Fireware v11.11.4 Update 2 Release Notes

Supported Devices	Firebox T10, T30, T50, T70, M200, M300, M400, M440, M500, M4600, M5600 XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 XTMv, WatchGuard AP
Release Date:	Fireware v11.11.4: 20 September 2016 Fireware v11.11.4 Update 1: 29 September 2016 Fireware v11.11.4 Update 2: 26 October 2016
Fireware OS Build	Fireware v11.11.4: 511928 Fireware v11.11.4 Update 1: 513167 Fireware v11.11.4 Update 2: 514824
WatchGuard System Manager Build	511291
WatchGuard AP Device Firmware	For AP 100, 102, 200: Build 1.2.9.9 For AP 300: Build 2.0.0.4
Release Notes Revision Date	31 October 2016

Introduction

On 26 October, we released Fireware v11.11.4 Update 2, which replaces v11.11.4 Update 1 for all customers. This maintenance update fixes numerous bugs, as described in the Resolved Issues in Fireware v11.11.4 Update 2 section of these release notes. This release includes the updated AP300 software that was released with Update 1.

Since the original release of Fireware v11.11.4, we have also released Mobile VPN with IPSec client software for Windows and Mac (powered by NCP). See Enhancements and Resolved Issues for more information about this new client.

There is no update for WatchGuard System Manager, which remains at v11.11.4.

WatchGuard is pleased to announce the release of Fireware v11.11.4 and WatchGuard System Manager v11.11.4. This release provides a localization update for the user interface, updating the localization of WatchGuard System Manager and Fireware Web UI to match Fireware v11.11 functionality for our French, Japanese, and Spanish (LA) users. The release also includes many bug fixes, updated AP firmware for AP 100/102/200/300 devices, and several small feature enhancements

Proxy Enhancements

- Perfect Forward Secrecy (PFS) is now supported in the SMTP and HTTPS proxies.
- POP3 proxy can now block files by extension within a ZIP or GZIP compressed archive file.
- Because of security vulnerabilities, SSLv2 is considered a non-compliant SSL protocol in Fireware v11.11.1 and higher. However, because some applications, such as Skype, require SSLv2, the HTTPS proxy can now be configured to allow SSLv2 traffic if necessary. For more information, see What's New in Fireware v11.11.4.

Gateway Wireless Controller (GWC) Enhancements

- You can now reset AP devices directly from GWC.
- You can now remove AP firmware from your Firebox with GWC.

Enhancements for WatchGuard Wi-Fi Cloud

- Domain names for WatchGuard Wi-Fi Cloud services are now included by default in the HTTP Proxy Exceptions and HTTPS Proxy Domain Names lists.
- A new packet filter template, *WG-Cloud-Managed-WiFi*, is available for WatchGuard Wi-Fi Cloud AP management to open the required ports to enable AP devices to communicate with cloud services.

Other Enhancements

- You can now select an IPSec VPN certificate that does not include an Extended Key Usage (EKU) identifier.
- This release also includes support for the new Firebox T70.

For more information on the bug fixes and enhancements in this release, see the Enhancements and Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Fireware v11.11.4, see the product documentation or review What's New in Fireware v11.11.4.

Important Information about Firebox Certificates

SHA-1 is being deprecated by many popular web browsers, and WatchGuard recommends that you now use SHA-256 certificates. Because of this, we have upgraded our default Firebox certificates. Starting 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. Starting with Fireware v11.10.5, all newly generated default Firebox certificates use SHA-256 for their signature hash algorithm. New CSRs created from the Firebox also use SHA-256 for their signature hash algorithm.

Default certificates are not automatically upgraded after you install Fireware v11.10.5 or later releases.

To regenerate any default Firebox certificates, delete the certificate and reboot the Firebox. If you want to regenerate default certificates without a reboot, you can use the CLI commands described in the next section. Before you regenerate the Proxy Server or Proxy Authority certification, there are some important things to know.

The Proxy Server certificate is used for inbound HTTPS with content inspection and SMTP with TLS inspection. The Proxy Authority certificate is used for outbound HTTPS with content inspection. The two certificates are linked because the default Proxy Server certificate is signed by the default Proxy Authority certificate. If you use the CLI to regenerate these certificates, after you upgrade, you must redistribute the new Proxy Authority certificate to your clients or users will receive web browser warnings when they browse HTTPS sites, if content inspection is enabled.

