Document Code: **PM-MC-ITAG**

Document Version: **1.5**

Document Date: **28 March 2024**

macOS Client: IT Admin Guide

Configure, deploy and manage your macOS workstations

Admin By Request

macOS Product Version: **4.2**

Admin By Request

Contact Admin By Request

1390 Market Street, Suite 200
San Francisco, CA 94102

Phone and Email:
adminbyrequest.com/contact

www.adminbyrequest.com
linktr.ee/adminbyrequest

Table of Contents

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

> **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

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

Resources > Documentation > Release Notes (macOS)

macOS Client - Install / Uninstall

Prerequisites

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

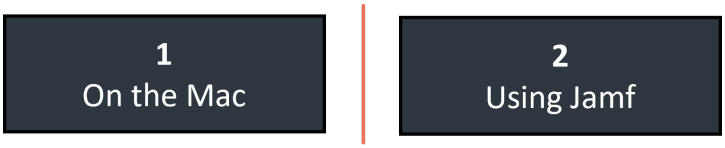
The following installation procedure is in three parts: the first outlines downloading and installing the Admin By Request package, the second describes how to enable FDA, and the third outlines the differences between an admin user and a standard user (as well as the need to test the installation as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

Installing Admin By Request

Installation steps are grouped into the following tasks:

A. **Download and install the Admin By Request package**.

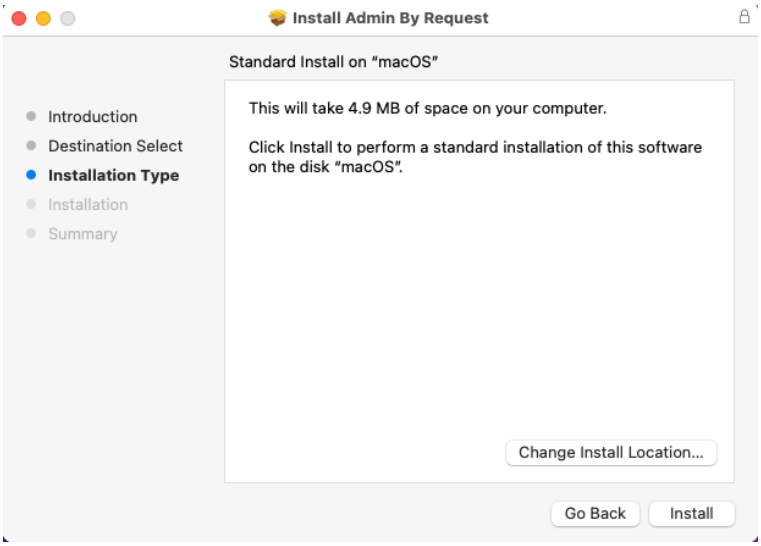
The following procedures describe two ways to install the Mac client:



1. **On the Mac**
    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.

4. Allow the installation to proceed, providing your credentials if necessary:

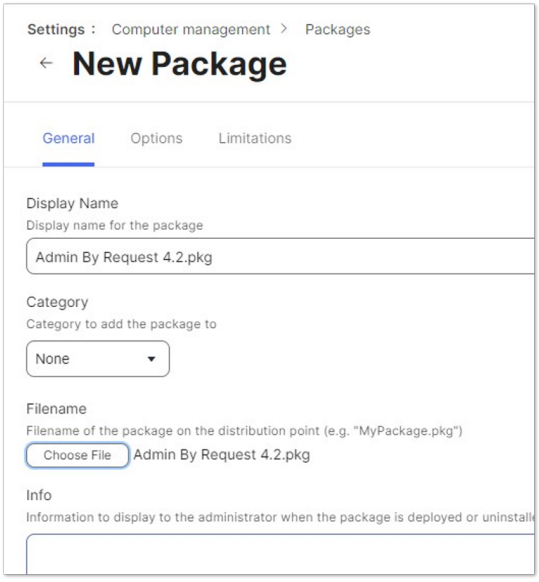


5. When done, close the installer and (optionally) move the installer package to the bin.

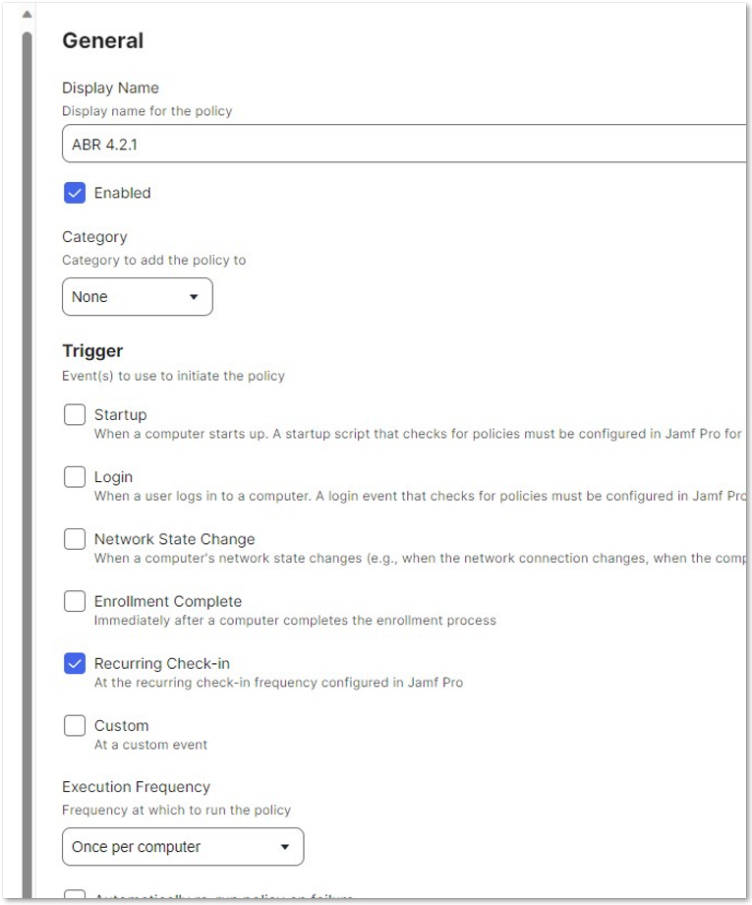
2. **Using Jamf**.

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



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



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

B. Enable Full Disk Access (FDA).

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

> **NOTE:**
> - The *adminbyrequest* application must be installed first, so that it appears in the list of apps available under Full Disk Access.
> - The procedures below are not sequential - choose one or a combination, depending on your requirements.

The following procedures describe three ways to enable FDA:

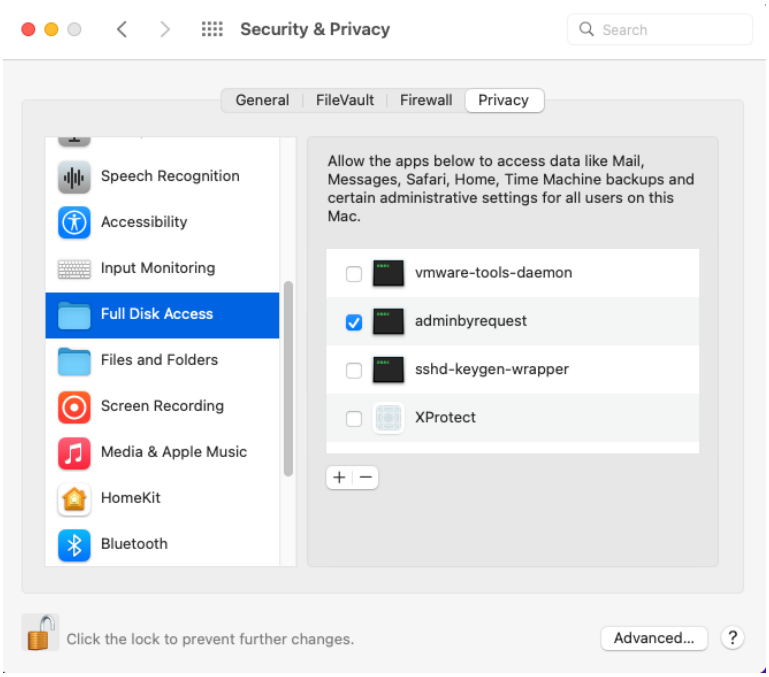
1 On the Mac	2 Using Jamf	3 Using Intune

1. **On the Mac**

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

   - **macOS 12 (Monterey)**.

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

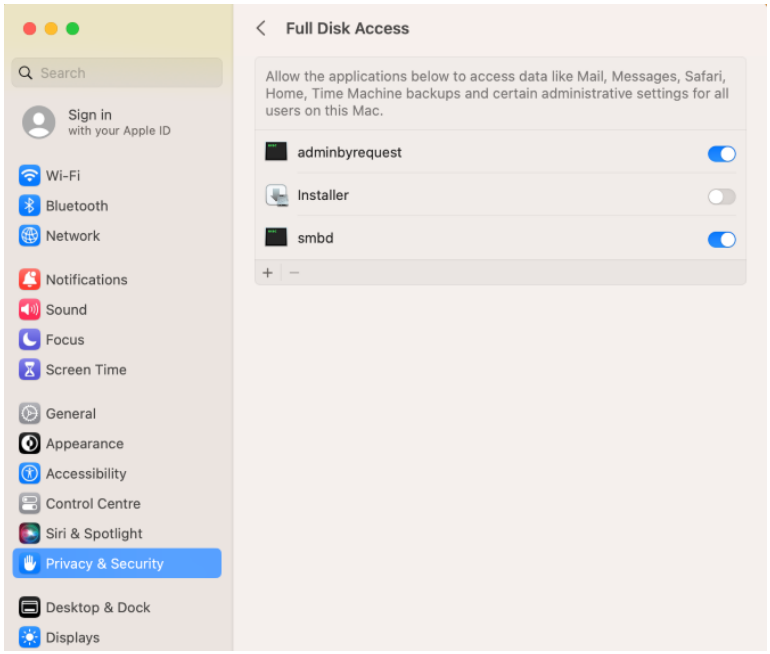


     3. Lock the tab to save changes.

   - **macOS 13 (Ventura)**.

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

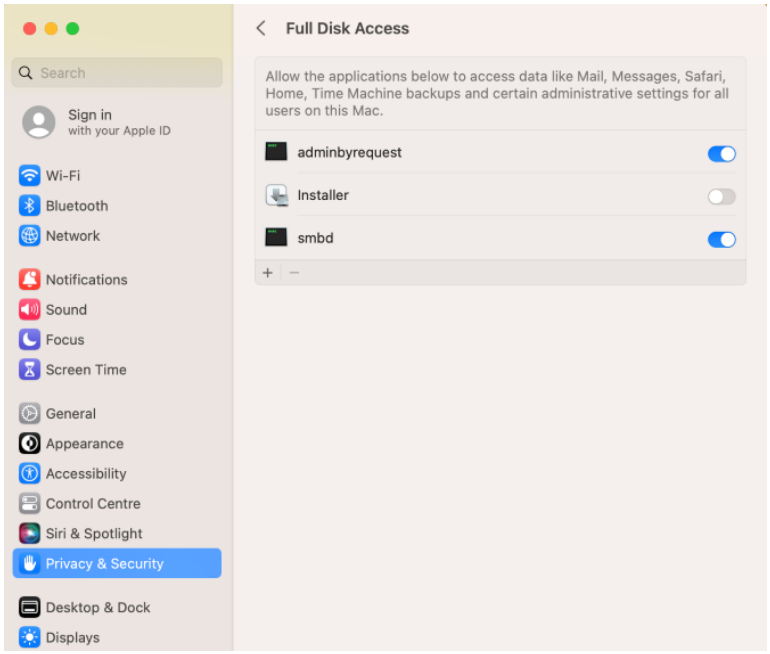
2. Select **adminbyrequest** in the list of apps (ensure the box is checked):



3. Lock the tab to save changes.

- **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 **adminbyrequest** in the list of apps (ensure the box is checked):



3. Lock the tab to save changes.

2. **Using Jamf**.

