

Fireware v12.1.3 Update 3 Release Notes

Supported Devices	XTM 25, XTM 26, XTM 33, XTM 330, XTM 515, XTM 525, XTM 535, XTM 545, XTM 1050, XTM 2050 XTM 8, 800, 1500, 2500 Series, and XTMv Firebox T10, T15, T30, T35, T50, T55, T70, M200, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600, FireboxV, Firebox Cloud, and WatchGuard AP
Release Date:	12.1.3 Update 3 -- 2 December 2019 Updated macOS applications -- 11 November 2019 12.1.3 Update 2 -- 4 February 2019
Release Notes Revision	3 February 2020
Fireware OS Build	12.1.3 Update 3 -- 608021 12.1.3 Update 2 -- 586018
WatchGuard System Manager Build	601717 (v12.5.1) 562818 (v12.1.3)
WatchGuard AP Device Firmware	For AP100, AP102, AP200: Build 1.2.9.16 For AP300: Build 2.0.0.11 For AP120, AP320, AP322, AP325, AP420: Build 8.8.0-179

Introduction



On 11 November 2019, WatchGuard released multiple new client applications for macOS. These releases add support for macOS Catalina 10.15, and require macOS High Sierra 10.13 or later. To learn more, see [macOS Catalina 10.15 software compatibility](#).

On 2 December, 2019, WatchGuard released Fireware v12.1.3 Update 3. This release features important fixes for wireless and VPN functionality.

On 4 February 2019, WatchGuard released Fireware v12.1.3 Update 2. This update includes fixes for several crash issues. There is no new release for WatchGuard System Manager. See *Enhancements and Resolved Issues in Fireware 12.1.3 Update 3* for more information.

For important information that might impact your upgrade experience, be sure to review the knowledge base article [Release-Specific Upgrade Notes](#).



This release is intended for users with XTM systems. If you use Firebox M-series, Firebox T-series, FireboxV or Firebox Cloud, we recommend you upgrade to the latest release for your device.

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 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, Firebox T 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.
- 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](#)

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>.

Known Issues and Limitations

Known issues for Fireware v12.1.3 Update 3 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.

Enhancements and Resolved Issues in Fireware 12.1.3 Update 3

General

- This release resolves TCP SACK panic kernel vulnerabilities (CVE-2019-11477, CVE-2019-11478, CVE-2019-11479). *[FB121X-93]*
- Gateway Wireless Controller now correctly displays list of managed AP devices and connected clients in both Firebox System Manager and Web UI. *[FBX121X-103,FB121X-112]*
- You can now manage a Firebox with BOVPN over TLS with a Default Route configuration with the external IP address. *[FB121X-81]*
- This release adds the Mobile VPN with SSL v12.5.2 client releases for direct download from the Firebox. *[FB121X-117]*
- You can now manually change the MTU for BOVPN Virtual Interfaces. *[FB121X-88]*

Resolved Issues in AP Firmware Update 8.8.0-192

- The transmit power is now correctly reported for AP120, AP320, and AP322 devices. *[AP-489]*
- APs can now correctly connect to WatchGuard servers if they receive a DNS suffix from DHCP. *[AP-534]*

Enhancements and Resolved Issues in WatchGuard IPSec Mobile VPN Client v14.0 for Windows

- This release supports QoS prioritization for outbound traffic through the Mobile VPN tunnel.
- You can now designate a zone as Home on a temporary basis.
- This release introduces Expert Mode for advanced client configuration.
- The client has new options to manage how internet connections function when the client is active.
- The Support Assistant now collects more useful log files for diagnosis of client issues by support.
- This release updates the directory structure for the Mobile VPN client installation for clarity and ease of troubleshooting.

- The NCP filter driver has been optimized for improved VPN throughput.
- The user interface now displays all options correctly when GUI scaling is enabled in Windows.

