Cisco Unified CallManager 4.x での LDAP ディレクトリ統合の保護

目次

概要

このドキュメントでは、次の項目について説明します。

- 権限を制限するためにいくつかの設定を行うことで、Cisco Unified CallManager (CUCM) との LDAP ディレクトリ統合のセキュリティが向上します。 これら

の手順により、ディレクトリ統合の既存および新規インストールの両方が向上します。
- ディレクトリへのアクセスとディレクトリの管理には、特殊なユーザとグループが必要です。 専用ユーザとグループを制限するためオブジェクトに権限が設定され、ディレクトリ統合が更新（既存のインストール）または完了（新規インストール）します。 最後に統合が確認されます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、Cisco Unified CallManager 4.x に関連しています。

次の手順では Microsoft Active Directory（AD）が使用されていますが、この手順はサポートされているその他のディレクトリ製品にも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

既存のディレクトリを統合する場合

既存のディレクトリを統合するには、次の手順を実行します。

1. 新しいグループ（例：*CUCM Directory Group*）を作成します。
2. ディレクトリ アクセスのグループ権限を設定します。
3. 既存のディレクトリ ユーザを新しいグループに移動します。
4. 古いグループからユーザを削除します。 メンバーは新しいグループだけに属するメンバーにできます。。
5. 確認を行います。

専用アカウントを使用していない既存のインストールの場合

専用アカウントを使用していない既存のディレクトリ統合では、次の手順を実行します。

1. 新しいユーザ（例：*CUCM Directory Manager*）を作成します。
2. このユーザを新しいグループだけに属するメンバーにします。
3. この新しいユーザを使用するように CUCM を変更します。 レジストリと ini ファイルを変更します。
4. Cisco Tomcat を再起動します。
5. 使用していた元のアカウントのパスワードを変更します。
6. 確認を行います。

新規インストールの場合

ディレクトリ統合の新規インストールの場合は、次の手順を実行します。

1. 新しいグループ（例：*CUCM Directory Group*）を作成します。
2. この新しいグループに対して制限を設定します。
3. 新しいユーザ（例：*CUCM Directory Manager*）を作成します。
4. Administrator 権限が設定されているグループ（例：*Domain Admins*）にこの新しいユーザを追加します。
5. プラグインのインストール時にこの新しいユーザを使用します。
6. 新しく作成した *CUCM Directory Group* にこのユーザを移動します。
7. この新しいグループを管理者ユーザのプライマリ グループとして設定します。
8. 古いグループからこのユーザを削除します。これで、このユーザは他のどのグループのメンバーでもありません。
9. 確認を行います。

確認

次の手順に従って確認を行います。

1. ディレクトリ サーバのディレクトリに新しいユーザ *ccmtest* を作成します。
2. ccmtest ユーザが [CUCM Users] にリストされていることを確認します。
3. [CUCM User Configuration] ページで ccmtest の PIN を変更します。
4. ディレクトリでフィールドが更新されていることを確認します。
5. ディレクトリで ccmtest の [ciscoCCNatCTIUseEnabled] を [True] に変更します。
6. CUCM で ccmtest の [Enable CTI Application Use] チェックボックスがオンであることを確認します。
7. **ccmtest** ユーザを削除します。
8. LDAP ブラウザに、ツリーの必要な部分だけが表示されていることを確認します。 [Cisco Organizational Unit (OU)] または [Users OU] の外部はすべて表示されていないはずです。

手順の詳細

注: この手順での専用アカウントの名前は *CUCM Directory Manager*、専用グループの名前は *CUCM Directory Group* ですが、異なる名前を使用できます。

Microsoft Active Directory（ADUC）の開始

[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] を選択します。

新しいグループの作成

新しいグループを作成するには、次の手順を実行します。

1. [Users] コンテナを右クリックします。
2. [New] > [Group] を選択します。

3. グループ名、スコープ、およびタイプを入力します（例：*CUCM Directory Group*、*Global*、および *Security*）。
4. [Next] をクリックします。
5. **[Finish] をクリックします。**

ディレクトリ アクセスのためのグループ アクセス許可の設定

グループには次の権限が付与されている必要があります。

```
Read/Write/Create all child objects/
   Delete all child objects on the Cisco OU
```

次の権限がこのオブジェクトとそのすべての子オブジェクトに適用されている必要があります。

```
Read privileges on the Users OU,
   Read/Write privileges on the ciscoatGUID,
   ciscoatUserProfile, and ciscoatUserProfileString
   attributes for all User objects.
```

Cisco OU の読み取り/書き込み/作成権限の設定

Cisco OU に対して読み取り/書き込み/作成権限を設定するには、次の手順を実行します。

1. [Cisco] コンテナを右クリックします。
2. **Properties** を選択します。
3. [Security] タブを選択します。
4. [Advanced] をクリックします。
5. [Add....] をクリックします。
6. CCM Directory Group と入力します。
7. [Apply onto] フィールドを [This object and all child objects] に設定します。
8. [Read All Properties] の [Allow] をオンにします。
9. [Write All Properties] の [Allow] をオンにします。
10. [Create All Child Objects] の [Allow] をオンにします。
11. [Delete All Child Objects] の [Allow] をオンにします。
12. [OK] をクリックします。

