

ABR vs EPM

Comparison and Recommendation



Data-Driven Comparison



Strategic Recommendation



DOCUMENT TYPE

Supporting attachment to the Realization Document



AUTHOR

Muhammad Zubair



COMPANY

Soudal NV — Turnhout, Belgium



ACADEMIC YEAR

2025–2026



DATE

March 2026

Table of Contents

Table of Contents	2
1. Executive Summary	3
2. Feature Comparison Matrix	4
3. Use Case Evaluation for Soudal	5
3.1 Engineering and Factory Floor Elevation	5
3.2 Service Desk Support	5
3.3 Application Installation	5
3.4 Permission Revocation	6
3.5 Compliance and Audit	6
3.6 Use Case Summary	6
4. Detailed Findings	7
4.1 ABR Strengths	7
4.2 ABR Limitations	7
4.3 EPM Strengths	7
4.4 EPM Limitations	8
5. Recommendation	9
5.1 Decisive Factor 1 Offline Capability	9
5.2 Decisive Factor 2 Operational Flexibility	9
5.3 Decisive Factor 3 Local Administrator Inventory	9
5.4 Consideration for a Hybrid Approach	9
6. Next Steps	10

1. Executive Summary

This document provides a structured comparison between Admin By Request (ABR) and Microsoft Endpoint Privilege Management (EPM) as candidate solutions for replacing permanent local administrator rights at Soudal NV. The comparison draws on the results of hands-on laboratory testing documented in the realization report (Chapters 3 and 4) and evaluates both tools against Soudal's operational requirements, technical environment, and compliance obligations.

The evaluation was conducted using a weighted scoring approach across eight categories: product type, operating system support, elevation types, offline capability, audit logging, approval workflows, Intune integration, and local administrator inventory. Each category was assessed against the five use cases identified during the analysis phase: engineering and factory floor elevation, Service Desk support, application installation, permission revocation, and compliance audit.

The recommendation is that Admin By Request should be adopted as the primary privilege elevation solution at Soudal. The three decisive factors supporting this recommendation are offline capability for factory and engineering environments, operational flexibility across all five use cases, and built-in local administrator inventory for the permission revocation phase.

2. Feature Comparison Matrix

The following table presents a side-by-side comparison of ABR and EPM across the dimensions most relevant to Soudal's requirements. The Advantage column indicates which tool performed better for each category based on the laboratory testing results.

Category	Admin By Request	Microsoft EPM	Advantage
Product type	Dedicated cloud PAM platform with its own management portal	Native Microsoft Intune add-on with no separate portal	Context-dependent
OS support	Windows, macOS, Linux	Windows only	ABR
Elevation types	Run As Admin, Admin Session, Break Glass, Offline PIN, Pre-approved rules	Virtual elevation via policy rules (automatic or user-confirmed)	ABR
Offline capability	Full offline support via Offline PIN with audit sync on reconnection	Limited; requires connectivity for policy evaluation in most scenarios	ABR
Audit logging	Comprehensive cloud logs with SIEM export capability	Integrated with Intune and Defender device telemetry	Tie
Approval workflow	Full real-time approval workflow with admin notification and offline fallback	No real-time approval; rules are pre-defined as automatic or user-confirmed	ABR
Intune integration	Deployed through Intune; managed via separate ABR portal	Fully native; all configuration within Intune admin center	EPM
Local admin inventory	Real-time inventory with remote revocation capability	Not provided as a standalone feature	ABR
Ideal use cases	Factory, engineering, mixed-connectivity, multi-platform environments	Corporate office, cloud-only, permanently connected Windows devices	Context-dependent
Licensing	Separate per-user pricing through ABR	Included in Intune Suite or Microsoft 365 E5 add-on	Context-dependent

Table 1: Feature comparison matrix — Admin By Request vs Microsoft Endpoint Privilege Management

3. Use Case Evaluation for Soudal

This section evaluates each tool against the five operational use cases identified during the analysis phase of the project. The use cases represent the real-world scenarios that any privilege elevation solution must support within Soudal's environment.