Also, if you use a third-party Proxy Server or Proxy Authority certificate:

- The CLI command will not work unless you first delete either the Proxy Server or Proxy Authority certificate. The CLI command will regenerate both the Proxy Server and Proxy Authority default certificates.
- If you originally used a third-party tool to create the CSR, you can simply re-import your existing third-party certificate and private key.
- If you originally created your CSR from the Firebox, you must create a new CSR to be signed, and then import a new third-party certificate.

CLI Commands to Regenerate Default Firebox Certificates

To regenerate any default Firebox certificates, delete the certificate and reboot the Firebox. If you want to regenerate default certificates without a reboot, you can use these CLI commands:

- To upgrade the default Proxy Authority and Proxy Server certificates for use with HTTPS content inspection, you can use the CLI command: `upgrade certificate proxy`
- To upgrade the Firebox web server certificate, use the CLI command: `upgrade certificate web`
- To upgrade the SSLVPN certificate, use the CLI command: `upgrade certificate sslvpn`
- To upgrade the 802.1x certificate, use the CLI command: `upgrade certificate 8021x`

For more information about the CLI, see the Command Line Interface Reference.

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, T70, 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, M4600, M5600, 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 v11.11.x 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 updated localized management user interfaces (WSM application suite and Web UI) current as of Fireware v11.11. UI changes introduced since v11.11 may remain in English. Supported languages are:

- 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.

Documentation

Localization updates are also available for *Fireware Help*, available on the WatchGuard website or as context-sensitive Help from the localized user interfaces.

Fireware and WSM v11.11.4 Operating System Compatibility

Last revised: 30 September 2016

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 & v10.12	Android 4.x & 5.x	iOS v7, v8, v9, & v10
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 11 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 -10.12, 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 5.0, 5.1, 5.5, or 6.0 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

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_11_4.exe` — Use this file to install WSM v11.11.4 or to upgrade WatchGuard System Manager from v11.x to WSM v11.11.4. There are no updates available for WSM.

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
Firebox M5600	`Firebox_OS_M4600_M5600_11_11_4.exe` `firebox_M4600_M5600_11_11_4.zip`
Firebox M4600	`Firebox_OS_M4600_M5600_11_11_4.exe` `firebox_M4600_M5600_11_11_4.zip`
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_11_11_4.exe` `xtm_xtm800_1500_2500_11_11_4.zip`
XTM 2050	`XTM_OS_XTM2050_11_11_4.exe` `xtm_xtm2050_11_11_4.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_11_4.exe` `xtm_xtm800_1500_2500_11_11_4.zip`
XTM 1050	`XTM_OS_XTM1050_11_11_4.exe` `xtm_xtm1050_11_11_4.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_11_4.exe` `xtm_xtm800_1500_2500_11_11_4.zip`
XTM 8 Series	`XTM_OS_XTM8_11_11_4.exe` `xtm_xtm8_11_11_4.zip`
Firebox M500 Series	`Firebox_OS_M400_M500_11_11_4.exe` `firebox_M400_M500_11_11_4.zip`
XTM 5 Series	`XTM_OS_XTM5_11_11_4.exe` `xtm_xtm5_11_11_4.zip`
Firebox M440	`Firebox_OS_M440_11_11_4.exe` `firebox_M440_11_11_4.zip`
Firebox M400 Series	`Firebox_OS_M400_M500_11_11_4.exe` `firebox_M400_M500_11_11_4.zip`
Firebox M300	`Firebox_OS_M200_M300_11_11_4.exe` `firebox_M200_M300_11_11_4.zip`
Firebox M200	`Firebox_OS_M200_M300_11_11_4.exe` `firebox_M200_M300_11_11_4.zip`
XTM 330	`XTM_OS_XTM330_11_11_4.exe` `xtm_xtm330_11_11_4.zip`
XTM 33	`XTM_OS_XTM3_11_11_4.exe` `xtm_xtm3_11_11_4.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_11_4.exe` `xtm_xtm2a6_11_11_4.zip`
Firebox T70	`Firebox_OS_T70_11_11_4.exe` `firebox_T70_11_11_4.zip`
Firebox T50	`Firebox_OS_T30_T50_11_11_4.exe` `firebox_T30_T50_11_11_4.zip`

If you have…	Select from these Fireware OS packages
Firebox T30	Firebox_OS_T30_T50_11_11_4.exe firebox_T30_T50_11_11_4.zip
Firebox T10	Firebox_OS_T10_11_11_4.exe firebox_T10_11_11_4.zip
XTMv All editions for VMware	xtmv_11_11_4.ova XTM_OS_XTMv_11_11_4.exe xtm_xtmv_11_11_4.zip
XTMv All editions for Hyper-V	xtmv_11_11_4_vhd.zip XTM_OS_XTMv_11_11_4.exe xtm_xtmv_11_11_4.zip

Single Sign-On Software

These files are available for Single Sign-On. There are no updates with this release.

