# Fireware v12.10.4 Update 2 Release Notes

| | |
|---|---|
| Supported Devices | Firebox NV5, T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M440, M470, M570, M590, M670, M690, M4600, M4800, M5600, M5800<br>FireboxV, Firebox Cloud, WatchGuard AP |
| Release Date | 12.10.4 Update 2: 5 September 2024<br>12.10.4 Update 1: 25 July 2024<br>12.10.4: 27 June 2024 |
| Release Notes Revision | 10 September 2024 |
| Fireware OS Build | 12.10.4 Update 2: 702217<br>12.10.4 Update 1: 701004<br>12.10.4: 699733 |
| WatchGuard System Manager Build | 12.10.4: 699520 |
| WatchGuard AP Firmware | AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36 |

# Introduction

## Fireware v12.10.4 Update 2

On 5 September 2024, WatchGuard released Fireware v12.10.4 Update 2. This release includes important security fixes and resolved issues. For more information, go to Enhancements and Resolved Issues in Fireware v12.10.4 Update 2.

## Fireware v12.10.4 Update 1

On 25 July 2024, WatchGuard released Fireware v12.10.4 Update 1. This release includes important security fixes and resolved issues. For more information, go to Enhancements and Resolved Issues in Fireware v12.10.4 Update 1.

## Fireware v12.10.4

Fireware v12.10.4 is a maintenance release that introduces enhancements to Fireware and resolves numerous issues and bugs.

Features in this release include:

*Block IP Addresses with Consecutive Failed Login Attempts*

To prevent brute force attacks against the login pages of the Firebox, you can enable the Block IP Addresses with Consecutive Failed Logins feature. The Firebox temporarily blocks an IP address after a specified number of consecutive, failed authentication attempts to Firebox login pages within a specified period. This feature is disabled by default.

*WatchGuard Mobile VPN with SSL Client v12.10.4*

Fireware v12.10.4 includes updated WatchGuard Mobile VPN for SSL clients for Windows and macOS. The updated Windows client includes security improvements. The updated macOS client supports macOS Big Sur 11 and higher, and adds support for devices with Apple silicon (M series ARM) processors.

With the release of Fireware v12.9, WatchGuard announced the deprecation of the WatchGuard Log Server, Report Server, and Quarantine Server. WSM v12.10.4 still includes these server components but they are no longer supported in v12.9 and higher. We will remove them in a future WSM release.

For a full list of the enhancements in this release, go to Enhancements and Resolved Issues or review the What's New in Fireware v12.10.4 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 NV5, T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M440, M470, M570, M590, M670, M690, M4600, M4800, M5600, M5800, FireboxV, or Firebox Cloud.
- 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 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.

# Enhancements and Resolved Issues in Fireware v12.10.4 Update 2

## General

- This release adds the ability to display a full dynamic routing list with the Firebox CLI (Command Line Interface). *[FBX-26316]*
- DNSWatch log messages are no longer rate-limited and are logged with normal traffic activity. *[FBX-27149]*
- An issue is resolved that caused the authentication server AuthPoint to be duplicated as Authpoint.1 on upgrade. *[FBX-26554]*
- This release resolves an issue with the authentication process crashing or causing problems when the Blocked Failed Logins feature was enabled. *[FBX-27765]*

# Enhancements and Resolved Issues in Fireware v12.10.4 Update 1

## Security Issues

- To resolve a critical security vulnerability (CVE-2024-6387), this release updates the version of OpenSSH used by the Firebox. View the full advisory details on psirt.watchguard.com. *[WGSA-2024-00012]*

## General

- This release resolves an HTTPS-Proxy connection failure when SSL offloading and IPS are enabled. *[FBX-27187]*
- When the diagnostic log level is set to Error, T80 and T85 appliances with no LTE modem no longer generate "systemd is_lte_modem_enabled: cfgapi_getint failed, ret = 1" log messages. *[FBX-26563]*
- This release adds the Referrer-Policy response header to responses from the Firebox web server. *[FBX-25970]*

# Enhancements and Resolved Issues in Fireware v12.10.4

## Security Issues

- This release resolves two security vulnerabilities with a maximum severity rating of High. View the full advisory details on psirt.watchguard.com. *[WGSA-2024-00010, WGSA-2024-00011]*

## General

- Firebox Cloud Pay As You Go (PAYG) instances now upgrade correctly. *[FBX-22068]*
- This release adds the Permission-Policy response header when you authenticate to the Fireware Web UI login page. *[FBX-26118]*

