新機能および変更された機能

情報保証機能

このセクションでは、Cisco Unified Communications Manager リリース 10.5(2) の一部として追加された新しい情報保証機能について説明します。

ログイン試行の情報

Cisco Unified Communications Managerまたは IM and Presence Service の Web アプリケーションにログインすると、メインのアプリケーションウィンドウに、最後に成功したシステムログインが表示され、現在のユーザに対する前回のシステムログイン試行が、ユーザID、日付、時刻、およびIP アドレスと共に表示されます。

次の Web アプリケーションには、ログイン試行に関する情報が表示されます。

- Cisco Unified Communications Manager:
  - Cisco Unified CM の管理
  - Cisco Unified のレポート

- Cisco Unified サービスアビリティ

- IM and Presence Service
  - Cisco Unified CM IM and Presence の管理
  - Cisco Unified IM and Presence のレポート
  - Cisco Unified IM and Presence サービスアビリティ

[ログイン失敗] CLI コマンドを使用して、災害復旧システムと Cisco Unified OS 管理 Web アプリケーションのログイン情報を表示することができます。

ユーザ インターフェイスの変更

Cisco Unified CM Administration の **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** では、**[ユーザの検索/一覧表示（Find and List Users）]** ウィンドウに次のボタンが追加されました。

- **選択したローカル ユーザの有効化**— 管理者は、必要に応じて、1 人のユーザまたは複数のユーザを一括で有効にできます。
- **選択したローカル ユーザの無効化**— 管理者は、必要に応じて、1 人のユーザまたは複数のユーザを一括で無効にできます。

Note **[選択したローカルユーザの有効化(Enable Selected Local User)]** および **[選択したローカルユーザの無効化(Disable Selected Local User)]** ボタンは、Cisco Database Layer Monitor サービスで **未使用のユーザアカウントを無効にする (日数)** サービス パラメータ値が 1 日以上に設定されている場合にのみ表示されます。

エンド ユーザの設定項目

Cisco Unified CM 管理では、**[エンド ユーザ設定]**ウィンドウに次のボタンが追加されました。

- **ローカル ユーザの有効化**: **ユーザ ステータス**が無効に設定されている場合、管理者は 1 人 のユーザを有効にすることができます。

  Note このボタンは、**ユーザ ステータス**が無効に設定されている場合にのみ表示されます。

- **ローカル ユーザの無効化**: **ユーザ ステータス**が有効に設定されている場合、管理者は 1 人 のユーザを無効にすることができます。

Note このボタンは、**ユーザステータス**が有効に設定されている場合にのみ表示されます。

Note **[選択したローカル ユーザの有効化（Enable Selected Local User）]** ボタンと **[選択したローカル ユーザの無効化（Disable Selected Local User）]** ボタンが表示されるのは、**Cisco Database Layer Monitor サービスで [未使用のユーザ アカウントを無効にする期間（日）（Disable User Accounts unused for (days)）]** サービス パラメータ値が 1 日以上に設定されている場合だけです。

新しいサービス パラメータ

[使用されないユーザアカウントの無効化 (日)] という新しいサービスパラメータ が、**サービスパラメータ設定** ウィンドウの Cisco Database Layer Monitor サービスの下に追加されています。このパラメータでは、ユーザが Cisco Unified Communications Manager を使用して、アカウントが自動的に無効化されるのを防ぐために、ユーザ認証を行う頻度を指定します。

ユーザアカウントは、ユーザが Cisco Unified Communications Manager に、**[未使用のユーザアカウントを無効にする (日)]** フィールドで指定された日数の間に、PIN またはパスワードを使用してログインしない場合は無効になり ます。

両方の**ユーザアカウントが未使用 (日)**フィールドで無効になっていて、**[クレデンシャルポリシーの設定]** ウィンドウの **[非アクティブな日数] 許可**フィールドが設定されている場合 、値が小さいフィールドが優先されます。

たとえば、**[非アクティブな日数]** フィールドが 30 日に設定されていて、**[使用して いないユーザアカウントを無効にする (日数)]** フィールドが 45 日に設定されていて、30 日以内にユーザが Cisco Unified Communications Manager にログインしていない場合 、ユーザ アカウントは 45 日まで有効です。

[ユーザアカウントを無効にする (日数)] フィールドが 30 日に設定されていて、**[非アクティブな日数]** フィールドが 45 日に設定されていて、その ユーザが Cisco Unified Communications Manager に 30 日以内にログオンしない場合 、そのユーザアカウントは無効になります。

失敗したログオン試行のデフォルトしきい値に更新

リリース 10.5(2) では、管理者アカウントとエンドユーザアカウントの両方で失敗したログオン試行回数のデフォルト値が 5 に変更されました。デフォルトでは、管理者またはエンドユーザが、誤ったユーザ名とパスワードの組み合わせを 5 回入力すると、そのアカウントはロックされます。

エンド ユーザの場合は、**[エンド ユーザの設定(End User Configuration)]** ウィンドウで新しいクレデンシャル ポリシーを割り当て、ログオンが失敗した回数を再設定 できます。

管理者は 、`reset_application_ui_administrator_password` を使用して管理者パスワードをリセットします。

新しいシステム ロール

次の表は、Cisco Unified Communications Manager にあらかじめ設定されている新しい標準権限およびアクセス コントロール グループの概要です。

Table 1: 標準権限、特権 およびアクセス制御グループ

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制御グループ
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（Standard CCMADMIN Administration）]	CCMAdmin システムをすべての面で管理できます。	[標準Cisco Unified CM IM & Presence管理（Standard Cisco Unified CM IM and Presence Administration）]
[標準CCMADMIN読み取り専用（Standard CCMADMIN Read Only）]	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 & Presence管理（Standard Cisco Unified CM IM and Presence Administration）]
[標準CUReporting（Standard 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 & Presenceのレポーティング

役割とユーザ グループの詳細については、*Cisco Unified Communications Manager* システム ガイドを参照してください。

セキュリティステータスの制御

Cisco TelePresence Multipoint Control Unit (MCU) リリース 4.5 および Cisco TelePresence Conductor Release 2.3 以前のリリースの場合 、Cisco Unified Communications Manager は 、Cisco Unified Communications Manager サーバと会議参加者に設定されたセキュリティ レベルに応じて、コール セキュリティ アイコンを提供します。Cisco TelePresence MCU リリース 4.5 と Cisco TelePresence Conductor リリース XC 2.33 を使用した場合、SIP ビデオ会議リソースは、ビデオ会議のセキュリティステータスを判別し、参加者にステータスを示すことができます。アドホック会議やMeet-Me会議では、SIP ビデオ会議リソースによって決定されるセキュリティ ステータスが、Cisco Unified Communications Manager によって決定されたセキュリティ ステータスと競合する場合があります。リリース 10.5(2) では、SIP Cisco TelePresence MCU または Cisco TelePresence Conductor を設定して、ビデオ会議でのコールセキュリティアイコンの表示を制御することができます。

