PROJECT PLAN

Privilege Management Modernization at Soudal

Muhammad Zubair
Student Bachelor Applied Computer Science

2025 – 2026

Summary

This project plan documents the scope, objectives, and methodology of the bachelor work placement carried out at Soudal NV during the 2025–2026 academic year. The placement addresses a concrete security and operational gap in Soudal's endpoint environment: the continued reliance on permanent local administrator rights across several user groups, including Engineering, Service Desk, and selected power users. This arrangement, while convenient for daily operations, creates an expanded attack surface, weakens compliance posture under ISO 27001 and the General Data Protection Regulation, and leaves administrative actions without a complete audit trail.

The work proposes to replace these permanent rights with a controlled, temporary, and fully auditable just-in-time privilege elevation workflow. Two candidate tools have been identified for structured evaluation: Admin By Request, a third-party cloud-based privileged access management platform, and Microsoft Endpoint Privilege Management, a native add-on to Microsoft Intune. Both tools will be assessed in a controlled laboratory environment against Soudal's operational requirements, with the most suitable solution selected for phased deployment to production. The project is scheduled over thirteen weeks, from 23 February to 22 May 2026, and is structured into three phases: research and evaluation, pilot rollout, and full migration.

On completion, Soudal will have a validated privilege elevation solution deployed for the in-scope user groups, supported by documented training material and operational procedures. The project will deliver measurable reductions in attack surface, improved compliance evidence, and a defined approval workflow for elevation requests. The remainder of this document presents the company background, project objectives, business case, planning, team responsibilities, scope, risks, deliverables, and conclusion.

Table of Contents

1. Company and Background

Soudal NV is a Belgian family-owned manufacturer of sealants, adhesives, and polyurethane foams for the professional construction and DIY markets. The company was founded in 1966 by Vic Swerts in Turnhout, Belgium, where its global headquarters remains today. From its origins as a small regional supplier, Soudal has grown into one of the largest independent manufacturers of chemical building products in the world, with operations on every inhabited continent. The company remains privately owned by the Swerts family, which allows for a long-term strategic horizon that is reflected in its sustained investment in production capacity, research and development, and digital infrastructure.

Soudal currently employs more than 3,500 people across more than 100 countries, with manufacturing sites and distribution centres in Europe, North and South America, Asia, the Middle East, and Africa. The company's product portfolio includes more than 800 product variants, ranging from silicone sealants and acrylic compounds to high-performance industrial adhesives and polyurethane foam systems. Soudal supplies major construction, automotive, and industrial sectors, and its products are present in projects ranging from residential renovations to large infrastructure work. In 2024 the company reported a turnover exceeding one billion euros, reflecting consistent double-digit growth over the past decade.

From an information technology perspective, Soudal operates a centralized ICT function based at the Turnhout headquarters that supports the global organization. The internal IT estate has migrated almost entirely to Microsoft cloud technologies in recent years, including Microsoft Intune for endpoint management, Microsoft Entra ID for identity, and Microsoft 365 for productivity. This Microsoft-first posture provides the operational context for the present project. The placement is hosted by the ICT Infrastructure team at the Turnhout headquarters, under the guidance of work placement mentors Dries Wuyts, Rob Verbiest, and Eduard Claessen, with academic supervision from Brent Pulmans at Thomas More.

1.1 IT Environment

The Soudal endpoint and identity infrastructure is built almost entirely on Microsoft cloud technologies. The identity backbone is a hybrid model in which on-premises Active Directory is synchronized one-way into Microsoft Entra ID through Entra Connect. Entra ID, formerly known as Azure Active Directory, is Microsoft's cloud identity platform and acts as the authoritative source for authentication, licensing, and access control across all Microsoft cloud services. All endpoint devices, including laptops and desktops, are enrolled into Microsoft Intune through Autopilot, Microsoft's cloud-based provisioning solution. Microsoft Intune is Microsoft's mobile device management and mobile application management service; it allows the ICT team to enforce compliance policies, distribute configuration profiles, and deploy applications to devices in a fully cloud-managed model.

