Fireware v12.7 Update 1 Release Notes

Supported Devices	Firebox T20, T40, T55, T70, T80, M270, M370, M400, M440, M470, M500, M570, M670, M4600, M4800, M5600, M5800 FireboxV, Firebox Cloud, WatchGuard AP
Release Date	12.7: 20 April 2021 12.7 Update 1: 10 May 2021
Release Notes Revision	10 May 2021
Fireware OS Build	12.7: 639066 12.7 Update 1: 640389
WatchGuard System Manager Build	638978
WatchGuard AP Firmware	AP120, AP320, AP322: 8.8.3-12 AP125, AP225W, AP325, AP327X, AP420: 9.0.1-14.3

On 10 May 2021 we released Fireware v12.7 Update 1 as a maintenance update for Firebox T20, T40, T55, T70, T80, Firebox M Series (except M200 and M300), FireboxV, and Firebox Cloud appliances. For details on the issues resolved in this update release, see *Enhancements and Resolved Issues in Fireware 12.7 Update 1*.

Introduction

Fireware v12.7 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 simplifies AuthPoint multi-factor authentication (MFA) integration with the Firebox, and includes other important enhancements. Key features in Fireware v12.7 include:

AuthPoint Integration with a Firebox

You can now use AuthPoint as an authentication server on your Firebox, which makes it easier to configure AuthPoint MFA for:

- Mobile VPN with SSL
- Mobile VPN with IKEv2
- Firebox Web UI
- Firebox Authentication Portal

Automatic Updates of the HTTPS Exceptions List

The HTTPS exceptions list can now automatically update without a Fireware upgrade. When WatchGuard adds new domains or sites to the exceptions list, you can receive the updates automatically.

802.1p Marking for VLAN Interfaces

You can now enable 802.1p priority marking (tagging) for VLAN interfaces on your Firebox. 802.1p is required by some ISPs and can help to ensure a high level of quality for real-time communications that are sensitive to latency, such as VoIP.

APT Blocker Enhancements

- You can now connect to the APT Blocker server through an HTTP proxy server.
- By default, APT Blocker no longer sends unrecognized PDF files to the data center for analysis. Now you can specify whether APT Blocker submits PDF files for analysis, which gives you more control to address privacy concerns.

Log Rate Limits

You can now specify how many log messages the Firebox sends when it denies different types of traffic.

No FQDN Limits

There is no longer a limit on the number of fully qualified domain names (FQDNs) in your Firebox configuration. This means that you can define an unlimited number of FQDNs to use in firewall policy rules.

DHCP Lease Counts

Fireware Web UI now provides more information about DHCP leases. You can now see the total number of DHCP leases included in each IPv4 DHCP range configured on the Firebox, and how many of those leases are in use.

Intra-Bridge Traffic Inspection

You can now select to apply firewall policies to traffic that passes between bridge member interfaces (intra-bridge traffic). The Firebox now inspects and logs this traffic.

Localization Update

This release provides updated translation of the Fireware user interface.

For a full list of the enhancements in this release, see Enhancements and Resolved Issues or review the What's New in Fireware v12.7 PowerPoint.

Fireware v12.7 is based on Linux kernel 4.14. This is the first version of Fireware to support Linux kernel v4.14 on Firebox T55 and T70 devices. On some Firebox models, Linux kernel 4.14 does not provide sufficient quality and performance. Because of this, Fireware v12.7 is not available for Firebox T10, T15, T30, T35, M200, and M300. We continue to support these models with Fireware v12.5.x. For more information, see this Knowledge Base article.

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, M370, M400, M440, M470, M500, M570, M670, M4600, M4800, M5600, M5800, Firebox Cloud, or FireboxV. You cannot install Fireware v12.7 on any other Firebox model.
- 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 12.7 Update 1

- This release includes important fixes to resolve a security issue. *[FBX-21579, FBX-21590, FBX-21596]*
- A scheduled reboot of a FireCluster no longer causes a cluster member to become inactive. *[FBX-17099]*
- This release resolves a stuck *Homer* process for *get_webblocker* requests. *[FBX-20438]*
- For Yahoo or AOL mail servers, email no longer fails to send when an inbound/outbound SMTP Proxy policy is configured to inspect on port 465. *[FBX-20570]*
- An *ADMD* process core dump no longer occurs when an Active Directory user authenticates to the Firebox. *[FBX-20878]*
- Users can no longer disable SafeSearch in the Google Images tab when an HTTP Proxy is configured to enforce SafeSearch. *[FBX-21204]*
- IPS now works correctly with Firebox Cloud on Fireware v12.7. *[FBX-21472]*

