーション パターンをヒットします。

- 発信側トランスフォーメーション CSS が指定された着信側トランスフォーメーション パターンをヒットします。

証明書モニタ頻度間隔

このドキュメントの更新により、CSCvc32210 が解決されます。

次の注意事項は、『*Cisco Unified Communications Manager* のアドミニストレーション ガイド』の「「証明書満了のモニター」」の手順では省略されています。 。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

電話機のファームウェアの管理に関する情報が不足している

このドキュメントの更新により、CSCvc69988 が解決されます。

「Cisco Unified Communications Manager のアドミニストレーションガイド」の「デバイスファームウェアの管理」の章では、次のタスクが欠落しています。

- 電話モデルのデフォルト ファームウェアの設定
- 電話機のファームウェア ロードの設定
- ロード サーバの使用

詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.htmlの『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』を参照してください。

新しいシステム ロール

このドキュメントの更新により、CSCvc54694 が解決されます。

次の表では、*Cisco* ユニファイド コミュニケーション マネージャ*IM* およびプレゼンスサービスのアドミニストレーション ガイド の 「ユーザ アクセスの管理」 の章 および*Cisco Unified Communications Manager* のシステム設定ガイド の 「ユーザ アクセスの設定」から省略されている新しいフィールドを説明します。

表 *14 :* 標準権限、特権 およびアクセス コントロール グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準 SSO 設定管理	SAML SSO の設定をすべての面で管理できます。	
標準機密アクセス レベル ユーザ	すべての機密アクセス レベル ページにアクセスできます。	標準 Cisco Call Manager 管理
標準 CCMADMIN 管理	CCMAdmin システムをすべての面で管理できます。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準 CCMADMIN 読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準CUReporting	アプリケーション ユーザが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM およびプレゼンスのレポーティング

[デバイス] ページの電話タイプのロゴ

このドキュメントの更新により、CSCvf80788 が解決されます。

次の注意事項は『*Cisco Unified Communications Manager* のアドミニストレーションガイド』の「Install a Device Pack Or Cisco Options Package File」で更新されました。

（注） デバイスパッケージのインストール後に[デバイス]ページに、電話タイプのロゴが表示されない場合は、すべてのノードで tomcat サービスを再起動します。

証明書の再作成

このドキュメントの更新により、CSCuz82667 が解決されます。

次の情報は、『 *Administration Guide for Cisco Unified Communications Manager AND IM And* 在席サービス』の「証明書の再生成」に記載されています。

証明書の詳細ページで **[再生成（Regenerate）]** ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

3072 または 4096 の新しいキー長の自己署名証明書を再生成するには、[自己署名証明書の生成（Generate Self-Signed Certificate）] をクリックします。

一括管理ガイド

テキストベースの CSV ファイル作成時の誤ったテキストエディタ

このドキュメントの更新により、CSCvd21759 が解決されます。

「Cisco Unified Communications Manager の一括管理ガイド」のテキストベースの *CSV* ファイルの章では、Microsoft メモ帳などのテキストエディタを使用して CSV データファイルを作成できます。CSV データファイルを作成するための正しいテキストエディタは、Notepad++ です。

Notepad++ などのテキスト エディタを使用すると、[エンコーディング（Encoding）] ドロップダウン リストから [バイト オーダー マーク（BOM）なしの UTF-8（UTF-8 without Byte Order Mark (BOM)）] を選択できます。

IP アドレスおよびホスト名の変更、

Unified オペレーティング システム GUI を使用して IP アドレスまたはホスト名を変更する

このドキュメントの更新により、CSCvc70649 が解決されます。

以下の情報は、*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 サービスの *IP* アドレスとホスト名の変更 の 「IP アドレスおよびホスト名の変更」 の章から削除されています。

IP アドレスまたはホスト名を変更すると、自己署名証明書が自動的に再生成されます。これにより、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできるようになります。クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

コマンドライン インターフェイス リファレンス ガイド

パスワード ユーザ セキュリティと utils ネットワーク接続の設定の更新

このドキュメントの更新により、CSCvf52786 が解決されます。

set password user security

次の注は、「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 リファレンスガイド」の「「コマンド設定」」の章の「パスワード ユーザ セキュリティの設定」のトピックから削除されています。

