WatchGuard System Manager 8.0 and Fireware Pro

Release Notes for WMS 8.0 and Fireware Pro RC2 (Build 3542/4049/WFS7.4)

Introduction

WatchGuard® is pleased to introduce a release candidate of WatchGuard System Manager (WSM) 8.0. WSM is the next version of our centralized management and monitoring software and delivers a host of new feature enhancements. One of the most significant advancements comes with Fireware Pro – the next generation security software system for the Firebox® X line of security appliances. It represents the convergence of the WatchGuard Firebox® System security capabilities with the WatchGuard Firebox Vclass advanced networking features.

Beta Technical Assistance

WatchGuard provides technical support for this beta through one representative at our corporate headquarters. This person sends your questions, ideas, and issues directly to the support representative and engineers with the highest level of expertise on the technology your message refers to.

Please send e-mail about this beta to WSMbeta@watchguard.com.

Platform Compatibility

Software Component	Install On
Fireware 8.0 Appliance Software	Firebox X500, X700, X1000, X2500, X5000, X6000, X8000
WFS 7.4 Appliance Software	Firebox X500, X700, X1000, X2500, Firebox III
WatchGuard System Manager 8.0	Windows 2000 Professional, Windows 2000 Server, Windows XP Professional, Windows 2003 Server
Server Components	Windows (same as WSM 8.0)

WSM 8.0 System Requirements

Minimum required platform:	Pentium-III, 750MHz CPU 394MB RAM 300MB disk space for software (no data)
Recommended platform:	Pentium-IV 1GHz 512MB RAM 300MB disk space for software 10+ GB for application data (logs)

Beta Software

The current version of the software and documentation are on the WatchGuard FTP server. The credentials will be provided via your beta test contact at WatchGuard. The latest beta release is located in a directory named with the following convention: “beta-01” for the first beta release, “beta-02” for the second beta release and so on. All necessary installers and documentation for each release will be in its own directory.

Before You Start

This software release is an important step forward for WatchGuard management software and appliance firmware. There are significant changes and enhancements to the software you install on the management station. We also introduce the new, next generation firmware for the Firebox X called Fireware 8.0.

Please read the *Known Issues and Limitations* section below for important information about limits to this beta. You can also learn more about known issues and methods to configure around these possible problems.

Before you install this beta, make sure that you have:

- One or more Firebox X devices
- An Ethernet cable
- You can also use a crossover cable to make a connection between the management station and the Firebox.
- One serial cable
- The installation software for the firmware
- The installation software for the management station
- Fireware 8.0 license key
- The documentation we include to help you install and use this product
- A backup copy your current WFS 7.x configuration file
- A full backup of the Firebox X WFS image

Installation, Upgrade and Downgrade

Please see the WatchGuard System Manager 8.0 *Migration Guide* for the full procedures to install the WSM 8.0 software and Fireware 8.0 firmware.

The *Migration Guide* also has the procedure to downgrade a Firebox X500, X700, X1000 or X2500 device from Fireware 8.0 to WFS version 7.4.

Beta Version Installation Limits

Beta7

With Beta7, we changed the license key format. You should have received new license keys at that time. To continue to test WatchGuard System Manager v8.0 and Fireware Pro, you must use the new keys. If you have not received keys, please contact the Beta Manager.

Beta8

Before you can install any release after Beta8, you must first uninstall the previous beta release. There are two known problems with the installer which can make it necessary for you to manually delete files from the previous installation. Here are the steps to fully uninstall the previous beta:

1. From the Windows desktop, select **Start > Control Panel > Add/Remove Programs**.
2. Select **Fireware Pro**. Click **Remove**.
3. Select **WatchGuard System Manager 8.0**. Click **Remove**.
4. Restart your management station.

5. There are two folders that the installation software fails to delete. You must remove these folders. The two folders are:

   C:\Program Files\Common Files\WatchGuard

   C:\Program Files\WatchGuard\wsm8

Beta9

You must use eth1 when you configure a Firebox X Peak with Quick Setup Wizard or the fbxinstall.exe utility.

Beta10

You must upgrade all Firebox devices which use Fireware Pro to a Beta10 or later version of the appliance software. A management station with Beta10 or later software can not manage a Firebox appliance with Beta9 or earlier Fireware.