Users OU の読み取り権限の設定

Users OU に読み取り権限を設定するには、次の手順を実行します。

1. [Users] コンテナを右クリックします。
2. **Properties** を選択します。
3. [Security] タブを選択します。
4. [Advanced] をクリックします。
5. [Add....] をクリックします。
6. CCM Directory Group と入力します。
7. [Apply onto] フィールドにユーザ オブジェクトを設定します。
8. [Read All Properties] の [Allow] をオンにします。
9. [OK] をクリックします。

Cisco 属性の読み取り/書き込み権限の設定

Cisco 属性に対して読み取り/書き込み権限を設定するには、次の手順を実行します。

1. [Users] コンテナを右クリックします。
2. **Properties** を選択します。
3. [Security] タブを選択します。
4. [Advanced] をクリックします。
5. [Add....] をクリックします。
6. CCM Directory Group と入力します。
7. [Apply onto] フィールドにユーザ オブジェクトを設定します。
8. [Read ciscoatGUID]、[Read ciscoatUserProfile]、[ReadatUserProfileString] の [Allow] をオンにします。
9. [Write ciscoatGUID]、[Write ciscoatUserProfile]、[Write atUserProfileString] の [Allow] をオンにします。
10. [OK] をクリックします。

新しいユーザの作成

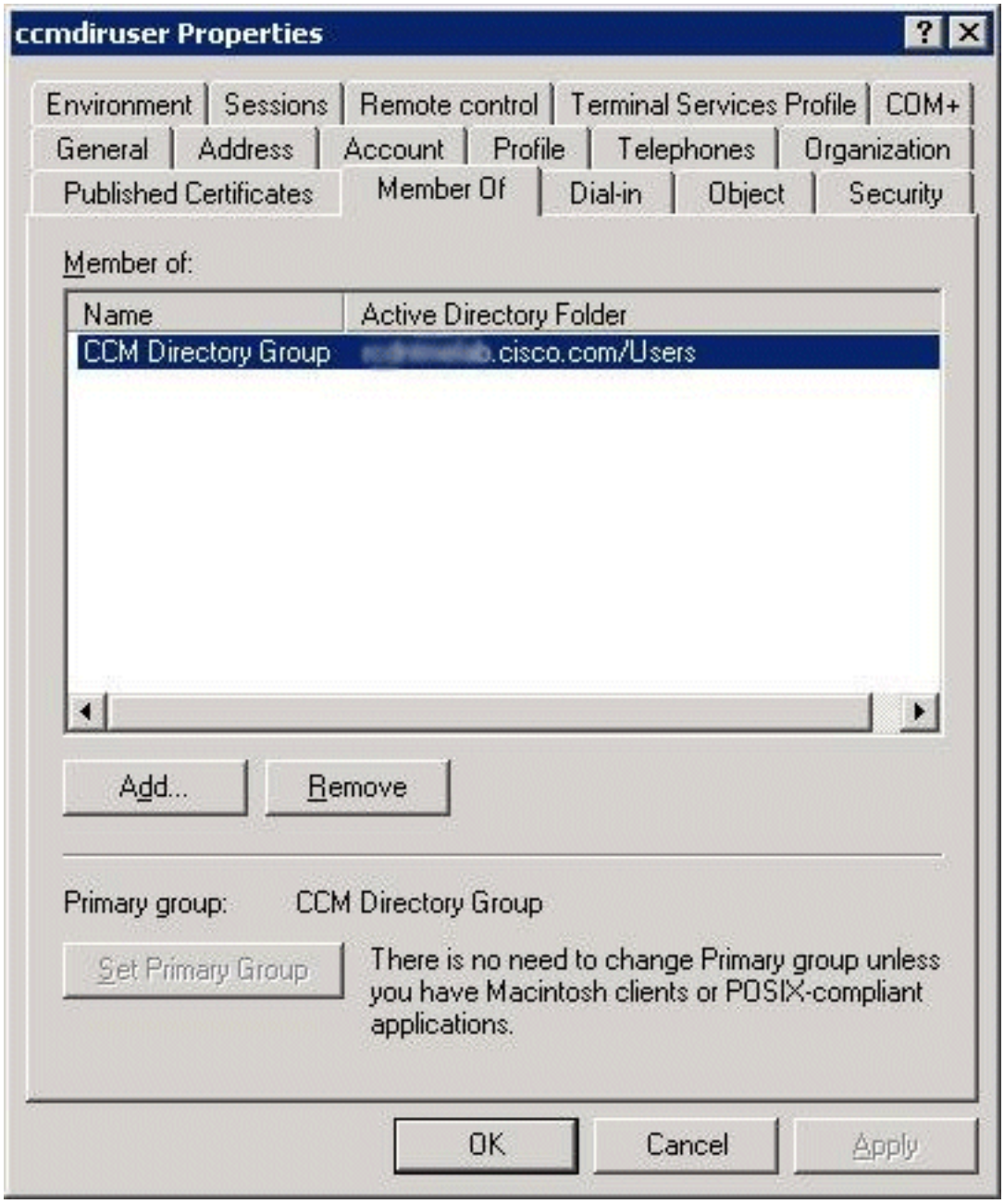
新しいユーザを作成するには、次の手順に従います。

1. [Users] コンテナを右クリックします。
2. [New] > [User] を選択します。
3. **名前**と**ログオン名**を入力します（例：*CUCM Directory Manager*、*ccmdiruser*）。
4. [Password] フィールドと [Confirm Password] フィールドにパスワードを入力します。
5. [Password Never Expires] チェックボックスをオンにします。
6. [Next] をクリックします。
7. **[Finish] をクリックします。**

