THOMAS MORE

Privilege Management Modernization at Soudal

Realization document

Muhammad Zubair
Student Bachelor Applied Computer Science

2025 - 2026

Table of Contents

Preface

This report was produced during a work placement at Soudal NV in the academic year 2025–2026, as part of the Bachelor of Applied Computer Science programme at Thomas More University of Applied Sciences. The project involved the evaluation and initial deployment of a privilege elevation solution to replace permanent local administrator rights across selected user groups within Soudal's endpoint environment.

The work covered hands-on laboratory testing of two platforms, stakeholder presentations to management, the development of a phased deployment strategy, and the creation of supporting scripts and configuration artefacts for the production rollout. The placement provided substantial practical exposure to enterprise identity management, endpoint security, and organizational change management in a live production environment.

Appreciation is extended to Dries Wuyts, Rob Verbiest and Eduard Claessen for their guidance and support throughout the placement, and to Brent Pulmans of Thomas More for academic supervision.

List of Figures

List of Tables

1. Introduction

Privilege management represents one of the most persistent challenges in modern enterprise endpoint security. When elevated access rights are granted without a structured process for revocation, organizations accumulate an expanding attack surface that is difficult to audit, difficult to justify under compliance frameworks, and difficult to recover from when exploited. This report documents the evaluation and implementation work conducted during a work placement at Soudal NV, a global manufacturer of chemical building products headquartered in Turnhout, Belgium.

Soudal operates a cloud-first endpoint environment built on Microsoft Intune, Microsoft Entra ID, Conditional Access policies, and Windows Autopilot. Despite this modern infrastructure, a significant portion of the user base retained permanent local administrator rights, the result of reactive access provisioning with no systematic revocation process in place. The central objective of this project was to replace those permanent rights with controlled, temporary, and fully auditable, granting elevated privileges only when operationally necessary, for only as long as the task requires, with every action leaving a traceable record.

The central research question of this project is: how can permanent local administrator rights at Soudal be replaced with a controlled, temporary, and fully auditable privilege elevation solution that satisfies operational and compliance requirements?

To identify the most suitable solution for Soudal's environment, two tools were evaluated in parallel. Admin By Request (ABR) is a third-party cloud-based Privileged Access Management (PAM) platform offering multiple elevation modes and offline capability. Microsoft Endpoint Privilege Management (EPM) is a native add-on to Microsoft Intune that integrates directly into the existing management infrastructure. Both tools were deployed and tested in a controlled laboratory environment, assessed against the same set of evaluation criteria, and compared directly against each other.

According to the 2024 Verizon Data Breach Investigations Report, privilege misuse and credential abuse remain among the most common attack vectors in enterprise environments (Verizon, 2024). Soudal's exposure to these risks, combined with compliance obligations under ISO 27001 and the General Data Protection Regulation (GDPR), provided the operational justification for the project. This report is structured as follows. A glossary of technical terms and abbreviations used throughout this report is provided at the end of the document. Chapter 2 presents the analysis of Soudal's environment, the problem definition, and the identified use cases. Chapter 3 documents the Admin By Request laboratory testing in full. Chapter 4 presents the Microsoft EPM evaluation across eighteen structured tests. Chapter 5 provides a side-by-side comparison and final recommendation. Chapter 6 describes the deployment strategy and phased rollout plan. Chapter 7 covers stakeholder communication activities, and Chapter 8 presents the conclusions and outlook.

1.1 Personal Role and Responsibilities

The goal of this work placement was to apply the knowledge from the Bachelor of Applied Computer Science programme in a real enterprise environment and to deliver a practical outcome for a concrete security problem at Soudal. The assignment covered the full lifecycle of the project, from understanding the existing situation through to a live pilot deployment and the start of the wider rollout.

My responsibilities throughout the placement included the following:

- Analyzing Soudal's existing identity, device, and access management environment, and defining the privilege management problem together with the placement mentors.
- Identifying the main use cases for privilege elevation and translating them into a structured set of evaluation criteria.
- Building a controlled laboratory environment that mirrored Soudal's production setup as closely as possible.
- Deploying and testing Admin By Request, including resolving the Intune RBAC deployment issue, and documenting all six core feature tests.
- Deploying and evaluating Microsoft Endpoint Privilege Management across eighteen structured tests using the same methodology.
- Comparing both tools against Soudal's requirements and formulating a recommendation.
- Designing a phased deployment strategy, tailored access models, approval workflows, and a risk mitigation plan.
- Communicating progress and findings to the placement mentors, to Soudal management, and to the school, and engaging in the pilot department ahead of the rollout.

In addition to the technical work, the placement required ongoing stakeholder communication and decision-making, since the outcome was not only a tested solution but also a deployment approach that the company could adopt in practice.

2. Analysis

The analysis phase was conducted during the first weeks of the placement and focused on establishing a thorough understanding of Soudal's existing IT environment, the scope of the privilege management problem, and the specific operational requirements that any solution would need to address. This chapter presents the findings of that analysis and explains how they shaped the evaluation criteria and testing approach that followed.

2.1 Soudal's IT Environment

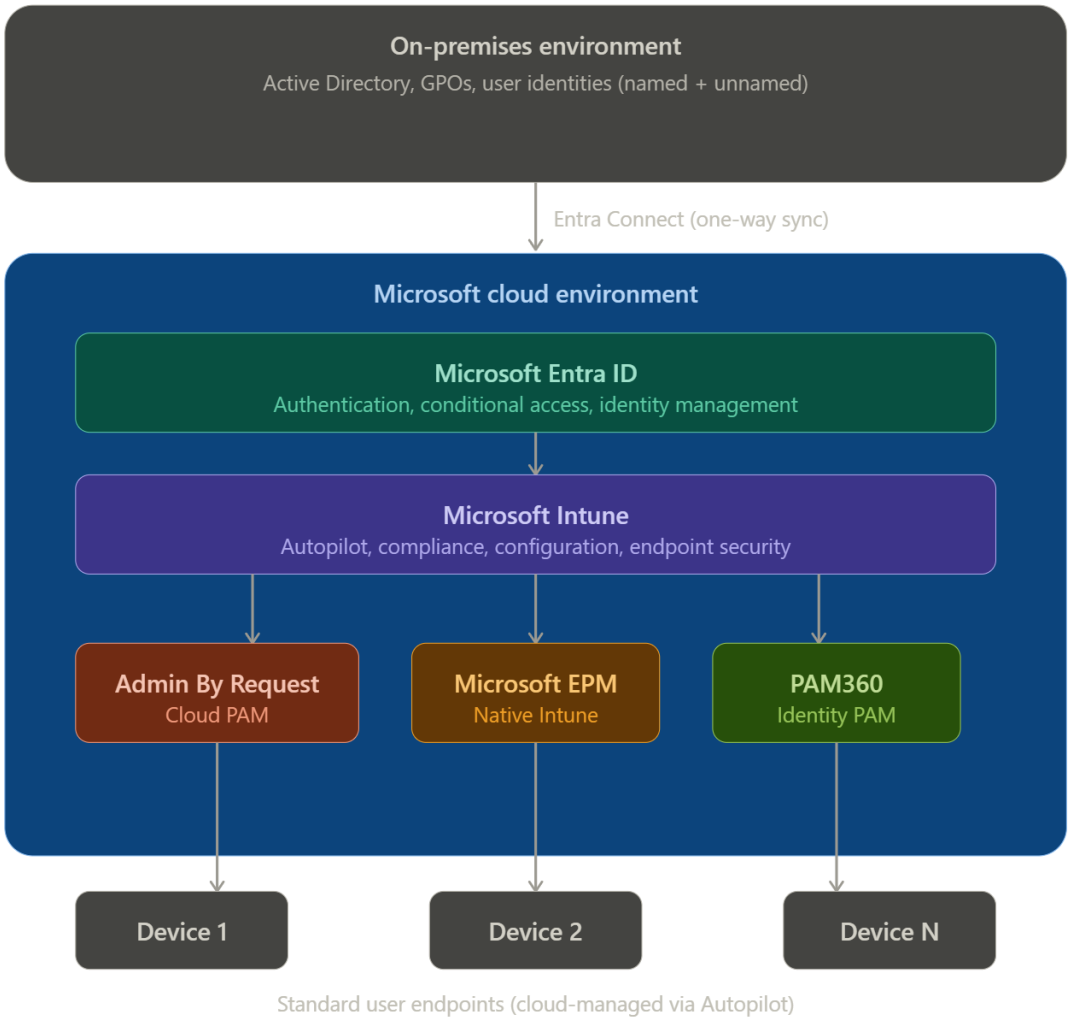
Soudal operates a hybrid identity and device management architecture built almost entirely on Microsoft cloud technologies. The backbone is a one-way synchronization between an on-premises Active Directory and Microsoft Entra ID (formerly Azure AD) via Entra Connect.

This means user accounts are created and managed on premises, then synchronized to the cloud, where they are used for authentication, licensing, and access control across all Microsoft cloud services. The architecture of Microsoft Entra ID and its role in cloud identity and Conditional Access enforcement are documented by Microsoft (Microsoft, 2026a).

All laptops and desktops are enrolled through Microsoft Intune using Autopilot for cloud-first device management. Intune is the central platform for everything endpoint-related: compliance policies, configuration profiles, application deployment, and endpoint security baselines. Conditional Access policies in Entra ID add another layer of control, ensuring that only compliant and properly authenticated devices can reach company resources.

In addition to the Microsoft stack, Soudal uses PAM360 as a SaaS-based privileged access management tool for infrastructure-level access scenarios. The environment supports several distinct network contexts: the corporate office network, factory floor networks in Turnhout and at other sites, and remote access for users working off-site (Soudal NV, 2026). That diversity of contexts, and especially the factory floor with its connectivity challenges, became one of the most important factors in the tool evaluation later.

Figure 1: Soudal IT environment architecture overview



Source: diagram provided by Soudal NV, reproduced with permission.

2.1.1 Identity and Access Structure

User accounts at Soudal fall into two distinct categories. Named accounts are assigned to full-time employees and come with a complete access profile: email, Microsoft 365 applications, cloud services, and VPN access. Unnamed accounts are used for factory and operational roles and are restricted to factory network segments, with no cloud application access.

Both account types are managed in Active Directory and synchronized to Entra ID, but the Conditional Access policies applied to them differ significantly. Named accounts go through full compliance checks including device compliance status, location signals, and risk assessment. Unnamed accounts have more restricted policies suited to their operational context.

What this means for privilege management is that any solution needs to work within this existing framework without disrupting Conditional Access or compliance policy enforcement. A tool that requires its own identity plane or bypasses Entra ID authentication was never going to be viable here.

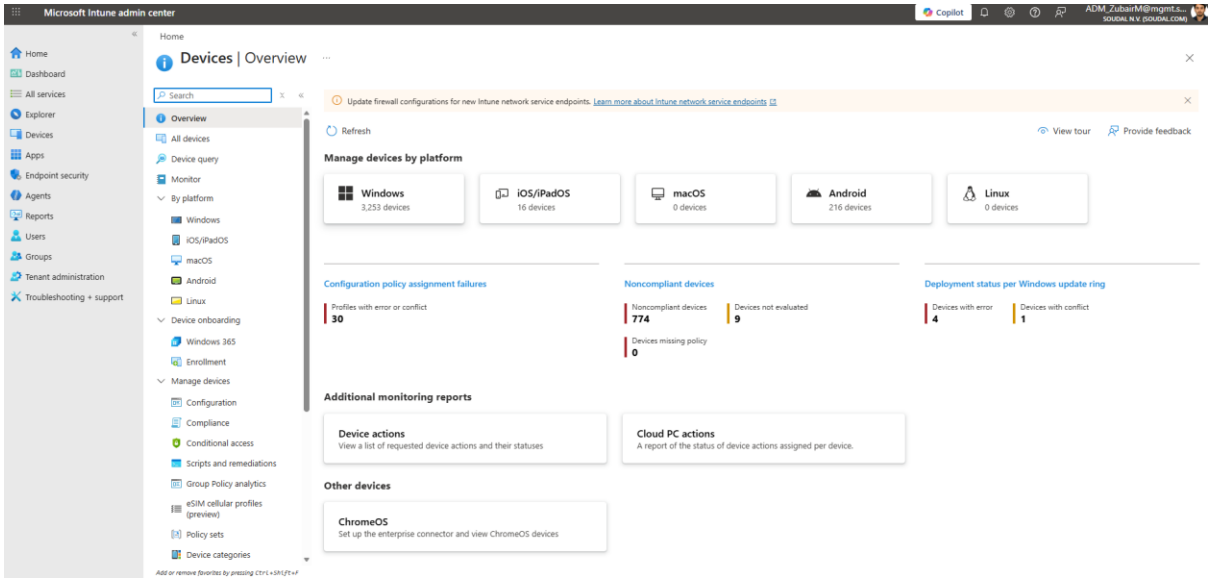
2.1.2 Device Management with Microsoft Intune

Microsoft Intune is not just a management tool at Soudal, it is the management platform. Every device that gets approved into the environment goes through Intune. Autopilot handles enrollment, which means devices arrive preconfigured with the right policies, applications, and security baselines already applied. Users just sign in and start working.

Intune manages compliance policies that enforce minimum security requirements such as BitLocker encryption, antivirus status, and patch levels. It distributes configuration profiles that control settings like password complexity and screen lock behavior. It deploys applications to device groups based on membership. And it enforces endpoint security policies including firewall rules, Defender settings, and disk encryption. A full description of these capabilities is provided in the Microsoft Intune documentation (Microsoft, 2026b).

Understanding this setup in depth was essential for the project because both ABR and EPM interact with Intune differently. ABR is deployed through Intune as an application but runs its own cloud-based management portal independently. EPM is natively embedded in Intune. It has no separate portal, and all configuration lives in the Intune admin center. That difference in architecture became one of the central comparison dimensions once testing began.

Figure 2: Microsoft Intune admin center



2.2 The Problem in Detail

The privilege problem at Soudal did not happen overnight, and it was not the result of poor IT management practice. It was the natural outcome of a growing organization where admin access was granted reactively, when someone needed it for a task, and then never systematically revoked. Over time, that accumulated into a situation where a meaningful portion of the user base had permanent local administrator rights that nobody could fully account for.

From a security standpoint, this is a significant risk. A user account with permanent local admin rights is a high-value target. If it is compromised through phishing, credential theft, or malware, the attacker gains immediate and unrestricted control over the device. From that foothold, lateral movement through the network becomes much easier. The 2024 Verizon Data Breach Investigations Report noted that privilege misuse and credential abuse remain among the most common attack vectors, and unnecessarily broad admin rights are a direct enabler of both.

From a compliance standpoint, the absence of an audit trail was equally problematic. Soudal is subject to multiple compliance frameworks including ISO 27001 and GDPR, both of which require demonstrable controls over who has privileged access and evidence of how that access is used. Without a centralized logging mechanism for admin activity, audits become difficult to pass and difficult to prepare for.

Following the initial analysis and discussions with the placement mentors, a more precise picture of the current state emerged. The issue was not that all users held admin rights. Rather, the wrong users held admin rights, without control, without logging, and without a mechanism to revoke those rights when they were no longer needed. At the same time, users who legitimately required elevated access for specific tasks were either blocked because access had been tightened, or they held permanent admin membership far broader than their actual needs justified.

The ideal outcome was not to remove admin rights and cause disruption. It was to replace permanent, uncontrolled admin access with something precise, temporary, and fully visible.

2.3 Use Cases Identified

Five main use cases were identified in collaboration with the placement mentors during the analysis phase. These cases define where and why privilege elevation is needed at Soudal, and they formed the foundation for the evaluation criteria, test designs, and deployment strategy that followed.

1. **Engineering Department:** Engineers at Soudal need admin access for two specific tasks: changing IP address configurations for factory equipment and installing hardware drivers. Both tasks happen in factory environments where the network connection can be intermittent or completely unavailable. This means any solution for this group must support offline elevation, it cannot require a cloud round-trip to approve an admin action.

2. **Service Desk:** Service Desk staff need consistent elevated access throughout the workday. They run remote support tools, deploy software to end-user machines, troubleshoot system issues that require admin interaction, and apply group policy updates. Unlike the engineering use case, Service Desk elevation needs to be reliable, fast, and available all day, constant approval workflows would create bottlenecks that undermine the team's ability to do its job.

3. **Application Installation:** This case splits into two sub-scenarios. The first is temporary full admin access for users who occasionally need to install applications or development tools, they need admin rights for thirty minutes, complete their task, and return to standard user status. The second is selective elevation for pre-approved applications: users who need a specific application to run elevated automatically every time they launch it, without requiring any approval interaction.

4. **Permission Revocation:** This is the operational side of the project. Once a privilege elevation solution is in place, the next step is systematically identifying and removing permanent admin rights from devices and user accounts where they are no longer necessary. This requires tooling that can inventory current privilege state, remove rights remotely, and track changes with a full audit trail.

5. **IT Policies and Compliance:** The compliance requirement threads through all of the above. Every elevation event, regardless of the use case, needs to be logged with enough detail to satisfy an audit: who requested elevation, on which device, for which application, at what time, for how long, and whether it was approved or denied. ISO 27001 and GDPR both have requirements that point directly at this.

2.4 Tool Selection

Two tools were selected for evaluation based on the problem analysis and use case mapping. The selection reflects both the existing Microsoft-centric technology stack at Soudal and the options available in the market for just-in-time privilege elevation.

2.4.1 Admin By Request (ABR)

Admin By Request is a dedicated, cloud-based Privileged Access Management platform that has been built specifically for the just-in-time elevation use case. It offers several distinct elevation modes: Run As Admin for elevating a single application, Admin Sessions for granting temporary full admin rights for a defined duration, an offline PIN mechanism for environments without connectivity, and pre-approved application rules for frictionless elevation of whitelisted software. ABR supports Windows, macOS, and Linux, integrates with Microsoft Intune for deployment, and operates through its own cloud management portal (Admin By Request, 2026).

The primary factor in selecting ABR for evaluation was the offline PIN feature. No other candidate solution offered a viable mechanism for the factory floor scenario where network connectivity cannot be guaranteed. This capability was considered essential for covering the engineering use case identified during the analysis phase.

2.4.2 Microsoft Endpoint Privilege Management (EPM)

EPM is part of the broader Microsoft Intune Suite, which packages a set of advanced endpoint management add-on capabilities including EPM, Remote Help, and Microsoft Tunnel for MAM (Microsoft, 2026e).

Microsoft EPM is a native component of the Microsoft Intune Suite, available as a paid add-on to Microsoft 365 E5 or as part of the Intune Suite bundle. It implements privilege elevation through virtual elevation accounts at the kernel level, meaning users never actually join the local Administrators group, but applications can be elevated through a controlled policy mechanism. All configuration and reporting lives inside the Intune admin center, making it invisible from a tooling overhead perspective for organizations that are already Intune-native. Detailed architecture and licensing information for Endpoint Privilege Management is provided by Microsoft (Microsoft, 2026d).

EPM's appeal is its architectural cleanliness. There is no extra portal, no additional agent to maintain beyond what Intune already deploys, and no separate vendor relationship to manage. For a

Microsoft-first environment like Soudal, that simplicity is operationally favorable. The open question going into testing was whether EPM's capabilities and especially its offline behavior was sufficient to cover all five use cases.

2.5 Evaluation Criteria

Eight evaluation criteria were established before testing began to ensure a structured and consistent comparison. These criteria were derived from the identified use cases and the operational requirements specific to Soudal's environment.

Criterion	Why It Matters for Soudal
OS Support	Soudal is primarily Windows today but may expand to macOS or Linux in the future. Platform lock-in is a risk worth assessing.
Offline Capability	Factory environments have unreliable connectivity. Any solution that cannot function offline is a non-starter for the engineering use case.
Elevation Methods	Different user groups need fundamentally different access models: permanent, session-based, app-specific, and offline PIN.
Audit Logging	ISO 27001 and GDPR compliance requires full traceability of every elevation event with sufficient detail for audit review.
Approval Workflows	The approval process needs to be fast and flexible enough to not become a bottleneck in day-to-day operations.
Intune Integration	All devices are managed through Intune. A tool that fits natively into that ecosystem reduces operational overhead.
User Experience	Elevation should be as frictionless as possible for legitimate use cases while maintaining security controls.
Cost	The licensing model needs to be sustainable for the number of users and the existing license footprint at Soudal.

Table 1: Evaluation criteria for tool selection at Soudal

3. Admin By Request Lab Testing

This chapter documents the laboratory evaluation of Admin By Request, covering the test environment setup, the Intune deployment process including the troubleshooting steps required to resolve a role-based access control issue, and the results of all six core feature tests.

3.1 Testing Environment

The laboratory environment was constructed to mirror Soudal's production infrastructure as closely as possible. This ensures that the test results are representative of real-world behavior and that any issues identified during testing would also be expected to arise in a production deployment.