ユーザインターフェイスの新機能

Cisco Unified CM の管理では、**メディアリソース** > **会議ブリッジ**の下にある **[コールセキュリティアイコンのコールを許可する]**チェックボックスが**デバイス情報**領域に追加されます。このチェックボックスは、デフォルトでオフになっています。このチェックボックスをオンにすると、MCU または導線で、コールセキュリティアイコンの表示を制御することができます。Cisco Unified Communications Manager でコールセキュリティアイコンの表示を制御する場合は、このチェックボックスをオフのままにしておくことができます。

このチェックボックスは、**Cisco Telepresence MCU** または **Cisco TelePresence Conductor** として**会議のブリッジタイプ**を選択した場合にのみ表示され ます。

仮想マシンのタッチレス インストール

以前のリリースの Cisco Unified Communications Manager クラスタ環境では、サブスクライバ ノードのインストールに進む前に、まず、パブリッシャ ノードをインストールする必要がありました。また、サブスクライバ ノードをパブリッシャ ノードのサーバ ページに追加した後にそれらのサブスクライバノードをインストールし、サブスクライバノードごとに同じ手順を繰り返す必要がありました。タッチレスインストール機能により、サブスクライバノードは、インストール時にパブリッシャ ノードとともに動的に設定されます。

タッチレス インストールは Cisco Unified Communications Manager の新機能です。この機能により、インストール プロセスがシームレスになり、クラスタ インストールが非常に簡単になります。タッチレスインストールでは、インストール ウィザードでサブスクライバの詳細情報を入力する必要がありません。サブスクライバはパブリッシャのインストールに依存しません。この機能には、次の利点があります。

- 新しいクラスタの展開時の手動による介入およびスケジュール設定が不要になります。
- 各サブスクライバの手動エントリが不要になり、既存のクラスタへの新しいサブスクライバの追加が簡素化されます。
- パブリッシャ ノードがアクティブになるまで待つ必要がなくなります。

タッチレス サーバの自動シーケンシング

自動シーケンシングは、クラスタで手動による介入なしにパブリッシャ ノードとサブスクライバ ノードの両方を同時に容易にインストールするためのアプローチです。サブスクライバ ノードは、パブリッシャ ノードのインストールが完了するまで待機し、それ自体のインストールを続行するためにパブリッシャ ノードのデータベースに追加されます。パブリッシャ ノードは、インストールが完了すると、各パブリッシャを認証します。認証後に、各サブスクライバ ノードは、パブリッシャ ノードから信号を受信し、そのサブスクライバ ノードのインストールを自動的に続行します。

[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）] タイマー チェックボックスにマークを付け、**[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]**

フィールドに値を入力することにより、自動シーケンシングを開始します。次のいずれかの方法により、このタイマーを有効にすることができます。

- 応答ファイル ジェネレータ（AFG）
- Cisco Unified Communications Manager パブリッシャ ノードでの CLI（コマンド ライン インターフェイス）コマンド

アンサー ファイル ジェネレータ

応答ファイル ジェネレータ（AFG）ツール（http://www.cisco.com/web/cuc_afg/index.html）を使用して、設定の応答ファイルまたはフロッピーイメージファイルを生成します。これらのファイルには `clusterConfig.xml` ファイルと `platformConfig.xml` ファイルが含まれます。`clusterConfig.xml` ファイルは、Cisco Unified Communications Manager Release 10.5(2) の新しいファイルです。

ISO およびフロッピーイメージをマウントした仮想マシンを起動して、Cisco Unified Communications Manager のインストールを開始します。スタンドアロン ノードまたはクラスタのインストール時は、手動による介入は不要です。

クラスタ環境では、パブリッシャ ノードとサブスクライバ ノードの両方を同時にインストールできます。時には、パブリッシャ ノードのインストール時にサブスクライバ ノードのインストールが停止することもあります。この場合、パブリッシャ ノードのインストールが完了すると、パブリッシャ ノードにより、サブスクライバ ノードのインストールを続行するための信号が生成されます。

事前定義クラスタ設定（AFG プロセス）

応答ファイル ジェネレータ（AFG）ツールは、既存の `platformConfig.xml` ファイルとともに `clusterConfig.xml` ファイルを生成します。サブスクライバ ノードの詳細情報を AFG ツールに提供すると、`clusterConfig.xml` ファイルにそれらの詳細情報が含まれます。Cisco Unified Communications Manager パブリッシャは、インストールされた後に `clusterConfig.xml` ファイルを読み取り、サブスクライバ ノードを検出すると、それらを processnode テーブルに追加します。サブスクライバを processnode テーブルに追加することにより、Cisco Unified Communications Manager パブリッシャのインストールの完了を待ってサブスクライバをサーバ ページに手動で追加する必要がなくなります。インストール プロセス全体が自動的に実行されます。

タッチレス インストール設定のタスクフロー

Procedure

	Command or Action	Purpose
Step 1	フロッピー イメージの生成およびダウンロード, on page 7。	応答ファイル ジェネレータ ツールを使用してフロッピー イメージを生成します。フロッピーイメージは、フロッピーイメージのダウンロード時に自動的にダウンロー

	Command or Action	Purpose
		ドされる platformConfig.xml ファイルと ClusterConfig.xmlファイルという2つの事前作成応答ファイルで構成されます。
Step 2	クラスタのインストール, on page 8 • ダイナミック クラスタ設定タイマーが有効になっているときのクラスタのインストール, on page 8 • ダイナミック クラスタ設定タイマーが有効になっていないときのクラスタのインストール, on page 9	次のいずれかの方法でクラスタをインストールします。 • **[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマーを有効にすることにより、手動による介入なしにパブリッシャ ノードとサブスクライバ ノードをインストールします。 • 応答ファイルの生成時に **[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマーを有効にしない場合にサブスクライバ ノードをインストールします。

フロッピー イメージの生成およびダウンロード

Web アプリケーションの Cisco Unified Communications 応答ファイル ジェネレータは、Cisco Unified Communications をインストールするための応答ファイルを生成します。これらの事前作成応答ファイルは platformConfig.xml ファイルと ClusterConfig.xml ファイルであり、これらはフロッピー イメージに含まれます。

フロッピー イメージを生成およびダウンロードするには、次の手順を実行します。

Procedure

Step 1 Cisco Unified Communications Answer File Generator アプリケーションにログインします。

Step 2 **[クラスタ全体の設定（Clusterwide Configuration）]** セクションに詳細情報を入力します。

Step 3 **[プライマリ ノードの設定（Primary Node Configuration）]**セクションにプライマリ ノードの詳細情報を入力します。

Step 4 ダイナミック クラスタ設定を有効にするには、**[ダイナミック クラスタ設定（Dynamic-Cluster-Configuration）]**セクションで、**[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマー チェックボックスにマークを付け、**[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]** フィールドに値を入力します。

