Fireware XTM v11.0.2

Release Notes for XTM 1050 and Firebox X Peak, Core, and Edge e-Series Appliances running WSM v11.0.2

Fireware XTM OS Build b243177
Revision Date: October 15, 2009

Introduction

WatchGuard® is pleased to release WatchGuard System Manager (WSM) v11.0.2 management software and Fireware XTM v11.0.2 appliance software. This release builds upon the release of Fireware XTM OS v11. Read the v11.0 release notes, available with the WSM v11.0 download, for more information on the new features in Fireware XTM v11.

The v11.0.2 release contains a number of defect fixes for issues reported by WatchGuard customers. Areas affected include multi-WAN, Mobile VPN, authentication, and changes to the Management Server.

See the Resolved Issues section below for a complete list of resolved issues.

Before You Start

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

- A Firebox X Core or Peak e-Series device running Fireware v10.2.x or higher, a Firebox X Edge e-Series device running v10.2.9 or higher, or a WatchGuard XTM 1050.
- The required hardware and software components as shown in the Systems Requirements table below.
- An active LiveSecurity subscription.
- Feature key for your Firebox – If you upgrade your Firebox e-Series from an earlier version of Fireware or Edge appliance software, you can use your existing feature key.
- Documentation for this product is available at www.watchguard.com/help/documentation

Fireware XTM and WSM v11.0.2 Operating System Compatibility

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit)	Microsoft Windows XP SP2 (64-bit)	Microsoft Windows Vista (32-bit)	Microsoft Windows Vista (64-bit)	Microsoft Windows Server 2003	Mac OS X V10.5 (Leopard)
WatchGuard System Manager application	✓	✓*	✓	✓*	✓	
Fireware XTM Web UI *Supported Browsers: IE 7, Firefox 3.x*	✓	✓	✓	✓	✓	✓
WatchGuard Servers	✓	✓*	✓	✓*	✓	
Single Sign-On Agent software	✓		✓		✓	
Single Sign-On Client software	✓		✓		✓	
Mobile VPN with IPSec client software	✓	✓	✓	✓		
Mobile VPN with SSL client software	✓		✓			✓

Revision: 10/09/09

* You can use 64-bit Windows operating systems that support 32-bit applications.

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software	Fireware XTM Web UI
Minimum CPU	Intel Pentium IV 1GHz	Intel Pentium IV 2GHz	N/A
Minimum Memory	1 GB	2 GB	N/A
Minimum Available Disk Space	250 MB	1 GB	N/A

Downloading Software

1. Go to the LiveSecurity web site's Software Downloads page at http://www.watchguard.com/archive/softwarecenter.asp
2. Log in to the LiveSecurity web site. Then, select the product line you use and look for the Fireware XTM software download section.

There are several software files available for download. See the descriptions below so you know what software packages you will need for your upgrade.

All users can now download the WatchGuard System Manager software. With this software package you can install WSM and the WatchGuard Server Center software:

- `WSM11s.exe` - Use this file to install WatchGuard System Manager v11.0.
- `WSM11_0_2.exe` - Use this file to upgrade WatchGuard System Manager from v11.0 or v11.0.1 to WSM v11.0.2. This is a partial installer. You must have WSM v11.0 or v11.0.1 installed before you can install this file.

Select the correct Fireware XTM OS image for your hardware.

XTM 1050

- `XTM_OS_1050_11_0_2.exe`

Firebox X Core or Peak e-Series

- `XTM_OS_Core_Peak_11_0_2.exe`

If you want to downgrade a Firebox X Core or Peak e-Series from Fireware XTM v11.0.x to Fireware v10.2.x, you must download this file:

- `utm_core_peakdown2fw.zip`

Firebox X Edge e-Series

- `XTM_OS_Edge_11_0_2.exe` - Use this file to upgrade your Edge OS and configuration from v11.0 or v11.0.1 to Fireware XTM v11.0.2.
- `edge_11_0_2.exe` - Use this file to upgrade your Edge OS and configuration from v10.2.9 or higher to Fireware XTM.
- `XTM_edge_11.0_2.zip` - Use this file to upgrade your Edge OS from v10.2.9 or higher to Fireware XTM. No configuration conversion is possible if you use this file.

There are two files available for download if you use Single Sign-on:

- WG-Authentication-Gateway.exe (SSO Agent software - required for Single Sign-on)
- WG-Authentication-Client.msi (SSO Client software - optional)

For information about how to install and set up Single Sign-on, see the product documentation.

Upgrade from Fireware XTM v11.0 or higher to v11.0.2

Before you upgrade from Fireware XTM v11.0 or v11.0.1 to Fireware XTM v11.0.2, go to the WatchGuard Software Downloads Center. Download and save the file that matches the WatchGuard device you want to upgrade. You can use Policy Manager or the Web UI to complete the upgrade procedure.

From the Web UI:

1. On your management computer, launch the OS executable file you downloaded from the WatchGuard Software Downloads Center. This installation extracts an upgrade file called `utm_[Firebox_model].sysa-dl` to the default location of `C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.0\[Firebox_model].`
2. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
3. Browse to the location of the `utm_[Firebox_model].sysa-dl` file from Step 1 and click **Upgrade**.

