Avaya MultiVantage™ Configuration Manager

Release 1.0
Installation and Configuration

555-233-137
Issue 1
June 2002

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.

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 Web site:
http://www.avaya.com/support/
If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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.

Voice Over Internet Protcal (VoIP)

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya's recommendations for configuration, operation and use of the equipment. YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.

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.
The equipment described in this manual complies with standards of the following organizations and laws, as applicable:

- Australian Communications Agency (ACA)
- American National Standards Institute (ANSI)
- Canadian Standards Association (CSA)
- Committee for European Electrotechnical Standardization (CENELEC) – European Norms (EN’s)
- Digital Private Network Signaling System (DPNSS)
- European Computer Manufacturers Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- FCC Rules Parts 15 and 68
- International Electrotechnical Commission (IEC)
- International Special Committee on Radio Interference (CISPR)
- International Telecommunications Union - Telephony (ITU-T)
- ISDN PBX Network Specification (IPNS)
- National ISDN-1
- National ISDN-2
- Underwriters Laboratories (UL)

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 Laser products, equipment classification and requirements:

- IEC 60825-1, 1.1 Edition
- 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

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.

This equipment complies with Part 68 of the FCC Rules. On the rear 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.

The REN is used to determine the quantity of devices which 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 table.

Manufacturer's Port Identifier	**FIC Code**	**SOC/REN/ A.S. Code**	**Network Jacks**
Off/On premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
CO trunk	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, 1KN, 1SN	6.0F	RJ48C, RJ48M
120A2 channel service unit	04DU9-DN	6.0Y	RJ48C

If the terminal equipment (for example, the MultiVantage™ Solution equipment) 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.

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 digital apparatus does not exceed Class A limits for radio noise emission set out in the radio interference regulation of the Canadian Department of Communications.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils manicures de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le ministére des Communications 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://support.avaya.com/elmodocs2/DoC/SDoC/index.jhtml/
All MultiVantage™ system products 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) signed by the Vice President of MultiVantage™ Solutions research and development, Avaya Inc., can be obtained by contacting your local sales representative and are available on the following Web site:
http://support.avaya.com/elmodocs2/DoC/IDoC/index.jhtml/

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。

Network Connections

Digital Connections - The equipment described in this document can be connected to the network digital interfaces throughout the European Union.
Analogue Connections - The equipment described in this document can be connected to the network analogue interfaces throughout the following member states:

Belgium	Germany	Luxembourg
Netherlands	Spain	United Kingdom

LASER Product

The equipment described in this document may contain Class 1 LASER Device(s) if single-mode fiber-optic cable is connected to a remote expansion port network (EPN). The LASER devices operate within the following parameters:

- Maximum power output –5 dBm to -8 dBm
- Center Wavelength 1310 nm to 1360 nm
- CLASS 1 LASER PRODUCT IEC 60825-1: 1998

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

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.410.568.3680
FAX 1.800.457.1764 or 1.410.891.0207
Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management
E-mail: totalware@gwsmail.com

Table of Contents

Preface

Purpose

This book explains how to install and configure Avaya MultiVantage™ Configuration Manager (MCM), how to test the installation, and how to troubleshoot it.

Prerequisites

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

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

Intended Audience

We wrote this book for workstation or network administrators.

Conventions Used in This Book

In this book, we use the following typographical conventions:

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

Additional Resources

You may find the following additional resources helpful.

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

For help with complex administration tasks, use the *Administrator's Guide for Avaya MultiVantage™ Software*, which explains system features and interactions in detail. You can access this document using the instructions in "How to Get This Book (and Others) on the Web" on page 9.

Tell Us What You Think!

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

Mail: Avaya, Inc.
MCM Documentation Team
Room B3-H25
1300 W. 120th Ave.
Denver, CO 80234-2726
USA

Fax: MCM Documentation Team
+ 1 303 538 1741

E-mail: document@avaya.com

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

To view or download the latest version of this book, complete the following steps:

1. Install your internet browser.

   Most computers are sold with browsers already installed.

