Avaya Integrated Management Release 3.0

Implementation Guidelines

555-233-163
Issue 10
June 2005

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.

Disclaimer

Avaya 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.

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, or IEC 60950-1, 1st 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, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

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 used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

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, EN55022:1998, and AS/NZS 3548.

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

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

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.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect 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

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) 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).

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

Purpose

This book provides the customer with an overall strategy for implementation of Avaya Integrated Management applications. It describes the roles and responsibilities of the customer and Avaya Services in the implementation of the applications. This book addresses:

- Pre-implementation requirements of the network management computing platforms
- Pre-implementation installation of the operating system on the computing platforms
- Post-implementation verification checklist

The Avaya Data Network Implementation Engineering team (formerly RNIS) provides implementation services for Avaya Integrated Management applications. See Support Resources on page 8 for more information about planning, consulting, and technical services that are available from Avaya. Avaya Authorized Business Partners may also provide implementation services. Details of implementation services offered by business partners must be obtained from the business partners and are not discussed in book.

Intended Audience

This book is intended for customers to describe the roles and responsibilities of the customer and Avaya Services in the implementation of Avaya Integrated Management applications.

Conventions Used in This Book

The following typographical conventions are used:

- **Bold** type is used to indicate information that you type, buttons in a window, and the **Enter** key on the keyboard. It is also used for emphasis.
- Courier font is used for any information that the computer screen displays.
- Arrows indicate options that you select from cascading menus; for example, “Select File > Open” means choose the “Open” option from the “File” menu.

Support Resources

Avaya provides a variety of planning, consulting, and technical services. The following sections describe the resources and services that are available.

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 11 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 11 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

Additional Resources

All Avaya Integrated Management Release 3.0 documents are listed in the following tables:

- Table 3: Overview Documents on page 12
- Table 4: Installation and Upgrade Guides on page 12.
- Table 5: Configuration Guides on page 13.
- Table 6: Help Systems on page 13.
- Table 7: Network Management Applications and Device Managers User Guides on page 14.

Table 3: Overview Documents

Document Title	Document Number
Avaya Integrated Management Release 3.0, Implementation Guidelines	555-233-163
Avaya Integrated Management Release 3.0, Roadmap	14-300615

Table 4: Installation and Upgrade Guides

Document Title	Document Number
Avaya Integrated Management Release 3.0, Enterprise Network Management Installation and Upgrade	14-300444
Avaya Integrated Management Release 3.0, Network Management for Solaris Installation and Upgrade	14-300445
Avaya Integrated Management Release 3.0, Monitoring Management Installation and Upgrade	14-300446
Avaya Integrated Management Release 3.0, System Management Installation and Upgrade	14-300448
Avaya Integrated Management Release 3.0, Standard Management Installation and Upgrade	14-300479
Avaya Integrated Management Release 3.0, Administration Tools Installation and Upgrade	14-300480

Table 5: Configuration Guides

Document Title	Document Number
Avaya Integrated Management Release 3.0, MultiSite Administration Configuration	555-233-137
Avaya Integrated Management Release 3.0, Fault and Performance Manager Configuration	555-233-138
Avaya Integrated Management Release 3.0, Proxy Agent Configuration	555-233-139
Avaya Integrated Management Release 3.0, Configuring Red Hat Linux	555-233-152
Avaya Integrated Management Release 3.0, VoIP Monitoring Manager Configuration	555-233-510
Avaya Integrated Management Release 3.0, Integrated Management Database Configuration	14-300039
Avaya Integrated Management Release 3.0, Enterprise Network Management Configuration	14-300210
Avaya Integrated Management Release 3.0, Provisioning and Installation Manager Configuration	14-300286

Table 6: Help Systems

Printable PDF Help System	Document Number
Avaya Integrated Management Release 3.0, MultiSite Administration Reference	14-300607
Avaya Integrated Management Release 3.0, Fault and Performance Manager Reference	14-300608
Avaya Integrated Management Release 3.0, Proxy Agent Reference	14-300609
Avaya Integrated Management Release 3.0, Site Administration Reference	14-300610
Avaya Integrated Management Release 3.0, Integrated Management Database Reference	14-300611
Avaya Integrated Management Release 3.0, Provisioning and Installation Manager Reference	14-300612
	1 of 2

Table 6: Help Systems (continued)

Printable PDF Help System	Document Number
Avaya Integrated Management Release 3.0, Voice Announcement Manager Reference	14-300613
Avaya Integrated Management Release 3.0, VoIP Monitoring Manager Reference	14-300614
	2 of 2

Table 7: Network Management Applications and Device Managers User Guides

Document Title	Document Number
Avaya Integrated Management Release 3.0, C360 Manager User Guide	14-300164
Avaya C360 SMON User Guide[a]	14-300207
Avaya C460 Manager User Guide[a]	14-300224
Avaya C460 SMON User Guide[a]	14-300225
Avaya Integrated Management Release 3.0, G350 Manager User Guide	14-300166
Avaya P130 Manager User Guide[a]	14-300218
Avaya P130 SMON User Guide[a]	14-300219
Avaya Integrated Management Release 3.0, P330 Manager User Guide	14-300221
Avaya P330 SMON User Guide[a]	14-300222
Avaya P330 Load Balancing Manager[a]	14-300223
Avaya P580/P882 Manager User Guide[a]	14-300165
Avaya P580/P882 SMON User Guide[a]	14-300214
Avaya Integrated Management Release 3.0, W310 Manager User Guide	14-300163
Avaya W310 SMON User Guide[a]	14-300208
Avaya Wireless AP Manager User Guide[a]	14-300212
Avaya Wireless AP MON User Guide[a]	14-300213
Avaya VLAN Manager[a]	14-300211
	1 of 2

Table 7: Network Management Applications and Device Managers User Guides

Document Title	Document Number
Avaya Network Management User Administration User Guide[a]	14-300217
Avaya Network Configuration Manager User Guide[a]	14-300167
Avaya Integrated Management Release 3.0, Software Update Manager User Guide	14-300168
Avaya Integrated Management Release 3.0, Network Management Console User Guide	14-300169
Avaya Integrated Management Release 3.0, SMON Manager User Guide	14-300209
Avaya Integrated Management Release 3.0, Address Manager User Guide	14-300170
Avaya Integrated Management Release 3.0, QoS Manager User Guide	14-300216
Avaya Integrated Management Release 3.0, Secure Access Administration User Guide	14-300537
Avaya Integrated Management Release 3.0, Reference Guide	14-300531
	2 of 2

a. This document was not updated for Release 3.0.

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 Enterprise Network Management CDs and is also available from http://www.adobe.com. See How to Access Books on the Web for instructions on how to view or download these books.

