WatchGuard® Firebox® X Edge e-Series

Release Notes for Release Notes for Firebox® X Edge e-Series v10.2

Introduction

WatchGuard is pleased to announce the release of Firebox® X Edge e-Series v10.2.

This release contains fixes for Edge defects reported by WatchGuard customers. Areas affected include PPPoE, proxies, multi-wan, branch office VPN, and more. See the resolved issues section for more information.

Appliances Supported with This Release

The Firebox® X Edge e-Series v10.2 software works only on Firebox® X Edge e-Series models. It does not operate and cannot be installed on the Edge, SOHO 6, SOHO 6 Wireless, S6, S6 Wireless or SOHO models.

Contact your account manager to purchase a Firebox® X Edge e-Series appliance.

Important Notice on Software Licensing

The Firebox® X Edge e-Series enforces the following software licensing rules:

- **Registration** — You must register the Firebox X Edge e-Series with LiveSecurity to receive a feature key. If you do not have a valid feature key, only one user can connect to the Internet through the Edge.
- **LiveSecurity** — You must have a current LiveSecurity subscription to install software upgrades.
- **WebBlocker** — When the WebBlocker subscription expires, the Edge device denies all outgoing HTTP traffic by default. You can control this behavior through the WebBlocker>Settings page.
- **spamBlocker** — When the spamBlocker subscription expires, spamBlocker stops evaluating mail and allows all mail.

Installation

Use these instructions to install the Firebox® X Edge v10.2 release. The v10.2 appliance software is installed only in English language by default; one additional language pack can be installed on the Edge during the **Edge Upgrade Wizard** as described in the installation instructions below. You can change the language for the Edge user interface on the Administration page in the Edge web interface.

If you use Windows XP (or other non-Vista version of Windows)

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and save the `Edge_10_2.exe` file to your hard disk.

2. We recommend that you reboot your Edge before you upgrade to Edge v10.2.
3. Double-click the `Edge_10_2.exe` file you downloaded in step 1 and complete the instructions in the **Upgrade Wizard** dialog box.
4. If you want to install a language pack, select the appropriate language during the Upgrade Wizard. You select the language for the Edge user interface in the Quick Setup Wizard or on the Administration page in the Edge web user interface.

If you use Windows Vista or another non-Windows operating system

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and save the `Edge_10_2.zip` file to your hard disk. Decompress the file.
2. We recommend that you reboot your Edge before you upgrade to Edge v10.2.
3. Connect to the Firebox® X Edge System Status page.
   To do this, type https:// in the browser address bar, and the IP address of the Edge trusted interface. The default URL is: https://192.168.111.1
4. On the System Status page, click **Update**.
5. Click **Browse**. Find and select the `yakfw.sysa-dl` file, then click **Open**.
6. Click **Update**. To complete the installation, you must restart the Firebox Edge.
7. To install a language pack, repeat Steps 3-5, but select one of the following files in Step 4:

French:	lang-fr-10.2-arm.wgpk-dl
Japanese:	lang-ja-10.2-arm.wgpkg-dl
Simplified Chinese:	lang-zh-10.2-arm.wgpkg-dl

8. After the Edge restarts, go to the Administration page to change the language in the user interface.

After the update, the System Status page shows the new version as: 10.2 June 3 2008 Build 179920

Note If you currently use Edge v8.0.x software on your Edge, there is a specific upgrade path that you must follow to install this release. Use this chart to determine your upgrade path:

If you are currently running:	Install in this order:
Edge e-Series v8.0	Edge e-Series v8.0.1 > v8.0.3 -> v10.2
Edge e-Series v8.0.3 or later	Edge e-Series v10.2

If you are not sure what version of software is currently installed on your Edge, log in to the administrative interface of your Edge and look at the System Status page. To get Edge e-Series v8.0.3 software, contact WatchGuard Technical Support.

To install Single Sign-On (SSO) agent software

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and download the WatchGuard Single Sign-On Agent 10.2. Save the `WG-Authentication-Gateway.exe` file to your hard disk.
2. Install the file on a domain computer with a static IP address and complete the setup wizard. It is a good idea to install the SSO agent software on your domain controller.

