Fireware v11.12 Update 1 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:	21 December 2016
Release Notes Revision Date	21 December 2016
Fireware OS Build	518719
WatchGuard System Manager Build	516771
WatchGuard AP Device Firmware	For AP100, 102, 200: Build 1.2.9.10 For AP300: Build 2.0.0.5 For AP120: Build 8.0.552 For AP320: Build 8.0.552

Introduction

On 21 December, WatchGuard released Fireware v11.12 Update 1, a maintenance update for Fireware v11.12 that resolves several outstanding issues. For information about the issues resolved in the Update 1 release, see Enhancements and Resolved Issues. We have updated these release notes for Fireware v11.12 Update 1 but most information related to Fireware v11.12 remains the same.

WatchGuard is pleased to announce the release of Fireware v11.12 and WatchGuard System Manager v11.12. In addition to resolving many outstanding bugs, we're pleased to announce these new features and functions for our Firebox users:

ConnectWise Integration

With Fireware v11.12, we deepen our integration capabilities with ConnectWise, a leading Professional Service Automation tool used by many managed service providers, to add support for the auto-synchronization of asset information, including subscription start and end dates, device serial numbers OS versions, etc., as well as closed-loop ticketing of system, security, and subscription events.

Threat Detection and Response

Built using technology acquired with Hexis, Threat Detection and Response (TDR) is our new cloud hosted security service that detects malware activity, correlates it with network events, and proactively responds to malware on endpoints. This release includes support for TDR, which is currently in Beta. Click here to join the TDR beta program.

Geolocation Service

With the Geolocation service, you can prevent malware communication and attacks from areas where you never have any need for legitimate business communication. Available as part of your Reputation Enabled Defense (RED) security subscription.

Dynamic VPN Tunnels to Azure

Hybrid cloud environments are becoming much more common, where companies have moved some workloads to cloud services such as AWS or Azure, but some key applications remain on premise. Secure VPN communication is needed between the on premise application and the cloud. Previously we supported only a single static or policy-based tunnel to Azure. Now we add the ability to have multiple tunnels, even with dynamic routes and failover between them.

IPv6 Support in Services and Proxies

WatchGuard firewalls have IPv6 Gold logo certification, but previously application proxies and the full set of security services were not supported. Now customers can apply full range of security services, including WebBlocker for content filtering and APT Blocker and Gateway AV to prevent malware in IPv6 environments.

Services and Proxies Enabled by Default

Customers that buy the appliance with Basic or Total Security Suite often neglect to turn on the security services that they have purchased. Now, services will be enabled by default during the initial setup wizard with a secure set of default settings to save time and simplify the initial setup for everyone.

Gateway Wireless Controller

This release introduces several updates to the Gateway Wireless Controller:
- Auto-channel selection to enable smoother deployments without channel conflict
- Wireless deployment that allows AP300 access points to communicate over the air without a physical Ethernet connection
- Remote management of AP devices with Mobile VPN with SSL

FireCluster with DHCP on External Interface

If your ISP provides external-facing interface IP addresses by DHCP, you can now enable an active/passive FireCluster to provide high availability.

X-forwarded Information from Header in Logs and Dimension

If a company uses an explicit proxy service or a web gateway, like WebMarshal, all of the information in Dimension shows only the IP address for that proxy. Now we can go a level deeper and find the original source IP address and show this in Dimension, too.

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 v11.12, see the product documentation or review What's New in Fireware v11.12.

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 v11.12 and all WSM server components with devices running earlier versions of Fireware v11.x. 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 http://www.watchguard.com/wgrd-help/documentation/overview.

Localization

This release includes 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 v11.12 Update 1 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)	Microsoft Windows Server 2016 (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_12.exe` — Use this file to install WSM v11.12 or to upgrade WatchGuard System Manager from an earlier version to WSM v11.12.

Fireware OS

If your Firebox is running Fireware v11.10 or later, you can upgrade the Fireware OS on your Firebox automatically from the Fireware Web UI **System > Upgrade OS** page.

