Muhammad Zubair

Admin By Request

Laboratory Testing Report

Policy Validation

Controlled Testing

DOCUMENT TYPE

Supporting attachment to the Realization Document

AUTHOR

Muhammad Zubair

COMPANY

Soudal NV — Turnhout, Belgium

ACADEMIC YEAR

2025–2026

DATE

March 9, 2026

Table of Contents

1. Executive Summary

This report documents the laboratory testing of Admin By Request (ABR), a cloud-based Privileged Access Management solution, in a controlled test environment at Soudal NV. The objective was to evaluate ABR's capabilities for replacing permanent local administrator rights with secure, auditable, just-in-time privilege elevation.

Testing was conducted on Microsoft Intune-managed devices enrolled in Microsoft Entra ID, aligned with Soudal's hybrid identity and cloud-first infrastructure strategy. All core ABR features were successfully validated, including deployment through Intune, elevation requests, time-bounded admin sessions, offline PIN elevation, pre-approved application rules, and local administrator inventory monitoring.

ABR demonstrates strong capability for privilege management across Soudal's workforce. Deployment via Intune succeeded after resolving an Intune RBAC permission issue. All six elevation workflows function correctly. Offline PIN support provides the resilience required for factory environments where network connectivity is intermittent. The detailed findings, test procedures, and evidence are presented in the sections that follow.

2. Testing Environment

2.1 Infrastructure Overview

The test environment was configured to reflect Soudal's production architecture as closely as possible within an isolated laboratory context:

- Identity: Hybrid model with on-premises Active Directory synchronized one-way to Microsoft Entra ID via Entra Connect.
- Device management: Microsoft Intune with Autopilot enrollment, compliance policies, and configuration profiles.
- Access control: Microsoft Entra ID Conditional Access policies governing device and user access.
- Network: Corporate WiFi on an isolated test segment.
- Management portals: Microsoft Intune Admin Center, Microsoft Entra ID, and the Admin By Request cloud portal.

2.2 Test Devices

Device Role	Description
Admin Laptop	Windows 11 Pro — used for managing the Intune Admin Center and ABR portal
Test Laptop 1	Windows 11 Pro (Intune-managed) — primary testing device for all ABR tests
Test Laptop 2	Windows 11 Pro (Intune-managed) — secondary device for verification

Table 1: Test devices used for ABR laboratory testing

2.3 Software Versions

Component	Version
Admin By Request Workstation Client	Version 8.7
Microsoft Intune	Current (2026)
Microsoft Entra ID	Current (2026)
Operating System	Windows 11 Pro (Build 22H2 or later)
PowerShell	7.x

Table 2: Software and platform versions used during testing

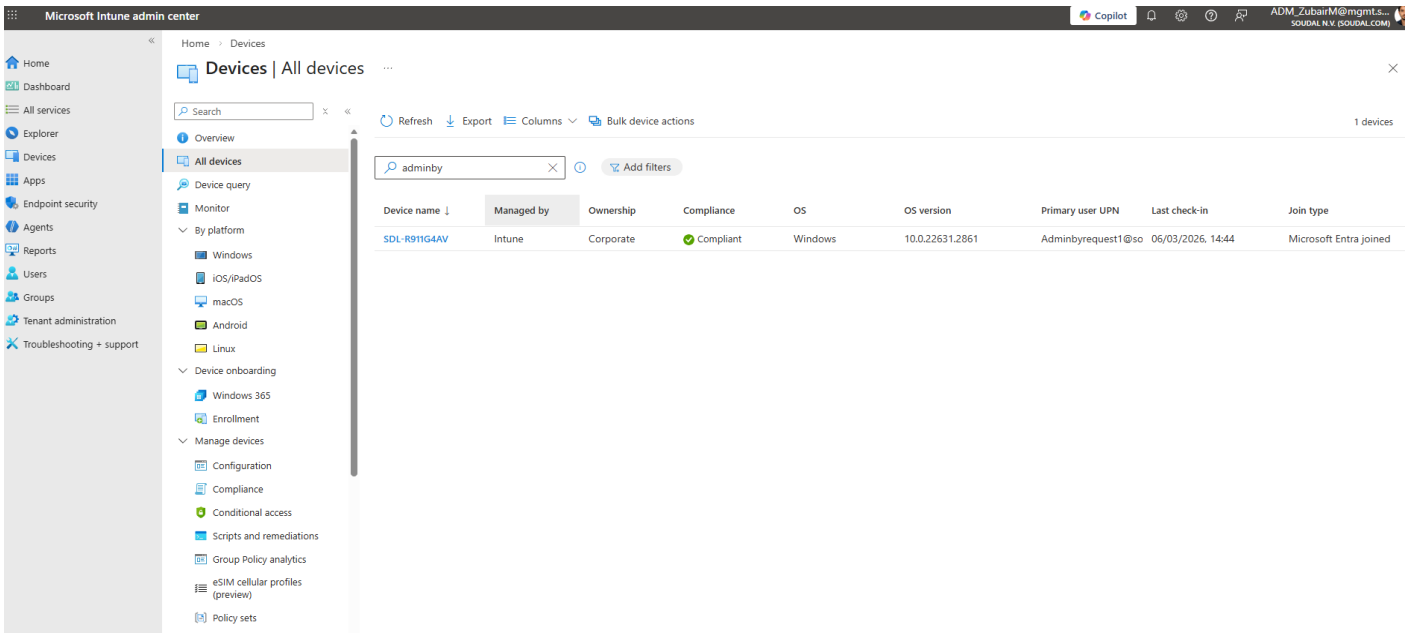
3. Device Preparation

3.1 Enrollment

The test device was enrolled into the Soudal Intune environment through the following steps:

- Connected the test laptop to the corporate WiFi network.
- Signed in using Soudal Entra ID credentials.
- The device automatically joined Microsoft Entra ID (Entra Join).
- Verified device presence in Microsoft Intune under Devices, with Join Type confirmed as Entra Joined and Ownership as Corporate.

