NOVA IAM

NOVA IAM

# Handbuch

Wie Nova Identitäten, Konten und Berechtigungen verwaltet – offen dokumentiert.

**Stand:** 28. September 2026

docs.nova-iam.com

# Inhalt

KAPITEL 1

# Einführung

## 1.1 Über dieses Handbuch

Nova IAM ist eine Plattform für Identity & Access Management. Nova verwaltet **Identitäten** – Mitarbeitende, externe Personen und technische Akteure –, ihre **Konten** in den angebundenen Zielsystemen und die **Berechtigungen**, die sie dort erhalten. Dazu gehören der Lebenszyklus mit Eintritt, Wechsel und Austritt, Anträge und Genehmigungen, Rezertifizierungen und die Protokollierung sicherheitsrelevanter Änderungen.

Dieses Handbuch beschreibt, wie Nova dabei vorgeht – offen und für alle lesbar.

### Für wen es geschrieben ist

- **Anwenderinnen und Anwender** – Administration, Genehmigende und Führungskräfte, die mit Nova arbeiten.
- **Prüferinnen und Prüfer** – Revision, Informationssicherheit und Wirtschaftsprüfung, die nachvollziehen wollen, wie Zugänge entstehen und wieder verschwinden.
- **Interessierte** – alle, die Nova bewerten, bevor sie es einsetzen.

### Was „geplant“ bedeutet

Wir dokumentieren nur, was Nova tut oder was beschlossen ist. Beschlossenes Verhalten, das noch kein Release ausliefert, ist gekennzeichnet:

- Ganze Seiten tragen oben den Hinweis **Geplant** und in der Navigation die Markierung geplant.
- Einzelne Aussagen auf sonst gültigen Seiten sind mit geplant markiert.

Sobald ein Release das Verhalten ausliefert, entfernen wir die Kennzeichnung.

### Sprachen

Das Handbuch erscheint auf Deutsch und Englisch. Beide Fassungen sind inhaltlich gleich; über das Sprachmenü gelangen Sie zur selben Seite in der anderen Sprache.

## Als PDF

Das gesamte Handbuch gibt es auch als ein PDF-Dokument ↗ – mit Inhaltsverzeichnis, zum Ablegen, Drucken oder Weitergeben. Es entsteht bei jeder Veröffentlichung neu und hat damit immer denselben Stand wie diese Website.

# 1.2 Was ist Nova

Nova IAM ist eine Plattform für Identity & Access Management. Nova verwaltet **Identitäten** – Personen, technische Identitäten und KI-Agenten –, ihre **Konten** in den angebundenen Zielsystemen und die **Berechtigungen**, die sie dort erhalten. Nova entsteht aus jahrzehntelanger Praxis mit SAP Identity Management.

## Was Nova leistet

- **Lebenszyklus:** Nova übernimmt Personaldaten aus dem Personalsystem und bildet Eintritt, Wechsel, Austritt und Wiedereintritt über konfigurierbare Routinen ab – siehe Anbindung an HR und Eintritt, Wechsel, Austritt.
- **Berechtigungsmodell:** Berechtigungen der Zielsysteme lassen sich zu Business-Rollen bündeln und Identitäten, Organisationseinheiten oder Planstellen zuweisen – siehe Berechtigungsmodell.
- **Anträge:** Anträge auf Berechtigungen und Business-Rollen durchlaufen festgelegte Genehmigungsabläufe – siehe Zugriff beantragen.
- **Provisionierung und Abgleich:** Nova legt Konten in den Zielsystemen an, überträgt Berechtigungen, sperrt Konten und vergleicht den Stand in Nova mit dem im Zielsystem – siehe Wie Zugriff entsteht und verschwindet.
- **Governance:** Rezertifizierung, Funktionstrennung (SoD) und Risikobewertung.
- **Nachvollziehbarkeit:** Audit-Log, Provisioning-Log und Änderungsjournal.

## Aufbau

| Baustein | Aufgabe |
|---|---|
| Weboberfläche | Bedienung im Browser, auf Deutsch und Englisch; keine Installation auf Arbeitsplätzen |
| Anwendung | Python-Anwendung (Flask) mit der Geschäftslogik: prüft Rechte, führt Abläufe aus, protokolliert und stellt die Schnittstelle für die Oberfläche bereit |
| Datenbank | PostgreSQL für Identitäten, Rollen, Zuweisungen, Konfiguration und Verlauf; das Schema passt Nova beim Start selbst an |
| Connectoren | Zielsysteme SAP (über RFC), Active Directory und LDAP, Microsoft Entra ID, Keycloak und SCIM; Quellsysteme „Nova HR Stage“ für Personaldaten und „SAP OM“ für die Organisationsstruktur – siehe Überblick über die Zielsysteme |
| Hintergrund-Jobs | zeitgesteuerte Aufgaben nach Cron-Zeitplan in der Zeitzone Europe/Berlin, etwa HR-Import oder Austrittsdatum-Scan; zu finden unter „Monitoring“ → „Hintergrund-Jobs“ |
| Benachrichtigungen | per E-Mail; über ein Zusatzmodul auch in Microsoft Teams |
| KI (optional) | lokale Modelle über Ollama oder ein Cloud-Anbieter; der Kern arbeitet ohne KI – siehe KI in Nova |

### Zusatzmodule

Zusatzmodule (Plugins) erweitern Nova um weitere Funktionen. Nach der Installation sind sie ausgeschaltet; Administratoren schalten sie einzeln unter „Administration“ → „Plugins“ ein. Module mit eigenen Schnittstellen verlangen danach einen Neustart. Zu den Zusatzmodulen gehören:

| Zusatzmodul | Funktion |
|---|---|
| „Planstellen (OSP)“ | Planstellen zwischen Organisationseinheiten und Personen, mit eigenen Business-Rollen |
| „SoD-Analyse (SAP ABAP)“ | prüft SAP-Rollen gegen ein SoD-Regelwerk |
| „GRC-Berechtigungsanalyse (SAP Access Control)“ | nutzt ein vorhandenes SAP GRC Access Control als Quelle für die Risikoanalyse |
| „Native MFA (TOTP)“ | zweiter Faktor für die Anmeldung mit Passwort |
| „OIDC Identity Provider“ | andere Anwendungen melden Personen über Nova an (OpenID Connect) |
| „Microsoft Teams Notifications“ | Benachrichtigungen in Microsoft Teams |

## Wie Daten fließen

1. **Quellsystem → Nova.** Das Personalsystem liefert Personaldaten. Nova legt daraus Identitäten an, hält sie aktuell und erkennt Eintritte und Wechsel.
2. **Soll-Zustand in Nova.** Welche Berechtigungen eine Identität haben soll und für welchen Zeitraum, hält Nova als Zuweisungen fest – aus Business-Rollen, Organisationseinheiten, Planstellen, genehmigten Anträgen und direkten Zuweisungen.
3. **Nova → Zielsysteme.** Provisionierungsläufe legen Konten an, übertragen Berechtigungen und sperren Konten.
4. **Zielsysteme → Nova.** Nova liest Konten und Berechtigungen aus den Zielsystemen ein. Weichen der Soll-Zustand in Nova und der Ist-Zustand im Zielsystem voneinander ab, zeigt der Abgleich die Unterschiede; Administratoren lösen sie in die eine oder die andere Richtung auf.

## Betrieb

Nova läuft heute auf den Servern des Betreibers: als Container-Anwendung mit einer PostgreSQL-Datenbank, bedient über den Browser. Welche Editionen es gibt und welche angekündigt sind, beschreibt Editionen und Betrieb.

# 1.3 Editionen und Betrieb

Nova ist ein Produkt in drei Editionen. Sie unterscheiden sich darin, wo Nova läuft und wer es betreibt.

## Die Editionen

| Edition | Betrieb | Stand |
|---|---|---|
| **Nova Native** | On-Premise: der komplette Stack auf den eigenen Servern | verfügbar |
| **Nova on BTP** | auf der SAP Business Technology Platform, eingebettet in die bestehende SAP-Landschaft und deren Betriebsmodell | angekündigt ab Q4/2026 geplant |
| **Nova as a Service** | in der Cloud als Service betrieben; ohne eigene Infrastruktur, im Browser startklar | angekündigt ab Q2/2027 geplant |

Nova on BTP und Nova as a Service sind angekündigt, aber noch nicht erhältlich. Heute läuft Nova auf den Servern des Betreibers.

## Lizenz

Für Nova fallen keine Lizenzkosten pro Identität an.

## Technische Betriebsvarianten

### Container auf eigenen Servern

Nova Native läuft in Containern: ein Container für die Anwendung einschließlich der Weboberfläche, dazu eine PostgreSQL-Datenbank. Für Docker Compose gibt es eine Konfiguration für Anwendung und Datenbank. Was der Betrieb voraussetzt und wie die Installation abläuft, beschreiben Voraussetzungen und Installation.

### Eine Instanz

Nova läuft als eine Instanz mit einem Anwendungsprozess. Die Hintergrund-Jobs laufen in diesem Prozess; mehrere parallele Instanzen würden sie mehrfach ausführen. Mehr Last trägt Nova über zusätzliche Threads im selben Prozess.

### SAP über RFC

Für SAP über RFC – als Zielsystem und als Quellsystem „SAP OM“ – braucht Nova das SAP NetWeaver RFC SDK, das von SAP bezogen wird. Ohne das SDK bleiben die SAP-Funktionen abgeschaltet; die übrigen Connectoren arbeiten unabhängig davon.

### SAP BTP mit Kyma

Für die Kyma-Laufzeit der SAP Business Technology Platform (Kubernetes) gibt es Vorlagen, die Anwendung und PostgreSQL bereitstellen – ebenfalls mit genau einer Instanz. Sie dienen derzeit Demo-Installationen. Die Edition Nova on BTP ist ab Q4/2026 angekündigt.

### KI

KI-Funktionen sind in jeder Variante optional. Statt eines Cloud-Anbieters lässt sich ein lokales Modell über Ollama anbinden – siehe KI in Nova.

KAPITEL 2

# Grundlagen

## 2.1 Identitäten und ihr Status

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Jede Person und jeder technische Akteur, dessen Zugänge Nova verwaltet, ist in Nova eine **Identität**. Ihr Status beschreibt, wo sie im Beschäftigungsverhältnis steht. Daraus folgt alles Weitere: ob sie sich anmelden darf, ob ihre Konten in den Zielsystemen aktiv sind und ob ihre Berechtigungen wirken.

### Der Grundsatz

**Nur aktive Identitäten dürfen etwas.** Jeder andere Status sperrt die Anmeldung an Nova, die Konten in den Zielsystemen und die Mitwirkung an Genehmigungen und Rezertifizierungen.

Nova setzt diese Regel als Positivliste um: Maßgeblich ist, ob eine Identität aktiv ist – nicht, ob ihr Status auf einer Sperrliste steht. Ein neu hinzukommender Status ist damit zunächst immer gesperrt.

### Die fünf Status

| Status | Anmelden, genehmigen, prüfen | Konten in Zielsystemen | Berechtigungen |
|---|---|---|---|
| **Vor Eintritt**<br>Vertrag unterschrieben, Eintritt liegt in der Zukunft | ● nein | ● vorbereitet, ● gesperrt | ● vorbereitet, wirksam ab Eintritt |
| **Aktiv**<br>beschäftigt | ● ja | ● aktiv | ● wirksam |
| **Ruhend**<br>vorübergehend ausgesetzt, z. B. Elternzeit, Sabbatical oder nach einem Sicherheitsvorfall | ● nein – Genehmigungen übernimmt die Vertretung | ● gesperrt | ● bleiben erhalten |
| **Ausgetreten**<br>Beschäftigung beendet | ● nein – Genehmigungen übernimmt die Vertretung | ● sofort gesperrt, nach der Aufbewahrungsfrist ● gelöscht | nach der Karenzzeit ● entzogen |

| | | | |
|---|---|---|---|
| **Papierkorb**<br>ausgetreten und zur endgültigen Löschung vorgemerkt | ● nein | ● gelöscht | ● entzogen |

**DIE KERNREGEL**

**Ruhend** heißt: Die Berechtigungen bleiben. Wer aus der Elternzeit zurückkommt, kann sofort weiterarbeiten.

**Ausgetreten** heißt: Die Berechtigungen gehen. Wer später wieder eintritt, beginnt ohne Altrechte.

## Karenzzeit nach dem Austritt

Beim Austritt sperrt Nova alle Konten der Identität sofort. Ihre Berechtigungen bleiben während einer einstellbaren **Karenzzeit** zugeordnet, wirken aber nicht, weil die Konten gesperrt sind.

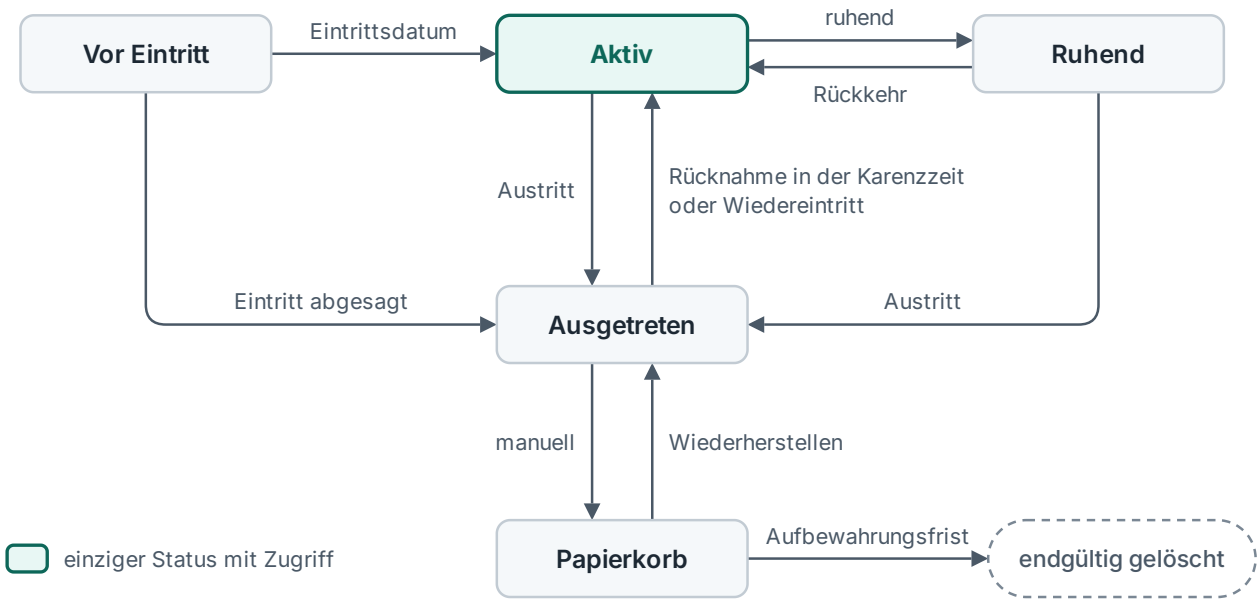
Die Karenzzeit hat zwei Zwecke:

- **Übergaben:** Solange die Berechtigungen zugeordnet sind, bleibt sichtbar, welche Aufgaben und Zugänge zu übergeben sind.
- **Korrekturen:** Ein versehentlich oder zu früh erfasster Austritt lässt sich zurücknehmen, ohne dass Berechtigungen neu beantragt werden müssen.

Nach Ablauf der Karenzzeit entzieht Nova die Berechtigungen – in Nova und in allen Zielsystemen.

## Übergänge

Ein Status ändert sich nur über festgelegte Abläufe. Nova protokolliert jeden Wechsel mit Zeitpunkt, auslösender Person oder auslösendem Prozess, Grund sowie dem Zustand vorher und nachher.




Übergänge zwischen den Status. Nur eine aktive Identität hat Zugriff.

| Von → nach | Auslöser | Was Nova tut |
|---|---|---|
| Vor Eintritt → Aktiv | Eintrittsdatum erreicht | Konten entsperren, Berechtigungen wirksam schalten |
| Vor Eintritt → Ausgetreten | Eintritt abgesagt | vorbereitete Konten und Berechtigungen verwerfen |
| Aktiv → Ruhend | ruhendes Beschäftigungsverhältnis laut HR oder manuelle Sperre | Konten sperren, laufende Sitzungen beenden, offene Genehmigungen an die Vertretung geben |
| Ruhend → Aktiv | Rückkehr | Konten entsperren; Berechtigungen unverändert |
| Aktiv oder Ruhend → Ausgetreten | Austrittsdatum erreicht, Austritt laut HR oder manueller Austritt | Konten sperren, laufende Sitzungen beenden, Eigentümerschaften übertragen, Karenzzeit starten |
| Ausgetreten → Aktiv, innerhalb der Karenzzeit | Austritt zurücknehmen | Konten entsperren; Berechtigungen bleiben erhalten |
| Ausgetreten → Aktiv, nach der Karenzzeit | Wiedereintritt | Neustart ohne Altrechte; Berechtigungen neu über Rollen und Anträge |
| Ausgetreten → Papierkorb | manuell | Identität ausblenden und zur endgültigen Löschung vormerken |
| Papierkorb → Ausgetreten | Wiederherstellen | nur den Datensatz zurückholen – ohne Zugriff |
| Papierkorb → endgültig gelöscht | Aufbewahrungsfrist abgelaufen | personenbezogene Daten entfernen; Protokolleinträge bleiben erhalten |

## Zuordnung aus SAP HCM

Übernimmt Nova Personaldaten aus SAP HCM, bestimmt der Beschäftigungsstatus (Infotyp 0000, Feld STAT2) den Status der Identität:

| Beschäftigungsstatus (STAT2) | Status in Nova |
|---|---|
| 3 – aktiv | Aktiv |
| 1 – inaktiv (ruhend) | Ruhend |
| 0 – ausgetreten | Ausgetreten |
| 2 – Rentner | Ausgetreten |

Ein Eintritt mit Datum in der Zukunft führt zu **Vor Eintritt**. Andere Quellsysteme bildet Nova über die Feldzuordnung auf dieselben Status ab.

