Fireware v11.12.2 Release Notes

Supported Devices	Firebox T10, T30, T50, T70, M200, M300, M400, M440, M500, M4600, M5600 XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 FireboxV, XTMv, Firebox Cloud, WatchGuard AP
Release Date:	11 April 2017
Release Notes Revision:	11 April 2017
Fireware OS Build	526900
WatchGuard System Manager Build	526973
WatchGuard AP Device Firmware	For AP100, AP102, AP200: Build 1.2.9.12 For AP300: Build 2.0.0.7 For AP120, AP320, AP322: Build 8.0.564

Introduction

WatchGuard is pleased to announce the release of Fireware v11.12.2 and WatchGuard System Manager v11.12.2. In addition to resolving many outstanding bugs, this release also delivers these new features and functions for our Firebox users:

Firebox Account Lockout

Account Lockout prevents attackers from repeatedly guessing passwords for Firebox authentication or Device Management accounts. You can now configure the Firebox to temporarily lock user accounts after a specified number of failed login attempts, and to permanently lock a user account after a specified number of temporary lockouts.

Gateway Wireless Controller Security Enhancements

- **Automatic AP Passphrase Management**
  To increase security and improve passphrase management, the Gateway Wireless Controller can now automatically create unique random passphrases for each AP device.
- **Default Wireless Security Mode**
  The default wireless security mode for AP devices locally managed by a Gateway Wireless Controller and wireless-capable Firebox devices is now WPA2-only (PSK) with AES encryption.
- **AP Device Trust Store**
  To help avoid security issues that result from the use of factory reset, unauthorized, or compromised AP devices in your deployment, the Gateway Wireless Controller now creates trust records for each AP device.

After you upgrade to Fireware v11.12.2, you must trust any AP100/102, AP200, and AP300 devices in your deployment. See the What's New in Fireware v11.12.2 presentation for important information about this new feature.

Perfect Forward Secrecy Ciphers for Firebox T10, T30, T50, XTM 25/26, and XTM 33

The HTTPS and SMTP proxies now support Perfect Forward Secrecy Ciphers for content inspection purposes for all Firebox and XTM device models.

VPN Tunnels to Amazon Web Services (AWS)

With Amazon Web Services (AWS), you can operate a hybrid network with resources on premises and in the cloud. WatchGuard now supports static and dynamic (BGP) VPN tunnels to AWS Virtual Private Clouds (VPC). When you configure a VPN between your Firebox and an AWS VPC, a secure tunnel is established that protects your data.

Dynamic DNS Enhancement

Dynamic DNS makes sure that your Firebox is always accessible by its domain name, even when the IP address attached to your domain name changes. Previously, when you enabled Dynamic DNS on your Firebox, the Firebox automatically sent the IP address of its external interface to DynDNS, a dynamic DNS service provider. Now, WatchGuard supports a second option—you can allow DynDNS to determine which IP address to use.

Support for DHCP in Bridge Mode

Fireboxes configured in bridge mode can now be configured to use DHCP on the primary interface, which enables the ability to quickly and easily install a Firebox with no impact on the network.

DNS Forwarding Enhancement

DNS forwarding enables network admins to configure network clients to point to the gateway Firebox as the DNS server for a network. Conditional DNS forwarding gives distributed enterprise, with many locations, the flexibility to point to a central corporate DNS server for some traffic, but local DNS servers for other domains. With the new conditional DNS forwarding enhancement, you can specify conditions that tell the Firebox where to forward DNS queries. For example, you can forward DNS queries for an internal domain through a VPN to your remote DNS server, and forward all other DNS queries to a public DNS server close to your location.

VPN Statistics and Monitoring Enhancements

With this release, we've added new VPN usage charts in Fireware Web UI to show the number of active VPN tunnels over time to help you keep track of license usage and investigate issues.

Other Enhancements

- Hotspot Guest User Accounts Device Limit
- Blocked Sites Exceptions list now contains the FQDNs for servers that the Firebox services must connect to.
- Modem support for Franklin U772 (Sprint) USB modem and NETGEAR Beam (AT&T) USB modem

For more information on the feature updates and bug fixes in this release, see the Enhancements and Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Fireware v11.12.2, see Fireware Help or review What's New in Fireware v11.12.2.

Important Information about Firebox Certificates

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

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

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

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

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

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

CLI Commands to Regenerate Default Firebox Certificates

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

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

For more information about the CLI, see the Command Line Interface Reference.

