

# Failure to Synchronize Directory Services in Cisco Desktop Administrator – Reset Password

Document ID: 63002

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Problem**

**Troubleshoot**

**Related Information**

---

## Introduction

This document describes one reason why the Synchronizing Directory Services fails to run in the Cisco Desktop Administrator and provides a solution in the Cisco Unified Contact Center Express environment.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Cisco Response Solutions (CRS)
- Cisco CallManager
- Microsoft Registry Editor (**regedit32**)

### Components Used

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

- Cisco CallManager version 3.x
- Cisco CRS version 3.1(3) SR2

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

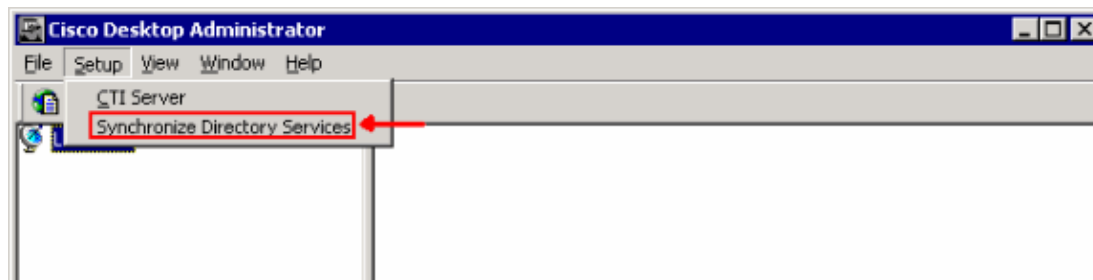
Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Problem

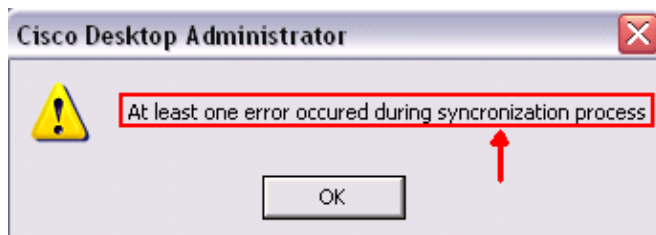
When you run the Synchronize Directory Services on Cisco Desktop Administrator, as shown in Figure 1, this error message appears, as shown in Figure 2:

At least one error occurred during synchronization process.

**Figure 1: Run Synchronize Directory Services**



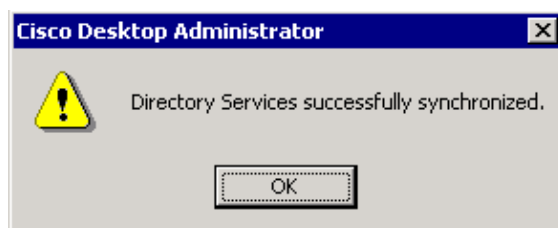
**Figure 2: Synchronize Directory Services – Failure**



If Synchronize Directory Services runs successfully, this message should appear, as shown in Figure 3:

Directory Services successfully synchronized.

**Figure 3: Synchronize Directory Services – Success**



In the related DirAccessSynSvrXXXX.log, located in the C:\Program Files\Cisco\Desktop\Directory Services\log directory and where XXXX ranges between 0001 through 9999, these messages are found:

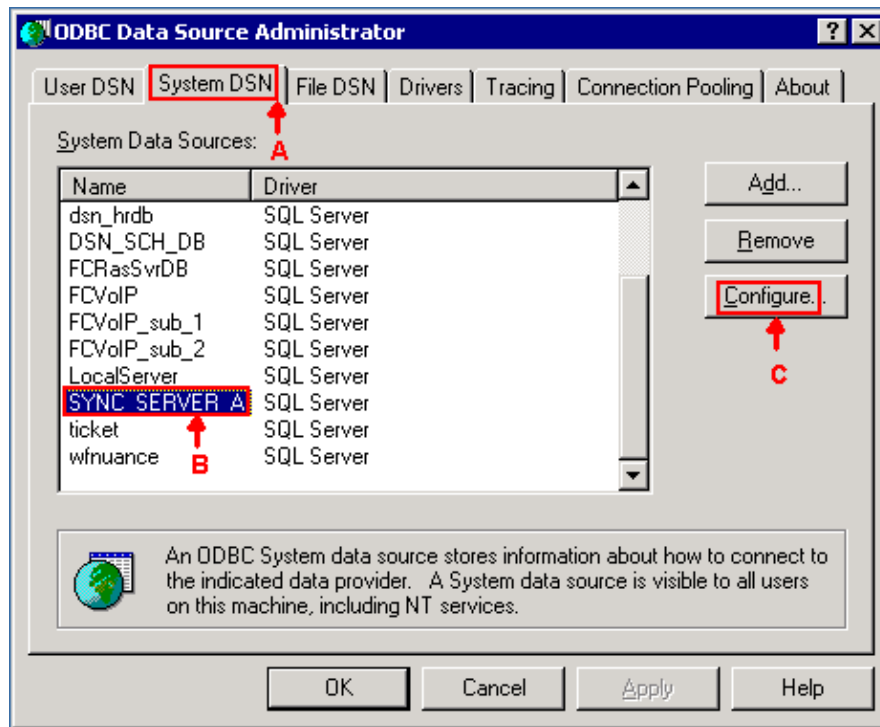
```
14:27:31 09/20/2004 INFO    DA0008  The program failed to connect to the ODBC client on the
PC - -1
14:27:59 09/20/2004 INFO    DA0008  The program failed to connect to the ODBC client on the
PC - -1
14:27:59 09/20/2004 MAJOR   DA0008  Could not connect, second try
14:27:59 09/20/2004 MAJOR   DA4533  Reset log failed
```

