Fireware v12.10 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 FireboxV, Firebox Cloud, WatchGuard AP
Release Date	14 September 2023
Release Notes Revision	15 September 2023
Fireware OS Build	685791
WatchGuard System Manager Build	685333
WatchGuard AP Firmware	AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36

Introduction

Fireware v12.10 introduces several major enhancements to Fireware and resolves numerous issues and bugs. Features in this release include:

AIA Fetching

You can now enable AIA Fetching certificate validation for HTTPS-Client proxy actions from Fireware Web UI and Policy Manager. Authority Information Access (AIA) is an extension in SSL certificates that helps to fetch intermediate certificates from the certificate issuer to provide a more secure browsing experience and avoid certificate errors.

WebSocket Connections Support

WebSocket connections allow bidirectional communication between a client and server over a single TCP connection to enable faster, more efficient data transfer. You can now specify whether HTTP proxy actions allow connections that use the WebSocket protocol.

New Microsoft365 Alias

A new Microsoft365 alias includes a list of domain names and IP addresses used by Microsoft 365 (previously named Office 365). Add the alias to your policies to allow network traffic to and from Microsoft 365 products and services. WatchGuard updates the alias automatically when Microsoft adds domains and IPs, so you no longer have to manually configure exceptions.

Network Access Enforcement Updates to Minimum OS Version

Network Access Enforcement (previously Endpoint Enforcement) now supports Windows 11 and macOS Ventura 13 as minimum operating system versions.

Diffie-Hellman Group 21 Support

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Fireware now supports Diffie-Hellman Group 21 (521-bit random) for numerous VPN settings.

Removal of Web Reputation Authority service from Reputation Enabled Defense (RED)

In Fireware v12.10 and higher, Reputation Enabled Defense (RED) no longer includes support for the Web Reputation Authority service. Other services enabled with the RED feature key are still supported in v12.10 and higher (Botnet Detection, Geolocation, and Tor Exit Node Blocking). For more information, go to this Partner Blog post.

SNMP Query Support for Dynamic Routing

You can now query the dynamic routing process with SNMP to obtain routing information for RIP, OSPF, and BGP. To enable the ability to query dynamic routing with SNMP, you must add the command "agentx" to your dynamic routing configuration file (FRR).

Firebox Storage Space Shown as a Percentage

On the Backup and Restore page, Policy Manager and Fireware Web UI now show the available storage space as a percentage.

WatchGuard Mobile VPN with SSL Client v12.10

Fireware v12.10 includes updated WatchGuard Mobile VPN for SSL clients for Windows and macOS.

> With the release of Fireware v12.9, WatchGuard announced the deprecation of the WatchGuard Log Server, Report Server, and Quarantine Server. WSM v12.10 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 in Fireware v12.10* or review the [What's New in Fireware v12.10 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 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.

WatchGuard Technologies, Inc.

Enhancements and Resolved Issues in Fireware v12.10

General

- Fireware now supports Diffie-Hellman Group 21 (521-bit random). *[FBX-4404]*
- You can no longer configure the Encryption Algorithm setting for a wireless network on a Firebox. *[FBX-24484]*
- You can no longer enable or disable TLS v1.0 for the WatchGuard Management Server and Log Server from WatchGuard Server Center. *[FBX-25347]*
- The default system name of a Firebox is now WatchGuard-Firebox. *[FBX-24744]*
- The Backup and Restore page now shows the available storage space as a percentage. *[FBX-25329]*
- You can now install a FireboxV virtual machine on VMware ESXi 8.0. *[FBX-25437]*
- The **wg-support** user account is no longer a default account. *[FBX-25285]*
- This release resolves an issue where T20-W and T40-W devices did not respond to SNMP polling. *[FBX-25091]*
- In Fireware Web UI, third-party Web Server certificates now appear with an asterisk when selected. *[FBX-21506]*
- This release resolves an issue that caused the incorrect Syslog level to show when Application Control is enabled. *[FBX-23120, FBX-25411]*
- This release resolves a Fireware Web UI log in *expired* error. *[FBX-25187]*
- This release resolves an issue with the `pxyworker` process that caused a memory leak. *[FBX-25491]*
- This release resolves a feature key synchronization issue with ConnectWise. *[FBX-22727]*
- A certificate validation error no longer occurs in WatchGuard Cloud when NTP is disabled or the Firebox system time is incorrect. *[FBX-25171]*
- The Management Server no longer listens for requests on TCP port 4110. *[FBX-25600]*

