



Fireware v12.8 Update 1 Release Notes

| | |
|---------------------------------|---|
| Supported Devices | Firebox T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, M570, M590, M670, M690, M4600, M4800, M5600, M5800 FireboxV, Firebox Cloud, WatchGuard AP |
| Release Date | 12.8 Update 1: 14 April 2022 12.8: 17 March 2022 |
| Release Notes Revision | 15 April 2022 |
| Fireware OS Build | 12.8 Update 1: 659436 12.8: 657104 |
| WatchGuard System Manager Build | 12.8: 656510 |
| WatchGuard AP Firmware | AP120, AP320, AP322: 8.8.3-12 AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36 |

Introduction



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

Fireware 12.8 Update 1

On 14 April 2022, WatchGuard released Fireware v12.8 Update 1. This release includes a number of resolved issues and security fixes. See *Enhancements and Resolved Issues in Fireware v12.8 Update 1* for more information.

Fireware 12.8

Fireware v12.8 is a major release for Firebox T20, T40, T55, T70, T80, Firebox M Series (except M200 and M300), FireboxV, and Firebox Cloud appliances.

This release provides updates to networking features such as SD-WAN and Bridge mode, and includes other important enhancements and fixes. Features in this release include:

SD-WAN Load Sharing

SD-WAN actions now support a new Round Robin method, which enables you to share traffic load across multiple SD-WAN interfaces. You can use this feature to distribute load across multiple ISPs or lines.

SD-WAN Actions in Device Configuration Templates

Management Server device configuration templates now support SD-WAN actions. This makes it easy to apply SD-WAN actions to multiple devices.

MOBIKE Support

The Firebox now supports MOBIKE (RFC4555) for mobile IKEv2 connections. This enables the Firebox to use the original VPN tunnel when a mobile device moves from one network to another.

IPv6 in Bridge Mode

Bridge mode now supports IPv6.

External VLANs

For increased network design flexibility, you can now configure an external VLAN to have more than one physical interface member. External VLAN members that are physical interfaces can now be untagged. An interface can now simultaneously belong to both an External and Internal VLAN.

Intra-Interface Inspection

In Fireware CLI, you can now specify a command to apply firewall policies to intra-interface traffic on physical and link aggregation interfaces.

Geolocation

You can now disable the Geolocation Deny page for incoming HTTP/HTTPS traffic. Disable the Geolocation deny page if you do not want inbound traffic to receive a deny page that attackers could use to confirm the presence of a Firebox in your network.

Disable GARP

You can now use the CLI to enable or disable Gratuitous ARP for each interface.

NCP Client Software Updates

New NCP client software supports Windows 11 and macOS Monterrey 12.x.

Deprecation of Log Server, Report Server, and Quarantine Server Components

With this release, WatchGuard announces the deprecation of the WatchGuard Log Server, Report Server, and Quarantine Server. WSM v12.8.x releases still include these server components, but higher WSM releases will include only the WSM Client and Management Server. More information will be posted in [Product and Support News](#).

Supported Operating Systems for WSM Components

With this release, WatchGuard announces that the supported operating systems for WSM and Management Server software will follow Microsoft's Mainstream Support end dates for Windows and Windows Server. For future feature releases, when Microsoft ends Mainstream Support for these operating systems, WSM and Management Server will no longer support them. More information will be posted in [Product and Support News](#).

For a full list of the enhancements in this release, see *Enhancements and Resolved Issues in Fireware v12.8* or review the [What's New in Fireware v12.8 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 T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, 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, see [Release-specific upgrade notes](#).

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

If you have a new Firebox, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. If this is a new FireboxV installation, make sure you carefully review [Fireware Help in the WatchGuard Help Center](#) for important installation and setup instructions. We also recommend that you review the [Hardware Guide](#) for your Firebox model. The *Hardware Guide* contains useful information about your device interfaces, as well as information on resetting your device to factory default settings, if necessary.

