FileWave Version 16.0.3

The FileWave endpoint management suite allows you to manage your devices wherever they are, wherever you are, whatever they are, and all in one platform!

In the 16.0.3 release we are thrilled to announce a significant upgrade to the FileWave Management Suite, featuring a completely redesigned version of the Client Monitor with enhanced functionalities. This update includes improvements in NAT compatibility allowing you to monitor devices on remote networks, security enhancements, and streamlined user experience, all aimed at empowering administrators with effective tools for device management. Additionally, the Kiosk Policy now allows for customization of the primary color, logo, and Kiosk app name, ensuring a tailored experience for users. Coupled with Software Update enhancements, these upgrades will elevate operational efficiency and provide our users with the best possible experience in managing their environments.

> ⚠ FileWave database engine has been upgraded to Postgres 17 to benefit from security fixes and performance improvements. The Database upgrade process which will take place when updating to FileWave 16.0 can take more time than usual, depending on the size of your set-up.
>
> Please make sure to plan accordingly for your upgrade to take a bit longer.

FileWave Official Version Support

FileWave supports the two latest major versions at any time. For example, if the current version is 16.0.3, we support versions 16.0.3 and 15.5.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 12) 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 14, 15 (Intel and Apple Silicon)

- Debian 12.8 x86_64 (Note that any Debian 12.x is expected to work, and applying security updates may move you to a higher version.)

Expected to work

- macOS 12, 13 (Intel and Apple Silicon)

Virtual Appliances

- HyperV - The images are available as Generation 1 or 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

> ⓘ Your existing FileWave Server must be version 13.3.1 or higher before you can upgrade to FileWave 14.7.2 and then from 14.7.2 you can upgrade to 16.0.3. The minimum memory requirement for FileWave Server is 8GB.

▼ FileWave Clients Platform Support

> ⓘ All OS must be 64bit.

Fully Tested by QA

- macOS 14, 15 (Intel and Apple Silicon)
- Windows 10 (Ent/Pro 21H1 and above), 11 (Ent/Pro 21H2 and above) - x64 architecture.

Expected to work

- Windows Server 2022, Windows Server 2025 - x64 architecture.
- Windows 10 (Edu 21H1 and above), 11 (Edu 21H2 and above) - x64 architecture.
- macOS 12, 13 (Intel and Apple Silicon)

Legacy

- macOS 10.11 → Legacy Version 13.1.5
- macOS 10.12 → Legacy Version 14.0.2
- 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

▼ FileWave Mobile Clients Platform Support

Fully Tested by QA

- iOS 17.6, 18
- iPadOS 17.6, 18
- tvOS 17.6, 18
- Android 14, 15 (EMM Client)
- Chromebook

Expected to work

- iOS 14, 15, 16
- iPadOS 14, 15, 16
- tvOS 14, 15, 16
- Android 8 to 13 (EMM Client)

Legacy

- iOS 13 → Legacy Version 15.0.1
- iOS 10, 11, 12 → Legacy Version 13.1.5

▼ FileWave Central (Native) Platform Support

ℹ All OS must be 64bit.

Fully Tested by QA

- macOS 14, 15 (Intel and Apple Silicon)
- Windows 10 (Ent/Pro 21H1 and above), 11 (Ent/Pro 21H2 and above) - x64 architecture.

Expected to work

- Windows 10 (Edu 21H1 and above), 11 (Edu 21H2 and above) - x64 architecture.
- macOS 12, 13 (Intel and Apple Silicon)

▼ FileWave Booster Platform Support

ℹ All OS must be 64bit.

Fully Tested by QA

- Debian 12.8 x86_64 (Note that any Debian 12.x is expected to work, and applying security updates may move you to a higher version.)
- macOS 14, 15 (Intel and Apple Silicon)
- Windows 10 (Ent/Pro 21H1 and above), 11 (Ent/Pro 21H2 and above) - x64 architecture.

Expected to Work

- Windows 10 (Edu 21H1 and above), 11 (Edu 21H2 and above) - x64 architecture.
- Windows Server 2022, Windows Server 2025 - x64 architecture.

Virtual Appliances

- HyperV - The images are available as Generation 1 or 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 10 and 11 UEFI and non-UEFI devices.

Virtual Appliances

- HyperV - The images are available as Generation 1 or 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

New Client Monitor (Central/Anywhere)

FileWave 16.0 brings significant improvements to the Client Monitor tool:

- NAT compatibility - admin and clients can be on a different network.
- More client logs can be retrieved.
- Unified interface for both Anywhere and Central.

> ℹ️ Note that although the standalone Client Monitor app is included with 16.0.0+ Admin installs, it is only functional for monitoring macOS and Windows clients running less than FileWave Client 16.0.0, but it also still is used to monitor a FileWave IVS for Windows Imaging as of 16.0.x. The old Client Monitor app will eventually be removed in a future version

> ℹ️ With these improvements, there is no longer a "Client Preferences" password used or needed to be able to use the new v.16+ Client Monitor with any FileWave managed devices that are running v.16+ of the FileWave Client..

Software Update revisited (Central)

We are excited to announce major improvements related to Software Update Management:

- Software Updates are now directly accessible from the main window in Central, like in Anywhere.
- Mass creation of multiple updates at once is now possible and you can specify where they go.
- Client Information dialog has better filtering options related to Software Update.
- More details are in the Windows section below for Windows-specific notes.

> ⚠️ The FileWave Software Update Assistant could automatically assign updates to devices that requested them, but this has been removed as a function. Automated deployments will be reintroduced in a future version of FileWave. In the meantime, you can deploy updates by mapping Fileset groups to Client groups. Devices that do not request updates will ignore them, and these filesets can be hidden within Client Information.

Association and Deployment information (Central)

A very useful FileWave Anywhere feature is coming to FileWave Central; In Client Information, each fileset status can now list all associations which could lead to the deployment of the Fileset.
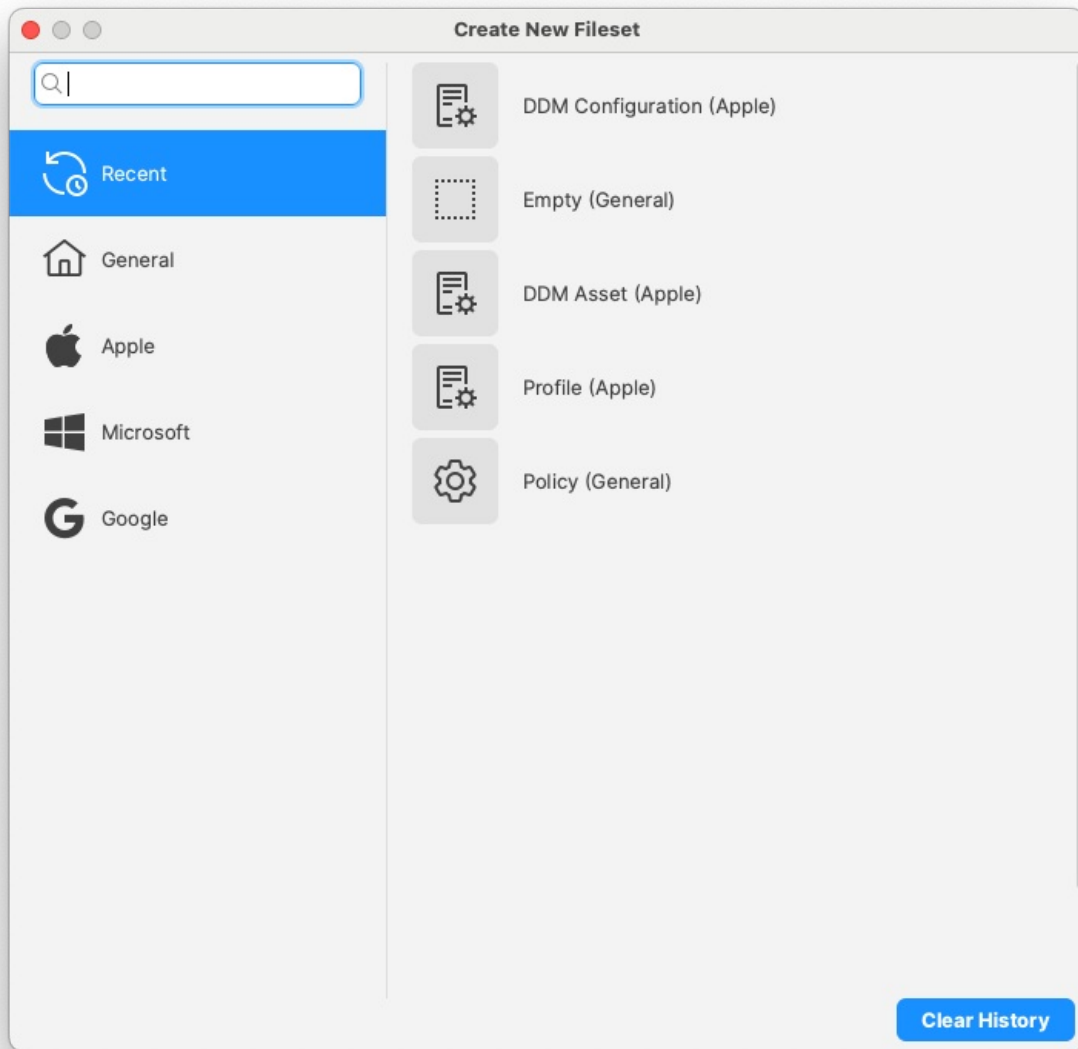
For instance, in this case, the fileset was directly associated to a (Smart Group) "All Windows Clients" containing the client, but there is another association between another client group ("All Windows") and the fileset group ("All Windows Devices") containing the fileset. Pressing "space" key (or using context menu) reveals the list of associations.

From there, you can quickly reveal corresponding association - if you double click on the association.

VLC 3.0.18×64 MSI KIOSK	50293382	<default> (Initial Revision)	50293382

Association ID	Clients or Groups	Filesets or Groups
50022904	**All Windows Clients** / AE-106JHX3-3340	All Windows Devices / **VLC 3.0.18×64 MSI KIOSK**
747828	**All Windows** / AE-106JHX3-3340	**All Windows Devices** / VLC 3.0.18×64 MSI KIOSK

Recent Filesets (Central)

New Fileset dialog, which has been revisited with FileWave 15.5, now shows the last 5 recently created fileset types, providing a smoother user experience.