- The `no default-packet-handling dangerous-active arp-spoof enable` CLI command now persists after you save the configuration in Policy Manager. *[FBX-26472]*
- The `no default-packet-handling dangerous-active arp-spoof enable` CLI command now persists after you save the configuration in Fireware Web UI. *[FBX-26023]*
- Memory usage no longer increases over time when you monitor the Firebox with SNMP. *[FBX-25825]*
- Syslog data in IBM LEEF format no longer omits port information. *[FBX-27259]*
- The Firebox now correctly generates event logs with message IDs 2500-0000 and 2500-0001 in IBM LEEF format. *[FBX-24671]*
- This release updates the log level for the FQDND log message "...Element cannot be added to the set..." to debug so the message appears less frequently. *[FBX-16800]*

## Authentication

- This release adds checks to prevent inadvertent changes to the built-in status and admin account permissions. *[FBX-26096]*
- You can now block the source IP address of consecutive authentication failures to the Firebox. *[FBX-9333, FBX-19172]*

## Networking

- When you configure the Multi-WAN Interface Overflow, you can now correctly set the interface overflow threshold for VLAN type external interfaces. *[FBX-27156]*
- Policy Manager now prevents erroneous configuration of DHCP server pools that overlap across two interfaces. *[FBX-27198]*

## Proxies, Policies, and Services

- WebBlocker Cloud Server connections no longer request IPV6 AAAA records. *[FBX-27205]*
- WebBlocker categorization requests that contain a space no longer cause "WebBlocker server is not available" errors. *[FBX-26545]*

## VPN

- The Mobile VPN with SSL client for macOS now supports devices with Apple silicon (M1/M2/M3 ARM) processors. *[FBX-20838]*
- This release resolves an issue that caused Mobile VPN with IKEv2 Phase 1 rekeys to reset user authentication session timeouts for connections authenticated with RADIUS. *[FBX-27193]*

## WSM

- WatchGuard System Manager is updated to use Reload4j instead of Log4j. *[FBX-22499]*
- The WatchGuard System Manager software installer now sets the correct display version in Windows. *[FBX-27412]*
- When an HTTP proxy handles traffic for a URI that contains special characters, traffic log messages now display correctly in Traffic Monitor. *[FBX-26318]*
- Policy Manager now creates backup image file names with leading zeroes in the date. *[FBX-26538]*

# Known Issues and Limitations

Known issues for Fireware v12.10.4 Update 1 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_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. 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_10_4_U2.exe`<br>`firebox_M270_M370_M470_M570_M670_12_10_4_U2.zip` |
| Firebox M290 | `Firebox_OS_M290_12_10_4_U2.exe`<br>`firebox_M290_12_10_4_U2.zip` |
| Firebox M390 | `Firebox_OS_M390_12_10_4_U2.exe`<br>`firebox_M390_12_10_4_U2.zip` |
| Firebox M440 | `Firebox_OS_M440_12_10_4_U2.exe`<br>`firebox_M440_12_10_4_U2.zip` |
| Firebox M590/M690 | `Firebox_OS_M590_M690_12_10_4_U2.exe`<br>`firebox_MM590_M690_12_10_4_U2.zip` |
| Firebox M4600/M5600 | `Firebox_OS_M4600_M5600_12_10_4_U2.exe`<br>`firebox_M4600_M5600_12_10_4_U2.zip` |
| Firebox M4800/M5800 | `Firebox_OS_M4800_M5800_12_10_4_U2.exe`<br>`firebox_M4800_M5800_12_10_4_U2.zip` |
| Firebox NV5 | `Firebox_OS_NV5_12_10_4_U2.exe`<br>`firebox_NV5_12_10_4_U2.zip` |

| If you have… | Select from these Fireware OS packages |
|---|---|
| Firebox T20/T40 | Firebox_OS_T20_T40_12_10_4_U2.exe<br>firebox_OS_T20_T40_12_10_4_U2.zip |
| Firebox T25/T45 | Firebox_OS_T25_T45_12_10_4_U2.exe<br>firebox_OS_T25_T45_12_10_4_U2.zip |
| Firebox T55 | Firebox_OS_T55_12_10_4_U2.exe<br>firebox_T55_12_10_4_U2.zip |
| Firebox T70 | Firebox_OS_T70_12_10_4_U2.exe<br>firebox_T70_12_10_4_U2.zip |
| Firebox T80 | Firebox_OS_T80_12_10_4_U2.exe<br>firebox_OS_T80_12_10_4_U2.zip |
| Firebox T85 | Firebox_OS_T85_12_10_4_U2.exe<br>firebox_OS_T85_12_10_4_U2.zip |
| FireboxV<br>All editions for VMware | FireboxV_12_10_4_U2.ova<br>Firebox_OS_FireboxV_12_10_4_U2.exe<br>firebox_FireboxV_12_10_4_U2.zip |
| FireboxV<br>All editions for Hyper-V | FireboxV_12_10_4_U2.vhd.zip<br>Firebox_OS_FireboxV_12_10_4_U2.exe<br>firebox_FireboxV_12_10_4_U2.zip |
| Firebox Cloud | Firebox_OS_FireboxCloud_12_10_4_U2.exe<br>fireboxCloud_12_10_4_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_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 |

