Fireware v12.7.2 Update 2 Release Notes

Supported Devices	Firebox T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, M570, M590, M670, M690, M4600, M4800, M5600, M5800 FireboxV, Firebox Cloud, WatchGuard AP Firebox M290, M390, M590, M690
Release Date	WSM 12.7.2 Update 3 — 24 February 2022 12.7.2 Update 2 — 23 February 2022 12.7.2 Update 1— 30 December 2021 12.7.2 — 5 October 2021
Release Notes Revision	15 April 2022
Fireware OS Build	12.7.2 Update 2 — 655803 12.7.2 Update 1 for Firebox T20/40/55/70/80, Firebox M270/370/400/500/570/670/4600/4800, Firebox Cloud, FireboxV — 652282 12.7.2 Update 1 for Firebox M290/390/590/690 — 652363 12.7.2 — 647073
WatchGuard System Manager Build	12.7.2 Update 3 — 656168 12.7.2 Update 2 — 655822 12.7.2 — 645573
WatchGuard AP Firmware	AP120, AP320, AP322: 8.8.3-12 AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36

Introduction

After you upgrade to Fireware v12.7.2 Update 2 or higher, you cannot downgrade to a previous Fireware version. For more information, see this Knowledge Base article.

AP Firmware Update v11.0.0-36

On 28 February 2022, WatchGuard released AP firmware v11.0.0-36. This firmware update resolves the FragAttacks vulnerabilities for the AP125, AP225W, AP325, AP327X, and AP420. For more information, see WatchGuard Wi-Fi products and the FragAttacks vulnerabilities.

WSM v12.7.2 Update 3

On 24 February 2022, WatchGuard released WSM v12.7.2 Update 3 to resolve an issue with the WSM Cyclops Blink Detector. See *Enhancements and Resolved Issues in WSM v12.7.2 Update 3* for more information.

Fireware v12.7.2 Update 2

On 23 February 2022, WatchGuard released Fireware v12.7.2 Update 2. This release includes a number of security enhancements. See *Enhancements and Resolved Issues in WSM v12.7.2 Update 3* for more information.

Do not upgrade the Firebox to v12.7.2 Update 2 until you read this Knowledge Base article about Cyclops Blink. If your Firebox is affected by Cyclops Blink, you must follow the remediation steps in the article to upgrade safely. If you do not follow the remediation steps and your Firebox is infected with Cyclops Blink or there is another issue with Firebox system integrity, your Firebox will shut down at reboot and you cannot connect to it.

WSM Cyclops Blink Detector

You can use the WSM Cyclops Blink Detector to diagnose whether or not a Firebox is infected by Cyclops Blink. This tool can scan individual locally-managed or cloud-managed Fireboxes, and multiple devices managed by WSM Management Server. To run the tool, in WSM, select **Tools > Cyclops Blink**.

WatchGuard also provides Cyclops Blink detection tools online and in WatchGuard Cloud. For more information about these tools and Cyclops Blink, see this Knowledge Base article.

System Integrity Checks

The Firebox now verifies the integrity of the appliance each time the Firebox boots, and the integrity of the upgrade file before each software upgrade. You can also run an on-demand integrity check from Fireware Web UI.

Firebox Management Policy Warnings

You now see a warning in the **Front Panel** and **Policies** pages (Fireware Web UI) and above the firewall policy list (Policy Manager) when your configuration includes a Firebox management policy that allows unrestricted Internet access to your Firebox.

Downgrade Restrictions

After you upgrade to this Fireware release, you cannot downgrade to a version of Fireware lower than Fireware v12.7.2 Update 2.

When WatchGuard releases future Fireware versions, you will be able to downgrade to Fireware v12.7.2 Update 2 or higher.

Fireware v12.7.2 Update 1

On 30 December 2021, WatchGuard released Fireware v12.7.2 Update 1. See *Enhancements and Resolved Issues in WSM v12.7.2 Update 3* for more information.