Component	Details
Identity	Hybrid (on-premises AD ↔ Microsoft Entra ID via Entra Connect)
Device Management	Microsoft Intune with Autopilot enrollment and policy distribution
Access Control	Microsoft Entra ID Conditional Access policies
Network	Corporate Wi-Fi with an isolated test segment for controlled testing
Admin Portals	Intune Admin Center, Microsoft Entra ID portal, ABR cloud portal

Table 2: ABR laboratory testing environment components

3.1.1 Test Devices

Device	Role	OS
Admin Laptop	Managing Intune policies, ABR portal administration, and audit log review	Windows 11 Pro
Test Laptop 1	Primary testing device, Intune-managed standard user account	Windows 11 Pro
Test Laptop 2	Secondary device for multi-user consistency testing and policy replication validation	Windows 11 Pro

Table 3: Test devices used for ABR evaluation

3.1.2 Software Versions

The ABR Workstation Client version 8.7 was used throughout testing. Both Intune and Entra ID were running current 2026 tenant versions. PowerShell 7.x was used for post-action verification commands throughout the testing process, including group membership checks and elevation state validation.

3.2 Device Preparation

Before deploying ABR, each test device was verified as properly enrolled in Intune and operating correctly under a standard user account. Establishing a clean, confirmed baseline before introducing any elevation tooling is essential for ensuring that test results accurately reflect the behavior of the tool rather than pre-existing configuration differences.

The device initially reported as non-compliant in Intune, which is expected behavior while the first policy synchronization cycle runs and compliance is evaluated. Compliance status resolved automatically after synchronization completed. Device readiness was further verified using the dsregcmd /status command and by inspecting the local Administrators group, which showed no unexpected member accounts.

Before any elevation tooling was introduced, several actions requiring administrator rights were attempted on the device, including opening an elevated command prompt, modifying system settings, and installing a test application. All attempts were blocked, confirming that the standard user baseline was correctly in place before testing began.

Figure 3: Test Device Compliant

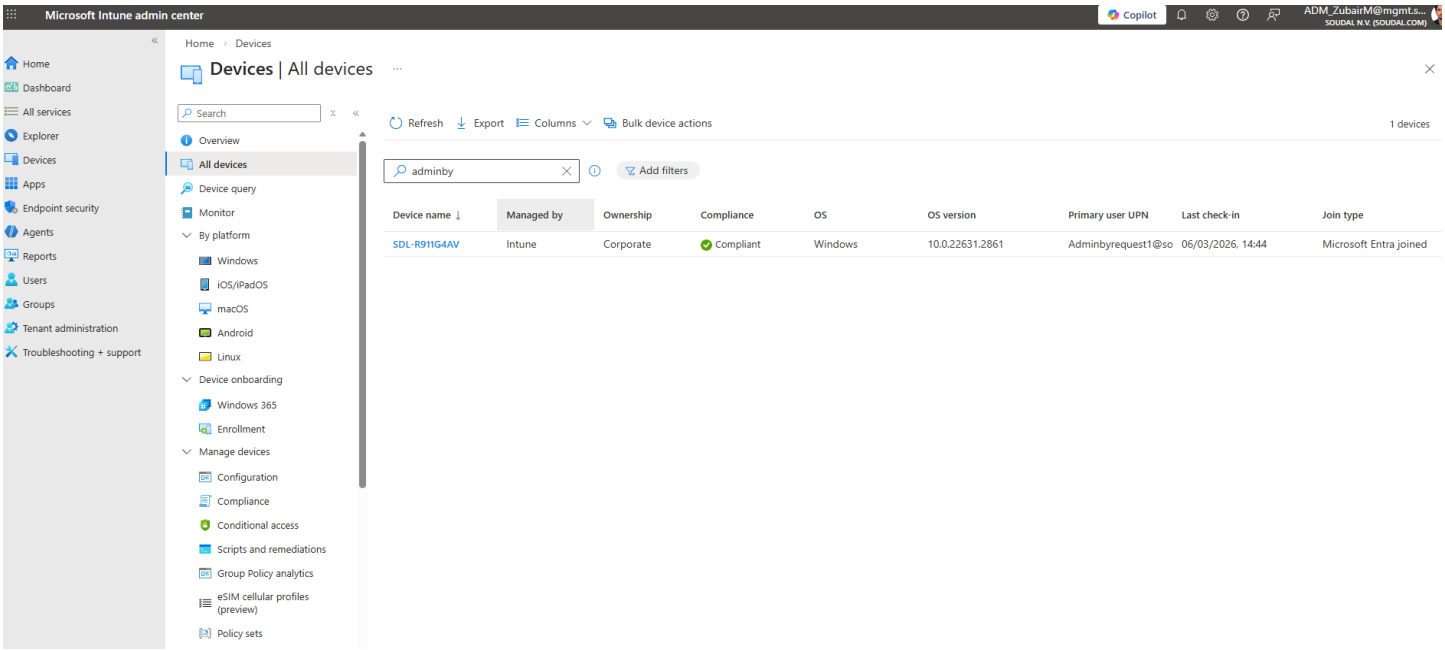
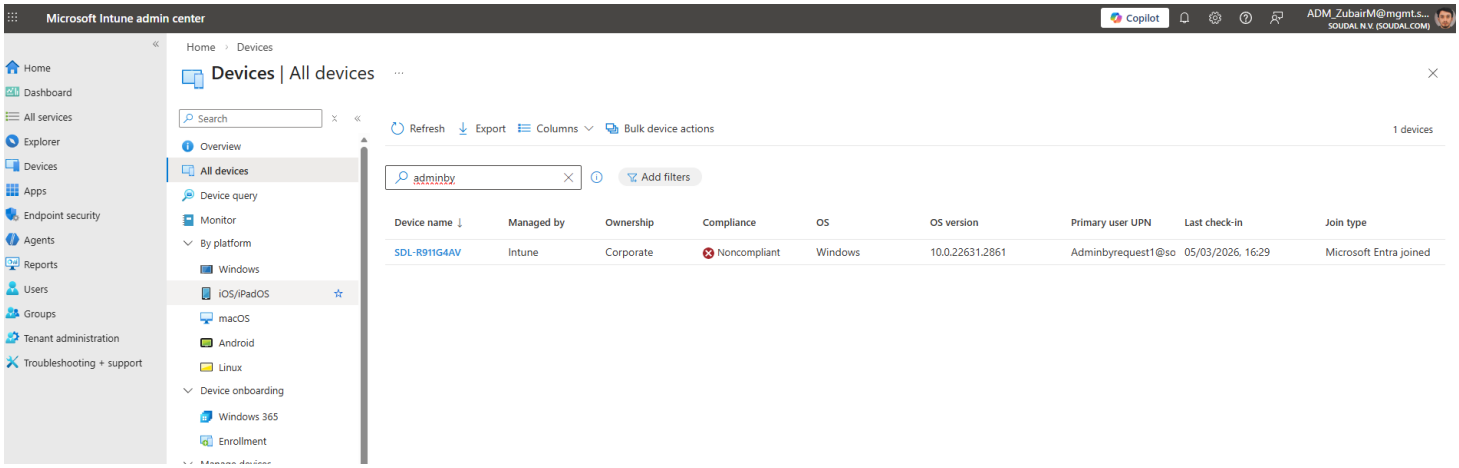


Figure 4: Test device non-compliant

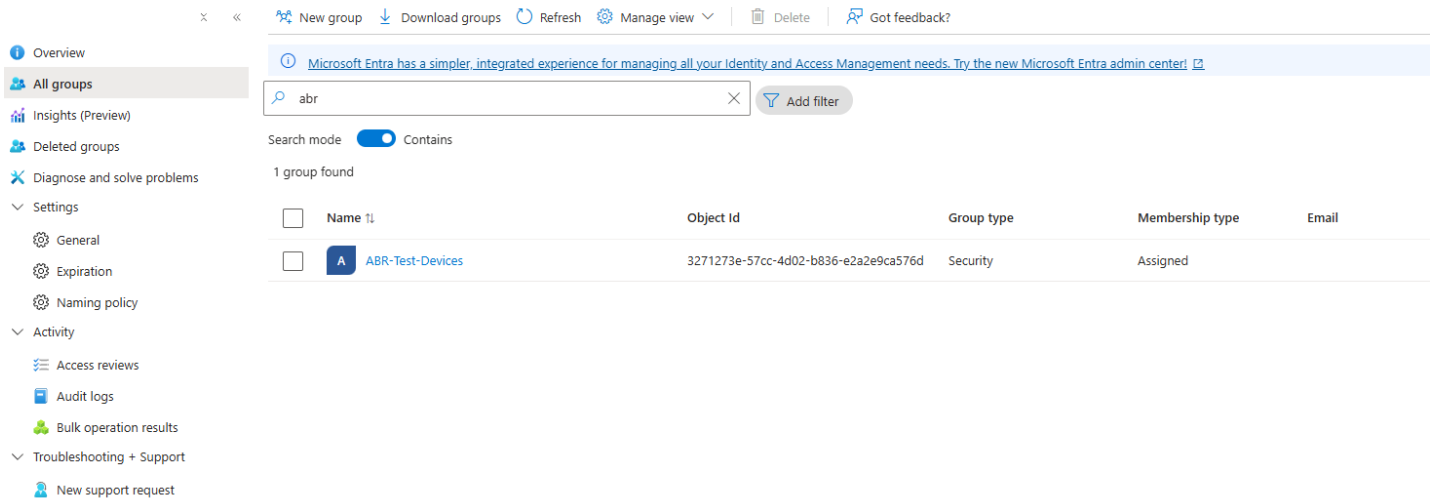


3.3 Deployment Scope Setup

To prevent any ABR configuration from reaching production devices, a dedicated Entra ID security group named ABR-Test-Devices was created before any deployment steps were taken. Scoping deployments to a controlled group is standard Intune practice, ensuring that only the intended devices receive the policy.

The group was created with dynamic membership rules based on device naming conventions so that only Test Laptop 1 and Test Laptop 2 would match. This group was then set as the assignment target for the ABR deployment package in Intune. No production devices were in scope at any point during the evaluation.

Figure 5: ABR-Test-Devices security group in Entra ID



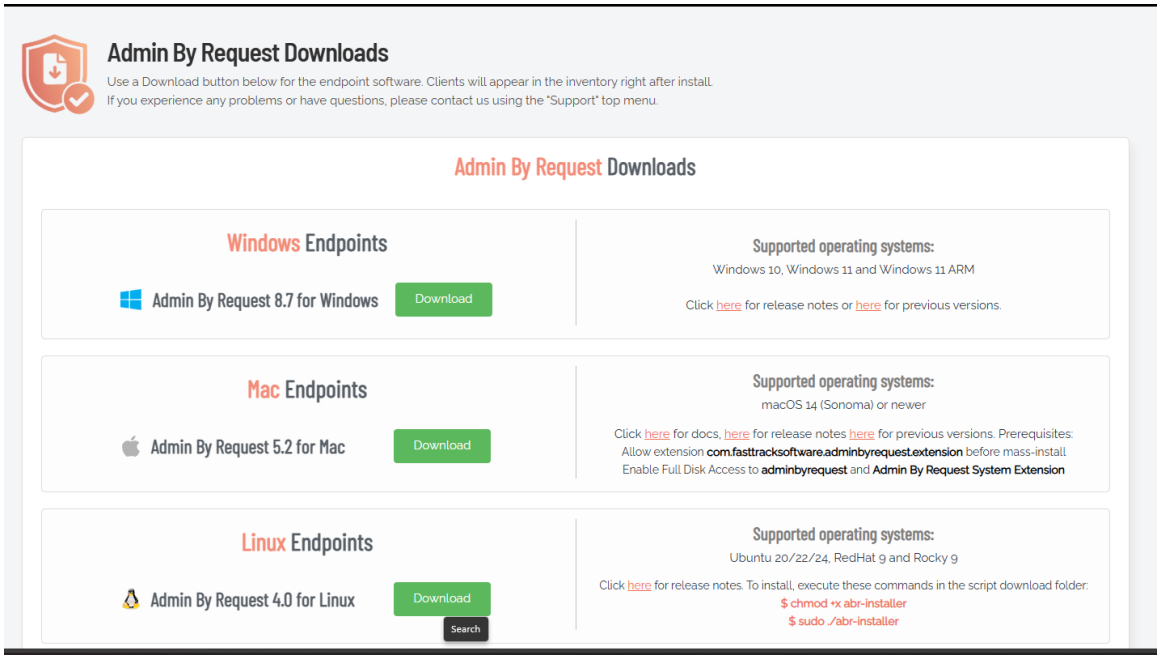
3.4 ABR Client Download and Verification

The ABR Workstation Client (version 8.7 MSI) was downloaded from the official ABR admin portal. Before proceeding with deployment, the installer was verified against several criteria to confirm its integrity and suitability for corporate deployment.

Verification included SHA256 hash comparison against the value published in the ABR portal, digital signature validation confirming the publisher certificate was valid and trusted, compatibility testing to confirm the MSI could be installed on Windows 11 Pro, and MSI structure inspection to confirm it was compatible with the msiexec deployment method Intune uses for LOB applications.

All checks passed. The installer was confirmed clean, correctly signed, and ready for deployment.

Figure 6: ABR installer SHA256 hash verification



3.5 Intune Deployment: Challenges and Resolution

The deployment of ABR through Intune required more time than anticipated due to a role-based access control configuration issue that was not immediately apparent from the error messages produced by the Intune portal. This section documents the troubleshooting process in full, as the root cause and resolution are relevant to any similar deployment in an Intune-managed environment.

3.5.1 First Attempt: Line-of-Business Deployment

The initial deployment approach used Intune's Line-of-Business app deployment type, which is the standard method for MSI installers. The steps were straightforward: open Intune Admin Center, navigate to Apps, select the LOB app type, upload the ABR MSI file, configure detection rules, and assign the deployment to ABR-Test-Devices with Required intent.

The upload appeared to process correctly. The deployment then failed with the following error:

Error: *"Save application failed, TypeError: Cannot read properties of null (reading 'appType')"*

The error was completely generic and did not indicate a specific cause. Additional application types were tested to determine whether the problem was specific to the ABR MSI, including Win32 apps, web apps, and a simple store app. Every attempt failed with a similar JavaScript error, indicating that the issue was not with the ABR installer itself but with the deployment environment at a more fundamental level.

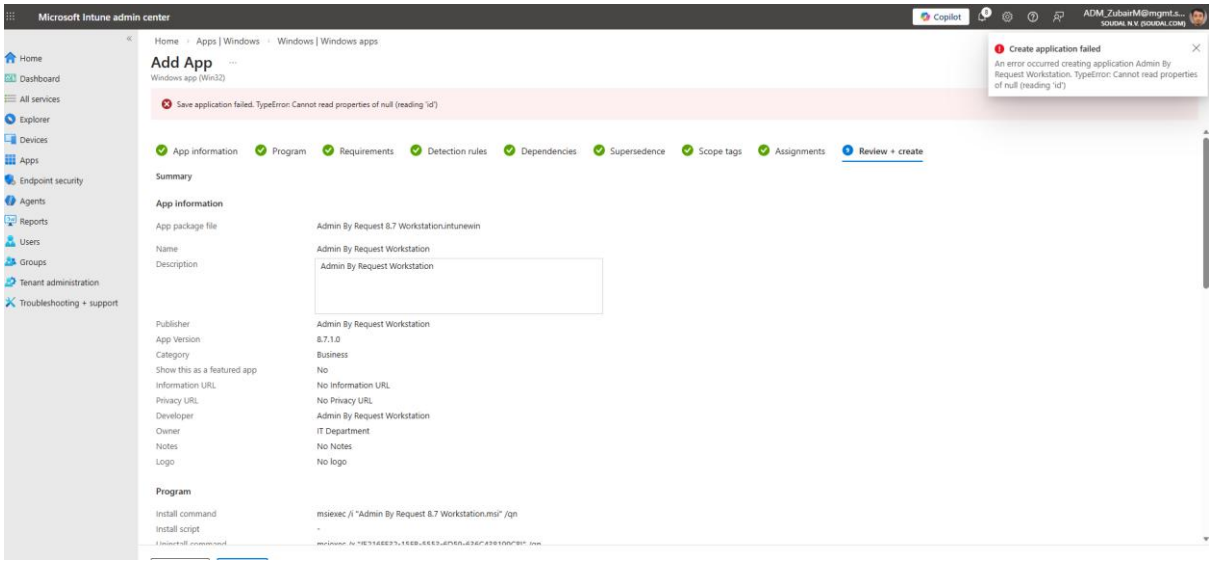
3.5.2 Troubleshooting Steps

A systematic set of troubleshooting steps was followed before the root cause was identified. Each step was documented throughout the process:

- Cleared browser cache and refreshed the Intune session in both Edge and Chrome
- Attempted the upload from an entirely different browser profile to rule out session token issues
- Re-downloaded the ABR MSI and verified its hash to rule out a corrupted file
- Renamed the installer file to remove version numbers, which is a known workaround for some Intune upload parsing issues
- Created a fresh application entry from scratch rather than modifying the failed one
- Checked Microsoft documentation and the Intune admin center service health page for known issues
- Attempted deployment from a different network segment to rule out proxy or firewall interference

None of these steps made any difference. The failures were consistent regardless of app type, file, browser, or network. That consistency was the key signal: this was a permissions issue, not a packaging issue.

Figure 7: Intune LOB app deployment error message



3.5.3 Root Cause: RBAC Permissions

After ruling out all other causes, the issue was identified as a misconfiguration in the Intune Role-Based Access Control (RBAC) settings for the account being used.

Intune was returning a generic JavaScript exception rather than a meaningful permission error, a known UI limitation that makes RBAC-related failures difficult to diagnose without prior knowledge of this behavior. The role assignments and required permission categories for application management are described in the Microsoft documentation for Intune RBAC (Microsoft, 2026c).

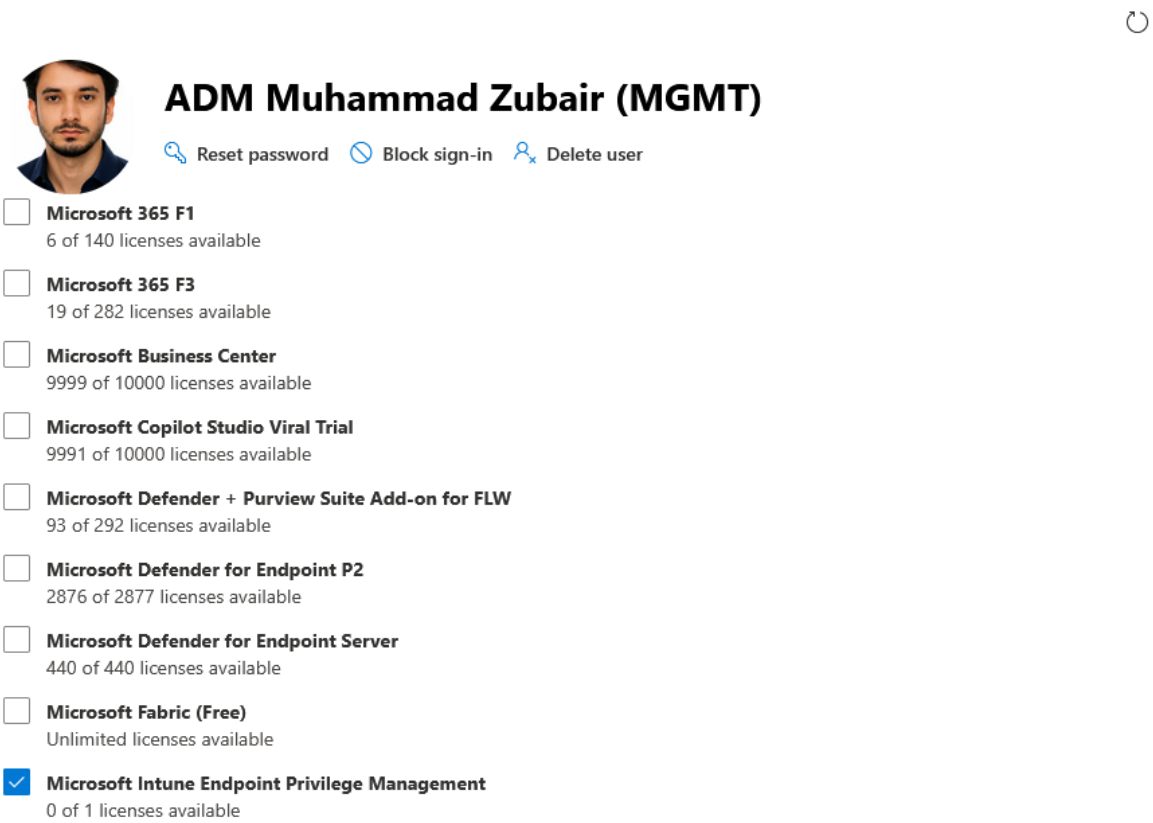
The specific missing or misconfigured roles were: Mobile Application Management (MAM) create applications permission, Microsoft Intune Administrator with full app management scope, Cloud Application Administrator for assigning cloud-based applications, and Application Administrator for delegated app management. Without all of these, Intune could not complete the app registration process, and the portal was not surfacing that as a clear permission denied message.

