AVAYA

Avaya Integrated Management Release 2.1

Implementation Guidelines

555-233-163
Issue 9
June 2004

Notice

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

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

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

The LASER devices operate within the following parameters:

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

Luokan 1 Laserlaite

Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

Means of Connection

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

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

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

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

Declarations of Conformity

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

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

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

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

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

European Union Declarations of Conformity

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). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

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

Japan

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

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

Preface

Purpose

This document 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 document 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

Avaya Remote Network Integration Services (RNIS) provides implementation services for Avaya Integrated Management applications. 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 this document.

Intended Audience

This document 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.

Additional Resources

The following additional resources may be helpful.

- Avaya Integrated Management, Advanced Converged Management Installation and Upgrade, document number 555-233-160
- Avaya Integrated Management, Enterprise Converged Management and Enhanced Converged Management Installation and Upgrade, document number 555-233-161
- Avaya Integrated Management, Network Infrastructure Management Installation and Upgrade, document number 555-233-167
- Avaya Integration Management, Configuring Red Hat Linux, document number 555-233-152
- Avaya MultiSite Administration Configuration, document number 555-233-137, and Help system
- Integrated Management Database (IMD) Configuration, document number 14-300039
- Avaya Fault and Performance Manager, document number 555-233-139
- Avaya Proxy Agent, document number 555-233-139
- Avaya ATM WAN Survivable Processor Manager Configuration, document number 555-233-223, and Help system
- Avaya Directory Enabled Management
  - — Installation and Implementation, document number 555-038-101
  - — Administration, document number 555-038-501
  - — Data Scheme, document number 555-233-164
  - — Help system
- Avaya Terminal Configuration Administration, document number 555-250-103, and Help system
- Avaya VoIP Monitoring Manager, User Guide, document number 555-233-510, and Help system
- Avaya Site Administration, Help system
- Avaya Voice Announcement Manager, Help system

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! Please 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

How to Access Books on the Web

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

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

1. Access http://www.avaya.com/support.
2. In the left column, click **System and Network Management**.
3. Scroll to **Integrated Management**, locate the product name, and click the link corresponding to the software release to display a list of available books for that product.

How to Order More Copies of This Book

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

Order: Document Number:555-233-163
Issue:Issue 9
Date: June 2004

Call: Avaya Publications Center
Voice:1 800 457 1235
Fax: 1 800 457 1764

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

Voice:+ 1 207 866 6701
Fax: + 1 207 626 7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835
USA

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 Advanced Converged Management offer manages 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 1.

Table 1: 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
S8500	Communication Manager 2.0
S8700 Media Server	MultiVantage
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

Operating Environment

The Avaya Integrated Management products are listed in Table 2. 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 3, Table 4, Table 5, and Table 6.

Table 2: 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)		✓	✓	
Avaya Proxy Agent	✓			
Avaya Network Management Console with System View			✓	
Avaya Network Configuration Manager		✓	✓	
Avaya Software Update Manager		✓	✓	
Avaya SMON^{TM} Manager		✓	✓	
Avaya Address Manager		✓	✓	
Avaya VLAN Manager		✓	✓	
Avaya QoS Manager		✓	✓	
Avaya VoIP Monitoring Manager			✓	✓
Avaya Device Managers		✓	✓	
Avaya ATM WAN Survivable Processor Manager			✓	
Avaya Site Administration				✓
Avaya Voice Announcement Manager				✓
Avaya Directory Enabled Management			✓	
Avaya Terminal Configuration			✓	

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 3, Windows Server Requirements, on page 13.
- Table 4, Red Hat Enterprise Linux Server Requirements, on page 14.
- Table 5, Solaris Server Requirements, on page 15.
- Table 6, Windows Client PC Requirements, on page 15.

Use of machines that are below the recommended configurations may result in poor performance.

Table 3: Windows Server Requirements[1] ***1 of 2***

Component	Recommended	Comments
Operating System	Microsoft Windows 2003 Standard Edition or Enterprise Edition server.	Microsoft Windows 2000 server is supported.
Processor	2.0 GHz Pentium® 4	1.3 GHz Pentium 4 is acceptable. 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 for remote access	
CD-ROM Drive	Required	Needed for installation.
Extra Software	Anti-virus software pcAnywhere	Required for Avaya support. pcAnywhere is needed for remote access by Avaya Services.
Web Browser	Internet Explorer 6.0	Needed for access to the Integrated Management Home Page and web-based clients.

