Administration Guide for Cisco Unified Messaging Gateway Release 8.6

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-25441-01

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.

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.

Administration Guide for Cisco Unified Messaging Gateway Release 8.6

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).

CONTENTS

PART 1

Overview and Initial Configuration

Cisco Unified Messaging Gateway Overview

Last updated: August 5, 2011

Cisco Unified Messaging Gateway (Cisco UMG) Release 8.6 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 Cisco UMG Release 8.6 preinstalled.

Cisco UMG Release 8.6 supports the following features:

- Enhanced Survivable Remote Site Telephony (E-SRST), page 1
- Cisco Unified Survivable Remote Site Voicemail (Cisco Unified SRSV), page 3
- Combined Cisco Unified SRSV and E-SRST on the Same Site, page 9
- Voice Profile for Internet Mail (VPIM) Networking, page 11

Enhanced Survivable Remote Site Telephony (E-SRST)

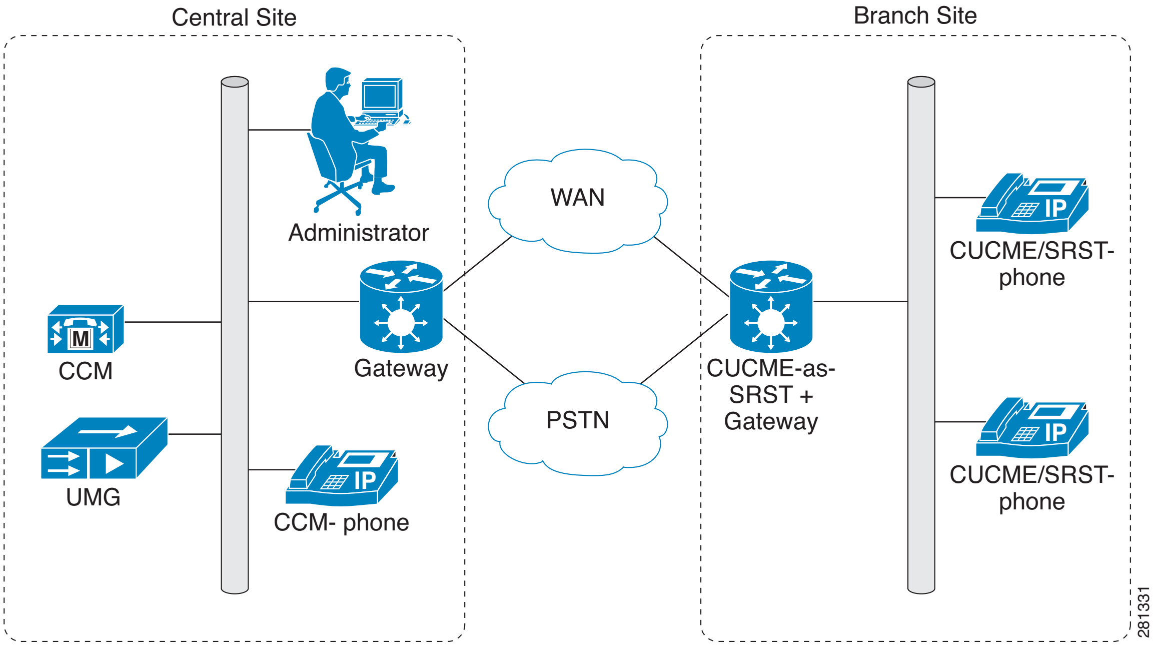
The Enhanced Survivable Remote Site Telephony (E-SRST) feature is supported in Cisco UMG Release 8.5 and later versions. The E-SRST feature requires that you install E-SRST licenses, with each license supporting up to 25 sites per license. The E-SRST feature can be deployed separately or combined on a given site with Cisco Unified Survivable Remote Site Voicemail (Cisco Unified SRSV). See the "Combined Cisco Unified SRSV and E-SRST on the Same Site" section on page 9.

The E-SRST feature provides an integrated solution that supports advanced Cisco Unified Communications Manager Express-as-Cisco Unified Survivable Remote Site Telephony (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 the E-SRST feature, the Cisco UMG system at the central site collects information from Cisco Unified Communications Manager, 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 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 site Cisco UMG system to provide enhanced Cisco Unified SRST services at the branch sites.

Figure 1 shows the supported topology model for E-SRST on a branch site. In this example, Cisco Unified SRSV is not deployed at the branch site.

Figure 1 E-SRST Only (No Cisco Unified SRSV) Topology



The E-SRST feature provides automated remote site provisioning of the following advanced telephony features in survivable mode by gathering the information from Cisco Unified Communications Manager:

- End-user phone numbers 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
- Directory numbers

The E-SRST feature allows you to set up provisioning schedules for defining when and how often to fetch configuration information from Cisco Unified Communications Manager and provision the branch site CUCME-as-SRST routers. You can also do an on-demand provisioning to synchronize a specific CUCME-as-SRST router with the Cisco Unified Communications Manager information.

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

For more information about Cisco Unified Communications Manager Express, see the documentation at: http://www.cisco.com/en/US/partner/products/sw/voicesw/ps4625/tsd_products_support_series_home.html.

E-SRST Limitations

- Provisioning advanced E-SRST features on an original Cisco Unified SRST gateway at the branch site is not supported. In this scenario, the central E-SRST gateway does not replace the original Cisco Unified SRST with CUCME-as-SRST.
- The E-SRST feature does not support a Cisco Unity-only or Cisco Unity Express-only messaging network. (The E-SRST feature only supports SRSV-CUE at the branch site with Cisco Unity Connection at the central site.)
- The E-SRST feature requires Cisco Unified Communications Manager Express Release 7.1 and later.
- The E-SRST feature does not support secure Cisco Unified SRST.
- The E-SRST feature does not actually configure or create dial peers and translation rules. The dial peers and translation rules must be manually configured on the branch site.
- Extension mobility on Cisco Unified Communications Manager is not supported.

Cisco Unified Survivable Remote Site Voicemail (Cisco Unified SRSV)

Introduction to Cisco Unified SRSV

Cisco Unified SRSV is supported in Cisco UMG Release 8.0 and later. The Cisco Unified SRSV feature requires that you install Cisco Unified SRSV licenses, with each license supporting up to 25 nodes per license. The Cisco Unified SRSV feature can be deployed separately on a given site or combined with E-SRST.

The Cisco Unified SRSV solution requires the following two components:

- Cisco Unified Messaging Gateway-Survivable Remote Site Voicemail (commonly referred to as Cisco UMG)

  The Cisco UMG component is deployed at the central site alongside Cisco Unified Communications Manager and Cisco Unity Connection. The SRSV-UMG component is deployed using Cisco UMG software with Cisco Unified SRSV licenses installed. For product versions compatible with Cisco UMG, see the *Release Notes for Cisco Unified Messaging Gateway Release 8.6*.
- Cisco Unified Survivable Remote Site Voicemail-Cisco Unity Express (SRSV-CUE)

  The SRSV-CUE component is deployed at the branch site alongside Cisco Unified Communications Manager Express or Cisco Unified SRST. SRSV-CUE is a separate orderable product, and has different hardware and software requirements. For more information, see the *Release Notes for Cisco Unified Messaging Gateway Release 8.6*.

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 Cisco Unified SRSV solution does not support interoperability with Cisco Unity Express.

The standalone Cisco Unified SRSV solution introduced in Cisco UMG Release 8.0 uses either original Cisco Unified SRST or CUCME-as-SRST. Original Cisco Unified SRST requires simple, very limited provisioning on the branch site gateway, but provides very limited features to support basic phone calls. CUCME-as-SRST, also known as Cisco Unified SRST Fallback Mode, provides advanced telephony features such as hunt groups and pick-up groups that are not available with original Cisco Unified SRST, but it requires more complex and manual provisioning on the branch site gateways. 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 E-SRST feature introduced in Cisco UMG Release 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 1.

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

When the WAN connection returns, the IP phones automatically re-home to the central site Cisco Unified Communications Manager. Call handling is then managed by Cisco Unified Communications Manager, and no-answer and busy calls are forwarded to the central site Cisco Unity Connection voicemail system.

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

Supported Cisco Unified SRSV Topologies

Several Cisco Unified SRSV topologies are supported beginning with Cisco UMG Release 8.0. Depending on the configuration, you can have either original Cisco Unified SRST or CUCME-as-SRST (also known as Cisco Unified SRST Fallback Mode) deployed at the branch site. Note that if you are running Cisco Unified 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 Cisco Unified 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 Cisco Unified SRSV Topology Using Cisco Unified SRST at the Branch Site

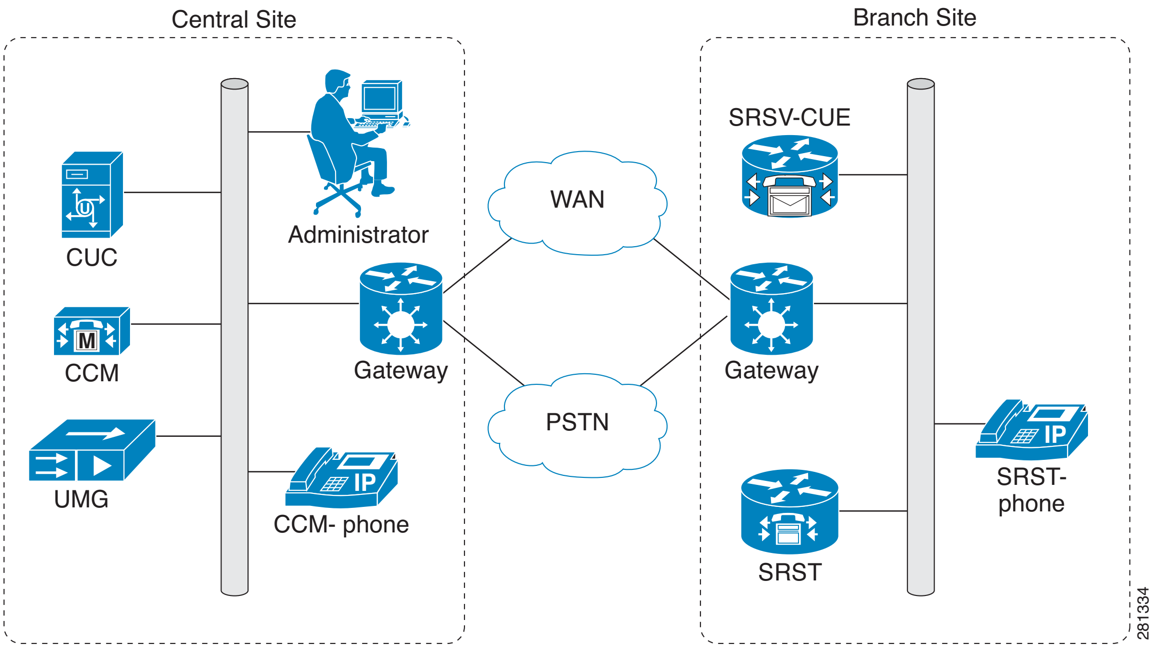


Figure 3 shows a topology where CUCME-as-SRST (also known as Cisco Unified SRST Fallback Mode) is providing call control at the branch site.

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

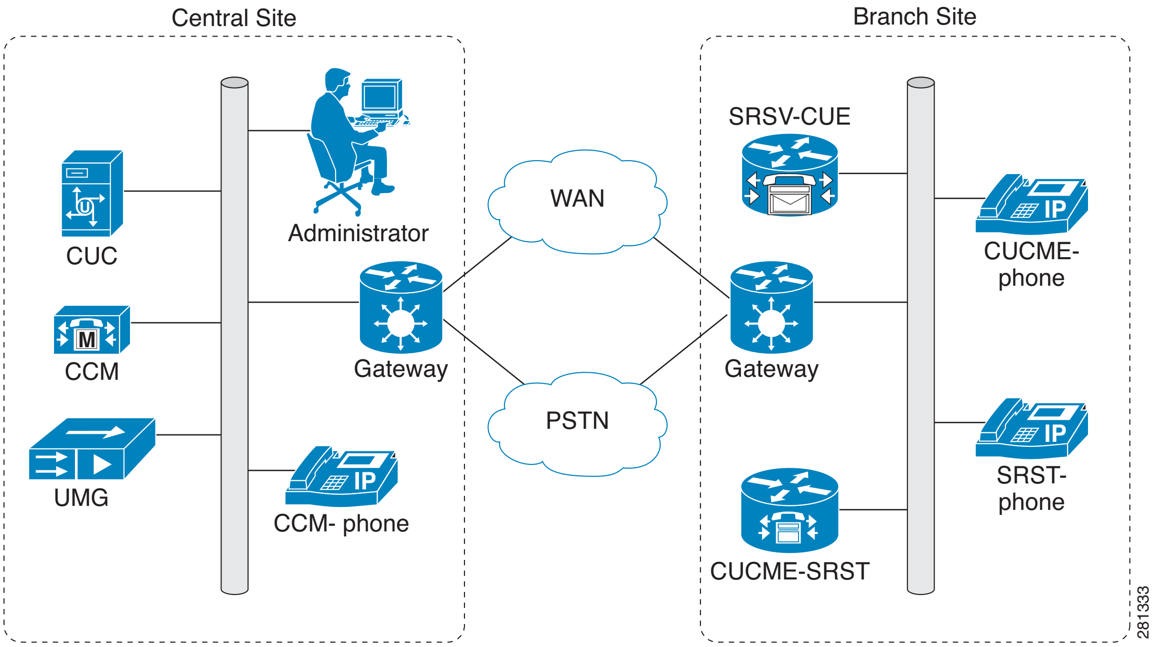
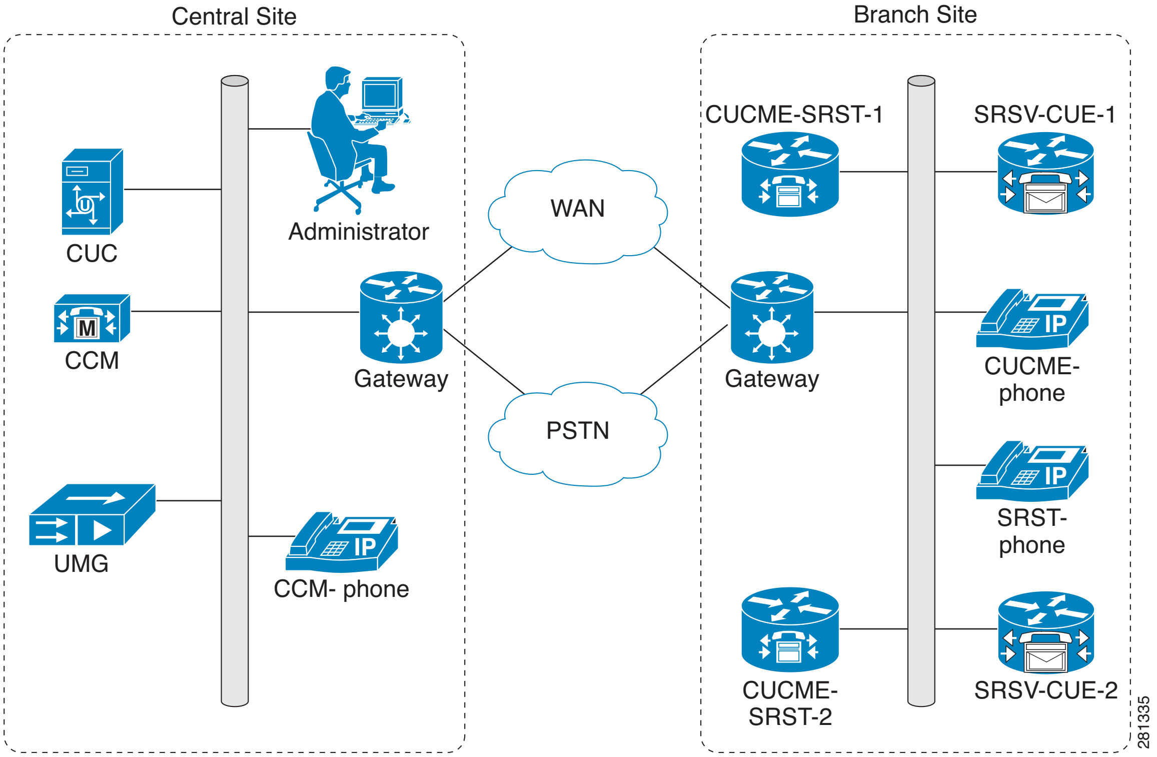


Figure 4 shows a topology where multiple CUCME-as-SRST and SRSV-CUE devices are paired for load balancing at the survivable branch site. In this scenario, the administrator uses Cisco Unified Communications Manager to divide the branch users between CUCME-SRST-1 and CUCME-SRST-2.

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 Cisco Unified SRSV Topology with Multiple CUCME-as-SRST Devices Load Balanced at Remote Site



Cisco Unified SRSV Limitations

- Limitations for Interoperating with Cisco Unified Communications Manager, page 6
- Voicemail Limitations and Restrictions, page 7
- Auto Attendant Limitations, page 7
- Network Address Translation (NAT) Restrictions, page 8
- Voicemail Backup and Restore Limitations, page 8
- Mailbox Limitations, page 8
- Live Record and Live Reply Limitations, page 9
- Distribution Lists, page 9

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 UMG Release 8.6 and later when using Cisco Unified SRSV:
  - Fax support
  - Addressing non-subscribers
  - Dispatch messages
  - 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 SRSV-CUE device.
- The Message Waiting Indicator (MWI) for an 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 Cisco Unified Communications Manager.
- 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 SRSV-CUE users (such as live reply, distribution list access, and message deletion behavior).
- Composed messages are not delivered immediately to branch voicemail servers in Cisco Unified SRSV mode. They are delivered after the WAN recovers.
- Subscribers cannot log in to SRSV-CUE devices until they set up their voicemail preferences on Cisco Unity Connection.
- SRSV-CUE devices only support PINs in the SHA1 format. If you are upgrading to Cisco Unified SRSV 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:
  - Selected Cisco Unity Connection call handler for branch auto attendant and all of its descendants
  - Local user only lookup
  - Standard greetings
  - Standard transfer options
- There is no support for the following auto attendant features:

  - 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 SRSV-CUE auto attendant greeting is the same as the greeting of the system call handler on Cisco Unity Connection selected for the branch site.
- Because the auto attendant greeting on 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 SRSV-CUE has fewer features.
- Through the SRSV-CUE auto attendant feature, subscribers can be reached using the directory service.
- Directory service on 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 SRSV-CUE device can be provisioned at each NAT site.
- Only static NAT and PAT are supported. Dynamic NAT is not supported.

Voicemail Backup and Restore Limitations

- Transport Layer Security (TLS) certificates and private keys are not backed up on SRSV-CUE devices. After restoring a backup, you must import the security certificates again.
- To avoid creating duplicate email messages, backing up data on 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 SRSV-CUE devices do not support all the characters that are supported on Cisco Unity Connection. 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 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.

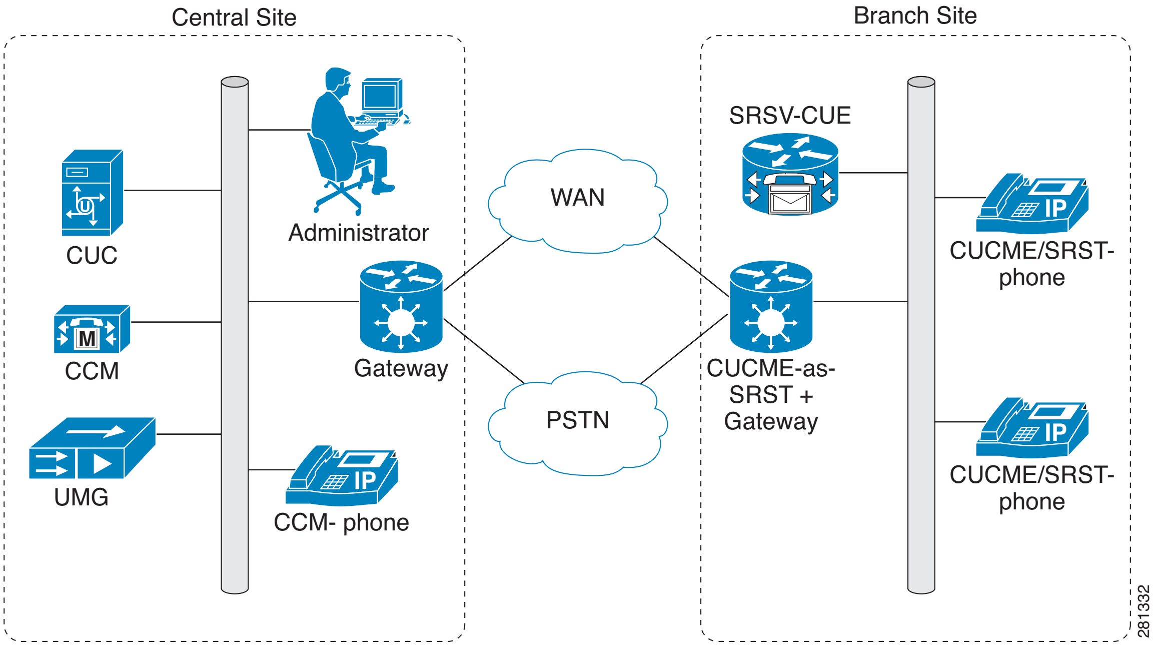
Combined Cisco Unified SRSV and E-SRST on the Same Site

Cisco UMG Release 8.5 and later supports enabling both Cisco Unified SRSV and E-SRST provisioning on the same site in certain cases. In the supported model, CUCME-as-SRST is configured on the branch site along with a SRSV-CUE device. A central call agent (Cisco Unified Communications Manager) and voicemail system (Cisco Unity Connection) 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 Cisco Unified Communications Manager and Cisco Unity Connection for changes, additions, and deletions that must be pushed to the remote branch SRSV-CUE and CUCME-as-SRST sites.

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

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

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



E-SRST and Cisco Unified SRSV Licenses and When to Deploy Them

Feature licenses for E-SRST, Cisco Unified SRSV, and VPIM are available in increments of 25 sites or nodes each. For example, if you are deploying 25 Cisco Unified SRSV sites, you must purchase one Cisco Unified SRSV feature license. If you are deploying 30 Cisco Unified SRSV sites, you must purchase two Cisco Unified SRSV feature licenses. For more information about feature licenses, see the *Release Notes for Cisco Unified Messaging Gateway Release 8.6*.

The E-SRST and Cisco Unified SRSV features can be deployed separately or together on a given site. You can configure a site for either feature or for both features 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:

- Cisco Unified SRST, also referred to as “original” Cisco Unified SRST.
- CUCME-as-SRST. This is also known as the Cisco Unified SRST Fallback Mode feature on Cisco Unified Communications Manager Express.

E-SRST is not required if you are using original Cisco Unified SRST and are not provisioning advanced telephony features for use in survivable mode. However, we recommend using E-SRST if you will be using advanced telephony features. For example, E-SRST is recommended if you plan to use advanced Cisco Unified Communications Manager telephony features in survivable mode.

Table 1 summarizes the different options for enabling E-SRST and/or Cisco Unified SRSV on a given site.

Table 1 Cisco UMG Release 8.6 Features and Call Control Options on a Branch Site

Features enabled on a branch site[1]	Call control method	Provisioning of advanced telephony features	Survivable Remote Site Voicemail supported on the branch site[2]	For a sample topology, see:
E-SRST only	CUCME-as-SRST	Provisioned on central Cisco Unified Communications Manager, automatically downloaded to the branch site.	No	Figure 1
Cisco Unified SRSV only	Cisco Unified SRST	Not applicable[3]	Yes	Figure 2
Cisco Unified SRSV only	CUCME-as-SRST	Manually provisioned on the branch site.	Yes	Figure 3
E-SRST and Cisco Unified SRSV	CUCME-as-SRST	Provisioned on central Cisco Unified Communications Manager, automatically downloaded to the branch site.	Yes	Figure 5

[1] A feature license must be installed on a per-site basis for provisioning to take place.

[2] Requires that you install SRSV-CUE software on the branch voicemail server.

[3] Original Cisco Unified SRST does not support advanced telephony features.

Voice Profile for Internet Mail (VPIM) Networking

Voice Profile for Internet Mail (VPIM) networking has not changed in this release. For information about VPIM-specific features, see earlier versions of the Cisco UMG documentation located at http://www.cisco.com/en/US/products/ps8605/tsd_products_support_series_home.html.

Cisco Unified Messaging Gateway Administration Interfaces

Last updated: August 5, 2011

Cisco UMG Release 8.6 utilizes both a command-line interface (CLI) and a graphical user interface (GUI).

- Command-Line Interface, page 13
- Graphical User Interface, page 13

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 How to Use the Cisco UMG CLI 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 Cisco Unified SRSV features require the GUI 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 Cisco Unified 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 Cisco Unified SRSV or E-SRST, and for routing maintenance operations, see About the Cisco Unified Messaging Gateway GUI.

Note You can configure the E-SRST and Cisco Unified 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 Cisco Unified 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.

About the Cisco Unified Messaging Gateway GUI

Last updated: August 5, 2011

Caution The Cisco UMG system functionality is not the same as other similar systems, such as Cisco Unity Express and Cisco Unity Connection. For example, the auto attendant and voicemail functions work differently. For more information about system limitations and caveats, see the *Release Notes for Cisco Unified Messaging Gateway Release 8.6*.

Tip When you use Cisco UMG GUI, you can use the Back and Forward buttons on your browser to view information in another window, but if you make changes in that window and submit your changes, you will receive an error and your changes will **not** be saved. **Do not submit information after using your browser's navigation tools to move to another window**. Click the appropriate button or menu to reach the window in which you want to enter information.

About the Cisco UMG Dashboard

You should periodically monitor the status of the system to ensure that the deployment remains ready for failover events. You can monitor the system from the Cisco UMG dashboard.

The Cisco UMG dashboard provides an at-a-glance view of the state of the system. The dashboard contains a summary of items that would typically require the attention of the administrator, such as error and warning messages. When the system is functioning normally, with no alerts or activity, the dashboard shows minimal information.

You can return to the dashboard from anywhere in the system by clicking **Dashboard** on the top right.

The dashboard is comprised of three areas:

- **Provisioning Status:** Displays a summary of the results of the most recent provisioning cycle. If all sites have been successfully provisioned, a single success message is displayed. If any sites are disabled, have failed provisioning, or have never been provisioned, the provisioning status panes displays a site count for each provisioning outcome respectively. For provisioning failures, the system generates a system alert message for each site that indicates the reason for the failure. To review site specific results by status, click the corresponding report link.
- **Activity Log:** Displays a summary of recent site activity. Each voicemail upload process is counted on the dashboard, and recorded in the SRSV Activity History report, which is described in Viewing the SRSV Activity History Report. To clear the activity log, click **Clear Activity Log**. This also clears the information from the SRSV Activity History report.

- **System Alerts:** Displays the number of critical, warning, error, and informational alert messages that require attention. To review system alert details by level, click the corresponding link. See System Alerts for more description of the alerts.

Overview of Configuration Tasks

Last updated: August 5, 2011

The following is a high-level overview of the tasks required before you can use the Cisco Unified Messaging Gateway (Cisco UMG) GUI to configure the following features:

- Cisco Unified SRSV. The Cisco Unified Messaging Gateway solution requires an SRSV-CUE device to be configured at the branch site.
- Enhanced Survivable Remote Site Telephony (E-SRST)

Task	Applies to the following features	Where to find more information
Before You Begin		
Install Cisco Unified Communications Manager, including security certificates at the central office.	SRSV E-SRST	Installation guide for your release of Cisco Unified Communications Manager. See 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.	SRSV E-SRST	Installation guide for your release of Cisco Unity Connection. See http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html
Enable SMTP support on the Cisco Unity Connection.	SRSV E-SRST	How to Enable SMTP Support for Cisco UMG on Cisco Unity Connection
Install a Cisco Unified SRST system at the branch office, including security certificates. The supported options are: • Sites using E-SRST require CUCME-as-SRST. • Sites using SRSV only can use either CUCME-as-SRST or original SRST.	SRSV E-SRST	For original SRST, see http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srstsa.html For CUCME-as-SRST, also known as Cisco Unified SRST Fallback Mode, see http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmesrst.html

Task	Applies to the following features	Where to find more information
Install Cisco UMG Release 8.6, including SRSV-CUE devices.	SRSV E-SRST	*Installation and Upgrade Guide for Cisco Unified Messaging Gateway Release 8.6*
Log into the Cisco UMG system.	SRSV E-SRST	Logging In to the Cisco UMG Graphical User Interface (GUI)
Global Configuration		
Configure global settings for the Cisco UMG system, including importing security certificates.	SRSV E-SRST	• Using the Setup Wizard • Configuring Backup and Restore • Working With Network Time and Time Zone Settings • Configuring Users • Setting User Defaults • Configuring Groups • Configuring Privileges • Configuring Authentication, Authorization, and Accounting
Configuring Central Call Agents and Voicemail Servers		
Configure a central voicemail server, such as Cisco Unity Connection, on the Cisco UMG system.	SRSV	Using the Central Voicemail Server Wizard to Add Cisco Unity Connection Information
Configure a central call agent, such as Cisco Unified Communications Manager, on the Cisco UMG system.	SRSV E-SRST	Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information
Configure advanced telephony features on Cisco Unified Communications Manager such as softkeys, hunt groups, call routing restrictions, and call pickups. When a branch site is selected to enable E-SRST provisioning using the Cisco UMG GUI, the configuration for these advanced telephony features are downloaded to the branch site.	E-SRST	See the Cisco Unified Communications Manager. See http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Configure an auto attendant for Cisco Unified Messaging Gateway.	SRSV E-SRST	• Get call handlers. SeeViewing the Call Handlers Associated With a Central Voicemail Server. • Select a call handler for a site in the Root Call Handler field on the Sites page. See Viewing and Provisioning Sites.

Task	Applies to the following features	Where to find more information
Import the TLS certificates.	SRSV E-SRST	Working With Trusted TLS Certificates
Provisioning Tasks		
Configure a backup central call agent for provisioning.	SRSV E-SRST	- Configure the secondary node field on the CUCM Profile page. See Viewing and Updating the Central Call Agent. - Configure additional clusters. See Viewing the Cluster Nodes Associated With a Central Voicemail Server.
Configure a backup central voicemail server for provisioning.	SRSV E-SRST	- Configure the secondary node field on the CUC Profile page. See Viewing and Updating a Central Voicemail Server. - Configure additional clusters. See Viewing the Cluster Nodes Associated With a Central Call Agent.
Configure a backup Cisco UMG. **Note** The software version for the secondary Cisco UMG must be the same as the software version of the primary Cisco UMG. This process only synchronizes passwords, the Cisco Unity Connection configuration, and trusted TLS certificates.	SRSV E-SRST	Supporting High Availability
Provision sites.	SRSV E-SRST	Viewing and Provisioning Sites
Monitor provisioning and understand the error messages associated with provisioning failure.	SRSV E-SRST	- Monitoring the Provisioning Status of a Branch Device - System Alerts
Configuring Branch Sites		
Register an SRSV-CUE device.	SRSV	Using the Add Branch Voicemail Server Wizard to Add an SRSV-CUE Device
Upgrade the software of an SRSV-CUE device.	SRSV	- Managing the Branch Voicemail Server Software - Viewing and Removing Branch Voicemail Servers
(Optional) Create and configure site templates for the Cisco UMG system.	SRSV E-SRST	Using Site Templates

Task	Applies to the following features	Where to find more information
Import Cisco Unified SRST sites by retrieving Cisco Unified SRST references from Cisco Unified Communications Manager.	SRSV E-SRST	Viewing the Cisco Unified SRST References
Configure sites, if needed.	SRSV E-SRST	Changing the Information for Cisco Unified SRST Sites
Enable support for Cisco Unified Messaging Gateway provisioning and E-SRST provisioning for one or more sites.	SRSV E-SRST	• Changing the Information for a Single Cisco Unified SRST Site • Changing the Information for Multiple Cisco Unified SRST Sites at Once
Assign branch voicemail servers to a site.	SRSV	Configuring Unassigned Branch Voicemail Servers
Changes as Needed		
View, edit, or remove a central voicemail server.	SRSV	• Viewing and Removing Central Voicemail Servers • Viewing and Updating a Central Voicemail Server • Viewing the Cluster Nodes Associated With a Central Voicemail Server • Viewing the Call Handlers Associated With a Central Voicemail Server
View, edit, or remove the central call agent.	SRSV	• Viewing and Removing the Central Call Agent • Viewing and Updating the Central Call Agent • Viewing the Cisco Unified SRST References • Viewing the Cluster Nodes Associated With a Central Call Agent
Add, edit, or remove a branch voicemail server.	SRSV	• Viewing and Removing Branch Voicemail Servers • Viewing and Updating a Branch Voicemail Server
Upgrade the branch voicemail server software.	SRSV	Managing the Branch Voicemail Server Software
Update the domain name settings.	SRSV E-SRST	Working With DNS Servers
Change the login banner.	SRSV E-SRST	Configuring the System Login Banner

Task	Applies to the following features	Where to find more information
Monitoring		
Monitor the status of the Cisco UMG system.	SRSV E-SRST	- About the Cisco UMG Dashboard - Monitoring the Learned Cisco Unified Communications Manager Express Routers - Monitoring the Provisioning Status of a Branch Device - Monitoring the Voicemail Upload - Monitoring the System - Viewing Reports
Maintenance		
Periodically back up the Cisco UMG system. Restore it as needed.	SRSV E-SRST	Configuring Backup and Restore
Review the licenses.	SRSV E-SRST	Displaying Cisco UMG License Information
Troubleshooting		
Troubleshoot the Cisco UMG system as necessary.	SRSV E-SRST	- Troubleshooting Using the GUI - Troubleshooting Using the CLI - Also see the DocWiki at http://docwiki.cisco.com/wiki/Cisco_Unified_Survivable_Remote_Site_Voicemail_--_Troubleshooting.

