Fireware XTM v11.8 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	432340
WatchGuard System Manager Build	432016
Revision Date	November 14, 2013

Introduction

On 11 November we updated the XTM Software Download Center and these release notes for the release of updated v11.8 Single Sign-On software and the release of a WatchGuard-branded Mobile VPN with IPSec client for Mac (powered by NCP).

WatchGuard is pleased to announce the release of Fireware XTM v11.8 and WatchGuard System Manager v11.8.

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 v11.8, see the product documentation or review What's New in Fireware XTM v11.8.

New Features in Fireware XTM v11.8

Data Loss Prevention

The Fireware XTM Data Loss Prevention (DLP) service enables you to detect, monitor, and prevent unauthorized transmission of confidential information outside your network or across network boundaries. The DLP service includes built-in auditing sensors that you can use to monitor compliance with HIPAA or PCI information security requirements. You can also create new DLP sensors that use content control rules you select. DLP includes a predefined library of over 200 rules for 18 countries around the world, covering personally identifiable information (PII), financial and health care data.

Branch Office VPN Virtual Interface Support

To provide more flexibility and capabilities, Fireware XTM now supports the option to configure a Branch Office VPN as a virtual interface. This enables you to use the branch office VPN virtual interface with static routing, dynamic routing or policy-based routing.

New Fireware XTM Web UI and FireWatch

The Web UI has been completely redesigned for Fireware XTM v11.8. It is now mobile-ready, no longer requires Adobe Flash, and includes a new set of tools to help you monitor your XTM device.This new toolset includes FireWatch, a new real-time, interactive visualization tool that graphically shows the current state of client connections through your XTM device.

YouTube for Schools

You can now add YouTube Edu-Filters to your HTTP proxy policies so that school and education districts can enforce safe and appropriate web browsing of YouTube content at the firewall level.

Enhancements to IPv6 Support

The set of Fireware XTM features for which we support both IPv4 and IPv6 addresses now includes:

- FireCluster now supports IPv6.
- IPS now scans IPv6 traffic.
- Application Control now scans IPv6 traffic.
- DHCPv6 is now supported on external, trusted, and optional interfaces.
- The Default Packet Handling settings to block flood attacks apply to both IPv6 and IPv4 traffic.
- Authentication portal web page access is now supported from an IPv6 address.

Authentication Enhancements

We have made significant enhancements in two authentication-related features:

- Support for indirect LDAP queries simplifies authentication requests to non-Microsoft LDAP servers.
- Single Sign-On support for Mac OS X, iOS, and Android users.

SSL-Based Management Tunnels

Management Tunnels over SSL enable you to make a management connection to your remote XTM devices that are behind a third-party NAT gateway device over TCP port 443, which is helpful when you do not control the third party NAT gateway device in front of your managed XTM device.

WatchGuard AP Device Enhancements

- The ability to set channel and bandwidth on WatchGuard AP devices
- Management VLAN tagging is now supported

The release also includes the addition of a number of smaller features that might interest you, including:

- SHA2 encryption support on all XTM models except XTM 21, 22, 23, 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.
- Support for up to 20 PPPoE sessions on a single external interface.
- SSO Port Tester feature you can use to verify that your SSO Agent can contact the Event Log Monitor and Exchange Monitor.
- New global SNAT setting you can use to control whether or not the XTM device clears active connections that use an SNAT action you modify.

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 v11.8.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 all WatchGuard products is available on the WatchGuard web site at www.watchguard.com/help/documentation.

Localization

This release includes a localized management user interface for the WSM application suite, and localized product help, current to Fireware XTM v11.7.2. Updates for Fireware XTM v11.8 will be available at a later date. There is no localization for the Web UI or Web UI Help in this release. For WSM, supported languages are:

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

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. Any software components provided by third-party companies remain in English.

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.