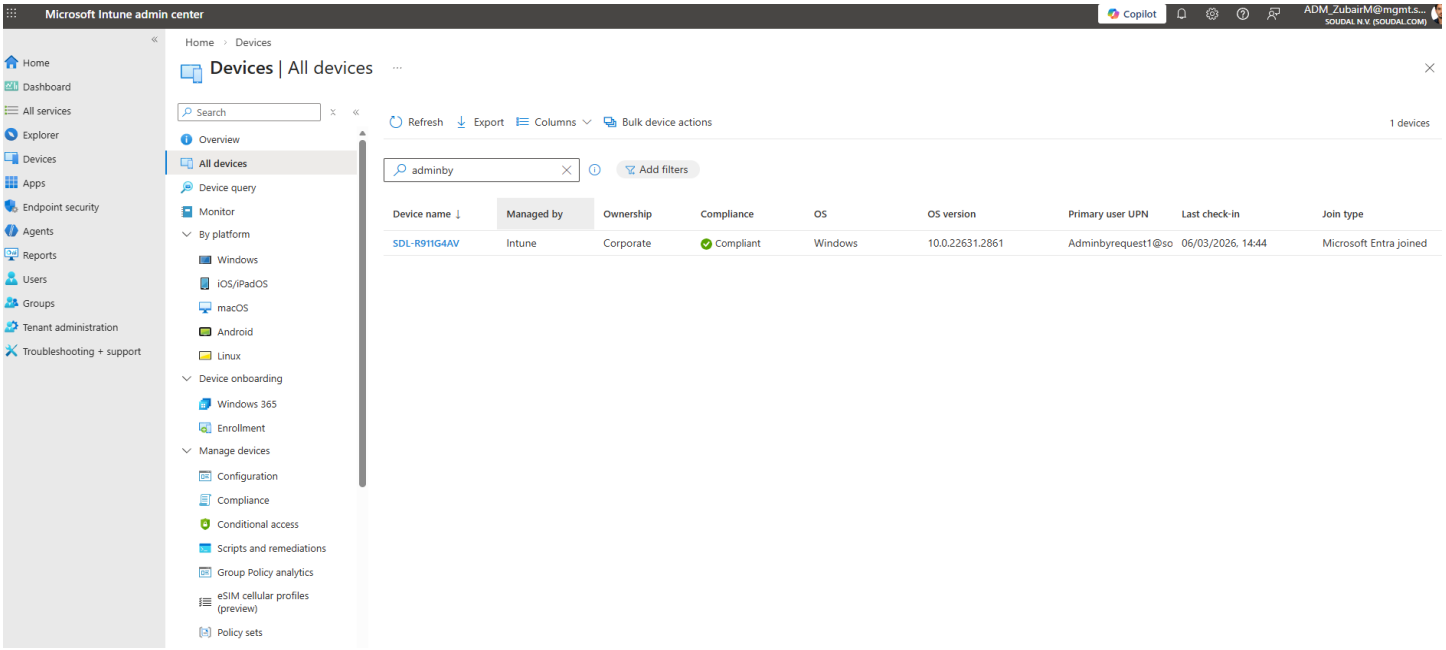
Figure 1: Test device enrollment confirmation in Microsoft Intune



3.2 Initial Device Status

After enrollment, the device initially reported as non-compliant in Intune. This is expected behavior while device synchronization and policy application occurs. Compliance status was monitored and resolved automatically after the policy synchronization cycle completed.

Figure 2: Test device compliance status in Intune admin center



3.3 Verification

Device readiness was confirmed through three methods: the device About page showing Entra ID enrollment, the Intune Company Portal app confirming compliance status, and a PowerShell verification command confirming the device name, domain, and manufacturer.

4. Deployment Scope Setup

4.1 Rationale

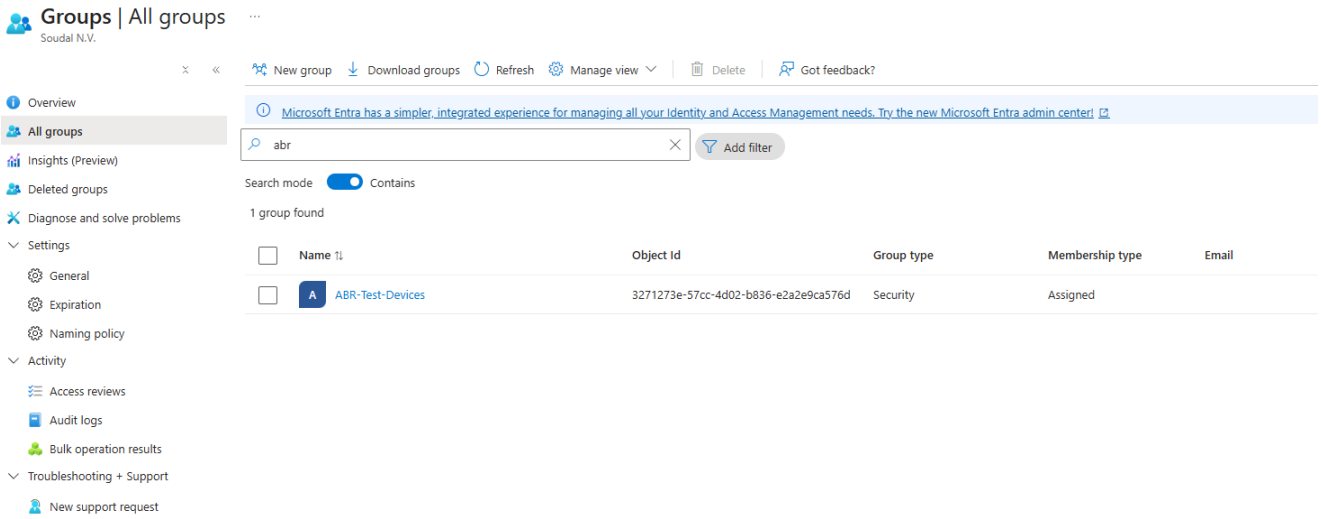
To ensure that testing did not affect production devices, a dedicated security group was created in Microsoft Entra ID. This scoped deployment ensures that only authorized test devices receive the Admin By Request client during the evaluation phase.

