

FileWave Version 16.3.3

(Unsupported)

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

The FileWave endpoint management suite enables you to manage your devices wherever they are, wherever you are, whatever they are—all in one platform. FileWave 16.3 is a stability- and modernization-focused release designed to reduce operational risk and prepare the platform for safer, more automated lifecycle management in upcoming versions. This release lays critical groundwork for future self-updating workflows across Central and Clients, while immediately delivering automated, sequenced Booster upgrades with proactive reminders and reporting. FileWave 16.3 also improves upgrade reliability and administrative visibility across Central and Anywhere, and strengthens security with built-in brute-force login protection that is enabled by default, helping protect administrative access without requiring additional configuration. Together, these improvements establish a strong foundation for the more automated upgrade experience planned for FileWave 16.4 and beyond.

On Apple platforms, FileWave 16.3 continues to advance alignment with Apple’s evolving management model and 2026 OS changes. Declarative Device Management (DDM) support is expanded with improved handling of mixed DDM/MDM environments, a technical preview of DDM-based FileWave Agent installation on supported macOS versions, and new lifecycle controls for DDM-installed apps, including update behavior and version pinning. Profile management is updated to reflect the latest Apple payload schemas, ADE gains new skip keys and backup-handling options, VPP application delivery becomes faster and more reliable through improved notifications, and Apple’s transition to “Background Security Improvements” is fully supported. Beneath the surface, FileWave 16.3 reinforces long-term stability through database and component upgrades, stronger integrity checks during upgrades, improved client local data handling, and continued internal modernization. FileWave 16.3 also establishes Debian 13 as the base for FileWave-provided Server, Booster, and IVS appliances, aligning the platform with current OS and security standards.

FileWave Official Version Support

FileWave supports the two latest major versions at any time. For example, if the current version is 16.3.3, we support versions 16.3.x and 16.2.x. Major releases occur roughly every quarter.

What does “officially support” mean?

We will investigate and patch significant issues in these versions. We do not produce patches for versions older than N-1, focusing instead on current versions and future improvements. If an issue is found in an older version, remediation will be in the form of an upgrade or a patch to a more recent version.

You can still contact our support teams about earlier versions. They will assist you to the best of their ability but won’t escalate tickets to our development teams. Upgrading is recommended to access the latest features and bug fixes.

Compatibility

A Note on Compatibility

A note on the Compatibility charts: There are several states of compatibility for FileWave clients:

- "Fully Tested by QA" indicates that we have run QA regression tests against these operating system versions, and they are fully supported.
- "Expected to Work" Not being on the fully tested by QA list (such as macOS 13 or 14) does not mean that platform is not supported...it just means we did not actively test against it, but we do expect it to function. Support of any issues experienced specifically on these platforms would be considered on a case-by-case basis (but these cases are exceedingly rare.)
- "Legacy" versions mean that we don't test, but we do provide a retro-version of a client so that the device can still report in but as FW Server changes there may be challenges to these working. There is NO support for these platforms beyond the availability of the older client, and in almost all cases these are for OSes that are no longer supported by the OS vendor in question.
- Lastly, items do fall out of support, such as Windows XP and the older Android APK client as examples, but we always include these items in our release notes.

An additional note on third-party software inclusion, such as TeamViewer:

- Partnerships we have with third party providers have their own set of system requirements for those released applications. We test against their most recent versions, and support of those applications is limited to third-party vendor specifications.

FileWave Server Platform Support



Fully Tested by QA

- macOS 15 and 26 (Intel and Apple Silicon)
- Debian 13.2 x86_64 (Note that any Debian 13.x is expected to work, and applying security updates may move you to a higher version.)

Expected to work

- macOS 13 and 14 (Intel and Apple Silicon)
- Debian 12.x (x86_64)

Virtual Appliances

- Hyper-V - The images are available as Generation 2
- VMware ESX - The images require vmx-19 support which means VMware vCenter 7.0 Update 2 is the minimum version. (<https://knowledge.broadcom.com/external/article?legacyId=2007240>)

- VMware Fusion
- VMware Player and Workstation
- VirtualBox

Important FileWave Server upgrade requirement

FileWave Server upgrades that include PostgreSQL database changes must follow a path where each step supports at least one PostgreSQL version from the previous step. For more detail and examples, see [FileWave Server upgrade paths and PostgreSQL migrations](#).

The PostgreSQL overlap points are:

- FileWave 13.3.1 through 14.7.2 include PostgreSQL 12.
- FileWave 16.0.x through 16.2.x include PostgreSQL 12 and PostgreSQL 17.
- ! • FileWave 16.3.x and 16.4.x include PostgreSQL 17 and PostgreSQL 18.

Recommended upgrade path from older versions:

13.3.1–14.7.2 → 16.0.x–16.2.x → 16.3.x or 16.4.x

If your server is already running FileWave 16.0.x, 16.1.x, or 16.2.x, you can upgrade directly to FileWave 16.3.x or 16.4.x because those releases overlap on PostgreSQL 17; if your server is running a version earlier than 16.0.0, upgrade first to a release in the 16.0.x–16.2.x range, then continue to FileWave 16.3.x or later.

i The minimum memory requirement for FileWave Server is **8GB**.

FileWave Clients Platform Support



Fully Tested by QA

- macOS 15 and 26 (Intel and Apple Silicon)
- Windows 11 (Pro/Enterprise, version 24H2 and newer, x64)
- Windows Server 2022 (x64)

Expected to work

- macOS 13 and 14 (Intel and Apple Silicon)
- Windows 10 (Pro/Enterprise, version 21H1 and newer, x64)
- Windows 10 (Education, version 21H1 and newer, x64)
- Windows 11 (Education, version 23H2 and newer, x64)
- Windows 10 Enterprise LTSC (version 2021 and newer, x64)
- Windows 11 Enterprise LTSC (version 23H2, x64)
- Windows Server 2025 (x64)

i Note about LTSB/LTSC: [Microsoft Long Term Service Channel](#)

Legacy

- macOS 10.11 → End of Life due to OpenSSL age
- macOS 10.12 → [Legacy Version 14.10.2](#)
- macOS 10.13 → [Legacy Version 14.5.4](#)
- macOS 10.14 → [Legacy Version 14.8.0](#)
- macOS 10.15 → [Legacy Version 15.0.1](#)
- macOS 11 → [Legacy Version 15.5.2](#)
- macOS 12 → [Legacy Version 16.2.5](#)

FileWave Mobile Clients Platform Support



Fully Tested by QA

- iOS 18, 26
- iPadOS 18, 26
- tvOS 18, 26
- Android 8 and above (EMM Client)
- Chromebook

Expected to work



Currently Apple is investigating an issue enrolling iOS 16 or older via ADE/DEP. Enrollment via profile works.

- iOS 14, 15, 16, 17
- iPadOS 14, 15, 16, 17
- tvOS 14, 15, 16, 17

Legacy

- iOS 13 → [Legacy Version 15.0.1](#)
- iOS 10, 11, 12 → [Legacy Version 13.1.5](#)

FileWave Central (Native) Platform Support



Fully Tested by QA

- macOS 15 and 26 (Intel and Apple Silicon)
- Windows 11 (Pro/Enterprise, version 21H2 and newer, x64)

Expected to work

- macOS 13 and 14 (Intel and Apple Silicon)
- Windows 10 (Pro/Enterprise, version 21H1 and newer, x64)
- Windows 10 (Education, version 21H1 and newer, x64)
- Windows 11 (Education, version 21H2 and newer, x64)

FileWave Booster Platform Support



Fully Tested by QA

- Debian 13.2 x86_64 (Note that any Debian 13.x is expected to work, and applying security updates may move you to a higher version.)
- macOS 15 and 26 (Intel and Apple Silicon)
- Windows 11 (Pro/Enterprise, version 24H2 and newer, x64)
- Windows Server 2022 (x64)

Expected to Work

- Debian 12.x (x86_64)
- macOS 13 and 14 (Intel and Apple Silicon)
- Windows 10 (Pro/Enterprise, version 21H1 and newer, x64)
- Windows 10 (Education, version 21H1 and newer, x64)
- Windows 11 (Education, version 23H2 and newer, x64)
- Windows Server 2025 (x64)

Virtual Appliances

- Hyper-V - The images are available as Generation 2
- VMware ESX - The images require vmx-19 support which means VMware vCenter 7.0 Update 2 is the minimum version. (<https://knowledge.broadcom.com/external/article?legacyId=2007240>)
- VMware Fusion
- VMware Player and Workstation
- VirtualBox

FileWave Imaging Virtual Server Platform Support



The FileWave Imaging Virtual Server (IVS) is a special appliance that provides imaging support for Windows 11 UEFI and non-UEFI devices. Windows 10 imaging is expected to work.

