WatchGuard® System Manager for Firebox X Core and Firebox III

Release Notes for WSM v7.4.1 (Build 2039)

New Features and Enhancements in WSM v7.4.1

WatchGuard System Manager (WSM) v7.4.1 is the latest release of the software that supports the Firebox III and Firebox X Core appliances.

New features in WatchGuard System Manager v7.4.1 include:

- 40 Category WebBlocker: Customers who use the optional WebBlocker service now have more granular control over the web sites their users can access. For more details, please see the *Reference Guide* for WSM7.4.1.
- Gateway AntiVirus outbound email scanning: Customers who subscribe to the optional Gateway AntiVirus for Email service can now configure the service to scan outgoing email.

Enhancements in WatchGuard System Manager v7.4.1 from earlier hotfixes include:

- Gateway AntiVirus Engine has been updated to the ClamAV v0.88 engine. This includes fixes for vulnerabilities in handling of TNEF, CAB and FSG files in addition to other enhancements.
- Because of recent vulnerabilities discovered in different media players, the default behavior for some content types has been changed. This does not affect existing configurations. For new configurations, you can choose to enable these behaviors.
  - ‘audio/*’ are blocked by default in HTTP safe content types.
  - ‘*.pls’ MPEG playlist files are added as unsafe patterns in HTTP proxy.
  - ‘*.pls’ MPEG playlist files are also added to default denied file patterns in SMTP proxy.

Warning: This software cannot be installed on the same management station as WSM 8.X. WSM 8.X includes the WFS 7.4.1 appliance software and tools to manage it.

Note: If you already have WebBlocker Server installed from WSM 8.2 or later, you can use the same WebBlocker Server with your WSM 7.4.1 installation.

Technical Assistance

For technical assistance, please contact WatchGuard Technical Support via telephone (see the numbers in the table below) or check the website at http://www.watchguard.com/support. When contacting Technical Support, please have your registered LiveSecurity key or Partner ID ready.

	Phone Number
U.S. End Users	877.232.3531
International End User	+1.206.613.0456
Authorized WatchGuard Resellers	206.521.8375

Installation and Upgrade

Before installing WatchGuard System Manager Software, please read the information in the Known Issues section.

To install WatchGuard System Manager v7.4.1 management software:

1. Back up your current configuration files.
2. Close all applications.
3. Launch the application file that you downloaded and use the on-screen procedure.
4. If you currently use the WebBlocker service, you need to install the WebBlocker Server for WSM 7.4.1 software separately. Please follow the instructions at the end of this section.

To upgrade your Firebox III and Firebox X appliances to WFS v7.4.1:

1. Back up the current Firebox configuration.
2. If WatchGuard System Manager v7.4.1 software is not installed on your Management Station, follow the instructions in the previous procedure to install the software.
3. Use the WFS Policy Manager to open the Firebox III or Firebox X configuration file.
4. Select **File > Save > To Firebox**. Use the Firebox drop-down list to select a Firebox. Enter the configuration passphrase. Click **OK**. The configuration file is saved to the local hard disk, and then it is saved to the primary area of the Firebox flash disk.

- **Note:** If you are upgrading a Firebox III that is running SpamScreen v7.2.1 or earlier, you must retype your existing SpamScreen license key in Policy Manager, or SpamScreen will not function properly.

To install the WebBlocker Server for WSM7.4.1 software:

1. Stop currently running WebBlocker service.
2. Launch the application file (WSM741_wbserver.exe) that you downloaded and use the on-screen procedure.

Note: You need to download the full WebBlocker database again after the WebBlocker Server completes the installation.

