FileWave Version 13.1.0 (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 10.14 (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

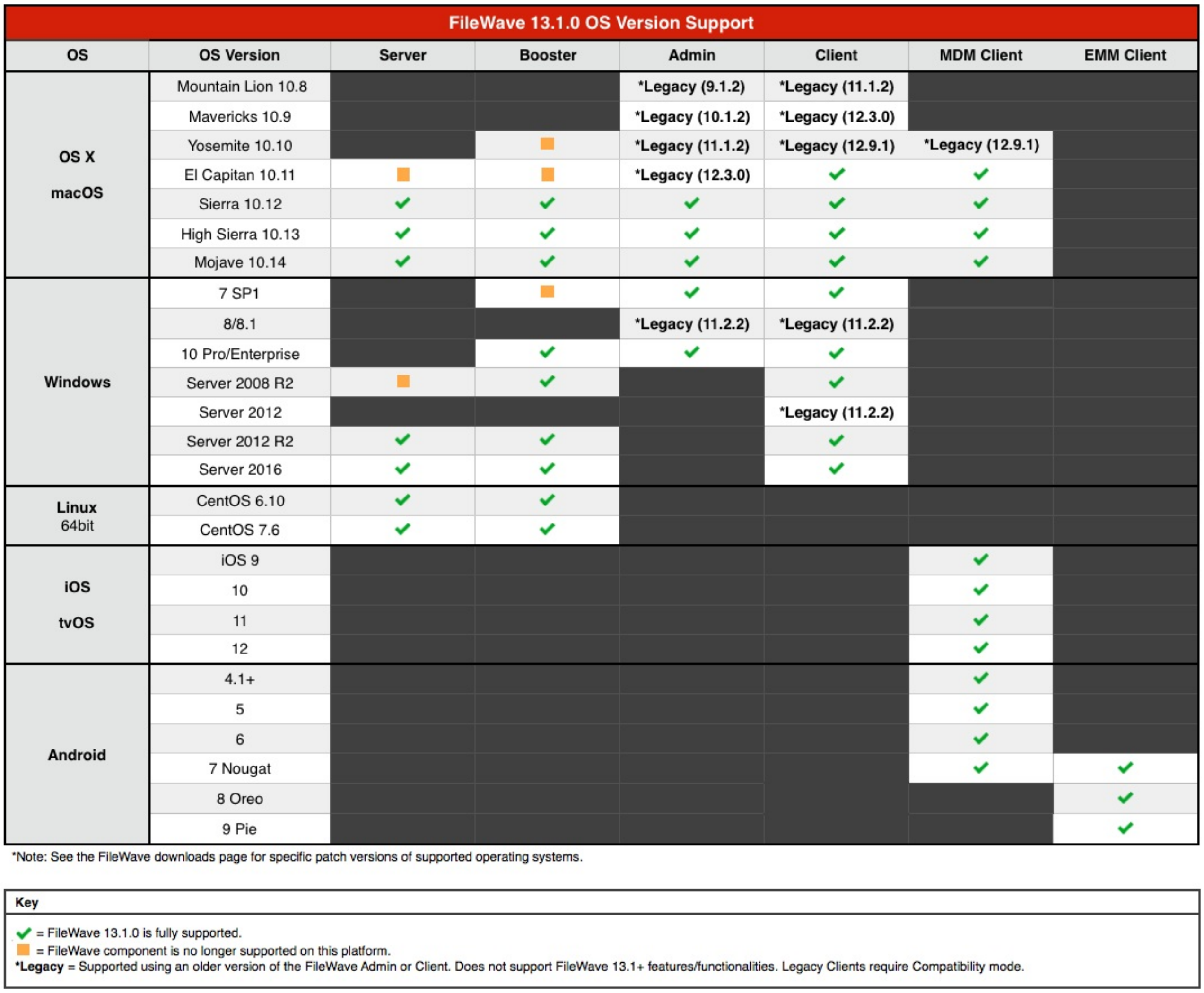
Admin

- macOS 10.12 through 10.14 (binaries are 64 bit only)
- Windows 7 SP1 and Windows 10

Mobile Clients

- iOS 9 through iOS 12
- tvOS 10 through tvOS 12
- 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 13.1.0 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	✓	✓	✓	✓	✓	
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	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 13.1.0 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)