Fully Tested by QA

- Debian 13.2 x86_64 (Note that any Debian 13.x is expected to work, and applying security updates may move you to a higher version.) Note that unlike Server and Boosters we know you must run Debian 13 for the 16.3.0 IVS.

Virtual Appliances

- Hyper-V - The images are available as Generation 2
- VMware ESX - The images require vmx-19 support which means VMware vCenter 7.0 Update 2 is the minimum version. (<https://knowledge.broadcom.com/external/article?legacyId=2007240>)
- VMware Fusion
- VMware Player and Workstation
- VirtualBox

Features and Updates in this Release

FileWave Management Suite Changes

Debian 13 Support

FileWave 16.3 transitions its Linux base platform to Debian 13, replacing Debian 12 across all FileWave-provided appliances and establishing the new baseline for upcoming releases. The upgrade command lines in the download section will seamlessly handle the upgrade from Debian 12 to 13 when going to FileWave 16.3.0 so just upgrade as normal, but give it extra time. Much better logging is also in the upgrade scripts which log to /var/log/ and can help support to troubleshoot issues.



Platform Support Overview

- Stand-alone Server and Booster installs - FileWave 16.3 Server and Booster are supported on both Debian 12 and Debian 13 when installed on customer-managed systems.
- FileWave Appliances (OVA/VHD images) - All FileWave 16.3 Server, Booster, and IVS (Imaging Virtual Server) appliances provided as OVA or VHD images are now built exclusively on Debian 13, replacing the previous Debian 12 base.

Upgrade Requirements and Recommendations

- Appliance-based Server or Booster - Existing Server or Booster appliances running Debian 12 can continue operating without migrating to Debian 13; however, upgrading to Debian 13 is recommended to align with the new platform baseline and ensure long-term compatibility.
- IVS (Imaging Virtual Server) - FileWave IVS 16.3 requires Debian 13. Upgrading from Debian 12 to Debian 13 is mandatory when updating an IVS to version 16.3.

Upgrade made simpler

Automatic Central Upgrade on Server Connection

Starting with FileWave 16.3.0, FileWave Central can now automatically upgrade itself when connecting to a newer FileWave Server. Instead of rejecting the connection, Central will download the appropriate installer package from the server, stop the current instance, perform the upgrade, and restart automatically.

- If the connected server runs a compatible minor version (for example, Central 16.3.0 and Server 16.3.1), Central will only suggest the upgrade—allowing the administrator to postpone it and continue working.
- If the server runs an incompatible version (for example, Central 16.3.2 and Server 16.4.0), Central will require an upgrade before connecting.
- In all cases, the user may choose to cancel the upgrade and close Central, ensuring administrators with multiple environments can avoid unintended upgrades.

This feature simplifies maintenance and ensures version alignment between Central and Server while respecting compatibility boundaries. Note that this feature was added to 16.3.0 so you will not benefit from it until 16.3.1 or higher.

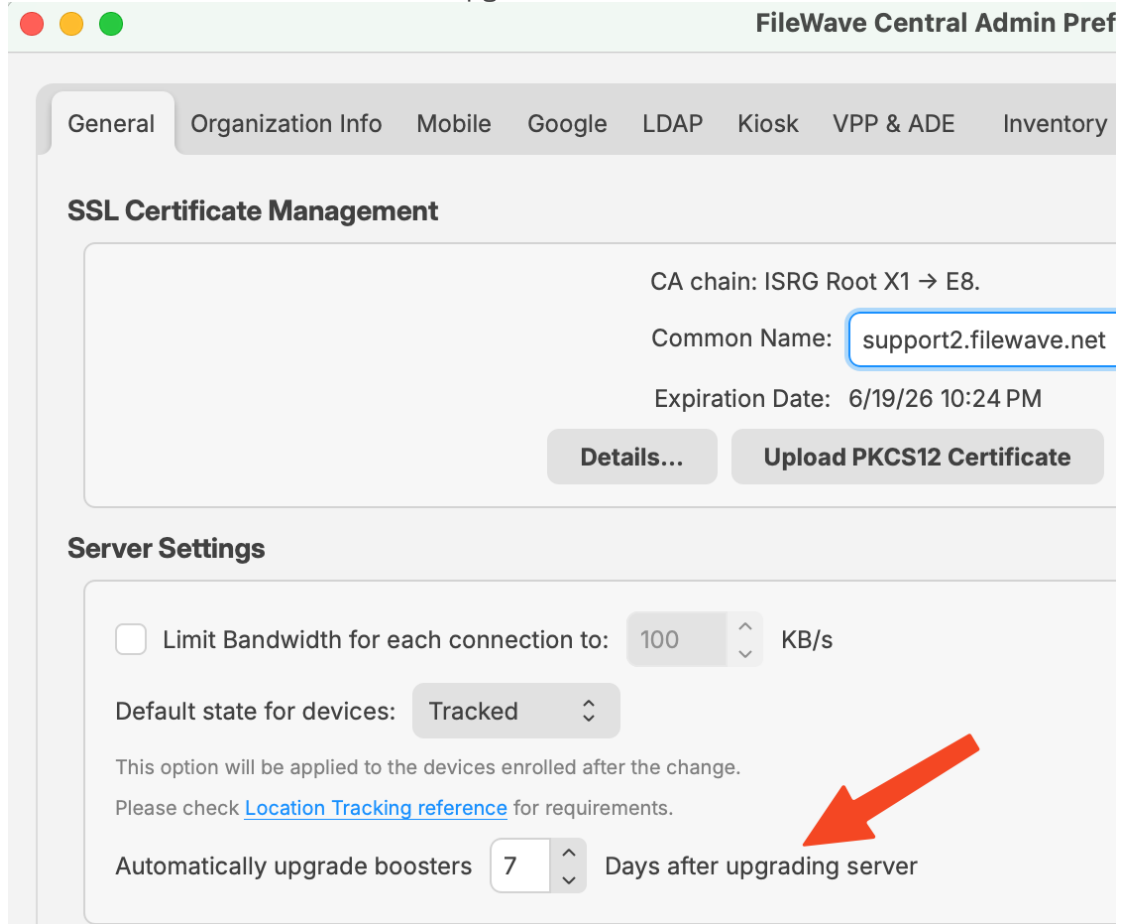
Outdated Booster Upgrade Reminder and Automatic Upgrade

Since FileWave 14.3, Boosters have supported a controlled and reliable upgrade process—FileWave upgrades them sequentially, ensures that at least one remains online, and halts the process if any upgrade fails.

With FileWave 16.3, this process is further enhanced with automated monitoring and reminder capabilities:

- Outdated Booster detection: FileWave now identifies any Booster running an older but compatible version. In most cases, this means the Booster should match the Server version, though exceptions exist when OS support limits apply.
- Central and Anywhere notifications: Both FileWave Central and FileWave Anywhere display reminders when outdated Boosters are detected.
- Automatic upgrades: By default, Boosters are automatically upgraded one week after the Server upgrade. The delay is configurable in FileWave Central -> Preferences, and

administrators can unschedule the upgrade if desired.



The screenshot shows the FileWave Central Admin Preferences window. The 'General' tab is selected. Under 'SSL Certificate Management', the CA chain is 'ISRG Root X1 → E8', the Common Name is 'support2.filewave.net', and the Expiration Date is '6/19/26 10:24 PM'. There are buttons for 'Details...' and 'Upload PKCS12 Certificate'. Under 'Server Settings', there is a checkbox for 'Limit Bandwidth for each connection to: 100 KB/s'. Below that, 'Default state for devices:' is set to 'Tracked'. A note says 'This option will be applied to the devices enrolled after the change. Please check [Location Tracking reference](#) for requirements.' At the bottom, 'Automatically upgrade boosters' is set to '7 Days after upgrading server'. A red arrow points to this setting.

- Sequenced rollout and reporting: Upgrades occur one Booster at a time, with notifications shown in Central at the start of the process and after each successful upgrade.

This enhancement helps ensure Booster infrastructure stays aligned with the Server version with minimal administrative effort, maintaining stability and version consistency across the environment.

