

FileWave Release History

FileWave issues major releases on a roughly quarterly basis. You'll find the history of features in previous releases shown below.

FileWave 15.4.x (June 2024)

[FileWave Version 15.4.0 details.](#)

[FileWave Version 15.4.1 details.](#)

FileWave 15.3.x (April 2024)

[FileWave Version 15.3.1 details.](#)

FileWave 15.2.x (November 2023)

[FileWave Version 15.2.1 details.](#)

FileWave 15.1.x (September 2023)

[FileWave 15.1.1 details.](#)

FileWave 15.0.x (June 2023)

[FileWave Version 15.0.1 details.](#)

FileWave 14.10.x (March 2023)

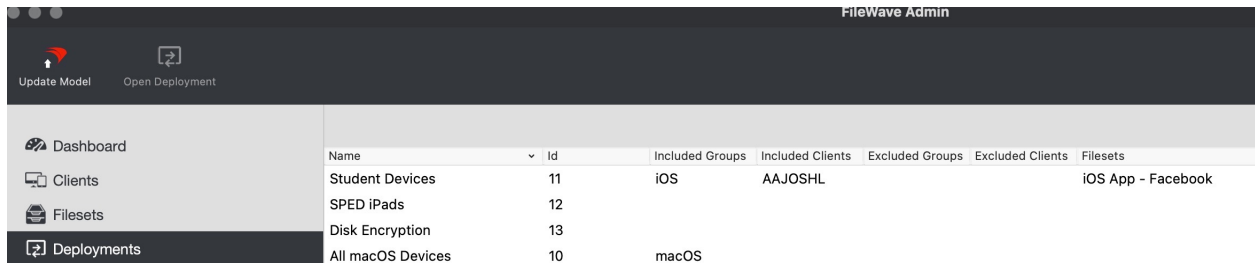
▼ FileWave 14.10.x (March 2023) Release Notes

14.10.2 is a security and bug fix release:

- Apache upgraded to 2.4.56
- Fixed Issues related to Model Update
- Fixed issues related to Wallpaper Overlay

FileWave Suite

- Deployments in FileWave Central:
 - Deployments are now visible in Native Admin Console. Deployments are mostly read-only in this release: it is possible to delete deployments, but not to edit existing ones or create new deployments.



FileWave Admin							
Update Model		Open Deployment					
Dashboard	Name	Id	Included Groups	Included Clients	Excluded Groups	Excluded Clients	Filesets
Clients	Student Devices	11	iOS	AAJOSHL			iOS App - Facebook
Filesets	SPED iPads	12					
Deployments	Disk Encryption	13					
	All macOS Devices	10	macOS				

- Force reboot:
 - There is a new option for reboot for a Fileset to forcibly restart the client 2 minutes after the Fileset has been installed. This should be used only when required because open documents may not be saved.

Fileset Name: Software Update - 2023-02 Cumulative Update for Windows 11 Version 22H2 for ARM64-based Syste...

Revision: <default> (Initial Revision) ⬇ Manage Revisions

Properties Requirements Dependencies Delete Files Kiosk

☒ Requires Reboot Message... Color:

☐ Force reboot

Device will force reboot 2 minutes after either activation or reboot deadline (if specified) when this fileset is deployed.
Warning: Forced reboots can result in a loss of unsaved data on the device, and should be used sparingly.

☐ Authenticated restart

Applies to devices with Full Disk Encryption and an escrowed Personal Recovery Key.

- Help Menus:
 - In Anywhere and Central, the Help menus now include links to the KB, Foundry, Discord, and Alliance Forums.
- Quality/Stability:
 - A great deal of extra effort was placed this go-round on correcting some long standing bugs and defects that we hadn't been able to get to prior.

Apple


- Customized Wallpaper:
 - It is now possible to add a text overlay on top of iOS / iPadOS wallpaper; the text can be parameterized with any inventory variable. ([Customizing iOS Device Wallpaper with Dynamic Text](#))

Profile Editor

Search


☒ show only configured

macOS, iOS and tvOS

 **General** 1

Mandatory

iOS and macOS 10.10+

 **Command Policy**


1 payload(s) configured.

Wallpaper (iOS devices only)

Set wallpaper (supervised devices only). Wallpaper will be reset once a day.

Lock and Home Screen ⬇

Preview



Browse...

Text overlay

%SerialNumber%

Text overlay size

Big ⬇

Text overlay color Text overlay position

☐ ☐ ☐

☐ ☐ ☐

☐ ☒ ☐

Bluetooth (iOS 11.3+ and macOS 10.13.4+)

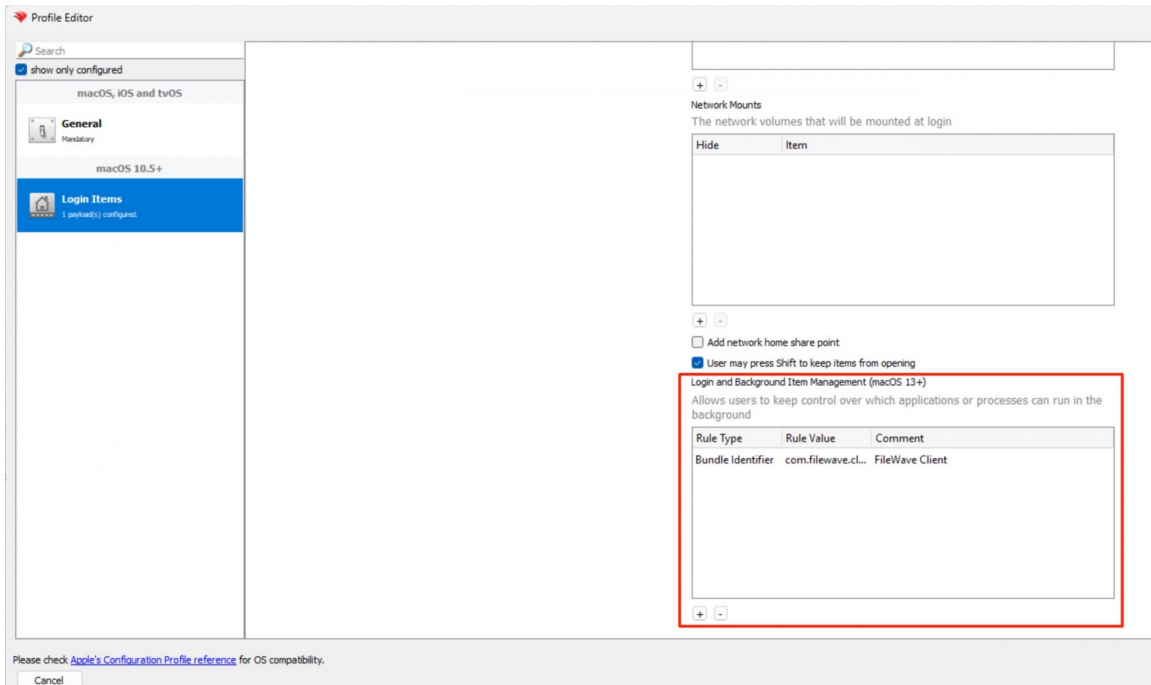
This setting takes effect even when the "allow Bluetooth Modification" restriction is set.

