Fireware v11.9.4 Update 1 Release Notes

Supported Devices	XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 Firebox T10, Firebox M400, M440, and M500, XTMv, WatchGuard AP
Fireware OS Build	463675
WatchGuard System Manager Build	462272
Release Notes Revision Date	21 January 2015

Introduction

On December 18th, WatchGuard released an update to Fireware v11.9.4 for all Firebox and XTM device models. This update includes several key bug fixes, as well as:
- OpenVPN components are updated to the latest version to address a memory leak vulnerability (CVE-2014-8104)
- OpenSSL components are also updated to the latest version. Although WatchGuard appliances are not subject to attacks from the latest reported Poodle vulnerability over TLS (CVE-2014-8730), this update also addresses a memory leak vulnerability (CVE-2014-3513)
- Feature key handling has been updated so that all features, including Dynamic Routing, Server Load Balancing, and Policy Based Routing, now work correctly on the new Firebox M400 and M500 devices

See the Resolved Issues section for more information. There is no update available for WatchGuard System Manager, which remains at v11.9.4.

WatchGuard is pleased to announce the release of Fireware v11.9.4 and WatchGuard System Manager v11.9.4. This maintenance release includes several significant enhancements, as well as many bug fixes. Highlights include:

- Expanded hotspot feature functionality now allows you to require users to provide credentials before they can connect to the Internet. When you configure your Firebox or XTM device as a hotspot, you can:
  - Require a user name and passphrase, or just a passphrase
  - Add one or more guest administrators who can manage hotspot users on a dedicated guest administrator web page
  - Print vouchers for hotspot users that include their hotspot user name/passphrase, as well as contact information for questions on their hotspot connection

- SNI-based content inspection for the HTTPS proxy.
  - You can selectively choose to inspect or bypass based on domain name or WebBlocker category.
  - If you currently use HTTPS with deep inspection enabled, we recommend that you review your policies and the What's New in Fireware XTM v11.9.4 presentation to understand what changes occur in your configuration when you upgrade. You now have much more flexibility.
  - All WebBlocker categories are not selected by default.
- Support for the new Firebox M400 and M500 models, both feature 64-bit architecture to support a high number of concurrent connections.
- Updated Linux kernel on XTM 800, XTM 1500, and XTM 2500 devices from 32-bit architecture to 64-bit architecture to enable a higher number of concurrent connections on those devices.
- Ability to configure a BOVPN virtual interface with a local gateway on any internal or external interface.
- Printable Branch Office VPN configuration reports that show BOVPN gateway and tunnel configuration settings.
- Single Sign-On has been updated to support failover and load balancing for the Event Log Monitors installed on multiple domains in your network, in addition to other overall performance improvements.
- Support for a locally installed WatchGuard security subscription service signature server (available on request through your local WatchGuard sales representative).
- SSLv3 is now disabled by default, with an option to turn it on, in response to the POODLE vulnerability.
- Support for /31 and /32 subnets on Firebox or XTM device external interfaces.
- Localized language support in the user interface, updated to XTM v11.9.1.

For more information on bug fixes, see the Enhancements and Resolved Issues section. For more information about the feature enhancements and functionality changes included in Fireware XTM v11.9.4, see the product documentation or review What's New in Fireware XTM v11.9.4.

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, 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 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 XTM 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 XTM OS, you can use your existing feature key. If you use XTMv, your feature key must be generated with the serial number you received when you purchased XTMv.

Note that you can install and use WatchGuard System Manager v11.9.x and all WSM server components with devices running earlier versions of Fireware XTM v11. In this case, we recommend that you use the product documentation that matches your Fireware XTM 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.