To install local WebBlocker and Quarantine Server software

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and save the `WGEdge10_2QWB.exe` file to your hard disk.
2. Install the file on a local computer and complete the setup wizard.

Resolved Issues

General

- The MAC Address override feature now operates correctly when WAN1 is configured as a wireless client. [23459]
- The Edge no longer assumes that the subnet for 1-to-1 NAT IP is a standard Class C (/24). The subnet mask from the external interface is now used for the 1-to-1 NAT subnet. [27320]
- An issue in the Japanese language version of WSM v10.1 that caused the WPA shared key to disappear after a change to the interface has been fixed. [27214]
- The option to schedule a reboot of the Edge is now available on the Administration page. [27383]
- An issue that caused the Edge to show 'Evaluation Unit' for the serial number after running the Quick Setup Wizard has been fixed. [27147]
- We have added a new time zone option for Venezuela (GMT-4:30). [22975]

Authentication

- A log message that incorrectly showed the RADIUS server as unavailable no longer appears when a user attempts to authenticate to the Edge using an incorrect username or password. [23362]
- The **Session idle timeout** setting for user accounts now operates correctly and is no longer the same as the **Session maximum timeout** setting. [23820]

Single Sign-On (SSO)

- The SSO agent now works in a multiple domain scenario and retrieves authentication information regardless of parent and child domain. [26905]

Proxies

- We have improved the MTU handling for all proxies when the external interface is configured to use PPPoE. The improved MTU handling addresses customer reported problems with receiving attachments using Yahoo mail and AOL mail, slowness when using Yahoo search functions, and accessing parts of some web sites such as www.mappy.fr. [21771] [27093] [26762]
- Email that is not spam is now correctly logged through the POP3 proxy as `Message is classified as not spam (POP3-Proxy).` [23431]
- ICQ is now blocked when the IM - ICQ action is set to **Deny** in the Outgoing Proxy. [22804]
- When you upgrade to v10.2, the content of your custom WebBlocker deny message created in v8.6.x or older software is not lost. [26903]
- Logging options for proxies available on the Debug page now operate correctly. [23680]

spamBlocker

- When you configure spamBlocker for the SMTP proxy, log messages for quarantined confirmed spam are now shown as "ProxyQuarantine: SMTP Confirmed spam" instead of “ProxyQuarantine: SMTP Confirmed”. [23733]

Multi-WAN/WAN Failover

- The reply to a ping request received on WAN1 is now correctly replied to through WAN1. [23556]
- You no longer need to reboot the Edge after you configure the Edge for WAN failover. [23578]

VPN

- Aggressive mode tunnels that use the FQDN for both local and remote no longer fail after you upgrade from v8.6.x to v10.x. [27319] [27331]
- The `Iked` daemon no longer crashes when the local ID type is incorrectly configured as domain name for an IPV4_ADDR. [26924]
- An issue that allowed BOVPN traffic to leave the Edge un-encrypted during a configuration save that included changes to BOVPN settings has been fixed. [23597]
- A VPN tunnel now establishes correctly between two Edge devices when they are both configured with WAN failover and VPN failover and the ping host for WAN1 on both devices becomes unreachable. [23780]
- The VPN statistics page now displays both incoming and outgoing packet count information. [25799]

Known Issues

Network Configuration

- The Wireless Client configuration tab for WAN1 is available on all Edge e-series models. Do not use this wireless tab if you do not have a Firebox X Edge e-Series Wireless. [23910]

1-to-1 NAT

- You cannot use 1-to-1 NAT for IPSec traffic. [13516]

DHCP

- DHCP relay server does not take priority over the Edge DHCP server. [16796]
- DHCP lease times are always reported in GMT. [15431]
- If you use the legacy MUVPN with IPSec client software and create a Mobile VPN default route (0.0.0.0/0) tunnel for a DHCP internal client, the client cannot renew its IP address and the connection terminates when the DHCP lease times out. If you use this configuration, set the DHCP lease timeout to be greater than 8 hours. [15912]