Fireware v12.7.2

Fireware v12.7.2 adds support for the new Firebox M290, M390, M590, M690 models and provides numerous bug fixes and feature enhancements.

Introducing New Firebox Models

WatchGuard continues our mission to deliver powerful performance and security services with the release of the Firebox M290, M390, M590, and M690. These new Firebox appliances provide an upgrade path for existing M Series customers,

- Faster and more powerful – Each appliance benefits from improved performance (especially for HTTPS throughput) and more on-board memory for more efficient scanning.
- Flexible and future-proof – Module expansion bays and available expansion modules enable you to customize your port configuration to meet current needs while ensuring the flexibility to adapt as the network evolves.
- Extensible – Add modules to increase the number of copper or fiber ports available to support the growing use of 10G copper and fiber in midsize enterprise data centers.
- Optional PoE+ ports on the Firebox M590 and M690 – Simplify the process of powering other devices, like security cameras or WatchGuard Wi-Fi Access Points.
- Reliable – Redundant power supplies on the Firebox M590 and M690 ensures maximum availability.

For a full list of the enhancements in this release, see *Enhancements and Resolved Issues in WSM v12.7.2 Update 3* or review the What's New in Fireware v12.7.2 PowerPoint.

Fireware v12.7.2 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 v12.7.2 is not available for Firebox T10, T15, T30, T35, M200, and M300. We continue to support these models with Fireware v12.5.x. 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 Firebox T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, M570, M590, M670, M690, M4600, M4800, M5600, M5800
  FireboxV, Firebox Cloud, WatchGuard AP.
- 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 the 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 WSM v12.7.2 Update 3

- The WSM Cyclops Blink Detector now correctly scans Fireboxes that run Fireware v12.7.2 Update 2, Fireware v12.5.9 Update 2, or Fireware v12.1.3 Update 8. *[FBX-22843]*
- This release resolves an error that appeared when you saved a configuration to a Firebox M290 device. *[FBX-22851]*

Enhancements and Resolved Issues in Fireware v12.7.2 Update 2

- This release resolves a vulnerability that could allow an unauthenticated user to execute arbitrary code on the Firebox (CVE-2022-26318). *[FBX-22786]*
- WSM now includes the WSM Cyclops Blink Detector that you can use to diagnose whether or not a Firebox is infected by Cyclops Blink. *[FBX-22694]*
- The Firebox now automatically runs integrity checks at boot time and when Fireware upgrades. You can also run on-demand system integrity checks from Fireware Web UI. *[FBX-22205]*
- If you have a Firebox management policy that allows unrestricted Internet access to your Firebox, you now see a warning message in Policy Manager and Fireware Web UI. *[FBX-22562]*
- You can no longer enable FIPS mode. *[FBX-22628]*
- This release removes expired certificates from the trusted CA certificates list. *[FBX-21783]*
- This release resolves an issue that caused Fireware Web UI to become unresponsive when you managed FireCluster. *[FBX-16790]*
- TDR Host Sensor enforcement now works correctly when AuthPoint is used as an authentication server. *[FBX-21902]*
- The Firebox now correctly resolves LDAP/RADIUS FQDNs received from AuthPoint. *[FBX-22011]*
- This release resolves an issue that caused SAML logins to the Access Portal to fail. *[FBX-22206]*
- 802.1p marking now works correctly on external interfaces that use VLAN with PPPoE. *[FBX-22336]*
- You can now correctly set the link speed to 10Gbps on a link aggregation interface. *[FBX-21657]*
- This release resolves a vulnerability that could allow an authenticated, unprivileged management user to retrieve certificate private keys (CVE-2022-25290). *[FBX-22680]*
- This release resolves several buffer overflow vulnerabilities in the firmware upgrade process (CVE-2022-25291, CVE-2022-25292, CVE-2022-25293). *[FBX-22719, FBX-22720, FBX-22738]*
- This release resolves a vulnerability that could allow an authenticated management user to upload arbitrary files (CVE-2022-25360). *[FBX-22593]*
- This release resolves a vulnerability that could allow an authenticated, unprivileged management user to modify other management user credentials (CVE-2022-25363). *[FBX-22594]*
- The OS Checksum feature is now deprecated.
- WatchMode is currently unavailable.

