A PRACTICAL GUIDE FOR BANKS & CREDIT UNIONS

From access reviews to identity governance.

Govern human and non-human identities.
Build roles. Put access decisions into action.

Start with the review you need today.
Build the foundation for the lifecycle you need next.

SYSTEM OF RECORD + APPLICATIONS

Access reviews and cleanup

Identity and service-account visibility

Access Analysis and role building

Manager requests and HR-led automation

INSIDE THIS GUIDE

Your path through identity governance.

Follow the journey from trusted source data to reviews, role definitions, and governed lifecycle workflows. Finish with an evaluation checklist and a clear budget starting point.

01 Establish the foundation — 03
Onboard your SOR, applications, and access data.

02 Review, resolve, and clean — 04
Run repeatable reviews and improve the access baseline.

03 Govern human and non-human identities — 05
Understand human and service-account access relationships.

04 Analyze access and build roles — 06
Turn access patterns into approved business roles.

05 Choose how access is initiated — 07
Separate manager requests from HR-led automation.

06 Evaluate competing solutions — 08
Use 18 questions to test coverage, execution, and value.

07 Special pricing and expansion options — 09
Compare UAR, NeXus AI, and GRC investment options.

08 Consolidate vendors with a purpose — 10
Bring access, AI, and risk governance into one vendor strategy.

01 / ESTABLISH THE FOUNDATION

Connect the people. Connect the access.

Start with a trusted system of record and the applications your institution needs to govern. This foundation supports every review, access analysis, and lifecycle workflow that follows.

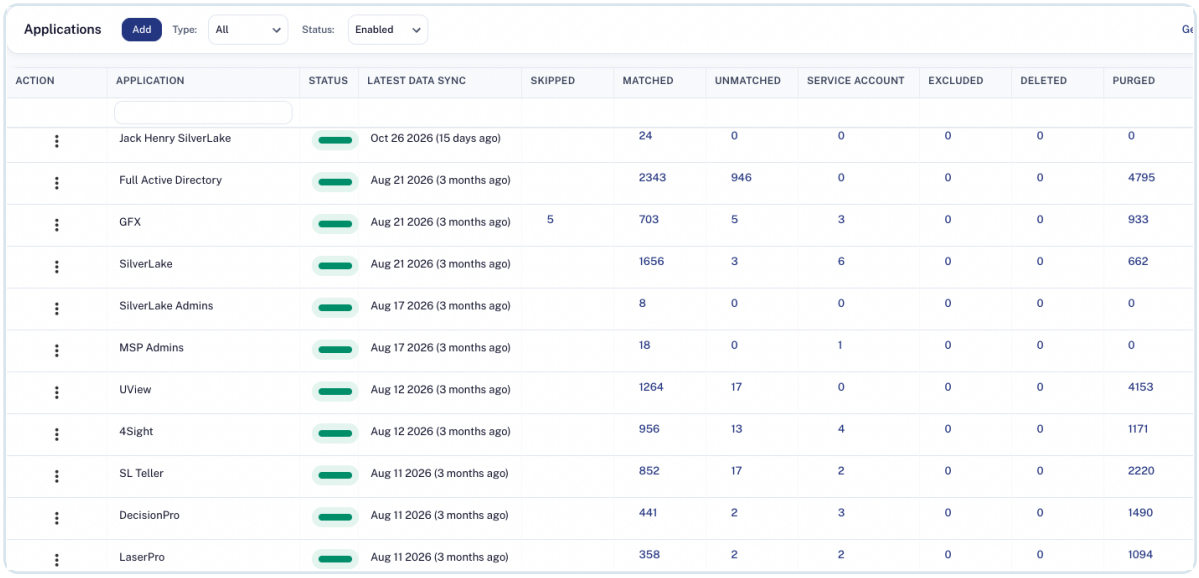
Onboard your system of record (SOR).

Use HR, a directory, or an agreed combination to establish the identities in scope. Bring in the attributes needed to connect people to accounts and route decisions: employee ID, name, email, manager, employment status, department, and job title.

HR can anchor employee status and job changes. Directory or other agreed sources can extend coverage to contractors and vendors who are not represented in HR. Validate attribute ownership, matching rules, and refresh schedules before relying on the data.

Onboard applications using the right ingestion method.

