

Recovering an SQLSvc Account Password

Document ID: 20693

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Problem

Solution for CallManager versions 3.0, 3.1 and 3.2

Solution for Cisco CallManager Version 3.3 and 4.0

Related Information

Introduction

The SQLSvc is the core account used for server-to-server interaction within a Cisco CallManager system. This account must be the same on every Cisco CallManager in the cluster. Otherwise, database replication will not work properly. The SQLSvc account must log in to the local system before the Cisco CallManager, SQLServerAgent, MSSQLServer, and COM+ Event System services can start and execute their specific functions. If the SQLSvc account password and the dependent service passwords are not same throughout the cluster, many of the services will not start. This will affect the basic functionality of the Cisco CallManager, both locally and within the cluster.

This document describes how to change an SQLSvc account password and dependent services password in a Cisco CallManager in order to synchronize the password throughout the cluster. The procedure is different for versions 3.3 and 4.0. In these versions, Admin Utility is used to synchronize the password.

Prerequisites

Requirements

Readers of this document should have knowledge of Cisco CallManager Administrative accounts and passwords. This will help to understand the contents of this document better. Refer to **Administrative Accounts and Passwords** for details.

Components Used

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

- Cisco CallManager versions: 3.0, 3.1, 3.2, 3.3 and 4.0.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Problem

The SQLSvc user must log in to the local system before the Cisco CallManager, SQLServerAgent, MSSQLServer, and COM+ Event System services can start and execute their specific functions. If the SQLSvc password is not configured correctly, both locally and within the cluster, the SQLSvc user cannot log in, and these dependent services will not start. As a result, Cisco CallManager and its basic functionality can be affected.

Note: The SQLSvc password should be the same across the entire cluster.

This problem affects the following:

- Cisco CallManager
- Microsoft SQL server for Cisco Call Manager
- Cisco Music on Hold (MOH) Audio Translator
- Cisco Trivial File Transfer Protocol (TFTP)

Solution for CallManager versions 3.0, 3.1 and 3.2

To solve this problem, synchronize the password for all dependent services running in the Cisco CallManager. This procedure is explained in detail here for the Publisher Cisco CallManager.

1. Select **Start > Programs > Administrative Tools > Computer Management**.
2. Click + (the plus sign) beside Local Users and Groups in the left column.
3. Click **Users**.
4. Right-click **SQLSvc** in the right column, and select **Set Password**.
5. Enter the new password and confirm the password.
6. Click **OK** to confirm, and close the Change Password dialog box.
7. Click + (the plus sign) beside Services and Applications in the left column.
8. Click **Services**.
9. In the right column, click and highlight **Cisco Database Layer Monitor**.
10. Right-click **Cisco Database Layer Monitor**, and select **Properties**.
11. Select the **Log On** tab.
12. Change the password, and confirm that the password matches the local .\SQLSvc user password set in step 5 above.
13. Click **OK** to return to the Services List.
14. Repeat steps 10–13 for the services **MSSQLServer** and **SQLServerAgent**.
15. Close the Computer Management window.
16. Select **Start > Programs > Administrative Tools > Component Services**.
17. Click + (the plus sign) beside Component Services.
18. Click + (the plus sign) beside Computers.
19. Click + (the plus sign) beside My Computer.
20. Click + (the plus sign) beside COM+ Applications.
21. Right-click **DBL** and select **Properties**.
22. Click the **Identity** tab.
23. Change the password, and confirm that the password matches the SQLSvc user password set in step 5 above.
24. Click **OK** to go back to the Component Manager.
25. Right-click **DBL**, and click **Shut Down**.
26. Right-click **DBL**, and click **Start**.
27. Close the Component Manager window.
28. Repeat steps 1–27 for all Subscribers in the Cisco CallManager Cluster. The SQLSvc password needs to be identical for all servers in the Cluster.

