



Cisco Unified Messaging Gateway 8.5 Administrator Guide

First Published: December 2, 2010

Last updated: August 5, 2011

Americas 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: 408 527-0883

Customer Order Number: OL-23984-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



CONTENTS

Notices	iii
OpenSSL/Open SSL Project	iii
License Issues	iii

Preface xiii

About this Guide	xiii
Obtaining Documentation and Submitting a Service Request	xiii
Technical Assistance	xiv

PART 4

Overview and Initial Configuration

Cisco Unified Messaging Gateway Overview 15

Introduction	15
E-SRST and SRSV Licenses and When to Deploy Them	16
Enhanced Survivable Remote Site Telephony (E-SRST)	17
E-SRST Limitations	19
Survivable Remote Site Voicemail (SRSV)	19
Introduction to SRSV	19
Supported SRSV Topologies	20
SRSV Limitations	22
Limitations for Interoperating with Cisco Unified Communications Manager	23
Voicemail Limitations and Restrictions	23
Auto Attendant Limitations	24
Network Address Translation (NAT) Restrictions	24
High Availability Restrictions	24
Voicemail Backup and Restore Limitations	25
Mailbox Limitations	25
Live Record and Live Reply Limitations	25
Distribution Lists	25
Combined SRSV and E-SRST on the Same Site	26
Voice Profile for Internet Mail (VPIM) Networking	27
VPIM Endpoint Management	27
Managing a Network of Cisco UMG VPIM Nodes	29
Administration Interfaces	29
Command-Line Interface	29

Graphical User Interface 30

Entering and Exiting the Command Environment 15

- About EXEC and Configuration Modes 15
 - Similarities Between the Cisco UMG CLI and the IOS CLI 15
 - Differences Between the Cisco UMG CLI and the IOS CLI 15
- Entering the Command Environment 16
 - Prerequisites 16
- Exiting the Command Environment 17
- Finding More Information about CLI Commands 17

Initial Configuration Tasks 15

- Adding a DNS Server 15
 - Adding a DNS Server: Systems with Cisco Unity 15
 - Adding a DNS Server: Systems without Cisco Unity 15
- Setting Backup Parameters 16
 - About Backup Parameters 16
 - Prerequisites 16
 - Example 18
- Configuring NTP Servers 18
 - Adding NTP Servers 18
 - About Adding NTP Servers 18
 - Examples of Adding NTP Servers 19
 - Removing an NTP Server 20
 - Displaying NTP Server Information 21
 - Commands to Display NTP Server Information 21
 - Examples of Showing NTP Server Information 21
- Setting the Time Zone 23
 - Example of Setting the Time Zone 23
- Configuring Logging Operations 24
 - About Logging Operations 24
 - Prerequisites 24
 - Example 25

PART 2

E-SRST and SRSV Configuration

Preparing Cisco UMG to Support E-SRST and SRSV Functionality 51

- Prerequisites 51
 - How to Enable SMTP Support for Cisco UMG on Cisco Unity Connection 52
- About Security for Cisco UMG 52

About Security	52
About Security Certificates	53
Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager	53
Installing the Security Certificates	54

Configuring E-SRST Site Provisioning 51

Using E-SRST to Pull an Advanced Telephony Configuration from CUCM to the Branch Site	51
Initial Configuration Using the Cisco UMG GUI	52
Preparing the Central CUCM Call Agent for E-SRST Provisioning	52
Adding the Central Call Agent Using the Cisco UMG Central Call Agent Wizard	54
Configuring the CUCME Branch Call Agent to Prepare for E-SRST Provisioning	54
Configuring the CUCME Branch Call Agent to Support E-SRST Provisioning	54
Configuring CUCME Dial Peers to Support E-SRST Provisioning of Ephone-dns and Hunt Groups	55
Enabling E-SRST Provisioning on the Site Using the Cisco UMG GUI	56
Verifying the Updated Configuration on the Branch Call Agent Router	57

Verifying Site and Provisioning Status on the Cisco UMG 51

Verifying E-SRST and SRSV Site Information	51
Verifying E-SRST and SRSV License Information	51
Verifying Site Information	51
Verifying Site Template Information	52
Verifying Central Call Agent Information	52
Verifying Branch Call Agent Information	52
Verifying Branch Voicemail Server Information	52
Verifying the Site Provisioning History	52

PART 3

VPIM Network Configuration

Configuring Endpoints for VPIM Networks 67

Configuring Peer Messaging Gateways	68
Prerequisites	68
Examples	69
Message Handling	69
Default Destination	69
Notice of Delayed Delivery or Non-delivery	69
Prerequisites	70
Examples	71
Configuring Endpoint Autoregistration Support	71
Prerequisites	72

Examples	74
Provisioning Endpoints Manually	74
Prerequisites	75
Examples	79
Setting Up NAT Entries	80
Prerequisites	80
Examples	81
Forcing Data Convergence	81
Prerequisites	82
Examples	83
Managing System Distribution Lists	83
Prerequisites	84
Examples	86
Managing System Broadcasts	87
Prerequisites	87
Examples	89
Deleting Peer Messaging Gateways	89
Examples	90
Deleting or Clearing Endpoints	91
Examples	92
Blocking Endpoint Registration	92
Prerequisites	92
Viewing Network Status	94
Locating and Viewing Individual Mailbox Details	94
Examples	96
Configuring Cisco Unity Express Endpoints for Autoregistration to Cisco UMG	67
Overview of the Autoregistration Process	67
Configuring Cisco Unity Express Autoregistration with Cisco UMG	68
Example	72
Manually Registering a Cisco Unity Express Endpoint	73
Verifying the Registration Status of a Cisco Unity Express Endpoint	73
Enabling or Disabling Remote Lookup, With or Without TUI Confirmation	75
Viewing Cached and/or Configured Network Locations	76
Refreshing Locations	76
Setting the Expiration for Cached Locations	76
Overloading a NAT Device: the Consequences for Endpoints	76

PART 4**Other Features****Configuring Authentication, Authorization, and Accounting 109**

- Overview 109
- Configuring the Accounting Server 110
 - Specifying AAA Accounting Settings 110
- Configuring the Authentication Server 112
 - Specifying AAA Authentication Settings 112
- Configuring the AAA Policy 114
 - Authentication Failover 114
 - Unreachable Failover 114
 - Example 114
 - Specifying the Policy that Controls the Behavior of Authentication and Authorization 115
- Configuring Privileges 116
 - Configuration Example 119
 - Creating and Customizing Privileges 121
- Configuring Accounting Event Logging 123
 - Configuring Accounting Event Logging 124
- Configuring Console Authentication 126
 - Specifying Whether the Console Connection is Subject to Authentication 126

PART 5**Maintenance and Troubleshooting****Backing Up and Restoring Data 131**

- About Backing Up and Restoring Data 131
- Restrictions for Backing Up and Restoring Data 132
- Setting Backup Parameters 132
 - Prerequisites 132
 - Required Data for This Procedure 132
 - Examples 133
- Backing Up Files 134
 - Examples 135
- Restoring Files 136
 - Example 138
- Backup and Restore Using SFTP 139
 - Overview 139
 - Configuring Backup and Restore Using SFTP 139
 - Prerequisites 139
 - Required Data for This Procedure 139

Backup Server Authentication Using a SSH Host Key	140
Overview	140
Configuring Backup Server Authentication Without Using the SSH Host Key	141
Prerequisites	141
Required Data for This Procedure	141
Configuring Backup Server Authentication Using the SSH Host Key	142
Prerequisites	142
Required Data for This Procedure	142
Encrypting and Signing of Backup Content on the Server	143
Overview	143
Configuring the Encryption and Signing of Backup Content on the Server	143
Prerequisites	143
Required Data for This Procedure	143
Configuring Scheduled Backup Jobs	144
Prerequisites	145
Examples	147
Disabling or Reenabling All Scheduled Backups	147
Prerequisites	147
Monitoring the Cisco UMG System	131
Checking Hard Disk Memory Wear Activity	131
Checking Log and Trace Files	131
Troubleshooting	131
About Troubleshooting	131
Running a Network Connectivity Test	131
Log and Trace Files	132
About Logging	132
Example of Log Output	133
Log Commands in Cisco UMG Configuration Mode	133
Log Commands in Cisco UMG EXEC Mode	133
Saving and Viewing Log Files	133
Saving Configuration Changes	134
Using Trace Commands	134
Examples	134
Maintaining the Cisco UMG System	131
Copying Configurations	131
Copying the Startup Configuration from the Hard Disk to Another Location	131
Copying the Startup Configuration from the Network FTP Server to Another Location	132

Examples	133
Copying the Running Configuration from the Hard Disk to Another Location	133
Examples	133
Copying the Running Configuration from the Network TFTP Server to Another Location	134
Examples	134
Restoring Factory Default Values	134
Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online	135
Taking the Cisco UMG System Offline	135
Example	136
Restarting the Cisco UMG System	136
Example	136
Shutting Down the Cisco UMG System	137
Shutting Down the Software	137
Shutting Down the Hardware	137
Putting the Cisco UMG System Back Online	137

INDEX



Preface

Last updated: December 2, 2010

- [About this Guide, page xiii](#)
- [Obtaining Documentation and Submitting a Service Request, page xiii](#)

About this Guide

This guide provides an overview to the Cisco Unified Messaging Gateway features, as well as information on how to configure Voice Profile for Internet Mail (VPIM) networking using the command line interface (CLI). This guide also describes how to use the CLI to perform routine maintenance such as troubleshooting, monitoring operations, and backing up and restoring data.

For information on configuring the Enhanced Survivable Remote Site Telephony (E-SRST) and Survivable Remote Site Voicemail (SRSV) features using the GUI, see [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and RSS Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com username and password.</p>	http://www.cisco.com/techsupport



PART 1

Overview and Initial Configuration



Cisco Unified Messaging Gateway Overview

Last updated: December 2, 2010

This chapter provides an overview of Cisco Unified Messaging Gateway and the features supported. This chapter covers the following topics:

- [Introduction, page 15](#)
- [Enhanced Survivable Remote Site Telephony \(E-SRST\), page 17](#)
- [Survivable Remote Site Voicemail \(SRSV\), page 19](#)
- [Combined SRSV and E-SRST on the Same Site, page 26](#)
- [Voice Profile for Internet Mail \(VPIM\) Networking, page 27](#)
- [Administration Interfaces, page 29](#)

Introduction

Cisco Unified Messaging Gateway 8.5 is an application that resides on an enhanced network module (NME) or Services Ready Engine service module (SM-SRE). The module plugs into a host Cisco router running Cisco IOS software. All models are shipped from the factory with the software preinstalled.

Cisco Unified Messaging Gateway (UMG) release 8.5 is supported on the following modules:

- NME-UMG
- NME-UMG-EC
- SM-SRE-700-K9
- SM-SRE-900-K9

For more information about hardware support requirements, see the [Release Notes for Cisco Unified Messaging Gateway](#).

Cisco UMG supports the following features:

- [Enhanced Survivable Remote Site Telephony \(E-SRST\), page 17](#)
- [Survivable Remote Site Voicemail \(SRSV\), page 19](#)
- [Voice Profile for Internet Mail \(VPIM\) Networking, page 27](#)

For information about how each feature is deployed, see the following sections. For information about deployment scenarios combining E-SRST and SRSV on a site, see the [“Combined SRSV and E-SRST on the Same Site” section on page 26](#). For information on the different options for deploying E-SRST and SRSV licenses, see the [“E-SRST and SRSV Licenses and When to Deploy Them” section on page 16](#).

Feature licenses for E-SRST, SRSV, and VPIM are available in increments of 25 sites or nodes each. For example, if you are deploying 25 SRSV sites, then you must purchase one SRSV feature license. If you are deploying 30 SRSV sites, then you must purchase two SRSV feature licenses. For more information about feature licenses, see the [Release Notes for Cisco Unified Messaging Gateway](#).

E-SRST and SRSV Licenses and When to Deploy Them

The E-SRST and SRSV features can be deployed separately or together on a given site. You can configure a site for either feature or both depending on your needs. For each feature deployed at each site, a feature license must be purchased.

The supported call control methods on a branch site are:

- Survivable Remote Site Telephony (SRST), also referred to as “original” SRST.
- Cisco Unified Communications Manager Express as Survivable Remote Site Telephony (CUCME-as-SRST)

CUCME-as-SRST is also known as the SRST Fallback Mode feature on Cisco Unified Communications Manager Express (CUCME).

E-SRST is not required if you are using original SRST and are not provisioning advanced telephony features for use in survivable mode. E-SRST is recommended if you plan to use advanced Cisco Unified Communications Manager (CUCM) telephony features in survivable mode.

[Table 1](#) summarizes the different options for enabling E-SRST and/or SRSV on a given site.

Table 1 *Cisco UMG 8.5 Features and Call Control Options on a Branch Site*

Features Enabled on a Site ¹	Call Control Method	Provisioning of Advanced Telephony Features	Survivable Remote Site Voicemail Supported on the site ²	For a Sample Topology, see:
E-SRST only	CUCME-as-SRST	Provisioned on central CUCM, automatically downloaded to the branch site.	No	Figure 1
SRSV only	SRST	Not Applicable ³	Yes	Figure 2
SRSV only	CUCME-as-SRST	Manually provisioned on the branch site.	Yes	Figure 3
E-SRST and SRSV	CUCME-as-SRST	Provisioned on central CUCM, automatically downloaded to the branch site.	Yes	Figure 5

1. Feature license must be installed on a per-site basis for provisioning to take place.
2. Requires SRSV-CUE software to be installed on the branch voicemail server.
3. Original SRST does not support advanced telephony features.

For more detailed information about each feature, see the [Enhanced Survivable Remote Site Telephony \(E-SRST\)](#) below and the “[Survivable Remote Site Voicemail \(SRSV\)](#)” section on page 19.

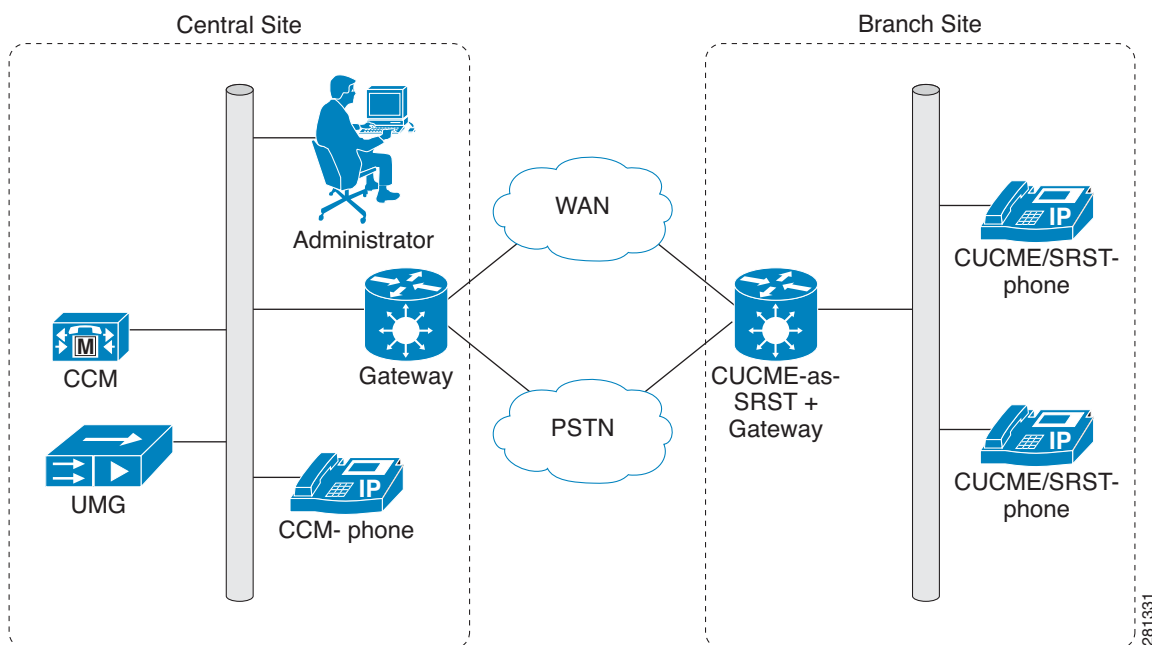
Enhanced Survivable Remote Site Telephony (E-SRST)

Enhanced Survivable Remote Site Telephony (E-SRST) is supported in Cisco UMG 8.5 and later versions. The E-SRST functionality requires the installation of E-SRST licenses, with each license supporting up to 25 sites per license. The E-SRST feature can be deployed separately or combined on a given site with [Survivable Remote Site Voicemail \(SRSV\)](#). See also the “[Combined SRSV and E-SRST on the Same Site](#)” section on page 26.

E-SRST provides an integrated solution that supports advanced CUCME-as-SRST telephony features such as hunt groups and pick-up groups, but reduces the complex and manual configuration required at the branch site.

If deploying E-SRST, the UMG system at the central office collects information from CUCM, generates the complex configuration information required for advanced features such as hunt groups and pick-up groups, and then distributes this configuration information to the branch office sites. In the event of a WAN outage, when the CUCME-as-SRST service running on the branch office routers takes over call processing, it leverages the configuration provisioned by the central office UMG system to provide enhanced SRST services at the branch.

[Figure 1](#) shows the supported topology model for E-SRST on a branch site. In this example, SRSV is not deployed at the branch site.

Figure 1 E-SRST Only Topology

E-SRST provides automated remote site provisioning of the following advanced telephony features in survivable mode by gathering the information from CUCM:

- End-user phones and extensions (speed dials, lines, softkeys)
- Voicemail and call forward configuration
- Call routing restrictions (local and long distance, and time of day)
- Call pickup and group pickup
- Hunt groups
- Pick-up groups
- After-hours
- Class of Restrictions (COR)
- Directory numbers

E-SRST enables an administrator to set up provisioning schedules for defining when and how often to fetch configuration information from CUCM and provision the branch office CUCME-as-SRST routers. The administrator can also do an on-demand provisioning to synchronize a specific CUCME-as-SRST router with the CUCM information.

The CUCME-as-SRST configuration in the E-SRST solution enables a phone in SRST mode to operate similarly to when the system is in normal CUCM mode. The look and feel of the phone displays and softkeys in SRST mode are similar to those in normal CUCM mode.

For more information about CUCME, see the documentation at:

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps4625/tsd_products_support_series_home.html.

E-SRST Limitations

This section describes the limitations for E-SRST.

- The following scenarios for E-SRST are not supported in Cisco UMG 8.5:
 - Provisioning advanced E-SRST features on an original SRST router at the branch. In this scenario, the central E-SRST router does not replace the original SRST with CUCME-as-SRST.
 - E-SRST supports only SRSV-CUE at the branch site, with Cisco Unity Connection at the central site. E-SRST does not support a Unity-only or Cisco Unity Express-only messaging network.
- E-SRST requires CUCME 7.1 and higher.
- Secure SRST is not supported.
- E-SRST does not actually configure or create dial peers and translation rules. The dial peers and translation rules are configured on CUCM and propagated to the branch site.
- Extension Mobility on CUCM is not supported.

Survivable Remote Site Voicemail (SRSV)

This section describes the Survivable Remote Site Voicemail (SRSV) solution and it covers the following topics:

- [Introduction to SRSV, page 19](#)
- [Supported SRSV Topologies, page 20](#)
- [SRSV Limitations, page 22](#)

Introduction to SRSV

Survivable Remote Site Voicemail (SRSV) is supported in Cisco UMG 8.0 and later versions. The SRSV functionality requires the installation of SRSV licenses, with each license supporting up to 25 nodes per license. The SRSV feature can be deployed separately on a given site or combined with [Enhanced Survivable Remote Site Telephony \(E-SRST\)](#).

The SRSV solution requires the following two components:

- Cisco Unified Messaging Gateway-Survivable Remote Site Voicemail (SRSV-UMG)

The SRSV-UMG component is deployed at the central office alongside Cisco Unified Communications Manager (CUCM) and Cisco Unity Connection (CUC). The SRSV-UMG component is deployed using Cisco Unified Messaging Gateway software with SRSV licenses installed. For product versions compatible with Cisco SRSV-UMG, see the [Release Notes for Cisco Unified Messaging Gateway](#).

- Cisco Unified Survivable Remote Site Voicemail-Cisco Unity Express (SRSV-CUE)

The SRSV-CUE component is deployed at the branch office alongside Cisco Unified Communications Manager Express (CUCME) or Cisco Unified Survivable Remote Site Telephony (SRST). Cisco Unified SRSV-CUE is a separate orderable product, and different hardware and software requirements apply. For more information, see the [Release Notes for Cisco Unified Survivable Remote Site Voicemail](#) and the [Installation and Administration Guide for Cisco Unified Survivable Remote Site Voicemail](#).

**Note**

While similar to Cisco Unity Express, SRSV-CUE is a different product and provides a limited subset of features for survivable mode only. The SRSV solution does not support interoperability with Cisco Unity Express.

The standalone SRSV solution introduced in Cisco Unified Messaging Gateway 8.0 uses either original SRST or CUCME-as-SRST. Original SRST requires simple, very limited provisioning on the remote office router, but provides very limited features to support basic phone calls. CUCME-as-SRST, also known as SRST Fallback Mode, provides advanced telephony features such as hunt groups and pick-up groups that are not available with original SRST, but it requires more complex and manual provisioning on the branch routers. For information about configuring CUCME-as-SRST, see the “[Configuring SRST Fallback Mode](#)” chapter in the *Cisco Unified Communications Manager Express System Administrator Guide*.

The Enhanced Survivable Remote Site Telephony (E-SRST) feature introduced in Cisco Unified Messaging Gateway 8.5 reduces the manual provisioning required for selected advanced telephony features supported by CUCME-as-SRST. For more information, see the “[Enhanced Survivable Remote Site Telephony \(E-SRST\)](#)” section on page 17.

When deployed and provisioned, the SRSV-CUE system sits idle in the branch office, ready to receive calls from the SRST system (either original SRST or CUCME-as-SRST). The SRST component (provisioned by Cisco Unified Communications Manager), also sits idle, waiting for IP phones to register with it. When a WAN outage occurs, the branch office IP phones that are registered to the central office CUCM detect the loss of connectivity and re-home to the SRST. Incoming PSTN calls to the branch office are then handled by the SRST. For calls that are either no-answer or reach a busy line, the SRST can forward to the SRSV system. As a result, the branch office voicemail is supported during WAN outages when the central office voicemail system is unreachable.

When the WAN connection returns, the IP phones automatically re-home to the central office CUCM. Call handling is then managed by CUCM, and no-answer / busy calls are forwarded to the central office CUC voicemail system.

**Note**

The documentation and product may refer to the branch office as the branch voicemail server or the SRSV-CUE device. These terms are used interchangeably and refer to the same device.

Supported SRSV Topologies

Several SRSV topologies are supported beginning with Cisco UMG 8.0. Depending on the configuration, you can have either original SRST or CUCME-as-SRST (also known as SRST Fallback Mode) deployed at the branch site. Note that if you are running SRST at the branch site, you cannot also deploy the E-SRST feature. See [Table 1](#) for the supported combinations of features.

[Figure 2](#) shows a topology in which SRST is deployed at the branch site. If the WAN or PSTN goes down, the SRSV-CUE at the branch site provides limited voicemail support in failover mode.

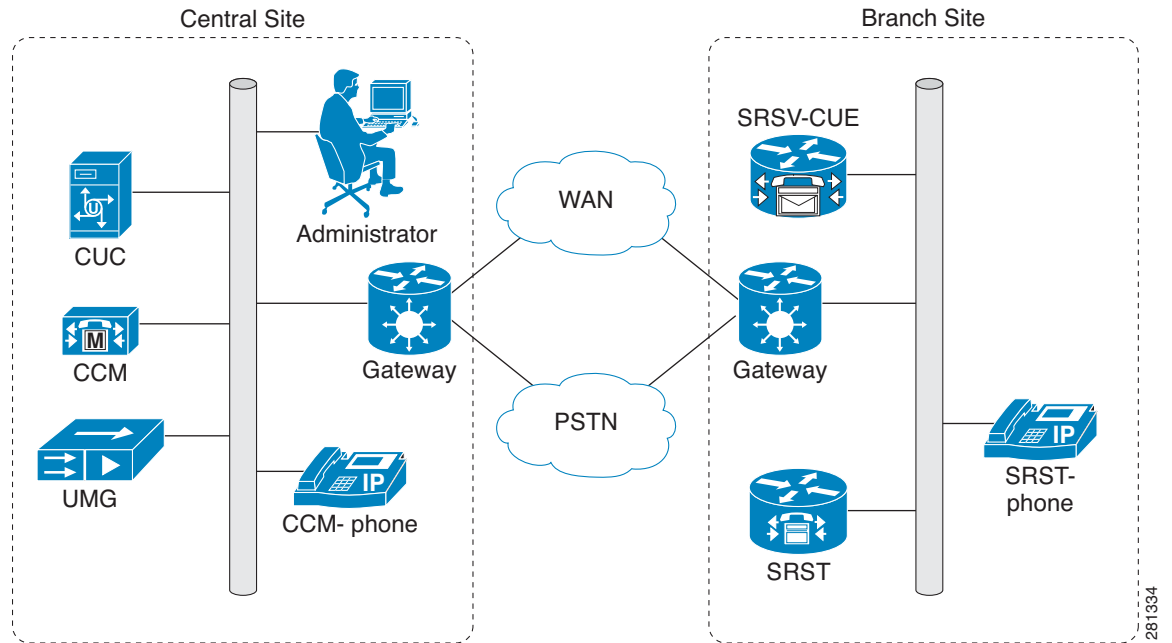
Figure 2 *SRSV Topology Using SRST at the Branch Site*

Figure 3 shows a topology where CUCME-as-SRST (also known as SRST Fallback Mode) is providing call control at the branch site.

