VPNremote Client 4.1
Administrator’s Guide

June 2002
Licenses, Warranties, Copyrights, and Trademarks

THE SPECIFICATIONS REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

SOFTWARE LICENSE

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE SOFTWARE. BY USING THIS SOFTWARE YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE, PROMPTLY RETURN THE UNUSED SOFTWARE, MANUAL, AND RELATED EQUIPMENT AND HARDWARE (WITH PROOF OF PAYMENT) TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Avaya and its suppliers grant to Customer (Customer) a nonexclusive and nontransferable license to use the VPNremote Client software (Software) in object code form solely on a single central processing unit owned or leased by Customer or otherwise embedded in equipment provided by Avaya, except as provided below.

Avaya and its suppliers grant to Customer a nonexclusive and nontransferable license to copy and use the VPNremote Client software for Windows (Client Software) in object code form a specified number times based upon the product Customer purchased.

Customer may make one (1) archival copy of the software provided Customer affixes to such copy all copyright, confidentiality, and proprietary notices that appear on the original. EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, CUSTOMER SHALL NOT: COPY, IN WHOLE OR IN PART, SOFTWARE OR DOCUMENTATION; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE SOFTWARE.

Customer agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Avaya. Customer agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Avaya. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with Avaya.

This License is effective until terminated. Customer may terminate this License at any time by destroying all copies of Software including any documentation. This License will terminate immediately without notice from Avaya if Customer fails to comply with any provision of this License. Upon termination, Customer must destroy all copies of Software.

Software, 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 Software.

This License shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Avaya software.
Restricted Rights - Avaya’s software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph ‘C’ of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the government’s rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202.

**LIMITED WARRANTY**

Software. Avaya warrants that for a period of ninety (90) days from the date of shipment from Avaya: (i) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (ii) the Software substantially conforms to its published specifications. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to Customer as the original licensee. Customer’s exclusive remedy and the entire liability of Avaya and its suppliers under this limited warranty will be, at Avaya or its service center’s option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to the party supplying the Software to Customer. In no event does Avaya warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.

Restrictions. This warranty does not apply if the product (a) has been altered, except by Avaya (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Avaya, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultrahazardous activities.

**DISCLAIMER OF WARRANTY.** EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL Avaya OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT EVEN IF Avaya OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Avaya’s or its suppliers’ liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

VPNware, VSU, VPNmanager, VPNremote, VPLink, VPNos, and Avaya are trademarks belonging to Avaya. MD5 Message Digest Algorithm Copyright RSA Data Security, Inc. All other product names mentioned in this manual are trademarks or registered trademarks of their respective manufacturers.
Table of Contents

Chapter 1 — Introduction

VPNremote Features ........................................ 1-1
Functional Overview ........................................ 1-4
    VPNremote Main Console ............................ 1-4
    User Profile Manager .............................. 1-5
    Certificate Manager ............................... 1-6
    SmartCard Manager ............................... 1-8
    Log Details ......................................... 1-9

Chapter 2 — Pre-Configuration and Distribution

Installation and Configuration Choices ....................... 2-1
The Initialization File .................................... 2-1
    Editing the Initialization File .................. 2-3
Distributing VPNremote to the Remote Users ............... 2-12
Information Required by Remote Users .................... 2-12

Chapter 3 — Installation

Installing VPNremote ..................................... 3-2
Uninstalling VPNremote ................................. 3-5

Chapter 4 — VPNremote Main Console

Pre-Configuring VPNremote ............................... 4-1
Establishing a Remote Connection using a Non Certificate-Based User Profile .......................... 4-2
Establishing a Remote Connection using a Certificate-Based User Profile .......................... 4-3
    To Change the Cryptographic Module Password .. 4-5
VPNremote Taskbar Icon .................................. 4-8
    Before Connecting to VPNremote ................ 4-9
    After Connecting to VPNremote .................. 4-9
Preferences ................................................. 4-10

Chapter 5 — Profile Manager

Adding a User Profile .................................... 5-2
Viewing or Modifying a User Profile ..................... 5-2
Deleting a User Profile .................................. 5-5
Chapter 6 — Profile Manager Wizard

Create a Typical User Profile ......................... 6-1
Create a Custom User Profile ......................... 6-3
Choose Configuration Method ......................... 6-4

Chapter 7 — Monitoring

Event Log Details Viewer ......................... 7-1
Set Log Level ........................................ 7-2
Select Log Destinations .......................... 7-2
Configuration Statistics ......................... 7-3
Session Security Associations (SA) ........... 7-4

Chapter 8 — Certificate Manager

Importing a Signing Certificate ................... 8-2
Acquiring a Personal Certificate ................... 8-3
Online Certificate Request ......................... 8-4
File-based Certificate Request .................... 8-5
Maintaining a List of Valid Certificates ............ 8-7
Verifying a Certificate ............................. 8-7
Viewing Certificate Details ......................... 8-8
Deleting an Invalid Certificate ..................... 8-8
Selecting a Default Certificate ..................... 8-9
Exporting a Signed Certificate ..................... 8-9

Chapter 9 — SmartCard Manager

Adding a Cryptographic Module ................... 9-2
View Cryptographic Module ......................... 9-3
Deleting a Cryptographic Module .................. 9-4

Appendix A — VPNremote Client Software Installation Checklist

Appendix B — Troubleshooting
1 Introduction

The need to provide secure remote access over public networks has produced a succession of network access and security technologies. Typically, these technologies have proven to be costly to deploy, scale, and manage, as well as, complex for the typical end user. The complexity of secure remote access has placed an undue strain on already taxed information technology and end user technical support staffs. Due to the strain on specific departments within an organization, secure remote access adoption and deployment occurs at a slow rate.

VPNremote Client overcomes the complexities typically faced when deploying a secure remote access solution. VPNremote Client eases the burden faced by Network Administrators when distributing, configuring, and managing a VPN remote access solution. VPNremote provides advanced capabilities such as Dyna-Policy™ dynamic configuration of VPN and security policy information at the client software, comprehensive system-level integration with public key infrastructure (PKI) systems, and simple User-Profile-based operation. Together, these features provide a client software environment that overcomes difficulties commonly encountered in deploying and supporting IPSec VPN secure remote access.

VPNremote Features

The following summarizes a number of significant feature, performance, and usability enhancements provided by VPNremote Client.


- **Integration with Microsoft Dial-up Networking** – VPNremote’s main console window allows the remote user to connect to a VSU using a network adapter or dial-up modem configured on the user’s PC. All dial-up networking connections that have been defined within the Windows Dial-Up Networking utility are made available by VPNremote through a drop-down selection menu. Selecting a dial connection launches the modem that enables network connectivity and VPN authentication to be performed as a single, unified log-on step.
■ **IP Softphone** – VPNremote creates a secure VPN dial-up networking connection. Use VPNremote and IP Softphone to establish a secure VPN dial-up connection to dial the call securely. For more information about the IP Softphone, refer to the *Definity IP Softphone* documentation.

■ **IKE (Internet Key Exchange) Protocol Support** – VPNremote supports the standard IKE key management protocol for IPSec. For additional information on IKE Protocol Support, see the *VPNmanager Administrator’s Guide*.

■ **NAT Traversal** – Beginning with VPNremote 4.1, VPNremote Client supports remote users behind a PNAT device. In order for this feature to function correctly, the VSU the remote user is connecting to must be running VPNos 3.2. With this feature, VPNremote Client will initiate IKE negotiation on a port other than Port 500. This type of initiation will avoid any conflicts with IPSec Pass-through on Port 500.

■ **Broad Support for PKI (Public Key Infrastructure)** – VPNremote provides standards-based support for all major PKI vendors. All certificate management and usage functions are implemented locally in VPNremote, thus eliminating dependencies on third-party tool kits offered by the various PKI vendors that can introduce proprietary dependencies on their products.

■ **User Profile Management Utility** – The VPNremote graphical user interface (GUI) provides a User Profile management utility that bundles digital certificate and private key, VPN connection configuration parameters, and Public Key Infrastructure (PKI) integration parameters into one unified file format. To launch a VPN session, the remote user need only to select the desired profile and enter a user password. The User Profile is exportable as a file that enables remote users to access their network resources from any PC hosting VPNremote software.

■ **Certificate Life-Cycle Management Tools** – VPNremote offers a full-featured, GUI-based utility for end-user certificate life-cycle management. It allows users to easily and intuitively get and use digital certificates as an IPSec and user authentication enabling technology. The VPNremote Certificate Manager provides users with a pre-configured environment which they can get, securely store, and use RSA private keys and digital certificates.

■ **SmartCard Enabled** – VPNremote provides standards-based support for smartcards to store and protect RSA keys and digital certificates. A SmartCard Manager utility enables users to easily install and use smartcard devices.

■ **Dynamic Client Configuration** – VPNremote retains and extends the utility of the two-stage configuration process used in earlier releases. An initialization file coupled to the install package has been extended to allow an administrator to pre-configure all VPN connection profile parameters required to enable the remote user to: (1) contact a VSU, (2) get authenticated to receive a Client Configuration Download (CCD), and (3) generate Certificate
requests and then submit them to a Certificate Authority. CCD dynamic client configuration protocol Dyna-Policy™ provides a hands-off procedure that dynamically configures VPN policy in the remote user software with no interaction on the part of the user required.

- **User Authentication** – The remote access authentication process in VPNremote is a two-step procedure that first uses local authentication, RADIUS, SecurID, or LDAP to secure the delivery of VPN configuration information from the VSU, and then offers the option of using digital certificates within IPSec to provide a second, strong two-factor authentication. Though the second step is operationally transparent to the end user, it is optional and can be bypassed when pre-shared secrets are used as the security seed for the IKE key management protocol.

- **Next Token/New Pin Mode** – Remote-user Dyna-Policy™ configuration download authentication is supported for RADIUS or LDAP authentication servers. The RSA Security ACE/Server is supported via RADIUS proxy for SecurID authentication. Next Token and New Pin modes are supported.

- **Traffic-Driven IPSec Tunneling** – IPSec tunnels are built only on an as-needed basis or IPSec tunnels are configured. If configured, VPNremote will build a secure tunnel at start-up. Sessions are established with the VSUs only as traffic flow requirements dictate. VPNos retrieves the user’s complete set of VPN policy configuration information from either the VPNmanager LDAP directory server or from the local VSU database and provides a comprehensive configuration download at the time the initial CCD authentication is processed.

