Fireware v12.6.2 Update 3 Release Notes

Supported Devices	Firebox T20, T40, T80, M270, M370, M400, M440, M470, M500, M570, M670, M4600, M4800, M5600, M5800 FireboxV, Firebox Cloud, WatchGuard AP
Release Date	20 August 2020 WSM Update 1: 27 August 2020 WSM Update 2: 25 September 2020 Fireware v12.6.2 Update 2: 5 October 2020 Fireware v12.6.2 Update 3: 22 October 2020
Release Notes Revision	02 November 2020
Fireware OS Build	12.6.2: 628197 12.6.2 Update 2: 630604 12.6.2 Update 3: 631387
WatchGuard System Manager Build	12.6.2: 628132 12.6.2 Update 1: 628957 12.6.2 Update 2: 630401
WatchGuard AP Firmware	AP120, AP320, AP322: 8.8.3-12 AP125, AP225W, AP325, AP327X, AP420: 8.9.0-63

On 22 October we released Fireware v12.6.2 Update 3 to address several significant bugs. See the *Enhancements and Resolved Issues in Fireware v12.6.2 Update 3* section for more information.

Introduction

With the release of Fireware v12.6.2 Update 3, we're happy to announce two new Fireware models: Firebox M4800 and M5800. These latest Firebox models are ideal as the ‘hub’ for distributed, hub-and-spoke type deployment scenarios and provide an upgrade path for our existing Firebox M Series customers.

Fireware v12.6.2 is also a maintenance release for Firebox T20, T40, T80 and is the first v12.6.x release for Firebox M Series (except M200 and M300), FireboxV, and Firebox Cloud appliances.

This release includes important bug fixes, and these feature improvements:

CSfC Mode

The U.S. National Security Agency (NSA) Commercial Solutions for Classified (CSfC) program certifies security-enabled products to be used for classified applications.

Fireware 12.6.2 includes enhancements to support NIAP Common Criteria certification against the Firewall and VPN protection profiles.

KVM Support

Kernel-based Virtual Machine (KVM) is the open source hypervisor included with Linux. Fireware v12.6.2 supports FireboxV on KVM.

Test WebBlocker Actions in Web UI (Fireware v12.6.2 Update 2)

In Fireware Web UI, you can now test WebBlocker actions. This helps you to determine if a WebBlocker action allows or blocks a specified URL before you enable the action.

Other Enhancements

- New Source Port settings in policy properties.
- Additional encryption options for Certificate Signing Requests (CSRs).
- Support for ICMPv6 policy templates.
- CA certificate verification for VPN peers.
- Predefined exceptions for URLs used by Panda products and services.

For a full list of the enhancements in this release, see Enhancements and Resolved Issues or review the What's New in Fireware v12.6.2 PowerPoint.

Fireware v12.6.x is based on Linux kernel 4.14. On some Firebox models, Linux kernel 4.14 does not provide sufficient quality and performance. Because of this, Fireware v12.6.x is not currently available for Firebox T10, T15, T30, T35, T55, T70, M200, and M300. We are continuing to work to bring all models to a common kernel in a future release. For more information, see this Knowledge Base article.

Before You Begin

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

- A supported WatchGuard Firebox. This device can be a WatchGuard Firebox T20, T40, T80, M270, M370, M400, M440, M470, M500, M570, M670, M4600, M4800, M5600, M5800, Firebox Cloud, or FireboxV. You cannot install Fireware v12.6.2 on any other Firebox model.
- 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. 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, 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.