3.5.4 Resolution with Mentor Support

The issue was escalated to Eduard Claessen, who reviewed the RBAC configuration and identified the missing role assignments. The required permissions were corrected, and after approximately 20 minutes for the role changes to propagate through Entra ID, application creation was tested again and completed without errors.

The key lesson from this troubleshooting exercise is that when Intune fails to create applications regardless of app type or source file, RBAC configuration should be the first thing checked. The portal's error messages do not reliably indicate permission-related failures, and troubleshooting the package rather than the account permissions wastes significant time. Permissions should be verified at the start of any Intune deployment, particularly in environments where role assignments have been added incrementally over time.

Figure 8: EPM license verification in Microsoft 365 admin center



3.5.5 Alternative Method: Win32 Packaging

Following resolution of the permissions issue, the Win32 packaging method was also validated as an alternative deployment approach. Using the Microsoft Win32 Content Prep Tool (IntuneWinAppUtil.exe), the ABR MSI was converted into an .intunewin package. Win32 deployment provides more granular control over detection rules, return codes, and dependency handling, which is beneficial for more complex installers.

Both the LOB and Win32 deployment paths were confirmed working. The LOB method was used as the primary approach for this evaluation since the ABR installer is a straightforward MSI. The Win32 path is documented here as a validated alternative for production deployment if needed.

3.6 Successful Deployment Confirmation

With the permission issue resolved, ABR deployed successfully to Test Laptop 1 through Intune as a Required LOB application. The device picked up the deployment policy automatically on its next sync cycle and installed ABR without any user interaction.

Post-installation verification confirmed that the ABR system tray icon was visible and active, the ABR client process was running in Task Manager, the device appeared correctly in the ABR portal under the Inventory view, the device authentication certificate was present in the Windows certificate store, and the ABR service was listed as running in Windows Services.

A resilience test was also performed by manually uninstalling ABR from the test device to verify that the Required Intune assignment would trigger automatic reinstallation. On the next synchronization cycle, Intune detected the missing application and pushed the reinstall without manual intervention, confirming that the deployment is correctly enforced and self-healing.

Figure 9: ABR Panel on installed machines

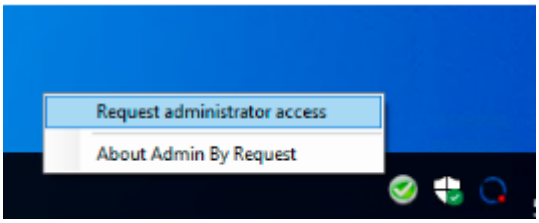


Figure 10: Inventory overview of devices

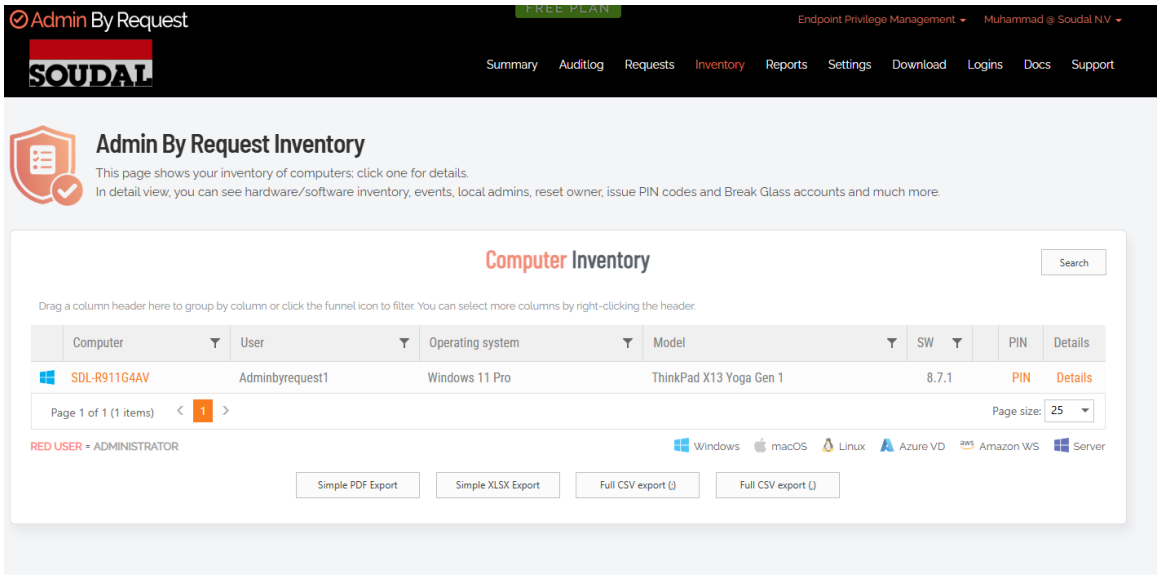
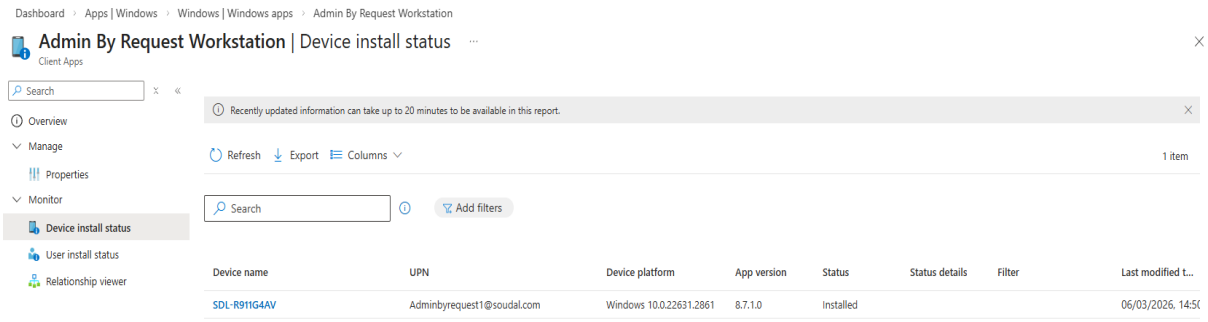


Figure 11: Installed status on Intune



3.7 Core Feature Testing

With ABR successfully deployed and the baseline verified, the core feature testing phase began. All tests were performed using a standard user account with no pre-existing administrator rights, replicating the conditions that would apply to end users in a production deployment.

3.7.1 Test 1: Run As Administrator Request

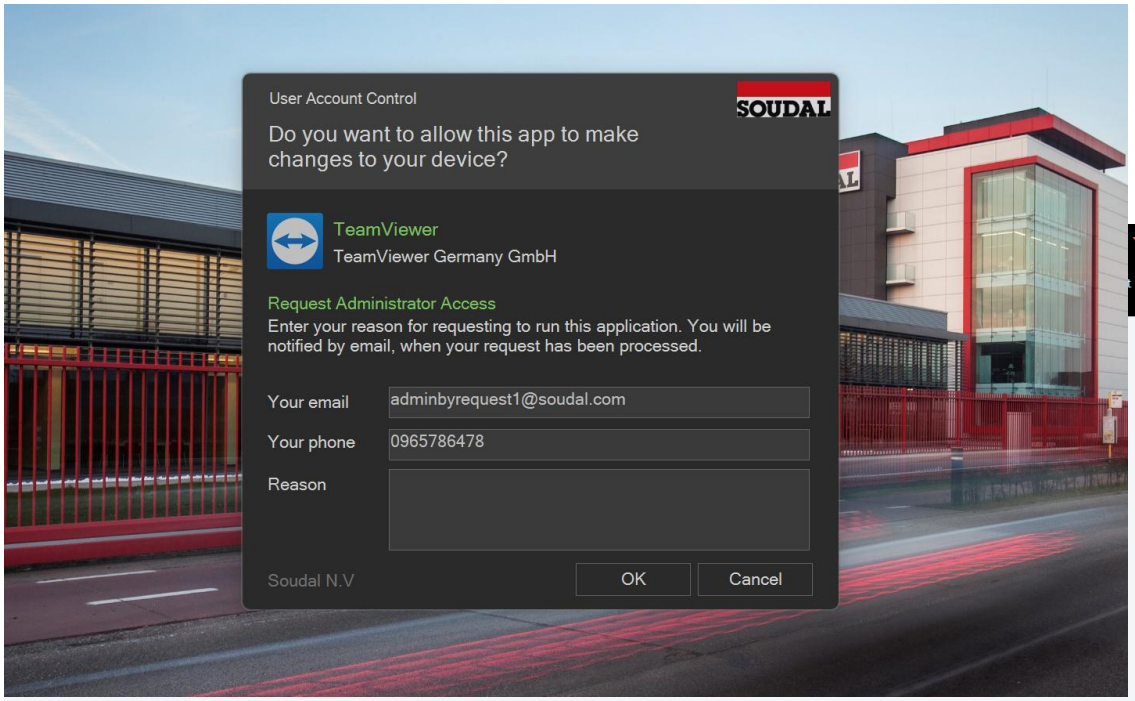
The first test validated the primary ABR workflow: a user needs to run an application with elevated privileges, submits a request, and receives approval from an administrator. This is the most common day-to-day scenario for users who do not have permanent admin rights.

To conduct this test, Command Prompt was launched using the Run as Administrator option from a standard user account. The ABR client intercepted the request and displayed the elevation request form, where an optional business reason was entered before submission.

The request appeared immediately in the ABR portal under the Requests view and was approved from the administrator account. Within seconds, Command Prompt opened elevated on the test device. The full audit entry appeared in the portal with all expected fields populated, including timestamp, requesting user, application name, device name, and the reason text provided.

Result: Run As Administrator request captured, approved, and executed correctly. Audit trail complete. **Status:** **Pass**

Figure 12: Run as administrator elevation prompt



3.7.2 Test 2: Admin Session Request

The Admin Session feature grants temporary full administrator rights for a defined duration, the equivalent of being added to the local Administrators group for a period of time. This is the right elevation model for Service Desk staff and engineers who need to perform multiple admin actions sequentially without requesting elevation for each individual application.

The Admin Session was initiated by right-clicking the ABR system tray icon and selecting Request Administrator Access. The request form presented options for session duration, including 15 minutes, 1 hour, and custom durations, as well as a field for a business justification. After approval through the ABR portal, the session was activated from the tray.

Session activation was verified using the Get-LocalGroupMember Administrators command in PowerShell, which confirmed that the test user account had been temporarily added to the local Administrators group. Administrative commands that had previously failed executed correctly during the active session. The session countdown timer was visible in the ABR tray icon.

Result: Admin Session activated successfully. User gained temporary Administrators group membership. All elevated operations worked correctly during the session. **Status:** **Pass**

Figure 13: Admin session approval screen

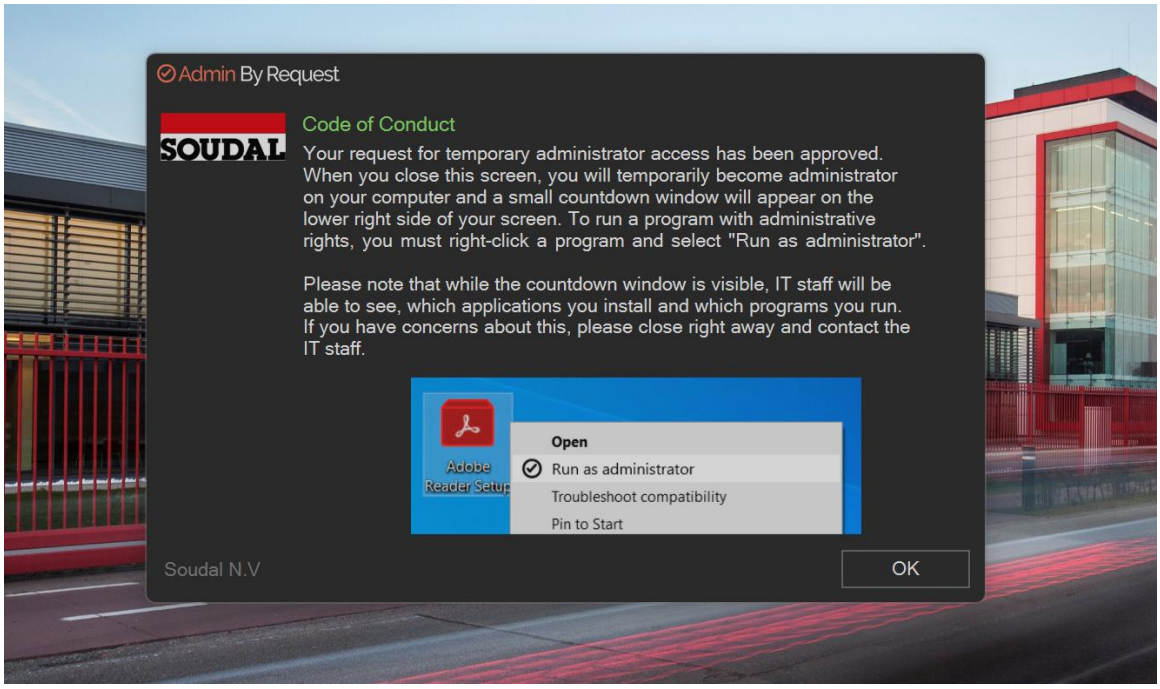
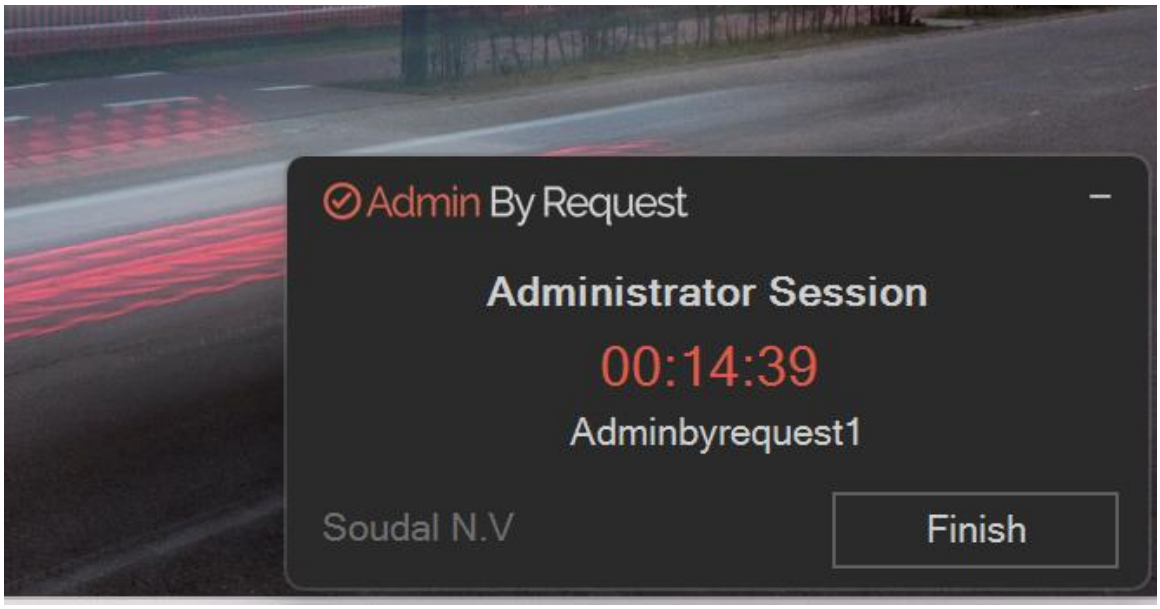


Figure 14: Timed admin session



3.7.3 Test 3: End Admin Session

This test verified that privilege revocation works as expected when a session is manually terminated. Reliable revocation is just as important as reliable elevation. An admin session that does not end cleanly is a security liability.

With an active session running, the End Administrator Session option was selected from the ABR tray icon. The client confirmed termination and returned to its idle state. The Get-LocalGroupMember Administrators command was run again immediately, confirming that the test user account was no longer a member of the local Administrators group. A subsequent attempt to launch an elevated command prompt triggered the ABR elevation request form, confirming the session state had been fully reset.

Result: Admin Session terminated correctly. Privilege revocation was immediate. User returned to standard user state and ABR intercepted the next elevation attempt as expected. **Status: Pass**

3.7.4 Test 4: Offline PIN Elevation

This test was the most critical test for Soudal's requirements. Factory environments at Soudal are not always connected to the corporate network. Engineers working with PLC equipment or factory hardware may need to elevate their privileges in a location where there are no Wi-Fi signals and no cellular fallback. A solution that cannot handle this scenario is a solution that cannot cover the engineering use case.

An offline PIN was configured in the ABR portal prior to testing. The Wi-Fi adapter on the test device was then disabled to simulate a fully offline environment, and the absence of network connectivity was confirmed before proceeding.

With the device offline, an application was launched using Run as Administrator option. The ABR client detected the offline state and presented a PIN entry prompt rather than the standard online request form. After the PIN was entered, the application launched with elevated privileges. No network connection was used at any point in the elevation flow.

When the Wi-Fi adapter was reconnected, the offline elevation event synchronized automatically to the ABR portal. The resulting audit entry contained all expected fields, including timestamp, device, application, an offline event indicator, and a hash of the PIN used.

Result: Offline PIN elevation worked reliably with no network connectivity. Audit event synchronized correctly after reconnection. This feature directly addresses the engineering and factory use case.
Status: **Pass**

Figure 15: ABR Offline PIN elevation prompt

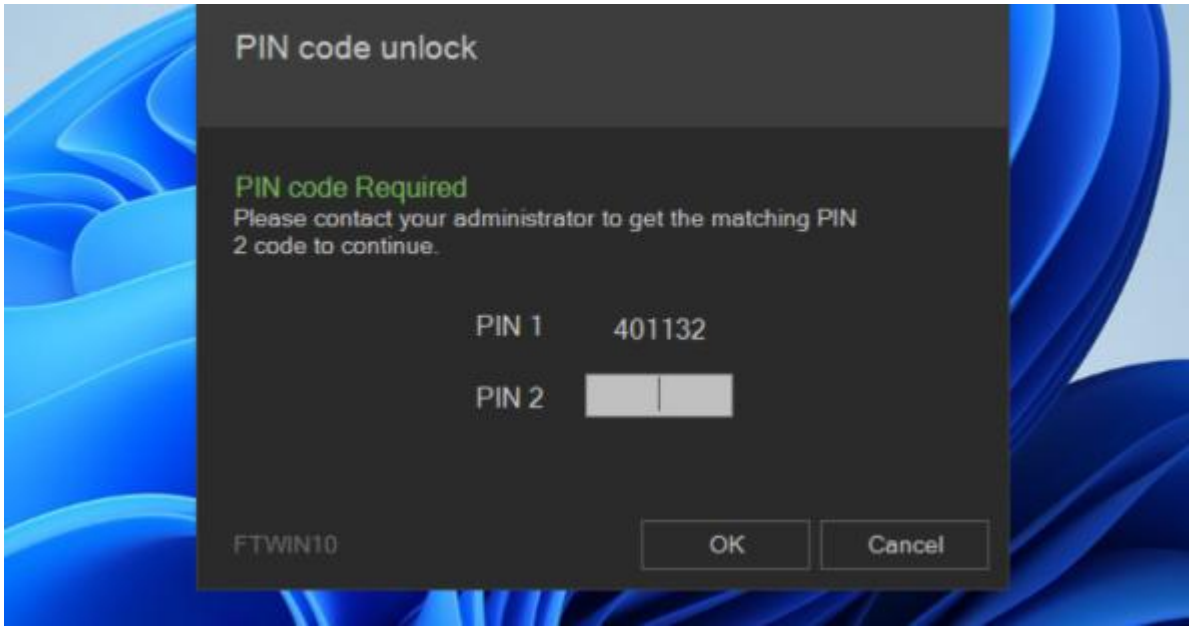
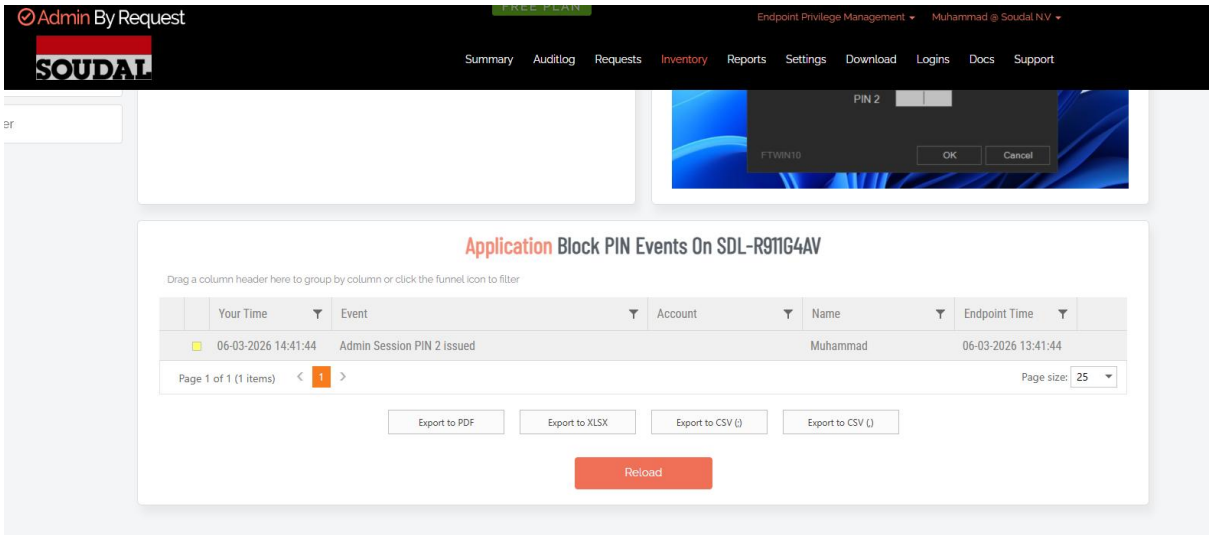


Figure 16: Audit event after offline PIN elevation



3.7.5 Test 5: Pre-Approved Application Rule

Pre-approved application rules allow specific applications to run elevated automatically without requiring any approval interaction. This is the right model for applications that are known to be safe, are frequently used, and would create constant approval requests if handled through the standard elevation workflow.

