RouteFinder™
Internet Security Appliance

SSH IPSec Client
Models RFIPSC-1/5/10/50

Quick Start Guide

MultiTech®
Systems

Quick Start Guide
82013151 Revision B
SSH IPSec Client Model # RFIPSC-1/5/10/50
for RouteFinder Model # RF650VPN

Record of Revisions

Revision	Date	Description
A	9/7/01	Manual released for SSH Sentinel v1.2.0.15.
B	11/21/01	Manual revised to add RFIPSC-1, license agreement text and editorial changes.

Patents
This Product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562**; **5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

TRADEMARKS
Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo and RouteFinder.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
SSH, ssh, SSH Secure Shell, and SSH Sentinel are trademarks or registered trademarks of SSH Communications Security Corp.
All products or technologies are the trademarks or registered trademarks of their respective holders.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Tech Support (800) 972-2439
Internet Address: http://www.multitech.com

iv

Contents

Chapter 1 – Introduction and Description

Chapter 2 – SSH IPSec Client Installation and Setup

Chapter 3 - Service, Warranty and Tech Support

Appendix A - RFIPSC-1/5/10/50 Client Software CD   41

Appendix B - Multi-User Software License Agreement   45

Figures

Chapter 1 – Introduction and Description

Introduction

Welcome to Multi-Tech's new RouteFinder, model RF650VPN. The RF650VPN is an Internet security appliance that lets you use data encryption and the Internet to securely connect to telecommuters, remote offices, customers or suppliers while avoiding the cost of expensive private leased lines.

The SSH Sentinel IPSec VPN Client software is available in 1-, 5-, 10- and 50-user packages. The RF650VPN provides SSH Sentinel version 1.1.1 client software (30-day trial Internet Pilot version with Static IP support). It allows client computer connection to the RF650VPN using PSK (Pre Shared Keys) in a Host-to-Net connection.
Chapter 2 of this manual describe the SSH IPSec VPN client installation and setup process for the full 1-, 5-, 10- or 50-user Sentinel SSH IPSec VPN client packages with these Multi-Tech model numbers:

Model	Description
RFIPSC-1	SSH IPSec VPN Client 1-User License
RFIPSC-5	SSH IPSec VPN Client 5-User License
RFIPSC-10	SSH IPSec VPN Client 10-User License
RFIPSC-50	SSH IPSec VPN Client 50-User License

Product Description

SSH Sentinel is a software product for securing Internet Protocol (IP) based traffic using the IPSec protocol - as specified by Internet Engineering Task Force (IETF) standards.
SSH Sentinel is an easy-to-use product designed for end users. It allows you to encrypt and authenticate important network connections, like remote access to corporate networks remote administration, file transfer, sending and receiving email (SMTP, POP) and IP telephony.
SSH Sentinel software currently supports the following Microsoft Windows operating systems: Windows 95, Windows 98, Windows NT4, Windows Me and Windows 2000.
SSH Sentinel is designed to be a *client* type IPSec application. The features are designed for a single user workstation using a single network adapter and the Internet Protocol (IP). SSH Sentinel supports all network connection types, including dial-up.
The product is designed to be secure and robust, easy to use, and quick to adapt to the environment at hand.
Key characteristics include intuitive installation and configuration, as well as an easy way to use certificates for authentication.

Internet Protocol (IP)

The open architecture of the Internet Protocol (IP) makes it a highly efficient, cost-effective and flexible communications protocol for local and global communications. IP is widely adopted, not only on the global Internet, but also in the internal networks of large corporations.

The Internet Protocol was designed to be highly reliable against random network errors. However, it was not designed to be secure against a malicious attacker. In fact, it is vulnerable to a number of well-known attacks. This is preventing it from being used to its fullest for business and other purposes involving confidential or mission-critical data. The most common types of attacks include:

- Eavesdropping on a transmission, for example, looking for passwords, credit card numbers, or business secrets.
- Taking over communications, or hijacking communications, in such a way that the attacker can inspect and modify any data being transmitted between the communicating parties.
- Faking network addresses, also known as IP spoofing, in order to fool access control mechanisms based on network addresses, or to redirect connections to a fake server.

Internet Protocol Security (IPSec)

Internet Engineering Task Force (IETF) has developed the Internet Protocol Security (IPSec) protocol suite to prevent misuse and attacks on IP. IETF is an international standards body with representation from hundreds of leading companies, universities, and individuals developing Internet-related technologies. Its track record includes the Internet Protocol itself and most of the other protocols and technologies that form the backbone of the Internet.

The IPSec protocol suite adds security to the basic IP version 4 protocol and is supported by all leading vendors of Internet products. IPSec is a mandatory part of the next generation of IP protocol, IP version 6. The IPSec protocol works on the network level. It adds authentication and encryption to each data packets transmitted. It protects each packet against eavesdropping and modification, and provides authentication of the origin of the packet.

IPSec works independently of any application protocol. Thus, all applications that use IP protocol for data transfer are equally and transparently protected. IPSec makes it safe to use the Internet for transmitting confidential data. By doing so, it solves the main obstacle that is slowing down the adoption of the Internet for business use.

About this Manual and Related Manuals

This Quick Start Guide manual contains four chapters and one appendix, and is intended to provide the experienced client user or system administrator with the information needed to quickly get the SSH IPSec Client software up and running. The full Sentinel SSH IPSec Client User Guide manual is provided on the SSH IPSec Client CD-ROM included in the license pak.

Please address comments about this manual to the Multi-Tech Publications Dept. Related manuals may include add-on product documentation for options such as the Windows PPTP client, the E-Mail Anti-Virus Upgrade, etc.

This document may contain links to sites on the Internet, which are owned and operated by third parties. Multi-Tech Systems, Inc. is not responsible for the content of any such third-party site.

Ship Kit Contents

The SSH IPSec Client License Pak is shipped with the following:

· one SSH IPSec CD-ROM
· one SSH IPSec Client License
· one printed Quick Start Guide manual
· one Multi-User Software License Agreement
· one Registration Card

If any of these items are missing, contact Multi-Tech Systems or your dealer or distributor. Inspect the contents for signs of any shipping damage. If damage is observed, do not install the software; contact Multi-Tech's Tech Support for advice.

PN 82013151

Chapter 2 - SSH IPSec Client Installation and Setup

Introduction

This section describes the SSH Sentinel software, an IPSsec client product by SSH Communications Security Corp, providing secure communications over a TCP/IP connection. The Sentinel SSH software is used by client devices for secure connection to the Multi-Tech RouteFinder model RF650VPN. The SSH Sentinel client installation and setup procedures are described in the following sections.

The installation of the SSH Sentinel software is a straightforward process guided by an installation wizard, and you should be able to complete it without studying this manual. This beginning of this section describes the first installation of the SSH Sentinel software. During the installation, you create an authentication key pair and a matching certificate to be used for authentication. However, if a previous version of the software is already installed on your computer, then launching the installation only updates the existing software to the new version. The security policy rules and the authentication keys that you have configured with the previous version of the software are preserved. You can always remove the software completely and then reinstall it.

Pre-Installation Requirements

SSH Sentinel client software works on the following Microsoft Windows platforms and versions:

Platform	Version Build	Notes
Windows 95	OSR1, OSR2	Winsock2 required
Windows 98	SE	-
Windows NT 4.0	SP3 to SP6	-
Windows Me		-
Windows 2000	SP1	-

SSH Sentinel is a client-type implementation of IPSec; it is not IPSec gateway software, even though some of the Windows platforms are capable of functioning as routers. Before starting SSH Sentinel client installation, make sure that there are no other IPSec implementations, network sniffers, NAT applications, firewalls, or third party intermediate network drivers installed. SSH Sentinel may affect the functionality of such software.

The SSH Sentinel installation requires that you have full access rights for the system files on your computer. On a Windows NT system, you must log in with administrator rights.

11

To run the SSH Sentinel client software, you need a personal computer with at least the following configuration:
- Processor Pentium 100 MHz
- Memory (RAM) 32 MB for Windows 9x, or 64 MB for Windows NT4/2000
- Hard disk space 10 megabytes of free disk space
- Network connection TCP/IP network protocol

Starting the SSH Sentinel Installation
The SSH Sentinel installation requires that you have full access rights for the system files on your computer. On a Windows NT system, you must log in with administrator rights.

1. In Windows Explorer, double click the SSH Sentinel installation package icon **Sentinel.exe**.   The **Sentinel.exe** file is included on the RFIPSC-5/10/50 SSH Sentinel IPSec Client CD (refer to Appendix A of this manual for more information on the CD).

Figure 1. The SSH Sentinel installation package icon.

The self-extracting package automatically initiates InstallShield® software to install and set up SSH Sentinel Client software.

Figure 2. SSH Sentinel Welcome screen.

The installer will run Installation Wizard, which creates the initial configuration and sets up the SSH Sentinel client software.

Note: If a previous version of the SSH Sentinel software is installed on your computer and you try to install a new version, the wizard updates the software and the steps described here are skipped.

3. When started, the Installation Wizard goes through a sequence of basic installation dialogs, displaying the licensing agreement and allowing you to select the installation directory and the program folder. The installation can only be performed on a local computer. Remote installation of SSH Sentinel is not possible, because the installation program updates kernel mode components related to networking and remote access.
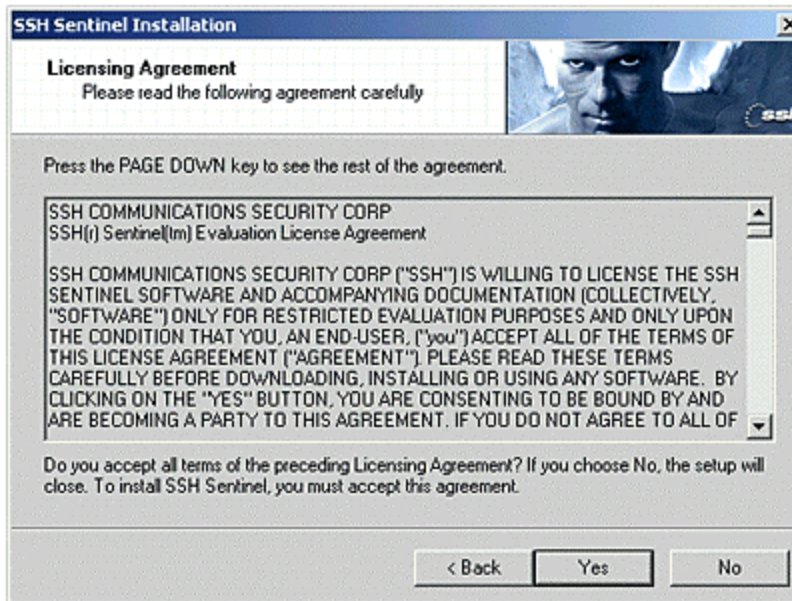

Figure 3. Licensing Agreement

Note that the installation will terminate immediately if you do not accept the licensing agreement.
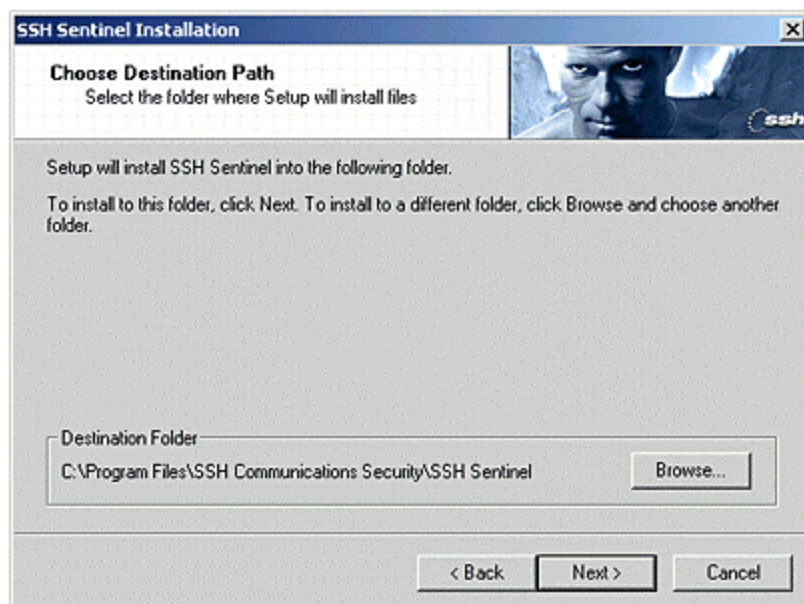
Figure 4.   Choose Destination Path.

