

Endpoint Privilege Management (EPM) | Mac

Product Version: 5.0

Mac Client: IT Admin Guide

Document Information

Code: **PM-MC-ITAG**

Version: **2.1**

Date: **6 September 2024**

Copyright © 2024 Admin By Request

All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement (NDA). The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the customer's stated use without the written permission of Admin By Request.

Contact Admin By Request

 +64 21 023 57020

 marketing@adminbyrequest.com

 adminbyrequest.com

 Unit C, 21-23 Elliot St, Papakura

Table of Contents

Mac Client - Overview	1
Introduction	1
In this document	1
Audience	1
Product Release Notes	1
Mac Client - Install / Uninstall	2
Prerequisites	2
Your Tenant License	2
Installing Admin By Request	3
Single endpoint installation (manual)	3
Multiple endpoint installation (automated via MDM)	7
Upgrading Admin By Request	11
Deploying new releases	11
For more information	12
Uninstalling Admin By Request	12
User rights after installation	16
Tamper Prevention	17
Mac Performance after Installation	17
Logging	17
The Mac Client User Interface	18
Introduction	18
In this topic	18
About Admin By Request	19
Submitting Diagnostics	22
Requesting Assistance (Support Assist)	22
Assistance example scenario	23
Assistance sequence	24
Security checks	24
Uninstalling via PIN Code	25
Using Run As Admin	26
Example 1 - Install app VLC	26
Example 2 - Install app Foxit PDF Reader	28
Multi-Factor Authentication (MFA)	31
Intuitive app updates	31
Requesting Administrator Access	32
Multi-Factor Authentication (MFA)	34

Setting-up a Break Glass Account	34
Security benefits	34
When would I use a Break Glass account?	35
Using the Break Glass feature	35
Portal Administration for Mac	39
Introduction	39
In this topic	39
Entra ID Support	40
Run As Admin Settings	42
Admin Session Settings	43
Changing Admin Session Duration	43
Authentication Setting	44
System Settings	45
Enabling sudo	46
Pre-Approval Settings	47
Machine Learning	50
Privacy Settings	50
Preventing Abuse	51
Policies for macOS	52
Clean up Local Admins	55
Purpose	55
Functionality	55
How It Works	55
Using the Feature via Reports Page	56
Example - Olivia's Mac	56
Supplementary Technical Information	57
Local Administrator Accounts	57
Active Directory	58
Sub-Settings	58
Sudo	59
Machine Settings	59
Tampering	59
Terms and Definitions	60
Privileged Access	60
Glossary	62
Synchronizing Clients with the Portal	64
Introduction	64
Periodic Synchronization	64

Manual Synchronization	64
Scripted Synchronization	65
Factors Affecting Synchronization Timing	65
Handling Hybrid Environments	65
Common Issues and Solutions	65
Document History	67
Index	69

Mac Client - Overview

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 using secure methods to safely elevate 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 guide describes key IT administrator concepts and tasks related to installing, configuring, deploying, and managing macOS endpoints.

In this document

The content of this guide describes:

- How to install the Admin By Request client on endpoints running 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.
- Selected Settings tables, describing how to use each setting.
- Terms and definitions.

Audience

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

NOTE:

Although the guide is written from the point of view of an IT Administrator, the procedure steps and screenshots are described from an end user's perspective. This has two benefits:

1. You can clearly see how something works from an end user's point of view.
2. If required, you can create your own customized end user documentation by simply copying and pasting the procedures with minimal rework.

Product Release Notes

This version of the IT Admin Guide is **2.1** and it is written for the macOS client, version **5.0**.

Release notes for all product versions are available on the Admin By Request website:

[Release Notes \(macOS\)](#)

Mac Client - Install / Uninstall

Prerequisites

Admin By Request supports the following macOS versions:

- macOS 10.15 (Catalina)
- macOS 11 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)
- macOS 14 (Sonoma)

Installation **may** work on macOS 10.12 (Sierra) through 10.14 (Mojave), but product development and testing is not done on these versions and they are not officially supported.

Note that certain Mac 5.0 features, such as Admin Auditing and the new app installation flow, require macOS 11 or higher.

Full Disk Access (FDA) must be enabled for both the *adminbyrequest* application and the Admin By Request *System Extension*.

IMPORTANT:

The **order of installation tasks** matters and it differs depending on manual installation of a **single endpoint**, or automated installation of **multiple endpoints** via an MDM such as Jamf or Intune.

Your Tenant License

The installer file downloaded from the portal is **unique to your tenant**. Depending on the target operating system, it can be an executable file, a package or a script and it is signed with a license that applies *only* to installers downloaded from the tenant in which you are currently logged-in. The same license file is applied to each of the operating system client installers: Windows, macOS, Linux and Server.

This is true for free plans as well as paid plans.

When installed on an endpoint, once the endpoint connects successfully, you will see in real time the status of the endpoint in your Inventory, which is also unique to your tenant. You will not see other endpoints installed with files downloaded from other tenants - this is simply not possible.

Installing Admin By Request

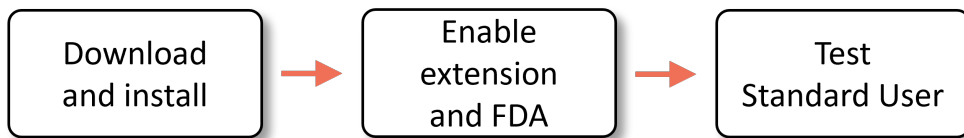
Single endpoint installation (manual)

This procedure describes how to manually install the Mac client on a single endpoint.

IMPORTANT:

To make Mac 5.0 work with **all features**, you need to enable the following on the Mac:

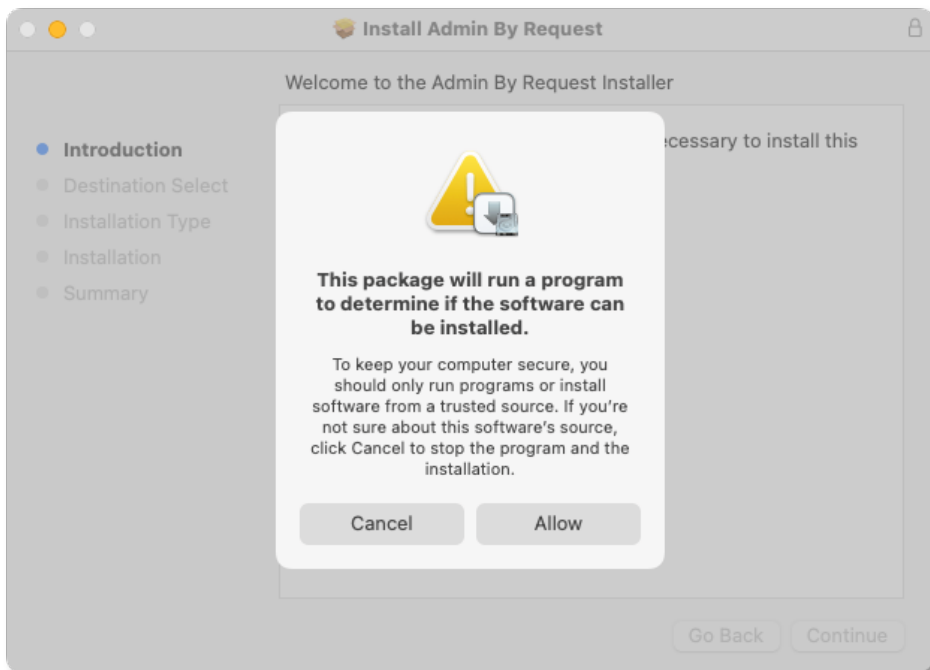
- Allow the Admin By Request System Extension (during installation - **Download and install** step 5)
- Enable Full Disk Access to “adminbyrequest” (after installation - **Enable FDA for two apps**)
- Enable Full Disk Access to the “Admin By Request System Extension” (after installation - **Enable FDA for two apps**)



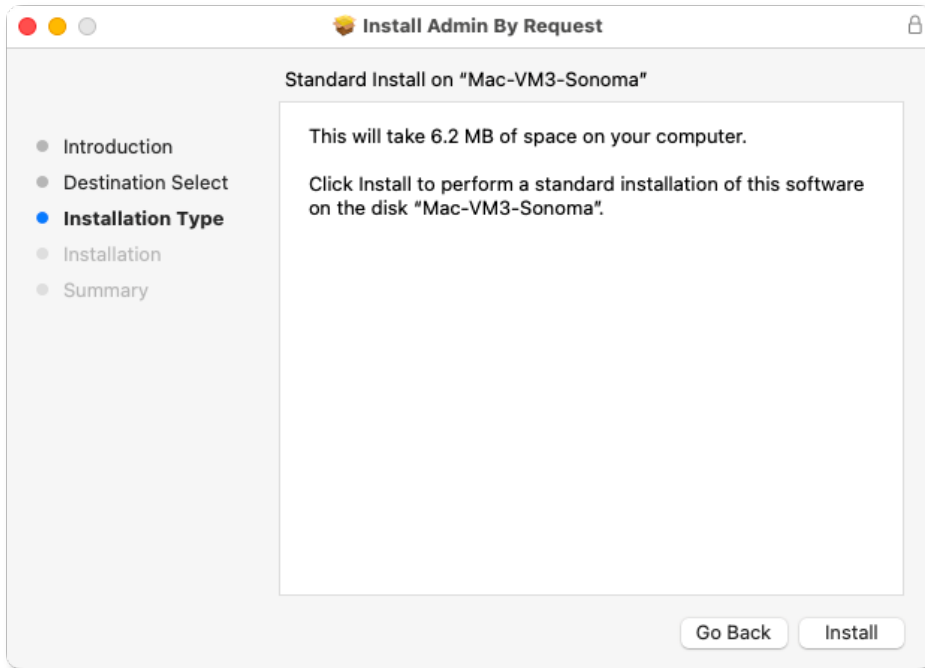
Download and install

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.

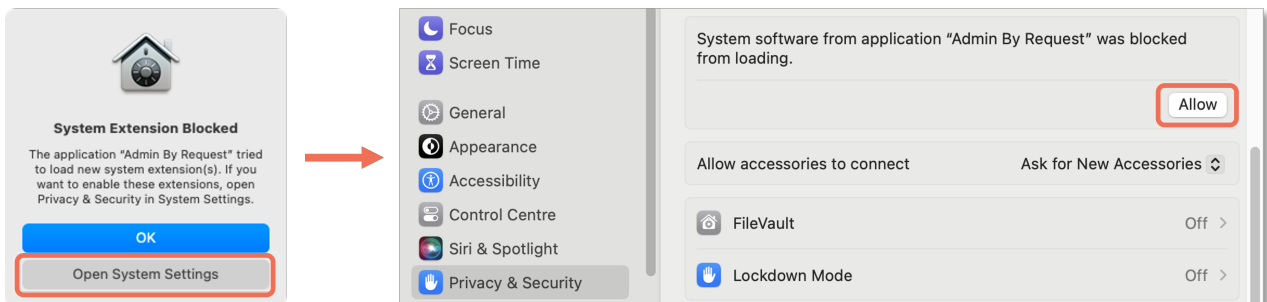
The package runs a check to determine if Admin By Request can be installed:



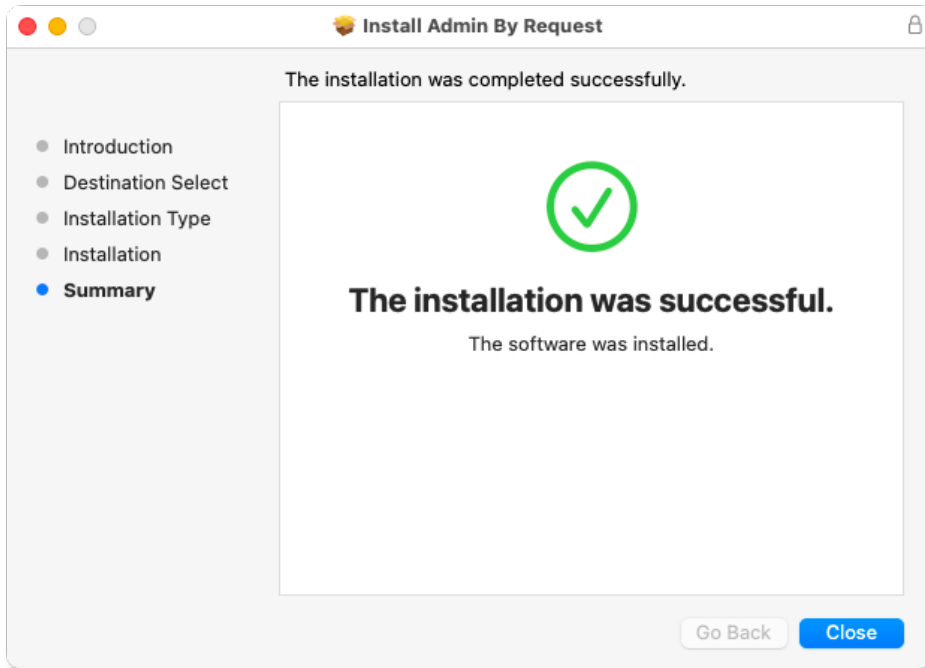
- Continue with the installation, providing Administrator credentials if necessary:



- If prompted with *System Extension Blocked*, click **Open System Settings** and allow system software from Admin By Request:



6. When done, close the installer and (optionally) move the installer package to the bin:



Installation is now complete. The next step is to ensure that Full Disk Access (FDA) is enabled for Admin By Request.

Enable FDA for two apps

Following installation of the Mac 5.0 endpoint client, there are two apps that need full disk access:

- **adminbyrequest** - The main app for enabling Admin By Request endpoint client features, including the ability to drag a file over the ABR icon in the dock to elevate privileges.
- **Admin By Request System Extension** - The extension app enables a range of functionality, but the main feature for Mac 5.0 is the ability to install an app by dragging its icon over the Applications folder. This requires operating system version macOS 11+.

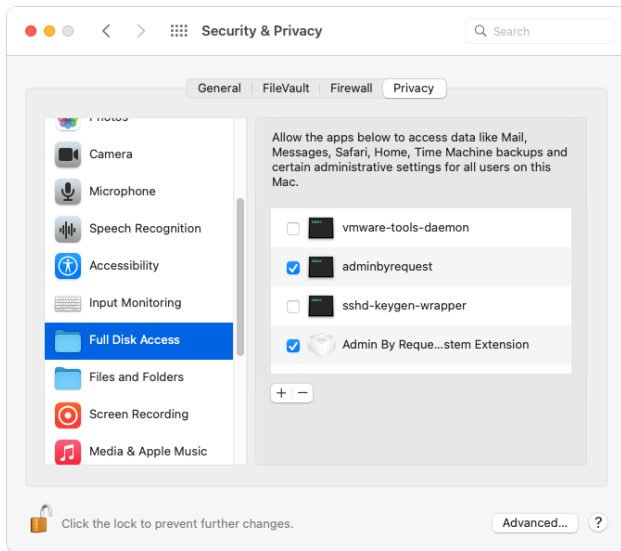
The procedure to enable FDA is slightly different for different macOS versions. The following steps describe how to enable FDA on Apple Macs running:

- macOS 10.15 (Catalina), macOS 11 (Big Sur) and macOS 12 (Monterey)
- macOS 13 (Ventura) and macOS 14 (Sonoma)

macOS 10.15 Catalina), macOS 11 (Big Sur) and macOS 12 (Monterey)

1. 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.

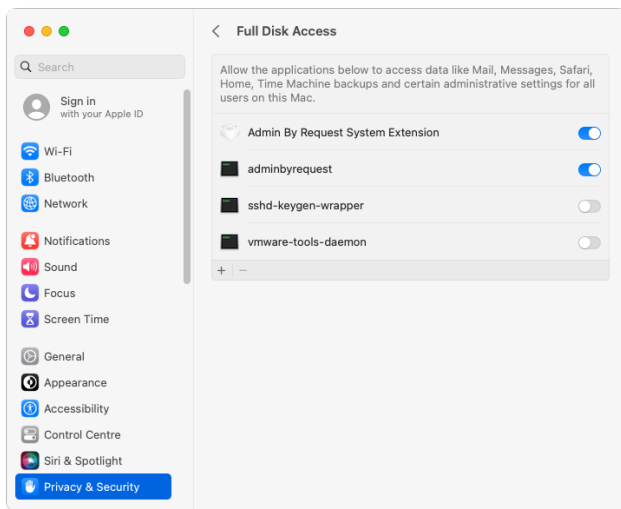
2. Select both **adminbyrequest** and **Admin By Request System Extension** in the list of apps (i.e. ensure the boxes are checked):



3. Lock the tab to save changes and close the System Preferences window.

macOS 13 (Ventura) and macOS 14 (Sonoma)

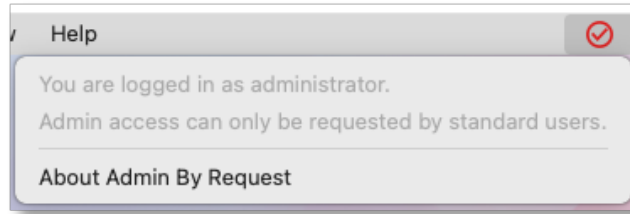
1. On your Mac device, navigate to **System Settings > Privacy & Security** tab and select **Full Disk Access** from the list. You'll need to supply your password to unlock and make changes.
2. Select both **adminbyrequest** and **Admin By Request System Extension** in the list of apps (i.e. ensure the toggles are on):



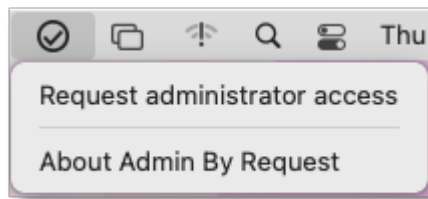
3. Close the System Settings window.

Test as a Standard User

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 the product is working.

Refer to "[Using Run As Admin](#)" on page 26 and "[Requesting Administrator Access](#)" on page 32 for more information on tasks that require elevated privileges.

Multiple endpoint installation (automated via MDM)

This procedure describes how to install the Admin By Request Mac client on multiple endpoints using an MDM such as Jamf or Intune. The examples here use Jamf but the same Code Requirements can be used with any MDM.

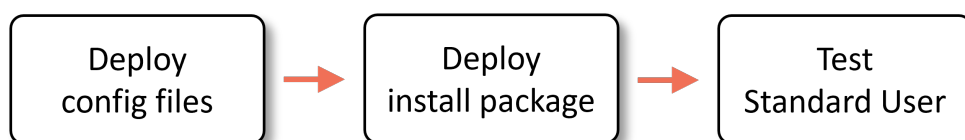
IMPORTANT:

For the Mac 5.0 client, we supply two configuration files to help with allowing the Admin By Request System Extension and enabling Full Disk Access for two apps. These are:

1. AdminByRequest - System Extension.mobileconfig
2. AdminByRequest - FDA PPPC_v2.mobileconfig

Download both in a zip file [here](#).

These configuration files must be deployed in your MDM scripts **before** installing (or upgrading to) Admin By Request Mac 5.0. Failure to do so means the new features in the Mac 5.0 client will not work.



Deploy config files using Jamf

The important step in this procedure is the last one - deploy the config profile. Skip the rest of this procedure unless you want to understand how the Admin By Request config files were created.