Collect account and entitlement data from core banking, Active Directory/Entra, payments, lending, and other business applications. Use a supported native/API connection, report or file ingestion, or a database extract according to what each source provides.



ACTION	APPLICATION	STATUS	LATEST DATA SYNC	SKIPPED	MATCHED	UNMATCHED	SERVICE ACCOUNT	EXCLUDED	DELETED	PURGED
	Jack Henry SilverLake		Oct 26 2026 (15 days ago)		24	0	0	0	0	0
	Full Active Directory		Aug 21 2026 (3 months ago)		2343	946	0	0	0	4795
	GFX		Aug 21 2026 (3 months ago)	5	703	5	3	0	0	933
	SilverLake		Aug 21 2026 (3 months ago)		1656	3	6	0	0	662
	SilverLake Admins		Aug 17 2026 (3 months ago)		8	0	0	0	0	0
	MSP Admins		Aug 17 2026 (3 months ago)		18	0	1	0	0	0
	UView		Aug 12 2026 (3 months ago)		1264	17	0	0	0	4153
	4Sight		Aug 12 2026 (3 months ago)		956	13	4	0	0	1171
	SL Teller		Aug 11 2026 (3 months ago)		852	17	2	0	0	2220
	DecisionPro		Aug 11 2026 (3 months ago)		441	2	3	0	0	1490
	LaserPro		Aug 11 2026 (3 months ago)		358	2	2	0	0	1094

Application inventory: source synchronization dates and account classifications help administrators see what has been brought into scope and what needs investigation.

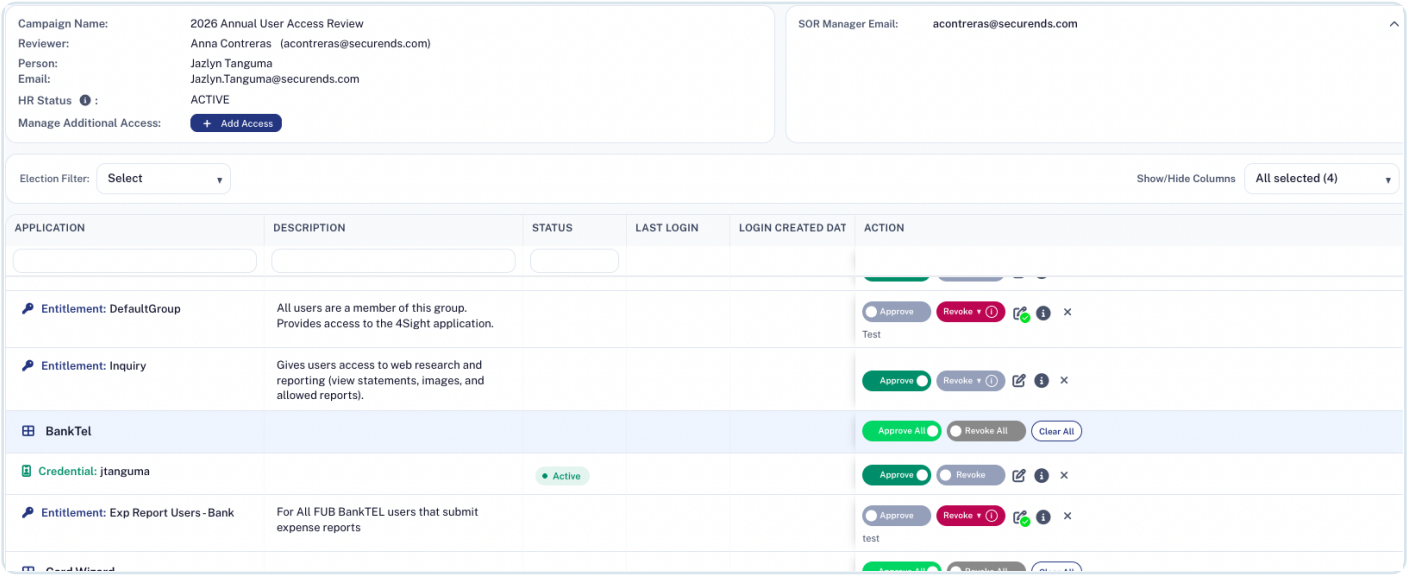
02 / REVIEW, RESOLVE, AND CLEAN

Make your first review the start of a better baseline.

