Fireware v12.5 Update 1 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 12.5 -- 11 July 2019 Fireware 12.5 Update 1 -- 12 August 2019 AP Firmware Update -- 4 September 2019
Release Notes Revision	20 November 2019
Fireware OS Build	Fireware 12.5 -- 597646 Fireware 12.5 Update 1 -- 599856
WatchGuard System Manager Build	596863
WatchGuard AP Firmware	AP100, AP102, AP200: 1.2.9.16 AP300: 2.0.0.11 AP120, AP125, AP320, AP322, AP325, AP420: 8.8.0-179

Introduction

On 4 September 2019, WatchGuard released AP firmware update 8.8.0-179 for AP120, AP125, AP320, AP322, AP325, and AP420. See Enhancements and Resolved Issues for more information.

On 12 August 2019, WatchGuard released Fireware v12.5 Update 1 to resolve several bugs. See Enhancements and Resolved Issues for more information.

Fireware v12.5 is a major release for Firebox T Series, Firebox M Series, FireboxV, and Firebox Cloud appliances. Together with other features new to Fireware v12.5, we're especially excited to launch the next generation of Access Portal functionality.

Key features in Fireware 12.5 include:

Access Portal Enhancements

The Access Portal now has reverse proxy technology built in, to enable the Access Portal to communicate with local/internal web servers. It also now supports Microsoft ActiveSync.

Proxy Warn Message Customization

This release introduces the Warn message for HTTP and Explicit proxy.

WebBlocker Override Enhancements

You can now configure WebBlocker override for specific categories, and for specific authentication groups.

Multiple RADIUS server support

All features that support RADIUS authentication servers now support multiple RADIUS servers in both Web UI and Policy Manager.

RADIUS Domain Name

You must now configure a domain name when you add a new RADIUS server.

To authenticate with RADIUS, users must now specify the RADIUS domain name. Mobile VPN and Access Portal users must specify the domain name to authenticate to a server other than the primary server.

If your configuration includes a RADIUS server, and you upgrade to Fireware v12.5 or higher, the Firebox automatically uses RADIUS as the domain name for that server. To authenticate to that server, users must specify RADIUS as the domain name.

Updated WatchGuard Mobile VPN with IPSec client

This release includes new client versions for both macOS and Windows users.

This release also features important fixes for issues that impact VPN functionality and proxy handling of encrypted traffic.

For a full list of the enhancements in this release, see *Resolved Issues in AP Firmware Update 8.8.0-179* or review the What's New in Fireware v12.5 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 T Series 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. In this release, a change affects some inbound NAT policies with policy-based routing or an SD-WAN action. 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 WebBlocker server component is not supported by Fireboxes with v12.2 or higher, and it is no longer possible to download a database for WebBlocker server.

Known Issues and Limitations

Known issues for Fireware v12.5 Update 1 and its management applications, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To see known issues for a specific release, from the **Product & Version** filters you can expand the Fireware version list and select the check box for that version.

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

This page does not include every issue resolved in a release.
Issues discovered in internal testing or beta testing are not usually included in this list.

Resolved Issues in AP Firmware Update 8.8.0-179

- This release resolves TCP SACK panic kernel vulnerabilities (CVE-2019-11477, CVE-2019-11478, CVE-2019-11479). *[AP-498]*
- The use of the Fast Roaming (802.11r) option no longer results in slow speeds after roaming on the AP325 and AP420. *[AP-323]*
- APs no longer reboot when they connect to switches with 802.3az enabled. 802.3az has been disabled on all APs to prevent connectivity issues. *[AP-275]*