（注） IM およびプレゼンス サービス サーバ（ノード）の `set user password security` コマンドを実行する前に、各 IM およびプレゼンス サービス サーバ（ノード）用の**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [CUCM パブリッシャ（CUCM Publisher）]** ウィンドウに最初に移動し、新しいセキュリティ パスワードを入力します。

utils network connectivity

次の情報は、「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 リファレンスガイド」の「「ユーティリティ コマンド」」の章の「ユーティリティ ネットワーク接続」のトピックから省略されています。

ユーティリティネットワーク接続コマンドは、リモートノードへのノードネットワーク接続を確認します。

utils network connectivity

このコマンドは、クラスタ内の最初のノード（この接続は後続のノードでのみ有効）とリモート ノードとのノード ネットワーク接続を確認します。

utils network connectivity [{**reset**}] [*hostname/ip address*]

```
utils network connectivity  [hostname/ip address] [port-number] [timeout]
```

構文の説明

パラメータ	説明
connectivity	このコマンドは、クラスタの最初のノードに対するノードネットワーク接続を確認します。 また、2 つの必須パラメータ **hostname/ip address** および **port-number** があるリモートノードへの接続をチェックするためにも使用されます。
reset	（任意）前の戻りコードをクリアします。

パラメータ	説明
hostname/ip address	• （オプション）パブリッシャまたは最初のノードとのネットワーク接続を確認するためのクラスタノードのホスト名またはIP アドレス。 • （必須）リモート サーバでのネットワーク接続を確認するために、TCP 接続についてテストする必要があるホストのホスト名または IP アドレス。
port-number	（必須）接続テストが必要なホストのポート番号。
timeout	（オプション）ポート接続メッセージが表示されるまでの時間を秒単位で指定します。

コマンド モード

管理者（admin:）

使用上のガイドライン

- **utils network connectivity** ［**reset**］ *[hostname/ip address]* コマンドは、パブリッシャまたは最初のノードへのネットワーク接続をチェックするために使用されます。
- **utils network connectivity** ［**hostname/ip address**］［**port-number**］ *[timeout]* コマンドは、リモート サーバへのネットワーク接続を確認するために使用されます。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

適用対象：Unified Communications Manager、Unified Communications Manager の IM およびプレゼンスサービス および Cisco Unity Connection。

utils ntp server delete

このドキュメントの更新により、CSCvf91347 が解決されます。

次の情報は、 *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 ガイドの「ユーティリティコマンド」の章では省略されています。

少なくとも1つの Network Time Protocol (NTP) サーバが設定されている必要があります。したがって、NTP サーバが1つだけ設定されている場合は削除できません。すべての NTP サーバをすべて削除するオプションを選択した場合、NTP サーバは上から順に削除され、リストの最後の NTP サーバは削除されません。

utils dbreplication clusterreset

このドキュメントの更新により、CSCvf93618 が解決されます。

utils dbreplication clusterreset コマンドは廃止され、代わりに **utils dbreplication reset**コマンドを実行し、レプリケーションを修復します。

```
admin:utils dbreplication clusterreset

********************************************************************************
This command is deprecated, please use 'utils dbreplication reset' to repair replication!
********************************************************************************

Executed command unsuccessfully
```

utils dbreplication reset 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 Guide For Cisco Unified Communications Solutions 』」 の「 *Utils Commands* 」の章を参照してください。

『Configuration and Administration of IM and Presence Service on Ciscoユニファイド コミュニケーション マネージャ』

交換されたノードでチャットルームを取得する

このドキュメントの更新により、CSCuy96037 が解決されます。

次の情報は、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』ガイドの「チャット ノードエイリアスの管理」から省略されています。

ユーザがすべての古いチャットルームにアクセスできるようにするには、ノードを削除する前に、既存のすべてのエイリアスのバックアップを取得し、新しいノードに同じエイリアスを割り当てます。

機能設定ガイド

デバイスへの電話番号の追加

このドキュメントの更新により、CSCvd22758 が解決されます。

次の注記は、『 *Feature Configuration Guide for a Cisco Unified Communications Manager* 』の「「Add Directory Number to a Device 」」の手順では省略されています。

