Fireware v12.5.4 Release Notes

Supported Devices	Firebox T10, T15, T30, T35, T50, T55, T70, M200, M270, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600 FireboxV, Firebox Cloud, WatchGuard AP
Release Date	Fireware v12.5.4: 30 June 2020 WSM 12.6.2 Update 2: 25 September 2020
Release Notes Revision	6 January 2021
Fireware v12.5.4 Build	622768
WatchGuard System Manager v12.6.2 Update 2 Build	630401
WatchGuard AP Firmware	AP120, AP320, AP322: 8.8.3-12 AP125, AP225W, AP325, AP327X, AP420: 8.9.0-63

On 18 September 2020, we removed the Fireware v12.5.5 release from the Software Downloads Center. On 25 September 2020, we released WSM 12.6.2 Update 2 to enable customers to downgrade from Fireware v12.5.5 to Fireware v12.5.4.

Introduction

Fireware v12.5.4 is a feature release for Firebox T Series (except T20, T40, T80), Firebox M Series, FireboxV, and Firebox Cloud appliances.

This release introduces new features and many feature enhancements, including:

TDR Host Sensor Enforcement for Mobile VPN

Adds integrity checks to make sure endpoints that connect to corporate networks follow corporate policy and are not likely to be compromised by malware.

VPN Feature Enhancements

- Hex-based pre-shared keys for BOVPNs — Required for compliance with Commercial Solutions for Classified (CSfC), an NSA program
- MTU setting for BOVPN virtual interfaces — You can now specify a custom MTU value to ensure VPN connectivity between a Firebox and a third-party VPN endpoint
- Mobile VPN with SSL Client Download page — You can use a new CLI option to disable the download page if it does not comply with your corporate security policy

spamBlocker Engine Update

spamBlocker now uses Cloudmark, a cloud-based service from Proofpoint, to improve spam detection. Note that spamBlocker now sends the full email body over TLS to the cloud for scoring, not only an email hash. For a complete overview of the new service, see the What's New in Fireware v12.5.4 PowerPoint presentation and product documentation.

Networking Enhancements

- Support for dynamic DNS through Cloudflare
- Default multi-WAN method changes from Routing Table to Failover
- SD-WAN metrics have new default values to prevent early failover

Other Enhancements

- RADIUS server failover improvements
- Support for a new Microsoft API for communication with SSO Event Log Monitor
- Firebox Configuration Report updates

For a full list of the enhancements in this release, see *Enhancements and Resolved Issues in Fireware v12.5.4* or review the What's New in Fireware v12.5.4 PowerPoint.

There is no WSM v12.5.4. Use the latest version of WSM v12.6.2 to manage Fireboxes that run Fireware v12.5.4.

Before You Begin

Before you install this release, make sure that you have:

- A supported WatchGuard Firebox. This device can be a WatchGuard Firebox T Series (except T20, T40, T80) or Firebox M Series device. You can also use this version of Fireware on FireboxV and Firebox Cloud for AWS and Azure. *We do not support Fireware v12.2.x or higher on XTM devices.*
- 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 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[1] 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.

[1]The WatchGuard System Manager WebBlocker server component is not supported by Fireboxes with v12.2 or higher, and it is no longer possible to download a database for the WebBlocker server bundled with WatchGuard System Manager.