Don't change Bluetooth ⬇

Please check [Apple's Configuration Profile reference](#) for OS compatibility.

Cancel 1 validation error Settings Load Profile Save

- Force reboot as mentioned in the FileWave Management Suite section.
- Login and Background Items settings has been added to Login Items Profile.



Windows

- Force reboot as mentioned in the FileWave Management Suite section.

Network Imaging / IVS

- FileWave Networking Imaging 14.10.x brings compatibility with FileWave 14.10.x.
- PXE Kernel: 5.19.9
- Grub: 2.06

Deprecated Features

The following features are deprecated in FileWave 14.10.2 and will be removed in a future version:

- Device Discovery (Network Scanning) function of FileWave Boosters
 - Reason: This tool was never effective in production environments, has hardly ever been used, and is easily replaced by any off-the-shelf network scanning tool
- ZMQ based features for clients running 14.7 or older
 - Reason: ZMQ has been replaced by NATS, so older client devices must be updated to use the new notification framework
- Android device management prior to Android EMM (using APKs, etc)
 - Reason: Android EMM is the replacement for the much older method of managing Android devices

FileWave 14.9.x (November 2022)

▼ FileWave 14.9.x (November 2022) Release Notes

New Features

14.9.3 is a security and bug fix release:

- OpenSSL upgraded to 3.0.8
- Apache upgraded to 2.4.56
- NATS Server upgraded to 2.9.14
- Fixed memory leaks impacting Windows Client

FileWave Management Suite

- IDP Group Name/Display improvements in Native and Webadmin consoles
 - This may seem a rather small change, but if you were the one building reports or smart groups before using IDP groups, you'll be very happy to no longer see group IDs:



- Associations → Deployments Conversion Tool (Webadmin)

- Most likely, you'll want to wait to actually convert Associations until after we have included deployments in the native admin tool, but this tool is so well done, we wanted you to be able to take a test run now: [Read more](#)



- Upgrade of Grafana and Prometheus (which supports Grafana) to the most recent versions
 - This change provides both security and behavioral/UI changes for the web dashboard (which is a great tool if you haven't tried it):



- German has now been added to our product translations
- Quality/Stability:
 - A great deal of extra effort was placed this go-round on correcting some long standing bugs and defects that we hadn't been able to get to prior. More than 150 issues were corrected in version 14.9!

Apple

macOS 13 Ventura / iOS 16.1



- Added support for macOS 13 Ventura
 - Now identified in Inventory reports/groups
 - And identified in Fileset requirements
 - Added to "Incompatible with SIP" fileset lookup
- Also, of course, added support for iOS/iPadOS 16.1

Profile Changes

Cellular Profile

- There is a new option to configure IPv4/IPv6 translation (464XLAT):



Restriction Profile

- New option to disable Universal Control (macOS 13)
- New option to prohibit the user from installing configuration profiles and certificates interactively (Now on macOS 13+)
- New options to prohibit the user from installing or removing Rapid Security Response (iOS 16, iPadOS 16 and macOS 13+)



Setup Assistant

- New option to hide Terms Of Address (French, Italian, Portuguese)



Finder

New options:

- Disables the Power Off menu item when the user is logged in
- Disables the Log Out menu item when the user is logged in
- Disables the Automatic Login option when using FileVault



Security and Privacy

- New option to allow FireWall settings change



Single Sign-On Extensions

- Platform SSO Authentication method can be configured if the extension supports it (Password or Secure Enclave)
- Registration Token for Platform SSO registration
- List of applications which can't use the extension for SSO
- Screen Lock behavior





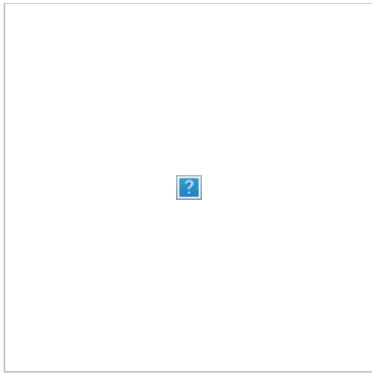
Transparency, Consent and Control

- New service to grant an application permission to update or delete another application