A pre-approval rule was created in the ABR portal targeting chrome.exe located in the Program Files directory, configured for automatic silent elevation without a user prompt. When Chrome was launched on the test device, the ABR client evaluated the launch against the configured rule set, matched the file, and elevated the application without displaying any dialog.

The resulting audit log entry in the ABR portal was tagged as auto-approved and contained a reference to the specific rule that matched, providing full visibility into the auto-elevation event.

Result: Pre-approved application rule matched correctly. Application elevated automatically with no user prompt. Audit entry confirmed auto-approval and rule reference. **Status:** **Pass**

Figure 17: ABR pre-approved rule

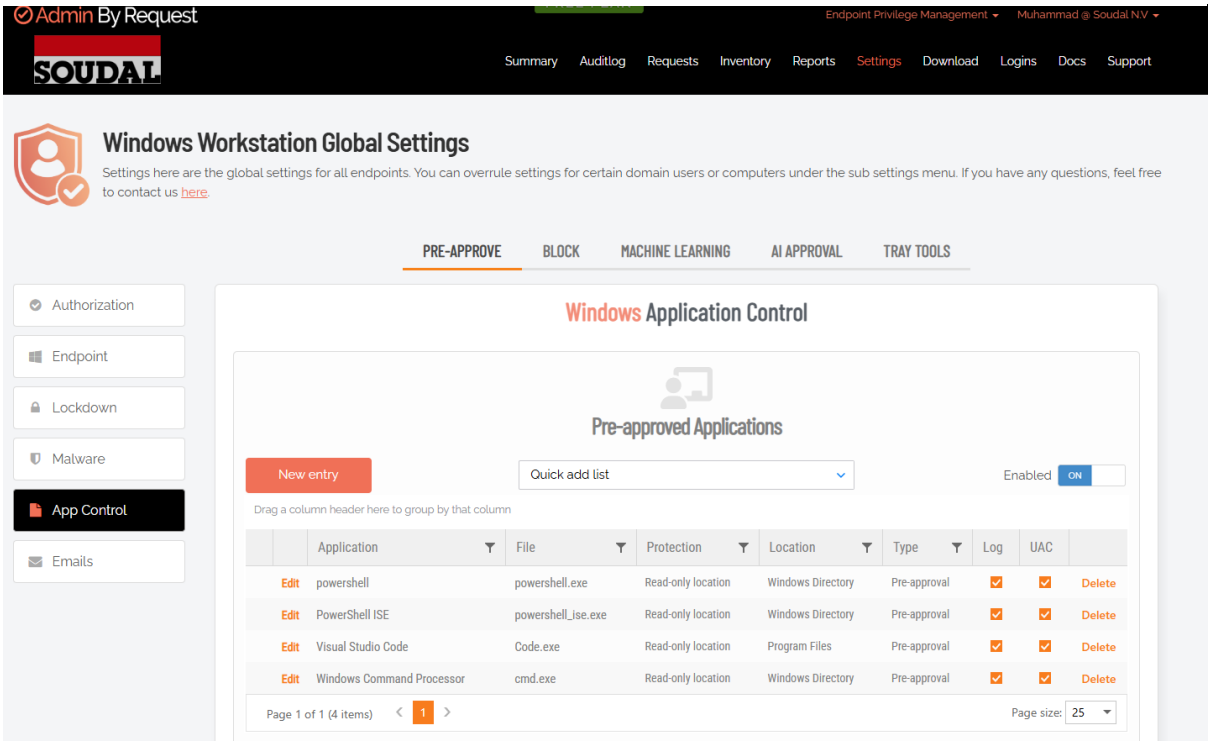
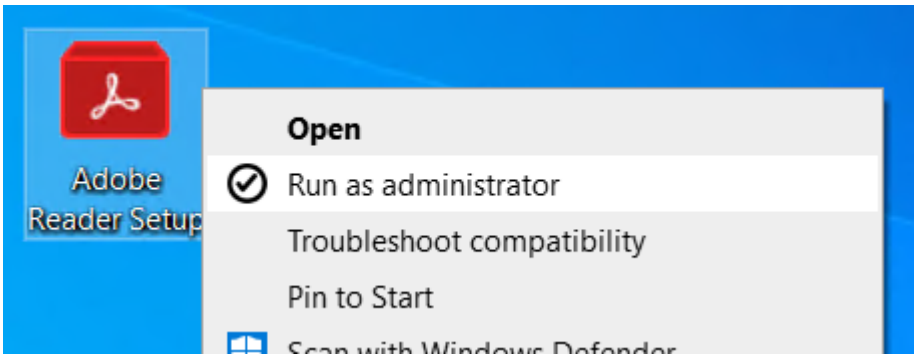


Figure 18: Normal elevation demonstration

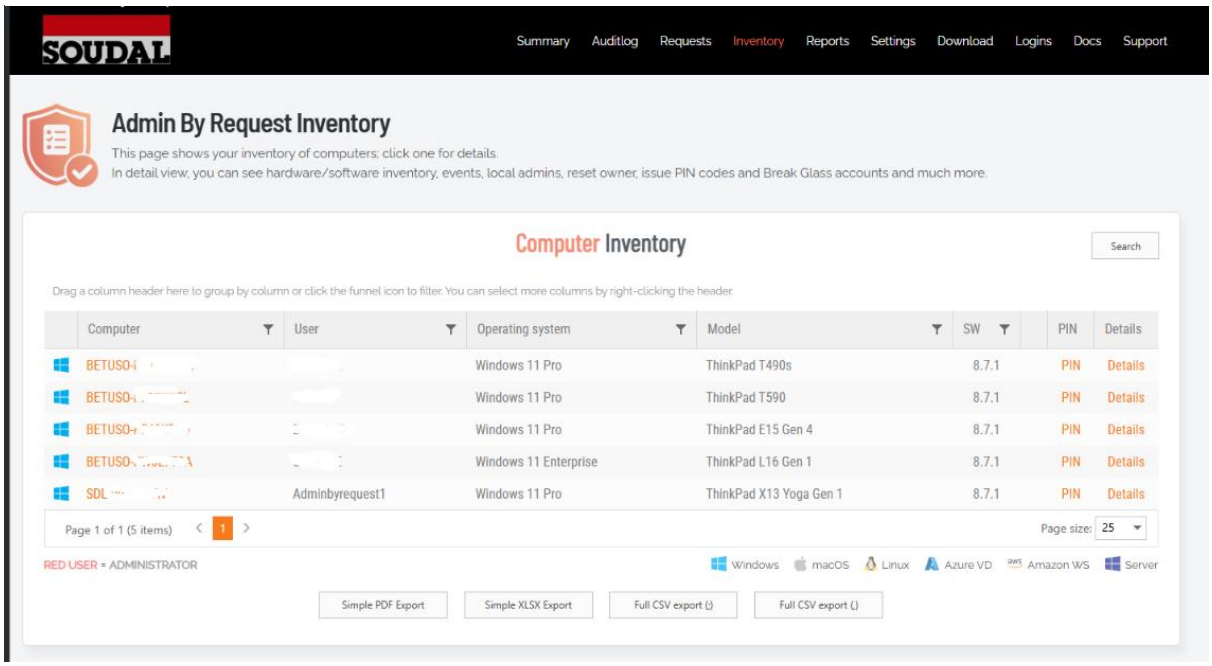


3.7.6 Test 6: Local Administrator Monitoring

The final ABR test evaluated its inventory and monitoring capabilities, specifically, its ability to identify which users currently have permanent local administrator rights on which devices. This capability is essential for the permission revocation use case, which requires a clear picture of the current state before anything can be systematically cleaned up.

The Devices view in the ABR portal displayed a real-time breakdown of the local Administrators group membership on the test device, showing individual accounts with their names, types, and membership status. Remote revocation was tested by removing a test admin account from the group through the portal without any physical interaction with the device. The change was confirmed to have taken effect immediately by checking the local group on the device.

Figure 19: Local administrator inventory in ABR portal



Result: Local administrator inventory was accurate and real-time. Remote revocation through the portal worked immediately. This capability is directly relevant to Phase 2 of the deployment strategy.
Status: **Pass**

3.8 Testing Summary

All six core ABR features were tested and passed. The table below summarizes the results.

Feature / Scenario	Test	Result	Status
Run As Administrator	Test 1	Request captured, approved, executed with full audit trail	Pass
Admin Session	Tests 2–3	Activation and termination both worked correctly	Pass
Offline PIN Elevation	Test 4	Elevation without network; audit synced on reconnection	Pass
Pre-Approved Rules	Test 5	Auto-elevation without prompt; audit entry confirmed	Pass
Local Admin Monitor	Test 6	Real-time inventory and remote revocation confirmed	Pass
Intune Enforcement	Manual test	Auto-reinstall on removal confirmed	Pass

Table 4: ABR core feature testing summary

3.9 Key Strengths Identified

ABR performed well across all six tests. The strengths that were most relevant to Soudal's requirements were:

- The offline PIN is reliable and audit-preserving. This is the single most important capability for the engineering and factory use case, and it works exactly as documented.
- The audit trail is comprehensive. Every elevation event, online or offline, manual or auto approved, is logged with timestamp, user, device, application, and outcome.
- Multiple elevation modes let ABR serve different user groups with different access models from a single platform.
- The local administrator monitoring and remote revocation tools make the permission revocation phase of the project operationally realistic.
- Deployment through Intune is clean and the Required assignment enforcement is consistent.
- The platform supports Windows, macOS, and Linux, which provides flexibility if Soudal’s endpoint landscape expands beyond Windows in the future.
- The system tray UX is intuitive enough that users can figure out how to submit a request without training.

3.10 Observations and Considerations

Alongside the strengths, the testing also surfaced several things worth noting for anyone planning a production deployment at Soudal:

- The initial deployment failure due to RBAC misconfiguration was not obvious from the error messages. Anyone deploying ABR (or any Intune application) should verify RBAC permissions before beginning, not during troubleshooting.
- The approval workflow requires operational discipline. If IT staff do not respond to approval requests promptly, users will experience friction. Clear SLAs and multiple approvers are needed before this goes to production.
- Offline PINs need to be managed carefully. A PIN that is never rotated becomes a security liability. A PIN rotation policy and secure distribution process needs to be defined before enabling the offline feature at scale.
- User training is needed, particularly for users who have never interacted with an elevation request workflow before. The system is intuitive but not completely self-explanatory for non-technical users.
- Performance impact was negligible during testing. ABR consumed less than 1% CPU at rest and introduced no perceptible delay to the elevation workflow.

4. Microsoft Endpoint Privilege Management Lab Testing

Following the completion of the ABR evaluation, the project moved on to Microsoft Endpoint Privilege Management. Where ABR is a dedicated third-party PAM platform with its own portal and cloud infrastructure, EPM is a native component of Microsoft Intune, deployed and managed entirely within the environment Soudal already operates.

EPM testing was conducted using the same structured methodology applied to ABR, covering eighteen tests across basic elevation behavior, offline functionality, policy conflict handling, and child process control. The objective was to generate an evidence-based assessment of EPM's capabilities in Soudal's environment without a predetermined conclusion.

4.1 EPM Overview

Microsoft EPM implements privilege elevation through a virtual elevation account at the kernel level. This is architecturally different from the way most PAM tools work. When EPM elevates an application, the user does not join the local Administrators group. Instead, the elevation is granted at the process level through a virtualized context, which means the user's account remains a standard user for all other purposes. This is a genuine security advantage, there is no window during which the user is broadly privileged, even for a fraction of a second.

Elevation is defined through policies configured in the Intune admin center. Two main policy types are used: an elevation settings policy that defines overall behavior and user prompt requirements, and elevation rule policies that specify which applications or processes are permitted to elevate and under what conditions. Rules can match applications by file path, file hash, publisher certificate, or combinations of these. EPM also allows administrators to control child process behavior, specifically whether child processes started by an elevated application inherit or are denied elevation.

All elevation events are logged in Microsoft Intune's reporting infrastructure, where they can be reviewed alongside device compliance data, configuration policy status, and other endpoint telemetry. There is no separate portal, no separate log store, and no separate agent beyond what Intune already deploys.

4.2 Testing Environment

Component	Details
Identity	On-premises Active Directory synchronized to Microsoft Entra ID via Entra Connect
Device Management	Microsoft Intune with Autopilot enrollment
Access Control	Conditional Access policies through Entra ID
Endpoint Platform	Windows 11 Pro devices enrolled and compliant in Intune
Security Context	Standard user accounts with no permanent local admin rights
Management Portal	Microsoft Intune Admin Center (no separate EPM portal)

Table 5: EPM testing environment components

4.2.1 Test Devices

Device	Role	OS
Admin Laptop	Intune administration, EPM policy creation, monitoring, and audit log review	Windows 11 Pro
Test Laptop 1	Primary EPM testing device, Intune-managed standard user account	Windows 11 Pro
Test Laptop 2	Secondary device for consistency validation and multi-user testing	Windows 11 Pro

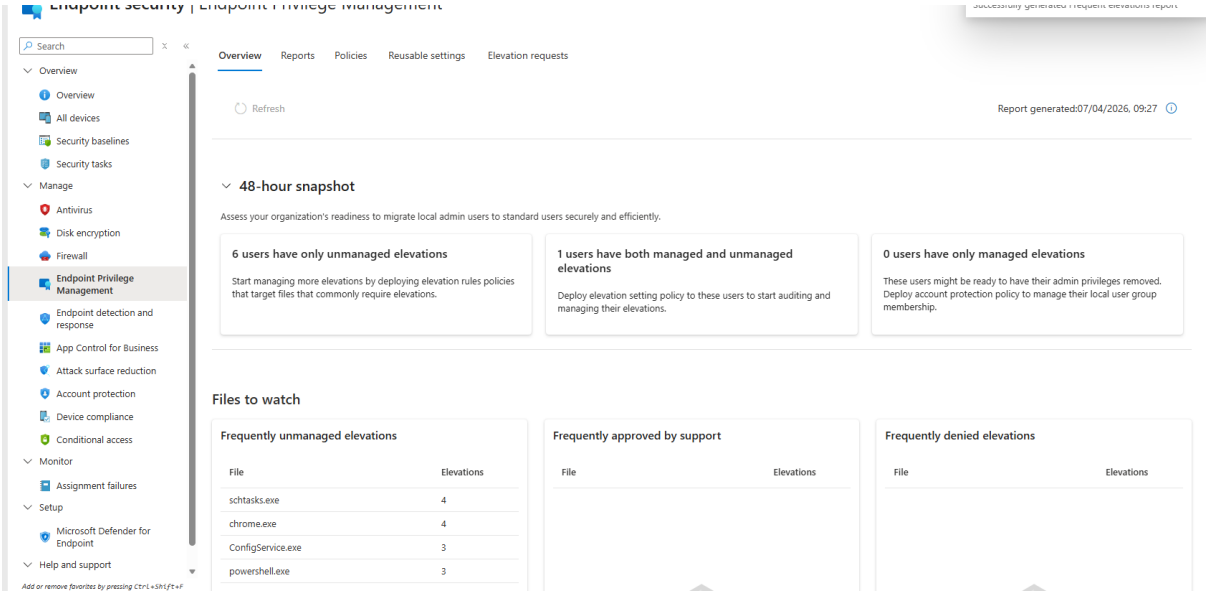
Table 6: Test devices used for EPM evaluation

4.2.2 Licensing and Software

Component	Status / Version
Microsoft Intune	Current tenant version (2026)
Microsoft Entra ID	Current tenant version (2026)
Windows 11 Pro	10.0.26100.8037
EPM License	Active and assigned to test device

Table 7: EPM licensing and software versions

Figure 20: EPM overview



4.3 Device Preparation and Baseline Verification

Before any EPM rules were deployed, each test device was verified against the same baseline used for ABR testing. Each device needed to be enrolled, compliant, and confirmed as operating under a standard user account with no existing administrator privileges. This baseline is essential for valid test results, as testing privilege elevation on a device where the user already holds admin rights through a separate mechanism would produce meaningless outcomes.

The following verification steps were completed for each test device:

- Connected to the corporate test network and signed in with Entra ID credentials
- Verified Entra Join status using dsregcmd /status in Command Prompt
- Confirmed device enrollment and compliance status in the Intune admin center
- Verified the user account was not a member of the local Administrators group using Get-LocalGroupMember Administrators in PowerShell
- Attempted several admin-required actions (opening elevated Command Prompt, modifying system settings) and confirmed all were blocked before any EPM rule was applied
- Confirmed device was correctly assigned to the EPM test group in Intune