Fireware XTM and WSM v11.8 Operating System Compatibility

Revised November 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 v10.6, v10.7, v10.8	Android 4.x	iOS v5, v6 & v7
WatchGuard System Manager	✓	✓	✓	✓	✓			
WatchGuard Servers	✓	✓	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)			✓	✓	✓			
Single Sign-On Client	✓	✓	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[1]			✓[2]	✓	✓			
Terminal Services Agent[3]			✓	✓	✓			
Mobile VPN with IPSec	✓	✓				✓[4]	✓	✓[4]
Mobile VPN with SSL	✓	✓	✓			✓	✓	✓

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.*

The following browsers are supported for both Fireware XTM Web UI and WebCenter (Javascript required):

- *IE 9 and later*
- *Firefox v22 and later*
- *Safari 5 and later*
- *Safari iOS 6 and later*
- *Chrome v29 and later*

[1]Microsoft Exchange Server 2003, 2007, and 2010 are supported.

[2]Exchange Monitor is supported on Windows Server 2003 R2.

[3]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.

[4]Native (Cisco) IPSec client and OpenVPN are supported for Mac OS and iOS. For Mac OS X 10.7 and v10.8, we also support the WatchGuard IPSec Mobile VPN Client for Mac, powered by NCP.

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[1]	LDAP	RADIUS [2]	SecurID [2]	Firebox (Firebox-DB) Local Authentication
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓3	–	✓
Mobile VPN with IPSec/WatchGuard client (NCP)	✓	✓	✓	✓	✓
Mobile VPN with IPSec for OS and Mac OS X native VPN client				✓	✓
Mobile VPN with IPSec for Android devices	✓	✓	✓	–	✓
Mobile VPN with SSL for Windows	✓	✓	✓4	✓4	✓
Mobile VPN with SSL for Mac	✓	✓	✓	✓	✓
Mobile VPN with SSL for iOS and Android devices				✓	✓
Mobile VPN with L2TP	✓6	–	✓	–	✓
Mobile VPN with PPTP	–	–	✓	N/A	✓
Built-in Authentication Web Page on Port 4100	✓	✓	✓	✓	✓
Single Sign-On Support *(with or without client software)*	✓	✓	–	–	–
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

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_8.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.8.

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_8.exe` `xtm_xtm800_1500_2500_11_8.zip`
XTM 2050	`XTM_OS_XTM2050_11_8.exe` `xtm_xtm2050_11_8.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_8.exe` `xtm_xtm800_1500_2500_11_8.zip`
XTM 1050	`XTM_OS_XTM1050_11_8.exe` `xtm_xtm1050_11_8.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_8.exe` `xtm_xtm800_1500_2500_11_8.zip`
XTM 8 Series	`XTM_OS_XTM8_11_8.exe` `xtm_xtm8_11_8.zip`
XTM 5 Series	`XTM_OS_XTM5_11_8.exe` `xtm_xtm5_11_8.zip`
XTM 330	`XTM_OS_XTM330_11_8.exe` `xtm_xtm330_11_8.zip`
XTM 33	`XTM_OS_XTM33_11_8.exe` `xtm_xtm33_11_8.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_8.exe` `xtm_xtm2a6_11_8.zip`

XTMv
All editions for VMware
	`xtmv_11_8.ova`
	`xtmv_11_8.exe`
	`xtmv_11_8.zip`

XTMv All editions for Hyper-V	`xtmv_11_8_vhd.zip`

Single Sign-On Software

New and updated Single Sign-On software is available with v11.8:

- `WG-Authentication-Gateway_11_8.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_8.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_8.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_8.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_8.exe` (Exchange Monitor for 64-bit operating systems)

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

Terminal Services Authentication Software

- `TO_AGENT_SETUP_11_8.exe` (This installer includes both 32-bit and 64-bit file support and has been updated for the XTM v11.8 release.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL. These files have been updated for this release.

- `WG-MVPN-SSL_11_8.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_8.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are three available files to download.

- `Shrew Soft Client 2.2.0 for Windows` - Shrew Soft has recently 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 v2.2.0 VPN client. If you want to use the v2.2.1 client, we recommend you read this Knowledge Base article first.
- `WatchGuard IPSec Mobile VPN Client for Windows, powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.
- `WatchGuard IPSec Mobile VPN Client for Mac OS X, powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.

