



Data Migration Assistant User Guide **Release 6.0(1)**

This document describes the Data Migration Assistant (DMA), explains how to install and use it, and provides related information.

Use this document if you are running Cisco Unified Communications Manager versions 4.1(x) or 4.2(x) and are ready to upgrade to Cisco Unified Communications Manager 6.0(1).

This document includes the following topics:

- [Overview of DMA](#)
- [Obtaining DMA](#)
- [Installing DMA](#)
- [Removing DMA](#)
- [Before You Begin](#)
- [Running DMA](#)
- [DMA Backup Information File](#)
- [Administering and Troubleshooting DMA](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)

Overview of DMA

DMA migrates data for Cisco Unified Communications Manager and Cisco Emergency Responder, as specified in the following sections.

DMA assists you with the first step in migrating Cisco Unified Communications Manager data from versions 4.1(x) and 4.2(x) to Cisco Unified Communications Manager 6.0(1) by backing up this data in a format that Cisco Unified Communications Manager 6.0(1) can read. Cisco Unified Communications Manager 4.2(x) and older versions runs in a Windows environment, and Cisco Unified Communications Manager 6.0(1) runs in a Linux environment, so DMA exports Windows-based data to a format that Linux can import. The Cisco Unified Communications Manager 6.0(1) installation process converts the backed up data as needed for Cisco Unified Communications Manager 6.0(1), which completes the data migration.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

DMA saves the data that it exports in a tape archive (TAR) file in a location that you specify.

You must install and run DMA on the Cisco Unified Communications Manager publisher server before you upgrade to Cisco Unified Communications Manager 6.0(1). If you make any configuration changes after running DMA, the system does not retain these changes when you upgrade.

In addition to exporting Cisco Unified Communications Manager data, DMA exports data for these related applications:

- Cisco Unified Communications Manager Attendant Console (AC)
- Cisco Extension Mobility (EM)
- Cisco Unified Communications Manager CDR Analysis and Reporting (CAR)
- Certificate Authority Proxy Function (CAPF)
- Certificate Trust List (CTL)
- International Dial Plan (IDP)

DMA does not export this information:

- Custom Music on Hold (MOH) files—You must reapply these files after you upgrade to Cisco Unified Communications Manager 6.0(1).
- TFTP phone load files—You must reapply these files after you upgrade to Cisco Unified Communications Manager 6.0(1).
- Files on Cisco Unified Communications Manager subscriber servers—Subscriber servers obtain required information from the publisher server as part of the Cisco Unified Communications Manager upgrade process.

DMA also exports data for upgrading Cisco Emergency Responder 1.3. For more information, refer to *Cisco Emergency Responder Administration Guide*.

Obtaining DMA

If you do not have DMA software on a disk, perform the following steps to download it to the Cisco Unified Communications Manager publisher server. Only a registered user of Cisco.com can download this software.

Procedure

-
- Step 1** Go to this URL:
<http://cco/cgi-bin/tablebuild.pl/cmva-3des>
 - Step 2** Select DMA file.
 - Step 3** Follow the prompts and provide the required information to download the software.
-

Installing DMA

This section provides detailed installation information and instructions for DMA. It includes the following topics:

- [Preinstallation Guidelines and Procedures, page 3](#)—Review this information before you install DMA.
- [DMA Installation Procedure, page 3](#)—Follow these steps to install DMA.

Preinstallation Guidelines and Procedures

Review the following guidelines and perform the appropriate procedures before you install DMA:

- Ensure that one of the supported products is installed on the server before you install DMA on that server:
 - A supported release of Cisco Unified Communications Manager is installed and configured as the publisher server.: 4.1(x) and 4.2(x)
 - Cisco Emergency Responder 1.3.



Note DMA installation wizard checks for the presence of a supported product. You cannot install DMA unless a supported product has been previously installed on the server.

- Do not use Terminal Services to install DMA.
- You can use Virtual Network Computing (VNC) to install DMA. For more information about VNC, refer to the latest version of *Using Virtual Network Computing*, which is available at this URL:
http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_installation_guide09186a0080799db7.html
- DMA requires 4 GB of free disk space on the C:\ drive and 5 KB of free disk space on the D:\ drive of the Cisco Unified Communications Manager server.
- Disable the Cisco Security Agent for Cisco Unified Communications Manager, if it is enabled.