新しいグループへのユーザの移動と古いグループからのユーザの削除

新しいグループにユーザを移動して古いグループからユーザを削除するには、次の手順を実行します。

1. [Users] OU を選択します。
2. [ccmdiruser] を右クリックし、[Properties] を選択します。
3. [Member Of] タブを選択します。
4. [Add....] をクリックします。
5. CCM Directory Group と入力します。
6. [OK] をクリックします。
7. [CCM Directory Group] を選択します。
8. [Set Primary Group] をクリックします。
9. 古いグループを選択します。
10. [Remove] をクリックします。



新しいユーザを使用するように CUCM を変更する際に必要な 3 つのステップ

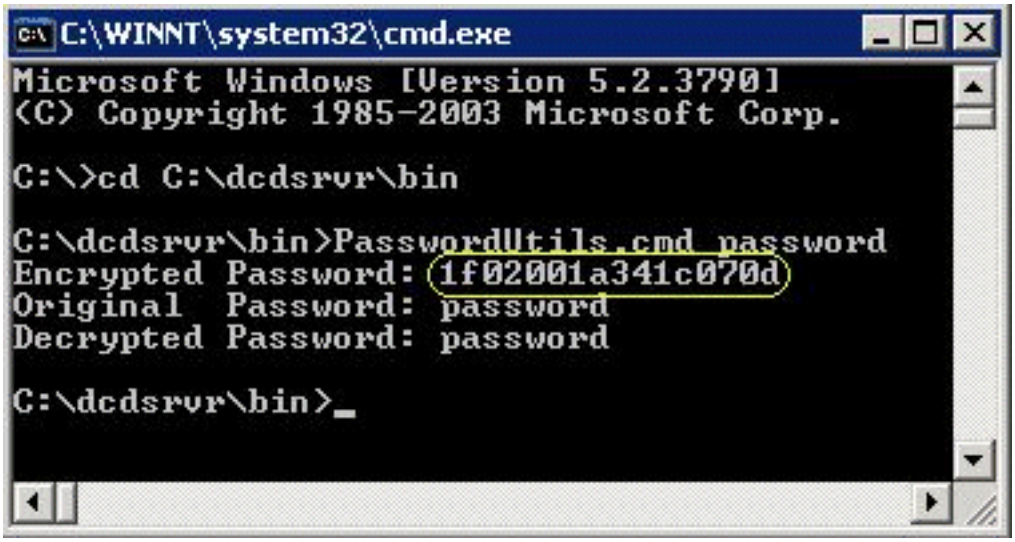
新しいユーザを使用するように CUCM を変更するには、3 つの手順を実行する必要があります。

- 暗号化されたパスワードを取得します。
- レジストリのアカウントとパスワードを設定します。
- DC Directory 初期化ファイルでアカウントとパスワードを設定します。

暗号化されたパスワードの取得

注: この手順では説明の目的でパスワード ***password*** を使用していますが、これよりも複雑なパスワードを使用する必要があります。

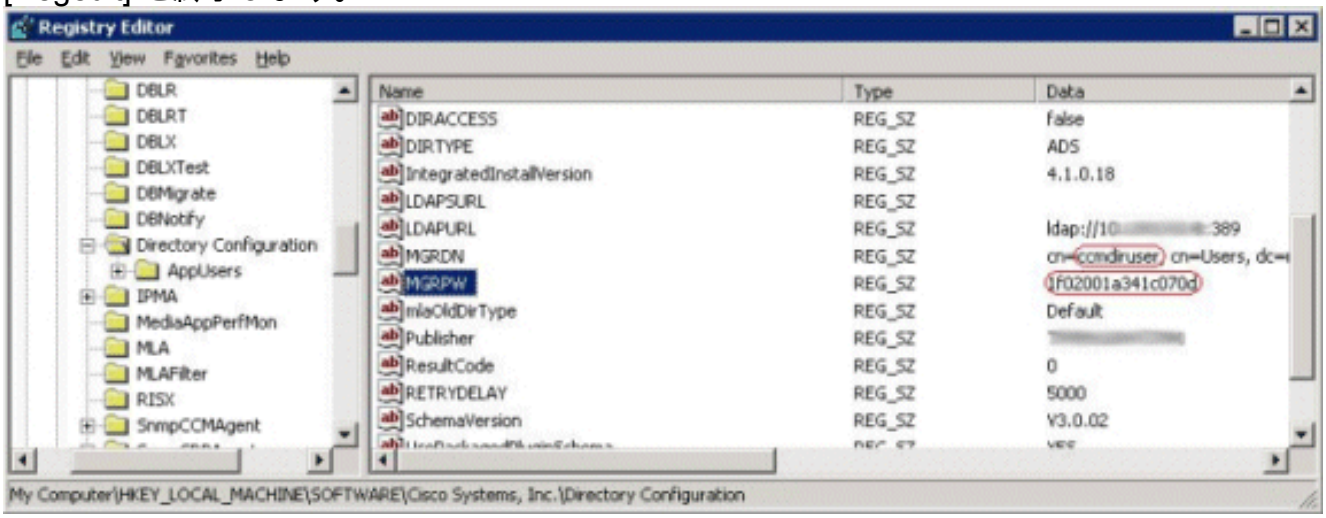
1. [Start] > [Run] を選択します。
2. **cmd** と入力します。
3. **cd C:\dcdsrvr\bin** と入力します。
4. **PasswordUtils.cmd password** と入力します。