Authentication Key Generation
The SSH Sentinel Installation Wizard generates a primary authentication key for IPSec peer (host) authentication purposes. The primary authentication key is a 1024-bit RSA key pair that is used for digital signatures and strong authentication.

Authentication key generation begins with random seed generation. A random pool of data is collected from the user moving the mouse or typing in random text. The data is then used as a seed to ensure that all authentication keys will be unique. With this method, the likelihood of generating two identical authentication keys is infinitesimal.

The general level of security that can be provided with 1024-bit RSA authentication keys is considered military strength. The Internet Key Exchange (IKE) protocol used in key negotiation is better by design and security than most of the other solutions that currently exist.
The SSH Sentinel key generation process will take some 30 seconds and may momentarily use most of the computer's CPU resources.

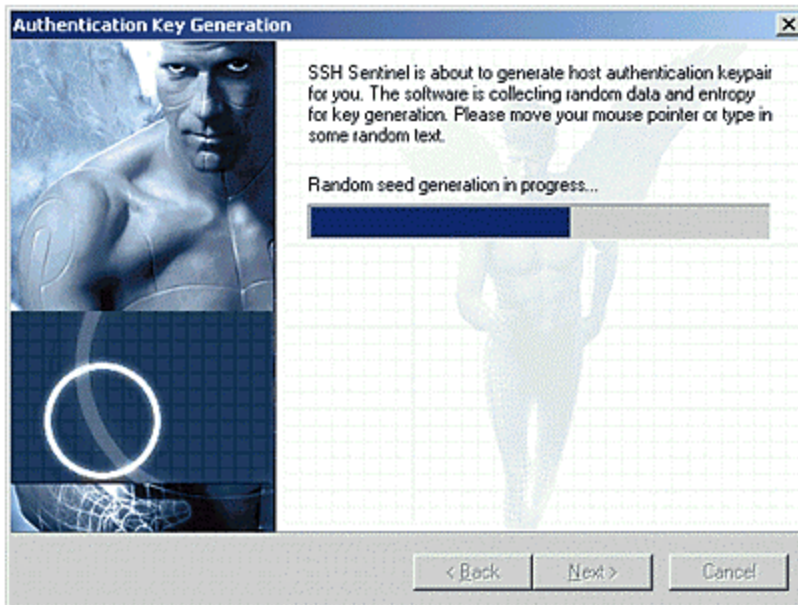4. Once the authentication key generation is complete, proceed with the installation.

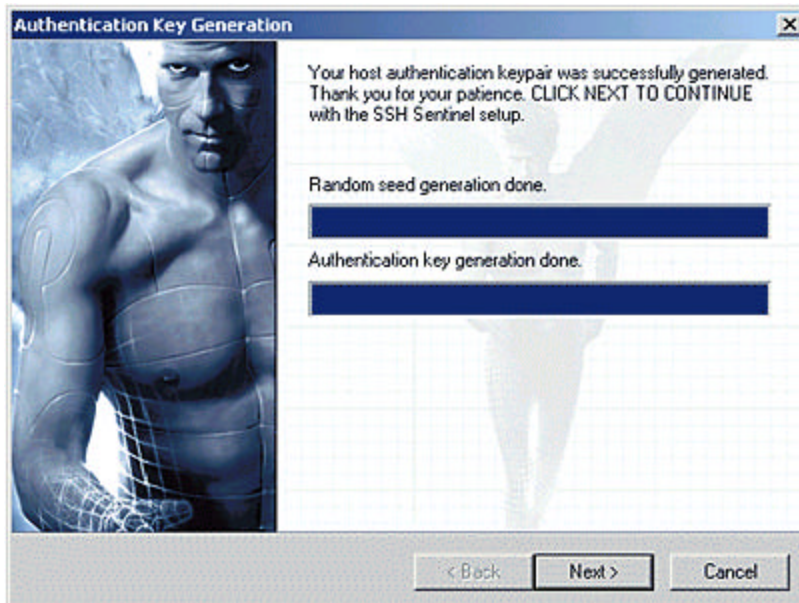Figure 5.   Generating the Authentication Key.

Figure 6.   Authentication Key Generation Done.

Identity Information

5. SSH Sentinel uses certificates and digital signatures as its primary authentication method. SSH Sentinel processes certificates according to the IETF Public-Key Infrastructure X.509v3 standards, allowing you to take advantage of the public-key infrastructure (PKI). SSH Sentinel supports certificate revocation lists (CRLs) and authority revocation lists (ARLs, that is, CRLs for CAs) and is very configurable. However, you can run the software as stand-alone, separately from any public-key infrastructure.

The setup requires host identity information that is to be associated with the authentication key pair and its certificate. A commonly preferred identity is the host DNS name, also referred to as the Fully Qualified Domain Name (FQDN). The DNS name should be used as the identity whenever the host has a static DNS name and whenever it is safe to assume that name service will be available. If the host does not have a static DNS name, its static IP address may be used as the host identity.

If neither static DNS name nor IP address is available, you may use an email address as the identity. However, using an email address as the identity makes it difficult for remote hosts to bind IPSec rules for the host, since rules are normally bound to a host name or an IP address.

Figure 7. Inquiring Certificate Identity.

Choose the Enrollment Method

6. A certification request can be created as part of the installation process. You can either enroll online, in other words create and send the request immediately, or save the request in a file and deliver it later to the certification authority (CA). If there is no certification authority available or you for some reason want to postpone the creation of the request, create a self-signed certificate. It should be noted that once you've installed the software, you can create as many certification requests as you wish with the SSH Sentinel user interface but you cannot create a self-signed certificate with it.
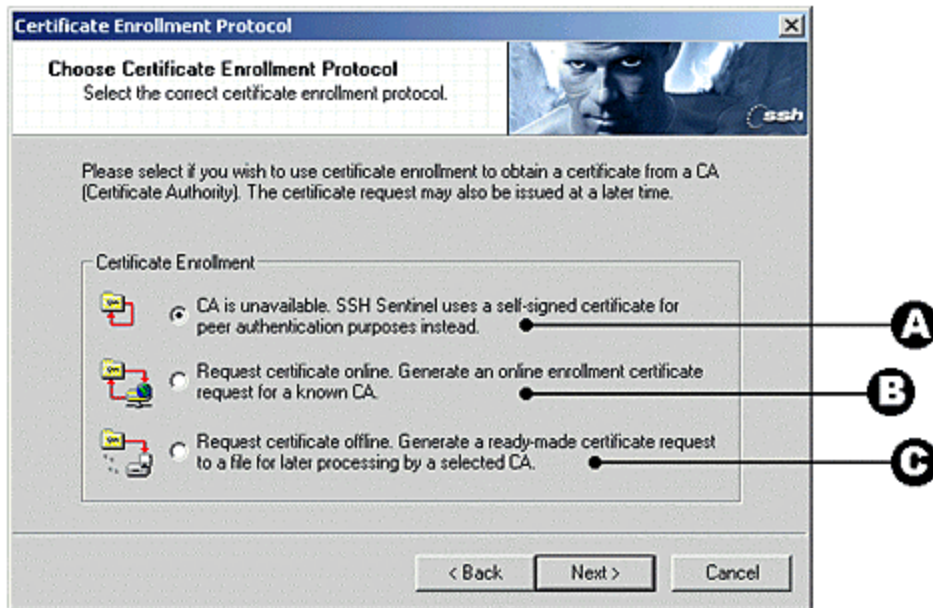
Figure 8. Choosing a Certificate Enrollment Protocol.

7. Choose a **Certificate EnrollmentProtocol:**

A - To create a **self-signed** certificate, select the option **CA is unavailable. SSH Sentinel uses...**
(option A in Figure 8 above). The keys created in the previous step are used when the system creates the certificate.

B - To issue an **online** certification request, select the option **Request certificate online**. **Generate an online...** (option B in Figure 8 above). The installation wizard shows you a dialog where further information on the certification authority and the enrollment protocol is asked for. Refer to the section entitled **Online Enrollment** for reference.

C - **Offline**   - To create a certification request and save it in a file for later processing , select the **option Request certificate off-line. Generate a ...** (option C in Figure 8 above). Refer to the section on **Off-line Certification Request** for the next step.

Online Enrollment Information
To enroll online, you must locate the certification authority server and you must possess the certification authority certificate. Most often, you can download the certificate of the certification authority from its web site.
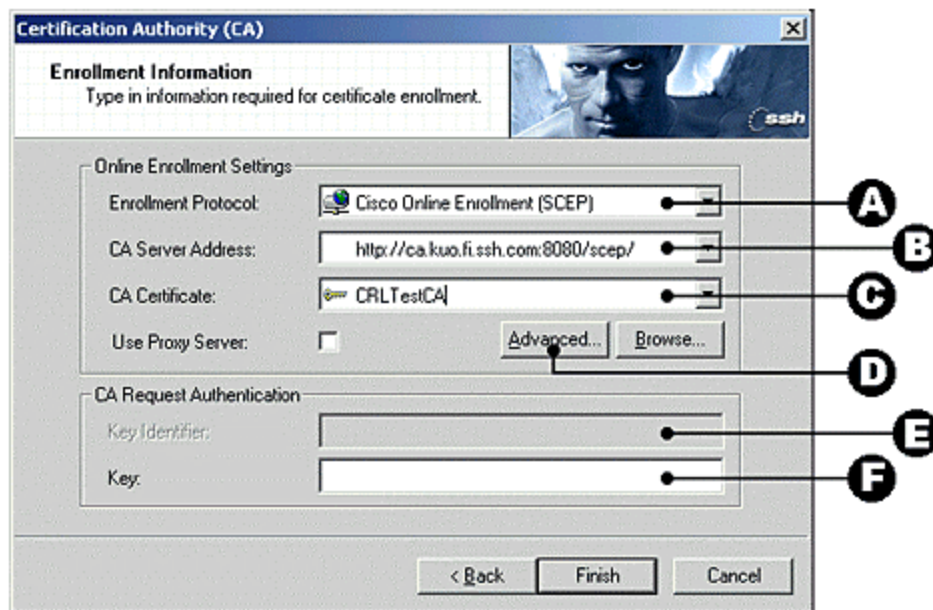

Figure 9. Online Enrollment Settings

You must also specify the enrollment protocol. In addition, you may configure the Socks and proxy settings to get through the firewall if the local server is protected by one.

