



Fireware v12.6.1 Update 1 Release Notes

Supported Devices	Firebox T20/T20-W, T40/T40-W, T80
Release Date	Fireware v12.6.1: 2 June 2020 WSM 12.6.2 Update 2: 25 September 2020
Release Notes Revision	5 May 2021
Fireware OS Build	621842
WatchGuard System Manager v12.6.2 Update 2 Build	630401
WatchGuard AP Firmware	AP120, AP320, AP322: 8.8.3-12 AP125, AP225W, AP325, AP327X, AP420: 8.9.0-63



On 18 September 2020, we removed the Fireware v12.6.2 release from the Software Downloads Center. On 25 September 2020, we released WSM 12.6.2 Update 2 to enable customers to downgrade from Fireware v12.6.2 to Fireware v12.6.1.

Introduction

With the release of Fireware v12.6.1 Update 1, we're happy to announce three new Fireware models: Firebox T20, T40, and T80. These latest Firebox models provide an upgrade path for our existing Firebox T Series customers and offer faster processors and more memory. The Firebox T40 and T80 support PoE+ (Power over Ethernet) that you can use to power peripheral devices, such as wireless access points. The Firebox T20 and T40 models are available in both wired and wireless models; the wireless models include support for the fast 802.11ac wireless standard.

Features by Model

	Ports	IntelligentAV Support	Access Portal Support	PoE+	Wi-Fi Option	Enclosure Type	Expansion Model
Firebox T20	5	No	No	0	T20-W	Metal base, plastic top	No
Firebox T40	5	Yes	Yes	1	T40-W	Metal base, plastic top	No
Firebox T80	5	Yes	Yes	2	No	Metal	1 SFP+

These new Fireboxes were manufactured with Fireware v12.6.1. We recommend that you upgrade your Firebox to Fireware v12.6.1 Update 1 immediately to take advantage of important bug fixes included in this update release. See the *Enhancements and Resolved Issues in WSM and Fireware v12.6.1 Update 1* section for more information about these fixes.

We're also excited to let you know about the new features and functionality included in Fireware v12.6.1. Most of these new features will be available in Fireware 12.5.4 for other Firebox models, and include:

TDR Host Sensor Enforcement for Mobile VPN

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

VPN Feature Enhancements

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

spamBlocker Engine Update

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

Application Control/IPS Engine Update

Application Control and Intrusion Prevention Service (IPS) now use an updated engine and signature set that offer improved performance.

Networking Enhancements

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

Other Enhancements

- Gateway Wireless Controller updates to support the AP225W access point
- RADIUS server failover improvements
- Support for a new Microsoft API for communication with SSO Event Log Monitor
- Firebox Configuration Report updates

For a full list of the enhancements in this release, see *Enhancements and Resolved Issues in WSM and Fireware v12.6.1 Update 1* or review the [What's New in Fireware v12.6.1 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, T20-W, T40, T40-W, or T80. You cannot install Fireware v12.6.1 on any other Firebox model.
- The required hardware and software components as shown below. If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware OS installed on your Firebox and the version of WSM installed on your Management Server.
- Feature key for your Firebox — If you upgrade your device from an earlier version of Fireware OS, you can use your existing feature key. If you do not have a feature key for your device, you can log in to the WatchGuard website to download it.
- 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. We also recommend that you review the [Hardware Guide](#) for your Firebox model. The *Hardware Guide* contains useful information about your device interfaces, as well as information on resetting your device to factory default settings, if necessary.

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

Enhancements and Resolved Issues in WSM and Fireware v12.6.1 Update 1

- VPN connections are no longer disrupted during normal IKE rekey operations. [FBX-19406]
- For SSL VPN connections to the Firebox, the minimum accepted TLS version is now TLS 1.2. [FBX-19462]
- This release adds a Command Line Interface option to disable the Mobile VPN with SSL Client Download page hosted by the Firebox. [FBX-135]
- This release includes an updated installation script for Mobile VPN with IKEv2. The script no longer fails when Windows Group Policy Objects specify digital signature restrictions for PowerShell scripts. [FBX-19598]
- Several potential backup failure scenarios are resolved. [FBX-19089, FBX-19564]
- Authentication for an account in multiple groups now works correctly. [FBX-19402]
- All virtual IP addresses are now correctly used with Mobile VPN. [FBX-19320]
- This release includes several improvements in proxy performance. [FBX-17497, FBX-19314]
- An issue that caused an RDP connection freeze is resolved. [FBX-19200]
- Several issues related to logging and error message displays are resolved. [FBX-19154, FBX-19242]
- Feature keys now include a separate entry for Cloud Visibility. [FBX-19444]
- The timeout to establish an IKEv2 connection is now configurable through the CLI. [FBX-19386]
- The time taken to delete multiple entries from the Blocked Sites list has been reduced. [FBX-18965]

