Muhammad Zubair

Use Case Documentation

User Group Mapping and Access Model Specifications

Project	Privilege Management Modernization at Soudal
Company	Soudal NV, Turnhout, Belgium
Author	Muhammad Zubair
Academic Year	2025 – 2026
Date	March 2026

Table of Contents

1. Purpose and Scope

This document defines the five operational use cases that drive the privilege elevation requirements at Soudal NV. Each use case describes a distinct user group, the tasks that require elevated privileges, the working conditions under which those tasks are performed, and the access model assigned to each group within the Admin By Request (ABR) deployment.

The use cases were identified during the analysis phase of the project (Chapter 2 of the realization report) and validated through hands-on laboratory testing (Chapters 3 and 4). They form the basis of the deployment strategy (Chapter 6) and the approval workflow design. This attachment serves as a standalone reference for IT administrators, the Service Desk team, and compliance reviewers who need to understand what privileges each user group holds and why.

The five use cases are:

- Use Case 1: Engineering and factory floor elevation (offline-capable).
- Use Case 2: Service Desk support operations.
- Use Case 3: Application installation for standard users.
- Use Case 4: Permission revocation and administrator inventory.
- Use Case 5: Compliance audit and elevation reporting.

2. User Group Overview

Soudal's endpoint user population is divided into four groups based on their operational role and privilege elevation requirements. Each group receives a tailored access model within ABR, designed to provide the minimum level of elevated access necessary to perform their defined tasks without granting unnecessary permanent privileges.

User Group	Access Model	Description and Justification
Engineering / Factory	Permanent Admin + Offline PIN	Equipment calibration, PLC software, driver installation. Work environment is frequently offline. Consistent elevated access is required. Offline PIN is essential for operational continuity.
Service Desk	Permanent Admin Session	Troubleshooting, remote support tools, software deployment throughout the day. Requires reliable elevated access without repeated approval interactions for each tool or action.
Power Users / Developers	Temporary Admin Sessions (15 min – 2 hr)	Occasional application installs, development environment setup, tooling configuration. Needs elevation sometimes, but not continuously. Time-bounded sessions enforce least privilege.
Standard Users	App-Specific Elevation Only	Pre-approved applications auto-elevate for specific tasks (e.g., IP configuration changes). No broad administrator rights needed or appropriate for this group.

Table 1: User group mapping with access models and justifications

The access model for each group was determined by the operational requirements identified during the analysis phase, validated through laboratory testing, and aligned with the principle of least privilege. Users receive the minimum elevation necessary for their defined tasks, with all elevation events logged for audit purposes.

3. Detailed Use Case Specifications

3.1 Use Case 1: Engineering and Factory Floor Elevation

Use Case ID	UC-01
Title	Engineering and Factory Floor Elevation
User Group	Engineering / Factory staff
Access Model	Permanent Admin + Offline PIN
ABR Feature	Offline PIN elevation, Run As Administrator, Admin Session
Network Requirement	Must function fully offline (no corporate network dependency)
Validated In	ABR Test 4 (Offline PIN), Realization Report Chapter 3

Table 2: Use Case 1 specification — Engineering and factory floor elevation

3.1.1 Description

Engineering staff at Soudal work on factory floors and in production environments where network connectivity to the corporate infrastructure is not guaranteed. These users perform tasks that require elevated privileges on a daily basis, including equipment calibration and PLC software configuration, industrial control system driver installation and updates, network interface and IP configuration on production devices, and factory automation tool maintenance.

Because these tasks are performed in environments with intermittent or absent corporate network connectivity, the privilege elevation mechanism must function without any network dependency. ABR's Offline PIN feature satisfies this requirement by allowing a pre-configured PIN to be used for elevation when the device is disconnected, with the elevation event logged locally and synchronized to the ABR cloud portal on reconnection.

3.1.2 Operational Flow

- Engineering user encounters a task requiring elevated privileges on a factory floor device.
- If the device has network connectivity: the user submits a standard elevation request through ABR.
- If the device is offline: the user enters the pre-configured Offline PIN in the ABR prompt.
- ABR grants elevation. The user performs the required task.
- The elevation event is logged locally on the device.
- When the device reconnects to the corporate network, the local log synchronizes to the ABR cloud portal.
- The IT team has full audit visibility into the elevation event, including the offline indicator.

3.1.3 Constraints and Controls

- Offline PINs must follow the PIN management policy: minimum complexity, quarterly rotation, secure storage.
- Users in this group are enrolled in the ABR Permanent Admin tier, meaning they do not require per-request approval for standard elevation tasks.
- All elevation events, including offline elevations, are logged with timestamp, user identity, device identity, and action performed.
- The IT team retains the ability to remotely revoke admin rights through the ABR portal if a device or account is compromised.

