

Release Notes

Release Information

Product Platform: **macOS**

Product Version: **6.0**

Date: **26 October 2026**

Mac 6.0

Introduction

Admin By Request for Mac 6.0 is a major release. Its headline feature is **managed sudo**, which lets a standard user run named commands with sudo without an *Admin Session*, with every allowed and denied command audited. Alongside it:

- a refreshed, native client interface across dialogs, request flows, Remote Support and session timers
- extension of an *Admin Session* that is already running, when allowed by policy
- remote termination of elevated access from the portal, with an optional blackout period
- System Settings pre-approval decided per setting, under *App Control*
- Platform SSO as an identity source for MFA *Email match*
- Remote Support requests during an active *Admin Session*
- support for macOS 27 (Golden Gate).

Admin By Request for Mac 6.0 also improves how application installers and updaters are handled, and brings many customer-requested fixes.

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

In this document

- "Prerequisites" below
- "Managed sudo" below
- "Refreshed client interface" on the next page
- "Admin Session extension" on the next page
- "Remote termination of elevated access" on page 4
- "System Settings pre-approval" on page 4
- "Platform SSO for MFA Email match" on page 4
- "Remote Support during an Admin Session" on page 4
- "Application installers and updaters" on page 5
- "Other improvements" on page 5
- "Bug fixes" on page 5
- "How does the Update Process work?" on page 5

Prerequisites

Organizations wishing to evaluate endpoints running Admin By Request for Mac 6.0 need the following:

- One or more devices running Apple **macOS 15 (Sequoia)**, **macOS 26 (Tahoe)** or **macOS 27 (Golden Gate)**
- Credentials to access the Admin By Request portal at <https://adminbyrequest.com/login>
- **Mac 6.0** client software, downloaded from the portal and available to each endpoint

macOS 14 (Sonoma) is no longer supported. Installation might work on older versions starting with macOS 13 (Ventura), but only the versions listed above are officially supported.

Refer to [Prerequisites](#) for more information.

Managed sudo

Before 6.0, sudo on a Mac was available only inside an *Admin Session*, and individual sudo commands could not be audited. Managed sudo turns sudo into a per-command policy decision:

- **sudo command pre-approval** rules, under **Endpoint Privilege Management > Settings > Mac Settings > App Control > PRE-APPROVE**, let a standard user run a named command with sudo, without an *Admin Session* and without being made an administrator.
- **sudo command block** rules, under **Endpoint Privilege Management > Settings > Mac Settings > App Control > BLOCKED**, withhold a named command from a user who is in an *Admin Session*.

Each rule names the absolute path of an executable, such as `/usr/sbin/dseditgroup`. The user types the command as usual, and Admin By Request resolves it to its path before applying policy. Allowed commands are recorded in the auditlog, and refused commands are reported as events. Sensitive values such as passwords and tokens are redacted, on a best-effort basis, before command lines are reported.

Permanent local administrators keep normal macOS sudo behavior and are not subject to managed sudo rules. Managed sudo is enforced from the first rule that reaches an endpoint.

In 6.0, rules match the command path only. Arguments are recorded in the auditlog but are not used for matching, so pre-approve only commands that are safe with any arguments.

The *Allow sudo terminal commands* setting under **Endpoint Privilege Management > Settings > Mac Settings > Lockdown > ADMIN SESSION** is being retired gradually. New configurations allow sudo during an *Admin Session*.

Refer to [Managed sudo](#) for more information.

Refreshed client interface

The client has a more modern, native macOS look across its dialogs, request flows, Remote Support and session timer screens, and follows the light or dark appearance selected in macOS. Among the visible changes:

- When more than one session is running at the same time, they are shown together in a single **Sessions** window, each with its own timer.
- Multi-factor sign-in is completed in a window inside the client, rather than in the default browser.
- *Support Assist* can be started directly from the main client window.
- The *About* panel shows the client version, and whether Endpoint Privilege Management and Secure Remote Access are enabled on the device.

Policy behavior is unchanged by the new interface, except where this release note describes a new feature.

Refer to [The updated 6.0 interface](#) for more information.

Admin Session extension

A user whose work is not finished can now ask for more time on an *Admin Session* that is already running, instead of letting it expire and submitting a new request. In the last minute of the session, the session window offers an **Extend** button.

