Fireware v12.11 Release Notes

Supported Devices	Firebox NV5, T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M470, M570, M590, M670, M690, M4600, M4800, M5600, M5800 FireboxV, Firebox Cloud, WatchGuard AP
Release Date	7 November 2024
Release Notes Revision	7 November 2024
Fireware OS Build	706602
WatchGuard System Manager Build	705338
WatchGuard AP Firmware	AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36-4

Introduction

Fireware v12.11

Fireware v12.11 introduces several major enhancements to Fireware and resolves numerous issues and bugs.

Features in this release include:

Firebox Authentication with SAML

With this feature, you can integrate a Firebox with a SAML IdP, such as Microsoft Entra ID (formerly Azure AD), and use single sign-on (SSO) and SAML for Firebox user authentication.

You can configure SSO and SAML to authenticate with Access Portal, the Firebox Authentication Portal, and Mobile VPN with SSL.

FIPS 140-3 Support

The Firebox is designed to meet the overall requirements for FIPS 140-3 Level 2 security when configured in a FIPS-compliant manner with Fireware v12.11 (Product Certification status).

These hardware models support FIPS 140-3:

- WatchGuard Firebox T Series: T20, T20-W, T40, T40-W, T80, NV5, T25, T25-W, T45, T45-PoE, T45-W-PoE, T45-CW, T85-PoE
- WatchGuard Firebox M Series: M290, M390, M590, M690, M4800, M5800

For more information, go to FIPS Support in Fireware.

WatchGuard AP Compatibility with Gateway Wireless Controller in Fireware v12.11

As of Fireware v12.11 and higher, only AP125, AP225W, AP325, AP327X, AP420 devices that run the latest v11.0.0-36-4 firmware are supported by the Gateway Wireless Controller on a Firebox. Make sure you upgrade your access points to the latest firmware version before you upgrade to Fireware v12.11.

AP100, AP102, AP120, AP200, AP300, AP320, and AP322 devices are no longer supported and cannot be managed with the Gateway Wireless Controller on a Firebox. Devices will still operate with their last known configuration, but they can no longer be updated from the Gateway Wireless Controller.

TLS Minimum Protocol Version

In Fireware v12.11 and higher, in TLS profile configurations, the minimum supported TLS protocol version is TLS v1.2.

Threat Telemetry Collection

This release adds an option to send threat telemetry information to WatchGuard. This feature is enabled by default.

Block Failed Logins Enabled by Default

In Fireware v12.11 and higher, the Block Failed Logins feature is enabled in new configurations by default in Fireware Web UI, Policy Manager, and WatchGuard Cloud.

Internet Watch Foundation WebBlocker Category

The Internet Watch Foundation (IWF) WebBlocker category is now included in the list of recommended categories to block in setup wizards and the default WebBlocker action.

With the release of Fireware v12.9, WatchGuard announced the deprecation of the WatchGuard Log Server, Report Server, and Quarantine Server. WSM v12.11 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 v12.11 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, 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 v12.11

