FileWave Version 13.1.5 (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 10.11 through 10.15 (binaries are 64 bit only)
- Windows 7 SP1, Windows 10, Windows Server 2008 R2, 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 through iOS 13, iPadOS 13
- tvOS 10 through tvOS 13
- Android 4.1, 4.2 *known issues, 4.3 (Jelly Bean), 4.4 (KitKat), 5, 6 and 7 (Legacy Android)
- Android 7, 8 and 9 (EMM Client)
- Chromebook: ChromeOS 43+

Compatibility Chart

FileWave 13.1.5 OS Version Support							
OS	**OS Version**	**Server**	**Booster**	**Admin**	**Client**	**MDM Client**	**EMM Client**
OS X **macOS**	Mountain Lion 10.8			***Legacy (9.1.2)**	***Legacy (11.1.2)**		
	Mavericks 10.9			***Legacy (10.1.2)**	***Legacy (12.3.0)**		
	Yosemite 10.10		■	***Legacy (11.1.2)**	***Legacy (12.9.1)**	***Legacy (12.9.1)**	
	El Capitan 10.11	■	■	***Legacy (12.3.0)**	✔	✔	
	Sierra 10.12	✔	✔	✔	✔	✔	
	High Sierra 10.13	✔	✔	✔	✔	✔	
	Mojave 10.14	✔	✔	✔	✔	✔	
	Catalina 10.15**	✔	✔	✔	✔	✔	
Windows	7 SP1		■	✔	✔		
	8/8.1			***Legacy (11.2.2)**	***Legacy (11.2.2)**		
	10 Pro/Enterprise		✔	✔	✔		
	Server 2008 R2	■	✔		✔		
	Server 2012				***Legacy (11.2.2)**		
	Server 2012 R2	✔	✔		✔		
	Server 2016	✔	✔		✔		
Linux 64bit	CentOS 6.10	✔	✔				
	CentOS 7.6	✔	✔				
iOS **tvOS** **iPadOS**	iOS 9					✔	
	10					✔	
	11					✔	
	12					✔	
	13**					✔	
Android	4.1+					✔	
	5					✔	
	6					✔	
	7 Nougat					✔	✔
	8 Oreo						✔
	9 Pie						✔

*Note: See the FileWave downloads page for specific patch versions of supported operating systems.
** FileWave 13.1.5 installs on 10.15 and manages 10.15, iOS/tvOS/iPadOS 13 devices without new feature support.

Key

✔ = FileWave 13.1. is fully supported.
■ = FileWave component is no longer supported on this platform.
***Legacy** = Supported using an older version of the FileWave Admin or Client. Does not support FileWave 13.1+ features/functionalities. Legacy Clients require Compatibility mode.

New Features (13.1.5)

- Compatibility support for macOS Catalina

macOS Catalina brings new restrictions and security changes; one of these changes is the new Read-Only System Volume, introduced to protect the system from un-wanted changes. As your FileWave server stores files in /fwxserver, it is impacted by this change. FileWave 13.1.5 is now locating files in /usr/local/filewave/fwxserver; if you are upgrading from a previous version, files will be moved during upgrade.

If you upgrade from a previous version of FileWave, /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; Automated FileWave Server Backup

- TLS self-signed certificate for MDM

Generated self-signed cert is compliant with iOS 13, tvOS 13 and macOS 15 new security requirements.

fwcontrol generateSelfSignedCert command uses previous private key, allowing to unblock already upgraded devices

- Duplicated devices detection

FileWave clients are identified by a user-friendly identifier (client name) and a machine-fingerprint identifier (device id). Re-enrolling devices with a different name or enrolling a new device with the same name as an existing client creates duplicated entries in the

system, which can lead to various problems. FileWave 13.1.5 integrates duplicated detection:

- At enrollment time; enrolling a device matching either the client name or the fingerprint, but not both (so not a in place re-enrollment) will not be possible without solving the conflict (removing the old entry or ignoring the new enrollment).
- tools are provided to detect and resolve existing duplicated entries
- OpenSSL updated to 1.0.2t

