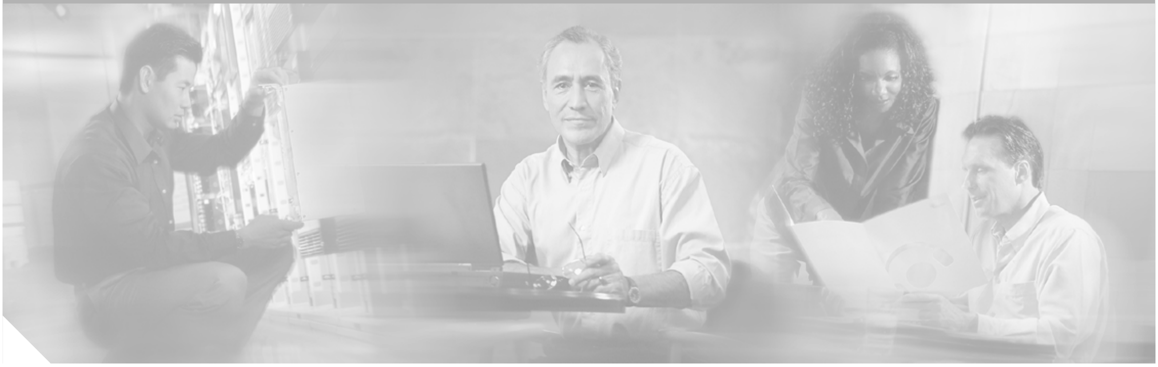

Cisco MobilityManager Administration Guide

Release 1.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7886-01

Cisco MobilityManager Administration Guide

CONTENTS

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

The preface covers these topics:

Purpose

The *Cisco MobilityManager Administration Guide* provides instructions for administering Cisco MobilityManager using the Cisco MobilityManager web interface.

Audience

The *Cisco MobilityManager Administration Guide* provides information for network administrators who are responsible for managing the Cisco MobilityManager. This guide requires working knowledge of Cisco CallManager administrative procedures and of telephony and IP networking technology.

Organization

This guide is organized as follows:

Chapter	Description
Chapter 1, "An Overview of Cisco MobilityManager"	Explains the features and benefits of the Cisco MobilityManager solution and how to access the administrative web interface.
Chapter 2, "Getting Started"	Explains how to set up your system to use Cisco MobilityManager and how to add user accounts.
Chapter 3, "System Configuration"	Explains how to set up the Cisco MobilityManager parameters for call handling.
Chapter 4, "Serviceability Configuration"	Explains how to display alarms, measurements, and debugging information.

Chapter	Description
Chapter 5, "File Export"	Explains how to save and export system and call information.
Chapter 6, "Platform Administration"	Explains how to administer the Cisco MobilityManager server platform using the IPT Platform Administration web pages.

Related Documentation

Refer to the following documents for further information about related Cisco IP telephony applications and products:

Cisco MobilityManager

These Cisco MobilityManager documents are located at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

- *Cisco MobilityManager Quick Start Guide*
- *Cisco MobilityManager Installation Guide*
- *Cisco MobilityManager User Guide*
- *Release Notes for Cisco MobilityManager*

Cisco CallManager

These Cisco CallManager documents are located at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

- *Installing Cisco CallManager Release 4.1(3)*
- *Upgrading Cisco CallManager Release 4.1(3)*
- *Release Notes for Cisco CallManager Release 4.1(3)*
- *Cisco CallManager System Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*

- *Cisco CallManager Features and Services Guide*
- *Troubleshooting Guide for Cisco CallManager*
- *Bulk Administration Tool Guide for Cisco CallManager*
- *Cisco CallManager Compatibility Matrix*

Other

This Cisco IP Telephony document is located at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm

- *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*
- *Cisco IP Telephony Solution Reference Network Design Guide*

Conventions

This document uses the following conventions.

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.

Convention	Description
italic screen font	Arguments for which you supply values are in *italic screen* font.
⟶	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

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

An Overview of Cisco MobilityManager

This chapter describes Cisco MobilityManager and includes these sections:

Definitions

Table 1-1 lists definitions of important terms used in this guide.

Table 1-1 Terms and Definitions

Term	Definition
Caller ID	Phone number that appears on the display of the receiving phone when a call is made from the remote destination.
Group	Record that ties together a set of phone lines and remote destinations for the user. Identified by Group ID. Currently one group can be added per user.
Line appearance	Desktop phone line or extension for the user. Identified by line number. Currently one line appearance can be added per user.
Mobile Connect	Set of features that enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Connect features are supported by Cisco MobilityManager.
Mobile Voice Access	An integrated voice response (IVR) system used to initiate Mobile Connect calls and to activate or deactivate Mobile Connect capabilities.
Remote destination	Cellular phones that are available for Mobile Connect responses and pickup, plus other phones that are used to reach Mobile Voice Access.
User Profile	Set of records that defines a user account, identified by Mobile Voice Access User ID. The group, line appearance, and remote destinations are part of the user profile.

Cisco MobilityManager Solution

Cisco MobilityManager is an enterprise application server that provides Mobile Connect functionality in conjunction with Cisco CallManager, Unity, and other IP communications applications. Mobile Connect refers to the set of features that includes the ability to answer incoming calls on the desktop phone or cellular phone, to pick up in-progress calls on the desktop phone or cellular phone without losing the connection, and to originate enterprise calls from the cellular phone.

Together with Cisco CallManager, Cisco MobilityManager controls call routing and device mobility between enterprise desktop IP phones and cellular and other remote phones. Cisco MobilityManager is provided as a software application on compatible Cisco servers. A web interface is available for administrative access and for users to administer their person profiles.

Cisco MobilityManager is part of Cisco AVVID (Architecture for Voice, Video and Integrated Data) and is compatible with enterprise public service telephone network (PSTN), WAN, LAN, and wireless LAN infrastructures.

The following components are required to implement the full Cisco MobilityManager solution:

- Voice-enabled IP network, including LAN and PSTN voice gateways
- Enterprise CPE-based IP telephony and messaging system, including Cisco CallManager, Cisco Unity voice mail applications, and Cisco IP Phone 79xx Series
- Cisco MobilityManager
- Existing cellular phones devices and other remote phone endpoints

Note Existing cellular phones can be used with the Cisco MobilityManager with no modification to the cellular phones or cellular network. Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) cellular phones are compatible with the Cisco MobilityManager.

Related Topics

- Key Features and Benefits, page 1-4
- Use Case Examples, page 1-5
- Administrative Web Interface, page 1-9

- Where to Find More Information, page 1-12

Key Features and Benefits

The Cisco MobilityManager enables more flexible management of enterprise and cellular telephone communications and provides these benefits:

- Simultaneous desktop ringing—Incoming calls ring simultaneously on the IP phone extension and the designated mobile handset.When the user answers one line, the unanswered line automatically stops ringing. Users can choose the preferred device each time a call comes in.
- Desktop call pickup—Users can switch between desktop phone and cellular phone during an active call without losing the connection. Based on the needs of the moment, they can take advantage of the reliability of the wired office phone or the mobility of the cellular phone.
- Single enterprise voice mailbox—The enterprise voice mail box can serve as single, consolidated voicemail box for all business, including calls to the desktop or configured remote devices. Incoming callers have a predictable means of contacting employees and less time is required for users to check multiple voice mail systems.
- System remote access—A user’s cellular phone can initiate calls as if it were a local IP PBX extension. User-initiated calls can take advantage of local voice gateways and WAN trunking, and the enterprise can track employee call initiation.
- Allowed Caller and Blocked Caller filters—Users can restrict the set of callers that cause a designated remote destination to ring on an incoming call (Allowed Caller filter) or for which the remote destinations do *not* ring on an incoming call (Blocked Caller filter).
- Caller ID—Caller ID is preserved and displayed on all calls. Users can take advantage of Mobile Connect with no loss of expected IP phone features.
- Remote on/off control—Users can turn their mobility features on or off from the cellular phone using Mobile Voice Access or from the user configuration pages, assuring flexibility in how mobility is managed.
- Call tracing—Detailed Mobile Connect calls are logged, providing information to help the enterprise optimize trunk usage and debug connection problems.

- Security and privacy for Mobile Connect calls—During an active Mobile Connect call, the associated desktop IP phone is secured. Access to the call from the desktop is eliminated as soon as the cellular connection becomes active, precluding the possibility of an unauthorized person listening in on the call that is bridged to the cellular phone.

Related Topics

- Cisco MobilityManager Solution, page 1-3
- Use Case Examples, page 1-5
- Administrative Web Interface, page 1-9
- Where to Find More Information, page 1-12

Use Case Examples

Cisco MobilityManager supports these use cases:

- Receiving an outside call on desk or cellular phone—An outside caller dials the user's desktop extension. The desktop phone and cellular phone ring simultaneously. When the user answers one of the phones, the other phone stops from a desktop telephone to a cellular phone—The user can switch from the desktop phone to cellular phone during a call without losing the connection. Switching is supported for incoming and outgoing calls.
- Moving back from a cellular phone to a desktop phone—If a call was initiated to or from the desktop phone and then shifted to the cellular phone, the call can be shifted back to the desktop phone.
- Initiating a mobility call from a remote phone, such as a cellular phone—Users can use Mobile Voice Access to initiate calls from a cellular phone as if dialing from the desktop phone.
- Moving from a cellular phone to a desktop phone during a cellular-phone initiated call—If the user has initiated a call from a cellular phone using Mobile Voice Access, the user can shift to the desktop phone during the call without losing the connection, and can shift back again as needed.

Related Topics

- Cisco MobilityManager Solution, page 1-3
- Key Features and Benefits, page 1-4

- Administrative Web Interface, page 1-9
- Where to Find More Information, page 1-12

Usage Limitations

Cisco MobilityManager is designed to manage a maximum of one call at a time for each configured line appearance (extension). This section describes the system response based on several calling scenarios involving Extension “A,” “B,” and “C.” In each scenario, Extension A is configured for Mobile Connect services and Mobile Voice Access, and the cellular phone is configured as a remote destination.

Scenario 1

A is idle when B calls A. A can pick up the call on the cellular phone.

Scenario 2

A makes a call to C. While the call is in progress, B calls A, who answers the call on the desktop phone. A can pick up the C call on the cellular phone, but cannot pick up B’s call on the cellular phone, since Mobile Connect services are being used for the C call.

Scenario 3

B calls A, who picks the call up on the cellular phone. While the call is in progress, C calls A, who answers on the desktop phone. A now ends B’s call and continues with C. Mobile Connect services will be available for the next incoming call to A.

Scenario 4

B calls A, who picks the call up on the cellular phone. While the call is in progress, C calls A, who answers on the desktop phone. A now ends C’s call and continues with B. The B call is still using Mobile Connect services, so no other call can use the service until the B call is terminated.

Scenario 5

A uses a cellular phone to make a Mobile Voice Access call. While the call is in progress, C calls A's extension. The call will not be extended to the cellular phone, since A was using Mobile Voice Access when the call from C came in. After A hangs up the Mobile Voice Access call, Mobile Connect services can be applied to the next incoming call.

