Fireware v12.4 Update 2 Release Notes

Supported Devices	Firebox T10, T15, T30, T35, T50, T55, T70, M200, M270, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600 FireboxV, Firebox Cloud, WatchGuard AP
Release Date	4 April 2019
Release Notes Revision	10 October 2019
Fireware OS Build	592447 (updated for Fireware v12.4 Update 2 on 26 April 2019 *589964 (original Fireware v12.4 release)*
WatchGuard System Manager Build	592565 (updated for Fireware v12.4 Update 2 on 26 April 2019 *591532 (updated for WSM v12.4 Update 1 on 11 April 2019)* *59007 (original WSM v12.4 release)*
WatchGuard AP Firmware	AP100, AP102, AP200: 1.2.9.16 AP300: 2.0.0.11 AP125: 8.6.0-644.3 AP120, AP320, AP322, AP325, AP420: 8.6.0-646

Introduction

On 29 April 2019, we release Fireware and WatchGuard System Manager (WSM) v12.4 Update 2 to resolve several issues, mostly related to Firebox management and the HTTPS proxy. See Enhancements and Resolved Issues for more information.

On 11 April 2019, we released WatchGuard System Manager (WSM) v12.4 Update 1 to resolve an issue with Policy Manager. See Enhancements and Resolved Issues for more information.

Fireware v12.4 is a significant release for Firebox T Series, Firebox M Series, FireboxV, and Firebox Cloud appliances. This release offers major enhancements, feature improvements, and resolves numerous bugs. Some of the key features included in this release are:

SD-WAN for VPN and Private Lines

This release extends SD-WAN benefits to more than just external WAN connections, enabling organizations to cut back on expensive MPLS connections. You can now measure loss/latency/jitter on Virtual Interface VPNs and internal interfaces and fail over when values do not meet the defined threshold for acceptable line quality.

Warn option in WebBlocker

The Warn option provides flexibility to Firebox administrators to enforce acceptable use policies. Organizations can generate employee awareness in cases where “Deny” is too strict.

DNSWatch Blackhole Page

When users try to get access to a domain on the DNSWatch Blackholed domain list, the Firebox now treats the connection to the Blackhole Server educational page as a trusted host connection and allows it.

The Firebox also writes a ProxyDeny log message for the blackholed domain.

If a domain is in both the DNSWatch Blackholed Domain list and matches a denied WebBlocker category, the Blackhole Server page now appears instead of the WebBlocker deny message.

DNSWatch in Bridge Mode

You can now apply full DNS security, even when the Firebox is not the network gateway.

BOVPN over IPv6

Your Firebox can now create VPN tunnels directly between two IPv6 IP addresses. Your IPv6 VPNs no longer need to tunnel over IPv4.

Syslog Export to Two Servers

Your Firebox can now simultaneously send log messages to two different syslog servers. This enables export to third party SIEM while continuing to log to a local syslog server for log retention.

TLS 1.3 Support

You can now configure the Firebox for full inspection of connections with TLS 1.3. The Firebox also now supports TLS 1.3 for all web servers hosted by the Firebox.

For a full list of the enhancements in this release, see *Resolved Issues in Fireware and WSM 12.4 Update 2*. or review the What's New in Fireware v12.4 PowerPoint.

Before You Begin

Before you install this release, make sure that you have:

- A supported WatchGuard Firebox. This device can be a WatchGuard Firebox T Series or Firebox M Series device. You can also use this version of Fireware on FireboxV and Firebox Cloud for AWS and Azure. *We do not support Fireware v12.2.x or higher on XTM 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 and the version of WSM installed on your Management Server.
- Feature key for your Firebox — 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.
- Some Known Issues are especially important to be aware of before you upgrade, either to or from specific versions of Fireware. In this release, a change affects some inbound NAT policies with policy-based routing or an SD-WAN action. To learn more, see Release-specific upgrade notes.

Note that you can install and use WatchGuard System Manager v12.x and all WSM server components[1] 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, 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 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.

[1] The WebBlocker server component is not supported by Fireboxes with v12.2 or higher, and it is no longer possible to download a database for WebBlocker server.

Known Issues and Limitations

Known issues for Fireware v12.4 Update 2 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.

