



Avaya MultiSite Administration

Release 2.1

Configuration

555-233-137
Issue 6
July 2004

**Copyright 2004, Avaya Inc.
All Rights Reserved**

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the following Web site: <http://www.avaya.com/support>.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: <http://www.avaya.com/support>. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: <http://www.avaya.com/support>.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: <http://www.part68.org> by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Européenne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: <http://www.avaya.com/support>.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: <http://www.avaya.com/support>.

Contents

Preface	7
• Purpose	7
• Prerequisites	7
• Intended Audience	7
• Conventions Used in This Book	7
• Additional Resources	8
• Tell Us What You Think!	8
• How to Get This Book (and Others) on the Web	8
• How to Order More Copies of This Book	9
1 Resources and Notices	11
• Getting Help with the Installation	11
• Avaya Technology and Consulting (ATAC)	11
• Avaya Remote Network Integration Services (RNIS)	11
• Avaya Technical Service Organization (TSO)	12
• Avaya Network Management Software Systems Support Group (NMSSS)	12
• Avaya Contact Information	12
• Third-Party Resources	13
• System Security Notices	14
Network Security	14
Toll Fraud Security	14
Avaya Disclaimer	14
Toll Fraud Intervention	14
2 Overview	15
• Client Requirements	15
• Configuration Checklist	16
3 Setting Up MultiSite Administration	17
• Starting MultiSite Administration	17
• Setting Up the MultiSite Administration Server	18
• Assigning Messaging Systems	18
• Changing the Administrative Password	19

Contents

- Adding Users 19
- Starting the Queue 21
- Initializing Voice Systems 21
- Adding a Voice System 22
- Adding a Messaging System 23

Glossary and Abbreviations 25

Index 27

Preface

Purpose

This book explains how to configure Avaya MultiSite Administration (MultiSite Administration) and how to troubleshoot it.

Prerequisites

Installing and setting up MultiSite Administration requires familiarity with network administration, knowledge of the Red Hat implementation of the Linux operating system, and proficiency with Linux administration. This knowledge is not taught in this book but is essential for a successful installation.

For this reason, we highly recommend that workstation or network administrators take the primary role in installation.

Intended Audience

We wrote this book for workstation or network administrators.

Conventions Used in This Book

In this book, we use the following typographical conventions:

- We use bold type for emphasis and for any information that you should type; for example: **save translation**.
- We use Courier font for any information that the computer screen displays; for example: `login`.
- We use arrows to indicate options that you should select on cascading menus; for example: “Select File>Open” means choose the “Open” option from the “File” menu.

Additional Resources

You may find the following additional resources helpful.

For help using MultiSite Administration, access the MultiSite Administration online help. It explains how to perform basic administration tasks. To access the online help, start the MultiSite Administration client and choose **Help>Help Topics**.

For help with complex administration tasks, see the *Administrator's Guide for Avaya Communication Manager Software*, which explains system features and interactions in detail. You can access this document from the Integrated Management home page.

Tell Us What You Think!

Let us know how this book measured up to your expectations. Your opinions are crucial to helping us meet your needs! You can send us your comments by mail, fax, or e-mail, as follows:

Mail: Avaya, Inc.
MultiSite Administration Documentation Team
Room 3C-313
307 Middletown Lincroft Rd.
Lincroft, NJ 07738-1526
USA

Fax: MultiSite Administration Documentation Team
+ 1 732 852-2469

E-mail: document@avaya.com

How to Get This Book (and Others) on the Web

You can view or download the latest version of this book from the Avaya, Inc. web site. You must have access to the Internet, an Internet browser, and Adobe Acrobat Reader (version 5.0 or later) with Search. Adobe Acrobat Reader is available from <http://www.adobe.com>.

To view or download the latest version of the Avaya Integrated Management documentation:

- 1 Access <http://www.avaya.com/support>.
- 2 Click **Product Documentation**.
- 3 Click **System and Network Management**.
- 4 Locate the heading "Avaya Integrated Management," and click the link corresponding to the software release.
- 5 Locate the title of the book, and click the link corresponding to the book.