Give reviewers enough context to decide. Use the findings to improve identity matching, account ownership, and the quality of future access decisions.

Build a repeatable review process.

Create reusable campaign templates for the applications, identities, and permissions you need to review. Separate high-risk, privileged, and service-account reviews where appropriate. Assign managers or application owners and configure instructions, reminders, and escalations.



Reviewer experience: HR status, application and account context, permission descriptions, and approve/revoke actions in one view.

Resolve findings and retain the reason for the decision.

- Investigate unmatched accounts. Establish whether each belongs to an employee, third party, service account, or a user who has left.

- Add clear permission descriptions and capture business justifications so decisions can be explained later.

- Assign service-account owners and confirm who is accountable for reviewing their access.

- Track approved removals through fulfillment, then check refreshed source data to confirm the result.

03 / GOVERN HUMAN AND NON-HUMAN IDENTITIES

Bring human and non-human identities under governance.

SecurEnds connects people to the accounts and permissions they use, while bringing service accounts and other non-human identities into accountable ownership and recurring access reviews.

Human identity: see who has access to what.

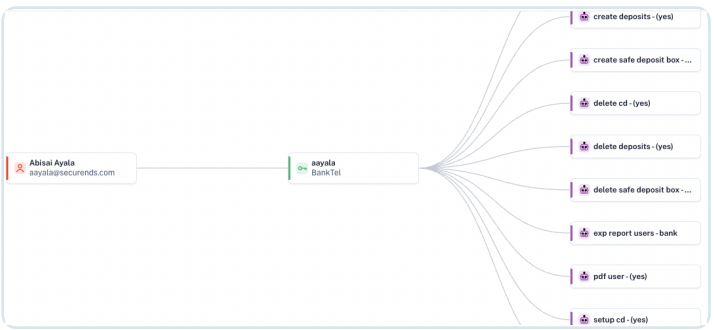
Identity Mind Map follows a person across connected applications, credentials, and entitlements. Use it to investigate access after a role change or departure, including locally managed accounts outside Active Directory.



First view: a human identity connected to application accounts and permissions.

Human-to-service-account access: make it accountable.

The second mind map shows a human identity connected to service-account or non-human access. Review who can use that access, what permissions it carries, and who owns it. As AI agents use service accounts, include those accounts in the same governance discipline.



Why service accounts matter

They can retain persistent or privileged access without an employee record. Ownership may become unclear when staff move or leave. SecurEnds lets you assign owners and include these accounts in recurring permission reviews.

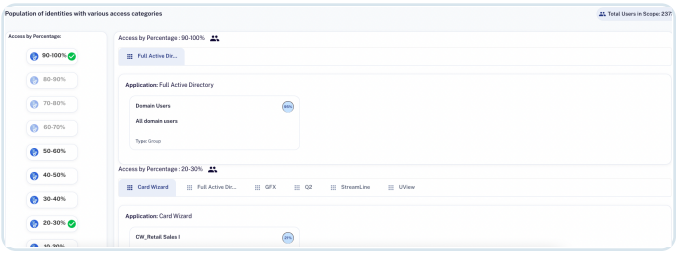
04 / ANALYZE ACCESS AND BUILD ROLES

Turn access patterns into approved business roles.

Start with the access people actually have. Validate it with the business, then define the applications, permissions, ownership, and approvals each role should carry.

Use Access Analysis to find the starting point.

Compare relevant employee groups by department, title, or job code. Identify common permissions and investigate exceptions before deciding what belongs in a standard role. Common access is evidence for a discussion, not automatic authorization.