2. Get access to the Internet.

   If you do not already have access to the Internet, contact an Internet Service Provider (ISP) and set up an account.

3. Set up your browser preferences.

   Refer to the documentation that came with your browser.

4. Install Adobe Acrobat Reader with Search, version 5.0 or later.

   This is available on your CD-ROM or from: http://www.adobe.com.

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

6. Click `Online Services`.

7. Click `Documentation`.

8. Click `Recent Documents.`

9. Locate the title of the book you want and then click it.

How to Order More Copies of This Book

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

Order: Document Number: 555-233-137
Issue: Issue 1
Date: 6/99

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: + 1 410 568 3680
Fax: + 1 410 891 0207

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

1 Resources and Notices

This chapter contains resources and notices that are pertinent to Avaya MultiVantage™ Configuration Manager (MCM).

Avaya Resources

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

Client executives the customers' primary source to obtain information and explore custom options to meet their specific business needs.

The Avaya Enterprise Management Support Home page web site contains the system requirements and other provisioning and connectivity information for MCM. See "Avaya Contact Information" on page 12 for the web address.

Avaya Technology and Consulting (ATAC)

ATAC works with client teams to develop detailed solutions for connectivity to MultiVantage™ solutions. The ATAC also designs network configurations to support MCM.

Avaya Remote Network Implementation Services (RNIS)

For this product, RNIS offers customers the following services:

- Verify platform readiness
- Remotely install MCM
- Connect and configure voice systems to work with MCM
- Verify customer acceptance

Avaya Technical Service Organization (TSO)

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

- Customers do not have a current maintenance agreement
- Customers do not procure and install the required systems and software as defined in the VisAbility Management Provisioning Package
- 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 Contact Information

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

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

Table 1. Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://support.avaya.com/
Avaya Technical Services Organization (TSO)	Technical Support: 1-800-242-2121, ext. 4-1080 or 720-444-1080
Remote Network Implementation Services (RNIS)	http://www1.avaya.com/enterprise/who/docs/dataimplementation/fullprodinfo.html
Toll Fraud Intervention	1-800-643-2353 prompt 1
VM001 Form	http://support.avaya.com/ Then click System/Network Management. Then click Enterprise Class IP Solutions (ECLIPS)

Table 2. Avaya Internal Resources

Resource	Contact Information
Avaya Enterprise Management Support	http://aem-support.dr.avaya.com/
Avaya Technology and Consulting (ATAC)	Phone: 1-888-297-4700, prompt 6 Main site (requires a password): http://sdsc.avaya.com
Connectivity Guide	http://sdsc.avaya.com/Connectivity_Guide/default.htm
Remote Network Implementation Services (RNIS)	http://associate2.avaya.com/sales_market/products/data-implementation-services/
VisAbility Management Provisioning Package	http://aem-support.dr.avaya.com/vmspp10.doc

Third-Party Resources

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

Table 3. Vendor web sites

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

System Security Notices

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

Network Security

MCM uses the standard security features on the Red Hat Linux.

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

SECURITY ALERT:

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

Toll Fraud Security

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

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

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

Avaya Disclaimer

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

Toll Fraud Intervention

If customers suspect that they are a victims of toll fraud and need technical assistance, they should refer to the "Avaya Contact Information" on page 12 for the Toll Fraud Intervention phone number.

2 Overview

Avaya MultiVantage™ Configuration Manager (MCM) is a client-server based MultiVantage software administration application that offers these powerful features:

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

Installation Checklist

1. **Prepare the MCM server.**

   a. Purchase computers (if necessary) that meet the hardware and software requirements on page 17.

   b. Install computers (if necessary).

   c. Ensure TCP/IP connectivity between the MCM server, MCM client, and MultiVantage solutions. Troubleshoot problems with the LAN/WAN administrator.