Compatibility with Cisco CallManager and Related Devices and Services

Cisco MobilityManager is integrated with Cisco CallManager. Most of the standard Cisco CallManager features are compatible with Cisco MobilityManager and related devices and services, except as indicated here:

- To use Mobile Connect features, you must first disable the Auto Call Pickup feature in Cisco CallManager.
- The Cisco CallManager Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with Mobile Voice Access. JAVA telephony programming interface (JTAPI) does not support the events required for FAC/CMC.
- In order for Cisco MobilityManager to support different types of codecs, a transcoder must be configured in Cisco CallManager for shared line CTI ports.
- Mobile Connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Mobile Connect features are disabled for that call.
- Mobile Connect services do not extend to video calls. A video call received at the desktop phone cannot be picked up on the cellular phone.
- Remote destinations must be Time Division Multiplex (TDM) devices. You cannot configure IP phones within a Cisco CallManager cluster as remote destinations.

- Mobile Connect services are available only to directory numbers (DNs) that are in the same partition as the Shared Line CTI User. If the same DN is used in two different partitions, service is only extended to the DN in the same partition as the Shared Line CTI User.
- CDR Analysis and Reporting (CAR) support is not available with Cisco MobilityManager.
- The H.323 gateway does not support failover of Cisco CallManager. If the primary Cisco CallManager goes out of service for some reason and the secondary takes over, the in-progress Mobile Connect calls will be dropped.
- When the outbound H.323 dial-peer is down or is unavailable and remote access calls are attempted, the CTI ports are not released after the call is completed. Although the calls are unsuccessful and are properly released, some CTI ports become unusable and are not released by Cisco MobilityManager. To avoid this problem, disable the System Remote Access parameter when H.323 dial-peers are shut down or are unavailable.
- If two or more users share the same extension number, the parameters configured on the Line Appearances page correspond to the most recent update. Only one set of parameters is stored in Cisco MobilityManager for each extension, whether or not the extension is shared by multiple users.
- Users cannot access Meet-Me using Mobile Voice Access.
- Cisco MobilityManager does not support QSIG (Q Signaling) path replacement.
- When configuring CTI ports for outgoing calls, make sure the Media Resource group for the CTI Ports does not include Music-On-Hold (MOH) servers.

Administrative Web Interface

This section explains how to access the Cisco MobilityManager administration application from a web browser running on your PC.

- Cisco MobilityManager Solution, page 1-3
- Web Browsers, page 1-9
- Using Internet Explorer with Cisco MobilityManager Administration, page 1-10

Web Browsers

The Cisco MobilityManager administration application supports the following Microsoft Windows operating system browsers:

- Microsoft Internet Explorer, version 6.0 or later
- Netscape Navigator version, 7.2 or later

The administrative interface can be reached from any user PC in your network. For instructions on logging in, see the "Accessing Cisco MobilityManager Administration" section on page 2-2.

Related Topics

- Cisco MobilityManager Solution, page 1-3
- Using Internet Explorer with Cisco MobilityManager Administration, page 1-10
- Using Netscape with Cisco MobilityManager Administration, page 1-11

Using Internet Explorer with Cisco MobilityManager Administration

You can save the certificate authority (CA) root certificate in the trusted folder so that the Security Alert dialog box does not display each time that you access the web application. The first time that you or a user accesses Cisco MobilityManager Administration, a Security Alert dialog box asks whether you trust the server. You must select *one* of the these options:

- Click **Yes** to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box opens each time that you access the application, unless you install the certificate in the trusted folder.
- Choose **View Certificate > Install Certificate** to perform certificate installation tasks. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- Click **No** to cancel the action. No authentication occurs, and you cannot access the web application.

To save the security certificate, follow these steps:

Procedure

Step 1 Browse to the Cisco MobilityManager Administration web page (see "Accessing Cisco MobilityManager Administration" section on page 2-2).

Step 2 When the Security Alert dialog box displays, click **View Certificate**.

Step 3 In the Certificate pane, click **Install Certificate**.

Step 4 Click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to **Trusted Root Certification Authorities**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

Step 9 To install the certificate, click **Yes**.

A message states that the import was successful.

Step 10 Click **OK**.

Step 11 In the lower, right corner of the dialog box, click **OK**.

Step 12 To trust the certificate so you do not receive the dialog box again, click **Yes**.

Note If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Related Topics

- Cisco MobilityManager Solution, page 1-3
- Using Netscape with Cisco MobilityManager Administration, page 1-11

Using Netscape with Cisco MobilityManager Administration

Using Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

Tip If you trust the certificate for one session only, you must repeat the following procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

To save the certificate to the trusted folder, follow these steps:

Procedure

Step 1 Access the application through Netscape.

Step 2 After the New Site Certificate window displays, click **Next**.

Step 3 After the next New Site Certificate window displays, click **Next**.

Tip To view the certificate credentials before you click Next, click **More Info**. Review the credentials, and click **OK**.; then, click **Next** in the New Site Certificate window.

Step 4 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Step 5 Click **Next**.

Step 6 If you clicked the Do not accept this certificate... radio button, go to Step 8.

Step 7 If you want Netscape to warn you before sending information to other sites, check the **Warn me before I send information to this site** check box; then, click **Next**.

Step 8 Click **Finish**.

Related Topics

- Cisco MobilityManager Solution, page 1-3
- Using Internet Explorer with Cisco MobilityManager Administration, page 1-10

Where to Find More Information

See the following documents for additional information on web interfaces to Cisco MobilityManager and Cisco CallManager.

- *Cisco CallManager System Guide*
- *Cisco IP Telephony Solution Reference Network Design Guide*
- *Cisco MobilityManager Installation Guide*

CHAPTER 2

Getting Started

This chapter explains how to set up your system to use Cisco MobilityManager and add user accounts. Before you follow the procedures in this chapter, you must complete these tasks:

1. Install the Cisco MobilityManager application according to the procedures in the *Cisco MobilityManager Installation Guide*.
2. Configure Cisco CallManager to support Mobile Connect features according to the procedures in the *Cisco MobilityManager Installation Guide*.
3. Review the information about web browser, HTTPS, and security certificates in "Administrative Web Interface" section on page 1-9.

Refer to these topics in this chapter to begin administering Cisco MobilityManager:

- Accessing Cisco MobilityManager Administration, page 2-2
- Configuring CallManager Links, page 2-3
- Setting Up User Accounts, page 2-11

Accessing Cisco MobilityManager Administration

From a supported web browser, follow these steps to open the Cisco MobilityManager administration application. See the "Administrative Web Interface" section on page 1-9 for browser requirements.

Procedure

Step 1 Start a supported version of Internet Explorer or Netscape.

Step 2 In the address bar of the web browser, enter the following URL:

http://<*Mobility Server*>*:8080/cmmadmin*

where <*Mobility Server*> equals the name or IP address of the server.

If you have not saved the certificate authority (CA) root certificate on your local computer, a Security Alert dialog box. Click **Yes** to trust the certificate for the current session, or follow the procedures in "Using Internet Explorer with Cisco MobilityManager Administration" section on page 1-10 or "Using Netscape with Cisco MobilityManager Administration" section on page 1-11 to download and save the certificate.

Step 3 Log in with the administrator ID and password. The default ID is **CMMAdmin** and the default password is **ciscocisco**.

Navigating the Administration Application

Use the menus at the top of the Cisco MobilityManager administration application to navigate to the individual configuration windows. Some windows also contain a Related Links pull-down list box in the upper right hand corner. Use the related links to return to the top window of a nested series of menus.

On the initial Cisco MobilityManager screen, the pull-down list box in the upper right corner includes an option to open the IPT platform administration pages. For information on using the IPT platform pages, see the IPT Platform online help system.

Related Topics

- Administrative Web Interface, page 1-9
- Configuring CallManager Links, page 2-3
- Setting Up User Accounts, page 2-11

Managing Administrator Passwords

To change the password required to access the Cisco MobilityManager administration application, follow these steps:

Procedure

Step 1 Choose **System** > **Administrator Password Management**.

Step 2 In the Password field, enter the new password. The password must be 6-30 characters in length. There are no restrictions on the types of characters used.

Step 3 In the Confirm Password field, re-enter the password.

Step 4 Click **Save**.

Related Topics

- Accessing Cisco MobilityManager Administration, page 2-2
- Navigating the Administration Application, page 2-2

Configuring CallManager Links

This section describes how to configure shared lines and outgoing port links in Cisco MobilityManager. The Shared Line User Link is a connection between Cisco MobilityManager and the CTI user in Cisco CallManager that was set up during installation to control all shared lines. The Outgoing Port User Link is a connection between Cisco MobilityManager and the CTI user in Cisco CallManager that was set up during installation to control all outgoing call CTI ports.

These links are necessary to complete the connection to Cisco CallManager for the purpose of supporting Mobile Connect features.

Note The Cisco CallManager Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with Mobile Voice Access calls. JTAPI does not support the events required for FAC/CMC.

Before setting up the shared line and outgoing port links as described in this section, you must have performed the following procedures in Cisco CallManager to support Mobile Connect features. Refer to the following sections in the *Cisco MobilityManager Installation Guide:*

1. Setting Parameters for the Mobile Connect Service
2. Creating a Partition for the Route Point
3. Creating the Calling Search Space
4. Creating a Pool of CTI Ports for Outgoing Calls
5. Creating a CTI Port for the Shared Line
6. Creating a Route Point
7. Creating Cisco MobilityManager CTI Users

After these procedures have been completed, complete these tasks to configure the Cisco CallManager links:

1. Adding a New Shared Line User Link, page 2-5
2. Adding a New Outgoing Port User Link, page 2-8

Note You must configure the shared link user link before configuring the outgoing port user l ink.

Adding a New Shared Line User Link

You must create a link between Cisco MobilityManager and the CTI user in Cisco CallManager that was set up as a shared line during installation. See the *Cisco MobilityManager Installation Guide* for more information.

To add a new Shared Link User Link from Cisco MobilityManager to Cisco CallManager, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System > CallManager Links > Shared Line User Links**.

Step 2 Click **Add New**.

The Shared Line User Links Configuration window opens.

Step 3 Enter a unique name for the new link in the Name field. The maximum length is 50 characters.

Step 4 In the Primary CTI Manager IP Address field, enter the IP address of the Cisco CallManager in which the CTI manager is running.

Step 5 If a secondary CTI manager has been configured, enter its IP address in the optional Secondary CTI Manager IP Address field.

Step 6 Cisco recommends that you maintain the default setting of 6000 milliseconds for the CTI Provider In Service Timer field. This value controls timing for the communications link between Cisco MobilityManager and Cisco CallManager and should be modified only if there are connection problems between the two systems. The range of values is 1000-11000 milliseconds.

Step 7 In the Shared Line CTI User field, enter the exact ID of the CTI user that was defined in Cisco CallManager. The maximum length is 50 characters. For more information, see the section on creating CTI users in the *Cisco MobilityManager Installation Guide*.

Step 8 In the Shared Line CTI User Password field, enter the password of the CTI user as assigned in Cisco CallManager, and confirm the password. The maximum length is 50 characters.

Step 9 Click **Save**.

