

WatchGuard® System Manager Upgrade Guide

Instructions to Upgrade from
WatchGuard System Manager 7.x to 8.1



Notice to Users

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, Trademark, and Patent Information

Copyright© 1998 - 2005 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*.

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Software: WFS 8.0

WatchGuard System Manager Upgrade Instructions

Introducing WatchGuard System Manager 8.0/8.1

WatchGuard® System Manager (WSM) 8.0 was an important software release for WatchGuard customers. This release introduced Fireware™ Pro appliance software and added enhancements to the previous 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 Firebox X Peak, you can use advanced network features that include dynamic routing and a feature-rich IPS (intrusion prevention service).

WatchGuard® System Manager (WSM) 8.1 adds the capability to support drop-in mode. Drop-in mode gives the ability to put a Firebox appliance into a well-established network infrastructure with minimal disruption.

This Upgrade Guide is primarily for users who must upgrade from WFS 7.x to WSM 8.1. If you must upgrade from WSM 8.0 to WSM 8.1, see “Upgrading from WSM 8.0 to WSM 8.1” on page 12.

What’s New with WatchGuard System Manager?

With the 8.0/8.1 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

One Management Server can manage all the Firebox devices in your network and create all VPN tunnels. From WSM you can start the tools that monitor and configure your Firebox: Policy Manager, HostWatch, and Firebox System Manager.

WatchGuard System Manager also includes:

- Software that manages 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 and not 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 information. You can also transmit SNMP traps to SNMP servers.
- Log messages that use XML.

New features introduced with Fireware Pro

The Fireware Pro software makes it easy for WatchGuard to supply new features on the same hardware platform. Fireware Pro is available as an upgrade to WatchGuard System Manager. Speak to your reseller or go to the WatchGuard Web site for more information. Features of the Fireware Pro upgrade include:

- Enhancements to the Gateway AntiVirus service that include a feature to examine outgoing messages, to lock attachments with suspicious content, and better reports
- Interfaces that operate independently
- Signature-based intrusion prevention with stateful signature matching
- Support for multiple WANs (wireless area networks) for more flexible configurations and faster network connections
- Dynamic routing of the BGP, OSPF, RIPv1 and RIPv2 protocols
- QoS (Quality of Service) that uses “virtual pipes” to control the traffic to align with your business requirements
- Integration of Active Directory and LDAP
- Application Server Load Sharing and policy management interface enhancements that give you more control of your security policies

Enhancements to WFS appliance software

WatchGuard System Manager 8.0/8.1 includes WFS (WatchGuard Firebox System) 7.4 appliance software. This version has two important features.

- WSM 8.0/8.1 uses a Management Server that operates on a Windows server and not on a gateway Firebox. This allows more scalable and flexible configurations when you set up a large network with many locations.
- The Log Server messages in XML.

WatchGuard Servers

There are three servers in this release:

- Management Server
- Log Server
- WebBlocker Server

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



Installing the Software

WatchGuard® System Manager 8.0/8.1 has 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.

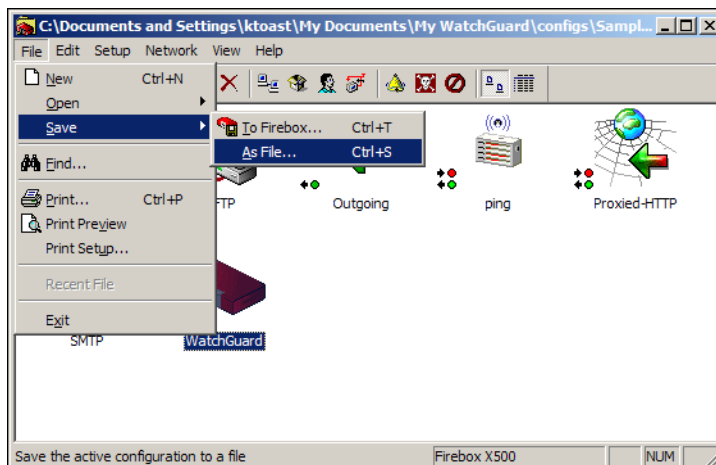
Saving your WFS configuration

Before you install the WatchGuard System Manager 8.0/8.1 upgrade, save your current configuration file and device 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. Before you install an upgrade, we recommend that you save the configuration file to a local hard disk.

