

How to Change the DC Directory Password

Document ID: 12100

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure the DC Directory Manager Password

- Change the Password

- Restart Worldwide Web Publishing Service

Verify

Troubleshoot

Related Information

Introduction

This document describes the steps required to change the Data Connection (DC) directory password. Directory Manager is the superuser account for the integrated Lightweight Directory Access Protocol (LDAP) database in Cisco IP Telephony systems. The default DC Directory Manager password for Cisco CallManager systems is *ciscocisco*. This document describes how to change the default DC Directory password to a password that you choose.

Note: With Cisco CallManager 3.1 and later, you can specify a new password at the start of the product installation. If you upgrade from Cisco CallManager 3.0(x) to CallManager 3.09 or later, the password remains as *ciscocisco*, and you must follow these procedures to change the password. These procedures have been verified for use with Cisco Call Manager Version 3.3 and earlier.

Prerequisites

Requirements

You must have superuser account privileges before you can change the DC Directory Manager password. Also, you should be familiar with the Cisco CallManager Administration application.

If you use CallManager version 3.2 or earlier, complete these steps in order to download the DC Directory scripts:

1. Download **DCDScripts.1-0-5.exe** from the Cisco CallManager Version 3.2 (registered customers only) website.
2. Copy and run **DCDScripts.1-0-5.exe** on *all* the nodes in the Cisco CallManager cluster and on the CRA/CRS application servers.
3. Accept the default settings when prompted to do so, and click **Unzip**.

Components Used

This document was developed and tested with Cisco CallManager 3.1(2c).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

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

Configure the DC Directory Manager Password

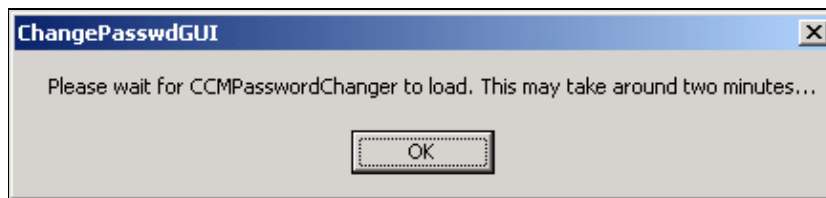
This section presents you with the information to configure the features this document describes. Complete these procedures in order to replace the default DC Directory password with a password that you choose.

Change the Password

Complete these steps in order to change the password:

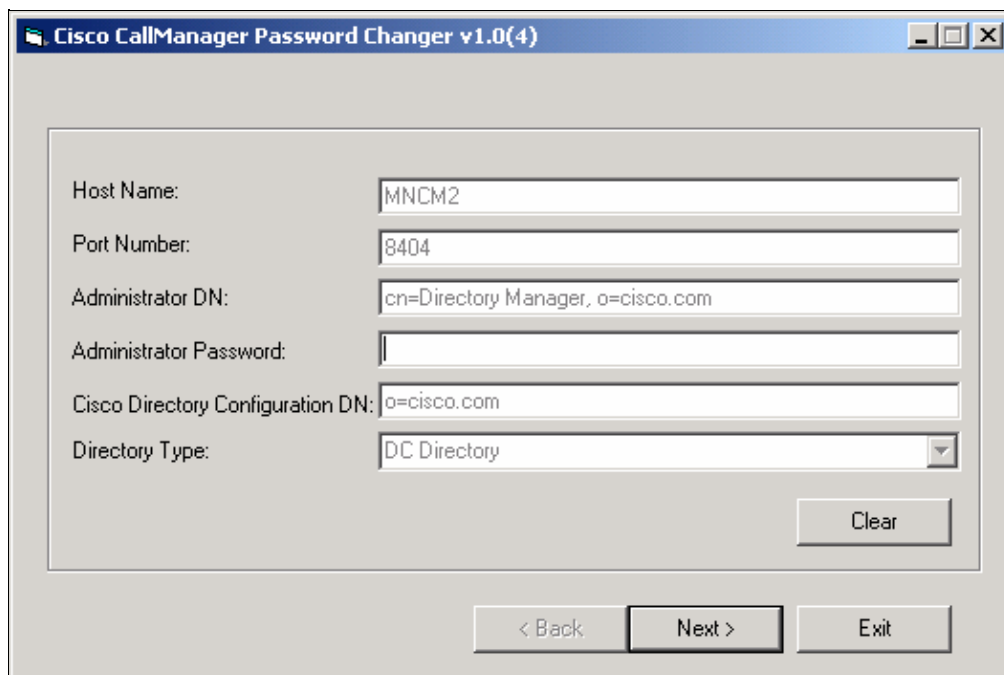
1. From Cisco CallManager, go to **Start > Run**, type **CCMPWDChanger**, and press **enter**.