General

- The Firebox is designed to meet the overall requirements for FIPS 140-3 Level 2 security when configured in a FIPS-compliant manner with Fireware v12.11. *[FBX-22173]*
- As of Fireware v12.11, only AP125, AP225W, AP325, AP327X, AP420 devices that run the latest v11.0.0-36-4 firmware are supported by the Gateway Wireless Controller on a Firebox. *[FBX-27755]*
- The Send Log Messages to Syslog Server option for legacy access points is deprecated and removed. *[FBX-28121]*
- In addition to advanced device feedback, you can now send threat telemetry information to WatchGuard. *[FBX-27307]*
- In Fireware Web UI, the Firebox Configuration Report now includes the device serial number and Fireware version. *[FBX-27231]*
- This release removes the obsolete pop-up notification option from logging and notification preferences in Fireware Web UI and Policy Manager. *[FBX-9113]*
- The Firebox internal web server now includes Referrer-Policy response headers. *[FBX-25970]*
- Access Portal SSH resources now work with SSH servers that run OpenSSH 8.6 and higher. *[FBX-23321]*
- When you use Access Portal SSH resources with SSH servers based on OpenSSH 7.6 and higher with older SSH-1 algorithms, you must use DSA keys. RSA is not supported. *[FBX-27508]*
- This release resolves an issue that caused high CPU usage when a USB drive was plugged in. *[FBX-24321]*
- The FQDN process no longer sends Assertion Failed debug logs during a cache refresh. *[FBX-25939]*
- The reload time for the static Blocked Sites list is reduced. *[FBX-27315]*
- When there are multiple routes and VLAN interfaces, FireCluster health checks now complete faster after a failover. *[FBX-27271]*
- The backup master cluster member now correctly rejoins a T Series FireCluster after a reboot. *[FBX-27841]*
- A certificate sync between FireCluster members no longer causes a *Resource conflict* error when you perform certificate actions. *[FBX-27950]*
- The Firebox no longer attempts to download the LiveSecurity RSS feed. *[FBX-26459]*
- The Wireless Statistics page now loads correctly on Wi-Fi capable Fireboxes. *[FBX-26535]*
- User permissions now apply correctly applied to devices in nested folders on a Management Server. *[FBX-25838]*
- To prevent Add Device Wizard failures, CRLF characters are removed from user inputs in WatchGuard Management Server. *[FBX-10541]*
- The Reboot role property no longer enables a user to save a configuration to the WSM Management Server. *[FBX-26493]*
- The Web Setup Wizard now recommends Firebox management by WatchGuard Cloud. *[FBX-27459]*
- Fireware Web UI now includes a Device Information page that shows the system information for a cloud-managed Firebox. *[FBX-20973]*

Authentication

- This release supports a new SAML authentication server type. *[FBX-26372]*
- The Block Failed Logins feature is enabled in new configurations by default in Fireware Web UI, Policy Manager, and WatchGuard Cloud. *[FBX-27549]*

- The Block Failed Logins feature now blocks failed AuthPoint authentications. *[FBX-27443]*
- You can now configure the Block Failed Logins feature in WSM Management Server templates. *[FBX-27636]*

Networking

- Fireware Web UI now prevents erroneous configuration of DHCP server pools that overlap across two interfaces. *[FBX-25835]*
- When you enter a network for a Virtual IP address pool, Policy Manager now warns you if that network is already in use. *[FBX-13770]*
- You can now configure multiple DHCP pools in drop-in mode. *[FBX-25931]*
- When you add a static route, the Destination Type now defaults to Network IPv4. *[FBX-3826]*
- You can now use the CLI to view dynamic routing entries older than two weeks. *[FBX-26316]*
- On T80/T85 appliances, this release disables logging related to the LTE modem when the module is not installed. *[FBX-26563]*
- This release resolves an issue that overwrote VIF IPv4/IPv6 routes when you saved the configuration from both Fireware Web UI and Policy Manager. *[FBX-18879]*
- This release improves Static NAT with Server Load Balancing actions to handle cases where all connections come from the same IP address. *[FBX-15080]*
- The timeout to validate dynamic routing configurations is increased. *[FBX-26499]*
- Wildcard aliases in the dynamic NAT table are now correctly applied. *[FBX-26466]*
- When you clear the Enable Sticky Connection check box, SNAT action sticky connections do not occur for 8 hours. *[FBX-15080*]