The config files supplied were built in Jamf as follows:

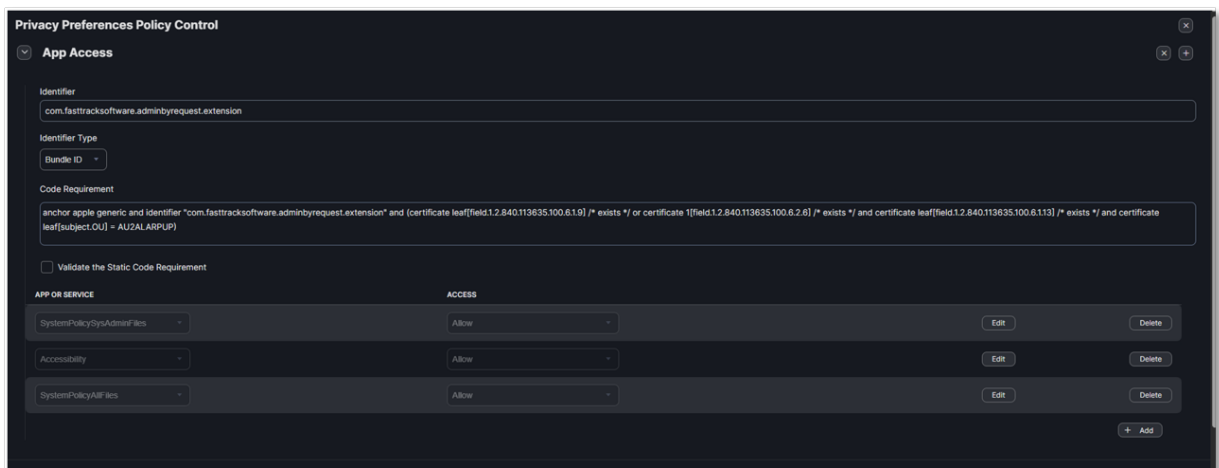
1. In Jamf, go to **Computers > Configuration Profiles**.
2. Create a new profile and configure it as follows:
 - a. *Name*: give the profile a name that helps explain what application it is giving rights to. In this example, we use **ABR - PPPC**.
 - b. *Category*, select **Applications**.
 - c. *Distribution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

```
anchor apple generic and identifier
"com.fasttracksoftware.adminbyrequest.extension" and (certificate leaf
[field.1.2.840.113635.100.6.1.9] /* exists */ or 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)
```

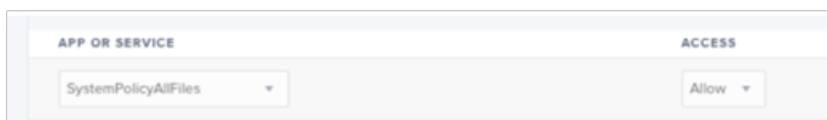
IMPORTANT:

The code snippet is all one line. When copying from this PDF document, make sure you remove all line breaks when entering into *Code Requirement*.

For example:



- d. Under *App or Service*, select **SystemPolicyAllFiles** and under *Access*, select **Allow**:



Under *App or Service*, select **Accessibility** and under *Access*, select **Allow**.

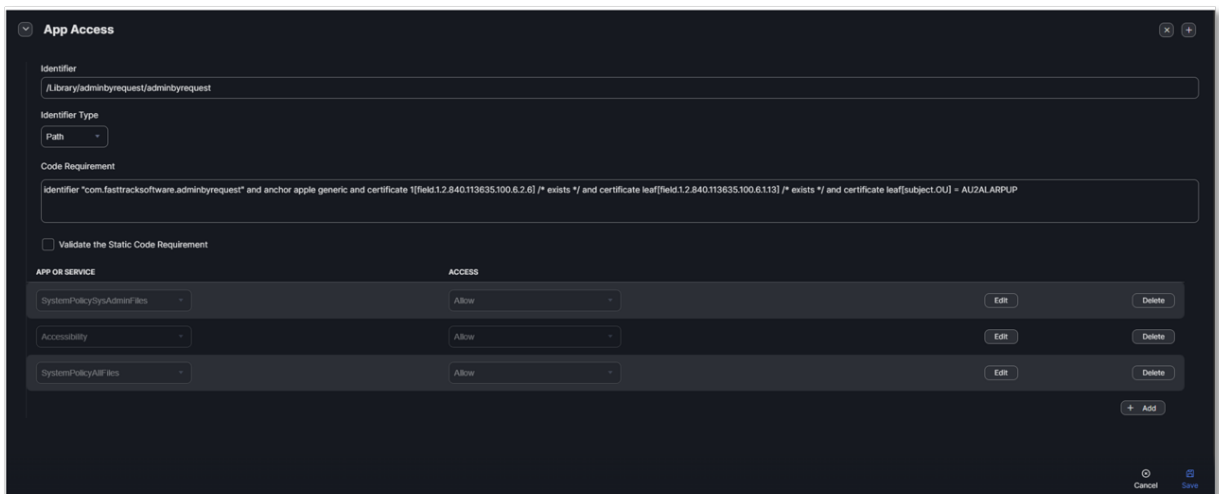
e. For *Code Requirement*, enter the following line of code:

```
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:

The code snippet is all one line. When copying from this PDF document, make sure you remove all line breaks when entering into *Code Requirement*.

For example:



f. Save the profile.

4. Deploy the profile using Jamf (or your MDM) to allow the System Extension and enable FDA for all your macOS endpoints.

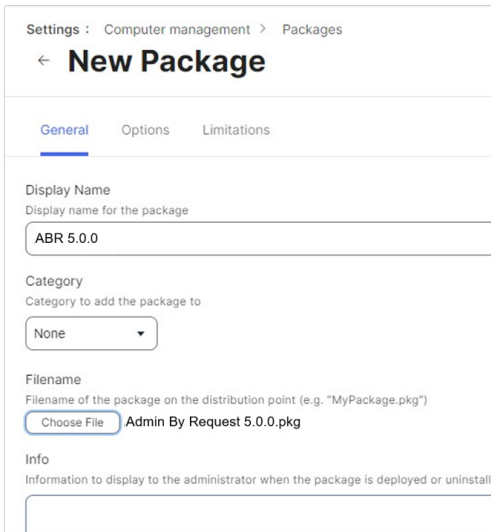
Download and deploy Admin By Request using Jamf

This procedure describes how to create and deploy an Admin By Request installation package.

Make sure that deployment of the installation package comes **after** deployment of the Admin By Request config files.

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. In Jamf, go to **Settings > Computer Management > Packages**.
4. Click **New** and enter a Display Name (e.g. **ABR 5.0.0**).

- Click **Choose File** and browse for the PKG downloaded from the ABR portal:



Settings : Computer management > Packages

← **New Package**

General Options Limitations

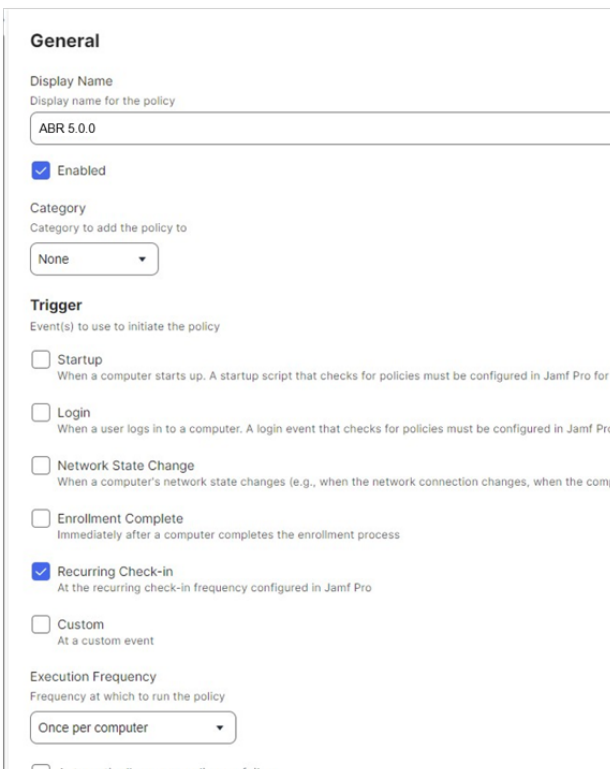
Display Name
Display name for the package
ABR 5.0.0

Category
Category to add the package to
None

Filename
Filename of the package on the distribution point (e.g. "MyPackage.pkg")
Choose File Admin By Request 5.0.0.pkg

Info
Information to display to the administrator when the package is deployed or uninstalled

- Click **Save**.
- Now create a new policy in Jamf.
Enter the *Display Name* from step 3 above and choose the relevant trigger for your deployment:



General

Display Name
Display name for the policy
ABR 5.0.0

Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for

Login
When a user logs in to a computer. A login event that checks for policies must be configured in Jamf Pro

Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the comp

Enrollment Complete
Immediately after a computer completes the enrollment process

Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

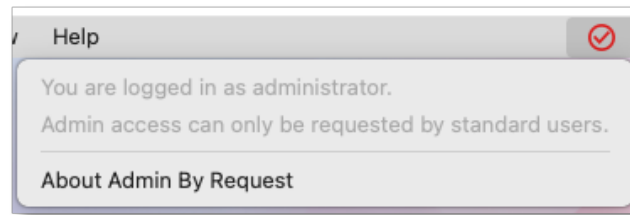
Custom
At a custom event

Execution Frequency
Frequency at which to run the policy
Once per computer

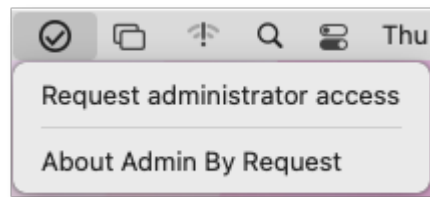
- Open **Packages**, and click **Configure**.
- Select the package just created and click **Save**.
- In *Scope*, choose the devices to which you want to deploy the ABR client.
- Deploy the package.

Test as a Standard User

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 the product is working.

Refer to ["Using Run As Admin" on page 26](#) and ["Requesting Administrator Access" on page 32](#) for more information on tasks that require elevated privileges.

Upgrading Admin By Request

You can manually upgrade any client immediately by simply installing the latest version, although upgrading endpoint client software occurs automatically when new versions are released.

Deploying new releases

Admin By Request software updates are deployed by 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 issues that arise after beta testing.

Our rule-of-thumb is to activate auto-update of new releases 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.

Refer to the [Download Archive](#) for previous versions of Admin By Request.

NOTE:

If your Macs are not auto-updating to the latest version of Admin By Request, check the currently installed version on your endpoints. There was an auto-update problem with macOS version **3.2.1** - any Macs running that version of ABR will need to be **manually updated**.

The problem has been fixed in later versions of Admin By Request (macOS client).

For more information

Refer to ["Synchronizing Clients with the Portal" on page 64](#) for a description of how endpoint clients communicate with the portal inventory.

Refer to [Release Notes \(macOS\)](#) for details on what is covered in each new release.

Uninstalling Admin By Request

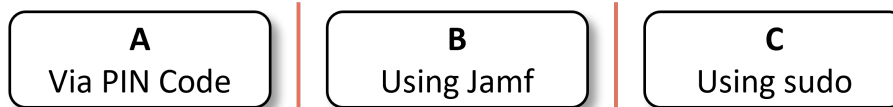
IMPORTANT:

If managing macOS endpoints using an MDM (e.g Intune, Jamf, Workspace ONE etc.), a post-uninstall script might be needed to revert at least one user account to admin permissions on each affected endpoint *after* completing the uninstall steps below.

This will be required only if all accounts have been downgraded to standard users. Check your Mac Settings in the portal (Lockdown > Admin Rights). If setting *Revoke admin rights* is **On** and there are **no** excluded accounts, then *all* accounts on each managed endpoint will have been downgraded.

Once Admin By Request is removed, the post-uninstall script needs to promote at least one account to admin permissions. Refer to (external) page [Script to revoke or grant admin rights to standard users in macOS](#) for an example.

The following procedures describe three ways to uninstall Admin By Request on a Mac:



These procedures are not sequential - pick one or a combination of all three, depending on your requirements.

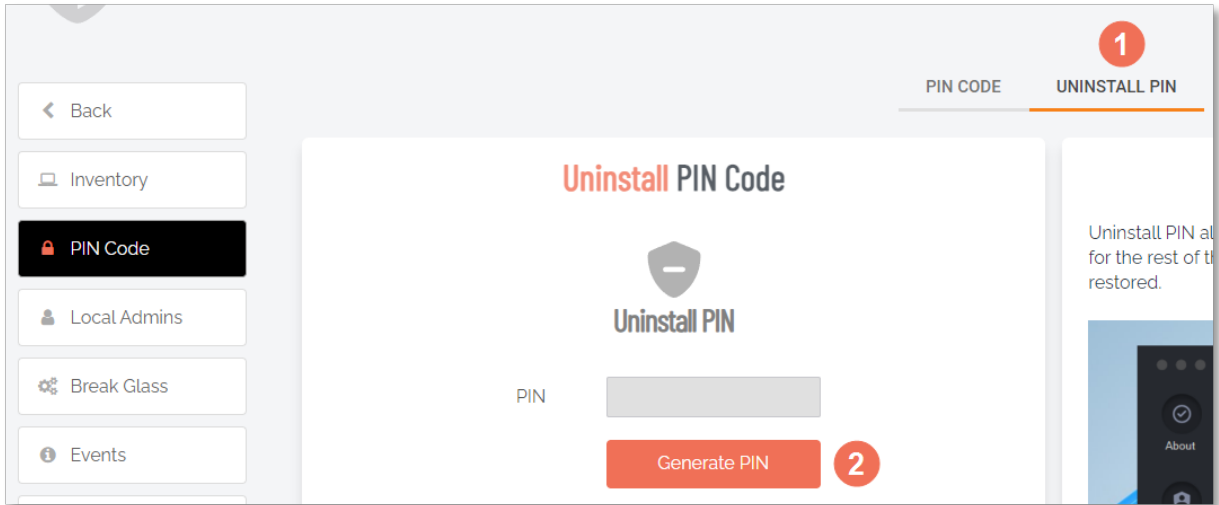
A. Via portal PIN Code - uninstall.

The first few steps in this procedure require access to the portal.

1. In the Admin By Request portal, navigate to the *Inventory* page and identify the device on which to perform the uninstall.
2. Locate the device in the inventory list - in the PIN column, click **PIN** for that device (columns can be switched around - the PIN column in your portal might not be the right-most column):

Computer Inventory										
Computer	User	Operating system	Model	SW	Remote	PIN	Details			
EDITH	Steve	Windows 10 Pro	Precision M6700	8.3.3		PIN	Details			
HUGH	Steve	Windows Server 2008 R2 Datacenter	Studio 1735	8.3.1	Remote	PIN	Details			
LATITUDE-E6540	Steve Dodson	Ubuntu 20.04.6 LTS	Latitude E6540	3.1.9		PIN	Details			
OLIVIAS-MAC	Olivia Lim	macOS 12 Monterey	VMware 20.1	5.0.0		PIN	Details			
PETER-VM	Peter Bloggs	Ubuntu 22.04.4 LTS	VMware Virtual Platform	3.1.10		PIN	Details			

- Click tab **UNINSTALL PIN** and then click button **Generate PIN**:



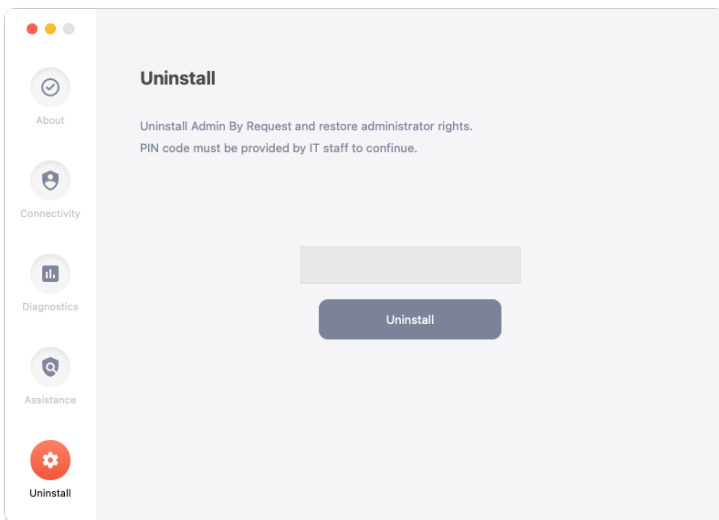
Note that clicking **UNINSTALL PIN** also displays a list of previous uninstall events on this computer (below the *Uninstall Pin Code* window):

Uninstall PIN Events On OLIVIAS-MAC						
Drag a column header here to group by column or click the funnel icon to filter						
Your Time	Event	Account	Name	Endpoint Time		
01-08-2024 10:51:57	Uninstalled by PIN code	OLIVIAL	olivial	01-08-2024 10:51:57		
01-08-2024 10:51:43	Uninstall PIN issued		Steve	31-07-2024 22:51:43		

Page 1 of 1 (2 items) Page size: 25

Export to PDF Export to XLSX Export to CSV (j) Export to CSV (j)

- Copy the PIN.
- Back on the device on which you want to uninstall Admin By Request, go to the *About* panel (i.e. select the *Admin By Request* icon from the top menu bar and click **About Admin By Request**).
- In the *Uninstall* window, select **Uninstall** from the left button group, enter the PIN copied from the Portal, and click **Uninstall**:



B. Using Jamf - uninstall

In this example, *Remove ABR* is the script and *Remove ABR TEST* is the policy.

1. Create a script in Jamf.
Go to **Settings > Computer Management > Scripts** and click **New Script**.
2. Enter a name for the script and open it:

General Script Options Limitations

Display Name
Display name for the script

Remove ABR

Required

Category

3. For *Mode*, select **Shell/Bash**, and enter **/Library/adminbyrequest/uninstall**:

Settings : Computer management > Scripts

← **Remove ABR**

General Script Options Limitations

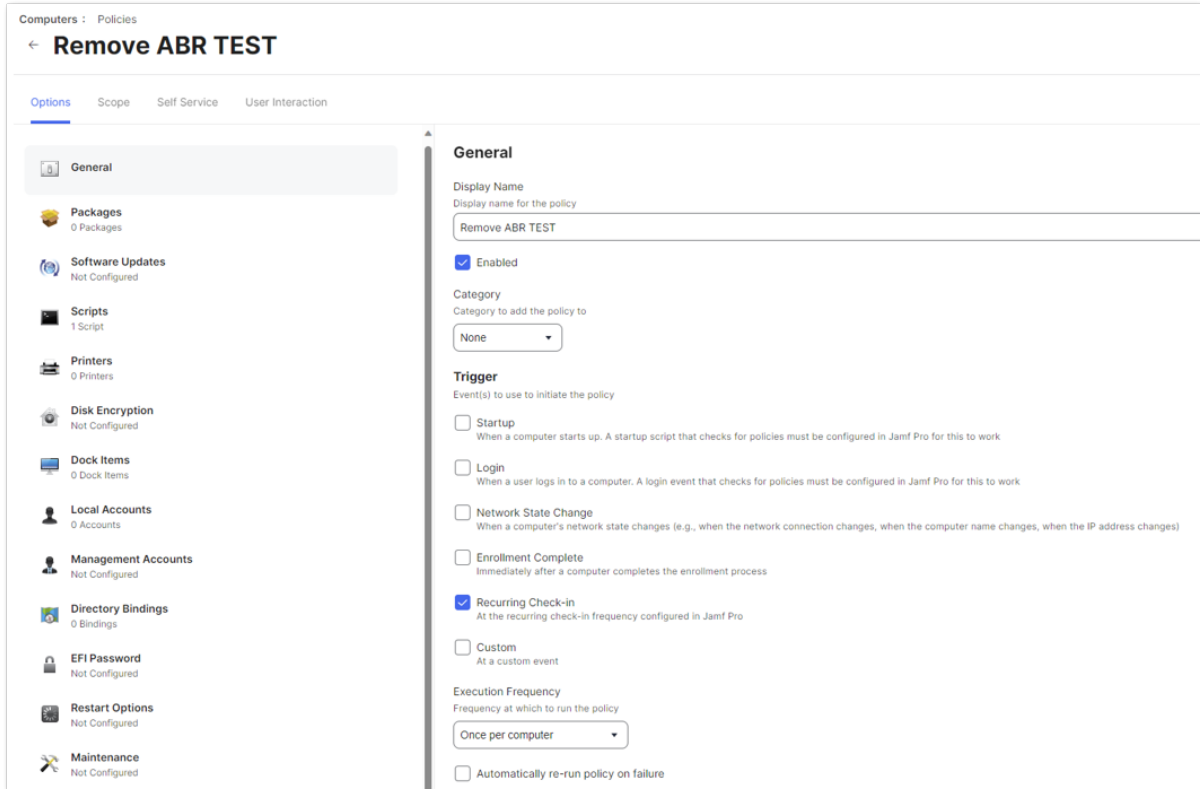
Mode Theme

Shell/Bash Default

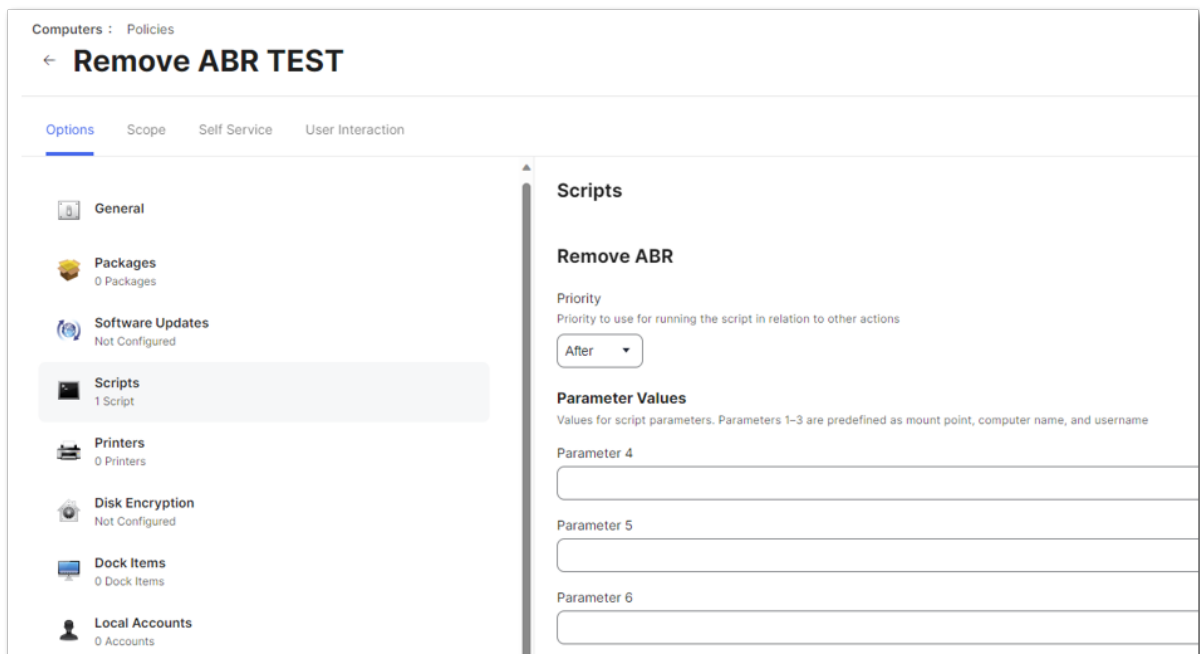
1 /Library/adminbyrequest/uninstall

4. Click **Save** to save the script.
The next step is to create a policy for deployment of the uninstall script (see next page).

5. Enter a display name for the policy and choose an appropriate trigger for your deployment:

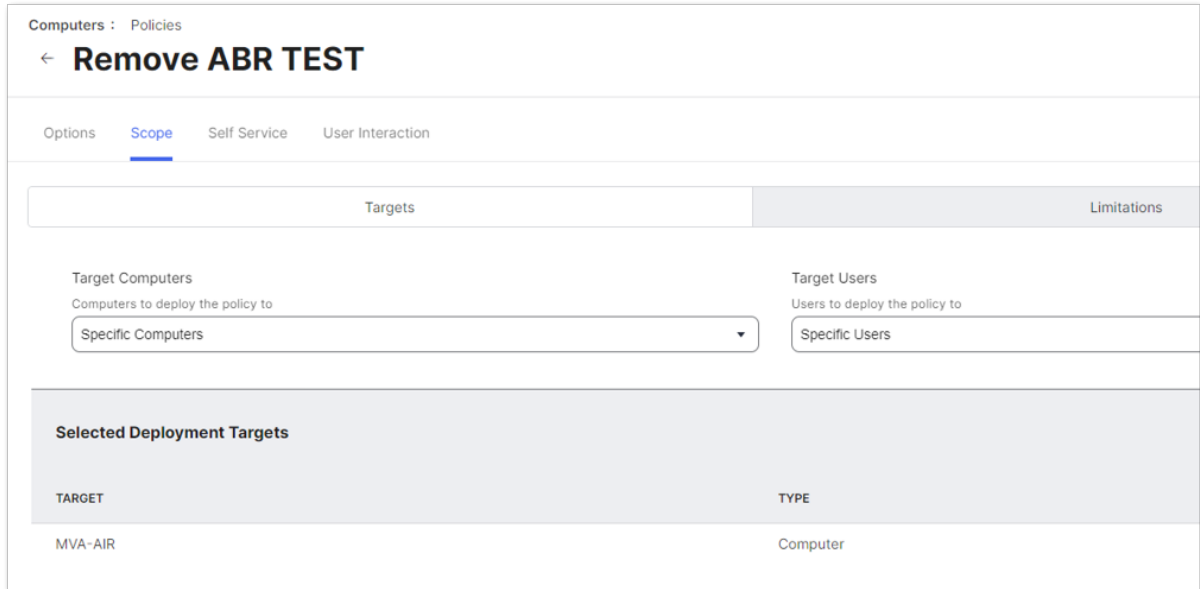


6. Open **Scripts**, and click the + symbol to add:



7. Add your uninstall script and click **Save**.

8. Scope deployment of the script to the correct devices:



C. Using sudo - uninstall.

Uninstallation using sudo is straightforward for an admin user and simply requires executing an uninstall program once sudo is authorized.

NOTE:

The program cannot be run by a standard user during an Admin By Request administrator session. You need to log in as an admin user and also check/modify certain Mac settings in the portal.

1. Login to the portal and go to **Settings > Workstation Settings > Mac Settings**.
2. Select **Lockdown** in the vertical menu at left and check the *Excluded accounts* list.
3. If your admin 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
```