Enhancements and Resolved Issues in Fireware v12.6.1

General

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

Authentication

- In RADIUS Server Settings, the default Dead Time value is now 10 minutes. The new default setting only applies to new configurations. [\[FBX-4448\]](#)
- Event Log Monitor now supports the Microsoft Windows Event Log API. [\[FBX-16551\]](#)
- You can now successfully save your configuration from Fireware Web UI after you disable the secondary RADIUS server settings. [\[FBX-5152\]](#)



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

You cannot use SSO Client v12.5.4 with versions of the SSO Agent lower than v12.5.4. Fireware v12.6.1 supports previous versions of the SSO Agent.

Networking

- The Firebox now supports dynamic DNS through Cloudflare. [\[FBX-17815\]](#)
- The default multi-WAN method is now Failover. The new default method only applies to new configurations. [\[FBX-17226\]](#)
- In SD-WAN Metrics Settings, the default value for Latency is now 400ms and the default value for Jitter is now 100ms. The new default settings only apply to new configurations. [\[FBX-16815\]](#)
- A problem has been resolved that caused many `network_v` debug messages to appear in the log file. [\[FBX-18134\]](#)
- This release resolves a `networkd` process crash. [\[FBX-18065\]](#)
- Wireless clients can now obtain DHCP IP address information after a Rogue AP scan is completed on Firebox Wireless devices. [\[FBX-15530\]](#)
- Fireware Web UI now correctly displays DHCP lease information. [\[FBX-16566\]](#)
- The tabletop Firebox Wireless `hostapd` process now better handles process shutdown and recovery. [\[FBX-17298\]](#)
- This release resolves an issue with the default route for some external interfaces with a /31 subnet mask. [\[FBX-18050\]](#)
- This release resolves a crash in the DHCPv6 process. [\[FBX-18694\]](#)

Proxies and Security Services

- spamBlocker now uses a new engine that improves performance. [\[FBX-17268\]](#)
- Application Control and Intrusion Prevention Service now use an updated engine and signature set. [\[FBX-7035\]](#)
- APT Blocker now correctly scans HWP and ISO files. [\[FBX-17493, FBX-13133\]](#)
- The Firebox Configuration Report now includes spamBlocker settings and exceptions for SMTP proxy actions, and WebBlocker exceptions for WebBlocker actions. [\[FBX-15911, FBX-15914\]](#)
- The WebBlocker Server Timeout setting has been updated with a new default range of 15-600 seconds. This change applies after you save a configuration to your device from WSM v12.6.1. [\[FBX-16536\]](#)
- In Policy Manager, in the Policy Properties dialog box, the SD-WAN Action drop-down list now shows the full name of SD-WAN actions. [\[FBX-15219\]](#)

VPN

- This release adds TDR Host Sensor Enforcement for mobile VPN connections from hosts to the Firebox. *[FBX-17530, FBX-17532]*
- This release adds an option to specify a custom maximum transmission unit (MTU) for BOVPN virtual interfaces. *[FBX-15920]*
- BOVPN and BOVPN virtual interface configurations now support hex-based pre-shared keys. *[FBX-16247]*

Enhancements and Resolved Issues in AP Firmware Update 8.9.0-63

- Added support for AP325 revision B hardware with improved antenna design.



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

Enhancements and Resolved Issues in AP Firmware Update 8.8.3-12

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

Known Issues and Limitations

Known issues for Fireware v12.6.1 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_6_2_U2.exe — Use this file to install WSM v12.6.2 Update 2 or to upgrade WatchGuard System Manager from an earlier version.

Fireware OS

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

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



The file name for software downloads will always include the product group, such as T30-T50 for the Firebox T30 or T50.

If you have...	Select from these Fireware OS packages
Firebox T20/T40	Firebox_OS_T20_T40_12_6_1_U1.exe Firebox_OS_T20_T40_12_6_1_U1.zip
Firebox T80	Firebox_OS_T80_12_6_1_U1.exe Firebox_OS_T80_12_6_1_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.