Logging In to the Cisco UMG Graphical User Interface (GUI)

Last updated: August 5, 2011

Restrictions

The Cisco UMG GUI only supports the following web browsers:

- Internet Explorer Releases 6, 7, and 8
- Mozilla Firefox Release 3

Before You Begin

- Install the Cisco UMG software. See the *Installation and Upgrade Guide for Cisco Unified Messaging Gateway Release 8.6* for information.
- Gather the administrator username and password that you entered during the installation.

Procedure

Step 1 Open a web browser.

Step 2 Enter the IP address of the Cisco UMG system.

The system displays the log-in screen.

Step 3 Enter the administrator name.

Step 4 Enter the administrator password.

Step 5 Click **Log In**.

The system displays the Cisco UMG dashboard within the Cisco UMG GUI.

About the Cisco UMG Dashboard

You should periodically monitor the status of the system to ensure that the deployment remains ready for failover events. You can monitor the system from the Cisco UMG dashboard.

The Cisco UMG dashboard provides an at-a-glance view of the state of the system. The dashboard contains a summary of items that would typically require the attention of the administrator, such as error and warning messages. When the system is functioning normally, with no alerts or activity, the dashboard shows minimal information.

You can return to the dashboard from anywhere in the system by clicking **Dashboard** on the top right.

The dashboard is comprised of three areas:

- **Provisioning Status:** Displays a summary of the results of the most recent provisioning cycle. If all sites have been successfully provisioned, a single success message is displayed. If any sites are disabled, have failed provisioning, or have never been provisioned, the provisioning status panes displays a site count for each provisioning outcome respectively. For provisioning failures, the system generates a system alert message for each site that indicates the reason for the failure. To review site specific results by status, click the corresponding report link.
- **Activity Log:** Displays a summary of recent site activity. Each voicemail upload process is counted on the dashboard, and recorded in the SRSV Activity History report, which is described in Viewing the SRSV Activity History Report. To clear the activity log, click **Clear Activity Log**. This also clears the information from the SRSV Activity History report.
- **System Alerts:** Displays the number of critical, warning, error, and informational alert messages that require attention. To review system alert details by level, click the corresponding link. See System Alerts for more description of the alerts.

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

Last updated: August 5, 2011

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*

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 Cisco Unified Communications Manager:

- 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 Cisco Unified Communications Manager central call agent, and on the CUCME-as-SRST call agent at the branch site. Most of the configuration on Cisco UMG is handled using the GUI.

This procedure assumes that the security certificates have been installed on the Cisco UMG. For more information, see About Security for Cisco UMG.

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 Cisco Unified Communications Manager to the remote site.

- Initial Configuration Using the Cisco UMG GUI, page 28
- Preparing the Central Cisco Unified Communications Manager Call Agent for E-SRST Provisioning, page 28
- Configuring the Cisco Unified Communications Manager Express Branch Call Agent to Prepare for E-SRST Provisioning, page 30
- Enabling E-SRST Provisioning on the Site Using the Cisco UMG GUI, page 31
- Verifying the Updated Configuration on the Branch Call Agent Router, page 31

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.
2. Add central 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.
3. Import the Cisco Unified SRST sites. For more information, see Viewing the Cisco Unified SRST References.

Preparing the Central Cisco Unified Communications Manager Call Agent for E-SRST Provisioning

This section assumes that the advanced telephony features have already been configured on Cisco Unified Communications Manager. For more information, see the Cisco Unified Communications Manager documentation at
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

To configure Cisco Unified Communications Manager to prepare for E-SRST provisioning, perform the following steps on Cisco Unified Communications Manager.

Procedure

Step 1 Configure the Cisco Unified SRST references on Cisco Unified Communications Manager with the following:

- site name
- port number for CUCME-as-SRST
- IP address of the router

Step 2 Create a device pool in Cisco Unified Communications Manager that has the SRST reference. Gather the following information:

- device pool name
- Cisco Unified SRST reference, which 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 Cisco Unified Communications Manager that will be downloaded to the branch site using E-SRST provisioning.

Cisco UMG Release 8.6 supports selected Cisco Unified Communications Manager 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 Cisco Unified Communications Manager Advanced Telephony Features Supported in Cisco UMG Release 8.6

Cisco Unified Communications Manager Advanced Telephony Configuration	Instructions for Preparing Cisco Unified Communications Manager Feature for E-SRST Site Provisioning
Call list and assigned call list to the ephone domain name	• 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	1. Select the Hunt Pilot setting. 2. Select **Hunt Pilot**. The route partition must be set to **internal**. 3. Select **Hunt List**. 4. 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	Cbarge, Newcall
Ringing	Answer, Dnd, Hlog
Seized	CallBack, Cfwdall, Endcall, Gpickup, Hlog, Pickup, Redial

Configuring the Cisco Unified Communications Manager Express Branch Call Agent to Prepare for E-SRST Provisioning

The E-SRST solution requires that Cisco Unified Communications Manager Express be configured in CUCME-as-SRST mode, also known as Cisco Unified SRST fallback mode. For more information, see the *Cisco Unified Communications Manager Express Administrator Guide*.

The Cisco Unified Communications Manager Express site must also be configured with additional CLI commands to ensure that the Cisco Unified Communications Manager Express site can contact the Cisco UMG so that the Cisco Unified Communications Manager configuration can successfully be pulled through the Cisco UMG device to the branch site.

Perform the following steps in Cisco Unified Communications Manager Express.

Procedure

Step 1 Configure the IP address for the interface on the branch router that connects back to the Cisco 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 Cisco 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 Cisco Unified Communications Manager 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

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 Cisco Unified Communications Manager telephony configuration during the provisioning process. You can either perform on-demand site provisioning for the site, or configure Cisco UMG to perform scheduled provisioning on the site.

For information, see Viewing and Provisioning Sites.

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 call agent 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.

Using the Setup Wizard

Last updated: August 5, 2011

Use the Setup Wizard to set initial values for the Cisco UMG system.

Before You Begin

Gather the following information before you run the Setup Wizard:

Table 3 System Setup Parameters

Parameter	Description
Feature Selection	
SRSV Provisioning	Determines whether the system can perform Cisco Unified SRSV provisioning. If you select Yes, you must also enter information for the following: • UMG REST Password • SRSV-CUE REST Password • Auto-Learn Voicemail Pilot and Pilot Number • TLS Security • Hostname or IP Address of Secondary UMG
eSRST Provisioning	Determines whether the system can perform E-SRST provisioning. If you select Yes, you must also enter information for the following: • Auto-Learn Voicemail Pilot and Pilot Number • TLS Security

Table 3 System Setup Parameters (continued)

Parameter	Description
UMG REST Interface	
UMG REST Password	Password that the system assigns to the Cisco UMG REST interface. The system automatically shares this password with the SRSV-CUE device to provide authenticated communications from the SRSV-CUE device to the Cisco UMG device during provisioning and voicemail uploads. By default, the password is initialized to "umg-rest-secret." This value is required and may not be left blank. We recommend that you change this value to provide increased system security. The Cisco UMG REST password is used only if Cisco Unified SRSV is enabled on the site.
SRSV-CUE REST Interface	
SRSV-CUE REST Password	Password that the system will assign to the SRSV-CUE REST interface. The system automatically shares this password with the SRSV-CUE device to provide authenticated communications from the Cisco UMG device to the SRSV-CUE device during provisioning and voicemail uploads. By default, the password is initialized to "srsv-rest-secret." This value is required and may not be left blank. We recommend that you change this value to provide increased system security. The SRSV-CUE REST password is used only if Cisco Unified SRSV is enabled for the site.
Voicemail Pilot	
Auto-Learn Voicemail Pilot	Determines whether the system should auto-learn the voicemail pilot number.
Pilot Number	The voicemail pilot number for the branch office call agent. The system saves this number to the default site template. If E-SRST provisioning is enabled, the voicemail pilot number is automatically learned from the central call agent during the provisioning process. The voicemail pilot number must be entered in the following situations: • If Cisco Unified SRSV provisioning is enabled only • If E-SRST provisioning is enabled, but you want to override the automatically learned pilot number

Table 3 System Setup Parameters (continued)

Parameter	Description
TLS Security	
TLS Security	Enables security between the Cisco UMG and SRSV-CUE devices at the branch. If TLS security is set to On, Cisco UMG uses a secure HTTPS connection for provisioning the device. If TLS security is set to Off, Cisco UMG uses a non-secure Telnet connection for provisioning the device.
High Availability	
Hostname or IP Address of Secondary UMG	Hostname of the secondary Cisco UMG device, used for high availability deployments. Entering a value here enables the high availability feature. See Supporting High Availability. You can enter either a hostname or IP address. If you enter an IP address, the system performs a DNS reverse look-up to store the secondary Cisco UMG device by its hostname.

Procedure

Step 1 Select **Setup Wizards > Setup**.

The system displays the Introduction page of the setup wizard.

Step 2 Click **Next**.

The system displays the Feature Selection page of the setup wizard.

Step 3 Select the features that will be enabled on the Cisco UMG system. You must select at least one feature to continue.

- Select **Yes** for SRSV Provisioning
- Select **Yes** for eSRST Provisioning

Note These settings apply to the Cisco UMG setup wizard only. Depending on the features enabled, the setup wizard will only take you through the required steps.

Step 4 Click **Next**.

- If you selected SRSV Provisioning, the system displays the Cisco UMG REST Interface page of the setup wizard. Proceed to Step 5.
- If you did not select SRSV Provisioning (you only selected E-SRST Provisioning), click **Next**. The system displays the Voicemail Pilot page of the setup wizard. Proceed to Step 9.

Step 5 On the Cisco UMG REST Interface page, enter the following information:

- UMG REST Password
- Confirm the UMG REST Password

Step 6 Click **Next**.

The system displays the SRSV-CUE REST Interface page of the setup wizard.

Step 7 On the SRSV-CUE REST Interface page, enter the following information:

- SRSV-CUE REST Password
- Confirm the SRSV-CUE REST Password

Step 8 Click **Next**.

The system displays the Voicemail Pilot page of the setup wizard.

Step 9 Choose one of the following:

- If you only selected SRSV Provisioning, enter the Voicemail Pilot number.
- If you selected E-SRST Provisioning, the system automatically learns the Voicemail Pilot number from the central call agent.
- To override the auto-learned voicemail pilot, select **No** for Auto-Learn Voicemail Pilot and enter the Voicemail Pilot number.

Step 10 Click **Next**.

The system displays the TLS Security page of the setup wizard.

Step 11 Choose whether to enable TLS Security.

Step 12 Choose one of the following:

- If you selected only E-SRST Provisioning, click **Finish** to complete the Cisco UMG setup wizard and save this information.
- If you selected SRSV Provisioning, click **Next**.

The system displays the High Availability page of the setup wizard.

Step 13 (Optional) Enter the Hostname or IP Address of Secondary UMG.

Step 14 Click **Finish** to complete the Cisco UMG setup wizard and save this information.

Related Topics

- Supporting High Availability
- Changing Cisco Unified SRSV System Settings

Supporting High Availability

Last updated: August 5, 2011

About High Availability

The high availability feature provides failover for the Cisco Unified SRSV system by providing a mechanism to upload voicemail through a secondary Cisco UMG device. The secondary Cisco UMG device acts as a backup for the primary Cisco UMG device in case the SRSV-CUE device cannot reach the primary Cisco UMG device.

Note Cisco UMG Release 8.6 supports high availability for sites enabled with Cisco Unified SRSV only. High availability for deployments using E-SRST is not supported in this release.

When an SRSV-CUE device has voicemail to upload to the central voicemail server, it first attempts to contact the primary Cisco UMG device. If the primary Cisco UMG device is unreachable, and a secondary Cisco UMG device has been provisioned through the high availability feature, the SRSV-CUE device attempts to reach the secondary Cisco UMG device to upload the voicemail messages.

The system enables the secondary Cisco UMG device after the next provisioning cycle. A provisioning cycle is required to allow the primary Cisco UMG device the opportunity to provision the newly-configured secondary Cisco UMG device hostname to all SRSV-CUE devices. After the secondary Cisco UMG device is provisioned, the SRSV-CUE devices begin to use it to upload voicemail whenever the primary Cisco UMG device cannot be reached.

Enabling High Availability

To enable high availability, you must enter the Hostname or IP Address of Secondary UMG. You can do this in one of two ways:

- Using the setup wizard. See Using the Setup Wizard.
- From the System > SRSV Settings page. See Changing Cisco Unified SRSV System Settings.

Restriction

The software release number for the primary Cisco UMG device and secondary Cisco UMG device must be the same. If the versions are not the same, the primary Cisco UMG device does not provision the secondary Cisco UMG device with the most recent configuration.

Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information

Last updated: August 5, 2011

The Add Central Call Agent Wizard adds Cisco Unified Communications Manager information that identifies the Cisco Unified Communications Manager to the Cisco UMG device, as well as the necessary credentials to retrieve Cisco Unified SRST phone extension information for provisioning to the SRSV-CUE devices.

Note When deploying E-SRST, a deployed Cisco UMG device can be configured for only one central call agent. Do not configure more than one Cisco UMG device to access the same Cisco Unified Communications Manager. In Cisco UMG Release 8.6, Cisco Unified Communications Manager is the only central call agent supported for E-SRST.

No changes are made to the Cisco Unified Communications Manager configuration.

Before You Begin

Gather the following information before you add a Cisco Unified Communications Manager:

Table 4 Central Call Agent Parameters

Parameter	Description
CUCM Hostname	
Hostname or IP Address	Identifies the Cisco Unified Communications Manager to the Cisco UMG device. You can enter either a hostname or IP address. If you enter an IP address, the system performs a DNS reverse look-up to store the Cisco Unified Communications Manager by hostname.

Table 4 Central Call Agent Parameters (continued)

Parameter	Description
CUCM AXL Interface	
AXL Username	The user name that the Cisco UMG device uses to access the Cisco Unified Communications Manager AXL interface. This user name must exist on the Cisco Unified Communications Manager as an "application user" and be assigned the role of "standard AXL API access" or "standard CUCM super users."
AXL Password	The password that corresponds to the Cisco Unified Communications Manager AXL interface user. This password must correspond to the password configured on Cisco Unified Communications Manager for this user name. **Note** If the password changes on Cisco Unified Communications Manager, you must also change the password on the Cisco UMG device. There is no password synchronization between Cisco Unified Communications Manager and the Cisco UMG device for AXL credentials.
CUCM Cluster	
Cluster Name	A descriptive name that uniquely identifies this Cisco Unified Communications Manager cluster. By default, the system uses the hostname that you entered at the beginning of this wizard as the cluster name.
Secondary Node	A second member of the Cisco Unified Communications Manager cluster to be used by Cisco UMG provisioning when the Cisco UMG can not contact the primary Cisco Unified Communications Manager.
CUCM Schedule	
Defines how often you want the Cisco UMG device to contact the Cisco Unified Communications Manager to synchronize configuration data and to provision the SRSV-CUE devices. **Tip** We recommend that you set the schedule so that the Cisco UMG device contacts the Cisco Unified Communications Manager during off-peak hours. By default, the schedule is set to every day at 12am EST.	
Daily	Frequency in days. Enter the number of days between provisioning cycles.
Weekly	Frequency in weeks. Enter the number of weeks between provisioning cycles and the day of the week.

Table 4 Central Call Agent Parameters (continued)

Parameter	Description
Monthly	Frequency in months. Enter the day of the month. **Note** In the case where the day of the month is beyond the number of days the month contains (for example, if you choose the 31st day of every month, but February has only 28 days), the provisioning occurs on the last day of that month. Enter the number of months between provisioning cycles.
Start Time	Start time for the provisioning cycle. This indicates the time of day at which the Cisco UMG device initiates contact to Cisco Unified Communications Manager.
End Time	(Optional) Indicates whether the Cisco UMG device should suspend provisioning at a certain time. If you do not enter an end time, the system continues provisioning until all sites have been processed. If you enter an end time, and the end time is reached during a provisioning cycle, the system suspends provisioning and waits until the next provisioning cycle to continue, at which time any sites not yet provisioned from the previous cycle will be processed first.
Call Agent Time Zone	Indicates the time zone in which the Cisco Unified Communications Manager is physically located. It allows the start and end times to be specified relative to the Cisco Unified Communications Manager time so that peak call load hours can be avoided.
CUCM Voicemail Server	
Default Voicemail Server	Defines the default Cisco Unity Connection voicemail server for the Cisco Unified Communications Manager. The default value will be applied to new sites as Cisco Unified SRST references are identified on the Cisco Unified Communications Manager. If the Cisco Unified Communications Manager is supported by more than one Cisco Unity Connection voicemail server, we recommend that you set this default value to the hostname of the Cisco Unity Connection voicemail server supporting the most Cisco Unified SRST sites (if there is one). If the Cisco Unified SRST sites are evenly distributed across Cisco Unity Connection voicemail servers, select any Cisco Unity Connection.
CUCM Enable	
Enable Provisioning	Controls the Cisco UMG device access to the Cisco Unified Communications Manager. By default, this is set to On.

Table 4 Central Call Agent Parameters (continued)

Parameter	Description
Site Provisioning Defaults	Controls whether provisioning for new sites learned by the Cisco Unified Communications Manager should be enabled by default. • Set Site Provision Enable Default to On to enable provisioning for any new sites learned from Cisco Unified Communications Manager. • Set SRSV Provision Enable Default to On to enable Cisco Unified SRSV provisioning on any new sites learned from Cisco Unified Communications Manager. • Set E-SRST Provisioning to On to enable E-SRST provisioning on any new sites learned from Cisco Unified Communications Manager. These settings are independent of each other, and are applied directly to the sites.

Procedure

Step 1 Select **Setup Wizards > Add Central Call Agent**.

The system displays the Introduction page of the Add Central Call Agent Wizard.

Step 2 Click **Next**.

The system displays the CUCM Hostname page of the Add Central Call Agent Wizard.

Step 3 Enter the Cisco Unified Communications Manager Hostname or IP Address.

Step 4 Click **Next**.

The system displays the CUCM AXL Interface page of the Add Central Call Agent Wizard.

Step 5 Enter the following information:

- AXL Username
- AXL Password
- Confirm the AXL Password

Step 6 Click **Next**.

The system displays a message stating that it will contact the Cisco Unified Communications Manager and downloads all the configured cluster nodes. This can take a few minutes.

Step 7 Click **OK** at the warning message.

The system displays the CUCM Cluster page of the Add Central Call Agent Wizard.

Step 8 Enter the following information:

- Cluster Name
- Secondary Node

Step 9 Click **Next**.

The system displays the CUCM Schedule page of the Add Central Call Agent Wizard.

Step 10 Enter information about how often the Cisco UMG device should contact Cisco Unified Communications Manager to retrieve configuration information. See CUCM Schedule.

Step 11 Enter a start time. You can optionally enter an end time.

Step 12 Enter a time zone.

Step 13 Click **Next**.

The system displays the CUCM Voicemail Server page of the Add Central Call Agent Wizard.

Step 14 Select the default voicemail server from the drop down list.

Step 15 Click **Next**.

The system displays the CUCM Enable page of the Add Central Call Agent Wizard.

Step 16 Set Enable Provisioning to On to enable Cisco UMG to access Cisco Unified Communications Manager.

Step 17 Set the Site Provisioning Defaults values:

- Set Site Provision Enable Default to On to enable provisioning for any new sites learned from Cisco Unified Communications Manager.
- Set SRSV Provision Enable Default to On to enable SRSV provisioning on any new sites learned from Cisco Unified Communications Manager.
- Set E-SRST Provisioning to On to enable E-SRST provisioning on any new sites learned from Cisco Unified Communications Manager.

These three settings establish the default values for this Cisco Unified Communications Manager device and the settings are applied directly to the sites. You can enable or disable provisioning on individual sites as needed. See Changing the Information for a Single Cisco Unified SRST Site and Changing the Information for Multiple Cisco Unified SRST Sites at Once.

Step 18 Click **Finish** to complete the Central Call Agent Wizard and save this information.

Related Topics

- Viewing and Removing the Central Call Agent
- Viewing and Updating the Central Call Agent
- Viewing the Cisco Unified SRST References
- Viewing the Cluster Nodes Associated With a Central Call Agent

Using the Central Voicemail Server Wizard to Add Cisco Unity Connection Information

Last updated: August 5, 2011

Use the Add Central Voicemail Server Wizard to add a Cisco Unity Connection voicemail server to the Cisco Unified SRSV system. The Cisco UMG device uses the Cisco Unity Connection server to retrieve details about Cisco Unified SRSV subscribers.

No changes are made to the Cisco Unity Connection server configuration.

Before You Begin

Gather the following information before you add a Cisco Unity Connection server to the central office:

Table 5 Central Voicemail Server Parameters

Parameter	Description
CUC Hostname	
Hostname or IP Address	Identifies the Cisco Unity Connection server to the Cisco UMG device. You can enter either a hostname or IP address. If you enter an IP address, the system performs a DNS reverse look-up to store the Cisco Unity Connection by hostname.
CUC REST Interface	
REST Username	Username that the Cisco UMG device uses when accessing the Cisco Unity Connection REST interface. This username must exist on the Cisco Unity Connection voicemail server and be assigned the role of system administrator.
REST Password	The password that corresponds to the Cisco Unity Connection REST interface user. This password must correspond to the password configured on Cisco Unity Connection for this username. **Note** If the password changes on Cisco Unity Connection, you must also change the password on the Cisco UMG device. There is no password synchronization between Cisco Unity Connection and the Cisco UMG device for REST credentials.

Table 5 Central Voicemail Server Parameters (continued)

Parameter	Description
CUC Cluster	
Cluster Name	Cisco Unity Connection cluster name. A cluster is a group of connected devices, such as Cisco Unity Connection, that are managed as a single entity. The devices can be in the same location, or they can be distributed across a network.
Secondary Node	The name of the secondary node. This is a replica of the primary node and is configured for use in case the primary node fails.
CUC Root Call Handlers	
Default Root Call Handler	The default call handler to use for a site's auto attendant when a site is bound to a Cisco Unity Connection.
CUC Voicemail Access	
E.164 Phone Number (digits only)	Phone number used by the branch offices to reach the Cisco Unity Connection voicemail server from the PSTN. This number will be provisioned to the SRSV-CUE devices to support a PSTN dial-out feature for reaching the Cisco Unity Connection voicemail server during WAN outages. This parameter is optional. To disable the feature, leave this field blank. This parameter can be up to 15 digits.
CUC Provision Enable	
Enable Provisioning	Controls the Cisco UMG device access to the Cisco Unity Connection voicemail server. By default, this is set to On.

Procedure

Step 1 Select **Setup Wizards > Add Central Voicemail Server**.

The system displays the Introduction page of the Add Central Voicemail Server Wizard.

Step 2 Click **Next**.

The system displays the CUC Hostname page of the Add Central Voicemail Server Wizard.

Step 3 Enter the Cisco Unity Connection Hostname or IP Address.

Step 4 Click **Next**.

The system displays the CUC REST Interface page of the Add Central Voicemail Server Wizard.

Step 5 Enter the following information:

- REST Username
- REST Password
- Confirm the REST Password

Step 6 Click **Next**.

The system displays a message stating that it will now contact the Cisco Unity Connection and download all the configured cluster nodes. This may take a while.

Step 7 Click **OK** at the warning message.

The system displays the CUC Cluster page of the Add Central Voicemail Server Wizard.

Step 8 Enter the following information:

- Cluster Name
- Secondary Node

Step 9 Click **Next**.

The system displays the CUC Root Call Handlers page of the Add Central Voicemail Server Wizard.

Step 10 Enter the Default Root Call Handler.

Step 11 Click **Next**.

The system displays the CUC Voicemail Access page of the Add Central Voicemail Server Wizard.

Step 12 (Optional) Enter the E.164 Phone Number (digits only) used to dial into this voicemail server.

Step 13 Click **Next**.

The system displays the CUC Provision Enable page of the Add Central Voicemail Server Wizard.

Step 14 Select **On** to enable provisioning, which allows the Cisco UMG device to access Cisco Unity Connection.

Step 15 Click **Finish** to complete the Add Central Voicemail Server Wizard and save this information.

Related Topics

- Viewing and Removing Central Voicemail Servers
- Viewing and Updating a Central Voicemail Server
- Viewing the Cluster Nodes Associated With a Central Voicemail Server
- Viewing the Call Handlers Associated With a Central Voicemail Server

Using the Add Branch Voicemail Server Wizard to Add an SRSV-CUE Device

Last updated: August 5, 2011

To add an SRSV-CUE device, also known as a branch voicemail server, to a Cisco UMG device, you can either manually add it using the Add Branch Voicemail Wizard, or automatically register it from the SRSV-CUE device itself. We recommend using the automatic registration from the SRSV-CUE device since it will upload system details to the Cisco UMG device automatically. For instructions on registering automatically, see messaging-gateway srsx register, page 236.

Before You Begin

Gather the following information before you add an SRSV-CUE device:

Table 6 Branch Voicemail Server Parameters

Parameter	Description
SRSV-CUE Hostname	
Hostname or IP Address	Identifies the SRSV-CUE device to the Cisco UMG device. You can enter either a hostname or IP address. If you enter an IP address, the system performs a DNS reverse look-up to store the SRSV-CUE device by hostname. **Note** For sites that use Network Address Translation (NAT), enter the hostname or IP address of the NAT public interface.
Branch Call Agent	
Local Hostname or IP Address	Identifies the branch call agent that will provide telephony services during a WAN outage. This is typically a Cisco Unified Communications Manager Express-as-SRST system (CUCME-SRST). If you do not enter a value here, the system does not provide telephony services. You can enter either a hostname or IP address. If you enter an IP address, the system performs a DNS reverse look-up to store the gateway by hostname.

Table 6 Branch Voicemail Server Parameters (continued)

Parameter	Description
Port Address Translation	
IP Port	The public IP port. If the system is located behind a NAT device, specify the public IP port that has been mapped to the Cisco Unified SRSV system HTTP (port 80) or HTTP (port 443) interface.
Site Assignment	
Site	The name of the site for which this SRSV-CUE device will provide survivable voicemail service.

Procedure

Step 1 Select **Setup Wizards > Add Branch Voicemail Server**.

The system displays the Introduction page of the Add Branch Voicemail Server Wizard.

Step 2 Click **Next**.

The system displays the SRSV-CUE Hostname page of the Add Branch Voicemail Server Wizard.

Step 3 Enter the Hostname or IP Address of the SRSV-CUE device that you are adding.

Step 4 Click **Next**.

The system displays the Branch Call Agent page of the Add Branch Voicemail Server Wizard.

Step 5 Enter the Local Hostname or IP Address.

Step 6 Click **Next**.

The system displays the Port Address Translation page of the Add Branch Voicemail Server Wizard.

Step 7 Enter the IP Port.

Step 8 Click **Next**.

The system displays the Site Assignment page of the Add Branch Voicemail Server Wizard.

Step 9 Choose a Site from the drop-down box. If your site name is not listed, it may have another SRSV-CUE device associated with it or the system may not have learned it yet. In this case, choose “unassigned.”

Step 10 Click **Finish** to complete the Add Branch Voicemail Server Wizard and save this information.

Related Topics

- Viewing and Removing Branch Voicemail Servers
- Viewing and Updating a Branch Voicemail Server
- Managing the Branch Voicemail Server Software

Configuring Users

Last updated: August 5, 2011

- User Profile Fields
- Viewing a List of Users
- Adding a New User
- Displaying or Changing a User Profile
- Displaying or Changing Group Subscriptions
- Finding a User
- Deleting a User
- Changing Your Password

User Profile Fields

Table 7 lists the fields on the User Profile page.

Table 7 User Profile Parameters

Parameter	Description
User ID	Unique alphanumeric identifier used to identify this Cisco UMG administrator.
First Name	First name of the Cisco UMG administrator.
Last Name	Last name of the Cisco UMG administrator.
Nick Name	Optional nickname of the Cisco UMG administrator.
Display Name	Name displayed within Cisco Unified SRSV applications.
Primary E.164 Number	Primary telephone number, including area code, for the Cisco UMG administrator.
Fax Number	Fax number for the Cisco UMG administrator.
Language	Not supported. **Note** Although there is space to choose a language, the Cisco UMG system always uses the system default.

Table 7 User Profile Parameters (continued)

Parameter	Description
Password Login	When set to Enabled, allows you to log in. The system automatically sets this field to Disabled when both of the following conditions are met: • The Account Lockout Policy field on the User Defaults page is set to either **Permanent** or **Temporary**. See Configuring Account Lockout Policy. • The user unsuccessfully attempts to log into the account more times than is acceptable according to the values of the Number of Allowable Attempts and Temporary Lockout Duration fields on the Configure > User Options page. When this field is set to Disabled, only a user who is a member of the administrative group can reset it to Enabled. To reset this field to Enabled, and thus allow the user to log in again, reset the password. See Password options.
Password options	For the password used by the Cisco UMG administrator to access the Cisco UMG GUI, select one of the following: • Generate a random password—To have the system generate a random password. • Blank password—To leave the password blank. • Password specified below—To specify a password for this user.
Password	Consists of letters and numbers and is at least 3 characters but not more than 32 characters long.
PIN Login	Not supported. **Note** Although there is space to set a PIN, the Cisco UMG system does not use PINs. If you set values here, they will not be used.
PIN options	Not supported. **Note** Although there is space to set a PIN, the Cisco UMG system does not use PINs. If you set values here, they will not be used.
PIN	Not supported. **Note** Although there is space to set a PIN, the Cisco UMG system does not use PINs. If you set values here, they will not be used.

Viewing a List of Users

Follow this procedure to view administrative users of the Cisco UMG system.

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page, containing the following fields:

- User ID. By default, the system displays users in alphabetical order by user ID.
- Display Name
- Primary Extension

Step 2 To see a different number of users on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all users.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To sort users, click any of the headers.

Adding a New User

Follow this procedure to add a new Cisco UMG administrator.

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page.

Step 2 Click **Add**.

Step 3 Enter information into the fields. See Table 7.

Step 4 Click **Add**.

Note If you selected a random password, a message appears with the new password. Write the value in a secure place to give to the user. The value is also displayed on the user profile page (see Displaying or Changing a User Profile).

Displaying or Changing a User Profile

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page.

Step 2 If you do not see the user, click **Find** to search for the user (see Finding a User).

Step 3 Click the user ID of the person whose profile you want to see.

The system displays the User Profile page, containing the fields in Table 7.

Step 4 Make any changes and click **Apply**.