From Policy Manager:

1. On your management computer, launch the OS executable file you downloaded from the WatchGuard Software Downloads Center. This installation extracts an upgrade file called `utm_[Firebox_model].sysa-dl` to the default location of `C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.0\[Firebox_model].`
2. Open WSM v11.0.2. Connect to your Firebox and launch Policy Manager.
3. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the `utm_[Firebox_model].sysa-dl` file from Step 1.

Installation and Upgrade Instructions for Firebox X Edge v10.2.9 or higher

Before you install Fireware XTM v11.0.2 software, read the information in the Known Issues section below.

Note To upgrade your Firebox X Edge e-Series to Fireware XTM from Edge v10.x or earlier, you must have Edge v10.2.9 or higher installed on your Edge.

Any Edge devices that are centrally managed with a WatchGuard Management Server must be updated individually using the process in these release notes. You cannot use the Scheduled Firmware Updates feature to update a device from Edge v10.x to Fireware XTM v11.0.x.

Upgrade your Firebox X Edge e-Series v10.2.9 or higher to Fireware XTM v11

Your Edge must have Firebox X Edge v10.2.9 or higher installed before you can upgrade to Fireware XTM v11.0.x. To upgrade your Edge, connect to your Edge from a Windows-based computer on a local (not routed) network behind the Edge on which you have administrator privileges. You can also upgrade your Edge from a computer on an external network (see the specific instructions below for more information).

The Update Wizard updates the operating system on your Edge and converts your Edge configuration to be compatible with Fireware XTM. The wizard converts all predefined and custom policies, security subscriptions, authentication settings, network settings, NAT settings, branch office VPNs, default threat protection settings, and logging and time settings. If you do not use the wizard (i.e. if you update directly from the v10.2.9 or higher web interface using the "sysa-dl" file), your configuration is not converted and your Edge reverts to its default configuration when the upgrade to Fireware XTM is complete.

Note The new Web UI is available only on port 8080 by default. You can change this port in the Web UI after you complete the Update Wizard. To connect to the Edge after it has been successfully updated, you must connect to the Edge with this URL:
https://<IP address of your Edge>:8080

Note The default credentials for the Edge are: admin/readwrite and status/readonly. After you upgrade your Edge to Fireware XTM, you must use the user name "admin" when you want to log in to the Edge with read/write privileges.

Note After you upgrade your Edge from v10.2.9 or higher to v11.0.2, you must enable each type of Mobile VPN that you used in your previous Edge configuration again. This includes Mobile VPN with IPSec, SSL, or PPTP.

Note When you upgrade an Edge to v11.0.2, the SSL VPN client software is not installed on the Edge by default. After you upgrade to v11.0.2, you must load the SSL VPN clients manually. To install the clients manually:
1. Connect to your Edge with the Web UI and select **System > Upgrade OS**.
2. Browse to the location `C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.0.2\Edge`.
3. Select **vpn-data-11.0.2-armeb.wgpkg-dl** and choose **Upgrade**.
4. The SSL VPN client software is loaded to the Edge.

The Update Wizard does not convert some features. After you finish this procedure, examine your configuration for the following features, which are not converted by the Update Wizard:

- MAC access control lists
- Traffic Management
- VLANs
- Modem settings
- Mobile VPN with IPSec
- Mobile VPN with SSL

- Mobile VPN with PPTP
- SNMP
- Single Sign-On

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11.0.2 from a local Windows computer:

1. Connect to your Edge System Status page and select **Administration > Backup** to back up your existing Edge configuration file.
2. Run the `edge_11_0_2.exe` file you downloaded from the software download site. The Firebox X Edge Update Wizard starts.
3. Use the Firebox X Edge Update Wizard to load Fireware XTM v11.0.2 on your Edge and convert your configuration file to v11.0.2. This upgrade can take as much as 10 minutes. Do not disconnect the power to your Edge during the upgrade.
4. When the wizard is complete, you can connect to the Fireware XTM Web UI on your Edge with the URL https://<IP address of Edge>:8080.
5. If you want to use WSM and Policy Manager with your Edge, you must install WSM software. To install WSM, download the `WSM11s.exe` and the `WSM11_0_2.exe` files from the software download site.

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11 from a local non-Windows computer:

> ***Note*** If you upgrade your Edge to Fireware XTM from a non-Windows-based computer or from any computer using the XTM_edge_11_0_2.zip file, your Edge configuration will be reset to its factory default settings when the upgrade is complete.

1. Connect to your Edge System Status page and select **Administration > Backup** to back up your existing Edge configuration file.
2. Decompress the `XTM_edge_11_0_2.zip` file you downloaded from the software download site.
3. On the System Status page, click **Update**.
4. Click **Browse**. Find and select the `utm_edge.sysa-dl` file, then click **Open**.
5. Click **Update**. To complete the installation, you must restart the Firebox X Edge. When the update is complete the System Status page shows Fireware XTM v11_0_2.

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11 from a Windows computer on the external network:

To upgrade your Edge from a computer on the external network, you can use the same instructions as for a local Windows computer, except you must know:

- Before you try to upgrade the Edge, the Edge must be configured to allow WatchGuard System Manager (WSM) access. To enable WSM access, go to **Administration > WSM Access**.