Enhancements and Resolved Issues in Fireware v12.5 Update 1

- The Firebox T30, T35, T50, M200, and M300 can now successfully receive traffic from a device with a MAC address that ends in `:88:08`. *[FBX-16948]*
- This release resolves an issue that causes the RADIUS NAS-IP addressed to appear in reverse order in Access-Request packets. *[FBX-16368]*
- This release resolves a DNSWatch issue on the Firebox and corrects an error on external interfaces when retrieving data. *[FBX-15477]*
- The `iked` process no longer crashes when your Firebox has a short RSA certificate. *[FBX-16606]*
- This release resolves a memory leak in the `admd` process. *[FBX-16915, FBX-16983]*
- This release resolves an issue which caused a FireboxV to become unregistered in WatchGuard Cloud if it uses a local DNS server and the external interface is down for more than 4 minutes. *[FBX-16888]*
- This release resolves an issue that causes the default route to disappear after a FireCluster failover. *[FBX-16604, FBX-16799]*
- A proxy process crash no longer occurs when traffic connects through a SIP-ALG proxy policy. *[FBX-16581, FBX-16778]*
- This release resolves an issue that causes some websites to fail to load with a browser message `ERR_CONTENT_LENGTH_MISMATCH`. *[FBX-16354]*
- This release resolves an issue that causes the Firebox to stop sending updates to DNSWatch Cloud after an upgrade to Fireware 12.5. *[FBX-17207]*
- This release resolves a Web UI syntax error that occurs when you configure DNS servers through Dimension Command. *FBX-16608*

Enhancements and Resolved Issues in WSM and Fireware v12.5

General

- Policy Manager now displays the OS version for a Fireware upgrade file. *[FBX-16667]*
- The Samoa time zone name is updated in Policy Manager. *[FBX-16509]*
- WatchGuard System Manager now supports the upcoming Firebox T35-R model. *[FBX-15682]*
- Policy Manager now shows the correct Mobile VPN with SSL licenses for your Firebox M270. *[FBX-16376]*
- This release resolves a kernel crash specific to Firebox M200 and M300 devices. *[FBX-12412]*
- Management Server policy templates now include the Dynamic NAT and 1-to-1 NAT options in the Advanced tab. *[FBX-3982]*

Networking

- VLAN Hotspot configuration is no longer removed when you change the VLAN ID. *[FBX-11625]*
- Firebox M270 devices configured for auto-negotiation of network interfaces now display the correct interface speed in Status Report. *[FBX-16452]*
- The *Set Source IP address* feature now works correctly for HTTPS proxy traffic with NAT configured but no Content Inspection. *[FBX-16392]*
- A configured SD-WAN action is no longer applied to traffic sent to the Firebox. *[FBX-16341]*
- After a FireCluster failover, the link monitor now continues to operate correctly and external interfaces do not show as failed. *[FBX-16572, FBX-16576]*
- Policy Manager now consistently allows you to remove or edit DHCP reservations. *[FBX-16400]*
- Web UI now correctly imports aliases that include /128 IPv6 addresses. *[FBX-12580]*

Proxies and Services

- Users can now use WebBlocker override with their Firebox-DB or Active Directory group membership. *[FBX-4652]*
- You can now create a custom *Warn* message for proxy actions. *[FBX-15542]*
- DNSwatch now correctly updates protected networks when the Firebox is inside a network that applies NAT to internet-bound traffic. *[FBX-16737]*
- DNSWatch now adds client-related information to request headers for connections to the blackhole server. *[FBX-15541]*
- spamBlocker for IMAP proxy can now apply exceptions to emails that do not have a `TO:` header. *[FBX-16210]*
- This release resolves an HTTPS proxy issue that required intermediate CA certificates to be imported as General Use for pages to load correctly. *[FBX-14768]*

Access Portal

- This release adds reverse proxy functionality to the Access Portal. *[FBX-8916]*
- Users can no longer log in to Access Portal with an AD user name when AD is not configured as an authentication server. *[FBX-15845]*

Logging and Notification

- The SNMPd process no longer causes high CPU usage. *[FBX-16426]*

Authentication

- You can now configure multiple RADIUS servers for authentication. *[FBX-15605]*
- You can now consistently use Policy Manager to save account lockout settings for Firebox-DB users. *[FBX-10455]*
- RADIUS authentication no longer fails because of unsupported RADIUS attributes in the `access-accept` reply. *[FBX-16056]*

VPN

- You can now use ECDSA Certificates for BOVPN and BOVPN Virtual Interface phase 1 authentication. *[FBX-15511]*
- You can no longer modify the Authentication drop-down in predefined VPN Phase 2 options. *[FBX-16642]*
- You can now configure BOVPN using the secondary IP address of a VLAN. *[FBX-16492, FBX-16493]*
- The BOVPN remote gateway IP address is now sent in the correct order when the domain name option is enabled. *[FBX-16515]*
- Mobile VPN with IPSec DNS server settings no longer revert to the global DNS settings when you use Web UI to modify the VPN configuration. *[FBX-16026]*