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 XTM 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 XTM 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 XTM and WSM v11.9.4 Operating System Compatibility

Last revised: 21 January 2015

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit) & Vista (32 &64-bit)	Microsoft Windows 7, 8, 8.1 (32-bit & 64-bit)	Microsoft Windows Server 2003 SP2 (32-bit)	Microsoft Windows Server 2008 & 2008 R2	Microsoft Windows Server 2012 &2012 R2 (64-bit)	Mac OS X v10.6, v10.7, v10.8, v10.9, v10.10	Android 4.x	iOS v5, v6, 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]			✓ 2	✓	✓			
Terminal Services Agent[3]			✓	✓	✓			
Mobile VPN with IPSec	✓	✓				✓ 4	✓	✓ 4
Mobile VPN with SSL	✓	✓ 5	✓			✓	✓	✓

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.*

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

- *IE 9 and later*
- *Firefox v22 and later*
- *Safari 5 and later*

- *Safari iOS 6 and later*
- *Chrome v29 and later*

[1]Microsoft Exchange Server 2003, 2007, and 2010 are supported.

[2]Exchange Monitor is supported on Windows Server 2003 R2.

[3]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.

[4]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.

[5] Mobile VPN with SSL is supported on Windows 8.1 with an installation workaround described in this Knowledge Base article.

Authentication Support

This table gives you a quick view of the types of authentication servers supported by key features of Fireware XTM. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your 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 XTM 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 XTM 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 Pentium IV 1GHz	Intel Pentium IV 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 or 5.1 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_9_4.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.9.4. There are no updates to WSM with the Update 1 release.

Fireware XTM OS

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

If you have…	Select from these Fireware XTM OS packages
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_11_9_4_U1.exe` `xtm_xtm800_1500_2500_11_9_4_U1.zip`
XTM 2050	`XTM_OS_XTM2050_11_9_4_U1.exe` `xtm_xtm2050_11_9_4_U1.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_9_4_U1.exe` `xtm_xtm800_1500_2500_11_9_4_U1.zip`
XTM 1050	`XTM_OS_XTM1050_11_9_4_U1.exe` `xtm_xtm1050_11_9_4_U1.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_9_4_U1.exe` `xtm_xtm800_1500_2500_11_9_4_U1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_9_4_U1.exe` `xtm_xtm8_11_9_4_U1.zip`
Firebox M500 Series	`Firebox_OS_M400_M500_11_9_4_U1.exe` `firebox_M400_M500_11_9_4_U1.zip`
Firebox M440	`Firebox_OS_M440_11_9_4_U1.exe` `firebox_M440_11_9_4_U1.zip`
Firebox M400 Series	`Firebox_OS_M400_M500_11_9_4_U1.exe` `firebox_M400_M500_11_9_4_U1.zip`
XTM 330	`XTM_OS_XTM330_11_9_4_U1.exe` `xtm_xtm330_11_9_4_U1.zip`
XTM 33	`XTM_OS_XTM33_11_9_4_U1.exe` `xtm_xtm33_11_9_4_U1.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_9_4_U1.exe` `xtm_xtm2a6_11_9_4_U1.zip`
Firebox T10	`Firebox_OS_T10_11_9_4_U1.exe` `firebox_T10_11_9_4_U1.zip`

XTMv
All editions for VMware
	`xtmv_11_9_4_U1.ova`
	`xtmv_11_9_4_U1.exe`
	`xtmv_11_9_4_U1.zip`

XTMv
All editions for Hyper-V
	`xtmv_11_9_4_U1_vhd.zip`
	`xtmv_11_9_4_U1.exe`
	`xtmv_11_9_4_U1.zip`

Single Sign-On Software

These files are available for Single Sign-On. Several of these files were updated with the original v11.9.4 release.

- `WG-Authentication-Gateway_11_9_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_8_1.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_9_3.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_9_3.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_9_3.exe` (This installer includes both 32-bit and 64-bit file support and was updated with the original v11.9.4 release.)

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_9_3.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_9_4.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download. No clients have been updated with this release, but the original v11.9.4 release included an update to the Mobile VPN License Server, disabling support for SSL v3 and enabling multiple license keys to be combined for a single customer.

- `Shrew Soft Client 2.2.0 for Windows` - Shrew Soft has recently released a v2.2.1 client, available on their web site, which introduces a new "Pro" version available at an extra cost with additional features. WatchGuard recommends you use the no-cost Standard version of the client as it includes all functionality supported in the v2.2.0 VPN client. If you want to use the v2.2.1 client, we recommend you read this Knowledge Base article first.
- `WatchGuard IPSec Mobile VPN Client for Windows, 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 (MVLS) v2.0, powered by NCP` - Click here for more information about MVLS.

