Fireware v11.10 Beta 2 Release Notes

Supported Devices	XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 Firebox T10, Firebox M400, M440, and M500, XTMv, WatchGuard AP
Fireware OS Build	471928
WatchGuard System Manager Build	471146
WatchGuard AP Device Firmware	1.2.9.4 Build 150318
Release Notes Revision Date	19 March 2015

Introduction

WatchGuard is pleased to announce the Beta 2 release of Fireware v11.10 and WatchGuard System Manager v11.10. With Fireware v11.10, we add many new features to Fireware OS to make your firewall easier to set up and configure, and manage.

. Highlights include:

- Support for the use of fully qualified domain names (FQDN) as the source or destination in a policy, or blocked sites entry, including support for wildcards. (NEW in Beta 2!)
- Time and data quotas - Administrators can now set daily limits on the amount of time that users spend on Internet surfing each day and the amount of data/bandwidth that is used. With quotas, you can create an acceptable usage policy that is flexible and accommodates the needs of employees, but restricts Internet use to a reasonable amount.
- Expanded Gateway Wireless Controller functionality - Including Rogue AP detection, time-based configuration of wireless SSIDs, and more exposure for wireless activity in Dimension.
- Numerous ease-of-use improvements - New subscription service setup wizards in the Fireware Web UI, greatly improved VPN diagnostics

With Beta 2, we also offer an update to the WatchGuard AP device firmware, to v1.2.9.4 to resolve several stability and performance issues.

For information on the many feature updates in this release, as well as minor improvements and bug fixes, see the Enhancements and Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Fireware XTM v11.10, see the product documentation or review What's New in Fireware XTM v11.10, updated for Beta 2 to include information on the using FQDN in your firewall policies.

During beta testing, click Help anywhere in the product user interface to get access to updated documentation, or go to www.watchguard.com/help/docs/fireware/11/en-US/index.html.

Beta Notes

During beta testing, you may encounter certain known problems, including those shown below. If you need technical support or want to report a problem related to beta testing, you can open a support case through the usual channel and the case will not be counted against the case limit associated with your Firebox.

- From the Web UI Front Panel, or from FireWatch when launched from the Web UI, you cannot filter by domain names. *[84501, 84503]*
- When you add a domain name to the Blocked Sites list, all traffic destined for that domain is blocked, but traffic that originates from that domain is not blocked. *[84768]*
- Policies configured to use domain names as their source or destination may not correctly handle traffic during FireCluster formation. *[83780]*

Before You Begin

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

- A supported WatchGuard Firebox or XTM device. This device can be a WatchGuard Firebox T10, 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, Firebox M400. M500, M440, 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 Firebox or XTM device and the version of WSM installed on your Management Server.
- Feature key for your Firebox or XTM device — If you upgrade your device from an earlier version of Fireware XTM OS, you can use your existing feature key. If you do not have a feature key for your device, you can log in to the WatchGuard website to download it.

Note that you can install and use WatchGuard System Manager v11.10 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 Firebox or XTM physical device, make sure you use the instructions in the *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. During beta testing, click Help anywhere in the product user interface to get access to updated documentation, or go to www.watchguard.com/help/docs/fireware/11/en-US/index.html.

Localization

This release includes localized management user interfaces (WSM application suite and Web UI) current as of Fireware XTM v11.9.1. UI changes introduced since v11.9.1 remain in English. 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. 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.

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.

Dimension, WebCenter, Quarantine Web UI, and Wireless Hotspot

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

Fireware and WSM v11.10 Operating System Compatibility

Last revised: 15 February 2015

WSM/ Fireware XTM Component	Microsoft Windows 7, 8, 8.1 (32-bit & 64-bit)	Microsoft Windows Server 2008 & 2008 R2	Microsoft Windows Server 2012 & 2012 R2 (64-bit)	Mac OS X v10.9, v10.10	Android 4.x	iOS v7 & v8
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, see the Dimension Release Notes.*	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)		✓	✓			
Single Sign-On Client	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[1]		✓	✓			
Terminal Services Agent[2]		✓	✓			
Mobile VPN with IPSec	✓			✓ [3]	✓	✓ [3]
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.x support does not include Windows RT.*
- *Windows Server 2013 is supported if you install Windows Sever 2012 and .Net framework 3.5.*

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

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

[1] *Microsoft Exchange Server 2007, 2010, and 2013 are supported.*

[2] *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.*

[3] *Native (Cisco) IPSec client and OpenVPN are supported for Mac OS and iOS. For Mac OS X 10.8 -10.10, 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 iOS 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 Core or Xeon 2GHz	Intel Core or Xeon 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, 5.0, 5.1, or 5.5 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

You can download software from the WatchGuard Software Downloads Center.