Enhancements and Resolved Issues in Fireware v12.6.2 Update 3

- The SMTP-proxy now correctly handles emails with attachments when Gateway Antivirus is enabled. *[FBX-20080]*
- A problem has been resolved that caused a process crash when IPS or Application Control services scanned UDP traffic, The crash resulted in the error message: `Unable to handle kernel paging request - __do_udp_state_check`. *[FBX-20604]*

Enhancements and Resolved Issues in Fireware v12.6.2 Update 2

- In Fireware Web UI, you can now test WebBlocker actions to determine if they allow or block a specified URL. *[FBX-7897]*
- In the Default Packet Handling dialog box, the **Drop IP Source Route** check box is renamed to **Drop IP Source Route and Record Route Attacks** to better reflect the action that occurs. *[FBX-17826]*
- This release adds a new **fan-mode** command to the Command Line Interface for Firebox T80 devices. *[FBX-20280]*
- This release resolves an issue where HTTP Content Actions incorrectly handle HTTP POST requests. *[FBX-18838]*
- HTTP Basic Auth now works correctly when you use HTTP Content Actions with Gateway AntiVirus enabled. *[FBX-19782]*
- This release resolves a proxy memory leak. *[FBX-20203]*
- Firebox interfaces are no longer marked as down when an interface MTU is configured with a value greater than 1500. *[FBX-20414]*
- This release resolves a *networkV* memory leak with Firebox Cloud. *[FBX-19150]*
- Firebox Cloud devices no longer show virtual hard disk errors after upgrade. *[FBX-20356]*
- Certificates with CRL distribution points are no longer marked as revoked if the CRL response is not handled within the expected amount of time. *[FBX-20505, FBX-20345]*
- The Gateway AntiVirus scan process no longer incorrectly marks .GZIP and .DEB files as corrupt. *[FBX-20071]*
- This release resolves an *fwatch* process crash on Firebox Cloud devices. *[FBX-17188]*
- This release resolves kernel crashes. *[FBX-20379, FBX-20402]*
- This release resolves a memory leak in the *VPN IKED* process. *[FBX-20217]*
- This release improves logging for TLS negotiations when content inspection is enabled. *[FBX-19800]*
- Fireware Web UI now prevents the addition of users with reserved user names to the Firebox-DB authentication server. We recommend that you delete or replace any user with a reserved name before you upgrade to Fireware v12.6.2 Update 2.

  These user names are reserved: admin, all, any, Any-Multicast, BOVPN-Dimension-Allow, Hotspot-Users, Modem, None, PPTP, PPTP-Users, RADIUS-SSO-Users, SSL-VPN, SSLVPN-Users, SSLVPN-Mgmt-Clients, status, WebBlocker, WG-Loopback.

  After you upgrade, you cannot edit these users and can only delete them from the Command Line Interface. *[FBX-20347]*

- Gateway Wireless Controller now communicates successfully with Access Points that run AP Firmware 8.5.x or lower. *[FBX-20140]*
- This release resolves an issue with the *DHCP* process that caused the Firebox to not respond correctly to DHCP requests. *[FBX-20372]*
- This release resolves an issue that caused proxy connections to fail with the error log message "Failed to find policy for id = 131”. *[FBX-19216]*
- This release resolves an issue where you could not enable Network Discovery. *[FBX-20105]*
- SecurID PINs now work correctly with BOVPN. *[FBX-20121]*
- This release resolves a memory leak in the VPN *IKED* process. *[FBX-20217]*
- You can now assign device roles to users who have an @ symbol in their user name. *[FBX-20447]*
- This release resolves a crash in the *fwatch* process. *[FBX-20427]*
- Excessive API calls to Autotask servers no longer occur when the account name in the Firebox Autotask configuration is incorrect. *[FBX-20494]*
- Changes to a configuration on the Autotask server now correctly update the Firebox Autotask configuration. *[FBX-20511]*

WatchGuard IPSec Mobile VPN Client for Windows (v11.14)

- The client now prompts you to enter credentials when you set up the connection if you do not enter the VPN user name and password in the client configuration for IKEv2/EAP.
- This release resolves an issue where the Credential Provider did not appear correctly during Windows login if the WatchGuard Mobile VPN Client was not installed in the C:\Program Files directory.

