パスワード、PIN、および認証規則の管理

Cisco Unity Connection では、認証規則によって、すべてのユーザアカウントのユーザ パスワード、PIN、およびアカウント ロックアウトが管理されます。Unity Connection の認証規則を次のように定義することを推奨します。

- ユーザが PIN とパスワードを頻繁に変更することを必須にする。
- ユーザの PIN およびパスワードには、一意で、簡単に推測できないものを設定することを必須にする。

綿密に考えられた認証規則により、無効な PIN またはパスワードを何回も入力したユーザをロックすることで、Cisco Personal Communications Assistant（Cisco PCA）や Cisco Unity Connection Survivable Remote Site Voicemail などの Unity Connection アプリケーションへの不正アクセスを阻止できます。

この章では、上に挙げたタスクの実行や、PIN およびパスワードのセキュリティに関連するその他の問題に関する情報を提供します。Cisco Unity Connection パスワードの管理の範囲を理解するのに役立つように、この章の最初の項では、Cisco Personal Communications Assistant（PCA）、Unity Connection カンバセーション、Cisco Unity Connection Administration、およびその他の管理 Web アプリケーションへのアクセスに必要な、さまざまなパスワードについて説明します。その後の各項では、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を紹介します。

Unity Connection パスワードを保護する手順および認証規則を定義する手順については、次の各項を参照してください。

- パスワード、PIN、および認証規則の管理 （1 ページ）

パスワード、PIN、および認証規則の管理

Cisco Unity Connection では、認証規則によって、すべてのユーザアカウントのユーザ パスワード、PIN、およびアカウント ロックアウトが管理されます。Unity Connection の認証規則を次のように定義することを推奨します。

- ユーザが PIN とパスワードを頻繁に変更することを必須にする。

- ユーザのPINおよびパスワードには、一意で、簡単に推測できないものを設定することを必須にする。

綿密に考えられた認証規則により、無効な PIN またはパスワードを何回も入力したユーザをロックすることで、Cisco Personal Communications Assistant（Cisco PCA）や Cisco Unity Connection Survivable Remote Site Voicemail などの Unity Connection アプリケーションへの不正アクセスを阻止できます。

この章では、上に挙げたタスクの実行や、PINおよびパスワードのセキュリティに関連するその他の問題に関する情報を提供します。Cisco Unity Connection パスワードの管理の範囲を理解するのに役立つように、この章の最初の項では、Cisco Personal Communications Assistant（PCA）、Unity Connection カンバセーション、Cisco Unity Connection Administration、およびその他の管理 Web アプリケーションへのアクセスに必要な、さまざまなパスワードについて説明します。その後の各項では、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を紹介します。

Unity Connection パスワードを保護する手順および認証規則を定義する手順については、次の各項を参照してください。

ユーザが Unity Connection アプリケーションへのアクセスに使用する PIN およびパスワードについて

Cisco Unity Connection ユーザは、さまざまな Unity Connection アプリケーションへのアクセスに異なる PIN やパスワードを使用します。Unity Connection パスワードの管理の範囲を理解するうえで、各アプリケーションにどのパスワードが必要なのかを知ることが重要です。

電話機の PIN

ユーザは、電話機の PIN を使用して、 Cisco Unity Connection カンバセーションに電話機からサインインします。PIN（数値だけで構成）は、電話機のキーパッドを使用して入力するか、音声認識が有効な場合は読み上げます。

Web アプリケーション（Cisco PCA）のパスワード

管理の役割を割り当てられているユーザは、Webアプリケーションのパスワードを使用して次の Unity Connection アプリケーションにサインインすることもあります。

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- [Cisco Unified Serviceability]
- Real-Time Monitoring Tool
- Cisco Unity Connection SRSVの管理

(注) Cisco Unified Communications Manager Business Edition（CMBE）または LDAP の認証を使用している場合、ユーザは、ユーザの Cisco Unified CMBE または LDAP アカウント パスワードを使用して Unity Connection Web アプリケーションにアクセスする必要があります。ユーザに対して、Cisco Unity Connection で、一意で安全な PIN およびパスワードを最初に割り当てるようにします。

不正アクセスや不正通話から Cisco 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（Cisco PCA）パスワードを割り当てる必要があります。

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用したテンプレートによって、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 つのテンプレートから作成されたすべてのユーザに、同じ PIN およびパスワードが割り当てられます。

