# Fireware v12.9 Update 1 Release Notes

| | |
|---|---|
| Supported Devices | Firebox T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, M570, M590, M670, M690, M4600, M4800, M5600, M5800<br>FireboxV, Firebox Cloud, Firebox NV5, WatchGuard AP |
| Release Date | 12.9 Update 1: 18 January 2023<br>12.9: 13 December 2022 |
| Release Notes Revision | 18 January 2023 |
| Fireware OS Build | 12.9 Update 1 (Firebox NV5): 673780<br>12.9 Update 1 (Other Supported Devices): 673767<br>12.9 (Firebox NV5): 672249<br>12.9 (Other Supported Devices): 672226 |
| WatchGuard System Manager Build | 12.9 Update 1: 673693<br>12.9: 672165 |
| WatchGuard AP Firmware | AP120, AP322: 8.8.3-12<br>AP125, AP225W, AP325, AP327X, AP420: 11.0.0-36 |

# Introduction

## Fireware v12.9 Update 1

On 18 January 2023, WatchGuard released Fireware v12.9 Update 1. This release includes a number of resolved issues. See Enhancements and Resolved Issues in Fireware v12.9 Update 1 for more information.

## Fireware v12.9

Fireware v12.9 is a major release for Firebox T20, T40, T55, T70, T80, Firebox M Series (except M200 and M300), FireboxV, Firebox NV5, and Firebox Cloud appliances.

This release introduces several major enhancements to Fireware and addresses many smaller issues and bugs. Features in this release include:

- Multi-factor authentication (MFA) support for the WSM Management Server
- Client certificate authentication support for LDAPS
- Split tunneling support for Mobile VPN with IKEv2
- Domain name suffix support for Mobile VPN with IKEv2
- Routing engine update from Quagga to Free Range Routing (FRR)
- New configurable DNS Forwarding policy
- Support for intra-interface inspection on physical and link aggregation interfaces
- Updated user interface for endpoint enforcement
- Streamlined identification of spamBlocker false positives and false negatives
- Firebox feature key updates for WatchGuard Cloud support
- Updated WatchGuard IPSec Mobile VPN Client for Windows (64-bit) software:
  - Supports Windows 10 64-bit and Windows 11 64-bit (version 21H2)
  - Adds a new **DNS domains to be resolved in the tunnel** option to configure split DNS functionality

For a full list of the enhancements in this release, see *Enhancements and Resolved Issues* or review the What's New in Fireware v12.9 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 T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, M570, M590, M670, M690, M4600, M4800, M5600, M5800, FireboxV, Firebox NV5, or Firebox Cloud.
- The required hardware and software components as shown below. If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware OS installed on your Firebox and the version of WSM installed on your Management Server.
- Feature key for your Firebox — If you upgrade your device from an earlier version of Fireware OS, you can use your existing feature key. If you do not have a feature key for your device, you can log in to the WatchGuard website to download it.
- If you are upgrading to Fireware v12.x from Fireware v11.10.x or earlier, we strongly recommend you review the Fireware v11.12.4 release notes for important information about significant feature changes that occurred in the Fireware v11.12.x release cycle.
- Some Known Issues are especially important to be aware of before you upgrade, either to or from specific versions of Fireware. To learn more, see Release-specific upgrade notes.

Note that you can install and use WatchGuard System Manager v12.x and all WSM server components with devices running earlier versions of Fireware. In this case, we recommend that you use the product documentation that matches your Fireware OS version.

If you have a new Firebox, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. If this is a new FireboxV installation, make sure you carefully review Fireware Help in the WatchGuard Help Center for important installation and setup instructions. We also recommend that you review the Hardware Guide for your Firebox model. The *Hardware Guide* contains useful information about your device interfaces, as well as information on resetting your device to factory default settings, if necessary.

Product documentation for all WatchGuard products is available on the WatchGuard web site at https://www.watchguard.com/wgrd-help/documentation/overview.