# 2.2 Berechtigungsmodell

Nova ordnet Zugriff auf drei Ebenen: **Berechtigungen** in den Zielsystemen, **Business-Rollen** als Bündel von Berechtigungen und **Zuweisungen**, die beides mit Identitäten verbinden. Berechtigungen und Business-Rollen stehen unter „Rollen“ in eigenen Reitern.

## Berechtigungen

Eine Berechtigung ist ein einzelnes Recht in genau einem Zielsystem – eine SAP-Rolle (Einzel- oder Sammelrolle) oder eine Gruppe in Active Directory und LDAP, Microsoft Entra ID, Keycloak oder einer SCIM-fähigen Anwendung. Nova übernimmt diese Berechtigungen per Import aus dem Zielsystem; sie stehen im Reiter „System-Rollen“.

Daneben kennt Nova Berechtigungen ohne Zielsystem. Nova überträgt sie in kein Zielsystem:

- **„Nova Entitlements“** regeln, was jemand in Nova selbst darf. Voreingestellt sind „Admin“ für die Administration von Nova, „Security“ und „SoD Reviewer“ für Entscheidungen in bestimmten Genehmigungsschritten sowie „Manager“. Diese Berechtigung weist Nova Personen zu, die in einer Organisationseinheit als Manager gesetzt sind.
- **„Nova AI“** sind Fähigkeiten für KI-Agenten. Nur Identitäten vom Typ KI-Agent erhalten sie – siehe KI-Agenten als Identitäten.

## Business-Rollen

Eine Business-Rolle bündelt Berechtigungen – oft aus mehreren Zielsystemen – für eine fachliche Tätigkeit. Im Reiter „Zuweisungen“ einer Business-Rolle legen Administratoren je Zielsystem fest, welche Berechtigungen sie enthält. Außerdem trägt jede Business-Rolle:

- „Risiko“ – ihre Risikobewertung,
- „Owner“ – die verantwortliche Person,
- „Bereich“ – den fachlichen Bereich, der auch die Farbe bestimmt,
- „Genehmigungs-Workflow“ – den Ablauf für Anträge auf diese Business-Rolle.

Beantragen lassen sich nur Business-Rollen und Berechtigungen, denen ein Genehmigungs-Workflow mit mindestens einem Schritt zugeordnet ist – siehe Genehmigungsabläufe.

Ändern Administratoren den Inhalt einer Business-Rolle, passt Nova beim Speichern die Zuweisungen aller Identitäten an, die sie halten.

## Zuweisungen

Eine Zuweisung verbindet eine Identität mit einer Business-Rolle oder einer Berechtigung. Nova unterscheidet drei Typen:

| Typ | Bedeutung |
|---|---|

| | |
|---|---|
| Business-Rolle | Die Identität hält eine Business-Rolle. |
| indirekt | Eine Berechtigung aus einer zugewiesenen Business-Rolle. Nova legt sie mit der Business-Rolle an und entfernt sie mit ihr. |
| direkt | Eine einzelne Berechtigung ohne Business-Rolle – etwa aus einem genehmigten Antrag auf diese Berechtigung, aus der Übernahme eines Kontos aus dem Zielsystem oder eine Nova-eigene Berechtigung. |

Eine Identität hält jede Business-Rolle höchstens einmal. KI-Agenten erhalten keine Business-Rollen.

## Gültigkeit

Zuweisungen haben in Nova einen Gültigkeitszeitraum, „Gültig ab“ und „Gültig bis“. Er beschreibt den Soll-Zustand:

- Eine Business-Rolle ohne Beginn gilt ab dem Tag der Zuweisung. Das Ende ist optional und darf nicht vor dem Beginn liegen; ohne Ende gilt die Zuweisung unbefristet.
- Die indirekten Zuweisungen übernehmen den Zeitraum ihrer Business-Rolle.
- Das Ende zählt mit: Eine Zuweisung gilt bis einschließlich des Tages unter „Gültig bis“.
- Für SAP hält Nova zusätzlich den Zeitraum fest, den es zuletzt aus SAP gelesen hat – den Ist-Zustand.

Was zu Beginn und am Ende eines Zeitraums geschieht, beschreibt Wie Zugriff entsteht und verschwindet.

## Organisationseinheiten und Planstellen

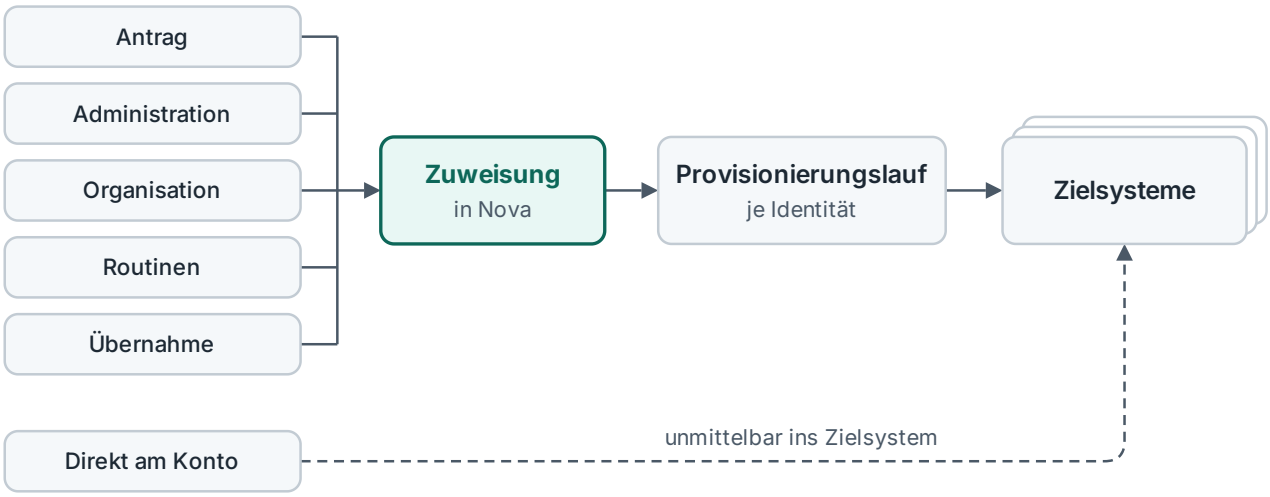
Business-Rollen lassen sich an Organisationseinheiten hängen; die Mitglieder der Einheit erhalten sie als eigene Zuweisung. Ist bei einer Einheit „Vererbung“ eingeschaltet, erhalten ihre Mitglieder zusätzlich die Business-Rollen aller übergeordneten Einheiten. Mit dem Zusatzmodul „Planstellen (OSP)“ tragen auch Planstellen Business-Rollen; ihre Inhaber erhalten sie zusammen mit denen der Einheit, zu der die Planstelle gehört. Einzelheiten beschreibt Organisation und Planstellen.

## Risikobewertung

Jede Berechtigung und jede Business-Rolle trägt eine Risikobewertung: „Kein Risiko“, „Niedrig“, „Mittel“, „Kritisch“ oder „Nicht bewertet“. Voreingestellt ist „Nicht bewertet“. Wie Nova Risiken darüber hinaus bewertet, beschreibt Risikobewertung.

# 2.3 Wie Zugriff entsteht und verschwindet

In Nova ist Zugriff eine Zuweisung (siehe Berechtigungsmodell). In die Zielsysteme bringt Nova Zuweisungen durch Provisionierung. Diese Seite beschreibt, wie Zuweisungen entstehen und enden und wann Nova sie überträgt.




Zuweisungen entstehen auf fünf Wegen und gelangen per Provisionierungslauf in die Zielsysteme. Änderungen direkt am Konto schreibt Nova unmittelbar.

## Wie Zugriff entsteht

| Weg | Was geschieht |
|---|---|
| Antrag | Ist über einen Antrag abschließend entschieden, weist Nova die genehmigten Business-Rollen und Berechtigungen zu – siehe Zugriff beantragen. |
| Administration | Administratoren weisen einer Identität Business-Rollen zu, auf Wunsch mit Gültigkeitszeitraum. |
| Organisation | Mitglieder einer Organisationseinheit und Inhaber einer Planstelle erhalten deren Business-Rollen – siehe Organisation und Planstellen. |
| Routinen | Schritte in Routinen können Business-Rollen zuweisen, etwa über die Planstelle – siehe Eintritt, Wechsel, Austritt. |
| Übernahme | Liest Nova Konten aus einem Zielsystem ein, kann es deren vorhandene Berechtigungen als direkte Zuweisungen übernehmen – je nach Import-Einstellung. |
| Direkt am Konto | Administratoren ändern Rollen oder Gruppen eines Kontos bei der Identität im Reiter „Systeme“; Nova schreibt diese Änderung unmittelbar in das Zielsystem. |

## Wann Nova in die Zielsysteme überträgt

Nova überträgt Zuweisungen in **Provisionierungsläufen**. Ein Lauf gilt einer Identität: Für jedes betroffene Zielsystem prüft er das Konto, legt es bei Bedarf an und überträgt die Berechtigungen. Scheitert ein Schritt in einem Zielsystem, laufen die Schritte für die anderen Zielsysteme weiter. Die Läufe stehen unter „Monitoring“ → „Provisioning-Log“.

Nach der Installation ist die Einstellung „Zielsysteme automatisch provisionieren“ ausgeschaltet („Administration“ → „Provisionierung“ → „Mapping“, Reiter „Provisioning-Einstellungen“). Ist sie eingeschaltet, startet Nova einen Lauf, wenn

- Administratoren die Business-Rollen einer Identität ändern – zuweisen, entziehen oder den Zeitraum ändern,
- über einen Antrag abschließend entschieden ist; übertragen werden die genehmigten Positionen,
- Administratoren nach einer Änderung am Inhalt einer Business-Rolle „Änderungen auf Nutzer anwenden“ wählen; dann startet je Identität, die die Business-Rolle hält, ein Lauf. Bis dahin zeigt die Business-Rolle „Änderungen ausstehend“,
- eine Routine Zuweisungen geändert hat – auch die Routine „Wechsel“, die Nova ausführt, nachdem eine Person in eine Organisationseinheit aufgenommen, aus ihr entfernt oder in eine andere verschoben wurde,
- beim Abschluss einer Rezertifizierung die Entzüge ausgeführt werden,
- ein Job „Abgelaufene Zuweisungen bereinigen“ abgelaufene Zuweisungen entfernt.

Schritte von Routinen, die Konten sperren, entsperren oder löschen, starten dafür eigene Läufe für die verknüpften Konten der Identität – auch bei ausgeschalteter automatischer Provisionierung.

Nova überträgt nur Berechtigungen, die zu einem Zielsystem gehören. Hat eine Identität dieselbe Berechtigung aus mehreren Zuweisungen, entfernt Nova sie im Zielsystem erst, wenn keine dieser Zuweisungen mehr gilt.

Abweichungen zwischen Nova und einem Zielsystem zeigt der Reiter „Abgleich & Provisionierung“ einer Identität. Administratoren lösen sie dort je Zielsystem in die eine oder die andere Richtung auf.

## Beginn und Ende der Gültigkeit

**Beginn.** An SAP überträgt Nova eine Rolle zusammen mit Beginn und Ende; auch eine vorausdatierte Zuweisung geht deshalb gleich mit dem Lauf nach SAP. An Active Directory und LDAP, Microsoft Entra ID, SCIM und Keycloak überträgt Nova keine Gültigkeitszeiträume; dort hält Nova eine vorausdatierte Zuweisung zurück. Der Job „Vorausdatierte Zuweisungen aktivieren“ überträgt sie für aktive Identitäten, sobald ihr Beginn erreicht ist; voreingestellt läuft er täglich um 02:30 Uhr.

**Ende.** Abgelaufene Zuweisungen entfernt der Job „Abgelaufene Zuweisungen bereinigen“: Er löscht Zuweisungen, deren Ende überschritten ist, und startet bei eingeschalteter automatischer Provisionierung Läufe, die die Berechtigungen aus den Zielsystemen entfernen. Nova richtet diesen Job nicht selbst ein; Administratoren legen ihn unter „Monitoring“ → „Hintergrund-Jobs“ mit „Neuer Job“ an und geben ihm einen Zeitplan – siehe Überwachung und Jobs.

## Wie Zugriff verschwindet

| Weg | Was geschieht |
|---|---|
| Entzug | Administratoren entziehen einer Identität eine Business-Rolle; Nova entfernt sie samt ihren indirekten Zuweisungen. |
| Ablauf | Der Job „Abgelaufene Zuweisungen bereinigen“ entfernt Zuweisungen, deren Ende überschritten ist. |
| Rezertifizierung | Beim Abschluss einer Kampagne können Administratoren die Entzüge ausführen lassen; Nova entfernt dann die entzogenen Zuweisungen. |
| Organisation | Verlässt eine Person eine Organisationseinheit, verliert sie deren Business-Rollen, sofern keine andere Einheit oder Planstelle sie ihr gewährt. |
| Austritt | Die Routine „Austritt“ startet in der Voreinstellung Läufe, die die verknüpften Konten der Identität sperren; Zuweisungen entfernt sie nur mit einem zusätzlichen Schritt – siehe Eintritt, Wechsel, Austritt. |

Ob und wann eine dieser Änderungen die Zielsysteme erreicht, beschreibt der Abschnitt „Wann Nova in die Zielsysteme überträgt“ oben.

# 2.4 Begriffe

Dieses Handbuch verwendet die folgenden Begriffe durchgehend. In Klammern steht jeweils der englische Begriff.

### Abgleich (Reconciliation)

Vergleich zwischen dem, was in Nova für eine Identität vorgesehen ist, und dem, was im Zielsystem tatsächlich vorhanden ist. Nova zeigt Abweichungen an und lässt sie in die eine oder die andere Richtung auflösen.

### Antrag (Access request)

Anfrage auf eine Berechtigung oder Business-Rolle, über die ein Genehmigungsablauf entscheidet.

### Aufbewahrungsfrist (Retention period)

Zeitraum, für den Nova eine Identität im Papierkorb aufbewahrt, bevor ihre Daten endgültig gelöscht werden.

### Berechtigung (Entitlement)

Ein einzelnes Recht in einem Zielsystem, zum Beispiel eine SAP-Rolle oder eine Gruppe im Active Directory.

### Business-Rolle (Business role)

Ein Bündel von Berechtigungen – oft über mehrere Zielsysteme hinweg –, das eine fachliche Tätigkeit beschreibt. Wer eine Business-Rolle erhält, erhält alle enthaltenen Berechtigungen.

### Eintritt, Wechsel, Austritt (Joiner, mover, leaver)

Die drei Ereignisse im Lebenszyklus einer Identität. Für jedes führt Nova einen festgelegten Ablauf aus, etwa Konten anlegen, Berechtigungen anpassen oder Konten sperren.

### Genehmiger (Approver)

Person, die einen Antrag freigibt oder ablehnt. Wer genehmigt, legt der Genehmigungsablauf fest.

### Identität (Identity)

Eine Person oder ein technischer Akteur, dessen Zugänge Nova verwaltet. Eine Identität kann in mehreren Zielsystemen Konten besitzen. Siehe Identitäten und ihr Status.

### Karenzzeit (Grace period) geplant

Frist nach einem Austritt, während der die Berechtigungen einer Identität zugeordnet bleiben, bevor Nova sie entzieht. Siehe Karenzzeit nach dem Austritt.

### Konto (Account)

Der Zugang einer Identität zu einem Zielsystem, zum Beispiel ein SAP-Benutzer oder ein Konto im Active Directory. Ein Konto gehört immer genau einer Identität.

### Papierkorb (Trash)

Ablage für gelöschte Identitäten. Von dort lassen sich Identitäten wiederherstellen oder endgültig löschen.

### Protokoll (Audit log)

Chronologischer Nachweis sicherheitsrelevanter Aktionen: wer hat wann was getan.

### Provisionierung (Provisioning)

Das Übertragen von Konten und Berechtigungen aus Nova in die Zielsysteme.

### Quellsystem (Source system)

System, aus dem Nova Daten über Identitäten übernimmt – typischerweise das Personalsystem, zum Beispiel SAP HCM.

### Rezertifizierung (Recertification)

Regelmäßige Überprüfung, ob bestehende Berechtigungen noch benötigt werden. Berechtigungen, deren Bedarf verneint wird, entzieht Nova.

