Spec Sheet

Admin By Request
ZERO TRUST PLATFORM

Endpoint Privilege Management

Product Platform: **Mac**
Product Version: **6.0**
Document Date: **26 October 2026**

Introducing Admin By Request

The powerful, highly compact EPM solution for macOS Workstations. Built on the company's extensive experience writing highly robust, portable & powerful network applications, Admin By Request (ABR) for Mac is simple to deploy, easy to use and affordable to organizations of all sizes.

ABR enables IT departments to identify *Local Admin* rights usage, automate rights revocation and replace permanent un-audited admin rights use with an easy-to-use per request or time-limited privilege elevation system that includes a full audit trail.

With ABR, both office-based and remote workers can safely perform tasks that would previously have required support tickets and valuable helpdesk time. Elevated rights operations such as printer setups, installation/removal of approved software and plugin management can all be safely performed by users, maximizing productivity whilst still maintaining full security framework compliance.

What is it?

ABR comprises two parts:

1. **On-premises endpoint agent (Windows, Mac or Linux)**. The agent initiates elevation requests and performs elevation workloads. When online, the endpoint communicates configured information to the portal (e.g. logs, requests and settings). Management portal communication is not mandatory for the solution to function: the agent keeps working offline, although services that need a connection (MFA, OPSWAT checks and portal approval) are unavailable until it reconnects.
2. **Cloud-based management portal**. A secure Microsoft Azure-managed enterprise-class SaaS hosted environment in which agent settings, computer inventory and elevation workflow requests are collected. The portal also enables mobile app & API functionalities.

ABR requires no additional on-premises infrastructure (servers, VM appliances, databases etc.); all that is required to start a full proof of concept is to sign up to our Free Plan, giving you a full product experience for a maximum of **25 endpoints, free, forever**.

Product Editions

Subscription	Max. Endpoints	License Model	OS Version	Support
Free Plan (ABR Workstation)	25	Free	macOS 15 (Sequoia) or later	None
Paid Plan (ABR Workstation)	Unlimited	Annual Subscription	macOS 15 (Sequoia) or later	Included

Easier Administration

Privilege Management

- Reduce the ability of malware and ransomware to spread
- Automatic revocation of Local Admin Rights with specific user exclusions
- Per app. or time-limited privilege elevation modes
- Entra ID / Microsoft 365 / SAML MFA elevation options, with Platform SSO as an identity source for Email match
- Allow or block Local Admin Rights for device owner, Intune compliance status, specific applications (by vendor, Team ID, Team ID and Bundle ID, or file checksum, optionally limited to a version range)
- System Settings pre-approval: choose which System Settings a standard user can change, with the rest left as macOS intends
- OPSWAT Meta Defender integration for 'in line' pre-elevation reputation checking
- 'Break Glass' feature (Enhanced LAPS) solution. Generate single use, time-limited full admin accounts with one click
- Managed sudo: pre-approve or block individual sudo commands, with every allowed and refused command audited



Auditing & Reporting

- Powerful inventory solution included as standard
- Full audit trail of user elevation activity, admin logons & software installs
- Schedulable reporting of key user activity
- API access to audit logs, request logs, PIN codes, security events and inventory for SIEM and external reporting
- Full settings log of all portal configuration changes

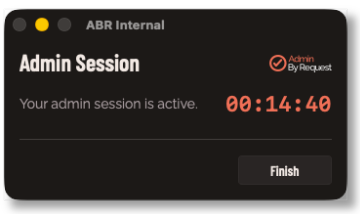


Convenience

- Simultaneous support for no-AD, multi-domain Active Directory and Entra ID endpoints
- No need to deploy server appliances or install software on existing server infrastructure; endpoint-only solution
- Zero config endpoint installer deploys using standard MDM tools such as Jamf and Intune
- Approve or deny elevation requests from your smart phone using our free mobile app.
- Keeps working offline, with a PIN code as the route to an Admin Session



Key Features



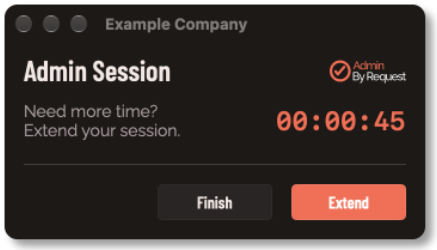
Time-limited Privilege Elevation

An *Admin Session* is activated by selecting **Request Administrator access** via the Admin By Request checkmark icon in the system tray (Windows) or icon bar (Mac and Linux).