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 (**EPM > Settings > Mac 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 a domain administrator.

Please refer to "[Supplementary Technical Information](#)" on page 57 for more information.

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.

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 Mac Client User Interface

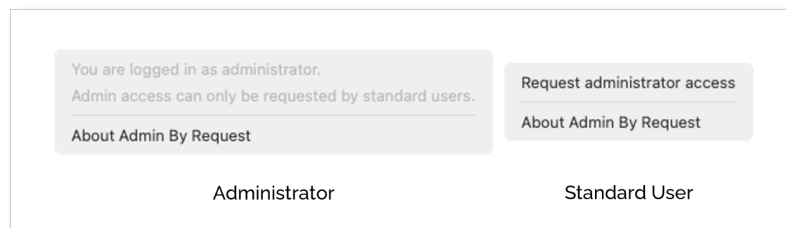
Introduction

The user interface is graphical and is accessed via the icon menu in the menu bar (top right) of the screen.

The color of the icon depends on the currently logged-in user: if the user is an administrator, the icon is red, whereas if the user is a standard user, the icon is black:



Click the icon to display the menu and select *About Admin By Request* for further information (Administrator and Standard User) or *Request Administrator Access* to carry out an admin task (Standard User only):



In this topic

["About Admin By Request" on the next page](#)

["Submitting Diagnostics" on page 22](#)

["Requesting Assistance \(Support Assist\)" on page 22](#)

["Uninstalling via PIN Code" on page 25](#)

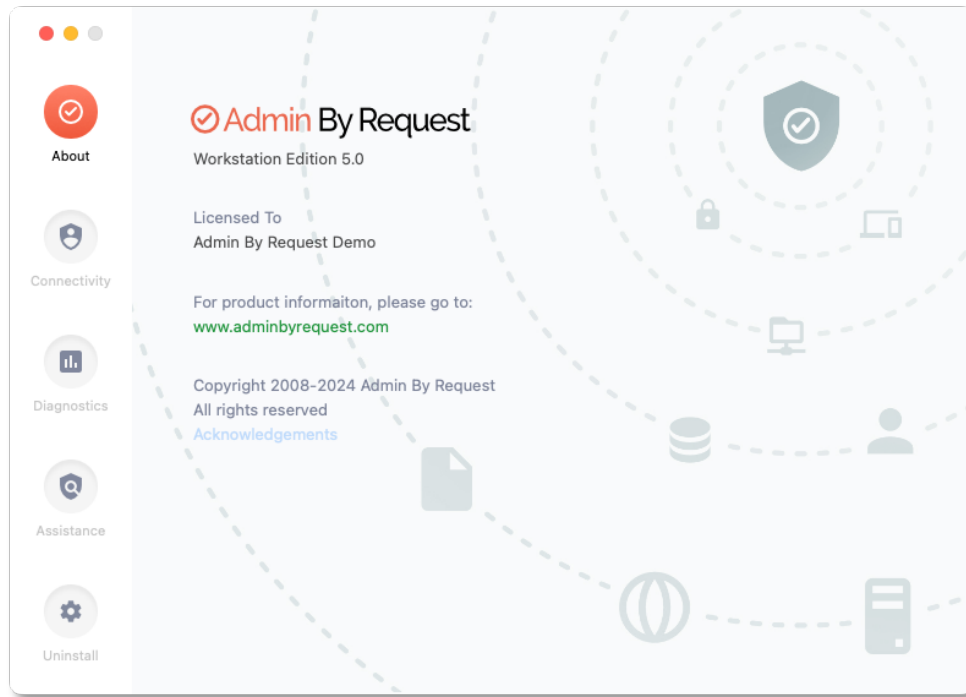
["Using Run As Admin" on page 26](#)

["Requesting Administrator Access" on page 32](#)

["Setting-up a Break Glass Account" on page 34](#)

About Admin By Request

Once installed, Admin By Request is running in the background for as long as the endpoint is powered-on. Selecting the app from the menu bar or the dock launches the *user interface*, which comprises a simple window with four buttons down the left-hand side:



The default panel is *About Admin By Request*, which is accessed via the top button. It shows the following information:

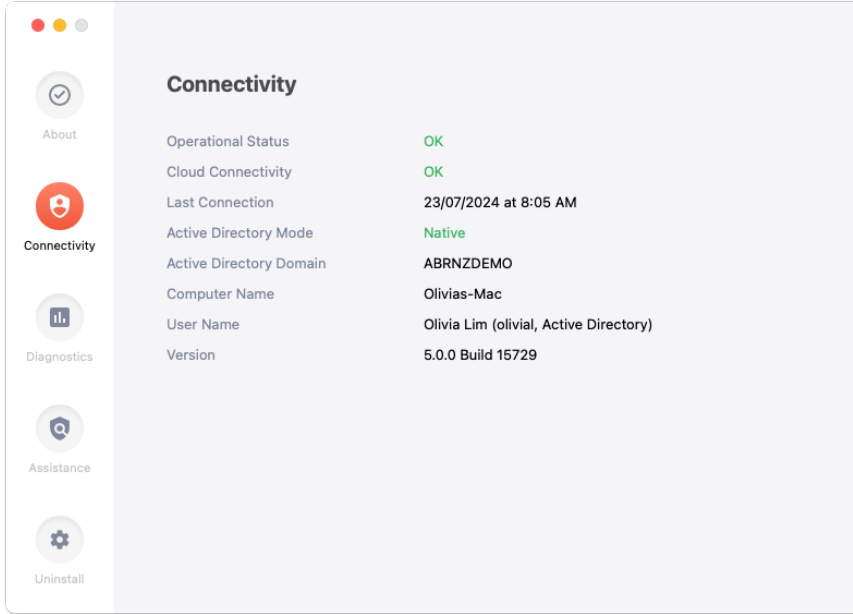
- Current workstation edition
- License details - this information matches the organization details in the portal
- Website link
- Copyright information

Other panels presented in the user interface are accessed via buttons at the left. Clicking a button opens its corresponding panel and clicking the **About** button gets back to the default panel if viewing one of the others.

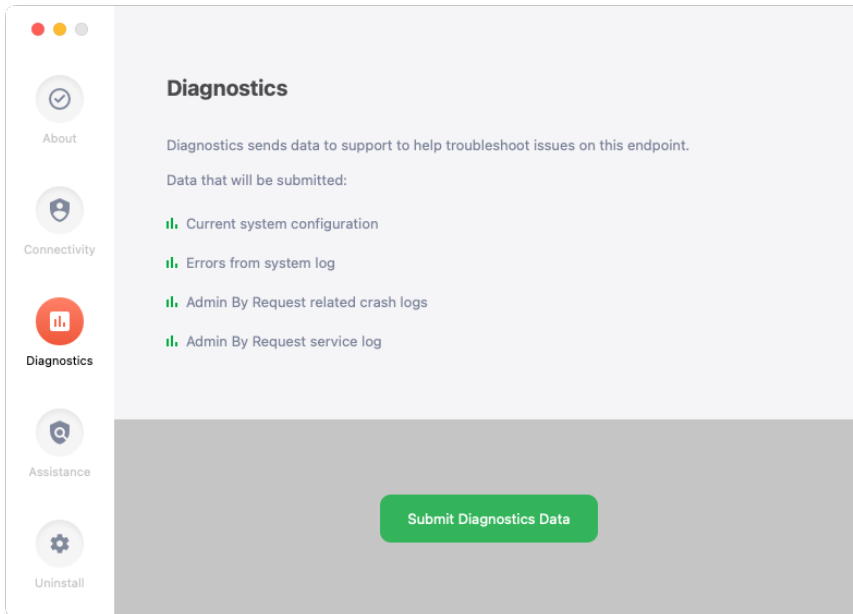
Panels are shown on the following two pages.

Other Panels

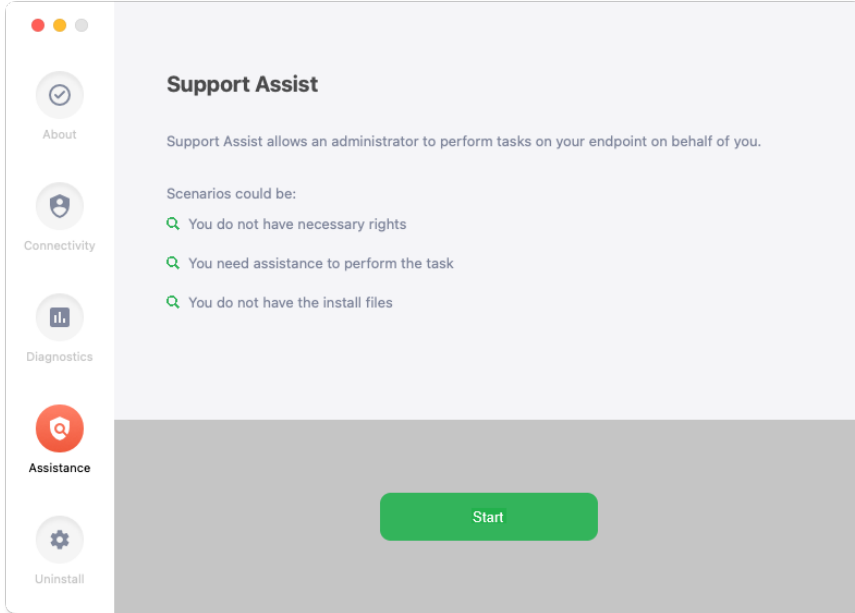
- **Connectivity** – displays the current operational status of the Admin By Request system, including Internet and Cloud connectivity, and details about the current workstation and user:



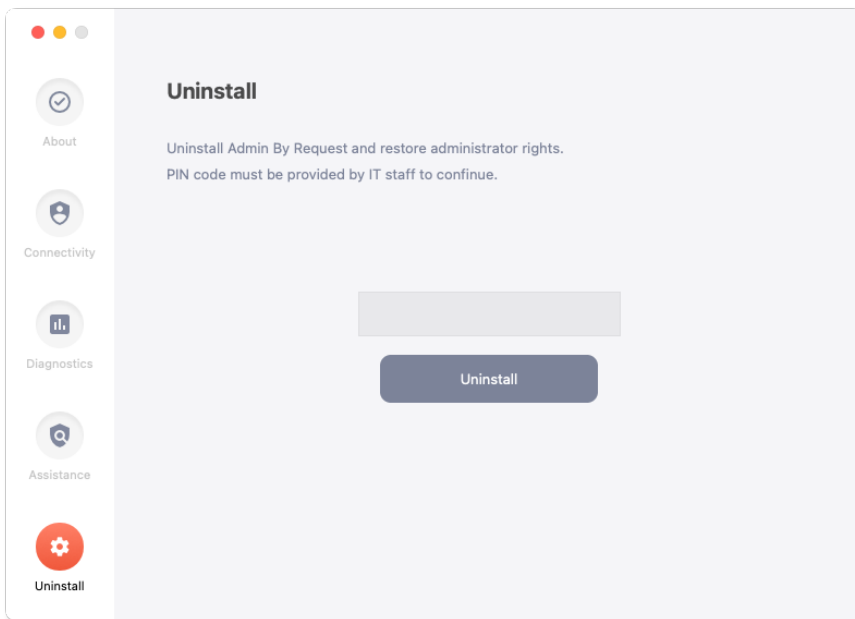
- **Diagnostics** – provides a way to send useful diagnostic data on this workstation to the ABR support team (see "[Submitting Diagnostics](#)" on page 22 for more information):



- **Assistance** - (Standard User only) allows users to ask a *knowledgeable support person* to access the endpoint remotely and carry out tasks on the user's behalf (see "[Requesting Assistance \(Support Assist\)](#)" on the next page for more information):



- **Uninstall** – enables administrators to uninstall Admin By Request from this workstation. See "[Uninstalling via PIN Code](#)" on page 25 for more information:



Submitting Diagnostics

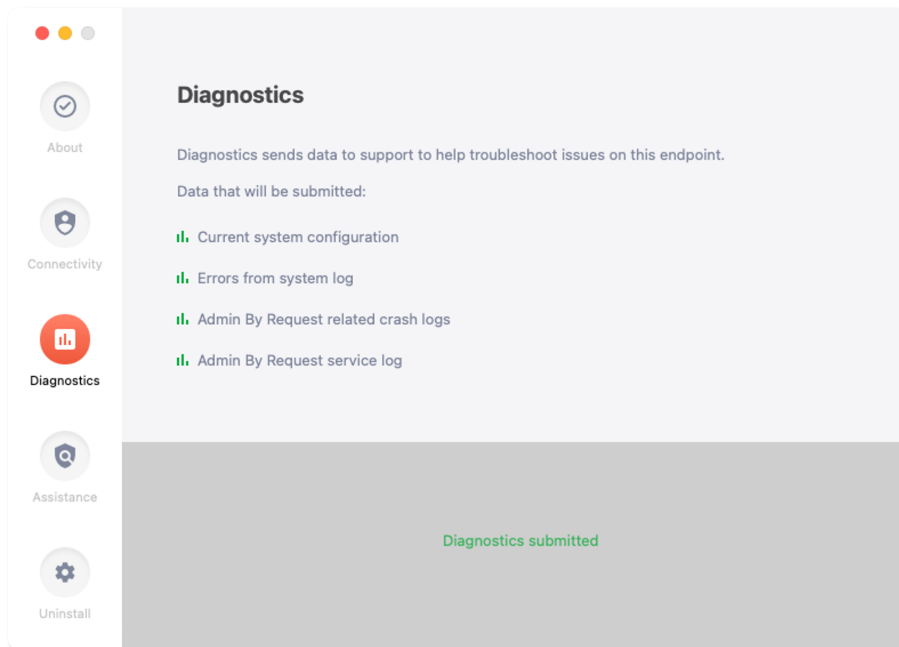
Diagnostic information is available on each endpoint that has Admin By Request installed. The details recorded help IT administrators and the Admin By Request support team to troubleshoot issues that might be occurring.

