RSU IDENTITY BRIEF

Active Directory Migration Strategies

A decision guide for migrations without SIDHistory and controlled transitions that use SIDHistory.

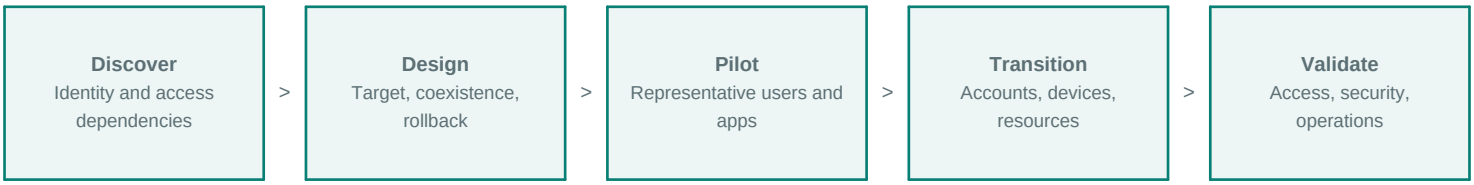
A high-level, public reference for business and technology leaders

Two valid patterns - one deliberate decision

When an account moves to another Active Directory domain, it receives a new security identifier (SID). Access to legacy resources must therefore be remapped to the new SID or temporarily supported through SIDHistory. The correct pattern depends on application readiness, migration duration, trust design, risk tolerance, and the ability to update permissions.

SIDHistory is not a migration requirement. It is a compatibility mechanism that can reduce disruption during a controlled transition, but it expands the trust and monitoring considerations that must be addressed.

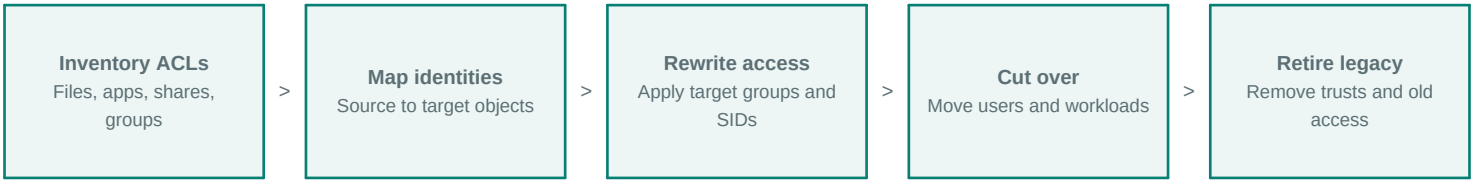
Common migration lifecycle



Pattern A: migration without SIDHistory

This pattern creates or migrates target identities, translates permissions to target SIDs, updates application and service dependencies, and validates access without retaining legacy SIDs on target accounts.

Clean access transition



Best fit

- The organization can inventory and update resource permissions before or during migration.
- Applications support target identities and do not depend on legacy domain identifiers.
- A clean security boundary and simpler post-migration state are priorities.
- Migration waves can include access remediation and validation.

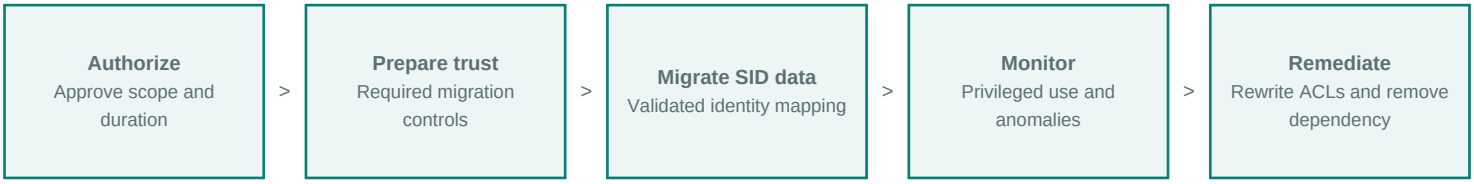
Key controls

- Authoritative identity mapping and duplicate/collision handling.
- Permission translation with before-and-after evidence.
- Service account, scheduled task, certificate, SPN, delegation, and application dependency testing.
- Pilot cohorts, rollback checkpoints, access validation, and orphaned-permission review.

Pattern B: migration with SIDHistory

This pattern places approved source SIDs in the target account's SIDHistory attribute so existing resource ACLs can continue recognizing the user while permissions and workloads are transitioned.

Controlled coexistence



Best fit

• Large or complex legacy estates cannot have all permissions remediated before user cutover.

• A staged migration requires temporary access to source-domain resources.

• The organization can secure the trust path, tightly control migration privileges, and monitor SIDHistory usage.

Security requirements

• Use dedicated, time-limited migration administration with strong MFA and isolated workstations.

• Restrict scope to mapped objects; audit privileged and sensitive SIDs; investigate unexpected values.

• Validate trust, SID filtering, name resolution, time synchronization, and network paths for the approved design.

• Maintain an exit plan: translate ACLs, validate target-native access, remove residual dependency, and retire migration privileges.

Decision matrix

Decision factor	Without SIDHistory	With SIDHistory
Legacy resource access	Permissions remapped to target identities	Temporary compatibility with legacy ACLs
Target-state cleanliness	Cleaner immediately	Requires planned dependency removal
Migration speed	May require more remediation before cutover	Can accelerate staged coexistence
Security complexity	Lower ongoing complexity	Higher trust, privilege, and monitoring demands
Best outcome	Target-native authorization	Controlled bridge to target-native authorization

Required discovery

- Domains, forests, trusts, DNS, sites, replication, and authentication flows.
- Users, groups, nesting, privileged identities, service accounts, devices, and workloads.
- File shares, applications, databases, certificates, SPNs, delegation, scripts, policies, and ACLs.
- Cloud identity, synchronization, collaboration platforms, remote access, and third-party integrations.
- Business owners, outage tolerance, migration waves, communications, support, rollback, and acceptance criteria.

Public references

Microsoft Learn, Security Identifiers - https://learn.microsoft.com/windows-server/identity/ad-ds/manage/understand-security-identifiers
Microsoft Learn, Security assessment: Unsecure SIDHistory attributes - https://learn.microsoft.com/defender-for-identity/security-assessment-unsecure-sid-history-attribute

RSU migration approach

RSU provides discovery, target-state design, coexistence planning, pilots, staged cutover, access validation, rollback planning, and post-migration cleanup without naming or constraining the engagement to a particular migration product.