Enrollment Protocol (A)
Select the enrollment protocol from the drop-down list. Naturally, you should choose a protocol that is supported by the certification authority. The following protocols are available: Simple Certificate Enrollment Protocol (SCEP) and Certificate Management Protocol (CMP).

CA Server Address (B)
Specify the address (URL) of the certification authority web site.

CA Certificate (C)
The certificate of the certification authority is needed to encrypt the certification request before sending it to the certification authority. You can usually fetch it from the authority's Web site.
In the drop-down menu, you see the possibilities on how to import the certification authority certificate into the request: The most convenient way is to specify here the URL where the certificate is located. In this case, the certificate must be in PEM encoded format. SSH Sentinel then automatically fetches the certificate from the web site. You may also have downloaded the certificate earlier using a web browser and

18

either saved it in a file or copied the contents of it to the Windows clipboard. In a file, the certificate may be in binary (X.509), PEM (Privacy Enhanced Mail) or HEX format. Pasted from the clipboard, the certificate must be in PEM encoded format.

Advanced button (D)
Opens a dialog box for configuring the socks and proxy settings.

Reference Number (E) (Key Identifier)
The key identifier is used *only in connection with the Certificate Management Protocol (CMP).* The key identifier is used along with the key to identify the user requesting a certificate.

Key (F)
This selection is used *only in connection with the CMP protocol.* The **Key** selected is a shared secret granted by the certification authority to be used in the certification request. This **Key** is used for verification of the user requesting a certificate.

Off-line Certification Request
An off-line certification request is simply a file, where the request is stored for later use.
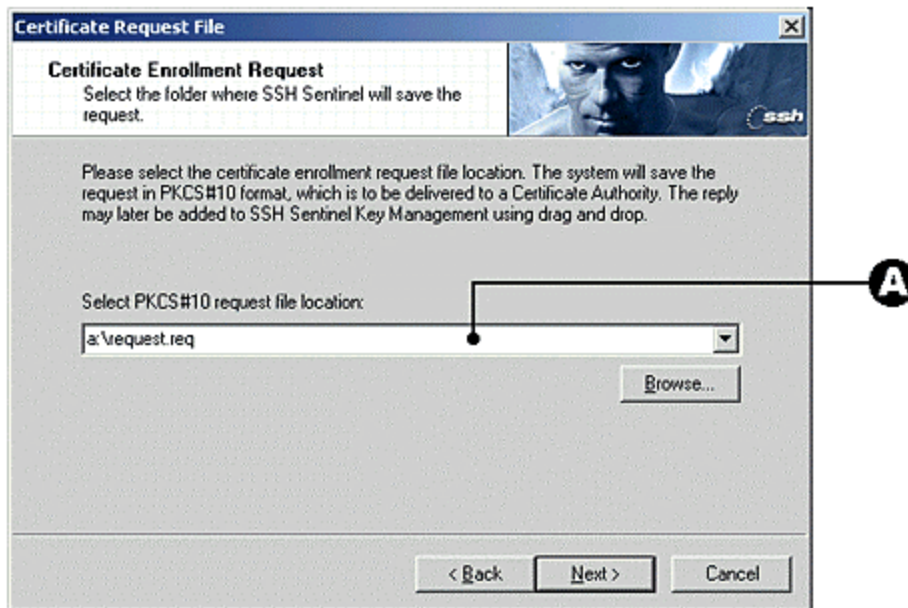

Figure 10: Off-line request: specifying where the request file is to be temporarily stored.

The request is of PKCS#10 format and saved in Privacy Enhanced Mail (PEM) encoded format.
To complete the enrollment, you must deliver the request to the certification authority. You might save the request on a floppy disk and deliver the floppy to the authority, or

19

you may prefer sending the request via email or using an enrollment service on the Web.

Select PKCS#10 request file location
In the text field (callout A in Figure 10 above), enter the path and the name of the file where the certification request will be stored. You can also click the **Browse** button to select.   Click **Next** and continue installation.

Encryption Speed Diagnostics
8. SSH Sentinel runs diagnostics on the encryption algorithms as the last step of the installation. You can bypass this step by clicking the **Skip** button on the dialog box. These diagnostics reveal the speeds of the encryption algorithms compared to each other. SSH Sentinel supports the following ciphers: Rijndael, Twofish, Blowfish, Cast, 3DES and DES.
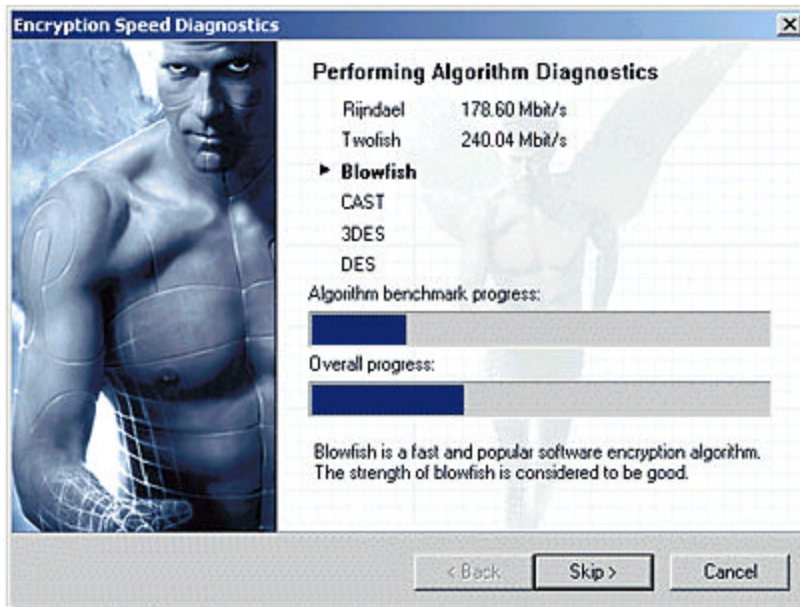
Figure 11. Encryption Speed Diagnostics screen.

With the exception of DES, all of these ciphers can be considered secure for commercial use.
The DES encryption algorithm is supported as a fallback option for interoperability reasons. Rijndael, an encryption algorithm widely considered fast, secure and reliable, is used as the default cipher by SSH Sentinel.

The diagnostics also reveal the relative speed of your computer running the algorithms. There is a lot of contradictory information available on encryption speeds. The diagnostics give you the chance to use your own judgment. The diagnostics measure the encryption speed of your computer within the memory. The data packets are not transmitted to the network. This is a common way to measure performance by

20

encryption hardware vendors. It has the advantage of giving simple figures on the speed: Due to a number of variables that affect the final result, it would be very complicated to define a standard environment in which to reliably measure the overall network throughput. Moreover, the real-world network throughput simply cannot be measured during the installation, because the kernel-mode IPSec engine is not available before the first reboot.

An Intel P3 personal computer with processor speed of 800 MHz should be able to provide a maximum IPSec throughput of over 40 Mbit/s on the preferred cipher. However, other variables, such as the operating system, network bandwidth and CPU load, naturally set limitations to the throughput.

Completing the Installation
9. The installation of the SSH Sentinel client software adds kernel-mode components to the operating system network management. For this reason, you must restart the computer before using the software.
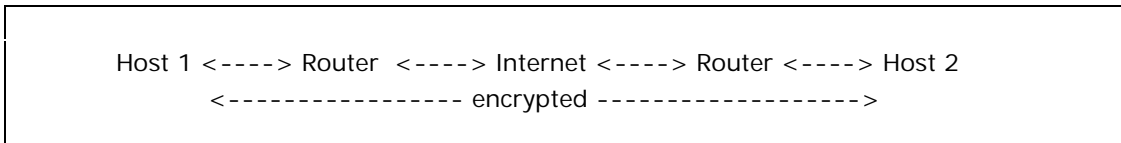

Figure 12. SSH Sentinel Installation Completed screen.

The SSH Sentinel installation is complete. Proceed to the next section for SSH IPSec client setup.

SSH IPSec Client Setup

The RouteFinder supports VPN (Virtual Private Networking), which provides the ability to encrypt IP network traffic.

```
         Host 1 <----> Router  <----> Internet <----> Router <----> Host 2
                 <---------------- encrypted ------------------->
```
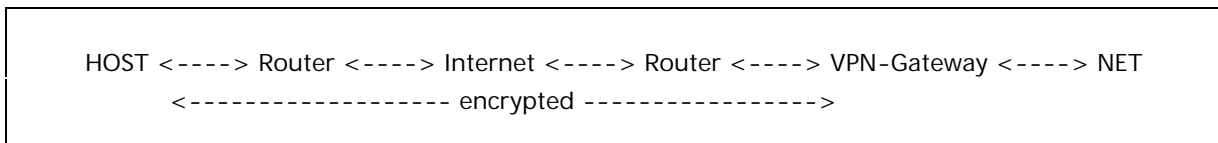
All communication between the hosts uses strong encryption, so that nobody is able to listen to this communication. As discussed earlier, the three methods of VPN setup are Host to Host, Host to Net, and Net to Net. This section covers the client-side aspects of a Host to NET connection using SSH Sentinel 1.1.1 (Static IP) to connect to a RouteFinder using Pre Shared Keys (PSK)

Host to Net Setup

This is one of the most common setups, and is often used for the roadwarrior setup. This setup lets the Host access an Internet connection that is encrypted and authenticated.
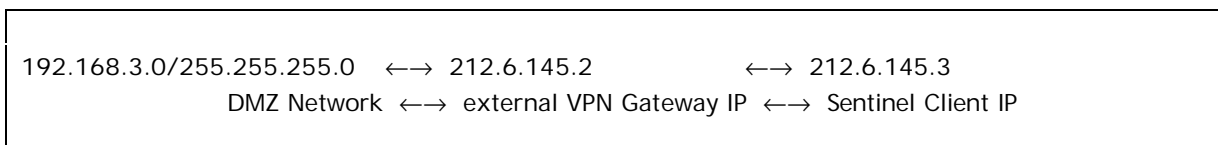
An example of a Host to Net setup is a sales representative that dials into the Internet and establishes a VPN connection to the company RouteFinder, and gains with that an encrypted and authenticated connection to the corporate LAN or DMZ or E-mail server.

```
      HOST <----> Router <----> Internet <----> Router <----> VPN-Gateway <----> NET
             <------------------ encrypted ------------------>
```

Note: Make sure that all routers between both SSH IPSec ends can route IP protocol 50 (IPSec). Sometimes routers are configured to route only TCP (protocol 6), UDP (protocol 17) and ICMP (protocol 1) and drop all other protocols. Routers configured that way won't work for VPN with IPSec!