How to Access Books on the Web

To view or download books from the Avaya Support Web Site, follow these steps:

1. Access http://www.avaya.com/support.
2. Click **Find Documentation and Downloads by Product Name**.
3. Click the appropriate letter in the alphabet listing.
4. Locate the product name and click the corresponding link.
5. Select the software release from the drop-down menu and click the arrow to display a list of available books for that product.

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! Send us your comments by mail, fax, or e-mail as follows:

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

Fax: Avaya Integrated Management Documentation Team
+ 1 732 852-2469

E-mail: document@avaya.com
Subject: Avaya Integrated Management Documentation Team

Chapter 1: Application Environment

Overview

Avaya Integrated Management provides a standards-based infrastructure for an open application program interface and integrated network management in a converged, multi-vendor environment. Avaya Integrated Management is comprised of a set of applications that provide systems administration, network management, and business integration in a converged voice and data environment. While many of the individual management products have been available on an individual basis, Avaya Integrated Management integrates voice-centric management products and data-centric management products and provides a common user interface.

Voice and Messaging System Compatibility

The Avaya Integrated Management products manage devices using IP. All adjunct devices and non-IP enabled devices may relay alarms to the Avaya Proxy Agent using dial-up (serial) alarming. Avaya Integrated Management is compatible with voice systems, messaging systems, and call management systems as shown in Table 8.

Table 8: Avaya Integrated Management System Compatibility

System	Release
DEFINITY R, DEFINITY SI, DEFINITY CSI, DEFINITY ONE, IP600	Release 9, 10 or MultiVantage (System must be configured for IP administration)
S8100 Media Server	MultiVantage
S8300 Media Server	MultiVantage and later or Communication Manager
S8500	Communication Manager
S8700 Media Server	MultiVantage and later or Communication Manager
S8710 Media Server	MultiVantage and later or Communication Manager
	1 of 2

Table 8: Avaya Integrated Management System Compatibility (continued)

System	Release
INTUITY AUDIX	Release 5.1 and later
INTUITY AUDIX LX	Release IA 1.0-17.X
DEFINITY AUDIX	Release 3.1 or later
Modular Messaging	Release 1.1
Multipoint Control Unit (MCU)	Release 7.2
S8300 INTUITY AUDIX	MultiVantage
IP600/DEFINITY ONE AUDIX	Release 9 or later
INTUITY Interchange	5.1 or later
Call Management System (CMS)	Release 8.3 or later
CONVERSANT	7.0 or later
	2 of 2

Operating Environment

The Avaya Integrated Management products are listed in Table 9. The table identifies the servers on which the products are installed and identifies the products that are installed on the Windows Client PC. The minimum hardware and software requirements of the Windows, Linux, and Solaris servers and the Windows Client PC are described in Table 10, Table 11, Table 12, and Table 13.

Table 9: Operating Environment for Avaya Integrated Management Applications

Product Name	Linux Server	Solaris Server	Windows Server	Windows Client PC
Avaya MultiSite Administration	✓			
Avaya Fault and Performance Manager	✓			
Network Management System Integration (NMSI)		✓	✓	
				1 of 2

Table 9: Operating Environment for Avaya Integrated Management Applications (continued)

Product Name	Linux Server	Solaris Server	Windows Server	Windows Client PC
Avaya Proxy Agent	✓			
Avaya Integrated Management Database	✓			
Avaya Network Management Console with System View			✓	
Avaya Network Configuration Manager		✓	✓	
Avaya Software Update Manager		✓	✓	
Avaya SMON™ Manager		✓	✓	
Avaya Address Manager		✓	✓	
Avaya VLAN Manager		✓	✓	
Avaya QoS Manager		✓	✓	
Avaya Secure Access Administration		✓	✓	
Avaya VoIP Monitoring Manager			✓	✓
Avaya Device Managers		✓	✓	
Avaya Provisioning and Installation Manager			✓	
Avaya Site Administration				✓
Avaya Voice Announcement Manager				✓

2 of 2

Hardware and Software Components

The customer is responsible to provide the hardware platform, operating system, software, and network used to host the Avaya Integrated Management applications. The minimum hardware and software requirements needed to support the Avaya Integrated Management applications are provided in the following tables:

- Table 10: Windows Server Requirements on page 21.
- Table 11: Red Hat Enterprise Linux Server Requirements on page 23.
- Table 12: Solaris Server Requirements on page 23.
- Table 13: Windows Client PC Requirements on page 24.

In addition to the specifications provided in these tables, Avaya recommends the use of servers that are certified for use with Red Hat Enterprise Linux as listed on Red Hat's Hardware Compatibility List, which can be found at: http://hardware.redhat.com/hcl/.

Use of a computing platform that is below the recommended configurations may result in poor performance.

Server Requirements for VoIP Monitoring Manager

In addition to ensuring the Windows server meets the requirements provided in Table 10: Windows Server Requirements on page 21, it is recommended that you use the VoIP Monitoring Manager Configurator prior to installing VoIP Monitoring Manager. See Appendix C: Sample VMM Configurator on page 49 to view a copy of the VoIP Monitoring Manager Configurator completed with sample data.

Completing the VoIP Monitoring Manager Configurator will help you determine whether the MSDE database that comes with the VoIP Monitoring Manager application will meet the customer's needs. It will also help you determine whether a single VoIP Monitoring Manager server will be sufficient. For example, in cases where there are more than 4000 simultaneous RTCP streams (2000 concurrent calls) coming into the server, multiple VoIP Monitoring Manager servers should be considered.

You can also use the VoIP Monitoring Manager Configurator to help determine how to configure VoIP Monitoring Manager parameters once the application is installed. For example, you can adjust numbers in the VoIP Monitoring Manager Configurator, such as RTCP Reporting Intervals and History Days to get an idea of how to configure them to achieve the desired goal.

Using the VoIP Monitoring Manager Configurator will require that you gather information from the customer about their volume of IP calls.

To access the VoIP Monitoring Manager Configurator, go to: http://www.auslabs.avaya.com/ClearCaseView/VMM/StandardsAndGuidelinesSet/General/VMMConfigurator.xls. To access this link, you must be able to access the Avaya intranet.

