



Fireware v2026.4 Release Notes

Supported Devices	Firebox T115-W, T125, T145, T175, T185, M295, M395, M495, M595, M695, M4850, M5850, M6850
Release Date	27 October 2026
Release Notes Revision	27 October 2026
Fireware OS Build	750021
WatchGuard System Manager Build	750197

Introduction

Fireware v2026.4 includes several significant enhancements to Fireware, as well as important security fixes for Fireboxes.

Features in this release include:

BOVPN over WireGuard

You can configure a WireGuard branch office VPN (BOVPN) tunnel between Fireboxes that run Fireware v2026.4. WireGuard uses public key authentication and a configurable UDP listening port.

Let's Encrypt Integration

Enables native issuance and automatic renewal of trusted Let's Encrypt SSL/TLS certificates for cloud-managed Fireboxes in WatchGuard Cloud. This eliminates manual certificate renewal workflows and helps prevent service interruptions from expired certificates.

IPv6 Support for Mobile VPN with IKEv2

Mobile VPN with IKEv2 configurations can use IPv6 for tunnel and related network settings.

Custom Dynamic Alias Support

Adds support for custom dynamic aliases that periodically retrieve IP address and domain entries from an externally hosted feed file.

Network Management Firebox Collector

Adds an embedded Network Management agent on supported Fireboxes to automate and send local asset discovery and telemetry collection (SNMP, WMI, SSH) directly into WatchGuard Cloud (in support of the upcoming Network Management release).

Support for FireCloud/Network as a Resource

Enables Fireboxes to define local networks as FireCloud resources, providing remote users with high-performance, WireGuard-powered mobile VPN access (in support of the upcoming FireCloud Network as a Resource release).

DNS Proxy Connection Idle Timeout

In the DNS-proxy general settings, you can set the connection idle timeout. This setting specifies how long the Firebox keeps an idle DNS proxy connection open before it closes the session.

Default RDP Policy Includes UDP 3389

The default RDP policy now includes TCP port 3389 and UDP port 3389. The Fireware v2026.4 update adds UDP port 3389 and supports Microsoft Remote Desktop clients that use UDP to improve session performance and responsiveness.

For a full list of the resolved issues and enhancements in this release, go to [Enhancements and Resolved Issues](#).

Resolved Issues and Enhancements in Fireware v2026.4

Security Issues

- This release resolves an improper authentication issue in AuthPoint MFA verification (CVE-2026-82332). Read the full advisory on psirt.watchguard.com.
- This release resolves an authenticated stack-based buffer overflow in the certd process (CVE-2026-90442). Read the full advisory on psirt.watchguard.com.
- This release resolves an authenticated external control of file path issue in the management CLI (CVE-2026-90464). Read the full advisory on psirt.watchguard.com.
- This release resolves a missing authentication issue in FireCluster synchronization (CVE-2026-90465). Read the full advisory on psirt.watchguard.com.
- This release resolves a pre-authentication XPath injection in SSH authentication (CVE-2026-93434). Read the full advisory on psirt.watchguard.com.
- This release resolves a pre-authentication stack-based buffer overflow in the SIP proxy (CVE-2026-93857). Read the full advisory on psirt.watchguard.com.
- This release resolves an out-of-bounds read in FireCluster synchronization (CVE-2026-93862). Read the full advisory on psirt.watchguard.com.
- This release resolves a link following issue in the firewalld process (CVE-2026-93864). Read the full advisory on psirt.watchguard.com.
- This release resolves a missing authentication issue in FireCluster synchronization (CVE-2026-93865). Read the full advisory on psirt.watchguard.com.
- This release resolves a pre-authentication integer overflow in the Access Portal (CVE-2026-93866). Read the full advisory on psirt.watchguard.com.
- This release resolves a stack-based buffer overflow in the logging service (CVE-2026-103593). Read the full advisory on psirt.watchguard.com.
- This release resolves a stack-based buffer overflow in WireGuard configuration processing (CVE-2026-103594). Read the full advisory on psirt.watchguard.com.
- This release resolves a missing authentication issue in FireCluster state synchronization (CVE-2026-104381). Read the full advisory on psirt.watchguard.com.
- This release resolves a pre-authentication NULL pointer dereference in the management interface (CVE-2026-111107). Read the full advisory on psirt.watchguard.com.
- This release resolves heap-based buffer overflows in Active Directory authentication (CVE-2026-112709, CVE-2026-112710). Read the full advisory on psirt.watchguard.com.
- This release resolves an authenticated stack-based buffer overflow in Mobile VPN Network Access Enforcement (CVE-2026-113881). Read the full advisory on psirt.watchguard.com.
- This release updates OpenSSH to resolve multiple vulnerabilities. [FBX-34753, FBX-32519]
- This release updates OpenSSL to resolve multiple vulnerabilities. [FBX-34124]
- This release resolves a local credential exposure issue in the Mobile VPN with SSL client for Windows. [FBX-27798]