DEP Profile Changes

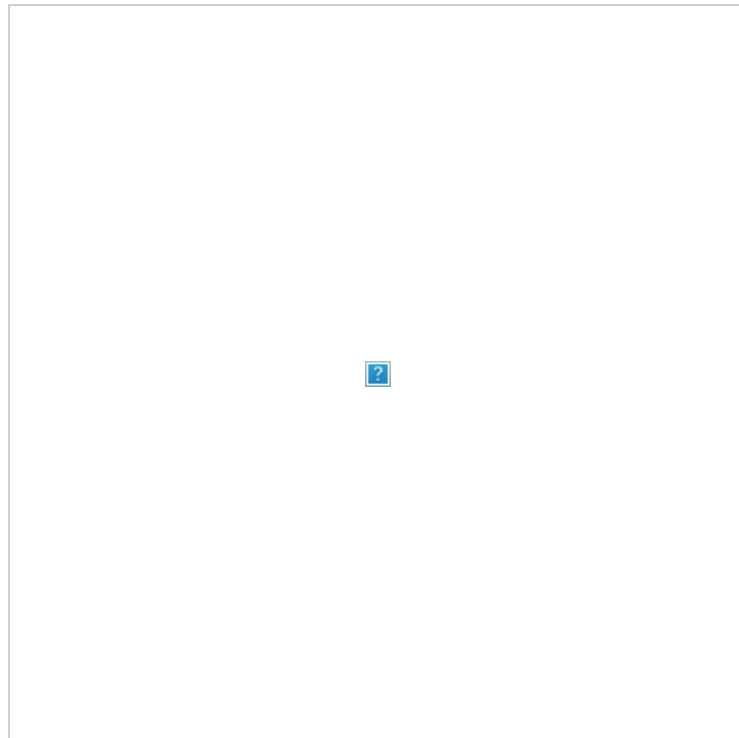
- New option to skip Terms Of Address (French, Italian, Portuguese) during setup



Shared iPad Settings

- New Setting to define a list of (up to) 3 domains which will be proposed to the end user to simplify Shared iPad login.
- New Setting to define a grace period, in days, for Shared iPad online authentication. The Shared iPad only verifies the user's passcode locally during login for users that already exist on the device. However, the system requires an online authentication (against Apple's identity server) after the number of days specified by this setting.

Both settings are made available via Command Policy Profile and current settings are reported in Inventory.





Accessibility Settings

It is now possible to configure various accessibility settings, making it easier for IT department to prepare devices for users requiring some accessibility configurations like increased text size or increased contrast:



Inventory Changes

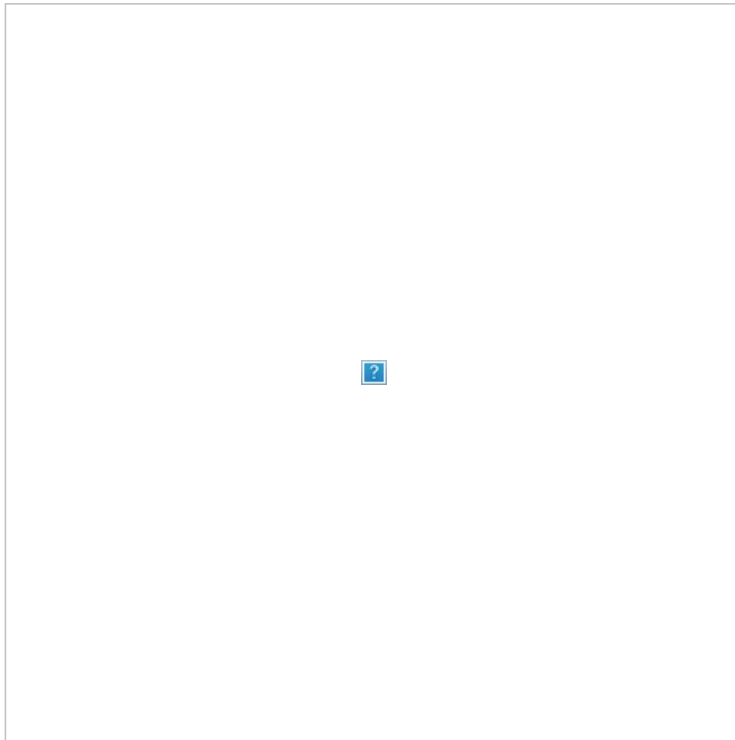
The following data is now reported and stored in inventory:

- Accessibility Settings (iOS)
- Managed Apple ID default domains (Shared iPads)
- Online Authentication grace period (Shared iPads)
- Installed Applications report if the application is an AppClip, if the application is being installed (iOS)
- Service subscription now replaces Carrier information and can report multiple subscriptions (iOS)

Per App Web Content Filter and DNS Proxy

Apple lets IT configure global Web Content Filter and DNS proxy via profiles ; starting with iOS 16, it is now possible, likewise with VPN, to configure those settings for a specific application, giving IT more granular control.

If you create a Web Content Filter or a DNS Proxy profile, you can now configure iOS applications to use them in Properties:



Microsoft

- Completion of Windows MDM Device Wipe Command
- MDM Sync is now forced after delivery of MDM based commands (like wipe above)
- Windows Defender CSP Added (Policy)
 - The Windows Defender Policy allows you to define alternate sources and their priorities for Windows Defender signature downloads:



- User-Based CSPs are now applied to all AzureAD users, not simply the current user

Google

- Implementation of Global Proxy Policy for Android devices
 - This addition allows devices in the environment to have a global proxy defined:



- Migrated Chromebook Inventory Extension to manifest v3 (a maintenance update only...the plug-in will be updated through the Play Store automatically once approved/posted)

Imaging (IVS)

- FileWave Networking Imaging 14.9.x brings compatibility with FileWave 14.9.x.
- PXE Kernel: 5.19.9
- Grub: 2.06

Deprecated Features

The following features are deprecated in FileWave 14.9.3 and will be removed in a future version:

- Device Discovery (Network Scanning) function of FileWave Boosters
 - Reason: This tool was never effective in production environments, has hardly ever been used, and is easily replaced by any off-the-shelf network scanning tool
- ZMQ based features for clients running 14.7 or older
 - Reason: ZMQ has been replaced by NATS, so older client devices must be updated to use the new notification framework
- Android device management prior to Android EMM (using APKs, etc)
 - Reason: Android EMM is the replacement for the much older method of managing Android devices

Deprecated features are still functional in a current release, but will no longer be updated and in future will be removed.

FileWave 14.8.x (July 2022)

▼ FileWave 14.8.x (July 2022) Release Notes

FileWave Management Suite

User preferences in main views will be stored on the user account (Web Console):

- Pinned columns
- Width of the columns
- Visibility of the columns
- Order of the columns

User preferences in main views will be stored in the active session (Web Console):

- Filters
- Quick filters
- Search
- Applied sorting on a column

Profiles section error handling improvements (Web Console):

- Error handling in the profiles is more user friendly and the mandatory fields are better highlighted

Apple

Apple Silicon Support

Client and Booster components are now fully Universal - run natively on mac with Intel or Apple Silicon chips.