Some Known Issues are especially important to be aware of before you upgrade, either to or from specific versions of Fireware. To learn more, see Release-specific upgrade notes.

This page does not include every issue resolved in a release.
Issues discovered in internal testing or beta testing are not usually included in this list.

Resolved Issues in Fireware and WSM 12.4 Update 2

General

- The Fireware Web UI Front Panel now loads correctly for all users. *[FBX-15555]*
- This release resolves an appliance kernel lockup issue. *[FBX-15247]*

Networking

- The Firebox now consistently adds default routes to VLAN external interfaces. *[FBX-16358]*
- This release resolves an issue that caused the Firebox to fail to save a Management Server Policy Template with configured FQDNs. *[FBX-16237]*
- Policy Manager now correctly handles the configuration of BOVPN Virtual Interface settings in pre-Fireware v12.0 configurations. *[FBX-16291]*

Proxies and Services

- This release resolves an issue that caused websites to fail to load through the HTTPS Proxy when messages are split over multiple TLS records. *[FBX-16195]*
- The `pxyassist` process no longer crashes when PDF files are analyzed. *[FBX-16197]*
- This release adds additional PFS grade ciphers for better compatibility with HTTPS web servers with content inspection in the HTTPS Proxy. *[FBX-16227]*
- The HTTPS Proxy can now Inspect uncategorized sites when you also use an On-Premise WebBlocker Server. *[FBX-15847]*
- Proxy traffic for 1-to-1 NAT hosts now use the correct NAT Base IP address. *[FBX-16234]*
- When content inspection is disabled, the HTTPS Proxy can now correctly handle Client Authentication during the SSL handshake. *[FBX-15916]*
- This release resolves several issues that caused websites to fail with the HTTPS Proxy with content inspection disabled. *[FBX-16143, FBX-16203]*

Resolved Issues in WSM 12.4 Update 1

- Policy Manager license compliance now correctly recognizes Fireware/XTM Pro licenses on FireCluster devices. *[FBX-16172]*

Enhancements and Resolved Issues in Fireware and WSM 12.4

General

- You can now configure the Firebox to automatically retrieve a new feature key after upgrade to a new Fireware OS version. *[FBX-12257]*
- You can now use Command Line Interface and Web UI to add Blocked Sites entries that overlap existing entries. *[FBX-3608]*
- Firebox M5600 devices no longer incorrectly send `Warning:'VBat' is out of valid range` log messages. *[FBX-3399]*
- The Web UI Front Panel now loads correctly. *[FBX-14174]*
- You can now modify a policy with Web UI after you press return in a comment you add to that policy with Policy Manager. *[FBX-12328]*
- Policy Manager now consistently launches dialog boxes on the same monitor as the parent window. *[FBX-15291]*
- This release resolves an issue that caused the retrieval of the support diagnostic file to time out. *[FBX-14026]*
- This release reduces the occurrence of log messages that include `netlink: 64 bytes leftover after parsing attributes`. *[FBX-15556]*
- The Firebox can simultaneously send log messages to up to three syslog servers. *[FBX-9401]*
- This release resolves multiple crash issues:
  - An `S0` fault on XTMv and FireboxV virtual platforms. *[FBX-9758]*
  - A Firebox kernel driver crash issue. *[FBX-14267]*
  - A crash that resulted in a `kernel panic scheduling while atomic` message. *[FBX-15114, FBX-7483]*
  - An issue that caused Firebox M440 devices to crash because of low available memory. *[FBX-11497*]
  - An issue that caused Firebox M200 devices to crash. *[FBX-14455]*

SD-WAN and Multi-WAN

- You can now configure SD-WAN for traffic to leave any Firebox interface. *[FBX-3849]*
- Policy Manager and Web UI now show the same interface status for Link Monitor. *[FBX-14702]*
- You can now configure Link Monitor when the Firebox has only one external interface. *[FBX-4325]*
- This release resolves an issue that caused the Firebox to incorrectly send TCP reset log messages when SD-WAN is configured. *[FBX-14982]*
- Probing both TCP and ICMP no longer marks the interface down when the upstream link is down. *[FBX-2413]*
- You can now configure a Virtual Interface as a failover option in Multi-WAN and SD-WAN. *[FBX-4395]*
- This release resolves an issue that changed the order of interfaces in SD-WAN when you renamed a participating interface. *[FBX-15093]*
- You can now modify the SD-WAN configuration after you change the name of a participating interface. *[FBX-15092]*
- Policy Manager now consistently displays the configured Link Monitoring setting. *[FBX-15026]*

