Data Migration Assistant User Guide Release 7.1(2)

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 supported versions of Cisco Unified CallManager and are ready to upgrade to Cisco Unified Communications Manager 7.1(1x). The DMA version number that you use must match the major version of Cisco Unified Communications Manager. [For example, if you were upgrading to Cisco Unified Communications Manager 7.0(1a), you could use DMA Release 7.0(1) or DMA Release 7.0(1a).]

Note For information on supported releases, refer to the Cisco Unified Communications Manager Software Compatibility Matrix located at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Note When you use DMA to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade and become standard end users. You must reset the CAR administrator privileges after the upgrade. Refer to the "Configuring CAR Administrators, Managers, and Users" section in the *CDR Analysis and Reporting Administration Guide* for more information on how to configure CAR administrators.

This document includes the following topics:

- Overview of DMA
- Obtaining DMA
- Installing DMA
- Removing DMA
- Before You Begin
- Running DMA

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

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 supported versions of 4.x to Cisco Unified Communications Manager 7.1(2) by exporting this data in a format that Cisco Unified Communications Manager 7.1(2) can read.

Note For information on supported releases, refer to the Cisco Unified Communications Manager Software Compatibility Matrix located at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Note When you use DMA to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade and become standard end users. You must reset the CAR administrator privileges after the upgrade. Refer to the "Configuring CAR Administrators, Managers, and Users" section in the *CDR Analysis and Reporting Administration Guide* for more information on how to configure CAR administrators.

Cisco Unified Callmanager 4.x versions run in a Windows environment, and Cisco Unified Communications Manager 7.1(2) runs in a Linux environment, so DMA exports Windows-based data to a format that Linux can import. The Cisco Unified Communications Manager 7.1(2) installation process converts the backed up data as needed for Cisco Unified Communications Manager 7.1(2), which completes the data migration. DMA also exports data for upgrading Cisco Emergency Responder 1.3. For more information, refer to *Cisco Emergency Responder Administration Guide*.

DMA saves the data that it exports in a tape archive (TAR) file in a location that you specify. DMA also generates a configuration file (platformConfig.xml) to facilitate installation of Cisco Unified Communications Manager, for both first nodes (publishers) and subsequent nodes (subscribers). DMA users enter site-specific data at DMA's Answer File Generator window during the upgrade, including domain name, IP address, primary DNS, secondary DNS, and NTP server. You may choose where to store the platformConfig.xml file when you generate it at the Answer File Generator window. You may only save this file to a local disk (or locally attached USB drive, network drive, etc.). You must move this file to a USB drive and inserted during the upgrade process. Refer to "Entering Answer File Generator Data" section on page 21 for details.

Note For information on using the configuration file during an upgrade, refer to the *Upgrade to Cisco Unified Communications Manager Release 7.1(2) from Cisco Unified Communications Manager 4.x Releases*.

Note Make sure that you copy the platformconfig.xml to the Universal Serial Bus (USB) key and apply this USB to the publisher before the upgrade.

You must install and run DMA on the Cisco Unified Communications Manager publisher server before you upgrade to Cisco Unified Communications Manager 7.1(2).

Note 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)
- Quality Reporting Tool (QRT)

  Note The last QRT report is not exported when the Cisco Extended Function service is running.

- RTMT reports

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 7.1(2).
- TFTP phone load files—You must reapply these files after you upgrade to Cisco Unified Communications Manager 7.1(2).
- 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.
- CDR data—Data Migration Assistant does not migrate CDR data except the records in the CAR database. If you generate CDRs after you have run CDR loader in CAR, DMA does not migrate those CDRs. For information on configuring the CAR load schedule before you upgrade, see the *Cisco Unified CallManager Serviceability Administration Guide* for the version of Cisco CallManager running on your system.

  Data Migration Assistant allows you to choose whether to export CAR data. If you export CAR data, Data Migration Assistant allows you to specify how much time that you want to allot for CAR migration. Refer to Selecting Custom Options, Step 5.
- Bulk Administration Tool Templates—Data Migration Assistant does not export Bulk Administration Tool templates.
- Passwords and PINs—Data Migration Assistant does not migrate passwords and PINs for users.

For Cisco Emergency Responder, DMA exports the following data from the publisher server:

- Cisco Emergency Responder database
- Call history files located in C:\Program Files\Cisco Systems\CiscoER\CallHistory
- Contents of the following directories:

- C:\Program Files\Cisco Systems\CiscoER\etc
- C:\Program Files\Cisco Systems\CiscoER\export
- C:\Program Files\Cisco Systems\CiscoER\Import
- C:\Program Files\Cisco Systems\CiscoER\nena_msag_records
- C:\Program Files\Cisco Systems\CiscoER\Subscriber_backup

The platformConfig.xml file that DMA generates supports upgrades for the publisher server as well as for the subscriber servers. DMA provides a window where you can make detailed configuration specifications. Refer to the "Entering Answer File Generator Data" section on page 21.

DMA provides a window where users can customize the behavior of DMA by specifying which types of logs to include in the output file. Refer to the "Selecting Custom Options" section on page 14.

DMA explicitly lists the pre-DMA export tasks. DMA provides both information and the automation of pre-export tasks when possible to ensure that users know which tasks they need to complete before running DMA. Refer to the "Verifying Pre-DMA Export Tasks" section on page 15.

DMA supports the generation of a license file upon successful DMA validation. Refer to "Upgrading Product Licensing" in the document *Upgrading to Cisco Unified Communications Manager Release 7.1(2)*.

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://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

Step 2 Type your Cisco.com **User Name:** and **Password:** in the text boxes, then click the **Log In** button.

Step 3 Choose **IP Telephony > Call Control > Cisco Unified Communications Manager (CallManager) > Cisco Unified Communications Manager Version 7.1**.

Step 4 Click the **Unified Communications Manager Data Migration Assistant** link.

Step 5 Browse the folders and click the **7.1(2)** link.

Step 6 If you are trying to install Data Migration Assistant for the first time, click the **For new and full installations - click here to order** link on the right side of the window.

Step 7 If you are upgrading from a previous version of Data Migration Assistant, click the **DataMigrationAssistant-7-1-2.exe** link and click the **DOWNLOAD** button. 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 5—Review this information before you install DMA.
- DMA Installation Procedure, page 7—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.

    Note For information on using the configuration file during an upgrade, refer to the *Upgrade to Cisco Unified Communications Manager Release 7.1(2) from Cisco Unified CallManager 4.x Releases*.

  Tip If you have installed an (a), (b), (c), (and so on), version of Cisco Unified Communications Manager, you only need to match the DMA major version number. For example, if you had Cisco Unified Communications Manager Release 6.1(1b), you could use DMA Release 6.1(1a).

