Spec Sheet

Admin By Request
ZERO TRUST PLATFORM

Endpoint Privilege Management

Product Platform: **Windows**
Product Version: **8.5**
Document Date: **20 January 2025**

Introducing Admin By Request

The powerful, highly compact EPM solution for Windows Workstations and Servers. Built on the company's extensive experience writing highly robust, portable & powerful network applications, Admin By Request is simple to deploy, easy to use and 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 that includes a full audit trail.

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

What is it?

Admin By Request 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 (i.e. it works offline too).
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.

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

Subscription	Max. Endpoints	License Model	OS Version	Support
Free Plan (ABR Workstation)	25	Free	Windows 10 or later (x86/x64 or ARM64)	None
Free Plan (ABR Server)	10	Free	Windows Server 2008R2 or later	None
Paid Plan (ABR Workstation)	Unlimited	Annual Subscription	Windows 10 or later (x86/x64 or ARM64)	Included
Paid Plan (ABR Server)	Unlimited	Annual Subscription	Windows Server 2008R2 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
- 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 (by 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

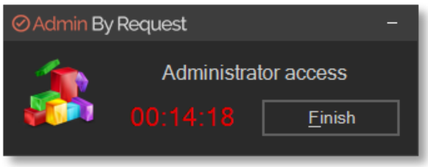
Auditing & Reporting

- 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, sub 2MB endpoint installer silently installs using standard deployment tools (SCCM/Intune/Jamf)
- Approve or deny privilege elevation requests from your smart phone using our free mobile app.
- Solution works whether online or offline (approval with PIN code)

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.

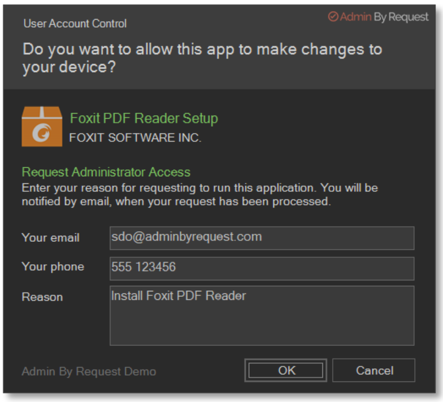
Admin Session mode is ideal for users like developers who need the freedom to run multiple elevated applications within a set amount of time. Once the user either stops the timer or the time runs out, details relating to the session (processes run, software installed / removed) are uploaded to the portal.

Per-app Privilege Elevation (sandboxed)

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.



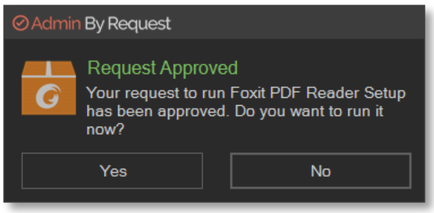
User Account Control

Do you want to allow this app to make changes to your device?

Foxit PDF Reader Setup
FOXIT SOFTWARE INC.

Request Administrator Access
Enter your reason for requesting to run this application. You will be notified by email, when your request has been processed.

Your email: sdo@adminbyrequest.com
Your phone: 555 123456
Reason: Install Foxit PDF Reader



Request Approved
Your request to run Foxit PDF Reader Setup has been approved. Do you want to run it now?

Elevation Approval (per request)

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

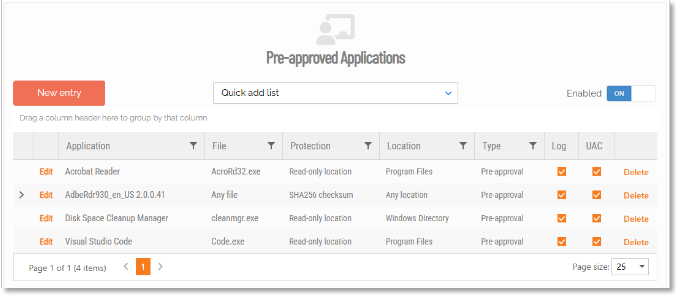
When a request is actioned by selecting either Approve or Deny button, the requesting user will receive the outcome of the request via email and/or desktop notification.

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.

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).



Pre-approved Applications

		Application	File	Protection	Location	Type	Log	UAC	
	Edit	Acrobat Reader	AcroRd32.exe	Read-only location	Program Files	Pre-approval	☑	☑	Delete
›	Edit	AdbeRdr930_en_US 2.0.0.41	Any file	SHA256 checksum	Any location	Pre-approval	☑	☑	Delete
	Edit	Disk Space Cleanup Manager	cleanmgr.exe	Read-only location	Windows Directory	Pre-approval	☑	☑	Delete
	Edit	Visual Studio Code	Code.exe	Read-only location	Program Files	Pre-approval	☑	☑	Delete

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

Policies can be based on several rule types such as file location (network share), the vendor certificate on the application or specific checksum.

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 allows 'unattended' user elevation.