- The Update Wizard prompts you for a WSM Access passphrase. The WSM Access passphrase is the configuration passphrase you set when you enable WSM access on the Edge.
- The upgrade can take as much as 20 minutes to complete.
- When the upgrade is complete, you can connect to the Edge from the external network only with WatchGuard System Manager or the CLI. To enable external connections from the Web UI, you must edit the WatchGuard Web UI policy with Policy Manager or the CLI.

Downgrade Firebox X Edge e-Series from Fireware XTM v11.0.x to v10.2.9

Before you downgrade a Firebox X Edge e-Series from Fireware XTM v11 to Firebox X Edge v10.2.9 or higher, go to the WatchGuard Software Downloads Center. Download and save the file that matches the version of Edge software to which you want to downgrade. You can use Policy Manager or the Web UI to complete the downgrade procedure.

From the Web UI:

1. Connect to your Edge System Status page and select **System > Upgrade OS**.
2. Browse to and select the `yakfw.sysa-dl` file that you saved. Click **Upgrade**. This restores the operating system version you selected. The Edge will reboot and become active with the v10.2.x configuration that was in use on the Edge immediately before the upgrade to v11.
   After the downgrade, make sure to use the correct URL to connect to the Edge device (a URL that does not specify port 8080).
3. You can also choose to restore the backup configuration file you saved before you upgraded to v11.

Installation and Upgrade Instructions for Firebox X Core/Peak v10.2.x

Before you install the WSM and Fireware XTM v11 software, read the information in the Known Issues section below.

> ***Note*** To upgrade your Firebox X Core or Peak e-Series to Fireware XTM v11 from an earlier version of Fireware, you must have Fireware v10.2.x installed on your Firebox.

Upgrade your Firebox X Core or Peak e-Series from Fireware to Fireware XTM v11.0.x

1. We strongly advise you to back up your current Fireware v10.2.x or higher system configuration before you upgrade. From Policy Manager, select **File > Backup** to back up your existing Fireware configuration file and Fireware image.
2. Close all other programs on your management computer.

3. It is not necessary to uninstall previous versions of WSM unless you have installed WatchGuard server software on your computer. If you have installed server software, uninstall WSM using these instructions:
   From the Windows Start Menu, select **Control Panel > Add/Remove Software** and uninstall your previous version of WSM. If you use any WatchGuard servers, select **No** when asked if you want to remove data from these servers. Make sure that you restart your computer to complete the uninstall process.
4. Launch `WSM11s.exe` and use the on-screen procedure to install the software. When you run the WSM v11 install program, select the options to install client software and the appropriate server software.
5. Launch `WSM11_0_2.exe` and use the on-screen procedure to install the software. When you run the WSM v11.0.2 install program, select the options to install client software and the appropriate server software.
6. After the `WSM11_0_2.exe` install program is complete, launch `XTM_OS_Core_Peak_11_0_2.exe` and use the on-screen procedure to install the software.
7. Open WSM v11 and select **File > Connect to Device**. The **Connect to Firebox** dialog box appears. In the **Name/IP address** text box, type the IP address of your Firebox. Click **OK**.
8. Launch Policy Manager. Click **Yes** when prompted to upgrade to v11.
9. Click **Yes** to convert the configuration file to v11.
10. From Policy Manager, select **File > Upgrade**.
11. When the **Save** dialog box appears, click **Save**. Click **Yes** to save the file to your management computer.
12. When the Upgrade dialog box appears, type your configuration passphrase and click **OK**.
13. Click **OK**.
    The default path is C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.0\Core_Peak\ FW1100BNNNNNN.wgu where "NNNNNN" is the release build number.
14. Click **OK**.
15. Click **Yes** to upgrade your Firebox now.
16. Click **Yes** when asked to create a Firebox backup image.
17. Type an encryption key to encrypt the backup file. Click **OK**.
    If you get an error, click OK or Cancel and continue with the procedure.

When the backup and upgrade are finished, the Firebox reboots.

Downgrade your Firebox X Core/Peak e-Series from Fireware XTM v11.0.x to Fireware v10.2.x

To downgrade from Fireware XTM to Fireware, you must download a special downgrade file from the software downloads page. The file is called `utm_core_peakdown2fw.zip` and downgrades your device to Fireware v10.2.8. Once your Firebox is downgraded to v10.2.8,

you can then restore your Fireware configuration, or upgrade to v10.2.9 or higher and try the upgrade to Fireware XTM again.

1. Before you downgrade your Firebox X Core or Peak e-Series from Fireware XTM v11 to Fireware v10.2.8, you must browse to the WatchGuard Software Downloads page. Download and save the `utm_core_peakdown2fw.zip` file and extract the contents to your WSM management computer. Then:
2. Open WSM v11. Connect to your Firebox and launch Policy Manager.
3. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the `utm_core_peakdown2fw.sysa-dl` file that you saved.

During the downgrade procedure, the Storage LED on the front of the Firebox will blink rapidly. When the downgrade procedure is complete, the Firebox will start v10.2.8 with the configuration file you had before the upgrade to v11. The version number appears as "10.2.8dwn" to indicate that it is a downgrade. We recommend that you restore your previous v10.2.x backup after you downgrade from v11, or install any released v10.2.x operating system before you perform another upgrade to v11.