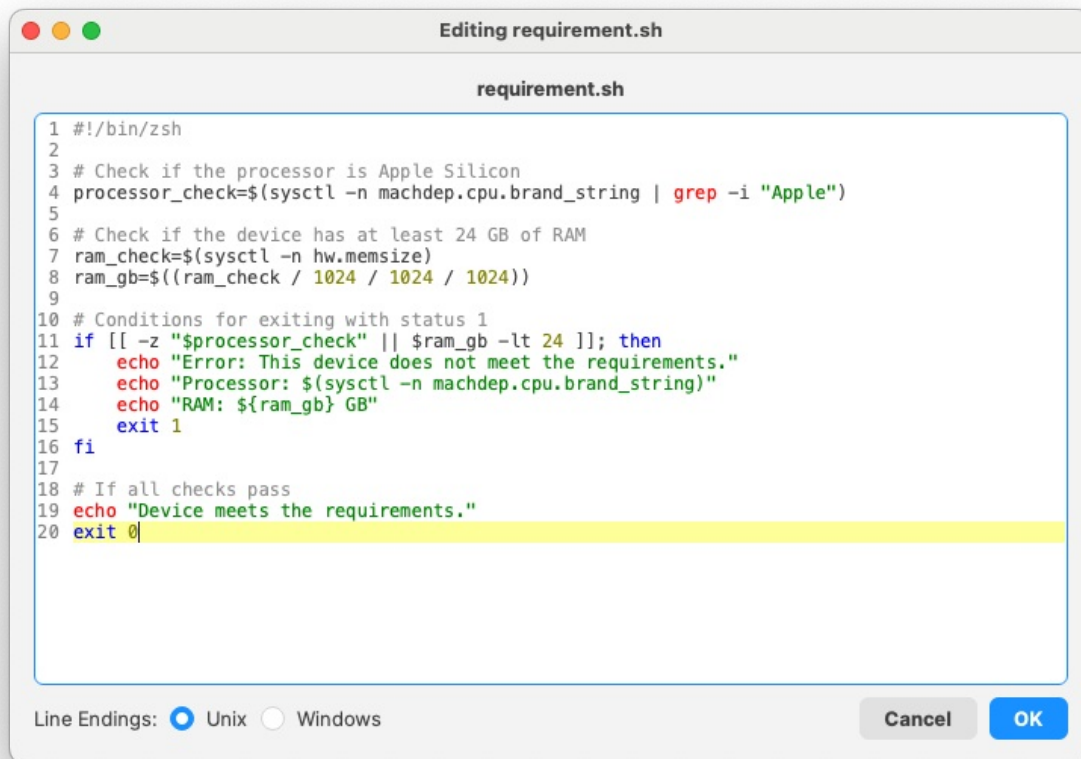## Submit feedback (Central/Anywhere)

If you have anything to suggest us, use the new "Submit Feedback" option in Central and Anywhere Help menus so that you no longer need to login to the KB to access it.

Client Info - Tools Menu (Central)

All relevant options available when you perform right-click on a client in the main client view are now available in the Tools menu option of Client Info dialog.

Script syntax highlighting and line numbers (Central)

Central script editor now features line number and syntax highlighting:

requirement.sh

```zsh
1  #!/bin/zsh
2
3  # Check if the processor is Apple Silicon
4  processor_check=$(sysctl -n machdep.cpu.brand_string | grep -i "Apple")
5
6  # Check if the device has at least 24 GB of RAM
7  ram_check=$(sysctl -n hw.memsize)
8  ram_gb=$((ram_check / 1024 / 1024 / 1024))
9
10 # Conditions for exiting with status 1
11 if [[ -z "$processor_check" || $ram_gb -lt 24 ]]; then
12     echo "Error: This device does not meet the requirements."
13     echo "Processor: $(sysctl -n machdep.cpu.brand_string)"
14     echo "RAM: ${ram_gb} GB"
15     exit 1
16 fi
17
18 # If all checks pass
19 echo "Device meets the requirements."
20 exit 0
```

Line Endings: ● Unix   ○ Windows   Cancel   OK

FileWave desktop client (fwcld) configuration change

Starting with FileWave 16.0, fwcld will periodically check if it's configuration (file or registry) has been changed by an external process, allowing more flexible, dynamic and automated configurations.

▼ Inventory-Specific Changes

Default revision (Fileset)

Default revision flag has been added to the Fileset Revision model.

Profile Display Name and Application Bundle ID in MDM Command history

FileWave 15.5.0 introduced MDM command history in Inventory. Applications were linked using an internal "applink id", and profiles would use the profile UUID. 16.0 adds Bundle Identifier for applications and Profile Display Name for profiles, making reporting much easier.

Last time FileWave Agent connected to FileWave fwxserver

To help troubleshoot device management issues, the last time the agent (fwcld) contacted server (fwxserver) is now in Inventory, allowing reports for devices having connectivity issues. The new field is called "Last Connected To fwxserver" and shows the date and time of the last connection.

▼ Apple-Specific Changes

VPP licenses in Client Info

VPP licenses consumed by a device (for both user and device based licenses) are now listed in client info.

ATHMOB028 - iOS Client Info

ATHMOB028

Device Name: ATHMOB028
Device Type: iPad
Last Connected: 16/11/2024 06:10
iOS Version: 18.0.1
Enrollment Type: DEP Enrollment

| Export Current Tab | Execute Verify | Tools ⌄ |

Filesets Status | Device Details | Command History | Managed Apps | Installed Apps | **VPP Licenses** | Managed Documents | Installed Profiles | Managed Certificates | Installed Certificates | Position Map | DDM Declarations

🔍 Search VPP Licenses

iTunes App Identifier ⌄	Product Name	Product Version	Bundle Identifier	Developer	Assignment Time	License type
901148186	C3 App		com.icomettechnologies.C3	i-Comet Technologies, Inc.	15/08/2024 17:20	Device
881513062	SkyCoach	16.1.0	com.Synapse.SkyCoach	SkyCoach, LLC	15/08/2024 17:20	Device
661649585	TeamViewer QuickSupport	15.60.1	com.teamviewer.teamviewerQS	TeamViewer Germany GmbH	15/08/2024 17:20	Device
535886823	Google Chrome	131.0.6778.103	com.google.chrome.ios	Google	15/08/2024 17:20	Device
507874739	Google Drive	4.2447.11801	com.google.Drive	Google	18/09/2024 15:12	Device
412223222	Hudl	7.19.0	com.hudl.modi	Agile Sports Technologies, Inc.	15/08/2024 17:20	Device
377672876	Scanner App: Genius Scan	7.23.1	com.geniussoftware.GeniusScan	The Grizzly Labs	15/08/2024 17:20	Device
1582121124	Vivi User App	3.9.0	io.vivi.app	Vivi Australia	15/08/2024 17:20	Device
1579070294	Rank One	2.7.8	com.rankone.r1	AllPlayers Network, Inc.	15/08/2024 17:20	Device
1282518969	Cisco Security Connector	1.7.2	com.cisco.ciscosecurity.app	Cisco	15/08/2024 17:20	Device
1191272202	Incident IQ	3.9.4	com.incidentiq.mobile	Incident IQ, LLC	15/08/2024 17:20	Device

Device Declarative Management

DDM configurations are not categorized depending on the device support.

The following new DDM configurations are now supported

Accounts:

- CardDAV:
  Use the Contacts configuration to provide account settings for connecting to the CardDAV-compliant server.

  Contacts declarative configuration for Apple devices 🔲

Apple DDM Configuration Editor

🔍 Search

📋 **General**
Mandatory

📋 **Account: CardDAV**
1 payload(s) configured.

Account: CardDAV

Apple Platform Deployment guide

Account name
The name that apps show to the user for this contact's account. If not present, the system generates a suitable default.
[optional]

Credentials
The credentials for this account.
No Asset is configured ⇕   Create New

Hostname
The hostname or IP address of the CardDAV server.
card.server.net

Port
The port number for the CardDAV server.
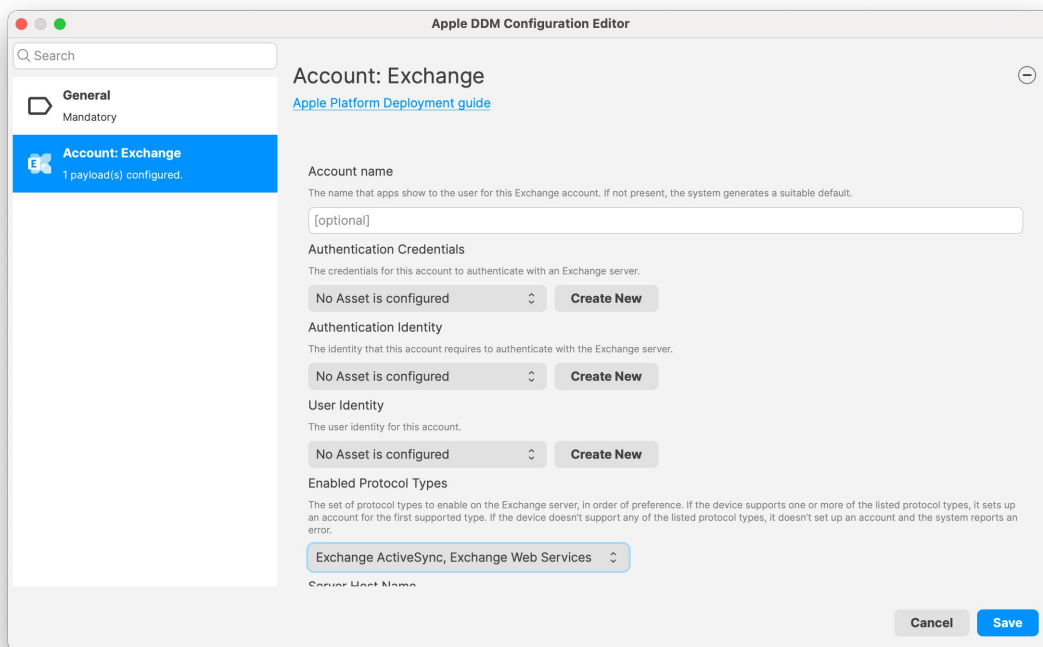Not set ⇕