Table 10: Windows Server Requirements

Component	Required	Comments
Operating System [1]	Microsoft Windows 2003 Standard Edition server, Microsoft Windows 2003 Enterprise Edition server, or Microsoft Windows 2000 server; VoIP Monitoring Manager can also be installed on Windows XP Professional	Only English operating systems are supported.
Processor	2.8 GHz Pentium® 4	A maximum of two processors is supported.
Hard Drive	40 GB	
Memory	1.5 GB RAM	
Network Connectivity	TCP/IP 100 Mbit Network Card	Only one network interface is supported. Dual network interface cards (NICs) or additional software network interfaces, such as a VPN interface, are not supported.
Modem	56K modem for remote access	
CD-ROM Drive		Required for installation.
Monitor	SVGA 1024 X 768 display	
SNMP Agent	The Simple Network Management Protocol (SNMP) Agent is the Windows Service that runs on your computer. SNMP must be installed prior to installing VoIP Monitoring Manager.	
Extra Software	Anti-virus software pcAnywhere	Required for Avaya support. pcAnywhere is required for remote access by Avaya Services.
Web Browser	Internet Explorer 6.0	Required for access to the Integrated Management Launch Page and web-based clients.

1 of 2

Table 10: Windows Server Requirements (continued)

Component	Required	Comments
Integration with HP OpenView Network Node Manager	HP OpenView 7.0.1 or HP OpenView 7.5. HP OpenView 7.5 requires a patch.	HP OpenView is not included on any Avaya Integrated Management CD. Customers must purchase, install, and maintain HP OpenView. While Avaya services support Integrated Management when installed over HP OpenView, they do not support the HP OpenView product itself.
Port (for Avaya VoIP Monitoring Manager)	The Avaya VoIP Monitoring Manager client and server software communicate using Java Remote Method Invocation (RMI), and use port 1099 on the machine on which the server is running. If this port is unavailable, the server will attempt to use the following ports: 49177, 51173, or 63006. Although it is unlikely that all of these ports will be in use on a single machine, ensure that at least one of these ports is available.	
		2 of 2

1. The operating system can be on a high-end desktop machine. A server class hardware platform is not required.

Table 11: Red Hat Enterprise Linux Server Requirements

Component	Required	Comments
Operating System	Red Hat Enterprise Linux ES R3.0 or Red Hat Enterprise Linux AS R3.0	For upgrade installations, Red Hat Enterprise Linux ES R2.1 is supported. Only English operating systems are supported.
Processor	2.8 GHz Pentium® 4	A maximum of two processors is supported.
Hard drive	40 GB	
Memory	1.5 GB RAM	
Network Connectivity	TCP/IP 100 Mbit Network Card	
Modem	56K external modem connected to COM1 for remote access	
Web Browser	Not required	Linux web client is **not** supported.
CD-ROM Drive		Required for installation.
Monitor	SVGA 1024 X 768 display	

Table 12: Solaris Server Requirements

Component	Required	Comments
Operating System	Solaris 9 or 10	Only English operating systems are supported.
Processor	SPARC architecture 500MHz	
Hard Drive	40 GB	
Memory	1.5 GB RAM	
Network Connectivity	TCP/IP 100 Mbit Network Card	
Modem	56K external modem connected to COM1 for remote access	
Web Browser	Not required	Solaris web client is not supported.

1 of 2

Table 12: Solaris Server Requirements (continued)

Component	Required	Comments
CD-ROM Drive		Required for installation.
Monitor	SVGA 1024 X 768 display	
Integration with HP OpenView Network Node Manager	HP OpenView 7.0.1 or HP OpenView 7.5. HP OpenView 7.5 requires a patch.	HP OpenView is not included on any Avaya Integrated Management CD. Customers must purchase, install, and maintain HP OpenView. While Avaya services support Integrated Management when installed over HP OpenView, they do not support the HP OpenView product itself.
		2 of 2

Table 13: Windows Client PC Requirements

Component	Required	Comments
Operating system	Microsoft Windows 2000, Windows XP Professional, or Windows 2003	
Processor	600 MHz Pentium®	
Hard Drive	1 GB	Required to install all of the client components.
Memory	256 MB RAM	
Monitor	SVGA 1024 X 768 display	
Network Connectivity	TCP/IP 10/100 Network Card	
Modem	56K Modem	May be required for remote access to the client PC.
CD-ROM Drive		Required for installation.
Web Browser	Internet Explorer 6.0	Required to access the Integrated Management Launch Page and web-based clients.

Connectivity/Network Connections

Avaya Integrated Management requires a local (or wide) area network connection to all network devices and supporting databases. The customer is responsible for designing and implementing local (or wide) area network connections. The network connections must be in place and tested prior to Integrated Management implementation. Assistance with network setup is not part of an Avaya Integrated Management offer but may be performed by Avaya Services under a different offer.

Implementation requires the following network information:

- The IP address of each DEFINITY® system
- The IP address of each INTUITY® Audix system
- The IP address of each S8300/S8500/S8700/S8710 media server.
- The C-LAN port used for SAT access on each DEFINITY® system or S8500/S8700/S8710 media server.

Remote Access Hardware and Software

Table 10 and Table 11 provide the requirements for a modem and remote access software on Windows and Linux-based computing platforms. However, where multiple network management servers are present and connected via an IP network, only one network management server requires remote access capabilities. The remaining network management servers may be accessed through use of a Telnet session originating at the server with remote access. This arrangement is not dependent on the operating systems (Linux or Windows Server) of the network management servers. This topic is discussed in detail in Remote Connectivity on page 33.

Symmetric Multi-Processor (SMP) Support

Linux-based applications in Avaya Integrated Management require the latest kernel from Red Hat to run properly in a Symmetric Multi-Processor (SMP) environment.

Microsoft and Red Hat each provide a website where customers can download patches to the Windows and Linux operating systems, respectively. It is strongly recommended that customers keep their servers up-to-date, as patches correct software bugs and also contain security updates.

Chapter 2: Implementation Services

Product Packaging

There are six Avaya Integrated Management offers:

- Enterprise Network Management
- Network Management for Solaris
- Monitoring Management
- System Management
- Administration Tools
- Standard Management

For more information about the offers, see *Avaya Integrated Management Release 3.0, Roadmap*, document number 14-300615. Irrespective of product packaging, Avaya will provide implementation services for the following individual applications on the customer's computing platform:

- Avaya MultiSite Administration
- Avaya Proxy Agent
- Avaya Fault and Performance Manager
- Avaya SMON Manager
- Avaya VoIP Monitoring Manager (full version)
- Avaya Site Administration
- Avaya Voice Announcement Manager (Voice Announcement Board Administration)
- Avaya Provisioning and Installation Manager

Customer Implementation Options

Many of the Avaya Integrated Management applications are customer installable. Due to the complexity of application configuration, however, it is strongly recommended that customers seek professional implementation services from Avaya Services to implement any of the following applications:

- Avaya MultiSite Administration
- Avaya Proxy Agent
- Avaya Fault and Performance Manager

If a customer attempts a self-installation and requires assistance with the installation or configuration of an Avaya Integrated Management application, they should contact the Avaya Technical Services Organization (TSO). Note that charges may apply for TSO assistance with application installation or configuration. The Avaya TSO also provides warranty and maintenance services for an application after that application has been properly installed and configured. An application is considered properly installed when the implementation verification tasks defined in Implementation Verification on page 35 have been successfully completed.