- **Configurable ‘Split-Tunneling’ Option** – The VPNmanager application allows the Network Administrator to control dual access to the Internet and a VPN connection by providing the ability to deny split-tunneling access to an individual user. When this option is employed, only VPN traffic will be allowed into and out of the remote user’s PC while VPNremote is active, all non-VPN traffic is dropped.

- **Comprehensive Event and Error Logging** – Enhanced event-logging features in VPNremote provide a GUI-based tool to view events filtered by a combination of priority and type. Events can be optionally logged to a Syslog server and/or saved to a local file.

- **Detailed Error Messaging** – The VPNremote GUI provides a comprehensive array of error messages designed to help the user intuitively detect the cause of authentication, configuration management, and IPSec tunneling problems.

- **Taskbar Icon** – The VPNremote GUI taskbar icon provides users with a single location to perform a variety of tasks. The taskbar icon tasks include: establishing a secure VPN connection, configuring user preferences, generating diagnostic reports, and connecting to a Customer Care website for customer support. The taskbar icon also displays for colors indicating the state of the VPN connection.
Chapter 1

Functional Overview

VPNremote Client includes the following five functional modules:

- VPNremote Main Console
- User Profile Manager
- Certificate Manager
- SmartCard Manager
- Log Details

VPNremote Main Console

The primary purpose of the Main Console window (Figure 1-1.) is to allow the remote user to establish a VPN connection. In the simplest case for a remote user to establish a secure network connection, the remote user only needs to enter their name, password, and click Connect. For a remote user to establish a secure dial-up connection, the remote user needs to enter their name, password, select an Internet Connection from the Options\Internet Connection drop-down menu, and click Connect. This is assuming that the Network Administrator has pre-configured the user’s Default Profile prior to distributing the VPNremote software to the user, and pre-shared secret VPNs are used.

When the VPNremote Client contacts a VSU over an SSL connection, an initial user ID and password authentication challenge is presented to the remote client. The response is authenticated by the VPNos, which then automatically configures the VPNremote Client with real-time configuration information. This process serves to identify the remote user for the purpose of distributing policy information; however it does not yet allow the remote user to access any of the network resources protected by the VPN.

For pre-shared secret VPNs, all the information required to build an IPSec tunnel is provided as part of the configuration. For certificate-based VPNs, an additional authentication step is performed at the time a remote user tries to access VPN resources. This second authentication step takes place within the scope of the IKE/IPSec tunnel management negotiations. In the initial phase of the IKE key management protocol, both ends of an IPSec tunnel negotiation must exchange certificates and a signed response. This information is used to authenticate each party and also to negotiate a session key for encrypting the data passing through the tunnel.

The Main Console window also includes an Options button and Advanced button that allow the remote user to open the User Profile Manager, Certificate Manager, SmartCard Manager, and Log Details.
Introduction

User Profile Manager

The User Profile Manager (Figure 1-2.) simplifies the configuration of all VPN connection parameters. When the software is installed, the Default User Profile is pre-configured with information provided in the initialization file (VPNREMOTE.INI) that is required to contact a VSU, and to get authenticated for a Dyna-Policy™ VPN policy configuration download prior to distributing VPNremote to the user. The user is only required to enter a username and password.
Figure 1-2. User Profile Manager

The Advanced features in the Profile Manager are used to configure the parameters required to generate and submit certificate requests to a PKI. All parameters in this window, excluding the username, certificate name, and users e-mail address, can be pre-configured for the Default User Profile by the Network Administrator prior to installation.

The remote user can create new user profiles or modify existing profiles as required. Additionally, export and import functions are included in the User Profile Manager that allow the remote user to save a selected User Profile to a file that can be later imported onto another system with VPNremote software.

Certificate Manager

One of the primary challenges in deploying digital certificate-based IPSec client software is the process of requesting, retrieving, and managing the life-cycle of remote user keys and certificates. The Certificate Manager (Figure 1-3.) addresses this challenge by providing a comprehensive set of
Introduction

capabilities to seamlessly integrate VPNremote with all major PKI vendors for the purpose of enrolling, distributing, and managing private keys and certificates. The Certificate Manager also provides the capability to store and manage keys and certificates on external devices such as smartcards.

The first step in providing certificates to remote users is the key generation process. VPNremote supports both centralized and distributed PKI system architectures. The user keys can be generated centrally by a security administrator and delivered to the users, or the users can generate their own keys and submit the request for certification with the aid of the intuitive and easy to use Certificate Manager.

Centrally generated keys and certificates can be distributed to end users as an import file or on a SmartCard. In either case, the users do not get involved in the processes of generating keys or submitting certificate requests. This flexibility allows organizations with highly-centralized security administration to use PKI in a way that mirrors their current security practices while at the same time eases the burden faced by end users in getting started as remote access users.

For organizations with a more stringent security policy that requires an end user to be the only person ever to have possession of their private key, the Certificate Manager provides a utility that enables the generation of keys as well as the submittal of certificate requests to a Certificate Authority. Both CRS (Certificate Request Syntax) on-line enrollment and PKCS#10 file-based enrollment are supported.

The Certificate Manager has been designed to make the request and submittal processes very simple. The typical usage of this utility will require the user to supplement pre-configured PKI integration information by entering little more than a user ID and e-mail address.
SmartCard Manager

The SmartCard Manager (Figure 1-4.) maintains a list of Cryptographic Modules which provide access to smartcards and software tokens present in the local database.
Log Details

To assist in isolating problems that may occur, VPNremote includes an event logging and viewing utility. The log details are captured during operation and written to a local file. The Log Details viewer (Figure 1-5.) allows the user to filter and view the file by event status (level of importance) and type (functionality affected). This allows help desk personnel to quickly guide users in providing the exact data required to diagnose and solve VPN operation problems.
VPNremote can be configured through the Advanced User Profile window to automatically send log messages to a Syslog server. This allows an administrator to monitor performance and troubleshooting for all users on a specific workstation.

Figure 1-5. Log Details

VPNremote can be configured through the Advanced User Profile window to automatically send log messages to a Syslog server. This allows an administrator to monitor performance and troubleshooting for all users on a specific workstation.
The principal challenge faced by organizations when deploying a remote access VPN solution is the ease with which the average end user can install, configure, and use the client software.

VPNremote employs a server-based distribution model that allows Network Administrators to pre-configure and distribute VPNremote to the end users over the Internet (via ftp, http, or email) or on a portable storage medium (diskettes or CDs). VPNremote works with all Windows operating systems, including Windows98, Windows2000, WindowsNT, Windows ME, and Windows XP.

Installation and Configuration Choices

To aid the remote users in installing and configuring the VPNremote Client software, Network Administrators can either pre-configure the VPNremote initialization file (VPNREMOTE.INI) or provide the information required by the remote users in written form as summarized below:

- Distribute the VPNremote self-extracting installer file to remote users. Note that this installer uses the default initialization file (VPNREMOTE.INI). In this case, Network Administrators must provide instructions and information required by remote users to configure their VPNremote Client.

- Customize the remote configuration by editing the VPNREMOTE.INI file, located in VPNremote folder on the VPNremote Client CD, then package the installation files either on a server or portable medium for distribution. This option minimizes the remote users involvement in getting VPNremote installed and configured correctly.

The Initialization File

The VPNremote Client software contains an initialization file (VPNREMOTE.INI) used to pre-configure VPNremote to connect to a VSU and authenticate the user to receive a dynamic VPN policy configuration download, as well as to provide ready-to-use integrated PKI (Public Key Infrastructure) support. Information contained in the initialization file (VPNREMOTE.INI) will be used to automatically configure the default user profile during installation on the remote user’s system. This allows
VPNremote users to easily install VPNremote without needing to interpret or understand the broad range of parameters involved to support remote connections with the IPsec tunneling protocol.

To customize the initialization file, copy the VPNremote directory and its contents from the VPNremote Client CD to your hard disk. Using a text editor, edit the VPNREMOTE.INI file, located in the VPNremote folder. The VPNREMOTE.INI file is a self-documented file organized in the following sections:

- **Install** – Includes information that is used to install the VPNremote Client in a predetermined and predictable manner.
- **System** – Specifies which user name to display in the User Name field on the VPNremote Main Console and authentication method for the Default User Profile.
- **Download** – Sets the IP address, and port number for the VSU used to download client configuration information for the Default User Profile.
- **Config** – Set the IP address, primary WINS, secondary WINS, primary DNS, and secondary DNS for the default network.
- **Certificate** – Includes parameters to be set only if the remote users are expected to obtain their user certificates from a designated PKI. This information is used to pre-configure the Certificate Request Profile in the Advanced section of the Default User Profile.
- **Log** – Determines where to send log messages for the Default User Profile. Log messages can be stored locally on the user’s PC and/or sent to a Syslog server at a specified IP address and port number.
- **Binding** – Includes network adapters that are not supported by VPNremote. The adapter name is the network adapter as shown in Network Properties.
- **Preferences** – Includes parameters that allow the Network Administrator to modify VPNremote behavior when a successful connection is established using Windows 2000, Windows NT, or Windows XP.

*Note:* The section titles are required. Do not remove or alter the section title while editing the VPNREMOTE.INI file.

When you have finished editing the VPNREMOTE.INI file, save the file in text-only format, then refer to Distributing VPNremote to the Remote Users on page 12 for additional instructions.
Editing the Initialization File

**Install**

**DefaultIniLocation**

**Default:** WINDOWS
This value sets the default location of the ini file. If the Network Administrator modifies the default location, the full directory path for the VPNREMOTE.INI file must be specified. VPNremote installation reads other parameters from the VPNREMOTE.INI file based upon the location.

**Default location:**

- Windows NT, Windows 2000, and Windows XP
  `\SystemRootDrive\WINNT`
- Windows 98 and Windows ME
  `\SystemRootDrive\WINDOWS`

**ReadLicenseAndIAgree**

**Options:** YES | NO **Default:** NO
If this value is set to YES, the user will be prompted to read and agree with the VPNremote license. Otherwise set this variable to NO.