このフィードには時間を示す 1 ~ 24 の値を指定します。

Note 応答ファイルの生成時に **[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマーを有効にせず、**[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]** フィールドに値を入力しない場合は、後で、パブリッシャ ノードが自動インストールされ、サブスクライバ ノードのインストールを待っているときに、このタイマーを有効にする必要があります。その後、インストールが自動的に行われるように、サブスクライバ ノードを手動で追加する必要があります。

Step 5 **[セカンダリ ノードの設定（Secondary Node Configuration）]** セクションにセカンダリ ノードの詳細情報を入力します。

Step 6 **[セカンダリ ノードのリスト（List of Secondary Nodes）]** リスト ボックスで、**[セカンダリ ノードの追加（Add Secondary Node）]** を選択します。
セカンダリ ノードとして追加するノードがこのリスト ボックスに表示されます。

Step 7 追加のセカンダリ ノードについて手順 5 と 6 を繰り返します。

Step 8 **[応答ファイルの生成（Generate Answer Files）]** をクリックします。
プライマリ ノード、セカンダリ ノード、および `clusterConfig` ファイルの詳細情報を示すダイアログボックスが表示されます。

Step 9 **[Communications Answer File Generator]** ダイアログボックスで、ダウンロードの指示に従い、**[ファイルのダウンロード（Download File）]** ボタンをクリックして応答ファイルをコンピュータにダウンロードします。

クラスタのインストール

応答ファイル ジェネレータ ツールで **[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマーを有効にしたかどうかに応じて、次のいずれかのクラスタ インストール方法を選択できます。

- **[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマーを有効にすることにより、手動による介入なしにパブリッシャ ノードとサブスクライバ ノードをインストールします。ダイナミック クラスタ設定タイマーが有効になっているときのクラスタのインストール, on page 8を参照してください。
- 応答ファイルの生成時に **[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマーを有効にしない場合にサブスクライバ ノードをインストールします。「ダイナミック クラスタ設定タイマーが有効になっていないときのクラスタのインストール, on page 9」を参照してください。

ダイナミック クラスタ設定タイマーが有効になっているときのクラスタのインストール

Before you begin

次のいずれかの方法で、**[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]** フィールドを有効にします。

- 応答ファイル ジェネレータ ツールで、**[ダイナミック クラスタ設定の有効化（Dynamic Cluster Config Enable）]** タイマー チェックボックスにマークを付け、**[ダイナミック クラスタ設定タ**

イマー（**Dynamic Cluster Config Timer**）**]**フィールドに値を入力します。詳細については、フロッピー イメージの生成およびダウンロード, on page 7の手順 4 を参照してください。

- **set network cluster subscriber dynamic-cluster-configuration**{ デフォルト | 時間数 }CLI コマンドを入力します。

Procedure

Step 1 フロッピー イメージを仮想マシンにマウントします。

Note 仮想マシンが Cisco Unified Communications Manager パブリッシャ ノードである場合は、フロッピー イメージに `platformConfig.xml` ファイルと `ClusterConfig.xml` ファイルの両方が含まれます。ただし、仮想マシンが Cisco Unified Communications Manager サブスクライバ ノードまたは IM and Presence パブリッシャ ノード/サブスクライバ ノードである場合は、フロッピーイメージには`platformConfig.xml` ファイルのみが含まれます。

新しい仮想フロッピー イメージの作成方法の詳細については、http://docwiki.cisco.com/wiki/How_to_Use_the_AFG_with_the_Virtual_Floppy_Driveを参照してください。

Step 2 パブリッシャ ノードとすべてのサブスクライバ ノードを起動します。
パブリッシャノードとサブスクライバノードが手動による介入なしで自動的にインストールされます。自動シーケンシングアプローチにより、各サブスクライバノードがパブリッシャに自動的に追加されます。

ダイナミック クラスタ設定タイマーが有効になっていないときのクラスタのインストール

応答ファイル ジェネレータ ツールの **[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]**フィールドを有効にしなくても、パブリッシャ ノードは自動的にインストールされます。ただし、サブスクライバ ノードはインストールを待機します。

サブスクライバノードの待機時間を回避してクラスタインストールを続行するには、次のいずれかのタスクを実行します。

- Cisco Unified Communications Manager から、**[Web インターフェイス（Web Interface）]** を選択し、**[サーバ（Server）]**タブをクリックして、サブスクライバノードの手動で追加します。
- Cisco Unified Communications Manager リリース 10.5(2) で使用可能な新しい CLI コマンドを使用して、発行元ノードの CLI から **[ダイナミック クラスタ設定タイマー]**フィールドを有効にします — **set network cluster subscriber dynamic-cluster-configuration**{ デフォルト | 時間数}。このタイマーを有効にすると、サブスクライバ ノードがパブリッシャに自動的に追加され、サブスクライバ ノードのインストールが続行されます。

Note

- 1 つまたは複数のサブスクライバを、パブリッシャ ノードに対する指定を適用して追加する必要がある場合は、`platformconfig.xml` ファイルの生成時にそれらを追加できます。パブリッシャ ノードとサブスクライバ ノードを指定する必要があります。**[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]** タイマーがアクティブのままであれば、サブスクライバがパブリッシャに自動的に追加され、サブスクライバ ノードのインストールが続行されます。
- この機能には、パブリッシャ ノードに追加する必要があるサブスクライバ ノードの数の事前定義に関する制限はありません。

WinImage ツールを使用してディスク イメージを作成します。VMware ESXi を使用して ISO イメージをマウントします。

Before you begin

フロッピー イメージを、マウントのための仮想マシンにアクセスできるデータストアに配置します。

Procedure

Step 1 仮想マシンを起動してクラスタ インストールを開始します。

Step 2 **[VM]** メニューから、**[設定の編集（Edit settings）]** を選択して、応答ファイル ジェネレータ ツールで作成したフロッピー イメージをマウントします。
[仮想マシンのプロパティ（Virtual Machine Properties）] ダイアログボックスが表示されます。

Step 3 使用可能なハードウェアのリストから、**[フロッピー ドライブ 1（Floppy drive 1）]** を選択します。

Step 4 **[デバイスタイプ（Device Type）]** セクションで、**[データベースの既存のフロッピー イメージを使用する（Use the existing floppy image in the database）]** を選択し、**[参照（Browse）]** をクリックしてフロッピー イメージを選択します。

