

# WatchGuard® VPN Manager Guide

---

VPN Manager 2.1

---

## Disclaimer

---

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

## Copyright and Patent Information

---

Copyright© 1998 - 2001 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, LiveSecurity, and SpamScreen are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

Red Hat® is a registered trademark of Red Hat, Inc. This product is not a product of Red Hat, Inc. and is not endorsed by Red Hat, Inc. This is a product of WatchGuard and we have no relationship with Red Hat, Inc.

Adobe, Acrobat, the Acrobat logo, and PostScript are trademarks of Adobe Systems Incorporated.

© 1999 BackWeb Technologies, Inc. All rights reserved. BackWeb is a registered trademark of BackWeb Technologies, Inc.

CyberNOT, CyberNOT List, CyberYES, and CyberYES List are trademarks of Learning Company Properties Inc.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-1999 The OpenSSL Project. All rights reserved.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TIEPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

VPCOM™ Copyright © 1997-1999 Ashley Laurent, Inc. All rights reserved.

All other trademarks and tradenames are the property of their respective owners.

Printed in the United States of America.

DocVer: WatchGuard Firebox Security System 4.6 VPN Manager Guide - 2.1.1

---

# Table of Contents

---

CHAPTER 1 Introduction to VPN Manager .....	1
What is VPN Manager? .....	1
Physical description .....	2
VPN Manager features .....	2
How does DVCP work? .....	3
CHAPTER 1 Installing VPN Manager .....	5
Purchasing VPN Manager .....	5
Activating VPN Manager .....	5
Installing VPN Manager .....	6
Planning your Internet Distributed Enterprise (IDE) .....	6
CHAPTER 1 Setting Up a Firebox as a DVCP Server .....	7
CHAPTER 1 Setting Up Certificates in Web Browsers .....	9
Enabling Web-based management .....	9
Importing a certificate for Microsoft Internet Explorer 5 (IE5.0) .....	9
Certificate import process for Netscape 4.75 .....	10
Resetting certificates .....	11
Removing Certificates .....	11
CHAPTER 1 Adding Devices to VPN Manager .....	13
Enabling Fireboxes as DVCP clients .....	13
Adding devices to VPN Manager .....	15
Removing a device from VPN Manager .....	15

---

CHAPTER 1 Creating Tunnels Between Devices .....	17
Adding policy templates .....	17
Adding security templates .....	18
Connecting devices .....	18
Enabling a SOHO single-host tunnel .....	20
Removing or changing a tunnel .....	21
CHAPTER 1 Managing the Internet Distributed Environment .....	23
Opening the VPN Manager display .....	23
Viewing device status .....	23
Viewing Tunnels .....	25
Viewing log servers .....	26
Creating a custom view .....	26
Launching applications from VPN Manager .....	27
CHAPTER 1 Using Remote Administration .....	29
Starting the Remote Management feature .....	29
Index .....	33

---

WatchGuard VPN Manager offers an unprecedented level of convenience and control for creating IPsec tunnels and virtual private networks (VPN) simply and quickly. VPN Manager provides an intuitive graphical user interface (GUI) for rapidly creating IPsec tunnels of varying types of authentication and levels of encryption. Rather than configuring multiple dialog boxes and multi-tab tools, VPN Manager offers speed and reliability through drag-and-drop tunnel creation, automatic wizard launching, and the application of templates. This eliminates the time-consuming, error-prone processes typically associated with the creation of IPsec VPNs. With VPN Manager, you can actually create fully authenticated and encrypted tunnels in minutes, and be assured that they do not clash with other tunnels or security policies.

From the same graphical user interface, you can then administer and monitor the network of created tunnels and know the status of the various components and tunnels at a glance. VPN Manager configures and manages any combination of the WatchGuard Firebox family of appliances.

## What is VPN Manager?

---

VPN Manager is a centralized point for creating and managing the network security of an Internet Distributed Enterprise (IDE). An IDE is an organization that uses the Internet extension to conduct business. It usually consists of multiple locations behind security devices, connected by virtual private networks (VPN). VPN Manager administers and monitors an enterprise's sum total of Fireboxes, Event Processors, networks, and VPN tunnels. VPN Manager also has the controls to launch the applications of the WatchGuard Firebox System.

### Centrally managing devices

VPN Manager is a powerful tool for: viewing all VPN connections; determining their status; configuring or reconfiguring either or both ends of the tunnels that it monitors and controls; and configuring Fireboxes from a single control center. One of the most

---

## Physical description

innovative features in VPN Manager is its drag-and-drop graphical user interface for creating IPSec tunnels. The key to this drag-and-drop convenience is the underlying technology, the WatchGuard proprietary DVCP (Dynamic VPN Configuration Protocol).

### Virtual private networking and IPSec

DVCP eliminates much of the confusion of creating IPSec tunnels, and keeps the operator from creating unworkable configurations.

VPN Manager consists of several parts: a client (referred to as VPN Manager), a server (a Firebox that you designate and activate as the DVCP server), and WatchGuard security appliances.

---

## Physical description

VPN Manager is a Microsoft Windows NT 4.0, Windows 98, and Windows 2000 application with a toolbar at the top and a main window that consists of four tabbed tree-view windows.

The four tabs are:

- Device View
- VPN View
- Logging View
- Custom View

All devices and VPNs are managed through VPN Manager. It can also launch all other programs associated with the WatchGuard Firebox System.

A DVCP Server must run on a WatchGuard Firebox (not a SOHO). The server provides centralized storage of all configured devices under management and builds VPNs quickly and interactively for those devices.

The log server consists of the Event Processor, the reporting processes, and their associated supporting files. The VPN Manager's Log Server View provides centralized management of log servers currently in use.

