

Document Code: PM-MITAM
Document Release: 1.1
Release Date: 25 May 2023

macOS Client: IT Admin Manual

Configure, deploy and manage your Apple Mac workstations
Product Version: 4.0

 **Admin** By Request

Table of Contents

INTRODUCTION	3
In this document	3
Audience.....	3
Product Release Notes	3
INSTALLING AND UNINSTALLING	4
Prerequisites.....	4
Installing Admin By Request.....	4
<i>A) Download and install the Admin By Request package</i>	4
<i>B) Enable Full Disk Access (FDA)</i>	5
<i>C) Test the installation</i>	10
Uninstalling Admin By Request.....	10
<i>A) Via Admin Portal PIN code</i>	10
<i>B) Using sudo and /uninstall</i>	11
User rights after installation.....	11
Tamper Prevention	11
Mac Performance after Installation.....	12
Logging	12
THE USER INTERFACE	13
About Admin By Request	13
Requesting Administrator Access	14
Using Run As Admin	17
PORTAL ADMINISTRATION FOR MACOS	19
Pre-Approval.....	19
Run as Admin.....	20
Machine Learning	20
Azure AD Support	21
Supplementary Technical Information	21
Removed in macOS Version 3.0 Onwards:	24
POLICIES FOR MACOS	25
About Policies	25
Overruling portal settings	25
Overruling groups for subsettings.....	26
TERMS AND DEFINITIONS	27
Privileged Access	27
Glossary.....	28

Introduction

Admin By Request's Privileged Access Management (PAM) solution is designed to solve the security and productivity challenges relating to Local Administration rights usage within today's security conscious and highly distributed enterprises.

Employees achieve optimum productivity by utilising secure methods to safely elevate the everyday trusted tasks. IT departments achieve significant time and resource savings as employee requests for elevation are offloaded and routed through streamlined, fully audited and automated workflows.

This document describes key IT administrator concepts and tasks related to installing, configuring, deploying, and managing macOS endpoints.

In this document

The content of this document describes:

- How to install the Admin By Request client on endpoints running Apple's macOS.
- Three ways to enable Full Disk Access (FDA), including using Jamf and Intune.
- How to uninstall Admin By Request.
- The user interface, including screen panels associated with menu selections.
- Key portal administration tasks, specific to macOS.
- Using policy files to control portal settings.

Audience

The macOS Client: IT Admin Manual is intended for IT system administrators who install and manage user workstations running the macOS operating system and desktop software.

Product Release Notes

Admin By Request 4.0 – January 9th 2023

- Support for installation of application files by dragging them to the Admin By Request dock icon. Previously there was only support for .pkg files.
- Support for pre-approving applications based on vendor or checksum.
- Support for Azure AD groups for sub-settings based on the Azure AD Connector configured under Authentication in settings. The connector configuration is shared between Windows, Mac and Linux and does not need to be re-configured for Mac, if already set up for Windows.
- Machine Learning auto-approvals: When an application has been approved a certain number of times, Machine Learning can automatically approve requests. Refer to [Features > Machine Learning](#) for more information.

Installing and Uninstalling

Prerequisites

Full Disk Access (FDA) must be enabled for the *adminbyrequest* application, but this can only be done *after* installation.

The following installation procedure is in three parts: the first outlines downloading and installing the Admin By Request package, the second describes how to enable FDA, and the third outlines the differences between an admin user and a standard user (as well as the need to test the installation as a *standard* user).

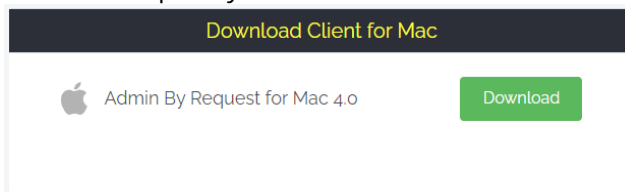
Installing Admin By Request

Installation steps are grouped into the following tasks:

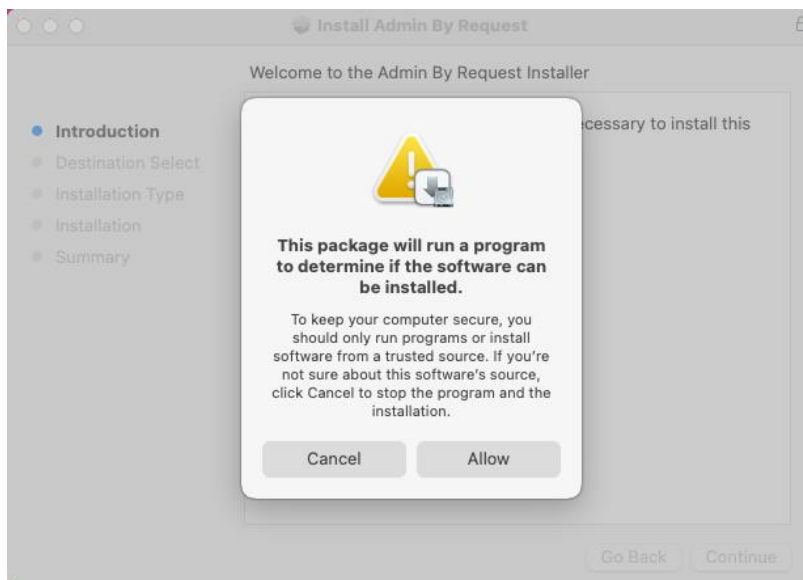
- Download and install the Admin By Request package
- Enable Full Disk Access (FDA): on the Mac, via Jamf and via Intune
- Test the installation as a standard user

A) Download and install the Admin By Request package

1. Sign-in to your Admin By Request account at <https://www.adminbyrequest.com/Login>.
2. Download the Mac client from the **Download** page and store the client file in a suitable temporary location:



3. Double-click the downloaded package to begin the installation:

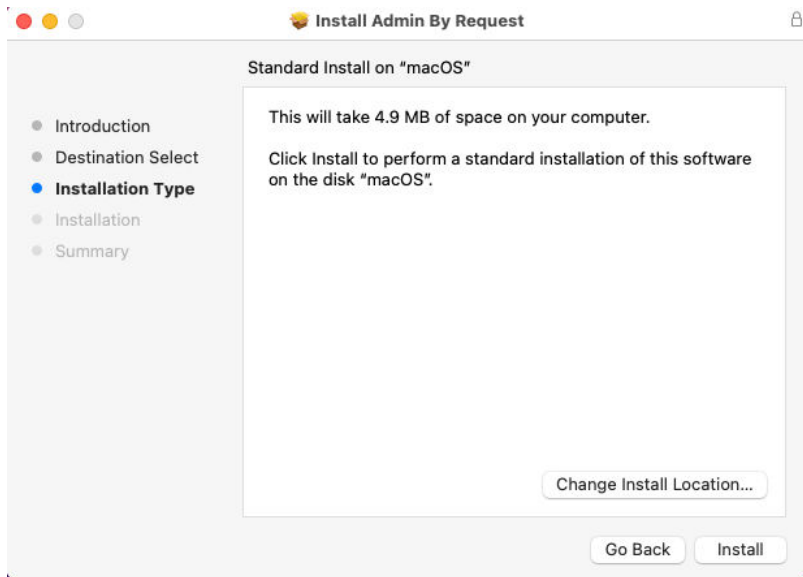


Continued ...

