Avaya Integrated Management Release 3.1 MultiSite Administration Configuration

Contents

Contents

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

Product Documentation

The latest version of Avaya Integrated Management product documentation, including this book, is available from the Avaya Support Web Site. To view or download these books from the Web, you must have access to the Internet, an Internet browser, and Adobe Acrobat Reader, version 5.0 or later. Adobe Acrobat Reader is provided on the Avaya Integrated Management CDs and is also available from http://www.adobe.com. See How to Access Books on the Web on page 7 for instructions on how to view or download these books.

How to Access Books on the Web

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

1. Access http://www.avaya.com/support.

2. Click **Find Documentation and Downloads by Product Name**.

3. Click the letter **I** in the alphabet listing.

4. Locate the Integrated Management product or offer name and click the corresponding link.

5. Click **View All Documents** to display a list of available books for that product or offer.

Chapter 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)

Avaya Technology and Consulting (ATAC) works with client teams to develop detailed solutions for connectivity to Avaya Communication Manager solutions. The ATAC also designs network configurations.

Communications, Solutions, and Integration (CSI) Group of Software Services

Avaya Communications, Solutions, and Integration (CSI) Group of Software Services offers customers the following services:

- Platform readiness verification
- Remote implementation and installation
- Network management server configuration
- Customer acceptance verification
- Custom on-site services

The CSI Group consists of the following two teams:

- **Converged Solutions Implementation Engineering**

  The Converged Solutions Implementation Engineering (CSIE) team implements multi-site media gateway (G350/G650/G700) deployment projects for both voice and data design. The overall direction of the CSIE team is to bring the correct methodology to these complex deployments that span various regions and to provide continuity to the overall project from the voice and data implementation standpoint.

- **Data Network Implementation Engineering (formerly RNIS)**

  The Data Network Implementation Engineering team implements and/or upgrades existing or new data networks. This team analyzes the customer's network design requirements and performance expectations, and then creates the hardware and software installation specification used to implement data devices including Cajun, VPN, Wireless LAN, Secure Gateways, Extreme, and multi-vendor data equipment.

The CSI Group provides support on a contract basis. You can purchase various implementation offers from the CSI Group in Tampa, Florida. See Table 1: Customer-Accessible Resources on page 12 for contact information.

Avaya Technical Service Organization (TSO)

The Avaya Technical Service Organization (TSO) provides support to the Avaya Integrated Management 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 provide remote access.

- Customers do not have a current maintenance agreement.

- Customers do not procure and install the required systems and software as defined in the 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 Avaya Network Management Software Systems Support Group (NMSSS) in Tampa Bay, Florida answers customer calls about products in Avaya Integrated Management. NMSSS will either answer your questions directly or connect you with an associate who can answer questions about the products.

Customized Management Solutions for Avaya Integrated Management

The Integrated Management Product Team understands customer's needs and is focused on customer satisfaction. See Table 1: Customer-Accessible Resources on page 12 for contact information. The Product Team will assist customers with Avaya Integrated Management projects and will provide:

- **Project Management** — An Integrated Management project person will work with the customer to access configuration and customization requirements for any or all applications within each Avaya Integrated Management offer. If custom work is required, the evaluation will include a proposed statement of work and price. Note that this offer is *not* intended to provide installation for customers that choose to implement Integrated Management applications using Avaya Services or third-party implementation services.

- **Training** — Basic training can be performed remotely using an interactive medium to display the applications and a conference bridge for audio. On-site training can be customized to meet the customer's needs. Customized training will focus on application functionality that is relevant to the customer and provide focused knowledge transfer to facilitate application-specific training.

Avaya Contact Information

Table 1 and Table 2 provide contact information that you may use if you need assistance during the process of installing and setting up Avaya Integrated Management. To access the links in Table 2, you must be able to access the Avaya intranet.

