

Securing LDAP Directory Integration with Cisco Unified CallManager 4.x

Document ID: 109804

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

- For Existent Directory Integration
- For Existent Installation Without Dedicated Account
- For a New Installation
- Verification

Detailed Steps

- Start Microsoft Active Directory (ADUC)
- Create New Group
- Set Group Permissions for Directory Access
- Set Read/Write/Create Privileges on the Cisco OU
- Set Read Privileges on OU of Users
- Set Read/Write Privileges on Cisco Attributes
- Create New User
- Move User to New Group and Remove From Old Group
- Three Steps Required to Change CUCM to Use the New User
- Obtain the Encrypted Password
- Set the Account and Password in the Registry
- Set Account and Password in the DC Directory ini File
- Restart Cisco Tomcat
- Verify that Temporary ccctest User is in CUCM Directory
- Change the PIN of the ccctest User
- Change the ciscoCCNatCTIUseEnabled Field
- Delete the ccctest User

Related Information

Introduction

This document discusses these items:

- Improve the security of LDAP Directory Integration with Cisco Unified CallManager (CUCM) with several configuration steps to restrict permissions. These procedures improve both an existent and new installation of directory integration.
- The access and management of the directory require a special user and group. Permissions are set on objects to restrict the dedicated user and group, and the directory integration is then updated (for an existent install) or completed (for a new install). Finally, the integration is verified.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is specific to Cisco Unified CallManager 4.x.

These steps, which are shown with the Microsoft Active Directory (AD), can also apply to other supported directory products.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

For Existent Directory Integration

Follow these steps for an existent directory integration:

1. Create a new group, such as *CUCM Directory Group*.
2. Set the group permissions for directory access.
3. Move the existent directory user to the new group.
4. Remove the user from the old group; members can only be of the new group.
5. Perform verification.

For Existent Installation Without Dedicated Account

Follow these steps for an existent directory integration where a dedicated account was not used:

1. Create a new user, such as *CUCM Directory Manager*.
2. Make the user a member of the new group only.
3. Change CUCM to use the new user; modify the registry and ini file.
4. Restart the Cisco Tomcat.
5. Change the password of the original account that had been used.
6. Perform verification.

For a New Installation

Follow these steps for a new installation of Directory Integration:

1. Create a new group, such as *CUCM Directory Group*.
2. Set restrictions on this new group.
3. Create a new user, such as *CUCM Directory Manager*.
4. Put the new user into a group with Administrator privileges, for example, *Domain Admins*.
5. Use the new user when you install the plug-in.
6. Move the user to the newly created *CUCM Directory Group*.
7. Set the new group as the primary group for the admin user.
8. Remove this user from the old group, which must no longer be a member of any other group.
9. Perform verification.

Verification

Perform Verification with this procedure:

1. Create a new user, *ccmtest*, in the directory (on the directory server).
2. Check that the *ccmtest* user is listed in CUCM Users.
3. Change the PIN of the *ccmtest* on the CUCM User Configuration page.
4. Ensure that the field is updated in the directory.
5. Change `ciscoCCNatCTIUseEnabled` to **True** for *ccmtest* in the directory.
6. Confirm that the **Enable CTI Application Use** check box is checked for *ccmtest* in CUCM.
7. Delete **ccmtest** user.
8. Ensure that only wanted parts of the tree are visible with an LDAP browser: must not be able to view anything outside the Cisco Organizational Unit (OU) or Users OU.

Detailed Steps

Note: The names that are used here for the dedicated account and group are *CUCM Directory Manager* and *CUCM Directory Group*, respectively, but you can choose different names.

Start Microsoft Active Directory (ADUC)

Choose **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

Create New Group

Follow these steps to create the new group:

1. Right-click the **Users** container.
2. Choose **New > Group**.
3. Enter the Group name, scope, and type, such as *CUCM Directory Group*, *Global*, and *Security*.
4. Click **Next**.
5. Click **Finish**.

Set Group Permissions for Directory Access

The group must be granted these rights:

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

These rights must apply to this object and all child objects.

