Fireware v12.1.1 Release Notes

Supported Devices	Firebox T10, T15, T30, T35, T50, T55, T70, M200, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600 XTM 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 33, XTM 330,XTM 515, XTM 525, XTM 535, XTM 545, XTM 1050, XTM 2050 FireboxV, XTMv, Firebox Cloud, WatchGuard AP
Release Date:	4 April 2018
Release Notes Revision:	4 April 2018
Fireware OS Build	558423
WatchGuard System Manager Build	557822
WatchGuard AP Device Firmware	For AP100, AP102, AP200: Build 1.2.9.14 For AP300: Build 2.0.0.9 For AP120, AP320, AP322, AP325, AP420: Build 8.5.0-646

Introduction

WatchGuard is pleased to announce the release of WSM and Fireware v12.1.1. Fireware v12.1.1 is a planned update to the Firebox operating system that features critical enhancements to network security and resolves a number of longstanding Firebox limitations. At a high level, this release introduces:

DNSWatch

DNSWatch is a new cloud-based service that monitors DNS requests through the Firebox to prevent connections to known malicious domains. It protects against malicious clickjacking and phishing domains regardless of connection type, protocol. or port. DNSWatch is included in the Total Security Suite subscription for Firebox T Series, M Series, XTMv, FireboxV, and Firebox Cloud appliances. Make sure you update your Firebox feature key to get access to this new service.

Support for New Dynamic DNS Providers

You can now configure Dynamic DNS with No-IP, Dynu, DNSdynamic, Afraid.org, Duck DNS, and Dyn.

Firebox Wireless Enhancements

This release includes multiple enhancements to wireless security, including the ability to manually disconnect Firebox wireless clients.

BOVPN over TLS Support in WatchGuard System Manager

You can now configure a Branch Office VPN over TLS in all Firebox user interfaces.

TLS Profiles

We have moved the content inspection settings from HTTPS proxy actions to TLS profiles.

Networking Enhancements

This release introduces many improvements to device networking, including:

- USB Modem Support for Verizon 620L and 730L
- Ability to connect USB modems to the Firebox with no reboot
- Ability to configure a default gateway other than the Firebox IP address in the Firebox DHCP server
- Per-interface configuration of DHCP relay
- Apply firewall policies to intra-VLAN traffic setting is now enabled by default for external VLAN interfaces

Mobile VPN with IPSec for Windows v12.13

This release also includes an update the the Mobile VPN with IPSec Windows client from NCP. The v12.13 client includes:

- Updated look to the Mobile VPN client and connection indicator icon
- Ability to configure VPN Bypass in the client firewall to allow users to connect directly to specified networks without using the VPN
- New Home Zone feature to enable connections to the user local network without specific administrator configuration on the client firewall

For more information on the feature updates and available bug fixes in this release, see the Enhancements and Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Fireware v12.1.1 see Fireware Help or review What's New in Fireware v12.1.1.

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, T15, T30, T35, T50, T55, T70, XTM 2 Series (models 25 and 26 only), XTM 33 or 330, 5 Series (515/525/535/545), 8 Series, 800 Series, XTM 1050, XTM 1500 Series, XTM 2050 device, XTM 2500 Series, or Firebox M Series. You can also use this version of Fireware on FireboxV or XTMv (any edition), and Firebox Cloud for AWS and Azure. *We do not support Fireware v12.x on XTM 505, 510, 520 or 530 devices.*
- 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.
- If you are upgrading to Fireware v12.x from Fireware v11.10.x or earlier, we strongly recommend you review the Fireware v11.12.4 release notes for important information about significant feature changes that occurred in Fireware v11.12.x release cycle.

Note that you can install and use WatchGuard System Manager v12.x and all WSM server components with devices running earlier versions of Fireware. 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 FireboxV installation, make sure you carefully review Fireware help in the WatchGuard Help Center 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 https://www.watchguard.com/wgrd-help/documentation/overview.

