システム設定

概要

Cisco Unity Connection Administration の [システム設定（System Settings）] メニューにあるオプションを使用して、さまざまな機能やパラメータに関するシステム全体の設定を管理できます。

全般設定

管理者は [全般設定（General Configuration）] を使用して、Unity Connection 内のさまざまなシステム設定およびカンバセーション設定を管理できます。

システム設定には、デフォルト パーティション、デフォルト サーチ スペース、および Unity Connection がユーザと発信者に対してシステム プロンプトを再生するタイムゾーンが含まれます。カンバセーション設定には、Unity Connection システムでのデフォルト電話言語設定、メッセージとグリーティングのターゲット デシベル レベル、グリーティングの最大長が含まれます。

全般設定の管理

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して、[全般設定（General Configuration）] を選択します。

ステップ 2 [全般設定の編集（Edit General Configuration）] ページで、必要な設定値を入力します（各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照）。

ステップ 3 [保存（Save）] を選択します。

クラスタ

クラスタ設定ページにより、管理者は Unity Connection クラスタ関連の情報を表示したり管理したりできます。クラスタの設定にアクセスするには、Cisco Unity Connection Administration にサインインし、[システム設定（System Settings）] を展開し、[クラスタ（Cluster）] を選択します。

[サーバの検索とリスト（Find and List Servers）] ページには、インストールされている Unity Connection サーバのホスト名または IP アドレスとサーバの種類が表示されます。パブリッシャサーバのみがインストールされている場合、クラスタを構成するにはクラスタ設定でサブスクライバサーバの詳細を追加する必要があります。詳細については、「Configuring Cisco Unity Connection Cluster」（『Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 12.x』、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html）を参照してください。

パブリッシャ サーバまたはサブスクライバ サーバの詳細を [サーバの設定（Server Configuration）] ページで管理できます。そこでは、サーバのホスト名、IP アドレス、MAC の詳細、およびローカル帯域幅管理（LBM）の情報を指定します。各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照してください。

認証規則

Unity Connection の認証規則は、ユーザのパスワード、PIN、ユーザ アカウント ロックアウトに関するポリシーに反映されます。認証規則では、無効な PIN やパスワードを入力したユーザをロックアウトすることで、Unity Connection Web アプリケーション（Cisco PCA、Web Inbox など）への不正アクセスを防止します。事前に定義されている 2 つの認証規則は、[ボイスメール認証規則（推奨）（Recommended Voice Mail Authentication Rule）] と [Web アプリケーション認証規則（推奨）（Recommended Web Application Authentication Rule）] です。

ユーザを Unity Connection に追加する際には、そのユーザ アカウントの作成に使われたユーザ テンプレートにより、電話機 PIN と Web アプリケーション パスワードが決まります。デフォルトでは、ユーザ テンプレートには、ランダムに生成された文字列が電話機 PIN および Web パスワードとして割り当てられます。1 つのユーザ テンプレートから作成されたすべてのユーザには、同じ PIN とパスワードが割り当てられます。アカウント詳細情報へのアクセスを保護するために、ユーザは次回のサインイン時にこのパスワードまたは PIN を変更する必要があります。

Unity Connection で PIN とパスワードを設定するときには、次の点を考慮してください。

- セキュリティ設定を強化するには、PIN とパスワードを頻繁に変更してください。Web アプリケーションと電話機のパスワードの変更については、ユーザの章を参照してください。

（注） ユーザは Messaging Assistant を使用して PIN とパスワードを変更することもできます。

- 不正アクセスや不正通話から Unity Connection を保護するには、すべてのユーザに一意の電話機 PIN および Web アプリケーション パスワードを割り当てる必要があります。
- PIN とパスワードは、6 文字で容易に推測できないものにする必要があります。

さまざまな Unity Connection アプリケーションで使用する PIN とパスワードを次に示します。

- ボイスメール パスワード：ボイスメール パスワードは、電話機を使用して Unity Connection カンバセーションにサインインするときに使われます。ユーザは電話機のキーパッドを使用して、数字だけからなるパスワードを入力するか、音声認識が有効な場合は PIN を読み上げます。
- Web アプリケーション パスワード：これは、Unity Connection の Web アプリケーション（Messaging Assistant や Web Inbox など）にサインインするためにユーザが使用するパスワードです。

（注） Cisco Business Edition または LDAP 認証を使用している場合、ユーザが Unity Connection Web アプリケーションにアクセスするには、Cisco Business Edition または LDAP のユーザ パスワードを使用する必要があります。

認証規則の設定

Cisco Unity Connection Administration で認証規則を設定すると、次の項目を決定するのに役立ちます。

- アカウントがロックされる条件となる、Unity Connection 電話インターフェイス、Cisco PCA、または Unity Connection Administration へのサインイン試行失敗回数。
- アカウントがリセットされるまでロックが維持される分数。
- ロックされたアカウントを管理者が手作業でロック解除する必要があるかどうか。
- パスワードと PIN に許可される最小長。
- パスワードまたは PIN の有効期限が切れるまでの日数。

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して、[認証規則（Authentication Rules）] を選択します。
[認証規則の検索（Search Authentication Rules）] ページが表示され、現在設定されている認証規則が示されます。

ステップ 2 認証規則を設定します（各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照）。

- 認証規則を追加するには、次の手順を実行します。

  [認証規則の検索（Search Authentication Rules）] ページで [新規追加（Add New）] を選択します。

  [認証規則の新規作成（New Authentication Rules）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します。

- 既存の認証規則を編集するには、次の手順を実行します。

  [認証規則の検索（Search Authentication Rules）] ページで、編集する認証規則を選択します。

  [認証規則の編集（Edit Authentication Rules）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します。

- 1 つ以上の認証規則を削除するには、次の手順を実行します。

  [認証規則の検索（Search Authentication Rules）] ページで、削除する認証規則を選択します。

  [選択項目の削除（Delete Selected）] を選択し、[OK] を選択して削除を確定します。

ロール

ロールは、システムに対するアクセス レベルを定義する一連の権限で構成されています。システム管理者は管理上の必要に基づいて複数のロールを設定できます。必要な操作のセットに基づいて、ユーザ アカウント用のロールを割り当てることができます。Unity Connection では 2 種類のロールを提供しています。

- システム ロール：システム ロールは、Unity Connection と一緒にインストールされる定義済みのロールです。
- カスタム ロール：カスタム ロールは、システム管理者が作成、更新、削除できるロールです。