Before You Begin

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

- A supported WatchGuard Firebox or XTM device. This device can be a WatchGuard Firebox T10, T30, T50, T70, XTM 2 Series (models 25 and 26 only), 3 Series, 5 Series, 8 Series, 800 Series, XTM 1050, XTM 1500 Series, XTM 2050 device, XTM 2500 Series, Firebox M200, M300, M400, M500, M440, M4600, M5600. You can also use this version of Fireware on FireboxV or XTMv (any edition), and Firebox Cloud for AWS.
- The required hardware and software components as shown below. If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware OS installed on your Firebox or XTM device and the version of WSM installed on your Management Server.
- Feature key for your Firebox or XTM device — If you upgrade your device from an earlier version of Fireware OS, you can use your existing feature key. If you do not have a feature key for your device, you can log in to the WatchGuard website to download it.

Note that you can install and use WatchGuard System Manager v11.12.x and all WSM server components with devices running earlier versions of Fireware v11.x. In this case, we recommend that you use the product documentation that matches your Fireware OS version.

If you have a new Firebox or XTM physical device, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. If this is a new FireboxV or XTMv installation, make sure you carefully review Fireware Help for important installation and setup instructions. We also recommend that you review the Hardware Guide for your Firebox or XTM device model. The *Hardware Guide* contains useful information about your device interfaces, as well as information on resetting your device to factory default settings, if necessary.

Product documentation for all WatchGuard products is available on the WatchGuard web site at http://www.watchguard.com/wgrd-help/documentation/overview.

Localization

This release includes localized management user interfaces (WSM application suite and Web UI) current as of Fireware v11.11. UI changes introduced since v11.11 may remain in English. Supported languages are:

- French (France)
- Japanese
- Spanish (Latin American)

Note that most data input must still be made using standard ASCII characters. You can use non-ASCII characters in some areas of the UI, including:

- Proxy deny message
- Wireless hotspot title, terms and conditions, and message
- WatchGuard Server Center users, groups, and role names

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the Web UI System Status menu and any software components provided by third-party companies remain in English.

Fireware Web UI

The Web UI will launch in the language you have set in your web browser by default.

WatchGuard System Manager

When you install WSM, you can choose what language packs you want to install. The language displayed in WSM will match the language you select in your Microsoft Windows environment. For example, if you use Windows 7 and want to use WSM in Japanese, go to Control Panel > Regions and Languages and select Japanese on the Keyboards and Languages tab as your Display Language.

Dimension, WebCenter, Quarantine Web UI, and Wireless Hotspot

These web pages automatically display in whatever language preference you have set in your web browser.

Documentation

Localization updates are also available for *Fireware Help*, available on the WatchGuard website or as context-sensitive Help from the localized user interfaces.

Fireware and WSM v11.12.2 Operating System Compatibility

Last revised: 5 April 2017

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10 (32-bit & 64-bit)	Microsoft Windows Server 2012 & 2012 R2 (64-bit)	Microsoft Windows Server 2016 (64-bit)	Mac OS X v10.9, v10.10, v10.11 & v10.12	Android 4.x &5.x	iOS v7, v8, v9, & v10
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]		✓	✓			
Terminal Services Agent[2]		✓	✓			
Mobile VPN with IPSec	✓			✓ 3	✓	✓ 3
Mobile VPN with SSL	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *Windows 8.x support does not include Windows RT.*
- *Windows Exchange Server 2013 is supported if you install Windows Sever 2012 or 2012 R2 and .Net framework 3.5.*

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

- *IE 11 and later*
- *Microsoft Edge*
- *Firefox v22 and later*
- *Safari 6 and later*

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

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

[2]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, 6.5, 7.6, or 7.12 environment.

[3]Native (Cisco) IPSec client and OpenVPN are supported for Mac OS and iOS. For Mac OS X 10.8 -10.12, we also support the WatchGuard IPSec Mobile VPN Client for Mac, powered by NCP.

Authentication Support

This table gives you a quick view of the types of authentication servers supported by key features of Fireware. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your Firebox or XTM device configuration. With each type of third-party authentication server supported, you can specify a backup server IP address for failover.

 *Fully supported by WatchGuard*  *Not yet supported, but tested with success by WatchGuard customers*