The server component is mostly Universal (Dashboard using Grafana still requires Rosetta)

Apple Spring 2022 Release support

- Profile changes:
 - New macOS restriction to disable AirPlay Receiver
 - New macOS firewall options (finer settings to allow application connectivity and logging options)
 - New tvOS restriction to disable automatic screen saver

VPP changes

- When adding a VPP token, FileWave will now check if already imported tokens are not from the same location to prevent adding the same location twice.
- When renewing a VPP token, FileWave will now check that the new token has been generated from the same location as the one it replaces.

Windows

Wipe

- Windows devices can be wiped from the Web Console

Software update view improvements

- Apple and Microsoft patches have separate sections now
- The list can be sorted by the assigned subtype (e.g. successful, remaining, warning, error)
- Visual improvements in the software update section

Software updates MDM profile

- Different software updates settings can be applied to the Windows devices via MDM
 - Deadlines, grace period, automatic update behavior, restart check, option to pause updates, option to check for updates

Automatic MDM certificate renewal

- Windows devices will get the MDM certificate automatically renewed before they expire

Imaging (IVS)

- FileWave Networking Imaging 14.8.x brings compatibility with FileWave 14.8.x.
- PXE Kernel: 5.17.1
- Grub: 2.06

Deprecated Features

The following features are deprecated in FileWave 14.8.0 and will be removed in a future version:

- Apple profile management is deprecated in the Native Admin Console.
- DEP profile addition and creation are deprecated in the Native Admin Console.

Decommissioned Features

The following features have been removed from FileWave 14.8.0:

- Clever is not available as an SIS source anymore.
- Engage is not supported anymore.
- Observe Client functionality has been replaced by the TeamViewer integration

FileWave 14.7.x (February 2022)

▼ FileWave 14.7.x (February 2022) Release Notes

Software Update improvements

- Client Info reports (extended) Software Update information in a new tab (native admin)
- Windows Software update improvements:
 - Devices now report "online" updates
 - More information (category, support URL, KB article number...) is reported
 - Devices now report on already installed updates, even if they haven't been installed via FileWave
 - Provides independent confirmation outside of the fileset/payload mechanism
 - Read more about Windows Software Update improvements [here](#)
- FileWave is now reading information from Apple Software Lookup Service (GDMF).
 - Read more [here](#)

Web Console

- Improvements for Deployments: added the possibility to "add to deployment" from the device/device details views
 - Allows for adding a group to an already existing deployment for instance
- FileWave policies can now be managed in the Web Console
- Packages (MSI, PKG) files can be dragged from explorer/finder and dropped onto the Payload list

Internals

- Improved internal code related to object identifiers to avoid possible identifiers exhaustion for large installations

Remote Control

- Unattended access is now possible for macOS and Windows devices with the use of the TeamViewer integration
 - You can read more about your TeamViewer options [here](#)

FileWave 14.6.x (October 2021)

▼ FileWave 14.6.x (October 2021) Release Notes

Apple Fall Release

Support for macOS 12 Monterey, iOS, iPadOS and tvOS 15:

- Support for macOS 12
- Additional Inventory data reported by MDM DeviceInformation Command (IsAppleSilicon, DeviceId for Software Update)
- App portal (for Kiosk) native application has been updated for iOS 15:
 - Minimum iOS supported version is now iOS 12.5
 - Retrieving geo-location is now processed in the background. On iOS 13 and later, the native portal uses the native background task to retrieve more frequently the position even if the application is not in foreground.
 - Preparation for Remote Session using Team Viewer.

DEP changes:

- new Skip Key "Unlock your Mac with Apple Watch"

Profile changes:

- Skip Unlock with Apple Watch and Skip Accessibility in macOS Login Window profile (Setup Assistant)
- System Extensions have additional "Removable" option
- New Restrictions:
 - On device only translation
 - Requires Managed Pasteboard
 - Allow iCloud Private Relay
 - Touch ID timeout before asking password
- DNS Proxy profile is available on macOS 10.15+
- TVRemote profile has new "Device Name" Field
- A new command policy option has been added to configure Software Update Policy (Update for current Major version, previous Major version, both)

VPP new API support (Technical preview)

Apple introduced a new version of the VPP API ; FileWave 14.6.1 allows to use the new API as a technical preview ([read more](#)):

- In 14.6.1, this will be an in-place replacement, no feature change
- Future versions will benefit from the new API's additional features (better bulk license management, notifications based communication with Apple service)

MDM Software Update Improvements ([read more](#)):

- MDM Command OSUpdateStatus is now used to report download progress
- Both macOS and iOS updates are now deployed in two steps (one command to have the device downloading the update, one command to have the device installing the update) as this process is more reliable than requesting the device to handle the whole process automatically

Web Admin Updates

There are three main changes to the Web Admin Console in this release:

- The web admin now has a great looking [script editor](#)
- And in-progress [deployment definitions](#) are now saved when you navigate away from them
- Lastly, [VPP application updates](#) can now be controlled much more easily

Native FileWave Admin Changes

Verify for Desktop devices can now be triggered from the native admin without direct network connection (within the Client Info window).

TeamViewer Integration (Technical Preview)

Version 14.6 introduces TeamViewer as the eventual replacement for Observe Client. You can read much more about that integration [here](#).

Imaging Mac Address

A new inventory field has been added to assist with Windows Imaging for devices with pass-through MAC addresses. You can read about this change further [here](#).

IDP Changes

Version 14.6 introduces the much-demanded Google as an IDP source. Specific instructions for setting up that integration can be found [here](#). Additionally, you can now also setup easy smart groups using IDP group membership. That topic is covered in this [kb article](#).

FileWave 14.5.x (July 2021)

▼ FileWave 14.5.x (July 2021) Release Notes

New Features

FileWave 14.5.4 primarily updates Apache to [Version 2.4.51](#) to fix a critical CVE and addresses several small FileWave-related bugs.