# Enhancements and Resolved Issues

## Enhancements and Resolved Issues in Fireware v12.9 Update 1

- This release resolves a WatchGuard Cloud disconnection issue that occurred after a successful connection. *[FBX-24480, FCCM-5457]*
- This release resolves an issue where BOVPN tunnels failed to reconnect after a scheduled FireCluster reboot. *[FBX-21088]*
- 10GbE interfaces on the Firebox M690 no longer fail after a reboot or upgrade. *[FBX-23881]*
- This release resolves an *iked* crash. *[FBX-23907]*
- This release resolves a POP3 proxy error during Gateway AntiVirus scans. *[FBX-23922]*
- The backend service user now re-authenticates successfully after FireCluster members reboot. *[FBX-24409]*
- The Mobile VPN with SSL portal is now accessible from internal networks. *[FBX-24447]*
- HTTPS proxies now work with a Firebox configured in Bridge mode. *[FBX-24473]*
- Link detection settings in the XML configuration file are no longer enabled unexpectedly. *[FBX-24490]*
- This release resolves a Management Server scheduled software upgrade issue. *[FBX-24482]*

## Enhancements and Resolved Issues in Fireware v12.9

### General

- This release updates the feature key for WatchGuard Cloud support. *[FBX-24326]*
- In Fireware Web UI, the Blocked Sites page now uses pagination when there are more than 50 blocked sites. *[FBX-22596]*
- This release resolves an issue that sometimes caused the Blocked Sites list to add a site from the Block Sites Exception list. *[FBX-23979]*
- Fireware Web UI Traffic Monitor now displays the query_type parameter from the DNSproxy log type (1DFF-0006). *[FBX-23679]*
- The Firebox System Manager front panel and traffic log messages now show the correct time offset for the GMT -3:00 Brasilia time zone. *[FBX-20748]*
- This release resolves an issue that sometimes caused Access Portal users who use Microsoft Edge to see a 403 error page when they accessed OWA. *[FBX-20818]*
- The Firebox M290 now successfully boots when you insert the 8*1 Gbps Interface module (WG9022). *[FBX-23923]*
- This release resolves an issue that caused `Firewalld` to crash. *[FBX-23148]*
- This release resolves an issue that caused the wgagent to crash when you enable WatchGuard Cloud through the Fireware Web UI. *[FBX-22461]*
- WatchGuard System Manager can now show Sent and Received counts that exceed 2,147,483,647 bytes. *[FBX-6972]*
- You can now use a registry key to enable timeout adjustment for configuration reports in Management Server. This resolves an issue that caused reports to fail for devices with large configuration files. *[FBX-17882]*
- This release resolves an issue that caused unprintable characters to appear in diagnostic log messages when the diagnostic log level for Reputation Enabled Defense was set to Debug. *[FBX-23736]*

## Authentication

- You can now configure RADIUS servers and use multi-factor and RADIUS challenge/response authentication with the WatchGuard Management Server. *[FBX-22937]*
- When you configure LDAP authentication and enable LDAPS, you can now specify a client certificate. *[FBX-19999]*

## Proxies and Subscription Services

- You can now include a spamBlocker spam ID when you send a false positive or false negative spam report to WatchGuard. *[FBX-20701]*
- The Quick Setup Wizard now correctly enables Geolocation if the feature is included in the device feature key. *[FBX-17933]*
- Autotask tickets are now correctly created by Intrusion Prevention Service for detection from HTTPS proxy with Content Inspection. *[FBX-23913]*
- The example for the regular expression of a WebBlocker exception in Policy Manager now shows correct syntax. *[FBX-23803]*
- This release resolves an issue that caused FTP Proxy connections to fail. *[FBX-22165]*
- You can now apply Geolocation exceptions against a Firebox public IP address. *[FBX-23213]*
- You can now import and export WebBlocker exceptions when WatchGuard System Manager uses the Japanese language. *[FBX-23967]*
- This release resolves an issue that sometimes caused Access Portal and Reverse Proxy to fail with a 502 Bad Gateway error. *[FBX-23236]*
- This release resolves an issue that caused the SIP Proxy to incorrectly add a Record-Route IP address to the header, which prevented call completion. *[FBX- 23422]*

## FireCluster

- OSPF no longer advertises routes on networks after you enable an active/passive FireCluster. *[FBX-22383]*
- This release resolves an issue that caused the FireCluster diagnostic process to crash and created inconsistent FireCluster statistics in the Fireware Web UI and WatchGuard System Manager. *[FBX-23608]*