Enhancements and Resolved Issues in Fireware v12.5.4

General

- In WSM v12.6.x, Policy Manager now includes an OS Compatibility setting for Fireware v12.6 or higher. WatchGuard Management Server also now supports Device Configuration Templates for Fireware v12.6 or higher. *[FBX-18048]*
- Device Configuration Templates now support Default Packet Handling settings. *[FBX-5779]*
- The Firebox now only sends diagnostic log messages to WatchGuard Cloud when Support Access is enabled. The diagnostic log messages are not visible in WatchGuard Cloud. For more information, see this knowledge base article. *[FBX-16749]*
- The Fireware Web Setup Wizard now includes the Cloud-Managed (Beta) configuration option. This option is not yet supported by WatchGuard Cloud. *[FBX-19532]*
- A problem has been resolved that caused pending CSR certificates to remain present after successful WatchGuard Cloud registration. *[FBX-17225]*
- WatchGuard Cloud device monitoring no longer generates extraneous error messages when monitoring WatchGuard Cloud appliances. *[FBX-18133]*
- The Firebox now denies connections to auto-blocked sites. *[FBX-18320]*
- When an IP address is automatically added to the Blocked Sites list, an event log is now generated with the reason it was auto-blocked. *[FBX-17520]*
- You can now successfully add an entry to the Blocked Sites list that includes a wildcard FQDN. *[FBX-18268]*
- This release resolves a memory leak in the `homer` process. *[FBX-19481]*
- The SNMP Counter64 object is no longer restricted to 32-bit boundaries. This resolves a connection count display issue in the CLI. *[FBX-18325]*
- An issue that caused an RDP connection freeze is resolved. *[FBX-19200]*
- Several potential backup failure scenarios are resolved. *[FBX-19089, FBX-19564]*
- Several issues related to logging and error message displays are resolved. *[FBX-19154, FBX-19242]*

Authentication

- In RADIUS Server Settings, the default Dead Time value is now 10 minutes. The new default setting only applies to new configurations. *[FBX-4448]*
- Event Log Monitor now supports the Microsoft Windows Event Log API. *[FBX-16551]*
- You can now successfully save your configuration from Fireware Web UI after you disable the secondary RADIUS server settings. *[FBX-5152]*
- Authentication for an account in multiple groups now works correctly. *[FBX-19402]*
- SSO software now includes improved encryption. *[FBX-19075, FBX-19034, FBX-18889]*

SSO Agent v12.5.4 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.5.4, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.5.4, we recommend that you upgrade all SSO Clients to v12.5.4.

You cannot use SSO Client v12.5.4 with versions of the SSO Agent lower than v12.5.4. Fireware v12.5.4 supports previous versions of the SSO Agent.

Networking

- The Firebox now supports dynamic DNS through Cloudflare. *[FBX-17815]*
- The default multi-WAN method is now Failover. The new default method only applies to new configurations. *[FBX-16809]*
- In SD-WAN Metrics Settings, the default value for Latency is now 400ms and the default value for Jitter is now 100ms. The new default settings only apply to new configurations. *[FBX-16815]*
- A problem has been resolved that caused many `network_v` debug messages to appear in the log file. *[FBX-18134]*
- This release resolves a `networkd` process crash. *[FBX-18065]*
- Wireless clients can now obtain DHCP IP address information after a Rogue AP scan is completed on Firebox Wireless devices. *[FBX-15530]*
- Fireware Web UI now correctly displays DHCP lease information. *[FBX-16566]*
- The tabletop Firebox Wireless `hostapd` process now better handles process shutdown and recovery. *[FBX-17298]*
- This release resolves a crash in the `DHCPv6` process. *[FBX-18694]*

Proxies and Security Services

- spamBlocker now uses a new engine that improves performance. *[FBX-17268]*
- APT Blocker now correctly scans HWP and ISO files. *[FBX-17493, FBX-13133]*
- The Firebox Configuration Report now includes spamBlocker settings and exceptions for SMTP proxy actions, and WebBlocker exceptions for WebBlocker actions. *[FBX-15911, FBX-15914]*
- The WebBlocker Server Timeout setting has been updated with a new default range of 15-600 seconds. This change applies after you save a configuration to your device from WSM v12.6.x. *[FBX-16536]*
- In Policy Manager, in the Policy Properties dialog box, the SD-WAN Action drop-down list now shows the full name of SD-WAN actions. *[FBX-15219]*

