FileWave Version 13.1.3 (Unsupported)

> ℹ 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

This version includes preliminary support for iOS 13. It contains a change to support iOS 13 MDM protocol changed related to Unlock Token which could prevent previous versions of FileWave from clearing passcode on iOS 13 devices.

Included in the Installer

- Server

Compatibility

Server

- macOS 10.12 through 10.14 (binaries are 64 bit only)
- Windows Server 2012 R2 and Server 2016
- Linux CentOS 6.10 x86_64, and 7.6 x86_64 (binaries are 64 bit only)

Booster

- macOS 10.12 through 10.14 (binaries are 64 bit only)
- Windows 10, Windows Server 2012 R2 and Server 2016
- Linux CentOS 6.10 x86_64 and 7.6 x86_64 (binaries are 64 bit only)

Clients

- macOS 10.11 through 10.14 (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 10.14 (binaries are 64 bit only)
- Windows 7 SP1 and Windows 10

Mobile Clients

- iOS 9 through iOS 12 ; preliminary support for iOS 13
- tvOS 10 through tvOS 12 ; preliminary support for iOS 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

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		✓	✓	✓	✓	
Windows	7 SP1				✓		
	8/8.1		⚠	*Legacy (11.3.2)	*Legacy (11.3.2)		
	10 Pro/Enterprise		✓		✓		
	Server 2008 R2	⚠	✓				
	Server 2012		✓		*Legacy (11.3.2)		
	Server 2012 R2	✓	✓				
	Server 2016	✓	✓				
Linux 64bit	CentOS 6.10	✓	✓				
	CentOS 7.6	✓	✓				
iOS tvOS	iOS 9					✓	
	10					✓	
	11					✓	
	12					✓	
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]

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.

Version 13.1.3 is supported on the same platforms as 13.1.1, but brings preliminary support for iOS 13.

New Features (13.1)

Please read Version 13.1.0 Release notes for new features introduced in 13.1 release.

Additional Information

Included Open Source Software

⌄

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

Fixes in 13.1.3

⌄

- FW-24018 Fixed an issue where VPP synchronization may take time if several tokens are used
- FW-23966 Fixed an issue where model update would fail due to deleted device re-enrolled before model is updated
- FW-23757 Fixed an issue where request VPP license from Apple API would fail with error 9600
- FW-24015 Fixed a possible issue during SCEP enrollment due to server load
- FW-24012 Fixed an issue where requesting MDM device check-in fails when server is under load
- FW-24031 Fixed an issue where devices requesting CSR would be temporarily removed from Smart Groups
- FW-24060 Fixed an issue where InviteToProgram command is sent despite App Store restriction
- FW-24013 Fixed an issue where instances impacted by FW-23810 would contain invalid commands in command queue which could not be sent to devices
- FW-23267 Fixed an issue where permanent connection to Apple APN service would not be re-created if closed by network issue
- FW-24064 Fixed an issue where large MDM command history could slow the server
- FW-24063 Added a way to ignore Apple stock apps from management to workaround recurring issue on unboxed devices
- FW-24068 Fixed an issue where enrolling DEP device fails if multiple clients have the same serial number in the model
- FW-24151 Ensures iOS 13 sending empty Unlock Token is not clearing token from database, preventing Clear Passcode
- FW-24052 Fixed a possible issue where devices could be removed from LDAP smart groups

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: 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 13.1.0 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... The Location Tracking KB (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 /wiki/spaces/DRAFT/pages/4327696 KB article
- restart FileWave 13.0.x
- restart other service

macOS Downloads

macOS Server

Windows Downloads

Windows Server

This package is provided to upgrade existing Windows instances. New instances are recommended to be installed on linux server.

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 Server

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

wget https://fwdl.filewave.com/13.1.3/fwxserver-13.1.3-1.0.x86_64.rpm

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

yum install -y --nogpgcheck fwxserver-13.1.3-1.0.x86_64.rpm

Virtual Appliance Downloads

VMware and VirtualBox (OVA) Server Appliance

For more information about importing the appliances please see: Importing FileWave Appliances

Hyper-V Appliance Downloads

Hyper-V (VHD) Server Appliance