## Networking

- You can now enable or disable intra-interface inspection on physical and link aggregation interfaces. *[FBX-22161]*
- The Firebox now uses secondary DNS resolvers when it resolves host names specified in FQDN policy objects. *[FBX-22056]*
- Fireware now uses the Free Range Routing (FRR) routing engine, which replaces Quagga. *[FBX-22412*
- Secondary PPPoE IP addresses now remain active even when the PPPoE line is down. *[FBX-23578]*
- Conditional DNS forwarding now applies to DNS requests from the Access Portal. *[FBX-17253]*
- This release resolves an issue that caused the `sessiond` process on a FireCluster to crash. *[FBX-23985]*
- This release resolves an issue that prevented the backup master member diagnostics to show in the Fireware Web UI. *[FBX-23512]*
- Unknown LLC protocols now do not decrease available memory on the Firebox. *[FBX-23678]*
- This release resolves an issue where, in an SD-WAN setup, traffic from a routed BOVPN tunnel would route for the wrong interface. *[FBX-23207]*

### VPN

- This release updates the user interface for VPN endpoint enforcement. *[FBX-22956]*
- In the Mobile VPN with IKEv2 configuration on the Firebox, you can now configure split tunneling.*[FBX-13505]*
- When you authenticate with AuthPoint OTP, endpoint enforcement is now applied. *[FBX-22918]*
- BOVPN virtual interfaces that use IKEv2 now work correctly with modem failover. *[FBX-22904]*
- When you boot a Firebox without an External interface, the default gateway for a VIF route now correctly installs. *[FBX-22950]*
- The Mobile VPN with IKEv2 client configuration files for Windows, iOS, and macOS can now include a domain name suffix. *[FBX-13723]*
- This release resolves an issue that caused VIF traffic to fail on a remote Firebox where no reverse route existed. *[FBX-6919]*

## WatchGuard IPSec Mobile VPN Client for Windows (v15.11)

- This release of the IPSec Mobile VPN Client for Windows supports these operating system versions:
  - Windows 11, 64-bit (up to and including version 21H2)
  - Windows 10, 64-bit (up to and including version 21H2)
- This version of the NCP client invokes Microsoft Edge to log in to a hotspot. To use this feature, Windows must have WebView2 Runtime version 101.0.1210.39 or higher installed (https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section).
- For security reasons and compatibility with Windows, the directory structure of the WatchGuard Mobile VPN changes with this release. The new directory structure is created automatically and the configuration is transferred in the update process.
- You can now configure split DNS functionality with **DNS domains to be resolved in the tunnel**. If you configured split tunneling, the DNS requests of configured domains are sent into the VPN tunnel. All other DNS requests bypass the VPN tunnel.
- The user permissions and structure in the C:\ProgramData\WatchGuard\ directory are now limited:
  - Users can no longer store CA certificates in the directory.
  - No applications in the user and system context write to the same directory.
- This release resolves an issue that caused the Windows login to not work when you selected the **Automatic Windows Logon with Configured Credentials** option or used multi-factor authentication with a time-based one-time password (TOTP).
- This release resolves an issue that caused the cached VPN user name to sometimes not show correctly in the log in dialog box.
- This release resolves an issue where, when you change from a certificate-based profile with a successful PIN entry to a profile with shared key, the entered PIN does not delete and the PIN icon is not removed.
- This release resolves an issue where, when you switch profiles from a certificate-based profile with *.p12 file to a profile with SmartCard reader, a PKI error shows.
- The zlib version used in the VPN client is raised to 1.2.12. This closes the zlib security vulnerability [CVE-2018-25032].
- This release resolves the vulnerabilities [CVE-2022-0778] and [CVE-2020-1971] in OpenSSL.
- TLS versions 1.0 and 1.1 are no longer supported with this client release.
- The cURL version used in the VPN client is upgraded to 7.84.0. This closes the cURL vulnerabilities [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207], and [CVE-2022-32208].