VPN

- This release adds TDR Host Sensor Enforcement for mobile VPN connections from hosts to the Firebox. *[FBX-17530, FBX-17532]*
- This release adds an option to specify a custom maximum transmission unit (MTU) for BOVPN virtual interfaces. *[FBX-15920]*
- BOVPN and BOVPN virtual interface configurations now support hex-based pre-shared keys. *[FBX-16247]*
- VPN connections are no longer disrupted during normal IKE rekey operations. *[FBX-19406]*
- This release adds a Command Line Interface option to disable the Mobile VPN with SSL Client Download page hosted by the Firebox. *[FBX-135]*
- All virtual IP addresses are now correctly used with Mobile VPN. *[FBX-19320]*
- The timeout to establish an IKEv2 connection is now configurable through the CLI. *[FBX-19386]*
- This release includes an updated installation script for Mobile VPN with IKEv2. The script no longer fails when Windows Group Policy Objects specify digital signature restrictions for PowerShell scripts. *[FBX-19598]*

Enhancements and Resolved Issues in AP Firmware Update 8.9.0-63

- Added support for AP325 revision B hardware.

AP firmware versions 8.9.0-63 and higher are only available for 802.11ac Wave 2 access points. Wave 1 access points (AP120, AP320, and AP322) will remain on 8.8.x firmware versions for maintenance releases only.

Enhancements and Resolved Issues in AP Firmware Update 8.8.3-12

- The Minimum Association RSSI and Smart Steering options now work correctly when the default configuration is modified for APs managed locally by a Gateway Wireless Controller. *[AP-601]*
- AP120 and AP320 devices now retain their network configuration if they have a tagged VLAN configured when they upgrade. *[AP-622]*
- LLDP power allocation from a switch is now ignored if the received power value from the network switch is 0. This prevents APs from switching to lower PoE power if they connect through a PoE+ injector and receive LLDP messages from a PoE switch. *[AP-625]*

Known Issues and Limitations

Known issues for Fireware v12.5.4 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

There is no WSM v12.5.4. Use WSM v12.6.2 to manage Fireboxes that run Fireware v12.5.4.

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

`WSM_12_6_2_U2.exe` — Use this file to install WSM v12.6.2 Update 2 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 T30-T50 for the Firebox T30 or T50.

If you have…	Select from these Fireware OS packages
Firebox M4600/M5600	Firebox_OS_M4600_M5600_12_5_4.exe firebox_M4600_M5600_12_5_4.zip
Firebox M270/M370/M470/M570/M670	Firebox_OS_M270_M370_M470_M570_M670_12_5_4.exe firebox_M270_M370_M470_M570_M670_12_5_4.zip
Firebox M400/M500	Firebox_OS_M400_M500_12_5_4.exe firebox_M400_M500_12_5_4.zip
Firebox M440	Firebox_OS_M440_12_5_4.exe firebox_M440_12_5_4.zip
Firebox M200/M300	Firebox_OS_M200_M300_12_5_4.exe firebox_M200_M300_12_5_4.zip
Firebox T70	Firebox_OS_T70_12_5_4.exe firebox_T70_12_5_4.zip
Firebox T55	Firebox_OS_T55_12_5_4.exe firebox_T55_12_5_4.zip
Firebox T30/T50	Firebox_OS_T30_T50_12_5_4.exe firebox_T30_T50_12_5_4.zip
Firebox T35	Firebox_OS_T35_12_5_4.exe firebox_T35_12_5_4.zip
Firebox T15	Firebox_OS_T15_12_5_4.exe firebox_T15_12_5_4.zip
Firebox T10	Firebox_OS_T10_12_5_4.exe firebox_T10_12_5_4.zip
FireboxV All editions for VMware	FireboxV_12_5_4.ova Firebox_OS_FireboxV_12_5_4.exe firebox_FireboxV_12_5_4.zip
FireboxV All editions for Hyper-V	FireboxV_12_5_4_vhd.zip Firebox_OS_FireboxV_12_5_4.exe Firebox_FireboxV_12_5_4.zip
Firebox Cloud	FireboxCloud_12_5_4.zip Firebox_OS_FireboxCloud_12_5_4.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.

