✅ IAM Tools Tab —

Purpose: The IAM Tools tab provides centralized access to identity auditing, access control analysis, and group membership visibility. It is designed for system administrators, cybersecurity teams, and compliance officers who need to verify user entitlements, investigate access anomalies, and enforce least privilege.

Key Capabilities:

- **Identity Selection:** Operators can select any user identity from Active Directory and immediately view their group memberships, token SIDs, and effective permissions.
- **Audit Logging:** Auditing Requires AD DS Event Logging. Every identity selection and access review is logged with timestamp, operator ID, and object details. This ensures traceability and supports incident response workflows.
- **ACL Search & Retrieval:** RDAM can search shared folders (local or network paths) for ACL entries matching the selected identity. Results include explicit and inherited permissions, SID mappings, and access types.
- **Effective Permissions Panel:** Displays consolidated access rights across all group memberships, including nested groups and inherited ACLs.
- **Compliance Dashboard Integration:** IAM audit results feed directly into RDAM's compliance scoring engine, allowing stakeholders to quantify identity risk posture.

Organizational Benefit:

- **For ISSMs/ISSOs:** Enables rapid entitlement reviews and supports audit readiness for RMF, NIST 800-53, and CMMC controls.
- **For CIOs:** Demonstrates centralized identity governance without requiring external IAM platforms.
- **For System Integrators:** Accelerates deployment of secure access workflows and reduces time-to-compliance.
- **For SOC/IR Teams:** Provides immediate visibility into who had access to what, when, and why — without scripting or manual ACL parsing.