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



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

Saving the Firebox software image

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

- 1 Open Control Center, and connect to the Firebox.
- 2 Click **Tools > Advanced > Flash Disk Management**.
- 3 Click **Make Backup of Current Image**. Click **Continue**.
A verification prompt appears. Make sure that the Management Station can connect to the Firebox Trusted interface with the network (TCP/IP) or with a modem that uses out-of-band management.
- 4 Click **Yes**.
The Connect To Firebox dialog box appears.
- 5 From the **Firebox** drop-down list, select a Firebox or type the IP address used by the Management Station to communicate with the Firebox. Type the configuration (read/write) passphrase. Click **OK**.
- 6 Select a file name for the Firebox backup.
The Enter Encryption Key dialog box appears.
- 7 Type a key to encrypt the backup file. Click **OK**.
This makes sure that no one can get sensitive information from the backup file.
- 8 When the backup is successful, an Operation Complete message appears.
- 9 Click **OK**.
It is not necessary to restart the Firebox after this procedure.

Installation requirements

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

- WatchGuard Firebox hardware
- WatchGuard System Manager installation software
- Serial cable (blue)
- Crossover Ethernet cable (red)
- Power cable
- LiveSecurity Service login name and password
- Serial number of the Firebox

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

- 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.
- 2 Open the file and use the instructions on the screens to complete 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 use 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 the Management Server.

Setting Up the Management Server

WatchGuard System Manager 8.0/8.1 has a Management Server Setup Wizard that migrates your WFS DVCP server configuration to the new WatchGuard management server. You start this wizard from the WatchGuard toolbar in the Windows taskbar.

WatchGuard introduced simple VPN configuration with the Dynamic VPN Configuration Protocol (DVCP). A DVCP server controls many VPN tunnels with one easy-to-use management interface. A limit to previous versions of WatchGuard System Manager (WSM) was that you could only use the Firebox® as a DVCP server.

With WSM 8.0/8.1, we move the DVCP off the Firebox and on to a computer that uses the Windows operating system. This makes the Firebox a more scalable and flexible solution for the network administrator. The Management Server has the same functions as the DVCP server. These functions are:

- Central 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 a Management Server license key
- Configure the diagnostic log messages from the Management Server
- Set the Certificate Authority properties that include the domain name and publication period
- Start the Certificate Authority user interface

Management Server licenses

You use the VPN Manager license to operate the Management Server. 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 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. It uses a number of passwords to protect sensitive information saved 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 create the password. Do not use the same string for the master password and the administrator password.
- Administrative password – You use the administrative password to connect to the WatchGuard System Manager. You use this password frequently. Use best practices when you create 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 that operates on a Firebox to a server that operates on a Windows computer.

Note

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

The wizard:

- Gets a master encryption key to encrypt the configuration and password files of the Management Server
- Gets a password to connect to the DVCP server on the management station
- Gets the IP address and configuration password for the Firebox that 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
- Changes the “wg_dvcp” and “wg_ca” services of the gateway Firebox use the NAT (network address translation) set up on the new DVCP server on the management station.
- Saves the changes to the Firebox.
- Starts the Management Server.

If the Firebox was an advanced DVCP server

If the Firebox was an advanced DVCP server, the wizard:

- Uses the configuration properties of the DVCP server to configure the CA on the 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 the Firebox.
- Removes the DVCP server configuration properties from the Firebox configuration file.

If the Firebox was a basic DVCP server

The wizard converts any basic DVCP tunnels that connect to the gateway Firebox into regular tunnels. Basic DVCP tunnels are not supported in WSM 8.0/8.1.

The Management Server Setup Wizard may not convert all the basic DVCP tunnels that you have in your network. It only converts the tunnels that use the gateway Firebox as one of the endpoints. Tunnels without a gateway Firebox endpoint are isolated from the gateway Firebox. If you have basic DVCP tunnels in your network that are isolated, you must use one of these two procedures to convert your tunnels to WSM 8.0/8.1.

Procedure #1

To use this procedure, you must disable the tunnels that are isolated before you use the Management Server Setup Wizard.