Solution for Cisco CallManager Version 3.3 and 4.0

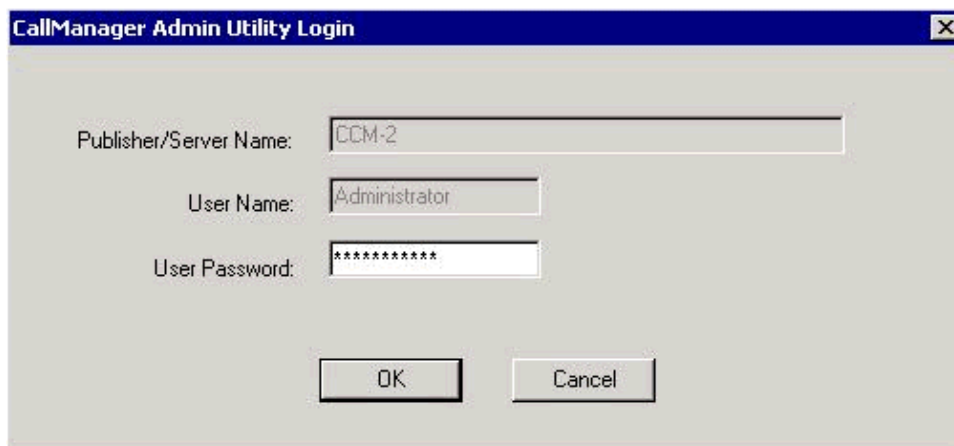
Use the Admin Utility to synchronize all the core service passwords throughout the Cluster in Cisco CallManager version 3.3 and 4.0.

Due to the complexity of Cisco CallManager interoperability relationships, administrators and installers should not manually change any Cisco CallManager passwords or services. If you decide to change these passwords, use these steps with the Cisco provided **AdminUtility.exe**:

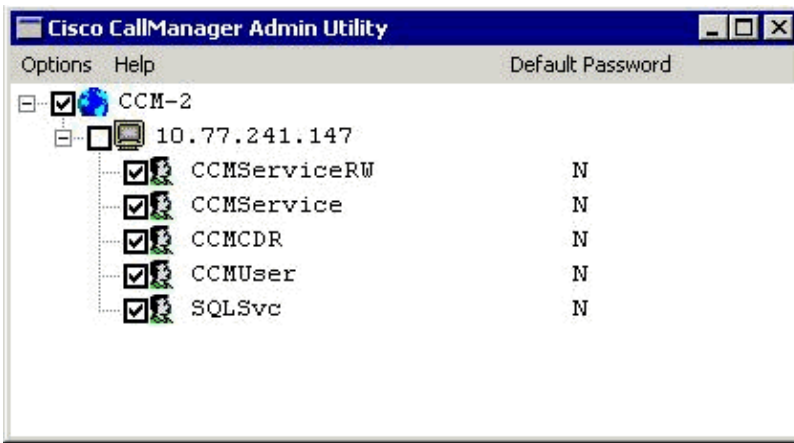
- If you need to add or replace a subscriber system after you use the **AdminUtility.exe** to change passwords from defaults, reset the passwords for all accounts and services back to the ones generated by the default system. This needs to be done before you attempt the installation. Otherwise subscriber installation fails.
- The local administrator account passwords must be identical for every Cisco CallManager system within the cluster.
- Always log on with the local administrator account to run the **AdminUtility.exe** utility.
- The **AdminUtility.exe** is located in the C:\Program Files\Cisco\Bin directory. Use the local administrator account on the publisher server to run it. The Admin Utility cannot be successfully executed on subscriber servers.

Note: As with any installation or upgrade, execute the **Admin Utility during off peak hours**. This utility changes the affected local NT account, services and virtual directories. If you choose to change all accounts on all systems within the cluster, **all call processing will be terminated** until the entire cluster is updated. Based on the number of servers within the cluster, and the call volume at the time this utility is executed, the update process could take several minutes per server.

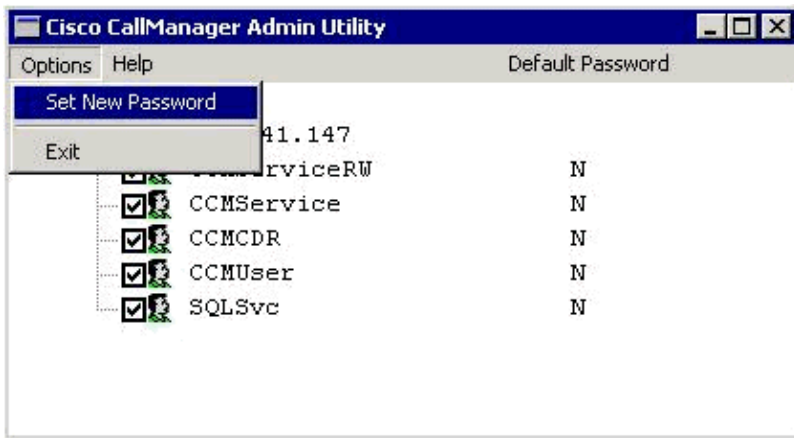
1. When you run or double-click the Admin Utility in the C:\Program Files\Cisco\Bin directory you, will be prompted for password.