---

## VPN Manager features

VPN Manager allows you to:

- Configure and monitor multiple Firebox devices
- Configure and monitor multiple SOHO devices
- Create and view contact and location information for each device
- Customize the view of devices and device properties to suit an environment and implementation

- Associate devices in a GUI to create drag-and-drop VPNs without error or confusion
- Centralize management of distributed log servers

---

## How does DVCP work?

---

WatchGuard's DVCP automates the creation of IPsec VPNs. The user interfaces for configuring DVCP tunnels are templates, automated wizards, and point-and-click GUIs. Configurations of various types and levels of authentication and strengths of encryption reside in templates that are selected and applied to the IPsec tunnels you create.

After you have configured VPN Manager by supplying the name or IP address of each Firebox you want to monitor, you can then drag and drop one device upon another in the GUI, which then launches a tunnel creation wizard that already knows the IP addresses and read-write passwords of the two devices, based on their registration information. The wizard creates the tunnel based on this information along with the security template that you designate for that purpose. The security templates contain specific authentication and encryption combinations that you select and apply according to the security you want for the tunnel you are creating.

### Configuring VPN Manager

Configuring VPN Manager involves:

- Designating a Firebox as a DVCP server
- Adding Fireboxes as devices to the VPN Manager device list
- Creating tunnels — virtual private network connections between devices

When the VPN Manager starts (after configuration), it downloads the lists of configured devices and configured security templates, policy templates, and tunnels. It distributes this information among the appropriate tabs of its display. VPN Manager then gets the current status of the devices in each VPN.

### DVCP device and tunnel management

VPN Manager maintains an open connection to the DVCP server. VPN Manager downloads the DVCP configuration at startup and sends a modified configuration when a user makes changes. VPN Manager also accounts for lost connections with an easy reconnect method, remembering its state if it was in the middle of a transaction.

When you make configuration changes via VPN Manager, VPN Manager stores the updated configuration. When the new configuration is saved to the DVCP server, VPN Manager notifies the devices involved that a new configuration exists and forces it to expire its lease/lookup and use the new configuration.

---

**How does DVCP work?**

# Installing VPN Manager

---

Installing VPN Manager on a computer involves four major activities:

- Purchasing
- Activating
- Installing
- Planning your Internet Distributed Enterprise

This chapter describes how to perform each of these tasks.

## Purchasing VPN Manager

---

To purchase VPN Manager, contact a WatchGuard reseller and purchase a license key for this product. The license key is printed on a certificate and is not replaceable. Keep it safe but accessible for installing VPN Manager onto your computer.

## Activating VPN Manager

---

- 1 Open your Web browser to the LiveSecurity Service Web site at <http://www.watchguard.com/support/>
- 2 Log in.
- 3 Click **Register VPN Manager**.
- 4 Enter your VPN Manager license key, including the hyphens.  
The most common reason for registration to fail is incorrectly typing the license key numbers and hyphens.
- 5 Click **Register**.  
The VPN Manager license key is associated with your LiveSecurity license to ensure that you receive regular updates to the VPN Manager utility. The download page appears.

- 6 Click **Download Now**.  
A prompt appears to either open or save the VPN Manager installation file. The file name is `WGInstallVPNM.wls`.
- 7 Save the file to your Windows Desktop.

---

## Installing VPN Manager

- 1 On your Windows desktop, double-click `WGInstallVPNM.wls`.  
The WatchGuard Player appears.
- 2 Click **Install**.  
The WinZip Self-Extractor appears.
- 3 Click **Setup**.  
The installation wizard starts and displays a status screen that informs you that it is installing WatchGuard VPN Manager.
- 4 Click **Next**.  
The wizard displays the End User License Agreement (EULA).
- 5 Click **Yes**.  
The wizard displays the directory selection screen.
- 6 Select a directory in which to install VPN Manager. Click **Next**.  
The installation wizard enables VPN Manager in the QuickSetup wizard.
- 7 Click **Finish**.  
The installation program installs VPN Manager software in the proper directories. VPN Manager automatically appears as an application under Start ⇒ Programs ⇒ WatchGuard.

---

## Planning your Internet Distributed Enterprise (IDE)

The remainder of this user guide discusses how to use VPN Manager to create, configure, and administer virtual private networks and tunnel combinations. However, before you configure your IDE, plan your configuration and gather the information you will need to do the following:

- Organize your IDE by domains, each of which should contain a Firebox.
- Make sure you know which devices need to have tunnels between them and what level of encryption and method of authentication to use for each tunnel.
- Organize the tunnels into virtual private networks according to the clusters of tunnels they form among Fireboxes.
- Assign names to each tunnel and to each VPN.
- Make sure that you have the IP addresses or DNS names, and monitoring (read-only) and configuration (read-write) passphrases for all the Fireboxes to be managed by VPN Manager. After you have this information for each security device, you can add devices and create tunnels between them at will.

# Setting Up a Firebox as a DVCP Server

---

After you have installed VPN Manager, you must choose a Firebox within your IDE to be the DVCP server. DVCP is a specialized tool developed by WatchGuard to make VPN configuration simple and straightforward. The Firebox that is physically closest to the VPN Manager workstation is probably the best candidate for the DVCP server.

From VPN Manager:

- 1 Select **Tools** ⇒ **Policy Manager**.  
The WatchGuard Policy Manager appears.
- 2 Select **Network** ⇒ **Enhanced DVCP Server**.  
The DVCP Server Setup window appears.
- 3 Click the checkbox labeled **Enable this Firebox as a DVCP Server**.
- 4 Enter a name in the **Domain Name** field and click **OK**.  
You can name the domain anything you want. After you click OK, the display returns to the Policy Manager.
- 5 At the Policy Manager, select **File** ⇒ **Save** ⇒ **To Firebox**, create or verify the name for the configuration file, and enter the designated Firebox's read-write passphrase.  
This saves the new configuration to the Firebox. The Firebox can now function as a DVCP server, but it has not been activated yet.
- 6 Select the VPN Manager window.
- 7 Select **File** ⇒ **New**.  
The New Server dialog box appears.
- 8 Enter the following:
  - Display Name**  
A friendly name of your choosing.
  - Firebox Type**  
Select the device type that describes the DVCP server device from the drop-down list.
  - Enter the Host Name or IP Address**  
This is either the device's DNS name or its IP address.

