Fireware v12.2.1 Release Notes

Supported Devices	Firebox T10, T15, T30, T35, T50, T55, T70, M200, M270, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600 FireboxV, Firebox Cloud, WatchGuard AP
Release Date:	5 September 2018
Release Notes Revision	6 June 2019
Fireware OS Build	572649
WatchGuard System Manager Build	573863 (for v12.2.1 U1) *586863 (original v12.2.1 release)*
WatchGuard AP Device Firmware	For AP100, AP102, AP200: Build 1.2.9.16 For AP300: Build 2.0.0.11 For AP120, AP320, AP322, AP325, AP420: Build 8.6.0-634

Introduction

Fireware v12.2.1 is a new release for Firebox T Series, Firebox M Series, FireboxV, and Firebox Cloud appliances, that also includes several new features and feature enhancements.

This release does not support XTM appliances, and has changes to WebBlocker functionality for some users. WatchGuard System Manager 12.2.1 is compatible with Fireboxes with FIreware v12.1.x , including XTM devices. Be sure to review the Upgrade Notes for more information.

Firebox Management Enhancements

- This release features a new and much improved certificate import wizard.
- The Backup and Restore features on the Firebox provide more options, and more enable more reliable backups for tabletop appliances with lower memory.
- This release features several improvements to WatchMode functionality (used primarily by WatchGuard Partners).

Proxy and Service Enhancements

- You can now configure SafeSearch Enforcement Level for Youtube as Strict or Moderate.
- The SMTP proxy can now use the Deny action for Gateway AV and spamBlocker Virus Outbreak Detection actions.
- This release features usability improvements for WebBlocker.
- You can now view statistics for File Exceptions in Firebox System Manager and Web UI.

Networking Enhancements

- Firebox System Manager and Web UI now allow you to view loss, latency, and jitter for WAN interfaces in Multi-WAN configuration.
- You can now specify a loopback IP address in static NAT actions.
- Gateway Wireless Controller now supports the option to bridge LAN interfaces on AP devices.

VPN Enhancements

- You can now configure the DF bit and PMTU in BOVPN and Virtual Interface configuration for each gateway.
- You can now configure separate DNS settings for each Mobile VPN configuration.
- This release features a new version of the WatchGuard IPSec Mobile VPN Client.

Other Enhancements

- You can now configure the minimum password length for FIrebox-DB accounts.

For a full list of the enhancements in this release, see *Enhancements and Resolved Issues in WatchGuard System Manager 12.2.1 U1* or review the What's New in Fireware v12.2.1 PowerPoint or recording.

Before You Begin

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

- A supported WatchGuard Firebox. This device can be a WatchGuard Firebox T Series or Firebox M Series device. You can also use this version of Fireware on FireboxV and Firebox Cloud for AWS and Azure. *We do not support Fireware v12.2.x on XTM devices.*
- 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 — 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.
- If you are upgrading to Fireware v12.x from Fireware v11.10.x or earlier, we strongly recommend you review the Fireware v11.12.4 release notes for important information about significant feature changes that occurred in Fireware v11.12.x release cycle.

Note that you can install and use WatchGuard System Manager v12.x and all WSM server components with devices running earlier versions of Fireware. In this case, we recommend that you use the product documentation that matches your Fireware OS version.

If you have a new Firebox, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. If this is a new FireboxV installation, make sure you carefully review Fireware help in the WatchGuard Help Center for important installation and setup instructions. We also recommend that you review the Hardware Guide for your Firebox 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 https://www.watchguard.com/wgrd-help/documentation/overview.

Localization

This release includes localization for the management user interfaces (WSM application suite and Web UI) current as of Fireware v12.0. UI changes introduced since v12.0 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 10 and want to use WSM in Japanese, go to Control Panel > Language and select Japanese 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

The latest version of localized Fireware Help is available on the Fireware documentation page.

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.