Installing and Uninstalling, Continued

Installing Admin By Request, Continued

- Allow the installation to proceed:



- Provide your password to allow installation.
- When done, close the installer and (optionally) move the installer package to the bin.

B) Enable Full Disk Access (FDA)

Immediately *after* installation, FDA must be enabled to allow Admin By Request to fully protect Mac endpoints.

NOTE: The *adminbyrequest* application must be installed first, so that it appears in the list of apps available under Full Disk Access.

The following procedures describe three ways to enable FDA:

- (1) On the Mac (for macOS 12 and macOS 13)
- (2) Using Jamf
- (3) Using Intune

(1) Enabling FDA on the Mac

The procedure to enable FDA is slightly different for different macOS versions. The following steps describe how to enable FDA on Apple Macs running:

- macOS 12 (Monterey)
- macOS 13 (Ventura)

macOS 12 (Monterey)

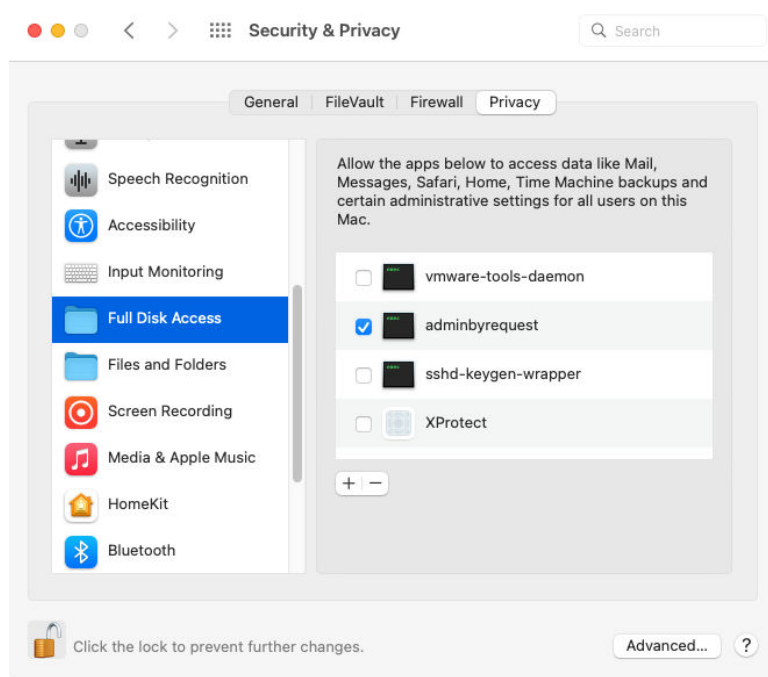
- On your Mac device, navigate to **System Preferences > Security & Privacy > Privacy** tab and select **Full Disk Access** from the list. You'll need to supply your password to unlock and make changes.

Continued ...

Installing and Uninstalling, Continued

(1) Enabling FDA on the Mac, Continued

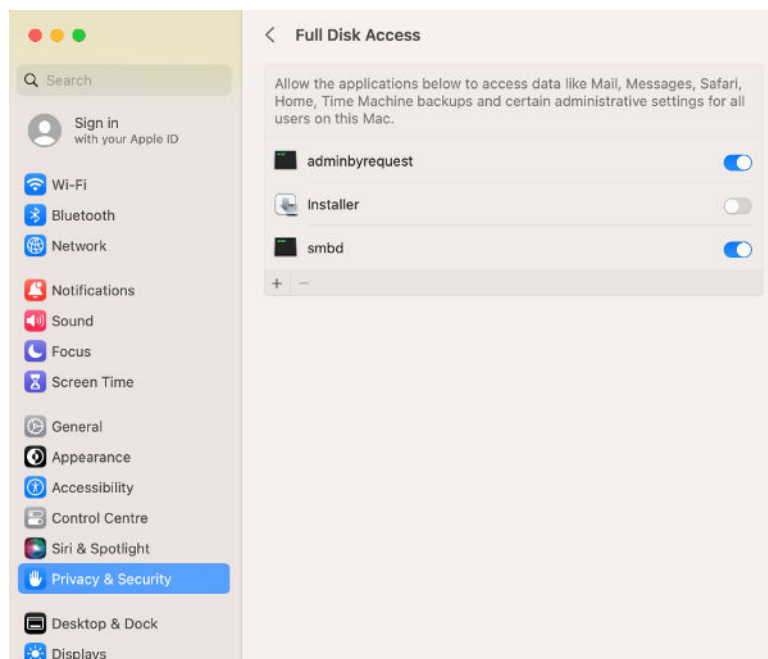
2. Select **adminbyrequest** in the list of apps (ensure the box is checked):



3. Lock the tab to save changes.

macOS 13 (Ventura)

1. On your Mac device, navigate to **System Settings > Privacy & Security** and select **Full Disk Access** from the list. You'll need to supply your password to make changes.
2. Select **adminbyrequest** in the list of apps (ensure the box is checked):



3. Close System Settings.

Installing and Uninstalling, Continued

(2) Enabling FDA using Jamf

Jamf uses *Configuration Profiles* to manage Mac endpoints:

1. In Jamf, go to **Computers > Configuration Profiles**.
2. Create a new profile and configure it as follows:
 - a) *Name*: give the profile a name that helps explain what application it is giving rights to. In this example, we use **ABR - PPPC**.
 - a) *Category*, select **Applications**.
 - b) *Distribution Method*, select **Install Automatically**.
 - b) *Level*, select **Computer Level**.
 - c) Navigate from the *General* tab to the **Privacy Preferences Policy Control** tab.
 - d) *Identifier*, enter **/Library/adminbyrequest/adminbyrequest**.
 - e) *Identifier Type*, select **Path**.
 - f) For *Code Requirement*, enter the following exactly as stated below
(**Tip**: copy/paste this text to ensure accuracy):

```
identifier "com.fasttracksoftware.adminbyrequest" and anchor apple
generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists
*/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */
and certificate leaf[subject.OU] = AU2ALARPUP
```

IMPORTANT: If you do not enter the above code correctly, this procedure for enabling FDA will not work properly.

- c) Under *App or Service*, select **SystemPolicyAllFiles** and under *Access*, select **Allow**:

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow

- d) Under *App or Service*, select **Accessibility** and under *Access*, select **Allow**:

APP OR SERVICE	ACCESS
Accessibility	Allow

- e) Save the profile.
4. Deploy and use this profile to enable FDA for all your macOS endpoints.

Installing and Uninstalling, Continued

(3) Enabling FDA using Intune

Similar to Jamf, Intune uses *Configuration Profiles* to manage Mac endpoints:

1. In *Intune*, under Configuration Profiles, select Create Profile.
2. Enter the following details into the *Create a Profile* form:
 - Platform: **macOS**
 - Profile type: **Templates**
 - Template name: **ABR – FDA**

Create a profile

Platform
macOS

Profile type
Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. [Learn more](#)

Search

Template name

- Custom
- Device features
- Device restrictions**
- Endpoint protection

3. Click **Create**.
4. Under **Device restrictions**, go to **Configuration settings**.
5. Select **Privacy preferences** and click **Add**:

Device restrictions

macOS

Basics Configuration settings Assignments Review + create

- App Store, Doc Viewing, Gaming
- Built-in apps
- Cloud and Storage
- Connected devices
- Domains
- General
- Password
- Privacy preferences**

Configure an app's access to specific data, folders, and apps on a device. These settings apply to devices running macOS Mojave 10.14 and later.