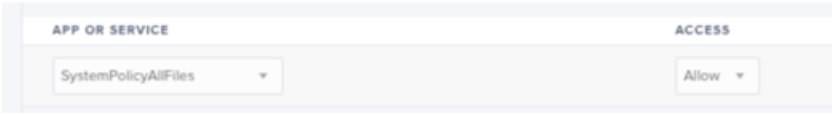
   Jamf uses *Configuration Profiles* to manage Mac endpoints:

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

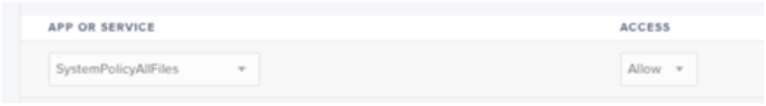
         ```
         identifier "com.fasttracksoftware.adminbyrequest" and anchor
         apple generic and certificate 1[field.1.2.840.113635.100.6.2.6]
         /* exists */ and certificate leaf
         [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate
         leaf[subject.OU] = AU2ALARPUP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

         > **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*.

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

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

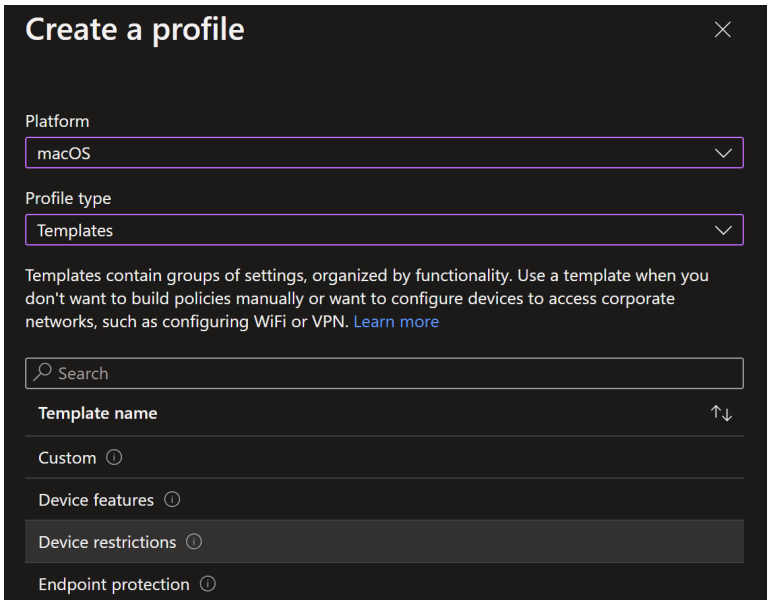
      5. Save the profile.
   4. Deploy and use this profile to enable FDA for all your macOS endpoints.

3. **Using Intune**.

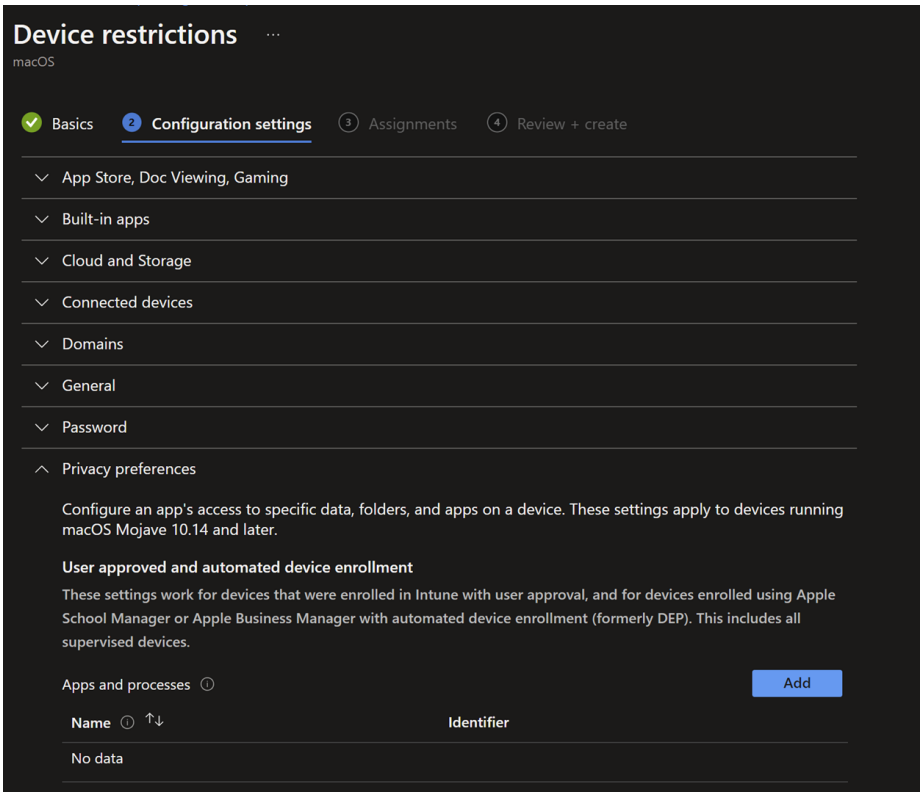
   Similar to Jamf, Intune uses *Configuration Profiles* to manage Mac endpoints:

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

- Template name: **ABR – FDA**



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



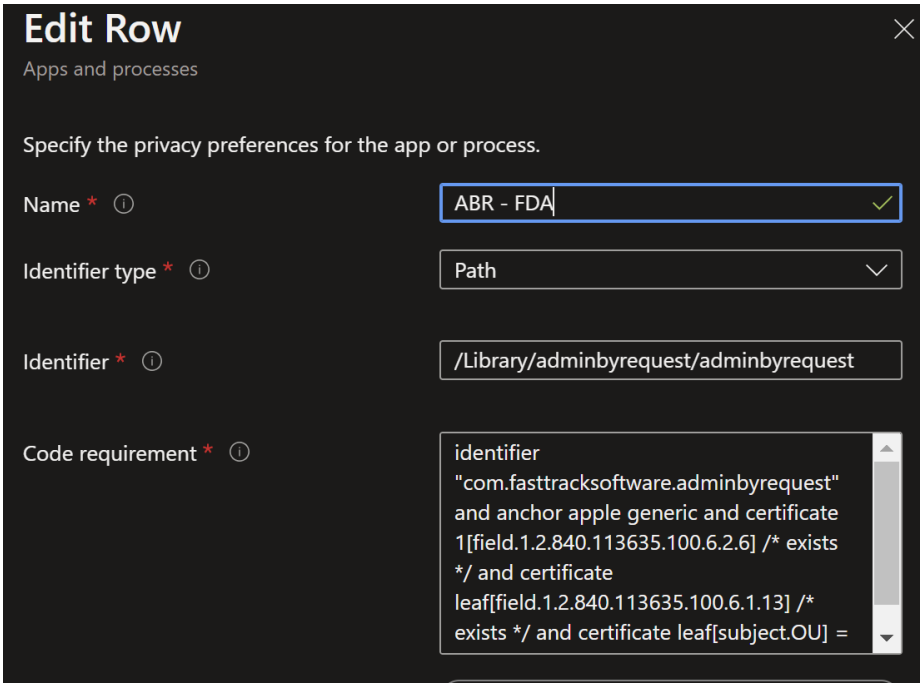
6. In the *Edit Row* form, enter the following:
   - Name: **ABR – FDA**
   - Identifier type: **Path**
   - Identifier: **/Library/adminbyrequest/adminbyrequest**

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

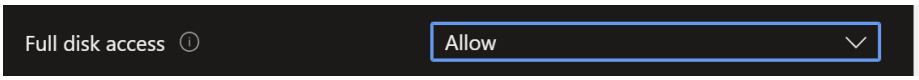
```
identifier "com.fasttracksoftware.adminbyrequest" and anchor
apple generic and certificate 1[field.1.2.840.113635.100.6.2.6]
/* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate
leaf[subject.OU] = AU2ALARPUP
```

> **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*.

The completed form:

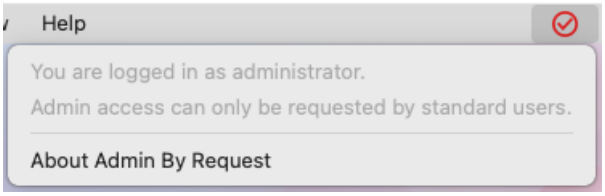


7. Finally, select **Allow** in field *Full disk access*:

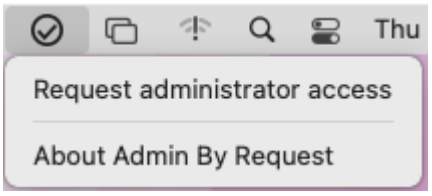


C. **Test the installation as a standard user**.

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 Admin By Request is working.

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.

> **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).

Refer to Resources > Documentation > Release Notes (macOS) for full details on what is covered in each new release.

Uninstalling Admin By Request

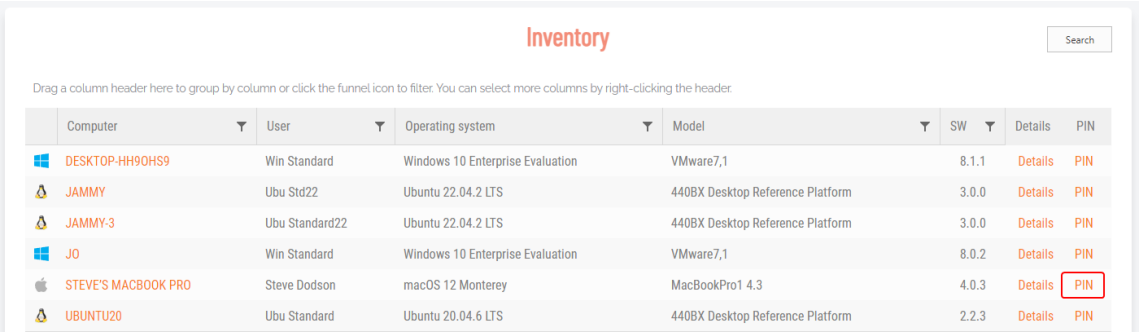
Three ways to uninstall Admin By Request on a macOS device are described here:

A. **Via Admin Portal PIN Code**.

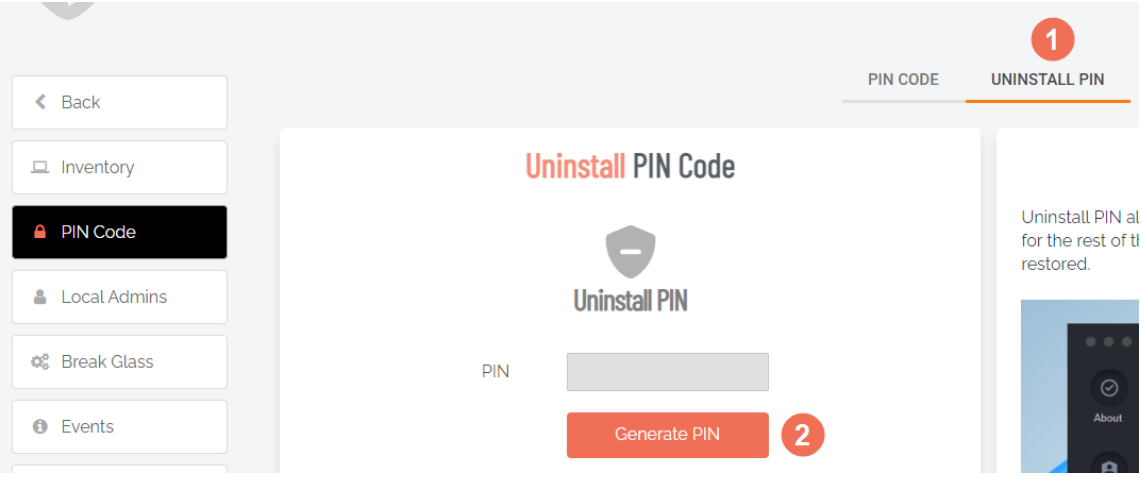
The first few steps in this procedure require access to the portal.

