

Fireware v11.10.5 Release Notes

Supported Devices	Firebox T10, T30, T50, Firebox M200, M300, M400, M440, M500 XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 XTMv, WatchGuard AP
Release Date	7 January 2016
Release Notes Revision Date	11 February 2016
Fireware OS Build	492938
WatchGuard System Manager Build	492531
WatchGuard AP Device Firmware	For AP 100, 102, 200: Build 1.2.9.6 (151211) For AP 300: Build 2.0.0.1 (151216)

Introduction



On 11 February, we posted updated Fireware v11.10.5 executable (.exe) files in the WatchGuard Software Downloads Center. There are no functional changes to the updated .exe files, but each file has now been signed with a SHA-256 certificate, which is more secure than the SHA-1 certificate that was previously used. Some recent browser versions, including Internet Explorer v11, require the updated cert.

WatchGuard is pleased to announce the release of Fireware v11.10.5, WatchGuard System Manager v11.10.5, and the newest addition to the WatchGuard AP device family, the AP300. The new AP300 devices add support for critical wireless features, including fast handover, band steering, fast roaming and per-radio channel client limits. These new features are supported only on AP300 devices. You must use a Firebox running Fireware v11.10.5 to manage AP300 devices.

The release also includes many bug fixes and several feature enhancements, including:

- The signature hash algorithm used for default Firebox certificates has been changed from SHA-1 to SHA-256. Click [here](#) for important information about this change.
- Ability to configure the interval for automatic wireless scans for Wireless Deployment Maps and Rogue Access Point detection.
- New wireless event alarms trigger notifications if an AP device goes offline or a rogue access point is detected.
- Ability to see the hostname and IP address of connected wireless clients.
- APT Blocker now supports the POP-3 Proxy.
- 3G/4G USB modem support for the Verizon Novatel U620L modem.

- For traffic that is allowed through Packet Filter policies, you can now enable the Firebox to send log messages that are only used in reports.
- In accordance with PCI DSS 3.1 requirements, the Firebox no longer supports TLSv1.0 for connections to Fireware web services such as the Web UI and Authentication Portal page.
- UI localization update for Web UI and WatchGuard System Manager. Click [here](#) for more information.

For more information on the bug fixes and enhancements in this release, see the [Enhancements and Resolved Issues](#) section. For more detailed information about the feature enhancements and functionality changes included in Fireware v11.10.5, see the product documentation or review [What's New in Fireware v11.10.5](#).

Important Information about Firebox Certificates

SHA-1 is being deprecated by many popular web browsers, and WatchGuard recommends that you now use SHA-256 certificates. Because of this, we have upgraded our default Firebox certificates. Starting with Fireware v11.10.4, all newly generated default Firebox certificates use a 2048-bit key length. In addition, newly generated default Proxy Server and Proxy Authority certificates use SHA-256 for their signature hash algorithm. Starting with Fireware v11.10.5, all newly generated default Firebox certificates use SHA-256 for their signature hash algorithm. New CSRs created from the Firebox also use SHA-256 for their signature hash algorithm.

Default certificates are not automatically upgraded after you install Fireware v11.10.5.

To regenerate any default Firebox certificates, delete the certificate and reboot the Firebox. If you want to regenerate default certificates without a reboot, you can use the CLI commands described in the next section. Before you regenerate the Proxy Server or Proxy Authority certification, there are some important things to know.

The Proxy Server certificate is used for inbound HTTPS with content inspection and SMTP with TLS inspection. The Proxy Authority certificate is used for outbound HTTPS with content inspection. The two certificates are linked because the default Proxy Server certificate is signed by the default Proxy Authority certificate. If you use the CLI to regenerate these certificates, after you upgrade, you must redistribute the new Proxy Authority certificate to your clients or users will receive web browser warnings when they browse HTTPS sites, if content inspection is enabled.