Enhancements and Resolved Issues in Fireware v12.7.2 Update 1

- This release includes several general security enhancements. *[FBX-21579, FBX-21596, FBX-21590]*
- This release includes a security enhancement for Fireware Web UI. *[FBX-22493]*

- When IPS is enabled and configured to auto-block threats, the source IP address is now correctly blocked. *[FBX-22034]*
- The IPS signature set no longer blocks internal mail servers when a brute scan attack occurs. *[FBX-17255, FBX-17486]*

Enhancements and Resolved Issues in Fireware v12.7.2

General

- This release adds modem support for the Huawei E3372 USB LTE Variant. *[FBX-20723]*
- An issue that caused a firewall crash to occur is resolved. *[FBX-21958]*
- This release fixes an incorrect Policy Manager link to the certification portal when you use the French localized user interface. *[FBX-22014]*
- The CLI command **show status-report** has been updated to display the OEM serial number to identify whether a Firebox has a populated TPM chip. *[FBX-22036]*
- This release resolves an issue that caused the *wgagent* process to crash. *[FBX-22066]*
- A system crash is resolved that occurred when connections to the log server are broken because of a log process problem. *[FBX-21768]*
- A crash issue is resolved that occurred when the *loggerd* logging process was blocked when trying to send communications to other Firebox processes. *[FBX-21700]*
- Policy Manager can now save changes to Fireboxes that use v12.5.7 or lower with no DNS cache window prompt. *[FBX-21928]*

Proxies and Subscription Services

- A new SIP-proxy CLI command, **extended-rewrite**, adds support for compatibility with G12 Communications cloud-based PBX systems. *[FBX-20939]*
- An issue that caused DNSWatch to refuse requests is resolved. *[FBX-22069]*
- An issue is resolved that caused the IMAP proxy to crash when it processed connections. *[FBX-22112]*
- Several issues that caused proxy crash issues are resolved. *[FBX-21213, FBX-21961]*
- The DNS forwarding address no longer changes when you add a new DHCP reservation on a VLAN. *[FBX-22018]*

Networking and VPN

- VPNs now work correctly with VPN tunnels created with Management Server that use certificates. *[FBX-22012]*
- This release resolves an issue with the user permissions associated with the Mobile VPN with SSL Client for macOS installation folder. *[FBX-21854]*
- An *iked* process crash is resolved. *[FBX-21659, FBX-21786]*
- You can now correctly adjust the Access Portal reverse proxy buffer settings with the CLI. *[FBX-22043, FBX-17336]*
- An issue is resolved that caused the *ADMD* authentication process to reach 100% capacity and stop processing connections because of a Management Server negotiation problem. *[FBX-18014]*

Authentication

- You can now choose to enable or disable Active Directory (AD) Mode in the SSO Agent Configuration Tool. AD Mode is now disabled by default. *[FBX-21898]*
- Secondary authentication servers now correctly show in Fireware Web UI after an upgrade to Fireware v12.7.1 or higher. *[FBX-22048]*

- The number of supported Terminal Service Agents is increased to 512. *[FBX-21545]*
- An Access Portal authentication problem issue is resolved. This issue occurred when using the authentication portal on port 4100 and caused the error *502 Bad Gateway*. *[FBX-21840]*

Resolved Issues in AP Firmware v11.0.0-36

- This firmware update resolves the FragAttacks vulnerabilities for the AP125, AP225W, AP325, AP327X, and AP420. For more information, see WatchGuard Wi-Fi products and the FragAttacks vulnerabilities.