- WG-Authentication-Gateway_11_11_2.exe (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- WG-Authentication-Client_11_11.msi (SSO Client software for Windows)
- WG-SSOCLIENT-MAC_11_11_2.dmg (SSO Client software for Mac OS X)
- SSOExchangeMonitor_x86_11_11_2.exe (Exchange Monitor for 32-bit operating systems)
- SSOExchangeMonitor_x64_11_11_2.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_11.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. There are no updates with this release.

- WG-MVPN-SSL_11_11_2.exe (Client software for Windows)
- WG-MVPN-SSL_11_11.dmg (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download.

Shrew Soft Client

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

WatchGuard IPSec Mobile VPN Clients

The current WatchGuard IPSec Mobile VPN Client is version 12.10. All clients were updated with the Fireware v11.11.4 Update 1 release.

- 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.

Upgrade to Fireware v11.11.4 Update 2

Before you upgrade to Fireware v11.11.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, or v11.10.x before you upgrade to Fireware v11.11.x or your Firebox will be reset to a default state.

Before you upgrade from Fireware v11.x to Fireware v11.11.4 Update 2, 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.

Upgrade Notes for XTMv

For Fireware v11.11 and higher, the XTMv device is a 64-bit virtual machine. You cannot upgrade an XTMv device from Fireware v11.10.x or lower to Fireware v11.11 or higher. Instead, you must use the OVA file to deploy a new 64-bit Fireware v11.11.x XTMv VM, and then use Policy Manager to move the existing configuration from the 32-bit XTMv VM to the 64-bit XTMv VM. For more information about how to move the configuration, see *Fireware Help*. For more information about how to deploy a new XTMv VM, see the latest *WatchGuard XTMv Setup Guide* available on the product documentation page at http://www.watchguard.com/wgrd-help/documentation/xtm. When your XTMv instance has been updated to v11.11 or higher, you can then use the usual upgrade procedure, as detailed below.

WatchGuard updated the certificate used to sign the .ova files with the release of Fireware v11.11. When you deploy the OVF template, a certificate error may appear in the OVF template details. This error occurs when the host machine is missing an intermediate certificate from Symantic (Symantec Class 3 SHA256 Code Signing CA), and the Windows CryptoAPI was unable to download it. To resolve this error, you can download and install the certificate from Symantec.

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 v11.11.4. You can install the v11.11.4 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) to a safe location 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 v11.11.x from Web UI

If you have already installed Fireware v11.11.4 on your computer, you must run the Update 2 installer twice (once to remove v11.11.4 and again to install v11.11.4 Update 2).

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\11.11.4U2\[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\11.11.4U2
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 v11.11.x from WSM/Policy Manager

If you have already installed Fireware v11.11.4 on your computer, you must run the Update 1 installer twice (once to remove v11.11.4 and again to install v11.11.4 Update 2).

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\11.11.4U2\[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\11.11.4U2.
3. Install and open WatchGuard System Manager v11.11.4. 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.

Update AP Devices

On 29 September, we released Fireware v11.11.4 Update 1. This update contains new AP 300 firmware to resolve an issue that caused some AP300 devices to take a long time to reboot. The AP 300 firmware is updated from v2.0.0.4 build 160830 to v2.0.0.4 build 160923.

With the release of Fireware v11.11.4 we are releasing new AP firmware for all AP devices. The process to update to new AP firmware has changed. Please review this section carefully for important information about updating AP devices.

Update your AP100, AP102, and AP200 Devices

Fireware v11.11.4 includes new AP firmware v1.2.9.9 for AP100/102 and AP200 devices. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 or v11.10.5 to Fireware v11.11.x, your AP devices are automatically updated between midnight and 4:00am local time. You can also see and use the new feature to check for and download AP firmware updates to Gateway Wireless Controller for future updates.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.11.x (without first upgrading to Fireware v11.10.4 or v11.10.5), there is an additional step you must take to make sure AP v1.2.9.9 is applied to your AP devices. When you upgrade to Fireware v11.11.x with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the **Gateway Wireless Controller > Summary** tab, select **Check for Updates** to download the latest AP firmware to the Firebox.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. From the **Gateway Wireless Controller > Summary** tab, select **Check for Updates** to download the latest AP firmware to the Firebox again.