Host to NET using SSH Sentinel 1.1.1 (Static IP) to connect to a RouteFinder using Pre Shared Keys (PSK)

This section describes how to set up a Host to Net connection between a Sentinel SSH version 1.1.1 client and a RouteFinder using IKE, PSK and static IPs. The setup involves 1) RouteFinder Configuration steps, and 2) Sentinel Configuration steps.

```
192.168.3.0/255.255.255.0   ←→  212.6.145.2               ←→  212.6.145.3
              DMZ Network  ←→  external VPN Gateway IP  ←→  Sentinel Client IP
```

22

RouteFinder Configuration

1. Define two networks in **Definitions**|**Networks**:

   DMZ Network   192.168.3.0 255.255.255.0
   Sentinel ssh Client 212.6.145.3 255.255.255.255

2. Define and enable the following Packet Filter rules:

   Sentinel ssh Client ←→ Any ←→ DMZ Network ←→ Allow
   DMZ Network ←→ Any ←→ Sentinel ssh Client ←→ Allow

The first rule allows the Sentinel SSH Client to initiate connections to the DMZ Network. The second rule allows the DMZ Network to initiate connections to the Sentinel SSH client.

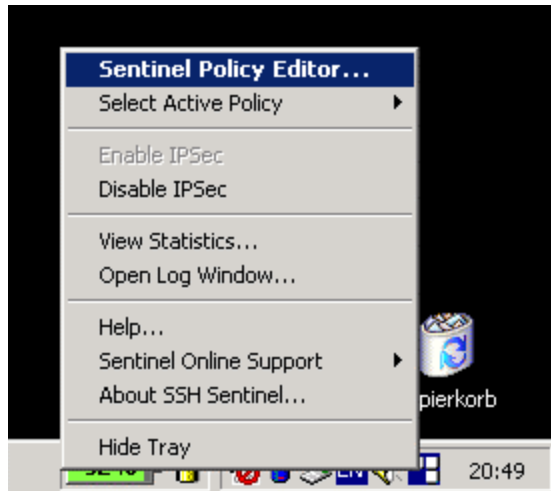3. At **VPN**|**IPSec Configurations** add a **New connection** for the Sentinel SSH IPSec client.

Figure 13. RouteFinder Add a **New Connection** screen.

23

PN 82013151

Sentinel Configuration

4. From the Control panel select the **Sentinel Policy Editor**.

5. At **Key Management** select **Authentication Keys**.

6. Click **OK**.

24
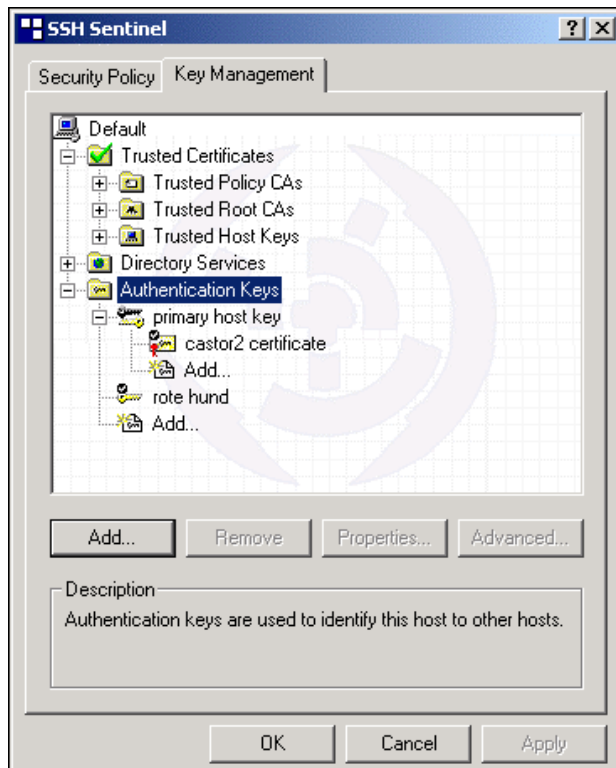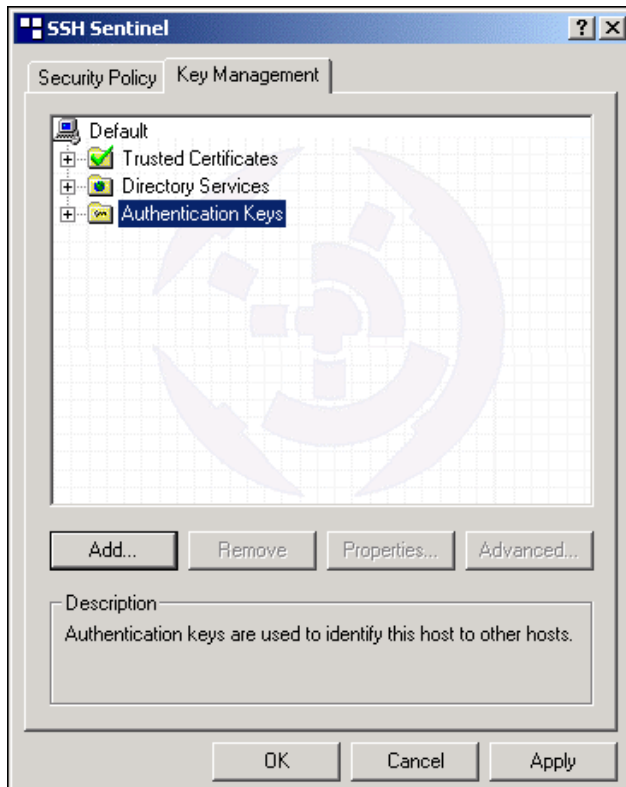
7. Click **Add** to create a new Authentication Key.
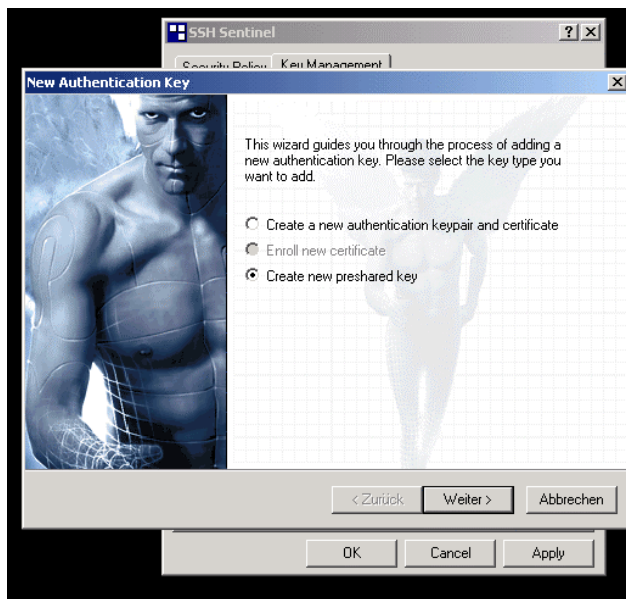
8. Check the **Create new preshared key checkbox** and click **OK**.
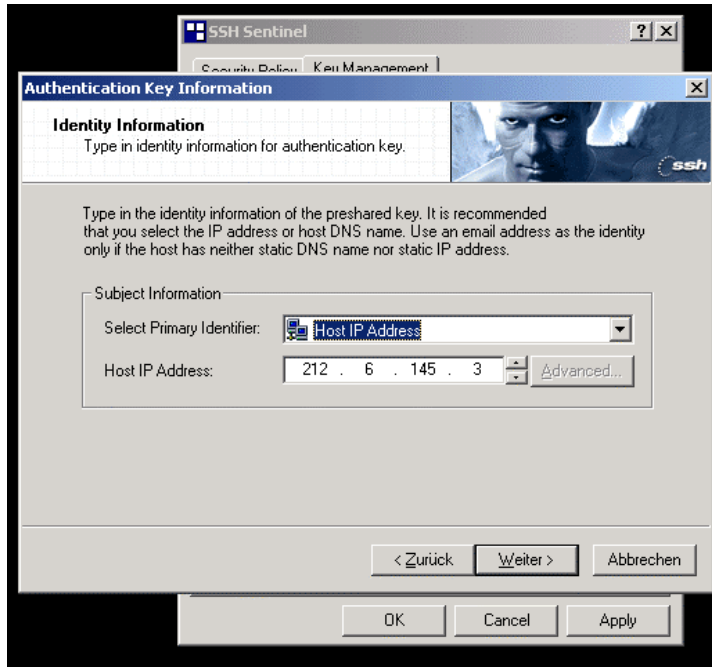
9. Select a Primary Identifier from the **Select Primary Identifier** drop down list.
Select a **Host IP Address** and click **OK**.
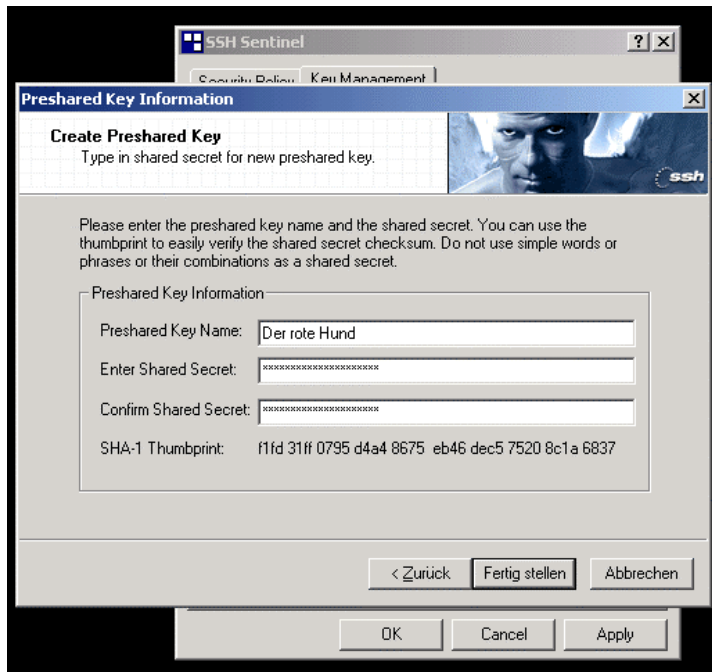
10. Enter the **Preshared Key Information** and click **OK**.
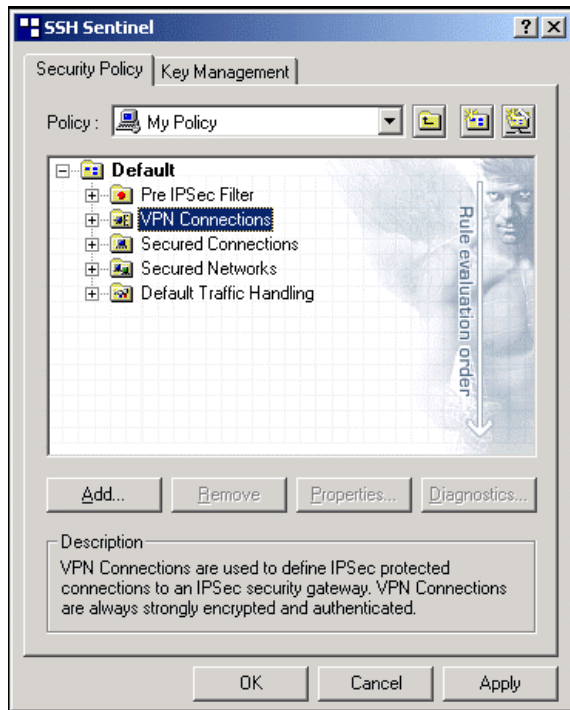
11.   Select **VPN Connection** and click **OK**.
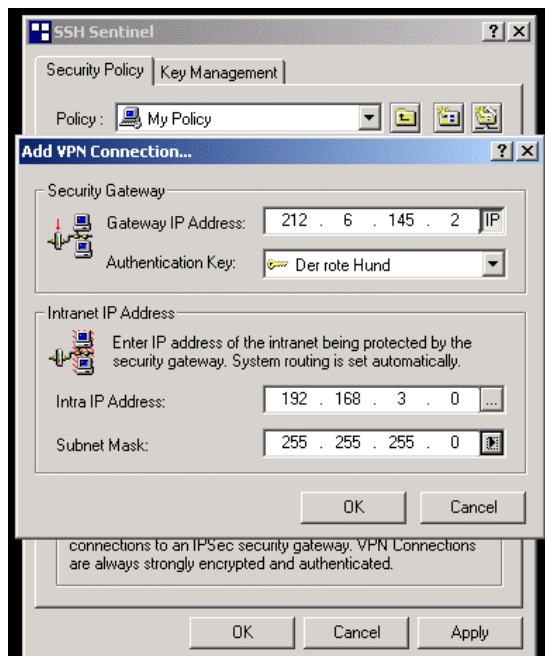
12. Select the **Security Gateway** and **Intranet IP Address** information and click **OK**. Note that the System routing (**Subnet Mask**) is set automatically. The RouteFinder looks for the **Intra IP Address** that you entered.
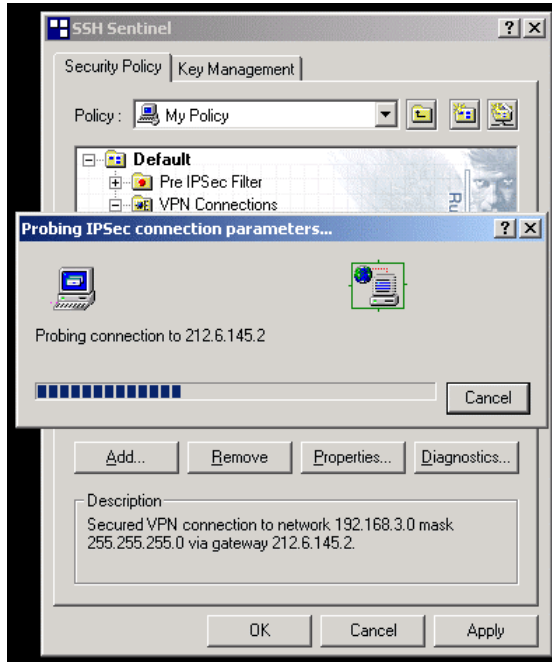
If the **Intra IP Address** that you entered is not found, the **Probe Results** .. **unsuccessful** screen is displayed.
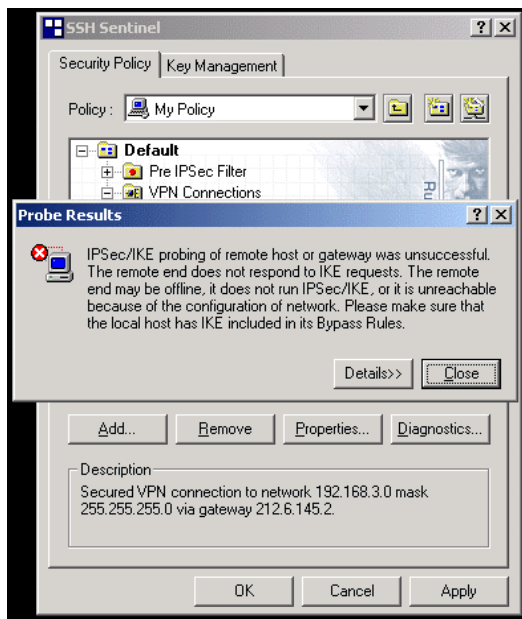
13. Click **Details>>** . The **Connection Properties|General** screen is displayed.
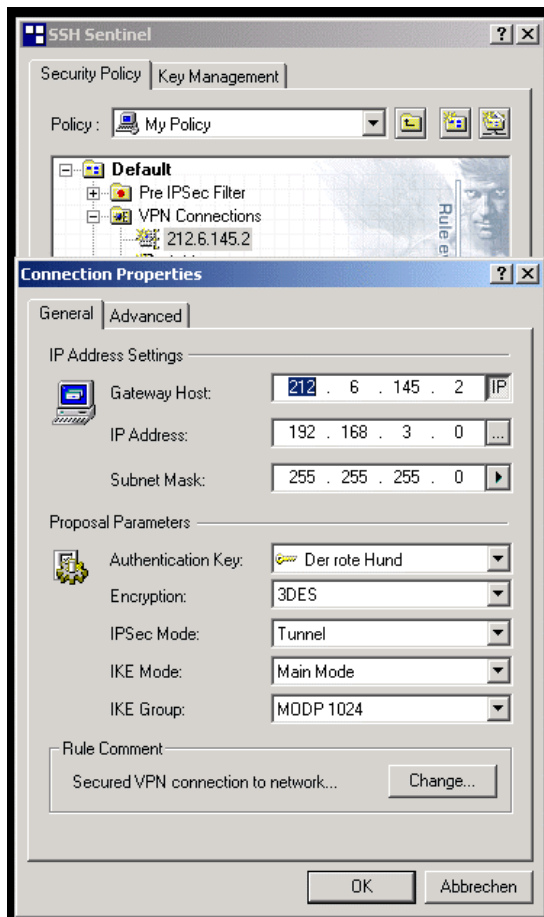
14. Edit the **IP Address Settings** and the **Proposal Parameters**, then change the **Rule Comment** (if necessary). Click **OK**.