Networking

- This release resolves an issue with Firebox Cloud for AWS in which multiple public or local IP addresses on an interface would break configured Static NATs. *[FBX-14983]*
- You can now configure OSPF and BGP in Policy Manager on Firebox T15 devices. *[FBX-15523]*
- This release improves the ability of the Firebox `fqdnd` process to handle DNS reply packets. *[FBX-15213, FBX-15200]*
- You can now configure domains that begin with an underscore in DNS forwarding. *[FBX-14233]*
- This release resolves an issue that caused the Firebox to drop Inter-VLAN traffic as spoofing when a different device handles the routing. *[FBX-14837]*
- In this release, the FQDN limit is raised to 2048 for Firebox M200, M270, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600, T55, T70, FireboxV, and Firebox Cloud. *[FBX-14836]*
- You can now configure a Static NAT with more than 47 characters in a destination FQDN. *[FBX-13502]*
- The Firebox no longer removes 1-to-1 NAT entries as duplicate because the interface names are too similar. *[FBX-7601]*
- Web UI no longer shows double values in Interface Bandwidth Graphs. *[FBX-3108]*
- This release resolves an issue that caused BGP to fail to advertise a network that includes a route map. *[FBX-15436]*
- Policy Manager no longer incorrectly changes the Firebox default gateway metric to 20 when you modify the network configuration. *[FBX-15687]*
- This release resolves an issue that caused slow VLAN throughput on Firebox M200/M300 devices. *[FBX-15461]*
- This release resolves a compatibility issue in which the network monitoring system NetXMS does not receive interface information over SNMP. *[FBX-10159]*
- Dynamic Routing no longer adds all learned routes with metric 20. *[FBX-15085]*
- This release resolves a `ripd` process crash issue. *[FBX-15199]*

Authentication

- RADIUS SSO configuration now supports shared secret values up to 64 characters in length. *[FBX-13991]*
- RADIUS server configuration now supports shared secret values up to 64 characters in length. *[FBX-13523]*
- The Firebox now uses the correct source IP address for connections when it switches between the primary and backup RADIUS servers. *[FBX-14092]*

VPN

- This release resolves an issue that caused non-VPN traffic to use the wrong interface when a zero-route BOVPN over TLS is configured. *[FBX-14835, FBX-14547*]
- The Firebox no longer disconnects Mobile VPN with SSL connections from users that share the same external IP address. *[FBX-14628]*
- This release resolves several IKE process crashes. *[FBX-14780, FBX-15359]*
- This release resolves a file descriptor leak issue in the `iked` process. *[FBX-14679]*
- You can now successfully use a group name created with Mobile VPN IPSec in Mobile SSLVPN with Web UI. *[FBX-13933]*
- You can now reconfigure L2TP from PSK to Certificate from Web UI. *[FBX-3267]*
- This release resolves an issue that caused the Mobile VPN with SSL client to fail to retrieve the client profile on connection. *[FBX-15432]*