Upgrade HA to FireCluster

WSM v11 includes a HA upgrade wizard to help you upgrade the software on both your HA devices so you can enable FireCluster. With FireCluster, you can choose to configure your two devices in an active/passive cluster or an active/active cluster. Before you begin the upgrade process, we strongly recommend that you connect to the online help at http://www.watchguard.com/help/docs/wsm/11/en-US/index.html and read the chapter about FireCluster. There are important differences in license requirements and network integration you must understand before you implement FireCluster. Note that the HA upgrade wizard helps you to update the OS on your HA devices. You must reconfigure the devices for FireCluster manually when the upgrade is complete.

If you are in routed mode and have HA enabled in your Fireware v10.2.x configuration file, WSM launches the HA Upgrade Wizard automatically when you select **File > Upgrade** from Policy Manager. The Wizard upgrades the OS on your first HA device, then puts it in a factory-default state until the second HA box is updated. The Wizard then prompts you to upgrade your second device.

Now, you can connect to the second HA device with WSM Policy Manager and select **FireCluster > Setup**. The FireCluster Setup Wizard will launch to help you enable and configure your FireCluster. When you complete the Setup Wizard, you must save your configuration to the active device. Then, you must reboot both devices in your FireCluster.

As with High Availability in Fireware v10.x, you cannot enable FireCluster if any external interface is configured to use DHCP or PPPoE.

Resolved Issues

The Fireware XTM v11.0.2 release resolves a number of problems found in earlier Fireware XTM v11.0.x releases.

General

- The Fireware XTM OS installer now installs SNMP MIB files in `C:\Documents and Settings\All Users\Shared WatchGuard\SNMP`. [40283]
- Time zones using GMT -1 now operate correctly. [39984]
- The on-demand report "Top Client by Send and Received" now runs correctly. [40652]
- The Quarantine Server **Email Notification** text box now allows more than 32 characters. [40339]
- Firebox System Manager no longer displays Trial Subscription Service licenses as "unlicensed." [40005]
- This release resolves an issue that caused incorrect time on the Firebox X Edge e-Series (up to 15 minutes a day). [40099]
- You can now enable logging for traffic sent from the Firebox. The new logging option is available in Policy Manager under **Setup > Logging > Diagnostic Log Level > Turn on logging of traffic sent by the Firebox itself**. [40066]

Authentication

- The Active Directory server optional settings now apply to Mobile VPN with IPSec clients. [33083]
- This release resolves an issue in which an Authentication Redirect loop occurred when the same user had multiple authenticated sessions to the Firebox from the same IP address and one of the sessions was terminated by the Firebox. [39739]
- When you use Active Directory authentication with *userPrincipalName* or *sAMAccountName* for the **Login Attribute** and a *Searching User* configured, the Firebox no longer allows authentication attempts to succeed with invalid usernames. [40386]

Proxies

- The `spamd` process no longer restarts when you make changes to your spamBlocker settings. [39893]

Networking

- 1-to-1 NAT configured from an optional network to an external network now works correctly. [40025]
- The ARP Spoof Attack threshold has been increased to prevent false detection of ARP spoof attacks from Linux servers using multiple NIC cards on the same subnet (also known as ARP flux). [40122]

Multi-WAN

- This release resolves an issue that caused the Firebox to reboot every 2 minutes when multi-WAN is configured in round-robin mode. [40038]
- This release resolves an issue that prevented an external interface from becoming active again after ping or TCP interface monitoring failed. [40682]
- Multi-WAN interfaces configured with dynamic IP addresses now respond correctly to ping packets and management connections. [39870]
- The Firebox no longer routes traffic out all external interfaces when you select only one external interface in your multi-WAN Routing Table configuration. [39968]
- The method to determine Multi-WAN sticky connections has been improved to look at both the destination IP address and the source IP address. [39970]
- This release resolves an issue that caused the WAN Fail Back button to appear in FSM even though the WAN failback had already occurred. [38722]
- When you configure multi-WAN interface monitoring by domain name, the Firebox now does a DNS lookup after the first failed TCP or ping probe. [40578]

FireCluster

- You can now connect to the Management IP address of the Backup Master Firebox or Passive Firebox from a trusted or optional interface when the Management IP address is on an external interface. [40372]
- When you configure an Active/Passive FireCluster, you no longer need to have active security subscriptions licenses on the Passive Firebox. [40096]

Branch Office VPN

- Fireware XTM now includes the ability to configure inbound dynamic NAT in a branch office VPN tunnel. [40027]
- You can now configure BOVPN tunnel Phase 2 encryption settings as "Null". [38176]
- The Web UI now allows you to configure BOVPN tunnel settings, and set the Phase 2 key expiration lifetime to "0". [39869]
- You can now enable 1-to-1 NAT for a BOVPN tunnel when the tunnel direction is set to incoming. [40103]

Mobile VPN

- When you use individual users in a Mobile VPN with IPSec policy, Fireware XTM no longer limits the connection to the first user in the policy. [40114]
- When the idle timeout is reached for a Mobile VPN connection, Fireware XTM now correctly disconnects the user. This allows the client to re-connect and pass traffic. This issue applies to Mobile VPN with PPTP, IPSec, and SSL. [40497] [40529]
- PPTP connections are no longer disconnected when you modify a static NAT configuration. [39774]

Web UI

- When a licensed feature is expired, the Web UI now shows the feature as expired instead of showing a negative number. [40537]