User approved and automated device enrollment

These settings work for devices that were enrolled in Intune with user approval, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.

Apps and processes **Add**

Name	Identifier
No data	

Continued ...

Installing and Uninstalling, Continued

(3) Enabling FDA using Intune, Continued

6. In the *Edit Row* form, enter the following:

- Name: **ABR - FDA**
- Identifier type: **Path**
- Identifier: **/Library/adminbyrequest/adminbyrequest**
- For *Code Requirement*, enter the following exactly as stated below
(**Tip:** copy/paste this text to ensure accuracy):

```
identifier "com.fasttracksoftware.adminbyrequest" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = AU2ALARPUP
```

IMPORTANT: If you do not enter the above code correctly, this procedure for enabling FDA will not work properly.

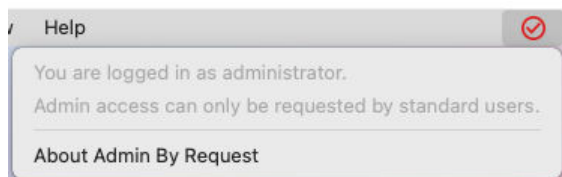
Here is an example of the completed *Edit Row* form:

7. Finally, allow **Full disk access**:

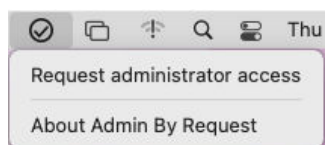
Installing and Uninstalling, Continued

C) Test the installation

Users logged-in with administrator privileges see the following icon and options from the menu bar:



Users logged-in with standard privileges see a different icon and menu options:

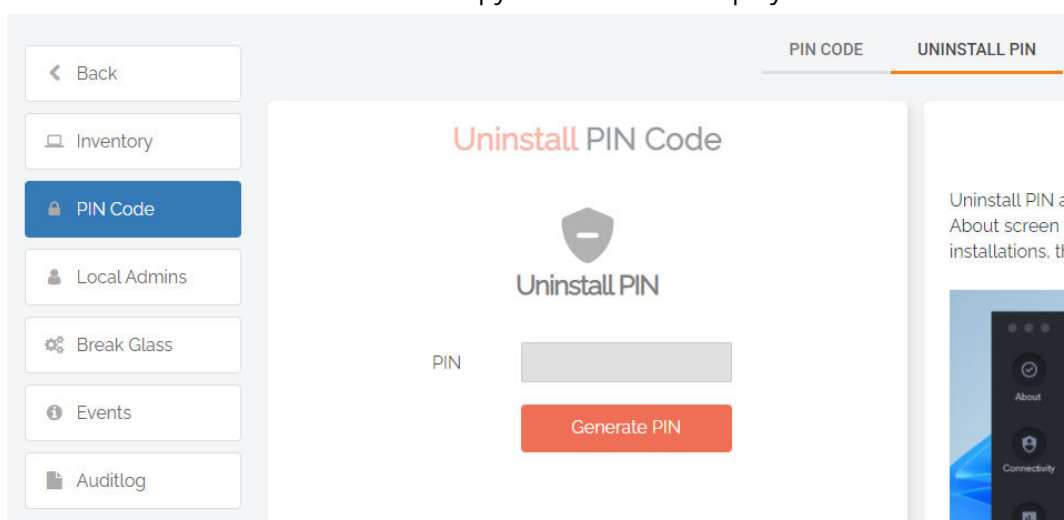


To test that Admin By Request is working properly, login to a Mac as a *standard user* and attempt a task that requires elevated privileges (such as modifying Users/Groups) to test that Admin By Request is working.

Uninstalling Admin By Request

A) Via Admin Portal PIN code

1. In the Admin By Request Portal, navigate to the *Inventory* page and select the device on which to perform the uninstall.
2. Select **PIN Code** from the left-hand menu and go to tab **UNINSTALL PIN**.
3. Click the **Generate PIN** button and copy the PIN that is displayed:



4. Back on the device on which you want to uninstall Admin By Request, select the *Admin By Request* icon from the top menu bar and click **About Admin By Request**.
5. In the *Uninstall* window (see next section [About Admin By Request](#), point 4 Uninstall), enter the PIN copied from the Portal, and click **Uninstall**.

Installing and Uninstalling, Continued

B) Using sudo and /uninstall

Uninstallation is straightforward and simply requires executing an uninstall program.

NOTE: The program cannot be run during an Admin By Request administrator session. You need to log in to the Admin By Request Portal and check/modify Mac settings there.

1. Using the Portal, go to **Settings > Mac Settings**.
2. Click **Lockdown** in the vertical menu at left and check the *Excluded accounts* list.
3. If your account is in the *Excluded accounts* list, continue with the next step. If your account is not in the list, add it and click **Save**. This must be an account with administrator privileges.
4. On the Mac(s) to be uninstalled, log in with an account in the list. If you are already logged in, log out and log back in again.
5. Run the following program on the Macs to be uninstalled:

```
sudo /Library/adminbyrequest/uninstall
```

NOTE: You could achieve the same result by allowing sudo terminal commands without an account in the excluded accounts list, but that is a global setting and opens up sudo access to *all* users for as long as sudo is allowed.

User rights after installation

When a user logs on, the account is downgraded from *Admin* to *Standard User* unless:

- You have turned off **Revoke Admins Rights** in the portal settings (**Settings > Lockdown > ADMIN RIGHTS**).
- Also under **Revoke Admins Rights**, the user is in the list of *Excluded accounts*.
- The computer is domain joined and the user is domain admin.

Please refer to the [Mac client technical details page](#) for more information (section *Technical Info*).

Tamper Prevention

When a user initiates an administrator session, the user's role is not actually changed from user to admin. The user is granted all administrator rights, *except* the right to add, modify or delete user accounts. Therefore, there is no case where the user can create a new account or change their own role and become a permanent administrator.

The user also cannot uninstall Admin By Request, as the only program, to keep the administrator session open forever. Furthermore, all settings, configuration and program files are monitored during administrator sessions. If the user tries to remove or change any of the Admin By Request files, these are restored straight away and the attempted activity is logged.

Installing and Uninstalling, Continued

Mac Performance after Installation

When users are not using Admin By Request, it does not consume resources, except for a brief daily inventory and settings check.

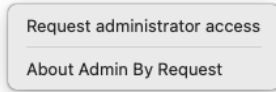
Logging

Client activity and errors are logged in file **`/var/log/adminbyrequest.log`**.