### Wiedereintritt (Rehire)

Rückkehr einer ausgetretenen Identität. Nova führt dafür einen eigenen, festgelegten Ablauf aus.

### Zielsystem (Target system)

System, in dem Nova Konten und Berechtigungen verwaltet – zum Beispiel SAP, Active Directory und LDAP, Microsoft Entra ID, Keycloak oder SCIM-fähige Anwendungen.

KAPITEL 3

# Lebenszyklus

## 3.1 Eintritt, Wechsel, Austritt

Für die Ereignisse im Lebenszyklus einer Identität – Eintritt, Wechsel, Austritt, Wiedereintritt und Archivierung – kennt Nova je eine **Routine**: eine Folge von Schritten. Administratoren legen die Schritte unter „Administration“ → „Identitätsmanagement“ → „Benutzer-Lebenszyklus“ fest; je Routine lassen sich Schritte hinzufügen, per Anfasser umsortieren und einzeln ein- und ausschalten.

### Die Routinen und ihre Auslöser

#### Eintritt

- **Auslöser:** Im Dashboard listet das Fenster „HR-Integration“ die Eintritte des Tages aus dem HR-Import. „Onboarden“ startet die Routine für die ausgewählten Personen, nach einer Vorschau der Schritte.
- **Voreinstellung:** „Setze Identität aktiv - Entsperrung von Konten“ und „Setze Identität auf Planstelle“.

#### Wechsel

- **Auslöser:** der HR-Import, wenn sich die Planstelle einer Person geändert hat; das Aufnehmen einer Person in eine Organisationseinheit, ihr Entfernen oder Verschieben; „Umsetzen“ im Fenster „HR-Integration“.
- **Voreinstellung:** „Setze Identität auf Planstelle“.

#### Austritt

- **Auslöser:** der Job „Austrittsdatum-Scan“ (voreingestellt täglich um 02:00 Uhr) für aktive Identitäten, deren Austrittsdatum überschritten ist; das Löschen einer Identität, die Nova danach in den Papierkorb legt.
- **Voreinstellung:** „Ownership-Übergabe für KI-Agenten“ und „Setze Identität inaktiv - Sperrung von Konten“. Zuweisungen entzieht die voreingestellte Routine nicht; dafür lässt sich etwa „Entzug aller bestehenden Berechtigungen (Clean Start)“ ergänzen.

Eine Karenzzeit, nach der Nova die Berechtigungen ausgetretener Identitäten entzieht, sieht das Statusmodell unter Identitäten und ihr Status vor. geplant

#### Wiedereintritt

- **Auslöser:** Der HR-Import findet eine aktive Person, deren Identität im Papierkorb liegt – erkannt an Personalnummer oder E-Mail-Adresse –, und holt die Identität zurück.

- **Voreinstellung:** „Entzug aller bestehenden Berechtigungen (Clean Start)“, ausgeschaltet. Zuweisungen, die die Identität noch hat, bleiben damit erhalten; ist der Schritt eingeschaltet, beginnt sie ohne Altrechte.

### Archivierung

- **Auslöser:** das endgültige Löschen einer Identität aus dem Papierkorb – über „Endgültig löschen“ oder durch einen Job vom Typ „Gelöschte Users bereinigen“. Dieser Job löscht Identitäten, die länger als die Aufbewahrungsfrist im Papierkorb liegen; voreingestellt sind 90 Tage, einstellbar unter „Aufbewahrung (Tage)“.
- **Voreinstellung:** keine Schritte.

## Die Schritte

| Schritt | Wirkung |
|---|---|
| „Setze Identität aktiv - Entsperrung von Konten“ | setzt die Identität aktiv und startet einen Lauf, der ihre verknüpften Konten in den Zielsystemen entsperrt |
| „Setze Identität inaktiv - Sperrung von Konten“ | setzt die Identität inaktiv und startet einen Lauf, der ihre verknüpften Konten sperrt |
| „Setze Identität auf Planstelle“ | setzt die Identität auf die Planstelle aus den Personaldaten (Attribut P0001-PLANS); sie erhält deren Business-Rollen. Setzt das Zusatzmodul „Planstellen (OSP)“ voraus |
| „Zuweisung Standardmitarbeiterrolle“ | weist die Business-Rolle mit der Kennung `standard-mitarbeiter` zu, sofern es sie gibt |
| „Entzug aller bestehenden Berechtigungen (Clean Start)“ | entfernt alle Zuweisungen der Identität |
| „Irreversible Löschung von Backend Konten“ | startet einen Lauf, der alle verknüpften Konten in den Zielsystemen endgültig löscht |
| „Ownership-Übergabe für KI-Agenten“ | überträgt die KI-Agenten der austretenden Person an ihre Vertretung, sonst an ihre aus der Organisation abgeleitete Führungskraft; ohne Nachfolger markiert Nova den Agenten als verwaist |

Über „Methoden verwalten“ legen Administratoren eigene Methoden an. Sie bestehen ausschließlich aus Bausteinen eines festen Katalogs – etwa Status setzen, Business-Rolle zuweisen oder entziehen, Konto anlegen, sperren oder löschen, Antrag stellen – und lassen sich an Bedingungen zu Feldern der Identität knüpfen. Ist KI eingeschaltet, schlägt „Mit KI generieren“ eine Methode aus einer Beschreibung in Worten vor. „Testen“ führt eine Methode an einer gewählten Identität wirklich aus; es ist kein Probelauf.

## So läuft eine Routine ab

- Nova führt die eingeschalteten Schritte in der festgelegten Reihenfolge aus.
- Scheitert ein Schritt, nimmt Nova dessen Änderungen zurück und fährt mit dem nächsten Schritt fort.

- Haben die Schritte Zuweisungen geändert, startet Nova bei eingeschalteter automatischer Provisionierung je Identität einen Provisionierungslauf. Schritte, die Konten sperren, entsperren oder löschen, starten ihre Läufe auch bei ausgeschalteter automatischer Provisionierung – siehe Wie Zugriff entsteht und verschwindet.

# 3.2 Anbindung an HR

Nova übernimmt Personaldaten aus einem Quellsystem, legt daraus Identitäten an und hält sie aktuell. Quellsysteme richten Administratoren unter „Systeme“ → „Quellsysteme“ mit „Quellsystem hinzufügen“ ein.

## Zwei Arten von Quellsystemen

| Typ | Liefert | Verbindung |
|---|---|---|
| „Nova HR Stage“ | Personaldaten: Stammdaten, Beschäftigungsstatus, Planstelle | Staging-Bereich in der Nova-Datenbank |
| „SAP OM“ | Organisationsstruktur: Organisationseinheiten und Planstellen | SAP über RFC |

Das Quellsystem „SAP OM“ beschreibt Organisation und Planstellen. Diese Seite behandelt die Personaldaten.

## Personaldaten im Format von SAP HCM

Die Personaldaten stellt ein Export aus dem Personalsystem im Staging-Bereich von „Nova HR Stage“ bereit; wie dieser Export eingerichtet wird, legt das Einführungsprojekt fest. „Nova HR Stage“ erwartet je Person eine Personalnummer und Attribute, die nach Infotyp und Feld von SAP HCM benannt sind – etwa `P0002-VORNA` für den Vornamen. Werte können einen Gültigkeitszeitraum tragen. In der Voreinstellung übernimmt Nova Attribute dieser Infotypen:

| Infotyp | Daraus übernimmt Nova |
|---|---|
| 0000 Maßnahmen | Personalnummer, Beschäftigungsstatus (STAT2), Eintritts- und Austrittsdatum |
| 0001 Organisatorische Zuordnung | Abteilung, Planstelle (PLANS), Stellenbeschreibung, Standort, Gebäude, Etage, Raum |
| 0002 Daten zur Person | Vorname, Nachname, Anrede, akademischer Titel, Namenszusatz |
| 0105 Kommunikation | E-Mail-Adresse, Telefon, Mobiltelefon, Logon-UID |

In der Feldzuordnung heißt das Feld für die Planstelle „Werk“.

Als aktiv gilt eine Person, wenn ihr Beschäftigungsstatus (STAT2) den Wert 3 hat; jeder andere Wert gilt als nicht aktiv. Liefert die Quelle keinen Beschäftigungsstatus, gilt die Person als aktiv. Eine feinere Zuordnung, etwa für ruhende Beschäftigung, beschreibt Identitäten und ihr Status. geplant

## Feldzuordnung

Welches Attribut in welches Feld der Identität fließt, legen Administratoren unter „Administration“ → „Provisionierung“ → „Mapping“ im Reiter „Quellsystem“ fest. Für jedes Feld gibt es vier Möglichkeiten: ein Quell-Attribut, einen „Festwert“, einen „Ausdruck“, der Attribute umformt oder kombiniert, oder „Deaktiviert“. Ohne eigene Zuordnung gilt die Voreinstellung aus der Tabelle oben. Die „Vorschau“ zeigt das Ergebnis für eine Personalnummer; bei eingeschalteter KI schlägt „Vorschlag generieren“ einen Ausdruck vor.

Mit welchem Status Nova neue Identitäten anlegt, bestimmt der „Joiner-Status“ im „Feld-Mapping“ des Quellsystems: „Onboarding“ (Voreinstellung) oder „Aktiv“.

## Vom Quellsystem zur Identität

Das Quellsystem bietet dafür eigene Schaltflächen:

1. **„Rohdaten einlesen“** übernimmt die bereitgestellten Personaldaten in die Arbeitstabelle, mit der Simulation und Import arbeiten. Die Quelle gilt dabei als maßgeblich: Leere Werte überschreiben vorhandene.
2. **„Simulieren“** zeigt, was ein Import ändern würde, und ändert selbst nichts.
3. **„Personen importieren“** führt den Import aus – für alle Personen oder für eine Auswahl. Zeitgesteuert übernimmt diesen Schritt ein Job vom Typ „HR-Nutzer importieren“.

„Person debuggen“ zeigt für eine Personalnummer die Rohdaten, die Zuordnung und die daraus berechneten Werte.

Nova findet die Identität einer Person über die Personalnummer, ersatzweise über die E-Mail-Adresse, und ordnet jede Person ein:

| Einordnung | Bedeutung | Was der Import tut |
|---|---|---|
| „Joiner“ | aktiv, in Nova noch keine Identität | legt eine Identität mit dem „Joiner-Status“ an |
| „Mover“ | Planstelle laut Quelle weicht von der in Nova ab | schreibt die Änderungen, danach läuft die Routine „Wechsel“ |
| „Update“ | andere Angaben geändert | schreibt die Änderungen |
| „Leaver“ | nicht mehr aktiv, Identität in Nova noch aktiv | nichts, siehe unten |
| „Unverändert“ | keine Änderung | nichts |

Abgesehen vom Wiedereintritt ändert der Import den Status vorhandener Identitäten nicht. Die Routine „Eintritt“ starten Administratoren im Dashboard mit „Onboarden“ – siehe Eintritt, Wechsel, Austritt.

**Austritt.** Personen, die nicht mehr aktiv sind, verarbeitet der Import nicht. Solange eine Person aktiv ist, übernimmt er aber ihr Austrittsdatum, sofern die Quelle eines liefert. Ist es überschritten, startet der Job „Austrittsdatum-Scan“ die Routine „Austritt“.

**Wiedereintritt.** Findet der Import eine aktive Person, deren Identität im Papierkorb liegt, holt er die Identität zurück und startet die Routine „Wiedereintritt“.

## Datumsangaben und künftige Änderungen

Nova verwendet von jedem Attribut den Wert, der am Tag des Einlesens gilt. Gilt an diesem Tag noch kein Wert, übernimmt Nova den nächsten künftigen. Eine künftige Änderung wird damit wirksam, wenn Nova die Daten an oder nach ihrem Stichtag einliest und importiert. Gilt eine neue Planstelle bereits, übernimmt Nova ihren Beginn aus dem Gültigkeitszeitraum der Quelle – auch wenn der Import erst später läuft.

# 3.3 Organisation und Planstellen

Die Organisation in Nova besteht aus Organisationseinheiten und – mit dem Zusatzmodul „Planstellen (OSP)“ – aus Planstellen. Sie bestimmt, welche Business-Rollen Personen über ihre Einheit oder Planstelle erhalten und wer als Führungskraft gilt. Administratoren pflegen sie unter „Organisation“.

## Organisationseinheiten

Organisationseinheiten bilden eine Hierarchie: Jede Einheit hat höchstens eine übergeordnete Einheit. Nova vergibt für jede Einheit eine achtstellige Objekt-ID; Einheiten aus SAP OM tragen die Objekt-ID aus SAP.

- **Mitglieder:** „Person hinzufügen“ nimmt eine Person in die Einheit auf. Nova setzt dabei ihre Abteilung auf die Objekt-ID der Einheit.
- **Manager:** Die Schaltfläche „Manager“ bei einem Mitglied macht es zum Manager der Einheit; ein weiterer Klick nimmt das zurück. Nova weist Managern die Nova-eigene Berechtigung „Manager“ zu und entzieht sie wieder, wenn die Person nirgends mehr Manager ist. Wer in eine andere Einheit verschoben wird, verliert den Manager-Status.
- **Business-Rollen:** Eine über „Business-Rolle zuweisen…“ angehängte Business-Rolle erhalten die Mitglieder der Einheit. Nimmt ein Administrator sie wieder von der Einheit, entzieht Nova sie den Mitgliedern; wer sie auch über eine andere Einheit erhält, behält sie.
- **Vererbung:** Ist „Vererbung“ eingeschaltet („Business-Rollen übergeordneter Einheiten erben“), erhalten die Mitglieder der Einheit zusätzlich die Business-Rollen aller übergeordneten Einheiten. Voreingestellt ist sie ausgeschaltet.

Business-Rollen, die ein Mitglied über seine Einheit erhält, lassen sich an der Identität nicht einzeln entfernen – nur, indem die Person die Einheit verlässt oder die Business-Rolle von der Einheit genommen wird.

Nimmt ein Administrator eine Person in eine Einheit auf, entfernt er sie oder verschiebt er sie in eine andere, führt Nova anschließend die Routine „Wechsel“ aus – siehe Eintritt, Wechsel, Austritt.

## Planstellen

Planstellen gibt es mit dem Zusatzmodul „Planstellen (OSP)“. Administratoren schalten es unter „Administration“ → „Plugins“ ein; nach einem Neustart zeigt eine Einheit den Reiter „Planstellen“.

- Eine Planstelle gehört zu genau einer Organisationseinheit und kann Inhaber haben. Eine Planstelle mit „Leitung“ führt die Einheit: Ihr Inhaber gilt als Manager der Einheit.
- Business-Rollen lassen sich direkt an eine Planstelle hängen. Der Inhaber erhält sie zusammen mit den Business-Rollen der Einheit, zu der die Planstelle gehört – bei eingeschalteter „Vererbung“ auch mit denen der übergeordneten Einheiten.
- Eine Identität besetzt jeweils höchstens eine Planstelle. Wird sie auf eine neue gesetzt, endet die bisherige Besetzung; Business-Rollen, die nur die bisherige Planstelle gewährt hat, entzieht Nova.

- Aus den Personaldaten setzt der Routine-Schritt „Setze Identität auf Planstelle“ eine Identität auf die Planstelle, die das Attribut P0001-PLANS nennt. Dazu braucht es in Nova eine Planstelle mit dieser Objekt-ID, etwa aus dem Abgleich mit SAP OM.

## Struktur aus SAP OM

Das Quellsystem „SAP OM“ liest die Organisationsstruktur über RFC aus SAP (Tabellen HRP1000 und HRP1001), begrenzt auf eine „Planvariante“ (voreingestellt 01). Über „Wurzel-Orgeinheit (optional)“ lässt sich der Ausschnitt weiter eingrenzen.

- „Org-Struktur lesen“ legt das Ergebnis als Job-Lauf ab und ändert nichts an Nova.
- „Org-Struktur abgleichen“ legt Organisationseinheiten und – mit dem Zusatzmodul – Planstellen in Nova an oder aktualisiert sie, erkannt an der Objekt-ID. Namen, übergeordnete Einheit und leitende Planstellen übernimmt Nova aus SAP. Inhaber setzt der Abgleich nicht; sie kommen über die Personaldaten – siehe Anbindung an HR.

Im Baum unter „Organisation“ zeigt ein farbiger Punkt, ob eine Einheit aus SAP OM stammt und ob ihre übergeordnete Einheit noch mit SAP übereinstimmt.

## Führungskräfte

Bei Anträgen für eine Identität gehen Genehmigungsschritte vom Typ „Manager“ an ihre Führungskraft. Das ist der „Manager“, der bei der Identität eingetragen ist. Fehlt dieser Eintrag, leitet Nova die Führungskraft aus der Organisation ab: Maßgeblich ist der nächste Manager in der Einheit der Identität – ein als Manager gesetztes Mitglied oder der Inhaber der leitenden Planstelle –, andernfalls der nächste in den übergeordneten Einheiten. In der „Übersicht“ der Identität steht die abgeleitete Führungskraft als „Org-abgeleitet“.

Wann Nova Änderungen an Zuweisungen in die Zielsysteme überträgt, beschreibt Wie Zugriff entsteht und verschwindet.