Fireware and WSM v12.2.1 Operating System Compatibility

Last revised 1 October 2018

WSM/ Fireware Component	Microsoft Windows 7, 8, 8.1, 10	Microsoft Windows Server 2008 R2 SP1 & 2012 & 2012 R2	Microsoft Windows Server 2016	Mac OS X/macOS v10.10, v10.11, v10.12 & v10.13	Android 6.x, 7.x, & 8.x	iOS v8, v9, v10 & v11
WatchGuard System Manager	✓	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, see the Dimension Release Notes.*	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)[1]		✓	✓			
Single Sign-On Client	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[2]		✓	✓			
Terminal Services Agent[3]		✓	✓			
Mobile VPN with IPSec	✓[4]			✓[4,5]	✓[5]	✓[5]
Mobile VPN with SSL	✓			✓	✓[6]	✓[6]
Mobile VPN with IKEv2	✓			✓	✓[7]	✓
Mobile VPN with L2TP	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *Windows 8.x support does not include Windows RT.*

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

- *IE 11*
- *Microsoft Edge42*
- *Firefox v62*
- *Safari 12*

- *Safari iOS 12*
- *Chrome v69*

[1]*The Server Core installation option is supported for Windows Server 2016.*

[2]*Microsoft Exchange Server 2010 SP3 and Microsoft Exchange Server 2013 is supported if you install Windows Server 2012 or 2012 R2 and .NET Framework 3.5.*

[3]*Terminal Services support with manual or Single Sign-On authentication operates in a Microsoft Terminal Services or Citrix XenApp 6.0, 6.5, 7.6, or 7.12 environment.*

[4]*WatchGuard Mobile VPN with IPSec client (NCP) v3.0 or above is required if you use macOS 10.13.*

[5]Native (Cisco) IPSec client is supported for all recent versions of macOS and iOS.

[6]OpenVPN is supported for all recent versions of Android and iOS.

[7]StrongSwan is supported for all recent versions of Android.

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 macOS X native VPN client	⚑	⚑	⚑	✓	✓
Mobile VPN with IPSec for Android devices	✓	✓	✓	–	✓
Mobile VPN with SSL for Windows	✓	✓	✓[4]	✓[4]	✓
Mobile VPN with SSL for macOS	✓	✓	✓	✓	✓
Mobile VPN with SSL for iOS and Android devices	⚑	⚑	⚑	✓	✓
Mobile VPN with IKEv2 for WIndows	✓[6]	–	✓	–	✓
Mobile VPN with IKEv2 for macOS	✓[6]	–	✓	–	✓
Mobile VPN with IKEv2 for iOS	✓[6]	–	✓	–	✓
Mobile VPN with IKEv2 for Android by StrongSwan	✓[6]	–	✓	–	✓
Mobile VPN with L2TP	✓[6]	–	✓	–	✓
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	2048 MB
Medium	4	4096 MB
Large	8	4096 MB
Extra Large	16	4096 MB

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:

`WSM12_2_1_U1.exe` — Use this file to install WSM v12.2.1 or to upgrade WatchGuard System Manager from an earlier version to WSM v12.2.1.

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 FireboxV device.

If you have…	Select from these Fireware OS packages
Firebox M5600	Firebox_OS_M4600_M5600_12_2_1.exe firebox_M4600_M5600_12_2_1.zip
Firebox M4600	Firebox_OS_M4600_M5600_12_2_1.exe firebox_M4600_M5600_12_2_1.zip
Firebox M670	Firebox_OS_M270_M370_M470_M570_M670_12_2_1.exe firebox_M270_M370_M470_M570_M670_12_2_1.zip
Firebox M570	Firebox_OS_M270_M370_M470_M570_M670_12_2_1.exe firebox_M_270_M370_M470_M570_M670_12_2_1.zip
Firebox M500	Firebox_OS_M400_M500_12_2_1.exe firebox_M400_M500_12_2_1.zip
Firebox M470	Firebox_OS_M270_M370_M470_M570_M670_12_2_1.exe firebox_M_270_M370_M470_M570_M670_12_2_1.zip
Firebox M440	Firebox_OS_M440_12_2_1.exe firebox_M440_12_2_1.zip
Firebox M400	Firebox_OS_M400_M500_12_2_1.exe firebox_M400_M500_12_2_1.zip
Firebox M370	Firebox_OS_M270_M370_M470_M570_M670_12_2_1.exe firebox_M_270_M370_M470_M570_M670_12_2_1.zip
Firebox M300	Firebox_OS_M200_M300_12_2_1.exe firebox_M200_M300_12_2_1.zip
Firebox M270	Firebox_OS_M270_M370_M470_M570_M670_12_2_1.exe firebox_M270_M370_M470_M570_M670_12_2_1.zip
Firebox M200	Firebox_OS_M200_M300_12_2_1.exe firebox_M200_M300_12_2_1.zip
Firebox T70	Firebox_OS_T70_12_2_1.exe firebox_T70_12_2_1.zip
Firebox T55	Firebox_OS_T55_12_2_1.exe firebox_T55_12_2_1.zip
Firebox T50	Firebox_OS_T30_T50_12_2_1.exe firebox_T30_T50_12_2_1.zip
Firebox T35	Firebox_OS_T35_12_2_1.exe firebox_T35_12_2_1.zip
Firebox T30	Firebox_OS_T30_T50_12_2_1.exe firebox_T30_T50_12_2_1.zip