WatchGuard AP Firmware

If you manage WatchGuard AP devices and your Gateway Wireless Controller is enabled to update these devices automatically, your AP devices will be upgraded to new firmware when you upgrade your XTM device. If you want to update your WatchGuard AP devices manually, you can now open the WatchGuard AP Software Download page and download the latest AP firmware and manually update your AP devices. We also provide one previous version of AP firmware on this page for recovery purposes only. The file names for the latest AP firmware are:

- `AP100-v1.2.9.0.bin`
- `AP200-v1.2.9.0.bin`

Upgrade from Fireware XTM v11.x to v11.8

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.8, 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. Also, make sure to upgrade WSM before you upgrade the version of XTM OS on your XTM device.

If you use an XTM 5 Series or 8 Series device, you must upgrade to Fireware XTM v11.7.4 before you can upgrade to Fireware XTM v11.8.

We recommend that you reboot your XTM device before you upgrade. While this is not necessary for most higher-model XTM devices, a reboot clears your XTM device memory and can prevent many problems commonly associated with upgrades in XTM 2 Series, 3 Series, and some 5 Series devices.

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 v11.8. You can install the v11.8 server and client software on top of your existing installation to upgrade your WatchGuard software components.

Upgrade to Fireware XTM v11.8 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* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.8\[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 v11.8 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* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.8\[model] or [model][product_code].
3. Install and open WatchGuard System Manager v11.8. 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 v11.8

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.

If you use an XTM 5 Series or 8 Series device, you must upgrade your FireCluster to Fireware XTM v11.7.4 before you can upgrade your FireCluster to Fireware XTM v11.8.

Upgrade a FireCluster from Fireware XTM v11.4.x–v11.7.x to v11.8

Use these steps to upgrade a FireCluster from Fireware XTM v11.4.x, v11.5.x, v11.6.x,or v11.7.x to Fireware XTM v11.8:

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 v11.8, 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 v11.8 to WSM v11.x

If you want to revert from v11.8 to an earlier version of WSM, you must uninstall WSM v11.8. 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 v11.8.

Next, install the same version of WSM that you used before you upgraded to WSM v11.8. 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 v11.8. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.8 to Fireware XTM v11.x

If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.8 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 v11.8 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 v11.8. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.8 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.

When you downgrade the Fireware XTM OS on your XTM device, the firmware on any paired AP devices is not automatically downgraded. We recommend that you reset the AP device to its factory-default settings to make sure that it can be managed by the older version of Fireware XTM OS.

Resolved Issues

Fireware XTM v11.8 addresses many previously reported bugs and enhancement requests, including the issues shown below.

General

- This release resolves a reported buffer overflow vulnerability in the WGagent code supporting the web management UI. *[76752]*
- Active connections are now terminated immediately when adding a blocked site using Firebox System Manager, Policy Manger or Web UI. *[67762]*

Proxies and Services

- You can now add YouTube Edu-Filters to your HTTP proxy policies so that school and education districts can enforce safe and appropriate web browsing of YouTube content. *[63988]*
- XTM 515, XTM 525, XTM 535, and XTM 545 devices configured for the Gateway AV service now use the expanded, enterprise set of Gateway AV signatures. *[72095]*
- This release resolves an issue with AV scanning that prevented large text based files from passing through the proxy with a log message: “AV scanning error="no text for this error code". *[75868]*
- Log messages now correctly show in Firebox System Manager Traffic Monitor when the SMTP proxy processes an email with UTF-8 encoding in the message body. *[70927]*
- In this release, we have optimized system resource and CPU consumption for HTTPS proxy with deep packet inspection. *[68267, 70319]*
- HTTPS DPI (Deep Packet Inspection) now operates correctly 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]*
- When you launch Policy Manager from French-language WatchGuard System Manager, changes made to allow or deny SurfControl categories are now correctly saved. *[71881]*
- Several issues that caused the XTM device to become unstable under heavy proxy traffic load have been resolved. *[73709, 75971]*
- This release improves the expired connection handling for the DNS Proxy. *[60901]*
- An issue that caused WebBlocker Server connection errors and prevented successful web browsing has been resolved in this release. *[72770]*
- An issue has been resolved that caused WebBlocker, when configured to use the Websense cloud for URL lookups, to occasionally miscategorize web sites. *[74804]*
- You can now correctly view quarantined email content that includes rich text or double-byte characters. *[60094]*