4.2 Security Group

Property	Value
Group Name	ABR-Test-Devices
Group Type	Security (not Microsoft 365)
Membership Type	Dynamic device-based membership
Members	Test Laptop 1 (primary), Test Laptop 2 (secondary)

Table 3: ABR-Test-Devices security group configuration

Figure 3: ABR-Test-Devices security group in Microsoft Entra ID



5. Admin By Request Client Download

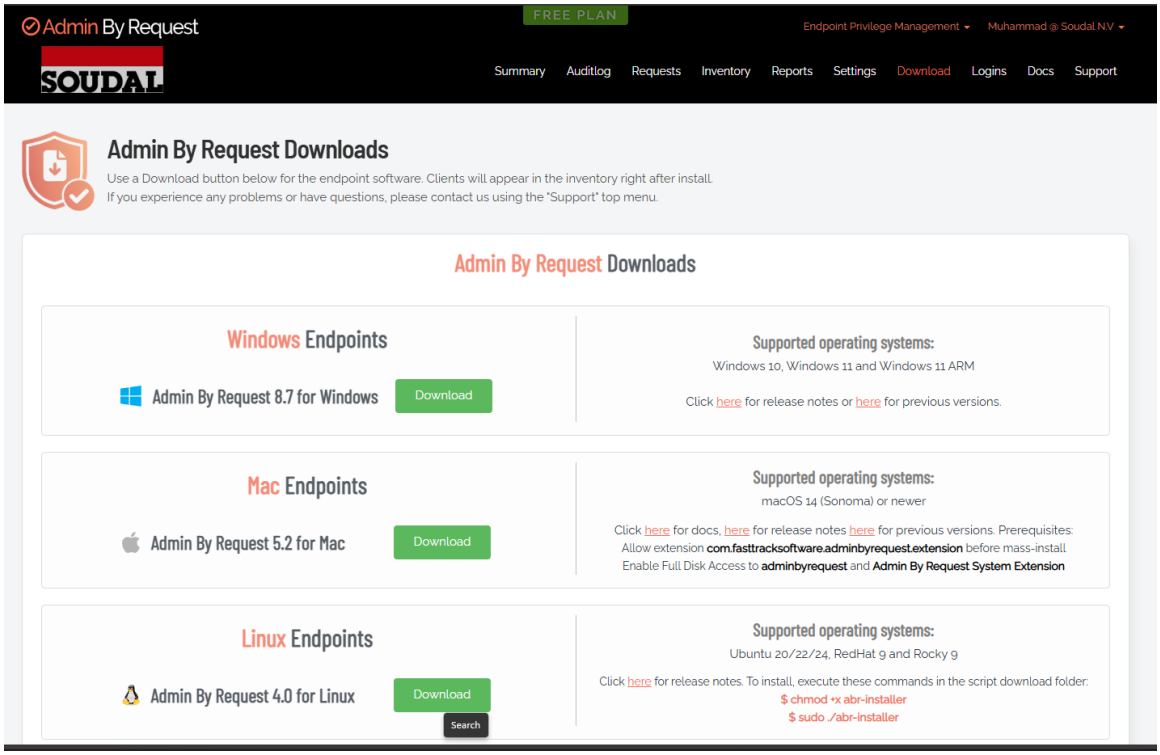
5.1 Download Details

The Admin By Request client for Windows endpoints was downloaded from the official ABR portal. The installer was obtained as an MSI package (Microsoft Installer format), version 8.7, suitable for deployment through Microsoft Intune.

5.2 File Verification

Prior to deployment, the installer was verified for file integrity through SHA256 hash comparison, digital signature validation, compatibility with Windows 11 Pro, and MSI structure validation to confirm that it could be installed via msiexec.

Figure 4: ABR installer SHA256 hash verification



6. Intune Deployment and Troubleshooting

Multiple deployment strategies were attempted to integrate the ABR client with Microsoft Intune. Initial attempts encountered obstacles related to Intune RBAC permissions. With the assistance of Eduard Claessen (work placement mentor), the underlying access control issue was identified and resolved. This section documents the troubleshooting process and lessons learned.

6.1 Method 1: Line-of-Business MSI Deployment

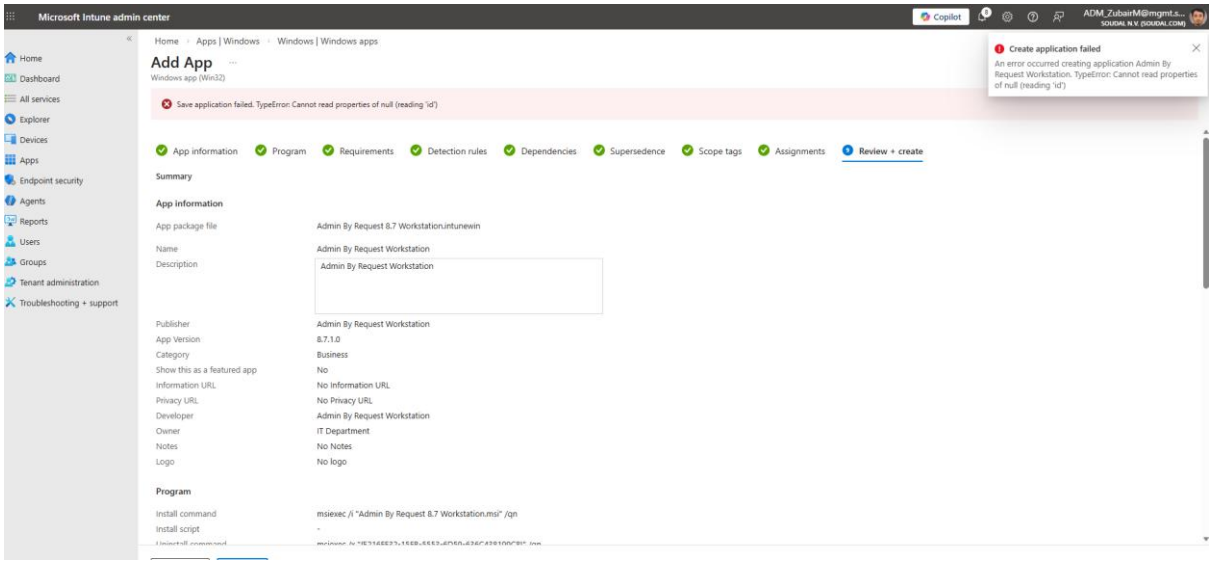
6.1.1 Procedure

The initial deployment approach used Intune's native LOB app type. The ABR MSI installer was uploaded through the Intune Admin Center under Apps, Windows Apps, Add, with the Line-of-Business app type selected. The application was assigned to the ABR-Test-Devices group with Required intent.

