



## Fireware XTM v11.7 Release Notes

---

Supported Devices	XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 XTMv
Fireware XTM OS Build	359571
WatchGuard System Manager Build	362542
Revision Date	27 February 2013

## Introduction

---

### **Note**

*On 8 February, WatchGuard released an update to WatchGuard System Manager v11.7 to support three new XTM model families: XTM 800 Series, XTM 1500 Series, and XTM 2500 Series. WatchGuard System Manager v11.7 Update 1 replaces WatchGuard System Manager v11.7 in the WatchGuard Portal, and can seamlessly manage all XTM devices. Update 1 also fixes several WSM-related issues in the original WSM v11.7 release, as detailed in the Resolved Issues section. The v11.7 Release Notes have been updated to reflect the latest additions to the XTM family: XTM 800, 1500, and 2500 Series.*

WatchGuard is pleased to announce the release of Fireware XTM v11.7 and WatchGuard System Manager v11.7. You can install Fireware XTM OS v11.7 on most WatchGuard XTM devices, including 2 Series (models 25 and 26 only), 3 Series, 5 Series, 8 Series, XTM 1050, and XTM 2050 devices, and with any edition of XTMv.

WatchGuard XTM release v11.7 is not available for XTM 21, XTM 21-W, XTM 22, XTM 22-W, XTM 23, and XTM 23-W, nor the new XTM 800, 1500, and 2500 Series devices.

The new features, feature enhancements, and bug fixes included in this release have been carefully chosen to improve the efficiency, performance, and reliability of your XTM devices. In addition to these product enhancements, we are pleased to release a large number of bug fixes and smaller enhancements. For more information, see the [Resolved Issues](#) section. For detailed information about the feature enhancements included in Fireware XTM v11.7, see the product documentation or review [What's New in Fireware XTM v11.7](#).

## New features in Fireware XTM v11.7

### Policy Grouping

With Policy Grouping, you can create and apply tags to policies and then use the tags to easily filter the list of policies and streamline the number of policies in the policy list at one time. This is particularly helpful for users who have complicated device configuration files with many policies to manage. Policy tags are not available for devices running older versions of Fireware XTM OS (pre-v11.7) or for configuration files created for pre-v11.7 devices.

### **Link Aggregation**

You can now group your XTM device physical interfaces together to work as a single logical interface. With link aggregation, you can increase the cumulative throughput of your XTM device beyond the capacity of a single physical interface, and provide redundancy if there is a physical link failure.

### **WebBlocker Cloud Option with Websense**

New support for the Websense URL database in the cloud. Now, you can use the Websense cloud, with over 100 content categories and many new categories, as your WebBlocker Server. Or, if you prefer, you can continue to use a WebBlocker Server with the SurfControl database and 54 content categories. For new WebBlocker activations, the Websense cloud configuration is the default setting. When you upgrade to Fireware XTM v11.7, WebBlocker continues to use the previously configured WebBlocker server. After you upgrade, you can update the WebBlocker configuration to use the Websense cloud for WebBlocker lookups. When you switch between WebBlocker server options, the management software can automatically convert the currently blocked categories to similar categories in the other database.

### **WatchGuard Mobile VPN App for iOS and Android**

New apps make it easy for end users to build a VPN connection from iOS and Android devices. The administrator of the XTM appliance can securely email a file with the required configuration details, which the user can simply click to install the VPN profile after the app is installed. For Android, we now provide a WatchGuard client for Mobile VPN with IPSec. The WatchGuard VPN app for iOS operates with both Mobile VPN with IPSec and Mobile VPN with L2TP connections. The iOS app will be available in the Apple store later this month. The Android app will be available in the Google Play app store later this month as well.

### **Mobile VPN with L2TP**

Support for a new type of Mobile VPN connection - L2TP (Layer 2 Tunneling Protocol) v2, as described in RFC 2661.

### **IPS and Application Control Support in the HTTPS Proxy**

IPS and Application Control security subscriptions are now fully supported by the HTTPS proxy to allow the XTM device to scan for IPS and Application Control signatures on the decrypted HTTPS content stream.

Other new features include:

- **New web interface for CA Manager** - The CA Manager Web UI has moved to the Log and Report Manager Web UI. The combined web interface has been renamed to WebCenter.
- **New web UI to manage quarantined email messages** - New look and feel for the Web UI that email recipients use to see and manage their quarantined email messages.
- **Support for more than four external interfaces on your XTM device**
- **Hardware Health Monitoring** - Your XTM device now self-monitors the health of specific hardware areas and sends an email notification if it detects a problem in those areas.
- **FireCluster support with wireless devices** - You can now configure FireCluster for XTM 2 Series Models 25 and 26 Wireless and XTM 33 Wireless. Only active/passive mode is supported for wireless devices.

