Fireware XTM v11.9.1 Release Notes

Supported Devices	XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 Firebox T10, XTMv, WatchGuard AP
Fireware XTM OS Build	451786
WatchGuard System Manager Build	451850
Release Notes Revision Date	11 November 2014

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.9.1 and WatchGuard System Manager v11.9.1.

On June 5th the OpenSSL team released a critical update to patch six vulnerabilities affecting all versions of the OpenSSL libraries that are widely used in networking applications today. The most serious of the vulnerabilities is a Man-in-the-Middle (MitM) flaw that could allow an attacker to intercept traffic if both the client and server are vulnerable. This release includes the patch for both Fireware XTM OS and the Mobile VPN with SSL client to resolve the issue. Unlike the earlier Heartbleed vulnerability, no certificate updates are required once the patch is installed. More details about the vulnerabilities are posted at the WatchGuard Security Center. If you are not already subscribed to this blog, we recommend that you sign up now to always stay current with breaking news about security vulnerabilities and any impact on WatchGuard products.

This release also includes numerous bug fixes and minor feature updates, including:

- New alert and wizard to help new customers make sure have a feature key installed on their device
- Improved XTM Configuration Report
- Option to remember Mobile VPN with SSL client password
- Support for Spring u301 3G/4G USB modem
- Support for the Firebox or XTM default gateway to be on a different subnet that its external interface
- Ability to run the SSO Agent and Event Log Monitor as a member of the Domain Users or Domain Admin group

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 v11.9.1, see the product documentation or review What's New in Fireware XTM v11.9.1.

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, 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 updated, localized management user interfaces (WSM application suite and Web UI). The user interface has been updated with content for Fireware XTM v11.8. Supported languages are:

- Chinese (Simplified, PRC)
- French (France)
- Japanese
- Spanish (Latin American)

The Web UI is not localized for this release.

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.

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 v11.9.1 Operating System Compatibility

Revised May 2014 with the release of v11.9

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	Android 4.x	iOS v5, v6 & v7
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 and 10.9, 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

To download software:

1. Go to the WatchGuard Software Downloads page.
2. Select the Firebox or XTM device for which you want to download software.

There are several software files available for download. 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_1.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.9.1.

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_1.exe` `xtm_xtm800_1500_2500_11_9_1.zip`
XTM 2050	`XTM_OS_XTM2050_11_9_1.exe` `xtm_xtm2050_11_9_1.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_9_1.exe` `xtm_xtm800_1500_2500_11_9_1.zip`
XTM 1050	`XTM_OS_XTM1050_11_9_1.exe` `xtm_xtm1050_11_9_1.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_9_1.exe` `xtm_xtm800_1500_2500_11_9_1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_9_1.exe` `xtm_xtm8_11_9_1.zip`
XTM 5 Series	`XTM_OS_XTM5_11_9_1.exe` `xtm_xtm5_11_9_1.zip`
XTM 330	`XTM_OS_XTM330_11_9_1.exe` `xtm_xtm330_11_9_1.zip`
XTM 33	`XTM_OS_XTM33_11_9_1.exe` `xtm_xtm33_11_9_1.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_9_1.exe` `xtm_xtm2a6_11_9_1.zip`
Firebox T10	`XTM_OS_T10_11_9_1.exe` `firebox_T10_11_9_1.zip`

XTMv
All editions for VMware
	`xtmv_11_9_1.ova`
	`xtmv_11_9_1.exe`
	`xtmv_11_9_1.zip`

XTMv
All editions for Hyper-V
	`xtmv_11_9_1_vhd.zip`
	`xtmv_11_9_1.exe`
	`xtmv_11_9_1.zip`

Single Sign-On Software

For Single Sign-On (SSO) capability in a Windows Active Directory Domain. Agent requires the Microsoft .NET Framework v2.0 –4.5 or later. These files are available for Single Sign-On. The SSO Agent software has been updated in the v11.9.1 release.

- `WG-Authentication-Gateway_11_9_1.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_9.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_8_1.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_9.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_9.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

For User Authentication in Terminal Services or Citrix XenApp Environments.

- `TO_AGENT_SETUP_11_9_1.exe` (This installer includes both 32-bit and 64-bit file support and has been updated for the XTM v11.9.1 release.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL. Both clients are updated for the XTM v11.9.1 release.

- `WG-MVPN-SSL_11_9_1.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_9_1.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are three available files to download. No clients have been updated with this release.