Resolved Issues

Issues Fixed in Beta10

- When you upgrade your management station to WSM 8.0, the installation utility automatically gets your VPN Manager key from your previous installation. [5300]
- The display of tunnel information in WatchGuard System Manager matches the display in Firebox System Manager. [883]
- The QuickSetup Wizard help is complete. [502]
- Policy Manager operates correctly when you change the IP address of the interface which the management station uses to connect to the Firebox. [3892]

Issues Fixed in Beta9

- You can use the fbxinstall.exe utility to upgrade from beta to beta. [4364, 4365]
- You can import an MUVPN configuration file (*.wgx) which includes a WatchGuard RSA certificate. [4311]
- Firebox devices with WFS 7.3 or earlier can send log messages to a WSM 8.0 Log Server. However, Fireboxes with WFS 7.4 or Fireware 8.0 can not send log messages to a WatchGuard Security Event Processor 7.3 or earlier. This is by design and the documentation now clearly explains it. [4367]
- You must use eth1 when you configure the Firebox X Peak with Quick Setup Wizard or the fbxinstall.exe utility. [5055]

Issues Fixed in Beta8

- It is not necessary to restart the Firebox after you change the TCP Maximum Segment Size setting. [4591]
- With this beta, the documentation is content complete. You can find the documentation in the Documentation folder of your installation directory. We welcome your review and comment. These documents are currently in technical review with WatchGuard Engineering: [4362]

  - WatchGuard System Manager User Guide
  - Fireware Configuration Guide
  - WFS Configuration Guide
  - Reference Guide

- There is no longer a long interval between the time you make an IPSec tunnel and the time a Firebox X Edge or Firebox SOHO6 connects to the Management Server. [4445]
- When the remote gateway is a Firebox SOHO6 or Firebox X Edge and the WAN speed is high, an IPSec rekey negotiation is shorter than 20 seconds and no longer disrupts traffic. [3532]

Issues Fixed in Beta7

- A blank screen no longer appears when you open Firebox System Manager from the WatchGuard System Manager. [4323]
- The Service Watch and Bandwidth Meter continue to scroll when you select a different tab. [4940]

Issues Fixed in Beta6

- Fireware supports IP address ranges for 1:1 NAT. You can use Policy Manager to configure the range. [4151]
- The pre-configured PPTP policy is complete. PPTP connections through the Firebox now operate. [4336]
- LogViewer and Traffic Monitor default colors are changed. Log messages for allowed traffic are green. Log messages for denied messages are red. You can change these colors. [4527]

Issues Fixed in Beta5

- The Quick Setup Wizard now has its final graphics. [502]
- The installation application will no longer crash and display the error: “Unhandled exception: Dll function call crashed: ISTR._DoSprintf” [4359]
- The Policy Manager now shows the correct High Availability license information. [3568]
- The Firebox System Manager now correctly monitors license limits and notifies the user when a license is about to expire. [4318]
- The Add MUVPN Wizard now works correctly if you use address ranges. [3727]
- You can now save a configuration file to the Firebox if your management station is on the external network and the external interface uses a dynamic IP address. [4205]
- When you enable the Auto-Order Policies command, Policy Manager now correctly disables the Up and Down buttons. [4270]
- The HTTP Proxy no longer interferes with some Java script software applications. [4316]
- When configuring a SOHO box with a tunnel by means of the Management Server, the SOHO box will erroneously contact the Management Server every 30-60 seconds. The SOHO box is misinterpreting the Management Server’s instructions to only contact the server every 60 minutes. Rather than fix this problem on the Management Server, we have decided the SOHO Firebox must be fixed. [3873]
- A Firebox X Edge version 7.1 can now get its VPN configuration settings from a WSM 8.0 management server correctly in all situations. [4185]
- When you import an MUVPN configuration file (*.wgx), it now works correctly when the configuration:
  - Routes all Internet traffic through the VPN tunnel [4353]
- If the IPS engine blocks HTTP traffic, the Firebox now correctly records a log message. [3970]

Issues Fixed in Beta4

- The utility to upgrade log files from *.wgl format to *.xml format did not always operate correctly. [341]
- The TCP-proxy policy correct examines FTP traffic. [3669]
- You can now use passive mode FTP static network address translation. [3718]
- We corrected a problem which occurred when you disconnected and immediately connected again, with MUVPN would stop all IPSec traffic through the Firebox. [3509]
- When you clone an FTP-server proxy action, all FTP patterns now save correctly. When you clone an FTP-server proxy action, some FTP command patterns do not save correctly. The Firebox denies the invalid commands automatically. [3831]
- The LogViewer correctly shows log messages from a Firebox SOHO or Firebox X Edge. [677]