On top of this management layer, Soudal applies privilege elevation tooling to control administrative access on endpoints. Two candidate solutions are currently under evaluation as part of this project. Admin By Request, abbreviated as ABR, is a third-party privileged access management platform that provides a cloud portal for approving and monitoring elevation requests. Microsoft Endpoint Privilege Management, abbreviated as EPM, is a native add-on to Microsoft Intune that implements privilege elevation through virtual elevation accounts at the kernel level. Separately, Soudal operates PAM360, a privileged access management product used for infrastructure-level scenarios such as server administration. PAM360 sits at the identity layer and is distinct from the endpoint-level elevation tooling that this project evaluates. The overall environment also accommodates multiple network contexts, including the corporate office network, isolated factory networks, and remote access for staff working off-site, each of which imposes its own constraints on how privilege elevation must behave.

1.2 Hybrid Architecture Overview

The diagram below illustrates the hybrid identity and device management architecture at Soudal. User accounts are created and maintained in the on-premises Active Directory, and Entra Connect performs a one-way synchronization into Microsoft Entra ID, which is the authoritative source for cloud authentication and Conditional Access enforcement. Devices are enrolled into Microsoft Intune through Autopilot, and configuration, compliance, and endpoint security policies are distributed from the Intune admin centre. The privilege elevation tooling selected by this project will operate on top of this management layer, against the device population that Intune already controls. PAM360 sits separately at the identity layer and addresses infrastructure access scenarios that fall outside the scope of endpoint-level privilege elevation.