3.1 Engineering and Factory Floor Elevation

This is the most decisive use case in the comparison. Engineering staff at Soudal operate in factory environments where network connectivity to the corporate infrastructure is not guaranteed.

Privilege elevation must function reliably in disconnected or intermittently connected conditions.

ABR's Offline PIN mechanism was tested and confirmed working during ABR Test 4 (Chapter 3 of the realization report). A user was able to request and receive a time-limited PIN through an out-of-band channel, enter it on the disconnected device, and elevate privileges without any network dependency. The elevation event was logged locally and synchronized to the ABR cloud portal on reconnection. EPM's offline behavior was tested in EPM Test 15 (Chapter 4). EPM requires connectivity for policy evaluation in most operational scenarios, which limits its effectiveness in factory and engineering contexts.

Result: ABR is the only viable option for this use case.

3.2 Service Desk Support

Service Desk staff perform a wide variety of administrative tasks across multiple tools during a support session. The elevation model must accommodate frequent, varied administrative actions within a defined time window.

ABR's Admin Session model is well suited to this workflow. It grants temporary full administrator access for a defined period, matching the reality of a support session where many tools and actions are needed. EPM's rule-based model requires a separate elevation rule for each approved application, which creates administrative overhead and may not scale cleanly to the variety of tools Service Desk staff use.

Result: ABR is better suited; EPM is functional but less flexible.

3.3 Application Installation

Standard users occasionally need to install approved applications that require administrator privileges during the installation process.

Both tools handle this use case effectively. EPM's rule-based approach is precise: elevation is granted for a specific installer binary, and nothing else. ABR's pre-approved rules deliver equivalent functionality with comparable granularity. Both tools were tested successfully for this scenario during laboratory testing.

Result: Tie. Both tools perform equally well.

3.4 Permission Revocation

The deployment plan for this project includes a phase where existing permanent local administrator rights are identified and removed across the device fleet. The selected tool must support visibility into current privilege state and the ability to revoke rights remotely.

ABR provides a built-in local administrator inventory and remote revocation feature, tested and confirmed during ABR Test 6 (Chapter 3). This capability is essential for the permission revocation phase. EPM does not provide local administrator inventory or remote revocation as a standalone feature, which means additional tooling or manual processes would be required.

Result: ABR has a clear advantage.

3.5 Compliance and Audit

Both tools must generate sufficient audit data to satisfy Soudal's compliance obligations under ISO 27001 and GDPR. Elevation events must be logged with timestamp, user identity, device identity, action requested, and outcome.

Both tools provide comprehensive audit logging. ABR's cloud portal offers detailed filtering and export capabilities for audit review. EPM's integration into Intune means that elevation data is co-located with device compliance and configuration data, which some compliance teams may find more convenient for centralized reporting.

Result: Tie. Both tools meet compliance requirements.

3.6 Use Case Summary

Use Case	ABR	EPM	Winner
Engineering / Factory floor	Full offline support via PIN	Limited offline capability	ABR
Service Desk support	Flexible Admin Session model	Rule-per-app, less flexible	ABR
Application installation	Pre-approved rules	Per-binary elevation rules	Tie
Permission revocation	Built-in inventory + remote revoke	Not available as standalone	ABR
Compliance and audit	Rich cloud logs, SIEM export	Integrated Intune/Defender logs	Tie

Table 2: Use case evaluation summary — ABR vs EPM at Soudal

4. Detailed Findings

4.1 ABR Strengths

- Offline PIN elevation provides reliable privilege escalation without network connectivity, which is essential for Soudal's factory and engineering environments.
- The Admin Session model supports Service Desk workflows where multiple administrative actions are required within a single support interaction.
- The local administrator inventory and remote revocation features directly support the permission revocation phase of the deployment plan.
- Multi-platform support (Windows, macOS, Linux) provides flexibility for potential future expansion beyond the current Windows-focused scope.
- The real-time approval workflow with admin notification provides an additional layer of control for high-risk elevation requests.
- SIEM export capability supports integration with centralized security monitoring.

4.2 ABR Limitations

- ABR operates through a separate cloud portal, introducing a second management surface alongside the Intune admin center.
- The ABR agent is deployed as an independent application through Intune, requiring its own update and maintenance cycle.
- Separate licensing introduces an additional cost line that must be managed alongside existing Microsoft licensing.