If you have…	Select from these Fireware OS packages
Firebox T15	`Firebox_OS_T15_12_2_1.exe` `firebox_T15_12_2_1.zip`
Firebox T10	`Firebox_OS_T10_12_2_1.exe` `firebox_T10_12_2_1.zip`

FireboxV
All editions for VMware
	`FireboxV_12_2_1.ova`
	`XTM_OS_FireboxV_12_2_1.exe`
	`xtm_FireboxV_12_2_1.zip`

FireboxV
All editions for Hyper-V
	`FireboxV_12_2_1_vhd.zip`
	`XTM_OS_FireboxV_12_2_1.exe`
	`xtm_FireboxV_12_2_1.zip`

Firebox Cloud	`FireboxCloud_12_2_1.zip`

Single Sign-On Software

These files are available for Single Sign-On.There are no updates with the Fireware v12.2.1 release.

- `WG-Authentication-Gateway_12_2.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11.12.2.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_12_0.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_12_0.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_12_0.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 is not updated with the Fireware v12.2.1 release.

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

WebBlocker Server

The 12.2 release introduced support for an on-premises server for WebBlocker. The current release of WebBlocker Server is 1.0

- `watchguard-webblocker_1_0.ova` (For vSphere deployment.)
- `watchguard-webblocker_1_0.vhd.zip` (For Hyper-V deployment.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL.

- `WG-MVPN-SSL_12_2.exe` (Client software for Windows)
- `WG-MVPN-SSL_12_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

These files are updated with this release. The current WatchGuard IPSec Mobile VPN Client for Windows version is 13.10

- `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 file is updated with this release. The current macOS client version is 3.1.0.

- `WatchGuard IPSec Mobile VPN Client for macOS, 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. If you have a VPN bundle ID for macOS, it must be updated on the license server to support the macOS 3.00 or later client. To update your bundle ID, contact WatchGuard Customer Support. Make sure to have your existing bundle ID available to expedite the update.

Upgrade Notes

Fireware 12.2 changed how VPNs function with Secondary IP addresses on the External interface

With Fireware 12.2 and higher, you can now configure a Branch Office VPN with a secondary network IP address as the local gateway IP address. If you already used a secondary IP address, you must update those Branch Office VPN Gateways after you upgrade to select the IP address you want to use. You can select the IP address from the new **Interface IP Address** drop-down list in the BOVPN gateway configuration settings. For more information, see Define Gateway Endpoints for a BOVPN Gateway.

XTM Appliances do not support FIreware 12.2 and higher

WatchGuard continues to add new features and services to enhance our customers' security. The continued growth of the Fireware OS means it is no longer suitable for older generation appliances with more limited resources. The new Fireware 12.2 release is only available on Firebox appliances. Fireware 12.2 and subsequent releases greater than 12.2 will not be available on any XTM appliances. WatchGuard will continue to provide updates to the 12.1.x firmware versions to provide bug fixes and important security updates as required.

You can use WatchGuard System Manager v12.2 or later to manage any Firebox with Fireware v12.1.x.

Customers with XTM appliances may want to consider trade-up to the newer Firebox models. Full details about the WatchGuard Trade-up program are available here: Customer Loyalty Trade Up Program.

WebBlocker Server with SurfControl End of Life

The local WebBlocker Server with SurfControl is not supported in Fireware v12.2. If you use Policy Manager v12.2 to save a configuration file to a Firebox that runs v12.1.x or lower and uses a local WebBlocker Server with SurfControl, the configuration file will be automatically updated to use WebBlocker Cloud.

If you want to continue to use the local WebBlocker Server with SurfControl, save your configuration file with Fireware Web UI or Policy Manager v12.1.x.

It is important to understand that, after 30 November 2018, all new and cached queries made to the WebBlocker Server with SurfControl will return uncategorized responses. We recommend that you upgrade to WebBlocker Cloud immediately. The Firebox will automatically translate your blocked categories for SurfControl to the WebSense list.