（注） コーリング サーチ スペース（CSS）と DN のパーティションは、デバイスで必須です。

CTI リモート デバイスは、自身の DN をブロックしてはいけません。CSS は、CTIRD デバイスが自身の DN に到達するために重要です。

Cisco IPMA 制限

このドキュメントの更新により、CSCvc37425 が解決されます。

Cisco Unified Communications Manager の機能設定ガイドの*Cisco Unified Communications Manager Assistant* の概要の章では、次の制約事項は省略されています。

1 名のマネージャを一度に支援できるのは 1 名のアシスタントのみです。

誤ったマルチキャスト保留音制限

このドキュメントの更新により、CSCvb28136 が解決されます。

保留音 (MOH) 設定の章では、MTP リソースが呼び出されたときに回線上で無音にならないように、ユニキャスト MOH を設定する必要があるという制限があります。正しい制限は次のとおりです。

マルチキャスト MoH を使用しているサイトでコール レッグ中に MTP リソースが呼び出されると、Ciscoユニファイド コミュニケーション マネージャ はマルチキャスト MoH の代わりにユニキャスト MoH にフォール バックされます。

SIP 電話での Private Line Automatic Ringdown の設定タスク フローの前提条件

このドキュメントの更新により、CSCvd72787 が解決されます。

次の前提条件は、『 「Feature Configuration Guide for Cisco Unified Communications Manager 』」の「 *Private Line Automatic Ringdown Configuration TASK Flow fIP* 電話*hone* 」のトピックで省略されています。

- パーティションの作成
- コーリング サーチ スペースへのパーティションの割り当て
- 電話機での Private Line Automatic Ringdown のトランスレーション パターンの設定

エクステンション モビリティ サービスのエラー コード

このドキュメントの更新により、CSCve51354 が解決されます。

エラーコード 39、40、41 および 44は、「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 サービス エラー コード」セクションで更新されています。

Dial Via Office Reverse

このドキュメントの更新により、CSCvf55794 が解決されます。

次の情報は、『「Feature Configuration Guide for Cisco Unified Communications Manager 』」の「Cisco Unified Mobility」の章の「*Configure a Mobility Profile*」の項に追加されています。

オフィスリバース経由のダイヤル (DVO-R) コール機能は、enbloc ダイヤルを使用します。

『InstallingCiscoユニファイドコミュニケーションマネージャ』

既存のクラスタへの新しいノードのインストール

このドキュメントの更新により、CSCvd10033 が解決されます。

次の注は、「Cisco Unified Communications Manager および IM And Presence サービスのインストールガイド」の「既存のクラスタ内の新しいノードのインストール」の章では省略しています。

（注） トレース コレクション サービスを再起動した場合にのみ、既存の FQDN クラスタに追加した新しいノードの RTMT からログを収集できます。トレース コレクションを再起動せずに Unified RTMT にサインインすると、次のエラー メッセージが表示されます：「`Could not connect to 'Server' <new node name>.`」

Ciscoユニファイド コミュニケーション マネージャ のオンラインヘルプ

DHCP サブネットの設定のヒント

このドキュメントの更新により、CSCve07463 が解決されます。

Cisco Unified CM Administration オンラインヘルプでは、DHCP サブネットのセットアップのヒントが正しくありません。「DHCPサブネットのセットアップのヒント」についての正しい情報は次のとおりです。

サーバの構成に加えた変更は、DHCP モニタ サービスを再起動するまで有効になりません。

Opus コーデックに関する情報が不足している

このドキュメントの更新により、CSCva48193 が解決されます。

『「Cisco Unified CM Administration Online Help」』の「システム メニュー」の章には、[**Opus Codec**] フィールドに関する十分な情報が含まれていません。次の注記は、このガイドでは省略されています。

（注） [エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] ウィンドウの [G.722 コーデックのアドバタイズ（Advertise G.722 Codec）] サービス パラメータは、Opus コーデックを使用する SIP デバイスに対しては [有効化（Enabled）] に設定する必要があります。エンタープライズ パラメータの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151.html）を参照してください。

誤った時間帯の例

このドキュメントの更新により、CSCvb74432 が解決されます。

この期間のドキュメントには、設定の問題を引き起こす可能性のある誤った例が含まれています。1日の期間に対して日付範囲を使用することを推奨します。「Jan と1の値で年を選択し、1月1日を指定して、この期間が適用される唯一の日を指定します。」