6.1.2 Error Encountered

The upload failed with the error: *Save application failed — TypeError: Cannot read properties of null (reading 'appType').* All subsequent attempts to create any application in Intune encountered similar errors, indicating a systemic issue in the Intune portal configuration rather than a problem with the ABR installer.

Figure 5: Intune LOB app deployment error message



6.1.3 Troubleshooting Attempts

The following troubleshooting steps were performed before the root cause was identified:

- Refreshed the Intune Admin Center session and cleared the browser cache.
- Attempted the upload from different browsers (Edge, Chrome).
- Recreated the application entry with a freshly downloaded MSI file.
- Renamed the installer file to remove version numbers from the filename.
- Verified MSI file integrity and re-downloaded from the ABR portal.
- Tested with different application types (Win32 app, Web app) — all failed with similar errors.

All application creation attempts failed consistently, pointing to a tenant or permission configuration issue rather than a file-level problem.

6.2 Root Cause Analysis: RBAC Permissions

6.2.1 Discovery

The root cause was identified as insufficient Intune role-based access control (RBAC) permissions on the user account performing the deployment. The Intune portal was returning generic JavaScript errors that obscured the underlying permission denial. Specifically, the Mobile Application Management, Intune Administrator, Cloud Application Administrator, and Application Administrator roles were either missing or incorrectly configured.

6.2.2 Resolution with Mentor Support

With the assistance of Eduard Claessen (ICT Infrastructure mentor at Soudal), the Intune RBAC configuration was reviewed and corrected. Eduard reviewed the current role assignments, identified the missing Intune Administrator and Cloud Application Administrator roles, assigned the appropriate permissions with granular app creation and assignment capabilities, verified role propagation through Entra ID, and tested application creation to confirm access was restored.

6.2.3 Outcome

After the RBAC permissions were corrected, all Intune portal errors were resolved. The user account could successfully create LOB apps, Win32 packaged applications, and assign applications to device groups. All subsequent deployment attempts succeeded without errors.

6.3 Method 2: Win32 Packaging

After the RBAC issue was resolved, Win32 app packaging was tested as an alternative deployment method. The MSI was packaged using the Microsoft Win32 Content Prep Tool (IntuneWinAppUtil.exe) to produce an .intunewin package. The Win32 app was configured in Intune with the appropriate install command, uninstall command, detection rule (MSI product code), and assigned to the ABR-Test-Devices group.

Setting	Value
Install command	msiexec /i "Admin By Request 8.7 Workstation.msi" /qn /norestart
Uninstall command	msiexec /x {product-code} /qn /norestart
Detection rule	MSI product code match
Assignment group	ABR-Test-Devices (Required)

Table 4: Win32 app configuration settings in Intune

Both LOB and Win32 deployment methods were validated successfully after the permission correction.

7. Deployment Confirmation

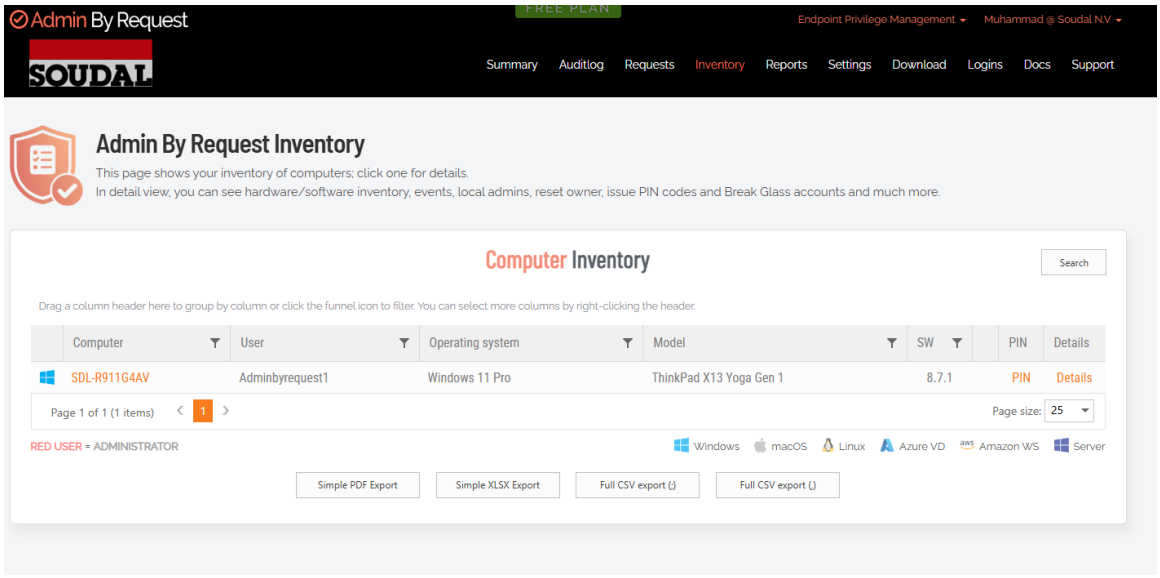
Following the RBAC permission resolution, Admin By Request was successfully deployed to Test Laptop 1 via Intune as a Line-of-Business app with Required assignment to the ABR-Test-Devices group. Installation occurred automatically during the next device synchronization cycle without user intervention.