Authentication

- The v11.8 SSO client includes numerous bug fixes and performance improvements. *[77238, 73607, 71303, 76843]*
- This release adds Single Sign-On support for Mac OS X with the release a new SSO client for Mac users, and new Exchange Monitor software. *[64443]*

- This release introduces a new SSO Port Tester feature you can use to verify that your SSO Agent can contact the Event Log Monitor and Exchange Monitor. *[65446]*
- The new SSO Agent software now works more effectively in a DHCP environment. *[71882]*
- Unnecessary log messages "###ERROR### NetworkStream. Write exception..." and "NOT AUDIT SUCCESS" are no longer written to log files. *[74956, 71621]*
- Event Log Monitor includes numerous bug fixes related to user detection and group retrieval. *[76711, 76860, 76842, 76841, 77003, 77055, 76661, 73341]*
- The Event Log Monitor UI element **IP Addresses of Domain Controller** has been updated to **IP Addresses of Event Log Monitor** to be less confusing. *[76663]*
- Support for indirect LDAP queries simplifies authentication requests to non-Microsoft LDAP servers. *[41729]*
- The Session Timeout and Idle Timeout settings for hotspot external guest authentication are now optionally configurable. *[75598]*
- If you configure a Redirect URL in your hotspot Custom Page settings, it is no longer incorrectly applied to External Guest Authentication. *[75599]*

Logging and Reporting

- A problem that caused the Report Server to stop pulling log data from the Log Server for reporting has been resolved in this release. *[74567]*
- User names now show correctly in log messages when you use syslog. *[41761]*

Networking

- A problem with the ordering of routes in the routing tables that caused Multi-WAN to fail has been resolved. *[65540]*
- This release includes a new option to terminate active connections when an SNAT action changes. This new check box appears in the Global Settings > Network tab. *[62716]*
- The Multi-WAN Routing Table configuration mode now works correctly if you use BGP dynamic routing. *[72190]*
- With this release, we add support for up to 20 PPPoE sessions on a single external interface. *[55921]*
- Link aggregation interfaces are now 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]*
- It is no longer necessary to 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]*
- DHCP Relay now works correctly with VLANs. *[73746]*

Centralized Management

- You can now create SSL-based Management Tunnels to remotely manage XTM devices behind 3rd party NAT devices. *[70895]*
- It is no longer necessary to have at least one internal physical interface in order to create a Management Tunnel. *[71512]*

FireCluster

- An issue that causes load balancing to fail in an active/active FireCluster has been resolved. *[76463]*
- A memory leak that could occur on the backup member of a FireCluster has been addressed. The leak was specific to static NAT FTP traffic on XTM 800, XTM 1500, and XTM 2500 devices. *[74628]*
- An issue that caused a cluster member to get stuck in the IDLE role (and not move to the BACKUP role) has been fixed. *[73159]*

- A problem has been resolved that resulted in FireCluster failover after saving centralized management template changes through an active/passive FireCluster acting as your Gateway Firebox. *[73159]*

VPN

- The addition of Branch Office VPN Virtual Interface support in this release resolves these issues:
  - The XTM device can now redistribute its configured BOVPN routes to internal routers. *[64553]*
  - You can now use multiple BOVPN peers with overlapping networks.
- A configuration error in a Branch Office VPN tunnel no longer causes all VPN traffic to fail. *[73387]*
- Branch Office VPN no longer fails if you have Multi-WAN configured but only one interface selected in the interface group. *[57153]*
- You can now use the same name for both a VPN Gateway and a VPN Tunnel. *[66412]*
- Managed branch office VPN tunnels can now be established when the CRL distribution point (for example, the WatchGuard Management Server or a third-party CRL distribution site you use) is offline. *[55946]*
- This release resolves an issue that caused the IKED process to crash. *[75131]*
- This release resolves a kernel crash associated with L2TP. *[76580, 72593]*
- You can now make an L2TP connection with an IPSec pre-shared key when the L2TP tunnel passes through a device configured for static NAT. *[69350]*
- Mobile VPN with PPTP connections from Android v2.2 mobile devices now work consistently on 3G mobile networks. *[63451]*
- Mobile VPN with SSL now works correctly when bridged to a wireless interface. *[70267]*
- You can now configure the Mobile VPN with SSL client to not remember passwords. *[71111]*
- The Mobile VPN with SSL installation no longer warns Windows users that the Tap Driver is not signed. *[43072]*

