MANUAL · V1.0

AccessGuard

Know who has access to what.

Complete reference for using AccessGuard, from first matrix to periodic reviews, from onboarding new staff to offboarding leavers without any access staying open.

Contents

01 Introduction

AccessGuard is access management for SMBs without an IT department. This manual covers everything from the first setup to daily operation.

What problem does this solve?

In most SMBs, access management is scattered across Excel sheets, emails and people's memory. Nobody has a reliable answer to "who has access to Salesforce?" or "did we revoke everything when Lisa left?". This chaos is invisible, until there's an audit, an incident, or a former employee who still has access to sensitive data.

Who is this for?

- Organisations of 10-200 staff
- No dedicated IT or IAM team
- Using 5-30 SaaS systems (M365, Slack, Salesforce, Exact, etc.)
- Compliance requirements (ISO 27001, NEN 7510, GDPR audits)
- External suppliers and temporary staff that also get access

Core concepts

TERM	MEANING
Person	An employee, contractor or external party whose access you track. Has a status: active, scheduled_in, scheduled_out or inactive.
System	An app or service someone might have access to. Categorised as SaaS, on-prem, infra, finance, security, comm or other.
Cell	The intersection of a person and a system in the Access Matrix. Holds one of four states.

Access item	A fine-grained permission within a system (role, licence, account). Optional; only used when the system has them.
Review cycle	A periodic exercise where every cell (or item) gets a keep/revoke/change decision from a reviewer.
Process	An onboarding or offboarding workflow for a single person, with checklist, evidence uploads and automatic access-effects.

02 Getting started

In about 15 minutes you have your first matrix filled in and can start deciding what to clean up.

PREREQUISITES

AccessGuard is available on the Pro plan (€12/month) and higher. Sign up, choose Pro, and you're in.

01. Add your people

Go to AccessGuard → Personen. Add every employee, contractor and external party whose access you want to track. You don't need to import from HR, a handful of rows to start with is fine.

02. Add your systems

AccessGuard → Systemen. Everything your staff might have access to: M365, Slack, Salesforce, Exact, 1Password, AWS, domain admin, the physical alarm code. Think broadly.

03. Fill in the matrix

AccessGuard → Access Matrix. Click a cell to cycle the status: unknown → has_access → no_access → needs_review. Don't aim for perfection; fill in what you already know.

04. Start your first review cycle

AccessGuard → Reviews → Nieuwe cyclus. The current matrix is snapshotted; you decide keep/revoke/change per row. On completion, IT gets an actions list.

03 The Access Matrix

The matrix is the heart of AccessGuard. A 2D grid where the rows are people and the columns are systems. Each cell shows one of four states.

The four cell states

STATE	MEANING
✓ has_access	The person currently has access to the system. Status is confirmed.
× no_access	The person has no access, and that's deliberate. Confirmed negative.
? needs_review	Not sure, flag for the next review. Used when state is unclear or suspicious.
, unknown	Never decided. The default state for new cells. Aim to reduce this to zero.

How to click through the matrix

Click any cell without items to cycle through the four states in order. Click again to continue. Every click is timestamped in last_verified_at, useful for the review cycle to see "when did we last confirm this?".

> **TIP**
>
> Start by filling in only has_access cells, the people who definitely have access. That alone already shows you where access is excessive. Everything else can stay "unknown" until the first review cycle.

04 Fine-grained access items

Sometimes "access to Salesforce" is too coarse. Is this person a global admin, a standard user, or read-only? Access items let you track per role/licence/account within a system.

When to use items

- Systems with multiple licence tiers (M365: Basic / E3 / E5)
- Systems with role hierarchies (Salesforce: Admin / Standard / Read-only)
- Systems where different accounts matter (Google Workspace: personal / service account)
- Where compliance reports require role-level detail

How the matrix behaves with items

Once a system has one or more active items, the cell on the matrix becomes a drill-down link instead of a click-to-cycle button. The cell-state is derived automatically:

ITEM COMBINATION	CELL STATE
≥1 item has_access, all same	has_access
Any needs_review or mix of states	needs_review
All items no_access	no_access
No items set yet	unknown

Managing items

AccessGuard → Systemen → click "Items" next to the system. Add / edit / deactivate items. Each item has a type (role, licence, account, key, badge, group, other) and a sort order. Deactivated items disappear from the drill-down but their history stays in the audit log.