Localization

This release includes localization update for the management user interfaces (WSM application suite and Web UI) current as of Fireware v12.0. UI changes introduced since v12.0 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 not yet available for *Fireware Help.*

Fireware and WSM v12.1.1 Operating System Compatibility

Last revised 12 December 2017

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10 (32-bit & 64-bit)	Microsoft Windows Server 2012 & 2012 R2 (64-bit)	Microsoft Windows Server 2016 (64-bit)	Mac OS X/macOS v10.10, v10.11, v10.12 & v10.13	Android 6.x, 7.x, & 8.x	iOS v8, v9, v10 & v11
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, see the Dimension Release Notes.*	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)[1]		✓	✓			
Single Sign-On Client	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[2]		✓	✓			
Terminal Services Agent[3]		✓	✓			
Mobile VPN with IPSec	✓			✓[4]	✓	✓[4]
Mobile VPN with SSL	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *Windows 8.x support does not include Windows RT.*

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

- *IE 11 and later*
- *Microsoft Edge*
- *Firefox v55*
- *Safari 10*
- *Safari iOS 10*
- *Chrome v60*

[1]The Server Core installation option is supported for Windows Server 2016.

[2]Microsoft Exchange Server 2007 and 2010 are supported. Microsoft Exchange Server 2013 is supported if you install Windows Server 2012 or 2012 R2 and .NET Framework 3.5

[3]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, 7.6, or 7.12 environment.

[4]Native (Cisco) IPSec client and OpenVPN are supported for all recent versions of Mac OS and iOS. To use The WatchGuard Mobile VPN with IPSec client with OS 10.13, you must upgrade to the v3.00 client release.

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]	–	✓	–	✓
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

FireboxV System Requirements

With support for installation in both a VMware and a Hyper-V environment, a WatchGuard FireboxV virtual machine can run on a VMware ESXi 5.5, 6.0, or 6.5 host, or on Windows Server 2012 R2 or 2016, or Hyper-V Server 2012 R2 or 2016.

The hardware requirements for FireboxV are the same as for the hypervisor environment it runs in.

Each FireboxV virtual machine requires 5 GB of disk space. CPU and memory requirements vary by model:

FireboxV Model	vCPUs (maximum)	Memory (recommended)
Small	2	2048 MB
Medium	4	4096 MB
Large	8	4096 MB
Extra Large	16	4096 MB

System requirements for XTMv are included in Fireware Help.

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:

`WSM12_1_1.exe` — Use this file to install WSM v12.1.1 or to upgrade WatchGuard System Manager from an earlier version to WSM v12.1.1.

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_12_1_1.exe firebox_M4600_M5600_12_1_1.zip
Firebox M4600	Firebox_OS_M4600_M5600_12_1_1.exe firebox_M4600_M5600_12_1_1.zip
Firebox M670	Firebox_OS_M370_M470_M570_M670_12_1_1.exe firebox_M370_M470_M570_M670_12_1_1.zip
Firebox M570	Firebox_OS_M370_M470_M570_M670_12_1_1.exe firebox_M370_M470_M570_M670_12_1_1.zip
Firebox M500	Firebox_OS_M400_M500_12_1_1.exe firebox_M400_M500_12_1_1.zip
Firebox M470	Firebox_OS_M370_M470_M570_M670_12_1_1.exe firebox_M370_M470_M570_M670_12_1_1.zip
Firebox M440	Firebox_OS_M440_12_1_1.exe firebox_M440_12_1_1.zip
Firebox M400	Firebox_OS_M400_M500_12_1_1.exe firebox_M400_M500_12_1_1.zip
Firebox M370	Firebox_OS_M370_M470_M570_M670_12_1_1.exe firebox_M370_M470_M570_M670_12_1_1.zip
Firebox M300	Firebox_OS_M200_M300_12_1_1.exe firebox_M200_M300_12_1_1.zip
Firebox M200	Firebox_OS_M200_M300_12_1_1.exe firebox_M200_M300_12_1_1.zip
Firebox T70	Firebox_OS_T70_12_1_1.exe firebox_T70_12_1_1.zip
Firebox T55	Firebox_OS_T55_12_1_1.exe firebox_T55_12_1_1.zip
Firebox T50	Firebox_OS_T30_T50_12_1_1.exe firebox_T30_T50_12_1_1.zip
Firebox T35	Firebox_OS_T35_12_1_1.exe firebox_T35_12_1_1.zip
Firebox T30	Firebox_OS_T30_T50_12_1_1.exe firebox_T30_T50_12_1_1.zip
Firebox T15	Firebox_OS_T15_12_1_1.exe firebox_T15_12_1_1.zip
Firebox T10	Firebox_OS_T10_12_1_1.exe firebox_T10_12_1_1.zip