Avaya TSO support is available at 1-800-242-2121, then follow the prompts for “Avaya Integrated Management”.

Overview of Avaya Implementation Services

Avaya implementation services are available for individual or small groups of applications included in Avaya Integrated Management. Due to installation and configuration complexities, it is strongly recommended that Avaya Services implement Avaya MultiSite Administration, Avaya Proxy Agent, and Avaya Fault and Performance Manager. The customer may choose to implement the remaining applications or have Avaya Services perform these implementations. Basic implementation services can be provided in the following ways:

- **Remote Implementation** — Data Network Implementation Engineers can perform basic implementation remotely using remote access technology (e.g., dial-up modem) to access the customer servers. The remote Data Network Implementation Engineer is in telephone contact with the designated customer representative as necessary during the implementation process. The customer representative assists with the implementation as follows:
  - Verifies server readiness (system is powered-on and the operating system is booted)
  - Verifies availability of remote connectivity to the customer servers and managed devices (e.g., voice systems)
  - Places product CDs into the server CD drive as directed by the remote engineer

Once these activities have been completed, the customer representative's assistance is completed. The remote Data Network Implementation Engineer completes the configuration and customization of the application software.

- **Onsite Installation** — For customers in the United States, onsite installation is available for an additional charge. When requested, a field technician is dispatched to the customer site to replace the customer representative. The field technician acts as the hands of the remote Data Network Implementation Engineer. The onsite field technician assists with the implementation as follows:
  - Verifies server readiness (system is powered-on and the operating system is booted)
  - Verifies availability of remote connectivity to the customer servers and managed devices (e.g., voice systems)
  - Places product CDs into the server CD drive as directed by the remote engineer

  Once these activities have been completed, the field technician leaves the customer site while the remote Data Network Implementation Engineer completes the configuration and customization of the application software.
- **Onsite Implementation** — Onsite Implementation is available as an add-on offer. The Data Network Implementation Engineer travels to the customer site to perform the implementation. Onsite Installation and Onsite Implementation should never be ordered together.

Basic Implementation

Basic implementation services include the following:

- Installation of an Avaya Integrated Management application on a customer-supplied server
- Configuration of the application to operate with one voice or messaging system (DEFINITY or INTUITY) or one Avaya P130/P330/P580/P880 device/stack as appropriate for the application
- Verification that the application operates correctly with that managed device

Basic implementation services do not include setup of customer server hardware or operating environment, or design/implementation of network connectivity.

For Avaya Integrated Management applications that manage voice systems, some parameters must be configured on the voice system for it to operate with the application. In particular, a login and password is required for all applications. An application-specific login is recommended to enable appropriate access rights and create an application-specific audit trail in the voice system log. In addition, some applications require configuration of the IP address of the network management server and alarm notification information into the voice system.

Note:

In all cases, Data Network Implementation Engineering services described in this document do not include administration of configuration parameters on any Avaya ECLIPS or DEFINITY voice systems.

The following additional services are available:

- **Configuration of Managed Devices Offer** — The customer can request Avaya Services to configure Avaya Integrated Management applications to work with additional managed devices.
- **Solution Evaluation Offer**— The customer can request a Data Network Implementation Engineer to work with them via telephone for a 4-hour block of time to assess configuration and customization requirements for any or all Avaya Integrated Management applications. This offer may be ordered in multiple units if more time is required. Where custom work is required, the evaluation results in a proposed statement of work and price.

Services Organizations Involved in Avaya Integrated Management Implementations

Avaya Communications, Solutions, and Integration (CSI) Group of Software Services provides implementation services for Avaya Integrated Management applications. The CSI Group consists of the following two teams:

- Converged Solutions Implementation Engineering
- Data Network Implementation Engineering (formerly RNIS)

For more information about the CSI Group, see Communications, Solutions, and Integration (CSI) Group of Software Services on page 8.

The Data Network Implementation Engineering team is composed of the following service groups:

- **Data Help Desk (DHD)** — The primary objective of the DHD is management and scheduling of Data Network Implementation Engineering resources. The DHD team receives and tracks all requests to engage Data Network Implementation Engineering support. Requests are reviewed for assignment feasibility, entered into an internal tracking system and assigned to an Implementation Engineer and a Case Implementation Coordinator (CIC) associate.
- **Case Implementation Coordinator (CIC)** — An internal administrative group that tracks Data Network Implementation Engineering service orders from receipt to completion. This group interfaces with all sales teams for service order accuracy, confirms or negotiates service delivery dates with customers, and provides status on service progress throughout the life cycle of an order. Where applicable, the CIC group will see that the necessary FSO/ISO resources have been scheduled for service projects. At the completion of service, the CIC group contacts the customer to gain acceptance of the work performed.

- **Data Network Implementation Engineer** — The Data Network Implementation Engineer receives the order documentation, including the Implementation Request Form (IRF) and Configuration Request Forms (CRFs) from the DHD team and creates the Installation Specification. The Implementation Engineer gathers additional information from the customer technical contact to add to the Installation Specification. The Installation Specification provides technical information to guide the implementation and is available to Avaya technical services teams that provide maintenance support for the applications. See Service Request Documentation on page 31 for more information about the IRF and CRFs.

Service Request Documentation

When implementation services for Avaya Integrated Management applications are ordered, the customer must work with your account team to complete an Implementation Request Form (IRF) and applicable Configuration Request Forms (CRFs). These forms provide information that the Data Network Implementation Engineer uses to configure the Avaya Integrated Management software to meet customer requirements.

Implementation Request Form

The Implementation Request Form (IRF) provides the Implementation Engineer with basic customer contact and site information, including:

- Order and contact information
- Product and services requested
- Application description
- General network information

Configuration Request Form

In addition to the IRF, a Configuration Request Form (CRF) must be completed for key Avaya Integrated Management applications to be installed. The CRF contains information that describes the customer requirements for the implementation of the specific application, for example:

- Information on each voice system or data device to be configured
- Filters for forwarding of alarms (for Avaya Fault and Performance Manager).

The Linux CRF must be submitted for implementation of one or more of the following Linux-based applications:

- Avaya Fault and Performance Manager
- Avaya Proxy Agent
- Avaya MultiSite Administration

The Windows CRF must be submitted for implementation of one or more of the following Windows-based applications:

- Avaya VoIP Monitoring Manager
- Avaya Network Management Console
- Avaya Provisioning and Installation Manager

Avaya and Customer Responsibilities

Table 14: Customer and Avaya Responsibilities on page 39 summarizes the responsibilities of the customer and the Avaya Data Network Implementation Engineering team for implementation of Avaya Integrated Management applications.