- **New DHCP options for VoIP support** - You can now configure your XTM device to support DHCP options 66, 67 and 150.
- **Per user/group and concurrent login support** - You can now set the number of concurrent, authenticated sessions you want to allow, and you can control this on a per user or per group basis.
- **Wireless Hotspot external authentication support** - You can optionally configure the wireless hotspot on the XTM device to redirect hotspot users to an external web server before they connect to the wireless network.
- **IPv6 enhancements** - We add support for IPv6 stateful firewalling for these networking and security features:
  - IPv6 host/network/address ranges in From and To lists in policies
  - IPv6 addresses in blocked sites and blocked site exceptions
  - Blocked ports applies to both IPv6 and IPv4 traffic
  - TCP SYN checking applies to both IPv6 and IPv4 traffic
- **Branch office VPN failover to modem** - If you have enabled serial modem failover on your XTM 25, 26, 3 Series, or 5 Series device, you can configure the branch office VPN to fail over to a modem if all external interfaces cannot connect.
- **Stream packet capture data to a file** - A new advanced option to stream packet capture data to a file.
- **Global Dynamic NAT enhancements** - When you configure a global dynamic NAT rule, you can now set the source IP address to use.
- **IPS Scan mode** - You can now select between two scan modes, Fast Scan and Full Scan. The default setting is Full Scan, which directs IPS to scan all packets. To improve performance, you can select Fast Scan, which directs IPS to scan fewer packets. Fast Scan mode greatly improves throughput for scanned traffic, with a slight drop in IPS effectiveness.
- **New Management Tunnels** - New support for remote XTM devices behind a NAT gateway.

## 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 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](http://www.watchguard.com/help/documentation).

## Localization

---

This release includes localized management user interfaces (WSM application suite and Web UI) and product help, but the localization has not yet been updated for features new to Fireware XTM v11.7. Supported languages are:

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

**Note** *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 Operating System Compatibility

Revised February 2013

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 and higher, iOS
<b>WatchGuard System Manager Application</b>	✓	✓	✓	✓	✓		
<b>Fireware XTM Web UI</b> <i>Supported Browsers: IE 7, 8, and 9, Firefox 3.x &amp; above</i>	✓	✓	✓	✓	✓	✓	
<b>WebCenter Web UI</b> <i>Supported browsers: Firefox 3.5 &amp; above, IE8 &amp; above, Safari 5.0 &amp; above, Chrome 10 &amp; above. Javascript required.</i>	✓	✓	✓	✓	✓	✓	
<b>WatchGuard Servers</b>	✓	✓	✓	✓	✓		
<b>Single Sign-On Agent Software (Includes Event Log Monitor)</b>			✓	✓	✓		
<b>Single Sign-On Client Software</b>	✓	✓	✓	✓			
<b>Terminal Services Agent Software*</b>			✓	✓	✓		
<b>Mobile VPN with IPsec Client Software</b>	✓	✓				✓ **	✓ **
<b>Mobile VPN with SSL Client Software</b>	✓	✓	✓			✓	

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

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

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

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. *Only single 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.*

## XTMv System Requirements

To install an XTMv virtual device, you must have a VMware ESXi 4.1 or 5.0 host installed on any server hardware supported by the ESXi version you use. You must also install the VMware vSphere Client 4.1 or 5.0 on a supported Windows computer. If you prefer, you can use vCenter Server instead of the vSphere client.

The hardware requirements for XTMv are the same as the hardware requirements for VMware ESXi. For information about VMware hardware compatibility, see the VMware Compatibility Guide at <http://www.vmware.com/resources/compatibility/search.php>.

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

1. Log in to the [WatchGuard Portal](#) and select the Articles & Software tab.
2. From the Search section, clear the Articles and Known Issues check boxes and search for available Software Downloads. Select the 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

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

`WSM11_7s.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.7 Update 1.