- When the Log Server gets a large number of log messages at the same time, it now correctly rolls the log files. [3589]

Issues Fixed in Beta3

- The Firebox is set to its factory default configuration if the Quick Setup Wizard fails to setup the Firebox. [3700]
- The maintenance mode option of the Installer now works correctly. [3758]
- In certain conditions, a secondary appliance in a High Availability pair can become permanently caught in the "initializing state" during configuration. This problem is now fixed. [3585]
- After you move your DVCP and Certificate Authority server from the Firebox to a WatchGuard Management Server on your computer, MUVPN tunnels now work correctly. [2898]
- The Policy Manager can now save a configuration file to the Firebox that contains policies with Static NAT rules when the external interface uses dynamic IP addressing. [3424]
- The Policy Manager now makes the correct rules for your Firebox when the **From** field is set to an alias and the **To** field uses static NAT. [882]
- The PPTP RADIUS client now does authentication server failover. [2642]
- The Log Server now installs properly if it is installed by itself. [3942]
- The Log Server now properly fails over to a secondary log server. [3798]
- After you install the WatchGuard System Manager 8.0 software, you no longer need to configure the log system on the Firebox and on the management station. [444]
- When you save a configuration file to the primary Firebox in a High Availability pair, the secondary Firebox no longer becomes the primary. [3112]
- Policy Manager correctly saves a configuration to the Firebox if it contains a policy with one TCP port and a TCP port range. [3301]
- We added a check to prevent a user from accidentally adding their own network to the list of Blocked Sites. [3470]
- Using Policy Manager, you can turn off the log message of allowed packets for a specified policy. This feature now works correctly. [3671]

Issues Fixed in Beta2

- VPN tunnels that use IPSec certificates now operate correctly. [501]
- There is no longer an error message when you click the Authentication tab of the Firebox System Manager. [3850]
- You can now use a Firebox with Fireware 8.0 as a border Firebox for the management server. [573]
- You can use the Firebox System Manager to connect to a Firebox for more than one hour. [3540]
- When you move your DVCP server for a Firebox to a management server, the VPN connection to a remote Firebox with a dynamic IP address now starts correctly in most conditions. [3606]
- A timeout no longer occurs when you save a configuration with a large number of proxy policies to the appliance. [3608]
- Policy Manager did not correctly save the custom MSS adjustment value to the Firebox. The value incorrectly saved as 1460. [3306]
- When Using Policy Manager to restore a backup image to your Firebox, this error message can appear: "Lost connection to the appliance, it is probably restarting now." The backup did in fact complete successfully. [3647]

- When using Policy Manager to create aliases, be careful to not create a circular relationship. An alias must not include itself or an alias that includes the first alias. If you do this, you see the error message: "com.watchguard.vpm.config.ConfigManagerException: java.lang.StackOverflowError". [3655]
- The range of IP addresses for us by PPTP must be more than one address. If you enter only one IP address, the PPTP connection does not operate correctly. [3649]
- There is no longer an error message when you click the Authentication tab of the Firebox System Manager. [3850]
- You can not add a RADIUS or LDAP authentication group to a policy. The user interface operates correctly but the configuration on the Firebox does not. [3430]
- You can only use a maximum of 31 characters for a membership ID or the name of an authentication user group. [3725]
- If you set up static NAT for an incoming SMTP proxy rule and the destination SMTP proxy server does not reply to SYN, no diagnostic log messages are available in Traffic Monitor. [3550]

Known Issues and Limitations

Provisional Features

A provisional feature is one that is available during the beta, but the feature might not be in the version of WSM 8.0 software we release to the public. Your comments and experience with these features helped us to decide if the feature is appropriate for general release. With Beta5, we resolved that:

- High Availability - WSM/Fireware 8.0 includes this feature.
- Drop-In Mode – WSM/Fireware 8.0 does NOT include this feature. It will appear in a future release of the product.

Known Issues with WMS 8.0 and Fireware Pro

The following are known issues with the Beta2 release of the WatchGuard System Manager 8.0 and Fireware Pro. Where available, we include a way to work around the issue.