WatchGuard AP Firmware

If you manage WatchGuard AP devices and your Gateway Wireless Controller is enabled to update these devices automatically, your AP devices will be upgraded to new firmware when you upgrade your XTM device to XTM OS v11.9.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-v1.2.9.2.bin`
- `AP200-v1.2.9.2.bin`

Upgrade Notes

In addition to new features and functionality introduced in Fireware XTM v11.9.x.releases, these releases also changes the functionality of several existing features in ways that you need to understand before you upgrade. In this section, we review the impact of some of these changes, as well as highlight several known issues related to upgrading.

- Because of changes associated with SNI-based content inspection with the HTTPS proxy, it is important to understand that, when you upgrade to v11.9.4:
  - Any IP addresses on the Bypass List will be converted to a Domain Names rule with the action of **Allow** and the **Action to take if no rule above is matched** set to **Inspect** if the previous action was **Allow**. The Bypass List applies to devices that run XTM v11.9.3 or lower only.
  - Any entries in the Certificate Names list will be converted to equivalent rules in the Domain Names rule list.
- Because many features in Fireware XTM v11.9.x operate very differently than in previous versions and Policy Manager can manage devices that use different versions of Fireware XTM OS, you must now select the Fireware XTM version the device uses before you can configure some features. In Policy Manager, go to **Setup > OS Compatibility** to select a version.
- The Mobile VPN with SSL **Bridge VPN Traffic** option now requires that you first configure a network bridge. When you upgrade to v11.9 or higher, if Mobile VPN with SSL was configured to bridge VPN traffic to an interface, the upgrade process automatically creates a new bridge that includes the interface.
- Previously, you had to associate your wireless interface with your trusted or optional interface (or use the wireless guest network). When you upgrade, a network bridge is created that has the trusted or optional interface and the wireless interface as members. After you upgrade, make sure to verify your wireless policies meet the needs of your network. If you use Centralized Management, see this Knowledge Base article for important information about this upgrade.
- Because the redesigned traffic management feature works differently than in previous versions, when you upgrade a configuration from 11.8.x or lower to 11.9 or higher, any existing traffic management actions are removed.

Upgrade from Fireware XTM v11.x to v11.9.4 Update 1

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.9.4 Update 1, download and save the Fireware XTM OS file that matches the WatchGuard device 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 device 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 XTM OS installed on your XTM device and the version of WSM installed on your Management Server. Also, make sure to upgrade WSM before you upgrade the version of XTM OS on your XTM device.

If you have already installed Fireware v11.9.4 on your computer, you must run the Update 1 installer twice (once to remove v11.9.4 and again to install v11.9.4 Update 1).

If you use an XTM 5 Series or 8 Series device, you must upgrade to Fireware XTM v11.7.4 or v11.7.5 before you can upgrade to Fireware XTM v11.9.x.

We recommend that you reboot your XTM device before you upgrade. While this is not necessary for most higher-model XTM devices, a reboot clears your XTM device memory and can prevent many problems commonly associated with upgrades in XTM 2 Series, 3 Series, and some 5 Series devices.

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 v11.9.x. You can install the v11.9.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, or WatchGuard Dimension Log Server) before you upgrade. You 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 XTM v11.9.x from Web UI

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 *[xtm series]_[product code].sysa-dl* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.9\[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\FirewareXTM\11.9
3. Connect to your XTM device with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the *[xtm series]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

Upgrade to Fireware XTM v11.9.x from WSM/Policy Manager v11.x

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 *[xtm series]_[product code].sysa-dl* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.9\[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\FirewareXTM\11.9
3. Install and open WatchGuard System Manager v11.9.4. Connect to your XTM device and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[xtm series]_[product code].sysa-dl* file from Step 2.

Upgrade your FireCluster to Fireware XTM v11.9.x

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

If you use an XTM 5 Series or 8 Series device, you must upgrade your FireCluster to Fireware XTM v11.7.4 or v11.7.5 before you can upgrade your FireCluster to Fireware XTM v11.9.x.