---

***Status Pass Phrase***

This is the monitoring (read-only) passphrase.

***Configuration Pass Phrase***

This is the configuration (read-write) passphrase.

***License Key***

Enter the Key listed on your VPN Manager License Key Certificate.

- 9 Click **OK**.  
A message appears confirming the DVCP server setup.
- 10 Click **OK**.  
The Firebox reboots.

# Setting Up Certificates in Web Browsers

---

The WatchGuard SOHO is designed for remote management through the use of a Web browser. There are also other transactions performed in VPN Manager that may require your Web browser to have certificates enabled. To maintain security in such an open environment, the browser uses SSL (Secure Sockets Layer). The authentication medium is the X.509v3 certificates, which provide client/server authentication. You cannot securely administer Firebox SOHO devices without proper authentication, which in this case is X.509.v3 certificates.

## Enabling Web-based management

---

When you configure a DVCP server, a certificate file is created and sorted in the directory where you installed WatchGuard. For example:

```
c:\Program Files\WatchGuard\Certificates\[DVCP Server's IP  
Address]\SOHOAdmin
```

This file must be imported by the browsers that will be used to contact and configure the SOHOs in your IDE.

## Importing a certificate for Microsoft Internet Explorer 5 (IE5.0)

---

To configure a Microsoft IE 5.0 Web browser as an administration tool:

- 1 Open an IE 5.0 browser.
- 2 Select **Tools** ⇒ **Internet Options**.  
The Internet Options tool appears.
- 3 Click the **Content** tab.
- 4 Click **Certificates**.  
The Certificate Manager screen appears.

- 5 Select the **Personal** tab and click **Import**.  
This activates the import wizard.
- 6 Click **Next**.  
You are prompted for the file name.
- 7 Type the full path to the file, or browse to it. Click **Next**.
- 8 Type the password that encrypts the certificate file.  
This is the same as the DVCP server's read-write key.
- 9 Click **Next**.  
You are prompted to select a certificate store.
- 10 Let the default selection stand. Click **Next**.
- 11 Click **Finish**.  
This screen completes the import process. If you are prompted to accept a certificate as trusted, click Yes.  
You should get a message indicating that import is successful.  
The imported certificate should show in the Certificate Manager.  
The browser is now ready to be enabled for SSL client authentication.
- 12 Select the certificate and click **Advanced**.  
You are presented with a list of certificate purposes.
- 13 Check **Client authentication**.
- 14 Click **OK**, click **Close**, and click **OK** again.

### **Troubleshooting IE 5.0 certificate setup**

If any of the preceding steps fail, check the following:

- Make sure you have the strong encryption (128-bit) version of IE.
- Make sure you have the right password for the .p12 (or .pfx) file. This must be the read-write password of the Firebox that is your DVCP server.
- Make sure the certificate file is not 0 length. If it is, delete it and run VPN Manager again.
- Sometimes, at installation, IE5 does not enable strong encryption. You can check this by looking in the registry. Look at

