Avaya VPNmanager® 3.7 Quick Installation Guide

System Requirements

Console Minimum System Requirements

- **MS Windows®**
  - -Microsoft Windows® 2000 with Service Pack 2 or later, or Windows 2003 operating systems
  - -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
- **Solaris™**
  - -Solaris™ 8 or 9 OE
  - -256 MB RAM
  - -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 Minimum System Requirements

- **MS Windows®**
  - - Microsoft Windows® 2000 Server; Advanced Sever with Service Pack 2 (X86) or later, or Windows 2003
  - - 256 MB RAM (up to 1 GB for best performance on large VPNs)
  - - 200 MB of free hard disk space for small VPNs; 2 GB for large VPNs
  - - CD-ROM drive
  - - VGA monitor
  - - 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
- **Solaris™**
  - - Solaris™ 8 or 9 OE
  - - 256 MB RAM (up to 1 GB for best performance on large VPNs)
  - - 200 MB of free hard disk space for small VPNs; 2 GB for large VPNs
  - - CD-ROM drive
  - - VGA monitor
  - - The DNS and Host name for the computer must be properly configured
  - - A static IP address must be assigned to the computer

To download the VPNmanager Configuration Guide, go to:
http://support.avaya.com
Click Product Documentation, go to VPN & Security link.

VPNmanager Components

VPNmanager console is a client 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 defines the structure and the type of configuration data.

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**.** Depending on the size of the network, the directory server and console may reside on the same or separate computers. Generally, with smaller networks, the directory server and console are installed on the same machine. In any case, the server must be installed on a high-end machine.

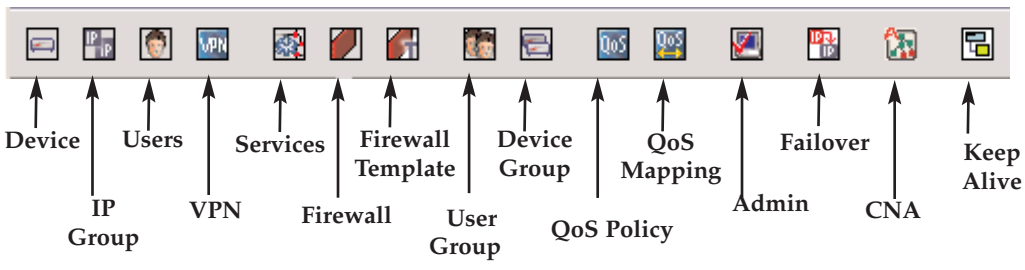
By default, read-only access to the directory server is allowed with an anonymous login. To disable, refer to the VPNmanager Installation Guide, “Removing the Anonymous Login” section.

Note: 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 Active Directory and the Sun ONE directory server 5.1, previously the iPlanet directory server. For additional installation information, refer to the VPNmanager Installation Guide.

Solaris User: The directory server is installed manually. Click the **Server Install** on the Avaya VPNmanager CDROM.

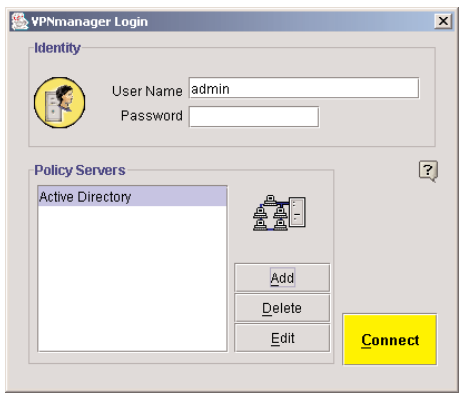
Icons

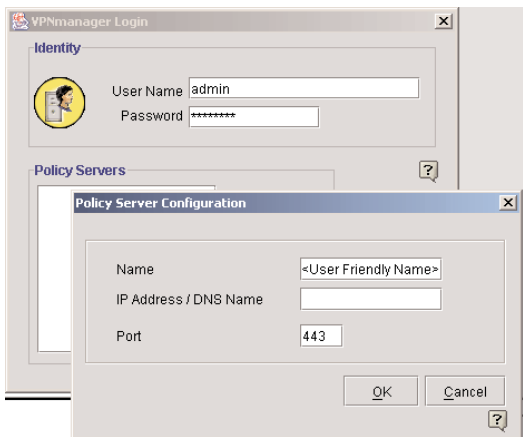
The icon toolbar on the main VPNmanager screen contains buttons that are shortcuts for the tasks on the menu bar and the Device Update button.