High Availability

- Do not use the same appliance for High Availability and the gateway appliance of your management server. [4117]

WatchGuard System Manager

- The certificate information for your gateway Firebox does not appear in WatchGuard System Manager until you select Update Device for that appliance. [403]
- When WatchGuard System Manager connects to a remote Management Server, the two applications must use the same time zone. [5356]
- When you install an additional WatchGuard server component on a management station, the new server does not appear in the toolbar. [4616]

  Workaround: Disable the WatchGuard toolbar, and then enable the toolbar again.

Management Server

- You can only set the Key Bits property for Client Certificates with the Management Server Configuration Wizard. [3980]

- The time on the Management Server and a managed client Firebox must be within 5 minutes. The Firebox time must be later than the Management Server time. [3464]
- On the Management Server, you can enter an invalid value for the Publication Interval of the Certificate Revocation List. [3996]

  Workaround: Only use positive integers for the Publication Interval setting.

- In some conditions, a managed Firebox can not connect to the Management Server. This can occur if the Firebox does not download the certificate correctly. [4401]

  Workaround: Change the Management Server Distribution IP Address and update the Firebox client.

Firebox System Manager

- The Lease Time value which appears in the Status Report is incorrect. [4686]
- In certain conditions, Firebox System Manager will not open a configuration file stored on a Firebox. It gives an error: “A connection could not be established to the Firebox.” [4324]

Policy Manager

- The Retry field on the Radius tab of the Authentication Servers dialog box sets the number of times the Firebox tries to connect to the server for each login. This field does not change when the Firebox does a failover to the backup server. [5121]
- The Policy Manager backup and restore features can fail in some conditions.

  Workaround: Do not use backup and restore features with this beta. You only need to backup your configuration file and your license file.

Routing

- The Multi-WAN and High Availability features of the product are not designed to work in a DVCP managed environment. WatchGuard does not support use of this product in these combinations with WSM/Fireware 8.0. This restriction may be removed in a future release.
- Multi-WAN does not work with 1to1 NAT. [5059]

Virtual Private Networking, DVCP, Management Server

- In some conditions, Internet Explorer 5.0 can not open the WatchGuard Certificate Authority Web page. [3714]
- You must restart the Firebox after you change the virtual address pool for MUVPN clients. [5500]
- Active PPTP connections stop after a Firebox restart. [4893]
- The Firebox can not negotiate an MUVPN and a BOVPN tunnel at the same time if there is a branch office gateway configured in Main mode with a Remote Gateway of “Any". [4056]

Logging

- The tool to convert log files from WFS 7.x format to Fireware 8.0 does not convert all log messages. It only converts log messages that the system uses for Historical Reports or LogViewer. [301]
- The Traffic Monitor shows escape characters for some log messages with extra fields. These can be safely ignored. [4577]
- You can safely ignore these log messages which appears during system start up: “OTHER_POLICY_ERR” and “ESP_POLICY_ERR”. [1498]

Proxy Policies

- The IPS engine does not scan most UDP traffic. The only UDP traffic it scans is DNS. [5161]

- The FTP Proxy policy does not give the number of bytes sent or received for use in log messages and reports. [13, 4396]

  Workaround: None. This will also be a limit in the final version.

Documentation and Help

- You get an error message or placeholder text when you click the Show button on a page of context-sensitive help. [5199]
- The Online Help for the WatchGuard System Manager is partially complete. There are links to the help files that do not give help or do not open the Help window. [440]

WFS Appliance Software Issues

WatchGuard Firebox System 7.3 Users

WatchGuard released the final version of WFS 7.3 on December 23, 2004. WatchGuard System Manager 8.0 and Fireware Pro Beta2 includes the WFS 7.3 appliance software with some minor differences.

Differences

- WFS 7.4Beta2 includes the SYNFlood and Link Negotiation hotfixes. It does not include the PPPoE hotfix.
- WFS 7.4 requires that you move your DVCP server from the Firebox to a computer.
- WFS 7.4 does not support Basic DVCP.
- The Management Server is the computer you use as the DVCP server. It can not be a Firebox.
- The VPN Manager is now known as the WatchGuard System Manager.
- You can not use the WatchGuard System Manager to connect to a Firebox DVCP server with WFS 7.3 or earlier firmware. The WSM will only connect to WSM 8.0 DVCP servers. It will also connect directly to Firebox devices with WFS 7.4 or Fireware 8.0 firmware.
- WFS 7.4Beta2 includes the Gateway AntiVirus for E-mail feature.

File Locations

In our continuing effort to clean up the locations of data files used/created by the WatchGuard System Manager software, we changed the default location of many important files in the Beta7 release. We do not plan to make any more changes to the locations of these files.