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Defaults\Provides\001
```

It should be set to Microsoft Enhanced Cryptographic Provider v1.0. If not, edit the line to fix it manually, and restart the browser.

---

### **Certificate import process for Netscape 4.75**

- 1 Open the Netscape 4.75 browser and click **Security**.
- 2 On the left-side menu, find the **Certificates** heading and click **Yours**.
- 3 Click **Import a Certificate**.
- 4 Browse to the file location and click **Open**.  
The Password Entry dialog box appears.

- 5 Enter the read-write password of the DVCP server and click **OK**.  
A screen appears that says your certificate has been successfully imported.

### Troubleshooting Netscape 4.75 certificate setup

- Make sure you have the strong encryption (128-bit) version of Netscape.
- Make sure you have the right password for the .p12 (or .pfx) file. This must be the read-write password of the Firebox that is your DVCP server.
- Make sure the certificate file is not 0 length. If it is, delete it and run VPN Manager again.

## Resetting certificates

---

Certain situations might require you to update the certificates that VPN Manager uses. For example, if the Firebox's configuration passphrase is changed, you will need to update the certificate that VPN Manager uses for management sessions. The certificates need to be removed, then new certificates will be generated and used instead. To remove the old certificates, first, in your browser:

- 1 Select **Tools ⇒ Internet Options**.  
The Internet Options dialog box appears.
- 2 Select the **Control** tab.
- 3 Click **Certificates**.  
The Certificates dialog box appears.
- 4 Highlight the certificate or certificates to remove.
- 5 Click **Remove**.  
The selected certificates will be deleted from your browser.

After you have removed the old certificates from your browser, in the VPN Manager:

- 1 Select **File ⇒ Certificates ⇒ Clean up on PC**.  
This will delete the VPN Manager's certificates on the computer on which VPN Manager is installed.

## Removing Certificates

---

When you are reinstalling the DVCP server, the certificates associated with the deleted DVCP server must be removed. From the browser in which the certificates were installed:

- 1 Select **Tools ⇒ Internet Options**.  
The Internet Options dialog box appears.
- 2 Select the **Control** tab.
- 3 Click **Certificates**.  
The Certificates dialog box appears.
- 4 Highlight the certificate or certificates to remove.

5 Click **Remove**.

The selected certificates will be deleted from your browser.

After you have removed the old certificates from your browser, in the VPN Manager:

1 Select **File ⇒ Certificates ⇒ Clean up on PC**.

This will delete the VPN Manager's certificates on the computer on which VPN Manager is installed.

2 Select **File ⇒ Certificates ⇒ Clean up on DVCP Server**.

This will delete the VPN Manager's certificates on the Firebox designated as the DVCP server. The Firebox reboots and then reconnects to the VPN Manager, entering its certificates in the VPN Manager's Certificates folder.

# Adding Devices to VPN Manager

---

Before you create tunnels between devices, you first add devices to VPN Manager. VPN Manager makes adding devices straightforward and error-free by launching a wizard to configure each device. For each device, you must know its name or IP address and its configuration (read-write) passphrase, and be able to configure it as a DVCP client.

Before a tunnel can be created, devices must be enabled as a DVCP client. Then those devices (DVCP clients) can be added to the VPN Manager device list.

## Enabling Fireboxes as DVCP clients

---

The VPN Manager will configure the Firebox as a DVCP client. The only prerequisite is that the WatchGuard service be configured to allow incoming connections from the DVCP server to the Firebox (DVCP client).

From Policy Manager:

- 1 Select the WatchGuard icon in the Services Arena.
- 2 Click **Edit** ⇒ **Modify Service**.
- 3 Under **From**, click **Add**.  
The Add Address dialog box appears.
- 4 Click **Add Other**.  
The Add Member dialog box appears.
- 5 From the **Choose Type** drop list, click **Host IP Address**.
- 6 Enter the IP address of the DVCP server in the **Value** box. Click **OK**.
- 7 Under **To**, click **Add**.  
The Add Address dialog box appears.
- 8 Click **Firebox**.  
The Add Member dialog box appears.
- 9 Click **Add**.

10 Click OK.

## Enabling SOHOs as DVCP clients



For a SOHO to be configured as a DVCP client, for VPN tunnels, it must have the VPN feature enabled.

To enable a SOHO with a static IP address as a DVCP client, on the SOHO:

- 1 Browse to the WatchGuard **SOHO Configuration** menu.  
The default configuration IP address is 192.168.111.1.
- 2 Click **System Administration**.  
The System Administration page appears.
- 3 Click **Remote Configuration**.  
The Remote Configuration page appears.
- 4 Enter a read-write and read-only passphrase.  
The read-write and read-only passphrases will be used by the DVCP server to communicate with the SOHO.

To enable a SOHO with a dynamically assigned IP address as a DVCP client, on the SOHO:

- 1 Browse to the WatchGuard **SOHO Configuration** menu.  
The default configuration IP address is 192.168.111.1.
- 2 Click **Virtual Private Networking**.  
The Virtual Private Networking page appears.
- 3 Select **VPN Manager SOHO** from the drop list.
- 4 Click **Configure**.  
The VPN Manager SOHO page appears.
- 5 Check **Enable IPsec Network**.
- 6 Enter the following
  - DVCP Server Address**  
Enter the IP address of the DVCP server (defined in VPN Manager) to which this device will be a client.
  - User ID**  
Use the IP address or any identifying name or number. The same ID must be entered in the VPN Manager when adding the device.
  - Shared Secret**  
Enter a passphrase for use between the client and server. The same secret must be entered in the VPN Manager when adding the device.

---

## Adding devices to VPN Manager

---

From VPN Manager:

- 1 Select either the **Device** or the **VPNs** tab. Select **Edit ⇒ Insert Device**.  
The WatchGuard Device wizard appears.
- 2 Click **Next**.
- 3 Enter a display name for the device.  
This is a name of your own choosing. It is not tied to the device's DNS name.
- 4 From the **Device Type** drop list, select the device type.
- 5 Enter the host name or IP address.  
This is the DNS name, not the name you entered in Step 3.
- 6 Enter the monitoring (read-only) and configuration (read-write) passphrases.  
These must be at least seven characters long.
- 7 Set the **Initial Lease Time-out**, if necessary.  
This is the amount of time that the configuration is run before the device contacts the DVCP server to see if its configuration has changed.
- 8 Click **Next**.  