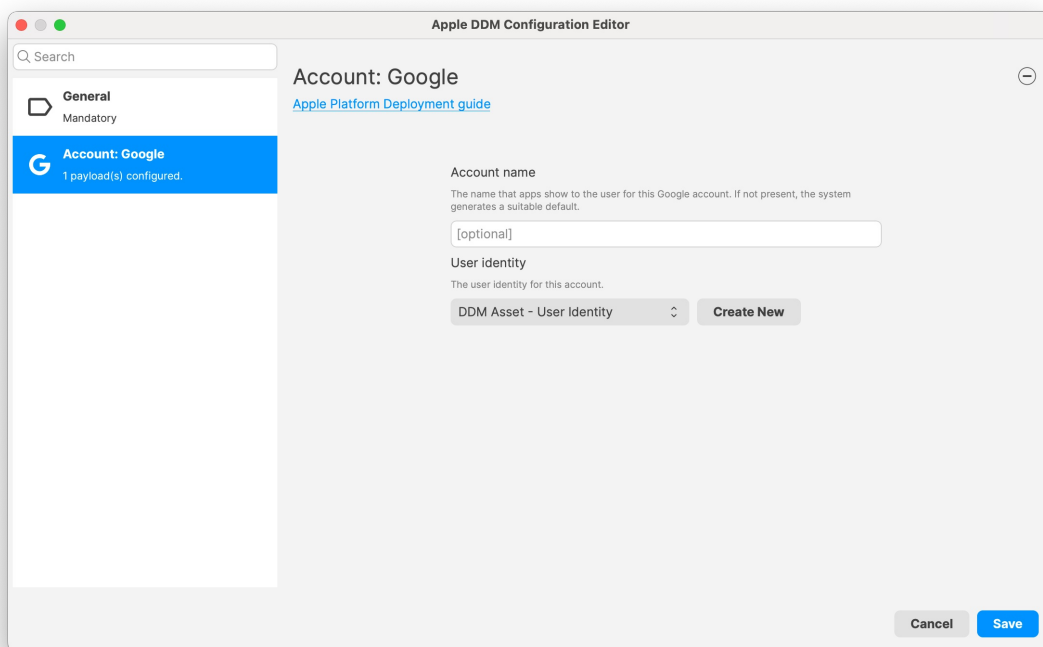**Path**
The path for the CardDAV server.
[optional]

Cancel   **Save**

- Exchange:
  Use the Exchange configuration to set up Exchange ActiveSync (EAS) and Exchange Web Services (EWS) accounts for your users. In iOS 14 and iPadOS 14 or later, Exchange accounts configured for OAuth and Microsoft cloud-based services (such as Office365 or outlook.com) are automatically upgraded to use Microsoft's OAuth 2.0 authentication service. Exchange declarative configuration for Apple devices 🔲

- Google:
  Use the Google Accounts configuration to specify settings for a Google account.

  Google Accounts declarative configuration for Apple devices

- LDAP:
  Use the LDAP configuration to enter settings for connecting to an LDAPv3 directory.

  LDAP declarative configuration for Apple devices

- Mail:
  Use the Mail configuration to configure POP or IMAP mail accounts for users. Apple devices support industry-standard IMAP4 and POP3 mail solutions on a range of server platforms, including macOS, Windows, UNIX and Linux.
  Mail declarative configuration for Apple devices

- Subscribed Calendars:
  Use the Subscribed Calendars configuration to add read-only calendar subscriptions to the Calendar app.
  Subscribed Calendars declarative configuration for Apple devices

Apple DDM Configuration Editor

Account: Subscribed Calendar

Apple Platform Deployment guide

Account name

The name that apps show to the user for this calendar account. If not present, the system generates a suitable default.

[optional]

Calendar URL

The URL of the subscribed calendar.

https://calendar.server.net

Authentication credentials

The credentials for this account to authenticate with a calendar server.
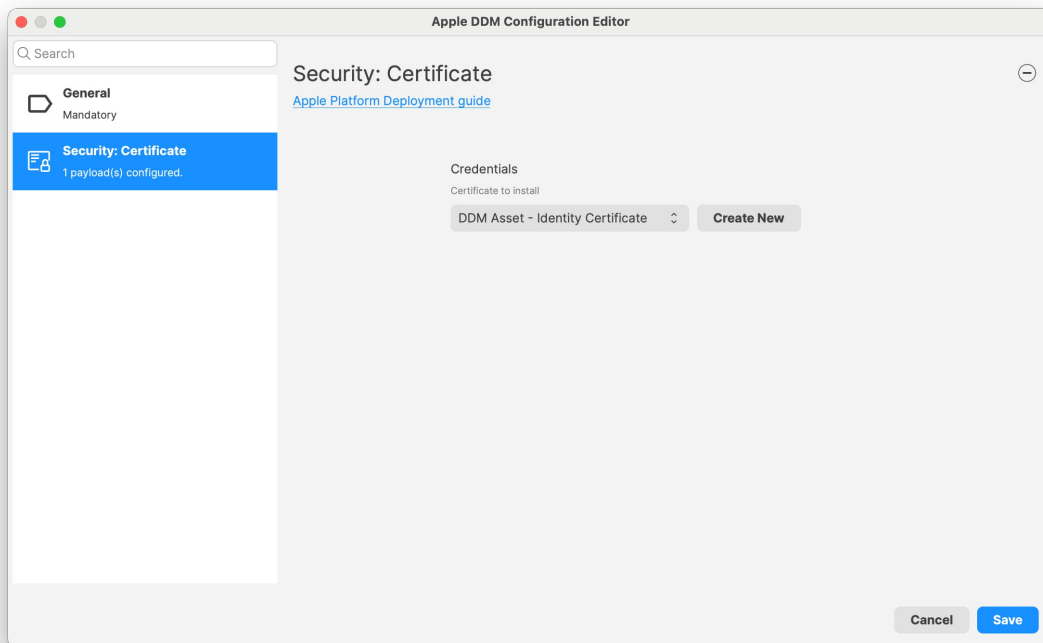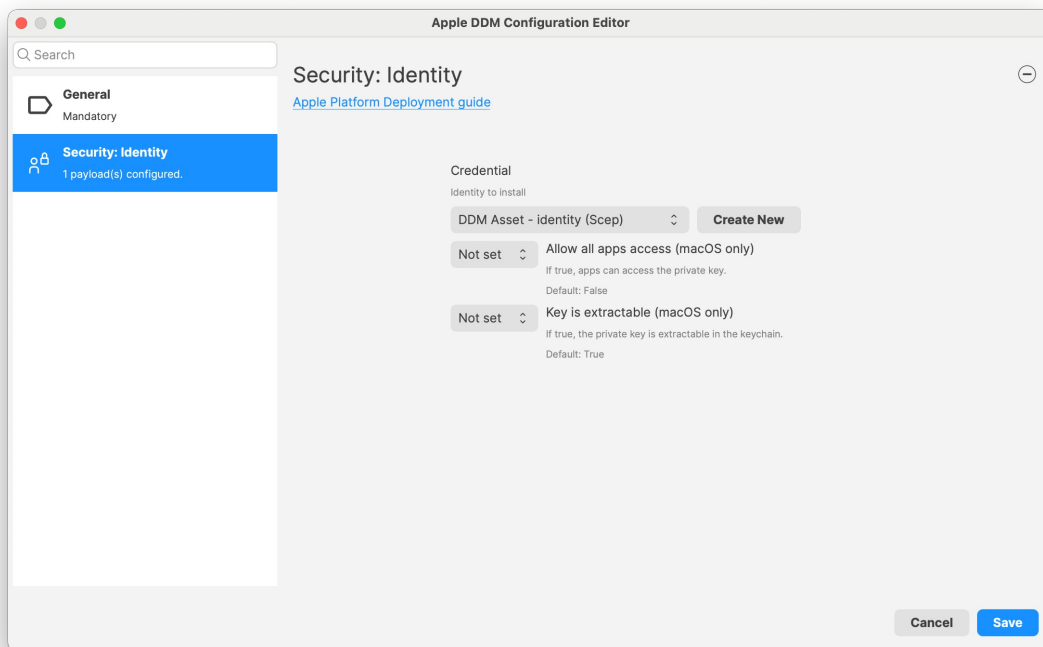
DDM Asset - creds   Create New

Cancel   Save

Security:

- Certificate:
  Use the Certificates configuration to deploy certificates and identities. If the certificate is a self-signed Certificate Authority (CA), it's automatically added to the device's trusted root certificates.
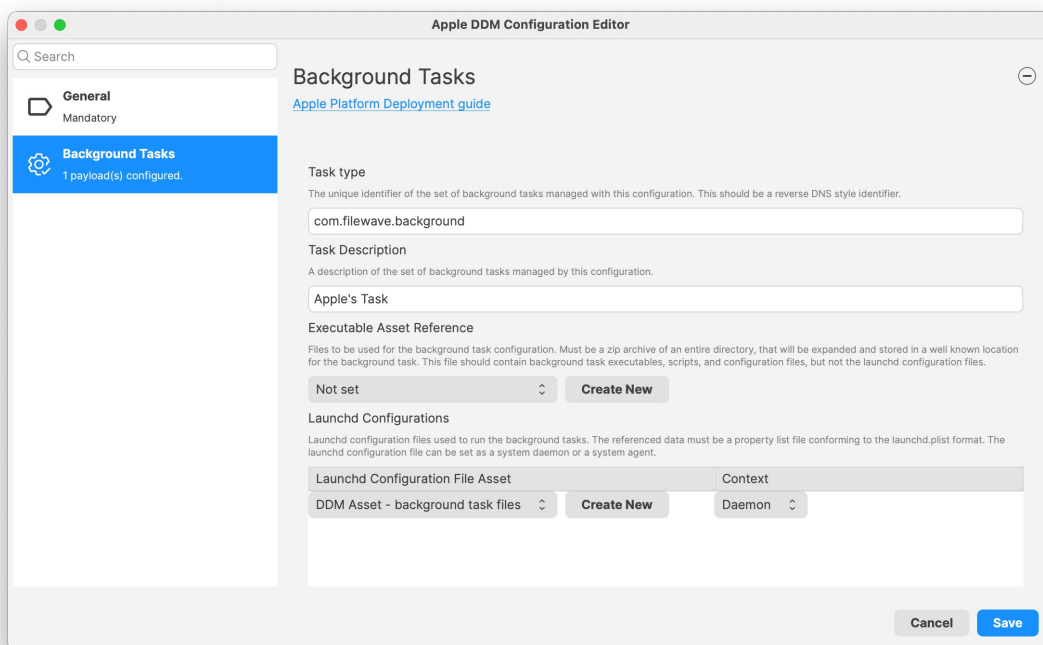 Certificates declarative configuration for Apple devices

Apple DDM Configuration Editor

Security: Certificate

Apple Platform Deployment guide

Credentials

Certificate to install

DDM Asset - Identity Certificate   Create New

Cancel   Save

- Identity:

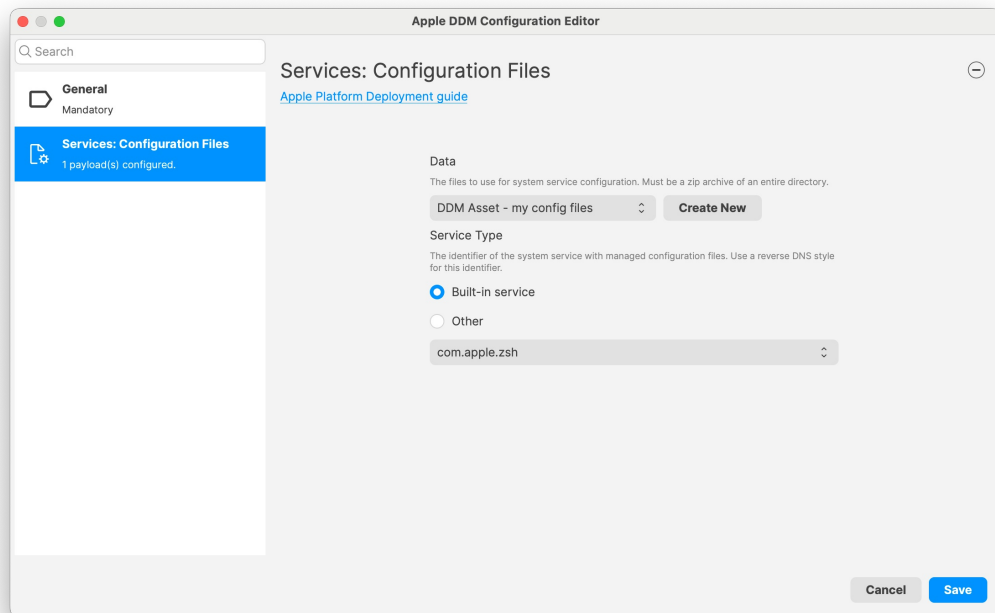Security Configuration can use ACME, Identity (certificate) and SCEP asset.

