Avaya VPNmanager® 3.5 Installation Guide

670-100-100
Issue 2
February 2004

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of release. 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 website:
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 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.

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

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.

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

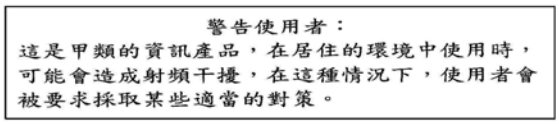
Japan

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。

China

BMSI (Chinese Warning Label)



Hardware, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import hardware.

Acknowledgments

This product includes software developed by the Apache Software Foundation (http://www.apache.org).

Documentation

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

Table of Contents

Installation

Appendix A *Installation Prerequisites for Microsoft Active Directory Server*

Installation

This document provides information you need to install Avaya VPNmanager® 3.5. Use the VPNmanager CD to install or to upgrade the *VPNmanager Console*.

Beginning with VPNmanager 3.5, the Sun ONE directory server is no longer included with the VPNmanager software, and is no longer part of the installation process.

Prior to beginning the installation process, VPNmanager software requires a previously installed directory server. VPNmanager is compatible with Microsoft's Active Directory and the Sun ONE directory server 5.1, previously the iPlanet directory server.

The *VPNmanager 3.5 Configuration Guide* with information about configuring VPNmanager can be downloaded from the Product Document page of the Avaya Support Web site at http://support.avaya.com.

Avaya VPNmanager installation

The installation sequence detailed in this chapter is listed in Table 1.

Table 1 VPNmanager Installation Sequence

	Installation Task	See Page
☐	Security gateway prerequisite	page 8
☐	VPNmanager system requirements	page 8
☐	Installing Avaya VPNmanager	page 10
☐	Changing the user name and password	page 21
☐	Integrating HP Openview with VPNmanager	page 22

Security gateway prerequisite

This guide does not give details about installing new security gateways to your existing VPN or building a new VPN with new security gateways. See the configuration guide for your security gateway model for installation instructions. To install the VPNmanager console, the security gateways only need to be configured with an IP address. The VPNmanager console can be used to perform the remaining configuration as described in the *Configuration Guide*.

For VPNmanager, you will need the security gateway's password. As a good practice, keep all the security gateway console passwords the same. The passwords will be needed when updating the security gateway from the VPNmanager console. If necessary, the security gateway console passwords can be changed from the VPNmanager console. After the security gateways are installed, review the system requirements for the VPNmanager software on page 9, then install the VPNmanager using the instructions on page 10.

VPNmanager system requirements

The VPNmanager software includes the VPNmanager console and the policy server software. The console is used for configuring and managing your VPN. The previously installed directory server stores your VPN data.

This section describes the system requirements that must be met before you install VPNmanager console and policy server.

VPNmanager console system requirements

VPNmanager console can be installed on computers running the following operating systems:

- Window NT 4.0 with Service Pack 6a (X86 only) or later
- Microsoft Windows 2000 Server; Advanced Server with Service Pack 2 (X86) or later
- Sun Solaris 8 or 9 for SPARC (32 x 64 bit)
  - The recommended Solaris patches and the J2SE patches should be installed.
  - The Sun recommended patch cluster can be obtained from your Sun support representative or from http://sunsolve.sun.com.

The minimum system requirements are listed in Table 2.

Table 2 VPNmanager console minimum system requirements

MS Windows	Solaris OS
• 256 MB RAM (up to 1 GB for best performance on large VPNs) • CD-ROM drive • 120 MB of free hard disk space • VGA monitor • 16-bit color video controller • From the TCP/IP properties, the DNS and Host name must be properly configured • An IP address must be assigned to the computer	• 256 MB RAM (up to 1 GB for best performance on large VPNs) • CD-ROM drive • 120 MB of free hard disk space • VGA monitor • 16-bit color video controller • The DNS and Host name for the computer must be properly configured • An IP address must be assigned to the computer

Policy server system requirements

The policy server can be installed on computers running the following operating systems:

- Microsoft Windows NT 4.0 with Service Pack 6a (X86 only) or later
- Microsoft Windows 2000 Server; Advanced Server with Service Pack 2 (X86) or later
- Sun Solaris 8 or 9 for SPARC (32 x 64bit)
  - The recommended Solaris patches and the J2SE patches should be installed. In addition, the recommended patch ID numbers, 108434 and 109147, are required.
  - The Sun recommended patch cluster can be obtained from your Sun support representative or from http://sunsolve.sun.com.