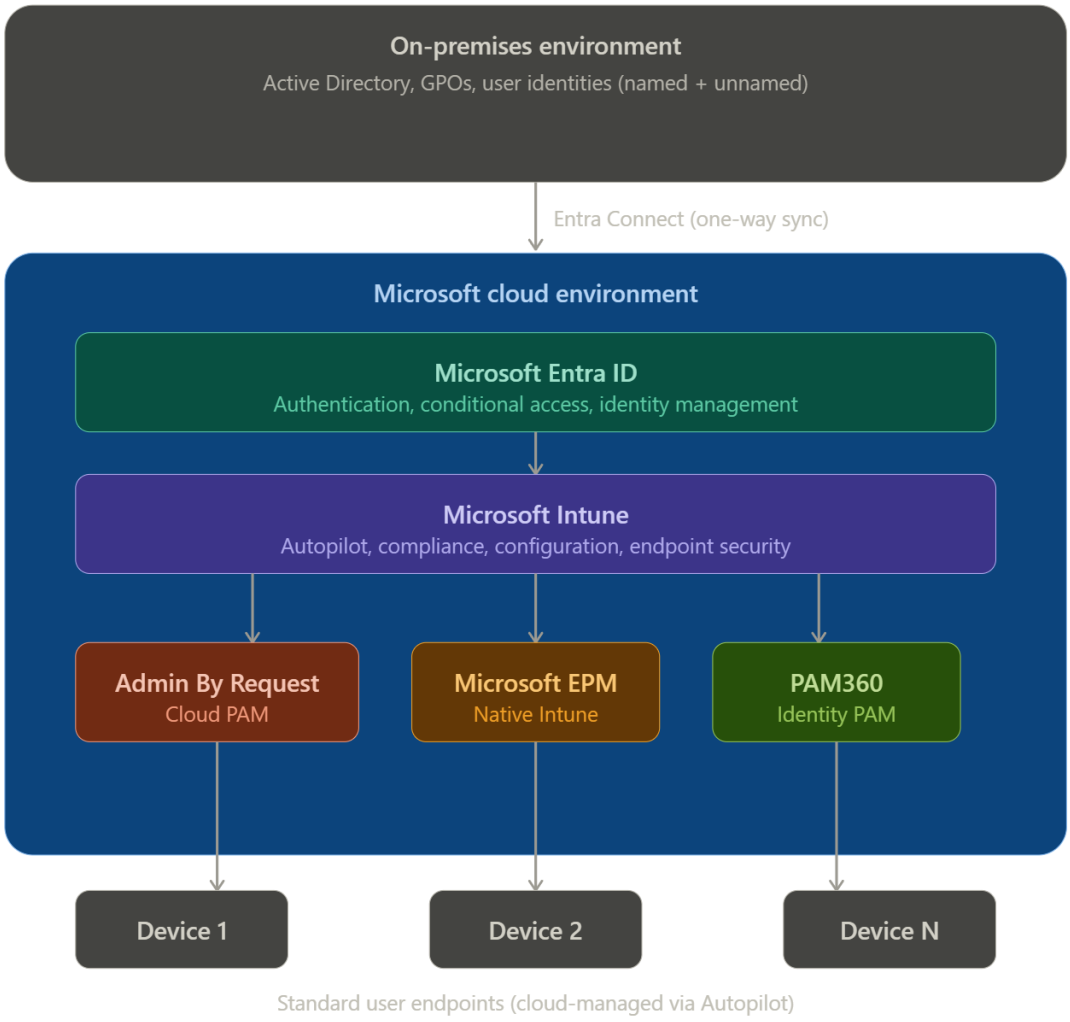

Figure 1: Hybrid identity and device management architecture at Soudal

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

1.3 Identity and Access Architecture

Soudal's identity model distinguishes between two account types based on user role and operational context. Named accounts are issued to full-time employees and provide a complete access profile, including email, productivity applications, and Soudal's internal systems. Unnamed accounts are used for service contexts and for shared factory floor scenarios where individual identification is not feasible; these accounts are restricted to factory networks only and cannot authenticate from outside the production environment. Conditional Access policies in Microsoft Entra ID govern access to all cloud resources based on a combination of user identity, device compliance status, network location, and risk signals. Software-as-a-service systems integrated into the environment, such as PAM360, authenticate through Microsoft Entra ID to ensure consistent identity governance across the estate. Device compliance status, as reported by Microsoft Intune, feeds directly into Conditional Access decisions, meaning that only compliant devices are permitted to receive elevated privileges or access sensitive resources.

1.4 Problem Statement

The Soudal endpoint environment continues to rely on permanent local administrator rights for several user groups, including Engineering staff, Service Desk operators, and selected power users. This arrangement has historical roots in operational pragmatism: granting these users local administrator rights allowed them to perform technical tasks without raising tickets to the ICT team. However, the permanence of the rights creates a number of risks that conflict with modern security baselines and Soudal's compliance obligations. Permanent rights expand the attack surface available to an adversary who compromises an endpoint, enabling lateral movement, persistence, and credential harvesting. They also leave audit trails incomplete, since elevated actions are not centrally logged. This weakens Soudal's compliance posture under ISO 27001, which requires evidence of access control, and under the General Data Protection Regulation, which demands accountability for actions affecting personal data.

The current model also creates operational overhead. The Service Desk handles ad-hoc privilege requests manually, and there is no centralized logging of administrative actions performed by end users. The principle of least privilege, which holds that users should hold only the permissions necessary for their work and only for as long as required, is not consistently applied across the device fleet. The cumulative effect is an environment where a single compromised endpoint can yield broad administrative reach, where compliance evidence is fragmented, and where IT resources are spent on routine privilege management instead of higher-value work.

1.5 Proposed Solution

This project proposes to replace permanent local administrator rights with a controlled, temporary, and fully auditable privilege elevation workflow based on just-in-time access. Just-in-time access, abbreviated as JIT, is a privilege model in which elevated rights are granted only at the moment they are needed, only for the duration required, and only after a defined approval or policy check. The two candidate tools identified for evaluation, Admin By Request and Microsoft Endpoint Privilege Management, both implement variations of this model. The project will evaluate both tools in a controlled laboratory environment, select the most appropriate solution for Soudal's specific operational requirements, and produce a phased deployment strategy that can be applied to production endpoints with minimal disruption to user productivity.

2. Objectives

The overall objective of this project is to modernize Soudal's privilege management approach by eliminating permanent local administrator accounts on Intune-managed endpoints and replacing them with a secure, auditable, just-in-time elevation mechanism. The solution must preserve productivity for users who legitimately require elevated permissions while reducing the organization's overall attack surface and improving compliance posture. The objectives are described below in two parts: the primary objectives that define what the project will achieve, and the success criteria that define how achievement will be measured.