Note:

All customer requirements must be completed prior to the scheduled start date of implementation. For a complete list of customer responsibilities, please contact the Data Help Desk.

For all Data Network Implementation Engineering service orders, the customer is responsible to:

- Identify a principal contact for this work
- Schedule a time with the Data Network Implementation Engineering for the implementation
- Complete and submit the Implementation Request Form (IRF) and Configuration Request Forms (CRFs)

For remote implementation, the customer must provide an onsite contact to assist during installation. For onsite installations or onsite implementations, the customer must provide Avaya personnel with access to appropriate facilities and computer systems.

Note:

If required documentation is not provided to the Implementation Engineer or dial-up connectivity has not been verified at least 5 business days prior to the scheduled implementation date, the implementation will be rescheduled to the next available date.

Specific Implementation Tasks

Implementation of Avaya Integrated Management applications includes the following tasks:

- Platform and Network Readiness
  - Remote connectivity
  - Computing platform
  - IP connectivity
- Installation and configuration of one or more of the Avaya Integrated Management applications on customer management servers
- Implementation Verification

The following sections describe these tasks in more detail.

Remote Connectivity

For remote implementations, the Data Network Implementation Engineer must have remote access to the customer's network management server(s). Avaya Services also requires remote access for ongoing maintenance support of installed Avaya Integrated Management applications. The customer is responsible for the installation, configuration, and testing of modems on the server(s) prior to implementation of Avaya Integrated Management applications. Remote access is typically provided by an analog modem connected directly to the server in conjunction with an analog phone line with a telephone number accessible on the public phone network. Testing must include:

- Establishing a dial-up connection and initiation of a pcAnywhere session on a Windows server, and
- Establishing a dial-up connection and initiation of a Telnet session from the Linux command prompt on a Linux server.

Where multiple network management servers are present and connected via an IP network, only one network management server requires remote access capabilities. The remaining network management servers may be accessed through use of a Telnet session originating at the server with remote access. This arrangement is not dependent on the operating systems (Linux or Windows Server) of the network management servers.

If a Linux server hosts remote access, a modem must be connected to serial port COM1 (ttyS0). While internal and USB modems can be configured to work with Red Hat Linux, Avaya recommends a US Robotics Sportster 56k external modem to provide reliable remote connectivity in support of remote implementation and maintenance services.

No additional software is required on Linux servers because the Red Hat Linux installation loads Virtual Network Computing (VNC) software. The Implementation Engineer uses a modem to establish a dial-up point-to-point-protocol (PPP) connection. Once the PPP session is established, they can use VNC to continue installation, configuration, and verification of the Avaya Integrated Management applications.

If a Windows server hosts remote access, it is the customer's responsibility to obtain and load Symantec's pcAnywhere remote control software (version 10.0 or higher). This enables the Implementation Engineer to accomplish remote implementation of Avaya Integrated Management applications, and it is also required for warranty and maintenance services provided by Avaya Services.

Note that Avaya Proxy Agent, running in a Linux environment, may receive alarms from adjunct units, such as messaging systems and integrated voice response systems, over a serial link. Dial-up serial alarming is also used for DEFINITY voice systems running R9.1 and R9.2 software. Additional analog modem(s) and phone line(s) are used to receive these alarms, as the modem on COM1 must be dedicated to implementation and maintenance. Typically, one modem is required to support alarm reception, while a second modem is required to support alarm forwarding. However, the number of required modems (and the possible need for a Serial I/O Board to provide additional serial ports) is dependent on the following:

- Number of managed nodes using serial alarming
- Whether the proxy server is providing alarm reception only or must perform alarm forwarding and filtering
- Whether the managed nodes are duplicated for redundancy or high-reliability.

As a result, the number of modems required to support serial alarming must be determined on a case-by-case basis by the Data Network Implementation Engineer.

Computing Platform

The customer is responsible for acquiring servers and loading the Windows server, Red Hat Enterprise Linux server, or Solaris server operating systems. It is important that the computing platform meet the minimum requirements specified in the following tables:

- Table 10: Windows Server Requirements on page 21
- Table 11: Red Hat Enterprise Linux Server Requirements on page 23
- Table 12: Solaris Server Requirements on page 23

Failure to meet these requirements may result in poor system performance. If desired, Avaya Services will install the Windows server, Red Hat Enterprise Linux server, or Solaris server operating systems for an additional charge.

When loading the Red Hat Enterprise Linux server operating system, it is important to note that the default settings are not appropriate for the Linux-based applications in Avaya Integrated Management. It is mandatory that the installation guidelines provided in Appendix B: Installation of Red Hat Linux on page 43 be closely followed. Deviation from these guidelines may result in failure of the Linux-based applications to operate on the server or the platform acceptance test to fail, thus delaying the completion of the implementation process.

After Red Hat Enterprise Linux server software has been installed and configured on the computing platform, it is important that the customer verify that a dial-up connection can be established by dialing into the server via a phone line connected to the modem on serial port COM1 (ttyS0). A successful connection is indicated by display of a Linux login prompt. Remote connectivity is required as a condition of warranty and post-warranty service. Where Avaya Services will provide remote implementation services, the customer must verify that a dial-up connection can be established prior to the scheduled date of implementation.

IP Connectivity

Network verification is performed by the Data Network Implementation Engineer prior to implementation of any server-based application in Avaya Integrated Management. This test is performed to ensure that the network management server(s) have IP connectivity to all devices to be managed, including voice systems, messaging systems, and data switches.

It is the customer’s responsibility to design and implement local and/or wide area networking such that each management server has IP connectivity to each device it will manage.

Application Installation and Configuration

Based on information on the customer’s Implementation Request Form (IRF) and Configuration Request Forms (CRFs) submitted with the order and direct communications with the customer technical contact, the Data Network Implementation Engineer will create an Installation Specification. This document provides technical information to guide the implementation and is available to Avaya technical services teams that provide maintenance support for the applications.

Implementation Verification

Once an application is installed and configured for operation with one or more managed devices, the Data Network Implementation Engineer performs an application-specific Acceptance Test to verify application implementation.

Avaya Fault and Performance Manager and Avaya Proxy Agent

Once Avaya Fault and Performance Manager and Avaya Proxy Agent have been installed and configured, the Data Network Implementation Engineer performs the following steps to verify proper operation with each managed voice and messaging system for which the applications were configured:

- Establish a connection between each voice or messaging system and Avaya Proxy Agent.
- Verify that each voice or messaging system can **send** alarms to the Avaya Proxy Agent.
- Verify that the Avaya Fault and Performance Manager server can **receive** alarms from each voice system.
- Verify that the Avaya Fault and Performance Manager server can retrieve **configuration data** from each voice system.
- Generate a test alarm for each managed node and verify that Avaya Fault and Performance Manager received the alarm.

