



Fireware XTM v11.7.5 Release Notes

Supported Devices	XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 XTMv, WatchGuard AP
Fireware XTM OS Build	451172
WatchGuard System Manager Build	<i>WatchGuard recommends you use WatchGuard System Manager v11.9 to manage Fireware XTM v11.7.5</i>
Revision Date	11 November 2014

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.7.5.

On June 5th the OpenSSL team released a critical update to patch six vulnerabilities affecting all versions of the OpenSSL libraries that are widely used in networking applications today. The most serious of the vulnerabilities is a Man-in-the-Middle (MitM) flaw that could allow an attacker to intercept traffic if both the client and server are vulnerable. This release includes the patch for both Fireware XTM OS and the Mobile VPN with SSL client to resolve the issue. Unlike the earlier Heartbleed vulnerability, no certificate updates are required once the patch is installed. More details about the vulnerabilities are posted at the [WatchGuard Security Center](#). If you are not already subscribed to this blog, we recommend that you sign up now to always stay current with breaking news about security vulnerabilities and any impact on WatchGuard products.

This release includes updated Fireware XTM OS and new Mobile VPN with SSL client software (v11.9.1) that include the OpenSSL patch. When your Mobile VPN with SSL users connect to a device running Fireware XTM v11.7.5, they will update automatically to the v11.9.1 SSLVPN client software.

This release also includes numerous bug fixes and minor feature updates. For more information on bug fixes, see the [Resolved Issues](#) section.

Before You Begin

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

- A supported WatchGuard XTM device. This device can be a WatchGuard XTM 2 Series (models 25 and 26 only), 3 Series, 5 Series, 8 Series, 800 Series, XTM 1050, XTM 1500 Series, XTM 2050 device, XTM 2500 Series, or XTMv (any edition).

- The required hardware and software components as shown below. If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware XTM OS installed on your XTM device and the version of WSM installed on your Management Server.
- Feature key for your XTM device — If you upgrade your XTM device from an earlier version of Fireware XTM OS, you can use your existing feature key. If you use XTMv, your feature key must be generated with the serial number you received when you purchased XTMv.

Note that you can install and use WatchGuard System Manager v11.7.x and all WSM server components with devices running earlier versions of Fireware XTM v11. In this case, we recommend that you use the product documentation that matches your Fireware XTM OS version.

If you have a new XTM physical device, make sure you use the instructions in the *XTM Quick Start Guide* that shipped with your device. If this is a new XTMv installation, make sure you carefully review the [XTMv Setup Guide](#) for important installation and setup instructions.

Product documentation for this product is available on the WatchGuard web site at www.watchguard.com/help/documentation.

Localization

This release includes an update to the localized management user interfaces (WSM application suite and Web UI) and product help. Both the user interfaces and product help have been updated with content for Fireware XTM v11.7.2. Supported languages are:

- Chinese (Simplified, PRC)
- French (France)
- Japanese
- Spanish (Latin American)



In addition to these languages, we offer localized Web UI support for Korean and Traditional Chinese. Only the Web UI itself has been localized. WSM, and all help files and user documentation, remain in English for these two languages.

Note that most data input must still be made using standard ASCII characters. You can use non-ASCII characters in some areas of the UI, including:

- Proxy deny message
- Wireless hotspot title, terms and conditions, and message
- WatchGuard Server Center users, groups, and role names

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the Web UI System Status menu and any software components provided by third-party companies remain in English.

Fireware XTM Web UI

The Web UI will launch in the language you have set in your web browser by default. The name of the currently selected language is shown at the top of each page. To change to a different language, click the language name that appears. A drop-down list of languages appears and you can select the language you want to use.

WatchGuard System Manager

When you install WSM, you can choose what language packs you want to install. The language displayed in WSM will match the language you select in your Microsoft Windows environment. For example, if you use Windows 7 and want to use WSM in Japanese, go to Control Panel > Regions and Languages and select Japanese on the Keyboards and Languages tab as your Display Language.

