Avaya Integrated Management Release 4.0

MultiSite Administration Configuration

555-233-137
Issue 10
May 2007

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the website, simply go to http://www.avaya.com/support **and search for the document number in the search box.**

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

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

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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://www.avaya.com/support

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.

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 Reader. Adobe Reader 7.0 is provided on the Avaya Integrated Management CD and is also available from http://www.adobe.com. See How to Access Books on the Web on page 6 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) 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 10 for contact information.

Avaya Global Services Delivery (GSD)

Avaya Global Services Delivery (GSD) provides support to the Avaya Integrated Management client teams, field technicians, and customers. The GSD 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 GSD does not support hardware or software that customers purchase from third-party vendors.

Avaya Global Technical Services

Avaya Global Technical Services answers customer calls about products in Avaya Integrated Management. They 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 10 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
Avaya Global Technical Services	+1 800 242-2121 x15921
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 Customer-Accessible Resources on page 10.

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 4.0 introduces the following enhancements:

- Support for the following new media servers:
  - S8300C server
  - S8500C server
  - S8720XL server
- Disable FTP and telnet services by default for secure connectivity. In Avaya Communication Manager Release 4.0, FTP and telnet are disabled by default.
- Improvements to Avaya Communication Manager logging. When you perform a task on a voice system running Avaya Communication Manager Release 4.0, Avaya MultiSite Administration will automatically change the secondary user name in the syslog to the client-side IP address and the MultiSite Administration user ID. This enhancement will enable you to identify the tasks performed by each MultiSite Administration user.
- Support for 13-digit dial plan in Avaya Communication Manager Release 4.0. You can now enter up to 13 digits and punctuation in extensions on voice systems running Avaya Communication Manager Release 4.0. You can enter dashes (**-**) and periods (**.**) in extensions. Since dashes are now allowed in extensions, you must enter a colon (**:**) to indicate a range of extensions.
- Support for call vectoring enhancements in Avaya Communication Manager Release 4.0. You can now enter up to 99 vector steps (and comments for vector steps) on voice systems running Avaya Communication Manager Release 4.0.

- Support for AES encryption. The default encryption algorithm has changed from blowfish to AES. The communication between Avaya MultiSite Administration and Avaya Communication Manager is now encrypted using the AES algorithm.

Client Requirements

MultiSite Administration client workstations should meet the following requirements:

Parameter	Requirement
Operating system	Microsoft Windows XP Professional with Service Pack 2, Microsoft Windows 2000 Professional with Service Pack 4, Microsoft Windows 2000 Server with Service Pack 4, Microsoft Windows 2003 Standard Edition Server with Service Pack 1, or Microsoft Windows 2003 Enterprise Edition Server with Service Pack 1
Other software	Internet Explorer 6.0 with Service Pack 1 and Java Runtime Environment 1.5.0 (provided)
Processor	1.5 GHz
RAM	512 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 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.

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)
- assigned which users have access to which voice systems in 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 28. To add a voice system, see Add a Voice System on page 25. To add a messaging system, see Add a Messaging System on page 26.

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

1. Start MultiSite Administration on page 18.
2. Set Up the MultiSite Administration Server on page 18.
3. Assign Messaging Systems on page 19.
4. Create Custom Privilege Profiles on page 20
5. Assign Custom Privilege Profiles to Users on page 21.
6. Start the Queue on page 22.
7. Initialize Voice Systems on page 23.

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 3.1, 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 steps in this section.

Before you can set up a messaging system in MSA, you must be assigned access to that messaging system in Integrated Management Database (IMD). You can only access those messaging systems to which you were assigned in Integrated Management Database (IMD).

Note:

A messaging system must first be administered via Integrated Management Database (IMD). See Add a Messaging System on page 26.

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 profiles that you can assign to users. With a custom privilege profile, you can specify which tasks users can perform and restrict users from accessing certain objects within the MultiSite Administration System Manager. You can also specify the range of stations and range of ports that a user can access. 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 privilege 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. By default, MultiSite Administration provides the DEFAULT custom privilege profile. The DEFAULT custom privilege profile has the System Manager role selected, but provides no access to any of the objects. You can modify the DEFAULT custom privilege profile to suit the needs of your organization.

   Note:

   The DEFAULT custom privilege profile is assigned automatically to non-super users when those users are added to a new voice system.
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. Click the check box for each MultiSite Administration manager (for example, Station Manager and Report Manager) or task you want to assign to this profile.
7. If you want to assign permissions for certain features in MultiSite Administration System Manager:
   a. Click the **System Manager** check box.
   b. Click **System Manager**.