With approval enabled, a portal administrator must process the Admin Session request as part of the elevation workflow. With approval disabled, the user gets to start the Admin Session automatically and become a time-limited administrator with a full audit trail.

Admin Session mode is ideal for users like developers who need the freedom to run multiple elevated applications within a set amount of time. Once the user either stops the timer or the time runs out, details relating to the session (processes run, software installed / removed) are uploaded to the portal.

Extend Active Session Timer



A user whose work is not finished can ask for more time on an Admin Session that is **already running**, instead of letting it expire and submitting a new request.

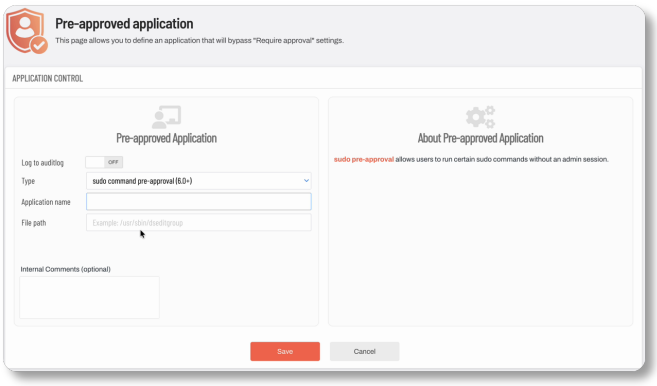
In the last minute of the session, the session window offers an **Extend** button. Note that extending *resets* the countdown to the number of minutes set in the portal; it does not add those minutes to the time left.

Extension is controlled by policy under **Mac Settings > Lockdown > Admin Session**: *Extensions* caps how many times a single session may be extended (from 1 to 5), and *Minutes* sets the length each extension resets the countdown to. Where extension is not allowed, the Extend button is not shown.

Remotely Terminate Elevated Access (Remote Kill)

Portal administrators can end elevated access on a Mac before it expires, covering both an active *Admin Session* and a *Run As Admin* elevation. Termination takes effect immediately: for an Admin Session, the user is removed from the local administrators group and any elevated applications are closed.

Remote termination is started from the auditlog, by expanding the running entry and using the **Remote Kill** panel. A *Blackout period* can be applied at the same time; while it is in force, the user cannot start a new Admin Session or Run As Admin request on that device, which gives IT time to investigate. The blackout expires automatically, and the auditlog records who ended the session.



Managed sudo

Managed sudo turns sudo on a Mac into a per-command policy decision. A *sudo command pre-approval* rule lets a standard user run a named command with sudo, without an Admin Session and without being made an administrator.

A *sudo command block* rule does the opposite: it withholds a sensitive command from a user who is in an Admin Session. Both rule types are created on the same **App Control** screen as application pre-approval and blocking.

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

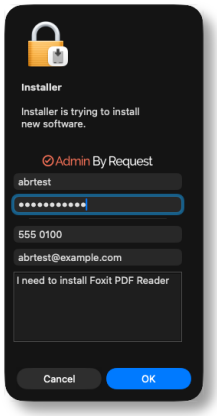
Permanent local administrators keep normal macOS sudo behavior and are not subject to managed sudo rules.

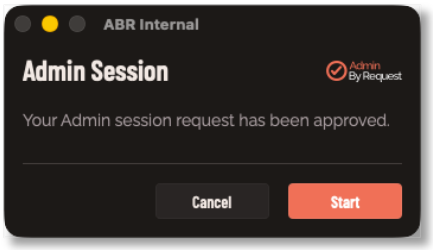
Per-app Privilege Elevation

With *Run As Admin* elevation mode, users can launch individual applications and run them with elevated rights on demand or with manual approval if required. When a launched application is elevated, the rest of the system remains in de-elevated state.

As requests are processed one at a time, this mode is best suited for users that need occasional ad-hoc elevation use.

On a Mac, *Run As Admin* starts when the user does something that needs administrator rights, such as dragging an app into the Applications folder to install it. Admin By Request intercepts the macOS administrator prompt and authorizes that one action, so users install apps the way they already know and need no additional training.





Elevation Approval (per request)

Elevation requests can be approved via the management portal, the mobile app or even through the API if enabled.