2.1 Primary Objectives

The primary technical objective of the project is the removal of permanent local administrator rights from all Intune-managed devices that fall within scope. Removal will be paired with the introduction of seamless, time-bounded elevation workflows so that legitimate business operations are not disrupted. The combined effect should be a measurable reduction in the risk of lateral movement following an endpoint compromise. From the user perspective, the project must maintain or improve productivity for the Engineering, Service Desk, and power user groups; this is a non-negotiable design constraint, as a solution that creates significant friction will not see adoption regardless of its security benefits.

Beyond the technical implementation, the project pursues three further objectives. First, it must ensure that all elevation events are logged with sufficient detail to support audit and reporting requirements under ISO 27001 and the General Data Protection Regulation. Second, it must align Soudal's endpoint privilege management with Microsoft cloud-native security guidance, in keeping with the wider Microsoft-first posture of the IT estate. Third, the work should establish a scalable foundation that supports further security improvements in subsequent project cycles, rather than producing a point solution that solves only the immediate problem.

2.2 Success Criteria

The following measurable criteria will be used to evaluate the success of the project. Each criterion is paired with a defined measurement method to ensure that the assessment is evidence-based rather than subjective.

Metric	Target	Measurement Method
Permanent local administrator account reduction	95% or greater	Active Directory and local administrator inventory audit
Elevation request approval rate	95% or greater	Tool reporting dashboard
Audit trail coverage	100% of elevation events	Log aggregation and verification
User productivity impact	Less than 5% negative	Post-implementation user survey
Device compliance and stability	99% or greater	Intune device compliance reports

Table 1: Project success criteria and measurement methods

2.3 Expected Learning Outcomes

Alongside the deliverables expected by Soudal, this placement is an academic exercise with its own personal learning goals. On the technical side, I expect to gain practical, hands-on experience with privileged access management and the just-in-time elevation model, including the configuration and day-to-day operation of Admin By Request and Microsoft Endpoint Privilege Management. I also expect to deepen my understanding of the Microsoft cloud management plane, in particular Microsoft Intune, Microsoft Entra ID, Conditional Access, and device compliance, and to learn how these services work together to enforce endpoint security in a real enterprise environment.

On the professional side, I expect to strengthen the skills needed to run a structured technical evaluation, from defining weighted criteria and designing reproducible laboratory tests to documenting evidence-based recommendations. I also expect to improve how I communicate technical findings to different audiences, since the project requires presenting both to the technical ICT team and to non-technical management at Soudal. Finally, the placement should give me experience working to professional standards within an established ICT team, managing my own planning across a thirteen-week project, and adapting to requirements as they evolve.

3. Business Case

The decision to invest in a modern privilege elevation solution at Soudal is driven by three interlocking factors: a measurable reduction in attack surface, alignment with compliance obligations, and a reduction in operational overhead for the Service Desk team. Industry research, including the annual Verizon Data Breach Investigations Report, consistently identifies credential abuse and privilege misuse as among the most common attack vectors in enterprise environments. Soudal's compliance obligations under ISO 27001 and the General Data Protection Regulation require demonstrable audit trails for administrative actions and evidence that the principle of least privilege is applied across the device fleet. The current state, with permanent local administrator rights distributed across multiple user groups, does not meet either of these requirements.

A structured evaluation of candidate tools is necessary because the two leading solutions on the market, Admin By Request and Microsoft Endpoint Privilege Management, differ substantially in architecture, feature set, licensing model, and integration depth. The two tools are not interchangeable, and selecting one over the other has significant consequences for the long-term operational model at Soudal. A decision made on the basis of marketing material or vendor demonstrations alone would carry unacceptable risk: features that look equivalent on paper may behave differently under real Soudal workloads, and architectural differences may only surface during hands-on deployment. A controlled laboratory evaluation, in which both tools are deployed against representative workloads and assessed against the same set of criteria, is the only reliable way to produce an evidence-based recommendation. The evaluation will also surface integration and licensing constraints that would otherwise emerge only after a commitment has been made, when the cost of changing course would be considerably higher.