Displaying or Changing Group Subscriptions

Use this procedure to modify the groups to which a user is assigned.

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page.

Step 2 Click the name of the user whose group subscription you want to view or modify.

The system displays the User Profile page.

Step 3 Click the **Groups** tab.

The system displays the following fields:

- Group ID
- Rights—whether the user is a member or owner of the group
- Description
- Primary Extension—primary extension of the general-delivery mailbox assigned to the group

Step 4 To make the user the owner of another group, click **Subscribe as owner**. To make the user a member of another group, click **Subscribe as member**.

The system displays the Find page.

Step 5 Enter the group ID, description, or extension number and click **Find**.

Step 6 Check the box next to the group that you want this user to join and click **Select Rows**.

Step 7 To unsubscribe the user from a group, check the box next to the group name and click **Unsubscribe**.

Related Topics

- Configuring Groups

Finding a User

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page.

Step 2 Click **Find**.

The system displays the following fields:

- User ID

- Name
- Extension

Step 3 Enter the search criteria in one or more fields and click **Find**.

The system displays the results of your search.

Deleting a User

Follow this procedure to delete a Cisco UMG administrator.

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page.

Step 2 Check the check box of the user ID that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK** to confirm the deletion.

Changing Your Password

Follow this procedure to change the password of the Cisco UMG administrator.

Restrictions

- By default, passwords should be at least 3 and no more than 32 alphanumeric characters in length. However, you can change this on the Configure User Defaults page. See Configuring Password Options.
- Use a mixture of uppercase and lowercase letters and numbers.
- Spaces are not allowed.

Procedure

Step 1 Select **Configure** > **Users**.

The system displays the Configure Users page.

Step 2 Click your underlined name in the list of users.

Step 3 Ensure that **Password specified below** is selected in the Password options field.

Step 4 Enter your new password.

Step 5 Enter your new password again for verification.

Step 6 Click **Apply**.

Setting User Defaults

Last updated: August 5, 2011

When you create a user, the defaults that you set in the Configure User window take effect. Use these procedures to specify the default global password policy settings for all users. This default set of parameters is applied when a new user is created.

Note Even after you have set defaults in this window, you can change the password policy for an individual user. See Adding a New User.

- Configuring Password Options
- Configuring Account Lockout Policy

Configuring Password Options

If you choose to generate passwords for users automatically, they are configured in the following steps.

Note Although there is space to set a PIN, Cisco UMG does not use PINs. If you set values here, they will not be used.

Procedure

Step 1 Choose **Configure** > **User Defaults**.

The system displays the Configure User Defaults page.

Step 2 Configure password options by performing the following tasks in the Password column:

a. Select whether the auto-generation policy will be random or blank.

b. (Optional) Check **Enable expiry (days)** to set an expiration date for the password. The range is 3 to 365.

c. Set the history depth. The range is 1 to 10.

d. Select the minimum length of the password. The range for the password is 3 to 32.

Step 3 Click **Apply**.

Configuring Account Lockout Policy

The account lockout policy determines how the system acts when a user tries to log in and fails.

Note Although there is space to set a PIN, Cisco UMG does not use PINs. If you set values here, they will not be used.

Procedure

Step 1 Choose **Configure** > **User Defaults**.

The system displays the Configure User Defaults page.

Step 2 Choose one of the following lockout policy types for the Password fields:

- Disable lockout—The user can continue to try to login with no consequences for failing.
  - Continue to Step 3.
- Permanent—The user is permanently locked out after a certain number of failed login attempts.
  - Enter the maximum number of failed attempts. The range is 1 to 200.
  - Continue to Step 3.
- Temporary—The user is temporarily locked out of the system. Enter values for the following:
  - Number of allowable attempts. The range is 1 to 200.
  - Temporary lockout duration. Pick any number in minutes.
  - Maximum number of failed attempts. The range is 1 to 200.
  - Continue to Step 3.

Step 3 Click **Apply** to save your settings.

Configuring Groups

Last updated: August 5, 2011

Group Fields

Table 8 lists the fields on the Groups page.

Table 8 Group Parameters

Parameter	Description
Group ID	Alphanumeric user identifier.
Full name	Long name of the group as it should appear on telephone displays.
Description	Description of the group. The word “group” is automatically added to the Group ID entry.
Primary Extension	Primary extension of the group’s general-delivery mailbox.
Primary E.164 Number	Full telephone number and area code associated with this group.
Fax Number	Fax number associated with this group.

Viewing a List of Groups

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page, containing the following fields:

- Group ID
- Display Name
- Primary Extension
- Privileges

Step 2 To see a different number of groups on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all groups.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To sort groups, click any of the headers.

Step 5 To find a group, click **Find**.

The system displays the Find page.

Step 6 Enter the search criteria in one or more fields and click **Find**.

The system displays the Configure Groups page with the results of your search.

Adding a New User Group

Configuring one or more groups is optional. Many organizations find that having a mailbox for a group, called a general-delivery mailbox, is very convenient. Members of a group can retrieve voice messages left in the general-delivery mailbox. For example, a Customer Service mailbox could be configured to receive messages from customers, and anyone assigned to a Customer Service group could retrieve the messages. Members of the general-delivery mailbox can be individual users or other groups. Individual users also have their individual mailboxes, and groups that are members of another group have their own mailboxes.

Before You Begin

Determine the Primary Extension to be assigned to the group. Ensure that this extension is active.

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Click **Add**.

The system displays the Add a New Group page.

Step 3 Enter information into the fields shown below:

- Group ID
- Full name
- Description
- Primary Extension
- Primary E.164 Number
- Fax Number

Step 4 Check the check box next to the capabilities that you want this group to have. See About Capabilities.

Step 5 Click **Add**.

The system displays the Configure Groups page, with the new group in the table.

Deleting a Group

Deleting a group also deletes the group's mailbox but it does not delete the members of the group.

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Check the check box next to the name of the group that you want to delete.

Step 3 Click **Delete**.

Step 4 At the prompt, click **OK** to delete the group.

Subscribing Members or Owners to a Group

When you add members to a group, each member has access to the voice messages that are stored in that group's mailbox.

A group owner has control of the group's mailbox, but cannot access the group's messages. To access messages, the group owner must also be a member of the group.

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Check the check box next to the name of the group to which you are adding new members.

The system displays the Group Profile page, containing current information about the group.

Step 3 Click **Owners/Members**.

The system displays all members of the group.

Step 4 To add a new member, click **Subscribe Member**. To add a new owner, click **Subscribe Owner**.

The system displays the Find page.

Step 5 Under type, select either users or groups. Enter the User ID or Group ID, Name or Description, and Extension of the person or group that you want to add to this group. All fields are optional.

Step 6 Click **Find**.

The system displays all users or groups that meet the search criteria.

Step 7 Do one of the following:

- Add one or more members to the group by checking the box next to each selected member's name and clicking **Select Rows**. The system displays the Group page with the new member added.
- Look for other people to add by clicking **Back to Find** without checking a box next to any name. The system displays the Find page. Return to Step 5 and continue.

Step 8 To add more members to the group, repeat Step 4 through Step 7.

Unsubscribing Members and Owners from a Group

Restriction

Only group owners can delete members and owners.

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Check the check box next to the name of the group that you want to manage.

The system displays the Group Profile page, containing information about the group.

Step 3 Click **Owners/Members**.

The system displays all members and owners of the group.

Step 4 Check the check box next to the name of each member or owner who you want to unsubscribe from this group.

Step 5 Click **Unsubscribe**.

The system displays the Group Members page with the members or owners removed.

Displaying or Modifying Group Parameters

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Check the check box next to the name of the group that you want to view or modify.

The system displays the Group Profile page for this group, with the following fields:

- Group ID
- Full name
- Description
- Primary Extension
- Primary E.164 Number
- Fax Number

Step 3 Check the check box next to the superuser capability if you want this group to have superuser capabilities. See About Capabilities.

Step 4 To edit these fields, enter the new information and click **Apply**.

Viewing Group Membership in Another Group

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Check the check box next to the name of the group that you want to display.

The system displays the Group Profile page for that group.

Step 3 Click the **Owner/Member of Groups** tab.

Step 4 To see a different number of groups on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all groups.

Step 5 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 6 To sort groups, click any of the headers.

Modifying Group Ownership and Membership in Other Groups

A group has its own set of members, but a group can also be assigned as a member or an owner of one or more other groups. If a group is assigned as an owner of another group, any individual member of the owner group has privileges as an owner of the owned group. For example, if the Administrator group is added as an owner of the Technical Support group, any individual member of the Administrator group can add, modify, or delete members of the Technical Support group. Additionally, individual users that do not belong to another group can be added as owners of the Technical Support group.

Procedure

Step 1 Choose **Configure** > **Groups**.

The system displays the Configure Groups page.

Step 2 Click the name of the group whose membership you want to modify.

The system displays the Group Profile page for that group.

Step 3 Click **Owner/Member of Groups**.

The system displays the Owner/Member of Groups page.

Step 4 To see a different number of groups on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all groups.

Step 5 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 6 To sort groups, click any of the headers.

Step 7 To designate your group as an owner of another group, click **Subscribe as owner**. To subscribe your group as a member of another group, click **Subscribe as member**.

The system displays the Find page.

Step 8 Enter the group ID, description, or extension of the groups that you want to find.

Step 9 Click **Find**.

The system displays all the groups that meet the search criteria.

Step 10 To select one or more groups, click the box next to each group's name and click **Select Rows**.

The system adds the new groups to the list of groups on the Owner/Member of Groups page.

About Capabilities

You can assign capabilities to groups. The Cisco UMG system has only one capability and that is superuser. This capability gives administrator privileges to any users in this group.

Configuring Privileges

Last updated: August 5, 2011

- Viewing Privileges
- Creating a Privilege
- Editing a Privilege
- Deleting a Privilege

Viewing Privileges

Procedure

Step 1 Choose **Configure** > **Privileges**.

The system displays the Configure Privileges page.

Step 2 To see a different number of privileges on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all privileges.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To sort the privileges, click any header.

Step 5 To delete a privilege, do the following:

a. Check the check box of the privilege that you want to delete.

b. Click **Delete**.

Tip You cannot delete the superuser privileges.

Overview of Privileges

Cisco UMG provides one predefined privilege, called superuser, that you can assign to groups. This privilege grants unrestricted system access and includes all operations. 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. Most operations include only one CLI command and GUI function. 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.

Note You cannot modify the superuser privilege. The superuser privilege includes all the operations.

To configure privileges, see Creating a Privilege.

Table 9 describes all available operations that you can add to privileges.

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

Note Users do not need privileges to access their own data. User data is primarily associated with the voicemail application and includes the following:

- Language (configured for the user’s voice mailbox)
- Password
- Membership to groups owned by the user
- Ownership of groups owned by the user
- Notification profile
- Cascade settings
- Personal voicemail zero out number
- Voicemail greeting type
- Voicemail play tutorial flag
- Public distribution lists owned by the user
- Private distribution lists

Table 9 List of Operations

Operation	Description
group.configuration	Creates, modifies, and deletes groups.
security.aaa	Configures and modifies AAA service settings.
security.access	Configures system level security regarding encryption of data, including defining crypto keys. **Note** Also includes permission to reload the system.

Table 9 List of Operations (continued)

Operation	Description
security.password	Configures settings for the system password and policy, such as: • Expiry • Lockout (temporary and permanent) • History • Length
security.pin	Configures settings for the system PIN and policy, such as: • Expiry • Lockout (temporary and permanent) • History • Length
services.configuration	Configures system services such as DNS, NTP and 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	Configures system level service commands not related to configuration, such as clearing DNS cache and ping.
software.install	Installs, upgrades, or inspects system software or add-ons such as languages and licenses. **Note** Also includes permission to reload the system.
srsx	Configures the Cisco UMG application.
srsx.register	Registers SRSV-CUE devices with Cisco UMG.
system.backup	Configures backup parameters.
system.configuration	Configures system settings such as the clock, hostname, domain name, default language, and interfaces (counters).
system.debug	Collects and configures trace and debug data. Includes copying data such as core and log files.
system.view	Views system settings and configuration.
umg.config	Configures the Cisco UMG.
umg.sdl	Configures the Cisco UMG system distribution list.

Table 9 List of Operations (continued)

Operation	Description
user.configuration	Creates, modifies, and deletes users and groups, including the following: • First and last name • Nickname • Display name • Language
user.password	Creates, sets, or removes user passwords.

Creating a Privilege

Use this procedure to create a new privilege and or specify which operations are included in it.

Procedure

Step 1 Choose **Configure** > **Privileges**.

The system displays the Configure Privileges page.

Step 2 Click **Add**.

The system displays the Configure Privileges > Add page.

Step 3 Enter a name and description for the privilege.

Step 4 Check the operations that you want to add to the privilege. See Table 9.

Step 5 Click **Add**.

Editing a Privilege

Use this procedure to change or display which operations are included a privilege.

Restrictions

- You cannot modify the superuser privilege.

Before You Begin

- Create a privilege. See Creating a Privilege.

Procedure

Step 1 Choose **Configure** > **Privileges**.

The system displays the Configure Privileges page.

Step 2 Click the underlined name of the privilege that you want to edit.

Note You might have to change the number of rows per page or select a different page to see the privilege that you want to change.

The system displays the Configure Privileges > Edit page.

Step 3 Select the operations that you want to add to the privilege or deselect the operations that you want to remove, or edit the description.

Step 4 Click **Apply**.

Step 5 Click **OK** to save your changes.

Deleting a Privilege

Procedure

Step 1 Choose **Configure** > **Privileges**.

The system displays the Configure Privileges page.

Step 2 Check the check box of the privilege that you want to delete.

Step 3 Click **Delete**.

Configuring Authentication, Authorization, and Accounting

Last updated: August 5, 2011

- Configuring the AAA Authentication Server
- Specifying the Policy that Controls the Behavior of Authentication and Authorization
- Configuring the AAA Accounting Server

Configuring the AAA Authentication Server

- About the Authentication Order
- About Authentication Failover
- About Unreachable Failover
- Example of Authentication Sequence
- Configuring Connection Parameters for the AAA Authentication Server

About the Authentication Order

The AAA policy specifies the failover functionality that you can optionally configure for the authentication server. You can use these two types of failover functionality separately or in combination:

- Authentication failover
- Unreachable failover

About 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:

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

- The remote server first, then the local database

When using both local and remote authentication, you can also configure whether you want the user attributes that are retrieved from a remote RADIUS AAA server to be merged with the attributes found in the local user database for the same username.

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. The auto-attendant interface does not require authentication because it is user independent.
- Login information is not synchronized between the local system and the remote server. Therefore:
  - Any security features such, as password expiration, must be configured separately for Cisco UMG and the RADIUS server.
  - Cisco UMG users are not prompted when security events, such as password expiration or account lockout, occur on the RADIUS server.
  - RADIUS server users are not prompted when security events, such as password expiration or account lockout, occur on Cisco UMG.

About Unreachable Failover

The Unreachable Failover feature 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, the system sends messages to users to notify them when a RADIUS server either cannot be reached or fails to authenticate the user.

Example of Authentication Sequence

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 sequence of events 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.

Configuring Connection Parameters for the AAA Authentication Server

Procedure

Step 1 Choose **Configure** > **AAA** > **Authentication**.

The system displays the Configure AAA Authentication page.

Step 2 Enter the following information in the appropriate fields for the primary server, and optionally, for the secondary server:

- Authentication order
- Number of login retries
- Length of login timeout
- Hostname
- Port
- Password

Step 3 Click **Apply**.

Step 4 Click **OK** to save your changes.

Specifying the Policy that Controls the Behavior of Authentication and Authorization

Use this procedure to configure the information used to log into the authentication server.

Procedure

Step 1 Choose **Configure** > **AAA** > **Authorization**.

The system displays the Configure AAA Authorization page.

Step 2 Select or deselect whether you want to merge the attributes of the remote AAA server with the attributes in the local database.

Step 3 Click **Apply**.

Step 4 Click **OK** to save your changes.

Configuring the AAA Accounting Server

- Overview
- AAA Accounting Event Logging
- Configuring the AAA Accounting Server and Event Logging

Overview

You can configure up to two AAA accounting servers. Automatic failover functionality is provided if you have two accounting servers configured. If the first server is unreachable, the accounting information is sent to 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 the Cisco UMG system.

Note Only RADIUS servers are supported.

AAA 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:

Log Name	Description
login	All forms of system access when a login is required.
logout	All forms of system access when a login is required before logout.
login-fail	Failed login attempts for all forms of system access when a login is required.
config-commands	Any changes made to the system configuration using any interface.
exec-commands	Any commands entered in EXEC mode using any interface.
system-startup	System startups, which include information about the system’s software version, installed licenses, installed packages, installed languages, and so on.
system-shutdown	System shutdowns, which include information about the system’s software version, installed licenses, installed packages, installed languages, and so on.

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

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

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 the AAA Accounting Server and Event Logging

Use this procedure to configure the information used to log into the accounting server.

Procedure

Step 1 Choose **Configure** > **AAA > Accounting**.

The system displays the Configure AAA Accounting page.

Step 2 Enter the following information in the appropriate fields:

- If accounting is enabled
- Number of login retries
- Length of login timeout, in seconds
- Server IP address or DNS name for the primary server
- Port number used for the primary server
- Password for the primary server
- Server IP address or DNS name for the secondary server
- Port number used for the secondary server
- Password for the secondary server

Step 3 Select the log events that you want to include in the log and deselect those you do not want to include.

Step 4 Click **Apply**.

Step 5 Click **OK** to save your changes.

Viewing and Removing Central Voicemail Servers

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Central Voicemail Servers**.

The system displays the Central Voicemail Servers page, containing a list of the central voicemail servers that you have configured.

Step 2 To view the details of a central voicemail server, click the underlined name of a server. See one of the following:

- Viewing and Updating a Central Voicemail Server
- Viewing the Cluster Nodes Associated With a Central Voicemail Server
- Viewing the Call Handlers Associated With a Central Voicemail Server

Step 3 To add a central voicemail server, click **Add**.

The system displays the Add Central Voicemail Server Wizard. See Using the Central Voicemail Server Wizard to Add Cisco Unity Connection Information.

Step 4 To remove a central voicemail server, do the following:

a. Check the check box next to the name of the central voicemail server that you want to remove.

b. Click **Remove**.

c. Click **OK** at the warning message.

Viewing and Updating a Central Voicemail Server

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Central Voicemail Servers**.

The system displays the Central Voicemail Servers page, containing a list of the central voicemail servers that you have configured.

Step 2 To view the details of a central voicemail server, click the underlined name of a server.

The system displays the CUC Profile page with the Profile tab highlighted. The system displays the cluster profile information.

Parameter	Description
Cluster Name	Name of this cluster.
Primary Node	The primary node for this cluster.
Secondary Node	The secondary node for this cluster.
REST Username	The user name for the REST user.
REST Password	The password for the REST user.
REST Pacing Interval	The delay (measured in milliseconds) that the Cisco UMG device inserts between accesses of the Cisco Unity Connection REST interface. We recommend that you leave this value at 0, unless you notice a significant performance impact on the Cisco Unity Connection system during Cisco UMG device provisioning.
E.164 Phone Number	The E.164 phone number that can be dialed from the Cisco Unified SRST site to reach the central Cisco Unity Connection via the PSTN. If configured, this phone number is provisioned on the SRSV-CUE device and allow users to speed dial the central Cisco Unity Connection by pressing 1-1.

Parameter	Description
Enable Provisioning	Whether provisioning is enabled for this cluster.
Auto Attendant Default Root Call Handler	The call handler, or greeting, that is configured on SRSV-CUE devices that have this Cisco Unity Connection as their central voicemail system.

Step 3 To update the profile information, enter the new information and click **Update**.

Related Topics

- Viewing and Removing Central Voicemail Servers
- Viewing the Cluster Nodes Associated With a Central Voicemail Server
- Viewing the Call Handlers Associated With a Central Voicemail Server

Viewing the Cluster Nodes Associated With a Central Voicemail Server

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Central Voicemail Servers**.

The system displays the Central Voicemail Servers page, containing a list of the central voicemail servers that you have configured.

Step 2 To view the cluster nodes associated with a central voicemail server, click the underlined name of the server.

The system displays the CUC Profile page with the Profile tab highlighted.

Step 3 Click the **Cluster Nodes** tab.

The system displays the CUC Cluster Nodes page with the cluster nodes that have been configured.

Step 4 To see a different number of cluster nodes on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 cluster nodes.

Step 5 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 6 To retrieve a node, do the following:

a. Click **Retrieve Nodes**. The system displays a warning message stating that the Cisco UMG will automatically contact the central voicemail server and download all configured cluster nodes.

b. Click **OK** to retrieve the nodes.

Note You do not need to enter the cluster hostnames. The system uses the AXL interface to query the central voicemail server and learn which cluster members have been configured.

Related Topics

- Viewing and Removing Central Voicemail Servers
- Viewing and Updating a Central Voicemail Server

- Viewing the Call Handlers Associated With a Central Voicemail Server

Viewing the Call Handlers Associated With a Central Voicemail Server

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Central Voicemail Servers**.

The system displays the Central Voicemail Servers page, containing a list of the central voicemail servers that you have configured.

Step 2 To view the call handlers associated with a central voicemail server, click the underlined name of the server.

The system displays the CUC Profile page with the Profile tab highlighted.

Step 3 Click the **Call Handlers** tab.

The system displays the Call Handlers page with the call handlers that have been configured.

Step 4 To see a different number of call handlers on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 call handlers.

Step 5 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 6 To retrieve a call handler, do the following:

a. Click **Retrieve Call Handlers**. The system displays a warning message stating that the Cisco UMG will automatically contact the central voicemail server and download all configured call handlers.

b. Click **OK** to retrieve the call handlers.

Related Topics

- Viewing and Removing Central Voicemail Servers
- Viewing and Updating a Central Voicemail Server
- Viewing the Cluster Nodes Associated With a Central Voicemail Server

Viewing and Removing the Central Call Agent

Last updated: August 5, 2011

Restriction

You can only configure one central call agent per system.

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the details of the central call agent, click the underlined name. See one of the following:

- Viewing and Updating the Central Call Agent
- Viewing the Cisco Unified SRST References
- Viewing the Cluster Nodes Associated With a Central Call Agent

Step 3 To add a central call agent, click **Add**.

Note You can only configure one central call agent per system. If one is already configured, the Add button is grayed out.

The system displays the Add Central Call Agent Wizard. See Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information.

Step 4 To remove a central call agent, do the following:

a. Select the central call agent.

b. Click **Remove**.

c. Click **OK** at the warning message.

Viewing and Updating the Central Call Agent

Last updated: August 5, 2011

You can change information about the central call agent that you previously configured.

Before You Begin

Enter initial values by using the Add Central Call Agent Wizard. See Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information.

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the details of the central call agent, click its underlined name.

The system displays the CUCM Profile page with the Profile tab highlighted.

Step 3 Update the information on the page. See Table 4 for a description of the parameters.

Step 4 Click **Update** to save this information.

Related Topics

- Viewing and Removing the Central Call Agent
- Viewing the Cisco Unified SRST References
- Viewing the Cluster Nodes Associated With a Central Call Agent

Viewing the Cisco Unified SRST References

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the details of the central call agent, click the underlined name. See Viewing and Updating a Central Voicemail Server.

The system displays the CUCM Profile page. Click the **SRST References** tab to view a list of the Cisco Unified SRST references.

Step 3 To see a different number of Cisco Unified SRST references on each page, choose another number from the drop-down box on the top right and click **Go**. You can choose to see 10, 25, 50, 100, or 500 Cisco Unified SRST references.

Step 4 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 5 To retrieve additional Cisco Unified SRST references, do the following:

a. Click **Retrieve SRST References**. The system displays a warning message stating that the Cisco UMG will automatically contact the central voicemail server and download all configured Cisco Unified SRST references.

b. Click **OK** to retrieve the references.

The system automatically creates new branch office sites for each Cisco Unified SRST reference.

When finished, the system refreshes the CUCM Profile page to display the Cisco Unified SRST references that were retrieved.

Step 6 To view the sites, go to **Configure > Sites**.

The system displays all the sites, including the following information:

- Site name
- If provisioning is enabled
- Name of the corresponding Cisco Unified Communications Manager
- Hostname and IP address of the corresponding Cisco Unified SRST
- Name of the corresponding Cisco Unity Connection

- Name of the SRSV-CUE device to which this site is assigned (if any)

Related Topics

- Viewing and Removing the Central Call Agent
- Viewing and Updating a Central Voicemail Server
- Viewing the Cluster Nodes Associated With a Central Call Agent

Viewing and Removing Branch Voicemail Servers

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Branch Voicemail Servers > Server List**.

The system displays the Branch Voicemail Servers page, including the following information:

Parameter	Description
Hostname	Hostname of the branch voicemail server.
Port	Port number of the branch voicemail server. Can be 80 for HTTP or 443 for HTTPS. By default the system uses port 80 (unless TLS is configured, in which case the system uses port 443). You can override this value and specify a different port number.
Branch Call Agent	The IP address or hostname of the Cisco Unified SRST or CME-as-SRST gateway. Defines the address of the entity that routes calls to the device.
Module Type	Type of Cisco network module hardware on which the SRSV-CUE device resides. Can be AIM2, NME-CUE, ISM-SRE, SM-SRE, or 1861.
Memory	Amount of memory installed in the SRSV-CUE device.
Serial Number	Manufacturing serial number of the SRSV-CUE device.
Version	Software version running on the SRSV-CUE device.

Step 2 To see a different number of branch voicemail servers on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 branch voicemail servers.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To filter the list of branch voicemail servers, do the following:

- **a.** Select a filter from the Filter drop-down list.
- **b.** Select a condition from the Match if drop-down list.
- **c.** Enter a keyword.
- **d.** Click **Go**.
- **e.** To clear the values, click **Clear Filter** and click **Go**.

Step 5 To add a branch voicemail server, click **Add**.

The system displays the Add Branch Voicemail Server Wizard. See Using the Add Branch Voicemail Server Wizard to Add an SRSV-CUE Device.

Step 6 To see additional information about a branch voicemail server, click the underlined name of the branch voicemail server. See Viewing and Updating a Branch Voicemail Server.

Step 7 To upgrade the software for one or more branch voicemail servers, see Managing the Branch Voicemail Server Software.

Step 8 To remove a branch voicemail server, do the following:

- **a.** Check the check box next to the name of the branch voicemail server that you want to remove.
- **b.** Click **Remove**.
- **c.** Click **OK** at the warning message.

Viewing the Cluster Nodes Associated With a Central Call Agent

Last updated: August 5, 2011

You can change information about the central call agent that you previously configured.

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the cluster nodes associated with the central call agent, click the underlined name of the call agent.

The system displays the CUCM Profile page with the Profile tab highlighted.

Step 3 Click the **Cluster Nodes** tab.

The system displays the CUCM Profile page with the cluster nodes that have been configured.

Step 4 To see a different number of cluster nodes on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 cluster nodes.

Step 5 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 6 To retrieve a node, do the following:

a. Click **Retrieve Nodes**. The system displays a warning message stating that the Cisco UMG will automatically contact the central call agent and download all configured cluster nodes.

b. Click **OK** to retrieve the nodes.

Related Topics

- Viewing and Removing the Central Call Agent
- Viewing and Updating a Central Voicemail Server
- Viewing the Cisco Unified SRST References

Viewing and Updating a Branch Voicemail Server

Last updated: August 5, 2011

Before You Begin

Add branch voicemail servers to the Cisco Unified SRSV system by using the Add Branch Voicemail Server Wizard. See Using the Add Branch Voicemail Server Wizard to Add an SRSV-CUE Device.

Procedure

Step 1 Select **Configure > Branch Voicemail Servers > Server List**.

The system displays the Branch Voicemail Servers page.

Step 2 To see additional information about a branch voicemail server, click the underlined name of the branch voicemail server.

The system displays the SRSV-CUE Profile page.

Step 3 (Optional) Update the branch call agent hostname or IP address.

Step 4 (Optional) Update the IP port.

Step 5 Click **Update** to save this information.

What To Do Next

Associate the branch voicemail server with a site. See Changing the Information for a Single Cisco Unified SRST Site or Configuring Unassigned Branch Voicemail Servers.

Related Topics

- Viewing and Removing Branch Voicemail Servers
- Managing the Branch Voicemail Server Software

Managing the Branch Voicemail Server Software

Last updated: August 5, 2011

Note The information in this section only applies to Cisco UMG Release 8.6.1 and later. If you are using Cisco Unified SRSV Release 8.5 or earlier, you must manually upgrade the branch voicemail server software.

This page lists the available software upgrades that are available for the branch voicemail servers, listed by platform. If you want to upgrade the software on a branch voicemail server, follow these steps:

1. Determine which of the listed branch voicemail servers you want to upgrade and the version that you want to upgrade to.
2. Determine the version of the software that is currently running on that branch voicemail server. See the Version field on the **Configure > Branch Voicemail Servers > Server List** page. If this is the version you want to upgrade to, stop. The server has already been upgraded to that version. If this is not the version you want, continue.
3. Check if the version of the software that you want to upgrade to is already uploaded onto your Cisco UMG system for your platform. (Before you can upgrade any of the branch voicemail servers, you have to download the upgrade software from Cisco.com and upload it to the Cisco UMG system.) See the **Configure > Branch Voicemail Servers > Software Upgrade** page for a list of all the software upgrade images that have been uploaded onto your Cisco UMG system already.
4. If the version of the software for your platform is not there, upload it. See Step 3 below.
5. Return to the **Configure > Branch Voicemail Servers > Server List** page.
6. Check the check box next to the branch voicemail server that you want to upgrade.
7. Click **Upgrade Software**.

Procedure

Step 1 Select **Configure > Branch Voicemail Servers > Software Upgrade**.

The system displays the Branch Voicemail Server Software Upgrade page listing all the installed images.

Step 2 Check the Software Upgrade Enable check box to enable the software upgrade functionality.

Step 3 To upload an image, do the following:

- **a.** Go to cisco.com and download the upgrade software. The name will have “upgrade” in it and be similar to srsv-vm-k9.upgrade.nmx.8.6.1.zip. See the *Release Notes for Cisco Unified Messaging Gateway Release 8.6* for complete information about the files.
- **b.** On the **Configure > Branch Voicemail Servers > Software Upgrade** page, click **Upload**. The system displays the Branch Voicemail Server Software Upload page.
- **c.** Click **Browse** to search for the upgrade file that you downloaded.
- **d.** Select the file and click **Open**.
- **e.** Click **Upload**. The system displays a message stating that the image will be uploaded to the server and this may take several minutes.
- **f.** Click **OK** at the warning message.
- **g.** Click **Update**.

Step 4 To remove an image, do the following:

- **a.** Check the check box next to the name of the SRSV image that you want to remove.
- **b.** Click **Remove**.
- **c.** Click **OK** at the warning message.

Related Topics

- *Installation and Upgrade Guide for Cisco Unified Messaging Gateway Release 8.6*
- Viewing and Removing Branch Voicemail Servers
- Viewing and Updating a Branch Voicemail Server

Viewing and Provisioning Sites

Last updated: August 5, 2011

Before You Begin

- You must have imported at least one site. See Viewing the Cisco Unified SRST References.

Restrictions

- (For provisioning only) The site that you want to provision must have either Cisco Unified SRSV or E-SRST provisioning enabled. The system displays a green check mark next to the name of sites for which provisioning is enabled.
  - If E-SRST provisioning is enabled for the site, the site must have a branch call agent device running CUCME-as-SRST associated with it.
  - If Cisco Unified SRSV provisioning is enabled for the site, the site must have a SRSV-CUE device associated with it.

Note If provisioning is not enabled on a site, the site will not be provisioned.

Procedure

Step 1 Select **Configure > Sites**.

The system displays the Sites page listing all the sites that have been added to your Cisco UMG system. For each site, the following information is listed:

Parameter	Description
Site	Name of the site.
Provisioning	Displays a green check mark if provisioning is enabled.
Central Voicemail Server	Name of the corresponding central voicemail server.
Branch Voicemail Server	Name of the SRSV-CUE device to which this site is assigned (if any). If it is not assigned, lists <unassigned>.
Branch Call Agent	Name of the branch call agent associated with this site.