KAPITEL 4

# Zielsysteme

## 4.1 Überblick

Ein **Zielsystem** ist ein System, in dem Nova Konten und Berechtigungen verwaltet. Nova spricht Zielsysteme über Connectoren an; fünf bringt Nova mit:

- SAP – ABAP-Systeme über RFC und BAPIs
- Active Directory und LDAP
- Microsoft Entra ID – über Microsoft Graph
- Keycloak – über die Admin-API
- SCIM – Anwendungen mit SCIM-2.0-Schnittstelle

Zielsysteme vom Typ „Sonstiges“ haben keinen Connector; mit ihnen tauscht Nova keine Daten aus.

### Was Nova in Zielsystemen verwaltet

Alle fünf Connectoren beherrschen dieselben Grundfunktionen:

- **Konten** anlegen, Stammdaten ändern, sperren, entsperren und löschen
- **Passwörter** setzen
- **Berechtigungen** zuweisen und entziehen – in SAP sind das Rollen, in den übrigen Zielsystemen Gruppen
- den **Zustand** eines Kontos lesen: ob es existiert, ob es gesperrt ist und, soweit das Zielsystem es liefert, wann es zuletzt benutzt wurde

Den Katalog der Rollen oder Gruppen übernimmt Nova per Import-Job als Berechtigungen. Welche Stammdaten einer Identität in welches Attribut des Zielsystems fließen, legen Administratoren unter „Administration“ → „Provisionierung“ → „Mapping“ fest.

| Zielsystem | Berechtigungen | Sperren über | Gültigkeit |
|---|---|---|---|
| SAP | Einzel- und Sammelrollen | SAP-Benutzersperre | im Zielsystem |
| Active Directory | Gruppen, auch verschachtelt | `userAccountControl` | in Nova |
| LDAP | Gruppen | Password Policy | in Nova |
| Entra ID | Gruppen | `accountEnabled` | in Nova |
| Keycloak | Gruppen | `enabled` | in Nova |
| SCIM | Gruppen | `active` | in Nova |

**Gültigkeit:** Nur SAP kennt Gültigkeitszeiträume von Rollenzuweisungen selbst. Nova überträgt Beginn und Ende dorthin mit, auch wenn eine Zuweisung erst in der Zukunft beginnt. Die übrigen Zielsysteme kennen nur „Mitglied oder nicht“. Dort hält Nova eine vorausdatierte Zuweisung zurück, bis ihr Beginn erreicht ist. Ein voreingestellter Job vom Typ „Vorausdatierte Zuweisungen aktivieren“ provisioniert solche Zuweisungen aktiver Identitäten täglich um 2:30 Uhr (Zeitzone Europe/Berlin).

## Zielsystem einrichten

Administratoren legen ein Zielsystem unter „Systeme“ → „Zielsysteme“ → „Zielsystem hinzufügen“ an. Nur Administratoren können Zielsysteme anlegen, ändern oder löschen. Zu einem Zielsystem mit Connector gehören:

- **„Verbindung“** – Adresse und Zugangsdaten, seltene Einstellungen unter „Erweitert“. Welche Felder es gibt, steht auf den Seiten der einzelnen Connectoren.
- **„Account-Einrichtung“** – „Account-ID-Vorlage“, „Passwort-Ruleset“ und „Account-ID-Ruleset“. Alle drei sind Pflicht; ohne sie speichert Nova das Zielsystem nicht. Die Regelwerke pflegen Administratoren unter „Administration“ → „Provisionierung“ → „Passwortregeln“ bzw. „Nutzerkonto-Regeln“.

### Kontokennungen

Die „Account-ID-Vorlage“ legt fest, wie Nova die Kennung eines neuen Kontos bildet, z. B. `{first_initial_lower}{name_lower}` → `emustermann`. Platzhalter gibt es für Vor- und Nachname, Initiale, vollständigen Namen, E-Mail-Adresse, Personalnummer und Abteilung; Namensbestandteile auch in Klein- oder Großschreibung. Akzente und Umlaute entfernt Nova (Müller → Muller). Ein unbekannter Platzhalter führt zu einem Fehler statt zu einer falschen Kennung.

Legt ein Provisionierungslauf ein Konto an, bildet Nova die Kennung aus der Vorlage und kürzt sie auf die Höchstlänge des „Account-ID-Ruleset“. Ist die Kennung in Nova oder im Zielsystem bereits vergeben, hängt Nova eine Zahl an (`emustermann2`, `emustermann3` … bis höchstens 99). Künftig hängt Nova die Zahl nur noch an, wenn die Kennung in Nova vergeben ist; existiert im Zielsystem ein Konto mit dieser Kennung, das Nova nicht kennt, meldet Nova einen Konflikt – siehe Konten und Passwörter. geplant

Das **„Account-ID-Ruleset“** begrenzt Länge und erlaubte Sonderzeichen oder schreibt einen regulären Ausdruck vor. Beim manuellen Anlegen und beim Verknüpfen eines Kontos prüft Nova die Kennung dagegen. Für jeden Connector bringt Nova ein Standard-Regelwerk mit, etwa höchstens 12 Zeichen für SAP.

Das **„Passwort-Ruleset“** gilt für manuell eingegebene Passwörter beim Anlegen eines Kontos und beim Setzen eines Passworts. Initialpasswörter, die Nova selbst erzeugt, sind zufällig, richten sich nach dem Regelwerk und haben mindestens 12 Zeichen.

## Verbindung prüfen

„Status prüfen“ in der Liste der Zielsysteme oder im Detail eines Zielsystems testet die Verbindung und speichert das Ergebnis – „online“ oder „offline“ mit Fehlermeldung. Was geprüft wird, hängt vom Connector ab:

| Zielsystem | Test |
| --- | --- |
| SAP | Aufruf von `RFC_PING` |
| Active Directory, LDAP | Anmeldung (Bind) mit dem Dienstkonto |
| Entra ID | Abruf eines Zugriffstokens |
| Keycloak | Token-Abruf und Zählen der Konten im Realm |
| SCIM | Abruf von `ServiceProviderConfig`, ersatzweise der Base URL |

Ein erfolgreicher Test belegt Erreichbarkeit und Anmeldung, nicht jede Berechtigung, die Nova später im Zielsystem braucht.

Zusätzlich prüft ein voreingestellter Job vom Typ „Zielsystem-Health-Poll“ alle zehn Minuten die Erreichbarkeit der Zielsysteme. Wird ein System dabei neu als offline erkannt, vermerkt Nova das im „Audit-Log“.

## Zugangsdaten

Passwörter, Client-Secrets und Tokens der Zielsysteme speichert Nova verschlüsselt in der Datenbank. Den Schlüssel stellt der Betreiber beim Start bereit; er liegt nicht in der Datenbank. Gespeicherte Geheimnisse gibt Nova weder in der Oberfläche noch über die Programmierschnittstelle zurück; an ihrer Stelle steht ein Platzhalter. Wer ein Geheimnis ändern will, gibt einen neuen Wert ein. Über den KI-Assistenten lassen sich Geheimnisse weder lesen noch setzen.

## Nachvollziehbarkeit

Schreibvorgänge der Connectoren in Zielsystemen hält Nova im Änderungsjournal fest – mit den Werten vorher und nachher.

# 4.2 SAP

Nova verwaltet in SAP-ABAP-Systemen Konten – in SAP „Benutzer“ genannt – und ihre Rollen. Dazu ruft Nova per RFC Standard-BAPIs und den Funktionsbaustein `RFC_READ_TABLE` auf.

> **VORAUSSETZUNG: SAP NETWEAVER RFC SDK**
>
> Nova nutzt für RFC die Python-Bibliothek pyrfc, die das SAP NetWeaver RFC SDK voraussetzt. Das SDK liefert Nova nicht mit; der Betreiber bezieht es von SAP. Ohne SDK stehen die SAP-Funktionen nicht zur Verfügung.

## Verbindung

Ein Zielsystem steht für ein SAP-System mit einem Mandanten. Die Felder: „SID“, „Application Server Host“, „System-Nummer“, „Mandant“, „Benutzer“ und „Passwort“ des RFC-Benutzers sowie „Sprache“. Unter „Erweitert“ stehen „Message-Server-Host“, „Message-Server-Port“ und „Logon-Gruppe“ für die Lastverteilung sowie der „SAP-Router-String“. „Status prüfen“ ruft `RFC_PING` auf.

## Konten

| Aktion | Funktionsbaustein |
|---|---|
| Anlegen | `BAPI_USER_CREATE1` |
| Adressdaten ändern | `BAPI_USER_CHANGE` |
| Sperren, Entsperren | `BAPI_USER_LOCK`, `BAPI_USER_UNLOCK` |
| Löschen | `BAPI_USER_DELETE` |

Jede Änderung schreibt Nova mit `BAPI_TRANSACTION_COMMIT` fest. Vor- und Nachname müssen für SAP getrennt vorliegen; einen Gesamtnamen teilt Nova nicht selbst auf. Nach dem Anlegen und nach Namensänderungen liest Nova die Namensfelder zurück und meldet eine Abweichung.

**Passwörter** übergibt Nova als Initialpasswort, nicht als produktives Passwort. SAP verlangt deshalb bei der ersten Anmeldung eines Dialogbenutzers ein neues Passwort. Legt Nova ein Konto ohne Passwort an, ist die Anmeldung per Passwort deaktiviert. Passwörter, die Nova für SAP erzeugt, haben höchstens 40 Zeichen, beginnen nicht mit „!“ oder „?“ und nicht mit drei gleichen Zeichen.

Den **letzten Login** liest Nova aus der Tabelle `USR02`.

## Rollen

Nova kennt Einzel- und Sammelrollen. Ein Job vom Typ „SAP-Roles importieren“ liest den Rollenkatalog, auf Wunsch gefiltert (etwa `Z*`). Sammelrollen erkennt Nova am Kennzeichen in `AGR_FLAGS`, ihre Einzelrollen liest Nova aus `AGR_AGRS`, Kurztexte auf Deutsch und Englisch aus `AGR_TEXTS`. Liefert SAP

die Rollenstruktur unvollständig, bricht der Import ab und lässt die bisher importierten Definitionen unverändert. Rollen gelten je Zielsystem: Gleichnamige Rollen zweier SAP-Systeme bleiben getrennte Berechtigungen.

### Gültigkeit

SAP verwaltet Gültigkeitszeiträume von Rollenzuweisungen selbst (`FROM_DAT`, `TO_DAT`). Nova überträgt Beginn und Ende jeder Zuweisung mit, auch wenn sie erst in der Zukunft beginnt. Ohne Beginn setzt Nova das aktuelle Datum, ohne Ende den 31.12.9999. Hat dieselbe Rolle für ein Konto mehrere Zeiträume mit einer Lücke dazwischen, schreibt Nova nichts und meldet einen Fehler, statt die Lücke zu überbrücken.

### Schreiben und Rücklesen

SAP nimmt Rollenzuweisungen nur als vollständige Liste an (`BAPI_USER_ACTGROUPS_ASSIGN`). Nova sendet deshalb bei jeder Änderung den vollständigen Soll-Rollenbestand des Kontos mit seinen Zeiträumen.

> ⚠ **BESTEHENDE KONTEN ÜBERNEHMEN**
>
> Weil SAP die gesendete Liste als vollständigen Bestand übernimmt, sollten die vorhandenen Rollen eines bestehenden Kontos in Nova bekannt sein, bevor Nova ihm zum ersten Mal Rollen zuweist: Rollenkatalog importieren, dann einen Abgleich mit dem Zielsystem als führender Seite durchführen. Künftig bleiben Rollen, die Nova nicht verwaltet, bei Zuweisungen durch Nova unberührt. geplant

Nach dem Festschreiben liest Nova die Rollen des Kontos zurück und vergleicht Namen und Zeiträume mit dem Soll; die Einzelrollen einer Sammelrolle berücksichtigt Nova dabei. Weicht etwas ab, gilt die Änderung als fehlgeschlagen, und Nova nennt die betroffenen Rollen. Die festgestellten Änderungen je Rolle hält Nova im Änderungsjournal fest.

### Eine Rolle für viele Konten

Ein Hintergrund-Job vom Typ „SAP-Rolle massenhaft zuweisen“ gibt eine SAP-Rolle vielen Konten oder entzieht sie ihnen, mit optionalem Gültigkeitszeitraum. Die Auswahl erfolgt über Filter wie Identitätstyp oder Abteilung; ohne Statusfilter wählt Nova nur aktive Identitäten aus, KI-Agenten nie. Ein Lauf umfasst höchstens 500 Konten.

Nova bearbeitet die Konten nacheinander und schreibt und prüft jedes wie oben beschrieben. Rollen, die eine gültige Business-Rolle der Identität verlangt, entzieht der Job nicht. Fehler einzelner Konten sammelt Nova im Ergebnis, ohne den Lauf abzubrechen. Ein Abbruch durch Administratoren greift zwischen zwei Konten.

## Welche Rechte Nova im SAP-System braucht

Der SAP-Connector ruft die folgenden Funktionsbausteine auf. Das SAP-Basis-Team kann daraus eine Rolle für den RFC-Benutzer ableiten.

| Funktionsbaustein | Zweck |
|---|---|
| `RFC_PING` | Verbindungstest |

| | |
|---|---|
| `BAPI_USER_GETLIST` | Konten auflisten (Import) |
| `BAPI_USER_GET_DETAIL` | Adresse, Sperrstatus und Rollen lesen |
| `BAPI_USER_CREATE1` | Konten anlegen |
| `BAPI_USER_CHANGE` | Adressdaten ändern, Passwort setzen |
| `BAPI_USER_LOCK`, `BAPI_USER_UNLOCK` | Sperren, Entsperren |
| `BAPI_USER_DELETE` | Konten löschen |
| `BAPI_USER_ACTGROUPS_ASSIGN` | Rollen zuweisen |
| `BAPI_TRANSACTION_COMMIT` | Änderungen festschreiben |
| `RFC_READ_TABLE` | Tabellen lesen, siehe unten |

| Tabelle | Gelesene Felder | Zweck |
|---|---|---|
| `AGR_DEFINE` | `AGR_NAME`, `PARENT_AGR` | Rollenkatalog |
| `AGR_FLAGS` | `AGR_NAME`, `FLAG_TYPE`, `FLAG_VALUE` | Sammelrollen erkennen |
| `AGR_AGRS` | `AGR_NAME`, `CHILD_AGR` | Einzelrollen einer Sammelrolle |
| `AGR_TEXTS` | `AGR_NAME`, `SPRAS`, `TEXT` | Rollentexte |
| `USR02` | `BNAME`, `TRDAT`, `LTIME` | letzter Login |

Zur Orientierung: SAP prüft solche Aufrufe üblicherweise über die Berechtigungsobjekte `S_RFC` (Funktionsbausteine), `S_USER_GRP` (Benutzerpflege), `S_USER_AGR` (Rollenzuweisung) sowie `S_TABU_NAM` oder `S_TABU_DIS` (Tabellen lesen). Welche Objekte und Werte ein System tatsächlich prüft, legt das SAP-Basis-Team fest.

Das Zusatzmodul „SoD-Analyse (SAP ABAP)“ muss eigens eingeschaltet werden. Es liest zusätzlich die Tabelle `AGR_1251` mit den Berechtigungswerten der Rollen; siehe Funktionstrennung (SoD).

# 4.3 Active Directory und LDAP

Ein Connector bindet LDAP-Verzeichnisse an. Unter „Variante“ legen Administratoren fest, wie das Verzeichnis aufgebaut ist:

| Merkmal | Generic LDAP (ApacheDS) | OpenLDAP | Active Directory |
|---|---|---|---|
| Gruppen | `groupOfNames`, `member` | `posixGroup`, `memberUid` | `group`, `member` |
| Kontokennung | `uid` | `uid` | `sAMAccountName` |
| Eindeutige ID | `entryUUID` | `entryUUID` | `objectGUID` |
| Sperre | `pwdAccountLockedTime` | `pwdAccountLockedTime` | `userAccountControl` |
| Letzter Login | nicht voreingestellt | `authTimestamp` | `lastLogonTimestamp`, `lastLogon` |

## Verbindung

Die Felder: „Host“, „Port“, „Base DN“ sowie „Bind DN“ und „Bind-Passwort“ des Dienstkontos. Unter „Erweitert“ stehen „User Search Base“ und „Group Search Base“ – ohne Angabe gilt der Base DN – und „SSL (LDAPS) verwenden“. Für Active Directory kommen weitere Felder hinzu, darunter „AD-Domain“ und „Initialer Kontostatus“. „Status prüfen“ meldet sich mit dem Dienstkonto am Verzeichnis an.

## Konten

Nova legt neue Konten direkt unterhalb der „User Search Base“ an: bei Generic LDAP und OpenLDAP als `uid=<Kennung>`, bei Active Directory als `cn=<Name>`. In Active Directory setzt Nova `sAMAccountName` auf die Kennung und `userPrincipalName` nach der „UPN-Regel“, ohne Regel auf Kennung@AD-Domain. Die „Mail-Regel“ belegt bei allen Varianten das Attribut `mail`. Steht „Initialer Kontostatus“ auf „Deaktiviert“, entsteht ein AD-Konto gesperrt und bleibt es, bis es ausdrücklich aktiviert wird. Weitere Attribute schreibt Nova nach dem „Mapping“.