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

Set Read/Write/Create Privileges on the Cisco OU

Follow these steps to set the Read/Write/Create privileges on the Cisco OU:

1. Right-click the **Cisco** container.
2. Choose **Properties**.

3. Choose the **Security** tab.
4. Click **Advanced**.
5. Click **Add....**
6. Enter *CCM Directory Group*.
7. Set **Apply onto** field to **This object and all child objects**.
8. Check **Allow** for **Read All Properties**.
9. Check **Allow** for **Write All Properties**.
10. Check **Allow** for **Create All Child Objects**.
11. Check **Allow** for **Delete All Child Objects**.
12. Click **OK**.

Set Read Privileges on OU of Users

Follow these steps to set Read privileges on the Users OU:

1. Right-click the **Users** container.
2. Choose **Properties**.
3. Choose the **Security** tab.
4. Click **Advanced**.
5. Click **Add....**
6. Enter *CCM Directory Group*.
7. Set **Apply onto** field to user objects.
8. Check **Allow** for **Read All Properties**.
9. Click **OK**.

Set Read/Write Privileges on Cisco Attributes

Follow these steps to set Read/Write privileges on the Cisco attributes:

1. Right-click the **Users** container.
2. Choose **Properties**.
3. Choose the **Security** tab.
4. Click **Advanced**.
5. Click **Add....**
6. Enter *CCM Directory Group*.
7. Set **Apply onto** field to user objects.
8. Check **Allow** for **Read ciscoatGUID, Read ciscoatUserProfile, ReadatUserProfileString**.
9. Check **Allow** for **Write ciscoatGUID, Write ciscoatUserProfile, Write atUserProfileString**.
10. Click **OK**.

Create New User

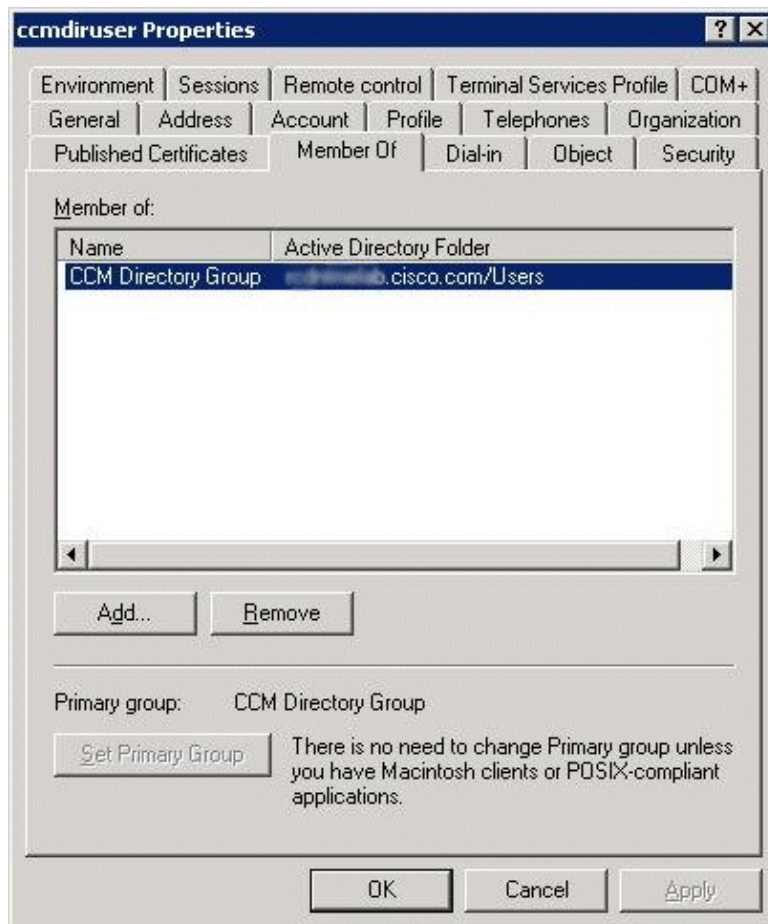
Follow these steps to create a new user:

1. Right-click the **Users** container.
2. Choose **New > User**.
3. Enter the **name** and **logon** name, such as, *CUCM Directory Manager, ccmdiruser*.
4. Fill in the **Password** and **Confirm Password** fields.
5. Check the **Password Never Expires** check box.
6. Click **Next**.
7. Click **Finish**.

