Fireware v12.3.1 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	25 January 2019
Release Notes Revision	6 June 2019
Fireware OS Build	585922 (updated for Fireware v12.3.1 Update 1 on 2 April 2019) *584973 (original Fireware v12.3.1 release)*
WatchGuard System Manager Build	584274 (for 12.3.1)
WatchGuard AP Firmware	AP100, AP102, AP200: 1.2.9.16 AP300: 2.0.0.11 AP125: 8.6.0-644.3 AP120, AP320, AP322, AP325, AP420: 8.6.0-646

Introduction

On 27 March 2019, we released AP firmware 8.6.0-646 (AP120, AP320, AP322, AP325, AP420) and 8.6.0-644.3 (AP125). For more information, see *Enhancements and Resolved Issues* and *Update AP Devices*.

On 25 January 2019, we released Fireware 12.3.1 Update 1. This updated release resolves an issue with Gateway Wireless Controller.

Fireware v12.3.1 is a maintenance release for Firebox T Series, Firebox M Series, FireboxV, and Firebox Cloud appliances. This release includes localization updates for the Fireware user interfaces and addresses numerous bugs and minor feature enhancements. For a full list of the enhancements in this release, see *Enhancements and Resolved Issues*. or review the What's New in Fireware v12.3.1 PowerPoint.

Fireware v12.2 and later versions do not support XTM appliances, and have changes to WebBlocker functionality for some users. The current release of WatchGuard System Manager is compatible with Fireboxes and XTM devices with Fireware v12.1.x. For more information, be sure to review the knowledge base article Release-Specific Upgrade Notes

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. 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.

Known Issues and Limitations

Known issues for Fireware v12.3.1 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.

Enhancements and Resolved Issues

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.

Enhancements and Resolved Issues in AP Firmware 8.6.0-646 and 8.6.0.644.3

- With this update, an AP no longer reserves an IP address for each VLAN on an SSID. An IP is only reserved for the management communications VLAN. *[AP-396]*

Enhancements and Resolved Issues in Fireware and WSM 12.3.1 Update 1

- The update on January 25th resolves an issue with Fireware v12.3.1 in which the Gateway Wireless Controller could not manage most AP devices. *[FBX-15365, FBX-15183]*

Enhancements and Resolved Issues in Fireware and WSM 12.3.1

General

- This release resolves an issue with FireCluster log messages that caused Traffic Monitor to fail to display any log messages. *[FBX-14840]*
- The Firebox no longer fails to send log messages to Dimension or a WatchGuard Log Server after you enable FIPS mode. *[FBX-13318]*
- This release resolves a kernel crash on the Firebox T30, T50, T35, M200 and M300 models. *[FBX-14699]*

Authentication

- SSO Exceptions configured as a host range are no longer restricted to a single class C (/24) network. *[FBX-14459, FBX-14753]*
- This release resolves an issue with Event Log Monitor threads not responding to user queries. *[FBX-14317]*

Networking

- The Firebox System Manager SD-WAN status page now correctly displays failback options. *[FBX-14639]*
- The new cluster master now correctly updates with routes from OSPF after a FireCluster failover event. *[FBX-14909]*
- This release resolves an issue with PPPoE negotiation after FireCluster failover when a secondary network IP address is configured on the interface. *[FBX-13499]*
- This release resolves a localization issue in Japanese-language Web UI in the TCP MTU Probing configuration. *[FBX-10285]*
- The Firebox now correctly sends diagnostic log messages for Link Monitor. *[FBX-13764]*
- This release corrects an issue that caused several CLI diagnostic commands for FQDN to fail. *[FBX-13834]*
- You can now add domains that include underscore characters to DNS forwarding rules. *[FBX-14012]*
- This release resolves an issue in which a flood of broadcast packets caused excessive memory usage. *[FBX-14439]*

VPN

- IKEv2 multi-wan VPN failback now works correctly when one side of Branch Office VPN is behind a NAT device. *[FBX-14842]*