Figure 21: EPM security group

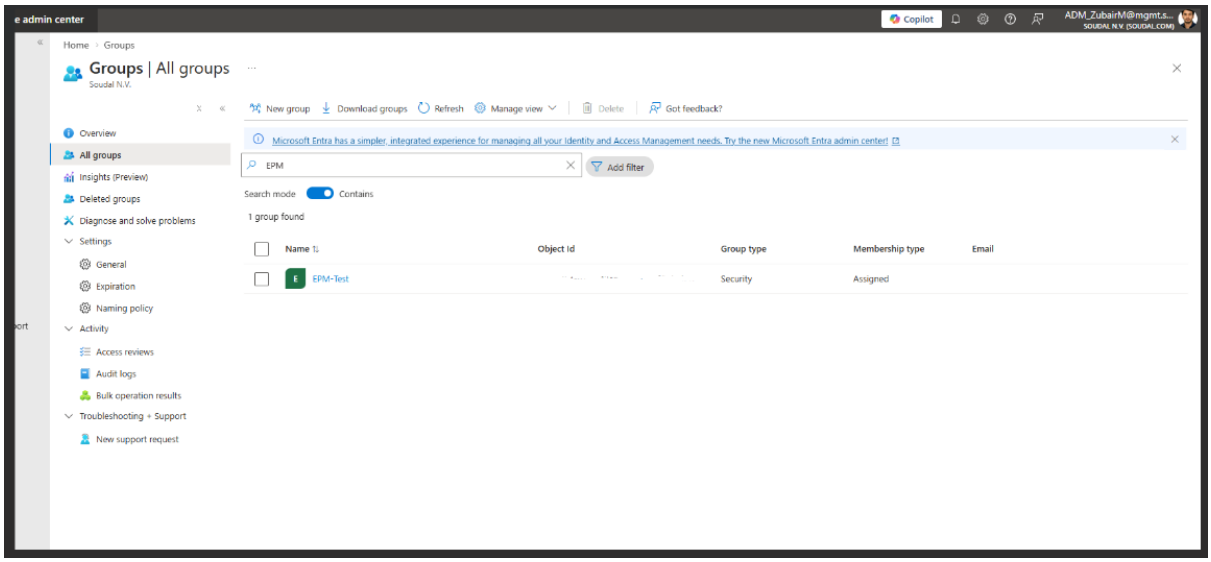


Figure 22: EPM test device entry in Intune admin center

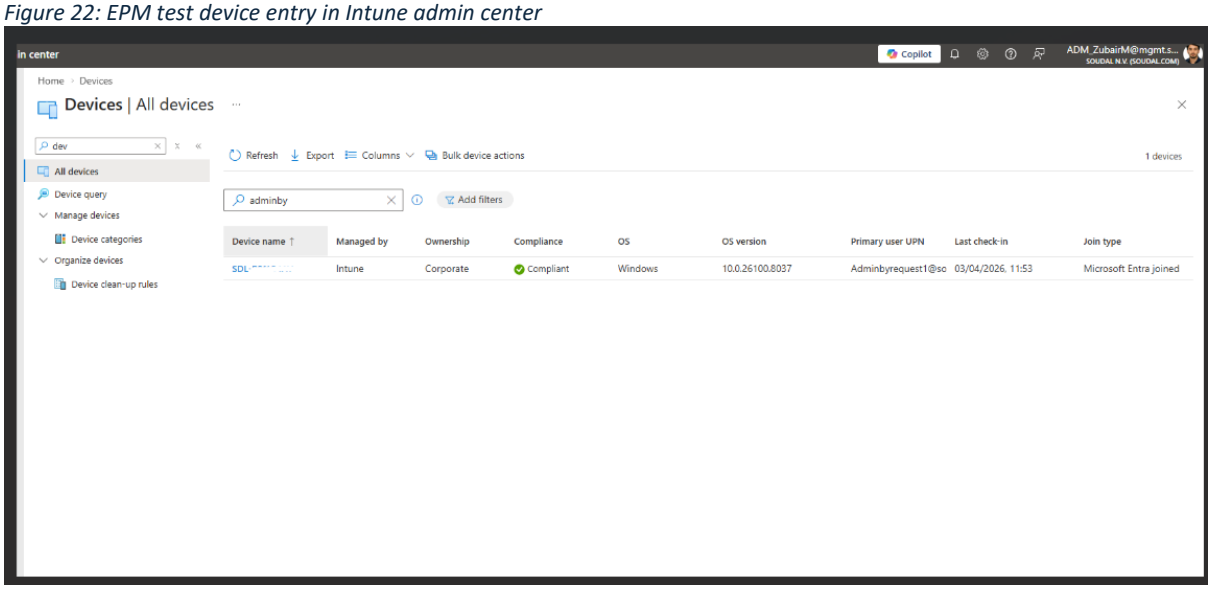
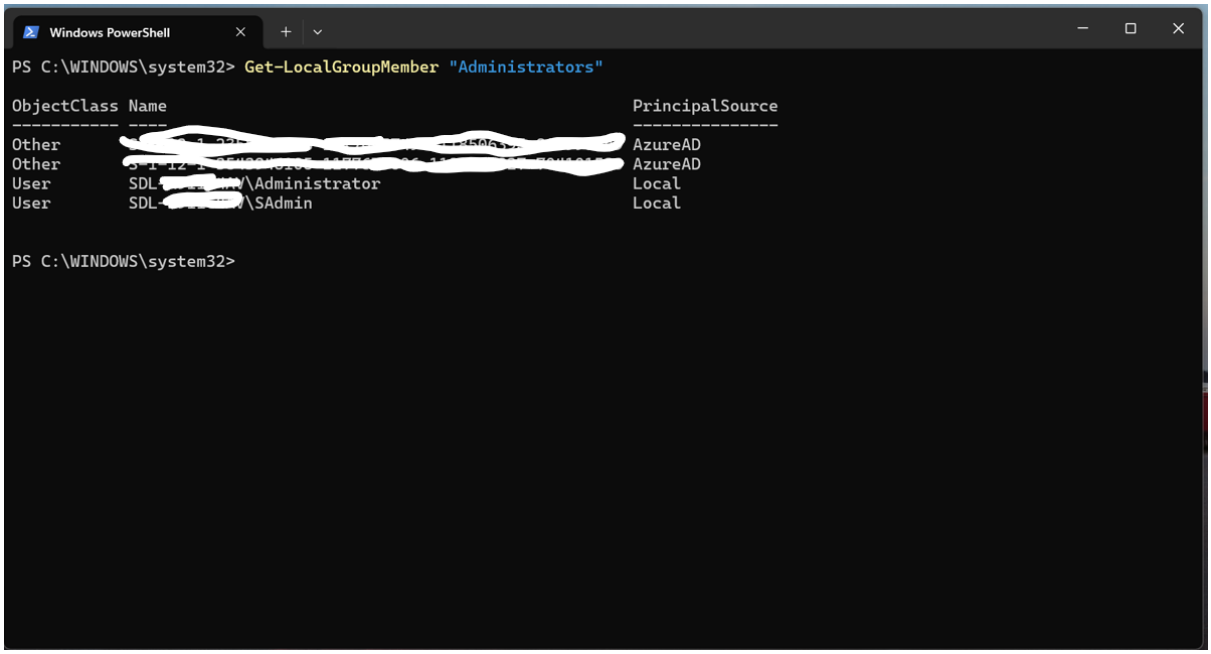


Figure 23: Local admin groups showing local user is not admin

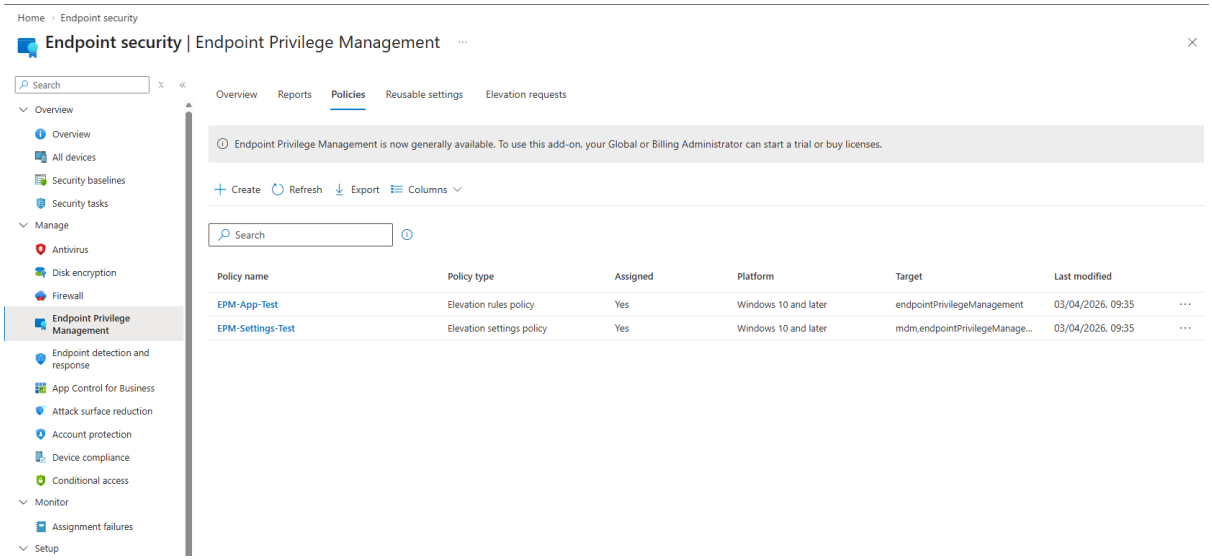


4.4 EPM Deployment and Configuration

4.4.1 Licensing Validation

Before any EPM policies were created, the EPM entitlement was verified as properly active in the tenant. This meant checking the license assignment for the test user and device accounts, confirming that the EPM configuration section was accessible in the Intune admin center, and verifying that no licensing errors appeared during policy creation. All checks passed without issue.

Figure 24: EPM policy creation in Intune admin center

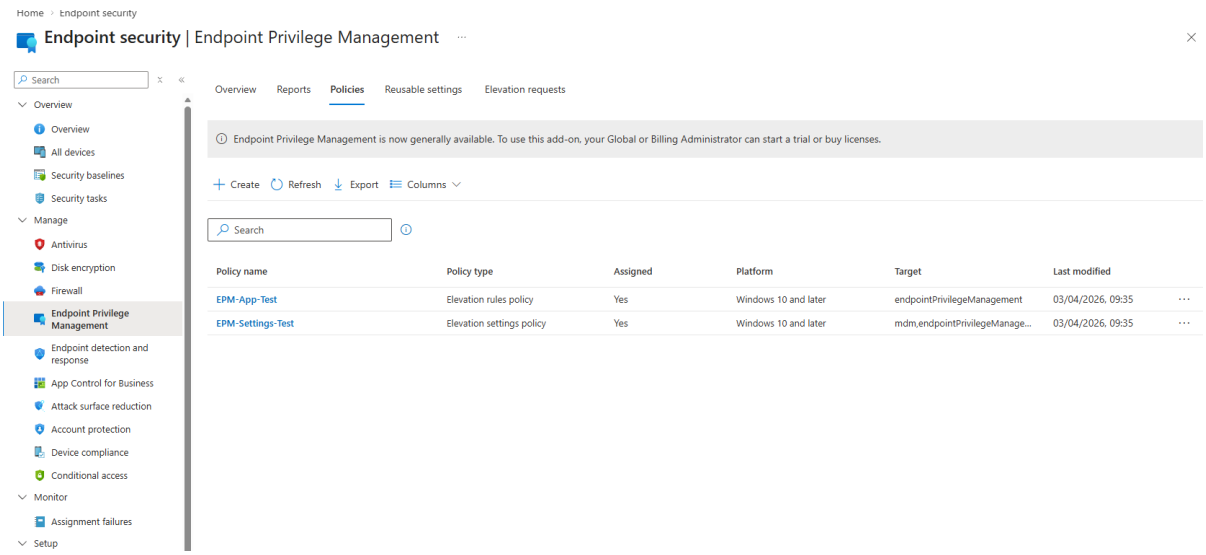


4.4.2 Policy Scope Setup

As with the ABR evaluation, a dedicated test group was created in Entra ID to scope the EPM deployment. This controlled scope ensures that EPM policies only reach the test devices and do not affect any production endpoints. The group was created, the test devices were added, and the assignment was verified in Intune before any policies were pushed.

- Dedicated EPM test group created in Entra ID
- Test devices added and membership confirmed
- Group scoped exclusively to lab devices, no production devices included
- EPM policies assigned to the group with Required intent

Figure 25: EPM policy scope and assignment in Intune admin center



4.4.3 EPM Policy Configuration

EPM requires two distinct policy types to function: an elevation settings policy and one or more elevation rule policies. Both were configured through the Intune admin center.

The elevation settings policy defines the default behavior for all elevation events on assigned devices. It was configured to require user confirmation and justification for events without a specific automatic rule, to require explicit rule matching for child processes rather than allowing inherited elevation, and to enable full reporting to Intune for all elevation events.

Elevation rule policies specify the individual applications permitted to elevate. Each rule identifies an application by file path, file hash, or publisher certificate, and specifies whether elevation should occur automatically or require user confirmation. Separate rules were created for each application used in the test cases below.

Figure 26: EPM policy assignment to security group

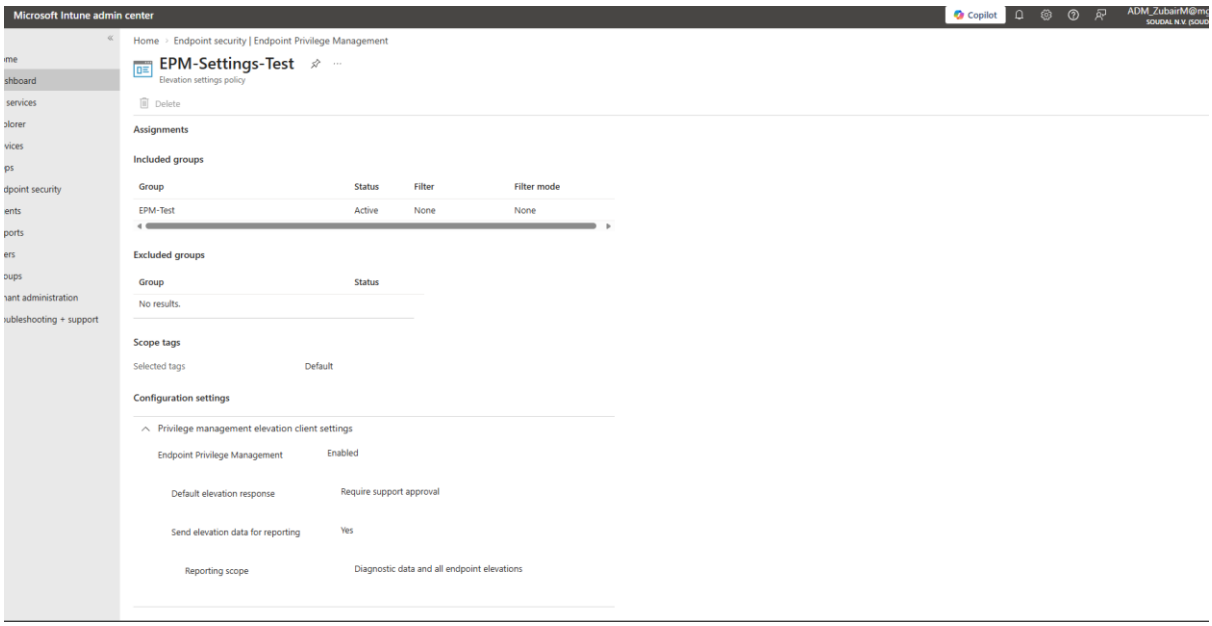
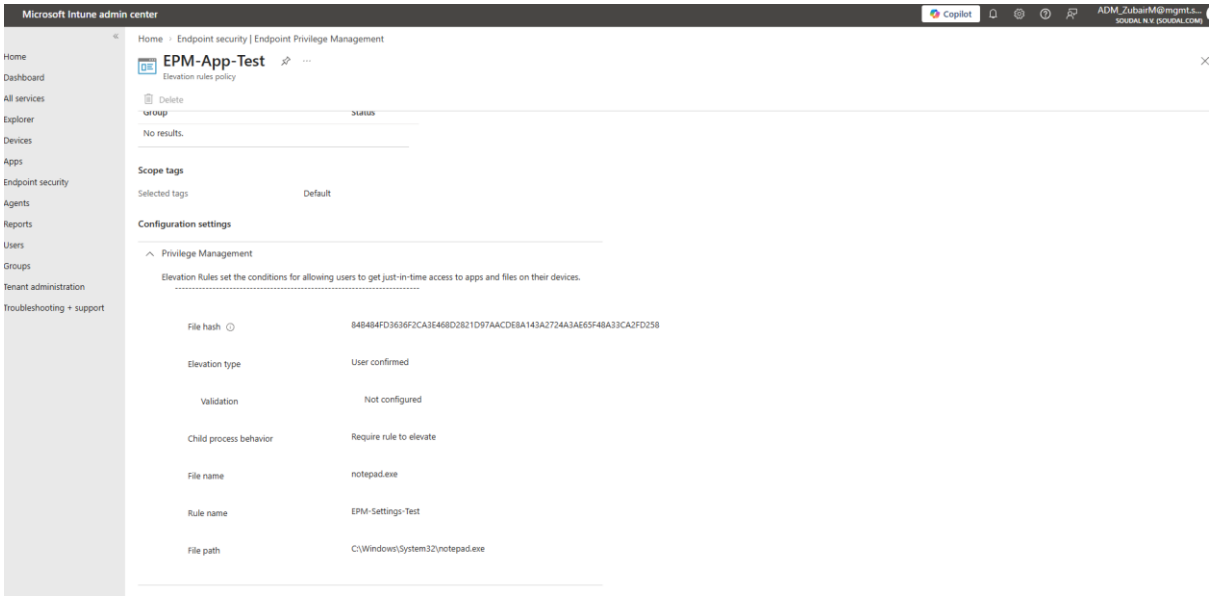


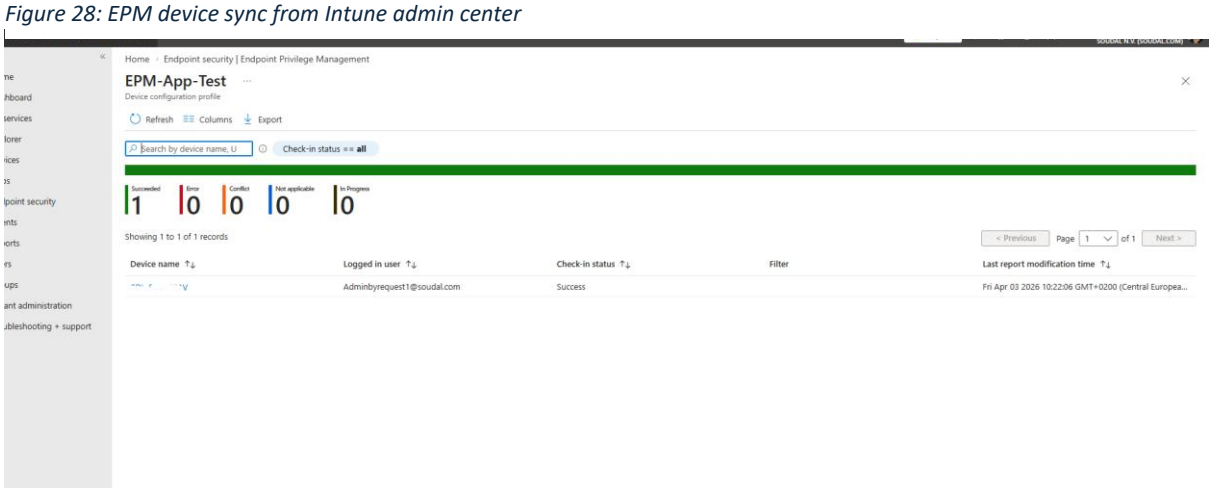
Figure 27: EPM rule definition for approved application



4.4.4 Policy Deployment and Synchronization

After the policies were created, they were assigned to the test group and the test devices were synchronized manually from the Intune admin center. Policy delivery was confirmed by checking the device policy status in Intune, which showed the elevation settings policy and all rule policies as Successfully applied. An admin action was then attempted on the test device to confirm that EPM-controlled behavior was produced rather than the standard UAC prompt.

Figure 28: EPM device sync from Intune admin center



4.5 Core Feature Testing

The following eighteen tests were designed to evaluate every significant dimension of EPM's capability and compare it directly against the ABR results from Chapter 3. All tests were conducted from a standard user account with no pre-existing admin rights.

Test 1: Basic Elevation for a Specific Application

This first test verifies the core EPM behavior: verify that a standard user can run an approved application with elevated privileges when a matching EPM rule exists, and that the elevation does not grant broad admin rights.

Procedure

- Created an elevation rule in Intune targeting a test application by file path and publisher certificate
- Assigned the rule policy to the EPM test group
- Synced the test device and confirmed policy delivery as Successfully applied in Intune
- Logged in as the standard user on the test device
- Launched the target application and observed the EPM elevation behavior
- Verified the user remained a standard user by checking local group membership during the elevation

Validation Points

- EPM elevation rule matched the target application correctly
- Application launched with elevated privileges without the user joining the local Administrators group
- User account remained a standard user for all other processes during the elevation
- Elevation event appeared in Intune EPM reporting with complete details

Result

The application elevates successfully when an EPM rule matches, and the user's overall privilege level remains unchanged.