2. **Prepare MultiVantage solutions for MCM. 19**
3. **Install MCM. 21**
4. **Configure MCM. 31**
5. **Test the Installation.**

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

6. **Troubleshoot, if appropriate.**

Getting Help with the Installation

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

If you are located outside the United States and you want help installing or setting up MCM, call your Avaya representative or distributor. Call at least 4 weeks before the date on which you want to install MCM.

3 System Requirements

Client Requirements

Avaya MultiVantage™ Configuration Manager (MCM) Client workstations should meet the following requirements:

Parameter	Requirement
Operating system	Windows NT 4.0, 98, or 2000.
Other software	Netscape 6.2 (provided), or Internet Explorer 5.5 and Java Runtime Environment 1.3.1_02 (provided)
Processor	PII-600 MHz
RAM	256 MB
Available Disk Space	Minimum: 100 MB on the drive that contains the Windows System folder (normally but not always the C: drive)
	Maximum: Up to 1GB (if this computer is running all client applications in the suite)
CD-ROM	Optional
Network Connectivity	TCP/IP
IP Addresses	Static or dynamic (DNS preferred)
Display	SVGA

Server Requirements

Any server that you use to run MCM server software must meet the following requirements:

Parameter	Recommended
Operating system	Linux 7.1 or 7.2
Processor	1.3 GHz Pentium 3 or Pentium 4
RAM	1 GB
Available Disk Space	40 GB
CD-ROM	Required for installation
Network Connectivity	10/100 network card
Modem	56K required for remote support

Red Hat Recommendations

For MCM to work, when Red Hat is installed and configured on the MCM server, specific options Red Hat must be enabled. For a list of the recommended settings, contact your client executive and request a copy of the Avaya VisAbility Management Provisioning Package.

4 Preparing MultiVantage Solutions for Use with MCM

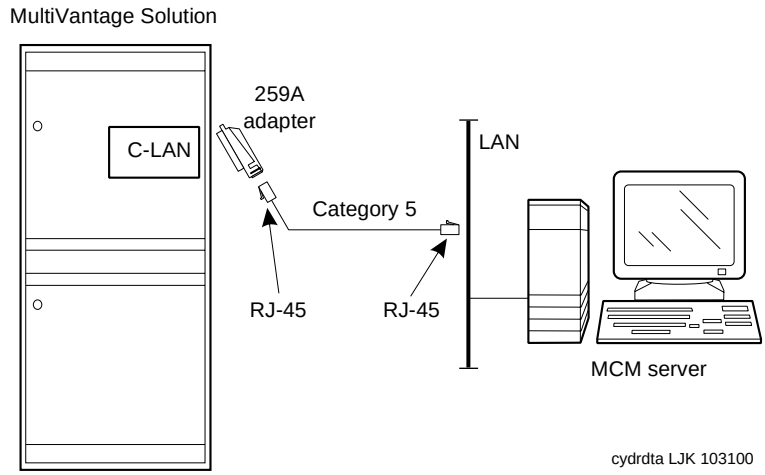
Before you can use Avaya MultiVantage™ Configuration Manager (MCM), you must complete the following activities for each MultiVantage solution that you want to access using MCM:

- Connect MultiVantage solutions to the network
- (Optional) Create a login for MCM on each MultiVantage solution.

Connecting servers to the network

To function properly, MCM must be connected to your MultiVantage solutions via a TCP/IP connection. New Avaya voice systems have TCP/IP connectivity built-in, whereas legacy voice systems require the use of a C-LAN circuit pack. Figure 1 illustrates a TCP/IP connection from the MCM server to a legacy Avaya voice system via a C-LAN circuit pack.

Figure 1. Connecting via C-LAN circuit pack



Creating a MultiVantage software login

If you want to track what MCM does on any given Avaya voice system, you must create a dedicated login on the voice system and enable it with super-user privileges. For instructions, refer to the *Avaya MultiVantage™ Systems Little Instruction Book for Basic Administration*. See "How to Get This Book (and Others) on the Web" on page 9.