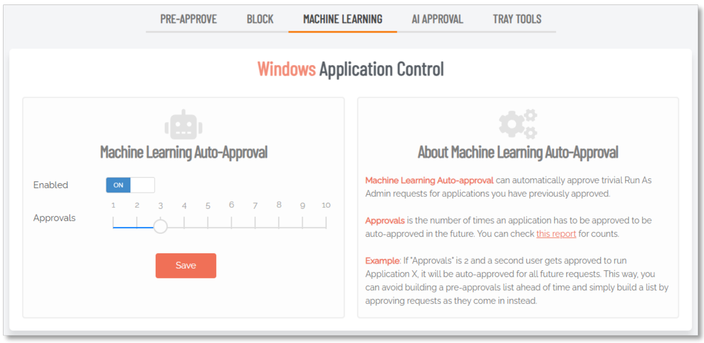
Unattended elevation can be useful in situations where applications need elevation when you do not want user input, such as system start up or user context scripting.

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

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 separate times.


PRE-APPROVE
BLOCK
MACHINE LEARNING
AI APPROVAL
TRAY TOOLS
Windows Application Control
Machine Learning Auto-Approval
Enabled
ON
Approvals
1
2
3
4
5
6
7
8
9
10
Save
About Machine Learning Auto-Approval

Machine Learning Auto-approval can automatically approve trivial Run As Admin requests for applications you have previously approved.

Approvals is the number of times an application has to be approved to be auto-approved in the future. You can check this report for counts.

Example: If "Approvals" is 2 and a second user gets approved to run Application X, it will be auto-approved for all future requests. This way, you can avoid building a pre-approvals list ahead of time and simply build a list by approving requests as they come in instead.

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

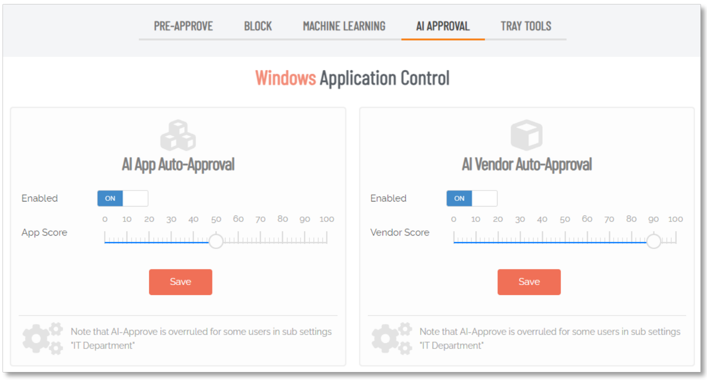
Machine Learning, like *Pre-Approval* is a sub-setting-configured feature, which means that different sub-settings can be configured with different Machine Learning thresholds. Applications that are learnt can later be individually 'unlearnt' (i.e. forgotten) if you no longer want to allow users to gain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

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

Pre-Approval (AI learnt)

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.

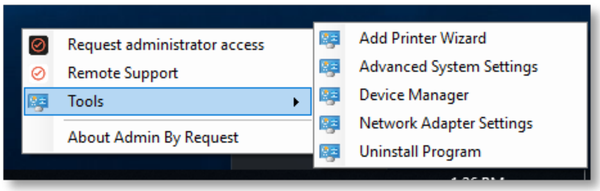
AI Approval enables the portal administrator to set, per sub setting thresholds over which applications can be auto elevated depending on either their specific application score or vendor score.



Note that AI-Approve is overruled for some users in sub settings "IT Department"

Note that AI-Approve is overruled for some users in sub settings "IT Department"

> Enabling both App and Vendor thresholds will match the lowest of the two. Like Machine-learnt approvals, AI-learnt approvals are still subject to OPSWAT Blocking and App-control blocking rules.



Tray Tools

Components of the Windows 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.

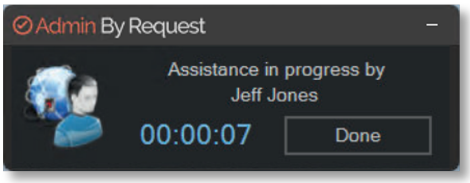
Fully integrated OPSWAT MetaDefender

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.

Support Assist (workstation edition only)



Assistance in progress by Jeff Jones

00:00:07

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 was not given permission to elevate Windows system files with Admin By Request, an IT Helpdesk user might find the user's configuration too restrictive to work on to resolve system issues.

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 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 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.

Generation of Break Glass accounts are 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.

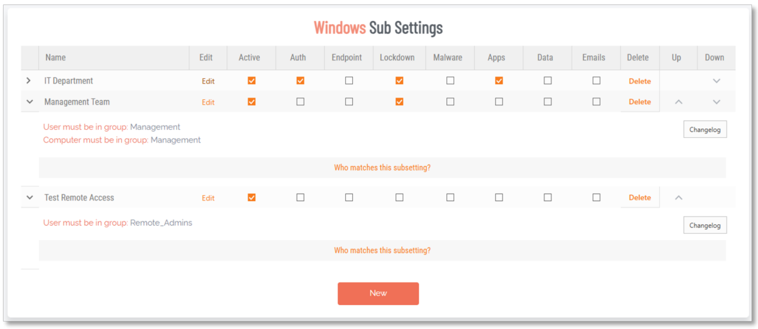
Using *Pre-Revocation Logging* is an ideal technique for an initial roll-out/discovery phase in environments where it is not known what users are doing with their existing admin rights, or where strong resistance is likely.