レジストリでのアカウントとパスワードの設定

注意： 誤ったレジストリ キーを編集したり、レジストリの編集でミスをすると、レジストリを修復するまでシステムが使用できなくなることがあります。 変更前にレジストリのバックアップを作成しておく必要があります。 続行する前に、必ずレジストリをバックアップから復元する方法を理解しておいてください。 サーバ レジストリの維持方法についてはこのドキュメントの対象外であるため、その情報についてはシステムのドキュメントを参照してください。

1. [Start] > [Run] を選択します。
2. **regedit** と入力し、[OK] をクリックします。
3. レジストリ内で **\\HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\Directory Configuration** を参照します。
4. 右側のペインで、[MGRDN] レジストリ キーをダブルクリックします。
5. ユーザを変更します（例：[Administrator] > [ccmdiruser]）。
6. [MGRPW] レジストリ キーをダブルクリックします。
7. 暗号化されたパスワードを、**PasswordUtils** ツールから取得した値に変更します。
8. [Regedit] を終了します。

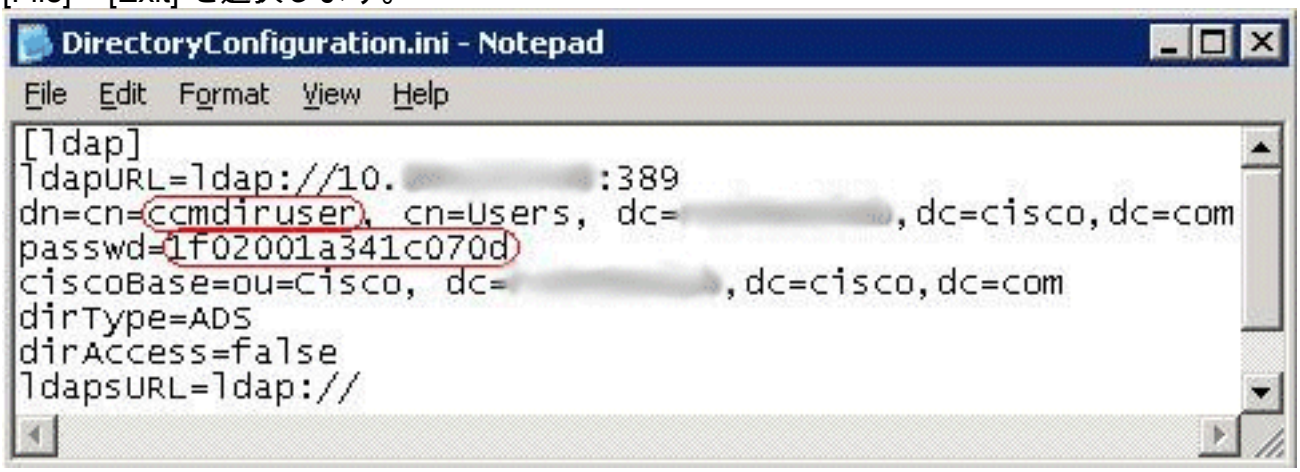