When a request is actioned by IT admins using one-click Approve or Deny, the requesting user receives the outcome of the request via email and/or desktop notification.

Off the shelf integrations with MS Teams, Slack, ServiceNow and Jira enable approval notifications to be sent out to groups using alternate team or ticketing applications.

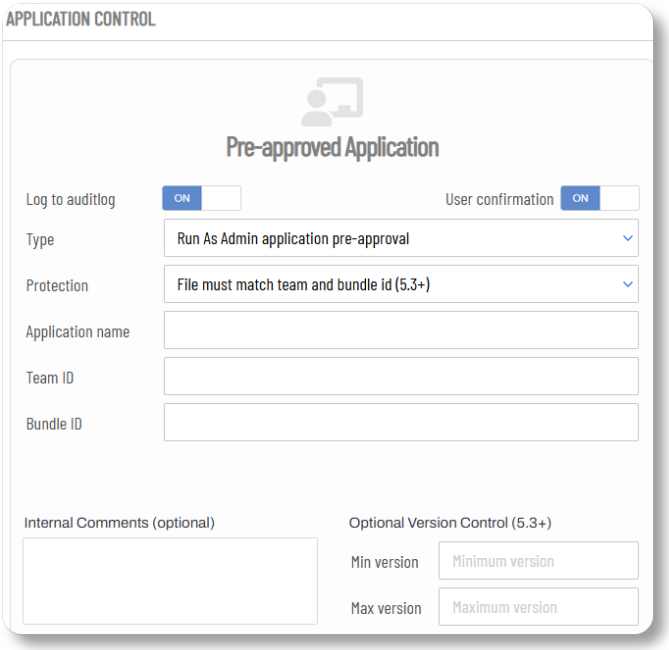
Elevation Approval (automated)

The *Pre-approval* feature is for situations where you would like to require approval for unknown applications, but allow automatic elevation for already vetted, specifically approved apps.

With application pre-approval, a portal administrator can set policies, either tenant-wide or per sub-setting (i.e. per group of users).

Policies can match on vendor, Team ID, Team ID and Bundle ID, or file checksum, and any rule can be limited to a minimum and maximum version.

Application rules can also be configured with user confirmation, requiring a user to click a 'yes/no' box at elevation, or without user confirmation, which lets supported, pre-approved actions go ahead in the logged-in user's session without the confirmation step.

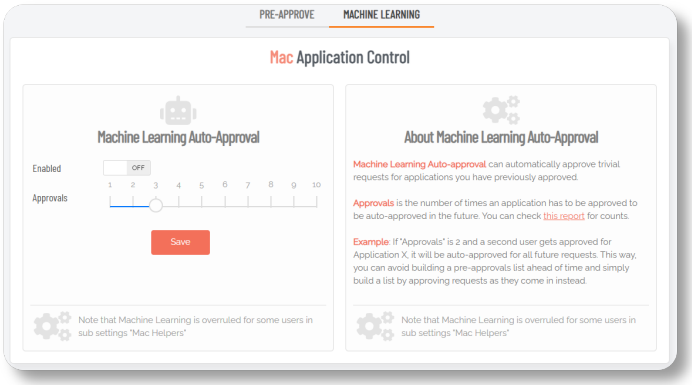


Skipping confirmation is useful for vetted apps that users run often. It is not a general service for running startup scripts as administrator, and MFA can still require user interaction, depending on policy.

Pre-Approval (machine learnt)

When both Approval and Machine Learning are enabled, the portal administrator can define a threshold over which manually approved applications are subsequently auto-learnt.

For example, setting the Machine Learning threshold to **3** would result in an application needing to be manually approved **three** times before being automatically approved.



After three manual approvals, the fourth elevation would not require manual approval - it (and all subsequent elevations of the app) would be automatically approved.

Machine Learning, like Pre-Approval is a sub-setting-configured feature, which means that different sub-settings can be configured with different Machine Learning thresholds. Applications that are learnt can later be individually 'unlearnt' (i.e. forgotten) if you no longer want to allow users to gain automatic approval.

> Unlike Pre-Approval, application approvals that are Machine Learnt are still subject to OPSWAT blocking and App-Control blocking rules.

Fully integrated OPSWAT MetaDefender

This innovative feature adds a pre-elevation file reputation check to application approval requests. When switched on, the checksum of the requested application is checked against a substantial database of checksums from over 20 world leading Antivirus vendors, inline, in real time.