	Active Directory[1]	LDAP	RADIUS [2]	SecurID [2]	Firebox (Firebox-DB) Local Authentication
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓ 3	–	✓
Mobile VPN with IPSec/WatchGuard client (NCP)	✓	✓	✓	✓	✓
Mobile VPN with IPSec for iOS and Mac OS X native VPN client	⚑	⚑	⚑	✓	✓
Mobile VPN with IPSec for Android devices	✓	✓	✓	–	✓
Mobile VPN with SSL for Windows	✓	✓	✓ 4	✓ 4	✓
Mobile VPN with SSL for Mac	✓	✓	✓	✓	✓
Mobile VPN with SSL for iOS and Android devices	⚑	⚑	⚑	✓	✓
Mobile VPN with L2TP	✓ 6	–	✓	–	✓
Mobile VPN with PPTP	–	–	✓	N/A	✓
Built-in Authentication Web Page on Port 4100	✓	✓	✓	✓	✓
Single Sign-On Support *(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 supports RADIUS Filter ID 11 for group authentication.*
5. *Both single and multiple domain Active Directory configurations are supported. For information about the supported Operating System compatibility for the WatchGuard TO Agent and SSO Agent, see the current Fireware and WSM Operating System Compatibility table.*
6. *Active Directory authentication methods are supported only through a RADIUS server.*

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Minimum CPU	Intel Core or Xeon 2GHz	Intel Core or Xeon 2GHz
Minimum Memory	1 GB	2 GB
Minimum Available Disk Space	250 MB	1 GB
Minimum Recommended Screen Resolution	1024x768	1024x768

FireboxV System Requirements

With support for installation in both a VMware and a Hyper-V environment, a WatchGuard FireboxV virtual machine can run on a VMware ESXi 5.5, 6.0, or 6.5 host, or on Windows Server 2012 R2 or 2016, or Hyper-V Server 2012 R2 or 2016.

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

Each FireboxV virtual machine requires 5 GB of disk space. CPU and memory requirements vary by model:

FireboxV Model	vCPUs (maximum)	Memory (recommended)
Small	2	1024 MB
Medium	4	2048 MB
Large	8	4096 MB
Extra Large	16	4096 MB

System requirements for XTMv are included in *Fireware Help*.

Downloading Software

You can download software from the WatchGuard Software Downloads Center.

There are several software files available for download with this release. See the descriptions below so you know what software packages you will need for your upgrade.

WatchGuard System Manager

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

`WSM11_12_2.exe` — Use this file to install WSM v11.12.2 or to upgrade WatchGuard System Manager from an earlier version to WSM v11.12.2.

Fireware OS

If your Firebox is running Fireware v11.10 or later, you can upgrade the Fireware OS on your Firebox automatically from the Fireware Web UI **System > Upgrade OS** page.

If you prefer to upgrade from Policy Manager, or from an earlier version of Fireware, you can use download the Fireware OS image for your Firebox or XTM device. Use the .exe file if you want to install or upgrade the OS using WSM. Use the .zip file if you want to install or upgrade the OS manually using Fireware Web UI. Use the .ova or .vhd file to deploy a new XTMv device.

If you have…	Select from these Fireware OS packages
Firebox M5600	Firebox_OS_M4600_M5600_11_12_2.exe firebox_M4600_M5600_11_12_2.zip
Firebox M4600	Firebox_OS_M4600_M5600_11_12_2.exe firebox_M4600_M5600_11_12_2.zip
XTM 2500 Series	XTM_OS_XTM800_1500_2500_11_12_2.exe xtm_xtm800_1500_2500_11_12_2.zip
XTM 2050	XTM_OS_XTM2050_11_12_2.exe xtm_xtm2050_11_12_2.zip
XTM 1500 Series	XTM_OS_XTM800_1500_2500_11_12_2.exe xtm_xtm800_1500_2500_11_12_2.zip
XTM 1050	XTM_OS_XTM1050_11_12_2.exe xtm_xtm1050_11_12_2.zip
XTM 800 Series	XTM_OS_XTM800_1500_2500_11_12_2.exe xtm_xtm800_1500_2500_11_12_2.zip
XTM 8 Series	XTM_OS_XTM8_11_12_2.exe xtm_xtm8_11_12_2.zip
Firebox M500	Firebox_OS_M400_M500_11_12_2.exe firebox_M400_M500_11_12_2.zip
XTM 5 Series	XTM_OS_XTM5_11_12_2.exe xtm_xtm5_11_12_2.zip
Firebox M440	Firebox_OS_M440_11_12_2.exe firebox_M440_11_12_2.zip
Firebox M400	Firebox_OS_M400_M500_11_12_2.exe firebox_M400_M500_11_12_2.zip
Firebox M300	Firebox_OS_M200_M300_11_12_2.exe firebox_M200_M300_11_12_2.zip
Firebox M200	Firebox_OS_M200_M300_11_12_2.exe firebox_M200_M300_11_12_2.zip
XTM 330	XTM_OS_XTM330_11_12_2.exe xtm_xtm330_11_12_2.zip
XTM 33	XTM_OS_XTM3_11_12_2.exe xtm_xtm3_11_12_2.zip
XTM 2 Series Models 25, 26	XTM_OS_XTM2A6_11_12_2.exe xtm_xtm2a6_11_12_2.zip
Firebox T70	Firebox_OS_T70_11_12_2.exe firebox_T70_11_12_2.zip