The minimum system requirements are listed in Table 3.

Table 3 VPNmanager policy server minimum system requirements

Computers running MS Windows	Computers running Solaris OS
• 256 MB RAM (up to 1 GB for best performance on large VPNs) • 20 MB of free hard disk space for small VPNs • CD-ROM drive • VGA monitor with resolution of 600x800 pixels • 100 Mbps ethernet connection • From the TCP/IP properties, the DNS and Host name must be properly configured • A static IP address must be assigned to the computer	• 256 MB RAM (up to 1 GB for best performance on large VPNs) • 20 MB of free hard disk space for small VPNs • CD-ROM drive • VGA monitor with resolution of 600x800 pixels • The DNS and Host name for the computer must be properly configured • A static IP address must be assigned to the computer

Avaya VPNmanager components

The VPNmanager CD-ROM includes all the files necessary to install VPNmanager console, policy server, and to update the directory server schema.

- **VPNmanager console** — The VPNmanager console is a client that is used for configuring, managing, and monitoring one or more VPNs. The console is a Java application that can be run anywhere and is used as a front-end to the policy server and directory server.
- **Directory server schema update** — The directory server schema update defines the structure and the type of configuration data.
- **Policy server** — The policy server distributes configuration and security policies. The VPNmanager console is a client that communicates with the policy server to retrieve security policies. The policy server then communicates with the directory server.

Installing Avaya VPNmanager

To install all of the VPNmanager components on the same machine, select the **Complete** option in the Setup Type dialog and follow the installation wizard. To install the VPNmanager components on different machines select the **Custom** option from the Setup Type dialog.

Note: *It is suggested that the directory server and the policy server be installed on the same machine.*

Choose the appropriate installation procedure listed below to guide you through your installation. It is important to follow the installation procedure in the sequence presented in this document.

Installation for Windows:

- Installing the policy server for Windows — page 14
- Updating the directory server schema for Windows — page 13
  - Updating the directory schema for Sun One the directory server — page 13
  - Updating the directory schema for Active Directory server — page 13
- Installing the policy server for Windows — page 14

Installation for Solaris:

- Installing VPNmanager console for Solaris — page 16
- Updating the directory server schema for Solaris — page 17

Installing the VPNmanager console for Windows

This procedure describes how to install VPNmanager console on computers running Windows 2000, or Windows NT 4.0 operating systems. Use this procedure, if you plan to install the console and servers on different computers or at different times.

To install the VPNmanager console:

1. Insert the *VPNmanager CD* into the computer where VPNmanager will be installed. When the Overview page opens, click **Installation** to go to the installation page.

   ***Note:** If autorun does not happen, from **Start>Run** click **Browse** to navigate to the install program \VPNmanager\disk1\windows\setup.exe.*

2. Click **Next**.

3. When the *Welcome* dialog box appears, click **Next**.

4. The *License Agreement* dialog box appears. Select the button that suits your license needs. Click **Next**.

5. Confirm that the directory server was previously installed. Click **Next**.

6. Choose the folder location where VPNmanager should be installed. Click **Next.**

7. The *Setup Type* dialog box appears. Select the **Console Only** option. Click **Next**.

8. Review the information on the Setup Type Summary. Verify that there is sufficient disk space to install the software. Click **Next** to begin installation.

   *If the information is not correct, click **Previous** and make the necessary corrections.*

Updating the directory server schema for Windows

This procedure describes how to update the directory server schema.

During this portion of the installation procedure, you will see *Directory Server Schema Update Program* screens.

