Release Notes for Data Migration Assistant (DMA) 5.0(4)

July 5, 2006

These release notes describe new documentation and caveats for DMA 5.0(4).

Contents

These release notes discuss the following topics:

Introduction

The Cisco Data Migration Assistant (DMA) assists you with the first step in migrating Cisco Unified CallManager 4.0 or 4.1 data to Cisco Unified CallManager 5.0 by backing up Cisco Unified CallManager 4.0 or 4.1 data in a format that Cisco Unified CallManager 5.0 can read. Cisco Unified CallManager 4.x runs in a Windows environment, and Cisco Unified CallManager 5.0 runs in a Linux environment, so the Cisco DMA exports Windows-based data to a format that Cisco Unified CallManager 5.0 can import. The Cisco Unified CallManager 5.0 installation process converts the backed-up data as needed for Cisco Unified CallManager 5.0, which completes the data migration.

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

CISCO SYSTEMS

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

You must install and run the Cisco DMA on the Cisco Unified CallManager publisher server before you upgrade to Cisco Unified CallManager 5.0. If you make any Cisco Unified CallManager configuration changes after running the Cisco DMA, the system does not retain these changes when you upgrade.

For more information

For more information on Data Migration Assistant 5.0(2a), refer to the following document:

- *Data Migration Assistant 5.0(4) User Guide*

Caveats

The following sections contain information on how to obtain the latest resolved caveat information and descriptions of open caveats of severity level 1, 2, and 3.

Caveats describe unexpected behavior on a Cisco Unified CallManager server. Severity 1 caveats represent the most serious caveats, severity 2 caveats represent less serious caveats, and severity 3 caveats represent moderate caveats.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Unified CallManager Release 5.0(3) 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 (Cisco Connection Online) 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.

This section includes the following topics:

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

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

To use Bug Toolkit, follow this procedure.

Procedure

Step 1　To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Log on with your Cisco.com user ID and password.

Step 2   Click the **Launch Bug Toolkit** hyperlink.

Step 3   If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco Unified CallManager, go to the "Search for bugs in other Cisco software and hardware products" section, and enter Cisco Unified CallManager in the Product Name field. Alternatively, you can scroll through the product name list and click Cisco Unified CallManager.

Step 4   Click **Next**. The Cisco Unified CallManager search window displays.

Step 5   Choose the filters to query for caveats. You can choose any or all of the available options:

a.   Choose the Cisco Unified CallManager version:

- Choose the major version for the major releases (such as, 5.0, 4.1, 4.0).

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information; for example, choosing major version 5.0 and revision version 3 queries for release 5.0(3) caveats.

  A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

b.   Choose the Features or Components to query; make your selection from the "Available" list and click Add to place your selection in the "Limit search to" list.

- To query for all Cisco Unified CallManager caveats for a specified release, choose "All Features" in the left window pane.

![Note icon]

Note   The default value specifies "All Features" and includes all of the items in the left window pane.

- To query only for Cisco Unified CallManager-related caveats, choose "ciscocm" and then click **Add**.
- To query only for phone caveats, choose "ciscocm-phone" and then click **Add.**
- To query only for gateway caveats, choose "voice-gateway" and then click **Add**.

c.   Enter keywords to search for a caveat title and description, if desired.

![Note icon]

Note   To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

d.   Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the **Fixed** check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e.   Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by submitting another query and using different criteria.

- You can save your query for future use. See the "Saving Bug Toolkit Queries" section on page 4.

✎ **Note** For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

Step 1 Perform your search for caveats, as described in the "Using Bug Toolkit" section on page 2.

Step 2 In the search result window, click the **This Search Criteria** button that displays at the bottom of the window.

A new window displays.

Step 3 In the Name of saved search field, enter a name for the saved search.

Step 4 Under My Bug Groups, use one of the following options to save your defects in a bug group:

- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
- To create a new group for this saved search, click the **Create new group named:** radio button and enter a group name.

✎ **Note** This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the My Stuff link to see a list of all your bug groups.)

Step 5 Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include
  - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
  - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
- **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.

Step 6 To save your changes, click **Save**.

Step 7 A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

Note For complete Cisco Unified IP Phone firmware release note information, refer to the applicable firmware release notes for your specific model IP phone at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/.

Open Caveats

Table 1 describes possible unexpected behaviors 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 CallManager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified CallManager 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 CallManager maintenance releases may not be as clearly identified.

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco Unified CallManager release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 003.003(003.144) = Cisco CallManager Release 3.3(4)
- 004.000(000.123) = Cisco Unified CallManager Release 4.0(1)
- 004.000(001.008) = Cisco Unified CallManager Release 4.0(2)
- 004.001(002.201) = Cisco Unified CallManager Release 4.1(3)

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" section on page 2.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). 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://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

.

Table 1   Open Caveats

Identifier	Headline
CSCsd04482	DMA does not install Informix correctly on CSA enabled system.
CSCse43227	DMA database verification has run for 5+ days with out completion.
CSCse24397	DMA verifcation of database in IDS failed due to MLPP errors.
CSCse69771	Data validation process cannot be completed. When checking the ODBC data source connection, the return result fails.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have.PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip   We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note   Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command

output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation" section.