If you have…	Select from these Fireware OS packages
Firebox T50	Firebox_OS_T30_T50_11_12_2.exe firebox_T30_T50_11_12_2.zip
Firebox T30	Firebox_OS_T30_T50_11_12_2.exe firebox_T30_T50_11_12_2.zip
Firebox T10	Firebox_OS_T10_11_12_2.exe firebox_T10_11_12_2.zip
FireboxV All editions for VMware	FireboxV_11_12_2.ova XTM_OS_FireboxV_11_12_2.exe xtm_FireboxV_11_12_2.zip
FireboxV All editions for Hyper-V	FireboxV_11_12_2_vhd.zip XTM_OS_FireboxV_11_12_2.exe xtm_FireboxV_11_12_2.zip
XTMv All editions for VMware	xtmv_11_12_2.ova XTM_OS_xtmv_11_12_2.exe xtm_xtmv_11_12_2.zip
XTMv All editions for Hyper-V	xtmv_11_12_2_vhd.zip XTM_OS_XTMv_11_12_2.exe xtm_xtmv_11_12_2.zip
Firebox Cloud	firebox_FireboxCloud_11_12_2.sysa-dl

Single Sign-On Software

These files are available for Single Sign-On and all have been updated for this release:

- WG-Authentication-Gateway_11_11_2.exe (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- WG-Authentication-Client_11_11_2.msi (SSO Client software for Windows)
- WG-SSOCLIENT-MAC_11_11_2.dmg (SSO Client software for Mac OS X)
- SSOExchangeMonitor_x86_11_11_2.exe (Exchange Monitor for 32-bit operating systems)
- SSOExchangeMonitor_x64_11_11_2.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

This file was updated with the Fireware v11.12 release.

- TO_AGENT_SETUP_11_12.exe (This installer includes both 32-bit and 64-bit file support.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL and are both updated with this release:

- WG-MVPN-SSL_11_11_2.exe (Client software for Windows)
- WG-MVPN-SSL_11_11_2.dmg (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are several available files to download.

Shrew Soft Client

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

WatchGuard IPSec Mobile VPN Clients

The current WatchGuard IPSec Mobile VPN Client for Windows is version 12.10.

- `WatchGuard IPSec Mobile VPN Client for Windows (32-bit), powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.
- `WatchGuard IPSec Mobile VPN Client for Windows (64-bit), powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.

This release includes an update to the IPSec Mobile VPN Client for Mac OS X. The updated Mac OS X client remains version 2.0.5.

- `WatchGuard IPSec Mobile VPN Client for Mac OS X, powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.

WatchGuard Mobile VPN License Server

- `WatchGuard Mobile VPN License Server (MVLS) v2.0, powered by NCP`- Click here for more information about MVLS.

Upgrade Notes

In addition to new features introduced in Fireware v11.12, v11.12.1, and v11.12.2, there were other changes that affect the functionality of several existing features in ways that you need to understand before you upgrade to v11.12 or higher. In this section, we review the impact of some of these changes. For more information, see the What's New presentation for each release or Fireware Help.

Gateway Wireless Controller and AP Device Security

Fireware v11.12.2 includes updates to the Gateway Wireless Controller to improve AP device security. Some of these changes require that you take action after you upgrade so that all AP devices are trusted and use secure passphrases.

Gateway Wireless Controller now creates trust records for each AP device

Beginning with Fireware v11.12.2, to help prevent potential security issues from the use of factory reset, unauthorized, or compromised AP devices in your deployment, the Gateway Wireless Controller now creates trust records for each AP device. The Gateway Wireless Controller will not communicate with an AP device that has no trust record. Wireless data functions will continue to work for a previously configured AP device , but the Gateway Wireless Controller will not manage or monitor an AP device with no trust record.

After the upgrade to Fireware v11.12.2, existing AP120, AP320, and AP322 devices in your deployment will be automatically trusted.

After you upgrade to Fireware v11.12.2 you must manually trust any current AP100/102, AP200, and AP300 devices in your deployment.

You must always trust your AP devices again if they are reset to factory default settings or if you reset the trust store.

Secure Global AP Passphrase

Beginning with Fireware v11.12.2, the minimum length for the global AP passphrase is 8 characters. In addition, the previous default AP passphrases (**wgwap** and **watchguard**) are no longer valid.