Configuring VPNmanager

1. Login VPNmanager





1. In the User Name field, type the administrator name, if it is not displayed.
2. Type the password that was configured when the VPNmanager software was installed.
3. The IP address or name of the policy server is listed in the policy servers list. Select the policy server, if it is not highlighted and click Connect to log into the server.

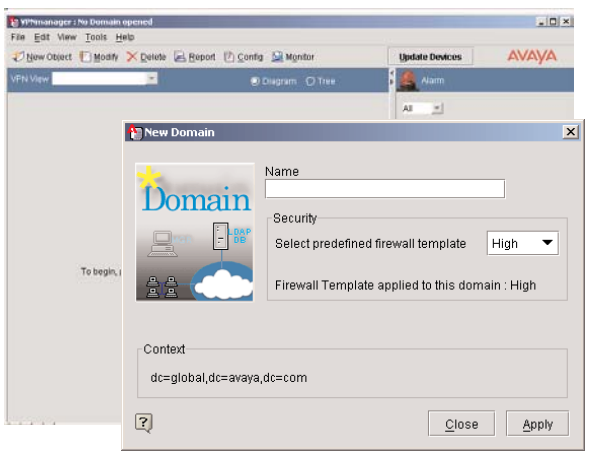
The policy server is installed during the installation process. The VPNmanager console communicates with the policy server to retrieve security policies. The policy server then communicates with the directory server.

4. From the VPNmanager Login dialog, click Add.
5. Enter a user-friendly name that identifies the policy server.
6. Enter the IP address of the policy server.
7. Enter the port. The default is 443.
8. Click OK. The name or address is displayed on the login screen.

You can edit or delete the policy server information.

 670-100-700, Issue 4

2. Create VPN Domain



1. Select File>Domain>New. The New Domain dialog is displayed.
2. Type a name for the domain. Names can be up to 255 characters and can use any characters, except a comma (,).

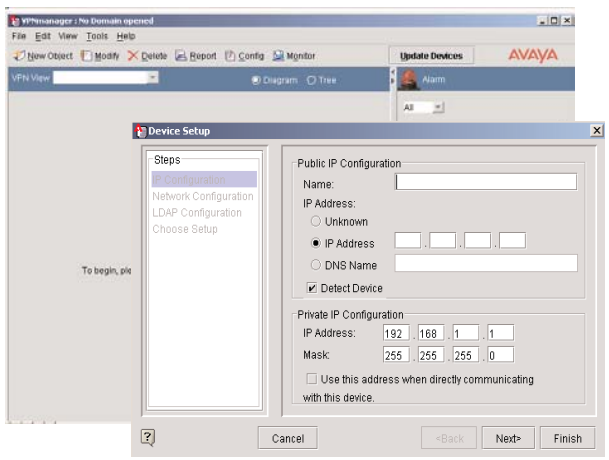
   All VPN components must have unique names. To prevent naming conflicts:

   Check the names of existing VPNs to avoid duplication.

   Use organization names (for example, World Wide Sales_Domain) since VPNs usually represent functional organizations within a corporation.

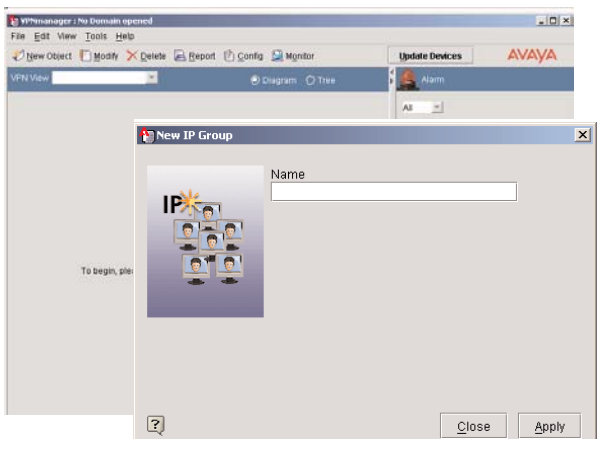
   Note: Once the domain name is created, you cannot change it.
3. In the Security text box, select the firewall template to be applied to this domain. For detailed information regarding the security policies included in this template, see Establishing security in the VPNmanager Configuration Guide.
4. Click Apply to create the domain.