Multi-WAN/WAN Failover

- When you configure policy-based routing to a specific interface (WAN1), the Edge sometimes continues to use round robin. When this occurs, the packet leaving the other interface (WAN2) shows as Policy Based Routing rule interface (WAN1) IP. [27602]
- When using multi-WAN, all packets going out WAN2 (eth3) are shown in the log files as coming from the initial interface Eth1 (for trusted) or Eth2 (for optional). [27519]

- Failover of BOVPN tunnels may not work correctly if WAN1 and the remote IPSec gateway are on the same subnet. [15935]
- Ping intervals are 2 seconds longer than the configured interval. [15598]
- IPSec tunnels always try to negotiate using WAN1. If the Edge is configured for multi-WAN, all IPSec tunnels use WAN1 unless a failover occurs. [23704]
- When the Edge is configured to use multi-WAN, you can use the policy-based routing feature to select the external interface you want traffic for any policy to use. By default, the External interface is selected and load balancing is applied. If you select either WAN1 or WAN2, you must reboot the Edge for the change to take effect. [23519]
- When the Edge is configured for WAN failover to a modem, IPSec tunnel connections may fail to correctly re-key when a large amount of traffic is sent. [23560]

Authentication

- When the setting **Require user authentication (enable local user accounts)** is not selected, anonymous users that access the internet do not register as an "Active session" but do use one of the user licenses. [26493]
- Using the Single Sign-On agent on Vista returns an "Access denied" message to a remote computer that tries to enumerate the current users. [23590]
- When a user authenticates to the Edge and the Edge is configured for Single Sign-On, the user is not able to log off from the Edge. [23708]

Workaround

Use the **Enable automatic session termination** setting to enforce short authentication sessions if necessary.

- We strongly recommend that you do not enable Single Sign-On if multiple users authenticate on the same computer.
- You must use Active Directory authentication for Single Sign-On to work. LDAP authentication is not supported for Single Sign-On.

Proxies

- The initial Bit-Torrent connection is successfully blocked by the TCP-UDP (outgoing) proxy. Bit-Torrent will then attempt to connect on TCP port 80, which will successfully pass through the HTTP proxy or HTTP filter policy. [27474]
- When you use the unsafe file name pattern feature of the HTTP proxy, file name patterns are applied to the full URI and may block some redirects. [23758]

Workaround

Allow unsafe file types and rely on content type blocking, or eliminate the unsafe file name patterns from the default list if they cause a problem.

- When you enable the Outgoing proxy, outbound SIP connections are not correctly sent to the SIP proxy. [23546, all platforms]

Workaround

Configure the SIP proxy to directly handle SIP connections.

- You cannot call from one trusted endpoint to another trusted endpoint behind the same Firebox using an external PBX. This is commonly known as a NAT “hairpinning” scenario. [23872]

- The SMTP proxy does not completely strip Uuencoded and Binhex attachments. A small section of the attachment header remains in the body of the email together with the deny message. [22989]
- VoIP deployments are often complex and use many standard and proprietary protocols. Our current proxies only support standards-based traffic using H.323 and SIP protocols, for basic voice and video transfer. In VoIP industry terminology, these new proxies are more accurately called Application Layer Gateways (ALG). Some ALG features, services, and configurations may not be supported. Unsupported features include data file transfer (such as for chat, whiteboarding, fax transmission, etc), traffic control (QoS), and other limitations noted below for each protocol. Because of all these variables, we strongly recommend that you perform compatibility and interoperability tests within your own environment, before any production deployment.
- The H.323 proxy supports NAT-traversal for voice and video traffic. Note that H.323 Gatekeeper (PBX hosting/trunking) and T.120 multimedia support are not included in this release. This limits proxy use to point-to-point scenarios (such as videoconferences). While compatibility and interoperability cannot be guaranteed, point-to-point audio and video connectivity has been demonstrated with common software clients and videoconference hardware.
- Our transparent SIP proxy supports NAT-traversal for voice and video traffic. It does not provide the PBX registration capabilities of a typical standalone SIP Registrar-Proxy, but instead is an Application Layer Gateway that is transparent to SIP traffic. Although our transparent SIP proxy does support passthrough of this PBX traffic, you must have your own Registrar-Proxy server to route these connections. For this release, our transparent SIP proxy has only been tested with PBX’s located on the external segment of the Firebox (hosted scenario, no trunking). While compatibility and interoperability cannot be guaranteed, point-to-point audio/video connectivity has been demonstrated with common software clients. Hosted audio connectivity has been demonstrated with various telephone handsets.