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

Enhancements and Resolved Issues in Fireware v12.8 Update 1

- To address CVE-2022-0778, this release updates the version of OpenSSL used by the Firebox to the latest version of v1.1.1 (1.1.1n). *[FBX-23107]*
- VLAN traffic no longer drops when you update the VLAN network on the same interface. *[FBX-22787]*
- This release resolves an AuthPoint authentication resource issue for FireCluster deployments. *[FBX-22985]*
- This release resolves an SSH key issue for Firebox Cloud devices that upgrade to v12.8. *[FBX-23029]*
- Performance is improved when Fireware Web UI loads Firewall policies in the configuration. *[FBX-21092]*
- This release resolves an issue with the assignment of DNS Servers to Mobile VPN with IKEv2 clients. *[FBX-23036]*
- FireboxV devices no longer randomly fail to authenticate management users. *[FBX-22826]*
- This release resolves a Mobile VPN with IKEv2 Dead Peer Detection (DPD) stability issue. *[FBX-23104]*

Enhancements and Resolved Issues in Fireware v12.8

General

- Fireware Web UI now includes logging and notification settings for different Default Packet Handling dangerous activities. *[FBX-21826]*
- You can no longer enable FIPS mode. *[FBX-22628]*
- This release removes expired certificates from the trusted CA certificates list. *[FBX-21783]*

Authentication

- TDR Host Sensor enforcement now works correctly when AuthPoint is used as an authentication server. *[FBX-21902]*
- The Firebox now correctly resolves LDAP/RADIUS FQDNs received from AuthPoint. *[FBX-22011]*

Policies, Proxies, and Subscription Services

- If you have a Firebox management policy that allows unrestricted Internet access to your Firebox, you now see a warning message in Policy Manager and Web UI. *[FBX-22562]*
- You can now enable or disable the Geolocation deny page for an inbound HTTP or HTTPS policy. *[FBX-21864]*
- This release resolves an issue that caused SAML logins to the Access Portal to fail. *[FBX-22206]*
- APT Blocker now always submits unrecognized PDF files to the data center for analysis. *[FBX-16919]*

Networking

- Bridge mode now supports IPv6. *[FBX-20979]*
- External VLAN configurations now have fewer restrictions. *[FBX-22233]*
- SD-WAN actions now support a new Round Robin method. *[FBX-21620]*
- Management Server device configuration templates now support SD-WAN actions. *[FBX-14867]*
- The new **intra-if-inspection** CLI command enables you to apply firewall policies to intra-interface traffic. *[FBX-17332]*

- You can use the new CLI **garp** command to enable or disable Gratuitous ARP (GARP) for interfaces. *[FBX-21856]*
- 802.1p marking now works correctly on external interfaces that use VLAN with PPPoE. *[FBX-22336]*
- You can now correctly set the link speed to 10Gbps on a link aggregation interface. *[FBX-21657]*
- This release resolves an issue that caused Fireware Web UI to become unresponsive when you managed FireCluster. *[FBX-16790]*
- You can now select which interface you want to use as the external interface on a Firebox in the Quick Setup Wizard. *[FBX125X-73]*
- You can now set a VLAN ID when you configure the external interface on a Firebox in the Quick Setup Wizard. *[FBX-22060]*

VPN

- The Firebox now supports MOBIKE (RFC4555) for mobile IKEv2 connections. *[FBX-21143]*
- WatchGuard IPSec Mobile VPN Client for Windows v14.20 supports Windows 11. *[FBX-22307]*
- WatchGuard IPSec Mobile VPN Client for macOS v4.60 supports macOS Big Sur 11.x, macOS Monterey 12.x, and Mac devices with the ARM-based Apple M1 processor. *[FBX-22281]*
- You can use the new CLI **mobile_ikev2_dfbit** command to clear, copy, or set the DF-bit for all Mobile VPN with IKEv2 traffic. *[FBX-22085]*

Resolved Issues in AP Firmware v11.0.0-36

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

Known Issues and Limitations

Known issues for Fireware v12.8 Update 1 and its management applications, including workarounds where available, can be found on the [Technical Search > Knowledge Base](#) tab. To see known issues for a specific release, from the **Product & Version** filters you can expand the Fireware version list and select the check box for that version.

Some Known Issues are especially important to be aware of before you upgrade, either to or from specific versions of Fireware. To learn more, see [Release-specific upgrade notes](#).

Download Software

You can download software from the [WatchGuard Software Downloads Center](#).

There are several software files available for download with this release. See the descriptions below so you know what software packages you will need for your upgrade.