If you have…	Select from these Fireware OS packages

FireboxV
All editions for VMware
	`FireboxV_12_1_1.ova`
	`XTM_OS_FireboxV_12_1_1.exe`
	`xtm_FireboxV_12_1_1.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_1_1_vhd.zip`
	`XTM_OS_FireboxV_12_1_1.exe`
	`xtm_FireboxV_12_1_1.zip`

Firebox Cloud	`FireboxCloud_12_1_1.zip`
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_12_1_1.exe` `xtm_xtm800_1500_2500_12_1_1.zip`
XTM 2050	`XTM_OS_XTM2050_12_1_1.exe` `xtm_xtm2050_12_1_1.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_12_1_1.exe` `xtm_xtm800_1500_2500_12_1_1.zip`
XTM 1050	`XTM_OS_XTM1050_12_1_1.exe` `xtm_xtm1050_12_1_1.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_12_1_1.exe` `xtm_xtm800_1500_2500_12_1_1.zip`
XTM 8 Series	`XTM_OS_XTM8_12_1_1.exe` `xtm_xtm8_12_1_1.zip`
XTM 5 Series, *Models 515, 525, 535, and 545 only*	`XTM_OS_XTM5_12_1_1.exe` `xtm_xtm5_12_1_1.zip`
XTM 330	`XTM_OS_XTM330_12_1_1.exe` `xtm_xtm330_12_1_1.zip`
XTM 33	`XTM_OS_XTM3_12_1_1.exe` `xtm_xtm3_12_1_1.zip`
XTM 25/26	`XTM_OS_XTM2A6_12_1_1.exe` `xtm_xtm2a6_12_1_1.zip`

XTMv
All editions for VMware
	`xtmv_12_1_1.ova`
	`XTM_OS_xtmv_12_1_1.exe`
	`xtm_xtmv_12_1_1.zip`

XTMv
All editions for Hyper-V
	`xtmv_12_1_1_vhd.zip`
	`XTM_OS_XTMv_12_1_1.exe`
	`xtm_xtmv_12_1_1.zip`

Single Sign-On Software

These files are available for Single Sign-On. There are no updates with the v12.1.1 release.

- `WG-Authentication-Gateway_12_0.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11.12.2.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_12_0.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_12_0.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_12_0.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 is not updated with the Fireware v12.1.1 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:

- `WG-MVPN-SSL_12_0.exe` (Client software for Windows)
- `WG-MVPN-SSL_12_0.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download. The Mac client is updated with this release to add support for macOS 10.13.

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 for Windows version is 12.13.

- `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.

The current macOS client version is 3.00.

- `WatchGuard IPSec Mobile VPN Client for macOS, 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. If you have a VPN bundle ID for macOS, it must be updated on the license server to support the new macOS 3.00 client. To update your bundle ID, contact WatchGuard Customer Support. Make sure to have your existing bundle ID available to expedite the update.

Upgrade Notes

SSL/TLS Settings Precedence and Inheritance

Four Firebox features use SSL/TLS for secure communication and share the same OpenVPN server: Management Tunnel over SSL on hub devices, BOVPN over TLS in Server mode, Mobile VPN with SSL, and the Access Portal. These features also share some settings. When you enable more than one of these features, settings for some features have a higher precedence than settings for other features. Shared settings are not configurable for the features with lower precedence. For more information, see this topic in *Fireware Help*.

Modem Configurations Converted to External Interfaces with Failover Enabled

If your Firebox was configured for modem failover, when you upgrade your Firebox to Fireware v12.1, the modem configuration is automatically converted to an external interface with modem failover enabled. If all other external interfaces become unavailable, traffic automatically fails over to the modem interface. Modem interfaces can also participate in multi-WAN on all devices except the Firebox T10, Firebox T15, and XTM 2 Series devices that do not have the Pro upgrade.