Centralized Management

- You can now assign user roles in Management Server. *[FBX-14816]*
- This release resolves an issue that caused managed Firebox templates to fail with the error message: Invalid Configuration. *[FBX-14881]*

Proxies and Services

- The Firebox now correctly registers external secondary IP addresses when you enable DNSWatch. *[FBX-14763]*
- This release resolves an IMAP proxy crash. *[FBX-14123]*
- This release introduces APT scanning for objects identified as `suspicious` by Intelligent AV. *[FBX-14716]*

Certificates

- The Firebox now correctly labels Certificate Signing Requests for the Proxy Authority by that name instead of Proxy Server. *[FBX-14134, FBX-13884]*
- You can now import a certificate with an Elliptical Curve (EC) private key. *[FBX-14754]*

Firebox Integrations

- You can no longer specify invalid values for Memory Usage in a Tigerpaw configuration. *[FBX-13881]*

Gateway Wireless Controller and WatchGuard APs

- The Gateway Wireless Controller now indicates the AP power source detected by the Access Points which support detection. *[FBX-14035, FBX-14662, FBX-14661]*

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_3_1.exe` — Use this file to install WSM v12.3.1 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_3_1_U1.exe firebox_M4600_M5600_12_3_1_U1.zip
Firebox M270/M370/M470/M570/M670	Firebox_OS_M270_M370_M470_M570_M670_12_3_1_U1.exe firebox_M270_M370_M470_M570_M670_12_3_1_U1.zip
Firebox M400/M500	Firebox_OS_M400_M500_12_3_1_U1.exe firebox_M400_M500_12_3_1_U1.zip
Firebox M440	Firebox_OS_M440_12_3_1_U1.exe firebox_M440_12_3_1_U1.zip
Firebox M200/M300	Firebox_OS_M200_M300_12_3_1_U1.exe firebox_M200_M300_12_3_1_U1.zip
Firebox T70	Firebox_OS_T70_12_3_1_U1.exe firebox_T70_12_3_1_U1.zip
Firebox T55	Firebox_OS_T55_12_3_1_U1.exe firebox_T55_12_3_1_U1.zip
Firebox T30/T50	Firebox_OS_T30_T50_12_3_1_U1.exe firebox_T30_T50_12_3_1_U1.zip
Firebox T35	Firebox_OS_T35_12_3_1_U1.exe firebox_T35_12_3_1_U1.zip
Firebox T15	Firebox_OS_T15_12_3_1_U1.exe firebox_T15_12_3_1_U1.zip
Firebox T10	Firebox_OS_T10_12_3_1_U1.exe firebox_T10_12_3_1_U1.zip
FireboxV All editions for VMware	FireboxV_12_3_1_U1.ova Firebox_OS_FireboxV_12_3_1_U1.exe firebox_FireboxV_12_3_1_U1.zip
FireboxV All editions for Hyper-V	FireboxV_12_3_1_U1_vhd.zip Firebox_OS_FireboxV_12_3_1_U1.exe Firebox_FireboxV_12_3_1_U1.zip
Firebox Cloud	FireboxCloud_12_3_1_U1.zip Firebox_OS_FireboxCloud_12_3_1_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_3_1.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_2.exe	Moblie VPN with SSL client for Windows	
WG-MVPN-SSL_12_2.dmg	Mobile VPN with SSL client for macOS	
WG-Mobile-VPN_Windows_x86_1313_41322.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP [2]	
WG-Mobile-VPN_Windows_x86-64_1313_41322.exe[1]	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]	
WG-Mobile-VPN_macOS_x86-64_310_40218.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.

Upgrade to Fireware v12.3.1 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 v12.3.1 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\12.3.1\[product-group].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\12.3.1
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 Fireware v12.3.1 on your computer, you must run the Fireware v12.3.1 Update 1 installer twice (once to remove v12.3.1 software and again to install v12.3.1 Update 1).