Outdated server upgrade reminder

Keeping your FileWave server up to date is recommended. We are working hard to bring a lot of new features and improvements to make your IT admin life simpler, and if you stay behind you don't benefit from them. Equally important, each FileWave release comes with bug fixes, and we take the time to update third-party libraries such as Qt, OpenSSL, Apache, or PostgreSQL; these third-party library updates often bring bug fixes but can also contain critical security fixes.

In addition, we only support the two latest major versions of FileWave. With FileWave 16.3 released, FileWave 16.1 is no longer supported, and if you don't upgrade you'll leave your server at risk.

Starting with FileWave 16.3, FileWave Central will remind you if your server is outdated (so when 16.5 is out) and no longer supported. Don't hesitate to reach out if you need any help to upgrade your system.

Simplified and More Robust Client Upgrade Process

Upgrading the FileWave Client is critical for accessing new features, security enhancements, and performance improvements. However, client upgrades have traditionally been risky operations:

the FileWave Client is the core management component on macOS and Windows devices, and a failed upgrade may leave devices unmanaged, sometimes requiring manual recovery at scale.

Historically, the upgrade mechanism relied on the FileWave Client updating itself through the Client Upgrade Fileset. This approach works in many scenarios but has inherent limitations, since the Client must stop itself mid-process and restart successfully. Any disruption at that stage can break communication with the server.

New Upgrade Architecture in FileWave 16.3.0

FileWave 16.3.0 introduces the foundation for a safer, more controlled, and more automated client upgrade workflow through a new dedicated component: the FileWave Client Upgrader. This new process runs independently alongside the FileWave Client and assumes full responsibility for orchestrating the upgrade.

Key Capabilities

1. Independent and resilient upgrade controller - The FileWave Client Upgrader is a standalone process capable of stopping, replacing, and restarting the FileWave Client safely. Because it operates independently, it continues supervising the upgrade even if the client itself is temporarily offline, greatly reducing the risk of incomplete upgrades.
1. Built-in compatibility validation - Before initiating an upgrade, the Upgrader performs its own compatibility checks to ensure only safe upgrade paths are executed. These checks run regardless of the FileWave Client's state.
1. Automatic retry and rollback logic - If an upgrade fails, the Upgrader can retry automatically. When necessary, it can roll back to the last known working version, preventing devices from falling into an unmanaged state. If the rollback succeeds, the upgrade target is marked as requiring manual intervention, and this version will not be attempted again automatically. Administrators may trigger a retry manually after resolving the underlying issue, or the Upgrader will attempt again automatically if a newer version (release or custom build) becomes available.
1. Configurable batch-based rollout - Administrators will still be able to initiate a full-fleet upgrade, but FileWave will execute upgrades in batches. The batch size will be admin-configurable. If issues appear within a batch, subsequent batches are automatically paused.

This concept is inspired by the Booster upgrade workflow, but adapted for client-scale operations where per-device serial upgrading is impractical.

1. Support for custom builds - The new Upgrader fully supports delivery of custom or support-provided builds (e.g., test or fix versions). These can be distributed and upgraded with the same safety and automation guarantees as official releases.

Looking Ahead: Operational Use in 16.4

Because the new architecture is introduced in FileWave 16.3.0, the next upgrade, to FileWave 16.4.0, will be the first to fully leverage it. FileWave Central will include a dedicated module for managing, scheduling, and monitoring client upgrades, giving administrators full visibility and control over the process.

Recommendation

Since the new upgrade infrastructure becomes active only once a device is running FileWave Client 16.3, upgrading to 16.3 is strongly recommended. This ensures all subsequent client upgrades, including important future releases, benefit from the enhanced safety, automation, and fault-tolerance mechanisms provided by the FileWave Client Upgrader.

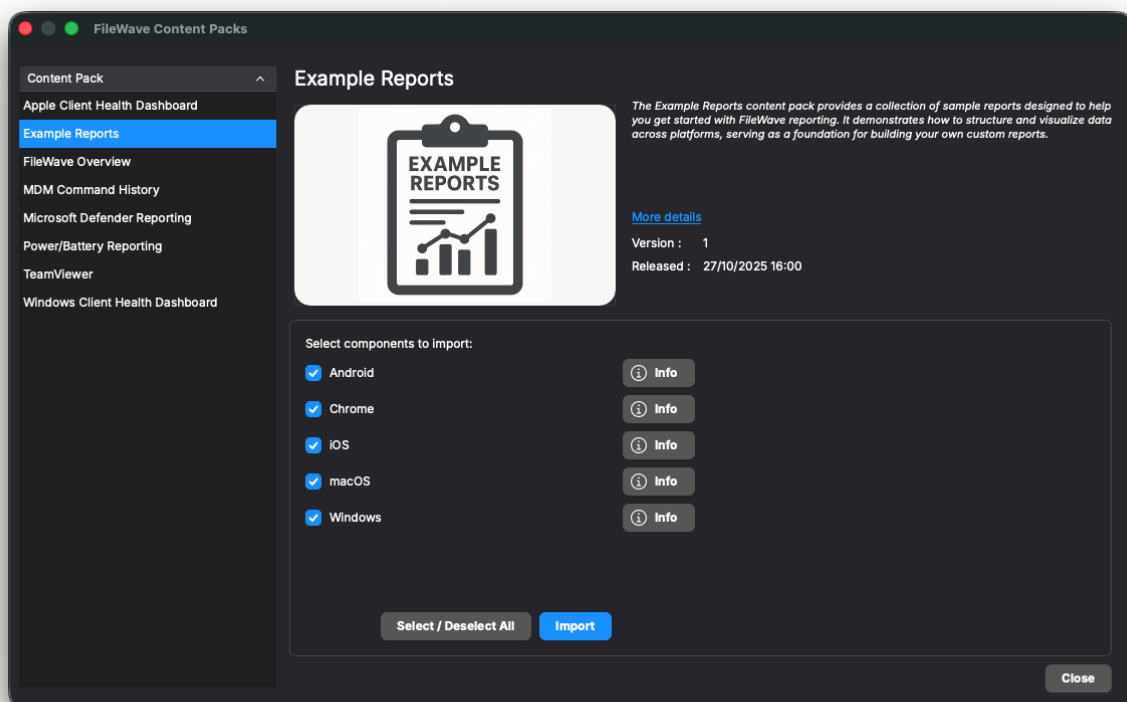
Inventory Queries Renamed to Reports

To align FileWave Central with FileWave Anywhere, the Inventory Queries module has been renamed to Reports. This change standardizes terminology across interfaces without altering the underlying data model or API—existing queries remain fully compatible, and all API endpoints continue to use “query” for backward compatibility.

User-created queries are unaffected; only the module name and user interface labels have changed.

As part of this update, the legacy Default Queries have been replaced with a new Default Reports content pack. These updated examples provide modern, platform-specific templates to help administrators build complex reports more efficiently.

Additionally, content packs can now include per-platform reports, allowing more tailored and relevant default reporting across different operating systems.



Consistent “Reinstall Fileset” Functionality Across All Fileset Types

The Reinstall Fileset feature allows administrators to manually trigger the reinstallation of one or more filesets directly from Client Info (per-device view) or from Fileset Reports (per-fileset view). This function is commonly used to repair or refresh deployments.

In FileWave 16.1, Fileset Reports were unified to merge Desktop and Mobile reports into a single consistent view. This major refactor also refined how the Reinstall Fileset action is handled, leading to limited support for certain fileset types in some cases. Partial improvements were delivered in 16.2, and with FileWave 16.3, the feature now operates consistently across all supported fileset types, for both Desktop and Mobile environments.