Step 5 [OK] をクリックします。
フロッピー イメージが接続されます。

Step 6 ツールバーから **[CD/DVD ドライブ 1（CD/DVD Drive 1）]** > **[ローカル ディスクの ISO イメージに接続（Connect to ISO image on local disk）]** オプションを選択し、**[CD/DVD ドライブ 1（CD/DVD Drive1）]** > **[データストアの ISO イメージに接続（Connect to ISO image on a datastore）]** を選択してデータストアに移動し、インストーラ ISO イメージを選択して **[OK]** をクリックします。
ISO イメージが接続され、インストールが開始されます。

Step 7 （オプション）インストールの前にメディアをテストする場合は、**[検出されたディスク（Disc Found）]** メッセージ ボックスで **[OK]** をクリックします。**[スキップ（Skip）]** をクリックすると、インストール前のメディア テストがスキップされます。
インストールは手動による介入なしで続行されます。パブリッシャがインストールされ、サブスクライバがパブリッシャに追加されます。

IM and Presence Service の統合

この機能は、Cisco Unified Communications Manager ノードと IM and Presence Service ノードを含む異機種クラスタ全体のインストールをサポートします。IM and Presence Service の概念およびインストール プロセスは、クラスタの Cisco Unified Communications Manager のインストール プロセスと同じです。

AFG ツールで、**[ダイナミック クラスタ設定タイマー（Dynamic Cluster Config Timer）]** チェックボックスにマークを付け、IM and Presence Service を選択し、Cisco Unified Communications Manager パブリッシャ ノード、IM and Presence Service パブリッシャ ノード、および IM and Presence Service サブスクライバの詳細（存在する場合）を入力します。その後、AFG ツールは、ノードごとに、`platformConfig.xml` ファイルとともに `clusterConfig.xml` ファイルを生成します。この `clusterConfig.xml` ファイルは、Cisco Unified Communications Manager パブリッシャ ノードによってのみ、このノード用に生成された `platformConfig.xml` ファイルとともに使用することができます。その他のすべてのノードについては、`platformConfig.xml` ファイルのみが使用されます。

応答ファイル ジェネレータ（AFG）は IM and Presence Service パブリッシャのドメイン名を既存の詳細情報とともに `clusterConfig.xml` ファイルに保存します。

Cisco Unified Communications Manager と IM and Presence の統合には、次のタスクが含まれます。

- Cisco Unified Communications Manager のインストール後に、IM and Presence Service パブリッシャが、ドメイン名を使用して processnode テーブルに追加されます。
- Cisco Unified Communications Manager ノードと IM and Presence Service ノードが IPアドレス（使用可能な場合）を使用して processnode テーブルに追加されます。
- CLI を使用して IM and Presence Service パブリッシャを追加すると、ドメインが追加されます。

CLI コマンド

Cisco Unified Communications Manager リリース 10.5(2) には、次の新しい CLI コマンドが含まれています。

Note CLI コマンドの詳細については、*Cisco Unified Communications Solutions* のコマンドライン インターフェイス ガイドおよび *Cisco Unified Communications Manager* の インストールを参照してください。

set network cluster subscriber details

Tomcat Web サーバがダウンして GUI にアクセスできない間は、このコマンドを使用してサブスクライバを processnode または appserver テーブルに追加します。

set network cluster subscriber details サーバタイプ *hostname ip domainname*

Syntax Description

パラメータ	説明
servertype	このパラメータには、Unified Communications Manager、IM and Presence サービス、Cisco Unity Connection のいずれかの製品を選択します。このフィールドは必須です。
hostname	クラスタに追加するノードのホスト名。ホスト名は同じドメインでサポートされます。このフィールドは必須です。
ip	クラスタに追加するノードの IPv4 アドレス。IM and Presence パブリッシャおよび Cisco Unity Connection の場合、これは必須フィールドです。
domainname	IM and Presence サービス パブリッシャのドメイン名。IM and Presence パブリッシャの場合、これは必須フィールドです。

Command Modes

管理者（admin:）

要 件

コマンド特権レベル：1

アップグレード時の使用：可能

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、および Cisco Unity Connection に適用されます。

set network cluster subscriber dynamic-cluster-configuration

パブリッシャでダイナミック クラスタ設定をイネーブルにするには、このコマンドを使用します。このコマンドを使用して、ユーザがサブスクライバ ノードをパブリッシャ サーバ テーブルに追加できる期間を指定します。サブスクライバ ノードの追加はただちに認証されるため、これらのノードは、サブスクライバ ノードのインストール時に、パブリッシャの詳細を待機する必要はありません。

set network cluster subscriber dynamic-cluster-configuration {**default** | **no. of hours**}

Syntax Description

パラメータ	説明
default	24時間ダイナミック クラスタ設定をイネーブルにします。
no. of hours	1 ～ 24 時間の値を指定します。

Command Modes

管理者（admin）

要件

適用対象：Unified Communications Manager、IM and Presence サービス、および Cisco Unity Connection。

show network cluster

このコマンドは、ダイナミッククラスタの設定が有効になっている場合に、残りのタイマー値を表示するように拡張されています。

show network cluster

Command Modes 管理者（admin:）

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：Cisco Unified Communications Manager、Cisco Unified Communications Manager の IM and Presence Service、および Cisco Unity Connection。

unset network cluster subscriber details

このコマンドは、コマンド プロンプトの代わりに GUI からサブスクライバ ノードを削除する必要があることを通知するメッセージを表示します。

unset network cluster subscriber details

Command Modes 管理者（admin:）

要 件

コマンド特権レベル：1

アップグレード時の使用：不可

適用対象：Unified Communications Manager、Communications Manager の IM and Presence サービス、および Cisco Unity Connection。

GUI からサブスクライバを削除するメッセージ

```
admin: unset network cluster subscriber details
Please use the Cisco Unified Communications Manager on the first node.
Navigate to System > Server and click “Find”.
   Unable to del: NULL
Executed command unsuccessfully.
```

unset network cluster subscriber dynamic-cluster-configuration

このコマンドは、パブリッシャのダイナミック クラスタ設定をディセーブルにします。[ダイナミッククラスタ設定（Dynamic Cluster Configuration）] オプションの値は、パブリッシャでゼロに設定されます。

unset network cluster subscriber dynamic-cluster-configuration

Command Modes

管理者（admin:）

要 件

コマンド特権レベル：1

アップグレード時の使用：不可

適用対象：Unified Communications Manager、Unified Communications Manager の IM and Presence サービス、および Cisco Unity Connection。

ログインの表示に失敗しました

次の Web アプリケーションへの最近のログイン試行の失敗をリストするには、このコマンドを使用します。

- Unified Communications Manager 上
  - Disaster Recovery System
  - Cisco Unified OS Administration
- IM and Presence Service の場合
  - IM and Presence のディザスタ リカバリ システム
  - Unified IM and Presence OSの管理

show logins unsuccessful [番号を入力します]