The following data is recorded and submitted:

- Current system configuration
- Errors from the system log
- Admin By Request-related crash logs
- Admin By Request service log

To send diagnostic information about how Admin By Request is running on this workstation, select the **Diagnostics** button on the *About Admin By Request* panel and click **Submit Diagnostics Data**.

The button changes to text *Diagnostics submitted*, indicating that diagnostics have been sent for analysis:



NOTE:

It's a good idea to submit diagnostics when raising a support ticket for a new issue. The Admin By Request support team will frequently ask for diagnostics when responding to tickets if the information is not already available.

Requesting Assistance (Support Assist)

Assistance (also known as *Support Assist* or *Remote Assist*) is a feature that allows users to ask for help from someone who can use a third-party tool to connect remotely to the user's computer and provide technical assistance with tasks that the logged-on user would not normally be able to complete.

Support Assist has been designed to be used with a **non-admin user**, so that customers can apply the best practice "principle of least privilege" to help desk staff as well as end users. The non-admin user helps the logged-on user (also non-admin) to carry out a task with less restrictive settings than the logged-on user during a remote control session.

IMPORTANT:

At the time of writing, *Support Assist* is available only to users logged-in under **Azure SSO**. *Support Assist* does not establish a remote control session - a third-party tool must be used for that.

The following scenarios are examples of when this might be useful:

- End users who are not allowed to install software at all (i.e. neither *Run As Admin* nor *Admin Sessions* are enabled).
- End users who don't know where to get the software they need to use.
- End users who are not IT savvy enough to self-service.
- End users who refuse to take on the responsibility of installing software on their work computers, knowing they will be audited.

Assistance example scenario

An example of the first scenario could be in Customer Relations, where users do not need to install software by default. When the time inevitably arrives that new or upgraded software is required, they have to call your help desk. If the request is accepted, a help desk staff member can assist by connecting remotely and using screen sharing with the end user.

Let's take this scenario and say Customer Relations employee, Olivia, calls Steve at the help desk to assist with a task for which Olivia does not have privileges, but Steve does.

There are several (problematic) ways this could be solved *without* the Support Assist feature, with or without Admin By Request:

1. Steve could have a local administrator account to all computers. However, this is an absolute security no-no and there is no auditing.
2. You could have Microsoft's Local Administrator Password System (LAPS) in place, but this also lacks proper auditing and doesn't work without a LAN or VPN connection.
3. Olivia and Steve could agree to use the Admin By Request feature *Run As Admin* and use Olivia's credentials, but then Olivia gets audited for Steve's changes.
4. Steve could log on and use *Run As Admin*, but then Steve gets audited for Olivia's request and furthermore, Olivia cannot see Steve executing the request.

Ideally, Steve should execute the request with Olivia watching and auditing should clearly show that Olivia requested the change and Steve executed it.

If you have a change management or ticketing system, you would also want a reference to document this change. This is exactly what the Support Assist feature does.

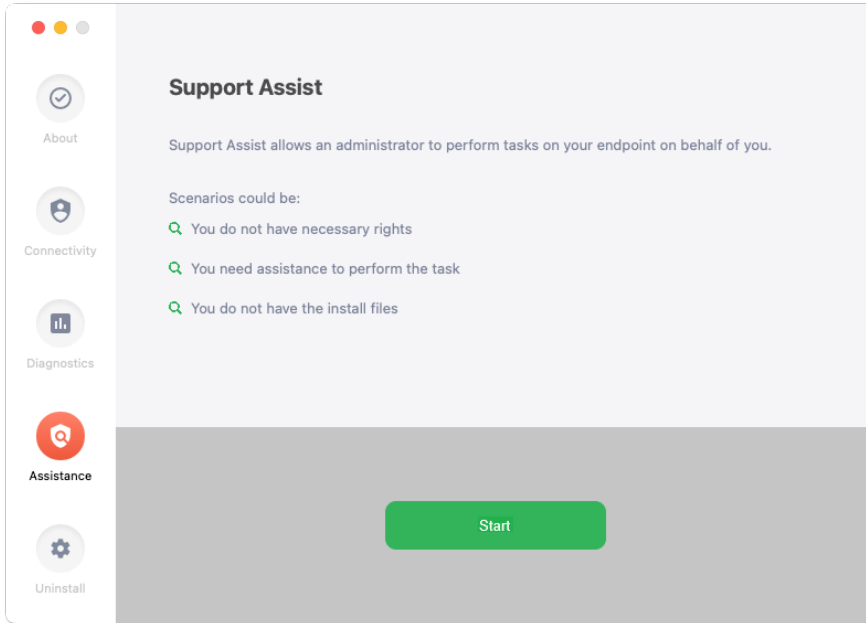
Multi-Factor Authentication (MFA)

If MFA is enabled (EPM > Settings > Mac Settings > Endpoint > AUTHENTICATION), the support person (i.e. Steve) must authenticate using MFA.

Refer to [Mac Settings \(Authentication tab\)](#) for more information.

Assistance sequence

1. Olivia submits a request for help to the Help Desk.
2. Steve is assigned the task and connects remotely to Olivia's computer using a third-party application.
3. Steve starts Admin By Request, selects **Assistance** from the About panel and clicks **Start**:



4. At the *UAC Support Assist* window, Steve enters his own **User account** and **Password** credentials.
5. The session starts, indicated by a progress timer, which displays for the duration of the session.
6. When the assist task is complete, Steve clicks **Done**. If he forgets, Olivia can click done before the timer counts down, or it will simply expire. Note that Olivia cannot use her credentials while Steve is signed-in to Admin By Request.

Security checks

Is it risky if a user finds and clicks the *Start* button from the Assistance panel? No - the UAC window at step 4 checks the credentials supplied to see if the person logging-on has the necessary privileges to carry out the task. If they don't, the task is denied and this is logged.

For Help Desk employee Steve, it is essentially the same as logging in to Windows: whatever Admin By Request settings are in effect for Steve are also in effect when he uses Support Assist. For example, if Steve is not allowed to start an Admin Session, he is also not allowed to while using Support Assist.

Think of Support Assist as a shortcut to logging in to Windows and starting Admin By Request. If someone who is not from the Help Desk uses this feature, nothing is achieved as this would be the same as if this user was simply logging in to Windows.

Uninstalling via PIN Code

Offline users can obtain a challenge/response PIN, which allows the user to perform tasks requiring elevated privileges. A PIN Code can also be used to uninstall Admin By Request when online and this is the purpose of the Uninstall panel in the *About Admin By Request* window.

The first few steps in this procedure require access to the portal.

1. In the Admin By Request portal, navigate to the *Inventory* page and identify the device on which to perform the uninstall.
2. Locate the device in the inventory list - in the PIN column, click **PIN** for that device (columns can be switched around - the PIN column in your portal might not be the right-most column):

Computer	User	Operating system	Model	SW	Remote	PIN	Details
EDITH	Steve	Windows 10 Pro	Precision M6700	8.3.3		PIN	Details
HUGH	Steve	Windows Server 2008 R2 Datacenter	Studio 1735	8.3.1	Remote	PIN	Details
LATITUDE-E6540	Steve Dodson	Ubuntu 20.04.6 LTS	Latitude E6540	3.1.9		PIN	Details
OLIVIAS-MAC	Olivia Lim	macOS 12 Monterey	VMware 20.1	5.0.0		PIN	Details
PETER-VM	Peter Bloggs	Ubuntu 22.04.4 LTS	VMware Virtual Platform	3.1.10		PIN	Details

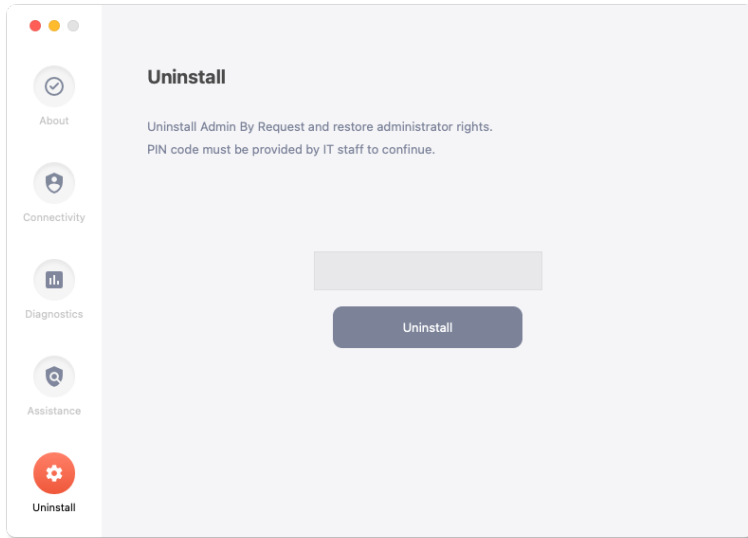
3. Click tab **UNINSTALL PIN** and then click button **Generate PIN**:

Note that clicking **UNINSTALL PIN** also displays a list of previous uninstall events on this computer (below the *Uninstall Pin Code* window):

Your Time	Event	Account	Name	Endpoint Time
01-08-2024 10:51:57	Uninstalled by PIN code	OLIVIAL	olivial	01-08-2024 10:51:57
01-08-2024 10:51:43	Uninstall PIN issued		Steve	31-07-2024 22:51:43

4. Copy the PIN.

5. Back on the device on which you want to uninstall Admin By Request, go to the *About* panel (i.e. select the *Admin By Request* icon from the top menu bar and click **About Admin By Request**).
6. In the *Uninstall* window, select **Uninstall** from the left button group, enter the PIN copied from the Portal, and click **Uninstall**:



Using Run As Admin

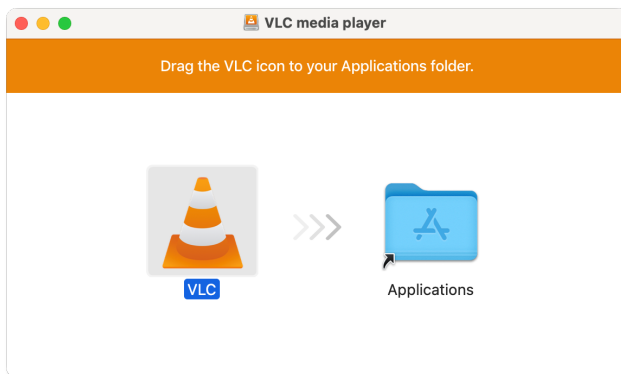
Run As Admin (also known as *App Elevation*) allows for the elevation of a single application.

This capability negates the need for users to initiate an *Admin Session*. Elevating privileges for execution of a single file is the much safer option compared to elevating the user's privileges across the endpoint.

Example 1 - Install app VLC

A standard user, requiring elevated privileges to execute the VLC installation program, initiates the following sequence of events:

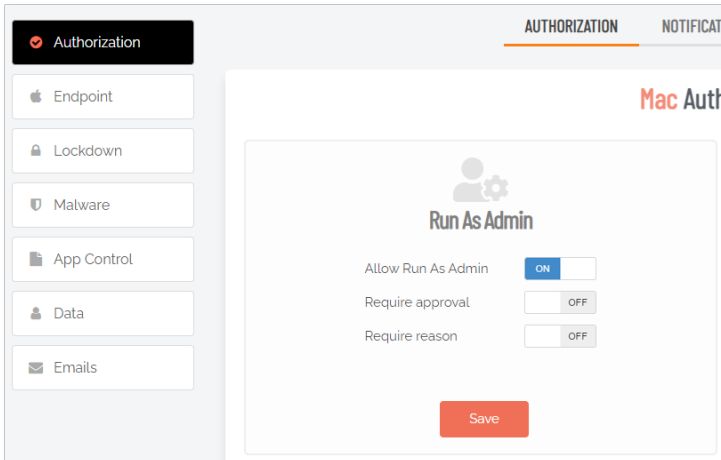
1. Download the package or application file for installation.
2. Start the installation by opening the **Downloads** folder and dragging the VLC icon to the **Applications** folder. If the download is a **.dmg** file, double-click it first to mount it:



If a warning about VLC being downloaded from the Internet pops-up, click **Open** to continue.

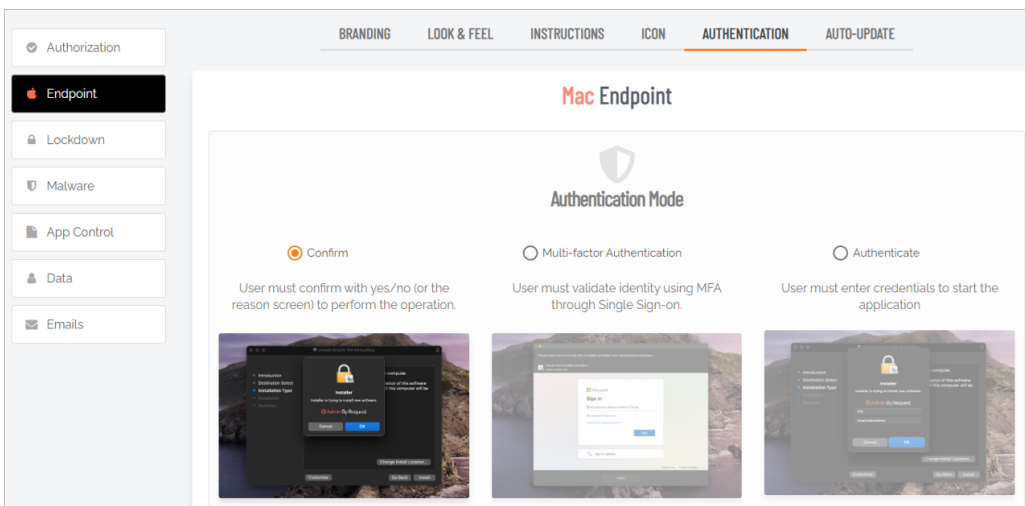
3. Admin By Request suspends installation and checks the organization's portal settings.

a. **EPM > Settings > Mac Settings > Authorization > AUTHORIZATION:**

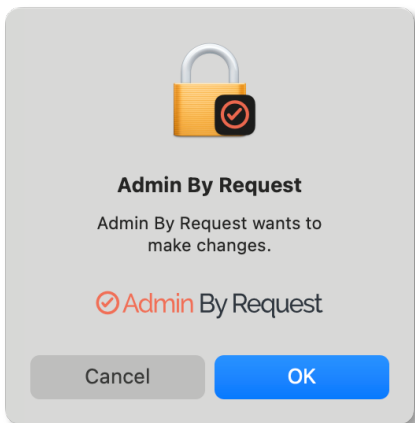


Authorization (i.e. approval) is not required, so installation can proceed. This is also the case when approval *is* required, but the app is pre-approved.

b. **EPM > Settings > Mac Settings > Endpoint > AUTHENTICATION:**



Authentication is *always* required and the mode in this case is **Confirm**. so the following prompt is displayed and the user simply has to click **OK** to continue:



- Once authenticated, installation proceeds to completion and Admin By Request displays a note from the application installer saying that installation has completed successfully.

After installation, portal administrators can check the audit log in the portal for details on the user, the endpoint, the application and execution history:

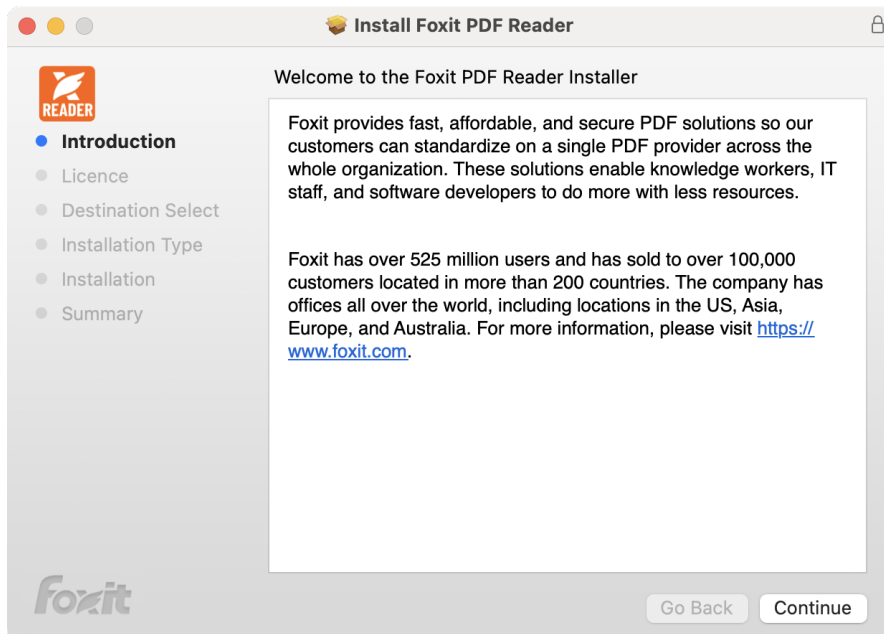
The screenshot displays the audit log for a VLC media player installation. The interface is organized into several sections:

- Summary:** Application: VLC media player, User: Rose Smith, Computer: Roses-Mac, Time: 13-08-2024 12:27:37, Duration: 00:03:00, Activity: 1/0/0, Status: Finished.
- Contact Information:** Full name: Rose Smith, User account: rosesmith, Approval: Not required.
- Application:** Name: VLC media player 2.2.8, Vendor: VideoLAN, File name: VLC.app, Path: /Volumes/vlc-2.2.8.
- Execution:** Start time: 13-08-2024 12:27:37, End time: 13-08-2024 12:30:37, Duration: 00:03:00, Settings: Global Settings, Trace no: 204264777.
- Actions:** Malware scan: Not available, Virustotal: Check status, AI assistance: Ask ChatGPT what this is, Pre-approve: Pre-approve this file, Block: Block this file.
- Installed or uninstalled software:** A table showing the installation of VLC (Version 2.2.8, Publisher VideoLAN).