### 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 2050	<code>XTM_OS_XTM2050_11_7.exe</code> <code>xtm_xtm2050_11_7.zip</code>
XTM 1050	<code>XTM_OS_XTM1050_11_7.exe</code> <code>xtm_xtm1050_11_7.zip</code>
XTM 8 Series	<code>XTM_OS_XTM8_11_7.exe</code> <code>xtm_xtm8_11_7.zip</code>
XTM 5 Series	<code>XTM_OS_XTM5_11_7.exe</code> <code>xtm_xtm5_11_7.zip</code>
XTM 330	<code>XTM_OS_XTM330_11_7.exe</code> <code>xtm_xtm330_11_7.zip</code>
XTM 33	<code>XTM_OS_XTM33_11_7.exe</code> <code>xtm_xtm33_11_7.zip</code>
XTM 2 Series Models 25, 26	<code>XTM_OS_XTM2A6_11_7.exe</code> <code>xtm_xtm2a6_11_7.zip</code>
XTMv All editions	<code>xtmv_11_7.ova</code> <code>xtmv_11_7.exe</code> <code>xtmv_11_7.zip</code>



## Single Sign-On Software

There are two files available for download if you use Single Sign-On.

- 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

- TO\_AGENT\_SETUP.exe (This installer includes both 32-bit and 64-bit file support)

## Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL:

- WG-MVPN-SSL\_11\_7.exe (Client software for Windows)
- WG-MVPN-SSL\_11\_7.dmg (Client software for Mac)

## Mobile VPN with IPSec client for Windows

You can download the Shrew Soft VPN client for Windows from our web site. For more information about the Shrew Soft VPN client, see the help or visit the [Shrew Soft, Inc. web site](#).

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

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.7, 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.

**Note** You *MUST* uninstall WatchGuard System Manager v11.7 before you can install WatchGuard System Manager v11.7 Update 1. If you use a WatchGuard Management Server, you must upgrade your Management Server to v11.7 before you upgrade your XTM device to Fireware XTM v11.7.

## 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 necessary to uninstall your previous v11.x server or client software when you update from v11.0.1 or higher to WSM v11.7. You can install the v11.7 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 to WSM v11.7 before you upgrade your XTM device.

### Upgrade to Fireware XTM v11.7 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, 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\[model] or [model][product\_code].
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 from WSM/Policy Manager v11.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\[model] or [model][product\_code].
3. Install and open WatchGuard System Manager v11.7. 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

---

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

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:

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, 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 to WSM v11.x

If you want to revert from v11.7 to an earlier version of WSM, you must uninstall WSM v11.7. 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.

Next, install the same version of WSM that you used before you upgraded to WSM v11.7. 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. Verify that all WatchGuard servers are running.

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

**Warning** If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.7 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 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. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.7 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.

**Note** 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 to a version of Fireware XTM OS lower than v11.5.4.

## Resolved Issues

---

This release resolves a number of problems found in earlier Fireware XTM releases. While most of these issues referenced here were resolved in v11.7, we first include the list of issues resolved in WSM Update 1.

### Issues Resolved in WSM 11.7 Update 1

- After a fully managed XTM device is upgraded, the Management Server no longer crashes with an Apache process error "Error (10279), Error getting current revision information for device xxx (failure)". [71255]
- Fully managed devices connected to a v11.7 Management Server no longer experience configuration corruption when they are upgraded to XTM OS v11.6.3. [71304]
- This release resolves an issue that prevented WSM centralized management of devices running a version of Fireware XTM prior to v11.6. [70952]

- You can now add an IP address to the Blocked Sites list correctly from Firebox System Manager. *[70980]*
- A problem that prevented multiple configuration changes to configuration files for XTM devices running Fireware XTM v11.3.x through v11.5.x has been resolved. *[70983]*
- SIP ALG configuration settings are now correctly maintained when you upgrade to WSM v11.7. *[67504]*
- WatchGuard System Manager no longer crashes when you use a French Windows OS to connect to and manage a FireCluster. *[71074]*

## General

- WFS firmware component files and management applications are no longer bundled with WatchGuard System Manager. *[67508]*
- A problem that caused the XTM 1050 10 Gigabit Fiber ports to fail has been resolved. *[70118]*
- This release resolves a problem that caused a kernel crash when a reset packet is sent out through the 10 Gigabit Fiber ports on the XTM 1050 and XTM 2050. *[70384, 70296]*
- When an IP address is added to the Temporary Blocked Site list by the administrator through the Firebox System Manager > Blocked Sites tab, the expiration time is no longer reset when traffic is received from the IP address. *[42089]*

## Proxies and Subscription Services

- File downloads no longer stall when you use an HTTP packet filter policy with IPS. *[67659]*
- The SIP ALG now supports REFER method for call transfers. *[59635]*
- The IPS deny message contents have been improved. *[66839]*
- We have improved the scand daemon so that it restarts faster in the event of a crash.