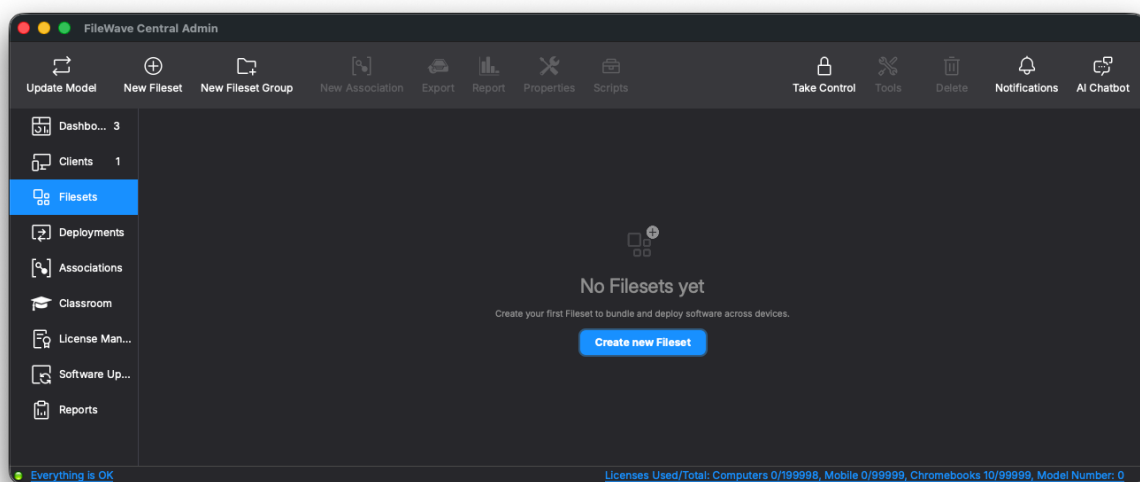
This enhancement completes the unification work started in 16.1 and ensures consistent, predictable reinstall behavior across all platforms.

Improved Empty States in Central Tables

To enhance usability and provide a smoother onboarding experience, FileWave 16.3 introduces improved empty state views in the Clients, Filesets, and Reports tables.

When no data is available—for example, no enrolled clients, no created filesets, or no existing reports—Central now displays a clear message with an icon and an action button (such as Enroll New Client or Create New Fileset) instead of showing an empty table. The same visual feedback also appears when search or filter results return no matches, prompting users to adjust their criteria.

This enhancement improves first-time setup clarity, streamlines user guidance, and aligns the Central UI design with FileWave Anywhere. Similar improvements will be extended to other views in future releases.



Enhanced Policy Tab in Client Info

The Policy tab in Client Info has been improved to provide better visibility and management of FileWave Policies.

Previously, the tab displayed basic policy information but did not indicate which Fileset each policy originated from. Starting with FileWave 16.3, the tab now shows the associated Fileset name and includes a context menu option to reveal the Fileset directly in Central.

This enhancement simplifies troubleshooting and administration by allowing faster access to the Fileset defining each applied policy—especially valuable as FileWave Policy expands to additional areas such as Kiosk and Software Update.

Inventory Improvements

Fileset Creation and Modification Dates Added to Inventory

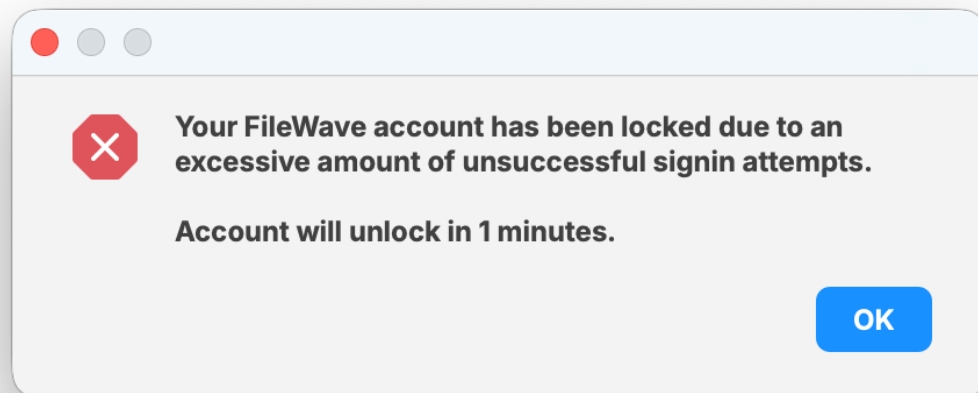
FileWave Inventory has long tracked information about installed Filesets, primarily for use by the Licensing module (where installed Filesets consume licenses). Starting with FileWave 16.2, Inventory was expanded to include all Filesets, not just the installed ones, enabling broader reporting and visibility.

With FileWave 16.3, the Inventory now also records and reports each Fileset's creation and last modification dates. This enhancement allows administrators to audit content changes more easily, identify recently updated Filesets, and better manage Fileset lifecycle and version tracking.

Security Improvements

Brute Force Lockout

Enabled by default in Central -> Preferences the Brute Force protection will prevent dictionary attacks attempting to login to Central or Anywhere. On lockout you will see a dialog indicating how long the lockout is for. It begins at 1 minute by default and escalates with additional incorrect logins. This feature can also be disabled, but it is strongly recommended to keep it enabled. ([more details](#))



Apple-Specific Changes

iOS/iPadOS Kiosk now deploys as a VPP app

! This is a very important change to understand before upgrading to 16.3.0.

In FileWave 16.3.0, the iOS/iPadOS FileWave Kiosk moves to the Apple App Store and is now deployed as a VPP / Apps and Books app, so customers should make sure FileWave is syncing with Apple School Manager (ASM) or Apple Business Manager (ABM) and that they have already acquired enough free FileWave Kiosk licenses before upgrading; otherwise deployment of the new Kiosk can be delayed until licensing is in place and devices verify again. Customers should review [Automatic updating of iOS/iPadOS Kiosk](#) for the full behavior change and, if they want notifications to appear without prompting, review [Force Enable Notifications on iOS and macOS for FileWave Kiosk](#), since the iOS/iPadOS Kiosk bundle identifier for 16.3.0+ is now com.filewave.ios.app.kiosk3.

Enhanced DDM Fileset Status in Client Info

Certain DDM-based Filesets—such as Screen Sharing Configuration—combine multiple DDM configurations within a single Fileset. Since each configuration can install or fail independently, earlier versions of FileWave could only display an overall Fileset status, making troubleshooting difficult.

With FileWave 16.3, the Client Info → Fileset Status view in FileWave Central now provides detailed status information for each configuration within multi-configuration DDM Filesets. This allows administrators to identify which specific configuration succeeded or failed during deployment.

The DDM status information is displayed in the same area as Script status, as scripts and DDM configurations cannot coexist within the same Fileset.

This enhancement improves diagnostic accuracy for complex DDM-based Filesets without affecting single-configuration ones.

macOS 26 Composed Icons for Central and Tools

Arguably the most important change in FileWave 16.3: FileWave Central (and companion tools such as the standalone Superprefs Editor) now feature macOS 26 (Tahoe) composed icons. These new icons support Apple's Liquid Glass Design and tinted accent coloring, ensuring full visual harmony with the latest macOS look and feel.

While this won't improve deployment speed or database performance, it will make your Dock look noticeably more modern.

Profile Editor Updates

The Profile Editor in FileWave 16.3 has been updated to include the latest Apple-defined payload keys and schema changes as per the official [Device Management documentation](#). These updates ensure full compatibility with recent iOS, iPadOS, and macOS releases and improve accuracy when creating or editing configuration profiles.

iOS Restrictions payload:

- safariAcceptCookies and autonomousSingleAppModePermittedAppIDs are now optional keys, aligning with Apple's updated specification.

Per-App VPN payload:

- Added new keys:
 - AssociatedDomains — defines the list of domains to be routed through the VPN.
 - ExcludedDomains — specifies domains excluded from VPN routing.
 - SMBDomains — identifies domains accessed via SMB that should use the VPN connection.

VPN (IKEv2) payload:

- Added new security-related keys:
 - AllowPostQuantumKeyExchangeFallback — allows fallback to classical key exchange if post-quantum algorithms are not supported.
 - PostQuantumKeyExchangeMethods — specifies permitted post-quantum key exchange algorithms.
 - EnforceStrictAlgorithmSelection — enforces strict adherence to the configured cryptographic methods.
- Updated supported values for DiffieHellmanGroup and EncryptionAlgorithm to match current Apple specifications.

Web Content Filter payload:

- Added SafariHistoryRetentionEnabled — controls whether Safari browsing history is retained when content filtering is enabled.

DDM changes

Support for FileWave Agent Installation via DDM Protocol

FileWave 16.3 adds support for installing the FileWave Agent using the Declarative Device Management (DDM) protocol on compatible macOS devices (macOS 26 / Tahoe and later).

Previously, the Agent was installed using the traditional MDM protocol. In FileWave 16.3, DDM-based Agent deployment is available as a technical preview for supported systems, but it is not enabled by default. When enabled, FileWave uses DDM for Agent deployment on supported systems while continuing to use MDM for older macOS versions.

This change affects only the Agent installation process. Installation of customer packages remains unchanged and continues to be handled by the FileWave Agent through the standard Fileset mechanism.