Services:

- Background Tasks:
  macOS includes support for background tasks that either start on behalf of the user or run as a standalone process to provide persistent services in the background.
  In macOS 15 or later, executables, scripts and launchd configuration files can be installed using MDM and are stored in a secure and tamper-resistant location (similar to service configuration files introduced last year), providing an easy way for organisations to deploy and control managed services.
  Background task management declarative configuration for Apple devices
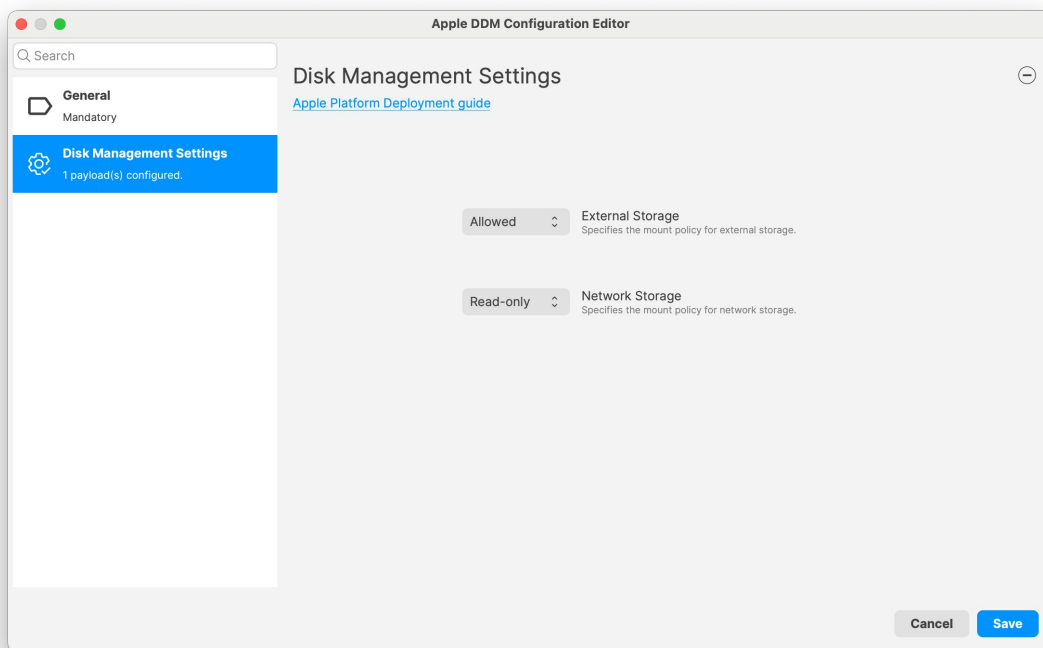

- Configuration Files:
  Use the Service configuration files configuration to provide managed settings for common system services in a robust and tamper-resistant way. When the configuration is activated, the archive is downloaded and expanded into a special tamper-proof, service-specific location. The service-specific location can be found by calling a function in a public library, so that any service can adopt managed service configuration files. The following built-in services are modified to look for the managed service configuration files, which take precedence over built-in settings:
  - `sshd`
  - `sudo`

- ○ `PAM`
- ○ `CUPS`
- ○ `Apache`
- ○ `zsh (/private/etc/zprofile)`
- ○ `bash (/private/etc/profile)`

Service configuration files declarative configuration for Apple devices

- Disk Management:
  Use the Storage management configuration to limit access to storage on a Mac.
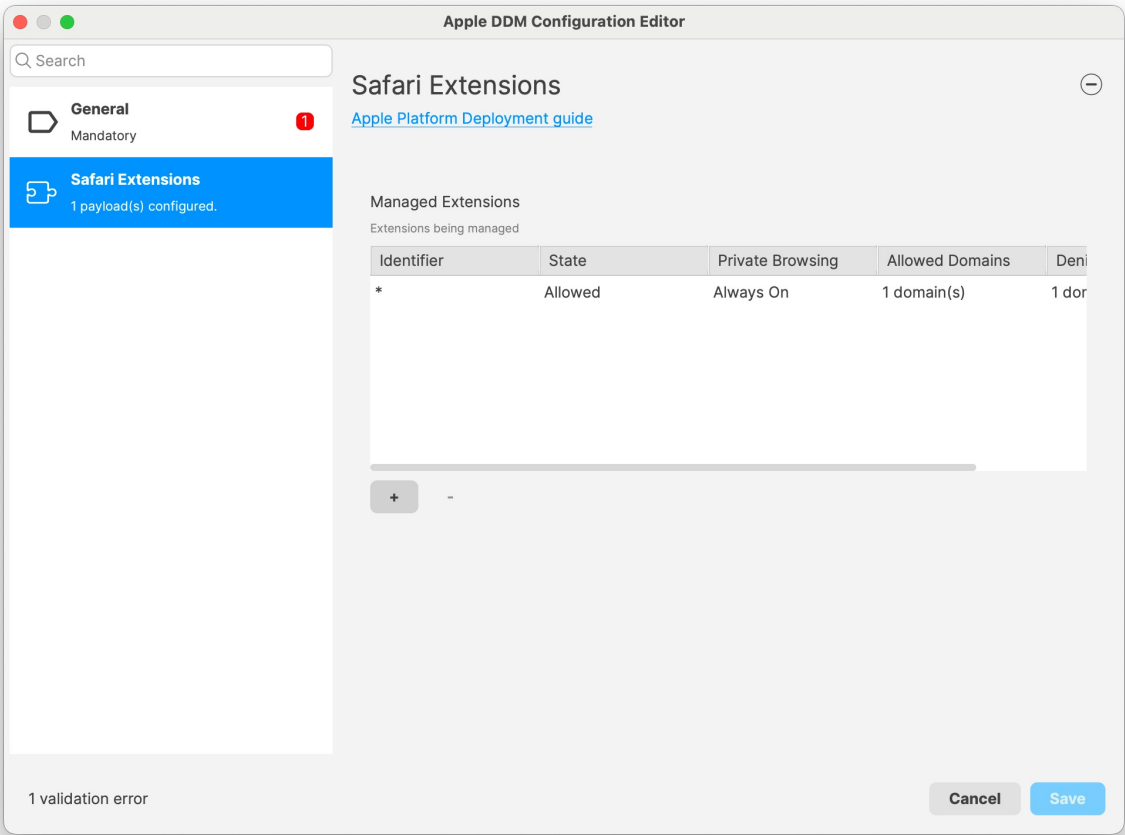 Storage management declarative configuration for Apple devices
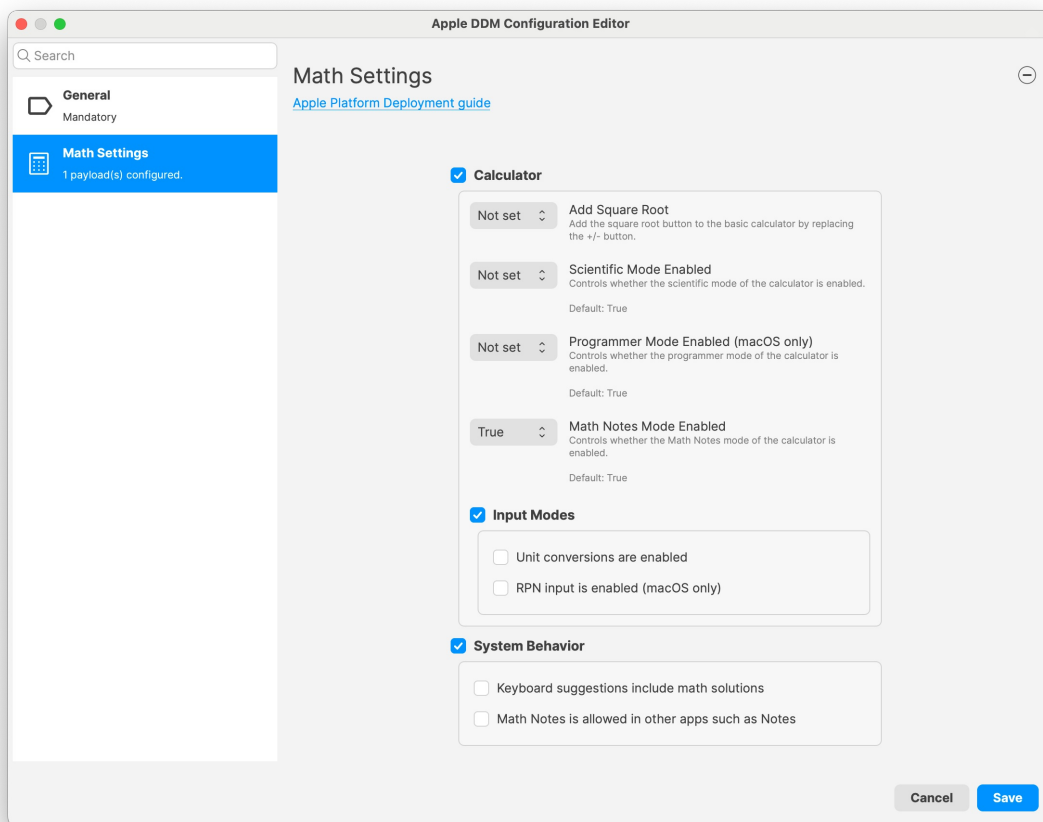

System:

- Safari extensions:
  Use the Safari extensions management configuration to provide management of Safari extensions management on iPhone, iPad and Mac devices enrolled in a mobile device management (MDM) solution.
  Safari extensions enhance and customise the web browsing experience on iPhone, iPad and Mac. In iOS 18, iPadOS 18, macOS 15, or later, organisations can now use MDM solutions to manage how Safari extensions are used on supervised devices. For example, a business may want specific extensions installed and turned on to provide access to internal services, or an educational institution may want to prevent students using extensions that provide information that goes against school policy. These extension management features work for standard browsing and Private Browsing, and include:
  - ○ Defining which extensions are allowed

- Controlling which extensions are always on or always off
- Configuring an extension to access websites by specific domains and subdomains

Safari extensions management declarative configuration for Apple devices

Apple DDM Configuration Editor

🔍 Search

General
Mandatory   1

Safari Extensions
1 payload(s) configured.