The User Interface

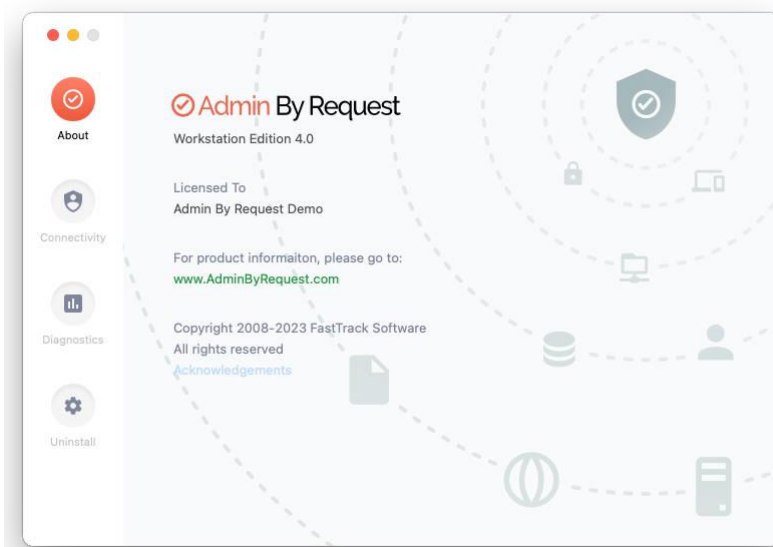
About Admin By Request

The user interface is graphical and is accessed via the icon menu in the top right corner of the screen. Click the icon to display the menu and select a menu option for further information or to carry out an admin task:

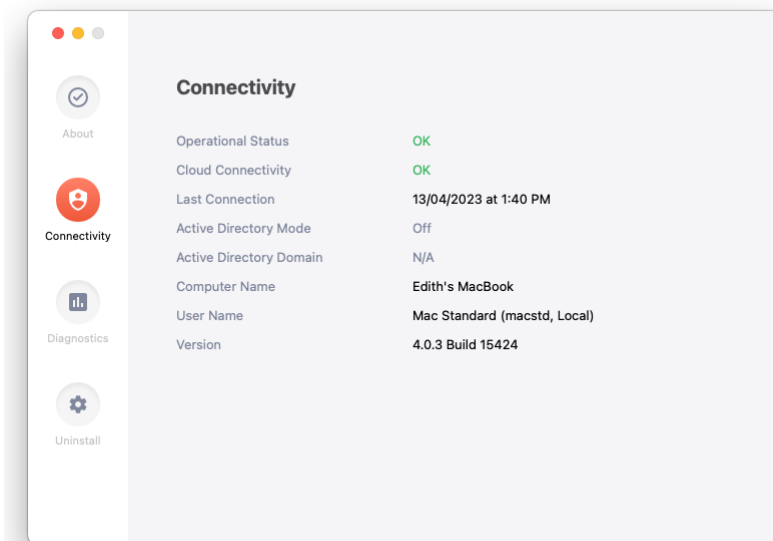


Selecting **About Admin By Request** shows the *About Admin By Request* panel.

1. **About** – displays this panel, including current workstation edition, license details, website link, and copyright information:



2. **Connectivity** – displays the current operational status of the Admin By Request system, including Internet and Cloud connectivity, and details about the current workstation and user:

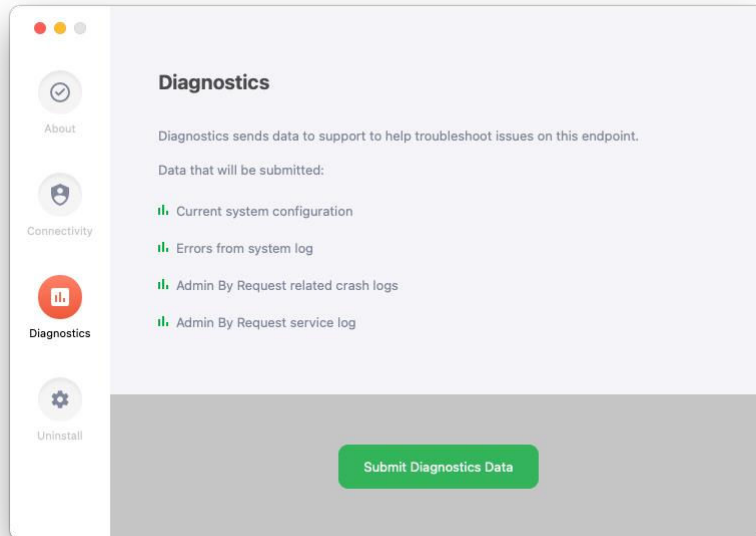


Continued ...

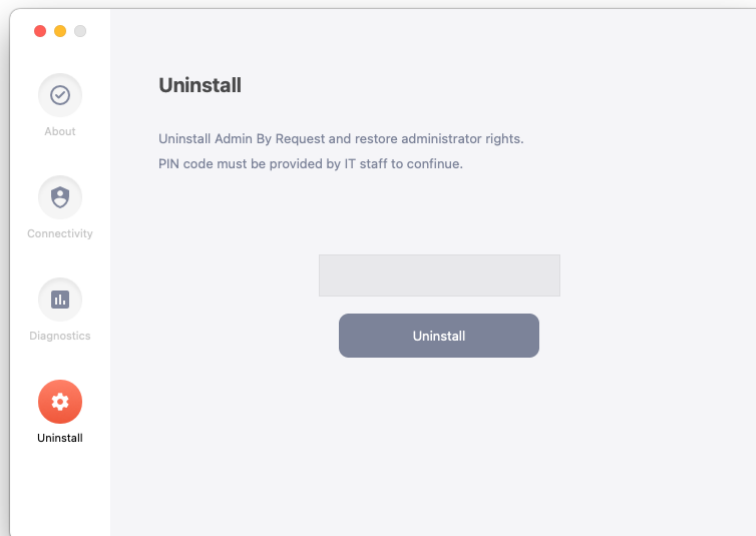
The User Interface, Continued

About Admin By Request, Continued

3. **Diagnostics** – provides a way to send useful diagnostic data on this workstation to the IT administration team:

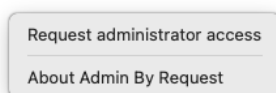


4. **Uninstall** – enables administrators to uninstall Admin By Request from this workstation. See [Uninstalling Admin By Request](#) for more information:



Requesting Administrator Access

As with *About Admin By Request*, click the menu bar icon to display the menu and select **Request administrator access**:



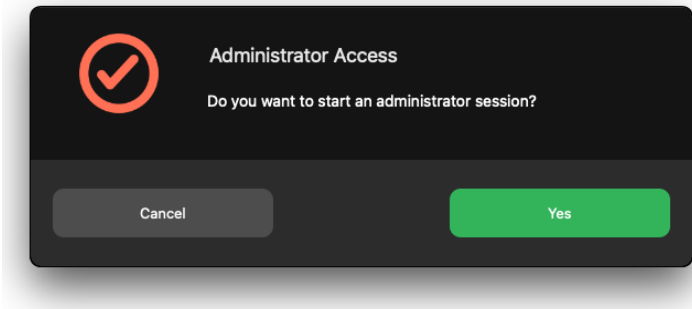
Continued ...

The User Interface, Continued

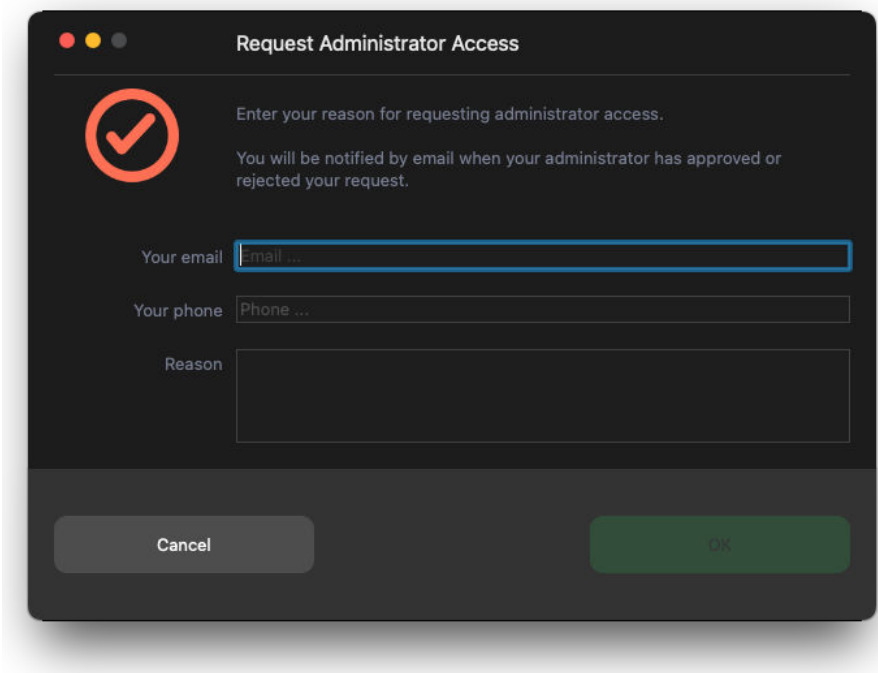
Requesting Administrator Access, Continued