Filename	Description	Updated in this release
WG-Authentication-Gateway_12_5_4.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO	Yes
WG-Authentication-Client_12_5_4.msi	Single Sign-On Client software for Windows	Yes
WG-SSOCLIENT-MAC_12_5_4.dmg	Single Sign-On Client software for macOS	Yes
SSOExchangeMonitor_x86_12_0.exe	Exchange Monitor for 32-bit operating systems	No
SSOExchangeMonitor_x64_12_0.exe	Exchange Monitor for 64-bit operating systems	No
TO_AGENT_SETUP_11_12.exe	Terminal Services software for both 32-bit and 64-bit systems.	No
WG-MVPN-SSL_12_5_3.exe	Mobile VPN with SSL client for Windows	No
WG-MVPN-SSL_12_5_3.dmg	Mobile VPN with SSL client for macOS	No
WG-Mobile-VPN_Windows_x86_1400_45109.exe ¹	WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP ²	No
WG-Mobile-VPN_Windows_x86-64_1400_45109.exe ¹	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP ²	No
WG-Mobile-VPN_macOS_x86-64_400_46079.dmg ¹	WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP ²	No
Watchguard_MVLS_Win_x86-64_200_rev19725.exe ¹	WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP ³	No

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

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

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

⁴ *SSO Agent v12.5.4 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.5.4, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.5.4, we recommend that you upgrade all SSO Clients to v12.5.4. You cannot use SSO Client v12.5.4 with versions of the SSO Agent lower than v12.5.4. Fireware v12.6.1 supports previous versions of the SSO Agent.*

Upgrade to Fireware v12.6.1 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.

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 v12.6.1 Update 1 from WatchGuard Cloud

From WatchGuard Cloud, you can upgrade the firmware for a Firebox. To upgrade from WatchGuard Cloud, see [Upgrade Firmware from WatchGuard Cloud](#) in *WatchGuard Cloud Help*.

Upgrade to Fireware v12.6.1 Update 1 from 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 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 v12.6.1 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 AP firmware is managed by the Gateway Wireless Controller on your Firebox. The Gateway Wireless Controller automatically checks for new AP firmware updates and enables you to download the firmware directly from WatchGuard servers.

AP Firmware Upgrade

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

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

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

To manually update firmware on your APs:

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

About AP Firmware and Fireware Versions

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

Important Steps for Upgrades from Fireware 12.0 or Lower

If you have not previously upgraded to Fireware 12.0.1 or higher and the latest AP firmware, you must perform these steps:

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



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

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

Upgrade your FireCluster to Fireware v12.6.1 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](#).

Fireware 12.6.1 Operating System Compatibility Matrix

Last revised 2 June 2020

WSM/ Fireware Component	Microsoft Windows 8.1, 10	Microsoft Windows Server 2012 & 2012 R2	Microsoft Windows Server 2016 & 2019	macOS v10.13, v10.14, & v10.15	Android 7.x, 8.x, 9.x, & 10.x	iOS v9, v10, v11, v12, & v13
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers <i>For information on WatchGuard Dimension, see the Dimension Release Notes.</i>	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)¹		✓	✓			
Single Sign-On Client	✓	✓	✓	✓ ⁴		
Single Sign-On Exchange Monitor²		✓	✓			
Terminal Services Agent³		✓	✓			
Mobile VPN with IPsec	✓			✓ ^{4,5}	✓ ⁵	✓ ⁵
Mobile VPN with SSL	✓			✓ ⁴	✓ ⁶	✓ ⁶
Mobile VPN with IKEv2	✓			✓ ⁴	✓ ⁷	✓
Mobile VPN with L2TP	✓			✓ ⁵	✓	✓

Notes about Microsoft Windows support:

- Windows 8.x support does not include Windows RT.
- Documentation might include references and examples for Windows OS versions that are no longer supported. This is provided to assist users with those OS versions, but we cannot guarantee compatibility.

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

- IE 11
- Microsoft Edge⁴
- Firefox v66
- Safari 12

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

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

²Microsoft 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.

³Terminal 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.

⁴On 11 November 2019, WatchGuard released multiple new client applications for macOS. These releases add support for macOS Catalina 10.15, and require macOS High Sierra 10.13 or later. To learn more, see [macOS Catalina 10.15 software compatibility](#).

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

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

⁷StrongSwan is supported for all recent versions of Android.

Authentication Support

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

 Fully supported by WatchGuard - Not supported by WatchGuard

	AuthPoint	Active Directory	LDAP	RADIUS	SecurID	Firebox (Firebox-DB) Local Authentication	SAML
Mobile VPN with IPsec for iOS, Windows, and macOS	✓	✓	✓	✓	✓	✓	–
Mobile VPN with IPsec for Android	✓	✓	✓	✓	–	✓	–
Mobile VPN with SSL	✓	✓	✓	✓	✓	✓	–
Mobile VPN with IKEv2 for Windows	✓	✓ ¹	–	✓	–	✓	–
Mobile VPN with L2TP	✓	✓ ¹	–	✓	–	✓	–
Built-in Web Page on Port 4100 and 8080	✓	✓	✓	✓	✓	✓	–
Access Portal	✓	✓	✓	✓	✓	✓	✓
AD Single Sign-On Support (<i>with or without client software</i>)	–	✓	✓	–	–	–	–
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

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.