Safari Extensions
Apple Platform Deployment guide

Managed Extensions
Extensions being managed

Identifier	State	Private Browsing	Allowed Domains	Deni
*	Allowed	Always On	1 domain(s)	1 dor

+   –

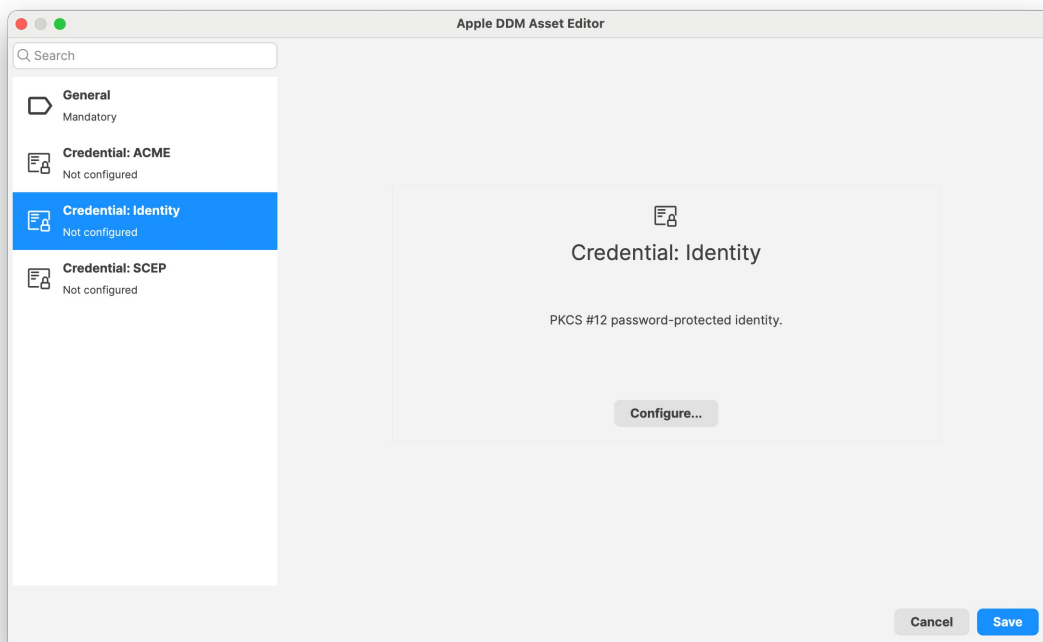1 validation error   Cancel   Save

- Math (Calculator):
  You can configure the built-in Maths and Calculator app settings on iPhone, iPad and Mac devices enrolled in a mobile device management (MDM) solution.

  Maths and Calculator app declarative configuration for Apple devices

Assets:

- ACME, SCEP and plain certificates can be used in configurations:

- When you create a new Asset from a configuration, this new asset is now automatically selected, and the right type of asset is automatically picked when the DDM Asset Editor opens

Status reports:

- Managed certificates are now reported using DDM status mechanism.
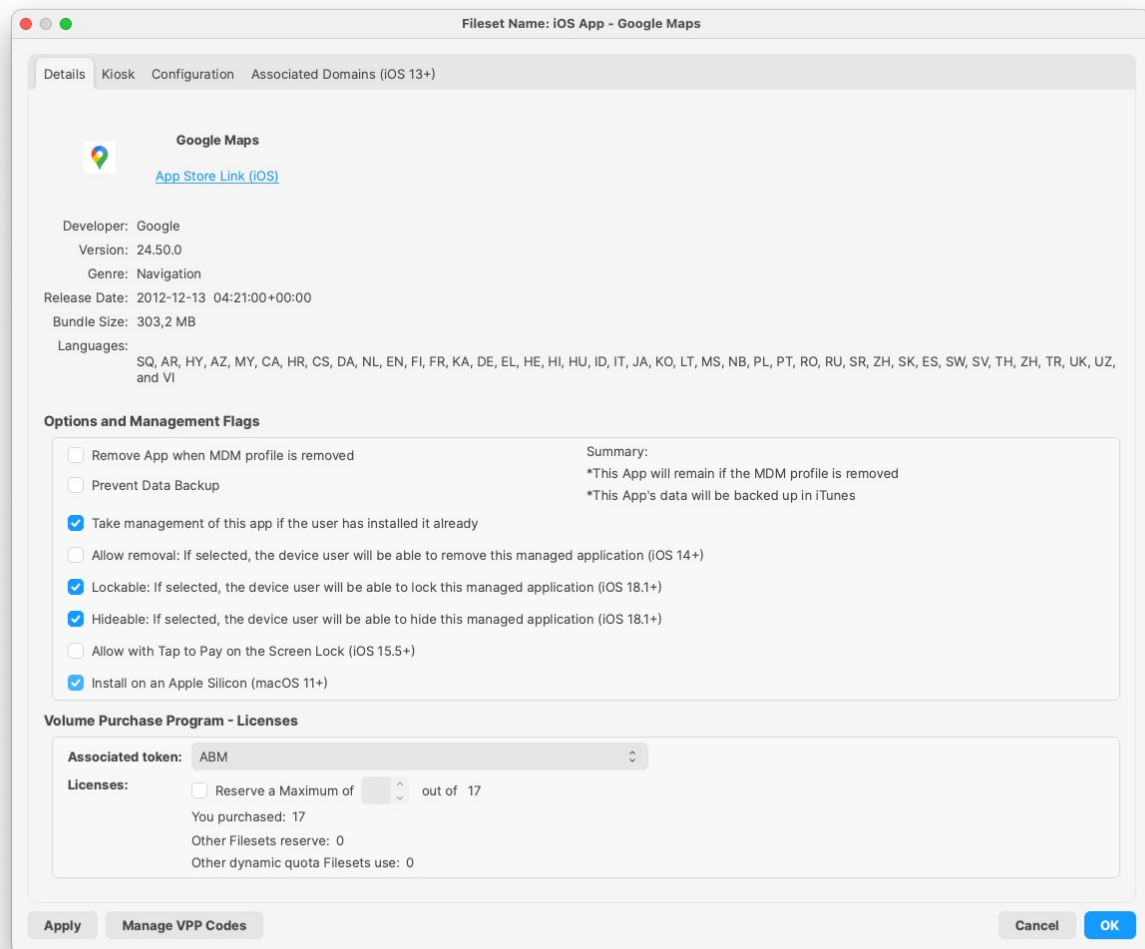
MDM Enhancements

New DEP skip keys (and corresponding Setup Assistant profile):

- Camera Control

Delete All Users feature (shared iPad) now uses MDM option instead of deleting users one by one

Hide-able and Lock-able apps

It is now possible to define if end user can hide and lock managed applications on iOS 18.1 and later:

New restrictions

- Use the new allowDefaultBrowserModification Restriction key to prevent users from modifying the default browser.
- You control when ChatGPT is used and will be asked before any of your information is shared. Anyone can access ChatGPT for free, without creating an account. ChatGPT subscribers can connect accounts to access paid features within these experiences. MDM can disable ChatGPT integration with the allowExternalIntelligenceIntegrations restriction.
- One can use the allowedExternalIntelligenceWorkspaceIDs restriction key with an array containing a single workspace ID to require sign in for requests to external intelligence integrations like ChatGPT
- Allow external intelligence integrations sign-in using allowExternalIntelligenceIntegrationsSignIn
- Transcription summarization in Notes can be configured with the allowNotesTranscriptionSummary restriction

Managed domains

CrossSiteTrackingPreventionRelaxedApps support has been added to allow configuring apps which will have relaxed enforcement of cross-site tracking prevention for the domains listed in the 'CrossSiteTrackingPreventionRelaxedDomains' key.
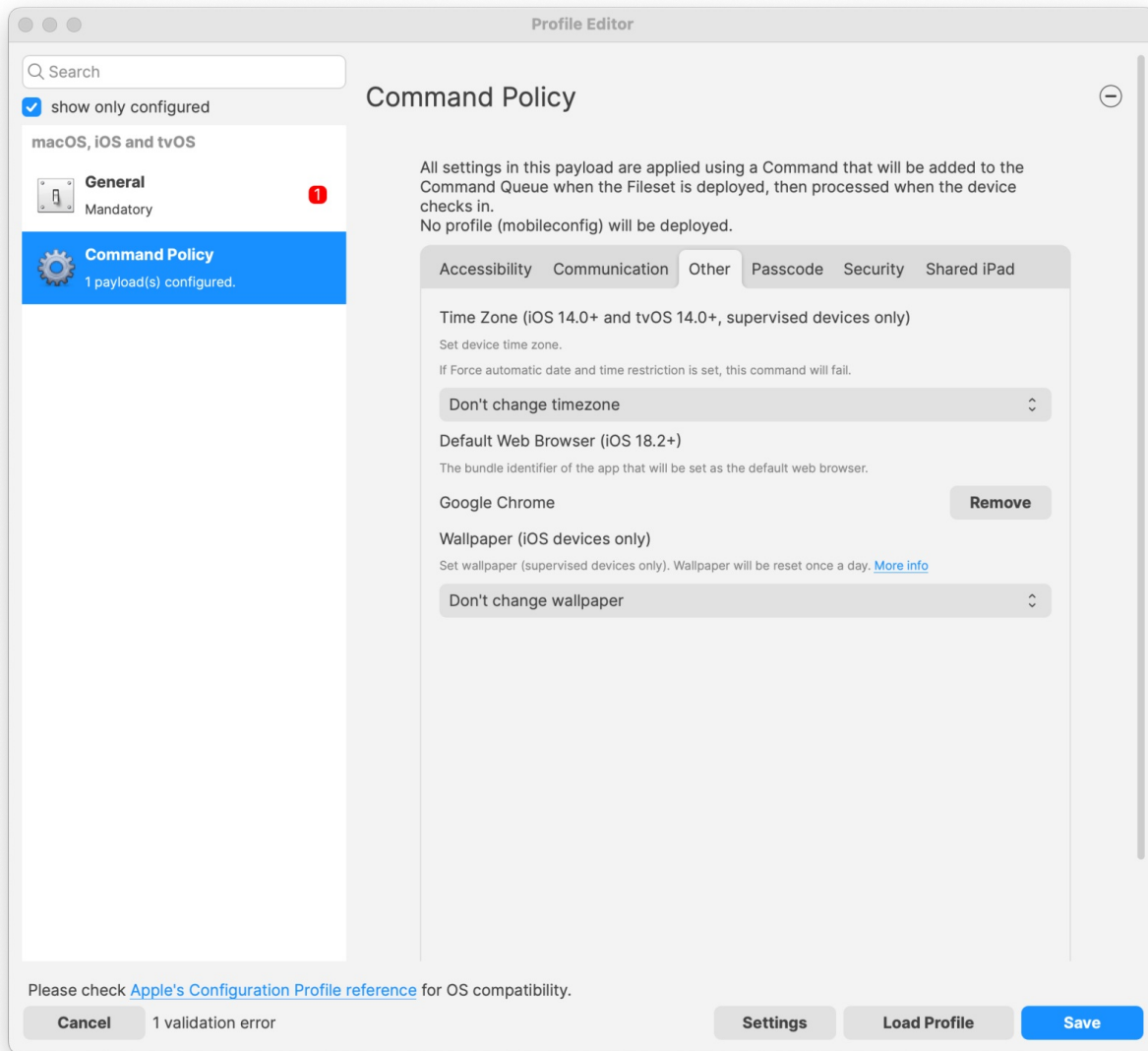
Full Disk Encryption