Example 2 - Install app Foxit PDF Reader

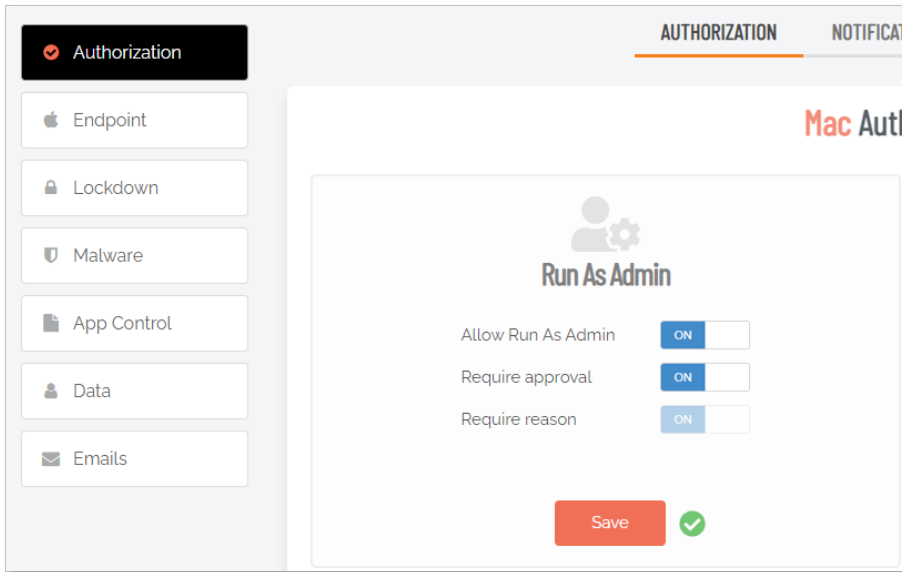
A standard user, requiring elevated privileges to execute the Foxit PDF Reader installation program, initiates the following sequence of events:

1. Download the package or application file for installation.
2. Start the installation by opening the **Downloads** folder and double-clicking the **.pkg** file:

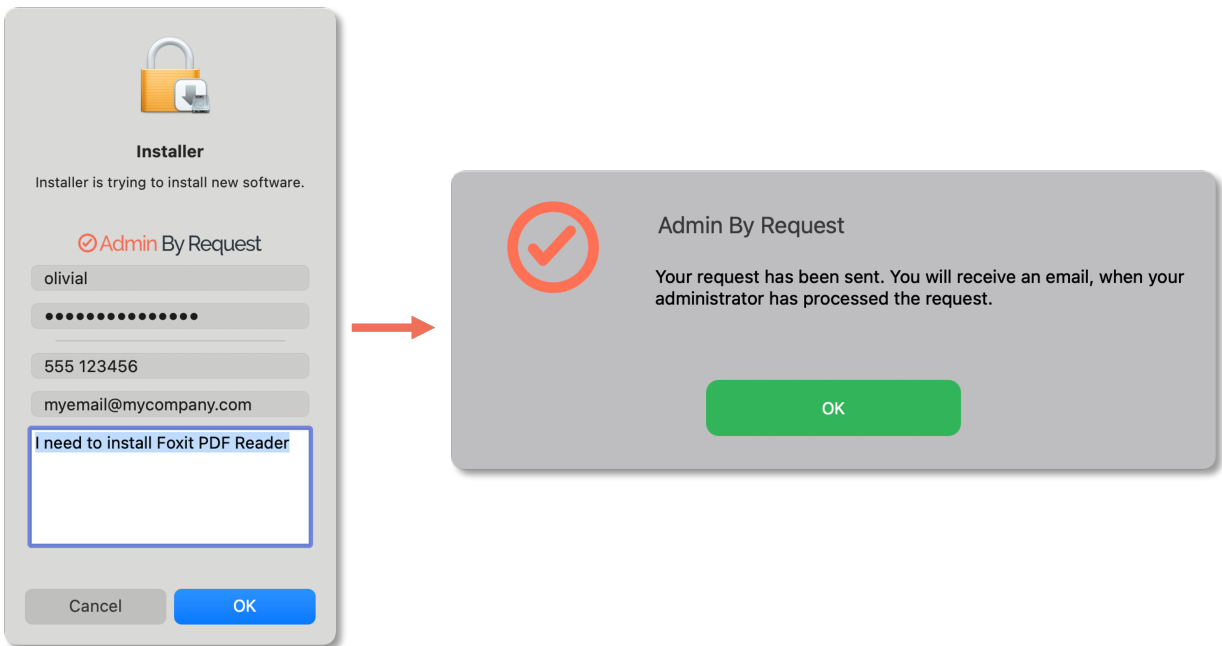


3. Admin By Request suspends installation and checks the organization's portal settings.

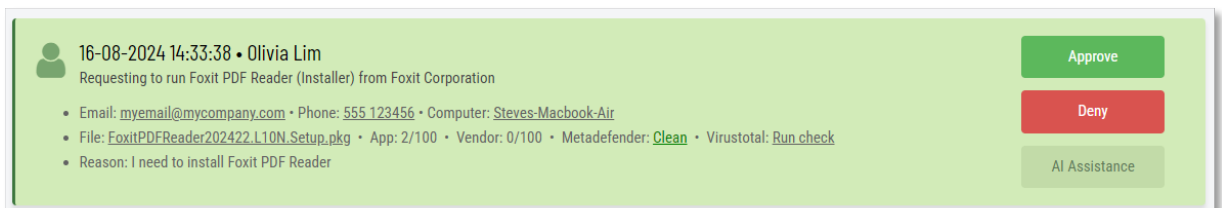
a. **EPM > Settings > Mac Settings > Authorization > AUTHORIZATION:**



Authorization (i.e. approval) is required, so Admin By Request prompts for phone, email address and reason. This information is submitted for approval and the user is advised they will be notified via email when approved:

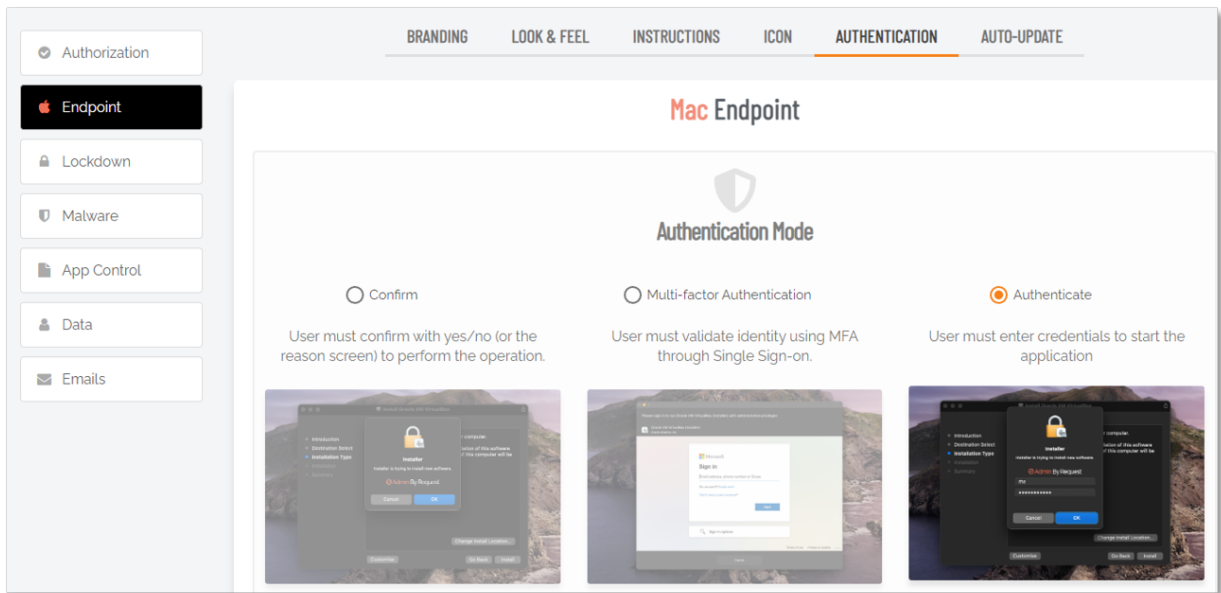


A portal administrator receives the request and approves it:

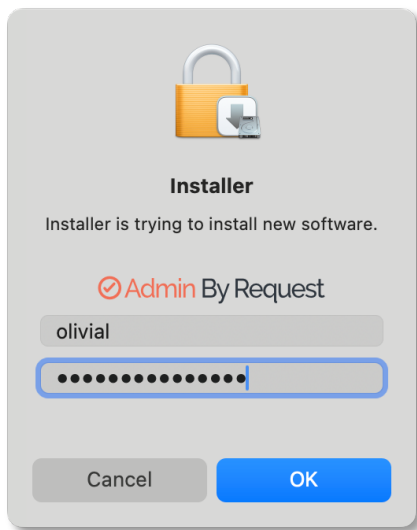


When approval arrives via email, the user can continue the installation with authentication (step **3.b** below).

b. **EPM > Settings > Mac Settings > Endpoint > AUTHENTICATION:**



Authentication is *always* required and the mode in this case is **Authenticate**, so the following prompt is displayed and the user must supply credentials to continue:



- Once authentication is provided, installation proceeds to completion and Admin By Request displays a note from the application installer saying that installation has completed successfully.

After installation, portal administrators can check the audit log in the portal for details on the user, the endpoint, the application and execution history:

The screenshot displays the audit log for a 'Foxit PDF Reader (Installer)' application. The interface is divided into several sections:

- Contact Information:**
 - Full name: Olivia Lim
 - User account: OLIVIAL
 - Email: myemail@mycompany.com
 - Phone: 555 123456
 - Approved by: Steve Dodson
 - Response In: 00:02:52
 - Reason: I need to install Foxit PDF Reader
- Execution:**
 - Start time: 16-08-2024 14:37:34
 - End time: 16-08-2024 14:52:10
 - Duration: 00:14:36
 - Settings: Global Settings
 - Trace no: 205067565
- Application:**
 - Name: Foxit PDF Reader (Installer)
 - Vendor: Foxit Corporation
 - File name: FoxitPDFReader202422.L10N.Setup.pkg
 - Path: /Users/olivial/Downloads
- Actions:**
 - Malware scan: [Unknown](#)
 - Virusotal: [Check status](#)
 - AI assistance: [Ask ChatGPT what this is](#)
 - Pre-approve: [Pre-approve this file](#)
 - Block: [Block this file](#)
- Installed or uninstalled software:**

Action	Application	Version	Publisher
Install	Foxit PDF Reader	2024.2.2.64388	Foxit Corporation

IMPORTANT:

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

Multi-Factor Authentication (MFA)

MFA is available as an option for authenticating users prior to granting *Run As Admin* privileges. The three options in the portal for authenticating users are:

1. **Confirm** - User must confirm with **Yes** or **No** to elevate via *Run As Admin*.
2. **Multi-factor Authentication** - User must validate identity using MFA through SSO.
3. **Authenticate** - User must validate with credentials, face recognition, fingerprint, smartcard or similar.

Refer to [Mac Settings \(Authentication tab\)](#) for more information.

Intuitive app updates

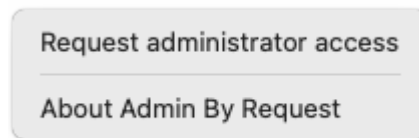
Prior to Mac 5.0, updating already-installed applications required an *Admin Session*. Now, pre-approved apps can be updated when the apps themselves prompt for it on manufacturer release. Alternatively, IT departments can control app updating by withholding pre-approval for the next release of an app until full testing has been completed.

As with the initial installation, portal settings determine if users must request approval to update (authorization) and, once approved, they are asked to confirm an update via **Confirm**, **MFA** or **Authenticate** with credentials (authentication).

Requesting Administrator Access

Requesting administrator access is also known as requesting an *Admin Session*, which is a time-bound period during which a standard user has elevated privileges and can carry out administrator-level tasks..

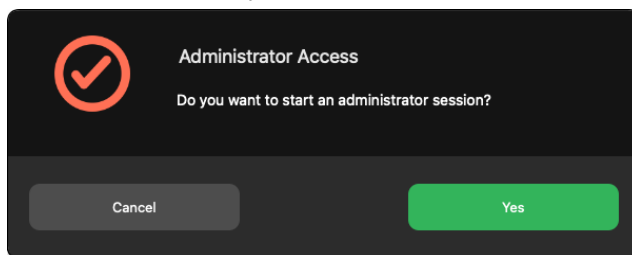
As with *About Admin By Request*, click the menu bar icon to display the menu and select **Request administrator access**:



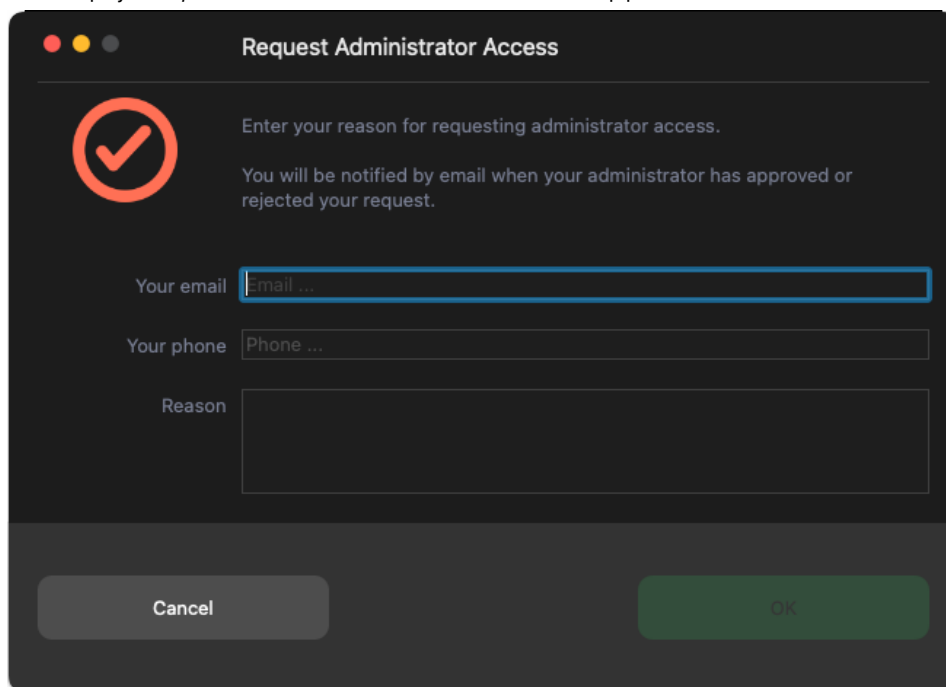
Submitting a request for administrator access is the primary mechanism for gaining elevated privileges.

A standard user making this selection *where approval is required* 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:



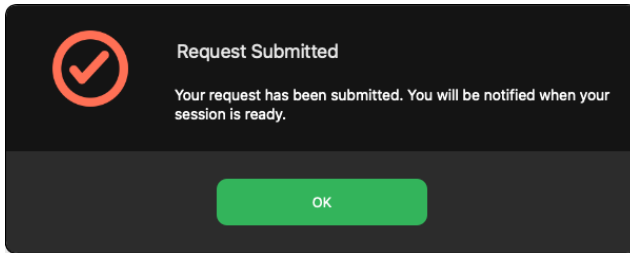
3. The user enters *email*, *phone* and *reason* information into the form and clicks **OK**.

NOTE:

Settings in the portal control the full extent of what is displayed to the user:

- If *Code of Conduct* is enabled, the user must acknowledge a Code of Conduct pop-up to continue (**EPM > Settings > macOS Settings > Endpoint > INSTRUCTIONS**).
- If *Require approval* is OFF, the approval steps are skipped (**EPM > Settings > macOS Settings > Authorization > AUTHORIZATION > Admin Session**).

4. The request is submitted to the IT administration team and the user is advised accordingly:

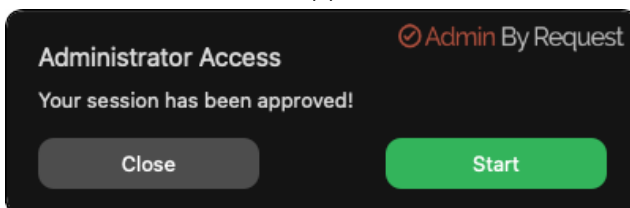


5. The IT administration team is notified via the Admin By Request portal that a new request for administrator access has arrived.

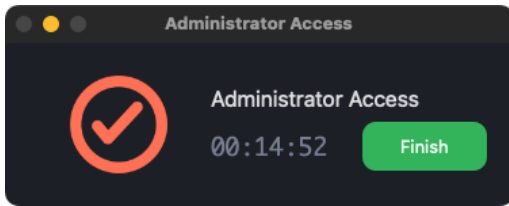
The following example shows how two new requests might appear in the portal:



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



- The user clicks **Yes**, which starts the session and displays a countdown timer:



- 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 optionally end the session at any time once it has started by clicking **Finish**.

See "[Changing Admin Session Duration](#)" on page 43 for more information on changing the duration of the countdown timer.

During an *Admin Session*, users can install programs requiring admin rights, install drivers and change system settings other than user administration. All activity during the elevated session is audited, so you can see in the audit log the reason why the person needs the elevation; anything installed, uninstalled, or executed.

IMPORTANT:

During an *Admin Session*, users **cannot** uninstall Admin By Request, or add, remove or modify user accounts.

Multi-Factor Authentication (MFA)

MFA is available as an option for authenticating users prior to allowing an *Admin Session*. The three options in the portal for authenticating users are:

- Confirm** - User must confirm with **Yes** or **No** to start an *Admin Session*.
- Multi-factor Authentication** - User must validate identity using MFA through SSO.
- Authenticate** - User must validate with credentials, face recognition, fingerprint, smartcard or similar.

Refer to [Mac Settings \(Authentication tab\)](#) for more information.

Setting-up a Break Glass Account

The Break Glass feature extends the functionality of MS LAPS. It creates a new, temporary, one-time-use Administrator account on an endpoint, that works on domains, Azure AD, and stand-alone, which audits all elevated activity, and terminates within a pre-defined amount of time or on log out.

Security benefits

The Break Glass feature includes the following security benefits:

- Break Glass **circumvents the need to use the built-in local Administrator account** – you can disable it completely to add an extra layer of security to your endpoints.
- The account **must be used within an hour of being generated**, minimizing the potential attack window and risk of account compromise.
- Risk is further minimized by a **one-time-only log in functionality**: the user can log in once, and after log out, the account is terminated.

- The user has **only the time specified under Expiry** when the Break Glass account was generated to use the administrator account; this duration is indicated on the built-in desktop background of each account. When the time-period is up, the session is terminated.
- Measures are in place to ensure **the Expiry time cannot be tampered with**: if the Account user attempts to extend their time limit by adjusting the clock, the Account automatically logs out / terminates.
- All **Usernames and Passwords are automatically generated**, random, and complex, minimizing the possibility for a successful brute force attack.
- Passwords are **stored within the web application**, only accessible by Portal users / IT Admins via credentials – a safer option compared to MS LAPS' storage of admin account passwords in plain text along with the AD computer record.