Enhancements and Resolved Issues in Fireware v12.7

General

- You can now specify the maximum number of log messages to generate each minute for traffic denied by Blocked Sites, Blocked Ports, and several Default Packet Handling categories. *[FBX-19762]*
- This release corrects an invalid FireCluster *HAOPEvent* log message that caused the Status Report to not load. *[FBX-20746]*
- To address CVE-2021-3449 and CVE-2021-3450, the OpenSSL version used in Fireware is updated to version 1.1.1k. *[FBX-21412]*

Authentication

- You can now configure Mobile VPN with IKEv2, Mobile VPN with SSL, Fireware Web UI, and the Firebox Authentication Portal to authenticate users directly with AuthPoint. *[FBX-14607]*

Policies and Services

- You can now configure APT Blocker to connect through an HTTP proxy server. *[FBX-4750]*
- You can now specify whether APT Blocker submits unrecognized PDF files to the data center for analysis. *[FBX-21255]*
- There is no longer a limit on the number of FQDNs you can define in a Firebox configuration. *[FBX-20351]*
- You can now select to update the HTTPS exceptions list automatically when WatchGuard makes changes. *[FBX-19380]*
- IPS and Application Control now detect Wuji/UltraSurf traffic more accurately. *[FBX-20350]*
- Service Watch now accurately reports connection counts for configured policies. *[FBX-20977]*

Networking

- You can now disable the DNS cache on the Firebox. *[FBX-6806]*
- The Firebox now supports 802.1p priority marking (tagging) for VLAN interfaces. *[FBX-20173]*
- In Fireware Web UI, the DHCP Leases page now includes a **DHCPv4 Lease Summary** section that shows DHCP lease information for each configured IPv4 DHCP range. *[FBX-20574]*
- When you configure a bridge, you can now apply firewall policies to traffic that passes between bridge member interfaces. *[FBX-20630, FBX-14319]*

VPN

- Mobile VPN with SSL for macOS clients can now authenticate with Active Directory passwords that contain **§** or **£** characters. *[FBX-5996]*
- Mobile VPN with SSL client uninstallation now removes cached server and user information. *[FBX-7008]*
- This release resolves an issue where the **Enable Host Sensor Enforcement** check box did not remain selected in Policy Manager. *[FBX-21073, FBX-20389]*

Resolved Issues in Fireware 12.6.4 Update 1

- The Firebox proxy module no longer caches the server timeout action for sites when the WebBlocker Server is unavailable. *[FBX-21307]*
- This release resolves an issue that caused some web pages to fail to load and generated a *URI normalization failed* log when an HTTPS-proxy policy is configured with IPS enabled. *[FBX-20526]*
- Allowed WebBlocker categories are no longer incorrectly denied when multiple WebBlocker actions are configured. *[FBX-21036]*
- SMTP proxy auto detection no longer detects *application/x-pkcs7-signature* as binary. *[FBX-15726]*
- Traffic is no longer delayed when Google Safe Browsing is enabled with HTTPS content inspection and Application Control. *[FBX-20731]*
- When the IMAP proxy **Enable content type auto detection** option is selected, the configured action is now correctly performed on the value stated in the Content-Type header. *[FBX-20409]*
- The Firebox no longer generates the proxy debug log message *pxy_is_sndbuf_saturated* at the Error log level. *[FBX-21175]*
- Application Control no longer blocks all traffic and the Firebox no longer generates large numbers of log messages when the IPS/Application Control engine is accessed. *[FBX-20840]*
- This release resolves an *FQDND* process crash when domain names were longer than 64 bytes. *[FBX-21096]*
- This release resolves an issue that disconnected Mobile VPN with SSL users while a Firebox saves a configuration. *[FBX-21183]*
- NAT is no longer applied to Mobile VPN with IPSec traffic when that traffic is sent between Mobile VPN clients. *[FBX-20960]*
- Branch office VPNs that use IKEv2 now connect correctly to third-party endpoints when the **Start Phase 1 tunnel when Firebox starts** option is enabled. *[FBX-21065]*
- An issue that caused the Firebox to respond to ARP requests on the wrong interface is resolved. *[FBX-21044]*
- OSPF default route distribution logic is improved. *[FBX-21032, FBX-21033]*
- Interface link status is now updated correctly when you use Multi-WAN with FireCluster. *[FBX-20984]*
- Link monitoring no longer prevents valid traffic from passing over an active VPN connection. *[FBX-20868]*
- DHCP relay packets are now correctly delivered through VPN tunnels after a FireCluster failover event. *[FBX-19805]*
- You can now edit policies that use VIF from Fireware Web UI. *[FBX-21280]*
- Dynu.com dynamic DNS registration now works correctly. *[FBX-20970]*
- This release resolves an issue that caused a kernel warning stack trace related the *refcount_error_report*. *[FBX-20819]*
- This release removes expired Trusted Proxy CA certificates. *[FBX-21003]*

Enhancements and Resolved Issues in AP Firmware Update 9.0.1-14.3

This update release maintains compatibility for the latest AP firmware across all WatchGuard AP platforms and cloud services.