- 1 In Policy Manager, remove the basic DVCP tunnel configuration at each endpoint (Firebox) for the tunnel.
Do this for each Firebox that is an endpoint for an isolated tunnel.
- 2 Download the configuration to each Firebox and restart the Firebox.
- 3 Use the Management Server Setup Wizard to:
 - Move your DVCP server to your management server
 - Convert your current DVCP server into a gateway Firebox
 - Convert any basic DVCP tunnels that connect to the gateway Firebox to regular tunnels
- 4 Enable one of the tunnels you disabled.
- 5 Start WatchGuard System Manager
- 6 Add each endpoint Firebox to the management server
- 7 Use drag-and-drop to move one Firebox to a second Firebox to create a tunnel between them.
- 8 Repeat this procedure for each tunnel you want to add.

Procedure #2

This procedure allows you to minimize the downtime for your basic DVCP tunnels that are isolated.

- 1 Purchase a VPN Manager license key with sufficient capacity to convert all the basic DVCP tunnels to advanced DVCP tunnels.
- 2 Install the license key into VPN Manager.
- 3 Use VPN Manager to convert all the basic DVCP tunnels to advanced DVCP tunnels.

Note

The Management Server Setup Wizard can move only basic DVCP tunnels that use the gateway Firebox as one endpoint. To replace basic DVCP tunnels between two Firebox devices that do not have the gateway Firebox as an endpoint, see "Moving basic DVCP tunnels," on page 9.

Setting Up the Management Server

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 Click **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

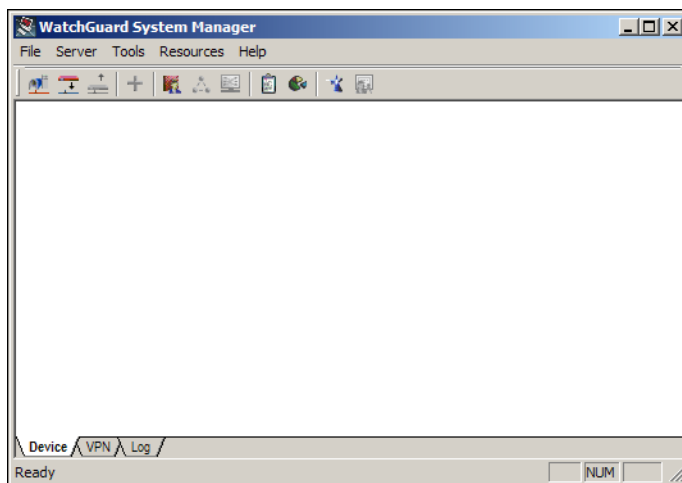
If you change the IP address of the Management Server, you must remove the Management Server software. Then install the software again.

Viewing the network with WatchGuard System Manager

After you complete the Management Server Configuration Wizard, your network can use WSM 8.0/8.1. If you had Firebox clients that connected to a Firebox DVCP server, these clients 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, click **Start > Program Files > WatchGuard System Manager 8.1 > WatchGuard System Manager**.

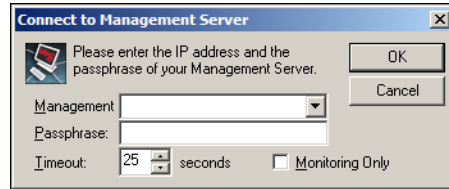
WatchGuard System Manager 8 is the default name of the folder for the Start menu icons. You can change this folder name during installation. The WatchGuard System Manager appears.



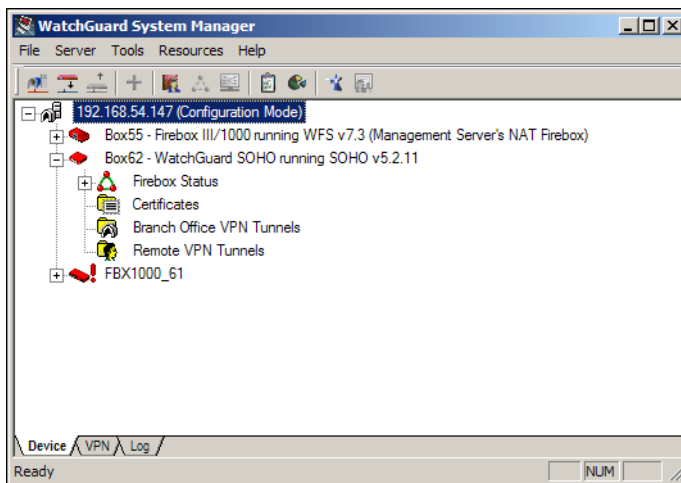
- From WatchGuard System Manager, click **File > Connect To > Management Server**.