Resolved Issues

WebBlocker

- The Firebox appliance can now be configured to communicate with a WebBlocker service that is running on a port that is not the default (5003). The port can be specified when you add a WebBlocker Server to a proxy configuration in the Policy Manager. WatchGuard recommends that you use the default port (5003) if it does not create any conflicts in your network. [12543]

  If you have to configure the WebBlocker service listening port, please see the FAQ at:

  https://www.watchguard.com/support/advancedfaqs/wb_serverport.asp
- This version of the software handles multibyte character-based URLs correctly when WebBlocker is active. This problem prevented access to some Korean and Japanese websites. [1816]
- When trying to configure an exception to the WebBlocker allowed or denied sites list, the use of the tilde character (~) is now allowed in the URLs. [1372]

Gateway AntiVirus for E-Mail

- GAV no longer strips the line feeds from an Outlook Express text file (.eml) when it is sent as an attachment. [12753,12748]
- GAV no longer reports an attached zip file with a nested archive as a virus when the decompression level is set to a lower limit. [10464]
- When a GAV license expires, the message that appears when you save the configuration file is more user-friendly. [1870]
- An issue where GAV could change large attachments during a scan is fixed. [2277]
- Signature update logging is enhanced to indicate conditions for unreachable servers and the existence of the latest signatures. [2056]
- Added support for selecting and copying the GAV/SpamScreen statistics displayed in the Security Services tab of FSM. [1918]
- Text for a GAV dialog control modified to remove redundant wording.[2039]
- A hotkey added for a control in the GAV dialog.[2035]
- The Firebox correctly manages files that it can not decompress. Use Policy Manager to configure how the Firebox manages these files. [1644]
- There is a new option to allow or deny attachments that are malformed. [1882, 1907]
- You can use a configuration passphrase that includes a space when you update the signature database. [1952]
- Gateway AntiVirus for Email can block UUencoded attachments. [1361]
- Gateway AntiVirus for Email can examine and identify a virus if it uses more than one MIME section. [1363 (18018)]

SpamScreen

- In the default configuration, SpamScreen no longer identifies malformed Outlook Express headers and they will be denied or tagged properly as spam. [1420]
- Statistics now appear on the Front Panel display of the Firebox System Manager. [1830]
- Log messages include the To: and Cc: addresses. [1747]
- The rules are the same rules included in the SpamScreen Update Kit v 2.0. [1864]
- The SpamScreen header is in all e-mail messages that the Firebox scans. [1790]
- When the RBL lookup does not work (e.g. there is no DNS resolution, or the DNS is server down), the Firebox does not use SpamScreen rules to examine the message. When this occurs the Firebox can miss some spam. [1310]
- The Firebox does not send a blank log message when you use SpamScreen. [1982]
- The Firebox immediately closes the connection to an incoming e-mail server after it identifies the server as a source of spam. [1658 (14555)]
- The Firebox sends a log message with the e-mail address of the spam source. [1656 (18094)]

SMTP

- The Firebox responds with the correct max e-mail size value for outgoing traffic. [12731]
- The SMTP proxy now logs the reason an attachment is removed. [12805]
- The SMTP proxy has been updated to handle international filename attachments where the encoding is not specified correctly. [13178]
- You can set the maximum attachment size in SMTP proxy as 0 (unlimited) to allow larger mail attachments. [11918]

- Firebox accepts BDAT transactions containing the message body in the same IP packet as the BDAT command. [1380]
- Removing a file extension from the SMTP denied list removes it from the deny list that triggers PAD.[2021]
- The SMTP Proxy no longer sends a large number of log messages when an error occurs. [1657 (18101)]

Management

- In Policy Manager, after sorting the BOVPN routes, changes to any route will not affect the displayed information for other routes. [12737]
- The default backup name was not populated when saving a new flash image to the Firebox. This has been fixed. [2032]
- Additional GAV statistics as indicated below are displayed in the Security Services tab of FSM [1943]
    - Attachments too big to scan
    - Attachments too big to decompress
    - Current e-mail queue length
    - Longest pending e-mail queue length
- Support for adding any number of address patterns for SMTP proxy has been added. [2041]

Mobile User VPN

- The MUVPN client correctly uses the default gateway of the remote network when you enable this setting in the client configuration file. [1735]
- You can use the Policy Manager to make an MUVPN configuration file (*.wgx) that is read-only. [1667]

