

---

## What is DVCP?

Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard-proprietary protocol that creates a virtual private network. DVCP automates this process by providing templates, automated wizards, and a point-and-click graphical user interface (GUI). Configurations of various types, levels of authentication, and strengths of encryption reside in templates that are selected and applied to the tunnels you create.

DVCP causes a Firebox to act as a server. All policy information— including network address range and tunnel properties such as encryption, timeouts, and authentication— reside on the server. Other Fireboxes, SOHOs, and SOHO | tcs are the clients. The only information the client requires is an identification name, shared key, and the IP address of the server External interface.

Use the DVCP Client Wizard to configure the server to support DVCP tunnels. The wizard creates a tunnel to each client SOHO. The clients then contact the server and automatically download the information needed for them to connect securely.

---

## If You Need Technical Support

If you have problem, please contact us through our Web site to submit a profile of your case. Follow up with a phone call only if the need is too time-critical to wait for a Web response. The WatchGuard Technical Support Web site is located at:  
<https://www.watchguard.com/support/>  
The WatchGuard Technical Support phone numbers are:

- 877-232-3531 (U.S.; End-user support)**
- 206-521-8375 (U.S.; Authorized Reseller support)**
- 360-482-1083 (International)**

WatchGuard Technologies  
505 Fifth Avenue S, Suite 500  
Seattle, WA 98104

---

# WatchGuard® SOHO

## Provisioning Quick Start Guide

This guide provides step-by-step instructions for configuring a virtual private network (VPN) between a Firebox™ running WatchGuard LiveSecurity System™ 4.5 and a SOHO version 2.2. This task consists of three main parts:

- Enabling the VPN Feature Key
- Enabling and configuring SOHO as a DVCP client
- Creating a tunnel to the SOHO

---

### Enabling the VPN Feature Key

Before configuring virtual private networking, you need to enable the VPN Feature Key. To do this requires:

- Installed SOHO
- Internet connectivity
- VPN Feature Key Upgrade Certificate
- Serial number of your SOHO (this is located on the bottom of your SOHO)

When you have all the required items, use the following procedure to enable the VPN Feature Key:

1. Browse to <http://bisd.watchguard.com/soho/upgrade>  
The Upgrade Certificate Redemption Center appears.
2. Enter the following:
  - SOHO serial number
  - Upgrade Certificate Serial Number
  - Upgrade Key
3. Check the information. Upgrade is a permanent, irreversible option. Click **Upgrade**.  
A message appears telling you reboot the SOHO.

4. **Enter the SOHO IP address.**  
The SOHO Configuration menu appears.
5. **Click System Information.**  
The System page appears.
6. **Click Features and Version Information.**  
The Status Page appears.
7. **Click Reboot.**  
The LED lights on the SOHO go out temporarily. The SOHO reboots.

---

## Enabling the SOHO as a DVCP Client

### With a Static IP Address

1. **Browse to the 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 pass phrase.**  
Ask your System Administrator to write these down.
5. **Click Submit.**  
The SOHO reboots and negotiates a tunnel.

### With a Dynamic IP Address

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.

#### User ID

The same ID must be entered in the VPN Manager when adding the device.

#### Shared Secret

Enter a pass phrase for use between the client and server. Ask your System Administrator to write this down in the spaces provided.

7. **Click Submit.**  
The SOHO reboots and negotiates a tunnel to the Firebox II.

---

## Important Numbers

Have the System Administrator enter the information needed to complete your provisioning.

SOHO IP address: \_\_\_\_\_

Read-write pass phrase: \_\_\_\_\_

Read-only pass phrase: \_\_\_\_\_

DVCP server address: \_\_\_\_\_

User ID: \_\_\_\_\_

Shared secret: \_\_\_\_\_

---

## Creating a Tunnel to a SOHO

The following information is for use by the System Administrator when creating a tunnel between the Firebox II and a SOHO. (You cannot perform these procedures on the SOHO side of the tunnel.)

### Using Drag-and-Drop Tunnel Creation

From VPN Manager:

1. **Click the Device tab.**
2. **Click the device name of one of the tunnel endpoints to highlight it. 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.

3. **For each device (endpoint), select a policy template from the drop-down list. Click Next.**  
The policy template determines the resources available through the tunnel. Resources can be a network or a host. The listbox displays any policy templates added to VPN Manager. The Wizard displays the Security Policy dialog box.
4. **Select the appropriate 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.
5. **Click Next.**  
The Wizard displays the DVCP configuration.
6. **Enable the Restart devices now to download VPN configuration checkbox. Click Finish** to restart the devices and deploy the VPN tunnel.

### Using Menu-Driven Tunnel Creation

1. **From VPN Manager 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 list boxes that each list all devices registered in VPN Manager. Select 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 end of the tunnel.**  
The listbox displays any templates added to VPN Manager.
6. **Click Next.**  
The Security Template dialog box appears.
7. **Choose the security template for this VPN. Click Next.**  
The Wizard displays the DVCP configuration.
8. **Enable the Restart devices now to download VPN configuration checkbox.**
9. **Click Finish** to restart the devices and deploy the VPN tunnel.