5 Installing MCM

Installation Prerequisites

Before you install Avaya MultiVantage™ Configuration Manager (MCM), be sure that the computers you plan to install it on meet the requirements listed in "System Requirements" on page 17.

MCM requires a functioning LAN to operate. The instructions in this section assume that your LAN is fully operational and that all MCM computers can ping each other.

In addition, to install MCM server software, you must have a Red Hat Linux login with Administrator privileges, and to install the MCM client shortcut, you must have Windows Administrator privileges.

Giving Avaya Access to MCM

If your company has a support agreement with Avaya, then you need to install a modem on the Linux server. This enables Avaya service personnel to remotely troubleshoot and correct problems.

If you ever need remote Avaya support for MCM, complete the following steps:

1. Install a modem on the Linux server.
2. Contact Avaya's Technical Service Center (TSC).

   From the US, dial: 1 800 242 2121. From outside the US, contact your Avaya representative or dealer.
3. Give the TSC the phone number that they should use to access the modem that is connected to your MCM server.

Installing the MCM Server Software

To install the MCM server software, you must have an Administrator login on your UNIX system. Then, complete the following steps:

1. Insert the Avaya VisAbility Management Suite: System Management Linux Server CD into the CD-ROM drive.

   The CD browser window should appear automatically.

2. Open terminal emulation by clicking the terminal emulation icon in the Red Hat toolbar.

3. In the terminal emulation window, type **cd /mnt/cdrom** and press **Enter.**

4. Type **./vms_setup.bin** and press **Enter.**

   Red Hat displays the installation wizard.

5. At the Welcome page, click **Next.**

   If rpmspec has not already been installed, a message appears indicating this.

6. If the above message appears, click "Yes, launch the install routine for rpmspec for me" and click **Next.**

7. In the product installation screen, ensure that MultiVantage Configuration Manager is selected and click **Next.**

   By default, all of the listed applications are selected. Be sure to clear the check boxes of any applications that you do not want to install on this Linux server.

8. Review the summary page, and do one of the following:

   — If the information is accurate, click **Next.**

   — If the information is inaccurate, click **Back** to correct the error.

9. Read the Sun license agreement, click **Accept** if you accept it, and click **Next.**

10. Read the Apache license agreement, click **Accept** if you accept it, and click **Next.**

11. Read the Avaya MCM license agreement, click **Accept** if you accept it, and click **Next.**

    The installation wizard displays the message, "Installing System Management Linux Server. Please wait." Subsequently, the installer displays the message, "Creating uninstaller." Finally, it displays the message, "The InstallShield Wizard has successfully installed System Management Linux Server. Click Finish to exit the wizard."

12. Click **Finish.**

    The wizard closes.

13. In the terminal emulation window, type **reboot** and press **Enter.**

    This ensures that the Tomcat web server shuts down and restarts properly. Wait while the system reboots. After the system has rebooted, it displays the Red Hat login dialog box.

Installing MCM Client Software

To install MCM clients, you must use a Windows login that has Administrator privileges. Then, complete the following sections.

Starting the Installation

1. Shut down all applications running on the PC.
2. Insert the Avaya VisAbility Management Suite: Network Management Client for Windows CD into the CD-ROM drive.

   Wait a moment for the CD browser window to appear automatically.

3. Click **Install Network Management Client Products.**

   The installation program prepares the installation wizard and displays the Welcome page.

4. At the Welcome page, click **Next.**

   The installation program displays a list of the applications and shortcuts that you can install. By default, the option for Required Components is checked.

5. Select Shortcut for MultiVantage Configuration Manager, along with any other programs or shortcuts you want to install.

   When you select MCM, the installation program automatically also selects the option for Avaya Site Administration because Avaya Site Administration must be installed with MCM to enable cut-thru access to voice systems.

6. Verify that you have enough available hard disk space on your PC to install the shortcut(s).

   a. If you don't, click **Cancel** to exit the installation program.

      Restart the installation at **Step 1** when you have made adequate hard disk space available.

   b. If you do, click **Next.**

      The installation program displays the summary page.

7. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Finish.**

      A note advises you that if an installation wizard asks you if you want to reboot, you should NOT reboot until the final installation wizard (in your situation) has run. Click **OK.**

      Depending on which options you selected in **Step 5**, the "master installer" program launches one or more of the following installation wizards, in the following order:

      —Netscape installation wizard

      —Java Runtime Environment (only if you select a shortcut, Directory Enabled Management, or VAL Manager)

      —Required components installation wizard

      —Avaya Site Administration installation wizard

      —Avaya Terminal Emulation installation wizard

      —VAL Manager installation wizard

      —VoIP Monitor installation wizard

—System Management Client Shortcuts installation wizard.

—Adobe installation wizard

This book explains only the screens that appear if you select the MCM shortcut option. If you select additional options, you may see other screens in between the ones described below.

Installing the Java Runtime Environment

First, The Java Runtime Environment installation wizard runs.

1. Read the terms and conditions of the Sun license agreement, and do one of the following:

   a. If you agree to the terms and conditions, click **Yes.**

      The installation wizard displays any Release Notes.

   b. If you do not agree to the terms and conditions, click **Cancel.**

      This will terminate the installation wizard for this application. The installation program will display the wizard for the next application that you selected (if any) in **Step 5**. In that event, **refer to the installation documentation for that application and skip the rest of this procedure.**

2. Specify the location where you want to install the JRE and click **Next.**

   To change the location, click **Browse** and navigate to where you want to install the JRE.

3. Specify the browser(s) that you want this JRE plug-in to work with and click Next.

   The installation wizard copies the necessary files to your computer, then displays a message and exits when the installation is complete.

   Then, the Required Components installation wizard runs.

Installing the Required Components

When you install the Required Components, the installation program is setting up the necessary files so that you can launch VisAbility Management applications from the VisAbility Management home page.

1. At the Welcome screen, click **Next.**
2. Specify the location where you want to install the Required Components and click **Next.**

   To change the location, click **Browse** and navigate to where you want to install the Required Components.
3. Enter the computer name or FQDN of the VisAbility Network Management Server.

   The VisAbility Network Management Server is either a Windows server or a Linux server. It is the location where this client PC will look for the VisAbility Management web page. If you have installed (or plan to install) both the Windows server and the Linux server, enter the Windows server information here. If you have installed (or plan to install) only the Linux server, then enter the Linux server information here.

   You can type the computer name or the fully-qualified domain name (FQDN). The FQDN is the host name followed by the IP domain name. For example: `dnapc1.department.company.com`.
4. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Next.**

   The installation wizard displays a message that the installation of Required Components is complete.
5. Click **Finish.**

   The Avaya Site Administration installation wizard runs.

Installing Avaya Site Administration

1. At the Welcome screen, click **Next.**

   The installation wizard checks to see if you have earlier versions of Avaya Site Administration already installed on this computer. If you do, it will indicate this, and it will ask if you want the wizard to remove the old version, or if you want to remove it yourself.

2. When you see the above message, do one of the following:

   a. To preserve your Avaya Site Administration settings, click **Yes.**

      We recommend this option.

   b. To uninstall the old version yourself, click **No.**

      This will terminate the installation wizard for this application. The master installation program will display the next installation wizard (if any) corresponding to the selections you chose in **Step 5**.

      After you finish any other installation wizards, and after you remove Avaya Site Administration yourself, you must restart the master installation program (**Step 2**) to install MCM.

   If the installation wizard does *not* detect a copy of Avaya Site Administration on this computer, then it displays the appropriate license agreements.

3. If applicable, read the terms and conditions of the Avaya Site Administration license agreement, and do one of the following:

   a. If you agree to the terms and conditions, click **Yes.**

      The installation wizard displays any Release Notes.

   b. If you do not agree to the terms and conditions, click **Cancel.**

      This will terminate the installation wizard for this application. The installation program will display the wizard for the next application that you selected (if any) in **Step 5**. In that event, **refer to the installation documentation for that application and skip the rest of this procedure.**

4. Read the Release Notes and click **Next.**

   If this is the first time Avaya Site Administration has been installed on this computer, then the installation wizard displays the Destination page.