After you upgrade to Fireware v11.12.2, your previous global AP passphrase is maintained. If your existing configuration uses the default passphrases or if the global AP passphrase is shorter than 8 characters, you must choose a new global AP passphrase, or use the new automatic AP passphrase security feature before you can save the Gateway Wireless Controller configuration.

Automatic AP Passphrase Management

To increase security and improve passphrase management, the Gateway Wireless Controller can now automatically create unique random passphrases for each AP device. This feature is disabled by default. If you want to enable automatic AP passphrase management, you must disable the manual global AP passphrase.

Blocked Sites Exceptions

When you upgrade the Firebox to Fireware v11.12.2 or higher, FQDNs for WatchGuard servers are automatically added to the Blocked Sites Exceptions list in the configuration on the Firebox.

If you use Policy Manager to upgrade the Firebox, you must manually reload the configuration from the Firebox in Policy Manager after the upgrade completes. This is to make sure that the configuration in Policy Manager includes the Blocked Sites Exceptions that were added to the Firebox as part of the upgrade.

If you use Policy Manager to open a configuration file that was created before the Firebox was upgraded to v11.12.2, and then save that configuration file to the Firebox, the old blocked sites configuration overwrites the configuration on the Firebox, and FQDNs for WatchGuard servers are no longer on the Blocked Sites Exceptions List.

TCP Port 4100 and the WatchGuard Authentication Policy

Beginning with Fireware v11.12, TCP port 4100 is used only for firewall user authentication. In earlier versions, a WatchGuard Authentication policy was automatically added to your configuration file when you enabled Mobile VPN with SSL. This policy allowed traffic over port 4100 and included the alias Any-External in the policy **From** list. In Fireware v11.12, when you enable Mobile VPN with SSL, this policy is no longer created.

When you upgrade to Fireware v11.12, the External alias will be removed from your WatchGuard Authentication policy in the configuration on the Firebox, even if you had manually added the alias previously and regardless of whether Mobile VPN with SSL is enabled.

If you use Policy Manager to upgrade the Firebox, you must manually reload the configuration from the Firebox in Policy Manager after the upgrade completes to avoid adding the alias back with a subsequent configuration save (since Policy Manager is an offline configuration tool).

The Mobile VPN with SSL authentication and software download pages are no longer accessible at port 4100. See Fireware Help for more information.

Setup Wizard Default Policies and Settings

You use the Web Setup Wizard or WSM Quick Setup Wizard to set up a Firebox with a basic configuration. Beginning with Fireware v11.12, the setup wizards configure policies and enable most Subscription Services to provide better security by default.

In Fireware v11.12 and higher, the setup wizards:

- Configure FTP-proxy, HTTP-proxy, HTTPS-proxy policies
- Configure DNS and Outgoing packet-filter policies
- Enable licensed security services — Application Control, Gateway AntiVirus, WebBlocker, Intrusion Prevention Service, Reputation Enabled Defense, Botnet Detection, Geolocation, APT Blocker
- Recommend WebBlocker categories to block

The default policies and services that the setup wizards configure depend on the version of Fireware installed on the Firebox, and on whether the Firebox feature key includes a license for subscription services. If your new Firebox was manufactured with Fireware v11.11.x or lower, the setup wizards do not enable subscription services, even if they are licensed in the feature key. To enable the security services and proxy policies with recommended settings, upgrade the Firebox to Fireware v11.12 or higher, reset it to factory-default settings, and then run the setup wizard again.

Upgrade to Fireware v11.12.2

Before you upgrade to Fireware v11.12.2, your Firebox must be running:
- Fireware XTM v11.7.5
- Fireware XTM v11.8.4
- Fireware XTM v11.9 or higher

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

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

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x, or v11.10.x before you upgrade to Fireware v11.12.2 or your Firebox will be reset to a default state.

Important Information about the upgrade process:

- We recommend you use Fireware Web UI to upgrade to Fireware v11.12.2. You can also use Policy Manager if you prefer.
- We strongly recommend that you save a local copy of your Firebox configuration and create a Firebox backup image before you upgrade. It is not possible to downgrade without these backup files.
- If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware OS installed on your Firebox and the version of WSM installed on your Management Server. Also, make sure to upgrade WSM *before* you upgrade the version of Fireware OS on your Firebox.

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

Upgrade Notes for XTMv

You cannot upgrade an XTMv device to FireboxV. For Fireware v11.11 and higher, the XTMv device is a 64-bit virtual machine. You cannot upgrade an XTMv device from Fireware v11.10.x or lower to Fireware v11.11 or higher. Instead, you must use the OVA file to deploy a new 64-bit Fireware v11.11.x XTMv VM, and then use Policy Manager to move the existing configuration from the 32-bit XTMv VM to the 64-bit XTMv VM. For more information about how to move the configuration, see *Fireware Help*. For more information about how to deploy a new XTMv VM, see the latest *WatchGuard XTMv Setup Guide* available here. When your XTMv instance has been updated to v11.11 or higher, you can then use the usual upgrade procedure, as detailed below.

