Avaya Hospitality Messaging Server 400 Installation and Commissioning

Release 2.0
NN42350-301, Standard 06.02
March 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release....7
- Features....7
  - Platform servers....7
  - Avaya Communication Server 1000 Signaling Server....8
  - Windows 2003 operating system....8
  - Voice Channel Grouping....8
  - SQL support....8
  - Property Management System Interface over TCP/IP....8
  - Script-based call flows....9
  - Group code support....9
  - Operator Console Interface....9
  - VPIM networking-Avaya CallPilot™ integration....9
  - HMS 400 Release 2.0 keycodes....9
- Other changes....10

Chapter 2: Introduction....11

Chapter 3: Installation preparation....13
- Site inspection checklist....13
- Preinstallation checklist....14
- Site preparation checklist....14

Chapter 4: Network cabling installation....17
- HMS 400 PMSI serial connections....17
- HMS 400 to Property Management System connection specifications....18
- HMS 400 to CS 1000E MGC interface....19
  - MGC interface connections....19
  - Crossover configuration....20
  - Straight-through configuration....20
  - RS-232 signals....21
- HMS 400 PMSI IP connections....22

Chapter 5: CS 1000 configuration (Release 7.0)....25
- CS 1000 configuration procedures....25
- CS 1000 configuration navigation....26
- Checking LDN0....27
- Defining LDN0....27
- Defining customer support for ISDN....28
- Configuring the SIP gateway....28
- Enabling a SIP virtual trunk....30
- Creating a virtual D-Channel....31
- Configuring zones (LD 117)....31
- Creating a virtual route (LD 16)....33
- Creating virtual trunks (LD 14)....34
- Enabling the D-Channel....35
- Checking codec and QoS settings....35
- Disabling the G.729 codec on Media Gateways....36
- Creating the HMS 400 pilot number....37
- Creating a PMS PTY port....37

Creating additional PTY ports....38
Creating a PMS TTY Port for serial connection....39
Creating a PMS PTY user name and password....40
Configuring PMSI login with UCM on Security Domain....41
Confirming subscribers....42
Creating an ACD queue....43

Chapter 6: Avaya Hospitality Messaging Server 400 hardware installation....45
HMS 400 hardware installation procedures....45
HMS 400 hardware installation procedures task flow....46
Unpacking the HMS 400....47
Removing the server top cover....48
Job aid....49
Inspecting the server interior....49
Job aid....50
Installing the dongle (HP DL360G7 server only)....51
Installing a multiport serial adapter....55
Job aid....56
Replacing the server top cover....57
Installing the HMS 400....57
Connecting peripherals to the HMS 400....58
Job aid....58
Connecting the modem to the HMS 400 server....59
Connecting the HMS 400 server to power....60
Starting HMS 400....60

Chapter 7: Avaya Hospitality Messaging Server 400 software installation....63
Installing or restoring the HMS 400 image....63
Installing Auto Attendant software on the HMS 400 HP ProLiant server....64
Configuring Dialogic HMP....65

Chapter 8: Avaya Hospitality Messaging Server 400 server commissioning....67
Single-server configuration....67
Single-server configuration procedures....67
Entering a key code....70
Starting the Web configuration module in a Web browser....70
Changing the password....71
Configuring a single line....72
Configuring multiple lines....73
Configuring an entry point....74
Configuring the PMS setting....76
Configuring Communication Server 1000 settings....78
Configuring HMS 400 server settings....80
Configuring SIP Setting....81
Configuring Log Printer Setting....82
Multi-server configuration....82
Multi-server configuration procedures....83
Imaging servers....84
Restarting the servers....84
Configuring multi-server settings in HMS400 v2 Web UI....84
Configuring the Main Server IP in Data Sources (ODBC) for client servers....86
Starting the HMS 400 application....87

Chapter 9: Avaya Hospitality Messaging Server 400 system settings commissioning....89
Configuring Outcall Attempts....89
Configuring ring duration....90
Configuring default check in language....91
Configuring Message Housekeep....92
Configuring room change requirements....93
Configuring TUI settings....93
Configuring Guest Mailbox PIN options....95
Configuring AWU setting....96
Configuring Minibar setting....98
Configuring Room Status setting....101
Configuring Operator setting....101
Configuring VPIM shortcut....102
Editing the VPIM shortcut....103
Configuring additional VPIM options....103
Configuring Language Mapping....104
Configuring Remote Message Notification Setting....105

Chapter 10: Commissioning the Avaya Hospitality Messaging Server 400 database....107
Configuring a guest room....107
Adding extensions to a Guest Room....109
Configuring a single mailbox single extension Admin Mailbox....109
Configuring a multiple mailbox single extension Admin Mailbox....111
Configuring a single mailbox multiple extension Admin Mailbox....113
Adding an extension to an Admin Mailbox....114
Adding a mailbox to an Admin Mailbox....115
Viewing or deleting an extension....116
Creating users....117
Editing user details....118
Configuring Admin Classes of Service....119
Automatic file synchronization....121
Configuring Guest Classes of Service....122
Automatic file synchronization....125
Configuring an introductory message....125

Chapter 11: Common procedures....127
Starting the Avaya Hospitality Messaging Server 400 server....127
Stopping or restarting the HMS 400....128
Manually starting the Dialogic HMP service....128
Starting the Web configuration module in the HMS 400 application....129
Shutting down the multi-server system....129
Starting the multi-server system....130

Chapter 1: New in this release

The following sections detail what's new in *Avaya Hospitality Messaging Server 400 Installation and Commissioning, NN42350-301* for HMS 400 Release 2.0.

Navigation:

- Features on page 7
- Other changes on page 10

Features

See the following sections for information about feature changes.

- Platform servers on page 7
- Avaya Communication Server 1000 Signaling Server on page 8
- Windows 2003 operating system on page 8
- Voice Channel Grouping on page 8
- SQL support on page 8
- Property Management System Interface over TCP/IP on page 8
- Script-based call flows on page 9
- Group code support on page 9
- Operator Console Interface on page 9
- VPIM networking-Avaya CallPilot™ integration on page 9
- HMS 400 Release 2.0 keycodes on page 9

Platform servers

The Avaya Hospitality Messaging Server (HMS) 400 is installed on commercial off-the-shelf (COTS) servers that are provided with the system. For more information about platform servers, see *Avaya Hospitality Messaging Server 400 Fundamentals, NN42350-104*.

Avaya Communication Server 1000 Signaling Server

HMS 400 Release 2.0 connects to virtual trunks on the Avaya Communication Server 1000 (CS 1000) (Release 5.0 and later) Signaling Server employing Intel Host Media Processing (HMP) 3.0 software driver and API. The CS 1000 handles call processing tasks (incoming and outgoing), and HMS 400 handles the Real-time Transfer Protocol (RTP) sessions and Dual Tone Multi-Frequency (DTMF) transmission and processing. The CS 1000 still handles call routing.

Windows 2003 operating system

HMS 400 Release 2.0 is installed on the Windows 2003 operating system (OS). The Windows 2003 OS ensures continued OS support from Microsoft and interoperability with Microsoft SQL and .NET technology.

Voice Channel Grouping

In HMS 400 Release 2.0 on new systems, call routing occurs on the CS 1000 using dummy ACD queues, not the Group Hunt and Round Robin hunting used in Release 1.0.

SQL support

HMS 400 Release 2.0 replaces the Jet (Access) database, with the MySQL 5.0 Enterprise Edition database. The MySQL database offers improved stability and reduced chance of database corruption through the use of an intelligent data manager rather than direct queries to the database. MySQL offers a comprehensive security model, the ability to handle more simultaneous connections at higher speeds, and greater scalability. Therefore, you can deploy the HMS 400 in large implementations (more than 10 000 rooms).

Property Management System Interface over TCP/IP

HMS 400 Release 2.0 supports a TCP/IP interface between the Property Management System Interface (PMSI) module, the HMS 400, and the CS 1000 using IP. This interface eliminates unsightly cabling and removes the distance limitation of 50 feet with RS 232 links. The TCP/IP provides a more robust method of communication than the RS 232 links, permitting higher transaction speeds and reducing the likelihood of lost data packets. RS 323 links are still supported on new and upgraded HMS 400 2.0 systems.

Script-based call flows

All system call flows now run on Visual Basic (VB) scripts, which means anyone with some programming skills can read and understand a flow.

As a security measure, the system generates a CRC-32 checksum for each script file. The system performs a comparison each time you start HMS 400 to detect if you installed a patch that changed the scripts. If changes occur, a warning message appears and you must decide whether to continue (starting the system) or abort (perhaps to restore the scripts from backup).

Group code support

HMS 400 Release 2.0 supports group codes, permitting a simple method for configuring wake-up calls for specific groups, such as tour groups, and to form temporary distribution lists for hotel promotions and announcements. A distribution list is automatically created based on the group code created during check-in. Use group code to create custom welcome messages, distribution list messages, and group Auto Wake-Up messages.

Operator Console Interface

HMS 400 Release 2.0 supports an optional Operator Console application programming interface (API). This interface permits third-party operator consoles to control the HMS 400 Auto Wake-Up feature using a TCP/IP link. For more information about the Operator Console, see *Avaya Hospitality Messaging Server 400 Administration, NN42350-600*.

VPIM networking-Avaya CallPilot™ integration

HMS 400 Release 2.0 supports the Voice Profile for Internet Messaging (VPIM) Internet standard version 2. VPIM permits messaging between Avaya CallPilot™ and HMS 400, HMS 400 and Avaya CallPilot™, and between HMS 400 systems. Avaya does not support VPIM networking on non-Avaya systems. For more information about VPIM, see *Avaya Hospitality Messaging Server 400 Installation and Commissioning, NN42350-301*.

HMS 400 Release 2.0 keycodes

Avaya controls the feature set for each HMS 400 Release 2.0 system by issuing an encrypted keycode. This keycode enables only the features or capacities that you require.

Other changes

This document contains the following other changes:

- Changed references to Avaya HMS 400 servers to be generic.
- Added information to the section about confirming subscribers on Configuring PMSI login with UCM on Security Domain on page 41 .
- Added an attention note to the section Confirming subscribers on page 42 and a procedure to section Configuring AWU setting on page 96.
- Added a procedure on disabling the G.729 codec. See Disabling the G.729 codec on Media Gateways on page 36.
- Updated the *CS 1000 Configuration* chapter for Communication Server 1000 Release 6.0 and Release 7.0. See CS 1000 configuration (Release 7.0) on page 25.

Chapter 2: Introduction

This document explains how to install and commission the Avaya Hospitality Messaging Server 400.

Important:
Ensure that any cable you purchase is foil shielded for protection from EMI/RFI interference caused by surrounding office equipment and fluorescent lights.

- Installation preparation on page 13
- Network cabling installation on page 17
- CS 1000 configuration (Release 7.0) on page 25
- Avaya Hospitality Messaging Server 400 hardware installation on page 45
- Avaya Hospitality Messaging Server 400 software installation on page 63
- Avaya Hospitality Messaging Server 400 server commissioning on page 67
- Avaya Hospitality Messaging Server 400 system settings commissioning on page 89
- Commissioning the Avaya Hospitality Messaging Server 400 database on page 107
- Common procedures on page 127

Chapter 3: Installation preparation

Before you install the Avaya Hospitality Messaging Server 400 application, ensure you complete the checklists provided in this chapter.

Navigation:

- Site inspection checklist on page 13
- Preinstallation checklist on page 14
- Site preparation checklist on page 14

Site inspection checklist

Complete the following site inspection checklist before you install the HMS 400 hardware to ensure the installation site is ready for the hardware installation.

Table 1: Site inspection checklist

Check	Description
❒	Ensure that a water fire-retardant system is not in the chosen location. If a water fire-retardant system is activated accidentally, it can severely damage the server.
❒	Ensure that no heat sources are near the peripherals and ventilation.
❒	Ensure the area is clean and clear of debris.
❒	Ensure adequate space is available for all equipment.
❒	Ensure a desk, shelf, or table for the monitor, keyboard, mouse, and modem and are available. Additional space is needed for a multi-server environment.
❒	Ensure that an external analog phone line is available for the support modem. For multi-server systems, one analog line and modem is required for each server.
❒	Ensure enough power outlets for the server, monitor, and modem are available. Additional power outlets are required for multi-server systems.
❒	For multi-server systems, ensure that customer supplied 100/Gigabit BaseT Hub/Switch and CAT5 cables are available.

Preinstallation checklist

Complete the following preinstallation checklist to ensure all required information is available before you install the HMS 400 hardware.

Table 2: Preinstallation checklist

Check	Description
❒	Obtain the Communication Server 1000 (CS 1000) software version and ensure that you install the required dependency patches.
Yes No	Is the Minibar items list and charges available?
Yes No	Do you have a direct line to access the HMS 400 System?
Yes No	Is one analog direct line connected to the modem?
Yes No	Is the guest rooms and extensions list available?
Yes No	Is the admin extensions list, a list of who should have a mailbox, and the required CoS available?
❒	Obtain Room and Maid Status Codes from the Hotel PMS.
❒	Obtain Language Codes from the Hotel PMS.
❒	Obtain the Hotel PMS Serial Link Transmission Rate and Communication Protocols (for example, 9600,N,8,1) or IP Address and Port Number.
❒	Obtain the CS 1000 PMS Serial Link Transmission Rate and Communication Protocols (for example, 9600,N,8,1) or CS 1000 ELAN IP Address, PTY Number, and (LAPW) User Password.
❒	Obtain the most recent CS 1000 PMSI patches.

Site preparation checklist

Complete the following site preparation checklist before you install the HMS 400 hardware to ensure all installation requirements are met.

Table 3: Site preparation checklist

Check	Description
❒	Complete site inspection checklist. See Site inspection checklist on page 13.

Check	Description
❒	Complete preinstallation checklist. See Preinstallation checklist on page 14.
❒	Ensure a sufficient number of power outlets with an AC rating of 110 V or 220 V are available.
❒	Ensure a UPS of at least 400 VA with Power Management software is available.
❒	Ensure two LAN points or a connection to a network switch is available.
❒	Ensure a 56 Kb USB Modem for remote technical support is available. Avaya recommends the NTUB30HA modem. North American customers can order the NTUB30HA modem from Avaya. Customers outside of North America must supply their own USB modem.
❒	If Serial connectivity is preferred, ensure that you have a Perle 4-port PCIe Serial card.
❒	Ensure a 9-pin female terminated RS-232 cable connected between the PMS Interface PC and HMS 400 PC (PMSI) is available. If the cable length is greater than 50 feet, you require a line modem/booster. Alternatively, you can choose PMSI over IP.
❒	Ensure a 9-pin female terminated RS-232 cable connected between the CS 1000 PMS serial port and the HMS 400 computer is available. For the proper cabling, see Network cabling installation on page 17. Alternatively, you can choose PMSI over IP.

Chapter 4: Network cabling installation

This chapter provides information about installing network cables for an Avaya Hospitality Messaging Server 400 system. Individual sites can have unique cable requirements. The interface between the Avaya HMS 400, Avaya Communication Server 1000 (Avaya CS 1000), and Property Management System (PMS) uses customer-supplied equipment.

Important:
The customer must supply all cables.

Navigation:

- HMS 400 PMSI serial connections on page 17
- HMS 400 to Property Management System connection specifications on page 18
- HMS 400 to CS 1000E MGC interface on page 19
- HMS 400 PMSI IP connections on page 22

HMS 400 PMSI serial connections

You can use a serial connection to connect the HMS 400 Property Management System Interface (PMSI) to the Property Management System (PMS) and the CS 1000 system.

Serial connections to the CS 1000 are is only supported for CS 1000 Release 6.0 and earlier and only to a CS 1000E Media Gateway Controller (MGC). Connection to a CS 1000M paddle board is not supported. HMS 400 does not support serial connections to CS 1000 Release 7.0 and later. If the IBM x3350 server requires a serial connection to the CS 1000, you must install the four-port serial interface card, as the IBM x3350 server has only one serial port.

Note:
The HP Proliant DL360 G7 does not support the four-port serial interface card.

Prerequisites:

Install the four-port serial interface card. See Installing a multiport serial adapter on page 55.

The HP Proliant DL360 G7 server does not support the installation of the four-port serial interface card. The serial interface card can only be installed on the HMS 400 IBM x3350 server.

The following serial interfaces are available.

- HMS 400 to PMS
- HMS 400 to CS 1000 Release 6.0 and lower

The following diagram shows the two serial connections for an HMS 400 system. Customer-supplied line drivers are required for distances over 50 feet.

Important:

You must follow specifications (such as protocol requirements, pin outs, and distance limitations) for the CS 1000 and PMS for proper integration.

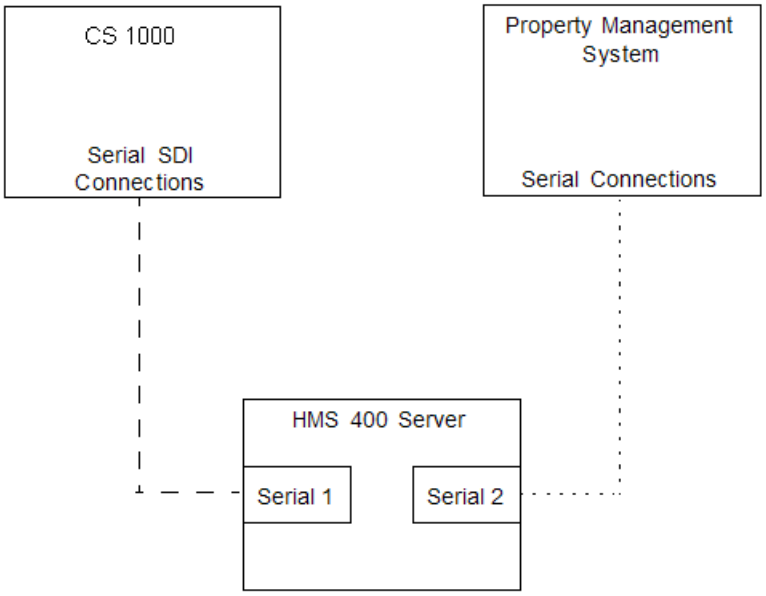


Figure 1: HMS 400 PMSI serial connections

HMS 400 to Property Management System connection specifications

This section provides information about HMS 400 and PMS connection specifications.

Prerequisites:

- PMSI cabling must follow the CS 1000 specifications for shielding, distance limitations, and grounding requirements.
- RS-232 cables are required to connect the HMS 400 main server to the CS 1000 or PMS. RS-232 cables are not required to connect HMS 400 client servers to the CS 1000 or PMS.

To connect the HMS 400 (DTE) and PMS (DTE), a customer-supplied 9-pin female end to end crossover cable (also called a null modem) is required. Ensure that the DB9 Female to Female null modem cable you purchase is foil shielded for protection from EMI/RFI interference caused by surrounding office equipment and fluorescent lights. The following table shows the pin connections for HMS 400 and PMS.

Table 4: HMS and PMS connections

HMS 400 9-pin (female)	PMS 9-pin (female)
2	3
3	2
5	5

HMS 400 to CS 1000E MGC interface

You can connect the HMS 400 to the CS 1000E Media Gatewway Controller (MGC) interface.