The following sections present each candidate tool, followed by a feature comparison matrix that will guide the recommendation. The detailed evaluation criteria, weighted scoring, and final recommendation will be documented in the realization report.

3.1 Admin By Request (ABR)

Admin By Request is a third-party software-as-a-service platform dedicated to privileged access management on endpoints. It is operated as a cloud service with its own management portal, which is independent of Microsoft Intune. ABR provides multiple elevation modes, including a Run As Administrator workflow for one-off application elevations, time-bounded Admin Sessions for sustained administrative work, and an Offline PIN mechanism for elevation when network connectivity is unavailable. The platform supports Windows, macOS, and Linux endpoints from a single agent. Although ABR is typically deployed through Microsoft Intune as a line-of-business application, it operates independently of the Intune management layer once installed; the ICT team manages elevation policies, approval workflows, and audit logs through the ABR cloud portal. ABR

includes pre-built integrations with major identity providers and security information and event management platforms, which simplifies onboarding into existing operational tooling.

3.2 Microsoft Endpoint Privilege Management (EPM)

Microsoft Endpoint Privilege Management is a native Microsoft solution that integrates tightly with the Microsoft Intune Suite and the broader Microsoft cloud ecosystem. Unlike ABR, EPM is configured entirely within the Microsoft Intune admin centre, which removes the need for a second management portal or a separate vendor relationship. Privilege elevation is implemented through virtual elevation accounts at the kernel level, meaning that users never actually join the local Administrators group; instead, individual applications can be elevated through a controlled policy mechanism. EPM is currently available only for Windows endpoints. The product is sold as a paid add-on to Microsoft 365 E5 or as a component of the Intune Suite licensing bundle. Integration extends directly to Microsoft Entra ID for identity, Microsoft Intune for device management, and Microsoft Defender for Endpoint for security telemetry.

3.3 Feature Comparison

The table below presents a side-by-side comparison of Admin By Request and Microsoft Endpoint Privilege Management across the dimensions most relevant to Soudal's requirements. This comparison is preliminary and is intended to frame the evaluation; the detailed weighted scoring and final recommendation will be documented in the realization report after the laboratory testing phase.

Feature	Admin By Request (ABR)	Microsoft EPM
Platform	Cloud SaaS, independent portal	Native within Microsoft Intune
Operating system support	Windows, macOS, Linux	Windows only
Audit logging	Comprehensive cloud audit logs	Integrated with Intune and Defender
Elevation modes	Run As Admin, Admin Session, Offline PIN, Pre-approved rules	Per-application policies via virtual elevation accounts
Deployment	Deployed through Intune; operates independently	Native Intune configuration
Licensing	Separate per-device or per-user licence	Included in Intune Suite or Microsoft 365 E5 add-on
Integration	Third-party SIEM and identity provider integrations	Native Microsoft ecosystem integration
Approval workflows	Flexible, customizable approval flows	Policy-based with conditional rules

Table 2: Feature comparison between Admin By Request and Microsoft Endpoint Privilege Management

4. Planning

The project is scheduled over thirteen weeks, running from 23 February 2026 to 22 May 2026. The work is structured into three phases: research and evaluation, pilot rollout, and full migration. Each phase has a defined set of deliverables and milestones, which are summarized in the timeline table at the end of this section. The phasing reflects the natural progression from understanding the candidate tools, through validating the selected tool against real workloads, to deploying the validated solution into production.

4.1 Phase 1 — Research and Evaluation (Weeks 1–6)

The first phase concentrates on building a thorough understanding of the two candidate tools and producing an evidence-based recommendation. The work begins with a detailed technical analysis of the Admin By Request and Microsoft Endpoint Privilege Management architectures, drawing on vendor documentation, available case studies, and informal contact with reference customers where possible. This is followed by hands-on functional testing of both tools in an isolated laboratory environment, in which a representative set of elevation workflows is executed against each tool to validate that documented behaviour matches actual behaviour. A feature comparison matrix and weighted evaluation criteria are developed in parallel, ensuring that the comparison is both consistent and aligned with Soudal's operational priorities.

