Fireware v11.10.4 Release Notes

Supported Devices	Firebox T10, T30, T50, Firebox M200, M300, M400, M440, M500 XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 XTMv, WatchGuard AP
Release Date	23 November 2015
Fireware OS Build	490278
WatchGuard System Manager Build	488818
WatchGuard AP Device Firmware	1.2.9.5 Build 151030
Release Notes Revision Date	15 January 2016

Introduction

WatchGuard is pleased to announce the release of Fireware v11.10.4 and WatchGuard System Manager v11.10.4. The release includes many bug fixes and several feature enhancements, including:

- The SMTP Proxy can now be configured for actions based on the file names and file types that appear in compressed archive files, for example to block .exe files within zip archives
- Ability to disable the TLS v1.0 protocol for connections to your WSM Management Server and Log Server
- WSM Log Server can now automatically delete log messages after a specified amount of time
- Drag-and-drop policy ordering in Fireware Web UI
- Updated Mobile VPN with SSL client to support Max OS X 10.11 (El Capitan)
- XTMv support for VMware ESXi 6.0

To see more enhancements and bug fixes included in this release, see the Enhancements and Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Fireware v11.10.4, see the product documentation or review What's New in Fireware v11.10.4.

Important Information about Firebox Certificates

With Fireware v11.10.4, all newly generated default Firebox certificates use a 2048-bit key length. In addition, newly generated default Proxy Server and Proxy Authority certificates use SHA-256 for their signature hash algorithm.

To regenerate any default Firebox certificates, delete the certificate and reboot the Firebox.

To regenerate the default Proxy Authority and Proxy Server certificates without a reboot, you can use the CLI command: `upgrade certificate proxy`. If outbound HTTPS content inspection is enabled, you must redistribute the newly regenerated Proxy Authority certificate to your clients or users will receive web browser warnings when they browse HTTPS sites.

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, T30, T50, 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 M200, M300, 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 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 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 v11.10.4 and all WSM server components with devices running earlier versions of Fireware v11. In this case, we recommend that you use the product documentation that matches your Fireware 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. We also recommend that you review the Hardware Guide for your Firebox or XTM device model. The *Hardware Guide* contains useful information about your device interfaces, as well as information on resetting your device to factory default settings, if necessary.

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

Localization

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

- Simplified Chinese
- 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 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 v11.10.4 Operating System Compatibility

Last revised: 23 November 2015

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10 (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, v10.11	Android 4.x & 5.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 Exchange Server 2013 is supported if you install Windows Sever 2012 or 2012 R2 and .Net framework 3.5.*

The following browsers are supported for both Fireware Web UI and WebCenter (Javascript required):
- *IE 9 and later*
- *Microsoft Edge*
- *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, 6.5 and 7.6 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. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your Firebox or 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 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 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_4.exe — Use this file install WSM v11.10.4 or to upgrade WatchGuard System Manager from v11.x to WSM v11.10.4.

Fireware OS

Select the correct Fireware OS image for your Firebox or 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 Web UI. Use the .ova or .vhd file to deploy a new XTMv device.

If you have…	Select from these Fireware OS packages
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_11_10_4.exe` `xtm_xtm800_1500_2500_11_10_4.zip`
XTM 2050	`XTM_OS_XTM2050_11_10_4.exe` `xtm_xtm2050_11_10_4.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_10_4.exe` `xtm_xtm800_1500_2500_11_10_4.zip`
XTM 1050	`XTM_OS_XTM1050_11_10_4.exe` `xtm_xtm1050_11_10_4.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_10_4.exe` `xtm_xtm800_1500_2500_11_10_4.zip`
XTM 8 Series	`XTM_OS_XTM8_11_10_4.exe` `xtm_xtm8_11_10_4.zip`
Firebox M500 Series	`Firebox_OS_M400_M500_11_10_4.exe` `firebox_M400_M500_11_10_4.zip`
XTM 5 Series	`XTM_OS_XTM5_11_10_4.exe` `xtm_xtm5_11_10_4.zip`
Firebox M440	`Firebox_OS_M440_11_10_4.exe` `firebox_M440_11_10_4.zip`
Firebox M400 Series	`Firebox_OS_M400_M500_11_10_4.exe` `firebox_M400_M500_11_10_4.zip`
Firebox M300	`Firebox_OS_M200_M300_11_10_4.exe` `firebox_M200_M300_11_10_4.zip`
Firebox M200	`Firebox_OS_M200_M300_11_10_4.exe` `firebox_M200_M300_11_10_4.zip`
XTM 330	`XTM_OS_XTM330_11_10_4.exe` `xtm_xtm330_11_10_4.zip`
XTM 33	`XTM_OS_XTM3_11_10_4.exe` `xtm_xtm3_11_10_4.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_10_4.exe` `xtm_xtm2a6_11_10_4.zip`
Firebox T30	`Firebox_OS_T30_T50_11_10_4.exe` `firebox_T30_T50_11_10_4.zip`
Firebox T50	`Firebox_OS_T30_T50_11_10_4.exe` `firebox_T30_T50_11_10_4.zip`

WatchGuard Technologies, Inc.