7.1 Post-Installation Verification

Client installation was confirmed through five verification methods:

- Admin By Request icon visible in the system tray (taskbar notification area).
- ABR client process running, confirmed in Task Manager.
- ABR portal showing the device in the Inventory section under Devices.
- Device certificate present in the local certificate store for portal authentication.
- ABR service running in Windows Services (status: Running).

Figure 6: ABR client running in system tray and confirmed in Task Manager



7.2 Enforcement Validation

Intune enforcement was validated by manually uninstalling ABR from the test device. Upon the next device synchronization cycle, Intune automatically reinstalled the application, confirming that Required assignments are properly enforced.

8. Core Functionality Testing

With ABR successfully deployed, comprehensive functional testing was performed to validate all major privilege elevation workflows. Six structured tests were conducted, each with a defined objective, procedure, and documented result.

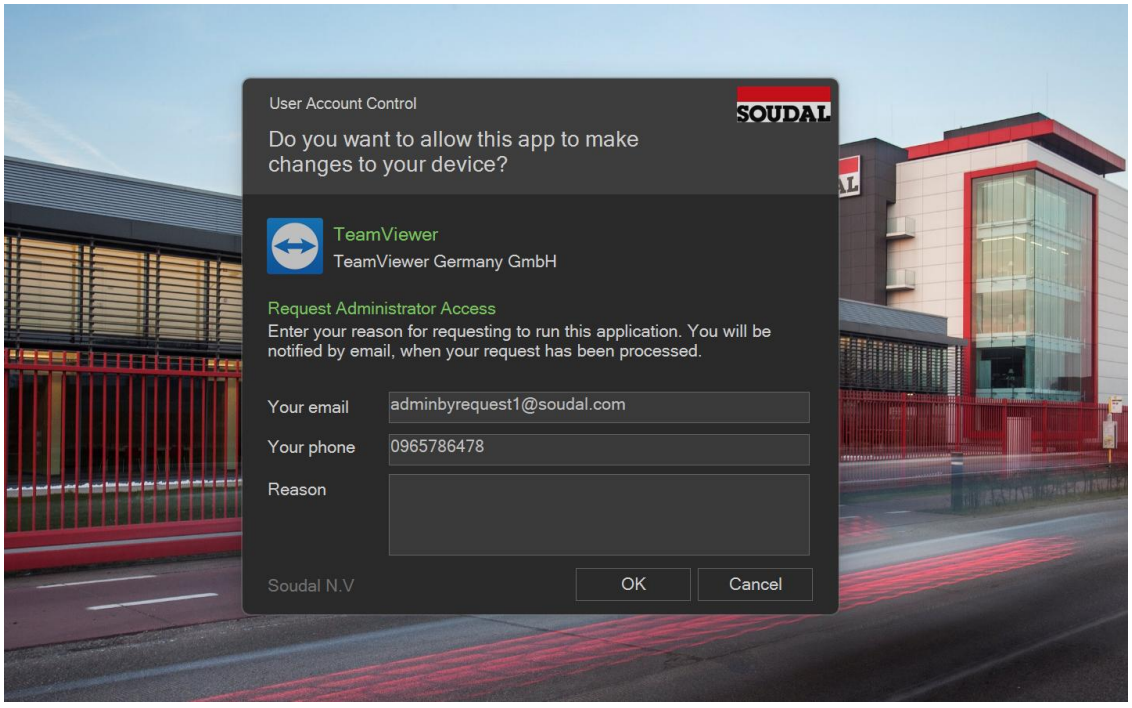
8.1 Test 1: Run As Administrator Request

Objective: Verify that end users can request elevated privileges for specific applications without permanently holding administrator rights.

Procedure: Logged in as a standard user on Test Laptop 1, right-clicked an application (Command Prompt), and selected Run as administrator. ABR intercepted the elevation request, displayed a request form, and transmitted the request to the ABR portal for approval. The administrator approved the request in the portal, and the application launched with elevated privileges.

Result: Pass. The elevation request was captured, approved, and executed successfully. The audit trail recorded the timestamp, user, application, and request reason.