Step 2 To see a different number of sites on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, 500, or all sites.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To filter the list of sites, do the following:

a. Select a filter from the Filter drop-down list.

b. Select a condition from the Match if drop-down list.

c. Enter a keyword.

d. Click **Go**.

e. To clear the values, click **Clear Filter** and click **Go**.

Step 5 To provision a site, do the following:

a. Check the check box next to the name of the site that you want to provision.

b. Click **Provision Selected Sites**. The system displays a warning message stating that the Cisco UMG system will immediately contact the Cisco Unified Communications Manager and Cisco Unity Connection systems and download all the information about the selected sites.

c. Click **OK** to continue.

Note For more information about provisioning, including the difference between automatic (scheduled) and manual provisioning, see About Provisioning Branch Site Devices.

d. To view the status of the provisioning, click **Monitor > Provisioning Status**. See Monitoring the Provisioning Status of a Branch Device.

Step 6 To see more information about a specific site or to edit the information about a site, click the underlined name of the site. See Changing the Information for a Single Cisco Unified SRST Site.

Step 7 To edit more than one site at a time, click **Bulk Edit Selected Sites**. See Changing the Information for Multiple Cisco Unified SRST Sites at Once.

About Provisioning Branch Site Devices

The Cisco UMG provisions the following device types in each branch:

- Branch call agent
- SRSV-CUE voicemail device

There are two ways you can provision a branch device: automatically according to a schedule or manually.

Typically, provisioning takes place based on the Cisco Unified Communications Manager provisioning schedule. The schedule defines a recurrence frequency that dictates how often the Cisco UMG will synchronize voicemail subscriber accounts between the central office and the branch.

About Scheduled Provisioning

The Cisco UMG device automatically initiates the provisioning based on the schedule configured. Provisioning scheduled times are relative to the time zone of the Cisco Unified Communications Manager. This enables you to accurately select the time of day when the Cisco Unified Communications Manager call load is the lowest. The Cisco UMG automatically adjusts the provisioning start and end times based on the time difference between the Cisco UMG and the configured call agent time zone.

For example, if the Cisco UMG is in the U.S. EST time zone and the Cisco Unified Communications Manager is in the U.S. PST time zone, if the provisioning schedule is configured to run at 1:00 a.m. daily, the Cisco UMG will wait until 4:00 a.m. EST to provision sites.

See Table 4 for more information about the provisioning schedule.

Manually Provisioning a Site

You can manually provision sites from the **Configure > Sites** page. During the provisioning cycle, the system contacts the Cisco Unified Communications Manager, Cisco Unity Connection, and SRSV-CUE devices. We recommend that you perform this procedure when the central systems are not busy.

Changing the Information for a Single Cisco Unified SRST Site

Last updated: August 5, 2011

Before You Begin

- You must have imported at least one site. See Viewing the Cisco Unified SRST References.

Procedure

Step 1 Select **Configure > Sites**.

The system displays the Sites page.

Step 2 Click the underlined name of the site for which you want to update the information.

The system displays the Site Profile page.

Step 3 Update fields.

Table 10 Update Site Parameters

Parameter	Description
Site Name	Initially set to the Cisco Unified SRST reference name retrieved from the Cisco Unified Communications Manager. **Note** Site names must be unique.
Operator Extension	Phone extension on this system for the operator.
Central Voicemail Server	Defines the Cisco Unity Connection system on which subscribers for this site are configured.
Branch Voicemail Server	Defines the SRSV-CUE device that is supporting this site.
Site Provisioning Enable	Determines if provisioning is enabled for the site.
Template	Defines the name of the site template to be used when provisioning the branch device. See Using Site Templates.

Table 10 Update Site Parameters (continued)

Parameter	Description
Feature Enable	Selects whether Cisco Unified SRSV or E-SRST is enabled or disabled on the site. You can enable either Cisco Unified SRSV or E-SRST, or both. **Note** There must be enough feature licenses installed for the number of sites provisioned. If provisioning for both E-SRST and Cisco Unified SRSV is enabled on the same site, E-SRST is provisioned before Cisco Unified SRSV.
Username	Defines the username login credentials for the device at the site.
Password	Defines the password login credentials for the device at the site.
Root Call Handler	Selects the default root call handler, which defines the auto attendant call flow for the SRSV-CUE device.

Step 4 Click **Update** to save this information.

Related Topics

- Viewing and Provisioning Sites
- Changing the Information for Multiple Cisco Unified SRST Sites at Once

Changing the Information for Multiple Cisco Unified SRST Sites at Once

Last updated: August 5, 2011

Before You Begin

- You must have imported at least one site. See Viewing the Cisco Unified SRST References.

Restrictions

- You must configure all Cisco Unified SRST sites with a user name and password for provisioning to succeed.
- Do not use the Bulk Edit Selected Sites feature if each Cisco Unified SRST site has a unique user name and password. When you use the Bulk Edit Selected Sites feature, the system changes each Cisco Unified SRST site user name and password on the Cisco UMG to the same values. These new values must match the values configured on the individual Cisco Unified SRST sites.
- You must have enough Cisco Unified SRSV or E-SRST feature licenses installed for the number of sites being provisioned. If there are not enough feature site licenses installed, the system will not provision all of the sites.
- If both Cisco Unified SRSV and E-SRST are enabled on the same site, the system provisions E-SRST before Cisco Unified SRSV.

Procedure

Step 1 Select **Configure > Sites**.

The system displays the Sites page.

Step 2 Check the check boxes next to the sites that you want to modify.

Step 3 Click **Bulk Edit Selected Sites**.

The system displays the Site Profile Bulk Edit page.

Step 4 To make changes, check the checkbox next to a field name and then enter a value for any or all of the following:

- Operator Extension
- Central Voicemail Server
- Site Provisioning Enable

- Feature Enable: SRSV Provisioning Enable
- Feature Enable: E-SRST Provisioning Enable
- Template
- Unassign Branch Voicemail Server
- Router login credentials: Username
- Router login credentials: Password
- Default Root Call Handler

Step 5 Click **Update**.

The system applies the changes to each of the sites.

Related Topics

- Viewing and Provisioning Sites
- Changing the Information for a Single Cisco Unified SRST Site

Using Site Templates

Last updated: August 5, 2011

Because many sites have common sets of information, the Cisco UMG system provides site templates. Use these templates to apply configuration settings to new sites.

The Cisco UMG system automatically contains one site template called "default." You cannot change the name of this site template or delete it, but you can change its values. You can also create custom site templates.

Procedure

Step 1 Select **Configure > Site Templates**.

The system displays the Site Templates page, containing a list of the site templates that you have configured.

Step 2 To create a new site template, update an existing site template, or view the details about an existing site template, see Creating, Changing, and Viewing a Site Template.

Step 3 To remove a site template, do the following:

a. Select the site template that you want to delete.

b. Click **Remove**.

c. Click **OK** at the warning message.

Creating, Changing, and Viewing a Site Template

Last updated: August 5, 2011

Procedure

Step 1 Select **Configure > Site Templates**.

The system displays the Site Templates page and a list of all the site templates.

Step 2 Do one of the following:

- To create a new site template, click **Add**.
- To view the details about or to change an existing site template, click the underlined name of the site template.

The system displays the Site Template Profile page, including the following information:

Table 11 Site Template Profile Parameters

Parameter	Description
Name	The name of the site template. Restriction: The name cannot have spaces in it.
Auto-Learn Voicemail Pilot	Specifies whether the Cisco UMG device automatically learns the voicemail pilot number from Cisco Unified Communications Manager. If you select No, you must enter the pilot number in the Pilot Number field.
Pilot Number	The phone extension that the Cisco UMG device assigns as the pilot number on the SRSV-CUE device. This number must agree with the dial-peer extension configured on the Cisco Unified Communications Manager directory number for call-forward busy/noan for the SRSV-CUE device to receive incoming voicemail calls. The number must be between one and 15 digits. Only digits are allowed; spaces and dashes are not allowed.
Enable Live Record	Enables the live record feature to be provisioned on the SRSV-CUE device.

Table 11 Site Template Profile Parameters (continued)

Parameter	Description
Live Record Pilot Number	The phone extension that the Cisco UMG device provisions on the SRSV-CUE device to support the live record feature. **Note** This parameter is only available if you check Enable Live Record. The number must be between one and 15 digits. Only digits are allowed; spaces and dashes are not allowed.
Live Record Beep Enable	Enables an audible beep to be played during a live record session. **Note** This parameter is only available if you check Enable Live Record.
Live Record Beep Interval	The interval, in seconds, between beeps when the live record feature is in use. **Note** This parameter is only available if you check Enable Live Record and Live Record Beep Enable. The range is from 1 to 30.
Live Record Beep Duration	The duration, in milliseconds, of the live record beep. **Note** This parameter is only available if you check Enable Live Record and Live Record Beep Enable. The range is from 50 to 1000.
Enable Live Reply	Enables the live reply voicemail feature to be provisioned on the SRSV-CUE device.
Mailbox Size	Default size, in seconds, of a subscriber mailbox on the SRSV-CUE device. The range is from 1 to 10000000.
Maximum Message Size	Maximum size, in seconds, of any voicemail message that can be left on the SRSV-CUE device. The range is from 1 to 10000000 and the maximum message size cannot be larger than the Mailbox Size.
Message Expiration	Default number of days after which a message expires on the SRSV-CUE device. The range is from 1 to 365.
Enable Menu Items Changed Prompt	Enables a special voicemail prompt to be played when the Cisco Unified SRSV system is active, indicating that users are currently connected to the survivable voicemail system.
MWI Mode	Determines the message waiting indicator (MWI) mode. The options are: • Automatic • Always-on • Always-off

Table 11 Site Template Profile Parameters (continued)

Parameter	Description
MWI Type	MWI control type. The options are: • Sub-Notify • Unsolicited This setting must match the configuration of the central Cisco Unified Communications Manager.

Step 3 Enter information in the fields. See Table 11.

Step 4 Click **Update**.

Related Topics

- Using Site Templates

Configuring Unassigned Branch Voicemail Servers

Last updated: August 5, 2011

After you manually configure a branch voicemail server, you must associate it with a specific site. You can do this from the Site Profile page (see Changing the Information for a Single Cisco Unified SRST Site), but if you need to make many associations, this can become tedious. Use the Unassigned Branch Voicemail Servers page as a faster method of assigning SRSV-CUE devices to sites.

Procedure

Step 1 Select **Configure > Unassigned Branch Voicemail Servers**.

The system displays the Unassigned Branch Voicemail Servers page with a list of all the unassigned branch voicemail servers on one side and all the unassigned sites on the other side.

Step 2 Select the unassigned branch voicemail server that you want to assign to a site.

Step 3 Select a site to assign to the unassigned branch voicemail server.

Step 4 Click **Assign Branch Voicemail Server to Site**.

Tip If you select an unassigned branch voicemail server, you can simply double-click a site to assign the site to it.

Changing Cisco Unified SRSV System Settings

Last updated: August 5, 2011

Before You Begin

- Enter initial values by using the Setup Wizard. See Using the Setup Wizard.

Procedure

Step 1 Select **System > SRSV Settings**.

The system displays the SRSV Settings page with the values that you entered previously.

Step 2 Update any of the following fields:

- UMG REST Password
- SRSV-CUE REST Password
- Hostname or IP Address of Secondary UMG
- TLS Security—whether TLS security is enabled or not

Step 3 Click **Update** to save this information.

PART 2

Making Updates to the System

Working With DNS Servers

Last updated: August 5, 2011

Restriction

You can have a maximum of four DNS servers.

Procedure

Step 1 Select **System** > **Domain Name Settings**.

The system displays the Domain Name Settings page.

Step 2 To update the domain name settings, enter values in either or both of the following fields:

- The hostname of the Cisco UMG system.
- The domain name or IP address of the DNS server.

Step 3 To add a DNS server, do the following:

a. Click **Add**.

b. Enter the IP address of the DNS server.

c. Click **Add**.

Step 4 To remove a DNS server, do the following:

a. Check the check box next to the DNS server that you want to delete.

b. Click **Delete**.

c. At the prompt, click **OK**.

What To Do Next

If you have made any changes, save and then reload the configuration. See Saving and Reloading the Cisco Unified Messaging Gateway Configuration.

Working With Network Time and Time Zone Settings

Last updated: August 5, 2011

You must add an NTP server to your Cisco UMG system and configure the time zone to ensure that voicemails and system processes have the correct date and time associated with them.

Restriction

You can have a maximum of four NTP servers.

Procedure

Step 1 Select **System** > **Network Time & Time Zone Settings**.

The system displays the Network Time & Time Zone Settings page.

Step 2 To add an NTP server, do the following:

a. Click **Add**. The system displays the Add a NTP Server page.

b. Enter the IP address of the NTP server.

c. Check Preferred to make this the preferred NTP server.

d. Click **Add**.

Step 3 To remove an NTP server, do the following:

a. Check the check box next to the NTP server that you want to delete.

b. Click **Delete**.

c. At the prompt, click **OK**.

Step 4 To update the time zone settings, change the values for the country or time zone where your Cisco UMG system resides. Click **Apply**.

What To Do Next

If you have made any changes, save and then reload the configuration. See Saving and Reloading the Cisco Unified Messaging Gateway Configuration.

Configuring the System Login Banner

Last updated: August 5, 2011

Use this procedure to change the text on the login banner that users see when they log in to the CLI.

Procedure

Step 1 Choose **System** > **Login Banner**.

The system displays the Login Banner page.

Step 2 Enter the text for the login banner.

Step 3 Click **Apply** to save your settings.

Configuring SNMP Settings

Last updated: August 5, 2011

- About MIBs
- Working With SNMP Community Strings
- Viewing and Removing an SNMP Trap Host
- Adding and Editing SNMP Trap Hosts
- Displaying MIBs
- Editing the SNMPv2-MIB

About MIBs

Cisco UMG supports SNMP MIBs and traps for monitoring its status. Cisco UMG supports the basic SNMP MIBs and traps:

- SNMPv2-MIB
- IF-MIB
- IP-MIB
- SYSAPPL-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSLOG-MIB

Note The system uses the CISCO-SYSLOG-MIB to convey alert information generated by Cisco UMG. You can filter the syslog records to find Cisco UMG alerts by finding records where clogHistSeverity = “srsx” and clogHistMsgName = “Alerts”. For more information about the log, see Viewing a Log File.

You can identify information about your system by reviewing the object ID. See Table 12 for the SNMPv2-MIB object IDs that describe the system software and Table 13 for the entity object IDs that describe the hardware used. Note that there is currently no way to distinguish between a UMG-NME and a UMG-NME-EC.

These are the expected results from doing an SNMP request or query:

Table 12 SNMPv2 MIB Object IDs

Platform	Description	SysObjectID (OID)
NME	Cisco UMG running on NME. The software version is 8.6.1 and the firmware version is 2.1.36.	.1.3.6.1.4.1.9.1.866
NME-EC	Cisco UMG running on NME. The software version is 8.6.1 and the firmware version is 2.1.36.	.1.3.6.1.4.1.9.1.866
SM-700	Cisco UMG running on an SM-700. The software version is 8.6.1 and the firmware version is 2.1.36.	.1.3.6.1.4.1.9.1.1150
SM-900	Cisco UMG running on an SM-900. The software version is 8.6.1 and the firmware version is 2.1.36.	.1.3.6.1.4.1.9.1.1150

Table 13 Entity MIB Object IDs

Platform	Description	SysObjectID (OID)
NME	Network Module Cisco UMG.	.1.3.6.1.4.1.9.12.3.1.9.2.155
NME-EC	Network Module Cisco UMG.	.1.3.6.1.4.1.9.12.3.1.9.2.155
SM-700	Service Module SRE-700.	.1.3.6.1.4.1.9.12.3.1.9.2.237
SM-900	Service Module SRE-900.	.1.3.6.1.4.1.9.12.3.1.9.2.239

Working With SNMP Community Strings

Communities can either be read-only or read-write only.

Restriction

- You can only define up to five read-only community strings and up to five read-write community strings.

Procedure

Step 1 Select **System** > **SNMP > Communities**.

The system displays the SNMP Communities page.

Step 2 To add an SNMP community string, do the following:

a. In an empty space, enter the SNMP community string. If there are no empty spaces, you must first delete another SNMP community string before you can add a new one. You can only define up to five read-only community strings and up to five read-write community strings.

b. Click **Update**.

Step 3 To edit an existing SNMP community string, do the following:

a. Go to the SNMP community string that you want to edit and edit the name.

b. Click **Update**.

Step 4 To remove an SNMP community string, do the following:

a. Go to the SNMP community string that you want to delete and highlight the name.

b. Click **Delete** on your keyboard.

c. Click **Update**.

Related Topics

- About MIBs

Viewing and Removing an SNMP Trap Host

Procedure

Step 1 Select **System** > **SNMP > Hosts**.

The system displays the SNMP Trap Hosts page.

Step 2 To add an SNMP trap host, click **Add**. See Adding and Editing SNMP Trap Hosts.

Step 3 To edit an SNMP trap host, click the underlined name of the host. See Adding and Editing SNMP Trap Hosts.

Step 4 To remove an SNMP trap host, do the following:

a. Check the check box next to the SNMP trap host.

b. Click **Remove**.

Related Topics

- About MIBs

Adding and Editing SNMP Trap Hosts

If traps are enabled on Cisco UMG, the system sends SNMP traps, as they occur, to the configured SNMP hosts. See also Displaying MIBs.

Before You Begin

Gather the following information:

- The hostname of the SNMP trap host.
- The community string of the SNMP trap host.

Restriction

The hostname that you enter must be found in the DNS.

Procedure

Step 1 Select **System** > **SNMP** > **Hosts**.

The system displays the SNMP Trap Hosts page.

Step 2 To add an SNMP trap host, do the following:

- **a.** Click **Add**. The system displays the SNMP Host Profile page.
- **b.** Enter the hostname and the community string for the SNMP trap.
- **c.** Click **Update**.

Step 3 To edit an existing SNMP trap host, do the following:

- **a.** Click the underlined hostname of the SNMP trap host that you want to edit. The system displays the SNMP Host Profile page.
- **b.** Edit the values for the hostname or the community string for the SNMP trap.
- **c.** Click **Update**.

Related Topics

- About MIBs

Displaying MIBs

Procedure

Step 1 Select **System** > **SNMP** > **MIBs**.

The system displays the SNMP MIBs page listing all the MIBs in your system.

Step 2 To enable the traps for all the SNMP MIBs, do the following:

- **a.** Check **Enable SNMP Traps**.
- **b.** Click **Updates**.

Step 3 To edit the SNMPv2-MIB, click its underlined name. See Editing the SNMPv2-MIB.

Related Topics

- About MIBs

Editing the SNMPv2-MIB

The only MIB that you can edit is the SNMPv2-MIB.

Procedure

Step 1 Select **System** > **SNMP > MIBs**.

The system displays the SNMP MIBs page listing all the MIBs in your system.

Step 2 Click the underlined name of the SNMPv2-MIB.

The system displays the SNMPv2-MIB page.

Step 3 Enter or update the contact or location for the SNMPv2-MIB.

Step 4 Click **Update**.

Related Topics

- About MIBs

Displaying System Information

Last updated: August 5, 2011

The system displays the System Information page with the following information:

Parameter	Description
Module SKU	Unique ordering identifier for a Cisco UMG module.
Module Serial Number	Serial number of the Cisco UMG module.
Chassis Type	Type of chassis of the Cisco UMG module.
Chassis Serial Number	Serial number of the chassis.
Software Version	Version of Cisco UMG software that is running on this system.
Uptime	Amount of time that the Cisco UMG system has been running.
SDRAM	Amount of memory on the Cisco UMG blade.
Disk Size	Hard disk size of the Cisco UMG blade.

About Security for Cisco UMG

Last updated: August 5, 2011

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 Cisco UMG
- Between Cisco UMG and the Cisco Unified SRSV-CUE device at the branch site
- Between Cisco UMG and the Cisco Unified SRST or CUCME-as-SRST device at the branch site

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 Cisco Unified Communications Manager, 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, Cisco UMG needs the security certificate from each device to which it connects.

The TLS security certificate can be represented in one of two formats: 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.

Procedure

Step 1 Log in to the Cisco Unified OS Administration interface.

Step 2 Select **Security > Certificate Management**.

Step 3 Click **Find** to show the certificates.

Step 4 Click the *.pem or *.der link for the desired certificate.

Step 5 Click **Download** to save the certificate to the local file system.

Working With Trusted TLS Certificates

Last updated: August 5, 2011

- Viewing and Removing Trusted TLS Certificates
- Adding a Trusted TLS Certificate
- Viewing a Trusted TLS Certificate

Viewing and Removing Trusted TLS Certificates

Restriction

- Trusted TLS certificates cannot be edited.

Procedure

Step 1 Select **System** > **Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page with the following information:

- Label
- Owner
- Issuer

Step 2 To add a trusted TLS certificate, click **Add**. See Adding a Trusted TLS Certificate.

Step 3 To see more information about a trusted TLS certificate, click the underlined name of the certificate. See Viewing a Trusted TLS Certificate.

Step 4 To remove a trusted TLS certificate, do the following:

a. Check the check box next to the trusted TLS certificate that you want to remove.

b. Click **Remove**.

Related Topics

- Adding a Trusted TLS Certificate
- Viewing a Trusted TLS Certificate

Adding a Trusted TLS Certificate

You can either add a trusted TLS certificate by uploading a file or by uploading text.

Before You Begin

If you will be uploading a file, upload the trusted TLS certificate to a location where you can find it easily.

Restriction

TLS certificates that you paste into the text window must be in PEM format. Certificate files that you upload to Cisco UMG may be in PEM or DER format.

Procedure

Step 1 Select **System** > **Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page.

Step 2 Click **Add**.

The system displays the Add Trusted TLS Certificate page.

Step 3 Enter the keystore label for this trusted TLS certificate. This is a unique identifier for this certificate.

Step 4 Select **Certificate File** if the trusted TLS certificate will be a file or select **Certificate Text** if the certificate will be uploaded as plain text.

Step 5 Do one of the following:

- If you selected Certificate File, click **Browse**. Navigate to the file, highlight it, and click **Open**.
- If you selected Certificate Text, paste the contents of the trusted TLS certificate in the text box.

Step 6 Click **Update**.

Related Topics

- Viewing and Removing Trusted TLS Certificates
- Viewing a Trusted TLS Certificate

Viewing a Trusted TLS Certificate

Procedure

Step 1 Select **System** > **Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page.

Step 2 To see more information about a trusted TLS certificate, click the underlined name of the certificate. The system displays the <*name_of_trusted_TLS_certificate*> TLS Certificate Profile page with the following information:

Parameter	Description
Owner Info	
Common Name (CN)	The X.500 common name attribute, which contains the name of an object. If the object corresponds to a person, it is typically the person’s full name. This is usually the hostname of the server to which you are talking.
Organization (O)	The name of an organization.
Organization (OU)	The name of an organizational unit.
Location (L)	The name of a locality, such as a city, county or other geographic region.
State (ST)	The full name of a state or province.
Country (C)	The country name. A two-letter ISO 3166 country code.
Issuer Info—The entity that verified the information and issued the certificate.	
Common Name (CN)	The X.500 common name attribute, which contains the name of an object. If the object corresponds to a person, it is typically the person’s full name. This is usually the hostname of the server to which you are talking.
Organization (O)	The name of an organization.
Organization (OU)	The name of an organizational unit.
Location (L)	The name of a locality, such as a city, county or other geographic region.
State (ST)	The full name of a state or province.
Country (C)	The country name. A two-letter ISO 3166 country code.
Validity	
Valid From	The date from which the certificate is first valid.
Expires On	The date on which the certificate expires.
Fingerprint	
MD5	The fingerprint (also known as thumbprint) is a cryptographic hash value that uniquely identifies the certificate. The MD5 message-digest algorithm is a widely used cryptographic hash function with a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.

Step 3 To return to the Trusted TLS Certificates page, click **Back to list**.

Related Topics

- Viewing and Removing Trusted TLS Certificates
- Adding a Trusted TLS Certificate

PART 3

Monitoring and Maintaining the System

Monitoring the Learned Cisco Unified Communications Manager Express Routers

Last updated: August 5, 2011

Procedure

Step 1 Select **Monitor > Learned CUCME Routers**.

The system displays the Learned CUCME Routers page listing all the Cisco Unified Communications Manager Express routers that have been added to your Cisco UMG system. For each router, the system lists the following information:

Parameter	Description
Site	Name of the site where the learned Cisco Unified Communications Manager Express device resides.
CUCME IP Address	IP address for the learned Cisco Unified Communications Manager Express device.
Platform	Hardware platform on which the learned Cisco Unified Communications Manager Express site is installed.
CUCME Version	Version of Cisco Unified Communications Manager Express installed.

Step 2 To see a different number of routers on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500, routers.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To filter the list of routers, do the following:

a. Select a filter from the Filter drop-down list.

b. Select a condition from the Match if drop-down list.

c. Enter a keyword.

d. Click **Go**.

e. To clear the values, click **Clear Filter** and click **Go**.

Monitoring the Provisioning Status of a Branch Device

Last updated: August 5, 2011

While the Cisco UMG system is actively provisioning the branch call agent devices or SRSV-CUE devices, you can examine the realtime status of the provisioning process by clicking **Monitor > Provisioning Status**. If you manually started the provisioning cycle, the system automatically displays the provisioning monitor page.

The system automatically refreshes the Provisioning Status page until all the selected sites have finished the provisioning cycle. During this time, you can navigate away from this page and return later to review the updated status. If the provisioning has not finished, the page will display the updated status for individual sites.

- Site—The name of the site being provisioned.
- Progress—The current state of provisioning. Can be one of the following: not started, in progress, or complete.
- Result—Indicates the outcome of the provisioning process for the site. Can be either success or failed.

If the system is not currently provisioning any sites, the system displays an informational message stating this.

Related Topics

- See Viewing the Site Provisioning History Report to learn how to generate the Site Provisioning report.
- See System Alerts for a list of all the alert descriptions.

Monitoring the Voicemail Upload

Last updated: August 5, 2011

You can view the realtime status of a voicemail upload after a WAN outage. Depending upon the duration of the WAN outage, the number of sites affected, and the volume of voicemail messages received at the branch offices during the outage, it can take several minutes for each site to upload all the voicemail messages to the central office Cisco Unity Connection system.

Procedure

Step 1 Select **Monitor > Voicemail Upload Status** to see the upload status for each site.

The system displays the Voicemail Upload Status page.

If the system is not currently uploading voicemail from any sites, the system displays an informational message stating this. Otherwise, the system displays the following information:

Parameter	Description
Branch Voicemail Server	Name of the branch voicemail server.
Site	Name of the site. **Note** The system does not display this field if this is a secondary Cisco UMG.
Progress	The system supports parallel uploading from multiple sites, so the page shows a progress bar indication of the percentage complete for each site.
Total	Total number of messages that must be uploaded to Cisco Unity Connection for the site.
Remaining	Number of remaining messages that have not yet been uploaded to Cisco Unity Connection.
State	The state of the upload. If this value is “Active,” the system is uploading voicemails.

Step 2 To see the results of past voicemail uploads, see the SRSV Activity History report at Viewing the SRSV Activity History Report.

Monitoring the Software Upgrade Status

Last updated: August 5, 2011

You can monitor the status of the sites that you are upgrading.

Procedure

Step 1 Click **Monitor > SRSV Software Upgrade Status.**

The system displays the status of the software upgrade for the SRSV-CUE devices.

If the system is not currently upgrading the software for any SRSV-CUE devices, the system displays an informational message stating this.

Step 2 To stop the page from automatically refreshing the status, click **Pause Auto Refresh**.

Step 3 To cancel the remainder of the software upgrade, click **Cancel Waiting Upgrade Tasks**.

The system stops the upgrade, but any sites that have already been upgraded will remain upgraded.

Related Topics

- See Managing the Branch Voicemail Server Software to learn how to start the software upgrade process.

Monitoring the System

Last updated: August 5, 2011

- Monitoring the System Resources: CPU
- Monitoring the System Resources: Memory

Monitoring the System Resources: CPU

The following graphs display the percentage of CPU resources that your system uses. Use this information to help diagnose and prevent system problems.

Tip If your system is using too much CPU, you can turn down or turn off the trace log (see Configuring Trace Settings), or you can go into the CLI to turn down or turn off the SIP message log or the peg count log.

Restriction

Your system must have Adobe Flash Player Release 9 or later installed to see the graphs.

Procedure

Step 1 Choose **Monitor** > **System Resources** > **CPU**.

The system displays the System Resource Utilizations page that contains three graphs showing the following:

- CPU use by percentage per second for the past 60 seconds
- CPU use by percentage per minute for the past 60 minutes
- CPU use by percentage per hour for the past 72 hours

Tip If you cannot see all graphs, scroll down.

For each graph, the system displays the percentage of CPU use on the vertical scale and the time across the horizontal scale.

For the second and third graphs, the system also displays the average CPU use.

Monitoring the System Resources: Memory

These graphs display the amount of memory that your system uses.

Restriction

Your system must have Adobe Flash Player Release 9 or later installed to see the graphs.

Procedure

Step 1 Choose **Monitor** > **System Resources > Memory**.

The system displays the System Memory Utilizations page that contains three graphs showing the following:

- Memory utilization for the past 60 seconds
- Memory utilization for the past 60 minutes
- Memory utilization for the past 72 hours

Tip If you cannot see all graphs, scroll down.

For each graph, the system displays the amount of memory used, measure in kilobytes, on the vertical scale and the time across the horizontal scale.

Maintaining the Cisco UMG System

Last updated: August 5, 2011

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

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: *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 (e.g. ftps://server/dir/filename)
tftp:*tftp-server-url*	URL of the TFTP server including directory and filename (e.g. tftps://server/dir/filename)

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@ftps://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? tftps://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@ftps://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@tftps://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:tftps://***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**} **tftps:**//*server/dir/filename*

Syntax Description

running-config	Active configuration on hard disk.
startup-config	Startup configuration on hard disk.
tftp-server-url	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? tftps://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 155
- Restarting the Cisco UMG System, page 156
- Shutting Down the Cisco UMG System, page 157

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** command 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

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 157
- Shutting Down the Hardware, page 157

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.

Viewing Reports

Last updated: August 5, 2011

Viewing the Alert History Report

The Alert History Report displays a list of all system alert messages that have occurred on the system. The alerts include critical, error, warning, and informational messages, and are in chronological order by alert level. You can filter the alerts by using the check boxes at the top of the report.

Procedure

Step 1 Select **Reports** > **Alert History**.

The Alert History Report contains the following fields:

- Level—Alert level. Can be critical, error, warning, or informational.
- System—The system originating the alert message.
- Date and Time—Date and time when the system created the alert.
- Description—Description of the alert. See System Alerts for a list of all the alerts.
- Help—Additional information about the alert. To see the details, click **details**.

Step 2 To see a different number of alerts on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 alerts.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To delete all of the alerts, click **Delete Alert History**.

System Alerts

The following tables list all the alerts:

- Table 1: System Alerts – Warnings
- Table 2: System Alerts – Errors
- Table 3: System Alerts – Informational Messages

Table 1 System Alerts – Warnings

Alert Name	Description
CallHandlerDeleted	The default call handler for this site was deleted from the Cisco Unity Connection.
CcmFailoverToSecondary	The primary central call agent was unavailable for provisioning, but the secondary central call agent was successfully utilized.
CucFailoverToSecondary	The primary central voicemail server was unavailable for provisioning, but the secondary central voicemail server was successfully utilized.
CcmUnreachableForProvisioning	The Cisco UMG was unable to pull provisioning information from the configured telephony service server because it could not be reached on the network. Typically telephony service is provided by a central call agent like Cisco Unified Communications Manager.
CucUnreachableForProvisioning	The Cisco UMG was unable to pull provisioning information from the configured central voicemail server because it could not be reached on the network. Typically voicemail service is provided by a central voicemail server like Cisco Unity Connection.
CucUnreachableForVoicemailUpload	The Cisco UMG was unable to deliver voicemail to the provisioned central voicemail server that it received from the Cisco UMG system because it could not contact the central voicemail server. Typically voicemail service is provided by a central voicemail server like Cisco Unity Connection.