DC Directory ini ファイルでのアカウントとパスワードの設定

DC Directory ini ファイルでアカウントとパスワードを設定するには、次の手順を実行します。

1. [Start] > [Run] を選択します。

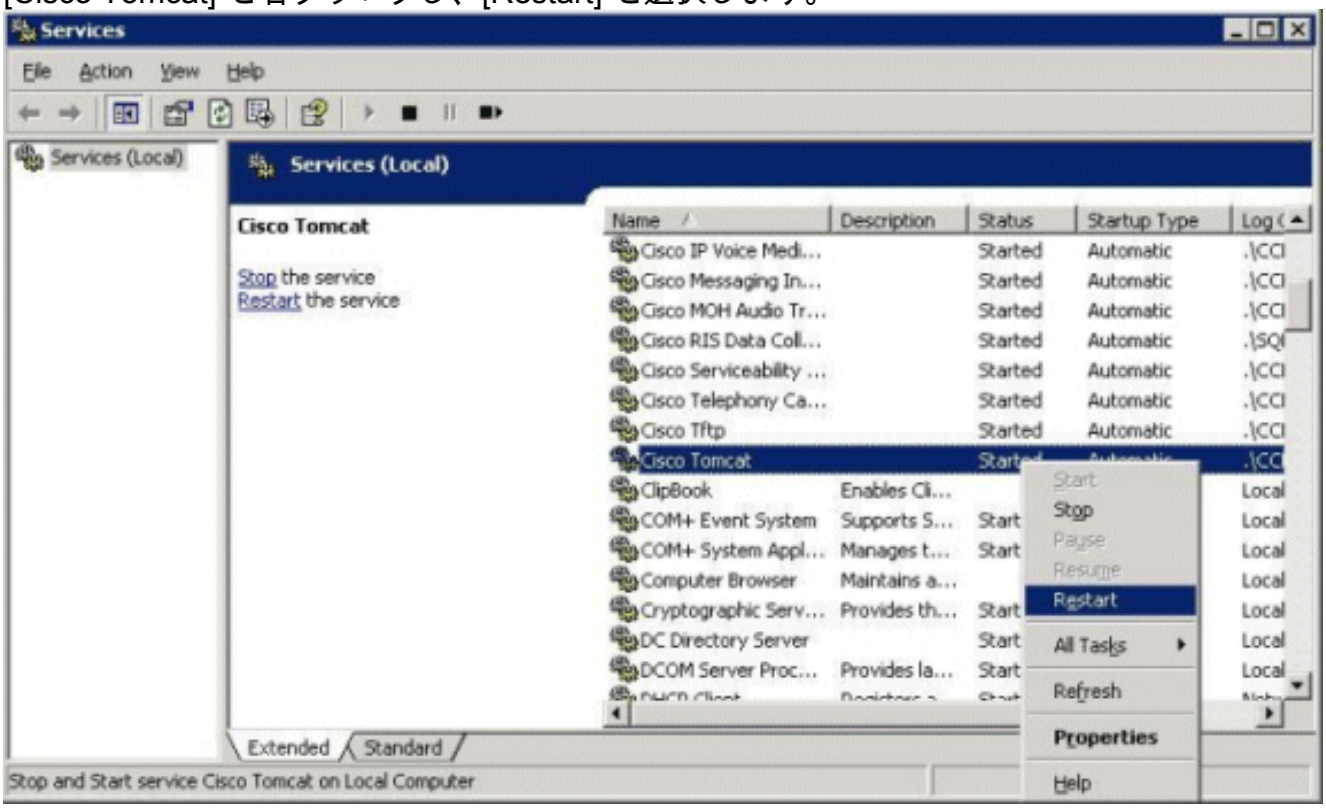
2. **notepad C: //dcdsrvr/DirectoryConfiguration.ini** と入力し、[OK] をクリックします。
3. ユーザを変更します（例：[Administrator] > [ccmdiruser]）。
4. passwd= の右側の値を、**PasswordUtils** ツールから取得した暗号化パスワードに変更します。
5. [File] > [Save] を選択します。
6. [File] > [Exit] を選択します。



Cisco Tomcat の再起動

Cisco Tomcat サービスを再起動するには、次の手順を実行します。

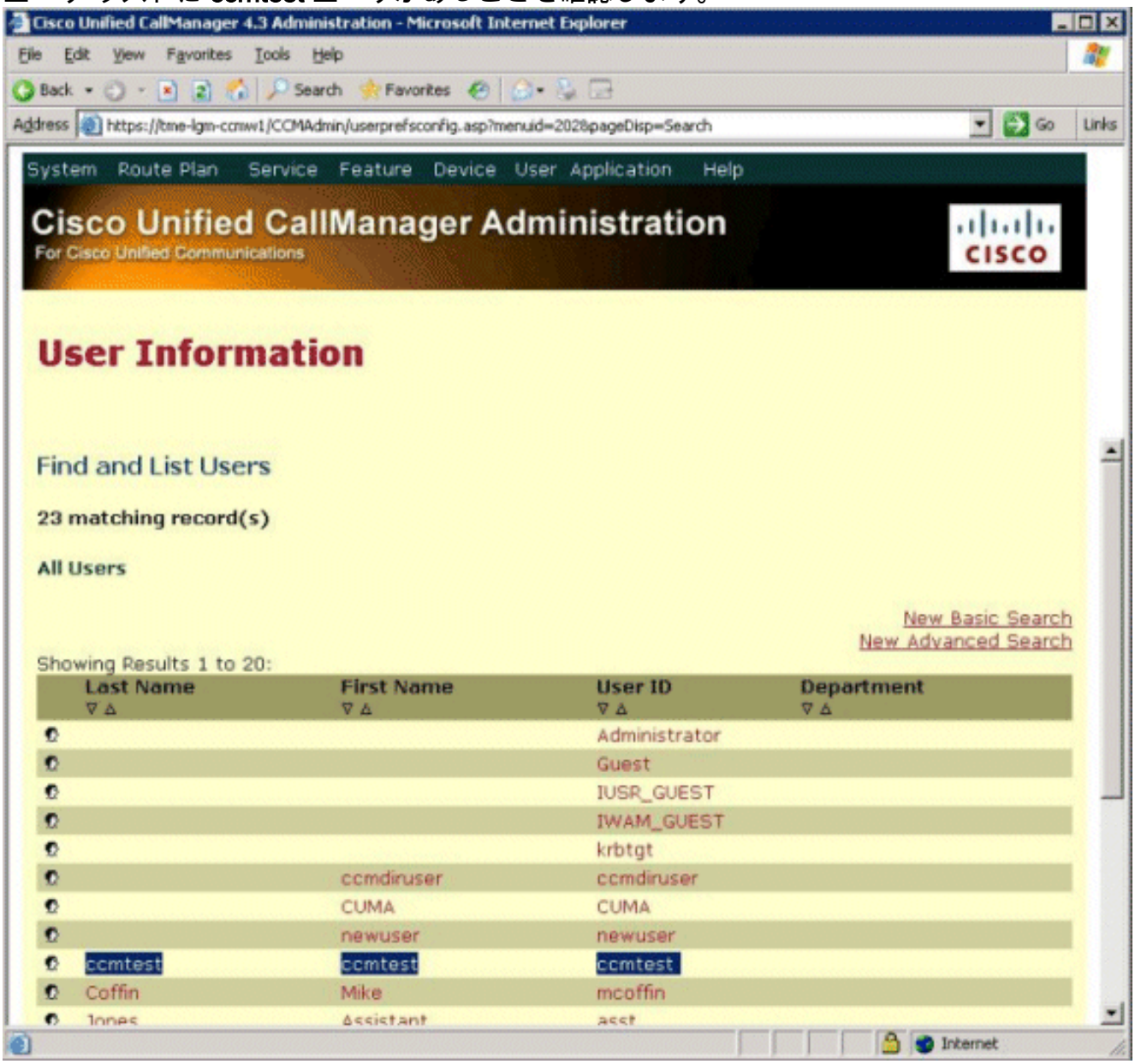
1. [Programs] > [Administrative Tools]> [Services] を選択します。
2. [Cisco Tomcat] を右クリックし、[Restart] を選択します。