（注） ユーザの [役割の編集（Edit Roles）] ページで、1 人以上のユーザに対する任意のロールの割り当てまたは削除を行うことができます。詳細については、ユーザの章を参照してください。

ロールの設定

要件に基づいてカスタム ロール（役割）を作成、変更、削除できます。

カスタム役割を設定するには

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] > [役割（Roles）] を展開して、[カスタム役割（Custom Roles）] を選択します。
[カスタム役割の検索（Search Custom Role）] ページが表示され、現在設定されているカスタム役割が示されます。

ステップ 2 カスタム役割を設定します。

- カスタム役割を追加するには、次の手順を実行します（各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照）。

1. [新規追加（Add New）] を選択します。[カスタム役割の新規作成（New Custom Role）] ページが表示されます。
2. フィールドに必要な情報を入力します。
3. カスタム役割に割り当てる権限を選択します。
   （注） [システム設定データへの読み取りアクセス権 - 読み取りアクセス権（Read Access to System Configuration Data - Read Access）] 権限を必ず選択してください。
4. [保存（Save）] を選択します。

- カスタム役割を更新するには、次の手順を実行します。
  1. 編集するカスタム役割を選択します。[カスタム役割の編集（Edit Custom Role）] ページが表示され、カスタム役割の現在の設定が示されます。
  2. 必要に応じて、カスタム役割の設定を編集します。
  3. [保存（Save）] を選択します。
- カスタム役割を削除するには、次の手順を実行します。
  1. 削除するカスタム役割の横にあるチェックボックスをオンにします。
  2. [選択項目の削除（Delete Selected）] を選択します。
     （注） 「ロールの削除後には、ユーザとの関連付けが削除されます（After role deletion, it's association with the users will be removed）」というメッセージが表示されます。
  3. [OK] を選択して削除を確認します。
     （注） 複数の役割を削除するには、複数のチェックボックスを一緒にオンにします。

ユーザへのロールの割り当てまたは削除

システム設定からユーザへのロール（役割）の割り当てまたは削除を行うには

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）]> [役割（Roles）] を展開して、以下のいずれかを選択します。

- [システム役割（System Roles）] : [役割の検索（Search Roles）] ページが表示され、すでに設定されているシステム役割が示されます。
- [カスタム役割（Custom Roles）] : [カスタム役割の検索（Search Custom Roles）] ページが表示され、すでに設定されているカスタム役割が示されます。

ステップ 2 次のようにして、1 人以上のユーザに役割を割り当てます（各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照）。

a) 1 人以上のユーザに割り当てる役割を選択します。

b) 選択した役割の [編集（Edit）] ページで [役割の割り当て（Role Assignments）] を選択します。

（注） 割り当てる特定の役割に関する [ユーザ検索（Find Users）] ドロップダウン リストから、[次の役割に属さない（not in）] を必ず選択してください。

c) 役割を割り当てるユーザの横にあるチェックボックスをオンにし、[選択項目の割り当て（Assign Selected）] を選択します。

ステップ 3 1 人以上のユーザから役割を削除します（各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照）。

a) 1 人以上のユーザから削除する役割を選択します。

b) 選択した役割の [編集（Edit）] ページで、[役割の割り当て（Role Assignments）] を選択します。
c) 役割を削除するユーザの横にあるチェックボックスをオンにし、[選択項目の削除（Remove Selected）] を選択します。

規制テーブル

規制テーブルを使用することで、ユーザや管理者がコール転送、メッセージ通知、およびファクス発信に使用できる電話番号または URI を制御したり、特定の内線番号が代行内線番号として追加されないよう規制したりできます。詳細については、「規制テーブル」を参照してください。

ライセンス

[ライセンス（License）] 設定ページには、Unity Connection サーバのライセンス情報が表示されます。Unity Connection 12.0(1) 以降では、ライセンスは**シスコ スマート ソフトウェア ライセンシング**で管理されます。このライセンシング モデルではライセンシングの柔軟性が高まり、企業全体でライセンシングが簡素化されます。さまざまなライセンス機能を使用するには、Unity Connection を Cisco Smart Software Manager（CSSM）または Cisco スマート ソフトウェア マネージャ サテライトに登録する必要があります。

Cisco Smart Software Manager（CSSM）または Cisco スマート ソフトウェア マネージャ サテライトに登録されるまでは、Unity Connection は評価モードのままになります。Unity Connection ライセンスについては、『*Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 12.x*』の「Managing Licenses」の章を参照してください。このガイドは https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html から入手できます。

スケジュール

[スケジュール（Schedule）] 設定ページは、Unity Connection 内のさまざまなスケジュールを管理するのに役立ちます。管理者は、ユーザまたはコール ハンドラに適用されるスケジュールに基づき、グリーティング、転送タイプ、アクセス権を制御できます。詳細については、「スケジュール」（ページ 8-24）を参照してください。

祝日スケジュール

祝日スケジュールはアクティブ スケジュールと連動して、グリーティング、転送タイプ、アクセス権を制御します。詳細については、祝日スケジュール（ページ 16-4）を参照してください。

グローバル ニックネーム

グローバル ニックネーム リストは、発信者が音声認識を使用して電話をかけたりメッセージを送ったりするときにUnity Connectionが考慮する、一般的なニックネームの包括的リストです。たとえば、Unity Connection は名前「William」に対応するニックネームとして「Bill」、「Billy」、「Will」を検討します。

ユーザの名前が一般的なものでない場合や、別の名前（旧姓など）で他のユーザに知られている場合には、ユーザに別名を追加することを考慮してください。ユーザの別名を追加することで、発信者がユーザを名前で呼び出したときに Unity Connection で通話できる確率が高くなります。

Unity Connection でのグローバル ニックネームの設定

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して、[グローバル ニックネーム（Global Nicknames）] を選択します。
[グローバル ニックネームの検索（Search Global Nicknames）] ページが表示され、現在設定されているグローバル ニックネームが示されます。

ステップ 2 ニックネームを設定します（各フィールドの詳細については、[ヘルプ（Help）]>[このページ（This Page）] を参照）。

- ニックネームを追加するには、次の手順に従います。

  [グローバル ニックネームの検索（Search Global Nicknames）] ページで [新規追加（Add New）] を選択します。

  [グローバル ニックネームの新規作成（New Global Nicknames）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します。

- ニックネームを編集するには、次の手順を実行します。

  [グローバル ニックネームの検索（Search Global Nicknames）] ページで、編集するニックネームを選択します。

  [グローバル ニックネームの編集（Edit Global Nicknames）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します。