1. In the Admin By Request portal, navigate to the *Inventory* page and identify the device on which to perform the uninstall.

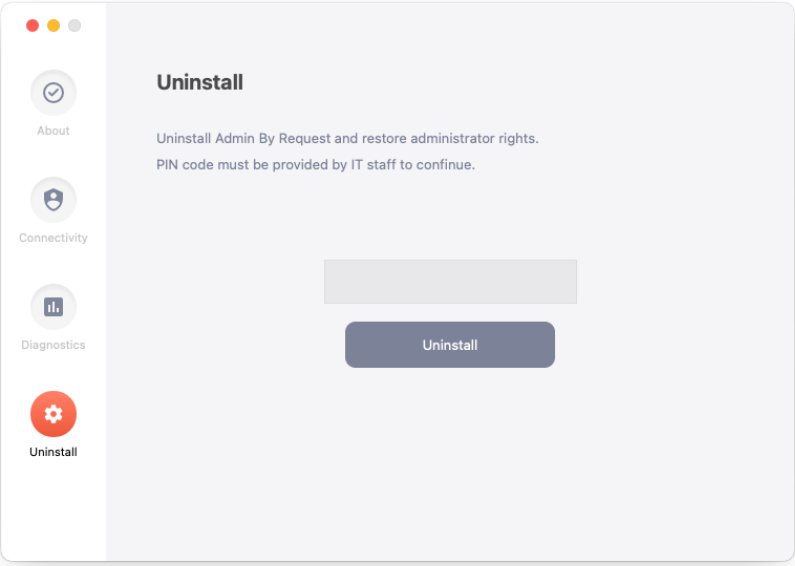
2. Locate the device in the inventory list - in the PIN column, click **PIN** for that device (columns can be switched around - the PIN column in your portal might not be the right-most column):



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

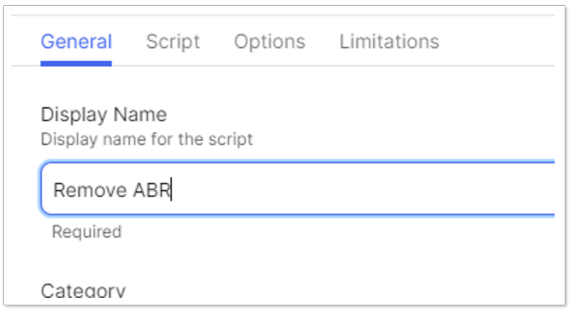


4. Back on the device on which you want to uninstall Admin By Request, select the *Admin By Request* icon from the top menu bar and click **About Admin By Request**.
5. In the *Uninstall* window, select **Uninstall** from the left button group, enter the PIN copied from the Portal, and click **Uninstall**:

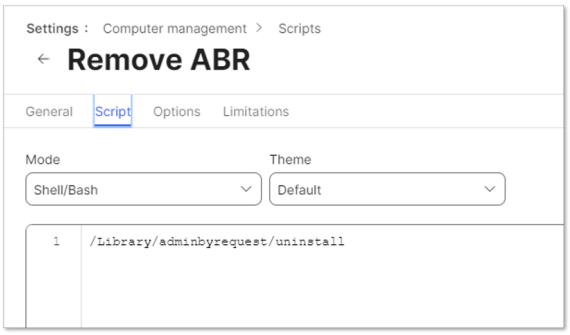


B. Using Jamf

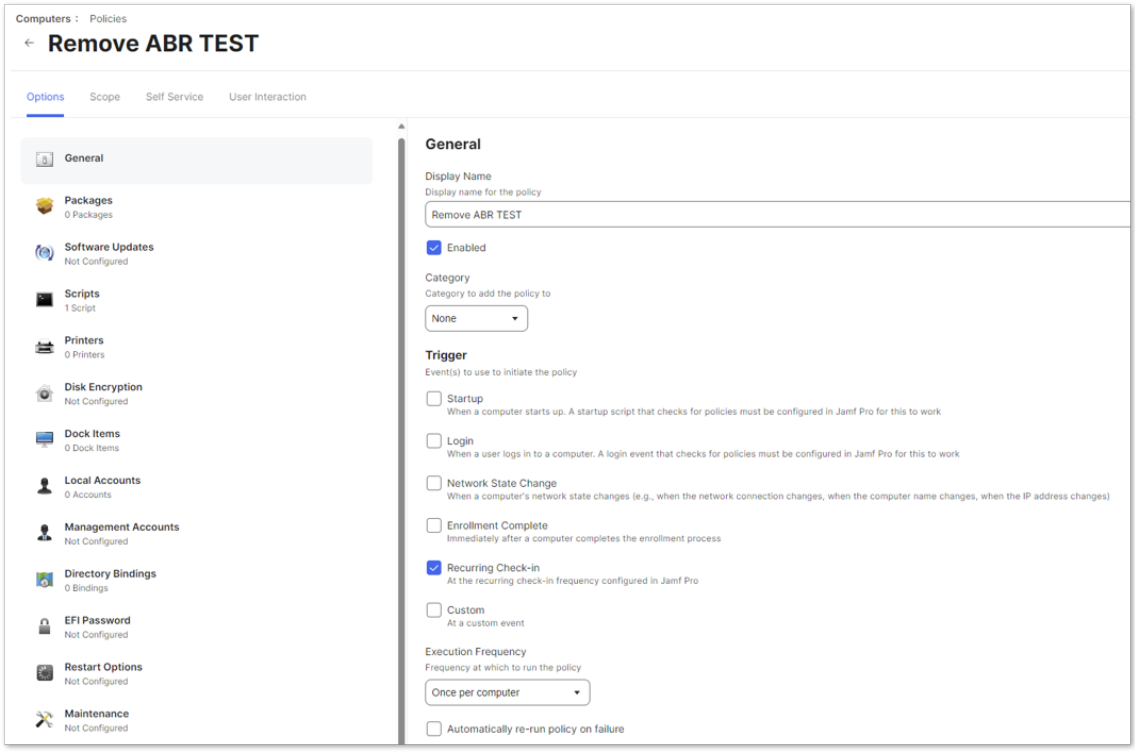
1. Create a script in Jamf.
   Go to **Settings > Computer Management > Scripts** and click **New Script**.
2. Enter a name for the script and open it:



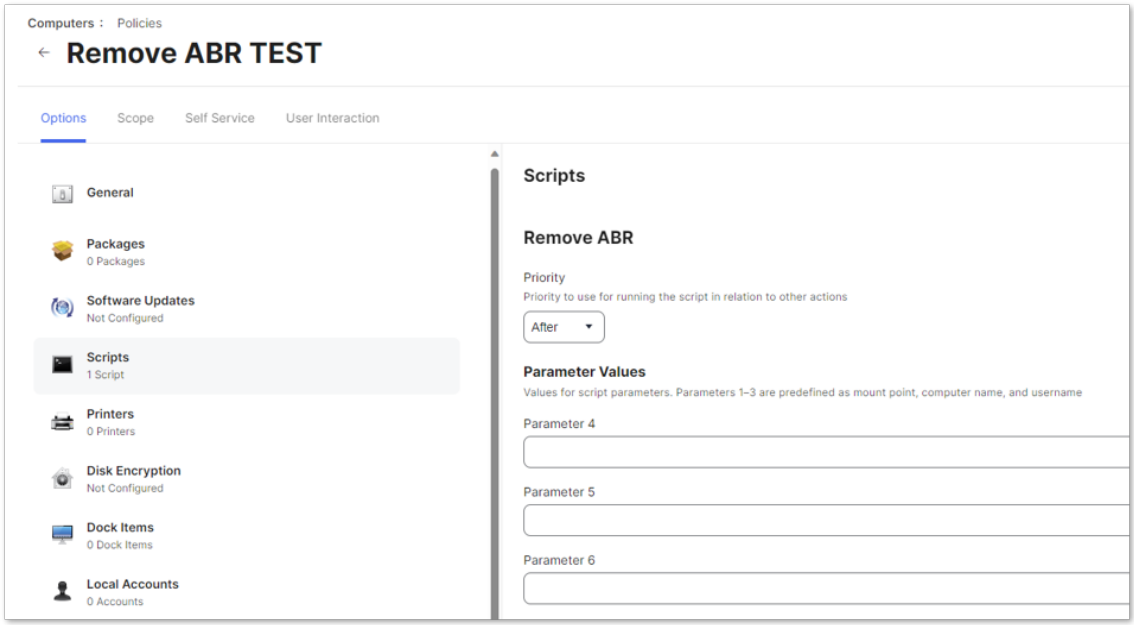
3. For *Mode*, select **Shell/Bash**, and enter **/Library/adminbyrequest/uninstall**:



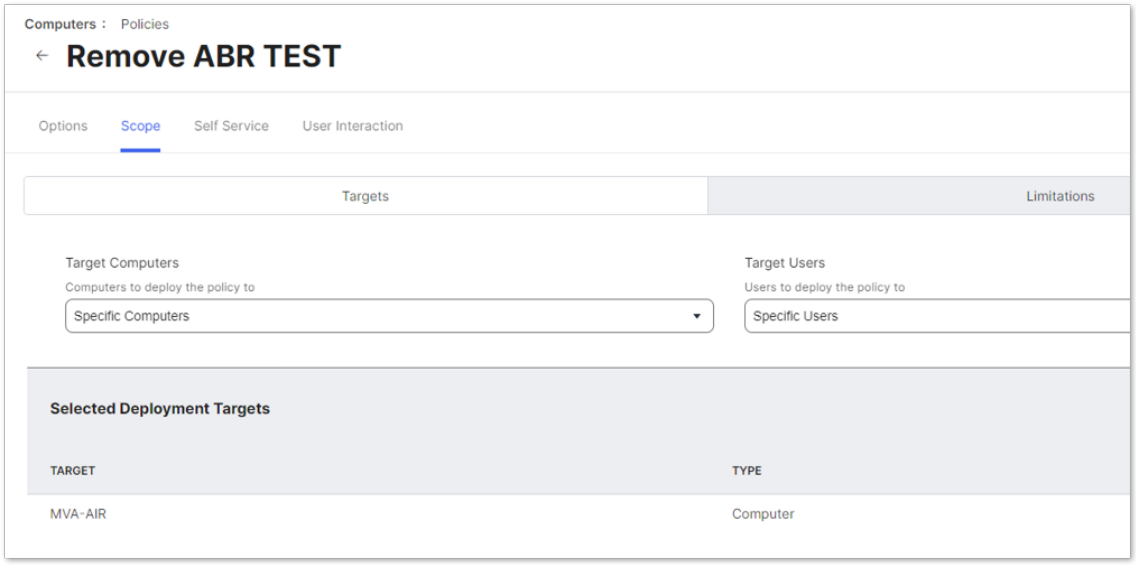
4. Click **Save** to save the script.
5. Next, create a policy for the deployment of the uninstall script (*Remove ABR* in this example).
   Enter the display name and choose an appropriate trigger for your deployment:



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 and /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 (**Settings Workstation 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 41 for more information (section *Technical Info*).