1 of 2

Table 3: Windows Server Requirements[1] *2 of 2*

Component	Recommended	Comments
Network Management System	HP OpenView 7.0.1 for Windows	**Optional**. HP OpenView 6.4 is also supported. HP OpenView is **not** included on the Windows server CD. Customers must purchase, install, and maintain HP OpenView. Avaya Services does not support HP OpenView in any Integrated Management offer.
Java Runtime Environment	1.4.2	Needed to support web-based applets and Java applications. JRE is included on the Windows Server CD.
		2 of 2

[1] Avaya Integrated Management requires a Microsoft Windows 2003 Standard or Enterprise edition or a Microsoft 2000 server operating system on a high-end desktop machine. A server class hardware platform is not required.

Table 4: Red Hat Enterprise Linux Server Requirements

Component	Recommended	Comments
Operating System	Red Hat Enterprise Linux ES R3.0 or Red Hat Enterprise Linux AS R3.0	For new installations, Red Hat Enterprise Linux ES R3.0 or Red Hat Enterprise Linux AS R3.0 are required. For upgrade installations, Red Hat Enterprise Linux ES R2.1 is required.
Processor	2.0 GHz Pentium® 4	1.3 GHz Pentium 4 is acceptable. 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	Needed for installation.

Table 5: Solaris Server Requirements

Component	Recommended	Comments
Operating System	Solaris 9	Solaris 9 is required for new installations. Solaris 8 is also supported.
Network Management System	HP OpenView 7.0.1 for Solaris	**Required**. HP OpenView 6.4 is also supported. HP OpenView is **not** included on the Solaris server CD. Customers must purchase, install, and maintain HP OpenView. Avaya Services does not support HP OpenView in any Integrated Management offer.
Processor	SPARC architecture 500MHz	
Hard Drive	40 GB	
Memory	1.5 GB RAM	
Network Connectivity	TCP/IP 100 Mbit Network Card	
Web Browser	Not required	Solaris client is not supported.
CD-ROM Drive	Required	Needed for installation.

Table 6: Windows Client PC Requirements

Component	Recommended	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	Required for Avaya support.
Network Connectivity	TCP/IP 10/100 Network Card	
Modem	56K Modem	**Optional**. May be needed for remote access to the client PC.
CD-ROM Drive	Required	Needed for installation.
Web Browser	Internet Explorer 6.0	Required to access the Integrated Management Home Page and web-based clients.

Connectivity/Network Connections

The Avaya Integrated Management Advanced Converged Management offer requires a local (or wide) area network connection to all network devices to be managed systems and supporting databases (for Directory Enabled Management). 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 S8500/S8700/S8710 media server.
- The C-LAN port used for SAT access on each DEFINITY® system or S8500/S8700/S8710 media server.

Computing Platform

The customer is responsible for obtaining the computing platform(s) used to host applications in Avaya Integrated Management. The specifications for the computing platforms needed to support Avaya Integrated Management applications are provided in the following tables:

- Table 3, Windows Server Requirements, on page 13
- Table 4, Red Hat Enterprise Linux Server Requirements, on page 14
- Table 5, Solaris Server Requirements, on page 15

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.

Remote Access Hardware and Software

Table 3 and Table 4 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 25.

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.

2 Implementation Services

Support Resources

The Remote Network Integration Services (RNIS) team, part of Avaya's Implementation Services Organization (ISO), provides implementation services for applications in Avaya Integrated Management. Servicing North American, multinational and international accounts from its location in St. Petersburg, Florida, USA, ISO delivers implementation services, maintenance services and remote network management services for multi-vendor networks. There are over 300 highly trained associates that provide Tier 1 through Tier 3 level remote support, including remote implementation support, network troubleshooting, and performance optimization for WAN and LAN equipment.

In the U.S., on-site support is provided by the Field Services Organization (FSO), a team that is geographically distributed across the U.S. and dedicated to the data networking business. This team of over 500 service professionals is supported by an elite team of data communications professionals in the St. Petersburg Technical Assistance Center (TAC).