- ニックネームを削除するには、次の手順に従います。

  [グローバル ニックネームの検索（Search Global Nicknames）] ページで、削除するニックネームを選択します。

  [選択項目の削除（Delete Selected）] を選択し、[OK] を選択して削除を確定します。

件名行の形式

Web Inbox、Messaging Inbox、IMAP クライアント、RSS クライアント、またはメッセージ件名を表示する他のいずれかのビジュアル クライアントでユーザがメッセージを表示または再生すると、メッセージの件名行が表示されます。ユーザが電話機でボイス メッセージを再生するときには、件名行が提供されません。

ボイス メッセージの件名行に含める単語と情報の両方を設定できます。受信者の言語に応じて、件名行をローカライズすることもできます。

次のタイプのメッセージに関して、件名行の形式が定義されています。

1. ボイス メッセージの場合：

- 外部発信者のメッセージ：識別できないボイス メッセージ、または Unity Connection ユーザではない発信者からのメッセージ。これには、システム コール ハンドラに残されたメッセージも含まれます。
- ユーザ間のメッセージ：識別されたボイス メッセージ、または Unity Connection ユーザからのメッセージ。
- インタビュー ハンドラ メッセージ：インタビュー ハンドラに残されたメッセージ。
- ライブ レコード メッセージ：ユーザと発信者との間の通信中に録音された会話が含まれるメッセージ。

2. 通知の場合：

- メッセージ通知：これには、Unity Connection ユーザに送信される新規ボイス メッセージの電子メール通知が含まれます。
- 不在着信通知：これには、不在着信に関する電子メール通知が含まれます。
- スケジュールされたサマリ通知：これには、スケジュールされた時刻に送信される電子メール通知が含まれます。

件名行の形式の設定

件名行の形式を定義するときは、次のことに注意してください。

- パラメータの前後に % を指定する必要があります。
- システムにインストールされている言語ごとに、別の件名行の形式を定義できます。
- ユーザの優先言語に件名行の形式が定義されていない場合、システムのデフォルト言語の件名行の形式定義が代わりに使用されます。
- メッセージが同報リストに送信されるときには、同報リストのすべての受信者に、システム デフォルト言語の件名行の形式が使用されます。各受信者の優先言語で件名行を定義する必要はありません。

- ボイス メッセージをデータベースに保存するときに、件名フォーマットがボイス メッセージに適用されます。件名行の形式定義を変更しても、すでにユーザ メールボックスにあるメッセージは変更されません。新しい件名定義は、変更の保存後に録音されるボイス メッセージにだけ反映されます。

Unity Connection での件名行の形式の設定

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して [件名行の形式（Subject Line Formats）] を選択します。

ステップ 2 [件名行の形式の編集（Edit Subject Line Formats）] ページで、必要なフィールドまたはパラメータに値を入力します（各フィールドの詳細については、[ヘルプ（Help）] > [このページ（This Page）] を参照）。

ステップ 3 [保存（Save）] を選択します。

添付ファイルの説明

サードパーティ製のメッセージ ストアに統合されている Unity Connection は、電話でメッセージを確認するユーザ向けに、メッセージ添付ファイルに関するテキスト/スピーチ（TTS）による説明を使用します。たとえば、拡張子 .jpg が付いた添付ファイルは「イメージ」と説明されます。

メッセージ添付ファイルの説明の設定

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して、[添付ファイルの説明（Attachment Descriptions）] を選択します。
[メッセージ添付ファイルの TTS 説明の検索（Search TTS Descriptions of Message Attachments）] ページが表示され、現在設定されているメッセージ添付ファイルの説明が示されます。

ステップ 2 メッセージ添付ファイルの説明を設定します（各フィールドの詳細については、[ヘルプ（Help）]>[このページ（This Page）] を参照）。

- メッセージ添付ファイルの説明を追加するには、次の手順を実行します。

  [メッセージ添付ファイルの TTS 説明の検索（Search TTS Descriptions of Message Attachments）] ページで [新規追加（Add New）] を選択します。

  [メッセージ添付ファイルの TTS 説明の新規作成（New TTS Description of Message Attachment）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します

- メッセージ添付ファイルの説明を編集するには、次の手順を実行します。

[メッセージ添付ファイルの TTS 説明の検索（Search TTS Descriptions of Message Attachments）] ページで、編集する添付ファイルを選択します。

[メッセージ添付ファイルの TTS 説明の編集（Edit TTS Descriptions of Message Attachments）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します

- メッセージ添付ファイルの説明を削除するには、次の手順を実行します。

[メッセージ添付ファイルの TTS 説明の検索（Search TTS Descriptions of Message Attachments）] ページで、削除する添付ファイルを選択します。

[選択項目の削除（Delete Selected）] を選択し、[OK] を選択して削除を確定します。

エンタープライズ パラメータ

Unity Connection のエンタープライズ パラメータは、Cisco Unified Serviceability のすべてのサービスに適用されるデフォルト設定を提供します。エンタープライズ パラメータを表示および管理するには、Cisco Unity Connection Administration にサインインし、[システム設定（System Settings）] を展開して [エンタープライズ パラメータ（Enterprise Parameters）] を選択します。

Cisco Unified Serviceability サービスの詳細については、『Cisco Unified Serviceability Administration Guide Release 10.0(1)』（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/10_0_1/admin/CUCM_BK_CDDBCDEB_00_cisco-unified-serviceability-merge-100.html）を参照してください。

表 16-1 では、Unity Connection で使用できるエンタープライズ パラメータについて説明します。この表に記述されていないフィールドは、Cisco Unified Communications Manager から管理します。

エンタープライズ パラメータの説明

パラメータ名	説明
[クラスタID（Cluster ID）]	サーバのパラメータ値を指定します。管理者は[エンタープライズ パラメータ（Enterprise Parameters）] ページからこのパラメータ値を編集することができません。
[デバイス レベル トレースの最大数（Max Number of Device Level Trace）]	Cisco Unified Serviceability の [トレース設定（Trace Configuration）] でデバイス名ベースのトレースを選択した場合は、同時にトレースできるデバイスの数を指定します。 デフォルト設定：12 最小値：0 最大値：256
ローカリゼーション パラメータ	