- This release resolves an issue that caused a profile with multi-factor authentication to incorrectly show a smart card icon and indicate that the smart card was not initialized correctly.
- This release resolves an issue that occurred after you change DNS entries in the VPN Bypass configuration.
- This release resolves an issue where, when you selected the **Icon in System Tray** autostart option, the hotspot log in would not call correctly.
- This release resolves an issue where, when you use the CertificateStore CSP, a PIN sometimes incorrectly prompted. The PIN query option in the CertificateStore CSP is also removed in the client plug-in.
- This release updates the **Connect Before Windows Logon** function to prevent privilege escalation. You can now only select batch files created by the administrator in the C:\ProgramData\WatchGuard\Mobile VPN\scripts\ directory.
- This release resolves an issue that caused the network connection to permanently disconnect after client installation.
- You can now import an exported profile into a client.
- This release improves **.INI** file imports.

# Known Issues and Limitations

Known issues for Fireware v12.9 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.

# 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:

`WSM_12_9.exe` — Use this file to install WSM v12.9 or to upgrade WatchGuard System Manager from an earlier version.

## Fireware OS

You can upgrade the Fireware OS on your Firebox automatically from the Fireware Web UI **System > Upgrade OS** page or from WatchGuard Cloud.

If you prefer to upgrade from Policy Manager, or from an earlier version of Fireware, you can download the Fireware OS image for your Firebox. Use the .exe file if you want to install or upgrade the OS using WSM. Use the .zip file if you want to install or upgrade the OS manually using Fireware Web UI. Use the .ova or .vhd file to deploy a new FireboxV device.

The file name for software downloads always includes the product group, such as T20_T40 for the Firebox T20 or T40.

| If you have… | Select from these Fireware OS packages |
|---|---|
| Firebox M270/M370/M470/M570/M670 | `Firebox_OS_M270_M370_M470_M570_M670_12_9_U1.exe`<br>`firebox_M270_M370_M470_M570_M670_12_9_U1.zip` |
| Firebox M290 | `Firebox_OS_M290_12_9_U1.exe`<br>`firebox_M290_12_9_U1.zip` |
| Firebox M390 | `Firebox_OS_M390_12_9_U1.exe`<br>`firebox_M390_12_9_U1.zip` |
| Firebox M400/M500 | `Firebox_OS_M400_M500_12_9_U1.exe`<br>`firebox_M400_M500_12_9_U1.zip` |
| Firebox M440 | `Firebox_OS_M440_12_9_U1.exe`<br>`firebox_M440_12_9_U1.zip` |
| Firebox M590/M690 | `Firebox_OS_M590_M690_12_9_U1.exe`<br>`firebox_MM590_M690_12_9_U1.zip` |
| Firebox M4600/M5600 | `Firebox_OS_M4600_M5600_12_9_U1.exe`<br>`firebox_M4600_M5600_12_9_U1.zip` |
| Firebox M4800/M5800 | `Firebox_OS_M4800_M5800_12_9_U1.exe`<br>`firebox_M4800_M5800_12_9_U1.zip` |

| If you have… | Select from these Fireware OS packages |
|---|---|
| Firebox T20/T40 | `Firebox_OS_T20_T40_12_9_U1.exe`<br>`firebox_OS_T20_T40_12_9_U1.zip` |
| Firebox T55 | `Firebox_OS_T55_12_9_U1.exe`<br>`firebox_T55_12_9_U1.zip` |
| Firebox T70 | `Firebox_OS_T70_12_9_U1.exe`<br>`firebox_T70_12_9_U1.zip` |
| Firebox T80 | `Firebox_OS_T80_12_9_U1.exe`<br>`firebox_OS_T80_12_9_U1.zip` |
| FireboxV<br>All editions for VMware | `FireboxV_12_9_U1.ova`<br>`Firebox_OS_FireboxV_12_9_U1.exe`<br>`firebox_FireboxV_12_9_U1.zip` |
| FireboxV<br>All editions for Hyper-V | `FireboxV_12_9_U1.vhd.zip`<br>`Firebox_OS_FireboxV_12_9_U1.exe`<br>`firebox_FireboxV_12_9_U1.zip` |
| Firebox NV5 | `Firebox_OS_NV5_12_9_U1.exe`<br>`firebox_NV5_12_9_U1.zip` |
| Firebox Cloud | `Firebox_OS_FireboxCloud_12_9_U1.exe`<br>`fireboxCloud_12_9_U1.zip` |