Policies and Proxies

- The HTTP Proxy now supports downloads of files larger than 2.5 GB over an HTTP connection using the Mozilla Firefox browser. Internet Explorer does not support download of file sizes beyond 2.5 GB. [12640]
- Resolved multiple issues where the SMTP Proxy would use 100% of the Firebox CPU capacity. [2165, 2185, 2298]

HA

- On failover, the appliance updates the device connected to the external interface with the new MAC addresses of the 1-to-1 NAT Base IPs, which makes NAT base IPs more accessible. [1673]

Authentication

- The Windows NT Authentication server or the ADS server needs to be manually contacted to get the list of users. To do this, use the **Test** button in the **Authentication Servers** dialog box.[1665]

IKE

- The Firebox no longer fails to keep the tunnels up when vulnerability assessment attacks are executed against IKE. [13162]

Others

- The occasional Firebox lockup observed in some unusual cases has been fixed. [1779]
- You can now configure the date format in traffic monitor.[2033]
- The PPPoE send and receive counters update correctly on the Front Panel tab of the Firebox System Manager. [1942]
- The Firebox System Manager correctly displays the MAC address on the Front Panel tab. [1882]
- When the SMTP proxy strips an attachment, the replacement file is now called “WatchGuard Replacement File.” [1952]

- It is not necessary to restart the Firebox after you change the **Temporarily decompress attachments** setting. [17963, 1649]
- Two issues with PPPoE on the external interface have been fixed:
  - The Firebox tries to get a new PPPoE lease when its initial lease expires. [1646 (18091)]
  - The Firebox does not restart when it gets a new lease. [1812]
- Some unhelpful GARP log messages that appeared on a Firebox in drop-in mode have been removed. [1750]
- Some IPSec authentication messages are corrected. [1650 (18056)]

Resolved issues included from previous hotfixes

This software release includes three hotfixes released since v7.3. It also corrects more issues that customers identified.

- For Firebox X Core customers who subscribe to WebBlocker, GAV and/or Spamscreen, the service expiration behavior has been enhanced to provide limited functionality after expiration.
- The resource exhaustion issue that caused VPN tunnels to drop has been fixed. This is applicable to Firebox X only.
- The PPPoE connection reestablishment issue that required a reboot of the Firebox has been fixed.
- The Firebox no longer stops operating when SYN Flood is enabled. [16398]
- The Firebox now detects viruses within CAB files. [17970]
- The Firebox now strips ZIP files that it cannot scan when you enable the "Strip compressed attachments that cannot be scanned" check box. The Firebox is not able to scan password-protected zip files, encrypted Zip files, and compressed files that decompress to a very large size. [17967,18022, 1566]
- Resolved an issue when processing a large number of inbound emails simultaneously that caused this error message: "AV: error contacting AV daemon". [1289]
- The Firebox passes traffic after the link is renegotiated. [18020]

Known Issues

Management

- Sometimes the WSEP system tray icon may disappear after WSEP service restarts. [15121]

  Workaround: In Firebox System Manager, select **Tools > Logging > Event Processor Interface** to show the WSEP system tray icon again.

- Policy Manager may not accept a BOVPN license if it is added from the **Network > Branch Office VPN > Manual IPSEC** dialog box. [10344]

  Workaround: Upload the BOVPN license from Policy Manager. Select **Setup > Licensed Features**.

- When a configuration change that requires a reboot is made to an HA cluster, Policy Manager may not alert you before rebooting the primary Firebox. [10344]
- Uninstallation of WSM7.4.1 after an upgrade from WSM7.3 may leave certain WebBlocker Server binaries and database files on the hard disk. [14740]
- Configuration changes saved to the primary Firebox in an HA cluster are not automatically saved to the standby Firebox. [14743]

  Workaround: The primary and standby Firebox must have IP addresses configured in the same subnet to share configuration changes. They must also have a physical connection to each other. An example of a physical connection is a crossover cable connecting the primary and standby Fireboxes to pass

the heartbeat. When no physical connection is available, you can configure a standby IP address on an interface different than the interface being used for the heartbeat.