WebBlocker

- No deny message is sent back to the client when an HTTPS connection is correctly blocked because of your WebBlocker configuration. Blocked HTTPS connections are accurately recorded in the log file. [22515]

spamBlocker

- On the Quarantine Server > Edit-Auto Remove rule dialog box, changes to the **Auto Remove messages with specific text in the subject** rule are not saved to the Quarantine Server. While the UI shows that the rule has been deleted, it remains effective. The only way to make that rule ineffective is to clear the check box for **Auto Remove messages with specific text in the subject**. [26796]
- If you use both spamBlocker with Virus Outbreak Detection (VOD) enabled and Gateway AV to scan your email and the SMTP proxy detects an email message that is both spam and a virus, the SMTP proxy applies the action that is configured for VOD to the message. Specifically, if the VOD action is set to **Strip**, then the attachment(s) are removed from the message and cannot be recovered. If the VOD action is set to **Lock**, the attachment is locked in the quarantined message. [23709, 23711]
- When spamBlocker finds a Virus Outbreak Detection (VOD) indication for an email message, all of the email’s attachments are stripped or quarantined. This includes the body of the email, if the sending client has sent it in HTML format.
- When an infected email message with multi-part attachments (i.e., embedded email messages) is detected by VOD, and Firebox is configured with the **Strip** action, a small section of the email header in the attachment remains in the delivered attachment, together with the deny message for the attachment. This header information should cause no problems because viral content is always stripped. [23550]

- spamBlocker does not work if the Edge cannot reach the primary DNS server. [18159]

Gateway AV/IPS

- Signature update log messages show the previous time and date information after a time zone change is made. The correct time zone does not show until the Edge is rebooted. [17754]

Wireless

- Some legacy wireless client hardware and software may not show all the wireless networks when the client has connected to one of those networks already. If you need to connect to another Edge's wireless network, you may need to disable and re-enable the wireless network adapter.
- When the WAN1 interface is configured as a wireless client, the Traffic Control feature does not work correctly. [23757]
- Wireless clients running Windows XP SP1 may not be able to connect when the Edge is configured to use WPA2 ONLY for authentication. [23808]
- The WAP light on the front panel of the Edge illuminates when the Edge is configured as a Wireless Access point or when the External WAN1 interface is configured as a wireless client. [23121]
- When you activate the Wireless Guest account you may see the Edge DHCP server die three times when the Edge restarts. This is expected and the DHCP server will work normally within two minutes after the Edge has restarted. [23792]
- You cannot use an XBX 360 wireless client to establish a wireless connection to the Edge. [27481]
- If your Edge is running an earlier version of Wireless Guest Services (Edge v8.0 through Edge v8.5), you must re-configure Guest Services after you upgrade to Edge v10.2.

VPN

- If the Edge is configured with a BOVPN tunnel to a remote network that is in the same subnet as the trusted network on the Edge, the trusted interface may become inaccessible. Do not configure the Edge to have overlapping networks between the trusted and remote BOVPN network. [27106]
- The Edge uses more memory than desired when IKE rekeys are configured to occur frequently. This can cause slow Edge management connections. If you change the default IPSec rekey settings, make sure that the tunnel does not rekey more than twice each hour. [24221]
- An Edge installed with v8.6.2 under WSM management shows a red exclamation mark for tunnels that rekeyed based on time expiration when no traffic has passed through that tunnel since the rekey occurred. Once traffic attempts to pass through this tunnel, the red exclamation mark disappears and the tunnel operates correctly. [22412]
- An Avaya phone using H.323 through a BOVPN tunnel may cause the Edge to reboot. [24191]
- Outgoing Mobile VPN with IPSec connections through the Edge may not establish when you use a Cisco VPN Client. [19183]

Mobile VPN with SSL

- If an SSL client is connected to the Edge and the administrator changes the SSL configuration, the SSL client is not disconnected from the Edge. The user must manually disconnect and then reconnect to get the new configuration file. [23921]
- When you edit the Default group from the Firebox Users page, the **Allow remote access with Mobile VPN with SSL** check box appears selected, However, it is not enabled and cannot be changed. [23449]
- You cannot install the Mobile VPN with SSL client on a Windows 2000 Pro computer. [23667]

- The Mobile VPN with SSL client cannot connect to the Edge from the trusted network. [22547]

> **Workaround**
>
> Configure Mobile VPN with SSL clients to connect to the Edge from the optional network.