Figure 7: Run As Administrator elevation request in ABR client



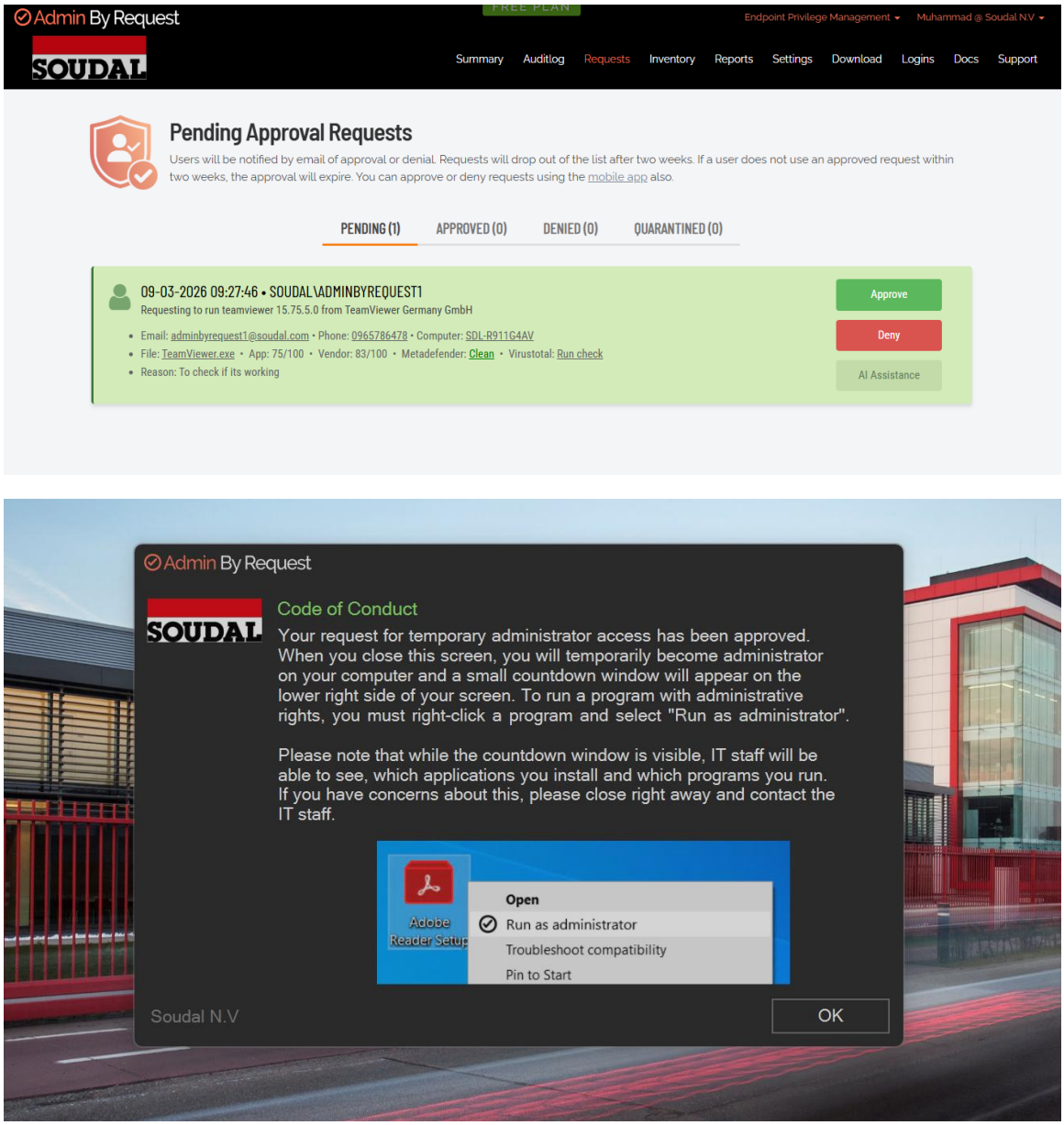
8.2 Test 2: Admin Session Request

Objective: Verify that users can request a temporary administrator session for a defined duration.

Procedure: Right-clicked the ABR tray icon and selected Request Administrator Access. Specified a session duration and submitted the request. The administrator approved the session in the ABR portal. The user activated the session locally, receiving temporary administrator group membership. Verification was performed using PowerShell (Get-LocalGroupMember Administrators) confirming the test user appeared in the Administrators group.

Result: Pass. Admin session activation, temporary group membership, and elevated command execution all functioned as expected.

Figure 8: Admin session request and activation in ABR



8.3 Test 3: End Admin Session

Objective: Verify that administrator privileges are properly revoked when the session expires or is manually terminated.

Procedure: With an active admin session running, right-clicked the ABR tray icon and selected End Administrator Session. ABR confirmed the termination. Post-termination verification using PowerShell confirmed the user was no longer listed in the Administrators group. Subsequent elevation attempts were intercepted by ABR and required a new approval request.

Result: Pass. Admin rights were immediately revoked. The user returned to standard privilege state.

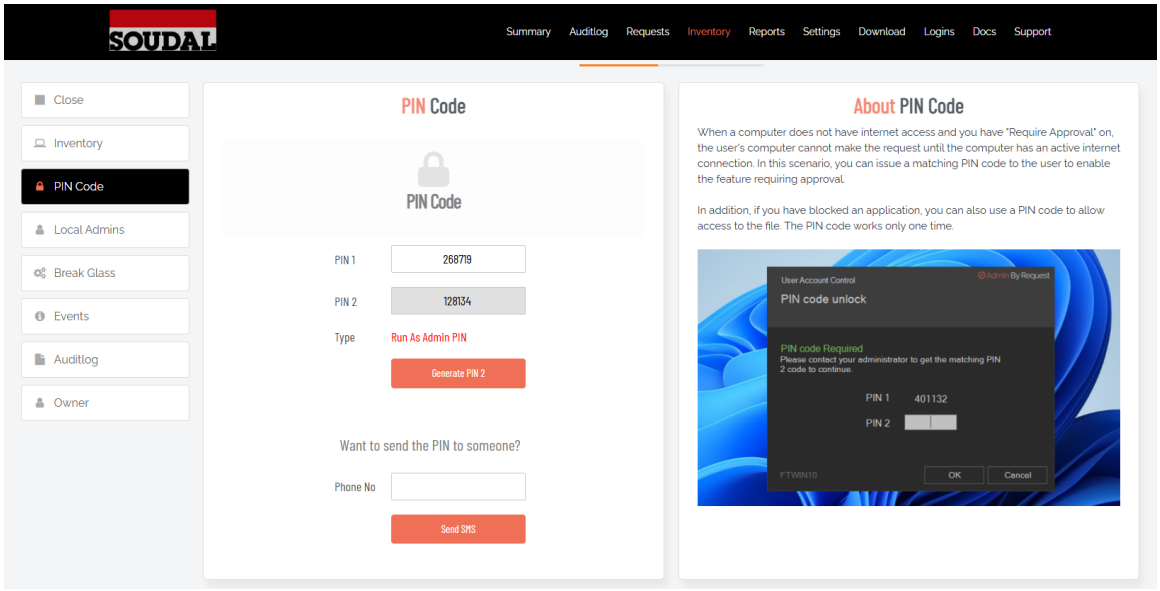
8.4 Test 4: Offline PIN Elevation

Objective: Verify that ABR supports offline privilege elevation using a PIN, which is critical for factory environments where network connectivity is intermittent.

Procedure: Configured an offline PIN in the ABR client through the ABR portal. Disabled the WiFi adapter on Test Laptop 1 to simulate an offline scenario. Right-clicked an application and selected Run as administrator. ABR detected the offline status and displayed the Offline PIN entry prompt. Entered the configured PIN. The application launched with elevated privileges despite the absence of network connectivity.

Result: Pass. Offline elevation was successful. The elevation event was logged locally and synchronized to the ABR cloud portal upon WiFi reconnection. This feature is essential for Soudal's factory operations.