You cannot install the AP firmware on a Firebox that uses Fireware v11.4.x or lower. If you try to install the AP Component Package on a Firebox that uses Fireware v11.4.x or lower, the package appears to install successfully, but the AP firmware is not installed and log messages show that the packet installation was aborted.

Update your AP300 Devices

Update from v2.0.0.3 and earlier

Fireware v11.11.4 includes AP firmware v2.0.0.4. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 or v11.10.5 to Fireware v11.11.x, your AP devices will be automatically updated between midnight and 4:00am local time. You can also see and use the new feature to check for and download AP firmware updates directly from Gateway Wireless Controller.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.11.x (without first upgrading to Fireware v11.10.4 or v11.10.5), there is an additional step you must take to make sure AP v2.0.0.4is applied to your AP devices. When you upgrade to Fireware v11.11.x with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the **Gateway Wireless Controller > Summary** tab, select **Check for Updates** to download the latest AP firmware to the Firebox.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. From the **Gateway Wireless Controller > Summary** tab, select **Check for Updates** to download the latest AP firmware to the Firebox again.

Update from v2.0.0.4 to an updated v2.0.0.4 build

If you have already upgraded to Fireware v11.11.4 and you have already updated your AP300 devices to AP firmware v2.0.0.4, the automatic firmware update feature may not work to install the newer build of AP firmware v2.0.0.4 that we are releasing with Fireware v11.11.4 Update 1. To upgrade, use the Gateway Wireless Controller tab in Firebox System Manager, or the Gateway Wireless Controller dashboard in the Web UI.

Upgrade your FireCluster to Fireware v11.11.x

Before you upgrade to Fireware v11.11 or higher, 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 v11.11.x or your Firebox will be reset to a default state.

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 this Knowledge Base article.

You can upgrade Fireware OS for a FireCluster from Policy Manager or Fireware Web UI. To upgrade a FireCluster from Fireware v11.10.x or lower, we recommend you use Policy Manager.

As part of the upgrade process, each cluster member reboots and rejoins the cluster. Because the cluster cannot do load balancing while a cluster member reboot is in progress, we recommend you upgrade an active/active cluster at a time when the network traffic is lightest.

For information on how to upgrade your FireCluster, see this Help topic.

Downgrade Instructions

Downgrade from WSM v11.11.4 to WSM v11.x

If you want to revert from v11.11.4 to an earlier version of WSM, you must uninstall WSM v11.11.4. 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 v11.11.4.

Next, install the same version of WSM that you used before you upgraded to WSM v11.11.4. 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 v11.11.4. Verify that all WatchGuard servers are running.

Downgrade from Fireware v11.11.4 or v11.11.4 Update 2 to Fireware v11.x

If you use the Fireware Web UI or CLI to downgrade from Fireware v11.11.4 or v11.11.4 Update 2 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 v11.11.4 or v11.11.4 Update 2 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v11.11.4. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v11.11.4 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

See this Knowledge Base article for a list of downgrade restrictions.

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.

Resolved Issues in Fireware v11.11.4 Update 2

General

- The Gateway Wireless Controller dashboards now correctly populate data in Firebox System Manager and the Web UI for a large number of AP devices. *[92129]*
- This release resolves an XSS vulnerability in the logon disclaimer configuration of the Web UI. *[92288]*
- This release resolves a rare occurrence of the compact flash card on the Firebox M400, M500 and M440 becoming unreadable, resulting in the Firebox no longer passing traffic. *[90957]*
- You can now use the Server Load Balancing feature on Firebox T30, T50 and T70 appliances. *[92081*
- Firebox feature keys can now be successfully updated from Dimension. *[92046*
- Domain names from HTTP and HTTPS proxy policies now display correctly in Fireware Web UI Front Panel. *[91851]*

Networking

- This release resolves an issue that caused the Firebox to send ARP packets with zeros as MAC addresses within the Ethernet Frame. *[92276]*
- When your Firebox is configured with multiple external interfaces, a reboot no longer causes an interface to be marked as failed. *[91997]*