Gateway AV Engine Upgrade with Fireware v12.0

With Fireware v12.0, we updated the engine used by Gateway AV to a new engine from BitDefender. As a result, any Firebox that upgrades from Fireware v11.x version to v12.0 or later must download a new signature set, which can take 7-10 minutes for the first update. It can take an additional 5-7 minutes to synchronize a FireCluster. We recommend that you upgrade to Fireware v12.x at a quiet time on your network. After the initial update, signature updates are incremental and much faster than in previous versions.

While the new signature set is being downloaded, network users could experience issues related to Gateway AV scan failures for several minutes after the update, and inbound emails sent through the SMTP proxy could be locked.

XTMv Upgrade Notes

You cannot upgrade an XTMv device to FireboxV. 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 or v12.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 or deploy a new XTMv VM, see Fireware Help. When your XTMv instance has been updated to v11.11 or higher, you can then use the usual upgrade procedure, as detailed in the next section.

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.

Upgrade to Fireware v12.1.1

If your Firebox is a T10, XTM 25, or XTM 26 device, you may not be able to perform a backup before you upgrade the Firebox. This occurs because the memory use by recent versions of Fireware does not leave enough memory free to successfully complete the upgrade process on these devices. For these devices, we recommend you save a copy of the .xml configuration file with a distinctive name, as described here: Save the Configuration File.

If you need to downgrade the Firebox after you complete the upgrade to Fireware v12.x, we recommend you Downgrade with Web UI. This process deletes the configuration file, but does not remove the device feature keys and certificates. After you downgrade the Firebox, you can use Policy Manager to Save the Configuration File to the Firebox.

Important Information about the upgrade process:

- We recommend you use Fireware Web UI to upgrade to Fireware v12.x. 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.
- 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 a Firebox T10, XTM 2 Series, 33, 330, 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.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x or v12.x server or client software when you upgrade to WSM v12.x. You can install the v12.x 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.

You cannot restore a WatchGuard Server backup file created with WatchGuard System Manager v12.x to to a v11.x installation. Make sure to retain your older server backup files when you upgrade to v12.0 or later in case you want to downgrade in the future.

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 v12.1.1 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\12.1.1\[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\FirewareXTM\12.1.1
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 installed a beta release of Fireware v12.1.1 on your computer, you must run the Fireware v12.1 .1installer twice (once to remove v12.1.1 software and again to install v12.1.1).

Upgrade to Fireware v12.1.1 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\FirewareXTM\12.1.1\[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\FirewareXTM\12.1.1.
4. Install and open WatchGuard System Manager v12.1.1. 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 installed a beta release of Fireware v12.1.1 on your computer, you must run the Fireware v12.1.1 installer twice (once to remove v12.1.1 software and again to install v12.1.1).

If you like to make updates to your Firebox configuration from a saved configuration file, make sure you open the configuration from the Firebox and save it to a new file after you upgrade. This is to make sure that you do not overwrite any configuration changes that were made as part of the upgrade.

Other Upgrade Issues:
There is an upgrade issue that affects some Firebox M400/M500 and M440 devices. Please review this knowledge base article carefully before you upgrade.

Fireware v12.x is not supported on XTM 5 Series devices, models 505, 510, 520 or 530.

Before you upgrade to Fireware v12.x, your Firebox must be running:
- Fireware XTM v11.7.5
- Fireware XTM v11.8.4
- Fireware XTM v11.9 or higher

If you try to upgrade from Policy Manager and your Firebox is running an unsupported version, the upgrade is prevented.
If you try to schedule an OS update of managed devices through a Management Server, the upgrade is also prevented.
If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x, or v11.10.x before you upgrade to Fireware v12.x or your Firebox will be reset to a default state.

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.

Update AP Devices

Beginning with Fireware v11.12.4, AP firmware is no longer bundled with Fireware OS. All AP device firmware is managed by the Gateway Wireless Controller on your Firebox. The Gateway Wireless Controller automatically checks for new AP firmware updates and enables you to download the firmware directly from WatchGuard servers.