## Troubleshoot

In order to troubleshoot this problem, complete these steps:

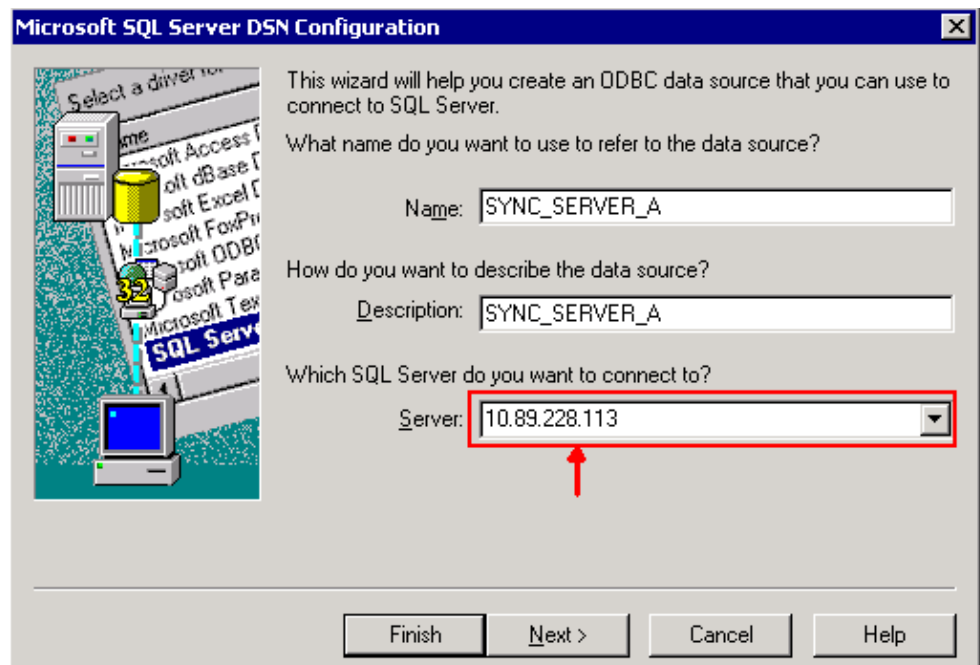
1. Verify the connection.
  - a. Choose **Start > Programs > Data Sources (ODBC)**. The ODBC Data Source Administrator window appears, as shown in Figure 4.

**Figure 4: ODBC Data Source Administrator**



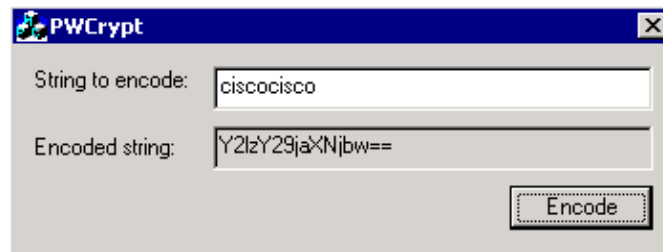
- b. Click the **System DSN** tab, see Figure 4.
- c. Choose **SYNC\_SERVER\_A** in the **System Data Sources** section, see Figure 4.
- d. Click **Configure**, see Figure 4. The Microsoft SQL Server DSN Configuration appears, as shown in Figure 5.

**Figure 5: Microsoft SQL Server DSN Configuration**



- e. Verify that the IP address for the SQL Server in the **Server** field is correct.
2. Use **pwcrypt.exe**, a password encryption tool, located in the C:\Program Files\Desktop\_Config\Util directory. In order to do this, complete these steps:
    - a. Double-click **pwcrypt.exe**. The PWCrypt box appears, as shown in Figure 6.