A standard user making this selection initiates the following sequence of events:

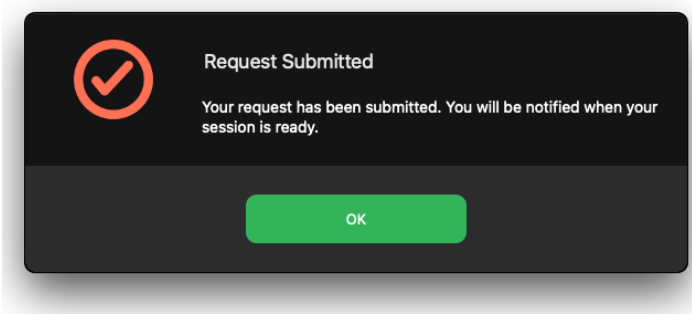
1. A prompt asks "Do you want to start an administrator session?". The user clicks **Yes** to continue:



2. An empty Request Administrator Access form appears:



3. The user enters *email*, *phone* and *reason* information into the form and clicks **OK**.
4. The request is submitted to the IT administration team and the user is advised accordingly:



Continued ...

The User Interface, Continued

Requesting Administrator Access, Continued

- The IT administration team is notified via the Admin By Request portal that a new request for administrator access has arrived. The following example shows how two new requests might appear in the portal:

The screenshot shows the Admin By Request portal interface. At the top, there is a navigation bar with the following items: Admin By Request, Summary, Auditlog, Requests, Reports, Inventory, Settings, Download, Logins, Docs, and Support. Below the navigation bar, there is a section titled "Pending Approval Requests" with a sub-header "Users will be notified by email of approval or denial." and a note "Requests will drop out of the list after two weeks. If a user does not use an approved request within two weeks, the approval will expire. You can approve or deny requests using the [mobile app](#) also." Below this, there are four tabs: PENDING (2), APPROVED (0), DENIED (0), and QUARANTINED (0). The PENDING (2) tab is selected. Below the tabs, there are two request cards. Each card displays the request time, user name, email, phone number, and computer name. The first card is for a request from "Mac Standard" at 12:10:01 on 13-04-2023, with the reason "Testing and Documentation". The second card is for a request from "Mac Standard" at 11:26:58 on 13-04-2023, with the reason "Testing and Documentation". Each card has "Approve" and "Deny" buttons.

- One of the team either approves or denies the request. If approved, the user is advised accordingly:

The screenshot shows a notification dialog titled "Administrator Access" with the Admin By Request logo. The message says "Your session has been approved!". There are two buttons: "Close" and "Start".

- The user clicks **Start** and is prompted once more if they want to start an administrator session. Clicking **Yes** one more time starts the session and displays a countdown timer:

The screenshot shows a window titled "Administrator Access" with a large red checkmark icon. The message says "Administrator Access" and "00:14:52". There is a "Finish" button.

- The duration of an admin session is set via the portal (15 minutes in this example) and the countdown timer ticks down to zero, at which time the session ends. The user can end the session at any time once it has started by clicking **Finish**.

See [Changing Admin Session Duration](#) for more information on changing the duration of the countdown timer.

The User Interface, Continued

Requesting Administrator Access, Continued

During an admin session, users can install programs requiring admin rights, install drivers and change system settings other than user administration. Users cannot run sudo or add, remove or modify user accounts.

Using Run As Admin

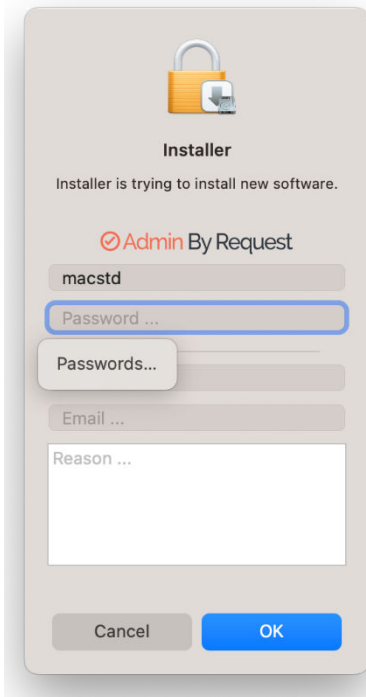
The Admin By Request *Run as Administrator* feature allows for the elevation of a single application. This capability negates the need for users to initiate an Administrator Access session (i.e., an extended period of time during which the user has elevated privileges on the device) to simply install one program.

Elevating privileges for execution of a single file is the much safer option compared to elevating the user's privileges across the endpoint.

Run As Admin supports both **package files (.pkg)** and **application files (.app)**.

To use Run As Admin:

1. Download the package or application file for installation.
2. Start the installation (e.g., by double-clicking the downloaded package):



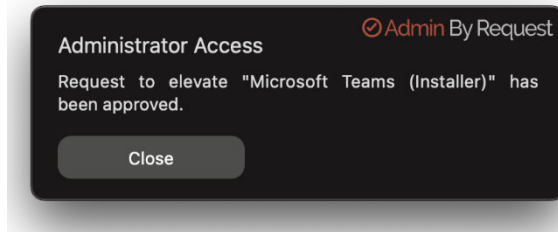
3. Admin By Request suspends installation and asks for *phone*, *email*, and *reason*. Enter these details and click **OK** to continue.

Continued ...

The User Interface, Continued

Using Run As Admin, Continued

4. A notification now advises that the request has been sent. When the request is approved, a further notification advises the request has been approved:



5. Now the installer has the elevated privileges required to run, but it still needs authorization from the current user. Start the installation a second time, supply credentials for the current user (who will be a standard user) and click **OK** to start authorized installation with elevated privileges.

The elevated privileges last only for the duration of the install and apply only to the particular application or package authorized.

NOTE: Run As Admin can also be initiated by dragging and dropping an application or package over the Admin By Request *Dock* icon. A pop-up will appear asking for credentials – simply enter them and hit **OK** to run the installer as an administrator.

Portal Administration for macOS

This topic describes several key areas of the Admin Portal that can be used to manage *Mac Settings* and *Mac Sub Settings*, specifically Pre-Approval, Machine Learning, Azure AD Support and Admin Session Duration.

Pre-Approval

Pre-Approval (known sometimes as Whitelisting) refers to the method of working out which applications are trusted and frequently used, and adding them to a list that automatically allows users to elevate those applications when they need to. This is essentially the opposite of Blocklisting/Blacklisting – creating a list of applications that cannot be elevated.