- The Mobile VPN with SSL Mac client does not check for its configuration when its connection to the Firebox is lost (not disconnected). You must disconnect and reconnect to establish the VPN connection again. [23109]

SNMP

- When you configure the Edge to use SNMP v3, the password must be 8 characters or more to work correctly. [23531]

Traffic Control

- Traffic Control for IPSec uses the VPN-ANY rule instead of the most specific rule. [24206]

Logging and Real-time Monitoring

- When you select the System Status page in the Edge UI, you may see this error in your log files: `httpd doInclude: INCLUDE failed for "lang.inc" result code was -1.` The log message is informational and can be ignored. [27322]
- Logs appear truncated when the Edge sends log messages to a legacy WatchGuard Security Event Processor Log Server. [27430]
- Traffic between the trusted and optional networks is not shown in the event log file. [15611]
- When you enable **Log traffic prioritization** on the **Network > Traffic Control** page, the prioritization is not included in log messages generated by any proxy policy. [23164]

Resetting an Edge to Factory Default Settings

- The configuration file is not erased when you restore the factory default settings. [15174]

> **Workaround**
>
> When you restore the Edge to factory default settings, make sure you hold the reset button on the Firebox X Edge e-Series for 45 seconds to erase the configuration file.

User Interface

- The Edge v10.2 software includes many bug fixes that do not affect the user interface. Any changes to the user interface included in the v10.2 release are not localized. If you upgrade from the localized v10.1 release to the v10.2 release, note that new UI elements remain in English. There are no updates to the localized help content.
- During the Quick Setup Wizard, a second login prompt is requested after you enter the feature key. [21994]
- You may need to clear your browser cache after you update the Edge from v8.x to v10.1 to see new user interface options and all new features. [20457]
- If you use Internet Explorer v7 to manage your Firebox X Edge e-Series, you see a Certificate Security warning. The warning is normal with all versions of IE and Firefox, but the warning in IE7 is strongly worded and suggests you not continue. You can disregard this message. Because the Firebox X Edge can change its IP address from the default setting, the certificate on the Firebox does not include an IP address. This mismatch between the requested IP address and the certificate causes this warning. [14434]

Single Sign-On (SSO) Implementation Notes

The Firebox X Edge v10.0 release introduced support for Single Sign-On (SSO) for Firebox administrators currently using Active Directory user authentication. For SSO to work, you must install SSO agent software, also known as the WatchGuard Authentication Gateway software, on a domain computer on your network with a static IP address. Make sure that the computer on which you install the SSO agent software has the Microsoft .NET Framework 2.0 installed. Single Sign-on has been tested with Windows 2000 Advanced Server domain controllers and Windows 2003 domain controllers.

Before you install the Single Sign-On agent software, you must create a user account. The software will run with the permissions of the user account you create.

- You must add the user account to the Domain Admin group and set the Domain Admin group as the primary group for this user.
- The user account must be configured with a password that never expires.
- The user account must be configured with the rights to log on as a service (Domain Security Policy > Local Policies > User Rights Assignment > Log on as a service).
- You must add the IP address of the computer on which you install the SSO agent software to the SSO Exceptions List in your Edge configuration (**Firebox Users > Settings**).

Implementation Notes

- Make sure that printing and file sharing is enabled on every computer from which users authenticate using SSO.
- Make sure that NetBIOS and SMB ports are not blocked on every computer from which users authenticate using SSO. NetBIOS uses TCP/UDP ports 137, 138, 139 and SMB uses TCP port 445.
- Make sure that all computers from which users authenticate using SSO are members of the domain with unbroken trusts.

User Documentation

Documentation changes for the Edge v10.2 release are included in an updated English help system available at www.watchguard.com/help/documentation. There is no updated Edge User Guide for this release.

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	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375