



Release Notes for Data Migration Assistant (DMA) Release 7.0(1a)

September 16, 2008

This document comprises the new features that are included and caveats that are resolved in Data Migration Assistant (DMA) Release 7.0(1a).

Contents

These release notes discuss the following topics:

- [Introduction, page 1](#)
- [Important Notes, page 2](#)
- [Caveats, page 7](#)
 - [Caveats Resolved in DMA Release 7.0\(1a\), page 7](#)
 - [Use BugToolkit to Find the Latest Resolved Caveat Information, page 8](#)
 - [Open Caveats as of August 27, 2008](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)
- [Cisco Product Security Overview, page 10](#)

Introduction

Data Migration Assistant (DMA) Release 7.0(1a) collects application data from a Cisco Unified Communications Manager Releases 4.1(x), 4.2(x) and 4.3(x) system for upgrade to Cisco Unified CM Release 7.0(1a). DMA exports data in the current Windows based system (with SQL Server database) that later will get imported to the Linux based system (with Informix database).

DMA also collects application data from a Cisco Emergency Response (CER) 1.3 system for upgrade to CER 7.0.

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



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

© 2008 Cisco Systems, Inc. All rights reserved.

In addition to creating an export, DMA also performs a set of migration compatibility tests (data validation) on the exported Unified CM 4.x data

- If DMA discovers issues, either in the export itself, or in the data validation, DMA may report some type of "Failure." Do not consider such a message to be alarming.
- Even when DMA completes successfully, but especially if any "Error" or "Warning" occurs, the user should examine the generated messages. These messages may be
 - Simply information about auto-data-correction that will be performed in the migration.
 - Alerts to let you know the problems that DMA encountered as it attempted to check the data.

Generally, these problems require user expertise to determine how best to alter the data to remove the migration incompatibility.



Note

You must install and run DMA Release 7.0(1a) on the Cisco Unified Communications Manager publisher server before you upgrade to Unified CM 7.0(1). If you make any configuration changes to Cisco Unified Communications Manager after you run DMA, the system does not retain these changes when you upgrade.



Note

Do not consider the DMA Export a substitute for a system backup. You cannot use it to restore your Cisco Unified Communications Manager system in the unlikely event that you are unable to complete your upgrade.

Important Notes

The following section contains important information to help you get started with Data Migration Assistant Release 7.0(1a).

- [Upgrades That Are Supported, page 3](#)
- [Run DMA Early, page 3](#)
- [Cisco Security Agent \(CSA\), page 3](#)
- [Completion Status Recognition, page 3](#)
- [Configuration File, page 4](#)
- [Cisco Unified CM Target Version Checking, page 4](#)
- [Unified CM Target Version Gets Saved in the DMABackupInfo.inf, page 5](#)
- [Support For Mapped Network Drive, page 5](#)
- [Exporting RTMT Reports, page 5](#)
- [Exporting Quality Reporting Tool \(QRT\) Reports, page 5](#)
- [DMA Uninstall, page 6](#)
- [Proper Return Code Sent To the DMA Framework, page 6](#)
- [Linux Install, page 6](#)
- [What Gets Migrated via DMA When Unified CM Gets Integrated Into a Corporate LDAP Store, page 6](#)

Upgrades That Are Supported

Supported upgrade paths comprise:

- Unified CM releases 4.1(3), 4.2(3), 4.3(1) and 4.3(2) to Unified CM 7.0(1)
- CER 1.3 to CER 7.0



Note

DMA 7.0(1a) does not support upgrades from Unified CM releases 5.1(x), 6.0(x), or 6.1(x).

Run DMA Early



Note

Be aware that it is important that you run DMA early – possibly as early as weeks before the actual upgrade window to allow time for you to fix any non compliant data.

A successful DMA run does not completely prepare you for migration and upgrade.

To understand critical tasks that must be completed, Cisco recommends that you read the "Before You Begin" section of the *Data Migration Assistant User Guide Release 7.0(1a)* before you use DMA to export data from the Windows system.