Also, if you use a third-party Proxy Server or Proxy Authority certificate:

- The CLI command will not work unless you first delete either the Proxy Server or Proxy Authority certificate. The CLI command will regenerate both the Proxy Server and Proxy Authority default certificates.
- If you originally used a third-party tool to create the CSR, you can simply re-import your existing third-party certificate and private key.
- If you originally created your CSR from the Firebox, you must create a new CSR to be signed, and then import a new third-party certificate.

CLI Commands to Regenerate Default Firebox Certificates

To regenerate any default Firebox certificates, delete the certificate and reboot the Firebox. If you want to regenerate default certificates without a reboot, you can use these CLI commands:

- To upgrade the default Proxy Authority and Proxy Server certificates for use with HTTPS content inspection, you can use the CLI command: `upgrade certificate proxy`
- To upgrade the Firebox web server certificate, use the CLI command: `upgrade certificate web`
- To upgrade the SSLVPN certificate, use the CLI command: `upgrade certificate sslvpn`
- To upgrade the 802.1x certificate, use the CLI command: `upgrade certificate 8021x`

For more information about the CLI, see the [Command Line Interface Reference](#).

Before You Begin

Before you install this release, make sure that you have:

- A supported WatchGuard Firebox or XTM device. This device can be a WatchGuard Firebox T10, T30, T50, XTM 2 Series (models 25 and 26 only), 3 Series, 5 Series, 8 Series, 800 Series, XTM 1050, XTM 1500 Series, XTM 2050 device, XTM 2500 Series, Firebox M200, M300, M400, M500, M440, or XTMv (any edition).
- 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 or XTM device and the version of WSM installed on your Management Server.
- Feature key for your Firebox or XTM device — 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.

Note that you can install and use WatchGuard System Manager v11.10.5 and all WSM server components with devices running earlier versions of Fireware v11. In this case, we recommend that you use the product documentation that matches your Fireware OS version.

If you have a new Firebox or XTM physical device, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. If this is a new XTMv installation, make sure you carefully review the [XTMv Setup Guide](#) for important installation and setup instructions. We also recommend that you review the [Hardware Guide](#) for your Firebox or XTM device 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 www.watchguard.com/help/documentation.

Localization

This release includes localized management user interfaces (WSM application suite and Web UI) current as of Fireware v11.10.2. UI changes introduced since v11.10.2 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 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 v11.10.5 Operating System Compatibility

Last revised: 6 January 2016

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, v10.11	Android 4.x & 5.x	iOS v7, v8, & v9
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)		✓	✓			
Single Sign-On Client	✓	✓	✓	✓		
Single Sign-On Exchange Monitor¹		✓	✓			
Terminal Services Agent²		✓	✓			
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
- Firefox v22 and later
- Safari 6 and later
- Safari iOS 6 and later
- Chrome v29 and later



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

²Terminal Services support with manual or Single Sign-On authentication operates in a Microsoft Terminal Services or Citrix XenApp 4.5, 5.0, 6.0, 6.5 and 7.6 environment.

³Native (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 (<i>with or without client software</i>)	✓	✓	–	–	–
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

XTMv System Requirements

With support for installation in both a VMware and a Hyper-V environment, a WatchGuard XTMv virtual machine can run on a VMware ESXi 4.1, 5.0, 5.1, 5.5, or 6.0 host, or on Windows Server 2008 R2, Windows Server 2012, Hyper-V Server 2008 R2, or Hyper-V Server 2012.

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

Each XTMv virtual machine requires 3 GB of disk space.

Recommended Resource Allocation Settings

	Small Office	Medium Office	Large Office	Datacenter
Virtual CPUs	1	2	4	8 or more
Memory	1 GB	2 GB	4 GB	4 GB or more

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 for your upgrade.

WatchGuard System Manager

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

`WSM11_10_5.exe` — Use this file install WSM v11.10.5 or to upgrade WatchGuard System Manager from v11.x to WSM v11.10.5.