Syntax Description

パラメータ	説明
number	表示する最近のログインの数を指定します。デフォルトは20です。

Command Modes

管理者（admin）

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 および IM and Presence サービス。

ユーティリティ vmtools ステータスのサポートが削除されました

`utils vmtools status` CLI コマンドはサポートされなくなりました。VMware ステータスの場合は、代わりに vSphere クライアントを確認します。

シングルサインオンの更新

次の SAML SSO 関連の機能拡張は、Cisco Unified Communications Manager リリース 10.5(2) で導入されています。

SSO メタデータのエクスポート/インポート

Cisco Unified Communications Manager 管理では 、**システム** > **SAML シングルサインオン**で、SAML SSO の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、**[すべてのメタデータのエクスポート (All Metadata)]** ボタンがデフォルトでは有効になっています。

[SAML SSO の有効化（Enable SAML SSO）]

次の注意書きは、「機能およびサービスガイド」の「SAML SSO の有効化手順」に追加されました 。

Note **[IdP メタデータのインポート (Import IdP Metadata)]** をクリックした後 、**[次へ (Next)]** をクリックすると 、**SAML シングルサインオンの設定**ウィンドウにステータスメッセージが表示され ます。サーバのメタデータを IdP にアップロードする手順をスキップまたは続行するための情報を表示します。

IP Voice Media Streaming Application のキャパシティの増加と MOH オーディオ ソースの拡張

Cisco IP Voice Media Streaming Application は Cisco Unified Communications Manager のインストール時に自動でインストールされます。このアプリケーションをアクティブ化して、保留音（MoH）機能を有効にします。

このリリースでは、MOH サーバで保留音サービスが実行中に、固有の同時 MOH オーディオ ソースをサポートするために、Cisco Unified Communications Manager のキャパシティが 51 から 501 に増やされました。MOH オーディオ ソースには 1 から 501 までの番号が振られ、固定 MOH オーディオ ソースの番号は 51 のままです。

Cisco Unified Communications Manager は VMware 上での実行時に USB をサポートしないため、固定 MoH デバイスは USB MoH デバイス経由で接続するオーディオ ソースを使用できません。

VMware では固定 MoH USB デバイスの使用はサポートされません。一方、Cisco Unified Survivable Remote Site Telephony（SRST）マルチキャスト MoH を利用する導入向けには、外部のサウンドデバイスをプロビジョニングします。

初期グリーティングとしてのカスタム アナウンス、または音楽を聞く発信者に対して定期的に再生されるアナウンスのいずれかまたは両方を使用するために、各 MOH オーディオ ソースを設定できます。Cisco Unified Communications Manager には 1 つまたは複数の MOH オーディオ ソースで使用可能なカスタム アナウンスが 500 個用意されています。これらのアナウンスはクラスタ内の Cisco Unified Communications Manager サーバ間での配信はされません。これらのカスタム アナウンス ファイルは MoH およびアナウンス サービスを提供する各サーバにアップロードする必要があります。また、MOH オーディオ ソースの各カスタム音楽ファイルも各サーバにアップロードする必要があります。

サービス付きメディア デバイスのパフォーマンスへの影響

Cisco IP Voice Media Streaming Application は、アナンシエータ（ANN）、ソフトウェア会議ブリッジ、保留音（MOH）、ソフトウェア メディア ターミネーション ポイントの 4 つのメディア デバイス向けのサービスとして実行します。Cisco Unified Communications Manager のサーバ上で呼処理と共存するようにこのサービスを有効にします。このサービスを有効にする際、呼処理への影響を避けるために必ず限定的な容量でこれらのメディアデバイスを設定します。メディアデバイスのデフォルト設定はこの共存操作に基づいて定義されます。1 つ以上のメディア デバイスの使用を減らし、その他の設定を増加させることでこれらの設定を調整できます。

たとえば、ソフトウェア メディアターミネーション ポイントデバイスを使用していない場合は、SWMTP から **False** に対して **[フラグの実行]** 設定を選択でき、次のオプションを選択します。 **システム** > **サービス パラメータ** > **Cisco IP Voice Media Streaming App Service** > **MTP パラメータ**から、**[MTP コール数]** 設定を以下に追加します。 **メディアリソース** > **MOH サーバ** > **最大半二重ストリーム**ありません。コールのトラフィックによって、デフォルト設定を変更できます。ただし、サーバ パフォーマンスのアクティビティで CPU、メモリ、I/O 待機をモニタします。ユーザ数 7500 人の OVA 設定を使用しているような、容量の大きなクラスタでは、コール カウントのデフォルトのメディア デバイス設定を 25 %増やすことができます。

保留音のようにメディア デバイスの使用率が高くなることが予期される場合や、コールの数が多くてより多くのメディア接続数が必要とされる場合のインストールでは、呼処理が有効になっていない 1 つ以上の Cisco Unified Communications Manager サーバで Cisco IP Voice Media Streaming Application サービスを有効にします。このサービスを有効にすると、メディア デバイスの使用によって呼処理などのその他のサービスが受ける影響が限定的なものになります。次に、メディア デバイスのコールの最大数の構成時の設定を増加させることができます。

Cisco Unified Communications Manager サービスと共存するように Cisco IP Voice Media Streaming Application を有効にした場合、呼処理のパフォーマンスに影響を与える可能性があります。保留音やアナンシエータの容量設定をデフォルトの設定から増やす場合は、Cisco Unified Communications Manager を有効にせずにサーバで Cisco IP Voice Media Streaming Application を有効化することが推奨されています。

アクティブな発信者が保留中になっているときやマルチキャスト MOH のオーディオ ストリームが設定されているときは、CPU のパフォーマンスは MOH に影響されます。

Table 2: 一般的なパフォーマンス結果

設定に関する注意事項	CPU パフォーマンス
専用の MOH サーバ、保留中のコール 1000、グリーティングと定期アナウンスの MOH 音源 500。	25 ～ 45%（7500 ユーザの OVA 設定）
専用 MOH サーバとアナンシエータ サーバでのネイティブのコール キューイング、キューに入ったコール 1000、グリーティングと定期アナウンスの MOH 音源 500。アナンシエータでは、最大 300 のグリーティング アナウンスを同時に再生できます。	25 ～ 45%（7500 ユーザの OVA 設定）
専用の MOH サーバ、保留中のコール 500、グリーティングと定期アナウンスの MOH 音源 500。	15 ～ 35%（7500 ユーザの OVA 設定）

