



Release Notes for Cisco Unified MobilityManager Release 1.2(2)

August 30, 2006

These release notes describe limitations and restrictions, important notes, caveats, and documentation updates for Cisco Unified MobilityManager Release 1.2(2).

Contents

- [Related Documentation, page 2](#)
- [Installation Notes, page 2](#)
- [Important Notes, page 3](#)
- [Limitations and Restrictions, page 5](#)
- [Caveats, page 7](#)
- [Obtaining Documentation, page 10](#)
- [Documentation Feedback, page 11](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Cisco Product Security Overview, page 12](#)
- [Obtaining Technical Assistance, page 14](#)
- [Obtaining Additional Publications and Information, page 16](#)

Related Documentation

Cisco Unified MobilityManager Documentation

Refer to the documentation set for Cisco Unified MobilityManager for detailed configuration and use information. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/1_2/index.htm

Cisco Unified IP Phone Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified CallManager version. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

Cisco Unified CallManager Documentation

Refer to the Cisco Unified CallManager Documentation Guide and other publications specific to your Cisco Unified CallManager version. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

Installation Notes

The following installation notes apply to Cisco Unified MobilityManager Release 1.2(2):

- Cisco Unified MobilityManager should be restarted whenever Cisco Unified CallManager is upgraded.
- If you are upgrading from Cisco Unified MobilityManager Release 1.2(1), you can perform a software upgrade.

- If you are upgrading from Cisco Unified MobilityManager Release 1.1(2), you must do a new install when upgrading Cisco Unified MobilityManager. The new install must be on a system with the same IP address as the system used for Cisco Unified CallManager 1.1(1). Instructions are in the *Cisco Unified MobilityManager Installation Guide*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/index.htm

Important Notes

This section includes information about support for the Cisco IP Telephony Platform. See the *Cisco IP Telephony Platform Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/1_2/admins/p1at1_2/index.htm

The following Cisco IP Telephony Platform GUI options are *not* supported:

- Clusters
- SMTP
- Security: Certificate Management and IPSec Management



Note

Cisco Security Agent (CSA) is supported in Cisco Unified MobilityManager Release 1.2(2).

The following platform CLI commands are *not* supported:

- **delete ipsec**
- **delete smtp**
- **file delete tftp**
- **file dump tftp**
- **file get tftp**
- **file list tftp**
- **file search tftp**
- **file tail tftp**

- **file view tftp**
- **run sql**
- **set ipsec**
- **set password security**
- **set smtp**
- **set trace**
- **set web-security**
- **show firewall**
- **show ipsec**
- **show perf**
- **show registry**
- **show risdb**
- **show smtp**
- **show trace**
- **show web-security**
- **unset ipsec**
- **utils service**
- **utils sftp**
- **utils snmp**
- **utils soap**

The following commands are the only **show tech** commands that are supported:

- **show tech all**
- **show tech network**
- **show tech runtime**
- **show tech system**

The following CSA commands are new:

- **utils csa**
- **utils csa start**
- **utils csa status**
- **utils csa stop**

The following Database Storage Manager (DSM) commands are new:

- **utils dsm**
- **utils dsm start**
- **utils dsm status**

Limitations and Restrictions

This section describes limitations and restrictions that apply to Cisco Unified MobilityManager Release 1.2(2).

Cryptographic Features

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.

Supported MCS Servers

Cisco Unified MobilityManager Release 1.2(2) requires that you use one of the following MCS servers:

- MCS-7815-I1 (3.0 GHz)
- MCS-7815-I2
- MCS-7825-H1 (3.4 GHz)
- MCS-7825-H2
- MCS-7825-I2
- MCS-7835-H1 (3.4 GHz)
- MCS-7835-H1 retrofit
- MCS-7835-I1 (3.4 GHz)
- MCS-7835-I1 retrofit
- MCS-7845-H1 (3.4 GHz dual processor)
- MCS-7845-H1 retrofit
- MCS-7845-I1 (3.4 GHz dual processor)
- MCS-7845-I1 retrofit



Note

Cisco Unified MobilityManager Release 1.2(2) does not currently support the MCS-7825-I1 server.