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

WatchGuard System Manager

With this software package you can install WSM and the WatchGuard Server Center software:

`WSM11_10.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.10.

Fireware 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 or .vhd 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_10.exe` `xtm_xtm800_1500_2500_11_10.zip`
XTM 2050	`XTM_OS_XTM2050_11_10.exe` `xtm_xtm2050_11_10.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_10.exe` `xtm_xtm800_1500_2500_11_10.zip`
XTM 1050	`XTM_OS_XTM1050_11_10.exe` `xtm_xtm1050_11_10.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_10.exe` `xtm_xtm800_1500_2500_11_10.zip`
XTM 8 Series	`XTM_OS_XTM8_11_10.exe` `xtm_xtm8_11_10.zip`
Firebox M500 Series	`Firebox_OS_M400_M500_11_10.exe` `firebox_M400_M500_11_10.zip`
Firebox M440	`Firebox_OS_M440_11_10.exe` `firebox_M440_11_10.zip`
Firebox M400 Series	`Firebox_OS_M400_M500_11_10.exe` `firebox_M400_M500_11_10.zip`
XTM 330	`XTM_OS_XTM330_11_10.exe` `xtm_xtm330_11_10.zip`
XTM 33	`XTM_OS_XTM33_11_10.exe` `xtm_xtm33_11_10.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_10.exe` `xtm_xtm2a6_11_10.zip`
Firebox T10	`Firebox_OS_T10_11_10.exe` `firebox_T10_11_10.zip`

XTMv
All editions for VMware
	`xtmv_11_10.ova`
	`xtmv_11_10.exe`
	`xtmv_11_10.zip`

XTMv
All editions for Hyper-V
	`xtmv_11_10_vhd.zip`
	`xtmv_11_10.exe`
	`xtmv_11_10.zip`

Single Sign-On Software

These files are available for Single Sign-On. Most files are updated in this release.

- `WG-Authentication-Gateway_11_10.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_9_4.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_10.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_10.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_10.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_10.exe` (This installer includes both 32-bit and 64-bit file support and has been updated for this release.)

Mobile VPN with SSL Client for Windows and Mac

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

- `WG-MVPN-SSL_11_10.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_10.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download.

Shrew Soft Client

The Shrew Soft client is updated with this release.

- `Shrew Soft Client 2.2.2 for Windows` - No client license required.

WatchGuard IPSec Mobile VPN Clients

The Windows client has been updated for this release. There are now separate installation files for 32-bit and 64-bit Windows computers. You must uninstall the previous client before you install the new client. See What's New in Fireware v11.9.5 for information about the updated client software.

- `WatchGuard IPSec Mobile VPN Client for Windows (32-bit), 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 Windows (64-bit), 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 Mobile VPN License Server

- `WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP`- Click here for more information about MVLS.

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 v1.2.9.4 firmware when you upgrade your Firebox to Fireware v11.10 Beta 2.

Upgrade from Fireware v11.x to v11.10

Before you upgrade from Fireware v11.x to Fireware v11.10, download and save the Fireware OS file that matches the Firebox 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 Firebox 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 OS installed on your Firebox and the version of WSM installed on your Management Server. Also, make sure to upgrade WSM *before* you upgrade the version of Fireware OS on your FIrebox.

> If you use an XTM 5 Series or 8 Series device, you must upgrade to Fireware v11.7.4 or v11.7.5 before you can upgrade to Fireware v11.10.

> We recommend that you reboot your Firebox before you upgrade. While this is not necessary for most higher-model Firebox or XTM devices, a reboot clears your 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 Servers

It is not usually necessary to uninstall your previous v11.x server or client software when you update to WSM v11.10. You can install the v11.10 server and client software on top of your existing installation to upgrade your WatchGuard software components. We do, however, strongly recommend that you back up your WatchGuard Servers (for example: WatchGuard Log Server, WatchGuard Report Server, or WatchGuard Dimension Log Server) before you upgrade. You will need these backup files if you ever want to downgrade.

To back up your 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.