**Custom**

**Options:** YES | NO **Default:** NO
If this value is set to NO (recommended), default values will be used for the variables InstallDir, Folder, and ViewReadme. If this value is set to YES, the these values must be set individually: InstallDir, Folder, and ViewReadme.

* **Note:** The Reboot parameter is independent of this parameter.

**Reboot**

**Options:** YES | ASK **Default:** ASK
If this value is set to ASK, you will be given an option to reboot after installation. If this value is set to YES, the target machine will reboot automatically after installation.

* **Note:** Reboot is not required on Windows 2000. If this value is set on Windows 2000, it will be ignored.

**DefaultInstallDir**

**Options:** YES | ASK **Default:** YES
If this value is set to YES, VPNremote will be installed in the Windows Program Files. If this value is set to ASK, the user will be prompted to choose a different installation path.
If the Custom parameter is set to **NO**, the DefaultInstall Dir value will be ignored.

**DefaultFolder**

**Options:** YES | ASK **Default:** YES
If this value is set to **YES**, VPNremote will use the default installation folder. If this value is set to **ASK**, you will be prompted with a dialog box to choose a different installation folder.

If the Custom parameter is set to **NO**, the DefaultFolder value will be ignored.

**ViewReadme**

**Options:** YES | NO | ASK **Default:** ASK
If this value is set to **YES**, the Readme file will open during installation. If this variable is set to **NO**, the Readme file will not open. If this variable is set to **ASK**, you will be prompted to view the Readme file.

If the Custom parameter is set to **NO**, the ViewReadme value will be ignored.

* **Note:** The Readme file can be copied to target machines for future reference.

**SupportURL**

**Default:** support.Avaya.com
The value sets the internet address for the technical support website.

**System**

**ResetoldProfiles**

**Options:** YES | NO | ASK **Default:** NO
If this value is set to **YES**, VPNremote will overwrite the existing Profile during upgrade. The VPNremote user will have to reset their Profiles. If this value is set to **NO**, VPNremote will not overwrite the existing Profile during upgrade. The VPNremote user’s existing Profiles will be retained during installation. If this value is set to **ASK**, VPNremote will prompt the user to overwrite or retain the existing Profiles during upgrade.

**NoOfProfiles**

**Value Options:** 1 to 8 Profiles **Default Values:** 1
If this value is set to 1, the Administrator enters the Profile information in the [Profile1] section only. If this value is set to **N**, the Administrator enters the Profile information in the [ProfileN] section.

Beginning with VPNremote Release 4.1, there are three profile sections (Profile1, Profile2, and Profile3) in the ini file. If additional profiles are
required, create additional profiles sections within the ini file. Be sure to name the new Profiles a unique number (Profile4, Profile5, Profile6).

**UserName**

**Default:** Actual Name
This value sets the actual user name assigned to the remote user in the Default User Profile. The Default User Profile specifies the user name that displays in the User Name field in the VPNremote Main Console.

**Authentication**

**Options:** CHAP | PAP **Default:** CHAP
This value specifies the authentication method to use for the Default User Profile. The method chosen is dependent on the type of authentication used by the RADIUS server. If your RADIUS server uses CHAP (Challenge-Handshake Authentication Protocol) or you are not using a RADIUS server, set this variable equal to CHAP. If the RADIUS server uses PAP (Password Authentication Protocol), set this variable to PAP.

* **Note:** This value is read only during installation. To change authentication type after installation, use the Advanced button in the authentication dialog box.

**LDAP**

**Options:** YES | NO **Default:** NO
If this value is set to NO, the Profile Manager Wizard will not prompt the user for a DNS Suffix when VPNremote is launched for the first time. If this value is set to YES, the remote user will be prompted to enter a DNS Suffix for Directory Server (LDAP) authentication.

**VPNmanagerSuffix**

Set this value equal to the Administrative Domain in the VPNmanager Directory Server where the VPN policy information resides. This value is used during remote user authentication. The remote user enters the Common Name value and the suffix is appended. This value will be ignored if the LDAP value is set to NO.

**Download**

By setting the following parameters with valid values, VPNremote will automatically download the specified configuration when VPNremote is initially launched. If automatic configuration download is not specified, the remote user will be prompted to download or import the specified configuration.

**VSUIPAddress**

Set the VSUIPAddress to the IP address or the DNS of the Avaya VPNware Service Unit.
Port

Set the Port value to 1443. This is the port value used for the VPNremote Client to connect to the VSU. Changing this value requires all remote users on the VPN to change the port value in their user profile.

BackUpVSUAddress

Set the BackUpVSUAddress to the IP address or the DNS name of the secondary or backup Avaya VPNware Service Unit. This value will be used if the primary VSU is unavailable.

Config

By setting the following parameters with valid values, VPNremote will automatically download the specified network configuration for the virtual adapters when VPNremote is initially launched.

IPAddress

Set this value equal to the IP address of the VSU that the remote user will be using for CCD (Client Configuration Download).

Subnet Mask

Set this value equal to the subnet mask of the VSU that the remote user will be using for CCD (Client Configuration Download).

PrimaryWINS

Set this value to the address of the primary WINS server that is protected by the VSU the remote user will connect to.

SecondaryWINS

Set this value to the address of the secondary WINS server that is protected by the VSU the remote user will connect to.

PrimaryDNS

Set this value to the address of the primary DNS server that is protected by the VSU the remote user will connect to.

SecondaryDNS

Set this value to the address of the secondary DNS server that is protected by the VSU the remote user will connect to.

Certificate

EnableCertificateSupport

Options: YES | NO  Default: NO
If this value is set to NO, the values for CommonName and DNSuffix will
be ignored. If this value is set to **YES**, the remote user will need a personal certificate to authenticate to the VSU.

**CommonName**

In most cases the Common Name should be the same as the User Name assigned to the remote user through the VPNmanager. The Network Administrator may choose to leave this variable blank and let the remote users enter their specific common name in the Advance section of the User Profile.

**OrganizationUnit, CompanyName**

Set these two variables equal to the organization unit (e.g., division, department, etc.) and company name of the remote users.

**RAName**

Set this variable equal to the name of the PKI system Registration Authority (RA) that will be used to process on-line certificate requests. Contact your PKI Administrator for instructions concerning the configuration and usage of the RA. This variable should be left blank for file-based certificate requests.

**CA_URL**

Set this variable equal to the URL of the Certificate Authority (CA) that will be processing online certificate requests for your organization. This variable should be left blank for file-based certificate requests.

**EMail**

This variable specifies the email address that is used to notify the remote users that their certificate requests have been processed. The Network Administrator may choose to leave this variable blank and let the remote users enter their specific email address in the Advance section of the User Profile.

**Locality**

This variable specifies the locality used to uniquely identify the remote users in the Certificate Authority database. The Network Administrator may choose to leave this variable blank and let the remote users enter their specific locality in the Advance > Certificate section of the User Profile.

**State**

This variable specifies the State used to uniquely identify the remote users in the Certificate Authority database. The Network Administrator may choose to leave this variable blank and let the remote users enter their specific locality in the Advance > Certificate section of the User Profile.
Country

This variable specifies the Country used to uniquely identify the remote users in the Certificate Authority database. The Network Administrator may choose to leave this variable blank and let the remote users enter their specific locality in the Advance > Certificate section of the User Profile.

Log

LogToLocalFile

Options: YES | NO Default: YES
To configure the Default User Profile to send log information to a local log file in the VPNremote folder, set this variable equal to YES.

LocalLogFileMaxSize

Default: 1024 (1K byte)
Set this variable equal to maximum size allowed for the local log file in 64K byte increments. When the maximum size is reached, the log file is backed up and flushed.

LocalLogFileLogLevel

Default: 0 (LOW)
This variable sets the priority level of messages sent to the event log destination. Message priority levels are listed in ascending order as follows:

- 0– LOW: Includes error messages. Error messages include notification that VPNremote could not establish a VPN connection.
- 1– MEDIUM: Includes information messages.
- 2– HIGH: Includes error messages and debug messages used only for troubleshooting purposes.

For example, if the priority level is set to 1, all warning and error condition messages (levels 0 and 1) will be logged. Debugging messages (level 2) will not be logged.

LogToSysLogServer

Options: YES | NO Default: NO
To configure the Default User Profile to send log information to a Syslog Server, set this variable equal to YES.

SysLogIPAddress

If LogToSysLogServer=YES, set this variable equal to the IP address or DNS name of the Syslog Server.
SyslogPort

If LogToSysLogServer=YES, set this variable equal to the port number of the Syslog Server. Default value = 514.

Binding

The following sections contains the list of network adapters that are not supported by VPNremote. The adapter name is the network adapter as shown in Network Properties. The action specifies the necessary user action.

AdapterName#1

* Note: Check Network Properties for exact adapter name.

Action: IGNORE | ASK Default: IGNORE
If this value is set to IGNORE, VPNremote will not bind to this adapter. If this value is set to ASK, the user will be prompted to ignore or bind to the adapter.

AdapterName#2

* Note: Check Network Properties for exact adapter name.

Action: IGNORE | ASK Default: IGNORE
If this value is set to IGNORE, VPNremote will not bind to this adapter. If this value is set to ASK, the user will be prompted to ignore or bind to the adapter.

AdapterName#3

* Note: Check Network Properties for exact adapter name.

Action: IGNORE | ASK Default: IGNORE
If this value is set to IGNORE, VPNremote will not bind to this adapter. If this value is set to ASK, the user will be prompted to ignore or bind to the adapter.

AdapterName#4

* Note: Check Network Properties for exact adapter name.

Action: IGNORE | ASK Default: IGNORE
If this value is set to IGNORE, VPNremote will not bind to this adapter. If this value is set to ASK, the user will be prompted to ignore or bind to the adapter.

AdapterName#5

* Note: Check Network Properties for exact adapter name.

Action: IGNORE | ASK Default: IGNORE
If this value is set to IGNORE, VPNremote will not bind to this adapter. If
this value is set to ASK, the user will be prompted to ignore or bind to the adapter.

Preferences

The following parameters allow the Network Administrator to modify VPNremote behavior when a successful connection is established using Windows 2000, Windows NT, or Windows XP.

ResetPreferences

**Options:** YES | NO | ASK  
**Default:** NO
If this value is set to YES, VPNremote will overwrite the existing Preferences during upgrade. The VPNremote user will have to reset their Preferences. If this value is set to NO, VPNremote will not overwrite the existing Preferences during upgrade. The VPNremote user's existing Preferences will be retained during upgrade. If this value is set to ASK, VPNremote will prompt the user to overwrite or retain the existing Preferences during upgrade.