次のオプションを検討して、アカウントの作成時、またはその直後に、各ユーザに一意で安全な PIN およびパスワードが確実に割り当てられるようにしてください。

- 少数のユーザアカウントを作成する場合、または Cisco Unity Connection Administration を使用してアカウントを作成した後は、[Users（ユーザ）] > [Users（ユーザ）] > [Change Password（パスワードの変更）] ページで各ユーザの電話機 PIN と Web パスワードを変更します。または、ユーザに対し、できるだけ速やかにサインインして自分の PIN とパスワードを変更するように指示します（この場合は、アカウントの作成に使用したテンプレートの [パスワードの編集（Edit Password）] ページにある [次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）] チェックボックスをオンにしてください）。
- 複数のユーザアカウントを作成する場合は、アカウント作成後、Bulk Password Edit ツールを使用して Unity Connection の各エンドユーザアカウント（メールボックスを持つユーザ）に一意のパスワードと PIN を割り当てます。Bulk Password Edit ツールは、CSV ファイルとともに使用します。CSV ファイルには、複数のパスワードおよび PIN を一括して適用するための、パスワードおよび PIN 用の一意の文字列が含まれています。

Bulk Password Edit ツールは、Windows ベースのツールです。
http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html からツールをダウンロードし、トレーニング ビデオとヘルプを参照してください。

Unity Connection SRSV のパスワードと共有秘密

中央 Unity Connection サーバから Unity Connection SRSV サーバに対するすべての要求は通信に Unity Connection SRSV 管理者ログイン情報を使用しますが、Unity Connection SRSV から Unity Connection への要求は、認証に秘密トークンを使用します。

中央 Unity Connection サーバは、Unity Connection SRSV の管理者ユーザ名とパスワードを使用してサーバへのアクセスを認証します。Unity Connection SRSV のユーザ名とパスワードは、中央 Unity Connection サーバに新しいブランチを作成するときに、Connection データベースに格納されます。

Unity Connection SRSV を使用するプロビジョニング サイクルごとに、中央 Unity Connection サーバは秘密トークンを生成し、Unity Connection SRSV と共有します。Unity Connection SRSV サイトからプロビジョニングが完了した後、中央 Unity Connection サーバに同じトークンを使用して通知します。その後、プロビジョニング サイクルの完了後すぐ、このトークンは中央 Unity Connection と Unity Connection SRSV サーバの両方から削除されます。ランタイム トークン キーの概念は、共有秘密として知られています。

Unity Connection SRSV の詳細については、以下のリンクから『Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) Release 14』を参照してください。https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/srsv/guide/b_14cucsrsvx.html

Web アプリケーション パスワードの変更

Web アプリケーション（Cisco PCA）の個人ユーザのパスワードは、Cisco Unity Connection Administration の [ユーザ（Users）]>[ユーザ（Users）]>[パスワードの変更（Change Password）] ページでいつでも変更できます。

パスワードの有効期限が切れると、ユーザおよび管理者は、Cisco PCA や Connection Administration に次にサインインするときに新しいパスワードを入力する必要があります。

また、ユーザは Unity Connection Messaging Assistant で各自の Cisco PCA パスワードを変更することもできます。

複数のエンド ユーザ アカウント（メールボックスを持つユーザ）のパスワードを変更する場合は、Bulk Password Edit ツールを使用して、一意の新しいパスワードを各アカウントに割り当てることができます。Bulk Password Edit ツールは、CSV ファイルとともに使用します。CSV ファイルには、複数のパスワードを一括して適用するための、パスワード用の一意の文字列が含まれています。Bulk Password Edit ツールは、Windows ベースのツールです。X http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html からツールをダウンロードし、トレーニング ビデオとヘルプを参照してください。また、Cisco Unity Connection 一括管理ツール（BAT）を使用して、複数のユーザ パスワードを一括で変更できます。

IMAP クライアントのボイス メッセージにアクセスできるユーザの場合は、Cisco PCA パスワードを Messaging Assistant で変更するたびに、IMAP クライアント内のパスワードも更新する必要があることを認識する必要があります。パスワードは、IMAP クライアントと Cisco PCA の間で同期されません。

ベスト プラクティス：

8 文字以上の長さの、単純でないパスワードを指定します。同じ方法に従ってパスワードを変更するようにユーザに奨励するか、それを必須とする認証規則をユーザに割り当てます。Cisco PCA パスワードは、6 か月ごとに変更する必要があります。

