



Release Notes for Cisco MobilityManager Release 1.1(1)

Revised: October 10, 2005, OL-8425-01

These release notes describe limitations and restrictions, important notes, caveats, and documentation updates for Cisco MobilityManager Release 1.1(1).

Contents

- [Limitations and Restrictions, page 2](#)
- [Important Notes, page 2](#)
- [Caveats, page 4](#)
- [Documentation Updates, page 6](#)
- [Obtaining Documentation, page 8](#)
- [Documentation Feedback, page 9](#)
- [Cisco Product Security Overview, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 14](#)



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

© 2005 Cisco Systems, Inc. All rights reserved.

Limitations and Restrictions

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.

Important Notes

This section includes notes regarding Cisco MobilityManager Release 1.1(1).

DNS

To use DNS, the IP address of the DNS server must be correct and the Cisco MobilityManager server hostname must be configured in the DNS server. If DNS is not used, then the administrator should verify that Cisco MobilityManager hostname settings are correct in the Cisco IPT Platform Administration pages: Settings > Host Settings.

Minimum Cellular Phone Ring Timer

The default of the Minimum Cellular Phone Ring Timer parameter is 1500 milliseconds. If you experience dropped inbound calls in cell phones that are configured as remote destinations, try adjusting them to suit your cell phone requirements for voice mail.

Access to Interfaces During Upgrade

Cisco MobilityManager administration pages, user pages, and Mobile Voice Access are unavailable during post-installation script execution in system upgrade. This is due to the IDS database shutdown required to install the database in the inactive partition.

SNMP Settings

The System Configuration page contains these new fields located under the SNMP settings:

- SNMP Community String
- SNMP Version

Server IP Address Change

When changing the IP address of the Cisco MobilityManager server after installation, you must open the Cisco IPT Platform Administration application and verify that the Host settings reflect the new IP address. If the host settings do not reflect the new IP address, you must perform these tasks:

1. Update the host IP address in the Platform pages and restart the Cisco MobilityManager server.
2. In the H.323 Gateway configuration, reload the Cisco MobilityManager application using the command:

call application voice load *<application name>*.

Internal Extension Calls

When a Mobile Connect call is placed from one internal extension call, only the internal extension is presented as the caller ID. If an H.323 gateway is used, then this can be solved using translation patterns.

Caveats

This section lists product caveats pertaining to Cisco MobilityManager Release 1.1(1).

Open Caveats for Release 1.1(1)

- CSCsa66121
Outgoing calls to remote destination fail when a CTI Route Point is shared by two Shared line users. SNR sends two outgoing calls but none of the calls gets connected.
- CSCsb67632
If a Backup/Restore fails due to an IP address that is not reachable from the Cisco MobilityManager server, the error message displayed on the Back/Restore page will be inconsistent with the error in the log file (tar.log or untar.log). A GUI display of Server Unknown is the same as No route to the host shown in the log file.
- CSCsb73789
If the device name is configured on the User Information page and the AXL server IP or user name or password is incorrect, then Cisco MobilityManager cannot connect to the AXL server for device name validation. In this case, if the administrator updates the user page and clicks **Save**, the page will time out with a message of “The page cannot be displayed” being displayed due to the AXL response failure. To solve the problem, do not configure the device name, or be sure to configure a valid AXL server IP and user name and password.
- CSCsa74903
If a caller uses Using Mobile Voice access to make a call to an internal line that is busy, the call will be dropped without a busy tone.
- CSCsb75274
If cell pickup is unsuccessful, a Cancel option is displayed on the phone. The phone does not display Pickup again unless the user manually presses Cancel and tries again.

- CSCsb76332

The Cisco MobilityManager server may hang during boot up. When this occurs, the server is in a state where it cannot continue startup routines or be gracefully shut down. If you restore IP connectivity to the rest of the network, the boot sequence will continue after a few minutes.

- CSCsb76617

Pickup fails intermittently if one of the remote destination is an un-allocated number and if other three are valid remote destinations. If the un-allocated number is removed from the configuration, then cellular phone pickup will work.

- CSCsb79997

The device name for the user's phone should contain only characters dots, numbers, letters, dashes, and underscores.

- CSCsb85176

The SNMP community string should not have any blank spaces. If the string contains blanks, SNMP traps will not be received by the target machine.

- CSCsb85601

Users should not add new remote destinations from the User Profile configuration pages when there are no user groups configured for that user, even though the Administration application currently permits this.

- CSCsa96106

If the remote destination (cellular phone) is in a different area code than the user's desk phone, then the user may intermittently experience a slight audio delay for 2 to 3 seconds when picking up an incoming Mobile Connect call.

- CSCsa96776

When using the Join feature, if the first call is in the talking state, Pickup will not work. To prevent this, you must always put the first call on Hold and then invoke Join.

- CSCsb99515

The Use Secured Auto JTAPI Update parameter on the System Parameters page (System > System Parameter) should always be set to "no." HTTPS connection is not supported by Cisco CallManager for the

CCMPluginsServer folder, and Cisco MobilityManager always uses HTTP for the connection to Cisco Call Manager to download the jtapi.jar file. Therefore, the parameter should be set to “no.”

- CSCsc10575

Cisco MobilityManager will not be able to extend calls to cellular phones if FXO ports are used in the gateway to connect to the PSTN. The call to the cellular phone is answered too quickly, and Cisco MobilityManager assumes that the cell phone voice mail picked up the call and pulls it back. In this case, it is recommended that you use PRI to connect to the PSTN.

Documentation Updates

This section contains documentation updates.

Errors

The errors in this section apply to the *Cisco MobilityManager Installation Guide*.

CTI Ports for Outgoing Calls

In the section “Creating a Pool of CTI Ports for Outgoing Calls,” this step:

In the Partition pull-down list box, choose the partition that you created in “Creating a Partition for the Route Point” section on page 18.

should read

In the Partition pull down list box, choose the partition for the outgoing ports. This should not be the partition that was created for the CTI route point.

H.323 Configuration

In the section “Configuring a H.323 Gateway for System Remote Access,” this step is not required:

- Step 6** Add a dial-peer to make calls to the public service telephone network (PSTN) from the enterprise. This is used to play announcements after the System Remote Access Call Take back Timer expiration.

Sample configuration:

- dial-peer voice 3 pots
- destination-pattern T
- port 1/0:23

Omissions

The item in this section applies to the *Cisco MobilityManager Installation Guide*. In the section “Setting Parameters for the Mobile Connect IP Phone Service in Cisco CallManager,” step 10 states:

Step 10 Enter **dn** as the parameter name.

Note that the **dn** parameter is case-sensitive. It must be specified as lower case.

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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 send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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>

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, 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. (0709R)

© 2005 Cisco Systems, Inc. All rights reserved.