When would I use a Break Glass account?

A Break Glass account is useful in the following scenarios:

1. Regaining Domain-Trust Relationship

As the name suggests, the Break Glass feature is ideal for "last resort" situations, such as when the domain-trust relationship is broken and needs to be reconnected using an Administrator account.

2. Provisioning a Just-In-Time Administrator Account

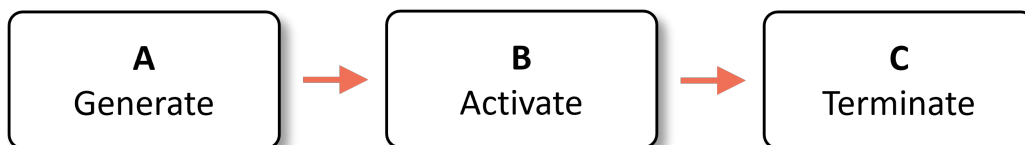
The Break Glass Account doubles up as a *Just-In-Time* account that can be used for specific purposes / situations when necessary; e.g., provisioning an account for someone who doesn't have credentials, but requires access to service an endpoint.

3. Extra Possibilities with Server Edition

Further to point 2, with Admin By Request Windows Server Edition you can provision an admin account to a consultant without giving them domain-wide permissions at any point in time.

Using the Break Glass feature

Setting-up and using a Break Glass account comprises three tasks:



A. Generate

Create a Break Glass account:

1. Log in to the Portal and navigate to the **Inventory** page. Select an endpoint on which you want to enable the Break Glass account and select **Break Glass** from the left-hand menu:
2. From the **Expiry** drop-down menu, select an amount of time for which you want the Account to be available. The default is **2 hours**, but the period can range from a minimum of 15 minutes, to an unlimited amount of time.

- Click the **Generate Account** button, which issues a Break Glass account and displays its *User* and *Password* in the read-only text boxes:

- Once generated, the status of the Break Glass account is updated in real-time in the Portal. The four possible states are:
 - Waiting for Endpoint** – The account is generated in the User Portal but not yet created on the endpoint (to create the account on the endpoint, see the next section **"Activate" on the next page**).
 - Ready to Log On** – The account is created but has not yet been activated / used (i.e., logged in to).
 - Session in Progress** – The account is currently in use.
 - Account Removed** – The account has been terminated either due to the user logging out, or the pre-defined *Expiry* time being reached.

Break Glass Account Events on DESKTOP-LMSEFL8

Drag a column header here to group by column or click the funnel icon to filter

Your Time	Event	Account	Name	Endpoint Time
20-12-2023 11:24:11	Break Glass Account removed	ABR855696		20-12-2023 11:24:11
20-12-2023 09:28:25	Break Glass Account logged on	ABR855696		20-12-2023 09:28:25
20-12-2023 09:21:48	Break Glass Account created	ABR855696		20-12-2023 09:21:48
20-12-2023 09:11:59	Break Glass Account issued	ABR855696	Steve	20-12-2023 09:11:59

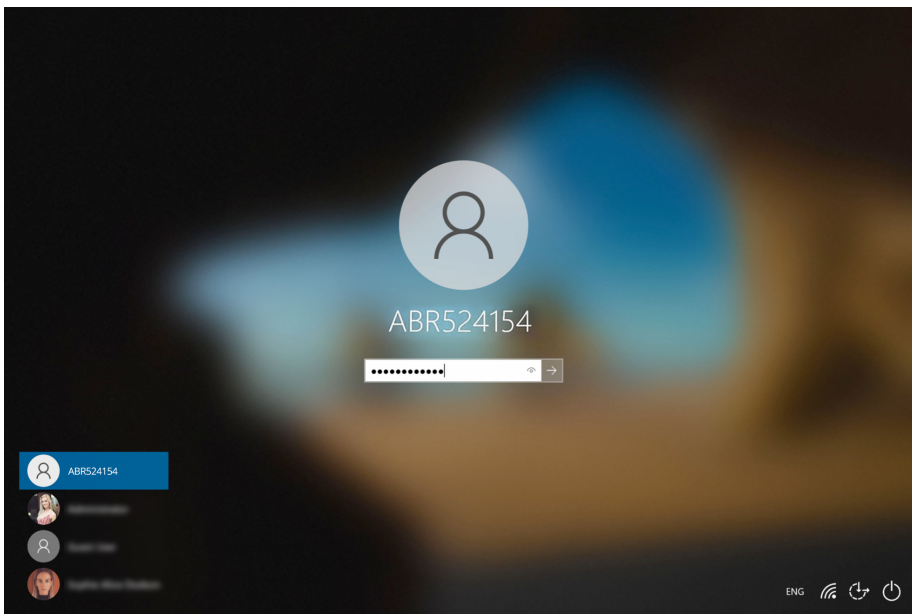
Page 1 of 1 (4 items) Page size: 25

5. Optionally, you can send the new Break Glass account credentials via SMS (i.e., text message) by entering the intended recipient’s mobile number into the text box and clicking **Send SMS**.

B. Activate

Activate the Break Glass account using one of the following methods:

- a. Restart the device, then wait approximately 30 seconds for the account to be created. The Portal will update the status message when the account is ready, and the account will appear in the bottom-left of the Windows log on screen along with the other accounts available on the endpoint:



- b. If enabled, you can select **Other User** in the Windows log in screen and enter the generated Break Glass account *User* and *Password* into the fields. Remember to prefix the User credential with the device name (e.g. DESKTOP-LMSEFL8\ABR524154).

NOTE:

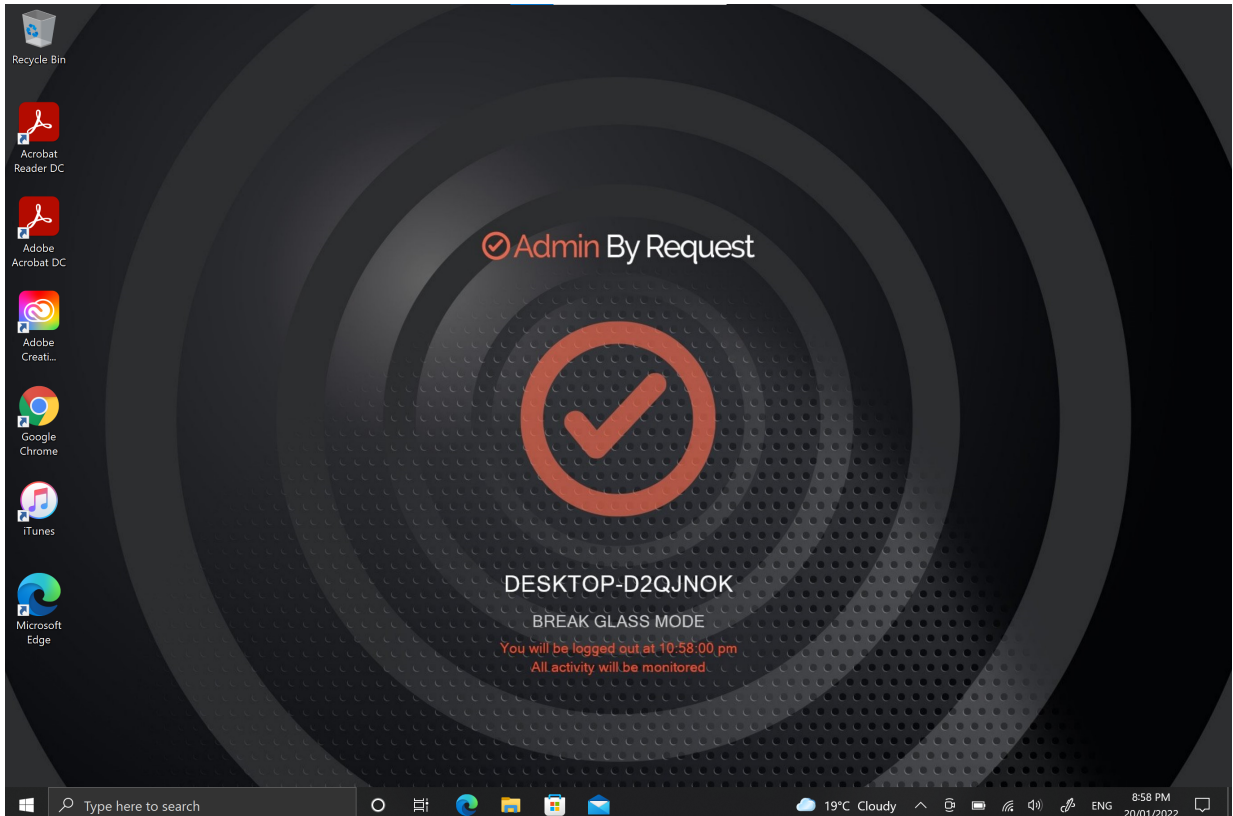
This may fail on the first attempt; if so, wait 10 seconds and then try again.

- C. A third method to activate the account is by logging in to another account on the endpoint, selecting the Admin By Request icon from the bottom toolbar, and clicking the **About** item from the menu.

C. Terminate

Use the account and log out:

1. Once logged in to the Break Glass account, the user has administrator privileges to do what they need to do, within the *Expiry* time displayed on the built-in screensaver:



2. Terminate the account by either logging-out, or allowing the account to log out automatically when the *Expiry* time is reached – whichever comes sooner.

Refer to [Features > Break Glass / LAPS](#) for more information on the feature.

Portal Administration for Mac

Introduction

This topic describes several key areas of the Admin Portal that can be used to manage *Mac Settings* and *Sub Settings*.

Fields that can be set and/or configured in the portal are presented in tables, with each table showing:

- **Setting** - the name of the field that controls the setting
- **Type** - the type of value that can be entered or selected and its default value
- **Description** - how the setting is used and notes about any implications it may have on other settings

To change any of the settings in the portal, [log in to the portal](#) and select the setting from the menu.

In this topic

["Entra ID Support" on the next page](#)

["Run As Admin Settings" on page 42](#)

["Admin Session Settings" on page 43](#)

["Authentication Setting" on page 44](#)

["System Settings" on page 45](#)

["Enabling sudo" on page 46](#)

["Pre-Approval Settings" on page 47](#)

["Machine Learning" on page 50](#)

["Privacy Settings" on page 50](#)

["Preventing Abuse" on page 51](#)

["Policies for macOS" on page 52](#)

["Clean up Local Admins" on page 55](#)

["Supplementary Technical Information" on page 57](#)

Entra ID Support

Portal menu: **Settings > Tenant Settings > Groups > ENTRA ID / AZURE AD**

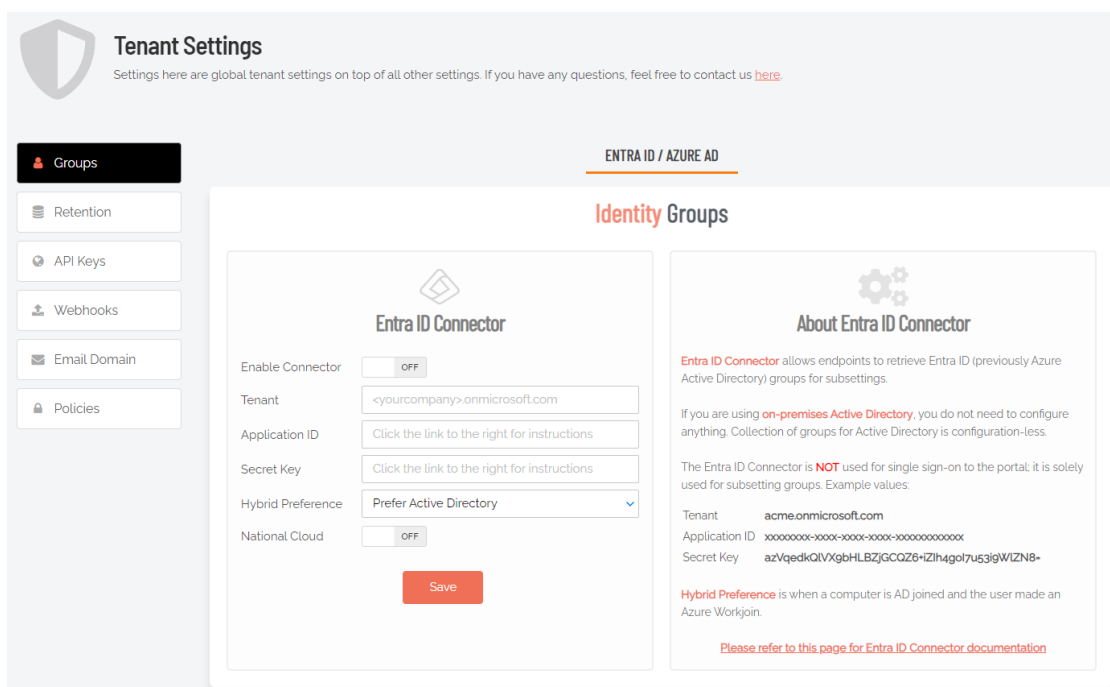
NOTE:

Azure AD has been renamed by Microsoft to Entra ID. This version of the document uses both terms interchangeably, but future versions will refer to Entra ID only.

A selling point for the 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.

For all endpoint clients, we've built in support for Entra ID groups, meaning you can now apply Sub-Settings to existing Entra ID / Azure AD user and device groups.



For more information on the Entra ID / Azure AD feature, refer to [Features > Azure AD Connector](#).

Settings Table - Entra ID

The *Entra ID Connector* allows endpoints to retrieve Entra ID (previously Azure AD) groups for sub-settings. The Entra ID Connector is NOT used for single sign-on to the portal; it is used solely for sub-setting groups.

If you are using on-premise Active Directory, you do not need to configure anything - collection of groups for Active Directory is "configuration-less".

Example values:

- Tenant **acme.onmicrosoft.com**

- Application ID XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
- Secret Key azVqedkQlVX9bHLBZjGCQZ6+iZlh4gol7u53igWlZN8=

Refer to <https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app> for more information on registering apps with the Microsoft identity platform.

NOTE:

The *National Cloud* regions of Azure are designed to make sure that data residency, sovereignty, and compliance requirements are honored within geographical boundaries.

Setting	Type	Description
Enable Connector	Toggle On Off Default: Off	On - Turns on the Entra ID Connector and allows endpoints to retrieve Entra ID groups for sub-settings. Off - The Entra ID Connector is disabled and endpoints will use sub-settings as described under "Sub-Settings", rather than using Entra ID rules.
Tenant	Text	Standard email address format. Use a new line for each address.
Application ID	Text	The value assigned to an application when it is registered with the Microsoft identity platform.
Secret Key	Text	The application certificate or client secret generated when the app is registered.
Hybrid Preference	Selection Default: Prefer Active Directory	An option available for selection when a computer is both AD-joined and the user makes an Entra ID Workjoin: <ul style="list-style-type: none"> • Prefer Active Directory - User is AD-joined only. • Prefer Entra ID / Azure AD - User is AD-joined and makes an Entra ID Workjoin.
National Cloud	Toggle On Off Default: Off	On - Enables selection of a physically isolated instance of Azure. Unhides <i>National Service</i> , which is where the actual geographic instance is selected. Off - Disables selection of a physically isolated instance of Azure.
National Service (hidden if <i>National Cloud</i> is Off)	Selection Default: US Government L4 / GCC High	The geographic instance selected: <ul style="list-style-type: none"> • US Government L4 / GCC High - Azure portal (global service) • US Government L5 / DoD - Azure portal for US Government • China (21Vianet) - Azure portal China operated by 21Vianet
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

Run As Admin Settings

Portal menu: **EPM > Settings > Mac Settings > Authorization > AUTHORIZATION**

Settings Table - Run As Admin

Run As Admin (also known as Application Elevation) elevates privileges for only the file or application selected.

It is invoked when a user drops an application on the Admin By Request dock icon to install it or by running a .pkg file. After re-authenticating with credentials, the user is able to install the application or .pkg file without having administrator rights.

Full Disk Access must be enabled. Please refer to ["Mac Client - Install / Uninstall" on page 2](#) for more information.

Setting	Type	Description
Allow Run As Admin	Toggle On Off Default: On	<p>On - Allows users to elevate privileges for a selected file. Enables <i>Require approval</i> and <i>Require reason</i>. Disables <i>Block Run As Admin</i>.</p> <p>Off - Denies users the ability to elevate privileges for a selected file. Enables <i>Block Run As Admin</i>, which is how users with admin credentials can still elevate privileges.</p>
Block Run As Admin (enabled only if <i>Allow Run As Admin</i> is Off)	Toggle On Off Default: Off	<p>On - Denies users the ability to execute <i>Run As Admin</i> even if administrator credentials are available (i.e. no authentication window is presented).</p> <p>Off - Allows users with administrator credentials to execute <i>Run As Admin</i> (i.e. authentication window pops-up asking for admin credentials).</p>
Require approval	Toggle On Off Default: Off	<p>On - Sends a request to the IT team, which must be approved before elevation is granted. Makes <i>Require reason</i> mandatory (i.e. must be On).</p> <p>Off - Allows the user to elevate file privileges (and thus perform the action) as soon as the action is selected. For example, selecting "Run as administrator" to execute a program occurs immediately, without requiring approval. Makes <i>Require reason</i> optional (i.e. can be either On or Off).</p>
Require reason	Toggle On Off Default: Off	<p>On - Extends the authentication window and asks the user to enter email address, phone number and reason. Reason must comprise at least <i>two words</i>. This information is stored in the Auditlog.</p> <p>Off - No reason is required by the user, but details of the actions performed are stored in the Auditlog.</p>
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

Admin Session Settings

Portal menu: **EPM > Settings > Mac Settings > Authorization > AUTHORIZATION**

Settings Table - Admin Session

Admin Session (also known as User Elevation) elevates the current user's privileges across the endpoint for the duration of the session.

Invoked when the user clicks the menu bar icon to request a protected administrator session, which makes the user a temporary member of the local administrator's group for a limited period of time under full audit.

Setting	Type	Description
Allow Admin Sessions	Toggle On Off Default: On	On - Allows users to effectively become a local administrator for the number of minutes specified in <i>Access time (minutes)</i> . Enables <i>Require approval</i> , <i>Require reason</i> and <i>Access time (minutes)</i> . Off - Denies users the ability to become a local administrator. Hides all other options under Admin Session.
Require approval	Toggle On Off Default: Off	On - Sends a request to the IT team, which must be approved before the request is granted. Makes <i>Require reason</i> mandatory (i.e. must be On). Off - Allows the user to become a local administrator as soon as the request is made. Makes <i>Require reason</i> optional (i.e. can be either On or Off).
Require reason	Toggle On Off Default: Off	On - Extends the authentication window and asks the user to enter email address, phone number and reason. This information is stored in the Auditlog. Off - No further information is required by the user, but user and computer details are stored in the Auditlog.
Access time (minutes)	Integer Default: 15 (minutes)	The maximum duration in minutes an Admin Session may last. This time must be sufficient for the user to install software or perform any other tasks that require elevation.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

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:

The screenshot shows a configuration window titled "Admin Session". It contains the following settings:

- Allow Admin Sessions: ON
- Require approval: ON
- Require reason: ON
- Access time (minutes): 15 (with left and right arrow buttons)

A red "Save" button is located at the bottom center of the panel.