- You can now use the Web UI to configure a DNS server for the DHCP settings of a wireless guest account. [39980]
- You can now configure MAC Address Override for an external interface. [40012]

Policy Manager

- When you edit a Traffic Management action associated with a firewall policy, the selected Traffic Management action no longer resets to "Defaults (No Limits)". [39586]
- When you configure policy-based routing for a VLAN that is configured on an external interface, Policy Manager now shows the correct configuration. [39491]

Management Server

- When FireCluster is configured on a managed device and then disabled, the Management Server now correctly shows the device as not having FireCluster enabled. [39875]
- The Management Server Setup Wizard no longer imports the external secondary IP addresses. [40242]
- When a **Scheduled OS Update** is in process and the Management Server tries to update a remote device that is not available, the update now times out after 60 seconds to prevent delaying the rest of the device OS updates. [39771]
- The **Cleanup Tasks** option no longer removes tasks that are still active or in the scheduled state. [39874]
- The Scheduled Feature Key Synchronization wizard now remembers the previously selected devices. [39873]
- The Scheduled Feature Key Synchronization feature now shows only supported devices. [39872]
- When you drag a device onto a Policy Template to change its configuration mode from *basic management* to *full management*, a "Login Failure" error no longer occurs. [40108]
- When you use role-based administration, a user with *Device Monitor* privileges can no longer remove a managed BOVPN tunnel. [40236]
- When a managed device has never contacted the Management Server, the update status for that device now shows as "Pending" instead of "Complete (Jan 01, 1970 08:00:00)". [39786]

Upgrade from version 10.2.x Issues

- When you upgrade from Edge v10.2.9 or higher, custom policies are now correctly shown in the XTM Custom Folder. [40489]
- This release resolves an issue in which WatchGuard System Manager was not able to connect to a Firebox X Core or Peak e-Series device after you upgraded from v10.2.x to v11.0.1 when PPTP was enabled. [39981]

Known Issues and Limitations

These are known issues for Fireware XTM v11.0.x and all management applications. Where available, we include a way to work around the issue.

General

- The minimum recommended screen resolution for all WatchGuard System Manager applications and the Fireware XTM Web UI is 1024x768.
- If your Firebox X Edge e-Series device is connected to a modem, it may not boot correctly if you try to set your Edge to its factory default settings. [30284]
- When you use the **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. [35450]
- In Fireware XTM v11.x, the Blocked Ports feature applies to all network interfaces. In Fireware and Edge v10.x, blocked ports applied only to traffic on the external interface. [39918]

Upgrade Issues

- After you upgrade a Firebox X Edge, it is important to know that you must use the user name "admin" when you want read/write access to the Edge. In versions older than v11.0 of Edge appliance software, you could use a name other than "admin" in your administrative credentials, but this is no longer possible in Fireware XTM. You must log in to the Edge with the user name "admin" and the read/write passphrase you set during the upgrade.
- If you upgrade to Fireware XTM from an earlier version of Fireware and used a branch office VPN Phase 2 encryption setting of **None**, this setting is not correctly converted during the configuration upgrade. You must edit your Phase 2 encryption setting manually when the upgrade is complete to select an appropriate encryption setting.
- If you have special characters (, ;) in the policy names of your v10.x configuration, you must remove them from your policy names after you upgrade to Fireware XTM v11 so that reporting and monitoring operate correctly. [36577]
- In WSM v10.x, you could create a Traffic Management action that set both incoming and outgoing traffic bandwidth for an external interface. This action could operate on a policy that managed traffic to and from a trusted network. To reproduce this feature in Fireware XTM v11, you must create a Traffic Management action that sets the maximum upload speed on the external interface and the maximum download speed on the trusted interface.
- Fireware XTM includes a new standard TFTP packet filter option. If your v10.2.x configuration file had a custom packet filter named "TFTP," you cannot save changes to your configuration after your upgrade until you delete your custom packet filter and move the policy configuration to a standard TFTP policy template. [39817]
- The Firebox X Edge **Require user authentication** and **Trusted Hosts** features do not exist in Fireware XTM, because of the increased granularity available when you configure policies for Edge users. During the Edge upgrade, the users are added to

a local group called *Local-Users*. If you previously had **Require user authentication** enabled, you must use this group in your policies to enforce user authentication. The **Trusted Hosts** feature is no longer necessary.

- The DNS suffix and second DNS server entries are not converted when you upgrade from v10.2.x to v11.0.x on Firebox X Edge e-Series. [40774]

> **Workaround:**
>
> Add the DNS suffix and second DNS entries again after you upgrade to v11.0.x.

WatchGuard System Manager

- The WSM Quick Setup Wizard does not allow you to enter a feature key that contains a model upgrade for Edge e-Series. [40405]

> **Workaround:**
>
> Do not enter the feature key in the Quick Setup Wizard. You can complete the wizard with no feature key, and the Edge will be configured in "limited access mode". When the Quick Setup Wizard is done, you can connect to the Edge with either Policy Manager or the Web UI and enter the feature key that contains the model upgrade.

- Remote managed Firebox devices configured in drop-in mode may not be able to connect to a Management Server that is behind a gateway Firebox also configured in drop-in mode. [33056]
- If you restore a backup image to a managed client device managed by a Management Server, it is possible that the shared secret becomes out of sync.