Updating the directory schema for Sun One the directory server

To update the directory server schema:

1. The schema update wizard appears. This updates the schema of the directory server. Click **Next**.
   - **Type:** Select the directory server schema to be updated.
   - **IP Address:** Enter the IP address of the machine on which the directory server resides.
   - **Port:** Enter the port number of the directory server.
   - **Login ID:** Enter the login ID of the directory server. This is also called the directory server DN and begins with cn=. For example, cn=Directory Manager.
   - **Password:** Enter the directory server password.
   - **Directory Tree:** Enter the domain name assigned to the computer on which the directory server is installed.
   - **Fetch:** Displays the contexts that are available in the directory server. You can choose to install any of the contexts. You can create a branch and install the selected context into this branch.
2. Click **Update Schema.**
3. When the schema is updated, a *Schema Update Complete* dialog box appears. Click **Finish**.

Continue with installation of the policy server.

Updating the directory schema for Active Directory server

Before you begin, verify the following:

- Confirm that Active Directory is installed. Refer to Appendix A, Installation Prerequisites for Microsoft Active Directory Server.
- Configuration of an administrator with the privileges to update the schema and data

  It is important that you verify that the administrator ID you are using has permissions to extend the schema. If the administrator id does not have these permissions, you must **add** the administrator to the Schema Admins Group.
- Enable the computer to extend the schema

The configuration fields are as follows:

- **Type:** Select the Active Directory directory server schema to be updated.
- **IP Address:** Enter the IP address of the machine on which the directory server resides.
- **Port:** Enter the port number of the directory server.
- **Login ID:** Enter the login ID the directory server. This is also called the directory server DN and begins with cn=. For example, cn=Administrator, cn=Users.
- **Password:** Enter the directory server password.
- **Schema Tree:** Enter the credentials and click Fetch to retrieve the schema tree.
- **Fetch:** Displays the contexts that are available in the directory server. You can choose to install any of the contexts. You can create a branch and install the selected context into this branch.
- **Directory Tree:** Upon fetching the schema tree, the directory tree will be prepopulated. If your domain name is abc.com, your directory tree will be ou=VPNmanager, dc=abc, dc=com. Accept the directory tree.

Installing the policy server for Windows

This procedure describes how to install the policy server.

During this portion of the installation procedure, you will see *Policy Server Configuration Setup* screens.

To install the policy server:

1. The *Policy Server Wizard* dialog box appears. This installs and configures the policy server. Click **Next**.
   - **Type:** Enter the type of directory server that the policy server will communicate with.
   - **IP Address:** Enter the IP address of the machine on which the directory server resides.

Note: *Enter the IP address even when the policy server and directory server reside on the same machine. Enter the IP address through which the VPNmanager console can access the directory server.*

- **Port:** Enter the directory server port number. The policy server will use this port to communicate with the directory server.
- **Login ID:** Enter the login ID the policy server will use to access the directory server data. This is also called the directory server DN and typically starts with cn=.
- **Password:** Enter the password the policy server will use to access the directory server data.
- **Directory Tree:** Enter the directory tree that was used during the schema update.
- **Advanced:** The advanced button is used to secure the communication with the directory server using SSL.

Note: *The directory server must be enabled for SSL before this can be configured. Refer to the VPNmanager Administrator's Guide for directions on configuring SSL.*

2. Enter the directory server password. Click **Next**.

   The policy server stores the directory server configuration and uses the configuration to connect to the directory server.

3. The *Policy Server Configuration Setup* dialog appears.

   Enter a **new login ID and password**. This login ID is used to configure an administrator ID that can be used to login using the VPNmanager console. This ID can also be used to create another administrator.

   - **Administrator ID:** Enter the administrator ID. This is the login information used to log into the VPNmanager console. This administrator ID is the super user that can create additional administrators.
   - **Password:** Enter the password that will be used with the administrator ID. To confirm the password, retype it in the **Confirm Password** field.
   - **Policy Server Port:** Enter the port or accept port 443.

4. Click **Install**.

5. When the Policy Server Configuration Setup is complete, the *Policy Server Configuration Complete* dialog appears. Click **Finish** to exit the installation wizard.