電話機 PIN の変更

個々のユーザの電話機 PIN は、Cisco Unity Connection Administration の [ユーザ（Users）] > [ユーザ（Users）] > [パスワードの変更（Change Password）] ページでいつでも変更できます。

ユーザは、Unity Connection の電話カンバセーションや Unity Connection Messaging Assistant を使用して、電話機 PIN を変更できます。

複数のエンド ユーザ アカウント（メールボックスを持つユーザ）の PIN を変更する場合は、Bulk Password Edit ツールを使用して、一意の新しい PIN を各アカウントに割り当てることができます。Bulk Password Edit ツールは、CSV ファイルとともに使用します。CSV ファイルには、複数の PIN を一括して適用するための、PIN 用の一意の文字列が含まれています。Bulk Password Edit ツールは、Windows ベースのツールです。http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html からツールをダウンロードし、トレーニング ビデオとヘルプを参照してください。また、Cisco Unity Connection 一括管理ツール（BAT）を使用して、複数のユーザ PIN を一括で変更できます。

PIN が期限切れになると、ユーザは、Unity Connection カンバセーションに次にサインインするときに新しい PIN を入力する必要があります。

ユーザは Messaging Assistant を使用して電話機 PIN を変更できるため、適切な手段を講じて Web アプリケーション（Cisco PCA）のパスワードの安全も維持することによって、PIN のセキュリティを確保できます。

ユーザは、電話機 PIN と Cisco PCA パスワードが同期されないことを理解する必要があります。初回登録時に、電話機の初期 PIN を変更するように求められますが、そのときには Cisco PCA の Web サイトへのサインインに使用するパスワードを変更することはできません。

ベスト プラクティス：

各ユーザに、6 桁以上で単純でない、一意の PIN が割り当てられる必要があります。同じ方法に従うようにユーザに奨励するか、それを必須とする認証規則をユーザに割り当てます。

パスワード、PIN、およびロックアウト ポリシーを指定する認証規則の定義

（注） Cisco Unity Connection 認証規則は、Cisco Unified Communications Manager Business Edition（CMBE）でのユーザ パスワードの管理や、LDAP 認証が有効な場合には適用されません。これは、このような状況では認証が Unity Connection で処理されないためです。

認証規則を使用して、ユーザが電話で Unity Connection にアクセスするときに Cisco Unity Connection によって適用されるサインイン、パスワード、およびロックアウトのポリシーをカスタマイズします。また、ユーザが Cisco Unity Connection Administration、Cisco PCA、およびその他のアプリケーション（IMAP クライアントなど）にアクセスする方法もカスタマイズします。

Connection Administration の [認証規則の編集（Edit Authentication Rule）] ページで指定する設定によって、次の値が決まります。

- アカウントがロックされるまでに許容される、Unity Connection 電話インターフェイス、Cisco PCA、または Connection Administration へのサインイン試行回数。
- 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。

ベスト プラクティス：

セキュリティを強化するため、認証規則を定義する際には、次のベストプラクティスに従うよう推奨します。

- ユーザが少なくとも 6 か月に 1 回 Unity Connection のパスワードと PIN を変更することを必須とする。
- Web アプリケーションのパスワードは 8 文字以上の単純でないパスワードにすることを必須とする。
- ボイスメール PIN は 6 文字以上の単純でない PIN にすることを必須とする。

セキュリティをさらに強化するには、PIN やパスワードを簡単に推測できないものにし、また、長期間使用しないようにする認証規則を設定します。それと同時に、複雑すぎる PIN やパスワードを設定するようにしたり、PIN やパスワードをあまりに頻繁に変更するようにしたりすると、ユーザが PIN やパスワードを書き留めなくてはならなくなるので、そのような規則は避けます。

また、次の各フィールドで認証規則を指定する際には、次のガイドラインに従ってください。

サインイン試行回数（Failed Sign-In __ Attempts）：

このフィールドでは、ユーザが間違った PIN またはパスワードを繰り返し入力した場合に、Unity Connection がどのように処理するかを指定します。サインインの試みが 3 回失敗した場合にユーザ アカウントをロックするように設定することを推奨します。

サインイン試行回数をリセットする間隔（Reset Failed Sign-In Attempts Every __ Minutes）：

このフィールドでは、サインインの試みが失敗した回数を Unity Connection がクリアするまでの分数を指定します（サインイン失敗回数の制限をすでに超えて、アカウントがロックされている場合を除く）。30 分超過してから、サインインの試みが失敗した回数をクリアするように設定することを推奨します。