Figure 9: ABR Offline PIN elevation prompt on disconnected device



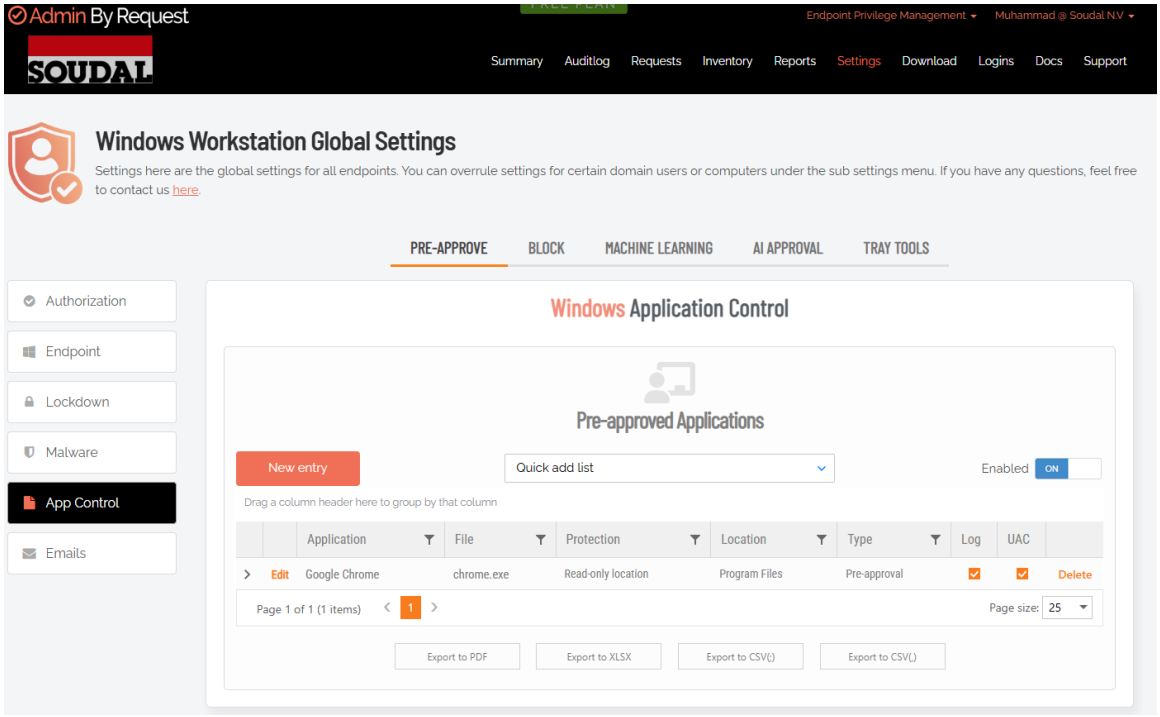
8.5 Test 5: Pre-Approved Application Rule

Objective: Verify that administrators can pre-authorize specific applications to run with elevated privileges without requiring an approval request each time.

Procedure: Created a pre-approval rule in the ABR portal targeting a specific application executable. The rule specified the allowed file path and directory conditions. As a standard user, launched the application. ABR evaluated the file path against the pre-approval rule, matched it, and launched the application with administrator privileges automatically.

Result: Pass. The application launched with elevated privileges without user intervention or an approval delay. The ABR audit log recorded the event as auto-approved (pre-authorization rule match).

Figure 10: ABR pre-approved rule configuration and audit log entry



8.6 Test 6: Local Administrator Monitoring

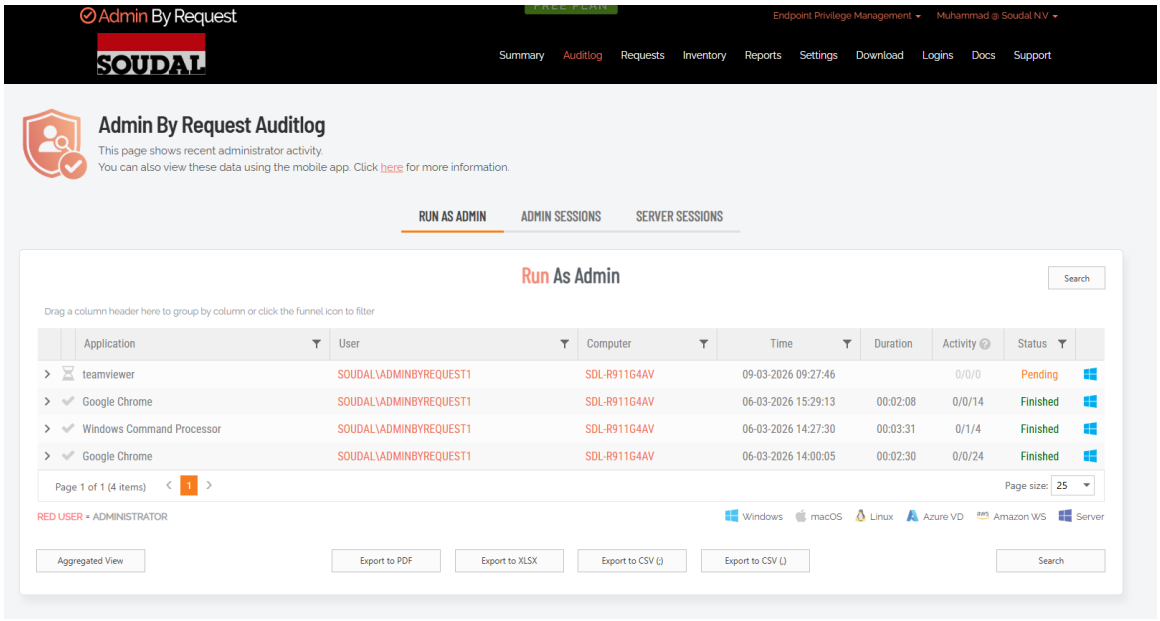
Objective: Verify that ABR can detect, report, and manage users with permanent local administrator rights, supporting the transition to just-in-time elevation.

Procedure: Accessed the ABR portal under Devices, selected Test Laptop 1, and reviewed the Local Administrators section. ABR displayed an inventory of all users with permanent administrator group membership, including usernames, domains, and administrator status.

