

WatchGuard System Manager



Upgrade Instructions

Instructions to upgrade from WatchGuard System Manager 7.x to 8.0

Introducing WatchGuard System Manager 8.0

WatchGuard® System Manager (WSM) 8.0 is an important software release for WatchGuard customers. This release introduces our next-generation, Fireware™ Pro appliance software. It also enhances the current WSM management software. With WSM 8.0, you can manage Firebox® X Edge, Firebox III, Firebox X Core, and Firebox X Peak devices at the same time from the same management station. With Fireware Pro appliance software on a Firebox X Core or Peak, you can use advanced network features such as dynamic routing and a feature-rich IPS.

This document introduces the features of WatchGuard System Manager 8.0. It also shows you how to:

- Install the software
- Configure WatchGuard servers
- Move your DVCP server from a Firebox to the Management Server

What's New with WatchGuard System Manager?

With this release, there are many changes to the WatchGuard System Manager – some large and some small. In this section we tell you the most important enhancements.

New WatchGuard System Manager features

We made the VPN Manager the primary management software for all the Firebox devices, log servers, and Management Servers in your network. From WatchGuard System Manager, you can start monitor and configuration tools such as Policy Manager, HostWatch, and the Firebox System Manager.

WatchGuard System Manager also includes:

- Simple management of a network with more than one WatchGuard hardware platform:
 - Firebox III
 - Firebox X Core
 - Firebox X Edge
 - Firebox X Peak
 - Firebox SOHO6 and Firebox SOHO6 Wireless
 - Firebox S6 and Firebox S6 Wireless
- A Management Server that operates on a Windows server instead of on a gateway Firebox. This solution is more scalable and flexible and lets you easily set up a large network with many offices and VPN tunnels.
- A feature that allows you to use SNMP to monitor important device statistics. You can also transmit SNMP traps to SNMP servers.
- Log messages kept in an XML format.

New features introduced with Fireware Pro

The Fireware Pro appliance software improves WatchGuard's ability to supply new features on the same hardware platform. Fireware Pro is available as an upgrade to the WatchGuard System Manager. Speak to your reseller or browse to the WatchGuard Web site for more information. Features of the Fireware Pro upgrade include:

- Enhancements to the Gateway AntiVirus service such as a feature to examine outgoing messages, to lock attachments with suspicious content, and better reports
- Interface independence
- Signature-based intrusion prevention with stateful signature matching
- Multi-WAN for more flexibility and network connection time
- Dynamic routing of these protocols: BGP, OSPF, RIPv1 and v2
- Quality of Service (QoS) which uses “virtual pipes” to regulate the traffic to align with your business requirements
- Active Directory and LDAP integration
- Application Server Load Sharing and enhanced policy management interface for advanced controls and more granular control of your security policy

Enhancements to WFS appliance software

The WatchGuard System Manager 8.0 includes WFS 7.4 appliance software. This version has two important features.

- WSM 8.0 uses a Management Server that operates on a Windows server instead of on a gateway Firebox. This allows for much more scalability and flexibility when you set up a large network with many locations.
- The Log Server keeps log messages in an XML format.

WatchGuard Servers

There are three servers in this release that do Firebox management functions:

- Management server
- Log server
- WebBlocker server

You can configure the servers from a Windows toolbar which you install with the servers. The toolbar appears in the Windows taskbar at the bottom of your computer monitor. The toolbar is used to start, stop, and configure each server.



Installing the software

WatchGuard® System Manager 8.0 is an important release with many changes to the software. It is important that you save all of your current settings. In this section, we show how to:

- Back up the WFS configuration file and image
- Install WatchGuard System Manager software on a management station

You must install all the WatchGuard management software and appliance software before you create a new configuration.

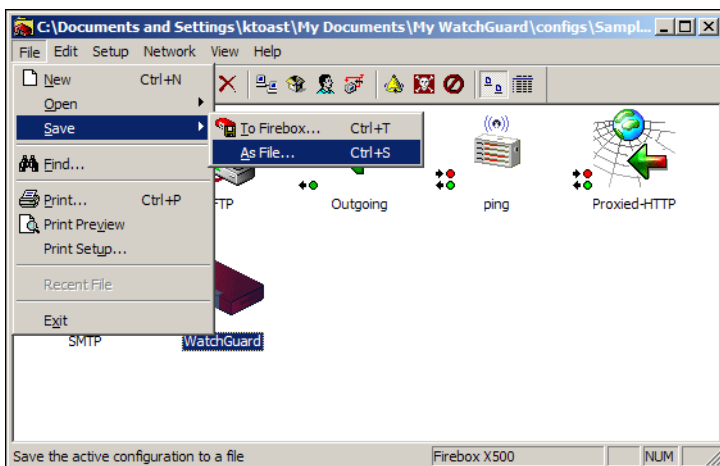
Saving Your WFS Configuration

Before you install the WatchGuard System Manager 8.0 upgrade, save your current configuration file and appliance software image.

