

Change Passwords in Cisco CallManager and Cisco Unity Configuration Example

Document ID: 71555

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Change Passwords in Cisco CallManager

- CCMPWDChanger Tool
- Change CallManager Services Passwords with the Admin Utility

Change Password in Cisco Unity

Change Your Phone Password from the Cisco Unity Assistant

Change the Password of the Personal Communication Assistant (PCA) User

- Set the PCA Password to Never Expire

Verify

Troubleshoot

- SQLSvc User Cannot Log in
- Unable to Log in to CCMAAdmin after Password is Changed with CCMPWDChanger

Related Information

Introduction

For security reasons, you should change administrative passwords for Cisco Unity and Cisco CallManager whenever the administrator changes. This document discusses how to change the passwords and different utilities you can use in order to perform the task.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of Windows Active Directory and DC Directory
- Knowledge of Cisco CallManager
- Knowledge of Cisco Unity

Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 3.x and 4.x
- Cisco Unity 2.4x, 3.x, and 4.x

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.

Background Information

When the Administrator changes the passwords in Cisco CallManager and Cisco Unity, the Administrator should be knowledgeable about the dependency of each account and services. Many of the service passwords should be the same throughout the cluster.

Change Passwords in Cisco CallManager

You can change the administrative passwords using either one of these methods on Cisco CallManager servers that run on a Windows Operating System. It is necessary to reboot the cluster after you change the passwords in order to remove any potential problems with Windows password caching.

Note: If the Lightweight Directory Access Protocol (LDAP) setting is Microsoft Active Directory instead of DC Directory, you must manually set this password using Active Directory.

Note: The Administrator account serves as the default Windows NT administration account. Cisco CallManager does not use this password.

- Choose **Start > Program Files > Administrative Tools > Computer Management > Users**, select **Administrator Account** and right-click **Set Password**.
- The Windows Administrator account password is a login password into the physical server. You can change the Windows Administrator password when you press **Ctrl+Alt+Delete** and click on **Change Password**.

CCMPWDChanger Tool

The CCMPWDChanger tool is used to change the passwords for Directory Manager, CCMSysUser, CCMAAdministrator, and IPMASysUser.

From the Cisco CallManager, choose **Start > Run**, type **CCMPWDChanger** and press **Enter**. Refer to Change the Password for more details on the CCMPWDChanger tool.

Note: The CCMPWDChanger tool should be used only on the Cisco CallManager Publisher server.

Change CallManager Services Passwords with the Admin Utility

The Admin Utility is used in order to change the services password and synchronize for SQLSvc, CCMSERVICE, CCMSERVICE, CCMCDR, and CCMUser in the Cisco CallManager cluster. Run this from **C:\Program Files\Cisco\Bin\Adminutility.exe**. The Admin Utility changes the cluster private password, which in turn generates new encrypted passwords for the SQLSvc, CCMSERVICE, CCMSERVICE, CCMCDR, and CCMUser accounts. Keep this in mind when running this utility. Refer to Check Password Synchronization with the Admin Utility in the Cisco CallManager Cluster for more information on the Admin Utility.

Change Password in Cisco Unity

Check your version of Cisco Unity before you change the passwords and make sure that the Cisco Unity service account is associated with more applications in your network. The procedure you use to change

passwords is different in some versions of Cisco Unity. For more details on how to change password in the Exchange server and Cisco Unity, refer to How to Change the NT Password for the Exchange and Unity Service Accounts.

Change Your Phone Password from the Cisco Unity Assistant

Complete these steps in order to change your phone password from the Cisco Unity Assistant:

1. Logon to Cisco Unity Assistant on the **Preferences** menu and click **Personal**.
2. In the New Password box, enter a password. Enter digits in the range of 0 through 9.
3. In the Confirm New Password box, enter the password again and click **Save**.

Change the Password of the Personal Communication Assistant (PCA) User

The password for the PCA user is the password for the user in Active Directory, but *not* the phone password of the Cisco Unity subscriber. You can change the PCA user's password from Active Directory when you complete these steps:

1. Log off the Cisco PCA, press **Ctrl–Alt–Delete**, and then click **Change Password**.
2. Specify the domain name for the Cisco Unity server if the Cisco Unity server is in a different domain than the one that you typically access with your Windows password.
3. Complete these steps in order to reset the user's password from Active Directory.
 - a. Choose **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
 - b. Open the domain and then open the Users folder.
 - c. Right-click on a user for PCA login and select **Reset Password**.
 - d. Reset the password.
 - e. Try to login to PCA.

Set the PCA Password to Never Expire

Complete these steps in order to set the PCA password to never expire:

1. Choose **Start > Programs > Administrative Tools > Active Directory Users and Computers**
2. Open the domain.
3. Open the Users folder.
4. Right-click on a user for PCA login.
5. Choose **Properties > Account > Account Options**.
6. Check **Password Never Expires**.

Verify

After you change the passwords in Cisco CallManager, refer to Cisco CallManager: Detecting and Solving SQLSvc Password Problems in order to verify whether it works properly.

Troubleshoot

SQLSvc User Cannot Log in

Sometimes the SQLSvc user cannot log in and dependent services do not start after the passwords are changed. This problem can be resolved by using the same SQLSvc password across the entire cluster. Refer to SQLSvc User Cannot Log In for more information.

Unable to Log in to CCMAAdmin after Password is Changed with CCMPWDChanger

If you are unable to log in to the CCMAAdmin after you change the CCM cluster password with the CCMPWDChanger, you should rerun the AD Plugin in order to resolve the issue as described in Active Directory 2000 Plugin Installation for Cisco CallManager.

Related Information

- [Failure to Synchronize Directory Services in Cisco Desktop Administrator – Reset Password](#)
 - [Active Directory and Cisco CallManager Integration Troubleshooting Guide](#)
 - [Cisco Security Advisory: Cisco Unity with Exchange Has Default Passwords](#)
 - [Unity: Changing Passwords](#)
 - [Cisco CallManager System Issues](#)
 - [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: May 24, 2007

Document ID: 71555