ShowExpandedLoginDialog

**Options:** YES | NO  
**Default:** NO
If this value is set to YES, VPNremote displays the Login Dialog Box in the expanded state. If this value is set to NO, VPNremote displays the Login Dialog Box in the contracted state.

EnableDomainLogin

**Options:** YES | NO  
**Default:** NO
If this value is set to NO, the Windows default login screen will appear when the system is booted. If this value is set to YES, the VPNremote login screen appears before Windows 2000, Windows NT, and Windows XP login screen when the system is booted.

*Note:* This parameter is valid for Windows 2000 and Windows NT only.

SavePasswordOption

**Options:** YES | NO  
**Default:** NO
If this value is set to YES, VPNremote will allow the user to save the password in the Connected dialog box. If this value is to NO, VPNremote will not allow the user to save the password in the Connected dialog box.

LaunchAtStartUp

**Options:** YES | NO  
**Default:** NO
If this value is set to NO, the VPNremote application will not launch at Startup. If this value is set to YES, the VPNremote application will launch at Startup.
MinimizeAfterConnect

**Options:** YES | NO  **Default:** NO  
If this value is set to NO, VPNremote will not minimize the application upon successful connection. If this value is set to YES, VPNremote will minimize the application upon successful connection.

AutoConnect

**Options:** YES | NO  **Default:** NO  
If this value is set to NO, VPNremote will not automatically connect. If this value is set to YES, the Save Password Option value is set to YES, and VPNremote is launched VPNremote will establish a secure connection automatically.

BuildSecureTunnelsAutomatically

**Options:** YES | NO  **Default:** NO  
If this value is set to NO, VPNremote will not build a secure tunnel at Startup. If this value is set to YES, VPNremote will build a secure tunnel automatically after establishing a secure connection.

EnableKeepAlive

**Options:** YES | NO  **Default:** NO  
If this value is set to NO, VPNremote will not attempt to ping the secure host. If this value is set to YES, VPNremote will attempt to ping the secure host according to the interval specified in the KeepAliveTimer.

KeepAliveTimer

**Options:** YES | NO  **Default:** NO  
If this value is set to NO, VPNremote will ignore the timer. If this value is set to YES, VPNremote will ping the host server at the specified interval.

MTUSize

Set this parameter for the Maximum Transmission Unit (MTU) value for the VPNremote Virtual Adapter. All packets transmitted over the VPN will not exceed the specified MTU value. MTU minimum value = 1020. MTU maximum value = 1348. Default value = 1348.

EnableMSTCPDUNHook

* **Note:** This parameter is applicable to VPNremote users running Windows 98 and Windows ME only.

**Options:** YES | NO  **Default:** NO  
Set this value to YES, if the VPNremote user is running on Windows 98 or Windows ME with dial-up networking. Set this value to NO, for all VPNremote users not running Window 98 or Windows ME.
EnableUDPEncapsulation

**Options:** YES | NO  
**Default:** YES

Set this value to YES, if the VPNremote user is using an IPSEC Passthrough Device that is not compatible with IKE NAT Traversal. Set this value to NO, if the VPNremote user is not using an IPSEC Passthrough Device.

Distributing VPNremote to the Remote Users

The method used to deploy VPNremote is primarily dependent on if you are providing a customized initialization file or a default initialization file to the remote users. The software distribution procedures currently employed by your organization also must be considered.

* **Note:** For certificate-based VPN users, you will need to provide a signing certificate along with instructions for obtaining a personal certificate from your PKI, regardless of the method chosen to deploy the VPNremote Client software.

If you have decided not to customize the Avaya initialization file, you can simply copy the VPNremote self-extracting installer file, located in the VPNremoteZip directory on the VPNremote Client CD, to a server and notify the remote users how to get and install the VPNremote software. However, you will also need to provide remote users with detailed instructions and information required to initially configure their VPNremote Client software. See “Information Required by Remote Users” on page 2-12.

If you have customized the VPNREMOTE.INI file, you can choose any of the following methods to distribute the VPNremote Client software:

- Use a utility like WinZip Self-Extractor to create a single self-extracting installation file that includes the customized initialization file.
- Put the contents of the VPNremote directory that includes the customized initialization file on a server and provide the users with instructions for downloading and running VPNremote. To launch the VPNremote installer program, run SETUP.EXE, located in the Disk1 directory.

Information Required by Remote Users

At a minimum, the Network Administrator must provide the name and password assigned to the remote user through the VPNManager. However, depending on if and to what extent the initialization file has been customized for the remote users, the Network Administrator may need to provide additional information and instructions to the remote users. For example, if the Network Administrator decides not to customize the
initialization file, all of the information required to connect to a VSU and
download their configuration must be provided to the remote users.
Additionally, if the remote users are required to obtain user certificates
from a PKI, instructions for contacting the PKI along with any required
information must also be given to the remote users.

The best way to determine what information and instructions are required
by the remote users for your particular implementation is to examine the
information that will be conveyed to the remote users through the
initialization file, and then provide the remote users with any additional
information that has not been specifically set in the initialization file. A
checklist is provided in AppendixA to assist you in gathering the
information that must be supplied to remote users.

The remaining chapters in this guide provide installation and configuration
instructions intended for the remote users and for the most part are written
from the end user’s prospective. The information provided in this guide is a
reference for the Network Administrators and when appropriate, includes
notes specifically intended for the Network Administrator.
3 Installation

This chapter provides instructions for loading the VPNremote Client software on a Windows 98, Windows 2000, Windows NT, Windows ME, or Windows XP system.

Before installing the VPNremote Client software make sure that your system meets the following minimum system requirements:

- Microsoft Internet Explorer 5.0 or Netscape Navigator 6.1 or later
- A Pentium II Processor or higher with 12 MB of available disk space, 64 MB of RAM for Windows 98 and Windows ME, and 128 MB of RAM for Windows 2000 and Windows NT
- An installed modem or network interface card (see the VPNremote README file for an up-to-date list of supported modems and network adapters)
- Microsoft TCP/IP installed on the modem or network interface card
- Color monitor and video card that supports 16-bit color
- Optional SmartCard reader installed and tested

The VPNremote Client installation procedure has been designed to simplify the installation for most users while providing Network Administrators the ability to customize the installation to meet their specific requirements. This is accomplished by editing the VPNREMOTE.INI file prior to distributing VPNremote to the remote users. The VPNREMOTE.INI file also can be used to pre-configure VPNremote to automatically download its configuration information from a specified VSU when VPNremote is first started.

The remainder of this chapter describes how to install the VPNremote software on a Windows 98 system using the default VPNREMOTE.INI file provided by Avaya. With a couple of noted exceptions, the installation procedure for Windows 2000, Windows NT, Windows ME, or Windows XP is the same.
Installing VPNremote

To install the VPNremote software:

1. Launch the VPNremote Client installation program.

   The procedure for launching the installation program will vary depending on how the Network Administrator has decided to distribute the VPNremote software.

   The Network Administrator should provide instructions to the remote users on how to install VPNremote.

   When the installation program has successfully launched, a dialog box will appear asking you to confirm that you want to install VPNremote for your specific version of Windows (Figure 3-1.).

   ![Figure 3-1. Install VPNremote for Windows Confirmation](image)

2. Click Yes to continue.

3. When the Welcome dialog box (Figure 3-2.) appears, verify that you do not have any other Windows programs running, then click Next to continue.
If a previous version of VPNremote is detected during installation that requires uninstallation, an uninstall message will be displayed (Figure 3-3.).

*Note:* The VPNremote Client can be used with multiple adapters including both a Dial-Up and LAN Adapter without reinstalling the VPNremote Client software.

4. Click **Yes** to uninstall the previous version.

5. You will be given the opportunity to view the README file (Figure 3-4.). Click **Yes** to view the README file now or click **No** to continue. If you choose to view the README file now, exit the text editor when you are finished.
Chapter 3

6. Before you can use VPNremote, you must restart your computer. Click Next in the Restart Windows dialog box (Figure 3-5.) to restart your computer now.

* Note: Windows NT and Windows 2000: A VPNremote login screen may appear immediately following the Windows login. This allows you to establish a VPNremote connection so that the primary domain name server can be reached prior to actually logging on to the network. Refer to the VPNremote Main Console Chapter for instructions on how to control the VPNremote Domain Login feature.

After restarting your computer, you can launch the VPNremote Client by double-clicking on the VPNremote shortcut icon, which was automatically placed on your desktop. Follow the instructions provided by your Network Administrator to configure and use VPNremote.
Uninstalling VPNremote

To uninstall VPNremote:

1. Exit VPNremote if enabled.

2. On the Windows task bar, select Start, Programs, VPNremote for Windows, Uninstall VPNremote for Windows (Figure 3-6.).

3. When asked to confirm that you want to completely remove VPNremote (Figure 3-7.), click Yes.

4. When the Remove Programs From Your Computer dialog box indicates that the uninstall is completed (Figure 3-8.), click OK.
5. When you are prompted to restart your computer (Figure 3-9.), click Yes.
4 VPNremote Main Console

The primary purpose of the Main Console window (Figure 4-1.) is to allow remote users to establish a VPN connection.

Pre-Configuring VPNremote

Depending on if and to what extent VPNremote has been customized, the Network Administrator may need to provide the remote users additional information and instructions to pre-configure VPNremote as summarized below:

- If the Network Administrator decided not to customize VPNremote, the Network Administrator should provide the remote user with the information required to configure their User Profile to establish a VPN connection.
- When VPNremote is launched for the first time following installation, the Profile Manager Wizard automatically takes the remote user through a series of screens to configure the User Profile. The user should enter the information supplied by the Network Administrator as described in the Profile Manager Wizard chapter.
- If the remote user is using a SmartCard reader, the user will need to add a new cryptographic module to the list of modules supported by VPNremote as described in the SmartCard Manager chapter. The Network Administrator should help the remote user determine the name and location of the cryptographic module's driver file.
- If the remote user is required to obtain a user certificate from a PKI, the Network Administrator should provide the remote user with instructions for obtaining a user certificate as described in the Certificate Manager chapter.
Establishing a Remote Connection using a Non Certificate-Based User Profile

Once VPNremote is configured, the remote user can establish a secure VPN connection. A remote user can establish a secure network connection or a secure dial-up connection as described below:

1. If the User Name field is blank, enter the user name assigned to you by your Network Administrator.
2. Enter the password assigned to you by your Network Administrator.
3. Confirm that the correct Internet Connection is selected.
   a. Select the Options button.
   b. Select the Internet Connection type from the drop-down menu.
   * Note: The Internet Connection type selection remains the same based on the previous login.
4. Click Connect.