Navigation:

- MGC interface connections on page 19
- RS-232 signals on page 21

MGC interface connections

The following configurations to connect the HMS 400 system to the CS 1000E Media Gateway Controller (MGC) interface are available:

- crossover configuration
- straight-through configuration

You must supply the cables. You can use one of the following configurations:

- Use a common, straight DB9 Female to DB25 Male modem cable connected to a DB25 F/M Null modem that connects to a Female gender changer and to the PBX DB25 CS 1000 octopus cable.
- Use a DB25 Female to Female null modem cable with a DB9 Female to DB25 Male gender changing adapter.

Navigation:

- Crossover configuration on page 20
- Straight-through configuration on page 20

Crossover configuration

You can connect the HMS 400 to the CS 1000E MGC interface using a crossover configuration.

The following table show the pin connections using the crossover configuration.

Table 5: Crossover configuration connections

HMS 400 9-pin (female)	CS 1000E MGC 25-pin (female)
1	22
2	2
3	3
4	6
5	7
6	20
7	5
8	4
9	8

Straight-through configuration

You can connect the HMS 400 to the CS 1000E MGC interface using a straight-through configuration.

The following table show the pin connections using the straight-through configuration.

Table 6: Straight-through configuration connections

HMS 400 9-pin (female)	CS 1000 MGC 25-pin (female)
1	8
2	3
3	2
4	20
5	7
6	6
7	4
8	5
9	22

RS-232 signals

The following table outlines the standard RS-232 signals.

Table 7: RS-232 signals

Wiring signals	Abbreviation	DB25	DB9
CHASIS GROUND	GND	1	5
TRANSMIT DATA	TXD	2	3
RECEIVE DATA	RXD	3	2
REQUEST TO SEND	RTS	4	7
CLEAR TO SEND	CTS	5	8
DATA SET READY	DSR	6	6
SIGNAL GROUND	SG	7	5
DATA CARRIER DETECT	DCD	8	1
DATA TERMINAL READY	DTR	20	4
RING INDICATOR	RI	22	9

HMS 400 PMSI IP connections

You can connect the HMS 400 PMSI connections to the Hotel PMS and the PMS port on the CS 1000 using IP. Compared to RS-232, TCP/IP offers enhanced communication. TCP/IP does not require line boosters over long distances to provide higher transaction speeds and lower loss of data packets.

Important:

Not all hotel PMS support TCP/IP connectivity. If TCP/IP is not supported, you can connect the HMS 400 to the PMS using RS-232 cables and connect the HMS 400 to the CS 1000 using IP.

You can use either a CAT5 or CAT6 cable for interconnectivity. Because the HMS 400 server has only two LAN ports, to support IP connectivity (one for SIP and two for PMSI) all interfaces (CS 1000, HMS 400, and Hotel PMS) must be on the same domain and must connect to a dedicated network switch. The following diagram shows the connections between the CS 1000, HMS 400 and Hotel PMS.

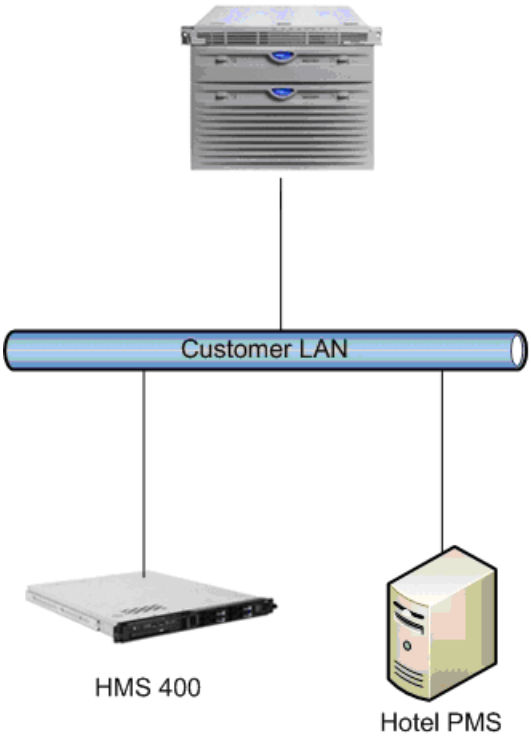


Figure 2: HMS 400 PMSI IP connections

For information about configuring the CS 1000 for PMSI over TCP/IP, see CS 1000 configuration (Release 7.0) on page 25. For information about configuring the HMS 400, see Avaya Hospitality Messaging Server 400 server commissioning on page 67.

Chapter 5: CS 1000 configuration (Release 7.0)

This chapter provides information about configuring Avaya Communication Server 1000 (CS 1000) Release 7.0 to connect to the Avaya Hospitality Messaging Server 400 (HMS 400 Release 2.0.

The HMS 400 connects to Session Initiation Protocol (SIP) virtual trunks on the CS 1000. The CS 1000 handles incoming and outgoing call processing tasks and the HMS 400 handles RTP sessions and DTMF transmission and processing. Up to 120 simultaneous SIP sessions can be established between the HMS 400 and CS 1000.

Prerequisites:

- For more information about CS 1000 topics such as the CS 1000 Element Manager and connecting to the Call Server, see the CS 1000 documentation for Release 6.0 or Release 7.0.
- The only supported codec is G.711.
- The maximum number of channels for each server is 120.
- Avaya does not support Network Routing Server (NRS) as a SIP gateway for HMS 400.

  Important:

  An additional Signaling Server node is required for SIP interoperability between CS 1000 and other end points.
- You must configure virtual D-channel, SIP routes, and up to 120 virtual SIP trunks for CS 1000.

CS 1000 configuration procedures

The following task flow shows you the sequence of procedures you perform to configure a CS 1000.

CS 1000 configuration navigation

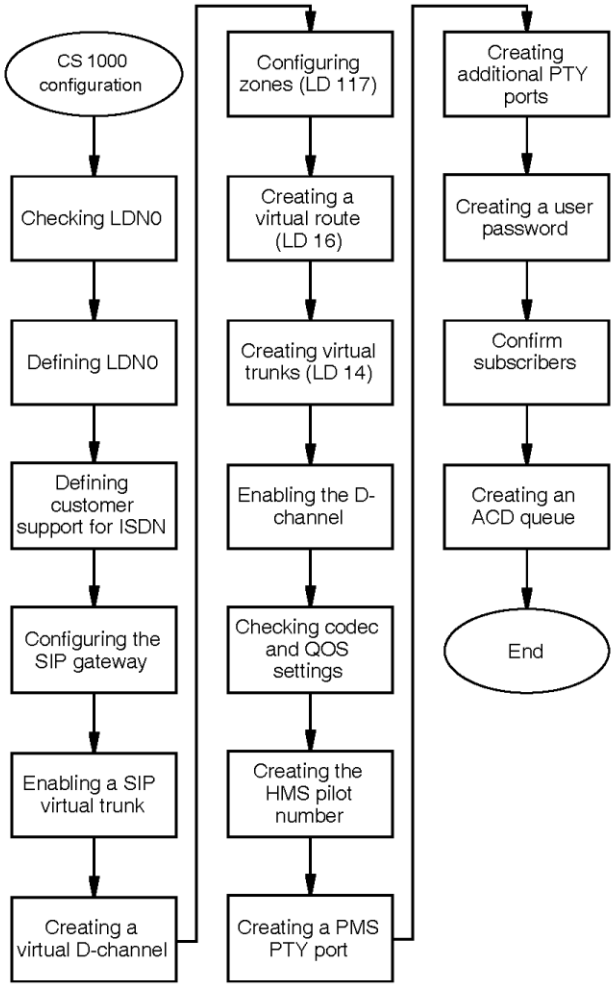


Figure 3: CS 1000 configuration procedures

CS 1000 configuration navigation:

- Checking LDN0 on page 27
- Defining LDN0 on page 27
- Defining customer support for ISDN on page 28
- Configuring the SIP gateway on page 28
- Enabling a SIP virtual trunk on page 30
- Creating a virtual D-Channel on page 31

- Configuring zones (LD 117) on page 31
- Creating a virtual route (LD 16) on page 33
- Creating virtual trunks (LD 14) on page 34
- Enabling the D-Channel on page 35
- Checking codec and QoS settings on page 35
- Disabling the G.729 codec on Media Gateways on page 36
- Creating the HMS 400 pilot number on page 37
- Creating a PMS PTY port on page 37
- Creating additional PTY ports on page 38
- Creating a PMS PTY user name and password on page 40
- Configuring PMSI login with UCM on Security Domain on page 41
- Confirming subscribers on page 42
- Creating an ACD queue on page 43

Checking LDN0

Determine if LDN0 is defined or not defined on the Call Server. LDN0 is used as an attendant DN.

1. At a command prompt on the Call Server, type `LD 21` and press **Enter**.
2. At the **REQ** prompt, type `PRT` and press **Enter**.
3. At the **TYPE** prompt, type `ldn_data` and press **Enter**.
4. At the **CUST** prompt, type the customer number and press **Enter**.
5. Check that LDN0 is defined.

Defining LDN0

Define LDN0 on the Call Server.

1. At a command prompt on the Call Server, type `LD 15` and press **Enter**.
2. At the **REQ** prompt, type `CHG` and press **Enter**.
3. At the **TYPE** prompt, type `ldn_data` and press **Enter**.
4. At the **CUST** prompt, type the customer number and press **Enter**.
5. At the **LDN0** prompt, type the published directory number and press **Enter**.

Defining customer support for ISDN

Define customer support for ISDN.

Prerequisites:

Log on to the CS 1000 Element Manager.

1. In the Element Manager navigation pane, click **Customers**.
2. Click the customer number used for HMS 400 integration.
3. Click **Feature Packages**.
4. In the list of available features, expand **Integrated Services Digital Network - Package 145**.
5. In the **Integrated Services Digital Network - Package 145** section, select the **Integrated Services Digital Network** check box.
6. In the **Private Network Identifier** box, type a value for a private network identifier.
7. Click **Save**.

Configuring the SIP gateway

Configure the SIP gateway in the CS 1000 Element Manager (Release 6. and Release 7.0). This procedures applies only to SIP-enabled HMS 400 servers (post-Release 1.0).

Prerequisites:

- To confirm which route is configured as SIP, print (PRT) your route data block (RDB) in LD 21.
- Log on to the CS 1000 Element Manager.

---

1. In the **Element Manager** navigation pane, select **System > IP Network > Nodes: Servers, Media Cards**.

   The **IP Telephony Node** page appears.
2. On the **IP Telephony Node** page, click the **Node ID** of the node you want to configure.

   The **Node Details** page for the selected node appears
3. Click on the **Gateway (SIPGw)** link.

   The **Virtual Trunk Gateway Configuration Details** page appears.
4. At the top of the page, select the **Enable Gateway service on this node** check box.
5. In the **General** pane, in the **Vtrk Gateway Application:** drop-down list, select **SIP Gateway (SIPGw)**.
6. In the **SIP Domain Name** field, enter the customer domain or **HMS400v2**.
7. In the **Local SIP Port** field, type **5060**.
8. In the **Gateway endpoint name:** field, enter **HMS400v2**.
9. Under **SIP Gateway Settings**, from the drop-down list, select **Security Disabled in TLS Security**.
10. In the **Primary TLAN IP Address** field, type the HMS 400 TLAN IP address.
11. In the **Port** box, type `5060`.
12. From the **Transport protocol** drop-down list, select a transport protocol.
13. In the **Options** section, ensure the **Supports Registration** check box is cleared.
14. Scroll down to the **SIP URI Map:** section.
15. In the **Private Domain Names** section, in the **UDP:** field, type the L1 domain.
16. In the **CDP:** field, type the L0 and L1 domains in the format: `<L0 domain.L1domain>`.
17. Click **Save**.
18. Click **Save** again.
19. Click **Transfer Now**.
20. Select the HMS 400 Node Signaling Server and click **Start Sync**.

21. Click **OK** to accept the confirmation prompt.
22. When the transfer is complete, click **OK**.

Enabling a SIP virtual trunk

Enable a SIP virtual trunk in the CS 1000 Element Manager.

Prerequisites:

- Log on to the CS 1000 Element Manager.
- The SIP domain name must not exceed 128 characters. Valid characters are the letters a to z, numbers 0 to 9, period (.), hyphen (-), comma (,), and underscore (_).

1. In the **Element Manager** navigation pane, select **System > IP Network > Nodes: Servers, Media Cards**.
2. On the **Node Configuration** page, click **Edit** beside the node to configure.
3. Expand **Signaling Servers**.
4. Under **Signaling Servers**, expand **Signaling Server Properties**.
5. In the **Signaling Server Properties** section, in the **Enable Line TPS** list, select **SIP only**.
6. Ensure that **Local SIP TCP/UDP Port to Listen to** is **5060**.
7. In the **SIP Domain** name box, type the SIP domain name.

   The SIP domain name builds all SIP messages and appears in the URI phone context.
8. Click **Save and Transfer**.
9. If you receive a prompt to restart the SIP sever, click **OK**.
10. After the transfer is complete, click **OK**.
11. In the Element Manager navigation pane, select **System > IP Network > Maintenance and Reports**.
12. In the **Node Maintenance and Reports** pane, expand **Node ID**.
13. Under **Node ID**, click **Reset**.
14. If a confirmation message appears, click **OK**.

Creating a virtual D-Channel

Create a virtual D-Channel in the CS 1000 Element Manager.

Important:
D-Channels 0, 1, and 2 are usually used or shared with other applications. Avaya recommends that you begin configuring virtual D-channels on Channel 3 or greater.

Prerequisites:

Log on to the CS 1000 Element Manager.

1. In the Element Manager navigation pane, select **Routes and Trunks > D-Channels**.
2. If a D-channel is not configured, a message appears; click **OK**.
3. In the **D-Channels** page, in the **Choose a D-Channel Number** drop-down list, select the desired D-Channel number.
4. In the type list, select **DCH**.
5. Click **to Add**.
   The **D-Channels Property Configuration** page appears.
6. In the **D channel Card Type (CTYP)** list, select **DCIP** (D-Channel is over IP).
7. In the **Designator (DES)** field, type a meaningful name for the D-channel.
   The Designator (DES) name cannot contain spaces. Use underscores (_) instead of spaces.
8. In the **User (USR)** list, select **Integrated Services Signaling Link Dedicated (ISLD)**.
9. In the **Interface type for D-channel (IFC)** list, select **Meridian 1 (SL1)**.
10. Click **Submit** to create the new D-channel.

Configuring zones (LD 117)

Perform this procedure to configure the zones required for virtual routes and trunks.

You must configure the following zones before you configure virtual routes and trunks:

- Zone 1 – Zone for IP Deskphones (ZBRN=MO)
- Zone 2 – Zone for voice gateway channels (ZBRN=VTRK)

Important:
Do not configure Zone 0.

Prerequisites:

- Log on to the CS 1000 Element Manager.
- Ensure that the bandwidth allocated for zones with heavy traffic is available.

1. In the Element Manager navigation pane, select **System > IP Network > Zones**.
   The **Zones** page appears.
2. Click **Bandwidth Zones**
   The **Bandwidth Zones** page appears.
3. On the **Bandwidth Zones** page, if only Zone 0 exists in the **Please Choose the** drop-down list:
   a. Select **Zone 1** in the drop-down list and click **to Add**.
   b. Select **Zone 2** in the drop-down list and click **to Add**.
4. Expand **Bandwidth Zones 1** and select **Zone Basic Property and Bandwidth Management**.
   The **Zone Basic Property and Bandwidth Management** page appears.
5. If you are prompted to use the Zone Basic Property and Bandwidth Management Spreadsheet, click **OK**.
6. On the **Zone Basic Property and Bandwidth Management** page, in the **Zone Intent (ZBRN)** list, select **MO (MO)**.
7. In the **Description (ZDES)** box, type a meaningful name for Zone 1.
8. Click **Submit**.
9. On the **Bandwidth Zones** page, expand **Zone 2** and select **Zone Basic Property and Bandwidth Management**.
10. If you are prompted to use the Zone Basic Property and Bandwidth Management Spreadsheet, click **OK**.
11. On the **Zone Basic Property and Bandwidth Management** page, in the **Zone Intent (ZBRN)** drop-down list, select **VTRK (VTRK)**.
12. In the **Description (ZDES)** box, type a meaningful name for Zone 2.
13. Click **Submit**.

Creating a virtual route (LD 16)

Create a virtual route for LD 16 in the CS 1000 Element Manager.

Prerequisites:

Log on to the CS 1000 Element Manager.

1. In the Element Manager navigation pane, select **Routes and Trunks > Routes and Trunks**.

   The **Routes and Trunks** page appears.
2. On the **Routes and Trunks** page, click **Add route**.
3. On the **New Route Configuration** page, in the **Basic Configuration** section, from the **Route Number (ROUT)** drop-down list, select the route number.
4. In the **Designator field for Trunk (DES)** box, type a meaningful name for the route.
5. In the **Trunk Type (TKTP)** list, select **TIE Trunk data block (TIE)**.
6. In the **Incoming and Outgoing Trunk (ICOG)** list, select **Incoming and Outgoing (IAO)**.
7. In the **Access Code for the trunk route (ACOD)** box, type a value for the trunk route access code.
8. Select the **The route is for a virtual trunk route (VTRK)** check box.
9. In the **Zone for codec selection and bandwidth management (ZONE)** box, type the number of the zone that is configured as ZBRN=VTRK.
10. In the **Node ID of signaling server of this route (NODE)** box, type the node ID of the Signaling Server.

    If you are unsure of the node ID, choose **System > IP Network > Node: Servers Media Cards** in the Element Manager navigation pane to find the node ID.
11. In the **Protocol ID for the route (PCID)** list, select **SIP (SIP)**.
12. Select the **Integrated Services Digital Network option (ISDN)** check box.
13. In the **Mode of operation (MODE)** list, select **Route uses ISDN Signaling Link (ISLD)**.
14. In the **D Channel number (DCH)** list, select the D-channel number that you previously configured.
15. In the **Interface type for route (IFC)** list, select **Meridian M1 (SL1)**.

16. In the **Private Network Identifier (PNI)** box, type a value for the private network identifier.
17. In the **Call Type for outgoing direct dialed TIE route (CTYP)**, ensure **Unknown Call type (UKWN)** is selected.
18. Select the **Insert ESN Access Code (INAC)** check box.
19. Click **Save**.

    The route you created appears on the **Route and Trunks** page.

Creating virtual trunks (LD 14)

Create a virtual trunk for LD 14 in the CS 1000 Element Manager.

Prerequisites:

Log on to the CS 1000 Element Manager.

1. In the Element Manager navigation pane, select **Routes and Trunks > Routes and Trunks**.

   The **Routes and Trunks** page appears.
2. Expand the desired Customer Number.
3. Under the Customer number, click **Add trunk** beside the route to which you want to add the trunk.

   The **New Trunk Configuration** page appears.
4. On the **New Trunk Configuration** page, select **Multiple trunk input number (MTINPUT)** if you configure multiple trunks.