Resolved Issues in WSM v12.6.2 Update 2

- When you import a certificate from Firebox System Manager through the Management Server, the **Passphrase** text box now populates correctly. *[FBX-20363, FBX-20364]*
- When the configuration contains BOVPN over TLS settings, you can now save the configuration to a Firebox that runs a Fireware version lower than v12.6.2. *[FBX-20422]*
- When Access Portal users contain an `@` symbol in their names, you can now save the configuration to a Firebox that runs Fireware v12.5.x. *[FBX-20453]*
- When a Management Tunnel exists with a name longer than 42 characters, you can now save the configuration to a Firebox that runs Fireware v12.5.3 or lower. *[FBX-20397]*
- When an alias exists with a name longer than 47 characters, you can now save the configuration to a Firebox that runs Fireware v12.5.x or lower. *[FBX-20450]*
- You can now change the **OS Compatibility** setting for Fireware to **11.9-11.12.x**. *[FBX-20286]*
- WatchGuard System Manager can now save changes to a device that runs Fireware v11.12.x or lower. *[FBX-20426]*
- Management Server v12.6.2 no longer saves invalid configurations to fully managed devices that run Fireware versions lower than v12.6.2. *[FBX-20408]*
- You can now change the **OS Compatibility** setting in Policy Manager from **12.6 or higher** to **11.9-11.12.x** and **12.0-12.5.x**. *[FBX-20308]*
- Firebox System Manager now displays data correctly for Firebox Cloud devices that run Fireware v12.5.2. *[FBX-19862]*
- When configuration objects exist with names longer than 42 characters, you can now save the configuration to a Firebox that runs Fireware v12.5.3 or lower. *[FBX-20404]*

Resolved Issues in WSM v12.6.2 Update 1

- Policy Manager now saves configurations to devices that run Fireware v12.5.4 or lower when Active Directory settings include a SearchUser DN value. *[FBX-20344]*
- Policy Manager now saves configurations to devices that run Fireware v12.5.4 or lower when you add a Firebox-DB admin user in Fireware Web UI. *[FBX-20346]*
- Policy Manager no longer deletes previously added IP addresses from an alias when you edit the alias from a policy. *[FBX-20349]*
- Policy Manager no longer deletes an alias when you edit it from **Setup > Aliases**. *[FBX-20359]*
- This release resolves an issue where you could not create a policy from the Mobile VPN with IPSec tab in Policy Manager if the policy name included periods. *[FBX-20355]*

Enhancements and Resolved Issues in WSM and Fireware v12.6.2

General

- Fireware now supports FireboxV on the open source KVM hypervisor.
- The Command Line Interface now includes a `CSfC enable` command to enable CSfC mode on the Firebox. *[FBX-17850]*
- In Firebox System Manager, it now takes less time to delete multiple entries from the Blocked Sites List. *[FBX-10061]*
- This release resolves an issue that caused a kernel panic crash when the Blocked Sites List contained many configured FQDNs. *[FBX-19855]*
- The Firebox Web Server no longer accepts connections that use TLS 1.1 or lower. *[FBX-19392]*
- This release resolves an issue that caused WatchGuard Cloud registration failures on non-TPM platforms after a backup image was restored. *[FBX-17394]*
- This release resolves a kernel crash. *[FBX-16496]*
- Updated localized Fireware Help is now available from Help Center. Localized Help content for AuthPoint and WatchGuard Cloud is also now available for the first time.

> Although some Web UI and Policy Manager fields might accept Unicode characters, problems can occur if you enter non-ASCII characters in those fields.