This enhancement ensures FileWave remains compliant with Apple's evolving DDM framework and prepares the platform for future DDM-based management capabilities.



Note: This functionality is currently offered as a technical preview and is not enabled by default. It will be enabled by default in a future release.

Update Behavior and Version Pinning for Apps Installed via DDM

FileWave 16.3 enhances Declarative Device Management (DDM) support by adding precise controls over how managed applications are installed and updated on iOS, iPadOS, and macOS devices.

When deploying applications through DDM, administrators can now configure app lifecycle behavior directly in Fileset Properties, similar to other deployment options:

- Update behavior: define whether the app should automatically update when a new version becomes available on the App Store, or remain on its current version.
- Version pinning: specify an exact app version to install and keep, preventing automatic upgrades beyond that version.

These settings are based on Apple's latest DDM specifications:

- [AppManagedInstallBehaviorObject](#) — controls version targeting for app installation.
- [AppManagedUpdateBehaviorObject](#) — defines update rules for managed apps.

This enhancement provides administrators with fine-grained control over application versioning and update policies across all DDM-managed Apple platforms.

Improved Handling of Profile Installation with DDM

While Profiles continue to be installed through MDM, FileWave is actively preparing for the upcoming transition to Declarative Device Management (DDM) when Apple expands or mandates its use.

With FileWave 16.3, the system now correctly handles Command Policy Profiles during DDM processing. These Filesets are not real configuration profiles but represent MDM command wrappers (such as restart or update actions). They are now properly excluded from DDM installation and automatically converted into their corresponding MDM commands during deployment.

This refinement ensures accurate behavior for mixed DDM/MDM environments and provides a solid foundation for future DDM-based profile installation once it becomes the Apple standard.

DDM “Service Configuration Files” Configuration updated

Apple has now additional Built-in services : `com.apple.cryptoTokenKit` and `com.apple.authorization` ; DDM Configuration editor has been updated accordingly.

Configure Application extensions when installing applications via DDM

When installing applications using DDM, it is now possible to specify configuration for extensions which could be used by the application. This is similar to “App Config” feature, which allowed configuring application itself, but this one is for extensions.

“VPP notifications” improvements

Apple introduced VPP Notifications when the VPP API was redesigned. Instead of having the MDM server regularly poll Apple for VPP-related changes, the server can subscribe to notifications and let Apple push updates as they occur. This is particularly important for User-based licenses: when a VPP license is assigned, FileWave historically waited three minutes before installing the application to ensure that the Purchase History was fully updated. This delay was intentionally conservative but often resulted in slower app deployments and a poor user experience.

With VPP Notifications, this delay is eliminated. Apple notifies FileWave as soon as the license becomes effective, allowing FileWave to install the app immediately—without waiting three minutes.

VPP Notifications were originally introduced in FileWave 14.7.0, but required manual admin enablement, because a misconfigured setup (for example, a server not reachable by Apple) could interrupt VPP communication entirely.

Starting with FileWave 16.3, the configuration process has been redesigned. FileWave now automatically determines whether the server is reachable by Apple and will enable or disable VPP Notifications accordingly. As a result, most servers will benefit from notification-based behavior automatically, with no additional configuration required.

ADE Profile Update

ADE and Backup

It is now possible to set the `do_not_use_profile_from_backup` key in ADE profiles. As documented by Apple (see [Apple's deployment guide](#)), this flag ensures that a device restored from a backup behaves as if the backup were restored on a different device. This allows the device to receive the correct ADE configuration instead of reusing the profile embedded in the backup.

New “Age Based Safety Settings” Skip Key Added to ADE Profiles and Setup Assistant

A new Age Based Safety Settings skip key is now available for ADE profiles and Setup Assistant. One of Apple's documentation sources suggests that this key may replace the existing `AdditionalPrivacySettings` key. However, this change is not consistently reflected across all Apple documentation. Until Apple provides definitive confirmation, FileWave will support both keys.

Rapid Security Response Replaced by “Background Security Improvements”

Rapid Security Response (RSR), introduced by Apple in iOS 16, provided a mechanism to deliver urgent security fixes without requiring a full operating system update. With the release of Apple's 2026 operating systems, this mechanism has been replaced by a new system: Background Security Improvements. This is not a simple renaming—Apple has changed how rapid security fixes are delivered at the OS level. FileWave has been updated to support this new behavior.

Android-Specific Changes

Compliance with Google API Rate Limit Recommendations

FileWave 16.3 updates the communication between the FileWave Client and the Google Android Management API (AMAPI) used for Android Enterprise (EMM) device management.

The implementation now follows Google's recommended rate limit settings, ensuring full compliance with current API usage guidelines. This change prevents potential throttling by Google services and improves stability when managing large Android fleets.

All adjustments are internal—no administrative action or configuration change is required.

Windows-Specific Changes

Software Update Status Enhancements for Windows

Building on the improvements introduced in FileWave 16.2, which allowed Software Updates on Windows to be managed via FileWave Policy, FileWave 16.3 adds richer tracking capabilities.

Updates deployed through Policy are now clearly labeled as “Triggered by Policy” in the Software Update status view, enabling administrators to confirm that their policies are functioning correctly. This new status is visible in both FileWave Central and FileWave Anywhere, and the information is also recorded in Inventory for reporting and auditing purposes.

This enhancement applies to Windows devices only, as Software Update Policy management is not available for macOS.

FileWave Windows Imaging (IVS) Changes

FileWave Windows Imaging solution relies on PXE Boot, which delivers a tiny Linux image containing all required components to run the imaging process. Compatibility with different hardware depends on how the tiny Linux image is built - mainly which Linux kernel version and embedded packages and modules.

FileWave Network Imaging 16.3.0 brings compatibility with FileWave 16.3.x.

- Linux kernel: 6.17.7
- Buildroot: 2025.08.1
- partclone: 0.3.37

Internal Changes

macOS Code signing identity change

The code signing identity we use to sign FileWave binaries and applications changes from “FileWave (Europe) Gmbh” (team ID 83S2TRZ3CS) to “FileWave (USA), Inc.” (UWMR88SA8G).

FileWave 16.2.3 and beyond will automatically update the [TCC Profile](#) which is deployed to grant FileWave client (fwcld) the right permissions when deployed via MDM.

There should be no other impact except the name of the signing identity.

Supervisord for FileWave Server on macOS

Starting with FileWave 16.3, the macOS Server now uses supervisord—the same process management system used on Linux—to start, monitor, and stop FileWave services.

Previously, FileWave relied on multiple LaunchDaemons, and the fwcontrol script manually called launchctl while echoing status information. With the move to supervisord, fwcontrol now leverages supervisord's native service control and status reporting, providing clearer and more consistent output across macOS and Linux.

This change also simplifies service configuration, replaces multiple plist files with a single supervisord configuration, and improves log rotation reliability.

The migration is fully automatic during upgrade, and administrators can continue using fwcontrol commands as before—only the output format and detail have changed.

Database Access Code Modernization

Several internal components of FileWave's database access layer have been modernized in FileWave 16.3 as part of our ongoing effort to update legacy code, improve maintainability, and reduce resource consumption. While these changes are primarily internal, they improve code consistency and long-term reliability.

Key improvements include:

- Rewritten logic for generating unique client names, making the process faster and more robust.
- Extended Database Integrity Checks During Upgrade
- Improved Client Robustness and Local Data Handling
- PostgreSQL 18 Upgrade

These updates are foundational and prepare the system for future scalability and performance enhancements.

Extended Database Integrity Checks During Upgrade

FileWave runs a series of database integrity checks during upgrades to confirm that the database is in a valid and consistent state. When possible, issues are automatically corrected, and if a non-recoverable problem is found, the upgrade process safely stops, allowing FileWave Support to intervene before data integrity is compromised.

With FileWave 16.3, these checks now include validation of internal database sequences, ensuring that automatically generated IDs remain consistent across all related tables. These extended checks run as part of the upgrade process but can also be executed manually to verify the full database state when needed.

This enhancement improves overall database reliability without adding noticeable time to the upgrade process.

Improved Client Robustness and Local Data Handling

The FileWave Client keeps key operational data (such as the catalog) stored locally, enabling it to start and operate even before re-establishing a connection to the FileWave Server.

With FileWave 16.3, the client now uses an atomic file handling mechanism to store this local data, greatly reducing the chance of corruption in case of abrupt shutdowns or power loss. Although the client could previously recover automatically from corrupted data, such recovery required a full local reset and re-synchronization from the server, which could delay normal operation. This new approach minimizes that risk and ensures smoother, more reliable restarts.