XTM Wireless

- When you open a configuration in which the Hotspot feature is enabled for a wireless interface, the configuration no longer becomes corrupt. *[72831]*
- The XTM device no longer redirects the client browser to the authentication page of the external web server again after you have already successfully authenticated. *[64760]*

WatchGuard AP

- If you use an SSID name of "any", you can now get a correct list of connected users in Firebox System Manager or Web UI System Status > Gateway Wireless Controller. *[71614]*
- You can now use the back tick character ' in the SSID name. *[71904]*
- You can now use any non-alphanumeric characters in the password when you set the password for an AP device with the AP device web UI. *[71718]*
- It is now possible to change the diagnostic logging level for the Gateway Wireless Controller. *[71836]*
- You can now correctly update WatchGuard AP settings with Policy Manager running in a localized, double-byte language. *[75550]*

Known Issues and Limitations

These are known issues for Fireware XTM v11.8 and all management applications. Where available, we include a way to work around the issue.

General

- If you want to use the WSM Quick Setup Wizard Recovery Mode feature for an XTM 5 Series or 8 Series device, you must install Fireware XTM OS v11.7.4 on your management computer before you start the Quick Setup Wizard. See the *WatchGuard System Manager Help* for more information on Recovery Mode.
- 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]*

Installation and Upgrade

- If you have a DHCP MAC reservation name that includes an underscore character in your configuration file, the underscore will be converted to a hyphen when you upgrade to XTM v11.8.
- You cannot use WSM v11.7.4 to upgrade an XTM 5 Series or 8 Series device to Fireware XTM v11.8. If you try, you will see the error message: “The selected upgrade image does not appear to be for this WatchGuard device model(XTM xxx). Do you want to continue?” You must use WSM v11.8 to upgrade an XTM device to XTM v11.8. *[76625]*
- If the Gateway Wireless Controller is configured to automatically upgrade the firmware of your AP devices, all AP devices will upgrade to new firmware when you upgrade your XTM device to Fireware XTM v11.8. When the firmware is upgraded, the AP devices are reset to their default configuration. The AP device uses DHCP to request an IP address. The XTM device discovers and pairs the AP device again. If the AP device cannot get an IP address, you must assign it an IP address so that the XTM device can connect and discover it again.

Workaround
If DHCP is not enabled on the networks where your AP devices are connected, disable automatic AP firmware updates in the Gateway Wireless Controller configuration and then manually upgrade the firmware on your AP devices.

- If the Gateway Wireless Controller is configured to automatically upgrade the firmware of your AP devices and you use multiple AP devices, all AP devices will upgrade to new firmware when you upgrade your XTM device to Fireware XTM v11.8 at approximately the same time. This can result in less than optimal radio channel selection for your AP devices.

Workaround
You have several options:
1. You can disable the automatic update feature in the Gateway Wireless Controller and upgrade your AP devices manually.
2. You can reboot each AP device at a different time after the upgrade so that each AP device can select a radio channel.
3. You can manually set the channel for each AP device in the Gateway Wireless Controller after you upgrade to Fireware XTM v11.8.

WatchGuard AP and Gateway Wireless Controller

- In an active/passive FireCluster, the WatchGuard AP reboots each time there is a change in the cluster master. *[71859]*
- If you use an SSID name of "any", "on", or "off", the AP device does not broadcast the SSID. *[72965]*
- The Gateway Wireless Controller does not support individual RADIUS shared secrets per AP device in this release. All AP devices must use the same RADIUS shared secret in this release. *[71723]*
- Managed device templates on a WatchGuard Management Server do not support configuration of the Gateway Wireless Controller in this release.
- You cannot pair a WatchGuard AP device to more than one Gateway Wireless Controller/XTM device. If you do, the AP device will fail. *[71920]*
- Occasionally, the Site Survey operation fails to complete until the AP device is first rebooted. *[71944]*

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 **Cance**l buttons at the conclusion of the EULA do not appear in VMware Player.