Enhancements and Resolved Issues in Mobile VPN with SSL Client v12.5.2 for macOS

- This release adds support for macOS 10.15 Catalina. *[FBX-17621]*

Enhancements and Resolved Issues in WatchGuard IPsec Mobile VPN Client v4.00 r46079 for macOS

- This release adds support for macOS 10.15 Catalina. *[FBX-17838]*
- The macOS client now uses a virtual network adapter to improve support for some VoIP applications.
- You can now connect and disconnect the selected connection with a right-click on the Dock menu icon.
- This release improves the handling of DNS requests for users with an active VPN connection.
- The Mobile VPN client now features an Always connection mode for continuous VPN connection or continuous attempts.

Enhancements and Resolved Issues in Fireware 12.1.3 Update 2

General

- This release resolves a crash issue with Web Server certificate imports. *[FBX-15281, FBX121X-71]*
- Time zone data has been updated to include recent changes to DST dates in Brazil. *[FBX-14272, FBX121X-51]*
- This release resolves multiple firewalld process crash issues. *[FBX-12778, FBX121X-67, FBX-14041, FBX121X-52]*
- This release resolves an s0 fault on XTMv and FireboxV virtual platforms. *[FBX-9758, FBX121X-38]*

Networking

- Fireboxes configured to use both Multi-WAN and dynamic routing no longer drop traffic unexpectedly with tcp syn checking failed log messages. *[FBX-14719, FBX121X-55]*
- Firebox T30/T50 devices no longer fail to resolve ARP for MAC addresses that end with :81:00. *[FBX-14022, FBX-121X-57]*

Proxies and Services

- This release resolves an issue with memory usage which would occur when users downloaded files larger than the configured GAV scan limit from a website that uses a very small data chunk size. *[FBX-13359, FBX121X-45]*
- This release resolves an issue which would cause IPS/Application Control to fail in environments with high traffic volume. *[FBX121X-68]*
- The Explicit proxy now correctly handles and forwards URLs that include a port number, such as `www.example.com:80`. *[FBX-15209, FB121X-70]*
- This release features enhancements to log messages for TDR. *[FBX-14974, FBX121X-62]*

VPN

- This release resolves multiple IKE process crash issues. [FBX-14780, FBX-12732, FBX121X-42, FBX-121X-56]
- This release resolved an issue in which VPN tunnels would fail to renegotiate when a large number of VIF tunnels are configured. [FBX-13976, FBX121X-46]

Enhancements and Resolved Issues in Mobile VPN with IPSec from NCP v13.13

- This release supports Windows 10 Version 1809.
- The VPN client icon now only appears in the system tray when you minimize the client. [FBX-13747]
- This release includes improvements to the silent installation option.

Enhancements and Resolved issues in Mobile VPN with IPSec from NCP 13.10

- This release features a 64-bit version of each component.
- The Windows version now matches Windows 10 user interface style correctly.
- You can now use the pre-connect login client to connect to a hotspot.

Enhancements and Resolved Issues in Fireware 12.1.3 Update 1

General

- The Arm LED light no longer unexpectedly turns off when a Firebox M200/M300 completes the bootup process. [FBX-11502, FBX121X-25]
- This release resolves a memory leak in the SNMP process. [FBX-10994, FBX121X-22]
- The Access Portal login page no longer enables autocorrect for the password field. [FBX-10204, FBX121X-10]
- This release resolves an issue that caused an invalid FQDN for a domain with many IP addresses. [FBX-11083, FBX121X-17]
- This release resolves a memory leak in the dhcpd process. [FBX-11633, FBX121X-29]
- This release resolves an issue that caused the OSS daemon to crash. [FBX-12228, FBX121X-27]
- Traffic Monitor now correctly displays data when an invalid UTF-8 character appears in a log message. [FBX-12268]

VPN

- This release resolves multiple issues that caused the iked process to crash. [FBX-12555, FBX-12524, FBX-10289, FBX121X-24, FBX-12611]
- This release resolves an issue that caused the Firebox to send decrypted BOVPN VIF tunnel traffic to the wrong interface. [FBX-11987, FBX121X-7]
- IKE_Auth initiator request packets larger than 28674 are now supported to improve IKEv2 interoperability with Cisco devices. [FBX-11644, FBX121X-13]