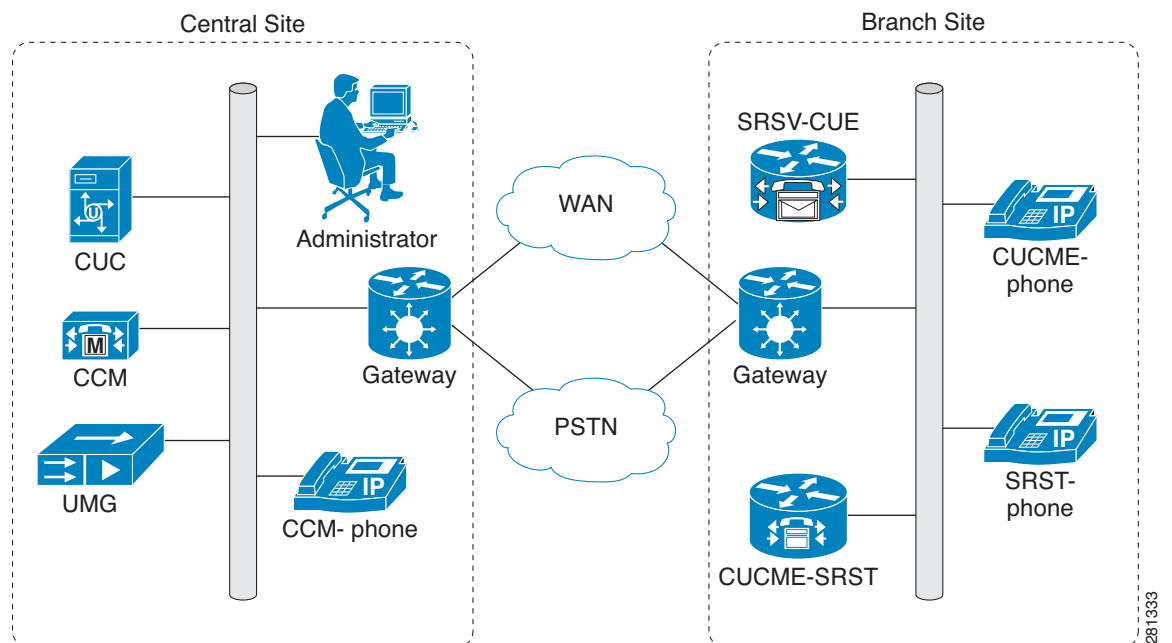
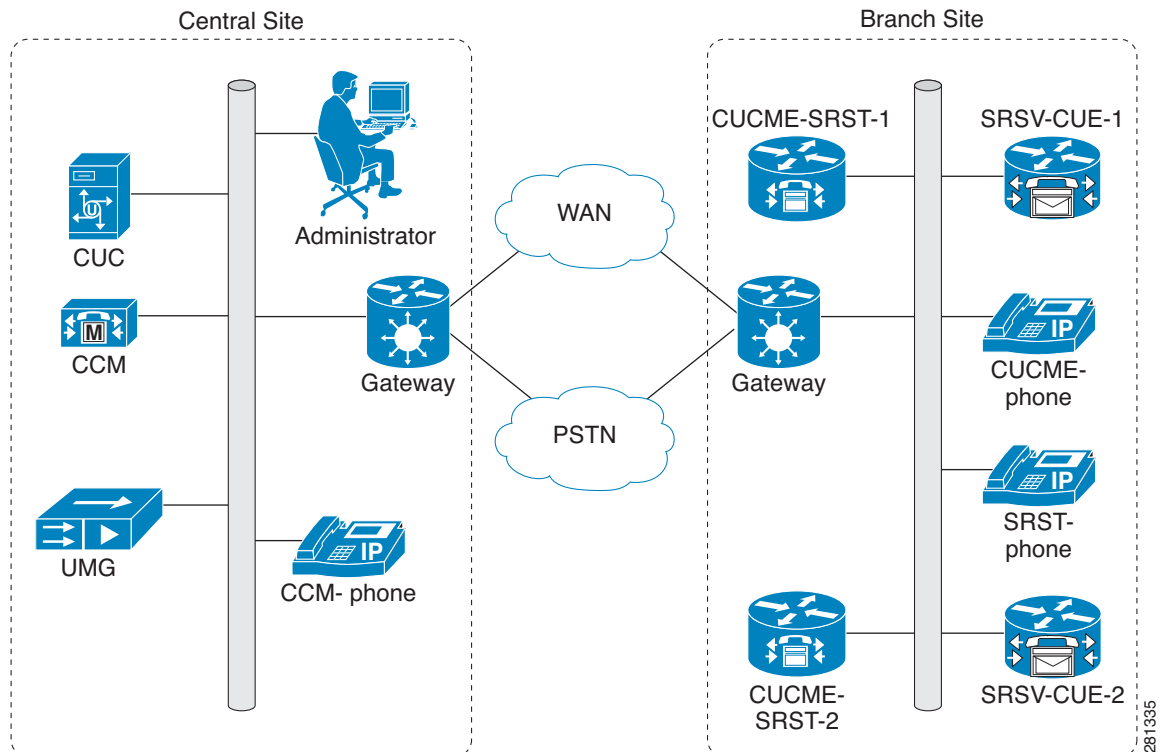
Figure 3 *SRSV Topology Using CUCME-as-SRST at the Branch Site*

Figure 4 shows a topology where multiple CUCME-as-SRST and SRSV-CUE devices are paired for load balancing at the survivable branch site. In this scenario, the administrator uses CUCM to divide the branch users between CUCME-SRST-1 and CUCME-SRST-2. The Cisco UMG learns about which phones are assigned to each device, and then pulls the relevant voicemail configuration from Cisco Unity Connection at the central site, and then pushes the appropriate configuration to SRSV-CUE-1 and SRSV-CUE-2 at the branch site. In the event of a WAN failure, each SRSV-CUE device will handle calls directed to it from the paired CUCME-as-SRST device.

Figure 4 SRSV Topology with Multiple CUCME-as-SRST Devices Load Balanced at Remote Site



SRSV Limitations

This section describes the limitations for the SRSV solution.

- [Limitations for Interoperating with Cisco Unified Communications Manager, page 23](#)
- [Voicemail Limitations and Restrictions, page 23](#)
- [Auto Attendant Limitations, page 24](#)
- [Network Address Translation \(NAT\) Restrictions, page 24](#)
- [High Availability Restrictions, page 24](#)
- [Voicemail Backup and Restore Limitations, page 25](#)
- [Mailbox Limitations, page 25](#)
- [Live Record and Live Reply Limitations, page 25](#)
- [Distribution Lists, page 25](#)

Limitations for Interoperating with Cisco Unified Communications Manager

- Extension Mobility is not supported.

Voicemail Limitations and Restrictions

- The following features are not supported with Cisco Unified Messaging Gateway 8.5:
 - Fax support.
 - Addressing non-subscribers.
 - Dispatch messages.
 - Scheduled base services, such as alternate greetings and notifications.
 - Advanced telephony features, such as call screening.
 - Updating spoken name, distribution lists, or PINs through the telephony user interface (TUI).
 - TUI administration interfaces, such as broadcast or greeting administration.
 - Private distribution lists.
 - Text-to-speech or voice recognition features.
 - Customizing the voicemail TUI flows on a SRSV-CUE device.
- Voicemail synchronization is one way. Voicemail received on Cisco Unity Connection is not replicated to the Cisco Unified SRSV-CUE device.
- The Message Waiting Indicator (MWI) for a Cisco Unified SRSV-CUE device does not track the state of the Cisco Unity Connection mailbox.
- Subscribers can permanently delete messages so that they will never be uploaded.
- Voicemail upload is not synchronized with phone re-home to CUCM.
- Only G.711 encoded spoken names and greetings are downloaded from Cisco Unity Connection. If no spoken names or greetings are downloaded, the system uses the system defaults from Cisco Unity Connection.
- Some class of service Cisco Unity Connection features are provisioned for all Cisco Unified SRSV-CUE users (such as live reply, distribution list access, and message deletion behavior).
- Before you can upload voicemail to a secondary Cisco UMG, you have to configure the Cisco Unity Connection information, including the Representational State Transfer (REST) password on the secondary Cisco UMG.
- Composed messages are not delivered immediately to branch voicemail servers in Cisco Unified SRSV mode. They are delivered after the WAN recovers.
- The system only updates the activity history after the voicemail is uploaded.
- You cannot monitor the upload of voicemail to a secondary UMG.
- Subscribers cannot log in to Cisco Unified SRSV-CUE devices until they set up their voicemail preferences on Cisco Unity Connection.
- Cisco Unified SRSV-CUE devices only support PINs in the SHA1 format. If you are upgrading to the Cisco Unified SRSV system from Cisco Unity Connection, ensure that all your subscribers reset their PINs so that they are saved in the SHA1 format.

Auto Attendant Limitations

- The following auto attendant features are supported:
 - Opening greeting call handler and its descendants
 - Local user only lookup
 - Standard greetings
 - Standard transfer options
- There is no support for the following auto attendant features:
 - Dial-by-extension at any time
 - Partitions or search spaces
 - Advanced calling features, such as call screening
 - Interview handlers
 - Dispatch messages
 - Distribution lists
- The auto attendant feature is supported with Cisco Unity Connection Release 8.0 only.
- The Cisco Unified SRSV-CUE auto attendant greeting is the same as the standard opening greeting of the system call handler of Cisco Unity Connection.
- Because the auto attendant greeting on Cisco Unified SRSV-CUE is provisioned from Cisco Unity Connection, the greeting can confuse users into thinking that the function works the same way that it works for Cisco Unity Connection. However, the auto attendant functionality for Cisco Unified SRSV-CUE has fewer features.
- The system does not support schedules. If other greetings such as alternate or holiday are enabled on Cisco Unity Connection, only the standard greeting is enabled on Cisco Unified SRSV.
- Through the Cisco Unified SRSV-CUE auto attendant feature, subscribers can be reached using the directory service. Subscribers cannot be reached directly by entering the subscriber's extension from the auto attendant.
- Dialing a subscriber's extension in auto attendant leads to an invalid selection.
- Directory service on Cisco Unified SRSV-CUE cannot locate users if either the first or last name of the user contains a number.

Network Address Translation (NAT) Restrictions

- Network Address Translation (NAT) is only supported at branch locations and not at the central site.
- Only one Cisco Unified SRSV-CUE device can be provisioned at each NAT site.
- Only static NAT and PAT are supported. Dynamic NAT is not supported.

High Availability Restrictions

- Site provisioning redundancy is not supported.
- You must manually synchronize the Cisco UMG and Cisco Unified SRSV-CUE device passwords between the primary and secondary Cisco UMG systems.
- To upload composed messages, you must configure the central site Cisco Unity Connection system, including the REST credentials, on the secondary Cisco UMG system.

- Upload monitoring may only be done on the primary Cisco UMG.

Voicemail Backup and Restore Limitations

- Transport Layer Security (TLS) certificates and private keys are not backed up on Cisco Unified SRSV-CUE devices. After restoring a backup, you must import the security certificates again.
- To avoid creating duplicate email messages, backing up data on Cisco Unified SRSV-CUE devices is not recommended.

Mailbox Limitations

- If a Cisco Unity Connection user has a spoken name that is longer than ten seconds, the system will use a default spoken name in Cisco Unity Express.
- If there is a mismatch in the codec format between Cisco Unity Connection and Cisco Unity Express (which only supports G.729 ulaw), the system will use the system default greetings and spoken names for users.
- The system determines the mailbox size based on the size of the site template mailbox and not based on the available space on the module.
- User IDs for Cisco Unified SRSV-CUE devices do not support all the characters that are supported on Cisco Unity Connection. Cisco Unified SRSV-CUE devices only support the following characters: alphanumeric, period [.] , dash [-], and underscore [_].
- User IDs cannot start with a number. User IDs can contain numbers, but cannot start with a number.
- In Cisco Unity Connection Release 7.1.3, the system uploads messages that were deleted in Cisco Unified SRSV as new messages. Therefore, the subscriber must manually log in to his voicemail on Cisco Unity Connection and delete the messages again. In Cisco Unity Connection Release 8.0, the system uploads deleted voicemails as deleted.

Live Record and Live Reply Limitations

- Recording can be clipped when the live record beep is played. To avoid this, do not use the speaker phone option when using the live record feature. (Speaker phones have algorithms that can stop sending voice if an incoming talk spurt of significant volume occurs. Incoming live record beeps cause the speaker phone to clip portions of the user's speech when the beep occurs.)
- Live reply is not supported for these message types:
 - Broadcast and expired messages
 - Non-Delivery Report (NDR)/Delayed Delivery Report (DDR)
 - Messages from local General Delivery Mailbox (GDM)

Distribution Lists

- Voice messages sent to distribution lists in survivable mode get sent to the members only after the WAN recovers.
- The system does not provision distribution lists with the spoken name.
- The system does not provision recorded names for distribution lists.
- Distribution list numbers can be up to 15 digits.

- Phone extensions and E.164 numbers are limited to 15 digits for all entities, including subscribers and distribution lists.
- Only public distribution lists are supported.
- Cisco UMG does not support pulling recorded names for distribution lists from Cisco Unity Connection and provisioning them on the Cisco Unified SRSV-CUE device.

Combined SRSV and E-SRST on the Same Site

Cisco UMG 8.5 supports enabling both SRSV and E-SRST provisioning on the same site in certain cases. In the supported model, CUCME-as-SRST is configured on the branch along with a SRSV-CUE device. A central call agent (CUCM) and voicemail system (CUC) is installed at the central site. These devices provide the primary telephony and voicemail services under normal conditions. A Cisco UMG at the central site monitors CUCM and CUC for changes/adds/deletes that must be pushed to the remote branch SRSV-CUE and CUCME-SRST sites.

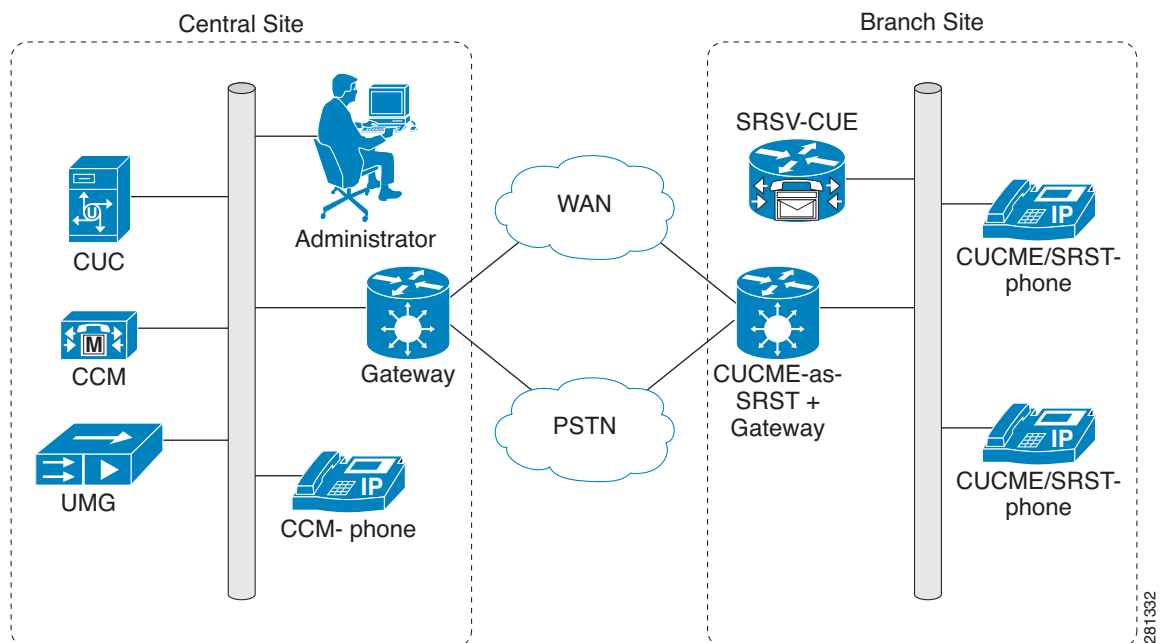


Note

Cisco UMG 8.5 does not support E-SRST at a branch site where original SRST is used. Only CUCME-as-SRST is supported for this configuration.

Figure 5 shows the deployment model for both SRSV and E-SRST that is supported in Cisco UMG 8.5.

Figure 5 *E-SRST and SRSV Deployed on the Same Site*



Voice Profile for Internet Mail (VPIM) Networking

Voice Profile for Internet Mail (VPIM) is supported in Cisco UMG 1.0 and later versions. The VPIM functionality requires the installation of VPIM licenses, with each license supporting up to 25 nodes per license. VPIM is typically not deployed with SRSV.

Cisco Unified Messaging Gateway (Cisco UMG) delivers the end-to-end message networking functionality required by larger distributed enterprises seamlessly migrating to Cisco's IP telephony solution. The majority of larger distributed enterprises consist of various legacy voice messaging products that do not support open standards. The Cisco UMG solution fulfills a gateway function for these networks, providing a method of intelligently routing messages, exchanging subscriber and directory information, and providing interoperability within a messaging network. It acts as a central hub for distributed messaging deployments using the following:

- Cisco Unity Express
- Cisco Unity Connection
- Cisco Unity 4.2 and later versions for Microsoft Exchange only
- Avaya Interchange 5.4

Cisco UMG VPIM enables the messaging network to scale as required for the largest of implementations and simplifies configuration of all the endpoints. The number of Cisco Unity Express endpoints supported depends on the Cisco UMG module being used. For more information, see the [Release Notes for Cisco Unified Messaging Gateway](#).

**Note**

Cisco UMG VPIM licenses support interoperability with Cisco Unity Express, but they do not support interoperability with Cisco Survivable Remote Site Voicemail-Cisco Unity Express (SRSV-CUE). For more information, see the [“Survivable Remote Site Voicemail \(SRSV\)” section on page 19](#).

VPIM Endpoint Management

Cisco Unified Messaging Gateway learns about endpoints either through autoregistration or if the endpoints are manually provisioned.

Autoregistration

Endpoints running Cisco Unity Express 3.1 and later support autoregistration with Cisco Unified Messaging Gateway. No other endpoint types support autoregistration.

The purpose of autoregistration between Cisco UMG and Cisco Unity Express is to facilitate scaling your messaging network while ensuring that messages can only be exchanged by trusted peers. Autoregistration is the means by which a messaging gateway can automatically “discover” legitimate endpoints. The messaging gateway authorizes such endpoints by validating shared secret information. Autoregistration also enables messaging gateways to learn about endpoint properties through directory exchange.

For a more detailed description of the autoregistration process, see the [“Overview of the Autoregistration Process” section on page 67](#).

Manual Provisioning of Cisco Unity and Avaya Interchange Endpoints

The following types of endpoints cannot autoregister, and must be manually provisioned from Cisco UMG:

- Endpoints running Cisco Unity Express Release 3.0 or earlier versions

- Cisco Unity
- Avaya Interchange

Manually provisioning these endpoints serves the same purpose as the registration described previously, ensuring that information is only exchanged between trusted peers. Also, because these endpoint types do not support automatic directory exchange, you must configure the directory information for them on the messaging gateway that manages them.

**Note**

Registered endpoints stay in the database. When an endpoint registers with Cisco UMG, it is assigned a guide number that it uses to identify itself to the messaging gateway on subsequent registrations. If an endpoint tries to register without that guide number or with a different messaging gateway, the registration is rejected as a duplicate location. If necessary, you can clear or delete the endpoint (see the [“Deleting or Clearing Endpoints” section on page 75](#)).

Directory Exchange Between Endpoints And Messaging Gateways

After endpoints are registered with or provisioned to a messaging gateway, this message gateway will propagate the endpoints' information to the rest of the network of Cisco UMGs.

Endpoints can:

- Exchange messages with the messaging gateway with which they are registered
- Retrieve remote subscriber information from that messaging gateway

**Note**

Endpoints of the type Cisco Unity Express Release 3.0 or earlier versions cannot perform autoregistration and directory exchange with Cisco UMG. Neither can Cisco Unity or Avaya Interchange.

Remote Lookup Function

Subscribers can use the remote lookup function to search for a subscriber. The subscriber thus has the ability to:

- Decide whether the remote mailbox exists on an autoregistered endpoint running Cisco Unity Express Release 3.1 and later versions (this directory exchange facility is not yet supported for other types of endpoint).
- Search the global directory, for example, when the message sender does not know the recipient's number.

**Note**

In the global directory, the subscriber will not find search results already delivered by the local directory. This feature serves to prevent the global search results from being flooded by results already obtained.

- Retrieve the spoken name of the remote subscriber. By default, the spoken name is carried in all directory exchange messages.

**Note**

This feature can be turned off in cases where network bandwidth, performance, and database storage might be problematic.

Managing a Network of Cisco UMG VPIM Nodes

Each messaging gateway is configured to recognize its peers. After endpoints are registered with or provisioned to a messaging gateway, this messaging gateway propagates the endpoints' information to the rest of the network of Cisco UMG nodes.

Cisco UMG VPIM uses the primary/secondary model to provide failover support. Each Cisco Unity Express endpoint identifies primary and secondary messaging gateway through its local configuration and autoregisters with both messaging gateways. For Cisco Unity, a DNS server is required for failover support, meaning that the messaging gateway domain name is mapped to two IP addresses on DNS: primary messaging gateway and secondary messaging gateway. Avaya Interchange does not support such failover provisions.

In the case of a firewall, a firewall pin hole must be opened to allow TCP connections between two different nodes (such as between an endpoint and Cisco UMG or between messaging gateways, and so on).

For more detailed information about deployment models for VPIM, see the [Design Guide for Cisco Unified Messaging Gateway 1.0](#).

Administration Interfaces

Cisco UMG Release 8.5 utilizes both a command-line interface (CLI) and a graphical user interface (GUI).

- [Command-Line Interface, page 29](#)
- [Graphical User Interface, page 30](#)

Command-Line Interface

The CLI is a text-based interface accessed through a Telnet session to the router hosting the Cisco UMG. Those familiar with Cisco IOS command structure and routers will see similarities.

The Cisco UMG commands are structured much like the Cisco IOS CLI commands. However, the Cisco UMG CLI commands do not affect Cisco IOS configurations. After you log in to the Cisco UMG, the command environment is no longer the Cisco IOS environment.

See the [“Entering and Exiting the Command Environment” section on page 15](#) for the instructions to enter the Cisco UMG CLI environment.

The CLI is accessible from a PC or server anywhere in the IP network.

The Cisco UMG features are configured as follows:

- The VPIM feature is configured using the CLI commands only. The graphical user interface is not supported for configuration, although backup/restore functions are available using the GUI.
- The E-SRST and SRSV features require the [Graphical User Interface](#) for configuration.

CLI commands can also be used for routine monitoring and maintenance of the Cisco UMG system regardless of the feature licenses installed.

Graphical User Interface

Cisco UMG provides a GUI that is used to configure and operate the SRSV and E-SRST features. For information on using the GUI, see the online help in the application or the selected chapters later in this guide.

Some monitoring and maintenance functions may be available both using the CLI commands and through the GUI. Some basic maintenance functions in the GUI can also be used for VPIM networks.

For information on using the GUI to configure SRSV and/or E-SRST, and for routing maintenance operations, see [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

**Note**

You can configure the E-SRST and SRSV features using the GUI before the required licenses are installed, but the licenses must be installed before the actual site provisioning takes place. If you attempt to provision the sites enabled for E-SRST and SRSV before the site licenses are installed, the provisioning will not be successful.

You can also configure more sites for provisioning than you have purchased licenses for, but the provisioning process will only provision the number of sites purchased. For example, if you have purchased a license for 25 sites but configure the GUI to provision 50, the 25 sites with licenses will be provisioned, but you will receive an error message for the other 25 sites stating that no more licenses are available.



Entering and Exiting the Command Environment

Last updated: December 2, 2010

This chapter describes the procedures for entering and exiting the Cisco UMG command environment, where Cisco UMG configuration commands are executed.

- [About EXEC and Configuration Modes, page 15](#)
- [Entering the Command Environment, page 16](#)
- [Exiting the Command Environment, page 17](#)
- [Finding More Information about CLI Commands, page 17](#)

About EXEC and Configuration Modes

Cisco UMG uses the network module's CLI, which you access through the host-router console. The network module CLI is similar to the router CLI.

Similarities Between the Cisco UMG CLI and the IOS CLI

For both interfaces, standard Cisco IOS navigation and command-completion conventions apply. For example, **?** lists options, **TAB** completes a command, and **|** directs **show** command output.

Differences Between the Cisco UMG CLI and the IOS CLI

Standard command names and options do *not* necessarily apply. A notable example is the command for accessing global configuration mode: the Cisco IOS command is **configure terminal**; the network module command is **config terminal** or **config t**.

Cisco UMG employs a last-one-wins rule. For example, if George and Frank both try to set the IP address for the same entity at the same time, the system starts and completes one operation before it starts the next. The last IP address set is the final result.

The Cisco UMG command modes, privileged EXEC, configuration, registration configuration, list configuration, endpoint configuration, and NAT configuration operate similarly to the EXEC and configuration modes in the Cisco IOS CLI.

After you enter configuration mode, all the CLI commands can be used in the **no** form, for example, **no network messaging gateway location-id { hostname | ip-address }**. This command deletes the specified peer messaging gateway.

Entering the Command Environment

After you install the Cisco UMG module, establish IP connectivity with it, and activate the software. Use this procedure to enter the command environment.

- [Prerequisites, page 16](#)

Prerequisites

Gather the following information before you enter the Cisco UMG command environment:

- IP address of the router that contains the Cisco UMG module
- Username and password to log in to the router
- Slot in the router where the Cisco UMG module resides
- Port through which the router communicates with Cisco UMG

SUMMARY STEPS

1. Open a telnet session.
2. **telnet** *ip-address*
3. Enter the username and password of the router.
4. Choose from the following, depending on the module installed:
 - On the NME-UMG and NME-UMG-EC, enter:
service-module integrated-Service-Engine slot/port session
 - On the SM-SRE-700-K9 and SM-SRE-900-K9, enter:
service-module sm slot/port session
5. **enable**

DETAILED STEPS

	Command or Action	Explanation and Notes
Step 1	Open a telnet session.	Use a DOS window, a secure shell, or a software emulation tool such as Reflection.
Step 2	telnet <i>ip-address</i> Example: C:\> telnet 192.0.2.22	Specify the IP address of Cisco UMG's host router.
Step 3	Username: Password:	Enter your username and password for the router.

	Command or Action	Explanation and Notes
Step 4	For NME-UMG and NME-UMG-EC: service-module integrated-Service-Engine slot/port session	Enters the Cisco UMG command environment using the module located in <i>slot</i> and <i>port</i> . The first time you do this, the prompt changes to “se” with the IP address of the Cisco UMG module. After that, the prompt is the hostname you give to the module. If entering <i>ip-address slot/port</i> elicits the response “Connection refused by remote host”, enter the command service-module integrated Service-Engine slot/port session clear or service-module sm slot/port session clear and retry this step.
	For SM-SRE-700-K9 and SM-SRE-900-K9: service-module sm slot/port session Example: Router# service-module integrated-Service-Engine 1/0 session	
Step 5	enable Example: se-10-0-0-0# enable	Enters Cisco UMG EXEC mode. You are ready to begin configuration.

Exiting the Command Environment

To leave the Cisco UMG command environment and return to the router command environment, in Cisco UMG EXEC mode enter the **exit** command once to exit EXEC mode, and again to exit the application.

The following example illustrates the exit procedure:

```
se-10-0-0-0# exit
se-10-0-0-0# exit
router-prompt#
```

Finding More Information about CLI Commands

This guide describes administration tasks, many of which use CLI commands. However, this guide does not contain complete information about the CLI commands. Complete information about the CLI commands can be found in the [Command Reference for Cisco Unified Messaging Gateway Release 8.0](#) for Cisco UMG commands, and in the [Cisco Unity Express Command Reference for 3.0 and Later Versions](#) for Cisco Unity Express commands.



Initial Configuration Tasks

Last updated: December 2, 2010

- [Adding a DNS Server, page 15](#)
- [Setting Backup Parameters, page 16](#)
- [Configuring NTP Servers, page 18](#)
- [Setting the Time Zone, page 23](#)
- [Configuring Logging Operations, page 24](#)

Adding a DNS Server

If you want to configure your Cisco UMG system for VPIM functionality, add a DNS server to your system by following one of these procedures:

- [Adding a DNS Server: Systems with Cisco Unity, page 15](#)
- [Adding a DNS Server: Systems without Cisco Unity, page 15](#)

Adding a DNS Server: Systems with Cisco Unity

If you are using Cisco UMG with Cisco Unity, you will need to have a DNS server for failover support. The primary/secondary Cisco UMG is transparent to Cisco Unity; however, because this information is configured only on the DNS server, Cisco Unity relies on Microsoft Exchange Simple Mail Transfer Protocol (SMTP) to determine to which Cisco UMG it should send outgoing messages. Cisco Unity should be able to receive messages from both primary and secondary Cisco UMGs if they share the same domain name. Map the Cisco UMG domain name to two IP addresses (primary Cisco UMG and secondary Cisco UMG) in DNS.

Adding a DNS Server: Systems without Cisco Unity

If you are not using Cisco Unity, we recommend that you do not use DNS servers. This improves message exchanging performance, allowing Cisco UMG and endpoints to use IP addresses to address each other instead of by using DNS hostnames. This can be achieved by provisioning peers with IP addresses, or by having each entity cache the resolved IP addresses from the DNS name.

Setting Backup Parameters

- [About Backup Parameters, page 16](#)
- [Prerequisites, page 16](#)
- [Example, page 18](#)

About Backup Parameters

Cisco UMG backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from Cisco UMG to the FTP server and the restore function copies the files from the FTP server to Cisco UMG. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

All Cisco UMG backup files are stored on the specified server. You can copy the backup files to other locations or servers, if necessary.

