

FileWave Version 13.2.3 (Unsupported)



These downloads are provided for the purposes of migrations and should not continue to be used in production. You should upgrade to either the most recent release or the one prior. They can always be found here: [Supported FileWave Versions](#)

FileWave Management Suite

Included in the Installer

- Admin
- Server
- Booster
- Client

Compatibility



Server

- macOS 10.12 through 10.15 (binaries are 64 bit only)
- Windows Server 2012 R2 and Server 2016
- Linux CentOS 6.10 x86_64, and 7.7 x86_64 (binaries are 64 bit only)



Booster

- macOS 10.12 through 10.15 (binaries are 64 bit only)
- Windows 10, Windows Server 2012 R2 and Server 2016
- Linux CentOS 6.10 x86_64 and 7.7 x86_64 (binaries are 64 bit only)



Clients

- macOS 10.12 through 10.15 (binaries are 64 bit only)
- Windows 7 SP1, Windows 10, Windows Server 2012 R2 and Server 2016



Admin

- macOS 10.12 through 10.15 (binaries are 64 bit only)
- Windows 7 SP1 and Windows 10



Mobile Clients

- iOS 9.3, iOS 12 and iOS 13
- iPadOS 13
- tvOS 13
- Android 4.1, [4.2 *known issues](#), 4.3 (Jelly Bean), 4.4 (KitKat), 5, 6 and 7 (Legacy Android)
- Android 7 and above (EMM Client)
- Chromebook: ChromeOS 43+

Compatibility Chart

FileWave 13.2.0 OS Version Support							
OS	OS Version	Server	Booster	Admin	Client	MDM Client	EMM Client
OS X macOS	Sierra 10.12	✓	✓	✓	✓	✓	
	High Sierra 10.13	✓	✓	✓	✓	✓	
	Mojave 10.14	✓	✓	✓	✓	✓	
	Catalina 10.15	✓	✓	✓	✓	✓	
Windows	7 SP1			✓	✓		
	10 Pro/Enterprise		✓	✓	✓		
	Server 2012 R2	✓	✓		✓		
	Server 2016	✓	✓		✓		
	Server 2019	✓	✓		✓		
Linux 64bit	CentOS 6.10	✓	✓				
	CentOS 7.7	✓	✓				
iOS	iOS 9					✓	
	12					✓	
	13					✓	
tvOS / iPadOS	13					✓	
Android	4.1+					✓	
	5					✓	
	6					✓	
	7 Nougat					✓	✓
	8 Oreo						✓
	9 Pie						✓
	10						✓

*Note: See the FileWave downloads page for specific patch versions of supported operating systems.

FileWave 13.2 has not been tested against iOS 10 and iOS 11; nevertheless devices running those iOS versions should still be manageable with FileWave 13.2.

If you upgrade from FileWave 13.1.3 or below, /fwxserver will be moved to its new location /usr/local/filewave/fwxserver. In case moving is not possible (specific mount point for instance), upgrade will stop and will require manual data folder move.

For Details please refer to [fwxserver folder relocation in FileWave Server 13.1.5+ on macOS and Linux Platforms](#)

New Features (13.2.0, 13.2.1, 13.2.2)

Apple 2019 Fall Release Support:

[Apple New OS Support](#)

[Profile Changes](#)

[DEP Changes](#)

[Bootstrap Token Management](#)

Google Related Updates:

[Android EMM and ChromeBook Feature Improvements](#)

Device Management

[Client Renaming Changes](#)

[Uninstall Script Change](#)

Inventory

Inventory Field Changes/Additions

Additional Information



Included Open Source Software

[Click here for an extensive list of Open Source Software included in the FileWave products.](#)