New Features (13.1)

Security Enforcement

- End-to-End encrypted notifications
- TLS certificates for all FileWave components:
- Clients and boosters now request a certificate when added to FileWave; the certificate is checked by other peers (client contacting booster, booster contacted by client...) to ensure communications are safe
- Boosters now need to be enrolled to be allowed to communicate
- Compatibility mode allows to transition to 13.1
- New admin permissions
- Activation Lock Bypass code management
- Server preferences
- OCSP Stapling support
- Updated MDM enrollment to follow updated Apple guidelines

Device Management

- iOS/tvOS Smart Groups are now as dynamic as Desktop Smart Groups
- iOS devices can now be locked like Desktop Devices to not impact them with Model Update
- New LDAP Safety - Missing clones can be kept for a defined number of extractions
- DEP Profile Auto assignment rules
- Inventory fields can be used in DEP naming scheme
- Custom Field definition can now be imported / exported
- License definitions can be based on Custom Field
- Improved usability of Reinstall Fileset feature when selecting several devices

Analytics

- Analytics are now collected daily and sent to an Elasticsearch database
- Information collected is the following:
- License information and usage
- Number of clients per device type
- Map of versions for clients/server/boosters
- Logging level
- Number of Filesets
- Imaging usage (count and associations)
- Number of fileset groups and number of associations to fileset groups
- Server and Boosters OS version
- Available and used disk-space
- Engage configuration
- Classroom configuration
- Number of model updates in the past 24h
- Number of restarts in the past 24h
- WebUI usage (general and fileset reinstall
- The information is packed in a JSON file and sent to Logstash for data validation and enrichment

UCS Improvements

- Automatic set-up of certificate and hostname (read from UCS)
- Automatic set-up of LDAP (Accessible in FileWave, configuration read from UCS)
- Login to FileWave using your UCS credentials

Apple "Spring 2019" release support

- Support for iOS 12.2, tvOS 12.2, macOS 10.14.4
- Classroom can now be used on macOS
  - 10.14.4 is required
  - Classes can be composed of iPads and macOS devices
  - Known issue: student pictures are currently not displayed on macOS teacher devices
- New or updated profiles:
- macOS - Restrictions - new options (Classroom, screen sharing related)
- macOS - Exchange - authentication options for Exchange Web Services
- macOS - Security And Privacy - FireWall can be excluded from the profile
- macOS - Content Caching has now more options
- macOS - Setup Assistant - "Skip True Tone" option
- macOS - Mobile Account - cachedaccounts.askForSecureTokenAuthBypass option
- Transparency and Consent Configuration profile has now a dedicated entry
- iOS - Restrictions - new options for Personal Hotspot modification and disable server-side Siri Logging
- iOS - Restrictions - allowESIMModification option
- tvOS - Restrictions - defer software update and force automatic date and time
- New Certificate Transparency Profile

- New MDM commands:
- Enable or Disable Remote Desktop (macOS)
- UnlockUserAccount - allows to unlock a local user account that has been locked for too many failed password attempts (macOS)
- Support for iOS Per-App-VPN, which allows to configure a specific VPN for a specific application.
- Support for iBoss Per-App-VPN
- Support for tvOS Software Update
- Update DEP profile:
- New Skip Item : "SIMSetup" (iOS)
- Updated Admin Account creation for macOS
- Support for MDM Activation Lock
- Improved Shared iPad support:
- When non-current user is deleted, current user won't be logged out.
- Scheduled log out verifies now iOS updates

Android (EMM) support

- Support for Android devices using Google EMM API
- Enroll devices to FileWave using QR or alphanumeric code
- Configure Play Store applications
- Deploy Play Store applications
- Gather inventory information
- Send commands
- Reboot device
- Lock device
- Unlock device
- Wipe device
- Deploy configuration (policy)
- Network (WiFi) policy
- Compliance policy
- Password policy
- Device Restrictions policy
- Permission Grants policy

Additional Information

Included Open Source Software

Click here for an extensive list of Open Source Software included in the FileWave products.

