Fireware v11.11 Release Notes

Supported Devices	Firebox T10, T30, T50, 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:	26 May 2016
Fireware OS Build	503344
WatchGuard System Manager Build	502713
WatchGuard AP Device Firmware	For AP 100, 102, 200: Build 1.2.9.7 (499343) For AP 300: Build 2.0.0.2 (499475)
Release Notes Revision Date	7 June 2016

Introduction

WatchGuard is pleased to announce the release of Fireware v11.11 and WatchGuard System Manager v11.11.

The release includes several feature enhancements and bug fixes, including:

- **Network Discovery** — The Network Discovery service enables the Firebox to discover devices on your internal network and display them on a network map. This service is supported on Firebox M and T Series and XTMv devices only and is included in the Security Suite subscription bundle.
- **Mobile Security** — Set security requirements for Android and iOS devices that connect to your network. This service is supported for Firebox M and T Series and XTMV only and requires a Mobile Security service subscription.
- **Botnet Detection** — The Botnet Detection service, enabled as part of the RED security subscription, uses a feed of known botnet site IP addresses from Kaspersky and adds these addresses to the Blocked Sites list.
- **Explicit proxy** — The explicit proxy enables the Firebox to accept direct requests from clients and then connect to specified servers and retrieve the information on behalf of the client.
- **Allowed Google Apps domains** — Use the HTTPS Proxy with content inspection enabled to allow domains used for Google for Work services and block users from logging into Google Gmail or other personal Google service accounts.
- **Multiple hotspot portals** — Configure multiple hotspot portals for different Firebox interfaces.
- **RADIUS Single Sign-On (RSSO)** — RSSO enables single sign-on for wireless users who have authenticated to a RADIUS server with 802.1x authentication.
- **BOVPN virtual interface interoperability** — Configure a BOVPN virtual interface to connect to a third-party VPN gateway that supports IPSec over GRE.
- **WatchGuard AP device automatic deployment** — Configure the Gateway Wireless Controller to automatically configure an unpaired AP device when it connects to the network.

- **APT Blocker** *Clean* **threat level** — The new *Clean* threat level enables the Firebox to send log messages for files that were scanned and allowed with no malware detected.
- **Loopback interface** — Use the loopback interface to improve reliability and performance in multi-path dynamic routing environments.

> If your Firebox M or T Series or XTMv device has an active Security Suite subscription, you must synchronize the Feature Key to enable Network Discovery.

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, see the product documentation or review What's New in Fireware v11.11.

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, 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 v11.11 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 v11.10.2. UI changes introduced since v11.10.2 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.

Fireware and WSM v11.11 Operating System Compatibility

Last revised: 10 May 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	Android 4.x & 5.x	iOS v7, v8, & v9
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 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.exe — Use this file to install WSM v11.11 or to upgrade WatchGuard System Manager from v11.x to WSM v11.11.

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.exe` `firebox_M4600_M5600_11_11.zip`
Firebox M4600	`Firebox_OS_M4600_M5600_11_11.exe` `firebox_M4600_M5600_11_11.zip`
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_11_11.exe` `xtm_xtm800_1500_2500_11_11.zip`
XTM 2050	`XTM_OS_XTM2050_11_11.exe` `xtm_xtm2050_11_11.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_11.exe` `xtm_xtm800_1500_2500_11_11.zip`
XTM 1050	`XTM_OS_XTM1050_11_11.exe` `xtm_xtm1050_11_11.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_11.exe` `xtm_xtm800_1500_2500_11_11.zip`
XTM 8 Series	`XTM_OS_XTM8_11_11.exe` `xtm_xtm8_11_11.zip`
Firebox M500 Series	`Firebox_OS_M400_M500_11_11.exe` `firebox_M400_M500_11_11.zip`
XTM 5 Series	`XTM_OS_XTM5_11_11.exe` `xtm_xtm5_11_11.zip`
Firebox M440	`Firebox_OS_M440_11_11.exe` `firebox_M440_11_11.zip`
Firebox M400 Series	`Firebox_OS_M400_M500_11_11.exe` `firebox_M400_M500_11_11.zip`
Firebox M300	`Firebox_OS_M200_M300_11_11.exe` `firebox_M200_M300_11_11.zip`
Firebox M200	`Firebox_OS_M200_M300_11_11.exe` `firebox_M200_M300_11_11.zip`
XTM 330	`XTM_OS_XTM330_11_11.exe` `xtm_xtm330_11_11.zip`
XTM 33	`XTM_OS_XTM3_11_11.exe` `xtm_xtm3_11_11.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_11.exe` `xtm_xtm2a6_11_11.zip`
Firebox T30	`Firebox_OS_T30_T50_11_11.exe` `firebox_T30_T50_11_11.zip`
Firebox T50	`Firebox_OS_T30_T50_11_11.exe` `firebox_T30_T50_11_11.zip`