Nova findet Konten über `uid` oder `mail`, in Active Directory über `sAMAccountName`, `userPrincipalName` oder `mail`.

## Gruppen

Gruppen übernimmt Nova mit einem Job vom Typ „LDAP-Gruppen importieren“ als Berechtigungen. Nova erkennt eine Gruppe an ihrer eindeutigen ID, sofern das Verzeichnis sie liefert. Wird sie innerhalb der „Group Search Base“ umbenannt oder verschoben, findet Nova sie darüber wieder und aktualisiert den gespeicherten DN. Ist die ID bekannt, akzeptiert Nova nur genau dieses Objekt: Eine neu angelegte Gruppe mit altem Namen oder DN gilt nicht als dieselbe Gruppe.

Mitgliedschaften ändert Nova einzeln; die übrigen Mitglieder einer Gruppe bleiben unberührt. Generic LDAP pflegt `memberOf` nicht selbst. Nova schreibt es dort zusätzlich, sofern das Verzeichnisschema das Attribut kennt.

### Verschachtelte Gruppen

Nova liest die Gruppenstruktur. Der Dialog „Gruppe hinzufügen“ am Konto zeigt zu jeder Gruppe ihre Unter- und übergeordneten Gruppen. Aus einer Verschachtelung leitet Nova keine Zuweisungen ab. Bei Generic LDAP und Active Directory können Administratoren in diesem Dialog Gruppen verschachteln („Untergruppe hinzufügen“) und Verschachtelungen wieder lösen. OpenLDAP-Gruppen ( `posixGroup` ) lassen keine Verschachtelung zu.

**Zyklusschutz:** Bevor Nova eine Gruppe als Untergruppe einträgt, prüft Nova, ob sie die übergeordnete Gruppe direkt oder über weitere Ebenen bereits enthält. Ist das so, nimmt Nova die Änderung nicht vor. Dasselbe gilt, wenn sich die Prüfung nicht vollständig durchführen lässt – etwa weil ein Objekt nicht lesbar ist oder die Grenze von 64 Ebenen, 512 Lesezugriffen oder 5 Sekunden erreicht ist. Enthält das Verzeichnis bereits einen Zyklus, zeigt Nova einen Hinweis und durchläuft den Zyklus nicht wiederholt. Die Anzeige liest höchstens 5.000 Gruppen und 64 Ebenen; ist sie unvollständig, weist Nova darauf hin.

## Passwörter

- **Active Directory:** Nova schreibt `unicodePwd` . Das Verzeichnis nimmt Passwörter nur über eine verschlüsselte Verbindung an; ohne „SSL (LDAPS) verwenden“ lehnt Nova das Setzen ab.
- **Generic LDAP und OpenLDAP:** Nova nutzt die Password-Modify-Operation nach RFC 3062 und, falls der Server sie nicht unterstützt, das Attribut `userPassword` .

## Sperren

- **Active Directory:** Nova setzt bzw. löscht das Bit `ACCOUNTDISABLE` in `userAccountControl` ; die übrigen Bits bleiben unverändert.
- **Generic LDAP und OpenLDAP:** Nova sperrt dauerhaft über das Password-Policy-Attribut `pwdAccountLockedTime` und entfernt es zum Entsperren. Das Passwort bleibt erhalten; das Ergebnis liest Nova zurück. Voraussetzung ist eine aktive Password Policy – bei OpenLDAP das Overlay ppolicy – und das Recht, dieses Attribut zu schreiben.

## Letzter Login

In Active Directory liest Nova `lastLogonTimestamp` , ersatzweise `lastLogon` ; bei OpenLDAP `authTimestamp` , sofern das Verzeichnis es pflegt. Für Generic LDAP ist kein Attribut voreingestellt; im Konfigurationsschlüssel `last_logon_attrs` lässt sich eines angeben.

## Nötige Verzeichnisrechte

Das Dienstkonto („Bind DN“) braucht:

- **Lesen:** Konten unterhalb der „User Search Base“; Gruppen mit Mitgliederattribut und eindeutiger ID unterhalb der „Group Search Base“; bei Generic LDAP außerdem das Schema, um `memberOf` zu prüfen; für den letzten Login die genannten Attribute.
- **Gruppen:** Schreiben des Mitgliederattributs (`member` bzw. `memberUid`) an den Gruppen, die Nova verwaltet; bei Generic LDAP zusätzlich `memberOf` an den Konten.
- **Konten:** Anlegen, Ändern und Löschen unterhalb der „User Search Base“.
- **Passwörter:** Zurücksetzen – in Active Directory über `unicodePwd`.
- **Sperren:** Schreiben von `userAccountControl` bzw. `pwdAccountLockedTime`.
- **Verschachtelung:** Schreiben von `member` an übergeordneten Gruppen und Lesen der beteiligten Untergruppen.

Nova sollte sich per LDAPS verbinden („SSL (LDAPS) verwenden“); Active Directory verlangt das für Passwortoperationen.

# 4.4 Microsoft Entra ID

Nova verwaltet in Microsoft Entra ID Konten und ihre Gruppenmitgliedschaften. Nova spricht Entra ID über Microsoft Graph (Version 1.0) an.

## Verbindung

Für Nova legen Administratoren in Entra ID eine App-Registrierung mit Client-Secret an. Nova meldet sich damit ohne Benutzerkontext an (OAuth 2.0 Client Credentials) und handelt mit den Anwendungsberechtigungen der App.

Die Felder: „Tenant ID“, „Client (App) ID“, „Client Secret“ und „UPN-Domain“. Unter „Erweitert“ stehen „Authority (optional)“, „Graph-Endpoint“ und „Scopes“ (Standard: `https://graph.microsoft.com/.default`). „Status prüfen“ fordert ein Zugriffstoken an. Das bestätigt die Anmeldedaten der App, nicht ihre Graph-Berechtigungen.

## Konten

- **Anlegen:** Nova legt das Konto aktiviert an, mit der Kennung als `userPrincipalName` und dem Teil vor dem „@“ als `mailNickname`; weitere Attribute folgen dem „Mapping“. Wird beim manuellen Anlegen nur der Namensteil angegeben, hängt Nova die „UPN-Domain“ an.
- **Ändern** und **Löschen** über den Graph-Endpunkt `/users`.
- **Sperren und Entsperren** über `accountEnabled`. Danach liest Nova den Status zurück und meldet einen Fehler, wenn er sich nicht bestätigen lässt.

## Gruppen

Gruppen übernimmt Nova mit einem Job vom Typ „Entra-Gruppen importieren“ als Berechtigungen. Nova schreibt direkte Gruppenmitgliedschaften; die übrigen Mitglieder einer Gruppe bleiben unberührt. Entra-Verzeichnisrollen verwaltet Nova nicht.

Verschachtelte Gruppen liest Nova bis zu einer Grenze von 500 Gruppen und 32 Ebenen. Daraus zeigt Nova die Gruppenstruktur und für ein Konto den Abschnitt „Wirksame geerbte Mitgliedschaften“. Zyklen und unvollständiges Lesen meldet Nova als Hinweis. Geerbte Mitgliedschaften schreibt Nova nicht; sie sind keine Zuweisungen in Nova.

### Prüfung nach dem Schreiben

Bei Provisionierung und Abgleich liest Nova zuerst alle direkten Gruppenmitgliedschaften des Kontos. Dann entfernt Nova die zu entziehenden Gruppen und fügt die neuen hinzu. Anschließend liest Nova die vollständige Liste erneut – über alle Seiten der Graph-Antwort – und vergleicht sie mit dem erwarteten Stand.

Weil Entra ID Änderungen verzögert sichtbar machen kann, wiederholt Nova das Lesen bis zu 30 Sekunden lang. Stimmt der Stand dann nicht, gilt der Schritt als fehlgeschlagen; Nova nennt fehlende und unerwartete Gruppen.

## Letzter Login

Nova liest `signInActivity` und nimmt den jüngsten Zeitpunkt aus interaktiver, nicht interaktiver und erfolgreicher Anmeldung. Das setzt die Berechtigung `AuditLog.Read.All` voraus.

## Benötigte Graph-Berechtigungen

Die Tabelle nennt je Aufgabe eine Anwendungsberechtigung, die Microsoft für die jeweiligen Aufrufe dokumentiert:

| Aufgabe | Graph-Aufrufe | Berechtigung |
|---|---|---|
| Konten lesen | `GET /users` | `User.Read.All` |
| Konten anlegen, ändern, sperren, löschen | `POST`, `PATCH`, `DELETE /users` | `User.ReadWrite.All` |
| Gruppen und Gruppenstruktur lesen | `GET /groups`, `…/members`, `…/memberOf` | `GroupMember.Read.All` |
| Gruppen eines Kontos lesen | `GET /users/{id}/memberOf` | `Directory.Read.All` |
| Mitgliedschaften schreiben | `POST`, `DELETE /groups/{id}/members` | `GroupMember.ReadWrite.All` |
| Letzter Login | `GET /users` mit `signInActivity` | `AuditLog.Read.All` |

Für das Setzen von Passwörtern ( `passwordProfile` ) verlangt Microsoft Rechte, die über diese Tabelle hinausgehen; sie beschreibt die Microsoft-Graph-Dokumentation zu „Update user“. Microsoft passt Berechtigungen gelegentlich an; maßgeblich ist die jeweils aktuelle Dokumentation.

# 4.5 Keycloak

Nova verwaltet in Keycloak Konten – dort „Benutzer“ genannt – und ihre Gruppenmitgliedschaften. Nova nutzt dafür die Admin-REST-API; ein Zielsystem entspricht einem Realm.

## Verbindung

Nova meldet sich über einen vertraulichen Client mit Service-Account an (OAuth 2.0 Client Credentials). Die Felder: „Base URL“, „Realm“, „Client ID“ und „Client Secret“.

Der Service-Account braucht die Rollen `manage-users`, `view-users`, `query-users` und `query-groups` des Clients `realm-management`. Hinzu kommen je nach Nutzung:

- `view-events` – um den letzten Login aus Login-Ereignissen zu lesen
- `manage-clients` und `view-clients` – um KI-Agenten als Clients anzulegen

„Status prüfen“ fordert ein Token an und zählt die Konten im Realm. Der Test prüft damit auch, ob der Service-Account Konten lesen darf.

## Konten

- **Anlegen:** Benutzername, E-Mail-Adresse, Vor- und Nachname; das Konto ist aktiviert. Weitere Attribute aus dem „Mapping“ legt Nova als Keycloak-Attribute des Kontos ab.
- **Ändern:** Nova liest das Konto, ergänzt die geänderten Werte und schreibt es zurück. So bleiben andere Attribute des Kontos erhalten.
- **Sperren und Entsperren** über das Feld `enabled`.
- **Löschen.**
- **Passwörter** setzt Nova über die Admin-API.

Keycloak speichert Benutzernamen in Kleinbuchstaben; Nova schreibt und vergleicht sie deshalb ebenfalls klein. Konten findet Nova über Benutzername, E-Mail-Adresse oder Keycloak-ID.

## Gruppen

Gruppen und Untergruppen übernimmt Nova mit einem Job vom Typ „Keycloak-Gruppen importieren“ als Berechtigungen. Nova zeigt sie mit ihrem Pfad an, etwa „Engineering/Backend“, und erkennt sie an ihrer Keycloak-ID. Realm- und Client-Rollen verwaltet Nova nicht.

Keycloak führt ein Konto nur in den Gruppen als Mitglied, denen es direkt angehört. Nova liest und schreibt ausschließlich diese direkten Mitgliedschaften, jeweils einzeln. Bei der Provisionierung liest Nova vorher die aktuellen Mitgliedschaften, damit das Änderungsjournal nur wirksame Änderungen enthält.

## Letzter Login

Nova nimmt den jüngsten Zeitpunkt aus den Login-Ereignissen des Realms und aus den aktiven Sitzungen des Kontos. Login-Ereignisse gibt es nur, wenn der Realm sie speichert und der Service-Account `view-events` hat. Ohne sie kennt Nova nur den letzten Zugriff aus gerade aktiven Sitzungen.

## KI-Agenten

Identitäten vom Typ „KI-Agent“ legt Nova in Keycloak nicht als Keycloak-Benutzer an, sondern als vertraulichen Client mit Service-Account. Ihre Gruppenmitgliedschaften liegen beim Service-Account dieses Clients. Das Client-Secret speichert Nova nicht; ein neues erzeugt „Secret rotieren“, und Nova zeigt es einmalig an. Mehr dazu unter KI-Agenten als Identitäten.

# 4.6 SCIM

SCIM 2.0 ist ein offener Standard für die Verwaltung von Konten und Gruppen. Über SCIM verwaltet Nova Konten und Gruppenmitgliedschaften in Anwendungen, die eine SCIM-2.0-Schnittstelle anbieten.

## Verbindung

- **„Base URL“:** Nova hängt die SCIM-Pfade selbst an, etwa `/scim/v2/Users`. Liegen die Endpunkte unter `https://app.example.com/api/scim/v2/`, lautet die Base URL `https://app.example.com/api`.
- **„Auth-Typ“:** „Bearer“ mit Token, „Basic“ mit „Benutzer“ und „Passwort“ oder „Keine“.
- **„Last-Logon-Attribut (SCIM)“** unter „Erweitert“, siehe Letzter Login.

„Status prüfen“ ruft `/scim/v2/ServiceProviderConfig` ab, ersatzweise die Base URL selbst.

## Konten

| Aktion | SCIM-Aufruf |
|---|---|
| Suchen | `GET /Users` mit Filter `userName eq "…"` |
| Anlegen | `POST /Users` |
| Ändern | `PATCH /Users/{id}`, Operation `replace` |
| Passwort setzen | `PATCH` auf das Attribut `password` |
| Sperren, Entsperren | `PATCH` auf das Attribut `active` |
| Löschen | `DELETE /Users/{id}` |

Beim Anlegen sendet Nova `userName` (die Kennung), `displayName`, `name` mit Vor- und Nachnamen aus dem Namen der Identität, `active`, die E-Mail-Adresse als primäre Adresse und, falls vorhanden, das Passwort. Weitere einfache Attribute folgen dem „Mapping“.

## Gruppen

Den Gruppenkatalog übernimmt ein Job vom Typ „SCIM-Gruppen importieren“; er liest die Gruppen seitenweise.

Mitgliedschaften ändert Nova per `PATCH` auf die Gruppe (`/Groups/{id}`, Operation `add` oder `remove` auf `members`); die übrigen Mitglieder bleiben unberührt. Als Mitgliedswert übergibt Nova die Kontokennung, unter der das Konto in Nova verknüpft ist. Bei der Provisionierung sucht Nova die Gruppe über ihren Anzeigenamen (`displayName eq "…"`). Wird eine Gruppe im SCIM-Server umbenannt, muss

ihr Name in Nova nachgezogen werden, etwa durch einen erneuten Import mit „Bestehende Roles überschreiben“. Vor dem Schreiben liest Nova die Mitglieder der Gruppe, damit das Änderungsjournal nur wirksame Änderungen enthält.

## Letzter Login

SCIM kennt kein Standardattribut für den letzten Login. Nova liest das Attribut, das unter „Last-Logon-Attribut (SCIM)“ eingetragen ist – auch als Pfad mit Punkten. Ist keines eingetragen oder liefert es keinen Wert, prüft Nova `lastLogin`, `lastLogon`, `lastLoginTime` und `loginTime`.

## Was sich zwischen SCIM-Servern unterscheidet

SCIM lässt Anbietern Spielraum. Vor dem Einsatz sollte geklärt sein:

- ob die Endpunkte unter einem Pfad liegen, der auf `/scim/v2/` endet
- welche Anmeldung der Server verlangt – Nova unterstützt Bearer-Token und Basic
- ob der Server die Kontokennung als Mitgliedswert einer Gruppe annimmt oder die interne SCIM-ID des Kontos verlangt
- ob der Server die Filter `eq` (für `userName` und `displayName`) und `co` (Gruppensuche) unterstützt
- ob `PATCH` für Konten (`/Users`) und Gruppen unterstützt wird und ob sich `password` und `active` darüber schreiben lassen
- ob und unter welchem Namen der letzte Login geliefert wird

Ein Durchlauf mit einem Testkonto – anlegen, Gruppe zuweisen und entziehen, sperren, löschen – zeigt, ob ein Server zu diesen Annahmen passt.

KAPITEL 5

# Konten und Provisionierung

## 5.1 Konten und Passwörter

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Ein **Konto** ist der Zugang einer Identität zu einem Zielsystem, zum Beispiel ein SAP-Benutzer oder ein Konto im Active Directory. Diese Seite beschreibt, wie Nova Konten bildet und zuordnet, woher der angezeigte Kontostatus stammt und wie Nova mit Passwörtern umgeht. Wie Nova Konten bei der Provisionierung anlegt, beschreibt Provisionierungsläufe.

### Ein Konto, eine Identität

Jedes Konto gehört genau einer Identität. Ist ein Konto bereits mit einer Identität verknüpft, lehnt Nova es ab, dasselbe Konto mit einer weiteren Identität zu verknüpfen.

### Kontokennungen

Die Kennung eines neuen Kontos bildet Nova nach der Namensregel des Zielsystems – siehe Zielsysteme – Überblick.