Saving the configuration file

You can save the configuration file of a Firebox on the device. You can also save it as a file on a local hard disk drive. Before you install an upgrade, we recommend that you save the configuration file to a local hard disk drive.

- 1 From WFS Policy Manager, select **File > Save > As File**.



- 2 Type the name of the configuration file. Click **Save**.
The configuration file has the file extension *.wfg. You can also save this to a network folder.

Saving the appliance software image

A very important step in the upgrade is to save the appliance software image. The Firebox keeps this file on a backup partition of the Firebox flash disk. To create the WFS backup file:

- 1 Open Control Center, and connect to the Firebox.
- 2 Select **Tools > Advanced > Flash Disk Management**.
- 3 Select **Make Backup of Current Image**. Click **Continue**.
A verification prompt appears. Verify that the Management Station connects to the Firebox Trusted interface either over the network (TCP/IP) or via a modem using out-of-band management.
- 4 Click **Yes**.
The Connect To Firebox dialog box appears.
- 5 Use the **Firebox** drop list to select a Firebox or type the IP address used by the Management Station to communicate with the Firebox. Enter the configuration (read/write) passphrase. Click **OK**.
- 6 Select a file name for the Firebox backup.
The Enter Encryption Key dialog box appears.
- 7 Enter a key for encrypting the backup file. Click **OK**.
This ensures that no one can obtain sensitive information from the backup file.
- 8 When the backup is successful, an Operation Complete alert appears.
- 9 Click **OK**.
You do not need to reboot the Firebox.

Installation requirements

Before you install WatchGuard System Manager, make sure that you have these items:

- WatchGuard Firebox appliance
- WatchGuard System Manager installation software
- A serial cable (blue)
- Three crossover Ethernet cables (red)
- Three straight Ethernet cables (green)
- Power cable
- LiveSecurity service license key

It is also good to restart your Firebox before you start the upgrade procedure. This clears the RAM component and helps to prevent problems during the upgrade.

Software encryption

The management station software is available with two types of encryption.

Base

Uses 40-bit encryption

Strong

Uses 128-bit 3DES encryption

To use virtual private networking with IPSec or PPTP, you must download the strong encryption software. Strong export limits apply to the strong encryption software. It is possible that it is not available for download. For more information, log in to the LiveSecurity service and refer to the online resources at:

https://www.watchguard.com/support/AdvancedFaqs/bovpn_ipsecgrey.asp

Installing the software

With WatchGuard System Manager 8.0, you can have more than one version of the management software on one computer. Make sure that you select a different folder name for each installation.

- 1 If it is necessary, download the WatchGuard System Manager software.
Make sure that you write down the name and the path of the file when you save it to your hard disk drive.
- 2 Open the file and use the instructions on the screens to help you through the installation.
The installation utility includes a screen in which you select the components of the software or the upgrades to install. A different license is necessary when you install some software components.
- 3 At the end of the installation wizard, a check box appears that you can select to start the QuickSetup Wizard. For this upgrade, we recommend that you use the QuickSetup Wizard at this time only if you do not have VPN tunnels and do not use VPN Manager.

Setting Up the Management Server

WatchGuard System Manager 8.0 provides a wizard that migrates your WFS DVCP server configuration to the new WatchGuard management server. This wizard is called the Management Server Setup Wizard and is launched from the WatchGuard toolbar in the Windows taskbar.

WatchGuard® pioneered simple, 1*2*3 VPN configuration with the Dynamic VPN Configuration Protocol (DVCP). A DVCP server controls the VPN tunnels of a distributed enterprise from one, easy to use management interface. A limit to earlier versions of WatchGuard System Manager (WSM) was that you could only use the Firebox® as a DVCP server. With WSM 8.0, we move the DVCP off the Firebox and on to a computer which uses the Windows operating system. This gives increased scalability and flexibility for the network administrator. The Management Server has the same functions as the DVCP server from previous releases of WSM. These functions are:

- Centralized management of VPN tunnel configurations
- Certificate Authority to make and to send out certificates for IPSec tunnels.