WatchGuard System Manager

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

WSM_12_8.exe — Use this file to install WSM v12.8 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_8_U1.exe firebox_M270_M370_M470_M570_M670_12_8_U1.zip |
| Firebox M290 | Firebox_OS_M290_12_8_U1.exe firebox_M290_12_8_U1.zip |
| Firebox M390 | Firebox_OS_M390_12_8_U1.exe firebox_M390_12_8_U1.zip |
| Firebox M400/M500 | Firebox_OS_M400_M500_12_8_U1.exe firebox_M400_M500_12_8_U1.zip |
| Firebox M440 | Firebox_OS_M440_12_8_U1.exe firebox_M440_12_8_U1.zip |
| Firebox M590/M690 | Firebox_OS_M590_M690_12_8_U1.exe firebox_MM590_M690_12_8_U1.zip |
| Firebox M4600/M5600 | Firebox_OS_M4600_M5600_12_8_U1.exe firebox_M4600_M5600_12_8_U1.zip |
| Firebox M4800/M5800 | Firebox_OS_M4800_M5800_12_8_U1.exe firebox_M4800_M5800_12_8_U1.zip |

| If you have... | Select from these Fireware OS packages |
|--------------------------------------|---|
| Firebox T20/T40 | Firebox_OS_T20_T40_12_8_U1.exe Firebox_OS_T20_T40_12_8_U1.zip |
| Firebox T55 | Firebox_OS_T55_12_8_U1.exe firebox_T55_12_8_U1.zip |
| Firebox T70 | Firebox_OS_T70_12_8_U1.exe firebox_T70_12_8_U1.zip |
| Firebox T80 | Firebox_OS_T80_12_8_U1.exe Firebox_OS_T80_12_8_U1.zip |
| FireboxV All editions for VMware | FireboxV_12_8_U1.ova Firebox_OS_FireboxV_12_8_U1.exe firebox_FireboxV_12_8_U1.zip |
| FireboxV All editions for Hyper-V | FireboxV_12_8_U1.vhd.zip Firebox_OS_FireboxV_12_8_U1.exe Firebox_FireboxV_12_8_U1.zip |
| Firebox Cloud | FireboxCloud_12_8_U1.zip Firebox_OS_FireboxCloud_12_8_U1.exe |

Additional Firebox Software

The files in the list below are not directly used by the Firebox or for Firebox management, but are necessary for key features to work. In most cases, the file name includes the Fireware version that was current at the time of release.

| File name | Description | Updated in this release |
|--------------------------------------|--|-------------------------|
| WG-Authentication-Gateway_12_7_2.exe | Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO | No |
| WG-Authentication-Client_12_7.msi | Single Sign-On Client software for Windows | No |
| WG-SSOCLIENT-MAC_12_5_4.dmg | Single Sign-On Client software for macOS | No |
| SSOExchangeMonitor_x86_12_0.exe | Exchange Monitor for 32-bit operating systems | No |
| SSOExchangeMonitor_x64_12_0.exe | Exchange Monitor for 64-bit operating systems | No |
| TO_AGENT_SETUP_11_12.exe | Terminal Services software for both 32-bit and 64-bit systems. | No |
| WG-MVPN-SSL_12_7_2.exe | Mobile VPN with SSL client for Windows ⁵ | No |

| File name | Description | Updated in this release |
|--|--|-------------------------|
| WG-MVPN-SSL_12_7_2.dmg | Mobile VPN with SSL client for macOS ⁵ | No |
| WG-Mobile-VPN_Windows_x86_1420_48591.exe ¹ | WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP ² | Yes (12.8) |
| WG-Mobile-VPN_Windows_x86-64_1420_48591.exe ¹ | WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP ² | Yes (12.8) |
| WG-Mobile-VPN_macOS_x86-64_460_29048.dmg ¹ | WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP ² | Yes (12.8) |
| Watchguard_MVLS_Win_x86-64_200_rev19725.exe ¹ | WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP ³ | No |

¹ The version number in this file name does not match any Fireware version number.

² There is a license required for this premium client, with a 30-day free trial available with download.

³ Click [here](#) for more information about MVLS. If you have a VPN bundle ID for macOS, it must be updated on the license server to support the macOS 3.00 or higher client. To update your bundle ID, contact WatchGuard Customer Support. Make sure to have your existing bundle ID available to expedite the update.