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



- From the **Management** drop-down list, 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.
- 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 that use WFS 7.3.

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



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

- From the drop-down list, 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.

- Select the Firebox on the **Device** tab. Then click **Tools > Policy Manager**.

- From Policy Manager, click **File > Save > To Firebox**.

First, Policy Manager shows a message to save to a local hard disk. Then it saves the new configuration file to the Firebox.

Moving basic DVCP tunnels

The Management Server Setup Wizard cannot convert all the basic DVCP tunnels in your network. It can convert only the tunnels that use the gateway Firebox as one of the endpoints. The wizard does not con-

Setting Up the Management Server

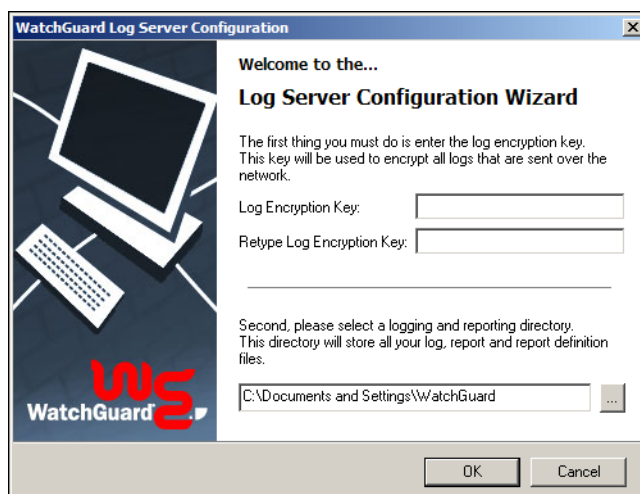
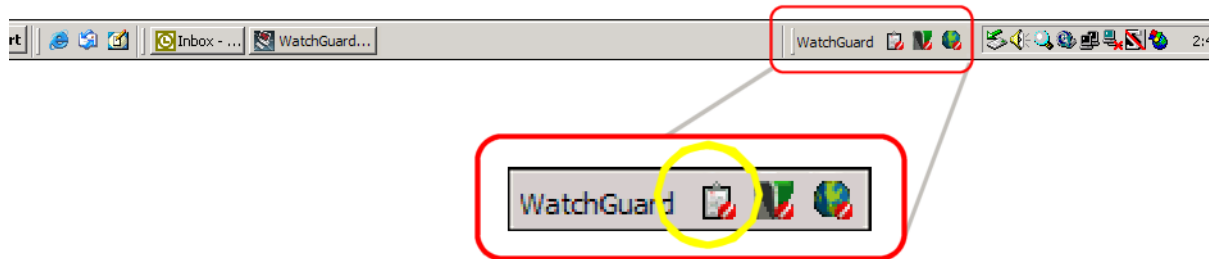
vert tunnels from one part of your network to a second part that does not use the gateway Firebox. You must use this procedure to convert these tunnels if you want to manage them with the Management Server.

- 1 Open each Firebox that 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 that does not connect to the Firebox that protects the Management Server from the Internet.
- 5 If necessary, configure your Management Server.
For more information, see "Moving a Firebox DVCP server," on page 6.
- 6 Start the WatchGuard System Manager. Connect to the remote Fireboxes.
- 7 Use drag-and-drop to move one Firebox icon to a second Firebox icon. Type the necessary information to make a tunnel between the two devices.
- 8 Complete this procedure for each Firebox pair that 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, click the **Log Server** icon.
The WatchGuard Log Server Configuration dialog box appears.



- 2 In the **Log Encryption Key** text box, 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 you selected in the QuickSetup Wizard.
Log Server encryption keys are a minimum of eight characters.
- 3 In the **Retype Log Encryption Key** text box, type the log encryption key.
- 4 Click the button next to the directory box to select a directory to keep all log files, 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 computer that manages log files. This computer is known as the Log Server. The log messages are saved in XML format in the WatchGuard folder on the log server. The extension of the file name is .wgl.xml. To see log messages, you can use an XML editor to open the file.