See below for new features introduced with FileWave 14.5:

FileWave Management Suite:

- Device enrollment conflict improvements ([read more](#)):
 - It is now possible to solve multiple conflicts at once
 - There is a new setting to automatically solve conflicts with a predefined option (ignore new device, remove previous client before enrolling new, replace old client with new client).
 - Placeholder replacement is more robust
- Windows client fingerprint is persistent during imaging process ; this avoids conflict in case the hardware setup (on which fingerprint is based) has changed.
- Fileset (Payload) Status in Inventory ([read more](#))

Apple:

- Profile changes:
 - New restrictions:
 - macOS now allows you to define different DeferUpdate delays for major, minor and non-OS software updates
- Device Information reports additional information:
 - LocalHostName, Hostname (macOS)
- New options for share iPads:
 - Shared iPads can now be configured as "Guest mode" only
 - It is possible to define logout timeouts for normal or guest mode users

Web Admin:

- Software Update enhancements ([read more](#)):
 - Deploy to groups
 - Install in specific time windows
- NAT Support for Client Monitor & Verify ([read more](#))
- Perform Actions on Multiple Devices ([read more](#))
- MSI & PKG Payload Creation ([read more](#))

Windows MDM ([read more](#)):

- Support for manual and AutoPilot MDM enrollment
- Guidance on importing devices into AutoPilot
- Creation/deployment of Windows MDM Policies (Profiles)

FileWave 14.4.x (June 2021)

▼ FileWave 14.4.x (June 2021) Release Notes

New Features

FileWave Management Suite:

- Booster upgrade mechanism (see related KB Articles: [Booster Auto-Upgrade](#)):
 - Starting from FileWave 14.4.0, it will be possible to upgrade boosters directly from admin console. Boosters will report if an update is available and upgrading it will be a one-click action.
 - When several boosters are defined to be upgraded, they will be upgraded one after the other to avoid situation where all boosters are down at the same time.
- As Windows device names have limitations, a device used in imaging can't be renamed if the new name does not respect those limitations, and devices not respecting those limitations need to be renamed before being used in imaging

Apple:

- Per-Account-VPN support: it is now possible to associate a Per-App-VPN payload (from same or different fileset) to an "account" payload (Mail, Exchange, CalDav,...), which enables corresponding VPN when device contacts corresponding account.
- Profile changes:
 - New "Certificate Revocation" Profile
 - New restrictions:
 - AllowNFC (iOS)
 - AllowAutoUnlock (iOS)
 - allowGameCenterFriendsSharingModification (iOS, macOS)
 - allowUnpairedExternalBootToRecovery (iOS)
 - allowWallpaperModification (macOS)
 - forceOnDeviceOnlyDictation (iOS)
 - New setting "EnforceRoutes" and "ApplicationExceptions" for VPN (and Per-App-VPN) profile
 - Web Content Filter is now available on macOS

- Single App Mode payload is not restricted to tvOS system applications anymore
- Device Information reports additional information:
 - Supports iOS App Installs (macOS)
 - Security Info fields (macOS)
- Restart MDM macOS has a new setting to notify user instead of rebooting immediately
- DEP: "Auto Advance", and regional options are now available for macOS
- macOS MDM state is now reported into inventory, allowing to detect properly MDM enrollment issues
- Associated domain management:
 - Associated Domain profile has new "Enable Direct Downloads" option
 - App Store and Enterprise applications have new options for Associated Domains

FileWave 14.2.x (April 2021)

▼ FileWave 14.2.x (April 2021) Release Notes

New Features

Apple:

- App store applications can now be managed by MDM enrolled mac running Big Sur:
 - VPP Applications are really managed and not simply installed
 - VPP Applications can be removed from managed device when fileset is not associated anymore
 - VPP Applications can be automatically removed by macOS 11 when MDM enrollment is removed
 - Client info reports Managed Application List and MDM installed application list for MDM enrolled macOS 11
- FileWave server and booster can be installed on Apple Silicon mac devices
- New OS numbering for macOS (Big Sur is macOS 11.x)

macOS 11 "Big Sur" changes:

One of the changes announced by Apple during WWDC 2020 is that macOS 11 will drop support for command line installation of profiles and Software Update.

FileWave 14.0.2 contains important change to [profile installation](#) for non-MDM enrolled macOS (or profiles installed before MDM enrollment).

Software Update Management

Command line management of software update is deprecated and limited on macOS Big Sur ; therefore, Software Update on macOS Big Sur is now managed via MDM. Unfortunately, the MDM protocol is more restrictive than what could be doable with the command line ; macOS 11 SoftwareUpdate management will behave roughly the same as what is available on iOS/tvOS/iPadOS:

- Updates are displayed in Software Update assistant when devices report it is available
- Software Update filesets are simple placeholders containing metadata about the update ; updates are not downloaded and prepared server side anymore and will be downloaded by each device from Apple CDNs. Using a Caching Server is highly recommended.
- MDM protocol currently provides less control over Update installation. FileWave will be able to trigger a Download and Install request on the device, but these actions will be entirely processed by macOS, which can decide to postpone the installation without more information. System logs (install.log mainly) can give more details.

Apple Silicon Support

- FileWave components are supported as x86 application and run through Rosetta2 translator.
- Device running on Apple Silicon reports properly the platform, filesets can have Intel or Apple Silicon only requirements
- PowerPC and mac OS X 10.7 and below support has been removed from FileWave admin. Legacy clients running older versions of FileWave should still work properly, but editing or creating PowerPC filesets is not working anymore.