Caveats

This section lists product caveats for Cisco Unified MobilityManager Release 1.2(2).

Open Caveats for Release 1.2(2)

Table 1 lists the open caveats for Cisco Unified MobilityManager Release 1.2(2).

Table 1 **Open Caveats**

Identifier	Headline and Bug Toolkit Link
CSCsc06315	System parameter default values shown in the help page are incorrect http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc06315
CSCsc69509	The join feature does not work for mobile pickup calls with the Select option http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc69509
CSCsd42377	Adding a user requires that AXL server settings be configured on the System page http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd42377
CSCsd52890	MTP should be checked in the SIP trunk to have a voice path in the mobile phone http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd52890
CSCsd76348	It is necessary to reboot Cisco Unified MobilityManager for restore to work after changing the network domain http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd76348
CSCsd99095	AXL device lookup fails with special characters in password http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd99095
CSCse31107	CTI Userids changed to all uppercase http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31107
CSCse31316	User cannot update the shared ports and out port users http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31316
CSCse34483	Upgraded from 121 to 122, CLI show hardware shows UNKNOWN http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse34483

Table 1 **Open Caveats (continued)**

Identifier	Headline and Bug Toolkit Link
CSCse34538	Cannot view file using CLI file view activelog http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse34538
CSCse36706	LDAP directory Admin password in plain text in web source file http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse36706
CSCse46504	Intermittent web page exception after click DRS Log Off http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse46504
CSCse51453	SNMP Description shows wrong platform type http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse51453
CSCse55253	During fresh install, DVD found/media check shown two or three times http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse55253
CSCse55259	No progress indication during the last 20 minutes of software upgrade http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse55259
CSCse58976	Delete account does not work http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse58976
CSCse97812	SNR / Mobility Manager. IOS Error "vxml version 1.0 not supported" http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse97812
CSCse98352	Multiple Shared Line User Links should be used for bulk calls http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse98352

Resolved Caveats

Table 2 lists the resolved caveats for Cisco Unified MobilityManager Release 1.2(2).

Table 2 **Resolved Caveats**

Identifier	Headline and Bug Toolkit Link
CSCsc70192	If Cisco Unified CallManager 5.0.1 is connected to an H.323 gateway, Call Park interaction with Cisco Unified MobilityManager cell pickup does not work properly http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc70192
CSCsc86924	Cisco Unified MobilityManager does not verify that the LDAP information that is entered works http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc86924
CSCsd45744	Cisco Unified MobilityManager SNMP provides the wrong information for sysObjectID and sysName http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd45744
CSCsd45760	Cisco Unified MobilityManager should provide MIB configuration information for system contact and location http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd45760
CSCsd48604	A SQLException occurs in the log following successful login to Cisco Unified MobilityManager administration http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd48604
CSCsd55789	The show account fails after changing the IP address from the GUI right after a fresh install http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd55789
CSCsd56373	Users should be prompted for the Directory User Setting whenever an older version of Cisco Unified MobilityManager is used http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56373
CSCsd56406	The CLI command show/set web-security pair should be either supported or removed http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56406

Table 2 **Resolved Caveats (continued)**

Identifier	Headline and Bug Toolkit Link
CSCsd56408	CLI command utilities network capture eth0/eth1 does not work if CSA is on http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56408
CSCsd56410	A CLI command set for password security should be added http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56410
CSCsd56639	The Backup Scheduler should give a warning if no features are selected http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56639
CSCsd61648	When multiple CTI links are out of service, an alarm is created only for the last out of service link http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd61648
CSCsd68388	The show cert trust command is not supported in the CLI http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd76348

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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

© 2006 Cisco Systems, Inc. All rights reserved.