If you run Cisco CallManager 3.3.3 only, you receive this message:

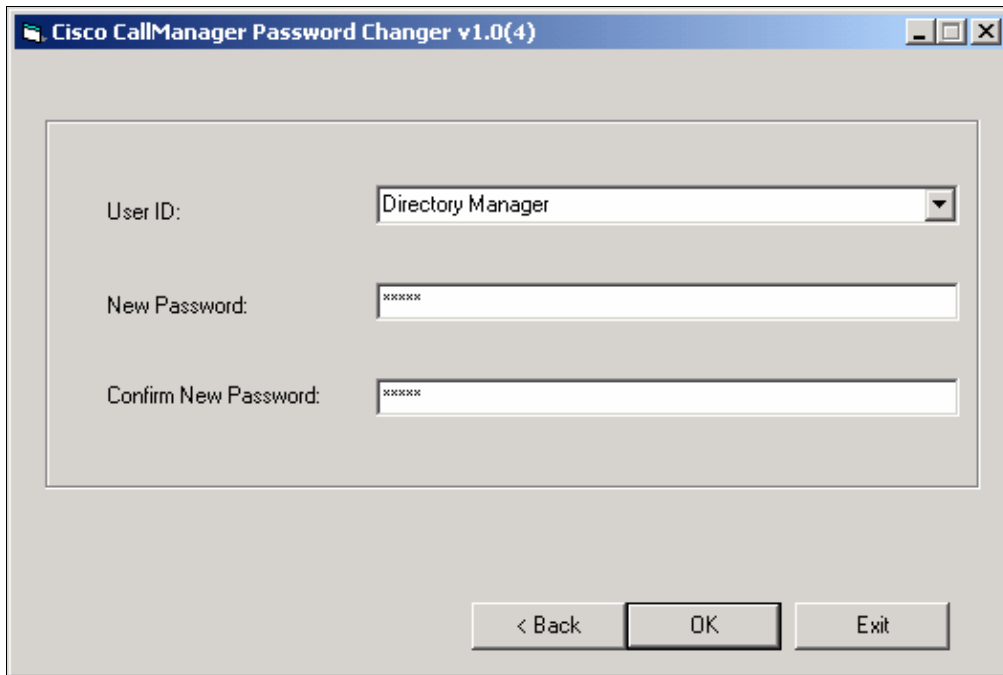


2. Click **OK** to continue.

The Cisco CallManager Password Changer dialog box appears.

A screenshot of the "Cisco CallManager Password Changer v1.0(4)" dialog box. The title bar is blue with standard window controls. The main area contains several input fields: "Host Name" (MNCM2), "Port Number" (8404), "Administrator DN" (cn=Directory Manager, o=cisco.com), "Administrator Password" (empty), "Cisco Directory Configuration DN" (o=cisco.com), and "Directory Type" (DC Directory). A "Clear" button is located at the bottom right of the input area. At the very bottom of the dialog box are three buttons: "< Back", "Next >", and "Exit".

3. In the Administrator Password field, enter the current password, and click **Next**.



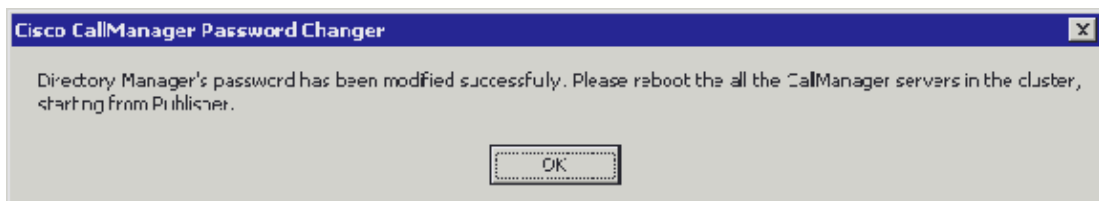
4. Type **Directory Manager** in the User ID field.
5. Enter a password in the New Password field, and confirm the password in the Confirm New Password.
6. Click **OK**.