⁴ SSO Agent v12.7 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.7, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.7, we recommend that you upgrade all SSO Clients to v12.7. You cannot use SSO Client v12.7 with versions of the SSO Agent lower than v12.5.4. Fireware v12.7.2 supports previous versions of the SSO Agent.

⁵ Not supported on ARM processor architecture.

Upgrade to Fireware v12.8 Update 1

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, see [Reserved Firebox-DB authentication server user names](#).
- In Fireware v12.7 or higher, you cannot name new authentication servers *AuthPoint*. If you have an existing authentication server called *AuthPoint*, it will be automatically renamed to *AuthPoint.1* when you upgrade your Firebox to Fireware v12.7 or higher, or when you use WSM v12.7 or higher to manage a Firebox that runs Fireware 12.6.x or lower.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous server or client software when you upgrade to WSM v12.x. You can install the v12.x server and client software on top of your existing installation to upgrade your WatchGuard software components. We do, however, strongly recommend that you back up your WatchGuard Servers (for example, your WatchGuard Management Server) to a safe location before you upgrade. You will need these backup files if you ever want to downgrade.

For instructions on how to back up your Management Server configuration, see [Fireware Help](#).

Upgrade to Fireware v12.8 Update 1 from WatchGuard Cloud

From WatchGuard Cloud, you can upgrade the firmware for a Firebox that runs Fireware v12.5.2 or higher. To upgrade from WatchGuard Cloud, see [Upgrade Firmware from WatchGuard Cloud](#) in *WatchGuard Cloud Help*.

Upgrade to Fireware v12.8 Update 1 from Fireware Web UI

You can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. To upgrade manually, see [Upgrade Fireware OS or WatchGuard System Manager](#) in *Fireware Help*.

If your Firebox runs Fireware v11.9.x or lower, follow the steps in [this knowledge base article](#).

If you have installed another release of this OS version on your computer, you must run the installer twice (once to remove the previous release and again to install this release).

Upgrade to Fireware v12.8 Update 1 from WSM/Policy Manager

To upgrade from WSM/Policy Manager, see [Upgrade Fireware OS or WatchGuard System Manager](#) in *Fireware Help*.

If you have installed another release of this OS version on your computer, you must run the installer twice (once to remove the previous release and again to install this release).



If you like to make updates to your Firebox configuration from a saved configuration file, make sure you open the configuration from the Firebox and save it to a new file after you upgrade. This is to make sure that you do not overwrite any configuration changes that were made as part of the upgrade.

Update Access Points

All access point (AP) firmware is managed by the Gateway Wireless Controller on your Firebox. The Gateway Wireless Controller automatically checks for new AP firmware updates and enables you to download the firmware directly from WatchGuard servers.

The AP firmware versions available to download from the Firebox are:

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

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

AP Firmware Upgrade

To manage AP firmware and download the latest AP firmware to your Firebox:

- From Fireware Web UI, select **Dashboard > Gateway Wireless Controller**. From the **Summary** tab, click **Manage Firmware**.
- From Firebox System Manager, select the **Gateway Wireless Controller** tab, then click **Manage Firmware**.

If you have enabled automatic AP firmware updates in Gateway Wireless Controller, your APs are automatically updated between midnight and 4:00am local time.

To manually update firmware on your APs:

1. On the **Access Points** tab, select one or more APs.
2. From the **Actions** drop-down list, click **Upgrade**.
3. Click **Yes** to confirm that you want to upgrade the AP.

About AP Firmware and Fireware Versions

You must upgrade your APs to firmware version 8.6.0 or higher before you upgrade to Fireware v12.5.4 or higher to remain compatible with the latest versions of Fireware.

Important Steps for Upgrades from Fireware v12.0 or Lower

If you have not previously upgraded to Fireware v12.0.1 or higher and the latest AP firmware, you must perform these steps:

1. Make sure all your APs are online. You can check AP status from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.
2. Make sure you are not using insecure default AP passphrases such as **wgwap** or **watchguard**. Your current AP passphrase must be secure and at least 8 characters in length. You can change your AP passphrase in **Network > Gateway Wireless Controller > Settings**.



If you do not have a secure passphrase correctly configured before the upgrade, you will lose the management connection with your deployed APs. If this occurs, you must physically reset the APs to factory default settings before you can manage the APs from Gateway Wireless Controller.