The backup parameters specify the FTP server to use for storing Cisco UMG backup files and the number of backups that are stored before the system overwrites the oldest one.

**Note**

Cisco UMG automatically assigns an ID to each successful backup. To find out what ID has been assigned to your backup, use the **show backup history** command. For more information, see the [“Restoring Files” section on page 136](#).

To backup or restore files, see the [“Backing Up and Restoring Data”](#) chapter.

Prerequisites

- Verify that the backup server is configured.
- Verify that an FTP administrator or a user who can log in to the FTP server has full permission on the FTP server, such as read, write, overwrite, create, and delete permissions for files and directories.
- Gather the FTP server URL and the username and password of the FTP server login.
- Determine the number of revisions to save before the oldest backup is overwritten.

SUMMARY STEPS

1. **config t**
2. **backup server url** *backup-ftp-url* **username** *backup-ftp-usrname* **password** *backup-ftp-password*
3. **backup revisions number** *number*
4. **end**
5. **show backup**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	backup server url ftp-url username ftp-username password ftp-password} Example: umg-1(config)# backup server url ftp://main/backups username "admin" password "wxyz" umg-1(config)# backup server url ftp://192.0.2.15/backups username "admin" password "wxyz"	Sets the backup parameters. Note The backup server must be configured before the backup revisions can be configured. <ul style="list-style-type: none"> • server url—The <i>ftp-url</i> value is the URL to the network FTP server where the backup files will be stored. • The <i>ftp-username</i> and <i>ftp-password</i> values are the username and password for the network FTP server. In the example, main is the hostname of the FTP server and backups is the directory where backup files are stored.
Step 3	backup revisions number Example: umg-1(config)# backup revisions 5	Sets the number of backup files that will be stored. When this number is reached, the system deletes the oldest stored file.
Step 4	exit Example: umg-1(config)# exit	Exits configuration mode.
Step 5	show backup Example: umg-1# show backup	Displays the backup server configuration information, including the FTP server URL and the maximum number of backup files available.

Example

The following example configures a backup server and displays the **show backup** output:

```
umg-1# config t
umg-1(config)# backup revisions 5
umg-1(config)# backup server url ftp://main/umg-1backups username "admin" password "wxyz"
umg-1(config)# end
umg-1# show backup
Server URL:                               ftp://branch/umg-1backups
User Account on Server:                   backupadmin
Security Protected:                       no
Security Enforced:                       no
Number of Backups to Retain:              5
umg-1#
```

Configuring NTP Servers

During the software postinstallation process, the Network Time Protocol (NTP) server may have been configured. If it was not configured, or if you want to change the configuration, use these procedures to add or delete NTP servers. Cisco UMG supports up to three NTP servers.

- [Adding NTP Servers, page 18](#)
- [Removing an NTP Server, page 20](#)
- [Displaying NTP Server Information, page 21](#)

Adding NTP Servers

- [About Adding NTP Servers, page 18](#)
- [Examples of Adding NTP Servers, page 19](#)

About Adding NTP Servers

You can specify an NTP server using its IP address or its hostname.

Cisco UMG uses the DNS server to resolve the hostname to an IP address and stores the IP address as an NTP server. If DNS resolves the hostname to more than one IP address, Cisco UMG randomly chooses one of the IP addresses that is not already designated as an NTP server. If you do not want to go with random choice, set the **prefer** attribute for one server.

To configure an NTP server with multiple IP addresses for a hostname, repeat the configuration steps using the same hostname. Each iteration assigns the NTP server to its remaining IP addresses.

SUMMARY STEPS

1. **config t**
2. **ntp server** {hostname | ip-address} [**prefer**]
3. **end**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	ntp server {hostname ip-address} [prefer] Example: umg-1(config)# ntp server 192.0.2.14 umg-1(config)# ntp server 192.0.2.17 prefer	Specifies the hostname or IP address of the NTP server. If more than one server is configured, the server with the prefer attribute is used before the others.
Step 3	end Example: umg-1(config)# exit	Exits configuration mode.
Step 4	show ntp status Example: umg-1# show ntp status	Displays the NTP subsystem status.
Step 5	show ntp configuration Example: umg-1# show ntp configuration	Displays the configured NTP servers.
Step 6	copy running-config startup-config Example: umg-1# copy running-config startup-config	Copies the configuration changes to the startup configuration.

Examples of Adding NTP Servers

The following commands configure the NTP server:

```
umg-1# config t
umg-1(config)# ntp server 192.0.2.14
umg-1(config)# exit
umg-1#
```

The output from the **show ntp status** command looks similar to the following:

```
umg-1# show ntp status

NTP reference server 1:      10.100.6.9
Status:                     sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):        0.1719226837158203
umg-1#
```

The following example configures an NTP server with a hostname that points to two IP addresses, 192.0.2.14 and 192.0.2.13:

```
umg-1# config t
umg-1(config)# ntp server NTP.mine.com
umg-1(config)# exit
umg-1#
```

```
umg-1# config t
umg-1(config)# ntp server NTP.mine.com
umg-1(config)# exit
umg-1#
```

The output from the **show ntp status** command might look similar to the following:

```
umg-1# show ntp status
```

```
NTP reference server 1:      192.0.2.14
Status:                     sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):        0.1719226837158203
```

```
NTP reference server 1:      192.0.2.13
Status:                     sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):        0.1719226837158203
umg-1#
```

Removing an NTP Server

You can remove an NTP server using its IP address or hostname.

SUMMARY STEPS

1. **config t**
2. **no ntp server {hostname | ip-address}**
3. **exit**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t	Enters configuration mode.
	Example: umg-1# config t	
Step 2	no ntp server {hostname ip-address}	Specifies the hostname or IP address of the NTP server to remove.
	Example: umg-1(config)# no ntp server 192.0.2.14 umg-1(config)# no ntp server myhost	

	Command or Action	Purpose
Step 3	exit Example: umg-1(config)# exit	Exits configuration mode.
Step 4	show ntp status Example: umg-1# show ntp status	Displays the NTP subsystem status.
Step 5	show ntp configuration Example: umg-1# show ntp configuration	Displays the configured NTP servers.
Step 6	copy running-config startup-config Example: umg-1# copy running-config startup-config	Copies the configuration changes to the startup configuration.

Displaying NTP Server Information

- [Commands to Display NTP Server Information, page 21](#)
- [Examples of Showing NTP Server Information, page 21](#)

Commands to Display NTP Server Information

The following commands are available to display NTP server configuration information and status:

- **show ntp associations**
- **show ntp servers**
- **show ntp source**
- **show ntp status**

Examples of Showing NTP Server Information

The following is sample output for the **show ntp associations** command:

```
umg-1# show ntp associations

ind assID status  conf reach auth condition  last_event cnt
=====
  1 61253 8000   yes  yes  none    reject
```

The following is sample output for the **show ntp servers** command:

```
umg-1# show ntp servers
```

```

      remote      refid      st t when poll reach  delay  offset  jitter
-----
  1.100.6.9      0.0.0.0      16 u   - 1024    0   0.000   0.000 4000.00
space reject,      x falsetick,      . excess,      - outlier
+ candidate,      # selected,      * sys.peer,      o pps.peer

```

The following is sample output for the **show ntp source** command:

```
umg-1# show ntp source
```

```

127.0.0.1: stratum 16, offset 0.000013, synch distance 8.67201
0.0.0.0:      *Not Synchronized*

```

The following is sample output for the **show ntp status** command:

```
umg-1# show ntp status
```

```

NTP reference server :      10.100.6.9
Status:                reject
Time difference (secs):  0.0
Time jitter (secs):     4.0

```

Setting the Time Zone

Typically, you set the time zone during installation. If you did not, or if you want to change it, use the **clock timezone** command in Cisco UMG configuration mode. The system will offer you a range of options to choose from.

To display the time zone, use the **show clock** command in Cisco UMG EXEC mode.

Example of Setting the Time Zone

```
umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# clock timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                4) Arctic Ocean          7) Australia            10) Pacific Ocean
2) Americas              5) Asia                  8) Europe
3) Antarctica            6) Atlantic Ocean        9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla              18) Ecuador              35) Paraguay
 2) Antigua & Barbuda     19) El Salvador          36) Peru
 3) Argentina            20) French Guiana        37) Puerto Rico
 4) Aruba                 21) Greenland            38) St Kitts & Nevis
 5) Bahamas              22) Grenada              39) St Lucia
 6) Barbados             23) Guadeloupe           40) St Pierre & Miquelon
 7) Belize               24) Guatemala            41) St Vincent
 8) Bolivia              25) Guyana                42) Suriname
 9) Brazil               26) Haiti                43) Trinidad & Tobago
10) Canada               27) Honduras             44) Turks & Caicos Is
11) Cayman Islands       28) Jamaica              45) United States
12) Chile                29) Martinique           46) Uruguay
13) Colombia             30) Mexico               47) Venezuela
14) Costa Rica           31) Montserrat           48) Virgin Islands (UK)
15) Cuba                32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica             33) Nicaragua
17) Dominican Republic  34) Panama
#? 45
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Standard Time - Indiana - most locations
 6) Eastern Standard Time - Indiana - Crawford County
 7) Eastern Standard Time - Indiana - Starke County
 8) Eastern Standard Time - Indiana - Switzerland County
 9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
```

```
22) Hawaii
#? 16
```

The following information has been given:

```
United States
Pacific Time
```

```
Therefore TZ='America/Los_Angeles' will be used.
Is the above information OK?
```

```
1) Yes
2) No
#? 1
```

```
Local time is now:      Mon Aug 27 17:23:54 PDT 2007.
Universal Time is now:  Tue Aug 28 00:23:54 UTC 2007.
Save the change to startup configuration and reload the module for the new timez
one to take effect.
umg-1(config)#
```

Configuring Logging Operations

- [About Logging Operations, page 24](#)
- [Prerequisites, page 24](#)
- [Example, page 25](#)

About Logging Operations

Cisco UMG captures messages that describe activities in the system. These messages are collected and directed to a messages.log file on the Cisco UMG module hard disk, the console, or an external system log (syslog) server. The messages.log file is the default destination.

This section describes the procedure for configuring an external server to collect the messages.



Note The external server must be configured to listen on UDP port 514 for traffic coming from the IP address of the Cisco UMG.

Prerequisites

Gather the hostname or IP address of the designated log server.

SUMMARY STEPS

1. **config t**
2. **log server address {hostname | ip-address}**
3. **exit**
4. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	log server address {hostname ip-address} Example: umg-1(config)# log server address 10.187.240.31 umg-1(config)# log server address logpc	Specifies the hostname or IP address of the NTP server designated as the log server.
Step 3	exit Example: umg-1(config)# exit	Exits configuration mode.
Step 4	show running-config Example: umg-1# show running-config	Displays the system configuration, which includes the configured log server.

Example

The output from the **show running-config** command looks similar to the following:

```
umg-1# show running-config

clock timezone America/Los_Angeles
hostname umg-1
ip domain-name localdomain
ntp server 192.0.2.13
log server address 192.0.2.14
```




PART 2

E-SRST and SRSV Configuration



Preparing Cisco UMG to Support E-SRST and SRSV Functionality

Last updated: December 2, 2010

If you want to configure your Cisco UMG system for E-SRST and SRSV functionality, follow these procedures:

- [Prerequisites, page 51](#)
- [About Security for Cisco UMG, page 52](#)

Prerequisites

Complete the following tasks before you configure your Cisco UMG for E-SRST and SRSV.

Table 1 Prerequisites for Configuring E-SRST and/or SRSV Functionality for Cisco UMG	
Task	For more information, see
Install Cisco Unified Communications Manager, including security certificates at the central office.	http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
Install Cisco Unity Connection, including security certificates at the central office.	http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html
Enable SMTP support on the Cisco Unity Connection.	How to Enable SMTP Support for Cisco UMG on Cisco Unity Connection, page 52
Install a Cisco Unified SRST system at the branch office, including security certificates. The supported options are: <ul style="list-style-type: none">• Sites using E-SRST require CUCME-as-SRST.• Sites using SRSV only can use either CUCME-as-SRST or original SRST.	<p>For CUCME-as-SRST, also known as SRST Fallback Mode, see:</p> <ul style="list-style-type: none">• http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmest.html <p>For original SRST, see:</p> <ul style="list-style-type: none">• http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

Table 1 Prerequisites for Configuring E-SRST and/or SRSV Functionality for Cisco UMG

Task	For more information, see
For sites deploying SRSV, install Cisco Survivable Remote Site Voicemail-Cisco Unity Express (SRSV-CUE) at the branch office.	http://www.cisco.com/en/US/products/ps10769/tsd_products_support_series_home.html

How to Enable SMTP Support for Cisco UMG on Cisco Unity Connection

You must configure the Cisco Unity Connection system to allow Cisco UMG to upload messages to it. There are two basic configurations to allow Cisco UMG to work with Cisco Unity Connection:

- Add Cisco UMG addresses to the SMTP access list.
- Allow untrusted connections to Cisco Unity Connection SMTP.

The quickest setup is to allow untrusted SMTP connections on Cisco Unity Connection but this configuration is also the most unsecure. Adding devices to the trusted list requires manually entering Cisco UMG addresses into all Cisco Unity Connections systems by using the System Settings > SMTP Configuration > Server page of the Cisco Unity Connection administration application.

For more information about Cisco Unity Connection SMTP configuration, see the following:

- *Interface Reference Guide for Cisco Unity Connection Administration: System Settings: SMTP Server*
- *Interface Reference Guide for Cisco Unity Connection Administration: System Settings: Search IP Address Access List*

About Security for Cisco UMG

- [About Security, page 52](#)
- [About Security Certificates, page 53](#)
- [Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager, page 53](#)
- [Installing the Security Certificates, page 54](#)

About Security

Security certificates play an essential role in the protection of voicemail messages as they are transferred from the branch site to the central office across the WAN network. Security certificates are required to provide a secure connection between systems. Security is needed for the following:

- Between Cisco Unity Connection and Cisco Unified Communications Manager
- Between Cisco Unified Communications Manager and the Cisco UMG
- Between Cisco UMG and the Cisco Unified SRSV-CUE device at the branch
- Between Cisco UMG and the Cisco Unified SRST or CUCME-as-SRST device at the branch

About Security Certificates

Use one of these methods to generate and sign security certificates:

- Trust chains. Trust chains use Certificate Authorities (CAs) to simplify large deployments. You install security certificates for the CUCM, Cisco Unity Connection, and Cisco UMG that were all signed by a CA and the connections are all part of a trusted chain.
- Self-signed certificates. You use self-signed certificates for each device. In this case, the Cisco UMG needs the security certificate from each device to which it connects.

There are two kinds of security certificates: distinguished encoding rules (DER) and privacy-enhanced mode (PEM).

Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager

Use this method to retrieve the certificates from the Cisco Unity Connection and Cisco Unified Communications Manager systems. You will later add these certificates to the Cisco UMG system.

**Note**

Described below is one method, using the Firefox browser, that you can follow to retrieve certificates in the PEM format. There may be other methods to retrieve security certificates.

Procedure

- Step 1** Using Firefox, open a web browser.
 - Step 2** Navigate to the Cisco Unity Connection home page. It is not necessary to log in.
 - Step 3** Select **Edit > Preferences**.
 - Step 4** Click **Advanced**.
 - Step 5** Click the **Encryption** tab.
 - Step 6** Click **View Certificates**.
 - Step 7** Click the **Servers** tab.
 - Step 8** Locate the servers from Cisco and click the arrow to expand the list of servers. Find the system name of the Cisco Unity Connection system.
 - Step 9** Highlight the row with the Cisco Unity Connection system.
 - Step 10** Click **Export...**
 - Step 11** Save the certificate file to a convenient location.
 - Step 12** Use Notepad to open the certificate file.
 - Step 13** Ensure that it has text that include lines with ---- BEGIN CERTIFICATE ----- and ---- END CERTIFICATE -----.
 - Step 14** Repeat this procedure on the Cisco Unified Communications Manager system.
-

Installing the Security Certificates

Cisco UMG needs both the Cisco Unity Connection and Cisco Unified Communications Manager public certificates installed to enable it to communicate securely with Cisco Unity Connection and Cisco Unified Communications Manager over the REST and AXL interfaces respectively.

Before You Begin

Download the security certificates from Cisco Unity Connection and Cisco Unified Communications Manager. See the [“Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager”](#) section on page 53.



Note

The following procedure installs security certificates in the PEM format. Your experience may be slightly different if you are using security certificates in the DER format.

Procedure

-
- Step 1** Enter the following CLI command:
- crypto key import trustcacert label *LABEL* terminal**
- where *LABEL* is the name of the security certificate.
- The system displays the following:
- ```
Enter certificate...
End with a blank line or "quit" on a line by itself
```
- Step 2** Paste the contents of the security certificate, starting with the line ----- BEGIN CERTIFICATE----- and ending with the line ----- END CERTIFICATE -----.
- The system displays the following:
- ```
Certificate info
*****
Owner: C=US, ST=MA, L=BXB, O=Cisco, OU=None, CN=CCM-7
Issuer: C=US, ST=MA, L=BXB, O=Cisco, OU=None, CN=CCM-7
Valid from: Thu Dec 18 14:34:23 EST 2008 until: Wed Dec 18 14:34:23 EST 2013
Certificate fingerprint (MD5): AD:B2:7F:7A:BB:91:08:0B:5A:59:51:45:BE:F1:CA:42

Do you want to continue to import this certificate, additional validation will be
performed? [y/n]:
```
- Step 3** Enter **y** to import the certificate.
- Step 4** Repeat steps 1 to 3 for the security certificate for Cisco Unified Communications Manager.
- Step 5** At the prompt, enter the following to exit config mode:
- ```
exit
```
- Step 6** At the prompt, enter the following to reload the system:
- ```
reload
```
- The system asks you if you really want to reload.
- Step 7** Enter **y** to confirm that you really want to reload the system.
-

Related Topics

Refer to the [Command Reference for Cisco Unified Messaging Gateway Release](#) for information about the CLI commands.



Configuring E-SRST Site Provisioning

Last updated: August 5, 2011

When enabled on a site, the Cisco UMG E-SRST functionality provides automated remote site provisioning of the following advanced telephony features in survivable mode by gathering the information from CUCM:

- End-user phones and extensions (speed dials, lines, softkeys)
- Voicemail and call forward configuration
- Call routing restrictions (local and long distance, and time of day)
- Call pickup and group pickup
- Hunt groups

This section describes the high-level tasks required to configure a site to support E-SRST. Enabling E-SRST requires configuration on Cisco UMG, the CUCM central call agent, and on the CUCME-as-SRST call agent at the branch. Most of the configuration on Cisco UMG is handled using the GUI. For more information, see the online help and the [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

This procedure assumes that the security certificates have been installed on the Cisco UMG. For more information, see the [“Preparing Cisco UMG to Support E-SRST and SRSV Functionality”](#) section on page 51.

Using E-SRST to Pull an Advanced Telephony Configuration from CUCM to the Branch Site

This section describes the high-level configuration tasks required to pull advanced telephony configuration information from CUCM to the remote site. This section is divided into the following sections:

- [Preparing the Central CUCM Call Agent for E-SRST Provisioning, page 52](#)
- [Adding the Central Call Agent Using the Cisco UMG Central Call Agent Wizard, page 54](#)
- [Configuring the CUCME Branch Call Agent to Prepare for E-SRST Provisioning, page 54](#)
- [Enabling E-SRST Provisioning on the Site Using the Cisco UMG GUI, page 56](#)
- [Verifying the Updated Configuration on the Branch Call Agent Router, page 57](#)

Initial Configuration Using the Cisco UMG GUI

Before you can configure Cisco UMG to support E-SRST on branch sites, you must first perform the following high-level tasks using the Cisco UMG GUI:

1. Configure the Cisco UMG initial values using the setup wizard.
For more information, see “Using the Setup Wizard” in the GUI online help.
2. Add central CUCM call agents using the Central Call Agent Wizard
For more information, see “Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information” in the GUI online help.
3. Import the Cisco Unified SRST sites.
For more information, see “Importing Cisco Unified SRST Sites” in the GUI online help.

Information in the GUI online help is also available in the document [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

Preparing the Central CUCM Call Agent for E-SRST Provisioning

This section assumes that the advanced telephony features have already been configured on CUCM. For more information, see the [Cisco Unified Communications Manager](#) documentation.

To configure CUCM to prepare for E-SRST provisioning, perform the following steps:

-
- Step 1** Configure the SRST references on CUCM with the following:
- site name
 - port number for CUCME-as-SRST.
 - IP address of the router
- Step 2** Create a device pool in CUCM that has the SRST reference.
- Device pool name
 - SRST reference, must match the site name
 - Devices and phones
- For each phone that you want to be registered for survivable mode, set the device pool to match the device pool configured in the previous step.
- Step 3** Configure the advanced telephony configuration on CUCM that will be downloaded to the branch site using E-SRST provisioning.
- Cisco UMG 8.5 supports selected CUCM features to be downloaded using E-SRST site provisioning, and operates in survivable fallback mode. [Table 1](#) lists the supported features and instructions for preparing for the E-SRST site provisioning.

Table 1 *CUCM Advanced Telephony Features Supported in Cisco UMG 8.5*

CUCM Advanced Telephony Configuration	Instructions for Preparing CUCM Feature for E-SRST Site Provisioning
Call list and assigned call list to the ephone domain name	<ul style="list-style-type: none"> Under Directory Number Information, the Directory number and route partition for a given phone are translated by E-SRST to the dial-peer cor configuration at the branch site. The Calling Search Space option under Directory Number Settings must be set to International. The route partition must be set to internal.
Call pickup and group pickup	
Hunt groups	<ol style="list-style-type: none"> Select the Hunt Pilot setting. Select Hunt Pilot. The route partition must be set to internal. Select Hunt List. Select Device Settings --> Softkey Templates. This is the template that you assign to all your e-phones. In fallback mode, these templates are translated into an ephone template, and assigned to the e-phones as well. As a result, the same softkey templates that appear in normal connected mode will appear in fallback mode.

Table 2 lists the softkey states and keys that E-SRST provisioning supports.

Table 2 *Softkeys Supported for E-SRST Provisioning*

Phone States	Softkey
Alerting	Endcall
Connected	Endcall, HLog, Hold, Join, Park, RmLstC, Select, TrnsfVM, Trnsfer
Hold	Join, Newcall, Resume, Select
Idle	Cfwdall, Dnd, Gpickup, Hlog, Join, Newcall, Pickup, Redial, RmLstC
Remote-in-use	Ccharge, Newcall
Ringing	Answer, Dnd, Hlog
Seized	CallBack, Cfwdall, Endcall, Gpickup, Hlog, Pickup, Redial

Adding the Central Call Agent Using the Cisco UMG Central Call Agent Wizard

The central call agent is added using the Central Call Agent Wizard in the GUI. See the Cisco Unified Messaging Gateway online help or the section “Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information” in the document [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

The required steps when using the Central Call Agent Wizard are:

-
- Step 1** Add the CUCM so the UMG knows the CUCM.
 - Step 2** Enter the IP address of the CUCM.
 - Step 3** Enter the AXL username and password, which are the same ones you used to log into the CUCM.
 - Step 4** Set Enable Provisioning to On to enable Cisco UMG to access the CUCM device.
 - Step 5** Set the Site Provisioning Defaults values:
 - Set Site Provision Enable Default to On to enable provisioning for any new sites learned from CUCM.
 - Set SRSV Provision Enable Default to On to enable SRSV provisioning on any new sites learned from CUCM.
 - Set E-SRST Provisioning to On to enable E-SRST provisioning on any new sites learned from CUCM.

These settings establish the default values for this CUCM device and the settings are applied directly to the sites. You can enable or disable provisioning on individual sites as needed.
 - Step 6** Click **Finish** to complete the Central Call Agent Wizard and save this information.
-

Configuring the CUCME Branch Call Agent to Prepare for E-SRST Provisioning

The E-SRST solution requires that CUCME be configured in CUCME-as-SRST mode, also known as SRST Fallback Mode. For more information, see the [Cisco Unified Communications Manager Express Administrator Guide](#).

This section describes the following tasks:

- [Configuring the CUCME Branch Call Agent to Support E-SRST Provisioning, page 54](#)
- [Configuring CUCME Dial Peers to Support E-SRST Provisioning of Ephone-dns and Hunt Groups, page 55](#)

Configuring the CUCME Branch Call Agent to Support E-SRST Provisioning

The CUCME branch call agent must be configured so that it can contact the Cisco UMG. This ensures that the CUCM central site configuration can successfully be pulled through the Cisco UMG device to the remote branch site.

Perform the following steps:

-
- Step 1** Configure the IP address for the interface on the branch router that connects back to the UMG, such as in the following example:

```
interface GigabitEthernet 0/1
 ip address 192.108.1.27 255.255.255.0
```

Step 2 Configure the user telnet name and password for the interface that connects back to the UMG.

username *name* **privilege 15 password** *password*



Note Privilege 15 is required for Cisco UMG to push the configurations to the branch site.

Step 3 Enter the line terminal configuration and enter line configuration mode.

line vty 0 4

Step 4 Enable local password checking at login.

login local

Step 5 Define which protocol to use to connect to the branch call agent.

- If TLS is not enabled on the Cisco UMG, enter the following command:

transport input telnet

- If TLS is enabled on the Cisco UMG, enter the following command:

transport input ssh

Step 6 Enable the IP HTTP server using the following command:

ip http server

Step 7 Set the IP HTTP authentication to the local setting using the following command:

ip http authentication local

Step 8 Enable or disable the HTTPS secure server, depending on whether TLS is enabled on the Cisco UMG:

- If TLS is enabled on the Cisco UMG, enter the following command:

ip http secure-server

- If TLS is disabled on the Cisco UMG, enter the following command:

no ip http secure-server

If TLS is disabled on the Cisco UMG, this setting is required for the CUCM voice configuration to be downloaded to the branch router.

Step 9 Set the IP HTTP timeout policy using the following command:

ip http timeout policy

Configuring CUCME Dial Peers to Support E-SRST Provisioning of Ephone-dns and Hunt Groups

To support E-SRST provisioning of hunt groups and ephone-dns, the CUCME dial peers require additional configuration steps. This additional configuration is required for each site only if the CUCME device is configured for H.323 or SIP; these configuration steps are not required if the CUCME device is configured for MGCP.

**Note**

Cisco UMG 8.5.1 requires that specific settings for the e-phone and voice hunt-group **preference** commands be configured on the CUCME branch call agent. For more information, see the description for CSCtl98820 in the [Release Notes for Cisco Unified Messaging Gateway 8.5](#).

To configure the dial-peer to support the hunt selection order required for E-SRST provisioning, perform the following step:

- Step 1** Configure the dial-peer setting to support the predefined hunt selection order 2.

dial-peer hunt 2

For more information about this command, see the [Cisco IOS Voice Command Reference](#).

Enabling E-SRST Provisioning on the Site Using the Cisco UMG GUI

You must enable E-SRST provisioning using the Cisco UMG GUI for each branch site that will download CUCM telephony configuration during the provisioning process. You can either perform on-demand site provisioning for the site(s), or configure Cisco UMG to perform scheduled provisioning on the site.

For more information, see [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

**Note**

Make sure all the router login credentials are the same for all your branch sites if you are provisioning multiple sites using the Bulk Edit option.

Procedure

- Step 1** Log in to the Cisco UMG GUI.
- Step 2** Select **Configure > Sites**.
- The system displays the Sites page.
- Step 3** To enable E-SRST on one site, click the underlined name of any site to see more information. The system displays the Site Profile page.
- Under Feature Enable, select **E-SRST**.
 - Click **Update**.
- Step 4** To enable E-SRST on multiple sites, check the checkboxes next to the sites that you want to modify.
- Click **Bulk Edit Selected Sites**.
 - Check the checkbox next to **E-SRST Provisioning Enable** and click **On**.