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

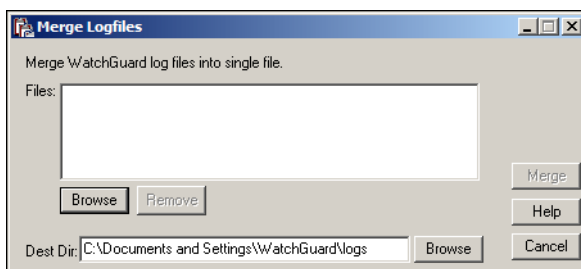
When you install the WatchGuard System Manager 8.0/8.1 upgrade, you can convert old log files from .wgl to .xml format. This is also helpful if you operate in a mixed environment with different versions of WSM. After you convert WSM 7.3 or earlier log files, you can use the WSM 8.0/8.1 LogViewer and 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 that 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.

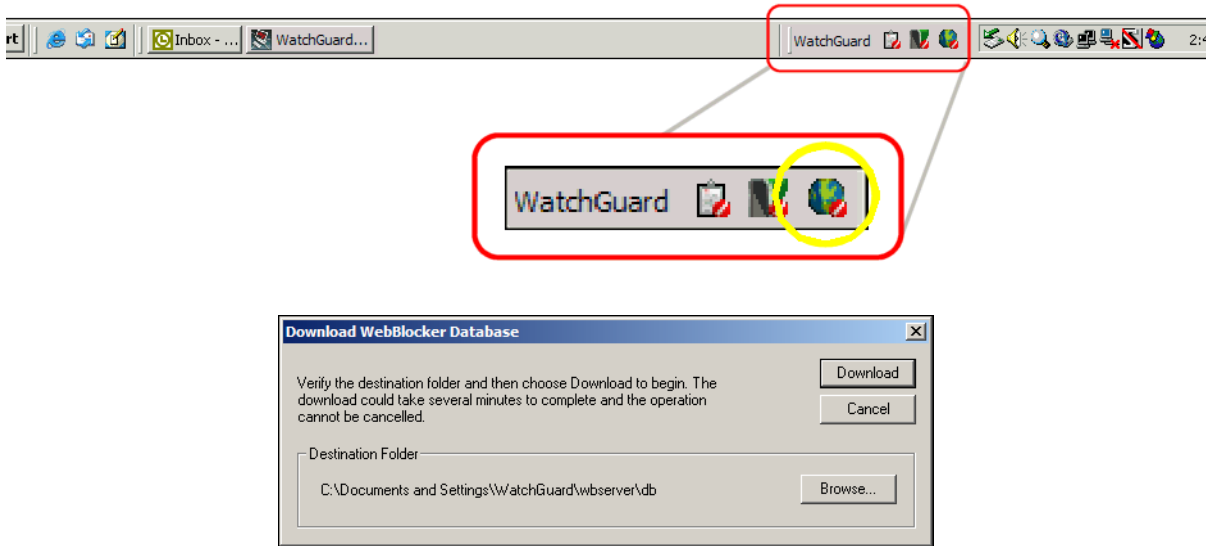


- 2 Click **Browse** to find the location of the log file to convert to XML. If you select more than one log file at the same time, the utility merges all the files into one file. It also converts the format to XML.
- 3 Click **Merge**.
The log files are updated to .xml format and saved to a new file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

Setting Up the WebBlocker Server

The WebBlocker Server operates with an HTTP Proxy policy so users cannot browse 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. 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 you complete the file download, right-click the WebBlocker Server icon. Click **Start Service**.

Upgrading from WSM 8.0 to WSM 8.1

To upgrade from WSM 8.0 to 8.1:

- 1 From the management station, run WSM81s.exe and fireware81.exe.
- 2 Connect to the Firebox and start Policy Manager.
- 3 Select **File > Upgrade**. Browse to the 8.1 folder and select FW810B6015.WGU to upload to the Firebox.

Please note that it may take a few minutes for the file upload to finish. The upgrade process automatically restarts the Firebox.

Note that the WSM 8.1 installer upgrades only the 8.0 components that already exist on the computer. The 8.1 installer keeps all the components in the same directory they were already in.

If you want to add new components, you must:

- 1 Run the installer to do the 8.0 to 8.1 upgrade.
- 2 Run the installer again to add new 8.1 components.

For example, if the original 8.0 installation included only the management station components and you want to add the 8.1 log server, you must run the 8.1 installer to upgrade the 8.0 management station components, and then run the installer again to install the 8.1 log server.