これは正しくありません。この例では時間帯のオプションに「Year on...」を使用しないでください。

タイム スケジュールに関する情報が不十分

このドキュメントの更新により、CSCvd75418 が解決されます。

Cisco Unified CM Administration オンラインヘルプの 「[Call Routing] メニュー」章の タイム スケジュール設定トピックには、1日の選択した期間に関する情報が不足しています。次のシナリオは、このガイドでは省略されています。

表 *15* : タイム スケジュールの設定

フィールド	説明
時間帯情報	

フィールド	説明
選択された時間帯	**シナリオ**： 複数の時間帯が 1 つのタイム スケジュールと関連付けられており、なおかつ時間帯が重なっていない場合。ただし、特定の日に重複がある場合は、その単一日期間が優先され、その日の他の時間帯は無視されます。 例 1： 3 つの時間帯が次のタイム スケジュールで定義されています。 日付の範囲： Jan 1 - Jan 31: 09:00 - 18:00 曜日： Mon - Fri: 00:00 - 08:30 曜日： Mon - Fri: 18:30 - 24:00 この場合、時間は重複していませんが、たとえば水曜日 10:00 のコールの場合、日付の範囲は無視されます。 例 2： 3 つの時間帯が次のタイム スケジュールで定義されています。 単一日： Jan 3 2017 (Tues): 09:00 - 18:00 曜日： Mon - Fri: 00:00 - 08:30 曜日： Mon - Fri: 18:30 - 24:00 このケースでは、時間は重複していませんが、たとえば、1 月 3 日 20:00 のコールの場合、曜日は無視されます。 （注） [通日（Day of Year）] を設定した場合は、その設定が全日（24 時間）について考慮され、その特定の日の [曜日（Day of Week）] 設定および [日付範囲（Range of Days）] 設定は無視されます。

LDAP ユーザ 認証の情報が不十分

このドキュメントの更新により、CSCvc30013 が解決されます。

『 *Cisco Unified CM Administration Online Help* 』の「 システム メニュー」章の*[LDAP* 認証設定*]* には、LDAP ユーザ認証に関する十分な情報が含まれていません。次の注記は、このガイドでは省略されています。

（注） LDAP ユーザ認証は、IP アドレスまたはホスト名を使用して実行できます。LDAP 認証を構成する際に IP アドレスを使用する場合は、`utils ldap config ipaddr` コマンドを使用して、その IP アドレスの LDAP 構成を作成する必要があります。LDAP 認証を構成する際にホスト名を使用する場合は、その LDAP ホスト名を解決するように DNS を構成する必要があります。

OLH のリモート接続先の設定ページを更新する必要がある

このドキュメントの更新により、CSCvb88447 が解決されます。

Cisco Unified CM Administration オンラインヘルプの「デバイスメニュー」の章には、「リモート接続先の設定」のヘルプページに誤った情報が含まれています。次の情報は、関連するフィールドに誤りがあるか省略されています。

- [**タイマー情報**] フィールドの [ヘルプ (help)] ページの情報が正しくありません。It states the time in 「milliseconds」、the correct time is set in 「seconds」.
- [**タイマー情報**)] セクションの [ヘルプ (help)] ページの順序が正しくありません。フィールドの正しい順序は次のとおりです。**タイマーの呼び出し前の遅延、応答が早すぎるタイマー、応答遅延タイマー**。
- [**Owner ユーザ ID**] フィールドは省略されます。このフィールドの説明を次に示します。
  - **Owner ユーザ ID** - ドロップダウン リストから、後でリモート接続先プロファイルを関連付ける適切なエンド ユーザ プロファイルを選択します。

セキュリティ ガイド

証明書

このドキュメントの更新により、CSCvg10775 が解決されます。

次のメモは『*Cisco Unified Communications Manager* の *Security Guide*』の「「Security Overview」」の章から削除されました。

（注） DER あるいは PEM の証明書のサポートされる最大サイズは 4096 ビットです。

ITL ファイル サイズ制約

このドキュメントの更新により、CSCvb44649 が解決されます。

次の情報は、「Cisco Unified Communications Manager のセキュリティガイド」の最初の信頼リストの章から省略されています。

Cisco Unified Communications Manager クラスタに 39 を超える証明書がある場合、Cisco Unified IP 電話 上の ITL ファイル サイズが 64 キロバイトを超えます。ITL ファイル サイズが増加すると、電話での ITL の正常なロードに影響し、Cisco Unified Communications Manager での電話登録が失敗することになります。