Proxies, Policies, and Services

- In the TLS profile configuration, the minimum supported TLS protocol version is now TLS v1.2. *[FBX-28101]*
- The Internet Watch Foundation (IWF) WebBlocker category is now included in the list of recommended categories to block in setup wizards and the default WebBlocker action. *[FBX-26548]*
- The WebBlocker global exceptions list now includes WatchGuard Endpoint Security URLs. *[FBX-26361]*
- The Configuration Report now includes Geolocation exceptions. *[FBX-26353]*
- This release resolves an issue that caused Geolocation to allow blocked traffic for a few seconds after a database update. *[FBX-23001]*
- Geolocation now works correctly after Firebox Cloud reboots. *[FBX-27762]*
- In Policy Manager, FQDN values now sort correctly in the policy list To and From fields. *[FBX-27592]*
- In Fireware Web UI, WebBlocker now correctly saves exceptions enabled from the Quick Action menu. *[FBX-27366]*
- This release resolves an issue where a `certd` crash deleted the trusted CA for proxies. *[FBX-25236]*
- DNSWatch no longer generates logs for unhandled internal packets. *[FBX-27150]*
- DNSWatch logs are no longer rate limited. *[FBX-27149]*

VPN

- The Download Client button in the SSL section of the Configure Mobile VPN page is replaced by a link to the Software Downloads Center. *[FBX-27865]*
- This release removes the Mobile VPN with SSL Client download page from the Firebox. *[FBX-27548]*
- The VPN Diagnostic Report now correctly shows the policy used when BOVPN-Allow policies are active. *[FBX-17742]*

- This release resolves an issue that created duplicate Mobile VPN with SSL users or groups in Policy Manager. *[FBX-27946]*

WSM

- WSM Help links now open in the default system browser instead of Internet Explorer. *[FBX-24526]*
- When you upgrade WSM to v12.11, the Log4j library is removed from your management computer. *[FBX-27979]*

WatchGuard Mobile VPN with SSL Client v12.11 for Windows

- The Mobile VPN with SSL Client for Windows now supports SAML authentication. *[FBX-26372]*

WatchGuard IPSec Mobile VPN Client for Windows, Powered by NCP

- This release of the IPSec Mobile VPN Client for Windows supports these operating systems:
  - Windows 11, 64 bit (from version 21H2 up to and including version 24H2)
  - Windows 10, 64 bit (from version 20H2 up to and including version 22H2)
- The TunnelVision vulnerability (CVE-2024-3661) targets remote workstations or networks connected via VPN. For more information, go to the WatchGuard Security Advisory page.
  - The attack is not carried out directly on an existing VPN client, but on the routing in the respective operating system.
  - The attacker imitates a DHCP server in the network of the remote user, which manipulates the routing table on the user computer using DHCP option 121. The aim of this manipulation is to make sure that data is not sent by the standard route through the VPN tunnel, but is instead routed past the VPN tunnel.
  - In this version of the WatchGuard IPSec Mobile VPN Client for Windows, DHCP options 121 and 249 are filtered out by default in the network adapter so that the routing table is not changed. To disable this behavior, you can set a registry parameter:

    ```
    \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt
    Valuename: AllowDHCPOption121and249
    Valuetype: DWORD (32bit)
    Value: 0 - off, 1 - on. // Default 0
    ```
- This release resolves a bug in the driver or network adapter of the WatchGuard IPSec Mobile VPN Client for Windows that, in rare cases, caused a blue screen during the first boot after installation. As a result, the name and version of the network adapter has changed from **WatchGuard Secure Client Virtual NDIS6.20 Adapter version 12.1.2102.0** to **WatchGuard Secure Client Virtual NDIS Adapter version 13.1.2409.0**.
- If activated, the firewall of the WatchGuard IPSec Mobile VPN Client for Windows can now be seen in Windows Security.
- This release resolves an issue where the VPN service of the WatchGuard IPSec Mobile VPN Client for Windows crashed, indicating a problem with the driver interface (Mif32Init).