Table 1: Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://www.avaya.com/support
Network Management Software Systems Support (NMSSS)	+1 800 237-0016
Communications, Solutions, and Integration (CSI) Group of Software Services	+1 800 730-9108, prompt 3
Integrated Management Product Team	Send email to: AIMtraining@avaya.com
Toll Fraud Intervention	+1 800 643-2353, prompt 1

Table 2: Avaya Internal Resources

Resource	Contact Information
Avaya System Management Support	http://aem-support.dr.avaya.com
Avaya Technology and Consulting (ATAC)	+1 888 297-4700, prompt 2,6 http://forum.avaya.com (requires a password)
Communications, Solutions, and Integration (CSI) Group of Software Services	http://associate2.avaya.com/sales_market/products/data-implementation-services/
Integrated Management Services Support Plan	http://associate2.avaya.com/solution/support_plans/#Enterprise

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 in .

Chapter 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.

What's New in this Release

Avaya MultiSite Administration Release 3.1 introduces the following enhancements:

- Support for the following media servers:
  - S8400 server
  - S8720 server
- Support for the following media modules and boards:
  - G250-DCP media module
  - G250-DS1 media module
  - MM716 analog 24-port (line only) media module
- Support for the following set types:
  - 4601+ IP Telephone
  - 4602+ IP Telephone
  - CTI
- Support for the Customized Label feature for the following set types:
  - 2410 Digital Telephone
  - 2420 Digital Telephone
  - 4610 IP Telephone
  - 4620 IP Telephone
  - 4621 IP Telephone

- 4622 IP Telephone

- 4625 IP Telephone

● Support for the Display Feature Button Labels report

● Support for the Maximum Time Agent in ACWS before Logout (secs) field in the Agent Login ID object

● Support for 996 Class of Restrictions (CORs) on systems running Avaya Communication Manager Release 3.1

● Support for 1 to 1999 vectors on systems running Avaya Communication Manager Release 3.1

● New default delimiter character for the Station Import wizard

● Integration with Modular Messaging

- The ability to connect securely to a Modular Messaging system using LDAP over SSL

- The ability to pass the station "Name2" value to the Modular Messaging system when you add or change mailbox information

  "Name2" is a secondary, alternative name field for certain Avaya Communication Manager objects that allows the input of a wide variety of Unicode, UTF-8 encoded character sets. "Name2" is also referred to as a "native language name" field.

● The ability to change your MSA password from the MSA Login dialog box

● Enhanced support for vector objects

- The ability to view, edit, and duplicate vectors

- The ability to set a system lock for vectors

- The ability to control access to the vector object using a System Manager Custom Privilege Definition

- New Quick Command support for changing a vector and duplicating a vector

● The ability to display all System Manager object data in a table format

● The merging of the Data Manager into the Report Manager

  The "Database format using field/record delimiters" option on the List Reports dialog box is now in the Report Manager.

● The ability to create a system lock on ports so you can reserve the ports for future use

  You will use the Non-Station Object Locks tab in the System Locks window under MSA Manager to lock ports.

● The ability to generate a report that lists all non-station object system locks

  This report lists all non-station locks and the object type with an associated qualifier. You can generate this report from a button on the Non-Station Object Locks tab in the System Locks window under MSA Manager.

- A recent command history for Quick Commands

  The Quick Command field now provides a drop-down list of the 25 most recently used commands. You may select entries from this list. Avaya MultiSite Administration will maintain a history for each user. This history will persist across login sessions. The drop-down list will also provide a static list of common commands.

- The ability to view all options for commands entered in the Quick Command field

- Support for file filters for file "Save as" operations

  Avaya MultiSite Administration supports .rpt and *.* file filters when you perform a "save as" operation.

- Consolidated Logs

  Avaya MultiSite Administration will store all past events (such as scheduled jobs, cut-through procedures, run now tasks, and service startups/shutdowns) in a single log that you can easily filter on a particular object (such as date or voice system). You can then view more detail about the selected event.

- Port validation before a task is submitted

  When you add a new station or change a set type, Avaya MultiSite Administration will verify whether the port type is valid for that set type. This validation will occur when you submit the task as a process now, a process in the background, or a scheduled task.

