

IGA

IDENTITY GOVERNANCE & ADMINISTRATION

The right access. Across the identity lifecycle.

Bring identities, roles, approvals and access reviews into a governed operating model. Give the business a clear way to decide who should have access, and keep those decisions connected to enterprise systems.



Govern the identity lifecycle

Coordinate access as people join, change roles and leave.



Make access decisions accountable

Use roles, policies, approvals and certification campaigns.



Keep evidence close to the decision

Connect identity context, provisioning outcomes and audit records.

CAPABILITIES

Make access a business decision.

Access spreads across people, departments and connected systems. Protect Identity IGA gives identity teams and business owners a shared foundation for managing that access throughout its lifecycle.

CAPABILITY	WHAT IT ENABLES
Identity lifecycle	Manage identity records, lifecycle states, assignments and linked resource accounts. Keep access aligned with a person's changing responsibilities.
Roles & organization	Model roles, organizational structure, ownership and policy-driven assignments. Make access easier to explain, review and maintain.
Requests & approvals	Route access requests through configured approval workflows and reviewer responsibilities. Replace informal requests with recorded, repeatable decisions.
Access certification	Run review campaigns with configured stages, reviewers, deadlines and outcomes. Help owners confirm continuing need and identify access to remove.
Provisioning & reconciliation	Use connectors, mappings and tasks to coordinate accounts and entitlements. Connect approved intent with observed access in target systems.
Audit & reporting	Review identity changes, task results, governance activity and reports. Support investigations and evidence gathering with operational context.

✓ Policy with context

Apply governance to the identity, role and resource in question. Review business exceptions and separation-of-duty requirements through your configured policy and approval process.

IN PRACTICE

From a new joiner to a reviewed exit.

Build a repeatable operating model for the moments when access changes most.

- 01 Establish the identity**
 Connect the person to lifecycle state, organizational context and relevant resource accounts.
- 02 Request and approve access**
 Assign roles or request entitlements. Route decisions to the configured owners and reviewers.
- 03 Provision and reconcile**
 Apply approved changes through configured connectors, then inspect task outcomes and observed access.
- 04 Review, change and remove**
 Certify continuing need, handle role changes and verify offboarding through provisioning and audit evidence.

WHERE IT HELPS

Identity operations

Coordinate joiners, movers and leavers across connected systems.

Business ownership

Give reviewers identity and entitlement context for access decisions.

Audit preparation

Trace approvals, review outcomes and resulting system changes.

Extend governance into privileged access

When paired with GovPAM, approved IGA eligibility can provision a normal PAM identity. GovPAM continues to control asset permissions, credentials and sessions. Offboarding disables the managed account and queues session termination; operators preview reconciliation before applying changes.

Review decisions and provisioning outcomes together: a recorded approval or revocation does not, by itself, prove that access changed on the target system.

YOUR NEXT STEP

See your governance model in action.

Use a tailored demonstration to connect the product to your identity sources, access decisions and review responsibilities.

01 Choose an identity journey

Walk through a joiner, a role change or an offboarding scenario.

02 Bring an access review

Explore reviewers, entitlement context, decisions and remediation evidence.

03 Scope the first integration

Identify a target system, role owner and provisioning outcome to validate.

Start with IGA. Expand when you need to.

Install Protect Identity IGA on its own or subscribe to additional Protect Identity products. Separate product entitlements let you build the offering around your priorities.

Each customer installation has its own service configuration, state, databases and keys. Choose one, two or all three products, with separate subscriptions.

LET'S PLAN YOUR DEMONSTRATION

Book an IGA demonstration

Make access ownership clear. Keep governance connected to operations.

sales@protectidentity.co.za

Deployment scope is defined by your identity sources, connector configuration, approval policies and target systems.