**Note**

Make sure you have enough E-SRST feature licenses installed for the number of sites being provisioned. If there are not enough feature site licenses installed, then the system will provision only the number of sites with installed licenses.

- Enter the Router Login Credentials.

**Note**

The router login credentials apply to the CUCME router at each site configured using the Site Profile Bulk Edit page. The router login credentials must be the same for all the branch sites being edited using the Bulk Edit tool. This field overwrites the router login credentials for a site configured on the Site Profile Bulk Edit page. If the router login credentials for a site are not configured, then the site will not be included in the provisioning process.

- Click **Update**.

Step 5 To perform an on-demand provisioning of the sites, check the checkbox next to the name of the sites that you want to provision.

- Click **Provision Selected Sites**.

The system displays a warning message.

- Click **OK** to continue.

The selected sites are provisioned. If E-SRST was enabled on the sites and the required steps above performed, then the advanced telephony configuration on CUCM is downloaded to the branch site configuration.

**Note**

The length of time required for provisioning the selected sites may depend on various factors. These include number of sites selected, number of items to be configured at each site (phones, phone numbers and other items), network bandwidth and system loads. Using the GUI, go to **Monitor > Provisioning Status** to monitor the provisioning progress.

Step 6 To perform scheduled provisioning, enter the schedule requirements when performing the wizard for adding a site.

Step 7 Verify that the site provisioning successfully completed by checking the Site Provisioning Report.

In the Cisco UMG GUI, choose **Reports > Site Provisioning History**. The status of the provisioned sites is displayed.

Verifying the Updated Configuration on the Branch Call Agent Router

Once the E-SRST provisioning is complete, the dial plan and ephone configuration settings configured on the central CUCM should now be propagated to the branch call agent router. Verify that the updated settings are now configured on the site by viewing the dial peer and ephone configuration settings.



Verifying Site and Provisioning Status on the Cisco UMG

Last updated: December 2, 2010

You can verify site and provisioning status on the Cisco UMG using either the CLI or the GUI. For more information about the CLI commands, see the [Cisco Unified Messaging Gateway Command Reference](#). For more information about using the Cisco UMG GUI, see the online help and [Configuring Cisco Unified Messaging Gateway 8.5 Using the GUI: SRSV and E-SRST](#).

Verifying E-SRST and SRSV Site Information

The following sections describe how to verify specific information about E-SRST and SRSV sites:

- [Verifying E-SRST and SRSV License Information, page 51](#)
- [Verifying Site Information, page 51](#)
- [Verifying Site Template Information, page 52](#)
- [Verifying Central Call Agent Information, page 52](#)
- [Verifying Branch Call Agent Information, page 52](#)
- [Verifying Branch Voicemail Server Information](#)
- [Verifying the Site Provisioning History, page 52](#)

Verifying E-SRST and SRSV License Information

To verify E-SRST and SRSV license information, choose one of the following:

- Using the CLI, enter the **show license status application [esrst | srsv]** command.
- Using the GUI, select **Administration > Licenses**.

Verifying Site Information

To display a list of E-SRST and SRSV sites, or to see the details of a specific site:

- Using the CLI, enter the **show srsx site [sitename]** command.
- Using the GUI, select **Configure > Sites**.

Verifying Site Template Information

To display the site templates used when provisioning SRST devices for E-SRST, or SRSV-CUE devices for SRSV:

- Using the CLI, enter the **show srsx site-template** *[name]* command.
- Using the GUI, select **Configure > Site Templates**.

Verifying Central Call Agent Information

To display a list of central CUCM call agents:

- Using the CLI, enter the **show srsx central-call-agent** *[hostname [srst-references]]* command.
- Using the GUI, select **Configure > Central Call Agents**.

Verifying Branch Call Agent Information

To display a list of all the branch CUCME-as-SRST sites that have been learned from the central CUCM, or to see details of a specific site:

- Using the CLI, enter the **show srsx branch-call-agent** *[name]* command.
- Using the GUI, select **Monitor > Learned CUCME Routers**.

Verifying Branch Voicemail Server Information

To view a list of branch voicemail servers for SRSV:

- Using the CLI, enter the **show srsx branch-voicemail-server** *[unassigned | hostname]* command.
- Using the GUI, select **Configure > Branch Voicemail Servers**.

Verifying the Site Provisioning History

To display the provisioning history for all E-SRST and SRSV sites:

- Using the CLI, enter the **show srsx provisioning history** command.
- Using the GUI, select **Sites > Provisioning History**.

In both the CLI and GUI display, check the Ephones Controlled column to display how many phones were configured on the site.



PART 3

VPIM Network Configuration



Configuring Endpoints for VPIM Networks

Last updated: December 2, 2010

This chapter describes how to configure endpoints for a VPIM network. The chapter contains the following sections:

- [Configuring Peer Messaging Gateways, page 68](#)
- [Message Handling, page 69](#)
- [Configuring Endpoint Autoregistration Support, page 71](#)
- [Provisioning Endpoints Manually, page 74](#)
- [Setting Up NAT Entries, page 80](#)
- [Forcing Data Convergence, page 81](#)
- [Managing System Distribution Lists, page 83](#)
- [Managing System Broadcasts, page 87](#)
- [Deleting Peer Messaging Gateways, page 89](#)
- [Deleting or Clearing Endpoints, page 91](#)
- [Blocking Endpoint Registration, page 92](#)
- [Viewing Network Status, page 94](#)
- [Locating and Viewing Individual Mailbox Details, page 94](#)

Cisco UMG is configured entirely using the command-line interface (CLI). You enter some commands in EXEC mode and others in configuration mode, and still others in submodes. The instructions for each of the tasks cover entering the mode to be used.

For instructions on entering and exiting command modes, see the “[Entering and Exiting the Command Environment](#)” chapter.

You must configure each messaging gateway in your system. If your endpoints are using Cisco Unity Express Release 3.1 and later versions, you only need to set up autoregistration on one messaging gateway.

With Cisco Unity Express Release 3.0 or earlier versions, Cisco Unity, and Avaya Interchange endpoints, you must manually provision each one on the messaging gateway associated with it. The messaging gateway on which you manually provision an endpoint becomes that endpoint’s primary messaging gateway. You can change the configuration of these types of endpoints only from their primary messaging gateway.

Configuring Peer Messaging Gateways

You can configure multiple peer Cisco UMGs. Location IDs for peer messaging gateways must be unique throughout the solution network.

Not only must you configure peers *on* each messaging gateway, you must also configure each peer *as* a messaging gateway. For this, use all the procedures in this chapter.

To delete a peer messaging gateway, see the [“Deleting Peer Messaging Gateways” section on page 73](#).



Note

The following commands do not validate the hostname or IP address of the peer messaging gateway.

Prerequisites

The following information is required to configure a peer Cisco UMG:

- A location ID for the peer messaging gateway that is unique throughout the system.
- A hostname.

SUMMARY STEPS

1. **config t**
2. **network messaging-gateway *location-id* {*hostname* | *ip-address* }**
3. **end**
4. **show messaging-gateway [*location-id*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode
Step 2	network messaging-gateway <i>location-id</i> {<i>hostname</i> <i>ip-address</i>} Example: umg-1(config)# network messaging-gateway 5 sj.mycompany.com	Configures a peer messaging gateway. The hostname can be in the form sj.mycompany.com or it can be an IP address.

	Command or Action	Purpose
Step 3	end Example: umg-1(config)# end	Exits configuration mode.
Step 4	show messaging-gateway [location-id] Example: umg-1# show messaging-gateway 5	Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. If a location ID other than the current configuring messaging gateway is specified, displays the named details for the specified messaging gateway.

Examples

The following output illustrates the use of these commands.

```
umg-1# config t
Enter configuration commands, one per line. End with CNTL/Z.
umg-1(config)# network messaging-gateway 5 sj.mycompany.com
umg-1(config)# end
umg-1# show messaging-gateway
LocationID      Hostname                      NAT
-----
5               sj.mycompany.com             disabled
55              sf.mycompany.com             disabled
555             ny.mycompany.com             disabled

Local Gateway ID: 51000
umg-1# show messaging-gateway 5
LocationID:      5
Hostname:        sj.mycompany.com
NAT:             disabled

umg-1#
```

Message Handling

Default Destination

You can set a default destination ('network default-route') for undeliverable messages; the destination can be either a messaging gateway or an endpoint.

Notice of Delayed Delivery or Non-delivery

If a message is not delivered within one hour of being sent, by default, Cisco UMG sends a delayed-delivery receipt (DDR) to the message-sender and a non-delivery receipt (NDR) after six hours. These settings are system-wide, they cannot be applied to individual endpoints.

Changing the defaults is optional. If you do not make the settings described in the following procedure, the system uses the defaults.

Prerequisites

The following information is required to configure the default destination for unroutable messages:

- The location ID of the endpoint or the messaging gateway to which unroutable messages are to be sent.

The following information is required to change the DDR and NDR settings:

- Delay in hours to be substituted for the current settings (defaults are DDR: 1 hour, NDR: 6 hours).

SUMMARY STEPS

1. **config t**
2. **network default-route** *location-id*
3. **ddr timeout** *0-24*
4. **ndr timeout** *1-48*
5. **end**
6. **show network default-route**
7. **show ddr timeout**
8. **show ndr timeout**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	network default-route <i>location-id</i> Example: umg-1(config)# network default-route 987654	Sets the default destination for undeliverable messages.
Step 3	ddr timeout <i><0-24></i> Example: umg-1(config)# ddr timeout 2	Sets the amount of time (in hours) before the system generates a DDR. Range: 1-24 hours. Set 0 to disable this feature. Default: 1 hour.
Step 4	ndr timeout <i><1-48></i> Example: umg-1(config)# ndr timeout 12	Sets the amount of time (in hours) before the system generates an NDR. Range: 1-48 hours. Default: 6 hours.
Step 5	end Example: umg-1(config)# end	Exits configuration mode.

	Command or Action	Purpose
Step 6	show network default-route Example: umg-1# show network default-route	Displays the default destination for messages that Cisco UMG cannot deliver.
Step 7	show ddr timeout Example: umg-1# show ddr timeout	Displays the delay before the system generates a DDR.
Step 8	show ndr timeout Example: umg-1# show ndr timeout	Displays the delay before the system generates an NDR.

Examples

The following example illustrates a default destination for undeliverable messages being set to the device with the location ID 51000, and the DDR and NDR timeouts being set for the system.

```
umg-1# config t
Enter configuration commands, one per line. End with CNTL/Z.
umg-1(config)# network default-route 51000
umg-1(config)# ddr timeout 2
umg-1(config)# ndr timeout 12
umg-1(config)# end
umg-1# show network default-route
Default route is location 51000.

umg-1# show ddr timeout
Timeout window for DDR messages is 2 hours.

umg-1# show ndr timeout
Timeout window for NDR messages is 12 hours.

umg-1#
```

Configuring Endpoint Autoregistration Support

For endpoints that are to autoregister with Cisco UMG, you must configure registration, connection, and authentication parameters.

You can configure multiple username/password sets on the same messaging gateway.



Note

Cisco Unity Express 3.0 and earlier versions do not support autoregistration. You must provision the endpoints manually. See the [“Provisioning Endpoints Manually”](#) section on page 74 for more information.

The endpoints themselves must be configured to present the corresponding information in a registration request.

The default registration period expires after 1440 minutes. After that time, any new configurations such as username and password take effect.

For an overview of the relevant Cisco Unity Express configuration, see the “[Configuring Cisco Unity Express Endpoints for Autoregistration to Cisco UMG](#)” section on page 67.

In the system logic, autoregistration is implicitly allowed for all endpoints, therefore to prevent autoregistration you must use the **block** command described in this section or in “[Blocking Endpoint Registration](#)” on page 76.

To clear the data associated with an autoregistered endpoint, see “[Deleting or Clearing Endpoints](#)” on page 75.

Prerequisites

The following information is required to configure endpoint autoregistration parameters on Cisco UMG.

- Username and password for endpoints to present to Cisco UMG at registration
- (Optional) Location IDs for endpoints that you want to prevent from autoregistering
- (Optional) Registration expiration period, in minutes

SUMMARY STEPS

1. **config t**
2. **registration**
3. **username *username* password {text | encrypted} *password***
4. **expiration *integer***
5. **block *location-id* *location-id***
6. **end**
7. **end**
8. **show run [paged | | [begin *word* | exclude *word* | include *word* | page]**
9. **write [erase | memory | terminal]**
10. **show start [paged | | [begin *word* | exclude *word* | include *word* | page]**
11. **show registration {block | status | users }**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	registration Example: umg-1(config)# registration	Enters registration configuration mode.

	Command or Action	Purpose
Step 3	username <i>username</i> password { text encrypted } <i>password</i> Example: umg-1(config-reg)# username bob password text cue31	Sets username and password.
Step 4	expiration <i>integer</i> Example: umg-1(config-reg)# expiration 2000	(Optional) Sets the length of time (in minutes) after which autoregistration expires.
Step 5	block <i>location-id</i> <i>location-id</i> Example: umg-1(config-reg)# block location-id 29	Prevents the specified endpoint from autoregistering.
Step 6	end Example: umg-1(config-reg)# end	Exits registration configuration mode.
Step 7	end Example: umg-1(config)# end	Exits configuration mode.
Step 8	show run [paged [begin <i>word</i> exclude <i>word</i> include <i>word</i> page] Example: umg-1# show run inc username	Displays the running configuration.
Step 9	write [erase memory terminal] Example: umg-1# write memory	Writes the running configuration to memory or terminal or <ul style="list-style-type: none"> Erases NV memory Writes to NV memory Writes to terminal.
Step 10	show start [paged [begin <i>word</i> exclude <i>word</i> include <i>word</i> page] Example: umg-1 show start inc username	Displays the startup configuration.
Step 11	show registration { block status users } Example: umg-1# show registration block	Displays endpoint registration status.

Examples

The following example shows an expiration being set for all autoregistered endpoints. A block is set, then a username and password. Finally, the results of these operations are displayed. Note that the expiration is not displayed, because the **no expiration** command caused the default to be set.

```
umg-1# config t
Enter configuration commands, one per line. End with CNTL/Z.
umg-1(config)# registration
umg-1(config-reg)# expiration 20000
Currently registered endpoint expiration will be unaffected.
umg-1(config-reg)# block location-id 33
umg-1(config-reg)# username bob password text cue31
umg-1(config-reg)# end
umg-1(config)# end
umg-1 show run | inc username
username bob password text cue31
umg-1# write memory
umg-1 show start | inc username
username bob password text cue31
umg-1# show registration block
UMG registration block list :
    location-id 33
se-10-1-12-95# show registration status
Endpoint registration stats :
    Auto-registered : 1
    Offline : 10
    Total number : 11

Auto-registered endpoint :
    Loc. 40000 : cue, registered at 19-Aug-07 17:02:31:212

Offline auto-registered endpoint :
    Loc. 40 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 41 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 42 : cue, deregistered/unreachable since 17-Aug-07 16:56:32:169
    Loc. 43 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 44 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 45 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 46 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 47 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
    Loc. 48 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
umg-1#
```

Provisioning Endpoints Manually

You must manually provision the following endpoints to Cisco UMG:

- Cisco Unity
- Avaya Interchange
- Endpoints running Cisco Unity Express 3.0 and earlier

The configuring Cisco UMG automatically becomes the primary messaging gateway for the endpoint being provisioned.

It is most efficient if you group your endpoints by type (Cisco Unity, Cisco Unity Express, Avaya Interchange) before provisioning them, because each type has one or two parameters that are different from those required for other types.

**Note**

To provide failover support for Cisco Unity endpoints, you need at least one DNS server (maximum 4) so that you can map the Cisco UMG domain name to two IP addresses on it (them): primary messaging gateway and secondary messaging gateway.

When you configure a domain for an endpoint, Cisco UMG does an MX lookup on the domain provided and uses those host addresses.

If you have multiple endpoints with the same prefix, you must use the **number-only** addendum to the **prefix** command to specify the range of extensions handled by the endpoint you are provisioning. All endpoints sharing a prefix must use this addendum. In other words, you cannot have endpoint 1 with just prefix 1, and endpoint 2 with prefix 1 plus a range of extensions.

After provisioning each endpoint and before leaving the endpoint configuration mode, you must enable the endpoint.

If you try to provision an endpoint with a location ID that is already in use, and if both location ID and endpoint type actually match the existing one, you will re-configure the first one. If the location ID and the type do not match the existing one, the system will warn you, for example, “Invalid endpoint type. The specified type does not match the existing endpoint.” If you use a location ID similar to one already in your network, the system will warn you, for example, “Possible conflict with existing location ID(s): 3, 333.”

To delete an endpoint, see the [“Deleting or Clearing Endpoints” section on page 75](#).

**Note**

The system does not allow you to change the configurations for an autoregistered endpoint.

Prerequisites

In the following, note that what Cisco UMG refers to as **endpoint** *location-id* is the same as the Cisco Unity Express **network** *location-id* *number*.

For each endpoint type, you have different parameters to set:

Table 1 **Endpoint Types: Cisco Unity Express Release 3.0 or earlier versions**

Keyword	Description
broadcast-id <i>broadcast-id</i>	(Optional) Endpoint’s broadcast ID. This is an alphanumeric string (Range: 1-32) that cannot include spaces.
domain <i>domain</i>	Fully qualified name of domain to which endpoint belongs; for example, sj.mycompany.com.
messaging-gateway secondary <i>location-id</i>	(Optional) Location ID of secondary messaging-gateway.
hostname <i>hostname</i>	Endpoint’s hostname or IP address.
prefix <i>prefix</i>	Messaging system telephone number prefix—phone number prefix that is added to a subscriber’s extension (Range: 1-15 digits).
extension <i>extension</i>	Subscribers’ extension (Range: 1-15 digits).

Table 2 **Endpoint Types: Cisco Unity**

Keyword	Description
domain <i>domain</i>	Fully qualified name of domain to which endpoint belongs; for example, sj.mycompany.com
hostname <i>hostname</i>	Endpoint's hostname or IP address.
messaging-gateway secondary <i>location-id</i>	Location-ID of the endpoint's secondary messaging gateway.
prefix <i>prefix</i>	Messaging system telephone number prefix that is added to a subscriber's extension (Range: 1-15 digits).
extension <i>extension</i>	Subscribers' extension (Range: 1-15 digits).
serial-number <i>serial-number</i>	(Optional) Endpoint's serial number.

Table 3 **Endpoint Types: Avaya Interchange**

Keyword	Description
domain <i>domain</i>	Fully qualified name of endpoint's domain; for example, sj.mycompany.com..
hostname <i>hostname</i>	Endpoint's hostname or IP address.
prefix <i>prefix</i>	Messaging system telephone number prefix—phone number prefix that is added to a subscriber's extension (maximum 15 digits)
extension <i>extension</i>	Subscribers' extension (Range: 1-15 digits).

**Note**

Avaya Interchange does not support a secondary messaging gateway.

**Note**

When you use a **show** command to display the domain name, only the truncated name appears; for example, "mycompany".

**Note**


The **default** command available in the endpoint configuration mode serves as an alternative to the **no** command when used in combination with any of the other commands available in that mode; for example, **hostname default**.

SUMMARY STEPS

1. **config t**
2. **endpoint** *location-id* {**unity** | **interchange** | **cue**}
3. **hostname** *hostname*
4. (Optional) **messaging-gateway secondary** *location-id*

5. **domain** *domain*
6. Either:
 - a. **prefix** *prefix*
or
 - b. **prefix** *prefix* **number-only**
extension *extension*
end
7. (Optional) **broadcast-id** *broadcast-id*
8. (Optional) **serial-number** *serial-number*
9. **enable**
10. **end**
11. **end**
12. **show endpoint** {**local** | **network**} [*location-id* | **filter** *filter*]
13. **show mailbox** {*location-id* | **prefix** *prefix*} [*mailbox* | **filter** *filter*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	endpoint <i>location-id</i> (unity interchange cue) Example: umg-1(config)# endpoint 77777 unity	Enters endpoint configuration mode and identifies the endpoint to be provisioned by location and type.
Step 3	hostname <i>hostname</i> Example: umg-1(config-endpoint)# unity-7	Specifies the endpoint's hostname or IP address.
Step 4	messaging-gateway secondary <i>location-id</i> Example: umg-1(config-endpoint)# messaging-gateway secondary 51000	(Optional) Specifies the endpoint's secondary messaging gateway by means of its location ID. <div>  Note </div> Avaya Interchange does not support secondary messaging gateways.
Step 5	domain <i>domain</i> Example: umg-1(config-endpoint)# domain sj.mycompany.com	Specifies the endpoint's domain name.

	Command or Action	Purpose
Step 6	<p>a) <code>prefix</code> <i>prefix</i></p> <p>Example: <code>umg-1(config-endpoint)# prefix 231</code></p> <p>b) <code>prefix</code> <i>prefix</i> number-only extension <i>extension</i> end</p> <p>Example: <code>umg-1(config-endpoint)# prefix 231 number-only</code> <code>umg-1(config-endpoint-extension)# extension 777</code> <code>umg-1(config-endpoint-extension)# end</code></p>	<p>a. Specifies the endpoint's phone number prefix (Range: 1-9 digits).</p> <p>b. Specifies the prefix, enters endpoint extension configuration mode, specifies the range of extensions (Range:1-15 digits), and then leaves endpoint extension configuration mode.</p> <p>Note If you have multiple endpoints with the same prefix, you must use the number-only addendum (keyword) to the prefix command to specify the range of extensions handled by the endpoint you are provisioning.</p>
Step 7	<p><code>broadcast-id</code> <i>broadcast-id</i></p> <p>Example: <code>umg-1(config-endpoint)# broadcast-id 222222</code></p>	<p>(Optional) Specifies the endpoint's broadcast ID, an alphanumeric string (range: 1-10); cannot include spaces).</p> <p>Avaya Interchange does not support the broadcast messaging function.</p>
Step 8	<p><code>serial-number</code> <i>serial-number</i></p> <p>Example: <code>umg-1(config-endpoint)# serial-number-13</code></p>	<p>(Optional) Specifies the endpoint's serial number.</p>
Step 9	<p><code>enable</code></p> <p>Example: <code>umg-1(config-endpoint)# enable</code></p>	<p>Enables the endpoint.</p>
Step 10	<p><code>end</code></p> <p>Example: <code>umg-1(config-endpoint)# end</code></p>	<p>Exits endpoint configuration mode and enters configuration mode.</p>
Step 11	<p><code>end</code></p> <p>Example: <code>umg-1(config-endpoint)# end</code></p>	<p>Exits configuration mode.</p>

	Command or Action	Purpose
Step 12	<p>show endpoint {<i>local</i> <i>network</i>} [<i>location-id</i> <i>filter filter</i>]</p> <p>Example: umg-1# show endpoint local 77777</p>	<p>Displays a list of local or remote endpoints on the current configuring messaging gateway.</p> <p>If you have many endpoints, you might get this message:</p> <p>“Too many results, please use filter to limit the search result. Only the first 500 endpoints will be displayed.”</p> <p>The filter is any part of a location ID. For example, if you had the location IDs 123, 234, and 345 and you used a filter of 23, you would match 123 and 234. If you used a filter of 34, you would match 234 and 345.</p> <p>Regular expressions are not supported.</p>
Step 13	<p>show mailbox {<i>location-id</i> <i>prefix prefix</i>} [<i>mailbox</i> <i>filter filter</i>]</p> <p>Example: umg-1# show mailbox 77777</p>	<p>Displays a list of the mailboxes associated with the specified endpoint.</p>

Examples

The following example is an example of how to manually provision a Cisco Unity endpoint. An endpoint of this type requires a prefix, and because the number-only attribute has been used, it can be safely assumed that at least two of the user's Cisco Unity endpoints are using the same prefix.

```
umg-1# config t
umg-1(config)# endpoint 77777 unity
umg-1(config-endpoint)# messaging-gateway secondary 51000
umg-1(config-endpoint)# domain sj.mycompany.com
umg-1(config-endpoint)# hostname unity-7
umg-1(config-endpoint)# prefix 231 number-only
umg-1(config-endpoint-extension)# extension 777
umg-1(config-endpoint-extension)# end
umg-1(config-endpoint)# serial-number 13
umg-1(config-endpoint)# broadcast-id 222222
umg-1(config-endpoint)# enable
umg-1(config-endpoint)# end
umg-1(config)# end
se-10-1-12-95# show endpoint local 77777
Location Id:          77777
Hostname:             unity-7
Domain:               sj.mycompany.com
Prefix:               231
NAT:                  Enabled
Type:                 Unity
Serial-number:        13
Addressing Mode:      Number-only
Primary Gateway ID:   50000
Secondary Gateway ID: 51000
Status:               Disabled
umg-1#
```

Setting Up NAT Entries

If you have NAT devices in your network, and they are between messaging gateways and/or endpoints, you must configure NAT entries on Cisco UMG for both messaging gateways and endpoints. For a message to reach its destination, Cisco UMG must know the external HTTP IP address and port number and the external VPIM IP address and port number of the NAT device in front of the destination.



Note

When multiple messaging gateways are behind the same NAT device, configure the endpoints so that they can talk to messaging gateways on ports other than 80/25, because multiple endpoints may be sharing the same external IP address.

(When Cisco Unity Express registers with Cisco UMG, it has the option to specify the HTTP and SMTP ports to match the external PORT used in your setup. For reference, see the [“Configuring Cisco Unity Express Endpoints for Autoregistration to Cisco UMG”](#) section on page 67)

Prerequisites

For each endpoint and peer messaging gateway in your system, the following information is required to set up NAT entries:

- Location ID of the device
- VPIM external IP address and listening port
- HTTP external IP address and listening port

SUMMARY STEPS

1. **config t**
2. **nat location** *location-id*
3. **http external** *ip port*
4. **vpim external** *ip port*
5. **end**
6. **end**
7. **show nat location** *location-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	nat location <i>location-id</i> Example: umg-1(config)# nat location 77777	Enters NAT configuration mode to configure NAT settings for the specified device.

	Command or Action	Purpose
Step 3	http external ip port Example: umg-1(config-nat)# http external 192.0.2.13 8080	Configures NAT entry for HTTP protocol, setting external IP address and listening port (default port is 80).
Step 4	vpim external ip port Example: umg-1(config-nat)# vpim external 192.0.2.13 26	Configures NAT entry for VPIM protocol, setting external IP address and listening port (default port is 25).
Step 5	end Example: umg-1(config-nat)# end	Exits NAT configuration mode.
Step 6	end Example: umg-1(config)# end	Exits configuration mode.
Step 7	show nat location location-id Example: umg-1# show nat location 77777	Lists out configured NAT entries for the device.

Examples

The following example illustrates the the method for configuring NAT:

```
umg-1# config t
umg-1(config)# nat location 77777
umg-1(config-nat)# vpim external 192.0.2.13 26
umg-1(config-nat)# http external 192.0.2.13 8080
umg-1(config-nat)# end
umg-1(config)# end
umg-1# show nat location 77777
Protocol      Ext-IP      Ext-Port
-----
HTTP          192.0.2.13  8080
SMTP          192.0.2.13  26
umg-1#
```

Forcing Data Convergence

Data convergence normally takes place automatically, any time an endpoint (including the mailboxes associated with it) or a messaging gateway is added, deleted, or modified. You can also force directory exchange.

**Note**

This operation does not apply to Cisco Unity Express 3.0 and earlier versions.

Cisco UMG can request that one or all endpoints send their full directories, or just updates. The current configuring messaging gateway can request one or all peer messaging gateways to send their full directories or just updates.

The current configuring messaging gateway can also send either its full directory or just an update to all endpoints and messaging gateways in the system or to specified ones.

The following procedure requests a directory from an endpoint, then sends the current configuring Cisco UMG's updated directory to a peer messaging gateway.

Prerequisites

The location IDs of the endpoints and/or messaging gateways with which directories or updates are to be exchanged.