Move User to New Group and Remove From Old Group

Follow these steps to move the user to a new group and remove from the old group:

1. Choose the **Users** OU.
2. Right-click **ccmdiruser** and choose **Properties**.
3. Choose the **Member Of** tab.
4. Click **Add...**
5. Enter the CCM Directory Group.
6. Click **OK**.
7. Choose the CCM Directory Group.
8. Click **Set Primary Group**.
9. Choose the old group.
10. Click **Remove**.



Three Steps Required to Change CUCM to Use the New User

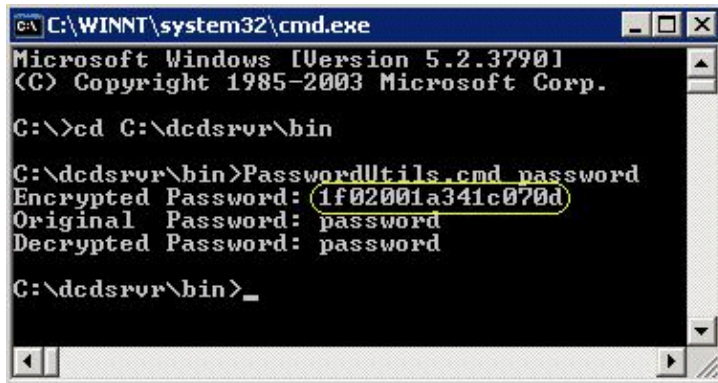
Three steps are required to change CUCM to use the new user:

- Obtain the encrypted password.
- Set the account and password in the registry.
- Set the account and password in the DC Directory initialization file.

Obtain the Encrypted Password

Note: Although the password that is used here is *password* for demonstration purposes, you must use a complex password instead.

1. Choose **Start > Run**.
2. Enter **cmd**.
3. Enter **cd C:\dcldr\bin**.
4. Enter **PasswordUtils.cmd password**.



```
C:\WINNT\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>cd C:\dcldr\bin

C:\dcldr\bin>PasswordUtils.cmd password
Encrypted Password: 1f02001a341c070d
Original Password: password
Decrypted Password: password

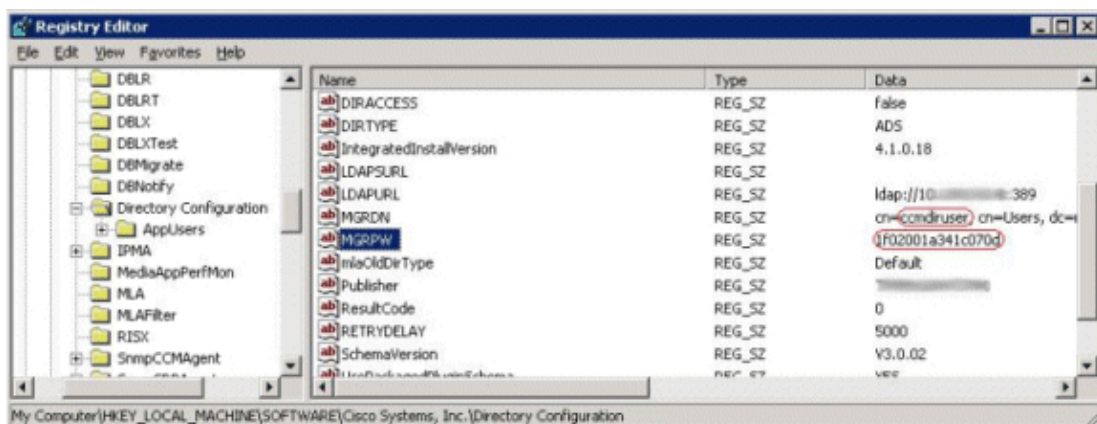
C:\dcldr\bin>_
```

Set the Account and Password in the Registry



Caution: If you edit the wrong registry key or make a mistake while you edit the registry, your system can be unusable until you repair the registry. You must backup your registry before you make any changes. Make sure that you know how to restore the registry from the backup before you continue. Because an explanation of how to maintain the server registry is beyond the scope of this document, consult your system documentation for this information.