WatchGuard System Manager

- If you connect to a Firebox e-Series Core or Peak device running Fireware v10.2.12 or earlier with WatchGuard System Manager v11.8, you cannot open Policy Manager. *[77119]*

Workaround
Install and run WatchGuard System Manager v10.2 on a different workstation, or install WatchGuard System Manager v10.2 before you install WatchGuard System Manager 11.8. For more information, see this knowledge base article.

- The process of saving your configuration from Policy Manager can take a long time if you have more than 1000 secondary IP addresses configured on the same interface. *[75262]*
- WatchGuard Server Center incorrectly shows WatchGuard Server status in the Log Server > Firebox Status table. *[76468]*
- The Report Manager > Servers list may not display correctly in this release. *[73530]*
- 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.

- 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**).

- 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

- When you log out of the Web UI with the admin account, any user currently logged in with the status account is automatically logged out as well. *[75698]*
- FireWatch results for users may not be accurate if your users are not explicitly defined in your XTM configuration file as authorized users. *[76781]*
- If you log in to the Web UI with IE 9 or IE 10, pressing the Enter key on your keyboard may clear any unsaved configuration settings on the current page. *[74571]*
- You cannot enable logging for the default packet handling rule in the Web UI. You must use Policy Manager. *[74274]*
- 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.

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

- If you configure a TCP-UDP Proxy policy with the actions for HTTP and HTTPS set to Allow, and you enable Application Control or IPS on that same policy, the TCP-UDP Proxy will fail to identify HTTP and HTTPS traffic. *[77410]*

Workaround
If you use separate packet filter policies for HTTP and HTTPS, you will not see this issue. Also, if you use HTTP and HTTPS proxy actions instead of **Allow** for those protocols, the TCP-UDP proxy will correctly identify the traffic.

- If you disable the default Outgoing policy and enable the HTTP proxy in your XTM device configuration, Skype connections may fail. *[77272]*

Workaround
Use the Outgoing policy to handle Skype traffic, or create a custom proxy policy for port 80, with the TCP-UDP proxy enabled. The TCP-UDP proxy will detect the non-HTTP traffic and allow the request through. This may allow other applications to connect on port 80 that do not follow the normal behavior for HTTP.

- When you enable deep inspection of TLS in the SMTP proxy, the SMTP process may crash if you have imported a certificate for content inspection that is not a CA certificate. *[77207]*

Workaround
Import a certificate with CA privileges as the proxy authority certificate, or delete the imported certificate and use the default self-signed certificate from the XTM device. A reboot is required to generate a new certificate after you delete the imported third-party certificate.

- When you configure SMTP proxy with deep inspection of TLS enabled for inbound SMTP traffic, mail delivery may fail for some senders that use TLS. The SMTP proxy accepts the email from the sender, but fails to send the second required EHLO to the internal SMTP server. *[77312]*

Workaround
If you have identified a particular sender that cannot send email to your network, you can create a packet filter policy to handle the traffic from this sender only. In that policy, allow traffic from the external IP address of that sender to forward to your internal mail server.

- When you configure an FTP Proxy policy for 1-to-1 NAT traffic, the FTP login will succeed but it is not possible to transfer any data. *[77218]*

Workaround
Add the NAT Base IP address for the 1-to-1 NAT rule to the Secondary Networks tab of the external interface, in CIDR format, or use Static NAT for incoming FTP connections to your FTP server.

- In the HTTPS proxy settings, if you select the option Enable deep inspection of HTTPS traffic, together with the default option Use OCSP to validate certificates, any site that does not support OCSP (such as Google) will not load correctly for your users. *[76194]*
- WebBlocker exceptions configured for a host IP address do not work correctly if you specify a port other than the default port. *[75287]*
- The Policy Manager and Web UI do not provide any warning that the WebBlocker Override may not work for HTTPS. *[67208]*
- 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