Depending on the version of Fireware you upgrade from, you may need to mark APs as trusted after the upgrade to Fireware v12.0.1 or higher. You can mark APs as trusted from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.

Upgrade a FireCluster to Fireware v12.8 Update 1

You can upgrade Fireware OS for a FireCluster from Policy Manager or Fireware Web UI. To upgrade a FireCluster from Fireware v11.10.x or lower, we recommend you use Policy Manager.

As part of the upgrade process, each cluster member reboots and rejoins the cluster. Because the cluster cannot do load balancing while a cluster member reboot is in progress, we recommend you upgrade an active/active cluster at a time when the network traffic is lightest.

For information on how to upgrade your FireCluster, see [this Help topic](#).

Fireware v12.8 Update 1 Operating System Compatibility Matrix

Last reviewed 18 March 2022

| WSM/ Fireware Component | Microsoft Windows 8.1, 10, 11 | Microsoft Windows Server 2012 & 2012R2 | Microsoft Windows Server 2016, 2019 & 2022 | macOS v10.14, v10.15, v11.x, & v12.x | Android 7.x, 8.x, 9.x, 10.x, 11.x, & 12.x | iOS v9, v10, v11, v12, v13, v14, & v15 |
|---|-------------------------------------|---|--|--|---|--|
| WatchGuard System Manager | ✓ | ✓ | ✓ | | | |
| WatchGuard Servers <i>For information on WatchGuard Dimension, see the Dimension Release Notes.</i> | ✓ | ✓ | ✓ | | | |
| Single Sign-On Agent (Includes Event Log Monitor)¹ | | ✓ | ✓ | | | |
| Single Sign-On Client | ✓ | ✓ | ✓ | ✓ ⁴ | | |
| Single Sign-On Exchange Monitor² | | ✓ | ✓ | | | |
| Terminal Services Agent³ | | ✓ | ✓ | | | |
| Mobile VPN with IPSec | ✓ | | | ✓ ^{4,5} | ✓ 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

¹The Server Core installation option is supported for Windows Server 2016.

²Microsoft 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.

³Terminal 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.

⁴To learn more about client support for macOS Catalina, see [macOS Catalina 10.15 software compatibility](#). To learn more about client support for macOS Big Sur 11.x, see [macOS Big Sur 11.x software compatibility](#). To learn more about client support for macOS Monterey 12.x, see [macOS Monterey 12.x software compatibility](#).

⁵Native (Cisco) IPsec client is supported for all recent versions of macOS and iOS.

⁶OpenVPN is supported for all recent versions of Android and iOS.

⁷StrongSwan is supported for all recent versions of Android.

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

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

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 (<i>with or without client software</i>) | — | — | ✓ | ✓ | — | — | — | — |
| Terminal Services Manual Authentication | — | — | ✓ | ✓ | ✓ | ✓ | ✓ | — |
| Terminal Services Authentication with Single Sign-On | — | — | ✓ | — | — | — | — | — |

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

System Requirements

| | If you have WatchGuard System Manager client software only installed | If you install WatchGuard System Manager and WatchGuard Server software |
|---------------------------------------|--|---|
| Minimum CPU | Intel Core or Xeon 2GHz | Intel Core or Xeon 2GHz |
| Minimum Memory | 1 GB | 2 GB |
| Minimum Available Disk Space | 250 MB | 1 GB |
| Minimum Recommended Screen Resolution | 1024x768 | 1024x768 |

FireboxV System Requirements

A WatchGuard FireboxV virtual machine can run on:

- VMware ESXi 6.0, 6.5, 6.7, or 7.0
- Windows Server or Hyper-V Server 2012 R2, 2016, 2019, or 2022
- 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 MB¹
- Recommended minimum total memory: 4096 MB

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

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



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

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

Downgrade Instructions

You cannot downgrade a Firebox to a version of Fireware lower than Fireware v12.7.2 Upgrade 2.

Downgrade from WSM v12.8

If you want to revert from WSM v12.8 to a lower version, you must uninstall WSM v12.8. 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 v12.8.

Next, install the same version of WSM that you used before you upgraded to WSM v12.8. 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 v12.8. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.8 Update 1

If you want to downgrade from Fireware v12.8 to a lower version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.8. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.8 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 [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.

See [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

See 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, click the Globe icon and select your language from the drop-down list.