Wireless

- The Gateway Wireless Controller now supports the upcoming AP327X device. *[FBX-15650]*
- Gateway Wireless Controller SSID scheduling is no longer affected by the switch to daylight savings time. *[FBX-16326]*

Integrations

- NetFlow connections can now leave over any Firebox interface. *[FBX-14021]*

WatchGuard Mobile VPN with IPSec Client for Windows (v11.14)

- This release restricts the connection test by the client to a maximum of four pings.
- This release features optimization updates to the HotSpot login feature, specifically with Seamless Roaming.
- This release resolves a vulnerability caused by the NCP Credential Provider that allowed unintended access to Windows Explorer.
- The client uninstall no longer fails to remove the filter driver.
- This release improves connection behavior after your computer wakes from sleep mode.

WatchGuard Mobile VPN with IPSec Client for macOS (v3.20)

- This release features support for dark mode, introduced in macOS Mojave release.
- This release supports the macOS Keychain for certificate storage.
- This release features user interface improvements, including split-tunneling configuration with multiple DNS suffixes.
- The client uninstall no longer asks for permission to access your address book, calendar, and photos.
- This release improves detection of friendly networks that were already connected when the system booted.

- This release resolves a log file rights issue that occurred after an OS update.
- This release resolves a connection failure that occurred when a certificate was used in macOS keychain with RSA-PSS padding enabled.

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_5.exe` — Use this file to install WSM v12.5 or to upgrade WatchGuard System Manager from an earlier version.

Fireware OS

If your Firebox is running Fireware v11.10 or later, you can upgrade the Fireware OS on your Firebox automatically from the Fireware Web UI **System > Upgrade OS** page.

If you prefer to upgrade from Policy Manager, or from an earlier version of Fireware, you can use 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_U1.exe` `firebox_M4600_M5600_12_5_U1.zip`
Firebox M270/M370/M470/M570/M670	`Firebox_OS_M270_M370_M470_M570_M670_12_5_U1.exe` `firebox_M270_M370_M470_M570_M670_12_5_U1.zip`
Firebox M400/M500	`Firebox_OS_M400_M500_12_5_U1.exe` `firebox_M400_M500_12_5_U1.zip`
Firebox M440	`Firebox_OS_M440_12_5_U1.exe` `firebox_M440_12_5_U1.zip`
Firebox M200/M300	`Firebox_OS_M200_M300_12_5_U1.exe` `firebox_M200_M300_12_5_U1.zip`
Firebox T70	`Firebox_OS_T70_12_5_U1.exe` `firebox_T70_12_5_U1.zip`
Firebox T55	`Firebox_OS_T55_12_5_U1.exe` `firebox_T55_12_5_U1.zip`
Firebox T30/T50	`Firebox_OS_T30_T50_12_5_U1.exe` `firebox_T30_T50_12_5_U1.zip`
Firebox T35	`Firebox_OS_T35_12_5_U1.exe` `firebox_T35_12_5_U1.zip`
Firebox T15	`Firebox_OS_T15_12_5_U1.exe` `firebox_T15_12_5_U1.zip`
Firebox T10	`Firebox_OS_T10_12_5_U1.exe` `firebox_T10_12_5_U1.zip`

FireboxV
All editions for VMware
	`FireboxV_12_5_U1.ova`
	`Firebox_OS_FireboxV_12_5_U1.exe`
	`firebox_FireboxV_12_5_U1.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_5_U1_vhd.zip`
	`Firebox_OS_FireboxV_12_5_U1.exe`
	`Firebox_FireboxV_12_5_U1.zip`

Firebox Cloud	`FireboxCloud_12_5_U1.zip` `Firebox_OS_FireboxCloud_12_5_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.