General File Locations

This table describes the location where data files are stored by the WatchGuard System Manager software. Since it is possible to configure the Windows OS to place these directories on different disk drives, you will need to determine the exact location of these files based on the configuration of Windows on your computer.

File Type	Location
User Created Data	C:\Documents and Settings\<username>\My Documents\My WatchGuard\ (User created data includes files such as Firebox Config files, License files, and certificates. In many case, the WSM software will create subfolders in the My WatchGuard folder to store these files)
User Created Data (Shared)	C:\Documents and Settings\All Users\Shared WatchGuard
Firebox Configuration Files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs <username> = the Windows username for the current user

Firebox Log Files	C:\Documents and Settings\WatchGuard\logs\
Certificates	C:\Documents and Settings\All Users\Shared WatchGuard\certs (Except for certificates used by the Logging Server, the Management Server, and the Certificate Authority)
WatchGuard Applications	C:\Program Files\WatchGuard\wsm8\
Shared Application Libraries	C:\Program Files\Common Files\WatchGuard\wsm8\
Management Server Data	C:\Documents and Settings\WatchGuard\dvcp\
Certificate Authority Data	C:\Documents and Settings\WatchGuard\wmserver\wgca\
WebBlocker Server Data	C:\Documents and Settings\WatchGuard\
Application Specific Data (Internal Operational Data)	C:\Documents and Settings\<username>\Application Data\WatchGuard\ <username> = the Windows username for the current user
Shared Application Data (Internal Operational Data)	C:\Documents and Settings\All Users\Application Data\WatchGuard\
Future Product Upgrade Images	C:\Program Files\Common Files\WatchGuard\Resources
Help Files (Fireware)	C:\Program Files\WatchGuard\wsm8\help\
Help Files (WFS)	C:\Program Files\WatchGuard\wsm8\wfs\

Default Locations

The following tables describe the initial default locations where the WatchGuard applications and servers will look for their data files or for user-created data files, such as Firebox configuration files. In some cases, the default location changes, depending on the last place the application opened a file of a similar type. In the case, the application remembers the last place the file was read/written and looks in that location first.

Quick Setup Wizard

Operation	File Type	Default Location
Write	Application Log	C:\Documents and Settings\<username>\Application Data\WatchGuard\qswiz.log
Write	Firebox Config file	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\<fb-name_wizard>.xml
Write	License file	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\<fb-name_wizard>.tgz
Read	License file	C:\Documents and Settings\<username>\My Documents\My WatchGuard\

Firebox System Manager for Fireware appliances

Operation	File Type	Default Location
Read	Application Config file	C:\Documents and Settings\All Users\Application Data\WatchGuard\fsm.conf
Read/Write	Preferences file	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm_preference
Write	Application Log file	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm.log
Write	Support log file	C:\Documents and Settings\<username>\My Documents\My WatchGuard\<ip-addr>
Read	Help files	C:\Program Files\WatchGuard\wsm8\help\fsm_help_map.csv

HostWatch for Fireware appliances

Operation	File Type	Default Location
Write	Application Log file	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm.log
Read/Write	Preferences file	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm_preference
Read	Help files	C:\Program Files\WatchGuard\wsm8\help\fsm_help_map.csv

Policy Manager for Fireware appliances

Operation	File Type	Default Location
Read/Write	Firebox Backups	C:\Documents and Settings\All Users\Shared WatchGuard\backups\
Read	Product Upgrade Images	C:\Program Files\Common Files\WatchGuard\Resources\
Read	DVCP/CA Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs
Read	Dynamic Routes (RIP, OSPF, BGP)	C:\Documents and Settings\<username>\My Documents\My WatchGuard\

Read	Blocked Sites	C:\Documents and Settings\<username>\My Documents\My WatchGuard\
Read	Blocked Sites Exceptions	C:\Documents and Settings\<username>\My Documents\My WatchGuard\
Read/Write	Firebox Config files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Read/Write	Firebox License Files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Read	Initial License Import	C:\Documents and Settings\<username>\My Documents\My WatchGuard\
Write	MUVPN .wgx file	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\
Read	Help files	C:\Program Files\WatchGuard\wsm8\help\pm_help_map.csv