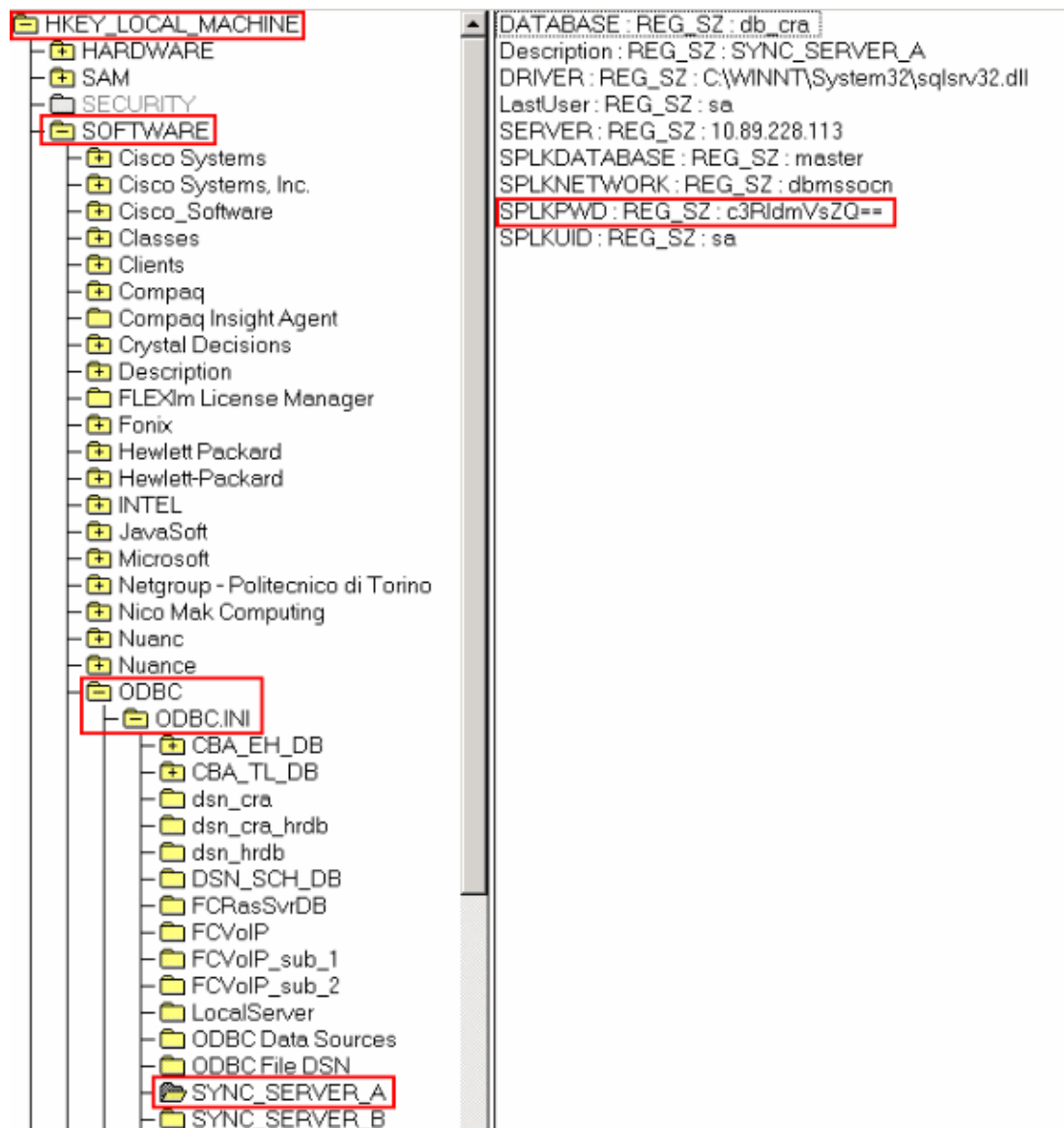
**Figure 6: PWCrypt**



- b. Enter the password in the **String to encode** field.
  - c. Click **Encode**.
  - d. An encoded string appears in the **encoded string** field.
3. Verify the encoded password in this registry key:

HKLM\SOFTWARE\ODBC\ODBC.INI\SYNC\_SERVER\_A\SPLKPWD

**Figure 7: SPLKPWD Registry Value**



4. If the results from step 2 and 3 do not match, reset the password with these steps in order to resolve the issue:
- a. Reset the system administrator (sa) password for SQL Server.
  - b. Run PWCrypt.exe with the new sa password.

- c. Replace the SPLKPWD registry value with the encoded string obtained in step 2.
5. This issue can also occur if the CCMSERVICE Password Phrase does not match between the Cisco CallManager server and the Cisco Unified Contact Center Express Server.

**Note:** When you install or upgrade Customer Response Solutions, you are prompted to enter an Account Password Phrase. Customer Response Solutions uses the string that you enter to create a unique, encrypted password for the Customer Response Solutions Administrator account and for the services that run under this account (CCMSERVICE). This password phrase must be the same on all Customer Response Solutions servers in the cluster. In order to change this password phrase after installation, use the Customer Response Solutions AdminUtility.

In order to synchronize the CCMSERVICE password phrase on both the servers, you need to use the **AdminUtility** on the Cisco CallManager server and the **Customer Response Solutions AdminUtility** on the Cisco Unified Contact Center Express server.

6. If the problem is still not resolved, restart the Cisco Desktop Sync Server service.

**Note:** If the CRS server has two NICs installed, the NIC for normal CRS traffic must be on the top of the TCP/IP bind order. The Directory Services Synchronization issue can also be due to an incorrect NIC binding order. In order to change the NIC binding order, refer to the *Background Information* section of CRA Engine Not Starting with Second NIC Installed.

---

## Related Information

- [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: Jan 26, 2006

Document ID: 63002

---