Logging

- Log messages generated by spamBlocker Virus Outbreak Detection are now marked with a VOD tag. *[91398]*
- The FireCluster Backup Master no longer generates the log message: `Couldn't resolve host 'analysis.lastline.com'`. *[91921]*
- The unnecessary log message `fwsess_event: Unable to process notification event due to missing IP address or inter` is now suppressed and no longer appears in log files. *[91785]*
- Email notifications for Blocked Port events now include the detected port instead of a system variable. *[91798]*
- The syslog event length has been extended to 2048 bytes. *[91878]*
- The FireCluster Backup Master no longer generates the log message: `sessiond CLST: failed to sync sess idle timeout msg to remote box`. *[85119]*

Authentication

- If you log in to a Terminal Server with the Authentication applet using the TO Agent, you can now successfully log out with the Authentication applet. *[91879]*
- You can now see the **Log Out** option on the Authentication applet when you use the option to **Send a redirect to the browser after successful authentication**. *[91884]*

VPN

- When you create a VPN between a Firebox and a Yamaha router, you no longer see an error when the Yamaha router initiates a Phase 2 rekey. *[77071]*

Enhancements and Resolved Issues in Fireware v11.11.4

General

- This release includes a localization update for WatchGuard System Manager and Fireware Web UI to match Fireware v11.11 functionality for our French, Japanese, and Spanish (LA) users.
- This release resolves a kernel crash on Firebox M400 and M500 appliances when using IPSec VPNs. *[90930]*
- This release includes multiple updates to the lighttpd service used by the Firebox web server to ensure best cipher suite compatibility with modern web browsers. *[91311]*
- This release resolves an issue that prevented changes from saving correctly from Fireware Web UI when using the localized French interface. *[92008]*
- Several Fireware Web UI pages have been updated to guard against XSS injection attempts. *[86039]*
- The Fireware Web UI Configuration Report now correctly displays all ports and protocols for a firewall policy when multiple ports and protocols are configured. *[91347]*

Proxies and Security Subscriptions

- The SMTP and HTTPS proxy now support Perfect Forward Secrecy (PFS). *[82389, 90567]*
- The HTTPS-proxy log messages now contain application identification information when Content Inspection is not enabled. *[87532]*
- For a new WebBlocker action, the **Log this action** option is now always enabled by default. *[89834, 91177]*
- The HTTPS proxy no longer crashes when Content Inspection is enabled and an HTTPS request is sent that uses an unsupported cipher. *[91455]*
- This release resolves an issue introduced in Fireware v11.11.1 that prevented traffic from passing through a proxy policy if the receiving interface has an MTU set below 1500. *[91761]*
- This release resolves an issue that caused some unhandled denied traffic to show as *allowed* in the traffic log message even though the traffic was denied. *[91566]*
- Mobile Security trial licenses now work correctly. *[91754]*
- The POP3 proxy now provides the ability to detect file extensions inside compressed attachments. *[89078]*
- This release improves the proxy detection of Visual Basic Script macros inside of Microsoft Office documents. *[91388]*
- This release resolves an issue that occurred when you edit an existing Explicit Proxy action where Content Inspection is not enabled in CONNECT Tunneling. *[91887]*
- The SMTP proxy Return-Receipt-To header rule now correctly matches the header field name. *[91504]*
- POP3 proxy log messages now correctly include the **User** field. *[91493]*
- HTTP Proxy Exceptions now save correctly from the French localized Fireware Web UI. *[92008]*
- The SIP ALG no longer crashes when referencing a pointer to a proxy connection structure that has already been freed and is no longer valid. *[91563]*
- This release updates the proxy handling of SSLv2 traffic. SSLv2 traffic will now pass through the HTTPS-Proxy if **Allow only SSL compliant traffic** is not enabled and Content Inspection is disabled. *[91749]*
- SSL unknown protocol event log messages no longer occur when incomplete SSL authentication connections are closed by the Firebox. An example of those log messages looks like this: *SSL:1 error;140760FC:SSL routines;SSL23_GET_CLIENT_HELLO;unknown protocol*. *[91641]*

- The proxy will now classify documents containing a file description of 'Microsoft OOXML' as mime-type 'application/vnd.openxmlformats-officedocument' when no definite mime-type exists within the file. *[91853]*
- This release resolves an issue that caused the file scanning process (scand) to crash. *[89261]*
- APT Blocker notification logging has been improved to more consistently capture the analysis results for files submitted to the Lastline data center's next-generation sandbox. *[91301]*
- The correct set of DLP content rules is now displayed in Policy Manager for Firebox M200 and M300 appliances. *[91044]*
- APT Blocker reports no longer include information about clean objects in their summary details. *[91628]*
- The Firebox Configuration Report now correctly displays Denied WebBlocker categories when using the Websense Cloud. *[91190]*
- New WebBlocker profiles created manually in Policy Manager now have **Log this action** enabled by default for WebBlocker categories. *[89834]*