Fixes in 13.1.4 and 13.1.5

- FW-23423 Fixed a possible issue where clients could be removed from Smart Groups due to duplicate file ids
- FW-23757 Fixed appearing of VPP error 9600
- FW-23828 Fixed an issue preventing enrollment if client sends new certificate request before previous one has been accepted
- FW-23916 Fixed an issue where Windows Upgrade fileset would not upgrade on Spanish localized Windows
- FW-23917 Improve server stability when duplicating filesets with some specific file date time
- FW-23940 Fixed deadlock between house_keeping and send_next_queued_command on acquiring lock on ios_commands
- FW-23948 Moved FileWave agent on macOS to /Applications to be properly indexed under macOS 10.15 Catalina
- FW-23966 Fixed an issue where model update would fail if devices are removed, re-enrolled before model is updated, and auto-enroll is enabled
- FW-23984 Fixed a potential issue where re-enrolling devices while auto-enroll is turned on would fail due to renamed clients
- FW-23986 Fixed an issue where server could be frozen when processing inventory data of auto-enrolled devices
- FW-24012 Fixed an exception when the server is busy during model update
- FW-24013 Fixed an issue where instances impacted by FW-23810 (fixed in 13.1.5) may contain invalid commands in command queue which can't be sent to device
- FW-24014 Fixed a potential issue preventing model update when server is under load
- FW-24015 Fixed a potential issue preventing SCEP process to succeed when server is under load
- FW-24018 Fixed an issue where VPP synchronization could last long in case of multiple tokens
- FW-24020 Fixed a possible upgrade from 13.0.0 issue due to Classroom certificate revocation
- FW-24023 Fix VPN profile not properly storing "Send All Traffic" option
- FW-24031 Fixed an issue where client sending certificate request would be temporarily removed from smart groups
- FW-24046 Fixed an issue where some results could be missing in inventory query based smart groups
- FW-24048 Added to Custom VPN profile missing options like Provider Type, ProviderBundleIdentifier or On Demand options
- FW-24052 Fixed an issue where Smart Group evaluation for automatically created LDAP groups could not return consistent results over time
- FW-24059 Improve FileWave component reliability when server is under load
- FW-24060 Fixed an issue where InviteToProgram command could be sent in loop when App Store is restricted on devices
- FW-24064 More smart approach of handling MDM commands was implemented to not have large MDM command history which can slow server
- FW-24067 Fixed exception if renamed client has the same name as placeholder without serial
- FW-24068 Fixed exception during enrollment, if 2 UCGs have same serial_number for enrolled device
- FW-24072 Improved server responsiveness when several auto-assignment DEP rules are configured
- FW-24073 Fixed an issue where client could request previous dependency, impacting booster performance
- FW-24078 Improved client error message when file download fails
- FW-24080 Improved booster performance when clients are requesting outdated files
- FW-24100 Updated Custom Setting profile to support macOS assessment profile

- FW-24151 Ensure Unlock Token is not removed when iOS 13 devices send Update Token message without UnlockToken
- FW-24158 Native Kiosk does not require developer trust on iOS 9 anymore
- FW-24169 Ensure generated self-signed certificate is compatible with iOS 13, tvOS 13 and macOS 10.15
- FW-24183 Fixed an issue where Android/Chromebook Firebase notification requests could not be sent

Fixes in 13.1.2

- FW-23969 Fixed an issue where enrollment username could be incorrectly cleared when desktop devices submit new certificate signing request
- FW-23792 Updated Google ChromeBook API after Google changes on paging - allows to get ChromeBook data again
- FW-23980 Fixed an issue where restarting booster while server is under load would reject older clients until booster can reach the server even with Compatibility Mode set