   Upon completion of the policy server installation, the directory server and policy server are able to communicate. If the directory server configuration changes, the changes must be reflected in the policy server. If correct configuration is not maintained, you may need to reconfigure the policy server to reflect the changes made in the directory server.

Confirming the Installation

1. To confirm that the policy server is successfully installed, do the following:
   - Windows NT — go to *Start\Settings\Control Panel\Services*
   - Windows 2000 — go to *Start\Settings\Control Panel\Administrative Tools\Services*
2. Scroll down the Service menu to VPNmanager policy server.
3. Confirm that VPNmanager policy server is started. If the *Status* does not say Started, select the Service and click **Start**.

The VPNmanager console can now be started from the Windows Start menu. Login to the policy server using the super user ID and password configured during the policy server setup.

The Windows Start menu also provides the option to start, stop, and reconfigure the policy server.

Installing VPNmanager console for Solaris

This procedure describes how to install the VPNmanager console on computers running Sun Solaris. It can be performed before or after the server is installed.

Note: *This procedure is performed from the Common Desktop Environment.*

To install VPNmanager console:

1. Insert the *VPNmanager CD* into the computer where VPNmanager will be installed. When the Overview page opens, click **Installation** to go to the installation page.
2. Click **VPNmanager Install**. A security warning dialog box appears. Click **Yes**.
3. When the *Introduction* dialog box appears, click **Next** to proceed.

   Note: *If the autorun does not start, navigate to the install program \\disk1\solarisdisk1\install.bin. Double-click* ***setup.bin*** *to open the Action - Run dialog box*
4. Choose the folder location where VPNmanager console should be installed. Click **Next**.
5. When the *Setup Type* dialog box appears, choose the **Console only** option. Click **Next**.
6. Review the information on the *Pre-Installation Summary*. Verify that there is sufficient disk space to install the software. Click **Next** to begin installing the VPNmanager console.
7. When the *Install Complete* dialog box appears, click **Finish** to return to the Solaris desktop.

Updating the directory server schema for Solaris

This procedure describes how to update schema for the directory server.

Note: *This procedure is performed from the common Desktop environment.*

1. Insert the VPNmanager CD into computer. When the *Overview* page opens, click **Installation** to go to the installation page.
2. Click **VPNmanager install**. A security warning dialog box appears, click **yes**.
3. When the *Introduction* dialog box appears, click **Next** to proceed.

   Note: *If the autorun does not start, navigate to the install program \\vpnmanager\disk1\solaris\install.bin. Double-click* ***setup.bin*** *to open the Action - Run dialog box*

4. Choose the folder location. Click **Next**.

5. When the *Setup Type* dialog box appears, select the **Custom** option and select **Directory Server Schema Update**.

6. Review the information on the Pre-Installation Summary. Verify that there is sufficient disk space to install the software. Click **Next**, to begin the Schema update.

7. The *Schema Update* wizard appears. Click **Next**.

8. In the *Schema Update Input* dialog box, complete the following information and click **Update Schema**.

   - **Type:** Enter the type of directory server schema to be updated.
   - **IP Address:** Enter the IP address of the machine on which the directory server resides.
   - **Port:** Enter the port number of the directory server.
   - **Login ID:** Enter the login ID of the directory server. This is also called the directory server DN and begins with cn=. For example, cn=Directory Manager.
   - **Password:** Enter the directory server password.
   - **Directory Tree:** Enter the domain name assigned to the computer on which the directory server is installed.
   - **Fetch:** Displays the contexts that are available in the directory server. You can choose to install any of the contexts. You can create a branch and install the selected context into this branch.

9. When the schema is updated, a *Schema Update Complete* dialog box appears. Click **Finish**.

10. When the *Install Complete* dialog appears, click **Finish** to return to the Solaris desktop.

Installing the policy server for Solaris

1. Insert the VPNmanager CD into computer. When the *Overview* page opens, click **Installation** to go to the installation page.