Note In some cases, you may have to uninstall Cisco Security Agent for Cisco Unified Communications Manager before you can run DMA. If you have difficulties, contact Cisco support for more information.

Make sure to enable the CSA after you complete the installation.

For instructions on disabling and enabling the CSA, refer to *Installing Cisco Security Agent for Cisco Unified Communications Manager*.

DMA Installation Procedure

To install DMA, perform the following steps.

This procedure should take about 20 minutes to complete.


Before you install DMA, make sure to review the information in the [“Preinstallation Guidelines and Procedures”](#) section on page 3.



Note

If you have an earlier version of DMA installed, you must remove it before you can install another version. See the [“Removing DMA”](#) section on page 4 for more information.

Procedure

-
- Step 1** Log in to the server as the Windows Administrator.
- Step 2** Take one of these actions:
- If you have a DMA installation disk, insert the disk.
 - If you have downloaded DMA, go to the folder in which you saved the DMA installation file and double-click the file.
- The DMA Welcome window displays.
- Step 3** In DMA Welcome window, click **Next**.
- The License Window displays.
- Step 4** Accept the license agreement and click **Next**. The Informix Password window displays.
- Step 5** Enter a password for the Informix Database Server (IDS) in the **Informix Password** text box.
- The password must contain 8-14 characters, including at least one of each of the following character types:
- Upper case letter (A-Z)
 - Lower case letter (a-z)
 - Numeral (0-9)
 - Special character ({ } , . < > : ? / | \ ` ~ ! @ \$ ^ & * () _ - +)
-
-  **Caution** Do not change the Informix password after installing DMA. Changing the password will cause DMA backups to fail.
-
- Step 6** Enter the password again in the **Confirm Password** text box.
- The Ready to Install the Program window displays.
- Step 7** In the Ready to Install window, click **Install**.
- The installation begins. The Installing Data Migration Assistant window shows you the status as the installation proceeds.
- After about 20 minutes, the InstallShield Wizard Completed window displays.
- Step 8** In the InstallShield Wizard Completed window, click **Finish**.
- You are prompted to restart the server.
- Step 9** To restart the server, click **Yes**.
- The server restarts, and DMA installation completes.
-

Removing DMA

You must remove DMA and the applications that are installed with it before installing another DMA version. See the following sections for instructions:

- [“Uninstalling DMA” task on page 5](#)

- [“Removing Informix Dynamic Server” task on page 5](#)
- [“Uninstalling Informix Client SDK” task on page 6](#)

Uninstalling DMA

To uninstall DMA, follow these steps:

Procedure

-
- Step 1** Choose **Start > Settings > Control Panel > Add/Remove Programs**.
- Step 2** From the Add/Remove Programs Window, choose **Cisco Data Migration Assistant**.
- Step 3** Click **Remove**.
- Step 4** Reboot the system.
-

Removing Informix Dynamic Server

To remove Informix Dynamic Server (IDS), follow these steps:

-
- Step 1** Uninstall the IDS application:
- Choose **Start > Settings > Control Panel > Add/Remove Programs**.
 - From the Add/Remove Programs Window, choose **IDS (Informix Dynamic Server)**.
 - Click **Remove**. The Uninstall Informix Dynamic Server dialog box displays.
 - Choose the uninstallation method **Remove all database server files and all database information**, then choose **OK**. The Delete User Account dialog box displays.
 - To delete the informix user account, choose **Yes**. You are asked whether to remove Informix Storage Manager (ISM) servers.
 - To remove Informix Storage Manager (ISM) servers, choose **Yes**. You are asked whether to remove SNMP extension agents.
 - To remove SNMP extension agents, choose **Yes**.
- Step 2** Delete the following folders from the hard drive:
- C:\informix
 - C:\ifmxdata
 - C:\ciscoverbs\dma\bin\IIF
 - C:\tmp
 - C:\preferences
 - C:\DMAROOT
 - C:\Program Files\Cisco\Trace\DMA
 - C:\Program Files\Cisco\Trace\DBL\installldb*
 - C:\Program Files\Cisco\Trace\DBL\dbl_INSTALLLDB*

Step 3 Reboot the system.