Tamper Prevention

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

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

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 macOS Client User Interface

Introduction

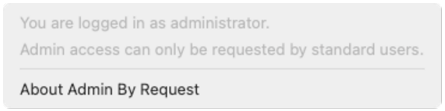
The user interface is graphical and is accessed via the icon menu in the menu bar (top right) of the screen.

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 tray icon is black:

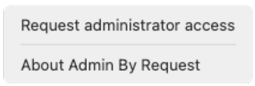
Administrator

Standard User

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):



Administrator

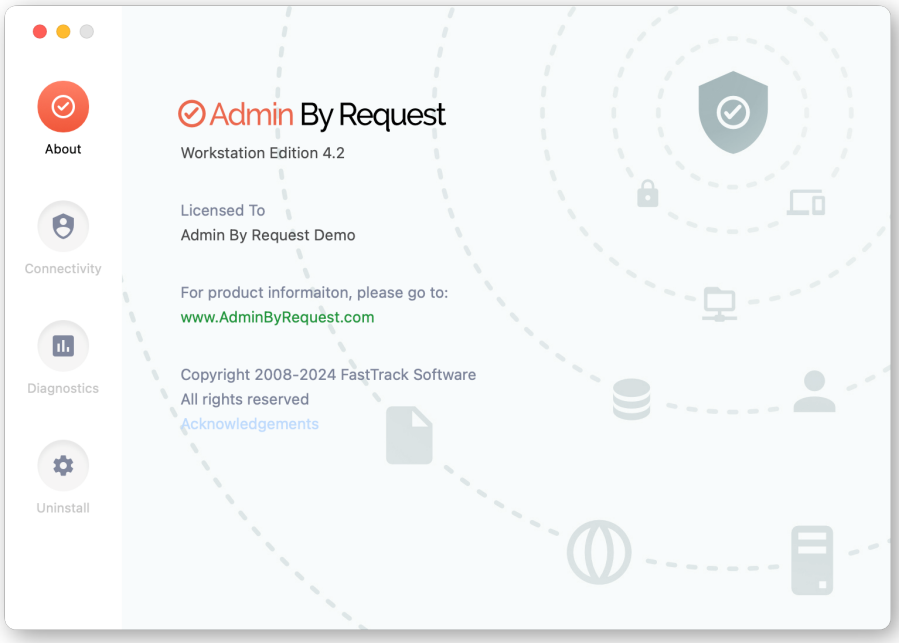


Standard User

In this topic

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:

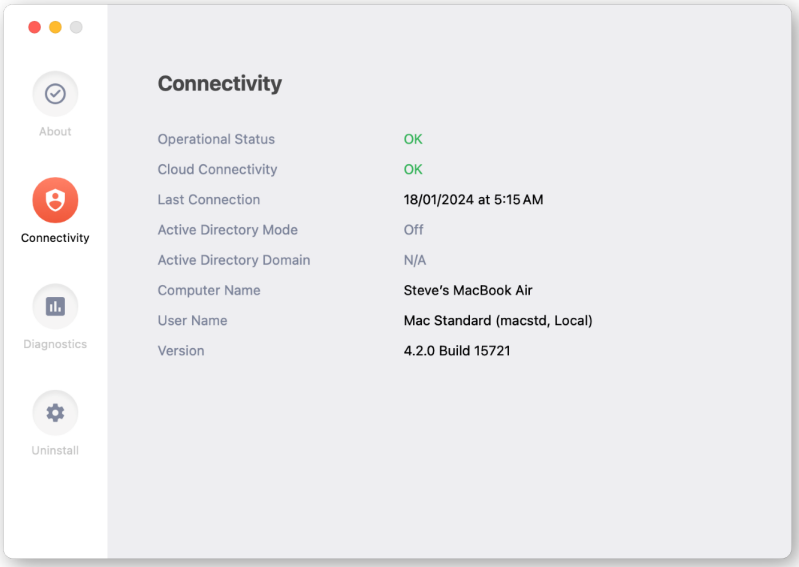


The default panel is *About Admin By Request*, which is accessed via the top button. It shows the current workstation edition, license details, website link, and copyright information.

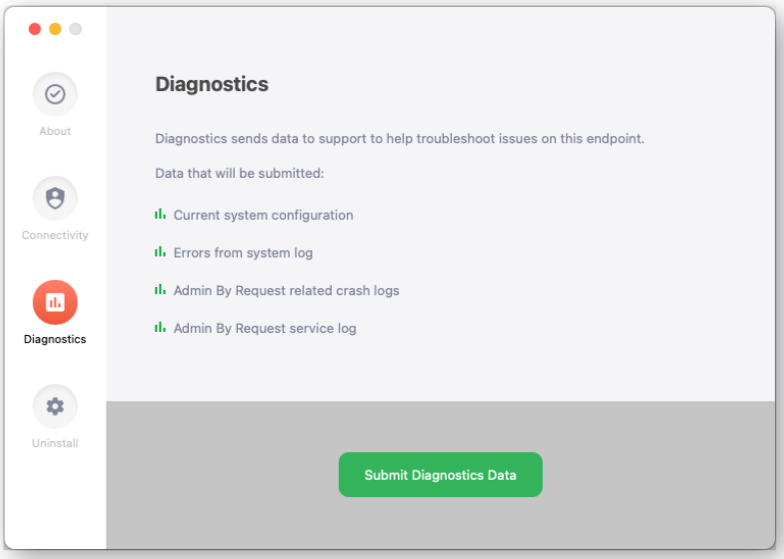
Click the *About* button to get back to this panel if viewing one of the other panels.

Other Panels (accessed via their respective buttons).

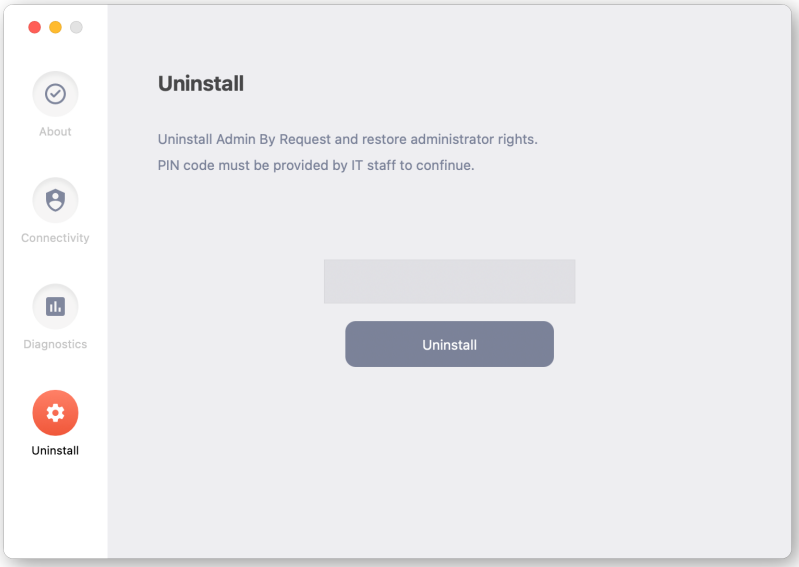
- **Connectivity** – displays the current operational status of the Admin By Request system, including Internet and Cloud connectivity, and details about the current workstation and user:



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



- **Uninstall** – enables administrators to uninstall Admin By Request from this workstation. See "Uninstalling Admin By Request" on page 10 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.

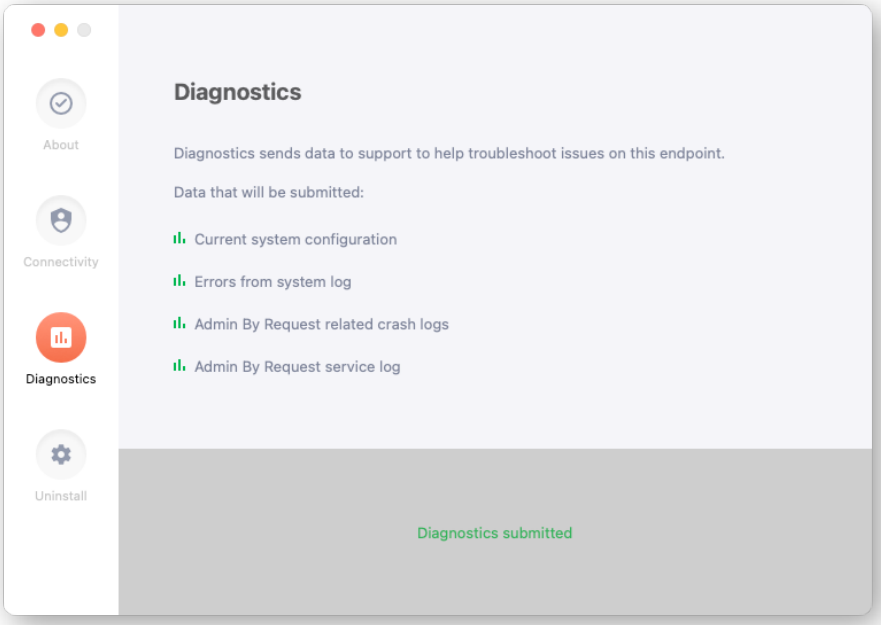
The following data is recorded and submitted:

- 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.

Using Run As Admin

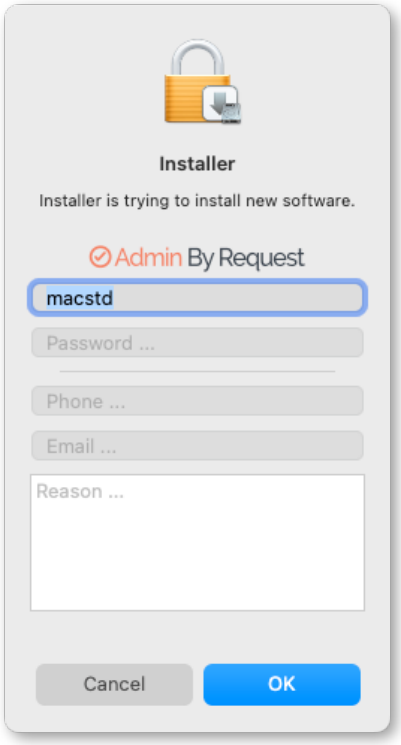
Run As Admin (also known as *App Elevation)* allows for the elevation of a single application.

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.

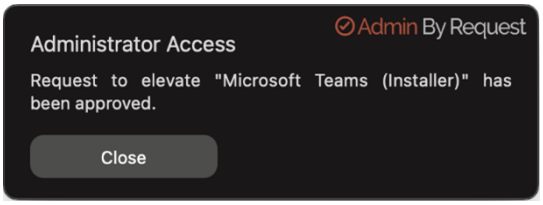
> **IMPORTANT:**
> Some Mac applications (e.g. Grammarly) require wide-ranging permissions to install properly and can only be successfully installed via an *Admin Session*. Further, these applications almost always require the same wide-ranging permissions when they auto-upgrade, meaning that another *Admin Session* must be started before upgrading the app.
>
> This is simply due to the nature of how processes work on the macOS operating system. When attempting to run an installation or upgrade via *Run As Admin*, a pop-up window prompting for admin credentials will be triggered by the OS whenever a separate executable that handles access to another area of the file system is invoked. At the time of writing, the only way around this is to carry out the installation or upgrade via an *Admin Session*.