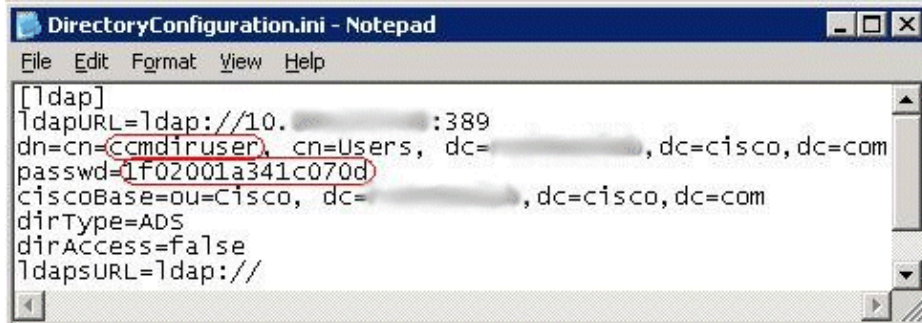
1. Choose **Start > Run**.
2. Enter **regedit** and click **OK**.
3. Browse to **\\HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\Directory Configuration** within the registry.
4. In the right pane, double-click the **MGRDN** registry key.
5. Change the user, for example, *Administrator > cmmdiruser*.
6. Double-click the **MGRPW** registry key.
7. Change the encrypted password with the value obtained from the **PasswordUtils** tool.
8. Exit **Regedit**.



Set Account and Password in the DC Directory ini File

Follow these steps to set the account and password in the DC Directory ini file:

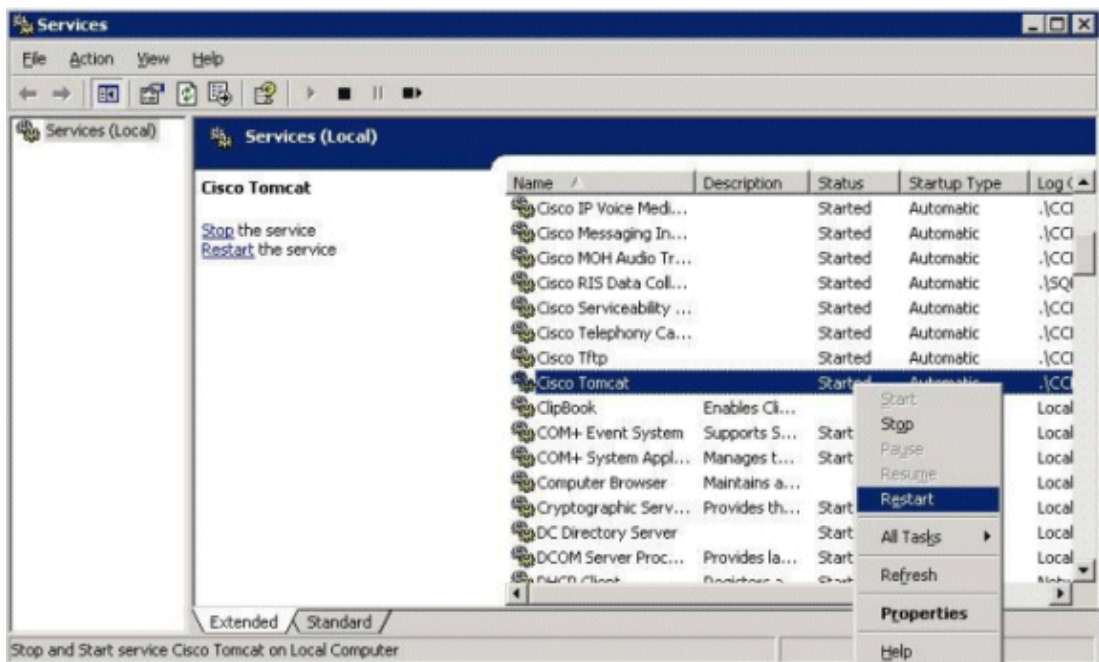
1. Choose **Start > Run**.
2. Enter **notepad C:/dcsvr/DirectoryConfiguration.ini** and click **OK**.
3. Change the user, for example, *Administrator > ccmdiruser*.
4. Change the value to the right of `passwd=` to the encrypted password that you obtained from the **PasswordUtils** tool.
5. Choose **File > Save**.
6. Choose **File > Exit**.