Proxies and Services

- You can now add Geolocation exceptions that overlap with existing exceptions. *[FBX-10187]*
- The HTTPS proxy can now inspect connections with TLS v1.3 *[FBX-11152]*
- The Access Portal now supports TLS v1.2 encryption for RDP. *[FBX-13084]*
- The SMTP proxy now replies to non-STARTTLS connections with a 530 error code when STARTTLS Sender Encryption is required. *[FBX-15067]*
- The Explicit proxy now correctly handles and forwards URLs that include a port number, such as `http://www.example.com:80.` *[FBX-15209]*
- This release resolves an issue that caused IPS/Application Control to fail in environments with high traffic volume. *[FBX-14649]*
- This release resolves an issue that caused the IKE process to become stuck and fail to respond. *[FBX-15491]*
- This release improves IMAP proxy message handling to allow correct email retrieval instead of blank emails. *[FBX-11892]*
- This release resolves an issue that caused RDP sessions to freeze in the Access Portal for Chrome users. *[FBX-14843]*
- The OS Compatibility option in Policy Manager correctly removes legacy OCSP settings from HTTPS server proxy actions. *[FBX-14602]*
- Users no longer need to re-authenticate when they resize the Access Portal RDP browser window. *[FBX-10106]*
- All necessary domains are now added to the WatchGuard Threat Detection and Response policy when you enable first enable TDR. *[FBX-7319]*
- The Firebox TDR configuration no longer accepts invalid UUID values. *[FBX-12202]*
- The spamBlocker statistics `Total messages processed` value now includes the `Messages on white/black list` value. *[FBX-14847]*
- The HTTPS proxy can now correctly override the global Geolocation settings with Content Inspection enabled. *[FBX-14152]*
- Configuration options for RED are now cloned correctly for HTTP proxy actions. *[FBX-14767]*
- Gateway AV and Intelligent AV can now correctly scan files larger than 10MB in size. *[FBX-15215]*
- Log messages for HTTPS Proxy no longer have negative values in the rcvd_byte field. *[FBX-15190]*

Centralized Management

- You can now configure SD-WAN actions in a policy template. *[FBX-14772]*
- Policy templates now include QoS options in the advanced tab. *[FBX-3894]*
- You can now download the IKEv2 profile from Management Server with no invalid password error. *[FBX-15218]*
- You can now save a configuration with Policy Manager for a device that has a configured Dimension Command VPN tunnel. *[FBX-15138]*

Certificates

- This release resolves a crash issue with Web Server certificate imports. *[FBX-15281]*
- This release removes the `cn=Root Agency` certificate from the `Trusted CA for Proxies` store. *[FBX-15437]*
- A change to the Trusted CA for Proxies Certificate store no longer requires a reboot to take effect. *[FBX-15537]*

Firebox Integrations

- Autotask can now display company names that include non-US ASCII characters. *[FBX-14979]*
- The Firebox now includes a required client identifier in all ConnectWise requests. *[FBX-15527]*

Gateway Wireless Controller and WatchGuard APs

- Gateway Wireless Controller now displays the full wireless clients list. *[FBX-15430]*
- With the release of AP firmware 8.6.0-646 (AP120, AP320, AP322, AP325, AP420) and 8.6.0-644.3 (AP125), your AP no longer reserves an IP address for each VLAN on each SSID. An IP address is reserved for the management VLAN. *[AP-396]*

Download 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_4_U2.exe` — Use this file to install WSM v12.4 Update 2 or to upgrade WatchGuard System Manager from an earlier version.

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. 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 FireboxV device.

> The file name for software downloads will always include the product group, such as T30-T50 for the Firebox T30 or T50.

If you have…	Select from these Fireware OS packages
Firebox M4600/M5600	`Firebox_OS_M4600_M5600_12_4_U2.exe` `firebox_M4600_M5600_12_4_U2.zip`
Firebox M270/M370/M470/M570/M670	`Firebox_OS_M270_M370_M470_M570_M670_12_4_U2.exe` `firebox_M270_M370_M470_M570_M670_12_4_U2.zip`
Firebox M400/M500	`Firebox_OS_M400_M500_12_4_U2.exe` `firebox_M400_M500_12_4_U2.zip`
Firebox M440	`Firebox_OS_M440_12_4_U2.exe` `firebox_M440_12_4_U2.zip`
Firebox M200/M300	`Firebox_OS_M200_M300_12_4_U2.exe` `firebox_M200_M300_12_4_U2.zip`
Firebox T70	`Firebox_OS_T70_12_4_U2.exe` `firebox_T70_12_4_U2.zip`
Firebox T55	`Firebox_OS_T55_12_4_U2.exe` `firebox_T55_12_4_U2.zip`
Firebox T30/T50	`Firebox_OS_T30_T50_12_4_U2.exe` `firebox_T30_T50_12_4_U2.zip`
Firebox T35	`Firebox_OS_T35_12_4_U2.exe` `firebox_T35_12_4_U2.zip`
Firebox T15	`Firebox_OS_T15_12_4_U2.exe` `firebox_T15_12_4_U2.zip`
Firebox T10	`Firebox_OS_T10_12_4_U2.exe` `firebox_T10_12_4_U2.zip`