ロックアウト期間（Lockout Duration）：

このフィールドでは、ロックアウトされたユーザが再度サインインを試みるまで待機する時間を指定します。

セキュリティをさらに強固にするには、[管理者によるロック解除が必要（Administrator Must Unlock）] チェックボックスをオンにします。そうすることで、ユーザは、管理者が該当する [ユーザ（User）] > [パスワードの設定（Password Settings）] ページでそのユーザのロックを解除するまで、アカウントにアクセスできなくなります。[管理者によるロック解除が必要（Administrator Must Unlock）] チェックボックスは、管理者がすぐに対応できる場合、またはシステムが不正アクセス/不正通話されやすい場合にだけ、オンにしてください。

ログイン情報の期限切れ(日)（Credential Expires After __ Days）：

[無期限（Never Expires）] オプションは有効にしないことを推奨します。その代わりに、このフィールドを 0 より大きい値に設定し、ユーザが X 日（X は、[クレデンシャルの有効期限（Credential Expires After）] フィールドで指定した値）ごとにパスワードの変更を求められるようにします。

Web パスワードは 120 日後に、電話機 PIN は 180 日後に期限切れになるように設定することを推奨します。

最小クレデンシャル長（Minimum Credential Length）：

このフィールドは 6 以上の値に設定することを推奨します。

Web アプリケーションのパスワードに適用される認証規則については、ユーザが 8 文字以上のパスワードを使用することを必須にするよう、推奨します。

電話機 PIN に適用される認証規則については、ユーザが 6 桁以上の PIN を使用することを必須にするよう、推奨します。

最小クレデンシャル長を変更すると、ユーザは、ユーザの PIN およびパスワードを次回変更するときに、最小クレデンシャル長の新しい値を使用する必要があります。

既存のログイン情報から必要な最小変更文字数（Minimum Number of Character Changes between Successive Credentials）：

このフィールドを使用して、ユーザが Web アプリケーション パスワードの更新時に変更する必要がある文字の数を指定します（PIN には適用されません）。

このフィールドの値は、[最小クレデンシャル長（Minimum Credential Length）] フィールドの値以下に設定してください。

デフォルトでは、このフィールドの値は 1 に設定されており、ユーザは古いパスワードと新しいパスワードの間で少なくとも 1 文字を変更する必要があります。

以前のクレデンシャルの保存数（Stored Number of Previous Credentials）：

このフィールドに値を指定することを推奨します。そうすることによって、Unity Connection が各ユーザの以前のパスワードまたは PIN を、指定した数だけ保存して、パスワードの一意性を強制できるようになります。ユーザがパスワードと PIN を変更すると、Unity Connection で、新しいパスワードまたは PIN が、ログイン情報履歴に保存されているパスワードまたは PIN と

比較されます。Unity Connection では、履歴に保存されているパスワードまたは PIN と一致するパスワードまたは PIN が拒否されます。

デフォルトでは、Unity Connection のクレデンシャル履歴に 5 つのパスワードまたは PIN が保存されます。

安易なパスワードかどうかのチェック（Check For Trivial Passwords）：

ユーザが単純すぎないPINおよびパスワードを使用するように、このフィールドを有効にすることを推奨します。

単純すぎない電話機 PIN には、次の特性があります。

- PIN が、ユーザの姓または名を数値で表したものと一致しない。
- PIN に、ユーザのプライマリ内線番号や代行内線番号が含まれていない。
- PIN に、ユーザのプライマリ内線番号や代行内線番号を逆順で示す数値が含まれていない。
- PIN に、数値の組み合わせが繰り返されたもの（408408、123123 など）が含まれていない。
- PIN に含まれているのが 2 つの数値のみ（121212 など）ではない。
- 数字は 3 回以上続けて使用できない（たとえば 28883）。
- PIN は、昇順または降順の連続する数値（012345、987654 など）ではない。
- PINに、許可されている最小クレデンシャル長と一致する数値グループの場合、キーパッド上で 1 列に並んだ数値グループが含まれていない（たとえば、3 桁の長さが許可されている場合、123、456、または 789 を PIN として使用することはできない）。

単純すぎない Web アプリケーション パスワードには、次の特性があります。

- パスワードに、大文字、小文字、数値、および記号のうち、少なくとも3つの文字が含まれている。
- パスワードに、ユーザのエイリアス、または逆順にしたユーザのエイリアスが含まれていない。
- パスワードに、プライマリ内線番号や代行内線番号が含まれていない。
- 文字は 4 回以上続けて使用できない（たとえば !cooool）。
- 昇順または降順の、すべて連続する文字（abcdef、fedcba など）が使用されていない。