Restart Cisco Tomcat

Follow these steps to restart the Cisco Tomcat service:

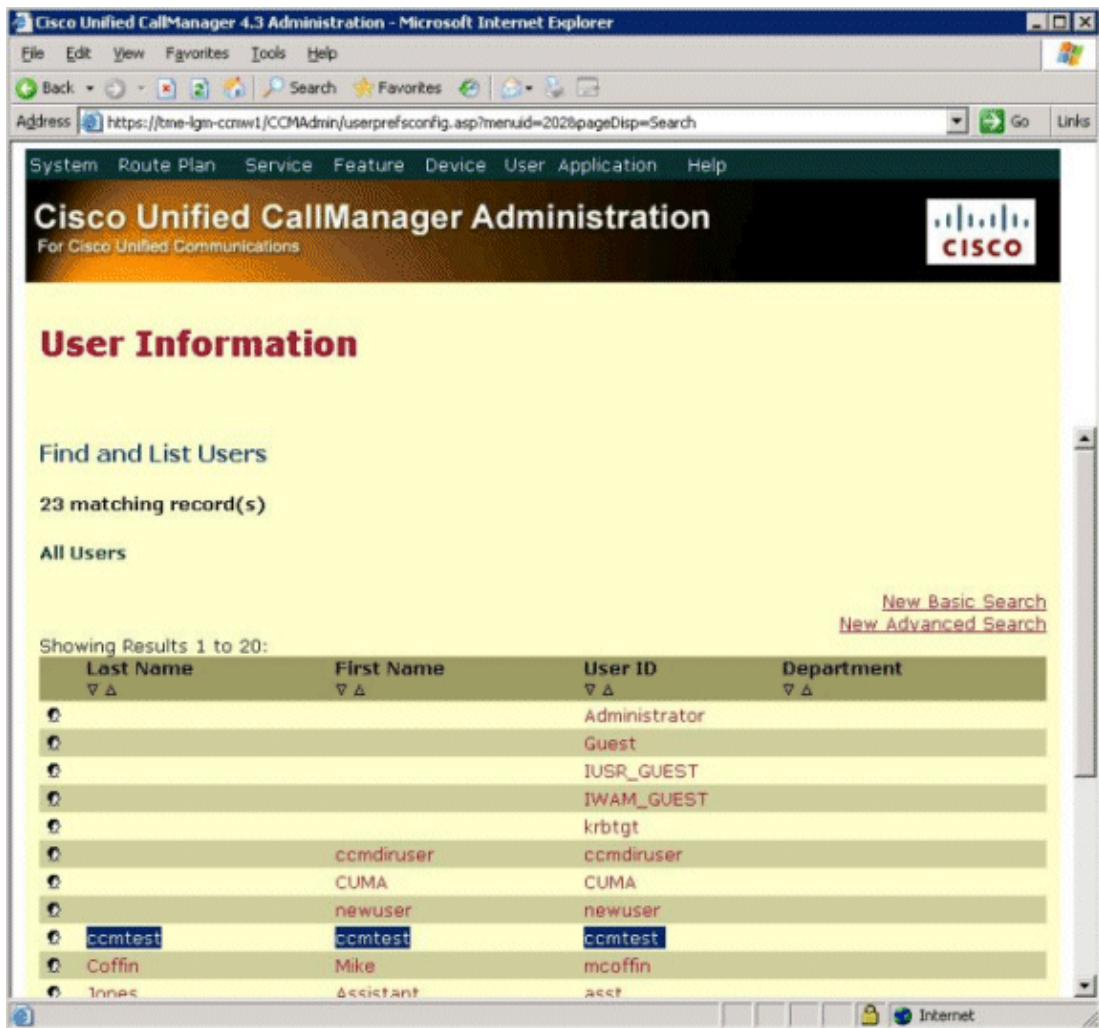
1. Choose **Programs > Administrative Tools > Services**.
2. Right-click **Cisco Tomcat** and choose **Restart**.