In addition to verification of the application, the Data Network Implementation Engineer assists the customer in understanding basic operations of Avaya Fault and Performance Manager and Avaya Proxy Agent:

- Verify that the customer has changed the **root** and **g3maadm** logins for the Linux server platform.
- Verify that the customer can **start** and **stop** Avaya Proxy Agent.
- Verify that the customer can **display** the status screen to view the status and statistics of the Avaya Proxy Agent connection and the managed node.
- Verify that the customer can add/modify/delete managed devices from Avaya Proxy Agent via the change managed-nodes command.
- Verify that the customer can set/change voice system login information for Avaya Proxy Agent via the change managed-nodes command.

Avaya MultiSite Administration

Once Avaya MultiSite Administration has been installed and configured, the Data Network Implementation Engineer performs the following steps to verify proper operation with each managed voice system and each messaging system for which the application was configured:

- Verify successful client configuration by launching from **Start** menu and Avaya Integrated Management Launch Page.
- Change the default admin password and report this to the customer.
- Create at least one Avaya MultiSite Administration user for the customer in the Avaya Integrated Management Database application. Then, in Avaya MultiSite Administration, assign a voice system to that user.
- Verify the queue is running for each configured voice system and messaging system.

- Kick-off an initialization for each configured voice system (this can take some time, up to several hours).
- Add and then delete a station on each voice system.
- Add and then delete a voice mail subscriber for each messaging system.
- Ensure that a unique login for use by Avaya MultiSite Administration has been administered on each voice system. (This is necessary to ensure that the Avaya MultiSite Administration cache of system changes remains accurate.)
- Configure the Task Manager to run scheduled housekeeping tasks as recommended for each individual task and as directed by the customer.

Avaya SMON Manager

Verify successful installation by launching from **Start** menu and Avaya Integrated Management Launch Page.

Avaya VoIP Monitoring Manager

Once the Avaya VoIP Monitoring Manager has been installed, the Data Network Implementation Engineer assists the customer in performing the following steps to verify proper operation:

1. Make sure that the voice system is configured with the IP address of the management server hosting the VoIP Monitoring Manager Server.
   Start the VoIP Monitoring Manager server application. From the Windows server hosting the VoIP Monitoring Manager Server application, select **Start > Programs > Avaya > VoIP Monitoring Manager > Server**.
2. From the machine hosting the VoIP Monitoring Manager client, select **Start > Programs > Avaya > VoIP Monitoring Manager > Client** to start the VoIP Monitoring Manager client.
3. Start a call between two IP phones.
4. In the left-hand panel in the VoIP Monitoring Manager client, select the **Endpoint** tab, and then click the **Search** button to launch the Search dialog. Select the search option **Sessions active in the last 1 minute**. This is the default setting.
5. Click the **Search** button. The Search Results List updates with a list of Active Endpoints. At least two endpoints should appear in the list. It will also list the Endpoint type, IP address and phone number. Now, select the Endpoint from the list and click the **Report** button to view the QoS data for that Endpoint.
6. Hang up the call and wait one minute.
7. In the left-hand panel of the VoIP Monitoring Manager client, select the **Endpoint** tab, and then click the **Search** button to launch the Search dialog. Select the search option **Sessions active in the last 1 minute**.
8. Click the **Search** button and confirm that there are no active endpoints.
9. Select the **Sessions active from** radio button.

10. Click the top date drop-down arrow to access the calendar and time for the starting period of your Search. Select hours, minutes, seconds and AM/PM, then select the day. Click outside the calendar window to close the calendar. Click the bottom date drop-down arrow to access the calendar and time for the ending period of the query as described above. The top and bottom date fields display the selected date.
11. Click the **Search** button. The Search Results List updates with a list of Historical Endpoints. It also lists the endpoint type, IP address, and phone number. To view the QoS data, select the Endpoint and click the **Report** button.

Avaya Site Administration

Perform the following tasks:

- Verify successful installation by launching from **Start** menu and Avaya Integrated Management Launch Page.
- For upgrades from an existing version of Avaya Site Administration, verify that all customer settings remain in place.

Avaya Voice Announcement Manager

Perform the following tasks:

- Verify successful installation by launching from **Start** menu and Avaya Integrated Management Launch Page.
- Configure at least one voice system in Avaya Voice Announcement Manager and verify IP connectivity to the voice system and Avaya Voice Announcement Manager board.

Avaya Provisioning and Installation Manager

Perform the following tasks:

- Verify successful installation by launching from **Start** menu and Avaya Integrated Management Launch Page.
- Verify that a simple Device Profile can be created and sent successfully.
- Verify that a simple Template can be created and sent successfully
- Verify that for a G250 with Survivability, the SLS data can be collected and viewed in the Device Profile wizard.

Appendix A: Overview of Responsibilities

Table 14 provides an overview of customer and Avaya responsibilities.

Table 14: Customer and Avaya Responsibilities

Task		Customer	Avaya
1.	**Software/Hardware Procurement:**		
	a. Platform and Software Procurement		
	Server hardware	✓	
	Windows Server Operating System	✓	
	Red Hat Linux Enterprise Server	✓	
	HP OpenView Network Node Manager for Windows (optional)	✓	
	b. Connectivity Device Procurement		
	Remote access equipment to support product maintenance	✓	
2.	**Platform Installation and Configuration:**		
	a. Microsoft Windows Installation and Configuration	✓	
	Hardware-specific patches and drivers loaded	✓	
	LAN Interface Card configuration	✓	
	Platform Acceptance Test	✓	
	Verification of Platform Readiness		✓
	b. Red Hat Linux Enterprise Server Installation and Configuration	✓	
	Hardware-specific patches and drivers loaded	✓	
	LAN Interface Card configuration	✓	
	Platform Acceptance Test	✓	
	Verification of Platform Readiness		✓

1 of 3

Table 14: Customer and Avaya Responsibilities (continued)

Task		Customer	Avaya
	c. NMS O/S Installation and Configuration (optional)	✓	
	Hardware-specific patches and drivers loaded	✓	
	LAN Interface Card configuration	✓	
	Install and Configure Trouble Ticketing software	✓	
	Platform Acceptance Test	✓	
	Verification of Platform Readiness		✓
3.	**Switch and Connectivity Configuration and Testing:**		
	Remote access (via phone line connectivity)	✓	
	LAN and IP connectivity	✓	
	Creation of application-specific administration User ID and Password on managed voice and messaging systems	✓	
	Administration of server IP addresses on voice systems (where required)	✓	
4.	**Avaya Integrated Management Application Installation and Configuration:**		
	Avaya Site Administration	✓	✓
	Avaya Voice Announcement Manager	✓	✓
	Avaya VoIP Monitoring Manager	✓	✓
	Avaya Network Manager	✓	✓
	Avaya SMON Manager	✓	✓
	Avaya Integrated Management Database	✓	✓
	Avaya Fault and Performance Manager		✓
	Avaya MultiSite Administration		✓
	Avaya Proxy Agent		✓
	Avaya Provisioning and Installation Manager	✓	