Table 1 System Alerts – Warnings (continued)

Alert Name	Description
ProvisioningCycleSuspended	The Cisco UMG has suspended the process of provisioning remote sites based on the central site configuration.
SiteProvisioningSkipped	Provisioning for a site was skipped due to incomplete configuration. Possible causes for the failure include: • Site was not assigned a central voicemail server • Site was not assigned an SRSV-CUE device
SrstCSSNameConflictFound	A name conflict was found for Cisco Unified Communications Manager Calling Search Space names when applied to the Cisco Unified Communications Manager Express class of restriction lists.
SrstDialPeerMatchingToCUCMRoutePatternNotFound	Unable to find a matching dial peer to a Cisco Unified Communications Manager route pattern.
SrstLongHuntGroupChainFound	Hunt group configuration: Unable to configure long hunt pilot.
SrstMultipleTimeZonesFound	Multiple time zones for a site were found on the central Cisco Unified Communications Manager.
SrstPartitionNameConflictFound	A name conflict was found for Cisco Unified Communications Manager partition names when applied to the Cisco Unified Communications Manager Express class of restriction names.
SrstTimeBasedPartitionsDayOfMonthLimitReached	After hours configuration: The Cisco UMG was unable to add more day of month schedules because the Cisco Unified Communications Manager Express time-based-partitions day of month limit has been reached.
SrstVMDialPeerConfigurationSkipped	The voicemail dial peer configuration was skipped because the Cisco UMG was unable to get the SRSV-CUE IP address for the site.
SrstVMPilotConfigurationFailed	The voicemail pilot configuration was skipped because the Cisco UMG was unable to provision the voicemail pilot number.
SrsvNoUpgradeImage	No upgrade image found on Cisco UMG. Upload an SRSV-CUE upgrade image bundle on this Cisco UMG and try again.

Table 1 System Alerts – Warnings (continued)

Alert Name	Description
SrsvProvisioningWarnings	Provisioning of a remote Cisco Unified SRSV site has some anomalies. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco Unified SRSV aggregated into a single alert.
SrsvUnreachableForProvisioning	The Cisco UMG was unable to provision an SRSV-CUE device because it was unable to create a connection to the device.
SrsvUpgradeConflict	The SRSV-CUE device upgrade was aborted because of one of the following reasons: • Another upgrade or install was already active. • There are active calls on the system. • The SRSV-CUE is uploading messages after a failover. This error will probably be resolved by the next upgrade attempt. If this problem persists, try manually installing the SRSV-CUE image.
SrsvUpgradeImageMissing	The SRSV-CUE upgrade image was not uploaded properly to the SRSV-CUE device. Check the network connection between the Cisco UMG and the SRSV-CUE device.
SrsvUpgradeSkipped	The SRSV-CUE device could not be upgraded because a requirement was not met, such as the Cisco Unified SRSV does not exist or needs to be upgraded.
SrsvUpgradeUnsupported	The SRSV-CUE device does not meet the minimum version requirement. Manually upgrade the SRSV-CUE device to at least Release 8.6.1 and try again.
TlsCredentialExpired	A TLS credential on the Cisco UMG has expired.
UmgProvisioningWarnings	Provisioning of the secondary Cisco UMG has some anomalies. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco UMG aggregated into a single alert.

Table 1 System Alerts – Warnings (continued)

Alert Name	Description
UmgUnreachableForProvisioning	The Cisco UMG was unable to provision a secondary Cisco UMG because it was unable to create a connection to the device. Possible causes for the failure include Cisco UMG REST authentication, TLS configuration, or a network problem.

Table 2 System Alerts – Errors

Alert Name	Description
CcmGlobalDataRetrievalFailure	The Cisco UMG was unable to update the global Cisco Unified SRST data from Cisco Unified Communications Manager. See the logs for more details.
CcmProvisiningFail	The Cisco UMG could not provision because of a communications problem with the central call agent.
CcmProvisioningFailAuth	The Cisco UMG could not provision because of bad central call agent AXL credentials. Update the AXL username and password for the central call agent and try again.
CcmProvisioningFailTls	The Cisco UMG could not provision because of a bad central call agent public TLS certificate. Add the central call agent's TLS certificate to the Cisco UMG and try again.
CcmSrstReferenceDataRetrievalFailure	The Cisco UMG was unable to update site-specific Cisco Unified SRST data from Cisco Unified Communications Manager. See the logs for more details.
CucProvisioningFail	The Cisco UMG could not provision because of a communications problem with the central voicemail server.
CucProvisioningFailAuth	The Cisco UMG could not provision because of bad central voicemail server REST credentials. Update the REST username and password for the central voicemail server and try again.
CucProvisioningFailTls	The Cisco UMG could not provision because of a bad central voicemail server public TLS certificate. Add the central voicemail server's TLS certificate to the Cisco UMG and try again.

Table 2 System Alerts – Errors (continued)

Alert Name	Description
CucUploadFail	The Cisco UMG could not upload voicemail because of a communications problem with the central voicemail server.
CucUploadFailAuth	The Cisco UMG could not upload voicemail because of bad central voicemail server REST credentials. Update the REST username and password for the central voicemail server.
CucUploadFailTls	The Cisco UMG could not upload voicemail because of a bad central voicemail server public TLS certificate. Add the central voicemail server's TLS certificate to the Cisco UMG.
LocalhostDnsFailure	The Cisco UMG host cannot be resolved by the DNS server.
RestUriRejectedBadCredentials	Bad credentials were provided to the Cisco UMG for a REST configuration request that was rejected.
RestUriRejectedMalformed	A REST request was received that could not be decoded by the Cisco UMG. This could be an indication that the client has a different version of the REST interface than the Cisco UMG.
RestUriRejectedUntrustedCertificate	An untrusted certificate was provided to the Cisco UMG for a REST configuration request that was rejected.
SrstAfterHoursBlockPatternFailed	The after-hours configuration was unable to configure some after hours block patterns. See the logs for more details.
SrstAfterHoursConfigurationFailed	The after-hours configuration failed. See the logs for failure details.
SrstCallParkConfigurationFailed	One or more errors were seen while trying to configure call park entries. See the logs for more details.
SrstCcpDiscoveryFailure	The Cisco UMG was unable to do configuration discovery for the Cisco Unified SRST site. See the logs for more details.
SrstCMENotSupportedFailure	Cisco Unified Communications Manager Express voice is not supported on the router. Check the router version and image.
SrstCreateDnFailure	The Cisco UMG was unable to create the DN in Cisco Unified SRST. See the logs for more details.

Table 2 System Alerts – Errors (continued)

Alert Name	Description
SrstCreateExternalCallRoutingFailure	The Cisco UMG was unable to create the external call routing configuration in Cisco Unified SRST.
SrstCreatePhoneFailure	The Cisco UMG was unable to create a phone in Cisco Unified SRST. See the logs for more details.
SrstCreateSoftkeyTemplateFailure	The Cisco UMG was unable to create a softkey template in Cisco Unified SRST. See the logs for more details.
SrstCreateSpeedDialFailure	The Cisco UMG was unable to create speed dial in Cisco Unified SRST. See the logs for more details.
SrstCreateTranslationRulesFailure	The Cisco UMG was unable to create translation rules in Cisco Unified SRST.
SrstDeleteDnFailure	The Cisco UMG was unable to delete the DN in Cisco Unified SRST. See the logs for more details.
SrstDeleteExternalCallRoutingFailure	The Cisco UMG was unable to delete the external call routing configuration in Cisco Unified SRST.
SrstDeletePhoneFailure	The Cisco UMG was unable to delete a phone in Cisco Unified SRST. See the logs for more details.
SrstDeleteSokftKeyTemplateExceeded	The maximum number of configured softkey templates was exceeded.
SrstDeleteSokftKeyTemplateFailure	The Cisco UMG was unable to delete the softkey template in Cisco Unified SRST. See the logs for more details.
SrstDeleteSpeedDialFailure	The Cisco UMG was unable to delete speed dial in Cisco Unified SRST. See the logs for more details.
SrstDeleteTranslationRulesFailure	The Cisco UMG was unable to delete translation rules in Cisco Unified SRST.
SrstFetchingCcmSRSTConfigurationFailure	The Cisco UMG was unable to fetch the Cisco Unified SRST configuration from Cisco Unified Communications Manager. See the logs for more details.
SrstFetchingHardwareConfigurationFailure	The Cisco UMG was unable to provision the site because it was unable to get hardware information for the site. See the logs for more details.
SrstFetchingMappingConfigurationFailure	The Cisco UMG was unable to fetch the Cisco Unified SRST mapping configuration from the database. See the logs for more details.

Table 2 System Alerts – Errors (continued)

Alert Name	Description
SrstFetchingPlatformInformationFailure	The Cisco UMG was unable to provision the site because it was unable to get hardware platform information based on the hardware. Ensure that this hardware is supported.
SrstFetchingSRSTConfigurationFailure	The Cisco UMG was unable to fetch the Cisco Unified SRST configuration from the router. See the logs for more details.
SrstFetchingTelephonyConfigurationFailure	The Cisco UMG was unable to fetch the telephony configuration from the router. See the logs for more details.
SrstFetchTranslationRulesFailure	The Cisco UMG was unable to fetch translation rules from Cisco Unified SRST.
SrstHuntGroupConfigurationFailed	The hunt groups configuration failed. See the logs for failure details.
SrstHuntGroupLongPilotFound	The hunt group configuration was unable to configure a long-chained hunt pilot.
SrstInvalidDateFormatFound	The Cisco UMG was unable to provision the date format because an invalid or unsupported date format was found.
SrstInvalidTimeZoneFound	The Cisco UMG was unable to provision the time zone because an invalid or unsupported time zone was found.
SrstMaxConfiguredCoRExceeded	The maximum configured class of restrictions was exceeded.
SrstMaxConfiguredPhoneExceeded	The number of maximum configured phones was exceeded.
SrstMaxConfiguredSpeedDialsExceeded	The maximum configured speed dials was exceeded in the phone.
SrstMaxConfiguredDnExceeded	The number of maximum configured DNs was exceeded.
SrstMultipleExternalPhoneNumMaskFound	Multiple external phone number masks were found in Cisco Unified Communications Manager.
SrstMultipleTimeBasedPartitionsFound	The after-hours configuration was unable to configure a site because multiple time-based partitions were found on Cisco Unified Communications Manager.
SrstMultipleVMPilotsFound	Multiple voicemail pilots for a site were found on Cisco Unified Communications Manager.
SrstNodeLicenseAllocationFailure	A Cisco Unified SRST node license was not available. Ensure that the licenses are current and try again.

Table 2 System Alerts – Errors (continued)

Alert Name	Description
SrstPickupGroupConfigurationFailed	One or more errors was seen while trying to configure pickup group entries. See the logs for more details.
SrstProvisioningFailed	The Cisco UMG was unable to provision a Cisco Unified SRST site. See the logs for more details.
SrstRouterModeDetectionFailure	The Cisco UMG was unable to detect the router properties. See the logs for more details.
SrstSystemInSRSTModeFailure	The Cisco UMG was unable to provision a site because the site is in Cisco Unified SRST mode. Remove the “call-manager-fallback” configuration and try again.
SrstUnsupportedCMEVersionFailure	The Cisco UMG was unable to provision the site because the version of Cisco Unified Communications Manager Express found is unsupported. Check the router version and image.
SrstUpdateDnFailure	The Cisco UMG was unable to update the DN in Cisco Unified SRST. See the logs for more details.
SrstUpdatePhoneFailure	The Cisco UMG was unable to update a phone in Cisco Unified SRST. See the logs for more details.
SrstVMConfigurationFailed	The voicemail configuration was skipped due to failures. See the logs for failure details.
SrstWritingMappingConfigurationFailure	The Cisco UMG was unable to write the Cisco Unified SRST mapping configuration to the database. See the logs for more details.
SrsvCorruptUpgradeImage	The upgrade was aborted because the SRSV-CUE device upgrade image is corrupt. Upload the SRSV-CUE upgrade image bundle to the Cisco UMG again.
SrsvNodeCreateFailed	An attempt to provision a new Cisco UMG node on the Cisco UMG failed because the license limit for adding Cisco UMG nodes has been reached. **Note** A Cisco UMG node is any supported survivable remote site voicemail system configured to be provisioned by the Cisco UMG such as an SRSV-CUE device.

Table 2 System Alerts – Errors (continued)

Alert Name	Description
SrsvNodeLicenseAllocationFailure	A Cisco Unified SRSV node license was not available. Ensure licenses are current and try again.
SrsvProvisioningFailed	Provisioning of a remote Cisco UMG site has failed. Possible causes for the failure include: • Cisco Unified SRSV REST authentication problem • Version mismatch • Cisco UMG license problem
SrsvUpgradeAuthError	The Cisco UMG could not start the upgrade because SRSV-CUE device could not authenticate the Cisco UMG. This is most likely a result of out-of-sync Cisco Unified SRSV secrets. Reregister the SRSV-CUE device with Cisco UMG and try again.
SrsvUpgradeFailed	The Cisco Unified SRSV upgrade did not complete successfully. Depending on the upgrade error, the Cisco Unified SRSV may require immediate attention to get it operational if the upgrade failure corrupted the installed image.
TlsCredentialSigningFailed	There was a failed TLS credential signing request to an external SCEP certificate authority.
TlsCredentialSigningTimeout	There was a failed TLS credential signing request to an external SCEP certificate authority because the certificate authority never completed the transaction and returned the signed credentials.
UmgProvisioningFailed	Problems were encountered while provisioning the secondary Cisco UMG. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco UMG aggregated into a single alert.
UmgSecretSyncFailed	The secondary Cisco UMG secrets may be stale. The secondary Cisco UMG will not operate properly for voicemail upload until with old secrets. Check network and TLS configuration. If no problems are found, manually correct the secrets on the secondary Cisco UMG.

Table 2 System Alerts – Errors (continued)

Alert Name	Description
VoicemailMessageUploadRejected	The Cisco UMG was unable to deliver voicemail that it received from Cisco UMG systems to the provisioned central voicemail server because the central voicemail server rejected the message. Typically voicemail service is provided by a central voicemail server like Cisco Unity Connection.

Table 3 System Alerts – Informational Messages

Alert Name	Description
NewSrstReferenceDetected	A new Cisco Unified SRST reference has been detected on the central telephony server (typically Cisco Unified Communications Manager). This could be an indication of a new Cisco UMG site to prepare.
ProvisioningCycleComplete	Completed the process of provisioning remote sites based on the central site configuration.
ProvisioningCycleResuming	Restarted the process of learning of any configuration changes from the central site to complete the configuration that must be pushed down to SRSV-CUE devices on a remote site.
ProvisioningCycleStarted	Starting the process of learning of any configuration changes from the central site that must be pushed down to SRSV-CUE devices on a remote site.
SrsvDeviceRegistered	An SRSV-CUE device has registered with the Cisco UMG and is available to be configured.
SrsvNoUpgradeRequired	The software installed on the SRSV-CUE device is at or above the target software version. If an upgrade is desired, upload a newer SRSV-CUE upgrade image bundle to the Cisco UMG.
SrsvProvisioningInfo	This message is an indication that provisioning of a remote Cisco Unified SRSV site has some additional information to convey. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco Unified SRSV aggregated into a single alert.
SrsvUpgradeSuccess	The Cisco Unified SRSV upgrade completed upgrading to a newer image.
TlsCredentialRenewed	A TLS credential on the Cisco UMG has expired but has been automatically renewed through a SCEP certificate authority.

Table 3 System Alerts – Informational Messages (continued)

Alert Name	Description
UmgProvisioningInfo	This message is an indication that provisioning of the secondary Cisco UMG has some additional information to convey. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco UMG aggregated into a single alert.

Related Topics

- About the Cisco UMG Dashboard

Viewing the Site Provisioning History Report

The Site Provisioning History Report shows the results of the most recent and last successful site provisioning cycle. These results cannot be cleared or deleted.

Procedure

Step 1 Select **Reports** > **Site Provisioning History**.

The Site Provisioning History Report contains the following fields:

- Site—The site name. The report displays every site known to the Cisco UMG device.
- Last Attempt—Indicates the outcome of the most recent provisioning attempt made by the Cisco UMG device for that site. Results can include never, success, failed, or disabled.
  - “Never” indicates that the site has never been provisioned. The site may be newly created and neither the manual nor scheduled provisioning has occurred yet.
  - “Disabled” indicates that the site was administratively disabled for provisioning during the last provisioning cycle. You can enable a disabled site on the Site Profile page. See Changing the Information for a Single Cisco Unified SRST Site.
  - If the last attempt field is set to “Failed,” the system displays the date and time of the failure, and generates an alert. The system also increments the failed provisioning status count on the dashboard. To see the alert details, click **Reports > Alert History**.

  Note Site provisioning failures are severe. We recommend that you correct the failure as soon as possible by reviewing the corresponding alert.

- Date and Time—The date and time of the last provisioning attempt. This field is blank if the Last Attempt field is Never or Disabled.
- Last Successful—Indicates the last time that the Cisco UMG device successfully provisioned the branch device. Can be either “Success” or “Never.”
- Date and Time—If the status of the Last Successful field is Success, the report shows the date and time (relative to the branch device) when the successful provisioning was completed.

- Voicemail Subscribers—Displays the number of subscribers that have been provisioned on the SRSV-CUE device by the Cisco UMG device. This number should be consistent with the number of Cisco Unity Connection voicemail subscribers located at the site.

Note Voicemail subscriber data is shown only if SRSV is enabled on the site.

- Ephones Controlled—Displays the number of ephones being controlled by the CUCME-as-SRST device. The number should be consistent with the number of ephones provided by Cisco Unified Communications Manager.

Note Ephone data is shown only if E-SRST is enabled on the site.

Step 2 To see a different number of sites on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 sites.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To filter by status, such as success, failed, or never, check the check box next to a status and click **Go**.

Related Topics

- About the Cisco UMG Dashboard
- Monitoring the Provisioning Status of a Branch Device
- Viewing and Provisioning Sites

Viewing the SRSV Activity History Report

The SRSV Activity History Report shows all voicemail upload activity that occurs from each SRSV-CUE device.

Procedure

Step 1 Select **Reports > SRSV Activity History**.

The SRSV Activity History Report contains the following fields:

- Branch Voicemail Server—The hostname of the SRSV-CUE device that uploaded voicemail messages.
- Total Voicemails—The total number of voicemail messages uploaded from the SRSV-CUE device.
- Undeliverable—The number of voicemails that could not be delivered because they were sent to an unknown voicemail subscriber.
- Start Date and Time—The date and time that the voicemail upload began.
- End Date and Time—The date and time that the voicemail upload ended.

Step 2 To view the activity for all SRSV-CUE devices, click **Expand All**. To view the activity for a specific SRSV-CUE device, click **Collapse All** and choose a device from the down arrow.

Step 3 To see a different number of SRSV-CUE devices on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or 500 SRSV-CUE devices.

Step 4 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 5 To delete the activity history, click **Delete Activity History**.

Related Topics

- About the Cisco UMG Dashboard
- Monitoring the Voicemail Upload

Viewing the Backup History Report

Procedure

Step 1 Select **Reports** > **Backup History**.

If there is any backup history to report, the Backup History report contains the following fields:

- ID—ID of the backup.
- Server URL—The server where the backup history is stored.
- Backup Time and Date—Date and time when the system was last backed up.
- Version—The version of the Cisco UMG software that is installed.
- Description—A description of the backup.
- Result—Displays the status of the last backup procedure for system configuration information and for data. Values can be either Success or Fail.

Step 2 To see a different number of backup reports on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all backup reports.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To sort backup reports, click any of the headers.

Related Topics

- Configuring Backup and Restore

Viewing the Restore History Report

The Restore History report shows the history of all the restore processes done on the current system since installation.

Procedure

Step 1 Select **Reports** > **Restore History**.

If there is any restore history to report, the Restore History report contains the following fields:

- ID—ID of the restore.
- Server URL—The server where the restore history is stored.
- Restore Time and Date—Date and time when the system was last backed up.
- Version—The version of the Cisco UMG software that is installed.
- Result—Status of the last restore procedure. Result shows Success or Fail for the components that were restored.

Step 2 To see a different number of restore history reports on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all restore history reports.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To sort restore history reports, click any of the headers.

Related Topics

- Configuring Backup and Restore

Viewing the Network Time Protocol Report

Procedure

Step 1 Choose **Reports** > **Network Time Protocol**.

The system displays the Network Time Protocol Report with the following fields:

- #—The prioritized number of the NTP server. The system attempts to synchronize its time starting with NTP server number one.
- NTP Server—IP address or hostname of the NTP server.
- Status—Indicates if the NTP server connected with the Cisco UMG system or if it was rejected.
- Time Difference (secs)—Time offset between the NTP server and the client.
- Time Jitter (secs)—Estimated time error of the system clock, measured as an exponential average of RMS time differences.

Related Topics

- Working With Network Time and Time Zone Settings

Backing Up and Restoring Data

Last Updated: August 5, 2011

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)

Two types of backup requests are available: data and configuration only. You can choose one or both.

- 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).

Backups are performed only in offline mode. The system displays a message before performing the backup alerting you that the system will be taken offline.

Cisco UMG automatically numbers and dates the backup files. 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.

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.

Restrictions for Backing Up and Restoring Data

- Both the backing up and restoring functions require that the system be in 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.

Configuring Backup and Restore

Last updated: August 5, 2011

- Configuring the Backup Server
- Manually Starting a Backup
- Viewing and Removing Scheduled Backups
- Adding a Scheduled Backup
- Disabling Scheduled Backups
- Starting a Restore

Configuring the Backup Server

Before you begin the backup process, set the backup configuration parameters.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Configuration**.

The system displays the Backup / Restore Configuration page.

Step 2 Enter the information shown in the following fields:

- Server URL—The URL of the server on the network where the backup files are stored. The format should be *ftp://<server/directory>/* where <*server/directory*> is the IP address or hostname of the server.
- User ID—The account name or user ID on the backup server. You must have an account on the system to which you are backing up your data. Do not use an anonymous user ID.
- Password—The password for the account name or user ID on the backup server.
- Maximum revisions—The maximum number of revisions of the backup data that you want to keep on the server. The maximum number is 50. The default value is 5.

Step 3 Click **Apply** to save the information.

Manually Starting a Backup

Before You Begin

- Configure the server used to back up the data. See Configuring the Backup Server.
- Save your Cisco UMG configuration. See Saving and Reloading the Cisco Unified Messaging Gateway Configuration.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Start Backup**.

The system displays the Backup / Restore Start Backup page and automatically generates a backup ID. The backup ID increases by 1 every time you back up the server.

Step 2 Enter a description of the backup file; for example, “backupdata6-2-11.”

Step 3 Check the check box for the types of data that you want to save. You can choose one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves your application data.

Step 4 Click **Start Backup**.

Step 5 Click **OK** at the confirmation message.

Viewing and Removing Scheduled Backups

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Scheduled Backups**.

The system displays the Backup / Restore Scheduled Backups page with the following information:

- Name
- Description
- Schedule
- Next Run
- Categories of backup (type of data to save)

Step 2 To see a different number of scheduled backups on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all scheduled backups.

Step 3 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 4 To sort scheduled backups, click any of the headers.

Step 5 To modify an existing scheduled backup, click the underlined schedule name, edit the parameters, and click **Apply**.

Step 6 To add a new scheduled backup, click **Schedule Backup**. See Adding a Scheduled Backup.

Step 7 To disable all existing scheduled backups, which means that the system ignores all scheduled backups and does not collect any backup data, click **Bulk Disable**. See Disabling Scheduled Backups.

Note Disabling scheduled backups allows you to temporarily turn off backups without deleting the backup schedule.

Step 8 To remove a scheduled backup, do the following:

a. Check the check box next to the name of the backup.

b. Click **Delete**.

c. Click **OK** at the confirmation message.

Adding a Scheduled Backup

You can configure scheduled backups to occur once or recurring jobs that repeat:

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

Before You Begin

You must do the following before starting a backup:

- Configure the server used to back up the data. See Configuring the Backup Server.
- Save your Cisco UMG configuration. See Saving and Reloading the Cisco Unified Messaging Gateway Configuration.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Scheduled Backups**.

The system displays the Backup / Restore Scheduled Backups page.

Step 2 Click **Schedule Backup**.

The system displays the Backup / Restore Scheduled Backups page.

Step 3 Enter a name for the scheduled backup.

Step 4 Enter a description of the scheduled backup; for example, “backupdata6-2-11.”

Step 5 Check the checkbox for the type of data that you want to save. You can choose one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves your application data messages.

Step 6 Select whether the scheduled backup will occur:

- Once
- Daily

- Weekly
- Monthly
- Yearly

Step 7 Select whether the scheduled backup will start:

- Immediately
- On a specific date and time. If you choose this option, enter the date and time.

Step 8 Click **Add**.

Step 9 If you choose Immediately, the system displays a message stating that running a backup will put the system in offline mode and disable management interfaces. Click **OK** to continue.

Disabling Scheduled Backups

Procedure

Step 1 Select **Administration** > **Backup/Restore** > **Scheduled Backups**.

The system displays the Backup / Restore Scheduled Backups page listing all the backups that are scheduled.

Step 2 To disable a single scheduled backup, do the following:

a. Click the underlined name of the scheduled backup. The system displays the Scheduled Backups page with information about this scheduled backup.

b. Click the **Disabled** check box.

c. Click **Apply**.

Step 3 To disable all scheduled backups, do the following:

a. Click **Bulk Disable**. The system displays the Scheduled Backups page with disabling information.

b. Select **Disabled Range** and enter a date range for when the scheduled backups will be disabled.

c. Click **Apply**.

Step 4 To enable.

Starting a Restore

After you have backed up your configuration and data, you can restore it for every new installation or upgrade.

Restriction

After you perform a restore, you cannot run the Setup Wizard.

Before You Begin

Configure a backup server. See Configuring the Backup Server.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Start Restore**.

The system displays the Backup / Restore Start Restore page with the following fields:

- Backup ID—The backup ID of previous backups.
- Version—Version
- Description—Name of this backup.
- Backup Time and Date—Date and time when this backup was made.
- Categories—The type of data that you want to restore.

Step 2 Select the row containing the configuration that you want to restore.

Step 3 Check the check box for the type of data that you want to save. You can choose one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves your application data.

Step 4 Click **Start Restore**.

Backing Up and Restoring Data Using the CLI

Last Updated: August 5, 2011

Backup and Restore Using SFTP

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 sftp://*hostname*/*directory*.

Step 3	**end**
	Example:
	`umg-1(config)# end`
		Returns to privileged EXEC mode.

Backup Server Authentication Using a SSH Host Key

- Overview, page 183
- Configuring Backup Server Authentication Without Using the SSH Host Key, page 185
- Configuring Backup Server Authentication Using the SSH Host Key, page 186

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.

	Command or Action	Purpose

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 knowhost**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `umg-1# config t`	Enters configuration mode.

	Command or Action	Purpose
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: *host* — 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. *fingerprint-string* — MD5 fingerprint string.

Step 3	**end**
	Example:
	`umg-1(config)# end`
		Returns to privileged EXEC mode.

Step 4	**show security ssh knownhost** **Example:** `umg-1(config)# show security ssh knownhost`	Displays a list of configured SSH servers and their fingerprints.

Encrypting and Signing of Backup Content on the Server

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.

Saving and Reloading the Cisco Unified Messaging Gateway Configuration

Last updated: August 5, 2011

Restriction

Reloading the system terminates all user sessions and lose all unsaved data.

Procedure

Step 1 Select **Administration** > **Control Panel**.

The system displays the Administration Control Panel page.

Step 2 To save the current configuration, do the following:

a. Click **Save Configuration**.

b. If the system displays a warning or confirmation message, click **OK**.

Step 3 To reload the saved configuration, do the following:

a. Click **Reload**. The system displays a warning message stating that this will terminate all user sessions and you will lose any unsaved data.

b. Click **OK**.

Displaying Cisco UMG License Information

Last updated: August 5, 2011

Procedure

Step 1 Select **Administration > Licenses**.

The system displays the Licenses page with the following information:

- Product ID—The type of hardware on which the Cisco UMG system resides.
- Serial Number—The serial number for the hardware on which the Cisco UMG system resides.
- Feature—The installed license feature.
- Description—Description of the license.
- Type—Type of license, either permanent or evaluation.
- State—State of the license. Can be one or more of active, inactive, in use, or not in use.
- Priority—Priority of the license, either high, medium, or low.
- Usage—Number of licenses that are being used.
- Validity left—Number of days left that the license is valid. Applies to evaluation licenses only.

PART 4

Troubleshooting

Troubleshooting Using the GUI

Last updated: August 5, 2011

- Running a Network Connectivity Test
- Viewing Results from a Network Connectivity Test
- Configuring Trace Settings
- Viewing Tech Support Information
- Viewing a Trace Buffer
- Viewing a Log File

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 secondary Cisco UMG, the central call agent, central voicemail servers, Cisco Unified 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 Select **Troubleshoot** > **Network Connectivity**.

The system displays the Network Connectivity Test page.

Step 2 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. See Viewing Results from a Network Connectivity Test. 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 3 To cancel the network connectivity test that is currently running, click **Cancel Network Connectivity Test**.

Step 4 To see the results of previous network connectivity tests, click **Click here for results of previously run test**. The system displays the results. See Viewing Results from a Network Connectivity Test.

Note Results of previous tests are only available for the current login session.

Step 5 To restart a previous network connectivity test, click **Restart Network Connectivity Test**.

Viewing Results from a Network Connectivity Test

After you run a network connectivity test (see Running a Network Connectivity Test), the system displays the results.

Parameter	Description
Central Call Agents	
Cluster Name	Name of the central call agent cluster.
Hostname	Hostname of the central call agent to which the Cisco UMG system tried to connect.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.
Central Voicemail Servers	
Cluster Name	Name of the central voicemail server cluster.
Hostname	Hostname of the central voicemail server to which the Cisco UMG system tried to connect.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.
Branch Voicemails Servers	
Hostname	Hostname of the branch voicemail server to which the Cisco UMG system tried to connect.
Port	The IP port number used by the connectivity test to see if the branch voicemail server is reachable. Can be 80 for HTTP or 443 for HTTPS.
Type	The type of port. Can be either HTTP or HTTPS.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.
Branch Call Agents	

Parameter	Description
Hostname	Hostname of the branch call agent to which the Cisco UMG system tried to connect.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.
Secondary Cisco UMG	
Hostname	Hostname of the secondary Cisco UMG to which the primary Cisco UMG system tried to connect.
Port	The IP port number used by the connectivity test to see if the secondary Cisco UMG is reachable. Can be 80 for HTTP or 443 for HTTPS.
Type	The type of port. Can be either HTTP or HTTPS.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.

Configuring Trace Settings

Use this procedure to enable traces, or debug message output, for components in the Cisco Unified SRSV system. Components are modules, entities, and activities in the system. You can review the output by selecting **Troubleshoot > View > Trace Buffer**. See Viewing a Trace Buffer.

Restriction

Enabling too many traces can adversely affect the system performance.

Procedure

Step 1 Select **Troubleshoot** > **Traces**.

The system displays the Traces page, with a hierarchical listing of the system components.

Step 2 To enable a trace on a system component, check the check box next to the name of the component.

Step 3 To expand the listing of components, click the + sign next to the upper-level components.

Step 4 Check the check box next to an upper-level component (a module or entity) to enable the traces for all of the components under that component. Uncheck the check box next to an upper-level component to disable the traces for all of the components under that component.

Step 5 Click **Apply** to save your changes.

Step 6 Click **OK** in the confirmation window.

Viewing Tech Support Information

Procedure

Step 1 Select **Troubleshoot > View > Tech Support**.

The system displays the Tech Support page and shows a collection of configuration data.

Step 2 To save the tech support information, do the following:

a. Click **Download Tech Support**.

b. Save the file to a convenient location.

Viewing a Trace Buffer

Procedure

Step 1 Select **Troubleshoot > View > Trace Buffer**.

The system displays the Trace Buffer page and shows the contents of the trace buffer.

Step 2 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 3 To save the trace buffer information, do the following:

a. Click **Download Trace Buffer**.

b. Save the file to a convenient location.

Step 4 To clear the trace buffer information, do the following:

a. Click **Clear Trace Buffer**.

b. Click **OK** at the confirmation message.