- This release resolves an issue that caused some UDP traffic to incorrectly route over a Branch Office VPN Virtual Interface tunnel. *[FBX-11488, FBX121X-26]*

Proxies and Services

- Proxy memory usage is improved. *[FBX-9563, FBX121X-11]*
- This release resolves an issue in which files that exceed Gateway AV scan limits fail to pass through the HTTP proxy. *[FBX-12046, FBX121X-18]*
- The `dnswatchd` process no longer uses CPU when the DNSwatch feature is not enabled. *[FBX-12198, FBX121X-14]*
- Subscription service updates no longer fail when you use the Firebox Cloud `pay as you go` license. *[FBX-11762, FBX121X-12]*
- This release resolves an issue with multiple file submissions by APT Blocker when enabled in the IMAP proxy. *[FBX-12376, FBX121X-19]*
- This release resolves an issue that prevented some applications that use a “custom TLS record type” from passing through the HTTPS proxy when matching a Domain Name configured to bypass content inspection. *[FBX-9478, FBX121X-30]*
- Web UI now allows you to disable Application Control when the license is expired. *[FBX121X-16]*
- This release resolves a proxy crash that caused general web browsing failure for users. *[FBX-12785]*
- This release resolves an attachment processing issue caused by the APT Blocker Message Hold feature. *[FBX-12213, FBX121X-20]*

Integrations

- Autotask or ConnectWise tickets for “botnet-detection threshold exceeded” are no longer created when Botnet Detection is first enabled. *[FBX-12237, FBX121X-23]*

Enhancements and Resolved Issues in Fireware 12.1.3

General

- This release removes weak ciphers that do not support forward secrecy from the Firebox web server. *[FBX-10752]*
- Web pages served by the Firebox now include security headers outlined in the OWASP Secure Headers Project in HTTP responses. *[FBX-9691]*
- This release resolves a vulnerability that made possible a SAML assertion replay attack against the Access Portal. *[FBX-9731]*
- This release corrects the Japanese localization of FireCluster upgrade error messages in Fireware Web UI. *[FBX-10941]*
- Firebox System Manager no longer reports an error when you view the Front Panel of a Firebox Cloud instance. *[FBX-10910]*
- Firebox System Manager no longer frequently disconnects when you connect to a Firebox with an older version of Fireware. *[FBX-11814]*
- This release resolves an issue that prevented certificate sync when the Firebox first joins a FireCluster. *[FBX-11449]*
- This release resolves an issue that caused all authenticated sessions to terminate after configuration changes are made to authentication server settings with Fireware Web UI. *[FBX-11263]*

Integrations

- This release resolves an issue that resulted in Autotask creating unintended duplicate configurations. *[FBX-11533]*
- Fireware Web UI no longer allows invalid configuration options that cause AutoTask to fail. *[FBX-11771]*

Networking

- This release resolves an issue that caused the Firebox to stop replying to DHCP requests. *[FBX-9213, FBX-10643]*
- This release resolves an issue that caused DHCP relay to stop working after a Firebox reboot. *[FBX-11464]*
- This release resolves an issue that caused the removal of the default route after PPPoE interface re-negotiation. *[FBX-11668]*
- The Huawei E3372 modem now works correctly. *[FBX-10888]*
- This release resolves an issue with the WebUI that prevented changing the Link Monitor settings on T10/T15 when using a Modem as external interface. *[FBX-11040, FBX-10535]*
- The Enable Link-Monitor check box no longer re-selects itself after you disable it. *[FBX-10214]*

Centralized Management

- Management Server now correctly restricts configuration options for active Directory based on RBAC role. *[FBX=9167]*

