Fireware XTM v11.9 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	448467
WatchGuard System Manager Build	448586
Revision Date	20 March 2015

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.9 and WatchGuard System Manager v11.9.

Many new features, feature enhancements, and bug fixes have been included in this release, including:

APT Blocker

Detect and stop zero day threats that signature based solutions miss. The new UTM service sends Windows executable files, Microsoft Office, and PDF files to run in a cloud-based sandbox to look for malware characteristics, including multiple types of evasive behavior. APT Blocker is integrated closely with WatchGuard Dimension to provide logs, proactive alerts, and full visibility into why a file is detected as malware.

Redesigned Traffic Management

Control and limit bandwidth use for applications, application categories, IP addresses, guest wireless access, and VLANs. With this update to Traffic Management, you can preserve expensive Internet bandwidth for those business critical applications that truly need it, and limit the use of streaming media, games, and other resource-intensive applications.

Increased Compliance with Industry-Standards (PCI, HIPAA, etc.)

- Expanded authentication and auditing options for administrative users of the XTM appliances.
- New custom DLP signatures let you create your own text-based patterns to detect and prevent the loss of critical company information.
- Integration with IBM's industry leading SIEM system, QRadar.
- New custom network zone lets you easily segregate wireless guest networks, as required by the PCI standard on appliances with integrated wireless.

VPN Enhancements

- Ability to enable and disable VPN Gateways and Tunnels.
- Support for Diffie-Hellman Group 14 and 15, and Elliptic Curve Diffie-Hellman Group 19 and 20.
- Ability to add IPv6 routes to a BOVPN virtual interface. With this functionality, two IPv6 networks can get access to each other through an IPv4 VPN tunnel.

- 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.
- Other Mobile VPN with SSL enhancements, including:
  - Domain list on the Mobile VPN with SSL authentication page
  - Mobile VPN with SSL automatic reconnect setting

FireCluster Enhancements

- Active/passive FireCluster support for static PPPoE external IP addresses.
- You can now select which interfaces to monitor for active/passive FireCluster member health.
- You can now connect to a FireCluster with the Fireware XTM Web UI, and make any type of configuration change you could make to a non-clustered device.

Wireless XTM Device Enhancement

- You can now configure an XTM wireless interface as an independent interface in any security zone.
- More flexibility in configuration of your wireless guest network.

WatchGuard AP Enhancements

- New Wireless Deployment Map provides interactive, graphical wireless coverage information to help you quickly achieve the optimal arrangement and configuration of wireless access points in your buildings.
- Better control over DFS and channel limitations, transmit rate and power control for WatchGuard Access Points.
- Support for the new AP 102 indoor/outdoor access point.

Other New Features and Feature Enhancements

- IPv6 support for link aggregation, bridge, and VLAN interfaces.
- IPv6 support for dynamic routing.
- New Gateway AV signature set for XTM 2 Series, 3 Series, and XTM 505/510/520/530 Series devices to provide greater malware detection capabilities
- Gateway AV now automatically scans file uploads, using the same rules you have configured in your proxy policies for file downloads.
- Enhanced device reporting functionality to help WatchGuard collect device usage statistics from deployed devices.
- Updated ECMP algorithm used for the Multi-WAN Routing Table mode and for OSPF so that correct interfaces are used based on the source and destination IP address of the traffic flow.
- Phone factor authentication support, with a new timeout setting for authentication requests.

Because this release includes several significant changes to existing functionality, we recommend you carefully review the Upgrade Notes section carefully before you upgrade. For more information on the bug fixes included in this release, see the Resolved Issues section. For more information about the feature enhancements included in Fireware XTM v11.9, see the product documentation or review What's New in Fireware XTM v11.9.

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 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 a localized management user interface for the WSM application suite, current to Fireware XTM v11.7.2. Updates will be available at a later date. There is no localization for the Web UI in this release. For WSM, 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. Any software components provided by third-party companies remain in English.

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.

Localized Help for Fireware XTM v11.7.2 is available on the WatchGuard Documentation web site.

Fireware XTM and WSM v11.9 Operating System Compatibility

Revised May 2014

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	✓	✓	✓			✓	✓	✓

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.

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

1. Log in to the WatchGuard Portal and select the Articles & Software tab.
2. From the Search section, clear the Articles and Known Issues check boxes and search for available Software Downloads. Select the 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.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.9.

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.exe` `xtm_xtm800_1500_2500_11_9.zip`
XTM 2050	`XTM_OS_XTM2050_11_9.exe` `xtm_xtm2050_11_9.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_9.exe` `xtm_xtm800_1500_2500_11_9.zip`
XTM 1050	`XTM_OS_XTM1050_11_9.exe` `xtm_xtm1050_11_9.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_9.exe` `xtm_xtm800_1500_2500_11_9.zip`
XTM 8 Series	`XTM_OS_XTM8_11_9.exe` `xtm_xtm8_11_9.zip`
XTM 5 Series	`XTM_OS_XTM5_11_9.exe` `xtm_xtm5_11_9.zip`
XTM 330	`XTM_OS_XTM330_11_9.exe` `xtm_xtm330_11_9.zip`
XTM 33	`XTM_OS_XTM33_11_9.exe` `xtm_xtm33_11_9.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_9.exe` `xtm_xtm2a6_11_9.zip`
Firebox T10	`XTM_OS_T10_11_9.exe` `firebox_T10_11_9.zip`

XTMv
All editions for VMware
	`xtmv_11_9.ova`
	`xtmv_11_9.exe`
	`xtmv_11_9.zip`

XTMv
All editions for Hyper-V
	`xtmv_11_9_vhd.zip`
	`xtmv_11_9.exe`
	`xtmv_11_9.zip`

Single Sign-On Software

Most Single Sign-On software has been updated for v11.9:

- `WG-Authentication-Gateway_11_9.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

- `TO_AGENT_SETUP_11_9.exe` (This installer includes both 32-bit and 64-bit file support and has been updated for the XTM v11.9 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 release.

