Fireware XTM v11.8.4 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	451833
WatchGuard System Manager Build	N/A *You must use WatchGuard System Manager v11.9.1 to manage a device running v11.8.4.*
Revision Date	11 November 2014

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.8.4.

The minor feature enhancements and bug fixes included in this release have been carefully chosen to improve the efficiency, performance, and reliability of your WatchGuard network security devices. For more information on the bug fixes included in this release, see the Enhancements and Resolved Issues section.

This release also includes updated localization for the Fireware XTM Web UI, as described in the Localization section.

There is no update to WatchGuard System Manager (WSM) with this release. If you use WSM to manage your Firebox or XTM device, you must use WSM v11.9.x to manage a device running Fireware XTM v11.8.4.

Before You Begin

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

- A supported WatchGuard XTM device. This device can be a Firebox T10, WatchGuard 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 device — If you upgrade your Firebox or XTM 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 v11.8.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 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 localization update to the Fireware XTM Web UI. The Web UI has been localized current to Fireware XTM v11.8.4. There is no localization available for WatchGuard System Manager, or the product documentation, with this release. Localization for WatchGuard System Manager is available with v11.9.1, currently available.

The Web UI is available in:

- Chinese (Simplified, PRC)
- Chinese (Traditional)
- French (France)
- Japanese
- Korean
- 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.

Fireware XTM and WSM v11.8.4 Operating System Compatibility

Revised February 2014. There are no new changes with v11.8.4.

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 (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 OS 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

There is no release of WatchGuard System Manager with Fireware XTM v11.8.4. To manage a device running v11.8.4, you must use WatchGuard System Manager v11.9.x or the Web UI.

Fireware XTM OS

Select the correct Fireware XTM OS image for your Firebox or XTM device. Use the .exe file if you want to install or upgrade the OS using WSM. Use the .zip file if you want to install or upgrade the OS using the Fireware XTM Web UI. Use the .ova 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_8_4.exe` `xtm_xtm800_1500_2500_11_8_4.zip`
XTM 2050	`XTM_OS_XTM2050_11_8_4.exe` `xtm_xtm2050_11_8_4.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_8_4.exe` `xtm_xtm800_1500_2500_11_8_4.zip`
XTM 1050	`XTM_OS_XTM1050_11_8_4.exe` `xtm_xtm1050_11_8_4.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_8_4.exe` `xtm_xtm800_1500_2500_11_8_4.zip`
XTM 8 Series	`XTM_OS_XTM8_11_8_4.exe` `xtm_xtm8_11_8_4.zip`
XTM 5 Series	`XTM_OS_XTM5_11_8_4.exe` `xtm_xtm5_11_8_4.zip`
XTM 330	`XTM_OS_XTM330_11_8_4.exe` `xtm_xtm330_11_8_4.zip`
XTM 33	`XTM_OS_XTM33_11_8_4.exe` `xtm_xtm33_11_8_4.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_8_4.exe` `xtm_xtm2a6_11_8_4.zip`
Firebox T10	`XTM_OS_T10_11_8_4.exe` `firebox_T10_11_8_4.zip`

XTMv
All editions for VMware
	`xtmv_11_8_4.ova`
	`xtmv_11_8_4.exe`
	`xtmv_11_8_4.zip`

XTMv All editions for Hyper-V	`xtmv_11_8_4_vhd.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. Single Sign-On software available for this release includes:

- `WG-Authentication-Gateway_11_8_1.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_8_1.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_8_1.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_8_1.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_8_1.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_8.exe` (This installer includes both 32-bit and 64-bit file support and was updated for the XTM v11.8 release.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL. After you upgrade to v11.8.4, Mobile VPN with SSL clients will be prompted to upgrade automatically when they connect to your Firebox or XTM device.

- `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.The Windows client software provided by NCP was updated on March 19, after the initial release of Fireware XTM v11.8.3.

- `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` - This file was updated on March 19 to resolve a bug in the Phase 1 DH group setting. 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 v11.8.x for the first time. If you want to update your WatchGuard AP devices manually, 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 from Fireware XTM v11.x to v11.8.x

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.8.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 Firebox or 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 v11.8.x.

> We recommend that you reboot your Firebox or XTM device before you upgrade. While this is not necessary for most higher-model XTM devices, a reboot clears your 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 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.

General Information for WatchGuard Server Software Upgrades

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.x.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.