4.3 EPM Strengths

- Native integration with Microsoft Intune eliminates the need for a second management portal or vendor relationship.
- All configuration, policy assignment, and reporting exist within the Intune admin center, reducing operational complexity for the IT team.
- Virtual elevation accounts at the kernel level provide precise, per-application privilege escalation without adding the user to the local Administrators group.
- Licensing is bundled with the Intune Suite or Microsoft 365 E5, which Soudal may already hold or plan to adopt.

4.4 EPM Limitations

- Windows-only support limits applicability if Soudal's device fleet expands to include macOS or Linux endpoints.
- Limited offline capability restricts use in factory and engineering scenarios where network connectivity is intermittent or unavailable.
- The absence of a real-time approval workflow means all elevation decisions must be pre-configured through policy rules.
- No built-in local administrator inventory or remote revocation feature, which complicates the permission revocation phase.
- EPM does not provide Service Desk-friendly session-based elevation; each tool or action requires a separate policy rule.

5. Recommendation

Based on the evaluation documented in this attachment and the laboratory testing results presented in Chapters 3 and 4 of the realization report, Admin By Request is recommended as the primary privilege elevation solution for Soudal NV. The recommendation is supported by three factors that directly reflect Soudal's operational requirements.

5.1 Decisive Factor 1 Offline Capability

The engineering and factory floor use case requires privilege elevation without network connectivity. This requirement is not optional for Soudal. ABR's Offline PIN mechanism was tested and confirmed working in a fully disconnected state, with complete audit synchronization on reconnection. EPM's architecture requires network connectivity for policy evaluation in most scenarios, which means it cannot reliably serve factory and engineering users. This single factor disqualifies EPM as the sole solution for Soudal's environment.

5.2 Decisive Factor 2 Operational Flexibility

Soudal's five use cases span a range of elevation needs: permanent-style elevation for Service Desk, offline PIN for engineering, temporary sessions for power users, app-specific elevation for standard users, and centralized audit for compliance. ABR covers all five from a single platform with a single agent. EPM's rule-based model is well suited to some of these scenarios but requires significantly more administrative overhead to cover the full range, and cannot address the offline requirement at all.

5.3 Decisive Factor 3 Local Administrator Inventory

The phased deployment plan for this project includes a permission revocation phase in which existing permanent local administrator rights are identified and removed across the device fleet. ABR provides a built-in local administrator inventory with remote revocation capability. EPM does not offer this as a standalone feature. Without ABR's inventory and revocation tooling, the permission revocation phase would require additional tools or manual processes, increasing operational risk and complexity.

5.4 Consideration for a Hybrid Approach

EPM remains a technically sound solution for a subset of Soudal's device population. For office-based, permanently connected Windows users who do not require offline elevation, EPM's native Intune integration provides genuine operational advantages: no second portal, no separate agent, no additional vendor relationship. A hybrid approach in which EPM is used for corporate office users and ABR is retained for engineering, factory, and mixed-connectivity scenarios may be worth evaluating in a future project cycle, once the initial ABR deployment is stable and the permission revocation phase is complete.

6. Next Steps

The following actions are recommended based on the findings of this comparison:

- Proceed with the phased deployment of Admin By Request as the primary privilege elevation solution for all in-scope user groups at Soudal, following the deployment strategy documented in Chapter 6 of the realization report.
- Use ABR's local administrator inventory to identify and document existing permanent local administrator accounts across the in-scope device population before removing any rights.
- Configure elevation policies tailored to each user group: Offline PIN for engineering, Admin Session for Service Desk, pre-approved rules for standard application installation, and approval workflows for ad-hoc elevation requests.
- Establish the audit logging and SIEM integration configuration during the pilot phase to validate compliance reporting before broader rollout.
- Monitor EPM's product roadmap for improvements to offline capability and approval workflows. Reassess the hybrid approach after the initial ABR deployment has been validated in production.
- Present this comparison and recommendation to Soudal leadership and the work placement mentors for final sign-off before proceeding with pilot deployment.