Unity Connection SRSV ユーザ PIN の変更

Unity Connection SRSV ユーザ PIN を変更する場合、Cisco Unity Connection Administration インターフェイスを介して実行できます。選択したユーザの PIN を変更した後、Unity Connection SRSV データベースのユーザ情報を更新するよう、関連するブランチをプロビジョニングする必要があります。

（注） Cisco Unity Connection SRSV Administration インターフェイスを介して SRSV ユーザの PIN を変更することはできません。

同時セッションの最大数の制限

Unity Connection では、ユーザが次に示すインターフェイスで実行できる同時セッションの数を管理者が制限できるようにすることで、セキュリティ強化を図っています。

- **テレフォニー インターフェイス**：テレフォニー インターフェイスでは、設定されている最大制限数を超えてユーザが新しいセッションを試行すると、コールが切断されます。
- **ビジュアルボイスメールインターフェイス**（*PIN*ベースの認証）：ビジュアルボイスメールインターフェイスでは、設定されている最大制限数を超えてユーザが新しいセッションを試行すると、ユーザはインターフェイスにログインできなくなります。

  テレフォニー セッションまたはビジュアルボイスメール セッションには、プライマリ内線番号と代行内線番号の両方からのコールが含まれます。両方のインターフェイスでこの機能を有効にするには、Cisco Unity Connection Administration にログインし、**[システム設定（System Settings）] > [詳細設定（Advanced）] > [カンバセーション（Conversation）]** に移動し、**[テレフォニー インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for Telephony Interface (Per User)）]** フィールドにセッションの最大数の値を入力します。

- **IMAP インターフェイス**：IMAP インターフェイスでは、設定されている最大制限数を超えてユーザが IMAP アカウントにログインしようとすると、ログインが失敗します。IMAP インターフェイスでこの機能を有効にするには、Cisco Unity Connection Administration にログインし、**[システム設定（System Settings）] > [詳細設定（Advanced）] > [メッセージング（Messaging）]** に移動し、**[IMAP インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for IMAP Interface (Per User)）]** フィールドにセッションの最大数の値を入力します。

デフォルトでは、**[テレフォニー インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for Telephony Interface (Per User)）]** と **[IMAP インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for IMAP Interface (Per User)）]** フィールドの値がゼロに設定されています。この場合、この機能は無効です。

（注） このフィールドの推奨最小値は、Outlook 2010 では 4、Outlook 2013 では 2 です。

非アクティブ タイムアウトの設定

Unity Connection のセキュリティ強化のための新機能では、管理者がユーザの非アクティブ タイムアウトの日数を設定できます。ユーザが Unity Connection インターフェイス（TUI や Web

Inbox など）からボイスメール アカウントにログインしていない期間が、設定された日数に達すると、アカウントが無効になり、今後のアクセスが拒否されます。

この機能を有効にするには、Cisco Unity Connection Administration にログインし、**[システム設定（System Settings）]** > **[詳細設定（Advanced）]** > **[Connection 管理（Connection Administration）]** に移動し、**[ユーザの非アクティブ タイムアウト（日数）（User Inactivity Timeout (in Days)）]** フィールドに非アクティブ タイムアウトの値を入力します。

（注） デフォルトでは **[ユーザの非アクティブ タイムアウト（日数）（User Inactivity Timeout (in Days)）]** フィールドの値はゼロに設定されており、この機能は無効になっています。

この機能が有効な場合は、以下の設定が Unity Connection に適用されます。

- 非アクティブなユーザを検索するため、Cisco Unity Connection Administration の **[ユーザ（Users）]** > **[ユーザの検索（Search Users）]** ページで検索条件を **[非アクティブ ユーザ（Inactive Users）]** に絞り込むことができます。
- Cisco Unity Connection Administration の **[ユーザ（Users）]** > **[ユーザの基本設定の編集（Edit User Basics）]** で、ユーザの **[ボイスメール アプリケーションへのアクセス（VoiceMail Application Access）]** を **[アクティブ（Active）]** または **[非アクティブ（Inactive）]** に更新できます。
- 設定された間隔で **[非アクティブ ユーザの確認（Check Inactive Users）]** sysagent タスクを実行し、ユーザがログインしていない期間が設定されている日数を超えている場合にそのユーザを非アクティブにするように設定できます。