  - 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 previously has been installed on the server.

- Ensure that the Administrator user DMA Registry Settings are correct. If Administrator user permissions are set to Everyone, DMA install fails.
- 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/customer/products/hw/voiceapp/ps378/prod_installation_guides_list.html
- Make sure that you uninstall previous versions of DMA. For detailed procedures, refer to the "Removing DMA" section on page 8.
- 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*.

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

- Before you upgrade the Cisco Unified Communications Manager or Cisco Emergency Responder servers, consider the following situations:
  - If you choose to store the DMA TAR file in a local directory when you run DMA, make sure that you move the TAR file to an external device before you begin the upgrade.
  - Make sure that the server that is being used for the upgrade is supported. Refer to the release notes for your product.
  - Make sure that you obtain the necessary licenses for your product. Refer to the *Cisco Emergency Responder Administration Guide 2.0* or to the *Upgrading to Cisco Unified Communications Manager Release 7.1(2)*.
  - DMA does not export the Cisco Emergency Responder cluster configuration. You must set up the clusters again after you upgrade successfully to Cisco Emergency Responder 2.0.

DMA Installation Procedure

Before you install DMA, make sure to review the information in the "Preinstallation Guidelines and Procedures" section on page 5.

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 8 for more information.

To install DMA, perform the following steps. This procedure should take about 20 to 40 minutes to complete.

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: DataMigrationAssistant-7-1-1.exe.

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:

- Capital letter (A-Z)
- Lowercase letter (a-z)
- Numeral (0-9)
- Special character ({ } , . < > : ? / | \ ` ~ ! @ $ ^ & * ( ) _ - +)

Note The Informix password cannot contain 3 back slash (\) characters.

Caution Do not change the Informix password after installing DMA. Changing the password will cause DMA exports 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:

- "Stopping DMA" section on page 8
- "Uninstalling DMA" task on page 9

Note To uninstall previous versions of DMA, refer to uninstall instructions in the guide for that release. This section applies only to uninstalling DMA 7.1(2).

Stopping DMA

Ensure that DMA is not running on your system. DMA, a server application that is controlled through a browser interface, can continue to run after you close the browser. To verify that you have stopped DMA, perform the following procedure:

Procedure

Step 1 Choose **Start > Programs > Cisco Data Migration Assistant> Cisco DMA**.

Step 2 When prompted, log in as the Windows Administrator.

The Security Alert window displays. To continue running DMA, you must click **Yes**.

The Data Migration Assistant Home window displays.

Step 3 If you are running DMA on a secure server, the Warning - Security window displays. It asks whether you want to accept a certificate from the secure server to exchange encrypted information.

To continue running DMA, you must click either **Yes** or **Always**. If you click **Always**, this window will not display again when you access this server.

The Data Migration Assistant Home window displays.

Step 4 From the Data Migration Assistant menu bar, choose **Export > Export Data**.

The Export Data window displays.

Step 5 Click the **View Status** link.

Step 6 Review the status to determine whether the last execution completed.

If you are not sure whether the DMA process completed, you can cancel the DMA operation by choosing **Start > Programs > Cisco DMA > Cancel Export**. The system could require several minutes to cancel the export process.

Step 7 Continue the DMA removal, as described in the "Uninstalling DMA" section on page 9.

Uninstalling DMA

Note To uninstall previous versions of DMA, refer to uninstall instructions in the guide for that release. This section applies only to uninstalling DMA 7.1(2).

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 Choose **Yes** to uninstall.

Step 5 Make sure that a restart of the server is possible and choose **Yes** to restart the server.

Note If you use Virtual Network Computing (VNC) to access your server, you may want to remotely restart the server by choosing **No** and restarting the server by using the VNC facility that sends Ctrl-Alt-Delete to the server.

Before You Begin

Before you start DMA, refer to one of the following tables:

- For Cisco Unified Communications Manager, perform the procedures that are shown in Table 1.
- For Cisco Emergency Responder, perform the procedures that are shown in Table 2.

Table 1 Procedures to Follow Before Running DMA for Cisco Unified Communications Manager

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 *Backup and Restore Utility Administration Guide* and related documentation at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
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 *Using Cisco Unified Communications Manager Upgrade Utility* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
To back up CAR data, ensure the CAR plug-in is installed on the publisher server.	See the "Migrating CAR Data" section on page 11.
Purge any system data that you no longer need, such as CAR database records. Purging the CAR data speeds up the migration process and decreases the size of the DMA TAR file. You may need to purge the CAR database or other system data if the DMA TAR file exceeds 2 GB. The version of CAR that runs on Cisco Unified Communications Manager 7.1(2) does not retain CDR records older than the ART Database Age configured in the 4.x ART database. You can configure the ART database age through the Configure Automatic Database Purge window of ART. The default ART database age specifies 180 days. If the ART database age is greater than 180 days, the CAR database in 7.x will retain only 180 days (maximum) of data. However if the ART database age is less than 180 days, only the data within the age limit that is specified will get retained in CAR 7.x database after migration. If you migrate records older than 180 days, the system deletes them immediately after you upgrade. Any records that are not exported during the specified time will not get migrated. If you want to export the CAR database, you must choose to do so within the Data Migration Assistant Custom Options window. If you export CAR data, Data Migration Assistant allows you to specify the amount of time that you want to allot for CAR migration. For more information on exporting the CAR database, or other functions of the Data Migration Assistant, refer to "Selecting Custom Options" procedure on page 14.	For information on manually purging CAR records, refer to the *CDR Analysis and Reporting Administration Guide*. For information on configuring automatic database purging after you upgrade, refer to the *CDR Analysis and Reporting Administration Guide* for Cisco Unified Communications Manager.
If you use Cisco Unified Communications Manager CDR Analysis and Reporting, make sure that the latest CDRs exist in the CAR database by setting the CDR load schedule to run before you execute the Data Migration Assistant. DMA will not migrate any CDRs that are generated after you have run the CDR loader.	For information on configuring the CAR load schedule before you upgrade, see the *Cisco Unified Communications Manager Serviceability Administration Guide* for the version of Cisco Unified Communications Manager that is running on your system.
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 12.

Table 1 Procedures to Follow Before Running DMA for Cisco Unified Communications Manager (continued)

Procedure	Reference
Copy CAPF data from the subscriber servers to the publisher server.	See the "Migrating Existing CAPF 1.0(1) Data" section on page 12.
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 14.
Make sure that you manually move the reports to the publisher server's local directory and update the service parameter to reflect the new location if the QRT report is residing in the network drive that is defined in the service parameter.	
Specify which logs you want to export.	See the "Selecting Custom Options" section on page 14.
Verify that you have performed all tasks that are necessary for a successful DMA export.	See the "Verifying Pre-DMA Export Tasks" section on page 15.

