Fireware v11.10.3 Update 1 Release Notes

Supported Devices	Firebox T30 and T30 Wireless Firebox T50 and T50 Wireless
Fireware OS Build	487537
WatchGuard System Manager Build	486754
WatchGuard AP Device Firmware	1.2.9.4 Build 150508
Release Notes Revision Date	7 December 2015

Introduction

Fireware v11.10.3 Update 1 is available for Firebox T30 and T50 devices only. We strongly recommend that all Firebox T30 and T50 appliance users upgrade their Firebox to use Update 1 immediately to take advantage of bug fixes and enhancements added since the device was manufactured.

WatchGuard is pleased to announce the release of Fireware v11.10.3 Update 1 and WatchGuard System Manager v11.10.3. The release supports the latest additions to our award-winning line of network security appliances -- the Firebox T30 and Firebox T50 (wired and wireless).

To see the enhancements and bug fixes included in this release, see the Enhancements and Resolved Issues section.

Before You Begin

Before you install this release, it is important to understand:

- Fireware v11.10.3 Update 1 can be installed on a Firebox T30 or T50, wired or wireless.
- You must use WatchGuard System Manager v11.10.3, Fireware Web UI, or the Fireware CLI to manage your Firebox T30 or T50. Earlier versions of WatchGuard System Manager do not recognize these new models. You can also use WatchGuard System Manager v11.10.3 to manage Firebox or XTM devices running earlier versions of Fireware.
- You must activate your Firebox and apply a feature key for your Firebox to operate correctly.

Product documentation for all WatchGuard products is available on the WatchGuard web site at www.watchguard.com/help/documentation. There are no updates for the Fireware v11.10.3 release.

Localization

This release includes localized management user interfaces (WSM application suite and Web UI) current as of Fireware v11.9.1. UI changes introduced since v11.9.1 remain in English. Supported languages are:

- Chinese (Simplified, PRC)
- 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 7 and want to use WSM in Japanese, go to Control Panel > Regions and Languages and select Japanese on the Keyboards and Languages tab 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.

Fireware and WSM v11.10.3 Operating System Compatibility

Last revised: 2 November 2015

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10 (32-bit & 64-bit)	Microsoft Windows Server 2008 & 2008 R2	Microsoft Windows Server 2012 &2012 R2 (64-bit)	Mac OS X v10.9, v10.10	Android 4.x & 5.x	iOS v7 & v8
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	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[1]		✓	✓			
Terminal Services Agent[2]		✓	✓			
Mobile VPN with IPSec	✓			✓ 3	✓	✓ 3
Mobile VPN with SSL	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *For Microsoft Windows Server 2008, we support both 32-bit and 64-bit support. For Windows Server 2008 R2, we support 64-bit only.*
- *Windows 8.x support does not include Windows RT.*
- *Windows Exchange Server 2013 is supported if you install Windows Sever 2012 or 2012 R2 and .Net framework 3.5.*

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

- *IE 9 and later*
- *Microsoft Edge (because Edge has not yet been officially released by Microsoft, all testing was done with a release candidate)*
- *Firefox v22 and later*
- *Safari 6 and later*
- *Safari iOS 6 and later*
- *Chrome v29 and later*

[1]Microsoft Exchange Server 2007, 2010, and 2013 are supported.

[2]Terminal Services support with manual or Single Sign-On authentication operates in a Microsoft Terminal Services or Citrix XenApp 4.5, 5.0, 6.0 and 6.5 environment.

[3]Native (Cisco) IPSec client and OpenVPN are supported for Mac OS and iOS. For Mac OS X 10.8 -10.10, we also support the WatchGuard IPSec Mobile VPN Client for Mac, powered by NCP.

Authentication Support

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

 *Fully supported by WatchGuard*  *Not yet supported, but tested with success by WatchGuard customers*

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

1. *Active Directory support includes both single domain and multi-domain support, unless otherwise noted.*
2. *RADIUS and SecurID support includes support for both one-time passphrases and challenge/response authentication integrated with RADIUS. In many cases, SecurID can also be used with other RADIUS implementations, including Vasco.*
3. *The Shrew Soft client does not support two-factor authentication.*
4. *Fireware supports RADIUS Filter ID 11 for group authentication.*
5. *Both single and multiple domain Active Directory configurations are supported.For information about the supported Operating System compatibility for the WatchGuard TO Agent and SSO Agent, see the current Fireware and WSM Operating System Compatibility table.*
6. *Active Directory authentication methods are supported only through a RADIUS server.*

System Requirements

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

Downloading 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.

WatchGuard System Manager

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

`WSM11_10_3.exe` — Use this file to install WatchGuard System Manager v11.10.3 or to upgrade WatchGuard System Manager from v11.x to WSM v11.10.3.

Fireware OS

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 using the Fireware Web UI.