Fireware OS

Select the correct Fireware OS image for your Firebox or XTM device. 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. Use the .ova or .vhd file to deploy a new XTMv device.

If you have...	Select from these Fireware OS packages
XTM 2500 Series	XTM_OS_XTM800_1500_2500_11_10_5.exe xtm_xtm800_1500_2500_11_10_5.zip
XTM 2050	XTM_OS_XTM2050_11_10_5.exe xtm_xtm2050_11_10_5.zip
XTM 1500 Series	XTM_OS_XTM800_1500_2500_11_10_5.exe xtm_xtm800_1500_2500_11_10_5.zip
XTM 1050	XTM_OS_XTM1050_11_10_5.exe xtm_xtm1050_11_10_5.zip
XTM 800 Series	XTM_OS_XTM800_1500_2500_11_10_5.exe xtm_xtm800_1500_2500_11_10_5.zip
XTM 8 Series	XTM_OS_XTM8_11_10_5.exe xtm_xtm8_11_10_5.zip
Firebox M500 Series	Firebox_OS_M400_M500_11_10_5.exe firebox_M400_M500_11_10_5.zip
XTM 5 Series	XTM_OS_XTM5_11_10_5.exe xtm_xtm5_11_10_5.zip
Firebox M440	Firebox_OS_M440_11_10_5.exe firebox_M440_11_10_5.zip
Firebox M400 Series	Firebox_OS_M400_M500_11_10_5.exe firebox_M400_M500_11_10_5.zip
Firebox M300	Firebox_OS_M200_M300_11_10_5.exe firebox_M200_M300_11_10_5.zip
Firebox M200	Firebox_OS_M200_M300_11_10_5.exe firebox_M200_M300_11_10_5.zip
XTM 330	XTM_OS_XTM330_11_10_5.exe xtm_xtm330_11_10_5.zip
XTM 33	XTM_OS_XTM3_11_10_5.exe xtm_xtm3_11_10_5.zip
XTM 2 Series Models 25, 26	XTM_OS_XTM2A6_11_10_5.exe xtm_xtm2a6_11_10_5.zip
Firebox T30	Firebox_OS_T30_T50_11_10_5.exe firebox_T30_T50_11_10_5.zip
Firebox T50	Firebox_OS_T30_T50_11_10_5.exe firebox_T30_T50_11_10_5.zip

If you have...	Select from these Fireware OS packages
Firebox T10	Firebox_OS_T10_11_10_5.exe firebox_T10_11_10_5.zip
XTMv All editions for VMware	xtmv_11_10_5.ova xtmv_11_10_5.exe xtmv_11_10_5.zip
XTMv All editions for Hyper-V	xtmv_11_10_5_vhd.zip xtmv_11_10_5.exe xtmv_11_10_5.zip

Single Sign-On Software

These files are available for Single Sign-On. No files have been updated with the v11.10.5 release.

- WG-Authentication-Gateway_11_10_4.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_4.exe (Exchange Monitor for 32-bit operating systems)
- SSOExchangeMonitor_x64_11_10_4.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_4.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. There are no updates with the v11.10.5 release.

- WG-MVPN-SSL_11_10_4.exe (Client software for Windows)
- WG-MVPN-SSL_11_10_4.dmg (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download. There are no updates with the v11.10.5 release.

Shrew Soft Client

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

WatchGuard IPSec Mobile VPN Clients

- 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.

Upgrade to Fireware v11.10.5

Before you upgrade to Fireware v11.10.x, your Firebox must be running:

- Fireware XTM v11.7.5
- Fireware XTM v11.8.4
- Fireware XTM v11.9 or higher



If you try to upgrade from Policy Manager and your Firebox is running an unsupported version, the upgrade is prevented.

If you try to schedule an OS update of managed devices through a Management Server, the upgrade is also prevented.

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x before you upgrade to Fireware v11.10.x or your Firebox will be reset to a default state.

