WatchGuard® System Manager for Firebox X Core and Firebox III

Release Notes for WSM v7.5 (Build 2063)

New Features and Enhancements in WSM v7.5

WatchGuard System Manager v7.5 is the latest release of the WFS software that supports the Firebox III and Firebox X Core appliances.

New Features in WatchGuard System Manager v7.5 include:

- AES-CBC 128/192/256 bit encryption support for IKE Phase 2.
- Dynamic GAV engine update for customers who subscribe to the GAV for Email service.

Other Enhancements in WatchGuard System Manager v7.5 include (also from earlier hotfixes):

- Revised US/Canada Daylight Saving Time is supported with this release.
- Gateway AntiVirus Engine updated to Clam 0.88.7. This includes major fixes for bugs and vulnerabilities reported since Clam 0.88 version.
- To counter recent security threats more effectively, the default list for denied attachment types in SMTP Proxy has been updated for new configurations.
- A new tab, “RFC Compliance,” has been added to the SMTP Proxy configuration and contains RFC822 and RFC2231 specific controls.
- Administrators are provided with menu options to force a disconnect for Mobile User VPN and PPTP users. You can go to **FSM > Front Panel** or **FSM > Authentication List**, select the remote user tunnel, and right click to pop up the menu.
- Now, IPSEC tunnel configuration provides an option to set or clear type of service (TOS) bit in IP datagram.
- There is a new GUI option for users to specify ICMP rate limits in the Default Packet Handling dialog box.
- Traffic bandwidth on Firebox X Core Models FB X500 and X700 has been improved to provide better performance.
- New license expiration behavior for SpamScreen, GAV, and WebBlocker services for Firebox X Core users keeps these services from functioning after subscription license for the service expires.

Warning: This software cannot be used with WSM 8.X or 9.0. It is only intended for WSM 7.X installations. Support for this WFS update is included in the WSM 9.0 release.

Note: If you already have WebBlocker Server for WSM7.4.1 installed, you do not need a newer version for WSM7.5.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number, LiveSecurity key or Partner ID.

	Phone Number

U.S. End Users	877.232.3531
International End Users	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 v7.5 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 may need to install the WebBlocker Server for WSM 7.5 software separately. Use the instructions at the end of this section.

To upgrade your Firebox III and Firebox X appliances to WFS v7.5:

1. Back up the current Firebox configuration.
2. If WatchGuard System Manager v7.5 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 operate correctly.

To install the WebBlocker Server for WSM7.5 software:

1. Stop the WebBlocker service.
2. Launch the application file (WSM75_wbserver.exe) that you downloaded and use the on-screen procedure.

Note: You must download the full WebBlocker database again after you complete the WebBlocker Server installation.

Resolved Issues

Packet Filter/ NAT

- **Double NAT Enhancement Support** – The hosts on the trusted network can now access servers on the optional network using the public IP address of the Firebox external interface. To do this, the administrator must make an additional static NAT entry of the form "External_IP → Optional_Server_IP" in the outgoing direction. When you do this, there are two limitations:
  - ❖ The Firebox External IP or network address must not conflict with any of the source networks specified in the Dynamic NAT configuration.

- ❖ The second limitation is best illustrated with an example: A host on the trusted network needs to connect to a server on the optional network using the Firebox external IP address. As described above, you must create an outgoing static NAT entry. However in this situation, if you already have a dynamic NAT entry of type "Trusted → External," you may need to add a dynamic NAT exception of the type "Trusted → External IP" for double NAT to operate correctly.

  Similarly, you may need to configure an appropriate dynamic NAT exception for connections from the optional network to the trusted network.

- A problem where a high number of simultaneous TCP NAT connections caused the Firebox to lock up has been fixed. This fix is applicable on 128/256 MB boxes only. [14770]
- The Firebox now correctly allows 'remsh' connections between HPUX machines.[14770]

WebBlocker

- The invalid characters in a custom WebBlocker deny message are parsed correctly to fix the issue where Policy Manager could not connect to Firebox. [14767]
- Now, the URL field under URL-based WebBlocker exceptions dialog only accepts fully qualified domain names. To define exceptions with subfolders, you must use a directory pattern. [14824]

SMTP

- The SMTP proxy now sends attachments with no file name to the GAV scanning engine. [14332]
- The SMTP proxy correctly handles an email that has another email attached within its body. [17360]
- There is a new GUI control to block attachments that use non-standard MIME encoding. [13988]
- SMTP proxy configuration provides a new option to enable/disable RFC2231 parsing. [16864]
- The SMTP Proxy configuration page now allows users to configure an SMTP greeting (Ready) message. [14805]
- An SMTP proxy issue that caused failure of the Firebox to NAT outbound FIN packets has been fixed. [14766]
- The SMTP proxy correctly parses the MIME boundary characters to comply with relevant RFC requirements. This issue caused the insertion of extra carriage returns in very specific circumstances. [16140]