WatchGuard updated the certificate used to sign the .ova files with the release of Fireware v11.11. When you deploy the OVF template, a certificate error may appear in the OVF template details. This error occurs when the host machine is missing an intermediate certificate from Symantic (Symantec Class 3 SHA256 Code Signing CA), and the Windows CryptoAPI was unable to download it. To resolve this error, you can download and install the certificate from Symantec.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x server or client software when you upgrade to WSM v11.12.2. You can install the v11.12.2 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, your WatchGuard Management Server) to a safe location before you upgrade. You will need these backup files if you ever want to downgrade.

To back up your Management Server configuration, from the computer where you installed the Management Server:

1. From WatchGuard Server Center, select **Backup/Restore Management Server**.
   The WatchGuard Server Center Backup/Restore Wizard starts.
2. Click **Next**.
   The Select an action screen appears.
3. Select **Back up settings**.
4. Click **Next**.
   The Specify a backup file screen appears.
5. Click **Browse** to select a location for the backup file. Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.
   The WatchGuard Server Center Backup/Restore Wizard is complete screen appears.
7. Click **Finish** to exit the wizard.

Upgrade to Fireware v11.12.2 from Web UI

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

1. Before you begin, save a local copy of your configuration file.
2. Go to **System > Backup Image** or use the USB Backup feature to back up your current device image.
3. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads page.
   If you use the Windows-based installer on a computer with a Windows 64-bit operating system, this installation extracts an upgrade file called *[product series]_[product code].sysa-dl* to the default location of C:\Program Files(x86)\Common Files\WatchGuard\resources\FirewareXTM\11.12.2\[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\11.12.2
4. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
5. Browse to the location of the *[product series]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

If you have already installed Fireware v11.12.2 on your computer, you must run the Fireware v11.12.2 installer twice (once to remove v11.12.2 software and again to install v11.12.2).

Upgrade to Fireware v11.12.2 from WSM/Policy Manager

1. Before you begin, save a local copy of your configuration file.
2. Select **File > Backup** or use the USB Backup feature to back up your current device image.
3. On a management computer running a Windows 64-bit operating system, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called *[Firebox or xtm series]_[product code].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.12.2\[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\11.12.2.
4. Install and open WatchGuard System Manager v11.12.2. Connect to your Firebox and launch Policy Manager.
5. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[product series]_[product code].sysa-dl* file from Step 2.

If you like to make updates to your Firebox configuration from a saved configuration file, make sure you open the configuration from the Firebox and save it to a new file after you upgrade. This is to make sure that you do not overwrite any configuration changes that were made as part of the upgrade.

If you have already installed Fireware v11.12.2 on your computer, you must run the Fireware v11.12.2 installer twice (once to remove v11.12.2 software and again to install v11.12.2).

Update AP Devices

With the release of Fireware v11.12.2, we are also releasing new AP firmware for AP100, AP102, AP200, and AP300 devices. The process to update to new AP firmware changed recently. Please review this section carefully for important information about updating AP devices.

After you upgrade to Fireware v11.12.2, you must trust any current AP100/102, AP200, and AP300 devices in your deployment. You must trust AP devices again after the first time the devices upgrade to v1.2.9.12 or v2.0.0.7. Finally, you must trust any new AP devices that you deploy when you first set up the devices. See the What's New in Fireware v11.12.2 presentation for important information about this new feature.

Update your AP100, AP102, and AP200 Devices

Fireware v11.12.2 includes new AP firmware v1.2.9.12 for AP100/102 and AP200 devices. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 or later to Fireware v11.12.2, your AP devices are automatically updated between midnight and 4:00am local time. You can also see and use the new feature to check for and download AP firmware updates to Gateway Wireless Controller for future updates.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.12.2, there is an additional step you must take to make sure AP v1.2.9.12 is applied to your AP devices. When you upgrade to Fireware v11.12.2 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the Fireware Web UI **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** to download the latest AP firmware to the Firebox.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. From the Fireware Web UI **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** to download the latest AP firmware to the Firebox again.

You cannot install the AP firmware on a Firebox that uses Fireware v11.4.x or lower. If you try to install the AP Component Package on a Firebox that uses Fireware v11.4.x or lower, the package appears to install successfully, but the AP firmware is not installed and log messages show that the packet installation was aborted.