VPN

- Mobile VPN with SSL download page no longer fails to load for two-factor authentication users. *[FBX-10085]*
- This release resolves an issue that caused the Mobile VPN with SSL process to crash when FIPS is enabled on Firebox. *[FBX-2558]*
- BOVPN over TLS clients can now connect to a remote VPN server with its primary server configured as a domain name. *[FBX-11556]*
- This release resolves a kernel crash that occurs when Mobile VPN with SSL traffic is sent through a Virtual Interface (VIF). *[FBX-11800]*
- This release adds enhancements to BOVPN Dead Peer Detection when the Firebox is located behind a NAT device. *[FBX-11192]*
- This release adds several IPsec BOVPN stability improvements for Fireboxes in a NAT environment. *[FBX-11188]*
- This release resolves an issue that causes Managed Branch Office VPN tunnels to restart when the Management server changes the Firebox configuration. *[FBX-11400]*
- SLVPN Management tunnels can now use the # symbol as the first character of the password. *[FBX-11271]*
- This release resolves an issue that caused packet loss through Branch Office VPN on M4600 and M5600 with large amounts of traffic. *[FBX-11584]*

Proxies and Services

- This release reduces load on the Firebox processor caused by excessive proxy log messages. *[FBX-10691]*
- The HTTP proxy no longer fails to get the MD5 hash during a file upload when the file exceeds the Gateway AV scan limit. *[FBX-11577]*

- This release improves IPS and Application Control scanning when Content inspection is enabled on T15, T30 and XTM330 platforms. *[FBX-11354]*
- IMAP proxy connection count is now correctly reported in Proxy Connection Statistics for connections handled by the TCP-UDP proxy. *[FBX-10586]*
- This release resolves an issue that caused some websites to fail to load in the Chrome browser for connections through the HTTPS proxy with TCP MTU probing enabled. *[FBX-11280]*
- A FireCluster member without a DNSWatch license will now correctly register to the DNSWatch service when it becomes Master. *[FBX-10180]*
- This release resolves an issue that prevented HostWatch from correctly displaying data related to SIP and H323 proxies. *[FBX-10238]*
- This release includes several improvements in Proxy memory usage. *[FBX-11465, FBX-9256, FBX-10886]*
- This release resolves a memory leak that occurred when the IMAP proxy was enabled. *[FBX-11255]*
- This release resolves an issue that prevented mail from downloading through the IMAP proxy with log messages that included: “fail to parse fetch argument list”. *[FBX-10782]*
- The status of Content Inspection is now included in IMAP proxy log messages when viewed from the Fireware Web UI. *[FBX-10822]*
- Log messages generated by the IMAP Proxy now include the TLS Profile name configured in the proxy. *[FBX-10125]*

Wireless

- Gateway Wireless Controller updates of AP420 and AP325 no longer fail because of an AP reboot during the upgrade process. *[FBX-11081]*
- This release resolves an issue that caused the Firebox T35-W model to crash when wireless is enabled. *[FBX-9760]*

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_5_1.exe — Use this file to install WSM v12.5.1 or to upgrade WatchGuard System Manager from an earlier version to WSM v12.5.1.

WSM12_1_3.exe — Use this file to install WSM v12.1.3 or to upgrade WatchGuard System Manager from an earlier version to WSM v12.1.3.