PostgreSQL 18 Upgrade

FileWave 16.3 upgrades the embedded database engine to PostgreSQL 18 (previously PostgreSQL 17, introduced in FileWave 16.0). The database upgrade is performed automatically as part of the FileWave Server upgrade process.

For safety, the installer includes both PostgreSQL 17 and PostgreSQL 18. If the upgrade to version 18 fails, FileWave automatically reverts to PostgreSQL 17 and continues running in a degraded mode. In this state, most features will remain functional, but stability or performance cannot be guaranteed. A clear warning will be shown in this case, and administrators are advised to contact FileWave Support immediately to complete the migration.

Because of this database transition, upgrading to FileWave 16.3 is only supported from FileWave 16.0 or newer.

VPP Improvements

The code responsible for communicating with Apple's VPP servers has been thoroughly reviewed using insights gathered from real-world server behavior. This analysis allowed us to implement several under-the-hood optimizations. For example, we significantly reduced the number of database queries executed during Apple VPP synchronizations, lowering overall resource consumption and improving performance.

Many 3rd party updates

Most relevant:

- Apache 2.4.67
- OpenSSL 3.6.2
- Postgres 18.3 and 17.9
- Python 3.14.3
- Redis 8.4.0
- Qt 6.10.2

Deprecated Features

The following features have been deprecated from FileWave 16.3. They are present but will be removed in a future release:

- None

We encourage you to provide product feedback if you have any concerns: [FileWave Product Management](#) or in the Help menu of Central/Anywhere you can send feedback as of 16.3.

Decommissioned Features

The following features have been removed from FileWave 16.3.0:

macOS 12 Monterey platform support

Starting with FileWave 16.3.0, macOS 12 Monterey was removed from the Expected to work platform support lists for FileWave Clients, FileWave Server, FileWave Central, and FileWave Booster. This change was made because macOS 12 is no longer receiving current security updates from Apple, and FileWave 16.3 and later releases need to continue moving forward with current macOS frameworks, platform behavior, and security requirements. Customers who still need to manage macOS 12 devices should use the FileWave 16.2.5 client listed in the Legacy section. For details, see [macOS 12 Monterey Platform Support - EOL](#).

IVS Upgrade Simplification

Previously, Imaging Virtual Server (IVS) could be upgraded using standard Debian package commands (apt update / apt upgrade), which updated the IVS components, kernel, admin, and client. Although convenient, this method was rarely used, as most administrators preferred the upgrade script provided on the FileWave download page.

Starting with FileWave 16.3, the Debian repository will no longer be maintained. It will remain accessible but will not receive updates, meaning existing systems configured to use it will simply stop retrieving new packages.

All IVS upgrades should now be performed using the official upgrade script, available on the FileWave download page together with the corresponding upgrade instructions. This unified process simplifies maintenance and ensures version consistency across all components.

Removal of Model Update v1 (Legacy Implementation)

The legacy Model Update v1 process—implemented across multiple components with a mix of C++ and Python—has been removed in FileWave 16.3.

Since FileWave 16.0, all instances have used the unified Model Update v2 (100% Python) as the default. v1 remained present only for transition purposes between 16.0 and 16.2; it is now no longer included or supported.

No administrator action is required. This decommissioning completes the migration to the unified framework, simplifying internals, improving testability, and paving the way for future enhancements.

Changes and Fixes in 16.3.3

Changes and Fixes in 16.3.3

Updated third party components:

- Apache 2.4.68
- openssl 3.6.3
- pgbouncer 1.25.1
- python 3.14.6
- redis 8.6.3
- nats server 2.12.6
- nginx 1.31.2
- grafana 12.0.9

- prometheus 3.11.3
- SQLite 3.53.2
- xz 3.8.3

Bug fixes:

- FWRD-17731 Ensure pre-16.3 launch agent files are removed in early stages of macOS package to improve upgrade robustness
- FWRD-17734 Optimize checks done during server upgrade to mitigate macOS installer timeout causing upgrade failures
- FWRD-17742 Fixed an issue where a booster restart would be required after server is upgraded
- FWRD-17764 Fixed an issue where Windows MDM client would require a restart after installation to connect to server
- FWRD-17781 Fixed regression introduced in 16.3.2 where imported non-reboot flat pkg would incorrectly have reboot flag

Changes and Fixes in 16.3.2

Updated third party components:

- Apache 2.4.67
- curl 8.20.0
- expat 2.8.1
- libArchive 3.8.7
- libXML2 2.15.3
- nginx 1.31.1
- PostgreSQL 17.10 and 18.4

Bug fixes:

- FWRD-17553 Fixed a potential database deadlock when processing inventory reports and MDM communications for the same device
- FWRD-17586 Fixed a Central crash that could occur when closing the Fileset Script dialog before closing the script editor
- FWRD-17595 Improved handling of communication and service errors when synchronizing VPP asset information
- FWRD-17626 Fixed an issue where the FileWave agent could wait up to 20 minutes to download the Upgrader Service, causing enrollment or startup delays
- FWRD-17627 Introduced a dedicated download location for the Client Upgrader to avoid versioning-related confusion
- FWRD-17633 Fixed an issue where a Windows Upgrade Fileset could wait indefinitely if the MSI installation returned a generic 1603 error
- FWRD-17634 Improved the robustness of the Client Upgrader on Windows
- FWRD-17648 Fixed an issue where an incorrect VC Redistributable version could be installed when installing components on Windows
- FWRD-17649 Fixed an issue where upgrading to version 16.3 could fail if scheduled tasks used custom schedules defined in the settings_custom.py file
- FWRD-17664 Fixed potential database deadlocks that could occur during macOS MDM enrollment
- FWRD-17685 Restored support for the Realtek R8169 network adapter in Imaging

Changes and Fixes in 16.3.1

Updated third party components:

- Apache 2.4.67

Bug fixes:

- FWRD-16703 Fixed an issue where email username and password were required when SMTP server did not require them.
- FWRD-17368 Fixed an issue where deploying a profile with legacy variables like WIRELESS_INTERFACE_NAME could fail
- FWRD-17547 Fixed a 16.3.0 regression related to Apple BSI support which could prevent Boosters from reporting data to Inventory
- FWRD-17551 Fixed a 16.3.0 regression which would prevent moving FileWave Central on macOS
- FWRD-17553 Fixed a potential database deadlock when server processes fwcd inventory report and MDM communication for the same device
- FWRD-17554 Fixed an issue where imported intermediate CA certs would be ignored when creating ADE profiles, system relying on AIA url or certifi trust store only

Changes and Fixes in 16.3.0

Updated third party components:

- OpenSSL 3.6.2
- Postgres 18.3 and 17.9
- Python 3.14.3
- Redis 8.4.0
- Qt 6.10.2

Bug fixes:

- FWRD-2731 Ensure deleted client names are properly recorded in Audit History Logs so administrators can fully trace client lifecycle events.
- FWRD-3386 Ensured all MDM server logs under /usr/local/filewave/log follow consistent rotation rules
- FWRD-3534 Fixed an issue where updating a placeholder client name in a template did not update the corresponding FileWave Client name in the MDM admin interface
- FWRD-3980 Fixed an issue where unmodified MDM policy filesets could be saved and treated as modified
- FWRD-11697 Surface Shared iPad-specific property entries in FileWave Anywhere so Shared iPad deployments can be inspected and managed consistently with other iOS devices.
- FWRD-12537 Align default kiosk fileset icon color and size so kiosk icons are consistent across filesets and platforms.
- FWRD-13407 Fixed an issue where the main menu bar on macOS was no longer displayed globally in the admin application
- FWRD-14830 Reduce excessive backend logging while a CM session is open to lower noise in logs and improve diagnosability.
- FWRD-14895 Fixed an issue where the remote wipe dialog for tvOS devices incorrectly referenced iOS
- FWRD-15108 Fixed an issue where an incorrect context menu could be shown for clients in the Create New Association dialog