Viewing a Log File

Procedure

Step 1 Select **Troubleshoot > View > Log File**.

The system displays the Log File page and shows the contents of the log file.

Step 2 To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

Step 3 To save the log file, do the following:

a. Click **Download Log File**.

b. Save the file to a convenient location.

Troubleshooting Using the CLI

Last updated: August 5, 2011

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.

Log and Trace Files

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.

For a detailed list of all the arguments associated with the **trace** command, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions*.

Note Logs for E-SRST are turned on by default. Logs for Cisco Unified 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 trace

- **log trace local enable**
- **log trace server enable**
- **log trace server url** *ftp-url*

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.

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 trace, page 296.

PART 5

CLI Reference Information

How to Use the Cisco UMG CLI

Last Updated: August 5, 2011

This chapter provides helpful tips for understanding and configuring the Cisco UMG software using the CLI.

About the Cisco UMG CLI

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.

The Cisco UMG CLI commands have a structure very similar to that of Cisco IOS CLI commands. 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. However, the Cisco UMG CLI commands do not affect Cisco IOS configurations. After you have logged in to the Cisco UMG module, the command environment is no longer the Cisco IOS environment.

The following are differences between the Cisco UMG CLI and the Cisco 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.

Understanding Command Modes

The Cisco UMG command environment is divided into two basic modes:

- EXEC—This is the mode that you are in after you log in to the Cisco UMG command environment. Some Cisco UMG EXEC commands only display or clear parameter values, stop or start the entire system, or start troubleshooting procedures. However, unlike Cisco IOS EXEC mode, Cisco UMG EXEC mode has a few commands that change parameter values. These changes are stored in the module's NV memory, rather than in the startup configuration, so that the system has some minimum information available if a catastrophic event, such as a power or disk failure, occurs.
- Configuration—This mode permits you to make system configuration changes, which are stored in the running configuration. If you later save the running configuration to the startup configuration, the changes made with the configuration commands are restored when you reboot the software.

  Cisco UMG configuration mode has various subconfiguration levels. The global configuration mode changes the command environment from EXEC to configuration. You can modify many software parameters at this level. However, certain configuration commands change the environment to more specific configuration modes where modifications to the system are entered. For example, the **registration** command changes the environment from config to config-reg. At this point, you can enter or modify registration parameter values.

The commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. The descriptions in this command reference indicate each command's environment mode.

Table 1 describes how to access and exit various common command modes of the Cisco UMG software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Cisco UMG Release	Access Method	Prompt	Exit Method

Cisco UMG EXEC	1.0 and later	When the Cisco UMG software prompt appears, you can enter the **enable** command, but it is not necessary.	**`with enable:`**
			`umg-1#`
			`without enable:`
			`umg-1>`
				Press **CTRL-SHIFT-6** and then enter **x**.

Cisco UMG configuration	1.0 and later	From EXEC mode, use the **configure terminal** command.	`umg-1(config)#`	To return to EXEC mode from configuration mode, use the **end** or **exit** command.
Registration	1.0 and later	From Cisco UMG configuration mode, use the **registration** command.	`umg-1(config-reg)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
List manager	1.0 and later	From Cisco UMG configuration mode, use the **list-manager** command.	`umg-1(listmgr)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.

Table 1 Accessing and Exiting Command Modes (continued)

Command Mode	Cisco UMG Release	Access Method	Prompt	Exit Method
List manager edit	1.0 and later	From Cisco UMG configuration mode, use the **list number** command.	`umg-1(listmgr-edit)#`	To return to Cisco UMG list manager mode, use the **end** or **exit** command.
NAT configuration	1.0 and later	From Cisco UMG configuration mode, use the **nat location** command.	`umg-1(config-nat)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
Endpoint configuration	1.0 and later	From Cisco UMG configuration mode, use the **endpoint** command.	`umg-1(config-endpoint)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
AAA accounting	8.0 and later	From Cisco UMG configuration mode, use the **aaa accounting server remote** command.	`umg-1(aaa-accounting)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
AAA accounting event	8.0 and later	From Cisco UMG configuration mode, use the **aaa accounting event** command.	`umg-1(aaa-accounting-event)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
AAA accounting policy	8.0 and later	From Cisco UMG configuration mode, use the **aaa policy** command.	`umg-1(aaa-policy)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
backup schedule	8.0 and later	From Cisco UMG configuration mode, use the **backup schedule** command.	`umg-1(backup-schedule)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.
kron-schedule	8.0 and later	From Cisco UMG configuration mode, use the **kron schedule** command.	`umg-1(kron-schedule)#`	To return to Cisco UMG configuration mode, use the **end** or **exit** command.

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 209
- Summary Steps, page 210
- Detailed Steps, page 210

Prerequisites

The following information is required to enter the command environment:

- IP address of the router that contains the Cisco UMG module
- Username and password to log in to the router
- Slot number of the module

- 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. 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. Start configuration by entering **enable**.

Detailed Steps

	Command or Action	Purpose
Step 1	Open a Telnet session.	Use a Microsoft DOS window, a secure shell, or a software emulation tool such as Reflection.

Step 2	`telnet` *`ip-address`*
	Example:
	`C:\> telnet 192.0.2.24`
		Specifies the IP address of the Cisco Unified Communications Manager router.

Step 3	`Username:`
	`Password:`
		Enter your username and password for the router.

Step 4	**On the NME-UMG and NME-UMG-EC, enter:**
	`service-module integrated-service-engine` *`slot/port`* **`session`**
	On the SM-SRE-700-K9 or SM-SRE-900-K9, enter:
	`service-module sm` *`slot/port`* **`session`**
	Example:
	`Router# service-module integrated-service-engine 1/0 session`
		Enters the Cisco Unity Express command environment using the module located in the specified *slot* and *port*. The prompt changes to “se” with the IP address of the Cisco UMG module or the hostname you have assigned to it.
		Note If the message “`Trying` *`ip-address slot/port`* `... Connection refused by remote host`” appears, enter the command **`service-module integrated service-engine`** *`slot/port`* **`session clear`** and try Step 4 again.

Step 5	Start configuration. You can enter **`enable`**. **Example:** `umg-1# enable`	Enters Cisco UMG EXEC mode. You are ready to begin the configuration tasks.

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#
```

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Using the no and default Forms of Commands

Where available, use the **no** form of a command to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. The command reference entry for each command provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. In those cases where a command is disabled by default, using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. Where available, the command reference entry describes the effect of the **default** form of a command if the command does not function the same way as the **no** form.

Saving Configuration Changes

Starting in Cisco UMG EXEC mode, use the following command to copy the running configuration in flash memory to another location:

copy running-config {**ftp:***user-id***:***password***@***ftp-server-address*[/*directory*] | **startup-config** | **tftp:***tftp-server-address*} *filename*

Keyword or Argument	Description
ftp:*user-id***:***password***@**	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-address	IP address of the FTP server.
/directory	(Optional) Directory on the FTP server where the copied file will reside. If you use it, precede the name with the forward slash (/).
startup-config	Startup configuration in flash memory.
tftp:*tftp-server-address*	IP address of the TFTP server.
filename	Name of the destination file that will contain the copied running configuration.

When you copy the running configuration to the startup configuration, enter the command on one line. In the following example, the running configuration is copied to the startup configuration as file start. In this instance, enter the command on a single line.

```
umg-1# copy running-config startup-config start
```

When you copy to the FTP or TFTP server, this command becomes interactive and prompts you for the information. You cannot enter the parameters on one line. The following example illustrates this process. In the following example, the running configuration is copied to the FTP server, which requires a username and password. The IP address of the FTP server is 192.0.2.24. 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:voice@192.0.2.24/configs
Source filename? saved_start
```

Troubleshooting 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 151.

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.

Scheduling CLI Commands

Last Updated: August 5, 2011

Beginning in Cisco UMG Release 8.0, you can schedule the execution of a block of CLI commands. Blocks of commands are entered interactively, using a symbol delimiter character to start and stop the execution. The execution of the block of commands begins in EXEC mode, but mode-changing commands are allowed in the command block.

The following limitations apply in Cisco UMG Release 8.6:

- The maximum size of the block of commands is 1024 characters ,including new lines.
- Commands in the block cannot use the comma "," character or the delimiter character. For example, if the delimiter character is configured to be "#", then that character cannot be used in the command blocks.
- Only system administrators can schedule the execution of blocks of commands.
- CLI commands are executed under system super-user privileges.
- Notification for the execution of these command blocks is not available. Error messages and results are available in log files only.

Caution Use caution when scheduling CLI commands. Interactive commands will cause the execution to hang. Some commands might cause system instability.

SUMMARY STEPS

1. **kron schedule** [*name*]
2. **description**
3. **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*

4. **start-date** *date*
5. **stop-date** *date*
6. **commands** *delimiter*
7. **exit**
8. **show kron schedules**
9. **show kron schedule detail job**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`kron schedule [name]`
	Example:
	`umg-1# kron schedule kron1011`
		Enters kron schedule configuration mode.

Step 2	`description description`
	Example:
	`umg-1(kron-schedule)# description backup`
		(Optional) Enters a description for the scheduled kron job.

Step 3	`repeat every {number days |number weeks on day | number months on day date | number years on month month} at time time`
	Example:
	`umg-1(kron-schedule)# repeat every 2 days at time 10:00`
		Specifies how often a recurring scheduled kron job occurs. To configure a one-time kron job, use the **repeat once** command. You can also optionally use one of the other **repeat** commands listed in the previous note.

Step 4	`start-date date`
	Example:
	`umg-1(kron-schedule)# start-date 05/30/2009`
		Specifies the start date for the recurring scheduled kron job to occur.

Step 5	`stop-date date`
	Example:
	`umg-1(kron-schedule)# stop-date 10/20/2009`
		Specifies the stop date for the recurring scheduled kron job to occur.

	Command or Action	Purpose

Step 6	`commands` *`delimiter`*
	Example:
	`umg-1(kron-schedule)# commands %`
	`Enter CLI commands to be executed. End with the character ‘%’. Maximum size is 1024 characters, it may not contain symbol %.`
	`%show version`
	`show running-config`
	`config t`
	`hostname aaa`
	`%`
	`umg-1(kron-schedule)#`
		Enters an interactive mode where commands in the the command block can be entered for the scheduled kron job. Use the delimiter character to delimit the command block.
		Note Any symbol can be a delimiter. The “%” symbol is shown for example purposes only.

Step 7	**`exit`**	Exits kron schedule configuration mode.

Step 8	**`show kron schedules`**
	Example:
	`umg-1# show kron schedule`
		Displays a list of scheduled kron jobs.

Step 9	**`show kron schedule detail job`** *`name`*
	Example:
	`umg-1# show kron schedule detail job kron1011`
		Displays information about a specific scheduled kron job.

Examples

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

```
umg-1# show kron schedules
Name          Schedule                          Commands
krj1          Every 1 days at 12:34             show ver,sh run,conf t,host...
Total: 1
```

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

```
umg-1# show kron schedule detail job krj1
Job Name         krj1
Description
Schedule         NOT SET
Last Run         NEVER
Last Result
Next Run         NEVER
Active           from Feb 15, 2010 until INDEFINITE
Disabled
CLI Commands
                 show ver
                 sh run
                 conf t
                 hostname aaa
umg-1#
```

C

Last Updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

clear counters interfaces

To clear interface counters, use the **clear counters interfaces** command in Cisco UMG EXEC mode.

clear counters interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

None. Interface counters are not cleared.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command when you have interface counters you want to clear, for example, the general debug counters. This command clears all counters, including statistics counters.

Examples

The following example illustrates the use of the **clear counters interfaces** command.

```
umg-1> enable
umg-1# clear counters interfaces
umg-1# show interfaces ide 0
IDE hd0 is up, line protocol is up
     0 reads, 0 bytes
     0 read errors
     0 write, 0 bytes
     0 write errors
umg-1#
```

Related Commands

Command	Description
clear crashbuffer	Clears the kernel crash buffer.

clear crashbuffer

To clear the kernel crash buffer, use the **clear crashbuffer** command in Cisco UMG EXEC mode.

clear crashbuffer

Syntax Description

This command has no arguments or keywords.

Command Default

None. Crash buffer is not cleared.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to clear the kernel crash buffer after the reasons for a crash are fully investigated.

Examples

The following example illustrates the use of the **clear crashbuffer** command.

```
umg-1 enable>
umg-1# clear crashbuffer
umg-1#
```

Related Commands

Command	Description
clear counters interfaces	Clears the interface counters.

D

Last Updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

domain

domain

To provision the domain name of an endpoint to Cisco UMG, use the **domain** command in Cisco UMG endpoint configuration mode. To clear this configuration, use the **no** form of this command or precede the command with **default**, as in **default domain**.

domain *domain*

no domain

Syntax Description

domain	Domain name of the endpoint, for example, sj.mycompany.com.

Command Default

The default domain name is none.

Command Modes

Cisco UMG endpoint configuration (config-endpoint)

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how the domain name is set as part of the process of provisioning an endpoint to Cisco UMG:

```
umg-1> enable
umg-1# config t
umg-1(config)# endpoint 12345 unity
umg-1(config-endpoint)# domain sj.mycompany.com
umg-1(config-endpoint)# prefix 408902
umg-1(config-endpoint)# hostname unity-408
umg-1(config-endpoint)# end
umg-1(config)#
```

Related Commands

Command	Description
endpoint	Enters the endpoint configuration mode to provision endpoints manually.
hostname (endpoint)	Specifies the hostname of an endpoint you are provisioning manually.
prefix	Sets the phone number prefix of an endpoint.

L

Last Updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

license activate srsv mailboxes

To activate the licenses for Cisco Unified SRSV-CUE mailboxes, use the **license activate srsv mailboxes** command in Cisco Unified SRSV-CUE mode. Using the **no** form of this command sets the usage to zero and disables the feature.

license activate srsv mailboxes *number*

no license activate srsv mailboxes

Syntax Description

number	The number of mailboxes to activate. Must be a multiple of 5.

Command Modes

Cisco SRSV-CUE EXEC

Command History

Cisco Unified SRSV-CUE Release	Modification
8.0	This command was introduced.

Examples

The following example illustrates the use of the **license activate srsv mailboxes** command when the license has not yet been activated:

```
se-192-1-1-171# license activate srsv mailboxes 10

Evaluation licenses are being activated in the device for the following feature(s):

        Feature Name: SRSV-CUE-MBX

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BOUND BY ALL THE TERMS SET FORTH HEREIN.

You hereby  acknowledge  and  agree that  the  product feature  license
is terminable and that the product  feature  enabled  by  such  license
may  be  shut  down or  terminated by  Cisco  after  expiration of  the
applicable  term  of  the license  (e.g., 30-day  trial  period). Cisco
reserves the  right to terminate or shut down  any such product feature
electronically  or by  any other  means available. While alerts or such
messages  may  be provided, it is  your sole  responsibility to monitor
your terminable  usage of any  product  feature enabled by  the license
and to ensure that your systems and  networks are prepared for the shut
down of the product feature. You acknowledge  and agree that Cisco will
not have any liability  whatsoever for  any damages, including, but not
limited to, direct, indirect, special, or consequential damages related
to any product  feature  being shutdown or terminated. By clicking  the
"accept" button  or typing "yes" you are  indicating  you have read and
agree to be bound by all the terms provided herein.
ACCEPT? [y/n]?y

License activation count saved for use at next reload
```

The following example illustrates the use of the **license activate srsv mailboxes** command when the license has already been activated:

```
se-192-1-1-149# license activate srsv mailboxes 25

Current license already active, count saved for use at next reload
```

The following example illustrates the use of the **license activate srsv mailboxes** command to disable the licenses:

```
se-192-1-1-149# no license activate srsv mailboxes

License will be disabled at next reload
```

Related Commands

Command	Description
show license status application srsv	Displays the Cisco Unified SRSV-CUE license status.

license activate srst nodes

To activate the license for Cisco Unified E-SRST nodes, use the **license activate srst nodes** command in Cisco UMG EXEC mode. Using the **no** form of this command sets the usage to zero and disables the feature.

license activate srst nodes *number*

no license activate srst nodes

Syntax Description

number	The number of nodes to activate.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.5	This command was introduced.

Usage Guidelines

The *number* argument can be between 0 and the maximum number of nodes supported by the device and must be a multiple of 25. This activation count is applied for all types of licenses, so it can be used to reduce the count below the module maximum count or below the count of any other installed license.

Examples

The following example illustrates the use of the **license activate srst nodes** command when the license has not yet been activated:

```
se-192-1-1-149# license activate srst nodes 25

Evaluation licenses are being activated in the device for the following feature(s):

        Feature Name: CUMG-SRST-NODE

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BOUND BY ALL THE TERMS SET FORTH HEREIN.

You hereby  acknowledge  and  agree that  the  product feature  license
is terminable and that the product  feature  enabled  by  such  license
may  be  shut  down or  terminated by  Cisco  after  expiration of  the
applicable  term  of  the license  (e.g., 30-day  trial  period). Cisco
reserves the  right to terminate or shut down  any such product feature
electronically  or by  any other  means available. While alerts or such
messages  may  be provided, it is  your sole  responsibility to monitor
your terminable  usage of any  product  feature enabled by  the license
and to ensure that your systems and  networks are prepared for the shut
down of the product feature. You acknowledge  and agree that Cisco will
not have any liability  whatsoever for  any damages, including, but not
limited to, direct, indirect, special, or consequential damages related
to any product  feature  being shutdown or terminated. By clicking  the
```

```
"accept" button  or typing "yes" you are  indicating  you have read and
agree to be bound by all the terms provided herein.
ACCEPT? [y/n]?y

License activation count saved for use at next reload
```

The following example illustrates the use of the **license activate srst nodes** command when the license has already been activated:

```
se-192-1-1-149# license activate srst nodes 25

Current license already active, count saved for use at next reload
```

The following example illustrates the use of the **license activate srst nodes** command to disable the licenses:

```
se-192-1-1-149# no license activate srst nodes

License will be disabled at next reload
```

Related Commands

Command	Description
show license status application srst	Displays the Cisco Unified SRST license status.

license activate srsv nodes

To activate the license for Cisco Unified SRSV nodes, use the **license activate srsv nodes** command in Cisco UMG EXEC mode. Using the **no** form of this command sets the usage to zero and disables the feature.

license activate srsv nodes *number*

no license activate srsv nodes

Syntax Description

number	The number of nodes to activate.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

The *number* argument can be between 0 and the maximum number of nodes supported by the device and must be a multiple of 25. This activation count is applied for all types of licenses, so it can be used to reduce the count below the module maximum count or below the count of any other installed license.

Examples

The following example illustrates the use of the **license activate srsv nodes** command when the license has not yet been activated:

```
se-192-1-1-149# license activate srsv nodes 25

Evaluation licenses are being activated in the device for the following feature(s):

        Feature Name: CUMG-SRSV-NODE

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BOUND BY ALL THE TERMS SET FORTH HEREIN.

You hereby  acknowledge  and  agree that  the  product feature  license
is terminable and that the product  feature  enabled  by  such  license
may  be  shut  down or  terminated by  Cisco  after  expiration of  the
applicable  term  of  the license  (e.g., 30-day  trial  period). Cisco
reserves the  right to terminate or shut down  any such product feature
electronically  or by  any other  means available. While alerts or such
messages  may  be provided, it is  your sole  responsibility to monitor
your terminable  usage of any  product  feature enabled by  the license
and to ensure that your systems and  networks are prepared for the shut
down of the product feature. You acknowledge  and agree that Cisco will
not have any liability  whatsoever for  any damages, including, but not
limited to, direct, indirect, special, or consequential damages related
to any product  feature  being shutdown or terminated. By clicking  the
```

```
"accept" button  or typing "yes" you are  indicating  you have read and
agree to be bound by all the terms provided herein.
ACCEPT? [y/n]?y

License activation count saved for use at next reload
```

The following example illustrates the use of the **license activate srsv nodes** command when the license has already been activated:

```
se-192-1-1-149# license activate srsv nodes 25

Current license already active, count saved for use at next reload
```

The following example illustrates the use of the **license activate srsv nodes** command to disable the licenses:

```
se-192-1-1-149# no license activate srsv nodes

License will be disabled at next reload
```

Related Commands

Command	Description
show license status application srsv	Displays the Cisco Unified SRSV license status.

license activate srsv ports

To activate the license for Cisco Unified SRSV-CUE ports, use the **license activate srsv ports** command in Cisco Unified SRSV-CUE EXEC mode. Using the **no** form of this command sets the usage to zero and disables the feature.

license activate srsv ports *number*

no license activate srsv ports

Syntax Description

number	The number of ports to activate. Must be a multiple of 2.

Command Modes

Cisco Unified SRSV-CUE EXEC

Command History

Cisco Unified SRSV-CUE Release	Modification
8.0	This command was introduced.

Examples

The following example illustrates the use of the **license activate srsv ports** command when the license has not yet been activated:

```
se-192-1-1-171# license activate srsv ports 4

Evaluation licenses are being activated in the device for the following feature(s):

        Feature Name: SRSV-CUE-PORT

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BOUND BY ALL THE TERMS SET FORTH HEREIN.

You hereby  acknowledge  and  agree that  the  product feature  license
is terminable and that the product  feature  enabled  by  such  license
may  be  shut  down or  terminated by  Cisco  after  expiration of  the
applicable  term  of  the license  (e.g., 30-day  trial  period). Cisco
reserves the  right to terminate or shut down  any such product feature
electronically  or by  any other  means available. While alerts or such
messages  may  be provided, it is  your sole  responsibility to monitor
your terminable  usage of any  product  feature enabled by  the license
and to ensure that your systems and  networks are prepared for the shut
down of the product feature. You acknowledge  and agree that Cisco will
not have any liability  whatsoever for  any damages, including, but not
limited to, direct, indirect, special, or consequential damages related
to any product  feature  being shutdown or terminated. By clicking  the
"accept" button  or typing "yes" you are  indicating  you have read and
agree to be bound by all the terms provided herein.
ACCEPT? [y/n]?y

License activation count saved for use at next reload
```

The following example illustrates the use of the **license activate srsv ports** command when the license has already been activated:

```
se-192-1-1-149# license activate srsv ports 6

Current license already active, count saved for use at next reload
```

The following example illustrates the use of the **license activate srsv ports** command to disable the licenses:

```
se-192-1-1-149# no license activate srsv ports

License will be disabled at next reload
```

Related Commands

Command	Description
show license status application srsv	Displays the Cisco Unified SRSV-CUE license status.

M

Last updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

messaging-gateway srsx register

messaging-gateway srsx register

To register a Cisco Unified SRSV-CUE device with Cisco UMG so that it can begin the provisioning process, use the **messaging-gateway srsx register** command in Cisco Unified SRSV-CUE EXEC mode.

messaging-gateway srsx register *address* **user** *user_name* **password** *password*
[srst-gateway *IP_address* **] [site-name** *site_name* **] [pat-port** *port_number* **]**

Syntax Description

address	Fully specified domain name or IP address of the Cisco UMG to which the Cisco Unified SRSV-CUE device is being registered.
user_name	User name of the administrator who is registering the Cisco Unified SRSV-CUE device. This user must belong to a group with a privilege containing the srsv-registration operation. Operations are set using the Cisco UMG GUI.
password	Password of the administrator who is registering the Cisco Unified SRSV-CUE device.
IP_address	Fully specified domain name or address of telephony service local to the site that can route voice calls when the Cisco Unified SRSV-CUE device is in operation. If the Cisco Unified SRSV-CUE device is deployed on a local network, this must be the local address to the Cisco Unified SRSV-CUE device that provides telephony services during loss of connection to the central site.
site_name	The site to which the Cisco Unified SRSV-CUE device is bound. If the site is already bound to a different Cisco Unified SRSV-CUE device or if this Cisco Unified SRSV-CUE device is bound to a different site, the administrator must confirm the binding before registration will complete.
port_number	The PAT port number that the Cisco UMG uses to reach the Cisco Unified SRSV-CUE device. This port number specifies the port on the public side of the NAT that maps to port 80 (or port 443 when TLS is enabled) in order to communicate to the Cisco Unified SRSV-CUE device.

Command Modes

Cisco Unified SRSV-CUE EXEC

Command History

Cisco Unified SRSV-CUE Release	Modification
8.0	This command was introduced.

Usage Guidelines

- If SSL/TLS security is used on Cisco UMG, then SSL/TLS must be configured on the Cisco Unified SRSV-CUE device before registering.

- If Cisco UMG detects a problem with the Cisco Unified SRSV-CUE device during registration, it sends a message to the Cisco Unified SRSV-CUE device. There are two problems that can occur: Cisco UMG detects that NAT is enabled but no PAT port has been supplied, or a site name is passed but the Cisco Unified SRSV-CUE device cannot be bound to that site.

Examples

The following example illustrates the use of the **messaging-gateway srsx register** command. The output is successful registration:

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V

Registration complete
```

The following example illustrates the use of the **messaging-gateway srsx register** command and the output is successful registration with site binding:

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V site-name boston

Registration complete
Bound to site boston
```

The following example illustrates the use of the **messaging-gateway srsx register** command and the output is successful registration with unsuccessful site binding:

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V site-name boston

Registration complete
Unable to bind SRSV (site boston does not exist)
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output shows re-registration when the Cisco Unified SRSV-CUE device is already bound to a different site. You can use Ctrl-C to cancel registration.

```
SRSV# messaging-gateway srsx register UMG.central.site user me password 5r5V site-name
boston

SRSV-CUE bos-srsv.srsv.lab already bound to site san-jose,
Continue with registration to bind to site boston? [confirm]

Registration complete
Bound to site boston
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output shows registration when the Cisco Unified SRSV-CUE device attempts to bind to a site that is bound to another Cisco Unified SRSV-CUE device. You can use Ctrl-C to cancel registration.

```
SRSV# messaging-gateway srsx register UMG.central.site user me password 5r5V site-name
boston

Site boston is already bound to SRSV-CUE nyc-srsv.srsv.lab.
Continue with registration to bind to site boston and orphan SRSV-CUE nyc-srsv.srsv.lab?
[confirm]

Registration complete
Bound to site boston (SRSV-CUE nyc-srsv.srsv.lab orphaned)
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output shows re-registration when the Cisco Unified SRSV-CUE device is already bound to the same site as currently configured on Cisco UMG.

```
SRSV# messaging-gateway srsx register UMG.central.site user me password 5r5V site-name
boston
```

```
Registration complete
Bound to site boston (unchanged)
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output is successful registration using the PAT port option:

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V pat-port 1080

Registration complete
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output is successful registration without using the PAT port option:

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V

NAT detected for this device.
If port address translation is utilized,
the public PAT port configured to reach
the SRSV-CUE must be identified.

Specify the public PAT port to use for
this device or press return to accept
default port: 1080

Registration complete
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output is successful registration using the srst-gateway parameter:

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V srst-gateway
192.168.1.58

Registration complete
```

The following example illustrates the use of the **messaging-gateway srsx register** command. The output is unsuccessful registration.

```
SRSV# messaging-gateway srsx register 192.168.1.27 user me password 5r5V (…)

Registration failed.
<FAILURE-DETAILS>
```

The failure details specify why the registration failed and can include authorization failure, connection failure, or the system is unable to look up the hostname in DNS.

P

Last Updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

prefix

To set the phone number prefix of an endpoint, use the **prefix** command in Cisco UMG endpoint configuration mode. To clear this configuration, use the **no** form of this command.

prefix *number*

no prefix *number*

Syntax Description

number	Phone number prefix for the endpoint.

Command Default

The default prefix is none.

Command Modes

Cisco UMG endpoint configuration (config-endpoint)

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

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.

Examples

The following example shows how the prefix is set as part of the process of manually adding an endpoint to the messaging gateway network:

```
umg-1(config)# endpoint 12345 unity
umg-1(config-endpoint)# hostname unity.mycompany.com
umg-1(config-endpoint)# serialnumber 12345
umg-1(config-endpoint)# prefix 408902
umg-1(config-endpoint)# end
umg-1(config)# end
umg-1# show endpoint local 12345
```

Related Commands

Command	Description
endpoint	Enters endpoint configuration mode in order to provision endpoints manually.
show endpoint	Displays a list of the endpoints in the system and their details or a specific endpoint's details.

privilege (list-manager edit)

To configure an authorized sender to a system distribution list (SDL), use the **privilege** command in Cisco UMG edit list manager mode. To revoke the privilege, use the **no** form of the command.

privilege *authorized-sender*

no privilege *authorized-sender*

Syntax Description

authorized-sender	The mailbox number of the authorized sender.

Command Default

No privilege is configured.

Command Modes

Cisco UMG list manager edit (listmgr-edit)

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

No list members can receive messages from an SDL until you configure an authorized sender for it.

You must create members for an SDL so that they can receive the messages published by the authorized sender.

Examples

The following example illustrates the use of the **privilege** command to create an authorized sender for the 1234 list:

```
umg-1# list-manager
umg-1(listmgr)# list number 1234
umg-1(listmgr-edit)# privilege 4505550111
umg-1(listmgr-edit)# end
umg-1#
```

Related Commands

Command	Description
list-manager	Enters list manager mode in order to create, edit, or publish SDLs.
list number	Enters list manager edit mode in order to configure an SDL in detail.
list publish	Publishes one or more SDLs to peer messaging gateways.
member	Assigns members to an SDL.
name	Assigns a name to an SDL.
show list	Displays a list of the SDLs that are configured and their details.

Command	Description
show list privilege	Displays the authorized sender to a specific SDL.
show list tracking version	Displays an SDL tracking version.

S

Last Updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

show srsx srsv-upload-history

show srsx system-settings

show statistics

software download uninstall

serial-number

To configure a serial number for a Cisco Unity endpoint, use the **serial-number** command in Cisco UMG endpoint configuration mode. To clear this configuration, use the **no** form of this command.

serial-number *numeric_string*

no serial-number *numeric_string*

Syntax Description

numeric_string	Serial number of the Cisco Unity endpoint.

Command Default

The default serial-number is no serial number or the empty string " ".

Command Modes

Cisco UMG endpoint configuration (config-endpoint)

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure a serial number for a Cisco Unity endpoint.

Note This command is not applicable to Avaya Interchange or to <Abbreviation>Cisco Unity Express endpoints.

Examples

The following example shows how the serial number is set as part of the process of provisioning a Cisco Unity endpoint:

```
umg-1# config t
umg-1(config)# endpoint 12345 type unity
umg-1(config-unity)# serial-number 12345
umg-1(config-unity)# secondary gateway 10.100.50.2
umg-1(config-unity)# end
umg-1(config)#
```

Related Commands

Command	Description
domain	Sets the domain name for an endpoint.
prefix	Sets the phone number prefix for an endpoint.

show clock

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

show clock

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Cisco UMG uses the Network Time Protocol (NTP) server for clocking functions. Use the **show clock** command to display the Cisco UMG clock status.

Examples

The following is sample output for the **show clock** command:

```
umg-1# show clock

19:20:33.724 PST Wed Mar 17 1993
time zone:                                America/Los_Angeles
clock state:                              unsync
delta from reference (microsec):          0
estimated error (microsec):               175431
time resolution (microsec):               1
clock interrupt period (microsec):        10000
time of day (sec):                        732424833
time of day (microsec):                   760817
```

Table 2 describes the significant fields shown in the display.

Table 2 show clock Field Descriptions

Field	Description
time zone	Current time zone setting.
clock state	Synchronization state of the clock.
delta from reference (ms)	Difference between the module clock and the NTP reference clock.
time of day (sec)	Current time of day in seconds.
time of day (ms)	Current time of day in microseconds.

Related Commands

Command	Description
ntp server	Specifies the NTP server for Cisco UMG.
show ntp	Displays the time source for an NTP server.

show configuration

To display the contents of the non-volatile memory, use the **show configuration** command in Cisco UMG EXEC mode.

show configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command for troubleshooting.