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 with the Web UI.

Upgrade a FireCluster from Fireware XTM v11.4.x–v11.8.x to v11.9.x

Use these steps to upgrade a FireCluster to Fireware XTM v11.9.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 XTM v11.3.x

To upgrade a FireCluster from Fireware XTM v11.3.x to Fireware XTM v11.9.x, you must perform a manual upgrade. For manual upgrade steps, see the Knowledge Base article Upgrade Fireware XTM OS for a FireCluster.

Downgrade Instructions

Downgrade from WSM v11.9.x to WSM v11.x

If you want to revert from v11.9.x to an earlier version of WSM, you must uninstall WSM v11.9.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 v11.9.x.

Next, install the same version of WSM that you used before you upgraded to WSM v11.9.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 v11.9.x. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.9.x to Fireware XTM v11.x

If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.9.x to an earlier version, the downgrade process resets the network and security settings on your XTM 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 XTM v11.9.x to an earlier version of Fireware XTM, the recommended method is to use a backup image that you created before the upgrade to Fireware XTM v11.9.x. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.9.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 *WatchGuard System Manager Help* or the *Fireware XTM Web UI 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 M440 to a version of Fireware lower than v11.9.2.
- 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 XTM OS on your 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 XTM OS.

Enhancements and Resolved Issues in Fireware v11.9.4 Update 1

- This release patches the OpenVPN component of Fireware to address vulnerability CVE-2014-8104. *[83478]*
- This release updates the OpenSSL version of Fireware to 1.0.1j to address CVE-2014-3513. *[83498]*
- This release updates the OpenSSL version of Fireware to 1.0.1j to address the POODLE vulnerability on TLS TA14-290A. *[83594]*
- The Firebox DB user list now displays correctly in the Web UI. *[82938]*
- Domain Name rules in the HTTPS Proxy configured with the action of *Block* will no longer add the client host to the Blocked Sites list. *[83412]*
- HTTPS proxy exceptions for Content Inspection by Domain Name now correctly override rules for Content Inspection by WebBlocker Category. *[83274]*
- The Web Setup Wizard now completes correctly when using the Web UI in Japanese. *[83315]*
- All proxy rules now load correctly after a reboot when the configuration contains a large number of policies. *[83413]*
- This release resolves an issue that caused Branch Office VPN traffic to fail after a VPN re-key event. *[82440]*
- This release resolves several crash issues, including:
  - An *IKED* process crash that resulted in all IPSec VPN tunnels failing. *[83179]*
  - A spamBlocker *spamd* process crash. *[82796]*
  - A wireless driver crash and failure of all wireless traffic. *[82769]*
  - A scand process crash when using Data Loss Prevention. *[83299]*
  - A *wgagent* process crash that prevented management connections. *[83022]*
- IPv6 traffic is now handled correctly when the **Log traffic from firewall** option is selected in the v11.9.4 configuration. *[83419]*
- An issue has been resolved that prevented an external interface configured with PPPoE from reconnecting for up to five minutes under certain conditions. *[83239]*

Enhancements and Resolved Issues in WSM/Fireware v11.9.4

General

- In response to the recent “Poodle” vulnerability, this release disables support for SSLv3 for HTTPS connections to the Firebox XTM Web UI. *[82823]*
- You can now change the order of the IP addresses you add to the Management Server CRL Distribution IP address list. *[78662]*
- This release resolves a CPU crash which occurred in v11.9.3. *[82348, 82700]*
- This release resolves a crash in the WGagent process that handles management connections to XTM or Firebox devices. *[83079]*

WatchGuard System Manager

- This release resolves an issue that occurred in WatchGuard System Manager v11.9.3 that prevented management of Firebox e-Series devices. *[82670]*
- WatchGuard System Manager (WSM) can now be installed for *All Users* in addition to the user installing WSM. *[81916]*
- WatchGuard System Manager > Policy Manager will no longer disable an interface if the interface name is the same as a newly created Interface Bridge, VLAN or Link Aggregation. *[82366]*