Authentication

- When enabled, logon disclaimer text now appears before an administrative user logs in.*[FBX-19079]*
- The `Sessiond` log messages now shows the RADIUS authentication server type correctly when an email address is used as a username. *[FBX-19287]*
- This release resolves an issue that caused the incorrect SSO Agent version to appear in Authentication debug log messages. *[FBX-19936]*
- This release resolves an issue that affected communication between Fireboxes and the 12.5.4 SSO Agent. *[FBX-19996]*

Certificates

- Certificate Signing Requests (CSRs) now support RSA 3072, RSA 4096, ECDSA P-256, and ECDSA P-38 encryption settings. *[FBX-19137]*
- This release includes updated Trusted CA Certificates. *[FBX-19545]*

Networking

- This release resolves a memory leak with the Firebox multicast routing feature. *[FBX-14823]*
- In Firebox System Manager, the Status Report now shows the total number of DHCP leases in use on the Firebox. *[FBX-17654]*
- In Drop-in mode, DNS forwarding to configured DNS servers now works correctly when DNSWatch is enabled. *[FBX-19220]*
- This release resolves a crash in the `dhcprelayd` process. *[FBX-19956]*

Proxies and Security Services

- Some firewall policies now include Source Port settings on the Advanced tab to limit policy scope based on the source port of the connection. *[FBX-19003]*
- You can now configure a custom firewall policy template for ICMPv6. *[FBX-18148]*
- By default, WebBlocker now allows users to view a website when the WebBlocker server times out. *[FBX-19378]*
- To allow connections to Panda products and services through the Firebox, URLs were added to the WebBlocker Exceptions list, Blocked Sites Exceptions list, and the HTTPS-Proxy predefined list of Content Inspection Exceptions. *[FBX-19582/FBX19583]*
- When you upgrade to Fireware v12.6.2, configurations that have a Gateway AntiVirus scan limit lower than the minimum value for the Firebox model are automatically updated to use the default scan limit for that model. *[FBX-16773]*
- The reverse proxy in Access Portal no longer logs out active user sessions. *[FBX-16699]*
- Access Portal RDP connections now use the complete browser window on hosts that have a non-100% Display Scale setting for different resolutions. *[FBX-17866]*
- The Command Line Interface now includes a `show file_exceptions` command that shows the list of configured file exceptions. *[FBX-19007]*
- The `X-WatchGuard-Spam-ID:` header is no longer truncated in messages processed by spamBlocker. *[FBX-20016]*
- Macro-enabled Microsoft Office documents are now correctly identified by the IMAP-proxy. *[FBX-19955]*

VPN

- In the BOVPN and BOVPN virtual interface configurations, you can now specify a root or intermediate CA certificate for VPN peer verification. *[FBX-18842]*
- This release resolves an issue where AuthPoint did not request a push notification for some Android-based IKEv2 clients. *[FBX-19102]*
- The Command Line Interface `show sslvpn` command now shows if `default-route-client` is in use for Mobile VPN with SSL. *[FBX-19253]*
- You can now use the Command Line Interface to increase the authentication timeout for Mobile VPN with IKEv2 connections. *[FBX-19386]*
- This release resolves an issue where Mobile VPN with IPSec users were sometimes disconnected when a different user connected. *[FBX-19669]*
- Mobile VPN with IKEv2 user sessions are now cleared correctly if there are no matching phase 1 SAs for the user. *[FBX-19890]*

- To prevent Mobile VPN login issues, the Firebox now automatically converts Mobile VPN with SSL and IKEv2 Groups that are not configured correctly. *[FBX-19960]*
- Traffic that traverses a BOVPN Virtual Interface is no longer processed as *Unhandled* if the interface name starts with a `+` or `*` character. *[FBX-20098]*
- Firebox System Manager now correctly displays authenticated mobile VPN users in the Front Panel. *[FBX-16739]*
- This release resolves a crash in the `iked` process that occurred when source ports change in established mobile VPN connections. *[FBX-19399]*

Gateway Wireless Controller

- The Gateway Wireless Controller now displays the correct number of connected users after an AP firmware upgrade to v8.9.0-63. *[FBX-20124]*
- In Firebox System Manager, the Gateway Wireless Controller tab now correctly shows the firmware version for each AP. *[FBX-18212]*

Known Issues and Limitations

Known issues for Fireware v12.6.2 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.