Update Your AP300 Devices

Fireware v11.12.2 includes AP firmware v2.0.0.7. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller AND you upgrade from Fireware v11.10.4 or later to Fireware v11.12.2, your AP devices will be automatically updated between midnight and 4:00am local time. You can also see and use the new feature to check for and download AP firmware updates directly from Gateway Wireless Controller.

If you upgrade from Fireware v11.10.3 or lower to Fireware v11.12.2, there is an additional step you must take to make sure AP v2.0.0.6 is applied to your AP devices. When you upgrade to Fireware v11.12.2 with Fireware Web UI or Policy Manager, you must do the upgrade process twice. From the Fireware Web UI **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** to download the latest AP firmware to the Firebox.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. From the Fireware Web UI **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** to download the latest AP firmware to the Firebox again.

Update AP120, AP320, or AP322 Devices Managed with Gateway Wireless Controller

Fireware v11.12.2 does NOT include firmware for AP120, AP320, or AP322 devices. To get the latest firmware, from Fireware Web UI **Gateway Wireless Controller > Summary** tab, select **Manage Firmware**. Look for `8.0.564` and select **Download** to download the new firmware to your Firebox. If you have enabled automatic AP device firmware updates in Gateway Wireless Controller, your AP devices will be automatically updated between midnight and 4:00am local time.

If you reset your Firebox to factory-default settings, the AP firmware is removed from the Firebox. From the Fireware Web UI **Gateway Wireless Controller > Summary** tab, select **Manage Firmware** to download the latest AP firmware to the Firebox again.

Upgrade your FireCluster to Fireware v11.12.2

Before you upgrade to Fireware v11.11 or higher, your Firebox must be running:
- Fireware XTM v11.7.5
- Fireware XTM v11.8.4
- Fireware XTM v11.9 or higher

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

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

If you use the Fireware Web UI to upgrade your device, you see a warning, but it is possible to continue so you must make sure your Firebox is running v11.7.5, v11.8.4, or v11.9.x before you upgrade to Fireware v11.11.x or higher or your Firebox will be reset to a default state.

To upgrade a FireCluster from Fireware v11.3.x to Fireware v11.9.x or higher, you must perform a manual upgrade. For manual upgrade steps, see this Knowledge Base article.

You can upgrade Fireware OS for a FireCluster from Policy Manager or Fireware Web UI. To upgrade a FireCluster from Fireware v11.10.x or lower, we recommend you use Policy Manager.

As part of the upgrade process, each cluster member reboots and rejoins the cluster. Because the cluster cannot do load balancing while a cluster member reboot is in progress, we recommend you upgrade an active/active cluster at a time when the network traffic is lightest.

For information on how to upgrade your FireCluster, see this Help topic.

Downgrade Instructions

Downgrade from WSM v11.12.2 to WSM v11.x

If you want to revert from v11.12.2 to an earlier version of WSM, you must uninstall WSM v11.12.2. 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 v11.12.2.

Next, install the same version of WSM that you used before you upgraded to WSM v11.12.2. 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 v11.12.2. Verify that all WatchGuard servers are running.

Downgrade from Fireware v11.12.2 to Fireware v11.x

If you use the Fireware Web UI or CLI to downgrade from Fireware v11.12.2 to an earlier version, the downgrade process resets the network and security settings on your device to their factory-default settings. The downgrade process does not change the device passphrases and does not remove the feature keys and certificates.

If you want to downgrade from Fireware v11.12.2 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v11.12.2. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v11.12.2 to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device. This is not an option for XTMv users.

See the *Fireware Help* for more information about these downgrade procedures, and information about how to downgrade if you do not have a backup image.

Downgrade Restrictions

See this Knowledge Base article for a list of downgrade restrictions.

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

Enhancements and Resolved Issues in Fireware v11.12.2

General

- Single TCP stream now provides the expected throughput on a Firebox M440. *[FBX-380]*
- This release includes improvements to reduce CPU usage when Management Tunnels are established over SSL. *[FBX-2087, FBX-2085, 93080]*
- This release resolves an issue that caused IKED to crash after internal hash table corruption. *[FBX-1906, 92942]*
- Various process crashes have been fixed in this release. *[92706, FBX-2751, 92684]*
- ConnectWise now creates new tickets when a user removes the default "Quick Response" priority type. *[FBX-1821]*
- This release resolves a kernel crash that occurred after a FireCluster failover. *[92667, 92230]*
- A Certd process crash has been fixed. *[FBX-1167, 92526]*
- A problem that caused some websites to fail to load with a "content decoding error" has been resolved in this release. *[FBX-2410]*
- Policies that include a VLAN name in the **From** or **To** field no longer fail after you change the VLAN name. *[92966]*