The installation software automatically installs the Management Server on the same computer as the management station. You can also install it on a different computer. You must install the Management Server software on a computer that is behind a Firebox with a static external IP address. The Management Server does not operate correctly if it is behind a Firebox with a dynamic IP address on its external interface.

Management Server tasks include:

- Start and stop the Management Server
- Set Management Server passphrases
- Enter the WatchGuard System Manager license key (or VPN Manager license key)
- Configure diagnostic log messages from the Management Server
- Set the Certificate Authority properties such as domain name and publication period
- Start the Certificate Authority user interface

Management Server licenses

NOTE

You must have your VPN Manager license before you can move a DVCP server from a Firebox to a Management Server. You can use a VPN Manager license or a WatchGuard System Manager license to increase the total number of devices managed by the Management Server.

Passwords and the Key Files

The WatchGuard Management Server encrypts important information that it keeps on the Firebox and on your local hard disk drive. It uses a number of passwords to protect sensitive information stored on disk or to secure traffic with client systems. During configuration, you set two passwords and the system creates system passwords:

- Master password – The Management Server uses the master password to encrypt the password file. This protects all of the other passwords. Select and save the master password carefully and safely. Use best practices when you select the password. Do not use the same string for the master password and the administrator password. It is necessary to use the master password to:
 - Move the Management Server data to a different computer
 - Restore a lost or damaged master key file
 - Change the master password
- Administrative password – You use the administrative password to connect to the WatchGuard System Manager software. You use this password frequently. Use best practices when you select the password.
- System passwords – The Management Server automatically makes other passwords. It uses these passwords to encrypt files, traffic on VPN tunnels, and for the Certificate Authority private keys. You cannot see these passwords with the user interface.

Moving a Firebox DVCP Server

The Management Server Setup Wizard moves the configuration properties of a DVCP server which operates on a Firebox to a server which operates on a Windows computer.

NOTE

To do this procedure, the Firebox which you use as a DVCP server must have WatchGuard System Manager 7.3 or later appliance software.

The wizard:

- Requests a master encryption key to encrypt the configuration and password files of the Management Server
- Requests a password to connect to the DVCP server on the management station
- Requests the IP address and configuration password for Firebox which was used as a DVCP server
- Connects to the Firebox
- Gets the DVCP server configuration file from the Firebox
- Uses this configuration file to identify if the Firebox was a basic DVCP server or an advanced DVCP server
- If the Firebox was a basic DVCP server:
 - Gets the list of DVCP clients from the configuration file.
 - Adds those devices to the Management Server configuration file.
 - Gets the domain name, CRL distribution point, CRL publication period, client certificate life time, and root certificate life time of the Management Server. This configures the CA piece of the Management Server.
 - Requests a license key for the Management Server.
 - Requests the name of your organization which it uses as the CA organization.
- If the Firebox was an advanced DVCP server:
 - Uses the configuration properties of the DVCP server to configure the CA on Management Server.
 - Gets the DVCP configuration file (dvcp.cfg) from the Firebox.

- Uses the DVCP configuration file to set the Management Server license key, policy templates, security templates, and DVCP clients.
- Removes the DVCP server from Firebox.
- Removes the DVCP server configuration properties from the Firebox configuration file.
- Changes the “wg_dvcp” and “wg_ca” services of the gateway Firebox to NAT to the new DVCP server on the management station
- Saves the changes to the Firebox
- Starts the Management Server

NOTE

The Management Server Setup Wizard can only move Basic DVCP tunnels that use the gateway Firebox as one endpoint. To replace Basic DVCP tunnels between two Firebox devices which do not have the gateway Firebox as an endpoint, see “Moving Basic DVCP tunnels,” on page 8.

To start the Management Server Setup Wizard:

- 1 From the Windows desktop, double-click the Management Server icon on the WatchGuard toolbar. The Management Server Setup Wizard appears.



- 2 Select **Start Service**.
If the Management Server is not configured, then the Management Server Setup Wizard starts automatically. Use the instructions on each step of the wizard to configure your Management Server.

NOTE

If you change the IP address of the Management Server, you must remove the Management Server software. Then install the software again.