Table 2 Procedures to Follow Before Running DMA for Cisco Emergency Responder

Procedure	Reference
Use the Cisco Unified Communications Manager Backup and Restore Utility (BARS) to back up your data on the Cisco Emergency Responder publisher server. You can use the BARS backup to fall back to your current software version, if necessary.	Refer to the appropriate version of *Backup and Restore Utility Administration Guide* and related documentation at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
Create the following directory on the publisher server: C:\Program Files\Cisco Systems\CiscoER\Subscriber_backup. Copy the call history files from the Cisco Emergency Responder subscriber servers that are located in the following directory: C:\Program Files\Cisco System\CiscoER\callHistory Copy these call history files into the directory that you created on the publisher server.	For more information, refer to the appropriate version of *Cisco Emergency Responder Administration Guide*.
Disable Cisco Security Agent.	
Before you run DMA, make sure to shut down all Windows monitoring programs, such as PROGNOSIS.	

Migrating CAR Data

Before you can migrate 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*.

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 13.

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

Review the following details before you upgrade to Cisco Unified Communications Manager 7.1(2):

- Upgrades from Cisco Unified Communications Manager (formerly Cisco Unified CallManager) Release 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 Release 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 Release 7.1(2).

⚠

Caution If you fail to copy the data prior to the Cisco Unified Communications Manager 7.1(2) upgrade, the CAPF data on the Cisco Unified Communications Manager 4.x subscriber server does not migrate to the Cisco Unified Communications Manager 7.1(2) 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 7.1(2) 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 7.1(2)—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 Release 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 Release 7.1(2). 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 7.1(2) 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 12. To copy the files, perform the following procedure:

Procedure

Step 1 Copy the files in Table 3 from the machine where CAPF 1.0 is installed to the publisher database server where Cisco Unified Communications Manager Release 4.x is installed:

Table 3 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 Release 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 Release 7.1(2).

Step 3 After you upgrade the cluster to Cisco Unified Communications Manager Release 7.1(2), 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 Release 4.x.

Step 5 See the "Generating a New CAPF Certificate" section on page 14.

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

For instructions on disabling and enabling the CSA, refer to *Installing Cisco Security Agent for Cisco Unified Communications Manager*, which is available at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

If you manually disable Cisco Security Agent for Cisco Unified Communications Manager, remember to enable it after the DMA export 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:

- Cisco Security Agent for Cisco Unified Communications Manager versions lower than 2.0(5) are automatically disabled during DMA export.
- Cisco Security Agent for Cisco Unified Communications Manager versions 3.0(2) and higher can remain running without interfering with the DMA export.
- Cisco Security Agent for Cisco Unified Communications Manager versions between 2.0(5) and 3.0(2) do not automatically get disabled. You must disable Cisco Security Agent for Cisco Unified Communications Manager manually prior to DMA export.

Selecting Custom Options

The Custom Options window allows you to customize the contents of the DMA TAR file.

Perform the following procedure to enter data at the Custom Options window.

Procedure

Step 1 Choose **Start > Programs > Cisco Data Migration Assistant > Cisco DMA.**

Step 2 When prompted, log in as the Windows Administrator.

The Security Alert window displays. To continue running DMA, you must click **Yes**.

The Data Migration Assistant Home window displays.

Step 3 If you are running DMA on a secure server, the Warning - Security window displays. It asks whether you want to accept a certificate from the secure server to exchange encrypted information.

To continue running DMA, you must click either **Yes** or **Always**. If you click **Always**, this window will not display again when you access this server.

Step 4 From the Data Migration Assistant menu bar, choose **Export > Custom Options**.

Step 5 If you installed the CAR plug-in as described in the“Migrating CAR Data” section on page 11, you can make the following selections according to the way that you want to customize your CAR data:

a. If you want to export the CAR database, check the **Export CAR** check box.

Note DMA exports no CAR data unless you check the preceding check box.

b. If you checked the **Export CAR** check box in the preceding step, use the **CAR W1 Migration Time** pulldown menu to select the amount of time that you want to allot for CAR migration. Refer to the information in this field to determine the amount of time that you want to choose. The default is 1 hour.

Step 6 In the **Log file Options** field, read each option and select the checkbox of any that you wish to enable. You may select from among the following types of files to include in your TAR:

- Database export logs (C:\Program Files\Cisco\Trace\DMA\DB\*.* files)
- Directory export logs (C:\Program Files\Cisco\Trace\DMA\DirExport\logs\*.* files)
- DBL logs (C:\Program Files\Cisco\Trace\DBL\dbl_INSTALLDB*.txt file)
- DMA install logs (C:\Program Files\Common Files\Cisco\Logs\DMAInstall*.log files)
- DMA trace logs (C:\Program Files\Cisco\Trace\DMA\*.* files)

Step 7 When you finish, click the **Update** button.

Verifying Pre-DMA Export Tasks

DMA has an interface window, Pre-DMA Export Tasks, that you use to

- Consolidate all tasks that are needed to run DMA
- Provide the status of tasks that are needed to run DMA, so you can see which tasks you have done and which tasks remain to be done
- Acknowledge that you either completed these tasks or have decided to skip them.

Perform the following procedure to enter data at the Pre-DMA Export Tasks window:

Procedure

Step 1 Choose **Start > Programs > Cisco Data Migration Assistant > Cisco DMA.**

Step 2 When prompted, log in as the Windows Administrator.

The Security Alert window displays. To continue running DMA, you must click **Yes**.

The Data Migration Assistant Home window displays.

Step 3 If you are running DMA on a secure server, the Warning - Security window displays. It asks whether you want to accept a certificate from the secure server to exchange encrypted information.

To continue running DMA, you must click either **Yes** or **Always**. If you click **Always**, this window will not display again when you access this server.

Step 4 From the Data Migration Assistant menu bar, choose **Export > Pre-Export Tasks**.

The Pre-DMA Export Tasks window displays.

Step 5 Read each step, follow the instructions, and acknowledge the fact that you have completed the task by checking the associated check box. Some tasks may not require any further action and may simply be acknowledged. You may refresh the window at any time to update the "STATUS" messages based on any changes that you have made. Table 4 summarizes the tasks that you must acknowledge.

Step 6 When you finish, click the **Complete** button.