Windows:

- Windows devices are now excluded from "Device with same serial number" conflict detection

Google:

- New admin permissions for:
 - Chromebook de-provisioning
 - EMM configuration access in preferences

Identity Provider Integration: (Read related KB Articles here: [FileWave IDP Integration](#))

- New support for IDP providers (AzureAD/Okta) for:
 - Apple Device Enrollment
 - FileWave Admin Authentication (which in turn can then support multi-factor authentication)

Important third party upgrade:

- Qt 5.15.2
- Various Python libraries
- OpenSSL 1.1.1k

FileWave 14.1.x (Dec 2020)

▼ FileWave 14.1.x (Dec 2020) Release Notes

New Features

Support following iOS 14, iPadOS 14, tvOS 14 and macOS 11 features:

- Support for iOS 14, iPadOS 14 and macOS 11 "Big Sur"
- Support for Apple Silicon mac:
 - New fileset requirements
 - Architecture is reported in inventory
 - Restart Device option has new options related to Kernel Extension management
- New / modified profiles:
 - New payload to configure DNS
 - Override Previous Password option
 - macOS restriction, allows apps to get File provider Info
 - Disable Association MAC randomization (added in 14.0.2)
 - Define preview type
 - Media Rating settings have been updated by Apple (Warning, some settings have been modified by Apple like UK "Cautious")
 - Allow App Clips
 - Force Delayed App Software Update
 - Allow Apple Personalized Advertizing
 - Added options to allow non-admin user to allow screen recording
 - Now supports 4096 key size
 - IKEv2 : MTU can be defined
 - Setting to disable On Demand Override option for end user
 - Certificate type can now be Ed25519
 - Enable fallback option
 - Defines if a full screen web clip can navigate to an external web site without showing Safari UI
 - Application bundle identifier opening the URL
 - DNS Settings:
 - Exchange:
 - File Provider:
 - Network
 - Notifications
 - Restrictions
 - Setup Assistant (which allows skipping panes like DEP, but post enrollment, for upgrades)
 - Security and Privacy
 - System Extensions
 - SCEP:
 - VPN:
 - Webclip:
- TimeZone can be defined via Command Policy Profile (reference [Setting Timezones on Devices](#))
- on iOS and iPadOS 14, Managed VPP Applications can now be marked as unremovable (reference [Unremovable VPP Applications \(FileWave 14.1+\)](#))
- New DEP skip setup panes:
 - Accessibility (macOS) ;
 - Update and restore completed (iOS)
 - Software Update are now managed using Apple MDM on macOS Big Sur
- New Device information report:
 - EstimatedResidentUser (Shared iPad)
 - TimeZone
 - EID

Support for Geo-Fencing:

- Geo-Fencing has been added for Android Devices (reference [Geofencing](#))

macOS 11 "Big Sur" changes:

One of the changes announced by Apple during WWDC 2020 is that macOS 11 will drop support for command line installation of profiles and Software Update.

FileWave 14.0.2 contains important change to [profile installation](#) for non-MDM enrolled macOS (or profiles installed before MDM enrollment).

Software Update Management (reference [Software Updates in the age of macOS MDM \(Big Sur +\)](#))

Command line management of software update is deprecated and limited on macOS Big Sur ; therefore, Software Update on macOS Big Sur is now managed via MDM. Unfortunately, the MDM protocol is more restrictive than what could be doable with the command line ; macOS 11 SoftwareUpdate management will behave roughly the same as what is available on iOS/tvOS/iPadOS:

- Updates are displayed in Software Update assistant when devices report it is available
- Software Update filesets are simple placeholders containing metadata about the update ; updates are not downloaded and prepared server side anymore and will be downloaded by each device from Apple CDNs. Using a Caching Server is highly recommended.
- MDM protocol currently provides less control over Update installation. FileWave will be able to trigger a Download and Install request on the device, but these actions will be entirely processed by macOS, which can decide to postpone the installation without more information. System logs (install.log mainly) can give more details.

Apple Silicon Support

- FileWave client is supported as x86 application and runs through Rosetta2 translator. Rosetta2 is required and is currently not pre-installed on macOS. We recommend you to use our [Custom Package service](#) to deploy FileWave client ; the custom package will ensure Rosetta2 is properly installed.
- Device running on Apple Silicon reports properly the platform, filesets can have Intel or Apple Silicon only requirements
- PowerPC and mac OS X 10.7 and below support has been removed from FileWave admin. Legacy clients running older versions of FileWave should still work properly, but editing or creating PowerPC filesets is not working anymore.

Internals:

Important third party upgrade:

- Apache 2.4.46
- OpenSSL 1.1.1h
- Qt 5.15.1

FileWave 14.0.x (Sept 2020)

▼ FileWave 14.0.x (Sept 2020) Release Notes

New Features

New Web admin (Beta !)

Apple devices management:

- Enhanced support for Shared iPads (iPadOS 13.4)
- User Enrollment support for iOS / iPadOS devices:
 - New enrollment url to "User enroll" devices in a Bring Your Own Device scenario - see <https://www.apple.com/business/it/>
 - Automatically create and associate VPP users to User Enrolled devices to ease VPP apps and books deployment
 - Enrollment type is now shown in Client info
- 32b only applications are reported and not installed on incompatible iOS / iPadOS devices
- macOS: use of InstallEnterpriseApplication command to install FileWave agent on compatible devices
- Simplify VPP license management:

- New Licensing option "Device when possible, user if not"
- License reservation is not mandatory anymore - fileset can consume license from VPP token without reservation
- Support for universal apps
- Basic support for macOS "Big Sur"
 - Devices running macOS 11 properly report macOS version
 - Fixed an issue where updating profiles on non-MDM macOS 11 devices would remove the profile (see below)
- iOS 14 / macOS 11: "Disable MAC address randomization" option in Network profile

macOS 11 "Big Sur" changes:

One of the changes announced by Apple during WWDC 2020 is that macOS 11 will drop support for command line installation of profiles and Software Update.

FileWave 14.0.2 contains important change to [profile installation](#) for non-MDM enrolled macOS (or profiles installed before MDM enrollment).

Desktop devices management:

- New Fileset revision system:
 - Allows regrouping different versions of the same application inside the same fileset
 - More control over staging and application upgrade
- Association conflict resolution is now more consistent:
 - The "Winning" association now follows clear and consistent rules for the distance (no difference between normal clones and smart group clones for instance)
 - All association attributes (kiosk, licensing, schedule) are now from the winning association
- Smart groups can be used in Imaging Views to create Imaging Associations
- Verify can now be triggered via command line on device

Native console:

- Enhanced booster monitor to only accept valid settings
- "Move to..." option for fileset
- It is now possible to filter inventory query results
- It is now possible to create a smart group from an inventory query
- it is now possible to duplicate a smart group
- Added more information to Inventory-based Smart Groups to clarify membership

Installers:

- A backup of FileWave database and important settings will be taken before upgrade

Internals:

- Important third party upgrade:
 - OpenSSL 1.1.1g
 - Apache 2.4.43
- Postgres Log rotation now uses integrated postgres log rotation mechanism