WatchGuard System Manager

Operation	File Type	Default Location
Read	Config file	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Write	Management Server Config file	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Write	CA Admin Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs\<IP ADDRESS OF DVCP>
Write	SOHO Admin Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs\<IP ADDRESS OF DVCP>
Write	CA Client cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs\<IP ADDRESS OF DVCP>
Read	Help files	<Program Files>\WatchGuard\<product>\wfs\help

Policy Manager for WFS Appliances

Operation	File Type	Default Location
Read	Logging Notification	*Current Working Directory*
Read	Spam Rules Import	*Current Working Directory*
Write	Save Backup	C:\Documents and Settings\All Users\Shared WatchGuard\backups\
Read/Write	Firebox Config files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Write	MUVPN SPD's	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\
Read	Blocked Sites import	*Current Working Directory*
Read	Help files	C:\Program Files\WatchGuard\wsm8\wfs\

Firebox System Manager for WFS appliances

Operation	File Type	Default Location
Read	Help files	<Program Files>\WatchGuard\<product>\wfs\help\

HostWatch for WFS appliances

Operation	File Type	Default Location
Read	Firebox Log file	C:\Documents and Settings\All Users\Shared WatchGuard\logs\
Read	Help files	C:\Program Files\WatchGuard\wsm8\wfs\help\

Flash Disk Management Tool for WFS appliances

Operation	File Type	Default Location
Read/Write	Backup Image	C:\Documents and Settings\All Users\Shared WatchGuard\backups\
Read	Help Files	C:\Program Files\WatchGuard\wsm8\wfs\help\

LogViewer

Operation	File Type	Default Location
Read/Write	Application Config file	C:\Documents and Settings\<username>\Application Data\WatchGuard\
Read	Log4j file	C:\Documents and Settings\<username>\Application Data\WatchGuard\
Write	Application Log file	C:\Documents and Settings\<username>\Application Data\WatchGuard\logviewer.log
Read	Firebox Log files	

Read	Help File	C:\Program Files\WatchGuard\wsm8\help\

Management Server

Operation	File Type	Default Location
Read/Write	All files	C:\Documents and Settings\WatchGuard\wmserver\dvcp\

WebBlocker Server

Operation	File Type	Default Location
Read/Write	All files	C:\Documents and Settings\WatchGuard\wbserver\

Log Server User Interface

Operation	File Type	Default Location
Read/Write	Log Server Config file (WFS)	C:\Program Files\WatchGuard\wsm8\wfs\controld.wgc
Write	Log Server Cert	C:\Documents and Settings\WatchGuard\wlserver\certs\wglog.pem
Write	Log Server Cert file (WFS)	C:\Documents and Settings\WatchGuard\wlserver\keys\wglog.pem
Write	Log Server Config	C:\Program Files\WatchGuard\wsm8\wlserver\conf\httpd.conf
Write	Log Server Config	C:\Program Files\WatchGuard\wsm8\wlserver\conf\logserver.conf
Read	Help Files	<Program Files>WatchGuard\<product>\wfs\help

Log Server for WFS appliances

Operation	File Type	Default Location
Read/Write	Log Server Config file	C:\Program Files\WatchGuard\wsm8\wfs\controld.wgc
Write	Log Server Log	C:\Documents and Settings\WatchGuard\logs\controld.log
Read/Write	Active Firebox Logs	C:\Documents and Settings\WatchGuard\logs\controld.ini
Read/Write	Firebox Log Files	C:\Documents and Settings\WatchGuard\logs\<appliance>-...
Write	WFS Appliance Config file	C:\Documents and Settings\WatchGuard\logs\<appliance>.wgc
Read	Read/Write cert file	C:\Documents and Settings\WatchGuard\wlserver\certs\wglog.pem

Log Server for Fireware appliances

Operation	File Type	Default Location
Read	Log Server Config (Fireware)	C:\Program Files\WatchGuard\wsm8\wlserver\conf\httpd.conf
Read	Log Server Config (Fireware)	C:\Program Files\WatchGuard\wsm8\wlserver\conf\logserver.conf
Read	Cert	C:\Documents and Settings\WatchGuard\wlserver\certs\wglog.pen
Write	Log Server Log	C:\Documents and Settings\WatchGuard\logs\wlserver.log
Read/Write	Active Firebox logs	C:\Documents and Settings\WatchGuard\logs\wlserver.ini
Write	Firebox logs (Fireware)	C:\Documents and Settings\WatchGuard\logs\<appliance>-...