- `WG-MVPN-SSL_11_9.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_9.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are three available files to download. Both WatchGuard IPSec Mobile VPN 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 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

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

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. You can install the v11.9 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 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 Center.
   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 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. 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

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 before you can upgrade your FireCluster to Fireware XTM v11.9.

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 with the Web UI.

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

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, 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 to WSM v11.x

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

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

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

If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.9 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 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. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.9 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.

Resolved Issues

- OpenSSL has been upgraded to v1.0.1g in this release. *[80065]*
- The DHCP server now responds to DHCP Option 50 requests from DHCP clients. *[66321]*
- You can now generate an SNMP trap when a Firebox or XTM device is rebooted or powered on. *[66012]*
- SNMP MIB OID support for Firebox or XTM device software version information. *[66395]*
- WatchGuard System Manager now displays the correct IP address for the default gateway of an XTM device that has no External interface. *[56385]*
- This release offers improved performance for customers who use both global QoS and Traffic Management. *[61143]*
- You can now successfully save a configuration with more than 10 VLANs to an XTM 1520-RP with Policy Manager. *[79920]*

Proxies and Subscription Services

- This release resolves several proxy stability issues. *[80328, 78819, 78217, 78664, 70366, 78667, 78731, 78932]*
- This release resolves several issues in which HTTPS web sites did not load correctly when using HTTPS Content Inspection. *[77987, 78807, 78939]*
- This release resolves an issue that caused excessive CPU use when using the SMTP proxy with TLS. *[80328, 79733]*

Networking

- You can now configure static ARP entries in the Web UI.*[80146]*
- You can now add static ARP entries for Bridge, VLAN, and Link Aggregation interfaces. *[80130]*
- You can now configure traffic management actions on VLANs. *[56971]*

Wireless

- You can now bridge a wireless interface to a VLAN interface. *[41977]*
- If a connection from a user on the Wireless Guest Network matches a policy with Any-Trusted in the From field, that connection is now handled by the correct policy. *[69328]*

Authentication

- Exchange Monitor now works correctly in an active/active Exchange cluster environment. *[75892]*
- Authentication now works correctly when the authentication server is located at the remote end of a BOVPN virtual interface. *[75714]*
- If you use Active Directory (AD) authentication for Terminal Services users, a mismatch in capitalization (case) between the domain name configured in **Setup > Authentication > Servers** and your actual AD server no longer causes a failure to apply policies correctly to the users. *[72721]*
- The SSO Client can now retrieve full group membership in an Active Directory environment. *[77805]*
- The SSO Client now correctly handles user sessions when a user logs in an then locks their computer, and then remotely logs in to the computer and locks the computer again. *[77415]*

- The SSO Agent can now distinguish telnet logins from appliance logins. *[78669]*
- The SSO Agent installer now correctly recognizes .NET 4.0 and higher installations. *[79078]*
- The SSO Agent now correctly refreshes the user cache. *[78495]*
- It is now easier to view and manage log messages for each SSO component because messages are now stored in a separate log file for each component, with a backup file for each. Files are compressed for easier storage and up to 30 compressed files are kept at a time. *[42864]*

VPN

- Firebox T10, XTM 25, 26, 33, and 330 devices now proactively start branch office VPN tunnel negotiations whenever the connection to a remote gateway is down. *[79959]*
- The L2TP configuration now syncs correctly from a master XTM device to a backup XTM device in an active/passive FireCluster. *[69776]*
- In a Branch Office VPN virtual interface configuration, if both the local and remote gateways are configured to use policy-based routing (with no zero route), traffic now routes correctly through the tunnel. *[76779]*
- Manual Branch Office VPNs now work correctly when the pre-shared key exceeds 50 characters. *[65215]*
- When a VPN tunnel is first initiated, the XTM device now correctly sends an "icmp destination unreachable" message back to the computer that initiated the tunnel. *[72199]*
- You cannot configure Mobile VPN with SSL to bridge network traffic to a bridged interface. *[61844]*

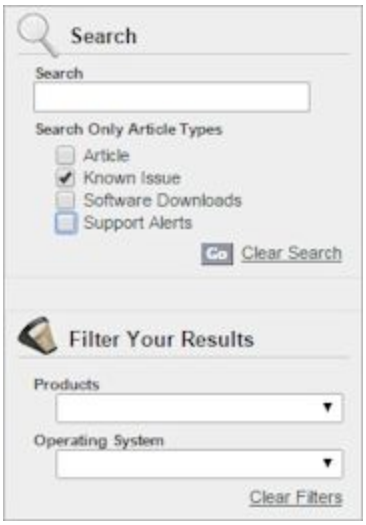
WatchGuard AP

- The AP device supports a new LED pattern to indicate pairing status. The Power LED flashes red and green on an unpaired AP device. *[77891]*
- You can now disable LEDs on an AP device, or cause the Power LED to flash green for easy AP device identification. *[77772]*
- You can now restart the wireless process on an AP device to trigger automatic channel selection without a reboot. *[76613]*
- You can now restrict an AP device to use only outdoor channels. *[78593]*
- You can now disable DFS channels to ensure maximum channel reliability in a noisy environment. *[77217]*
- SSH is now disabled by default for AP devices, with a new global setting to enable it for all AP devices under management. *[71739]*
- You can now control the Transmit Rate and Transmit Power on an AP device radio. *[71610, 77645]*

Known Issues and Limitations

Known issues for Fireware v11.9.x 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 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