If you have…	Select from these Fireware OS packages
Firebox T30	`Firebox_OS_T30_T50_11_10_3_U1.exe` `firebox_T30_T50_11_10_3_U1.zip`
Firebox T50	`Firebox_OS_T30_T50_11_10_3_U1.exe` `firebox_T30_T50_11_10_3_U1.zip`

Single Sign-On Software

These files are available for Single Sign-On.

- `WG-Authentication-Gateway_11_10.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_9_4.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_10.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_10.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_10.exe` (Exchange Monitor for 64-bit operating systems)

For information about how to install and set up Single Sign-On, see the product documentation.

Terminal Services Authentication Software

- `TO_AGENT_SETUP_11_10.exe` (This installer includes both 32-bit and 64-bit file support.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL.

- `WG-MVPN-SSL_11_10.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_10.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download.

Shrew Soft Client

- `Shrew Soft Client 2.2.2 for Windows` - No client license required.

WatchGuard IPSec Mobile VPN Clients

All client software has been recently updated to v12.02, which includes support for Windows 10 Enterprise.

- `WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.
- `WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.
- `WatchGuard IPSec Mobile VPN Client for Mac OS X, powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.

WatchGuard Mobile VPN License Server

- `WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP`- Click here for more information about MVLS.

WatchGuard AP Firmware

If you have Gateway Wireless Controller configured to update devices automatically, any AP device which your Gateway Wireless Controller manages will be upgraded to v1.2.9.4 firmware (Build 150508) when you upgrade your Firebox to Fireware v11.10.x for the first time. You can also upgrade the AP device software for an individual AP device from the Gateway Wireless Controller. If you want to update your WatchGuard AP devices manually without using the Gateway Wireless Controller, you can open the WatchGuard AP Software Download page and download the latest AP firmware and manually update your AP devices. We also provide the files to manually update the firmware for an unpaired AP device, if required. The file names for the most current AP firmware are:

- `AP100-v1.2.9.4.bin`
- `AP200-v1.2.9.4.bin`

Upgrade to Fireware v11.10.3 Update 1

Before you upgrade from Fireware v11.10.3 to Fireware v11.10.3 Update 1, download and save the Fireware OS file for your Firebox. You can use Policy Manager or the Web UI to complete the upgrade procedure. We strongly recommend that you back up your Firebox configuration and your WatchGuard Management Server configuration before you upgrade. It is not possible to downgrade without these backup files.

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 v11.x server or client software when you update to WSM v11.10.x. You can install the v11.10.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: WatchGuard Log Server, WatchGuard Report Server) before you upgrade. You will need these backup files if you ever want to downgrade.

To back up your Management Server configuration, from the computer where you installed the Management Server:

1. From WatchGuard Server Center, select **Backup/Restore Management Server**.
   The WatchGuard Server Center Backup/Restore Wizard starts.
2. Click **Next**.
   The Select an action screen appears.
3. Select **Back up settings**.
4. Click **Next**.
   The Specify a backup file screen appears.
5. Click **Browse** to select a location for the backup file. Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.
   The WatchGuard Server Center Backup/Restore Wizard is complete screen appears.
7. Click **Finish** to exit the wizard.

Upgrade to Fireware v11.10.x from Web UI

You can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page.

Upgrade to Fireware v11.10.3 Update 1 from WSM/Policy Manager

1. Select **File > Backup** or use the USB Backup feature to back up your current device image.
2. On a management computer running a Windows 64-bit operating system, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called *[Firebox or xtm series]_[product code].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\Fireware\11.10.3\[model] or [model][product_code].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\Fireware\11.10.3
3. Install and open WatchGuard System Manager v11.10.3. Connect to your Firebox and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[product series]_[product code].sysa-dl* file from Step 2.

Enhancements and Resolved Issues

- A problem that caused a kernel crash on bootup when a Firebox is configured with bridged interfaces and multicast traffic has been resolved in this release. [87892]
- A Firebox can now successfully download its configuration from a WatchGuard Management Server after it is upgraded from Fireware v11.9.5 to v11.10.x. *[86894, 87140]*
- An issue that caused a RapidDeploy Management Server registration to fail has been resolved in this release. *[86737]*
- The Log Server upgrade feature has been improved to prevent schema errors during upgrade. *[85756]*
- Policy Manager no longer displays policies created with the same policy template with the same order number. *[86994]*

Known Issues and Limitations

Known issues for Fireware v11.10.3 and its management applications, including workarounds where available, can be found on the WatchGuard website. To see Known Issues, log in to the WatchGuard website and use the filters available on the Technical Search > Knowledge base tab.

Using the CLI

The Fireware CLI (Command Line Interface) is fully supported for v11.x releases. For information on how to start and use the CLI, see the *Command Line Reference Guide*. You can download the latest CLI guide from the documentation web site at http://www.watchguard.com/wgrd-help/documentation/xtm.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at http://www.watchguard.com/support. 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