- The Cut-Through window now appears in the foreground

- The ability to copy the entire contents of abbreviated dial personal lists when you duplicate stations

Client Requirements

MultiSite Administration client workstations should meet the following requirements:

Parameter	Requirement
Operating system	Windows XP Professional, Windows 2000 with Service Pack 2 or later, or Windows 2003
Other software	Internet Explorer 6.0 with Service Pack 1 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

Follow these steps:

1. **Set up MultiSite Administration.** See **Setting Up MultiSite Administration** .

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.

Chapter 3: Setting Up MultiSite Administration

This guide assumes that the Avaya MultiSite Administration software has been installed and that you have already added users, voice systems, and messaging systems using Avaya Integrated Management Database (IMD).

Note:
> The procedures for adding users, voice systems, and messaging systems using Avaya Integrated Management Database are provided in this guide. To add a user, see Add a User on page 31. To add a voice system, see Add a Voice System on page 28. To add a messaging system, see Add a Messaging System on page 29.

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

1. Start MultiSite Administration on page 20.
2. Set Up the MultiSite Administration Server on page 20.
3. Assign Messaging Systems on page 21.
4. Create Custom Privilege Profiles on page 22
5. Assign Users to Systems on page 23.
6. Start the Queue on page 24.
7. Initialize Voice Systems on page 25.
8. Change the Administrative Password on page 27.

Start MultiSite Administration

To start MultiSite Administration:

1. Using Microsoft Internet Explorer, go to the Launch Products page, and click **Avaya MultiSite Administration.**

   The Login dialog box appears.

2. Enter your login ID and your password.

   Note:

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

3. Click **Login.**

   If more than one voice system is registered with MultiSite Administration in IMD, the Select Voice System dialog box appears. Select the voice system you want to administer, and click **OK**.

   Note:

   > If you upgraded from Avaya MultiSite Administration 3.0, the upgrade is now complete.

Set 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 Avaya MultiSite Administration Server Configuration Wizard 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 be disconnected automatically from the server.

8. Click **Next**.

   A summary of the MultiSite Administration server configuration appears.

9. If the information presented is accurate, click **Finish**.

   If the information is not accurate, click **Back** to correct the error.

Assign 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 Add a Messaging System on page 29.

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**.

   The Audix Nodes in MSA screen appears.

3. Select a messaging system where no IP address is listed, and then 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. Click **OK**.

6. Repeat Steps 3 through 5 for any other messaging systems you want to assign.

7. When finished, click **Done**.

Create Custom Privilege Profiles

This procedure describes how to create custom privilege profile that you can assign to users. With a 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.

To create a custom privileges profile, complete the following steps:

1. From the main screen, click the **MSA Manager** tab, if it is not already displayed.

2. Click **MSA User Configuration.**

   The MSA User Configuration screen appears.

3. Click the **Define System Manager Custom Privilege** tab.

   The Define System Manager Custom Privilege tab displays all of the existing custom privilege profiles for the MultiSite Administration server.

4. Click **Add**.

   The Add Custom Privilege dialog box appears.

5. In the Custom privilege name box, enter the name for this custom privilege profile.

6. For each feature, select the option button for the type of permission you want this profile to provide.

7. If you want this profile to allow users to use quick commands, click the **Use Quick Command** check box.

8. If you want this profile to allow users to have full access to reports via the List/Display button, click the **Full access to reports via List/Display Button** check box.

9. If you want this profile to allow users to access the jobs of other users in the Translation Editor, click the **Access other user's jobs in Translation Editor** check box.

10. In the Notes box, enter any notes you want about this custom privileges profile. For example, you may want to enter a brief description of this profile.

11. When finished, click **Done**.

    Then new custom privileges profile appears.

12. Repeat Steps 4 through 11 for each custom profile you want to add.

13. When finished, click **Done**.

Assign Users to Systems

This procedure describes how to assign users to voice systems that are registered in MultiSite Administration.