VPNremote will display a series of messages as it downloads the configuration for the selected user profile. When this process is completed,
the Main Console screen will change (Figure 4-2.) indicating that a connection has been established.

* **Note:** If the Network Administrator has disabled split-tunnel, a “Connected (VPN Secure Traffic Only)” message will be displayed indicating that this connection can only be used for transmitting secured traffic. All other internet traffic will be blocked until VPNremote is closed.

![VPNremote Connected](image)

**Figure 4-2. VPNremote Connected**

### Establishing a Remote Connection using a Certificate-Based User Profile

Once VPNremote is configured, the remote user can establish a secure VPN connection using a Certificate-Based User Profile as described below:

1. If the User Name field is blank, enter the user name assigned to you by your Network Administrator.

2. Enter the password assigned to you by your Network Administrator.

3. Select the Certificate-based User Profile associated with the cryptographic module.

   To select a User Profile, click the Options button to expand the Main Console window.
4. Select an Internet Connection type from the drop-down menu.

5. Click Connect.

6. Because the selected profile is certificate-based and the password has been changed, you will be prompted to enter the password assigned to the cryptographic module associated with the profile certificate (Figure 4-3.).

* Note: The default password for the VPNremote Certificate DB is NULL (no password). It is strongly recommended that the remote user change the Remote Certificate DB Password. To change the default password, see To Change the Cryptographic Module Password on page 4-5.

![Figure 4-3. Cryptographic Module Password](image)

VPNremote will display a series of messages as it downloads the configuration for the selected user profile. When this process is completed, the Main Console screen will change (Figure 4-2.) indicating that a connection has been established.

* Note: If the network administrator has disabled split-tunnel, a “Connected (VPN Secure Traffic Only)” message will be displayed indicating that this connection can only be used for transmitting secured traffic. All other internet traffic will be blocked until VPNremote is disconnected.
VPNremote Client Administrator's Guide

To Change the Cryptographic Module Password

Before a VPN connection is established, remote users can change the Certificate DB password by using the following procedure:

1. From the Main Console window, click the **Options** button to expand the window.

2. Click the **Advanced** button.

3. Click the **SmartCard** tab to bring the SmartCard options to the front.
4. Click the View button in the SmartCard Manager window (Figure 4-5.). The View Cryptographic Module window appears (Figure 4-6.).
5. Click the Change Password button in the Cryptographic Module window (Figure 4-6.).

* Note: The default password for the VPN Remote Certificate DB is NULL (no password). It is strongly recommended that the remote user change the Remote Certificate DB Password to an easy to remember and unique password.
If the unique cryptographic module password is forgotten, you will not be able to use the certificate for the cryptographic module associated with the forgotten password. If the forgotten password was for a SmartCard, a replacement SmartCard is required. If the forgotten password was associated with database files, the cryptographic module must be reinstalled, and a new certificate must be downloaded. If all passwords are forgotten, re-install the VPNremote software.

*Note:* Re-installing the VPNremote software will result in a loss of all cryptographic-module data and any certificates that may have been downloaded.

6. Enter your new password.

7. Click OK.

![Figure 4-8. Password Changed Successfully]

**VPNremote Taskbar Icon**

The Taskbar Icon is available upon launching VPNremote. By default, VPNremote will minimize and an icon appears in the taskbar.

The Taskbar Icon allows the remote user a single location to perform a variety of tasks that include: establish a secure VPN connection, configure user preferences, and generate diagnostic reports.

![Figure 4-9. Taskbar Icon]
The Taskbar Icon displays four colors: white, flashing white and yellow, green, and flashing red. Each color indicates a stage in the VPN connection process:

- **White** – Indicates no connection.
- **Flashing White and Yellow** – Indicates that VPNremote is attempting to establish a VPN connection.
- **Green** – Indicates a successful secure VPN connection.
- **Flashing Red** – Indicates an alarm.

### Before Connecting to VPNremote

The Taskbar Icon is available before VPNremote is connected.

The following options are available from the Taskbar Icon before connection to the VPN:

- **Help** – Displays available links to the VPNremote online Help contents and index, about VPNremote, and a customer care website.
- **Hide VPNremote** – Displays VPNremote as an icon in the Taskbar.
- **Preferences** – Displays user configurable settings.
- **Show Profile Manager** – Displays the Profile Manager and Log Details window.
- **Generate Diagnostic Report** – Displays system and VPNremote configuration information.
- **Quit** – Exits VPNremote.

![Figure 4-10. Before Connected Taskbar Icon Options](image)

### After Connecting to VPNremote

The Taskbar Icon is available during the VPNremote session.
The following options are available from the Taskbar Icon after connection to the VPN:

- **Help** – Displays available links to the VPNremote online Help contents and index, about VPNremote, and a customer care website.
- **Show VPNremote** – Displays VPNremote and as an icon in the Taskbar.
- **Preferences** – Displays user configurable settings.
- **Disconnect** – Disconnects the VPN connection.
- **Show Secure Connection** – Displays the Advanced information window that includes the Secure Connection tab, Networking Info tab, and Log Details tab.
- **Generate Diagnostic Report** – Displays system and VPNremote configuration information.
- **Quit** – Exits VPNremote.

![Taskbar Icon Options]

**Figure 4-11. After Connected Taskbar Icon Options**

### Preferences

The preferences or user configurable settings are available to the user from the Taskbar Icon either before or after VPNremote is connected.

Use the following preferences to modify VPNremote behavior when a successful connection is established using Windows 2000, Windows NT, or Windows XP:

- **Hide After Connect** – Displays VPNremote as an icon in the Taskbar.
- **Hide When Minimized** – Displays VPNremote as an icon in the Taskbar when minimize button is clicked.
■ **Enable Domain Login** – A VPNremote connection must be established so that the primary domain name server on the enterprise network can be reached when starting up and logging into Windows. Enabling the VPNremote Domain Login feature causes a VPNremote login screen to be displayed immediately before the Windows login. Actually logging into Windows is delayed until after the VPNremote connection has been established. Disabling the VPNremote Domain Login feature suppresses the VPNremote login and allows the Windows system user to log in normally.

■ **Enable UDP Encapsulation** – Allows a VPNremote connection to discover NAT devices between the VPNremote user and the VSU. If a NAT device is discovered, VPNremote and the VSU will negotiate NAT traversal. Upon successful NAT traversal negotiation, IPSEC packets will be UDP encapsulated. If this preference is disabled, VPNremote will not attempt to discover NAT devices, and IKE and IPSEC packets will operate normally. This preference is enabled by default.

■ **Automatically Launch VPNremote During Start Up** – Launches VPNremote at Start Up.

■ **Save Password** – Saves the user password in the Connected dialog box.

■ **Automatically Connect VPNremote** – When Save Password is enabled, VPNremote will automatically build a secure tunnel downloading the VPN configuration from the secure gateway.

■ **Build Secure Tunnels Automatically** – Builds a secure tunnel after downloading the VPN configuration from the secure gateway.

* **Note:** This feature is not supported if using RSA’s ACE Server for client authentication in a VPN with more than one VSU.

■ **Enable Keep Alive** – Attempts to ping the secure host according to the interval specified by the Keep Alive Timer.

■ **Keep Alive Timer** – Sets the interval to ping the secure host.

■ **MTU Size** – Sets the Maximum Transmission Unit value for the VPNremote Virtual Adapter.
Use the following preferences to modify VPNremote behavior when a successful connection is established using Windows 98:

- **Hide After Connect** – Displays VPNremote as an icon in the Taskbar.
- **Hide When Minimized** – Displays VPNremote as an icon in the Taskbar when minimize button is clicked.
- **Enable MSTCP DUN Hook** – Enables Windows 98 VPNremote users to successfully receive all packets from the dial-up adaptor. The VPNremote user must reboot their system upon enabling this preference.
- **Enable UDP Encapsulation** – Allows a VPNremote connection to discover NAT devices between the VPNremote user and the VSU. If a NAT device is discovered, VPNremote and the VSU will negotiate NAT traversal. Upon successful NAT traversal negotiation, IPSEC packets will be UDP encapsulated. If this preference is disabled, VPNremote will not attempt to discover NAT devices, and IKE and IPSEC packets will operate normally. This preference is enabled by default.
- **Automatically Launch VPNremote During Start Up** – Launches VPNremote at Start Up.
- **Save Password** – Saves the user password in the Connected dialog box.
- **Automatically Connect VPNremote** – When Save Password is enabled, VPNremote will automatically build a secure tunnel downloading the VPN configuration from the secure gateway.

- **Build Secure Tunnels Automatically** – Builds a secure tunnel after downloading the VPN configuration from the secure gateway.

*Note:* This feature is not supported if using RSA’s ACE Server for client authentication in a VPN with more than one VSU.

- **Enable Keep Alive** – Attempts to ping the secure host according to the interval specified by the Keep Alive Timer.

- **Keep Alive Timer** – Sets the interval to ping the secure host.

- **MTU Size** – Sets the Maximum Transmission Unit value for the VPNremote Virtual Adapter.

---

*Figure 4-13. Advanced Parameters for Windows 98*
5 Profile Manager

The Profile Manager (Figure 5-1) allows remote users to create and maintain a list of User Profiles, which are used for establishing VPN connections. It is accessed by clicking the Options button on the VPNremote main console to expand the window. Click the Advanced button to open the Advanced window.

![Profile Manager Step 1](image)

**Figure 5-1. Profile Manager Window**

The Profile Manager window includes a list of User Profiles along with the following control buttons:

**Add** – Launches the Profile Manager Wizard that steps the user through a series of dialog boxes to create a new User Profile. See Profile Manager Wizard, for instructions on how to set up a new User Profile.
Modify – Allows the user to view and if necessary modify the selected User Profile as described under Viewing or Modifying a User Profile on page 2.