| File name | Description | Updated in this release |
|---|---|---|
| TO_AGENT_SETUP_12_10.exe | Terminal Services software for both 32-bit and 64-bit systems | No |
| **WG-MVPN-SSL_12_10_4.exe** | **Mobile VPN with SSL client for Windows** | **Yes**(with Fireware v12.10.4) |
| **WG-MVPN-SSL_12_10_4.dmg** | **Mobile VPN with SSL client for macOS** | **Yes**(with Fireware v12.10.4) |
| WG-Mobile-VPN_Windows_x86-64_1514_29669.exe[1] | WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP[2] | No |
| WatchGuard_Mobile_VPN_x86-64_v470_30008.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 v12.10.1 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.10.1, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.10.1, 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 v12.10.1 supports previous versions of the SSO Agent.*

# Upgrade to Fireware v12.10.4 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 v12.6.2 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, go to 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, go to Fireware Help.

## Upgrade to Fireware v12.10.4 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 v12.10.4 Update 12 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 v12.10.4 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 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.

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 v12.7.2 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.

# Upgrade a FireCluster to Fireware v12.10.4 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 v12.10.4 Update 2 Operating System Compatibility Matrix

*Last reviewed: 5 September 2024*

| WSM/ Fireware Component | Microsoft Windows 10, 11 | Microsoft Windows Server 2019 & 2022 | macOS v10.14, v10.15, v11, v12, v13, & v14 | Android 7, 8, 9, 10, 11, 12, 13, & 14 | iOS v9, v10, v11, v12, v13, v14, v15, v16, & v17 |
|---|---|---|---|---|---|
| **WatchGuard System Manager** | ✓ | ✓ | | | |
| **WatchGuard Servers** *For information on WatchGuard Dimension, go to the Dimension Release Notes.* | ✓ | ✓ | | | |
| **Single Sign-On Agent (Includes Event Log Monitor)**[11] | | ✓ | | | |
| **Single Sign-On Client** | ✓ | ✓ | ✓[2] | | |
| **Single Sign-On Exchange Monitor** | | ✓ | | | |
| **Terminal Services Agent**[1] | | ✓ | | | |
| **Mobile VPN with IPSec** | ✓ | | ✓[2,3,8] | ✓ | ✓[3] |
| **Mobile VPN with SSL** | ✓ | | ✓ 2,6,9,12 | ✓[4] | ✓[4] |
| **Mobile VPN with IKEv2** | ✓ | | ✓[2,7] | ✓[5] | ✓ |
| **Mobile VPN with L2TP** | ✓ | | ✓[3] | ✓[10] | ✓ |

*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, and macOS Sonoma 14.*

*[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.*

## 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] | – | ✓ | – | ✓ | – |
| 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<br>2GHz | Intel Core or Xeon<br>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 6.5, 6.7, 7.0, or 8.0
- Hyper-V for Microsoft Windows Server 2019 or 2022, and Hyper-V Server 2019
- KVM in CentOS 8.1

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 |
|---|---|---|---|
| Micro | 2048 MB[1] | 4096 MB | 2 |
| 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, go to 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, go to the Firebox Cloud Deployment Guide.

# Downgrade Instructions

You cannot downgrade a Firebox T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M440, M470, M570, M590, M670, M690, M4600, M4800, M5600, or M5800 to a version of Fireware lower than Fireware v12.7.2 Update 2.

## Downgrade from WSM v12.10.4

If you want to downgrade from WSM v12.10.4 to a lower 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 v12.10.4 Update 2

If you want to downgrade from Fireware v12.10.4 Update 2 to a lower version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.10.4 Update 2. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.10.4 Update 2 to complete the downgrade.
- 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 Use the Web UI to Downgrade Fireware. 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.

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 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.