Important Upgrade Steps

If you have not previously upgraded to Fireware 12.0.1 or higher and the latest AP firmware, you must perform these steps:

1. Make sure all your APs are online. You can check AP status from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.
2. Make sure you are not using insecure default AP passphrases such as **wgwap** or **watchguard**. Your current AP passphrase must be secure and at least 8 characters in length. You can change your AP passphrase in **Network > Gateway Wireless Controller > Settings**.

If you do not have a secure passphrase correctly configured before the upgrade, you will lose the management connection with your deployed APs. If this occurs, you must physically reset the APs to factory default settings to be able to manage the APs from Gateway Wireless Controller.

Depending on the version of Fireware you are upgrading from, you may need to mark AP100, AP102, AP200, and AP300 devices as trusted after the upgrade to Fireware v12.0.1 or higher. You can mark APs as trusted from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.

AP Firmware Upgrade

The current AP firmware versions for each AP device model are:

AP Device Model	Current Firmware Version
AP100, AP102, AP200	1.2.9.14
AP300	2.0.0.9
AP120, AP320, AP322, AP325, AP420	8.5.0-646

To manage AP firmware and download the latest AP firmware to your Firebox:

- From Fireware Web UI, select **Dashboard > Gateway Wireless Controller**. From the **Summary** tab, click **Manage Firmware**.
- From Firebox System Manager, select the **Gateway Wireless Controller** tab, then click **Manage Firmware.**

Note that you cannot upgrade an AP120, AP320, AP322, or AP420 to 8.3.0-657 or higher unless your Firebox is running Fireware v11.12.4 or higher. If your Firebox does not run v11.12.4. or higher, you will not see an option to upgrade to AP firmware v8.3.0-657 or higher.

If you have enabled automatic AP device firmware updates in Gateway Wireless Controller, your AP devices are automatically updated between midnight and 4:00am local time.

To manually update firmware on your AP devices:

1. On the **Access Points** tab, select one or more AP devices.
2. From the **Actions** drop-down list, click **Upgrade**.
3. Click **Yes** to confirm that you want to upgrade the AP device.

Upgrade your FireCluster to Fireware v12.1.1

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.

There is an upgrade issue that affects some Firebox M400/M500 and M440 devices. Please review this knowledge base article carefully before you upgrade.

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.

Downgrade Instructions

Downgrade from WSM v12.1.1 to earlier WSM v12.x or v11.x

If you want to revert from v12.1.1 to an earlier version of WSM, you must uninstall WSM v12.1.1. 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 v12.1.1.

Next, install the same version of WSM that you used before you upgraded to WSM v12.1.1. 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 v12.1.1. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.1.1 to earlier Fireware v12.x or v11.x

If you use the Fireware Web UI or CLI to downgrade from Fireware v12.1.1 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 v12.1.1 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.1.1. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.1.1 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 *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 12.1.1

General

- Firebox log messages no longer reference policy 0. *[FBX-8734]*
- Firebox M440 appliances now correctly return information for eth0-eth3 for SNMP. *[FBX-9918]*
- This release resolves a Firebox M370 crash issue that would cause a reboot with the message: `BUG: work queue leaked lock or atomic...` *[FBX-9848]*
- You can now edit Custom Policy templates in Policy Manager. *[FBX-10089]*
- This release resolves a Firewalld process crash. *[FBX-10011]*
- The Firebox web server now correctly continues to use the 3rd Party certificate after a Firebox reboot. *[FBX-9523]*
- An issue that caused Policy Manager to fail to display Policy Properties has been fixed. *[FBX-8591]*
- The **Allow SSLVPN Policy** is no longer moved to the bottom of the list in Web UI when Manual Order mode is used. *[FBX-7625]*
- This release resolves an issue in which Management Server client Fireboxes unexpectedly change status to `Heartbeat (Unavailable)`. *[FBX-9748]*
- This release resolves a wgagent daemon crash issue. *[FBX-6831]*
- This release allows small devices, such as Firebox T10 devices, to free enough memory to perform system backups. *[FBX-2373]*
- The WLAN light on wireless Fireboxes now lights consistently and as expected. *[FBX-2993]*
- This release resolves an issue in which Management Server Policy Templates fail to apply, resulting in the Firebox log message: `trace-type': [facet 'maxInclusive'] The value '52' is greater than the maximum value allowed ('49').` *[FBX-10330]*
- Fully Managed Firebox Policy Manager is now correctly locked when you try to open Policy Manager from Firebox System Manager when more than one RBAC user is connected to the Firebox. *[FBX-9223]*
- This release resolves a memory leak that occurs when you use SNMP. *[FBX-9313]*
- Firebox NTP server no longer unexpectedly stops responding. *[FBX-9026]*
- This release resolves an issue in which Autotask event monitoring fails when FireCluster failover monitoring is enabled. *[FBX-9660]*