A standard user executing a program that requires elevated privileges initiates the following sequence of events:

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



3. Admin By Request suspends installation and asks for phone, email, and reason. Enter these details and click **OK** to continue.
4. A notification now advises that the request for approval has been sent. When the request is approved, a further notification advises the request has been approved:



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

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

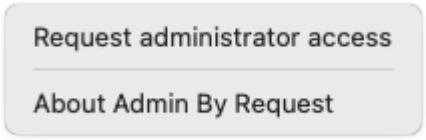
> **NOTE:**
> For .app files, *Run As Admin* can be initiated by dragging and dropping the application file over the Admin By Request Dock icon. At the account control pop-up, enter credentials and hit **OK** to run the installer as an administrator. Note that this works **only** for .app files; it does **not** work for .pkg files.

Check the audit log in the portal for details on the user, the endpoint, the application run and execution history.

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..

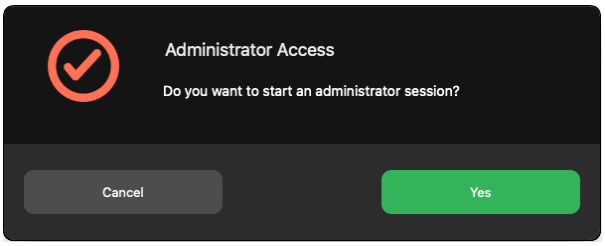
As with *About Admin By Request*, click the menu bar icon to display the menu and select **Request administrator access**:



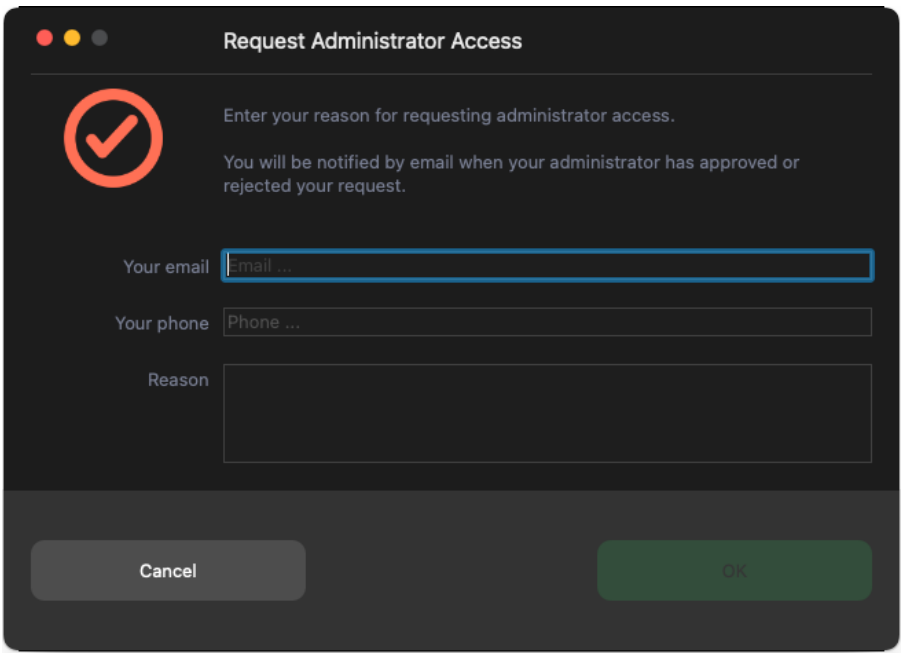
Submitting a request for administrator access is the primary mechanism for gaining elevated privileges.

A standard user making this selection 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:

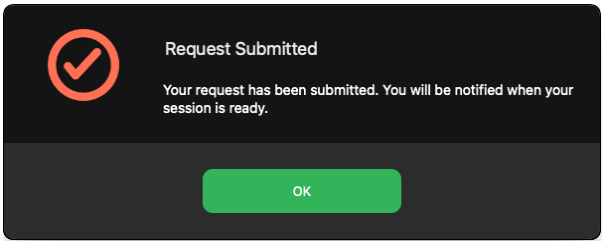


3. The user enters *email*, *phone* and *reason* information into the form and clicks **OK**.

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

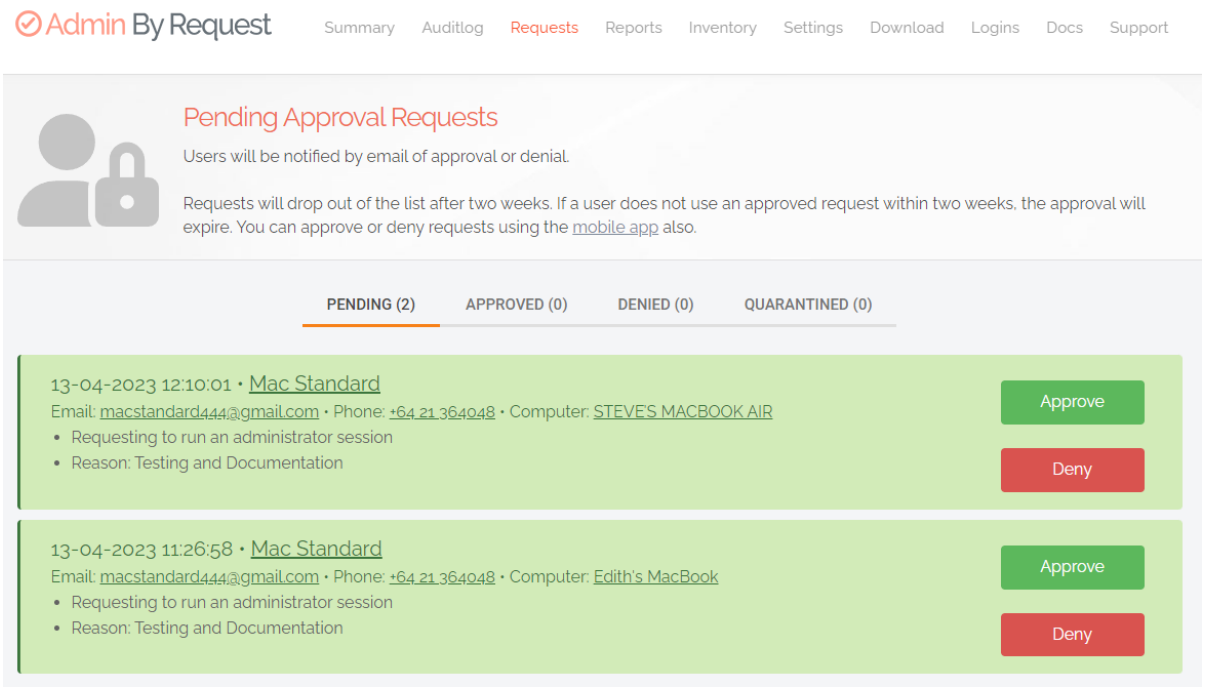
- If *Code of Conduct* is enabled, the user must acknowledge a Code of Conduct pop-up to continue (**Portal > Settings > Workstation Settings > macOS Settings > Endpoint > INSTRUCTIONS**).
- If *Require approval* is OFF, the approval steps are skipped (**Portal > Settings > Workstation Settings > macOS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

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

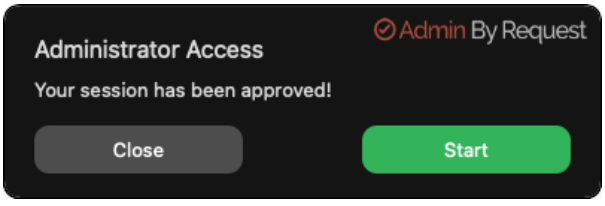


5. The IT administration team is notified via the Admin By Request portal that a new request for administrator access has arrived.

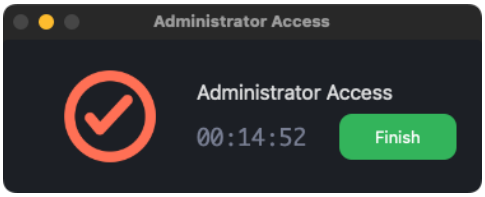
   The following example shows how two new requests might appear in the portal:



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



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



8. 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 29 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.

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 later 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.