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.



Windows Sub Settings

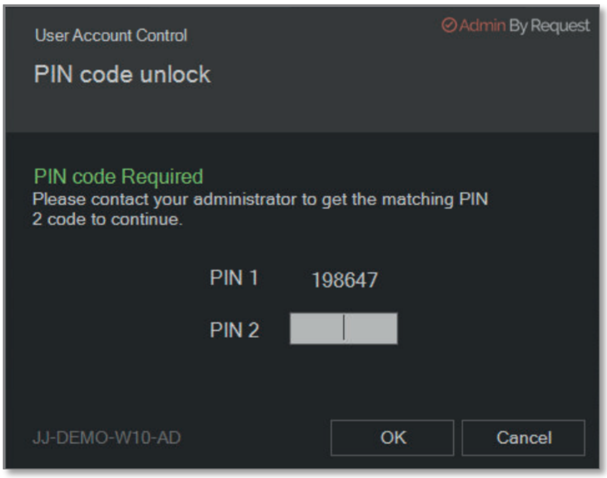
	Name	Edit	Active	Auth	Endpoint	Lockdown	Malware	Apps	Data	Emails	Delete	Up	Down
›	IT Department	Edit	☑	☑	□	☑	□	☑	□	□	Delete		˅
˅	Management Team	Edit	☑	□	□	☑	□	□	□	□	Delete	˄	˅
˅	Test Remote Access	Edit	☑	□	□	□	□	□	□	□	Delete	˄	

Management Team:
User must be in group: Management
Computer must be in group: Management
Changelog
Who matches this subsetting?

Test Remote Access:
User must be in group: Remote_Admins
Changelog
Who matches this subsetting?

New

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.



User Account Control
Admin By Request
PIN code unlock

PIN code Required
Please contact your administrator to get the matching PIN 2 code to continue.

PIN 1 198647
PIN 2

JJ-DEMO-W10-AD
OK Cancel

Offline Computers

Admin By Request handles *Offline Computers* easily, working the same whether the computer is online or offline. Portal settings and offline elevation logs are cached locally on the client and synced with the portal when the client is next online.

If a user requires manual approval while their computer is offline, they can obtain a temporary one-time action-specific PIN code by contacting an IT administrator / help desk with portal access, which is where the codes are generated.

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.

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/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.

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.

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

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.

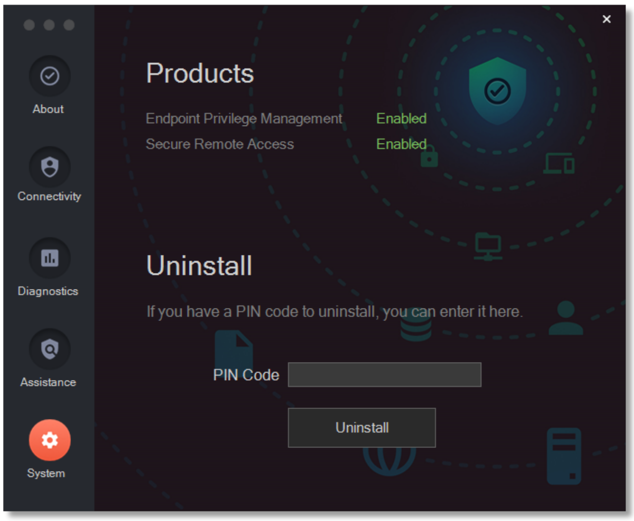
PIN Code Uninstall

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

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 during uninstallation of the product.

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



Products

Endpoint Privilege Management: Enabled
Secure Remote Access: Enabled

Uninstall

If you have a PIN code to uninstall, you can enter it here.

PIN Code:

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.

Benefits of using Admin By Request

Implementation & Deployment

Feature	Benefit
Thin Agent (under 2MB in total size)	Quick and easy to deploy, ultra-low resource footprint
Multilingual Endpoint UI support	Auto language detection for seven languages
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, 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
Driver assisted elevation mode	Simple Yes/No confirmation on app elevation
Native UAC elevation mode	Driver-less Windows UAC elevation with re-authentication on 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 (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' at end of Admin Session (apps are forced closed)
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

Feature	Benefit
Real Time OPSWAT on elevation malware check	Check by 20+ A/V providers ensures only reputable files are elevated
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 (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	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	Track all portal setting changes; who, when, previous & new setting

Management & Administration

Feature	Benefit
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 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/AAD 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 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 requests, approvals & status into existing ticketing systems