Upgrade to Fireware v11.10 from Web UI

1. Go to **System > Backup Image** or use the USB Backup feature to back up your current device image.
2. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads page.
   If you use the Windows-based installer on a computer with a Windows 64-bit operating system, this installation extracts an upgrade file called *[product series]_[product code].sysa-dl* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\Fireware\11.10\[model] or [model][product_code].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\Fireware\11.10
3. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the *[product series]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

Upgrade to Fireware v11.10 from WSM/Policy Manager v11.x

1. Select **File > Backup** or use the USB Backup feature to back up your current device image.
2. On a management computer running a Windows 64-bit operating system, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called *[Firebox or xtm series]_[product code].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\Fireware\11.10\[model] or [model][product_code].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\Fireware\11.10
3. Install and open WatchGuard System Manager v11.10. Connect to your Firebox and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[product series]_[product code].sysa-dl* file from Step 2.

Upgrade your FireCluster to Fireware XTM v11.10

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 or v11.7.5 before you can upgrade your FireCluster to Fireware XTM v11.9.x or higher.

> We recommend that you use Policy Manager to upgrade, downgrade, or restore a backup image to a FireCluster. It is possible to do some of these operations from the Web UI but, if you choose to do so, you must follow the instructions in the Help carefully as the Web UI is not optimized for these tasks. It is not possible to upgrade your FireCluster from v11.8.x to v11.9.x or higher with the Web UI.

Upgrade a FireCluster from Fireware XTM v11.4.x–v11.9.x to v11.10.x

Use these steps to upgrade a FireCluster to Fireware XTM v11.10.x:

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

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

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

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

Upgrade a FireCluster from Fireware XTM v11.3.x

To upgrade a FireCluster from Fireware XTM v11.3.x to Fireware XTM v11.9.x or higher, 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 v11.10 to WSM v11.x

If you want to revert from v11.10..x to an earlier version of WSM, you must uninstall WSM v11.10. 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 v11.10.

Next, install the same version of WSM that you used before you upgraded to WSM v11.10. 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 v11.10. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.10 to Fireware XTM v11.x

⚠ If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.10 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 v11.10 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 v11.10. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.10 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 *Fireware Help* for more information about these downgrade procedures, and information about how to downgrade if you do not have a backup image.

Downgrade Restrictions

Some downgrade restrictions apply:

- You cannot downgrade an XTM 2050 or an XTM 330 to a version of Fireware lower than v11.5.1.
- You cannot downgrade an XTM 25, 26, or 33 device to a version of Fireware lower than v11.5.2.
- You cannot downgrade an XTM 5 Series model 515, 525, 535 or 545 to a version of Fireware lower than v11.6.1.
- You cannot downgrade a Firebox T10 to a version of Fireware lower than v11.8.3. You cannot downgrade a Firebox T10-D to a version of Fireware lower than v11.9.3.
- You cannot downgrade a Firebox M440 to a version of Fireware lower than v11.9.2.
- You cannot downgrade a Firebox M400 or M500 to a version of Fireware lower than v11.9.4.
- You cannot downgrade XTMv in a VMware environment to a version of Fireware lower than v11.5.4.
- You cannot downgrade XTMv in a Hyper-V environment to a version of Fireware 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.

Enhancements and Resolved Issues in Fireware v11.10

General

- The features associated with Fireware Pro, such as Policy Based Routing, Server Load Balancing, and Dynamic Routing, now work correctly on the Firebox M400 and M500 models. *[83576]*
- This release patches the OpenVPN component to address vulnerability CVE-2014-8104. *[83478]*
- OpenSSL has been updated to version to 1.0.1j to address CVE-2014-3513. *[83498]*
- OpenSSL has been updated version to 1.0.1j to address POODLE vulnerability on TLS TA14-290A. *[83594]*
- This release updates the glibc component to apply the patch for the "GHOST" vulnerability (CVE-2015-0235). *[84277]*
- This release updates code related to Firebox and XTM wireless devices to improve stability. *[82920, 82705]*

User Interface and Centralized Management

- This release resolves an issue that prevented the Firebox DB users list from displaying correctly in the Web UI. *[82938]*
- This release resolves an issue that caused the wgagent process to crash and prevented management connections. *[83022]*
- The Web Setup Wizard now completes correctly when viewed in Japanese. *[83315]*
- This release adds Click Jacking and XFS protection to the Firebox XTM Web UI. *[84136]*
- This release resolves an issue that prevented all proxy rules from loading correctly after a reboot when the configuration contains a large number of policies. *[83413]*
- An issue has been resolved that caused Policy Manager to fail to save configurations after an upgrade to v11.94 with a log message that referred to “Java NullPointerException”. *[83483]*
- When using SSL Management Tunnels, the remote firewall now uses the IP address for the SSL Management Tunnel first when contacting the server. *[81377]*