Note:

Before you can assign a user to a voice system, you must first add that user for MultiSite Administration in IMD. See Add a User on page 31. Once you add MultiSite Administration users to IMD, you must then assign those users to the voice systems you want them to access.

To assign a user to a voice system, complete the following steps:

1. From the main screen, click the **MSA Manager** tab, if it is not already displayed.

2. Click **MSA User Configuration.**

   The MSA User Configuration screen appears.

3. Click the **Users on Systems** tab.

   The Users on Systems tab displays all the user IDs for the MultiSite Administration server.

4. Select the ID of the user to whom you want to assign access to a voice system.

5. Click **Assign User**.

   The Assign User dialog box appears.

6. 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.

   To select multiple contiguous voice systems, click on the first voice system, and then press and hold the SHIFT key, and click on the last voice system.

   To select multiple non-contiguous voice system, press and hold the CTRL key, and click on the appropriate voice systems.

7. Perform one of the following steps:

   ● If the Super User check box is selected, the user has super user privileges. These super user privileges for MultiSite Administration were assigned when the user was added to IMD. You can assign or remove super user privileges from IMD only. Go to Step 10.

   ● If the Super User check box is not selected, go to Step 8.

8. In the User Roles area, perform the following steps:

   a. If you want the user to be able to access objects in the System Manager:

      1. Place a check mark in the System Manager check box.

2. From the drop-down list box, select 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 a custom privileges profile, this user will have the permissions you specified in that custom privileges profile. You can create custom privileges profiles via the Define System Manager Custom Privilege tab in the MSA User Configuration screen. See <u>Create Custom Privilege Profiles</u> on page 22.

   b. 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).

9. 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).

10. When finished, click **Assign**.

    A message box appears.

11. Click **OK**.

12. Repeat Steps <u>4</u> through <u>11</u> for each user you want to add.

13. When finished, click **Done**.

Start 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**.

Initialize 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.

You can initialize a voice system manually or schedule it to be initialized at a specific time via the Task Scheduler. See the Avaya MultiSite Administration online help for information on how to use the Task Scheduler.

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**.

Change Your Password

You can change your password for Avaya MultiSite Administration in two ways:

- from the Avaya Integrated Management Database Login dialog box

- from the Avaya MultiSite Administration Login dialog box

To change your Avaya MultiSite Administration password from the Avaya MultiSite Administration Login dialog box, complete the following steps:

1. Using Microsoft Internet Explorer, go to the Launch Products page, and click **Avaya MultiSite Administration.**

   The Login dialog box appears.

2. Click **Change Password**.

   The Change Password page appears.

3. In the User ID box, enter your MSA login.

4. In the Current Password box, enter the current password for your login.

5. In the New Password box, enter the new password you want to use for your login.

6. In the Re-Type New Password box, re-enter the new password you want to use for your login.

7. Click **Change Password**.

8. Click **Cancel** to return to the Logon page.

To change your Avaya MultiSite Administration password from the Avaya Integrated Management Database Login dialog box, complete the following steps:

1. Using Microsoft Internet Explorer 6.0 or later, go to the IP address or hostname of the Linux server to view the Avaya Integrated Management Launch Products page.

2. On the System Management tab, click **Avaya Integrated Management Database**.

   The Logon window appears.

3. Click **Change Password**.

   The Change Password page appears.

4. In the User ID box, enter your MSA login.

5. In the Current Password box, enter the current password for your login.

6. In the New Password box, enter the new password you want to use for your login.

7. In the Re-Type New Password box, re-enter the new password you want to use for your login.

8. Click **Change Password**.

9. Click **Cancel** to return to the Logon page.

IMD Tasks

You must use IMD to perform the following tasks:

- Change the password for the MultiSite Administration logins
- Add a voice system
- Add a messaging system
- Add a user to MultiSite Administration

Change 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.

If you want to change the administrative password, you must log into Integrated Management Database (IMD) and perform the following steps:

1. In the Integrated Management Database Administrator window, click **Users** in the navigation panel.

    The Users page appears.