How to Order More Copies of This Book

To order paper copies of this book, call or write us and request the following publication:

Order: Document Number:555-233-137

Issue: Issue 6

Date: July 2004

Call: Avaya Publications Center

Voice: 1 800 457 1235

Fax: 1 800 457 1764

If you are calling from somewhere that cannot access US 1-800 numbers, then call:

Voice: + 1 207 866 6701

Fax: + 1 207 626 7269

Write: Globalware Solutions

200 Ward Hill Avenue

Haverhill, MA 01835
USA

Preface

How to Order More Copies of This Book

1 Resources and Notices

Avaya provides our customers with a variety of planning, consulting, and technical services. The sections below briefly describe the resources and services that are available.

Client executives are your primary contact to obtain information and explore options to meet your specific business needs.

Getting Help with the Installation

If you are located within the United States and you want help installing or setting up MultiSite Administration, call your Avaya representative.

If you are located outside the United States, call your Avaya representative or distributor. Call at least 4 weeks before the date on which you want to install MultiSite Administration.

Avaya Technology and Consulting (ATAC)

ATAC works with client teams to develop detailed solutions for connectivity to Avaya media servers running Communication Manager software. The ATAC also designs network configurations to support MultiSite Administration.

Avaya Remote Network Integration Services (RNIS)

For this product, RNIS offers customers the following services:

- Verify platform readiness
- Remotely install MultiSite Administration
- Configure the network management server for each voice system to be managed by MultiSite Administration
- Verify customer acceptance

Avaya Technical Service Organization (TSO)

The TSO provides support for MultiSite Administration to client teams, field technicians, and customers. The TSO will bill customers for support on a time and materials basis if the following conditions exist:

- Customers do not have a current maintenance agreement
- Customers do not procure and install the required systems and software as defined in the Avaya Integrated Management Services Support Plan
- Customers request support that is outside the purchase agreement

The TSO does not support hardware or software that customers purchase from third-party vendors.

Avaya Network Management Software Systems Support Group (NMSSS)

The Network Management Software Systems Support (NMSSS) group in Tampa Bay answers customer calls about applications in Avaya Integrated Management. NMSSS will either answer your questions directly or connect you with an associate who can answer questions about your application.

Avaya Contact Information

You may find the following contact information helpful at various times during the process of installing and setting up this product. This information was accurate at the time this book went to press. We update this information with each new release of MultiSite Administration.

Customers can access only the resources in [Table 1](#) (not [Table 2](#)). To view Avaya web sites, Avaya recommends that you use Internet Explorer.

Table 1: Customer-Accessible Resources

Resource	Contact Information
Avaya Support Centre	http://www.avaya.com/support
Network Management Software Systems Support group	1-800-237-0016.
Avaya Technical Services Organization (TSO)	For calls about Avaya Site Administration: 1-800-242-2121 extension 15312.
Remote Network Integration Services (RNIS)	http://www1.avaya.com/enterprise/brochures/svc1369.pdf
Toll Fraud Intervention	1-800-643-2353 prompt 1.

Table 2: Avaya Internal Resources

Resource	Contact Information
Avaya Enterprise Management Support	http://aem-support.dr.avaya.com/
Avaya Technology and Consulting Team (ATAC)	Phone: 1-888-297-4700 Main site (requires a password): http://forum.avaya.com
Remote Network Integration Services (RNIS)	http://associate2.avaya.com/sales_market/products/data-implementation-services/
Integrated Management Services Support Plan	http://associate2.avaya.com/solution/support_plans/Enterprise
AIM002 Form	http://associate2.avaya.com/sales_market/products/data-implementation-services/ Then click “Avaya Integrated Management Configuration Request Form #2.”

Third-Party Resources

The table below lists contact information for third-party vendors.

Table 3: Vendor web sites

Vendor	Web Sites
Microsoft	Main site: http://www.microsoft.com
Red Hat Linux	Main site: http://www.redhat.com

System Security Notices

Customers are solely responsible for the security of their system, network, and access to hardware and software. The sections below define the precautions that all customers should take to maintain the security of their systems.