Capabilities verified: real-time detection of local admin group membership, granular visibility into individual user and service accounts, remote revocation of admin rights without physical device access, audit trail of admin right changes, and the option to re-grant rights through an approval workflow.

Result: Pass. ABR successfully inventoried all local administrators on the test device and provided centralized management options. This capability is critical for the permission revocation phase of the deployment plan.

Figure 13: Local administrator inventory in ABR portal for Test Laptop 1



9. Findings and Results

9.1 Feature Validation Summary

Feature	Test	Result	Status
Run As Administrator	Test 1	Request captured, approved, executed	**Pass**
Admin Session	Tests 2–3	Activation and termination successful	**Pass**
Offline PIN Elevation	Test 4	Elevation without network; audit preserved on sync	**Pass**
Pre-Approved Rules	Test 5	Auto-elevation with no approval prompt	**Pass**
Local Admin Monitoring	Test 6	Real-time inventory and remote revocation	**Pass**
Intune Enforcement	Manual	Auto-reinstall after manual removal	**Pass**

Table 5: Feature validation summary — all ABR tests passed

9.2 Key Strengths Identified

- Offline capability: PIN-based elevation functions without network connectivity, which is critical for factory environments.
- Rich audit trail: Comprehensive logging of all elevation events including timestamp, user, application, approval outcome, and duration.
- Granular rules: Pre-approval rules and conditions enable fine-grained control without reducing security.
- Multi-mode elevation: Supports Run As Administrator, Admin Session, and Break Glass scenarios from a single platform.
- Cross-platform support: ABR supports Windows, macOS, and Linux, though the evaluation scope focused on Windows.
- User experience: The tray-based interface is intuitive and the approval workflow is responsive.
- Intune integration: Deploys seamlessly through Intune and integrates with Entra ID identity.
- Local administrator visibility: Provides a clear, centralized inventory of privilege distribution across managed devices.

9.3 RBAC Lessons Learned

The initial deployment failure caused by insufficient RBAC permissions highlighted an important operational lesson: Intune error messages do not always clearly indicate permission issues. Portal errors may mask underlying RBAC denials, and multiple application creation failures should prompt an immediate review of role assignments rather than extended troubleshooting of the application

package itself. Proper role assignment (Intune Administrator, Cloud Application Administrator) is a prerequisite for application management workflows.

9.4 Observations and Considerations

- User training is required: users must understand when and how to request elevation, and cultural change management will be needed.
- Approval workflow requires operational discipline: if IT staff do not respond to approval requests promptly, users will experience delays.
- Offline PIN security: PINs must be managed securely with regular rotation.
- Performance impact: negligible; the ABR client consumes less than one percent CPU at rest.
- Licensing: ABR uses a per-user licensing model; cost depends on the number of managed users.

10. Recommendations and Next Steps

Based on the laboratory testing results, Admin By Request demonstrates strong capability for implementing just-in-time privilege elevation at Soudal. The following recommendations are provided for the next phases of the project.

10.1 Proceed with Pilot Deployment

A limited pilot deployment targeting 10 to 20 users in the Engineering and Service Desk groups is recommended. The pilot should cover engineering tasks (IP/network configuration, driver installation), Service Desk operations (software deployment, endpoint troubleshooting), and factory floor scenarios (selective elevated access for maintenance). A pilot duration of two to four weeks is recommended to gather sufficient usage data and user feedback.

10.2 Establish Approval Workflow SLAs

A structured approval process should be defined before the pilot begins, including approval tier structure (department manager, IT, escalation to CTO), target response times (urgent: under five minutes, routine: under fifteen minutes), after-hours escalation procedures, and deny-reason logging for compliance purposes.

10.3 Offline PIN Management Policy

For factory environments, a PIN management policy should be established covering PIN complexity requirements, rotation schedule (quarterly recommended), secure storage procedures, and reset procedures if a device is lost or compromised.

10.4 Complete the EPM Comparison

The side-by-side evaluation of ABR versus Microsoft Endpoint Privilege Management should be completed before a final procurement decision. The comparison criteria should include total cost of ownership, integration depth with Intune and Entra ID, cross-platform support requirements, feature parity (offline capability, audit trail, approval workflow), and vendor roadmap.

10.5 Change Management and Communication

A comprehensive change management plan should be developed to support user adoption. This should include executive sponsorship and leadership buy-in, user communication explaining the benefits and the new workflow, hands-on training for Engineering, Service Desk, and factory IT staff, a clear escalation path for elevation request issues, and metrics to track approval rates, denial rates, and audit events during the pilot.

11. Appendices

11.1 Technical Specifications

Admin By Request Workstation Client v8.7: Supported on Windows 7 SP1 and later (tested on Windows 11 Pro). Requires approximately 100 MB disk space and 50 MB available RAM. Installed via MSI (msiexec-compatible). Service name: AirWatch Admin By Request. Configuration stored in the local device registry (encrypted). Communicates with the ABR cloud portal over HTTPS (port 443). Offline fallback via PIN-based elevation without network connectivity.

11.2 Intune RBAC Permissions Reference

The following Entra ID roles are required for Intune application deployment and management:

- Intune Administrator: full access to all Intune features including application management.
- Cloud Application Administrator: delegated permissions for cloud application management.
- Application Administrator: manage applications in Entra ID and Intune.

Role propagation through Entra ID may take 15 to 30 minutes after assignment.

11.3 PowerShell Commands Used

- Get-LocalGroupMember Administrators — verify local administrator group membership.
- Get-Service | Where-Object {$_.Name -like "*AirWatch*"} — check ABR service status.
- Get-ComputerInfo | Select Name, Domain — verify device identity.
- Test-NetConnection [ABR-portal-domain] -Port 443 — verify ABR portal connectivity.

11.4 Acknowledgments

This testing was conducted with the support of Eduard Claessen (ICT Infrastructure, Soudal NV), who provided critical assistance in identifying and resolving the Intune RBAC permission issue. His expertise in Microsoft cloud identity and access management was essential to the successful completion of this phase of the project.