



Directory Issues

This section covers the solutions for the most common issues related to a Cisco Unified CallManager DC Directory (DCD), which uses a Lightweight Directory Access Protocol (LDAP) directory, and the Microsoft Active Directory (AD).

This section covers the following directory issues:

- [DC Directory Stability](#)
- [Application Profiles Are Not Shown for User Configuration with the DC Directory](#)
- [Add a New User Does Not Work and You Cannot Access the DC Directory Administrator](#)
- [Schema Update Fails in Active Directory if Child domain is Down](#)
- [Netscape Directory Plugin Over SSL Fails After Failure in Accessing the User Pages](#)
- [Netscape Directory Integration Using LDAP over SSL requires CA Certificate in Database](#)

If the following procedures do not solve your directory issues, contact TAC for a more detailed investigation.



Caution

Using Katakana, Cyrillic, or other double-byte character sets with DC Directory, Netscape Directory, or Active Directory can cause directory database errors. This release of Cisco Unified CallManager does not support using any double-byte character set with any directory.

For IP phone directory issues, refer to the following URL for detailed information:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

Replication Issues

For replication issues, see [Chapter 3, “Cisco Unified CallManager System Issues,”](#) and the [“Replication Fails Between the Publisher and the Subscriber”](#) section on page 3-33.

DC Directory Stability

The [DCD Instability](#) procedure is valid for Cisco Unified CallManager servers running versions 4.0(1) and later.

DCD Instability

Symptom

The following issues relate to the instability of the DCD:

- Cisco Unified CallManager publisher server has correct user data and one or more Cisco Unified CallManager subscriber servers either do not have user data or the user data is out of date with the Publisher's database.
- DC Directory Service on the Cisco Unified CallManager publisher server takes a long time to start-up (appears to stall/hang on startup).
- DC Directory Replication errors are logged to the Cisco Unified CallManager publisher and/or subscriber server(s) in the Application Event Viewer.

Possible Cause

Examination of C:\dcdsrv\run\dcx500\dcx500.out shows duplicate and/or invalid replication agreements.

The presence of invalid replication agreements causes the DC Directory database (files in C:\dcdsrv\run\dcx500\database) to grow extremely large (more than 100 MB), which results in the DC Directory taking much time to shut down and start up.

These duplicate and invalid agreements are caused by one of the following:

- The customer reinstalling the Cisco Customer Response Solutions (CRS) server (or a Cisco Unified CallManager subscriber) one or more times (each reinstall of CRS server/Cisco Unified CallManager server will cause the publisher to have a new replication agreement to the subscriber).
- Decommissioning an existing CRS server (or a Cisco Unified CallManager subscriber) without performing the DC Directory reconfiguration procedure in the Cisco Unified CallManager cluster.



Note

When removing a directory node from a Cisco Unified CallManager cluster, the DC Directory replication agreements to the removed subscriber are not automatically cleaned up.

- Manually running the **avvid_scfg** command on the subscriber more than once (for instance, a partial DC Directory reconfiguration procedure was attempted).



Note

Never perform a partial DC Directory reconfiguration procedure, (for example, run **avvid_scfg** without a preceding **cleandsa** on the publisher and the CRS server and/or Cisco Unified CallManager subscriber).

The root cause of the database growing to such large sizes is that DC Directory tries to save the state for each and every replication operation that it fails to perform. Over time, this saved state information for the invalid replication agreements causes the database to grow to several hundred MBs.

DcDirectory replication should not be confused with SQLServer replication. They are two completely independent processes.

If you perform a reinstallation of a Cisco Unified CallManager subscriber, you must perform the DC Directory reconfiguration procedure on all of the nodes in the cluster, including the standalone CRS servers, starting with the DC Directory publisher.

Recommended Action

While performing these tasks, it is required to be either directly at the console of the Media Convergence Server (MCS) servers, connected through a Keyboard/Video/Mouse (KVM) switch, or connected via Telnet to the servers. Performing these specific tasks while connected through a Terminal Services Client connection has not been fully tested and may produce unexpected results.



Note Cisco recommends that you schedule downtime to run the procedure.

Reconfiguration

There are two possible scenarios when you go to reconfigure your DC Directory after installation.

- The DC Directory database is larger than 100 Mb.
- The DCD database is less than 100 Mb.

Both procedures follow:

Reconfiguring DC Directory on Cisco Unified CallManager Publisher (database more than 100 Mb)

These steps ensure that your user data in DC Directory on the publisher Cisco Unified CallManager server is backed up in case of a failure during these steps or otherwise when the DC Directory database is larger than 100 Mb (C:\dcdsrvr\run\dcx500\database).

1. Backup your current directory information by either using the MCS backup utility or running the **dcbkdb /y backup C:\dcdsrvr\backup** command from a DOS command prompt.



Note The C:\dcdsrvr\backup folder must exist prior to running the preceding command.