パラメータ名	説明
[デフォルトのネットワーク ロケール（Default Network Locale）]	音声の変調とトーンに関するデフォルト ネットワーク ロケールを指定します。選択されたネットワーク ロケールは、デバイスまたはデバイスプール レベルでネットワーク ロケールが設定されていない、すべてのゲートウェイと電話機に適用されます。 （注） 選択されたネットワーク ロケールが、すべてのゲートウェイと電話機にインストールされ、サポートされていることを確認してください。パラメータ変更を反映するには、すべてのデバイスをリセットしてください。 デフォルト設定：United States
[デフォルトのユーザ ロケール（Default User Locale）]	言語選択のデフォルトのユーザ ロケールを指定します。すべてのモデルで、すべてのロケールがサポートされるわけではありません。この設定がサポートされないモデルの場合は、サポートされているロケールを明示的に設定します。 （注） パラメータ変更を反映するには、すべてのデバイスをリセットしてください。 デフォルト設定：English United States
ロールバック用のクラスタ準備	
[8.0以前へのロールバック用のクラスタ準備（Prepare Cluster for Rollback to Pre 8.0）]	Unity Connection クラスタを新しいバージョンにアップグレードする場合、この設定で Unity Connection の旧バージョンを指定します。 デフォルト設定：False
トレース パラメータ	
[ファイル クローズ スレッド フラグ（File Close Thread Flag）]	個別のスレッドを使用して、トレース ファイルを閉じられるようにします。トレース ファイル終了時のシステム パフォーマンスが向上する場合があります。 デフォルト設定：True
FileCloseThreadQueueWaterMark	トレース ファイルを閉じるために使用される個別のスレッドが、トレース ファイルを閉じることを停止する上限を定義します。その後は、個々のスレッドを使用せずにトレース ファイルが閉じられます。 デフォルト設定：100 最小値：0 最大値：500
クラスタ全体のドメイン設定パラメータ	

パラメータ名	説明
[組織の最上位ドメイン（Organization Top Level Domain）]	組織のトップ レベル ドメインを定義します（たとえば、cisco.com）。 最大長：255 許容される値：大文字および小文字の英字（a ～ z、A ～ Z）、数字（0 ～ 9）、ハイフン（-）、またはピリオド（.）からなる最大 255 文字の有効なドメイン（たとえば cisco.com）を指定します。ドメイン ラベルの区切り文字はドットです。ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベル（たとえば、.com）の先頭文字を数字にすることはできません。たとえば、Abc.1om は無効なドメインです。
[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]	このクラスタの 1 つまたは複数の完全修飾ドメイン名（FQDN）を定義します。複数の FQDN はスペースで区切る必要があります。アスタリスク（*）を使用して、FQDN 内でワイルドカードを指定することができます。たとえば、cluster-1.rtp.cisco.com や *.cisco.com のように定義します。ホスト部分がこのパラメータの FQDN と一致する URL を含む要求（たとえば SIP コール）は、このクラスタまたはこのクラスタに接続されたデバイスあるいはその両方に対する要求として認識されます。 最大長：255 許容される値：1 つ以上の FQDN、または * ワイルドカードを使用した FQDN の一部（たとえば cluster-1.cisco.com または *.cisco.com）を指定します。複数の FQDN はスペースで区切る必要があります。使用可能な文字は、次のとおりです。 • 大文字または小文字（a ～ z または A ～ Z） • 数字（0 ～ 9） • ハイフン（-） • アスタリスク（*） • ドット（.）ドメイン ラベルの区切り文字はドットです。 ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベル（たとえば、.com）の先頭文字を数字にすることはできません。たとえば、Abc.1om は無効なドメインです。
Cisco サポートが使用	
Cisco Support Use 1	シスコ テクニカル サポートだけが使用します。 最大長：10
Cisco Support Use 2	シスコ テクニカル サポートだけが使用します。 最大長：10

パラメータ名	説明
Cisco Syslog Agent	
[リモート Syslog サーバ名 1 ～リモート Syslog サーバ名 5（Remote Syslog Server Name 1 to Remote Syslog Server Name 5）]	Syslog メッセージ受信のために使用する、リモート Syslog サーバの名前または IP アドレスを入力します。Syslog メッセージを受け入れるためのリモート Syslog サーバを最大 5 つ設定できます。サーバ名が指定されていない場合、Cisco Unified Serviceability は syslog メッセージを送信しません。Cisco Unified Communications Manager サーバは別のサーバからの Syslog メッセージを受信しないため、Cisco Unified Communications Manager サーバを宛先として指定しないでください。 最大長：255 許容される値：次の文字を使用した有効なリモート Syslog サーバ名を指定します。 • A ～ Z • a ～ z • 0 ～ 9 • . • -
[リモート Syslog メッセージの Syslog 重大度（Syslog Severity for Remote Syslog Messages）]	リモート Syslog サーバの、対象となる Syslog メッセージの重大度を選択します。選択された重大度以上のすべての Syslog メッセージが、リモート Syslog に送信されます。リモート サーバ名が指定されていない場合、Cisco Unified Serviceability は Syslog メッセージを送信しません。 デフォルト設定：Error
CUCReports パラメータ	
[レポート ソケット Unity Connection タイムアウト（Report Socket Unity Connection Timeout）]	別のサーバとの Unity Connection を確立するときに使用される最大秒数を指定します。低速ネットワークで Unity Connection に問題が発生する場合は、この時間を長くしてください。 デフォルト設定：10 最小値：5 最大値：120
[レポート ソケット読み取りタイムアウト（Report Socket Read Timeout）]	別のサーバからデータを読み取るときに使用される最大秒数を指定します。低速ネットワークで Unity Connection に問題が発生する場合は、この時間を長くしてください。 デフォルト設定：60 最小値：5 最大値：600

サービス パラメータ

Unity Connection のサービス パラメータを使用して、Cisco Unified Serviceability のさまざまなサービスを設定できます。サービス パラメータのリストと説明を確認するには、[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの疑問符ボタンを選択します。

Cisco Unified Serviceability でサービスをオフにした場合、Unity Connection は、更新されたサービス パラメータの値を保持します。サービスを再起動したときに、Unity Connection はサービス パラメータを変更後の値に設定します。

サービス パラメータを表示および管理するには、Cisco Unity Connection Administration にサインインし、[システム設定（System Settings）] を展開して [サービス パラメータ（Service Parameters）] を選択します。

Cisco Unified Serviceability サービスの詳細については、『Cisco Unified Serviceability Administration Guide Release 10.0(1)』（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/10_0_1/admin/CUCM_BK_CDDBCDEB_00_cisco-unified-serviceability-merge-100.html）を参照してください。

注意 サービス パラメータの一部の変更は、システム障害の原因になることがあります。変更しようとしている機能を完全に理解している場合や、Cisco Technical Assistance Center（TAC）から変更の指定があった場合を除いて、サービス パラメータに変更を加えないようにしてください。

