Release Note

Admin By Request
ZERO TRUST PLATFORM

Release Information

Product Platform: **macOS**
Product Version: **5.0**
Date: **26 August 2024**

What's New in Mac 5.0?

Introduction

Admin By Request for Mac 5.0 includes a number of significant updates. These allow for easier client installation, more conventional app install and updating, better auditing and local admin control, and the introduction of MFA and Support Assist for macOS clients.

In this document

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

Prerequisites

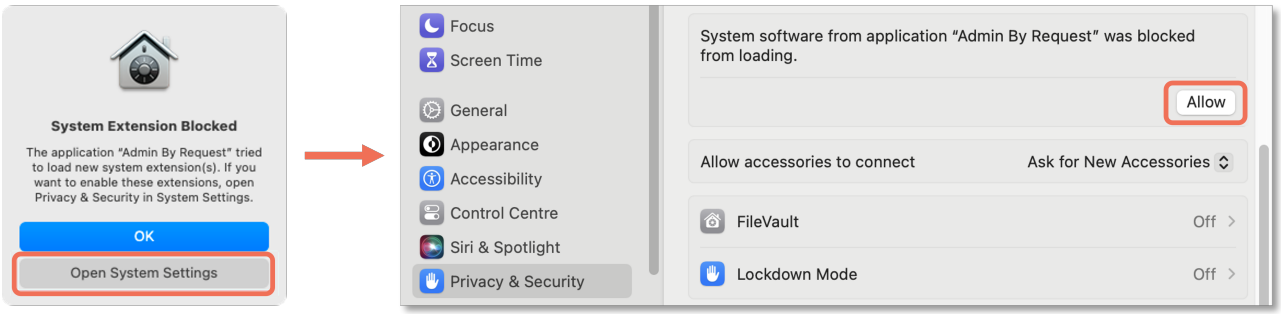
Organizations wishing to test endpoint clients running Mac 5.0 need the following:

- Access to the test portal at **https://test.adminbyrequest.com**
- Admin By Request for **Mac 5.0.0**, **build 15733**+ on each test client

Easier client installation

Installing the Admin By Request endpoint client is now more straightforward, allocating extensions and prompting for permission as required:

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:
4. Continue with the installation, providing Administrator credentials if necessary:
5. 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.

The endpoint client can also be installed via MDM - refer to chapter "macOS Client - Install / Uninstall" in document **macOS Client: IT Admin Guide** for a description of how to install the client using Jamf.

Conventional app installation

Prior to macOS 5.0, app installation required different procedures, depending on the type of install file downloaded. As well as double-clicking .pkg files, apps can now be installed by simply dragging to the Applications folder.

Using *Run As Admin* for app install

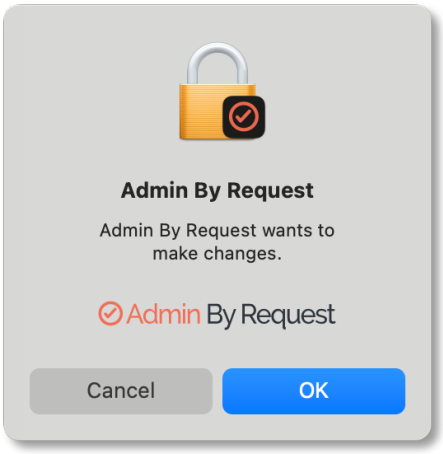
Run As Admin (also known as *App Elevation)* allows for the elevation of a single application.

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.

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 (VLC in this example).
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 pops-up, click **Open** to continue.
3. Admin By Request suspends installation and checks the organization's portal settings:
   - If authorization is required (**Settings > Mac Settings > Authorization > AUTHORIZATION**), it will ask for phone, email and reason, which must be submitted and approved before installation can proceed.
   - If authentication is required (**Settings > Mac Settings > Endpoint > AUTHENTICATION**), a prompt will appear that matches the portal setting; **Confirm**, **MFA** or **Authenticate** (with credentials).

   For example, if the portal setting is **Confirm**, the user simply has to click **OK** to continue:



4. Installation proceeds to completion and Admin By Request displays a note from the application installer saying that installation has completed successfully.

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

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

For more information, including additional examples, refer to section *Using Run As Admin* in chapter "The macOS Client User Interface" of document **macOS Client: IT Admin Guide**.

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).

Authentication via MFA

Multi-Factor Authentication is now available for macOS endpoint clients.

> **IMPORTANT:**
> At the time of writing, MFA is available only to users logged-in under **Azure SSO**.

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

Setting	Type	Description
Authentication Mode	Choice: • **Confirm** • **Multi-factor Authentication** • **Authenticate** Default: **Confirm**	**Confirm** - User must confirm with **Yes** or **No** (or via the reason screen) to perform the operation.. **Multi-factor Authentication** - User must validate identity using MFA through Single Sign-on. Choosing this option unhides *Multi-factor Configuration* (see table below). **Authenticate** - User must validate with credentials, face recognition, fingerprint, smartcard or similar..
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 Authentication Mode.

Setting	Type	Description
Sign-on method	Selection: • **Azure AD / Office 365** • **-- ADD NEW METHOD --** Default: **Azure AD / Office 365**	**Azure AD / Office 365** - Use this as the SSO method. **-- 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: • 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 Support[1]. 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.