The wizard displays the DNS and WINS settings for the DHCP window.
- 9 Enter any WINS or DNS server IP addresses you want in your configuration.  
Click **Next**.  
If you are not using DNS or WINS servers, ignore this page, and click Next.  
The wizard displays the Contact Information page.
- 10 Enter any contact information you want for contacting administrators of this Firebox. Click **Next**.  
The information on this panel is optional. The wizard displays the Gather Information and Configure Device information panel.
- 11 Click **Next**.  
When finished, the wizard displays the message "New Device Successfully Changed."
- 12 Click **Close**.  
The wizard uploads the new configuration to the DVCP server and exits.

---

## Removing a device from VPN Manager

---

Removing a device from VPN Manager does not remove it from its associated tunnels. To remove it completely from VPN Manager, you will also have to delete any tunnels for which that device is an endpoint.

### Removing Fireboxes

From Policy Manager:

- 1 Select **Network ⇒ Enhanced DVCP Client**.  
The Enhanced DVCP Client Setup dialog box appears.
- 2 Disable the **Enable This Firebox as a DVCP Client** checkbox.
- 3 Click **OK**.

## Removing SOHOs

In VPN Manager, in the **VPNs** tab:

- 1 Expand the **Devices** folder to reveal the SOHO device to be deleted.
- 2 Right-click the device.
- 3 Select **Remove**.



Tunnels associated with a deleted device are not deleted from the **VPNs** tab view. Before deleting the device, manually delete any tunnels associated with a deleted device.

# Creating Tunnels Between Devices

---

After devices are added to VPN Manager, they can be connected to each other by tunnels. VPN Manager uses a graphical interface that launches the VPN Manager Configuration wizard, which knows the endpoint device IP addresses and their read-write passwords. The wizard uses templates to simplify tunnel creation. The policy template defines what resources will be accessible through the tunnel, to the other endpoint. The security template defines the encryption level and authentication method to be used. When you finish the wizard, it creates the new tunnel.



A SOHO device, with VPN enabled, can be configured for a maximum of five tunnels.

## Adding policy templates

---

One of the benefits of a VPN is that you can define (and limit) the resources that are accessible through the tunnel: A VPN can be created between only two hosts or between multiple networks — or any combination in between. To define the resources accessible through a given VPN device, create a policy template. By default, the VPN Manager provides a Trusted network policy template, which allows access to the Trusted network behind the VPN device to which the policy is applied. To create a policy template, on the **VPNs** tab:

- 1 Highlight the device for which you want to define a policy template.
- 2 Right-click and select **Insert Policy** or click the Insert Policy Template icon. The Device Policy dialog box for that device appears.
- 3 Enter a policy name of your choosing.
- 4 Enter the bypass rule (the type of IPSec policy applied to the VPN tunnel):
  - **Block** — IPSec will not allow traffic that matches the rule in associated tunnel policies.

---

## Adding security templates

- **Bypass** — IPsec will not encrypt any traffic between the two hosts. (this cannot be used if the hosts are networks).
  - **Secure** — IPsec will encrypt all traffic that matches the rule in associated tunnel policies.
- 5 Click **Add** to define the accessible resources for the device.  
The Resource dialog box appears.
  - 6 Select the type of resource (host or network) from the **Allow To/From** menu.
  - 7 Enter the resource's IP address (for host) or network address (for network). Click **OK**.
  - 8 Click **OK**.  
The policy template has been defined. It can now be selected in the VPN wizard when creating a VPN tunnel involving that device.

---

## Adding security templates

Default security templates are provided for available encryption levels. New templates can also be created. A variety of security templates makes it easy to match the appropriate level of encryption and type of authentication to the tunnel created with the Configuration wizard.

From the VPN Manager display:

- 1 Click the **VPN** tab.
- 2 Right-click anywhere in the window, and select **Insert Security Template**.  
The Security Template dialog box appears.
- 3 Enter the template name, SAP (security authorization packet) type (either ESP or AH), authentication, and encryption.
- 4 If you want to force key encryption, enable the corresponding checkbox, and then specify either kilobytes or hours.  
The security template has been defined. It can now be selected in the VPN wizard when creating a VPN tunnel involving that device.
- 5 Click **OK**.

---

## Connecting devices

There is more than one way to designate endpoints in a tunnel and work through the VPN Manager Configuration wizard. Here are two ways to create a tunnel.

## Drag-and-drop tunnel creation



This method cannot be used to create tunnels for dynamically addressed SOHO devices.

From VPN Manager:

- 1 Click the **Device** tab.
- 2 Click the device name of one of the tunnel endpoints to highlight it and drag it to the device name of the other tunnel endpoint.  
This launches the VPN Manager Configuration wizard, starting with the dialog box that shows (in two list boxes) the two endpoint devices you selected using drag-and-drop.
- 3 For each device (endpoint), select a policy template from the drop list.  
The policy template determines the resources available through the tunnel. Resources can be a network or a host.  
The listbox displays any policy templates you have added to VPN Manager.
- 4 Click **Next**.  
The wizard displays the Security Policy dialog box.
- 5 Select the security template appropriate for the level of security and type of authentication to be applied to this tunnel.  
The listbox displays any templates you have added to VPN Manager.
- 6 Click **Next**.  
The wizard displays the DVCP configuration.
- 7 Enable the checkbox labeled **Restart devices now to download VPN configuration**. Click **Finish** to restart the devices and deploy the VPN tunnel.



If you are configuring a large number of devices, you can delay restarting the devices until you have created all the tunnels. To restart any device, right-click it and select Restart. Or you can wait until a given device's lease expires, at which time VPN Manager uploads the new configuration automatically.

## Menu-driven tunnel creation



This method must be used to create tunnels for dynamically addressed SOHO devices.

Follow these steps from VPN Manager:

- 1 Click the **VPNs** tab.
- 2 Select **Edit ⇒ Create a New VPN**.  