Table 4 Pre-DMA Export Tasks and Comments

Pre-DMA Export Task	Comment
BARS Check	--
Upgrade Assistant Check	--
CAR Plug-In Check	--
CAR Data Check	DMA displays the number of CDRs and identifies the oldest and most recent records.
Attendant Console Data	To copy files from a subscriber server automatically, input the subscriber IP address and login information into this task's "Instructions" field. Then, click this field's **Copy Files** button.
CAPF Data	To copy files from a subscriber server automatically, input the subscriber IP address and login information into this task's "Instructions" field. Then, click this field's **Copy Files** button.
CSA Check	--
Custom Options	Refer to "Selecting Custom Options" section on page 14

Running DMA

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

Note While you are running DMA, you may see a message if you have low disk space on your drive. Make sure that you clean up your drives routinely to have enough space. However, this does not affect the upgrade process in any way. Cisco recommends having around 500 MB disk space in the storage location where the DMA TAR file will be stored. The required space may vary, depending on the amount of data in the database and other data files. Make sure that you have enough disk space in the C: drive for the log files to be created.

Note You cannot run DMA if a BARS backup or restore is in progress. Running DMA simultaneously with BARS can result in CPU overload. If BARS is running, restart DMA after the BARS process completes.

Note If the DMA export process is started and the Cisco Unified Communications Manager server is connected to the network, the server must remain connected throughout the export process. If the Cisco Unified Communications Manager server gets disconnected from the network while a DMA export is running, the DMA error log does not list a network connection error. However, if the connection gets interrupted, the status page does not refresh properly and displays a “Page Not Found” error. Refer to “Network Outage May Cause a DMA Export Failure” section on page 38.

Note DMA does not support manual removal of the C:\DMARoot folder. If the folder is removed during the export process, DMA generates an error.

Before you start DMA, make sure to review the information in the “Before You Begin” section on page 9.

Procedure

Step 1 Choose **Start > Programs > Cisco Data Migration Assistant > Cisco DMA**.

Step 2 When prompted, log in as the Windows Administrator.

The Security Alert window displays. To continue running DMA, you must click **Yes**.

The Data Migration Assistant Home window displays.

Step 3 If you are running DMA on a secure server, the Warning - Security window displays. It asks whether you want to accept a certificate from the secure server to exchange encrypted information.

To continue running DMA, you must click either **Yes** or **Always**. If you click **Always**, this window will not display again when you access this server.

Step 4 From the Data Migration Assistant menu bar, choose **Export > Storage Location**.

The Storage Location window displays.

Step 5 In the Storage Location window

a. Choose the destination where DMA stores the TAR file by clicking one of the following radio buttons:

- **Windows Network Directory**—Stores the TAR file in a network folder. Enter information in these fields:

  Path Name—Network path to the appropriate folder or a mapped network drive path

  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.

Note DMA only supports saving the TAR file to the first tape drive. If you have multiple tape drives that are connected, you must use the first tape drive for DMA.

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. If you choose to have DMA generate the license file (licupgrade.lic), choose the local directory destination where DMA stores the file. 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.

c. Click **Update**.

d. If you chose **Local Directory** as the export 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 6 From the Data Migration Assistant menu bar, choose **Export > Export Data**.

The Export Data window displays. The window provides information on documentation that you need to read before proceeding as well as an estimate of the time that is required to perform the export.

Step 7 Read the "Before You Begin" section on page 9 of this document to help you understand and complete all the critical tasks before you use DMA to export data from the Windows system. After you have done so, check the check box to indicate that you understand and have completed all the pre-DMA tasks.

Step 8 Click **Start Export Now**.

The export begins.

A status window shows you the status of the export as it proceeds. The status window includes an estimate of the time that is required to complete the export, both at the start of the export 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 Export Data window.

You can also view a log of the export progress in the following 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 31.

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

Note Cisco recommends minimizing the DMA window rather than closing it. If you close the DMA window while a export process is running, the export continues; however, when you restart DMA, the main window will display the **Reset Status** button. Clicking the **Reset Status** button cancels the export process that is currently running.

DMA also displays a **Show Status** button so you can check the status of the export. If you close the window by accident, you can retrieve the old status without interrupting the export.

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

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

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

If the export does not complete successfully, the status window displays the appropriate messages. You must review the error logs and correct problems, as described in "Validating Export Data" section on page 20.

Step 9 If you saved the TAR file in a local directory in Step 5, copy that file to a network server or to a tape device before you upgrade.

The name of the TAR file varies, depending on whether the successful validation completes with errors, warnings, or no warnings:

- If the DMA export and validation succeeds without warnings or errors, the system creates DMAExportSuccessful<mm-dd-yy>#<hh:mm>.tar.
- If the DMA export succeeds but DMA detects warnings during the validation phase, the system creates DMAExportWithWarnings<mm-dd-yy>#<hh:mm>.tar.

  Note Cisco suggests that you correct these warnings and run DMA again.

- If DMA export succeeds but DMA detects errors during the validation phase, the system creates DMAExportFailed<mm-dd-yy>#<hh:mm>.tar.

  Note You must correct these errors and run DMA again.

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 get deleted when the upgrade process reformats the local server disks.

Note Any changes to the system after DMA generates the TAR file will not get migrated. To include those changes, you must run DMA export again.

Step 10 Verify that the TAR file does not contain errors, as described in "Validating Export Data" section on page 20.

Validating Export Data

After performing a DMA export, you must examine the error, warning, and auto-correction logs that DMA creates to ensure that the TAR file does not contain any problems that may result in a loss of functionality after the Cisco Unified Communications Manager upgrade. You can access these logs by clicking the appropriate log button on the status page or by navigating to the following folder

C:\Program Files\Cisco\Trace\DMA

The logs contain the following information:

- Errors Log (DMAErrors.log)—Errors found during the DMA export data and data validation phases. You must review and fix these errors in the Windows 4.x system before running DMA export again.

⚠ **Caution** Failure to correct these issues prior to the final DMA export and subsequent upgrade will result in an unsuccessful upgrade. This could present a serious service-impacting situation because the upgrade involves a complete software replacement.

- Warnings Log (DMAWarnings.log) —Warnings that are found during the DMA export and data validation phases. The warnings indicate that some data does not comply with all rules in the version of Cisco Unified Communications Manager to which you are attempting to upgrade. Cisco strongly recommends that you address the warnings and run DMA again prior to running the upgrade. Using a DMA archive that contains warnings may result in a loss of functionality after the Cisco Unified Communications Manager upgrade.

⚠ **Caution** Failure to correct these issues before or after migration may prevent future successful upgrades, including upgrades to service releases.

- Auto-corrected Log (DMAAutoCorrected.log)—Data that is not compliant with the Cisco Unified Communications Manager schema and that DMA automatically corrected during the Cisco Unified Communications Manager database and directory data export. Review the auto-corrected logs. If you do not agree with the changes, make your own changes and run DMA again.