Integration testing with Microsoft Intune and Microsoft Entra ID is performed during this phase to confirm that each tool can be deployed and managed within Soudal's existing cloud management plane. A security assessment, including an analysis of plausible attack vectors against each solution, accompanies the functional testing. An indicative cost analysis and total cost of ownership comparison provides the financial dimension of the evaluation. The phase concludes with a presentation of findings to Soudal leadership on 20 March 2026, at which the recommendation is delivered along with the supporting evidence.

4.2 Phase 2 — Pilot Rollout (Weeks 7–10)

The second phase moves the recommended solution from the laboratory into a controlled pilot deployment. The selected tool is deployed to a pilot group of approximately ten to twenty devices, drawn from the Engineering and Service Desk teams in coordination with the work placement mentors. Elevation policies, approval workflows, and audit logging are configured to reflect the operational reality of these user groups. During the pilot, audit logs and user behaviour are actively monitored, and a feedback channel is established so that pilot users can report friction or unexpected behaviour. Compliance and reporting requirements against ISO 27001 expectations are validated during this phase, and any issues encountered are documented along with the corresponding remediation steps. The phase concludes with a set of recommendations for the full migration based on observed pilot results.

4.3 Phase 3 — Full Migration (Weeks 11–13)

The third and final phase brings the validated solution into broader production use. Remaining local administrator accounts within the project scope are converted to standard user accounts, and the elevation policies validated during the pilot are applied across the in-scope device population. Monitoring dashboards and a reporting cadence are configured so that the ICT team can track elevation activity and compliance status without manual reporting. End-user training materials and IT administrator documentation are delivered during this phase, accompanied by targeted communication to affected user groups. Elevation rules are tuned based on early operational feedback, and the final implementation report and supporting documentation are prepared for submission to Thomas More and to Soudal.

4.4 Timeline and Milestones

The following timeline summarizes the activities and deliverables for each week of the placement, along with the key milestone presentations to Thomas More and Soudal leadership.

Timeline	Activities	Deliverables
Weeks 1–2	Environment discovery, requirements gathering, stakeholder meetings	Environment documentation
Week 3	Tool evaluation planning and laboratory setup	Lab environment ready for testing
Week 4	Project Plan presentation at Thomas More	Project Plan document and presentation
Weeks 5–6	Hands-on testing of Admin By Request and Microsoft EPM	Testing documentation and result logs
20 March	Presentation of tool comparison to Soudal leadership	Tool comparison matrix and recommendation
Weeks 7–8	Migration planning, policy design, pilot preparation	Migration strategy document
Weeks 9–10	Pilot deployment, monitoring, feedback collection	Pilot testing report
Weeks 11–12	Full rollout preparation and execution	Implementation guide and rollout documentation
Week 13	Final reports, project reflection, summary preparation	Realization document, summary, and final deliverables

Table 3: Project timeline, activities, and deliverables

5. Progress Reporting

Progress is reported through three complementary channels to ensure visibility for both Soudal and Thomas More throughout the placement. The combination of written reports, academic supervision meetings, and ongoing contact with the work placement mentors at Soudal provides regular feedback loops at different levels of detail.

Written status reports are submitted on a regular basis, documenting the work completed during the period, progress against the planned milestones, challenges encountered, and the plan for the next period. Academic supervision meetings with Brent Pulmans, the academic supervisor at Thomas More, take place at two key moments during the placement: an interim meeting at the midpoint of the work, and a final review meeting near the conclusion of the placement. Between these scheduled meetings, contact with the academic supervisor is maintained through email correspondence and asynchronous feedback on draft deliverables. At Soudal, contact with the work placement mentors, Dries Wuyts, Rob Verbiest, and Eduard Claessen, is more frequent and informal; regular check-ins provide technical guidance and operational coordination as the project progresses. Stakeholder presentations at key project phases, including the initial project plan presentation, the tool comparison and recommendation presentation, and the final implementation review, provide structured opportunities for broader audiences to engage with the project.

6. Team and Responsibilities

This section sets out the roles and responsibilities of the three parties involved in the placement: the student intern, the academic supervisor at Thomas More, and the work placement mentors at Soudal. A shared understanding of these roles is essential to ensure that responsibilities do not fall between the parties and that the project receives the support it needs at each stage.