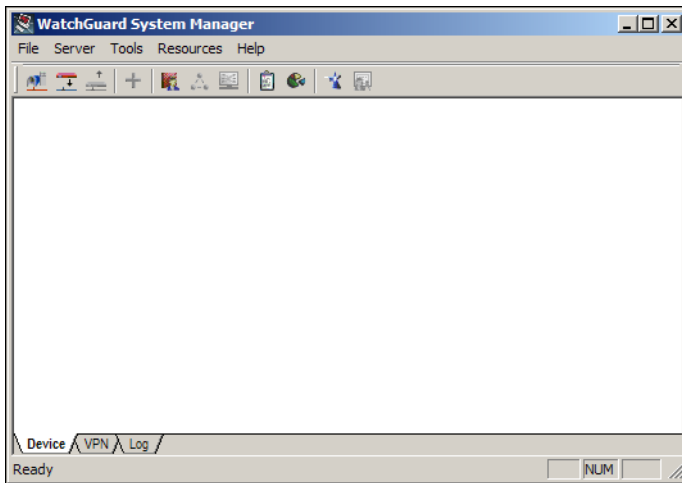
Viewing the network with WatchGuard System Manager

After you complete the Management Server Configuration Wizard, your network can use WSM 8.0. If you had Firebox clients connected to a Firebox DVCP server, those Firebox devices now connect to the Management Server. There is a

policy on your gateway Firebox to allow traffic from your Firebox clients to the Management Server. To examine the new Management Server and tunnels:

- 1 From the Windows desktop, select **Start > Program Files > WatchGuard System Manager 8.0 > WatchGuard System Manager**.

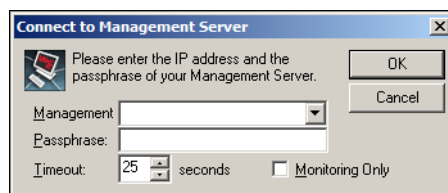
WatchGuard System Manager 8 is the default name of the folder for the Start menu icons. You can change this folder name during installation. The WatchGuard System Manager window opens.



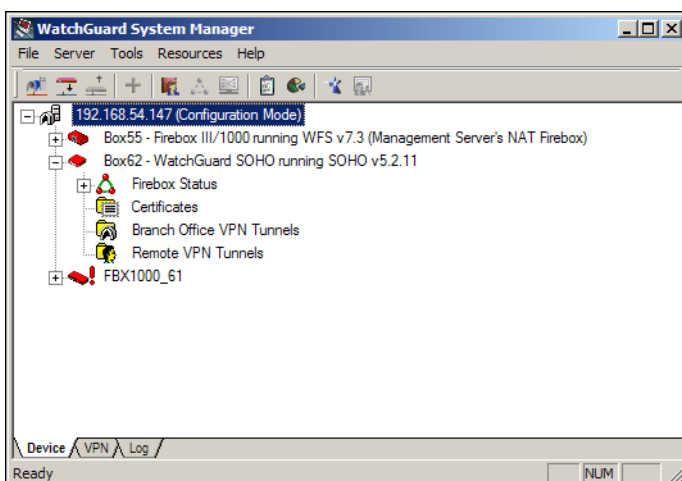
- 2 From WatchGuard System Manager, select **File > Connect To > Management Server**.



Or, click the Connect to Management Server icon on the WatchGuard System Manager toolbar. The Connect to Management Server dialog box appears.



- 3 Use the drop-down list to select your Management Server or type its IP address. Type the management passphrase. Click **OK**.
The server appears in the WatchGuard System Manager Device tab.
- 4 Expand the Management Server entry to see the Firebox clients managed by this Management Server.



Upgrade appliance software to WFS 7.4

After you install the WSM management software and WFS 7.4 on the gateway Firebox, you can use WFS Policy Manager to put WFS 7.4 on other Firebox devices. This is an optional procedure. Your Management Server can connect to and manage Firebox devices which use WFS 7.3.

- 1 From WatchGuard System Manager, select **File > Connect To > Device**.



Or, click the Connect to Device icon on the WatchGuard System Manager toolbar. The Connect to Device dialog box appears.

- 2 Use the drop-down list to select your Firebox or type its trusted IP address. Type the status passphrase. Click **OK**. The device appears in the WatchGuard System Manager **Device** tab.
- 3 Select the Firebox on the **Device** tab. Then, select **Tools > Policy Manager**.
- 4 From Policy Manager, select **File > Save > To Firebox**.
First, Policy Manager shows a prompt to save to a local hard disk drive. Then it saves the new configuration file to the Firebox.