Uninstalling Informix Client SDK

To remove Informix Client SDK, follow these steps:

- Step 1** Choose **Start > Settings > Control Panel > Add/Remove Programs**.
- Step 2** From the Add/Remove Programs Window, choose **IBM Informix Client-SDK**.
- Step 3** Click **Remove**. The Uninstall IBM Informix Client-SDK dialog box displays.
- Step 4** To remove the IBM Informix Client-SDK, click **Yes**.
- Step 5** Reboot the system.

Before You Begin

Before you start DMA, perform the procedures that are shown in [Table 1](#).

Table 1 Procedures to Follow Before Running DMA

Procedure	Reference
Use the Cisco Unified Communications Manager Backup and Restore Utility (BARS) to back up your data. You can use the BARS backup to fall back to your current software version, if necessary.	Refer to the appropriate version of <i>Backup and Restore Utility Administration Guide</i> and related documentation at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco recommends that you use the Cisco Unified Communications Manager Upgrade Utility to verify that your system is in a good state before the upgrade	Refer to the appropriate version of <i>Using Cisco Unified Communications Manager Upgrade Utility</i> at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
To back up CAR data, ensure the CAR plug-in is installed on the publisher server	See the “Migrating CAR Data” section on page 7.
If you use Cisco Unified Communications Manager Attendant Console, ensure the required files exist on the publisher server.	See the “Migrating Cisco Unified Communications Manager Attendant Console Data” section on page 7.
Copy CAPF data from the subscriber servers to the publisher server.	See the “Migrating Existing CAPF 1.0(1) Data” section on page 7.
Ensure that DMA will work correctly if Cisco Security Agent is installed on the server.	See the “Ensuring DMA Compatibility with Cisco Security Agent for Cisco Unified Communications Manager” section on page 9.

Table 1 **Procedures to Follow Before Running DMA (continued)**

Procedure	Reference
If you are running DMA on a Cisco Emergency Responder system, create the following file and move all subscriber data to be backed up into it: C:\Program Files\Cisco Systems\CiscoER\Subscriber_backup	For more information, refer to the appropriate version of <i>Cisco Emergency Responder Administration Guide</i> .
Obtain licenses for Cisco Unified Communications Manager 6.0 before upgrading to this release. You must import your new licenses after upgrading to Cisco Unified Communications Manager 6.0 to enable the system.	Refer to <i>Cisco Unified Communications Manager Administration Guide</i> for information about licensing and obtaining licenses.

Migrating CAR Data

Before you can back up Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) data, you must ensure that the CAR plug-in is installed on the publisher server. If the CAR plug-in is not installed, navigate to **Application>Install Plugins** and install the CAR plug-in. For more information, see the *Cisco Unified Communications Manager Administration Guide* or the *Cisco Unified Serviceability Administration Guide*.



Note

If you do not need to carry over your CDR records to Cisco Unified Communications Manager 6.0(1), Cisco recommends that you purge the CDR records before you run DMA.

Migrating Cisco Unified Communications Manager Attendant Console Data

If you use Cisco Unified Communications Manager Attendant Console, make sure that the following files exist on the publisher server before you run DMA. If the files do not exist on the publisher server, copy them to the publisher server from the subscriber server before you run DMA.

- C:\Program Files\Cisco\Communications ManagerAttendant\etc\acserver.properties
- C:\Program Files\Cisco\Communications ManagerAttendant\etc\DialRules.xml

DMA backs up the file CorporateDirectory.txt if it exists in the following location on the server:
C:\Program Files\Cisco\Communications ManagerAttendant\UserLists\CorporateDirectory.txt.

Migrating Existing CAPF 1.0(1) Data



Caution

Failing to perform the tasks that are described in this section may cause a loss of CAPF data. Use the following information in conjunction with the [“Copying CAPF 1.0\(1\) Data from a 4.x Subscriber Server to the 4.x Publisher Database Server”](#) section on page 8.

For information on using CAPF with Cisco Unified Communications Manager 6.0(1), refer to the *Cisco Unified Communications Manager Security Guide*.