Verify that Temporary cmtest User is in CUCM Directory

Follow these steps to verify that the temporary cmtest user is in the CUCM Directory:

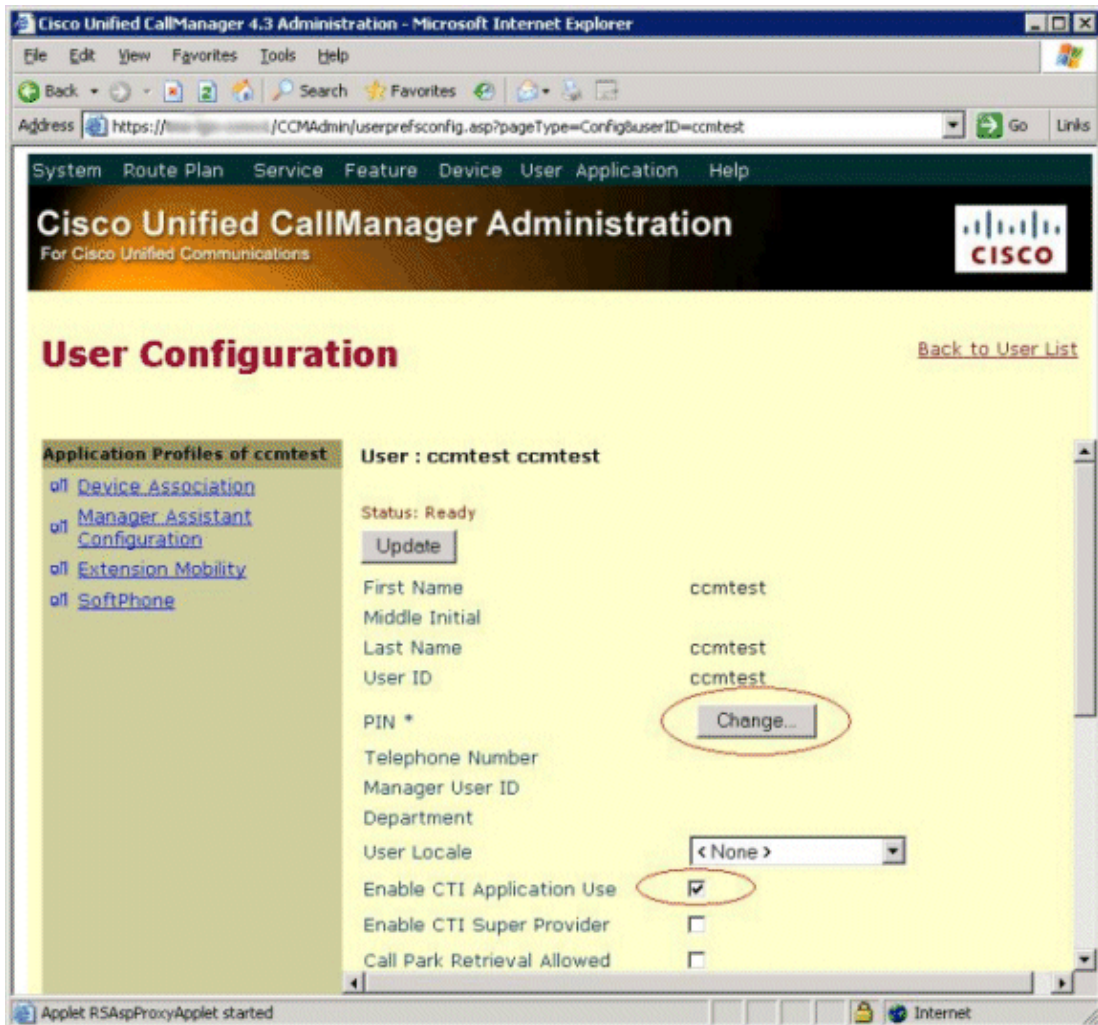
1. From the CUCM Administration pages, choose **User > Global Directory**.
2. Press the **Search** button.
3. Ensure that the **ccmtest** user is in the list of users.