   The maximum number of trunks is 32.
5. In the **Trunk data block (TYPE)** list, select **IP Trunk (IPTI)**.
6. In the **Terminal Number (TN)** box, type the trunk terminal number.
7. In the **Designator field for trunk (DES)** box, type a meaningful name for the trunk.
8. Ensure **Extended Trunk (XTRK)** is **Virtual trunk (VTRK)**.
9. In the **Route number, Member number (RTMB)** box, type the route number and member number separated by a space.
10. In the **Start arrangement Incoming (STRI)** list, select **Immediate (IMM)**.
11. In the **Start arrangement Outgoing (STRO)** list, select **Immediate (IMM)**.

12. In the **Channel ID for this trunk (CHID)** box, type the channel ID for the trunk.
13. To optionally configure a class of service, click **Edit** beside **Class of Service (CLS)**.
14. Select **Advanced Trunk Configurations** to optionally configure advanced options. The default values are acceptable.
15. Click **Save**.

Enabling the D-Channel

After you configure routes and trunks, you must enable the D-Channel.

Prerequisites:

Log in to the CS 1000 Element Manager.

1. In **Element Manager Navigation** pane, select **Routes and Trunks > D-Channels**.
   The **D-Channels** page appears.
2. In the **Maintenance** section, click the **D-channel Diagnostics (LD 96)** link.
3. From the **Enable Auto Recovery** list, select **Enable D-Channel (ENL DCH)**.
4. Select the D-Channel option to use for the HMS 400.
5. Click **Submit**.

Checking codec and QoS settings

Confirm codec and QoS settings in CS 1000 Element Manager.

Prerequisites:

Log on to the CS 1000 Element Manager.

1. In the Element Manager navigation pane, select **System > IP Network > Nodes: Servers, Media Cards**.
   The **IP Telephony Nodes** page appears.
2. Click the desired Node ID.

The **Node Details** page appears

3. On the right, click the **Voice Gateway (VGW) and Codecs** link.
   The **Voice Gateway (VGW) and Codecs** page appears.
4. In the **Voice Codecs** section, make sure the **G729A Enabled** check box is not selected. If the check box is selected, remove the check.
5. Click **Save**.
   The **Node Details** page appears again.
6. Click **Save**.
   The **Node Saved** window appears.
7. Click **Transfer Now**.
   The **Synchronize Configuration Files** window appears.
8. Select the HMS 400 Node Signaling Server and click **Start Sync**.
   The **Synchronization Status** column displays **Synchronized** when the synchronization finishes.

Disabling the G.729 codec on Media Gateways

Currently, HMS 400 does not support the G.729 codec. To disable the G.729 codec, follow this procedure.

1. Log on to the CS 1000 Element Manager .
2. . In the Element Manager navigation pane on the left, select **System > IP Network > Media Gateways**.
   The **Media Gateways** page appears.
3. Click on the link of the desired IPMG.
   The **IPMG Property Configuration** page appears.
4. At the bottom of the page, click **Next**.
5. Scroll down to the **VGW and IP phone codec profile** section and expand the section.
6. If the **Codec G729A** check box is checked, uncheck it.
7. Click **Save** and then click **OK**.
   The **Media Gateways** page appears again.
8. Click the radio button for the IPMG and then, at the top of the page, click **Reboot**.

Creating the HMS 400 pilot number

The HMS 400 pilot number is the primary number where all subscriber calls are forwarded to in busy or no answer situations. This number is also the Night Call Forward (NCFW) destination for all Automatic Call Distribution (ACD) queues created that access HMS 400 services.

Prerequisites:

Create a Route List Index (RLI). For more information, see *Avaya Communication Server 1000 Software Input Output Reference — Administration, NN43001-611*.

1. At a command line, type `LD 87` and press **Enter**.
2. At the **REQ** prompt, type `NEW` and press **Enter**.
3. At the **FEAT** prompt, type `CDP` and press **Enter**.
4. At the **TYPE** prompt, type `DSC` and press **Enter**.
5. At the **DSC** prompt, type `DN` for the pilot number and press **Enter**.
6. At the **FLEN** prompt, type the length of the DN and press **Enter**.
7. At the **DSP** prompt, press **Enter**.
8. At the **RLI** prompt, type the value for the Route List Block and press **Enter**.

Creating a PMS PTY port

Create a PMS PTY port to enable HMS 400 communication with the switch to perform functions such as check in, check out, and Class of Service (CoS) or Class of Restriction (COR) change.

Prerequisites:

- The PMS PTY port must be the lowest-numbered PTY port.
- Avaya recommends that you create at least two additional PTY ports that have higher port numbers than the PMS PTY port. For information about creating additional PTY ports, see Creating additional PTY ports on page 38.

1. At a command line, type `LD 17` and press **Enter**.
2. At the **REQ** prompt, type `CHG` and press **Enter**.

3. At the **TYPE** prompt, type `CFN` and press **Enter**.
4. At the **ADAN** prompt, type `NEW TTY X` (where *X* is the port number) and press **Enter**.
5. At the **CTYP** prompt, type `PTY` and press **Enter**.
6. At the **PORT** prompt, type the port number and press **Enter**.
   The port number range is usually 0 to 7 but it can match *X*.
7. At the **DNUM Y** prompt, press **Enter**.
8. At the **DES** prompt, type a description (for example, PMSI) and press **Enter**.
9. At the **FLOW** prompt, type `NO` and press **Enter**.
10. At the **USER** prompt, type `BGD PMS` and press **Enter**.
11. At the **TTYLOG** prompt, type `NO` and press **Enter**.
12. At the **BANR** prompt, press **Enter**.

Creating additional PTY ports

Create at least two additional PTY ports that have port numbers greater than the PMS PTY port.

1. At the command prompt type `LD 17` and press **Enter**.
2. At the **REQ** prompt, type `CHG` and press **Enter**.
3. At the **ADAN** prompt, type `NEW TTY X` (*X* is a number greater than the first port) and press **Enter**.
4. At the **CTYP** prompt, type `PTY` and press **Enter**.
5. At the **PORT** prompt, type the port number and press **Enter**.
   The port number range is usually 0 to 7 but it can match *X*.
6. At the **DNUM Y** prompt, press **Enter**.
7. At the **DES** prompt, type a description (for example, ptyY) and press **Enter**.
8. At the **FLOW** prompt, type `NO` and press **Enter**.
9. At the **USER** prompt, type `MTC SCH BUG` and press **Enter**.

10. At the **TTYLOG** prompt, type `NO` and press **Enter**.
11. At the **BANR** prompt, press **Enter**.

Creating a PMS TTY Port for serial connection

Create a TTY port if the user chooses serial connectivity rather than IP (rlogin) for their PMSI interface.

Important:

HMS 400 Release 2.0 supports serial connection only to CS 1000E. Serial connection to CS 1000M is not supported.

The HMS 400 IBM X3350 server only supports TTY connections to CS 1000 Release 6.0 and earlier. CS 1000 Release 7.0 and later only supports an IP interface connection to the HMS 400.

The HMS 400 HP Proliant DL360 G7 server does not support serial connection to the CS 1000. The ELAN IP interface is the only option for HP Proliant DL360 G7 PMSI connectivity to the CS 1000.

Prerequisites:

- Check the status of the TTY port 1 using LD 37. If it is enabled, disable it.
- Ensure PCML and PMSI settings are configured accordingly in LD 17.

1. At a command prompt, type `LD 17` and press **Enter**.
2. At the **REQ** prompt, type `CHG` and press **Enter**.
3. At the **TYPE** prompt, type `CFN` and press **Enter**.
4. At the **ADAN** prompt, type `OUT TTY 1` and press **Enter**.
5. At the next **ADAN** prompt, type `NEW TTY 1` and press **Enter**.
6. At the **CTYP** prompt, type `MGC` and press **Enter**.
7. At the **IPMG** prompt, type the appropriate cabinet number, such as "4 0", and press **Enter**.
8. At the **DNUM** prompt, type `1` and press **Enter**.
9. At the **PORT** prompt, type `1` and press **Enter**.
10. At the **DES** prompt, type a description, such as "PMS", and press **Enter**.
11. At the **BPS** prompt, type `2400` (or higher if needed) and press **Enter**.
12. At the **BITL** prompt, type `7` and press **Enter**.

13. At the **STOP** prompt, type `1` and press **Enter**.
14. At the **PARY** prompt, type `NONE` and press **Enter**.
15. At the **FLOW** prompt, press **Enter**.
16. At the **USER** prompt, type `BGD PMS` and press **Enter**.
17. Press **Enter** until the **ADAN DATA CHGED** message appears.
18. At the **ADAN** prompt, type `**` and press **Enter**.
19. At the **REQ** prompt, type `CHG` and press **Enter**.
20. At the **TYPE** prompt, type `PARM` and press **Enter**.
21. Press **Enter** until the system displays the **PCML** prompt.
22. Type `MU` or `A` , depending on the region you are in, and press **Enter**.

    If you are in the NA/CALA region, type `MU`. If you are in the EMEA/APAC region, type `A`.
23. Press **Enter** until the system displays the **PMSI** prompt.
24. Type `YES` and press **Enter**.
25. At the **MANU** prompt, type `PMS1` and press **Enter**.
26. At the **PMCR** prompt, press **Enter**.
27. At the **PORT** prompt, type `1` and press **Enter**.

    This corresponds to the TTY port number created earlier.
28. Press **Enter** until the system displays the **REQ** prompt.
29. Type `****` and press **Enter** to exit.

Creating a PMS PTY user name and password

Create a user name and password for the PTY port. A password is required for the PTY port because the IP connection requires a constant connection.

Prerequisites:

- You must log on to the CS 1000 Element Manager at Admin level 2 or higher to create the PMS PTY user name and password.
- Ensure that you know the PMS PTY port number that you created in Creating a PMS PTY port on page 37. The port number is part of the PMS PTY user name.

1. At a command prompt, type `LD 17` and press **Enter**.
2. At the **REQ** prompt, type `NEW` and press **Enter**.
3. At the **TYPE** prompt, type `PWD` and press **Enter**.
4. At the **PSWD_COMP** prompt, press **Enter** six times until the **ACCOUNT_REQ** prompt appears.
5. At the **ACCOUNT_REQ** prompt, type `NEW` and press **Enter**.
6. At the **PWD_TYPE** prompt, type `LAPW` and press **Enter**.
7. At the **PWTP** prompt, press **Enter**.
8. At the **USER_NAME** prompt, type `PTY`*x* (where *x* is the port number used when you created the PMS PTY port) and press **Enter**.
9. At the **PASSWORD** prompt, type the password and press **Enter**.

   Note:
   The password is case-sensitive.
10. At the **CONFIRM** prompt, type the password again and press **Enter**.
11. At the **OVLA** prompt, press **Enter**.
12. At the **CUST** prompt, press **Enter** until the system indicates Account Settings saved.

Configuring PMSI login with UCM on Security Domain

Use this procedure to configure PMSI login with UCM on Security Domain.

1. Log in to UCM with the admin username and password.
2. Click **Administrative Users**.
3. Click **Add** to add a new user.
   The username should be same as PTY built for PMS.
4. Type the password.

   Important:
   This is a temporary password. Later you are prompted to change the password.

5. Click **Save** and continue.
6. Select **Roles** for new log in **CS1000 Admin2**, **Network Administration**, **PDT2**, and **Custom role HMS**.
7. Click **Save**.
8. Log out of UCM.
9. Log in using the newly-created user.

   The system prompts you to change the password. Change and save the password.
10. Log in to the HMS 400 as superadmin and open the **Web GUI** page.
11. Select the **PBX Setting** from the left menu.
12. Select the **IP Setting** bubble.
13. Type the Call Server **ELAN IP** address.
14. Type the user name created earlier in UCM.
15. Type the password for user created earlier and update.
16. Restart **HMS 400** service for the change to take effect.

    After the system restarts, use the connectivity test in the PMSI to verify that the PBX link has been successfully connected.

Confirming subscribers

Ensure that all subscriber telephones (analog (500/2500–type), digital, or IP) are programmed with the following parameters.

Important:

Class of service LPA is necessary for the Message Lamp to work on analog (500/2500–type) telephones. For telephones without MW LED, use AMW and LPD to activate stutter tone instead.

1. Ensure Administrative telephones have the following settings:
   - FDN 2000—Forward to HMS Pilot Number
   - CLS tld hta fna mwa cnia ccsa mra nama
   - HUNT 2000—Hunt to HMS Pilot Number
2. Ensure Guest telephones have the following settings:
   - CLS tld lpa hta fna mwa cnia ccsa mra nama

- HUNT 2000—Hunt to HMS Pilot Number
- FTR fdn 2000—Forward to Voicemail Pilot Number

Important:

HMS 400 does not support the default Message/Inbox Key 16 (MWK) Softkeys. Softkeys can be suppressed by applying Product Enhancement Patch MPLR 24565.

Creating an ACD queue

Use ACD queues to access voice mail services. You can create one ACD DN for each service. Create an ACD queue that forwards calls to the HMS 400 pilot number created in Creating the HMS 400 pilot number on page 37.

Prerequisites:

Print the list of HMS 400 Services (Entry Points).

1. At a command prompt, type `LD 23` and press **Enter**.
2. At the **REQ** prompt, type `NEW` and press **Enter**.
3. At the **TYPE** prompt, type `ACD` and press **Enter**.
4. At the **CUST** prompt, type `0` and press **Enter**.
5. At the **ACDN** prompt, type `7000` (or any number you want to assign) and press **Enter**.
6. Press **Enter** until the **MAXP** prompt appears.
7. At the **MAXP** prompt, type `1` and press **Enter**.
   This number creates one agent but forwards all callers to the NCFW number.
8. Press **Enter** until the **NCFW** prompt appears.
9. At the **NCFW** prompt, type the HMS 400 pilot number.
10. Press **Enter** until your changes are saved.

Chapter 6: Avaya Hospitality Messaging Server 400 hardware installation

This chapter describes how to install the Avaya HMS 400 hardware.

HMS 400 hardware installation procedures

The following task flow shows you the sequence of procedures you perform to install the HMS 400 hardware.

HMS 400 hardware installation procedures task flow

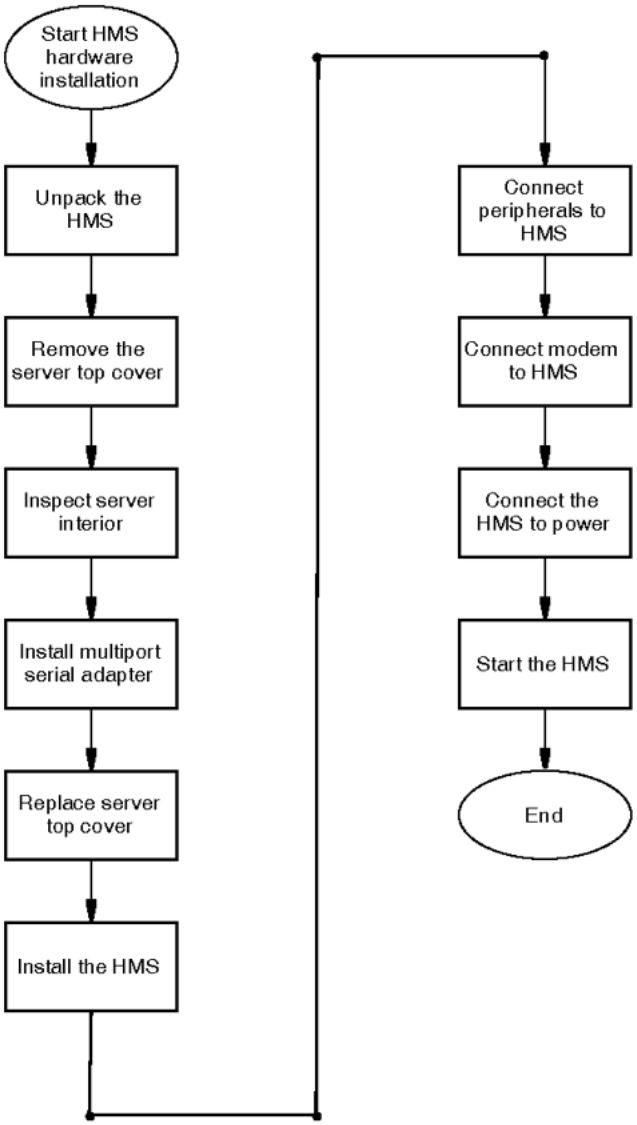


Figure 4: HMS 400 hardware installation procedures

HMS 400 hardware installation navigation:

- Unpacking the HMS 400 on page 47
- Removing the server top cover on page 48
- Inspecting the server interior on page 49
- Installing the dongle (HP DL360G7 server only) on page 51
- Installing a multiport serial adapter on page 55
- Replacing the server top cover on page 57
- Installing the HMS 400 on page 57
- Connecting peripherals to the HMS 400 on page 58
- Connecting the modem to the HMS 400 server on page 59
- Connecting the HMS 400 server to power on page 60
- Starting HMS 400 on page 60

Unpacking the HMS 400

Unpack the HMS 400 server and peripherals. After you unpack each item, check the item off on the packing list.

Warning:
The HMS 400 shipped from manufacturing weighs approximately 15 kilograms. Ensure you take proper precautions to avoid injury while unpacking the server.

1. Carefully open the cardboard carton that contains the server.
2. Remove the server from the carton and place it on the floor.
3. Carefully open the cartons that contain the keyboard and mouse and set the peripherals aside.
4. Place all manuals, CD-ROMs, operating system disk, any disks for peripherals, and the Windows emergency repair disk in a safe place.
5. Save all packing materials and cartons in case you must return any equipment.

Removing the server top cover

Remove the server top cover to work with the interior server components.

Warning:

Risk of personal injury

Handle sharp edges of the panel and chassis carefully to prevent injury.

Caution:

Risk of equipment damage

- Use an Electrostatic Discharge (ESD) wrist strap to protect static-sensitive components.
- Place the server on its side to prevent the server from accidentally falling over and to provide optimal stability. If you attempt to work with the server in the standing position, it may tip over when you work with the interior components.

1. Remove the protective power-supply cover from the back of the server by pulling the cover straight back from the power supplies.

   Store the power-supply cover in a safe place.

2. To install or remove a memory module, PCI adapter, battery, or other non hot-swap optional device, turn off the server and all attached devices and disconnect all external cables and power cords.
3. If the server is rack-mounted, press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.

   You can reach the cables on the back of the server when the server is in the locked position.

4. Loosen the thumbscrew at the back of the server.

   You cannot remove the thumbscrew.

5. Slide the two cover-release latches on the fan door on the right side of the top of the server back; then open the fan door cover.
6. Slide the server cover back until the locking tabs release.
7. Lift the server cover off the server and set the cover aside.

Job aid

The following graphics show the power supply cover, the location of the thumbscrew and the fan door.