CUCM Directory に一時 ccmtest ユーザが含まれていることの確認

CUCM Directory に一時ユーザ ccmtest が含まれていることを確認するには、次の手順を実行します。

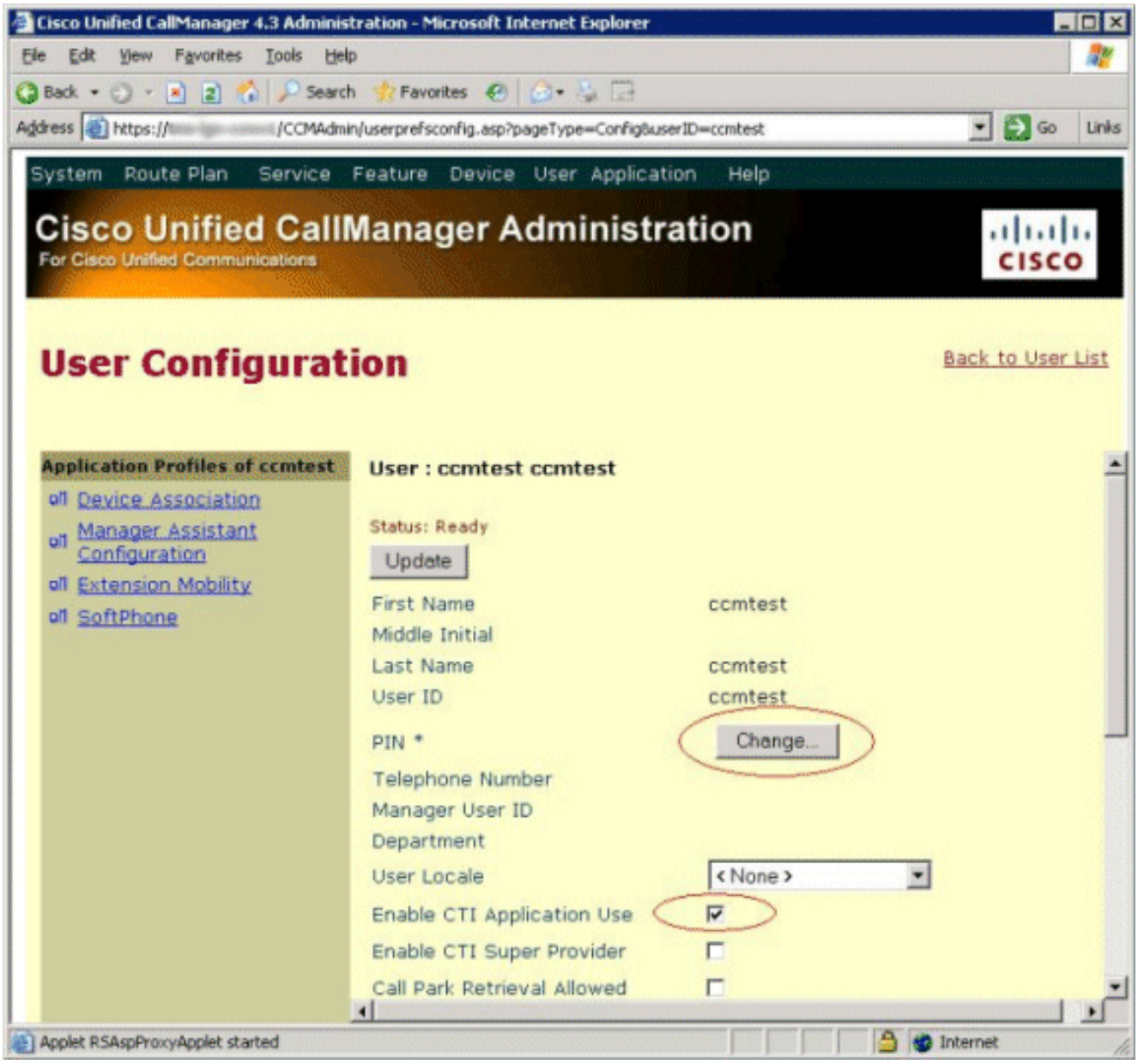
1. [CUCM Administration] ページから、[User] > [Global Directory] を選択します。
2. [Search] ボタンを押します。
3. ユーザ リストに ccmtest ユーザがあることを確認します。