Upgrade to Fireware v12.3.1 from WSM/Policy Manager

1. Before you begin, save a local copy of your configuration file.
2. Select **File > Backup** 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\12.3.1\[product-group].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\12.3.1.
4. Install and open WatchGuard System Manager v12.3.1. 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 Fireware v12.3.1 on your computer, you must run the Fireware v12.3.1 Update 1 installer twice (once to remove v12.3.1 software and again to install v12.3.1 Update 1).

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
AP125	8.6.0-644.3
AP120, AP320, AP322, AP325, AP420	8.6.0-646

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 v12.3.1 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 12.3.1 Update 1 and WSM v12.3.1 Operating System Compatibility Matrix

Last revised 25 January 2019

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10	Microsoft Windows 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 v64*
- *Safari 12*
- *Safari iOS 12*
- *Safari (macOS Mojave 10.14.1)*
- *Chrome v71*

[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 yet supported, but tested*

	Active Directory[1]	LDAP	RADIUS[2]	SecurID[2]	Firebox (Firebox-DB) Local Authentication
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓[3]	–	✓
Mobile VPN with IPSec/WatchGuard client (NCP)	✓	✓	✓	✓	✓
Mobile VPN with IPSec for iOS and macOS X native VPN client	⚑	⚑	⚑	✓	✓
Mobile VPN with IPSec for Android devices	✓	✓	✓	–	✓
Mobile VPN with SSL for Windows	✓	✓	✓[4]	✓[4]	✓
Mobile VPN with SSL for macOS	✓	✓	✓	✓	✓
Mobile VPN with SSL for iOS and Android devices	⚑	⚑	⚑	✓	✓
Mobile VPN with IKEv2 for WIndows	✓[6]	–	✓	–	✓
Mobile VPN with IKEv2 for macOS	✓[6]	–	✓	–	✓
Mobile VPN with IKEv2 for iOS	✓[6]	–	✓	–	✓
Mobile VPN with IKEv2 for Android by StrongSwan	✓[6]	–	✓	–	✓
Mobile VPN with L2TP	✓[6]	–	✓	–	✓
Built-in Authentication Web Page on Port 4100	✓	✓	✓	✓	✓
Single Sign-On Support *(with or without client software)*	✓	✓	–	–	–
Terminal Services Manual Authentication	✓	⚑	⚑	⚑	✓
Terminal Services Authentication with Single Sign-On	✓[5]	–	–	–	–
Citrix Manual Authentication	⚑	⚑	⚑	⚑	✓
Citrix Manual Authentication with Single Sign-On	✓[5]	–	–	–	–

with success by WatchGuard customers

[1] Active Directory support includes both single domain and multi-domain support, unless otherwise noted.

[2] RADIUS and SecurID support includes support for both one-time passphrases and challenge/response authentication integrated with RADIUS. In many cases, SecurID can also be used with other RADIUS implementations, including Vasco.

[3] The Shrew Soft client does not support two-factor authentication.

[4] Fireware supports RADIUS Filter ID 11 for group authentication.

[5] Both single and multiple domain Active Directory configurations are supported. For information about the supported Operating System compatibility for the WatchGuard TO Agent and SSO Agent, see the current Fireware and WSM Operating System Compatibility table.

[6] 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 a VMware and a Hyper-V environment, 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 or 2016.

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 v12.3.1 to earlier WSM v12.x or v11.x

If you want to revert from WSM v12.3.1 to an earlier version, you must uninstall WSM v12.3.1 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 v12.3.1.

Next, install the same version of WSM that you used before you upgraded to WSM v12.3.1. 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 v12.3.1. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.3.1 Update 1 to earlier Fireware v12.x or v11.x

If you want to downgrade from Fireware v12.3.1 Update 1 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.3.1 Update 1. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.3.1 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 updates the localization for the management user interfaces (WSM application suite and Web UI) to 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.