⚠ **Caution** Failure to review the auto-corrections may result in auto-corrected changes in the migrated data with which you do not agree.

For information on displaying the status window, see the "Reviewing the Results of the last DMA Export Procedure" section on page 31.

For information about other logs that DMA generates, see the "Log Files" section on page 31.

DMA Export Information File

DMA automatically creates a export information file that is 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 whether 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.

Entering Answer File Generator Data

DMA includes an interface window, Answer File Generator, that you use to collect detailed data for the platformConfig.xml file. This window allows you to specify data for both the publisher server and the subscriber servers.

Perform the following procedure to enter data at the Answer File Generator window.

Procedure

Step 1 Choose **Start > Programs > Cisco Data Migration Assistant > Cisco DMA.**

Step 2 When prompted, log in as the Windows Administrator.

The Security Alert window displays. To continue running DMA, you must click **Yes**.

The Data Migration Assistant Home window displays.

Step 3 If you are running DMA on a secure server, the Warning - Security window displays. It asks whether you want to accept a certificate from the secure server to exchange encrypted information.

To continue running DMA, you must click either **Yes** or **Always**. If you click **Always**, this window will not display again when you access this server.

Step 4 From the Data Migration Assistant menu bar, choose **Export > Answer File Generator**.

The Answer File Generator window displays.

Step 5 Enter data about your Cisco Unified Communications Manager system in the Answer File Generator window. The window prompts you for the following configuration data about your system:

- Clusterwide Configuration, summarized in Table 5
- Primary Node Configuration, summarized in Table 6
- Secondary Node Configuration, summarized in Table 7

If you want more information about a particular field in the window, click the "?" icon near that field. When you click that icon a small pop-up window displays, which contains information about that field.

Step 6 When you finish, click the **Generate Answer Files** button.

If you want to export the CAR database, you must choose to do so within the Data Migration Assistant. If you export CAR data, Data Migration Assistant allows you to specify the amount of time that you want to allot for CAR migration. For more information on exporting the CAR database, or other functions of the Data Migration Assistant, see the *Data Migration Assistant User Guide*.

Table 5 Answer File Generator Clusterwide Configuration Settings

Field	Description
Administrator Credentials	
Administrator Username	Provides the ID of the administrator who is to be assigned to the administrator account. Ensure this ID is unique. It may contain alphanumeric characters, hyphens, and underscores.

Table 5 Answer File Generator Clusterwide Configuration Settings (continued)

Field	Description
Password	Provides the password that is assigned to the administrator account. This password allows a user to log in to the Command Line Interface (CLI) on the console. Ensure the password is at least 6 characters long. It may contain alphanumeric characters, hyphens, and underscores.
Confirm Password	Reenter the password.
Security Password	
Password	Provides the security password that is required for communication between nodes. This password also acts as the primary node database access password. Ensure the password is at least 6 characters long. It must start with an alphanumeric character and may contain alphanumeric characters, hyphens, and underscore.
Confirm Password	Reenter the password.
Application User Credentials	
Application Username	Provides the names of the Application User. Application users log in to the Application Administration windows to configure Cisco Unified Communication services. The Application Username must start with a letter and may contain alphanumeric characters, hyphens, and underscore.
Password	Provides the password that is assigned to the Cisco Unified Communications Manager application user. This password allows the user to log in to the Cisco Unified Communications Manager GUI. Ensure the password is at least 6 characters long. It may contain alphanumeric characters, hyphens, and underscores.
Confirm Password	Reenter the password.
Certificate Information	
Organization	Used to create the Certificate Signing Request. Allowable characters for Organization include letters, numbers, spaces, tabs, and the following special characters: . , - _ : ; { } ( ) [ ]
Unit	
Location	
State	
Country	Select a country by scrolling through the list of countries in the list.
SMTP	
Configure SMTP Host	Use Simple Mail Transfer Protocol (SMTP) for outbound e-mail. Check the check box to configure an SMTP host. Uncheck the check box to leave an SMTP host not configured.
SMTP Location	This field provides the name of the Simple Mail Transfer Protocol (SMTP) host that is used for outbound e-mail. You can specify the name as a host name or IP address. A host name can contain alphanumeric characters, hyphens, or periods and must start and end with an alphanumeric character. Ensure an IP address is in the format ddd.ddd.ddd.ddd, where each ddd is 255 or less.

Table 5 Answer File Generator Clusterwide Configuration Settings (continued)

Field	Description
Download Server for DMA Tarball	
Download Option	Specifies the upgrade retrieval mechanism to use to retrieve the DMA tarball file.
IP Address	Specifies the IP address of the download server. This node will uniquely identify the node on this network. **Caution** If another node in this network is using this address, you will get unpredictable results. You must enter the IP address in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
User Name	Specifies the user name that is used to access the download server.
Password	Specifies the password for the user name that is provided to access the download server.
Confirm Password	Reenter the password.
DMA Tarball Location	Specifies the DMA TAR file path in this download server. If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax. For example: • Begin the pathname with a forward slash (/) and use forward slashes throughout the pathname. • The pathname must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute pathname, which starts with a drive letter (for example, C:).
DMA Tarball File Name	Specifies the DMA Tarball File Name in this download server. For example, DMAExportSuccess08-01-08#12-27.tar
End User PIN	
End User PIN	The system uses this mandatory PIN field to reset the PIN for all end users that were configured on the Windows-based Cisco Unified Communications Manager.
Confirm PIN	Reenter the password.
End User Password	
End User Password	The system uses this mandatory field to reset the password for all end users that were configured on the Windows-based Cisco Unified Communications Manager. The password must be at least 6 characters long and can contain alphanumeric characters, hyphens, and underscores.
Confirm Password	Reenter the password.
CER (Cisco Emergency Responder systems only)	
CER Primary Route Point	Indicates the primary emergency number that is dialed and handled by CER. All characters must be numeric or * or # .
CER End User Language	Specifies the language the user would like to use for CER.
CERCCMVersion	Indicates the version of CER CCM.