Extending resets the countdown to the number of minutes set in the portal; it does not add those minutes to the time left. The session is not restarted, so the same auditing applies throughout, and when it finally ends, administrator rights are revoked as usual.

Extension is controlled under **Endpoint Privilege Management > Settings > Mac Settings > Lockdown > ADMIN SESSION**, by the number of extensions allowed per session and the number of minutes each extension gives. Where extension is not allowed, the **Extend** button is not shown.

Refer to [Extending an active Admin Session](#) for more information.

Remote termination of elevated access

Portal administrators can now end elevated access on a Mac before it expires, covering both an active *Admin Session* and a *Run As Admin* elevation. This is also known as *Remote Kill*. Termination takes effect immediately, and the auditlog records who ended the session.

A **blackout period** can be applied at the same time. While it is in force, the user cannot start a new *Admin Session* or *Run As Admin* request on that device, which gives IT time to investigate. The blackout expires automatically.

Refer to [Remotely terminating elevated access](#) for more information.

System Settings pre-approval

System Settings access for a standard user is now a pre-approval decided per setting, and it has moved from Lockdown to **Endpoint Privilege Management > Settings > Mac Settings > App Control > SYSTEM SETTINGS**:

- **On** means the setting is pre-approved, so a standard user can change it.
- **Off** means there is no pre-approval, and the setting behaves as macOS intends: a standard user can open and read it, but cannot change it.

Panes that are not pre-approved are no longer greyed out or shown as controlled by a profile. A standard user can open them, and macOS asks for administrator credentials when a change is attempted. A user in an active *Admin Session* can use all System Settings panes except Users & Groups.

The change comes from 5.3.x deployments, where some organizations preferred to leave the operating system's own behavior for standard users unchanged.

Refer to [System Settings pre-approval](#) for more information.

Platform SSO for MFA Email match

Where MFA uses *Email match*, the client can now take the user's trusted corporate email address or user principal name from Platform SSO when connector-based email resolution is unavailable. *Email match* therefore works on a Mac with no Entra ID Connector, provided that Platform SSO is configured and the user has completed Platform SSO registration on that Mac.

Refer to [Platform SSO as an identity source for Email match](#) for more information.

Remote Support during an Admin Session

A user can now request Remote Support while an *Admin Session* is active. The Remote Support request form has also been redesigned.

Refer to [Requesting Remote Support](#) for more information.

Application installers and updaters

Some applications start separate helper programs to install or update themselves. Mac 6.0 handles more of these through Admin By Request policy, so fewer of them need an *Admin Session* or raise an unexpected prompt:

- Updates built on Squirrel and Shiplt now follow Admin By Request policy instead of bypassing application pre-approval.
- Slack and Cloudflare WARP updates reuse the application's existing pre-approval or authorization without an additional prompt.
- Electron apps, such as Codex, can be installed directly from a mounted disk image through the application-approval flow.
- Postman and similar downloaded apps no longer hang when moved to the Applications folder.

Other improvements

- **macOS 27 (Golden Gate)** is supported, including a fix for System Settings panes that could stay disabled after being re-enabled in Mac Lockdown.
- **App Control:** a rule that combines a Team ID and a Bundle ID now matches only when both match.
- **Support Assist:** attempts to use the endpoint user's own identity are blocked with guidance to use a different account, and the auditlog shows the supported user's full name and Platform SSO email correctly.
- **Inventory:** faster on devices with many installed apps, and firewall settings, including *Block all incoming connections* and managed firewall settings, are reported correctly.
- **Security:** PIN unlock policy is enforced in the client, and sensitive diagnostic data is protected.
- **Email validation** accepts apostrophes in addresses and rejects addresses padded with spaces.

Bug fixes

Many customer-reported issues are fixed in Mac 6.0, including:

- elevation requests that could remain on *Please wait* after the client had been running for a long time
- `lpadmin` printer commands that could trigger an unnecessary authorization prompt
- an unusable authorization prompt during Wi-Fi selection in macOS Setup Assistant
- custom branding logos that could overlap contact fields in authentication and *Run As Admin* prompts
- *Run As Admin* audit entries that could stay open after Electron-based app updates
- inconsistent capitalization between *Device Owner* and *Logged On User*.

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.