



Release Notes for Data Migration Assistant (DMA) Release 6.1(2)

Updated April 24, 2008

This document comprises the new features that are included and caveats that are resolved in Data Migration Assistant (DMA) Release 6.1(2).

Contents

These release notes discuss the following topics:

- [Introduction, page 1](#)
- [New and Changed Information for Data Migration Assistant 6.1\(2\), page 2](#)
- [Caveats, page 10](#)
 - [Open Caveat as of April 28, 2008](#)
- [Obtaining Documentation and Submitting a Service Request, page 12](#)
- [Cisco Product Security Overview, page 12](#)

Introduction

Data Migration Assistant (DMA) Release 6.1(2) collects application data from a Unified CM Releases 4.1(x) and 4.2(x) system for upgrade to Cisco Unified Communications Manager Release 6.1(2). The purpose of the DMA is to export data in the current Windows based system (with SQL Server database) that will be later imported to the Linux based system (with Informix database).

Data Migration Assistant Release 6.1(2) also collects application data from a Cisco Emergency Response (CER) 1.3 system for upgrade to CER 2.0.

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

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



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

© 2008 Cisco Systems, Inc. All rights reserved.

- If DMA discovers issues, either in the export itself, or in the data validation, then DMA may report some type of "Failure." Do not consider such a message 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 6.1(2) on the Cisco Unified Communications Manager publisher server before you upgrade to Cisco Unified Communications Manager Release 6.1(2). 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.

New and Changed Information for Data Migration Assistant 6.1(2)

The following sections contain information that is new or changed for this release of Data Migration Assistant:

- [Enhancements for Data Migration Assistant, page 2](#)
- [Upgrades That Are Supported, page 3](#)
- [Directory Message Improvements, page 5](#)
- [CER Improved Messages, page 8](#)
- [Proper Return Code Sent To the DMA Framework, page 9](#)
- [Linux Install, page 10](#)
- [Unified CM Target Version Gets Saved in the DMABackupInfo.inf, page 10](#)

Enhancements for Data Migration Assistant

The Data Migration Assistant 6.1(2) generates a configuration file (platformConfig.xml) that can assist you in performing an upgrade of the first node to Cisco Unified Communications Manager 6.1(2) from supported releases of Cisco Unified CallManager 4.x. The configuration file prepopulates several fields during the upgrade, including domain name, IP address, primary DNS, secondary DNS, and NTP server.

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 6.1(2) 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 will have a W95 FAT32 format.

Installation/Upgrade (Migration) Considerations

To use the configuration file generated by Data Migration Assistant to prepopulate fields during and upgrade to Cisco Unified Communications Manager 6.1(2) 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 6.1(2) DVD.

Upgrades That Are Supported

DMA installation applications block any installation on Unified CM systems other than 4.1(3) and CUCM 4.2(3).

Linux installation application verifies the target versions to ensure the tarball version is compatible.

**Note**

DMA 6.1(2) does not support upgrades from 5.1(2), 5.1(3), 6.0(1a) and 6.1(1).

Database Message Improvements

DMA Data Validation executes the same operations on customer data as will be performed in the actual upgrade. This enables DMA to catch problems that might cause the upgrade to fail. Be aware that catching these errors during data validation, while the Cisco Unified CallManager 4.x system is still available and operating, is very important.

Because you cannot anticipate and test for every variation of a data problem variations in advance, the mechanism used to catch these errors depends on the built-in error reporting in the general-purpose database tools that are used. Unfortunately, the error messages that result are not very specific. They do not specify the problem and solution in terms that are familiar to the user.

Enhancements in this release now provide additional commentaries that are relevant to Cisco Unified Communications Manager on a few of the most commonly seen error messages.

Examples of the Most Commonly Seen Error Messages

- [The -691 Referential Integrity Error, page 4](#)
- [The -11005 IDS Connection Failure Error, page 4](#)
- [The -271 IDS I/O Related Error, page 4](#)
- [The -391 Null Value Error, page 4](#)
- [The -239 Duplicate Record Error, page 4](#)
- [The -530 Constraint Violation Error, page 4](#)

The -691 Referential Integrity Error

This record was not processed because another record it needs, (see reference name listed below), is missing. This likely may be due to a previous error already reported in the log above, or the result of Directory Services Export issues reported separately, or due to missing Product, Locale, or other add-on definition CSV files that should exist on the source system but do not.