SSL/TLS Settings Precedence and Inheritance

Four Firebox features use SSL/TLS for secure communication and share the same OpenVPN server: Management Tunnel over SSL on hub devices, BOVPN over TLS in Server mode, Mobile VPN with SSL, and the Access Portal. These features also share some settings. When you enable more than one of these features, settings for some features have a higher precedence than settings for other features. Shared settings are not configurable for the features with lower precedence. For more information, see this topic in *Fireware Help*.

Modem Configurations Converted to External Interfaces with Failover Enabled

If your Firebox was configured for modem failover, when you upgrade your Firebox to Fireware v12.1 or higher, the modem configuration is automatically converted to an external interface with modem failover enabled. If all other external interfaces become unavailable, traffic automatically fails over to the modem interface. Modem interfaces can also participate in multi-WAN on all devices except the Firebox T10, Firebox T15, and XTM 2 Series devices that do not have the Pro upgrade.

HTTPS Proxy Content Inspection with Fireware v12.1

With Fireware 12.1 we updated the HTTPS proxy action to include a Content Inspection Exceptions list, which includes domains for services such as Dropbox, Skype, and Microsoft Office that are known to be incompatible with content inspection. The HTTPS proxy does not perform content inspection for domains with enabled exceptions on the Content Inspection Exceptions list.

When you upgrade your Firebox to Fireware v12.1 or higher the Content Inspection Exceptions list is automatically enabled in all HTTPS proxy actions that have content inspection enabled. After the upgrade, we recommend that you review the Content Inspection Exceptions list in your configured HTTPS proxy actions, and disable the exception for any domain you do not want the HTTPS proxy to allow without content inspection. For more information, see Which applications are on the default exception list in an HTTPS proxy action in the *Knowledge Base*.

Gateway AV Engine Upgrade with Fireware v12.0

With Fireware v12.0, we updated the engine used by Gateway AV to a new engine from BitDefender. As a result, any Firebox that upgrades from Fireware v11.x version to v12.0 or later must download a new signature set, which can take 7-10 minutes for the first update. It can take an additional 5-7 minutes to synchronize a FireCluster. We recommend that you upgrade to Fireware v12.x at a quiet time on your network. After the initial update, signature updates are incremental and much faster than in previous versions.

While the new signature set is being downloaded, network users could experience issues related to Gateway AV scan failures for several minutes after the update, and inbound emails sent through the SMTP proxy could be locked.

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.

Upgrade to Fireware v12.2.1

If your Firebox is a T10 with Fireware v12.1 or older, you might not be able to perform a backup before you upgrade the Firebox. This occurs because the memory use by Fireware v12.1 or older does not leave enough memory free to successfully complete the upgrade process on these devices. For these devices, we recommend you save a copy of the .xml configuration file with a distinctive name, as described here: Save the Configuration File.

If you need to downgrade a Firebox without a backup file after you complete the upgrade to Fireware v12.x, we recommend you Downgrade with Web UI. This process deletes the configuration file, but does not remove the device feature keys and certificates. After you downgrade the Firebox, you can use Policy Manager to Save the Configuration File to the Firebox.
If your Firebox has Fireware v12.1.1 or later, the Firebox will temporarily disable some security services to free up enough memory to successfully perform a backup. To learn more, see Backup and Restore for XTM 25, XTM 26, and Firebox T10.

Important Information about the upgrade process:

- We recommend you use Fireware Web UI to upgrade to Fireware v12.x. 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.
- 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 a Firebox T10 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.

Back Up Your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x or v12.x server or client software when you upgrade to WSM v12.x. You can install the v12.x server and client software on top of your existing installation to upgrade your WatchGuard software components. We do, however, strongly recommend that you back up your WatchGuard Servers (for example, your WatchGuard Management Server) to a safe location before you upgrade. You will need these backup files if you ever want to downgrade.

You cannot restore a WatchGuard Server backup file created with WatchGuard System Manager v12.x to to a v11.x installation. Make sure to retain your older server backup files when you upgrade to v12.0 or later in case you want to downgrade in the future.

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 v12.2.1 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\12.2.1\[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\12.2.1
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 installed a beta release of Fireware v12.2.1 on your computer, you must run the Fireware v12.2.1 installer twice (once to remove v12.2.1 software and again to install v12.2.1).