外部 CA からの証明書のサポート

このドキュメントの更新により、CSCve06893 が解決されます。

次のメモは『*Cisco Unified Communications Manager* の *Security Guide*』の「「セキュリティ概要」」の章から削除されました。

（注） マルチサーバ（SAN）CA 署名付き証明書を使用する際、マルチサーバ証明書は、パブリッシャにアップロードされる時点でクラスタに存在するノードのみに適用されます。したがって、ノードを再構築したり、クラスタに新しいノードを追加したりするたびに、新しいマルチサーバ証明書を生成して、クラスタにアップロードする必要があります。

システム構成ガイド

共通サービス ポート

このドキュメントの更新により、CSCve02996 が解決されます。

「『Cisco Unified Communications Manager のシステム設定ガイド』」の「*CISCO UNIFIED COMMUNICATIONS MANAGER TCP And UDP Port Usage*」の章では、次の情報が省略されています。

表 *16*：共通サービス ポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント（Endpoint）	Unified Communications Manager	443、8443/TCP	Cisco ユーザ データ サービス（UDS）の要求に使用されます。

会議ブリッジの概要

このドキュメントの更新により、CSCvd37400 が解決されます。

次の注意事項は、『*Cisco Unified Communications Manager* のシステム設定ガイド』の「会議ブリッジの設定」の章では省略されています。

（注） Cisco Unified Communications Manager サーバが作成されると、会議ブリッジ ソフトウェアも自動的に作成されるため、作成できません。Cisco Unified Communications Manager の管理ページに会議ブリッジ ソフトウェアを追加できません。

機能グループテンプレートの同期の問題

このドキュメントの更新により、CSCux25861 が解決されます。

次の情報は、『システム設定ガイド』の「機能グループ テンプレート」の章では省略されています。

既存の機能グループ テンプレートを変更して、関連付けられた LDAP の完全同期を実行した場合、このテンプレートに関連付けられているユーザは更新されません。

新しい ILS ハブの追加に関する情報が不足している

このドキュメントの更新により、CSCva25662 が解決されます。

次の注意事項は、『*Cisco Unified Communications Manager* のシステム設定ガイド』の「「クラスタ間ルックアップ サービスの設定」」の章では省略されています。

制約事項	説明

ILS ハブ	ILS ネットワークにハブ クラスタを追加するには、次の条件がプライマリ ILS ハブ ノードで満たされているかどうかを必ず確認します。 • クラスタ ID が ILS クラスタ内のすべてのハブ ノードで一意である。 • 完全修飾ドメイン名（FQDN）が設定されている。 • UDS および EM サービスが、ILS クラスタのすべてのハブ ノードで動作している。 • DNS プライマリと逆引きの名前解決が適切に機能している。 • 統合された Tomcat 証明書をすべてのハブ ノードからインポートする。 条件が満たされない場合は、クラスタの再起動またはエラーを修正した後でも、「バージョン」情報が、[リモート クラスタの検索と一覧表示（Find and List Remote Clusters）] ウィンドウに表示されません。これを回避するには、ハブ クラスタを ILS ネットワークから削除し、上記の条件を満たした後に、ILS ネットワークに再度追加します。

サード パーティ制約についての情報が不十分

このドキュメントの更新により、CSCvc16660 が解決されます。

次の制約事項は、「『Cisco Unified Communications Manager のシステム設定ガイド』」の「サードパーティ *SIP* 電話の設定」の章では省略されています。

制約事項	説明
Cisco Video Communication Server（VCS）のリングバック トーンの制限は、サードパーティ製 SIP エンドポイントに登録されています。	Ciscoユニファイドコミュニケーションマネージャに登録された VCS エンドポイント上で発生する転送を要求するためのブラインド転送やスイッチには、リングバック トーンはありません。監視転送を行う場合、保留音（MOH）は割り当てますが、リングバック トーンは割り当てません。

Multilevel Precedence and Preemption の電話サポート

このドキュメントの更新により、CSCvb37715 が解決されます。

マルチレベル優先順位およびプリエンプション (MLPP) の章の制限により、SCCP 電話のみがこの機能をサポートしていることが誤って説明されています。

SCCP 電話機と一部の SIP 電話機は、MLPP をサポートしています。機能のサポートを確認するには、ご使用のモデルの『 Cisco Unified IP 電話 アドミニストレーション ガイド』を参照してください。