Before you upgrade from Fireware v11.x to Fireware v11.10.5, download and save the Fireware OS file that matches the Firebox you want to upgrade. 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.



If you want to upgrade an XTM 2 Series, 3 Series, or 5 Series device, we recommend that you reboot your Firebox before you upgrade. This clears your device memory and can prevent many problems commonly associated with upgrades in those devices.

Back up your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x server or client software when you upgrade to WSM v11.10.5. You can install the v11.10.5 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](#)) to a safe location 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

If your Firebox is running Fireware v11.10 or later, you can upgrade the Fireware OS on your Firebox automatically from the **System > Upgrade OS** page. If your Firebox is running v11.9.x or earlier, use these steps to upgrade:

1. Go to **System > Backup Image** or use the USB Backup feature to back up your current device image.
2. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads page.
If you use the Windows-based installer on a computer with a Windows 64-bit operating system, this installation extracts an upgrade file called `[product series]_[product code].sysa-dl` to the default location of `C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.10.5\[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\11.10.5`
3. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the `[product series]_[product code].sysa-dl` from Step 2 and click **Upgrade**.

Upgrade to Fireware v11.10.x 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\11.10.5\[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\11.10.5`

3. Install and open WatchGuard System Manager v11.10.5. 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.

Update AP Devices

With the release of Fireware v11.10.5, we are releasing new AP firmware for all AP devices. The process to update to new AP firmware has changed. Please review this section carefully for important information about updating AP devices.

Update your AP100, AP102, and AP200 Devices

Fireware v11.10.5 includes new AP firmware v1.2.9.6 for AP100/102 and AP200 devices. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 to Fireware v11.10.5, your AP devices are automatically updated. Note that, beginning with Fireware v11.10.5, automatic updates occur only between midnight and 4:00am local time.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.10.5 (without first upgrading to Fireware v11.10.4), there is an additional step you must take to make sure AP v1.2.9.6 is applied to your AP devices. When you upgrade to Fireware v11.10.5 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the Web UI:

1. Connect to your Firebox and select **System > Upgrade OS**.
2. Browse to the location of your Fireware v11.10.5 upgrade file and click **Upgrade**.
3. When the upgrade is complete, repeat Step 2.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. To reinstall the AP firmware on the Firebox you must reinstall Fireware v11.10.5 on the Firebox.

AP firmware v1.2.9.6 is not available in the Software Downloads Center. The only way to update your AP devices to v1.2.9.6 is through Gateway Wireless Controller.

Update your AP300 Devices

It is important to understand that you cannot manage AP300 devices unless you use the Gateway Wireless Controller with Fireware v11.10.5. If you manage AP300 devices and downgrade to an earlier version of Fireware, you will lose the ability to manage your AP300 devices.

Fireware v11.10.5 includes AP firmware v2.0.0.1. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 to Fireware v11.10.5, your AP devices will be automatically updated if necessary. Note that, beginning with Fireware v11.10.5, automatic updates occur only between midnight and 4:00am local time.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.10.5 (without first upgrading to Fireware v11.10.4), there is an additional step you must take to make sure AP v2.0.0.1 is applied to your AP devices. When you upgrade to Fireware v11.10.5 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the Web UI:

1. Connect to your Firebox and select **System > Upgrade OS**.
2. Browse to the location of your Fireware v11.10.5 upgrade file and click **Upgrade**.
3. When the upgrade is complete, repeat Step 2.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. To reinstall the AP firmware, use one of these two methods:

Reinstall Fireware v11.10.5 on your Firebox

1. Connect to your Firebox and select **System > Upgrade OS**.
2. Browse to the location of your Fireware v11.10.5 upgrade file and click **Upgrade**.

Download the AP firmware package from the Software Downloads Center and install it on the Firebox

1. Download and extract the AP firmware package. The component package file extension is `wgpkg-d1`.
2. From Fireware Web UI, select **System > Upgrade OS**.
3. Select **Use an upgrade file**.
4. Browse to the location of the `wgpkg-d1` file and click **Upgrade**.