FireboxV
All editions for VMware
	`FireboxV_12_4_U2.ova`
	`Firebox_OS_FireboxV_12_4_U2.exe`
	`firebox_FireboxV_12_4_U2.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_4_U2_vhd.zip`
	`Firebox_OS_FireboxV_12_4_U2.exe`
	`Firebox_FireboxV_12_4_U2.zip`

Firebox Cloud	`FireboxCloud_12_4_U2.zip` `Firebox_OS_FireboxCloud_12_4_U2.exe`

Additional Firebox Software

The files in the list below are not directly used by the Firebox or for Firebox management, but are necessary for key features to work. In most cases, the file name includes the Fireware version that was current at the time of release.

Filename	Description	Updated in this release
WG-Authentication-Gateway_12_4.exe	**Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO**	✓
WG-Authentication-Client_12_3.msi	Single Sign-On Client software for Windows	
WG-SSOCLIENT-MAC_12_3.dmg	Single Sign-On Client software for macOS	
SSOExchangeMonitor_x86_12_0.exe	Exchange Monitor for 32-bit operating systems	
SSOExchangeMonitor_x64_12_0.exe	Exchange Monitor for 64-bit operating systems	
TO_AGENT_SETUP_11_12.exe	Terminal Services software for both 32-bit and 64-bit systems.	
WG-MVPN-SSL_12_2.exe	Moblie VPN with SSL client for Windows	
WG-MVPN-SSL_12_2.dmg	Mobile VPN with SSL client for macOS	
WG-Mobile-VPN_Windows_x86_1313_41322.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP [2]	
WG-Mobile-VPN_Windows_x86-64_1313_41322.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]	
WG-Mobile-VPN_macOS_x86-64_310_40218.dmg[1]	WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP [2]	
Watchguard_MVLS_Win_x86-64_200_rev19725.exe[1]	WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP [3]	

[1] This version number in this file name does not match any Fireware version number.

[2] There is a license required for this premium client, with a 30-day free trial available with download.

[3] 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 macOS 3.00 or later client. To update your bundle ID, contact WatchGuard Customer Support. Make sure to have your existing bundle ID available to expedite the update.

Upgrade to Fireware v12.4 Update 2

Important Information about the upgrade process:

- We recommend you use Fireware Web UI to upgrade to Fireware v12.x.
- 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 your Firebox has Fireware v12.1.1 or later, the Firebox might temporarily disable some security services to free up enough memory to successfully perform a backup. To learn more, see Backup and Restore for XTM 25, XTM 26, and Firebox T10.

> If you want to upgrade a Firebox T10 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. If your Firebox T10 has Fireware v12.1 or older, you might not be able to perform a backup before you upgrade the Firebox. This occurs because the memory use by Fireware v12.1 or older 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.

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 v12.4 Upgrade 2 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-group].sysa-dl* to the default location of C:\Program Files(x86)\Common Files\WatchGuard\resources\FirewareXTM\12.4\[product-group].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\12.4
4. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
5. Browse to the location of the *[product-group].sysa-dl* from Step 2 and click **Upgrade**.

If you have installed another version of Fireware v12.4 on your computer, you must run the Fireware v12.4 Update 2 installer twice (once to remove the older v12.4 software and again to install v12.4 Update 2).

Upgrade to Fireware v12.4 Update 2 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 *[product-group].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\12.4\[product-group].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\12.4.
4. Install and open WatchGuard System Manager v12.4 Update 2. Connect to your Firebox and launch Policy Manager.
5. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[product-group].sysa-dl* file from Step 2.

If you have installed another version of Fireware v12.4 on your computer, you must run the Fireware v12.4 Update 2 installer twice (once to remove the older v12.4 software and again to install v12.4 Update 2).

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.

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 APs 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	1.2.9.16
AP300	2.0.0.11
AP125	8.6.0-644.3
AP120, AP320, AP322, AP325, AP420	8.6.0-646

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 v12.4 Update 2

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.