## Additional Firebox Software

The files in the list below are not directly used by the Firebox or for Firebox management, but are necessary for key features to work. In most cases, the file name includes the Fireware version that was current at the time of release.

| File name | Description | Updated in this release |
|---|---|---|
| WG-Authentication-Gateway_12_7_2.exe | Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO | No |
| WG-Authentication-Client_12_7.msi | Single Sign-On Client software for Windows | No |
| WG-SSOCLIENT-MAC_12_5_4.dmg | Single Sign-On Client software for macOS | No |
| SSOExchangeMonitor_x86_12_0.exe | Exchange Monitor for 32-bit operating systems | No |
| SSOExchangeMonitor_x64_12_0.exe | Exchange Monitor for 64-bit operating systems | No |
| TO_AGENT_SETUP_11_12.exe | Terminal Services software for both 32-bit and 64-bit systems. | No |

| File name | Description | Updated in this release |
|---|---|---|
| WG-MVPN-SSL_12_7_2.exe | Mobile VPN with SSL client for Windows[5] | No |
| WG-MVPN-SSL_12_7_2.dmg | Mobile VPN with SSL client for macOS[5] | No |
| **WG-Mobile-VPN_Windows_x86-64_1511_29631.exe[1]** | **WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP [2]** | **Yes** |
| WG-Mobile-VPN_macOS_x86-64_461_29053.dmg[1] | WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP [2] | No |
| Watchguard_MVLS_Win_x86-64_200_rev19725.exe[1] | WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP [3] | No |

*[1] The version number in this file name does not match any Fireware version number.*

*[2] There is a license required for this premium client, with a 30-day free trial available with download.*

*[3] Click here for more information about MVLS. If you have a VPN bundle ID for macOS, it must be updated on the license server to support the macOS 3.00 or higher client. To update your bundle ID, contact WatchGuard Customer Support. Make sure to have your existing bundle ID available to expedite the update.*

*[4] SSO Agent v12.7 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.7, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.7, we recommend that you upgrade all SSO Clients to v12.7. You cannot use SSO Client v12.7 with versions of the SSO Agent lower than v12.5.4. Fireware v12.7.2 supports previous versions of the SSO Agent.*

*[5] Not supported on ARM processor architecture.*

# Upgrade to Fireware v12.9 Update 1

Important information about the upgrade process:

- You can use WatchGuard Cloud, Fireware Web UI, or Policy Manager to upgrade your Firebox.
- We strongly recommend that you save a local copy of your Firebox configuration and create a Firebox backup image before you upgrade.
- If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware OS installed on your Firebox and the version of WSM installed on your Management Server. Also, make sure to upgrade WSM *before* you upgrade the version of Fireware OS on your Firebox.
- In Fireware v12.6.2 or higher, Fireware Web UI prevents the addition of users with reserved user names to the Firebox-DB authentication server. We recommend that you delete or replace any user with a reserved name before you upgrade to Fireware v12.6.2 or higher. For more information, see Reserved Firebox-DB authentication server user names.
- In Fireware v12.7 or higher, you cannot name new authentication servers *AuthPoint*. If you have an existing authentication server called *AuthPoint*, it will be automatically renamed to *AuthPoint.1* when you upgrade your Firebox to Fireware v12.7 or higher, or when you use WSM v12.7 or higher to manage a Firebox that runs Fireware 12.6.x or lower.

## Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous server or client software when you upgrade to WSM v12.x. You can install the v12.x server and client software on top of your existing installation to upgrade your WatchGuard software components. We do, however, strongly recommend that you back up your WatchGuard Servers (for example, your WatchGuard Management Server) to a safe location before you upgrade. You will need these backup files if you ever want to downgrade.

For instructions on how to back up your Management Server configuration, see Fireware Help.

## Upgrade to Fireware v12.9 Update 1 from WatchGuard Cloud

From WatchGuard Cloud, you can upgrade the firmware for a Firebox that runs Fireware v12.5.2 or higher. To upgrade from WatchGuard Cloud, see Upgrade Firmware from WatchGuard Cloud in *WatchGuard Cloud Help*.