- **Kennung bereits vorhanden:** Existiert im Zielsystem schon ein Konto mit der berechneten Kennung, übernimmt Nova es nie stillschweigend. Nova hält an und meldet einen Konflikt. Ein Administrator entscheidet: das vorhandene Konto nach Prüfung verknüpfen oder eine andere Kennung vergeben.
- **Anlage ungewiss:** Ist unklar, ob eine Anlage das Zielsystem erreicht hat – etwa nach einer Zeitüberschreitung –, behält Nova die gewählte Kennung. Beim nächsten Versuch sucht Nova genau dieses Konto und verknüpft es, statt ein zweites anzulegen.

### Kontostatus

Den Status eines Kontos, etwa aktiv oder gesperrt, zeigt Nova so, wie Nova ihn zuletzt im Zielsystem gelesen hat – zusammen mit dem Zeitpunkt dieses Lesevorgangs. Ein neu verknüpftes Konto zeigt „Unbekannt“, bis Nova es gelesen hat.

- **Sperren und Entsperren** gelten erst als erledigt, wenn Nova den neuen Zustand aus dem Zielsystem zurückgelesen hat.

- **Fehlende Konten:** Dass ein Konto im Zielsystem nicht existiert, stellt Nova nur fest, wenn die Suche dort fehlerfrei und eindeutig war. Eine gescheiterte oder mehrdeutige Suche gilt nicht als „nicht gefunden“.

## Passwörter

- **Erzeugte Passwörter** sind zufällig und folgen den Passwortregeln des Zielsystems.
- **Von Administratoren gesetzte Passwörter** muss die Identität bei der nächsten Anmeldung ändern – in jedem Zielsystem, das das unterstützt: SAP, Active Directory, Microsoft Entra ID und Keycloak.
- **Nur verschlüsselt:** Zu Verzeichnisdiensten wie Active Directory überträgt Nova Passwörter nur über LDAPS oder StartTLS.
- **Nicht gespeichert:** Passwörter von Konten in Zielsystemen speichert Nova nicht. In den Protokollen und im Änderungsjournal erscheinen sie nie.

## Austritt

Beim Austritt sperrt Nova alle Konten der Identität. Schlägt eine Sperre fehl, wiederholt Nova sie, bis sie bestätigt ist.

Endgültig löscht Nova eine Identität erst, wenn für alle ihre Konten bestätigt ist, dass sie gesperrt oder gelöscht sind – siehe Identitäten und ihr Status.

## Verwaiste Konten

Für jedes Zielsystem zeigt Nova die Konten, die dort existieren, aber keiner Identität gehören.

# 5.2 Provisionierungsläufe

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Ein **Provisionierungslauf** bringt den Soll-Zustand einer Identität aus Nova in die Zielsysteme. Ein Lauf gilt genau einer Identität. Er besteht aus Schritten je Zielsystem, etwa Konto prüfen, Konto anlegen und Berechtigungen übertragen.

## Wann ein Lauf entsteht

Ist die automatische Provisionierung eingeschaltet – siehe Wie Zugriff entsteht und verschwindet –, erzeugt jede Änderung am Soll-Zustand für jede betroffene Identität einen Lauf, unter anderem:

- ein genehmigter Antrag,
- das Zuweisen und Entziehen einer Business-Rolle,
- das Anhängen und Lösen von Business-Rollen an Organisationseinheiten und – mit dem Zusatzmodul „Planstellen (OSP)“ – an Planstellen, siehe Organisation und Planstellen,
- eine Änderung an der Definition einer Berechtigung oder Business-Rolle,
- das Löschen einer Berechtigung oder Business-Rolle,
- Beginn und Ende eines Gültigkeitszeitraums.

Nova speichert jeden Lauf, bevor er ausgeführt wird. Unterbricht ein Neustart einen Lauf, setzt Nova ihn danach fort.

Für eine Identität schreibt immer nur ein Vorgang zur selben Zeit in die Zielsysteme. Das gilt für Läufe ebenso wie für jeden anderen Weg, auf dem Nova in Zielsysteme schreibt.

## Übertragen und bestätigt

Nova unterscheidet zwei Zustände:

| Zustand | Bedeutung |
|---|---|
| **übertragen** | Das Zielsystem hat den Schreibvorgang angenommen. |
| **bestätigt** | Nova hat den Zustand aus dem Zielsystem zurückgelesen; er entspricht dem Soll. |

An jeder Zuweisung zeigt Nova, ob sie übertragen oder bestätigt ist und wann Nova sie zuletzt bestätigt hat.

**Entfernen:** Eine Berechtigung gilt erst als entfernt, wenn die Entfernung bestätigt ist. Kann Nova eine Gruppe oder Rolle im Zielsystem nicht nachschlagen, schlägt der Schritt fehl und wird wiederholt. Als erledigt meldet Nova ihn dann nie.

## Bestehende Rollen in SAP

Rollen an einem SAP-Konto, die Nova nicht verwaltet, bleiben erhalten. Vor dem ersten Schreiben in ein Konto liest Nova dessen vorhandene Rollen. Im Abgleich erscheinen sie als nur im Zielsystem vorhanden, bis ein Administrator ausdrücklich über sie entscheidet.

## Wiederholungen

- Fehlgeschlagene Läufe wiederholt Nova automatisch, in wachsenden Abständen.
- Jede Wiederholung bewertet Nova neu gegen den aktuellen Stand. Ob Nova ein Konto sperrt oder entsperrt, richtet sich zum Beispiel nach dem Status, den die Identität zum Zeitpunkt der Wiederholung hat.
- Hat ein neuerer Lauf einen älteren überholt, spielt Nova den älteren nicht erneut ab.

## Gültigkeit

Beginn und Ende von Gültigkeitszeiträumen wertet Nova in der eingestellten Geschäftszeitzone aus.

## Massenänderungen und Pause

- **Vorschau:** Betrifft eine Änderung viele Identitäten – etwa wenn eine geänderte Business-Rolle auf alle Inhaber angewendet wird –, zeigt Nova eine Vorschau mit der Zahl der betroffenen Identitäten und Berechtigungen, bevor Nova etwas schreibt.
- **Pause:** Jedes Zielsystem hat einen Pausenschalter, zusätzlich gibt es einen globalen. Während einer Pause hält Nova alle Schreibvorgänge in die betroffenen Zielsysteme zurück; sie bleiben in der Warteschlange.

## Was ein Lauf zeigt

Jeder Lauf zeigt

- wer oder was ihn ausgelöst hat: eine Person, ein Antrag, eine Änderung an einer Business-Rolle, eine Änderung der Organisation oder ein Job – bei einem Antrag mit Link zum Antrag,
- wann er ausgelöst wurde,
- seine Schritte und deren Ergebnisse.

Die Läufe stehen unter „Monitoring“ → „Provisioning-Log“. Wie Läufe mit Anträgen und Änderungen in den Zielsystemen zusammenhängen, beschreibt Protokolle.

# 5.3 Abgleich

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Beim **Abgleich** vergleicht Nova, was für eine Identität vorgesehen ist, mit dem, was im Zielsystem tatsächlich vorhanden ist. Nova zeigt die Abweichungen an; aufgelöst werden sie bewusst, in die eine oder die andere Richtung. Für eine einzelne Identität zeigt der Reiter „Abgleich & Provisionierung“ die Abweichungen je Zielsystem.

## Führende Seite

Für jedes Zielsystem ist festgelegt und sichtbar, welche Seite führt: Nova oder das Zielsystem.

## Nur vollständig Gelesenes zählt

Abgleich und Importe handeln nur auf Grundlage vollständig gelesener Daten:

- Liefert ein Zielsystem seine Ergebnisse seitenweise, liest Nova bis zur letzten Seite.
- Bleibt ein Lesevorgang unvollständig – wegen eines Fehlers, einer Zeitüberschreitung oder fehlender Leserechte –, ändert Nova nichts und kennzeichnet das Ergebnis als unvollständig.

## Was ein Import nie entfernt

Ein Import entfernt nie Zuweisungen, die noch ausstehen, erst in der Zukunft beginnen oder aus einem genehmigten Antrag stammen.

## Gültigkeit zählt

Eine abgelaufene oder noch nicht gültige Zuweisung zeigt Nova nie als „Synchron“ an.

## Änderungen außerhalb von Nova

Ändert jemand ein Zielsystem direkt, erkennt Nova die Abweichung beim nächsten Lesen und zeigt sie mit dem Zeitpunkt des letzten Lesevorgangs an. Administratoren lösen sie bewusst auf, in eine von zwei Richtungen:

- den Stand des Zielsystems in Nova übernehmen oder
- den Soll-Zustand aus Nova im Zielsystem wiederherstellen.

Massenaktionen zeigen vorab eine Vorschau, was sich genau ändert.

Das Änderungsjournal hält nur fest, was Nova selbst geschrieben hat. Änderungen von außen macht der Abgleich sichtbar.

KAPITEL 6

# Anträge

## 6.1 Zugriff beantragen

Berechtigungen und Business-Rollen lassen sich in Nova über einen **Antrag** anfordern. Über jede beantragte Rolle entscheidet der Genehmigungsablauf, der ihr zugeordnet ist. Erst nach dieser Entscheidung weist Nova den Zugriff zu.

### Wer was für wen beantragen kann

- **Antragsteller:** Jede angemeldete Identität kann einen Antrag stellen – für sich selbst, für eine andere Identität oder für eine Abteilung. Ob der Zugriff erteilt wird, entscheiden die Genehmiger.
- **Anfragbar** sind Berechtigungen und Business-Rollen, denen ein „Genehmigungs-Workflow" zugeordnet ist. Rollen ohne Workflow nimmt Nova in keinen Antrag auf.
- **Mehrere Rollen:** Ein Antrag kann mehrere Rollen enthalten. Jede durchläuft ihren eigenen Genehmigungsablauf.
- **KI-Agenten:** Zugriff für einen KI-Agenten beantragen nur seine verantwortliche Person, deren eingetragene Vertretung oder Administratoren. Ein KI-Agent erhält auf diesem Weg ausschließlich KI-Fähigkeiten (Rollen `nova-ai:*`); für alle anderen Identitäten sind diese nicht anfragbar.

### Einen Antrag stellen

Unter „Zugriffsanfragen" → „Meine Anfragen" öffnet „Neue Anfrage" das Formular:

1. **„Gestellt für"** – eine Person oder eine Abteilung. Voreingestellt ist die eigene Identität.
2. **„Rollen"** – die anfragbaren Berechtigungen und Business-Rollen, durchsuchbar und nach „Kategorie" filterbar. Rollen, die alle Ziel-Identitäten bereits besitzen, blendet Nova aus.
3. **Vorabprüfung** – Nova prüft die Auswahl gegen die Regeln zur Funktionstrennung und zeigt Konflikte als „Risiko-Befunde". Je nach Risiko-Policy warnt Nova nur, ergänzt einen Prüfschritt oder blockiert den Antrag.
4. **„Anfrage senden"**.

Für eine **Abteilung** entsteht ein gemeinsamer Antrag: Die Genehmiger entscheiden einmal für die ganze Abteilung, nicht je Person. Welche Personen den Zugriff erhalten, ermittelt Nova erst bei der abschließenden Genehmigung aus den dann aktuellen Mitgliedern.

Ein Antrag enthält keine Gültigkeitsdaten. Eine daraus entstehende Zuweisung gilt ab der Genehmigung und ohne Enddatum.

## Status eines Antrags

| Status | Bedeutung |
|---|---|
| „Ausstehend“ | Über mindestens eine beantragte Rolle ist noch nicht entschieden. |
| „Genehmigt“ | Alle beantragten Rollen sind genehmigt. |
| „Teilweise genehmigt“ | Alle Rollen sind entschieden – ein Teil genehmigt, ein Teil abgelehnt. |
| „Abgelehnt“ | Alle beantragten Rollen sind abgelehnt. |
| „Storniert“ | Der Antrag wurde zurückgezogen oder von Administratoren storniert. |

Die Seite „Zugriffsanfragen“ hat drei Reiter: „Zu genehmigen“ zeigt, was die angemeldete Identität entscheiden darf – auch in Vertretung –, „Meine Anfragen“ die eigenen offenen Anträge und „Abgeschlossen“ die erledigten. Administratoren sehen unter „Zu genehmigen“ und „Abgeschlossen“ alle Anträge. Zu jeder Anfrage gibt es einen Chat zwischen Antragsteller und Genehmigern; Entscheidungen hält Nova dort als Systemnachricht fest.

## Nach der Entscheidung

Sobald über alle Rollen eines Antrags entschieden ist, weist Nova die genehmigten Rollen den Ziel-Identitäten zu. Bestehende Zuweisungen bleiben unverändert. Abgelehnte und stornierte Anträge führen zu keiner Zuweisung.

Ist unter „Administration“ → „Provisionierung“ → „Mapping“ die Option „Zielsysteme automatisch provisionieren“ eingeschaltet, legt Nova für jede Identität, deren neue Rollen ein Zielsystem betreffen, einen **Provisionierungslauf** an:

- Zuweisung und Lauf speichert Nova in derselben Transaktion. Scheitert das Speichern, entsteht keins von beiden.
- Den Lauf startet Nova erst danach. Lässt er sich nicht starten, bleibt er gespeichert, und Nova nimmt ihn beim nächsten Start wieder auf.

Ist die Option ausgeschaltet, weist Nova die Rollen nur in Nova zu. In der Anfrage zeigt der Abschnitt „Provisionierung“ den Stand der Läufe. „Genehmigt“ bedeutet dabei: in Nova zugewiesen. Die Ausführung in den Zielsystemen verfolgt Nova separat.

## Zurückziehen und stornieren

Solange ein Antrag „Ausstehend“ ist, kann der Antragsteller ihn mit „Anfrage stornieren“ zurückziehen. Administratoren können jeden offenen Antrag stornieren. Ein stornierter Antrag lässt sich nicht wieder öffnen. Nova benachrichtigt die Genehmiger offener Schritte und protokolliert die Stornierung.

# 6.2 Genehmigungsabläufe

Ein **Genehmigungsablauf** – in der Oberfläche „Workflow“ – legt fest, wer über einen Antrag auf eine Rolle entscheidet. Jede Berechtigung und jede Business-Rolle verweist über das Feld „Genehmigungs-Workflow“ auf höchstens einen Ablauf. Ohne Ablauf ist sie nicht anfragbar.

## Abläufe pflegen

Administratoren pflegen Abläufe unter „Administration“ → „Workflows“. Ein Ablauf besteht aus den Feldern „ID (Slug)“, „Name“ und „Beschreibung“ sowie einer geordneten Liste von Schritten („Approval-Schritte“); jeder Schritt hat einen Genehmiger-Typ.

- Nur Administratoren legen Abläufe an, ändern oder löschen sie.
- Ein Ablauf braucht mindestens einen Schritt; ohne Schritte nimmt Nova keinen Antrag an.
- Einen Ablauf, auf den noch Rollen verweisen, löscht Nova nicht.
- Beim Einreichen übernimmt Nova die Schritte in den Antrag. Spätere Änderungen am Ablauf gelten für neue Anträge.

## Wer einen Schritt entscheidet

| Genehmiger-Typ | Wer entscheidet |
|---|---|
| „Manager“ | die Führungskraft der Ziel-Identität, eingetragen oder aus der Organisation abgeleitet; bei einer Abteilung deren Leitung |
| „Rollen-Eigentümer“ | der „Owner“ der beantragten Rolle |
| „Agent-Owner“ | die verantwortliche Person des KI-Agenten |
| „Risiko-Eigentümer“ | die im Schritt hinterlegte Identität |
| „Bestimmte Identität“ | die im Schritt hinterlegte Identität |
| „Security“ | jede Identität mit der Berechtigung „Security“ |
| „SoD-Prüfung“ | jede Identität mit der Berechtigung „SoD Reviewer“ oder „Security“ |

- Für offene Schritte ermittelt Nova die zuständige Person laufend neu. Wechselt etwa die Führungskraft, darf die neue entscheiden; die beim Einreichen ermittelte Person bleibt ebenfalls berechtigt.
- Lässt sich niemand ermitteln – etwa weil eine Rolle keinen Owner hat –, können nur Administratoren den Schritt entscheiden.

- Ein Schritt „SoD-Prüfung“ wird nur aktiv, wenn offene Risiko-Befunde vorliegen; sonst überspringt Nova ihn. Wer ihn trotz offener Befunde genehmigt, muss einen Kommentar angeben. Mehr dazu unter Funktionstrennung.
- Administratoren können jeden offenen Schritt entscheiden und einen Antrag als Ganzes mit „Genehmigen (Admin)“ oder „Ablehnen (Admin)“ abschließen. Nova protokolliert diesen Eingriff als eigenes Ereignis und benachrichtigt Antragsteller und offene Genehmiger.

## Reihenfolge und Ergebnis

- Alle Schritte eines Ablaufs sind ab dem Einreichen offen und lassen sich in beliebiger Reihenfolge entscheiden. Die Nummer eines Schritts bestimmt die Reihenfolge der Benachrichtigungen.
- Eine beantragte Rolle ist genehmigt, wenn alle ihre Schritte genehmigt oder übersprungen sind. Eine einzige Ablehnung lehnt sie ab.
- „Genehmigen“ und „Ablehnen“ in der Anfrage entscheiden alle offenen Schritte, für die die angemeldete Identität als Genehmiger ermittelt ist, auf einmal. Ein Kommentar ist optional.
- Besteht ein Ablauf nur aus Schritten „SoD-Prüfung“ und liegen keine Befunde vor, gilt die Rolle beim Einreichen als genehmigt.

