

Introducing Admin By Request

The powerful, highly compact EPM solution for Windows Workstation and Servers. Built on FastTrack Software's extensive experience writing highly robust, portable & powerful network applications, Admin By Request is simple to deploy, easy to use and is affordable to organisations of all sizes.

Admin By Request 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 with full audit trail.

With Admin By Request, office based or 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, maximising productivity whilst still maintaining full security framework compliance.



What is Admin By Request?

Admin By Request EPM consists of 2 parts:

On premises endpoint agent (Windows, Mac and Linux). This initiates elevation requests and performs elevation workloads. If 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.

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.

Admin By Request 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

INTEGRATION FEATURES	SKU	MAX. ENDPOINTS	LICENSE MODEL	SUPPORTED O/S	SUPPORT
Free Plan (Workstation Only)	N/A	25	Free	Windows 7 or newer. Mac O/S 10.8 or newer. Ubuntu 20.04 LTS / 22.04 LTS and Red Hat Enterprise 9 (RHEL9)	None
Admin By Request Workstation	ABR-WKS	Unlimited	Annual subscription	Windows 7 or newer. Mac O/S 10.8 or newer. Ubuntu 20.04 LTS / 22.04 LTS and Red Hat Enterprise 9 (RHEL9)	Included
Admin By Request Server	ABR-SRV	Unlimited	Annual subscription	Windows Server 2008R2 or newer	Included

KEY FEATURES

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
- Selectable driverless or driver assisted elevated modes
- O365/SAML MFA elevation options
- Allow or block Local Admin rights for device owner, Intune compliance status, specific applications (file location, vendor certificate or file checksum)
- 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.

Audit & Reporting

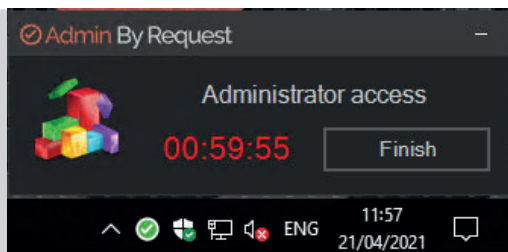
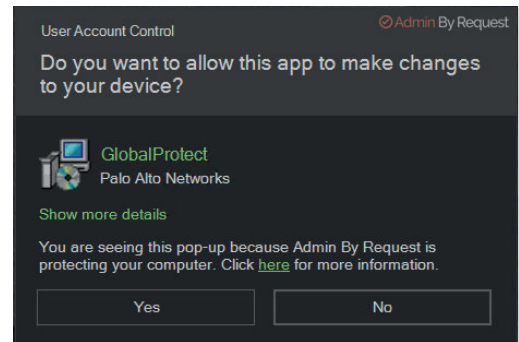
- Powerful inventory solution included as standard
- Full audit trail of user elevation activity, admin logons & software installs
- Schedulable reporting of key user activity
- API access to audit logs, request logs, PIN codes, security events and inventory for SIEM and external reporting
- Full settings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

Convenience

- Simultaneous support for no-AD, multi-domain Active Directory and Azure Active Directory endpoints
- No need to deploy server appliances or install software on existing server infrastructure. Endpoint only solution
- ZeroConfig, sub 2MB endpoint installer silently installs using standard deployment tools (SCCM/Intune)
- Action privilege elevation requests from your smart phone using our free mobile app.
- Solution works both online or offline (approval with PIN code)

'Run as admin' per app sandboxed 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. Because Run As Admin mode is invoked by right clicking on an application and selecting 'Run As Admin', this mimics standard Windows behaviour, and as such requires no additional user training.



Admin session time limited Privilege elevation

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

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 that 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.

'Fully integrated OPSWAT MetaDefender

This innovative feature enables a pre-elevation check for 'Run As Admin' and 'Admin Session' elevation modes. When switched on, this file reputation feature ensures that all user elevation operations, whether with or without approval are checked against a substantial database of checksums from over 20 world leading Antivirus vendors, inline, in real time.

