# Cisco Unity Connection の強化されたセキュリティ モード



# Cisco Unity Connection の強化されたセキュリティ モード

## 概要

Unity Connection が EnhancedSecurityMode で動作できる場合、システム導入を保護する一連の厳密なセキュリティおよびリスク管理コントロールが実装されます。

EnhancedSecurityMode には次の機能があります。

- **厳密なパスワード要件**：新規ユーザパスワードと既存のパスワードの変更時に適用される厳密なクレデンシャルポリシーが導入されました。「クレデンシャルポリシー（Credential Policy） （2 ページ）」を参照してください。
- **リモート監査ログ**：すべての監査ログとイベント syslog はローカルに保存され、またリモート syslog サーバにも保存されます。

  「リモート監査ログ （2 ページ）」を参照してください。
- **システム ロギング**：CLI ログインや間違ったパスワードの使用などのすべてのシステムイベントが記録、保存されます。
- **ログオンの制限**：インターフェイスの同時セッションの最大数を設定できます。設定されている制限を超えると、新しいセッションはすべて切断されます。EnhancedSecurityMode 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)）]** のデフォルト値は 2、**[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)）]** のデフォルト値は 5 です。詳細については、「パスワード、PIN、および認証規則の管理」の章を参照してください。

- **非アクティブ ユーザの無効化**：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、設定されている日数に達すると、アカウントは無効になり、今後のアクセスは拒否されます。

  EnhancedSecurityMode 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)）]** のデフォルト値は 90 です。詳細については、「パスワード、PIN、および認証規則の管理」を参照してください。

# ロール ベースのアクセス

EnhancedSecurityMode では、「スーパー カスタム管理者（Super Custom Administrator）」という新しい権限が [カスタム役割（Custom Roles）] ページの権限リストに追加されます。システム管理者は「スーパー カスタム管理者（Super Custom Administrator）」権限を使用して、システム内で 2 レベルの管理者階層を作成できます。

# クレデンシャル ポリシー（Credential Policy）

EnhancedSecurityMode が有効になると、プラットフォーム管理者に対し新規パスワードとパスワード変更に関する厳密なクレデンシャル ポリシーを適用できます。このポリシーにより適用されるデフォルトのパスワード要件を次に示します。

- クレデンシャルの長さは 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。
- 以前のクレデンシャルの保存数は 24 であり、過去に使用されたこれらの 24 個のパスワードはいずれも再利用できません。
- クレデンシャルの最小有効期間は 1 日、最大有効期間は 60 日です。
- 連続するクレデンシャル間での最小変更文字数は 4 文字です。

EnhancedSecurityMode を有効にした後で、管理者は認証規則を使用してパスワード要件を変更し、すべてのパスワード変更に関する厳密なパスワード ポリシーを適用できます。クレデンシャル ポリシーについては、「パスワード、PIN、および認証規則の管理」の章を参照してください。

# リモート監査ログ

セキュリティ要件に準拠するため、Unity Connection でリモート監査ログを設定する必要があります。

EnhancedSecurityMode では、システムはデフォルト プロトコルとして TCP を使用して、リモート syslog サーバに監査イベントとアラームを送信します。通常の動作モードでシステムで使用される UDP とは異なり、TCP にはすべてのパケットの配信を保証するメカニズムがあります。ただし、必要に応じてこのモードで UDP を使用するようにシステムを再設定することもできます。

転送エラーが発生すると、TCPRemoteSyslogDeliveryFailed アラームとアラートがトリガーされ、管理者に対しTCP転送エラーについて通知されます。スロットリングメカニズムにより、1時間あたりに送信されるアラームとアラートはそれぞれ1つずつに限定されます。このため、管理者に対して同じアラームとアラートが大量に送信されることがありません。管理者は通信の再確立時にローカル監査ログをバックアップとして使用できます。

