Fireware v12.5.12 Update 2 Release Notes

Supported Devices	Firebox T15, T35, WatchGuard AP
Release Date	12.5.12 Update 2: 1 August 2024 12.5.12 Update 1: 26 October 2023 12.5.12: 14 September 2023
Release Notes Revision	1 August 2024
Fireware OS Build	12.5.12 Update 2: 701324 12.5.12 Update 1: 687697 12.5.12: 685754
WatchGuard System Manager Build	12.10.4: 699520
WatchGuard AP Firmware	AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36

Introduction

Fireware v12.5.12 Update 2

On 1 August 2024, WatchGuard released Fireware v12.5.12 Update 2. This release resolves a security issue. Go to *Enhancements and Resolved Issues in Fireware v12.5.12 Update 2* for more information.

Fireware v12.5.12 Update 1

On 26 October 2023, WatchGuard released Fireware v12.5.12 Update 1. This release includes a number of resolved issues. Go to *Enhancements and Resolved Issues in Fireware v12.5.12 Update 1* for more information.

Fireware 12.5.12

Fireware v12.5.12 introduces enhancements to Fireware and resolves several issues and bugs.

You must use WSM v12.10.4 to manage devices that run Fireware v12.5.12.

Features in this release include:

IPS and Application Control Engine Update

Intrusion Prevention Service and Application Control now use the same engine and signature set used by Fireware v12.6.x and higher.

In Fireware v12.5.12, the three Network Protocols categories in Application Control are consolidated into a single Network Protocol category. If you previously configured actions for applications in these categories, we recommend that you review your Application Control settings after upgrade.

New OS Compatibility Option

The OS Compatibility setting in Policy Manager now includes a 12.5.12 or higher option.

Removal of Web Reputation Authority Service from RED

In Fireware v12.5.12 and higher, Reputation Enabled Defense (RED) no longer includes support for the Web Reputation Authority service. Fireware v12.5.12 and higher continue to support other services enabled with the RED feature key (Botnet Detection, Geolocation, and Tor Exit Node Blocking). For more information, go to this Partner blog post.

Fireware v12.6.x and higher are 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 and higher are not currently available for Firebox T10, T15, T30, T35, T55, T70, M200, and M300. Fireware v12.5.12 only supports Firebox T15 and T35. For more information, go to this Knowledge Base article.

For a full list of the enhancements in this release, go to *Enhancements and Resolved Issues in Fireware v12.5.12 Update 1* or review the What's New in Fireware v12.5.12 PowerPoint.

Before You Begin

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

- A supported WatchGuard Firebox. This device can be a WatchGuard Firebox T15 or T35.
- 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, go to Release-specific upgrade notes.

Note that you can install and use WatchGuard System Manager v12.x and all WSM server components[1] with devices running earlier versions of Fireware. In this case, we recommend that you use the product documentation that matches your Fireware OS version.

If you have a new Firebox, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. We also recommend that you review the Hardware Guide for your Firebox model. The *Hardware Guide* contains useful information about your device interfaces, as well as information on resetting your device to factory default settings, if necessary.

Product documentation for all WatchGuard products is available on the WatchGuard web site at https://www.watchguard.com/wgrd-help/documentation/overview.

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

Enhancements and Resolved Issues

Enhancements and Resolved Issues in Fireware v12.5.12 Update 2

- This release resolves a buffer overflow vulnerability (CVE-2024-5974) with a maximum severity rating of High. View the full advisory details on psirt.watchguard.com. *[WGSA-2024-00011]*

Enhancements and Resolved Issues in Fireware v12.5.12 Update 1

- The Web Download page status now appears in the Show SSLVPN output when you run the `sslvpn web-download enable` CLI command. *[FBX125X-252]*
- This release removes DHE ciphers susceptible to D(HE)ater attack (CVE-2002-20001) and SHA-1 ciphers used by Fireware CLI and Web services. *[FBX125X-239, FBX125X-241]*
- To improve communication between the Firebox and WatchGuard Cloud, this release adds a keepalive check that makes sure services on the Firebox that communicate with WatchGuard Cloud, such as AuthPoint integrations, recover quickly in the event of a disruption to IoT services. *[FBX125X-246]*
- This release resolves an issue that caused the Firebox to change its WatchGuard Cloud registration status to unregistered. *[FBX125X-247]*
- The Fireware version information now correctly appears in WatchGuard Cloud after a Fireware update. *[FBX125X-249]*
- The Firebox now continues to try to register with WatchGuard Cloud after it receives an error. Errors can occur when the local date and time of the Firebox is outside of the validity of the certificate used by the connection. *[FBX125X-245]*

Enhancements and Resolved Issues in Fireware v12.5.12

General

- In Fireware Web UI, the `query_type` parameter now appears in DNS-Proxy log messages in Traffic Monitor. *[FBX125X-188]*
- USB modems can now obtain a new IP address when DHCP renews. *[FBX125X-184]*
- The OS Compatibility setting in Policy Manager now includes a 12.5.12 or higher option. *[FBX-24812]*

Security Services

- Application Control and Intrusion Prevention Service now use an updated engine and signature set. *[FBX-23406]*
- In Fireware v12.5.12 and higher, Reputation Enabled Defense (RED) no longer includes support for the Web Reputation Authority service. *[FBX125X-233]*
- This release resolves a kernel crash when Intrusion Prevention Service (IPS) or Application Control is enabled. *[FBX125X-229]*

VPN

- BOVPN tunnels now reconnect after a scheduled FireCluster reboot. *[FBX125X-213]*
- BOVPN virtual interfaces with IKEv2 now work correctly with modem failover. *[FBX125X-185]*

Known Issues and Limitations

Known issues for Fireware v12.5.12 Update 2 and its management applications, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To view 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, go to 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. The descriptions below detail which software packages you need for your upgrade.