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
XTM 800/1500/2500 Series	XTM_OS_XTM800_1500_2500_12_1_3_U3.exe xtm_xtm800_1500_2500_12_1_3_U3.zip
XTM 2050	XTM_OS_XTM2050_12_1_3_U3.exe xtm_xtm2050_12_1_3_U3.zip
XTM 1050	XTM_OS_XTM1050_12_1_3_U3.exe xtm_xtm1050_12_1_3_U3.zip
XTM 8 Series	XTM_OS_XTM8_12_1_3_U3.exe xtm_xtm8_12_1_3_U3.zip
XTM 5 Series, Models 515, 525, 535, and 545 only	XTM_OS_XTM5_12_1_3_U3.exe xtm_xtm5_12_1_3_U3.zip
XTM 330	XTM_OS_XTM330_12_1_3_U3.exe xtm_xtm330_12_1_3_U3.zip
XTM 33	XTM_OS_XTM3_12_1_3_U3.exe xtm_xtm3_12_1_3_U3.zip
XTM 25/26	XTM_OS_XTM2A6_12_1_3_U3.exe xtm_xtm2a6_12_1_3_U3.zip
XTMv All editions for VMware	xtmv_12_1_3_U3.ova XTM_OS_xtmv_12_1_3_U3.exe xtm_xtmv_12_1_3_U3.zip
XTMv All editions for Hyper-V	xtmv_12_1_3_U3_vhd.zip XTM_OS_XTMv_12_1_3_U3.exe xtm_xtmv_12_1_3_U3.zip
Firebox M4600/M5600	Firebox_OS_M4600_M5600_12_1_3_U3.exe firebox_M4600_M5600_12_1_3_U3.zip
Firebox M270/M370/M470/M570/M670	Firebox_OS_M270_M370_M470_M570_M670_12_1_3_U3.exe firebox_M270_M370_M470_M570_M670_12_1_3_U3.zip
Firebox M400/M500	Firebox_OS_M400_M500_12_1_3_U3.exe firebox_M400_M500_12_1_3_U3.zip
Firebox M440	Firebox_OS_M440_12_1_3_U3.exe firebox_M440_12_1_3_U3.zip
Firebox M200/M300	Firebox_OS_M200_M300_12_1_3_U3.exe firebox_M200_M300_12_1_3_U3.zip
Firebox T70	Firebox_OS_T70_12_1_3_U3.exe firebox_T70_12_1_3_U3.zip
Firebox T55	Firebox_OS_T55_12_1_3_U3.exe firebox_T55_12_1_3_U3.zip

If you have...	Select from these Fireware OS packages
Firebox T30/T50	Firebox_OS_T30_T50_12_1_3_U3.exe firebox_T30_T50_12_1_3_U3.zip
Firebox T35	Firebox_OS_T35_12_1_3_U3.exe firebox_T35_12_1_3_U3.zip
Firebox T15	Firebox_OS_T15_12_1_3_U3.exe firebox_T15_12_1_3_U3.zip
Firebox T10	Firebox_OS_T10_12_1_3_U3.exe firebox_T10_12_1_3_U3.zip
FireboxV All editions for VMware	FireboxV_12_1_3_U3.ova Firebox_OS_FireboxV_12_1_3_U3.exe firebox_FireboxV_12_1_3_U3.zip
FireboxV All editions for Hyper-V	FireboxV_12_1_3_U3_vhd.zip Firebox_OS_FireboxV_12_1_3_U3.exe Firebox_FireboxV_12_1_3_U3.zip
Firebox Cloud	FireboxCloud_12_1_3_U3.zip Firebox_OS_FireboxCloud_12_1_3_U3.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_3_1.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO	
WG-Authentication-Client_12_5_2.msi	Single Sign-On Client software for Windows	✓
WG-SSOCLIENT-MAC_12_3.dmg	Single Sign-On Client software for Mac OS X⁴	✓
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	Mobile VPN with SSL client for Windows	
WG-MVPN-SSL_12_5_2.dmg	Mobile VPN with SSL client for macOS⁴	✓
WG-Mobile-VPN_Windows_x86_1400_45109.exe¹	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP²	✓
WG-Mobile-VPN_Windows_x86_64_1400_45109.exe¹	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP²	✓
WG-Mobile-VPN_macOS_x86-64_400_46079.dmgg	WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP^{2,4}	✓
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.

⁴On 11 November 2019, WatchGuard released multiple new client applications for macOS. These releases add support for macOS Catalina 10.15, and require macOS High Sierra 10.13 or later. To learn more, see [macOS Catalina 10.15 software compatibility](#).

Upgrade to Fireware v12.1.3 Update 3



If your Firebox is a T10, XTM 25, or XTM 26 device with OS version 12.1 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](#).