- `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 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 one previous version of AP firmware on this page for recovery purposes only. The file names for the latest AP firmware are:

- `AP100-v1.2.9.1.bin`
- `AP200-v1.2.9.1.bin`

Upgrade Notes

In addition to new features and functionality introduced in Fireware XTM v11.9, this release 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 many features in Fireware XTM v11.9 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, 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, any existing traffic management actions are removed.
- If you use multi-WAN configured in round-robin, interface overflow, or failover mode together with a hotspot associated with an interface configured as a LAN bridge, hotspot traffic will not pass through that interface after you upgrade to Fireware XTM v11.9. *[80532]*
- If you have Mobile VPN with SSL configured to bridge to the FireCluster Interface for Management IP Address, the FireCluster backup master will temporarily fail to join the cluster after reboot, and you will see an error message "`The cluster does not have a backup master. Continuing with the upgrade may result in service disruption through the cluster. Do you want to continue?`" If you click **Yes** to continue, the upgrade will successfully complete. *[80464]*

Upgrade from Fireware XTM v11.x to v11.9.1

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.9.x, 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 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 v11.9.1. 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.

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 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

General

- This release contains patches to OpenSSL version used in the appliance and the Mobile VPN with SSL client. The patch addresses the following OpenSSL advisories CVE-2014-0195, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470.
- This release resolves a Kernel vulnerability tracked under CVE-2014-0196. *[80741]*
- Firebox System Manager and the WSM Device Status tab now show the Fireware XTM OS build number for each connected device. *[65052]*
- The user interface used to create a device backup image has been improved to explain the encryption key. *[80119]*
- Policy Manager no longer displays the warning message "The OS version running on the device does not support DHCP Authentication and Force Renew IP address" when saving a configuration to a Firebox e-Series device running v11.3.x. *[80232]*
- The Report Manager > Servers list now displays correctly. *[73530]*
- You can now use private domain names (domain names without a public suffix) in the Web UI. *[79660]*
- Syslog now works correctly after you upgrade to v11.9.x when the syslog facility of "none" was used in your configuration. *[80751, 79593]*
- This release resolves an issue that prevented policy schedule intervals from saving correctly when using the Web UI. *[80578]*
- The ability to configure more than 32 MAC address reservations is now available for the AP100, AP102 and AP200 wireless access points. *[79335]*
- This release resolves an issue that caused the auto policy ordering in the Web UI to be different than Policy Manager when aliases or non-default interface names were used. *[74657]*

Proxies and Subscription Services

- This release resolves an issue that caused traffic to fail when using the HTTP Proxy with WebBlocker. When the issue occurred, this error showed in the log file: `err webblocker[1903]: scan_wb: no profile found`. *[80315]*
- This release resolves an issue that caused AV scanning and APT scanning to fail. *[80799]*
- Several issues related to the use of inbound HTTPS content inspection have been resolved in this release. *[79235, 75725]*
- This release resolves several issues in which HTTPS web sites did not load correctly when using HTTPS content inspection. *[80538, 80569]*
- Several improvements were made to SIP ALG to improve one way audio during VoIP calls.*[79962, 79311, 80385, 38567, 70349]*
- This release provides improvements to Application Control detection when not using HTTPS proxy with content inspection. *[81008, 80885, 81037]*
- When using the Quarantine Server, Japanese characters now display correctly in email notifications and in the Quarantine Server Web UI. *[79082]*

- This release resolves several proxy process crashes. *[78665, 80951,79579, 77948, 80800, 79314, 78665, 78828, 79314]*
- Mobile VPN with SSL connections using WatchGuard's SSLVPN client or OpenVPN client are no longer blocked by the HTTPS proxy. *[77969]*
- HTTPS sessions started from Internet Explorer v10 or higher on Windows 8 now establish more quickly when using an HTTPS proxy. *[78793]*
- A memory leak has been resolved that occurred when large files were transferred through the FTP proxy. *[79643]*
- This release resolved a kernel crash that occurred when IPS or Application Control is enabled. *[79832]*
- WebBlocker Override now works correctly through a BOVPN zero route. *[76007]*
- The HTTP proxy now correctly sends byte count data to the log file for data transfers larger than 4GBs. This improves the reporting on bandwidth usage. *[79421]*
- When you configure a SIP ALG policy with inbound static NAT in environments where external devices register through the Firebox or XTM device to an internal PBX, RTP traffic no longer causes the SIP ALG to crash and RTP connections to fail. *[79953]*
- This release resolves an issue that prevented inbound SMTP traffic using TLS from working correctly after a v11.9 upgrade. *[80694]*
- This release resolves an issue that caused the an FTP Proxy policy configured for 1-to-1 NAT traffic to not transfer any data. *[77218]*

Authentication

- Active Directory group names are no longer incorrectly truncated when they include the text "async" or "event". *[79669]*
- The supported number of SSO exceptions you can add to your configuration has been increased from 64 to 128 per category. *[78746]*
- You can now run the SSO Agent and Event Log Monitor as a user account that is a member of either Domain Users or Domain Admin group. *[77480]*
- A problem that prevented failover to a backup Event Log Monitor has been resolved. *[81052]*