The check does not cover every elevation. In particular, applications that a user runs during an *Admin Session* are not checked.

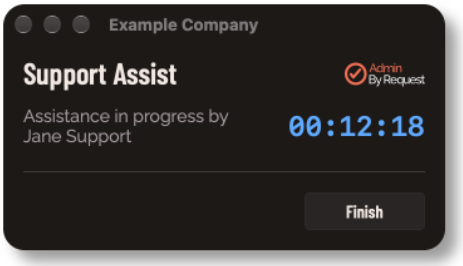
If checksum scores come back as suspicious or malicious, the elevation request is either flat denied or placed into quarantine for review by your security team.

> The OPSWAT MetaDefender feature is fully integrated inside the Admin By Request agent and does not interfere in any way with your existing endpoint security products.

Support Assist

The *Support Assist* feature enables a user with higher Admin By Request rights and feature access to perform a time-limited 'in profile' upgrade of Admin By Request rights.

If, for example, a user does not have permission to install a particular app with Admin By Request, a colleague who does have that permission can use Support Assist to help with the installation. All activity from both parties is logged.



Another scenario is the user has not been granted the right to start a full Admin Session without requesting manual approval.

Using Admin By Request's *Support Assist* feature, the IT Helpdesk user can temporarily switch the logged-in user's Admin By Request rights for their own, therefore allowing the Helpdesk user to elevate system files, and launch sessions without needing to wait for approval.

Support Assist sessions are 'joint logged' in the portal, so the details of both the user (owner) of the system and details of the executing user (Helpdesk staff) who started the Support Assist session are shown together in the audit log.

For Support Assist to work fully, Helpdesk staff should not be granted permanent admin rights (e.g. membership of Domain Admins), Support Assist mode is designed to be used by non-privileged users. This enables System Administrators to not only revoke admin rights from users, but also Helpdesk staff too.

Break Glass (enhanced LAPS)

Built in to Admin By Request is an easy to use, single click feature that delivers a one time, time-limited full local admin user to any endpoint. Being a local admin user, *Break Glass* accounts are not dependent on a working AD or Entra ID registration.

The generation of Break Glass accounts is logged in the portal; in addition, all processes elevated under a Break Glass account are audit logged.

A good use case scenario for the Break Glass feature is if a user has become disjoined / deregistered from a directory and there is no permanent admin-enabled account currently on the endpoint.

Pre-Revocation Logging

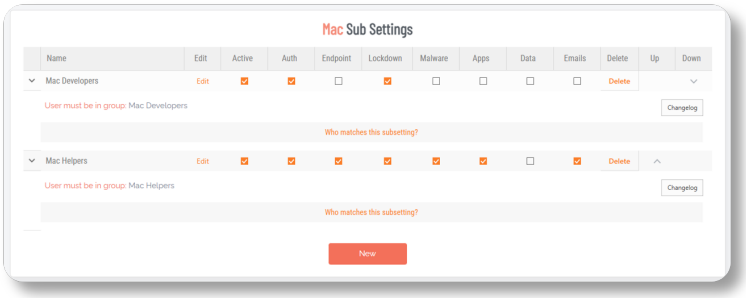
Deploying Admin By Request to users that are permanent administrators, without enabling the revoke feature, enables elevation activity to be logged without changing the elevation user experience. In this case, the user will not notice any change from using their computer as an administrator and will see no Admin By Request prompts.

Using *Pre-Revocation Logging* is an ideal technique for an initial roll-out/discovery phase in environments where it is not known what users are doing with their existing admin rights, or where strong resistance is likely.

Once application elevation activity is "logged", applications can easily be pre-approved, imported into the Machine Learning database or blocked. A report of all elevation activity is also easily exportable for auditing purposes.

Asset Segmentation

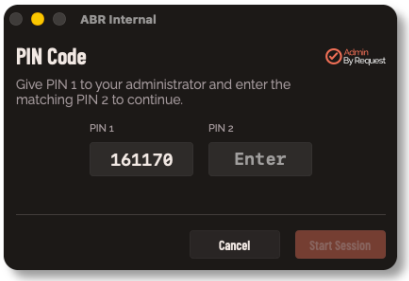
Within the portal you can achieve *Asset Segmentation* and *Workflow Delegation* by grouping and filtering assets per department to delegate request processing.