- When applying a Firebox X Model Upgrade Key, in some cases the model upgrade may not immediately take effect, and the new Firebox X model number will not appear on the Firebox X LCD panel.

  Workaround: Manually reboot the Firebox X to complete the model upgrade.

- After applying a 3-Port & High Availability upgrade to a Firebox X, the 3-port triangle view of traffic does not immediately change to the 6-port star view.

  Workaround: Close and reopen the WatchGuard System Manger to refresh to the 6-port traffic view.

- Installing two different versions of WatchGuard System Manager in different directories on the same management station can cause issues when you uninstall. If you install two versions, and then uninstall one of them, the version you did not uninstall may not work properly because shared registry keys have been removed. If you then uninstall the second version, you will see an error indicating some files were not successfully unregistered.

  Workaround: Uninstall all versions of the WatchGuard System Manager. Install only the version you want to use.

- In SpamScreen, after upgrading the spam rules to a new version, an attempt to revert to the previous version may not work correctly. You may encounter issues upgrading them again to a newer version.

  Workaround: To revert back to older rule set correctly, reinstall the WFS/WSM software that installed it in the first place. An untitled.cfg configuration file can be used from an installation where the rule update has not been run.

- In certain conditions, the Firebox sends this error message when Policy Manager cannot save a new configuration file to it: `Error connecting to Firebox: unable to sync: error parsing command output. Unknown return value: CAN'T SYNC (Success) [OK].` [15785]

  Workaround: Save the configuration to the Firebox again.

WebBlocker

- WebBlocker uninstall/database issue: If you uninstall an older version of WebBlocker without removing the database, then install a new version to a different hard disk, there can be problems. WebBlocker fails to start because it's looking at the new directory where there is no database.

  Workaround: Download the WebBlocker database again.

- You can install the WebBlocker server on a Windows XP or Windows 2003 server. Surf Control, which provides the WebBlocker database, does not officially support Windows XP or Windows 2003 server. However, our experience in the field indicates that the server functions normally on these operating systems.
- If you install the WebBlocker server and do not download the database, the WebBlocker Server Service fails to start. This is because the WebBlocker Server Service is looking for information in the CSPConfig.ini file for the database which is not present.

  Workaround: Install the WebBlocker Server, download the database, and then reboot the management station so the WebBlocker Server Service starts correctly.

Virtual Private Networking

- When you use the VPN Manager, the Policy Manager cannot edit, manage or remove the ANY service because the ANY service is generated automatically by DVCP server. As a result, clients behind the SOHO can access all networks and aliases behind the Firebox through the ANY service when a SOHO is configured to send all internet traffic through the VPN tunnel.

- When attempting to set up tunnel switching between a SOHO5 and a Firebox in VPN Manager, an error does not appear stating that tunnel switching between the SOHO5 and the Firebox is not supported in v7.2 or v7.3.
- Remote SOHO management fails when the DVCP client's "Unique Name or ID" is more than 13 characters. [17213]
- If you make a PPTP tunnel from the trusted or optional network to the external interface of the same Firebox, the tunnel operates correctly in Drop-In mode. It does not operate correctly in Routed Mode. [16895]
- If a client computer connects to a SOHO through an MUVPN tunnel and that SOHO is configured to send all internet traffic through a VPN tunnel to a Firebox, all traffic destined to the private network on the SOHO is sent to the Firebox.

  Workaround: Move the MUVPN tunnel from the SOHO to the Firebox and configure a service to allow the traffic from the MUVPN tunnel to the private network on the SOHO.

- When you enable the **Allow MUVPN connects from all interfaces** option on the Advanced Mobile User VPN Configuration dialog box, it is necessary for the Firebox to restart before the policy change can function. The Firebox does not automatically restart. [17951]

  Workaround: Save the configuration change and restart the Firebox manually. You can also use the Reboot IPSec command on the Firebox System Manager main menu.