Known Issues and Limitations

Known issues for Fireware v12.11 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_11.exe` — Use this file to install WSM v12.11 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_11.exe` `firebox_M270_M370_M470_M570_M670_12_11.zip`
Firebox M290	`Firebox_OS_M290_12_11.exe` `firebox_M290_12_11.zip`
Firebox M390	`Firebox_OS_M390_12_11.exe` `firebox_M390_12_11.zip`
Firebox M590/M690	`Firebox_OS_M590_M690_12_11.exe` `firebox_M590_M690_12_11.zip`
Firebox M4600/M5600	`Firebox_OS_M4600_M5600_12_11.exe` `firebox_M4600_M5600_12_11.zip`
Firebox M4800/M5800	`Firebox_OS_M4800_M5800_12_11.exe` `firebox_M4800_M5800_12_11.zip`
Firebox NV5	`Firebox_OS_NV5_12_11.exe` `firebox_NV5_12_11.zip`
Firebox T20/T40	`Firebox_OS_T20_T40_12_11.exe` `firebox_T20_T40_12_11.zip`

If you have…	Select from these Fireware OS packages
Firebox T25/T45	`Firebox_OS_T25_T45_12_11.exe` `firebox_T25_T45_12_11.zip`
Firebox T55	`Firebox_OS_T55_12_11.exe` `firebox_T55_12_11.zip`
Firebox T70	`Firebox_OS_T70_12_11.exe` `firebox_T70_12_11.zip`
Firebox T80	`Firebox_OS_T80_12_11.exe` `firebox_T80_12_11.zip`
Firebox T85	`Firebox_OS_T85_12_11.exe` `firebox_T85_12_11.zip`

FireboxV
All editions for VMware
	`FireboxV_12_11.ova`
	`Firebox_OS_FireboxV_12_11.exe`
	`firebox_FireboxV_12_11.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_11.vhd.zip`
	`Firebox_OS_FireboxV_12_11.exe`
	`firebox_FireboxV_12_11.zip`

Firebox Cloud	`Firebox_OS_FireboxCloud_12_11.exe` `fireboxCloud_12_11.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_11.exe	**Mobile VPN with SSL Client for Windows**	**Yes**
WG-MVPN-SSL_12_10_4.dmg	Mobile VPN with SSL Client for macOS	No
WG-Mobile-VPN_Windows_x86-64_1519_29720.exe[1]	**WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP**[2]	**Yes**
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 v12.10.2 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.10.2, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.10.2, we recommend that you upgrade all SSO Clients to v12.7. You cannot use SSO Client v12.7 with versions of the SSO Agent lower than v12.5.4. Fireware v12.11 supports previous versions of the SSO Agent.

Upgrade to Fireware v12.11

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 v12.11 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 v12.11 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 v12.11 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.

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

AP Firmware Upgrade

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

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

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

To manually update firmware on your APs:

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

Upgrade a FireCluster to Fireware v12.11

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 v12.11 Operating System Compatibility Matrix

Last reviewed: 24 October 2024

WSM/ Fireware Component	Microsoft Windows 10, 11	Microsoft Windows Server 2019 & 2022	macOS v10.14, v10.15, v11, v12, v13, v14, & v15	Android 7, 8, 9, 10, 11, 12, 13, 14, & 15	iOS v9, v10, v11, v12, v13, v14, v15, v16, v17, & v18
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, 13]		
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, and macOS Sequoia 15.

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

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

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

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

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

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

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

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

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

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

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

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	✓	✓	✓	✓	✓	✓	✓	✓[2]
Mobile VPN with IKEv2 for Windows	✓	✓	✓[1]	–	✓	–	✓	–
Mobile VPN with L2TP	–	✓	✓[1]	–	✓	–	✓	–
Built-in Web Page on Port 4100 and 8080	✓	✓	✓	✓	✓	✓	✓	✓[3]
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.

[2] Supported with the Mobile VPN with SSL Client for Windows.

[3] Port 8080 does not support SAML authentication.

System Requirements

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

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, 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 v12.11

If you want to downgrade from WSM v12.11 to a lower version, you must uninstall WSM v12.11. 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 v12.11.

Next, install the same version of WSM that you used before you upgraded to WSM v12.11. 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 v12.11. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.11

If you want to downgrade from Fireware v12.11 to a lower version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.11. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.11 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.