3.2 Use Case 2: Service Desk Support Operations

Use Case ID	UC-02
Title	Service Desk Support Operations
User Group	Service Desk / IT Support
Access Model	Permanent Admin Session
ABR Feature	Admin Session (time-bounded), Run As Administrator
Network Requirement	Corporate network or VPN connectivity required
Validated In	ABR Tests 1–3 (Elevation, Session, Termination), Realization Report Chapter 3

Table 3: Use Case 2 specification — Service Desk support operations

3.2.1 Description

Service Desk staff perform a wide variety of administrative tasks across multiple tools during the course of a support session. A typical support interaction may involve running diagnostic tools, modifying system settings, installing or updating software, and accessing protected configuration areas. These tasks require sustained elevated access across multiple tools rather than per-application elevation.

ABR's Admin Session model is well suited to this workflow because it grants temporary full administrator access for a defined period, matching the operational reality of a support session. The session duration is configurable and can be extended if needed. When the session ends (by expiry or manual termination), the user is immediately returned to standard privilege status.

3.2.2 Operational Flow

- Service Desk user begins a support session and requires elevated privileges.
- User right-clicks the ABR tray icon and requests an Admin Session with a defined duration.
- ABR grants the session (permanent admin tier users bypass the approval queue).
- User performs all required support tasks with full administrator access.
- When the session expires or the user manually ends it, admin rights are immediately revoked.
- All actions during the session are logged in the ABR audit trail.

3.2.3 Constraints and Controls

- Service Desk users are assigned to the Permanent Admin Session tier in ABR.
- Session durations are configurable by IT administrators. Default recommended: 4 hours (a typical shift).
- Users can request session extension if needed, which is logged.
- Session termination is automatic on expiry. Admin group membership is revoked immediately.
- The IT team can monitor active sessions and remotely terminate them if needed.

3.3 Use Case 3: Application Installation

Use Case ID	UC-03
Title	Application Installation for Standard Users
User Group	Standard Users / Power Users
Access Model	App-Specific Elevation (pre-approved rules) or Temporary Admin Session
ABR Feature	Pre-Approved Application Rules, Run As Administrator
Network Requirement	Corporate network or VPN connectivity required
Validated In	ABR Test 5 (Pre-Approved Rules), Realization Report Chapter 3

Table 4: Use Case 3 specification — Application installation

3.3.1 Description

Standard users and power users occasionally need to install approved applications that require administrator privileges during the installation process. These installations include approved productivity tools, browser updates, development environment components, and departmental software.

ABR handles this through pre-approved application rules. The IT team pre-configures rules that allow specific installer executables to run with elevated privileges automatically, based on file path, publisher certificate, or hash match. Users experience no delay or approval interaction; the application simply installs as expected.

For applications not covered by pre-approval rules, users can submit an elevation request through ABR. The request enters the approval queue and is processed according to the defined SLA.

3.3.2 Operational Flow

- User attempts to install an approved application.
- ABR evaluates the installer against pre-approval rules.
- If the installer matches a rule: elevation is granted automatically. The application installs without user interaction.
- If no rule matches: ABR presents an elevation request form. The user submits the request with a business justification.
- IT reviews and approves or denies the request within the defined SLA.
- All elevation events (auto-approved and manually approved) are logged in the ABR audit trail.

3.3.3 Constraints and Controls

- Pre-approval rules specify exact file paths, publisher certificates, or hash values. Broad wildcards are not permitted.
- Rules are managed centrally by the IT team through the ABR portal.
- New pre-approval rules are tested in the lab environment before deployment to production.
- Non-approved applications require manual approval, subject to the SLA defined in the approval workflow.

3.4 Use Case 4: Permission Revocation and Administrator Inventory

Use Case ID	UC-04
Title	Permission Revocation and Administrator Inventory
User Group	IT Administrators (operational use case)
Access Model	ABR Portal — Inventory and Remote Revocation
ABR Feature	Local Administrator Monitoring, Remote Revocation
Network Requirement	Target devices must sync with ABR portal
Validated In	ABR Test 6 (Local Admin Monitoring), Realization Report Chapter 3

Table 5: Use Case 4 specification — Permission revocation and administrator inventory

3.4.1 Description

This use case is operational rather than user-facing. Before permanent local administrator rights can be removed from the device fleet, the IT team needs complete visibility into the current state of privilege distribution. ABR provides a built-in local administrator inventory that detects, reports, and manages users with permanent local administrator group membership on each managed device.

The inventory includes the username, domain, administrator status, and the date the account was last detected in the local Administrators group. The IT team can use this inventory to identify accounts that should not have administrator rights, verify that ABR elevation rules are in place for accounts that legitimately need elevation, and then remotely revoke permanent admin rights through the ABR portal without requiring physical access to the device.