If you prefer to upgrade from Policy Manager, or from an earlier version of Fireware, you can use download the 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 manually using 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_12_U1.exe` `firebox_M4600_M5600_11_12_U1.zip`
Firebox M4600	`Firebox_OS_M4600_M5600_11_12_U1.exe` `firebox_M4600_M5600_11_12_U1.zip`
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_11_12_U1.exe` `xtm_xtm800_1500_2500_11_12_U1.zip`
XTM 2050	`XTM_OS_XTM2050_11_12_U1.exe` `xtm_xtm2050_11_12_U1.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_12_U1.exe` `xtm_xtm800_1500_2500_11_12_U1.zip`
XTM 1050	`XTM_OS_XTM1050_11_12_U1.exe` `xtm_xtm1050_11_12_U1.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_12_U1.exe` `xtm_xtm800_1500_2500_11_12_U1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_12_U1.exe` `xtm_xtm8_11_12_U1.zip`
Firebox M500 Series	`Firebox_OS_M400_M500_11_12_U1.exe` `firebox_M400_M500_11_12_U1.zip`
XTM 5 Series	`XTM_OS_XTM5_11_12_U1.exe` `xtm_xtm5_11_12_U1.zip`
Firebox M440	`Firebox_OS_M440_11_12_U1.exe` `firebox_M440_11_12_U1.zip`
Firebox M400 Series	`Firebox_OS_M400_M500_11_12_U1.exe` `firebox_M400_M500_11_12_U1.zip`
Firebox M300	`Firebox_OS_M200_M300_11_12_U1.exe` `firebox_M200_M300_11_12_U1.zip`
Firebox M200	`Firebox_OS_M200_M300_11_12_U1.exe` `firebox_M200_M300_11_12_U1.zip`
XTM 330	`XTM_OS_XTM330_11_12_U1.exe` `xtm_xtm330_11_12_U1.zip`
XTM 33	`XTM_OS_XTM3_11_12_U1.exe` `xtm_xtm3_11_12_U1.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_12_U1.exe` `xtm_xtm2a6_11_12_U1.zip`
Firebox T70	`Firebox_OS_T70_11_12_U1.exe` `firebox_T70_11_12_U1.zip`
Firebox T50	`Firebox_OS_T30_T50_11_12_U1.exe` `firebox_T30_T50_11_12_U1.zip`

If you have…	Select from these Fireware OS packages
Firebox T30	Firebox_OS_T30_T50_11_12_U1.exe firebox_T30_T50_11_12_U1.zip
Firebox T10	Firebox_OS_T10_11_12_U1.exe firebox_T10_11_12_U1.zip
XTMv All editions for VMware	xtmv_11_12_U1.ova XTM_OS_XTMv_11_12_U1.exe xtm_xtmv_11_12_U1.zip
XTMv All editions for Hyper-V	xtmv_11_12_U1_vhd.zip XTM_OS_XTMv_11_12_U1.exe xtm_xtmv_11_12_U1.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_1.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

This file was updated with the Fireware v11.12 release.

- TO_AGENT_SETUP_11_12.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_1.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. There are no updates with this 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 Notes

In addition to new features and functionality introduced in Fireware v11.12, there were other changes that affect the functionality of several existing features in ways that you need to understand before you upgrade. In this section, we review the impact of some of these changes. For more information, see the What's New in Fireware v11.12 presentation or Fireware Help.

TCP port 4100 now used for firewall user authentication only

Beginning with Fireware v11.12, TCP port 4100 is used only for firewall user authentication. In earlier versions, a WatchGuard Authentication policy was automatically added to your configuration file when you enabled Mobile VPN with SSL. This policy allowed traffic over port 4100 and included the alias Any-External in the policy From list. In Fireware v11.12, when you enable Mobile VPN with SSL, this policy is no longer created. When you upgrade to Fireware v11.12, the External alias will be removed from your WatchGuard Authentication policy, even if you had manually added the alias previously and regardless of whether Mobile VPN with SSL is enabled. If you upgrade with Policy Manager, you must manually reload the configuration from the Firebox after the upgrade completes to avoid adding the alias back with a subsequent configuration save (since Policy Manager is an offline configuration tool).

The Mobile VPN with SSL authentication and software download pages are no longer accessible at port 4100. See Fireware Help for more information.