## Logging and Reporting

- You can now show more than 5000 lines of log messages in Firebox System Manager. *[66518]*
- The contents of the XTM Configuration Report have been localized for both viewing and printing into all languages supported by the Fireware XTM Web UI. *[66546]*
- The behavior of the Report Server Maximum Database Size setting now matches that of the Log Server, and prevents the Report Server database from filling the disk partition. *[67245]*
- Log collector no longer crashes when it reaches the 2GB virtual size limit on 32-bit Windows systems. *[64249]*

## Networking

- If you manually created dynamic routing policies in Fireware XTM v11.5.x or earlier, the To and From lists in these policies are no longer cleared when you upgrade to v11.6 or v11.7. *[67721]*
- The SNMP process is now automatically restarted if it becomes stuck in a dormant state. *[66491]*
- The IGMP\_Max\_Membership setting for OSPF has been increased to support a large number of VLANs with dynamic routing. *[69979]*

## FireCluster

- This release resolves a problem that caused the master in an XTM 2050 FireCluster to go into an idle state when you added a new interface. *[70392]*
- The Terminal Services TO Agent now works correctly when used in an active/passive FireCluster. *[70098, 69944]*

## Wireless

- The 5GHz Wireless band now works correctly with channels 36, 40, 149 or 165. [65559]

## Authentication

- You can now set the number of concurrent, authenticated sessions you want to allow, and you can control this on a per user or per group basis. [61034, 60501]
- Firebox System Manager now correctly logs off SSO users when the client computer is physically disconnected. [64080]
- Domain local groups are now recognized with SSO for cross domain logons in multi-domain environments. [62662]
- You can now add multiple domain controller IP addresses when you set up clientless SSO. [64963]
- A problem with the Single Sign On client software that caused user group queries to fail has been resolved. [68363]
- Several problems that caused the SSO Agent to crash have been resolved. [67377, 68855, 68063]
- The Terminal Services TO Agent software has been optimized so it no longer uses large amount of CPU. [66057]
- It is no longer necessary to restart your server after you install Terminal Services TO Agent software. [59143]
- The Terminal Services TO Agent now works correctly when the NT domain name is different from the AD domain name. [69911]
- The Terminal Services TO Agent now works correctly when part of an active/passive FireCluster network environment. [70098]

## Branch Office VPN

- Managed BOVPN tunnels now include support for optional 1-to-1 NAT. [68244]
- The amount of time it takes to fail over from a leased line to a branch office VPN with OSPF or BGP has been reduced. [70460]

## Mobile VPN

- Frequent mobile VPN client log in/log out events no longer cause a low memory condition on the XTM device. [67538]
- When you use a native Cisco IPsec iOS client for Mobile VPN with IPsec, the client no longer disconnects after three minutes of idle time. [69430]
- If you set the diagnostic log level for Mobile VPN with SSL traffic to “debug” level, log messages now correctly display in Firebox System Manager > Traffic Manager. [65165]
- You can now correctly establish a Mobile VPN with SSL connection from a Windows-based computer when the Windows system account is Chinese. [58208]
- A continuous FTP session over a Mobile VPN with IPsec connection is no longer terminated if an IPsec rekey occurs during the FTP transfer. [32769]

## Known Issues and Limitations

---

These are known issues for Fireware XTM v11.7 and all management applications. Where available, we include a way to work around the issue.

## General

- The LCD display on XTM 800 Series, XTM 1500 Series, and XTM 2500 Series devices shows only nine interfaces. [71231]
- You can not use XTM 800, XTM 1500, or XTM 2500 Series devices with RapidDeploy. [71268]
- If you rename a policy tag from the policy settings configuration, the tag is removed instead of renamed. [70481]

### Workaround

You can rename a tag without this issue if you:

1. Right-click the policy table and select Policy Tags > Manage > Rename; or
2. Use View > Policy Tags > Manage > Rename.

- The "Sysb" version displayed in the Firebox System Manager Status Report will show blank for XTM 2, 5, 8, and 1050 devices that were manufactured prior to the XTM v11.5.1 release.
- When the level of free memory on your XTM device is lower than 20M, saving your XTM device configuration to the device can cause network disruption. [64474]
- To power off an XTM 5 Series device, you must press and hold the rear power switch for 4–5 seconds. [42459]
- For XTM 5 Series devices, Interface 0 does not support Auto-MDIX and does not automatically sense cable polarity.
- When you use the **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. [35450]
- Fireware XTM does not support BGP connections through an IPSec VPN tunnel to Amazon Web Services. VPN tunnels that do not use BGP are supported. [41534]
- The XTM Configuration Report does not contain all settings. Settings not included are:
  - Secondary interface IP address [66990]
  - Configured QoS settings [66992]
  - Static MAC bindings [66993]
  - IPv6 configuration [66994]
- The ETH1 interface on the XTM 830F is a fiber-optic port, so you cannot use the WSM Quick Setup Wizard from a computer with an Ethernet interface. Use a computer with a Fiber NIC, or connect using a switch with both Fiber and Ethernet interfaces. [59742]

## XTMv

- XTMv does not automatically change the self-signed certificate when its serial number changes. [66668]

### Workaround

A new self-signed certificate with the correct serial number is generated if you manually delete the certificate from Firebox System Manager > View > Certificates and then reboot the XTMv device.