Fixes in 13.1.1

- FW-23294 Fixed an issue where Windows upgrade Fileset would leave several cmd.exe processes running
- FW-23397 Fixed an issue where profiles installed via MDM on macOS would not report installation error
- FW-23418 Fixed an issue where Admin console would crash when getting Script Output from Client Info
- FW-23429 Fixed typo in Classroom association dialog
- FW-23446 Fixed an issue where ldap extraction status would not be reported in dashboard
- FW-23460 Fixed an issue where admin console would freeze when removing offline IVS server
- FW-23535 Fixed an error message in server logs about illegal tickle message
- FW-23546 Fixed an installer issue where Admin installer would remove fwcontrol on macOS
- FW-23553 Fixed an issue where iOS smartgroup data would be processed by MDM even when there is no iOS device, leading to misleading entries in log
- FW-23562 Fixed a potential admin crash when using "Move to" with root group
- FW-23631 Fixed an issue where enrolling iOS device would not work if enrollment would be blocked
- FW-23635 Fixed an issue where defining automatic DEP profile rules could lead to incorrect calls to Apple services
- FW-23637 Fixed an issue where re-enrolling wiped macOS device would not be possible due to CSR errors
- FW-23638 Fixed an issue where enrollment fails if IPv6 is enabled
- FW-23651 Fixed an issue where IVS could not be enrolled in some situations
- FW-23663 Fixed "Mass Enrollment" profile
- FW-23677 Fixed an issue where creating certificates for IVS instances must be done in the exact order
- FW-23691 Fixed an issue where model update would fail due to out of range identifier
- FW-23736 Fixed an issue where client would not be able to contact booster if server is under load and compatibility mode is set
- FW-23737 Fixed an issue where client could not get certificate (error 500) if model contains duplicated entries for the client
- FW-23744 Fixed an issue where MDM profile whiteboxing would prevent enrollment
- FW-23745 Fixed an issue where Database Checker tool would report false positive
- FW-23748 Fixed an issue where renaming device while no enrollment authentication is set would fail
- FW-23752 Fixed an issue where concurrent accesses to client information could cause various problems, including blocked model update
- FW-23756 Fixed fwxserver -s crash due to race condition when enrolling new device having associated software updates
- FW-23772 Fixed an issue where creating Custom Field values associated to all devices would fail during model update
- FW-23796 Fixed an issue where device fingerprint could not be generated from hardware details and therefore be common to multiple devices
- FW-23804 Fixed appearing of invalid entry in admin.user table
- FW-23808 Fixed an issue where model update would fail due to out of range identifier (iOS Updates)
- FW-23810 Fixed an exception when a DEP device is enrolled after being removed from admin without updating model. Naming scheme must be "use client name"
- FW-23827 Fixed appearing of error with code -200 when trying to re-enroll upgraded client
- FW-23842 Fixed an issue where iPad OS 13 Beta devices could not be enrolled
- FW-23872 Fixed an issue where model update could be blocked due to concurrent access to device serial numbers
- FW-23876 Fixed an issue where FileWave server could be hanging due to concurrent access to device login information
- GOOG-184 Android Service Account window can cut off text due to resizing on macOS
- GOOG-254 Android Devices hiding in new mobile UI
- GOOG-258 Unable to update policies (and thereby devices) after Google's complianceRules change
- GOOG-278 Prevent from creating a second EMM service account

Downloads

Your existing FileWave Server must be version 12.0.3 or higher before you can upgrade to FileWave 13.1+.

Upgrading

Please read: Upgrading your On-Premise 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 13.1.0 requires the 6.1 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... 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

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/13.1.5/FileWave_Linux_13.1.5.zip
```

```
unzip FileWave_Linux_13.1.5.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-13.1.5-1.0.x86_64.rpm
```

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

```
yum install -y --nogpgcheck fwbooster-13.1.5-1.0.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/13.1.5/app_kiosk/filewave/App%20Portal%2013.1.5.ipa
```

Android Downloads

This is the Android APK, and can be downloaded and associated to update already enrolled Android Devices.
FileWaveClient-13.1.5.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 #9
★Created 12 June 2023 18:18:43 by Josh Levitsky
✎Updated 9 December 2024 14:30:30 by Josh Levitsky