Changes and Fixes in 13.2.3

- Upgrade to Qt 5.12.7 - <https://www.qt.io/blog/qt-5.12.7-released>
- FW-22735 "Serial Number" is now reporting WMI Value on Windows
- FW-23432 Fixed an issue where booster could be configured to accept less than 10 connections
- FW-23873 Fixed an issue where duplicating VPP fileset would reserve incorrect number of licenses
- FW-23874 Fixed an issue where insufficient license count would prevent from deleting clients
- FW-24452 Fixed an issue where server installer would fail on Linux distributions without sudo
- FW-24536 Fixed an issue where re-enrollment of clients running FileWave 13.0 or earlier would not be listed in New Clients dialog
- FW-24538 Fixed an issue where changing Auto-Enrollment setting could create duplicated entries
- FW-24645 Fixed an issue where Inventory Query results may be incomplete for non super-admin users
- FW-24771 Fixed several issues related to memory footprint of notification broker
- FW-24874 Fixed an issue where model update could be stuck at "Sending Model to MDM" when having timed iOS associations
- FW-24878 Fixed performance issue of Classroom view
- FW-24879 Fixed an issue where macOS 10.15 device would not report requested Software Update
- FW-24882 Fixed an issue in imaging fwcmd where client fingerprint would be incorrect



Fixes in 13.2.2

- FW-24744 Updated App Store Country chooser with newly supported countries
- FW-24756 Fixed an issue introduced with 13.2.0 where a race condition could lead to smart group evaluation failure



Fixes in 13.2.1

- FW-24658 Generate new signing certificate and profile for native app portal
- FW-24678 Fixed an issue where removing client certificate API would be denied
- FW-24700 Fixed an issue where changing verification setting of files would lead client to consider those files as executable and report script run failures
- FW-24709 Fixed several issues with profile installation via MDM on macOS
- FW-24714 Ensures macOS Upgrade Fileset only upgrades supported macOS versions



Fixes in 13.2.0

- FW-21259 Made sure iOS/tvOS serials are uppercase when importing client list from CSV
- FW-22284 Fixed an issue where renaming "All users" folder would rename any folder containing "All users" string
- FW-22375 Fixed various issues related to profiles used as Fileset dependencies
- FW-22444 Improved reliability of Application usage report on Windows clients
- FW-22535 Made sure pre-uninstall scripts are executed in Passive phase and not Delete phase
- FW-22538 Made sure license counts are immediately updated after updating license code
- FW-22881 Improved how Classroom class names are populated from Apple School Manager
- FW-22997 Fixed an issue where macOS 10.14+ devices would not requests some required macOS Software Updates
- FW-23207 Fixed Parental control payload - Deny URLs was not working properly
- FW-23215 Fixed an issue where FileWave agent could not be added to TCC profile
- FW-23246 Fixed an issue preventing from renaming properly Apple TV
- FW-23447 Ensure all internal components are 64b on macOS to support 10.15 Catalina
- FW-23457 Improved memory usage of Linux server
- FW-23534 Fixed inconsistency in importFolder command
- FW-23580 Fixed typo in 'Remote Wipe Clear' dialog
- FW-23653 Create New Association(s) dialogs are not updated if already open
- FW-23746 Scheduler is now using system proxy to contact Apple APN server
- FW-23883 Reduce unnecessary noise in fwadmin.log
- FW-24016 Fixed an issue where importing folder would not follow symlinks
- FW-24025 Fixed an issue where Custom Field based inventory queries could be very slow
- FW-24102 Report itunes store account hash for mac devices as well
- FW-24113 Unify settings for Smart Group Evaluation interval ; now everything is driven by Admin console settings
- FW-24118 Allow "SetupMode" for non-Enterprise Wi-Fi Security modes
- FW-24198 Fixed an issue where negative association for MDM fileset would not remove the fileset
- FW-24200 Fixed an issue where iBooks would be self-healed on macOS while books can't be managed on macOS
- FW-24240 Fixed various server performance issues due to incorrect usage of internal cache
- FW-24249 Fixed Classroom self-signed certificate generation to be compliant with iOS 13 and macOS 10.15
- FW-24255 Fixed an issue where Observe Client feature may not work after client restart when "Route server messages via booster" is enabled