To understand critical upgrade tasks that must be completed, Cisco recommends that you refer to *Upgrading to Cisco Unified Communications Manager Release 7.0(1) from Cisco Unified Communications Manager 4.x Releases*.

These documents may be found at

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

Cisco Security Agent (CSA)

Before the DMA export begins, check the system CSA version by right-clicking the red CSA flag in the systray and, from the options that display, click **About**.

If the CSA version equals

- Less than 2.0(5), DMA stops CSA automatically during the export.
- Less than 3.0(3) but greater than 2.0(5), you must manually disable CSA before you run DMA.
- 3.0(3) or higher, CSA can remain enabled while DMA runs.

Completion Status Recognition

DMA completion can reflect four possible outcomes:

- Export Success & Validation Success



Note

If your DMA run results in one of the following three outcomes, you must fix the inconsistencies and rerun DMA.

- Export Success & Validation Success but with Warnings

- Export Success & Validation Failure
- Export Failure

You can access the DMA log files from the final status window. You can use them to see what needs to be fixed.

Configuration File

Data Migration Assistant 7.0(1a) generates a configuration file (platformConfig.xml) that can assist you in performing an upgrade of the first node to Cisco Unified Communications Manager 7.0(1) from supported releases of Cisco Unified CallManager 4.x. During the upgrade, the configuration file prepopulates several fields, including domain name, IP address, primary DNS, secondary DNS, and NTP server.

- platformConfig.xml extracts info from the CM 4.X servers to automate some steps during Linux installation on the publisher server.
- platformConfig.xml gets stored in the same location as the DMA tarball if the storage location is on local or network drives.
- platformConfig.xml gets stored in D:\DMA\ if the DMA tarball storage location is on the tape drive.
- Customer must copy platformConfig.xml to a USB key and plug in this USB key on the publisher server during the Linux installation.

When this platformConfig.xml is used during W1 install, the “Apply a Patch” screen gets skipped

The Linux install screen populates input data that is extracted from the platformConfig.xml

To use the configuration file, copy the platformConfig.xml file to a USB key and place the USB key into the Cisco Unified Communications Manager first node before you boot the server with the Cisco Unified Communications Manager 7.0(1) DVD.

If you choose to store the DMA tar file on a network directory or local directory, DMA stores the platformConfig.xml in the same directory. If you choose to store the DMA tar file on a tape drive, DMA stores the platformConfig.xml in D:/DMA.



Note

Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4 for the configuration file. These keys have a W95 FAT32 format.

Installation/Upgrade (Migration) Considerations

To use the configuration file that Data Migration Assistant generates to prepopulate fields during an upgrade to Cisco Unified Communications Manager 7.0(1) from supported releases of Cisco Unified CallManager 4.x, copy the platformConfig.xml file to a USB key before you boot the server with the Cisco Unified Communications Manager 7.0(1) DVD.

Cisco Unified CM Target Version Checking

DMA generates DMABackupInfo.inf and includes this file in the tarball, as in the previous releases.

TargetCCMVersion = X.Y.Z (for example 7.0.1) indicates the Unified CM version with which this DMA tarball is compliant.

In Linux installation application, additional logic got added to verify that TargetCCMVersion matches the Unified CM version that you are installing.

TargetCCMVersion gets saved in the DMABackupInfo, inf file in the DMA tarball.

This provides a hook for the Linux installation application to verify whether the DMA tarball is generated by the proper DMA version.

Unified CM Target Version Gets Saved in the DMABackupInfo.inf

DMA export saves the target Unified CM version in the DMABackupInfo.inf file:

Sample in the DMABackupInfo.inf:

```
CCMVersion= 4.1.X
TargetCCMVersion = X.Y.Z
```

For example, for DMA 7.0(1a), the target Unified CM upgrade version equals release 7.0(1). So, this field displays 7.0.1, which is the Unified CM version, not the DMA current version, in case the version numbers get out of sync in future releases.