## Vertretung bei Abwesenheit

An einer Identität lassen sich ein „Vertreter“ sowie unter „Abwesenheit“ die Daten „Abwesend von“ und „Abwesend bis“ pflegen. Sind beide Daten gesetzt und liegt der heutige Tag in diesem Zeitraum, darf die Vertretung die offenen Schritte der abwesenden Person zusätzlich entscheiden.

- Die abwesende Person bleibt selbst berechtigt.
- Ketten löst Nova nicht auf: Ist die Vertretung ebenfalls abwesend, geht die Befugnis nicht an deren Vertretung weiter.
- Im Reiter „Zu genehmigen“ tragen solche Anfragen den Hinweis „In Vertretung für …“. Nova protokolliert die Entscheidung zusammen mit der vertretenen Person.
- Benachrichtigungen an Genehmiger erhält während der Abwesenheit zusätzlich die Vertretung.

## Erinnerung und Eskalation

Der Hintergrundjob „Genehmigungs-Eskalation“ macht überfällige Schritte sichtbar. Nova legt ihn nicht selbst an; Administratoren richten ihn unter „Monitoring“ → „Hintergrund-Jobs“ mit „Neuer Job“ ein.

- Ab „Erinnerung nach (Tagen)“ – Voreinstellung 3 – erinnert Nova die zuständigen Genehmiger, höchstens einmal täglich.
- Ab „Eskalation nach (Tagen)“ – Voreinstellung 7 – alarmiert Nova einmalig die Administratoren. Die Erinnerungen laufen weiter.
- Das Alter eines Schritts zählt ab der letzten Entscheidung eines früheren Schritts derselben Rolle, sonst ab dem Einreichen.
- Der Job genehmigt nichts und überspringt keinen Schritt.

## Benachrichtigungen

| Ereignis | Empfänger |
|---|---|
| „Zugriffsanfrage eingereicht“ | ermittelte Genehmiger des ersten aktiven Schritts |
| „Genehmigungsschritt abgeschlossen“ | ermittelte Genehmiger des nächsten Schritts |
| „Zugriffsanfrage genehmigt“ | Antragsteller, Ziel-Identität |
| „Zugriffsanfrage abgelehnt“ | Antragsteller |
| „Zugriffsanfrage storniert“ | Genehmiger offener Schritte |
| „Admin-Eingriff bei Anfrage“ | Antragsteller, Genehmiger offener Schritte |
| „Erinnerung an offene Genehmigung“ | zuständige Genehmiger |
| „Überfällige Genehmigung eskaliert“ | Administratoren |

Unter „Administration“ → „Benachrichtigungen“ legen Administratoren je Ereignis fest, ob Nova benachrichtigt und über welche Kanäle; die Texte lassen sich anpassen. Der Kanal „E-Mail“ versendet nur mit eingerichtetem Mailserver. Der „Versandmodus“ („Aktiv“, „Pausiert“, „Aus“) gilt für alle Kanäle.

**Microsoft Teams** ist ein Zusatzmodul: Nach dem Einschalten von „Microsoft Teams Notifications“ unter „Administration“ → „Plugins“ kann Nova Nachrichten über einen Webhook in einen Teams-Kanal senden. Ist zusätzlich „Interaktive Genehmigungen (in Teams genehmigen)“ eingerichtet, erhalten die benachrichtigten Genehmiger über einen Power-Automate-Flow eine Karte mit „Approve“ und „Reject“. Ein Klick entscheidet einen offenen Schritt dieser Person; Nova prüft die Berechtigung dabei wie bei einer Entscheidung in Nova.

KAPITEL 7

# Governance

## 7.1 Rezertifizierung

Bei einer **Rezertifizierung** prüfen Verantwortliche, ob bestehende Zugriffe noch benötigt werden, und bestätigen oder entziehen sie. Nova bündelt diese Prüfung in **Kampagnen**. Administratoren verwalten Kampagnen unter „Compliance“ → „Rezertifizierung“.

### Kampagne anlegen

„Neue Kampagne“ legt eine Kampagne an:

- **„Scope“** – wessen Zugriffe geprüft werden: „Alle Benutzer“, eine „Abteilung“, eine „Organisationseinheit“ (ohne Untereinheiten), alle Identitäten mit Konto in einem „System“ oder „KI-Agenten“. Deaktivierte und gelöschte Identitäten schließt Nova aus.
- **„Reviewer“** – wer prüft: der „Manager“ der Identität, der „Rollen-Owner“ der Rolle, ein „Bestimmter Benutzer“ oder bei KI-Agenten deren „Agent-Owner (KI-Identität)“.
- **„Frist“** – optional.
- **„Kampagnentyp“** und **„Standard“** (z. B. ISO 27001) dienen der Einordnung.

Nova erzeugt sofort je Identität und Zuweisung einen Eintrag. Geprüft werden die am Tag der Anlage gültigen Zuweisungen von Business-Rollen und direkten Berechtigungen; Berechtigungen, die eine Identität über eine Business-Rolle erhält, deckt die Prüfung der Business-Rolle ab. Jeder Eintrag hält Identität, Rolle, System und Risikobewertung zum Zeitpunkt der Anlage fest. Einen Scope ohne Einträge lehnt Nova ab. Beim Scope „KI-Agenten“ kommen die Fähigkeiten verknüpfter Routinen-Agenten als eigene Einträge hinzu.

Lässt sich für einen Eintrag kein Reviewer ermitteln, prüft ihn die Person, die die Kampagne angelegt hat.

### Hinweise an den Einträgen

Nova markiert Einträge, die besondere Aufmerksamkeit verdienen; der Filter „Markiert“ zeigt sie gesammelt:

- **„SoD-Konflikt“** – die Zuweisung ist Teil eines Konflikts nach einer aktiven SoD-Regel.
- **„Externer mit hohem Recht“** – eine externe Identität hält eine als „Kritisch“ bewertete Rolle.
- **„Kein Peer hält diese Rolle“** – im Scope hält nur diese eine Identität die Rolle.
- **„Reviewer auf Admin zurückgefallen“** – für den Eintrag war kein Reviewer ermittelbar.

## Starten und entscheiden

Eine Kampagne beginnt als „Entwurf“. „Starten“ setzt sie auf „In Prüfung“; Nova benachrichtigt jeden Reviewer über die Zahl seiner Einträge.

- Jeder Eintrag wird mit „Bestätigen“ oder „Entziehen“ entschieden. Ein Entzug verlangt eine Begründung.
- Reviewer entscheiden nur die ihnen zugeordneten Einträge, Administratoren alle.
- Mehrere Einträge lassen sich auswählen und gemeinsam entscheiden. „Alle bestätigen“ bestätigt alle offenen Einträge – bei Reviewern nur die eigenen.
- Eine Entscheidung ist endgültig. Nova speichert sie mit Person, Zeitpunkt und Begründung am Eintrag.
- Entscheiden lässt sich nur, solange die Kampagne „In Prüfung“ ist.

Die „Frist“ schließt eine Kampagne nicht automatisch. Der Hintergrundjob „Rezertifizierungs-Fristerinnerung“ erinnert Reviewer mit offenen Einträgen höchstens einmal täglich, sobald die Frist innerhalb von „Erinnern innerhalb (Tage)“ – Voreinstellung 7 – liegt oder überschritten ist. Nova legt diesen Job nicht selbst an; Administratoren richten ihn unter „Monitoring“ → „Hintergrund-Jobs“ ein.

## Abschluss und Entzug

Sind alle Einträge entschieden, schließen Administratoren die Kampagne mit „Kampagne abschließen“ ab. Nova fragt dabei, ob die Entzüge jetzt ausgeführt werden sollen:

- **Ausführen:** Nova entfernt die entzogenen Zuweisungen in Nova – bei einer Business-Rolle einschließlich der darüber erhaltenen Berechtigungen. Ist „Zielsysteme automatisch provisionieren“ eingeschaltet, startet Nova für die betroffenen Identitäten Provisionierungsläufe, um die Rollen auch in den Zielsystemen zu entfernen. Werden die Fähigkeiten eines Routinen-Agenten entzogen, schaltet Nova diesen Routinen-Agenten ab.
- **Nicht ausführen:** Die Entscheidungen bleiben dokumentiert, der Zugriff bleibt bestehen. Die Kampagne ist trotzdem abgeschlossen; über sie lassen sich die Entzüge später nicht mehr ausführen.

> ⚠ **ENTZUG NUR BEIM ABSCHLUSS**
>
> Ein „Entziehen“ wirkt erst, wenn die Entzüge beim Abschluss ausgeführt werden. Bis dahin bleibt der Zugriff unverändert.

Nach dem Abschluss benachrichtigt Nova die Person, die die Kampagne angelegt hat, und die Administratoren. „CSV herunterladen“ liefert Administratoren alle Einträge mit Reviewer, Entscheidung, Begründung, Zeitpunkt, Hinweisen und Entzugsstatus als Nachweis. Abgeschlossene Kampagnen zeigen unter „Risikoreduktion (entzogen)“, wie viele entzogene Zuweisungen welche Risikobewertung hatten. Anlage, Start, Entscheidungen und Abschluss einer Kampagne protokolliert Nova.

# 7.2 Funktionstrennung (SoD)

Funktionstrennung (Segregation of Duties, SoD) soll verhindern, dass eine Identität Berechtigungen kombiniert, die getrennt bleiben müssen – etwa Kreditoren anlegen und Zahlungen buchen. Nova prüft dazu **SoD-Regeln**. Zwei Zusatzmodule erweitern die Prüfung für SAP.

## SoD-Regeln

Eine SoD-Regel beschreibt ein **Konfliktpaar**: zwei Berechtigungen oder Business-Rollen („Seite A“ und „Seite B“), die nicht dieselbe Identität halten soll. Jede Regel hat einen „Schweregrad“ – „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ – und lässt sich deaktivieren. Administratoren pflegen die Regeln unter „Compliance“ → „Risikoanalyse“ im Bereich „SoD-Regeln“. Die SoD-Regeln sind Teil von Nova und brauchen kein Zusatzmodul.

Nova bewertet dabei alle am Prüftag gültigen Zuweisungen einer Identität: direkte Berechtigungen, Business-Rollen und die Berechtigungen, die sie über Business-Rollen erhält.

## Wann Nova prüft

| Anlass | Geprüft wird | Ergebnis |
|---|---|---|
| neuer Antrag | Bestand der Ziel-Identität plus beantragte Rollen; nur Konflikte, zu denen der Antrag beiträgt | „Risiko-Befunde“ am Antrag |
| Scan | Bestand aller Identitäten außer deaktivierten und gelöschten | Register „SoD-Verstöße“ |
| Rezertifizierung | Bestand der Identitäten im Scope | Hinweis „SoD-Konflikt“ am Eintrag |

Zuweisungen, die nicht über einen Antrag entstehen – etwa direkt durch Administratoren oder über Org-Einheiten –, prüft Nova nicht vorab. Konflikte daraus erfasst der Scan.

Befunde zu einem Antrag zeigt Nova schon im Formular „Neue Anfrage“, danach in der Liste der Anfragen und in der Anfrage bei der betroffenen Rolle.

## Reaktion bei Anträgen

Die „Risiko-Policy“ unter „Risikoanalyse“ legt fest, wie Nova auf Befunde reagiert. Voreingestellt ist „Nur warnen“.

| „Risiko-Policy“ | Wirkung |
|---|---|
| „Nur warnen“ | Nova zeigt die Befunde am Antrag. |
| „SoD-Prüfschritt erzwingen“ | Hat eine beantragte Rolle Befunde und enthält ihr Ablauf keinen Schritt „SoD-Prüfung“, hängt Nova einen solchen Schritt an. |

| | |
|---|---|
| „Antrag blockieren“ | Bei Befunden legt Nova den Antrag nicht an. Administratoren können ihn mit einer „Übersteuerungs-Begründung“ trotzdem stellen. |

- Einen Schritt „SoD-Prüfung“ entscheiden Identitäten mit der Berechtigung „SoD Reviewer“ oder „Security“. Wer ihn trotz offener Befunde genehmigt, muss einen Kommentar angeben; die Befunde gelten dann als übersteuert. Steht ein solcher Schritt ohnehin im Genehmigungsablauf, wird er auch bei „Nur warnen“ aktiv, sobald Befunde vorliegen; ohne Befunde überspringt Nova ihn.
- Administratoren können einzelne Befunde in der Anfrage mit „Übersteuern“ und einer Begründung übersteuern. Auch „Genehmigen (Admin)“ verlangt bei offenen Befunden einen Kommentar.
- Übersteuerungen protokolliert Nova mit Person und Begründung.
- Mit den Schaltern „SoD-Regeln“ und „GRC-Plugin“ legen Administratoren fest, welche Quellen die Prüfung einbezieht.
- Scheitert eine Prüfung technisch, legt Nova den Antrag trotzdem an und protokolliert den Fehler.

## Register der SoD-Verstöße

„Scan starten“ unter „Risikoanalyse“ oder der Hintergrundjob „SoD-Verstoß-Scan“ gleicht den Bestand mit den aktiven Regeln ab; den Job legt Nova nicht selbst an. Das Ergebnis steht im Register „SoD-Verstöße“:

- Neue Konflikte erscheinen als „Offen“.
- Administratoren setzen einen Verstoß auf „Akzeptiert“ oder „Mitigiert“ – beides nur mit Begründung – oder öffnen ihn wieder.
- Findet ein Scan einen offenen oder akzeptierten Verstoß nicht mehr, setzt Nova ihn auf „Aufgelöst“. Taucht ein aufgelöster Konflikt wieder auf, öffnet Nova ihn erneut.
- Löschen Administratoren eine Regel, entfernt Nova auch deren Einträge im Register samt Begründungen. Beim Deaktivieren bleiben die Einträge erhalten.

## Zusatzmodule für SAP

Beide Module sind ab Werk ausgeschaltet. Administratoren schalten sie unter „Administration“ → „Plugins“ ein.

**„SoD-Analyse (SAP ABAP)“** prüft SAP-ABAP-Rollen in sich: auf kritische Einzelberechtigungen und auf Kombinationen, die nicht gemeinsam in einer Rolle vorkommen sollen. Grundlage sind die Berechtigungswerte der Rolle (Tabelle AGR_1251), die Nova per RFC aus dem SAP-System liest. Einlesen und Prüfen stoßen Administratoren an; beides läuft nicht automatisch. Betrifft ein SoD-Befund eines Antrags eine so geprüfte Rolle, speichert Nova deren Ergebnisse als technischen Nachweis mit dem Befund.

Beim Einschalten übernimmt das Modul das mitgelieferte Standard-Regelwerk – eine YAML-Datei –, sofern noch keine Regeln existieren. Eine Regel darin sieht so aus:

```yaml
rules:
  - key: vendor_create_and_payment   # stabiler Schlüssel
    name: "Kreditor anlegen UND Zahlung buchen"
    risk: critical                   # critical | high | medium | low
    type: conflict_combo             # oder critical_single
    requires_all:                    # alle Bedingungen müssen zutreffen
      - { auth_object: F_LFA1_APP, field: ACTVT, values: ["01", "02"] }
      - { auth_object: F_BKPF_BUK, field: ACTVT, values: ["01"] }
```

Eine Regel vom Typ `critical_single` nennt statt `requires_all` eine einzelne Bedingung unter `match`. `values: ["*"]` trifft auf jeden Wert des Felds zu.

**„GRC-Berechtigungsanalyse (SAP Access Control)“** liest das Regelwerk (Risiken und Funktionen) sowie die Zuordnungen von Rollen zu Konten aus einem vorhandenen SAP GRC Access Control. Bei Anträgen meldet Nova dann zusätzlich die Risiken, die die beantragten SAP-Rollen für die Ziel-Identität neu hinzufügen würden. Zur Antragszeit greift Nova dafür nicht auf SAP zu, sondern nutzt die zuvor gelesenen Daten.

# 7.3 Risikobewertung

Nova kennt zwei Arten von Risikoinformation:

- die **Risikobewertung** einer Berechtigung oder Business-Rolle – eine feste Einstufung, die Administratoren pflegen;
- **Risiko-Befunde** – Konflikte, die Nova bei einem Antrag aus Regeln ermittelt. Sie sind unter Funktionstrennung beschrieben.

## Die Stufen

Eine Rolle ist „Kritisch“, „Mittel“, „Niedrig“ oder „Kein Risiko“ bewertet. „Nicht bewertet“ steht für eine fehlende Einstufung und ist die Voreinstellung für neue Rollen. Eine Stufe „Hoch“ gibt es bei Rollen nicht; sie kommt nur bei Risiko-Befunden vor.