FileWave 13.3.x (April 2020)

▼ FileWave 13.3.x (April 2020) Release Notes

New Features

Apple 2020 Spring Release Support:

Changes in Restriction Profile

- - Allow accessing web sites using TLS 1.0 and 1.1 (iOS, macOS)
 - Allow Guest Mode for shared iPad
 - Allow access to Apple ID and Family Sharing Preference Pane (macOS)

Changes in Login Window Profile

- - Screen Time option is available in Setup Assistant

Changes in Notification Profile

- - Notification settings are now available for macOS

Changes in VPN Profile

- - UI clarification
 - New Provider Bundle Identifier and Provider type setting

macOS Content Caching changes

- - Additional Content Caching setting in profile
 - Content Caching information is reported in inventory and in client info

Miscellaneous

- Support for shared iPad guest mode and shared iPad in Apple Business Manager
- Generated Self-signed certificates (MDM, Classroom) are not valid more than 398 days (see <https://support.apple.com/en-gb/HT211025>)

Google Related Updates:

EMM

- - Embed Wifi added to EMM Enrollment QR Code
 - BYOD for EMM
 - Location Tracking

Chromebooks

- - Added ability to edit Chromebook Data
 - Moving devices in Admin now moves the devices in G Suite Domain structure
 - Delete/Create OU in G Suite Domain structure through FileWave Admin
 - The FileWave extension now gathers these fields in a more reliable way
 - Local Device Name
 - Device Serial Number
 - Current Logged in user
 - Current IP
 - Current Asset ID
 - Certificates

Device Management:

Inventory Fields in Clients View (Native Admin)

- - Customize your Admin clients view with inventory fields - including custom fields

Dedicated Booster Communication

- - Boosters can now use a dedicated communication channel for Booster-Booster or Booster-Server communication to avoid congestion. To enable this feature, you may have to open additional TCP port on your server and your boosters. See [TCP Port KB](#).

Device Identification

- - Algorithm used to identify device re-enrollment has been improved to detect different re-enrollment scenarios to prevent duplicated clients.
 - Windows agent fingerprint is now stored on disk to avoid permission issue accessing registry, which could lead to unstable fingerprint, making client identification unreliable.

FileWave 13.2.x (Jan 2020)

▼ FileWave 13.2.x (Jan 2020) Release Notes

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

FileWave 13.1.x (May 2019)

▼ FileWave 13.1.x (May 2019) Release Notes

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; <https://kb.filewave.com/display/KB/Automated+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)

[Click here to expand...](#)

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
- OSCP 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

FileWave 13.0.x (Oct 2018)

▼ FileWave 13.0.x (Oct 2018) Release Notes

New Features (13.0.3)

Changes and New Features

MDM Profile removal

By default, FileWave is no longer answering with HTTP 401 when an unknown MDM Apple device checks in. This allows FileWave to recover data from a previous backup without un-enrolling devices, which could lead to data loss if applications were removed. For 13.0.3, a new option was added in "FileWave Admin / Preferences / Mobile / Apple" that reverts to previous behavior.

Desktop Client and Booster Affinity

FileWave 13.0.0 introduced a behavioral change related to how desktop clients are communicating with boosters. Before 13.0.0, clients would always contact the first booster, unless the booster is not reachable (off network or offline). This could lead to very long delay for fileset deployment if first configured booster would be overloaded. Starting with 13.0.0, clients will try to stay on a given upstream booster instead of changing frequently. This provides better load balancing as the connections are more stable. Clients will also fallback to the server if none of the boosters are reachable.

13.0.3 ensures that a client will retry boosters regularly if it fell back to the server.

Memory Footprint

During model update, a large amount of data is processed to determine which fileset will be deployed to which device. Fileset statuses are also processed and updated, so deleted filesets are removed, newly-associated filesets are marked as "Associated" and so on. Starting with FileWave 13.0.0, iOS fileset statuses are now properly reported, which can create a large number of entries in the database, increasing the memory consumption during model update.

The Linux operating system is more sensitive to memory fragmentation (very summarized: it is not able to recover memory with a frequent and high number of allocations, even if the process is not using this memory anymore), and the additional features brought to FileWave in the previous versions made the Linux version consume more memory over time, which could lead to Out-Of-Memory management.

FileWave 13.0.3 is now using a more efficient memory allocation system, more efficient, and a special attention has been paid to reducing memory usage during model update to avoid memory fragmentation as much as possible.

VPN on Demand Option

IKEv2 VPN allows very granular configuration, based on VPN provider rules. For 13.0.3, VPN profile allows entering raw XML provided by VPN vendors.

New Features (13.0.2)

Changes and New Features

- Upgrade OpenSSL to 1.0.2q
- Several improvements related to performance during model update and "Database deadlocks":
 - Internal changes to decrease model update duration
 - Made sure iOS devices could not interfere with Model Update and cause database issues
- iOS App portal speed improvements
- Improved updating DEP associations to workaround potential issues on DEP Web service

New Features (13.0.1)

Changes and New Features

- Added DEP_FORCE_FULLSYNC settings to force DEP full sync to workaround possible issues with Apple DEP API

New Features (13.0.0)

Changes and New Features

- Discover the initial version of FileWave Admin Web Console
- Additional security internal changes:
 - fwxsrv and MDM/Inventory server share the same SSL certificate
 - admin console and clients are checking SSL certificate validity
 - helpers for self-signed certificates (usage of trusted CA issued certificate is recommended)
 - Please read this [Self-Signed Certificates](#) KB article
- This version adds support for iOS 12, tvOS 12, macOS 10.14 (see below)
- Service Now integration
- Dependency failures are better displayed in client information
- Updated Observe Client component on macOS.

Apple 2018 Fall release support

Device Enrollment Program:

- New skip items for Setup Assistant:
 - Screen Time
 - Software Update
 - iMessage and FaceTime
 - Appearance
- Change default settings according to Apple Guidelines (Non supervised devices will be deprecated).