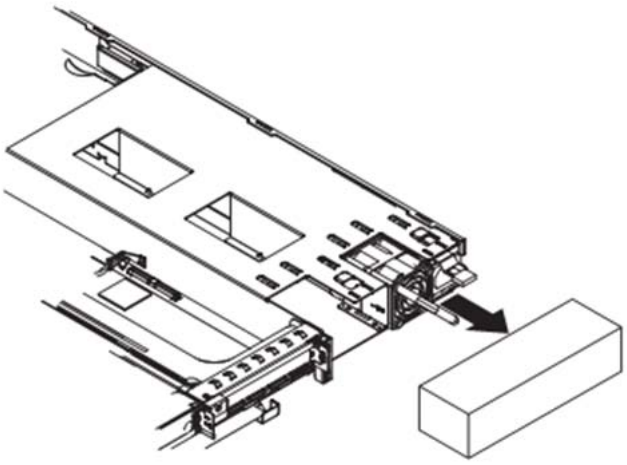


Figure 5: Removing HMS 400 power-supply cover

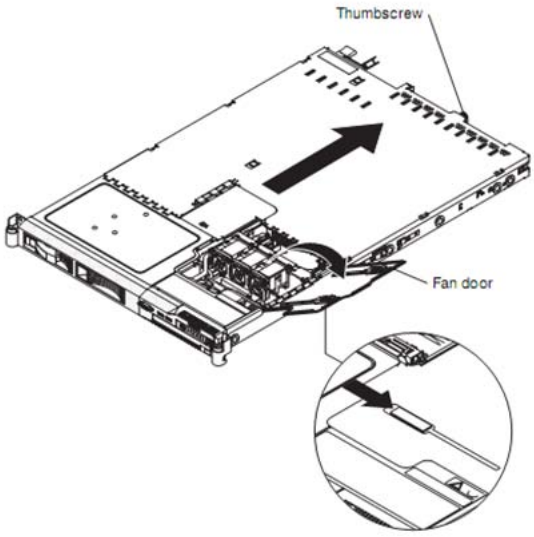


Figure 6: HMS 400 thumbscrew and fan door

Inspecting the server interior

Before you install the server, visually inspect it for loose components, foreign matter, or shipping damage inside the server.

Caution:

Risk of equipment damage

While you work with interior components, use an ESD wrist strap to protect static-sensitive components. The base package does not come with this strap.

Prerequisites:

For information about replacing the cover, see Replacing the server top cover on page 57.

1. Inside the server, check for loose wires or foreign objects (such as loose screws) inside the chassis.
2. Review the slot locations.
3. If you observe any damage, contact your Avaya technical support representative.
4. If components are loose, secure the components before you install the server.
5. If the server has no damage, replace the cover before you install the server.

Job aid

The following graphic show the interior components of the HMS 400.

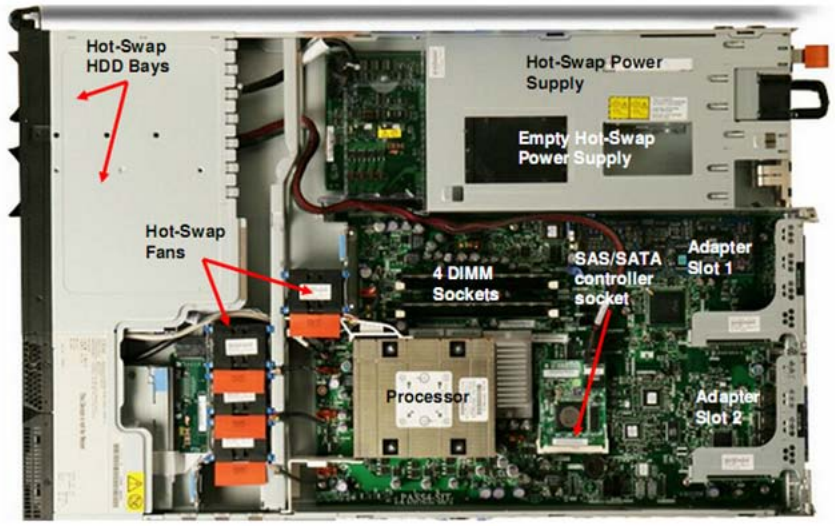


Figure 7: HMS 400 interior components

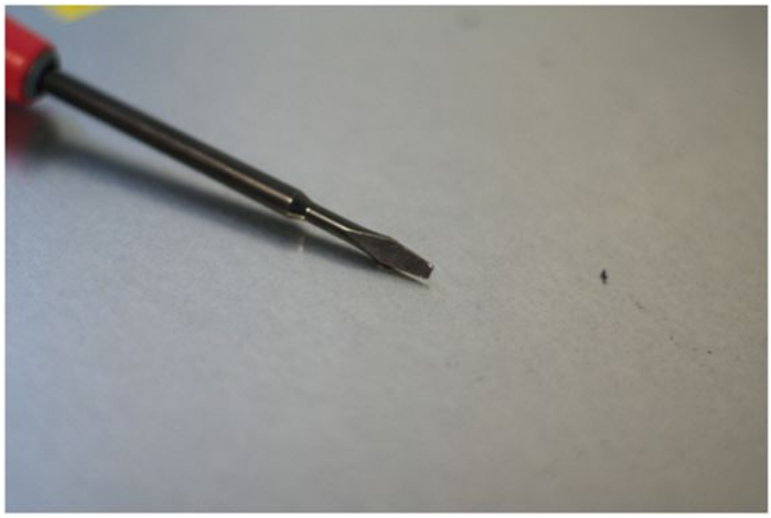
Installing the dongle (HP DL360G7 server only)

The dongle for the HP DL360G7 server must be installed into the internal USB port. Follow this procedure to install the dongle in the internal USB port..

Prerequisites:

Obtain a flat-edge screwdriver.

1. Obtain a flat-edge screwdriver.



2. Locate the lever on the top surface of the server.



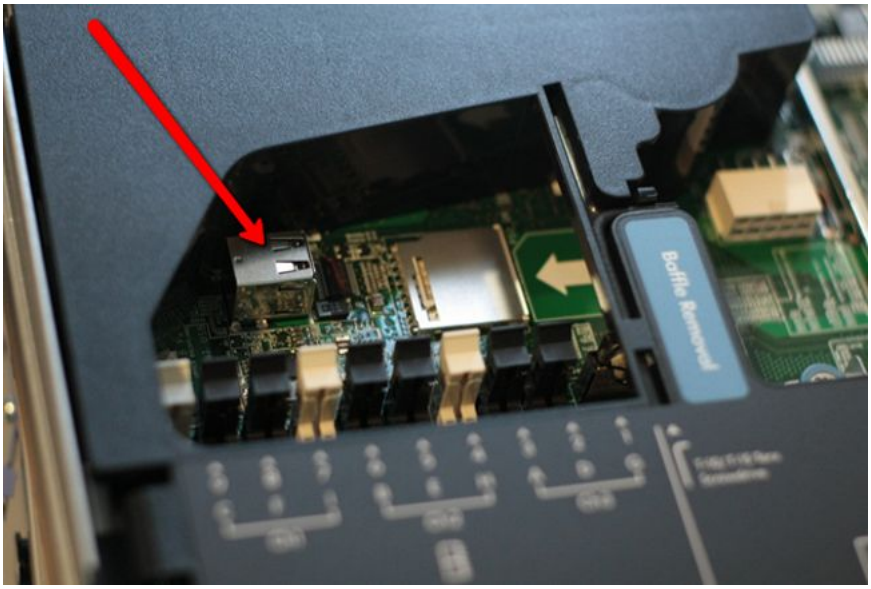
3. Turn the screw to the ‘unlock’ position.



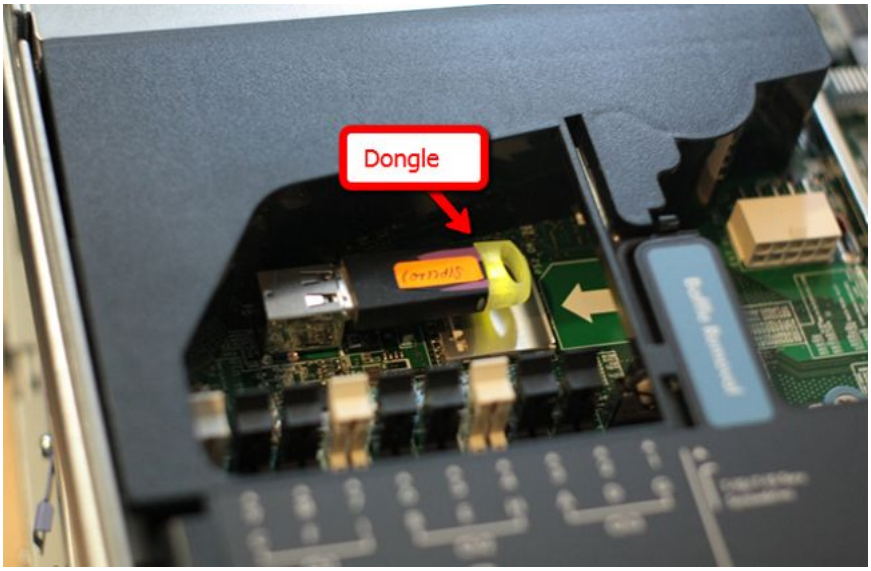
4. Gently pull the lever all the way upward to open the cover of the server.



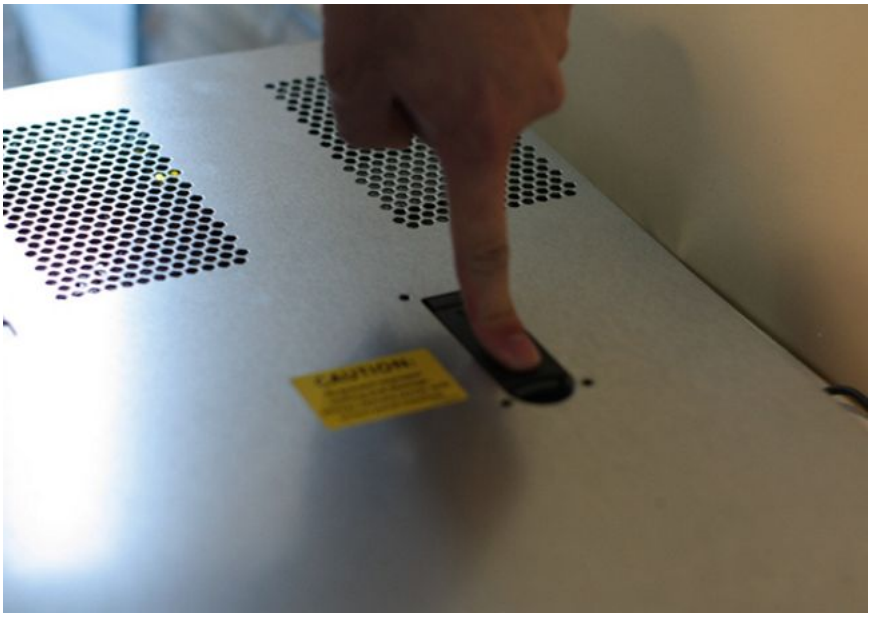
5. Lift up the cover to remove it and then locate the internal USB port.



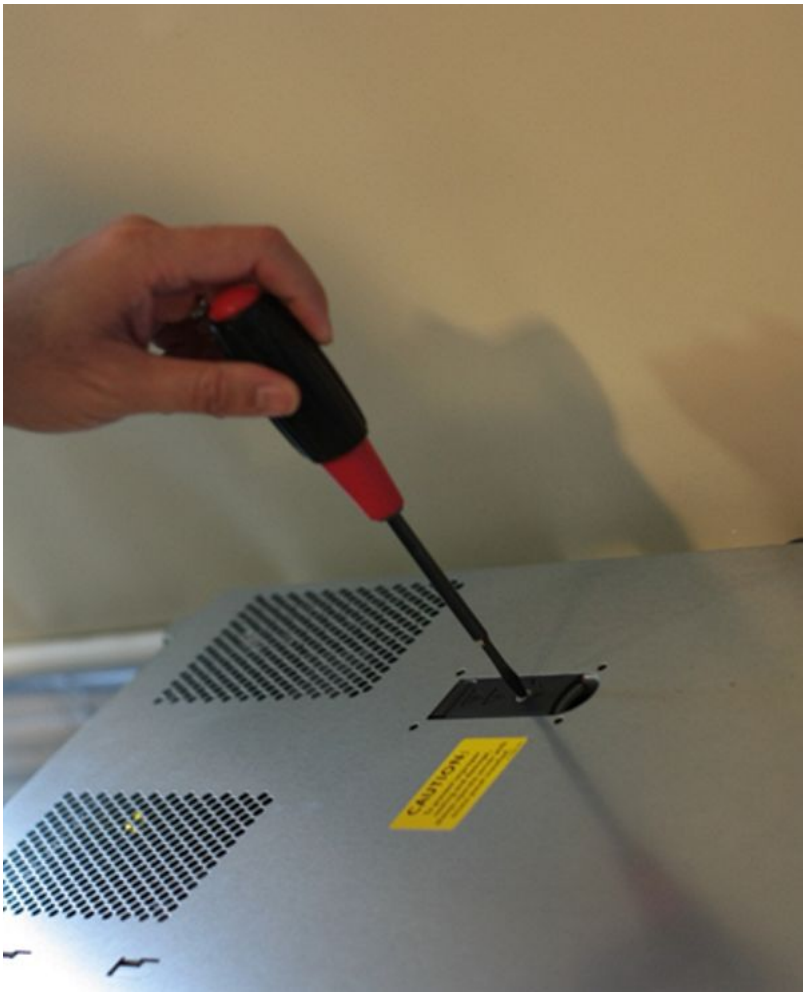
6. Carefully insert the USB dongle until the tip lights up.



7. Replace the cover and slide it back into position before pushing the lever all the way down.



8. Turn the screw back to its lock position.



Installing a multiport serial adapter

Important:

The HMS400 HP pProliant DL360 G7 server does not support the four-port serial interface card.

Important:

The HMS 400 IBM x3350 server only supports TTY connections to the CS 1000 Release 6.0 and earlier. CS 1000 Release 7.0 and later only supports an IP interface connection to the HMS 400.

The server provides two PCI Express slots on the riser-card assemblies and supports half-length, full-height, PCI Express x8 1.0a adapters in each expansion slot. You must remove the riser-card assemblies need to access the adapter slots.

1. Grasp the riser-card assembly at the rear edge and lift to remove it from the server.
2. Place the riser-card assembly on a flat, static-protected surface.
3. Remove the expansion-slot cover from the slot that you want to use.

   Important:
   You must install PCI expansion-slot covers on all vacant slots to maintain the electronic emissions characteristics of the server and to ensure server components are cooled properly.
4. Touch the static-protective package that contains the adapter to any unpainted metal surface on the server.
5. Remove the adapter from the static-protective package and avoid touching the components and gold-edge connectors on the adapter.
6. Insert the adapter into the riser-card assembly, aligning the connector on the adapter with the connector on the riser-card assembly.
7. Press the adapter connector firmly into the riser-card connector and ensure that the adapter snaps securely into the riser-card assembly.
8. Insert the riser-card assembly into the riser-card connector on the system board.
9. Press down on the assembly and ensure that the riser-card assembly is fully seated in the riser-card connector on the system board.
10. Connect the cables on the adapter.

Job aid

The following graphic shows the multiport serial adapter installation.

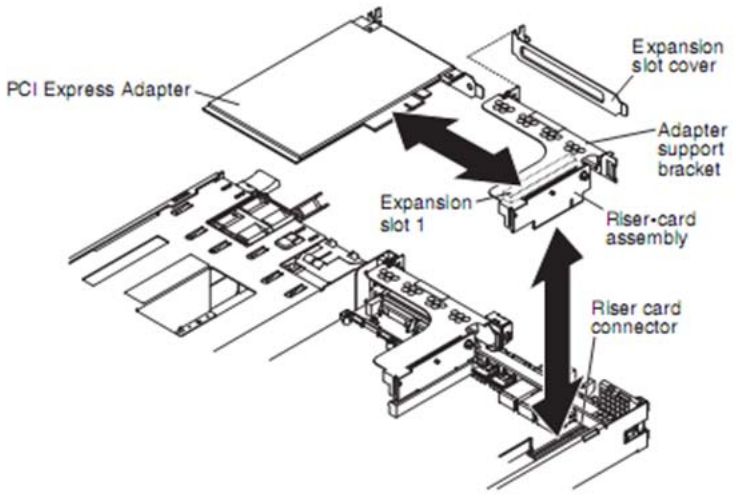


Figure 8: Multiport serial adapter

Replacing the server top cover

Replace the server top cover after you inspect the interior for damage.

Caution:

Risk of equipment damage

Ensure that no tools or loose parts are inside the server chassis before you replace the cover.

1. Slide the cover forward, and ensure that all the tabs on the front, rear, and side of the cover engage the chassis correctly.
2. Close the fan door and slide the cover release latches back to lock the cover in place.
3. Tighten the thumbscrew on the back of the server.

Installing the HMS 400

Install the HMS 400.

Prerequisites:

Ensure the chosen location meets the requirements defined in Site preparation checklist on page 14.

Install the HMS 400 in the 19 inch equipment rack according the instructions provided with your server.

Connecting peripherals to the HMS 400

Connect the monitor, keyboard, and mouse to the HMS 400.

Caution:

Risk of system failure

Install and use only Avaya-approved peripheral devices. To prevent system failure, install and use only Avaya-approved devices.

1. Place the monitor, keyboard, and mouse in the same location as the server.
2. Plug the keyboard and mouse into the appropriate USB connectors on the front panel.
3. Plug in the monitor connector and tighten the screws on the connector.
4. Connect the power cord to the monitor and plug the monitor into a power receptacle.
5. Turn on the monitor.

Job aid

The following graphics show the front and rear view of the HMS 400 server.

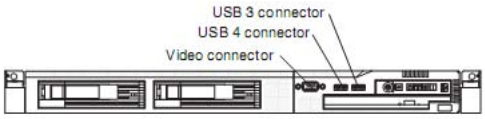


Figure 9: HMS 400 server front view

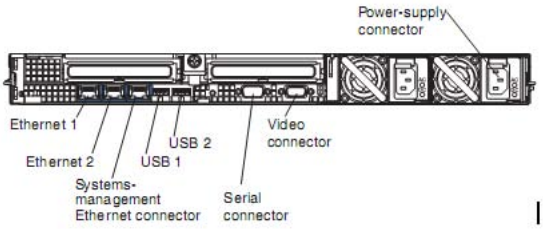


Figure 10: HMS 400 server rear view

Connecting the modem to the HMS 400 server

A modem is required for remote support dial-up access to the HMS 400 server. The modem enables Avaya technical support to connect to the HMS 400 server for troubleshooting purposes. Avaya requires that you connect the modem to your server only when you request technical assistance.

Prerequisites:

To install the modem, the following items are required:

- An analog modem that includes an analog RJ-11 analog phone cord and US Robotics 56 Kb/s USB modem. The Avaya order code for North America only is NTUB30HA. Other regions must supply an equivalent USB modem.
- An analog line jack.

1. To connect the modem, connect the B end of the USB A-B cable into the back of the modem.
2. Connect the A end of the USB A-B cable into an available USB port on the rear of the server.
3. Connect one end of the telephone cable into the modem RJ-11 jack that is labeled LINE.
4. Connect the opposite end of the telephone cable into the RJ-11 wall jack.