This method of “allow most, deny some” has proven to be extremely resource-efficient for large enterprises compared to the method of denying all applications and only allowing elevations on a case-by-case basis.

Admin By Request v4.0 for macOS allows for pre-approval of trusted applications. Once an application has been installed with Admin By Request:

1. Log in to the portal and navigate to the application’s corresponding entry in the portal **Auditlog**.
2. Expand on the application entry, and select **Pre-approve this file** under *Actions*:

The screenshot shows an audit log entry for 'Microsoft Teams (Installer)' on a 'MACBOOK AIR' machine. The entry details include user 'Mac Standard', start time '14-04-2023 13:22:08', and duration '00:04:44'. The 'Actions' section is expanded, showing options like 'Malware scan', 'Virusotal', 'Pre-approve', and 'Block'. The 'Pre-approve' option is highlighted with a red box.

3. Click **Save**.

The list of pre-approved macOS applications can be found under **Settings > Mac Settings > App Control > PRE-APPROVE**:

The screenshot shows the 'Pre-approve Applications' page in the Admin Portal. The page has a sidebar with navigation options like 'Authorization', 'Endpoint', 'Lockdown', 'Malware', 'App Control', and 'Data'. The main content area shows a table of pre-approved applications. The table has columns for 'Application', 'File', 'Protection', 'Type', 'Log', and 'Delete'. The 'Pre-approve' column has a checked box, and the 'Delete' column has a 'Delete' button. The page also includes a 'New entry' button and export options like 'Export to PDF', 'Export to XLSX', 'Export to CSV()', and 'Export to CSV()'.

Continued ...

Portal Administration for macOS, Continued

Pre-Approval, Continued

Pre-Approval is based on the application vendor or checksum.

You can also use the following commands to get the vendor's name for the files for Pre-Approval, without having to use the Auditlog in your User Portal. For example:

For applications (.app):

- Command: `codesign -d -vv /path/app.app`
- Result: Authority=Developer ID Application: VideoLAN (75GAHG3SZQ)

For packages (.pkg):

- Command: `pkgutil -check-signature /path/app.pkg`
- Result: Developer ID Installer: Oracle America, Inc. (VB5E2TV963)

In these examples, VideoLAN (75GAHG3SZQ) and Oracle America, Inc. (VB5E2TV963) are the vendors.

Run as Admin

The core Admin By Request *Run as Administrator* feature, which allows for the elevation of a single application, is new and improved in version 4.0. This feature negates the need for users to initiate an Admin Session (i.e., an extended period of time during which the user has elevated privileges on the device) to simply install on program. Elevating a single file is the much safer option compared to elevating the user's privileges across the endpoint.

Previously only supporting package files (.pkg), this feature now supports application (.app) files. Once you've downloaded the file for installation, drag and drop it over the Admin By Request Dock icon. A pop-up will appear asking for your credentials – simply enter them and hit **OK** to run the installer as Admin.

Refer to the animated GIF on the [Endpoint Software > macOS Client](#) page to see it in action.

Machine Learning

The idea behind Machine Learning Auto-Approval is to kill two birds with one stone by allowing customers to build a Pre-Approved list as their employees use the software. This removes the need for enterprises to spend considerable amounts of time and effort figuring out and manually configuring which applications should be pre-approved ahead of time.

The way it works is, it allows you to create a simple rule that says:

"If approval for elevation of an application is granted X times, that application is now automatically approved for incoming requests from then on."

This allows the system to handle creating the list of applications that are safe for approval, as applications are used.

For more information, including step-by-step procedures, refer to [Admin By Request Features, Machine Learning](#).

Portal Administration for macOS, continued

Azure AD Support

A huge selling point for Admin By Request PAM solution is its flexibility and tools for granular access control; organizations can configure every setting to their specific needs and the needs of all, some, or even individual users.

Settings act as rules, such as whether the *Run as Admin* or *Admin Session* features are enabled, and whether or not users need approval to use them. You likely wouldn't want the rules applied for an IT Administrator to be the same as those applied for a Customer Relations employee, so settings can be differentiated based on Sub-Settings, which allow different rules to be applied to different users and/or groups.

With macOS v4.0, we've built in support for Azure AD groups, meaning you can now apply Sub-Settings to existing Azure AD user and device groups.

Get this feature working using our *Azure AD Connector* integration, found under **Settings > Mac Settings > Authorization > AZURE AD**:

For more information, refer to [Admin By Request Integrations, Azure AD Connector](#).

Supplementary Technical Information

Local Administrator Accounts

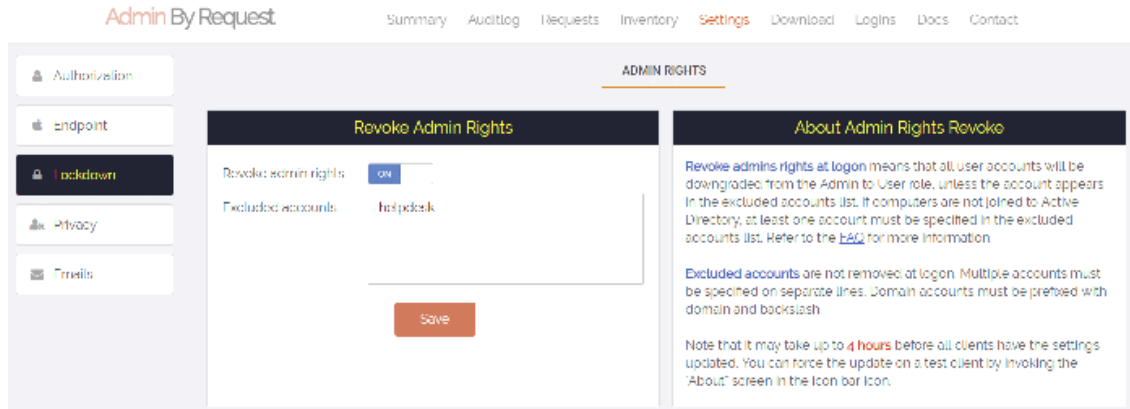
By default, users logging into a Mac are not downgraded from administrator to user unless the setting 'Revoke admin rights' is enabled in the portal and the user is not in the excluded accounts list. The reason all users are not downgraded immediately is because you may have service accounts that you have forgotten to list in the excluded accounts list.

Also, if someone cleared the excluded accounts list and clicked **Save** by mistake, the result would be unusable Mac endpoints; no users would be able to gain elevated privileges and would instead have very limited ability on their devices.