15. Click on the **Advanced** tab.
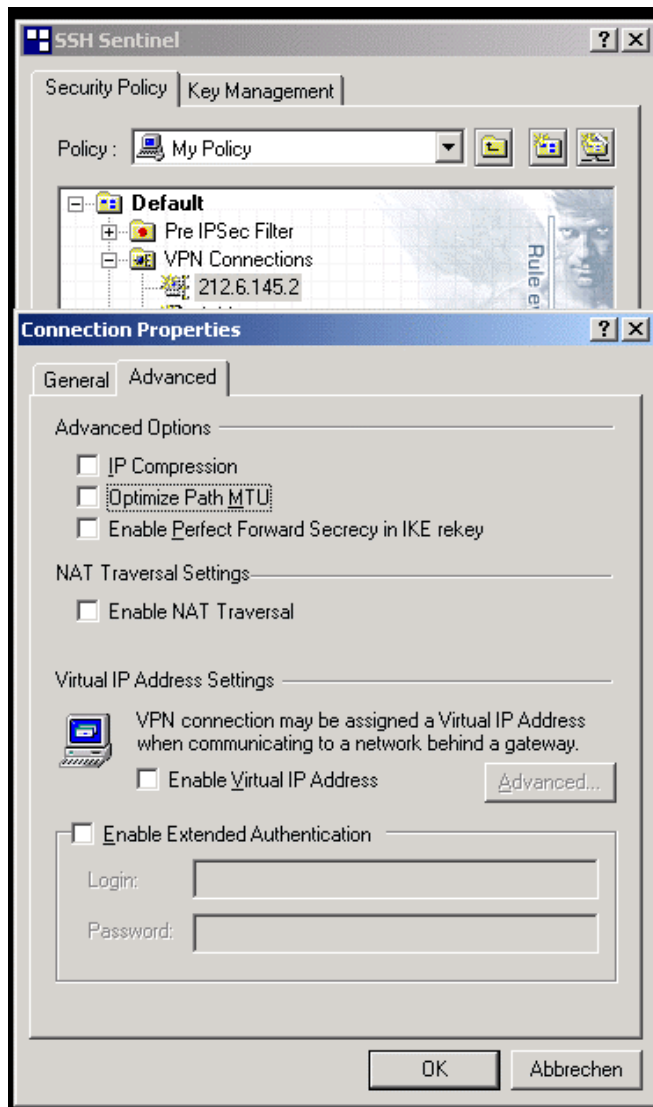
16. As necessary, edit the **Advanced Options**, **NAT Traversal**, **Virtual IP Address Settings**, and/or check the **Enable Extended Authentication** check box and click **OK**.
The Probe Results screen displays.
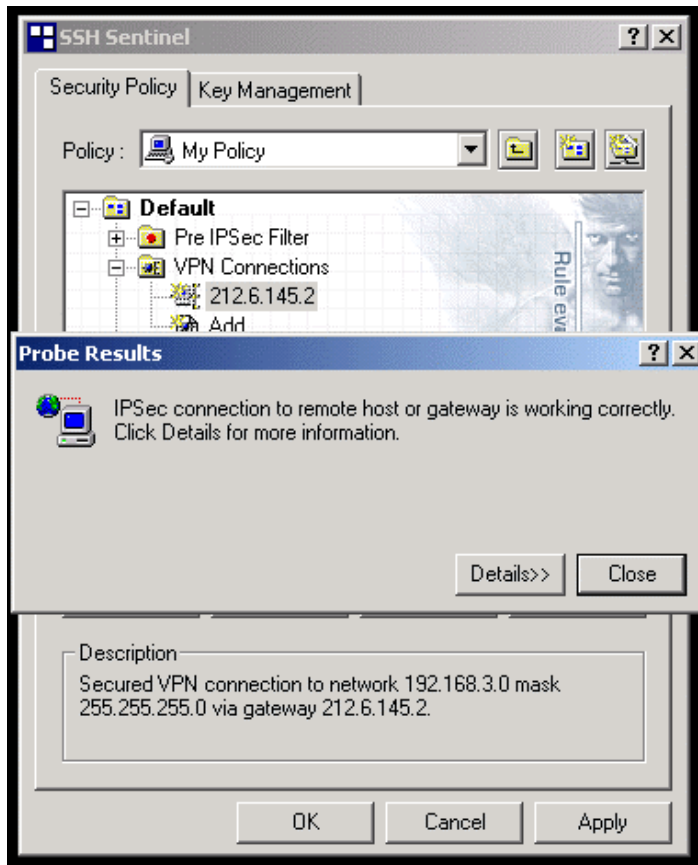
17. Click **Details>>** .
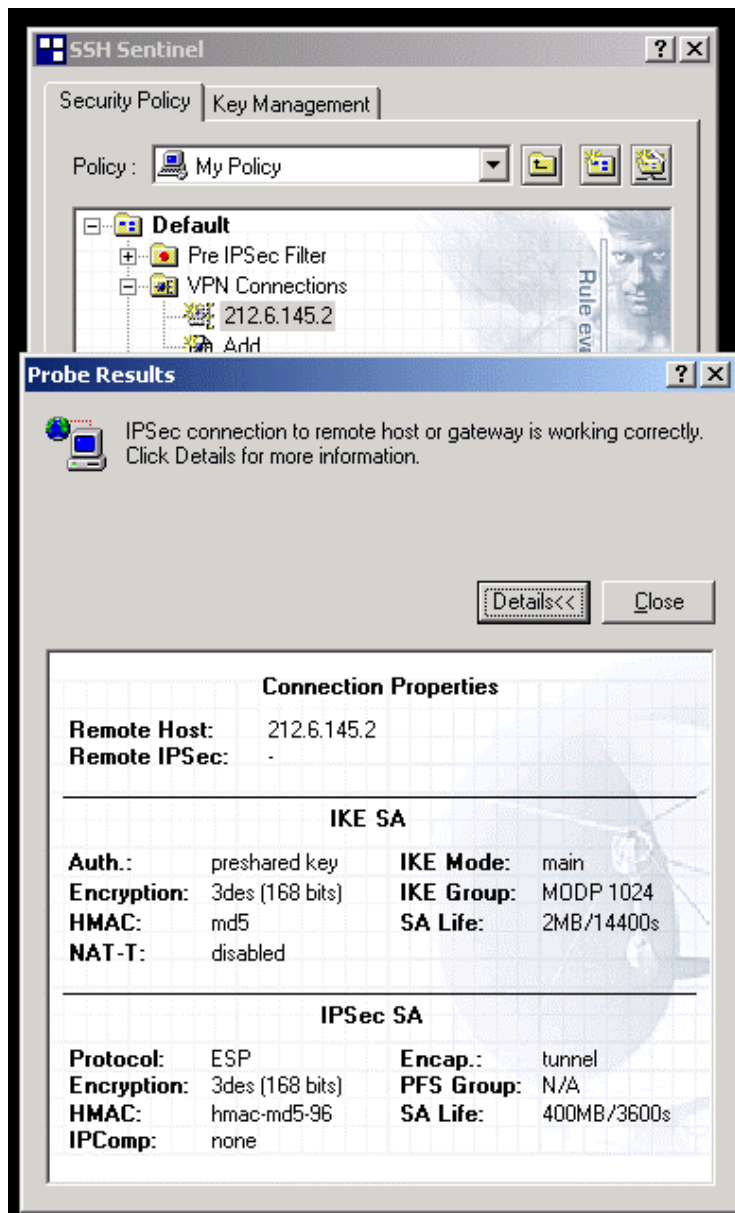
18. Verify the connection details information and click **Close** .