2. Enter the Local Administrator password to log into the Admin Utility, and click **OK**.



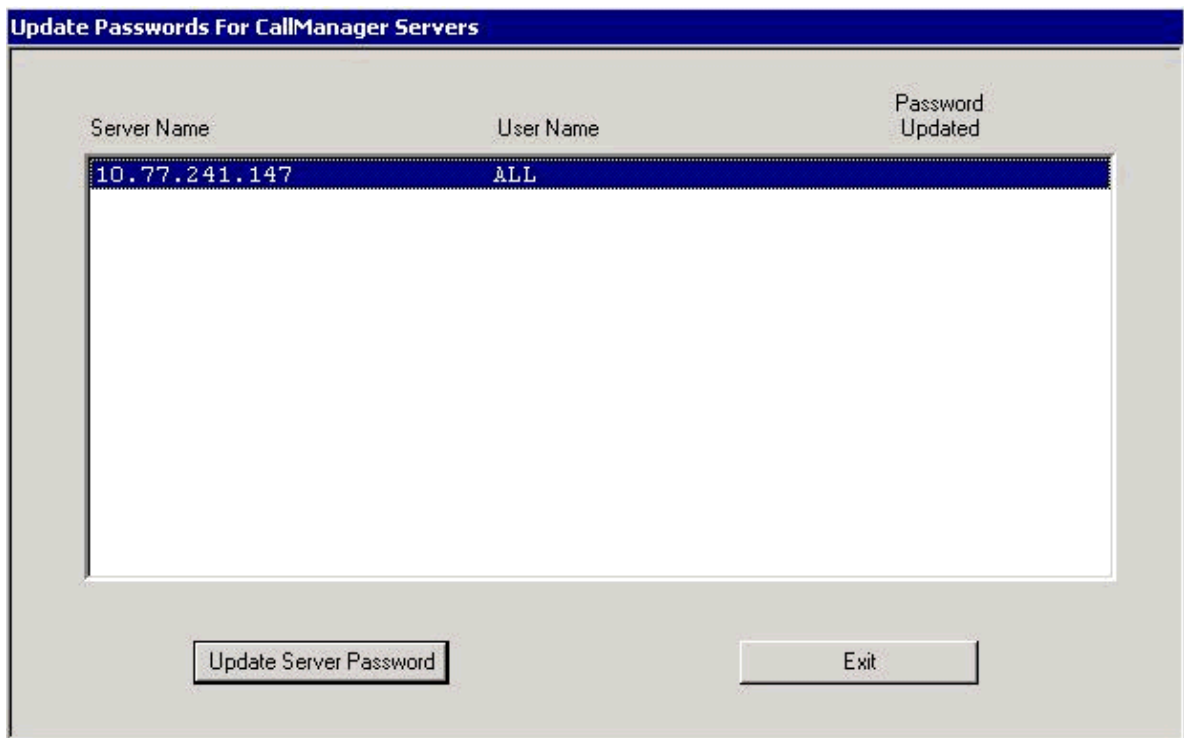
3. Select the DNS name of the cluster, which is, "CCM-2" in this case. To do so, click the check box.