表 16-2 に、Unity Connection で変更できるサービス パラメータを説明します。この表に記述されていないフィールドは、Cisco Unified Communications Manager から管理します。

サービス パラメータの説明

サービス パラメータ	説明
Cisco AMC サービス	
Primary Collector	クラスタ全体のリアルタイム情報を収集するプライマリ AMC（AlertMgr および Collector）サーバを指定します。値は、設定済みのサーバのいずれか（できれば、通話処理がほとんどないサーバ）と一致している必要があります。
Failover Collector	フェールオーバー AMC（AlertMgr および Collector）サーバを指定します。このパラメータで指定したサーバは、プライマリ AMC がダウンしている場合、または到達できない場合にリアルタイムデータを収集するために使用されます。Primary Collector がアクティブではなく、Failover Collector が指定されない場合は、データが収集されません。

サービス パラメータ	説明
Data Collection Enabled	リアルタイム クラスタ情報の収集とアラートを、有効（True）または無効（False）のいずれにするかを決定します。 デフォルト設定：True
Data Collection Polling Rate	AMC 収集レートを秒単位で指定します。 デフォルト設定：30 最小値：15 最大値：300 単位：秒
Server Synchronization Period	プライマリ AMC が動作し、アクティブに収集しているかどうかを判断するために、バックアップ AMC（AlertMgr および Collector）が起動時に待機する時間を秒単位で指定します。このパラメータによって、バックアップ AMC が、過度に早く収集タスクを引き継ぐことが防止されます。 （注） パラメータ変更を有効にするには、バックアップ サーバで AMC サービスを再起動します。 デフォルト設定：60 最小値：15 最大値：300 単位：秒
RMI Registry Port Number	RMI レジストリをオンにするポート番号を指定します。このポートを使用して、プライマリまたはバックアップ AMC が他の AMC を検出し、RTMT サーブレットがプライマリ/バックアップ AMC を検出します。 （注） パラメータ変更を有効にするには、AMC サービスを再起動します。 デフォルト設定：1099 最小値：1024 最大値：65535
RMI Object Port Number	RMI リモート オブジェクト用に使用するポート番号を指定します。このポートは、AMC が他の AMC および RTMT サーブレットとデータを交換するために使用されます。 （注） パラメータ変更を有効にするには、AMC サービスを再起動します。 デフォルト設定：1090 最小値：1024 最大値：65535
AlertMgr Enabled	（*AMC* トラブルシューティング専用）アラート（電子メールや epage）機能を有効または無効にします。 （注） パラメータ変更を有効にするには、AMC サービスを再起動します。 デフォルト設定：True

サービス パラメータ	説明
Logger Enabled	（*AMC* トラブルシューティング専用）ロギング機能（レポートを生成するための .csv ファイル）を有効または無効にします。 （注） パラメータ変更を有効にするには、AMC サービスを再起動します。 デフォルト設定：True
Cisco Database Layer Monitor サービス	
Maintenance Time	コール詳細記録（CDR）データベース メンテナンスを開始する時刻を指定します。このパラメータは、Maintenance Window パラメータと組み合わせて使用します。たとえば、このパラメータを 22 と指定すると、CDR メンテナンスは午後 10 時に開始します。Maintenance Window パラメータを 2 に設定すると、CDR メンテナンスは午後 10 時から深夜 0 時まで 1 時間ごとに実行されます。両方のパラメータを 24 に設定した場合、CDR メンテナンスは一日中、1 時間ごとに実行されます。CDR メンテナンス中は、最も古いCDR および関連するコール管理レコード（CMR）がシステムにより削除されます。したがって、最大CDR レコードパラメータで指定されたレコードの最大数は維持されます。また、メンテナンス中、CDR ファイル数が 200 を超えた場合はアラームが発生し、破損したサーバ間のレプリケーション リンクがチェックされ、その再初期化が試行されます。 デフォルト設定：24 最小値：1 最大値：24 単位：時間
Maintenance Window	CDR メンテナンスを実施する時間を指定します。たとえば、このパラメータを 12 に設定した場合、CDR メンテナンスは、Maintenance Time パラメータで指定した時刻から 12 時間にわたり、1 時間ごとに実行されます。たとえば、Maintenance Time パラメータが 7、このパラメータが 12 に設定されている場合、CDR メンテナンスは午前 7 時に開始し、午後 7 時まで毎時間実行されます。両方のパラメータが 24 に設定されている場合、CDR メンテナンスは全日、毎時間実行されます。CDR メンテナンス中は、最も古いCDR および関連する CMR がシステムにより削除されます。したがって、最大CDR レコードパラメータで指定されたレコードの最大数は維持されます。また、メンテナンス中、CDR ファイル数が 200 を超えた場合はアラームが発生し、破損したサーバ間のレプリケーション リンクがチェックされ、その再初期化が試行されます。 デフォルト設定：2 最小値：1 最大値：24 単位：時間

サービス パラメータ	説明
Table Out of Sync Detection	このパラメータをOnに設定した場合は、データベース レプリケーションステータスの概要が、メンテナンス時間中に毎日収集され、連続する3日間の出力と比較して、3日間を通じて同期されていない表があるかどうかが判断されます。それが存在する場合は、警告が発生します。デフォルトでは、このパラメータはOffに設定され、Maintenance Timeパラメータで指定した時間に実行されます。 デフォルト：Off
MaintenanceTaskTrace	メンテナンスタスクトレースを設定します。メンテナンスタスクからパフォーマンス カウンタ トレースを取得するには、このパラメータをオンにする必要があります。 必須フィールドです。 デフォルト設定：Off
Cisco DirSync	
Maximum Number of Agreements	Cisco Unified CM Administrationの [LDAPディレクトリ（LDAP Directory）] ウィンドウ（[システム（System）] > [LDAP] > [LDAPディレクトリ（LDAP Directory）]）で設定可能なLDAPディレクトリ（規定とも呼ばれます）の最大数を指定します。複数のLDAPディレクトリを作成すると、複数の検索ベースからユーザを同期する際に役立ちます。 （注） パラメータ変更を有効にするには、Cisco DirSyncサービスを再起動する必要があります。 デフォルト設定：5 最小値：1 最大値：5
Maximum Number of Hosts	フェールオーバー用として設定できるLDAPホスト名の最大数を指定します。 （注） パラメータ変更を有効にするには、Cisco DirSyncサービスを再起動する必要があります。 デフォルト設定：3 最小値：1 最大値：3
Retry Delay on Host Failure (secs)	Cisco Unified CM Administrationで設定した最初のLDAPサーバ（ホスト名）へのUnity Connection接続を再試行するまでに待機する時間（秒単位）を指定します。Unity Connection接続が失敗すると、同じホストへの再接続が3回試行されます。3回目の試行も失敗した場合、リスト内の階層順で次のホスト名への接続が試行されます。 デフォルト設定：5 最小値：5 最大値：60