The Security Policy begins updating.
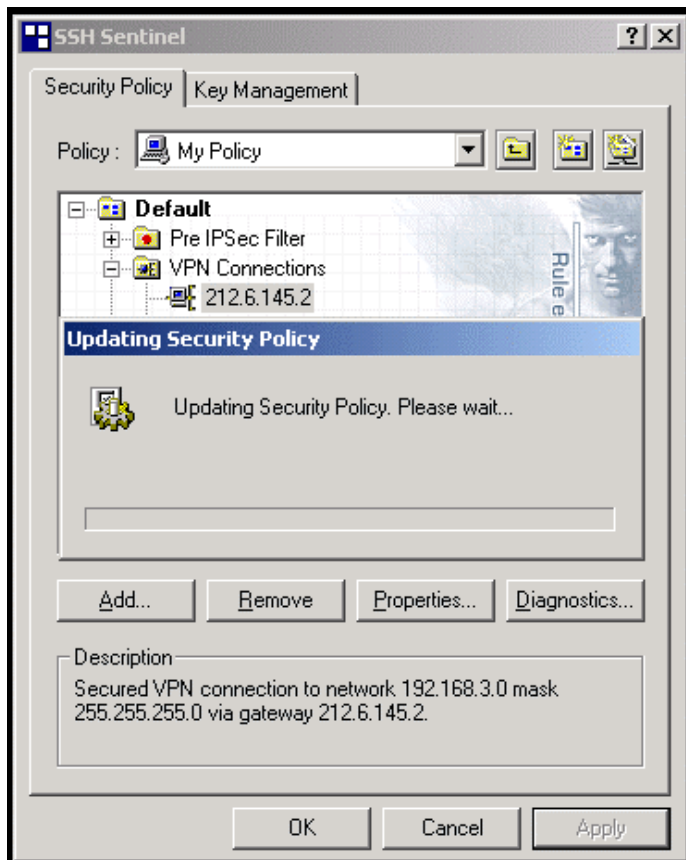
19. When the Security Policy is done updating, click **Diagnostics ...** to Ping the new connection.
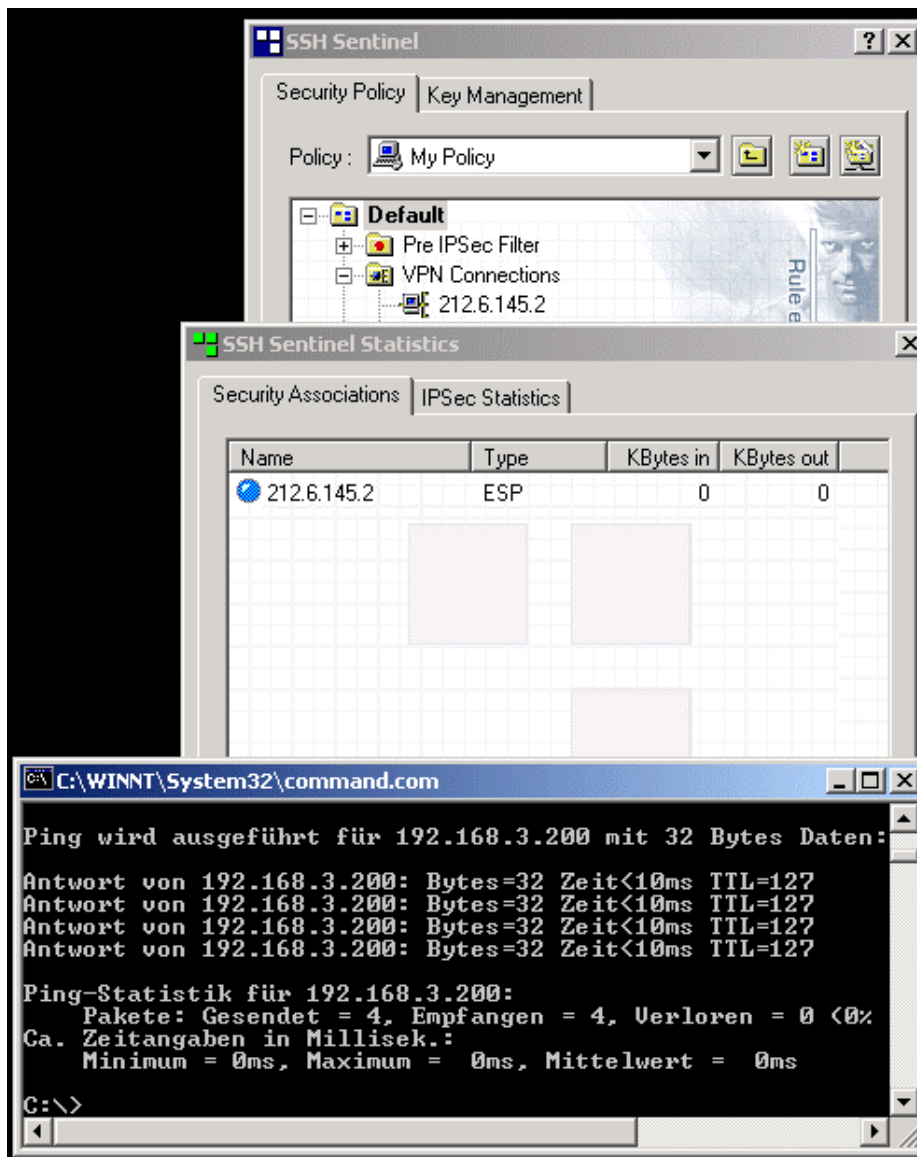
If the ping is successful, the Host to NET using SSH Sentinel 1.1.1 (static IP) to connect to a RouteFinder using Pre Shared Keys (PSK) process is complete.

SSH Sentinel Installation Notes

SSH Sentinel supports Microsoft Windows 95/98, Windows Me, Windows NT 4.0 and Windows 2000. The SSH Sentinel software download site is at http://www.ssh.com/products/sentinel/beta/.

Start the SSH Sentinel setup program (**Sentinel.exe**) by double clicking the icon and follow instructions on the screen. The installation procedure is documented in the SSH Sentinel User Manual.

One thing you might get stuck with is when the setup program asks you about creating certificates. You should determine whether to enroll for a certificate from a certification authority or to create a self-signed certificate. However, once you have the Sentinel running on your computer you can return to creating certificates at any time, using the user interface.
So, if you are not sure what to choose, select creating a self-signed certificate in order to successfully complete the installation procedure.
The self-signed certificate is a valid authentication document in many circumstances.
If you later discover a need for a certificate granted by a certification authority, you can enroll for it with no extra trouble.

For basic installation a network or Internet connection is not necessary. However, to enroll for a certificate online as part of the installation, you naturally need the Internet connection. But, you can also create an offline certificate request, store it in a file and later send it to a certification authority by e-mail, for example. Or, you can choose to create a self-signed certificate during the installation and enroll for a certificate later, if necessary. Both methods of enrolling, the online
and offline, produce a similar request. The online is, of course, more convenient, because the request is sent automatically.

SSH Sentinel v1.2.0.15 Release Notes

1. New Features:

* SA lifetime settings.
* Smart card support for PCSC / PKCS#15.
* Auditing.
  - Audit options dialog. (Agent menu: Tools\Audit options)
  - Audit log viewer. (Agent menu: Tools\Show audit logs)
* SSH agent's (sshtray) menu layout changed.
* Proposal type selector.
  - Legacy proposal: 3DES, DES, md5, modp 1024.

Updating SSH Sentinel

If you launch the installation package with a previous version of SSH Sentinel software on your computer, the existing version is automatically updated. The contents (i.e., the policies, the rules, the authentication keys, etc.) are preserved. Only the software version is updated.

Removing SSH Sentinel

Before removing the software, you are advised to do the following:

1. Export and save any data in the SSH Sentinel that you might need in the future. For example, you might want to save the trusted root certificates for later use. Since removing the software will delete all files related to the software, save the data in a separate folder.

2. Save all unsaved data in other applications and close all open applications.

To remove the software, use the standard Windows **Remove Programs** procedure:

1. Open **Add/Remove Programs** under **Settings** in the **Start** menu.

2. Select **SSH Sentinel** from the listing.

3. Complete the removal by restarting the computer.

You can re-install the software after completely removing it. Import the saved data to your security policy after installation.

Copyright © 2001 SSH Communications Security Corp. SSH, ssh, SSH Secure Shell, and SSH Sentinel are trademarks or registered trademarks of SSH Communications Security Corp.