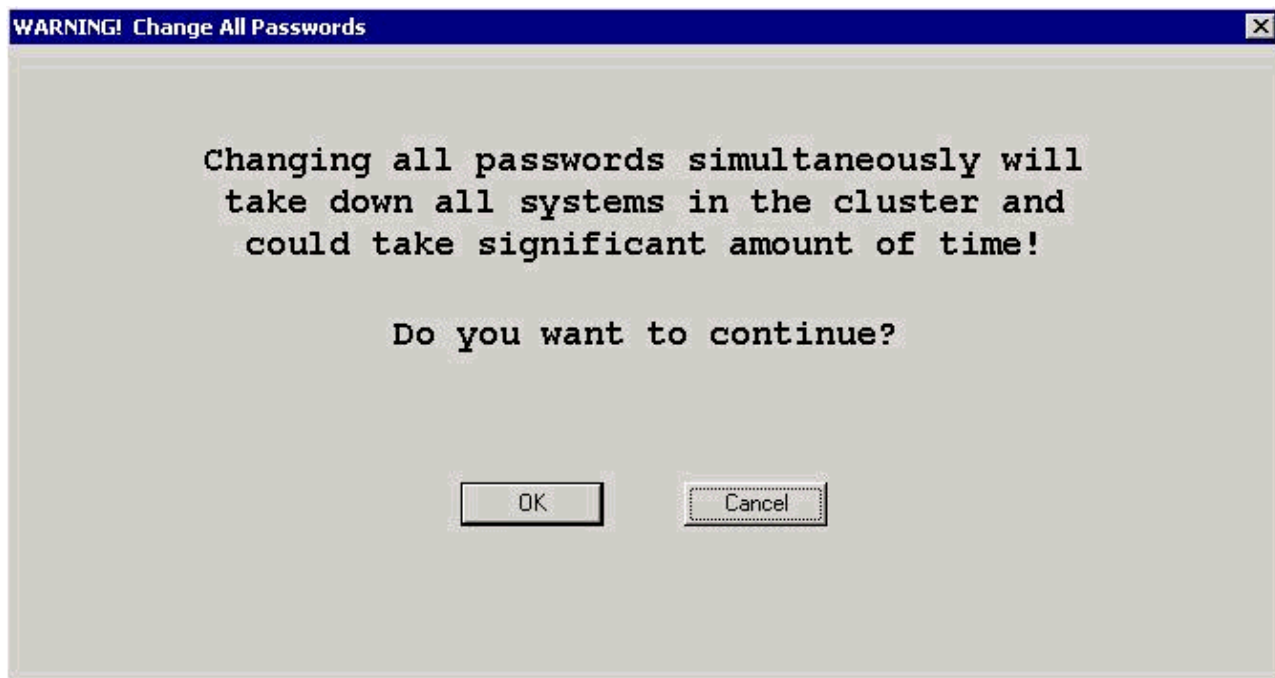
4. Select **Options** from the menu, and **Set New Password**.

Note: The Admin Utility used in CCM 3.3 and 4.0 is different. You can find one more tab called **Set default Password** under **Options** when you use CCM 3.3. This tab is not available in CCM4.0.

5. Enter your alphanumeric **Password phrase** that will be used to generate the complex passwords for each local account and service. Re-enter the string in the next field for verification. Click **OK**.



6. Select all systems within the cluster, and click **Update Server Password**.



When you do so, a warning is displayed, as shown above. Ensure that you run Admin Utility in off peak hours. This is because, all call processing will be terminated until the entire cluster is updated. Then click **OK** to continue.

7. Click **Exit** when all the passwords are updated.

Some of the problems related to the Admin Utility, and their solutions are listed here:

- Admin Utility hangs when subscriber server cannot be reached. The administration utility repeats the same messages when you click **OK**.


Workaround: Open the Windows Task Manager, and end the **AdminUtility.exe** process

- When you run this utility on the publisher, you can receive this error message: "**You can only execute this utility on the Publisher**".

Workaround: To resolve this issue, perform these steps:

1. Go to the Cisco CallManager Administration page.
2. From the menu, go to **System > Server**.
3. Click on the **Publisher** within the list on the left hand list.
4. Change the Publisher **DNS/IP Address** setting from **IP Address** to **DNS name**.
5. Click **Update**.
6. Run the **AdminUtility.exe** utility again.

Related Information

- [Cisco CallManager: Detecting and Solving SQLSvc Password Problems](#)
- [Call Manager Administrative Accounts and Passwords](#)
- [Cisco CallManager System Issues](#)
- [Voice Technology Support](#)
- [Voice and IP Communications Product Support](#)
- [Troubleshooting Cisco IP Telephony](#) 
- [Technical Support – Cisco Systems](#)

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

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 14, 2005

Document ID: 20693