SUGGESTED ACTION: Resolve all prior reported issues. If none, look at the Suspected Field, if listed, for an indication of what data reference could not be resolved. Some hints:

- if ...DirGroup related, check for a Directory Export failure
 - if ...Locale related, check for a missing Locale Plug-In
- Re-execute DMA when all other issues are addressed.

The -11005 IDS Connection Failure Error

This is a hard error probably related to a DMA installation problem. It is a general issue and NOT related to the record / request being processed. DMA was unable to perform migration testing due to this failure. This reflects an installation or system failure.

Likely causes include:

- improper prior uninstall of the DBMS in a DMA upgrade
- a bad Informix password perhaps containing backslashes
- a system or disk or space related issue

SUGGESTED ACTION: Uninstall and re-install DMA carefully following all documented procedures.

The -271 IDS I/O Related Error

This is a transient error related to DMA/DB data access issues. It is a general issue. While possibly related to the record / request being processed, it does not indicate a problem with that record / request. DMA was unable to perform migration testing due to a failure accessing the data. This may have been due to resource constraints on the system or other activity.

SUGGESTED ACTION: Re-boot the server and re-execute DMA.

The -391 Null Value Error

This record was not processed because it is missing a required value. This could also be caused by specifying the value NULL in a required field.

SUGGESTED ACTION: Check the Suspected Field information and record contents, if provided, to determine which data needs to be filled in and for which record. Update that record to specify the required data and then re-execute DMA.

The -239 Duplicate Record Error

This record was not processed because another record exists with the same key value in a field, (or combination of fields), required to be unique. For example, CM 4.x permits multiple NumPlan entries with the same DNorPattern+RoutePartition value combination. Later CUCM versions enforce uniqueness in these combined values.

SUGGESTED ACTION: Check the Suspected Field information and record contents, if provided, to determine which data may be causing the uniqueness violation. Find the records sharing these values and determine and make the appropriate changes to remove the duplication. Then re-execute DMA.

The -530 Constraint Violation Error

This record was not processed because it contains a value which is incompatible with the restrictions associated with this setting. (See reference name listed below).

SUGGESTED ACTION: Check the documented setting range limits for the problem field. Correct the setting to be compatible with the requirements of CUCM version to which you intend to migrate. Then re-execute DMA.

For More Information

Refer to the *Data Migration Assistant User Guide*.

Directory Message Improvements

Table 1 comprises the improvements that have been made to user-viewed messages.

Table 1 Directory Message Improvements

Old Message	Condition	Changed Message	Solution
Locale mapping not found for \$singleValue. User=\$userKey	The locale that is present in the directory for the user is not available in the database.	No change.	Verify that the locale mapped for this user is present and is a valid locale and is available the database.
IPMA: User PKID not found for IPMA-Assist=\$ipmaAAValue. IPMA admin=\$userKey	Either the user does not exist in the directory or has been tagged invalid.	IPMA-Assist=\$ipmaAAValue for user=\$userKey" not found. Invalid user.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
IPMA: User PKID not found for IPMA-Assist=\$readLine. IPMA-Admin=\$userKey, TxtFile=\$txtFileURL	Either the user does not exist in the directory or has been tagged invalid.	IPMA-Assist=\$readLine for user=\$userKey not found in TxtFile=\$txtFileURL. Invalid user.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
PKID not found for member \$grpMemValue, GroupName=\$grpNameKey	Either the user does not exist in the directory or has been tagged invalid.	Member = \$grpMemValue with GroupName=\$grpNameKey not found. Invalid user.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
PKID not found for member \$memberName, GroupName=\$grpNameKey	Either the user does not exist in the directory or has been tagged invalid.	Member = \$grpMemValue with GroupName=\$grpNameKey not found. Invalid user.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.