Related Topics

- Adding a New Shared Line User Link, page 2-5
- Deleting a Shared Line User Link, page 2-7

Finding Existing Shared Line User Link Records

To find existing Shared Line User Link records, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System** > **Call Manager Link** > **Shared Line User Links**.

The Find and List Cisco CTI Manager Shared Line User Links window opens.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items to display per page.

Note To find all matching records in the database, click **Find** without entering any search text. To refine a search that was just completed, choose **Search Within Results** before clicking **Find**.

Step 4 From the list of records, click the item that matches your search criteria.

The window displays the item that you choose.

Related Topics

- Adding a New Shared Line User Link, page 2-5
- Deleting a Shared Line User Link, page 2-7

Deleting a Shared Line User Link

To delete a Shared Line User Link, follow these steps:

Note It is not possible to modify a shared line user link. To make a change, you must delete the existing link and add a new one.

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System** > **CallManager Links** > **Shared Line User Links**.

Find the user link or links that you want to remove. See "Adding a New Shared Line User Link" section on page 2-5.

Step 2 Use either of the following methods to delete records:

From the list of records:

a. Use the check boxes to select specific records, or click **Select All** to choose all records.

b. Click **Delete Selected**.

c. Click **OK** to confirm.

From an open record:

a. Click **Delete**.

b. Click **OK** to confirm.

Related Topics

- Adding a New Shared Line User Link, page 2-5
- Adding a New Shared Line User Link, page 2-5

Adding a New Outgoing Port User Link

It is necessary to add a link between Cisco MobilityManager and the CTI user in Cisco CallManager that was set up as an outgoing port during installation. See the *Cisco MobilityManager Installation Guide* for more information.

To add a new outgoing port user link, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System > CallManager Links > Outgoing Port User Links**.

Step 2 Click **Add New**.

The Outgoing Port User Links Configuration window opens.

Step 3 Enter a unique name for the new link in the Name field. The maximum length is 50 characters.

Step 4 In the Primary CTI Manager IP Address field, enter the IP address of the Cisco CallManager in which the CTI manager is running.

Step 5 If a secondary CTI manager has been configured, enter its IP address in the optional Secondary CTI Manager IP Address field.

Step 6 Cisco recommends that you maintain the default setting for the number of 6000 milliseconds in the CTI Provider In Service Timer field. This value should be modified only if there are connection problems between Cisco MobilityManager and Cisco CallManager. The range of values is 1000-11000 milliseconds.

Step 7 In the Outgoing Port CTI User field, enter the ID of the CTI user that was defined in Cisco CallManager.

Note The user ID must be identical to the ID configured in Cisco CallManager. For more information, see the section on adding CTI users in the *Cisco MobilityManager Installation Guide*.

Step 8 Enter the password of the CTI user as assigned in Cisco CallManager, and confirm the password. The maximum length is 50 characters.

Step 9 Click **Save**.

Related Topics

- Finding an Existing Outgoing Port User Link Record, page 2-9
- Deleting an Outgoing Port User Link, page 2-10

Finding an Existing Outgoing Port User Link Record

To find an existing outgoing port user link record, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System > Call Manager Link > Outgoing Port User Links**.

The Find and List Cisco CTI Manager Outgoing Port User Links window opens.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.

Note To find all matching records in the database, click **Find** without entering any search text. To refine a search that was just completed, choose **Search Within Results** before clicking **Find**.

Step 4 From the list of records, click the item that matches your search criteria.

Step 5 The window displays the item that you choose.

You can delete multiple links from the Find and List window by checking the check boxes next to the appropriate items and clicking **Delete Selected**.

You can choose all the items in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

Related Topics

- Adding a New Outgoing Port User Link, page 2-8
- Deleting an Outgoing Port User Link, page 2-10

Deleting an Outgoing Port User Link

To delete an outgoing port user link, follow these steps:

Note It is not possible to modify an outgoing port user link. If you want to make a change, you must delete the existing link and add a new one.

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System** > **CallManager Links** > **Outgoing Port User Links**.

Find the user link or links that you want to remove. See "Adding a New Shared Line User Link" section on page 2-5.

Step 2 Use either of the following methods to delete records:

From the list of records:

a. Use the check boxes to select specific records, or click **Select All** to choose all records.

b. Click **Delete Selected**.

c. Click **OK** to confirm.

From an open record:

a. Click **Delete**.

b. Click **OK** to confirm.

Related Topics

- Finding an Existing Outgoing Port User Link Record, page 2-9
- Adding a New Outgoing Port User Link, page 2-8

Setting Up User Accounts

A user's Mobile Connect profile consists of the following elements:

- The *user account* stores all the Mobile Connect information for a user and is identified by the Mobile Voice Access User ID.
- A *group* ties together a set of phone lines and remote destinations for the user.
- A *line appearance* is a desktop phone line or extension for the user.
- *Remote destinations* include the cellular phones that are available for Mobile Connect responses and pickup, and other phones that are used to reach Mobile Voice Access.

To set up user accounts, perform these tasks:

1. Adding a New User Account, page 2-12
2. Adding a New Calling Group for an Existing User, page 2-15
3. Adding a New Line Appearance for an Existing User, page 2-16
4. Adding a New Remote Destination, page 2-17

Mobile Connect Parameters

Many of the Mobile Connect parameters can be defined at the system level or individual user level. When defining parameters for individual users, these rules apply:

- Parameters defined for individual users override the same parameters defined at the system level. To maintain system-level values, choose the <system default> option. To define a value for an individual user, choose the Enable option. To ignore the parameter, choose the Disable option. See "Configuring System Parameters" section on page 3-1 for a description of system level parameters.

- Individual user parameters can be defined in the User Information windows in the Administrative application or by users in the User web pages. The last implemented user-level change applies, whether made in the Administrative application or User pages. For more information on the User pages, see the *Cisco MobilityManager User Guide*.

Related Topics

- Configuring System Parameters
- Adding a New User Account

Mobile Voice Access

Mobile Voice Access allows users to access Mobile Connect features when they originate a call from a remote device. To originate a call from a remote device, the user dials the application from the remote device and enters the Mobile Voice Access User ID. The user is then prompted for the PIN assigned to the user in Cisco CallManager. Once authenticated, the user can make a call using the same mobility features that would be available if the user originated the call from the enterprise desktop phone.

Related Topics

- Adding a New User Account

Adding a New User Account

To add a new user account, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **User > User Information**.

Step 2 Click **Add New**.

Step 3 In the Mobile Voice Access User ID field, enter the numeric identifier that the user will use for Mobile Voice Access. The maximum length is 50 digits.

Step 4 In the Cisco CallManager User ID field, enter the exact user ID that was configured for in Cisco CallManager. The maximum length is 50 characters.

Step 5 In the Device Name field, enter the exact device name that is configured for the user in Cisco CallManager. The maximum length is 50 characters.

Step 6 In the Enable User Remote Access field, choose **yes** to permit the user to take advantage of Mobile Voice Access. Choose **no** to prohibit the user from using Mobile Voice Access.

Note In order for a user to be able to use Mobile Voice Access, this field must be set to yes, and the Enable System Remote Access field in the System Parameters Configuration window must also be set to yes. See the "Mobile Voice Access Settings" section on page 3-10.

Note To enable the user, the device name must be equal to the device name in the Cisco CallManager phone configuration.

Step 7 Do not change the default settings of 1 for Maximum Number of Groups Allowed and Maximum Number of Line Appearances Allowed.

Step 8 Enter the maximum number of remote destinations the user is allowed to create. The range is 1-4 destinations.

Step 9 Use the Maximum Number of Allowed Caller Filters Allowed field to limit the number of filters containing phone numbers that will cause designated remote destinations to ring on an incoming call. You can define up to 4 filters. Enter **0** if you do not want to permit filters to be defined.

Step 10 Use the Maximum Number of Blocked Caller Filters Allowed field to limit the number of filters that contain caller numbers for which the remote destinations do NOT ring on an incoming call. You can define up to 4 filters. Enter **0** if you do not want to permit filters to be defined.

Step 11 Click **Save**.

The user account is saved, and the window reopens with a link to add a new Mobile Connect group. See the "Adding a New Calling Group for an Existing User" section on page 2-15.

Related Topics

- Adding a New Calling Group for an Existing User
- Finding Existing End User Accounts
- Adding a New Line Appearance for an Existing User
- Adding a New Remote Destination

Finding Existing End User Accounts

To find an existing end user account, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **User > User Information**.

The Cisco Find and List Cisco Mobile Connect Users window opens.

Step 2 Choose **Mobile Voice Access User ID** or **Cisco CallManager User ID** as the basis for the search.

Step 3 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 4 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Note To find all matching records in the database, click **Find** without entering any search text. To refine a search that was just completed, choose **Search Within Results** before clicking **Find**.

Step 5 Click the underlined link to open the desired record.

The window displays the record that you selected.

Related Topics

- Adding a New User Account
- Adding a New Calling Group for an Existing User
- Adding a New Line Appearance for an Existing User
- Adding a New Remote Destination

Adding a New Calling Group for an Existing User

A group ties together a set of phone lines and remote destinations for the user. To add a new calling group for an existing user, follow these steps:

Procedure

Step 1 After finding an existing user record ("Finding Existing End User Accounts" section on page 2-14) or adding a new user account ("Adding a New User Account" section on page 2-12), click the underlined link.

The window reopens with a link to add a new associated group.

Step 2 Click **Add New Group.**

Step 3 In the Group Identification field, enter a numeric ID. The maximum length is 50.

Step 4 Enter an description, if desired. The maximum length is 50 characters.

Step 5 Click **Save**.

The information is saved, and the window reopens with links to add new line appearances and remote destinations.

Related Topics

- Adding a New User Account
- Finding Existing End User Accounts
- Adding a New Line Appearance for an Existing User

- Adding a New Remote Destination

Adding a New Line Appearance for an Existing User

The line appearance is the desktop phone line or extension for the user.

To add a new line appearance for an existing user, follow these steps:

Procedure

Step 1 Find the user account ("Finding Existing End User Accounts" section on page 2-14).

Step 2 Add a new group ("Adding a New Calling Group for an Existing User" section on page 2-15), or click the link for an existing group.

The window reopens with a link to add a new line appearances and remote destinations.

Step 3 Click **Add New Line Appearances.**

Step 4 In the Line Number field, enter the telephone number or extension for the line. Maximum field length is 20 characters; individual characters can take the values 0-9 or A-D.

Step 5 The new line appearance automatically inherits system level Mobile Connect settings. If needed, modify the values according to the descriptions in Table 2-1.

Step 6 If needed, change the default value in the Maximum Wait Time for Cellular Phone Pickup. This setting applies for calls that are switched from the cellular phone to desktop phone. If the wait time is exceeded before the desktop phone is picked up, the call is disconnected. The range is 5000-60000 milliseconds, and the default is 10000 milliseconds.

Step 7 In the optional Enable Cellular Phone Pickup field, choose whether to enable the Mobile Connect feature to allow pick-up of incoming calls on the cellular phone. The default is the system level default.

Step 8 Click **Save**.

The information is saved, and the window reopens with links to add new line appearances and remote destinations.