3. Click **Save** when done.

Authentication Setting

Portal menu: **EPM > Settings > Mac Settings > Endpoint > AUTHENTICATION**

Settings Table - System Settings

The setting allows portal administrators to specify the style of prompt that is presented when users must authenticate to elevate privileges.

Setting	Type	Description
Mode	Choice: <ul style="list-style-type: none"> • Confirm • Multi-factor Authentication • Authenticate Default: Confirm	<p>Confirm - User must confirm with Yes or No (or via the reason screen) to perform the operation..</p> <p>Multi-factor Authentication - User must validate identity using MFA through Single Sign-on. Choosing this option unhides <i>Multi-factor Configuration</i> (see table below).</p> <p>Authenticate - User must validate with credentials, face recognition, fingerprint, smartcard or similar..</p>
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

Multi-factor Configuration

Appears when Multi-factor Authentication is chosen as the Mode.

Setting	Type	Description
Sign-on method	Selection: <ul style="list-style-type: none"> • Azure AD / Office 365 • -- ADD NEW METHOD -- 	Azure AD / Office 365 - Use this as the SSO method.

Setting	Type	Description
	Default: Azure AD / Office 365	-- ADD NEW METHOD -- - Create a new method. Choosing this option takes you to the portal's Single Sign-on (SSO) Setup page. Note the following: <ul style="list-style-type: none"> If adding a new method, you can use any SAML-based provider. If you use Office 365 / Azure AD and email match is Off, you must configure Entra ID Support¹. This is to make sure only users within the same Azure tenant can authenticate.
Email match	Toggle On Off Default: On	On - SSO authentication must match the email address from Active Directory or Azure AD. Off - Email address does not need to match.
MFA on pre-approvals	Toggle On Off Default: Off	On - Force multi-factor authentication on pre-approved applications. Off - Multi-factor authentication is not required on pre-approved applications

System Settings

Portal menu: **EPM > Settings > Mac Settings > Lockdown > SYSTEM SETTINGS**

Settings Table - System Settings

System Settings (also known as *System Preferences* in earlier macOS versions) have long been part of the macOS platform, enabling users to locally customize the look and feel of their Macs. This can lead to problems if users have admin rights, because some settings chosen by users might conflict with requirements of the organization.

The Admin By Request System Settings Lockdown feature controls access to specific system settings in macOS by enabling or disabling access to their corresponding right-hand panels. Each of seven panels can be enabled or disabled from the portal simply by setting a toggle to On or Off.

Setting	Type	Description
Users & Groups	Toggle On Off Default: Off	On - Users & Groups panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.

¹Refer to section *Entra ID Support* in chapter "Portal Administration for macOS", document **macOS Client: IT Admin Guide**

Setting	Type	Description
Login Items	Toggle On Off Default: Off	On - Login Items panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.
Network	Toggle On Off Default: Off	On - Network panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.
Sharing	Toggle On Off Default: On	On - Sharing panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.
Startup Disk	Toggle On Off Default: On	On - Startup Disk panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.
Transfer or Reset	Toggle On Off Default: On	On - Transfer or Reset panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.
Wi-Fi	Toggle On Off Default: On	On - Wi-Fi panel is not blocked for this user and will display. Off - Panel is blocked for this user and will not display. No changes can be made.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

Enabling sudo

Portal menu: **EPM > Settings > Mac Settings > Lockdown > ADMIN SESSION**

Settings Table - Admin Session

These settings control whether or not users are able to run sudo commands during a terminal session.

Setting	Type	Description
Force sudo close at end	Toggle On Off Default: On	On - Forcibly close any sudo command or interactive sudo session at the end of the admin session. Off - Do not force closure of sudo sessions.

Setting	Type	Description
Allow sudo terminal commands	Toggle On Off Default: Off	On - Allow user to issue sudo commands from a terminal prompt. Off - Do not allow user to issue sudo commands.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

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](#)" on page 52). We do not recommend enabling sudo access unless absolutely necessary.

To enable sudo for Mac devices, login to the portal, go to EPM > Settings > Mac Settings > Lockdown > ADMIN SESSION and set *Allow sudo terminal commands* to **On**.

Admin By Request 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.

Pre-Approval Settings

Portal menu: **EPM > Settings > Mac Settings > App Control > PRE-APPROVE**

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.

Use the following commands to get a vendor's name for the files for Pre-Approval, without having to use the Auditlog in the portal. For example:

For applications (.app)	For packages (.pkg)
Command: <code>codesign -d -vv /path/app.app</code>	Command: <code>pkgutil -check-signature /path/app.pkg</code>
Result: Authority=Developer ID Application: VideoLAN (75GAHG3SZQ)	Result: Developer ID Installer: Oracle America, Inc. (VB5E2TV963)

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

Admin By Request allows for quick pre-approval of trusted applications from the Auditlog. Pre-Approval is based on the application vendor or checksum, visible when the *Application Control* screen is displayed (step 3 below).

NOTE:

At the time of writing, this functionality is not available for Linux clients.

Once an application has been installed on an endpoint 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 a detailed view of an application entry in the Auditlog. The application is 'Adobe Acrobat Reader (Continuous) (Installer)' on a 'Mac Standard' endpoint, installed by 'STEVE'S MACBOOK PRO' on '18-01-2024 12:15:24'. The status is 'Finished'.

Contact Information		Execution	
Full name	Mac Standard	Start time	18-01-2024 12:15:24
User account	MACSTD	End time	18-01-2024 12:16:35
Email	sdo@adminbyrequest.com	Duration	00:01:11
Phone	555 123456	Settings	Global Settings
Response In	00:01:21	Trace no	168341142
Reason	Documentation screenshots		

Application		Actions	
Name	Adobe Acrobat Reader (Continuous) (Installer)	Malware scan	Unknown
Vendor	Adobe Inc.	Virusotal	Check status
File name	AcroRdrDC_2300820470_MUI.pkg	AI assistance	Ask ChatGPT what this is
Path	/Volumes/AcroRdrDC_2300820470_MUI	Pre-approve	Pre-approve this file
		Block	Block this file

3. On the *Application Control* screen, modify any settings as required. For more information on pre-approval settings, refer to the Settings Table below.
4. Click **Save** verify that the app has been added to the list of pre-approved applications.

For example, the following applications are pre-approved:

The screenshot shows the 'Mac Application Control' interface. It features a sidebar with navigation options: Authorization, Endpoint, Lockdown, Malware, App Control (selected), Data, and Emails. The main area is titled 'Mac Application Control' and 'Pre-approved Applications'. A 'New entry' button is visible. A table lists the pre-approved applications:

	Application	File	Protection	Type	Log	
Edit	Brave-Browser-BRV010 (Installer)	Any file	SHA256 checksum	Pre-approval	<input type="checkbox"/>	Delete
Edit	Microsoft Teams (Installer)	Any file	SHA256 checksum	Pre-approval	<input checked="" type="checkbox"/>	Delete

Export options: Export to PDF, Export to XLSX, Export to CSV(), Export to CSV().

Settings Table - Pre-Approve

Pre-approved applications are application files that are pre-approved to run *Run As Admin*, when approval would normally be required. The intention is to remove trivial approval flows and avoid flooding the audit log with trivial data for applications known to be good, such as Adobe Reader installs.

When an application is on the pre-approval list, the difference is:

- The application is auto-approved, so the approval flow is bypassed
- A reason is not required, as the application is known to be good
- You have the option to not log to the Auditlog (e.g. for trivial data)
- If *Run As Admin* is disabled, a pre-approved application will still run

New entry

Click button **New entry** to create a new pre-approved application.

Setting	Type	Description
Log to auditlog (hidden if <i>User confirmation</i> is Off)	Toggle On Off Default: Off	On - .Relevant details about the application are logged. Off - No logging is performed for this application.
User confirmation	Toggle On Off Default: On	On - .The user must confirm elevation on the endpoint before the application can be run. This is the typical authentication window. Off - The user does not need to confirm elevation on the endpoint before execution. Hides the <i>Log to auditlog</i> field.
Type	Selection Default: Run As Admin application pre-approval	Run As Admin application pre-approval - Pre-approve this application for Run As Admin. Run As Admin vendor pre-approval - Pre-approve this vendor for Run As Admin. Selecting this option enables the <i>Vendor</i> field and hides all other fields.
Vendor (enabled when <i>Run As Admin vendor pre-approval</i> is selected)	Text	Enter vendor name. Adding the app via the Auditlog will auto-populate this field.
Protection	Selection Default: File must match vendor	Prevent users from bypassing pre-approval by file renaming. File must match vendor - The application name and the file name must align with the same details provided by the vendor. File must match checksum - A checksum of a specific file version. If the file is updated, the checksum no longer matches and a new one must be collected.

Setting	Type	Description
		No protection (not recommended) - Not recommended for anything except testing. The file can be located anywhere and is a file renaming vulnerability, in case a user is aware of (or can guess) the file name.
Application name	Text	The name of the application. Mandatory, although used for convenience only to help identify applications in the list.
File name	Text	Enter file name. Adding the app via the Auditlog will auto-populate this field.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.
Cancel	Button	Cancels all work done in this setting and returns to the Mac Workstation Global Settings page.

Enabled toggle

A global setting that indicates whether pre-approved applications are allowed at all (**On**) or not (**Off**).

Machine Learning

Portal menu: **EPM > Settings > Mac Settings > App Control > 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 [Features > Machine Learning](#).

Privacy Settings

Portal menu: **EPM > Settings > Mac Settings > Data > PRIVACY**

Settings Table - Privacy

The PRIVACY tab provides a way to anonymize data collection, so that data is still logged and available for analysis, but identification of individual users is not possible.

Key points:

- Obfuscation creates an alias for each user. You can track activity, but you cannot decode the true identity of any user.
- Collection of data should be left on unless you have a reason not to do this. If disabled, you will have to find contact information elsewhere.
- Inventory is a hardware and software inventory. If disabled, only the computer name is collected and shown in the "Inventory" menu.
- Geo-tracking maps the endpoint IP address to location using a public IP-to-location database to show in inventory and reports.

NOTE:

Changes apply *only to new data*. This is by design to avoid accidentally deleting existing data.

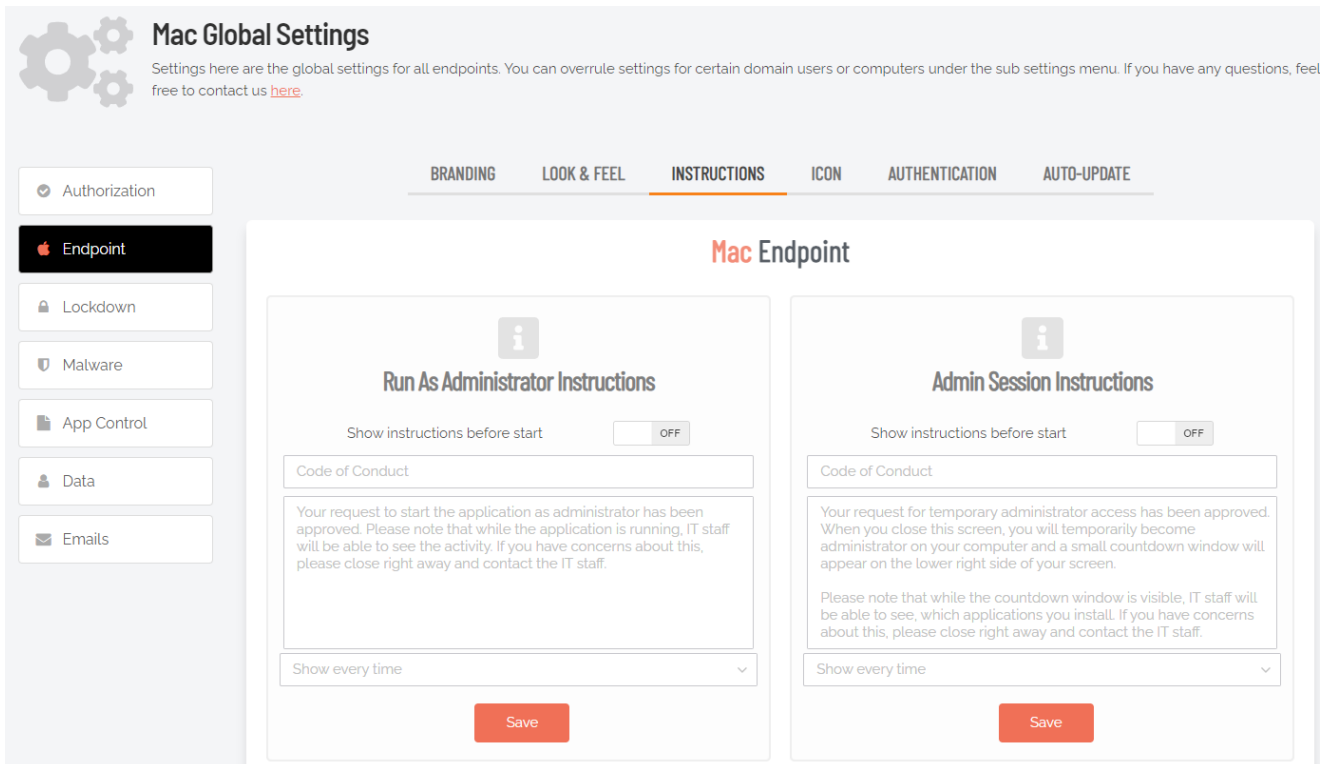
Setting	Type	Description
Obfuscate user accounts	Toggle On Off Default: Off	On - Create an alias for each user. Off - Do not create aliases for users.
Collect user names	Toggle On Off Default: On	On - Record the name of each user associated with an ABR event. Off - Do not record user names.
Collect user email addresses	Toggle On Off Default: On	On - Record email addresses associated with a user. Off - Do not record email addresses.
Collect user phone numbers	Toggle On Off Default: On	On - Record phone numbers associated with a user. Off - Do not record phone numbers.
Collect inventory	Toggle On Off Default: On	On - Record hardware and software inventory data. Off - Do not record inventory data.
Allow geo-tracking	Toggle On Off Default: On	On - Record the location of the public IP address associated with the user's endpoint. Off - Do not record IP addresses.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked.

Preventing Abuse

So what prevents the user from abusing an Admin Session? The fact that the user has to ask IT for access will in itself prevent the most obvious abuse. But as part of your settings, you can also configure a *Code of Conduct* page. Here you customize wording that suits your company policy. For example, what the penalty is for using the administrator session for personal objectives. You can also choose to explain the things you can monitor from the portal.

When you enable the *Code of Conduct* ("instructions") screen in the settings, this screen appears right before the administrative session starts. You can also customize company name and logo for all screens, so there is no doubt this message is authentic and indeed from the user's own company. This is the configuration part of the portal, where you set authorization, company logo, policies, email communications, etc.

For example:



Policies for macOS

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.

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 therefore cannot 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.

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

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:

```
open -g -n /Applications/Admin\ By\ Request.app --args -refresh
```

Key	Type	Default	Description
AdminMinutes	Integer	15	Number of minutes the user is administrator. This can also be set in your portal settings.
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.
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 from which to download logo. 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 device.
RequireApproval	Boolean	0	Elevate without requiring someone to approve requests.
RequireReason	Boolean	1	Require reason to elevate.

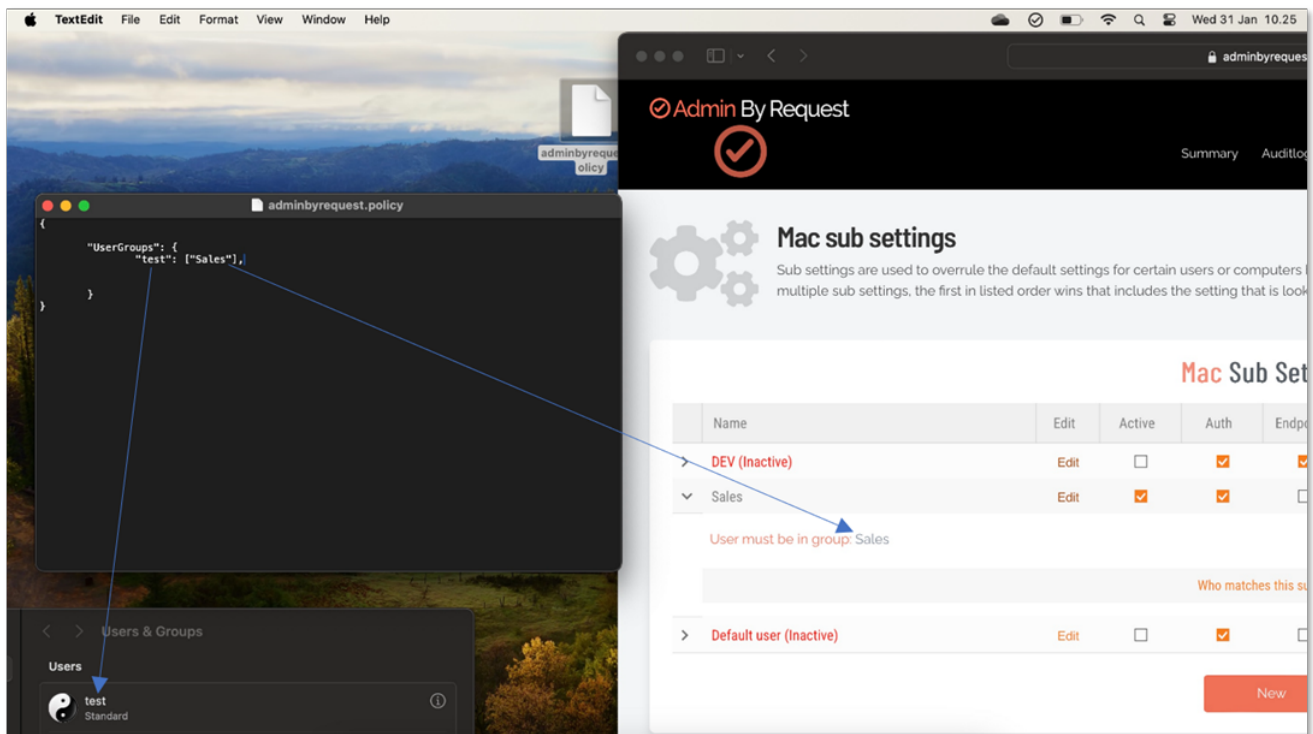
Key	Type	Default	Description
RequireAppApproval	Boolean	0	Elevate Run As Admin without requiring someone to approve requests.
RequireAppReason	Boolean	1	Require reason to Run As Admin.
ShowInstructions	Boolean	0	Show Code of Conduct screen.
UploadInventory	Boolean	1	Upload inventory data to the portal.
UserGroups	Dictionary with Array of Strings		User groups to match machine to sub settings when not using Active Directory.

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 do decide to use a policy file, you can use it if you do not have an AD or an Entra ID.

In the policy file, you can setup all groups to correspond to the Subsetting in the ABR portal, as per the example below:



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

Clean up Local Admins

The *Clean Up Local Admins* feature in Admin By Request is designed to help IT administrators easily manage and remove unused or rogue local administrator accounts across multiple endpoints. A quick check (and subsequent clean up if necessary) can be done directly from the portal, giving administrators an immediate and holistic view of just who currently has admin access on which computers.

The feature simplifies the process of identifying and revoking unnecessary admin rights, reducing the attack surface and enhancing security within an organization.