3. Security Gateway Setup



1. Select New Object>Device. The Setup Wizard dialog is displayed.
2. In the Public IP Configuration section, enter the name of the new device and the public IP address. Click Next.
3. In the Authentication section, enter the device Superuser name and Password.
4. If the Detect Device checkbox is selected, VPNmanager attempts to contact the device and retrieve the device details. Select the device from the drop down menu in the Network Configuration screen.
5. If the Public Interface Uses a Dynamic (User VPN) IP Address checkbox is selected, enter the device serial number. Enter the Policy Server IP/DNS name and port where the Policy Server is running.
6. In the SNMP Configuration section, select the SNMP version and enter the SNMP community string name. The public community string is the default.
7. In the Static Route section, click Configure Static Route to configure the static route destination address. Select Add to enter the IP address of the Next Hop for the static route. Click OK. Click Next.
8. Select either Setup Now or Setup Later. Setup Now send the configuration information to the directory server and the security gateway. Setup later sends the configuration information to the directory server only. Click Finsih.

4. New IP Group



1. Select New Object>IP Group. The New IP Group dialog is displayed.
2. Type a name for your new IP Group. Any characters can be used, except a comma [,]. Click Apply.

   A good practice is to incorporate identifiers in a name so they can be easily managed. For example, a LAN used by an accounting department in San Francisco that is made into an IP Group can be named SF Accounting LAN. Using this scheme clearly identifies who are the members of an IP Group.
3. Click Close to go to the Configuration Console window.

   Your new IP Group appears in the Contents column.
4. Click Save.

   After an IP Group is created, use the General and Memo tabs to configure it.

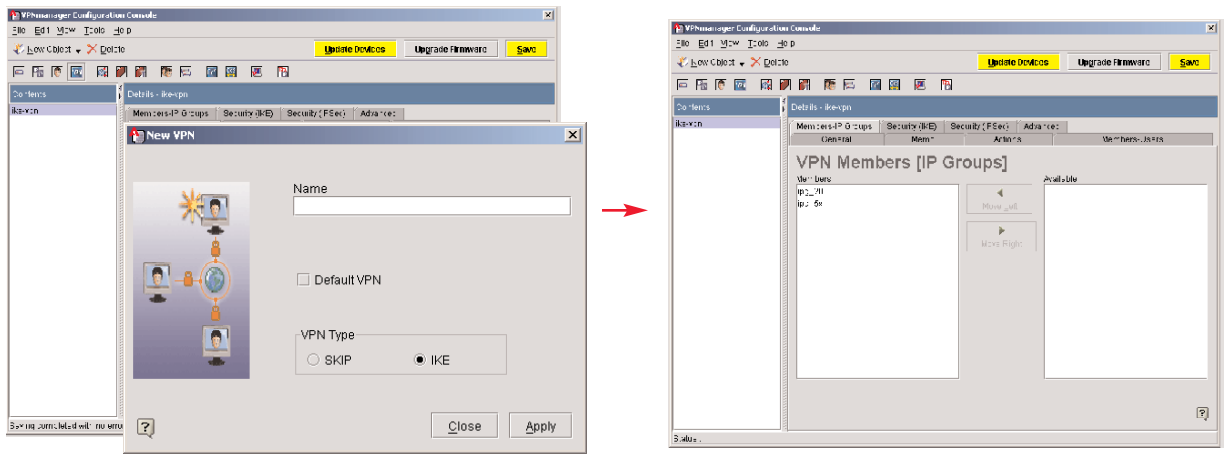
5. New User*

1. Select New Object>User. The New User dialog is displayed.
2. Type the name of a remote user. Any character, except a comma can be used.