Admin By Request endpoints that require different settings (i.e. different from the global default settings) can be grouped into an unlimited number of 'Sub Settings' configured in the portal.

For example, different departments could be set with different elevation request email recipients. The portal can be configured with multiple / unlimited admin accounts - the contents of which can be filtered to restrict a portal user so that they can view only the assets relevant to them.

Offline Computers



Admin By Request keeps working on *Offline Computers*. Portal settings are cached locally on the client, offline Admin Sessions are supported, and offline elevation logs are synced with the portal when the client is next online.

Services that need a connection are unavailable while the computer is offline: MFA, OPSWAT checks and portal approval.

If a user requires manual approval while their computer is offline, they can obtain a temporary one-time PIN code by contacting an IT administrator / help desk with portal access, which is where the codes are generated. On a Mac, entering the PIN code starts an *Admin Session*; it does not approve an individual application.

Each PIN code is unique and is valid for one offline request only. Further, a PIN code API enables custom PIN code requests and issuing via REST.

When the user comes back online, the audit logs for offline elevation activity are synced back to the management portal, ensuring there are no gaps in auditing to maintain full compliance.

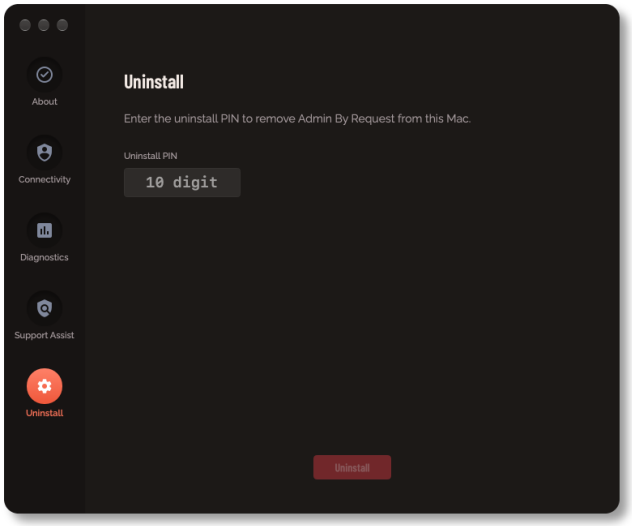
PIN Code Uninstall

Admin By Request cannot simply be uninstalled by using the admin rights that the product itself grants.

In such a situation that a user needs to remove Admin By Request, the *PIN Code Uninstall* feature ensures that this can be done quickly, and with an audited log of exactly when the product was uninstalled and who issued the uninstall code.

Uninstalling removes the client but does not restore administrator rights that Admin By Request revoked earlier; those rights stay revoked.

There are also ways to uninstall devices via scripts and MDM tools such as Intune.



Integration with Common Enterprise Apps

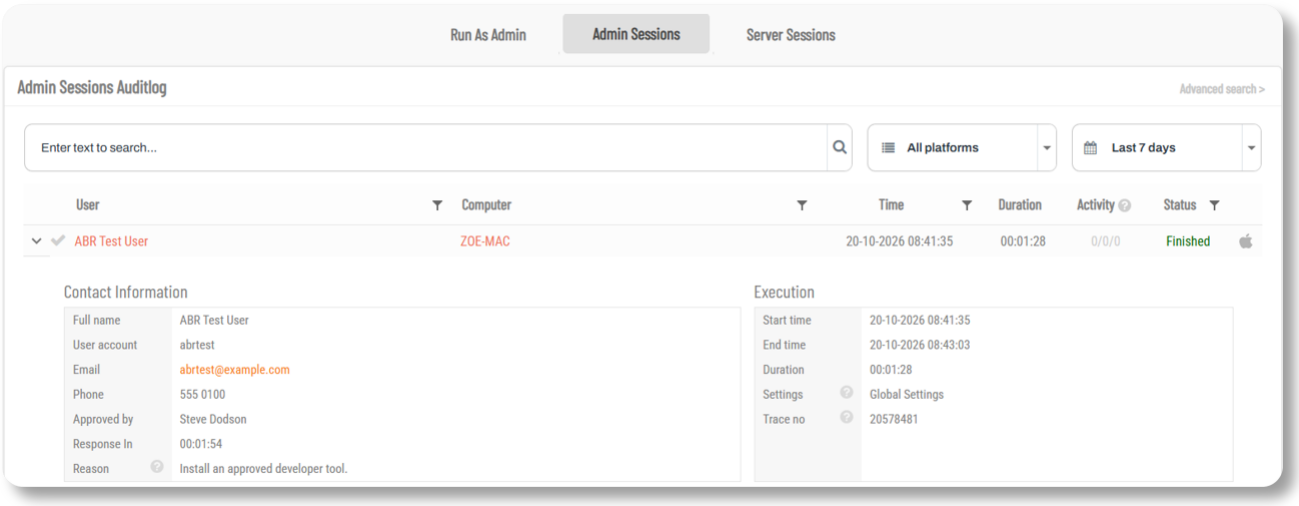
Admin By Request integrates with an ever-growing list of software, including ServiceNow, Teams, Slack and Jira; SIEM tools such as Sentinel and Splunk; identity providers Google Identity, JumpCloud and Okta; and existing infrastructure tools like Active Directory, Entra ID, Intune and Jamf.