WatchGuard System Manager

There is no WSM v12.5.12. Use WSM v12.10.4 to manage Fireboxes that run Fireware v12.5.12.

With this software package you can install WSM and the WatchGuard Server Center software:

`WSM_12_10_4.exe` — Use this file to install WSM v12.10.4 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.

If you have…	Select from these Fireware OS packages
Firebox T15	`Firebox_OS_T15_12_5_12_U2.exe` `firebox_T15_12_5_12_U2.zip`
Firebox T35	`Firebox_OS_T35_12_5_12_U2.exe` `firebox_T35_12_5_12_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.

Filename	Description	Updated in this release
WG-Authentication-Gateway_12_10.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO [4]	**Yes**
WG-Authentication-Client_12_7.msi	Single Sign-On Client software for Windows [4]	No
WG-SSOCLIENT-MAC_12_5_4.dmg	Single Sign-On Client software for macOS [4]	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_12_10.exe	Terminal Services software for both 32-bit and 64-bit systems.	**Yes**
WG-MVPN-SSL_12_7_2.exe	Mobile VPN with SSL client for Windows[5]	No
WG-MVPN-SSL_12_7_2.dmg	Mobile VPN with SSL client for macOS[5]	No
WG-Mobile-VPN_Windows_x86-64_1504_29378.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]	No
WG-Mobile-VPN_macOS_x86-64_461_29053.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 v12.10 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.10, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.10, 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 v12.10 supports previous versions of the SSO Agent.

[5] Not supported on ARM processor architecture.

Upgrade to Fireware v12.5.12 Update 2

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 v12.5.5 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 v12.5.5 or higher. For more information, go to Reserved Firebox-DB authentication server user names.
- In Fireware v12.5.12 and higher, the three Network Protocols categories in Application Control are consolidated into a single Network Protocols category. If you previously configured actions for applications in these categories, we recommend that you review your Application Control settings after upgrade.

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, go to Fireware Help.

Upgrade to Fireware v12.5.12 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, go to Upgrade Firmware from WatchGuard Cloud in *WatchGuard Cloud Help*.

Upgrade to Fireware v12.5.12 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, go to 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 v12.5.12 Update 2 from WSM/Policy Manager

To upgrade from WSM/Policy Manager, go to 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.

As of Fireware v12.5.10, the AP firmware versions available to download from the Firebox are: 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 v12.5.9 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.

Upgrade a FireCluster to Fireware v12.5.12 Update 2

You can upgrade Fireware 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, go to this Help topic.

Fireware v12.5.12 Operating System Compatibility Matrix

This operating system compatibility matrix was created for the original Fireware v12.5.12 release. It has not been updated for subsequent update releases.

WSM/ Fireware Component	Microsoft Windows 8.1, 10, 11	Microsoft Windows Server 2012 & 2012 R2	Microsoft Windows Server 2016, 2019 & 2022	macOS v10.14, v10.15, v11.x, & 12.x	Android 7, 8, 9, 10, 11, 12, 13, & 14	iOS v9, v10, v11, v12, v13, v14, & v15
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, go to 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	✓[10]			✓[4, 5, 11]	✓[5]	✓[5]
Mobile VPN with SSL	✓			✓[4, 8]	✓[6]	✓[6]
Mobile VPN with IKEv2	✓			✓[4, 9]	✓[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]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 about client support for macOS Catalina, go to macOS Catalina 10.15 software compatibility. To learn more about client support for macOS Big Sur 11.x, go to 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.

[9]In macOS 12.x (Monterey) you must manually update the authentication settings after you install the Mobile VPN with IKEv2 client profile. For more information, go to this KB article.

[10] Mobile VPN with IPSec NCP client for Windows (version 15.04 build 29378) supports Windows 10 and Windows 11 only.

[11] Mobile VPN with IPSec NCP client for macOS (version 4.61 build 29053) supports macOS Big Sur 11.x or higher only.

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

Downgrade Instructions

You cannot downgrade a T15 or T35 Firebox to a version of Fireware lower than Fireware v12.5.9 Update 2.

Downgrade from WSM v12.10.4

You must use WSM v12.10.4 to manage devices that run Fireware v12.5.12.

If you want to revert from WSM v12.10.4 to an earlier version, you must uninstall WSM v12.10.4. 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 v12.10.4.

Next, install the same version of WSM that you used before you upgraded to WSM v12.10.4. 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 v12.10.4. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.5.12 Update 2

If you want to downgrade from Fireware v12.5.12 Update 2 to an earlier version of Fireware, we recommend you use a backup image that you created before the upgrade to Fireware v12.5.12 Update 2. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.5.12 Update 2 to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device.

If you need to downgrade a Firebox without a backup file after you complete the upgrade to Fireware v12.x, we recommend you Downgrade with Web UI. This process deletes the configuration file, but does not remove the device feature keys and certificates. After you downgrade the Firebox, you can use Policy Manager to Save the Configuration File to the Firebox.

If you use the Fireware Web UI or CLI to downgrade to an earlier version, the downgrade process resets the network and security settings on your device to their factory-default settings. The downgrade process does not change the device passphrases and does not remove the feature keys and certificates.

Go to *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

Go to this Knowledge Base article for a list of downgrade restrictions.

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 v12.5.2. 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, select your language from the drop-down list.