If you have…	Select from these Fireware OS packages
Firebox T10	`Firebox_OS_T10_11_10_4.exe` `firebox_T10_11_10_4.zip`

XTMv
All editions for VMware
	`xtmv_11_10_4.ova`
	`xtmv_11_10_4.exe`
	`xtmv_11_10_4.zip`

XTMv
All editions for Hyper-V
	`xtmv_11_10_4_vhd.zip`
	`xtmv_11_10_4.exe`
	`xtmv_11_10_4.zip`

Single Sign-On Software

These files are available for Single Sign-On. Several files are updated with the v11.10.4 release.

- `WG-Authentication-Gateway_11_10_4.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_10.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_10.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_10_4.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_10_4.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_4.exe` (This installer includes both 32-bit and 64-bit file support.)

Mobile VPN with SSL Client for Windows and Mac

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

- `WG-MVPN-SSL_11_10_4.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_10_4.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download. There are no updates with the v11.10.4 release.

Shrew Soft Client

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

WatchGuard IPSec Mobile VPN Clients

- `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 have Gateway Wireless Controller configured to update devices automatically, any AP device which your Gateway Wireless Controller manages will be upgraded to v1.2.9.5 firmware (Build 151030) when you upgrade your Firebox to Fireware v11.10.4 for the first time. You can also upgrade the AP device software for an individual AP device from the Gateway Wireless Controller. If you want to update your WatchGuard AP devices manually without using the Gateway Wireless Controller, you can open the WatchGuard AP Software Download page and download the latest AP firmware and manually update your AP devices. We also provide the files to manually update the firmware for an unpaired AP device, if required. The file names for the most current AP firmware are:

- `AP100-v1.2.9.5.bin`
- `AP200-v1.2.9.5.bin`

Upgrade to Fireware v11.10.4

Before you upgrade to Fireware v11.10.x, your Firebox must be running:
 - Fireware XTM v11.7.5
 - Fireware XTM v11.8.4
 - Fireware XTM v11.9 or higher

If you try to upgrade from Policy Manager and your Firebox is running an unsupported version, the upgrade is prevented.

If you try to schedule an OS update of managed devices through a Management Server, the upgrade is also prevented.

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x before you upgrade to Fireware v11.10.x or your Firebox will be reset to a default state.

Before you upgrade from Fireware v11.x to Fireware v11.10.4, 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 want to upgrade an XTM 2 Series, 3 Series, or 5 Series device, we recommend that you reboot your Firebox before you upgrade. This clears your device memory and can prevent many problems commonly associated with upgrades in those devices.

Newer devices, such as the new Firebox T or Firebox M devices do not require a reboot to clear memory. With these devices, we have made improvements to the upgrade and backup processes to reduce memory use. It will, however, take up to two minutes longer to run the upgrade and backup processes on these devices.

Back up your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x server or client software when you upgrade to WSM v11.10.4. You can install the v11.10.4 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) 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.x from Web UI

If your Firebox is running Fireware v11.10 or later, you can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. If your Firebox is running v11.9.x or earlier, use these steps to upgrade:

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\FirewareXTM\11.10.4\[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\11.10.4
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.x from WSM/Policy Manager

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\11.10.4\[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\11.10.4

3. Install and open WatchGuard System Manager v11.10.4. 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 v11.10.4

Before you upgrade to Fireware v11.10.x, your Firebox must be running:
 - Fireware XTM v11.7.5
 - Fireware XTM v11.8.4
 - Fireware XTM v11.9 or higher

If you try to upgrade from Policy Manager and your Firebox is running an unsupported version, the upgrade is prevented.

If you try to schedule an OS update of managed devices through a Management Server, the upgrade is also prevented.

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x before you upgrade to Fireware v11.10.x or your Firebox will be reset to a default state.

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

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 v11.4.x–v11.9.x to v11.10.x

Use these steps to upgrade a FireCluster to Fireware 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 v11.3.x

To upgrade a FireCluster from Fireware v11.3.x to Fireware v11.9.x or higher, you must perform a manual upgrade. For manual upgrade steps, see the Knowledge Base article Upgrade Fireware OS for a FireCluster.