Both the Avaya Data Technical Assistance Center (TAC) engineers and the Field Services Organization (FSO) team have an average of 15+ years experience in supporting data networking products and telecommunications networks, while senior engineers average 20+ years experience.

Customized Management Solutions for Avaya Integrated Management

The Integrated Management Product Team understands customer's needs and is focused on customer satisfaction. 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 the Avaya Integrated Management suite. 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.

Training and Project Management is available for the following Integrated Management applications:

- Avaya Site Administration
- Avaya Voice Announcement Manager
- Avaya Fault and Performance Manager/Proxy Agent
- Communication Manager Native SNMP Agent Alarms
- Avaya MultiSite Administration
- Avaya VoIP Monitoring Manager
- Avaya Directory Enabled Management
- Avaya Terminal Configuration
- Avaya Network Management Console with VoIP System View

Please contact the Product Team for details at:

mrance@avaya.com
Phone: 303-538-2851
Cell Phone: 303-961-9691

Product Packaging

There are six Avaya Integrated Management offers:

- Standard Management Solutions
- Standard Management Solutions Plus
- Network Infrastructure Management
- Enterprise Converged Management
- Enhanced Converged Management
- Advanced Converged Management

Irrespective of product packaging, Avaya will provide implementation services for individual applications on the customer’s computing platform:

- Avaya MultiSite Administration
- Avaya Proxy Agent
- Avaya Fault and Performance Manager
- Avaya Directory Enabled Management with Avaya Terminal Configuration
- Avaya SMON Manager
- Avaya VoIP Monitoring Manager (full version)
- Avaya Site Administration
- Avaya Voice Announcement Manager (Voice Announcement Board Administration)
- Avaya ATM WAN Survivable Processor 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
- Avaya Directory Enabled Management

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 RNIS tier 2 technical support team at 1-800-237-0016, prompt 4. Note that charges may apply for RNIS implementation assistance.

Avaya's Technical Services Organization (TSO) provides warranty and maintenance services for an application only 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 27 have been successfully completed. Warranty and maintenance support is available at 1-800-237-0016, extension 73368 (or 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, Avaya Fault and Performance Manager, and Avaya Directory Enabled Management. The customer may choose to implement the remaining applications or have Avaya Services perform these implementations.

Basic implementation can be performed remotely using remote access technology (e.g., dial-up modem) to enable the RNIS Implementation Engineer(s) to have remote control/access to the customer servers. The remote RNIS Implementation Engineer(s) is in telephone contact with the designated customer representative as necessary during the implementation process. The customer representative assists with the implementation to verify server readiness (system powered-on and OS booted), verify availability of remote connectivity to the customer server(s) and managed devices (e.g., voice systems), and place product CDs into the server CD drive as directed by the remote engineer. Once these activities have been completed, the customer representative is not required to assist with configuration and customization of the application software.

For customers in the U.S, Onsite Installation is available for an additional charge. When requested, a field technician is dispatched to the customer site and replaces the customer representative to act as the hands of the remote RNIS Implementation Engineer in performing the implementation. The on-site technician verifies server readiness (system powered-on and OS booted), verifies availability of remote connectivity to the customer server(s) and managed devices (e.g., voice systems), and places product CDs into the server CD drive as directed by the remote engineer. Once these activities have been completed, the technician leaves the customer site while the remote RNIS Implementation Engineer completes configuration and customization of the application software.

Onsite Implementation is available as an add-on offer with any RNIS offer. With this offer, the RNIS Implementation Engineer travels to the customer site to perform the implementation. Onsite Installation and Onsite Engineer should never be ordered together.

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.

The application may be configured for additional managed devices under the Configuration of Managed Devices offer. As an additional service, the customer can request Avaya Services to configure Avaya Integrated Management applications to work with additional managed devices.

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 configuration parameters are required on the voice system to operate with the application. In particular, a login/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, RNIS implementation services described in this document do not include administration of configuration parameters on any Avaya ECLIPS or DEFINITY voice systems.