Upgrade to Fireware v12.2.1 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\12.2.1\[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\12.2.1.
4. Install and open WatchGuard System Manager v12.2.1. 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 have installed a beta release of Fireware v12.2.1 on your computer, you must run the Fireware v12.2.1 installer twice (once to remove v12.2.1 software and again to install v12.2.1).

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.

There is an upgrade issue that affects some Firebox M400/M500 and M440 devices. Please review this knowledge base article carefully before you upgrade.

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.

Update AP Devices

Beginning with Fireware v11.12.4, AP firmware is no longer bundled with Fireware OS. All AP device firmware is managed by the Gateway Wireless Controller on your Firebox. The Gateway Wireless Controller automatically checks for new AP firmware updates and enables you to download the firmware directly from WatchGuard servers.

Important Upgrade Steps

If you have not previously upgraded to Fireware 12.0.1 or higher and the latest AP firmware, you must perform these steps:

1. Make sure all your APs are online. You can check AP status from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.
2. Make sure you are not using insecure default AP passphrases such as **wgwap** or **watchguard**. Your current AP passphrase must be secure and at least 8 characters in length. You can change your AP passphrase in **Network > Gateway Wireless Controller > Settings**.

If you do not have a secure passphrase correctly configured before the upgrade, you will lose the management connection with your deployed APs. If this occurs, you must physically reset the APs to factory default settings to be able to manage the APs from Gateway Wireless Controller.

Depending on the version of Fireware you are upgrading from, you may need to mark APs as trusted after the upgrade to Fireware v12.0.1 or higher. You can mark APs as trusted from Fireware Web UI in **Dashboard > Gateway Wireless Controller** on the **Access Points** tab, or from Firebox System Manager, select the **Gateway Wireless Controller** tab.

AP Firmware Upgrade

The current AP firmware versions for each AP device model are:

AP Device Model	Current Firmware Version
AP100, AP102, AP200	1.2.9.16
AP300	2.0.0.11
AP120, AP320, AP322, AP325, AP420	8.6.0-634

To manage AP firmware and download the latest AP firmware to your Firebox:

- From Fireware Web UI, select **Dashboard > Gateway Wireless Controller**. From the **Summary** tab, click **Manage Firmware**.
- From Firebox System Manager, select the **Gateway Wireless Controller** tab, then click **Manage Firmware.**

Note that you cannot upgrade an AP120, AP320, AP322, or AP420 to 8.3.0-657 or higher unless your Firebox is running Fireware v11.12.4 or higher. If your Firebox does not run v11.12.4. or higher, you will not see an option to upgrade to AP firmware v8.3.0-657 or higher.

If you have enabled automatic AP device firmware updates in Gateway Wireless Controller, your AP devices are automatically updated between midnight and 4:00am local time.

To manually update firmware on your AP devices:

1. On the **Access Points** tab, select one or more AP devices.
2. From the **Actions** drop-down list, click **Upgrade**.
3. Click **Yes** to confirm that you want to upgrade the AP device.

Upgrade your FireCluster to Fireware v12.2.1

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.

There is an upgrade issue that affects some Firebox M400/M500 and M440 devices. Please review this knowledge base article carefully before you upgrade.

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.

Downgrade Instructions

Downgrade from WSM v12.2.1 to earlier WSM v12.x or v11.x

If you want to revert from WSM v12.2.1 to an earlier version, you must uninstall WSM v12.2.1 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 v12.2.1.

Next, install the same version of WSM that you used before you upgraded to WSM v12.2. 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 v12.2.1. Verify that all WatchGuard servers are running.

Downgrade from Fireware v12.2.1 to earlier Fireware v12.x or v11.x

If you use the Fireware Web UI or CLI to downgrade from Fireware v12.2 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 v12.2.1 to an earlier version of Fireware, the recommended method is to use a backup image that you created before the upgrade to Fireware v12.2.1. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware v12.2.1 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.

See *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, 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.

This page does not include every issue resolved in a release.
Issues discovered in internal testing or beta testing are not usually included in this list.