サービス パラメータ	説明
Retry Delay on HostList Failure (mins)	Cisco Unified CM Administration で設定したすべての LDAP サーバ（ホスト名）への接続を再試行するまでに待機する時間（分単位）を指定します。LDAP サーバへの Unity Connection 接続は、Cisco Unified CM Administration で表示される順序で試行されます。3 回の試行は、Retry Delay On Host Failure サービス パラメータで指定した待機間隔に基づいて実行されます。3回の試行がすべて失敗すると、リスト内の次の LDAP サーバが試行されます。リスト内のどのサーバにも接続できない場合は、エラーがログに記録され、次の同期間隔が経過するまで待機してから、リスト内の最初のサーバから接続が再試行されます。 デフォルト設定：10 最小値：10 最大値：120
LDAP Unity Connection Timeout (secs)	Unity Connection で LDAP 接続を確立するために許可される時間（秒単位）を指定します。指定した時間内に Unity Connection への接続を確立できない場合、LDAP サービス プロバイダーは接続試行を中止します。 デフォルト設定：5 最小値：1 最大値：60
Delayed Sync Start Time (mins)	Cisco DirSync サービスが起動してからディレクトリ同期プロセスを開始するまでの待機時間を指定します。ディレクトリ同期によって、LDAP サーバのユーザは、Cisco Unified Communications Manager データベースにコピーされます。 （注） パラメータ変更を有効にするには、Cisco Tomcat サービスを再起動する必要があります。 デフォルト設定：5 最小値：5 最大値：60
Cisco RIS Data Collector パラメータ	
RIS Cluster TCP Port	クラスタ内の Cisco RIS Data Collector サービスが相互通信するために使用する静的 TCP ポートを指定します。 必須フィールドです。 （注） パラメータ変更を有効にするには、クラスタ内の各サーバで Cisco RIS Data Collector サービスを再起動してください。 デフォルト設定：2555 最小値：1024 最大値：65535

サービス パラメータ	説明
RIS Client TCP Port	RIS クライアントが、クラスタ内の Cisco RIS Data Collector サービスと通信するために使用する静的 TCP ポートを指定します。注：このパラメータの変更を有効にするには、クラスタ内の各サーバで、Cisco Database Layer Monitor サービスと Cisco the RIS Data Collector サービスを再起動する必要があります。 （注） パラメータ変更を有効にするには、クラスタ内の各サーバで、Cisco Database Layer Monitor サービスと Cisco the RIS Data Collector サービスを再起動してください。 デフォルト設定：2556 最小値：1024 最大値：65535
RIS Client Timeout	RIS クライアントが Cisco RIS Data Collector サービスからの応答を待機する時間（秒単位）を指定します。各サーバで実行される RIS Data Collector サービスは、このパラメータで指定した値の 90% を内部に割り当てます。複数のサーバがあるクラスタに関してこのパラメータを正しく設定するには、クラスタ内で RIS Data Collector サービスを実行するサーバ数の 4 倍（以上）の値を指定します。 比較的高い値を選択すると、1 つのサーバの RIS Data Collector サービスが別のサーバの RIS Data Collector サービスから応答を受信するために十分な時間が割り当てられます。応答に必要な時間は、サーバのプロセッサ速度、サーバに登録されているデバイスの数、サーバ メモリの容量、コールの量などの要因、およびパフォーマンスに影響を及ぼすその他の要因によって変化します。 デフォルト設定：30 最小値：10 最大値：1000 単位：秒
RIS Cleanup Time of the Day	使われていない情報、古い情報、デバイス情報を削除するために、RIS データベースがクリーンアップされる時刻を指定します。この時刻に、すべてのデバイスの [登録試行回数（Number of Registration Attempts）] パフォーマンス カウンタは 0 にリセットされます。 デフォルト設定：22:00 最大長：5 許容される値：HH:mm 書式で時刻を指定（06:11 など） 単位：時:分
RIS Unused Cisco CallManager Device Store Period	Cisco CallManager サービスからの未登録のデバイス情報または拒否されたデバイス情報に関する RIS データベース情報保管期間を指定します。このパラメータで指定した時間が経過した後、Cisco CallManager によって、（RIS Cleanup Time of the Day パラメータで指定する）次の RIS データベース クリーンアップ時間中に期限切れとなったエントリが削除されます。 デフォルト設定：3 最小値：1 最大値：30 単位：日

サービス パラメータ	説明
RIS Unused CTI Records Storage Period	CTI Manager からのクローズされたプロバイダー、デバイス、またはラインの情報に対して、RIS データベース情報保管期間を指定します。このパラメータで指定した時間が経過した後、Cisco CTI Manager によって、（RIS Cleanup Time of the Day パラメータで指定する）次の RIS データベース クリーンアップ時間中に期限切れのエントリが削除されます。 デフォルト設定：1 最小値：0 最大値：5 単位：日
RIS Maximum Number of Unused CTI Records	RIS データベースに格納される、閉じられた CTI プロバイダー、デバイス、および回線の最大記録数を指定します。このパラメータで指定した制限に達すると、Cisco CTI Manager は、使用されていない CTI プロバイダー、デバイス、および回線の新しい記録を RIS データベースに保存しません。 デフォルト設定：3000 最小値：0 最大値：5000 単位：レコード数
TLC Throttling Enabled	Trace and Log スロットルの動作を有効または無効にします。 デフォルト設定：True
TLC Throttling IOWait Goal	TLC スロットルが目標とするシステム IOWait 比率を指定します。 デフォルト設定：10 最小値：10 最大値：40
TLC Throttling CPU Goal	TLC スロットルが目標とするシステム CPU 使用率を指定します。 デフォルト設定：80 最小値：65 最大値：90
TLC Throttling Polling Delay	トレース収集のスロットリング用として、IO 待機と CPU 使用率のポーリング間の最小待機時間（ミリ秒単位）を指定します。 デフォルト設定：250 最小値：200 最大値：2000
TLC Throttling SFTP Maximum Delay	タイムアウトを防止するために SFTP 転送を一時停止する最大時間を指定します。 必須フィールドです。 デフォルト設定：5000 最小値：1000 最大値：10000
Maximum Number of Processes and Threads	マシンで動作しているプロセスとスレッドの最大数を指定します。マシン上のプロセスとスレッドの合計数がこの最大数を超えた場合は、SystemAccess によって TotalProcessesThreadsExceededThresholdStart アラームが送信され、対応する警告が生成されます。 デフォルト設定：2000 最小値：1000 最大値：3000