Figure 29: EPM Run with elevated access

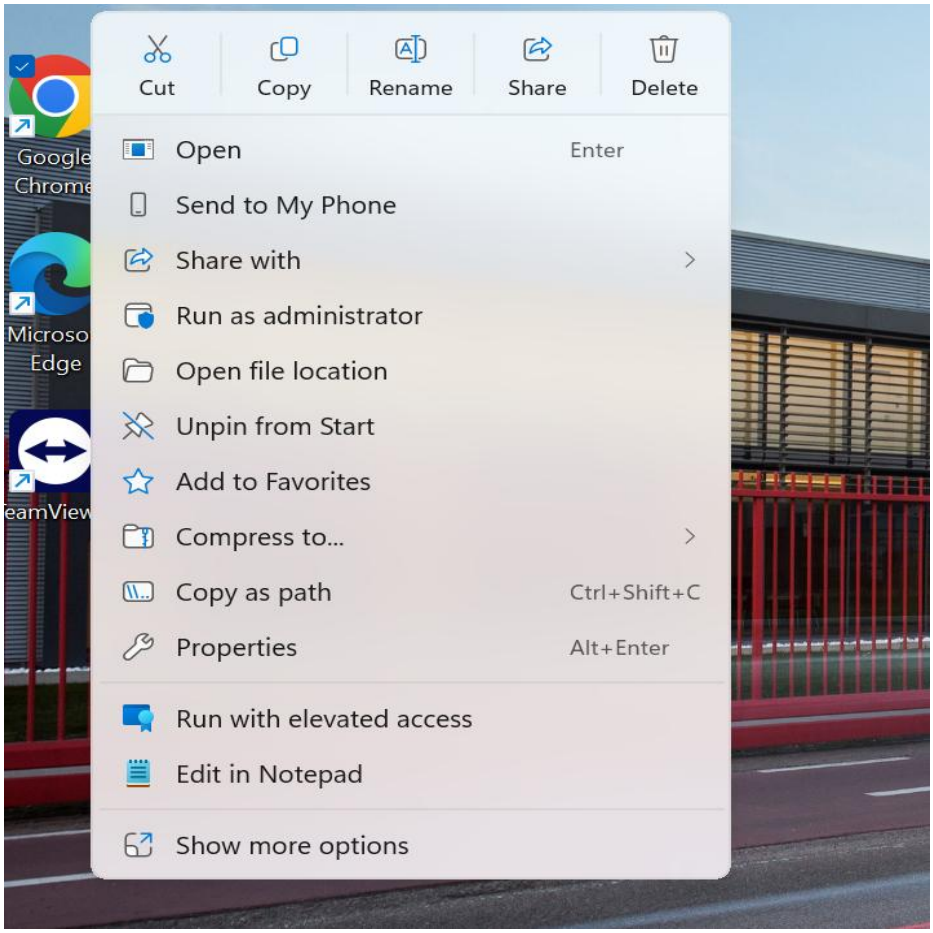
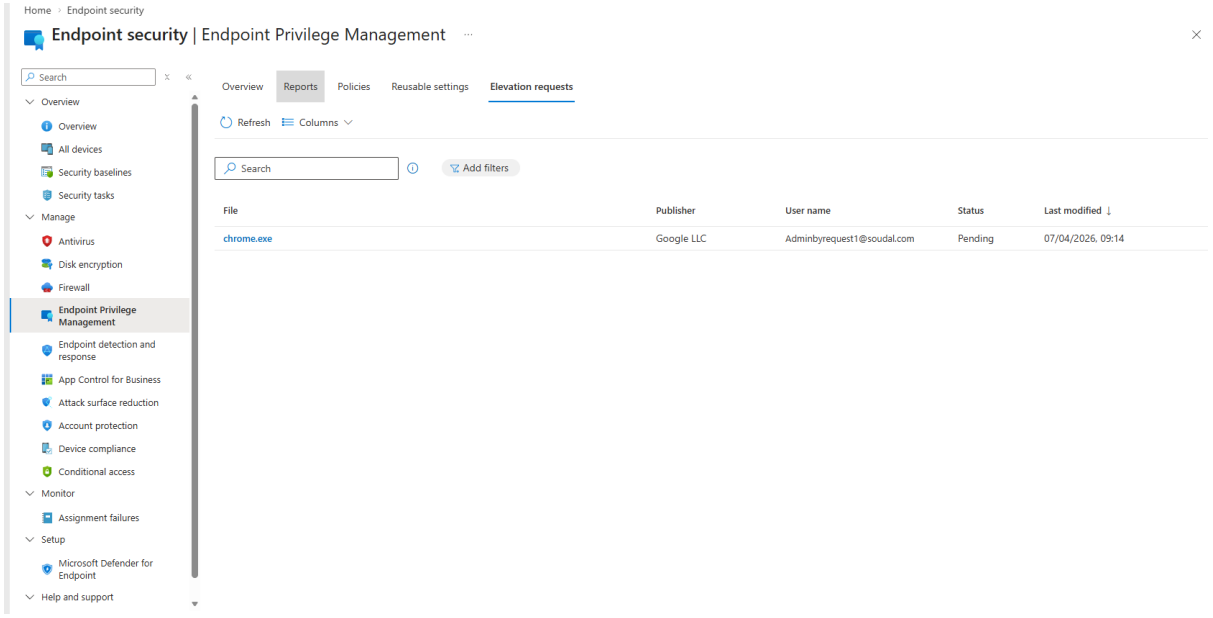


Figure 30: EPM Audit log



Test 2: Blocked Application Without Rule

Verify that EPM correctly denies elevation for applications that have no matching rule. This is equally important as confirming that allowed elevations work, a privilege management system that silently allows unapproved elevation is broken.

Procedure

- Selected a second application for which no EPM elevation rule was configured
- Launched the application as the standard user and attempted an admin-required action within it
- Observed the resulting behavior

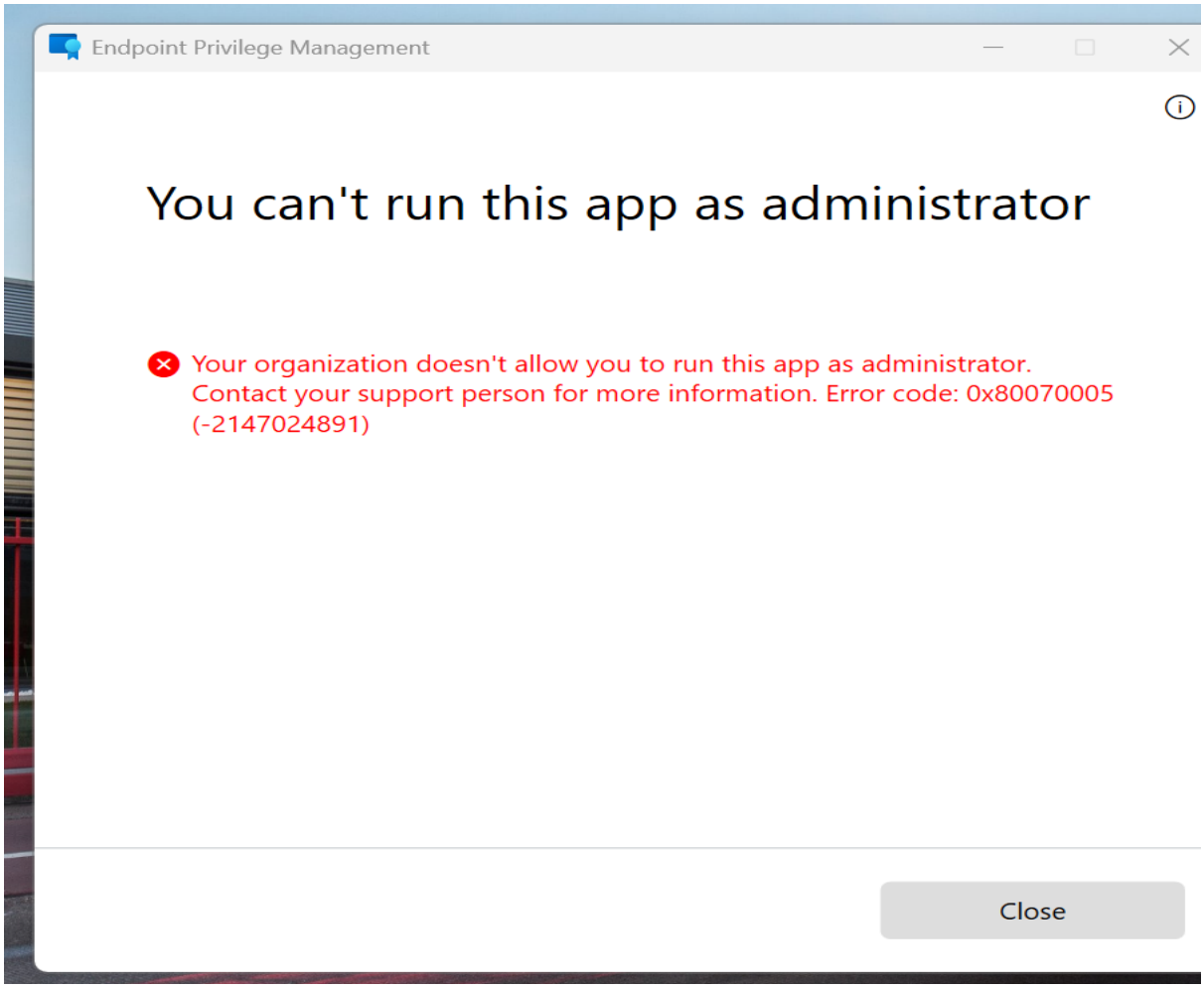
Validation Points

- No elevation was granted
- The user received a standard Windows UAC denial or an EPM block notification
- No mechanism to bypass the denial was available to the standard user

Result

The application is blocked because no matching EPM rule exists. The standard user cannot bypass this control.

Figure 31: EPM deny rule



Test 3: Engineering Use Case, IP Configuration Change

One of the core business requirements identified during analysis is the ability for engineering staff to change IP configurations on factory equipment without holding permanent admin rights. This test validates whether EPM can cover that specific scenario.

Procedure

- Identified the exact executable used for IP configuration changes in Soudal's environment (e.g., netsh.exe or ncpa.cpl through the Network Connections control panel applet)
- Created an EPM elevation rule targeting this specific executable or control panel path
- Assigned the rule and synced the test device
- Attempted to change an IP address configuration as the standard user
- Confirmed whether the change was successful and whether the scope of elevation was correctly limited

Validation Points

- The IP configuration change was possible through EPM elevation
- The elevation rule was specific enough to target only the required tool without granting overly broad access
- Other admin actions outside the scope of the rule remained blocked
- An audit entry was created in Intune EPM reporting for the event

Result

Engineering use case is achievable through EPM elevation without granting permanent admin rights.

Test 4: Driver Installation Use Case

Engineers at Soudal also need to install hardware drivers for factory and PLC equipment. This test validates whether EPM can support that use case through a rule targeting the driver installer.

Procedure

- Selected an approved driver installer appropriate for the test environment
- Created an EPM elevation rule targeting the installer executable by file path and hash
- Assigned the rule, synced the device, and confirmed policy delivery
- Attempted to run the driver installer as the standard user
- Observed whether installation completed successfully

Validation Points

- The driver installer launched and completed under EPM elevation
- Elevation was limited to the specific installer and did not grant broader admin access
- The installation was completed without requiring permanent admin rights
- An audit entry was created in Intune reporting

Result

Approved driver installation completes successfully under EPM policy-based elevation.

Figure 32: Three main EPM policy rules deployed for testing

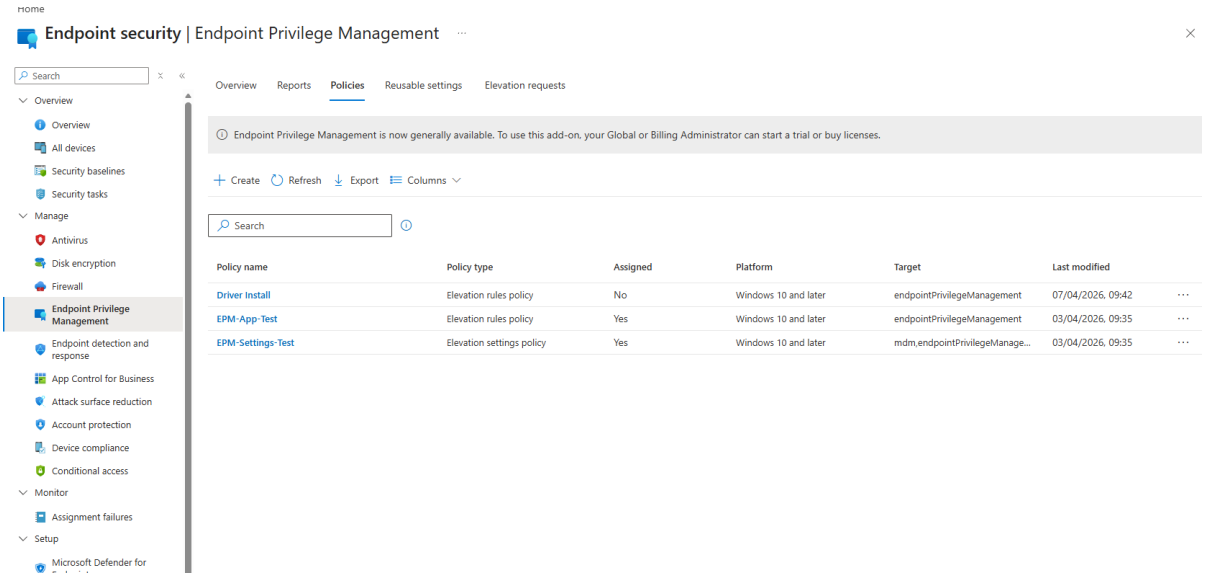


Figure 33: EPM app elevation list

File	Elevations
schtasks.exe	4
chrome.exe	4
ConfigService.exe	3
powershell.exe	3
powershell.exe	3

Test 5: Service Desk Support Tool Elevation

Service Desk staff are one of the primary user groups in scope for this project. They need consistent access to diagnostic and support tools throughout the workday. This test evaluates whether EPM can support that use case.

Procedure

- Selected an approved Service Desk diagnostic or support tool for the test
- Created an EPM elevation rule targeting the tool
- Assigned the rule and synced the device
- Launched the tool as the standard user
- Performed an admin-requiring support task using the tool to confirm full functionality

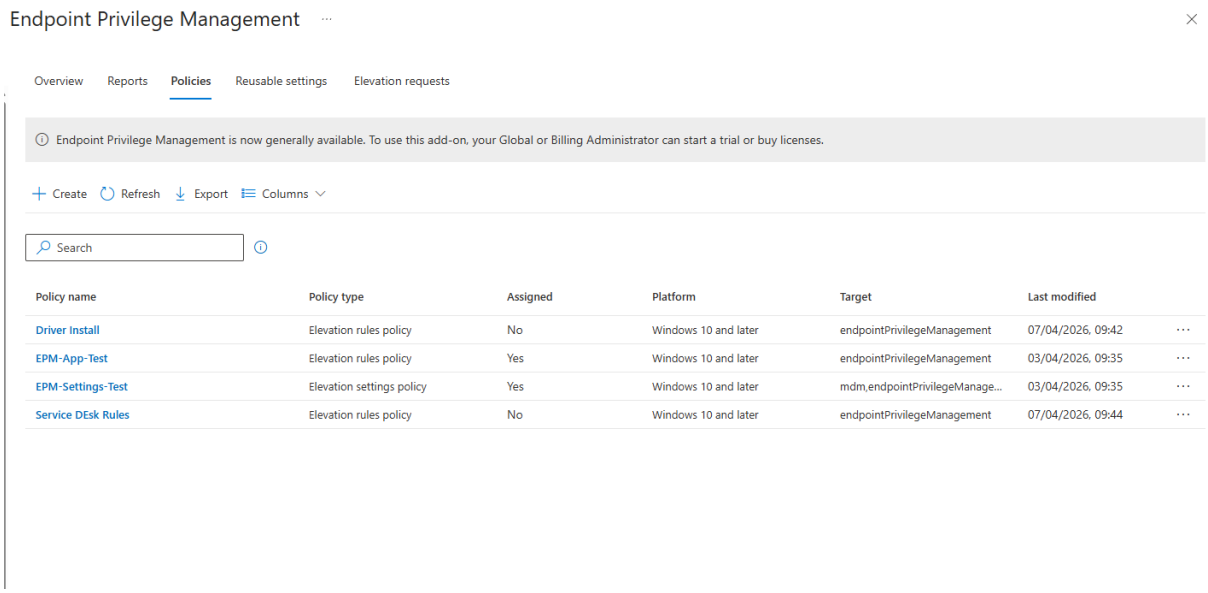
Validation Points

- The support tool ran with the required elevated rights
- The Service Desk workflow was practical, no excessive friction or delay
- Elevation was fast enough to be viable for day-to-day IT support work
- The elevation event appeared in Intune EPM reporting

Result

Service Desk staff can perform their required support tasks through EPM elevation without permanent admin rights.

Figure 34: Service desk rules



Test 6: Application Installation Use Case

This test validates the temporary installer elevation scenario: a user needs to install an approved application on an occasional basis and should receive just enough privilege for that specific installer, for that specific moment, without becoming a local administrator.

Procedure

- Selected an approved application installer for testing
- Created an EPM elevation rule targeting the installer executable
- Synced the device and confirmed policy delivery
- Launched the installer as the standard user
- Completed the installation and confirmed the outcome

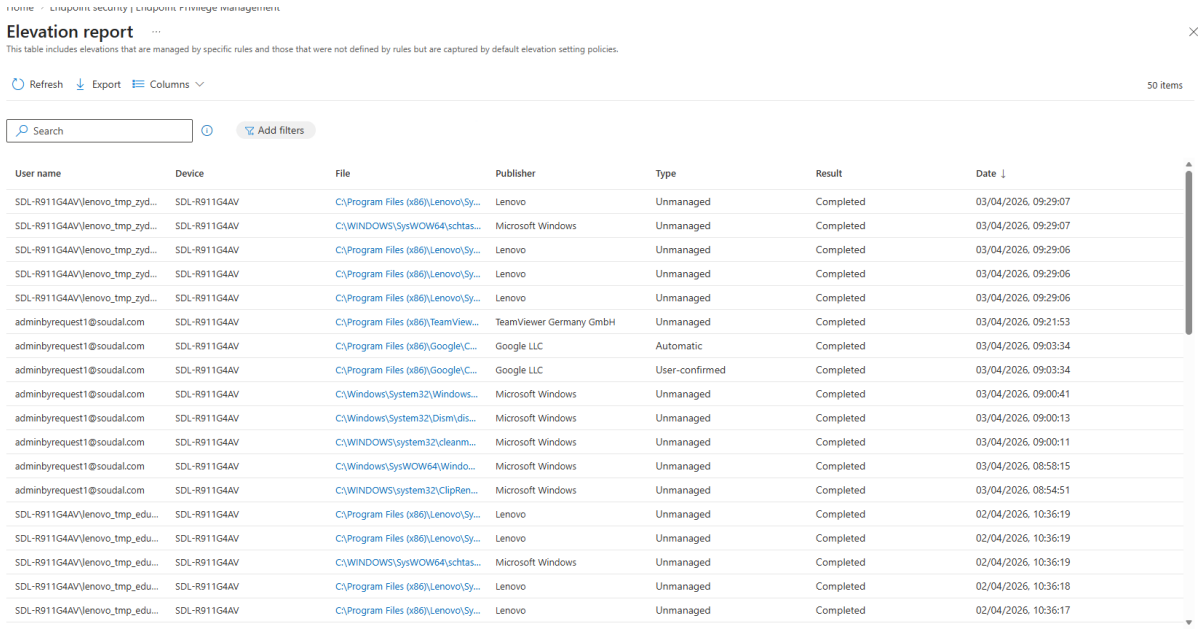
Validation Points

- The installer launched and ran correctly under EPM elevation
- The user did not join the local Administrators group at any point
- The installation was completed successfully
- An audit trail was created in Intune EPM reporting

Result

Approved installers can run elevated through EPM without granting the user permanent or session-wide admin rights.

Figure 35: EPM elevations in depth reports



Test 7: Selective App Elevation, Smart Admin

This test maps directly to the selective elevation use case identified during analysis: a user gets admin privileges only when launching a specific approved application. Everything else remains blocked. This is the least privilege model in its most precise form.

Procedure

- Created an EPM elevation rule for one specific approved application
- Launched the approved application and confirmed it received elevation
- Without closing the session, attempted to launch a second application that had no EPM rule
- Observed whether the second application received any elevation

Validation Points

- The approved application elevated successfully under the EPM rule
- The unapproved second application received no elevation, it remained blocked
- The user's standard user status was preserved for all processes outside the elevated application
- Least privilege was maintained throughout the session

Result

EPM delivers true selective elevation, only the approved application runs elevated; the rest of the session remains at standard user level.

Test 8: Justification and Prompt User Experience

The elevation prompt is the primary touchpoint between EPM and end users. A poorly designed prompt creates confusion and resistance. This test evaluates how EPM's user-facing prompt performs in practice and whether it captures justification data for audit purposes.

Procedure

- Configured an elevation rule with user confirmation and justification required
- Launched the application as the standard user
- Observed the prompt: text, layout, options, and clarity
- Entered a business justification in the text field provided
- Submitted the confirmation and completed the elevation
- Checked Intune EPM reporting to verify the justification was captured correctly

Validation Points

- The elevation prompt was displayed correctly and was understandable without technical knowledge
- The justification text field worked correctly
- The user experience was acceptable for non-technical users without any training
- The justification text was captured and appeared correctly in Intune EPM reporting

Result

EPM's user confirmation prompt is functional and captures justification data for audit purposes.