Related Topics

- Adding a New User Account
- Finding Existing End User Accounts
- Adding a New Calling Group for an Existing User
- Adding a New Remote Destination
- Entering Parameters for User Line Appearances and Remote Destinations

Adding a New Remote Destination

To add a new remote destination (cellular phone number or other remote phone number) for an existing user, follow these steps:

Procedure

Step 1 Find the user account ("Finding Existing End User Accounts" section on page 2-14).

Step 2 Add a new group ("Adding a New Calling Group for an Existing User" section on page 2-15), or click the link for an existing group.

The window reopens with link to add new line appearances and remote destinations.

Step 3 Click **Add New Remote Destination.**

Step 4 In the Remote Destination field, enter the telephone number for the destination. Include the area code and any additional digits required to obtain an outside line. Maximum field length is 20 characters; individual characters can take the values 0-9 or A-D.

Step 5 To enable calls to be made from the user's cellular phone to desktop phone, enter the caller ID used for the cellular phone in the Caller ID field. When the call is placed, the caller ID is detected, and the call is directed to the desktop phone without an attempt to ring the cellular phone as well. The caller ID is also automatically detected when the user calls Mobile Voice Access, and the user is prompted only for password.

Step 6 To activate the Mobile Connect features for this line, choose **yes** from the Enable Mobile Connect pull-down list box. The default is yes.

Step 7 The new remote destination automatically inherits the system level cellular timer settings. Refer to Table 2-2 if you need to change the settings.

Step 8 Click **Save**.

The record is saved. The window reopens with the user account information presented along with links to the remote destinations.

Related Topics

- Adding a New User Account
- Finding Existing End User Accounts
- Adding a New Calling Group for an Existing User
- Adding a New Line Appearance for an Existing User
- Entering Parameters for User Line Appearances and Remote Destinations

Entering Parameters for User Line Appearances and Remote Destinations

The tables in this section describe the parameters for user line appearances and remote destinations:

- Mobile Connect Settings, page 2-19
- Cellular Timer Settings, page 2-20

Mobile Connect Settings

Table 2-1 describes the Mobile Connect settings available in the Line Appearances window.

Table 2-1 Mobile Connect Settings

Field	Description
Enable Caller ID Override	Choose **Enable** if you want the caller ID display to show a number other than the ID of the call initiator. Choose **Disable** to show the ID of the call initiator. The default is the system level default.
Caller ID Override Number	Enter the telephone number to display for caller ID. Maximum field length is 20 characters; individual characters can take the values 0-9 or A-D. If the field is blank, then the display indicates that there is no caller ID. **Note** If Enable Caller ID Override is disabled, then this field is inactivated.
Enable Delay Before Ringing Cellular Phone	Choose **Enable** to introduce a delay before causing the remote device (cellular phone) to ring when an incoming call is received. By introducing a delay, the desktop phone maintains priority status for receiving incoming calls. Choose **Disable** to have no delay introduced. The default is the system level default.
Delay Before Ringing Cellular Phone	If you choose Enable in the Enable Delay Before Ringing Cellular Phone field, enter the time delay in milliseconds. The range is 1000-300000 milliseconds, and the default value is 4000 milliseconds.

Cellular Timer Settings

Table 2-2 describes the settings that control rings and timing for cellular phone pickup.

Table 2-2 Cellular Timer Settings

Field	Description
Enable Maximum Cellular Phone Pickup Timer	Choose **Enable** to set the maximum waiting time for the cellular phone to answer when a call is switched from the desktop phone. The default is the system level default.
Maximum Cellular Phone Pickup Timer	If you choose Enable for Maximum Wait Time for Cellular Phone Pickup, enter the maximum number of milliseconds that is permitted to pass before the cellular phone must be picked up when a call is switched from the desktop phone. If the remote device does not answer in the specified time, the call is disconnected. The range is 1000-300000 milliseconds, and the default is 20000 milliseconds.
Enable Maximum Cellular Phone Ring Timer	Choose **Enable** to set timing intervals for calls switched from the desktop phone to cellular phone. The default is the system level default.
Maximum Cellular Phone Ring Timer	If you choose Enable for Enable Maximum Cellular Phone Ring Timer, enter the maximum length of time that the cellular phone will ring before being disconnected. The range is 10000-300000, and the default is 19,000 milliseconds.

Table 2-2 Cellular Timer Settings

Field	Description
Enable Minimum Cellular Phone Ring/Pickup Timer	Choose **Enable** to set the minimum timing before the cellular phone rings for incoming calls and when switching from the desktop phone to cellular phone. The default is the system level default.
Minimum Cellular Phone Ring/Pickup Timer	If you choose Enable for Minimum Cellular Phone Ring Timer, enter the minimum time that must pass before the cellular phone can be answered. If an attempt is made to answer the cellular phone before this time passes, then the call is dropped (it is assumed that cellular phone voice mail has picked up the call). The range is 1000-10000 milliseconds, and the default is 1500 milliseconds. **Note** 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 Voicemail.

Related Topics

- Adding a New User Account
- Adding a New Calling Group for an Existing User
- Adding a New Line Appearance for an Existing User
- Adding a New Remote Destination

Updating Existing User Accounts

To update existing user accounts, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Find the user account that you want to update. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Enter the change in fields in the window, or click an underlined link to changes a group or line appearance.

Step 4 Click **Save**.

Related Topics

- Adding a New User Account
- Deleting Existing User Accounts

Deleting Existing User Accounts

To delete one or more existing user accounts, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Find the user accounts that you want to remove. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Use either of the following methods to delete records:

From the list of records:

a. Use the check boxes to select specific records, or click **Select All** to choose all records.

b. Click **Delete Selected**.

c. Click **OK** to confirm.

From an open record:

a. Click **Delete**.

b. Click **OK** to confirm.

Related Topics

- Adding a New User Account
- Updating Existing User Accounts

Updating a Group Record

To update a group record associated with a user, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Open the user record. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Click the link for the group.

Step 4 Make desired changes.

Step 5 Click **Save**.

Related Topics

- Adding a New Calling Group for an Existing User
- Deleting a Group Record

Deleting a Group Record

To delete a group associated with a user, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Open the user record. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Click the link for the group.

Step 4 Click **Delete** when the group record opens.

Step 5 Click **OK** to confirm.

Related Topics

- Adding a New Calling Group for an Existing User
- Updating a Group Record

Updating a Line Appearance

To update a line appearance associated with a user, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Open the user record. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Click the link for the group in which the line appearance is defined.

Step 4 Click the line for the line appearance.

Step 5 Make desired changes.

Step 6 Click **Save**.

Related Topics

- Adding a New Line Appearance for an Existing User
- Deleting a Line Appearance

Deleting a Line Appearance

To delete a line appearance associated with a user, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Open the user record. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Click the link for the group in which the line appearance is defined.

Step 4 Click the line for the line appearance.

Step 5 Click **Delete** when the line appearance record opens.

Step 6 Click **OK** to confirm.

Related Topics

- Adding a New Line Appearance for an Existing User
- Updating a Line Appearance

Updating a Remote Destination

To update a remote destination, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Open the user record for the remote destination that you want to remove. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Click the link for the group for which the remote destination is defined.

Step 4 Make desired changes.

Step 5 Click **Save**.

Related Topics

- Adding a New Remote Destination
- Deleting a Remote Destination

Deleting a Remote Destination

To delete a remote destination, follow these steps:

Procedure

Step 1 Choose **System** > **User Information**.

Step 2 Open the user record for the remote destination that you want to remove. See "Finding Existing End User Accounts" section on page 2-14.

Step 3 Click the link for the group for which the remote destination is defined.

Step 4 Click **Delete** when the remote destination record opens.

Step 5 Click **OK** to confirm.

Related Topics

- Adding a New Remote Destination
- Updating a Remote Destination

System Configuration

This chapter describes how to set up parameters for call handling in Cisco MobilityManager. Refer to the these topics to get started:

- Configuring System Parameters, page 3-1
- Enabling Data Synchronization, page 3-12
- Backing Up and Restoring the Database, page 3-12
- Configuring Directory User Settings, page 3-13

For information on setting up links to the Cisco CallManager system, see Chapter 2, “Getting Started.”

Configuring System Parameters

Cisco MobilityManager includes system-level mobility parameters for mobile connection, desktop and cellular phone rules and timers, settings for the JAVA telephony programming interface (JTAPI), and SNMP[1] and Mobile Voice Access settings.

Many of the system parameters can also be configured for individual users in the User Information windows. Settings for individual users override the system-level settings assigned in the System Parameters window.

[1] SNMP supports includes SNMP version 1, version 2c, and version 3 with multiple alarm/syslog recipients, setting of syslog read/write attributes, and periodic alarms.

Note For basic Cisco MobilityManager operation, it is not necessary to enter any information or change any of the default settings on the System Parameters page. Modify the settings only as needed to activate or modify desired features.

To configure system parameters, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System** > **System** Parameters.

The System Parameters Configuration page opens.

Step 2 Use the Restart Cisco MobilityManager button if Cisco MobilityManager services have been stopped and you need start them again.

Step 3 Keep the default setting of Yes for the Gateway Early Media field. This field is sometimes used for troubleshooting.

Step 4 Choose Mobile Connect settings as described in Table 3-1.

Step 5 In the Maximum Wait Time for Desktop Phone Pickup field, enter the maximum delay in milliseconds that is permitted before the user must pick up the desktop phone. If the specified time is exceeded, the call is disconnected. The range is 5000-60000 milliseconds, and the default is 10000 milliseconds.

Step 6 Choose cellular phone pickup settings as described in Table 3-2.

Step 7 Choose cellular timer settings as described in Table 3-3.

Step 8 Choose settings for automatic update of JTAPI, as described in Table 3-4.

Step 9 Choose SNMP settings, as described in Table 3-5

Step 10 Choose Mobile Voice Access settings as described in Table 3-6.

Step 11 Enter Cisco CallManager AXL server settings as described in Table 3-7.

Step 12 Click **Save**.

Related Topics

- Mobile Connect Settings, page 3-3
- Cellular Phone Pickup Settings, page 3-5

- Cellular Timer Settings, page 3-6
- Auto Update JTAPI File Settings, page 3-7
- SNMP Settings, page 3-9
- Mobile Voice Access Settings, page 3-10
- Cisco CallManager AXL Server Settings, page 3-11

Mobile Connect Settings

Table 3-1 describes the Mobile Connect settings available on the System Parameters screen.

Table 3-1 Mobile Connect Settings

Field	Description
Enable Caller ID Override	Choose **Yes** if you want the caller ID display to show a number other than the ID of the call initiator. Choose **No** to show the ID of the call initiator. The default is No.
Caller ID Override Number	Enter the telephone number to display for caller ID. Maximum field length is 20 characters; individual characters can take the values 0-9 or A-D. If the field is blank, then the display indicates that there is not caller ID. If Enable Caller ID Override is disabled, then this field is inactivated.
Enable Mobile Connect Feature	Choose **Yes** to activate Mobile Connect features. If you choose No, then the other fields in this window are ignored. The default is Yes.