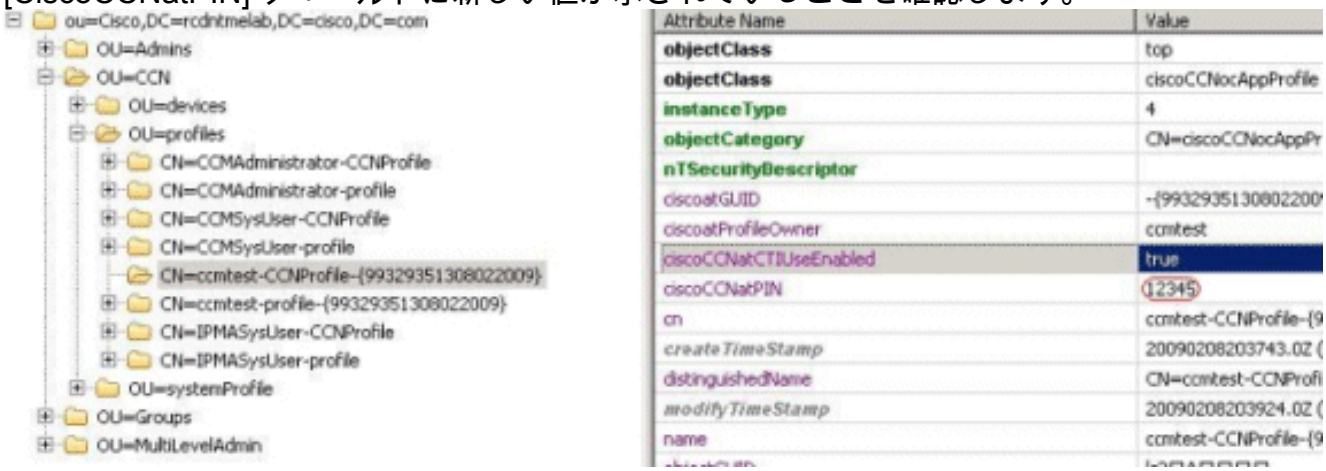
ccmtest ユーザの PIN の変更

ccmtest ユーザの PIN を変更するには、次の手順を実行します。

1. [User Information Page] で [ccmtest] を選択します。
2. [Change...] ボタンをクリックします。
3. 5 桁の PIN を入力します（例：12345）。
4. [Update] ボタンと [Close] ボタンをクリックします。



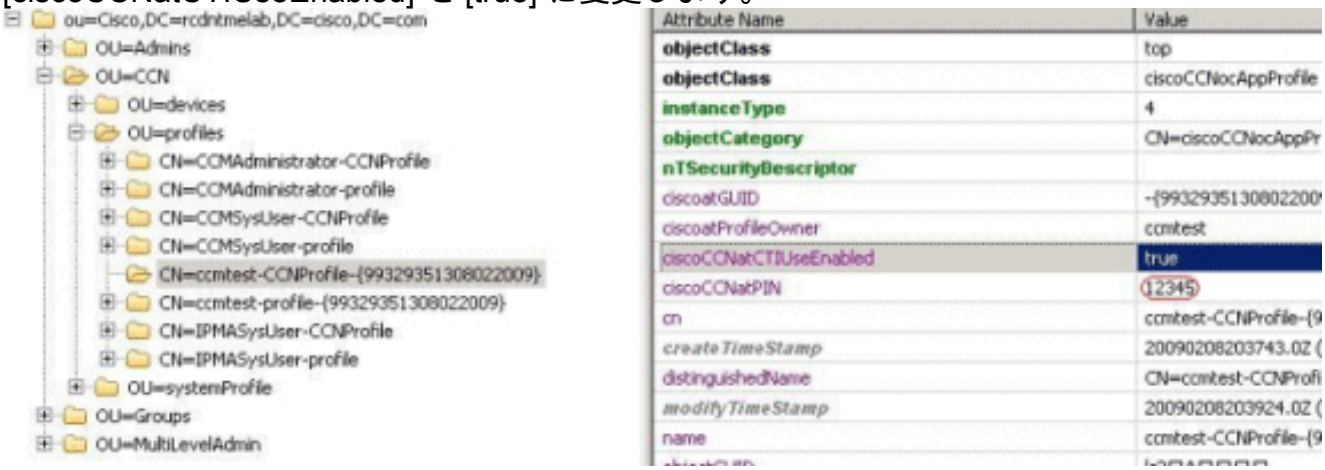
5. ディレクトリ ブラウザを使用して [Cisco OU] を選択します。
6. [CCN] > [profiles] > [ccm-test-CCNProfile] の順に移動します。
7. [CiscoCCNatPIN] フィールドに新しい値が示されていることを確認します。