Portal Administration for macOS, continued

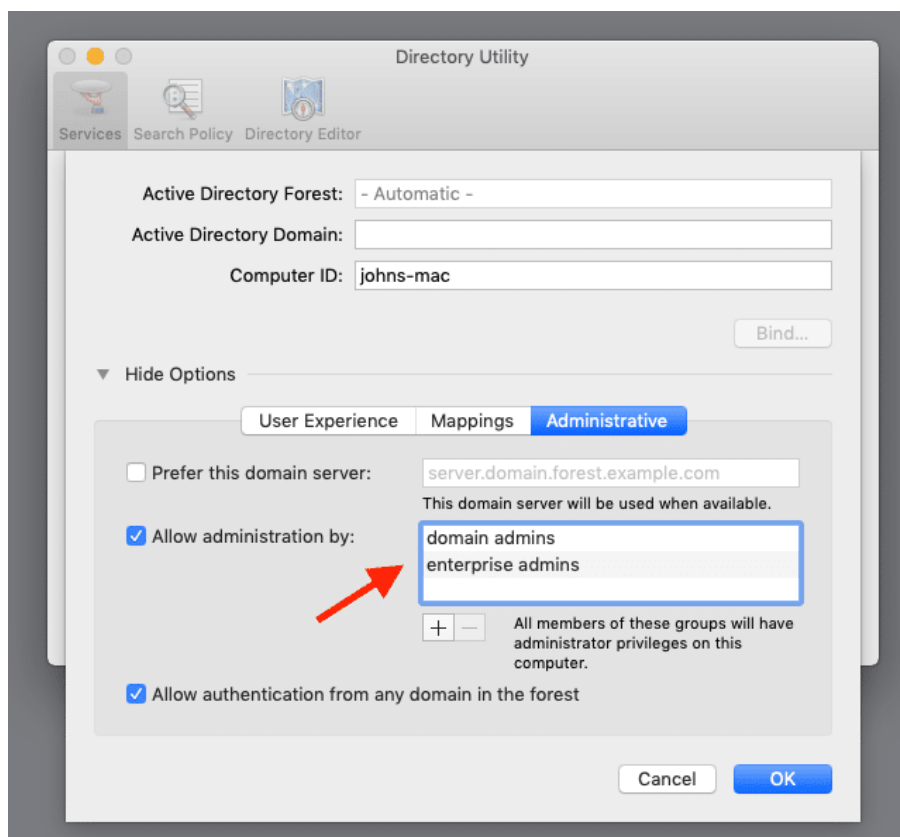
Supplementary Technical Information, Continued

The following graphic shows Revoke admin rights **ON**, except for user account helpdesk:



Active Directory

If a Mac is bound to an Active Directory, all local admin users will be downgraded unless listed in the excluded accounts setting. Admin By Request respects any group defined in the Directory Utility under "Allow administration by" and will not downgrade these users.



Continued ...

Portal Administration for macOS, Continued

Supplementary Technical Information, Continued

If no administrator groups are defined, the client will automatically grant administrator rights to members of the default Active Directory “Domain Admins” group. This is to prevent machines from ending up with no administrator accounts if the Active Directory binding is not setup correctly.

Sub-Settings

The portal has two levels of settings for mac users. *Mac Settings* apply to all users by default, unless overridden under *Mac Sub Settings*. With sub settings, you can define special settings based on Active Directory computer or user groups and/or Organizational Unit(s).

This can be used to allow sudo access for developers or automatically approve requests from users in the IT department. This feature is only available if the mac is bound to an Active Directory or using NoMAD or Idaptive. Sub settings can also be used by specifying machine / user groups in the policy file. See [Policies for macOS](#) Policies for macOS for more information.

Sudo

For security reasons, sudo access is disabled during administrator sessions by default. This can be enabled in the settings or a policy file (see [Policies for macOS](#) Policies for macOS). We do not recommend enabling sudo access unless absolutely necessary.

Admin By Requests has checks in place to prevent system tampering using sudo, but due to the root-level access, it is impossible to fully protect against tampering using sudo.

If only certain commands need to be run with sudo, consider using the built-in `/etc/sudoers` file. The Admin By Request sudo settings will not override normal `/etc/sudoers` settings.

System Extension

Admin By Request does not require any system extensions, unless you enable the Application Blocking feature introduced in version 3.2. If you use Application Blocking or the App Store blocking, the kernel extension has to be pre-approved using the following data:

- Team ID: **AU2ALARPUP**
- Bundle ID: **com.fasttracksoftware.adminbyrequest.extension**

You can verify that the system extension is installed in the Inventory in your User Portal: under ‘System Information’ in the client inventory details, there is an entry that shows whether the system extension is installed or not.

Machine Settings

You can use a local policy file to override all portal settings locally. Refer to [Policies for macOS](#) Policies for macOS for more information. Any setting defined in the policy file will override both default and sub settings. The policy file is locked during an Admin By Request administrator session, so users are unable to tamper policy settings.

Portal Administration for macOS, Continued

Supplementary Technical Information, Continued

Tampering

To prevent tampering with Admin By Request, the software monitors all important files during an administrator session. During a session, access to the Users & Groups preference panel is disabled to prevent users from adding new administrators. Further, by default, sudo access is disabled to prevent calling system critical tools and user management from the terminal.

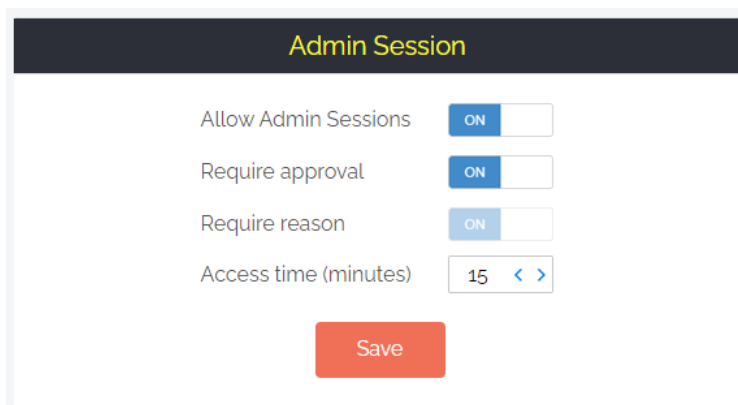
The service also monitors users and groups during the session to prevent tampering if sudo access is enabled. If Admin By Requests detects that the clock has been changed, the administrator session will end instantly to prevent users from extending their session.

Changing Admin Session Duration

Admin session duration (access time) is the maximum amount of time in minutes an *Admin Session* may last. This time must be sufficient for the user to install software or perform any other necessary tasks.

To change the time allocated for an administrator session:

1. Log in to the Portal and select menu **Settings > Mac Settings**.
2. From the *Authorization* left menu, make sure the **AUTHORIZATION** tab is displayed (it is the default) and update the **Access time (minutes)** field in the Admin Session panel:



4. Click **Save** when done.

Removed in macOS Version 3.0 Onwards:

- **Last Admin Check** – no longer relevant, removed in 3.0. The Last Admin Check feature is no longer relevant thanks to the addition of the PIN Code uninstall feature. The purpose of the Last Admin Check was to ensure that you always have at least one administrator account left, but is no longer necessary because you can now use PIN Code uninstall to remove the software on the endpoint and regain local admin rights (in the case of accidentally downgrading all users to standard user).
- **Log Files** – this service previously logged helpful information such as software version, detected Active Directory settings, admin downgrades, and similar changes to `/var/log/adminbyrequest.log`. It has been replaced in recent versions with functionality to submit diagnostics information from the *About* window, under *Diagnostics*.

Policies for macOS

About Policies

Settings in the Admin By Request client application are controlled under “Mac Settings” in the “Settings” menu, when logged in to the portal. If, for whatever reason, you want to overrule these settings on specific clients, you can set overruling policies in a policy file.

IMPORTANT: Please note we do not recommend that you use a policy file to control client behavior. Instead, we recommend that you use portal settings and sub settings for better transparency and for real-time control of computers not connected to your LAN.

If you have any questions about portal settings or would like a demo of these, please feel free to contact us.

Overruling portal settings

To overrule portal settings with a policy file, edit this file:

```
/Library/Application Support/Admin By Request/adminbyrequest.policy
```

Note that this file is protected during administrator sessions and can therefore not be hacked by end-users. The file is in json format and has an example non-used setting by default, as shown below. Simply add more settings from the following table to overrule web settings.