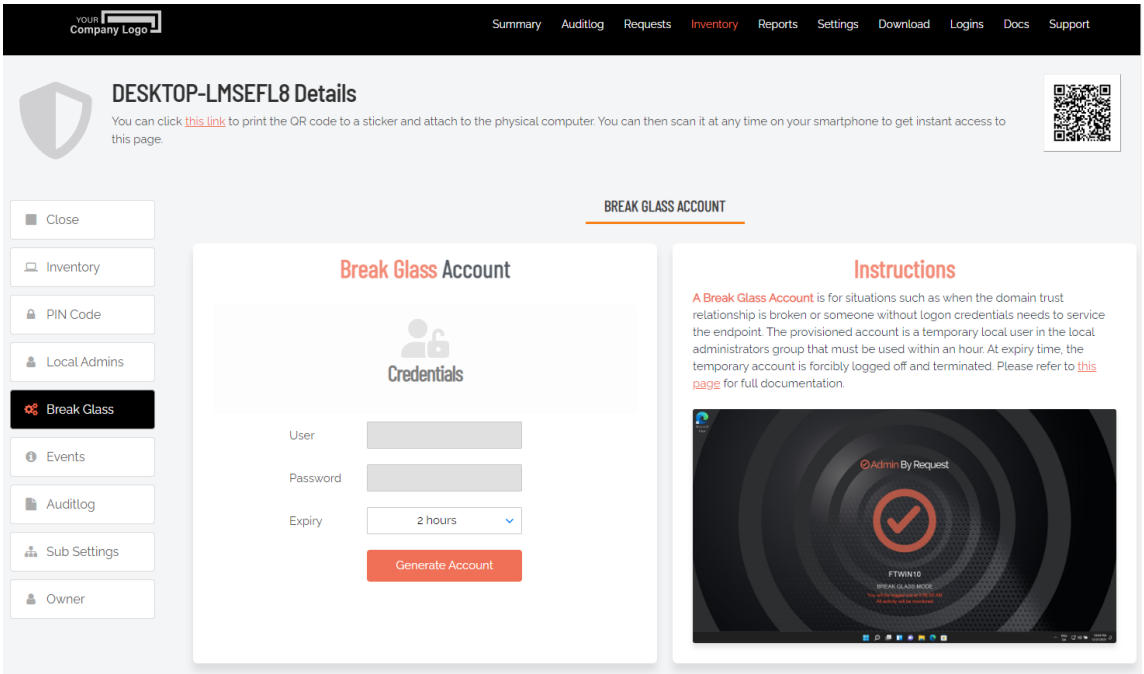
Using the Break Glass feature

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

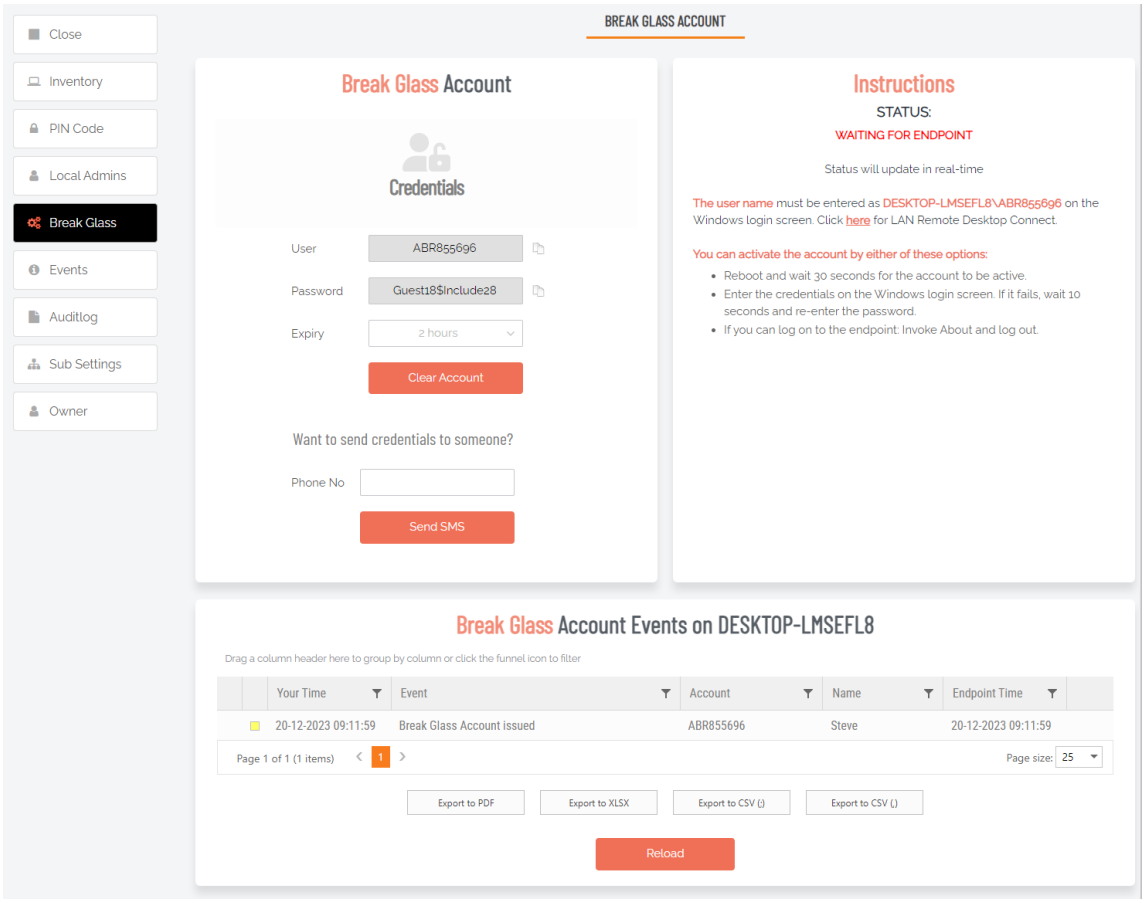
A. Generate

Create a Break Glass account:

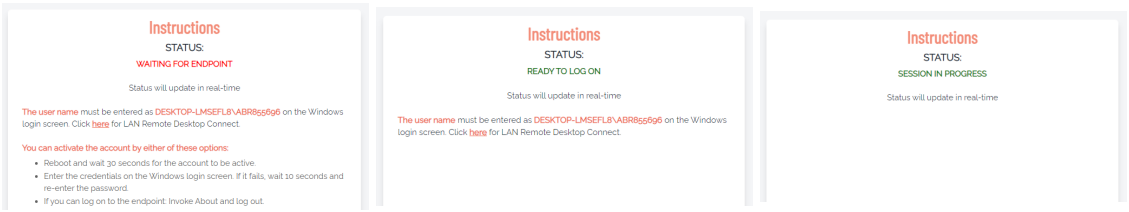
1. Log in to the Portal and navigate to the **Inventory** page. Select an endpoint on which you want to enable the Break Glass account and select **Break Glass** from the left-hand menu:

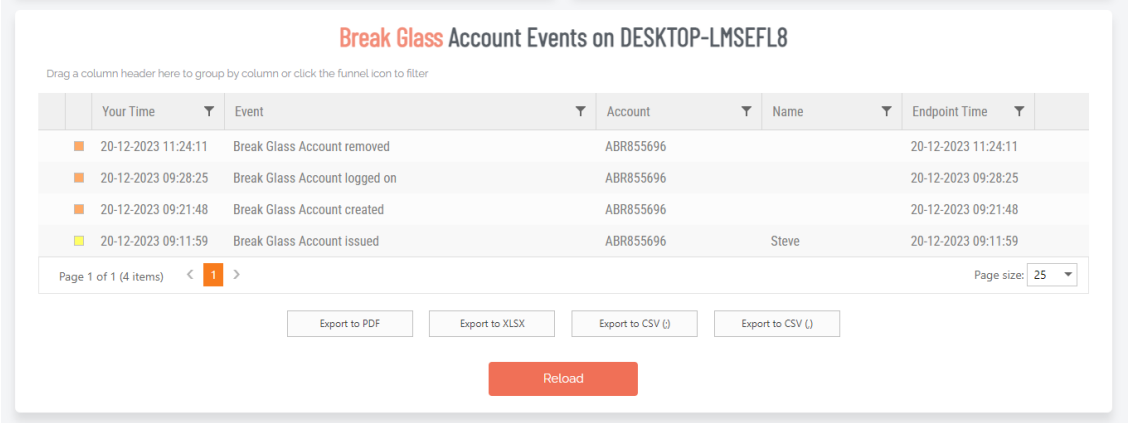


2. From the **Expiry** drop-down menu, select an amount of time for which you want the Account to be available. The default is **2 hours**, but the period can range from a minimum of 15 minutes, to an unlimited amount of time.
3. Click the **Generate Account** button, which issues a Break Glass account and displays its *User* and *Password* in the read-only text boxes:



4. 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.



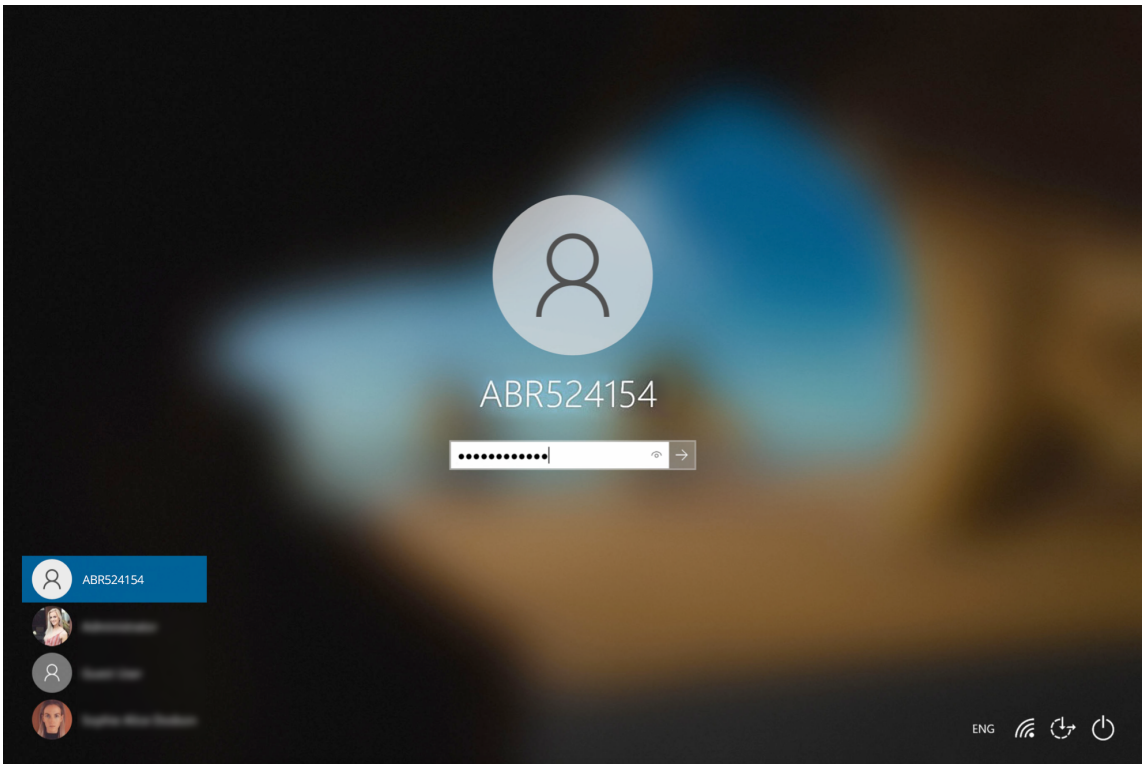


5. Optionally, you can send the new Break Glass account credentials via SMS (i.e., text message) by entering the intended recipient's mobile number into the text box and clicking **Send SMS**.

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).

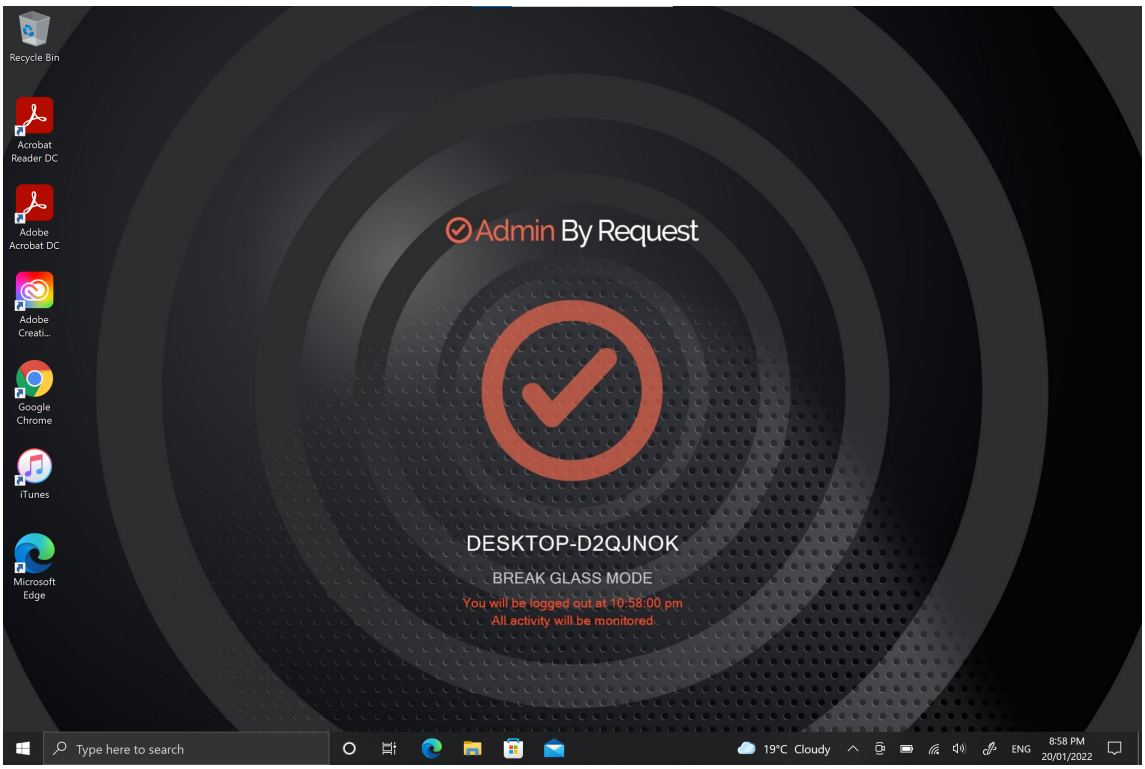
> **NOTE:**
> This may fail on the first attempt; if so, wait 10 seconds and then try again.

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.

Portal Administration for macOS

Introduction

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

Run As Admin Settings

Portal menu: **Settings > Workstation 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 "Enable Full Disk Access (FDA). " on page 4for more information.

Setting	Type	Description
Allow Run As Admin	Toggle On | Off Default: **On**	**On** - Allows users to elevate privileges for a selected file. Enables *Require approval* and *Require reason*. Disables *Block Run As Admin*. **Off** - Denies users the ability to elevate privileges for a selected file. Enables *Block Run As Admin*, which is how users with admin credentials can still elevate privileges.
Block Run As Admin (enabled only if *Allow Run As Admin* is Off)	Toggle On | Off Default: **Off**	**On** - Denies users the ability to execute *Run As Admin* even if administrator credentials are available (i.e. no authentication window is presented). **Off** - Allows users with administrator credentials to execute *Run As Admin* (i.e. authentication window pops-up asking for admin credentials).
Require approval	Toggle On | Off Default: **Off**	**On** - Sends a request to the IT team, which must be approved before elevation is granted. Makes *Require reason* mandatory (i.e. must be On). **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 *Require reason* 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. Reason must comprise at least *two words*. This information is stored in the Auditlog. **Off** - No reason is required by the user, but details of the actions performed are stored in the Auditlog.
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: **Settings > Workstation 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.