WebCenter, Quarantine Web UI, and Wireless Hotspot

These web pages automatically display in whatever language preference you have set in your web browser.

Fireware XTM and WSM v11.7.5 Operating System Compatibility

Last revised August 2013 - there are no changes with the release of v11.7.5

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit) & Vista (32 &64-bit)	Microsoft Windows 7 and 8 (32-bit & 64-bit)	Microsoft Windows Server 2003 SP2 (32-bit)	Microsoft Windows Server 2008 & 2008 R2	Microsoft Windows Server 2012 (64- bit)	Mac OS X v10.5, v10.6, & v10.7, v10.8	Mobile Devices: Android 4.x & higher, iOS
WatchGuard System Manager Application	✓	✓	✓	✓	✓		
Fireware XTM Web UI <i>Supported Browsers: IE 7, 8, 9, Firefox 3.x & above</i>	✓	✓	✓	✓	✓	✓	
WebCenter Web UI <i>Supported browsers: Firefox 3.5 & above, IE8 & above, Safari 5.0 & above, Chrome 10 & above. Javascript required.</i>	✓	✓	✓	✓	✓	✓	
WatchGuard Servers	✓	✓	✓	✓	✓		
Single Sign-On Agent Software (Includes Event Log Monitor)			✓	✓	✓		
Single Sign-On Client Software	✓	✓	✓	✓	✓		
Terminal Services Agent Software*			✓	✓	✓		
Mobile VPN with IPsec Client Software	✓	✓				✓ **	✓ **
Mobile VPN with SSL Client Software	✓	✓	✓			✓	✓

Notes about Microsoft Windows support:

- For Microsoft Windows Server 2008, we support both 32-bit and 64-bit support. For Windows Server 2008 R2, we support 64-bit only.
- Windows 8 support does not include Windows RT.

Browser compatibility:



- *Fireware XTM Web UI is supported on IE 7, 8, and 9, and Firefox 3.x and above.*
- *WebCenter Web UI is supported on IE 8 and above, Firefox 3.5 and above, Safari 5.0 and above, and Chrome 10 and above. Javascript is required.*















































** Terminal Services support with manual or Single Sign-On authentication operates in a Microsoft Terminal Services or Citrix XenApp 4.5, 5.0, 6.0 and 6.5 environment.*

*** Native (Cisco) IPSec client is supported for Mac OS and iOS.*

Authentication Support

This table gives you a quick view of the types of authentication servers supported by key features of Fireware XTM. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your XTM device configuration. With each type of third-party authentication server supported, you can specify a backup server IP address for failover.

 Fully supported by WatchGuard customers  Not yet supported, but tested with success by WatchGuard customers

	Active Directory ¹	LDAP	RADIUS ²	SecurID ²	Firebox (Firebox-DB) Local Authentication
Mobile VPN with IPSec/Shrew Soft			 ³	–	
Mobile VPN with IPSec for iPhone/iPad iOS and Mac OS X					
Mobile VPN with IPSec for Android devices				–	
Mobile VPN with SSL for Windows			 ⁴	 ⁴	
Mobile VPN with SSL for Mac					
Mobile VPN with L2TP	 ⁶	–		–	
Mobile VPN with PPTP	–	–		N/A	
Built-in Authentication Web Page on Port 4100					
Windows Single Sign-On Support <i>(with or without client software)</i>		–	–	–	–
Terminal Services Manual Authentication					
Terminal Services Authentication with Single Sign-On	 ⁵	–	–	–	–
Citrix Manual Authentication					
Citrix Manual Authentication with Single Sign-On	 ⁵	–	–	–	–