Networking

- If you use multi-WAN configured in round-robin, interface overflow, or failover mode together with a hotspot, hotspot traffic now uses the correct interface after you upgrade to Fireware XTM v11.9.x. *[80532]*
- A device configured in drop-In mode now correctly responds to an ARP request sent to a unicast address. *[79010]*
- This release resolves a `networkd` process crash. *[80440]*
- You can now correctly get access to a FireCluster member when using the Leave command. *[80459]*
- In FireWatch, the average duration time of a FireCluster connection is now accurate. *[80376]*
- FireCluster now supports a configuration with all interfaces set to VLAN, Bridge, or Link Aggregation. *[80441, 79795]*
- The Management Server now creates the Trusted and Optional network resources for an interface configured as a Bridge interface. *[56716]*
- You can now save your configuration to your Firebox or XTM device after you use Policy Manager to delete a bridge interface that has a wireless interface as a member. *[80501]*
- After you use the CLI to disable an IPv6-enabled network interface, Firebox System Manager no longer shows the error message `Invocation TargetException`. *[80390]*
- If you select the gradual failback as the multi-WAN failback for active connection settings, failback no longer occurs immediately. *[63932]*

- This release includes improvements to correctly route traffic through proxy policies using the correct multi-WAN interface when handling IPSec and SSL-based zero-route traffic from remote or branch office users. *[78947, 80309, 78814]*
- If you upgrade an active/passive FireCluster from a Windows host with an ARP cache time-out greater than four minutes, Policy Manager no longer shows an unnecessary warning. *[80114]*
- Multi-WAN interface down email notification now works correctly when the Log Server is external to the Firebox or XTM device. *[76898]*
- This release resolves an issue that prevented SMTP relay traffic from working correctly in a multi-WAN environment. *[80997]*
- You can now use a /23 subnet for a DHCP reservation. *[79269]*
- When you configure Dynamic Routing with OSPF for a Branch Office VPN virtual interface, OSPF may fail to learn routes if one of the VPN endpoints uses PPPoE or another Internet connection with an MTU setting lower than 1500. *[81226]*

Workaround
You can avoid this issue if you add these two lines to the OSPF configuration on each Firebox or XTM device:

```
interface bvpnX [replace X with the virtual interface number]
ip ospf mtu-ignore
```

VPN

- When you configure a 1-to-1 NAT rule with a NAT Base IP address that matches the IP address of the external interface, inbound traffic across any VPN that uses that external interface may fail. *[64766]*
- A branch office VPN tunnel no longer appears to be down after a Phase 1 rekey until traffic is sent through the tunnel. *[80609]*
- The Mobile VPN with SSL Mac client now supports the option to remember the user's password between sessions. *[80194]*
- Traffic now routes correctly through a BOVPN virtual interface when multiple external interfaces are configured. *[79026, 79948, 79791]*
- When a BOVPN virtual interface zero route has a routing metric lower than the default route, policy-based routing no longer sends traffic through the BOVPN virtual interface instead of the configured external interface. *[79339]*
- Firebox System Manager and the Web UI now display warning messages when the active Branch Office VPN tunnel count or current Mobile VPN with IPSec user count reaches the licensed maximum. *[71380]*
- The Mobile VPN with SSL client fails to connect on a Windows 8.1 client computer due to a failure of the TAP driver. *[79060]*

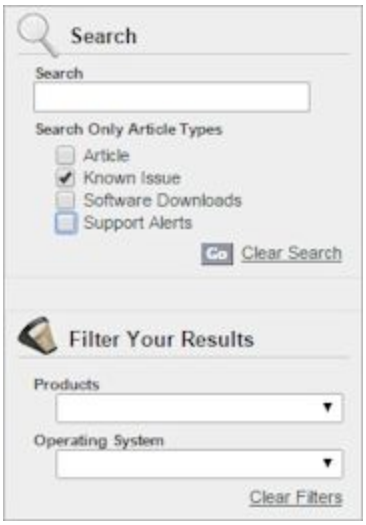
Workaround
Install the free OpenVPN Portable VPN client, which includes the TAP driver that works with Windows 8.1. Then reinstall the WatchGuard Mobile VPN with SSL client without the TAP driver. See this Knowledge Base article for more information about the workaround.

- The certificate used for Mobile VPN with SSL is no longer corrupted after you upgrade from v11.8.3 or older releases. *[80910]*

- If you have Mobile VPN with SSL configured to bridge to the FireCluster Interface for Management IP Address, the FireCluster backup master now correctly joins the cluster after reboot. *[80464]*
- DNS now works correctly after using the Mobile VPN with SSL Mac client on a computer that was not shut down correctly. *[75670]*
- The ability to disable allowed traffic logging is now available for the auto-created DVCP-Allow-SSLVPN-Mgmt policy created for SSLVPN management tunnels. *[79366]*

Known Issues and Limitations

You can find information about known issues for Fireware XTM v11.9.1 and its management applications, including workarounds where available, in the WatchGuard Knowledge Base. You must log in to the WatchGuard Portal to search for Known Issues. Known Issues are not available in the public version of the Knowledge Base. After you log in, you can use the filters available in the WatchGuard Portal > Knowledge Base tab to find articles about known issues for this release.



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