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

Setting	Type	Description
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

Support Assist capability

Admin By Request Mac 5.0 introduces *Assistance* to the feature set for macOS endpoint clients.

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.

For more information, including an example scenario, refer to section *Requesting Assistance (Support Assist)* in chapter "The macOS Client User Interface" of document **macOS Client: IT Admin Guide**.

For information on creating smaller subsets of users/computers for more granular access control, refer to configuring sub-settings online.

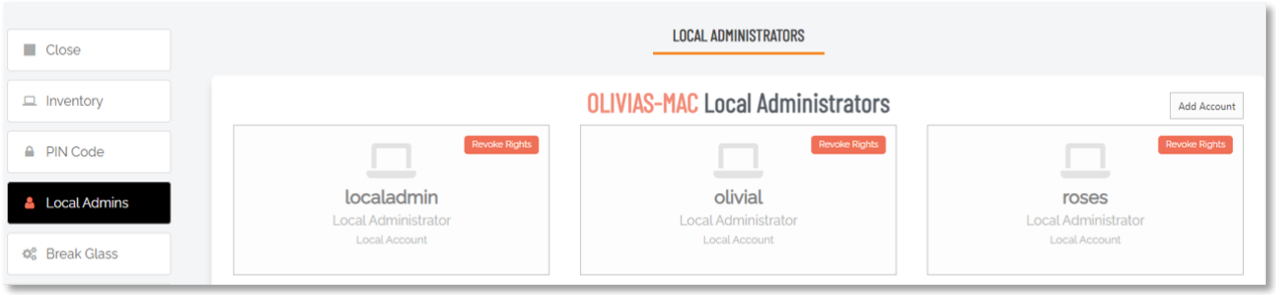
Control local admin rights from the portal

IT administrators can now easily clean up local admins on an endpoint by simply revoking their rights directly from the portal.

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**:



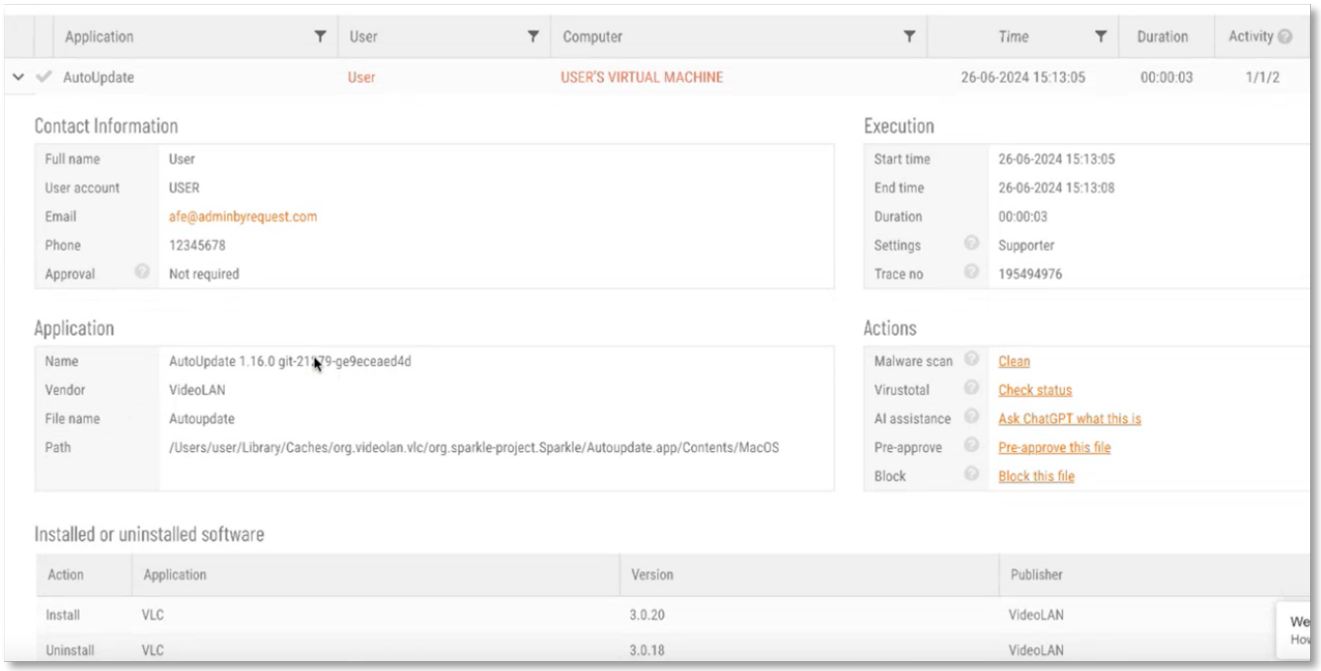
4. Finally, identify the users who should not be admin and use the **Revoke Rights** button to remove their administrator privileges.

For more information, refer to section *Clean up Local Admins* in chapter "Portal Administration for macOS" of document **macOS Client: IT Admin Guide**,

Better admin auditing

Auditable events are now fully logged in the Auditlog and/or the Events log, including sudo commands executed and steps taken to upgrade an app (e.g. **Uninstall** old version, followed by **Install** new version). As with events logged for apps on Windows clients, macOS apps can be pre-approved or blocked directly from the Auditlog.

In the example below, the program performing the update for VLC is **Autoupdate** from VideoLAN - other vendors will have different names for their update programs:



How does the Update Process work?

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.