> **Workaround:**
> Connect to the Management Server from WSM. Select the managed device and select **Update Device**. Select the radio button **Reset server configuration (IP address/ Hostname, shared secret)**.

- If you use more than 28 characters in a proxy policy name, the Firebox becomes unresponsive. [40679]
- You cannot uninstall WatchGuard System Manager successfully when the WatchGuard Server Center is running on a computer using 64-bit Windows Vista. [39078]

> **Workaround:**
>
> Exit the WatchGuard Server Center before you start the uninstall WSM. You can then uninstall WatchGuard System Manager successfully.

Web UI

- The Fireware XTM Web UI does **not** support the configuration of some features. These features include:
  - FireCluster
  - Full proxy configuration options

- The editing of static NAT rules
- Manual policy precedence
- Certificate export
- You cannot enable diagnostic logging or change diagnostic log levels
- You cannot turn on or off notification of BOVPN events
- You cannot add or remove static ARP entries to the device ARP table
- You cannot save a device configuration file to your local computer
- You cannot get the encrypted Mobile VPN with IPSec end-user configuration profile, known as the `.wgx` file. The Web UI generates only a plain-text version of the end-user configuration profile, with file extension `.ini`.
- You cannot edit the name of a policy, use a custom address in a policy, or use *Host Name (DNS lookup)* to add an IP address to a policy.

- If you configure a policy in the Web UI with a status of **Disabled**, then open Policy Manager and make a change to the same policy, the action assigned to the policy when it denies packets is changed to **Send TCP RST**. [34118]
- If you use the Web UI to edit an existing proxy policy that has alarm settings enabled, the alarm settings may be disabled when you save your configuration. [38585]
- You cannot create read-only Mobile VPN with IPSec configuration files with the Web UI. [39176]
- You cannot use angle brackets "< or >" in the Admin or Status password or login fails. [40823]

WatchGuard Server Center

- If the WatchGuard Server Center is open when you uninstall WSM, you see multiple warning messages to close the application, instead of just a single warning. [36901]
- If the initial installation of the full WebBlocker database fails, subsequent partial updates fail because the complete database was not successfully downloaded. [40794]

> **Workaround**
>
> 1) Stop the WebBlocker Server if it is running**.**
>
> 2) Locate the file wbserver.ini in the location `C:\Documents and Settings\WatchGuard\wbserver`.
>
> 3) Change the *DatabaseDownload* value from 1 to 0 and save the file**.**
>
> 4) From the Server Center > WebBlocker Server > General Settings page, select **Download full database from the WatchGuard Server**.

Management Server

- You cannot log in to the Management Server if you have configured a managed device that has a device name that is the same as a user name configured with an "administrator" role on the Management Server. [39692]

- When a Firebox is in Full Management Mode, TCP SYN checking continues to occur when you clear the **Enable TCP Syn Checking** check box. [40853]

Command Line Interface (CLI)

- The CLI does not support the configuration of some features:
  - You cannot add or edit a proxy action.
  - You cannot get the encrypted Mobile VPN with IPSec end-user configuration profile, known as the `.wgx` file. The CLI generates only a plain-text version of the end-user configuration profile, with file extension `.ini`.
- The CLI performs minimal input validation for many commands.

Logging and Reporting

- LogViewer can freeze if you move the scroll bar very quickly. [39461]
- The LogViewer *Search* function is very slow when you search a large log database. [38833]
- If you use an IIS server to serve published reports, you must configure the IIS server to recognize .png file extensions or you get an error about missing files. For information on how to configure your IIS server to recognize .png file extensions, see http://www.libpng.org/pub/png/png-iis-config.html. [39319]
- If you restart the PostgreSQL database, you must also restart the Report Server and the Log Server. [35063]
- You cannot use a v11.0 Report Server with a v10.x Log Server. You must upgrade both servers for reporting to work correctly. You can, however, use v11.0 Report Manager with a v10.x Report Server.

Networking

- You cannot correctly add multicast addresses in a policy with Policy Manager or the Web UI. If you must use a multicast address in a policy, you must use the CLI to add the address. [39947, 39948]
- You must reboot your Firebox after you enable the MAC access control list or add a new MAC address before the change takes effect. [39987]
- You must make sure that any disabled network interfaces do not have the same IP address as any active network interface or routing problems can occur. [37807]
- If you enable the MAC/ IP binding feature by clicking the **Only allow traffic sent from or to these MAC/IP addresses** check box but do not add any entries to the table, the MAC/IP binding feature does not become active. This is to help make sure administrators do not accidently block themselves from their own Firebox. [36934]
- The option to release or renew a DHCP lease manually when the external interface is configured to use DHCP is missing in this release. [37478]
- Any network interfaces that are part of a bridge configuration disconnect and re-connect automatically when you save a configuration from a computer on the bridge network that includes configuration changes to a network interface. [39474]