サービス パラメータ	説明
Enable Logging	トラブルシューティング パフォーマンス監視データの収集とロギングが、有効（True）または無効（False）のいずれであるかを決定します。 デフォルト設定：True
Polling Rate	トラブルシューティング パフォーマンス監視データのポーリングレートを秒単位で指定します。 デフォルト設定：15 最小値：5 最大値：300 単位：秒
Maximum No. of Files	ディスクに保存されるトラブルシューティング パフォーマンス監視ログ ファイルの最大数を指定します。「Maximum No. of Files」に大きな数値を設定する場合は、「Maximum File Size」の値を小さくします。 （注） この値を小さくすると、Troubleshooting Perfmon Data Logging が有効で RISDC がオンになっている場合、タイムスタンプが古いものから順にログ ファイルが削除されます。必要に応じて、Maximum No. of Files を変更する前に、これらのファイルを保存してください。 デフォルト設定：50 最小値：1 最大値：100
ファイルの最大サイズ（MB）（Maximum File Size (MB)）	次のファイルが作成されるまでの、各トラブルシューティング パフォーマンス監視ログ ファイルの最大ファイル サイズを MB 単位で指定します。「Maximum File Size」に大きな数値を設定する場合は、「Maximum No. of Files」の値を小さくする必要があります。 デフォルト設定：5 最小値：1 最大値：500
Cisco Serviceability Reporter	
RTMT Reporter Designated Node	RTMTReporter の実行場所となる特定のサーバを指定します。RTMT Reporter サービスは CPU を集中的に使用するため、非コール処理サーバをこのサーバにすることを推奨します。このフィールドには、Reporter が最初に開始されたローカル サーバ IP が自動的に取り込まれます。
RTMT Report Generation Time	Real-Time Monitoring Tool（RTMT）レポートが生成される時刻を、深夜 0 時（00:00）からの時間（分単位）で指定します。通話処理への影響を減らすため、リアルタイム以外のレポートは業務時間外に実行してください。 デフォルト設定：30 最小値：0 最大値：1200

サービス パラメータ	説明
RTMT Report Deletion Age	レポートが削除されるまでに経過する必要がある日数を指定します。たとえば、このパラメータを7に設定した場合、7日前に生成されたレポートは、8日目に削除されます。値に0を指定すると、レポートの生成が無効になり、既存のレポートはすべて削除されます。 デフォルト設定：7 最小値：0 最大値：30

プラグイン

アプリケーション プラグインは、Unity Connection の機能を拡張します。たとえば、Real-Time Monitoring Tool（RTMT）では、パフォーマンス モニタリング カウンタや Port Monitor などのツールから、リモートでシステムの稼働状態をモニタできます。

Real-Time Monitoring Tool

クライアント側アプリケーションとして実行される Real-Time Monitoring Tool（RTMT）は、HTTPS および TCP を使用して、システム パフォーマンス、デバイスのステータス、デバイス検出、および Unity Connection の CTI アプリケーションをモニタします。RTMT は、HTTPS を使用して直接デバイスに接続し、システムの問題をトラブルシューティングできます。また、RTMT は Unity Connection のボイス メッセージング ポートもモニタできます。

RTMT を使用すると、次の作業を実行できます。

- システムの稼働状態に注目した、事前定義済みの管理オブジェクトのセットをモニタする。
- 値がユーザ設定のしきい値を超えるか下回ったときに、オブジェクトのさまざまなアラートを電子メール形式で生成する。
- トレースを収集し、RTMT に備わっているさまざまなデフォルト ビューアで表示する。
- SysLog ビューアで Syslog メッセージおよびアラーム定義を表示する。
- パフォーマンス モニタリング カウンタと連動する。
- Unity Connection のボイス メッセージング ポートをモニタする。

Unity Connection クラスタが設定されている場合は、複数の RTMT インスタンスを開いて、Unity Connection クラスタの各サーバのボイス メッセージング ポートをモニタできます。

詳細については、該当するリリースの『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。このガイドは http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html. から入手できます。

（注） プラグインをインストールする前に、プラグインのインストール先サーバで実行されている侵入検知やアンチウイルス サービスをすべて無効にする必要があります。

Unity Connection でのプラグインのインストール

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して、[プラグイン（Plugins）] を選択します。

ステップ 2 [プラグインの検索（Search Plugins）] ページで [検索（Find）] を選択し、インストールするプラグインを選択します。

ステップ 3 [ダウンロード（Download）] を選択し、画面に表示される指示に従ってプラグインをインストールします。

ファクス サーバ

Unity Connection にファクスを統合すると、ユーザはメールボックスでファクスを受信し、そのファクスを他のユーザに転送したり、印刷用にファクス機に転送したりできます。ユーザは電話機、Messaging Inbox、または IMAP クライアントを使用してファクスを管理します。詳細については、ファクス サーバの章を参照してください。

LDAP

LDAP を統合すると、サポート対象の企業ディレクトリからユーザをインポートして同期させることができます。これにより、保守する必要のあるディレクトリ情報データベースが 1 つになります。詳細については、LDAPの章を参照してください。

SAML シングル サインオン

Security Assertion Markup Language Single Sign On（SAML SSO）は、既存のサインオン機能の拡張です。SAML SSO により、ユーザは以下の Unified Communications 製品上の Unity Connection サブスクライバ Web インターフェイスおよび管理 Web アプリケーション全体でシングル サインオンアクセスできるようになります。

- Unity Connection
- Cisco Unified Communications Manager
- Cisco Unified IM/Presence

SAML SSO では、LDAP ユーザと非 LDAP ユーザの両方に対して Web アプリケーションへのシングル サインオン アクセス権を付与できます。SAML SSO の詳細については、『Quick Start Guide for SAML SSO in Cisco Unity Connection, Release 12.x』を参照してください。このガイドは https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/quick_start/guide/b_12xcucqssamlsso.html から入手できます。