Examples

The following is sample output for the **show configuration** command:

```
umg-1# show configuration

clock timezone America/Los_Angeles

hostname umg-1

ip domain-name temp.com

system language preferred "en_US"

ntp server 192.0.2.24 prefer

software download server url "ftp://192.0.2.23/ftp" credentials hidden "6u/dKTN/h
sEuSAEfw40XlF2eFHnZfyUTSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfG
WTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

log trace local enable

groupname Administrators create
groupname Broadcasters create

username chambers create

groupname Administrators privilege superuser
groupname Administrators privilege ManagePrompts
groupname Administrators privilege broadcast
groupname Administrators privilege local-broadcast
groupname Administrators privilege ManagePublicList
groupname Administrators privilege ViewPrivateList
groupname Administrators privilege vm-imap
groupname Administrators privilege ViewHistoricalReports
groupname Administrators privilege ViewRealTimeReports
groupname Broadcasters privilege broadcast

backup server url "ftp://192.0.2.23/sd_backup_10" credentials hidden "+EdqgXXrw
vTq9Gr22KTpoknfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfG
WTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

security password lockout policy temp-lock
security pin lockout policy temp-lock

network local messaging-gateway 50000
network messaging-gateway 57000 192.0.2.22

registration
 username cue_02 password encrypted "Cnjf81Z1zXpbrA7+7/IBX0nfGWTYHfmPSd8ZZNgd+Y9
J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWT
YHfmP"
 username umg password encrypted "R30jwZyreaDX3TqGSvsp5EnfGWTYHfmPSd8ZZNgd+Y9J3x
lk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHf
mP"
 end registration

spoken-name enable

translation-rule message unity from-host to-host

end
umg-1
```

Related Commands

Command	Description
backup category	Specifies the type of data to be backed up and initiates the backup process.
hostname	Specifies the hostname of the current messaging gateway.
ip domain-name	Specifies the local messaging gateway’s domain name and/or domain name server.
restore factory default	Restores factory default settings.

show ip dns cache

To display the DNS cache, use the **show ip dns cache** command in Cisco UMG EXEC mode.

show ip dns cache

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Examples

The following is sample output for the **show ip dns cache** command:

```
umg-1> show ip dns cache


umg-1.unspecified.       2147483647 IN A         192.0.2.24
localhost.\(none\).      2147483647 IN A         192.0.2.23
192.0.2.22.in-addr.arpa. 2147483647 IN PTR               localhost.
stress-umg1-192.0.2.24.example.com.  2147483647 IN A     192.0.2.24
192.0.2.24.in-addr.arpa.             2147483647 IN PTR   192.0.2.24.te
mp.com.
se-192.0.2.24.localdomain.      2147483647 IN A          192.0.2.24
sundial1-umg-se-192.0.2.24.localdomain. 2147483647 IN A         10.1.12.95
localhost.temp.com.     2147483647 IN A         192.0.2.18
192.0.2.24.temp.com.    2147483647 IN A         192.0.2.24
192.0.2.24.\(none\).    2147483647 IN A         192.0.2.24
stress-umg1-192.0.2.24.example.com.    2147483647 IN A       192.0.2.24
localhost.                             2147483647 IN A       192.0.2.20
stress-umg1-192.0.2.22.\(none\).       2147483647 IN A       192.0.2.24
se-192.0.2.24.example.com.             2147483647 IN A       192.0.2.24
localhost.cisco.com.                   2147483647 IN A       192.0.2.23


se-10-1-12-95>
```

Related Commands

Command	Description
hostname	Specifies the hostname for the current configuring Cisco UMG.
ip name-server	Specifies the domain name server.
ntp server	Specifies the NTP clocking server.
show hosts	Displays all configured hosts.

show license agent

To display the license agent counters and session information, use the **show license agent** command in Cisco UMG EXEC mode.

show license agent {**counters** | **session**}

Syntax Description

counters	Displays the license agent counters.
session	Displays the license agent session.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

This command displays counter and session information.

Examples

The following is a sample output for the **show license agent counters** command:

```
UMG-1# show license agent counters
License Agent Counters
Request Messages Received:0: Messages with Errors:0
Request Operations Received:0: Operations with Errors:0
Notification Messages Sent:0: Transmission Errors:0
```

The following is a sample output for the **show license agent session** command:

```
SRST-UMG# show license agent session

License Agent Sessions: 0 open, maximum is 9
```

Related Commands

Command	Description
show license detail	Displays the details of the license installed on your system.
show license evaluation	Displays the evaluation licenses that are installed on your system.
show license expiring	Displays the expiring licenses.
show license feature	Displays the license feature information.
show license file	Displays the license file information
show license in-use	Displays information about the licenses that are in use.
show license permanent	Displays the status of the licenses installed.
show license status	Displays the status of the license applications installed.

show license status application srst

To display the Cisco Unified SRST license status, use the **show license status application srst** command in Cisco UMG EXEC mode.

show license status application srst

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.5	This command was introduced.

Examples

The following are sample outputs for the **show license status application srst** command:

```
umg-1# show license status application srst
srst enabled: 25 srst nodes

umg-1# show license status application srst
srst disabled, no activated srst node license available
```

Related Commands

Command	Description
license activate srst nodes	Activates the license for Cisco Unified SRST nodes.

show license status application srsv

To display the Cisco Unified SRSV license status, use the **show license status application srsv** command in Cisco UMG EXEC mode.

show license status application srsv

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Examples

The following are sample outputs for the **show license status application srsv** command:

```
umg-1# show license status application srsv
srsv enabled: 25 srsv nodes

umg-1# show license status application srsv
srsv disabled, no activated srsv node license available
```

Related Commands

Command	Description
license activate srsv nodes	Activates the license for Cisco Unified SRSV nodes.

show log name

To display logging data, use the **show log name** command in Cisco UMG EXEC mode.

show log name *word* [**containing** *expression* | **paged** | **tail**]

Syntax Description

word	The name of the log file to display. Use the **show logs** command to display a list of available log files.
containing *expression*	Only displays events that match a search expression.
paged	Displays in paged mode.
tail	Displays the latest events as they occur.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command has the following filtering options:

- **show begin**: Begins the output of any **show** command from a specified string.
- **show exclude**: Filters **show** command output so that it excludes lines that contain a particular regular expression.
- **show include**: Filters **show** command output so that it displays only lines that contain a particular regular expression.

Examples

The following partial output for the **show log name** command displays the dmesg log:

```
umg-1# show log name dmesg

Press <CTRL-C> to exit...
Linux version 2.4.24 (bld_adm@bld-system) (gcc version 2.95.3 20010315 (version4
Platform: nm
setup.c: handling flash window at [15MB..16MB]
setup.c: handling kernel log buf at [245.5MB]
setup.c: handling trace buf at [246MB]
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
 BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000e0800 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 0000000000f00000 (usable)
 BIOS-e820: 0000000000f00000 - 0000000001000000 (reserved)
 BIOS-e820: 0000000001000000 - 000000000f580000 (usable)
 BIOS-e820: 000000000f580000 - 000000000f600000 (reserved)
 BIOS-e820: 000000000f600000 - 0000000010000000 (reserved)
 BIOS-e820: 00000000fff00000 - 0000000100000000 (reserved)
245MB LOWMEM available.
On node 0 totalpages: 62848
```

```
zone(0): 4096 pages.
zone(1): 58752 pages.
zone(2): 0 pages.
DMI not present.
Kernel command line: root=/dev/hda1 ro plat=nm
Initializing CPU#0
Detected 498.674 MHz processor.
Calibrating delay loop... 996.14 BogoMIPS
Memory: 245128k/251392k available (1164k kernel code, 4852k reserved, 667k data)
kdb version 4.3 by Keith Owens, Scott Lurndal. Copyright SGI, All Rights Reservd
in atrace_init
log_head: h: 0, t: 8429274, l: 0, w: 0, s: 10484672
Using existing trace log
log_head: h: 0, t: 8429274, l: 0, w: 0, s: 10484672
Dentry cache hash table entries: 32768 (order: 6, 262144 bytes)
Inode cache hash table entries: 16384 (order: 5, 131072 bytes)
Mount cache hash table entries: 512 (order: 0, 4096 bytes)
Buffer cache hash table entries: 16384 (order: 4, 65536 bytes)
Page-cache hash table entries: 65536 (order: 6, 262144 bytes)
CPU: L1 I cache: 16K, L1 D cache: 16K
CPU: L2 cache: 256K
CPU serial number disabled.
```

The following sample output for the **show log** command displays the dmesg log using a search string:

```
umg-1# show log name dmesg containing setup

Press <CTRL-C> to exit...
setup.c: handling flash window at [15MB..16MB]
setup.c: handling kernel log buf at [245.5MB]
setup.c: handling trace buf at [246MB]
umg-1#
```

The following partial output for the **show log** command displays the dmesg log in paged mode:

```
umg-1# show log name dmesg paged

Linux version 2.4.24 (bld_adm@bld-system) (gcc version 2.95.3 20010315 (version
)) #1 Tue Nov 30 23:07:21 PST 2007
Platform: nm
setup.c: handling flash window at [15MB..16MB]
setup.c: handling kernel log buf at [245.5MB]
setup.c: handling trace buf at [246MB]
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
 BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000e0800 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 0000000000f00000 (usable)
 BIOS-e820: 0000000000f00000 - 0000000001000000 (reserved)
 BIOS-e820: 0000000001000000 - 000000000f580000 (usable)
 BIOS-e820: 000000000f580000 - 000000000f600000 (reserved)
 BIOS-e820: 000000000f600000 - 0000000010000000 (reserved)
 BIOS-e820: 00000000fff00000 - 0000000100000000 (reserved)
245MB LOWMEM available.
On node 0 totalpages: 62848
zone(0): 4096 pages.
zone(1): 58752 pages.
zone(2): 0 pages.
DMI not present.
Kernel command line: root=/dev/hda1 ro plat=nm
Initializing CPU#0
 -- More --
```

The following output for the **show log name** command displays the current dmesg log as events are being entered:

```
umg-1# show log name dmesg tail

Press <CTRL-C> to exit...
Freeing unused kernel memory: 88k freed
```

The following partial output for the **show log name** command displays the dmesg log beginning with the first line starting with ide0:

```
umg-1# show log name dmesg | begin ide0

    ide0: BM-DMA at 0xfc00-0xfc07, BIOS settings: hda:pio, hdb:pio
    ide1: BM-DMA at 0xfc08-0xfc0f, BIOS settings: hdc:pio, hdd:pio
hda: C/H/S=50127/232/176 from BIOS ignored
hdb: C/H/S=0/0/0 from BIOS ignored
hda: IC25N020ATMR04-0, ATA DISK drive
blk: queue c030c160, I/O limit 4095Mb (mask 0xffffffff)
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hda: attached ide-disk driver.
hda: host protected area => 1
hda: 39070080 sectors (20004 MB) w/1740KiB Cache, CHS=2432/255/63, UDMA(33)
init unit number == 0
```

Related Commands.

Command	Description
log console	Configures the types of messages to be displayed on the console.
log console monitor	Displays system messages on the console.
log server address	Specifies an external server for saving log messages.
log trace boot	Saves the trace configuration on rebooting.
log trace buffer save	Saves the current trace information.
show logging	Shows the types of messages that are displayed on the console.
show logs	Displays the list of available logs.

show ntp

To display the time source for a Network Time Protocol (NTP) server, use the **show ntp** command in Cisco UMG EXEC mode.

show ntp [**detail**]

Syntax Description

detail	Displays detailed information about the NTP servers.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command displays the chain of NTP servers back to their primary time source, starting from the local host.

Examples

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

```
umg-1# show ntp

192.0.2.24: stratum 9, offset 0.000015, synch distance 0.03047
192.0.2.23: stratum 8, offset -0.001124, synch distance 0.00003
```

Table 3 describes the significant fields shown in the display.

Table 3 show ntp Field Descriptions

Field	Description
(first field)	IP address of the host.
stratum	Server hop count to the primary clock source. Valid values are: • 0—Unspecified • 1—Primary clock reference • 2–255—Secondary reference via NTP
offset	Time offset between the host and the local host, in seconds.
synch distance	Host synchronization distance, which is the estimated error relative to the primary source.

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

```
umg-1# show ntp detail

server 192.0.2.24, port 123
```

```
stratum 9, precision -17, leap 00
refid [192.0.2.22] delay 0.00012, dispersion 0.00000 offset 0.000011
rootdelay 0.00058, rootdispersion 0.03111, synch dist 0.03140
reference time:      af4a3ff7.926698bb  Thu, Mar 11 1993 14:47:19.571
originate timestamp: af4a4041.bf991bc5  Thu, Mar 11 1993 14:48:33.748
transmit timestamp:  af4a4041.bf90a782  Thu, Mar 11 1993 14:48:33.748

server 192.0.2.23, port 123
stratum 8, precision -18, leap 00
refid [192.0.2.21] delay 0.00024, dispersion 0.00000 offset -0.001130
rootdelay 0.00000, rootdispersion 0.00003, synch dist 0.00003
reference time:      af4a402e.f46eaea6  Thu, Mar 11 1993 14:48:14.954
originate timestamp: af4a4041.bf6fb4d4  Thu, Mar 11 1993 14:48:33.747
transmit timestamp:  af4a4041.bfb0d51f  Thu, Mar 11 1993 14:48:33.748
```

Table 4 describes the significant fields shown in the display.

Table 4 show ntp detail Field Descriptions

Field	Description
server	IP address of the host server.
port	Port number of the host server.
stratum	Server hop count to the primary clock source. Valid values are: • 0—Unspecified • 1—Primary clock reference • 2–255—Secondary reference via NTP
precision	Precision of the clock, in seconds to the power of two.
leap	Two-bit code warning of an impending leap second to be inserted in the NTP time scale. Valid values are: • 00—No warning • 01—Last minute was 61 seconds • 10—Last minute was 59 seconds • 11—Alarm condition (clock not synchronized)
refid	IP address of the peer selected for synchronization.
delay	Round-trip delay of the packet, in milliseconds.
dispersion	Measure, in milliseconds, of how scattered the time offsets have been from a given time server.
offset	Time offset between the host and the local host, in seconds.
rootdelay	Total round-trip delay, in seconds, to the primary reference source at the root of the synchronization subnet.
rootdispersion	Maximum error, in seconds, relative to the primary reference source at the root of the synchronization subnet.
synch dist	Host synchronization distance, which is the estimated error relative to the primary source.
reference time	Local time, in time-stamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero.

Table 4 show ntp detail Field Descriptions (continued)

Field	Description
originate timestamp	Local time, in time-stamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is zero.
transmit timestamp	Local time, in time-stamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable, the value is zero.

Related Commands

Command	Description
ntp server	Configures the Network Time Protocol (NTP) server to keep the system time synchronized with the NTP server.
show clock	Displays clock statistics.

show srsv auto-attendant

To display the Cisco Unified SRSV-CUE auto-attendant configuration status that is provisioned by the Cisco UMG, use the **show srsv auto-attendant** command in Cisco Unified SRSV-CUE EXEC mode.

show srsv auto-attendant [call-handler [*display_name*] **] [directory-handler** [*display_name*] **]**

Syntax Description

display_name	Name of a specific call handler or directory handler for which you want to display the auto-attendant configuration.

Command Modes

Cisco Unified SRSV-CUE EXEC

Command History

Cisco Unified SRSV-CUE Release	Modification
8.0	This command was introduced.
8.6	Updated this command to include the "Schedule," "Holiday Schedule," and "Status" information in the output.

Usage Guidelines

You can use this command with no arguments to show all the auto-attendant configuration information.

Examples

The following example shows the output for the **show srsv auto-attendant** command when it is entered with no arguments:

```
SRSV# show srsv auto-attendant
CALL HANDLER
 Display Name                    : Amit-CH
 Language                        : INHERIT
 Schedule                        : All Hours
 Holiday Schedule                : Unknown
 Menu Delay                      : 1500
 Transfer Rule                   : ALTERNATE
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : OFF_HOURS
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : STANDARD
  Transfer calls to              : 9003
  Status                         : Enabled Indefinitely
 Greeting                        : Alternate
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Busy
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Greeting                        : Error
  Languages                      : en_US
  After greeting action          : restart-greeting
  Status                         : Enabled Indefinitely
 Greeting                        : Holiday
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Internal
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Off Hours
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Standard
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Menu Key                        : 1
  Action                         : transfer Amit-CH
 Menu Key                        : *
  Action                         : sign-in
 Menu Key                        : #
  Action                         : skip-greeting

CALL HANDLER
 Display Name                    : Opening Greeting
 Language                        : INHERIT
 Schedule                        : Amit Test Schedule
 Holiday Schedule                : Amit Holiday
 Menu Delay                      : 1500
 Transfer Rule                   : ALTERNATE
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : OFF_HOURS
  Transfer calls to              : 6003
  Status                         : Disabled
 Transfer Rule                   : STANDARD
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Greeting                        : Alternate
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Busy
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Error
  Languages                      : en_US
  After greeting action          : restart-greeting
  Status                         : Enabled Indefinitely
 Greeting                        : Holiday
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Greeting                        : Internal
  Languages                      : en_US
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Off Hours
  Languages                      : en_US
  After greeting action          : transfer Operator
  Status                         : Disabled
 Greeting                        : Standard
```

```
  Languages                      : en_US
  After greeting action          : transfer Operator
  Status                         : Enabled Indefinitely
 Menu Key                        : 0
  Action                         : transfer Operator
 Menu Key                        : 2
  Action                         : hang-up
 Menu Key                        : 4
  Action                         : DH System Directory Handler
 Menu Key                        : 7
  Action                         : transfer Amit-CH
 Menu Key                        : 8
  Action                         : greeting tdennler-CH
 Menu Key                        : *
  Action                         : sign-in
 Menu Key                        : #
  Action                         : transfer Operator

CALL HANDLER
 Display Name                    : tdennler-CH
 Language                        : INHERIT
 Schedule                        : Tdennler Schedule
 Holiday Schedule                : Tdennler Holidays
 Menu Delay                      : 1500
 Transfer Rule                   : ALTERNATE
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : OFF_HOURS
  Transfer calls to              : 6003
  Status                         : Disabled
 Transfer Rule                   : STANDARD
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Greeting                        : Alternate
  Languages                      : en_US
  After greeting action          : hang-up
  Status                         : Disabled
 Greeting                        : Busy
  Languages                      : en_US
  After greeting action          : hang-up
  Status                         : Disabled
 Greeting                        : Error
  Languages                      : en_US
  After greeting action          : restart-greeting
  Status                         : Enabled Indefinitely
 Greeting                        : Holiday
  Languages                      : en_US
  After greeting action          : hang-up
  Status                         : Disabled
 Greeting                        : Internal
  Languages                      : en_US
  After greeting action          : hang-up
  Status                         : Disabled
 Greeting                        : Off Hours
  Languages                      : en_US
  After greeting action          : hang-up
  Status                         : Disabled
 Greeting                        : Standard
  Languages                      : en_US
  After greeting action          : transfer Operator
  Status                         : Enabled Indefinitely
 Menu Key                        : 0
  Action                         : transfer Operator
 Menu Key                        : *
```

```
  Action                         : sign-in
 Menu Key                        : #
  Action                         : skip-greeting

CALL HANDLER
 Display Name                    : Operator
 Language                        : INHERIT
 Schedule                        : Weekdays
 Holiday Schedule                : Unknown
 Menu Delay                      : 1500
 Transfer Rule                   : ALTERNATE
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : OFF_HOURS
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Transfer Rule                   : STANDARD
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Greeting                        : Alternate
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Busy
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Greeting                        : Error
  After greeting action          : restart-greeting
  Status                         : Enabled Indefinitely
 Greeting                        : Holiday
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Internal
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Off Hours
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Greeting                        : Standard
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Menu Key                        : *
  Action                         : sign-in
 Menu Key                        : #
  Action                         : transfer Opening Greeting

CALL HANDLER
 Display Name                    : tdennler-CH2a
 Language                        : INHERIT
 Schedule                        : All Hours
 Holiday Schedule                : Unknown
 Menu Delay                      : 1500
 Transfer Rule                   : ALTERNATE
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : OFF_HOURS
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : STANDARD
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Greeting                        : Alternate
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Greeting                        : Busy
```

```
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Error
  After greeting action          : restart-greeting
  Status                         : Enabled Indefinitely
 Greeting                        : Holiday
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Internal
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Off Hours
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Standard
  After greeting action          : take-message
  Status                         : Enabled Indefinitely
 Menu Key                        : *
  Action                         : sign-in
 Menu Key                        : #
  Action                         : skip-greeting

CALL HANDLER
 Display Name                    : Goodbye
 Language                        : INHERIT
 Schedule                        : All Hours
 Holiday Schedule                : Unknown
 Menu Delay                      : 1500
 Transfer Rule                   : ALTERNATE
  Transfer calls to              : GREETING
  Status                         : Disabled
 Transfer Rule                   : OFF_HOURS
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Transfer Rule                   : STANDARD
  Transfer calls to              : GREETING
  Status                         : Enabled Indefinitely
 Greeting                        : Alternate
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Busy
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Error
  After greeting action          : restart-greeting
  Status                         : Enabled Indefinitely
 Greeting                        : Holiday
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Internal
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Off Hours
  After greeting action          : take-message
  Status                         : Disabled
 Greeting                        : Standard
  After greeting action          : hang-up
  Status                         : Enabled Indefinitely
 Menu Key                        : 0
  Action                         : transfer Operator
 Menu Key                        : *
  Action                         : sign-in
 Menu Key                        : #
  Action                         : transfer Opening Greeting
```

```
DIRECTORY HANDLER
 Display Name                    : System Directory Handler
 Language                        : INHERIT
 Repeat Request                  : 1
 Search order                    : last then first
 Auto route                      : DISABLED
 Use * to exit                   : ENABLED
 Maximum matches                 : 8
 Exit action                     : transfer Opening Greeting
 No input action                 : transfer Goodbye
 No selection action             : transfer Goodbye
 Zero action                     : transfer Operator
```

The following example shows the output for the **show srsv auto-attendant** command when the call-handler argument is invoked with one parameter:

```
SRSV# show srsv auto-attendant call-handler "opening greeting"
CALL HANDLER
    Display Name                  : Opening Greeting
    Language                      : SYSTEM
    Schedule                      : All Hours
    Holiday Schedule              : Unknown
    Menu Delay                    : 1500
    Transfer Rule                 : Standard
    Transfer calls to             : GREETING
    Status                        : Disabled
    Greeting                      : Standard
    Languages                     : en_GB, en_US
    After greeting action         : transfer Operator
    Status                        : Disabled
    Menu Key                      : 0
    Action                        : transfer Operator
    Menu Key                      : 1
    Action                        : take-message
    Menu Key                      : 3
    Action                        : greeting ForSRSV
    Menu Key                      : 4
    Action                        : DH System Directory Handler
    Menu Key                      : 5
    Action                        : greeting ForSRSV
    Menu Key                      : 6
    Action                        : greeting My AA
    Menu Key                      : 7
    Action                        : transfer harold
    Menu Key                      : 8
    Action                        : transfer 1002
    Menu Key                      : 9
    Action                        : DH Test-directory-handler
    Menu Key                      : *
    Action                        : sign-in
    Menu Key                      : #
    Action                        : transfer Operator
```

The following example shows the output for the **show srsv auto-attendant** command when the directory-handler argument is invoked with one parameter:

```
SRSV# show srsv auto-attendant directory-handler "system directory handler"
DIRECTORY HANDLER
    Display Name                  : System Directory Handler
    Language                      : INHERIT
    Repeat Request                : 1
    Search order                  : first then last
    Auto route                    : DISABLED
```

```
Use * to exit                   : ENABLED
Maximum matches                 : 30
Exit action                     : transfer Opening Greeting
No input action                 : transfer Goodbye
No selection action             : transfer Goodbye
Zero action                     : transfer Operator
```

Table 5 describes the significant fields relating to call handlers.

Table 5 show srsv auto-attendant Field Descriptions for Call Handlers

Field	Description
Display Name	The Cisco Unity Connection display name for the call handler.
Language	The language to use for the call handler. Can be one of these values: • INHERIT means inherit the language from the parent directory or call handler • SYSTEM means use the default system language • *language_code* means use the language indicated by the language code
Schedule	The name of the schedule.
Holiday Schedule	The name of the holiday schedule. If there is no holiday schedule set, displays “Uknown”.
Menu Delay	Time to delay after input before processing
Message Recipient	The subscriber assigned to this call handler. Typically used as voice mailbox for the call handler. If there is no subscriber on the site, this value will not be configured.
Transfer Rule	The type of transfer rule.
Transfer calls to	The target of the transfer for the call handler. This is used when some part of the call flow attempts to transfer to this particular call handler. There are two settings that are available for this configuration: “transfer to greeting” and “transfer to a specific extension”.
Status	Status of the transfer rule and greeting. Can be disabled, enabled indefinitely, or enabled until a certain date.
Greeting	The type of greeting.
Languages	The languages in which the greeting has been recorded and configured by Cisco Unified SRSV-UMG.
After greeting action	The action to take after the greeting has played. See Table 7 for a list of the actions.
Menu Key	The menu digit provisioned by Cisco Unified SRSV-UMG.
Action	The action to take when the menu key is pressed.

Table 6 describes the significant fields relating to directory handlers.

Table 6 show srsv auto-attendant Field Descriptions for Directory Handlers

Field	Description
Display Name	The Cisco Unity Connection display name for the directory handler.
Language	The language to use for the directory handler. Can be one of these values: • INHERIT means inherit the language from the parent directory or call handler • SYSTEM means use the default system language • *language_code* means use the language indicated by the language code
Repeat Request	The number of times to prompt the caller for input.
Search order	The search method for the subscriber's first and last names to use when searching for subscribers. Value is either "first then last" or "last then first".
Auto route	If enabled, immediately transfers to the match if only one match is returned from the search. Value is either ENABLED or DISABLED.
Use * to exit	If enabled, allows the caller to exit the directory handler by pressing *. Value is either ENABLED or DISABLED.
Maximum matches	The maximum number of matches that the system can return to the subscriber by directory lookup.
Exit action	The action to take if the subscriber presses *, which exits the directory handler. See Table 7 for a list of the actions.
No input action	The action to take if the subscriber does not make an input. See Table 7 for a list of the actions.
No selection action	The action to take if the subscriber does not make a selection. See Table 7 for a list of the actions.
Zero action	The action to take when the subscriber presses 0. See Table 7 for a list of the actions.

Table 7 describes the actions that the directory handlers can make.

Table 7 show srsv auto-attendant Field Descriptions for Directory Handler Actions

Field	Description
transfer *call_handler_name*	Transfers the caller to the call handler with the display name of *call_handler_name*. The call handler may be a system or subscriber call handler. In some cases a phone number may be supplied when transferring to an alternate contact.
greeting *call_handler_name*	Transfers the caller to the greeting for the call handler with the display name of *call_handler_name*. The call handler may be a system or subscriber call handler.

Table 7 show srsv auto-attendant Field Descriptions for Directory Handler Actions

Field	Description
DH *directory_handler_name*	Sends the caller to the directory handler with the name *directory_handler_name*.
sign-in	Sends the caller to the voicemail login conversation.
hang-up	Terminates the call to the auto attendant.
restart-greeting	Replays the call handler greeting.
skip-greeting	Skips the greeting.
take-message	Sends the caller to the subscriber's mailbox that is configured for this call handler. If there is no subscriber for this site, this option will not be provisioned by Cisco Unified SRSV-UMG.

Related Commands

Command	Description
show srsv subscriber call-handler	Displays the Cisco Unified SRSV-CUE subscriber configuration provisioned by Cisco Unified SRSV-UMG.

show srsv configuration

To display the Cisco Unified SRSV configuration, use the **show srsv configuration** command in Cisco Unified SRSV-CUE EXEC mode.

show srsv configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unified SRSV-CUE EXEC

Command History

Cisco Unified SRSV-CUE Release	Modification
8.0	This command was introduced.

Usage Guidelines

Use this command to verify that Cisco UMG correctly provisioned the Cisco Unified SRSV-CUE device.

Examples

The following are sample outputs for the **show srsv configuration** command:

```
umg-1# show srsv configuration
SRSV Global Configuration:
    Central Voicemail Server      : cuc-8.srsv.lab
    PSTN Access Number            : 95551234
    MWI mode                      : auto
    MWI type                      : sub-notify
    Menu items changed prompt     : disabled

SRSV AA Handler Configuration:
    Opening Greeting Call Handler : Opening Greeting
    Operator Call Handler         : Operator
    GoodBye Call Handler          : Goodbye
    System Directory Handler      : System Directory Handler
    Site operator extension       : 1005

SRSV UMG Gateways:
    central-umg.srsv.lab
    backup-umg.srsv.lab
```

Table 8 describes the significant fields shown in the display.

Table 8 show srsv configuration Field Descriptions

Field	Description
Central Voicemail Server	The central voicemail server to which the Cisco Unified SRSV-UMG should deliver voice messages.
PSTN Access Number	The PSTN number that subscribers should call to access their central site stored voicemail when the Cisco Unified SRSV-CUE device is active.

Table 8 show srsv configuration Field Descriptions

Field	Description
MWI mode	The MWI mode for the Cisco Unified SRSV-CUE device.
MWI type	The MWI type configured for the Cisco Unified SRSV-CUE device.
Menu items changed prompt	If this option is enabled, the Cisco Unified SRSV-CUE device will play the “Some menu items may have changed” prompt when users log in.
Opening Greeting Call Handler	The display name of the Cisco Unity Connection opening greeting call handler provisioned on the Cisco Unified SRSV-CUE device.
Operator Call Handler	The display name of the Cisco Unity Connection operator call handler provisioned on the Cisco Unified SRSV-CUE device.
GoodBye Call Handler	The display name of the Cisco Unity Connection goodbye call handler provisioned on the Cisco Unified SRSV-CUE device.
System Directory Handler	The display name of the default system directory handler provisioned on the Cisco Unified SRSV-CUE device.
Site operator extension	The phone number of a local subscriber who will act as the operator during an outage.
SRSV UMG Gateways	The Cisco Unified SRSV-UMG systems that will be contacted to upload voice messages to the central voicemail system once the site has been reconnected to the central office.

show srsv subscriber call-handler

To display the Cisco Unified SRSV-CUE subscriber configuration provisioned by Cisco Unified SRSV-UMG, use the **show srsv subscriber call-handler** command in Cisco Unified SRSV-CUE EXEC mode.

show srsv subscriber call-handler [*user_name*]

Syntax Description

user_name	Name of a specific call handler for which you want to display the subscriber configuration. If you do not specify a name, the system displays all subscriber call handler configuration information.

Command Modes

Cisco Unified SRSV-CUE EXEC

Command History

Cisco Unified SRSV-CUE Release	Modification
8.0	This command was introduced.

Examples

The following example shows the output for the **show srsv subscriber call-handler** command when it is entered with no arguments:

```
SRSV# show srsv subscriber call-handler

CALL HANDLER
    Display Name                : pparker
    Language                    : INHERIT
    Menu Delay                  : 1500
    Message Recipient           : pparker
    Transfer Rule               : Standard
    Transfer calls to           : 1013

CALL HANDLER
    Display Name                : mjwatson
    Language                    : INHERIT
    Menu Delay                  : 1500
    Message Recipient           : mywatson
    Transfer Rule               : Standard
    Transfer calls to           : 1014
```

The following example shows the output for the **show srsv subscriber call-handler** command with a call handler specified:

```
SRSV# show srsv subscriber call-handler pparker

CALL HANDLER
    Display Name                : pparker
    Language                    : INHERIT
    Menu Delay                  : 1500
    Message Recipient           : pparker
    Transfer Rule               : Standard
    Transfer calls to           : 1013
```

For descriptions of the output fields, see Table 5.

Related Commands

Command	Description
show srsv auto-attendant	Displays the Cisco Unified SRSV-CUE auto-attendant configuration status that is provisioned by the Cisco UMG.

show srsv system

To display the system schedule and holiday information that is learned from Cisco Unity Connection, which can be used for debugging purposes, use the **show srsv system** command in Cisco UMG EXEC mode. This command is useful for validating transfer rules and greetings based on configured holidays and schedules.

show srsv system [holiday *holiday_name* | **schedule** *schedule_name*]

Syntax Description

holiday *holiday_name*	Name of a specific holiday for which you want to see information.
schedule *schedule_name*	Name of a specific schedule for which you want to see information.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco Unified SRSV-CUE Release	Modification
8.6	This command was introduced.