Exporting FDE keys now requires to re-enter admin password and will be logged in Audit Log.

Activation Lock

Removing activation lock requires IMEI to be provided for SIM-enabled devices, but fails if IMEI contains spaces. FileWave 16.0 makes sure IMEI is properly formatted even if the device reports IMEI with spaces

Default Applications

Starting with iOS 18.2, it is possible to define default applications on the device. For now, only browsers can be configured, using Command Policy profile:

Certificates

Installed certificates are now reported in inventory and visible in Client Information for MDM enrolled devices.
DDM capable devices also provide details about managed certificates.

SSO Kerberos Extension

Single-Sign-On Extensions profile allows configuring Kerberos Extension. FileWave 16.0 replaces the generic PList editor with a complete User Interface to define Kerberos settings.

Packaging

The content of macOS packages has been optimized. Client and Admin packages are much smaller.

▼ Chromebook-Specific Changes

Chrome Extension

Introduced in 15.5 but including as a reminder; New version of the Extension is needed for Notifications to function properly and also contains several issues fixed. The extension should have automatically updated on clients.

Chrome Management in FileWave Anywhere

Introduced in 15.5 but including as a reminder; Verify option became available in FileWave Anywhere for single and bulk devices action. It is also supported as a bulk action for different platforms (i.e mac and chrome). Note: "Modify Chromebook" permission is not needed to preform Verify action.

▼ Android-Specific Changes

Android Lost Mode

Introduced in 15.5 but including as a reminder; EMM devices which are in "Missing" device state will now use Android Lost Mode mechanism. As Android Lost mode allows the end user to exit lost mode by entering device passcode, FileWave will then report in inventory the current state and the expected state. It is also possible to "Play Lost Mode Alert" on lost devices.

▼ Windows-Specific Changes
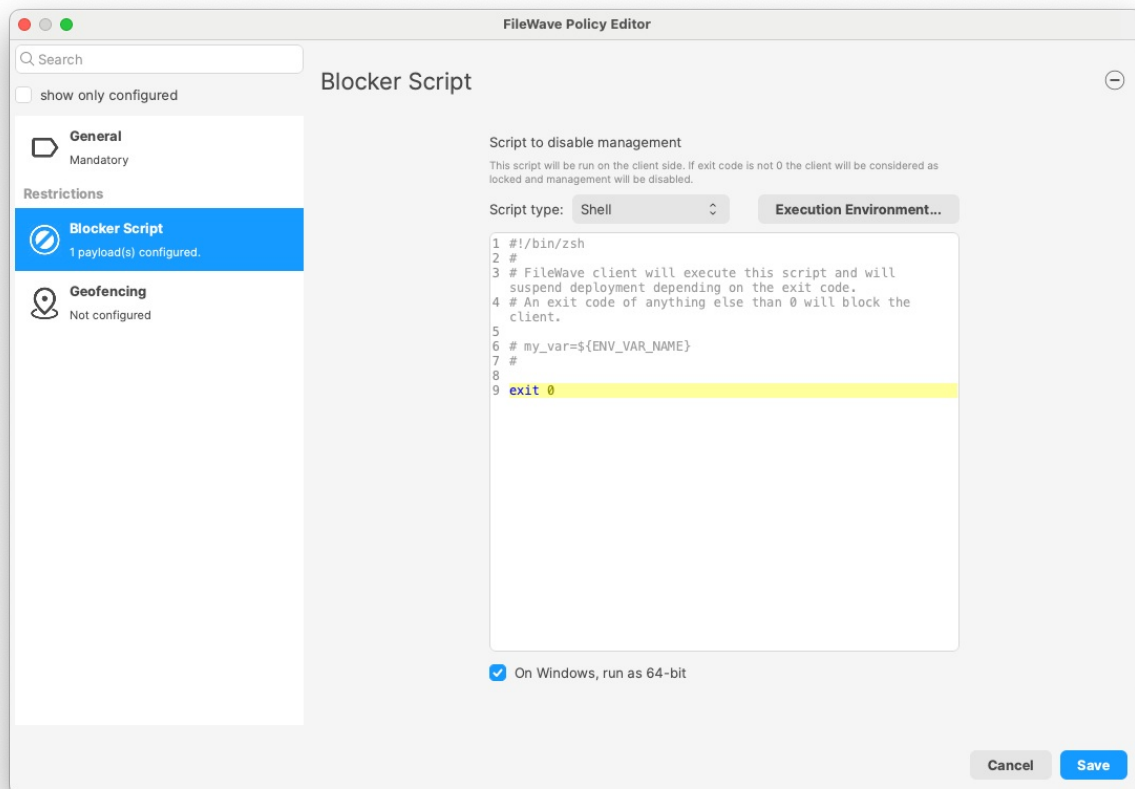
Software Update (Central)

Software Update management has been revisited for FileWave 16.0. Specifically for Windows:
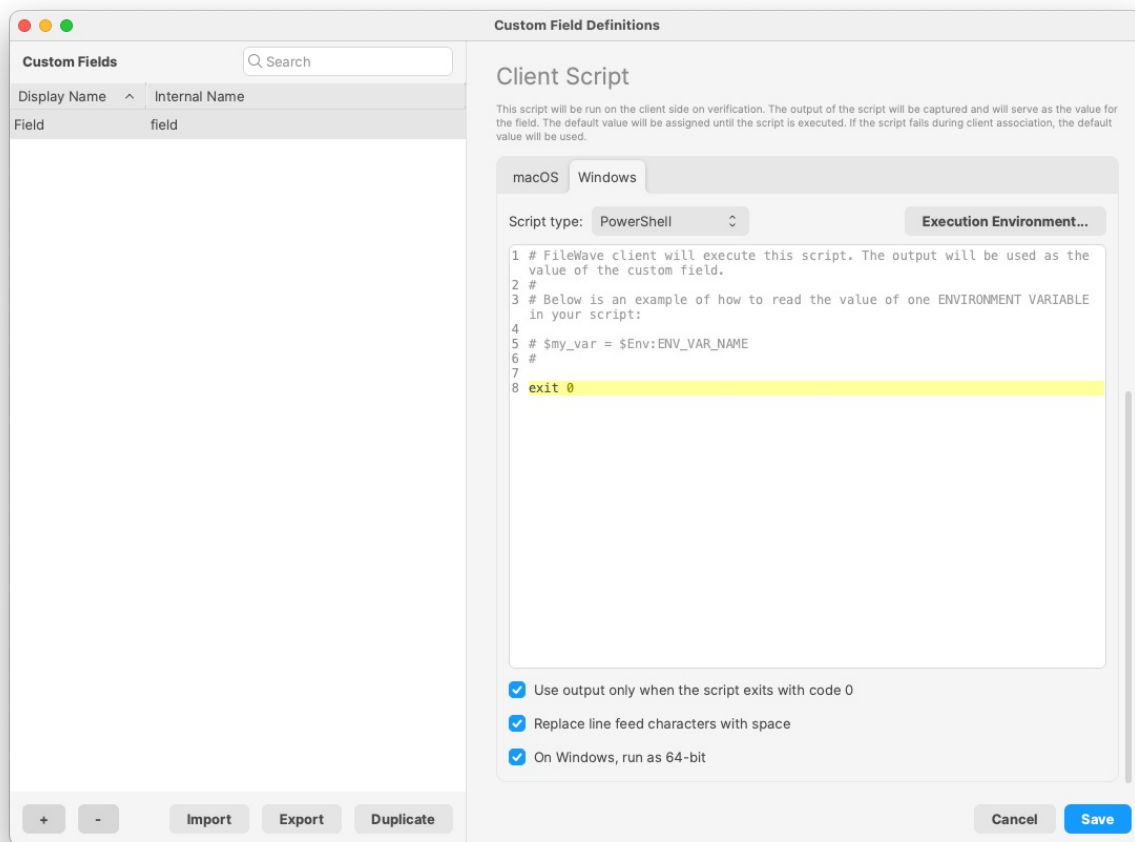
- Windows Updates are now relying on managed devices reporting what they need rather than the offline catalog. This removes the need for parsing offline catalog, which was resource consuming and due to Microsoft limitations not covering all existing updates.
- Updates are downloaded directly from Microsoft and installed using Microsoft Update tools, which allows support for an increased number of update types.
- Updates themselves are not imported in FileWave server (only metadata), which speeds up the process. Clients and Boosters download updates directly from Microsoft CDNs. FileWave boosters can be used to cache updates to avoid Network load and use a new port on the Boosters.
- FileWave Client is not stuck anymore if Windows Update Service is hanging on the device.
- On Windows, update installation history is now made available, even for updates not installed via FileWave.

> ⊘ Action Required: Pre-v16 Windows OS Update Filesets will not function and should be purged from your system to free up space.