05 Review cycles

A review cycle is a periodic exercise, quarterly or annually, where someone goes through every matrix cell and decides: keep this access, revoke it, or change it.

Cycle lifecycle

`planned ? active ? completed` (or cancelled)

Starting a cycle

AccessGuard → Reviews → Nieuwe cyclus. Pick a title ("Q1 2026 access review"), a scope (active people, or everyone including inactive), an optional deadline, and notes for the reviewer. On save, the current matrix is snapshotted into review_items, one row per cell (or per item when the system has items).

> **IMPORTANT**
>
> After the snapshot is taken, later changes to the matrix do NOT affect the cycle. The snapshot freezes what was being decided. This keeps the audit trail clean.

Making decisions

DECISION	WHAT HAPPENS AT COMPLETION
keep	The cell last_verified_at is bumped. No further action needed.
revoke	An open revoke_access action is created. IT has to act on it.
change	An open review_level action is created (e.g. downgrade admin to read-only).
(empty)	Undecided items default to "keep" when the cycle is closed.

Bulk decisions

Use the checkboxes to select multiple review items and apply the same decision in one click. Handy for large cycles where most decisions are "keep".

06 Actions queue

When a review cycle completes (or an offboarding completes), revoke and change decisions materialise as open actions. The actions queue is what IT works through.

Two action kinds

- **revoke_access**, Remove this access. On "mark done", the matrix cell flips to no_access (or the individual item if item-scoped).
- **review_level**, Change the level (e.g. admin → read-only). On "mark done", only the verified timestamp is bumped; you handle the actual level change externally and note it here.

Typical flow

1. Reviewer closes a cycle with 6 revoke decisions
2. 6 revoke_access actions appear in the queue with status=open
3. IT disables the accounts in the actual systems (M365 admin centre, Slack, etc.)
4. IT clicks "Afronden" on each action, the corresponding matrix cell flips to no_access
5. The audit log records who marked done + when + what was applied

07 Onboarding & offboarding processes

A process is a per-person workflow: a checklist of things that need to happen, with optional evidence uploads per item. Two kinds: onboarding (new hire) and offboarding (leaver).

Checklist item states

`todo ? in_progress ? done / blocked / na`

- **todo**: default, not started
- **in_progress**: being worked on
- **done**: completed successfully
- **blocked**: waiting for something external, reason required
- **na**: not applicable for this case, reason required

Offboarding → automatic revokes

Completing an offboarding process has a powerful side-effect: every has_access cell or item of the subject person automatically becomes a revoke_access action. This means you physically cannot "forget" to revoke access, the system surfaces every open door.

> **EVIDENCE UPLOADS**
>
> Per checklist item you can upload PDF / JPG / PNG files up to 15 MB. Useful for: signed hardware-return form, screenshot of disabled M365 account, photo of returned access badge. Each file is stored with a UUID, SHA-256 hashed for integrity, and only accessible within the tenant.

08 Risk detection

A scheduled scan runs every night at 03:00 and surfaces risky patterns as open risk flags. Seven detection rules cover the most common SMB access-control failures.

The seven detection rules

RULE	SEVERITY	TRIGGER
stale_admin	4	Admin-like item with has_access but no verification for 90+ days
orphan_access	5	Inactive person still has active has_access cells or items
excessive_access	3	Person has has_access on ≥10 different systems
overdue_review	4-5	Open cycle past its due_at (5 if >30 days overdue)
overdue_action	3-4	Open action older than 14 days (4 if >30 days)
pending_onboarding	3	Person scheduled_in but no active onboarding process
stale_credential	4-5	Vault credential past expires_at (5) or rotation overdue (4)

Working risks

For each open risk flag you have three actions:

- **Acknowledge**, I've seen this, will act on it. Moves to "acknowledged" status.
- **Resolve**, The underlying problem is fixed (account revoked, review completed, etc.). Moves to "resolved".
- **Reopen**, If something was resolved prematurely, you can reopen it.

09 Reminders

A second scheduled job (daily at 03:15) scans for upcoming deadlines and creates reminders. Reminders are in-app notifications, lightweight compared to risk flags.