Proxies and Services

- Perfect Forward Secrecy (PFS) ciphers are now available in HTTPS and SMTP proxies for Firebox T10, T30, T50, XTM 25/26, and XTM 33 models. *[FBX-2020, 93045]*
- The Blocked Sites Exceptions list now includes default FQDN exceptions for servers required for WatchGuard products and subscription services. To review the list of added exceptions, see What's New in Fireware v11.12.2. *[FBX-1416, 92658]*
- The HTTP proxy process no longer crashes when inflating data from web pages with content-encoding set to gzip or deflate. *[93220, FBX-2729]*

Authentication and Single Sign-On (SSO)

- You can now configure lockout settings for all user accounts that use Firebox authentication to protect user accounts from brute force attempts to find the user account login credentials. *[FBX-417, 45021, 67544, 45551]*
- You can now limit the number of devices that can connect to a Hotspot at the same time for each guest user account. *[FBX-433, 82879]*
- The SSO client for Mac OS now supports nested groups. *[FBX-1484, 92726]*
- WatchGuard Single Sign-On and Terminal Services components are now officially supported on Windows Server 2016. *[FBX-1153, 92398]*
- The SSO Client installer now creates a Windows firewall exception. *[FBX-1763, 91373]*

- Terminal Services support for manual Single Sign-On authentication now includes Citrix XenApp 7.12. *[FBX-1628, 90170]*
- When you associate a user with more than 256 authentication groups, the Firewalld process no longer crashes. *[93152, FBX-2681]*

VPN

- BOVPN Virtual Interface now supports an IPSec VPN tunnel to an Amazon AWS virtual private cloud (VPC). *[FBX-110, 41534]*
- You can now specify a different pre-shared key for each gateway endpoint for the same branch office VPN gateway. *[FBX-1290, FBX-1292]*
- In Fireware Web UI, the VPN Statistics System Status page has a new Statistics tab that shows bandwidth and tunnel statistics over time. *[FBX-1728]*
- The Global VPN setting **Enable TOS for IPSec** is now correctly applied to BOVPN traffic configured to use a Virtual Interface (VIF). *[FBX-2349]*
- Mobile VPN with IPSec no longer fails to reconnect after a non-graceful disconnection. *[92935, FBX-2195]*
- The use of many BOVPN Virtual Interfaces no longer causes a kernel crash. *[93193, FBX-2755]*
- This release resolves an issue with Mobile VPN with SSL that caused incorrect DNS resolution on Windows 10 clients. *[88918]*
- This release includes an updated Mobile VPN with IPSec client for Mac OS X to add support for Mac OS Sierra.

Wireless

- Gateway Wireless Controller now supports management of AP322 outdoor AP devices. *[FBX-100, FBX-1270]*
- The default wireless security mode for AP devices locally managed by a Gateway Wireless Controller and wireless-capable Firebox devices is now WPA2-only (PSK) with AES encryption. *[FBX-1974, 93047]*
- This release includes several other important security-related enhancements to Gateway Wireless Controller. See the Upgrade Notes topic for important information related to these enhancements. *[FBX-111]*

Networking and Modem Support

- In the Dynamic DNS configuration, you can select to have DynDNS use the IP address from your router or NAT device. *[FBX-1998, 92780]*
- You can now enable conditional DNS forwarding from Fireware Web UI and Policy Manager. *[FBX-559, 58214]*
- In Bridge Mode, you can now configure the Firebox to use DHCP to get an IP address. *[FBX-375]*
- This release includes support for two new USB modems:
  - Franklin U772 4G USB modem *[FBX-1232]*
  - NetGear Beam 3G/4G USB modem *[FBX-1676]*
- This release adds support for Spanning Tree Protocol support for VLAN interfaces. For specific information on supported scenarios, see Fireware Help or What's New in Fireware v11.12.2. *[FBX-753, 61035]*
- This release add spanning tree protocol support in Bridge mode. *[FBX-991, 56764]*
- A dynamic routing daemon crash has been fixed. *[92930, FBX-1744]*
- The PPPoE daemon now remains stable when Link Monitor probing cannot resolve a domain name. *[92024]*

- The BGP routing process no longer crashes when MD5 encryption is used. *[93038, FBX-1886]*
- BGP routes are now added correctly to the routing table after a FireCluster failover. *[FBX-2749, 93095]*

Known Issues and Limitations

Known issues for Fireware v11.12.2 and its management applications, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To see known issues for a specific release, from the **Product & Version** filters you can expand the Fireware version list and select the check box for v11.12.2.

Using the CLI

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

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at http://www.watchguard.com/wgrd-support/overview. 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