Connecting the HMS 400 server to power

Ensure that proper power and grounding are available for all the power outlets that serve the HMS 400 server and associated peripherals. Power for these devices must be wired and fused independently of all other receptacles and referenced to the same ground as the CS 1000. When the server connects to an AC power source but is not on, the operating system does not run, and all core logic except for the service processor (the baseboard management controller or optional Remote Supervisor Adapter II SlimLine) is shut down. The server can respond to requests from the service processor, such as a remote request to turn on the server. The power-on LED flashes to indicate that the server is connected to AC power but is not on.

Warning:

Use the connecting cables, power cord, and AC adaptors shipped with the equipment or specified by Avaya. If you use any other equipment, it can cause failures, malfunctions, or fire. Use power cords shipped only with this equipment. Not following these guidelines can lead to death or severe injury.

Warning:

Risk of personal injury and risk of hardware failure

You must connect the power outlets that are used by the HMS 400 server and the peripheral devices to the same single-point ground reference as the one used by the CS 1000 switch connected to the HMS 400 server. If this requirement is not met, power transients can cause personal injury, hardware failure, or both.

1. Plug the HMS 400 server AC power cord into the HMS 400 server rear panel.
2. Plug the opposite end of the HMS 400 server AC power cord into a wall receptacle or power bar.

Starting HMS 400

You can start the HMS 400 approximately 20 seconds after the server connects to AC power. The power-control button becomes active and one or more fans might start running to provide cooling while the server is connected to power.

Prerequisites:

- If a power failure occurs while the server is turned on, the server restarts automatically when power is restored.
- If you installed an optional Remote Supervisor Adapter II SlimLine, you can turn on the server from the Remote Supervisor Adapter II SlimLine user interface.
- If your operating system supports the Wake on LAN feature, the Wake on LAN feature can turn on the server.

1. To start the server, press the server power switch.
2. Observe the Power-On Self-Test (POST) and initialization messages on the monitor.

Chapter 7: Avaya Hospitality Messaging Server 400 software installation

This chapter describes how to install Avaya 400 software. For new Avaya HMS 400 servers, a trained technician must install the HMS 400 system image from the system image DVD.

For information about installing service updates, see *Avaya Hospitality Messaging Server 400 Maintenance, NN42350-101*.

Important:

Do not use DHCP.

- Obtain a static IP address from the administrator for the HMS 400 server.
- Ensure that the HMS 400 server has access to the CS 1000 TLAN (Node IP) and to the customer LAN (for Web configuration). To connect an Avaya HMS 400 server to the network, the hotel administrator must determine how to configure the network based on the security or IP policies deemed appropriate, as long as the HMS 400 server has access to the CS 1000 TLAN (Node IP) and customer LAN (for Web Configuration).
- If the hotel administrator plans to run PMSI over IP, then the administrator can run PMSI over IP to the hotel PMS only or to the hotel PMS and to the CS 1000. If the administrator plans to run PMSI over IP to both the hotel PMS and to the CS 1000, the server needs to access the CS 1000 ELAN. The number of NIC ports used depends on these factors. These factors also determine what IP address to configure for each NIC.
- If the hotel administrator plans to run PMSI over IP to both the hotel PMS and to the CS 1000, two NICs are required. Assign the first NIC to connect to the CS 1000 node IP (TLAN) and assign the second NIC to connect to the ELAN.
- To connect a 703t server, users must have access to the Web configuration. If the hotel administrator plans to implement PMSI over IP, then this determines which IP address to configure for each NIC.

Navigation:

- Installing or restoring the HMS 400 image on page 63
- Installing Auto Attendant software on the HMS 400 HP ProLiant server on page 64
- Configuring Dialogic HMP on page 65

Installing or restoring the HMS 400 image

Install the HMS 400 from an image DVD. To restore the system if a hard disk fails, the same steps apply.

Prerequisites:

Ensure that you configure the BIOS to start from the DVD drive. By default, the server starts from the DVD drive. If the DVD drive is not the default, you must configure the BIOS settings by pressing F12 on the POST screen and selecting CD-ROM.

1. Place Recovery DVD into the DVD-ROM drive.
2. Exit HMS 400 and reboot the server.
3. On the **Select desired operation** window, select **1. Recovery CD**.
4. Ensure that you read any warnings that appear and press any key to continue the installation.
5. When the following prompt appears, type `Y` .

   ```
   Do you wish to perform a system recovery function on this
   server, which will result in a complete overwrite of all
   present hard drive data? [Y/N]
   ```

6. When the following prompt appears, type `Y`.

   ```
   Would you like to proceed with this recovery function and a
   complete overwrite of all present hard drive data? [Y/N]
   ```

7. When the following prompt appears, press any key to continue.

   ```
   The system recovery function has completed successfully.
   Please remove all media from drives and reboot the server.
   Press any key to continue...
   ```

8. Remove the DVD and reboot the sever.

Installing Auto Attendant software on the HMS 400 HP ProLiant server

The HMS400 HP Server image does not have the Auto Attendant software installed by default. You must install it.

Follow this procedure to install the Auto Attendant software on the HMS400 HP ProLiant server.

1. Open the Web Administration user interface and click **Hotel Operations**.
2. At the bottom of the Hotel Operation menu, click **Download AA Setup**.
3. Click **Save** and save the **AA.zip** file to the hard drive of the HMS 400 system server.

4. Navigate to the saved AA.zip file and unzip the **AA.zip** file to a location on the HMS 400 system server.
5. Open the unzipped file and double click **setup.exe**.
6. If the system displays a security warning, click **Run**.
7. In the **HMS400V2 Auto Attendant Setup** dialog box, click **OK** to begin the Auto Attendant software installation.
8. Click the Installation icon to continue with the installation.

   See the following figure.



9. In the **HMS400V2 Auto Attendant Setup - Choose Program Group** dialog box, click **Continue** to accept the default folder name.
10. When installation is complete, select the Auto Attendant icon on the main HMS GUI on the server to access the Auto Attendant application.

    For information on using Auto Attendant, see *Avaya Hospitality Messaging Server 400 Administration. NN42350–600*.

Configuring Dialogic HMP

Configure the Dialogic Host Media Processing (HMP) to place and receive calls.

1. Select **Start > Programs > Intel Netstructure HMP > Configuration Manager-DCM**.
2. On the **Configuration Manager** window, right-click **HMP_Software #0 in slot 0/65535** and select **Configure Device**.
3. On the **Properties** window, select the **Default IP Address** tab.
4. Ensure the correct IP address is bound to the HMP Drivers.

   Important:

   If the wrong IP address is bound to the HMP, the system can function incorrectly; for example, it may not detect DTMF.
5. Click **OK**.

6. On the **Configuration Manager** window, click **Play**.
7. Select **Settings > System/Device autostart > Start System**.
8. Close the **Configuration Manager** window.
9. Reboot the server.

Chapter 8: Avaya Hospitality Messaging Server 400 server commissioning

This chapter describes how to commission the Avaya HMS 400 server.

- Enter a valid keycode to activate the number of channels and features in the HMS Keycode Setup application that is available on the desktop.
- You must restart the HMS 400 application to apply changes.
- Single-server configuration on page 67
- Multi-server configuration on page 82

Single-server configuration

This section describes how to configure an HMS 400 single-server system.

This configuration method applies to all Avaya HMS 400 servers.

Single-server configuration procedures

This task flow shows you the sequence of procedures you perform to configure an HMS 400 single-server system.

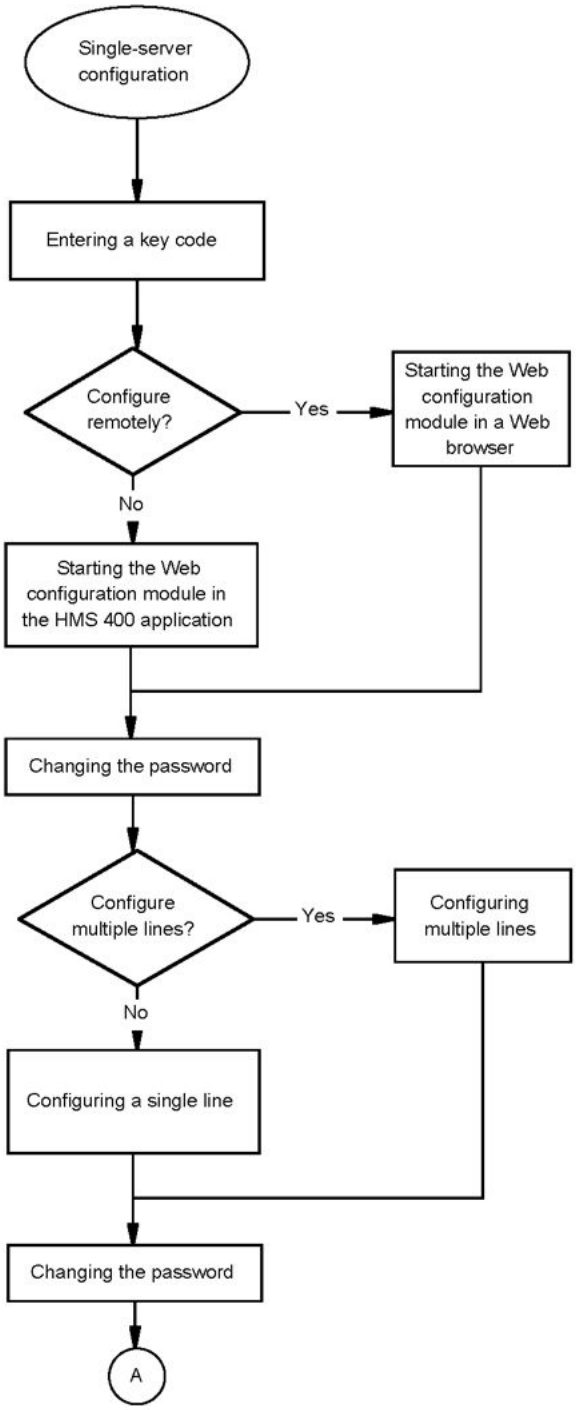
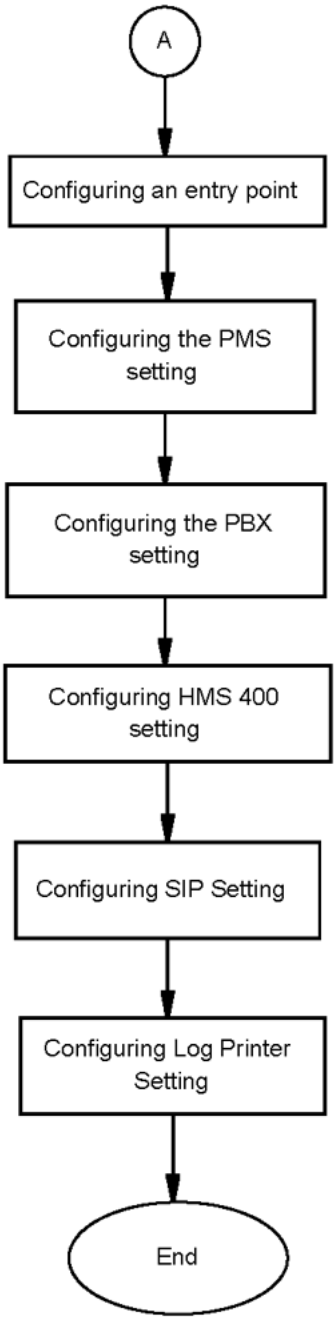


Figure 11: Single-server configuration procedures



Single-server configuration navigation:

- Entering a key code on page 70
- Starting the Web configuration module in a Web browser on page 70
- Starting the Web configuration module in the HMS 400 application on page 129
- Changing the password on page 71

- Configuring a single line on page 72
- Configuring multiple lines on page 73
- Configuring an entry point on page 74
- Configuring the PMS setting on page 76
- Configuring Communication Server 1000 settings on page 78
- Configuring HMS 400 server settings on page 80
- Configuring SIP Setting on page 81
- Configuring Log Printer Setting on page 82

Entering a key code

When the Web Configuration starts, the system detects the presence of a valid keycode. If a valid keycode is not available, a Key Code alert appears. The alert message provides information about how to address the key code issue. Ensure that the security dongle connects to a free USB port on the HMS 400 server before you start the Web configuration.

Prerequisites:

- The keycode is included in an envelope with your HMS 400 shipment.
- The keycode is case-sensitive.
- For information about the location of the USB ports, see *Avaya Hospitality Messaging Server 400 Fundamentals, NN42350-104*.
- On the Key Code Information window, the Security lock serial number appears in the Serial Number box. If the serial number does not appear, the Security lock may not be programmed or it is faulty.

1. In the **Key Code Information** dialog box, in the **Enter Key Code** box, type or paste your key code.
2. Click **Verify**.
   If the key code is invalid, the system does not start.
3. If the key code is valid, check the **Results** box to confirm the number of channels available and the active features.
4. Close the **Key Code Information** dialog box.
   The HMS 400 software loads automatically.

Starting the Web configuration module in a Web browser

Start Web Configuration from a Web browser to configure options for your system.

Prerequisites:

If this is the first time you access the Web configuration module, ensure that the security dongle connects to a free USB port on the HMS 400 server before you start Web configuration.

1. Open Internet Explorer and the following Web site appears by default:
   https://hms400v2/hms400webui/password.aspx
2. On the **HMS 400** window, in the **User Type** list, select **Admin User**.
3. In the **User ID** box, type the user **ID**.
   The default is SuperAdmin.
4. In the **Password** box, type the password.
   The default password is abc123. Ensure that you immediately change this password.
5. Click **Login**.

Changing the password

Change the Web configuration module password.

Prerequisites:

- The number of days a user password is valid before it expires is configured when you create a user.
- An administrator password is valid for 60 days. If the Administrator password expires, the administrator can log on one additional time using the old password and must create a new password that is valid for 60 days.
- Users are reminded seven days prior to the expiry date, and every day after until the actual expiry date, that their password is about to expire.
- The password must be six to eight alphanumeric characters.

1. On the **Web Configuration** main navigation bar, click **Change Password**.
2. On the **Change Password** window, in the **Old Password** box, type your old password.
3. In the **New Password** box, type a new password.
4. In the **Re-Type New Password** box, retype the new password.
5. Click **Update**.

Configuring a single line

Configure a single line.

Prerequisites:

Avaya recommends that you do not enable Auto Wake-Up and Remote Notification for all lines to ensure that enough channels are available for incoming calls during Auto Wake-Up peak periods. This is applicable to a 703t server only.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, click **Line Type**.
3. On the **Line Type** window, in the table of available lines, click **Edit** beside the line you want to configure.
4. (Applicable to 703t servers only) In the **Extn No** box, type the extension number of the line.
5. In the **Line Type** list, select the required line type.
6. In the **Language** list, select the language for the system prompts.
7. (Applicable to 703t servers only) To enable Auto Wake-Up (AWU) calls, select the **AWU Enabled** check box.
8. (Applicable to 703t servers only) To enable Remote Notification, select the **Remote Notification Enabled** check box.
9. (Applicable to 703t servers only) To enable the Message Waiting Lamp (MWL), select the **MWL Enabled** check box.
10. Click **Update Single** to save your changes.

Variable Definitions

Variable	Value
Line No	The line number selected.
Extn No	The extension number (DN) for the line. This is not required for SIP channels.
Line Type	The line type.

Variable	Value
	• VoiceMail • Minibar/RoomStatus • Auto Wakeup For SIP channels, only VoiceMail is available.
Language	Select the language for the system prompts.
AWU	Enables Auto Wake-Up calls.
Remote Notification	Enables Remote Notification calls.
MWL	Enables the Message Waiting Lamp notification.

Configuring multiple lines

Configure multiple lines.

Prerequisites:

Avaya recommends that you do not enable Auto Wake-Up and Remote Notification for all lines to ensure that enough channels are available for incoming calls during Auto Wake-Up peak periods. This is applicable to a 703t server only.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, click **Line Type**.
3. In the **Line Range** boxes, type the first and last line number of the range of lines that you want to edit.
4. (Applicable to 703t servers only) In the **Starting Extension** box, type the beginning extension number for lines you want to edit.

   The remaining lines in the specified line range are automatically assigned sequential extension numbers in ascending order.
5. In the **Line Type** list, select the required line type.
6. In the **Language** list, select the language for the system prompts.
7. (Applicable to 703t servers only) To enable Auto Wake-Up calls, select the **AWU Enabled** check box.
8. (Applicable to 703t servers only) To enable Remote Notification, select the **Remote Notification Enabled** check box.

9. (Applicable to 703t servers only) To enable the Message Waiting Lamp, select the **MWL Enabled** check box.
10. Click **Update Multiple** to save your changes.

Variable Definitions

Variable	Value
Line Range	The range of line numbers to edit.
Starting Extension	Assign the starting extension number for the first line in the specified range of lines. Subsequent lines are automatically assigned a sequential line number in ascending order.
Line Type	The line type. • VoiceMail • Minibar/RoomStatus • Auto Wakeup For SIP channels, only VoiceMail is available.
Language	Select the language for the system prompts.
AWU	Enables Auto Wake-Up calls.
Remote Notification	Enables Remote Notification calls.
MWL	Enables the Message Waiting Lamp notification.

Configuring an entry point

Entry points function as a translation table that the system can reference to determine how to respond to and handle a call. Ensure that you configure entry points correctly for proper system operation.

Entry points are comprised of two parts:

- Called/Calling Party Identification (CPI) string contains called party and calling party information. The CPI string is transmitted by the CS 1000 every time a call is answered.
- Call Flow. For information about call flows (also known as Auto Attendant Flows or AAF), see *Avaya Hospitality Messaging Server 400 Fundamentals, NN42350-104*.

The entry point format is as follows:

<Called Party>_<Calling Party>

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, click **Entry Point**.
3. On the **Entry Point** window, in the first **Entry Point Format** box, type the called party number or extension number of a specific service.
4. To configure advanced options for the calling party, select the **Advanced Setting** check box.
5. If you did not select Advanced Setting, a `W` appears in the second Entry Point Format box as the Calling Party.

   If you do not configure Advanced Setting, W is the only option available for Calling Party.
6. If you selected **Advanced Setting**, in the second **Entry Point Format** box, type `W`, `C`, or `X` as the Calling Party.
7. In the **Call Flow** list, select a call flow.
8. Click **Add**.
9. Click **Change Position** to change the order of the configured entry points.

   Ensure that the W_W entry point is the last entry in the entry points table.

Job aid

The following table identifies call flows that are available to configure an entry point.

Table 8: Available call flows

Call flow	Description
BUSY/NOANSWER	Used when a call is not answered. The caller can leave a message or be transferred to the operator. For a Busy/NoAnswer call flow, the only entry point required is W_W. This format is automatically added and must be the last item in the list.
DIRECT	Access a user mailbox to retrieve message or modify mailbox options.
SETAWU	A guest or operator can configure an Auto Wake-Up call.

Call flow	Description
XPRESS MESSAGE LEAVE	Leave a message without calling a user. Note: All messages left this way will have 'Hotel Staff' as the Call Sender ID.
XPRESS MESSAGE RETRIEVE	Retrieve a message from any phone on the system.
POST CO RETRIEVE	Retrieve messages for hotel guests that checked out recently.
MINIBAR/Room Status	Update the hotel PMS with charges for items guests consumed from the minibar and with guest room status.
TUI	Access the Telephone User Interface (TUI) to complete administrative transactions over the telephone.
CALLFLOW.AA	Access various Auto Attendant call flows.