These integrations allow you to leverage existing user attributes, enforce access policies, and automate provisioning through SCIM. Further, by connecting Admin By Request to your identity provider, you can streamline approvals, align with security policies, and simplify user lifecycle management across your environment.

Audit & Asset Tracking

An *Audit & Asset Tracking* feature is included as standard. This is a powerful tracking, auditing and inventory solution and requires no additional configuration to setup.

The inventory system provides a filterable view of all Admin By Request enabled computers, providing centralised reporting of all installed software, hardware, AD/Entra ID User and Computer group membership and Local Administrator group memberships. Inventory data can be output via easy access buttons for PDF, XLS, CSV format, it can also be exported via the API system.

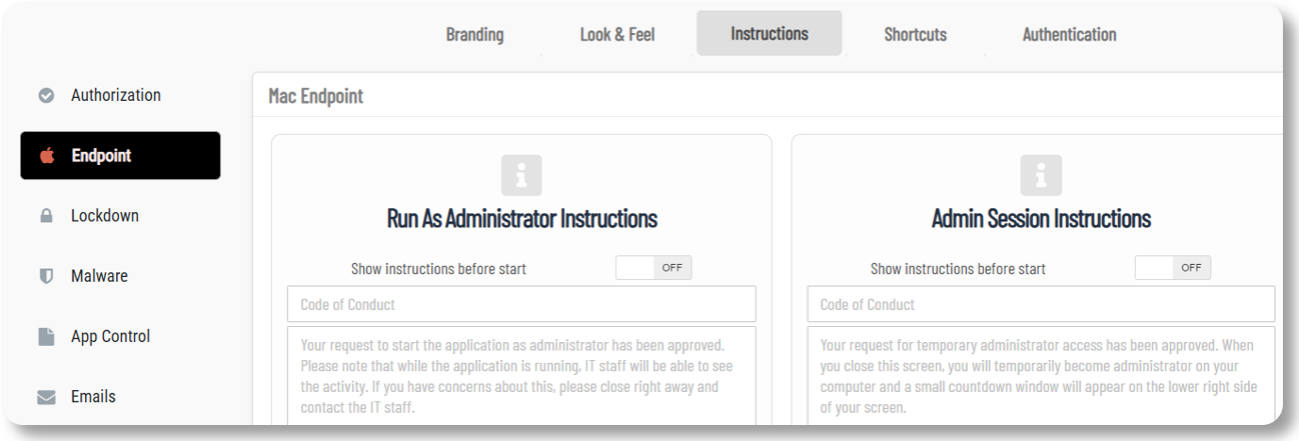


Anti-Tampering

Admin By Request comes with advanced *Anti-Tampering* functionality to prevent abuse and misuse of the product. Once installed, Admin By Request is the only means by which a user can gain privileged elevation. Further, it is not possible for the user to uninstall the client simply by using Admin By Request to gain full admin rights.

The *Device Owner* feature, when configured to lock, restricts the use of Admin By Request specifically to the designated 'owner' of that endpoint. Similar to the Device Owner feature, *Intune Compliance* locking prevents the user of Admin By Request if that endpoint falls outside of compliance, depending on how Intune Compliance has been configured and/or what constitutes compliance for that endpoint.

As a supplement to anti-tampering, we also enable the presentation of a customizable *Code of Conduct* message that informs users of company policy and that their actions are being audited.