   Note: If you plan on using RADIUS as an authentication method, this name must match the name used in the RADIUS server.
3. Type the user password for the local, RADIUS, and directory servers.
4. Confirm the password.
5. Click Apply to save the user name.
6. Click Close to go to the Configuration Console window. Your new IP Group appears in the Contents column. Click Save.

*A user is a person using the VPNremote Client software.

6. New VPN



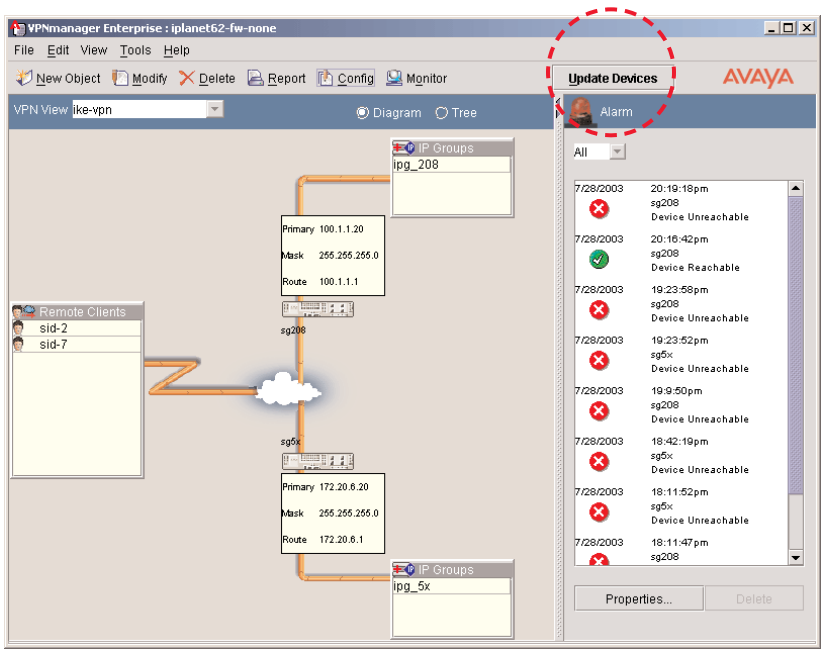
1. Select New Object>VPN. The New VPN dialog is displayed.
2. Type in a name for your new VPN Object. Any characters can be used, except a comma [,].
3. From the VPN Type options, do one of the following:

   Select SKIP to create a SKIP VPN Object.

   Select IKE to create an IKE VPN Object.
4. Click Apply to create the object. Click Close. The Configuration Console appears and the details pane displays a series of tabs.
5. If you want to create another object, repeat step 2 and step 3.
6. Click the Member-IP Groups tab to bring it to the front.
7. Associate the members to the new VPN. Use the Move Left and Move Right buttons to associate the selected members to the VPN.
8. Click Save on the Configuration Console.

*For Default VPN, see the VPNmanager Configuration Guide, *Creating a VPN Domain*.

7. Update Devices



The Update Devices button is located in the upper right-hand corner of the VPNmanager Console window. Click the Update Devices button whenever changes are made to the VPN.

To update the security gateways:

1. Make the changes to the VPN.
2. Click Update Devices to open the Update Devices dialog box.
3. From the list of security gateways, select the security gateway you want to update.
4. Click OK to view the status of the update.

If the Update Configuration dialog box appears, do the following:

1a. In the User Name text box, type in the SuperUser name you configured through the Quick Setup menu when the device was installed. If the device is running VPNos (VPN operating system) 3.X, type in root.

2a. In the Password text box, type in the SuperUser password configured at the security gateway Console Quick Setup Menu when the SG was installed.

If the security gateway had a firmware upgrade from 3.X and above and had an existing security gateway Console password, type in that password.

If the security gateway did not have an existing security gateway console password, type in "password".

3a. Click OK. The Update Devices dialog box will tell you when the update is completed.

 670-100-700, Issue 4