- FW-24332 Fixed a performance issue due to large Certificate Revocation List (CRL)
- FW-24341 Fixed a possible issue where LDAP based custom field would not be updated properly
- FW-24353 Improved security related to Observe Client feature on Windows
- FW-24360 Fixed an issue where iOS device smartgroup membership could temporarily out-dated just after hitting model update
- FW-24414 Fixed an issue where iOS devices would be sent APNs in case of membership change of SmartGroup, even if SmartGroup has no fileset associated
- FW-24498 Fixed an issue where enrolling a desktop device to another server would not work unless certificate is manually removed from device
- FW-24503 Fixed an issue where duplicated client would be added to the model and create duplicated entries
- FW-24515 Made sure conflict resolution actions are properly logged in audit log
- FW-24517 Fixed an issue where client in conflict would still be added if auto enrollment is set, creating duplicates
- FW-24527 Fixed an issue where conflict detection would not work for 13.0 clients or older
- FW-24551 Fixed an admin crash when Client Info dialog is open for a device and the device is removed by conflict resolution
- FW-24782 Fixed an issue where MDM or EMM devices impacted by Smart Group change would not be notified and thus would not get modifications in a timely manner
- GOOG-170 If FileWave recognizes that an error is permanent (e.g., a device no longer managed upstream) it elides all unnecessary upstream communication.
- GOOG-256 Audited EMM-borne log messages to include (where possible) precise information as to the error or state. For example, FileWave logs relevant Fileset IDs and exact upstream error messages.
- GOOG-274 Fixed EMM icon in Client Report.8
- GOOG-279 Passwords are obfuscated when viewed (e.g., Client Report dialog); implemented a checkbox to optionally show them during input or editing.
- GOOG-283 Fixed duplicate EMM entries. A device enrolled once, ten, or N times will always be matched to same record in FileWave.

Downloads

Your existing FileWave Server must be version 12.3.0 or higher before you can upgrade to FileWave 13.1+.



Upgrading

Please read: <https://kb.filewave.com/display/KB/Upgrading+your+FileWave+Server>

This article contains important information that will help ensure your upgrade runs smoothly. It is strongly advised that you review this for each release, since new notes or instructions may have been added.

Please make sure you have a recent backup before upgrading your server.

Upgrading FileWave requires the FileWave Imaging Appliance (IVS) is upgraded to a compatible version to ensure communication continues. Example: FileWave 13.2.0 requires the 6.2 IVS to image your computers.
The FileWave Engage Server must be version 1.2.0 or greater for compatibility.

In order to avoid problems with migrating database internal structures please make sure that you use a local administrator account, not domain administrator, when performing FileWave Server upgrade on Windows platform.



Location Tracking

The location reporting feature in FileWave is disabled by default.

It is recommended that you verify that this feature is in accordance with your organization's policies and AUP (Acceptable Use Policy). Notify your end users before activating location reporting, as enabling the feature will prompt for permission to location information.

Read more... [The Location Tracking KB \(https://kb.filewave.com/display/KB/Location+Tracking\)](https://kb.filewave.com/display/KB/Location+Tracking)

Before Upgrading

Version 13.0.x introduces higher security standards which have impact on self-signed certificate usage.

While it is recommended to use Trusted-CA issued certificates, you can still use self-signed certificate with FileWave ; please make sure you follow the upgrade steps described in this [KB article](#).

Following upgrade steps is important to make sure your FileWave setup works properly !

With FileWave 13.0.x, FileWave uses new [Apple Push Notifications service](#) with HTTP/2 protocol ; make sure your FileWave server can contact <https://api.push.apple.com> (port 443).

Security Changes

Starting with FileWave 13.1.0, all components (clients and boosters) will be assigned a certificate to validate their access to your FileWave instance. This implies that [Boosters need to be enrolled](#) to be part of your FileWave setup.