Known Issues and Limitations

Known issues for Fireware v12.7.2 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_7_2_U3.exe` — Use this file to install WSM 12.7.2 Update 3 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 always includes 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_7_2_U2.exe` `firebox_M270_M370_M470_M570_M670_12_7_2_U2.zip`
Firebox M290	`Firebox_OS_M290_12_7_2_U2.exe` `firebox_M290_12_7_2_U2.zip`
Firebox M390	`Firebox_OS_M390_12_7_2_U2.exe` `firebox_M390_12_7_2_U2.zip`
Firebox M400/M500	`Firebox_OS_M400_M500_12_7_2_U2.exe` `firebox_M400_M500_12_7_2_U2.zip`
Firebox M440	`Firebox_OS_M440_12_7_2_U2.exe` `firebox_M440_12_7_2_U2.zip`
Firebox M590/M690	`Firebox_OS_M590_M690_12_7_2_U2.exe` `firebox_M590_M690_12_7_2_U2.zip`
Firebox M4600/M5600	`Firebox_OS_M4600_M5600_12_7_2_U2.exe` `firebox_M4600_M5600_12_7_2_U2.zip`
Firebox M4800/M5800	`Firebox_OS_M4800_M5800_12_7_2_U2.exe` `firebox_M4800_M5800_12_7_2_U2.zip`

If you have…	Select from these Fireware OS packages
Firebox T20/T40	Firebox_OS_T20_T40_12_7_2_U2.exe Firebox_OS_T20_T40_12_7_2_U2.zip
Firebox T55	Firebox_OS_T55_12_7_2_U2.exe firebox_T55_12_7_2_U2.zip
Firebox T70	Firebox_OS_T70_12_7_2_U2.exe firebox_T70_12_7_2_U2.zip
Firebox T80	Firebox_OS_T80_12_7_2_U2.exe Firebox_OS_T80_12_7_2_U2.zip
FireboxV All editions for VMware	FireboxV_12_7_2_U2.ova Firebox_OS_FireboxV_12_7_2_U2.exe firebox_FireboxV_12_7_2_U2.zip
FireboxV All editions for Hyper-V	FireboxV_12_7_2_U2_vhd.zip Firebox_OS_FireboxV_12_7_2_U2.exe firebox_FireboxV_12_7_2_U2.zip
Firebox Cloud	Firebox_OS_FireboxCloud_12_7_2_U2.exe firebox_FireboxCloud_12_7_2_U2.zip

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.

File name	Description	Updated in this release
WG-Authentication-Gateway_12_7_2.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO	Yes (12.7.2)
WG-Authentication-Client_12_7.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

File name	Description	Updated in this release
WG-MVPN-SSL_12_7_2.exe	Mobile VPN with SSL client for Windows[5]	Yes (12.7.2)
WG-MVPN-SSL_12_7_2.dmg	Mobile VPN with SSL client for macOS[5]	Yes (12.7.2)
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 higher 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 v12.7 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.7, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.7, we recommend that you upgrade all SSO Clients to v12.7. You cannot use SSO Client v12.7 with versions of the SSO Agent lower than v12.5.4. Fireware v12.7.2 supports previous versions of the SSO Agent.

[5] Not supported on ARM processor architecture.

Upgrade to Fireware v12.7.2 Update 2

Do not upgrade the Firebox to Fireware v12.7.2 Update 2 until you read this Knowledge Base article about Cyclops Blink. If your Firebox is affected by Cyclops Blink, you must follow the remediation steps in the article to upgrade safely. If you do not follow the remediation steps and your Firebox is infected with Cyclops Blink or there is another issue with Firebox system integrity, your Firebox will shut down at reboot and you cannot connect to it.

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.
- To upgrade a Firebox that runs in CSfC mode from Fireware v 12.7.2 Update 1 or lower to Fireware v12.7.2 Update 2 or higher, you must disable CSfC mode before you upgrade. You can re-enable CSfC mode after the upgrade completes. For more information about CSfC mode, see Common Criteria Mode in Fireware.
- In Fireware v12.6.2 or higher, 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 or higher. For more information, see Reserved Firebox-DB authentication server user names.
- In Fireware v12.7 or higher, you cannot name new authentication servers *AuthPoint*. If you have an existing authentication server called *AuthPoint*, it will be automatically renamed to *AuthPoint.1* when you upgrade your Firebox to Fireware v12.7 or higher, or when you use WSM v12.7 or higher to manage a Firebox that runs Fireware 12.6.x or lower.