1. *Active Directory support includes both single domain and multi-domain support, unless otherwise noted.*
2. *RADIUS and SecurID support includes support for both one-time passphrases and challenge/response authentication integrated with RADIUS. In many cases, SecurID can also be used with other RADIUS implementations, including Vasco.*
3. *The Shrew Soft client does not support two-factor authentication.*
4. *Fireware XTM supports RADIUS Filter ID 11 for group authentication.*
5. *Both single and multiple domain Active Directory configurations are supported. For information about the supported Operating System compatibility for the WatchGuard TO Agent and SSO Agent, see the current Fireware XTM and WSM Operating System Compatibility table.*
6. *Active Directory authentication methods are supported only through a RADIUS server.*

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Minimum CPU	Intel Pentium IV 1GHz	Intel Pentium IV 2GHz
Minimum Memory	1 GB	2 GB
Minimum Available Disk Space	250 MB	1 GB
Minimum Recommended Screen Resolution	1024x768	1024x768

XTMv System Requirements

With support for installation in both a VMware and a Hyper-V environment, a WatchGuard XTMv virtual machine can run on a VMware ESXi 4.1 or 5.0 host, or on Windows Server 2008 R2, Windows Server 2012, Hyper-V Server 2008 R2, or Hyper-V Server 2012.

The hardware requirements for XTMv are the same as for the hypervisor environment it runs in.

Each XTMv virtual machine requires 3 GB of disk space.

Recommended Resource Allocation Settings

	Small Office	Medium Office	Large Office	Datacenter
Virtual CPUs	1	2	4	8 or more
Memory	1 GB	2 GB	4 GB	4 GB or more

Downloading Software

To download software:

1. Go to the WatchGuard [Software Downloads](#) page.
2. Select the Firebox or XTM device for which you want to download software.

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

WatchGuard System Manager

There are no updates to WSM available with this release. You must use WatchGuard System Manager v11.8 or higher to manage Fireware XTM v11.7.5.

Fireware XTM OS

Select the correct Fireware XTM OS image for your XTM device. Use the .exe file if you want to install or upgrade the OS using WSM. Use the .zip file if you want to install or upgrade the OS using the Fireware XTM Web UI. Use the .ova file to deploy a new XTMv device.

If you have....	Select from these Fireware XTM OS packages
XTM 2500 Series	XTM_OS_XTM800_1500_2500_11_7_5.exe xtm_xtm800_1500_2500_11_7_5.zip
XTM 2050	XTM_OS_XTM2050_11_7_5.exe xtm_xtm2050_11_7_5.zip
XTM 1500 Series	XTM_OS_XTM800_1500_2500_11_7_5.exe xtm_xtm800_1500_2500_11_7_5.zip
XTM 1050	XTM_OS_XTM1050_11_7_5.exe xtm_xtm1050_11_7_5.zip
XTM 800 Series	XTM_OS_XTM800_1500_2500_11_7_5.exe xtm_xtm800_1500_2500_11_7_5.zip
XTM 8 Series	XTM_OS_XTM8_11_7_5.exe xtm_xtm8_11_7_5.zip
XTM 5 Series	XTM_OS_XTM5_11_7_5.exe xtm_xtm5_11_7_5.zip
XTM 330	XTM_OS_XTM330_11_7_5.exe xtm_xtm330_11_7_5.zip
XTM 33	XTM_OS_XTM33_11_7_5.exe xtm_xtm33_11_7_5.zip
XTM 2 Series Models 25, 26	XTM_OS_XTM2A6_11_7_5.exe xtm_xtm2a6_11_7_5.zip
XTMv All editions for VMware	xtmv_11_7_5.ova xtmv_11_7_5.exe xtmv_11_7_5.zip
XTMv All editions for Hyper-V	xtmv_11_7_5_vhd.zip xtmv_11_7_5.exe xtmv_11_7_5.zip

Single Sign-On Software

For Single Sign-On (SSO) capability in a Windows Active Directory Domain. Agent requires the Microsoft .NET Framework v2.0–4.5 or later. There are two files available for download if you use Single Sign-On. These files have not been updated for this release.