Filename	Description	Updated in this release
WG-Authentication-Gateway_12_4.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO	
WG-Authentication-Client_12_3.msi	Single Sign-On Client software for Windows	
WG-SSOCLIENT-MAC_12_3.dmg	Single Sign-On Client software for macOS	
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.exe[4]	**Moblie VPN with SSL client for Windows**	✓
WG-MVPN-SSL_12_5.dmg[4]	**Mobile VPN with SSL client for macOS**	✓
WG-Mobile-VPN_Windows_x86_1316_43395.exe[1]	**WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP** [2]	✓
WG-Mobile-VPN_Windows_x86-64_1316_43395.exe[1]	**WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP** [2]	✓
WG-Mobile-VPN_macOS_x86-64_320_43098.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] This 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]With Fireware v12.5, the version of the Mobile VPN with SSL client updated to v12.5. This update is because of upgrades in our software development environment, which caused the md5 checksum of the Mobile VPN with SSL client installer to change. This release does not include any bug fixes or feature enhancements.

Upgrade to Fireware v12.5 Update 1

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.

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 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 Update 1 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\[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. 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 2 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 Update 1 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\[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. Install and open WatchGuard System Manager v12.5. 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 2.

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 AP Devices

Beginning with Fireware v11.12.4, AP firmware is no longer bundled with Fireware OS. All AP device 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.

Important Upgrade Steps

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.

AP Firmware Upgrade

The current AP firmware versions for each AP device model are:

AP Device Model	Current Firmware Version
AP100, AP102, AP200	1.2.9.16
AP300	2.0.0.11
AP120, AP125, AP320, AP322, AP325, AP420	8.8.0-179

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.**

Note that you cannot upgrade an AP120, AP320, AP322, or AP420 to 8.3.0-657 or higher unless your Firebox is running Fireware v11.12.4 or higher. If your Firebox does not run v11.12.4. or higher, you will not see an option to upgrade to AP firmware v8.3.0-657 or higher.

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

To manually update firmware on your AP devices:

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

Upgrade your FireCluster to Fireware v12.5 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.

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 Update 1 Operating System Compatibility Matrix

Last revised 12 August 2019

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10	Microsoft Windows Server 2008 R2, 2012, & 2012 R2	Microsoft Windows Server 2016 & 2019	Mac OS X/macOS v10.10, v10.11, v10.12, v10.13, & v10.14	Android 6.x, 7.x, 8.x, & 9.x	iOS v8, v9, v10, v11, & v12
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	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[2]		✓	✓			
Terminal Services Agent[3]		✓	✓			
Mobile VPN with IPSec	✓[4]			✓[4,5]	✓[5]	✓[5]
Mobile VPN with SSL	✓			✓	✓[6]	✓[6]
Mobile VPN with IKEv2	✓			✓	✓[7]	✓
Mobile VPN with L2TP	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *Windows 8.x support does not include Windows RT.*
- *For Windows Server 2008 R2, we support 64-bit only.*

The following browsers are supported for both Fireware Web UI and WebCenter (Javascript required):

- *IE 11*
- *Microsoft Edge42*
- *Firefox v66*
- *Safari 12*

- *Safari iOS 12*
- *Safari (macOS Mojave 10.14.1)*
- *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]WatchGuard Mobile VPN with IPSec client (NCP) v3.0 or above is required if you use macOS 10.13.

[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*

	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 Windows by Shrew Soft	✓	✓	✓[1]	–	✓	–
Mobile VPN with IPSec for Android	✓	✓	✓	–	✓	–
Mobile VPN with SSL	✓	✓	✓	✓	✓	–
Mobile VPN with IKEv2 for WIndows	✓[2]	–	✓	–	✓	–
Mobile VPN with L2TP	✓[2]	–	✓	–	✓	–
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] The Shrew Soft client does not support two-factor authentication with challenge responses.

[2] 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 5.5, 6.0, or 6.5 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 v12.5 to earlier WSM v12.x or v11.x

If you want to revert from WSM v12.5 to an earlier version, you must uninstall WSM v12.5 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 v12.5

Next, install the same version of WSM that you used before you upgraded to WSM v12.5. 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 v12.5. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.5 Update 1 to earlier Fireware v12.x or v11.x

If you want to downgrade from Fireware v12.5 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 Update 1. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.5 Update 1 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.

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 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.