2 of 3

Table 14: Customer and Avaya Responsibilities (continued)

Task		Customer	Avaya
5.	**Avaya Integrated Management integration with NMS:**		
	Avaya Network Manager	✓	✓
	Avaya Fault and Performance Manager		✓
6.	**System Verification and Acceptance:**		
	Verify proper operation of Avaya Integrated Management applications	✓	
	Customer acceptance		✓
			3 of 3

Appendix B: Installation of Red Hat Linux

Overview

This document specifies the options that you must select during the installation of Red Hat Enterprise Linux ES 3.0 or Red Hat Enterprise Linux AS 3.0 to support Avaya Fault and Performance Manager, Avaya Proxy Agent, and Avaya MultiSite Administration.

Note:

Red Hat Enterprise Linux ES 3.0 or Red Hat Enterprise Linux AS 3.0 is required for new installations. Red Hat Enterprise Linux ES 2.1 is supported only if you are upgrading from Avaya Integrated Management Release 2.1 to Avaya Integrated Management Release 3.0.

If an option is not specified in this document, select the default response.

Note:

Make sure a modem is attached to COM 1 (ttyS0) of the Linux server for dial-in access and turned on while you install Red Hat Linux.

Installing Red Hat Enterprise Linux ES 3.0 or Red Hat Enterprise Linux AS 3.0

To install Red Hat Enterprise Linux ES 3.0 or Red Hat Enterprise Linux AS 3.0, perform the following steps:

1. In the Disk Partitioning Setup dialog box, choose **Manually Partition with Disk Druid**, and click **Next**.
2. In the Disk Setup dialog box, use the **Delete** button to delete any partitioning that appears for the hard drive.

3. In the Disk Setup dialog box, use the **New** button to add partitions as shown in Table 15.

Table 15: Hard Drive Partitions

Mount Point	Partition Size (40 GB HD)	Proportion of Disk Space (>40 GB HD)	File System Type
/	800 MB	2%	ext3
/boot	100 MB	1%	ext3
/home	6000 MB	17%	ext3
/usr	6000 MB	15%	ext3
/opt	10000 MB	26%	ext3
/var	10000 MB	26%	ext3
swap	2048 MB	2048 MB	swap
/tmp	3000 MB	8%	ext3
Total	37948 MB	100%	

Note:

The precise partition sizes are shown for a 40 GB hard drive. (Note that a 40 GB hard drive partitions to approximately 38 GB.) If the hard drive is bigger than 40 GB, use the proportion column to partition the hard drive.

4. In the BootLoader Configuration dialog box, default settings are provided. Click **Next** to accept the default settings.
5. In the Network Configuration dialog box, click **Edit**, clear the **Configure using DHCP** check box, enter the static IP address and subnet mask, and then click **OK**.
6. In the Firewall dialog box, select **No Firewall**, and then click **Next**.
7. In the Network Configuration dialog box, enter the fully-qualified domain name in the hostname field; gateway; and primary, secondary, and tertiary DNS server IP addresses, and then click **Next**.
8. In the Package Install Defaults dialog box, select **Customize the set of packages to be installed**, and then click **Next**.

9. In the Package Group Selection dialog box, select the following packages:
   - **KDE Desktop**
   - **Editors**
   - **Web Server (php-pgsql)**
   - **FTP Server**
   - **Network Server (openldap)**
   - **Legacy Network Server (all)**
   - **KDE Software Development**
   - **Legacy Software Development**
   - **System Tools (vnc, tsclient, uucp)**

   If you are using analog modem-based alarming with Proxy Agent on this server, also select **System Tools**, click **Details**, select **UUCP**, and then click **OK**. When done, click **Next**.
10. In the About to Install dialog box, click **Next**. The files are installed.
11. In the Install Successful dialog box, click **Exit** to reboot the system. The system reboots.
12. In the User Account dialog box, add at least one regular user account to the system.
13. In the Red Hat Network dialog box, register the system with Red Hat to obtain OS updates and fixes and to use the up2date tool to keep the OS up to date.
14. In the Finish Setup dialog box, click **Next**.

Installing Additional Software

To install additional software, perform the following steps:

1. After you install Red Hat, you must install the **mgetty** Red Hat Package Manager (RPM) files from the Red Hat CD. The mgetty RPM is required for remote maintenance by Avaya Services. This may not be required if alternate remote network access (RAS/VPN) is being provided to Avaya Services personnel.
2. In addition, verify that the following RPM files were loaded during the Red Hat installation:
   - **ppp**

     The ppp RPM is required for remote maintenance by Avaya Services. This may not be required if alternate remote network access (RAS/VPN) is being provided to Avaya Services personnel.

- **vnc** (located in System Tools)

  The vnc RPM is required for remote maintenance by Avaya Services for access to graphical user interfaces for troubleshooting purposes. This may not be required if an alternate method for displaying the XWindow desktop of the Linux server is provided.

- **vnc-server** (located in XWindows System)

  The vnc-server RPM is required for remote maintenance by Avaya Services for access to graphical user interfaces for troubleshooting purposes. This may not be required if an alternate method for displaying the XWindow desktop of the Linux server is provided.

- **httpd** (installed with Integrated Management 3.0)

  The httpd RPM is required by the Integrated Management Database.

- **php** (located on Web Server)

  The php RPM is required by the Integrated Management Database.

- **php-pgsql** (located on Web Server)

  The php-pgsql RPM is required by the Integrated Management Database.

- **openldap (2.0.23-4)** (located on Network Server)

  The openldap RPM is required by MultiSite Administration for Modular Messaging and SSH support.

- **cyrus-sasl (1.5.24-25)** (installed with Integrated Management 3.0)

  The cyrus-sasl RPM is required by MultiSite Administration for Modular Messaging and SSH support.

- **openssl (0.9.6b-18)** (installed with Integrated Management 3.0)

  The openssl RPM is required by MultiSite Administration for Modular Messaging and SSH support.

Note:

Most of these RPM files are installed during the operating system installation, while others are installed during installation of the Integrated Management 3.0 applications that run on the Linux server.

To determine the RPM files installed, see Determining Whether RPM Files are Already Installed on page 47. To install an RPM file, see Installing RPM Files on page 47.