Chapter 3 - Service, Warranty and Tech Support

Introduction

This chapter starts out with statements about your RouteFinder two-year warranty. The next section, Tech Support, should be read carefully if you have questions or problems with your RouteFinder. It includes the technical support phone numbers, space for recording your product information, and an explanation of how to send in your RouteFinder should you require service.

Limited Warranty

Multi-Tech Systems, Inc. ("MTS") warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment. MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

On-line Warranty Registration

If you would like to register your RouteFinder electronically, you can do so at the following address: http://www.multitech.com/register/ Tech Support.

Multi-Tech has an excellent staff of technical support personnel available to help you get the

most out of your Multi-Tech product. If you have any questions about the operation of this unit, call 1-800-972-2439. Please fill out the RouteFinder information (below), and have it available when you call. If your RouteFinder requires service, the tech support specialist will guide you on how to send in your RouteFinder (refer to the next section).

Recording RouteFinder Information

Please fill in the following information on your Multi-Tech RouteFinder. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____ Serial No.: _____
Software Version: _____

The Model No. and Serial No. are on the bottom of the RouteFinder; additional information is provided on the SSH IPSec Client pak.

Provide the configuration information (e.g., Default Gateway and other IP addresses used) from the Address Table in Chapter 2 of the RF650VPN User Guide manual, as well as any available LiveLog or Reporting information.

Also, note the status of your RouteFinder including LED indicators, screen messages, diagnostic test results, problems with a specific application, etc. Use the space below to note the RouteFinder status:

_____

_____

_____

_____

_____

_____

_____

_____

Contacting Tech Support via E-mail

If you prefer to receive technical support via the Internet, you can contact Tech Support via e-mail at support@multitech.com or from http://www.multitech.com/ . When responding to e-mails from our technical staff please attach all previous e-mails to assist us in giving you a speedy response. Also include a Case Number if one was given to you. For faster service please contact the Technical Support Pool. Provide model, serial, firmware/software level and operating system as appropriate. Also provide your full name with surname in capitals, company name and contact telephone number.

Service

If your tech support specialist decides that service is required, your RouteFinder may be sent (freight prepaid) to our factory. Return shipping charges will be paid by Multi-Tech Systems. Include the following with your RouteFinder:

- a description of the problem.
- return billing and return shipping addresses.
- contact name and phone number.
- check or purchase order number for payment if the RouteFinder is out of warranty. (Check with your technical support specialist for the standard repair charge for your RouteFinder).
- if possible, note the name of the technical support specialist with whom you spoke.

If you need to inquire about the status of the returned product, be prepared to provide the serial number of the product sent. Send your RouteFinder to this address:

MULTI-TECH SYSTEMS, INC.
2205 WOODALE DRIVE
MOUNDS VIEW, MINNESOTA 55112
ATTN: SERVICE OR REPAIRS

You should also check with the supplier of your RouteFinder on the availability of loaner units and/or local service in your area.

Multi-Tech on the Internet

Multi-Tech's presence includes a Web site at http://www.multitech.com and an ftp site at ftp://ftp.multitech.com.

Ordering Accessories

SupplyNet, Inc. supplies replacement transformers, cables and connectors for select Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax or the Internet at:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989

Phone: 800 826-0279
Fax: 914 267-2420
Email: info@thesupplynet.com
Internet: http://www.thesupplynet.com

39

SupplyNet On-line Ordering Instructions

1. Browse to http://www.thesupplynet.com. In the **Browse by Manufacturer** drop-down list, select **Multi-Tech** and click **GO!** .

2. To order, type in the quantity, and click **Add to Order** .

3. Click **Review Order** to change your order.

4. After you have selected all of your items click Checkout to finalize the order. The SupplyNet site uses Verisign's Secure Socket Layer (SSL) technology to ensure your complete shopping security.

Appendix A - RFIPSC-5/10/50 Client Software CD

The RouteFinder RFIPSC-5/10/50 CD contains the SSH Sentinel IPSec Client files as shown below.

When you insert the CD in your computer's CD-ROM drive, the SSH Sentinel IPSec Client software Install screen displays. (If the **Program Not Found** message displays or if the Auto run feature does not function, click on the file **Autorun.bat** (⬛autorun.bat) in the CDs root directory.

Each of the initial CD Install screen selections is described below.

Click **Install IPSEC Client Software** to load the SSH Sentinel IPSec Client Software and either run the program from the CD or save it to your computer's hard disk drive (the initial screen is shown below).
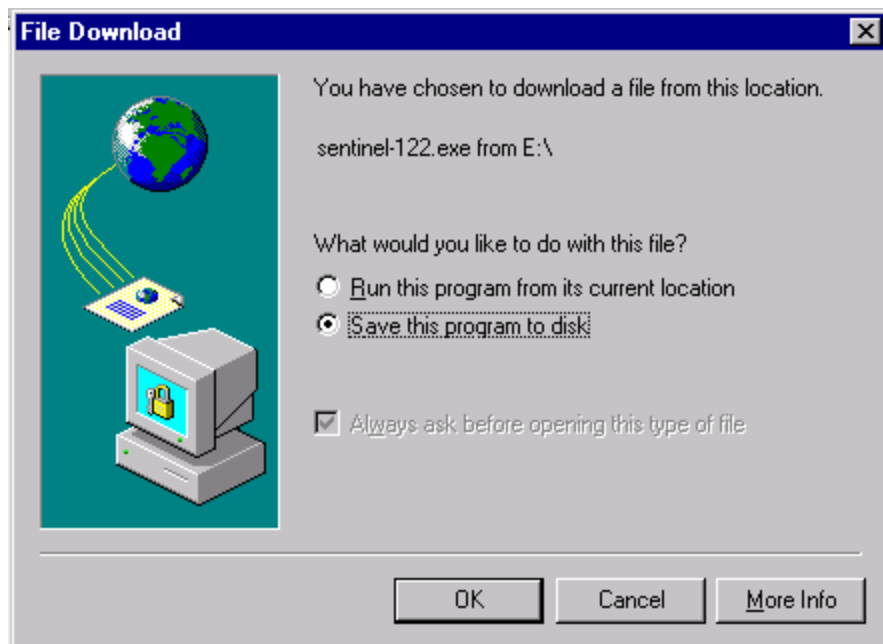
Click **Read the End User Licensing Agreement** to view the Multi-Tech Multi-User Software License Agreement (the initial screen is shown below).

```
Multi-Tech Systems, Inc.
Multi-User Software License Agreement
IMPORTANT - READ BEFORE OPENING OR ACCESSING SOFTWARE

This is a basic multi-user software license granted by Multi-Tech Systems, Inc.,
a Minnesota corporation, with its mailing address at 2205 Woodale Drive, Mounds
View, MN 55112.

This is a legal agreement between you (either an individual or a single entity)
and Multi-Tech Systems, Inc. for the Multi-Tech software product enclosed, which
includes computer software and may include associated media, printed materials,
and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE
PRODUCT also includes any updates and supplements to the original SOFTWARE
PRODUCT provided to you by Multi-Tech.

Any software provided along with the SOFTWARE PRODUCT that is associated with a
separate end-user license agreement is licensed to you under the terms of that
license agreement.
By installing, copying, downloading, accessing, or otherwise using the SOFTWARE
PRODUCT,
you agree to be bound by the terms of that separate end-user license agreement.

This copy of Multi-Tech Systems software is provided only on the condition that
you, Customer, agree to the following license agreement.  READ THIS LICENSE
CAREFULLY.  If you do not agree to the terms contained in this license, return
the packaged program UNOPENED to the place you obtained it. If you agree to the
terms contained in this license, fill out the enclosed Software Registration
Card, and return the card by mail.  Registration may also be done on Multi-Tech
```

Note that the Software License Agreement is also provided in Appendix B of this manual.

Click **Read the Installation User Guide** to view and/or print the full online User Guide manual (this document). You can also find it directly on the CD in Acrobat format *(InstallationGuide.pdf)*, as well as on the Multi-Tech web site (http://www.multitech.com). This is an Adobe Acrobat file - if you don't have the Acrobat Reader, download it from http://www.adobe.com. The full online User Guide manual provides all of the Quick Start Guide information, plus detatiled software operation and maintenance information, plus a glossary of terms and an index.
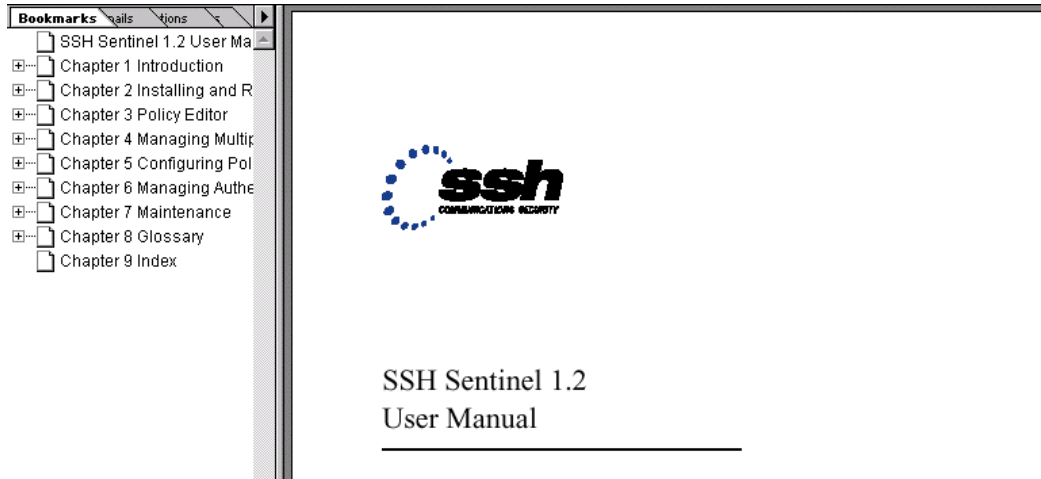
Click **Read the Installation Quick Start Guide** to view and/or print the online Quick Start Guide manual (the printed manual). You can also find it directly on the System CD in Acrobat format *(InstallationGuide.pdf)*, as well as on the Multi-Tech web site (http://www.multitech.com). This is an Adobe Acrobat file - if you don't have the Acrobat Reader, download it from http://www.adobe.com. The electronic version of the printed Quick Start Guide manual provides the information necessary to get the RF650VPN running quickly (how to set up and install the SSH IPSec Client software). For additional information refer to the full online User Guide manual.

Click **Register your product at** www.multitech.com to register your SSH Sentinel IPSEC Client software online at the Multi-Tech web site.

43

PN 82013151

44

Appendix B - Multi-User Software License Agreement

Multi-Tech Systems, Inc.
Multi-User Software License Agreement
IMPORTANT — READ BEFORE OPENING OR ACCESSING SOFTWARE

This is a basic multi-user software license granted by Multi-Tech Systems, Inc., a Minnesota corporation, with its mailing address at 2205 Woodale Drive, Mounds View, MN 55112.