5. If applicable, verify that the pathname displayed in the "Destination Folder" field is where you want to install Avaya Site Administration

   a. If it is, click **Next.**

   b. If it isn't, click **Browse**, specify to the location where you want to install, and click **Next.**

   The installation wizard displays the summary page.

6. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Finish.**

7. Indicate whether or not you want a shortcut for Avaya Site Administration installed on your desktop and click **Next.**

   The installation wizard displays a message indicating that the Avaya Site Administration installation is complete. Then, the master installation program launches the installation wizard for Avaya VisAbility Management Suite Client Shortcuts.

Specifying the MCM Server

1. At the Welcome screen, click **Next.**

2. Enter the computer name or FQDN of the MCM server computer and click **Next.**

   You recorded this information when you installed the MCM server software on Linux. The installation wizard then displays a summary page.

3. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Finish.**

Finishing the Installation

After the final wizard runs, a message appears indicating that the installation is complete and that you can now reboot your computer if any of the installation wizards indicated that this was necessary. To finish the installation, complete the following steps:

1. On the CD Browser screen, click **Exit.**
2. Remove the CD from the CD-ROM drive.
3. Reboot (if appropriate).

Repeat this process, starting at "Starting the Installation" on page 23, on all other Windows computers that you want to serve as MCM clients.

6 Configuring MCM

To configure Avaya MultiVantage™ Configuration Manager (MCM), you will complete the following basic activities, which are described in more detail in this chapter:

1. Start MCM. page 31
2. Configure the MCM server. page 32
3. Add voice systems and or messaging systems. page 32
4. Change the administrative password. page 35
5. Add users and specify permissions. page 35
6. Start the queue. page 36
7. Initialize voice systems. page 37

Starting MCM

1. Go to an MCM client PC and choose **Start>Programs>Avaya>MultiVantage Configuration Manager.**

   The above step assumes that you installed MCM in the default location. If you installed it elsewhere, navigate to that location to start MCM.

2. At the Login dialog box, enter your Login ID, your password, and click **Login.**

   The first time you start MCM, enter the administrative Login ID **admin** and the password **admin123.**

Configuring the MCM Server

The first time you log into MCM, it will automatically display the MCM Server configuration wizard. To configure the MCM Server, complete the following steps:

1. At the Welcome page, click **Next.**
2. Enter the name for this server that you want to appear in MCM screens.
3. (Optional) Complete any other fields on this screen.
4. Click **Next.**
5. Enter the IP Address of the MCM server.

   (Optional) You can click the **Ping** buttons next to any of these addresses to check connectivity to those servers. After clicking Ping, click **OK** to close the response window.
6. (Optional) Enter the Gateway IP addresses.
7. (Optional) Specify the number of minutes after which inactive MCM users should automatically be disconnected from the server.
8. Click **Next.**

   MCM displays the Summary page.
9. If the information presented is accurate, click **Finish.**

   If it is not accurate, click **Back** to correct the error. If you click **Finish,** then MCM displays the Voice System Table, which you will use to add voice systems, as explained in the next section.

Adding Voice and Messaging Systems

1. With the Voice System table displayed, click **Add Device.**

   MCM displays the Welcome page of the Add Device Configuration Wizard.
2. At the Welcome page, click **Next.**

   MCM displays the Company Information page and fills in some of the fields using information that you entered when you configured MCM server.