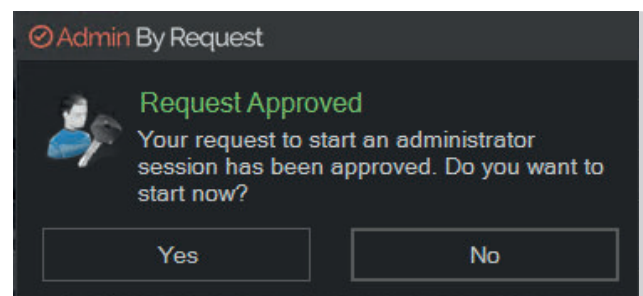
If checksum scores come back as suspicious or malicious the elevation request is either flat denied or placed into quarantine for review by your security team.

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.

Approving access

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 selecting either Approve or Deny button, the requesting user will receive the outcome of the request via email and/or desktop notification.

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



Automated approval for specific applications (pre-approval)

For situations where you would like to require approval for unknown applications but allow automatic elevation for specifically approved apps, the 'pre-approval' feature allows this.

With application pre-approval, a portal administrator can set policies either tenant wide or per sub-setting (group of users) based on several rule types such as files location (network share), the vendor certificate on the application or specific checksum.

Applications rules can also be configured to require user confirmation so to require a user to click a 'yes/no' box at elevation, or without user confirmation which allows 'unattended' user elevation. Unattended elevation mode can be useful in situations where applications need elevation when you do not want user input, such as system start up or user context scripting.

Elevations for pre-approved applications are not sent through the optional OPSWAT Meta Defender malware reputation checking system.

Machine learnt pre-approval for specific applications

When both Approval and Machine Learning are both enabled, the portal administrator can define a threshold over which manually approved applications are auto learnt in. For example setting the Machine Learning threshold to 'three' would result in an application being needed to be approved three separate times, after which the fourth elevation would not require to be manually 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 which are learnt in can later be individually 'forgotten' if you no longer want to allow users to gain automatic approval.

Note: Unlike Pre-Approval applications that are Machine Learnt in are still subject to OPSWAT blocking and App-Control blocking rules.

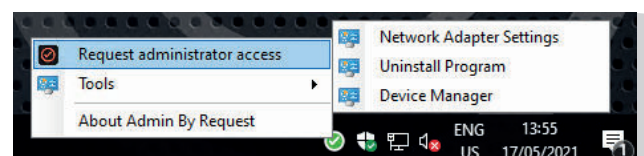
AI learnt pre-approval for applications that exceed app or vendor scores

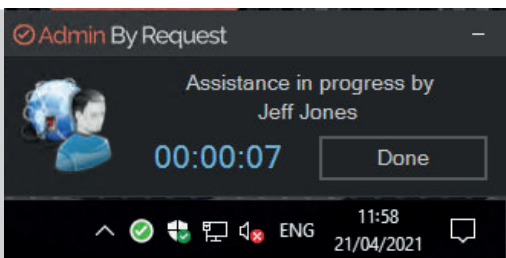
All applications elevated with Admin By Request are assigned both an Application Popularity Score for the specific application and a Vendor Popularity Score for the vendor of the application. AI Approval enables the portal administrator to set, per sub setting thresholds over which applications can be auto elevated depending on either their specific application score or vendor score. Enabling both App and Vendor thresholds will match the lowest of the two.

Like Machine Learning rules, AI Approvals are still subject to OPSWAT Blocking and App-control blocking rules.

Tray Tools

Components of the Windows 10 control panel such as Device Manager, Network Configuration and Add Printer Wizard can be run elevated using our Tray Tools feature. With Tray Tools, users can perform common system configuration tasks such as changing IP address, without the need to provide elevated rights to the entire system.





Support Assistance (Workstation edition only)

The Support Assistance 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 was not given permission to elevate Windows system files with Admin By Request, or they have not been granted the right to start a full Admin Session without requesting manual approval, an IT helpdesk user might find the users configuration too restrictive to work on to resolve system issues.

Using Admin By Requests Support Assistance feature, the IT Helpdesk user can temporarily switch the logged in users Admin By Request rights for their own, therefore allowing the helpdesk user to elevate system files, and launch sessions without requiring to wait for approval.