This is a legal agreement between you (either an individual or a single entity) and Multi-Tech Systems, Inc. for the Multi-Tech software product enclosed, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE PRODUCT also includes any updates and supplements to the original SOFTWARE PRODUCT provided to you by Multi-Tech.

Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement.
By installing, copying, downloading, accessing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of that separate end-user license agreement.

This copy of Multi-Tech Systems software is provided only on the condition that you, Customer, agree to the following license agreement. READ THIS LICENSE CAREFULLY. If you do not agree to the terms contained in this license, return the packaged program UNOPENED to the place you obtained it. If you agree to the terms contained in this license, fill out the enclosed Software Registration Card, and return the card by mail. Registration may also be done on Multi-Tech Systems web site at www.multitech.com/register. Opening the packaged program constitutes agreement to be bound by the terms and conditions of this Software License Agreement. Your right to use the software terminates automatically if you violate any part of this software license agreement.

Multi-Tech Software License Agreement
Multi-Tech Systems, Inc. (MTS) agrees to grant and Customer agrees to accept on the following terms and conditions, a non-transferable and non-exclusive license to use the software program(s) delivered with this Agreement.

GRANT OF LICENSE. MTS grants Customer the right to use one copy of the software on a single product (the Licensed System). You may not network the software or otherwise use it on more than one product at the same time.

COPYRIGHT. The software is owned by MTS and is protected by United States copyright laws and international treaty provisions. Therefore, Customer must treat the software like any copyrighted material. Customer may install the software to a single hard disk and keep the original for backup or archival purposes. Customer shall NOT copy, or translate into any language, in whole or in part, any documentation which is provided by MTS in printed form under this Agreement.

OTHER RESTRICTIONS. The software may not be assigned, sublicensed, translated or otherwise transferred by Customer without prior written consent from MTS. Customer may not reverse engineer, decompile, or disassemble the software. Any updates shall be used only on the Licensed System, and shall remain subject to all other terms of this Agreement. Customer agrees not to provide or otherwise make available the software including, but not limited to documentation, programs listings, object code, or source code, in any form, to any person other

45

than Customer and his employees and /or agents, without prior written consent from MTS. Customer acknowledges that the techniques, algorithms, and processes contained in the software are proprietary to MTS and Customer agrees not to use or disclose such information except as necessary to use the software.

Customer shall take reasonable steps consistent with steps taken to protect its own proprietary information to prevent the unauthorized copying or use by third parties of the software or any of the other materials provided under this Agreement. Any previous version of the software must be destroyed or returned to Multi-Tech Systems, Inc. within 90 days of receipt of the software upgrade or update.

LIMITED WARRANTY. MTS warrants that the software will perform substantially in accordance to the product specifications in effect at the time of receipt by Customer. If the MTS software fails to perform accordingly, MTS will optionally repair any defect, or replace it. This warranty is void if the failure has resulted from accident, abuse, or misapplication. A Software Registration Card must be on file at MTS for this warranty to be in effect. In all other respects, the MTS software is provided AS IS. Likewise, any other software provided with MTS software is provided AS IS.

THE FOREGOING WARRANTY IS IN LIEU ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MTS BE LIABLE FOR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE LICENSED PROGRAM, WHETHER AS A RESULT OF MTS NEGLIGENCE OR NOT, EVEN IF MTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. MTS ALSO DISCLAIMS ANY LIABILITY IN CONTRACT OR OTHERWISE FOR THE DEFECT OR NON-PERFORMANCE OF ANY SEPARATE END-USER LICENSED SOFTWARE PRODUCT INCLUDED WITH MTS' SOFTWARE.

INDEMNIFICATION. MTS will indemnify and defend Customer from any claim that the software infringes on any copyright, trademark, or patent. Customer will indemnify and defend MTS against all other proceedings arising out of Customers use of the software.

GENERAL. If any of the provisions, or portions thereof, of this Agreement are invalid under any applicable statute or rule of law, they are to that extent deemed to be omitted.

This is the complete and exclusive statement of the Agreement between the parties, which supersedes all proposals, oral, written and all other communications between the parties relating to the subject matter of this Agreement. This Agreement may only be amended or modified in writing, signed by authorized representatives of both parties.

This Agreement shall be governed by the laws of the State of Minnesota. The waiver of one breach or default hereunder shall not constitute the waiver of any subsequent breach or default.

Licensee also agrees to the following:
I am not a citizen, national, or resident of, and am not under the control of the government of: Afghanistan, Cuba, Iran, Iraq, Libya, Montenegro, North Korea, Pakistan, Serbia, Sudan, Syria, nor any other country to which the United States has prohibited export. I will not download or by any other means export or re-export the Programs, either directly or indirectly, to the above countries, nor to citizens, nationals or residents of the above countries. I am not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and/or Specially Designated Narcotics Traffickers, nor am I listed on the United States Department of Commerce Table of Denial Orders. I will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists. I will not use the Programs for, and will not allow the Programs to be used for, any purposes

46

prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical, or biological weapons of mass destruction.

Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement.

Multi-User Limited Warranty and License Agreement
The software contained in this package is licensed by Multi-Tech Systems, Inc., to the original end-user purchaser, hereafter referred to as Licensee, of this product for site use. A site is defined as a single business, government, or academic location, such as a building, a floor of a building, a campus, etc., and covers no more than 250 users at that location. A licensee may be a Local Area Network administrator, MIS director, purchasing agent, or other representative who acts on behalf of the users at that single site. This license provides for use of the distribution diskette, other accompanying programs, where applicable, and one copy of the documentation.

The software programs and installation utilities, hereafter referred to as Software, consist of the computer program files included on the original distribution diskette(s) or CD-ROM(s).

Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement.

In consideration of mutual covenants contained herein, and other good and valuable considerations, the receipt and sufficiency of which is acknowledged, Multi-Tech Systems, Inc., does hereby grant to the Licensee a non-transferable and non-exclusive license to use the Software and accompanying documentation under the following terms and conditions:
The software is furnished to the Licensee as the single site representative for execution and use on as many workstations as that single site contains, for up to 250 users inclusively. Software and manuals may be copied, with the inclusion of the Multi-Tech Systems, Inc., copyright notice, for use within that single site. Additional manuals may be ordered from Multi-Tech Systems, Inc., for a nominal charge.

This license covers only the stipulated single site.   The Licensee hereby agrees not to provide, or otherwise make available, any portion of this software in any form to any third party without the prior express written approval of Multi-Tech Systems, Inc. Licensee is hereby informed that this Software contains confidential, proprietary, and valuable trade secrets developed by or licensed to Multi-Tech Systems, Inc., and agrees that sole ownership shall remain with Multi-Tech Systems, Inc.

The Software and documentation are copyrighted. Except as provided herein, the Software and documentation supplied under this agreement may not be copied, reproduced, published, licensed, sub-licensed, distributed, transferred, or made available in any form, in whole or in part, to others without expressed written permission of Multi-Tech Systems, Inc. Copies of the Software may be made to replace worn or deteriorated copies, for archival, or back-up purposes.

Licensee agrees to implement sufficient security measures to protect Multi-Tech Systems, Inc.'s proprietary interests, and not to allow the use, copying, or transfer by any means, other than in accordance with this agreement.

Licensee agrees that any breach of this agreement will be damaging to Multi-Tech Systems, Inc.
LICENSEE AGREES THAT ALL WARRANTIES, IMPLIED OR OTHERWISE, WITH REGARD TO THIS SOFTWARE, INCLUDING ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR ANY PARTICULAR PURPOSE ARE EXPRESSLY WAIVED, AND NO LIABILITY SHALL EXTEND TO ANY

47

DAMAGES, INCLUDING CONSEQUENTIAL DAMAGES, WHETHER OR NOT KNOWN TO MULTI-TECH SYSTEMS, INC. IT IS HEREBY EXPRESSLY AGREED THAT LICENSEE'S REMEDY IS LIMITED TO REPLACEMENT OR REFUND OF THE LICENSE FEE, AT THE OPTION OF MULTI-TECH SYSTEMS, INC., FOR DEFECTIVE DISTRIBUTION MEDIA. There is no warranty for misused materials.

If this package contains multiple media formats (e.g., both 3.5" disk(s) and CD-ROM), they are provided only to facilitate use at a single site. Neither this Software, nor its accompanying documentation may be modified or translated without the written permission of Multi-Tech Systems, Inc.

This agreement shall be governed by the laws of the State of Minnesota. The terms and conditions of this agreement shall prevail regardless of the terms of any other submitted by the Licensee. This agreement supersedes any proposal or prior agreement. Licensee further agrees that this License Agreement is the complete and exclusive Statement of Agreement, and supersedes oral, written, or any other communications between Multi-Tech Systems, Inc., and Licensee relating to the subject matter of this agreement. This agreement is not assignable without written permission of an authorized agent of Multi-Tech Systems, Inc.

Register Your Software
(U.S. Residents)

Thank you for purchasing software from Multi-Tech Systems. Choose one of the
following options to register your software:
By Mail: Complete the registration form and mail.
By Fax: Fax this completed registration card to: (763) 785-9874
Via the Web: www.multitech.com/register

Date Purchased: ___/___/___   Product _____

Software Serial Number _____ Version # _____

First Name _____ Last Name _____

Company _____

Address _____

City _____ State _____ Zip _____

Daytime Phone with area code _____

Fax _____

Email address _____
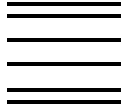
Purchased from:
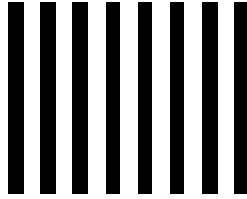? Distributor   ? Reseller   ? Other _____

The best way to contact me is by:
? Mail   ? Phone   ? Email
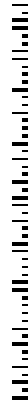? Fax   ? I do not wish to be on a mailing list

PN 82013151

BUSINESS REPLY MAIL
FIRST-CLASS MAIL   PERMIT NO. 5828   ST PAUL, MN

POSTAGE WILL BE PAID BY ADDRESSEE

Product Registration
MULTI-TECH SYSTEMS, INC.
2205 Woodale Drive
Mounds View, MN 55112-9941

50

Register Your Software
(outside the United States)

Thank you for purchasing software from Multi-Tech Systems. Choose one of the following options to register your software:
By Mail: Complete the registration card, affix postage and mail.
By Fax: Fax this completed registration card to: + (763) 785-9874
Via the Web: www.multitech.com/register

Date Purchased: ___/___/___   Product _____

Software Serial Number _____   Version _____

First Name _____ Last Name _____

Company _____

Address _____

City _____State/Providence _____ Zip/Postal Code _____

Country _____ Daytime Phone with area code _____

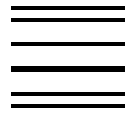Fax _____

Email address _____

Purchased from:
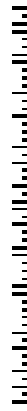? Distributor   ? Reseller   ? Other _____

The best way to contact me is by:
? Mail   ? Phone   ? Email
? Fax   ? I do not wish to be on a mailing list

PN 82013151

Product Registration
MULTI-TECH SYSTEMS, INC.
2205 Woodale Drive
Mounds View, MN 55112-9941

52

82013151 (B)

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com