2. Click **VPNmanager install**. A security warning dialog box appears, click **yes**.

3. When the *Introduction* dialog box appears, click **Next** to proceed.

   Note: *If the autorun does not start, navigate to the install program \\disk1\solaris\install.bin. Double-click* ***setup.bin*** *to open the Action - Run dialog box*

4. Choose the folder location. Click **Next**.

5. When the *Setup Type* dialog box appears, select the **Custom** option and select **Policy Server**.

   Note: *During the directory server input, fields are pre-populated only when the policy server and directory server are installed on the same computer.*

   - **Type:** Enter the type of directory server that the policy server will communicate with.
   - **IP Address:** Enter the IP address of the machine on which the directory server resides.

   Note: *Enter the IP address even when the policy server and directory server reside on the same machine. Enter the IP address through which the VPNmanager console can access the directory server.*

   - **Port:** Enter the directory server port number. The policy server will use this port to communicate with the directory server.
   - **Login ID:** Enter the login ID the policy server will use to access the directory server data. This is also called the directory server DN and typically starts with cn=.
   - **Password:** Enter the password the policy server will use to access the directory server data.
   - **Directory Tree:** Enter the directory tree that was used during the schema update.
   - **Advanced:** The advanced button is used to secure the communication with the directory server using SSL.

6. Enter the directory server password. Click **Next**.

   The policy server stores the directory server configuration and uses the configuration to connect to the directory server.

7. The *Policy Server Configuration Setup* dialog appears.

   Enter the administrator ID. This is the login information used to log into the VPNmanager console. This administrator ID is the super user that can create additional administrators.

   - **Administrator ID:** Enter the administrator ID. This is the login information used to log into the VPNmanager console.
   - **Password:** Enter the password that will be used with the administrator ID. To confirm the password, retype it in the **Confirm Password** field.
   - **Policy Server Port:** Accept port 443.

8. Click **Install** to begin installing the policy server.

9. When the Policy Server Configuration Setup is complete, the *Policy Server Configuration Complete* dialog appears. Click **Finish** to exit the installation wizard.

Creating a policy server restart script

The Policy Server will not automatically start if your Sun Solaris Sparc computer is restarted. The solution is to create a restart script file. The Policy Server should be started after you start the directory server

To create a restart script:

1. From a common text editor, create a file named S##PSstart, where ## is some number from 00 to 99.

2. Type the following script into the file, where InstallDir is the location where the Policy Server is installed
   /InstallDir/VPNmanager/PolicyServer/Tomcat/bin/startps.sh &

   /opt/Avaya/VPNmanager/PolicyServer/Tomcat/bin/startps.sh &

3. Save the script file to the /etc/rc2.d directory.

4. Use Table 4 to configure the access modes (permissions) for the script file.

Table 4 Script File Access Modes the policy server

User	Read	Write	Execute
Owner	yes	yes	yes
Group	yes	no	no
Other	yes	no	no

5. Restart the computer to verify the restart script.

After creating a restart script file, you can start the VPNmanager console at any time. Refer to the *Avaya VPNmanager Quick Installation Guide* for information about configuring VPNmanager.

Changing the user name and password

Changing the user name and password on the VPNmanager console, policy server, and directory server can enhance your corporate security policies.

VPNmanager console

To change the password for the VPNmanager console from the Configuration Console.

1. Select **View** form the VPNmanager menu bar.
2. Select **Admin** from the View menu.
3. Select the administrator to change the password from the Contents column.
4. From the General Tab, click the **Reset** button in the Reset Administrator Password dialog box.
5. Enter the new password, confirm the password, and click **OK**.

Directory server DN and password

To change the dn name, password, or any other configuration on the directory server, refer the directory server documentation.

Once the directory server configuration changes are made, go to:

Start>Programs>Avaya>VPNmanager>PolicyServer>Reconfigure

Superuser password for policy server

To change the superuser name and password for the policy server, go to:

Start>Programs>Avaya>VPNmanager>PolicyServer>Reconfigure

After the reconfigure command is complete, the VPNmanager begins using the new password.