Table 1 **Directory Message Improvements (continued)**

Old Message	Condition	Changed Message	Solution
Default end user group \$ccmEndUserGroupName not found in the list of default groups	End user group was not available in the default migration group.s	No change.	Contact TAC.
PersonalAddressBook: EndUser PKID not found for userName = \$pabUserName, PAB-DN=\$pabDN	Either the user does not exist in the directory or has been tagged invalid.	PersonalAddressBook: EndUser \$pabUserName not found. Invalid user. PAB-DN=\$pabDN	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
PersonalAddressBook: \$pabUserName has origNickname greater than 50 characters long. \$origNickname	PersonalAddressBook: PAB user has nickname that is greater than 50 characters long.	No change.	Change the nickname to less than 50 characters; else the nickname will be changed during migration.
PersonalPhoneBook: EndUser not found for \$pabFastDialUserName	Either the user does not exist in the directory or has been tagged invalid.	No change.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
PersonalPhoneBook: for user \$pabFastDialUserName, contact=\$pabContact has personalFastDialIndex beyond 0 to 500 range. Ignoring this contact	The fast dial index goes beyond 500 range.	Personal Fast Dial Index for user \$pabFastDialUserName, contact \$pabContact is beyond 0 to 500 range. Ignoring the user	Modify the index to a range of 0-500.
PKID not found in database for Device or DeviceProfile=\$devValue for user=\$userKeyVal	The device that is found in the directory does not exist in the database.	Device or DeviceProfile=\$devValue for user=\$userKeyVal not found in the database ALSO put a check for if value = ""	Verify that the user is associated to a valid device or a device profile.

Table 1 **Directory Message Improvements (continued)**

Old Message	Condition	Changed Message	Solution
KEY:\$lcKey User cannot be repaired. AppProfileOwner=\$newOwner and \$userSearchAttr=\$lcKey	The respective profiles do not exist for this user. The profile that is being pointed to by the user is owned by a user that does not exist or is invalid.	\$lcKey user is invalid. A user that does not exist or is invalid owns the profiles for this user. \$newOwner owns the profiles.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
Number of orphan entries of \$cleanObjClassName = \$orSize	Message indicates the number of orphan entries.	This should only get thrown for users and not for profiles because the customer does not need to know about profiles. For profiles, one can just trace the list.	See the solutions that are provided for individual users.
Number of duplicate entries found in \$csvObjectFileName = \$dupSize	Multiple users exist with the same id; or multiple profiles exist with the same owner.	No change.	The duplicate entries get removed automatically in the tar ball. One needs to remove them manually from the directory. The list follows.
\$cleanObjClassName for key \$name	None.	No change.	None.
Number of duplicate entries found in \$csvObjectFileName = \$dupSize	Multiple users exist with the same id; or multiple profiles exist with the same owner.	No change.	The duplicate entries get removed automatically in the tar ball. One needs to remove them manually from the directory. The list follows.
\$name is duplicate.	None.	No change.	None.
LDAP Bind Failed ErrorCode = \$bindResult->error LDAP_URL = "\$.Suri->host_port. LDAP_HOST = "\$.Suri->host. LDAP_PORT = "\$.Suri->port. LDAP_DN = \$MgrDN	LDAP bind failed.	No change.	See the LDAP error.

Table 1 **Directory Message Improvements (continued)**

Old Message	Condition	Changed Message	Solution
DN:\$dnEntry has SingleValueAttribute:\$AttributeName pointing to an invalid user:DN=\$dnStr	The value that is stored in a directory attribute is invalid.	The SingleValue Attribute \$AttributeName of the DN \$dnEntry contains a user \$dnStr that does not exist in the directory or is tagged invalid.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
DN:\$dnEntry has MultivaluedAttribute:\$AttributeName pointing to an invalid User DN:\$dnStr;	The value that is stored in a directory attribute is invalid.	TheMultivalues Attribute \$AttributeName of the DN \$dnEntry contains a user \$dnStr that does not exist in the directory or is tagged invalid.	Verify that the user exists in the directory and is a valid Cisco Unified Communications Manager user; that is, User with profiles.
\$EUID has an invalid numplan (\$DnorP) - it does not exist in the database\nIgnoring the user	Primary Extension for this user is invalid. It does not exist in the database.	Numplan (\$DnorP) for User \$EUID is invalid. Ignoring the user.	Associate the user with a valid primary extension/numplan.
validateOrphan: UserID:\$UserID: Attribute ciscoatUserProfileString is found empty.	The user does not contain a valid pointer to the User profile.	UserID:\$UserID: is invalid - Attribute ciscoatUserProfileString is found empty.	Verify that the user is a valid Cisco Unified Communications Manager user.
validateOrphan: UserID:\$UserID: Entry UserProfile is not found in search	The User profile for the user does not exist..	UserID:\$UserID: is invalid - User profile not found in LDAP search.	Verify that the user is a valid Cisco Unified Communications Manager user.
validateOrphan: UserID:\$UserID: Attribute ciscoatAppProfile is found empty.	The user does not contain a valid pointer to the Application profile.	UserID:\$UserID: is invalid - Attribute ciscoatAppProfile is found empty.	Verify that the user is a valid Cisco Unified Communications Manager user.
validateOrphan: UserID:\$UserID: Entry ApplicationProfile is not found in search	The Application profile for the user does not exist.	UserID:\$UserID: is invalid - Application profile not found in LDAP search.	Verify that the user is a valid Cisco Unified Communications Manager user.