3. (Optional) Enter any supplemental company information.
4. Click **Next.**
5. Complete the fields as follows and click **Next.**

Field Name	Description
Device Name	Enter the name of the voice system that you want to appear in MCM screens. What you enter here does not affect the voice system.
IP Address	Enter the IP address associated with the voice system.
Port Number	Enter the voice system administration IP port number that MCM should use to communicate with this voice system.
Cut-Through Port Number	Enter the IP port number that MCM should use when attempting to "cut through" to a MultiVantage solution using terminal emulation.
Group/Region Assignment	If your company uses any type of regional code or designation, enter it here.
Voice System Type	Enter the type of voice system this is (for example, DEFINITY R).
Version	Enter the release number of the MultiVantage software that is running on this voice system.
Administrative Login	Enter the login ID that MCM should use to access this system.
Password	Enter the password associated with this login ID.
Function Location Number	If your company uses any type of location code, enter it here.
Site Phone Number	Enter the phone number of a person who is physically proximate to this voice system.

6. (Optional) Specify information about any messaging systems that you want MCM to be able to access, and click **Next.**

Field Name	Description
Messaging System Name	Enter the name of the messaging system that you want to appear in MCM screens. What you enter here does not affect the messaging system.
IP Address	Enter the IP address associated with this messaging system.
Port Number	Enter the messaging system administration IP port number that MCM should use to communicate with this messaging system.
Login Name	Enter the login ID that MCM should use to access this system.
Password	Enter the password associated with this login ID
System Password	This is a second password that exists on some messaging systems. If you messaging system has a system password, enter it here.

7. Verify the information that you entered.

   If it is accurate, click **Finish.** If it is not, click **Back** to fix the error. If you click Finish, MCM displays the message, "Congratulations!"

8. Click **OK.**

   MCM displays the Voice Systems table again.

9. To exit the table, click **Cancel.**

   The first time you click Cancel, the MCM client closes. Restart the client. Subsequently, when you click Cancel on this screen, it simply clears the right side of the screen.

Changing the Administrative Password

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

To change the administrative password, complete the following steps:

1. With the MCM Manager tab displayed, click **User Configuration.**

   MCM displays the MCM User table.

2. Highlight the row associated with the Login ID `admin` and click **Update User.**

   MCM displays the Update User dialog box.

3. Click **Change** next to the Password label.

   MCM displays the Change Password dialog box.

4. Enter the new password twice and click **Change.**

   Remember to note the new password and save it in a secure location.

Adding MCM Users

To add users, complete the following steps:

1. From the MCM Manager tab, click **User Configuration.**
2. With the **MCM Users** tab on top, click **Add User.**
3. Complete the Add User screen.
4. Click **Add.**
5. Click the **Users on Switches** tab.
6. Click **Add User.**

7. Complete the fields on this page as follows, and click **Add.**

   a. Select the user's ID from the drop-down list.

   b. Enter and re-enter the password associated with that ID.

   c. Enter the user's name, company name, title, and phone number (the required fields).

   d. From the list on the right, select the voice system(s) that you want this user to be able to access using MCM.

      Shift-Click to select multiple contiguous voice systems.

   e. Place a check mark in each check box corresponding to the access permissions you want this user to have on the voice system(s) that you selected in the previous step.

   f. (Optional) Complete the non-required fields.

8. Repeat this process. for each user you want to add.

Starting the Queue

You must start the MCM queue running before you can use MCM to access or make changes to that system. To start the queue, complete the following steps:

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

Initializing Voice Systems

You must initialize each voice system that you want to use with MCM, before you use MCM to access or make changes to that system. To initialize a voice system in MCM, complete the following steps:

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

Glossary and Abbreviations

A

ATAC
See “Avaya Technology and Consulting (ATAC)” on page 11.

M

MCM
Avaya MultiVantage™ Configuration Manager

MFPM
Avaya MultiVantage™ Fault and Performance Manager

MPA
Avaya MultiVantage™ Proxy Agent

MultiVantage software
The call processing software that runs on MultiVantage solutions. Formerly known as DEFINITY software.

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

N

Network Management Server
This is the Windows box that you can install Windows-based VisAbility Management applications on.

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

R

RNIS
See “Avaya Remote Network Implementation Services (RNIS)” on page 11.

S

System Management Server
This is the Linux box that you install MCM on.

T

TSO
See “Avaya Technical Service Organization (TSO)” on page 12.

Index