Review the following details before you upgrade to Cisco Unified Communications Manager 6.0(1):

- Upgrades from Cisco Unified Communications Manager (formerly Cisco Unified CallManager) 4.0 where CAPF was installed on the Cisco Unified Communications Manager 4.0 publisher database server—If you performed certificate operations with Cisco Unified Communications Manager 4.0 and CAPF 1.0(1) ran on the publisher database server, the latest operation status migrates to the Cisco Unified Communications Manager 4.1 database.
- Upgrades from Cisco Unified Communications Manager where CAPF was installed on a Cisco Unified Communications Manager 4.0 subscriber server—If you performed certificate operations with Cisco Unified Communications Manager 4.0 and CAPF 1.0(1) ran on a subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade to Cisco Unified Communications Manager 6.0(1).

**Caution**

If you fail to copy the data prior to the Cisco Unified Communications Manager 6.0(1) upgrade, the CAPF data on the Cisco Unified Communications Manager 4.x subscriber server does not migrate to the Cisco Unified Communications Manager 6.0(1) database, and a loss of data may occur. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones, but CAPF 6.0(1) must reissue the certificates, which are no longer valid.

- Upgrades from Cisco Unified Communications Manager release 4.1 and later to Cisco Unified Communications Manager 6.0(1)—The upgrade automatically migrates the CAPF data.

Copying CAPF 1.0(1) Data from a 4.x Subscriber Server to the 4.x Publisher Database Server

**Caution**

If you installed CAPF utility 1.0(1) on a Cisco Unified Communications Manager 4.x subscriber server, you must copy the CAPF data to the 4.x publisher database server before you upgrade to Cisco Unified Communications Manager 6.0(1). Failing to perform this task causes a loss of CAPF data; for example, you may lose the phone record files in C:\Program Files\Cisco\CAPF\CAPF.phone. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones, but CAPF 6.0(1) must reissue the certificates because the certificates are not valid.

Use the following procedure in conjunction with the [“Migrating Existing CAPF 1.0\(1\) Data”](#) section on [page 7](#). To copy the files, perform the following procedure:

Procedure

- Step 1** Copy the files in [Table 2](#) from the machine where CAPF 1.0 is installed to the publisher database server where Cisco Unified Communications Manager 4.x is installed:

Table 2 Copy from Server to Server

Files to Copy	From Machine Where CAPF 1.0 Is Installed	To Publisher Database Server Where Cisco Unified Communications Manager 4.x Is Installed
*.0	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\Certificates
CAPF.phone	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\CAPF
CAPF.config files	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\CAPF

Step 2 Upgrade every server in the cluster to Cisco Unified Communications Manager 6.0(1).

Step 3 After you upgrade the cluster to Cisco Unified Communications Manager 6.0(1), perform the following tasks before you use the phones:

- a. Delete the existing Cisco CTL client.
- b. Install the latest Cisco CTL client by choosing **Application->Plugins** in Cisco Unified Communications Manager Administration.
- c. Configure the client to create or update the CTL file.



Tip For information on installing and configuring the Cisco CTL client, refer to the *Cisco Unified Communications Manager Security Guide*.

The Cisco CTL client copies the CAPF certificate to all the servers in the cluster.

Step 4 Uninstall the CAPF utility that you used with Cisco Unified Communications Manager 4.x.

Step 5 See the [“Generating a New CAPF Certificate” section on page 9](#).

Generating a New CAPF Certificate

If you need to regenerate the CAPF certificate, use the Cisco Unified Communications Manager Certificate Management features. For instructions and more information, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Ensuring DMA Compatibility with Cisco Security Agent for Cisco Unified Communications Manager

Cisco Security Agent for Cisco Unified Communications Manager will cause DMA backup to fail in some cases. In some of these cases, DMA automatically disables Cisco Security Agent for Cisco Unified Communications Manager during the backup. In other cases, you must manually disable the Cisco Security Agent for Cisco Unified Communications Manager service prior to running the DMA backup, or the backup will fail.

For instructions on disabling and enabling the CSA, refer to *Installing Cisco Security Agent for Cisco Unified Communications Manager*.

If you manually disable Cisco Security Agent for Cisco Unified Communications Manager, remember to enable it after the DMA backup finishes.

**Note**

In some cases, you may have to uninstall Cisco Security Agent for Cisco Unified Communications Manager before you can run DMA. If you have difficulties, contact Cisco support for more information.