Network Security

MultiSite Administration uses the standard security features on the Red Hat Linux.

Avaya strongly recommends that customers use passwords to prohibit access to their systems and to routinely change those passwords to maintain security.



SECURITY ALERT:

Customers should always change passwords immediately after external vendors have completed installation, maintenance, troubleshooting, or other tasks on their system.

Toll Fraud Security

Although MultiSite Administration is generally not at risk for toll fraud, customers are solely responsible for the security of their entire telecommunications system.

Toll Fraud is the unauthorized use of a company's telecommunications system by unauthorized parties. Unauthorized parties are persons other than the company's employees, agents, subcontractors, or persons working on behalf of the company. Toll fraud can result in substantial additional charges for the company's telecommunications services.

The company's system manager is responsible for the security of the company's system, which includes programming and configuring the equipment to prevent unauthorized use.

Avaya Disclaimer

Avaya does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunications services or facilities accessed through or connected to it. Avaya will not be responsible for any charges that result from such unauthorized use.

Toll Fraud Intervention

If customers suspect that they are a victims of toll fraud and need technical assistance, they should refer to the phone number listed for [Toll Fraud Intervention](#) on page 12.

2 Overview

MultiSite Administration is a client-server based application that enables you to administer Avaya media servers running Communication Manager software. MultiSite Administration offers these powerful features:

- enables multiple administrators to administer the same (or separate) Avaya media servers at the same time, remotely;
- offers graphical station and system administration screens;
- offers easy-to-use wizards for basic administration tasks;
- lets you cut through (using terminal emulation) to administer other telephony devices.

Client Requirements

MultiSite Administration client workstations should meet the following requirements:

Parameter	Requirement
Operating system	Windows XP Professional, Windows 2000, or Windows 2003
Other software	Internet Explorer 6.0 and Java Runtime Environment 1.4.2 (provided)
Processor	600 MHz
RAM	256 MB
Available Disk Space	Minimum: 100 MB on the drive that contains the Windows System folder (normally but not always the C: drive) Maximum: Up to 1GB (if this computer is running all Integrated Management client applications)
CD-ROM	Optional
Network Connectivity	TCP/IP
IP Addresses	Static or dynamic (DNS preferred)
Display	SVGA

Configuration Checklist

1 [Setting Up MultiSite Administration](#) on page 17

2 **Test the Installation.**

Test that a MultiSite Administration client can connect to each voice system. Test that clients can (or cannot) access the parts of MultiSite Administration that you specified when setting user permissions.

3 Setting Up MultiSite Administration

To set up MultiSite Administration, you will complete the following basic activities, which are described in more detail in this chapter:

- 1 [Starting MultiSite Administration](#) on page 17
- 2 [Setting Up the MultiSite Administration Server](#) on page 18
- 3 [Assigning Messaging Systems](#) on page 18
- 4 [Changing the Administrative Password](#) on page 19
- 5 [Adding Users](#) on page 19
- 6 [Starting the Queue](#) on page 21
- 7 [Initializing Voice Systems](#) on page 21

NOTE:

If you want to add a voice system or messaging system, you must use Integrated Management Database (IMD). To add a voice system, see [Adding a Voice System](#) on page 22. To add a messaging system, see [Adding a Messaging System](#) on page 23.

Starting MultiSite Administration

- 1 Go to the Launch Products page, and click **Avaya MultiSite Administration**.
- 2 At the Login dialog box, enter your Login ID, your password, and click **Login**.

The first time you start MultiSite Administration, enter the administrative Login ID **admin** and the default password.

If you upgraded from Avaya MultiSite Administration 2.0, enter your Login ID and password. The upgrade is now complete.