Web UI

- When using the Web UI, the password used for the AD/LDAP Searching User is no longer shown in clear text. *[82183]*
- You can now enable alarms for Subscription Services from the Web UI. *[82848]*

Logging and Reporting

- The unnecessary log message `scan_wg: failed to calculate MD5 hash for file` no longer appears in the log file. *[82036]*
- This release reduces the occurrence of the unnecessary log message `xt_wgaccount: wgact_get: Invalid policy ID XXX requested.` *[74936]*
- This release resolves an issue that prevented Traffic Monitor from displaying some DNS proxy log messages. *[82290]*

Proxies

- This release resolves several proxy process crashes. *[81811, 82091,82665,82196,82131,808871]*
- SIP invite requests are no longer dropped by the SIP-ALG when a VoIP call is put on hold. *[81794]*
- SIP-ALG custom policies for UDP now work correctly. *[79592]*
- This release resolves a memory leak when using the SIP-ALG. *[82764]*
- This release improves processing for RTP media connections when you use the SIP-ALG. *[82367]*
- You can now correctly enable and disable the individual policy diagnostic logging level for the TCP-UDP proxy. *[81846]*
- When you enable per Proxy Policy diagnostic logging for HTTPS Content Inspection, diagnostic logging for all HTTPS proxy policies with Content Inspection is no longer enabled. *[82374]*
- The SMTP proxy now correctly logs the recipient email addresses when multiple emails are sent through the same SMTP connection. *[82359]*
- This release resolves an issue that prevented some mail from passing through the SMTP proxy when the ESMTP BDAT option is enabled. *[59850]*

- Mail delivery in plain text no longer fails when TLS is enabled for the SMTP proxy and encryption is configured as optional-preferred. *[79344, 82712]*
- This release resolves an issue that prevented some TLS 1.0 and 1.1 transactions from completing successfully through the HTTPS proxy. *[82856]*
- The HTTP proxy no longer fails to pass traffic when you use a custom deny message that includes some problematic tags, such as <script>. *[78700]*
- A problem has been resolved that caused FTP data transfers to fail through an FTP proxy policy configured for 1-to-1 NAT. *[77218]*

Security Subscription Services

- This release resolves a memory leak that occurred when using the WebBlocker Override feature. *[82441,82442]*
- This release resolves an issue that caused the scand process used for Gateway AV to crash and restart. *[82047,82770]*
- The Quarantine Server now correctly displays German Umlaut and Cyrillic characters in the email subject line. *[82763]*
- When using the Quarantine Server, the error “Grid cannot be displayed in Quirks mode” no longer occurs. *[82706]*
- This release resolves an issue that caused large Zip files to corrupt when using IPS. *[82469]*

Networking

- Blocked sites now correctly handle duplicate entries where a CIDR entry and an IP range are within the same subnet. *[75696]*
- Secondary IP addresses now respond correctly to ARP request when your Firebox or XTM device is configured in drop-in mode. *[78329]*
- You can now use aliases that include IPv6 addresses in your Dynamic NAT configuration.*[81406]*
- Static routes now operate correctly when your device external interface is configured to use PPPoE. *[81490]*

VPN

- The Mobile VPN for SSL Mac client has been improved to allow the DNS server setting to stay in use after shutdown or hibernate events. *[75670]*
- VPN failover now works correctly when an IPSec Management Tunnel and a Branch Office VPN tunnel exist between two devices. *[82867]*

WatchGuard AP

- This release resolves an issue that prevented the AP 100/200 from correctly connecting to a Firebox T10 device when directly connected to a VLAN interface. *[82831]*

Known Issues and Limitations

Known issues for Fireware XTM v11.9.4 and its management applications, including workarounds where available, can be found in the WatchGuard Knowledge Base. Note that you must log in to the WatchGuard Portal to see Known Issues. Known Issues are not available in the public version of the Knowledge Base. We recommend that you use the filters available on the WatchGuard Portal > Knowledge Base tab to find Known Issues for Fireware XTM v11.9.x releases.

Using the CLI

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

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