Table 3-1 Mobile Connect Settings (continued)

Field	Description
Enable Delay Before Ringing Cellular Phone	Choose **Yes** to introduce a delay before causing the remote device (cellular phone) to ring when an incoming call is received. By introducing a delay, the desktop phone maintains priority status for receiving incoming calls. Choose **No** to have no delay introduced. The default is No.
Delay Before Ringing Cellular Phone	If you choose Yes for Enable Delay Before Ringing Cellular Phone, enter the time delay. The range is 1000-300000 milliseconds, and the default is 4000 milliseconds.

Related Topics

- Cellular Phone Pickup Settings, page 3-5
- Cellular Timer Settings, page 3-6
- Auto Update JTAPI File Settings, page 3-7
- SNMP Settings, page 3-9
- Mobile Voice Access Settings, page 3-10
- Cisco CallManager AXL Server Settings, page 3-11

Cellular Phone Pickup Settings

Table 3-2 describes the cellular phone pickup settings that determine rules regarding pick-up of the cellular phone on an incoming call.

Table 3-2 Cellular Phone Pick-Up Settings

Field	Description
Enable Cellular Phone Pickup	Choose **Yes** to permit a call to be switched from the desktop phone to a remote extension (cellular phone) while the call is taking place. The default is Yes.
Enable Maximum Cellular Phone Pickup Timer	Choose **Yes** to set the maximum waiting time for the cellular phone to answer when a call is switched from the desktop phone. The default is No.
Maximum Wait Time for Cellular Phone Pickup (msec)	If you choose Yes for Maximum Wait Time for Cellular Phone Pickup, enter the maximum number of milliseconds that is permitted to pass before the cellular phone must be picked up when a call is switched from the desktop phone. If the remote device does not answer in the specified time, the call is disconnected. The range is 1000-300000 milliseconds, and the default is 20,000 milliseconds.

Related Topics

- Mobile Connect Settings, page 3-3
- Cellular Timer Settings, page 3-6
- Auto Update JTAPI File Settings, page 3-7
- SNMP Settings, page 3-9
- Mobile Voice Access Settings, page 3-10
- Cisco CallManager AXL Server Settings, page 3-11

Cellular Timer Settings

Table 3-3 describes the cellular timer settings that control rings and timing for cellular phone pickup.

Table 3-3 Cellular Timer Settings

Field	Description
Enable Maximum Cellular Phone Ring Timer	Choose **Yes** to set timing intervals for calls switched from the desktop phone to cellular phone. The default is No.
Maximum Cellular Phone Ring Timer	If you choose Yes for Enable Maximum Cellular Phone Ring Timer, enter the maximum length of time the cellular phone rings before being disconnected. This value is measured from the end of the interval determined by the Delay Before Ringing Cellular Phone Field. (See Table 2-1 on page 2-19.) The range is 10000-300000 milliseconds, and the default is 19000 milliseconds. The timer should be set to be less than the No Answer Ring Duration timer configured for that line in Cisco CallManager. For further information, see the *Cisco CallManager Administration Guide*.

Table 3-3 Cellular Timer Settings (continued)

Field	Description
Enable Minimum Cellular Phone Ring Timer	Choose **Yes** to set the minimum timing for the cellular phone to ring for incoming calls and switching from the desktop phone to cellular phone. The default is Yes.
Minimum Cellular Phone Ring Timer	If you choose Yes for Minimum Cellular Phone Ring Time, enter the minimum time that must pass before the cellular phone can be answered. If an attempt is made to answer the cellular phone before this time passes, then the call is dropped (it is assumed that cellular phone voice mail has picked up the call). The range is 1000-10000 milliseconds, and the default is 1500 milliseconds. **Note** 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.

Related Topics

- Mobile Connect Settings, page 3-3
- Cellular Phone Pickup Settings, page 3-5
- Auto Update JTAPI File Settings, page 3-7
- SNMP Settings, page 3-9
- Mobile Voice Access Settings, page 3-10
- Cisco CallManager AXL Server Settings, page 3-11

Auto Update JTAPI File Settings

Table 3-4 describes the Auto Update JTAPI file settings that control updating of the JAVA telephony programming interface used for communications between Cisco MobilityManager and Cisco CallManager. Use the JTAPI file settings to configure automatic synchronization of the JTAPI versions. If you enable the automatic update, then the version of JTAPI is updated automatically to match that of Cisco CallManager.

The jtapi.jar file from Cisco CallManager 4.1.3 is bundled in the Cisco MobilityManager software distribution. If you are using a different version of Cisco CallManager, you need to configure the JTAPI file settings as described in this section.

Note The JTAPI automatic update takes effect only after Cisco MobilityManager is restarted.

Table 3-4 Auto Update JTAPI File Settings

Field	Description
Enable Auto Update JTAPI file	Choose **Yes** to enable automatic update of the JAVA telephony settings. The default is No.
Always Update JTAPI File	Choose **Yes** to always update the JTAPI file when when Cisco MobilityManager restarts. The default is No.
Auto Update JTAPI Server Name or IP Address	If you choose Yes for automatic update of the JTAPI file, enter the name or IP address of the server that will provide the automatic update. There is no default.
Use Secured Auto JTAPI Update	Choose **Yes** to add security to the automatic JTAPI update. The default is No.
Auto Update JTAPI Server Path	Enter the absolute path or URL the JTAPI server: The default path is http://<Cisco CallManagerserver>/CCMPluginsServer You do not need to enter anything in this field if the default path is to be used.
Auto Update JTAPI Server File Name	Enter the name of the automatic update file on the server. The default is jtapi.jar. You do not need to enter anything in this field if the default file is to be used.
Auto Update JTAPI Local File Name	Enter the name of the local automatic update file. The default is jtapi.jar. You do not need to enter anything in this field if the default file is to be used.

Related Topics

- Mobile Connect Settings, page 3-3
- Cellular Phone Pickup Settings, page 3-5
- Cellular Timer Settings, page 3-6
- SNMP Settings, page 3-9
- Mobile Voice Access Settings, page 3-10
- Cisco CallManager AXL Server Settings, page 3-11

SNMP Settings

Table 3-6 describes the SNMP settings.

Table 3-5 SNMP Settings

Field	Description
SNMP Target IP Address	Enter the IP address for the system that will receive SNMP traps.
SNMP Target Port Number	Enter the SNMP port number. The default port is 162.
SNMP Community String	Enter the code for the SNMP grouping for Cisco MobilityManager.
SNMP Version	Choose SNMP version V1 or V2C from the pull-down list box.

Related Topics

- Mobile Connect Settings, page 3-3
- Cellular Phone Pickup Settings, page 3-5
- Cellular Timer Settings, page 3-6
- Auto Update JTAPI File Settings, page 3-7
- Cisco CallManager AXL Server Settings, page 3-11

Mobile Voice Access Settings

Table 3-6 describes the settings for Mobile Voice Access.

Table 3-6 Mobile Voice Access Settings

Field	Description
Mobile Voice Access Numbers	Enter the phone number for Mobile Voice Access. Maximum field length is 200 characters; individual characters can take the values 0-9 or A-D. Use commas to enter multiple numbers.
Mobile Voice Access User Lock Out Timer (min)	Enter the number of minutes a user is prevented from using Mobile Voice Access after providing incorrect entries three times in succession. This applies to incorrect PIN or remote destination entries. The range is 0-1440 minutes, and the default is 15 minutes.
Enable System Remote Access	Choose **yes** to enable the system remote access feature or **no** to disable the feature. **Note** In order for an individual user to be able to take advantage of system remote access, this field must be set to yes, and the Enable User Remote Access field in the Cisco Mobile Connect User Configuration window must also be set to yes for the individual user. See the "Adding a New User Account" section on page 2-12.
System Remote Access Blocked Numbers	Enter any phone numbers that you want to prohibit users from calling using Mobile Voice Access. Maximum field length is 200 characters; individual characters can take the values 0-9 or A-D. Use commas to enter multiple numbers.
System Remote Access Call Take Back Timer (sec)	Enter the number of seconds after which the Mobile Voice Access session times out. The range is 120-180 seconds, and the default is 120 seconds.

Related Topics

- Mobile Connect Settings, page 3-3

- Cellular Phone Pickup Settings, page 3-5
- Cellular Timer Settings, page 3-6
- Auto Update JTAPI File Settings, page 3-7
- SNMP Settings, page 3-9
- Cisco CallManager AXL Server Settings, page 3-11

Cisco CallManager AXL Server Settings

Table 3-7 describes the Cisco CallManager AXL Server settings required for communication with Cisco CallManager.

Table 3-7 Cisco CallManager AXL Server Settings

Field	Description
Cisco CallManager Version	Enter the software version number for Cisco CallManager. Example: 4.1
Cisco CallManager AXL Server Name or IP Address	Enter the host name or IP address of the Cisco CallManager AXL server.
Cisco CallManager AXL User Name	Enter the user name for administrator access to the Cisco CallManager AXL server.
Cisco CallManager AXL User Password	Enter the password for administrator access to the Cisco CallManager AXL server.

Related Topics

- Mobile Connect Settings, page 3-3
- Cellular Phone Pickup Settings, page 3-5
- Cellular Timer Settings, page 3-6
- Auto Update JTAPI File Settings, page 3-7
- SNMP Settings, page 3-9
- Mobile Voice Access Settings, page 3-10

Enabling Data Synchronization

To synchronize the MobilityManager database with current runtime memory, follow these steps:

Procedure

Step 1 Choose **System** > **Data Synchronization**.

Step 2 Click **Start Now**.

Step 3 Click **OK** to confirm that you want to begin the data synchronization process.

Related Topics

- Configuring System Parameters, page 3-1
- Backing Up and Restoring the Database, page 3-12

Backing Up and Restoring the Database

You can back up and restore the remote system information for Cisco MobilityManager using an SFTP server.

To set backup and restore parameters, follow these steps:

Procedure

Step 1 Choose **System** > **Backup and Restore**.

The Backup and Restore screen opens.

Step 2 In the Host Name or IP Address field, enter the appropriate information to identify the backup server.

Step 3 Enter the User ID and password for the backup server.

Step 4 Enter the password again in the Confirm Password field.

Step 5 In the File Path field, enter the location to store or retrieve the backup files.

Step 6 Click **Start Backup Now** to begin backing up the database to the specified location, or click **Start Restore Now** to begin restoring from the specified file.

Step 7 After restoring the remote system information, perform data synchronization according to the procedure in "Enabling Data Synchronization" section on page 3-12.

Related Topics

- Configuring System Parameters, page 3-1
- Enabling Data Synchronization, page 3-12

Configuring Directory User Settings

Directory user settings are required for connection to the directory server that Cisco CallManager uses. For a working connection, you must configure the directory user settings for Cisco MobilityManager to be identical to those in the Cisco CallManager in which directory services are configured. If the settings are not correctly configured, users cannot log in to the User pages or change their user profiles. The directory services information is stored in the DirectorySevices.ini file, which is located in the Cisco CallManager c$\dcdsrvr directory.

Note If your Cisco CallManager installation uses Active Directory or Netscape directory, then refer to the *Cisco Customer Directory Configuration Plugin Guide* for Cisco CallManager. The file DirectoryConfiguration.ini will be created after the Directory User Settings page is configured, and this file should be the same as the file in Call Manger \dcdsrvr directory.