If you run Cisco CallManager 3.3.3, this message appears:



7. Click **OK**.

If you run other versions of Cisco CallManager, this message appears:



8. Click **OK**.

Note: Even though the message instructs you to reboot all the Callmanager servers in the cluster, it is not mandatory to reboot the servers.

9. Click **Exit** to close the application.

This utility modifies all the registry changes and synchronizes the new password with all Cisco CallManagers in the cluster. There is no need to run this utility in other Cisco CallManagers in the cluster. However, if you run other applications like CRS, PA, CER and so forth, those applications need to be configured with the new password.

Restart Worldwide Web Publishing Service

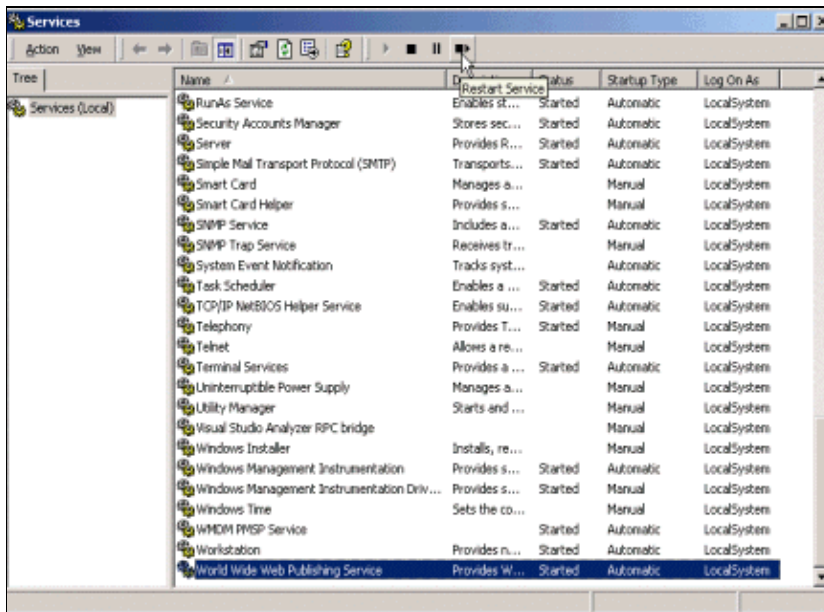
You have successfully changed the password. In order to complete the process, you must stop and start these services.

Note: This procedure must be performed on all Cisco CallManagers in the cluster.

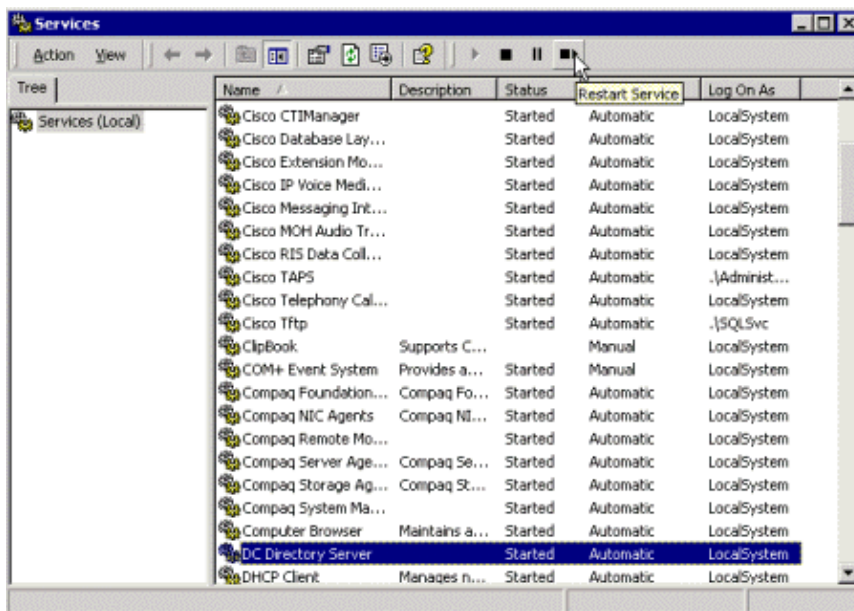
1. Go to the Control Panel, choose **Administrative Tools**, and then double-click **Services**.

