管理とサービス アカウントの保護

管理とサービス アカウントの保護

はじめに

この章では、アカウント保護に関連して発生する可能性があるセキュリティ上の問題について説明します。また、とるべき対策に関する情報、意思決定に役立つ推奨事項、下した決定の効果に関する情報、およびベスト プラクティスも紹介します。

Cisco Unity Connection の管理アカウントについて

Cisco Unity Connection サーバには 2 種類の管理アカウントがあります。表 1：Unity Connection サーバの管理アカウント は、これら 2 つのアカウントの用途と相違点の概要を示しています。

表 *1*：*Unity Connection* サーバの管理アカウント

	Operating System Administration アカウント	Application Administration アカウント
アクセス先	• Cisco Unified Operating System Administration • Disaster Recovery System • コマンドライン インターフェイス	• Cisco Unity Connection Administration • Cisco Unified Serviceability • Cisco Unity Connection Serviceability • Real-Time Monitoring Tool

	Operating System Administration アカウント	Application Administration アカウント
最初のアカウントの作成	インストール中に、管理者 ID およびパスワードを指定するときに作成	インストール中に、アプリケーション ユーザ名およびパスワードを指定するときに作成
アカウント名の変更方法	未サポート	Cisco Unity Connection Administration を使用。 **注意** アカウント名の変更に **utils reset_ui_administrator_name** コマンドを使用しないでください。このコマンドを使用すると、Unity Connection が適切に機能しなくなります。
アカウントパスワードの変更方法	**set password** CLI コマンドを使用	• Cisco Unity Connection Administration を使用 • **utils cuc reset password** CLI コマンドの使用 **注意** アカウント名の変更に **utils reset_ui_administrator_password** コマンドを使用しないでください。このコマンドを使用すると、Unity Connection が適切に機能しなくなります。
追加アカウントの作成方法	**set account** CLI コマンドを使用	Cisco Unity Connection Administration を使用 **注意** 追加アカウントの作成に **set account** コマンドを使用しないでください。このコマンドを使用すると、Unity Connection が適切に機能しなくなります。
最初のアカウント以外のアカウントの削除方法	**delete account** CLI コマンドの使用	Cisco Unity Connection Administration を使用 **注意** アカウントの削除に **delete account** コマンドを使用しないでください。このコマンドを使用すると、Unity Connection が適切に機能しなくなります。
管理アカウントのリスト方法	**show account** CLI コマンドの使用。	Cisco Unity Connection Administration を使用
LDAP ユーザ アカウントとの連動	なし	あり

Cisco Unity Connection Administration へのアクセスに使用するアカウントに関するベスト プラクティス

Cisco Unity Connection は、ほとんどの管理タスクに使用する Web アプリケーションです。管理アカウントを使用してConnection Administrationにアクセスし、個々のユーザ（またはユーザ グループ）に対してCisco Unity Connection がどのように機能するかを定義し、システム スケジュールを設定し、コール管理オプションを設定し、その他の重要なデータを変更します。これらの処理はすべて、管理アカウントが割り当てられているロールに依存します。サイトが複数の Unity Connection サーバで構成される場合、あるサーバで Connection Administration へのアクセスに使用されるアカウントが、ネットワーク上の他のサーバでConnection Administrationに対する認証とアクセスにも使用できることがあります。Connection Administration へのアクセスを保護するには、次のベスト プラクティスを検討してください。

ベスト プラクティス：Application Administration アカウントの使用の制限

Unity Connection のユーザ アカウントを Unity Connection の管理専用に作成するまでは、デフォルトの管理者アカウントと関連付けられている資格情報を使用して、Cisco Unity Connection Administrationにサインインします。デフォルトの管理者アカウントは、Unity Connectionのインストール中に、インストール時に指定したアプリケーション ユーザのユーザ名およびパスワードを使用して作成されます。デフォルトの管理者アカウントには、自動的にシステム管理者の役割が割り当てられます。この役割では、Connection Administration への完全なシステム アクセス権限が提供されます。つまり、管理者アカウントは、Connection Administration のすべてのページにアクセスできるだけでなく、Connection Administration のすべてのページに対する読み取り、編集、作成、削除、および実行の各特権を持ちます。このため、高い特権を持つこのアカウントは、1 人またはごく少数の人だけが使用できるように制限する必要があります。

デフォルトの管理者アカウントの代わりとなる管理アカウントを、追加で作成できます。追加するアカウントには、それらを使用する各ユーザが実行する管理タスクに応じて、より少ない特権を持つ役割を割り当てます。