64-bit script execution

Starting with FileWave 15.5, Windows agent (fwcld) is a 64-bit application. As former versions were 32-bit applications, script execution may run in a different context (pure 64-bit or 32-bit-on-64-bit). To simplify migration from FileWave 15.4, a new option has been added to Fileset scripts to define the context. This option is now available for Policy / Blocker Script and for Custom Field:

Client upgrade Fileset improvements

- Improved upgrade process when New kiosk process is running
- Added a step to backup and restore client configuration to ensure configuration is not lost during upgrade process

▼ 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.

- The list of modules and packages embedded with IVS 16.0 has been entirely revisited and supports a much broader set of hardware.
- IVS 16.0 fixes an issue which could prevent restoring images on disk using a different sector size than 512 B.
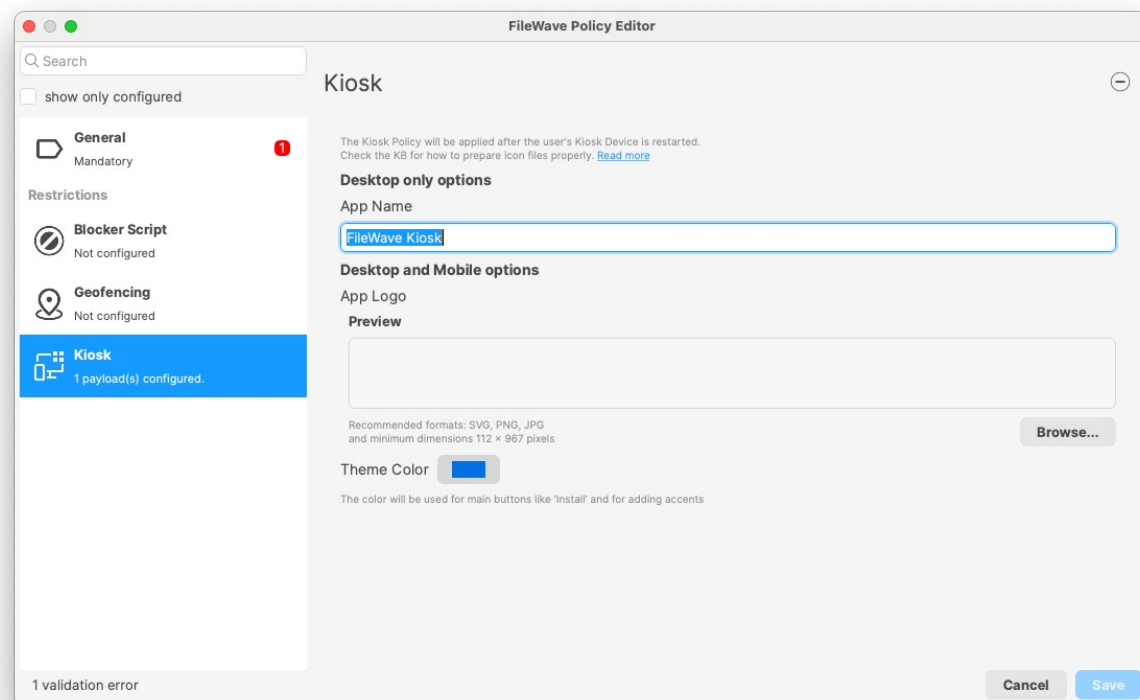
FileWave Networking Imaging 16.0.3 brings compatibility with FileWave 16.0.x.

- Linux Kernel: 6.12.4
- Buildroot: 2024.11

▼ FileWave Kiosk Changes

Kiosk customization as FileWave Policy (Central/Anywhere)

Kiosk customizations are now integrated as FileWave Policy, allowing simplified group deployment.

Removal of Legacy Kiosk UI

- The old Kiosk UI has been removed from Mac and Windows clients after three stable releases of the new Kiosk UI.
- Geolocation functionality remains unchanged.
- Reboot modals continue to function on both Mac and Windows in the old style.
- TeamViewer sessions are unaffected and continue to work on both Mac and Windows platforms.
- Note: This update eliminates duplicate tray icons by removing the old `fwGUI` tray icon.

New "Missing Device" Message in Kiosk for macOS and Windows

- When a macOS or Windows client is marked as "Missing" in FileWave Admin, a "Missing Device" message will now be displayed in the Kiosk, similar to the "Device Locked" message.
- The "Missing Device" message will include any custom Lost Mode Message and Lost Mode Footnote set in Central Admin under Organization Info.
- By default, if no custom message is set, the following message appears: "This device is currently marked as missing. Self-service Kiosk is not available. Please contact your administrator."
- Kiosk Restrictions: While in the "Missing" state, the Kiosk will prevent installation, uninstallation, and normal access to self-service options, similar to "Device Lock" functionality.
- Additional Information:
  - If only the Lost Mode Message is set, it will display alone.
  - If only the Lost Mode Footnote is set, the default lost mode message will appear with the custom footnote.
  - If an organization contact number is set, it will be displayed as a clickable link for easy access.

▼ Internal Changes

Third party libraries

Third-party libraries updated for improvements and security changes. Mainly:

- Postgres has been upgraded to 17

> ⚠ Upgrading Database engine requires upgrading Database data, which can take some time.
> Be patient when upgrading to FileWave 16.0

- Qt has been upgraded to 6.8
- Qlementine has been upgraded to 1.0.0
- Python has been upgraded to 3.13
- OpenSSL has been upgraded to 3.4.0

Dashboard

FileWave is now using more secure Service Account mechanism to connect to Grafana (Dashboard).

Desktop client communication

FileWave desktop agent (fwcld) is now capable of downloading fileset manifests using faster NATs communication channels, which decreases the resource load on boosters and servers while providing faster delivery.

▼ Deprecated Features

The following features have been deprecated from FileWave 16.0. They are present but will be removed in a future release:

- FileWave Central Dashboard: The Dashboard in FileWave Central will be replaced by a view of a Grafana Dashboard to not maintain 2 Dashboard systems.
- Client Monitor application: The standalone Client Monitor will be removed in a future release because it is only used for FileWave Clients < 16.0.0 as well as monitoring the IVS server. It will be included at least until the IVS dependency is removed.
- macOS 10.11 El Capitan: Released in September 2015, this version of macOS will not work with even a legacy client when FileWave 16.1.0 releases in the summer of 2025 due to an incompatibility with a current version of OpenSSL.

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 16.0.

▼ Decommissioned Features

The following features have been removed from FileWave 16.0:

- The concept of Automatic Deployments of Software Updates no longer exists but future changes will add this concept back in differently.

- Removal of Legacy Kiosk UI

  - The old Kiosk UI has been removed from Mac and Windows clients after three stable releases of the new Kiosk UI.
  - Geolocation functionality remains unchanged.
  - Reboot modals continue to function on both Mac and Windows in the old style.
  - TeamViewer sessions are unaffected and continue to work on both Mac and Windows platforms.
  - Note: This update eliminates duplicate tray icons by removing the old `fwGUI` tray icon.

The following features were removed from FileWave 15.5.0 and are worth mentioning again due to being major changes:

- Windows 32-bit - With FileWave 15.5, the FileWave Client, Boosters, and Admin are 64-bit only now.
- While it was not possible to create new MCX (Workgroup Manager) Fileset since FileWave 7.0, it was still possible to import and edit MCX configurations from 2013 and before. As MCX and Workgroup Manager has been made deprecated by Apple for 10 years, support has been removed from FileWave 15.5.

The following features were removed from FileWave 15.4.0 and are worth mentioning again due to being major changes:

- CentOS - As CentOS 7 being End-Of-Life on June 30, 2024, FileWave is available and supported on Debian. New versions of FileWave won't be released on CentOS after CentOS is EOL.

▼ Security Notices

The following security notices are relevant to this release:

- Fixed vulnerability WITH-ZD-2025-0001, reported by Withsecure Exposure Management (https://www.withsecure.com/). In non-default custom configurations, FileWave Windows clients (v15.5.2 and earlier) allowed local, non-privileged users to escalate privileges to SYSTEM. This issue is resolved in FileWave v16.0.0; a CVE was issued of CVE-2025-43922 on April 20, 2025.

Changes and Fixes in 16.0.3

▼ Changes and Fixes in 16.0.3

Bug fixes:

- FWRD-14859 Fixed an issue where it would not be possible to delete a deployment if all filesets or all clients used in this deployment are deleted
- FWRD-15272 Fixed an issue where MDM communication could break on non-DEP macOS at enrollment time, related to MDM tokens management
- FWRD-15283 Fixed an issue where buttons with drop down like "Tools" would not activate selected action
- FWRD-15325 Kiosk Information page is not loading on Windows
- FWRD-15355 Fixed an issue where Central Admin could crash if current administrator would lose permission when Edit Deployment dialog is opened
- FWRD-15371 Fixed an issue where Superprefs Editor would not show open dialog or save file Finder dialogs on macOS

15.4 or later

- FWRD-15374 Fixed an issue where restoring Windows Image would not clear pre-installed 64-bit client fingeprint
- FWRD-15385 Fixed an issue where "Last Status date" (shown in When column in client info) would be 0, displayed as January 1st 1970 UTC.
- FWRD-15388 Fixed an issue where incorrect filter would be applied to Open File System dialog preventing from selecting plist files
- FWRD-15397 Fixed an issue where Windows Upgrade fileset couldfail if upgrading from 64-bit custom package

▼ Changes and Fixes in 16.0.2

Bug fixes:

- FWRD-15300 Various improvements related to Fileset Statuses management (at model update, when desktop clients report them), reducing Model Update times for large deployments.
- FWRD-15354 Windows upgrade fileset may hang when restoring configuration

▼ Changes and Fixes in 16.0.1

Bug fixes:

- FWRD-14652 Fixed an issue where VPP Fileset Property dialog could not be closed if 0 licenses would be assigned to the fileset
- FWRD-15158 Ensured Hyper-V Gen2 Appliances have the right disk space
- FWRD-15190 Fixed an issue where script syntax highlighting would be missing when editing files directly from fileset content
- FWRD-15209 Fixed an issue where model update could error after editing fileset with multiple scripts due to file permission issue
- FWRD-15245 Fixed an issue related to DDM "Server Token" which could prevent DDM filesets (including updates) to be delivered properly
- FWRD-15247 Fixed an issue where model update would wait for Chromebook notifications to be sent, leading to longer model update times
- FWRD-15263 Fixed an issue where ignoring irrelevant updates in client info dialog would not work for macOS devices
- FWRD-15273 Fixed a potential Central crash when performing some actions like "Show FDE Recovery Key" from Client Info "Tools" Menu
- FWRD-15281 Fixed an issue where Central admin would not be able to show IDP login screen when requesting account confirmation when IDP is configured for admin login
- FWRD-15282 Fixed an issue where Software Update report data would not be shown in the right column