Removing the anonymous login

After installing the directory server on Windows or on Solaris, a user can start to log into the directory server with any name and no password. This anonymous login lets a user view all the VPN configuration information, but does not give them the right to change, add, or delete any parameters. For added security, you should remove this anonymous login.

Refer to the directory server documentation to remove anonymous login.

Integrating HP Openview with VPNmanager

HP Openview is a tool developed by Hewlet Packard for network management. This tool has an integrated set of network and system management applications for controlling and administering heterogeneous networks.

Integrating HP Openview using Windows

To integrate HP Openview using Windows:

1. Confirm that HP Openview is installed on the same system as the VPNmanager console.
2. From the **Start** menu, open the following file:

   Start/Avaya/VPNmanager/HPOpenview
3. Point to a file under **<HPOpenview>/conf/oid_to_sym**.

4. Open the file **<HPOpenview>/conf/oid_to_sym**.
5. Once the <HPOpenview>/conf/oid_to_sym file is open, the integration will happen automatically.

Integrating HP Openview using Solaris

To integrate HP Openview using Solaris:

1. From the Desktop Manager, open the **Hosts** menu, then select **Console** to open the *Console* window.
2. At the command prompt, type **opt/Avaya/VPNmanager/Console**, then press **Return** to change directories.
3. Type **vpn3ovw.bat**, then press **Return** to open the Openview Integration dialog box.
4. Point to a file under **<HPOpenview>/conf/oid_to_sym**.
5. Open the file **<HPOpenview>/conf/oid_to_sym**.
6. Once the <HPOpenview>/conf/oid_to_sym file is open, the integration will happen automatically.

The results of the integration are as follows:

- HP Openview will discover Avaya devices automatically by showing SG icons located in the network.
- VPNmanager can be launched from HP Openview's Network Manager console.
- Avaya MIB can be loaded by the customer from the network node.

From HP Openview, the results are as follows:

- An Avaya button will be added to HP Openview's menu bar. The Avaya button will open the Avaya home page and the VPNmanager console.
- The VPNmanager console can be started from the tool bar.
- SGs connected to the network will be visible on the Network Node Manager window. The color of the icon will also indicate if the SG is up and running.

Upgrading Avaya VPNmanager

Table 5 list the Upgrade steps that should be performed.

Table 5 Avaya VPN solutions upgrade checklist

	Upgrade Task	See Page
☐	VPNmanager system requirements	page 8
☐	Backing up all databases	page 24
☐	Upgrading Avaya VPNmanager for Windows	page 24
☐	Upgrading Avaya VPNmanager for Solaris	page 25

Backing up all databases

It is important to backup all databases prior to upgrading VPNmanager.

Refer to your directory server documentation to backup your database.

Upgrading Avaya VPNmanager for Windows

To upgrade the VPNmanager on a computer running Windows NT or Windows 2000, use the following procedures.

Note: *For systems running Windows NT, upgrade to VPNmanager 3.3 before upgrading to VPNmanager 3.5.*

Upgrading from VPNmanager 3.2 to VPNmanager 3.5

VPNmanager 3.5 uses the Sun ONE directory server 5.1 or the Microsoft Active Directory server. Previous versions of the VPNmanager used the Netscape Directory Server 4.1. You must upgrade and migrate to either the Sun ONE directory server 5.1 or the Microsoft Active Directory server.

Before beginning, verify that the system requirements, including the updated service packs are installed. See “VPNmanager system requirements” on page 8.

Note: *When you upgrade from 3.0 or 3.1, the older versions of the VPNmanager console have to be uninstalled. Go to the Start menu, VPNware3 and uninstall the Console.*

Upon completing the upgrade, the previous version of VPNmanager can be uninstalled.

Upgrading from VPNmanager 3.3 or VPNmanager 3.4 to VPNmanager 3.5

To upgrade the VPNmanager from 3.3 or 3.4 to 3.5, select the **Complete** option from the *Setup Type* dialog box in the install wizard. The wizard upgrades the VPNmanager console, updates the directory server schema, and installs the policy server.

