Fireware v2026.3.2 Release Notes

Supported Devices	Firebox T175, M4850, M5850, M6850
Release Date	29 September 2026
Release Notes Revision	29 September 2026
Fireware OS Build	747802
WatchGuard System Manager Build	746533

Introduction

Fireware v2026.3.2 adds support for the new Firebox T175 model and includes important security fixes in Fireware. We strongly recommend that you upgrade your Firebox to this release to prevent exposure.

For a full list of the enhancements in this release, go to Enhancements and Resolved Issues.

Before You Begin

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

- A supported WatchGuard Firebox. This device can be a WatchGuard Firebox T175, M4850, M5850, or M6850.
- The required hardware and software components. 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.
- 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 v2026.3.2 and all WSM server components with devices running earlier versions of Fireware. In this case, we recommend that you use the product software 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.

Resolved Issues and Enhancements in Fireware v2026.3.2

Security Issues

- This release resolves a resource exhaustion vulnerability in Fireware Web UI diagnostic tasks (CVE-2026-18105). Read the full advisory on psirt.watchguard.com.
- This release resolves a `wgagent` vulnerability that allowed arbitrary file validation and caused the management daemon to stop responding (CVE-2026-90441). Read the full advisory on psirt.watchguard.com.
- This release resolves a `wgagent` vulnerability that allowed arbitrary file initialization and caused the management daemon to stop responding (CVE-2026-86136). Read the full advisory on psirt.watchguard.com.
- This release resolves a path traversal vulnerability in Fireware Web UI that allowed an authenticated user to read arbitrary local files (CVE-2026-13224). Read the full advisory on psirt.watchguard.com.
- This release resolves a denial of service vulnerability in `wgagent` caused by gzip decompression during login requests (CVE-2026-86104). Read the full advisory on psirt.watchguard.com.
- This release resolves a NULL pointer dereference vulnerability in `wgagent` that caused the management daemon to crash (CVE-2026-86134). Read the full advisory on psirt.watchguard.com.
- This release resolves an authorization bypass vulnerability that allowed an authenticated SAML user to establish an unauthorized Mobile VPN with SSL session (CVE-2026-86101). Read the full advisory on psirt.watchguard.com.
- This release resolves path authorization and directory traversal vulnerabilities in the Access Portal reverse proxy (CVE-2026-86105). Read the full advisory on psirt.watchguard.com.
- This release resolves an untrusted data deserialization vulnerability in `samld` daemon session management (CVE-2026-13046). Read the full advisory on psirt.watchguard.com.
- This release resolves a buffer overflow vulnerability in the `fingerd` daemon when it processes DHCP option 60 requests (CVE-2026-81433). Read the full advisory on psirt.watchguard.com.
- This release resolves a NULL pointer dereference vulnerability in the `ipt_NETFLOW` IPv6 Authentication Header parser that caused a kernel crash (CVE-2026-86128). Read the full advisory on psirt.watchguard.com.
- This release resolves a stack-based buffer overflow vulnerability in the `spamd` daemon (CVE-2026-18145). Read the full advisory on psirt.watchguard.com.
- This release resolves a remote code execution vulnerability in BOVPN Over TLS client configuration file processing (CVE-2026-86131). Read the full advisory on psirt.watchguard.com.
- This release resolves an integer underflow vulnerability in the `iked` daemon when it processed IKEv2 AES-GCM encrypted messages (CVE-2026-86132). Read the full advisory on psirt.watchguard.com.
- This release resolves an integer underflow vulnerability in the `iked` daemon when it processed IKEv2 non-AEAD encrypted messages (CVE-2026-86133). Read the full advisory on psirt.watchguard.com.

General

- Default IKEv2 BOVPN security settings now use AES-GCM-256 and Diffie-Hellman Group 19 (DH-19) for new tunnels. *[FBX-32430]*

Known Issues and Limitations

Known issues for Fireware v2026.3.2 and its management applications, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To go to 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

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

`WSM_2026_3_2.exe` — Use this file to install WSM v2026.3.2 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.

If you have…	Select from these Fireware OS packages
Firebox M4850/M5850/M6850	`Firebox_OS_M4850_M5850_M6850_2026_3_2.exe` `firebox_M4850_M5850_M6850_2026_3_2.zip`
Firebox T175	`Firebox_OS_T175_2026_3_2.exe` `firebox_T175_2026_3_2.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_10_2.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO[4]	No
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_10.exe	Exchange Monitor for 32-bit operating systems	No
SSOExchangeMonitor_x64_12_10.exe	Exchange Monitor for 64-bit operating systems	No
TO_AGENT_SETUP_12_11_2.exe	Terminal Services software for both 32-bit and 64-bit systems	No
WG-MVPN-SSL_2026_2_2.exe	Mobile VPN with SSL Client for Windows	No
WG-MVPN-SSL_2026_2_2.dmg	Mobile VPN with SSL Client for macOS	No
WG-Mobile-VPN_Windows_x86-64_1533_29750.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP[2]	No
WatchGuard_Mobile_VPN_x86-64_473_30031.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.