Downgrade Instructions

Downgrade from WSM v11.10.x 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.x. When you uninstall, choose **Yes** when the uninstaller asks if you want to delete server configuration and data files. After the server configuration and data files are deleted, you must restore the data and server configuration files you backed up before you upgraded to WSM v11.10.x.

Next, install the same version of WSM that you used before you upgraded to WSM v11.10.x. The installer should detect your existing server configuration and try to restart your servers from the **Finish** dialog box. If you use a WatchGuard Management Server, use WatchGuard Server Center to restore the backup Management Server configuration you created before you first upgraded to WSM v11.10.x. Verify that all WatchGuard servers are running.

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

If you use the Fireware Web UI or CLI to downgrade from Fireware v11.10.x to an earlier version, the downgrade process resets the network and security settings on your 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 v11.10.x to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v11.10.x. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v11.10.x to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device. This is not an option for XTMv users.

See the *Fireware Help* for more information about these downgrade procedures, and information about how to downgrade if you do not have a backup image.

WatchGuard Technologies, Inc.

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 T30 or T50 to a version of Fireware lower than v11.10.3 Update 1.
- You cannot downgrade a Firebox M200/M300 to a version of Fireware lower than v11.9.6.
- You cannot downgrade a Firebox M440 to a version of Fireware lower than v11.9.3.
- 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 OS on your Firebox or 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 OS.

Enhancements and Resolved Issues in Fireware v11.10.4

General

- You can now use Policy Manager to save a configuration file with a feature key to your XTMv virtual appliance if a feature key was not previously saved to the appliance. *[86170]*
- When an external host that matches an entry on your Blocked Sites Exceptions list triggers the Block Port Space Probe protection, the Firebox no longer blocks the host. *[86716]*
- You can now use Fireware Web UI to successfully import and export the Blocked Sites list. *[83013]*
- This release resolves several issues that resulted in the Firebox crashing and rebooting. *[87488,87076,87408]*
- This release resolves an issue that caused some syslog message facilities to be incorrectly categorized as mail. *[87285]*
- You can now save changes to network interface types when the Web UI is set to Japanese. *[85981]*
- Configuration changes to a Firebox M300 made with Policy Manager or the Web UI no longer fail to save with the error message "unable to set config <error> config/full failed <error>". *[86611]*
- You can now disable support for the TLSv1.0 protocol in the WatchGuard Management Server and Log Server to comply with PCI DSS 3.1 requirements. *[86914]*
- WatchGuard Server Center now uses the SHA-256 algorithm to sign newly generated self-signed certificates. *[87246]*
- The Firebox now generates its default self-signed certificates using a 2048-bit key. *[81445] [81444]*
- The Java Runtime Environment packaged with WatchGuard System Manager has been updated to 8.0_u51. *[86155]*
- This release resolves an issue that caused the default "unhandled packet" deny policy to take precedence over user configured policies, usually after a configuration change was made using Manual Policy Order mode. When this issue occurred, all policies below the "unhandled packet" policy were ignored and the connection denied. While the changes in v11.10.4 prevent this issue from occurring, it will not fix the issue if the invalid policy ordering has already occurred. To resolve the issue, upgrade to Fireware v11.10.4, change the configuration mode from Manual to Auto-Order, then change back to Manual Order mode. You can then change the order of the policies. *[88005, 80932]*
- An issue that caused a CPU lockup on Firebox M200 devices has been resolved. *[87053, 87149]*

Networking

- When your Firebox has multiple interfaces configured with a DHCP relay to the same server IP address, each individual DHCP request no longer causes the Firebox to send multiple DHCP requests -- one for each relay. *[87890]*
- Resolved an issue that caused increased CPU usage by the 'wgif_static' process on the backup member of an active/passive FireCluster. *[86521]*
- Firebox M440 appliances configured to use a 100 Mbps full duplex link configuration no longer fail to pass traffic at full speed to some third party switches. *[87012]*
- An issue that caused the "homer" process to crash in FireCluster configurations on XTM 800 Series devices has been resolved. *[86245]*
- The Firebox now correctly removes the old default gateway from the routing table when you configure a new default gateway for an external network interface. *[86963]*
- This release resolves an issue with support for the Sierra Wireless Aircard 320U that caused DHCP failure after failover. *[87274]*