This launches the VPN Manager Configuration wizard.
- 3 Click **Next**.  
The wizard displays two listboxes that each list all the devices registered in VPN Manager. You will be selecting one device from each listbox as endpoints of a tunnel.
- 4 Select a device from each listbox as endpoints of the tunnel you are setting up.
- 5 Select the policy templates for each device's end of the tunnel.  
The listbox displays any templates that you have added to VPN Manager.

- 6 **Click Next.**  
The wizard displays the Security Template dialog box.
- 7 **Choose the security template you want for this VPN. Click Next.**  
The wizard displays the DVCP configuration.
- 8 **Enable the checkbox labeled **Restart devices now to download VPN configuration**. Click **Finish** to restart the devices and deploy the VPN tunnel.**



If you are configuring a large number of devices, you can delay restarting the devices until you have created all the tunnels. To restart any device, right-click it and select Restart. Or you can wait until a given device's lease expires, at which time VPN Manager uploads the new configuration automatically.

---

## Enabling a SOHO single-host tunnel

---

Any SOHO (static or dynamic) can be configured for a tunnel that allows only one host behind the SOHO to connect to another endpoint (host or networks). This tunnel is called a SOHO Telecommuter tunnel and is useful for situations where an entire family's network is behind a SOHO, but only one computer — the telecommuter — should be allowed access to corporate resources available via the tunnel. On the SOHO:

- 1 **Browse to the WatchGuard **SOHO Configuration** menu.**  
The default configuration IP address is 192.168.111.1.
- 2 **Click **Virtual Private Networking**.**  
The Virtual Private Networking page appears.
- 3 **Select **VPN Manager Telecommuter** from the drop list.**
- 4 **Click **Configure**.**  
The VPN Manager Telecommuter page appears.
- 5 **Check **Enable IPSec Network**.**
- 6 **Enter the following:**

***DVCP Server Address***

Enter the IP address of the DVCP server (defined in VPN Manager) to which this device will be a client.

***User ID***

Use the IP address or any identifying name or number. The same ID must be entered in the VPN Manager when adding the device.

***Shared Secret***

Enter a passphrase for use between the client and server. The same secret must be entered in the VPN Manager when adding the device.

***Private IP Allowed to Use VPN***

Enter the IP address of the trusted host behind the SOHO (the telecommuter's computer).

### Creating a Policy for a Telecommuter

A SOHO that has been enabled for a VPN Manager Telecommuter tunnel does not have an associated policy. A policy must be created for this device in the VPN Manager. On the **VPNs** tab:

- 1 Under the **Devices** folder, select the device.
- 2 Right-click the device and select **Insert Policy**.  
The Device Policy dialog box appears.
- 3 Enter the following:

*Policy Name*

Enter a friendly name of your choosing.

*Type*

Select **Telecommuter Tunnel** from the drop list.

*Virtual IP Address Behind the Firewall*

Enter a free IP address on the Trusted network of the remote Firewall to which the SOHO is connecting.

*Private IP Allowed to Use Tunnel*

Enter the IP address of the trusted host behind the SOHO (the telecommuter's computer). Use the same address entered on the SOHO VPN configuration.

---

## Removing or changing a tunnel

After a tunnel has been created, it will be visible on the **VPNs** tab of the VPN Manager. The VPN Manager allows tunnel resources on an existing VPN to be edited. You may also want to remove a tunnel that is no longer used.

### Editing a tunnel

The VPN Manager allows the tunnel name, security template, endpoints, and the policy used to be edited on an existing tunnel. On the **VPNs** tab:

- 1 Expand the tree to show the device and its policy that you want to edit.
- 2 Highlight the tunnel that you want to edit.
- 3 Right-click and select **Properties**.
- 4 You can modify:

*VPN Tunnel*

The name used to identify this tunnel

*Security Template*

Used to define the security for this tunnel

*Devices*

Defined as endpoints for this tunnel

***Policy Template***

Used to define the resources available (for a given endpoint of this tunnel)

- 5 Click **OK** to save the change.  
When the tunnel is renegotiated, the changes will be applied.

**Removing a tunnel**

To remove a tunnel, on the **VPNs** tab:

- 1 Highlight the tunnel on the **VPNs** tab.
- 2 Select **Edit ⇒ Remove**.

**Editing a policy template**

If resources defined for a given endpoint and/or tunnel need to be altered, you can do so without having to delete the tunnel. To edit the policy, on the **VPNs** tab:

- 1 Under the **Devices** folder, select a policy.
- 2 Right-click and select **Properties**.  
The Policy dialog box appears.
- 3 You can modify the resources in the following ways:

***Edit***

To alter an already-defined resource

***Add***

To add a new resource

***Remove***

To delete an already-defined resource

# Managing the Internet Distributed Environment

---

The Internet Distributed Enterprise (IDE) is managed through the use of the VPN Manager display. This display provides real-time information on all managed devices simultaneously. This information is used to determine current device status, to diagnose problems, and to plan how various devices need to be configured or reconfigured.

## Opening the VPN Manager display

---

To open VPN Manager, from the Windows interface:

- 1 Select **Start** ⇒ **Programs** ⇒ **WatchGuard** ⇒ **VPN Manager**.  
This displays a blank VPN Manager user interface:
- 2 Select **File** ⇒ **Connect** or select the Connect icon from the toolbar.
- 3 Enter the name or IP address of the DVCP server and the Firebox read-write password. Click **OK**.  
VPN Manager connects to the DVCP server and displays what you have configured up to now, distributed appropriately among the four tabs on the display.

## Viewing device status

---

Click the **Devices** tab of the VPN Manager Display to view the real-time status of all devices being managed by DVCP.

### Tree-view structure

All devices appear in a tree-view structure. When the box next to an entry contains a plus sign (+), the tree is collapsed. To expand it, click the plus sign. The tree view expands at that entry to display the properties of that device.

To collapse the display, click the minus sign (–) next to a device. The expanded tree disappears, leaving a single-line entry for that device.

The display is structured as follows:

- Device Name
  - Statistics folder
    - Log Host
    - Up Time
    - Number of connections
    - Authenticated Users
    - External MAC
      - # of packets sent
      - # of packets received
    - Trusted MAC
      - # of packets sent