Delete – Deletes the selected (highlighted) User Profile as described under Deleting a User Profile on page 5. Note that the profile currently selected at the VPNremote main console cannot be deleted.

Export/Import – The export function allows the user to save a selected User Profile to a file that can be imported onto another system with VPNremote. See Exporting and Importing a User Profile on page 6 for instructions on how to use this feature.

Adding a User Profile

To add a new User Profile, click the Add button. This launches the Profile Manager Wizard that steps the user through the process of gathering information required for the new User Profile. See Profile Manager Wizard, for instructions on how to set up a new User Profile.

Viewing or Modifying a User Profile

To view or modify a User Profile, select (highlight) the profile to modify and click the Modify button. The User Profile window (Figure 5-2.) for the selected profile will appear.

To modify the profile, edit the profile fields as described in the following section, then click OK to save the changes and return to the Profile Manager list.
The main user profile window (shown in Figure 5-2.) consists of the following sections:

**User Info** – Includes the following information required to authenticate the user when establishing a VPN connection:

- **Profile Name** – A read-only field displaying the name of the selected User Profile.
- **User Name** – The VPNremote account name assigned to the user by the Network Administrator.
- **VPNmanager Suffix** – The Administrative Domain in the VPNmanager Directory Server where the VPN policy information resides.

* **Note**: VPNmanager suffix is an optional field. This field will remain blank unless you are using a certificate-based VPN connection or an LDAP configuration.
Chapter 5

■ **User Certificate** – The name of the user certificate that is used to establish a certificate-based VPN connection. Refer to the Certificate Manager, for instructions on how to obtain a user certificate.

*Note:* User Certificate is an optional field. This field will remain blank unless you are using a certificate-based VPN connection.

**VSU Info** – Includes the following information required to download the VPN configuration from a VSU associated with the user’s VPN:

■ **VSU Address** – The IP address or domain name of the VSU used to download the VPN configuration.

■ **Backup VSU** – The IP address or domain name of the VSU used to download the VPN configuration when the primary VSU is unavailable.

■ **Port** – The port number to use on the VSU. The default port number is 1443.

**Authentication** – Specifies the authentication method, CHAP (Challenge-Handshake Authentication Protocol) or PAP (Password Authentication Protocol), used to authenticate the remote user.

The **Advanced** button takes the user to a second window (Figure 5-3.) that includes the following sections:

**Log Info** – Specifies where to send log information. If **Write to Local File** is selected, the log information will be saved locally in the vpnremote.log file in the VPNremote Program folder. If **Write to Syslog Server** is selected, the log information will be sent to a syslog server at the specified IP address and port number.

**Network Info** – Includes the following information used for virtual adapter network configuration that is sent to the remote user through CCD:

■ **IP Address/Subnet Mask** – Set these values equal to the values of the virtual adapter.

■ **Primary WINS** – Set this value to the address of the primary WINS server that is protected by the VSU the remote user will connect to.

■ **Secondary WINS** – Set this value to the address of the secondary WINS server that is protected by the VSU the remote user will connect to.

■ **Primary DNS** – Set this value to the address of the primary DNS server that is protected by the VSU the remote user will connect to.

■ **Secondary DNS** – Set this value to the address of the secondary DNS server that is protected by the VSU the remote user will connect to.
Deleting a User Profile

To delete a User Profile, select the profile to delete and click the **Delete** button. A dialog box (Figure 5-4.) will appear to confirm that the selected profile should be deleted. The user profile currently selected on the VPNremote main console cannot be deleted.
Exporting and Importing a User Profile

The export and import functions allow users to export a selected User Profile to a file and later import the file on to a different system using VPNremote.

Exporting a User Profile

To export a User Profile, select the profile to export and click the Export button. The Export Profile window (Figure 5-5.) will appear.

Enter the full path and filename; for example, a:\myprofile.txt) for where you want to save the exported profile in the Export Filename field. The Browse button provides a convenient way to select the location of the exported file.

Assign a password to the exported profile file by entering the password in both the Password and Confirm Password fields. This password will be required later to import the profile on another system running VPNremote software.
Importing a User Profile

To import a previously exported User Profile, click the Import button on the Profile Manager window. This launches the Import Profile Wizard (Figure 5-6.) that takes the user through the steps to import the User Profile.

In Steps 1 and 2, select the cryptographic module and slot/token the user profile certificate should be added.

In Step 3, do the following:

1. Enter the Profile Name.
2. Click the Browse button to select the previously exported profile file that will be imported.
3. Enter the password that was assigned to the file during the export process and click Next.
4. Select the cryptographic module and click Next.
5. Select the Slot/Token to add the certificate and click Next.
6. Click Finish to import the profile. The profile should now be available for selection in the profile drop-down menu at the main console.
Figure 5-6. Import User Profile Wizard
Before using VPNremote to initiate a VPN connection, the user must first set up a User Profile that contains information required to establish the VPN connection.

If the Network Administrator has not pre-configured the Default User Profile by editing the VPNREMOTE.INI file, the Profile Manager Wizard is automatically opened when VPNremote is launched the first time.

VPNremote supports multiple User Profiles. To set up a second User Profile, click the Options buttons on the VPNremote main console to expand the window. Click the Advanced button to open the Advanced window. Click the Profiles tab to bring it to the front. Click Add to add a User Profile.

The Profile Manager Wizard guides the user through the following steps to configure a User Profile:

- Create a Typical User Profile
- Create a Custom User Profile
- Choose Configuration Method
- Download Configuration from VSU or Import Configuration File

Create a Typical User Profile

The Typical User Profile uses the default setting in VPNremote. Use this User Profile for remote users who are standard remote users and that do not require user customization. For remote users who require a custom profile, go to Create a Custom User Profile.

The first dialog box in the Profile Manager Wizard (Figure 6-1.) is used to assign a unique name to the User Profile.

To create a Typical User Profile, use the Profile Manager Wizard:

1. Enter a descriptive name in the User Profile field. Click Next.

*Note: The User Profile name must be unique to all other profile names in the User Profile list. User Profile names are not
case-sensitive. For example, robert, Robert, and ROBERT are all treated as the same name.

Figure 6-1. Typical User Profile

2. Enter the User Name associated with the User Profile being created in the User Name field.

3. Enter the VSU IP Address the remote user will connect to in the VSU IP Address field.

4. Click Finish.
Create a Custom User Profile

Use Custom User Profiles for remote users who require a custom profile. Remote users that require a custom profile can be users who share a workstation with other remote users, or a user who need different profiles to establish a in-office connection and a remote connection.

The first dialog box in the Profile Manager Wizard (Figure 6-1.) is used to assign a unique name to the User Profile.

To create a Custom User Profile, use the Profile Manager Wizard:

1. Enter a descriptive name in the User Profile field.

* Note: The User Profile name must be unique to all other profile names in the User Profile list. User Profile names are not case-sensitive. For example, robert, Robert, and ROBERT are all treated as the same name.

2. Select the Custom radio button.
Figure 6-3. Custom User Profile

3. Click Next.

The Profile Manager Step 2 window displays.

Choose Configuration Method

Step 2 of the Profile Manager Wizard (Figure 6-4.) allows the user to select the configuration method specified by the Network Administrator.

If a VPN configuration file is used to configure the remote user’s client software, the user should select **Import configuration information from administrator supplied file** and click Next. Go to Import Configuration File on page 7.

Otherwise, the user should select **Download configuration from VSU**, click Next, and proceed to the next section, Download Configuration from VSU.
Download Configuration from VSU

Download Configuration from VSU is the preferred method for configuring VPNremote. To use this method, the Network Administrator must provide the following information to the remote user:

**User Info** – Includes the following information required to authenticate the remote user when establishing a VPN connection:

- **Profile Name** – The unique name assigned to the User Profile.
- **User Name** – The VPNremote account name assigned to the user by the Network Administrator.
- **VPN Manager DN Suffix** – The Administrator Domain in the VPNmanager Directory Server where the VPN policy information resides.
- **User Certificate** – The name of the user certificate that is used to establish a certificate-based VPN connection. Refer to the Certificate Manager in Chapter, for instructions on how to obtain a user certificate.

User Certificate is an optional field. This field will remain blank unless you are using a certificate-based VPN connection.

**VSU Info** –
■ **VSU Address** – The IP address of the DNS the Avaya VPNIware Service Unit will connect to.

■ **Port** – The port value used for VPNremote to connect to the VSU.

All of this information, except for the User Name and Password, can be conveyed to the remote users by editing the VPNREMOTE.INI file prior to distributing VPNremote.

In Step 3 of the Profile Manager Wizard (Figure 6-5), the remote user enters the User Name and DN Suffix specified by the Network Administrator in the User Name and VPN Manager Suffix fields.

![Profile Manager Step 3](image)

**Figure 6-5. User Name and DN Suffix**

The User Name selections determine the user name to use when establishing a VPN connection. In most cases, *Most recently used name* (the name entered to authenticate a previous connection) should be selected.

Click Next to proceed to the next step.

In Step 4 of the Profile Manager Wizard (Figure 6-6), enter the **VSU IP Address**, **Backup VSU IP Address**, and **Port** number specified by the Network Administrator. The authentication method chosen is dependent on the type of authentication used by the RADIUS server. If the RADIUS server uses CHAP (Challenge-Handshake Authentication Protocol) or a
RADIUS server is not used, set this variable equal to CHAP. If the RADIUS server uses PAP (Password Authentication Protocol), set this variable to PAP.

![Profile Manager Step 4](image)

**Figure 6-6. VSU Information and Authentication Method**

**Import Configuration File**

To import configuration information from an administrator supplied file, click the **Browse** button in Step 3 of the Profile Wizard (Figure 6-7.) to locate and select the configuration file then click **Finish**.
Figure 6-7. Import Configuration File

When the profile is selected from the VPNremote main console, the User Name field is replaced with a File Name field. VPNremote uses information from the selected file for configuration instead of downloading the client configuration information over the network.
7 Monitoring

To assist in isolating problems that may occur, VPNremote includes the following monitoring facilities:

- **Event Log Details Viewer** – Captures and records significant event information while VPNremote is operating. Event messages written to a local log file can be filtered and displayed in the Log Details viewer.