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.

Fireware 12.4 Update 2 and WSM v12.4 Update 2 Operating System Compatibility Matrix

Last revised 26 April 2019

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10	Microsoft Windows 2008 R2, 2012, & 2012 R2	Microsoft Windows Server 2016 & 2019	Mac OS X/macOS v10.10, v10.11, v10.12, v10.13, & v10.14	Android 6.x, 7.x, 8.x, & 9.x	iOS v8, v9, v10, v11, & v12
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]			✓[4,5]	✓[5]	✓[5]
Mobile VPN with SSL	✓			✓	✓[6]	✓[6]
Mobile VPN with IKEv2	✓			✓	✓[7]	✓
Mobile VPN with L2TP	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *Windows 8.x support does not include Windows RT.*
- *For Windows Server 2008 R2, we support 64-bit only.*

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

- *IE 11*
- *Microsoft Edge42*

- *Firefox v64*
- *Safari 12*
- *Safari iOS 12*
- *Safari (macOS Mojave 10.14.1)*
- *Chrome v71*

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

[2] *Microsoft Exchange Server 2010 SP3 and 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 6.0, 6.5, 7.6, or 7.12 environment.*

[4] *WatchGuard Mobile VPN with IPSec client (NCP) v3.0 or above is required if you use macOS 10.13.*

[5] *Native (Cisco) IPSec client is supported for all recent versions of macOS and iOS.*

[6] *OpenVPN is supported for all recent versions of Android and iOS.*

[7] *StrongSwan is supported for all recent versions of Android.*

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 supported by WatchGuard*

	Active Directory	LDAP	RADIUS	SecurID	Firebox (Firebox-DB) Local Authentication	SAML
Mobile VPN with IPSec for iOS, Windows, and macOS	✓	✓	✓	✓	✓	–
Mobile VPN with IPSec for Windows by Shrew Soft	✓	✓	✓[1]	–	✓	–
Mobile VPN with IPSec for Android	✓	✓	✓	–	✓	–
Mobile VPN with SSL	✓	✓	✓	✓	✓	–
Mobile VPN with IKEv2 for WIndows	✓[2]	–	✓	–	✓	–
Mobile VPN with L2TP	✓[2]	–	✓	–	✓	–
Built-in Web Page on Port 4100 and 8080	✓	✓	✓	✓	✓	–
Access Portal	✓	✓	✓	✓	✓	✓
AD Single Sign-On Support *(with or without client software)*	✓	✓	–	–	–	–
Terminal Services Manual Authentication	✓	✓	✓	✓	✓	–
Terminal Services Authentication with Single Sign-On	✓	–	–	–	–	–

[1] The Shrew Soft client does not support two-factor authentication with challenge responses.

[2] 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 VMware and a Hyper-V environments, 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 2016, or 2019, 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	Memory (recommended)	Maximum vCPUs
Small	2048 MB[1]	2
Medium	4096 MB	4
Large	4096 MB	8
Extra Large	4096 MB	16

[1] 4096 MB is required to enable Intelligent AV.

Downgrade Instructions

Downgrade from WSM v12.4 Update 2 to earlier WSM v12.x or v11.x

If you want to revert from WSM v12.4 Update 2 to an earlier version, you must uninstall WSM v12.4 Update 2 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 v12.4 Update 2.

Next, install the same version of WSM that you used before you upgraded to WSM v12.4 Update 2. 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 v12.4 Update 2. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.4 Update 2 to earlier Fireware v12.x or v11.x

If you want to downgrade from Fireware v12.4 Update 2 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.4 Update 2. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.4 Update 2 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.

If you need to downgrade a Firebox without a backup file 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.

> If you use the Fireware Web UI or CLI to downgrade 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.

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, 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.

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

Localization

This release includes updates to the localization for the management user interfaces (WSM application suite and Web UI) through Fireware v12.2.1. UI changes introduced since v12.2.1 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 10 and want to use WSM in Japanese, go to Control Panel > Language and select Japanese 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

The latest version of localized Fireware Help is available on the Fireware documentation page. Updated documentation to match the localization updates in the UI will be released in several weeks.