Moving Basic DVCP tunnels

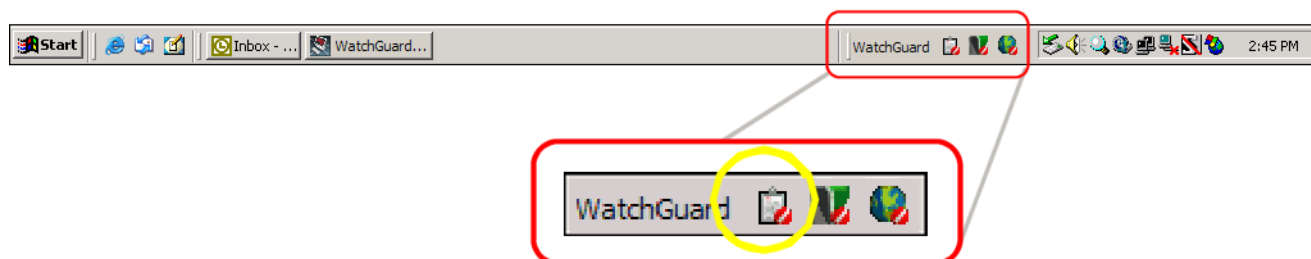
The Management Server Setup Wizard can not convert all the Basic DVCP tunnels in your network. It can only convert the tunnels that use the gateway Firebox as one of the endpoints. The wizard does not convert tunnels from one part of your network to another which do not use the gateway Firebox. You must use this procedure to convert those tunnels so that you can manage them with the Management Server.

- 1 Open each Firebox which uses a Basic DVCP tunnel.
- 2 Delete all Basic DVCP tunnel configurations.
- 3 Save the configuration file to the Firebox. Then restart the Firebox.
- 4 Do this for each Firebox that is an endpoint for a Basic DVCP tunnel and which does not connect to the Firebox which will protect the Management Server from the Internet.
- 5 If necessary, configure your Management Server.
For more information, see "Moving a Firebox DVCP Server," on page 5.
- 6 Start the WatchGuard System Manager. Connect to the remote Fireboxes.
- 7 Drag and drop one Firebox icon to a second Firebox icon. Enter the information necessary to make a tunnel between the two devices.
- 8 Do this for each pair of Firebox devices which must have a VPN tunnel.

Setting Up the Log Server

You must also use Policy Manager to identify the Log Servers for each Firebox. For more information, see the Configuration Guides in the Documentation folder on your management station.

- 1 From the WatchGuard toolbar, select the **Log Server** icon.
The WatchGuard Log Server Configuration dialog box appears.



- 2 Type the encryption key to use for the secure connection between the Firebox and the log hosts. The default encryption key is the status passphrase as selected in the QuickSetup Wizard.
Log Server encryption keys are a minimum of eight characters.
- 3 Confirm the encryption key.
- 4 Select a directory to keep all logs, reports, and report definition files.
- 5 Click **OK**.

Introducing the new LogViewer

The WatchGuard Firebox X Core and Firebox X Peak send log messages to one log management computer. This is known as the Log Server. The log messages are saved in an XML format in the WatchGuard folder on the log server. The extension of the file name is .wgl.xml. You can open this file using an XML editing tool to see log messages.

The Firebox sends log messages to a primary or backup Log Server. The default location for the files are on the installation drive at:

- \Documents and Settings\WatchGuard\Logs.
- \Documents and Settings\Watchguard\reports
- \Documents and Settings\Watchguard\report-defs

Merging log files from WFS 7.3 and before into the new XML format

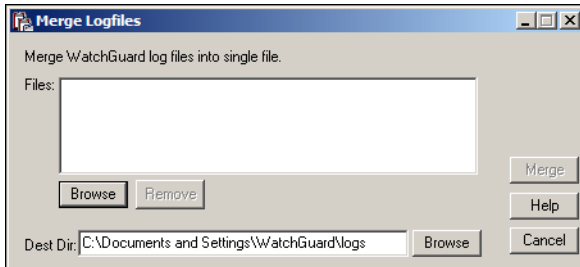
When you install the WatchGuard System Manager 8.0 upgrade, you can convert old log files from .wgl to .xml format. This is also helpful if you operate in a mixed environment with different versions of WSM. After converting WSM 7.3 or earlier log files, you can use the WSM 8.0 LogViewer and report tools to examine those log messages. A Firebox with WFS 7.4 or Fireware Pro appliance software makes log files in the XML format.