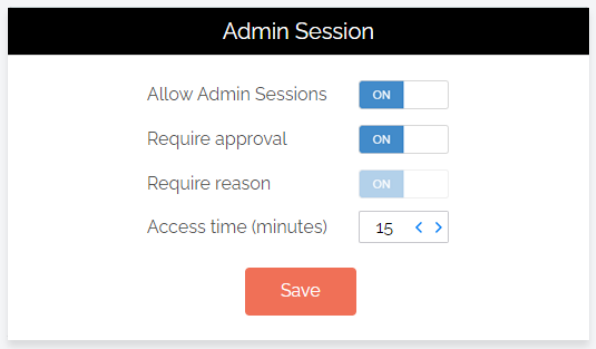
Setting	Type	Description
Allow Admin Sessions	Toggle On | Off Default: **On**	**On** - Allows users to effectively become a local administrator for the number of minutes specified in *Access time (minutes)*. Enables *Require approval*, *Require reason* and *Access time (minutes)*. **Off** - Denies users 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 *Require reason* mandatory (i.e. must be On). **Off** - Allows the user to become a local administrator as soon as the request is made. Makes *Require reason* 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:



3. Click **Save** when done.

Authentication Confirm Setting

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

Settings Table - System Settings

Confirm mode allows users to elevate applications with a single button click rather than entering their credentials.

Setting	Type	Description
User Authentication Mode	Selection Default: **Authenticate**	**Authenticate** - User must enter credentials to start the application. **Confirm** - User can confirm simply with "Ok" or "Cancel" to start the application.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

System Settings

Portal menu: **Settings > Workstation 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.
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.

Pre-Approval Settings

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

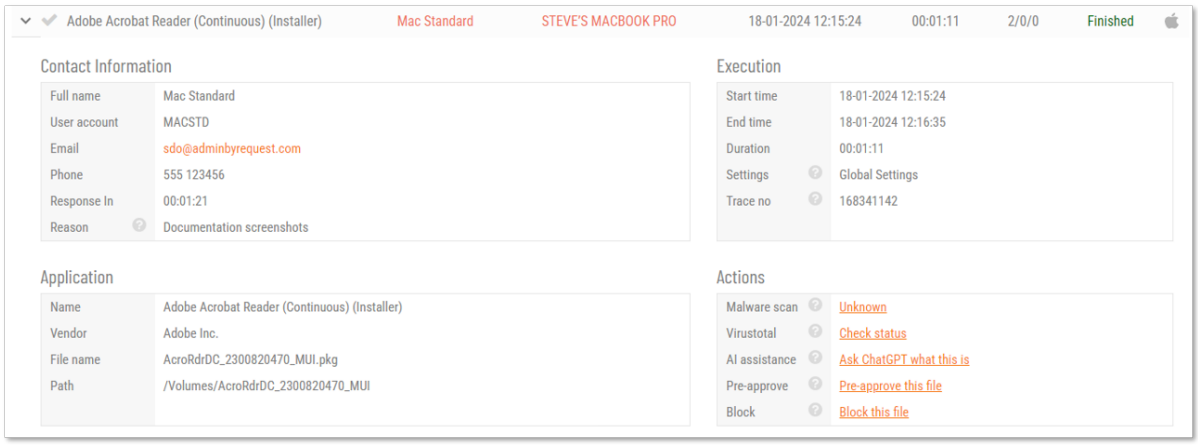
Pre-Approval (known sometimes as Whitelisting) refers to the method of working out which applications are trusted and frequently used, and adding them to a list that automatically allows users to elevate those applications when they need to. This is essentially the opposite of Blocklisting/Blacklisting – 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.

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).

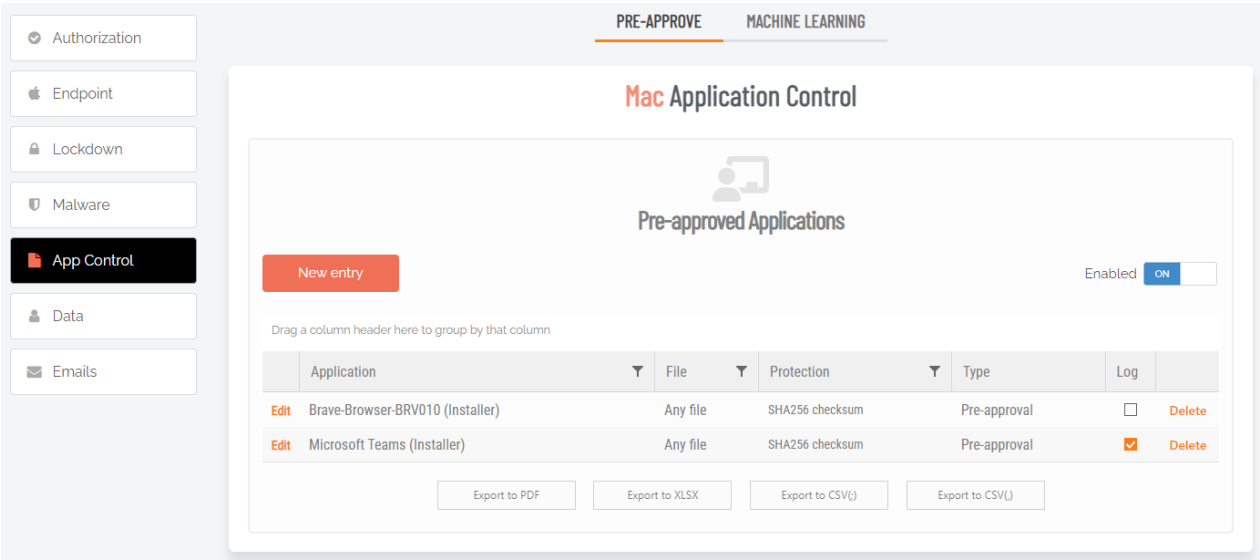
Once an application has been installed on an endpoint with Admin By Request:

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:



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:



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

For applications (.app)	For packages (.pkg)
Command: `codesign -d -vv /path/app.app`	**Command:** `pkgutil –check-signature /path/app.pkg`
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.

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-aproval 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 *User confirmation* 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 *Log to auditlog* 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 *Vendor* field and hides all other fields.
Vendor (enabled when *Run As Admin vendor pre-approval* is selected)	Text	Enter vendor name. Adding the app via the Auditlog will auto-populate this field.

Setting	Type	Description
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. **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: **Settings > Workstation 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: **Settings > Workstation 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.

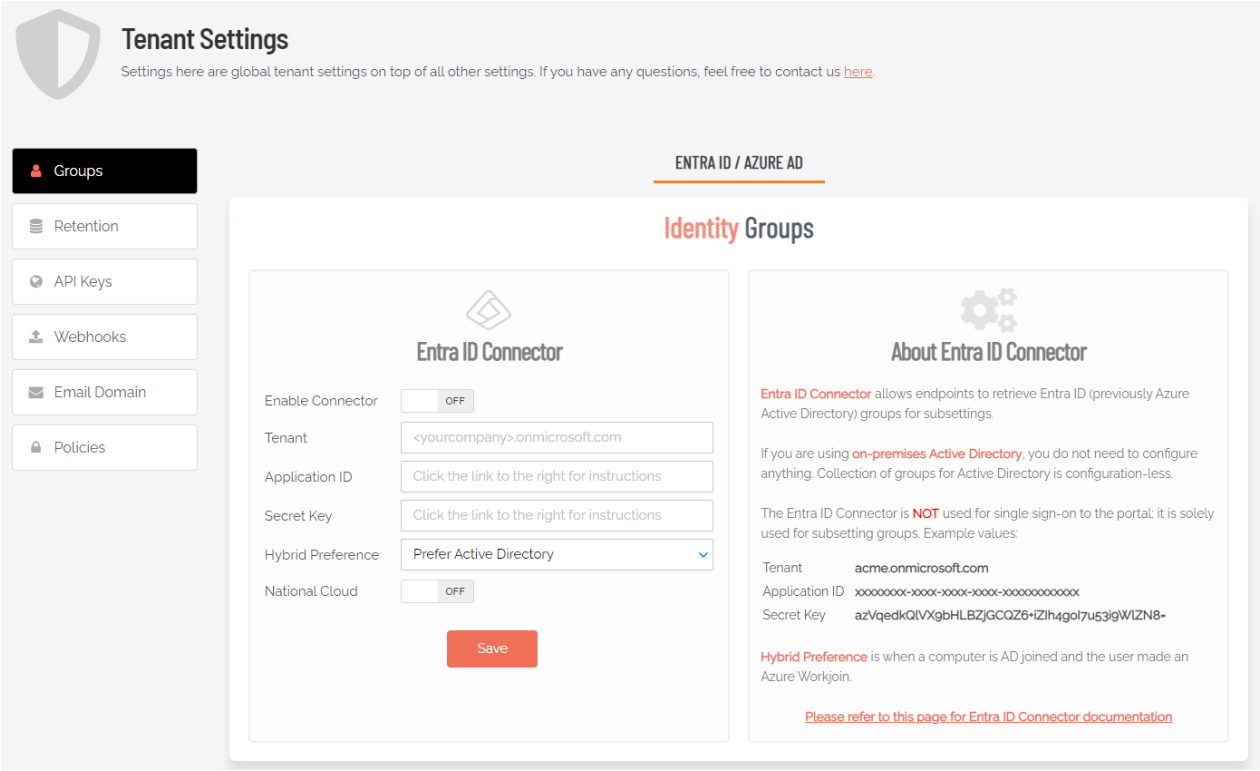
Entra ID Support

> **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 huge 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 the 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.

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

The Entra ID Connector is NOT used for single sign-on to the portal; it is solely used for sub-setting groups. Example values:

- Tenant **acme.onmicrosoft.com**
- Application ID **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**
- Secret Key **azVqedkQlVX9bHLBZjGCQZ6+iZIh4gol7u53i9WlZN8=**

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.