The Services window appears.

2. Choose the **Worldwide Web Publishing Service** entry, click **Stop**, and then click **Start**.



The DC Directory Server entry should show "Started" in the Status column.



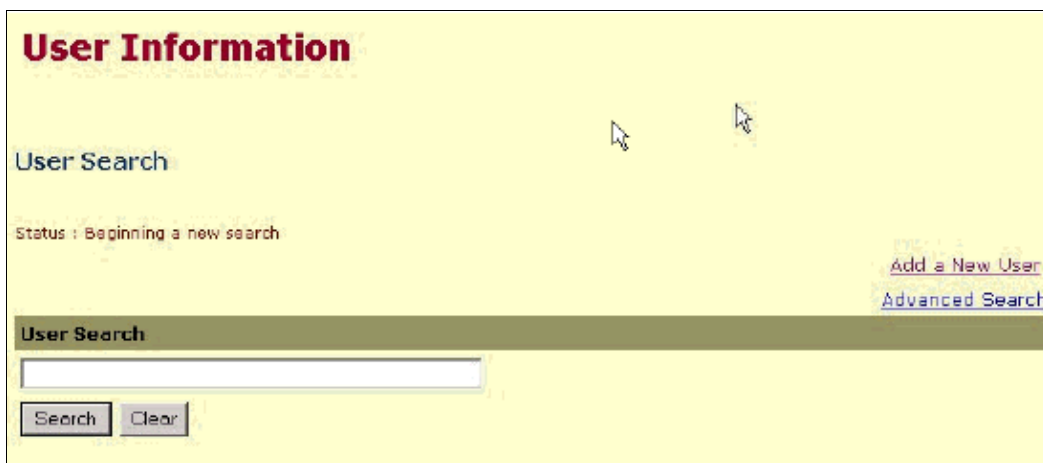
Verify

Complete these steps in order to verify that you successfully changed the Cisco CallManager DC Directory Manager password.

1. Go to the Cisco CallManager Administration page, and choose **User > Global Directory**.

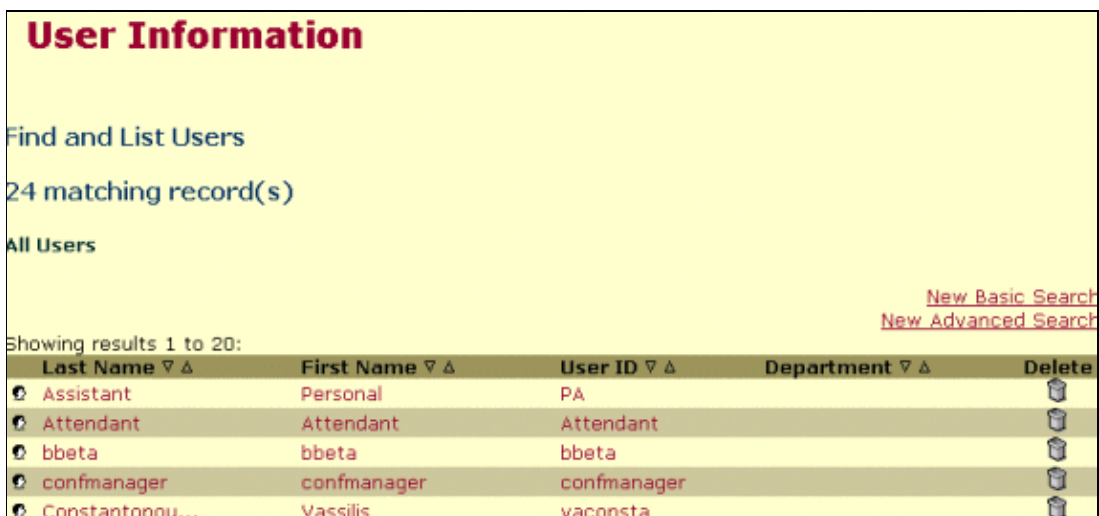


The User Information window appears.



2. Click **Search**.

The configuration is successful if you are able to view the users configured in the system, as shown in this image:



Troubleshoot

Verify these items if you are unable to view the users configured in the system:

1. Log in to the DC Directory with the new password in order to verify that the new password is active.
 2. Verify that the Worldwide Web Publishing Service has restarted and runs after the restart.
-

Related Information

- **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](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 17, 2009

Document ID: 12100