- WG-Authentication-Gateway_11_7.exe (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- WG-Authentication-Client_11_7.msi (SSO Client software - optional)

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

Terminal Services Authentication Software

For User Authentication in Terminal Services or Citrix XenApp Environments.

- TO_AGENT_SETUP_11_7_4.exe (This installer includes both 32-bit and 64-bit file support and was been updated for the XTM v11.7.4 release.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL, both updated for this release. If you update your VPN clients through your XTM device, you do not need to download these files.

- WG-MVPN-SSL_11_9_1.exe (Client software for Windows)
- WG-MVPN-SSL_11_9_1.dmg (Client software for Mac)

Mobile VPN with IPSec client for Windows

With this release, we support the Shrew Soft VPN client for Windows v2.2, which you can download from our web site. Shrew Soft has released a v2.2.1 client, available on their web site, which introduces a new "Pro" version available at an extra cost with additional features. WatchGuard recommends you use the no-cost Standard version of the client as it includes all functionality supported in the v2.2 VPN client. If you want to use the v2.2.1 client, we recommend you read [this Knowledge Base article](#) first.

Upgrade from Fireware XTM v11.x to v11.7.x

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.7.x, download and save the Fireware XTM OS file that matches the WatchGuard device you want to upgrade. You can use Policy Manager or the Web UI to complete the upgrade procedure. We strongly recommend that you back up your device configuration and your WatchGuard Management Server configuration before you upgrade. It is not possible to downgrade without these backup files.

If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware XTM OS installed on your XTM device and the version of WSM installed on your Management Server.

Back up your WatchGuard Management Server Configuration

From the computer where you installed the Management Server:

1. From WatchGuard Server Center, select **Backup/Restore Management Server**.
The WatchGuard Server Center Backup/Restore Wizard starts.

2. Click **Next**.
The Select an action screen appears.
3. Select **Back up settings**.
4. Click **Next**.
The Specify a backup file screen appears.
5. Click **Browse** to select a location for the backup file. Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.
The WatchGuard Server Center Backup/Restore Wizard is complete screen appears.
7. Click **Finish** to exit the wizard.

General Information for WatchGuard Server Software Upgrades

It is not usually necessary to uninstall your previous v11.x server or client software when you update to WSM v11.7.x. You can install the v11.7.x server and client software on top of your existing installation to upgrade your WatchGuard software components.

If you use a Management Server, you must upgrade it from WSM v6.x or previous to WSM v11.7.x before you upgrade your XTM device.

Upgrade to Fireware XTM v11.7.x from Web UI

1. Go to **System > Backup Image** or use the USB Backup feature to back up your current configuration file.
2. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads Center.
If you use the Windows-based installer on a computer with a Windows 64-bit operating system, this installation extracts an upgrade file called `[xtm series]_[product code].sysa-dl` to the default location of `C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.7.5\[model] or [model] [product_code]`.
On a computer with a Windows 32-bit operating system, the path is: `C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.7.5`
3. Connect to your XTM device with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the `[xtm series]_[product code].sysa-dl` from Step 2 and click **Upgrade**.

Upgrade to Fireware XTM v11.7.x from WSM/Policy Manager v11.8.x or v11.9.x

1. Select **File > Backup** or use the USB Backup feature to back up your current configuration file.
2. On your management computer, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called `[xtm series]_[product code].sysa-dl` to the default location of `C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.7.5\[model] or [model][product_code]`.
3. Install and open WatchGuard System Manager v11.8 or higher. Connect to your XTM device and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the `[xtm series]_[product code].sysa-dl` file from Step 2.

Upgrade your FireCluster to Fireware XTM v11.7.x

There are two methods to upgrade Fireware XTM OS on your FireCluster. The method you use depends on the version of Fireware XTM you currently use.