Table 3: 推奨される推定の上限数

設定	推奨される上限数
Cisco IP Voice Media Streaming Application が 2500 OVA 上で Cisco Unified Communications Manager と共存する場合（中程度の呼処理）。	MOH：保留中の発信者 500、MOH 音源 100、アナンシエータの発信者 48 ～ 64。
Cisco IP Voice Media Streaming Application が 2500 OVA 上の専用サーバである場合。	MOH：保留中の発信者 750、MOH 音源 250、アナンシエータの発信者 250。
Cisco IP Voice Media Streaming Application が 7500/10K OVA 上で Cisco Unified Communications Manager と共存する場合（中程度の呼処理）。	MOH：保留中の発信者 500、MOH 音源 250、アナンシエータの発信者 128。
Cisco IP Voice Media Streaming Application が 7500/10K OVA 上の専用サーバである場合。	MOH：保留中の発信者 1000、MOH 音源 500、アナンシエータの発信者 300 ～ 700（MOH のコーデックは 1 つ）。 **Note** MOH コーデックが 2 つの場合、アナンシエータの発信者を 300 に減らします。

Note この推奨の上限数は MOH や ANN デバイス固有のものです。これらのデバイスをソフトウェアのメディア ターミネーション ポイント（MTP）や話中転送（CFB）デバイスと組み合わせる場合、ストリームを提供するためには上限を減らします。

キャパシティ プランニングに関する設定の制限事項

Cisco IP Voice Media Streaming Application とセルフ プロビジョニング IVR サービスは、メディア カーネル ドライバを使用して Real-Time Transfer Protocol（RTP）ストリームを作成および制御します。このメディア カーネル ドライバのキャパシティは 6000 ストリームです。これらのストリームにより、メディア デバイスと IVR はリソースを予約できます。

この予約は、次のキャパシティ計算に基づきます。

メディア デバイス	容量
アナンシエータ	（[コール カウント（Call Count）] サービス パラメータ）* 3 3 はエンドポイントの受信（RX）コールと送信（TX）コール、および 1（.wav ファイル）の合計を示します。
ソフトウェア会議ブリッジ	（[コール カウント（Call Count）] サービス パラメータ）* 2 2 は RX および TX エンドポイントの合計ストリーム数を示します。
ソフトウェア メディア ターミネーション ポイント	（[コール カウント（Call Count）] サービス パラメータ）* 2 2 は RX および TX エンドポイントの合計ストリーム数を示します。
保留音	（（最大半二重ストリーム数）* 3）+（501 * 2 * [有効な MOH コーデックの数]） ここで、 • （最大半二重ストリーム数）は、MOH デバイス設定管理 Web ページの設定値です。 • 3 は、RX、TX、およびグリーティング アナウンスの .wav ファイルの合計ストリーム数を示します。 • 501 は、保留音（MOH）ソースの最大数を示します。 • 2 は、ミュージック .wav ストリームと発生する可能性のあるマルチキャスト TX ストリームを示します。 • [有効な MOH コーデックの数] は、Cisco IP Voice Media Streaming Application のサービス パラメータで有効な MOH コーデックの数に基づいています。
セルフ プロビジョニング IVR サービス	(500 * 2) 500 は発信者、2 は RX および TX ストリームからの合計ストリーム数を示します。

したがって、MOH が最大 1000 人の発信者をサポートできるようにする場合の式は、`1000 * 3 + 501 * 2 * 1 = 4002` ドライバ ストリーム（有効なコーデックの数は 1）、および `1000 * 3 +501 * 2 * 2 = 5004`（有効なコーデックの数は 2）となります。残りのデバイスの数を減

らし、セルフ プロビジョニング IVR サービスを無効にして、合計予約数を 6000 に制限します。これにより、MOH デバイスが予約を実行できるようになります。また、Cisco IP Voice Media Streaming Application と同じサーバでセルフ プロビジョニング IVR サービスをアクティブにできない場合があります。

メディア デバイスの設定がメディア デバイス ドライバのキャパシティを超える場合、デバイス ドライバに登録されているメディアデバイスが、必要なストリーム リソースを最初に予約できるようになります。後で登録されるメディアデバイスに対しては、必要なストリーム リソースよりも少ない数に制限されます。メディアデバイスを後から登録すると、一部のアラーム メッセージがログに記録され、制限されるメディア デバイスのコール数が自動的に削減されます。

Note キャパシティが 6000 ストリームのメディア カーネル ドライバでは、複数の同時メディア デバイス接続がサポートされていない可能性があります。

保留音オーディオ ソースの設定

保留音オーディオソースを設定するには、次の手順を使用します。オーディオストリームを設定し、アップロードされたファイルをオーディオストリームに関連付けることができます。最大500のオーディオストリームを設定できます。

Note オーディオ ソース ファイルの新しいバージョンを使用可能にするには、新しいバージョンを使用できるように更新手順を実行します。

Procedure

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **メディア リソース** > **複数のコールのオーディオ ソース**。

Step 2 次のいずれかを実行します。

- **[検索（Find）]** をクリックし、既存のオーディオ ストリームを選択します。
- 新しいストリームを設定するには、**[新規追加（Add New）]** をクリックします。

Step 3 **Moh オーディオストリーム番号**から、オーディオストリームを選択します。

Step 4 **[MOH オーディオ ソース名（MOH Audio Source Name）]** フィールドに、一意の名前を入力します。

Step 5 オプション。このファイルをマルチキャストできるようにするには、[**Allow Multi**] チェックボックスをオンにします。

Step 6 オーディオ ソースの設定：

- [**MOH WAV ファイル**ソースの使用] オプションボタンをオンにし、 **Moh オーディオソース ファイル**から、割り当てるファイルを選択します。

- [再ブロードキャスト **External Multicast source**] オプションボタンをオンにして、マルチキャスト送信元 IP アドレスの詳細を入力します。

Step 7 保留中**およびハントパイロットコールのアナウンス設定**セクションで、このオーディオソースに使用するアナウンスメントを割り当てます。

Step 8 **[保留音オーディオ ソースの設定（Music On Hold Audio Source Configuration）]** ウィンドウの残りのフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 9 [保存（Save）] をクリックします。

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration ソリューションは、Transport Layer Security（TLS）および Secure Real-time Transport Protocol（SRTP）を使用し、シグナリングとメディア暗号化を行います。現在、128ビット暗号キーを使用した Advanced Encryption Standard (AES) は、暗号化暗号として使用されています。AES では、認証方式として Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用されます。これらのアルゴリズムは、必要な変化するセキュリティとパフォーマンスのニーズに合わせて効果的に拡張することはできません。セキュリティとパフォーマンスの要件の増大に対応するため、Next-Generation Encryption（NGE）での、暗号化、認証、デジタル署名、およびキー交換用のアルゴリズムとプロトコルが開発されています。また、TLS および NGE をサポートするセッション開始プロトコル (SIP) SRTP の AES 128 の代わりに、AES 256 暗号化サポートが提供されます。