This means that if a Cisco Unified CM 7.0(1) respin becomes a reality in the future, the logic will work, and the customer can use DMA 7.0(1a) to upgrade to the Unified CM Release 7.0.1 respin release.

Support For Mapped Network Drive

DMA can create the DMA tarball in a mapped network drive that is defined in the Storage Location Window.

Select Network Directory Option and provide the path (for example, M:\export), userID, and password.

The drive letter gets translated to Windows UNC format (for example, 10.89.75.11\c\$\export)

CSCs152704

The system renamed Network Directory to Windows Network Directory.

Exporting RTMT Reports

DMA exports RTMT Reports data files that reside in C:\CiscoWebs\Service\RTMTReports\. DMA stores the files in the \serv\rtmt directory of the DMA TAR file.

Exporting Quality Reporting Tool (QRT) Reports

DMA exports QRT files to the DMA TAR file that exist in the location that is specified in the Log File field in the Service Parameter Configuration window for the Cisco Extended Functions service. The specified log file path must reside on the C:\ drive. If the path does not exist on the C:\ drive, DMA does not export the QRT reports, so the administrator must export the reports manually.



Note

If the Cisco Extended Function Service is running, the last (current) QRT file that is being used by this service cannot be exported. This is expected behavior, and is not an error.

DMA Uninstall

You can uninstall DMA by following these steps:

-
- Step 1** From the Start menu, click **Settings > Control Panel > Add/Remove Program**.
- Step 2** Locate Cisco Data Migration Assistant in the list of programs and click **Remove**. This removes IDS, IDS Client SDK (if it exists), DSNs, and the DMA application
- Step 3** When the removal completes, reboot the server as prompted. You will see IDS uninstall prompts that will be auto-selected for you. In the Add/Remove Programs list, the Informix Dynamic Server 10.00 and corresponding SDK Client specify no longer selectable.
-

Proper Return Code Sent To the DMA Framework

During DMA export and validation phases, the DMA framework launches separate processes to invoke the underlying component .exe files to export or validate the Unified CM database, directory, CAR, or CER data. When a fatal error exists in the data export or data validation, the logic returns failure to the DMA framework instead of continuing.

By using this information, the framework can determine whether fatal issues are encountered and whether DMA should be aborted.

Unified CM Database, CAR, CER Components

Exportdb.exe gets used to export and validate Unified CM, CAR, and CER databases. The return codes from the exportdb.exe follow:

- 0 - Indicates success, DMA framework continues
- 1 - Indicates warning, DMA framework continues but display proper warning messages on the status page
- -1 - Indicates failure. DMA framework halts.

Linux Install

During an upgrade, the Linux install application determines whether a platformConfig.xml file exists in the customer USB key. If it exists, the data gets read and populates in the UI. Default values gets used for data that is not found in the platformConfig.xml.

What Gets Migrated via DMA When Unified CM Gets Integrated Into a Corporate LDAP Store

The DirExport is the part of DMA that extracts user data from the directory and creates CSV files of that data. The CSV files get used to populate the database. All the user information gets migrated from the directory to the database.

When you upgrade from Cisco Unified CM 4.x to Cisco Unified CM 5.x or later, the following get migrated.

- EndUser
- IPMAManagerAssistant
- EndUserDeviceMap
- DirGroup
- EndUserDirGroupMap
- Endusenumplanmap .CSV
- PersonalAddressBook
- PersonalPhoneBook
- crsapplication

Caveats

This section contains information about the caveats that get resolved by this release of DMA and information about how to create your own list of resolved and open caveats.

- [Caveats Resolved in DMA Release 7.0\(1a\), page 7](#)
- [Use BugToolkit to Find the Latest Resolved Caveat Information, page 8](#)
- [Open Caveats, page 9](#)

Caveats Resolved in DMA Release 7.0(1a)

The release of DMA Release 7.0(1a) resolves the following caveats.