      The Add Custom Privilege dialog box appears.
   c. For each feature, select the option button for the type of permission you want this profile to provide.
   d. If you want to specify a range of stations that this profile can administer, enter the range of stations in the Station box in the Define Partitions area. For example, if you want this profile to administer station 1000 to 2000, you would enter **1000-2000**.

If you want this profile to administer stations 1000, 1001, and 2100 to 2150, you would enter **1000, 1001, 2100-2150**.

e. If you want to specify a range of gateways that this profile can administer:

1. In the Gateway box in the Define Partition area, enter the range of gateways. For example, if you want this profile to administer gateways 1 to 6, you would enter **1-6**. If you want this profile to administer stations 1, 2, 4, 5, and 6, you would enter **1, 2, 4-6**.
2. If this profile will need access to port networks, make sure the **Port Network** check box is enabled.
3. If this profile will need access to sites, make sure the **Sites** check box is enabled.

f. When finished, click **Done**.

8. 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.
9. When finished, click **Done**.

   Then new custom privileges profile appears.
10. Repeat Steps 4 through 9 for each custom profile you want to add.
11. When finished, click **Done**.

Assign Custom Privilege Profiles to Users

This procedure describes how to assign custom privilege profiles to users. You must have an MSA Super User login or an MSA User Admin Only login to be able to assign custom privilege profiles.

Note:

Before you can assign a profile to a user, you must first add that user for MultiSite Administration in IMD. See Add a User on page 28. By default, the DEFAULT custom privilege profile is assigned automatically to all new MultiSite Administration users who do not have super-user privileges.

To assign a custom privilege profile to a user:

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. From the System Name box, select the appropriate voice system.

5. Select the ID of the user to whom you want to assign a custom privilege profile.
6. Click **Update User**.

   The Update User dialog box appears.
7. From the list box on the right, select the voice system for which this custom privilege profile will be used.
8. From the drop-down list box, select the custom privilege profile you want to assign to this user for the selected voice system.
9. When finished, click **Save**.

   A message box appears.
10. Click **OK**.
11. Repeat Steps 5 through 10 for each user to whom you want to assign a custom privilege profile.
12. 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). If the limit for the maximum number of voice systems is reached already, the queue for the new voice system will not start (either manually or automatically). Before you can administer this new voice system, you must remove one of the other voice systems. For example, suppose you kept the maximum number of voice systems in the bob.ini file at the default of 300, and you have added 300 voice systems to the MultiSite Administration server. You then add another voice system, which gives you a total of 301 voice systems. You will be unable to start the queue for this new voice system because you exceeded the maximum number of voice systems.

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,” and the MultiSite Administration server has automatic initialization set. 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 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:

- Add a voice system
- Add a messaging system
- Add a user to MultiSite Administration

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.
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. If you have an Avaya S87xx voice system that is configured for high availability, enter the alternate SAT IP address in the Alternate IP Address box.

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.) If you have an Avaya S87xx voice system that is configured for high availability, enter the RSA SSH key for the server you specified in the IP Address box.

    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. If you have an Avaya S87xx voice system that is configured for high availability, in the Alternate SSH Key box enter the RSA SSH key for the server you specified in the Alternate IP Address box.
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. In the Allowed Users box, select which IMD users will have access to this element.

    To select multiple users, press and hold the CTRL key, and then click on the appropriate users.
23. When finished, click **Add**.
24. Repeat Steps 2 through 23 to add another voice system.

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 on adjuncts is required by Avaya Fault and Performance Manager.

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. In the Allowed Users box, select which IMD users will have access to this element.

    To select multiple users, press and hold the CTRL key, and then click on the appropriate users.
25. When finished, click **Add**.
26. Repeat Steps 2 through 25 to add another system.

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.

   Note:

   The Failed Attempts box displays the current number of failed login attempts this user has made. When a user is locked out, you can reset this value to **0**.
10. Perform one of the following steps to specify the user level setting:
    - If you want this user to have super user privileges on MultiSite Administration, select the **MSA Super User** check box.
    - If you want this user to have administration privileges on MultiSite Administration, select the **MSA** check box.
    - If you want this user to only administer users on MultiSite Administration, select the **MSA User Admin Only** check box.

11. From the Allowed Elements box, select the element(s) this user will be able to access.

    To select multiple elements, press and hold the CTRL key, and then click on the appropriate elements.

12. Click **Add.**
13. Repeat Steps 2 through 12 for any other users you want to add.

Glossary and Abbreviations

A

ATAC — See Avaya Technology and Consulting (ATAC) on page 7.

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.

S

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

Index