When you convert a log file from .wgl to .xml:

- The XML file is usually smaller than the .wgl file.
- If you open a log file in an XML editor, you can see some duplicate entries. This is a function of how report tools operated in WSM 7.3 and earlier and does not cause problems in reports which use the log file.

To convert a log file from .wgl to .xml:

- 1 Right-click the Log Server icon on your Windows desktop tray and select **Merge Log Files...**
The Merge Log files dialog box appears. This dialog box controls merges, and also updates, of log files.



- 2 Click **Browse** to find the location of the log file to convert to XML. If you select more than one log file at the same time, the utility merges all the files into one file. It also converts the format to XML.
- 3 Click **Merge**.
The log files are updated to .xml format and saved to a new file in the specified directory.

Setting Up the WebBlocker Server

The WebBlocker server operates with an HTTP Proxy policy to prevent users from browsing to specified Web sites. You set the categories of permitted Web sites during Firebox® configuration. The HTTP Proxy on the Firebox then uses information on the WebBlocker server to find out if a Web site is in a restricted category.

Doc Version: 050421
Software: WSM8.0

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:

www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with effective, affordable security. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

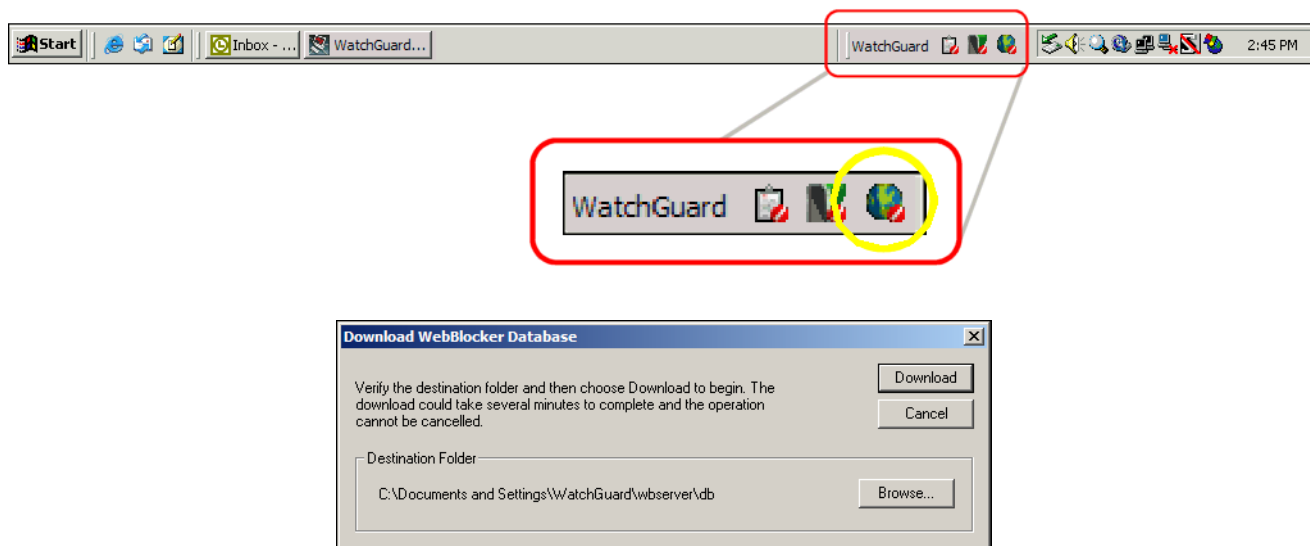
FOR MORE INFORMATION: Please visit us at www.watchguard.com or contact your reseller for more information.

SALES:

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

The first time you connect to the WebBlocker server, it downloads the WebBlocker database.

- 1 From the Windows desktop, click the WebBlocker server icon on the WatchGuard toolbar.
The Download WebBlocker Database dialog box appears.



- 2 Click **Download**.
The file is more than 60 megabytes.
- 3 When the file download is done, right-click the WebBlocker server icon. Select **Start Service**.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:

www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with effective, affordable security. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

FOR MORE INFORMATION: Please visit us at www.watchguard.com or contact your reseller for more information.

SALES:

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