Changes and New Features

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

⌄

- CT-747 Fixed an issue where filesets with invalid status are not properly filtered and counted (web console)
- CT-847 Fixed an issue where reinstall fileset would not work from web console
- FW-18330 Fixed an issue where non current users would receive APN on shared iPads
- FW-18468 Fixed an issue where Kiosk filesets would not be visible if they depended on non Kiosk filesets
- FW-18817 Fixed an issue where creating Software Update fileset at the same time as Model Update would lead to partial fileset
- FW-19336 Fixed an issue where deleting user data on shared iPad would log out the current user even if the deleted user was not the current one
- FW-20393 Fixed an issue where network users would not show up properly in Login Window profile
- FW-20842 Fixed a potential issue where internal database data would be incorrectly created twice for the same MDM user, which could cause Model Update failure
- FW-20932 Fixed an issue where admin would hang when duplicating large filesets, mainly on Windows
- FW-21654 Fixed an issue where LDAP custom fields would not find the matching user or computer when using Open Directory
- FW-21957 Fixed an issue where initially non-DEP enrolled devices re-enrolled via DEP would be duplicated after re-enrollment
- FW-22007 Fixed an issue where unchecking "Automatically deploy to requesting client" in Software Updates would not prevent devices waiting for reboot to install the fileset
- FW-22031 Fixed an issue where clients on hold due to limited free space would not continue deployment if the margin is lowered
- FW-22109 Fixed a performance issue when changing verification settings on large filesets
- FW-22139 13.0.0 Server installation failure on macOS
- FW-22170 Fixed an issue where removing a field used as sort column in query builder raised an error
- FW-22191 Fixed an issue where Inventory Query preview for Smart Group would return different results than Smart Group
- FW-22192 Fixed an issue where license management would report license details for devices even if the current admin has no read permission for those devices
- FW-22202 Fixed an issue where the DEP profile assistant could create an incorrect DEP profile
- FW-22207 Fixed an issue where admin would crash when replacing a fileset folder while another admin renames the folder
- FW-22219 Fixed a possible admin crash when an admin would delete a smart group while another admin edits it at the same time
- FW-22287 Added rotation for scheduler log
- FW-22438 Fixed an issue where Application bundle size would be reported as numeric value instead of byte size
- FW-22508 Fixed an issue where Activation Lock Bypass Codes would not be removed correctly
- FW-22520 Fixed an issue where Application Inventory Scanner would not run on a regular basis
- FW-22607 Fixed an issue where a logged out admin would still contact server until the message box is closed
- FW-22611 Fixed an issue where Apple TVs would not not report the updated version of tvOS
- FW-22901 Fixed an issue where restarting the admin console would be required to see newly auto-enrolled devices
- FW-23081 Fixed an issue where the macOS client package would not be deployed when enrolling to MDM
- FW-23112 Fixed an issue where discovery last status update would not be reported properly
- FW-23201 Fixed an issue where model update could hang due to a large number of requests
- FW-23217 Fixed an issue where Android enrollment would fail with Windows LDAP authentication
- FW-23219 Fixed an issue where booster would not serve file if Software Update data is not downloaded completely
- FW-23262 Fixed an issue leading to high CPU for fwxserver related to kiosk download statistics
- FW-23265 Fixed an issue where adding self-signed certificate to macOS upgrade fileset would modify folder permissions on existing filesets
- FW-23292 Fixed an issue where Windows trust store would not be updated when using globally trusted but not already installed CAs
- FW-23299 Fixed a possible crash on Windows due to openssl
- FW-23304 Fixed an issue where the macOS PIN code field was greyed out in the Remote Wipe dialog
- FW-23305 Fixed an issue where Engage on iOS would not respond to notifications
- FW-23396 Fixed an issue where associating VPP user to device would not work

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 Installers

macOS Upgrade Fileset

A known issue in original 13.1.0 Admin installer removes fwcontrol from the system. Installer has been updated June 12th and fixes the issue ; in case you installed the previous version, you can restore fwcontrol with the following command:

```
sudo mkdir -p /usr/local/bin; sudo curl http://fwdl.filewave.com/13.1.0/fwcontrol -o /usr/local/bin/fwcontrol; sudo chmod a+x
/usr/local/bin/fwcontrol
```

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/13.1.0/FileWave_Linux_13.1.0.zip
```

```
unzip FileWave_Linux_13.1.0.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-13.1.0-1.0.x86_64.rpm
```

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

```
yum install -y --nogpgcheck fwbooster-13.1.0-1.0.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/13.1.0/app_kiosk/filewave/App%20Portal%2013.1.0.ipa

Android Downloads

This is the Android APK, and can be downloaded and associated to update already enrolled Android Devices.
FileWaveClient-13.1.0.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 FileWave Appliances

Hyper-V Appliance Downloads

Hyper-V (VHD) Server Appliance

Hyper-V (VHD) Booster Appliance

⟲Revision #1
★Created 2 January 2024 16:20:52 by Josh Levitsky
✎Updated 27 August 2024 12:48:38 by Josh Levitsky