- Users of the Data Loss Prevention service should be aware that the additional service will add more scanning load on the appliance and consume more memory. Each sensor requires additional space in memory, and the number of DLP rules that are configured on each sensor also impacts the amount of memory used by the appliance. Only select those rules that are appropriate for your region and the use case that is relevant to your industry. This will also help to minimize any potential false positives. On the XTM 25/26, we recommend that you use no more than one or two sensors, and each sensor should not contain more than 6 DLP rules.
- DLP cannot detect violations in the body of an email when users use web-based mail, such as Gmail. *[73266]*
- DLP does not work with all compressed file types sent using the HTTP protocol. *[75372]*
- DLP does not work correctly in this release for these file formats: Microsoft Excel 97-2003, Visio VSD, OpenOffice, Microsoft Project v2010. *[73602, 73753, 73778, 73734, 74283]*
- 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. See Knowledge Base article 5544 for more information.
- You cannot use a WebBlocker Server through a branch office VPN tunnel. *[56319]*

Networking

- If you enable Policy-Based Routing on a policy for traffic to a non-external interface or Static NAT, that traffic will not work. *[77127, 77128]*

Workaround
Do not enable Policy-Based Routing on a policy for traffic to a non-external interface or Static NAT. Policy-Based Routing controls which external interface will pass outbound traffic, so it should not be used for traffic not directed to an external interface.
If you use a single policy for traffic for both external and non-external interfaces and must use Policy-Based Routing, create a separate policy for the traffic to the non-external interface.

- If you change the configuration of the primary PPPoE interface, all other PPPoE sessions disconnect, then reconnect. *[74918]*
- If your XTM device is configured in drop-in mode, the source IP address in an SNAT action is not correctly handled. *[75239]*
- If you change the configuration of your XTM device from routed mode to bridge mode, the IP addresses are not correctly removed from the configuration, causing traffic to fail through the device, even after a reboot. *[75998]*
- If you add more than 200 Blocked Site Exceptions, the last few IP addresses in the list will still be blocked. *[75696]*
- A user-defined alias cannot have the same name an XTM device interface. *[73198]*
- XTM devices can send and respond to IPv6 ping requests, however, the -6 flag is not supported by Firebox System Manager > Diagnostic Tasks. *[71631]*

Workaround
Connect to the XTM device with the CLI to use IPv6 ping.

- When you configure a 1-to-1 NAT rule, you cannot use an IP address that is already configured as a secondary network IP address. If you try to do this, incoming policies that handle IPSec traffic will not correctly pass the IPSec traffic. *[66806]*
- 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 Link Aggregation 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]*
- 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.

- 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 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]*
- 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]*

XTM Wireless

- If a connection from a user on the Wireless Guest Network matches a policy with Any-Trusted in the From field, that connection is handled by that policy if that policy has higher precedence than a policy that specifies WG-Wireless-Guest in the From field. *[69328]*

Workaround
Make sure that any policies that specify WG-Wireless-Guest access control for any port and protocol have higher precedence than matching policies with Any-Trusted in the From field. You can do this several ways:
1. In Policy Manager, use **View > Auto-Order mode** to disable Auto-Order Mode and then manually move the policies for WG-Wireless-Guest above the matching Any-Trusted policies in the list.
2. For any policy with Any-Trusted in the From field, remove that alias and manually add the specific interface alias or network IP address for all desired Trusted networks.

- When you configure the wireless guest network on your XTM device, or bridge a wireless interface to any trusted or optional network, these networks cannot be used in a policy in a Management Server template. *[62455]*

Workaround
In your template, create an alias that has the same name as the wireless alias created when you enabled your wireless interface.

Authentication

- Exchange Monitor may not work well in an active/active Exchange cluster environment. *[75892]*
- If you use both Exchange Monitor and Event Log Monitor at the same time, you can see a log message ERROR="Unknown User" for any Mac user that is authenticated by Exchange Monitor, even though there is no problem. *[73080]*
- Certain servers that integrate with Exchange are authenticated through Active Directory. Exchange Monitor authenticates the service account with the server's IP address and these servers appear in monitoring tools as authenticated users, unless you add them to the SSO exceptions list. *[77196]*
- For both Exchange 2003 and Exchange 2007, if you use the same domain account to access emails on several Windows devices using Outlook 2010 at the same time, end users must add a registry key in all Windows clients before the Exchange Monitor can detect the accurate IP address for each client.
- When you configure authentication with Active Directory, and you enter values to the DN of Searching User and Password field in the Active Directory configuration on the XTM device, the ADMD (Authentication) Process may use a large amount of CPU resources. The CPU spike occurs when a user tries to authenticate with an invalid username and this can cause authentication and other services to run more slowly. *[77138]*

Workaround
Use the sAMAccountName as the login attribute in your Active Directory configuration.