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:

> `WSM_12_6_2_U2.exe` — Use this file to install WSM v12.6.2 Update 2 or to upgrade WatchGuard System Manager from an earlier version.

Fireware OS

You can upgrade the Fireware OS on your Firebox automatically from the Fireware Web UI **System > Upgrade OS** page or from WatchGuard Cloud.

If you prefer to upgrade from Policy Manager, or from an earlier version of Fireware, you can 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 T20_T40 for the Firebox T20 or T40.

If you have…	Select from these Fireware OS packages
Firebox M270/M370/M470/M570/M670	`Firebox_OS_M270_M370_M470_M570_M670_12_6_2_U3.exe` `firebox_M270_M370_M470_M570_M670_12_6_2_U3.zip`
Firebox M400/M500	`Firebox_OS_M400_M500_12_6_2_U3.exe` `firebox_M400_M500_12_6_2_U3.zip`
Firebox M440	`Firebox_OS_M440_12_6_2_U3.exe` `firebox_M440_12_6_2_U3.zip`
Firebox M4600/M5600	`Firebox_OS_M4600_M5600_12_6_2_U3.exe` `firebox_M4600_M5600_12_6_2_U3.zip`
Firebox M4800/M5800	`Firebox_OS_M4800_M5800_12_6_2_U3.exe` `firebox_M4800_M5800_12_6_2_U3.zip`
Firebox T20/T40	`Firebox_OS_T20_T40_12_6_2_U3.exe` `Firebox_OS_T20_T40_12_6_2_U3.zip`
Firebox T80	`Firebox_OS_T80_12_6_2_U3.exe` `Firebox_OS_T80_12_6_2_U3.zip`

FireboxV
All editions for VMware
	`FireboxV_12_6_2_U3.ova`
	`Firebox_OS_FireboxV_12_6_2_U3.exe`
	`firebox_FireboxV_12_6_2_U3.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_6_2_vhd_U3.zip`
	`Firebox_OS_FireboxV_12_6_2_U3.exe`
	`Firebox_FireboxV_12_6_2_U3.zip`

Firebox Cloud	`FireboxCloud_12_6_2_U3.zip` `Firebox_OS_FireboxCloud_12_6_2_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_5_4.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO	No
WG-Authentication-Client_12_5_4.msi	Single Sign-On Client software for Windows	No
WG-SSOCLIENT-MAC_12_5_4.dmg	Single Sign-On Client software for macOS	No
SSOExchangeMonitor_x86_12_0.exe	Exchange Monitor for 32-bit operating systems	No
SSOExchangeMonitor_x64_12_0.exe	Exchange Monitor for 64-bit operating systems	No
TO_AGENT_SETUP_11_12.exe	Terminal Services software for both 32-bit and 64-bit systems.	No
WG-MVPN-SSL_12_5_3.exe	Mobile VPN with SSL client for Windows	No
WG-MVPN-SSL_12_5_3.dmg	Mobile VPN with SSL client for macOS	No
WG-Mobile-VPN_Windows_x86_1411_48297.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP [2]	No
WG-Mobile-VPN_Windows_x86-64_1411_48297.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]	No
WG-Mobile-VPN_macOS_x86-64_400_46079.dmg[1]	WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP [2]	No
Watchguard_MVLS_Win_x86-64_200_rev19725.exe[1]	WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP [3]	No

[1] The 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.

[4] SSO Agent v12.5.4 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.5.4, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.5.4, we recommend that you upgrade all SSO Clients to v12.5.4. You cannot use SSO Client v12.5.4 with versions of the SSO Agent lower than v12.5.4. Fireware v12.6.2 supports previous versions of the SSO Agent.