Policies, Proxies, and Subscription Services

- You can enable time and bandwidth usage quotas for users on your network for access to external sites. *[67517]*
- Gateway Antivirus, Intrusion Prevention, spamBlocker, and WebBlocker services now have activation wizards that guide you through the steps to enables these services and provide a basic configuration. *[79956, 80001, 83539]*
- A deny action is now available for DLP email actions. *[78300]*
- The HTTPS SNI Block action no longer adds the host sending the traffic to the Blocked Sites list. *[83412]*
- HTTPS proxy exceptions for Content Inspection by Domain Name now correctly override rules for Content Inspection by WebBlocker category. *[83274]*
- This release resolves a problem that caused the *spamd* process to crash. *[82796]*
- This release resolves an issue that caused the *scand* process to crash when DLP is in use. *[83299]*
- This release resolves an issue that caused the proxy process to crash and restart. *[83225]*
- This release resolves an issue in the HTTPS proxy with Content Inspection, where HTTPS websites failed when the HTTPS client hello contained multiple TLS protocols. *[83510]*
- After changing the DNS server IP addresses on the Firebox, spamBlocker now correctly uses the new IP addresses for DNS lookups. *[83658]*

- This release resolves an HTTPS proxy crash. *[83619, 83943]*
- This release resolves an issue that caused the Gateway AV scanning process to crash. *[83282]*
- This release resolves a memory leak that occurred when the SMTP or POP3 proxy was configured to quarantine. *[83003, 82782]*
- This release resolves an issue that prevented a Gateway AV scan error from occurring on password-protected files. *[82925]*
- This release resolves an issue that caused the HTTPS proxy to crash when a connection to an external server fails. *[84320]*

Authentication & Guest Services

- You can now configure time and bandwidth quotas for guest services. *[82323]*
- RDP is now supported for Event Log Monitor (Clientless SSO) mode. *[67281]*
- Single-Sign On is now supported for zero-route BOVPN tunnel traffic so customers can now apply UTM security services more easily on their hub devices. *[41635]*
- Support for switching between multiple users of the SSO Client. *[68827]*
- SSO Exchange Monitor (EM) now supports Exchange Server 2013. *[80697]*
- The new logging and archiving functionality we added in Fireware v11.9.x is now available for the Mac SSO client. *[83468]*
- This release resolves a kernel crash that occurred when using the Hot Spot feature. *[83557]*

Certificates

- You can now perform all the same certificate management tasks from the Web UI as are available in Firebox System Manager. This includes the ability to view certificate details, delete, install, and export certificates, import CRLs, and create certificate signing requests. *[79898]*
- You can now update the CA certificate on your Firebox or XTM device from the Firebox System Manager > Certificates dialog box. *[64308]*
- Your Firebox or XTM device can automatically get new versions of the trusted CA certificates stored on the device and automatically install the new certificates. *[64308]*

Networking Updates

- You can now add up to three DHCP servers for IPv4 DHCP Relay. *[43897]*
- Firebox System Manager > Status Report now has just two route tables, IPv4 Routes and IPv6 Routes.You can filter the resultst to show the routing table by protocol, route type, interface and destination on both Web UI (System Status -> Routes) and CLI (show [v6] ip route). Only the first 100 entries will be shown for the filtered results. The previously available CLI command 'show route' is now obsolete. *[79076]*
- In the IPv6 settings for an external interface, you can now enable DHCPv6 Client Prefix Delegation on an external interface, and add a DHCPv6 prefix pool or a reserved prefix on an internal interface. With this change, we support both client and server for DHCPv6 Prefix Delegation. *[76623]*
- IPv6 traffic is now correctly handled if the option **Enable logging for traffic sent from this device** is enabled in v11.9.4. *[83419]*
- An external interface configured with PPPoE no longer reconnects for up to 5 minutes under certain conditions. *[83239]*
- This release resolves an issue that caused an interface to be incorrectly marked as “down” when using an active/active FireCluster. *[77202]*