## Upgrade to Fireware v12.9 Update 1 from Fireware Web UI

You can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. To upgrade manually, see Upgrade Fireware OS or WatchGuard System Manager in *Fireware Help*.

If your Firebox runs Fireware v11.9.x or lower, follow the steps in this knowledge base article.

If you have installed another release of this OS version on your computer, you must run the installer twice (once to remove the previous release and again to install this release).

## Upgrade to Fireware v12.9 Update 1 from WSM/Policy Manager

To upgrade from WSM/Policy Manager, see Upgrade Fireware OS or WatchGuard System Manager in *Fireware Help*.

If you have installed another release of this OS version on your computer, you must run the installer twice (once to remove the previous release and again to install this release).

If you like to make updates to your Firebox configuration from a saved configuration file, make sure you open the configuration from the Firebox and save it to a new file after you upgrade. This is to make sure that you do not overwrite any configuration changes that were made as part of the upgrade.

# Update Access Points

All access point (AP) firmware is managed by the Gateway Wireless Controller on your Firebox. The Gateway Wireless Controller automatically checks for new AP firmware updates and enables you to download the firmware directly from WatchGuard servers.

The AP firmware versions available to download from the Firebox are:

- AP120, AP320, AP322: 8.8.3-12 and higher
- AP125, AP225W, AP325, AP327X, AP420: 10.0.0-124 and higher

These are the minimum versions required for Fireboxes that support system integrity checks introduced in Fireware v12.7.2 Update 2 and higher.

## AP Firmware Upgrade

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

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

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

To manually update firmware on your APs:

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

## About AP Firmware and Fireware Versions

You must upgrade your APs to firmware version 8.6.0 or higher before you upgrade to Fireware v12.5.4 or higher to remain compatible with the latest versions of Fireware.

## Important Steps for Upgrades from Fireware v12.0 or Lower

If you have not previously upgraded to Fireware v12.0.1 or higher and the latest AP firmware, you must perform these steps:

1. Make sure all your APs are online. You can check AP status from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.
2. Make sure you are not using insecure default AP passphrases such as **wgwap** or **watchguard**. Your current AP passphrase must be secure and at least 8 characters in length. You can change your AP passphrase in **Network > Gateway Wireless Controller > Settings**.

If you do not have a secure passphrase correctly configured before the upgrade, you will lose the management connection with your deployed APs. If this occurs, you must physically reset the APs to factory default settings before you can manage the APs from Gateway Wireless Controller.

Depending on the version of Fireware you upgrade from, you may need to mark APs as trusted after the upgrade to Fireware v12.0.1 or higher. You can mark APs as trusted from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.

# Upgrade a FireCluster to Fireware v12.9 Update 1

You can upgrade Fireware OS for a FireCluster from Policy Manager or Fireware Web UI. To upgrade a FireCluster from Fireware v11.10.x or lower, we recommend you use Policy Manager.

As part of the upgrade process, each cluster member reboots and rejoins the cluster. Because the cluster cannot do load balancing while a cluster member reboot is in progress, we recommend you upgrade an active/active cluster at a time when the network traffic is lightest.

For information on how to upgrade your FireCluster, see this Help topic.

# Fireware v12.9 Update 1 Operating System Compatibility Matrix

*Last reviewed: 18 January 2023*

| WSM/ Fireware Component | Microsoft Windows 10, 11 | Microsoft Windows Server 2019 & 2022 | macOS v10.14, v10.15, v11, v12, & v13 | Android 7, 8, 9, 10, 11, 12, & 13 | iOS v9, v10, v11, v12, v13, v14, v15, & v16 |
|---|---|---|---|---|---|
| **WatchGuard System Manager** | ✓ | ✓ | | | |
| **WatchGuard Servers** *For information on WatchGuard Dimension, see the Dimension Release Notes.* | ✓ | ✓ | | | |
| **Single Sign-On Agent (Includes Event Log Monitor)** | | ✓ | | | |
| **Single Sign-On Client** | ✓ | ✓ | ✓[2] | | |
| **Single Sign-On Exchange Monitor** | | ✓ | | | |
| **Terminal Services Agent**[1] | | ✓ | | | |
| **Mobile VPN with IPSec** | ✓ | | ✓[2,3,8] | ✓ | ✓[3] |
| **Mobile VPN with SSL** | ✓ | | ✓[2,6,9] | ✓[4] | ✓[4] |
| **Mobile VPN with IKEv2** | ✓ | | ✓[2,7] | ✓[5] | ✓ |
| **Mobile VPN with L2TP** | ✓ | | ✓[3] | ✓[10] | ✓ |

