

Enterprise XR Device Lifecycle Management –Best Practices for Secure Commissioning and Decommissioning

Category:
Business Process Innovation Issues



Problems this Research Would Address

1. **XR devices store sensitive enterprise data** - configurations, credentials, application content, and operational information —yet most organizations have no defined procedure for securely wiping and decommissioning them.
2. When devices are **broken, replaced, or returned**, they frequently end up in desk drawers or storage rooms with corporate data intact, creating data exposure risks that IT and security teams cannot accept.
3. **Inconsistent commissioning practices** slow rollouts, create deployment errors, and leave IT teams unable to manage XR programs at scale
 - a) Security teams refuse to approve XR programs without evidence of a reliable decommissioning process
 - b) MDM tools designed for smartphones are not fully adapted to the unique characteristics of AR and XR hardware.
 - c) Without a shared best practice framework, every organization is solving the same problem independently and inconsistently.

How would this research be conducted?

1. **Interview enterprise IT and security professionals** - conduct structured interviews with at least 15 practitioners responsible for XR device management to document current commissioning and decommissioning practices, risks identified, and gaps in existing tooling.
2. **Evaluate MDM and device management solutions** - review and assess at least 8 tools (e.g., Workspace ONE, SOTI, Microsoft Intune) for their current XR device management capabilities, covering remote wipe, application provisioning, and compliance reporting.
3. **Map the XR device lifecycle** - define the full lifecycle stages (procurement, provisioning, active use, maintenance, decommissioning) and document what security and operational requirements exist at each stage based on practitioner input.
4. **Identify framework gaps** - cross-reference practitioner findings with MDM tool capabilities to surface the specific gaps where no adequate solution currently exists, and document the security risks these gaps create.

Project Deliverables

Enterprise XR Device Lifecycle Management Framework - a structured best practice document covering at minimum 5 lifecycle stages with security and operational requirements at each stage.

MDM Tool Capability Matrix - a comparative assessment of at least 8 MDM solutions against XR-specific device management requirements, helping enterprises select the right tooling.

Implementation checklist - a practical, actionable checklist for IT teams to use when commissioning new XR devices and decommissioning retired or replaced ones.

Published best practices guide - a public-facing AREA report with findings, tool recommendations, and a reusable framework that security and IT teams can present internally to build programme approval

Executive summary of findings for **public release** and **member exclusive webinar**

How would this research be conducted

1. **Synthesise interview and tool evaluation findings**—cross-reference practitioner data with MDM capability assessments to produce a validated gap analysis and risk register for XR device lifecycle management.
2. **Draft the Lifecycle Management Framework**—develop the framework document with input from a working group of AREA member IT and security practitioners, ensuring it reflects real enterprise constraints and approval requirements.
3. **Pilot-test the implementation checklist**—validate the checklist with at least 3 member organisations before final publication, incorporating feedback to ensure practical usability.
4. **Validate and publish**—present draft findings and the framework to the AREA Research Committee for review, incorporate feedback, and deliver the final guide and supporting materials for member use

Why This Research Matters

- **Enables Secure Scale:** Enterprise AR cannot scale without a foundation for secure device commissioning, re-assignment, and retirement.
- **Removes Deployment Blockers:** Provides the evidence and decommission procedures IT and Security teams require to approve broad rollouts.
- **Mitigates Data Risk:** Prevents data exposure from devices that are lost, broken, or retired with enterprise credentials and content intact.
- **Adapts IT Standards for XR:** Replaces generic mobile MDM approaches with a framework, tool matrix, and checklist built for XR hardware.
- **Eliminates Process Rework:** Offers a validated baseline so organizations spend less time reinventing local processes and more time deploying.
- **Strengthens the Internal Business Case:** Equips AR champions with professional frameworks to secure buy-in from governance and procurement teams.