Filename	Description	Updated in this release
WG-Authentication-Gateway_12_5_4.exe	**Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO** [4]	✓
WG-Authentication-Client_12_5_4.msi	**Single Sign-On Client software for Windows** [4]	✓
WG-SSOCLIENT-MAC_12_5_4.dmg	**Single Sign-On Client software for macOS** [4]	✓
SSOExchangeMonitor_x86_12_0.exe	Exchange Monitor for 32-bit operating systems	
SSOExchangeMonitor_x64_12_0.exe	Exchange Monitor for 64-bit operating systems	
TO_AGENT_SETUP_11_12.exe	Terminal Services software for both 32-bit and 64-bit systems.	
WG-MVPN-SSL_12_5_3.exe	Mobile VPN with SSL client for Windows	
WG-MVPN-SSL_12_5_3.dmg	Mobile VPN with SSL client for macOS	
WG-Mobile-VPN_Windows_x86_1400_45109.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP [2]	
WG-Mobile-VPN_Windows_x86-64_1400_45109.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]	
WG-Mobile-VPN_macOS_x86-64_400_46079.dmg[1]	WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP [2]	
Watchguard_MVLS_Win_x86-64_200_rev19725.exe[1]	WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP [3]	

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

Upgrade to Fireware v12.5.4

Important information about the upgrade process:

- We recommend you use Fireware Web UI to upgrade to Fireware v12.x.
- 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.
- If your Firebox has Fireware v12.1.1 or later, the Firebox might temporarily disable some security services to free up enough memory to successfully perform a backup. To learn more, see Backup and Restore for XTM 25, XTM 26, and Firebox T10.
- To avoid a known issue that causes LDAP/AD user groups used by Mobile VPN to no longer appear, complete the workaround steps in this Knowledge Base article before you upgrade to Fireware v12.5.4.

If you want to upgrade a Firebox T10 device, we recommend that you reboot your Firebox before you upgrade. This clears your device memory and can prevent many problems commonly associated with upgrades in those devices. If your Firebox T10 has Fireware v12.1 or older, you might not be able to perform a backup before you upgrade the Firebox. This occurs because the memory use by Fireware v12.1 or older does not leave enough memory free to successfully complete the upgrade process on these devices. For these devices, we recommend you save a copy of the .xml configuration file with a distinctive name, as described here: Save the Configuration File.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x or v12.x 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.

You cannot restore a WatchGuard Server backup file created with WatchGuard System Manager v12.x to a v11.x installation. Make sure to retain your older server backup files when you upgrade to v12.0 or later in case you want to downgrade in the future.

To back up your Management Server configuration, from the computer where you installed the Management Server:

1. From WatchGuard Server Center, select **Backup/Restore Management Server**.
   The WatchGuard Server Center Backup/Restore Wizard starts.
2. Click **Next**.
   The Select an action screen appears.
3. Select **Back up settings**.
4. Click **Next**.
   The Specify a backup file screen appears.
5. Click **Browse** to select a location for the backup file. Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.
   The WatchGuard Server Center Backup/Restore Wizard is complete screen appears.
7. Click **Finish** to exit the wizard.

Upgrade to Fireware v12.5.4 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 v12.5.4 from Web UI

If your Firebox is running Fireware v11.10 or later, you can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. If your Firebox is running v11.9.x or earlier, use these steps to upgrade:

1. Before you begin, save a local copy of your configuration file.
2. Go to **System > Backup Image** or use the USB Backup feature to back up your current device image.
3. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads page.
   If you use the Windows-based installer on a computer with a Windows 64-bit operating system, this installation extracts an upgrade file called *[product-group].sysa-dl* to the default location of C:\Program Files(x86)\Common Files\WatchGuard\resources\FirewareXTM\12.5.4\[product-group].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\12.5.4
4. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
5. Browse to the location of the *[product-group].sysa-dl* from Step 3 and click **Upgrade**.

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 v12.5.4 from WSM/Policy Manager

1. Before you begin, save a local copy of your configuration file.
2. Select **File > Backup and Restore...** or use the USB Backup feature to back up your current device image.
3. On a management computer running a Windows 64-bit operating system, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called *[product-group].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\12.5.4\[product-group].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\12.5.4.
4. Install and open WatchGuard System Manager v12.6.x. Connect to your Firebox and launch Policy Manager.
5. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[product-group].sysa-dl* file from Step 3.