The following table identifies the options available for the Calling Party.

Table 9: Calling party options

Calling party option	Description
W	A wildcard that represents any length for the Called or Calling Party. The wildcard option can be used for any call flow and is the default option.
C	Use this option if the Called Party information is required. This option is used for the DIRECT and SETAWU call flows. This option is available only if you selected Advanced Setting.
X	Use this option to ignore the Calling Party information. This option is used for TUI, AA, MINIBAR, ROOMSTATUS, XPRESS MESSAGE, and SETAWU call flows. This option is available only if you selected Advanced Setting.

Configuring the PMS setting

Configure the Property Management System (PMS) settings for the Hotel PMS interface.

Important:
Obtain the required information from the Hotel PMS representative and configure only the options specified.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, select **PMS Setting**.
3. In the **PMS Setting** window, select **Comm Setting** or **IP Setting**.
4. In the **Comm Setting** or **IP Setting** section, click **Edit** to configure the required options.
5. If you selected **Comm Setting**, select the required options for **COM Port**, **BAUD Rate**, **Parity**, **Data Bit**, and **Stop Bit**.
6. If you selected **IP Setting**, type the required values for **PMS IP** and **Port No**.
   For PMS IP, type the ELAN IP address.
7. Click **Update** to save your changes.

Variable Definitions

Variable	Value
COM Port	The communications port number. The range is 1 to 9.
BAUD Rate	The data transmission rate in bits per second (b/s). • 110 • 300 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 • 230400

Variable	Value
	• 460800 • 921600
Parity	Select a parity bit for error detection. • None • Odd • Even
Data Bit	The data bit. The range is 4 to 8.
Stop Bit	The stop bit. • 1 • 1.5 • 2
PMS IP	The PMS IP (ELAN) address.
Port No.	The PMS port number.

Configuring Communication Server 1000 settings

Configure Communication Server 1000 (CS 1000) settings to enable communication between the HMS 400 and CS 1000.

Important:

Obtain the required information from the Hotel PBX representative and configure only the options specified.

Prerequisites:

Ensure that you know the PMS PTY user name and password that you created in Creating a PMS PTY user name and password on page 40.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, select **PBX Setting**.
3. In the **PBX Setting** window, select **Comm Setting** or **IP Setting**.
4. In the **Comm Setting** or **IP Setting** section, click **Edit** to configure the required options.
5. If you selected **Comm Setting**, complete the following:
   - From the **COM Port** list, select the COM port number.

- From the **BAUD Rate** list, select **2400**.
- From the **Parity** list, select **None**.
- From the **Data Bit** list, select **8**.
- From the **Stop Bit** list, select **1**.

6. If you selected **IP Setting**, complete the following:
   - In the **PBX IP (ELAN)** box, type the ELAN IP address.
   - In the **PBX PMS Login Name** box, type the PMS PTY user name.
   - In the **PBX PMS Password** box, type the PMS PTY user password.
7. Click **Update** to save your changes.

Variable Definitions

Variable	Value
COM Port	The communications port number. The range is 1 to 9.
BAUD Rate	The data transmission rate in bits per second (b/s). • 110 • 300 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 • 230400 • 460800 • 921600
Parity	Select a parity bit for error detection.

Variable	Value
	• None • Odd • Even
Data Bit	The data bit. The range is 4 to 8.
Stop Bit	The stop bit. • 1 • 1.5 • 2
PBX IP (ELAN)	The PMS IP address.
PBX PMS Login Name	The PBX PTY user name.
Password	The PBX PTY password.

Configuring HMS 400 server settings

Configure the HMS 400 server IP address and SNMP setting in the HMS 400 Server Settings section. Unless the IP address changes, you configure the HMS 400 server IP address only once. If the IP address changes, you must reconfigure the HMS 400 IP address setting. After you configure the SNMP settings, a third-party SNMP manager system can capture HMS 400 SNMP notifications.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, click **HMS400 Server Setting**.
3. In the **HMS400 Server Setting** window, in the **HMS400 TCP/IP Setting** section, click **Edit**.
4. In the **New HMS400 IP** box, type the HMS 400 IP (TLAN) address.
5. Click **Update** to save your changes, or click **Cancel** to discard your changes.
6. In the **SNMP Setting** section, click **Edit**.
7. In the **New SNMP Manager IP** box, type the SNMP Manager IP address.
8. (Optional) In the **Port No** box, type the SNMP port number if it is required.
9. Click **Update** to save your changes, or click **Cancel** to discard your changes.

Configuring SIP Setting

Configure the SIP setting.

Prerequisites:

The SIP Server IP is the CS 1000 TLAN Node IP address.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, click **SIP Setting**.
3. To change the IP address, in the **SIP Setting** section, in the **New SIP Server IP** box, type the server IP address.

   The current SIP server IP displays the current IP address.
4. For **Default Transport**, select **TCP** or **UDP**.
5. In the **Port No** box, type the default port number `5060`.
6. Select the **User Agent** check box to activate the sender name display in the packet.
7. Click **Save** to save your changes.

Variable Definitions

Variable	Value
Current SIP Server IP	The current SIP server IP address.
New SIP Server IP	The new SIP server IP address
Default Transport	The protocol used for packet transfer. • TCP—Transmission Control Protocol • UDP—User Datagram Protocol
Port No	The SIP server port number. The default port number is 5060.
User Agent	Activates the sender name display in the packet sent.

Configuring Log Printer Setting

Configure the Log Printer setting to specify the printer that transactions are sent to for printing. HMS 400 supports up to three printers and a printer can be either Local or Networked.

Prerequisites:

- You must configure printers separately and they must be recognized by the operating system before you can select the printer in the Log Printer Setting section.
- You can configure printers for the following options:
  - AWU
  - Minibar
  - Room Status

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, click **Log Printer Setting**.
3. In the **Local Printer** list, select the printer that you want to send print requests to for printing.
4. To configure a network printer for AWU Printer, Minibar Printer, or Room Status Printer, select **Network Printer**.
5. In the **Network Printer** box, type the URL of the network printer.
6. Click **Save** to save your changes.

Multi-server configuration

This section describes how to configure an HMS 400 multi-server (cascading) network.

This configuration method applies only to 703t servers. To support larger installations of HMS 400, you can group multiple servers over a private IP network. This installation method supports up to 120 ports, and up to 5 000 guest mailboxes (depending on how you allocate features). In this configuration, you store the databases and mailboxes only on the Main Server. Client Servers provide additional ports for AWU load sharing. Each server can have a maximum of 40 ports; that is, a two-server configuration supports 80 ports, and a three-server configuration supports 120 ports.

Multi-server configuration procedures

This task flow shows you the sequence of procedures you perform to configure an HMS 400 multi-server (cascading) network.

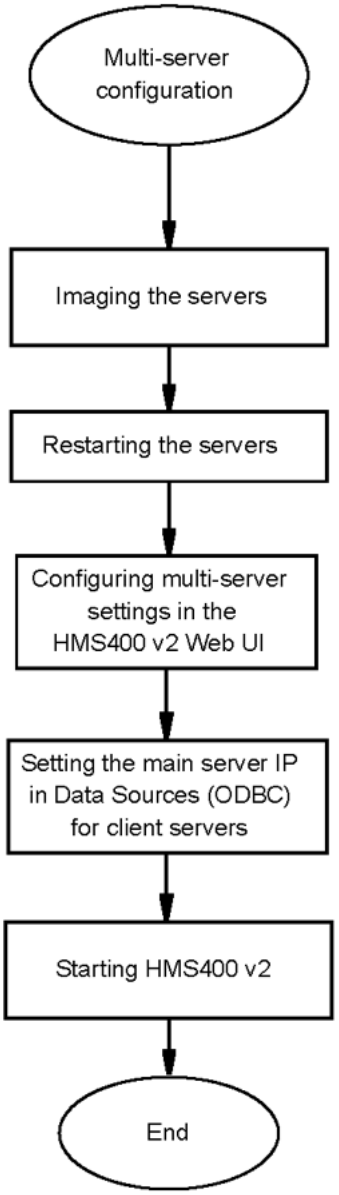


Figure 12: Multi-server configuration procedures

Multi-server configuration navigation:

- Imaging servers on page 84
- Restarting the servers on page 84
- Configuring multi-server settings in HMS400 v2 Web UI on page 84
- Configuring the Main Server IP in Data Sources (ODBC) for client servers on page 86
- Starting the HMS 400 application on page 87

Imaging servers

Install the HMS 400 software image on each 703t server in your multi-server configuration to ensure your network contains the correct software components.

Important:

Ensure you use the correct Image CD set. Do not connect the servers to the network at this point.

For information about installing an image on the servers, see Installing or restoring the HMS 400 image on page 63.

Restarting the servers

Restart the servers to implement the new image.

Important:

You must first connect the Main Server to the network, and then connect each Client Server. You must follow this rule because the network recognizes the first connected server as the Main Server (because all the servers have the same name).

For information about restarting the servers, see Stopping or restarting the HMS 400 on page 128.

Configuring multi-server settings in HMS400 v2 Web UI

Configure multi-server settings in the HMS400 v2 Web UI to configure the HMS 400 system as a cascading network.

You perform all cascading tasks only on the Main Server using the Cascading Server Setting page, which is the first page you see after you log on to the Web UI. You need only perform this procedure once.

1. On the **Cascading Server Setting** page, click the **Activate** option.
2. In the **Number of Server(s)** box, type the number of servers.
3. In the **Server ID** box, type `0` to configure the main server.
4. In the **Current Server IP** boxes, type the server IP address.
5. In the first **AWU Room Range** box, type the first room that you want the server to handle.
6. In the second **AWU Room Range** box, type the last room that you want the server to handle.

   Important:
   If you do not assign the AWU Room Range for each server, the system does not process Auto Wake-Up jobs. Each server must handle a different range of rooms; that is, you cannot assign duplicate room ranges on different servers.
7. Click **Update**.
8. Click **Add** to configure the first client server.

   The Server role automatically changes to CLIENT.
9. In the **Server ID** box, type `1` to configure the first client server.
10. Repeat step 3 on page 85 to step 7 on page 85.
11. Configure the C:\HMS400v2 folder as a shared network.
12. Configure the Administrator to have full access permission.

    Important:
    You cannot access the Web UI from the Client Server because it is disabled.
13. To configure a third server, in the **Server ID** box, type `2` to configure the second client server.
14. Repeat step 3 on page 85 to step 7 on page 85.

Variable Definitions

Variable	Value
Current Server IP	The current SIP server IP address.
Number of Server(s)	Maximum 3.
Server ID	Values: For the main server, type 0. For the first client server, type 1. For the second client server, type 2.

Configuring the Main Server IP in Data Sources (ODBC) for client servers

Configure the Main Server IP in Data Sources (ODBC) for client servers to access the HMS 400 database.

1. Choose **Start > All Programs > Administrative Tools > Data Sources (ODBC)**.
2. Click the **System DNS** tab.
3. In the **System Data Sources** box, double-click **voiceengine**.

   OR

   If the **voiceengine** data source is not listed in the **System Data Sources** box, go to 12 on page 86.
4. In the **Server** box, type the main server IP address.
5. In the **Port** box, type the port number.
6. In the **User** box, type your user name.
7. In the **Password** box, type your password.
8. Click **Test** to test the connection.

   A confirmation message appears
9. Click **OK**.
10. In the **System Data Sources** box, double-click **voicestatistic**.

    OR

    If the **voicestatistic** data source is not listed in the **System Data Sources** box, go to 12 on page 86.
11. Repeat step 4 on page 86 to 9 on page 86. Then, stop here.
12. Click **Add**.
13. In the **Create New Data Source** dialog box, click **MySQL ODBC 5.1 Driver**.
14. Click **Finish**.
15. On the **MySQL Connector / ODBC Data Source Configuration** page, in the **Server** box, type the IP address of the main server.
16. In the **Port** box, type `3306`.
17. In the **Password** box, type `000` (three zeros).
18. To configure the voiceengine data source, in the **Database** list, select **voiceengine**. Go to step 3 on page 86.

    OR

To configure the voicestatistic data source, in the **Database** list, select **voicestatistic**. Go to 10 on page 86.

Variable Definitions

Variable	Value
Password	The default password is 000. Do not change the password.
Port	The default port is 3306. Do not change the port.
Server	The HMS 400 main server IP address.
User	The default user is root. Do not change the user.

Starting the HMS 400 application

Start the HMS 400 application to start the multi-server system.

Important:
You cannot start the ExtLink and PMSI modules on client servers.

For information about starting an HMS 400 application multi-server system, see Starting the multi-server system on page 130 .

Chapter 9: Avaya Hospitality Messaging Server 400 system settings commissioning

This chapter describes how to commission the Avaya HMS 400 system settings.

Navigation:

- Configuring Outcall Attempts on page 89
- Configuring default check in language on page 91
- Configuring Message Housekeep on page 92
- Configuring room change requirements on page 93
- Configuring TUI settings on page 93
- Configuring Guest Mailbox PIN options on page 95
- Configuring AWU setting on page 96
- Configuring Minibar setting on page 98
- Configuring Room Status setting on page 101
- Configuring Operator setting on page 101
- Configuring VPIM shortcut on page 102
- Editing the VPIM shortcut on page 103
- Configuring additional VPIM options on page 103
- Configuring Language Mapping on page 104
- Configuring Remote Message Notification Setting on page 105

Prerequisites:

You must restart the HMS 400 system to apply changes.

Configuring Outcall Attempts

Configure the number of attempts or retries the HMS 400 system makes for a Remote Message Notification outgoing call when the initial attempt fails.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Pg 1** beside General Setting.
3. In the **Outcall Attempts** section, click **Edit**.
4. In the **Maximum Attempts** box, type the required number of attempts.
5. Click **Update** to save your changes or click **Cancel** to discard your changes.

Variable Definitions

Variable	Value
Maximum Attempts	The number of attempts or retries the HMS 400 system makes for a Remote Message Notification outgoing call when the initial attempt fails. The range is 1 to 99 attempts.

Configuring ring duration

Configure the number of seconds for an automatic wake up (AWU) call or remote notification call to ring before the system considers it to be unanswered.

Prerequisites:

Important:
The Call Forward No Answer (CFNA) duration on the CS 1000 must be longer than the number of seconds assigned for the AWU ring duration. In general, the default CFNA value is five rings, which translates to approximately 20 seconds. Therefore, it is recommended that you configure the AWU ring duration to something lower, such as 15 seconds. Otherwise, unintended results for the wake up call can occur.

1. Start **HMS 400 v2.0** and log on as an administrator.
2. On the menu bar, click **System Configuration**.
3. In the left pane, in the **System Settings** section, to the right of **General Setting**, click **Pg 1**.

4. In the right pane, in the **Ring Duration** section, click **Edit**.
5. From the **AWU** list, select the required number of seconds.
6. From the **RMN** list, select the required number of seconds.
7. Click **Update** to save your changes.
   OR
   Click **Cancel** to discard your changes.
8. Restart HMS 400 for the changes to take effect.

Variable Definitions

Variable	Value
AWU list	Select the number of seconds for an automatic wake up call to ring before the system considers the call unanswered.
RMN list	Select the number of seconds for remote notification call to ring before the system considers the call unanswered.

Configuring default check in language

When a customer checks into the hotel, the hotel PMS normally configures the preferred language for that customer. If the preferred language information is not provided, the HMS 400 system uses the Default Check In Language that you configure in the following procedure.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Pg 1** beside General Setting.
3. In the **Default Check In Language** section, click **Edit**.
4. In the **Language** list, select the default language.
   Only installed languages are available.
5. Click **Update** to save your changes, or click **Cancel** to discard your changes.

Configuring Message Housekeep

Deleted messages for the administrator, current guests, and guests who checked out are retained for a configurable number of days before the messages are permanently removed from the system. A guest who has checked out can retrieve messages with operator assistance.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Pg 2** beside General Setting.
3. In the **Message Housekeep** section, click **Edit**.
4. In the **Admin** box, type the maximum number of days that deleted messages are retained before being permanently deleted.
5. In the **Guest** box, type the maximum number of days that deleted messages are retained before being permanently deleted.
6. In the **Check Out Guest** box, type the maximum number of days that deleted messages are retained before being permanently deleted.
7. Click **Update** to save your changes, or click **Cancel** to discard your changes.

Variable Definitions

Variable	Value
Admin	The maximum number of days messages, deleted by the administrator, are retained before being permanently deleted. The range is 1 to 99 days. The default is 2.
Guest	The maximum number of days messages deleted by a current guest are retained before being permanently deleted. The range is 1 to 99 days. The default is 2.
Check Out Guest	The maximum number of days messages remain in a checked out guests mailbox before being permanently deleted. The range is 1 to 99 days. The default is 3.

Configuring room change requirements

Configure a timer (in seconds) to recognize the difference between a guest room change and a guest check out. The room change timer computes the time between receiving a check out record and a check in record for a guest. If the period is within the configured time frame, the system completes a room change and moves all the pertaining records to the new room.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Pg 3** beside General Setting.
3. In the **Room Change Requirements** section, click **Edit**.
4. In the **Room Change Interval** box, type a value for the room change interval in seconds.
5. Click **Update** to save your changes, or click **Cancel** to discard your changes.

Variable Definitions

Variable	Value
Room Change Interval	The time interval between a guest check out and check in that determines if the guest changed rooms instead of checking out. The default is 20 seconds. The range is 1 to 999 seconds.

Configuring TUI settings

Configure the default guest name and the PIN for any guest that is checked in using the TUI. An administrator can check a guest in using the Telephone User Interface (TUI). The default guest name is the new guest unless otherwise specified. You can base the PIN on the Room No. or Check In Date.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Pg 3** beside General Setting.
3. In the **TUI Setting** section, click **Edit**.
4. In the **Guest Name** box, type the default guest name or select the **Use default name** check box to use the default name.
5. In the **PIN** list, select the default PIN settings for the guest.
6. If you selected **Follow Check In Date** in the **PIN** list, select the PIN format in the **Date Format** list.
7. Click **Update** to save your changes, or click **Cancel** to discard your changes.

Variable Definitions

Variable	Value
Guest Name	The default guest name used for guests checked in using the TUI. The default name is New Guest.
PIN	The default PIN number for guests checked in using the TUI. • 1 - Follow Room No—the PIN is the same as the room number. • 2 - Follow Check In Date—the PIN is the check in date.
Date Format	The date format if Follow Check In Date is selected in the PIN list. The options available are: • mmdd—the PIN is the current month followed by the date. • ddmm—the PIN is the current date followed by the month.

Configuring Guest Mailbox PIN options

Configure the guest mailbox PIN format. Every guest requires a PIN to access their mailbox outside of their rooms. Guest PINs are automatically created when a guest checks in.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings Section**, click **Pg 3** beside General Setting.
3. In the **Guest Mailbox PIN Options** section, click **Edit**.
4. In the **PIN** list, select the PIN format.
5. If you selected **Default as Check In Date** in the PIN list, select the PIN format in the **Date Format** list.
6. If you selected **Default As Info From PMS** in the PIN list, in the **PIN Position** box type a value for the PIN position and in the **Pin Length** box, type a value for the PIN length.
7. If you selected **Default as Guest Name** in the PIN list, select the required language in the **Language** list and type a value for the PIN length in the **PIN Length** box.
8. Click **Update** to save your changes or click **Cancel** to discard your changes.