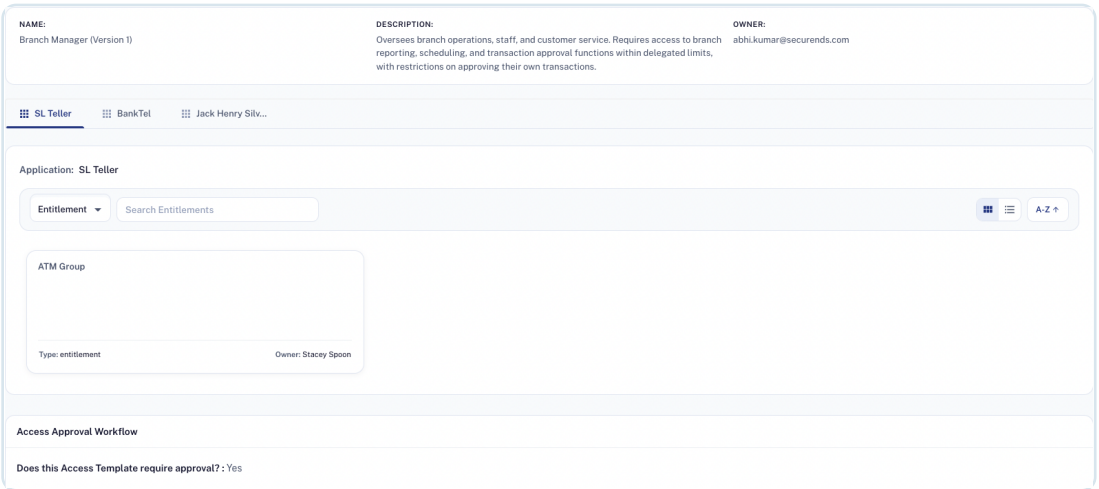


Ask why access differs.

Is it needed for the job, a temporary assignment, a missing permission, or access left over from a previous role? Resolve these differences with managers and application owners.

Build a reusable role with explicit access and approvals.

Name the role and describe its business purpose. Assign an accountable owner. Select the required applications and the specific entitlements within each. Define approval requirements, separate exceptions from baseline access, and validate the template with the business before using it for requests or HR policies.



Role example: Branch Manager. The template records its purpose and owner, groups access by application, and specifies whether approval is required.

05 / CHOOSE HOW ACCESS IS INITIATED

Manager action or HR automation. Two distinct operating models.

Both use approved access templates. The difference is who initiates the process: a manager making a request, or an HR change automatically processed by SecurEnds.

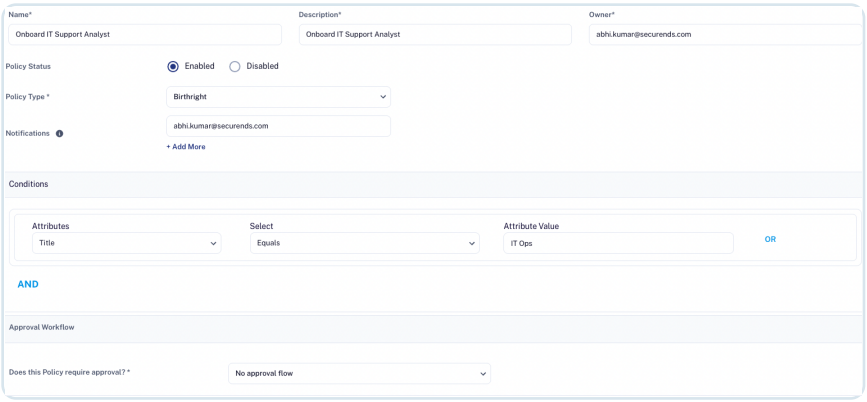
Manager-led: a person requests

The manager opens SecurEnds, selects the employee and role template, adds the business reason, and submits. The request follows the configured approval and fulfillment workflow. A manager must take action to initiate this path.

HR-led: the system initiates

The HR system syncs to SecurEnds. Configured rules evaluate new hires, job changes, and departures and automatically initiate the mapped access workflow. No manager request is needed to start the process.

HR sync + policy conditions + approved role template.



Configure the HR-driven rule

Map trusted attributes, such as title or department, to the appropriate access template. Define any required approvals and the actions for onboarding, role changes, and offboarding.



Apply the mapped template

The HR event starts the workflow automatically using the approved access definition.

AUTOMATED INITIATION AND APPLICATION FULFILLMENT

HR-led initiation is automated. Direct provisioning depends on supported write integrations; other applications use assigned tasks or tickets. Confirm sync timing and track completion.

06 / EVALUATE COMPETING SOLUTIONS

Ask every vendor to prove the complete flow.

Use the same identities, source files, applications, and lifecycle scenarios in each evaluation. Ask for a demonstration and evidence of the result, including exceptions and failures.

01 / Source and application coverage

- Can HR and directories be combined, including employees, contractors, and service accounts?
- Which exact core reports, fields, submenus, and entitlements are supported for our system and version?
- How are APIs, files, and database extracts refreshed? Who owns export failures and stale data?