Benefits of using Admin By Request

Implementation & Deployment

Feature	Benefit
Highly scalable	Active deployments of 80K+ endpoints
Endpoint Branding	Set company / departmental branding on endpoint GUI prompts
Zero Config single pkg	Agent automatically configures on install for 'hands free' deployment
SaaS based management	Infrastructure transparent / centrally managed & rapid implementation
Intuitive, easy to use management interface	Register, deploy & use in under 5 minutes
Standalone/Workgroup, AD, Entra ID in one tenant	Diverse deployment options for all situations
No network appliance needed	Lower management overhead /no additional equipment to H/A
No software required on AD servers	No need to touch your AD server infrastructure
No requirement to expose or manage passwords	Ideal for high security requirements
Agent 'Learning Mode'	Stealth discovery & reporting on app elevation before revoking rights
World class support included with all paid plans	No additional costs for support
Trust Centre document repository in ABR portal	Everything the DPO, CISO or external auditor needs in one place

Revocation & Privilege Elevation

Feature	Benefit
Global / Sub setting architecture	Apply global defaults and unlimited override setting groups
Rights revoke and account exclusion system	Revoke users from Local Admin group, except for specified exclusions
Pre-approval without confirmation	Skip the confirmation prompt for supported, pre-approved actions
MFA Elevation Mode	Require Entra ID / Microsoft 365 / SAML MFA for elevation
Real time elevation audit status (portal/mobile app)	Keep on top of all live elevation use
Per Process Elevation Mode	Elevation / approval on a per application basis
Admin Session Elevation Modes	Time-limited window-based elevation for system-wide elevation
Rights revoked on Admin Session End	Temporary admin rights removed; policy can also close sudo processes and System Settings
Elevation session promotion (Support Assist)	Upgrade in profile elevation mode for helpdesk staff
Extend Active Session Timer	Extend a running Admin Session without a new request
Remote termination (Remote Kill)	End elevated access at once, with an optional blackout period
Managed sudo pre-approval	Run named commands with sudo, with no Admin Session or admin rights
System Settings pre-approval	Let standard users change chosen System Settings without admin rights
PIN code for offline use	Starts an Admin Session for offline users

Enhanced Security

Feature	Benefit
Real Time OPSWAT on elevation malware check	20+ A/V providers check applications in approval requests
Automatic detection of Proxy & VPN solutions	Solutions such as Z-Scaler & Pulse Secure automatically supported
Customisable User Instruction screens	Present custom 'Code Of Conduct' messages to users pre-elevation
App Blacklisting (vendor cert/checksum)	Deny specific applications / vendors from elevation
Multiple anti-tamper features	Deny agent removal, process monitoring, service tampering
sudo command block rules	Withhold sensitive commands, even during an Admin Session
Portal Settings Activity Log	Track all portal setting changes; who, when, previous & new setting

Management & Administration

Feature	Benefit
Update Endpoint Agent via Internet Update	Single button internet auto-update of endpoint agents
Jamf, Intune & other MDM deployable	Easily deploy and update with existing software management solution
Mobile App (Android & Apple)	Process approvals & review logs away from your PC
Portal Settings Audit Change Log	Full log of all changes (old & new setting, when changed, by who)
Scheduled Email Reports	Automated scheduled email delivery of various pre-made portal reports
Full Inventory (SW, AD/Entra ID Grps, Local Admins)	Enhanced visibility of system status
Configurable data retention on portal	Minimum 3 months, maximum 5 years
Unlimited Portal Users	No limit on number of portal admins
Role-based portal user configuration	Assign portal users conditional access to portal specific to their role
Filter portal data by portal user (portal user scopes)	Restrict portal users to specific user / group data
Unlimited Sub Settings (specific settings for groups)	No limit on number of settings groups

Integration with Other Systems

Feature	Benefit
REST API for external integrations	APIs exist for Audit Log, Requests & Inventory output operations
MS Teams, Slack, ServiceNow and Jira	Receive and manage approval notifications & updates
SCIM integration with Okta and Entra ID	Populate and sync portal users from Entra ID or Okta
Entra ID SSO / Microsoft 365 / SAML for Portal Login	Seamless corporate SSO login to admin portal
Platform SSO for MFA Email match	Email match MFA without an Entra ID Connector
Ticketing system integration	Integrate requests, approvals & status into existing ticketing systems