To configure directory user settings, follow these steps:

Procedure

Step 1 Choose **System** > **Directory User Settings**.

Step 2 Enter values for each field in this window that are identical to those configured for Cisco CallManager, as shown Table 3-8.

Step 3 Click **Save**.

Table 3-8 Directory User Settings

Field	Description
Directory Administrator Host Name or IP Address	Enter the directory services hostname or IP address.
Directory Administrator Host Port Number	Enter the port number that is configured in the DirectoryConfiguration.ini file. Example: If you are using the Data Connection Directory (DC-Directory) in Cisco CallManager, then enter **8404**.
Directory Administrator DN	Enter the directory number for the administrator login that is configured in the DirectoryConfiguration.ini file. Example: If you are using the Data Connection Directory (DC-Directory) in Cisco CallManager, then enter **cn=Directory Manager, o=cisco.com**.
Directory Administrator Password	Enter the password used to log into Directory Services.
Confirm Directory Administrator Password	Reenter the password used to log into Directory Services.
Cisco Directory Administrator DN	Enter the number for the directory administrator that is configured in the DirectoryConfiguration.ini file. Example: If you are using the Data Connection Directory (DC-Directory) in Cisco CallManager, then enter **o=cisco.com**.
Directory Type	Enter Default, ADS, or NDS, as configured in the DirectoryConfiguration.ini file.

Related Topics

- Accessing Cisco MobilityManager Administration, page 2-2

- Configuring CallManager Links, page 2-3

Serviceability Configuration

A variety of measurements are available to help you monitor system and call operation. Refer to these topics in this chapter to display alarm, measurement, and debugging information:

Displaying Alarm Information

The Cisco MobilityManager Alarm window lists information about noteworthy events detected by the system. Alarms are set when the error conditions occur and are cleared when the errors are corrected.

To find and display alarm information, follow these steps:

Procedure

Step 1 Choose **Serviceability** > **Alarm**.

The Find and List Cisco MobilityManager Alarms window opens.

Step 2 From the drop-down list box, choose the category on which you want to search:

- alarmcategory

- alarmcomponent
- severity
- date

Step 3 From the drop-down list box, choose *one* of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 4 Enter search text, if applicable, and click **Find**. You can also specify how many items per page to display.

To find all alarms, click **Find** without entering any search text.

The requested alarms are displayed in the window.

Step 5 To change the number of alarm records displayed per page, choose a number from the Row per Page drop-down list box.

Table 4-1 lists the alarm information contained in each row of the alarm display. The alarms are sorted by date, with the most recent alarm listed first.

Table 4-1 Alarm Information

Category	Description
Alarm category	Type of alarm
Alarm component	Cisco MobilityManager area that generated the alarm
Alarm Severity	Seriousness of the alarm
Date	Date and time the alarm was generated

Related Topics

- Displaying Measurements, page 4-3
- Interpreting Measurements, page 4-4
- Configuring Logging Levels, page 4-6

Displaying Measurements

The Cisco MobilityManager Measurement window displays measurements that are collected by the Cisco MobilityManager server.

Note To reset the measurement counters to zero, click **Reset Measurement Counters**.

To display measurement statistics, follow these steps:

Procedure

Step 1 Choose **Serviceability** > **Measurement**.

The Find and List Cisco MobilityManager Measurements window opens.

Step 2 From the drop-down list box, choose *one* of the following criteria for searching the name of the measurement:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

To find all measurements, click **Find** without entering any search text.

The requested measurements are displayed in the window and are sorted alphabetically by Measurement Name.

Step 4 To change the number of records displayed per page, choose a number from the Row per Page drop-down list box.

Related Topics

- Interpreting Measurements, page 4-4
- Displaying Alarm Information, page 4-1
- Configuring Logging Levels, page 4-6

Interpreting Measurements

Table 4-2 describes the available measurements. For information on displaying the measurements, see the "Displaying Measurements" section on page 4-3.

Table 4-2 Measurement Categories

Measurement Name	Description
Attempted Calls	Number of attempted outgoing calls
Attempted Mobile Connect Calls	Number of attempted outgoing calls for which dial tone is detected
Attempted System Remote Access Calls	Number of attempted outgoing calls from remote devices
Completed Calls	Number of calls that are completed
Completed System Remote Access Calls	Number of completed calls that use Mobile Voice Access for system remote access
Desk Answered Calls	Number of calls answered by the desktop phone
Desk to Remote Handoff Calls	Number of calls that are picked up on a remote device
Failed Calls	Number of initiated calls that fail to complete

Table 4-2 Measurement Categories

Measurement Name	Description
Failed Mobile Connect Calls	Number of initiated calls that do not successfully obtain system remote access using Mobile Voice Access
Failed System Remote Access Calls	Number of initiated calls that obtain system remote access using Mobile Voice Access but for which the call is not completed
Handoff Calls	Number of pickups on the desktop phone or cellular phone
Incoming Calls	Number of completed incoming calls
Max Current Calls	Maximum number of calls taking place at the same time
Max Simultaneous Attempted Calls	Maximum number of attempted calls that are handled at the same time
Remote Answered Calls	Number of successful pickups on a remote device
Remote Answered Calls Pickup Key	Number of calls picked up on the cellular phone using the pickup key
Remote to Desk Handoff Calls	Number of calls successfully picked up on the desktop phone

Related Topics

- Displaying Measurements, page 4-3
- Displaying Alarm Information, page 4-1
- Configuring Logging Levels, page 4-6

Configuring Logging Levels

You can use the Cisco MobilityManager and Admin Log Level window to determine the types of alarms that are captured in system log files. The default logging level is for information only; changing the levels may be desirable for troubleshooting.

To configure logging levels, follow these steps:

Procedure

Step 1 Choose **Serviceability** > **Debug**.

The Cisco MobilityManager and Admin Log Level Configuration window opens.

Step 2 From the drop-down list boxes, choose the minimum alarm levels to be logged. See Table 4-3 for a description of the logging levels. The default level is info.

Step 3 Click **Save** to change the logging criteria to include the new levels.

Table 4-3 Logging Levels

Level	Description
debug	Includes messages intended for use in troubleshooting, plus higher level messages
info	Includes informational messages, plus higher level messages
warn	Includes messages that warn of possible operational issues, plus higher level messages
error	Includes error messages, plus higher level messages
fatal	Includes error messages that have caused the system to fail

Related Topics

- Displaying Measurements, page 4-3
- Displaying Alarm Information, page 4-1

Viewing the Status of Cisco MobilityManager Services

The Cisco MobilityManager Service Status window displays the current status of services that must be running for Cisco MobilityManager to operate.

To view the status of services, choose **Serviceability** > **Service Status**. Table 4-4 describes the services that are listed. The status for each is Running or Stopped.

If the Cisco MobilityManager service is listed as stopped, it can be restarted from the System Parameters screen.

To restart the Cisco MobilityManager service, follow these steps:

Procedure

Step 1 From the Cisco MobilityManager administration window, choose **System** > **System Parameters**. The System Parameters Configuration page opens.

Step 2 Click **Restart Cisco MobilityManager**.

Step 3 Click **OK** to confirm.

Table 4-4 Cisco MobilityManager Services

Service	Description
Cisco MobilityManager	Call processing software that supports Cisco MobilityManager
Cisco MobilityManager SNMP	SNMP network management agent process
Cisco Discovery Protocol	Process used to discovery Cisco devices and Cisco CallManager servers in the network
Cisco MobilityManager DATABASE	Process that controls the Cisco MobilityManager database (IBM IDS)

File Export

This chapter explains how to save and export system and call information to an SFTP server. Refer to these topics in this chapter to perform export functions:

Exporting Alarm Records

To export alarm records to a remote server, follow these steps:

Procedure

Step 1 Choose **Export** > **Alarm**.

The Alarm Export Information Configuration window opens. The available alarm files are listed under File Information near the top of the window.

Step 2 Select the log file you wish to export, and use the down facing arrow or double-click to move the selected file to the Exported Alarm Files area. Repeat for other files as needed.

Step 3 In the Remote Server Name field, enter the name or IP address of the remote server on which the files will be stored.

Step 4 Enter the destination directory in the Remote Directory field in the form /*<path>*.

Step 5 Enter the user ID and password for access to the remote server.

Step 6 Enter the password again in the Confirm Password field.

Step 7 Click **Save and Transfer** to save the information and begin the file transfer process.

When the process is completed, a status message is displayed near the top of the window. If the process is successful, the message states “Export successful.”

Related Topics

- Exporting Measurements, page 5-2
- Exporting the Call Detail Record, page 5-3
- Exporting Log Files, page 5-4

Exporting Measurements

To export measurements to a remote server, follow these steps:

Procedure

Step 1 Choose **Export** > **Measurement**.

The Measurement Export Information Configuration window opens. The available measurement files are listed under File Information near the top of the window.

Step 2 Select the file you wish to export, and use the down facing arrow or double-click to move the selected file to the Exported Measurement Files area. Repeat for other files as needed.

Step 3 In the Remote Server Name field, enter the name or IP address of the remote server on which the files will be stored.

Step 4 Enter the destination directory in the Remote Directory field in the form /<*path*>.

Step 5 Enter the user ID and password for access to the remote server.

Step 6 Enter the password again in the Confirm Password field.

Step 7 Click **Save** to save the information and begin the file transfer process.

When the process is completed, a status message is displayed near the top of the window. If the process is successful, the message states "Export successful."

Related Topics

- Exporting Alarm Records, page 5-1
- Exporting the Call Detail Record, page 5-3
- Exporting Log Files, page 5-4

Exporting the Call Detail Record

To export the call detail record (CDR) files to a remote server, follow these steps:

Procedure

Step 1 Choose **Export** > **CDR**.

The CDR Export Information Configuration window opens. The available CDR log files are listed under File Information near the top of the window.

Step 2 Select the file you wish to export, and use the down facing arrow or double-click to move the selected file to the Exported CDR Files area. Repeat for other files as needed.

Step 3 In the Remote Server Name field, enter the name or IP address of the remote server on which the files will be stored.

Step 4 Enter the destination directory in the Remote Directory field in the form /<*path*>.

Step 5 Enter the user ID and password for access to the remote server.

Step 6 Enter the password again in the Confirm Password field.

Step 7 Click **Save** to save the information and begin the file transfer process.

When the process is completed, a status message is displayed near the top of the window.

Related Topics

- Exporting Alarm Records, page 5-1
- Exporting Measurements, page 5-2
- Exporting Log Files, page 5-4

Exporting Log Files

To export log files to a remote server, follow these steps:

Procedure

Step 1 Choose **Export** > **Logs**.

The Log Export Information Configuration window opens. The available log files are listed under File Information near the top of the window.

Step 2 Select the log file you wish to export, and use the down facing arrow to move the selected file to the Exported Log Files area. Repeat for other files as needed.

Note To view a log file or download a log file to your computer, double-click the log file.

Step 3 In the Remote Server Name field, enter the name or IP address of the remote server on which the files will be stored.

Step 4 In the Remote Directory field, enter the destination directory in the form /<*path*>.

Step 5 Enter the user ID and password for access to the remote server.

Step 6 Enter the password again in the Confirm Password field.