- This release resolves a regex VLAN issue with access point configuration where VLAN X0 and VLAN X were being processed as the same VLAN ID. *[86241]*
- The Firebox now respects the interface order in the Multi-WAN Failover settings when a failover occurs. *[87355]*
- An issue that caused incorrect Multi-WAN behavior for Multi-WAN modes other than Failover mode with dynamic external IP addresses (PPPoE/DHCP) has been resolved *[73679]*
- When a BOVPN tunnel is configured to allow broadcast traffic, the Unhandled External Packets policy no longer denies Traffic for the 255.255.255.255 broadcast address. *[79866]*
- In Fireware Web UI you can now select the secondary IP address of a link aggregation interface in a static NAT action. *[87177]*

Logging and Reporting

- Events such as a BOVPN Failover on a FireCluster no longer generate log messages from both cluster members. *[87201]*

Authentication

- When you enable the Authentication Redirect feature, users that connect from behind a Custom interface are now correctly redirected for authentication. *[86324]*
- When you configure your WSM Management Server to validate the domain controller's SSL certificate for Active Directory Authentication, certificate validation no longer fails if the Active Directory server has a certificate with an RSASSA-PSS signature. *[80147]*
- This release resolved an issue that prevented domain users from being authenticated with SSO when logged in to a host running Windows 10. *[86926]*
- This release resolves an issue that prevented user authentication through SSO and Exchange Monitor in environments that use Exchange 2013 on Windows Server 2012 R2. *[87326]*

VPN

- This release includes an updated Mobile VPN with SSL Mac client that supports Mac OS X v10.11 (El Capitan). *[87413]*
- Resolved an issue that caused the BOVPN Virtual Interface to fail when the FireCluster Master reboots. *[85957]*
- Managed BOVPN tunnels and Management Tunnels are now correctly configured for VPN failover when both Firebox devices use Multi-WAN. *[83771]*
- The Mobile VPN with SSL client now correctly updates the DNS server addresses on German and Finnish versions of Windows. *[86629]*
- The Mobile VPN with SSL uninstaller for Mac OS X now correctly removes the Mobile VPN with SSL application directory *[87566]*

Proxies and Subscription Services

- DLP signatures now include:
    - Norwegian national identification number *[75405]*
    - Netherlands national identification number (BSN) *[75401]*
- Active FTP connections through the FTP Proxy no longer disconnect and time out if a user tries to access an empty folder. *[87027]*
- This release resolves an issue that caused the proxy process to leak memory when APT or WebBlocker is enabled. *[87792]*
- A proxy memory leak has been resolved. *[87377]*
- Specific proxy connections are now correctly removed from the proxy connection table. *[84436,87623]*

- Several proxy process crashes have been fixed in this release. *[87233,87356,87187,87192]*
- APT Blocker now correctly submits and tracks individual files when compressed in a single archive. *[86959]*
- The file name field inside the proxy deny message now contains the correct file extension. *[87041]*
- The SMTP proxy Content Type and Filename rules now apply to files found during archive decompression. *[77161]*
- The Quarantine Server now correctly decodes certain messages and allows them to be viewed and released. *[85303]*
- Quarantine Server user notification no longer fails when it decodes a subject header that contains a backslash character. *[85341]*
- The TCP timestamp option has been disabled for HTTP/HTTPS Proxy traffic after slow website access was observed when using an active/active FireCluster. *[85915]*
- The HTTPS proxy no longer accepts RC4-based cipher suites when it negotiates TLS encryption for Deep Inspection. [86700]

WatchGuard AP

- WatchGuard AP firmware has been updated to v1.2.9.5, with updates to country-specific operating parameters and radio performance improvements.
- This release resolves a conflict on AP10x/AP200 devices with the association handling function that caused client disconnections. *[87170]*
- WatchGuard AP devices no longer support RC4-based cipher suites for connections to the AP web UI. *[86023]*
- WatchGuard AP devices now support TLSv1.1 and TLSv1.2 for connections to the AP web UI. *[86464]*
- The OpenSSL library used on the WatchGuard AP devices has been updated to version 1.0.1p to address CVE-2014-0224 *[85127]*
- The lighttpd version used on the WatchGuard AP devices has been updated to 1.4.35 to address multiple security advisories. [85173]
- SNMP is no longer enabled by default on WatchGuard AP devices. *[85181]*
- WatchGuard AP devices now generate the default self-signed certificates using a 2048-bit key. *[85243]*

Known Issues and Limitations

Known issues for Fireware v11.10.4 and its management applications, including workarounds where available, can be found on the WatchGuard website. To see Known Issues, log in to the WatchGuard website and use the filters available on the Technical Search > Knowledge Base tab.

Using the CLI

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

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