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

For Support Assistance to work fully, Helpdesk staff should not be granted permanent admin rights (eg membership of domain admins). Support Assistance mode is designed to be used by non-privileged users. This enables you 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 which delivers a one time, time limited full local admin user to any endpoint. Being a local admin user, Break Glass accounts are not dependant on a working AD or Entra ID registration. Generation of Break Glass accounts are logged in the portal, in addition all processes elevated under a Break Glass account are audit logged also.

A good use case scenario for use of the Break Glass feature is if a user has somehow become un-joined / deregistered from a directory with no longer permanent admin / enabled built in account on the endpoint.

Pre-Revocation logging

Deploying Admin By Request to users that are permanent administrators, without enabling the revoke feature will enable elevation activity to be logged, without changing the elevation user experience, 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 initial roll out/discovery phase in environments where it is not known what users are doing with their existing admin rights. 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 and workflow delegation

Within the portal you can group and filter assets per department to delegate request processing.

Admin By Request endpoints that require different settings (from 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 and the contents of which can be filtered to restrict a portal user so that they can only view the assets relevant to them.

Offline computers

Admin By Request works the same whether the computer is online or offline. Portal settings are cached on the client, when offline elevation logs are stored locally on the client and synced with the portal when the client is next online.

If a user requires manual approval and their computer is offline, then they can obtain a temporary one time action specific PIN code by contacting an IT administrator/ help desk with portal access where the codes are generated. Each PIN code is unique and is valid for one offline request only. A PIN code API can be utilised to enable custom PIN code request and issuing via REST.

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

Audit & asset tracking

A powerful tracking, auditing and inventory solution is included as standard 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/AAD 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.

Preventing abuse

Admin By Request comes with a number of 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.

As a supplement to anti tampering, we also enable the presentation of a customisable code of conduct message which can inform users of company policy and that their actions are being audited.

It is not possible for the user to uninstall Admin By Request, simply by using Admin By Request to gain full admin rights.

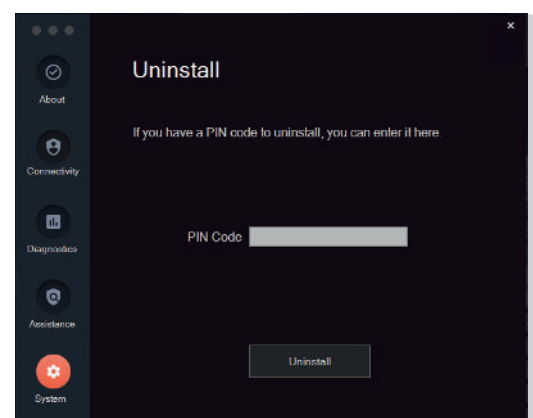
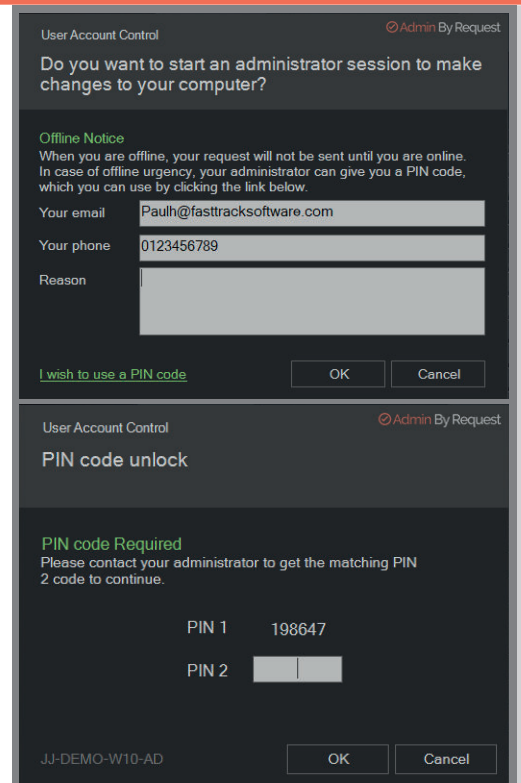
The Device Owner feature, when configured to lock, restricts the use of Admin By Request specifically to the designated 'owner' of that endpoint.

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 / what constitutes compliance for that endpoint.

PIN code uninstall

Admin By Request cannot simply be uninstalled by using the admin rights that 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 who issued the uninstall code, and when the product was uninstalled.