The following rules apply to the interaction between DMA and Cisco Security Agent for Cisco Unified Communications Manager:

- For DMA versions 6.0(1) and lower:
 - Cisco Security Agent for Cisco Unified Communications Manager versions lower than 2.0(5) are automatically disabled during DMA backup.
 - Cisco Security Agent for Cisco Unified Communications Manager versions 2.0(5) and higher are not automatically disabled. You must manually disable Cisco Security Agent for Cisco Unified Communications Manager prior to DMA backup.
- For DMA versions 5.1(1) and higher:
 - Cisco Security Agent for Cisco Unified Communications Manager versions 3.0(2) and higher can remain enabled during DMA backup.
 - Cisco Security Agent for Cisco Unified Communications Manager versions lower than 3.0(2) cannot remain enabled during DMA backup, and are not automatically disabled. You must manually disable Cisco Security Agent for Cisco Unified Communications Manager prior to DMA backup.

Running DMA

To run DMA on a Cisco Unified Communications Manager publisher server, perform the following steps.

Before you start DMA, make sure to review the information in the [“Before You Begin” section on page 6](#).

Procedure

-
- Step 1** Choose **Start > Programs > Cisco DMA > DMAAdmin**.
- Step 2** When prompted, log in as the Windows Administrator.
The Data Migration Assistant Home window displays.
- Step 3** From the Data Migration Assistant menu bar, choose **Backup > Storage Location**.
The Backup Storage Location window displays.
- Step 4** In the Backup Storage Location window
- a. Choose the destination where DMA stores the TAR file by clicking one of the following radio buttons:
 - **Network Directory**—Stores the TAR file in a network folder. Enter information in these fields:
 - Path Name—Network path to the appropriate folder
 - User Name—Username for network access
 - Password—Password for network access

- **Local Directory**—Stores the TAR file in a folder on the server on which you are running DMA. In the Path Name field, enter the path to the folder or click **Browse** to choose a folder.



Note Do not specify a mapped network directory for the Local Directory. If you do, DMA may not be able to create the destination folder.

- **Tape Device**—Stores the TAR file to a backup device. Choose an available tape device from the pulldown menu.

DMA allows you to save two TAR files in each destination directory. If you try to save a third TAR file, the older of the existing TAR files gets deleted, after the new TAR file is successfully created.

b. Click Update.

- c.** If you chose **Local Directory** as the backup storage location, click **OK** when you see this prompt:

```
Please ensure that you transfer the contents from the LOCAL path to an external device
before upgrading. The files will not be readable from the local directory during the
upgrade installation
```

Step 5 From the Data Migration Assistant menu bar, choose **Backup > Backup Now**.

The Migrate Data Source Server window displays. An estimate of the time required to perform the backup displays.

Step 6 In the Migrate Data Source Server window, click **Start Backup Now**.

The backup begins.

A status window shows you the status of the backup as it proceeds. The status window includes an estimate of the time that is required to complete the backup, both at the start of the backup and at the start of the validation phase. If you close the status window, you can display it again by clicking the **View Latest Status** link in the Migrate Data Source Server window.

The backup process can take a long time to complete. You can stop this process at any time by choosing **Start > Programs > Cisco DMA > Cancel Backup** and then clicking **Cancel Backup Now** in the Cancel Backup Process dialog box. The system could require several minutes to cancel the backup process.



Note If you close the DMA window while a backup process is running, the backup continues; however, when you restart DMA, the main window will display the **Reset Status** button. Clicking the **Reset Status** button cancels the backup process that is currently running.

When the backup completes, the status window displays the following lines:

```
Archive built successfully
Backup information file DMABackupinfo.inf saved to D:\DMA
```



Note DMA might make some minor modifications to your data to ensure that it can be successfully migrated.

Step 7 If you saved the TAR file in a local directory in [Step 4](#), copy that file to a network server or to a tape device before you upgrade.

The following format shows how the TAR file is named, where *date* and *time* indicate when the file was created:

DMABackup*date#time*.tar

You must perform this step because a TAR file on the local disk will not be accessible during the upgrade process, and the file will be deleted when the upgrade process reformats the local server disks.