- **Configuration Statistics** – Displays connection information for each VPN tunnel that is accessible to the remote client for secured communication across a public network. See Configuration Statistics on page 3 for additional information.

- **Session Security Associations (SA)** – ISAKMP and IPSec Security Association (SA) information can be accessed by clicking the Sessions button on the VPNremote main console. See “Session Security Associations (SA)” on page 4 for additional information.

### Event Log Details Viewer

To monitor and capture information on significant events as they occur, VPNremote includes an event logging and viewing utility. Log details captured during operation are written to the VPNREMOTE.LOG file in the VPNremote for Windows directory.

The Log Details viewer is accessed by clicking the Advanced button in the VPNremote main console then selecting the Log Details tab. In addition to displaying a list of logged events, the Log Details viewer (Figure 7-1.) allows users to perform the following functions:

- **Set Log Level** – Log settings allow users to set the priority level of messages to log. Log level settings are low, medium, and high.

- **Save the Event Log to a File** – To save the current contents of the event log to a file, click **Save As**. The User will be prompted to choose a name and location for the saved file.

- **Clear Log** – To clear the contents of the log file, click the **Clear Log** button. A warning message will be displayed asking for confirmation to remove all of the log file contents.
**Set Log Level**

The **Set Log Level** drop-down menu is used to set the priority level of messages sent to the event log destinations. Message priority levels are listed in ascending order as follows:

- **LOW** – Includes error messages. Error messages include notification that VPNremote could not establish a VPN connection.
- **MEDIUM** – Includes information messages.
- **HIGH** – Includes error messages and debug messages used only for troubleshooting purposes.

All messages at or above the set log level are sent to the event log destinations. For example, if the log level is set to **MEDIUM**, all Medium and Low condition messages will be logged. **HIGH log level** messages will not be logged.

**Select Log Destinations**

The Log Destination specifies where to send event messages. If **Write to Local File** is selected, event messages will be written in the **VPNREMOTE.LOG** file. If **Write to Syslog Server** is selected, the log
information will be sent to a Syslog server at the Syslog Server IP address and port number set in the Advanced User Profile window for the selected user. The Syslog IP address and port number for the selected user can be viewed or changed by clicking on the Set Syslog IP Address button. Note that the Write to Syslog Server selection is only available when an VPN connection is established.

## Configuration Statistics

The Configuration window (Figure 7-2.) displays connection information for a selected VPN tunnel. It is accessed by clicking Details>Advanced button from the VPNremote Connected window when a connection is established.

The Secure Connection tab displays the following information required to establish a secure connection.

- **Secure Gateway** – Displays the IP address of the VSU that the remote user is connecting to.

- **Secure Network** – Displays the network IP address the VSU is protecting.

- **Secure Connection State** – Displays the status of the IKE/IPSec session. A secure session state can be no state, in progress, connected, or failed.
Figure 7-2. Secure Connection

Clicking on the View Proposal Lists button, displays the IKE and IPSec security proposals acquired by VPNremote during CCD (see Figure 7-3.). Phase 1 and Phase 2 shows the IKE and IPSec security settings proposed by VPNremote. This information should coincide with the IKE and IPSec security settings for the VPN as defined in Chapter 7 of the VPNmanager Reference Manual.

Figure 7-3. Advanced Configuration

Session Security Associations (SA)

ISAKMP and IPSec SAs are required to establish secure communications between the VPNremote Client and a VSU. To view the SA information for both ISAKMP and IPSec, click the Details button from the Advanced button on the VPNremote main console when a connection is established. The ISAKMP SA and IPSec SA lists are shown in Figure 7-4.

The Advanced Session window displays the current security associations that VPNremote has established with the secure gateway(s) and the current state of each association.
**Figure 7-4. Advanced Session**
Depending on the security policies of your organization, the Network Administrator can choose from the following options to secure remote user VPN traffic:

- **Use Pre-shared Secrets** – This is the simplest method used to secure a VPN. Authentication exchanges between VPNremote Clients and the VSUs are based on a single pre-shared secret which is automatically acquired by the remote client during the Client Configuration Download (CCD) process. This eliminates the requirement for remote users to deal with keys and certificates.

- **Centralized Key and Certificate Distribution** – This method may be used when a company’s security policy does not require remote users to generate their own certificates. In this case, the PKI Administrator takes responsibility for generating and distributing user keys and certificates as PKCS#12 files which the remote users can import as User Profiles in VPNremote. Alternatively, the Administrator can write the keys and certificates on to smart cards, and distribute the smart cards to the remote users. In either case, the remote users are not required to generate keys or submit certificate requests.

- **User Controlled Keys and Certificates** – For organizations with a more stringent security policy that requires the end user to be the only person to ever have access to their private key, the Certificate Manager provides a utility that enables the generation of keys as well as the submittal of certificate requests to a Certificate Authority. Both CRS (Certificate Request Syntax) online enrollment protocol and PKCS#10 file-based enrollment are supported.

The remainder of this discussion, provides instructions to remote users on how to use the Certificate Manager to acquire and manage certificates.

To access the Certificate Manager (Figure 8-1) select the **Options** button to expend the window. Click the **Advanced** button to open the Advanced window.
Chapter 8

Figure 8-1. Certificate Manager Window

The Certificate Manager (Figure 8-1.) provides a simple environment that allows remote users to perform the following Certificate Management tasks:

- Importing a Signing Certificate
- Acquiring a Personal Certificate
- Verifying a Certificate
- Viewing Certificate Details
- Deleting an Invalid Certificate
- Selecting a Default Certificate
- Exporting a Signed Certificate

Importing a Signing Certificate

CA signing certificates are used in the VPNware system to verify the signature on certificates issued by a VSU or end user thereby assuring that the device or user certificate was signed by a known and trusted CA.
The Network Administrator should provide the remote users with a CA signing certificate file that they can import into the Certificate Manager database by performing the following procedure:

1. Click on the **Signing Certificate** radio button to select the Signing Certificate database.

2. Click **Import Certificate**.

   The Import Certificate dialog box (Figure 8-2.) appears.

3. Enter a descriptive name for the CA signing certificate in the **Certificate Name** field. This name is displayed in the Certificate Manager list.

4. Click the **Browse** button to locate the CA signing certificate provided by the Network Administrator.

5. Click **OK** to add the selected CA signing certificate to the list of signing certificates in the Certificate Manager.

---

**Figure 8-2. Import Certificate Dialog Box**

---

### Acquiring a Personal Certificate

The procedure used to obtain a personal certificate is dependent on the PKI services employed by your organization. VPNremote supports either of the following two methods:

- **Online Certificate Request** – Start by generating a CRS (Certificate Request Syntax) online request. When notified that the request has been fulfilled, download the certificate to the Certificate Manager database.

- **File-based Certificate Request** – Start by generating a PKCS#10 certificate request file. Follow the instructions of your PKI Administrator to deliver the certificate request and obtain a certificate file from your PKI service. Import the certificate into the Certificate Manager database.
Online Certificate Request

To request a personal certificate online, perform the following steps:

1. Click on the Personal Certificate radio button to select the Personal Certificate database.

2. Select the Request Online radio button then click OK.

The Online Certificate Request dialog box (Figure 8-3.) appears. The information in this dialog box is acquired from the Advanced section of the selected User Profile. Refer to page 5-4 for a description of these fields.

3. Enter a descriptive name in the Certificate Name field. This name is displayed in the Certificate Manager list.

4. Enter your Email address in the Email field. This email address is used to notify the user when the certificate is ready.

5. Verify that all required fields are filled in then click OK.

Your certificate request with a status of Pending will appear in the Certificate list (Figure 8-4.).

Figure 8-3. Online Certificate Request
6. When notified that the certificate request has been completed, select the pending certificate and click Retrieve Certificate to download the certificate.

File-based Certificate Request

To generate a certificate request to a file, perform the following steps:

1. Click on the Personal Certificate radio button to select the Personal Certificate database.

2. Select the Request to a file radio button then click OK.

The Certificate Request dialog box (Figure 8-5.) appears. The information in this dialog box is acquired from the Advanced section of the selected User. Refer to page 5-4 for a description of these fields.
3. Enter the full pathname (e.g., C:\certrequest.txt) to the location where you want the certificate request file saved.

   The certificate request file is saved in PKCS#10 format and PEM (Privacy Enhanced Mail) encoded. It can be thought of as an order form for a digital certificate.

4. Send the certificate request file to the PKI service as instructed by the PKI Administrator.

   The certificate request file can be delivered by diskette, email, or any other file transfer method which is acceptable to your PKI service.

5. After the PKI service has generated the certificate, save it to a file which is accessible from VPNremote.

6. In the Certificate Manager, click Import a Certificate.

   The Import Certificate dialog box (Figure 8-6.) appears.
7. Enter a descriptive name for the certificate in the Certificate Name field.

1. Click the Browse button to locate the certificate saved on disk.

2. Click OK to add the certificate to the list of certificates in the Certificate Manager.

Maintaining a List of Valid Certificates

The Certificate Manager includes several functions that allow end users to maintain the list of certificates including: verifying a certificate, viewing details of a certificate, and deleting an invalid certificate.

Verifying a Certificate

The validity of a certificate can be checked by selecting the certificate and clicking Verify. The following message should appear:

A certificate is determined to be invalid if its expiration date has pass or a signing certificate for the issuer is not available.
Viewing Certificate Details

To view a certificate’s detailed information, select the certificate and click Details. A message similar to the following should appear:

![Figure 8-8. View a Personal Certificate](image)

Deleting an Invalid Certificate

To delete a certificate, select (highlight) the certificate to delete and click the Delete button. A dialog box (Figure 8-9.) will appear to confirm that the selected certificate should be deleted.
Selecting a Default Certificate

To select a personal certificate for the currently active User Profile, select the certificate then click Select. The certificate’s status should show Selected.

The selected certificate name will be shown in the Certificate field on the VPNremote main console and in User Certificate field of the user profile.

Exporting a Signed Certificate

To export a certificate, select (highlight) the certificate then click Export.

When the Export Certificate dialog box (Figure 8-10.) appears, enter a full pathname for where to save the exported certificate and click OK. The certificate will be saved to the location specified as a PEM Encoded file.
The SmartCard Manager allows the remote users to maintain a list of Cryptographic Modules that provide access to SmartCards and software tokens present in the local database. To access the Smartcard Manager click the Options button on the VPNremote main console to expand the window. Click the Advanced button to open the Advanced window. Click the SmartCard tab to bring it to the front.