Upgrade your FireCluster to Fireware v11.10.5

Before you upgrade to Fireware v11.10.x, your Firebox must be running:

- Fireware XTM v11.7.5
- Fireware XTM v11.8.4
- Fireware XTM v11.9 or higher



If you try to upgrade from Policy Manager and your Firebox is running an unsupported version, the upgrade is prevented.

If you try to schedule an OS update of managed devices through a Management Server, the upgrade is also prevented.

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x before you upgrade to Fireware v11.10.x or your Firebox will be reset to a default state.

There are two methods to upgrade Fireware OS on your FireCluster. The method you use depends on the version of Fireware you currently use.



We recommend that you use Policy Manager to upgrade, downgrade, or restore a backup image to a FireCluster. It is possible to do some of these operations from the Web UI but, if you choose to do so, you must follow the instructions in the [Help](#) carefully as the Web UI is not optimized for these tasks. It is not possible to upgrade your FireCluster from v11.8.x to v11.9.x or higher with the Web UI.

Upgrade a FireCluster from Fireware v11.4.x–v11.9.x to v11.10.x

Use these steps to upgrade a FireCluster to Fireware v11.10.x:

1. Open the cluster configuration file in Policy Manager
2. Select **File > Upgrade**.
3. Type the configuration passphrase.
4. Type or select the location of the upgrade file.
5. To create a backup image, select **Yes**.

A list of the cluster members appears.

6. Select the check box for each device you want to upgrade.

A message appears when the upgrade for each device is complete.

When the upgrade is complete, each cluster member reboots and rejoins the cluster. If you upgrade both devices in the cluster at the same time, the devices are upgraded one at a time. This is to make sure there is not an interruption in network access at the time of the upgrade.

Policy Manager upgrades the backup member first and then waits for it to reboot and rejoin the cluster as a backup. Then Policy Manager upgrades the master. Note that the master's role will not change until it reboots to complete the upgrade process. At that time the backup takes over as the master.

To perform the upgrade from a remote location, make sure the FireCluster interface for management IP address is configured on the external interface, and that the management IP addresses are public and routable. For more information, see [About the Interface for Management IP Address](#).

Upgrade a FireCluster from Fireware v11.3.x

To upgrade a FireCluster from Fireware v11.3.x to Fireware v11.9.x or higher, you must perform a manual upgrade. For manual upgrade steps, see the Knowledge Base article [Upgrade Fireware OS for a FireCluster](#).

Downgrade Instructions

Downgrade from WSM v11.10.x to WSM v11.x

If you want to revert from v11.10.x to an earlier version of WSM, you must uninstall WSM v11.10.x. 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 v11.10.x.

Next, install the same version of WSM that you used before you upgraded to WSM v11.10.x. 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 v11.10.x. Verify that all WatchGuard servers are running.

Downgrade from Fireware v11.10.x to Fireware v11.x



If you use the Fireware Web UI or CLI to downgrade from Fireware v11.10.x 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.

If you want to downgrade from Fireware v11.10.x to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v11.10.x. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v11.10.x to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device. This is not an option for XTMv users.

See the [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

Some downgrade restrictions apply:

- You cannot downgrade an XTM 2050 or an XTM 330 to a version of Fireware lower than v11.5.1.
- You cannot downgrade an XTM 25, 26, or 33 device to a version of Fireware lower than v11.5.2.
- You cannot downgrade an XTM 5 Series model 515, 525, 535 or 545 to a version of Fireware lower than v11.6.1.
- You cannot downgrade a Firebox T10 to a version of Fireware lower than v11.8.3. You cannot downgrade a Firebox T10-D to a version of Fireware lower than v11.9.3.
- You cannot downgrade a Firebox T30 or T50 to a version of Fireware lower than v11.10.3 Update 1.
- You cannot downgrade a Firebox M200/M300 to a version of Fireware lower than v11.9.6.
- You cannot downgrade a Firebox M440 to a version of Fireware lower than v11.9.3.
- You cannot downgrade a Firebox M400 or M500 to a version of Fireware lower than v11.9.4.
- You cannot downgrade XTMv in a VMware environment to a version of Fireware lower than v11.5.4.
- You cannot downgrade XTMv in a Hyper-V environment to a version of Fireware lower than v11.7.3.