- FWRD-15160 Fixed an issue where rapidly duplicating filesets could result in unexpected behavior
- FWRD-15228 Fixed an issue where no clear error message was shown when creating an MDM client group without sufficient permissions in FileWave Central
- FWRD-15341 Removed unsupported "eng" language examples from ADE profile configuration to align with Apple MDM behavior
- FWRD-15449 Restore the "Remove" (X) icon in the deployment filesets tab so administrators can easily remove filesets from deployments.
- FWRD-15511 Renamed the Web Console to FileWave Anywhere
- FWRD-15588 Fixed an issue where deleting a FileVault profile while editing an ADE profile could trigger an error if the profile was selected
- FWRD-15618 Prevent fileset dependencies belonging to groups without permissions from being exposed in Anywhere, ensuring access control is respected.
- FWRD-15634 Fixed an issue where searches in MDM profile editors could display raw HTML tags in Central Admin
- FWRD-15698 Correct the verification script tooltip text in Anywhere so it accurately describes execution order and avoids misleading admins.
- FWRD-15734 Add clear UI feedback when an already registered VPP token is uploaded so admins understand the 412 error and can adjust configuration.
- FWRD-15883 Added the missing maxInactivity setting to the Apple Passcode MDM profile
- FWRD-15906 Fixed an issue where removing a serial number from an ADE placeholder could cause MDM database integrity errors
- FWRD-15910 Fixed an issue where an iPhone could be incorrectly named as an iPad before MDM enrollment completed
- FWRD-15953 Fixed an issue where filtering ADE accounts in the ADE association dialog produced inconsistent results
- FWRD-15995 Update Anywhere error messaging to use "Entra ID account" terminology when duplicate accounts are created, matching Microsoft's current naming.
- FWRD-16003 Fixed an issue where the Booster Monitor was unusable on low resolution displays
- FWRD-16021 Align the availability rules for the "Reinstall fileset" action between Anywhere and Central so reinstall behavior is consistent across UIs.
- FWRD-16025 Ensure backend correctly updates packet and modified flags whenever fileset dependencies change, improving model integrity and deployment accuracy.
- FWRD-16053 Fixed an issue where the Offer Program setting for DDM software update configurations was not properly initialized
- FWRD-16057 Fix dialog validation so once all errors are resolved, configuration changes can be saved without having to reopen the dialog.
- FWRD-16134 Fixed multiple issues affecting the System Extension Policy MDM profile
- FWRD-16138 Fixed an issue where Model Update failures were not correctly reported to MDM administrators
- FWRD-16167 Decouple app logos from kiosk configuration so kiosk behavior is not tied to or blocked by logo assets.
- FWRD-16175 Fixed an issue where UI elements in Central Preferences on Windows were misaligned when using 150 percent display scaling
- FWRD-16201 Close the IDP URL view automatically when Anywhere admin sessions time out to avoid stale authentication panels remaining visible.
- FWRD-16220 Fix ADE account creation so cancelling and reopening the form resets validation state (e.g., Save is disabled again until a valid token is uploaded).
- FWRD-16230 Improved German translations in the MDM admin interface
- FWRD-16264 Fixed an issue where a client clone could be added to an MDM deployment instead of the original client
- FWRD-16271 Allow admins to browse and select the correct group folder for fileset creation when importing Apple VPP tokens in Anywhere.
- FWRD-16307 Fixed an issue where the Fileset Status Report could not be saved on Windows

- FWRD-16308 Fixed an issue where the Source field of an MDM profile was not updated correctly
- FWRD-16309 Fixed an issue where Modify Filesets permissions were not enforced when creating AutoPKG or Winget filesets
- FWRD-16329 Fixed multiple UI inconsistencies in the Central Preferences dialog
- FWRD-16349 Fixed an issue where iOS applications installed via MDM kiosk could be reinstalled automatically after a device wipe when using DDM
- FWRD-16355 Fixed an issue where sorting date columns did not work correctly in the Fileset Status Report dialog
- FWRD-16370 Fixed an issue where client conflict resolution results were not correctly interpreted in Central Admin
- FWRD-16380 Fixed an issue where the DISABLE_PERMISSIONS_SET_ON_RESTART variable was ignored during MDM server upgrades, potentially increasing upgrade time
- FWRD-16383 Ensured daily and hourly scheduled MDM tasks do not run concurrently
- FWRD-16415 Fixed an issue where VPP applications could be reinstalled during a verify operation on macOS
- FWRD-16416 Hide or disable the "Allow removal" option for App Store filesets when DDM_APPS is enabled so removal settings stay aligned with DDM app management.
- FWRD-16427 Fixed an issue where scripts were not executed when included in AutoPKG filesets
- FWRD-16431 Fixed an issue where resolving client conflicts could result in a server error
- FWRD-16436 Improved the error message shown when duplicating a client without sufficient MDM licenses
- FWRD-16475 Fixed an issue where the New Release dialog could appear before login completed in Central
- FWRD-16477 Fixed an issue where closing the Central Admin main window did not close an open client monitor
- FWRD-16546 Ensure CSV imports correctly update the Imaging MAC Address field so imaging data stays accurate after bulk updates.
- FWRD-16569 Fixed an issue where the Content Pack Assistant dialog content could briefly shift when opening
- FWRD-16573 Fix a memory leak in NatsConnectionHandler to improve stability and long-running performance of the frontend.
- FWRD-16601 Fixed an issue where enrolling a device after adding an ADE placeholder could break the model update process
- FWRD-16648 Allow editing of custom fields with restricted value sets in Anywhere while still enforcing value constraints.
- FWRD-16771 Ensured policy based assistants such as DDM Assets and ADM Configurations are fully translated
- FWRD-16814 Fixed an issue where flat buttons in Central used an incorrect background color
- FWRD-17022 Fixed an issue where reports for macOS 14 and 26 SIP status were not generated when using Model Update v2
- FWRD-17049 Fixed an issue where conflicting timestamps would appear in Last Connected for Android devices
- FWRD-17086 Ensured the EnableIPv6 setting is available in the Network MDM payload
- FWRD-17109 Exclusions in deployments don't work
- FWRD-17128 [FE][16.3] URI special characters in log file might corrupt it when downloading it via CM
- FWRD-17191 Fixed an issue where custom field values would be kept when resolving enrollment conflict using "remove old" strategy.
- FWRD-17199 Fixed a rare issue where files uploaded from Central could become corrupted on disk, causing repeated re-downloads due to CRC mismatch.
- FWRD-17245 Fixed an issue where the server checked disk space for the full file instead of remaining chunks, causing valid uploads to be rejected.

- FWRD-17257 [BE][16.3] Invalid device platform breaks enrollment screen in AW and causes a false-positive "new device" badge (backport to 16.3)
- FWRD-17432 Fixed an issue where the Fileset status for Background Security Improvement OS updates was incorrectly reported as "superseded by another update" after successful installation.

Included Open Source Software

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

Upgrading Your Environment

Urgent: If you manage iOS/iPadOS devices you must ensure that you review the release notes and get VPP licenses for FileWave Kiosk (free) as outlined here: [Automatic updating of iOS/](#)

- !** [iPadOS Kiosk](#) The kiosk is no longer an IPA and does come as a VPP application now in following Apple best practices. You can get the licenses before or after upgrading but will have a better experience if you do it before and then sync VPP in Central -> Preferences to ensure the licenses are seen.

macOS Downloads



[macOS Upgrade Fileset](#) (md5: ffad459152eb7a02152f4cc7a7298b22)

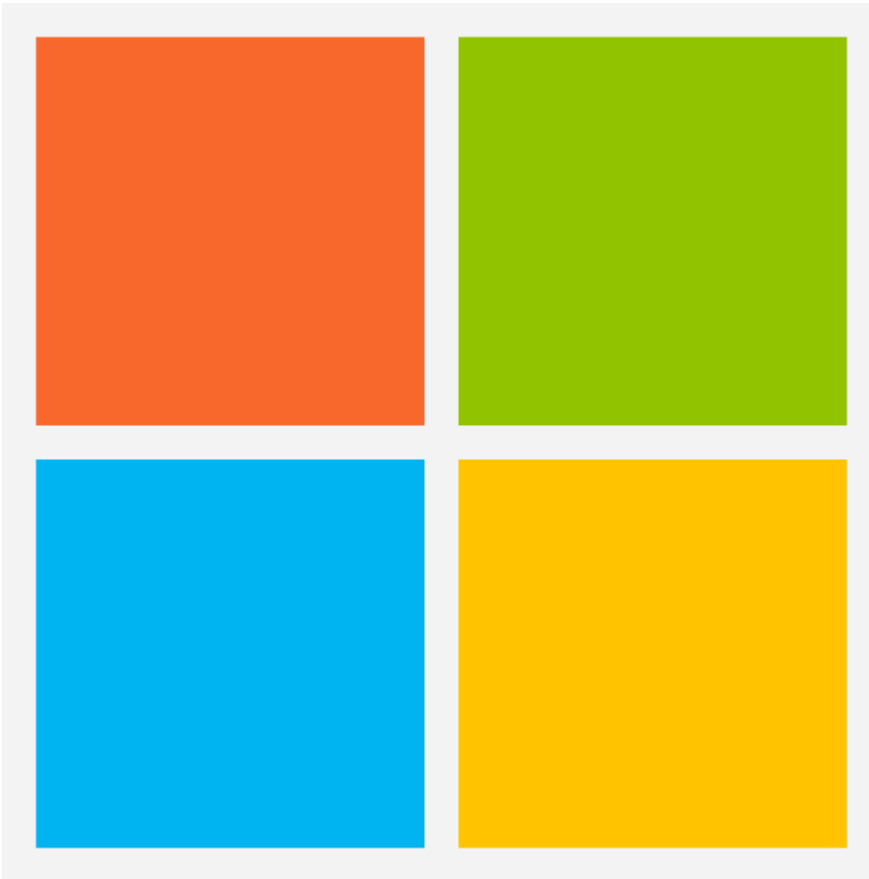
[macOS Central \(Admin\)](#) (md5: 966732eaba1ff712ba99083cc65097af)