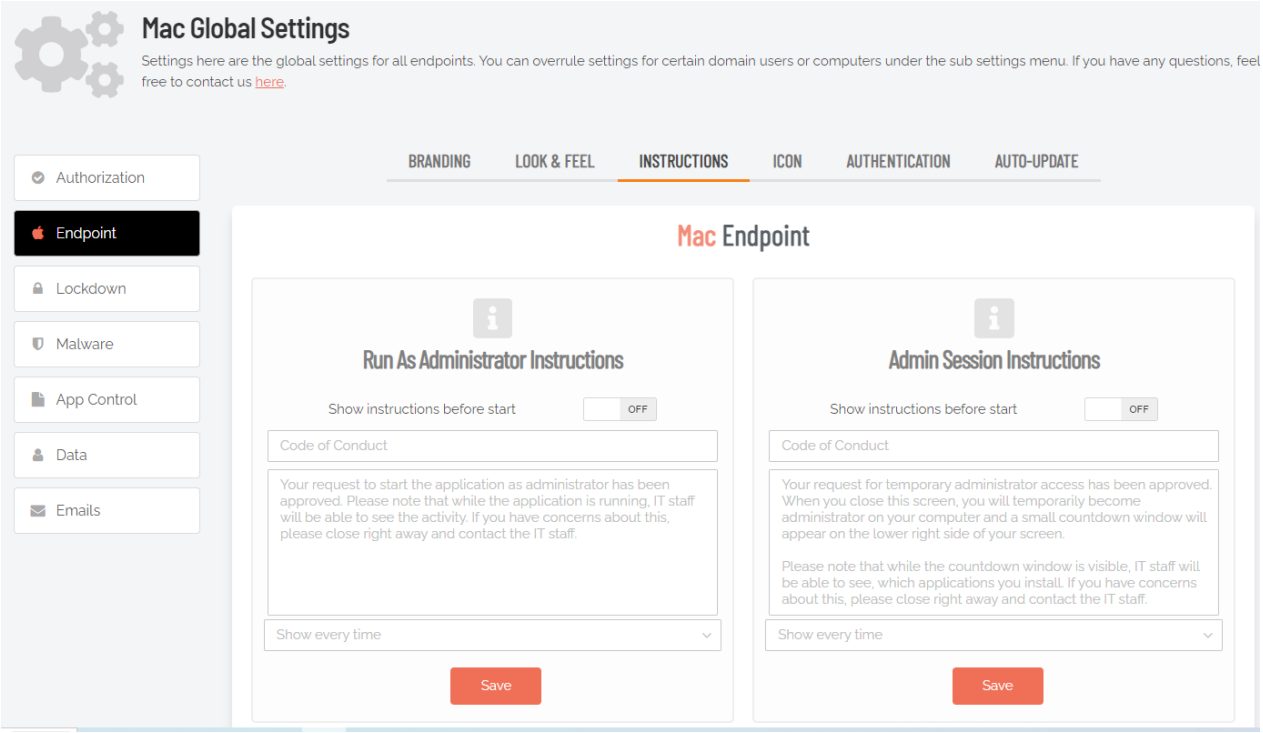
> **NOTE:**
> The *National Cloud* regions of Azure are designed to make sure that data residency, sovereignty, and compliance requirements are honored within geographical boundaries.

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: • **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 *National Service*, which is where the actual geographic instance is selected. **Off** - Disables selection of a physically isolated instance of Azure.
National Service (hidden if *National Cloud* is Off)	Selection Default: **US Government L4 / GCC High**	The geographic instance selected: • **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.

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:



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:

```
sudo killall adminbyrequest.
```

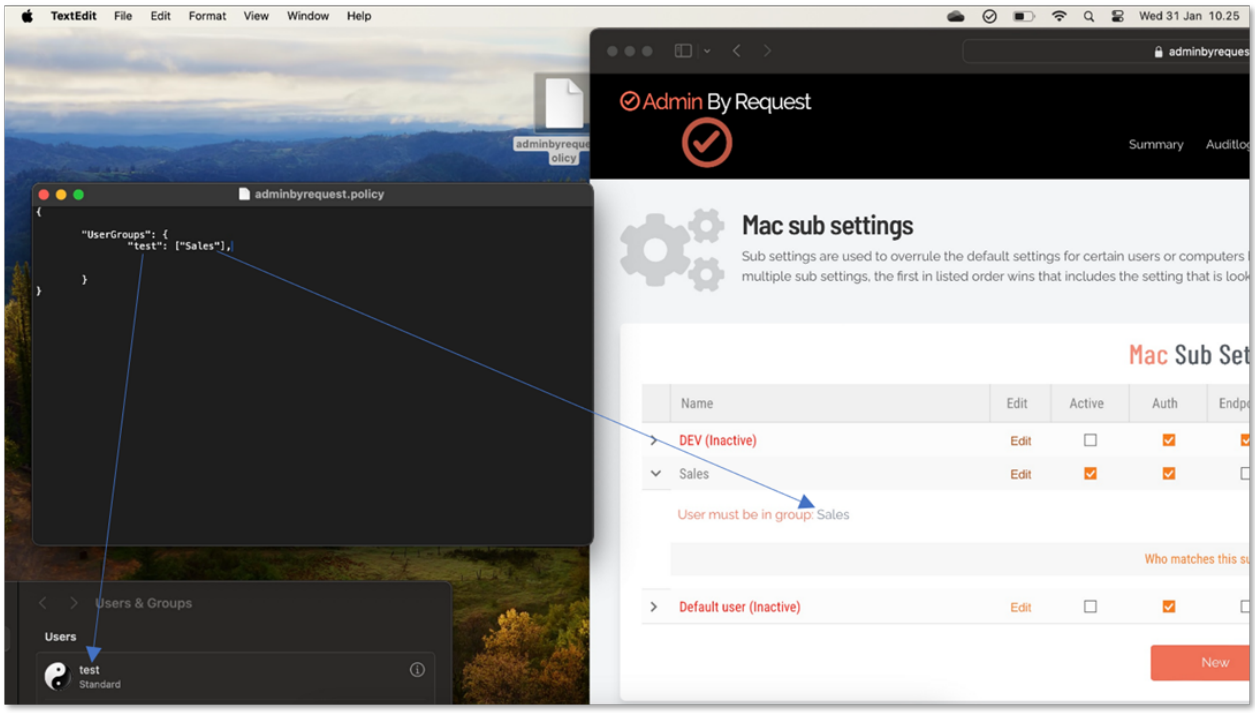
Key	Type	Default	Description
AdminMinutes	Integer	15	Number of minutes the user is administrator. This can also be set in your portal settings.
AllowAppStore	Boolean	1	Allow users to install software from the App Store without admin rights or an active Admin By Request session.
AllowSudo	Boolean	0	Allow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

Key	Type	Default	Description
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.
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.

Supplementary Technical Information

This section provides more information on the following:

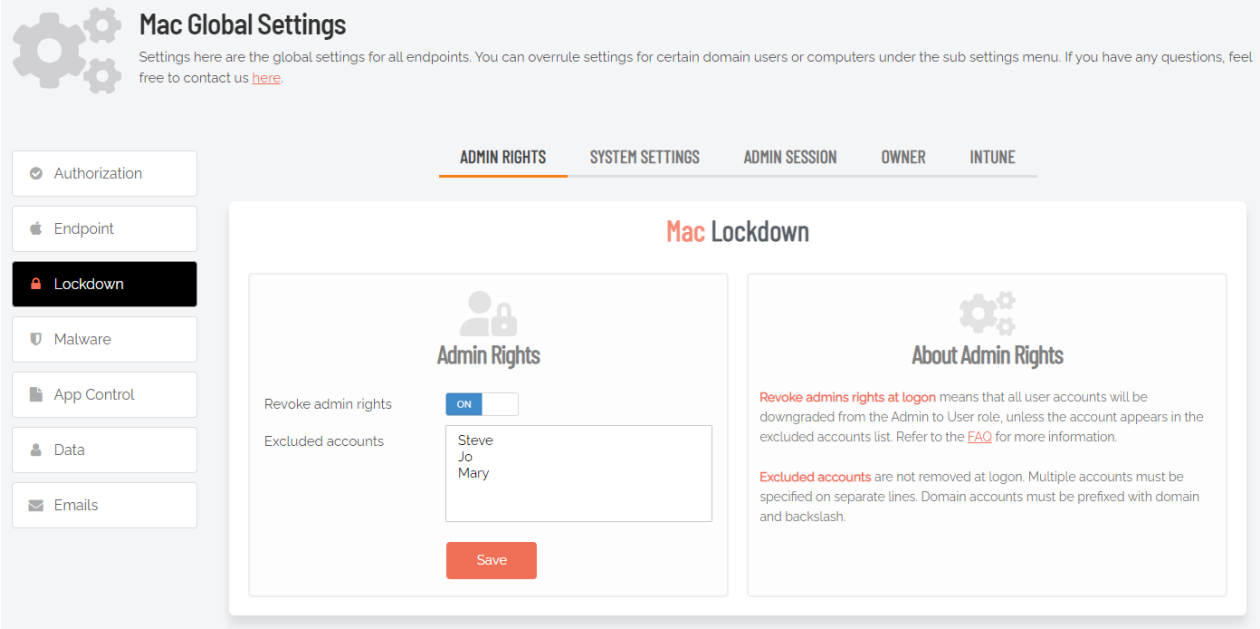
- Local Administrator Accounts
- Active Directory
- Sub-Settings
- Sudo
- Machine Settings
- Tampering

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.

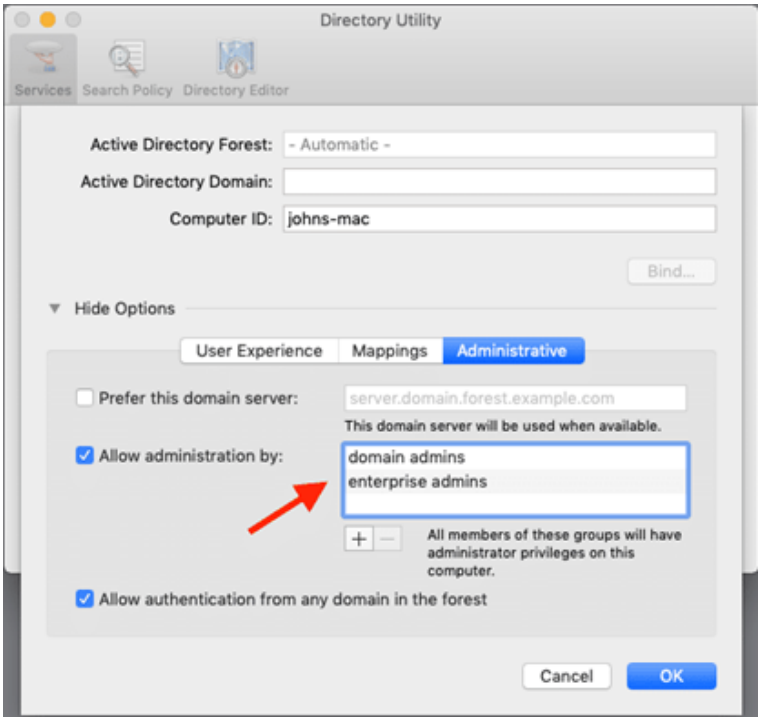
Also, if someone cleared the excluded accounts list and clicked **Save** by mistake, the result would be unusable endpoints; no users would be able to gain elevated privileges and would instead have very limited ability on their devices.

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



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. You can overrule settings for certain domain users or computers under the sub-settings menu.

Sub settings will *overrule* 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 38 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 38). We do not recommend enabling sudo access unless absolutely necessary.

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 38 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.

Removed in macOS Version 3.0 Onwards

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

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 47 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.

Term	Definition
Just-In-Time Access (JIT)	A way of enforcing the Principle of Least Privilege (POLP) by allowing access to privileged accounts and resources only when it is needed, rather than allowing "always on" access (also known as "standing access"). This reduces an organization's attack surface by minimizing the amount of time an internal or external threat has access to privileged data and capability.
Lateral Movement	A common technique used by malicious actors, in which they spread from the initial entry point further into the network, while evading detection, retaining access, and gaining elevated privileges using a combination of tactics. The purpose is generally to compromise as many accounts as possible, access high-value assets, and/or locate a specific target or payload.
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 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	Microsft 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	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. Passkeys are more secure than passwords and SMS OTPs, simpler for consumers to use, and easier for service providers to deploy and manage.
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.

Term	Short for	Definition
Jamf	Jamf	A UEM solution that manages Apple devices exclusively, via a single console, allowing users to self-enrol multiple Apple devices of their choice.
MAM	Mobile Application Management	Software and processes that secure and enable IT control over enterprise applications on end users' corporate and personal devices.
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.

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: • New *Owner* feature • New *Intune Compliance* 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: • New *System Setting* lockdown feature • New *Authentication Confirm* 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 *Using Run As Admin*, 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 Blocking 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.

Index

O

P

R

S

T

U

V