If you have…	Select from these Fireware OS packages
Firebox T10	`Firebox_OS_T10_11_11.exe` `firebox_T10_11_11.zip`
XTMv All editions for VMware	`xtmv_11_11.ova`
XTMv All editions for Hyper-V	`xtmv_11_11_vhd.zip`

Single Sign-On Software

These files are available for Single Sign-On.

- `WG-Authentication-Gateway_11_11.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_10.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_11.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_11.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.

- `WG-MVPN-SSL_11_11.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. There are no updates with the v11.11 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.

Upgrade to Fireware v11.11

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

Before you upgrade from Fireware v11.x to Fireware v11.11, 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, 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. Instead, you must use the OVA file to deploy a new 64-bit Fireware v11.11 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.

> WatchGuard updated the certificate used to sign the .ova files for this release. 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 at: https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=INFO2170.

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. You can install the v11.11 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 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\[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
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

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\[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
3. Install and open WatchGuard System Manager v11.11. 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

With the release of Fireware v11.11 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 includes new AP firmware v1.2.9.7 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, your AP devices are automatically updated between midnight and 4:00am local time.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.11 (without first upgrading to Fireware v11.10.4 or v11.10.5), there is an additional step you must take to make sure AP v1.2.9.7 is applied to your AP devices. When you upgrade to Fireware v11.11 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the Web UI:

1. Connect to your Firebox and select **System > Upgrade OS**.
2. Browse to the location of your Fireware v11.11 upgrade file and click **Upgrade**.
3. When the upgrade is complete, repeat Step 2.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. To reinstall the AP firmware on the Firebox you must reinstall Fireware v11.11 on the Firebox or download the AP firmware v1.2.9.7 Component Package from the Software Downloads Center and use Fireware Web UI or Policy Manager to install it.

> 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

Fireware v11.11 includes AP firmware v2.0.0.2. 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, your AP devices will be automatically updated between midnight and 4:00am local time.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.11 (without first upgrading to Fireware v11.10.4 or v11.10.5), there is an additional step you must take to make sure AP v2.0.0.2 is applied to your AP devices. When you upgrade to Fireware v11.11 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the Web UI:

1. Connect to your Firebox and select **System > Upgrade OS**.
2. Browse to the location of your Fireware v11.11 upgrade file and click **Upgrade**.
3. When the upgrade is complete, repeat Step 2.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. To reinstall the AP firmware, use one of these two methods:

Reinstall Fireware v11.11 on your Firebox

1. Connect to your Firebox and select **System > Upgrade OS**.
2. Browse to the location of your Fireware v11.11 upgrade file and click **Upgrade**.

Download the AP firmware package from the Software Downloads Center and install it on the Firebox

1. Download and extract the AP firmware package. The component package file extension is `wgpkg-dl`.
2. From Fireware Web UI, select **System > Upgrade OS**.
3. Select **Use an upgrade file**.
4. Browse to the location of the `wgpkg-dl` file and click **Upgrade**.

Upgrade your FireCluster to Fireware v11.11

Before you upgrade to Fireware v11.11, 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.

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 a FireCluster from Fireware v11.10.x or lower to Fireware v11.11. It is possible to do upgrade each cluster member from the Web UI but, if you choose to do so, you must follow the instructions in the Help carefully as the Web UI in previous versions of Fireware was not optimized for this task.

Upgrade a FireCluster from Fireware v11.4.x–v11.10.x to v11.11.x

Use these steps to upgrade a FireCluster to Fireware v11.11.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 v11.11 to WSM v11.x

If you want to revert from v11.11 to an earlier version of WSM, you must uninstall WSM v11.11. 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.

Next, install the same version of WSM that you used before you upgraded to WSM v11.11. 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. Verify that all WatchGuard servers are running.

Downgrade from Fireware v11.11 to Fireware v11.x

> If you use the Fireware Web UI or CLI to downgrade from Fireware v11.11 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 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. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v11.11 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.