When you downgrade the Fireware OS on your Firebox or XTM device, 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.

Enhancements and Resolved Issues in Fireware v11.10.5

Certificates and Security

- The Firebox now signs all default Firebox certificates using the SHA-256 signature hash algorithm. *[88328, 85771]*
- Certificate signing requests created on the Firebox now use the SHA-256 signature hash algorithm. *[82783]*
- In accordance with PCI DSS 3.1 requirements, the Firebox no longer supports TLSv1.0 for connections to Fireware web services such as the Web UI and Authentication Portal page. *[86810, 65817]*
- The Firebox now uses a 2048-bit key group when negotiating Diffie-Hellman cipher suites for connections to Fireware web services such as the Web UI and Authentication Portal page. *[85991]*
- The OpenSSH library, as used by the Fireware CLI, has been patched to resolve a potential OpenSSH brute force authentication vulnerability (CVE-2015-5600). *[86990]*
- The OpenSSH library, as used by WatchGuard AP devices, has been patched to resolve a potential OpenSSH brute force authentication vulnerability (CVE-2015-5600). *[88161]*
- The process that manages Firebox certificates no longer crashes when a certificate is imported. *[88754]*
- IP source route attacks are now correctly detected when a Firebox is configured with bridge mode. *[79653]*
- The Hotspot feature now redirects to HTTP instead of HTTPS when the **Require users to authenticate with generated credentials** check box is enabled to prevent guest users from receiving certificate warnings. *[83173]*
- The HTTPS Proxy now re-signs web server certificates using their original signature hash algorithm when Content Inspection is enabled. *[86291, 88725]*

AP and Wireless

- Radio Resource Management (802.11k) is now supported (on AP300 devices only). *[87456]*
- Fast handover is now supported (on AP300 devices only). *[87438]*
- Fast roaming is now supported (on AP300 devices only). *[79032]*
- Band steering is now supported (on AP300 devices only). *[83504]*
- You can now limit the number of concurrently connected client devices for a specific radio (on AP300 devices only). *[81178]*
- You can now specify a scan interval (in hours) for wireless rogue access point detection. *[85953]*
- Gateway Wireless Controller no longer includes support for the legacy security protocol, TKIP as a stand-alone encryption method. If your configuration included TKIP only, it will be converted to use the **TKIP or AES** setting. *[80905]*
- The redundant **Gateway Wireless Controller > Enable Client Association Logging** configuration control has been removed from the UI. *[88212]*
- Automatic AP firmware updates managed by the Gateway Wireless Controller now occur only between midnight and 4:00am local time. *[88056]*

Networking

- The Firebox no longer crashes and reboots when IPv6 is enabled. *[88623]*
- Traffic Management now works correctly on External Interfaces configured using PPPoE. *[56974]*
- Supported modems now work correctly with Firebox M400 and M500 appliances. *[87531]*

- An issue that caused an untagged VLAN interface to not be correctly recognized was resolved. This problem occurred most often when the Firebox was connected to a VoIP phone and negotiated at 100Mbps link speed. [87976]

Security Subscriptions

- APT Blocker is now supported with the POP-3 proxy. [80961]

Logging

- You can now send log messages for use in reports for packet filter policies without the need to enable logging for allowed traffic. [81624]

RapidDeploy

- You can now successfully register your Management Server for RapidDeploy after it is upgraded from v11.10.x to v11.10.4 or later. [88973]

Known Issues and Limitations

Known issues for Fireware v11.10.5 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