Authentication

- This release resolves an issue that caused the Event Log Monitor to crash. *[FBX-24556]*
- Terminal Services Agent performance is improved. *[FBX-1871]*
- This release corrects errors in Terminal Services Agent log messages and adds troubleshooting log messages. *[FBX-6432]*
- This release resolves a Terminal Services Agent page heap verification issue. *[FBX-6533]*
- This release resolves a Terminal Services Agent memory leak. *[FBX-5973]*

FireCluster

- This release resolves an issue that caused OSPF communication to fail for active/passive FireClusters. *[FBX-22383]*

Networking

- You can now query the dynamic routing process with SNMP to obtain routing information for RIP, OSPF, and BGP. *[FBX-22242]*
- This release resolves an issue that caused invalid traceroute results from ICMP error packets. *[FBX-23642]*
- This release resolves link speed issue with the eth10/eth11 interfaces on Firebox M690 devices. *[FBX-25206]*

- This release resolves an issue where MikroTik devices could not populate Gateway and Interface information after a Firebox upgraded to Fireware v12.9.3. *[FBX-25351]*
- Policy Manager now validates the dynamic routing configuration when you save it. *[FBX-25048]*
- You can now use the point-to-point /126 IPv6 prefix in Policy Manager. *[FBX-3381]*
- You can now select an interface with the traceroute `-i` argument. *[FBX-22479]*

Proxies, Policies, and Services

- You can now enable AIA Fetching certificate validation for HTTPS-Client proxy actions. *[FBX-24333]*
- You can now specify whether HTTP proxy actions allow connections that use the WebSocket protocol. *[FBX-4486]*
- The Firebox now includes a new Microsoft365 built-in alias for FQDNs and IP addresses used by Microsoft 365. *[FBX-23735]*
- The Web Reputation Authority service provided by Reputation Enabled Defense (RED) is not supported in Fireware v12.10 and higher. Other services enabled with the RED feature key are still supported in v12.10 and higher (Botnet Detection, Geolocation, and Tor Exit Node Blocking). *[FBX-25117]*
- The IMAP proxy no longer shows unsupported compression capabilities. *[FBX-11829]*
- Policies that use wildcard FQDN policy objects now work correctly with Firebox-generated traffic. *[FBX-25478]*
- This release resolves an issue that causes proxy processes to crash when they handled HTTP/HTTPS traffic. *[FBX-25397]*
- The correct Application Control signature set now shows in Policy Manager. *[FBX-24692]*

VPN

- Network Access Enforcement (previously Endpoint Enforcement) now supports Windows 11 and macOS Ventura 13 as minimum operating system versions. *[FBX-25402]*
- The Firebox now enforces idle timeout settings for users when Dead Peer Detection is enabled in Mobile VPN with IPSec Phase 1 settings. *[FBX-25215]*
- This release resolves an issue that caused slow VPN traffic from Apple devices to Windows servers. *[FBX-24611]*
- This release resolves a memory leak in the `IKED` process related to BOVPN IKEv2 tunnels. *[FBX-20217]*
- This release resolves an issue that caused Policy Manager to re-add older default IKEv2 shared settings. *[FBX-25436]*
- This release removes some Ephemeral Diffie-Hellman and Secure Hash Algorithm 1 cipher suites from the Fireware Mobile VPN with SSL web service. *[FBX-23467]*

Wireless

- The default country for wireless radio regions now defaults to Unknown when the Firebox cannot determine the country of operation. *[FBX-24077]*
- This release resolves an issue where the 2.4 GHz radio on the Firebox T20-W showed an SSID but wireless users could not connect. *[FBX-25078]*

WSM

- Global default gateway settings no longer appear on Firebox T25 and Firebox T45 models with only wireless external interfaces configured. *[FBX-25189]*