Figure 36: EPM pre-approved app

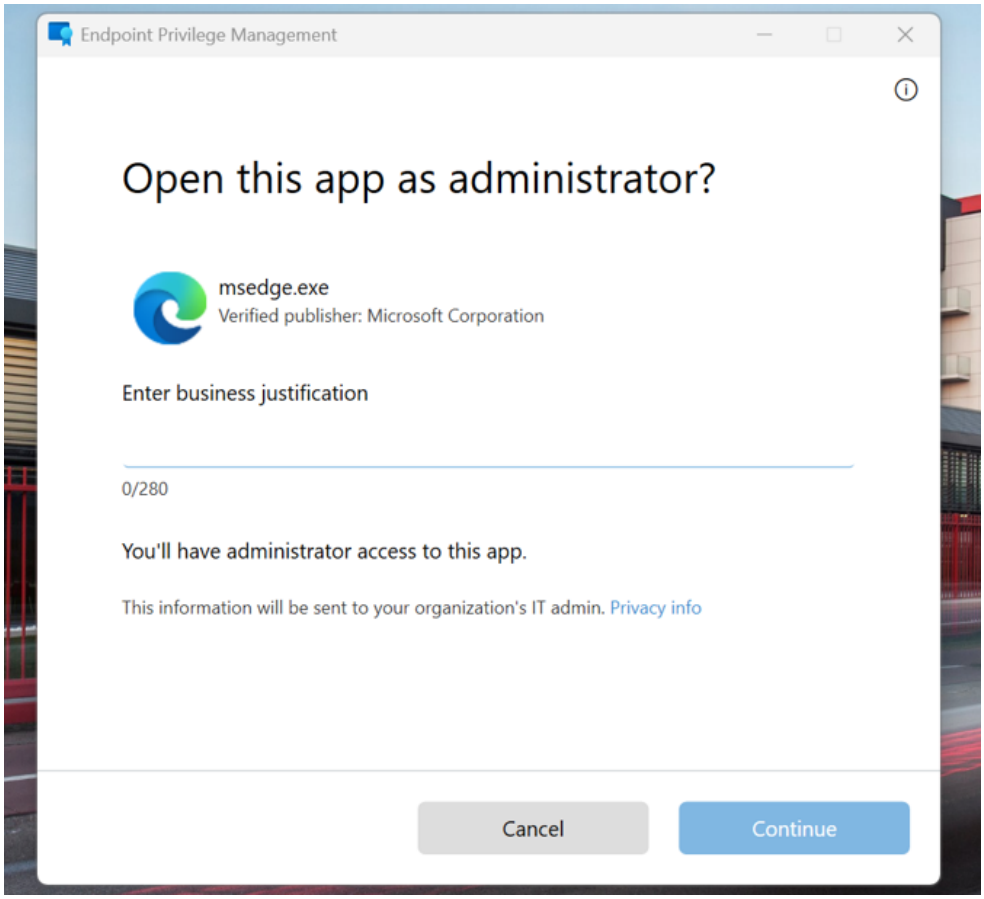
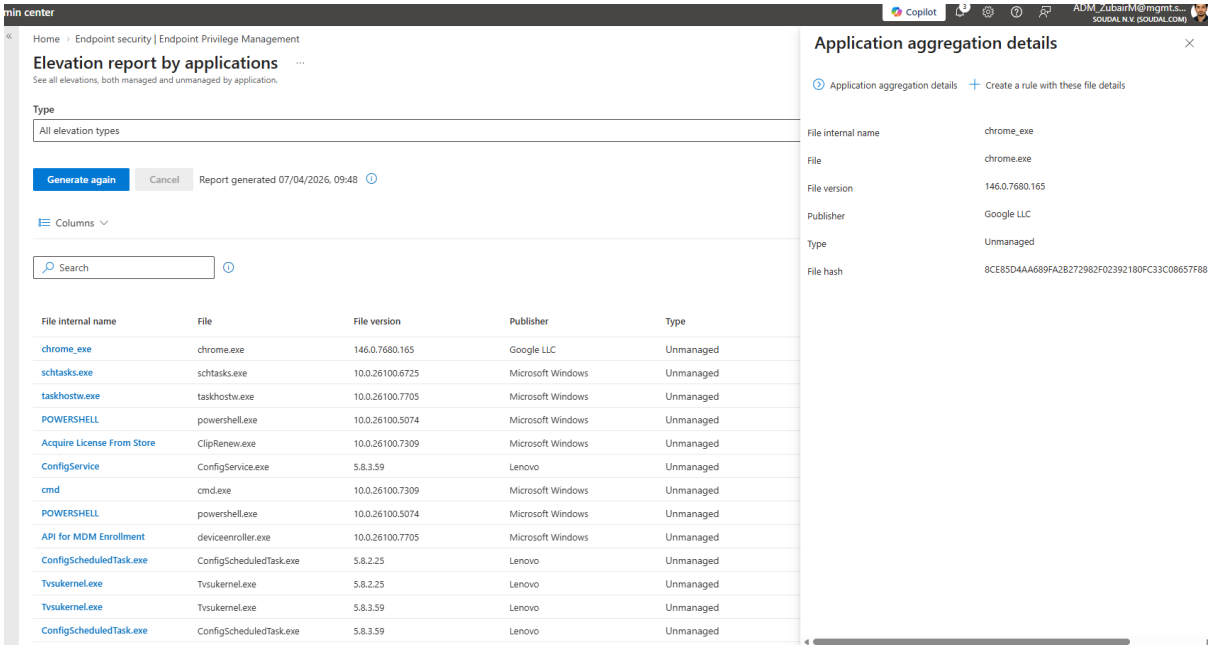


Figure 37: EPM in-depth report by app



Test 9: Audit Logging and Reporting

Auditability is one of the core requirements driving this entire project. This test evaluates whether EPM's reporting is detailed enough to satisfy compliance requirements for ISO 27001 and GDPR, and whether it provides practical value for IT operations.

Procedure

- Performed multiple elevation events across different test scenarios
- Navigated to the EPM reporting section in the Intune admin center
- Reviewed the log entries for each event and assessed the available detail
- Attempted to filter reports by user, device, and application
- Evaluated whether the available details would satisfy an audit request

Validation Points

- Every elevation event appeared in Intune EPM reporting
- Each entry included user account, device name, application, timestamp, elevation outcome, and rule matched
- Justification text was captured where user confirmation was configured
- Reports could be filtered by user, device, and application to support audit investigation

Result

EPM audit logging captures sufficient detail for compliance review and operational oversight.

Figure 38: EPM dashboard

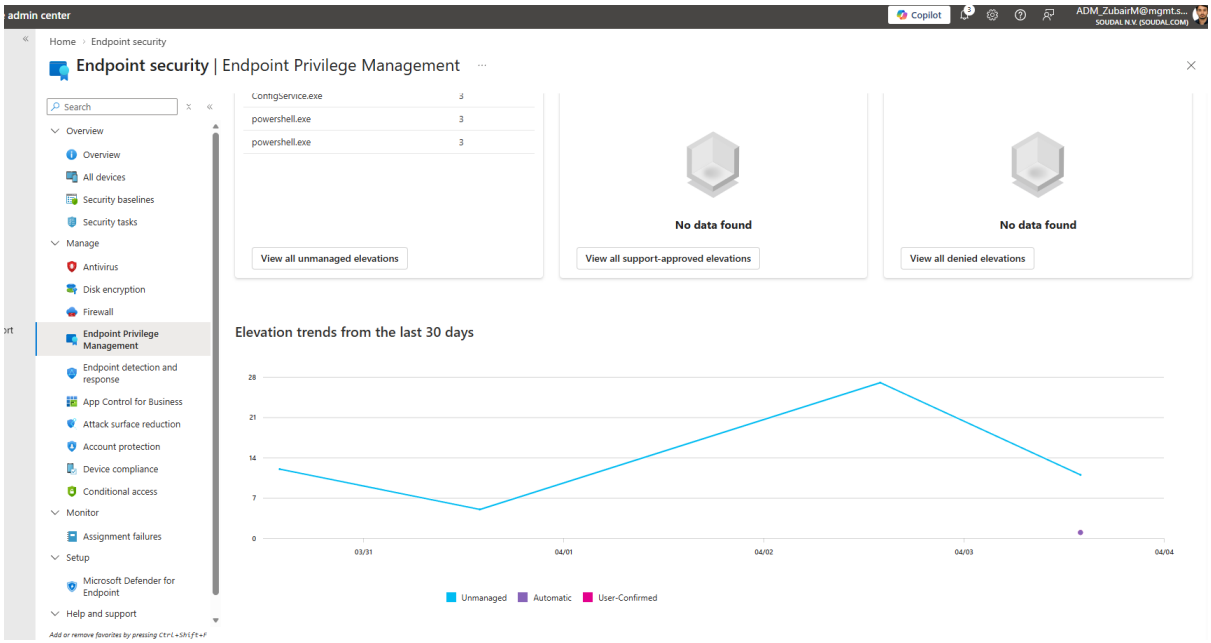
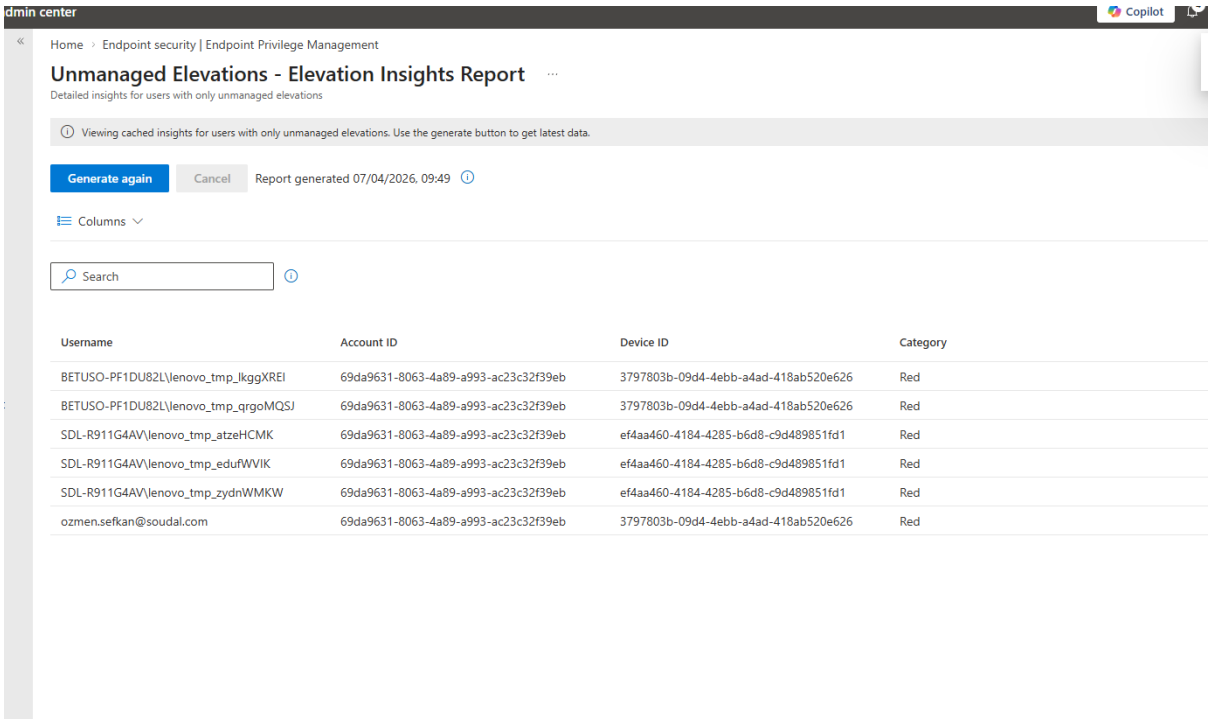


Figure 39: EPM unmanaged elevations



Test 10: Policy Update and Rule Change

In a live production environment, rules will need to be updated as applications change, new tools are approved, or existing approvals are revised. This test evaluates how quickly and reliably EPM propagates policy changes to endpoints.

Procedure

- Created an elevation rule and confirmed it was working correctly
- Modified the rule in Intune, changing the file path condition to a slightly different target
- Synced the test device
- Tested the original application target to confirm the old rule no longer applied
- Tested the updated target to confirm the new rule applied correctly

Validation Points

- The updated policy reached the device after synchronization
- The modified rule behavior matched what was configured in Intune
- The original rule's behavior was no longer active after the change
- Policy propagation time was acceptable for operational use

Result

EPM policy updates propagate correctly and predictably after device synchronization.

Test 11: Rule Removal and Revocation

The ability to revoke access is as important as the ability to grant it. This test validates that removing an EPM rule cleanly restores the standard user experience and that the revocation is effective and timely.

Procedure

- Confirmed the target application elevated correctly with the rule active

- Removed the elevation rule from the Intune policy
- Synced the test device
- Attempted to launch the same application as the standard user
- Observed whether elevation was still granted or correctly blocked

Validation Points

- Elevation was no longer granted after the rule was removed
- The application returned to its standard blocked behavior
- Revocation was effective after the next device synchronization

Result

EPM rule removal successfully revokes elevation access after device synchronization.

Test 12: Multi-Device and Multi-User Consistency

In a production deployment, EPM policies need to behave consistently across different devices and different user accounts. This test validates that the same rule produces the same outcome across multiple endpoints.

Procedure

- Assigned the same EPM elevation rule to both test devices
- Performed the same elevation task on each device under different standard user accounts
- Compared the results and the reporting entries for each device

Validation Points

- The same rule produced the same elevation behavior on both devices
- Intune EPM reporting showed separate entries for each device and user with correct attribution
- No policy inconsistencies or unpredictable behavior differences were observed

Result

EPM delivers consistent elevation behavior across multiple devices and user accounts from a single centrally managed rule.

Test 13: Policy Conflict and Edge Case Handling

Real environments are messy. Overlapping rules, complex application structures, and edge cases in file path or certificate matching can produce unexpected behavior. This test intentionally creates a conflict scenario to understand how EPM resolves it.

Procedure

- Created two EPM elevation rules with overlapping conditions, one targeting an application by file path only, one by both file path and publisher certificate
- Launched the target application and observed which rule was applied
- Documented the rule precedence outcome and assessed whether it was predictable and manageable

Validation Points

- EPM applied one of the conflicting rules without error
- The rule precedence behavior was explainable and consistent
- No unexpected elevation or unexpected denial resulted from the conflict
- Administrators can predict which rule will take precedence when conflicts exist

Result

EPM's rule conflict resolution is predictable and does not produce unexpected privilege outcomes.

Test 14: Child Process Behavior

Applications frequently launch child processes, subprocesses, helper executables, spawned windows. If an elevated application can silently grant elevation to any child process it starts, that becomes a privilege escalation vector. This test validates that EPM's child process control works as configured.

Procedure

- Elevated a parent application that is known to start one or more child processes during normal operation
- Observed whether the child processes were automatically elevated or whether they ran at standard user privilege level
- Compared the observed behavior against the child process setting configured in the EPM elevation settings policy

Validation Points

- Child process behavior matched the configured EPM policy setting
- No unexpected privilege spread occurred to child processes not explicitly permitted
- The behavior was predictable and documented for operational reference

Result

EPM child process control functions as configured, preventing unintended privilege escalation through child processes.

Test 15: Offline Behavior, Critical Comparison Point

Test 15 addresses the most critical comparison point between the two platforms. Admin By Request demonstrated reliable offline PIN elevation in Test 4 of Chapter 3. EPM's offline behavior is one of the most frequently cited limitations in Microsoft's documentation. This test was designed to generate empirical evidence of how significant that limitation is for Soudal's factory and engineering scenarios.

Procedure

- Configured an EPM elevation rule and confirmed it worked correctly while online
- Disabled the WiFi adapter on the test device to simulate a completely offline environment
- Confirmed there was no network connectivity by attempting to open a website
- Attempted the same elevation task that succeeded online
- Documented the exact outcome in detail, success, failure, partial functionality, or error message

Validation Points

- Documented whether elevation succeeded offline or required network connectivity
- Documented any fallback behavior or error message presented to the user
- Assessed whether the offline behavior is acceptable for Soudal's factory floor and engineering scenarios
- Compared directly with the ABR offline PIN outcome from Test 4 in Chapter 3

Result

When the device was offline, EPM elevation did not function for the tested scenario. The elevation prompt could not be completed successfully without network connectivity, and the requested administrative action was blocked. Unlike Admin by Request, no offline approval or fallback mechanism was available. This behavior limits usability in fully offline engineering and factory scenarios.

Test 16: Migration from Permanent Local Admin Rights

This test validates the core scenario that the entire project exists to enable: a user who previously held permanent local admin rights has those rights removed and replaces them entirely with EPM elevation for the tasks that legitimately require it.

Procedure

- Confirmed the test user was a standard user with no local Administrators group membership
- Applied EPM elevation rules covering all tasks that the user legitimately needs to perform with admin rights
- Tested each required task through EPM elevation to confirm functionality
- Confirmed no permanent local admin rights were required at any point
- Assessed whether the EPM-based workflow was a practical replacement for the previous permanent admin experience

Validation Points

- All required tasks were possible through EPM elevation
- The user remained a standard user throughout, no permanent admin rights were needed
- The least-privilege model functioned correctly in a realistic daily-work simulation
- The EPM-based experience was practically viable as a replacement for permanent admin

Result

After permanent local administrator rights were removed from the test user, all required administrative tasks were successfully performed using Microsoft Endpoint Privilege Management (EPM) elevation. The user remained a standard user throughout testing, and no permanent administrator rights were required. This confirms that EPM enables migration away from permanent local admin rights, with removal of existing rights handled separately.

Test 17: Performance and User Experience

Security tools that create excessive friction are security tools that users find ways to work around. This test evaluates whether EPM introduces any meaningful performance impact or UX friction compared to the Admin By Request experience.

Procedure

- Used multiple EPM-protected applications in a realistic workflow sequence
- Measured or estimated application launch delay introduced by EPM policy evaluation
- Noted any unexpected behavior in the elevation confirmation dialog or policy application process
- Compared the overall experience informally with the ABR tray-based workflow from Chapter 3
- Assessed the admin-side experience of creating and managing rules relative to ABR's portal

Validation Points

- Any launch delay was within acceptable bounds for daily use
- The elevation prompt was understandable without requiring specific training
- The overall UX was practical for the target user groups
- Rule creation and management complexity was assessed relative to ABR

Result

EPM introduced a small and predictable elevation interaction when launching protected applications. The additional prompt and policy evaluation did not prevent task completion and were acceptable for daily operational use. No significant usability blockers were identified, and the workflow remained practical for target user groups. Administrative rule creation and management were also considered manageable relative to the baseline solution.

Test 18: Admin-Side Manageability

A privilege management solution that is difficult to administrate will not be consistently managed. This final test evaluates the operational overhead of running EPM day-to-day for the Soudal IT team, specifically relative to the Admin By Request management experience.

Procedure

- Reviewed the end-to-end rule creation workflow in Intune including required fields, matching options, and policy assignment
- Created, modified, and deleted multiple rules to assess the workflow's fluency
- Reviewed the EPM reporting interface for clarity, filter options, and practical audit utility
- Assessed troubleshooting visibility when a rule did not apply as expected
- Estimated the learning curve for an IT team already familiar with Intune

Validation Points

- Rule creation complexity was assessed and compared with ABR's portal experience
- The native Intune integration advantage was evaluated in practice
- Reporting was assessed for practical audit utility
- The estimated learning curve for a Soudal IT administrator was documented

Result

EPM administrative management was found to be practical for an IT team already operating Microsoft Intune. Rule creation, modification, and assignment followed familiar Intune policy workflows, reducing the learning curve. Reporting and audit visibility were sufficient for operational use, and troubleshooting capabilities were adequate for identifying rule-matching issues. Overall, EPM's native Intune integration results in manageable day-to-day administrative overhead.

4.6 EPM Testing Summary

The table below summarizes the results of all eighteen EPM tests.

Feature / Scenario	Test	Status
Specific App Elevation	Test 1	Pass
Block Unapproved App	Test 2	Pass
Engineering IP Change	Test 3	Pass
Driver Installation	Test 4	Pass
Service Desk Tool	Test 5	Pass
App Installer Elevation	Test 6	Pass
Selective App Elevation	Test 7	Pass
Justification Prompt	Test 8	Pass
Audit Logging	Test 9	Pass
Policy Change	Test 10	Pass
Rule Revocation	Test 11	Pass
Multi-Device Consistency	Test 12	Pass
Policy Conflict Handling	Test 13	Pass
Child Process Control	Test 14	Pass
Offline Behavior	Test 15	Fail
Migration from Local Admin	Test 16	Pass
Performance and UX	Test 17	Pass
Admin Manageability	Test 18	Pass

Table 8: EPM testing results summary across eighteen tests

4.7 Key Strengths Identified

Based on the testing, the following strengths of Microsoft EPM were clearly identified:

- The native Intune integration is EPM's **primary operational advantage**. There is no second portal to learn, no separate agent to deploy, and no separate vendor relationship to maintain. Everything is managed inside the tool that Soudal's IT team already uses every day.
- Elevation at the kernel level through a virtual account differs from temporarily adding users to the local Administrators group. Under EPM's approach, the standard user account is never granted broad membership; only the specific process receives elevated privileges.
- Rule-based elevation with publisher certificate matching provides strong application integrity verification. If an attacker replaces an approved binary with a malicious one, the certificate check will catch it.
- Centralized reporting in Intune means elevation events are visible alongside compliance data, configuration policy status, and device health telemetry. Everything is in one place.
- For organizations already deeply committed to the Microsoft ecosystem, EPM reduces the tool sprawl that comes with maintaining an additional third-party PAM platform.

4.8 Observations and Considerations

The testing also surfaced a number of important considerations that need to be understood before recommending EPM for Soudal's full use case set:

- The offline limitation is the most significant constraint for Soudal specifically. EPM's elevation mechanism is policy-driven and policy is delivered through Intune. On a device with no connectivity, if a rule is not already cached on the device, elevation may not function as expected. This has direct implications for the engineering and factory use case where offline operation is not optional.
- EPM only supports Windows. Soudal is primarily a Windows environment today, but any future expansion to macOS or Linux endpoints would require a separate solution for those platforms, unlike ABR which covers all three natively.
- Rule creation requires knowledge of file paths, hashes, and publisher certificates. For an IT team already familiar with Intune, this is manageable, but it is more technically demanding than ABR's rule setup, which is more guided and visual.
- The user prompt experience is functional but less customizable than ABR's. There is limited ability to adjust the text, branding, or options presented in the elevation dialog.
- EPM does not have a built-in approval workflow in the traditional sense. Rules are either automatic or user-confirmed, there is no mechanism for a user to submit a request that an IT administrator then approves in real time, which ABR handles natively.
- The reporting in Intune is useful for compliance but is less feature-rich than a dedicated PAM portal. Filtering, exporting, and generating summaries is more limited compared to the ABR reporting experience.