- If you import the OVA file in VMware Player (which is not officially supported in this release), you must use the "Enter" key on your keyboard to accept the XTMv End User License Agreement (EULA). The **OK** and **Cancel** buttons at the conclusion of the EULA do not appear in VMware Player.

## WatchGuard System Manager

- You cannot launch the CA Manager from WSM connected to a Management Server unless you have a Log Server installed on the same computer as your Management Server. [68429]
- If you use Firebox System Manager to ping across a VPN tunnel, you get a message that reads “No Buffer Space Available.” This is not a memory problem. You see this message if the VPN tunnel is not established. Make sure the VPN tunnel is up and try again. [59399]
- WatchGuard System Manager does not display the correct IP address for the default gateway of an XTM device that has no External interface. [56385]
- If you install WatchGuard System Manager on a Windows 7 computer and enable XP Compatibility mode during the installation process, any WSM server component you install will not operate correctly. [56355]

### Workaround

Do not enable compatibility mode during the WatchGuard System Manager install. If it has already been installed, locate the file C:\Program Files\WatchGuard\wsm11\UninsHs.exe. Right-click on that file, click the Compatibility tab, and clear the option for compatibility mode.

- Remote managed Firebox or XTM devices configured in Drop-in Mode may not be able to connect to a Management Server that is behind a gateway Firebox or XTM device 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)**.

- During a WSM upgrade, install, or uninstall on a 64-bit Windows systems, any running applications detected by the WSM installer can be stopped successfully, but the installer may not recognize that they have been stopped. [39078]

### Workaround

Close the installer application. Right-click on the WatchGuard Server Center icon on your Windows task bar and exit the WatchGuard Server Center. Make sure all detected applications are stopped and then retry the WSM install or uninstall.

- When you run the WSM v11.3.x or higher installer (either the WSM client component only or any selected WSM server components) on Microsoft SBS (Small Business Server) 2008 and 2011 on a computer installed with a 64-bit operating system, you see a Microsoft Windows error "*IssProc.x64 has stopped working*". When you close the error dialog box, the installation completes. [57133]

## Web UI

- The Fireware XTM Web UI does not support the configuration of some features. These features include:
  - FireCluster
  - Certificate export



- 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 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]
- You cannot create read-only Mobile VPN with IPSec configuration files with the Web UI. [39176]

## 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.
- For the XTM 2050, the output of the CLI command “show interface” does not clearly indicate the interface number you use in the CLI to configure an interface. The “show interface” CLI command shows the interface number as the interface label on the front of the device (A0, A2 ... A7; B0, B1 ... B7; C0, C1) followed by a dash, and then the consecutive interface number (0 – 17), for all interfaces. [64147]

### Workaround

Use the consecutive interface number that appears after the dash as the interface number to configure the interface. For the B1-9 interfaces, the interface number in the CLI command should be in the range 8-15. For the C0-1 interfaces, the interface number in the CLI command should be 16-17.

## Proxies

- Google Maps and Gmail may fail to load if you use the HTTPS proxy with deep packet inspection enabled. [68267]
- The Policy Manager and Web UI do not provide any warning that the WebBlocker Override may not work for HTTPS. [67208]
- HTTPS DPI (Deep Packet Inspection) does not work for users who use IE 9.0 with TLS 1.1 and 1.2 enabled, but TLS 1.0 and SSL 3.0 not enabled. [65707]

### Workaround

Use a different browser, or enable TLS 1.0 and SSL 3.0 in your IE 9.0 configuration.

- The XTM device can store only one HTTPS Proxy Server certificate and can protect only one HTTPS web site at a time. [41131]
- The ability to use an HTTP caching proxy server is not available in conjunction with the TCP-UDP Proxy. [44260]
- When you try to stream YouTube videos from an Apple device running iOS, you may see this error message: "The server is not correctly configured."

#### Workaround

1. Edit your HTTP proxy policy.
2. Click **View/Edit proxy**.
3. Select the **Allow range requests through unmodified** check box.
4. Save this change to your XTM device.