CER Improved Messages

The following improvements are made in the CER areas:

"Error Messages Details

"Fixed logical errors

"Misc. minor corrections

Added the CSV file name in the error message - When parsing the CSV file, if the number of columns does not match number of column types, then an error message is logged, this error message was not having the CSV file name. Added the CSV file name in the error message.

Added error messages if not able to create "cer" and "exported" directories - CER DMA creates two directories named "cer" and "exported", there was no check to see whether the directory creation was successful or not. Added checks to see if the directory creation was successful or not. If directories are not created then an error message is logged.

Misc. Minor Corrections

Following messages are changed to specify the real cause:

Table 0-1

Old Error Message	New Error Message
Failure, CER Export	Failure, CER Export failed because of missing DllModifyCERSchema function
Failure, CER Exp	Failure, Export of CER database failed
Failure, Registry	Failure, Unable to retrieve value for DBConnection0 from registry
Failure, Failed to create cer DB for windows based W1 migration Verification	Failure, Failed to create cer DB for windows based W1 migration Verification. Please make sure that CSA is not running and there are no other IDS data base sessions opened

Proper Return Code Sent To the DMA Framework

During DMA export and validation phases, the DMA framework launches separate processes to invoke the underlying components' .exe 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.

Using this information the framework can determine if there are fatal issues encountered and if 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 are:

- 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 if 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.

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 6.1(2), the target Unified CM upgrade version is release 6.1(2). So, this field displays 6.1.2 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 CUCM 6.1.2 respin becomes a reality in the future, the logic will work and the customer can use DMA 6.1(2) to upgrade to the Unified CM Release 6.1.2 respin release.

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 That Are Resolved in Data Migration Assistant 6.1\(2\), page 10](#)
- [Resolved Caveats, page 11](#)
- [Open Caveats, page 11](#)

Caveats That Are Resolved in Data Migration Assistant 6.1(2)

This section contains a partial list of the defects that are resolved in this release of Data Migration Assistant. You can obtain a full list by reviewing and implementing the information in [“Using Bug Toolkit” section on page 11](#)

[CSCsm60491](#) and [CSCso00688](#) - DMA uninstall improvement

[CSCs157662](#) - Need to add Product Deployment field in platformConfig.xml file

[CSCs159339](#) - Need exists for user to see the file on tape - DMA backup tar files

[CSCs161200](#) - DMA does not check to see if the destination is writeable/accessible

[CSCs152704](#) - DMA cannot store the .tar file to a mapped drive letter

[CSCs185046](#) - URL displayed on the DMA result status.html page refers to Unified CM information

[CSCs185071](#) - DMA backup on CER does not update the results in status.html GUI properly

[CSCs185126](#) - DMA backup on CER132 box shows validation failed

Resolved Caveats

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 2](#) describes possible unexpected behaviors in Data Migration Assistant.



Tip

For more information about an individual defect, click the associated Identifier in [Table 2](#) 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 11](#).



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 2 Open Caveat as of April 28, 2008

Identifier	Headline
CSCso69307	DMA install does not populate SIP profile field on SIP trunks.
CSCs185152	Errors Log button opens an error file that does not display any errors.

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.

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2008 Cisco Systems, Inc. All rights reserved.

Printed in the USA on recycled paper containing 10% postconsumer waste.