Variable Definitions

Variable	Value
PIN	The guest mailbox PIN format options. • 1 - Default As Room No • 2 - Default As Check In Date • 3 - Default As Info From PMS • 4 - Default As Guest Name
Date Format	The date format for the PIN. • mmdd—the PIN is the current month followed by the date. • ddmm—the PIN is the current date followed by the month.

Variable	Value
PIN Position	The digit entered in this field indicates the start position for the extraction of the PIN from the Name field of a Check In packet. The range is 1 to 99.
PIN Length	The number of digits for the PIN. The range is 1 to 8.
Language	The preferred language for the guest.

Configuring AWU setting

Configure the Auto Wake-Up (AWU) settings.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **AWU Setting**.
3. On the **AWU Setting** page, in the **Max Attempts** box, type a value for the maximum number of attempts that a wake-up call is made to a guest room the guest does not answer or if the line is busy.
4. In the **Next Call** box, type a value for the interval (in minutes) between AWU attempts.
5. In the **Printer Logging** list, select the print logging option required.
6. In the **AWU Operator** box, type the AWU operator extension number to call when AWU calls are unanswered after the maximum number of attempts is reached.
7. In the **No. of Net Send Recipients** list, select the number of other recipients to send failed AWU notifications to.

   If you select at least one recipient, the **PC*X*** box appears, where *X* is the recipient number.
8. If you selected at least one recipient in the **No of Net Send Recipients** list, in the **PC** box for each recipient, type the IP address or server name of the recipient.

   Important:
   Only recipients in the Domain name *Workgroup* can receive Net Send alerts. Ensure that the recipient's PC has Messenger Service activated.

   Check if the Messenger Service is activated:

   a. Go to **Control Panel** and open **Administrative Tools**.

b. Double-click **Services**.

c. On the Services page, double-click **Messenger**.

d. On the **Properties** window, on the **General** tab, click the **Start** button if the **Service Status** shows `Stopped`.

e. In the **Startup type** list, select **Automatic**.

f. Click **Apply**.

g. Click **OK**.

9. Click **Save** to save your changes.

Variable Definitions

Variable	Value
Max Attempts	The maximum number of attempts that a wake-up call is made to a guest room if there is no answer or the line is busy. The number of attempts includes the original call. When the maximum number of attempts is reached, the AWU operator is notified of the wake-up call failure. The default is 3. The range is 1 to 99.
Next Call	The interval in minutes between each AWU attempt. The default is 2 minutes. The range is 1 to 99.
Printer Logging	Specify the AWU log transactions to print. The options available are: • Disable Print—disables AWU printing. • Print Answered Call (Set/Cancel/Operator)—prints successful AWU calls including snooze, set, cancel, and transfer to operator attempts. • Print Busy/No Answer Call (Set/Cancel/Fail/Operator)—prints rescheduled (unanswered/busy) calls including set, cancel, fail, and transfer to operator attempts. • Print Fail (Set/Cancel/Fail/Operator)—prints calls made to the AWU operator

Variable	Value
	including set, cancel, fail, and transfer to operator attempts. • Print Failed wake up calls only—prints only failed wake up calls. • Print All—prints all AWU call transactions.
AWU Operator	The extension number of the AWU operator. The AWU operator is notified when an AWU call is unanswered after the maximum number of attempts is reached. When the AWU operator is notified, the room number is announced so that the operator can take appropriate action. The default extension is 0.
No. of Net Send Recipients	The number of additional recipients to send AWU failure notifications to. The message appears as a pop-up message on the recipient computer. Select 0 to disable this feature. The range is 0 to 10.
PC X	The IP address or server name of the PC that you want to send AWU failure notifications to.

Configuring Minibar setting

Configure all minibar-related settings in the Minibar Setting section.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Minibar Setting**.
3. On the **Minibar Setting** page, in the **Minibar Posting to PMS** list, select **Yes** to send all minibar posting to the Hotel PMS or select **No** to disable postings.
4. In the Log Printing list, select Yes to permit log printing for minibar transactions or select No to disable log printing for minibar transactions.
5. In the **Posting Type** list, select **Total (Lump Sum)** or **Itemized**.
6. If you want to configure tax options, select the desired options for **Tax 1**, **Tax 2**, and **Tax 3**.

Important:

By default, tax options are disabled and taxation is handled by the Hotel PMS. You can configure up to three tax options.

7. Click **Save** to save your changes.

Variable Definitions

Variable	Value
Minibar Posting to PMS	Defines minibar posting options. • Yes—send all minibar postings to the Hotel PMS. The type of packet sent depends on the options selected for Posting Type. • No—disable all minibar postings.
Log Printing	Enables or disables log printing for minibar transactions. • Yes—enable log printing for minibar transactions. • No—disable log printing for minibar transactions.
Posting Type	Defines how information about items purchased from the minibar is reported to the Hotel PMS. • Total (Lump Sum)—all postings for the room are added up and sent as one record with a grand total to the Hotel PMS. • Itemized—one record for each item entered by housekeeping is sent to the Hotel PMS. Each record contains the room number, quantity, item code, item price, and applicable taxes.
Tax 1	The following tax options that charge tax based on a specified percentage are available. • Category—Configure options for Food, Beverage, and Others. • Government Tax • Surcharge

Variable	Value
	• Value Added Tax • None You can configure each tax option only once.
Tax 2	Tax 2 has four Tax options only available (excluding the selected option in Tax 1).
Tax 3	Tax 3 has three Tax options only available (excluding the selected option in Tax 1 and Tax 2).
Food	Available if you selected the Category tax option When you create minibar items, each item is assigned a category of Food, Beverage, or Other. Specify the amount, as a percent of the item price, to charge as a tax for Food items.
Beverage	Available if you selected the Category tax option. When you create minibar items, each item is assigned a category of Food, Beverage, or Other. Specify the amount, as a percent of the item price, to charge as a tax for Beverage items.
Others	Available if you selected the Category tax option. When you create minibar items, each item is assigned a category of Food, Beverage, or Other. Specify the amount, as a percent of the item price, to charge as a tax for Other items.
Tax Method	Available if you selected the Government, Surcharge, or Value Added Tax option. • Basic only—imposes tax based on the basic amount. • Basic + Tax—imposes tax based on the amount after previous taxes are added.
Surcharge	Available if you selected the Surcharge tax option. Defines the amount of surcharge tax to add as a percentage of the item price.
Value Added Tax	Available if you selected the Value Added Tax option.

Variable	Value
	Defines the amount of value added tax to add as a percentage of the item price.
Government Tax	Available if you selected the Government Tax option. Defines the amount of government tax to add as a percentage of the item price.

Configuring Room Status setting

Enable or disable log printing for the room status transactions.

Prerequisites:

To print room status transactions, you must assign a printer for the Room Status Setting. For more information, see Configuring Log Printer Setting on page 82.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Room Status Setting**.
3. On the **Room Status Setting** page, in the **Log Printing** list, select **Yes** to enable log printing for room status transactions or select **No** to disable log printing for room status transactions.
4. Click **Save** to save your changes.

Configuring Operator setting

Configure the Operator Setting to define the operator extension number and message desk retrieval extension.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Operator Setting**.
3. On the **Operator Setting** page, in the **Operator** box, type the Operator ACD queue DN or extension number of a specific attendant.

4. In the **Message Desk** box, type the extension number used for guest text message retrieval.
5. Click **Save** to save your changes.

Variable Definitions

Variable	Value
Operator	The operator ACD queue DN or extension number of a specific attendant. The maximum length is 10 digits.
Message Desk	Used to facilitate guest text message retrieval. The hotel staff member who attends this extension number reads messages left for the guest. The maximum length is 10 digits.

Configuring VPIM shortcut

Using the VPIM protocol, HMS 400 can exchange messages with a Call Pilot or another HMS 400 system on the same network. Configure the VPIM shortcut to permit the HMS 400 to communicate with other systems.

Important:
You cannot send messages using Outlook Express to HMS 400 as it does not conform to VPIM Protocol.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **VPIM Shortcut**.
3. On the **VPIM Shortcut** page, in the **Prefix** box, type the prefix number for the VPIM shortcut.
4. In the **PSTN** box, type the PSTN number to where to send a message.
5. In the **Domain** box, type the VPIM domain name.
6. Click **Save** to save your changes.

The prefix number is compared to existing extension numbers in the database. If you enter a prefix number that is the same as an existing number, an error occurs and you must change the prefix value.

Variable Definitions

Variable	Value
Prefix	The Prefix of the VPIM shortcut that indicates to the HMS 400 that the following message is to be sent to a VPIM recipient. The maximum length is 10 digits.
PSTN	The telephone number for . The maximum length is 20 digits.
Domain	The VPIM domain name.

Editing the VPIM shortcut

Edit the VPIM Shortcut to change an existing VPIM Shortcut configuration.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **VPIM Shortcut**.
3. On the **VPIM Shortcut** page, in the list of configured VPIM shortcuts, click **Select** beside the shortcut to edit.
4. Modify the **Prefix**, **PSTN**, and **Domain** options as required.
5. Click **Save** to save your changes, or click **Delete** to delete the VPIM Shortcut.

Configuring additional VPIM options

You can configure additional VPIM options after you start the HMS 400 system.

Prerequisites:

Ensure that you know the PSTN that you created when you configured the VPIM shortcut. See Configuring VPIM shortcut on page 102.

1. On the HMS 400 application main screen, click **VPIM**.
2. On the **Voice Profile For Internet Mail** window, select **Tools, Configure VPIM**.
3. On the **General** tab of the VPIM Configuration window, in the **Domain Name** box, type the domain name of the existing mail client or exchange server used in the hotel.
4. In the **PSTN** box, type the PSTN created earlier.
5. Select the **Send/Receive Configuration** tab.
6. In the **SMTP** box, type the IP address of the SMTP Server.
7. In the **SMTP Port** box, type the SMTP port number.
8. In the **POP3** box, type the IP address of the POP3 Server.
9. In the **POP3 Port** box, type the POP3 port number.
10. Click **OK** and minimize the Voice Profile For Internet Mail window.

Configuring Language Mapping

Configure Language Mapping options to ensure that hotel guests hear prompts in the language of their choice.

Prerequisites:

Obtain information about the Hotel PMS supported languages. Hotel PMSs have different ways of representing language codes. You must identify the language codes for your Hotel PMS.

1. On the **Web Configuration** main navigation bar, select **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Language Mapping**.
3. On the **Language Mapping** page, in the **Language** list, select the supported language.
4. In the **PMS Code** box, type the PMS code for that language.
5. Click **Add**.

6. To edit the Language Mapping, click **Edit** beside the mapping you want to edit.
7. To delete a Language Mapping, click **Delete** beside the mapping you want to delete.

Configuring Remote Message Notification Setting

The Administrator can configure the system to call a pre-defined external number to notify the user of a new voice message. Users can do these steps themselves if access is granted through their individual Mailbox Web page. Up to three numbers can be set per mailbox.

Prerequisites:

Obtain the external call prefix number(s), pause duration (if necessary), and the remote notification numbers from the customer.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **System Settings** section, click **Remote Message Notification Setting**.
3. On the **Remote Message Notification Setting** page, in the **Mailbox ID** box, key in the ID.
4. Click **Search**.
5. In the **Enable Notification** box, select **YES**.
6. In the **Phone#1** box, type the extension number (internal DN) OR The external prefix followed by "," then the phone number (external).
7. Click the check boxes beside **Phone#2** and **Phone#3** accordingly in order to key in the next numbers.
8. Click **Save** to save your changes.

Variable Definitions

Variable	Value
Enable Notification	Defines RMN options. The options available are: YES - Enable RMN NO - Disable RMN
Extension numbers	Valid Internal extension number (no).
External Prefix	The number(s) to dial before attempting an external call.
","	Indicates pause. Recommended maximum number of "," (pauses) can be used is two.
Maximum digits	A maximum of 26 digits can be entered in Phone#1, Phone#2, and Phone#3 boxes.

Chapter 10: Commissioning the Avaya Hospitality Messaging Server 400 database

Configure Avaya HMS 400 database options such as staff extension numbers, mailbox numbers, guest rooms, and guest extensions to ensure the HMS 400 can recognize each extension and room in the hotel as a valid configuration to prevent service disruption.

- Configuring a guest room on page 107
- Adding extensions to a Guest Room on page 109
- Configuring a single mailbox single extension Admin Mailbox on page 109
- Configuring a multiple mailbox single extension Admin Mailbox on page 111
- Configuring a single mailbox multiple extension Admin Mailbox on page 113
- Adding an extension to an Admin Mailbox on page 114
- Adding a mailbox to an Admin Mailbox on page 115
- Viewing or deleting an extension on page 116
- Creating users on page 117
- Editing user details on page 118
- Configuring Admin Classes of Service on page 119
- Configuring Guest Classes of Service on page 122
- Configuring an introductory message on page 125

Configuring a guest room

Configure a guest room to configure the CoS, number of rooms and number of extensions.

Prerequisites:

- Obtain a hotel room listing.
- For information about configuring a guest Class of Service (CoS), see Configuring Guest Classes of Service on page 122.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Guest Room Setup Pg 1**.
3. On the **Guest Room Setup** page, in the **No. of Rooms** box, type the number of rooms to create for a guest if the room numbers are sequential.

   OR

   In the **No. of Rooms** box, type `1`, and in the **Room No.** box, type the room number.
4. In the **COS** list, select the class of service for the guest.
5. In the **Extension 1** box, type the extension number for the guest.

   If you configure more than one room, succeeding extensions numbers are automatically assigned to the remaining rooms.
6. If each room has more than one line, select the check box beside each additional Extension and type the extension number in the **Extension** box.
7. Click **Create** to generate the guest room record.
8. Click **Update** to save the guest room record.

Variable Definitions

Variable	Value
No. of Rooms	The number of rooms to create for a guest. The default is 1.
Room No.	The guest room number.
COS	The class of service for the guest. This option determines the type of features and functions available to guest. The default is 0 - Default COS FOR Non VIP Guest.
Extension	The guest extension number. If you configure more than one room, succeeding extensions numbers are automatically assigned.

Adding extensions to a Guest Room

Perform this procedure to add extension number(s) to a guest room that has been configured.

Prerequisites:

Ensure that the extension numbers are not in use or taken.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Guest Room Setup Pg 2**.
3. On the **Guest Room Setup Pg 2**, in the **Mailbox ID** box, type the Mailbox of an existing room.
4. Click **Display Mailbox** to view the **Room No, Ext No, Mailbox ID, Ext type, and Status**.
5. In the **Extension** box, type the extension number.
6. Click **Save** to save your changes.

Variable Definitions

Variable	Value
Mailbox ID	Mailbox number of an existing room (generally, mailbox no = room number)
Extension	A valid new extension number

Configuring a single mailbox single extension Admin Mailbox

Configure an Admin Mailbox with one mailbox for each extension number to allow staff to access the voice mail services.

Prerequisites:

- You must create an extension for every staff member, even if the staff member does not have mailbox access for call transfer scenarios.
- For information about configuring Admin class of service, see Configuring Admin Classes of Service on page 119.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Admin Mailbox Setup Pg 1**.
3. On the **Admin Mailbox Setup** page, in the **No. of Extns** box, type the maximum number of extensions if the Admin extensions are sequential.

   If the Admin extensions are not sequential, type `1`.
4. In the **Extn Type** list, select the extension type.
5. In the **COS** list, select the class of service.
6. In the **Language** list, select the required language for the mailbox.
7. In the **Extension 1** box, type the starting extension number for the range of mailboxes.
8. Click **Create** to create the mailbox entries.
9. To modify the mailbox name, from the list, select the mailbox.
10. At the bottom of the page, in the box, type a name for the mailbox.

    You can type a first and last name.
11. Click **Add**.
12. Click **Update** to save the data.

Variable Definitions

Variable	Value
No. of Extns	The number of extensions to configure. The default is 1.
Extn Type	The extension type. The options available are:

Variable	Value
	• Mailbox—a valid extension with an active mailbox. • Extn—a valid extension without a mailbox. This is used for call transfer situations. • Phantom—a virtual extension with an active mailbox. Message waiting lamp (MWL) control now exists.
COS	The class of service (CoS) that determines the characteristics and behavior of the mailbox. The default is 1 - General Staff. You can configure up to 40 CoS.
Language	The language of the mailbox.
Extension 1	The starting extension number for the range of mailboxes.

Configuring a multiple mailbox single extension Admin Mailbox

Perform this procedure to create and assign up to five mailboxes to an extension number. If you configure this option, the system prompts the user to select the mailbox to leave a voice mail for.

Prerequisites:

- Confirm the mailbox numbers available. Mailbox numbers are usually the same as the extension numbers.
- Determine which extensions exist to help allocate the correct numbers and prevent duplication errors.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Admin Mailbox Setup Pg 1**.
3. On the **Admin Mailbox Setup** page, select the **Multiple Mailbox Single Extension** check box.
4. In the **Extension** box, type the extension number for the mailbox.
5. In the **Extn Type** list, select the extension type.
6. In the **COS** list, select the class of service.

7. In the **Language** list, select the required language for the mailbox.
8. In the **MailboxID1** box, type the mailbox identification number for mailbox 1.
9. To configure a second mailbox, select the check box beside **MailboxID2** and type the mailbox identification number for mailbox 2.
10. To configure a third mailbox, select the check box beside **MailboxID3** and type the mailbox identification number for mailbox 3.
11. To configure a fourth mailbox, select the check box beside **MailboxID4** and type the mailbox identification number for mailbox 4.
12. To configure a fifth mailbox, select the check box beside **MailboxID5** and type the mailbox identification number for mailbox 5.
13. Click **Create** to create the entries.
14. To modify the name of one of the mailboxes, from the list, select the mailbox.
15. At the bottom of the page, in the box, type a name for the mailbox.

    You can type a first and last name.
16. Click **Add**.
17. To modify the names of additional mailboxes, repeat steps 14 on page 112 to 16 on page 112.
18. Click **Update** to save the data.

Variable Definitions

Variable	Value
Extension	The mailbox extension number.
Extn Type	The extension type. • Mailbox—a valid extension with an active mailbox. • Extn—a valid extension without a mailbox. This is used for call transfer situations. • Phantom—a virtual extension with an active mailbox. Message waiting lamp (MWL) control now exists.
COS	The class of service (CoS) that determines the characteristics and behavior of the mailbox. The default is 1 - General Staff. You can configure up to 40 CoS.

Variable	Value
Language	The language of the mailbox.
MailboxID	The mailbox identification number.

Configuring a single mailbox multiple extension Admin Mailbox

Perform this procedure to create one mailbox that is shared by up to five extensions. A voice mail left for any of the configured extensions is saved in the assigned mailbox.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Admin Mailbox Setup Pg 1**.
3. On the **Admin Mailbox Setup** page, in the **No. of Extns** box, type `1`.