Management

- The Firebox now tries to restart running processes multiple times to eliminate unnecessary reboots when you save your configuration under high traffic load conditions. [15920]
- The WSEP Log Server user interface no longer disappears after the service is started. [15121]
- Policy Manager no longer accepts a DVCP client shared secret if it is weaker than 8 characters. [6524]
- You can now disable the automatic creation of the ANY service when you create VPN tunnels with VPN Manager. [14811]

Mobile User VPN

- Firebox certificate handling has been corrected to resolve an issue that blocked MUVPN clients from authenticating with certificates after 30 days. [18760]
- The Firebox no longer allows MUVPN users to connect after their certificates have expired. [14804]

Branch Office VPN

- There is no longer an IPSEC interoperability issue with Cisco Pix when you use NAT traversal. [14804]

Policies and Proxies

- The HTTP proxy now sends server responses correctly and does not alter the contents. [14772]
- The Firebox no longer requires a reboot for many small configuration changes, including when the HTTP proxy is configured but the policy is disabled. [14942]

- The HTTP proxy no longer fails to cache HTTP requests (terminated with '\r\n') under specifically designed test situations. [14773]

Logging/ Reporting

- You can now use Firefox to display Historical Reports. [18226]
- Administrators can now choose to run a report recursively for subfolders by selecting a check box at **Historical Reports > Report Properties > Setup**. [14983]
- A new UI option has been added to enable Routing Policy debugging for IPSEC. [14807]
- Logging for outgoing broadcast packets has been enabled by default for new configurations. [14777]
- The **Roll Log** feature now always runs a backup script on rolled log files. [5686]
- The Logging Scheduler feature now correctly updates the date/time for the next log roll after the new year. [16070]

Others

- An issue has been resolved that caused Ethernet packets smaller than 60 bytes to be dropped by receiving NIC cards when the Firebox padded them with non-zero bytes. [17290]
- Default Packet Handling now enables stateful ICMP by default for existing and new configurations. [15978]
- Support for service-based outbound static NAT has been added. [14806]

Known Issues

Management

- Under high load conditions, you may get an error when you try to save your configuration to the Firebox. Try to save the configuration again when the traffic load decreases. [19449]
- Information about GAV events that you see in log messages may not show up in Historical Reports. [18440]
- 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, such as a cross-over cable connecting the primary and standby Fireboxes to pass the heartbeat. When no physical connection is available, 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, WSM's 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 may cause problems when you uninstall. If you install two versions, and then uninstall one of them, the version you did not uninstall may not work correctly 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 you upgrade the spam rules to a new version, then attempt to revert back to your original ruleset, SpamScreen may not work correctly.

> **Workaround:** To revert to an older ruleset correctly, reinstall the WFS/WSM software that installed it in the first place. An untitled.cfg 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:** Try again to save the configuration to the Firebox.

Authentication

- Interoperability problem with access-requests in RSA SecurID Radius. [13636]

> **Workaround:**
>
> If Steel-Belted RADIUS receives an access-request with Service-Type=8 (Authenticate Only), by default, it will not return any attributes in the access-accept response. To correct this issue, edit the radius.ini file to include the following value in the Configuration section (follow the directions in the file):
> AuthenticateOnly=0
> Then, restart the Steel-Belted RADIUS/RSA RADIUS service. This value will override the default action. For more information, see RSA’s Document a29647.

WebBlocker

- Occasionally, WebBlocker may block some users from accessing web sites that are not part of the WebBlocker database. This can happen when certain links within a URL redirect users to unclassified sites. [13217]
- If you uninstall an older version of WebBlocker without removing the database, then install a new version to a different hard disk, WebBlocker may fail 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 operates normally on these operating systems.
- If you install the WebBlocker Server and do not download the database, the WebBlocker Server Service fails to start.

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

Virtual Private Networking

- Certificate-based manual IPSec tunnels may not establish when the MD5 authentication algorithm is used in phase 1. [19309]
- 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, you must restart the Firebox or reboot IPsec from FSM. The Firebox does not automatically restart. [17951]
- 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 cannot 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 small office 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 may not be able to create a tunnel. If this happens, a manual tunnel connection (right-click on the MUVPN icon and click **Connect**) may also not work. [17260]

  Workaround: Right-click the MUVPN icon in the system tray and click **Security Policy Editor**. Use the Virtual Adaptor 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 operational, return to the Security Policy Editor. Use the Virtual Adaptor 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 something 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.
- GAV for E-mail feature help may not accurately reflect the latest changes. [18856, 18996]
- 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. When you use the Idle Connection Timeout feature, make sure the LCP Echo Timeout is set to a positive reasonably 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 relating to 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. 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.