- The SIP-ALG does not send the Contact header correctly when the Contact header contains a domain name. It only sends an empty string of: Contact: < >. If the Contact header contains an IP address, the SIP-ALG sends the Contact header correctly: Contact: < sip: 10.1.1.2:5060 >. [59622]

#### Workaround

Configure the PBX to send the Contact header with an IP address, not a domain name.

## Security Subscriptions

- When the Application Control rules configured in a proxy policy are applied to traffic, the correct precedence is not applied. If Application Control is configured to Drop for an entire category, and you have specific applications set to Allow, the application is blocked.

#### Workaround

Do not set a rule to drop by category. Instead, manually set all unwanted applications to Drop.

- The URL to send category feedback to Websense in the WSM Help is incorrect. The correct URL is [suggest@websense.com](mailto:suggest@websense.com).
- Some IPS signature information, such as the CVE number, is not available in Firebox System Manager. We provide search capabilities and CVE information for IPS signatures on a web security portal for IPS on the WatchGuard web site, which you can access at <http://www.watchguard.com/SecurityPortal/ThreatDB.aspx>
- Skype detection blocks only new Skype sessions. If a user is already logged in to Skype and a Skype session is already started when Application Control is enabled, Application Control may not detect the activity.
- You cannot use a WebBlocker Server through a branch office VPN tunnel. [56319]

## Networking

- Although you can configure the XTM device to override the MAC address for an interface from the UI, this option does not work for XTM devices configured in Bridge or Drop-in mode. [70721]
- When you add or remove an LA member, traffic through the LA interface stops for 20-34 seconds. [69568]
- To change an interface used in a branch office VPN configuration from a physical interface to a link aggregation interface, you must first remove the physical interface from the branch office VPN configuration, then configure the link aggregation interface, and then edit the branch office VPN configuration again to use the link aggregation interface. [70133]
- Policy Checker does not work when your XTM device is configured in Bridge mode. [66855]
- An apostrophe in a DHCP reservation name causes the DHCP reservation to fail. [65529]
- You cannot configure traffic management actions or use QoS marking on VLANs. [56971, 42093]
- You cannot bridge a wireless interface to a VLAN interface. [41977]

- The Web Setup Wizard can fail if your computer is directly connected to an XTM 2 Series device as a DHCP client when you start the Web Setup Wizard. This can occur because the computer cannot get an IP address quickly enough after the device reboots during the wizard. [42550]

#### **Workaround**

1. If your computer is directly connected to the XTM 2 Series device during the Web Setup Wizard, use a static IP address on your computer.
2. Use a switch or hub between your computer and the XTM 2 Series device when you run the Web Setup Wizard.

- When a secondary network is configured for an XTM 2 Series device configured in Drop-In Mode, it can sometimes take a few minutes for computers that connect to the secondary network to appear in the ARP list of the XTM 2 Series. [42731]
- 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 with 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 accidentally block themselves from their own XTM device. [36934]
- 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]
- 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 XTM device 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 XTM device 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 XTM device is configured in Bridge mode. [36900]
- 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]
- The dynamic routing of RIPv1 does not work. [40880]

## **Multi-WAN**

- If you select the gradual failback as the multi-WAN failback for active connection settings, failback continues to occur immediately. [63932]
- The multi-WAN sticky connection does not work if your device is configured to use the multi-WAN Routing Table mode. [62950]
- When you enable the multi-WAN Immediate Failback option for WAN failover, some traffic may fail over gradually. [42363]

## **Wireless**

- The XTM device may redirect the client browser to the authentication page of the external web server again instead of to the page that they originally requested even though they have successfully authenticated. [64760]

## Authentication

- Citrix 4.5/5/0 servers installed in VMware do not work with Terminal Server Single Sign-On. [66156]

### Workaround

This feature works with Citrix 6.0 and 6.5 servers installed in VMware.

- Clientless SSO is not supported on a TLS-Enabled Active Directory environment.
- If you use Terminal Services authentication, no authentication verification is done against traffic of any protocol that is not TCP or UDP. This includes DNS, NetBIOS, and ICMP traffic.
- Terminal Services authentication is not supported in an active/active FireCluster environment. [70099]
- It is not possible to use the *Automatically redirect users to the authentication page* authentication option together with Terminal Services authentication.
- To enable your XTM device to correctly process system-related traffic from your Terminal or Citrix server, the Terminal Services Agent uses a special user account named Backend-Service. Because of this, you may need to add policies to allow traffic from this user account through your XTM device. You can learn more about how Backend-Service operates in the product help system.
- 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]

## Centralized Management

- Link aggregation interfaces are not correctly added as VPN resources for managed VPN tunnels when you add an XTM device configured to use Link aggregation to your Management Server. [70672]
- There is no option to set up a Traffic Management action in an XTM v11.x Device Configuration Template. [55732]
- If you used Centralized Management with devices subscribed to templates in earlier versions of WSM, when you upgrade from WSM 11.x to v11.4 or higher, these templates are updated and the devices are no longer subscribed. Each device retains its template configuration. Existing templates are updated to use "T\_" in their object names (to match the object names in the devices that used to subscribe to them). After you upgrade, you'll see the template upgrade that occurs during upgrade in your revision history.