General

- Fireware now supports native issuance and automatic renewal of trusted Let's Encrypt SSL/TLS certificates for cloud-managed Fireboxes in WatchGuard Cloud. [FBX-30338]
- Firebox T145 devices no longer repeatedly reboot after an upgrade. [FBX-31504]

- The botnet attribute now correctly shows as the source on traffic log messages for denied incoming botnet traffic. *[FBX-27935]*
- WatchGuard System Manager now correctly connects to Management Server on the configured port. *[FBX-24749]*
- Firebox T185 and M295 support files now include the `disk_usage.txt` diagnostic file. *[FBX-31440]*
- This release resolves a system clock shift issue on Firebox T125, T125-W, and T145 devices. *[FBX-33287]*
- When you open Policy Manager from Firebox System Manager, you no longer receive an invalid login error if your status passphrase contains the "%" symbol. *[FBX-34309]*
- The Fireware OS version number now appears correctly on the Upgrade OS page in Fireware Web UI. *[FBX-34515]*
- This release resolves an expired feature key issue in Policy Manager. *[FBX-34553]*
- SNMP query responses for the `wgClientDHCPConnMACAddr` OID now include IP address information. *[FBX-34893]*
- This release resolves a traffic bar display issue on the Firebox System Manager (FSM) Front Panel tab. *[FBX-36488]*
- You can now successfully use brackets in arguments for `tcpdump` diagnostic tasks. *[FBX-36521]*
- The Bandwidth Meter in Firebox System Manager now correctly shows data for FireboxV devices. *[FBX-36702]*

Authentication

- Access Portal server response headers no longer disclose internal system details. *[FBX-23292]*
- When a Firebox processes a RADIUS Access-Challenge packet, it no longer truncates the State attribute if the value contains an embedded null character (0x00). *[FBX-33084]*
- Single Sign-On (SSO) authentication now successfully enforces per-user login limits. *[FBX-34966]*

FireCluster

- This release resolves an issue that caused a FireCluster member to become unresponsive after an administrator saved a configuration with WebBlocker exceptions. *[FBX-34024]*
- This release resolves a kernel stack corruption issue in the `xt_WGL` module that caused intermittent FireCluster reboots. *[FBX-33469]*
- In a FireCluster, the Hostile Sites and Ports entry no longer persistently displays an Unmatched status when the Blocked Sites List updates frequently. *[FBX-33288]*
- The Monitored Ports Health Index (MPHI) calculation in FireCluster no longer incorrectly penalizes Link Aggregation member interfaces. *[FBX-34349]*
- The FireCluster `crd` heartbeat status no longer sticks after a process restart. *[FBX-34352]*

Networking

- An embedded Network Management agent on supported Fireboxes now automates and sends local asset discovery and telemetry collection (SNMP, WMI, SSH) directly into WatchGuard Cloud (in support of the upcoming Network Management release). *[FBX-34037]*
- Syslog messages now correctly include source and destination NAT IP addresses. *[FBX-22529]*
- The `fqdn` process now correctly uses the egress interface IP address for name resolution. *[FBX-25649]*
- You can now configure Custom Dynamic Aliases to automatically import and synchronize external lists of domain names and IP addresses. *[FBX-17962]*

- Network discovery scans no longer remain in a started state when no network devices are discovered. *[FBX-26498]*
- This release resolves an issue where connections failed to traverse with a Round-Robin multi-WAN action after an interface was disqualified by Link Monitor. *[FBX-28229]*
- You can now successfully modify and delete SD-WAN actions in Firebox Cloud. *[FBX-33121]*
- New VLANs are no longer automatically added to the DNS Forwarding list in Policy Manager. *[FBX-33209]*
- Fireboxes with Network Discovery enabled no longer return FOREIGN KEY and UNIQUE Constraint Failed Device Information Manager (DIM) database errors. *[FBX-33317]*
- When you remove a VLAN from an interface with multiple tagged VLANs, the remaining VLANs on that interface no longer stop responding. *[FBX-33709]*
- DHCP leases for a reserved IP address no longer remain active after a change to the DHCP address pool. *[FBX-35338]*

Proxies, Policies, and Services

- The DNS proxy action now includes an idle timeout setting (default: 10 seconds) and an option to include idle timeout events in log messages for UDP DNS proxy connections. *[FBX-32913]*
- The default RDP policy template now allows TCP 3389 and UDP 3389 to improve Remote Desktop session performance for clients that use UDP. *[FBX-36048]*
- This release resolves a latency issue with the DNS proxy. *[FBX-30163]*
- For locally-managed Fireboxes with Manual-Order Mode enabled, the policy order no longer becomes incorrect if you change the policy order in Policy Manager. *[FBX-33257]*
- Outbound traffic generated by the Firebox (such as Multi-WAN Link Monitor probes) no longer incorrectly matches preceding firewall policies. *[FBX-34094]*
- This release resolves an issue that caused Yahoo searches to bypass SafeSearch Strict enforcement when SafeSearch was disabled in user preferences. *[FBX-35502]*