- This release resolves an issue that caused duplicate users and groups in WSM and Fireware Web UI. *[FBX-23953]*
- You can no longer change the policy order when you filter policies by policy tag. *[FBX-25259]*
- This release resolves an issue where, when you import a custom policy template to replace an existing policy in WSM, Policy Manager removed the policy. *[FBX-24889]*
- The default action for an HTTPS proxy no longer changes to Deny when you import and export domain rules. *[FBX-24721]*
- Policy Manager now shows a warning when you try to create a password with a leading or trailing space. *[FBX-24358]*
- This release resolves a migration issue with older wireless devices. *[FBX-25362]*

Known Issues and Limitations

Known issues for Fireware v12.10 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.exe — Use this file to install WSM v12.10 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.exe firebox_M270_M370_M470_M570_M670_12_10.zip
Firebox M290	Firebox_OS_M290_12_10.exe firebox_M290_12_10.zip
Firebox M390	Firebox_OS_M390_12_10.exe firebox_M390_12_10.zip
Firebox M440	Firebox_OS_M440_12_10.exe firebox_M440_12_10.zip
Firebox M590/M690	Firebox_OS_M590_M690_12_10.exe firebox_MM590_M690_12_10.zip
Firebox M4600/M5600	Firebox_OS_M4600_M5600_12_10.exe firebox_M4600_M5600_12_10.zip
Firebox M4800/M5800	Firebox_OS_M4800_M5800_12_10.exe firebox_M4800_M5800_12_10.zip
Firebox NV5	Firebox_OS_NV5_12_10.exe firebox_NV5_12_10.zip

If you have…	Select from these Fireware OS packages
Firebox T20/T40	`Firebox_OS_T20_T40_12_10.exe` `firebox_OS_T20_T40_12_10.zip`
Firebox T25/T45	`Firebox_OS_T25_T45_12_10.exe` `firebox_OS_T25_T45_12_10.zip`
Firebox T55	`Firebox_OS_T55_12_10.exe` `firebox_T55_12_10.zip`
Firebox T70	`Firebox_OS_T70_12_10.exe` `firebox_T70_12_10.zip`
Firebox T80	`Firebox_OS_T80_12_10.exe` `firebox_OS_T80_12_10.zip`
Firebox T85	`Firebox_OS_T85_12_10.exe` `firebox_OS_T85_12_10.zip`

FireboxV
All editions for VMware
	`FireboxV_12_10.ova`
	`Firebox_OS_FireboxV_12_10.exe`
	`firebox_FireboxV_12_10.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_10.vhd.zip`
	`Firebox_OS_FireboxV_12_10.exe`
	`firebox_FireboxV_12_10.zip`

Firebox Cloud	`Firebox_OS_FireboxCloud_12_10.exe` `fireboxCloud_12_10.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.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_10.exe	Exchange Monitor for 32-bit operating systems	**Yes**
SSOExchangeMonitor_ x64_12_10.exe	Exchange Monitor for 64-bit operating systems	**Yes**
TO_AGENT_SETUP_12_ 10.exe	Terminal Services software for both 32-bit and 64-bit systems	**Yes**
WG-MVPN-SSL_12_ 10.exe	Mobile VPN with SSL client for Windows[5]	**Yes**
WG-MVPN-SSL_12_ 10.dmg	Mobile VPN with SSL client for macOS[5]	**Yes**
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 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 v12.10

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 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 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 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

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, go to this Help topic.

Fireware v12.10 Operating System Compatibility Matrix

Last reviewed: 07 September 2023

WSM/ Fireware Component	Microsoft Windows 10, 11	Microsoft Windows Server 2019 & 2022	macOS v10.14, v10.15, v11, v12, & v13	Android 7, 8, 9, 10, 11, 12, & 13	iOS v9, v10, v11, v12, v13, v14, v15, & v16
WatchGuard System Manager	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, go to the Dimension Release Notes.*	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)		✓			
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	✓		✓ [2,6,9,11]	✓[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, and macOS Ventura 13.*

[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) does 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] *Mobile VPN with SSL client does not support Macs that have the Apple M1 or M2 ARM-based processor.*

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 6.5, 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
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

If you want to downgrade from WSM v12.10 to a lower version, you must uninstall WSM v12.10. 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.

Next, install the same version of WSM that you used before you upgraded to WSM v12.10. 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. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.10

If you want to downgrade from Fireware v12.10 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. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.10 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.