6.1 Student Intern — Muhammad Zubair

As the student intern, my responsibility is to lead the technical evaluation of Admin By Request and Microsoft Endpoint Privilege Management, to conduct the hands-on laboratory testing, and to develop the feature comparison matrix and weighted scoring that will support the recommendation. I am responsible for presenting findings to Soudal leadership and to Thomas More academic staff at the agreed milestones, and for designing and executing the pilot deployment plan in coordination with the work placement mentors. I will also produce the training materials and administrator documentation that accompany the deployment, monitor the success metrics defined in Section 2.2 during the pilot and full migration phases, collect user feedback to inform tuning decisions, and prepare the final implementation report and personal reflection at the end of the placement.

6.2 Academic Supervisor — Brent Pulmans, Thomas More

Brent Pulmans, the academic supervisor at Thomas More, provides academic guidance and feedback on the project methodology and documentation throughout the placement. The academic supervision takes the form of two scheduled meetings during the placement, supplemented by ongoing asynchronous feedback through email correspondence and written reviews of draft deliverables. The academic supervisor reviews the project deliverables for academic alignment and ensures that the placement work meets the requirements of the Bachelor of Applied Computer Science programme at Thomas More.

6.3 Work Placement Mentors — Soudal NV

Dries Wuyts, Rob Verbiest, and Eduard Claessen serve as the work placement mentors at Soudal. Their responsibilities include providing access to the laboratory environment and the supporting test infrastructure, sharing environment documentation and technical specifications about the Soudal ICT estate, and reviewing technical findings as they emerge during the evaluation. They also provide the operational context that informs the design of elevation policies and approval workflows. Where required, the mentors coordinate with the broader Soudal ICT team to gather stakeholder feedback within the organization and to escalate or resolve issues that fall outside the immediate scope of the project.

7. Integration with Microsoft Intune

Microsoft Intune is the central platform for endpoint management, compliance enforcement, and policy distribution within Soudal's environment. Any privilege elevation solution selected through this project must integrate cleanly with Intune to avoid creating a parallel management plane, which would increase operational complexity and undermine the value of the existing cloud-first management model. The two candidate tools approach this integration in different ways, and the difference has practical consequences for the operational model that will be in place after deployment.

All in-scope devices are managed through Microsoft Intune, which serves as the foundation on which the privilege elevation solution will be layered. Microsoft Endpoint Privilege Management is configured natively within Intune through policy assignment, leveraging existing Entra ID security groups and device compliance status; it requires no additional management surface beyond the Intune admin centre. Admin By Request, in contrast, is deployed through Intune as a line-of-business application but operates through its own independent management portal once installed; configuration, policy management, and audit review take place in the ABR cloud portal rather than in Intune. In both cases, Conditional Access ensures that privilege elevation is only available on compliant devices, and device compliance status feeds directly into elevation decisions. All configuration changes follow the existing Intune governance and change management processes at Soudal.

8. Project Scope

This section defines the boundaries of the project, both what is included and what is explicitly excluded. The scope decisions reflect deliberate choices made in agreement with the work placement mentors at Soudal, balancing the ambition of the project against the constraints of a thirteen-week placement and the readiness of the surrounding environment.

8.1 In Scope

The project includes the comprehensive evaluation of Admin By Request and Microsoft Endpoint Privilege Management as candidate privilege elevation solutions for Soudal's endpoint estate. The evaluation covers feature comparison, gap analysis, weighted scoring, and a security and audit capability assessment for both candidate tools. The project also includes the pilot deployment of the selected solution on test devices within the Engineering and Service Desk user groups, the development of a migration strategy and phased rollout plan, and the production of end-user training materials and administrator documentation. An indicative cost analysis and licensing model comparison is included to inform Soudal's procurement decision.

8.2 Out of Scope

Several adjacent areas are explicitly excluded from the project. A complete network redesign is out of scope, as the existing network architecture is sufficient for the proposed elevation workflows. Replacement of non-Windows infrastructure is out of scope, since the evaluation focuses on the Windows endpoint estate, which represents the majority of in-scope devices. Identity governance changes beyond what is required for elevation are out of scope; broader identity governance is addressed by Soudal's existing PAM360 implementation. VPN and network access changes are managed by a separate Soudal team and are not affected by this project. The replacement or extension of PAM360 itself is out of scope: PAM360 remains the platform of record for infrastructure-level privileged access at Soudal. Finally, support for legacy on-premises devices is excluded; the project assumes Intune-managed devices only.