FireCluster

- This release resolves a connection count discrepancy in Firebox System Manager for an active/active FireCluster. *[FBX-9392]*
- Access Portal users no longer unexpectedly disconnect in a FireCluster environment because of idle timeout sync errors. *[FBX-10186]*
- This release resolves a soft lockup error in which one FireCluster member would go offline and require a reboot to correct. *[FBX-9782]*

Proxies and Services

- POP3 proxy log message now correctly includes the recipient email address when a Thunderbird client retrieves email. *[FBX-7749]*
- This release resolves an issue in which some websites fail to load through the HTTP and HTTPS proxies. [FBX-10265]
- DLP can now correctly match violations in web-based email services, such as Office365, that use HTTP-POST *[73266, 88158, FBX-2470, FBX-7853]*

- This release resolves an issue that impacted HTTP and HTTPS proxy performance in very large deployments with WebBlocker enabled. *[FBX-5248]*
- Policy Manager now correctly displays the Google Apps *Allowed Domain* settings in the HTTPS proxy configuration *[FBX-9550]*
- The Firebox can now smoothly detect new IP addresses for TDR cloud. *[FBX-11042]*
- This release introduces DNSWatch.
- Configuration of Content Inspection for HTTPS is now located in TLS profiles. *[FBX-9077]*
- This release resolves an issue that caused email messages to fail with Firebox log messages that include: `Destination unreachable (Fragmentation needed)`. *[FBX-9898]*
- The HTTPS proxy can better handle connections which use TLS 1.3 and apply WebBlocker categorization. *[FBX-11166]*
- The HTTPS proxy no longer denies TLS 1.3 protocol draft 28 connections when you enforce TLS compliance. *[FBX-11151]*

Networking

- This release resolves a connection stability issue with the Verizon USB730L modem. *[FBX-9450]*
- Blocked Sites traffic log messages now show the original reason an IP address has been blocked. *[FBX-9544]*
- Connections that use multi-WAN Round Robin in an active/active FireCluster now use the correct NAT IP address. *[FBX-9986]*
- This release resolves an issue that caused Policy Manager to display an incorrect error message when you configure IPv6 default gateway. *[FBX-3218]*
- Firebox System Manager and Web UI now correctly displays bandwidth for each client for Per client Traffic Management actions. *[FBX-9320]*
- The IP Spoofing feature now correctly drops traffic when the defined network range and VLAN ID tag do not match. *[FBX-9843]*
- Modem failover now works consistently with the Verizon U620L modem. *[FBX-7841]*
- This release resolves an issue that caused Policy Manager to fail to edit **Modem Failover** with an `Operation failed` message. *[FBX-9851]*
- Firebox System Manager and Web UI display of DHCP leases now include DHCP reservations. *[RFE84740, FBX-3787]*
- This release adds a selection of new Dynamic DNS providers. [FBX-11077]
- You can now connect a USB modem to the Firebox without the need for a reboot. *[FBX-9504]*
- You can now configure DHCP relay servers separately on a per-interface basis. *[FBX-9785]*
- When you configure an External VLAN interface, the **Apply firewall policies to intra-VLAN traffic option** is now enabled by default. *[FBX-9016]*
- This release resolves an issue in which the **Per IP Address Traffic Management** rules degraded throughput. *[FBX-8995]*
- Bandwidth quotas are no longer reset when a user logs in with different capitalization in their user name. *[FBX-5234]*