VPN

- You can now configure a branch office VPN that uses WireGuard for Firebox-to-Firebox tunnels. *[INIT-1035]*
- Mobile VPN configurations can now use IPv6 for tunnel and related network settings, so remote users can connect over IPv6 networks. *[FBX-14235, FBX-17525]*
- You can now define local networks as FireCloud resources, providing remote users with high-performance, WireGuard-powered mobile VPN access (in support of the upcoming FireCloud Network as a Resource release). *[FBX-26417]*
- TCP FIN packets for printer traffic can now correctly traverse a BOVPN tunnel. *[FBX-34103]*
- The VPN now successfully connects when you try to connect to a Mobile VPN with IKEv2 from a device that runs iOS 18 or higher. *[FBX-28074]*
- The Command Line Interface (CLI) now accepts domain names ending in a number as a BOVPN gateway ID. *[FBX-28922]*
- This release resolves an issue that caused the `iked` process to crash after receipt of an unsolicited IKE negotiation request with a large proposal list. *[FBX-29408]*
- This release resolves an issue that prevented the establishment of Mobile VPN with IKEv2 tunnels because of certificate private key format handling. *[FBX-31432]*
- BOVPN connections configured with a pre-shared key in Policy Manager now correctly establish over WireGuard tunnels. *[FBX-36465]*

- Mobile VPN with IKEv2 installation on Windows no longer fails because of Windows security restrictions. *[FBX-25556]*

Known Issues and Limitations

Known issues for Fireware v2026.4 and its management applications, including workarounds where available, can be found on the [Technical Search > Knowledge Base](#) tab. To go to 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, go to [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. The descriptions below detail which software packages you need for your upgrade.

WatchGuard System Manager

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

WSM_2026_4.exe — Use this file to install WSM v2026.4 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.

If you have...	Select from these Fireware OS packages
Firebox M295	Firebox_OS_M295_2026_4.exe firebox_M295_2026_4.zip
Firebox M395/M495/M595/M695	Firebox_M395_M495_M595_M695_2026_4.exe firebox_M395_M495_M595_M695_2026_4.zip
Firebox M4850/M5850/M6850	Firebox_OS_M4850_M5850_M6850_2026_4.exe firebox_M4850_M5850_M6850_2026_4.zip
Firebox T115-W/T125/T145	Firebox_OS_T115_T125_T145_2026_4.exe firebox_T115_T125_T145_2026_4.zip
Firebox T175	Firebox_OS_T175_2026_4.exe firebox_T175_2026_4.zip
Firebox T185	Firebox_OS_T185_2026_4.exe firebox_T185_2026_4.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_10_2.exe	Single Sign-On Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO ⁴	No
WG-Authentication-Client_12_7.msi	Single Sign-On Client software for Windows ⁴	No
WG-SSOCLIENT-MAC_12_5_4.dmg	Single Sign-On Client software for macOS ⁴	No
SSOExchangeMonitor_x86_12_10.exe	Exchange Monitor for 32-bit operating systems	No
SSOExchangeMonitor_x64_12_10.exe	Exchange Monitor for 64-bit operating systems	No
TO_AGENT_SETUP_12_11_2.exe	Terminal Services software for both 32-bit and 64-bit systems	No
WG-MVPN-SSL_2026_4.exe	Mobile VPN with SSL Client for Windows	Yes
WG-MVPN-SSL_2026_2_2.dmg	Mobile VPN with SSL Client for macOS	No
WG-Mobile-VPN_Windows_x86-64_1610_32527.exe¹	WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP²	Yes
WatchGuard_Mobile_VPN_x86-64_474_30037.dmg¹	WatchGuard IPSec Mobile VPN Client for macOS, powered by NCP²	Yes
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.

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 v12.10.2 supports Fireware v12.5.4 or higher only. Before you install SSO Agent v12.10.2, you must upgrade the Firebox to Fireware v12.5.4 or higher. If you install SSO Agent v12.10.2, 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 v2025.1.x supports previous versions of the SSO Agent.

Upgrade to Fireware v2026.4

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 v2026.4. You can install the v2026.4 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, go to [Fireware Help](#).

Upgrade to Fireware v2026.4 from WatchGuard Cloud

From WatchGuard Cloud, you can upgrade the firmware for a Firebox that runs Fireware v12.5.2 or higher. To upgrade from WatchGuard Cloud, go to [Upgrade Firmware from WatchGuard Cloud](#) in *WatchGuard Cloud Help*.