Upgrade a FireCluster from Fireware XTM v11.4.x–v11.6.x to v11.7.x

Use these steps to upgrade a FireCluster from Fireware XTM v11.4.x, v11.5.x, or v11.6.x to Fireware XTM v11.7.x:

1. Open the cluster configuration file in Policy Manager
2. Select **File > Upgrade**.
3. Type the configuration passphrase.
4. Type or select the location of the upgrade file.
5. To create a backup image, select **Yes**.
A list of the cluster members appears.
6. Select the check box for each device you want to upgrade.
A message appears when the upgrade for each device is complete.

When the upgrade is complete, each cluster member reboots and rejoins the cluster. If you upgrade both devices in the cluster at the same time, the devices are upgraded one at a time. This is to make sure there is not an interruption in network access at the time of the upgrade.

Policy Manager upgrades the backup member first and then waits for it to reboot and rejoin the cluster as a backup. Then Policy Manager upgrades the master. Note that the master's role will not change until it reboots to complete the upgrade process. At that time the backup takes over as the master.

To perform the upgrade from a remote location, make sure the FireCluster interface for management IP address is configured on the external interface, and that the management IP addresses are public and routable. For more information, see [About the Interface for Management IP Address](#).

Upgrade a FireCluster from Fireware XTM v11.3.x

To upgrade a FireCluster from Fireware XTM v11.3.x to Fireware XTM v11.7.x, you must perform a manual upgrade. For manual upgrade steps, see the Knowledge Base article [Upgrade Fireware XTM OS for a FireCluster](#).

Downgrade Instructions

Downgrade from WSM v11.7.x to WSM v11.x

If you want to revert from v11.7.x to an earlier version of WSM, you must uninstall WSM v11.7.x. When you uninstall, choose **Yes** when the uninstaller asks if you want to delete server configuration and data files. After the server configuration and data files are deleted, you must restore the data and server configuration files you backed up before you upgraded to WSM v11.7.x.

Next, install the same version of WSM that you used before you upgraded to WSM v11.7.x. The installer should detect your existing server configuration and try to restart your servers from the **Finish** dialog box. If you use a WatchGuard Management Server, use WatchGuard Server Center to restore the backup Management Server configuration you created before you first upgraded to WSM v11.7.x. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.7.x to Fireware XTM v11.x



If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.7.x to an earlier version, the downgrade process resets the network and security settings on your XTM device to their factory-default settings. The downgrade process does not change the device passphrases and does not remove the feature keys and certificates.

If you want to downgrade from Fireware XTM v11.7.x to an earlier version of Fireware XTM, the recommended method is to use a backup image that you created before the upgrade to Fireware XTM v11.7.x. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.7.x to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device. This is not an option for XTMv users.

See the [WatchGuard System Manager Help](#) or the [Fireware XTM Web UI Help](#) for more information about these downgrade procedures, and information about how to downgrade if you do not have a backup image.



Some downgrade restrictions apply:

- You cannot downgrade an XTM 2050 or an XTM 330 to a version of Fireware XTM OS lower than v11.5.1.
- You cannot downgrade an XTM 25, 26, or 33 device to a version of Fireware XTM OS lower than v11.5.2.
- You cannot downgrade an XTM 5 Series model 515, 525, 535 or 545 to a version of Fireware XTM OS lower than v11.6.1.
- You cannot downgrade XTMv in a VMware environment to a version of Fireware XTM OS lower than v11.5.4.
- You cannot downgrade XTMv in a Hyper-V environment to a version of Fireware XTM OS lower than v11.7.3.