VPN

- VPN diagnostic messages now appear below the branch office VPN gateway in WatchGuard System Manager, Firebox System Manager, and in the VPN Statistics page in the Fireware Web UI. The VPN diagnostic messages include information about why a VPN tunnel failed, and suggest an action to take to resolve the error. *[81287]*
- The VPN Diagnostic Report now shows the address pairs configured for the tunnel. *[79705]*
- The VPN Diagnostic Report now shows the policy checker results for policies that apply to each tunnel route. *[81575]*
- The VPN Diagnostic report now performs more checks to identify the most common VPN issues and includes a new *Conclusion* section that summarizes errors and suggests actions to take to resolve the error. The VPN Diagnostic report is also available in the VPN Statistics page in the Fireware Web UI. *[81286]*
- Mobile VPN with SSL clients for Mac and OS X now use OpenVPN 2.3.6. *[83352]*
- Traffic through a Branch Office VPN no longer fails after a tunnel rekey in some networks. *[82440]*
- This release resolves a crash with the *IKED* process that caused all IPSec VPN tunnels to renegotiate. *[83179]*
- This release resolves an issue that prevented large packets with the DF bit set to 1 from traversing through a Virtual Interface tunnel. *[82234]*
- This release resolves that caused the *IKED* process to crash and all BOVPN tunnels to fail. *[83584]*
- This release resolves a crash in the oss-daemon that caused all Mobile VPN with SSL tunnels to disconnect. *[83885]*

Wireless

- The Gateway Wireless Controller can detect rogue AP devices operating on your wireless network. You can enable rogue AP detection for each SSID, and view rogue AP devices in the Gateway Wireless Controller wireless maps feature. *[77186]*
- You can select multiple AP devices in the Gateway Wireless Controller dashboard page and Firebox System Manager Gateway Wireless Controller monitor page and perform specific actions (reboot, restart wireless, firmware upgrades) on multiple AP devices at the same time. *[77815]*
- In the Gateway Wireless Controller configuration, you can activate SSIDs for specific time periods. *[71806]*
- In the Gateway Wireless Controller configuration, you can enable wireless traffic shaping for each SSID. *[71611]*
- When you reboot an AP device, the configuration is automatically refreshed from the Gateway Wireless Controller to make sure the AP device has the latest configuration. *[71825]*
- In the Gateway Wireless Controller global settings, you can restart wireless services or reboot all of your AP devices at scheduled times on a daily or weekly basis. *[75225]*
- You can now view the signal strength of wireless clients in the Gateway Wireless Controller Dashboard page and Firebox System Manger Gateway Wireless Controller monitor page. *[81793]*
- Several new events from the Gateway Wireless Controller are now tracked in the logs, including AP device reboots, firmware upgrades, configuration updates, online/offline status, pairing status, and client connection events. *[79212]*
- You can now find access points that are not part of your network, and include only rogue access points in the Foreign BSSIDs list. *[77186]*
- You can review signal strength of connected wireless connections on the Wireless Clients tab in the

Gateway Wireless Controller. *[81793]*

- A wireless driver crash that caused all wireless traffic to fail has been resolved. *[82769]*

Logging, Reporting, and Monitoring

- You can now send log messages to two WatchGuard or Dimension Log Servers. *[81208]*
- FireWatch now supports full-screen mode. *[83474]*

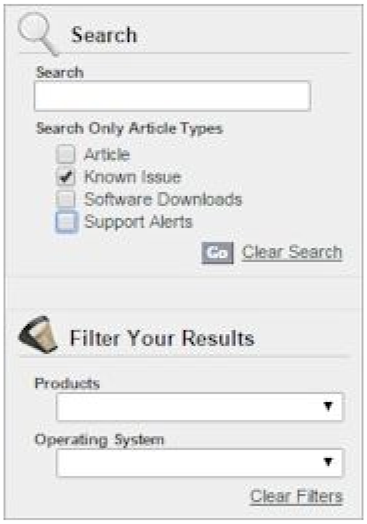
Other Enhancements

- If you use RapidDeploy, you can now use the rapid_ip.csv file on a USB drive to change the external interface to an interface other than eth0 on an appliance started with factory-default settings. *[78178]*
- After you enable the appliance to use NTP to synchronize the system time, you can enable the device as an NTP server. A policy called NTP Server is automatically created to allow connections to the NTP server from clients on the trusted and optional networks. *[79739]*
- The *WatchGuard System Manager Help* and *Fireware XTM Web UI Help* have been merged into a new *Fireware Help* system, available online or as a downloadable zip file only.

Known Issues and Limitations

Known issues for Fireware v11.9.x and its management applications, including workarounds where available, can be found in the WatchGuard Knowledge Base. Known Issues for this Beta release are included as Beta Notes in the Introduction section of these *Release Notes*.

Note that you must log in to the WatchGuard Portal to see Known Issues. Known Issues are not available in the public version of the Knowledge Base. We recommend that you use the filters available on the WatchGuard Portal > Knowledge Base tab to find Known Issues for this release.



Using the CLI

The Fireware XTM CLI (Command Line Interface) is fully supported for v11.x releases, but not yet updated for v11.10. 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. Any cases opened related to beta testing do not count against the case limit for your appliance.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375