Known Issues and Limitations

Known issues for Fireware v12.7 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:

`WSM12_7_0_12_7.exe` — Use this file to install WSM v12.7 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 will always include 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_7_U1.exe firebox_M270_M370_M470_M570_M670_12_7_U1.zip
Firebox M400/M500	Firebox_OS_M400_M500_12_7_U1.exe firebox_M400_M500_12_7_U1.zip
Firebox M440	Firebox_OS_M440_12_7_U1.exe firebox_M440_12_7_U1.zip
Firebox M4600/M5600	Firebox_OS_M4600_M5600_12_7_U1.exe firebox_M4600_M5600_12_7_U1.zip
Firebox M4800/M5800	Firebox_OS_M4800_M5800_12_7_U1.exe firebox_M4800_M5800_12_7_U1.zip
Firebox T20/T40	Firebox_OS_T20_T40_12_7_U1.exe Firebox_OS_T20_T40_12_7_U1.zip
Firebox T55	Firebox_OS_T55_12_7_U1.exe firebox_T55_12_7_U1.zip
Firebox T70	Firebox_OS_T70_12_7_U1.exe firebox_T70_12_7_U1.zip
Firebox T80	Firebox_OS_T80_12_7_U1.exe Firebox_OS_T80_12_7_U1.zip
FireboxV All editions for VMware	FireboxV_12_7_U1.ova Firebox_OS_FireboxV_12_7_U1.exe firebox_FireboxV_12_7_U1.zip
FireboxV All editions for Hyper-V	FireboxV_12_7_vhd_U1.zip Firebox_OS_FireboxV_12_7_U1.exe Firebox_FireboxV_12_7_U1.zip
Firebox Cloud	FireboxCloud_12_7_U1.zip Firebox_OS_FireboxCloud_12_7_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.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO	Yes
WG-Authentication-Client_12_7.msi	Single Sign-On Client software for Windows	Yes
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.exe	Mobile VPN with SSL client for Windows[5]	Yes
WG-MVPN-SSL_12_7.dmg	Mobile VPN with SSL client for macOS[5]	Yes
WG-Mobile-VPN_Windows_x86_1411_48297.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP [2]	No
WG-Mobile-VPN_Windows_x86-64_1411_48297.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]	No
WG-Mobile-VPN_macOS_x86-64_400_46079.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 v12.7 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 supports previous versions of the SSO Agent.

[5] Not supported on ARM processor architecture.

Upgrade to Fireware v12.7 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 v12.7 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 v12.7 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 v12.7 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.

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 v12.7 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 v12.7 Update 1 Operating System Compatibility Matrix

Last reviewed 20 April 2021

WSM/ Fireware Component	Microsoft Windows 8.1, 10	Microsoft Windows Server 2012 & 2012 R2	Microsoft Windows Server 2016 & 2019	macOS v10.14, v10.15, & v11.x	Android 7.x, 8.x, 9.x, 10.x, & 11.x	iOS v9, v10, v11, v12, v13, & v14
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, see the Dimension Release Notes.*	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)[1]		✓	✓			
Single Sign-On Client	✓	✓	✓	✓[4]		
Single Sign-On Exchange Monitor[2]		✓	✓			
Terminal Services Agent[3]		✓	✓			
Mobile VPN with IPSec	✓			✓[4,5]	✓[5]	✓[5]
Mobile VPN with SSL	✓			✓[4, 8]	✓[6]	✓[6]
Mobile VPN with IKEv2	✓			✓[4]	✓[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*

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

[2]Microsoft 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.

[3]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.

[4]To 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. The WatchGuard Mobile VPN with IPSec client does not currently support macOS Big Sur 11.x and does not support Mac devices that have the ARM-based Apple M1 processor.

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

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

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

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

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 6.0, 6.5, 6.7, or 7.0
- Windows Server or Hyper-V Server 2012 R2, 2016, or 2019
- Linux KVM

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, 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

Downgrade from WSM v12.7

If you want to revert from WSM v12.7 to a lower version, you must uninstall WSM v12.7. 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 v12.7.

Next, install the same version of WSM that you used before you upgraded to WSM v12.7. 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 v12.7. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.7

If you want to downgrade from Fireware v12.7 to a lower version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.7. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.7 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.