SUMMARY STEPS

1. **directory exchange endpoint request** { **full** [*location-id*] | **update** [*location-id*] }
2. **directory exchange messaging-gateway send** { **full** [*location-id*] | **update** [*location-id*] }
3. **directory exchange messaging-gateway request** { **full** [*location-id*] | **update** [*location-id*] }
4. **show messaging-gateway** [*location-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	directory exchange endpoint request { full [<i>location-id</i>] update [<i>location-id</i>] } Example: umg-1# directory exchange endpoint request full 42	Requests an endpoint to send either its full directory or the update information. Note This operation does not apply to Cisco Unity Express 3.0 and earlier versions.
Step 2	directory exchange messaging-gateway send { full [<i>location-id</i>] update [<i>location-id</i>] } Example: umg-1# directory exchange messaging-gateway send update	Sends the current configuring messaging gateway's full directory or the update information.

	Command or Action	Purpose
Step 3	<pre>directory exchange messaging-gateway request { full [location-id] update [location-id] }</pre> <p>Example:</p> <pre>umg-1# directory exchange messaging-gateway request update</pre>	Requests directory exchange updates from all peer messaging gateways.
Step 4	<pre>show messaging-gateway [location-id]</pre> <p>Example:</p> <pre>umg-1# show messaging-gateway</pre>	Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. If a location ID other than the current configuring messaging gateway is specified, the named details for the specified messaging gateway are displayed.

Examples

The following example illustrates requesting a full directory exchange from an endpoint, then sending out the current configuring Cisco UMG's directory update to all peer messaging gateways, and finally checking to make sure all peers were actually online to receive the update.

```
umg-1# directory exchange endpoint request full 42
umg-1# directory exchange messaging-gateway send update
umg-1# show messaging-gateway
LocationID      Hostname                               NAT
-----
59000           209.165.200.224                       disabled
777776         peer-1.mycompany.com                   enabled

Local Gateway ID: 51000

umg-1#
```

Managing System Distribution Lists

Cisco UMG enables subscribers to send messages to system distribution lists (SDLs) with recipients (list members) on remote endpoints.

To create an SDL, from EXEC mode, enter the list manager mode to lock list management on all peer Cisco UMGs. The purpose of locking is to prevent messaging gateways getting out of sync. When you have finished configuring SDLs, you must publish them to peer messaging gateways. You can publish to all messaging gateways or you can publish to individual messaging gateways.

If you leave list manager mode without publishing SDLs, the system will automatically publish to all peer messaging gateways.

If the system encounters an SDL lock on a peer messaging gateway, it will fail to lock, and will automatically exit list manager mode. In this situation, you can wait until the lock on the peer messaging gateway is released and/or exit by using the **exit** command.

It is possible that messaging gateways' SDLs can get out of sync. If this is the case, you will be warned when you attempt to lock SDLs. The system will tell you that the current configuring Cisco UMG is out of sync with other messaging gateways. In this case, determine which messaging gateway has the latest

SDL information (by using the **show list tracking version** command to look at the SDL version numbers), and publish from there. This will bring the other messaging gateway back into sync with the rest.

When you create an SDL, you must ensure the number you assign to it (which is also the number the authorized sender dials to send a message to the list) does not conflict with other SDL numbers nor with any subscriber's number.

SDLs can have members that are other lists, as well as subscribers. Although you can configure an SDL without an authorized sender, messages must have at least one authorized sender.

To delete an SDL, use the **no list number** command in list-manager mode.

Prerequisites

- An unique SDL number. This is the number an authorized sender dials to address a message to the SDL. It is a numeric string of 1-16 digits.
- (Optional) The SDL name is an alphanumeric string. If you use this variable, the name will be validated against the names of existing SDLs.
- The authorized sender is identified by an E.164 format number; the system will accept any authorized sender, even one whose number is not in the subscriber directory.
- SDL members can be subscribers or other lists. Each one is identified by a number. The system will accept any subscriber as a member, even one whose number it does not find in the subscriber directory. However, it will not accept lists that do not exist as members.

SUMMARY STEPS

1. **list-manager**
2. **list { number number | publish [location-id] }**
3. **name string**
4. **privilege number**
5. **member number type [sub | list]**
6. **member number type [sub | list]**
7. **end**
8. **show list [number | name]**
9. **list { number number | publish [location-id] }**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	list-manager Example: umg-1# list-manager	Enters list manager mode.
Step 2	list { number number publish [location-id] } Example: umg-1(listmgr)# list number 1111	Publishes lists to other messaging gateways or enters list manager mode and specifies an already existing list or creates a list.
Step 3	name string Example: umg-1(listmgr-edit)# name FirstList	Names a list.
Step 4	privilege number Example: umg-1(listmgr-edit)# privilege 4085550100	Grants a list member permission to send messages to the list.
Step 5	member number type [sub list] Example: umg-1(listmgr-edit)# member 4085550101 type sub	Specifies a list member and its type.
Step 6	member number type [sub list] Example: umg-1(listmgr-edit)# member 2222 type list	Specifies a list member and its type.
Step 7	end Example: umg-1(listmgr-edit)# end	Exits list manager mode.
Step 8	show list [number name] Example: umg-1(listmgr)# show list	Displays all lists.
Step 9	list { number number publish [location-id] } Example: umg-1(listmgr)# list publish	Publishes lists to other messaging gateways or enters list manager mode and specifies an already existing list or creates a list.
Step 10	end Example: umg-1(listmgr)# end	Exits list manager mode.

Examples

The first example shows the output when the system fails to lock the SDLs. The second shows the out-of-sync warning, and illustrates list creation and publication.

```
umg-1# list
Locking system distribution lists...Lock manager reports failure [FAILED]
umg-1#

umg-1# list
Locking system distribution lists...[OK]

**WARNING** This UMG is out of sync and contains old information, user should probably
publish to this UMG from a peer.
  SDL-Version                Last-Updated                List-Of-Remote-Gateways
  -----
  * 50000_20070807033625      Aug 7, 2007 3:36:25 AM      51000
  -----

umg-1(listmgr)# list number 1111
umg-1(listmgr-edit)# name FirstList
umg-1(listmgr-edit)# end
umg-1(listmgr)# list number 2222
umg-1(listmgr-edit)# SecondList
umg-1(listmgr-edit)# end
umg-1(listmgr)# list number 1111
umg-1(listmgr-edit)# privilege 4085550100
This authorized sender [4085550100] will be added. However this authorized sender does
not exist yet!
umg-1(listmgr-edit)# member 4085550101 type sub
WARNING! The subscriber has been added to the list, but it doesn't exist in the subscriber
directory.

umg-1(listmgr-edit)# member 2222 type list
umg-1(listmgr-edit)# end
umg-1(listmgr)# show list
The version of system distribution list is 50000_20070815050633.

A total of 2 System Distribution List(s) have been found:

Extension      Name
-----
1111           FirstList
2222           SecondList

umg-1(listmgr)# show list 1111
Extension:      1111
Name:           FirstList
Number of members: 2
Member(s):      4085550101 (subscriber)
                2222 (list)
                # of members: 2

umg-1(listmgr)# list publish
LocationID      Status      Description
-----
51000           Published
59000           Locked(Renewed)

# of network gateways published:      1
# of network gateways failed to publish:1

umg-1(listmgr)# end
```


umg-1#

Managing System Broadcasts

You can enable a subscriber to send a system broadcast message (SBM) to all subscribers on a specified endpoint, whether local or remote. If you grant to one subscriber the broadcast privilege for all endpoints, that person can reach all subscribers in the system by sending the same message. In Cisco UMG 1.0, this means a single SBM sent to each endpoint in succession, not one SBM sent simultaneously to all endpoints.

When you configure a broadcast VPIM ID on Cisco Unity Express, Cisco UMG automatically picks it up when the endpoint autoregisters.

For endpoints running Cisco Unity Express Release 3.0 or earlier versions, not only must you configure the broadcast VPIM ID on the endpoint itself, you must also configure it on Cisco UMG when you manually provision the endpoint.



Note

Avaya Interchange does not support SBMs.

You must create at least one authorized sender (that is, grant a broadcast privilege) for each endpoint; otherwise, no subscriber can send any messages to it.

Assign broadcast location privileges to local endpoints only because Cisco UMG only validates them locally. In other words, the configuring messaging gateway should be the endpoint's primary or secondary messaging gateway.

Prerequisites

- The broadcast VPIM ID for each Cisco Unity Express endpoint (read it off the configured endpoint).
- The telephone number of at least one subscriber who is to be granted the system broadcast privilege for that endpoint. The authorized sender can be associated with any endpoint in the Cisco UMG network.

SUMMARY STEPS

1. **config t**
2. **endpoint** *location-id* { **unity** | **interchange** | **cue** }
3. **broadcast-id** *broadcast-id*
4. **end**
5. **broadcast location** *location-id* **privilege** *number*
6. **end**
7. **show endpoint** { **local** [*location-id*] | **network** [*location-id*] }
8. **show broadcast location** *location-id* **privilege**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	endpoint location-id {unity interchange cue } Example: umg-1(config)# endpoint 11 cue	Enters endpoint configuration mode and specifies the endpoint to be provisioned, including its type.
Step 3	broadcast-id broadcast-id Example: umg-1(config-endpoint)# broadcast-id 0100	Configures the VPIM broadcast ID of the endpoint.
Step 4	end Example: umg-1(config-endpoint)# end	Exits endpoint configuration mode.
Step 5	broadcast location location-id privilege number Example: umg-1(config)# broadcast location 11 privilege 4085550101	Creates an authorized sender for SBMs to the specified endpoint.
Step 6	end Example: umg-1(config)# end	Exits configuration mode.
Step 7	show endpoint {local [location-id] network [location-id]} Example: umg-1# show endpoint local 11	Displays details of the specified endpoint, including and in particular, its broadcast-id.
Step 8	show broadcast location location-id privilege Example: umg-1# show broadcast location 11 privilege	Displays the authorized sender for this endpoint.

Examples

```

umg-1# config t
umg-1(config)# endpoint 11 cue
umg-1(config-endpoint)# broadcast-id 0100
umg-1(config-endpoint)# end
umg-1(config)# broadcast location 11 privilege 4085550101
umg-1(config)# end
umg-1# show endpoint local 11
Location Id:          11
Hostname:             Wally
Domain:               cuesim1
Prefix:               408555
NAT:                  Disabled
Type:                 CUE
Broadcast VPIM ID:    0100
Primary Gateway ID:   50000
Secondary Gateway ID:
Status:                Auto-Registered-Offline

umg-1# show broadcast location 11 privilege
A total of 1 Authorized Sender(s) have been found for location 11:

4085550101

umg-1#
```

Deleting Peer Messaging Gateways

To delete a peer messaging-gateway, use the **no** form of the **network messaging-gateway** command in Cisco UMG configuration mode.

In the following procedure, the viewing activities are optional.

SUMMARY STEPS

1. (Optional) **show messaging gateway**
2. (Optional) **show messaging gateway** [*location-id*]
3. **config t**
4. **no network messaging-gateway** *location-id*
5. **end**
6. **show messaging gateway** [*location-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	show messaging gateway Example: umg-1# show messaging-gateway	(Optional) Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway.
Step 2	show messaging gateway [<i>location-id</i>] Example: umg-1# show messaging-gateway 5	(Optional) Displays the location ID and hostname of the specified messaging gateway.
Step 3	config t Example: umg-1# config t	Enters configuration mode.
Step 4	no network messaging-gateway <i>location-id</i> Example: umg-1(config)# no network messaging-gateway 5	Clears (deletes) a specified messaging gateway.
Step 5	end Example: umg-1(config)# end	Enters EXEC mode.
Step 6	show messaging gateway [<i>location-id</i>] Example: umg-1# show messaging-gateway	Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway.

Examples

```

umg-1# show messaging-gateway
LocationID      Hostname                NAT
-----
5               www.mycompany.com      disabled
51000          192.0.0.10             disabled
59000          192.0.0.11             disabled

Local Gateway ID: 50000

umg-1# show messaging-gateway 5
LocationID:      5
Hostname:        www.mycompany.com
NAT:             disabled

umg-1# config t
Enter configuration commands, one per line. End with CNTL/Z.
umg-1(config)# no network messaging-gateway 5
umg-1(config)# end
umg-1# show messaging-gateway

```

```

LocationID      Hostname      NAT
-----
51000           192.0.0.10 disabled
59000           192.0.0.11 disabled

Local Gateway ID: 50000

umg-1#

```

Deleting or Clearing Endpoints

To delete a manually provisioned endpoint, use the **no** form of the **endpoint location-id { cue | unity | interchange }** command in Cisco UMG configuration mode on the endpoint's primary messaging gateway.

To delete an autoregistered endpoint, use the following procedure on the endpoint's primary messaging gateway.

Although the endpoint will remain online, any messages it attempts to forward will be rejected by the current configuring Cisco UMG. However, the endpoint will be able to reregister after its registration period has expired unless you either block the endpoint or set up autoregistration for it on a different messaging-gateway. In this case, remember also to change the primary messaging gateway configuration on the endpoint itself.

The **clear endpoint** command triggers directory exchange with peer messaging gateways.



Note

Cisco UMG does not display more than 250 endpoints without prompting. Use a filter to give you a better overview if you have more than a few endpoints.

SUMMARY STEPS

1. **show endpoint local** [*location-id* | **filter** *filter*]
2. **clear endpoint** *location-id*
3. **show endpoint local** [*location-id* | **filter** *filter*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	show endpoint local [<i>location-id</i> filter <i>filter</i>] Example: umg-1# show endpoint local	Displays all remote endpoints or details for the specified remote endpoint.

	Command or Action	Purpose
Step 2	clear endpoint <i>location-id</i> Example: umg-1# clear endpoint 35	Clears the data on the current configuring gateway for the specified endpoint.
Step 3	show endpoint local [<i>location-id</i> filter <i>filter</i>] Example: umg-1(config)# show endpoint local 35	Displays all remote endpoints or details for the specified remote endpoint.

Examples

```
umg-1# show endpoint local
A total of 5 local endpoint(s) have been found:
```

Location ID	Location Prefix	Endpoint Type	Primary Gateway	Secondary Gateway
33	408108	CUE	50000	59000
34	408109	CUE	50000	
35	408110	CUE	50000	
36	408111	CUE	50000	
37	408112	CUE	50000	

```
umg-1# clear endpoint 35
Clear all data associated with endpoint 35 [confirm]
[OK]
umg-1# show endpoint local
A total of 4 local endpoint(s) have been found:
```

Location ID	Location Prefix	Endpoint Type	Primary Gateway	Secondary Gateway
33	408108	CUE	50000	59000
34	408109	CUE	50000	
36	408111	CUE	50000	
37	408112	CUE	50000	

```
umg-1# show endpoint local 35
Local endpoint with location id 35 has not been found.
```

Blocking Endpoint Registration

Endpoints capable of autoregistering with Cisco UMG (only Cisco Unity Express Release 3.1 and later versions) can be prevented from registering.

The system logic implicitly allows autoregistration for all endpoints; therefore, preventing autoregistration must be explicit.

Prerequisites

The following information is required to prevent autoregistration-capable endpoints from registering.

- Location IDs for endpoints that you want to prevent from autoregistering.

SUMMARY STEPS

1. **config t**
2. **registration**
3. **block location-id** *location-id*
4. **end**
5. **end**
6. **show registration block**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	registration Example: umg-1(config)# registration	Enters registration configuration mode.
Step 3	block location-id <i>location-id</i> Example: umg-1(config-reg)# block location-id 29	Prevents the specified endpoint from autoregistering.
Step 4	end Example: umg-1(config-reg)# end	Exits registration configuration mode.
Step 5	end Example: umg-1(config)# end	Exits configuration mode.
Step 6	show registration block Example: umg-1# show registration block	Displays all remote endpoints or details for the specified remote endpoint.

Example:

```

umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# registration
umg-1(config-reg)# block location-id 34
umg-1(config-reg)# end
umg-1(config)# end
umg-1# show registration block
UMG registration block list :
location-id 34
umg-1#

```

Viewing Network Status

Use these commands to verify the status of peer messaging gateways and endpoints.

Table 4 *Network Status Commands*

Command	Function
show ddr timeout	Displays lapse of time (in hours) after which the system generates a DDR for a message. Default is one hour.
show endpoint local	Displays a list of all the endpoints associated with the current Cisco UMG.
show endpoint network	Displays a list of all the endpoints associated with peer Cisco UMGs.
show ndr timeout	Displays lapse of time (in hours) after which the system generates an NDR for a message. Default is six hours.
show registration block	Displays a list of endpoints that are prevented from registering.
show registration status	Displays a list of registered endpoints and their status: whether online or not, and so on.
show registration users	Displays the user credentials of the autoregistered endpoints.
show spoken-name	Indicates whether spoken-name has been enabled on the current configuring messaging gateway.
show statistics	Displays statistics relative to endpoints.

Locating and Viewing Individual Mailbox Details

To locate an individual mailbox in your system and view its details (the phone number, extension, and first and last names associated with the mailbox), use the following procedure.

This procedure assumes that you know the subscriber number, and that you do not know whether it is associated with a local or remote endpoint. It also assumes that you use the **show mailbox** command for each of the listed endpoints.

If you have provisioned your endpoints with prefixes, you can more easily identify which of the endpoints is worth searching. However, to find a mailbox, it is not sufficient to know the prefix associated with the mailbox's endpoint (unless each of your prefixes applies only to a single endpoint), you must know which endpoint the mailbox is associated with.

**Note**

The system only displays the first 300 search results. If necessary, the system asks you to use a filter to limit the search results.

SUMMARY STEPS

1. **show endpoint local**
2. **show mailbox** *location-id* **filter** *filter*
3. **show endpoint network** *location-id*
4. **show mailbox** *location-id* **filter** *filter*
5. **show mailbox** *location-id* *mailbox*

DETAILED STEPS

	Command or Action	Purpose
Step 1	show endpoint local Example: umg-1# show endpoint local	Displays all the endpoints associated with the current Cisco UMG, their location IDs, location prefixes, types, primary messaging gateways, and if applicable, secondary messaging gateways.
Step 2	show mailbox <i>location-id</i> filter <i>filter</i> Example: umg-1# show mailbox 300 filter 0100	Displays all the mailboxes associated with the specified endpoint, filtered by subscriber extension.
Step 3	Example: show endpoint network <i>location-id</i> Example: umg-1# show endpoint network	Displays all the endpoints associated with peer messaging gateways, their location IDs, their location prefixes, their types, their primary messaging gateways, and if applicable, their secondary messaging gateways.
Step 4	show mailbox <i>location-id</i> filter <i>filter</i> Example: umg-1# show mailbox 7 filter 0100	Displays all the mailboxes associated with the specified endpoint, filtered by subscriber extension.
Step 5	show mailbox <i>location-id</i> <i>mailbox</i> Example: umg-1# show mailbox 7 4085550100	Displays the details of the specified mailbox, that is, extension, first name and last name of the subscriber.

Examples

The following example illustrates the output for the **show endpoint local**, **show endpoint network**, and **show mailbox** commands when used in the sequence described previously:

```
se-10-1-12-96# show endpoint local
```

A total of 8 local endpoint(s) have been found:

Location ID	Location Prefix	Endpoint Type	Endpoint Status	Primary Gateway	Secondary Gateway
300	408555	CUE	Offline	51000	
365	408555	CUE	Offline	51000	
366	408555	CUE	Offline	51000	
369	408555	CUE	Offline	51000	
370	408555	CUE	Offline	51000	
375	408109	CUE	Offline	51000	
376	408110	CUE	Offline	51000	
379	408111	CUE	Offline	51000	

```
umg-1# show mailbox prefix 408555 filter 0100
```

No mailbox has been found for prefix 408555(filter='0100').

```
umg-1# show endpoint network
```

A total of 259 network endpoint(s) have been found:

Location ID	Location Prefix	Endpoint Type	Primary Gateway	Secondary Gateway
1	408101	CUE	50000	
2	408102	CUE	50000	
3	408103	CUE	50000	
4	408104	CUE	50000	
5	408105	CUE	50000	
6	408555	CUE	50000	
7	408555	CUE	50000	
8	408108	CUE	50000	

[...]

```
umg-1# show mailbox prefix 408555 filter 0100
```

1 mailbox(s) has been found for prefix 408555(filter='0100').

```
umg-1# show mailbox 7 4085550100
```

Phone: 4085550100

Extension: 0100

First Name: John

Last Name: Doe



Configuring Cisco Unity Express Endpoints for Autoregistration to Cisco UMG

Revised: December 2, 2010

This section covers describes how to enable Cisco Unity Express endpoints to autoregister with a Cisco Unified Messaging Gateway VPIM network. The procedures in this section are configured on Cisco Unity Express.



Note

Endpoints running Cisco Unity Express Release 3.0 or earlier versions do not support autoregistration. They must be manually configured on Cisco UMG. See the [“Manually Registering a Cisco Unity Express Endpoint”](#) section on page 73.

The section contains the following topics:

- [Overview of the Autoregistration Process, page 67](#)
- [Configuring Cisco Unity Express Autoregistration with Cisco UMG, page 68](#)
- [Manually Registering a Cisco Unity Express Endpoint, page 73](#)
- [Verifying the Registration Status of a Cisco Unity Express Endpoint, page 73](#)
- [Enabling or Disabling Remote Lookup, With or Without TUI Confirmation, page 75](#)
- [Viewing Cached and/or Configured Network Locations, page 76](#)
- [Refreshing Locations, page 76](#)
- [Setting the Expiration for Cached Locations, page 76](#)
- [Overloading a NAT Device: the Consequences for Endpoints, page 76](#)

Overview of the Autoregistration Process

The purpose of autoregistration is for Cisco UMG to automatically “discover” legitimate Cisco Unity Express endpoints.

A messaging gateway discovers whether an endpoint is legitimate by attempting to validate the shared secret information in the autoregistration message sent by the endpoint. Successful validation ensures that messages can only be exchanged between trusted peers.

The autoregistration process starts after the endpoint boots up. An appropriately configured endpoint is enabled to autoregister and it has the following information:

- The location ID and IP address or domain name of its primary (and where applicable, its secondary) messaging gateway
- Registration ID and password that the messaging gateways will be expecting
 - The instructions for configuring this ID and password on Cisco UMG are given in the [“Configuring Endpoint Autoregistration Support” section on page 28](#).
 - The instructions for configuring this ID and password on Cisco Unity Express Release 3.1 and later versions are given below, in the [“Configuring Cisco Unity Express Autoregistration with Cisco UMG” section on page 68](#).

Beginning the process, the endpoint sends registration requests to both the primary Cisco UMG and the secondary messaging gateway, in that order, if a secondary is configured.



Note

If autoregistration for the primary messaging gateway fails due to incorrect configuration, the endpoint does not attempt to proceed with the secondary messaging gateway. However, if connectivity problems prevent the endpoint from contacting the primary messaging gateway, the endpoint does try to reach the secondary messaging gateway.

The registration message contains information about itself, such as its own location ID, broadcast ID, and so on. If the primary messaging gateway encounters configuration problems during registration (for example, a missing location-id), the process will fail, and the endpoint will not try to register with the secondary messaging gateway. If the problems are of a different nature (for example, connectivity problems), the endpoint will go ahead and try to register with the secondary messaging gateway.

When the endpoint autoregisters, the messaging gateway adds the endpoint to a trusted endpoints table and the endpoint is then allowed to send and receive VPIM messages to and from the messaging gateway with which it has registered, as well as to retrieve remote user information.

Automatic directory information exchange takes place a couple of minutes after registration, thereby enabling the messaging gateway to learn about the endpoint's properties.



Note

Endpoints using Cisco Unity Express Release 3.0 or earlier versions, Cisco Unity, and Avaya Interchange do not support autoregistration, so they must be individually provisioned from messaging gateways. Instructions for doing this are given in the [“Provisioning Endpoints Manually” section on page 31](#). An endpoint running Cisco Unity Express Release 3.1 and later versions that is not enabled to autoregister will be treated the same as these other types of endpoint.

Configuring Cisco Unity Express Autoregistration with Cisco UMG

Endpoints running Cisco Unity Express 3.1 and later can autoregister with Cisco UMG. This means that when the endpoint comes online (or when you use the **messaging-gateway registration** command), it seeks out its messaging gateway(s), if configured, and registers itself. The alternative is manual provisioning, which entails configuring all relevant details for each endpoint on its messaging gateway. This is the only option available to supported endpoints not running Cisco Unity Express Release 3.1 and later versions.

After an endpoint autoregisters, its messaging gateway exchanges directories with its peers so that the whole system becomes aware that this endpoint is now online. After the endpoint administrator enables autoregistration, any time either the endpoint or the messaging gateway goes offline, the endpoint will re-register automatically as soon as both come back online.

Before enabling autoregistration, the administrator must specify the primary (and optionally the secondary) messaging gateway access information. Using these commands on the endpoint causes the profile(s) for the messaging gateways to be stored in the endpoint's running-config.

**Caution**

You must copy these configurations to the startup-config to make them persistent.

SUMMARY STEPS

1. **config t**
2. **messaging-gateway primary** *location-id* {*umg-ip-addr* | *umg-hostname*}
3. **username** *user* **password** {**text** | **encrypted**} *password*
4. (Optional) **retry-interval** *integer*
5. **end**
6. (Optional) **nat location** *location-id*
7. (Optional) **http external** *ip-addr* *port-number*
8. (Optional) **vpim external** *ip-addr* *port-number*
9. **end**
10. (Optional) **messaging-gateway secondary** *location-id* {*umg-ip-addr* | *umg-hostname*}
11. (Optional) **username** *user* **password** {**text** | **encrypted**} *password*
12. (Optional) **retry-interval** *integer*
13. **end**
14. (Optional) **nat location** *location-id*
15. (Optional) **http external** *ip-addr* *port-number*
16. (Optional) **vpim external** *ip-addr* *port-number*
17. **end**
18. **messaging-gateway registration**
19. **end**
20. **show messaging-gateway**
21. **write memory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	messaging-gateway primary location-id {umg-ip-addr umg-hostname} Example: se-10-0-0-0(config)# messaging-gateway primary 100 192.0.2.21	Enters messaging gateway configuration mode and specifies the following information for the primary messaging gateway: <ul style="list-style-type: none"> • <i>location-id</i>--the location-id of the primary messaging gateway • <i>umg-ip-addr umg-hostname</i>--the IP address or hostname of the primary messaging gateway Configure the primary messaging gateway before the secondary. If you do not, you will get the error message "Primary messaging gateway needs to be configured first."
Step 3	username user password {text encrypted} password Example: se-10-0-0-0(config-messaging-gateway)# username cue31 password text herein	Specifies the username and password required to autoregister with the messaging gateway. Note that the username is not necessarily the same as the endpoint's location ID, because the Cisco UMG administrator can configure a messaging gateway to expect the same username from multiple endpoints.
Step 4	retry-interval integer Example: se-10-0-0-0(config-messaging-gateway)# retry-interval 2	(Optional) The retry-interval is the delay in minutes before the endpoint attempts to reregister with the messaging gateway. The default is 5 minutes, range 0 - 65535.
Step 5	end Example: se-10-0-0-0(config-messaging-gateway)# end	Exits messaging-gateway configuration mode and enters configuration mode.
Step 6	nat location location-id Example: se-10-0-0-0(config)# nat location 77777	Enters NAT configuration mode.
Step 7	http external ip-addr port-number Example: umg-1(config-nat)# http external 192.0.2.13 8080	(Optional) Configures the external IP address and listening port for HTTP requests.
Step 8	vpim external ip-addr port-number Example: umg-1(config-nat)# vpim external 192.0.2.24 26	(Optional) Configures the external IP address and listening port for VPIM requests.