▼ Changes and Fixes in 16.0.0

Bug fixes:

- FWRD-1296 Fixed an issue where DEP profiles with identical names did not show their unique IDs, making it hard to distinguish which profile to select.
- FWRD-1305 Fixed an issue where the 'ID' column in the DEP Profile table was not displayed by default, making it difficult to differentiate profiles with identical names
- FWRD-1546 Fixed an issue where the backend attempted to translate into unsupported languages (e.g., Russian) instead of defaulting to English, causing partial translations in the Web UI.
- FWRD-1691 Fixed an issue where admins without the 'Configure EMM Enterprise' permission could still see EMM-related buttons, which are now hidden unless the required permission is granted
- FWRD-2088 Fixed an issue where DEP associations would not follow device filtering
- FWRD-3293 Fixed an issue where Android payloads (Google Policy, Play Store app) incorrectly showed 'None' in the Platform column, and now properly display 'Android.'
- FWRD-3299 Fixed an issue where EMM synchronization time in the Web Admin displayed the server's timezone instead of the admin's local timezone
- FWRD-3804 Fixed an issue where synchronizing data with iTunes would not retry in case of networking error
- FWRD-4434 Fixed an issue where status of a dependency fileset could incorrectly be displayed
- FWRD-4634 Fixed an issue where fwcld on IVS would not restart automatically after upgrade
- FWRD-12973 iOS restrictions workaround key is removed in FileWave Anywhere.
- FWRD-13952 Fixed an issue causing the FileWave logo to appear blurry in ChromeOS notification previews; the logo is now displayed with proper clarity.
- FWRD-13968 Fixed an issue where importing fileset may not be able to import properly scripts
- FWRD-13988 Fixed an issue where Audit Log entry would be missing when uploading custom MSI or PKG
- FWRD-14042 Fixed minor UI alignment issue in Fileset Revision dialog (Central)
- FWRD-14091 Fixed an issue where incorrect device could be used when Remote Session actions are started from inventory query results
- FWRD-14134 Made sure disk space is properly checked before upgrading server on Debian
- FWRD-14221 Fixed an issue where Grafana main dashboard would not be able to properly display some services status
- FWRD-14223 Improved "Main services" dashboard
- FWRD-14247 Fixed cosmetic missing "..." on a button in Fileset Magic Wizard
- FWRD-14259 Removed obsolete code that prevented Android EMM devices from receiving notifications in Client Info, ensuring EMM devices can now be notified if permissions allow.=
- FWRD-14297 Fixed an issue where Background location would not be working on Android 14+ devices
- FWRD-14308 Fixed cosmetic UI issue in FileWave Central when an Apple App Store Fileset supports many different languages

- FWRD-14317 Improved performance in code dealing with generating DDM configuration related to Software Update delivery
- FWRD-14338 Fixed an issue where Grafana may not start properly after upgrade
- FWRD-14378 Fixed an issue where some information like model number would not be up to date in Grafana dashboard until next restart
- FWRD-14411 Updated all appliances to Debian 12.8
- FWRD-14495 Fixed an issue where quoted launch arguments could be escaped with when running executables
- FWRD-14507 Fixed an issue where it would not be possible to get script output log file from Central Client Info
- FWRD-14516 Fixed an issue where the macOS Kiosk package contained only Intel binaries, preventing installation on Apple Silicon devices. The package is now universal and supports both architectures
- FWRD-14534 Fixed an issue where the NATS server's public key in the KV store could diverge from the actual certificate, causing client monitor commands to fail until a server restart
- FWRD-14550 Fix an issue where Android Global Proxy policy UI was missing the remove button
- FWRD-14598 Added a locking mechanism for FileWave policy filesets in Central Admin to prevent edits or deletions when another session is already modifying the policy, ensuring consistent concurrency handling
- FWRD-14638 Fixed an issue where 'Items' was incorrectly translated to 'Elementen' in German desktop Kiosk headers instead of 'Elemente.'
- FWRD-14665 Fixed an issue on Windows desktop Kiosk where hovering or clicking the close (x) button on a notification caused a display glitch, instead of simply dismissing the snackbar
- FWRD-14672 Fixed an issue in FileWave Anywhere's condition form where pasting data failed to refresh the preview or load correct results, now properly updating when users paste input
- FWRD-14674 Fixed an issue where it would be possible to create multiple DDM configurations using search feature
- FWRD-14702 Fixed an issue where search in DDM configuration could trigger useless calls to fwxserver
- FWRD-14706 Fixed an issue where dialog asking for current admin password when uploading SSL certificate would miss instructions
- FWRD-14721 Fixed an issue where DDM Software Update configuration scope could be set to user
- FWRD-14733 Fixed possible Central crash when removing Custom Settings payload if PList would be being edited
- FWRD-14748 Fixed an issue where macOS upgrade filesets could not properly deploy to requesting devices
- FWRD-14772 Fixed missing /run/lock folder in IVS PXE image, causing misleading error message regarding to sshd
- FWRD-14789 Fixed an issue where Imaging restoration may fail if disk sector size is not 512 and Windows partition can be enlarged, using GPT format
- FWRD-14802 Fixed a potential booster crash
- FWRD-14803 Fixed an issue where DDM would not be used on Shared iPad through User channel due to incomplete documentation
- FWRD-14818 "Add URL Link" Window Issue in Create New Notification
- FWRD-14851 Fixed a case where a specific server process would output to the wrong log file
- FWRD-14888 iOS Kiosk doesn't update if SELF_HEAL_APPS_BY_VERSION=False
- FWRD-14907 Fixed an issue where booster could not be easily upgraded on Appliances where root account has no password set
- FWRD-14909 Notification Makes Model Update Difficult, Anywhere Admin
- FWRD-14923 Fixed an issue where ADE/DEP association dialog would show last sync time as UTC when opened
- FWRD-15007 Fixed an issue where VPP codes would not work with Applications having itunes id larger than 32b integer
- FWRD-15009 Fixed an issue where Winget Fileset would incorrectly enable Install button in Kiosk even if no update is available
- FWRD-15022 Fixed an issue where re-enrolling client too quickly could require adding the client a 2nd time
- FWRD-15031 Fixed an issue where Certificate revocation list signature could be outdated if the list of revoked certificates does not change regularly
- FWRD-15090 Clients cannot send requests via NATS if the server was slow during startup

Included Open Source Software

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

Upgrading Your Environment

▼ macOS Downloads

macOS Upgrade Fileset (md5: 443281b7b70cb802e057613e462cffdd)

> ⊗ FileWave 16.0. requires macOS 12 or later ; Initial macOS Upgrade Fileset had macOS 11+ requirements. Make sure you download the most recent version (check md5) or verify version requirements.

macOS Admin (md5: f203426ff3dd6ffa7e4fc84287d908e6)
macOS Booster (md5: d3c4a81707f7a63dab760dc1e0400f61)
macOS Server (md5: 21dcf05c55578b449fe9e05fe9be5929)

> ℹ️ Remember that to upgrade macOS FileWave clients you should use the Upgrade Fileset. 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: f0094ae8f8ce1703d5f68772516fdfc1)
Windows Admin (md5: 65a58e718ef85ac3ceeb4a2e40825df3)
Windows Booster (md5: 828be5e6e4aea307157d88cbefdb9749)

> ℹ️ Remember that to upgrade Windows FileWave clients you should use the Upgrade Fileset. 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 automatically installed from a CDN. (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 Linux Server (md5: 11d094df2e55a8e202a32a9d05b94e31)
Debian Linux Booster (md5: 6069d58928e5eb6828eaa92a35884d59)
Debian Linux IVS: FileWave Admin (md5: 0337269eda1d0be46b8797f484578179)
Debian Linux IVS: FileWave Imaging Client (md5: 0ebb4b326e2d23b78efd96d102c66780))
Debian Linux IVS: IVS Kernel (md5: 037c9b71e39add6f75691d91a2cb5e71)
Debian Linux IVS: FileWave IVS (md5: 1fb7a825da56ab2e8b5903ffc8ecb125)

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.

> ℹ️ If you are using a FileWave appliance that before 15.4.0 the SSH access was with the user "root" and for any appliance setup from 15.4.0 or later the user is "fwadmin" and you would have been forced to set the password on first login.

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

```
wget -qO- https://kb.filewave.com/attachments/411 | sudo bash -s -- -v 16.0.3 -r 1 -p -y
```

Upgrading a Booster
To install or upgrade the FileWave Booster, use the following or Booster Auto-Upgrade :

```
wget -qO- https://kb.filewave.com/attachments/412 | sudo bash -s -- -v 16.0.3 -r 1 -p -y
```

Upgrading a IVS
To upgrade the FileWave IVS, use the following:

```
wget -qO- https://kb.filewave.com/attachments/408 | sudo bash -s -- -v 16.0.3 -r 1 -p -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: 85a48f2511707c4069ef5e994275ffb3)
VMware and VirtualBox (OVA) Booster Appliance (md5: b41f83bf83e135a41beecdd9fb390293)
VMware and VirtualBox (OVA) Imaging Appliance (md5: 292d216df4e843e4868d799c8ad2876a)

HyperV Images
These three images are Hyper-V images suitable for Microsoft Hyper-V (Gen 1):
Hyper-V (VHD) Server Appliance (md5: 69f8e63930fd416456dc89625fbf9ff5)
Hyper-V (VHD) Booster Appliance (md5: 9bedd83dbfebf6645354e7ba4c0e9f07)
Hyper-V (VHD) Imaging Appliance (md5: e52920c5997cd7be4f6188b712b80ecb)

These three images are Hyper-V images suitable for Microsoft Hyper-V (Gen 2):
Hyper-V (VHD) Server Appliance (md5: ffc3dc723a9e0ab6557e901236594758)
Hyper-V (VHD) Booster Appliance (md5: 96a86a32b8d08ee004f5c6f008493b72)
Hyper-V (VHD) Imaging Appliance (md5: 89757f1e3d5c5a50e80f07a3f9502ee6)

ℹ️ To get started with the FileWave Server appliance please see: 1. Installation and Setup | FileWave KB
For a Booster you would setup networking just like you do with Server and then: Booster Installation | FileWave KB
For more information about importing the IVS appliance please see: Importing FileWave Appliances

⊗ CentOS is EOL. You must Migrating your On-Premise FileWave Server to new Hardware to get to FileWave on Debian or consider our Cloud Hosting Product.

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: 6145f53cf91a60a2efb5a6fc46aad291)

[Windows Client](#) (md5: 1c7f2ca9c5f778644569448c507e34f6)