Purpose

The feature addresses the common problem of unmanaged or forgotten local admin accounts that could pose security risks. These accounts may belong to former employees or be leftover from previous configurations, making them prime targets for cybercriminals seeking to exploit elevated privileges.

Functionality

The feature centralizes the management of local admin accounts by allowing administrators to revoke admin rights from a single interface within the portal. This eliminates the need to manually disable accounts on individual endpoints.

How It Works

1. Access the Feature:
Navigate to the Inventory page within the portal.
Select the desired endpoint and click **Local Admins** from the left-hand menu. This brings up a 'birds-eye' view of all administrator accounts associated with that endpoint, displayed as individual account cards.
2. Identify Admin Accounts:
Each account card is labeled with an icon and a name indicating the type of account (e.g., Local Administrator, Domain Administrator etc.).
Rogue or unused accounts may be identified by non-descriptive names, often represented by long numeric sequences.
3. Revoke Admin Rights:
To revoke admin rights, click the **Revoke Rights** button located on the account card. This button is highlighted in orange.
The button will change to **Cancel Revoke**, allowing you to undo the action if it was selected by mistake.
4. Restore Admin Rights:
Admin rights can be restored by selecting the Restore Rights button within the Restore Revoked Local Administrators section during the two-week window.

Safeguards

The feature includes built-in safeguards to prevent the removal of essential accounts, such as the first Administrator account used to setup the computer. This ensures that critical administrative access is not inadvertently revoked, which could otherwise render endpoints inaccessible.

Using the Feature via Reports Page

Alternative Access

The *Clean Up Local Admins* feature can also be accessed through the *Reports* page for bulk management of admin accounts.

Navigate to **Reports > User Reports > Local Admins** to view admin accounts in a list format, grouped by account type.

Rogue accounts can be removed in bulk by selecting the **Remove** button next to the corresponding account group.

Undoing Removal:

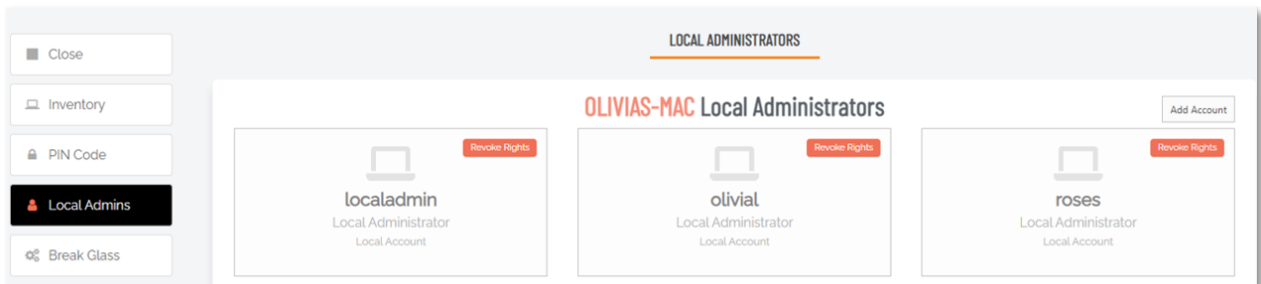
If an admin account is mistakenly removed, the action can be reversed by going to the **RESTORE RIGHTS** tab on the Local Admins page.

The removed group will be listed, and selecting the **Undo** button will restore the admin rights to the affected accounts.

Example - Olivia's Mac

The procedure is straightforward:

1. Log in to the portal and go to the **Inventory**.
2. Locate the endpoint concerned and drill-down using either its name in the *Computer* column, or **Details** in the *Details* column.
3. In the left menu, click **Local Admins**:



4. Finally, identify the users who should not be admin and use the **Revoke Rights** button to remove their administrator privileges.

Supplementary Technical Information

This section provides more information on the following:

- Local Administrator Accounts
- Active Directory
- Sub-Settings
- Sudo
- Machine Settings
- Tampering

Local Administrator Accounts

By default, users logging on to a Mac workstation 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 endpoints; no users would be able to gain elevated privileges and would instead have very limited ability on their devices.

The following graphic shows *Revoke Admin Rights* **ON**, except for user accounts Steve, Jo and Mary:

Mac Global Settings
Settings here are the global settings for all endpoints. You can overrule settings for certain domain users or computers under the sub settings menu. If you have any questions, feel free to contact us [here](#).

ADMIN RIGHTS | SYSTEM SETTINGS | ADMIN SESSION | OWNER | INTUNE

Mac Lockdown

Admin Rights

Revoke admin rights: ON

Excluded accounts: Steve, Jo, Mary

About Admin Rights

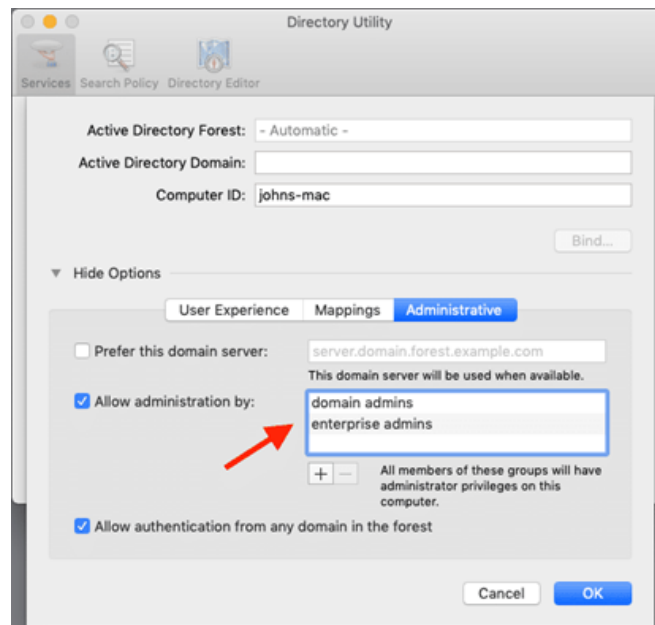
Revoke admins rights at logon means that all user accounts will be downgraded from the Admin to User role, unless the account appears in the excluded accounts list. Refer to the [FAQ](#) for more information.

Excluded accounts are not removed at logon. Multiple accounts must be specified on separate lines. Domain accounts must be prefixed with domain and backslash.

Save

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:



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:

1. *Mac Settings* (also known as Global Settings) apply to all users by default, **except** those settings overridden under Sub Settings.
2. *Mac Sub Settings*, where you can define special settings based on Active Directory computer or user groups and/or Organizational Unit(s).

Settings here are the global settings for all endpoints participating in the feature. You can overrule settings for listed domain users or computers under the sub-settings menu.

Sub settings will *override* the global settings for the users or computers to which they apply. Both users and computers can be in Active Directory groups or organizational units.

If a user or computer hits multiple sub settings, the first in listed order *that includes the setting concerned* wins.

Example sub-settings

This can be used, for example, to allow sudo access for *developers* or automatically approve requests from *users in the IT department*.

For Macs, the feature is only available if the mac is bound to Active Directory or using NoMAD or Idaptive. Sub settings can also be used by specifying machine / user groups in the policy file. Refer to ["Policies for macOS" on page 52](#) and [Sub-Settings](#) 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" on page 52](#)). We do not recommend enabling sudo access unless absolutely necessary.

To enable sudo for Mac devices, login to the portal, go to EPM > Settings > Mac Settings > Lockdown > ADMIN SESSION and set *Allow sudo terminal commands* to **On**.

Admin By Request 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.

Machine Settings

You can use a local policy file to override all portal settings locally. Refer to ["Policies for macOS" on page 52](#) 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 with policy settings.

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 Request detects that the clock has been changed, the administrator session will end instantly to prevent users from extending their session.

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. See also "Pre-Approved List" on the next page .
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.
Endpoint Security	An holistic approach to securing a network that goes beyond traditional anti-malware and aims to protect every endpoint from potential threats. See also "EDR" on page 62 in the glossary.
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. See also "Vertical Privilege Escalation" on the next page .
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.

Term	Definition
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.
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 "Blocklist " on the previous page.
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 "Horizontal Privilege Escalation" on the previous page.

Glossary

The following table lists the meanings of many acronyms used when discussing privileged access management and endpoint protection.

Term	Short for	Definition
Azure AD	Azure Active Directory	Azure Active Directory is part of Microsoft Entra, which is an enterprise identity service that provides single sign on, multi-factor authentication, and conditional access to guard against security threats.
Entra ID	Microsoft Entra	Microsoft Entra is a family of multi-cloud identity and access solutions that includes Azure AD. The term "Entra ID" replaces the term "Azure AD".
EDR	Endpoint Detection and Response	A method of securing endpoints that focuses on detecting and responding to threats that are present. Works in conjunction with EPP.
EPP	Endpoint Protection Platform	A method of securing endpoints that focuses on preventing threats from arriving. Combines analysis, monitoring & management, anti-malware software, EDR capabilities and other security features into a comprehensive endpoint security platform.
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.
FIDO	Fast Identity Online	<p>With FIDO Authentication, users sign in with phishing-resistant credentials, called "Passkey" on the next page. Passkeys can be synced across devices or bound to a platform or security key and enable password-only logins to be replaced with secure and fast login experiences across websites and apps.</p> <p>Passkeys are more secure than passwords and SMS OTPs, simpler for consumers to use, and easier for service providers to deploy and manage.</p>
Intune	Microsoft Intune	Microsoft Intune is a cloud-based UEM solution. It manages user access and simplifies device and application management for multiple platforms, including mobile devices, desktop computers, and virtual endpoints.
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.

Term	Short for	Definition
MAM	Mobile Application Management	Software and processes that secure and enable IT control over enterprise applications on end users' corporate and personal devices.
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.
Passkey	Passkey	Passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant.
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.

Synchronizing Clients with the Portal

Introduction

Admin By Request (ABR) clients synchronize with the portal to ensure they have the latest settings and policies. This synchronization process happens periodically and can also be triggered manually.

The following explanation is based on common questions and scenarios.

NOTE:

The term "Entra ID" is used here rather than the older "Azure AD (AAD)" term.

Periodic Synchronization

By default, ABR clients synchronize with the portal **every four hours**, subject to internet connectivity. This regular synchronization ensures that any changes in ABR portal configuration are reflected/applied to each endpoint.

Another purpose of synchronization is to ensure that Active Directory (AD) or Entra ID group memberships, settings, and policies are applied to the clients in a timely manner. While the AD Connector is **On** (portal: **Settings > Tenant Settings > Groups > ENTRA ID / AZURE AD > Enable Connector**), Entra ID groups are "looked-up" by the ABR client when one of the following happens:

1. The user logs on to the endpoint device.
2. Once every 4 hours if the ABR client is idle.
3. If a user clicks **About Admin By Request** via the tray icon or menu bar (see "[Manual Synchronization](#)" below)

Note that group modifications made on the Entra ID platform can take *between 30 seconds to 1 hour*. This is how the Entra ID platform works and is determined by Microsoft - Admin By Request has no control over this interval. Refer also to "[Factors Affecting Synchronization Timing](#)" on the next page.

Manual Synchronization

Users can manually trigger a synchronization to ensure that the latest portal settings and policies are immediately applied to the ABR client. This can be useful when changes need to be reflected quickly, such as during testing prior to roll-out, or when a user is added to or removed from an AD/Entra ID group that affects their permissions.

To trigger synchronization:

- Simply log on to the ABR client (i.e. the endpoint device).
- For Windows endpoints, click the *ABR icon in the tool tray* on the device and select **About Admin By Request**. This action triggers the *About* screen and also initiates an immediate synchronization with the portal.
- For macOS and Linux endpoints, click the *ABR menu bar icon* on the device and select **About Admin By Request**. This action triggers the *About* screen and also initiates an immediate synchronization with the portal.

Scripted Synchronization

On macOS endpoints, synchronization can be triggered by running command:

```
open -g -n /Applications/Admin\ By\ Request.app --args -refresh
```

On Linux endpoints, synchronization can be triggered by running command:

```
abr settings --reload
```

Contact us if you need to run a script to trigger synchronization for Windows endpoints.

Factors Affecting Synchronization Timing

While the default synchronization interval is four hours, the actual time it takes for changes to be reflected can vary. This variability can be due to the time it takes for changes to propagate through AD/Entra ID and be recognized by the ABR client. Factors such as network latency, AD replication schedules, and Entra ID synchronization cycles can all influence this timing.

IMPORTANT:

User/device group memberships are handled by Entra ID; ABR clients are in Microsoft's hands when it comes to propagation time.

In many cases (as indicated by customer tickets on this subject) we see customer screen grabs from Entra ID showing that users or devices are members of group XYZ and asking why the portal has not yet picked them up.

However, in these cases, the portal does not know the endpoint state. The actual time that synchronization with Entra ID/Intune "kicks in" on an endpoint can vary and depends on many factors. Note also that, with on-premise AD configuration, endpoints need to have a "line of sight" to the PDC (Primary Domain Controller). It's important to be aware of this, especially when users work remotely (i.e. off site) and are using VPN or similar to reach the corporate network.

Handling Hybrid Environments

In hybrid environments where devices may be joined to both on-prem AD and Entra ID, ABR provides a **Hybrid preference** setting. This setting allows administrators to specify whether the ABR client should prioritize synchronizing with AD or Entra ID. This is crucial for environments where different sub-settings are based on either AD or Entra ID groups.

If the environment is a hybrid setup, i.e. it's connected to both on-prem AD and Entra ID, then it very much depends on what the AD Connector hybrid preference is set to. If set to **Prefer Active Directory**, then AD groups will be the ones used to match sub-settings. If set to **Prefer Entra ID**, then Entra ID groups will be used instead.

Issues can arise if *different group names* are used for on-prem and Entra ID groups, or if group members are not synchronized properly between them.

Common Issues and Solutions

If synchronization issues arise, such as changes not being reflected in the ABR portal or incorrect group memberships, the first thing to check is the Connectivity panel in the user interface, accessed via **About Admin By Request > Connectivity**. If cloud connectivity status is failing, then the ABR client won't be able to synchronize with the portal.

To investigate this, or to look at other areas if connectivity is OK:

- Ensure that the ABR client is up to date. Upgrading to the latest version can resolve synchronization issues.
- Verify that the AD/Entra ID groups are correctly configured and that the client has network connectivity to the appropriate directory services.
- Use the `whoami /groups` command on Windows to verify group memberships directly on the client machine (see note below).
- For hybrid environments, ensure that the ABR portal is configured to correctly handle AD and Entra ID group memberships, according to the selected preference.

NOTE:

The `whoami /groups` command shows *only* on-prem AD groups. There are other options to show Entra ID groups:

- Use the Remote Server Administration Tools (RSAT) PowerShell module to look up a user's groups. In particular, the cmdlets **Get-ADUser** and **Get-ADGroup**. For more information on the RSAT PowerShell module, refer to <https://learn.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2022-ps>.
- Users can view their assigned groups by going to their Microsoft 365 account page. This can be accessed (in Microsoft 365) by going to **Settings > Accounts > Your info > Accounts : Manage my accounts > My Groups**.
- IT Admins and tech savvy users can login with an admin account on the device to look up the following registry subkey via the Registry Editor: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\CloudActiveSync\ADSI**Cache\.

For more information, including answers to questions and/or further assistance, please contact your account manager or get in touch via our [contact page](#).

Document History

Document	Product	Changes
1.0 11 May 2023	4.0 9 January 2023	Initial document release.
1.1 25 May 2023	4.0 9 January 2023	Corrected typos. Added User Interface screenshots.
1.2 20 July 2023	4.1 19 July 2023	Included 4.1 features: <ul style="list-style-type: none"> • New <i>Owner</i> feature • New <i>Intune Compliance</i> lockdown setting Updated old portal screenshots. Applied new document template and formatting.
1.3 16 February 2024	4.2 2 November 2023	Included 4.2 features: <ul style="list-style-type: none"> • New <i>System Setting</i> lockdown feature • New <i>Authentication Confirm</i> mode Added Break Glass section. Added key portal settings to Portal Administration chapter.
1.4 11 March 2024	4.2 2 November 2023	Added Settings Table for Mac Settings > Data > PRIVACY. Corrected an error in chapter "The macOS Client User Interface", section <i>Using Run As Admin</i> , where dragging to the ABR dock icon works only for .app files; it does not work for .pkg files. Corrected typos.
1.5 28 March 2024	4.2 2 November 2023	Removed <i>Blocking</i> paragraphs in chapter "Portal Administration for macOS", section Supplementary Tech Info. [Online only] Added FAQ advising that pre-approval might not work for all apps. Updated portal menu selection paths.
1.6 4 June 2024	4.2 2 November 2023	Added sections <i>Enabling sudo</i> in chapter "Portal Administration" and <i>Your Tenant License</i> in chapter "macOS Client - Install / Uninstall". Removed AllowAppStore key from <i>Policies</i> table in chapter "Portal Administration" and added remaining settings tables for <i>Endpoint</i> menu.

Document	Product	Changes
2.0 26 August 2024	5.0 26 August 2025	<p>Included 5.0 features:</p> <ul style="list-style-type: none">• macOS client now supports MFA• Support Assist capability added• Admin Auditlog improved• App elevation process improved• Added revoke/restore for local admin clean-up• Client installation process improved <p>Updated manual structure and layout. Removed section <i>Removed in macOS Version 3.0 Onwards</i> from chapter "Portal Administration".</p>
2.1 6 September 2024	5.0 6 September 2024	<p>Updated the installation procedure to more clearly highlight the order of tasks when installing and granting permissions for system extensions and FDA.</p> <p>Changed "macOS" to "Mac" when referring to the Admin By Request product.</p>

Index

A

- About ABR
 - Connectivity 20
 - Diagnostics 20
 - Uninstall 21
- About Admin By Request 19
 - Assistance 21
- Active Directory 58
- Admin Session
 - Settings 43
- Administrator Access
 - User Interface 32
- App 26
- Assistance 22
- Assistance example scenario 23
- Audience 1
- Authentication
 - Settings 44
- Azure AD 40

B

- Big Sur 5
- Break Glass Account
 - User Interface 34

C

- Catalina 5

D

- Diagnostics 22

E

- Enabling_sudo
 - Settings 46
- Entra ID 40
- Execution history 28, 31

I

- Install 2

L

- Local Administrator Accounts 57
- Local Admins 55
- Logging 17

M

- Machine Learning 50
- Machine Settings 59
- macOS 10.15 5
- macOS 11 5
- macOS 12 5
- macOS 13 6
- macOS 14 6
- macOS versions 5
- Monterey 5
- Multi-Factor Authentication 23, 31, 34
- Multiple endpoint installation 7

O

- Overview 1

P

Performance	17
PIN Code	12
Policies	52
Policy file	52
Portal Administration	
macOS	39
Pre-Approval	
Settings	47
Prerequisites	2
Preventing Abuse	51
Privacy	
Settings	50

R

Release Notes	1
Remote Assist	22
Reports Page	56
Run As Admin	
Settings	42
User Interface	26

S

Security checks	24
Single app (execution of)	26
Single endpoint installation	3
Sonoma	6
Sub-Settings	58
sudo	16, 59
Supplementary Technical Information	57
Support Assist	22
System Settings	
Settings	45

T

Tamper prevention	17
Tampering	59
Tenant License	2

U

Uninstall	2
Uninstall single	
PIN Code	25
Upgrading	11
User accounts	34
User Interface	18
User rights	16

V

Ventura	6
---------------	---