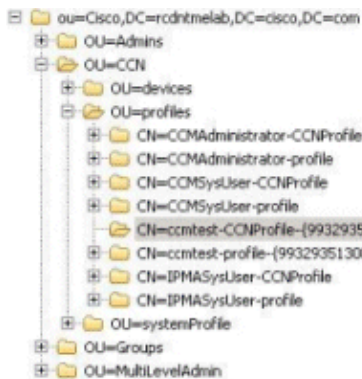
Change the PIN of the ccmtest User

Follow these steps to change the PIN of the ccmtest user:

1. Choose **ccmtest** at the User Information Page.
2. Press the **Change...** button.
3. Enter a 5-digit PIN, for example, 12345.
4. Press the **Update** and **Close** buttons.



5. Use a directory browser to choose the **Cisco OU**.
6. Navigate to **CCN > profiles > ccm-test-CCNProfile**.
7. Ensure that the **CiscoCCNatPIN** field has the new value.

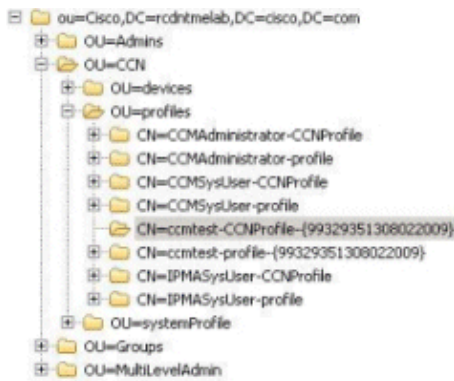


| Attribute Name | Value |
|-------------------------|--|
| objectClass | top |
| objectClass | ciscoCCNocAppProfile |
| instanceType | 4 |
| objectCategory | CN=ciscoCCNocAppPr |
| nTSecurityDescriptor | |
| ciscoatGUID | 99329351308022009 |
| ciscoatProfileOwner | ccmtest |
| ciscoCCNatCTIUseEnabled | true |
| ciscoCCNatPIN | 12345 |
| cn | ccmtest-CCNProfile-{99329351308022009} |
| create Time Stamp | 20090208203743.0Z |
| distinguishedName | CN=ccmtest-CCNProfi |
| modify Time Stamp | 20090208203924.0Z |
| name | ccmtest-CCNProfile-{99329351308022009} |