VPN

- The IKED process no longer restarts when a Branch Office VPN uses the Modem failover interface. *[FBX-9852]*
- WatchGuard System Manager now correctly displays the rekey option when you right-click a tunnel. *[FBX-9847]*
- This release resolves an issue that caused DHCP relay to fail over BOVPN virtual interfaces using the *Cloud VPN or Third-Party Gateway* Remote Endpoint Type. *[FBX-9746]*

- IKEv2 Mobile Clients can now successfully establish a VPN connection to a firewall enabled in FIPS Mode. *[FBX-10491]*
- You can now use all Firebox user interfaces, including Policy Manager, to configure Branch Office VPN over TLS. *[FBX-9810, FBX-9641]*
- This release resolves an IKEd process crash which occurs on the Backup Master device in FireCluster. *[FBX-9729]*
- The IKEd process no longer leaks memory when the Firebox recieves IKEv2 IKE SA_INIT requests for a non-configured gateway. *[FBX-11078]*

Wireless

- This release resolves a packet loss issue for iOS devices connected to wireless Fireboxes. *[FBX-9530]*
- This release improves Gateway Wireless Controller management and interface performance on Fireboxes with a large number of DHCP clients. *[FBX-9414]*
- You can now manually disconnect Firebox wireless clients. *[FBX-2712]*
- This release eliminates the ability to save a Firebox configuration with the insecure WEP Shared Key option for Firebox wireless. *[FBX-8974, FBX-8975, FBX-8976]*

Resolved Issues in Mobile VPN with IPSec for Windows v12.13

- The product and status icon now changes colors to reflect the connection status, with a line underneath that changes appearance based on the client firewall status.
- The NDIS driver has been optimized to correct problems during connection setup after leaving sleep mode.
- This release changes the network driver to a Virtual Adapter, and Windows Connection Manager no longer disconnects the interface when the Wi-Fi adapter is connected.
- You can now connect after client installation without the need for a reboot.
- This release resolves an issue in which the client would see a blue-screen error when the client system left hibernation mode with the Wi-Fi Manager active.
- This release resolves an issue in which the client license sometimes deactivates when the client system restarts.
- The client now provides the installed version number of Internet Explorer during Hotspot Logon to avoid logon problems.
- The installation wizard no longer prompts users to install the Windows Pre-Logon Credential Provider. You can still enable or disable this feature after installation.
- You can now select a default certificate for the user or computer in the client configuration menu below Certificates.
- The client firewall now includes a Home Zone option that allows users to access local network resources without specific configuration by the administrator.
- The client firewall now includes a VPN Bypass option to allow the administrator to define applications that can communicate directly over the internet even though split-tunneling is disabled in the mobile VPN.
- The client no longer fails to connect after an abrupt change of internet connection type, such as unplugging the LAN cable.
- Windows can now show the status of the client firewall in the Security and Maintenance control panel.
- This release resolves some issues with the Credential Provider for Pre-Connect Login with user names over 20 characters in length.

Resolved Issues in AP Firmware 8.5.0-646

AP Firmware Update for AP120, AP320, AP322, AP325, and AP420

- APs no longer remain in the "authenticating" state If you upgrade a Gateway Wireless Controller-managed AP that is configured with a static IP address. *[FBX-9704]*
- MAC Access Control is now correctly disabled when you disable this feature on an SSID. *[AP-150]*
- This release adds support for AP325 local management with a Gateway Wireless Controller. *[FBX-6688]*
- SSH login credentials now work correctly for technical support access to an AP. *[FBX-9776]*

After you update an AP325 or AP420 managed locally by a Gateway Wireless Controller to firmware 8.5.0-646, you cannot downgrade the AP to an earlier version of firmware from the Gateway Wireless Controller. If you experience issues with the 8.5.0-646 AP firmware and want to downgrade back to the previous version, you must contact WatchGuard technical support.

Known Issues and Limitations

Known issues for Fireware v12.1.1 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 that version.

Using the CLI

The Fireware CLI (Command Line Interface) is fully supported for v12.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 for WatchGuard Firebox, XTM & Dimension.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at https://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