Setup Wizard Default Policies and Settings

You use the Web Setup Wizard or WSM Quick Setup Wizard to set up a Firebox with a basic configuration. Beginning with Fireware v11.12, the setup wizards now configure policies and enable most Subscription Services to provide better security by default. The setup wizards:

- Configure FTP-proxy, HTTP-proxy, HTTPS-proxy policies
- Configure DNS and Outgoing packet-filter policies
- Enable licensed security services — Application Control, Gateway AntiVirus, WebBlocker, Intrusion Prevention Service, Reputation Enabled Defense, Botnet Detection, Geolocation, APT Blocker
- Recommend WebBlocker categories to block

The default policies and services that the setup wizards configure depend on the version of Fireware installed on the Firebox, and on whether the Firebox feature key includes a license for subscription services. If your new Firebox was manufactured with Fireware v11.11.x or lower, the setup wizards do not enable subscription services, even if they are licensed in the feature key. To enable the security services and proxy policies with recommended settings, upgrade the Firebox to Fireware v11.12 or higher, reset it to factory-default settings, and then run the setup wizard again.

Upgrade to Fireware v11.12 Update 1

Before you upgrade to Fireware v11.12 Update 1, 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 v11.12 Update 1 or your Firebox will be reset to a default state.

Important Information about the upgrade process:

- We recommend you use Fireware Web UI to upgrade to Fireware v11.12 Update 1. You can also use Policy Manager if you prefer.
- We strongly recommend that you save a local copy of your Firebox configuration and create a Firebox backup image 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 v11.12 Update 1. You can install the v11.12 Update 1 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, your WatchGuard Management 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 v11.12 Update 1 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. Before you begin, save a local copy of your configuration file.
2. Go to **System > Backup Image** or use the USB Backup feature to back up your current device image.
3. 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* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.12\[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\11.12
4. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
5. Browse to the location of the *[product series]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

If you have already installed Fireware v11.12 on your computer, you must run the Fireware v11.12 installer twice (once to remove v11.12 software and again to install v11.12 Update 1).

Upgrade to Fireware v11.12 Update 1 from WSM/Policy Manager

1. Before you begin, save a local copy of your configuration file.
2. Select **File > Backup** or use the USB Backup feature to back up your current device image.
3. 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\11.12\[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\11.12.
4. Install and open WatchGuard System Manager v11.12. Connect to your Firebox and launch Policy Manager.
5. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[product series]_[product code].sysa-dl* file from Step 2.

If you have already installed Fireware v11.12 on your computer, you must run the Fireware v11.12 installer twice (once to remove v11.12 software and again to install v11.12 Update 1).

Update AP Devices

With the release of Fireware v11.12, we released new AP firmware for AP100/102, AP200, and AP300 devices. The process to update to new AP firmware changed recently. Please review this section carefully for important information about updating AP devices.

Update your AP100, AP102, and AP200 Devices

Fireware v11.12 and v11.12 Update 1 include new AP firmware v1.2.9.10 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 later to Fireware v11.12 Update 1, 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 v11.12 Update 1, there is an additional step you must take to make sure AP v1.2.9.10 is applied to your AP devices. When you upgrade to Fireware v11.12 Update 1 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** 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 **Manage Firmware** 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

Fireware v11.12 and v11.12 Update 1 include AP firmware v2.0.0.5. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 or later to Fireware v11.12 Update 1, 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 v11.12 Update 1, there is an additional step you must take to make sure AP v2.0.0.5 is applied to your AP devices. When you upgrade to Fireware v11.12 Update 1 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** 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 **Manage Firmware** to download the latest AP firmware to the Firebox again.

Update AP120 or AP320 Devices Managed with Gateway Wireless Controller

Fireware v11.12 Update 1 does NOT include firmware for AP120 or AP320 devices. To get the latest firmware, from **Gateway Wireless Controller > Summary** tab, select **Manage Firmware**. Look for `8.0.552` and select **Download** to download the new firmware to your Firebox. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller, your AP devices will be automatically updated between midnight and 4:00am local time.

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 **Manage Firmware** to download the latest AP firmware to the Firebox again.

Upgrade your FireCluster to Fireware v11.12 Update 1

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 higher 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 v11.12 Update 1 to WSM v11.x

If you want to revert from v11.12 Update 1 to an earlier version of WSM, you must uninstall WSM v11.12 Update 1. 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 v11.12 Update 1.

Next, install the same version of WSM that you used before you upgraded to WSM v11.12 Update 1. 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 v11.12 Update 1. Verify that all WatchGuard servers are running.