- If you enable a network interface and change the **Interface Name (Alias)** at the same time you enable the interface, the interface does not become active until you reboot the Firebox. [39815]
- When you change the IP address of a VLAN configured on an external interface from static to PPPoE and the Firebox cannot get a PPPoE address, Firebox System Manager and the Web UI may continue to show the previously used static IP address. [39374]
- When you configure your Firebox with a Mixed Routing Mode configuration, any bridged interfaces show their interface and default gateway IP address as 0.0.0.0 in the Web UI. [39389]
- When you configure your Firebox in Bridge Mode, the LCD display on your Firebox shows the IP address of the bridged interfaces as 0.0.0.0. [39324]
- When you configure your Firebox in Bridge Mode, the HTTP redirect feature is configurable from the user interface but does not work in this release. [38870]
- Static MAC/IP address binding does not work when your Firebox is configured in Bridge mode. [36900]
- When your Firebox is configured to use Bridge mode, the physical interface of the Firebox does not appear correctly in log messages. Instead, the interface is represented as "tbrX". [36783]
- When you change your configuration mode from Mixed Routing to Bridge or from Bridge to Mixed Routing, the CLI and Web UI may continue to show the previous configuration mode. [38896]
- If you edit a static MAC entry and then change the MAC address, the change does not take occur. You must remove the original static MAC entry and add it again with the new MAC address. [40738]
- When you use multi-WAN, statically assigned DNS servers on WAN 1 cannot be used by the Firebox if other external interfaces use DNS servers from an ISP through PPPoE or DHCP. [40322]
- The dynamic routing of RIPv1 does not work. [40880]
- DHCP relay through a branch office VPN tunnel does not work. [40844]
- If you change the MTU of an external interface configured with PPPoE, the change does not take effect. The external interface continues to use the MTU value of 1492. [40705]

Wireless

- When you set the external interface as a wireless client and configure static NAT to use the eth0 interface as its source IP address, inbound static NAT does not operate correctly. [38239]
- The MAC Address Override feature is not available on a Firebox X Edge that has a wireless interfaced configured as an external interface. [38241]

FireCluster

- When you have an active/active FireCluster and use the WebBlocker Override feature, you may be prompted to enter your override password twice. [39263]

- Every network interface enabled in a FireCluster is automatically monitored by FireCluster. You must make sure that all enabled interfaces are physically connected to a network device.
- You cannot manage WatchGuard devices configured in a FireCluster through a branch office VPN tunnel. [39732]
- FireCluster is not supported if you use either a Drop-in or Bridge network configuration mode on your WatchGuard devices. [37287]
- If you use the Mobile VPN with IPSec client from the same network as the external network address configured on your FireCluster, some traffic may not go through the VPN tunnel. [38672]
- Mobile VPN with PPTP users do not appear in Firebox System Manager when you are connected to a passive FireCluster member, PPTP is only connected to the active Firebox when using Active / Passive. [36467]
- FireCluster does not support dynamic routing. [39442]
- When you configure an Active /Passive FireCluster, the Firebox does not send a GARP for 1-to-1 NAT IP addresses that are not configured as secondary network addresses on an external interface. [40688]

Authentication

- The Active Directory search algorithm has changed in Fireware XTM. For Active Directory authentication to work correctly in Fireware XTM v11.0.x, the groups that your users are members of must be included in the Search Base you specify in the Active Directory authentication setup. In Fireware v10.2.x and earlier, it was necessary for only the user objects to be in the Search Base. [40482]

  Workaround:

  If the Search Base that you currently use contains user objects but not the groups that the users are members of, make the Search Base broader. For example, use the root container dc=domain,dc=domain, as in dc=mycompany,dc=com.

- For the Authentication Redirect feature to operate correctly, HTTP or HTTPS traffic cannot be allowed through an outgoing policy based on IP addresses or aliases that contain IP addresses. The Authentication Redirect feature operates only when policies for port 80 and 443 are configured for user or user group authentication. [37241]
- The Authentication Redirect feature captures traffic sent between networks on the same interface. [39737]

Workaround:

Add an HTTP policy or HTTPS policy that matches the flow of traffic for which you do not want the auto-redirect to occur.
For example: After you enable the redirect feature, you want users on a secondary network of an interface to get to an internal web page hosted on a server on the primary network of the interface without having to authenticate. You can add a policy with the secondary network IP address in the **From** field and the primary network IP address in the **To** field.

Proxies

- Subscription services do not update correctly when you use an internal HTTP proxy server. [40517]
- When you enable IPS in POP3 proxy policies and a file is blocked by IPS, the resulting notification does not include the file name for the blocked file. [38087]
- Microsoft Outlook communication using RPC over HTTPS fails when you have deep packet inspection enabled in your HTTPS proxy. [37503]

  Workaround:

  Add Microsoft Exchange in your HTTPS proxy exception list.
- You cannot make a SIP-based call from Polycom PVX softphone behind a Firebox to a Polycom PVX on the external network. [38567]

  Workaround:

  You can use the H.323 protocol instead of SIP.

Security Subscriptions

- The AntiVirus engine used in Fireware XTM v11.0.2 has been updated to provide for faster downloads of signature definition updates. All WatchGuard XTM 1050 devices must be upgraded to v11.0.2 to continue to receive the latest signature updates after November 1, 2009. Firebox X e-Series devices (Edge, Core, and Peak) that run Fireware XTM v11.0 or v11.0.1 must upgrade to v11.0.2 or a later version to continue to receive updates after January 31, 2010.
- To optimize performance of web browsing on the Firebox X Edge e-Series, Gateway AntiVirus does not scan the following content types when used with the HTTP proxy: text/*, image/*, audio/*, video/*, application/javascript, application/x-javascript, and application/x-shockwave-flash. The content types appear in the HTTP-Client proxy action configuration for the Edge, but Gateway AV does not scan for these content types. All other content types, including executable files, are scanned. Gateway AntiVirus also does not use code emulation capabilities of the AV engine on Firebox X Edge e-series appliances.