9. Risks and Mitigation

The table below identifies the key risks to project delivery, their estimated probability and impact, and the planned mitigation strategy for each. The risk register will be reviewed during supervision meetings with the work placement mentors at Soudal and updated as new information becomes available during the placement.

Risk	Probability	Impact	Mitigation Strategy
Privilege elevation policies disrupt existing user workflows	Medium	High	Pilot on an isolated device population first; develop rollback procedures before broader rollout
User resistance to losing permanent local administrator rights	Medium	Medium	Communicate the security and compliance benefits early; provide targeted training; phase the rollout
Conditional Access blocks unnamed factory accounts after policy changes	Low	High	Validate all Conditional Access policies in the lab before applying them to production groups
Integration issues between elevation tooling and PAM360	Low	Medium	Test integration early in Phase 1; coordinate with the PAM360 administrator at Soudal
Licensing cost exceeds initial estimates	Medium	Medium	Engage Microsoft and ABR licensing contacts early; compare licensing models in the business case
Pilot user group adoption is slower than planned	Medium	Low	Designate champions in each pilot team; provide responsive support during the pilot window

Table 4: Project risk register and mitigation strategies

10. Deliverables

The following deliverables will be produced over the course of the placement. Each deliverable is reviewed by the appropriate audience before being marked as complete, ensuring that quality and relevance are maintained throughout the project.

The Project Plan, namely this document, is delivered in Week 4 and presented at Thomas More as part of the academic milestone. The Tool Comparison Matrix and Recommendation is produced in Week 6 and presented to Soudal leadership on 20 March, providing the evidence base on which the selected solution is chosen. The Hands-On Laboratory Testing Report, completed in Week 6, documents the test procedures, results, and observations from the laboratory evaluation of both candidate tools. The Migration Strategy Document, delivered in Week 8, sets out the phased deployment approach for the selected solution. The Pilot Testing Report, produced in Week 10, captures the outcomes and lessons of the pilot deployment, including user feedback and operational metrics.

End-User and Administrator Training Materials are delivered in Week 12, providing the content needed to support adoption of the new elevation workflows across the in-scope user groups. The Final Realization Report is submitted to Thomas More in Week 13, accompanied by the Summary, a concise document that condenses the project context, objectives, methodology, and outcomes for readers who require an executive overview without the full body of the report. The Personal Reflection completes the academic deliverable set and accompanies the final submission.

11. Conclusion

This project addresses a concrete operational and security gap in Soudal's endpoint environment by replacing permanent local administrator rights with a controlled, temporary, and fully auditable privilege elevation mechanism. The transition aligns Soudal's privilege management practices with Microsoft cloud-native security guidance and supports compliance obligations under ISO 27001 and the General Data Protection Regulation. The choice between the two candidate tools, Admin By Request and Microsoft Endpoint Privilege Management, will be made on the basis of evidence drawn from controlled laboratory testing rather than from vendor material, and will reflect the specific operational priorities of Soudal as identified during the placement.

The evaluation phase will produce a clear, evidence-based recommendation, supported by hands-on testing and weighted scoring. The pilot phase will validate the recommended solution against real user workflows before any broader rollout is undertaken, and the migration phase will deliver a measurable reduction in attack surface together with an improvement in audit coverage for elevated actions. The phased approach ensures that risk is managed deliberately throughout the placement and that disruption to ongoing Soudal operations is minimized.

On completion of the placement, Soudal will have a documented and validated privilege elevation solution in production for the in-scope user groups, supported by training materials and operational documentation. The Service Desk team will have a defined approval workflow for elevation requests, and the ICT team will have centralized visibility into elevation events for ongoing security monitoring. The work also establishes a foundation for further endpoint security improvements at Soudal, including potential extension of the elevation model to additional user groups in subsequent project cycles.