

WatchGuard System Manager

Documentation Errata



Errors and Changes to the Documentation From WSM 8.0 to WSM 8.1

The WatchGuard® System Manager 8.1 release introduces several product enhancements as well as corrects a number of product deficiencies. This document errata sheet identifies and corrects errors found in the WSM 8.0 version of the documentation. It also provides instructions on how to use functionality introduced with WSM 8.1. Unless noted in this document, functionality between WSM 8.0 and WSM 8.1 is identical.

WatchGuard System Manager User Guide

WSM 8.1 ships with a file in the \Documentation directory with the filename v8.0WSMUserGuide.pdf. All the content applies to WSM 8.0 and WSM 8.1 equally with the exception of the corrections listed here.

Chapter 4: Setting Up Logging and Notification

"Changing the Log Server Encryption Key" (page 33)

Add this step to prior to step 4:

In Policy Manager, select **Logging** and type the new log encryption key.

Chapter 6: Generating Reports of Network Activity

Add the following information about the Inbound Traffic tab, not previously documented:

On the **Inbound Traffic** tab, you see all possible network interface relationships that the Firebox considers to be incoming. For example, traffic that comes from the optional network to the trusted network is considered incoming traffic. If you want to remove a relationship from the list, select it and click **Remove**. You can also add your own source and destination pair to the list. Click **Add** and type the new source and destination you want to set as incoming.

WFS Configuration Guide

WSM 8.1 ships with a file in the \Documentation directory with the filename v7.4WFSConfigurationGuide.pdf. All the content applies to WSM 8.0 and WSM 8.1 equally with the exception of the corrections listed here.

Chapter 2: Using the Firebox System Manager

"Branch Office VPN Tunnels" (page 8)

Add the following sentence to the last bullet:

We support only one routing policy per tunnel.

Chapter 16: Controlling Web Site Access

"Automating WebBlocker database downloads" (page 165)

Replace the existing section with this text:

Automating WebBlocker database downloads

The best procedure to keep your WebBlocker database updated is to use Windows Task Scheduler. To do this, you add a procedure and name it updatedb.bat. This appears in your WatchGuard directory in the WSM8/WFS folder:

- 1 Open **Scheduled Tasks**. To open the Task Scheduler using Windows XP, click **Start**, click **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Scheduled Tasks**.
 - 2 Click **Add Scheduled Task**.
 - 3 The Scheduled Tasks wizard starts. Click **Next**.
-

-
- 4 The screen shows a list of programs. Click **Browse**.
 - 5 Go to your WSM8 directory and then to WFS. Select `updatedb.bat`.
 - 6 Give when it is necessary to do this task. WatchGuard recommends that you update your database each day. You can do it with less frequency, if you have a small bandwidth. Click **Next**.
 - 7 Type the time to start the procedure. Because these downloads are near 60 MB, select a time out of the usual hours of operation.
 - 8 Select how frequently it is necessary to do this task. WatchGuard recommends that you do the updates on weekdays, because the database is not updated on weekends.
 - 9 Select a start date. Click **Next**.
 - 10 Type the user name and the password to use this procedure. Make sure that this user has access to the necessary files. Click **Next**.
 - 11 Examine the configuration. Click **Finish**.

Fireware Pro Configuration Guide

WSM 8.1 ships with a file in the \Documentation directory with the filename `v8.1FirewareConfigurationGuide.pdf`. All the content applies to WSM 8.0 and WSM 8.1 equally with the exception of the corrections listed here.

Chapter 2: Monitoring Firebox Status

“Branch Office VPN Tunnels” (page 15)

Add the following sentence to the last bullet:

We support only one routing policy per tunnel.

“Clearing the ARP Cache” (page 18)

Add the following paragraph:

When a Firebox is in drop-in mode, this procedure clears only the content of the ARP table and not the MAC table. The oldest MAC entries in the MAC table are removed if the table has more than 2000 entries. If you want to clear the MAC table, you must restart the Firebox.

Chapter 4: Basic Firebox Configuration

Add the following sections:

To create a Firebox backup image

- 1 From Policy Manager, select **File > Backup**.
- 2 Type the configuration passphrase for your Firebox.
- 3 Type and confirm an encryption key.
This key is used to encrypt the backup file. If you lose or forget this encryption key, you will not be able to restore the backup file.
- 4 Select the directory in which to save the backup file.
The default location for a backup file with a “.fxi” extension is `C:\Documents and Settings\All Users\Shared WatchGuard\backups\<Firebox IP address> - <date>.fxi`.

To restore a Firebox backup image

- 1 From Policy Manager, select **File > Restore**.
- 2 Type the configuration passphrase for your Firebox.
- 3 Type the encryption key you used when you created the backup image.
The Firebox restores the backup image and restarts. It uses the backup image on restart.

Chapter 7: Configuring Proxied Policies

“Adding rulesets” (page 80)

Delete the following statement:

The actions **Strip** and **Lock** apply only to signature-based intrusion prevention actions.

Chapter 11: “Using Signature based Security Services”

“Configuring Gateway AntiVirus for E-mail in the SMTP proxy”

Add the following section

Unlocking an attachment locked by Gateway AntiVirus

WatchGuard System Manager provides an executable to unlock attachments locked by Gateway AntiVirus:

C:\Program Files\WatchGuard\wsm8\bin\unlock.exe

To open a locked file:

- 1 Open a command prompt.
- 2 Type: **Unlock** <path to locked file>

Chapter 16: Advanced Networking

"About Multiple WAN Support" (page 181)

Add the following sentence to the section on multi-WAN in backup order:

This option is used only on outgoing traffic.

Chapter 17: Controlling Web Site Access

"Getting Started with WebBlocker" (page 201)

Add the following section:

Automating WebBlocker database downloads

The best procedure to keep your WebBlocker database updated is to use Windows Task Scheduler. To do this, you add a procedure and name it updatedb.bat. This appears in your WatchGuard directory in the WSM8/Fireware Pro folder:

- 1 Open **Scheduled Tasks**. To open the Task Scheduler using Windows XP, click **Start**, click **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Scheduled Tasks**.
- 2 Click **Add Scheduled Task**.
- 3 The Scheduled Tasks wizard starts. Click **Next**.
- 4 The screen shows a list of programs. Click **Browse**.
- 5 Go to your WSM8 directory and then to Fireware Pro. Select updatedb.bat.
- 6 Give when it is necessary to do this task. WatchGuard recommends that you update your database each day. You can do it with less frequency, if you have a small bandwidth. Click **Next**.
- 7 Type the time to start the procedure. Because these downloads are near 60 MB, select a time out of the usual hours of operation.
- 8 Select how frequently it is necessary to do this task. WatchGuard recommends that you do the updates on weekdays, because the database is not updated on weekends.
- 9 Select a start date. Click **Next**.
- 10 Type the user name and the password to use this procedure. Make sure that this user has access to the necessary files. Click **Next**.
- 11 Examine the configuration. Click **Finish**.

Chapter 18: High Availability

"Configuring High Availability," (pages 210 - 211)

Replace steps 8 - 10 with the following:

8. Select the **Yes** radio button to encrypt all HA traffic between the Fireboxes. This is usually not necessary, and uses more resources.
9. Select the **No** radio button to not encrypt HA traffic between the Fireboxes.
10. (If you selected the **Yes** radio button) In the **Shared Secret** field, type a shared secret to encrypt HA traffic between the Fireboxes. Type the shared secret again in the **Confirm** field.