Step 7 Click **Save** to save the information and begin the file transfer process.

When the process is completed, a status message is displayed near the top of the window. If the process is successful, the message states “Export successful.”

Related Topics

- Exporting Alarm Records, page 5-1

- Exporting Measurements, page 5-2
- Exporting the Call Detail Record, page 5-3

Platform Administration

Cisco provides these tools to manage the Cisco MobilityManager server platform:

- Cisco IPT Platform Administration web pages that provide complete platform administration functions.
- Command Line Interface (CLI) that provides a subset of the platform administration functions.

Refer to these topics for instructions on using the browser-based interface and the command line interface:

- Using the Cisco IPT Platform Administration Web Pages, page 6-1
- Cisco IPT Platform Administration Command Line Interface, page 6-15

Using the Cisco IPT Platform Administration Web Pages

The Cisco IPT Platform Administration web pages allow you to configure and manage the Cisco MobilityManager server platform. You can perform these functions:

- Verify status of platform components—The Status window provides the following read-only hardware and platform information:
  - Platform status—Displays information that was entered during Cisco MobilityManager server installation, including the host name, status of Ethernet ports, IP addresses, memory usage, and CPU utilization.

  - Hardware status—Displays information about the hardware platform.

- Configure network settings—You can modify IP address and Dynamic Host Configuration Protocol (DHCP) information that was entered when the application was installed. You can also add Network Time Protocol (NTP) servers and clients and synchronize NTP settings.
- Verify connectivity with other network devices—You can use the Ping utility to verify network connectivity.
- Perform Software Upgrades—You can verify your current version of Cisco MobilityManager server software and upgrade software from a local source (CD-ROM or DVD) or remote source (server on the network).
- Reboot the System—You can reboot your system and continue to use the current software image or reboot your system and start using an alternative software image.

Related Topics

- Login, page 6-2
- Show Status, page 6-3
- Settings, page 6-5
- Software Upgrade Windows, page 6-10
- System Power-off or Reboot, page 6-14

Login

To access Cisco IPT Platform Administration and log in, follow these steps:

Procedure

Step 1 On the Cisco CallManager Administration window, click **Show Navigation**.

Step 2 In the left-hand pane, click **Platform Administration**.

Step 3 On the Cisco IPT Platform Administration Logon window, enter your user name and password.

Note The user name and password are established during installation.

Step 4 Click **Submit**.

Show Status

Use these Show Status menu options to view information on platform status and hardware status:

- Platform Status—Displays information that was entered during platform installation, including the host name, status of Ethernet ports, IP addresses, memory usage, and CPU utilization.
- Hardware Status—Displays the platform model, CPU type, memory, object ID, and OS version.

Platform Status

To open the Platform Status window, choose **Show Status** > **Platform Status**. Table 6-1 describes the fields displayed in the window.

Table 6-1 Platform Status Fields

Field	Description
System	
Host Name	Displays the name of the MCS 78xx host where Cisco Platform Administration is installed.
Date/Time	Displays the date and time based on the continent and region that were specified during platform installation.
Locale	Displays the language that was chosen during platform installation.
Time Zone	Displays the time zone that was chosen during installation.
Network	
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.

Table 6-1 Platform Status Fields (continued)

Field	Description
DHCP	Indicates whether DHCP is enabled for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet ports 0 and 1.
IP Mask	Shows the subnet mask address of Ethernet ports 0 and 1.
Primary DNS	Displays the IP address of the primary domain name server.
Domain	Displays the name of the platform domain.
Secondary DNS	Displays the IP address of the secondary domain name server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.
Resources	
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays the amount of total memory, free memory, and used memory in KBytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

Hardware Status

To open the Hardware Status window, choose **Show Status > Hardware Status**. Table 6-2 describes the fields displayed in the window.

Table 6-2 Hardware Status Fields

Field	Description
Hardware Platform	Displays the model identity of the platform server.
Number of Processors	Displays the number of processors in the platform server.
CPU Type	Displays the type of processor in the platform server.
Memory	Displays the total amount of memory in MBytes.
Object ID	Displays the software object ID.
OS Version	Displays the version of the software operating system that is running on the platform.

Settings

Use the Settings windows to display and change:

- IP settings
- Host settings
- Network Time Protocol (NTP) settings
- Ping utility

IP Settings

The IP Settings window indicates whether Dynamic Host Configuration Protocol (DHCP) is active on Ethernet connections 0 and 1, lists the related Ethernet IP addresses, and shows the IP address for the network gateway.

To modify the IP settings, follow these steps:

Procedure

Step 1 Choose **Settings** > **IP Settings**.

Step 2 Enter the new value in the appropriate field as described in Table 6-3.

Step 3 Click **Execute**.

Table 6-3 IP Settings Fields

Field	Description
Ethernet 0 and Ethernet 1	
DHCP	Indicates whether DHCP is active.
IP Address	Shows the IP address of the DHCP server.
IP Mask	Show the IP subnet mask address of the DHCP server.
Network	
Gateway	Shows the IP address of the network gateway.

Host Settings

The Host Settings window displays the name and IP address of the platform host. You must set the values as part of the platform installation procedure.

To add a new host, follow these steps:

Procedure

Step 1 Choose **Settings** > **Host Settings**.

Step 2 Click **Add**.

Step 3 Enter a new host name and IP address.

Step 4 Click **Save**.

NTP Settings

The NTP Settings window displays the NTP settings and enables you to configure the platform as either an NTP server or an NTP client. From this window, you can also start and stop the NTP service.

To configure NTP settings, follow these steps:

Procedure

Step 1 Choose **Settings** > **NTP Settings**.

Step 2 Enter information according to the descriptions in Table 6-4.

Step 3 Click **Save**.

Table 6-4 NTP Settings Fields

Field	Description
NTP Status	
Status	Indicates whether the NTP service is active. Click **Start** or **Stop** to control the status of the NTP service.

Table 6-4 NTP Settings Fields (continued)

Field	Description
NTP Server Configuration (Platform is a client)	
Add/Delete	Add or delete an NTP server. To add an NTP server: 1. Click **Add**. 2. Enter the server IP address or hostname. 3. Click **Save**. A confirmation message is presented. 4. Click **NTP Setting**s to return the NTP Settings window. To delete an NTP server: 1. Check the box to the left of the server entry. 2. Click **Delete**. 3. Click **Save**. A confirmation message is presented. 4. Click **NTP Setting**s to return the NTP Settings window.
Address	Displays the IP address of the NTP server.
Hostname	Displays the name of the NTP Server.
Status	Indicates whether the NTP server is active.

Table 6-4 NTP Settings Fields (continued)

Field	Description
NTP Client Configuration (Platform is a server)	
Add/Delete	Add or delete an NTP client. To add an NTP client: 1. Click **Add**. 2. Enter the IP address and mask or enter the hostname. 3. Click **Save**. A confirmation message is presented. 4. Click **NTP Setting**s to return to the NTP Settings window. To delete an NTP client: 1. Check the box to the left of the entry. 2. Click **Delete**. 3. Click **Save**. A confirmation message is presented. 4. Click **NTP Setting**s to return to the NTP Settings window.
Address	Displays the IP address of the NTP client.
Hostname	Displays the name of the NTP client.
Mask	Displays the subnet mask of the NTP client.

Ping Utility

The Ping Utility window enables you to send ping messages to another server in the network.

To use the Ping utility, follow these steps:

Procedure

Step 1 Choose **Utilities** > **Ping**.

Step 2 Enter the destination IP address and number of ping packet to send.

Step 3 Click **Execute**.

Step 4 The Ping Utility window displays the ping statistics. Click **Cancel** or **Done** to terminate the ping operation.

Software Upgrade Windows

These Software Upgrade windows enable you to upgrade the Cisco IPT platform software from a local or a remote source, show the current software version, and verify individual software components:

- From Local Source
- From Remote Source
- Show Current Version
- Check Component Info

⚠ **Caution** Before attempting to upgrade the platform software, be sure that all other software upgrades and installations have completed. Check the latest Install/Upgrade log to be sure that no other instance of the Install/Upgrade process exists.

From Local Source

Use the From Local Source window to upgrade the server software from a CD or DVD.

Before You Begin

- Create or obtain the upgrade disk.
- Back up your system data. See the "Backing Up and Restoring the Database" section on page 3-12.

To perform the upgrade, follow these steps:

Procedure

Step 1 Insert the new CD or DVD into the disk drive on the local server that is to be upgraded.

Step 2 Choose **Software Upgrade > From Local Source**.

Step 3 Enter the required upgrade information, as described in Table 6-5:

Step 4 Click **Submit**.

You will see upgrade status messages including a list of previously downloaded images.

Step 5 Click **Cancel** if you need to terminate the upgrade operation before it is completed.

Table 6-5 Local Source Upgrade Fields

Field	Description
Upgrade Software Directory on CD/DVD	Enter the directory (on the CD or DVD) where the software upgrade is located.
Platform	Choose Linux (default).

From Remote Source

Use the From Remote Source window to upgrade software from a remote network location.

Before You Begin

Back up your system data. See the "Backing Up and Restoring the Database" section on page 3-12.

To upgrade from a remote location, follow these steps:

Procedure

Step 1 Choose **Software Upgrade > From Remote Source**.

Step 2 Enter the required upgrade information.

Table 6-6 describes the upgrade information.

Step 3 Click **Submit**.

Step 4 Choose a software version to download.

Step 5 Confirm the software upgrade.

Step 6 Reboot your system.

You will see upgrade status messages, including a list of previously downloaded images.

Table 6-6 Remote Source Upgrade Fields

Field	Description
Remote Software Server	Enter the host name or IP address of the remote server from which software will be downloaded.
Remote User	Enter the name of a user who is configured on the remote server.
Remote User Password	Enter the password that is configured for this user on the remote server.
Upgrade Software Directory	Enter the name of the directory from which software will be downloaded.
Download Protocol	Choose sftp (default) or ftp.
Platform	Choose Linux.

Show Current Version

From the Show Current Version window, you can view the current version of software that is running on the Cisco IPT Platform.

To view the current software version, follow these steps:

Procedure

Step 1 Choose **Software Upgrade > Show Current Version**.

Step 2 Click **Retrieve** to obtain version information.

Step 3 When you have finished viewing the information, click **OK**.

Check Component Info

From the Check Component Info window you can check these categories of information:

- Installed software packages
- Installation process
- Post-installation process
- Upgrade process
- Contents of a directory or file

To check the component information, follow these steps:

Procedure

Step 1 Choose **Software Upgrade > Check Component Info**.

Step 2 Choose one of the following types of information:

- Software Packages
- Install
- Post Install
- Upgrade

Alternatively, enter a file name to retrieve.

Step 3 (Optional) enter the number of lines to retrieve from the file. Entering 0 retrieves the entire file.

Step 4 Click **Retrieve**.

Step 5 An information window opens. Perform these functions in the information window:

- Click **Refresh** to retrieve updated information.
- Click **Cancel** to close the information window.
- To continue using the IPT Platform Administration pages, select from the menu located on the left side of the window.