*Note:* Insert your SmartCard prior to launching VPNremote. Your Smartcard must remain inserted during your remote session.

The SmartCard Manager window (Figure 9-1.) includes a list of Cryptographic Modules along with the following control buttons:

- **View** – Displays information about the selected (highlighted) Cryptographic Module as described under View Cryptographic Module on page 3.

- **Add** – Adds a new Cryptographic Module to the list of modules as described under Adding a Cryptographic Module on page 2.

- **Delete** – Deletes the selected (highlighted) Cryptographic Module as described under Deleting a Cryptographic Module on page 4.

- **Logout All** – To use a Cryptographic Module that is managed by the SmartCard Manager, the user must be logged in to the module. The Logout All function simply logs the user out of all Cryptographic Module.
Chapter 9

Figure 9-1. SmartCard Manager

Adding a Cryptographic Module

To add a new Cryptographic Module to the list of modules supported by VPNremote, click the Add button. The Add Cryptographic Module dialog box (Figure 9-2.) will appear prompting the user to assign a descriptive name to the module and select a driver file. The Network Administrator should help the user determine the name and location of the module’s driver file.
View Cryptographic Module

To view a cryptographic module, select (highlight) the module to view and click the View button. The View Cryptographic Module window (Figure 9-3.) for the selected module will appear. In addition to displaying information provided by the manufacturer about the module, this window includes a list of token/slots associated with the module along with the following control buttons:

- **More Info** – Displays additional information for the selected token/slot.
- **Login** – Displays a dialog box which prompts the user for the password required to log in to the module.
- **Change Password** – Displays a dialog box which allows the user to change the password assigned to the module. The user will be prompted to enter the old password followed by the new password and confirmation.
Deleting a Cryptographic Module

Cryptographic Modules external to the VPNremote may be deleted using the SmartCard Manager. To delete an installed module, such as a smartcard reader/writer, select the module from the list of available modules and click the Delete button. This will remove the cryptographic module from VPNremote’s internal database.

* **Note:** Deleting a module will remove remote access to any user private keys and digital certificates stored on the module. Keys and certificates will not however be deleted from smartcards used on that module.
The best way to determine what information and instructions are required by the remote users for your particular implementation is to examine the information that will be conveyed to the remote users through the VPNREMOTE.INI file. Once you have reviewed the VPNREMOTE.INI file, you can determine any additional information that should be set in the initialization file.

The checklist on the following page is provided for your convenience for supplying your remote clients with essential installation information. If your VPN is certificate-based, you will also need to complete the “Certificate-Based VPNs Only” portion of the checklist.

* Note: For certificate-based VPN users, you will need to provide a signing certificate and instructions for obtaining a personal certificate from your PKI, regardless of the method chosen to deploy the VPNRemote Client software.

Table 1-1. VPNRemote Client Installation Checklist

<table>
<thead>
<tr>
<th>Item</th>
<th>In INI?</th>
<th>Entry</th>
<th>Source / Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td></td>
<td></td>
<td>User name and password assigned to remote user. See “Configuring User Objects” in VPNmanager Administrator’s Guide.</td>
</tr>
<tr>
<td>Password</td>
<td>NA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPNmanager Suffix</td>
<td></td>
<td></td>
<td>Administrative Domain in the VPNManager Directory Server.</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>CHAP or PAP</td>
<td>See the Pre-Configuration and Distribution chapter in this guide for instructions.</td>
</tr>
<tr>
<td>IPAddress (of VSU)</td>
<td></td>
<td></td>
<td>IP Address assigned to the VSU through the VSU console port.</td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td></td>
<td>Use default (1443)</td>
</tr>
<tr>
<td>VSUCertName</td>
<td></td>
<td></td>
<td>VPNManager Config Console, Policy Manager, My Certificates</td>
</tr>
<tr>
<td>LogToLocalFile</td>
<td>Yes or No</td>
<td></td>
<td>Determined by network administrator. See page 8 of this guide.</td>
</tr>
<tr>
<td>LocalLogFileMaxSize</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LocalLogFileLogLevel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogToSysLogServer</td>
<td>Yes or No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SysLogIPAddress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SyslogPort</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>In INI?</td>
<td>Entry</td>
<td>Source / Comments</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------</td>
<td>-------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Certificate-Based VPNs Only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CommonName</td>
<td></td>
<td></td>
<td>Normally the user name assigned to the remote user.</td>
</tr>
<tr>
<td>RAName</td>
<td></td>
<td></td>
<td>Supplied by PKI administrator.</td>
</tr>
<tr>
<td>CA_URL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OrganizationalUnit, CompanyName</td>
<td></td>
<td></td>
<td>Supplied by user or network administrator.</td>
</tr>
<tr>
<td>Locality, State, Country</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMail</td>
<td></td>
<td></td>
<td>User supplied.</td>
</tr>
</tbody>
</table>
# Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Things to Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Configuration Download (CCD) fails.</td>
<td>Make sure VSU is functioning properly and no network connectivity problems exist.</td>
</tr>
<tr>
<td></td>
<td>Verify that the VSU Information in the selected User Profile is correct.</td>
</tr>
<tr>
<td></td>
<td>Verify that the Authentication Flag is properly set in User Profile.</td>
</tr>
<tr>
<td></td>
<td>Verify that a user account has been created in the VPNmanager and any external authentication server being used.</td>
</tr>
<tr>
<td>Import certificate fails.</td>
<td>Make sure that the certificate acquired from your PKI is properly formatted. The certificate is a text-based file that starts with “-----BEGIN CERTIFICATE-----” and ends with “-----END CERTIFICATE-----”. Each line in the body of the certificate should be no more than 64 characters long with no spaces at the end of the line.</td>
</tr>
<tr>
<td>Preshared Secret VPN does not pass encrypted traffic.</td>
<td>Make sure that the VSU is functioning properly and no network connectivity problems exist.</td>
</tr>
<tr>
<td></td>
<td>Check for possible VPN policy mismatch between VSU and VPNRemote Client.</td>
</tr>
<tr>
<td>Preshared Secret VPN stops passing encrypted traffic.</td>
<td>Make sure that the VSU is functioning properly and no network connectivity problems exist.</td>
</tr>
<tr>
<td></td>
<td>Verify that the Client IP Address Pool on the VSU has not be exhausted.</td>
</tr>
</tbody>
</table>
## Problem
Certificate-based VPN does not pass encrypted traffic.

## Things to Check
Make sure that the VSU is functioning properly and no network connectivity problems exist.

Check for possible VPN policy mismatch between VSU and VPNremote Client.

Verify that the Client IP Address Pool has not been exhausted.

Verify that selected user profile has valid personal certificate selected.

Verify that the VSU’s signing certificate has been imported and is valid.

Verify that the VSU has a valid signing certificate for the user.

Verify that the user is logged into the Cryptographic module.

Certificate-based VPN stops passing encrypted traffic.

Make sure that the VSU is functioning properly and no network connectivity problems exist.

Verify that the VPN policy has not been changed while connected.

Network Neighborhood not visible.

Check that the WINS address in the client workstation is properly configured.
Index

A
add cryptographic module 9-2
add smart card 9-2
add user profile 5-2
authentication 2-5, 5-3, 5-4, A-1

B
Backup VSU IP 5-4

C
CA signing certificates 8-2
CA URL 2-7
CCD (Client Configuration Download) 1-2, 2-6, A-1
certificate A-1
Certificate Authority (CA) 2-7
certificate-based user profile 4-3
certificate-based VPN 1-4, 5-4, 6-5, A-2
CHAP (Challenge-Handshake Authentication Protocol) 2-5, 5-4, 6-6, A-1
client IP address pool A-2
common name 2-7
country name 2-7
configuration file 6-7
configuration methods 6-4
connecting 4-2, 4-3
Country 2-8
cryptographic module 4-4

default user profile 2-1, 2-2, 2-5, 2-8, 6-1
delete user profile 5-5, 8-8
DN suffix 2-5
domain name 5-4
domain login feature 4-11
download configuration from VSU 6-5

E
email address 2-7
error messages 1-3
event log 2-8
event log priority level 2-8

event-logging 1-3
export user profile 5-6

I
IKE (Internet Key Exchange) 1-2
import configuration 6-7
import user profile 5-6
initialization file 1-2, 2-12, A-1
installation 3-2
installation checklist A-1
Internet Connection 1-4, 4-4
IP address 5-4
IP address pool A-2

L
LDAP 1-3
locality 2-7
log file 2-8
log information 5-4

M
modify user profile 5-2

N
network neighborhood not visible A-2
Next Token/New Pin Mode 1-3

O
organization unit 2-7

P
PAP (Password Authentication Protocol) 2-5, 5-4, 6-7, A-1
password 1-4, 4-2, 4-3, A-1
PKI 2-13, A-1
port number 5-4
pre-shared secret VPN 1-4
problem solving A-1
Profile Manager 5-1
Profile Manager Wizard 6-1
profile name 5-3
RA name 2-7
RADIUS 1-3, 2-5, 6-6
Registration Authority (RA) 2-7

SecurID 1-3
SecurID token A-1
select configuration method 6-4
signing certificate 2-12, 8-2, 8-3, 8-7, A-2
SmartCard Manager 1-8, 9-1
software distribution procedures 2-12
split-tunnel 4-3, 4-4
split-tunneling 1-3
state 2-7
syslog 1-3, 2-8, 5-4, 7-3

troubleshooting A-1

uninstalling VPNremote 3-5
user authentication 5-3
user certificate 5-4
user ID 1-4, A-1
user name 4-2, 4-3, 5-3, 6-5, 6-6
User Profile
  create custom profile 6-3
  create typical 6-1
  user profile 5-1, 6-1

view smartcard module 9-3
view user profile 5-2
VPN connection 1-4
VPNmanager suffix 5-3
VPNremote
  installing 3-2
  self-extracting installer file 2-12
  uninstalling 3-5
VPNRemote Taskbar Icon 4-8
  After Connecting 4-9
  Before Connecting 4-9
vpnremote.log file 5-4, 7-2
VSU address 5-4
VSU signing certificate A-2

WINS address A-2