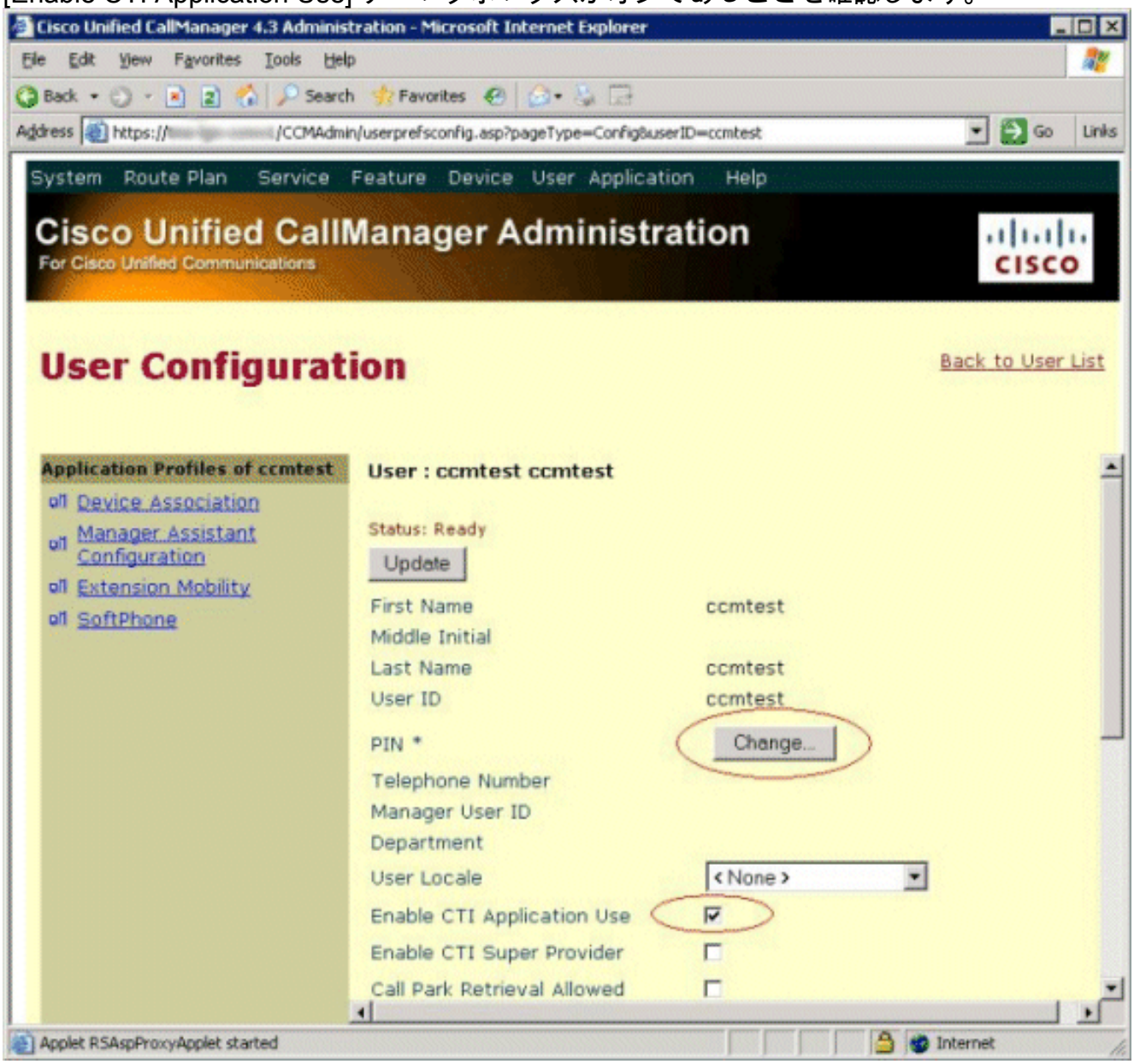
[ciscoCCNatCTIUseEnabled] フィールドの変更

[ciscoCCNatCTIUseEnabled] フィールドを変更するには、次の手順を実行します。

1. ディレクトリ ブラウザを使用して [Cisco OU] を選択します。
2. [CCN] > [profiles] > [ccm-test-CCNProfile] の順に移動します。
3. [ciscoCCNatCTIUseEnabled] を [true] に変更します。



4. ユーザ **ccmtest** の [User Configuration] ページを更新します。
5. [Enable CTI Application Use] チェックボックスがオンであることを確認します。



ccmtest ユーザの削除

ccmtest ユーザを削除するには、次の手順に従います。

1. [Users] OU を選択します。
2. [ccmtest] を右クリックし、[Delete] を選択します。
3. 確認のために [Yes] をクリックします。

関連情報

- LDAP ディレクトリ統合：Cisco Unified Communications SRND for CUCM 4.x
- Cisco CallManager 用の Active Directory 2000 プラグインのインストール
- Active Directory と Cisco CallManager の統合のトラブルシューティング ガイド
- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- Cisco IP Telephony のトラブルシューティング
- テクニカルサポートとドキュメント - Cisco Systems