The Solution Evaluation offer provides a 4-hour block of time for a RNIS engineer to work with the customer via telephone 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

The RNIS Services Organization is composed of the following service groups:

- **Data Help Desk (DHD) –** The primary objective of the DHD is management and scheduling of RNIS Resources. The DHD team receives and tracks all requests received to engage RNIS Implementation provisioning. 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 RNIS 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 team will see that the necessary FSO/ISO resources have been scheduled for service projects. At the completion of service, the CIC team contacts the customer to gain acceptance of the work performed.
- **RNIS Implementation Engineers** - The RNIS Implementation Engineers receive the order documentation, including the Implementation Request Form and Configuration Request Forms (described later in this document), from the DHD team and use this information to create the Installation Specification. The engineers communicate with customer technical contacts to gather additional information to add to the Installation Specification and Configuration files.

RNIS 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 RNIS Implementation Engineer uses to configure the Avaya Integrated Management software to meet customer requirements.

Based on information on the customer’s Implementation Request Form and Configuration Request Form(s) submitted with the order and direct communications with the customer technical contact, the RNIS Implementation Engineer creates 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 Request Form

The Implementation Request Form (IRF) provides RNIS 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
- Customer directory schema (for Directory Enabled Management)
- Filters for forwarding of alarms (for Avaya Fault and Performance Manager).

The Linux CRF must be submitted when one or more of the following Linux-based applications is to be implemented:

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

The Windows CRF must be submitted when one or more of the following Windows-based applications is to be implemented:

- Avaya Directory Enabled Management with Avaya Terminal Configuration
- Avaya ATM WAN Survivable Processor Manager
- Avaya VoIP Monitoring Manager
- Avaya Network Management Console

Avaya and Customer Responsibilities

Table 7, Customer and Avaya Responsibilities, on page 31 summarizes the responsibilities of the customer and Avaya RNIS 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 RNIS Data Help Desk.

For all RNIS service orders, the customer is responsible to:

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

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

> **NOTE:**
> If required documentation is not provided to the RNIS 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 RNIS 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 typically takes the form of an analog modem connected directly to the server in conjunction with an analog phone line having a telephone number accessible on the public phone network. Testing must include:

- Establishing a dialup connection and initiation of a pcAnywhere session on a Windows server, and
- Establishing a dialup 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 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 number of managed nodes using serial alarming, whether the proxy server is providing alarm reception only or must perform alarm forwarding and filtering, and if 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 RNIS Implementation Engineer.

Computing Platform

The customer is responsible for acquiring servers and loading the Windows server and Red Hat Enterprise Linux server operating systems. It is important that the computing platform meet the minimum requirements specified in Table 3, Windows Server Requirements, on page 13 and Table 4, Red Hat Enterprise Linux Server Requirements, on page 14. Failure to meet these requirements may result in poor system performance. If desired, Avaya Services will install the Windows server or Red Hat Enterprise Linux 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” 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 dialup 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 dialup connection can be established prior to the scheduled date of implementation.

IP Connectivity

Network verification is performed by the RNIS 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 RNIS 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 RNIS Implementation Engineer performs an application-specific Acceptance Test to verify application implementation.

Avaya Fault and Performance Manager and Avaya Proxy Agent

Once the Avaya Fault and Performance Manager and Avaya Proxy Agent have been installed and configured, the RNIS 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 RNIS 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** the 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 the Avaya Proxy Agent via the change managed-nodes command.
- Verify that the customer can set/change voice system login information for the Avaya Proxy Agent via the change managed-nodes command.

Avaya MultiSite Administration

Once Avaya MultiSite Administration has been installed and configured, the RNIS 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 Home Page.
- Change the default **admin** password and report this to the customer.
- Create at least one Avaya MultiSite Administration user for the customer.
- 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 Directory Enabled Management and Avaya Terminal Configuration

Verify successful installation by launching from START menu and Avaya Integrated Management Home Page.

Avaya SMON Manager

Verify successful installation by launching from START menu and Avaya Integrated Management Home Page.