## FireCluster

- The health index for a wireless FireCluster member is not accurate and therefore, if the interface that wireless is bridged to is disconnected, no failover will occur. [69868]
- You cannot disable Eth1 on a wireless device configured as a member of a FireCluster. [69458]
- You are not warned if you try to create a FireCluster with two wireless devices and you have not yet enabled the DHCP server on the bridge interface. [69483]
- You cannot use the secondary IP address of an XTM device interface to manage a FireCluster configured in active/active mode. [64184]

### Workaround

Use the primary IP address of an XTM device for all management connections to an active/active FireCluster.

- If the Log Server cannot be reached from the management IP addresses, only the current FireCluster master will be able to connect. This can occur if the Log Server is connected through an External network, but the management IP addresses are on a Trusted or Optional network. [64482]
- If a monitored link fails on both FireCluster members, the non-master member is switched into passive mode and consequently does not process any traffic. A multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond.
- Each XTM device has a set of default IP addresses assigned to the device interfaces in a range starting with 10.0.0.1. The highest default IP address depends on the number of interfaces. If you set the IP address of the Primary or Backup cluster interface to one of the default IP addresses, both devices restart, and the backup master becomes inactive. [57663]

#### Workaround

Do not use any of the default IP addresses as the Primary or Backup cluster interface IP address.

- 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.
- If you use HP ProCurve switches, you may not be able to configure your FireCluster in active/active mode because these switches may not support the addition of static ARP entries. [41396]
- 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 an active/passive FireCluster. [36467]
- It is not possible to use a VLAN interface IP address for a FireCluster management IP address. [45159]
- To perform a manual upgrade of a FireCluster from v11.3.x to a later version of Fireware XTM OS, the management computer must be on the same network as the FireCluster management IP addresses. [63278]

## Logging and Reporting

- When you use the WatchGuard Server Center Setup Wizard to install the Log Server or Report Server, installation will fail if you use a special character (non-alphanumeric) in the log encryption key you set. [71687]
- When you change the log level for your WatchGuard Log Server and click **Apply**, the change does not take effect. [60088]

#### Workaround

1. In WatchGuard Server Center, on the Log Server Logging tab, change the log level for log messages from the Log Server and click **Apply**.
2. In the Servers tree, right-click Log Server and select **Stop Server**. In the confirmation message, select **Yes**.
3. Right-click Log Server again and select **Start Server**.

- The Denied Packets Summary report is not yet available in Report Manager. [63192]
- The PDF output of the Web Activity Trend report does not include time labels on the x-axis when viewed in Report Manager. Date and time information is included in the table below the report. [64162]
- When you upgrade from Fireware XTM v11.4.x, reports generated near the time of the upgrade may not show up in Report Manager. [64325]
- If a daily report schedule name includes a colon or certain other characters (for example: "1:35"), the system returns an error. [63427]

#### **Workaround**

Make sure that your report schedule names use only characters that are valid in Windows file names. You can find valid characters in articles such as <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx> .

- There are two sorting issues in Report Manager. When you sort by Destination, the field sorts by IP address and not the destination host name (if available). When you sort by Disposition, some items in the "deny" state do not sort accurately within groups. [62879]
- Any configured daily or weekly "Archived Reports" you have in your v11.3 configuration are automatically converted to scheduled reports after you upgrade to WSM v11.4 or higher.

## **Mobile VPN**

- You can configure LDAP, Active Directory, and SecurID authentication methods for Mobile VPN with L2TP from the Web UI, but these authentication methods are not supported for L2TP. [70818]
- If a BOVPN is configured to use Main Mode for Phase 1, and has a dynamic remote gateway IP address, Mobile VPN with L2TP may not work correctly. Policy Manager prevents this configuration, but Web UI and CLI do not. WebUI and CLI also do not display an error message when you try to configure L2TP if a BOVPN is already configured in that way. [70588]

#### **Workaround**

Use Aggressive Mode for any BOVPN with a dynamic gateway IP address.