REMINDER KIND	TRIGGERS WHEN
cycle_due	Open review cycle's due_at within 7 days or overdue
process_due	Active onboarding/offboarding due_at within 7 days or overdue
action_overdue	Open action older than 14 days
person_starting	Person scheduled_in with start_date within 7 days
person_leaving	Person scheduled_out with end_date within 7 days

Dismissing a reminder marks it permanently dismissed, the next scheduled run will not resurrect it. Marking "Klaar" closes it cleanly.

10 Vault (encrypted credentials)

Store passwords, tokens, API keys, SSH keys and certificates, linked to systems or access items. Secrets are encrypted with AES-256 + HMAC; every view or decrypt is logged.

Access model

- The creator is implicit admin (view + decrypt + rotate + delete). No ACL row needed.
- Anyone else needs an explicit ACL grant with the appropriate flags.
- Four permission levels: can_view, can_decrypt, can_rotate, can_admin.

Reveal-on-click workflow

On the detail page, the secret is masked as bullets. Click "Toon" → the JSON endpoint decrypts and returns the plaintext. The UI shows it for 30 seconds with a ticking countdown, then auto-hides. You can click the copy button to put it on the clipboard.

> **AUDIT TRAIL**
>
> Every action on a credential is logged: created, updated, viewed (metadata), decrypted, rotated, deleted, and ACL grants/revokes. Each log row includes the user and a hashed IP. Keep this in mind, secret access is NOT silent.

Offboarding → automatic ACL revoke

When an offboarding process completes for a Person whose email matches a User in the tenant, every ACL row that User holds is automatically revoked. One email-match, zero credentials left accessible.

11 AI-powered explanations

Not everyone on your team is a security person. The AI-explain widget translates a risk flag into plain-language advice, what it is, why it matters, and three or four concrete next steps.

How it works

Click the □□ Uitleg button on any risk flag. A modal opens with:

- **Summary**, two-three sentences describing the risk
- **Why it matters**, business + security context
- **Recommended steps**, three or four concrete actions in AccessGuard
- **Warnings**, what to watch out for

> **PRIVACY**
>
> Only the risk flag's metadata is sent to OpenAI, never secrets, never full email addresses, never vault content. The payload is whitelisted to safe keys (ids, counts, dates). Every AI call is logged with tokens used. Rate-limited to 10 calls per tenant per hour; identical prompts are cached 24 hours.

12 Plans & limits

AccessGuard is included in the Pro plan and up. Business adds multi-user access and removes the AI rate limit.

FEATURE	FREE	PRO €12/MO	BUSINESS €39/MO
Access Matrix + items	,	✓	✓
Review cycles	,	✓	✓
Onboarding / offboarding	,	✓	✓
Risk flags + reminders	,	✓	✓
Vault	,	✓	✓
AI explanations	,	10/h	unlimited
Multi-user access	,	,	✓

13 Glossary

Quick reference for the terms and abbreviations used throughout AccessGuard.

TERM	MEANING
ACL	Access Control List, the per-user permission rows on a vault credential.
Access cell	The intersection of a person and a system in the matrix.
Access item	A fine-grained permission within a system (role, licence, account).
Cycle	A review cycle: a time-bound exercise of reviewing every cell in a snapshot.
has_access	Cell state: person currently has confirmed access.
IAM	Identity and Access Management, the broader discipline AccessGuard sits in.
last_verified_at	Timestamp of when a cell/item was last confirmed. Drives stale-admin detection.
needs_review	Cell state: status unclear, flag for next cycle.
no_access	Cell state: person deliberately has no access.
Offboarding	The process for someone leaving the organisation. Completion triggers automatic revoke actions.
Onboarding	The process for someone joining the organisation. Checklist-based with evidence uploads.
Person	Someone whose access you track, employee, contractor or external.
Risk flag	A detected risk pattern. Has severity 1-5 and states open / acknowledged / resolved.

Scope	A cycle scope: "active people" (default) or "everyone incl. inactive" (for yearly audit).
Snapshot	A frozen copy of the matrix at cycle-start. Later changes don't affect the cycle.
System	An app or service where people can have access. Can have items (for fine-grained tracking).
Tenant	Your organisation's isolated space. All AccessGuard data is scoped to a single tenant.
unknown	Cell state: never decided. Default for new cells.
Vault	Encrypted credential storage. Per-user ACL; every access is logged.

AccessGuard is a product of Beter Geregeld ICT. This manual is generated automatically, the digital version on the website is always authoritative.
Contact: info@betergeregeld.com · Manual generated: 11-07-2026