SSH パスワード文字の制限が正しくありません

このドキュメントの更新により、CSCvb33353 が解決されます。

『 「System Configuration Guide for Cisco Unified Communications Manager」 』の「 *Configure* アナログ*Phone* アダプタ」の章 および「 「Cisco Unified CM Administration Online Help」 」の「 「Device Menu」 」の章の「 *Phone Settings* 」のトピックでは、セキュアシェルパスワード (SSH) の英数字または特殊文字が最大**200**文字に制限されています。正しい文字の制限は、最大**127**文字です。

ストリーミング統計を収集するための品質レポートツールの最短コール時間

このドキュメントの更新により、CSCve60853 が解決されます。

次の情報は、『*Cisco Unified Communications Manager* のシステム設定ガイド』の「*Cisco Unified IP* 電話の診断とレポート設定の章から省略されています。

ユーザが QRT ソフトキーを押して問題の種類を選択すると、QRT はストリーミングの統計情報を収集しようとします。ストリーミングの統計情報を収集するには、QRT でコールを 5 秒以上アクティブにする必要があります。

電話機と Ciscoユニファイド コミュニケーション マネージャ との間のシグナリング、メディア およびその他の通信

このドキュメントの更新により、CSCvc53152 が解決されます。

「『Cisco Unified Communications Manager のシステム設定ガイド』」の「 *CISCO UNIFIED COMMUNICATIONS MANAGER TCP And UDP Port Usage* 」の章では、次の情報が省略されています。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	53 / TCP	Session Initiation Protocol（SIP）電話機が、ドメイン ネーム システム（DNS）を使用して、完全修飾ドメイン名（FQDN）を解決します。 （注） デフォルトでは、一部のワイヤレス アクセス ポイントは TCP の 53 番ポートをブロックし、FQDN を使用しながら CUCM を設定しているときに、ワイヤレス SIP 電話機が登録されないようにします。

SIP トランク（SIP Trunks）

このドキュメントの更新により、CSCve60892 が解決されます。

次の注意事項は「Cisco Unified Communications Manager のシステム設定ガイド』」の「*Configure SIP* トランク」の章では省略されています。

（注） クラスタ A からクラスタ B で小規模 IP テレフォニー（SIPT）の Q.SIG を有効にした場合、匿名またはテキストで 「"INVITE"」 を受領しても、Cisco Unified Communications Manager は "INVITE" を Q.SIG データにエンコードしません。リーフ クラスタで同じようにデコードすると、何も表示されず、空の番号が転送されます。

Q.SIG を有効にすると、URI ダイヤルが予期したとおりに応答しません。Q.SIG を無効にすると、Cisco Call Back が 2 つのクラスタ間で応答しません。

時間帯ルーティングは、メッセージ待機インジケータに対しては機能しない

このドキュメントの更新により、CSCva13963 が解決されます。

「『Cisco Unified Communications Manager の System Configuration Guide』」の「*Configure Time of Day Routing*」のトピックからは、次の情報が省略されています。

時間帯ルーティングは、メッセージ待機インジケータの代行に対しては機能しません。

SIP ルート パターン

このドキュメントの更新により、CSCvg31370 が解決されます。

次の情報は、*Cisco Unified Communications Manager* のシステム設定ガイドの「グローバルダイヤル プラン レプリケーションの概要」に記載されています。

（注） SIP ルート パターン名にダッシュが含まれる場合、ダッシュ間に数字が含まれていないことを確認する必要があります。ただし、ダッシュが 2 つ以上ある場合は、文字と数字または文字のみの組み合わせを使用できます。

SIP ルート パターンの良い例と悪い例は次のとおりです。

良い例：

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

悪い例：

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

ILS ネットワークでの着信コールのブロック

このドキュメントでは、CSCvg77238 を解決します。

次の情報は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『*Cisco Unified Communications Manager* 用のシステム設定ガイド』の「ILS インタラクション」セクションに追加されています。