Validating Backup Data

After performing a DMA backup, you can validate the data by examining the log file C:\CiscoWebs\DMA\bin\datavalidation.log. This log validates the data to ensure that it complies with your business rules.

If you find errors in this log, you can still use the DMA backup to upgrade your system. However, the faulty data will still be faulty on the upgraded system, and you will need to correct it before using it. To avoid restoring the faulty data to the upgraded system, you can correct the data using Microsoft SQL, then run DMA backup again.

You can view a log of the backup progress in the file C:\Program Files\Cisco\Trace\DMA\Progress\AllProgress.log. Additional log files are also located in that folder. For more information, see the [“Log Files” section on page 13](#).

DMA Backup Information File

DMA automatically creates a backup information file named DMABackupInfo.inf in the D:\DMA folder on the server on which you run DMA. This file contains configuration and environment data regarding the DMA software, the server on which you ran DMA, and the software for which you backed up data. The file also gets saved as part of the TAR file.

The product installation program checks for the presence of this file to determine if you are upgrading the same server or replacing the server during the upgrade. For this reason, do not do anything with the D:\DMA\DMABackupInfo.inf file.

Administering and Troubleshooting DMA

The following sections provide information that you can use to administer and troubleshoot DMA:

- [Determining DMA Software Version, page 12](#)
- [Reviewing the Results of the last DMA Backup Procedure, page 13](#)
- [Log Files, page 13](#)
- [Trace Files, page 16](#)

Determining DMA Software Version

To determine the version of DMA that is installed on a server, follow these steps:

Procedure

- Step 1** Take one of these actions to display the Data Migration Assistant window, if it does not display already:
- If DMA is running, choose **Backup > Home** from DMA menu bar.
 - If DMA is not running, choose **Start > Programs > Cisco DMA > DMAAdmin** and log in as the Windows Administrator when prompted.
- Step 2** In the Data Migration Assistant window, click the **Details** button.
-

Reviewing the Results of the last DMA Backup Procedure

To see the results of the last backup procedure that you performed with DMA, follow these steps:

Procedure

- Step 1** Choose **Start > Programs > Cisco DMA > DMAAdmin**.
- Step 2** When prompted, log in as the Windows Administrator.
- Step 3** From the Data Migration Assistant menu bar, choose **Backup > Backup Now**.
- Step 4** In the Migrate Data Source Server window, click the **View Latest Status** link.
- If you click the **View Latest Status** link during a backup procedure, the status of the current procedure displays.
-

Log Files

[Table 3](#) describes the log files that DMA creates. If necessary, you can provide log files to the Cisco Technical Assistance Center (TAC) for assistance with troubleshooting.

Table 3 DMA Log Files

File Type	Description	File Location	File Name
Installation log files	Created each time that you perform the DMA installation procedure.	C:\Program Files\ Common Files\Cisco\Logs	DMAInstall $date_time$.log, where $date_time$ specifies the date and time that the file was created DMAInstallUI.log IDSInstall.log
Backup operation log file	Created each day that you run DMA to back up data. If you run the backup procedure more than once on the same day, DMA appends information to the existing file for that day.	C:\Program Files\ Common Files\Cisco\Logs\ DMA\BACKUP	Backup $date$.log, where $date$ specifies the date that the file was created This log also displays when you click the View Latest Status link.
Database export operation log file	Created the first time that you run DMA to back up data. Each subsequent time that you run the backup procedure, DMA appends information to this file.	C:\CiscoWebs\DMA\Bin	exportdb.log These additional database export logs are located in this folder: <ul style="list-style-type: none"> • createdb.log • dropdb.log • dropdb_w.log
Directory export operation error log file	Created each time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Error.log
Directory export operation report file	Created the first time that you run DMA to back up data. Each subsequent time that you run the backup procedure, DMA appends information to this file.	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Reprt.txt
Directory export operation results file	Created each time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Result.txt
Data validation log	Contains any validation errors that are found during the verification of database and directory data during the backup process	C:\CiscoWebs\DMA\Bin	datavalidation.log

Table 3 DMA Log Files (continued)

File Type	Description	File Location	File Name
Backup progress indicator logs	Created when you run DMA. Contains a high-level log of backup and data validation progress.	C:\Program Files\Cisco\Trace\DMA\Progress	AllProgress.log If there are errors in the backup progress, the following log files are created in the same folder: <ul style="list-style-type: none"> • CSV_Import*.* • ExportDB_CCM*.* • ExportToCSVs*.* • InstallDB_Full*.*
Informix Dynamic Server (IDS) installation log	Created during DMA installation. Contains a log of the IDS installation.	C:\Program Files\Common Files\Cisco\Logs	IDSInstall.log

Common Errors

DMA can return the errors that are described in [Table 4](#), which can cause it to fail.