3.4.2 Operational Flow

- IT administrator opens the ABR portal and navigates to the Devices section.
- For each device, ABR displays the full inventory of local administrator accounts.
- IT reviews each account against the approved user group access model (Table 1 of this document).
- Accounts that should not have permanent admin rights are flagged for revocation.
- IT verifies that ABR elevation rules are configured for the affected user before revoking admin rights.
- Admin rights are revoked remotely through the ABR portal.
- The revocation is logged in the ABR audit trail with the administrator who performed the action, the target account, and the timestamp.

3.5 Use Case 5: Compliance Audit and Elevation Reporting

Use Case ID	UC-05
Title	Compliance Audit and Elevation Reporting
User Group	IT Administrators, Compliance Team
Access Model	ABR Portal — Audit Logs and SIEM Export
ABR Feature	Audit Logging, Reporting Dashboard, SIEM Export
Compliance Framework	ISO 27001, GDPR
Validated In	All ABR tests (audit trail verified in each), Realization Report Chapter 3

Table 6: Use Case 5 specification — Compliance audit and elevation reporting

3.5.1 Description

Soudal's compliance obligations under ISO 27001 and GDPR require demonstrable audit trails for administrative actions performed on managed endpoints. Every privilege elevation event must be logged with sufficient detail to answer the five audit questions: who elevated, on which device, what action was performed, when it happened, and whether it was approved.

ABR provides comprehensive audit logging across all elevation types. Every elevation event, whether it is an online approval, an offline PIN elevation, an auto-approved pre-approval rule match, or an admin session, is logged with timestamp, user identity, device identity, application or action, approval outcome, and session duration.

3.5.2 Audit Data Fields

Field	Description
Timestamp	Date and time of the elevation event (UTC)
User Identity	Entra ID user principal name of the requesting user
Device Identity	Device name and Intune device ID
Elevation Type	Run As Admin, Admin Session, Offline PIN, Pre-Approved Rule
Application / Action	Executable name and file path of the elevated process
Approval Outcome	Approved, Denied, Auto-Approved (rule match), Offline PIN
Approver	Identity of the administrator who approved the request (if applicable)
Session Duration	Length of the admin session (for session-based elevations)
Business Justification	User-provided reason for the elevation request (if submitted)
Offline Indicator	Flag indicating whether the elevation occurred while the device was offline

Table 7: ABR audit data fields captured for each elevation event

3.5.3 Reporting Capabilities

- The ABR portal provides a centralized dashboard showing elevation activity across all managed devices.
- Logs can be filtered by user, device, elevation type, date range, and approval outcome.
- Audit data can be exported for integration with external SIEM platforms.
- The compliance team can generate periodic reports showing elevation frequency, approval rates, denial rates, and offline elevation frequency.
- Reports support ISO 27001 control evidence requirements and GDPR accountability obligations.

4. Access Model Summary

The following table provides a consolidated view of the access model for each user group, including the ABR configuration, approval requirements, and audit obligations.

User Group	ABR Elevation Mode	Approval Required	Offline Capable	Audit Level
Engineering / Factory	Permanent Admin + Offline PIN	No (pre-approved tier)	Yes (Offline PIN)	Full (including offline sync)
Service Desk	Permanent Admin Session	No (pre-approved tier)	No (requires network)	Full (session-level logging)
Power Users	Temporary Sessions (15 min – 2 hr)	Yes (request-based)	No (requires network)	Full (per-request logging)
Standard Users	App-Specific Only	Auto for rules; manual for new apps	No (requires network)	Full (per-elevation logging)

Table 8: Consolidated access model summary across all user groups

5. Approval Workflow by User Group

The approval workflow is designed to minimize friction for users whose elevation needs are predictable and well-defined, while maintaining a controlled process for ad-hoc and edge-case requests. The following table specifies the approval behavior for each user group and request type.

User Group	Request Type	Approval Behavior	SLA
Engineering	Offline PIN elevation	No approval (PIN-based)	Immediate
Engineering	Online Run As Admin	No approval (permanent tier)	Immediate
Service Desk	Admin Session	No approval (permanent tier)	Immediate
Power Users	Temporary Session	IT approval required	Standard: within 15 minutes
Standard Users	Pre-approved app	Auto-approved (rule match)	Immediate
Standard Users	New application request	IT approval required	Standard: within 15 minutes
Any	Urgent / Break Glass	Phone verification + IT grant	Within 5 minutes
Any	After-hours request	On-call IT contact	Within 10 minutes

Table 9: Approval workflow by user group and request type

6. Revision and Maintenance

This use case documentation should be treated as a living document and reviewed at the following intervals:

- After each deployment phase (Pilot, Expand, Standard Users) to incorporate lessons learned and rule adjustments.
- Quarterly, as part of the regular IT security review cycle, to verify that user group assignments remain current.
- When new user groups, applications, or operational scenarios are identified that require changes to the access model.
- When organizational changes at Soudal (new departments, acquisitions, restructuring) affect the user group composition.

All changes to the access model should be documented in this attachment with a version number, date, and brief description of the change. The IT team is responsible for ensuring that ABR portal configurations remain aligned with the documented access models at all times.