For Local and Azure AD users, if Admin By Request was responsible for revoking Local Admin rights for the user, these rights are automatically returned on uninstallation of the product.



IMPLEMENTATION & DEPLOYMENT

IMPLEMENTATION & DEPLOYMENT FEATURES	FEATURE DESCRIPTION
Thin Agent (under 2MB in total size)	Quick and easy to deploy, ultra-low resource footprint
Multilingual Endpoint UI support	Auto language detection for English, French, German, Spanish, Norwegian, Swedish and Danish
Highly scalable	Active deployments of 80K+ endpoints
Endpoint Branding	Set company / departmental branding on endpoint GUI prompts
Zero Config single MSI	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, AZURE AD support in same 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 application elevation usage before revoking rights
World class support included with all paid plans	No additional costs for support
Trust Centre documentation repository in ABR portal	Everything the DPO, CISO or external auditor needs for compliance documentation in one place

REVOCACTION & PRIVILEGE ELEVATION

REVOCACTION AND PRIVILEGE ELEVATION FEATURES	FEATURE DESCRIPTION
Global / Sub setting architecture	Apply global defaults and unlimited override setting groups
Rights revoke and account exclusion system	Revoke users from Local Admin group / set specific exclusions not to revoke
Driver assisted elevation mode	Simple Yes/No confirmation on app elevation
Native UAC elevation mode	Driver-less Windows UAC elevation with re-authentication on app elevation
Windows Hello support for Native UAC elevation	Authenticate elevation with Windows Hello
Non-interactive (prompt less) elevation mode	Elevate applications without user interaction (start-up/login etc)
MFA Elevation Mode	Require Entra ID / Office 365 / SAML MFA for elevation
Real time Elevation audit status in portal / mobile app	Keep on top of all live elevation use
Per Process Elevation Mode	Sandboxed per process elevation / approval on per application basis
Admin Session Elevation Modes	Time limited window-based elevation for system wide elevation
Force Close on Admin Session End	Create a 'hard stop' to end of Admin Session mode - applications forced closed on session expiry
Elevation session promotion (Support Assist)	Upgrade in profile elevation mode for helpdesk staff
PIN code for offline use	Allows manual approval for offline users

ENHANCED SECURITY

ENHANCED SECURITY FEATURES	FEATURE DESCRIPTION
Real Time OPSWAT on elevation malware check	Pre-Elevation check over 20 A/V providers that ensures only reputable files are elevated
Automatic detection of Proxy & VPN solutions	Solutions such as Z-Scaler & Pulse Secure automatically detected supported
Customisable User Instruction screens	Present custom 'Code Of Conduct' messages to users pre-elevation
Application Blacklisting (location/vendor cert/checksum)	Deny specific applications / vendors from elevation
PIN code for Blacklist override	Manual approval for application blacklist override
UAC Secure Desktop mode	Native UAC mode option to use Secure Desktop mode (obscure screen on UAC prompt)
Multiple anti-tamper features	Deny agent removal, process monitoring, service tampering
Portal Settings Activity Log	Tracks all portal setting changes, by who, when, previous setting, new setting

MANAGEMENT

MANAGEMENT FEATURES	FEATURE DESCRIPTION
Update Endpoint Agent via LAN Update	Automatically update endpoint agent via network share
Update Endpoint Agent via Internet Update	Single button internet auto-update of endpoint agents
Intune & SCCM 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 settings changes in portal (old setting, new setting, when changed by who.)
Scheduled Email Reports	Automated scheduled email delivery of various pre-made portal reports
System Inventory (Installed Software / AD/ AAD Groups / 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 admin
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

INTEGRATIONS

INTEGRATION FEATURES	FEATURE DESCRIPTION
REST API for external integrations	APIs for Audit Log, Request System & Inventory can be read for external log storage and reporting
MS Teams, Slack, ServiceNow and Jira	Receive approval notifications and manage via integrations
SCIM integration with OKTA and Azure AD	Populate and sync portal users from AAD or OKTA
AAD SSO / O365 / SAML for Portal Login	Seamless corporate SSO login to admin portal
Ticketing system integration	Integrate approval request notifications & status into existing ticketing system