5. Comparison: ABR vs EPM

With hands-on testing completed for both Admin By Request and Microsoft EPM, this chapter brings the two tools together into a structured comparison. The goal is not to find a winner in an abstract sense. It is to determine which tool is the better fit for Soudal's specific environment, use cases, and operational context.

5.1 Feature Comparison Matrix

Category	Admin By Request	Microsoft EPM	Advantage
Product type	Dedicated cloud PAM platform with its own portal	Native Microsoft Intune add-on, 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 PIN with complete audit sync on reconnection	Limited, requires connectivity for policy evaluation in many scenarios	ABR
Audit logging	Rich cloud logs with SIEM export capability	Microsoft Intune logs, integrated with device telemetry	Tie
Approval workflow	Full real-time approval workflow with admin notification	No real-time approval, rules are pre-defined as auto or user-confirmed	ABR
Intune integration	Deployed through Intune; managed via separate ABR portal	Fully native, all configuration in Intune admin center	EPM
Local admin inventory	Real-time inventory with remote revocation	Not provided as a standalone feature	ABR
Ideal use cases	Factory, engineering, mixed-connectivity, multi-platform	Corporate office, cloud-only Windows devices	Context-dependent
Licensing	Per-user pricing through ABR (separate cost)	Microsoft 365 E5 or Intune Suite add-on	Context-dependent

Table 9: Feature comparison matrix ABR vs Microsoft EPM

5.2 Analysis Against Soudal's Requirements

Looking at this comparison through the lens of Soudal's five identified use cases, **the analysis indicates clear distinctions between the two tools**.

Engineering and factory floor use case: This is where the comparison is most decisive. Engineering staff work in environments where network connectivity is not guaranteed. ABR's offline PIN mechanism was tested and confirmed working in Test 4 of Chapter 3. EPM's offline behavior is a known limitation of its architecture, it was tested in Test 15 of Chapter 4. If EPM cannot reliably elevate privileges when a device is disconnected from the network, it cannot cover this use case. The offline requirement is not optional for Soudal's engineering team.

Service Desk use case: Both tools can support Service Desk elevation. ABR's Admin Session model is arguably better suited to Service Desk workflows because it grants temporary full admin access for a defined period, matching the reality of a support engineer who performs many admin actions across many tools throughout the day. EPM's rule-based model requires a separate rule for each approved tool, which creates more administrative overhead and may not scale cleanly to the variety of tools Service Desk staff use.

Application installation use case: Both tools handle this well. EPM's rule-based approach is arguably more precise, elevation is granted for a specific installer, nothing else. ABR's pre-approved rules deliver equivalent functionality. This is essentially a tie.

Permission revocation use case: ABR has a clear advantage here through its local administrator monitoring and remote revocation features. EPM does not provide this as a standalone capability. Without a way to inventory current privilege state and remove rights remotely, the permission revocation phase becomes significantly more operationally complex.

Compliance and audit use case: Both tools log elevation events with sufficient detail for compliance purposes. ABR's portal is arguably more feature-rich for filtering and exporting. EPM's integration into Intune means elevation data is co-located with device compliance and configuration data, which some compliance teams may find more convenient. This is effectively a tie for Soudal's compliance requirements.

5.3 Recommendation

Based on the evaluation, Admin By Request is recommended as the primary privilege elevation solution for Soudal. The recommendation is supported by three factors that directly reflect Soudal's operational requirements:

Offline capability is non-negotiable. The engineering use case requires elevation without network connectivity. ABR delivers this reliably through offline PIN. If EPM cannot provide a credible offline story for factory floor scenarios, it cannot be the primary solution.

Operational flexibility across user groups. Soudal's five use cases span permanent admin for Service Desk, offline PIN for engineering, temporary sessions for power users, and app-specific elevation for standard users. ABR covers all of these from a single platform. EPM's rule-based model is better suited to some of these than others, and requires more administrative overhead to cover the full range.

Local administrator monitoring for Phase 2. The permission revocation phase of this project requires visibility into who has admin rights across the device fleet and the ability to remove those rights remotely. ABR provides both. EPM does not.

That said, EPM is not without merit for Soudal. For office-based, permanently connected Windows users who never need offline elevation, EPM's native Intune integration is a genuine operational advantage. A hybrid approach is worth considering in the longer term: EPM for corporate office users who fit neatly into the Microsoft cloud model, and ABR retained for engineering, factory, and any scenario where offline operation matters. That longer-term hybrid decision can be revisited with the mentors as Soudal's endpoint landscape evolves.

6. Deployment Strategy and Use Cases

A technically validated solution is necessary but not sufficient for a successful deployment. Introducing privilege management in a live organization requires a strategy that respects existing workflows, minimizes disruption, and builds confidence among users and managers before expanding the scope. This chapter describes the deployment approach developed for Soudal based on the findings of the evaluation.

6.1 The Targeted Approach

The most important principle underpinning the deployment strategy is this: not every user at Soudal has the same privilege elevation need, and the deployment should reflect that. A single enterprise-wide rollout that treats a factory engineer the same as a finance assistant would fail, either by being too restrictive for the engineer or too permissive for the finance assistant.

Instead, the strategy targets four distinct user groups with tailored access models. This approach reduces disruption, lets the IT team validate each configuration before expanding scope, and ensures that users get the access they actually need rather than a one-size-fits-all compromise.

User Group	Access Model	Description and Justification
Engineering / Factory	Permanent Admin + Offline PIN	Equipment calibration, PLC software, driver installation. Work environment frequently offline. Need consistent elevated access. Offline PIN is essential, not optional.
Service Desk	Permanent Admin Session	Troubleshooting, remote support tools, software deployment throughout the day. Need reliable elevated access without repeated approval interactions.
Power Users / Developers	Temporary Admin Sessions (15 min–2 hr)	Occasional app installs, development environment setup, tooling configuration. Need elevation sometimes, not all the time.
Standard Users	App-Specific Elevation Only	Pre-approved apps auto-elevate for specific tasks (e.g., IP config changes). No broad admin rights needed or appropriate.

Table 10: Soudal user groups and tailored access models

6.2 Three-Phase Rollout Plan

The deployment is structured in three phases, each building on the previous one. This graduated approach allows the IT team to learn from each phase, address issues before they scale, and demonstrate value to stakeholders progressively.

6.2.1 Phase 1: Pilot

The pilot deploys first to the App department, a group of 3 users, selected as the initial group based on their practical need for elevation access and the willingness of their team lead to engage early in the process.

The scope covers the development and application tooling the team uses regularly, with pre-approved elevation rules configured for all identified runtime tools before day one so that no user experiences disruption from the moment ABR goes live on their device.

The focus during this phase is on validating that the deployment process works correctly, that the elevation features function as expected in the real production environment, and that the approval and monitoring workflows are operationally sustainable. Feedback from this group will directly shape how the rollout extends to Engineering, Service Desk, and the broader user population in subsequent phases.

6.2.2 Phase 2: Expand

Phase 2 expands the deployment to 13 users, adding power users and developers who need temporary admin sessions. This phase tests the session-based elevation workflow under a higher volume of requests and validates that the approval process can handle the increased load without creating bottlenecks.

Phase 2 also begins the permission revocation process for devices where pilot users previously held permanent admin rights. This is done carefully and methodically, verifying that each user's required tasks are covered by ABR elevation rules before removing their permanent access.

6.2.3 Phase 3: Standard Users

Phase 3 is the broadest in scope and the most operationally sensitive. It rolls out app-specific elevation rules for standard users across the organization, users who do not need broad admin access but who use specific applications that require elevation.

The scope and timing of Phase 3 will be adjusted based on the results from Phases 1 and 2. If the pilot reveals issues with specific applications or user workflows, those need to be resolved and the rules updated before deploying to a larger population. This phase also completes the permission revocation work for any remaining users who still hold legacy permanent admin rights.

6.3 Approval Workflow Design

For users who need to request elevation rather than having pre-configured or permanent access, the approval workflow needs to be fast enough to be practical. A workflow that takes 30 minutes to approve a standard request will drive users to find workarounds.

Request Type	Target SLA	Process
Urgent (Break Glass)	Within 5 minutes	User request → direct IT phone verification → immediate grant
Standard Elevation Request	Within 15 minutes	User request through ABR → IT portal review → approval and grant
After-Hours Request	Within 10 minutes via on-call	User request → on-call IT contact → grant elevation

Table 11: Approval workflow SLA design

Pre-approved applications and users in the permanent admin tier bypass this workflow entirely. The approval queue is designed to be as small as possible, only edge cases and new application requests should flow through it in steady state.

6.4 Training and Communication Approach

User adoption is not a given, particularly for users who are accustomed to having permanent admin rights and now find themselves needing to request elevation. The training approach is designed to minimize friction and avoid creating the impression that the IT team is making their lives harder for the sake of a compliance checkbox.

Rather than classroom sessions, a lightweight video-first approach was proposed: short tutorial clips of two to three minutes each covering the four main user-facing scenarios, Run As Admin, Admin Session, Offline PIN, and Pre-Approved Apps. These will be delivered through Teams and email before each phase of the rollout reaches the relevant user group. The messaging focuses on what the user gains, a clear, fast path to the elevated access they need, rather than dwelling on what they are losing.

For the IT team, the training need is primarily around the ABR portal: creating and managing rules, reviewing the approval queue, interpreting the audit logs, and handling edge cases. This is more technical and warrants a dedicated briefing session with the Intune administrators.

6.5 Risk Mitigation

Risk	Likelihood	Mitigation Strategy
User resistance to losing permanent admin	Medium	Gradual rollout, clear communication, fast approval SLAs, pre-approved rules for common tasks
Workflow disruption during transition	Medium	Pilot testing, rollback plan for each phase, pre-approved rules deployed before rights are removed
Approval queue bottleneck	Low-Medium	Multiple approvers, clear SLAs, pre-approval rules for high-frequency requests
Offline PIN security compromise	Low	Strong PIN policy, rotation schedule, device compliance enforcement
Rules missing a legitimate use case	Medium	Thorough pre-deployment rule testing, feedback channel for users to report blocked tasks

Table 12: Risk mitigation strategy summary

7. Stakeholder Communication

Effective stakeholder communication was an integral part of the project throughout all phases. This chapter summarizes the key communication activities that took place during the placement.

7.1 Regular Mentor Check-Ins

Regular check-ins with work placement mentors Dries Wuyts, Rob Verbiest and Eduard Claessen shaped the direction of the project at multiple points. These sessions informed the use case definitions in the analysis phase, the EPM test design, and the framing of the final comparison.

The resolution of the Intune RBAC deployment issue documented in Section 3.5 was reached through direct collaboration with Eduard Claessen during one of these sessions. The meeting with Rob Verbiest in Week 6 provided an opportunity to confirm the project direction and discuss the scope of the EPM licensing assessment.

7.2 Management Presentation

A presentation covering the project findings was delivered to the IT manager and department head at Soudal during Week 5.

The presentation was structured around four areas: the security and compliance risk justifying the project, the two tools evaluated and their comparative capabilities, the recommended solution and its rationale, and the proposed phased rollout plan.

The content was revised following feedback from the mentors, with the primary adjustment being a reduction in technical detail in favour of clearer business-level framing. Management approved the direction and the phased rollout approach following this session.

7.3 School Presentations

Two presentations were delivered at Thomas More as part of the work placement programme requirements. The project plan presentation took place in Week 4 of the placement, covering the environment analysis, use case definitions, tool selection rationale, and planned testing approach. A second presentation covering the work completed to date was delivered in Week 8.

7.4 App Department Pilot Engagement

During Week 8, a meeting was held with the head of the App department to present the Admin By Request pilot plan and walk through how the tool would affect the team in practice. Following that meeting, a communication was sent to the team explaining the upcoming changes and the timeline. The pilot deployment to the App department, covering 48 pre-approved applications identified through device discovery, began in Week 9 and forms part of the first phase of the production rollout.

8. Conclusion

This conclusion is written at the close of the placement, with the project delivered end to end. The evaluation phase for both ABR and EPM is complete, the recommendation has been presented to and approved by management, and the phased rollout has been carried through from the App department pilot to the wider user population. What began as a plan on paper is now a deployed, operational privilege management solution at Soudal.

8.1 What Was Achieved

This project demonstrated that just-in-time privilege elevation is a viable and operationally realistic replacement for permanent local administrator rights within Soudal's endpoint environment. The evaluation of Admin By Request and Microsoft Endpoint Privilege Management confirmed that both tools can deliver controlled elevation, but that their capabilities differ in ways that are directly relevant to Soudal's operational context.

The Admin By Request testing phase validated all six core features across a controlled Intune-managed environment, including offline PIN elevation for factory scenarios, pre-approved application rules, admin session management, and local administrator monitoring with remote revocation capability. The EPM evaluation, conducted across eighteen structured tests, confirmed EPM's strengths as a native Intune solution while identifying its offline limitation as a significant constraint for Soudal's engineering and factory use cases.

Based on the combined testing results and the use case analysis, Admin By Request was selected as the recommended solution and approved by management. The solution was then rolled out in three phases, beginning with the App department pilot covering 48 pre-approved runtime elevation applications and supported by Intune remediation scripts for local admin right auditing and removal. The pilot confirmed that the platform functions correctly in production and that the onboarding process is manageable for both administrators and end users. The deployment was subsequently expanded to power users and developers, and finally to standard users across the organization, with permanent local administrator rights removed incrementally as each group was onboarded.

8.2 Result Against the Project Plan

The project plan submitted at the start of the placement structured the work into three phases: research and evaluation, pilot rollout, and full migration, scheduled across thirteen weeks. The table below summarizes how the delivered result is mapped against that plan.

Project Plan Phase	Planned Work	Delivered Result	Status
Phase 1 — Research and Evaluation (Weeks 1–6)	Analyze the environment, define the problem and use cases, set evaluation criteria, and run hands-on lab testing of Admin By Request and Microsoft EPM, concluding with a recommendation to management	Environment analysis and problem defined with the mentors, evaluation criteria established, both tools tested in the lab (six ABR tests and eighteen EPM tests), and the recommendation presented to and approved by Soudal management	Completed
Phase 2 — Pilot Rollout (Weeks 7–10)	Deploy the selected tool to a pilot group, configure elevation policies and approval workflows, monitor audit logs, and collect user feedback	Admin By Request deployed to the App department pilot, with pre-approved application rules configured, audit logging in place, and user feedback collected to inform the wider rollout	Completed
Phase 3 — Full Migration (Weeks 11–13)	Remove remaining in-scope local admin rights, apply validated policies across the population device, deliver training and documentation, and produce the final report	Validated elevation policies applied across the in-scope groups, permanent local admin rights removed incrementally as each group was onboarded, training and administrator documentation delivered, and the final realization report produced	Completed

Table 13: Result against the project plan

All three phases defined in the project plan were completed. The EPM evaluation went beyond the original scope by expanding into eighteen structured tests, and the phased approach allowed each stage to be validated before the next began, which kept disruption to Soudal's operations to a minimum.

8.3 Reflecting on the Project

The project established a solid technical and operational foundation for privilege management modernization at Soudal and carried it through to a completed deployment. The solution was validated, the rollout strategy was defined and executed, and management alignment was secured throughout. The App department pilot served as the first production test of the end-to-end deployment process, and the feedback it generated directly shaped the Phase 2 and Phase 3 rollout.

The permission revocation work, the systematic removal of permanent local administrator rights from devices across the organization, was the most operationally sensitive part of the project and was executed incrementally as each user group was onboarded. The lessons learned during the ABR deployment, particularly around Intune RBAC configuration and the importance of verifying permissions early, were applied to each subsequent phase and reduced troubleshooting overhead as the rollout progressed.

Looking back, the project delivered on its central research question: permanent local administrator rights at Soudal were successfully replaced with a controlled, temporary, and fully auditable privilege elevation solution that satisfies the operational and compliance requirements identified at the outset. This realization report documents completed work end to end, from the initial environment analysis through to the production rollout and the removal of legacy permanent admin rights.

.

Glossary

ABR — Admin By Request. A cloud-based Privileged Access Management platform providing just-in-time privilege elevation for Windows, macOS, and Linux endpoints.

Autopilot — Microsoft Windows Autopilot. A cloud-based device provisioning service that automates the setup and configuration of new Windows devices through Microsoft Intune.

Break Glass — An Admin By Request emergency access feature that grants temporary full administrator rights in urgent situations, typically verified through a direct out-of-band approval such as a phone call, with the action fully logged for audit.

Conditional Access — A Microsoft Entra ID feature that enforces access policies based on user identity, device compliance state, sign-in location, and risk signals before granting access to resources.

EPM — Microsoft Endpoint Privilege Management. A native add-on to Microsoft Intune that enables rule-based just-in-time privilege elevation for Windows endpoints without granting permanent local administrator rights.

Entra ID — Microsoft Entra ID, formerly Azure Active Directory. Microsoft's cloud-based identity and access management service used for authentication, authorisation, and Conditional Access enforcement.

GDPR — General Data Protection Regulation. European Union regulation governing the processing and protection of personal data.

Intune — Microsoft Intune. A cloud-based endpoint management platform supporting device compliance, configuration profile deployment, application distribution, and endpoint security policy enforcement.

ISO 27001 — An international standard published by the International Organization for Standardization specifying requirements for an information security management system.

JIT — Just-in-Time. An access model in which elevated privileges are granted temporarily and only when operationally required, rather than being held permanently.

LOB app — Line-of-Business application. An application deployment type in Microsoft Intune used for distributing MSI-packaged software to managed devices.

MAM — Mobile Application Management. A component of Microsoft Intune for managing applications on enrolled and unenrolled devices.

Offline PIN — A feature of Admin By Request that allows privilege elevation to proceed on a device that has no active network connection, using a pre-configured PIN that is verified locally.

PAM — Privileged Access Management. A category of security tooling that controls, monitors, and audits the use of elevated or administrative access rights across an IT environment.

RBAC — Role-Based Access Control. An access control model in which system permissions are assigned based on the organizational roles held by individual users.

SIEM — Security Information and Event Management. A platform that collects, aggregates, and analyzes security event data from across an IT environment to support monitoring and incident response.

Use of AI Tools

AI tools were used as supporting aids during the writing of this document, not as a replacement for the analysis, testing, or decision-making behind the project. ChatGPT and Claude were used to help structure the report, improve the clarity and flow of the writing, and check spelling and grammar. All suggestions were reviewed and adjusted by me so that the wording reflected the actual work carried out during the placement, and so that every technical claim matched what was genuinely tested and observed.

The substance of the report, the environment analysis, the test design, the results, the comparison, and the recommendation, is based on my own work during the placement. The AI tools were used only to present that work more clearly. The final responsibility for the accuracy and content of this document remains with me.

References

Admin By Request. (2026). *Local admin rights, managed*. From Admin By Request: https://www.adminbyrequest.com/en/

Microsoft. (2026a). *Microsoft Entra ID documentation*. From Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/

Microsoft. (2026b). *Microsoft Intune documentation*. From Microsoft Learn: https://learn.microsoft.com/en-us/intune/

Microsoft. (2026c). *Role-based access control (RBAC) with Microsoft Intune*. From Microsoft Learn: https://learn.microsoft.com/en-us/intune/fundamentals/role-based-access-control/overview

Microsoft. (2026d). *Use Endpoint Privilege Management with Microsoft Intune*. From Microsoft Learn: https://learn.microsoft.com/en-us/intune/epm/overview

Microsoft. (2026e). *Use Intune Suite add-on capabilities*. From Microsoft Learn: https://learn.microsoft.com/en-us/intune/fundamentals/add-ons

Soudal NV. (2026). *Internal IT infrastructure architecture documentation.* From Soudal NV.

Verizon. (2024). *2024 Data Breach Investigations Report*. From Verizon Business: https://www.verizon.com/business/resources/reports/dbir/

Attachments

The following attachments are referenced throughout this document and are available as separate files.

Attachment A: ABR Testing Report (Full), Complete lab testing documentation with all screenshots and detailed technical evidence for all six ABR tests.

Attachment B: EPM testing evidence is documented inline in Chapter 4 of this report (Figures 20–39). No separate attachment is required, as all screenshots, test procedures, and results are presented within the main document.

Attachment C: ABR vs EPM Detailed Comparison, Extended side-by-side comparison matrix with weighted scoring across all eight evaluation criteria.

Attachment D: Project Plan, Original project plan as submitted and presented at Thomas More in week 4.

Attachment E: Stakeholder Presentation Slides, Technical version (mentor audience) and management version, including all iteration notes. (some available on request)

Attachment F: Use Case Documentation, Detailed use case descriptions, user group mapping, and access model specifications.

Attachment G: Weekly Status Reports, Complete set of weekly internship reports covering the full project period. (available on request)