*Note about Microsoft Windows support:*

- *Documentation might include references and examples for Windows OS versions that are no longer supported. This is provided to assist users with those OS versions, but we cannot guarantee compatibility.*

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

- *Microsoft Edge108*
- *Firefox v107*
- *Safari 16 (macOS)*
- *Chrome v108*

*[1]Terminal Services support with manual or Single Sign-On authentication operates in a Microsoft Terminal Services or Citrix XenApp 6.0, 6.5, 7.6, or 7.12 environment.*

*[2]To learn more about client support for different macOS versions, see the macOS software compatibility KB articles for macOS Catalina 10.15, macOS Big Sur 11, macOS Monterey 12, and macOS Ventura 13.*

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

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

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

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

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

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

*[9] macOS 13 (Ventura) does not accept SSL connections to untrusted self-signed certificates. For more information, see this KB article.*

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

## Authentication Support

This table provides a quick view of the types of authentication servers supported by key features of Fireware. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your Firebox or XTM device configuration. With each type of third-party authentication server supported, you can specify a backup server IP address for failover.

✓ *Fully supported by WatchGuard*

– *Not supported by WatchGuard*

| | AuthPoint Authentication Server | AuthPoint RADIUS Server | Active Directory | LDAP | RADIUS | SecurID | Firebox (Firebox-DB) Local Authentication | SAML |
|---|---|---|---|---|---|---|---|---|
| Mobile VPN with IPSec for iOS, Windows, and macOS | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – |
| Mobile VPN with IPSec for Android | – | ✓ | ✓ | ✓ | ✓ | – | ✓ | – |
| Mobile VPN with SSL | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – |
| Mobile VPN with IKEv2 for Windows | ✓ | ✓ | ✓[1] | – | ✓ | – | ✓ | – |
| Mobile VPN with L2TP | – | ✓ | ✓[1] | – | ✓ | – | ✓ | – |

| | AuthPoint Authentication Server | AuthPoint RADIUS Server | Active Directory | LDAP | RADIUS | SecurID | Firebox (Firebox-DB) Local Authentication | SAML |
|---|---|---|---|---|---|---|---|---|
| Built-in Web Page on Port 4100 and 8080 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – |
| Access Portal | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AD Single Sign-On Support *(with or without client software)* | – | – | ✓ | ✓ | – | – | – | – |
| Terminal Services Manual Authentication | – | – | ✓ | ✓ | ✓ | ✓ | ✓ | – |
| Terminal Services Authentication with Single Sign-On | – | – | ✓ | – | – | – | – | – |

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

## System Requirements

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

## FireboxV System Requirements

A WatchGuard FireboxV virtual machine can run on:

- VMware ESXi 6.5, 6.7, or 7.0
- Hyper-V for Microsoft Windows Server 2019 or 2022, and Hyper-V Server 2019
- KVM in CentOS 8.1

The hardware requirements for FireboxV are the same as for the hypervisor environment it runs in.

Each FireboxV virtual machine requires 5 GB of disk space. CPU and memory requirements vary by model:

| FireboxV Model | Minimum Total Memory | Recommended Memory | Maximum vCPUs |
|---|---|---|---|
| Small | 2048 MB[1] | 4096 MB | 2 |
| Medium | 4096 MB | 4096 MB | 4 |
| Large | 4096 MB | 8192 MB | 8 |
| Extra Large | 4096 MB | 16384 MB | 16 |

*[1] 4096 MB is required to enable Access Portal and IntelligentAV, and to use the Full signature set for IPS/Application Control.*

## Firebox Cloud System Requirements

Firebox Cloud can run on Amazon Web Services (AWS) and Microsoft Azure cloud computing platforms.