Unified Communications Manager リリース 10.5(2) では、AES 256 Encryption Support for TLS and SIP SRTP が、シグナリング暗号化とメディア暗号化での AES 256 暗号化のサポートに重点を置くために拡張されています。この機能は、Cisco Unified Communications Manager 上で実行されているアプリケーションが、SHA-2（Secure Hash Algorithm）標準規格および Federal Information Processing Standards（FIPS）に準拠する、AES-256 ベースの暗号を使用して TLS 1.2 接続を開始してサポートするために役立ちます。

この機能には、次の要件があります。

- SIP トランクと SIP 回線が開始する接続。
- Unified Communications Manager が SIP 回線と SIP トランクを通じた SRTP コール用にサポートする暗号化であること。

Note このリリースでは、TLS 1.2 は SIP などの一部のインターフェイスでサポートされていますが、すべてのインターフェイスでサポートされているわけではありません。TLS 1.0 および1.1 は、コラボレーション展開で有効にしたままにしておくことをお勧めします。

TLS での AES 256 および SHA 2 のサポート

Transport Layer Security（TLS）プロトコルでは、2つのアプリケーション間の通信の認証、データの整合性、および機密性が提供されます。TLS 1.2 はセキュア ソケット レイヤ（SSL）プロトコル バージョン 3.0 をベースにしていますが、これら 2 つのプロトコルに相互の互換性はありません。TLS はクライアント/サーバモードで動作し、一方がサーバとして機能し、もう一方がクライアントとして機能します。SSL は、伝送制御プロトコル (TCP) レイヤとアプリケーションの間のプロトコル層として配置され、クライアントとサーバ間のセキュアな接続を形成し、ネットワークを介して安全に通信できるようにします。TLS を動作させるには、信頼性の高いトランスポート層プロトコルとして TCP が必要です。

Unified Communications Manager リリース 10.5(2) における、TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポートは、SIP トランクおよび SIP 回線によって開始される接続を処理するための機能強化です。AES 256 および SHA-2 に準拠する、サポートされる暗号方式は次のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256: 暗号ストリングは AES128 で、...
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384: 暗号ストリングは AES256 です。 SHA384 です。

定義:

- TLS は、Transport Layer Security です
- ECDH は楕円曲線 Diffie-hellman (アルゴリズム) です。
- RSA is Rivest Shamir Adleman (アルゴリズム)
- AES は、Advanced Encryption Standards です
- GCM は、Galois/Counter Mode です

新しくサポートされた暗号方式に加えて、Unified Communications Manager リリース 10.5(2) では、TLS_RSA_WITH_AES_128_CBC_SHA が引き続きサポートされています。この暗号方式の暗号ストリングは AES128-SHA です。

Note

- Unified Communications Manager の証明書は、RSA に基づいています。
- Unified Communications Manager 10.5(2) では、シスコの各エンドポイント（各電話）で、上記の TLS 1.2 用の新しい暗号方式はサポートされません。
- Unified Communications Manager 10.5(2) において TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポート機能強化を使用すると、Certificate Authority Proxy Function（CAPF）のデフォルトのキー サイズが 2048 ビットに増えます。

SRTP SIP コールシグナリングでの AES 256 のサポート

Secure Real time Transport Protocol (SRTP) は、リアルタイムトランスポートプロトコル (RTP) の音声およびビデオメディアと、それに対応するリアルタイムトランスポート制御プロトコル(RTCP)ストリームの両方に機密性とデータの整合性を提供する方法を定義します。SRTPは、暗号化およびメッセージ認証ヘッダーを使用してこの方式を実装します。SRTP では、暗号化は rtp パケットのペイロードにのみ適用され、RTP ヘッダーには適用されません。ただし、メッセージ認証は RTP のヘッダーと RTP のペイロードの両方に適用されます。また、メッセージ認証がヘッダー内の RTP のシーケンス番号に適用されるため、SRTP ではリプレイ アタックに対する保護も間接的に提供されます。SRTP は、暗号化方法として 128 ビットの暗号キーによる Advanced Encryption Standard（AES）を使用します。また、認証方式として、Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用します。

Unified Communications Manager 10.5(2) では、SIP 回線と SIP トランクを通じた SRTP コール用の暗号方式がサポートされます。これらの暗号暗号方式は AEAD_AES_256_GCM と AEAD_AES_128_GCM であり、AEAD は関連データを使用して認証され、GCM は Galois/Counter モードです。これらの暗号方式はGCMに基づいています。これらの暗号方式がSession Description Protocol (SDP) に存在する場合、AES 128 および SHA-1 ベースの暗号方式よりも高いプライオリティで処理されます。シスコの各エンドポイント（電話）では、Unified Communications Manager 10.5(2) に SRTP のために追加した、これらの新しい暗号方式はサポートされません。

新たにサポートされる暗号方式に加えて、Unified Communications Manager 10.5(2) では次の暗号方式が引き続きサポートされます。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次のコールでサポートされています。

- Sip 回線から SIP 回線へのコールシグナリング
- Sip 回線から SIP トランクへのシグナリング
- Sip トランクから SIP トランクへのシグナリング

Cisco Unified Communications Managerの要求

- SIP トランクおよび SIP 回線接続での TLS バージョン1.2 のサポートを使用できます。
- 暗号サポート: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号ストリング ECDHE-AES256 SHA384) および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号ストリング ECDHE-AES128): TLS 1.2 接続が確立されたときに使用可能になります。これらの暗号方式は GCM に基づいており、SHA-2 カテゴリに準拠しています。
- Unified Communications Manager は TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号方式と TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号方式を使用して TLS 1.2 を開始し

ます。ピアが TLS 1.2 をサポートしていない場合、Unified Communications Manager は既存の AES128-SHA 暗号方式を使用した TLS 1.0 にフォールバックします。

- SIP 回線および SIP トランクを介した SRTP コールは、GCM ベースの AEAD_AES_256_GCM と AEAD_AES_128_GCM の暗号方式をサポートします。

連携動作と制限事項

- Unified Communications Manager の要件は、SIP 回線と SIP トランク、および基本的な SIP 間コールのみに適用されます。
- 非 SIP プロトコルに基づくデバイスタイプは、サポートされている暗号を使用した TLS バージョンの既存の動作を引き続きサポートします。Skinny Call Control Protocol (SCCP) は、以前にサポートされていた暗号方式を使用した TLS 1.2 もサポートしています。
- Sip から非 SIP へのコールでは、引き続き AES 128 および SHA-1 ベースの暗号方式が使用されます。

テレプレゼンス製品固有の構成のリモート制御

リリース 10.5(2) から、Cisco Unified Communications Manager は、Cisco TelePresence ユーザの代理として、Cisco TelePresence エンドポイントの製品固有の設定をリモートで取得し、管理することができます。