ILS ベースのネットワークで発信者番号に基づいて着信コールをブロックするには、発信者の CSS に SIP ルート パターンのパーティションを含める必要があります。たとえば、コールが SIP トランクから発信される場合、SIP トランク着信 CSS には SIP ルート パターンのパーティションを指定する必要があります。

システム エラー メッセージ

Missing Device Type ENUM Values

この更新は CSCvg70867 用です。

Cisco Unified Communications Manager のシステム エラー メッセージファイルには、78xx および 88 xx 電話の次の ENUM 定義がありません。

値	Device Type
508	Cisco IP 電話 7821
509	Cisco IP 電話 7841
510	Cisco IP 電話 7861
544	Cisco IP 電話 8831
568	Cisco IP 電話 8841
569	Cisco IP 電話 8851
570	Cisco IP 電話 8861
36665	Cisco IP 電話 7811
36669	Cisco IP 電話 8821
36670	Cisco IP 電話 8811
36677	Cisco IP 電話 8845
36678	Cisco IP 電話 8865
36686	Cisco IP 電話 8851NR
36701	Cisco IP 電話 8865NR

LastOutOfServiceInformation アラームに理由コードがない。

この更新は CSCvd71818 用です。

Cisco Unified Communications のシステム エラー メッセージファイルに、**LastOutOfServiceInformation**アラーム内の**アウトオブサービスの理由**パラメータの一部の ENUM 値が欠落しています。次は完全なリストです。

原因コード	説明
10	TCPtimedOut：Cisco Unified Communication Manager への TCP 接続でタイムアウト エラーが発生しました
12	TCPucmResetConnection：Cisco Unified Communication Manager は TCP 接続をリセットしました
13	TCPucmAbortedConnection：Cisco Unified Communication Manager は TCP を中断しました
18	TCPucmClosedConnection：Cisco Unified Communication Manager は TCP 接続をクローズしました
15	SCCPKeepAliveFailure：デバイスは SCCP キープアライブ エラーにより接続をクローズしました
16	TCPdeviceLostIPAddress：IP アドレスが失われたため接続がクローズしました。これは、DHCP リースが期限切れとなった、または IP アドレスの重複が検出された可能性があります。DHCP サーバがオンラインであり、DHCP サーバで重複が報告されていないことを確認します
17	TCPdeviceLostIPAddress：IP アドレスが失われたため接続がクローズしました。これは、DHCP リースが期限切れとなった、または IP アドレスの重複が検出された可能性があります。DHCP サーバがオンラインであり、DHCP サーバで重複が報告されていないことを確認します
18	TCPclosedConnectHighPriorityUcm：デバイスは、優先度の高い Cisco Unified CM に再接続するために TCP 接続をクローズしました
20	TCPclosedUserInitiatedReset：デバイスは、ユーザによるリセットのため TCP 接続をクローズしました
22	TCPclosedUcmInitiatedReset：デバイスは、Cisco Unified CM からのリセット コマンドのため TCP 接続をクローズしました
23	TCPclosedUcmInitiatedRestart：デバイスは、Cisco Unified CM からの再起動コマンドのため TCP 接続をクローズしました
24	TCPClosedRegistrationReject：デバイスは、Cisco Unified CM から登録拒否を受信したため TCP 接続をクローズしました
25	RegistrationSuccessful：デバイスが初期化されており、Cisco Unified CM への以前の接続は認識されません
26	TCPclosedVlanChange：デバイスは、新しい音声 VLAN 上の IP の再構成のための TCP 接続をクローズしました

原因コード	説明
27	Power Save Plus
30	電話のワイプ (CUCM からワイプ)
31	電話のロック (CUCM からロック)
32	TCPclosedPowerSavePlus：デバイスは、Power Save Plus モードに入るために TCP 接続をクローズしました
100	ConfigVersionMismatch：デバイスは、Cisco Unified CM の登録中にバージョン スタンプの不一致を検出しました
101	設定バージョンのスタンプがの不一致
102	ソフトキーバージョンスタンプの不一致
103	ダイヤルプランの不一致
104	TCPclosedApplyConfig：デバイスは、デバイスによる内部のトリガーで再起動し構成の変更を適用するために TCP 接続をクローズしました
105	TCPclosedDeviceRestart：デバイスは、デバイスが構成またはダイヤルプラン ファイルのダウンロードに失敗したため、デバイスによる内部のトリガーで再起動するために TCP 接続をクローズしました
106	TCPsecureConnectionFailed：デバイスは、Cisco Unified CM とのセキュアな TCP 接続のセットアップに失敗しました
107	TCPclosedDeviceReset：デバイスは、非アクティブ パーティションをアクティブなパーティションとして設定してからリセットを行い、新しいアクティブなパーティションから起動するために TCP 接続をクローズしました
108	VpnConnectionLost：デバイスは、VPN 接続が失われたため Unified CM に登録できませんでした。109 IP アドレス変更済。
109	IPアドレスが変更されました
110	アプリケーションが停止を要求しました (サービス制御が登録停止を通知)
111	アプリケーションが破棄を要求しました
114	最後のクラッシュ
200	ClientApplicationClosed：デバイスは、クライアントアプリケーションが閉じられたため登録解除されました