Resolved Issues

Fireware XTM v11.7.5 includes many resolved bugs and small enhancements, including:

General

- This release resolves multiple OpenSSL vulnerabilities, as identified in OpenSSL advisories: CVE-2014-0195, CVE-2014-0221, CVE-2014-0224, and CVE-2014-03470.
- Feature keys that contain more than 1024 characters are now correctly supported. [80403]
- The 10Gbps Fiber interface on the XTM 2050 now operates correctly after reboot or an interface down event. [77152]
- In this release, changes have been made to reduce the frequency of CPU stall checks and therefore increase stability.
- An issued that caused a process crash to occur after a WAN failover to a modem. [76448]
- The device kernel CPU lock behavior has been improved to prevent traffic disruption and increase system responsiveness. [69250]
- This release resolves an issue that prevented a managed XTM or Firebox from consistently contacting the Management Server when its lease expired. [78880]
- Firebox System Manager > Traffic Monitor now correctly displays log messages for email transactions that have non-ASCII characters in the email body. [70927]
- DHCP relay now operates correctly in a device configuration that uses VLANs. [73746,73246]
- A reported buffer overflow issue in the WGagent component, as referenced in CVE-2013-6021, has been addressed. [76752]
- The NETWORKD process no longer uses excessive CPU when your device is configured in bridge mode. [79604, 70574]

Proxies and Services

- An HTTPS proxy memory leak has been resolved. [77430]
- The HTTP proxy, enabled with WebBlocker with Websense, no longer stops passing traffic after a multi-WAN failover occurs. [77122]
- A problem that cause WebBlocker enabled web traffic to fail after an upgrade to Fireware XTM v11.7.4 for some customers has been resolved. [74595]
- With this release, the number of maximum connections for most device models has been increased to allow for high dynamic channel setup. [74313]
- spamBlocker now works correctly on XTM 15xx and 25xx device models. [76979]
- An issued that caused a Gateway AV scanning error "no text for this error code" that occurred when scanning large files has been resolved. [75868]

VPN

- This release resolves an issue that occurred during Phase 1 negotiation with a third-party IPSec device that caused a missing Phase 1 Security Association on the XTM device. [79260]
- A Branch Office VPN failover no longer occurs when one endpoint has a dynamic IP address and the VPN was configured with Command-Line Interface. [73506]
- This release resolves an issue that caused branch office VPN traffic to fail because the Global DNAT policy was incorrectly applied. [78840]
- A problem that caused a crash in the IKED process has been resolved. [75131]
- A kernel crash issue related to high BOVPN traffic has been resolved. [73505]

FireCluster

- This release resolves an issue that caused an interface to be incorrectly considered to be "down" and therefore incorrectly lowering the FireCluster health index. [77202]
- This release resolves several issues that caused an interface to get stuck in the "down" state after a FireCluster failover. [72916, 72904, 73159]
- This release includes several BOVPN stability improvements for FireCluster users. [74219, 71844, 71265, 71374]
- A FireCluster member no longer remains in the IDLE state when the member loses the Master election process. [78331]
- Load balancing now works correctly in an active/active FireCluster after the FireCluster forms. [76463]
- A log message is now correctly generated when a FireCluster failover occurs because of a failed Link Aggregation interface. [72763]
- An issue was resolved that caused a stack trace error "wgrelyad died unexpectedly on signal 6" and prevented a FireCluster failover. [73394]
- A kernel memory leak in a FireCluster backup member has been resolved in this release. [74628]

Known Issues and Limitations

You can find information about known issues for Fireware XTM v11.7.5 and its management applications, including workarounds where available, in the WatchGuard [Knowledge Base](#). Note that you must log in to the WatchGuard Portal to search for Known Issues. Known Issues are not available in the public version of the Knowledge Base. After you log in, you can use the filters available in the WatchGuard Portal > Knowledge Base tab to find articles about known issues for this release.



The screenshot shows a search interface with a search bar, a list of article types (Article, Known Issue, Software Downloads, Support Alerts), and a filter section for Products and Operating System. The 'Known Issue' checkbox is checked. There are 'Go', 'Clear Search', and 'Clear Filters' buttons.

Using the CLI

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

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at <http://www.watchguard.com/support>. When you contact Technical Support, you must supply your registered Product Serial Number 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