System Power-off or Reboot

When you upgrade your software from a local or remote source, the software upgrade downloads to the standby partition in your server. From the Switch Versions and Reboot window, you can switch from the active partition (which is running the older version of software) to the standby partition (containing the upgraded software).

You can also reboot the system that is running the current software version or power down the system completely.

Switch Versions and Reboot

When you upgrade your software from either a local or remote source, the software upgrade is downloads to the standby partition in your server. From this window, you can switch from the active partition (which is running the older version of software) to the standby partition (containing the upgraded software):

Caution Be sure to perform a complete data backup before proceeding with the version switch and reboot.

- To proceed with the software version switch and system reboot, click **Proceed**.
- To cancel the software version switch and system reboot, click **Cancel**.

Reboot Current Version

From the Reboot Current Version window, you can reboot your system and continue running the same version of software:

Caution Be sure to perform a data backup before proceeding with the system reboot.

- To proceed with the system reboot, click **Proceed**.
- To cancel the system reboot, click **Cancel**.

Poweroff System

From the Poweroff System window, you can shut your system down safely:

Caution Be sure to backup your system data before starting the shutdown process.

- To start the system shutdown, click **Confirm**.
- To cancel the system shutdown, click **Cancel**.

Cisco IPT Platform Administration Command Line Interface

This section describes commands to perform basic platform administration functions. All the commands described in this section are also available using the Cisco IPT Platform Administration web application, as described in the "Using the Cisco IPT Platform Administration Web Pages" section on page 6-1.

Note It is recommended that you use the command-line interface (CLI) only when the Cisco IPT Platform Administration web application is not available.

The following CLI commands are available:

- file list
- file view
- ping
- restart
- service list
- service start
- service stop
- set hostname
- set ip (DHCP)
- set ip (IP)
- set security
- set task alarm
- set task trace
- show status
- show hw
- show security
- show files activelog
- show files activlog cli.log
- show files inactive log
- show files install
- show files install ks.cfg
- show files install partAlloc
- show files install install.log
- show files install install.post
- tracert

Starting a CLI Session

You can access the Cisco IPT Platform Administration CLI from a local or remote location:

- Access the Cisco IPT Platform Administration CLI directly by using the monitor and keyboard that you used during Cisco MobilityManager installation or by using a terminal server that is connected to the serial port.
- Use SSH to make a secure connection to the Cisco IPT Platform Administration CLI from a client workstation.

Before You Begin

Ensure that the Cisco IPT Platform is installed with the following information configured:

- A primary IP address and hostname
- An administrator ID
- A password

You will need this information to log in to the Cisco IPT Platform Administration CLI.

To start a CLI session, perform these steps:

Procedure

Step 1 Choose one of these options to connect to the CLI:

- From a remote system, use SSH to connect securely to the Cisco IPT Platform Administration CLI. In your SSH client, enter

  ssh *adminname@hostname*

  where ***adminname*** specifies the Administrator ID and ***hostname*** specifies the hostname that waqs defined during installation.

  For example, **ssh admin@ipt-1**.

- From a direct connection, you receive this prompt automatically:

  ```
  ipt-1 login:
  ```

  where **ipt-1** represents the host name of the system.

Enter the administrator ID that was defined during installation.

Step 2 Enter the password.

The CLI prompt is presented. The prompt includes the Administrator ID, as in this example:

admin:

You can enter CLI commands.

Related Topics

CLI Basics

Ending a CLI Session

CLI Basics

This section contains basic tips for using the command line interface.

Completing Commands

To complete commands, use **Tab**:

- Enter the start of a command and press **Tab** to complete the command. For example, if you enter **se** and press **Tab**, **set** gets completed.
- Enter a menu command and press **Tab** to display all the commands or menu commands that are available at this menu. For example, if you enter **set** and press Tab you see all the set menu commands. An asterisk (*) identifies the menus.
- If you reach a command and keep pressing **Tab**, the current command line repeats; no additional expansion is available.

Getting Help on Commands

You can obtain two kinds of help on any command:

- Detailed help including a definition of the command and an example of its use
- Short query help including only command syntax

To obtain detailed help from the CLI prompt, enter:

help <command> where <command> specifies the command name or menu command and parameter. See Example 6-1.

To obtain command syntax information from the CLI prompt, enter:

<command> ? where <command> represents the command name or menu command and parameter. See Example 6-2.

Note Entering a question mark (?) after a menu command is equivalent to pressing the Tab key. The possible command completions are listed.

These examples show typical uses of the help commands.

Example 6-1 Detailed Help Example

```
admin: help ping

This will send one or more ping packets to a remote destination
Example:
admin:ping www.cisco.com 5
PING www.cisco.com (198.133.219.25) from 172.22.119.166 : 56(84) bytes
of data.
64 bytes from 198.133.219.25: icmp_seq=1 ttl=246 time=0.837 ms
64 bytes from 198.133.219.25: icmp_seq=2 ttl=246 time=0.962 ms
64 bytes from 198.133.219.25: icmp_seq=3 ttl=246 time=1.04 ms
64 bytes from 198.133.219.25: icmp_seq=4 ttl=246 time=0.635 ms
64 bytes from 198.133.219.25: icmp_seq=5 ttl=246 time=0.666 ms
```

Example 6-2 Query Example

```
ping?
Syntax:
ping dest [count]
dest     mandatory    dotted IP or host name
count    optional     count value (default is 4)
```

Ending a CLI Session

To end the CLI session, enter **quit** at the CLI prompt. The system responds in one of these ways:

- If you are logged in remotely, you are logged off, and the ssh session gets dropped.
- If you are logged in locally, you are logged off, and the login prompt returns, as in this example:

```
login:
```

Cisco IPT Platform CLI Command List

Table 6-7 lists and describes the commands that are available on the Cisco IPT Platform Administration CLI.

Caution Some commands may slow down call processing. Refer to the notes in Table 6-7 for more information.

Table 6-7 CLI Command Description

Command	Description	Counterpart in Cisco IPT Platform Administration
ping dest [count]	Execute a **ping** command to the specified destination. **dest** (mandatory): Destination, the ipV4 or domain name. *count* (optional): Number of pings to execute.	**Utilities** > **Ping**
file list	Lists the log files in a directory. Sort Modifiers: default dir (name) and files (name) d date (will override size if requested) s size r reverse of any sort Display Modifiers: default file only / 2 columns l long listing with date and size File-spec -Wild Carding file name will produce a regular listing using the above modifies directories will produce a listing showing full path of directories Syntax: **file list activelog [-options] [file-spec]** **inactivelog [-options] [file-spec]** **install [-options] [file-spec]** options optional -tsrl file-spec optional file to view	-

Table 6-7 CLI Command Description (continued)

Command	Description	Counterpart in Cisco IPT Platform Administration
file view	Displays a log file. Sort Modifiers: default dir (name) and files (name) d date (will override size if requested) s size r reverse of any sort Display Modifiers: default file only / 2 columns l long listing with date and size file-spec -wildcarding File name will produce a regular listing using the above modifier directories will produce a listing showing full path of directories Syntax: **file view activelog [file-spec]** **inactivelog [file-spec]** **install [file-spec]** file-spec optional file to view **Note** file-spec wildcarding is allowed, but must resolve to a single file.	

Table 6-7 CLI Command Description (continued)

Command	Description	Counterpart in Cisco IPT Platform Administration

set ip	Set or change various aspects of network configuration that are originally set at installation:
	• Set DHCP on or off
	• Set a new IP address and IP mask
	• Set a new gateway address
	Syntax:
	set dhcp iface op
	iface (mandatory): Interface name {eth0 | eth1}
	op (mandatory): Operation {yes | no}
	Example:
	`set dhcp eth0 on`
	set ip iface addr mask
	iface (mandatory): Interface name {eth0 | eth1}
	addr (mandatory): IP address to be assigned
	mask (mandatory): IP mask to be assigned
	Example:
	`set ip eth0 10.10.140.8  255.255.255.0`
	set gw addr
	addr (mandatory): IP address to be assigned
	Example:
	`set gw 10.107.140.1`
	Note Set ip commands force a system reboot so you should use with caution. You receive a warning asking for confirmation before this command executes.
		Settings > IP Settings

Table 6-7 CLI Command Description (continued)

Command	Description	Counterpart in Cisco IPT Platform Administration
set password admin	Change the password for the Administrator account (the default and only account) that was set during installation. You will be prompted to enter and confirm the new password.	-

set security orgunit orgname locality state country	Create a new security certificate and key for Tomcat on this machine. The security key gets used if you configured browser access to Cisco IPT platform to use the secure https protocol instead of http.
	Note This command does not apply to a Cisco IPT Platform which does not support https.
	Use the set security command if the original key is compromised or if your certificate has expired. After you create the new key, use show security to display it.
	Enter spaces between parameters
	orgunit (mandatory)—Organization unit
	orgname (mandatory)—Organization name
	locality (mandatory)—Location
	state (mandatory)—State
	country (mandatory)—Country (two letters)
	Example:
	`admin:set security mydept mycorp SanJose CA US`
	`Successful in generating self signed`
	`certificate for unitname tomcat`
	`Successfully generated self signed certificate`
	`for tomcat`
		-

Table 6-7 CLI Command Description (continued)

Command	Description	Counterpart in Cisco IPT Platform Administration
service list **service start [service name]** **service stop [service name]**	List, start, or stop services.	-
show files install [filename]	View the install logs file list. *filename* (optional): Name of the file to view	In Cisco IPT platform Administration, use the Collect Diagnostics command to collect diagnostic files
show hw	Show the hardware platform and serial number.	**Show Status > Hardware**
show security	Show the Tomcat security key and certificate information. The security key get used if you configured browser access to Cisco IPT Platform to use the secure https protocol instead of http.	-

Table 6-7 CLI Command Description (continued)

Command	Description	Counterpart in Cisco IPT Platform Administration
show status	Show the dynamic status of these properties: • Host name • Date • Time Zone • Primary DNS • Secondary DNS • Domain • Gateway • For Ethernet 0 and Ethernet 1: – DHCP (yes or no) – Status of the interface – IP Address – IP Mask • Resources: – Memory: Total, Free, Used – CPU (percent): Idle, System, User – Disk Usage: Disk/activecomes from partition /, Disk/inactivecomes from partition /partB, Disk/logging comes from partition /common	**Show Status > Platform Status**
show trace	Displays trace information.	
show version active **show version inactive**	Displays the active or inactive Cisco IPT Platform Administration software version.	-

Table 6-7 CLI Command Description (continued)

Command	Description	Counterpart in Cisco IPT Platform Administration
system [parameter]	Restart, switch versions and restart or shut down the server as specified in the parameter: system restart: Restart current version system switch-ver: Switch versions and restart system poweroff: Shut down gracefully. **Note** You receive a warning asking for confirmation before this command executes.	**System Poweroff or Reboot > Reboot Current Version** **System Poweroff or Reboot > Switch Versions and Reboot** **System Poweroff or Reboot > Poweroff System**
traceroute dest [ethX]	Execute a traceroute command, tracing the path a packet takes to a destination. Use to debug routing problems between hosts: **dest** (mandatory): Destination, the (ipV4 or domain name *ethX* (optional): Source Ethernet interface, eth0 or eth1	-

INDEX