2. Click **Edit** for the admin login.

    The Edit User page appears.

3. In the Password box, enter the new password. Remember to note the new password and save it in a secure location.

4. In the Re-type Password box, enter the password again.

5. Click **Update.**

6. Repeat Steps 2 through 5 if you want to change the password for any other users.

Add 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 Sold To Number box, enter the location.

6. In the Product Id box, enter the product ID for the voice system.

   Note:

   > The product ID is required for voice systems that are managed by a Proxy Agent application.

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. 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.)

11. From the MSA box, select the MSA system you want to use.

12. In the Login box, enter the SAT login for the voice system.

13. In the Password box, enter the password for the SAT login.

14. In the Re-enter Password box, re-enter the password for the SAT login.

15. In the IP Address box, enter the SAT IP address.

16. In the Alternate IP Address box, enter the alternate SAT IP address.

17. If the system uses SSH authentication:

    a. Select the **Use SSH** check box.

    b. 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.

   c. In the Alternate SSH Key box, enter the RSA SSH key for the alternate IP address.

18. In the Telnet/SSH Port box, enter the SAT port number.

19. If the system uses ASG:

   a. In the ASG Key box, enter the ASG key.

   b. In the Re-enter ASG Key box, re-enter the ASG key.

20. In the Total Channels box, enter the total number of channels.

21. In the Dedicated Channels box, enter the number of dedicated channels.

22. When finished, click **Add**.

Add 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 Sold To Number box, enter the location.

6. In the Product Id box, enter the product ID for the system.

   Note:

   The product ID is required for voice systems that are managed by a Proxy Agent application.

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. 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.)

11. From the MSA box, select the MSA system you want to use.

12. In the Login box, enter the login for the messaging system.

13. In the Password box, enter the password for the messaging system login.

14. In the Re-enter Password box, re-enter the password for the messaging system login.

15. In the IP Address box, enter the IP address of the messaging system.

16. If the system uses SSH authentication:

    a. Select the **Use SSH** check box.

    b. In the SSH Key box, enter the RSA SSH key. (See the messaging system 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.

    c. In the Alternate SSH Key box, enter the RSA SSH key for the alternate IP address.

17. In the Telnet/SSH/LDAP Port box, enter the TCP port number that should be used to connect to the messaging system.

18. In the System Password box, enter the password for the voice system. The system password is not usually required.

19. In the Re-enter System Password box, re-enter the password for the system.

20. 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.

21. In the Total Channels box, enter the total number of channels.

22. In the Dedicated Channels box, enter the number of dedicated channels.

23. 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.

24. Click **Add**.

Add a User

To add a user for MultiSite Administration, you must log into Integrated Management Database (IMD) and perform the following steps:

1. In the Integrated Management Database Administrator window, click **Users** in the navigation panel.

   The Users page appears.

2. Click **New User**.

   The Add User page appears.

3. In the Login box, enter the login for the user.

4. In the User Name box, enter the name of the user.

5. In the Email Address box, enter the email address of the user.

6. In the Phone Number box, enter the telephone number of the user.

7. In the Password box, enter the password for the user's login.

8. In the Re-type Password box, re-enter the password for the user's login.

9. If you want to prevent this user from logging in, select the **Login Disabled** check box.

10. If you want to specify the number of attempts a user can make to log into the system before being "locked out," enter that number in the Failed Attempts box.

11. Select the **MSA** check box.

12. If you want this user to have super user privileges on MultiSite Administration, select the **MSA Super User** check box.

13. Click **Add.**

14. Repeat Steps 2 through 13 for any other users you want to add.

Glossary and Abbreviations

A

ATAC   See [Avaya Technology and Consulting (ATAC)](#) on page 9.

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 on which you can install Windows-based Integrated Management applications.

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

S

System Management Server   This is the Linux box on which you install MultiSite Administration.

T

TSO   See [Avaya Technical Service Organization (TSO)](#) on page 10.

TSO

Index

Index