Enhancements and Resolved Issues in WatchGuard System Manager 12.2.1 U1

- Policy manager no longer locks pre 12.0 configurations into Bridge mode. [FBX-13355]
- You can now create Branch Office VPN Virtual Interfaces with no physical interfaces in Firebox configuration. [FBX-13473]

Enhancements and Resolved Issues in Fireware and WSM 12.2.1

General

- This release resolves an issue that sometimes caused tabletop model Fireboxes to crash during times of heavy traffic. *[FBX-12174]*
- This release resolves multiple crash issues related to FireCluster. *[FBX-12265, FBX-13265, FBX-12746*]
- Traffic Monitor no longer fails to display log messages because of invalid bytes in UTF-8 sequences. *[FBX-12268]*
- When you log in to Firebox System Manager with an AD account, you can now successfully launch Policy Manager from that Firebox System Manager session. *[FBX-9651]*
- This release resolves a crash that sometimes occurred on boot for Firebox M370 devices. *[FBX-9038]*

Access Portal

- This release eliminates an error with mouse detection on the right edge of the screen in Access Portal RDP sessions. *[FBX-10121]*

Networking

- This release correctly allows you to set Link Monitor settings for modems on Firebox T10 and T15 devices. *[FBX-11040]*
- Dynamic DNS no longer incorrectly fails with invalid response from server (-2) message with dnsdynamic.org. *[FBX-11795]*
- This release resolves a dhcpd memory leak. *[FBX-11633]*
- The oss-daemon on the Firebox no longer crasesh when you change the DHCP server configuration. *[FBX-12228]*
- You can now clear interface check boxes in the Routing Table configuration and they are not selected automatically. *[FBX-13107]*
- You can now configure IP addresses assigned to a loopback interface in static NAT. *[FBX-3734, 91091]*

VPN

- To improve IKEv2 interoperability with Cisco devices, this release supports IKE_Auth initiator request packets larger than 28674. *[FBX-11644]*
- This release resolves an issue in a non-default profile name for L2TP clients could cause L2TP configurations to break if you use a combination of Web UI and Policy Manager for L2TP configuration. *[FBX-12250]*
- This release resolves a crash issue that occurred when a user connected to Mobile VPN with SSL on a Firebox with Quotas configured. *[FBX-12620]*

- The Firebox no longer generates a user space crash for IKE after multiple L2TP connection attempts. *[FBX-12727]*
- This release resolves a Web UI issue in which the Firebox would re-enable the *Allow SSLVPN-Users* policy when you save configuration changes. *[FBX-12224]*
- You can now configure the DF-bit options for any interface in a Branch Office VPN or Virtual Interface configuration. *[FBX-4878]*
- You can now select the secondary network IP address of an External VLAN in the BOVPN Gateway settings from Policy Manager. *[FBX-13102]*
- Mobile VPN with SSL no longer fails to connect when 1-to-1 NAT is configured for same external IP address. *[FBX-12274]*

Proxies and Services

- The SMTP proxy now preserves mime headers when it locks attachments because of scan errors. *[FBX-9042]*
- Web UI no longer allows you to leave the Quarantine Server IP Address text box blank when you configure a Quarantine proxy or APT action. *[FBX-3635, FBX-3592]*
- This release resolves an issue in which the POP3 proxy appends an extra line at the end of each email. *[FBX-12830]*
- The Firebox now correctly submits Office files with non-standard magic bytes for APT analysis. *[FBX-10656]*
- DNS resolution no longer fails when the firewall global DNS server list contains more than one IP address on a network with DNSWatch enforcement enabled. *[FBX-11560]*
- DNSWatch no longer fails on some interfaces when a Local DNS server appears first for DNSWatch on a different interface. *[FBX-12272]*
- You can now configure the SMTP Proxy Gateway AV and VOD to deny connections. *[FBX-4200]*
- In HTTP and Explicit proxy actions, you can now specify the level at which SafeSearch is enforced on YouTube. *[FBX-10292]*

Gateway Wireless Controller and WatchGuard APs

- AP firmware security and maintenance update for AP120, AP320, AP322, AP325, and AP420 (version 8.6.0-634).

Enhancements and Resolved Issues in WatchGuard IPSec Mobile VPN for Windows 13.10

- This release features a 64-bit version of each component.
- The Windows version now matches Windows 10 correctly.
- You can now use the pre-connect login client to connect to a hotspot.

To learn more about new features and feature enhancements for this release, review the What's New in Fireware v12.2.1 PowerPoint or recording.

Known Issues and Limitations

Known issues for Fireware v12.2.1 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 that version.

Using the CLI

The Fireware CLI (Command Line Interface) is fully supported for v12.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 for WatchGuard Firebox & Dimension.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at https://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