Table 6 Answer File Generator Primary Node Configuration Settings

Field	Description
NIC Interface Settings	
Use Auto Negotiation	You can negotiate the speed and duplex settings of the Ethernet network interface card (NIC) automatically if the opposite access point (for example, hub or Ethernet switch) to which this node is attached supports this activity. Auto negotiation will negotiate the highest speed that is supported by both access points and favors full over half duplex. If you want to configure a speed of 1000 Megabits per second (Mbps) and it is supported by the opposite access point, you must choose auto negotiation because 1000 Mbps cannot be configured manually. Any explicit speed and duplex settings will get ignored, and full duplex will get chosen if 1000 Mbps is negotiated. If you do not know what the speed and duplex settings for your NIC should be, check the check box to enable automatic negotiation. If you want to enforce a particular speed and duplex and know what they should be, uncheck the check box to disable automatic negotiation and choose a speed and duplex setting.
NIC Speed	⚠ **Caution** If you do not know what the NIC Speed setting should be, enable auto negotiation by checking the Auto Negotiation check box. If you configure the NIC Speed or Duplex setting incorrectly, you will compromise network performance. If you want to configure a speed of 1000 Mbps and it is supported by the opposite access point, you must choose auto negotiation because 1000 Mbps cannot be configured manually. Any explicit speed and duplex settings will get ignored, and full duplex will get chosen if 1000 Mbps is negotiated. You can select 10 or 100 Mbps when you are manually setting the NIC speed.
NIC Duplex	⚠ **Caution** If you do not know what the NIC Duplex setting should be, enable auto negotiation by checking the Auto Negotiation check box. If you configure the NIC Speed or Duplex setting incorrectly, you will compromise network performance. You can select Full or Half duplex when you are manually setting the NIC duplex.
Change MTU Size	Indicates if the Maximum Transmission Unit (MTU) size is to be changed. **Note** MTU change is possible only when auto negotiation is enabled.
MTU Size	Indicates the size of the MTU. **Note** MTU change is possible only when auto negotiation is enabled.
DHCP	
Use DHCP for IP Address Resolution	Dynamic Host Configuration Protocol (DHCP) reduces the complexity of configuring nodes on your network You can configure a DHCP server to provide the IP address, net mask, default gateway, and possibly DNS servers and domain information when a machine first boots. If you have a DHCP server that is configured for this node, you can enable DHCP. Check the check box if DHCP server is enabled and you want to use DHCP; otherwise, Uncheck the check box to manually configure static networking information for this node.

Table 6 Answer File Generator Primary Node Configuration Settings (continued)

Field	Description
Host Name	Specifies a host name that is an alias that is assigned to an IP address to identify it. The host name can comprise up to 63 characters and can contain alphanumeric characters and hyphens. It must start with an alphabetic character.
IP Address	Uniquely identifies the node on this network. ⚠ **Caution** If another node in this network is using this address, you will get unpredictable results. You must enter the IP address in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). **Note** If DHCP is unchecked, consider this field as mandatory.
IP Mask	Specifies the IP mask of the node. It defines the part of the address that forms the base IP address. You must enter the IP mask in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). A valid IP mask should have contiguous “1” bits on left side and contiguous “0” bits on the right. Example of a valid mask: 255.255.240.0 (11111111.11111111.11110000.00000000) Example of an invalid mask: 255.255.240.240 (11111111.11111111.11110000.11110000) **Note** If DHCP is not checked, consider this field as mandatory.
Gateway Address	Represents a network point that acts as an entrance to another network. Configure the address of the gateway here, and outbound packets will get send to the gateway, which will forward them to their final destination. You must enter the gateway address in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). You may set the field to 255.255.255.255 if you do not want or have a gateway. However, doing so may limit you to only being able to communicate with devices on your subnet. **Note** If DHCP is not checked, consider this field as mandatory.
DNS	
Configure Client DNS	Domain Name System (DNS) client allows your computer to translate names of other computers on the network to IP addresses if a DNS server is available. When DNS is not configured, you should enter only the IP address for all network references. Check the check box if you want to configure your DNS client and have one or more available DNS servers. You may disable DNS. Doing so limits the server's ability to resolve some domain names. DHCP can also configure the DNS client. If you are using DHCP to configure your DNS Client, you can leave DNS disabled. Uncheck the check box if you want to configure all hosts manually in /etc/hosts or if you have configured DHCP to provide your DNS client information.

Table 6 Answer File Generator Primary Node Configuration Settings (continued)

Field	Description
Primary DNS	Provides the IP address of the primary DNS server. You must enter the Primary DNS in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). **Note** If DNS is checked, consider this field as mandatory.
Secondary DNS (optional)	For this optional field, the Secondary DNS provides the IP address of the secondary DNS server. You must enter the Secondary DNS in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	The Domain Name provides the name of the domain in which this node is located. **Note** If DNS is checked, consider this field as mandatory.
Time Zone	
Region	Lets you select a region for your time zone. After you select a region, the Time Zone dropdown list gets populated with time zones for that region.
Time Zone	Specifies the time zone in which the node is located. Time Zone comprises a list of time zones around the world. Scroll through the list to select the appropriate time zone.
Network Time Protocol	
Use Network Time Protocol (NTP)	Network Time Protocol (NTP) helps keep the machine clock accurate. A node that uses NTP will periodically query NTP server(s) for a time update. Check the check box if you want to configure NTP servers; otherwise, uncheck it. ⚠ **Caution** The server uses the machine hardware clock if NTP is not used. Be aware that the hardware clock may be inaccurate and is susceptible to change.
NTP Server 1	Enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server. If Use Network Time Protocol (NTP) is checked, you must specify at least one NTP server. **Note** Cisco recommends that you use a minimum of three external NTP servers.
NTP Server 2	
NTP Server 3	
NTP Server 4	
NTP Server 5	

Table 7 Answer File Generator Secondary Node Configuration Settings

Field	Description
NIC Interface Settings	
Use Auto Negotiation	You can negotiate the speed and duplex settings of the Ethernet network interface card (NIC) automatically if the opposite access point (for example, hub or Ethernet switch) to which this node is attached supports this activity. Auto negotiation will negotiate the highest speed that is supported by both access points and favors full over half duplex. If you want to configure a speed of 1000 Mbps and it is supported by the opposite access point, you must choose auto negotiation because 1000 Mbps cannot be configured manually; any explicit speed and duplex settings will get ignored, and full duplex will get chosen if 1000 Mbps is negotiated. If you do not know what the speed and duplex settings for your NIC should be, check the check box to enable automatic negotiation. If you want to enforce a particular speed and duplex and know what they should be, uncheck the check box to disable automatic negotiation and choose a speed and duplex setting.
NIC Speed	⚠ **Caution** If you do not know what the NIC Speed setting should be, enable auto negotiation by checking the Auto Negotiation check box. Be aware that if you configure the NIC Speed or Duplex setting incorrectly, network performance will be compromised. If you want to configure a speed of 1000 Mbps and it is supported by the opposite access point, you must choose auto negotiation because 1000 Mbps cannot be configured manually; any explicit speed and duplex settings will get ignored, and full duplex will get chosen if 1000 Mbps is negotiated. You can select 10 or 100 Mbps when you are manually setting the NIC speed.
NIC Duplex	⚠ **Caution** If you do not know what the NIC Duplex setting should be, enable auto negotiation by checking the Auto Negotiation check box. Be aware that if you configure the NIC Speed or Duplex setting incorrectly, network performance will be compromised. You can select Full or Half duplex when you are manually setting the NIC duplex.
DHCP	
Use DHCP for IP Address Resolution	Dynamic Host Configuration Protocol (DHCP) reduces the complexity of configuring nodes on your network You can configure a DHCP server to provide the IP address, net mask, default gateway, and possibly DNS servers and domain information when a machine first boots. If you have a DHCP server that is configured for this node, you can enable DHCP. Check the check box if DHCP server is enabled and you want to use DHCP. Otherwise, uncheck the check box to manually configure static networking information for this node.