When upgrading, a [Compatibility Mode](#) will automatically be enabled to ease transition ; in this mode, already enrolled clients will automatically be assigned a certificate, but [Boosters will require manual "create certificate" operation](#) once upgraded to 13.1. You can figure out which booster requires a certificate by looking at the booster view.

If you are using a self signed certificate for your FileWave Server, Booster trust store needs to be updated to trust this certificate. The

easiest way is to go through our [Custom Package Builder Service](#) and generate a Booster Package which will contain the server certificate.

Web admin console

With version 13.0.x comes the first iteration of FileWave web-based admin console. It will be installed automatically and uses default HTTPS port (443).

Upgrade to 13.0.x will fail if port 443 is not available (upgrade will fail without upgrading your server, leaving it with the previous version running).

It is recommended to use a dedicated server for FileWave ; if you want to share the server with other services that require HTTPs port, follow the following steps:

- stop other service using 443
- install FileWave 13.0.x
- change FileWave admin port to an unused as described in [Change Default Web Console Port](#) KB article
- restart FileWave 13.0.x
- restart other service

In order to support Catalina, if you upgrade from FileWave 13.1.3 or an earlier version, /fwxserver will be moved to its new location. In case moving is not possible (specific mount point for instance), upgrade will stop and will require manual data folder move.

For Details please refer to [fwxserver folder relocation in FileWave Server 13.1.5+ on macOS and Linux Platforms](#)

Backup Script Update:

With the relocation of /fwxserver, the backup script must be updated on your server to ensure a proper backup is being captured.

Please reference the following for more information; <https://kb.filewave.com/display/KB/Automated+Backup>

macOS Downloads

[macOS Installers](#)

[macOS Upgrade Fileset](#)

Windows Downloads

[Windows Installers](#)

[Windows Upgrade Fileset](#)

In order to avoid problems with migrating database internal structures please make sure that you use a local administrator account, not domain administrator, when performing FileWave Server upgrade on Windows platform.

Linux Downloads

[Linux Installers](#)

Note: Use the following command to download and unzip the installers:

```
wget https://fwdl.filewave.com/13.2.3/FileWave_Linux_13.2.3.zip
```

```
unzip FileWave_Linux_13.2.3.zip
```

Since v11+ only has one installer (that installs both mdm and server), the old standalone mdm will be removed automatically when doing an upgrade. This does not delete any mdm data.

To install or upgrade the FileWave Server, use the following :

```
yum install -y --nogpgcheck fwxserver-13.2.3-1.0.x86_64.rpm
```

To install or upgrade the FileWave Booster, use the following :

```
yum install -y --nogpgcheck fwbooster-13.2.3-1.0.x86_64.rpm
```

iOS Downloads

This is a native app version of the traditional Web Clip kiosk/app portal that is sent to devices ; it provides for a better end user experience and is highly recommended for iOS 9 devices (required for location information).

iOS 9+ : [FileWave Enterprise.ipa](#)

Static CDN URL :

```
https://fwdl.filewave.com/13.2.3/app_kiosk/filewave/App%20Portal%2013.2.3.ipa
```

Android Downloads

This is the Android APK, and can be downloaded and associated to update already enrolled Android Devices.

[FileWaveClient-13.2.3.apk](#)

[Skeleton for Android white-boxing](#)

Chrome

The FileWave Inventory extension for Chromebook has to be installed via the Google Admin Console for your domain. Please see [Quickstart Guide for Chromebooks](#) for detailed instructions

[Skeleton for Chromebook white-boxing](#)

Virtual Appliance Downloads

[VMware and VirtualBox \(OVA\) Server Appliance](#)

[VMware and VirtualBox \(OVA\) Booster Appliance](#)

For more information about importing the appliances please see: [Importing Virtual Appliances](#)

Hyper-V Appliance Downloads

[Hyper-V \(VHD\) Server Appliance](#)

[Hyper-V \(VHD\) Booster Appliance](#)

🔄Revision #4

★Created 12 June 2023 18:21:37 by Josh Levitsky

✍Updated 9 December 2024 14:30:30 by Josh Levitsky