- You cannot use an encryption password of "password" in the WatchGuard Mobile VPN app for iOS. [70510]
- Mobile VPN with L2TP clients cannot connect using x509 certification as their authentication method. [70642]
- You must restart your XTM device after you change the DNS server settings configured on the XTM device before Mobile VPN with L2TP clients can use the new DNS server settings. [70571]
- Mobile VPN with SSL does not work when bridged to a wireless interface. [70267]
- You cannot make an L2TP connection with an IPsec pre-shared key when the L2TP tunnel passes through a device configured for static NAT. [69350]
- The L2TP configuration does not sync correctly from a master XTM device to a backup XTM device in an active/passive FireCluster. [69776]
- If you use the Mobile VPN app for iOS, your web browser opens after you install the profile. You can close the web browser to continue.
- Occasional issues have been reported with the Mobile VPN app for Android on Samsung Galaxy II phones over 3G connections.
- You cannot generate a Mobile VPN with IPsec configuration file when the group name contains the characters the asterisk or period characters(\*, .). [66815]

- When you use the built in IPSec client from an iPhone or iPad, the client connection will disconnect when the connection duration reaches 1 hour and 45 minutes. This is caused by a limitation in the Cisco client used by iPhone/iPad. You must reconnect the IPSec client to reestablish the VPN tunnel. [63147]
- Mobile VPN with PPTP connections from Android mobile devices do not work consistently on 3G mobile networks. [63451]
- Connections from the Mobile VPN with IPSec client can route through the wrong external interface when the XTM device is configured for multi-WAN in round-robin mode. [64386]
- You cannot configure Mobile VPN with SSL to bridge network traffic to a bridged interface. [61844]
- Mobile VPN with SSL users cannot connect to some network resources through a branch office VPN tunnel that terminates on an active/active FireCluster. [61549]
- You cannot ping the IP address of the XTM device interface to which a Shrew Soft VPN client established a VPN tunnel. You can ping computers on that network, but not the interface IP address itself. [60988]
- Shrew Soft VPN client connections can drop if there are multiple clients connected to an XTM device at the same time issuing Phase 2 rekeys. [60261]
- Phase 1 rekeys initiated by the Shrew Soft VPN client cause the client to be disconnected, if connected more than 24 hours. In this case, we recommend that you set the rekey on your XTM device to 23 hours – one hour shorter than the rekey hard-coded in the Shrew Soft client configuration. This forces the XTM device to initiate the rekey, and gives the client a notification that the tunnel must be re-established. [60260, 60259]
- The Mobile VPN for SSL Mac client may not be able to connect to an XTM device when the authentication algorithm is set to SHA 256. [35724]

## Branch Office VPN

- If the name of a Branch Office VPN tunnel exceeds 28 characters in length, the BOVPN tunnel is built, but no traffic can pass through the tunnel. [71448]

### Workaround

Delete the VPN tunnel, create it again, and specify a name with less than 28 characters.

- To change an interface used in a branch office VPN configuration from a physical interface to a link aggregation interface, you must first remove the physical interface from the branch office VPN configuration, then configure the link aggregation interface, and then edit the branch office VPN configuration again to use the link aggregation interface. [70133]
- Manual branch office VPN fails when the pre-shared key exceeds 50 characters. [65215]
- Do not use the same name for both a VPN Gateway and a VPN Tunnel. [66412]
- When you configure your XTM device in multi-WAN mode, you must select which interfaces to include in your multi-WAN configuration. If there are any interfaces that you choose not to include in your multi-WAN configuration (i.e. you clear the check box for that interface), the system does not create a route for that network. This can cause a problem if you have a branch office VPN configured to include that same interface. In this case, the VPN tunnel can fail to negotiate with its remote peer. [57153]

### Workaround

If you use multi-WAN and have problems with your branch office VPN tunnels failing to negotiate with their remote peers, you must open your multi-WAN configuration and select Configure adjacent to your chosen multi-WAN configuration mode. Make sure that the appropriate interfaces are included in your multi-WAN configuration.

- A branch office VPN tunnel does not pass traffic if an inbound static NAT policy that includes IP 50 and IP 51 protocols exists for the external IP address of the XTM device. [41822]
- Managed branch office VPN tunnels cannot be established if the CRL distribution point (for example, the WatchGuard Management Server or a third-party CRL distribution site you use) is offline. [55946]
- 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 XTM device 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).

- 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]

**Workaround**

From Policy Manager, select **View > Policy Highlighting**. Clear the **Highlight Firewall policies based on traffic type** check box.

## 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