Before beginning, verify that the system requirements, including the updated service packs are installed. See "VPNmanager system requirements" on page 8.

Note: *When you upgrade from 3.0 or 3.1, the older versions of the VPNmanager console have to be uninstalled. Go to the Start menu, VPNware3 and uninstall the Console.*

Upon completing the upgrade, the previous version of VPNmanager can be uninstalled.

Upgrading Avaya VPNmanager for Solaris

VPNmanager 3.5 uses the Sun ONE directory server 5.1 or the Microsoft Active Directory server. Previous versions of the VPNmanager used the Netscape Directory Server 4.1. You must upgrade and migrate to either the Sun ONE directory server 5.1 or the Microsoft Active Directory server.

Before beginning, verify that the system requirements, including updated service packs are installed. See "VPNmanager system requirements" on page 8.

Upgrading from VPNmanager 3.2 to VPNmanager 3.5

1. Install the VPNmanager 3.5 console using the procedure in section "Installing VPNmanager console for Solaris" on page 16.
2. Update Schema using the procedure in "Updating the directory server schema for Solaris" on page 17.
3. After you have successfully upgraded, delete the old restart script file.

Note: *Users who are upgrading from VPNmanager 3.0 or 3.1, the older versions of the VPNmanager console has to be uninstalled.*

Confirming migration and choosing contexts

To confirm that the migration of database from your legacy server to VPNmanager 3.5 was successful and to choose the right context follow the steps below:

1. Launch the VPNmanager console.
2. Just before the console opens, you will see the *Select from Multiple Context List* following dialog.
3. Select the suffix that starts with “o=”. For example, if your domain is abc.com, than you would select suffix o=abc.com.

To make this context permanent do the following:

1. Go to **MainConsole>File>Logoff** and logoff the current policy server.
2. Choose the directory server and click **Edit**.
3. This opens the *Configure Server* dialog box. Click **Advanced**.
4. Click on **Add More Contexts**.
5. Add the context that you selected before, from the list of contexts.
6. Click **Close**. This context is now available in the Initial Context list.
7. Choose this context from the list and click **OK**.
8. Enter the password and connect to the directory server.

Upgrading from VPNmanager 3.3 or VPNmanager 3.4 to VPNmanager 3.5

1. Insert the VPNmanager CD into computer. When the *Overview* page opens, click **Installation** to go to the installation page.
2. When the *Introduction* dialog box appears, click **Next** to proceed.

   Note: *If the autorun does not start, navigate to the install program \\disk1\solaris\setup.bin. Double-click* ***install.bin*** *to open the Action - Run dialog box.*
3. Choose the folder location. Click **Next**.

4. When the *Setup Type* dialog box appears, select the **Complete or Custom** option. Click **Next**.

   The installation wizard upgrades the VPNmanager console, updates the directory server schema, and installs the policy server.

5. When the *Install Complete* dialog appears, click **Finish** to return to the Solaris desktop.

Note: *Users who are upgrading from VPNmanager 3.0 or 3.1, the older versions of the VPNmanager console has to be uninstalled.*

What next

After installing or upgrading Avaya VPNmanager, you can begin using the latest version of the VPNmanager. Refer to the Avaya VPNmanager Quick Installation Guide or the VPNmanager Configuration Guide.

Appendix A Installation Prerequisites for Microsoft Active Directory Server

Installing the Active Directory server snap-in

To install the Active Directory server snap-in:

1. Log in to the directory server as the administrator.
2. Insert the Windows 2000 Server compact disc into the CD-ROM drive. Click **Browse this CD**.
3. Double-click the **I386** folder.
4. Double-click **Adminpak** and follow the instructions that appear in the Windows 2000 Administration Tools Setup wizard.
5. Select **Install all of the Administrative Tools** option.