Cisco TelePresence エンドポイントが最初に Cisco Unified Communications Manager に登録された場合、または Cisco TelePresence ユーザがエンドポイントから製品固有の設定を変更した場合、SIP シグナリングマネージャデータベースにそれらの設定を伝達し、[電話の設定 (Phone Configuration)] ウィンドウの製品固有の設定の見出しの下に設定を表示します。

これらの設定を取得すると、Cisco Unified Communications Manager の管理者は、Cisco TelePresence ユーザに代わって、管理パスワードを含む製品固有の設定を設定および変更することができます。

新しい設定を電話機に戻すには、管理者が電話機をリセットする必要があります。

IM and Presence Service のストリーム管理

Cisco Unified Communications Manager IM and Presence Service リリース 10.5(2) では、インスタントメッセージング用のストリーム管理がサポートされています。ストリーム管理は、XEP-0198 仕様を使用して実装されています。これは、2 つの XMPP エンティティ間 (スタンザ受信確認とストリームの再開の機能を含む) をアクティブに管理するための Extensible Messaging and Presence Protocol (XMPP) を定義します。XEP-0198 の詳細については、次の仕様を参照してください。http://xmpp.org/extensions/xep-0198.html

IM and Presence Service と Cisco Jabber 間の通信が一時的に失われた場合、ストリーム管理によって、通信の停止中に送信されるすべてのインスタントメッセージが失われることはありません。設定可能なタイムアウト期間によって、メッセージの処理方法が決まります。

- Cisco Jabber がタイムアウト期間内にIM and Presence Service との通信を再確立した場合、メッセージは再送信されます。
- Cisco Jabber が IM and Presence Service との通信をタイムアウト期間内に再確立しない場合 、メッセージは送信者に返されます。
- タイムアウト期間の経過後に送信されたメッセージはオフラインで保存され、Cisco Jabber が IM and Presence Service との通信を再開するときに配信され ます。

管理者は、クラスタ全体でストリーム管理を有効にすることができます。次の Cisco XCP ルータのサービスパラメータを使用して、ストリームの管理を設定します。

サービス パラメータ	説明
ストリーム管理の有効化	ストリーム管理のクラスタ全体を有効または無効にします。 デフォルトの設定はイネーブルです。
ストリーム管理のタイムアウト	ストリームが再開されてメッセージが再送信されるまでにセッションが待機する最大秒数。IM and Presence Service への接続を この時間枠内に復元できない場合は、メッセージが送信者に返されます。 このタイムアウト後に送信されたメッセージはすべて、Cisco Jabber が IM and Presence Service を使用して再度ログインする前に、オフラインで保存され、再度ログインした後に再送信 されます。 デフォルト設定は 60 です。
ストリーム管理のバッファサイズ	バッファに保存可能なパケット最大数。Cisco Jabber がバッファ内の使用可能な容量を超えて必要とする場合、IM and Presence Service は、メッセージを受信するスペースを確保するために、メッセージがバッファから削除される前に、送信者にメッセージを返すようにします。 デフォルト設定は 100 です。

サービス パラメータ	説明
確認応答リクエスト率	Cisco Jabber の前に IM and Presence Service が送信したスタンザの数をリクエストすると、前回受信したスタンザのカウントが提供されます。 **Note** 確認応答リクエスト率が小さいと、ネットワークトラフィックが増加しますが、メモリ使用量は減少します。 デフォルト設定は 5 です。

これらのパラメータを設定するには、**Cisco Unified CM IM and Presence アドミニストレーション**にログインし、**システム** > **サービスパラメータ**を選択します。

IM and Presence Service の管理されたファイル転送

マネージド ファイル転送（MFT）を使用すると、Cisco Jabber などの IM and Presence サービス クライアントは他のユーザ、アドホック グループ チャット ルーム、および永続的なチャット ルームにファイルを転送することができます。ファイルは外部ファイル サーバのリポジトリに保存され、トランザクションが外部データベースのログに記録されます。

マネージドファイル転送の設定はこの機能に固有な設定であり、法規制コンプライアンスのためのメッセージ アーカイバ機能には影響しません。

管理ファイル転送機能の詳細については、*Cisco Unified Communications Manager* の *IM and Presence Service* の *[*設定とアドミニストレーションガイド*]* を参照してください。

2 つの新しいユーザインターフェイスウィンドウ

[外部ファイル サーバ（External File Servers）]

このウィンドウのコントロールを使用して、ユーザの資格情報や接続情報を含む IM and Presence Service 上の外部ファイルサーバを設定します。

ファイル転送設定

このウィンドウのコントロールを使用して、IM and Presence Service でのファイル転送に関する次のオプションのいずれかを設定できます。**無効化**、**ピアツーピア**、**マネージドファイル転送**、または**マネージドおよびピアツーピアのファイル転送**。

新しいファイル サーバのトラブルシューティング テスト

外部ファイルサーバの導入を完了すると、次の 7 つの新しいテストが実施されます。

- 外部ファイルサーバの到達可能性（ping 可能性）を確認します
- 外部ファイル サーバが接続をリッスンしていることを確認します。
- 外部ファイル サーバ公開キーが正しいことを確認します。

- ノードの公開キーが外部ファイル サーバで正しく設定されていることを確認します。
- 外部ファイル サーバ ディレクトリが有効であることを確認します。
- 外部ファイル サーバが正常に配置されたことを確認します。
- ファイル サーバ上に使用可能な空きディスク領域があることを確認します。

新しいリアルタイム監視ツールのマネージドファイル転送アラーム

アラームは 3 つあり、内 2 つはIM and Presence Serviceと外部ファイルサーバのディスク容量間の接続ステータスをテストするアラーム、もう 1 つは外部ファイルサーバ上のディスク容量をテストするアラームです。

- XcpMFTExtFsMountError—Cisco XCP File Transfer Manager で外部ファイル サーバとの接続が失われました。
- XcpMFTExtFsFreeSpaceWarn—Cisco XCP File Transfer Manager は、外部ファイル サーバの空きディスク領域が少ないことを検出しました。
- XcpMFTDBConnectError—Cisco XCP データ アクセス レイヤがデータベースに接続できませんでした。

新しいリアルタイム監視ツールのマネージドファイル転送カウンタ

リアルタイム監視ツール (RTMT) には、マネージドファイル転送機能用の新しいフォルダと 6 つの新しいカウンタが用意されています。

- Cisco XCP MFT カウンタ
  - MFTBytesDownloadedLastTimeslice
  - MFTBytesUpoadedLastTimeslice
  - MFTFilesDownloaded
  - MFTFilesDownloadedLastTimeslice
  - MFTFilesUploaded
  - MFTFilesUploadedLastTimeslice

廃止設定

Cisco xcp Router (Active) service の **[サービスパラメータの設定]** ウィンドウで、**[ファイル転送の有効化]** ドロップダウンリストが XCP ルータのグローバル設定 (Clusterwide) 領域から削除されています。