[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 v12.10.2 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.10.2, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.10.2, 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 v2025.1.x supports previous versions of the SSO Agent.

Upgrade to Fireware v2026.3.2

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.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous server or client software when you upgrade to WSM v2026.3.2. You can install the v2026.3.2 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 v2026.3.2 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 v2026.3.2 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 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 v2026.3.2 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.

Gateway Wireless Controller Access Point Firmware

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 v12.11, only AP125, AP225W, AP325, AP327X, AP420 devices that run the latest v11.0.0-36-4 AP firmware are supported by the Gateway Wireless Controller. Upgrade to the latest AP firmware before you upgrade to Fireware v12.11 or 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 4:00 AM 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.

Fireware v2026.3.2 Operating System Compatibility Matrix

Last reviewed: 29 September 2026

WSM/ Fireware Component	Microsoft Windows 10, 11	Microsoft Windows Server 2019, 2022, & 2025	macOS v10.14, v10.15, v11, v12, v13, v14, v15, & v26	Android 7, 8, 9, 10, 11, 12, 13, 14, 15, & 16	iOS v9, v10, v11, v12, v13, v14, v15, v16, v17, v18, & v26
WatchGuard System Manager	Supported	Supported	Not Supported	Not Supported	Not Supported
WatchGuard Servers *For information on WatchGuard Dimension, go to the Dimension Release Notes.*	Supported	Supported	Not Supported	Not Supported	Not Supported
Single Sign-On Agent (Includes Event Log Monitor)[11]	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Single Sign-On Client	Supported[14]	Supported[14]	Supported[2, 13]	Not Supported	Not Supported
Single Sign-On Exchange Monitor	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Terminal Services Agent[1]	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Mobile VPN with IPSec	Supported	Not Supported	Supported [2,3,8]	Supported	Supported[3]
Mobile VPN with SSL	Supported	Not Supported	Supported [2,6,9,12]	Supported[4]	Supported[4]
Mobile VPN with IKEv2	Supported	Not Supported	Supported [2,7,15]	Supported[5]	Supported[15]
Mobile VPN with L2TP	Supported	Not Supported	Supported[3]	Supported[10]	Supported

Note about Microsoft Windows support:

- *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):

- *Microsoft Edge116*
- *Firefox v117*

- *Safari 16 (macOS)*
- *Chrome v116*

[1]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.

[2]To learn more about client support for different macOS versions, go to the macOS software compatibility KB articles for macOS Catalina 10.15, macOS Big Sur 11, macOS Monterey 12, macOS Ventura 13, macOS Sonoma 14, macOS Sequoia 15, and macOS Tahoe 26.

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

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

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

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

[7]In macOS 12 (Monterey) or higher, 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.

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

[9] macOS 13 (Ventura) and higher do not accept SSL connections to untrusted self-signed certificates. For more information, go to this KB article.

[10] The built-in Android OS L2TP client is supported for all Android versions except Android 12 and higher (Android 12 removed support for L2TP VPN).

[11] The WatchGuard Single-Sign On Agent v12.10.1 supports computers that are joined to your domain with Azure Active Directory.

[12] The WatchGuard Mobile VPN with SSL Client v12.10.4 for macOS does not support macOS 10.15 (Catalina) or lower.

[13] The Single Sign-On Client does not support macOS 15 (Sequoia) or macOS 26 (Tahoe).

[14] The Single Sign-On Client does not support Windows devices with ARM processors.

[15] For IKEv2 VPNs, macOS v26 (Tahoe) and iOS v26 do not support DES, 3DES, SHA1-96, or SHA1-160 algorithms, and do not support Diffie-Hellman groups less than 14.

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.

	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	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
Mobile VPN with IPSec for Android	Not Supported	Supported	Supported	Supported	Supported	Not Supported	Supported	Not Supported
Mobile VPN with SSL	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Mobile VPN with IKEv2 for Windows	Supported	Supported	Supported [1]	Not Supported	Supported	Not Supported	Supported	Not Supported
Mobile VPN with L2TP	Not Supported	Supported	Supported [1]	Not Supported	Supported	Not Supported	Supported	Not Supported
Built-in Web Page on Port 4100 and 8080	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported [2]
Access Portal	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
AD Single Sign-On Support *(with or without client software)*	Not Supported	Not Supported	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported
Terminal Services Manual Authentication	Not Supported	Not Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
Terminal Services Authentication with Single Sign-On	Not Supported	Not Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

[1] Active Directory authentication methods are supported only through a RADIUS server.

[2] Port 8080 does not support SAML authentication.

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

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, select your language from the drop-down list.