2. On the Publisher server, while logged in as the Administrator, open a command prompt by selecting **Start > Run** and entering **cmd**.
3. Type the command **avvid_migrate_save.cmd** *<servername><password>* and press any key when prompted.

The output of this command will look similar to the following:

```
C:\>avvid_migrate_save jayas-w2k ciscocisco
A subdirectory or file C:\dcdsrrv\log already exists.
```

```
*****
*
* -- CISCO User Preferences Support -- *
*
*****
```

```
A subdirectory or file C:\dcdsrrv\suspense already exists.
```

```
Run the perl script avvid_migrate_save.pl
A subdirectory or file C:\dcdsrrv\log already exists.
A subdirectory or file
C:\dcdsrrv\run\DCX500\config\Migration-Backup already
exists.
Saving User Information...
Saving Profile Information...
Saving Apps20 Information...
Saving Admin Information...
Saving PA node Information...
Saving E911 node Information...
Saving systemProfile...
Saving MITRA data...
Saving Groups data...
```

```
C:\>
```

4. Stop the DC Directory service by entering **net stop dcdirectory** from the command prompt.
5. Run **cleandsa.cmd** or run **deletedib.cmd** if cleandsa.cmd reports that it is not supported.
6. Run **avvid_migrate_cfg** "*<password>*")
7. Run **avvid_migrate_restore** *<Server Name> <Directory Manager Password>*

8. Run **reconfig_cluster** <*Directory Manager Password*>

This command establishes replication agreements to all Cisco Unified CallManager subscribers; there is no need to perform any tasks on any of the Cisco Unified CallManager subscribers.

Reconfiguring DC Directory on Cisco Unified CallManager Publisher (database less than 100 Mb)

Use the following procedure to reconfigure DC Directory in the Cisco Unified CallManager publisher when the DCD database is less than 100 Mb (C:\dcdsrvr\run\dcx500\database).

1. Run **reconfig_cluster.cmd**.
2. This command establishes replication agreements to all Cisco Unified CallManager subscriber servers; no additional steps need to be performed on any of the Cisco Unified CallManager subscribers.



Note

If the network has a single Cisco Unified CallManager server with or without a co-located CRS server, run the **reconfig_cluster.cmd** command. In this case, do not perform any steps for the Cisco CRS server.

Application Profiles Are Not Shown for User Configuration with the DC Directory

Symptom

When you are adding a user to the directory, the Application Profiles (such as AutoAttendant, Softphone, and Extension Mobility) do not display, and a user cannot be linked to those profiles.

Possible Cause

The Application Profiles were configured incorrectly.

Recommended Action

Use the following procedure to configure the application profile, so you can add or view users in the DC Directory.

1. Connect to the **DC Directory Administrator**.
2. Choose **Directory > cisco.com > CCN**.
3. Click **systemProfile**.
4. Right-click **systemProfile** and choose **Properties**.
5. Click the **Application Install Status** tab.
6. Check the values for the applications. If the values for “AA Installed,” “Softphone Installed,” “ASR Installed,” and “Hotelling Installed” are blank, go to 7.

Otherwise, proceed to 11.

7. Choose **Modify**.
8. Change the values from true to **false** and those that are false to **true**.
9. Click **Apply**.
10. Click **OK**.
11. Repeat 4. and 5.
12. Click **Modify**.
13. All values should be visible.
14. Change the value of the installed applications to **true**.
15. Click **Apply**.
16. Click **OK**.
17. Click **Services**.

18. In the right panel, choose **World Wide Web Publishing Service**.
 19. Click the **Restart Service** icon.
 20. Repeat all steps for all servers in the cluster in which you experienced the problem.
-

Verification

The Application Profiles display in the DC Directory.

Add a New User Does Not Work and You Cannot Access the DC Directory Administrator

Symptom

You cannot add a user from Cisco Unified CallManager Administration. Also, cannot log in to the DC Directory Administrator.

Adding a new user returns the following error.

Error Message Sorry your session object has timed out. Click here to Begin a New search.

Searching for a new user results in the page refreshing and waiting for input.

Possible Cause

The Directory Manager user password contains special characters, such as “^”.

Recommended Action

Use the following procedure to change the DC Directory password to one that does not contain special characters.



Note

You must have superuser account privileges before you can change the DC Directory Manager password.



Note When you have a publisher server and one or more subscriber servers in a cluster, you must perform the steps in the following procedures on all Cisco Unified CallManagers within the cluster.

1. From Cisco Unified CallManager Administration, choose **Start > Programs > DC Directory Administrator**.
2. Click **Next**.
3. In the Password field, enter the default password, **cisco**, and click **Finish**.
The DC Directory Administrator window displays.
4. From the Tools menu, choose **Change Password**.
The Change User Password window appears.
5. In the Old Value field, enter **cisco**.
6. In the New Value field, enter a new *password*, without special characters.
7. In the Confirm New Value field, reenter your new *password*.
8. Click **OK**.
The DC Directory password is changed.
9. Continue with “Configuring the Windows Registry.”