Setting Up the MultiSite Administration Server

To set up the MultiSite Administration server, complete the following steps:

- 1 From the main screen, click the **MSA Manager** tab, if it is not already displayed.
- 2 Click **MSA Server Configuration**.
The Welcome dialog box appears.
- 3 Click **Next**.
- 4 (Optional) Complete the fields in this dialog box.
- 5 Click **Next**.
- 6 Specify whether you want to initialize voice systems manually or automatically.
If you want MultiSite Administration to perform an initialization automatically as soon as it receives notification from the Integrated Management database (IMD) of new data for a voice system, select the **Automatic Initialization** option button.
If you want to initialize the voice system manually, select the **Manual Initialization** option button. If you select this option button, you must use Task Scheduler or System Resources in MultiSite Administration to initialize the voice system.
- 7 (Optional) Specify the number of minutes after which inactive MultiSite Administration users should automatically be disconnected from the server.
- 8 Click **Next**.
MultiSite Administration displays the Summary dialog box.
- 9 If the information presented is accurate, click **Finish**.
If it is not accurate, click **Back** to correct the error.

Assigning Messaging Systems

By default, each messaging system is assigned automatically to the AUDIX node that has a matching IP address. If an AUDIX node does not have an IP address, you can assign a messaging system to that AUDIX node by performing the following steps.

NOTE:

A messaging system must first be administered via Integrated Management Database (IMD). See [Adding a Messaging System](#) on page 23.

To assign a messaging system:

- 1 From the main screen, click the **MSA Manager** tab, if it is not already displayed.
- 2 Click **Messaging System Configuration**.
MultiSite Administration displays the Audix Nodes in MSA screen.
- 3 For a messaging system where no IP address is listed, click **Assign**.
The Assign Messaging System dialog box appears.
- 4 From the drop-down list box, select the voice system you want to associate with this messaging system.

- 5 Repeat Steps 3 and 4 for any other messaging systems you want to assign.
- 6 When finished, click **Done**.

Changing the Administrative Password

So that anyone reading this manual cannot log in to your copy of MultiSite Administration as an administrator, it is highly advisable to change the administrative password very shortly after logging into MultiSite Administration for the first time.

To change the administrative password, complete the following steps:

- 1 Click **MSA User Configuration**.
The MSA User Configuration screen appears. The MSA Users tab displays all the user IDs for the MultiSite Administration server.
- 2 Select the Login ID **admin** and click **Update User**.
MultiSite Administration displays the Update User dialog box.
- 3 Click **Change** next to the Password label.
MultiSite Administration displays the Change Password dialog box.
- 4 In the Enter New Password box, enter the new password. Remember to note the new password and save it in a secure location.
- 5 In the Reenter Password box, enter the password again, and then click **Change**.
A message box appears.
- 6 Click **OK**.

Adding Users

You can create and assign a custom privileges profile to users. With this custom privileges profile, you can restrict users from accessing certain objects within the MultiSite Administration System Manager. For each object in the System Manager, you can select whether the user has no access, read-only access, change access, or full access. See the MultiSite Administration online help for more information on creating a custom privileges profile.

To add users, complete the following steps:

- 1 Click **MSA User Configuration**.
The MSA User Configuration screen appears.
- 2 Click the **MSA Users** tab.
The MSA Users tab displays all the user IDs for the MultiSite Administration server.
- 3 Click **Add User**.
The Add User dialog box appears.
- 4 Enter the user's MSA ID, MSA password, name, company name, title, and telephone number (the required fields).

- 5** (Optional) Complete the non-required fields.
- 6** Click **Add**.

A message box appears.
- 7** Click **OK**.

The user account you just added appears in the MSA User Configuration screen.
- 8** Click the **Users on Systems** tab.
- 9** Click **Add User**.

The Add User dialog box appears.
- 10** From the User ID drop-down list box, select the user you just added.
- 11** From the list box on the right, select the voice system(s) that you want this user to be able to access using MultiSite Administration. Shift-click to select multiple contiguous voice systems.
- 12** In the User Roles area, perform the following steps:
 - a** Place a check mark in the System Manager check box if you want the user to be able to access objects in the System Manager.
 - b** Select the option button for the type of System Manager privileges you want this user to have on the selected voice system(s).