Networking

- This release resolves an issue that prevented DHCP relay from working correctly through a Branch Office Virtual Interface (VIF) tunnel when PPPoE is enabled. *[91515]*
- This release resolves an issue that prevented traffic from correctly matching a policy configured with FQDN in the **From** field when the Terminal Services Agent is also in use. *[91583]*
- This release resolves an issue that caused low throughput for Tagged VLAN traffic on Firebox M200 and M300 appliances. *[90500]*
- The throughput of the Firebox built-in wireless interfaces is no longer limited to 56 Mbps when Traffic Management and QoS features are enabled. *[90954]*
- A Japanese localization issue related to configuring NTP from Policy Manager has been resolved in this release. *[72923]*
- An issue has been resolved that caused the error *Internal_Error: Unable to set config* to display when saving a configuration from Policy Manager. *[88214]*
- Internet traffic is no longer allowed after you remove the 0.0.0.0/0 and Any-External entries from Mobile VPN with IPSec policies. *[90205]*
- The Firebox no longer requires a restart when you change the dynamic NAT value in a BOVPN tunnel configuration. *[82116]*
- Policy Manager no longer accepts invalid SNAT configurations created when you upgrade older configuration files to WSM v11.10.7 or higher. *[90874]*
- This release corrects an issue that caused SFP load failures for Olink adapters. *[91844]*
- When a configuration is saved that uses many nested aliases, firewall policies no longer take several minutes to correctly handle network traffic. *[91078]*
- This release resolves an issue that resulted in the default *Unhandled External Packet-00* policy to be ordered incorrectly in the firewall policy list, denying legitimate traffic. *[91514]*
- This release resolves an issue that caused upgrades to fail when DNS forwarding is enabled. *[91753]*

Authentication

- You can now use certificates without IKE/IPSec extended key usage for certificate authentication of BOVPN tunnels. *[81227]*
- This release resolves a crash in the authentication process (admd) that occurred when you disabled the custom logo for hotspot authentication. *[91302]*

VPN

- WatchGuard System Manager now displays all active SSL VPN Management Tunnels above the section that shows inactive connections. *[85587]*
- PPPoE link stage changes no longer affect VIF VPN tunnels. *[91272]*
- With the release of Fireware v11.11.4 Update 1, we also released an update to the WatchGuard Mobile VPN with IPSec client software for Windows, powered by NCP. This v12.1 client resolves several issues:
  - This release resolves a problem that caused client licenses to become inactive after the device was restarted.
  - After installing or updating the NCP client, the network connection is now available immediately, with no restart required..
  - A problem that caused a blue-screen error when leaving hibernation mode when the Wi-Fi Manager was active has been resolved.

FireCluster

- This release resolves a FireCluster process crash in the CCD daemon. *[88594]*
- This release resolves an issue that resulted in high CPU usage by the FireCluster CAD daemon when Firebox System Manager is open on a FireCluster. *[91089]*
- A problem that caused a generic kernel crash on the backup master Firebox in a FireCluster has been resolved in this release. *[91791]*

Centralized Management

- Firewall policy icons now show correctly in Dimension Command. *[91968]*
- The WatchGuard Server Center Setup Wizard now correctly sets up the Log and Report Server components when using a log encryption key that contains special characters. *[71687]*

WatchGuard AP Devices and Gateway Wireless Controller

- Actions that you can perform on AP devices are now grouped in an **Actions** drop-down list. *[91451]*
- You can now remove AP firmware from your Firebox with Gateway Wireless Controller. *[91412]*
- A new packet filter template is available for WatchGuard Wi-Fi Cloud AP management. The packet filter template “WG-Cloud-Managed-WiFi" defines the required ports (TCP 443 and UDP 3851) and destination domains to enable AP devices to communicate with cloud services. *[91647]*
- Domain names for WatchGuard Wi-Fi Cloud services are now included by default in the HTTP Proxy Exceptions, and now configured to bypass HTTPS content inspection by default. *[91481, 91482]*

Known Issues and Limitations

Known issues for Fireware v11.11.4 and its management applications, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To see known issues for a specific release, from the **Product & Version** filters you can expand the Fireware version list and select the check box for v11.11.4.

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