認証サーバ

Unity Connection は、OAuth 2.0 認証コード付与フローをサポートすることで、Jabber ユーザの SAML SSO および非 SSO ログイン エクスペリエンスを拡張します。ログインにかかる時間を短縮するには、認証コード付与フローで認証サーバがアクセス トークンとリフレッシュ トークンを Jabber クライアントに提供する必要があります。Unity Connection では、電話システムに関連付けられている Cisco Unified CM のパブリッシャ サーバが認証サーバとして設定されます。認証サーバの設定が完了すると、Unity Connection は認証サーバから提供される認証キーを使用して Jabber クライアントのトークンを検証します。Cisco Unified CM で認証キーが変更された場合は、Unity Connection と認証サーバの間でキーを同期する必要があります。電話システムに関連付けられている Cisco Unified CM のクレデンシャルを指定して、複数の認証サーバを設定できます。

認証サーバを設定するには、「Unity Connection での認証サーバの設定」を参照してください。

Unity Connection で認証サーバを設定するときには、次の点を考慮してください。

- OAuth 認証コード付与フロー機能が Cisco Unified CM と Cisco Unity Connection の両方で有効になっていることを確認します。

  デフォルトでは、Cisco Unity Connection では OAuth フローが無効になっています。この機能を有効にするには、Cisco Unity Connection Administration で [システム設定（System Settings）] > [エンタープライズ パラメータ（Enterprise Parameters）] に移動します。[エンタープライズ パラメータ（Enterprise Parameters）] ページの [SSO および OAuth の設定（SSO and OAuth Configuration）] フィールドの下で該当する設定を入力し、[ログイン更新フローを使用した OAuth（OAuth with Refresh Login Flow）] で [有効（Enabled）] オプションを選択します。

- 入力する認証サーバのユーザ名とパスワードは、Cisco Unified CM のシステム管理者のユーザ名およびパスワードと同一でなければなりません。

- Cisco Unified CM の Tomcat サービスが稼働しています。

- Cisco Unified CM の有効な証明書を Cisco Unity Connection の tomcat トラストにアップロードするか、または [証明書エラーを無視する（Ignore Certificate Errors）] チェックボックスをオンにして認証サーバの証明書検証エラーを無視します。

  証明書の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 12.x*』の「Security」の章を参照してください。このドキュメントは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

- Jabber クライアントのバージョンは 11.9 以降でなければなりません。

- Cisco Unified CM のバージョンは 11.5.1 SU3 以降でなければなりません。

Unity Connection での認証サーバの設定

Unity Connection で検証サーバを設定するには、次の手順を実行します。

ステップ 1 Cisco Unity Connection Administration で、[システム設定（System Settings）] を展開して、[認証サーバ（Authz Server）] を選択します。[認証サーバの検索（Search Authz Server）] ページが表示され、現在設定されている認証サーバが示されます。

ステップ 2 認証サーバを設定します（各フィールドの詳細については、[ヘルプ（Help）]>[このページ（This Page）] を参照）。

- 認証サーバを追加するには、次の手順に従います。
  1. [新規追加（Add New）] を選択します。[新規認証サーバ（New Authz Server）] ページが表示されます。
  2. 必要な情報をフィールドに入力します。
  3. [保存（Save）] を選択します。
- 認証サーバを更新するには、次の手順に従います。
  1. 編集する認証サーバを選択します。[認証サーバの編集（Edit Authz Server）] ページが表示されます。
  2. 必要に応じて認証サーバの設定を編集します。
  3. [保存（Save）] を選択します。
- 認証サーバを削除するには、次の手順に従います。
  1. 削除する認証サーバの表示名の横にあるチェックボックスをオンにします。
  2. [選択項目の削除（Delete Selected）] を選択します。
  3. [OK] を選択して削除を確認します。

     複数の認証サーバを削除するには、複数のチェックボックスを一括でオンにします。

Cross-Origin リソース共有（CORS）

CORS 仕様を使用すると、クライアント アプリケーションはより安全な方法で Cross-Origin 要求を処理できます。Web アプリケーションでは通常、単一生成元ポリシーのために、元のドメイン（アプリケーションによる生成元）から別のドメインへの Cross-Origin 要求が Web ブラウザで禁止されます。CORS は、Web ブラウザがサーバとやり取りし、Cross-Origin 要求を許可するかどうかを決定するための手段を提供します。CORS 仕様では、許可されるドメインにサービスを提供するために Web ブラウザと Unity Connection サーバの間で合意を確立するのに HTTP ヘッダーが使用されます。

Unity Connection では、Unity Connection 内で Cross-Domain サーバ用のエントリを作成することにより、Cross-Domain サーバのクライアント アプリケーションが Unity Connection サーバ上のコンテンツに直接アクセスできます。CORS 要求を処理するには Unity Connection に Cross-Domain サーバのエントリが事前に存在していなければなりません。

Unity Connection では、CORS をサポートするよう、シングル サインオン（SAML SSO）エンドポイントが拡張されています。

（注） CORS 機能は、VMRest API を使用することにより Unity Connection の 10.5 以降のリリースでサポートされています。

Unity Connection での CORS の設定

ステップ 1 Cisco Unity Connection Administration で [システム設定（System Settings）] を展開し、[Cross-Origin Resource Sharing（CORS）] を選択します。
[Cross-Origin Resource Sharing（CORS）の検索（ Search Cross-Origin Resource Sharing）] ページが表示され、現在設定されている CORS が示されます。

ステップ 2 Cross-Origin Resource Sharing を設定します（各フィールドの詳細については、[ヘルプ（Help）]>[このページ（This Page）] を参照）。

- CORS を追加するには、次の手順を実行します。

  [Cross-Origin Resource Sharing（CORS）の検索（ Search Cross-Origin Resource Sharing）] ページで、[新規追加（Add New）] を選択します。

  [新規 Cross-Origin Resource Sharing（CORS）（New Cross-Origin Resource Sharing）] ページで、必要なフィールドに値を入力し、[保存（Save）] を選択します。

- 既存の CORS を編集するには、次の手順を実行します。

  [Cross-Origin Resource Sharing（CORS）の検索（ Search Cross-Origin Resource Sharing）] ページで、編集する CORS を選択します。

  [Cross-Origin Resource Sharing（CORS）の編集（Edit Cross-Origin Resource Sharing）] ページで、必要な設定の値を入力し、[保存（Save）] を選択します。

- 1 つ以上の CORS を削除するには、次の手順を実行します。

  [Cross-Origin Resource Sharing（CORS）の検索（ Search Cross-Origin Resource Sharing）] ページで、削除する CORS を選択します。

  [選択項目の削除（Delete Selected）] を選択して、CORS を削除します。

SMTP の設定

SMTP 設定は、ユーザが Unity Connection ボイス メッセージを送受信できるようにするメッセージングのタイプです。SMTP 設定について詳しくは、メッセージの章を参照してください。