If you select **Full Privileges**, this user will have full permission for all the System Manager objects.

If you select **Custom Privileges**, this user will have the permissions you specified in the custom privileges profile you created via the Configure System Manager Custom Privileges tab.
 - c** Place a check mark in each check box corresponding to the MultiSite Administration Manager you want this user to access (for example, Station Manager, Report Manager, and Data Manager).
- 13** In the Additional Privileges area, place a check mark in each check box corresponding to the action you want this user to be able to perform on the selected voice system(s).
- 14** When finished, click **Add**.

A message box appears.
- 15** Click **OK**.
- 16** Repeat Steps 2 through 15 for each user you want to add.
- 17** When finished, click **Done**.

Starting the Queue

You must start the queue before you can use MultiSite Administration to access or make changes to that voice system.

NOTE:

The queue will be started already if the voice system is set to “Active” in Integrated Management Database (IMD).

To manually start the queue, complete the following steps:

- 1 From the main screen, click the **MSA Manager** tab, if it is not already displayed.
- 2 Click **System Resources**.
- 3 Click **Start Queue**.
- 4 Click **OK**.

Initializing Voice Systems

You must initialize each voice system that you want to use with MultiSite Administration before you use MultiSite Administration to access or make changes to that system.

NOTE:

The voice system may be in the process of being initialized if the voice system was just added to IMD and set to “Active.” You can check the initialization status by clicking the **MSA Manager** tab and selecting **System Status** from the **View** menu.

To manually initialize a voice system in MultiSite Administration, complete the following steps:

- 1 From the main screen, click the **MSA Manager** tab, if it is not already displayed.
- 2 Click **System Resources**.
- 3 Click **Initialize System**.
A dialog box appears.
- 4 Click **OK**.

Adding a Voice System

If you want to add a voice system, you must log into Integrated Management Database (IMD) and perform the following steps:

- 1** In the Integrated Management Database Administrator window, click **Elements** in the navigation panel.
The Elements page appears.
- 2** Click **New Element**.
The Add Element page appears.
- 3** In the Element Name box, enter the name of the element.
- 4** From the Element Type box, select **Voice System**.
- 5** In the Group box, enter the group for the voice system.
- 6** In the Product Id box, enter the product ID for the voice system.
- 7** In the Note box, enter any notes you want for the voice system. This box is a “note pad” in which you can enter up to 255 characters.
- 8** From the Location box, select the location for the voice system.
- 9** From the Platform Type box, select the type of voice system.
- 10** In the Functional Location box, enter the location.
- 11** Select the **Active** check box if you want the new voice system element to be activated when you are finished adding it. (This check box is enabled by default.)
- 12** Perform the following steps to use MSA with this voice system:
 - a** From the MSA box, select the MSA system you want to use.
 - b** In the Login box, enter the SAT login for the voice system.
 - c** In the Password box, enter the password for the SAT login.
 - d** In the Re-enter Password box, re-enter the password for the SAT login.
 - e** In the IP Address box, enter the SAT IP address.
 - f** In the Telnet/SSH Port box, enter the SAT port number.
 - g** If the system uses SSH authentication:
 - 1** Select the **Use SSH** check box.
 - 2** In the SSH Key box, enter the RSA SSH key. (See the Avaya Communication Manager documentation for information on how to determine the RSA SSH key.)

NOTE:

If you do not enter the RSA SSH key, the key will not be validated, but SSH will be used for encryption only.

- h** If the system uses ASG:
 - 1** In the ASG Key box, enter the ASG key.
 - 2** In the Re-enter ASG Key box, re-enter the ASG key.

- i** In the Total Channels box, enter the total number of channels.
 - j** In the Dedicated Channels box, enter the number of dedicated channels.
- 13** When finished, click **Add**.