（注） 次のアプリケーション ユーザ名はエラーを生成するため、使用しないでください。

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

ベスト プラクティス：役割を使用した、Cisco Unity Connection Administration への各種レベルのアクセスの提供

Cisco Unity Connection Administration へのアクセスを保護するために役割の割り当てを変更する際には、次のベスト プラクティスを検討してください。

- デフォルトの管理者アカウントへの役割の割り当ては変更しません。その代わりに、Connection Administration への適切なレベルのアクセスを提供する、追加の管理ユーザ アカウントを作成します。たとえば、管理ユーザアカウントをユーザ管理者の役割に割り当てて、管理者がユーザアカウント設定を管理したり、すべてのユーザ管理機能にアクセスしたりできるようにします。または、管理ユーザ アカウントをヘルプ デスク管理者の役割に割り当てて、管理者がユーザ パスワードおよび PIN をリセットしたり、ユーザ アカウントのロックを解除したり、ユーザ設定ページを表示したりできるようにします。
- 追加の管理ユーザテンプレートを作成し、それぞれのテンプレートに、さまざまなレベルのアクセスを提供する役割を割り当てます。デフォルトでは、管理者ユーザ テンプレートには、システム管理者の役割が割り当てられます。管理者ユーザテンプレートから作成される管理ユーザアカウントはシステム管理者の役割に割り当てられ、管理者にはUnity Connectionのすべての管理機能に対するフルアクセス権が与えられます。この管理者テンプレートを慎重に使用して、管理ユーザ用のアカウントを作成します。
- デフォルトでは、ボイスメール ユーザ テンプレートにはどの役割も割り当てられず、このテンプレートに管理役割を割り当てることはできません。その代わりに、このテンプレートを使用して、メールボックスを持つエンド ユーザ用のアカウントを作成します。（メールボックスを持つエンド ユーザに割り当てる唯一の役割は、グリーティング管理者の役割です。この役割では、「管理」機能だけが Cisco Unity Greetings Administrator にアクセスでき、ユーザはコール ハンドラ用の録音済みグリーティングを電話で管理できます）。

ベスト プラクティス：異なるアカウントを使用した、ボイスメールボックスおよび Cisco Unity Connection Administration へのアクセス

Cisco Unity Connection 管理者が Cisco Unity Connection Administration にアクセスするときには、Cisco Personal Communications Assistant（PCA）または電話インターフェイスにサインインするときに使用するものと同じアカウントを使用しないことが推奨されます。

ユニファイド メッセージング サービス アカウントの保護

Cisco Unity Connection 12.x にユニファイド メッセージングを設定する場合は、Unity Connection が Exchange との通信に使用する 1 つ以上の Active Directory アカウントを作成します。Exchange メールボックスにアクセスする権限を持つ Active Directory アカウントと同様に、このアカウントのアカウント名とパスワードを知っているユーザは、メールを読んだり、音声メッセージを聞いたり、メッセージを送信および削除したりできます。このアカウントは、Exchange における広範囲の権限を持っていないため、たとえば、Exchangeサーバの再起動などに使用できない場合があります。

アカウント保護のために、大文字、小文字、数字、および特殊文字からなる20文字以上の長いパスワードをアカウントに与えることを推奨します。パスワードは AES 128 ビットの暗号化方式によって暗号化され、Unity Connectionデータベースに保存されます。データベースはルート アクセ

スによってしかアクセスできず、ルート アクセスは Cisco TAC からのサポートによってしか使用できません。

アカウントを無効にしないでください。無効にすると、Unity Connection がアカウントを使用して Exchange メールボックスにアクセスできなくなります。

ファイルの整合性の確認

Unity Connection では、さまざまなインターフェイス（Cisco Unity Connection の Cisco Unity Connection Administration や Cisco Unity Connection Serviceability など）からダウンロードできるファイルの整合性を管理者が確認できるようにし、セキュリティ強化を図っています。ファイルの整合性を検証するため、Unity Connection はすべてのダウンロード ファイルに対して SHA-512 チェックサム値を提供します。たとえば、Cisco Unified Real-Time Monitoring Tool プラグインの SHA-512 チェックサム値は [プラグインの検索（Search Plugin）] ページの [説明（Description）] フィールドに表示されます。

管理者は、ファイルの整合性を確認するためにファイルをダウンロードし、オンラインで利用できる外部ツールを使用してファイルのチェックサムを生成できます。次に、表示されているチェックサムと、ダウンロードしたファイルのチェックサムを比較します。両方のファイルのチェックサムが同一である場合は、ダウンロードしたファイルにはエラーがありません。