Table 4 DMA Errors Messages and Descriptions

Error Message	Description
Failure- Product check; Database contains models that are no longer supported in this release. AT, AS, and ICS gateways are not supported. Please remove unsupported models and repeat export.	This error displays if any of the following items are present in the device table: <ul style="list-style-type: none"> • Cisco AT-2 Gateway PRODUCT_AT2_GATEWAY • Cisco AT-4 Gateway PRODUCT_AT4_GATEWAY • Cisco AT-8 Gateway PRODUCT_AT8_GATEWAY • Cisco AS-2 Gateway PRODUCT_AS2_GATEWAY • Cisco AS-4 Gateway PRODUCT_AS4_GATEWAY • Cisco AS-8 Gateway PRODUCT_AS8_GATEWAY • All ICS platforms
Failure, Pre-SD Unified CM Migration	This error indicates that a problem occurred during the migration from Cisco Unified Communications Manager 3.x to Cisco Unified Communications Manager 4.x.

Table 4 DMA Errors Messages and Descriptions (continued)

Error Message	Description
Failure - Sony devices exist in the database, but there is no corresponding csv file. Please reinstall the Sony installation.	This error indicates that the system cannot find a CSV file for a Sony phone. Before you can continue with the migration, you must reinstall the device.
Failure - Tandberg devices exist in the database, but there is no corresponding csv file. Please reinstall the Tandberg installation.	This error indicates that the system cannot find a CSV file for a Tandberg phone. Before you can continue with the migration, you must reinstall the device.
Failure- Invalid enum 31970 in Zimbabwe Locale csv file. Zimbabwe network locale needs to be replaced with a newer version before upgrade.	The error indicates that you have an invalid version of the Zimbabwe locale file. Before you can continue with the migration, you must download a new copy of the Zimbabwe locale file from Cisco.com and install it on your system.
Failure- Zimbabwe network locale needs to be replaced with a newer version before upgrade.	The error indicates that you have an invalid version of the Zimbabwe locale file. Before you can continue with the migration, you must download a new copy of the Zimbabwe locale file from Cisco.com and install it on your system.
Failure- Tandberg.xml file is invalid and needs to be replaced before upgrade. Please reinstall Tandberg with a newer installation.	The error indicates that you have an invalid version of the Tandberg.xml file. Before you can continue with the migration, you must download a new copy of the Tandberg.xml file from Cisco.com and install it on your system.

Trace Files

[Table 5](#) describes the trace files that DMA creates. If necessary, you can provide trace files to the Cisco Technical Assistance Center (TAC) for assistance with troubleshooting.

Table 5 **DMA Trace Files**

File Type	Description	File Location	File Name
DMA operation trace file	Created each day that you run DMA to back up data. If you run the backup procedure more than once on the same day, DMA appends information to the existing file for that day	C:\Program Files\Cisco\Trace\DMA	Tracedate.log, where <i>date</i> specifies the date that the file was created or updated.
Database export operation trace file	DMA creates one file each time that it backs up Cisco Unified Communications Manager data and one file each time that it backs up CAR data.	C:\Program Files\Cisco\Trace\DBL	<ul style="list-style-type: none"> Export: installdbccm.log W1install: installdbw1.log
Directory export operation trace file	Created the first time that you run DMA to back up data. Each subsequent time that you run the backup procedure, DMA appends information to this file.	C:\CiscoWebs\DMA\DirExport\logs	DirExport_Trace.log
Database install setup trace file	Displays the Informix setup status	C:\CiscoWebs\DMA\Bin	dbcmds.log

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>. If you require further assistance please contact us by sending email to export@cisco.com.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Copyright © 2007. Cisco Systems, Inc. All rights reserved.