   Important:

   If you configure more than one extension, the extension numbers must be at least two numbers apart; they cannot be sequential.
4. In the **Extn Type** list, select **Mailbox**.
5. In the **COS** list, select the class of service.
6. In the **Language** list, select the required language for the mailbox.
7. In the **Extension 1** box, type the first extension number.
8. To configure a second extension, select the check box beside **Extension2** and type the second extension number in the **Extension2** box.
9. To configure a third extension, select the check box beside **Extension3** and type the third extension number in the **Extension3** box.
10. To configure a fourth extension, select the check box beside **Extension4** and type the fourth extension number in the **Extension4** box.
11. To configure a fifth extension, select the check box beside **Extension5** and type the fifth extension number in the **Extension5** box.
12. Click **Create** to create the entries.
13. To modify the mailbox name, from the list, select the mailbox.
14. At the bottom of the page, in the box, type a name.

    You can type a first and last name.

15. Click **Add**.
16. Click **Update** to save the data.

Variable Definitions

Variable	Value
No. of Extns	The number of extensions to configure.
Extn Type	The extension type. • Mailbox—a valid extension with an active mailbox. • Extn—a valid extension without a mailbox. This is used for call transfer situations. • Phantom—a virtual extension with an active mailbox. Message waiting lamp (MWL) control now exists.
COS	The class of service (CoS) that determines the characteristics and behavior of the mailbox. The default is 1 - General Staff. You can configure up to 40 CoS.
Language	The language of the mailbox.
Extension	The extension number for the mailbox.

Adding an extension to an Admin Mailbox

Perform this procedure to add an extension to an Admin Mailbox that has already been configured.

Prerequisites:

Ensure that the extension numbers entered are not in use or taken. You may also want to check the existing number to which additions are to be made by going to the **View/Delete** page.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Admin Mailbox Setup Pg 2**.

3. On the **Admin Mailbox Setup Pg 2**, select the **Add Extension** option.
4. In the **Mailbox ID** box, type the ID.
5. Click **Display** to view the details of the Mailbox ID.
6. In the **Extension** box, type the new extension number.
7. Click **Add** to save your changes.

Variable Definitions

Variable	Value
Extension	A valid new extension number

Adding a mailbox to an Admin Mailbox

Perform this procedure to add a mailbox to an Admin Mailbox that has already been configured.

Prerequisites:

Ensure that the mailbox numbers entered are not in use or taken. You may also want to check the existing mailbox number to which additions are to be made by going to the **View/Delete** page.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **Admin Mailbox Setup Pg 2**.
3. On the **Admin Mailbox Setup Pg 2**, select the **Add Mailbox** option.
4. In the **Extension** box, type the extension number.
5. Click **Display** to view the details of the extension.
6. In the **Mailbox ID** box, key in the new ID
7. Click **Add** to save your changes.

Variable Definitions

Variable	Value
Mailbox ID	A valid new Mailbox ID

Viewing or deleting an extension

Perform this procedure to view a list of the extensions or rooms in use or to delete an extension or room. You cannot delete a room that is still occupied.

Prerequisites:

- Admin extensions do not have a room number. The room number field is NULL.
- If more than one page of extension numbers is available, the number of pages appears at the bottom of the View/Delete Extension page. Select a page number to go to that page or click the ellipses (...) to view additional page numbers.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **Database Setup** section, click **View/Delete Extension**.
3. On the **View/Delete Extension** page, all extension numbers appear by default.
4. To view only guest extensions, select **Guest** and click **Display**.
5. To view only admin extensions, select **Admin** and click **Display**.
6. To view a specific extension using a room number, select **All**, type the room number in the **Room No** box and click **Display**.
7. To view a specific extension using an extension number, select **All**, type the extension number in the **Extension No** box, and click **Display**.
8. To delete an extension, select the check box beside each extension to delete.

   Important:
   Ensure mailboxes are not in use before you delete them.
9. Click **Delete**.
10. In the confirmation window, click **Yes** to delete the extension or **Cancel** to cancel the request.

Creating users

An administrator can create users with specific access rights for specific purposes. Current users appear at the bottom of the page.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **User Setup** section, click **Create User**.
3. On the **Create User** page, in the **User ID** box, type the user ID.
4. In the **User Name** box, type the user name.
5. In the **Password** box, type the user password.
6. In the **Confirm Password** box, retype the password.
7. In the **Password Retention** box, type the number of days that the user password is active before it expires.
8. In the **Access Rights** section, select the user access rights.

   Important:
   Avaya recommends that you enable the System Configuration Access Rights for only the administrator.
9. Click **Create User** to create the user or click **Clear** to discard your changes.

Variable Definitions

Variable	Value
User ID	The user identification name. The following rules apply to user IDs: • Must be at least four alphanumeric characters in length. • User ID is case-sensitive. • Spaces and symbols are not valid.
User Name	The user name.

Variable	Value
Password	The user password. The password must be six to eight characters in length and must contain at least one number and one letter. The password is case-sensitive.
Confirm Password	Password confirmation.
Password Retention	Password Retention determines how long the system keeps a user password active before it expires. The range is 1 to 120 days. If a user does not change the user password it expires, the user cannot access the Web module until the administrator creates a new password. Users are reminded that their password will expire seven days prior to the expiry date and every day after that until the expiry date is reached. For information about changing the user password, see Changing the password on page 71.
Access Rights	You can enable the following access rights for a user: • System Configuration • Hotel Operation—If you select Hotel Operation, the following options are enabled: Manual Posting, Hotel Employees, Room Status, Minibar, AWU, Auto Attendant. • Administration • Utilities • Reports

Editing user details

You can edit the user details.

Prerequisites:

You must create at least one user. For more information, see Creating users on page 117.

1. On the **Web Configuration** main navigation bar, click **System Configuration**.
2. In the **System Configuration** navigation, in the **User Setup** section, click **Create User**.
3. On the bottom of the **Create User** page, click **Edit** beside the user to edit.
4. On the **Edit User** page, modify the user details as necessary.
5. Click **Save** to save your changes, or click **Cancel** to discard your changes.

Configuring Admin Classes of Service

You can configure up to 40 Admin Classes of Service (CoS).

Prerequisites:

Two CoS are created by default. You can use the default CoS or create new ones.

- 1 General Staff
- 2 Executive Staff

1. On the **Web Configuration** main navigation bar, click **Administration**.
2. In the **Administration** navigation, in the **Mailbox Maintenance** section, click **Admin COS Configuration**.
3. On the **Admin Class of Service Configuration** page, in the **COS No** list, select the CoS number to configure.

   You can select an existing CoS or select number. You need not select numbers in sequence.
4. In the **Name** box, type a meaningful name for the CoS.
5. In the **Maximum Message(s) to Keep** box, type the total number of new and old messages to keep.
6. In the **Maximum Message Length** box, type the maximum message length in seconds.
7. In the **Number of Day(s) to Store New Messages** box, type the number of days to store new messages.

8. In the **Number of Day(s) to Store Old Messages** box, type the number of days to store old messages.
9. In the **Allow Message Broadcast** list, select **YES** to permit sending messages using a distribution list, or select **NO** to disable sending messages using a distribution list.
10. In the **Personal Identification Announcement** list, select **NAME** or **NUMBER** as the announcement type.
11. In the **Anonymity Mode** list, select **YES** to disable announcing the message sender ID or **NO** to announce the message sender ID.
12. In the **Pin Retention (in days)** box, type the number of days a user's PIN is valid for before it expires.
13. In the **Notify Before Pin Expires (in days)** box, type the number of days prior to the PIN Expiry date to begin alerting users that their PIN will expire.
14. In the **Remote Message Notification** list, select **Yes** to enable Remote Message Notification or **No** to disable it.
15. Click **Update** to save your changes.

Variable Definitions

Variable	Value
COS No	The Class of Service number.
Name	The CoS name. The maximum length is 30 characters.
Maximum Message(s) to Keep	The maximum capacity of the mailbox for new and old messages. **Important:** The range is 0 to 99 messages but Avaya recommends that you keep no more than 50 messages.
Maximum Message Length	The maximum recording length of a message in seconds. **Important:** The range is 0 to 999 seconds but Avaya recommends that you do not exceed 600 seconds.
Number of Day(s) to Store New Messages	The number of days to retain new messages. The range is 0 to 999 where 0 is unlimited.

Variable	Value
	This is typically 0 so the user can decide how to handle new messages.
Number of Day(s) to Store Old Messages	The number of days to retain old messages. The range is 0 to 999 where 0 is unlimited. This is typically 0 so the user can decide how to handle new messages.
Allow Message Broadcast	Enable or disable sending messages using a distribution list.
Personal Identification Announcement	The Personal Identification Announcement options are: • NAME—the user's recorded name is announced as the message sender. If no recorded name is available, the extension number is announced. • NUMBER—the user's extension number is announced as the message sender.
Anonymity Mode	Select YES to remain anonymous while sending messages. The system does not announce the message sender ID, a generic prompt is played that does not provide the sender name or number.
Pin Retention (in days)	The number of days a PIN is valid for before it expires.
Notify Before Pin Expires (in days)	The number of days prior to the PIN expiry date to begin notifying the user that their PIN will expire. Type 0 (zero) to disable this notification.
Remote Message Notification	This feature is useful for users who are frequently away from their desk. When you enable the feature, the system calls the user on a predefined number, such as the user’s mobile or home number, as soon as a new message is left for them. and the user can retrieve the message on the same call.

Automatic file synchronization

Automatic file synchronization occurs so that every server has the same set of files to ensure that each server can provide the same services that are available on the main server. By automating this function, you need not search for the location of all files and then manually copy them to each client server.

A full 24 hours must elapse before a message is considered as one day old. Because file synchronization runs once a day at midnight only, some messages are purged only on the next housekeeping cycle. For example, the CoS setting is one day for new messages and two days for old messages. A message is left at 8:00 a.m. on January 1 and a second message is left at 1:00 p.m. on the same day. The user listens to the first message (old) at 9:00 a.m. and hangs up. The first message is purged at 12:00 a.m. on January 4. The second message (new) is purged at 12:00 a.m. on January 3.

For the first (old) message, the logic is as follows:

- January 1 at 9:00 a.m. to January 2 at 9:00 a.m.—First day
- January 2 at 12:00 a.m.—Housekeeping runs. The first (old) message is less than one day old and is retained.
- January 2 at 9:00 a.m. to January 3 at 9:00 a.m.—Second day
- January 3 at 12:00 a.m.—Housekeeping runs. The first (old) message is less than two days old and is retained.
- January 4 at 12:00 a.m.—Housekeeping runs. The first (old) message is more than two days old and is purged.

For the second (new) message, the logic is as follows:

- January 1 at 1:00 p.m. to January 2 at 1:00 p.m.—First day
- January 2 at 12:00 a.m.—Housekeeping runs. The second (new) message is less than one day old and is retained.
- January 2 at 1:00 p.m. to January 3 at 1:00 p.m.—Second day
- January 3 at 12:00 a.m.—Housekeeping runs. The second (new) message is more than one day old and is purged.

Configuring Guest Classes of Service

You can configure up to 20 Guest Classes of Service (CoS). CoS 0 is the default CoS and you can configure CoS 1 to 20 as VIP classes.

Prerequisites:

CoS 0 is the default Guest CoS and is for cases when no CoS is specified or assigned for a room.

1. On the **Web Configuration** main navigation bar, click **Administration**.
2. In the **Administration** navigation, in the **Mailbox Maintenance** section, click **Guest COS Configuration**.

3. On the **Guest Class of Service Configuration** page, in the **COS No** list, select the CoS number to configure.

   You can select an existing CoS or another number. You do not need to select numbers in sequence.
4. In the **Name** box, type a meaningful name for the CoS.
5. In the **Maximum Message(s) to Keep** box, type the total number of new and old messages to keep.
6. In the **Maximum Message Length** box, type the maximum message length in seconds.
7. In the **Number of Day(s) to Store New Messages** box, type the number of days to store new messages.
8. In the **Number of Day(s) to Store Old Messages** box, type the number of days to store old messages.
9. In the **Prompt Message Sender Name** list, select **YES** to play the user's recorded name or select **NO** to play the extension number.
10. In the **Change Password** list, select **ALLOW** to hear the Change Password prompt or **DISALLOW** to disable the Change Password prompt.
11. In the **Record Personal Greeting** list, select **ALLOW** to hear the Record Personal Greeting prompt or **DISALLOW** to disable the Record Personal Greeting prompt.
12. In the **Set AWU** list, select **ALLOW** to hear the Set AWU prompt or **DISALLOW** to disable the Set AWU prompt.
13. In the **Enable Welcome** message list, select **YES** to hear a welcome message when a user accesses a mailbox for the first time or **NO** to disable the welcome message.
14. If you enabled the welcome message, you can select the **Turn MWL On When There Is A Welcome Message** check box to activate the MWL.
15. In the **VIP AWU Feature** list, select **YES** for an operator to manually make a wake-up call to the guest or select **NO** for the system to place the wake-up call to the guest.
16. Click **Update** to save your changes.

Variable Definitions

Variable	Value
COS No	The Class of Service number.

Variable	Value
Name	The CoS name. The maximum length is 30 characters.
Maximum Message(s) to Keep	The maximum capacity of the mailbox for new and old messages. **Important:** The range is 0 to 99 messages but Avaya recommends that you do not keep more than 50 messages.
Maximum Message Length	The maximum recording length of a message in seconds. **Important:** The range is 0 to 999 seconds but Avaya recommends that you do not exceed 600 seconds.
Number of Day(s) to Store New Messages	The number of days to retain new messages. The range is 0 to 999 where 0 is unlimited. This is typically 0 so the user can decide how to handle new messages.
Number of Day(s) to Store Old Messages	The number of days to retain old messages. The range is 0 to 999 where 0 is unlimited. This is typically 0 so the user can decide how to handle new messages.
Prompt Message Sender Name	If you select YES, the system plays the user's recorded name as the message sender or if a recorded name is not available, the user's extension number is played. If you select NO, the user's extension number is played.
Change Password	Enable or disable the Change Password prompt.
Record Personal Greeting	Enable or disable the Record Personal Greeting prompt.
Set AWU	Enable or disable the Set AWU prompt.
Enable Welcome Message	The Enable Welcome Message option has the following options: • YES - Welcome message is played when a mailbox is accessed for the first time. • NO - Welcome message is not played.
VIP AWU Feature	The VIP AWU Feature option has the following options:

Variable	Value
	• YES - The operator manually places the wake up call for the guest. • NO - The system places the wake up call for the guest.

Automatic file synchronization

Automatic file synchronization occurs so that every server has the same set of files to ensure that each server can provide the same services that are available on the main server. For more information, see Automatic file synchronization on page 121.

Configuring an introductory message

Configure an introductory message that plays every time users access their mailbox. It is the first prompt that is heard when users log into their mailbox. Once enabled, it is implemented system-wide so that both admin and guest mailboxes hear this prompt.

Prerequisites:

Record your introductory message prompt before activating this feature. For information about recording introductory message prompts, see *Avaya Hospitality Messaging Server 400 Front Desk Staff User Guide, NN42350-100*.

1. On the **Web Configuration** main navigation bar, click **Administration**.
2. In the **Administration** navigation, in the **Introductory Message** section, click **Activate Introductory Message**.
3. On the **Activate Introductory Message** page, select the **Enabled** check box to enable the introductory message.
4. Click **Update** to save your changes.

Chapter 11: Common procedures

The chapter includes common procedures that you use when you install and commission the Avaya Hospitality Messaging Server 400.

- Starting the Avaya Hospitality Messaging Server 400 server on page 127
- Stopping or restarting the HMS 400 on page 128
- Manually starting the Dialogic HMP service on page 128
- Starting the Web configuration module in the HMS 400 application on page 129
- Shutting down the multi-server system on page 129
- Starting the multi-server system on page 130

Starting the Avaya Hospitality Messaging Server 400 server

Start the Avaya HMS 400 server.

Important:

The HMS 400 cannot answer calls until the VoiceEngine shows that channels are ready. When Channels appear in the VoiceEngine window, the HMS 400 is ready to accept calls.

Prerequisites:

For more information, see *Avaya Hospitality Messaging Server 400 Fundamentals, NN42350-104*.

1. Ensure the server is properly connected to a power source.
2. Push the power button on the front panel of the server.
   Windows 2003 Server automatically loads.
3. After Windows 2003 Server starts, the HMS 400 application automatically loads.
4. Wait approximately 5 minutes for HMS 400 to become fully operational. The Dialogic Services must start before the Voice Engine starts.

Stopping or restarting the HMS 400

You can stop or restart the HMS 400 application.

1. On the HMS 400 application main screen, click **Stop**.
2. On the **Exit HMS 400 V2** window, type the password `000`.
3. Click **Exit**.
4. To restart the HMS 400, wait for the Voice Engine to completely shut down before attempting to restart HMS 400.

   If you do not wait for the Voice Engine to shut down, certain modules cannot start successfully. Wait for approximately 10 seconds and then check that the icon is no longer on the System Tray before continuing.
5. On the system tray, right-click the **PMSI** icon and select **Exit**.
6. On the **Exit HMS 400 v2** window, type the password `000`.
7. Click **Exit**.
8. If the **Operator Console** application is active, select **File > Exit** on the ExtLink Interface.
9. In the **Exit Password** window, type `000` and click **OK**.
10. On your desktop, double-click the **HMS400v2** icon to restart.

Manually starting the Dialogic HMP service

Manually start the Dialogic HMP service if the service does not automatically start.

1. Select **Start, Programs > Intel NetStructure HMP > Configuration Manager - DCM**.
2. In the **Configuration Manager** window, if the green **Play** button is active, the Dialogic service is active.

   OR

   If the red stop button is active, the Dialogic service is stopped or is in the process of starting. If the Dialogic service is stopped, click **Play** to start it.

3. Ensure the Dialogic service starts.
4. Select **Start > Programs > Avaya HMS V2 > HMS400v2** to start the HMS 400.

Starting the Web configuration module in the HMS 400 application

Start Web Configuration from the HMS 400 application to configure options for your system.

Prerequisites:

- Do not change the server name (hms400v2).
- Do not use the browser Back or Forward buttons to navigate pages. For security purposes, caching is disabled and errors can occur if you use the Back and Forward buttons.

1. In the HMS 400 application, click **Web Config**.
2. On the **HMS 400** window, in the **User Type** list, select **Admin User**.
3. In the **User ID** box, type the user ID.
   The default is SuperAdmin.
4. In the **Password** box, type the password.
   The default is abc123. Ensure that you immediately change this password.
5. Click **Login**.
6. If a Security Alert window appears, click **Yes** to proceed.

Shutting down the multi-server system

If you shut down a multi-server configuration, you must follow a specific order of steps to shut down properly. The HMS 400 on each client server stops automatically whenever the network connection is lost. The server automatically reboots when the connection is back up (after 10 seconds).

1. Shut down all client systems.
2. Shut down the main system.

Starting the multi-server system

If you start a multi-server configuration, you must follow a specific order of steps to start up properly. It can take up to five minutes for all services to start.

1. Start the main system.
2. Start the client systems.