- There is an error when the Firebox external interface uses a static PPPoE address and you upgrade from Basic DVCP to VPN Manager. The VPN Manager can not connect to a Firebox X Edge or Firebox SOHO model that uses a dynamic IP address. [17479]

  Workaround: After you upgrade the Firebox DVCP server, open the Firebox X Edge or Firebox SOHO configuration pages. Set the configuration and status passphrases. Configure the device for VPN Manager. See the Firebox X Edge or SOHO *User Guides* for more information.

- **Virtual Adapter** – If the MUVPN client policy (*.wgx file) has virtual adapter (VA) disabled, the client might not be able to create a tunnel. If this happens, a manual tunnel connection (right-click on the MUVPN icon and click **Connect**) might not work either. [17260]

  Workaround: Right-click the MUVPN icon in the system tray and click Security Policy Editor. Use the Virtual Adapter drop-down list to select Required.

  1. Click **File > Save** to save the security policy. Click **File > Exit** to close the MUVPN policy editor.
  2. Right-click the MUVPN tray icon, and select **Deactivate Security Policy**.
  3. Right-click the MUVPN tray icon, and select **Reload Security Policy**.
  4. Right-click the MUVPN tray icon, and select **Activate Security Policy**.
  5. Right-click the MUVPN tray icon, and select **Connect**.

  The client creates a tunnel. When the tunnel is working, return to the Security Policy Editor. Use the Virtual Adapter drop-down list to select Disabled. Repeat steps 1 through 5.

Gateway AntiVirus for E-mail

- Gateway Antivirus does not scan bin hex attachments. [1533]
- Setting the time zone to one different from GMT still displays the time in GAV/SpamScreen statistics as GMT.[1851]
- In some conditions, the Firebox reboots when put in Sys A - Loopback mode if the crossover cable is connected between the external and an optional interface. [1873]
- Even if you do not have a Gateway AntiVirus for E-mail license key, two of the links on the Security Services tab appear to be functional, but they are not. [17893]
  - The Update Signatures link works and you see a prompt for the configuration passphrase.
  - The Clear Statistics link accepts input and you see a prompt for the configuration passphrase.

- On the Security Services tab, you get a prompt for your configuration passphrase each time you click Clear Stats. [17828]

Other

- **PPPoE Idle Timeout** – If the Idle Connection Timeout is used and an idle timeout occurs, the server end of the PPP connection may not be terminated until the LCP Echo Timeout passes. Because of this it is important, when using the Idle Connection Timeout feature, that LCP Echo Timeout is set to a positive, small value. The default value for the LCP Echo Timeout is a good choice.
- **Incorrect Log Messages for Link Speed and Duplex** – Under some conditions, the log messages for link speed are not accurate. In all cases, the unit functions appropriately but logs incorrectly:
  - "10Mbs half-duplex operation Link OK" appears when a Firebox X NIC link negotiates at 100/10 Mbps full-duplex regardless of the setting in the Policy Manager.
  - "Auto-negotiation enabled" appears even when a Firebox III is configured to operate at a specific speed.
- **Data Channel Log Message** – A log message added for ICSA compliance with the phrase "`data channel created from`" was appearing frequently in the logs, in the default configuration. It is now turned off by default. However, you can still show these log messages. To show this log message, edit your configuration file to add the following configuration properties:

```
services.<your service>.proxies.ftp.incoming.log.data_channel: 1
services.<your service>.proxies.ftp.outgoing.log.data_channel: 1
```

- **Windows 2000/2003 Authentication** - When Windows 2000/2003 Domain Authentication is enabled in Policy Manager, the authentication applet may display the following message "authentication succeeded, but no access granted for user". This indicates incorrect choice of Local versus Global groups. [17911]

  Workaround: See the FAQ at https://www.watchguard.com/support/advancedfaqs/auth_2k3natv.asp for information on how to use NT Server Authentication with a Windows 2000/2003 domain controller installed in native mode.

Features No Longer Supported

- The WebBlocker server is no longer a part of the WSM7.x installation. You must download and install it separately.
- WSM7.4.1 no longer supports installation on Windows NT4 based machines.