Table 7 Answer File Generator Secondary Node Configuration Settings (continued)

Field	Description
Host Name	Specifies a host name that is an alias that is assigned to an IP address to identify it. The host name can comprise up to 63 characters and can contain alphanumeric characters and hyphens. It must start with an alphabetic character.
IP Address	Uniquely identifies the node on this network. ⚠ **Caution** If another node in this network is using this address, you will get unpredictable results. You must enter the IP address in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). **Note** If DHCP is unchecked, consider this field as mandatory.
IP Mask	Specifies the IP mask of the node. It defines the part of the address that forms the base IP address. You must enter the IP mask in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). A valid IP mask should have contiguous "1" bits on left side and contiguous "0" bits on the right. Example of a valid mask: 255.255.240.0 (11111111.11111111.11110000.00000000) Example of an invalid mask: 255.255.240.240 (11111111.11111111.11110000.11110000) **Note** If DHCP is not checked, consider this field as mandatory.
Gateway Address	Represents a network point that acts as an entrance to another network. Configure the address of the gateway here, and outbound packets will get send to the gateway, which will forward them to their final destination. You must enter the gateway address in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). You may set the field to 255.255.255.255 if you do not want or have a gateway. However, doing so may limit you to only being able to communicate with devices on your subnet. **Note** If DHCP is not checked, consider this field as mandatory.
DNS	

Table 7 ***Answer File Generator Secondary Node Configuration Settings (continued)***

Field	Description
Configure Client DNS	Domain Name System (DNS) client allows your computer to translate names of other computers on the network to IP addresses if a DNS server is available. When DNS is not configured, you should enter only the IP address for all network references. Check the check box if you want to configure your DNS client and have one or more available DNS servers. You may disable DNS. Doing so limits the server's ability to resolve some domain names. DHCP can also configure the DNS client. If you are using DHCP to configure your DNS Client, you can leave DNS disabled. Uncheck the check box if you want to configure all hosts manually in /etc/hosts or if you have configured DHCP to provide your DNS client information.
Use Primary Node DNS settings	When you are configuring secondary node DNS parameters, you can use the primary node's DNS settings for secondary nodes. When this check box is checked, the user is not required to enter DNS parameters because they are automatically copied from the primary DNS settings. **Note** If the primary node's DNS settings are changed after secondary node DNS settings are created, these secondary node settings automatically get updated to the primary node's modified settings when this check box is checked. Any changes made to these secondary DNS settings will get discarded because this check box enforces using the same settings as for the primary node. Check this check box to use primary node DNS settings for secondary nodes. Uncheck this check box if different DNS settings are to be used for secondary nodes.
Primary DNS	Provides the IP address of the primary DNS server. You must enter the primary DNS in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). **Note** If DNS is checked, consider this field as mandatory.
Secondary DNS (optional)	For this optional field, the Secondary DNS provides the IP address of the secondary DNS server. You must enter the secondary DNS in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	The Domain Name provides the name of the domain in which this node is located. **Note** If DNS is checked, consider this field as mandatory.

Table 7 Answer File Generator Secondary Node Configuration Settings (continued)

Field	Description
Time Zone	
Use Same Time Zone as Primary Node	When you are configuring the time zone for the secondary node, you can choose to use the Primary Time Zone value. When this setting is checked, the time zone for the secondary node automatically gets set to Primary Node Time Zone value. **Note** If the user changes the Primary Nodes Time Zone after secondary nodes are created by using the preceding functionality, the new primary time zone will automatically be applied to the already-created secondary nodes. If the user changes the Secondary Time Zone value that was loaded from the Primary Time Zone value when this functionality is enabled, the changes that the user gets are discarded, and the Primary Time Zone value will continue to be used. Check the check box if you want to use the primary node's time zone for the secondary node. Uncheck the check box if you want to enter a different time zone for the secondary node.
Time Zone	Specifies the time zone in which the node is located. Time Zone comprises a list of time zones around the world. Scroll through the list to select the appropriate time zone.
List of Secondary Nodes	Identifies the secondary nodes (subscribers) in the cluster by host name. In the text box, enter parameters that are required for the secondary node and use the **Add Secondary Node** button to add the secondary node. Use the **Delete Secondary Node** button to delete an added secondary node Click a secondary node in the list to view that secondary node’s parameters.

Administering and Troubleshooting DMA

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

- Determining DMA Software Version, page 30
- Reviewing the Results of the last DMA Export Procedure, page 31
- Log Files, page 31
- Trace Files, page 36
- Network Outage May Cause a DMA Export Failure, page 38

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 **Export > Home** from DMA menu bar.
- If DMA is not running, choose **Start > Programs > Cisco Data Migration Assistant > Cisco DMA** 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 Export Procedure

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

Procedure

Step 1 Choose **Start > Programs > Cisco Data Migration Assistant > Cisco DMA.**

Step 2 When prompted, log in as the Windows Administrator.

The Security Alert window displays. To continue running DMA, you must click **Yes**.

The Data Migration Assistant Home window displays.

Step 3 If you are running DMA on a secure server, the Warning - Security window displays. It asks whether you want to accept a certificate from the secure server to exchange encrypted information.

To continue running DMA, you must click either **Yes** or **Always**. If you click **Always**, this window will not display again when you access this server.

Step 4 From the Data Migration Assistant menu bar, choose **Export > Export Data**.

Step 5 In the Export Data window, click the **View Latest Status** link.

If you click the **View Latest Status** link during an export procedure, the status of the current procedure displays.

Step 6 After the export completes, you can view the errors log, warnings log, and auto-corrected log by clicking the corresponding button.