Avaya VoIP Monitoring Manager

Once the Avaya VoIP Monitoring Manager has been installed, the RNIS 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 > VoIP Monitoring Manager Server.**
2. From the machine hosting the VoIP Monitoring Manager client, select **Start > Programs > Avaya > VoIP Monitoring Manager > VoIP Monitoring Manager Client** to start the VoIP Monitoring Manager client.
3. Start a call between two IP phones.
4. From the Search dialog on the client, select the search option **Sessions active in the last 1 minute**. This is the default setting. If the Search dialog is not visible on the screen, click the **Search** button to display the Search dialog.
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. From the Search dialog, select the search option **Sessions active in the last 1 minute again.** If the Search dialog is not visible on the screen, click the **Search** button to display the Search dialog. Click the **Search** button to be informed that there are no active endpoints.
8. Select the **Sessions active from** radio button.
9. 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.
10. Click **Search**. 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 Home Page.
- For upgrades from an existing version of Avaya Site Administration, verify that all customer settings remain in place.

Avaya ATM WAN Survivable Processor Manager

Perform the following tasks:

- Configure ATM WAN Survivable Processor Manager to connect to the PPN and verify connection. Once connected, ATM WAN Survivable Processor Manager retrieves WSP(s) name(s).
- Configure connectivity information for each WSP and verify.
- Configure e-mail notification feature if desired by customer.
- Configure scheduled WSP updates to run as desired by customer.

Avaya Voice Announcement Manager

Perform the following tasks:

- Verify successful installation by launching from START menu and Avaya Integrated Management Home 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.

A Overview of Responsibilities

Table 7 provides an overview of customer and Avaya responsibilities.

Table 7: Customer and Avaya Responsibilities *1 of 2*

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		✓
	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		✓

1 of 2

Table 7: Customer and Avaya Responsibilities *2 of 2*

Task		Customer	Avaya
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 ATM WAN Survivable Processor Manager	✓	✓
	Avaya Directory Enabled Management		✓
	Avaya Fault and Performance Manager		✓
	Avaya MultiSite Administration		✓
	Avaya Proxy Agent		✓
	Avaya Terminal Configuration	✓	✓
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		✓

2 of 2

B Installation of Red Hat Linux

This appendix 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 2.0 to Avaya Integrated Management Release 2.1.

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

1 At the “Disk Partitioning Setup” prompt (screen #5), choose **Manually Partition with Disk Druid**, and click **Next**.

2 At the “Disk Setup” prompt (screen #7), use the **Delete** button to delete any partitioning that appears for the hard drive.

3 At the “Disk Setup” prompt (screen #7), use the **New** button to add partitions as shown in the following table.

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.

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%	

4 At the “Network Configuration” prompt (screen #8), click **Edit**, clear the **Configuration using DHCP** check box, enter the static IP address and subnet mask, and then click **OK**.

5 At the “Network Configuration” prompt (screen #8), enter the fully-qualified domain name in the hostname field; gateway; and primary, secondary, and tertiary DNS server IP addresses, and then click **Next**.

6 At the “Package Install Defaults” prompt (screen #13), select **Customize the set of packages to be installed**, and then click **Next**.

7 At the “Package Group Selection” prompt (screen #14), select **Editors**, **Legacy Software Development**, **KDE**, and **FTP Server**. 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**.

8 At the “About to Install” prompt (screen #15), click **Next**. The files are installed.

9 At the “Install Successful” prompt (screen #20), click **Exit** to reboot the system. The system reboots.

10 At the “User Account” prompt (screen #24), add at least one regular user account to the system.

11 At the “Red Hat Network” prompt (screen #25), 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.

12 At the “Finish Setup” prompt, click **Next**.

Installing Additional Software

1 After you install Red Hat, you must install the **mgetty** RPM (Red Hat Package Manager) 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**

  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 X window desktop of the Linux server is provided.

- **vnc-server**

  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 X window desktop of the Linux server is provided.

- **httpd**

  The httpd RPM is required by the Integrated Management Database.

- **php**

  The php RPM is required by the Integrated Management Database.

- **php-pgsql**

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

- **openldap (2.0.23-4)**

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

- **cyrus-sasl (1.5.24-25)**

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

- **openssl (0.9.6b-18)**

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

NOTE:
These RPMs are usually installed during the operating system installation.

To install an RPM or determine the RPMs installed, perform the procedures in the following sections.

Determining whether RPM Files are already Installed

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

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>**.

Index