[macOS Booster](#) (md5: 82e61ca79c0803b3762c1acb35cca92b)

[macOS Server](#) (md5: 87200b019f850d8f532871c2c3d85d36)

- i** Remember that to upgrade macOS FileWave clients you should use the Upgrade Fileset.
- i** Never deploy the macOS Client installer from <https://custom.filewave.com> to an existing device. It is intended for new installs.

Windows Downloads



[Windows Upgrade Fileset](#) (md5: b022d06173ca0d36db7504e1c507c04d)

[Windows Central \(Admin\)](#) (md5: a4800f56eabeba1b9ee742755604e8c8)

[Windows Booster](#) (md5: 51307c111c9c42e022a08320af69e438)

- Remember that to upgrade Windows FileWave clients you should use the Upgrade Fileset.
- i** Never deploy the Windows Client installer from <https://custom.filewave.com> to an existing device. It is intended for new installs.

iOS Downloads



Kiosk on iOS / iPadOS is now deployed from the Apple App Store as a VPP / Apps and Books app. Before upgrading, make sure FileWave is syncing with ASM/ABM and that enough free FileWave Kiosk licenses have already been acquired. ([Read More](#))

Chrome Extension



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

Debian Linux Downloads



debian

[Debian Linux Server](#) (md5: b10ee8695490f069749fb46f0d90068e)

[Debian Linux Booster](#) (md5: 8b28d06c4327b115db8712f922983187)

[Debian Linux IVS: FileWave Admin](#) (md5: 2690ee7cdcf0ee393d9c592e0400cd5c)

[Debian Linux IVS: FileWave Imaging Client](#) (md5: 2147ddaf52fa143baa42442bf6f1e874))

[Debian Linux IVS: IVS Kernel](#) (md5: f28910b29aa3b137461e78569cdd2dc2)

[Debian Linux IVS: FileWave IVS](#) (md5: 5277021cebb60d1e9e5ddb014e261d3)

For any of the below upgrades you would want to console or SSH to your Server/Booster/IVS and then run the command listed to upgrade the relevant component.

i If you are using a FileWave appliance that before 15.5.0 the SSH access was with the user "root" and for any appliance setup from 15.5.0 or later the user is "fwadmin" and you would have been forced to [set the password on first login](#).

i What the upgrade one-liners do: These commands do more than install the FileWave packages. When run on a Debian-based FileWave Server, Booster, or IVS, the upgrade script also handles the supported Debian 12 to Debian 13 operating system upgrade when needed and applies available Debian security updates as part of the process. This can take longer than a normal FileWave-only package upgrade, so run the command from the console or a stable SSH session and let the screen session finish before rebooting or starting another upgrade.

Upgrading the FileWave Server

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

```
sudo DEBIAN_FRONTEND=noninteractive bash -c 'set -e; apt-get update -y; apt-get install -y -o Dpkg::Options::="--force-confdef" -o Dpkg::Options::="--force-confold" screen wget; ts=$(date +%Y%m%d%H%M%S); scr=fwxserver_upgrade_$ts; tmp=/tmp/fwxserver_upgrade_$ts.sh; wget -qO "$tmp" https://kb.filewave.com/attachments/411; chmod +x "$tmp"; echo "Starting upgrade in screen session: $scr"; echo "Detach with Ctrl-A then D, reattach with: sudo screen -r $scr"; exec screen -S "$scr" bash -lc "\"$tmp\" -v 16.3.3 -r 1 -y"'
```

Upgrading a Booster

To install or upgrade the FileWave Booster, use the following or [Booster Auto-Upgrade](#) :

```
sudo DEBIAN_FRONTEND=noninteractive bash -c 'set -e; apt-get update -y; apt-get install -y -o Dpkg::Options::="--force-confdef" -o Dpkg::Options::="--force-confold" screen wget; ts=$(date +%Y%m%d%H%M%S); scr=fwbooster_upgrade_$ts; tmp=/tmp/fwbooster_upgrade_$ts.sh; wget -qO "$tmp" https://kb.filewave.com/attachments/412; chmod +x "$tmp"; echo "Starting upgrade in screen session: $scr"; echo "Detach with Ctrl-A then D, reattach with: sudo screen -r $scr"; exec screen -S "$scr" bash -lc "\"$tmp\" -v 16.3.3 -r 1 -y"'
```

Upgrading a IVS

To upgrade the FileWave IVS, use the following:

```
sudo DEBIAN_FRONTEND=noninteractive bash -c 'set -e; apt-get update -y; apt-get install -y -o Dpkg::Options::="--force-confdef" -o Dpkg::Options::="--force-confold" screen wget; ts=$(date +%Y%m%d%H%M%S); scr=ivs_upgrade_$ts; tmp=/tmp/ivs_upgrade_$ts.sh; wget -qO "$tmp" https://kb.filewave.com/attachments/408; chmod
```

```
+x "$tmp"; echo "Starting upgrade in screen session: $scr"; echo "Detach with Ctrl-  
A then D, reattach with: sudo screen -r $scr"; exec screen -S "$scr" bash -lc  
"\$tmp\" -v 16.3.3 -r 1 -y"
```

Virtual Appliance Downloads



OVA Images

These three images are OVA images suitable for VMWare or other systems that use OVAs:

[VMware and VirtualBox \(OVA\) Server Appliance](#) (md5: 916c8b9ed10e11797cadf994a376b3d1)

[VMware and VirtualBox \(OVA\) Booster Appliance](#) (md5: d3be457ab374fcf5d009280c42e5c063)

[VMware and VirtualBox \(OVA\) Imaging Appliance](#) (md5: 346707c68c4dc614f02d932a771e93c7)



Microsoft Hyper-V

HyperV Images

These three images are Hyper-V images suitable for Microsoft Hyper-V (Gen 2):

[Hyper-V \(VHD\) Server Appliance](#) (md5: aa350e5042463a99e39f291d8a0b0d84)

[Hyper-V \(VHD\) Booster Appliance](#) (md5: 6861ace17d84b0247626ac62b174ff2b)

[Hyper-V \(VHD\) Imaging Appliance](#) (md5: bffe72d8bcd44c5da7b9ad310903540)

To import our Virtual Appliances, please see: [FileWave Virtual Appliances](#)

To get started with the FileWave Server appliance please see: [Installation and Setup |](#)

i [FileWave KB](#)

For Booster setup: [Booster Installation | FileWave KB](#)

For more information about configuring the IVS appliance please see: [Getting started with](#)

[the Imaging Virtual Server](#)

This book covers how to import our provided OVA's and VHD's into your virtual environments.

Unconfigured Client Installers

macOS and Windows



Please note that the below is only to be used when Support has identified that they are needed to fix an issue. Normally these Client packages are not used. Pushing the PKG or MSI below from FileWave can break a client.

[macOS Client](#) (md5: f7960472cb2e535b55c305df7dcd00c0)

[Windows Client](#) (md5: 975ea837d6879dd34eb57bf9bbf2e650)

🔄Revision #11

★Created 2026-06-18 08:18:24 UTC by Pierre-Nicolas Rigal

✎Updated 2026-07-30 19:13:49 UTC by Josh Levitsky