Downgrade from Fireware v11.12 Update 1 to Fireware v11.x

If you use the Fireware Web UI or CLI to downgrade from Fireware v11.12 Update 1 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 v11.12 Update 1 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v11.12 Update 1. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v11.12 Update 1 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 v11.12 Update 1

- This release resolves a vulnerability that could allow an attacker to hijack an existing management session. *[EPA-1354]*
- This release reduces the Firebox memory storage data partition size to 1.2GB or less to prevent an issue that caused some Firebox M200, M300. M400, M440, and M500 devices to fail. *[92556]*
- Support.tgz snapshots no longer include the BOVPN shared secret file in plain text in the ikemsg.log file. *[92661]*
- The release patches the Firebox kernel to address the Dirty COW vulnerability (CVE-2016-5195). *[92517]*
- BOVPN tunnel status for XTMv devices now displays correctly in Firebox System Manager and Fireware Web UI. *[92479]*
- This release resolves a kernel crash that affected some Firebox M440 devices. [92609]
- This release resolves an issue that caused Mobile VPN with PPTP to fail when your Firebox was configured with multiple external interfaces. *[92528]*
- The Firebox now correctly blocks traffic from hosts that have been manually configured to be blocked using Firebox System Manager or Traffic Monitor. *[92569]*
- YouTube SafeSearch is now correctly enforced for users that are logged in to Google accounts when the HTTPS proxy is configured with Content Inspection enabled. *[80639]*
- Users can no longer evade YouTube SafeSearch by refreshing the web page when the HTTPS proxy is configured with Content Inspection enabled. *[92159]*

Enhancements and Resolved Issues in Fireware v11.12

General

- The number of blocked sites you can enter has been increased from 1000 to 8192 for Firebox models that have 1GB of memory or more. *[92149]*
- The *wgagent* process no longer crashes when you run the Configuration Report from Fireware Web UI. *[92451]*
- An issue that caused the *oss-daemon* process to crash has been resolved in this release. *[92166]*
- An issue that caused SFP interfaces on Firebox M400 and M500 devices to hang has been resolved. *[92047]*
- OpenSSL has been updated to version 1.0.2j to address several critical security vulnerabilities. *[92161, 92178]*

- DNS traffic from clients behind the Firebox now uses a random source port, and is no longer vulnerable to CVE-2008-1447. *[91517]*
- The Linux kernel has been patched to address a bug in the handling of TCP challenge ACK segments that could allow a remote attacker to hijack TCP sessions (CVE-2016-5696). *[91902]*
- The behavior of Policy Manager in a dual-monitor environment has been improved. *[92188]*
- Feature key auto-update functionality has been improved so the Firebox checks more frequently for feature key updates for services that are set to expire in a week or less. *[92328]*
- Firebox System Manager no longer truncates the list of interface IP addresses on the Status Report tab when a large number of secondary IP addresses are configured. *[81234]*
- Feature key expirations now take effect at the end of the specified day, instead of at the beginning of the day. *[91590]*
- The Firebox no longer provides any response on port 9032 unless configured to do so. *[91575]*
- This release resolves an issue that caused the Firebox to automatically block the source of unhandled packets after an upgrade. *[92373]*

Proxies and Security Subscriptions

- With the new Geolocation service, you can now configure the Firebox to deny connections to or from a particular country. *[35643, 73433]*
- This release provides an improvement to the behavior of the HTTP proxy when it receives a response from an HTTP server that does not include an HTTP response header. *[91900]*
- You can now use all Firebox proxy actions and signature services with connections over IPv6. *[65040]*
- The maximum file size for Advanced Persistent Threat scan has been increased from 8 megabytes to 10. *[91993]*
- WebBlocker with WebSense can now perform lookups through an external proxy server. *[72847]*
- The Firebox Status Report now contains the current number of connections for each type of proxy, such as HTTP, HTTPS, and DNS. *[63913]*
- Gateway AV will now classify Potentially Unwanted Programs (PUPs) as malware. *[92014]*
- The default non-allowed characters rule in the SMTP proxy action now allows email addresses with all RFC-standard characters. *[91005]*
- This release resolves an issue that caused the Firebox to fail to import intermediate certificates as Trusted CA for proxies. *[81517, 82401]*
- A rare issue that prevented the Proxy Authority Certificate from regenerating after it was deleted has been resolved in this release. *[92467]*
- This release resolves an issue that caused the Firebox to incorrectly create the Certificate Portal policy when you configure an SMTP policy with Content Inspection for TLS. *[92270]*
- This release resolves an issue that caused the Quarantine Server to fail to send scheduled notifications when the admin passphrase contained the percent (%) character. *[91869]*