Historical Reports

Operation	File Type	Default Location
Read/Write	Report Definitions	C:\Documents and Settings\WatchGuard\report-defs\<report name>.def (xml)
Read/Write	Report files	C:\Documents and Settings\WatchGuard\reports\<reportname>\report files\
Read/Write	Reporting graphics	C:\Program Files\WatchGuard\wsm8\reports\graphics\<report .jpg/.gif files>

Read	Firebox Logs	C:\Documents and Settings\WatchGuard\logs\<appliance>-...
Read/Write	Report Filters	C:\Documents and Settings\WatchGuard\report-defs\<filtername>.flt
Read	Help Files	<Program Files>WatchGuard\<product>\wfs\help\

Log Merge

Operation	File Type	Default Location
Read	Log files	C:\Documents and Settings\WatchGuard\logs\<appliance>
Write	Converted Log files	C:\Documents and Settings\WatchGuard\logs\<appliance>-... .wgl to .wgl.xml
Write	Merged Log file	C:\Documents and Settings\WatchGuard\logs\<appliance>-...-merged-wgl.xml
Read	Help Files	<Program Files>WatchGuard\<product>\wfs\help

Management Server Setup Wizard

Operation	File Type	Default Location
Read/Write	wg.cfg	C:\Documents and Settings\WatchGuard\\wmserver\tmp
Read/Write	wg.cfg.new	C:\Documents and Settings\WatchGuard\\wmserver\tmp
Read/Write	dvcp_config.xml	C:\Documents and Settings\WatchGuard\\wmserver\tmp
Read/Write	wgca_config.xml	C:\Documents and Settings\WatchGuard\\wmserver\tmp
Read/Write	advdvcp.cfg	C:\Documents and Settings\WatchGuard\\wmserver\tmp
Read/Write	dvcp.cfg	C:\Documents and Settings\WatchGuard\\wmserver\tmp
Read	dvcpinit.dat	conf\dvcpinit.dat (from cur directory)

Management Server User Interface

Operation	File Type	Default Location
Read	Help files	C:\Program Files\WatchGuard\wsm8\help

WatchGuard Certificate Authority

Operation	File Type	Default Location
Write	Publish CRL	C:\Documents and Settings\WatchGuard\wmserver\htdocs\wgca.crl
Read/Write	Manage Certs	C:\Documents and Settings\WatchGuard\wmserver\wgca\index.txt C:\Documents and Settings\WatchGuard\wmserver\wgca\index.txt.attr C:\Documents and Settings\WatchGuard\wmserver\wgca\serial C:\Documents and Settings\WatchGuard\wmserver\wgca\serial_server C:\Documents and Settings\WatchGuard\wmserver\wgca\wgca.cnf C:\Documents and Settings\WatchGuard\wmserver\wgca\wgca.ini C:\Documents and Settings\WatchGuard\wmserver\wgca\wgreq.cnf C:\Documents and Settings\WatchGuard\wmserver\wgca\certs\*.pem C:\Documents and Settings\WatchGuard\wmserver\wgca\keys\*.pem

Moving your existing data files

If you want to use your existing data files from previous beta releases of WatchGuard System Manager 8.0 with the Beta 7 release, follows these steps:

6. Completely uninstall all previous beta versions of WSM 8.0.
   Click **Start > Control Panel > Add or Remove Programs**. Select WatchGuard System Manager 8.0. Click Change/Remove.

7. Answer all the wizard questions. Do not remove the WebBlocker database.
   If you run into a defect that prevents you from completing the uninstall process, you must work with your WatchGuard beta contact to completely remove the previous beta release by hand.

8. Install the beta software.

9. Use Windows Explorer to move these files:

File Type		File Paths
Fireware Firebox config files	**From:**	C:\Documents and Settings\WatchGuard\Configs C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs
	To:	C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs\
WFS Firebox configure files	**From:**	C:\Program Files\WatchGuard\wsm8\wfs
	To:	C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs\
Firebox license files	**From:**	C:\Documents and Settings\WatchGuard\Configs C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs
	To:	C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs\
Backups	**From:**	C:\Program Files\WatchGuard\wsm8\wfs\backup C:\Documents and Settings\<username>\My Documents\
	To:	C:\Documents and Settings\All Users\Shared WatchGuard \Backups

Beta Feedback

To provide input about the software, documentation, or help systems associated with this beta release, we encourage you to contact us at any time at WSMbeta@watchguard.com. We look forward to hearing your feedback and comments.