Log Files

Table 8 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 8 DMA Log Files

File Type	Description	File Location	File Name
DMA installation log files	This file gets 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. *date_ time* is in the format MM-DD-YYYY HH.mm.ss
		C:\Program Files\ Common Files\Cisco\Logs\ DMA	DMAUninstall*date_time*.log, where *date_ time* specifies the date and time that the file was uninstalled. *date_ time* is in the format MM-DD-YYYY HH.mm.ss DMAInstUI.log IDSInstall.log InstallUtils.log
Database installation log file	This file contains logs that are generated by the Informix Dynamic Server (IDS) installation and contains information regarding the path settings and installation result. This represents a third-party-generated log file.	C:\Program Files\Common Files\Cisco\Logs\DMA\	dbcmds.log
Export operation log file	This file gets created each day that you run DMA to back up data. If you run the export procedure more than once on the same day, DMA appends information to the existing file for that day.	C:\Program Files\Cisco\Trace\DMA	DMAStatus*date*.log, where *date* specifies the date that the file was created in the format MM-DD-YY. This log also displays when you click the **View Latest Status** link.
Database export operation log file	This file gets created the first time that you run DMA to export data. The log contains information about each request that is made by the database export command during a single session. Each subsequent time that you run the export procedure, DMA deletes the file and creates a new one to hold the logging information for that session.	C:\Program Files\Cisco\ Trace\DMA\DB	exportdb.log This folder also contains these additional database export logs: • createdb.log • dropdb.log • dropdb_w.log

Table 8 DMA Log Files (continued)

File Type	Description	File Location	File Name
Directory export operation error log file	This file gets created each time that you run DMA to backup data. If the file exists, DMA overwrites it.	C:\Program Files\Cisco\Trace\DMA\DirExport\log	DirExport_Error.log
Data validation log	This file contains any validation errors that are found during the verification of database and directory data during the export process	C:\Program Files\Cisco\Trace\DMA\DB\	datavalidation.log
Export progress indicator logs	This file gets created when you run DMA. It contains a high-level log of export and data validation progress.	C:\Program Files\Cisco\Trace\DMA\Progress	AllProgress.log If errors occur in the export progress, the following log files get created in the same folder: • CSV_Import*.* • ExportDB_CCM*.* • ExportToCSVs*.* • InstallDB_Full*.*
Consolidated errors log	This file contains errors that were found during the DMA export data and data validation phases. You must review and fix these errors in the Windows 4.x system before running DMA export again.	C:\Program Files\Cisco\Trace\DMA	DMAErrors.log
Consolidated warnings log	This file contains warnings found during the DMA export and data validation phases. Cisco strongly recommends that you address the warnings and run DMA again prior to running the upgrade.	C:\Program Files\Cisco\Trace\DMA	DMAWarnings.log

Table 8 DMA Log Files (continued)

File Type	Description	File Location	File Name
Consolidated auto-corrected log	This file contains data that was found during the DMA export and data validation phases that are not compliant with the Cisco Unified Communications Manager schema but that DMA has auto-corrected. You do not need to taken any action for these items.	C:\Program Files\Cisco\Trace\DMA	DMAAutoCorrected.log
DMA uninstall log	This file logs the traces during DMA uninstall.	C:\ProgramFiles\Common Files\Cisco\Logs\DMA\DMAUninstall	<MM-DD-YY-HH.mm.ss>.log where DD-YY-HH.mm.ss specifies the date and time—(date-year-hours-minutes-seconds).

Common Errors

DMA can return the errors that are described in Table 9, which can cause it to fail.

Table 9 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: • 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.
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.

Table 9 DMA Errors Messages and Descriptions (continued)

Error Message	Description
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 10 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 10 DMA Trace Files

File Type	Description	File Location	File Name
DMA operation trace file	This file gets created each day that you run DMA to back up data. If you run the export procedure more than once on the same day, DMA appends information to the existing file for that day	C:\Program Files\Cisco\Trace\DMA	DMA<Trace*date*.log>, where *date* specifies the date that the file was created or updated in the format MM-DD-YY.
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\DMA\DB	• Export: installdbccm.log • W1install: installdbw1.log
Directory export operation trace file	This file gets created the first time that you run DMA to back up data. Each subsequent time that you run the export procedure, DMA appends information to this file.	C:\Program Files\Cisco\Trace\DMA\DirExport\log	DirExport_Trace.log
CAR export operation log file	This file gets created the first time that you run DMA to export CDR data.	C:\Program Files\Cisco\Trace\DMA\DB	installdbcar.log
Database install setup trace file	This file displays the Informix setup status	C:\Program Files\Common Files\Cisco\Logs\DMA	dbcmds.log

Table 10 DMA Trace Files (continued)

File Type	Description	File Location	File Name
Cisco Unified Communications Manager Pre-Migration Log and Trace	This file gets created by Cisco Unified CallManager 4.x migration processing, if the current Cisco Unified Communications Manager database version does not match the version that DMA needs to export. For DMA 7.1, the migration point export version equals Cisco Unified CallManager 4.2. If the Cisco Unified CallManager database version is less than 4.2, the system migrates the database to that version prior to export. DMA stores the logs and trace files that are associated with that pre-migration and do not typically require review.	C:\Install\DBInstall	Various The file modification dates allow you to determine which files apply
Cisco Unified Communications Manager Target Version Migration Test SQL Processing Logs	This file gets created when the migration validation testing processes various SQL files. If SQL processing fails, you can view the associated *.sql log file for a record of the problem.	various subdirectories within C:\tmp\db\sql	Files with a ".log" extension that match the sql file in that directory.
Directory export operation report file	This file gets created the first time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\Program Files\Cisco\Trace\DMA\DirExport\log	DirExport_Report.txt
Directory export operation Warning file	This file gets created each time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\Program Files\Cisco\Trace\DMA\DirExport\log	DirExport_Warning.log
Directory export operation Auto-corrected file	This file gets created each time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\Program Files\Cisco\Trace\DMA\DirExport\log	DirExport_Correctedusers.log

Network Outage May Cause a DMA Export Failure

Symptom

The Cisco Unified Communications Manager server gets disconnected from the network while running a DMA export. However, the DMA error log does not list a network connection error.

Possible Cause

This is not a performance error. This is standard DMA operation.

Recommended Action

If the DMA export process is started and the Cisco Unified Communications Manager server is connected to the network, the server must remain connected throughout the export process. If the connection is interrupted, the status page does not refresh properly, and displays a "Page Not Found" error. Furthermore, the connection to the database gets interrupted. Users must close the browser and reopen the DMA application to return to the status window. The log files still generate correctly. However, the DMA export fails due to the interruption to the database connection. In this case, you must restart the DMA export.

If the DMA export process is started and the Cisco Unified Communications Manager server is not connected to the network, there is no effect on the process if the connection state is changed.

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.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.