Networking

- An issue that caused the ETH6/ETH7 interface to bounce on Firebox M400/M500 devices has been resolved. *[92243]*
- The Firebox now supports failover to the Huawei E3372 USB LTE Modem Variant (E3372s-153; VID: 12d1 PID:14dc) *[90185]*
- This release resolves an issue where VLAN IDs would persist after being changed or removed from the configuration. *[92319]*
- When you configure policies that use Policy-Based Routing using Fireware Web UI, the Firebox now correctly drops connections when all selected external interfaces are down. *[92280]*

Authentication

- The Active Directory server configuration no longer allows you to input unnecessary *Searching User* information when using the sAMAccountName Login attribute. *[90546]*
- You can now configure exceptions for the forced redirect for External Guest Authentication Hotspot. Connections to these exceptions will not be redirected. *[79129]*
- Users authenticated by Firebox Hotspot Guest Services are now synchronized between FireCluster members. *[83130]*
- Custom logos used for the Firebox Hotspot Page now correctly appear when you uploaded the logos with Fireware Web UI and when the Hotspot is removed from an interface. *[92121, 91139]*
- You can now configure a domain name or IP address as the authentication URL for an external guest authentication hotspot. *[82974]*
- This release resolves an issue that slowed web browsing performance when using the TO Agent. *[92069]*

Logging

- A log message is now generated when Firebox connections to the Log Server fail. *[61456]*
- The Firebox now correctly validates the server certificate of a WatchGuard Log Server or Dimension when it initiates a connection to send log data. *[84177]*
- Quarantine Server now creates a log message for the success or failure of attempts to send email with the configured SMTP server. [91922]

VPN

- You can now configure a Branch Office VPN to Microsoft Azure with IKEv2 and a dynamic tunnel configuration. *[89072]*
- The Firebox now supports Branch Office VPNs that connect to a Cisco Virtual Tunnel Interface, or VTI. *[88140]*
- You can now successfully build a VPN tunnel initiated from AWS Cloud. *[92196]*
- The maximum length of Pre-Shared Keys has been increased from 63 characters to 79 characters. *[92275]*
- An issue that resulted in a memory allocation error that caused low memory and tunnel traffic to fail has been resolved. *[92374]*
- The cookies used to store user credentials for the Mobile VPN with SSL and manual user authentication portal now correctly set the HTTPONLY and Secure attributes. *[88687]*
- Mobile VPN with SSL now uses SHA-1 for authentication and AES-256 for encryption by default. *[91506]*
- The Mobile VPN with IPSec UI now prevents unnecessary tunnel routes from being added when you use the **Force All Traffic Through Tunnel** option. *[90530]*
- The Firebox no longer automatically adds **Any-External** to the WatchGuard Authentication policy when you enable Mobile VPN with SSL. *[67543]*
- When you allow access to the Authentication Portal for Mobile VPN with SSL, external hosts are no longer automatically able to also access the Firebox Authentication Portal. *[67545]*
- When you use the Mobile VPN with IPSec NCP client, Policy Manager now generates the client profile with the configured value for the Phase 1 lifetime instead of it always being set to 8 hours. *[91678]*

FireCluster

- You can now configure a FireCluster external interface as DHCP. *[41637]*
- An issue that caused the *systemd* process to crash when using FireCluster has been resolved. *[92115]*

- Policy Manager now reports status more accurately during the FireCluster OS upgrade process. *[91971]*

Centralized Management

- WatchGuard Server Center now requires text in the comment field when you save a Policy Template change. *[92078]*

WatchGuard AP Devices and Gateway Wireless Controller

- The Gateway Wireless Controller can now automatically change the channel assignments for your AP devices to reduce channel conflicts with nearby devices. *[84570]*
- You can now remotely manage AP devices using Mobile VPN with SSL. *[84692]*
- When the operating region of an AP device is not known, the Gateway Wireless Controller configuration will display **Unknown** instead of **World**. *[92249]*
- For manual channel selection, the Preferred Channel list now displays all channels.*[87679]*

Known Issues and Limitations

Known issues for Fireware v11.12 Update 1 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 v11.12.

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/wgrd-support/overview. 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