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 v12.7.2 Update 2 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 v12.7.2 Update 2 from Fireware 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 v12.7.2 Update 2 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 access point (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.

As of Fireware v12.7.2 Update 2, the AP firmware versions available to download from the Firebox are:

- AP120, AP320, AP322: 8.8.3-12 and higher
- AP125, AP225W, AP325, AP327X, AP420: 10.0.0-124 and higher

These are the minimum versions required for Fireboxes that support system integrity checks introduced in Fireware v12.7.2 Update 2 and higher.

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 a FireCluster to Fireware v12.7.2

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 v12.7.2 Operating System Compatibility Matrix

Last reviewed 5 October 2021

WSM/ Fireware Component	Microsoft Windows 8.1, 10	Microsoft Windows Server 2012 & 2012 R2	Microsoft Windows Server 2016 & 2019	macOS v10.14, v10.15, & v11.x	Android 7.x, 8.x, 9.x, 10.x, & 11.x	iOS v9, v10, v11, v12, v13, & v14
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, 8]	✓[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 v82*
- *Safari 13*
- *Safari iOS 14*
- *Safari (macOS Catalina)*

- *Safari (macOS Big Sur)*
- *Chrome v86*

[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]To learn more about client support for macOS Catalina, see macOS Catalina 10.15 software compatibility. To learn more about client support for macOS Big Sur 11.x, see macOS Big Sur 11.x software compatibility. The WatchGuard Mobile VPN with IPSec client does not currently support macOS Big Sur 11.x and does not support Mac devices that have the ARM-based Apple M1 processor.

[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.

[8]In macOS 10.15 (Catalina) or higher, you must install v12.5.2 or higher of the WatchGuard Mobile VPN with SSL client.

Authentication Support

This table provides 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 Authentication Server	AuthPoint RADIUS Server	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]	–	✓	–	✓	–

	AuthPoint Authentication Server	AuthPoint RADIUS Server	Active Directory	LDAP	RADIUS	SecurID	Firebox (Firebox-DB) Local Authentication	SAML
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, 6.7, or 7.0
- 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	Minimum Total Memory	Recommended Memory	Maximum vCPUs
Small	2048 MB[1]	4096 MB	2
Medium	4096 MB	4096 MB	4
Large	4096 MB	8192 MB	8
Extra Large	4096 MB	16384 MB	16

[1] 4096 MB is required to enable Access Portal and IntelligentAV, and to use the Full signature set for IPS/Application Control.

Firebox Cloud System Requirements

Firebox Cloud can run on Amazon Web Services (AWS) and Microsoft Azure cloud computing platforms.

Firebox Cloud CPU and memory requirements:

- Minimum CPU cores: 2
- Minimum total memory: 2048 MB[1]
- Recommended minimum total memory: 4096 MB

[1] 4096 MB is required to enable Access Portal and IntelligentAV, and to use the Full signature set for IPS/Application Control.

WatchGuard recommends an instance that has at least 1024 MB of memory for each CPU core. For example, if the instance has four CPU cores, we recommend a minimum total memory of 4096 MB. Refer to the AWS and Azure documentation to identify instances that meet these requirements.

For Firebox Cloud with a BYOL license, the Firebox Cloud model determines the maximum number of CPU cores. For more information, see Firebox Cloud License Options in Help Center.

For a BYOL license, Azure automatically selects an instance size based on the License Type you select. For more information, see the Firebox Cloud Deployment Guide.

Downgrade Instructions

After you upgrade to Fireware v12.7.2 Update 2, you cannot downgrade to a previous Fireware version. For more information, see this Knowledge Base article.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal 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 v12.6.4. UI changes introduced since v12.6.4 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 set in your web browser by default.

WatchGuard System Manager

When you install WSM, you can choose which 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 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.