Upgrade to Fireware v2026.4 from Fireware Web UI

You can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. To upgrade manually, go to [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 v2026.4 from WSM/Policy Manager

To upgrade from WSM/Policy Manager, go to [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.

Gateway Wireless Controller Access Point Firmware

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.



As of Fireware v12.11, only AP125, AP225W, AP325, AP327X, AP420 devices that run the latest v11.0.0-36-4 AP firmware are supported by the Gateway Wireless Controller. Upgrade to the latest AP firmware before you upgrade to Fireware v12.11 or 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 4:00 AM 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.

Fireware v2026.4 Operating System Compatibility Matrix

Last reviewed: 27 October 2026

WSM/ Fireware Component	Microsoft Windows 10, 11	Microsoft Windows Server 2019, 2022, & 2025	macOS v10.14, v10.15, v11, v12, v13, v14, v15, & v26	Android 7, 8, 9, 10, 11, 12, 13, 14, 15, & 16	iOS v9, v10, v11, v12, v13, v14, v15, v16, v17, v18, & v26
WatchGuard System Manager	Supported	Supported	Not Supported	Not Supported	Not Supported
WatchGuard Servers <i>For information on WatchGuard Dimension, go to the Dimension Release Notes.</i>	Supported	Supported	Not Supported	Not Supported	Not Supported
Single Sign-On Agent (Includes Event Log Monitor)¹¹	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Single Sign-On Client	Supported ¹⁴	Supported ¹⁴	Supported ^{2, 13}	Not Supported	Not Supported
Single Sign-On Exchange Monitor	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Terminal Services Agent¹	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Mobile VPN with IPSec	Supported	Not Supported	Supported ^{2, 3, 8}	Supported	Supported ³
Mobile VPN with SSL	Supported	Not Supported	Supported ^{2, 6, 9, 12}	Supported ⁴	Supported ⁴
Mobile VPN with IKEv2	Supported	Not Supported	Supported ^{2, 7, 15}	Supported ⁵	Supported ¹⁵
Mobile VPN with L2TP	Supported	Not Supported	Supported ³	Supported ¹⁰	Supported

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 Edge 116
- Firefox v117

- Safari 16 (macOS)
- Chrome v116

¹Terminal 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.

²To learn more about client support for different macOS versions, go to the macOS software compatibility KB articles for [macOS Catalina 10.15](#), [macOS Big Sur 11](#), [macOS Monterey 12](#), [macOS Ventura 13](#), [macOS Sonoma 14](#), [macOS Sequoia 15](#), and [macOS Tahoe 26](#).

³Native (Cisco) IPsec client is supported for all recent versions of macOS and iOS.

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

⁵StrongSwan is supported for all recent versions of Android.

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

⁷In 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, go to [this KB article](#).

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

⁹macOS 13 (Ventura) and higher do not accept SSL connections to untrusted self-signed certificates. For more information, go to [this KB article](#).

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

¹¹The WatchGuard Single-Sign On Agent v12.10.1 supports computers that are joined to your domain with Azure Active Directory.

¹²The WatchGuard Mobile VPN with SSL Client v12.10.4 for macOS does not support macOS 10.15 (Catalina) or lower.

¹³The Single Sign-On Client does not support macOS 15 (Sequoia) or macOS 26 (Tahoe).

¹⁴The Single Sign-On Client does not support Windows devices with ARM processors.

¹⁵For IKEv2 VPNs, macOS v26 (Tahoe) and iOS v26 do not support DES, 3DES, SHA1-96, or SHA1-160 algorithms, and do not support Diffie-Hellman groups less than 14.

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.

	AuthPoint Authenticatio n Server	AuthPoint RADIUS Server	Active Directory	LDAP	RADIUS	SecurID	Firebox (Firebox-DB) Local Authenticatio n	SAML
Mobile VPN with IPsec for iOS, Windows, and macOS	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
Mobile VPN with IPsec for Android	Not Supported	Supported	Supported	Supported	Supported	Not Supported	Supported	Not Supported
Mobile VPN with SSL	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Mobile VPN with IKEv2 for Windows	Supported	Supported	Supported ¹	Not Supported	Supported	Not Supported	Supported	Not Supported
Mobile VPN with L2TP	Not Supported	Supported	Supported ¹	Not Supported	Supported	Not Supported	Supported	Not Supported
Built-in Web Page on Port 4100 and 8080	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported ²
Access Portal	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
AD Single Sign-On Support (<i>with or without client software</i>)	Not Supported	Not Supported	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported
Terminal Services Manual Authenticatio n	Not Supported	Not Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
Terminal Services Authenticatio n with Single Sign-On	Not Supported	Not Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

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

² Port 8080 does not support SAML authentication.

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 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, select your language from the drop-down list.