Firebox Cloud CPU and memory requirements:

- Minimum CPU cores: 2
- Minimum total memory: 2048 MB[1]
- Recommended minimum total memory: 4096 MB

*[1] 4096 MB is required to enable Access Portal and IntelligentAV, and to use the Full signature set for IPS/Application Control.*

WatchGuard recommends an instance that has at least 1024 MB of memory for each CPU core. For example, if the instance has four CPU cores, we recommend a minimum total memory of 4096 MB. Refer to the AWS and Azure documentation to identify instances that meet these requirements.

For Firebox Cloud with a BYOL license, the Firebox Cloud model determines the maximum number of CPU cores. For more information, see Firebox Cloud License Options in Help Center.

For a BYOL license, Azure automatically selects an instance size based on the License Type you select. For more information, see the Firebox Cloud Deployment Guide.

# Downgrade Instructions

You cannot downgrade a Firebox T20, T40, T55, T70, T80, M270, M290, M370, M390, M400, M440, M470, M500, M570, M590, M670, M690, M4600, M4800, M5600, or M5800 to a version of Fireware lower than Fireware v12.7.2 Update 2.

## Downgrade from WSM v12.9

If you want to downgrade from WSM v12.9 to a lower version, you must uninstall WSM v12.9. 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 v12.9.

Next, install the same version of WSM that you used before you upgraded to WSM v12.9. 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 v12.9. Verify that all WatchGuard servers are running.

## Downgrade from Fireware v12.9 Update 1

If you want to downgrade from Fireware v12.9 Update 1 to a lower version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.9 Update 1. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.9 Update 1 to complete the downgrade.
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device.

If you need to downgrade a Firebox without a backup file after you complete the upgrade to Fireware v12.x, we recommend you Use the Web UI to Downgrade Fireware. This process deletes the configuration file, but does not remove the device feature keys and certificates. After you downgrade the Firebox, you can use Policy Manager to Save the Configuration File to the Firebox.

If you use the Fireware Web UI or CLI to downgrade to an earlier version, the downgrade process resets the network and security settings on your device to their factory-default settings. The downgrade process does not change the device passphrases and does not remove the feature keys and certificates.

See *Fireware Help* for more information about these downgrade procedures, and information about how to downgrade if you do not have a backup image.

## Downgrade Restrictions

See this Knowledge Base article for a list of downgrade restrictions.

When you downgrade the Fireware OS on your Firebox, the firmware on any paired AP devices is not automatically downgraded. We recommend that you reset the AP device to its factory-default settings to make sure that it can be managed by the older version of Fireware OS.

# Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal at https://www.watchguard.com/wgrd-support/overview. When you contact Technical Support, you must supply your registered Product Serial Number or Partner ID.

| | Phone Number |
|---|---|
| U.S. End Users | 877.232.3531 |
| International End Users | +1 206.613.0456 |
| Authorized WatchGuard Resellers | 206.521.8375 |

# Localization

This release includes updates to the localization for the management user interfaces (WSM application suite and Web UI) through Fireware v12.6.4. UI changes introduced since v12.6.4 might remain in English. Supported languages are:

- French (France)
- Japanese
- Spanish (Latin American)

Note that most data input must still be made using standard ASCII characters. You can use non-ASCII characters in some areas of the UI, including:

- Proxy deny message
- Wireless hotspot title, terms and conditions, and message
- WatchGuard Server Center users, groups, and role names

Although some other Web UI and Policy Manager fields might accept Unicode characters, problems can occur if you enter non-ASCII characters in those fields.

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the Fireware Web UI System Status menu and any software components provided by third-party companies remain in English.

## Fireware Web UI

The Web UI will launch in the language you set in your web browser by default.

## WatchGuard System Manager

When you install WSM, you can choose which language packs you want to install. The language displayed in WSM will match the language you select in your Microsoft Windows environment. For example, if you use Windows 10 and want to use WSM in Japanese, go to Control Panel > Language and select Japanese as your Display Language.

## Dimension, WebCenter, Quarantine Web UI, and Wireless Hotspot

These web pages automatically display in whatever language preference you set in your web browser.

## Documentation

The latest version of localized Fireware Help is available from WatchGuard Help Center. In the top-right of a Fireware Help page, click the Globe icon and select your language from the drop-down list.