# 強化されたセキュリティ モードの前提条件

- FIPS 140-2 モードの設定：拡張されたセキュリティ モードを有効にする前に、FIPS モードを有効にする必要があります。FIPS モードがまだ有効ではない場合は、EnhancedSecurityMode を有効にする時点で、FIPS モードを有効にするように促されます。
- リモート syslog サーバをセットアップし、Unity Connection とリモート サーバ（この間のゲートウェイを含む）の間で IPSec を設定します。
- スマート ホストをセットアップし、Unity Connection と Exchange（Exchange がスマート ホストとして稼働、この間のゲートウェイを含む）の間で IPSec を設定します。ISec の設定の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14*』の「Security」の章の「IPSEC Management」の項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/14/os_administration/guide/b_14cucosagx.html からご利用いただけます。
- Unity Connection サーバで拡張されたセキュリティ モードを有効にする前に、セキュリティ パスワードの長さが 14 文字以上であることを確認してください。Unity Connection をアップグレードする場合は、以前のバージョンで EnhancedSecurityMode が有効だった場合、パスワードを更新する必要があります。

# 強化されたセキュリティ モードでの設定タスクのフロー

**ステップ 1** Unity Connection で EnhancedSecurityMode を有効にします。「強化されたセキュリティ モードの設定 （4 ページ）」を参照してください。

**ステップ 2** システム クレデンシャル ポリシーがセキュリティ ガイドラインを満たしていることを確認します。「クレデンシャル ポリシーの設定 （4 ページ）」を参照してください。

**ステップ 3** モードの監査フレームワークを設定します。

Unity Connection の監査ロギング フレームワークをセットアップします。これには、すべての監査ログとアラームに対するリモート syslog サーバのセットアップも含まれます。「監査フレームワークの設定 （4 ページ）」を参照してください。

## 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**を有効または無効にするには、次の手順を使用します。ただし、**強化されたセキュリティ モード**を有効にする前に FIPS モードを有効にしておく必要があります。

**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 EnhancedSecurityModestatus** コマンドを実行して、モードステータスが有効と無効のいずれに設定されているかを確認します。

**ステップ 3** モードが無効な場合は、次のコマンドを実行して **EnhancedSecurityMode** を有効にします。

```
utils EnhancedSecurityMode enable
```

同様に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** Cisco Unity Connection のすべてのノードでこの手順を繰り返します。

## クレデンシャル ポリシーの設定

システム クレデンシャル ポリシーを更新するには、次の手順を実行します。

**ステップ 1** [Cisco Unity Connection の管理（Cisco Unity Connection Administration）] にログインします。

**ステップ 2** **[認証規則（Authentication Rules）]** > **[認証規則の編集（Edit Authentication Rule）]** を選択します。

**ステップ 3** 要件に基づいて認証規則を更新します。

**ステップ 4** **[保存（Save）]** をクリックします。

クレデンシャル ポリシーについては、「パスワード、PIN、および認証規則の管理」の章を参照してください。

## 監査フレームワークの設定

Unity Connection で **EnhancedSecurityMode** の監査要件を設定するには、次のタスクを実行します。

**ステップ 1** リモート監査ログを設定します。

リモート監査ログの監査ログ設定を行います。

**ステップ 2** リモート監査ログの転送プロトコルを設定します。

（オプション）デフォルトで **EnhancedSecurityMode** が有効な場合、システムはリモート監査ログの転送プロトコルとして TCP を使用します。この手順では、UDP を使用するようにシステムを再設定できます。

**ステップ 3** 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** TCPRemoteSyslogDeliveryFailed アラートの電子メール通知を設定します。

## リモート監査ログの設定

EnhancedSecurityMode で稼働している Unity Connection システムのリモート監査ログを設定する前に、次の点を確認してください。

- 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、IPSec を設定している必要があります。

  ISec の設定の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14*』の「Security」の章の「IPSEC Management」の項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/14/os_administration/guide/b_14cucosagx.html からご利用いただけます。

**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、パブリッシャ ノード以外の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** [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 6** [保存（Save）] をクリックします。

## リモート監査ログの転送プロトコルの設定

リモート監査ログの転送プロトコルを設定するには、次の手順を使用します。
**EnhancedSecurityMode** でのデフォルト設定は TCP です。

**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、設定されているプロトコルを確認します。

**ステップ 3** 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** ノードを再起動します。

**ステップ 5** すべての Unity Connection クラスタ ノードに対してこの手順を繰り返します。

### 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。

**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）]** を選択します。

**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。

### 電子メール アラートの有効化

TCPRemoteSyslogDeliveryFailed アラームの電子メールアラートをセットアップするには、次の手順を使用します。

**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）]** > **[設定アラートアクション（Config Alert Action）]** を選択します。

**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。