MDM Commands:

- Lock device on macOS can now display additional message

- VPP app installation is now supported on tvOS 12

Profile changes:

- Exchange and Email profiles have additional settings for S/MIME options
- Notification profile has additional settings
- Restriction profiles (iOS, tvOS and macOS) have additional settings
- VPN profile (IKEv2) has additional settings (Profiles: VPN IKEv2 changes)
- Xsan profile has additional settings
- New profile: Time server
- Smart Card profile has additional settings
- Privacy profile has additional entries for Transparency and Consent Control
- Energy profile has addition setting

Push Notification changes:

- New Apple APN server is now used by FileWave, using HTTP/2 protocol. Please make sure your FileWave server can contact <https://api.push.apple.com> (port 443).

FileWave 12.9.x (May 2018)

▼ FileWave 12.9.x (May 2018) Release Notes

New Features (12.9.0)

Architecture and Internals

- Admin authentication is now handled by the HTTP component ; this allows unified admin authentication for all components:
 - FileWave server
 - MDM/Inventory server
 - Future web admin system
- Communications between FileWave Admin and FileWave Server are now encrypted
- FileWave internal database now supports encryption for sensitive data. The following fields are for now encrypted:
 - ActivationLock Bypass Code
 - FileVault 2 Personal Recovery Key
 - Google Chromebook OAuth data
 - LDAP server password
 - Email password
 - Shared keys and Application tokens
 - Classroom settings (including clever settings inventory server, mdm server, imaging server, engage server settings)
- Apache (error / access) and postgres logs are now rotated by default as well

Changes and New Features

- The new authentication system brings changes in Manage Administrator Dialog:
 - Password generation
 - Application tokens
- More granular admin permissions:
 - Access to preferences
 - Access to Dashboard
 - Access to Classroom
 - Access to Full Disk Encryption (see below)
 - Access to Wipe Devices
- Support for FileVault 2 - configuration and Personal Recovery Key escrow service
- Added an option to disable WOW64 redirection for Windows
- Fileset status is now correctly reported for iOS devices
- Inventory Row Level restrictions:
 - Inventory queries results depend on admin permissions on clients, Filesets, VPP tokens: see Inventory and permissions
 - This impact everything using inventory queries:
 - Scheduled reports
 - License Management Tab
 - REST API
 - Scheduled reports are now stored per admin
- As iOS 11.4 fixes the 'bundle id' issue, RemoveApplication command is now enabled again on anything except iOS 11.3.x ; a setting (REMOVE_APPLICATION_DISABLED) has been added to override this behavior
- USB Restricted mode restriction (iOS 11.4.1)

- There is no restriction related to the number of FileWave admins - and the same admin can connect from different places at the same time
- Added a preference option to deploy MDM pkg to macOS if it's not already installed (i.e. no upgrade)

New Features (12.9.1)

Internals

- Upgrade OpenSSL to 1.0.2p
- Installer performs Database Integrity checks before upgrade to detect potential inconsistencies

FileWave 12.8.x (April 2018)

▼ FileWave 12.8.x (April 2018) Release Notes

New Features

This version adds support for iOS 11.3, tvOS 11.3, and macOS 10.13.4.

Device Enrollment Program

- New skip items for Setup Assistant:
 - "Privacy" consent (iOS 11.3, tvOS 11.3, and macOS 10.13.4)
 - "All your files in iCloud" storage setting (macOS)
 - "Where is the Apple TV" screen (tvOS)
- Regional settings added for tvOS.

MDM Commands

- New Bluetooth command (iOS 11.3 and macOS 10.13.4)
 - Note: the "Allow modifying Bluetooth setting" profile restriction has currently a higher priority on iOS 11.3.0 and can prevent the Bluetooth command from disabling or enabling the setting.
- New attributes for InstalledApplications commands - allows better and safer handling of application upgrades when there is a new version.
- New Remote Wipe option to disallow Proximity Setup post-wipe for iOS 11.3+.

Profile Changes

- New profile type: "TV Remote" (iOS 11.3+ and tvOS 11.3+)
- New profile type: "Content Caching" (macOS 10.13.4+)
- Support for Web Clip URL - Home Screen Layout (iOS)
- IKEv2 Cellular Service Exceptions - VPN (iOS and macOS)
- Access and Security options - AirPlay Security (tvOS)
- "Autonomous Single App Mode" - Restrictions (macOS 10.13.4+)
- "Check Certificate Trust" - Smart Card Settings (macOS)
- "Allow export from keychain" - SCEP (macOS)
- "Allow auto-renewal" - AD Certificate (macOS)
- "Disable Privacy consent window during login" - Login Window (macOS)
- "Disable iCloud Storage window during login" - Login Window (macOS)
- "Require teacher permission to leave Classroom unmanaged classes" - Restrictions (iOS)
- "Require Face ID authentication before AutoFill" - Restrictions (iOS)

MDM / Apple

- More DEP device naming options
- Updated SCEP configuration to comply with Apple 2017 recommendations regarding security
- Add new restrictions for iOS 11
- Support for 1:1 Managed Apple IDs

OS Update Changes

- For iOS 11.3+ clients it is now possible for FileWave to associate specific iOS OS versions and not just the "latest available" update.
- New Restrictions profile "Defer software updates" option can be used to delay the visibility of iOS and macOS client updates up to 90 days (iOS 11.3+ and macOS 10.13.4+).

FileWave 12.7.x (Feb 2018)

▼ FileWave 12.7.x (Feb 2018) Release Notes

New Features

Device Management

- Retry mechanism for Requirement Scripts
- Admin Command Line Interface:
 - New option to create device based license association
 - New option to specify executable during import
- End-user White-Boxing
- FileWave Policy Fileset: Blocker Script

Connectivity

- LDAPS Support
- Improved LDAP extraction speed
- New “Synchronize Now” action for LDAP extraction

Inventory

- Inventory Custom Fields
- Relative time query criteria

MDM / Apple

- More DEP device naming options
- Updated SCEP configuration to comply with Apple 2017 recommendations regarding security
- Add new restrictions for iOS 11
- Support for 1:1 Managed Apple IDs

Misc.

- Windows installers and binaries are now signed

🔄Revision #20

★Created 25 July 2023 12:31:19 by Josh Levitsky

✍Updated 15 July 2024 14:54:11 by Josh Levitsky