- [CSCsg96656](#) Unified CM repair did not fix database issue/replication.
- [CSCsh38822](#) DMA validation error on default credential policy received in CredentialPolicy.
- [CSCsi20684](#) DMA processing should handle invalid CSS failures better.
- [CSCsi30357](#) If the user orders members of routelist, database replication breaks.
- [CSCsi35186](#)- Extension mobility logins fail with an Error 6 database failure.
- [CSCsj42131](#) DMA assigns incorrect/unexpected partition to primary DN.
- [CSCsj50278](#) Consolidated log files and error files exist for directory export in DMA.
- [CSCsj78789](#) DMA validation fails with international dial plans.
- [CSCsk10706](#) Missing, mismatched and/or corrupted tables exist on subscriber nodes if replication get broken during a replicate set.
- [CSCsk56867](#) DMA performs premigration in staged upgrade when all servers not staged.
- [CSCsk70423](#) Encrypted password displays in plain text in DMA trace files.
- [CSCsl53087](#) H323 device got migrated with secure profile.
- [CSCsl78801](#) DMA shows validation warnings for unknown device.
- [CSCsm10541](#) dbreplication status returns an error when a subscriber is down.
- [CSCsm82734](#) Directory script in DMA failed to import users and process.

- [CSCsm95532](#) Device mobility data generates DMA warning: SQL error: -9794(validatesubnet).
- [CSCso69307](#) DMA install does not populate SIP profile field on SIP trunks.
- [CSCso77371](#) DMA DirExport failed to migrate PersonalAddressBook.
- [CSCsq00704](#) DMA export fails to export IPMA users.
- [CSCsq77338](#) DMA 4.1.3 -> 6.1.2.9901-63 loses user multi device associations.
- [CSCsq21832](#) End user to device mappings during DirExport contain multiple records.
- [CSCsr38524](#) Routepattern import failed for importing before associated RouteList.
- [CSCsq71657](#) CIPC device configuration does not contain the More Softkey Timer and AutoCallSelect.
- [CSCsr48902](#) User document link on user pages needs to be updated.
- [CSCsr29327](#) Inserting/updating two TODs with the same TS should be blocked.
- [CSCsr39946](#) Remote destination limit should be applied to Unified CM.
- [CSCsr52317](#) Uninstalling DMA gets stuck at "Cleaningup ISM files..." window.

Use BugToolkit to Find the Latest Resolved Caveat Information

You can find the latest resolved caveat information for Data Migration Assistant by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.



Tip

You need an account with Cisco.com to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Using Bug Toolkit

Known problems (bugs) get graded according to severity level. These release notes contain descriptions of

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

- Step 1** Access the Bug Toolkit, <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>.
- Step 2** Log in with your Cisco.com user ID and password.

Step 3 If you are looking for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field and click **Go**.



Tip

Click **Help** on the Bug Toolkit window for information about how to search for bugs, create saved searches, create bug groups, and so on.

Open Caveats

[Table 1](#) describes possible unexpected behaviors that you may encounter in Data Migration Assistant.



Tip

For more information about an individual defect, click the associated Identifier in [Table 1](#) to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version and the Integrated-in Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the "First Fixed-in Version" or "Integrated-in" fields. The information that displays in these fields identifies the list of Cisco Unified Communications Manager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Communications Manager releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1; however, the version information that displays for the Cisco Unified Communications Manager maintenance releases may not be as clearly identified.



Note

Because defect status continually changes, be aware that [Table 1](#) reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the [Using Bug Toolkit, page 8](#).



Tip

Bug Toolkit requires that you have an account with Cisco.com. By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>.

Table 1 *Open Caveats as of August 27, 2008*

Identifier	Headline
CSCsr06635	DMA Export - Not getting proper error logs on a network outage scenario.
CSCsr80272	Database - DMA export fails without proper error log.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0807R)