原因コード	説明
201	OsInStandbyMode：デバイスは、OS がスタンバイ モードに入ったため登録解除されました
202	OsInHibernateMode：デバイスは、OS が休止モードに入ったため登録解除されました
203	OsInShutdownMode：デバイスは、OS がシャットダウンしたため登録解除されました
204	ClientApplicationAbort：デバイスは、クライアント アプリケーションがクラッシュしたため登録解除されました
205	DeviceUnregNoCleanupTime：デバイスは、システムがクリーンアップに十分な時間を許可しなかったため以前のセッションで登録解除されました
206	DeviceUnregOnSwitchingToDeskphone：デバイスは、クライアントによるソフトフォンからデスクフォン コントロールへの切り替え要求のため登録解除されました
207	DeviceUnregOnSwitchingToSoftphone：クライアントがデスクフォン コントロールからソフトフォンへの切り替えを要求したためデバイスを登録しています
208	DeviceUnregOnNetworkChanged：クライアントがネットワークの変更を検出したためデバイスを登録解除しています
209	DeviceUnregExceededRegCount：デバイスが同時登録の最大数を超えたためデバイスを登録解除しています
210	DeviceUnregExceededLoginCount：クライアントが同時ログオンの最大数を超えたためデバイスを登録解除しています

IM and Presence サービスのオンライン ヘルプ

処理フィールドの説明が正しくありません

このドキュメントの更新により、CSCvc66409 が解決されます。

サードパーティのプロファイルには、TC および JSM イベントの**処理**と**Fire および Forget**のオプションがあります。コンプライアンス プロファイル設定のヘルプページでの混乱を避けるために、**処理**の説明が正しい情報で更新されました。

JSM および TC イベントの既存のステートメント

ハンドル

コンプライアンス サーバから返されるエラーが元のパーティまたはコンポーネントにバウンスされるようにする場合は **[bounce（バウンス）]** を、破棄する場合は **[pass]** をクリックします。[Fire] および [Forget] が選択されていない場合、処理設定は無視されます。

JSM および TC イベントの更新されたステートメント

ハンドル

- **[Fire と Forget]** がオフになっています。コンプライアンスサーバから返されたエラーが発信側またはコンポーネントにバウンスされる必要がある場合は、**[バウンス]** をクリックします。エラーを破棄する必要がある場合は、[**pass**] をクリックします。
- [**Fire and Forget**] がチェックされている: [**バウンス**] をクリックしてコンプライアンス サーバにパケットを送信し、送信元またはコンポーネントにイベントをキャンセルします (コンプライアンス サーバからの応答を待機せずにイベントをキャンセルします)。コンプライアンス サーバにパケットを送信するには、[**pass**] をクリックします。イベントは、ノードによってさらに処理されます (コンプライアンス サーバからの応答を待機せずに [pass on event])。

リアルタイム監視ツールアドミニストレーションガイド

RTMT TFTP BuildDeviceCount カウンタが決して減らない

このドキュメントの更新により、CSCvf34465 が解決されます。

次の注は、『 「Cisco ユニファイドリアルタイム監視ツール アドミニストレーション ガイド』」の「 *Cisco TFTP* サーバ」の章に記載されています。

（注） 11.5以上では、コンフィギュレーション ファイルを作成してキャッシングの代わりに提供することができます。

ビルドが行われると、BuildDeviceCount が増分します。電話からのリクエストがあると、カウンタが増加し、減少はしません。TFTP の安定したモニタリングは必要ありません。