Upgrade to Fireware v12.6.2 Update 3

Important information about the upgrade process:

- You can use WatchGuard Cloud, Fireware Web UI, or Policy Manager to upgrade your Firebox.
- 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.
- In Fireware v12.6.2 Update 2, Fireware Web UI prevents the addition of users with reserved user names to the Firebox-DB authentication server. We recommend that you delete or replace any user with a reserved name before you upgrade to Fireware v12.6.2 Update 2 or higher. For more information, see Enhancements and Resolved Issues.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous 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.

For instructions on how to back up your Management Server configuration, see Fireware Help.

Upgrade to Fireware v12.6.2 Update 3 from WatchGuard Cloud

From WatchGuard Cloud, you can upgrade the firmware for a Firebox that runs Fireware v12.5.2 or higher. To upgrade from WatchGuard Cloud, see Upgrade Firmware from WatchGuard Cloud in *WatchGuard Cloud Help*.

Upgrade to Fireware v12.6.2 Update 3 from Web UI

You can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. To upgrade manually, see Upgrade Fireware OS or WatchGuard System Manager in *Fireware Help*.

If your Firebox runs Fireware v11.9.x or lower, follow the steps in this knowledge base article.

If you have installed another release of this OS version on your computer, you must run the installer twice (once to remove the previous release and again to install this release).

Upgrade to Fireware v12.6.2 Update 3 from WSM/Policy Manager

To upgrade from WSM/Policy Manager, see Upgrade Fireware OS or WatchGuard System Manager in *Fireware Help*.

If you have installed another release of this OS version on your computer, you must run the installer twice (once to remove the previous release and again to install this release).

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 Access Points

All AP 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.

AP Firmware Upgrade

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.**

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

To manually update firmware on your APs:

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

About AP Firmware and Fireware Versions

You must upgrade your APs to firmware version 8.6.0 or higher before you upgrade to Fireware v12.5.4 or higher to remain compatible with the latest versions of Fireware.

Important Steps for Upgrades from Fireware v12.0 or Lower

If you have not previously upgraded to Fireware v12.0.1 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 before you can manage the APs from Gateway Wireless Controller.

Depending on the version of Fireware you upgrade 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.

Upgrade your FireCluster to Fireware v12.6.2

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.

Fireware 12.6.2 Operating System Compatibility Matrix

Last reviewed 11 August 2020

WSM/ Fireware Component	Microsoft Windows, 8.1, 10	Microsoft Windows 2012, & 2012 R2	Microsoft Windows Server 2016 & 2019	macOS v10.13, v10.14, & v10.15	Android 7.x, 8.x, 9.x, & 10.x	iOS v9, v10, v11, v12, & v13
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	✓	✓	✓	✓[4]		
Single Sign-On Exchange Monitor[2]		✓	✓			
Terminal Services Agent[3]		✓	✓			
Mobile VPN with IPSec	✓			✓[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 13*
- *Safari (macOS Catalina)*
- *Chrome v74*

[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] 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.

[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*

	AuthPoint	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

A WatchGuard FireboxV virtual machine can run on:

- VMware ESXi 6.0, 6.5, or 6.7
- Windows Server or Hyper-V Server 2012 R2, 2016, or 2019
- Linux KVM

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 IntelligentAV.

Downgrade Instructions

Downgrade from WSM v12.6.2

If you want to revert from WSM v12.6.2 to an earlier version, you must uninstall WSM v12.6.2. 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 v12.6.2.

Next, install the same version of WSM that you used before you upgraded to WSM v12.6.2. 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 v12.6.2. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.6.2

If you want to downgrade from Fireware v12.6.2 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.6.2. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.6.2 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.

> ℹ 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 v12.5.2. UI changes introduced since v12.5.2 might 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

> Although some other Web UI and Policy Manager fields might accept Unicode characters, problems can occur if you enter non-ASCII characters in those fields.

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the Fireware 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 from WatchGuard Help Center. In the top-right of a Fireware Help page, click the Globe icon and select your language from the drop-down list.