Usage Guidelines

You must use Cisco Unity Connection, and then reprovision the SRSV-CUE device from Cisco UMG, to enter or update the system schedule or holiday information. Each holiday schedule has a unique name and is made up of one or more user-entered holidays. Each system schedule has a unique name and is made up of one or more user-entered schedules.

Examples

The following example shows the output for the **show srsv system** command when it is entered with the **holiday** argument:

```
SRSV# show srsv system holiday

Holiday Schedule holiday-1
Holiday Name: april
  Date(s)                       : Apr 21, 2011
  Duration                      : All Day
Holiday Schedule holiday-reg
Holiday Name: Name not specified
  Date(s)                       : Jun 2, 2011
  Duration                      : All Day
```

The following example shows the output for the **show srsv system** command when it is entered with the **schedule** argument:

```
SRSV# show srsv system schedule

Schedule weekdays-credits
Detail Item: weekdays
  Start                         : 8:00 AM
  End                           : 2:00 PM
  Days                          : M, T, W, Th, F
```

```
Schedule All Hours
Detail Item: Name not specified
  Start                             : 12:00 AM
  End                               : End Of Day
  Days                              : M, T, W, Th, F, S, Su
Schedule regression-week
Detail Item: reg
  Start                             : 11:00 AM
  End                               : 5:30 PM
  Days                              : M, T, W, Th, F
Schedule Weekdays
Detail Item: test
  Start                             : 8:00 AM
  End                               : 9:00 PM
  Days                              : M, T, W, Th
```

show srsx alerts

To display the alerts received from all Cisco Unified survivable remote systems, use the **show srsx alerts** command.

show srsx alerts [**critical** | **error** | **warning** | **info**] [**detailed**]

Syntax Description

critical	Displays critical level alerts.
error	Displays warning level alerts.
warning	Displays error level alerts.
info	Displays informational level alerts.
detailed	Displays detailed information about the alert. Can be used alone or with any of the other arguments.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.6	Updated this command to include the **detailed** keyword.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx alerts** command:

```
umg-1# show srsx alerts

Level  |System      |Date                  |Description

WARNING|central-umg |Mon, Mar 22, 09:16 AM|Central telephony service server cucm.srsv.lab
could not be contacted for provisioning.
INFO   |central-umg |Mon, Mar 22, 09:17 AM|Central telephony service server cucm.srsv.lab
new SRST reference branch-bos-srst detected.
```

The following is an example of the **show srsx alerts detailed** command:

```
umg-1# show srsx alerts detailed
Level: ERROR
System: srsv-umg
Date: Fri, Apr 8, 06:02 PM
Description: SRSV provisioning failed for site srsv26.srsv.bxb.lab for various reason(s).
Check details link for more information
Details:
  Failed to retrieve SRSV dist. lists
  Failure to create subscriber tdennler @ 6001(6001)
**********
Level: INFO
System: srsv-umg
```

```
Date: Fri, Apr 8, 05:43 PM
Description: SRSV srsv26.srsv.bxb.lab upgraded to 8.6.2
Details:
  The SRSV upgrade completed upgrading to a newer image.
**********
Level: INFO
System: srsv-umg
Date: Fri, Apr 8, 05:43 PM
Description: SRSV srsv28.srsv.bxb.lab upgraded to 8.6.2
Details:
  The SRSV upgrade completed upgrading to a newer image.
**********
```

The following is an example of the **show srsx alerts info detailed** command:

```
umg-1# show srsx alerts info detailed
Level: INFO
System: srsv-umg
Date: Fri, Apr 8, 05:43 PM
Description: SRSV srsv26.srsv.bxb.lab upgraded to 8.6.2
Details:
  The SRSV upgrade completed upgrading to a newer image.
**********
Level: INFO
System: srsv-umg
Date: Fri, Apr 8, 05:43 PM
Description: SRSV srsv28.srsv.bxb.lab upgraded to 8.6.2
Details:
  The SRSV upgrade completed upgrading to a newer image.
**********
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx central-voicemail-server	Displays the central voicemail servers available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx branch-call-agent

To display information about all the SRST sites that have been learned from the central Cisco Unified Communications Manager, use the **show srsx branch-call-agent** command in Cisco UMG EXEC mode.

show srsx branch-call-agent [*name*]

Syntax Description

name	(Optional) Name of a specific SRST reference name.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.5	This command was introduced.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which Cisco recommends that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx branch-call-agent** command:

```
se-10-86-27-64# show srsx branch-call-agent
SRST Reference Name|SRST Host    |Platform    |CUCME Version|Router Username
----------------------------------------------------------------------------
2821_branch1       |172.16.0.1   |2821        |8.5          |admin
1861               |192.168.203.7|--          |--           |cisco
test_branch1       |202.202.202.1|--          |--           |cisco
2951-branch        |223.223.223.1|CISCO2951/K9|8.5          |admin
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx central-voicemail-server	Displays the central voicemail servers available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx branch-voicemail-server

To display the list of configured Cisco Unified SRSV devices, details for the specified Cisco Unified SRSV devices, or a list of the Cisco Unified SRSV devices that are not yet assigned, use the **show srsx branch-voicemail-server** command.

show srsx branch-voicemail-server [**unassigned** | *hostname*]

Syntax Description

unassigned	Displays the Cisco Unified SRSV devices that are not assigned to any site.
hostname	Hostname of a specific Cisco Unified SRSV device.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco UMG GUI, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx branch-voicemail-server** command:

```
umg-1# show srsx branch-voicemail-server

Hostname          |SRST Gateway     |Module Type|Memory|Serial Number
____________________________________________________________________
bos-srsv.srsv.lab|bos-srst.srsv.lab|NME        |512 mb|ABC12344M19
```

The following is an example of the **show srsx branch-voicemail-server** command asking for unassigned devices:

```
umg-1# show srsx branch-voicemail-server unassigned

Hostname          |SRST Gateway     |Module Type|Memory|Serial Number
____________________________________________________________________
nyc-srsv.srsv.lab|nyc-srst.srsv.lab|NME        |512 mb|DEF87644N22
```

The following is an example of the **show srsx branch-voicemail-server** command with a device specified:

```
umg-1# show srsx branch-voicemail-server srsv1.cisco.com

Hostname:      |bos-srsv.srsv.lab
________________________________________________
Module Type:   |NME
Memory:        |512 mb
Serial Number:|ABC12344M19
```

Related Commands

Command	Description
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx central-voicemail-server	Displays the central voicemail servers available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx central-call-agent

To display the list of configured Cisco Unified Communications Manager systems or details for the specified Cisco Unified Communications Manager system, use the **show srsx central-call-agent** command.

show srsx central-call-agent [*hostname* [**srst-references** | **nodes**]]

Syntax Description

hostname	Hostname of a specific Cisco Unified Communications Manager system.
srst-references	Displays the Cisco Unified SRST references for the specified Cisco Unified Communications Manager system.
nodes	Displays all the nodes discovered for the Cisco Unified Communications Manager system.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.6	Updated this command with the following: • Adds the *nodes* argument which lists all the nodes discovered for the Cisco Unified Communications Manager system. • In the output, displays the cluster name instead of the hostname. • In the output, displays the cluster name for the Cisco Unified Communications Manager system as well as the hostnames of the configured primary and secondary servers. • In the output, displays the default Cisco Unity Connection to use on new sites by cluster name instead of by hostname. • In the ourput, removed the IP address and managed sites information.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx central-call-agent** command:

```
umg-1# show srsx central-call-agent
Name |Provisioning|SRST-References
----------------------------------
CUCM8|enabled     |7
```

The following is an example of the **show srsx central-call-agent** command with a central call agent specified:

```
umg-1# show srsx central-call-agent CUCM8
```

```
Name:                          CUCM8
AXL Username:                  Administrator
AXL Password:                  *******
AXL Pacing:                    0 (milliseconds)
Provisioning Schedule:         Every day at 12:00 am
Default Voicemail:             CUC 8.5
Provisioning:                  enabled
Site Provision Enable Default:enabled
Primary Node:                  CentralCA.srsv.bxb.lab
Secondary Node:                CentralCA2.srsv.bxb.lab
```

The following is an example of the **show srsx central-call-agent** command with a central call agent specified and asking for a list of the Cisco Unified SRST references:

```
umg-1# show srsx central-call-agent ccm ccm.cisco.com srst-references

SRST-references          |IP Address
_______________________________________
branch-bos-srst          |192.168.1.2
branch-nyc-srst          |192.168.1.4
branch-sj-srst           |192.168.1.5
```

The following is an example of the **show srsx central-call-agent** command with a central call agent specified and asking for a list of the nodes discovered for the central call agent:

```
umg-1# show srsx central-call-agent CUCM8 nodes

Nodes
_______________________________________
CentralCA.srsv.bxb.lab
CentralCA2.srsv.bxb.lab
```

Related Commands

Command	Description
show srsx central-voicemail-server	Displays the central voicemail servers available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.

show srsx central-voicemail-server

To display the list of configured Cisco Unity Connection systems or details for the specified Cisco Unity Connection system, use the **show srsx central-voicemail-server** command.

show srsx central-voicemail-server [*hostname* [**nodes**]]

Syntax Description

hostname	Hostname of a specific Cisco Unity Connection system.
nodes	Displays all the nodes discovered for the Cisco Unity Connection system.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.6	Updated this command with the following: • Adds the *nodes* argument which lists all the nodes discovered for the Cisco Unity Connection system. • In the output, displays the cluster name instead of the hostname. • In the output, displays the cluster name for the Cisco Unity Connection system as well as the hostnames of the configured primary and secondary servers.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx central-voicemail-server** command:

```
umg-1# show srsx central-voicemail-server

Name           |Provisioning
___________________________
CUC 8.5        |enabled
```

The following is an example of the **show srsx central-voicemail-server** command with a Cisco Unity Connection specified:

```
umg-1# show srsx central-voicemail-server "CUC 8.5"

Name:              CUC 8.5
REST Username:     CucUser
REST Password:     ******
REST Pacing:       0 milliseconds
Provisioning:      enabled
Primary Node:      CentralVM.srsv.bxb.lab
Secondary Node:    CentralVM2.srsv.bxb.lab
```

The following is an example of the **show srsx central-voicemail-server** command with a Cisco Unity Connection specified and asking for a list of the cluster host peers that belong to the cluster:

```
umg-1# show srsx central-voicemail-server “CUC 8.5” nodes

Nodes
_______________________________________
CentralVM.srsv.bxb.lab
CentralVM2.srsv.bxb.lab
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx provisioning-history

To display the provisioning history for all sites, use the **show srsx provisioning-history** command.

show srsx provisioning-history

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.5	The display output was modified to include the Ephones Provisioned column.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx provisioning-history** command in Cisco UMG 8.0:

```
umg-1# show srsx provisioning-history

Site           |Last Result|Date                  |Last Success          |Users Provisioned
-------------------------------------------------------------------------------------------
branch-bos-srst|Success    |Mon, Mar 22, 09:24 AM|Mon, Mar 22, 09:24 AM|21
branch-nyc-srst|unknown    |                      |                      |0
branch-sj-srst |unknown    |                      |                      |0
```

The following is an example of the **show srsx provisioning-history** command in Cisco UMG 8.0:

```
umg-1# show srsx provisioning-history

Site           |Last Result|Date                  |Last Success          |Users Provisioned
-------------------------------------------------------------------------------------------
branch-bos-srst|Success    |Mon, Mar 22, 09:24 AM|Mon, Mar 22, 09:24 AM|21
branch-nyc-srst|unknown    |                      |                      |0
branch-sj-srst |unknown    |                      |                      |0
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx site

To display the list of sites managed by the Cisco UMG or to see details for the specified site, use the **show srsx site** command.

show srsx site [*sitename*]

Syntax Description

sitename	Name of a specific site.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.5	This command was modified to add support for E-SRST configurations. The following fields were added: SRST Provisioning, SRSV Provisioning, Router login username, Router login password.
8.6	This command was modified so that in the output, the central call agent and central voicemail servers are listed by their cluster names instead of by their hostnames.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx site** command:

```
umg-1# show srsx site

Site    |Provisioning|Call Agent   |Voicemail Server |SRST           |SRSV
_____________________________________________________________________________________
srsv1   |enabled      |CUCM8      |CUC 8.5            |192.168.1.2    |bos-srsv.srsv.lab
srst1   |enabled      |CUCM8      |CUC 8.6            |192.168.1.4    |bos-srsv.srsv.lab
srsv2   |enabled      |CUCM7      |CUC 7.0            |192.168.1.5    |bos-srsv.srsv.lab
```

The following is an example of the **show srsx site** command with a site specified:

```
umg-1# show srsx site srsv1

Sitename:                 srsv1
Central Call Agent:       CUCM8
Central Voicemail Server: CUC 8.5
Srst Reference:        srst1
Srst Address:             192.168.28.131
Srsv Voicemail:           bos-srsv.srsv.lab
Template:                 default
Provisioning:             enabled
SRSV provisioning         enabled
SRST provisioning         enabled
Router login username     bxb100 admin
Router login password     *******
```

Related Commands

Command	Description
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx central-voicemail-server	Displays the central voicemail servers available on the Cisco Unified SRSV system.
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.

show srsx site-template

To display the site provisioning templates used when provisioning SRSV-CUE devices, use the **show srsx site-template** command.

show srsx site-template [**default**] | [*name*] | [**auto-learned**]

Syntax Description

default	Displays default site provisioning templates.
name	Displays details for the selected template.
auto-learned	Displays site provisioning templates for auto-learned sites.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.5	This command was modified to add support for E-SRST configurations. The Autolearn Voicemail Pilot field was added.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx site-template** command:

```
umg-1# show srsx site-template

Name   |Voicemail Pilot
_______________________
default|1001
```

The following is an example of the **show srsx site-template** command in which the voicemail pilot has been auto-learned:

```
umg-1# show srsx site-template

Name   |Voicemail Pilot
_______________________
default|Auto-Learned
```

The following is an example of the **show srsx site-template** command with a template specified:

```
umg-1# show srsx site-template default

Template Name:                default
Autolearn voicemail pilot     enabled
Voicemail Pilot:              1001
Live Record:                  disabled
Live Record Beep:             disabled
Live Record Beep Interval:    15
Live Record Beep Duration:    250
Live Reply:                     disabled
Mailbox Size (seconds):         3600
Maximum Message Size (seconds): 240
Message Expiration (days):      30
Menu items changed prompt:      disabled
MWI mode:                       Automatic
MWI type:                       Sub-notify
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx software-upgrade

To determine if the system is enabled for an SRSV-CUE device software upgrade, and to see which version is on the system, use the **show srsx software-upgrade** command.

show srsx software-upgrade

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.6	This command was introduced.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx software-upgrade** command:

```
umg-1# show srsx software-upgrade

Software Upgrade Enabled : true

Platform|Version   |Size
------------------------------------------------------------------------------------------
nmx     |9.0.1     |805 MB
sme     |9.0.1     |811 MB
```

show srsx srsv-upload-history

To display the voicemail upload history for all Cisco Unified SRSV devices, use the **show srsx srsv-upload-history** command.

show srsx srsv-upload-history

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco UMG graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx srsv-upload-history** command:

```
umg-1# show srsx srsv-upload-history

SRSV             |Total Voicemails|Undeliverable|Start                 |End

bos-srsv.srsv.lab|3               |0            |Mon, Mar 22, 10:30 AM|Mon, Mar 22, 10:31
AM
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show srsx system-settings

To display the global Cisco Unified survivable remote system configuration values, use the **show srsx system-settings** command.

show srsx system-settings

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco UMG GUI, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx system-settings** command:

```
umg-1# show srsx system-settings

Secondary UMG:    backup-umg.srsv.lab
Use TLS Security: Off
SRSV UMG Secret:  ********
SRSV REST Secret: ********
```

Related Commands

Command	Description
show srsx branch-voicemail-server	Displays the SRSV-CUE devices on the Cisco Unified SRSV system.
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRSV system.
show srsx site	Displays the sites on the Cisco Unified SRSV system.

show statistics

To display a statistics report, use the show statistics command in Cisco UMG EXEC mode.

show statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Examples

The following example shows a partial output from the **show statistics** command:

```
umg-1# show statistics
SMTP Receive Failure: 0
SMTP Sent Failure: 0
SMTP Rejected: 0
NDR Message Generated: 0
DDR Message Generated: 0
Number of Lookup Request: 0
SDL Message Received: 0
SDL Message Sent: 0
SBM Message Received: 11
DirEx Message Received: 6
DirEx Message Send: 25
VPIM Message Received: 12
VPIM Message Sent: 12
Total SMTP Message Received: 18
Total SMTP Message Sent: 37
```

Related Commands

Command	Description
directory exchange messaging-gateway request	Manually forces data convergence between the current messaging gateway and its peers by requesting either full directory exchange or directory updates.
directory exchange messaging-gateway send	Manually forces data convergence between the current messaging gateway and its peers, by sending either full directory exchange or directory updates.
ndr timeout	Configures a timeout window whose elapse will result in a non- delivery receipt (NDR).
show ddr timeout	Displays the timeout window whose elapse will result in a DDR.
show list	Displays a list of the system distribution lists (SDLs) that are configured.
show list privilege	Displays the authorized senders for SDLs.
show ndr timeout	Displays the timeout window whose elapse will result in a NDR.

Command	Description
show translation-rule	Displays translation rules for the SMTP header for each supported endpoint.
translation-rule	Configures translation rules for both message header and SMTP header for each supported endpoint.
vpim external	Configures NAT entries for peer messaging gateways or endpoints.

software download uninstall

To upgrade to a newer version of Cisco UMG software, use the **software install upgrade** command in Cisco UMG EXEC mode.

software install upgrade {**pkg** *umg-package***.*pkg*** |
url ftp://*ftp-server-ip-address***/***umg-package***.*pkg***}

Syntax Description

pkg *umg-package***.*pkg***	Specifies a package name.
url ftp://*ftp-server-ip-address***/***umg-package***.*pkg***	Specifies the FTP server information.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to upgrade to a newer version of Cisco UMG software.

Neither Cisco UMG Release 1.0.1 nor Cisco UMG Release 8.0.1 supports upgrades.

Examples

The following is an example of the command to upgrade to a newer version of Cisco UMG software.

```
umg-1# software install upgrade url ftp://192.0.2.24/umg.nme.1.0.1.pkg
```

The following is an example of the command to upgrade to a newer version of Cisco UMG software if the FTP server has been configured or the software files have been downloaded previously with the **software download upgrade** command:

```
umg-1# software install upgrade pkg umg.nme.1.0.1.pkg
```

Related Commands

Command	Description
software download upgrade	Configures the FTP server information.
software download upgrade	Downloads the files for a future upgrade.
software install clean	Installs a new version of the Cisco UMG software and cleans the disk.
software install downgrade	Downgrades the current Cisco UMG software to an older version.

T

Last Updated: August 5, 2011

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

trace

trace

To view trace messages, use the **trace** command in Cisco UMG EXEC mode.

trace *{module {entity {activity}}}*

Syntax Description

module	Trace module values. Can be any combination of the values listed in Table 9. Entering **all** gives information for all the modules.
entity	Entity values. Each module has one or more entity values associated with it. Can be any combination of the values for that particular module. See Table 9. Entering **all** gives information for all the entities.
activity	Activity values. Each entity has one or more activity values associated with it. Can be any combination of the values for that particular entity. See Table 9. Entering **all** gives information for all the activities.

Table 9 lists all the modules, entities, and activities.

Table 9 Module, Entity, and Activity Values

Module Name	Entity Name	Activity Name	Description
aaa	authorization	jaas	Used for authentication, authorization, and accounting (AAA) debugging
		pam	
	authentication	jaas	
		pam	
	acct	service	
		queue	
		library	
dns	cache	daemon	Domain Name Service (DNS) debugging
		localzone	
		startup	
		ethconfig	
	enablecheck	dns_check	
		debug	
		ipv4_check	
		hostname_check	
		results	
		dns_query	
	resolver	send	
		receive	
	server	ask	
		answer	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
management	agent	debug	Management debugging
um2	store	attributes	User manager 2 (users and groups) debugging
		privilege	
		group	
		users	
	manager	search	
		attributes	
		groups	
		users	
		privileges	
		event	
		security	
		factory	
webInterface	group	save	Cisco UMG GUI debugging
		delete	
		read	
	user	save	
		delete	
		read	
	aaa	read	
	privileges	action	
	axl	delete	
		post	
		read	
	backupRestore	serverConfiguration	
		restore	
		backup	
	controller	startup	
		request	
	session	login	
		logout	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
webInterface (continued)	sysdb	get	Cisco UMG GUI debugging (continued)
		set	
		providerStart	
		providerGet	
		providerStop	
		providerSet	
	database	query	
		connection	
		results	
sysdb	producer	nodeDetach	Interprocess communication debugging
		nodeAttach	
		timeLimit	
		nodeHandle	
		mkdir	
		attrCreate	
		attrDelete	
		rmdir	
	lock	acquire	
		release	
		wait	
	traversal	directory	
		attribute	
		node	
	misc	allocation	
	provider	stop	
		other	
		events	
		deadline	
		get	
		startup	
		commit	
		check	
	utility	metaInfo	
		dealloc	
		chdir	
		nameLookup	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
sysdb (continued)	consumer	set	Interprocess communication debugging (continued)
		get	
		nameLookup	
limitsManager	vmcapacity	xdebug	System limits debugging
		debug	
		info	
		warning	
		crash	
		error	
	platform	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	cli	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	api	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	sysdb	xdebug	
		debug	
		info	
		warning	
		crash	
		error	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
limitsManager (continued)	port	xdebug	System limits debugging (continued)
		debug	
		info	
		warning	
		crash	
		error	
	language	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	vmport	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	license	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	utilities	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	ivr	xdebug	
		debug	
		info	
		warning	
		crash	
		error	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
limitsManager (continued)	vmmbox	xdebug	System limits debugging (continued)
		debug	
		info	
		warning	
		crash	
		error	
	histrep	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	feature	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	mainthread	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
operation	manager	ucid	Command authorization debugging
		operation	
license	debug	core_errors	CSL debugging
		events	
		core_events	
		ipc	
		errors	
		agent_info	
		agent_error	
		agent_all	
		core_all	
	monitor	monitor-license	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
BackupRestore	BackupRestore	CONF	Backup and restore debugging
		SERVER	
		INIT	
		OPERATION	
		HISTORY	
dbclient	debug	level0	Database client debugging
		level1	
		level2	
		level3	
		level4	
		level5	
	sysdb	set	
		get	
		commit	
	database	transaction	
		query	
		garbageCollect	
		connection	
		largeobject	
		mgmt	
		execute	
		results	
superthread	main	startup	Core Java services debugging
	parser	parse	
snmp	JNI	Net-SNMP	SNMP debugging
	agent	debug	
rest	base_resources	info	Common REST interface debugging
		warn	
		error	
	common	info	
		warn	
		error	
security	policy	password	PIN and password authentication policy debugging
		pin	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
umg	direx	receiver	Cisco UMG VPIM directory exchange debugging
		sender	
		message	
		mgmt	
		scheduler	
		processor	
	translation	CACHE	Cisco UMG VPIM translation rule debugging
		RULE	
	db	query	Cisco UMG VPIM database debugging
		connection	
	routing	gateway	Cisco UMG VPIM network message routing debugging
		spool	
		route	
		sender	
		monitor	
	system	cli	Cisco UMG VPIM CLI debugging
	sdl	servlet	Cisco UMG VPIM system distribution list debugging
		cli	
		messaging	
	smtp	debug	Cisco UMG VPIM SMTP service debugging
		wire	
		error	
	global	0_crash	Cisco UMG VPIM global settings debugging
		1_error	
		2_warn	
		3_debug	
		4_info	
	lookup	request	Cisco UMG VPIM lookup debugging
	registration	0_crash	Cisco UMG VPIM remote voicemail system registration debugging
		1_error	
		2_warn	
		3_debug	
		4_info	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
ntp	ntp	loopstatus	Network time protocol debugging
		clkselect	
		clkadj	
		clockstatus	
		packets	
		clkvalidity	
		peerstats	
		event	
		loopfilter	
udppacer	udppacer	debug	Voice UDP debugging
		ccncall	
		statistics	
		block_starve	
srsx	gui	actions	Cisco UMG SRSx GUI debugging
		error	
	registration	debug	Cisco UMG SRSx device registrationdebugging
		error	
	cli	debug	Cisco UMG SRSx CLI debugging
		error	
	controller	info	Cisco UMG SRSx controller debugging
		trace	
		debug	
		warning	
		error	
	upload	debug	Cisco UMG SRSV voicemail upload debugging
		error	
		rest	
	mgmt	debug	Cisco UMG SRSx management interface debugging
		error	
	srsv-engine	info	Cisco UMG SRSV provisioning engine debugging
		trace	
		debug	
		warning	
		error	

Table 9 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
srsx (continued)	service-point	info	Cisco UMG SRSx service point debugging
		trace	
		debug	
		warning	
		error	
	vm-server-client	info	Cisco UMG SRSx central voicemail server communication debugging
		trace	
		debug	
		warning	
		error	
	call-agent-client	info	Cisco UMG SRSx central call agent server communication debugging
		trace	
		debug	
		warning	
		error	
	srsv-secret-syncer	info	Cisco UMG SRSx shared secret synchronization debugging
		trace	
		debug	
		warning	
		error	
	site-manager	info	Cisco UMG SRSx site manager debugging
		trace	
		debug	
		warning	
		error	
	srst-engine	info	Cisco UMG E-SRST provisioning engine debugging
		trace	
		debug	
		warning	
		error	
		all	

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.
8.5	The **srst-engine** keyword was added.

Examples

The following example illustrates the use of the **trace srsx srsv-engine** command:

```
se-192-1-1-149# trace srsx srsv-engine all
```

Related Commands

Command	Description
log console monitor	Enables log monitor events for debugging.

GLOSSARY

A

AAA Authentication, authorization, and accounting. Specifies the failover functionality that you can optionally configure for the authentication server.

AIM2 Advanced integration module, second generation (AIM2-CUE).

auto attendant An automated attendant (auto attendant) allows you to create and change greetings that callers hear when your telephone system answers incoming calls. A welcome greeting is the first message that a caller hears when calling your company. A standard welcome greeting and other system messages are provided as part of the auto attendant included with Cisco UMG. These messages are collected into a script that guides the caller in performing various functions, such as pressing buttons to reach various departments and entering the extension for an employee.

B

backup and restore Captures the configuration of the Cisco UMG so that it can be restored later in case the Cisco UMG configuration becomes corrupted.

branch voicemail server Generic term for an SRSV-CUE device.

C

call handler A greeting that is played to listeners.

capability Defines what functions a group can perform.

central call agent Generic term for the Cisco Unified Communications Manager.

central voicemail server Generic term for the Cisco Unity Connection.

Cisco UMG GUI Provides the primary administrative interface for configuring the Cisco UMG system or Enhanced Survivable Remote Site Telephony (E-SRST). You can access the Cisco UMG graphical user interface from either Firefox or Internet Explorer.

Cisco Unified Communications Manager A call agent.

Cisco Unified SRST Cisco Unified Survivable Remote Site Telephony. A system, made up of a central office and one or more branch offices, that provides telephony services during a WAN outage.

Cisco Unified SRSV Cisco Unified Survivable Remote Site Voicemail. A system, made up of a central office and one or more branch offices, that provides voicemail services during a WAN outage.

Cisco Unified Messaging Gateway Cisco UMG. Software that has three main purposes: to configure VPIM networks, to support Enhanced Survivable Remote Site Telephony (E-SRST), and to run the Cisco Unified SRSV system.

Cisco Unity Connection A voicemail system.

cluster A group of connected devices, such as Cisco Unity Connection, that are managed as a single entity. The devices can be in the same location, or they can be distributed across a network. Any server in the cluster can do the job of any other server in the cluster.

D

DER A binary TLS certificate type.

Domain name system (DNS) server The DNS server provides translation from hostnames to IP addresses.

E

Enhanced Survivable Remote Site Telephony (E-SRST) Provides automated remote site provisioning of the following advanced telephony features in survivable mode by gathering the information from Cisco Unified Communications Manager about:

- 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 park and group call park
- Call pickup
- Hunt groups

F

Full Name Full group name. Callers use the full name to access the extension using the dial-by-name feature.

G

Group ID Name of a group of users, usually created to assign members to a general-delivery mailbox.

H

high availability Supports voicemail upload through a secondary Cisco UMG. The secondary Cisco UMG acts as a backup for the primary Cisco UMG in the event that the primary Cisco UMG system is unreachable by the SRSV-CUE devices.

I

ISM-SRE The Cisco ISM-SRE is a Services Ready Engine (SRE) internal service module that runs Cisco-authorized applications and plugs into a host Cisco ISR G2.

ISR Cisco Integrated Services Router.

ISR G2 Cisco Integrated Services Router Generation 2.

L

live record A voicemail system feature that allows you to record a phone conversation to your voice mailbox so that you can listen to it again later.

live reply A voicemail system feature that allows you, when listening to a message by phone, to call the user who left the message.

log file A file that lists actions that have occurred.

N

NAT Network Address Translation

Network time protocol (NTP) Used to set the system time to avoid manual configuration of the time. Using NTP helps the system to keep the system time synchronized with the NTP server in case there is a drift in the system clock. Typically Cisco Unified SRSV uses the host router as the NTP server, but you can also use other standard public NTP servers. NTP typically provides accuracy within a millisecond on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time. Typical NTP configurations utilize multiple redundant servers and diverse network paths to achieve high accuracy and reliability.

NME-CUE Network Module Enhanced-Cisco Unity Express (NME-CUE).

O

operation A set of CLI commands or GUI functions.

Operator extension Extension that callers can dial to reach the operator from the auto attendant and voice-mail systems. (Callers can also reach the operator by other methods.)

Owner User or group ID of the user or group that owns a mailbox. Mailbox owners can add or delete users to and from a general-delivery mailbox and can delete the general-delivery mailbox. (If you assign a group as the owner of a general-delivery mailbox, all members in that group have owner privileges for the mailbox.)

P

PAT Port Address Translation. Network address translation (NAT) variant where a single public address is shared for multiple private network devices and port translation is used to expose private services to the public network.

PEM Privacy Enhanced Mail. A TLS certificate type. It is a Base64 encoded DER certificate, enclosed between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”.

pilot number The number used to reach a desired service such as voicemail or auto attendant. Typically this number is not visible on IP phones as it is hidden behind the voicemail button on the phone which dials the pilot automatically.

Primary E.164 number User or group’s primary telephone number, including area code.

privilege A set of operations that are grouped together. Privileges are assigned to users.

provisioning The processing performed by an Cisco UMG device to configure SRSV-CUE devices for survivable voicemail services.

R

REST A programmatic interface.

S

secondary node A replica of the primary node. It is configured for use in case the primary node fails.

site A site is created on the Cisco UMG device based on the existence of a Cisco Unified SRST reference configured on the Cisco Unified Communications Manager.

site activity When the Cisco UMG system uploads voicemail.

SM-SRE The Cisco SM-SRE is a Services Ready Engine (SRE) service module that runs Cisco-authorized applications and plugs into a host Cisco ISR G2.

SMTP Simple Mail Transfer Protocol (SMTP). standard for e-mail transmissions across the Internet. Formally SMTP is defined in RFC 821 (STD 10) as amended by RFC 1123 (STD 3) chapter 5. The protocol used today is also known as ESMTP and defined in RFC 2821.

SRST See Cisco Unified SRST.

SRST reference A gateway that can provide limited Cisco Unified Communications Manager functionality when all other Cisco Unified Communications Manager servers for a device are unreachable.

SRSV See Cisco Unified SRSV.

SRSV-CUE Survivable Remote Site Voicemail—Cisco Unity Express. A device at the branch office that provides local voicemail services during a WAN outage. SRSV-CUE is a separate application from Cisco Unity Express, and is required as part of the Cisco UMG system.

SRSV-UMG Survivable Remote Site Voicemail—Unified Messaging Gateway. A device at the central office that mainly does the following: provisions the SRSV-CUE devices and uploads voicemail messages to Cisco Unity Connection after a WAN outage.

T

trace buffer Collection of debug traces for system activity.

U

Unified Messaging Gateway See Cisco UMG.

UMG interface See Cisco UMG GUI.

INDEX