Enhancements and Resolved Issues in Fireware v11.11

Security

- The OpenSSL library included in Fireware has been upgraded to version 1.0.1t to resolve multiple security advisories. *[91015]*
- The OpenSSL library included in Fireware has been patched to resolve security vulnerability CVE-2015-3197. *[90191]*
- The OpenSSL library included in Dimension has been upgraded to version 1.0.2h to resolve security advisory CVE-2016-2107. *[91013]*
- The OpenSSL library included in WatchGuard System Manager has been upgraded to version 1.0.2h to resolve security advisory CVE-2016-2107. *[91013]*
- The OpenSSL library included in WatchGuard System Manager has been patched to resolve security advisory CVE-2016-0705. *[90196]*

General

- Automatic feature key synchronization is now enabled by default in a new Firebox configuration. *[86582]*
- Certificate Revocation List is now immediately applied after import. *[86454]*
- An issue that caused the systemd process to crash has been fixed *[89503]*
- A configuration migrated from an older device that does not support Websense cloud to a newer model no longer causes blank HTTP Proxy actions. *[87765]*
- Resolved an issue that caused Policy Manager to prompt for a save of the configuration when no changes had been made. *[90473]*
- Resolved an issue that prevented changes to new and existing firewall policies from taking effect after a configuration save. *[90432]*

Networking

- This release adds support for a loopback interface, a virtual interface you can use with dynamic routing protocols to improve reliability and performance in multi-path dynamic routing environments. *[78118]*
- Added support for 32-bit BGP Autonomous System (AS) numbers. *[60085]*

WatchGuard AP Devices and Gateway Wireless Controller

- WatchGuard AP devices now support RADIUS Single Sign-On. *[86090]*
- In accordance with PCI DSS 3.1 requirements, the WatchGuard AP no longer supports TLSv1.0 for connections to the WAP Admin UI. *[89128, 89129]*
- This release resolves an issue with wireless stability where users were not able to connect to the SSID broadcast from AP100. *[85497]*
- WatchGuard AP device automatic deployment enables you to add an unpaired AP device to the network and have it configured automatically by the Gateway Wireless Controller (GWC). *[82977]*
- You can now configure the Gateway Wireless Controller to discover WatchGuard AP devices on specific interfaces. *[88758]*
- The Gateway Wireless Controller can now manage a much larger number of AP devices. *[88437]*
- Gateway Wireless Controller is now supported for a Firebox configured in drop-in mode. *[81007]*

Firewall

- Resolved an issue with validation of Traffic Management actions that caused the firewalld process to crash. *[89976]*

Authentication

- The Firebox now supports RADIUS Single Sign-On. *[73682, 81792]*
- The Hotspot feature now supports multiple hotspots for different interfaces. *[78825]*
- This release resolves an issue that caused SSO Agent with ELM to stop working after a period of time *[86676]*
- The WatchGuard Terminal Services Agent now is verified to support Citrix XenApp 7.x. *[86740]*
- RADIUS authentication through a BOVPN virtual interface now correctly use the Virtual Interface IP Address instead of the IP address of the external interface. *[89609]*
- The firewall web server lighttpd that handles Web UI, authentication and SSLVPN portal connections has been updated to support DHE and ECDHE SHA2 ciphers. *[84655]*

Proxies and Security Subscriptions

- This release includes the new Botnet Detection Subscription Service, which utilizes a feed of known botnet site IP addresses from Kaspersky and adds these addresses to the Blocked Sites List. This enables your Firebox to block botnet activity at the packet filter level. *[83311]*
- This release supports the new Mobile Security service, which enables you to set security requirements for Android and iOS devices and to allow only approved mobile devices to send traffic across your network. This service is supported for Firebox M and T Series and XTMv only and requires a Mobile Security subscription. *[85586]*
- This release adds support for the Explicit Proxy, which enables the Firebox to accept direct requests from clients and then connect to specified servers and retrieve the information on behalf of the client. *[43480]*
- This release includes support for Google Apps domains, to allow traffic to only domains used for Google for Work services and to block traffic to Google Gmail or other personal Google service accounts. *[72697]*
- Newly created proxy rules now work in configurations that contain more than 1024 policies. *[90673]*
- It is now possible for the SMTP proxy to detect and remove Microsoft Office documents containing VB script macros. *[88412]*
- You can now add a user name variable %(user-name)% in the HTTP Proxy Deny Message to show the authenticated user name. *[82431]*
- This release resolves an issue where the Firebox would fail to re-write the NAT on traffic through a SIP-ALG after transfer with an inactive media attribute and a 0.0.0.0 IP address. *[85988]*
- Application Control can now block TeamViewer through the HTTPS proxy. *[80560]*
- APT Blocker now correctly analyzes Word documents originally saved as RTF format (.rtf) with the file extension manually changed to .doc. *[90224]*
- APT Blocker now correctly analyzes Microsoft Office documents saved in web archive format. *[90158]*
- APT Blocker now supports Mac executable files (.app files), which can now be sent to the Lastline cloud server for analysis. *[86596]*
- APT Blocker scanning now supports rar and 7z compression formats. *[82526]*
- In the SMTP and POP3 proxies, additional file signatures have been added for content type auto detection to produce more accurate results. *[87801]*