Determining Whether RPM Files are Already Installed

To determine whether RPM files are already installed, perform the following steps:

1. In the terminal emulation window, at the command prompt, type **rpm –q <name of RPM package>**.
2. To search for RPM files using a partial RPM package name, at the command prompt type:

   rpm –qa | grep <partial name>

   For example, **rpm –qa | grep vnc** to determine if any RPM packages beginning with “vnc” have been installed.

Installing RPM Files

To install RPM files, perform the following steps:

1. Insert the Red Hat installation CD in the CD-ROM drive.
2. Open a terminal emulation window.
3. Type **cd /mnt/cdrom/RedHat/RPMS**.

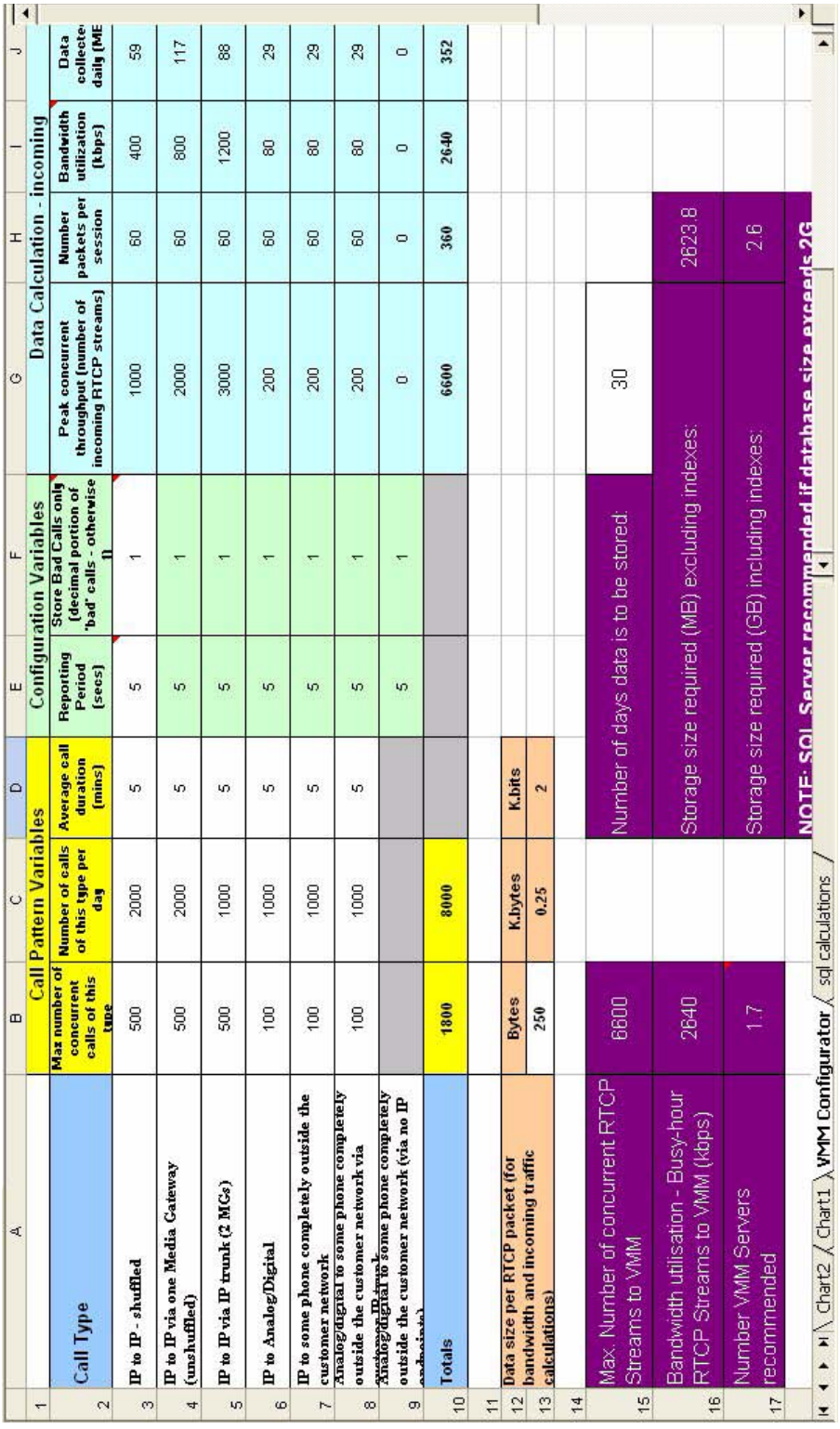
   Note:

   If Linux responds “directory does not exist,” you may have to manually mount the CD-ROM drive. To do so, perform the following steps:

   a. Type **mount /dev/cdrom**.

   b. Type **cd /dev/cdrom/RedHat/RPMS**.
4. At the command prompt, type **rpm –iv <name of RPM package>**.

Appendix C: Sample VMM Configurator



Call Type	Call Pattern Variables: Max number of concurrent calls of this type	Call Pattern Variables: Number of calls of this type per day	Call Pattern Variables: Average call duration (mins)	Configuration Variables: Reporting Period (secs)	Configuration Variables: Store Bad Calls only (decimal portion of 'bad' calls - otherwise 1)	Data Calculation - incoming: Peak concurrent throughput (number of incoming RTCP streams)	Data Calculation - incoming: Number packets per session	Data Calculation - incoming: Bandwidth utilization (kbps)	Data collecte daily (ME
IP to IP - shuffled	500	2000	5	5	1	1000	60	400	59
IP to IP via one Media Gateway (unshuffled)	500	2000	5	5	1	2000	60	800	117
IP to IP via IP trunk (2 MCs)	500	1000	5	5	1	3000	60	1200	88
IP to Analog/Digital	100	1000	5	5	1	200	60	80	29
IP to some phone completely outside the customer network	100	1000	5	5	1	200	60	80	29
Analog/digital to some phone completely outside the customer network via customer IP trunk	100	1000	5	5	1	200	60	80	29
Analog/digital to some phone completely outside the customer network (via no IP endpoints)				5	1	0	0	0	0
Totals	1800	8000				6600	360	2640	352

	Bytes	K.bytes	K.bits
Data size per RTCP packet (for bandwidth and incoming traffic calculations)	250	0.25	2

Max. Number of concurrent RTCP Streams to VMM	6600	Number of days data is to be stored:	30
Bandwidth utilisation - Busy-hour RTCP Streams to VMM (kbps)	2640	Storage size required (MB) excluding indexes:	2623.8
Number VMM Servers recommended	1.7	Storage size required (GB) including indexes:	2.6

NOTE: SQL Server recommended if database size exceeds 2G

Index

Symbols

A

B

C

D

F

G

H

I

M

O

P

R

S

T

V