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 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 As 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 12.0 or Lower

If you have not previously upgraded to Fireware 12.0.1 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 to be able to manage the APs from Gateway Wireless Controller.

Depending on the version of Fireware you are upgrading 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 your FireCluster to Fireware v12.5.4

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.

Before you upgrade to Fireware v11.11 or higher, your Firebox must be running:
- Fireware XTM v11.7.5
- Fireware XTM v11.8.4
- Fireware XTM v11.9 or higher

If you try to upgrade from Policy Manager and your Firebox is running an unsupported version, the upgrade is prevented.

If you try to schedule an OS update of managed devices through a Management Server, the upgrade is also prevented.

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x before you upgrade to Fireware v11.11.x or higher or your Firebox will be reset to a default state.

Fireware 12.5.4 Operating System Compatibility Matrix

Last revised 30 June 2020

WSM/ Fireware Component	Microsoft Windows, 8.1, 10	Microsoft Windows 2012, & 2012 R2	Microsoft Windows Server 2016 & 2019	macOS v10.13, v10.14, & v10.15	Android 7.x, 8.x, 9.x, & 10.x	iOS v9, v10, v11, v12, & v13
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]	✓[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 v66*
- *Safari 12*

- *Safari iOS 13*
- *Safari (macOS Catalina)*
- *Chrome v74*

[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]On 11 November 2019, WatchGuard released multiple new client applications for macOS. These releases add support for macOS Catalina 10.15, and require macOS High Sierra 10.13 or later. To learn more, see macOS Catalina 10.15 software compatibility.

[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.

Authentication Support

This table gives you 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	Active Directory	LDAP	RADIUS	SecurID	Firebox (Firebox-DB) Local Authentication	SAML
Mobile VPN with IPSec for iOS, Windows, and macOS	✓	✓	✓	✓	✓	✓	–
Mobile VPN with IPSec for Android	✓	✓	✓	✓	–	✓	–
Mobile VPN with SSL	✓	✓	✓	✓	✓	✓	–
Mobile VPN with IKEv2 for Windows	✓	✓[1]	–	✓	–	✓	–
Mobile VPN with L2TP	✓	✓[1]	–	✓	–	✓	–
Built-in Web Page on Port 4100 and 8080	✓	✓	✓	✓	✓	✓	–
Access Portal	✓	✓	✓	✓	✓	✓	✓
AD Single Sign-On Support *(with or without client software)*	–	✓	✓	–	–	–	–
Terminal Services Manual Authentication	–	✓	✓	✓	✓	✓	–
Terminal Services Authentication with Single Sign-On	–	✓	–	–	–	–	–

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

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Minimum CPU	Intel Core or Xeon 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

With support for installation in both VMware and a Hyper-V environments, a WatchGuard FireboxV virtual machine can run on a VMware ESXi 6.0, 6.5, or 6.7 host, or on Windows Server 2012 R2 2016, or 2019, or Hyper-V Server 2012 R2, 2016, or 2019.

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	Memory (recommended)	Maximum vCPUs
Small	2048 MB[1]	2
Medium	4096 MB	4
Large	4096 MB	8
Extra Large	4096 MB	16

[1] *4096 MB is required to enable Intelligent AV.*

Downgrade Instructions

Downgrade from WSM v12.6.2 Update 2 to earlier WSM v12.x or v11.x

You must use WSM v12.6.x to manage devices that run Fireware v12.5.4.

If you want to revert from WSM v12.6.2 Update 2 to an earlier version, you must uninstall WSM v12.6.2 Update 2. 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 v12.6.2.

Downgrade from Fireware v12.5.4 to earlier Fireware v12.x or v11.x

If you want to downgrade from Fireware v12.5.4 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.5.4. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.5.4 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 Downgrade with Web UI. 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.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web 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 v12.2.1. UI changes introduced since v12.2.1 may 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

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the 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 have set in your web browser by default.

WatchGuard System Manager

When you install WSM, you can choose what 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 have set in your web browser.

Documentation

The latest version of localized Fireware Help is available on the Fireware documentation page. Updated documentation to match the localization updates in the UI will be released in several weeks.