- APT Blocker now includes the Clean threat level, which provides the ability to send a log message for files that were scanned, and allowed with no malware detected. *[87789]*
- WebBlocker can now block websites based on their category when the site is translated through translate.google.com *[82262]*
- WebBlocker now includes URL query parameters, the '?', as part of the WebBlocker classification when using the Websense Cloud Server.*[82556]*

Management Server

- Duplicate Address Groups no longer causes Managed VPN Gateways to show a five octet IP address. *[89235]*
- The Apache server on the Management Server no longer crashes and causes disconnects when devices that run Fireware OS 11.6 or lower are managed by the Management Server. *[90482, 90180]*
- WatchGuard System Manager now does not allow a second user to open Policy Manager to make configuration changes to a Fully Managed appliance when another user already has the configuration open and locked in Policy Manager. *[89377]*

VPN

- This releases resolves a crash of the iked process which caused VPN status to disappear and prevented VPN traffic from passing. *[88500]*
- BOVPNs with PFS enabled now correctly rekey when remote third party endpoints pad the Diffie Hellman Key. *[90411]*
- DNS traffic from the Firebox to a remote DNS server through a BOVPN tunnel now uses an internal interface IP address that matches the tunnel route. *[89919]*
- The Firebox T10-W can now send wireless traffic through a BOVPN virtual interface tunnel. *[88580]*
- The native IPsec VPN clients for Windows and IOS devices can now successfully configure the Domain Suffix information during the client IPSec negotiations with Firewall. [66372][65109]

Monitoring and Reporting

- The new Network Discovery service discovers devices on your internal network and displays them on a network map. This service is supported on Firebox M and T Series and XTMv devices only and is included in the Security Suite subscription bundle. If your Firebox or XTMV device has an active Security Suite subscription, you must synchronize the feature key to enable Network Discovery. *[66309]*
- In Firebox System Manager, the Performance Console now displays all available policies in the Policy drop down list when the device configuration contains a large number of policies.
- Device configurations with a large number of policies no longer cause wgPolicy MIB to return truncated results. *[84651]*
- WatchGuard Report Server now generates scheduled PDF reports with the correct local time zone. *[90238]*

FireCluster

- This release includes FireCluster upgrade improvements. You can now upgrade both cluster members from Fireware Web UI. The process for a remote FireCluster upgrade is also improved. The cluster master uploads the Fireware OS upgrade file and manages the upgrades of both members. *[56656,63278]*

- Resolved an issue in which Fireboxes in a cluster would log messages like " tcp syn checking failed (expecting SYN packet for new TCP connection, but received ACK, FIN, or RST instead". *[74801]*
- The XML-RPC connection timeout message no longer appears during manual signature updates on a FireCluster. *[88279]*
- Resolved network hang and transmit timeout issues with cluster interfaces on the XTM 5 series and XTM 8 series models. *[87949, 88004]*

Web UI

- In the Fireware Web UI Interfaces Dashboard, the Bandwidth tab graphs have been relabeled to accurately show the direction of traffic. *[87063]*

Known Issues and Limitations

Known issues for Fireware v11.11 and its management applications, including workarounds where available, can be found on the WatchGuard website.

To see the known issues:

1. Log in to the WatchGuard website at login.watchguard.com.
2. Click the Technical Search icon to go to the Technical Search page.

3. On the Technical Search page, select the **Knowledge Base** tab.
   Knowledge Base filters appear on the left side of the page.
4. To see known issues for a specific release, use these filters:

   - From the **Category** filters, select the **Known Issues** check box.
   - From the **Status** filters, select the **Open** check box.
   - From the **Product & Version** filters, expand the Fireware version list and select the check box for v11.11.

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