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 your Firebox has Fireware v12.1.1 or later, the Firebox will 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](#).

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 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 v12.1.3 Update 3 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\12.1.3\[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\12.1.3`
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**.

Upgrade to Fireware v12.1.3 Update 3 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\12.1.3\[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\12.1.3.
4. Install and open WatchGuard System Manager v12.1.3. 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 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

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.

Update AP Devices



On 23 July 2018, WatchGuard released AP firmware version 8.5.0-658 for the AP320, AP322, AP325, and AP420. This release fixes several outstanding bugs and adds support for the new AP125 (coming soon).



On April 12, 2018, WatchGuard released AP firmware versions 1.2.9.15 for the AP100, AP102, and AP200, and 2.0.0.10 for the AP300 to address security vulnerabilities. We highly recommend you install these AP firmware updates. For more detailed information on these vulnerabilities, see [AP100/AP102/AP200 Chained Vulnerabilities](#). In addition to addressing these vulnerabilities, the AP firmware updates disable the AP local web UI. As these AP models can only be managed with the Gateway Wireless Controller, the AP local web UI is no longer supported.

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
AP120, AP320, AP322, AP325, AP420	8.8.0-192

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 v12.1.3 Update 3

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 12.1.3 Update 3 Operating System Compatibility Matrix

Last revised 2 December 2019

WSM/ Fireware Component	Microsoft Windows 8, 8.1, 10	Microsoft Windows 2012, & 2012R2	Microsoft Windows Server 2016 & 2019	macOS v10.13, v10.14, & v10.15	Android 6.x, 7.x, 8.x, & 9.x	iOS v8, v9, v10, v11, & v12
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers <i>For information on WatchGuard Dimension, see the Dimension Release Notes.</i>	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)¹		✓	✓			
Single Sign-On Client	✓	✓	✓	✓ ⁴		
Single Sign-On Exchange Monitor²		✓	✓			
Terminal Services Agent³		✓	✓			
Mobile VPN with IPSec	✓ ⁴			✓ ^{4,5}	✓ ⁵	✓ ⁵
Mobile VPN with SSL	✓			✓ ⁴	✓ ⁶	✓ ⁶
Mobile VPN with IKEv2	✓			✓ ⁴	✓ ⁷	✓
Mobile VPN with L2TP	✓			✓ ⁵	✓	✓

Notes about Microsoft Windows support:

- Windows 8.x support does not include Windows RT.
- Documentation might include references and examples for Windows OS versions that are no longer supported. This is provided to assist users with those OS versions, but we cannot guarantee compatibility.

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

- IE 11
- Microsoft Edge⁴²

- Firefox v66
- Safari 12
- Safari iOS 12
- Safari (macOS Mojave 10.14.1)
- Chrome v74

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

²Microsoft 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.

³Terminal 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.

⁴On 11 November 2019, WatchGuard released multiple new client applications for macOS. These releases add support for macOS Catalina 10.15, and require macOS High Sierra 10.13 or later. To learn more, see [macOS Catalina 10.15 software compatibility](#).

⁵Native (Cisco) IPsec client is supported for all recent versions of macOS and iOS.

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

⁷StrongSwan 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 Android	✓	✓	✓	–	✓	–
Mobile VPN with SSL	✓	✓	✓	✓	✓	–
Mobile VPN with IKEv2 for Windows	✓ ¹	–	✓	–	✓	–
Mobile VPN with L2TP	✓ ¹	–	✓	–	✓	–
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 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, 2016, or 2019.

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.x to earlier WSM v12.x or v11.x

If you want to revert to an earlier version of WSM, you must uninstall your current WSM version. 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 your current WSM version. .

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

Downgrade from Fireware v12.1.3 Update 3 to earlier Fireware v12.x or v11.x



If you use the Fireware Web UI or CLI to downgrade from Fireware v12.1.3 Update 3 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 v12.1.3 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 v12.1.3 Update 3. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.1.3 Update 3 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.

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 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*.