      - # of packets received
    - Optional MAC
      - # of packets sent
      - # of packets received
  - Branch Office VPN Tunnel folder
    - Tunnel Name/Encryption
    - Bytes Sent
    - Bytes Received
    - Renegotiation
    - Authentication
  - Remote User VPN Folder

## Connection status

The top level of the tree view for each device will show a red, yellow, or no exclamation point. The exclamation point (or lack of it) provides the device's status, even when the tree view is not expanded. The statuses indicated are as follows:

### *No exclamation point*

Normal operation. The device is connected to the VPN Manager.

### *Yellow exclamation point*

Questionable operation. VPN Manager is trying to contact the device. The exclamation point will either resolve or turn red.

### *Red exclamation point*

Failed operation. The device is no longer connected to the VPN Manager. Right-click the device, and select **Resume Connection**. If this fails to resolve the situation, examine the devices for other problems.

## Context menu options

Right-clicking a device in the **Device** tab presents the following functionality:

### *Create a new VPN*

Another means of starting the VPN wizard, to quickly create a VPN between identified devices.

### *Update Device*

Allows updating of network policies, resetting of the DVCP server configuration, and expiration of the lease.

***Insert Device***

Allows configuration of a new device to be added to the VPN Manager view.

***Remove***

Remove the selected device.

***Properties***

View the properties of the selected device, as configured in the VPN Manager's Device wizard.

***Pause/Resume Connection***

Pause or resume VPN Manager's connection and any tunnels to the device (available option depends on device status).

***Policy Manager***

Open Policy Manager for the device selected.

***SOHO Configuration***

Open the SOHO device's configuration (for SOHO devices only).

***Firebox Monitors***

View Firebox Monitors for the device selected.

***Log Viewer***

View LogViewer for the device selected.

***HostWatch***

View HostWatch for the device selected.

***Historical Reports***

View Historical Reports for the device selected.

***Front Panel***

View the Front Display (Firebox Triangle) for the device selected.

***Copy to Custom tab***

Copy the device to the **Custom** tab view.

---

## Viewing Tunnels

---

Click the **VPNs** tab of the VPN Manager Display to view IPSec tunnels configured for devices under management. This portion of the display shows the currently configured VPN tunnels, devices, and default security templates for each of the available encryption levels.

The display is structured as follows:

- Managed VPNs folder
  - List of managed tunnels
    - Endpoint device names and related policies
- Devices folder
  - Device Name
  - Associated Policies
- Security Templates folder

---

## Viewing log servers

List of security templates  
Security Association Type  
Encryption Type  
Authentication Type

---

## Viewing log servers

Click the **Logging** tab of the VPN Manager Display to view log servers in the IDE. The list of servers in use is compiled from the configuration files of the devices under management.

The display is structured as follows:

- Log Servers Folder
  - Log Server Name or IP
  - Log Server's Associated Device(s)
- Devices Not Currently Logging
- Associated Device(s)

---

## Creating a custom view

The **Custom** tab of the VPN Manager Display allows the creation of a customized workspace, optimized to your specific needs. Any of the resources in the Devices view can be listed on the **Custom** tab by tunnel location, level of encryption, device type used, and so on. The Firebox devices themselves (with all their corresponding settings and tunnel statistics), individual device statistics, individual tunnels, and individual remote users from any device can all be monitored. You can also create folders to group information in a way that is meaningful for your own environment.

To add devices to the **Custom** tab:

- 1 In the **Device** tab of the VPN Manager display, right-click the device you want to add to the **Custom** tab.
- 2 Select the **Copy to Custom** tab.
- 3 On the **Custom** tab, drag and drop the device into the desired location or folder in the tree view.

To add a folder on the **Custom** tab:

- 1 Right-click in the **Custom** tab window.
- 2 Select **Add New Folder**.
- 3 Double-click the name of the folder to select it.
- 4 Type a name of your choosing.
- 5 Click elsewhere to save the change.

## Launching applications from VPN Manager

---

Use the VPN Manager display to launch all WatchGuard LiveSecurity applications: Policy Manager, LogViewer, Report Generator, and Event Processor.

To launch any of these applications:

- 1 On the toolbar of the VPN Manager display, click the appropriate icon. These are identical to the ones in the Control Center.  
You can also select **Tools** ⇒ *Application*, where *Application* is the program you want to launch.



---

VPN Manager allows you to manage and configure devices remotely. This is especially helpful when working with a SOHO to set up a tunnel for an employee working offsite at a distant office or their home.

## Starting the Remote Management feature

---

- 1 From the toolbar on the VPN Manager display, highlight the device you want to monitor and then click the SOHO Management icon on the toolbar (to the right of the Policy Manager icon).  
The Client Authentication dialog box appears.
- 2 Select the certificate for this device and click **OK**.  
A dialog box appears telling you that an application is requesting access to a protected item.
- 3 Click **OK**.  
The Remote Management screen appears in your Web browser.

## System administration

The System Administration section allows you to:

- Configure system passwords
- Configure remote logging and configuration
- Configure DMZ settings
- View the configuration of the device

## System password

To view system password options, click **System Password**. Here you set the password for the SOHO and assign an administrator's name to the device.

### Remote logging

To view remote logging options, click **Remote Logging**.

To activate this option:

- 1 click **Enable Remote Logging**.
- 2 Enter the log server IP address and the pass phrase. Click **Submit**.

### Remote configuration

To view remote configuration options, click **Remote Configuration**. To enable this option, enter the pass phrases and click **Submit**.

### DMZ settings

To view DMZ settings, click **DMZ Settings**.

The demilitarized zone (DMZ) is an open area of your network where you allow information to pass unrestricted. To enable the option for this device, enter the information and click **Submit**.