- Nested group information cannot be retrieved when authenticating to a non-Microsoft LDAP server. *[75100]*
- Authentication does not work to an authentication server located at the remote end of a BOVPN virtual interface if there is no route for the return traffic. *[75714]*

Workaround
In the BOVPN virtual interface configuration, assign BOVPN virtual interface IP addresses. Or, use static or dynamic routing to make sure that each XTM device knows the routes to the local networks on the peer device.

- If you use Active Directory (AD) authentication for Terminal Services users, a mismatch in capitalization (case) between the domain name configured in **Setup > Authentication > Servers** and your actual AD server can cause a failure to apply policies correctly to the users. *[72721]*
- 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

- A spoke device connected via VPN to a FireCluster cannot send log data through an SSL-based management tunnel. *[74446]*
- Each time you make a change to the hotspot configuration of a fully managed device, you see an unnecessary warning that you can safely ignore. *[71938]*
- 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

- Traffic through a FireCluster that traverses a BOVPN virtual interface configuration and is processed by a policy that uses policy-based routing may not fail over correctly when your FireCluster fails over. *[76161]*
- Management of an active/active FireCluster with WSM or Firebox System Manager through an IPv6 address does not work correctly. *[76566]*

Workaround
To manage an active/active FireCluster, connect using an IPv4 address.

- Tunnel switching of BOVPN virtual interface traffic in an active/active FireCluster does not work. *[76431]*
- An active/active FireCluster cannot send IPv6 traffic through some Layer 3 routers or switches, including some Cisco models. *[76385]*
- A FireCluster failover is triggered if you change the name of an interface configured as part of a FireCluster. *[74669]*
- If you use the Firebox System Manager **Tools > Cluster > Leave** command to make a device leave a FireCluster, and then start the device in safe mode, the device cannot be discovered by the cluster master as a cluster member. *[72165]*

Workaround
Use the FireCluster management IP address to connect directly to the device and use the Firebox System Manager **Tools > Cluster > Join** command to rejoin the device to the cluster.

- 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]*
- In an active/active FireCluster, 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 onlywhen 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 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

- Logging does not work to a Log Server located at the remote end of a BOVPN virtual interface if there is no route for the return traffic.

> **Workaround**
> In the BOVPN virtual interface configuration, assign BOVPN virtual interface IP addresses. Or, use static or dynamic routing to make sure that each XTM device knows the routes to the local networks on the peer device.

- 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

- Mobile VPN with SSL users that authenticate with external authentication servers frequently disconnect and reconnect. *[77118]*
- When a VPN tunnel is first initiated, the XTM device incorrectly sends an "icmp destination unreachable" message back to the computer that initiated the tunnel. This does not affect the tunnel or traffic that uses the tunnel. *[72199]*
- 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. Web UI 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]*
- 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 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]*
- 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 you select the **VPN Settings > Enable the use of non-default (static or dynamic) routes to determine if IPSec is used** check box, and you have VPN failover configured, a failure of the external interface on either side of a branch office VPN tunnel can cause Dynamic Routes that overlap with the branch office VPN route to fail. *[76896]*
- WebBlocker override does not work through a BOVPN virtual interface. *[76007]*
- Logging does not work to a Log Server located at the remote end of a BOVPN virtual interface if there is no route for the return traffic.

> **Workaround**
> In the BOVPN virtual interface configuration, assign BOVPN virtual interface IP addresses. Or, use static or dynamic routing to make sure that each XTM device knows the routes to the local networks on the peer device.

- DHCP relay does not work through a BOVPN virtual interface. *[76816]*
- In a Branch Office VPN virtual interface configuration, if both the local and remote gateways are configured to use policy-based routing (with no zero route), traffic does not route correctly through the tunnel. *[76779]*
- Branch Office VPNs do not work correctly in this release if you enable FIPS mode on your XTM device. *[73154]*
- If you rekey a large number of BOVPN VIF tunnels at one time, it can take some time to complete the rekey of all tunnels. It does not happen instantly. *[75713]*
- 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]*
- 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]*
- 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).

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