Release Note

Admin By Request
ZERO TRUST PLATFORM

Release Information

Product Platform: **macOS**
Product Version: **5.3**
Date: **8 June 2026**

Mac 5.3

Introduction

Admin By Request (ABR) for Mac 5.3 contains bug fixes, performance improvements and no less than **8 new features**, including the much-requested **System Settings Pre-Approval**, which now covers System Extensions, Time Machine, Date & Time, Energy Saver, Printing and System Updates, in addition to those system settings already in place.

In this document

Refer to the Admin By Request Documentation Center for full details on these new features or any other aspect of Admin By Request.

Prerequisites

Organizations wishing to evaluate endpoints running ABR Mac 5.3 need the following:

- One or more devices running Apple **macOS 14 (Sonoma)** or higher
- Credentials to access the Admin By Request portal at **https://adminbyrequest.com/login**
- **ABR Mac 5.3** client software, downloaded from the portal and available to each endpoint

System Settings Pre-Approval

Standard users can now make changes to selected System Settings panes through ABR authentication, without being granted a full admin session. Administrators choose which panes to pre-approve from an expanded list under **Endpoint Privilege Management > Settings > Mac Settings > Lockdown > SYSTEM SETTINGS** in the portal. When a user opens a pre-approved pane, ABR intercepts the standard macOS admin prompt and authorizes the change in place.

Existing lockdown behavior is preserved: panes left toggled off remain hidden during an admin session (for example Startup, Transfer, Reset, Users & Groups).

> MDM policies take precedence over ABR's System Settings handling. Any pane restricted by an MDM configuration profile stays restricted, including outside an admin session, so customers can mix and match MDM-enforced controls with ABR pre-approval.

Refer to System Settings for more information.

App Uninstall from Applications

Standard users can now uninstall eligible apps from /Applications through ABR authentication, without being granted a full admin session. This closes a gap from 5.1, which already allowed installs from /Applications but still required a full admin session to remove an app. When a user removes an eligible app via Finder, ABR intercepts the standard macOS admin prompt and authorizes the uninstall in place.

Protected, restricted, and managed apps stay protected: removing them continues to require native administrator credentials, so business-critical software cannot be cleared out through this path.

Both Finder-based installs and uninstalls now route through ABR handling, giving administrators a single authorization path for app lifecycle changes from /Applications.

Refer to Removing an app from a Mac for more information.

App Blocking for macOS

Administrators can now block selected applications from launching on macOS endpoints, bringing parity with the existing Windows App Blocking capability. Blocks can be defined by **checksum**, **Team ID**, or **Bundle ID** in the App Blocking rules in the portal. When a user attempts to launch a blocked app, the launch is prevented and the user receives a notification.

The **Mac App Store** itself can be blocked for standard users while remaining available to administrators, so customers can restrict consumer app discovery without disabling the store for IT use.

Combined with "Version-Based App Pre-Approval" below, blocking rules can also be version-ranged, giving administrators fine-grained control over which builds of an app are permitted or denied on managed Macs.

Refer to Pre-Approval and Blocked Settings for more information.

Bundle ID App Pre-Approval

Application pre-approval on macOS now supports matching by **Bundle ID** in addition to the existing Team ID matching. Administrators can pre-approve one specific app from a vendor without implicitly approving every other app that vendor signs with the same Team ID.

Bundle ID is configured in the same app pre-approval rules in the portal alongside checksum and Team ID. Existing Team ID rules continue to work, and both identifiers appear together in audit log entries, so administrators can correlate approvals to specific apps rather than vendor groupings.

This feature is targeted at known business apps where vendor-level approval is too broad, for example trusting a single utility from a major vendor without trusting the rest of that vendor's catalog.

Refer to Protection matchers for more information.

Version-Based App Pre-Approval

App pre-approval rules now support **minimum** and **maximum version** constraints, so administrators can restrict approval to a trusted or tested version range rather than the app identity alone. Version bounds are configured per pre-approval rule alongside the existing checksum, Team ID, and Bundle ID matchers.

> Version ranges also apply to **App Blocking** rules added in 5.3, so blocks can target specific vulnerable versions rather than the whole application. This brings parity with the equivalent capability in the Windows 8.8 release.

The intended use is to avoid pre-approving known-vulnerable old builds or unverified new builds, and to support phased rollouts where only a tested version range should be allowed during a transition window.

Refer to Version constraints for more information.

Passwordless Unattended Access for Mac

Secure Remote Access now supports unattended sessions on macOS without a shared, pre-set password. Because macOS has no true passwordless login, ABR provisions a **just-in-time (JIT) local account** and emails one-time credentials to the admin when they click **Remote** from the inventory. The admin uses those credentials to sign in to the endpoint.

Enabled under **Secure Remote Access > Settings > Unattended Access Settings** by toggling ON unattended access. Account creation on first connect takes around 30 seconds on Apple Silicon, depending on other settings.

When the session ends, whether by logging out, clicking disconnect, or losing the connection ungracefully, the JIT user is automatically signed out and cleared from the login screen so it cannot be reused by anyone with physical access to the Mac.

Refer to Password-less access (Unattended Access) for more information.

Policy-Gated Admin Revocation

A new policy-controlled feature can sweep an endpoint and remove admin rights from any pre-existing local admin accounts that are not explicitly preserved. This is distinct from the existing local admin report, which requires logging into each account individually to demote it; the policy performs a general sweep at install time and revokes all eligible admins in one pass.

> Because of the potential impact of misuse, the feature is **deliberately not exposed in the ABR portal**. It is enabled per endpoint via **MDM policy only**, as a one-time action that runs once the policy is in place.

Excluded accounts, break-glass accounts, JIT users, and any user with an active ABR session are preserved, so legitimate administrative access paths are not disrupted. The intent is to reduce local admin drift across a fleet without running manual cleanup campaigns.

Refer to Revoke Admin Rights via policy for more information.

Jamf Group-Based Sub-Settings

ABR now integrates with Jamf Pro so macOS sub-settings can be targeted by Jamf computer group membership instead of being scoped manually inside ABR. Both **static** and **smart** computer groups are supported.

Setup is done in two places:

1. **In Jamf Pro:** create an API role with read access to *Computers*, *Static Computer Groups*, and *Smart Computer Groups*, then create an API client bound to that role.
2. **In the ABR portal:** under Tenant Settings, configure the new Jamf Pro Connector with the API client credentials (**Settings > Tenant Settings > Identity > JAMF**).

Once connected, sub-settings can use a rule of the form "computer must be in group X". When a user on an enrolled, Jamf Connect-installed endpoint requests an admin session, the sub-settings that match their device's Jamf group membership (for example a custom *company name* and *authorization access time*) are applied to that session.

Refer to Jamf Group-Based Sub-Settings for more information.

Bug fixes

Several bugs have been fixed in ABR Mac 5.3, resulting in improved performance and better stability.

How does the Update Process work?

Admin By Request software updates are deployed using our Auto-Update process. However, when we release a new version we do not deploy it right away to all customers via auto-update. This is simply to mitigate any unforeseen issues.

Our rule-of-thumb for a new release is to activate auto-update within **4 - 8 weeks** of release, but this is subject to change, depending on feedback and any potential issues that might arise.

Contact us if you wish to receive the latest version right now. You can also raise a support ticket requesting the latest update.