Certificates

- You cannot import a CRL in DER format into Firebox System Manager. You must convert the CRL from DER to an acceptable format before you import the CRL into Firebox System Manager. [36643]

- DSA algorithm-based digital certificates are not supported in this release. [38758]

  Workaround:

  Use RSA algorithm-based digital certificates.

Mobile VPN with SSL

- If you change your SSL configuration from **Routed Network Traffic** to **Bridge Network Traffic**, you must restart your Firebox before the configuration change occurs. [36159]
- The Macintosh SSL VPN client may not be able to connect to a Firebox when the authentication algorithm is set to SHA 256. [35724]
- If your Firebox X Edge e-Series is set to factory-default mode when you install Fireware XTM v11.0, the Mobile VPN client software is not available for download from the Edge. You must upload the v.11.x utm_edge.sysa-dl again to restore the SSLVPN clients. [33539]
- When the Macintosh SSL VPN client disconnects or is stopped manually, the client disables the AirPort wireless adapter on the Mac. [39914]

Mobile VPN with IPSec

- A continuous FTP session over a Mobile VPN with IPSec connection could get terminated if an IPSec rekey occurs during the FTP transfer. [32769]

  Workaround:

  Increase the rekey byte count.

- When you use the Web UI or CLI to configure Mobile VPN with IPSec user profiles, user groups with extended authentication may show incorrectly as Firebox Local Authentication groups. [39695]
- If you have an underscore "_" in the group name, the Mobile VPN with IPSec connection does not pass traffic. [40858]

Mobile VPN with PPTP

- If the PPTP client option to **include Windows logon domain** is selected, the PPTP connection to the Firebox does not work. [40856]

Manual Branch Office VPN

- If the Mobile VPN with IPSec virtual IP address pool overlaps with the branch office VPN network, no traffic goes through the branch office VPN tunnel. [40974]
- The use of *Any* in a BOVPN tunnel route is changed in Fireware XTM. If a branch office VPN tunnel uses *Any* for the Local part of a tunnel route, Fireware XTM interprets this to mean network 0.0.0.0 and subnet mask 0.0.0.0 (in slash notation, 0.0.0.0/0). If the remote IPSec peer does not send 0.0.0.0/0 as its Phase 2 ID, Phase 2 negotiations fail. [40098]

Workaround:

Do not use *Any* for the Local or the Remote part of the tunnel route. Change the Local part of your tunnel route. Type the IP addresses of computers behind the Firebox that actually participate in the tunnel routing. Contact the administrator of the remote IPSec peer to determine what that device uses for the Remote part of its tunnel route (or the Remote part of its Phase 2 ID).

- The VPN Keep-Alive feature is not available for the Firebox X Edge e-Series. [37769]
- If you have a large number of branch office VPN tunnels in your configuration, the tunnels may take a long time to appear in Policy Manager. [35919]
- When you set the Phase 2 SA expiration to zero by setting both the Life-time and Life-size values to 0, the Firebox changes the rekey life-time to 8 hours. [37209]

Using the CLI

The Fireware XTM CLI (Command Line Interface) is fully supported for the v11.0.x release. For information on how to start and use the CLI, see the *CLI Command Reference Guide*. You can download the CLI guide from the documentation web site at www.watchguard.com/help/documentation.

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

Resolved Issues in Fireware XTM v11.0.1

- Automatic Gateway AV updates on the XTM 1050 now work correctly. [39878]
- Incoming connections that use a Static NAT rule in the To field of the policy no longer fail when your configuration also contains a matching 1-to-1 NAT rule. [39895]
- When you upgrade your Firebox X Edge e-Series to Fireware XTM, Dynamic NAT is now enabled for any non-RFC1918 addresses on the trusted or optional interface. [39919]

- Active Directory and LDAP authentication are now correctly enabled when you upgrade from v10.2.x to v11 and do not save the configuration to your device again. [39937]
- The Firebox X Edge MAC address override feature is now correctly converted during the Fireware XTM upgrade. [39950]
- You can now correctly add multiple managed BOVPN tunnels and gateways after you upgrade to Fireware XTM. [39958]
- After you upgrade a Firebox X Edge e-Series from v10.2.9 or higher, PFS is no longer disabled in the BOVPN tunnel settings. [39898]
- WebBlocker on a Firebox X Edge e-Series no longer shows the log message "http-proxy failed to send urif request to 'default'" and stops working after you upgrade to Fireware XTM. [39913]
- A problem that caused the Firebox to crash with log messages that include the text "webblocker@0x08048000" has been fixed. [39741]
- An issue that caused WebBlocker to stop working on Firebox X Core/Peak e-Series devices because of invalid WebBlocker exceptions after an upgrade to Fireware XTM has been fixed. [39892]
- WebBlocker no longer stops working correctly on a Firebox X Edge e-Series after you upgrade from v10.2.9 or higher if a custom WebBlocker server URL was used. [40004]