Cisco Unified CallManager Administration also uses the Directory Manager account to perform add, remove, or update operations on the DC Directory LDAP server.

Configuring the Windows Registry

Use the following procedure to update the information that is stored in the registry to ensure that the registry is pointing to the correct directory.

1. Open a command line and enter **c:\dcdsrvr\bin**.
2. Enter the passwordutils.exe password.
`passwordutils.exe password`
3. Press **Enter**.

You need the Encrypted Password value information for the registry.

4. Choose **Start > Run**.
5. In the Open field, enter **regedit**.
The Registry Editor window displays.
6. Go to My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Directory Configuration.
LDAPURL must point to the correct directory.
`ldap://host:port`
7. Double-click **DCDMGRPW**.
The Edit String window appears.
8. In the Value Data field, enter the Encrypted Password value that you obtained in step 3.
9. Click **OK**.
10. From the Registry Editor window, double-click **MGRPW**.
The Edit String window appears.
11. In the Value Data field, enter the Encrypted Password value that you obtained in step 3.
12. Click **OK**.
You have successfully changed the password in the registry.



Note After changing the registry entries, you must restart the WWW and IIS services on the Cisco Unified CallManager node to pick up the latest settings from the registry.

13. Choose **Control Panel > Administrative Tools**.
14. Double-click **Services**.
The Services window displays.
15. Choose **Worldwide Web Publishing Service**.
16. Click **Stop**.
17. Click **Start**.
18. Choose **DC Directory Server**.

19. Click **Stop**.
20. Click **Start**.

If you are using Cisco Customer Response Solutions (CRS), Cisco Cisco Unified Contact Center Express 3.5(x), or Cisco Unified CallManager Auto-Attendant 3.5(x), go to the

“Reconfiguring Directory Manager Password for CRS and Extended Services” procedure that follows.

Reconfiguring Directory Manager Password for CRS and Extended Services

Use the following procedure to update the Directory Manager password.

1. Make a copy of the encrypted password used in the previous "Configuring the Windows Registry" procedure.
2. At the CRS server, open a CMD prompt, and change directory to `c:\winnt\system32\ccn` subdirectory
3. Type `'dir'`<Enter> to list the contents of the directory. You should find a file named `'ccndir.ini'`. Type `'copy ccndir.ini ccndir.ini.oldpass'`<Enter> to make a backup of this file.
4. Type `'notepad ccndir.ini'`<Enter> to open and edit the `ccndir.ini` file. Locate the line reading `'MGRPW'`. Look across this line, and replace the encrypted string inside the quotation marks, with the encrypted password recorded in Step 1.
5. Close and save the `ccndir.ini` file.
6. At the CRS server, open and log in to the Application Administration page. From the menus, select System, Engine. Stop and start the engine, and verify all Subsystems are `IN_SERVICE`.

Verification

To verify that you successfully changed the Cisco Unified CallManager DC Directory Manager password, use the following procedure.

1. From Cisco Unified CallManager Administration, choose **User > Global Directory**.

The User Information window appears.

2. Click **Search**.
3. If you can view the users that are configured in the system, the configuration was successful.

If you cannot view the users that are configured in the system, verify the following information:

- The new password is effective: Log in to the DC Directory with the new password.
- The encrypted password was entered correctly into the registry.
- The directory is pointing to the correct directory and not another directory (such as AD or an old directory which could be empty).
- The Worldwide Web Publishing and DC Directory services are restarted and running after the restart.

Schema Update Fails in Active Directory if Child domain is Down

Symptom Schema update fails in the two-domain Active Directory Forest setup with one child domain down.

Possible Cause A child domain may have been disconnected from the network.

Recommended Action When integrating Cisco Unified CallManager with an Active Directory Forest, all the domains must be connected to the network. The Schema Master server must have access to all the domains in order for the schema update to be replicated across the forest.

Netscape Directory Plugin Over SSL Fails After Failure in Accessing the User Pages

Symptom If the plugin to integrate Netscape Directory is run with an invalid SSL certificate, the user pages cannot be displayed.

Possible Cause The plugin to integrate Netscape Directory is run with an invalid SSL certificate. For example, the ND server has a Subordinate Certification Authority Certificate when it should have a WebServer Certificate.

Recommended Action Restart the Netscape Directory Service on the Netscape Directory machine. Then, run the plugin again to integrate Cisco Unified CallManager with the Netscape Directory with a valid certificate.

Netscape Directory Integration Using LDAP over SSL requires CA Certificate in Database

Symptom User Pages cannot be accessed with Netscape Directory integration over SSL.

Possible Cause The CA certificate is not present in the certificate database.

Recommended Action Copy the CA certificate to the certificate database and then run the plugin . If the Cisco Unified CallManager (LDAP client) cannot determine who signed the Netscape Directory Server (LDAP Server) certificate, the connection to the Netscape Directory Server fails because the LDAP Client has no means of trusting the authenticity of the certificate.