### View configuration

To view the configuration file for this device, click **View configuration**.

The detail of the configuration file is shown.

### Services

To configure services for this device, click **Services**. The services screen appears.

#### *Incoming services*

Click **Allowed Incoming Services**.

#### *Allowed incoming services*

At this point you can either add or remove a service. To add a service click **Add a Service**. All the services listed in the Firebox System 4.6 Policy Manager are also available for this device. The difference is that you do not have the device directly in front of you. Click any of the selections to add them to this device.

#### *Block outgoing services*

You also have the option to block outgoing services on this device. Services such as SMB Networking, TCP or UDP services, and protocols can be blocked from here. You can also remove any blocking that was set up.

The default for blocking outgoing services is like that for the Firebox: no services are automatically blocked. You must specifically designate which services to block.

### Private network

To view the private network settings click **Private Network**. The Private Network screen appears and lists the settings for the private network you are using.

## **Public network**

To view the public network settings click **Public Network**. You see this screen and the details of the public network.

If this device is connected using a PPOE client (frequently this is a DSL connection) the PPOE information is completed.

## **System information**

To view the system information for this device, click **System Information**. This screen provides links to features and the software version this device is using, network statistics, and the event log.

## **Features and Version Information**

This screen details the firmware installed on this device. You also see whether or not WebBlocker is enabled.

## **Network Statistics**

This screen details information about the network you are using. The IP address, public, and private networks are listed.

## **Event log**

This screen shows behind-the-scenes detail for this device.



---

# Index

---

## A

- Activating VPN Manager 5
- Add Device 15
- Adding
  - devices with VPN Manager 13
- Administering tunnels 1
- Authentication
  - VPNs 9

## B

- Browser
  - enabling certificates in 9

## C

- Certificate
  - for DVCP server 9
  - importing for IE 5.0 9
  - importing for Netscape 4.75 10
  - purchasing 5
  - troubleshooting IE 5.0 10
  - troubleshooting IE 5.0 setup 10
  - troubleshooting setup for Netscape 4.75 11
- Certificates
  - removing 11
- Configuration
  - VPN 3
- Configuring
  - VPN Manager 3
- Creating
  - tunnel 19
  - tunnels (drag-and-drop) 19

## D

- Device
  - adding 15

- removing 15
- removing Fireboxes 15
- removing SOHOs 16
- viewing status 23

## Devices

- connecting to a tunnel 18
- enabling 13
- enabling SOHOs 14
- devices 18
- Devices, managing remotely 29

## Domains

- setting up 6

## Drag-and-Drop

- creating tunnel 19
- with IPsec 1

## Drag-and-drop

- devices 3

## Drag-and-drop tunnel-creation 1

## DVCP 2

- device and tunnel management 3
- how it works 3
- server 2, 3
- server certificate 9

## DVCP Clients

- enabling 13
- enabling SOHOs 14

## DVCP Server

- setup 7

## DVCP server

- removing certificates 11

## E

- Editing a tunnel 21
- Enabling Web-based management 9
- Encryption
  - adding new security templates 18
- Encryption, with IPsec 3

---

## F

- Firebox
  - designating as DVCP server 3
- Firebox II
  - connecting to a tunnel 18

## I

- IDE 1, 26
  - planning 6
- IE 5.0
  - enable strong encryption 10
  - importing certificate 9
  - troubleshooting certificate setup 10
- Importing
  - certificate for IE 5.0 9
  - certificate for Netscape 4.75 10
- Installing
  - VPN Manager 6
- Internet Distributed Enterprise. See IDE.
- IPSec
  - creating tunnels 1
  - tunnel configuration 3
  - with DVCP 3
  - with VPN 2

## L

- Launching applications
  - from VPN manager. 27
- License key
  - purchasing 5
- Log server 2
- Lost connections 3

## M

- Management
  - enabling Web-based 9
- Managing devices remotely 29
- Menu options
  - tree-view menu context options 24
- Menu-driven tunnel
  - creating 19

## N

- Netscape 4.75
  - importing certificate for 10
  - troubleshooting certificate setup 11

## O

- Opening the VPN Manager Display 23

## P

- Policy

- adding templates 17
- Policy Template
  - editing 22
- Procedure
  - activating VPN Manager 5
  - add devices to custom tab 26
  - add folder in custom tab 26
  - adding Devices 15
  - adding new policy template 17
  - adding Security Templates 18
  - connecting Devices to a tunnel 18
  - creating Drag-and-Drop tunnel 19
  - creating Menu-driven tunnel 19
  - designating a DVCP server 7
  - editing a tunnel 21
  - importing Certificate for IE 5.0 9
  - importing Certificate for Netscape 4.75 10
  - importing certificate for Netscape 4.75 10
  - installing VPN Manager 6
  - opening the VPN Manager display 23
  - removing a tunnel 22
  - removing Certificates 11
- Purchasing VPN Manager 5

## R

- Reconnections 3
- Register VPN Manager 5
- Remote Management 29
- Removing
  - tunnel 21
- Removing certificates 11

## S

- Security
  - adding templates 18
- Server
  - certificate 9
  - DVCP 2
  - log 2
  - removing certificates 11
- SOHO
  - connecting to a tunnel 18
  - maximum tunnels 17
  - tunnel 20
- Structure of VPN Manager display 24

## T

- Templates 3
  - adding 17
  - adding new security 18
- Tree-view 23
  - connect status 24
  - context menu options 24
- Troubleshooting
  - certificate setup for Netscape 4.75 11
  - IE 5.0 certificate setup 10
- Tunnel
  - administering 1
  - changing 21
  - configuration 3
  - connecting devices to 18

---

- creating for dynamic SOHO 19
- creation wizard 3
- drag-and-drop creation 19
- editing 21
- management 3
- menu-driven creation 19
- removing 21, 22
- SOHO 20
- SOHO maximum 17
- SOHO single-host 20
- telecommuter 20
- viewing 25
- with DVCP, creating 3

Tunnel, creating 1

## V

### Viewing

- device status 23
- log servers 26
- tunnels 25

### VPN

- and IPSec 2
- centrally managing devices 1
- configuration 3

### VPN Manager 1

- activating 5
- add device to tab 26
- add folder to tab 26
- adding devices 13
- adding policy templates 17
- and IDE 6
- appliances 2
- configuration 3
- configuring 3
- description 1
- display structure 24
- enabling browser certificates 9
- features 2
- installing 6
- installing, intro 5
- introduction 1
- launching applications 27
- opening display 23
- physical description 2
- purchasing 5
- removing or changing a tunnel 21
- tree-view 23
- viewing device status 23
- viewing log servers 26
- viewing tunnels 25

## W

Web-based management  
enabling 9

## X

X.509.v3 certificates 9

---