   Note: *If you do not have the Windows Server 2000 compact disc or if you run into problems using the CD, you can use a local version of Adminpak*

   Based on your Windows 2000 installation, the Adminpak could be present in C:\WINNT\System32
6. Double-click **Adminpak** to continue with the installation of all the administrative tools
7. Click **Start>Run**.
8. Enter **mmc /a** in the Open field. Click **OK**.
9. In the menu, select **Console** and click **Add/Remove Snap-in**. Click **Add**.
10. From Snap-in, double-click **Active Directory Schema**. Click **Close**.

11. When all snap-ins are added to the console, click **OK**.

12. From the Console menu, click **Save** and give the name as Active Directory Schema snap-in.

Extending the Active Directory schema

To extend the Active Directory schema:

1. Open Active Directory schema.

2. In the console tree, click the **plus sign (+)** to expand the hive.

3. Right-click Active Directory Schema, and click **Operations Master**.

4. Check to see if the schema can be modified in this domain controller. Click **OK**.

Troubleshooting for extending the Active Directory schema

- If you attempt to view or change the Operations Master, you may receive the following error message: “The server is currently offline.”

  Solution: To resolve this problem, first click the plus sign (+) to expand the hive, then connect the snap-in to the Operations Master. After the hive has expanded, you can connect to the Operations Master.

- Sometimes the Active Directory Schema Manager snap-in does not connect to the Operations Master and gives the following error:

  “Could not connect to the current schema master server. The server may not be available, or you may have insufficient privileges to manage the schema.”

  It's likely that the userid that you used to log on to the computer does not have the permissions to enable schema modification.

  Solution: Log on as the administrator and try the schema update procedure. Add the administrator to the schema admins group as detailed below.

Adding a member to the schema admins group

To add a member tot he schema admins group:

1. Open **Active Directory Users and Computers**.
2. In the console tree, double-click the appropriate domain node then click **Users**. Or click the folder that contains the desired user.
3. In the details pane, right-click the user account that you want to add, and click **Properties**.
4. Click the **Member Of** tab, and click **Add**.
5. In the Select Groups dialog box, click **Schema Admins**.
6. Click **Add**.

Note: *To open Active Directory Users and Computers, click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers.*

Increasing the number of entries returned by Active Directory

By default Active Directory returns only 1000 entries when a search is initiated by a third party. If you have more than 1000 entries, increase the result size to 5000.

To increase the number entries returned by Active Directory:

1. Install ADSI Edit. To use ADSI Edit, install the Support Tools that are located in the Support\Tools folder on the Windows 2000 Server operating system CD. To install the tools, double-click the Setup icon in that folder.
2. On the Start menu, point to Programs, Windows 2000 Support Tools, Tools, and then click ADSI Edit

3. This should display a tree with the Configuration Container and other branches

   If the Configuration Container is not displayed, right-click the ADSI Edit icon. Click **Connect to**.

   Under Connection Point, select Naming Context, select Configuration Container.

   Click **Advanced**. Check Specify Credentials and enter the Administrator userid and password.

4. Select **Configuration** container and navigate to the following:

   CN=Configuration, <dc=domainname>

   CN=Services

   CN=Windows NT

CN=Directory Service

CN=Query-Policies

CN=Default Query Policy

5. Right click CN=Default Query Policy. Select **Properties**.
6. From *Select a property to view*, select **IDAPAdminLimits**.
7. From *Values*, select **MaxPageSize=1000**. Click **Remove**.
8. From **Edit Attribute type**, select **MaxPageSize=5000**. Click **Add.**
9. Click **OK** to exit the properties dialog.

Enabling Secure Socket Layer (SSL)

Before you begin, verify the following:

- Installation of Windows 200 High encryption pack from http://www.microsoft.com/windows2000/downloads/recommended/encryption/
- Configuration of Certificate Services using Start>Settings>Control Panel>Add/Remove Programs>Add/Remove Windows Components

To enable SSL:

1. Go to Start>Programs>Administrative Tools. Select **Domain Security Policy**.
2. Navigate to Security Settings>Public Key Policies.
3. Right click Automatic Certificate Request Settings. Select New> Automatic Certificate Request.
4. Select Domain Controller from the list of certificate templates.
5. Select the Certificate Authority that you have configured.