Change the ciscoCCNatCTIUseEnabled Field

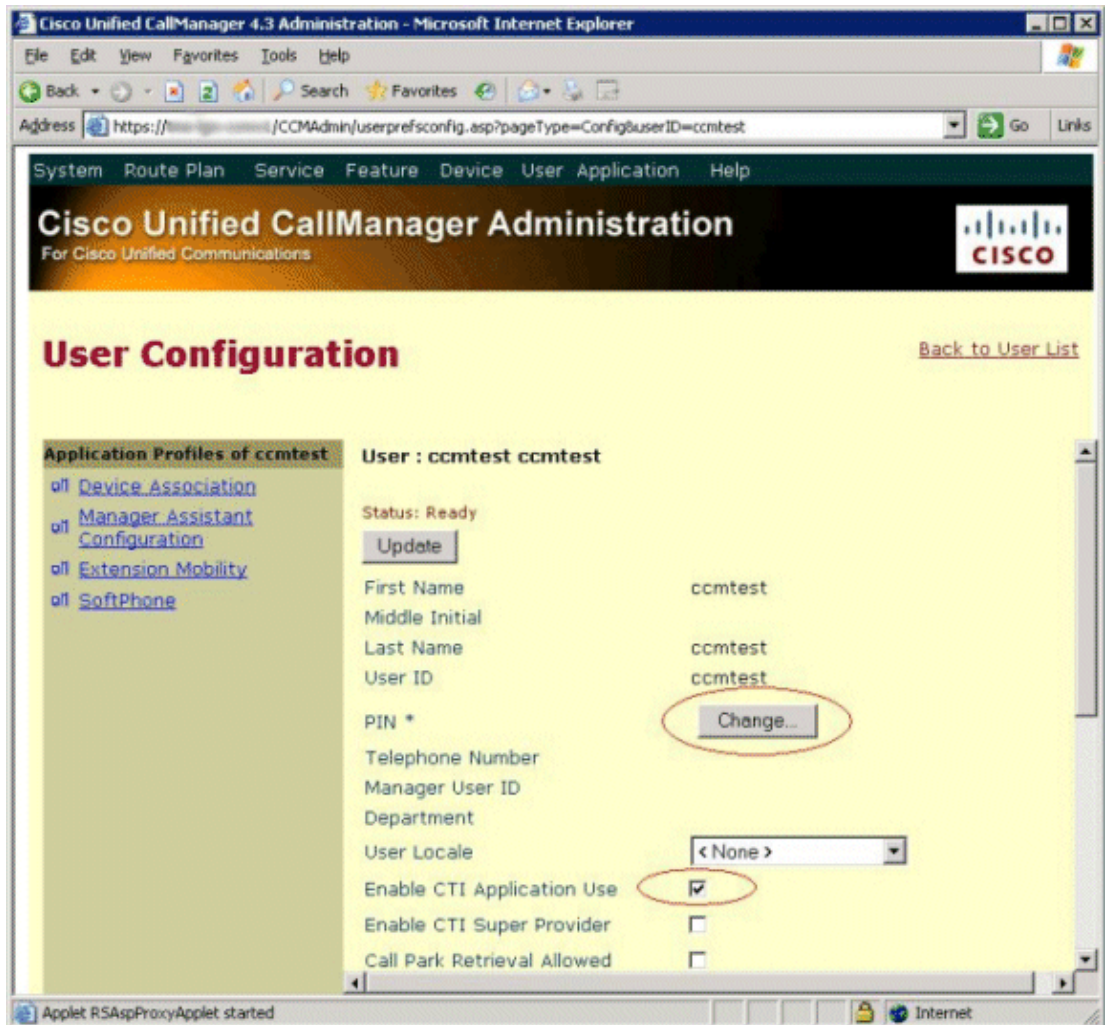
Follow these steps to change the ciscoCCNatCTIUseEnabled field:

1. Use a directory browser to choose the **Cisco OU**.
2. Navigate to **CCN > profiles > ccm-test-CCNProfile**.
3. Modify **ciscoCCNatCTIUseEnabled** to **true**.



| Attribute Name | Value |
|------------------------|---|
| objectClass | top |
| objectClass | ciscoCCNocAppProfile |
| instanceType | 4 |
| objectCategory | CN=ciscoCCNocAppPr |
| nTSecurityDescriptor | |
| ciscoatGUID | --{99329351308022009} |
| ciscoatProfileOwner | ccmtest |
| ciscoCNatCTIUseEnabled | true |
| ciscoCNatPIN | 12345 |
| cn | ccmtest-CCNProfile-(99329351308022009) |
| createTimeStamp | 20090208203743.02 (UTC) |
| distinguishedName | CN=ccmtest-CCNProfile-(99329351308022009) |
| modifyTimeStamp | 20090208203924.02 (UTC) |
| name | ccmtest-CCNProfile-(99329351308022009) |

4. Refresh the User Configuration page for user **ccmtest**.
5. Ensure that the **Enable CTI Application Use** check box is now marked.



Delete the ccmtest User

Follow these steps to delete the ccmtest user:

1. Choose the **Users OU**.
2. Right-click **ccmtest** and choose **Delete**.
3. Choose **Yes** to confirm.

Related Information

- **LDAP Directory Integration – Cisco Unified Communications SRND for CUCM 4.x**
 - **Active Directory 2000 Plug-in Installation for Cisco CallManager**
 - **Active Directory and Cisco CallManager Integration Troubleshooting Guide**
 - **Voice Technology Support**
 - **Voice and Unified Communications Product Support**
 - **Recommended Reading: Troubleshooting Cisco IP Telephony**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 09, 2009

Document ID: 109804