02 / Identity matching and reviews

- How are accounts matched to people, and how are ambiguous or unmatched accounts investigated?
- Can reviewers see understandable permissions, HR status, and business justifications?
- Can we configure review scope, cadence, privileged/service-account campaigns, reminders, and escalation?

03 / Human and non-human governance

- Can we trace a person to application accounts, service-account access, and specific permissions?
- Can service accounts have accountable owners and recurring access reviews?
- Which AI-related relationships are visible, and what additional products or integrations are required?

04 / Analysis and role building

- Can we compare access by department or job and investigate common access and outliers?
- Can a role specify applications, entitlements, owner, business purpose, and approval requirements?
- How are role definitions validated, updated, and distinguished from individual exceptions?

05 / Requests, HR automation, and fulfillment

- Can managers request access directly? Can HR sync initiate lifecycle workflows without a manager request?
- When someone changes jobs, how is old access assessed and removed alongside new access?
- For each application, what is automated versus ticket-based? How are failures, status, and removal verified?

06 / Evidence, delivery, and total cost

- Can we inspect source dates, review scope, decisions, approvals, and fulfillment evidence with our auditor?
- What are the hosting controls, data flows, implementation deliverables, training, and support commitments?
- What is included in subscriptions and services? Price connector work, application growth, and ongoing upkeep.

07 / SPECIAL PRICING AND EXPANSION OPTIONS

Start with UAR. Add NeXus AI or GRC.

Choose the next capability around your immediate priority: govern AI agents, strengthen IT and third-party risk management, or bring all three workstreams together.

USER ACCESS REVIEWS / SPECIAL FIRST-YEAR SUBSCRIPTION

$12,000

Up to 250 users and 25 applications using standard connectors.

Agreement	Three-year term. Years two and three: $15,000/year for UAR.
Implementation	$2,500 one time: agreed SOR, first five applications, configuration, test campaign, and administrator training.
Customer success	$1,500/year optional: monthly check-ins, campaign guidance, feature walkthroughs, and new-administrator training.

NeXus AI

$5,000 / year

Early Adopters Program: up to 100 AI agents. Commercial pricing is approximately $10,000/year. Previously offered to existing customers; now opening to new customers. Cotermed with UAR.

GRC

$5,000 / year

Includes IT Risk Management and Third-Party Risk Management together. Organize risk assessments, evidence collection, vendor reviews, and follow-through around accountable owners.

FIRST YEAR / INCLUDES UAR IMPLEMENTATION

UAR: $14,500 | UAR + NeXus AI or GRC: $19,500

UAR + NeXus AI + GRC: $24,500

Optional customer success adds $1,500/year. Additional module setup, custom integrations, direct provisioning, and access-management licensing are scoped and quoted separately.

08 / CONSOLIDATE VENDORS WITH A PURPOSE

One vendor strategy. Connected governance priorities.

Access reviews, AI governance, IT risk, and vendor risk are often managed by the same lean team. Consolidating with SecurEnds can simplify vendor oversight while preserving clear responsibilities for each workstream.

Choose the next step around the work you need to improve.

UAR + NEXUS AI

When AI adoption is moving ahead of governance

Extend the conversation from employee and service-account access to supported AI-agent discovery, ownership, access visibility, and governance policies. Confirm platform coverage and the controls in scope.

UAR + GRC

When audit evidence and vendor reviews consume the team

Add IT Risk Management and Third-Party Risk Management together. Coordinate risk assessments, evidence requests, vendor documentation, review ownership, and outstanding actions.

UAR + NEXUS AI + GRC

When you want a broader consolidation strategy

Address access governance, AI governance, IT risk, and third-party risk through one vendor relationship. Agree the implementation sequence, operating responsibilities, and any data-sharing or integration requirements.

Make the consolidation case in operational terms.

Fewer separate vendors to evaluate and oversee. More coordinated implementation and training. A clearer route to support and a combined commercial discussion across related priorities. Compare total cost, administrator effort, and integration needs against maintaining separate tools.

Year-end offer: sign by December 31, 2026. Extension through March 31, 2027 for a Q1 project requires finance approval. Final scope, eligibility, module setup, and commercial terms are confirmed in the proposal.

Plan your scope: securends.com/get-started/