Upgrade to Fireware XTM v11.8.x from Web UI

1. Go to **System > Backup Image** or use the USB Backup feature to back up your current configuration file.
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\11.8.4\[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\11.8.4
3. Connect to your XTM device with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the *[xtm series or firebox]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

Upgrade to Fireware XTM v11.8.x from WSM/Policy Manager v11.9.x

1. Select **File > Backup** or use the USB Backup feature to back up your current configuration file.
2. On your management computer, launch the OS executable file you downloaded from the WatchGuard Portal.
   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\11.8.4\[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\11.8.4
3. Install and open WatchGuard System Manager v11.9.x. 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 or firebox]_[product code].sysa-dl* file from Step 2.

Upgrade your FireCluster to Fireware XTM v11.8.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 before you can upgrade your FireCluster to Fireware XTM v11.8.x.

Upgrade a FireCluster from Fireware XTM v11.4.x–v11.7.x to v11.8.x

Use these steps to upgrade a FireCluster from Fireware XTM v11.4.x, v11.5.x, v11.6.x,or v11.7.x to Fireware XTM v11.8.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 v11.8.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 v11.8.x to WSM v11.x

If you want to revert from v11.8.x to an earlier version of WSM, you must uninstall WSM v11.8.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 v11.8.x.

Next, install the same version of WSM that you used before you upgraded to WSM v11.8.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 v11.8.x. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.8.x to Fireware XTM v11.x

⚠ If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.8.x to an earlier version, the downgrade process resets the network and security settings on your Firebox or 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 v11.8.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 v11.8.x. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.8.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 a Firebox T10 to a version of Fireware XTM OS lower than v11.8.3. You cannot downgrade an XTM 2050 or an XTM 330 to a version of Fireware XTM OS lower than v11.5.1.
- You cannot downgrade an XTM 25, 26, or 33 device to a version of Fireware XTM OS lower than v11.5.2.
- You cannot downgrade an XTM 5 Series model 515, 525, 535 or 545 to a version of Fireware XTM OS lower than v11.6.1.
- You cannot downgrade XTMv in a VMware environment to a version of Fireware XTM OS lower than v11.5.4.
- You cannot downgrade XTMv in a Hyper-V environment to a version of Fireware XTM OS lower than v11.7.3.

When you downgrade the Fireware XTM OS on your Firebox or XTM device, the firmware on any paired AP devices is not automatically downgraded. We recommend that you reset the AP device to its factory-default settings to make sure that it can be managed by the older version of Fireware XTM OS.

Enhancements and Resolved Issues in Fireware XTM v11.8.4

Fireware XTM v11.8.4 addresses many previously reported bugs and enhancement requests, including the issues shown below.

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]*
- Feature keys with more than 1024 characters are now supported. *[80403]*
- This release resolves a kernel crash. *[79832]*
- This release resolves a kernel crash triggered by a SYN flood directed at the XTM device. *[79909]*

Proxies and Services

- 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 resolves several proxy process crashes. *[78665, 78819]*
- 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]*
- Several issues related to the use of inbound HTTPS content inspection have been resolved in this release. *[79235, 75725]*
- This release provides improvements to Application Control detection when not using HTTPS proxy with content inspection. *[81008, 80885, 81037]*
- Several improvements were made to SIP ALG to improve one way audio during VoIP calls.*[79962, 79311, 80385]*
- 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]*
- This release resolves an issue that caused a kernel crash when maximum command line length for the FTP proxy is exceeded and auto-block is enabled. *[79841]*
- This release resolves a proxy process crash when using IPS. *[77948]*

Authentication

- 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]*

Networking

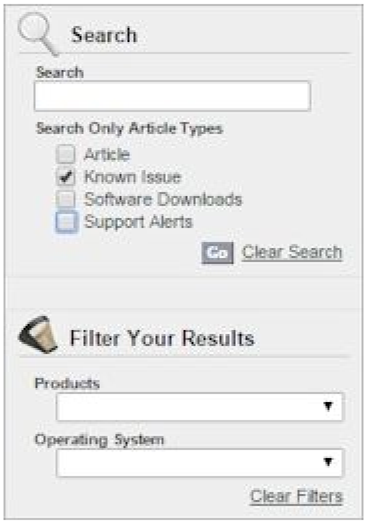
- You can now configure your XTM device default gateway on a different subnet than your XTM device external interface. *[79589]*
- This release updates the ECMP algorithm used for Multi-WAN Routing Table mode to improve WAN load balancing performance. *[77944, 77935]*
- A device configured in drop-in mode now correctly responds to an ARP request sent to unicast address. *[79010]*

VPN

- Mobile VPN with SSL connections using WatchGuard's SSLVPN client or OpenVPN client are no longer blocked by the HTTPS proxy. *[77969]*

Known Issues and Limitations

You can find information about known issues for Fireware XTM v11.8.4 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.



Search

Search

Search Only Article Types

☐ Article
☑ Known Issue
☐ Software Downloads
☐ Support Alerts

Filter Your Results

Products

Operating System

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