Adding a Messaging System

If you want to add a messaging system, you must log into Integrated Management Database (IMD) and perform the following steps:

- 1** Click **Elements** in the navigation panel.
The Elements page appears.
- 2** Click **New Element**.
The Add Element page appears.
- 3** In the Element Name box, enter the name of the element.
- 4** From the Element Type box, select **Other**.
- 5** In the Group box, enter the group for the system.
- 6** In the Product Id box, enter the product ID for the system.
- 7** In the Note box, enter any notes you want for the system. This box is a “note pad” in which you can enter up to 255 characters.
- 8** From the Location box, select the location for the system.
- 9** From the Platform Type box, select the type of system.
- 10** In the Functional Location box, enter the location.
- 11** Select the **Active** check box if you want the new element to be activated when you are finished adding it. (This check box is enabled by default.)
- 12** Perform the following steps to use MSA with this messaging system:
 - a** From the MSA box, select the MSA system you want to use.
 - b** In the Login box, enter the login for the messaging system.
 - c** In the Password box, enter the password for the messaging system login.
 - d** In the Re-enter Password box, re-enter the password for the messaging system login.
 - e** In the IP Address box, enter the IP address of the messaging system.
 - f** In the Telnet Port box, enter the port number of the messaging system.
 - g** In the System Password box, enter the password for the system. The system password is not usually required.
 - h** In the Re-enter Password box, re-enter the password for the system.
 - i** From the Queue Name box, select the voice system queue for the messaging system. MSA uses a voice system queue to control connectivity to a messaging system. While the MSA server makes a separate telnet connection to the messaging system, the voice system queue you specify here will control the starting and stopping of this connection.
 - j** In the Total Channels box, enter the total number of channels.
 - k** In the Dedicated Channels box, enter the number of dedicated channels.

- 1** If you are adding a Modular Messaging system (that is, you selected **Modular Messaging** in the Platform Type box), enter the Base DN of the system in the Base DN box. The default setting is “ou=people, dc=Avaya.” Change this setting only if you are sure it is a different value.

- 13** When finished, click **Add**.

Glossary and Abbreviations

A

ATAC

See [Avaya Technology and Consulting \(ATAC\)](#) on page 11.

C

Communication Manager software

The call processing software that runs on Avaya media servers (such as Avaya S8500 Media Server). Formerly known as MultiVantage software and DEFINITY software.

M

media server

Any of the products that run Communication Manager software. Formerly known as DEFINITY system, DEFINITY ECS, switch, PBX, MultiVantage Solution, or voice system.

N

Network Management Server

This is the Windows box that you can install Windows-based Integrated Management applications on.

Network Management System

A system that lets you monitor the health and status of devices on your data network. For example, HP OpenView.

R

RNIS

See [Avaya Remote Network Integration Services \(RNIS\)](#) on page 11.

S

System Management Server

This is the Linux box that you install MultiSite Administration on.

T

TSO

See [Avaya Technical Service Organization \(TSO\)](#) on page 12.

Index

A

ATAC, [13](#)
Avaya Support Center web site, [12](#)
Avaya Technology and Consulting (ATAC), [11](#)

C

configuration
 getting help, [11](#)
contact information
 for Avaya, [12](#)
 third party, [13](#)

E

Enterprise Management Support, [13](#)

H

help with configuration, [11](#)

I

installation
 checklist, [16](#)
 overview, [16](#)
 services, [11](#)

M

Microsoft web site, [13](#)

N

network
 security, [14](#)

P

passwords, changing, [14](#)

R

Red Hat web site, [13](#)
RNIS, [11](#)

S

security
 Avaya disclaimer, [14](#)
 for networks, [14](#)
 network, [14](#)
 notices, [14](#)
 toll fraud, [14](#)
 toll fraud intervention, [14](#)
Services Support Plan, [13](#)
Services Support Plan, Integrated Management, [13](#)

T

Technical Service Organization, [12](#)
Technical Services Organization, [12](#)
toll fraud, [14](#)
 Avaya disclaimer, [14](#)
 intervention, [14](#)
Toll Fraud Intervention phone number, [12](#)
TSO, [12](#)
 phone numbers, [12](#)
typographical conventions, [7](#)

W

web sites
 Avaya, [12](#)
 third-party, [13](#)