	Command or Action	Purpose
Step 9	end Example: se-10-0-0-0(config-nat)# end	Exits NAT configuration mode and enters configuration mode.
Step 10	messaging-gateway secondary <i>location-id</i> { <i>umg-ip-addr</i> <i>umg-hostname</i> } Example: se-10-0-0-0(config)# messaging-gateway secondary 101 192.0.2.21	(Optional) Enters messaging gateway configuration mode and specifies the following information for the secondary messaging gateway: <ul style="list-style-type: none"> <i>location-id</i>--the location-id of the secondary messaging gateway <i>umg-ip-addr</i> <i>umg-hostname</i>--the IP address or hostname of the secondary messaging gateway Configure the primary messaging gateway before the secondary. If you do not, you will get the error message "Primary messaging gateway needs to be configured first."
Step 11	username <i>user</i> password { text encrypted } <i>password</i> Example: se-10-0-0-0(config-messaging-gateway)# username cue32 password text herein	Specifies the username and password required to autoregister with the messaging gateway. Note that the username is not necessarily the same as the endpoint's location ID, because the Cisco UMG administrator can configure a messaging gateway to expect the same username from multiple endpoints.
Step 12	retry-interval <i>integer</i> Example: se-10-0-0-0(config-messaging-gateway)# retry-interval 2	(Optional) The retry-interval is the delay in minutes before the endpoint attempts to reregister with the messaging gateway. The default is 5 minutes, range 0 - 65535.
Step 13	end Example: se-10-0-0-0(config-messaging-gateway)# end	Exits messaging gateway configuration mode.
Step 14	nat location <i>location-id</i> Example: se-10-0-0-0(config)# nat location 77777	Enters NAT configuration mode.
Step 15	http external <i>ip-addr</i> <i>port-number</i> Example: umg-1(config-nat)# http external 192.0.2.13 8080	(Optional) Configures the external IP address and listening port for HTTP requests.
Step 16	vpim external <i>ip-addr</i> <i>port-number</i> Example: umg-1(config-nat)# vpim external 192.0.2.24 26	(Optional) Configures the external IP address and listening port for VPIM requests.

	Command or Action	Purpose
Step 17	end Example: se-10-0-0-0(config-nat)# end	Exits NAT configuration mode and enters configuration mode.
Step 18	messaging-gateway registration Example: se-10-0-0-0(config)# messaging-gateway registration	Causes the endpoint to send a registration message to its primary and, if applicable, to its secondary messaging gateway, unless registration with the primary fails due to a configuration error.
Step 19	end Example: se-10-0-0-0(config)# end	Exits configuration mode and enters EXEC mode.
Step 20	show messaging-gateway Example: se-10-0-0-0# show messaging-gateway	Displays the details associated with the registration with the messaging gateway, successful or otherwise. For more information, see the “Verifying the Registration Status of a Cisco Unity Express Endpoint” section on page 73.
Step 21	write memory Example: se-10-0-0-0# write memory	Copies the running-config to the startup-config.

Example

The following commands on a Cisco Unity Express Release 3.1 and later versions endpoint set it up to autoregister with Cisco UMG, and then enable autoregistration, and finally write the configuration to startup-config:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# messaging-gateway primary 100 192.0.2.0
se-10-0-0-0(config-messaging-gateway)# username cue31 password text herein
se-10-0-0-0(config-messaging-gateway)# retry-interval 2
se-10-0-0-0(config-messaging-gateway)# nat http 192.0.2.22 80
se-10-0-0-0(config-messaging-gateway)# end
se-10-0-0-0(config)# messaging-gateway secondary 101 192.0.2.21
se-10-0-0-0(config-messaging-gateway)# username cue32 password text herein
se-10-0-0-0(config-messaging-gateway)# retry-interval 2
se-10-0-0-0(cconfig-messaging-gateway)# nat vpim 192.0.2.23 9925
se-10-0-0-0(config-messaging-gateway)# end
se-10-0-0-0(config)# messaging-gateway registration
se-10-0-0-0(config)# end
se-10-0-0-0> show messaging-gateway
Messaging gateways :
AutoRegister to gateway(s) : Enabled
Remote directory lookup : Enabled (without TUI prompt)
Primary messaging gateway :
    192.0.2.0
    nat http 192.0.2.22 (80)
    Status : Registered (Wed Sep 19 18:04:45 PDT 2007)
    Reg-expiration : Thu Sep 20 18:04:45 PDT 2007
    Default route : Disabled
    Location-id : 100
```



```

Reg-id : cue31
Reg-password : (Not displayed)
Retry-interval : 2 minute(s)
Secondary messaging gateway :
  192.0.2.21
  nat http 10.1.3.150 (80)
  nat vpim 192.0.2.23 (9925)
Status : Registered (Wed Sep 19 18:04:45 PDT 2007)
Reg-expiration : Thu Sep 20 18:04:45 PDT 2007
Default route : Disabled
Location-id : 101
Reg-id : cue32
Reg-password : (Not displayed)
Retry-interval : 2 minute(s)
se-10-0-0-0> write memory

```

Manually Registering a Cisco Unity Express Endpoint

If you want to add a Cisco Unity Express endpoint to your Cisco UMG system, and:

- it is running Cisco Unity Express Release 3.0 or earlier versions, or
- you want to avoid autoregistration activity with an endpoint running Cisco Unity Express Release 3.1 and later versions,

you must manually provision it from Cisco UMG.

Configure the endpoint following the instructions in the Cisco Unity Express documentation. For more information, see the “Configuring Network Locations” section of the [Cisco Unity Express VoiceMail and Auto Attendant CLI Administrator Guide](#).



Note

You must perform the steps only if the endpoint has never undergone initial configuration. If the endpoint is already in operation, you will already have done all this.

Verifying the Registration Status of a Cisco Unity Express Endpoint

You can verify whether the current Cisco Unity Express endpoint is registered with a messaging gateway, and check all the details associated with the registration - successful or otherwise - by using the **show messaging-gateway** command in Cisco Unity Express EXEC mode.

You can see which Cisco UMGs you have configured as its primary and secondary messaging gateways, with their respective port numbers. Indications in the status column show whether or not the endpoint has registered with the messaging gateway successfully.

Table 1 *show messaging-gateway Output*

AutoRegister to messaging gateway(s)	Enabled / disabled		
Remote directory lookup	Enabled / disabled	with / without TUI prompt	
Primary/secondary messaging gateway	IP address (port number)		
	Status	Registered / Not Registered	If registered, timestamp of initial registration confirmation; if not registered, reason is given as a code (see Table 2).
	Default route	Enabled/ disabled	
	Location-id	location-id of the messaging gateway	
	Reg-id	Registration username the Cisco UMG expects from endpoint.	
	Reg-password	(Not displayed)	Registration password the Cisco UMG expects from endpoint. It is never displayed.
	Retry-interval	Delay in minutes before the endpoint attempts to register again. Default is 5 minutes.	Not displayed if not set.

If the endpoint has registered successfully, you will see the date and time of the initial registration in the status column. You can also check the configuration for a default routing destination for a message to a voicemail address that can be resolved by neither Cisco Unity Express nor Cisco UMG. To illustrate: if you give a phone number that cannot be found in a Cisco Unity Express local search or in a Cisco UMG remote lookup, the message will be forwarded to that default route destination.

If the endpoint has not registered successfully, the reason for the failure will be displayed in the status column.

Table 2 *show messaging-gateway: Status Codes*

Code	Meaning
Registered	
Not registered	Autoregistration is not enabled
Not configured	
Not registered (general error)	Autoregistration failed due to an error other than those specified in this table.
Not registered (connection timeout)	Connection timed out
Not registered (authentication failed)	Authentication failed

Table 2 *show messaging-gateway: Status Codes*

Code	Meaning
Not registered (link is down)	Link is down
Not registered (location is forbidden)	The Cisco Unity Express endpoint with that location-id has been blocked by Cisco UMG and is thus is not allowed to register (for instructions on how to prevent an endpoint from registering, see the “Configuring Endpoint Autoregistration Support” section on page 28).
Not Registered (duplicated location)	The Cisco Unity Express location ID is not globally unique: there is another entity in the system with the same location-id.
Not Registered (invalid configuration)	General configuration error such as the secondary messaging gateway location ID not being configured on the primary messaging gateway.
Not Registered (manually de-registered)	An intermediate state to indicate manually triggered re-registration, for example, the messaging gateway’s access information being updated.

Enabling or Disabling Remote Lookup, With or Without TUI Confirmation

Enabling Remote Directory Lookup Without TUI Prompt

When you enable autoregistration by issuing the **messaging-gateway registration** command on a Cisco Unity Express endpoint, you also enable the endpoint to do remote lookup automatically. This includes a short prompt informing subscribers that the lookup may take some time.

Enabling Remote Directory Lookup With TUI Prompt

Enabling the remote directory lookup feature does not also enable the directory lookup confirmation in the TUI flow feature, in which Cisco Unity Express gives subscribers the option to do remote lookup if there is no local match. To enable TUI directory lookup confirmation, use the config-mode command **messaging-gateway directory lookup tui-prompt**.

Disabling Remote Directory Lookup

To have no remote lookup at all, disable it by issuing the **no messaging-gateway directory lookup** command.



Note

Disabling the remote directory lookup feature also disables directory lookup confirmation in the TUI flow, and conversely, enabling directory lookup confirmation in the TUI flow will also enable remote directory lookup.

Viewing Status

To view the status of these features, use the **show messaging-gateway** command, which displays the following output:

Remote directory lookup status:

- No--remote directory lookup is disabled
- Yes--remote directory lookup is enabled
 - Enabled with TUI-prompt--TUI confirmation prompt is enabled
 - Enabled without TUI-prompt--TUI confirmation prompt is disabled.

Viewing Cached and/or Configured Network Locations

To view a list of all cached remote location entries on Cisco Unity Express, use the EXEC-mode **show network locations cached** command.

To list all configured remote location entries on Cisco Unity Express, use the EXEC-mode **show network locations configured** command. This command replaces the old **show network locations** command.

Refreshing Locations

To manually refresh a cached location entry on Cisco Unity Express Release 3.1 and later versions, use the **network location cache refresh *id*** command in EXEC-mode. This command will not generate any response if it is performed successfully. Otherwise, an error message appears.

Setting the Expiration for Cached Locations

To set the expiration time for a cached location on Cisco Unity Express, use the **network location cache expiry *int*** command in config-mode. The *int* value stands for number of days. By default, this value is set to 4. The **no** command will set the value back to its default value. The value is persisted by means of the nvgen method. It is not stored in the database.

Overloading a NAT Device: the Consequences for Endpoints

One endpoint can be configured to get to its primary messaging gateway with complete connectivity if:

- Two Cisco Unity Express endpoints are behind a NAT device that has only one IP address to assign --an overload situation--
- Those endpoints have two different messaging gateways configured as primary messaging gateways,



Note

The other endpoint can only do HTTP-related activities (assuming proper configuration) and not the SMTP activities.



PART 4

Other Features



Configuring Authentication, Authorization, and Accounting

Last Updated: December 2, 2010

This chapter contains procedures for:

- [Configuring the Accounting Server, page 110](#)
- [Configuring the Authentication Server, page 112](#)
- [Configuring the AAA Policy, page 114](#)
- [Configuring Privileges, page 116](#)
- [Configuring Accounting Event Logging, page 123](#)
- [Configuring Console Authentication, page 126](#)

Overview

Cisco Unified Messaging Gateway supports Authentication, Authorization, and Accounting (AAA) which enables you to determine which users could access restricted services by assigning predefined privileges to groups.

You can create privileges and then assign these privileges to groups. Cisco UMG supports the following features:

- The ability to log AAA accounting information that enables you to easily audit configuration changes, maintain security, accurately allocate resources, and determine who should be billed for the use of resources.
- The ability to use a remote RADIUS server for authentication.
- The ability to configure failover capabilities to for the accounting and authentication servers.

To configure the AAA features, use the following procedures:

- [Configuring the Accounting Server, page 110](#)
- [Configuring the Authentication Server, page 112](#)
- [Configuring the AAA Policy, page 114](#)
- [Configuring Privileges, page 116](#)
- [Configuring Accounting Event Logging, page 123](#)
- [Configuring Console Authentication, page 126](#)

Configuring the Accounting Server

You can configure up to two AAA accounting servers. Automatic failover functionality is provided if you have two accounting servers configured. In this case, if the first server is unreachable, the accounting information is sent the second server. If both accounting servers are unreachable, accounting records are cached until a server becomes available. If a server cannot be reached before the cache is full, the oldest accounting packets are dropped to make room for the new packets.

Because the configuration of the AAA accounting server is completely independent of the AAA authentication server, you can configure the AAA accounting server to be on the same or different machine from the AAA authentication server.

If you use a syslog server, it is not affected by the AAA configuration and continues to use the existing user interfaces. When the RADIUS server sends AAA accounting information to a syslog server, it is normalized into a single string before being recorded. If no syslog server is defined, the AAA accounting logs are recorded by the syslog server running locally on Cisco UMG.

For an accounting server, you can configure the following information used to log into the server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Number of login retries
- Length of login timeout

**Note**

Only RADIUS servers are supported.

Specifying AAA Accounting Settings

SUMMARY STEPS

1. **config t**
2. **aaa accounting server remote**
3. **address *address* [port *port*] secret *secret***
4. **address *address* [port *port*] credentials hidden *cred***
5. **retries *number***
6. **timeout *seconds***
7. **end**
8. **show aaa accounting service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	aaa accounting server remote Example: umg-1(config)# aaa accounting server remote	Enters aaa-authentication submode to enable you to configure the AAA authentication server.
Step 3	address address [port port] secret secret Example: umg-1(config)# address 10.2.2.10 prt 1808 secret ezsecret	Defines the access parameters for the AAA accounting server.
Step 4	address address [port port] credentials hidden cred Example:	Defines the access parameters for the AAA accounting server.
Step 5	retries number Example: umg-1(config)# retries 6	Specifies the maximum number of times an AAA accounting request is retried before the accounting request fails.
Step 6	timeout seconds Example: umg-1(config)# timeout 24	Specifies the amount of time to wait before an AAA accounting request is considered to be unanswered.
Step 7	end Example: umg-1(config)# end	Exits to privileged EXEC mode.
Step 8	show aaa accounting service Example: umg-1# show aaa accounting service	(Optional) Displays the settings for the AAA accounting server.

Examples

The following is sample output from the **show aaa accounting service** command:

```
umg-1# show aaa accounting service
AAA Accounting Service Configuration
Accounting: Enabled
Address: 192.168.1.101 Port: 1813 Credentials:
EugxIjn3MbL3WgUZUdUb90nfGWTYHfmPSd8ZZNgd+Y9J3x1k2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3x1k2B35j0nfGW
TYHfmPSd8ZZNgd+Y9J3x1k2B35j0nfGWTYHfmP
Address: 192.168.1.100 Port: 1813 Credentials:
EugxIjn3MbL3WgUZUdUb90nfGWTYHfmPSd8ZZNgd+Y9J3x1k2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3x1k2B35j0nfGW
TYHfmPSd8ZZNgd+Y9J3x1k2B35j0nfGWTYHfmP
Timeout: 5 (sec)
Retries: 3
```

Configuring the Authentication Server

The two procedures for configuring AAA authentication consist of:

- Configuring connection parameters for the AAA authentication server
- Configuring whether the authentication servers or local authentication database will be queried first

This section covers only the first procedure. The second procedure is covered in the [“Configuring the AAA Policy” section on page 114](#).

For an AAA authentication server, you can configure the following information used to log into the server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Number of login retries
- Length of login timeout



Note

To help protect the cryptographic information of the RADIUS server, you must view the running configuration to see this information.

Specifying AAA Authentication Settings

SUMMARY STEPS

1. **config t**
2. **aaa authentication server remote**
3. **address *address* [port *port*] secret *secret***
4. **address *address* [port *port*] credentials hidden *cred***
5. **retries *number***
6. **timeout *seconds***

7. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	aaa authentication server remote Example: umg-1(config)# aaa authentication server remote	Enters aaa-authentication submode to enable you to configure the AAA authentication server.
Step 3	address address [port port] secret secret Example: umg-1(config)# address 10.2.2.10 port 1808 secret ezsecret	Defines the access parameters for the AAA authentication server.
Step 4	address address [port port] credentials hidden cred Example:	Defines the access parameters for the AAA authentication server.
Step 5	retries number Example: umg-1(config)# retries 6	Specifies maximum number of times an AAA authentication request is retried before the authentication request fails.
Step 6	timeout seconds Example: umg-1(config)# timeout 24	Specifies the amount of time to wait before an AAA authentication request is considered unanswered.
Step 7	end Example: umg-1(config)# end	Exits to privileged EXEC mode.

Configuring the AAA Policy

The AAA policy specifies the failover functionality that you can optionally configure for the authentication server. You can choose from two types of failover functionality:

- Authentication failover
- Unreachable failover

You can also use a combination of both failover methods.

Authentication Failover

The authentication failover feature enables you to optionally use a remote RADIUS server for user login authentication in addition to the local database. The procedure in this section configures the order in which authentication is resolved. You can configure authentication to use:

- Only the local database
- Only the remote server
- The local database first, then the remote server
- The remote server first, then the local database

**Note**

The authentication failover feature has the following limitations:

- Authentication with a RADIUS server is available only when accessing the GUI or CLI interface and requires only a user ID and password.
 - Login information is not synchronized between the local system and the remote server. Any security features such, as password expiration, must be configured separately for Cisco Unified Messaging Gateway and the RADIUS server.
-

Unreachable Failover

The unreachable failover is used only with RADIUS servers. This feature enables you to configure up to two addresses that can be used to access RADIUS servers.

As Cisco UMG attempts to authenticate a user with the RADIUS servers, messages are sent to users to notify them when a RADIUS server:

- Cannot be reached
- Fails to authenticate the user

Example

In this example, authentication is performed by the remote server first, then by the local database. Also, two addresses are configured for the remote RADIUS server.

This is a sequence of events that could occur during authentication for this example:

1. Cisco UMG tries to contact the first remote RADIUS server.

2. If the first RADIUS server does not respond or does not accept the authentication credentials of the user, Cisco UMG tries to contact the second remote RADIUS server.
3. If the second RADIUS server does not respond or does not accept the authentication credentials of the user, the user receives the appropriate error message and Cisco UMG tries to contact the local database.
4. If the local database does not accept the authentication credentials of the user, the user receives an error message.

Specifying the Policy that Controls the Behavior of Authentication and Authorization

SUMMARY STEPS

1. `config t`
2. `aaa policy system`
3. `authentication-order {remote [local] | local [remote]}`
4. `authorization merge-attributes`
5. `end`
6. `show aaa policy`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>umg-1# config t</code>	Enters configuration mode.
Step 2	<code>aaa policy system</code> Example: <code>umg-1(config)# aaa policy system</code>	Enters aaa-authentication submode to enable you to specify the policy that controls the behavior of authentication and authorization.
Step 3	<code>authentication-order {remote [local] local [remote]}</code> Example: <code>umg-1(config)# authentication-order remote local</code>	Specifies the order in which to query the authentication servers and local authentication database.
Step 4	<code>authorization merge-attributes</code> Example: <code>umg-1(config)# authorization merge-attributes</code>	Specifies whether the user attributes that are retrieved from a remote RADIUS AAA server are merged with attributes for the same username found in the local user database.

	Command or Action	Purpose
Step 5	end Example: umg-1(config)# end	Exits to privileged EXEC mode.
Step 6	show aaa accounting policy Example: umg-1# show aaa policy	(Optional) Displays the AAA policy settings.

Examples

The following is sample output from the **show aaa policy** command:

```
umg-1# show aaa policy
authentication-order local
merge-attributes enable
preferred-server remote
```

Configuring Privileges

Cisco UMG software provides several predefined privileges that you can assign to groups. You can also create your own privileges and modify the predefined privileges.

When you assign a privilege to a group, any member of the group is granted the privilege rights. An administrator group is created automatically by the software initialization process from the imported subscribers designated as administrators.

When you create or modify privileges, you add or delete the operations allowed by that privilege. Operations define the CLI commands and GUI functions that are allowed. In addition to adding operations to a privilege, you can also configure a privilege to have another privilege nested inside of it. A privilege configured with a nested privilege includes all operations configured for the nested privilege.

As part of the planning process, you should decide:

- How many categories of user privileges you want to create for your company.
- Which functions each privilege will allow your users to perform.

After you decide which privileges you want your users to have:

1. Review the predefined privileges to determine whether any of them are similar to the permissions that you want to give to each of your categories of users.
2. Configure a separate privilege for each category by specifying which operations each category of users will be allowed to perform, optionally including predefined privileges (see [“Creating and Customizing Privileges” on page 121](#)).
3. Create a group for each category of user privilege and assign the appropriate privilege to each group of users.
4. Add your users to the appropriate group.



Tip

For an example of the commands used for these steps, see the [“Configuration Example” section on page 119](#).

**Note**

You cannot modify the superuser privilege.

Table 3 describes the predefined privileges provided with the Cisco UMG software and the operations associated with them. Table 4 describes all available operations that you can add to privileges.

To display a list of privileges, use the **show privileges** command in Cisco UMG EXEC mode. To display detailed information about a specific privilege, use the **show privilege detail** command.

Table 3 *Privileges*

Privilege	Description	Operations
Superuser	Grants unrestricted system access.	all
Broadcast	Allows subscribers to send broadcast messages across the network.	broadcast.local, broadcast.remote, system.debug
Local-broadcast	Allows subscribers to send broadcast messages only to subscribers on the local network.	broadcast.local, system.debug
ViewRealTime Reports	Allows subscribers to view real-time reports	report.realtime
manage-users	Allows subscribers to create, modify, and delete users	user.configuration, user.pin, user.password, user.mailbox, user.notification, user.remote, group.configuration, system.debug
manage-passwords	Allows subscribers to create, modify, and delete user passwords and PINs	user.pin, user.password, system. debug

Table 4 *List of Operations*

Operation	Description
group.configuration	Create, modify, and delete groups.
security.aaa	Configure and modify AAA service settings.
security.access	Configure system level security regarding encryption of data, including defining crypto keys. Note Also includes permission to reload the system.

Table 4 *List of Operations (continued)*

Operation	Description
security.password	Configure settings for the system password and policy, such as: <ul style="list-style-type: none"> • Expiry • Lockout (temporary and permanent) • History • Length
security.pin	Configure settings for the system PIN and policy, such as: <ul style="list-style-type: none"> • Expiry • Lockout (temporary and permanent) • History • Length
services.configuration	Configure system services: DNS, NTP/clock, SMTP, SNMP, Fax Gateway, Cisco UMG, hostname, domain, interfaces (counters), and system default language. Note Also includes permission to reload the system.
services.manage	System level services commands not related to configuration like clearing DNS cache and ping.
software.install	Install, upgrade, or inspect system software or add-ons such as languages and licenses. Note Also includes permission to reload the system.
system.backup	Configure backup.
system.configuration	Configure system settings such as the clock, hostname, domain name, default language, and interfaces (counters).
system.debug	Collect and configure trace and debug data. Includes copying data like core and log files.
system.view	View system settings and configuration.
user.configuration	Create, modify, and delete users and groups, including the configuration of: <ul style="list-style-type: none"> • First and Last Name • Nickname • Display Name • Language
user.password	Create, set, or remove others passwords.
user.pin	Create, set, or remove others PINs.

Configuration Example

In this example, a company wants a security structure with two levels of security administration. The two levels allow the following actions to be taken by the administrator:

- The first level enables the security administrator to reset the passwords and PINs for users that have locked themselves out of the system, whether they forgot their password or their account is locked because of too many failed login attempts. This level will be called PASSWORD RESET.
- The second level enables the security administrator to act as a system guardian by:
 - Ensuring that the proper security policies are implemented for issues such as password aging, account lockout, encryption, authentication, authorization, and accounting
 - Ensuring that data remain safe from attackers without over burdening end users with security related details and tasks
 - Monitoring the system to ensure that only legitimate users have access
 - Troubleshooting any problems that legitimate users have with accessing the system
 - Resetting passwords and PINs for users that have locked themselves out of the system, whether they forgot their password or their account is locked because of too many failed login attempts

This level is called SYSTEM GUARDIAN.

When you use the general planning and configuration steps as described in the [“Configuring Privileges” section on page 116](#), to set up the security administration levels for this example, these are the results:

- You have already decided:
 - How many levels or categories of user privileges you want to create for your company
 - Which functions each privilege will allow your users to perform

There will be two levels, called PASSWORD RESET and SYSTEM GUARDIAN, as described above.

- After reviewing the predefined privileges to determine whether any of them are similar to the permissions that you want to give each of your security levels, you find that:
 - The predefined privilege called *manage-passwords* can be used for the security level named PASSWORD RESET because it has all of the permissions needed to help users that have locked themselves out of the system.
 - The *manage-passwords* privilege also has a subset of the permissions needed the security level named SYSTEM GUARDIAN and is the predefined privilege closest to your requirements. However, to act as system guardian, the following additional operations will have to included: *security.access*, *security.aaa*, *security.password*, *security.pin*, *system.debug*, and *system.view*. See [Table 4 on page 117](#) for more information.
- Use the following commands to configure a privilege for the SYSTEM GUARDIAN security level by including the predefined privilege *manage-password* and adding the operations listed in the previous bullet:

```
umg-1(config)# privilege guardian-privilege create
umg-1(config)# privilege guardian-privilege member manage-passwords
umg-1(config)# privilege guardian-privilege operation security.access
umg-1(config)# privilege guardian-privilege operation security.aaa
umg-1(config)# privilege guardian-privilege operation security.password
umg-1(config)# privilege guardian-privilege operation security.pin
umg-1(config)# privilege guardian-privilege operation system.debug
umg-1(config)# privilege guardian-privilege operation system.view
```

**Note**

You do not have to configure a privilege for the PASSWORD RESET security level because you can use the predefined privilege *manage-passwords*.

- Use the following commands to create a new group called *password-reset* and assign the privilege called *manage-passwords* to it:

```
umg-1(config)# groupname password-reset create
umg-1(config)# groupname password-reset privilege manage-passwords
```

- Use the following commands to create a new group called *system-guardian* and assign the privilege called *guardian-privilege*:

```
umg-1(config)# groupname system-guardian create
umg-1(config)# groupname system-guardian privilege guardian-privilege
```

- Assign the appropriate users to the new groups, associating them with their roles. For example, if you want Bob and Ned to have the privileges of the PASSWORD RESET security administration level and Ann to have the privileges of the SYSTEM GUARDIAN security administration level, use the following commands:

```
umg-1(config)# groupname password-reset member bob
umg-1(config)# groupname password-reset member ned
umg-1(config)# groupname system-guardian member ann
```

- The configuration of this example is now complete. You can verify your configuration using the following commands.

The following is sample output from the **show group detail groupname password-reset expanded** command:

```
umg-1# show group detail groupname password-reset expanded
Groupname:          password-reset
Full Name:          password-reset
Description:
Email:
Epage:

Group Members:      <none>
User Members:       bob ned
Group Owners:       <none>
User Owners:        <none>
Privileges:         manage-passwords
```

The following is sample output from the **show group detail groupname system-guardian expanded** command:

```
umg-1# show group detail groupname system-guardian expanded
Groupname:          system-guardian
Full Name:          system-guardian
Description:
Email:
Epage:

Group Members:      <none>
User Members:       ann
Group Owners:       <none>
User Owners:        <none>
Privileges:         guardian-privilege
```

The following is sample output from the **show privilege detail manage-passwords expanded** command:

```
umg-1# show privilege detail manage-passwords expanded
Privilege:          manage-passwords
Description:        Privilege to reset user passwords

Privilege Members:  <none>
Operations:         system.debug user.password user.pin
```

The following is sample output from the **show privilege detail guardian-privilege expanded** command:

```
umg-1# show privilege detail guardian-privilege expanded
Privilege:          guardian-privilege
Description:

Privilege Members:  manage-passwords
Operations:         security.aaa security.access security.password security.pin
                   system.debug system.view
manage-passwords:  system.debug user.password user.pin
```

Creating and Customizing Privileges

SUMMARY STEP

1. **config t**
2. **privilege *privilege-name* create**
3. **privilege *privilege-name* description *string***
4. **privilege *privilege-name* operation *operation-name***
5. **privilege *privilege-name* member *privilege-name2***
6. **end**
7. **show operations**
8. **show operation detail *operation-name***
9. **show privileges**
10. **show privilege detail *privilege-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	privilege <i>privilege-name</i> create Example: umg-1(config)# privilege security-privilege create	Creates a new privilege. <ul style="list-style-type: none"> <i>privilege-name</i>—Label used to identify and configure a new or existing privilege.

	Command or Action	Purpose
Step 3	privilege <i>privilege-name</i> [description <i>string</i>] Example: umg-1(config)# privilege security-privilege description administer of system security	(Optional) Assigns a description to the privilege. <ul style="list-style-type: none"> <i>string</i>—Description to add to the privilege.
Step 4	privilege <i>privilege-name</i> operation <i>operation-name</i> Example: umg-1(config)# privilege security-privilege operation security.configuration	(Optional) Assigns an operation to the privilege: <ul style="list-style-type: none"> <i>operation-name</i>—Operation to associate with the privilege.
Step 5	privilege <i>privilege-name</i> member <i>privilege-name2</i> Example: umg-1(config)# privilege security-privilege include manage-users	(Optional) Includes or nests another privilege into this privilege: <ul style="list-style-type: none"> <i>privilege-name2</i>—Privilege to include or nest into this privilege.
Step 6	end Example: umg-1(config)# end	Exits to privileged EXEC mode.
Step 7	show operations Example: umg-1# show operations	(Optional) Displays information about all operations.
Step 8	show operation detail <i>operation-name</i> Example: umg-1# show operation detail security.configuration	(Optional) Displays information about the specified operation: <ul style="list-style-type: none"> <i>operation-name</i>—Label used to identify and configure a new or existing operation.
Step 9	show privileges Example: umg-1# show privilege	(Optional) Displays information about all privileges.
Step 10	show privilege detail <i>privilege-name</i> Example: umg-1# show privilege detail sales_vp	(Optional) Displays information about the specified privilege: <ul style="list-style-type: none"> <i>privilege-name</i>—Label used to identify and configure a new or existing privilege.

Examples

The following is sample output from the **show operations** command:

```
umg-1# show operations
show operations
group.configuration
security.aaa
security.access
security.password
security.pin
services.configuration
services.exec
```

```
services.manage
software.install
srx
system.backup
system.configuration
system.debug
system.view
user.configuration
user.password
user.pin
```

```
17 total operation(s)
```

The following is sample output from the **show operation detail** command:

```
umg-1# show operation detail user.password
Operation:      user.password
Description:    Set and reset passwords for other users
CLI:
               config-user-password
               exec-configure-terminal
               exec-copy-running-config-startup-config
               exec-show-user-auth
               exec-user-password
               exec-write
```

```
6 total command(s)
```

The following is sample output from the **show privileges** command:

```
umg-1# show privileges
ViewRealTimeReports
broadcast
local-broadcast
manage-passwords
manage-users
superuser
```

```
6 total privilege(s)
```

Configuring Accounting Event Logging

AAA accounting logs contain information that enables you to easily:

- Audit configuration changes
- Maintain security
- Accurately allocate resources
- Determine who should be billed for the use of resources

You can configure AAA accounting to log the following types of events:

- Logins—All forms of system access, including access to the CLI and GUI when a login is required.
- Logouts—All forms of system access, including access to the CLI and GUI when a login is required before logout.
- Failed logins—Failed login attempts for all forms of system access, including access to the CLI and GUI when a login is required.
- Configuration mode commands—Any changes made to the Cisco UMG configuration using the CLI or GUI.
- EXEC mode commands—Any commands entered in Cisco UMG EXEC mode using the CLI or GUI.
- System startups—System startups, which include information about the system's software version, installed licenses, installed packages, and so on.
- System Shutdowns—System shutdowns, which include information about the system's software version, installed licenses, installed packages, and so on.

In addition to information specific to the type of action performed, the accounting logs also indicate:

- User that authored the action
- Time when the action was executed
- Time when the accounting record was sent to the server

The detailed content of the log entries is explained in the [“Examples” section on page 126](#).



Note

Account logging is not performed during the system power-up playback of the startup configuration. When the system boots up, the startup-config commands are not recorded.

Configuring Accounting Event Logging

SUMMARY STEPS

1. **config t**
2. **aaa accounting enable**
3. **aaa accounting event**
4. **login**
5. **logout**
6. **login-fail**
7. **config-commands**
8. **exec-commands**
9. **system-startup**
10. **system-shutdown**
11. **end**
12. **show aaa accounting event**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	aaa accounting enable Example: umg-1(config)# aaa accounting enable	
Step 3	aaa accounting event Example: umg-1(config)# aaa accounting event	
Step 4	login Example: umg-1(config)# login	Enables the logging of logins.
Step 5	logout Example: umg-1(config)# logout	Enables the logging of logouts
Step 6	login-fail Example: umg-1(config)# login-fail	Enables the logging of failed logins.
Step 7	config-commands Example: umg-1(config)# config-commands	Enables the logging of configuration mode commands.
Step 8	exec-commands Example: umg-1(config)# exec-commands	Enables the logging of configuration mode commands.
Step 9	system-startup Example: umg-1(config)# system-startup	Enables the logging of system startups.
Step 10	system-shutdown Example: umg-1(config)# system-shutdown	Enables the logging of system shutdowns.

	Command or Action	Purpose
Step 11	end Example: umg-1(config)# end	Exits to privileged EXEC mode.
Step 12	show aaa accounting event umg-1# show aaa accounting	(Optional) Displays the AAA accounting events that are designated to be logged.

Examples

The following is sample output from the **show aaa accounting event** command:

```
umg-1# show aaa accounting event
Event           State      Description
login           Enabled    Log accounting events for successful login
logout          Enabled    Log accounting events for user logout
login-fail       Enabled    Log accounting events for failed login attempts
config-commands Enabled    Log accounting events for any changes to configuration
exec-commands   Enabled    Log accounting events for execution of commands
system-startup   Enabled    Log accounting events for system startup
system-shutdown Enabled    Log accounting events for system shutdown
imap            Enabled    Log accounting events for all imap events
```

Configuring Console Authentication

By default, console authentication is disabled, allowing any user logging into the system through the console to have superuser privileges and to log in without providing a username or password.

Therefore, to protect your console from unauthorized access, you must enter the **login** command in config-line mode, as described below.



Note

To see whether authentication is enabled for the console, you must view the running configuration.

Specifying Whether the Console Connection is Subject to Authentication

SUMMARY STEPS

1. **config t**
2. **line console**
3. **login**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	line console Example: umg-1(config)# line console	Enters config-line mode to enable you to specify whether the console connection is subject to authentication.
Step 3	login Example: umg-1(config-line)# line console	Requires that any user logging in through the console connection is subject to authentication. The no or default form of this command disables authentication for the console.
Step 4	end Example: umg-1(config)# end	Exits to privileged EXEC mode.



PART 5

Maintenance and Troubleshooting



Backing Up and Restoring Data

Last Updated: December 2, 2010



Note

Setting up a backup server is part of the initial configuration process. If you have not already done this, see the [Initial Configuration Tasks](#).

- [About Backing Up and Restoring Data, page 131](#)
- [Restrictions for Backing Up and Restoring Data, page 132](#)
- [Setting Backup Parameters, page 132](#)
- [Backing Up Files, page 134](#)
- [Restoring Files, page 136](#)
- [Backup and Restore Using SFTP, page 139](#)
- [Backup Server Authentication Using a SSH Host Key, page 140](#)
- [Encrypting and Signing of Backup Content on the Server, page 143](#)
- [Configuring Scheduled Backup Jobs, page 144](#)

About Backing Up and Restoring Data

Cisco UMG backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from the Cisco UMG module to the FTP server and the restore function copies the files from the FTP server to the Cisco UMG application. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

We recommend that you back up your configuration files whenever you make changes to the system or application files. Do backups regularly to preserve configuration data.

The system supports the following types of backup:

- All files (backs up configuration and data)
- Only data files (includes dynamic data such as local endpoint IDs, mailboxes, and system distribution lists)



Note

We strongly discourage doing the “only data” type of backup and restore because of its potential to introduce inconsistency between configuration and data files.

- Only configuration files (includes the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data)

Restrictions for Backing Up and Restoring Data

- Backing up and restoring both require offline mode, so we recommend performing this task when call traffic is least impacted. Offline mode terminates message forwarding and directory exchange.
- Cisco UMG does not support the following backup and restore capabilities:
 - Centralized message storage arrangement. Cisco UMG backup files cannot be used or integrated with other message stores.
 - Selective backup and restore. Only full backup and restore functions are available. Individual messages or other specific data can be neither stored nor retrieved.
- If you delete an endpoint, then do a system restore, the update will erase the information that the endpoint was deleted. You must reset it from the endpoint's primary messaging gateway.

Setting Backup Parameters

The backup parameters define the FTP server to use for storing Cisco Unified Messaging Gateway backup files and the number of backups that are stored before the system deletes the oldest one.

All Cisco Unified Messaging Gateway backup files are stored on the specified server. You can copy the backup files to other locations or servers, if necessary.

Cisco Unified Messaging Gateway automatically assigns an ID to each successful backup. Use this backup ID to restore the backup.

Prerequisites

- Verify that the backup server is configured.
- Verify that an FTP administrator or other user who can log in to the FTP server has full permission on the FTP server, such as read, write, overwrite, create, and delete permissions for files and directories.

Required Data for This Procedure

- Number of revisions to save before the oldest backup is written over
- FTP server URL
- User ID and password of the FTP server login

SUMMARY STEPS

1. **config t**
2. **backup {revisions *number* | server url *ftp-url* username *ftp-username* password *ftp-password*}**
3. **exit**

4. show backup

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	backup {revisions number server url ftp-url username ftp-username password ftp-password} Example: umg-1(config)# backup server url ftp://main/backups username "admin" password "wxyz" umg-1(config)# backup server url ftp://172.168.10.10/backups username "admin" password "wxyz" umg-1(config)# backup revisions 5	Sets the backup parameters. <ul style="list-style-type: none"> server url—The <i>ftp-url</i> value is the URL to the network FTP server where the backup files will be stored. The <i>ftp-username</i> and <i>ftp-password</i> values are the user ID and password for the network FTP server. <p>Note The backup server must be configured before the backup revisions can be configured.</p> <ul style="list-style-type: none"> revisions—The number of backup files that will be stored. When this number is reached, the system deletes the oldest stored file. <p>In the example, main is the hostname of the FTP server and backups is the directory where backup files are stored.</p>
Step 3	exit Example: umg-1(config)# exit	Exits configuration mode.
Step 4	show backup Example: umg-1# show backup	Displays the backup server configuration information, including the FTP server URL and the number of revisions.

Examples

The following example configures a backup server and displays the **show backup** output:

```
umg-1# config t
umg-1#(config)# backup server url ftp://172.16.0.0/backups username admin password voice
umg-1#(config)# backup revisions 10
umg-1#(config)# exit
umg-1#

umg-1# show backup
Server URL: ftp://172.16.0.0/backups
User Account on Server: admin
Number of Backups to Retain: 10
umg-1#
```

Backing Up Files

Three types of backup requests are available: data only, configuration only, or all.

- **Data**—Backs up dynamic data such as local endpoint IDs, mailboxes, and system distribution lists
- **Configuration**—Backs up system configuration, including the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data). Use the **show run** command to display the current running configuration.
- **All**—Backs up all data and configuration information.

Backups are performed only in offline mode.

Cisco Unified Messaging Gateway automatically numbers and dates the backup files and identifies the revision number in a **backupid** field.

Performing different backup types at various times causes different backup IDs for data backups and configuration backups. For example, the last data backup ID might be 3, and the last configuration backup might be 4. Performing an “all” backup might result in a backup ID of 5 for both data and configuration.

When restoring the files, refer to the backup ID for the backup file that you want to use. Use the **show backup server** command for a list of backup IDs.



Note

We recommend that you back up your configuration files whenever changes are made to the system or application files. Data files, which contain voice messages, should be backed up regularly to minimize data loss, such as from a hardware failure.

SUMMARY STEPS

1. **offline**
2. **backup category {all | configuration | data}**
3. **continue**
4. **show backup history**
5. **show backup server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	offline	Enters offline mode.
	Example: umg-1# offline	
Step 2	backup category {all configuration data} Example: umg-1 (offline) # backup category all umg-1 (offline) # backup category configuration umg-1 (offline) # backup category data	Specifies the type of data to be backed up and stored.

	Command or Action	Purpose
Step 3	continue Example: umg-1(offline)# continue	Exits offline mode and returns to EXEC mode.
Step 4	show backup history Example: umg-1# show backup history	Displays the backup procedures and the success or failure of those attempts.
Step 5	show backup server Example: umg-1# show backup server	Displays the backup files available on the backup server, the date of each backup, and the backup file ID.

Examples

The following is sample output from the **show backup history** command:

```
umg-1# show backup history

aaa# show backup history
#Start Operation
Category: Configuration
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Data
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Data
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:49 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Configuration
```

```

Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 8
Date: Fri Feb 19 14:36:33 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

```

The following is sample output from the **show backup server** command:

```

umg-1# show backup server

Category:      Data
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:52 PDT 2003
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:33 PDT 2003
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:32 PDT 2003
Description:

Category:      Configuration
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:48 PDT 2003
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:27 PDT 2003
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:29 PDT 2003
Description:

umg-1#

```

Restoring Files

After the backup files are created, you can restore them when needed. Restoring is done in offline mode. Use the **show backup server** command to locate the backup ID of the file that you want to restore.

SUMMARY STEPS

1. **show backup server**
2. **offline**
3. **restore id *backupid* category {all | configuration | data}**
4. **show restore history**
5. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show backup server Example: umg-1# show backup server	Lists the data and configuration backup files. Look at the backup ID field for the revision number of the file that you want to restore.
Step 2	offline Example: umg-1# offline	Enters offline mode. All active voice-mail calls are terminated.
Step 3	restore id <i>backupid</i> category {all configuration data} Example: umg-1(offline)# restore id 22 category all umg-1(offline)# restore id 8 category configuration umg-1(offline)# restore id 3 category data	Specifies the backup ID <i>backupid</i> value and the file type to be restored.
Step 4	show restore history Example: umg-1# show restore history	Displays the restore procedures and the success or failure of those attempts.
Step 5	reload Example: umg-1(offline)# reload	Resets the Cisco Unified Messaging Gateway module so that the restored values take effect.

Example

The following example displays the backup server:

```
umg-1# show backup server

Category:      Data
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:52 PDT 2003
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:33 PDT 2003
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:32 PDT 2003
Description:

Category:      Configuration
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:48 PDT 2003
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:27 PDT 2003
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:29 PDT 2003
Description:

umg-1#
```

The following example shows the restore history:

```
umg-1# show restore history

#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/CUE_backup
Operation:      Restore
Backupid:      129
Restoreid:      15
Description:    CUE test backup
Date:          Sun Jun 13 12:32:48 PDT 1993
Result:        Success
Reason:
Version: 8.0.0.1
#End Operation
```

Backup and Restore Using SFTP

This section discusses the following topics:

- [Overview, page 139](#)
- [Configuring Backup and Restore Using SFTP, page 139](#)

Overview

You can transfer files from any Cisco Unified Messaging Gateway application to and from the backup server using Secure File Transfer Protocol (SFTP). SFTP provides data integrity and confidentiality that is not provided by FTP.

Because SFTP is based on Secure Shell tunnel version 2 (SSHv2), only SSHv2 servers are supported for this feature.

To run backup and restore over SFTP, you must configure the URL of the backup server in the form of `sftp://hostname/dir`, and also the username and password to login to the server. The backup server must have an SSH daemon running with the SFTP subsystem enabled. The SSH protocol allows various user authentication schemes.

Configuring Backup and Restore Using SFTP

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

There is no data required.

SUMMARY STEPS

1. `config t`
2. `backup {revisions number | server url sftp-url username sftp-username password sftp-password}`
3. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	backup {revisions number server url sftp-url username sftp-username password sftp-password} Example: umg-1(config)# backup server url sftp://branch/vmbackups username admin password mainserver	Performs a backup to the specified SFTP or FTP server. To use SFTP, the URL must be of the form <i>sftp://hostname/directory</i> .
Step 3	end Example: umg-1(config)# end	Returns to privileged EXEC mode.

Backup Server Authentication Using a SSH Host Key

This section discusses the following topics:

- [Overview, page 139](#)
- [Configuring Backup Server Authentication Without Using the SSH Host Key, page 141](#)
- [Configuring Backup Server Authentication Using the SSH Host Key, page 142](#)

Overview

You can authenticate the backup server using the SSH protocol before starting a backup/restore operation. The SSH protocol uses public key cryptography for server authentication.

This feature provides two methods of authenticating a server:

- Establishing a secure connection based only on the URL of a trusted backup server.
- Obtaining the fingerprint of the backup server and using it to establish a secure connection. This fingerprint is also known as the host key or private key.

The first method is easier than the second method, but it is less secure because it does not depend on you knowing the backup server's private host key. However, if you know the URL of a trusted backup server, it is generally safe. In this case, the backup server securely provides the client with its private host key.

In both cases, when server authentication is enabled, the system validates the SSH server's private host key by comparing the fingerprint of the key received from the server with a preconfigured string. If the two fingerprints do not match, the SSH handshake fails, and the backup/restore operation does not occur.

You cannot use the GUI to configure this feature; you must use the CLI.

Both methods are explained in the following sections.

Configuring Backup Server Authentication Without Using the SSH Host Key

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

To enable SSH authentication of a backup server without knowing the server's fingerprint (private host key), you must know the URL of a trusted backup server.

SUMMARY STEPS

1. **config t**
2. **backup server url sftp://url**
3. **backup server authenticate**
4. **end**
5. **show security ssh knownhost**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	backup server url sftp://url Example: umg-1(config)# backup server url sftp://company.com/server22	Establishes an initial connection with the backup server.
Step 3	backup server authenticate Example: umg-1(config)# backup server authenticate	Retrieves the fingerprint of the backup server's host key and establishes a secure SSH connection.
Step 4	end Example: umg-1(config)# end	Returns to privileged EXEC mode.
Step 5	show security ssh knownhost Example: umg-1(config)# show security ssh knownhost	Displays a list of configured SSH servers and their fingerprints.

Configuring Backup Server Authentication Using the SSH Host Key

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

To use a backup server's fingerprint (private host key) to enable SSH authentication, you must first retrieve the fingerprint "out-of-band" by running the **ssh-keygen** routine on the backup server. This routine is included in the OpenSSH package. The following example shows the command and its output:

```
ssh-keygen -l -f /etc/ssh/ssh_host_dsa_key.pub
```

```
1024 4d:5c:be:1d:93:7b:7c:da:56:83:e0:02:ba:ee:37:c1 /etc/ssh/ssh_host_dsa_key.pub
```

SUMMARY STEPS

1. **config t**
2. **security ssh knownhost host {ssh-rsa | ssh-dsa} fingerprint-string**
3. **end**
4. **show security ssh knownhost**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	security ssh knownhost host {ssh-rsa ssh-dsa} fingerprint-string Example: umg-1(config)# security ssh knownhost server.cisco.com ssh-rsa a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3	Configures the MD5 fingerprint of the SSH server's host key using the following arguments and keywords: <i>host</i> — Fully qualified hostname or IP address of the SSH server. ssh-rsa — RSA algorithm was used to create this fingerprint for a SSH server's host key. ssh-dsa — DSA algorithm was used to create this fingerprint for a SSH server's host key. <i>fingerprint-string</i> — MD5 fingerprint string.

	Command or Action	Purpose
Step 3	<code>end</code> Example: <code>umg-1(config)# end</code>	Returns to privileged EXEC mode.
Step 4	<code>show security ssh knownhost</code> Example: <code>umg-1(config)# show security ssh knownhost</code>	Displays a list of configured SSH servers and their fingerprints.

Encrypting and Signing of Backup Content on the Server

This section discusses the following topics:

- [Overview, page 143](#)
- [Configuring the Encryption and Signing of Backup Content on the Server, page 143](#)

Overview

You can protect backed up configuration and data files using signing and encryption before the files are transferred to the backup server.

To enable this feature, you must configure a master key, from which the encryption and signing key (known as the session key) are derived. The backup files are encrypted and signed before they are sent to the backup server. When you restore the files, the master key is used to validate the integrity of the files and decrypt them accordingly. You can also restore the backup files to any other machine running Cisco Unified Messaging Gateway 8.0 or later versions, if you configure the same master key before you begin the restore process. To make it easier to automate a scheduled backup, the master key is stored securely on the hosting device. It is not included in the backup content.

During the restore process, if the system detects that backup content has been tampered with, the restore process aborts. The system also halts and waits for the administrator to take some action, such as restoring using a different revision.

For backward compatibility, you can allow unsigned backup files to be restored if the risk is acceptable.

Configuring the Encryption and Signing of Backup Content on the Server

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

There is no data required.

SUMMARY STEPS

1. **config t**
2. **backup security key generate**
3. **backup security protected**
4. **backup security enforced**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: umg-1# config t	Enters configuration mode.
Step 2	backup security key generate Example: umg-1(config)# backup security key generate	Creates the master key used for encrypting and signing the backup files.
Step 3	backup security protected Example: umg-1(config)# backup security protected	Enables secure mode for backups. In secure mode, all backup files are protected using encryption and a signature.
Step 4	backup security enforced Example: umg-1(config)# backup security enforced	Specifies that only protected and untampered backup files are restored.
Step 5	end Example: umg-1(config)# end	Returns to privileged EXEC mode.

Configuring Scheduled Backup Jobs

Beginning in release 8.0, you can configure one-time or recurring backup jobs.

For recurring backup jobs, you can configure the jobs to repeat:

- Every N days at a specific time
- Every N weeks on a specific day and time
- Every N months on a specific day of the month and time
- Every N years on a specific month

You can configure up to five repetitive scheduled backup jobs and five one-time scheduled backup jobs.

Whenever a backup job (or any scheduled activity) is started and in progress, any other activities that are scheduled to start at this time, are put in queue to wait for the first activity to finish. The maximum size of the queue is nine activities.

You cannot delete individual instances of a recurring scheduled backup schedule; you can only delete the entire series of backup jobs. However, you can enable forever a given scheduled action by configuring start and end dates for the action to specify when the action is active. You can also suspend a scheduled action indefinitely by not specifying an expiration date for the action.

Immediate backup requests are always given precedence over scheduled backup jobs. If the scheduled backup is configured to start at the same time as an immediate backup, the scheduled backup job is queued and the system waits for the immediate backup to finish before it attempts to start the scheduled backup job.

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

SUMMARY STEPS

1. **backup schedule** [*name*]
2. **repeat every** {*number days at time* | *number weeks on day* | *number months on day date* | *number years on month month*} **at** *time*



Note

Instead of the **repeat every** command, you can optionally use one of the following commands:

- **repeat once at** *time*
- **repeat daily at** *time*
- **repeat monthly on day** *date at time*
- **repeat weekly on day at** *time*
- **repeat yearly on month** *month at time*

3. **start-date** *date*
4. **stop-date** *date*
5. **disabled from** *date to date*
6. **backup categories** [*all*] [*configuration*] [*data*]
7. **end**
8. **show backup schedules** or **show schedules**
9. **show backup schedule detail job** *job-name* or **show schedule detail job** *job-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	backup schedule <i>[name]</i> Example: umg-1# backup schedule 22	Enters backup schedule configuration submode to enable you to configure a scheduled backup job.
Step 2	repeat every { <i>number days</i> <i>number weeks on day</i> <i>number months on day date</i> <i>number years on month month</i> } at time <i>time</i> Example: umg-1(backup-schedule)# repeat every 2 days at time 10:00	Specifies how often a recurring scheduled backup occurs. To configure a one-time backup job, use the repeat once command. You can also optionally use one of the other repeat commands listed in the previous note.
Step 3	start-date <i>date</i> Example: umg-1(backup-schedule)# start-date 05/30/2009	Specifies the start date for the recurring scheduled backup to occur.
Step 4	stop-date <i>date</i> Example: umg-1(backup-schedule)# stop-date 10/20/2009	Specifies the stop date for the recurring scheduled backup to occur.
Step 5	disabled from <i>date to date</i> Example: umg-1(backup-schedule)# disabled from 10/02/2009 to 10/06/2009	Specifies a time period that the recurring scheduled backup jobs are disabled.
Step 6	backup categories [<i>all</i>] [<i>configuration</i>] [<i>data</i>] Example: umg-1(backup-schedule)# backup categories configuration	Specifies which categories of data to backup.
Step 7	end Example: umg-1(backup-schedule)# end	Exits to privileged EXEC mode.
Step 8	show schedules or show backup schedules Example: umg-1# show schedules	(Optional) Displays all recurring scheduled events or all scheduled backup jobs configured on the local system.
Step 9	show schedule detail job <i>job-name</i> or show backup schedule detail job <i>job-name</i> Example: umg-1# show schedule detail job job-22	(Optional) Displays the details of the specified recurring scheduled event or backup job.

Examples

The following is sample output from the **show backup schedules** command:

```
umg-1# show backup schedules
```

Name	Schedule	Next Run	Description	Categories
A22	NOT SET	NEVER		
backup1000	Every 1 days at 12:34	Jun 25, 2002 12:34		Data
Total: 2				

The following is sample output from the **show schedules** command:

```
umg-1# show schedules
```

Name	Schedule	Next Run	Description	Categories
A22	NOT SET	NEVER		
backup1000	Every 1 days at 12:34	Jun 25, 2002 12:34		Data
Total: 2				

The following is sample output from the **show backup schedule detail job** command:

```
umg-1# show backup schedule detail job job-8
```

Name	job-8
Description	main backup
Categories	Configuration Data
Schedule	Daily at 06:00
Last Run	Jan 1, 2009 at 6:00
Last Result	Success
Next Run	Jan 2, 2009 at 6:00
Active	from Jan 01, 2000 until Dec 31, 2009

The following is sample output from the **show schedule detail job** command:

```
umg-1# show schedule detail job job-8
```

Job Name	job-8
Application	backup
Description	main backup
Schedule	Daily at 06:00
Last Run	5 hours 59 seconds ago
Next Run	in 18 hours 1 seconds
Active	from Jun 25, 2002 until INDEFINITE

Disabling or Reenabling All Scheduled Backups

Beginning in Cisco Unified Messaging Gateway 8.0, you can disable or reenabling all scheduled backups with a single command.

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

SUMMARY STEPS

1. `backup schedule disable all from date to date`
2. `no backup schedule disable all`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>backup schedule disable all from <i>date</i> to <i>date</i></code> Example: <code>umg-1# backup schedule disable all from 07/06/2010 to 07/08/2010</code>	Disables all scheduled backups for a specified period. Dates are entered in MM/DD/YYYY format.
Step 2	<code>no backup schedule disable all</code>	Reenables all the scheduled backups that were disabled with the previous command.



Monitoring the Cisco UMG System

Last updated: December 2, 2010

- [Checking Hard Disk Memory Wear Activity, page 131](#)
- [Checking Log and Trace Files, page 131](#)

Checking Hard Disk Memory Wear Activity

Cisco UMG tracks the use and wear of the hard disk memory as log and trace data are saved to the module. To display this data, use the **show interface ide 0** command in Cisco UMG EXEC mode.

The following is sample output:

```
umg-1# show interface ide 0

IDE hd0 is up, line protocol is up
  218224 reads, 1941088256 bytes
    0 read errors
  2208286 write, 27276906496 bytes
    0 write errors
```

Checking Log and Trace Files

To check the log and trace files on the hard disk, use the **show logs** command in Cisco UMG EXEC mode.

Logging and tracing to the hard disk is turned off by default. Executing the **log trace** command starts the log and trace functions immediately.

The command displays the **atrace.log** and **messages.log** files. Each file has a fixed length of 10 MB, and tracing or logging stops automatically when the file reaches this length. New files overwrite the old files.



Troubleshooting

Last updated: December 2, 2010

- [About Troubleshooting, page 131](#)
- [Running a Network Connectivity Test, page 131](#)
- [Log and Trace Files, page 132](#)
- [Saving Configuration Changes, page 134](#)
- [Using Trace Commands, page 134](#)

About Troubleshooting

Cisco technical support personnel may request that you run one or more of these commands when troubleshooting a problem. Cisco technical support personnel will provide additional information about the commands at that time.



Caution

Some of these commands may impact the performance of your system. We strongly recommend that you do not use these commands unless directed to do so by Cisco Technical Support.

Running a Network Connectivity Test

You can run a network connectivity test to initiate a connection between the Cisco UMG device and all the systems that are configured on the system, including the Cisco Unified Communications Manager, Cisco Unity Connection servers, SRST sites, and SRSV-CUE devices.

The test may take several minutes to complete, during which time the status page will refresh automatically. You can either wait for the test to complete or go to other pages and later return to this page to see the test results.

Procedure

Step 1 Log in to the Cisco UMG GUI.

Step 2 Choose **Troubleshoot > Network Connectivity**.

The system displays the Network Connectivity Test page.

Step 3 To start a network connectivity test, click **Start Network Connectivity Test**.

When the test is complete, the system displays a message stating that the test is complete and shows the results. After you run a network connectivity test, the system displays the results for the following:

- Central call agents
- Central voicemail servers
- Branch voicemail servers
- Branch call agents

For each category, the system shows the hostname of the system to which it tried to connect; the result, either success or failure; the amount of time in milliseconds that it took to connect; and any details.

If the connectivity test fails, the system displays a brief indication of the cause of the failure. You can find additional failure diagnostic information in the trace buffer or message log.

Step 4 To cancel the network connectivity test that is currently running, click **Cancel Network Connectivity Test**.

Step 5 To see the results of the previous test click **Click here for results of previous test**.



Note

Results of the previous test are only available for the current login session. For example, if the administrator logs out and then logs back in later, the previous results will not be available.

Step 6 To restart a previous network connectivity test, click **Restart Network Connectivity Test**.

Log and Trace Files

- [About Logging, page 132](#)
- [Example of Log Output, page 133](#)
- [Log Commands in Cisco UMG Configuration Mode, page 133](#)
- [Log Commands in Cisco UMG EXEC Mode, page 133](#)
- [Saving and Viewing Log Files, page 133](#)

About Logging

Logging and tracing to the hard disk is turned off by default. Executing the **log trace** command starts the log and trace functions immediately.

To check the log and trace files on the hard disk, use the **show logs** command in Cisco UMG EXEC mode. It displays the list of logs available, their size, and their dates of most recent modification.

Each file has a fixed length of 10 MB, and tracing or logging stops automatically when the file reaches this length. New files overwrite the old files.



Note

Logs for E-SRST are turned on by default. Logs for SRSV and VPIM are turned off by default.

Example of Log Output

The following is an example of the log output:

```
umg-1# show logs
SIZE                LAST_MODIFIED_TIME                NAME
1225782    Mon Aug 20 16:55:39 PDT 2007    linux_session.log
4585       Wed Aug 08 14:52:25 PDT 2007    install.log
7883       Mon Aug 20 17:10:00 PDT 2007    dmesg
5000139    Mon Aug 20 13:40:37 PDT 2007    messages.log.prev
9724       Mon Aug 20 17:10:05 PDT 2007    syslog.log
10418      Tue Aug 07 13:39:18 PDT 2007    sshd.log.prev
968        Wed May 09 20:51:34 PDT 2007    dirsnapshot.log
131357     Thu Aug 09 01:28:31 PDT 2007    shutdown.log
51325740   Tue Aug 21 17:56:10 PDT 2007    atrace.log
1534       Mon Aug 20 17:10:04 PDT 2007    debug_server.log
10274      Tue Jul 31 13:32:51 PDT 2007    postgres.log.prev
2398       Mon Aug 20 17:10:04 PDT 2007    sshd.log
104857899  Mon Aug 20 15:13:44 PDT 2007    atrace.log.prev
4119       Mon Aug 20 17:10:22 PDT 2007    postgres.log
4264       Mon Aug 20 17:10:07 PDT 2007    klog.log
984742     Tue Aug 21 18:04:36 PDT 2007    messages.log
55435      Wed Aug 08 14:52:06 PDT 2007    shutdown_installer.log
umg-1#
```

Log Commands in Cisco UMG Configuration Mode

- **log console errors**—Displays error messages (severity=3)
- **log console info**—Displays information messages (severity=6)
- **log console notice**—Displays notices (severity=5)
- **log console warning**—Displays warning messages (severity=4)
- **log server address** *a.b.c.d*

Log Commands in Cisco UMG EXEC Mode

- **log console monitor**
- **log trace boot**
- **log trace buffer save**

Saving and Viewing Log Files

Problem You must be able to save log files to a remote location.

Recommended Action Log files are saved to a disk by default. You can configure Cisco UMG to store the log files on a separate server by using the **log server address** command. Also, you can copy log files on the disk to a separate server if they need to be kept for history purposes, for example:

```
copy log filename.log url ftp://ftp-user-id:ftp-user-passwd@ftp-ip-address/directory
umg# copy log messages.log url ftp://admin:messaging@172.168.0.5/log_history
```

Problem You cannot display the contents of the log files.

Recommended Action Copy the log files from Cisco UMG to an external server and use a text editor, such as **vi**, to display the content.

Saving Configuration Changes

Problem You lost some configuration data.

Recommended Action Copy your changes to the running configuration at frequent intervals. See the [“Copying Configurations” section on page 131](#).

Problem You lost configuration data when you rebooted the system.

Explanation You did not save the data before the reboot.

Recommended Action Issue a **copy running-config startup-config** command to copy your changes from the running configuration to the startup configuration. When Cisco UMG reboots, it reloads the startup configuration.



Note

Messages are considered application data and are saved directly to the disk in the startup configuration. (They should be backed up on another server in case of a power outage or a new installation.) All other configuration changes require an explicit “save configuration” operation to preserve them in the startup configuration.

Using Trace Commands

To troubleshoot network configuration in Cisco UMG, use the **trace** command in EXEC mode. For a detailed list of all the arguments associated with the trace command, see the [Command Reference for Cisco Unified Messaging Gateway Release 8.0](#).

Examples

	Command or Action	Purpose
Step 1	trace dns resolver { all receive send } Example: umg-1# trace dns resolver all	Enables tracing for DNS network functions. <ul style="list-style-type: none"> all—Traces every DNS activity. receive—Traces DNS receiving. send—Traces DNS sending.
Step 2	trace sysdb all Example: umg-1# trace sysdb all	Enables tracing for every sysdb entity and activity.

	Command or Action	Purpose
Step 3	<pre>trace dns all</pre> <p>Example: umg-1# trace dns all</p>	Enables tracing for every DNS event. For example, displays DNS lookups that are performed and results that are given when a domain is verified and resolved using SMTP.
Step 4	<pre>trace dbclient database { garbagecollect largeobject mgmt query results transaction }</pre> <p>Example: umg-1# trace dbclient database results</p>	<p>Enables tracing for client database functions. The following keywords specify the type of traces:</p> <ul style="list-style-type: none"> • garbagecollect—Garbage collection process. • largeobject—Large object reads and writes to the database. • mgmt—Database management processes. • query—Queries performed on the database. • results—Results of queries, inserts, and updates. • transactions—Start and end of database transactions.
Step 5	<pre>trace srsx {gui registration cli controller upload mgmt srsv-engine service-point vm-server-client call-agent-client srsv-secret-syncer site-manager srst-engine }</pre>	<p>Enables tracing for SRSx functions. The following keywords specify the type of traces:</p> <ul style="list-style-type: none"> • gui — SRSx GUI debugging. • registration — SRSx device registration debugging • cli — SRSx CLI debugging • controller — SRSx controller debugging • upload — SRSV voicemail upload debugging • mgmt — SRSx management interface debugging • srsv-engine — SRSV provisioning engine debugging • service-point — SRSx service point debugging • vm-server-client — SRSx central voicemail server communication debugging • call-agent-client — SRSx central call agent server communication debugging • srsv-secret-syncer — SRSx shared secret synchronization debugging • site-manager — SRSx site manager debugging • srst-engine — E-SRST provisioning engine debugging



Maintaining the Cisco UMG System

Last updated: December 2, 2010

- [Copying Configurations, page 131](#)
- [Restoring Factory Default Values, page 134](#)
- [Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online, page 135](#)

Copying Configurations

Use Cisco UMG EXEC commands to copy the startup configuration and running configuration to and from the hard disk on the Cisco UMG module, the network FTP server, and the network TFTP server.



Note

Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

- [Copying the Startup Configuration from the Hard Disk to Another Location, page 131](#)
- [Copying the Startup Configuration from the Network FTP Server to Another Location, page 132](#)
- [Copying the Running Configuration from the Hard Disk to Another Location, page 133](#)
- [Copying the Running Configuration from the Network TFTP Server to Another Location, page 134](#)

Copying the Startup Configuration from the Hard Disk to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the startup configuration on the hard disk to another location:

```
copy startup-config {ftp: user-id:password@ftp-server-url | tftp:tftp-server-url}
```

Syntax Description

ftp: <i>user-id:password@</i>	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-url	URL of the FTP server including directory and filename (e.g. <code>ftp://server/dir/filename</code>)
tftp: <i>tftp-server-url</i>	URL of the TFTP server including directory and filename (e.g. <code>tftp://server/dir/filename</code>)

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following examples illustrate this process.

In this example, the startup configuration is copied to the FTP server, which requires a username and password to transfer files. The startup configuration file is saved on the FTP server with the filename **start**.

```
umg-1# copy startup-config ftp
Address or name of remote host? admin:messaging@ftp://server/dir/start
Source filename? temp_start
```

The following example shows the startup configuration copied to the TFTP server, which does not require a username and password. The startup configuration is saved in the TFTP directory **configs** as filename **temp_start**.

```
umg-1# copy startup-config tftp
Address or name of remote host? tftp://server/dir/temp_start
Source filename? temp_start
```

**Note**

Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Startup Configuration from the Network FTP Server to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the startup configuration on the network FTP server to another location:

```
copy ftp: {running-config | startup-config} user-id:password@ftp://server/dir/filename
```

Syntax Description

running-config	Active configuration on hard disk.
startup-config	Startup configuration on hard disk.
user-id:password@	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-url	URL of the FTP server.

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

Examples

In this example, the FTP server requires a username and password. The file **start** in the FTP server configs directory is copied to the startup configuration.

```
umg-1# copy ftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name or remote host? admin:messaging@ftps://server/configs
Source filename? start
```



Note

Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Running Configuration from the Hard Disk to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the running configuration on the hard disk to another location:

```
copy running-config {ftp: user-id:password@ftps://server/dir/filename |
startup-config | tftp:tftp://server/dir/filename }
```

Syntax Description

ftp: user-id:password@	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-url	URL of the FTP server including directory and filename..
startup-config	Startup configuration on hard disk.
tftp-server-url	URL of the TFTP server including directory and filename.

When you copy the running configuration to the startup configuration, enter the command on one line.

When you copy to the FTP or TFTP server, this command becomes interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

Examples

In the following example, the running configuration is copied to the FTP server, which requires a username and password. The running configuration is copied to the configs directory as file **saved_start**.

```
umg-1# copy running-config ftp:
Address or name of remote host? admin:messaging@ftps://server/configs
Source filename? saved_start
```

In the following example, the running configuration is copied to the startup configuration. In this instance, enter the command on a single line.

```
umg-1# copy running-config startup-config
```

**Note**

Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Running Configuration from the Network TFTP Server to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the running configuration from the network TFTP server to another location:

```
copy tftp: {running-config | startup-config} tftp://server/dir/filename
```

Syntax Description

running-config	Active configuration on hard disk.
startup-config	Startup configuration on hard disk.
<i>tftp-server-url</i>	URL of the TFTP server.

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

Examples

In this example, the file **start** in directory **configs** on the TFTP server is copied to the startup configuration.

```
umg-1# copy tftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? tftp://server/configs
Source filename? start
```

**Note**

Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Restoring Factory Default Values

Cisco UMG provides a command to restore the factory default values for the entire system. Restoring the system to the factory defaults erases the current configuration. This function is available in offline mode. When the system is clean, a message appears indicating that the system will reload, and the system begins to reload. When the reload is complete, the system prompts you to go through the postinstallation process.

**Caution**

This operation is irreversible. All data and configuration files are erased. Use this feature with caution. We recommend that you do a full system backup before proceeding with this feature.

Procedure

Step 1 Enter the following to put the system into offline mode:

```
umg-1# offline
```

Step 2 Enter the following:

```
umg-1 (offline) # restore factory default
```

The system displays a message stating that this will cause all the configuration and data on the system to be erased and this is not reversible, and asks if you want to continue.

Step 3 Do one of the following:

- Enter **n** if you want to retain the system configuration and data.
The operation is cancelled, but the system remains in offline mode. To return to online mode, enter **continue**.
- Enter **y** if you want to erase the system configuration and data.
When the system is clean, a message appears indicating that the system will start to reload. When the reload is complete, a prompt appears to start the postinstallation process.

Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online

You must take the Cisco UMG system offline before you can back up, reload, or restore the system; however, you do not need to take the system offline to shut down the system.

Always shut down Cisco UMG before power-cycling the router to avoid data loss or file corruption.

- [Taking the Cisco UMG System Offline, page 135](#)
- [Restarting the Cisco UMG System, page 136](#)
- [Shutting Down the Cisco UMG System, page 137](#)
- [Putting the Cisco UMG System Back Online, page 137](#)

Taking the Cisco UMG System Offline

Using the **offline** command in Cisco UMG EXEC mode takes the system into offline/administration mode and terminates all directory exchanges and message forwarding. All outstanding messages will be stored for processing when the system goes back online. When you use the **offline** command, the system asks for confirmation. The default is **no**, so to confirm, you must enter **yes**.

Procedure

Step 1 Enter the following command:

```
offline
```

Step 2 Enter **y** to confirm.

Example

```
umg-1# offline
!!!WARNING!!!: If you are going
offline to do a backup, it is
recommended
that you save the current
running configuration using the
'write' command,
prior to going to the offline
state.
Putting the system offline will
terminate all end user sessions.
Are you sure you want to go
offline[n]? :y
umg-1(offline)
```

Restarting the Cisco UMG System

To restart the system using the starting configuration, use the **reload** and **boot disk** commands in Cisco UMG offline/administration mode. Restarting the system will terminate all end-user sessions and cause any unsaved configuration data to be lost.

Procedure

Step 1 Enter the following command:

reload

Step 2 Enter the following:

boot disk

Example

```
umg-1(offline) reload
umg-1(offline)>
MONITOR SHUTDOWN...
EXITED: probe exit status 0
EXITED: SQL_startup.sh exit status 0
EXITED: LDAP_startup.sh exit status 0
[...]
Booting from Secure secondary boot loader..., please wait.

[BOOT-ASM]

Please enter '***' to change boot configuration:
[...]
STARTED: /bin/products/umg/umg_startup.sh

waiting 70 ...
```

```
SYSTEM ONLINE
umg-1#
```

Shutting Down the Cisco UMG System

To halt the system, use the **shutdown** command in Cisco UMG EXEC mode. Shutting down Cisco UMG not only terminates all directory exchange and message forwarding and causes any unsaved configuration data to be lost; it also causes all registered endpoints to go offline.

**Caution**

You must shut down the software before you shut down the hardware.

- [Shutting Down the Software, page 137](#)
- [Shutting Down the Hardware, page 137](#)

Shutting Down the Software

Procedure

Step 1 Enter the following command:

```
shutdown
```

Shutting Down the Hardware

Press the reset button on the network module faceplate for less than two seconds to perform a graceful shutdown of the hard disk before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to two minutes to fully shut down.

**Caution**

If you press the shutdown button for *more than 4 seconds*, an immediate, non-graceful shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After a non-graceful shutdown, the HD and SYS LEDs remain lit. Press the shutdown button for *less than 2 seconds* to gracefully reboot the network module.

Putting the Cisco UMG System Back Online

The **continue** command puts the messaging gateway online again. All endpoints previously marked as offline will be marked as online again.

Procedure

Step 1 Enter the following command:

continue



INDEX

A

AAA [109](#)

- accounting event logging configuration [123](#)
- accounting server configuration [110](#)
- authentication server configuration [112](#)
- console authentication configuration [126](#)
- policy configuration [114](#)

aaa accounting enable command [124](#)

aaa accounting event command [124](#)

aaa accounting server remote command [110](#)

aaa authentication server remote command [112](#)

aaa policy system command [115](#)

accounting event logging [123](#)

accounting server configuration [110](#)

adding the central call agent [54](#)

address command [110](#)

- command
- address [112](#)

authentication-order command [115](#)

authentication server configuration [112](#)

authorization merge-attributes command [115](#)

Avaya Interchange version 5.4 [27](#)

B

backup

- command [132](#)
- FTP server [16, 131](#)
- numbering scheme [134](#)
- parameters [16, 132](#)
- restrictions [132](#)

backup categories command [145](#)

backup category command [134](#)

backup jobs, scheduling [144](#)

backup revisions number command [16](#)

backup schedule command [145](#)

backup schedule disable all command [148](#)

backup server command [16](#)

block location-id command [72, 93](#)

branch call agent information [52](#)

branch voicemail server information [52](#)

broadcast-id command [77, 87](#)

broadcast location command [87](#)

broadcast privilege [117](#)

C

central call agent information [52](#)

Cisco Unity Express [27](#)

Cisco Unity version 4.2 and up [27](#)

clear endpoint command [91](#)

clock timezone command [23](#)

command

- aaa accounting enable [124](#)
- aaa accounting event [124](#)
- aaa accounting server remote [110](#)
- aaa authentication server remote [112](#)
- aaa policy system command [115](#)
- address [110](#)
- authentication-order [115](#)
- authorization merge-attributes [115](#)
- backup [132](#)
- backup categories [145](#)
- backup category [134](#)
- backup revisions number [16](#)

- backup schedule [145](#)
- backup schedule disable all [148](#)
- backup server [16](#)
- block location-id [72, 93](#)
- broadcast-id [77, 87](#)
- broadcast location [87](#)
- clear endpoint [91](#)
- clock timezone [23](#)
- config-commands [124](#)
- continue [134](#)
- copy ftp [132](#)
- copy running-config [133](#)
- copy startup-config [131](#)
- copy tftp [134](#)
- ddr timeout [70](#)
- directory exchange endpoint request [82](#)
- directory exchange messaging-gateway request [82](#)
- disabled (backup-schedule) [145](#)
- domain [77](#)
- enable (endpoint) [75](#)
- endpoint [76, 87](#)
- exec-commands [124](#)
- expiration [72](#)
- hostname [76](#)
- http external [80, 69](#)
- list-manager [84](#)
- list number [84](#)
- list publish [84](#)
- login-fail [124](#)
- logout [124](#)
- log server address [24](#)
- log trace [131, 132](#)
- member [84](#)
- messaging-gateway primary [69](#)
- messaging-gateway registration [69](#)
- messaging-gateway secondary [76, 69](#)
- name [84](#)
- nat location [80, 69](#)
- ndr timeout [70](#)
- network default-route [70](#)
- network location cache refresh id [76](#)
- network messaging-gateway [68](#)
- ntp server [18, 20](#)
- offline [134, 136](#)
- prefix [77](#)
- privilege [84, 121](#)
- registration [72, 93](#)
- reload [136](#)
- repeat daily (backup-schedule) [145](#)
- repeat every (backup-schedule) [145](#)
- repeat monthly (backup-schedule) [145](#)
- repeat once (backup-schedule) [145](#)
- repeat weekly (backup-schedule) [145](#)
- repeat yearly (backup-schedule) [145](#)
- restore id [136](#)
- retries [110, 112](#)
- retry-interval [69](#)
- serial-number [77](#)
- show aaa accounting event [124](#)
- show aaa accounting service [110](#)
- show aaa policy [115](#)
- show backup [16, 133](#)
- show backup history [134, 136](#)
- show backup schedule detail job [145](#)
- show backup schedules [145](#)
- show backup server [134, 136](#)
- show broadcast location [87](#)
- show ddr timeout [70](#)
- show endpoint [87, 91](#)
- show endpoint command [77](#)
- show interface ide 0 [131](#)
- show license status application [51](#)
- show list [84](#)
- show logs [132](#)
- show mailbox [77](#)
- show messaging gateway [89](#)
- show messaging-gateway [68](#)
- show nat location [80](#)

- show ndr timeout [70](#)
- show network default-route [70](#)
- show ntp configuration [18, 20](#)
- show ntp status [18, 20](#)
- show operation detail [121](#)
- show operations [121](#)
- show privilege detail [121](#)
- show privileges command [121](#)
- show registration [72](#)
- show registration block [93](#)
- show schedule detail job [145](#)
- show srsx branch-call-agent [52](#)
- show srsx branch-voicemail-server [52](#)
- show srsx central-call-agent [52](#)
- show srsx provisioning history [52](#)
- show srsx site [51](#)
- show srsx site-template [52](#)
- start-date (backup-schedule) [145](#)
- stop-date (backup-schedule) [145](#)
- system-shutdown [124](#)
- system-startup [124](#)
- telnet [16](#)
- timeout [110, 112](#)
- username [72, 69](#)
- vpim external [80, 69](#)
- command environment [16](#)
- command-line interface (CLI) [29](#)
- commands
 - show schedules [145](#)
- config-commands command [124](#)
- configuration
 - TFTP [134](#)
- configurations, copying [131](#)
- configuring
 - NTP server [18](#)
- configuring CUCME branch call agent [54](#)
- console authentication [126](#)
- continue command [134](#)
- copy ftp command [132](#)

- copying
 - configurations [131](#)
- copying log files, troubleshooting [133](#)
- copy running-config command [133](#)
- copy startup-config command [131](#)
- copy tftp command [134](#)
- CUCME configuration for hunt groups [55](#)

D

- ddr timeout command [70](#)
- directory exchange endpoint request command [82](#)
- directory exchange messaging-gateway request command [82](#)
- disabled (backup-schedule) command [145](#)
- disabling all scheduled backups [147](#)
- DNS server
 - resolving host name to IP address [18](#)
- domain command [77](#)

E

- enable (endpoint) command [75](#)
- enabling endpoints [75](#)
- enabling using the Cisco UMG GUI [56](#)
- endpoint command [76, 87](#)
- endpoints, enabling [75](#)
- E-SRST
 - combined with SRSV on same site [26](#)
 - overview [17](#)
- E-SRST site provisioning [51, 52, 54, 55, 56](#)
- exec-commands command [124](#)
- expiration command [72](#)

F

- failover support [75](#)
- file size
 - messages.log [132](#)

FTP configuration [132](#)

FTP server

 backup and restore [16, 131](#)

G

graphical user interface [30](#)

H

hostname command [76](#)

http external command [80, 69](#)

L

license information [51](#)

list-manager command [84](#)

list number command [84](#)

list publish command [84](#)

log files

 troubleshooting [133](#)

login command

 command

 login [124](#)

login-fail command [124](#)

logout command [124](#)

log server address command [24](#)

log trace command [131, 132](#)

lookup, MX [75](#)

lost data, troubleshooting [134](#)

M

member command [84](#)

messages.log, file size [132](#)

messaging-gateway primary command [69](#)

messaging-gateway registration command [69](#)

messaging gateway-secondary command [69](#)

messaging-gateway secondary command [76](#)

mode

 offline [134](#)

MX lookup [75](#)

N

name command [84](#)

nat location command [80, 69](#)

ndr timeout command [70](#)

network connectivity test [131](#)

network default-route command [70](#)

network location cache refresh id command [76](#)

network messaging-gateway command [68](#)

NME module

 usage [131](#)

 wear [131](#)

NTP server

 removing [20](#)

NTP server, configuring [18](#)

ntp server command [18, 20](#)

numbering scheme, backup files [134](#)

O

offline command [134, 136](#)

offline mode [134, 136](#)

open standards [27](#)

overview [xiii](#)

P

parameters

 backup [16, 132](#)

prefix command [77](#)

preparing the CUCM call agent [52](#)

privilege

 broadcast [117](#)

- superuser [117](#)
- privilege command [84, 121](#)
- privileges
 - configuring [116](#)
 - creating and customizing [121](#)

R

- registration command [72, 93](#)
- reload command [136](#)
- removing an NTP server [20](#)
- repeat daily (backup-schedule) command [145](#)
- repeat every (backup-schedule) command [145](#)
- repeat monthly (backup-schedule) command [145](#)
- repeat once (backup-schedule) command [145](#)
- repeat weekly (backup-schedule) command [145](#)
- repeat yearly (backup-schedule) command [145](#)
- resolving host name to IP address [18](#)
- restore
 - FTP server [16, 131](#)
 - procedure [136](#)
 - restrictions [132](#)
- restore id command [136](#)
- restrictions
 - backup and restore [132](#)
- retries command [110, 112](#)
- retry-interval command [69](#)

S

- saving data, troubleshooting [133](#)
- scheduled backup jobs, configuring [144](#)
- scheduled backups, disabling all [147](#)
- serial-number command [77](#)
- setting the time zone [23](#)
- show aaa accounting service command [110](#)
- show aaa policy command [115](#)
- show accounting event command [124](#)

- show backup command [16, 133](#)
- show backup history command [134, 136](#)
- show backup schedule detail job command [145](#)
- show backup schedules command [145](#)
- show backup server command [134, 136](#)
- show broadcast location [87](#)
- show ddr timeout command [70](#)
- show endpoint command [77, 87, 91](#)
- show interface ide 0 command [131](#)
- show license status application command [51](#)
- show list command [84](#)
- show logs command [132](#)
- show mailbox command [77](#)
- show messaging gateway command [89](#)
- show messaging-gateway command [68](#)
- show nat location [80](#)
- show ndr timeout command [70](#)
- show network default-route command [70](#)
- show ntp configuration command [18, 20](#)
- show ntp status command [18, 20](#)
- show operation detail command [121](#)
- show operations command [121](#)
- show privilege detail command [121](#)
- show privileges command [121](#)
- show registration block [93](#)
- show registration command [72](#)
- show schedule detail job command [145](#)
- show schedules command [145](#)
- show srsx branch-call-agent command [52](#)
- show srsx branch-voicemail-server command [52](#)
- show srsx central-call-agent command [52](#)
- show srsx provisioning history command [52](#)
- show srsx site command [51](#)
- show srsx-site-template command [52](#)
- site information [51](#)
- site provisioning history [52](#)
- site template information [52](#)
- softkeys supported [53](#)
- SRSV

- combined with E-SRST on same site [26](#)
 - limitations [22](#)
 - overview [19](#)
- standards, open [27](#)
- start-date (backup-schedule) command [145](#)
- stop-date (backup-schedule) command [145](#)
- superuser privilege [117](#)
- support, failover [75](#)
- system-shutdown command [124](#)
- system-startup command [124](#)
- vpim external command [80, 69](#)

T

- telnet command [16](#)
- Telnet session [16](#)
- TFTP configuration [134](#)
- timeout command [110, 112](#)
- troubleshooting
 - copying log files [133](#)
 - lost data [134](#)
 - saving data [133](#)

U

- username command [72, 69](#)

V

- verifying
 - branch call agent information [52](#)
 - branch voicemail server information [52](#)
 - central call agent information [52](#)
 - E-SRST and SRSV license information [51](#)
 - site information [51](#)
 - site provisioning history [52](#)
 - site template information [52](#)
- VPIM
 - overview [27](#)