Also note that any change to the policy file will take effect *after* the next reboot. Alternatively, if a policy change must take effect immediately without a reboot, an admin user or MDM can restart the service using **sudo killall adminbyrequest**.

```
{
    "ExampleSetting": "ExampleValue"
}
```

Key	Type	Default	Description
AdminMinutes	Integer	15	Number of minutes the user is administrator. This can also be set in your portal settings.
AllowAppStore	Boolean	1	Allow users to install software from the App Store without admin rights or an active Admin By Request session.
AllowSudo	Boolean	0	Allow users to run sudo commands. Should not be enabled unless there is a good reason to, because it allows the user to tamper the endpoint software.
CompanyName	String		Overrules the company name that appears on user interfaces, which is by default the licensed company name.
ComputerGroups	Array of Strings		Computer groups to match machine to sub settings when not using Active Directory.
DockIcon	Boolean	1	Place an icon in the dock.

Key	Type	Default	Description
ExcludedAccounts	Array of strings		List of accounts that will not be downgraded to user role, such as service accounts.
EnableSessions	Boolean	1	User can request an admin session.
EnableAppElevations	Boolean	1	User can authenticate apps without session.
Instructions	String		Body text on Code of Conduct ("Instructions") screen.
InstructionsHeader	String		Header text on Code of Conduct ("Instructions") screen.
LogoUrl	String		Url to download logo from. If not specified, default icons will be used.
RemoveRights	Boolean	1	Downgrade users from Admin to User, unless the account is in excluded accounts or is a domain administrator in on a domain joined Mac.
RequireApproval	Boolean	0	Elevate without requiring someone to approve requests.
RequireReason	Boolean	1	Require reason to elevate.
RequireAppApproval	Boolean	0	Elevate Run As Admin without requiring someone to approve requests.
RequireAppReason	Boolean	1	Require reason to Run As Admin.
ShowInstructions	Boolean	0	Show Code of Conduct screen.
UploadInventory	Boolean	1	Upload inventory data to the portal.
UserGroups	Dictionary with array of strings		User groups to match machine to sub settings when not using Active Directory.

Overruling groups for subsettings

With the addition of the *ComputerGroups* and *UserGroups* keys (available since macOS version 3.0), see the example below:

```
{
  "ComputerGroups": ["Accounting", "USA"],
  "UserGroups": {
    "jane": ["Developers", "Germany"],
    "john": ["Accountants"],
  }
}
```

Terms and Definitions

Privileged Access

Privileged access refers to abilities and permissions that go above and beyond what is considered “standard”, allowing users (with privileged access) more control and reach in the system and network.

The following table describes several common privileged access terms.

Term	Definition
Blocklist	The opposite of a pre-approved list. A list of blocked programs or applications that are denied access in an IT environment (i.e., they are denied the ability to run) when everything is allowed by default. All items are checked against the list and granted access unless they appear on the list. Might also be known as a “blacklist” – a term no longer used. <i>See also Pre-Approved List.</i>
Elevated Application	An application that has been given greater privileges than what is considered standard, which enables the application user to have more control over its operation, and the app itself to have more abilities and access within the computer.
Elevated Privileges	Also known as “privileged access”. Elevated privileges provide the ability to do more than what is considered standard; for example, install and uninstall software, add and edit users, manage Group Policy, and modify permissions. Elevated privileges are sought after by attackers, who can use them to propagate through a network, remain undetected, and gain a strong foothold from which to launch further attacks
Endpoint	A physical device that is capable of connecting to and exchanging information with a computer network. Endpoints include mobile devices, desktop computers, virtual machines, embedded devices, servers, and Internet-of-Things (IoT) devices.
Horizontal Privilege Escalation	Also known as “account takeover”. Occurs when access to an account of a certain level (e.g., Standard User) is obtained from an account at that same level. Usually occurs when a malicious actor compromises a lower-level account and propagates through the network by compromising other lower-level accounts. <i>See also Vertical Privilege Escalation.</i>
Just-In-Time Access (JIT)	A way of enforcing the Principle of Least Privilege (POLP) by allowing access to privileged accounts and resources only when it is needed, rather than allowing “always on” access (also known as “standing access”). This reduces an organization’s attack surface by minimizing the amount of time an internal or external threat has access to privileged data and capability.
Lateral Movement	A common technique used by malicious actors, in which they spread from the initial entry point further into the network, while evading detection, retaining access, and gaining elevated privileges using a combination of tactics. The purpose is generally to compromise as many accounts as possible, access high-value assets, and/or locate a specific target or payload.

Term	Definition
Phishing	A type of social engineering attack in which the victim is tricked into clicking a malicious link that can lead to malware installation or further duping of the victim into providing sensitive information such as credentials or credit card details.
Pre-Approved List	The opposite of a blocklist. A list of approved programs or applications that are trusted (considered safe) when everything is denied by default. Items are checked against the already approved list and are only able to run if they are included in that list. Might also be known as a “whitelist” – a term no longer used. See also <i>Blocklist</i> .
Privileged Account	An account that has been granted access and privileges beyond those granted to non-privileged accounts. More sought after by attackers because, if compromised, they provide a better vantage point from which to launch an attack.
Privileged User	A trusted user who is authorized to leverage privileged access, such as through a privileged account, to perform high-value functions for which standard users are not authorized.
Standard User Account	A basic account for undertaking day-to-day tasks, for users who is not authorized or required to perform activities that require elevated privileges. These accounts are typically safer than those with higher access and permissions, as they do not provide the capability to perform administrative tasks, such as change system settings, install new software, manage the domain, and change local user credentials.
Vertical Privilege Escalation	Occurs when a lower-privileged account gains privileged access beyond what it is intended to have. Usually occurs when a malicious actor compromises an account (e.g., a “Standard User” account) and then exploits system flaws or overrides privilege controls to escalate that account to one with higher privileges (e.g., a “Local Administrator” account). See also <i>Horizontal Privilege Escalation</i> .

Glossary

Term	Short for	Definition
FDA	Full Disk Access	A security feature included in Apple Mac operating systems since Mojave (macOS 10.14) that allows some applications full permissions to access a user’s protected files. For example, anti-malware applications need Full Disk Access to access and check files.
Jamf	Jamf	A UEM solution that manages Apple devices exclusively, via a single console, allowing users to self-enrol multiple Apple devices of their choice.
MAM	Mobile Application Management	Software and processes that secure and enable IT control over enterprise applications on end users’ corporate and personal devices.

Term	Short for	Definition
MDM	Mobile Device Management	A methodology and toolset used to provide a workforce with mobile productivity tools and applications, while keeping corporate data secure.
PAM	Privileged Access Management	A set of cybersecurity technologies and strategies that allow organizations to secure their infrastructure and applications by managing privileged access and permissions for all users across the IT environment.
POLP	Principle of Least Privilege	The idea that users, applications, programs, and processes should be allowed only the bare minimum privileges necessary to perform their respective functions.
PPPC	Privacy Preferences Policy Control	A way for IT administrators to specify macOS configuration profiles for deployment to multiple devices. Works closely with TCC.
TCC	Transparency Consent and Control	Introduced by Apple from macOS 10.14 to improve data protection for users. Enables a macOS device user to retain control over endpoint components such as camera and microphone. Works closely with PPPC.
UEM	Unified Endpoint Management	A way to securely manage all the endpoints in an enterprise or an organization from a central location.

End of Document