## Pflege

- Administratoren setzen die Bewertung im Feld „Risiko“ einer Berechtigung oder Business-Rolle.
- Die Bewertung einer Business-Rolle ist eigenständig: Nova leitet sie nicht aus den enthaltenen Berechtigungen ab. Ausnahme: Legt Role Mining eine Business-Rolle an, übernimmt Nova die höchste Bewertung ihrer Berechtigungen.
- Mit dem Zusatzmodul „GRC-Berechtigungsanalyse (SAP Access Control)“ können Administratoren die anhand des GRC-Regelwerks ermittelten Risiken als Bewertung auf die SAP-Rollen in Nova übertragen. Je Rolle zählt das höchste Risiko; „Hoch“ wird dabei zu „Kritisch“. Eine vorhandene Bewertung überschreibt Nova.

## Wo die Bewertung erscheint

- unter „Rollen“ in Liste und Detail jeder Berechtigung und Business-Rolle;
- an den Zuweisungen einer Identität;
- in einer Anfrage bei den beantragten Rollen;
- in der Rezertifizierung an jedem Eintrag – festgehalten bei Anlage der Kampagne – und nach dem Abschluss unter „Risikoreduktion (entzogen)“;
- auf dem „Dashboard“:
  - „Risiko-Exposition“ – Zahl der Zuweisungen kritisch bewerteter Berechtigungen und wie viele Identitäten sie halten;
  - „Risikoverteilung“ – alle Zuweisungen von Berechtigungen, direkt und über Business-Rollen, nach Stufe;
  - „Users mit höchstem Risiko“ – bis zu fünf Identitäten mit den meisten Zuweisungen kritisch bewerteter Berechtigungen;
  - „Risikobewertung“ im „Compliance-Status“ – der Anteil der Berechtigungen mit einer Bewertung.

## Was die Bewertung bewirkt

Die Risikobewertung allein ändert keinen Genehmigungsablauf und löst keinen Prüfschritt aus. Welche Schritte ein Antrag durchläuft, bestimmt der Genehmigungs-Workflow der Rolle; zusätzliche Schritte entstehen nur aus Risiko-Befunden. Die Bewertung fließt in den Rezertifizierungs-Hinweis „Externer mit hohem Recht“ ein und dient Role Mining und KI-Analysen als Kontext.

## KI-Analyse einer Identität

Ist ein KI-Modus aktiv, können Administratoren für eine Identität eine KI-Analyse erstellen lassen. Sie schätzt ein Risikoniveau ein und nennt Auffälligkeiten und Empfehlungen. Das Ergebnis lässt sich bearbeiten und speichern; Bewertungen und Zuweisungen ändert es nicht. Mehr dazu unter Überblick und Betriebsarten.

# 7.4 Role Mining

Role Mining sucht in den **direkten Zuweisungen** eines Bereichs nach wiederkehrenden Mustern und schlägt daraus Business-Rollen vor. Nova legt dabei nichts von selbst an: Administratoren prüfen jeden Vorschlag, und übernommen werden nur akzeptierte. Die Funktion steht nur Administratoren zur Verfügung, unter „Rollen“ → „Role Mining“.

## Welche Daten Nova auswertet

- **Scope:** eine Org-Einheit, auf Wunsch mit Unterbereichen („Unterbereiche einbeziehen“, voreingestellt an). Ein Lauf umfasst höchstens 10 000 Identitäten.
- **Identitäten:** nur aktive; technische Identitäten und KI-Agenten bleiben voreingestellt außen vor.
- **Zuweisungen:** nur direkte. Was eine Identität über Business-Rollen erhält, ist bereits gebündelt; bestehende Business-Rollen und ihre Zuweisungen lässt der Lauf unberührt. KI-Fähigkeiten ( `nova-ai:*` ) wertet Nova nicht aus.
- **Struktur:** Org-Einheiten und Planstellen nutzt Nova, um Vorschläge daran zu binden.

Zu Beginn friert Nova den Scope ein; Prüfung und Vorschau arbeiten auf diesem Stand. Es läuft immer nur ein Lauf zur selben Zeit.

## Wie Vorschläge entstehen

Nova rechnet vier Schichten nacheinander. Was eine Schicht abdeckt, zählt in den folgenden nicht mehr mit. So landet jede direkte Zuweisung in genau einem Vorschlag oder bleibt direkt.

| Schicht | Gebildet aus (Voreinstellung) | Bindung |
|---|---|---|
| „Globale Grundrolle“ | Rollen, die mindestens 90 % der Identitäten im Scope halten | Org-Einheit des Scopes |
| „Bereichs-Grundrollen“ | je Org-Einheit die Rollen, die mindestens 70 % ihrer Mitglieder halten | diese Org-Einheit |
| „Funktionsrollen“ | Rollen, die alle Inhaber einer Planstelle teilen, sowie häufige Kombinationen aus mindestens 2 Rollen bei mindestens 3 Identitäten | Planstelle oder Identitäten |
| „Sonderfunktionen“ | je Identität mindestens 2 Rollen, die im Scope weniger als 3 Identitäten halten | diese Identität |

Die Schwellen sind im Dialog „Neuer Mining-Lauf“ einstellbar, ebenso die „Maximale Anzahl BRs“ (Voreinstellung 12; Sonderfunktionen zählen nicht mit). Kandidaten jenseits dieses Budgets – gereiht nach der Zahl der überführten Zuweisungen – erscheinen als „Über BR-Budget“. Im „Ausreißer-Modus“ „Nur berichten“ erscheinen Sonderfunktionen nur als „Ausreißer“. Alle Zahlen, etwa Abdeckung und Auswirkungen, berechnet Nova selbst.

## KI-Prüfung (optional)

Ist ein KI-Modus aktiv, bewertet eine KI die Kandidaten, bevor sie als Vorschläge erscheinen:

- Sie schlägt Name und Beschreibung vor, bestätigt einen Kandidaten oder legt ein **Veto** ein und ordnet Sonderfunktionen als Sonderfunktion oder Anomalie ein.
- Ein Veto macht aus dem Kandidaten die Auffälligkeit „Keine Schicht gebildet“ mit der Begründung der KI; eine Anomalie erscheint als „Anomalie“ mit Empfehlung.
- Die KI kann keine Rollen oder Identitäten hinzufügen. Antworten mit unbekannten Kennungen verwirft Nova; Zahlen der KI übernimmt Nova nicht.
- Die KI erhält Kennzahlen, Namen, Beschreibungen und Bewertungen der Rollen sowie Namen von Org-Einheiten, Planstellen und bestehenden Business-Rollen. Bei personengebundenen Kandidaten kommen Namen von Identitäten hinzu, bei Sonderfunktionen auch deren Abteilung und Planstelle.
- Ohne KI oder bei einem Fehler der KI liefert der Lauf dieselben statistischen Kandidaten mit generischen Namen.

## Prüfen und übernehmen

- Vorschläge beginnen als „Offen“. Administratoren „Akzeptieren“ oder „Ablehnen“ sie, können sie umbenennen und einzelne Rollen entfernen („Rolle entfernen“). Ein Vorschlag ohne Rollen gilt als abgelehnt.
- „Anwenden…“ zeigt zuerst eine Vorschau gegen den aktuellen Datenbestand: wie viele direkte Zuweisungen überführt werden und welche Identitäten Rollen neu erhielten („Neuvergaben“).
- Nova übernimmt nur akzeptierte Vorschläge. Je Vorschlag legt Nova eine Business-Rolle an – mit der höchsten Risikobewertung ihrer Rollen –, weist sie den geprüften Identitäten zu und ersetzt deren abgedeckte direkte Zuweisungen durch Zuweisungen über die Business-Rolle. Gültigkeitsdaten übernimmt Nova dabei.
- „Business-Rollen an Org-Einheiten und Planstellen binden“ (voreingestellt an) hängt die Business-Rolle zusätzlich an die Org-Einheit oder Planstelle, sodass später Hinzukommende sie erben. Ausgeschaltet erhalten nur die geprüften Identitäten die Rolle.
- Weicht der aktuelle Datenbestand vom geprüften Stand ab, überspringt Nova den Vorschlag („Übersprungen (Drift)“). Ein neuer Lauf liefert dann ein aktuelles Bild.
- „Auffälligkeiten“ und „Verbleibende Direktzuweisungen“ sind nur ein Bericht; Nova entzieht daraus nichts. Entzüge laufen über die Rezertifizierung oder manuelle Pflege.

Nova protokolliert Start, Prüfentscheidungen und Übernahme eines Laufs sowie jede angelegte Business-Rolle mit ihrer Herkunft aus dem Lauf.

KAPITEL 8

# Nachvollziehbarkeit

## 8.1 Änderungsjournal

Das Änderungsjournal hält fest, was Nova in Zielsystemen geschrieben hat – mit den Werten vorher und nachher. Es beantwortet die Frage „Was hat Nova in diesem Zielsystem verändert?“ und ist die Grundlage, um einzelne Änderungen zurückzunehmen.

### Was ein Eintrag enthält

Das Journal erfasst Schreibvorgänge der Connectoren aller fünf Zielsystemtypen: angelegte, geänderte, gesperrte, entsperrte und gelöschte Konten, gesetzte Passwörter sowie hinzugefügte und entfernte Gruppenmitgliedschaften und SAP-Rollen. Ein Eintrag enthält:

- Zeitpunkt, Zielsystem und Objekt – Konto, Gruppe oder Rolle
- die Operation, etwa „Gruppe zugewiesen“ oder „Account deaktiviert“
- die betroffenen Werte „Vorher“ und „Nachher“
- soweit bekannt die auslösende Person („Auslöser“)
- ob sich die Änderung zurücknehmen lässt und ob sie bereits zurückgenommen wurde

Bei Gruppenmitgliedschaften und SAP-Rollen erfasst Nova nur wirksame Änderungen: Stellt Nova fest, dass etwa eine Mitgliedschaft schon bestand, entsteht kein Eintrag. Bei SAP ermittelt Nova die Rollenänderungen, indem es den Rollenbestand des Kontos vor und nach dem Schreiben liest.

**Passwörter** speichert das Journal nicht. Passwort-Attribute wie `userPassword`, `unicodePwd`, `password` oder `passwordProfile` ersetzt Nova durch `<redacted>` – auch in der Momentaufnahme eines gelöschten Objekts.

### Wo das Journal zu finden ist

Administratoren finden das Journal unter „Monitoring“ → „Provisioning-Log“. Die Auswahl „Backend-Änderung“ zeigt nur Journaleinträge. Ein Klick auf einen Eintrag öffnet die Details mit System, Objekt, Auslöser sowie den Werten „Vorher“ und „Nachher“.

Die Ansicht zeigt die jüngsten Einträge. Über die Programmierschnittstelle und den KI-Assistenten lässt sich das Journal zusätzlich nach Zielsystem, Operation, Konto und Zeitraum durchsuchen.

## Änderungen zurücknehmen

Für Active Directory, LDAP und Microsoft Entra ID können Administratoren einzelne Einträge zurücknehmen. In den Details steht dann „Rückgängig“; nach der Bestätigung „Änderung zurücksetzen“ führt Nova die Gegenoperation aus, etwa das Entfernen einer hinzugefügten Mitgliedschaft.

Vorher prüft Nova, ob der aktuelle Zustand im Zielsystem noch dem erfassten Nachher-Zustand entspricht. Wurde das Objekt seitdem anderweitig verändert, lehnt Nova die Rücknahme in der Oberfläche ab. Die Rücknahme erscheint als eigener Eintrag, und der ursprüngliche Eintrag erhält die Markierung „Zurückgesetzt“. Jeder Eintrag lässt sich nur einmal zurücknehmen; einen weiteren Versuch lehnt Nova mit „Diese Änderung wurde bereits zurückgesetzt“ ab.

| Zielsystem | Umkehrbar | Nicht umkehrbar |
|---|---|---|
| Active Directory, LDAP | Konto angelegt, geändert, gesperrt, entsperrt oder gelöscht; Gruppenmitgliedschaften | Passwörter |
| Entra ID | Gruppenmitgliedschaften | Kontoänderungen, Passwörter |
| SAP, Keycloak, SCIM | – | alle Einträge |

Außer beim Anlegen setzt eine Rücknahme einen erfassten Vorher-Wert voraus; konnte Nova ihn nicht lesen, ist der Eintrag nicht umkehrbar. Nicht umkehrbare Einträge dienen allein der Nachvollziehbarkeit.

### Gelöschte Konten in Active Directory und LDAP

Vor dem Löschen eines Kontos speichert Nova eine Momentaufnahme des Eintrags. Die Rücknahme legt das Konto daraus neu an, sofern unter dem DN kein Eintrag existiert. Das neue Objekt erhält eine neue eindeutige ID (`objectGUID`, `objectSid` bzw. `entryUUID`); Rechte, die an die alte ID gebunden waren, gehen nicht auf das neue Objekt über. Passwörter und vom Verzeichnis selbst verwaltete Attribute stellt Nova nicht wieder her. Gruppenmitgliedschaften stellt Nova nach Möglichkeit wieder her; Fehlschläge vermerkt Nova als Warnung im „Audit-Log“.

## Was das Journal nicht erfasst

Das Journal beschreibt Schreibvorgänge, die Nova selbst in Zielsystemen ausführt. Änderungen, die andere direkt im Zielsystem vornehmen, erfasst es nicht, ebenso wenig Änderungen innerhalb von Nova.

# 8.2 Protokolle

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Nova führt drei Protokolle. Jedes beantwortet eine eigene Frage:

| Protokoll | Beantwortet |
|---|---|
| „Audit-Log“ | Wer hat in Nova was getan? |
| „Provisioning-Log“ | Was hat Nova je Identität vorgesehen und ausgeführt? |
| Änderungsjournal | Was hat Nova im Zielsystem tatsächlich verändert? |

## Eine Kette, eine Korrelations-ID

Eine gemeinsame Korrelations-ID verbindet die Einträge, die zusammengehören:

**Antrag → Genehmigung → Zuweisung → Provisionierungslauf → Änderung im Zielsystem → Bestätigung**

So lässt sich ein Antrag bis in das Zielsystem verfolgen – und umgekehrt eine Änderung im Zielsystem bis zu ihrem Antrag.

## Was Nova festhält

- **Identitäten und Zuweisungen:** jede Änderung an Identitäten und an ihren Berechtigungen und Business-Rollen.
- **Konten:** jede Änderung an Konten, auch zurückgesetzte Passwörter und Sperren. Diese Einträge legt Nova bei der betroffenen Identität ab.
- **Katalog und Organisation:** Änderungen an Berechtigungen, Business-Rollen, Organisationseinheiten und Genehmigungsabläufen.
- **Konfiguration:** Änderungen an Zielsystemen und Einstellungen, jeweils mit den Werten vorher und nachher; Geheimnisse maskiert.
- **Anmeldungen:** erfolgreiche und fehlgeschlagene Anmeldungen an Nova – siehe Anmeldung an Nova.
- **KI-Assistenten:** Aktionen eines KI-Assistenten, gekennzeichnet mit dem Assistenten – siehe Leitplanken der KI.

Als **Akteur** nennt jeder Eintrag, wer oder was die Aktion ausgelöst hat: eine Person, ein Job oder ein KI-Assistent.

## Unveränderlich und dauerhaft

- Protokolleinträge werden nur angefügt. Keine Funktion in Nova ändert oder löscht sie, und der Datenbankbenutzer, mit dem Nova arbeitet, hat kein Recht dazu.
- Zeitstempel speichert Nova mit Zeitzone und zeigt sie in lokaler Zeit an.
- Wird eine Identität gelöscht, bleiben ihre Protokolleinträge erhalten.
- Geheimnisse wie Passwörter, Client-Secrets, Tokens und Schlüssel erscheinen in keinem Protokoll.

## Wer die Protokolle sieht

Die Protokolle sehen nur berechtigte Rollen: Administratoren und Prüfer. Zu finden sind sie unter „Monitoring“ → „Audit-Log“ und „Provisioning-Log“; das Änderungsjournal ist Teil des „Provisioning-Log“. Persönliche Protokollansichten zeigen jeder Identität nur ihre eigenen Einträge.

Wie Prüfer die Protokolle nutzen, zeigt der Leitfaden für Prüfer.

# 8.3 Leitfaden für Prüfer

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Diese Seite ordnet typische Prüfungsfragen den Stellen in Nova zu, die sie beantworten. Grundlage sind die drei Protokolle und die Korrelations-ID, die ihre Einträge verbindet.

## Einstieg: der Verlauf einer Identität

Der „Verlauf“ einer Identität zeigt als Zeitleiste die ganze Kette: Antrag → Genehmigung → Zuweisung → Provisionierungslauf → Änderung im Zielsystem → Bestätigung. Fragen zu einer einzelnen Person beginnen hier. Fragen über viele Identitäten beantworten Berichte unter „Reporting“ und deren Exporte.

> **EXPORT DES AUDIT-LOGS**
>
> Das gefilterte „Audit-Log“ lässt sich als CSV oder JSON exportieren.

## Typische Fragen

### Wer hat Zugriff auf X – und seit wann?

- **Wo:** ein Bericht unter „Reporting“, als Export.
- **Nachweis:** alle Identitäten mit gültiger Zuweisung der Berechtigung oder Business-Rolle, jeweils mit Beginn und Ende der Gültigkeit und dem Zeitpunkt der letzten Bestätigung im Zielsystem.

### Warum hat Person Y die Berechtigung Z?

- **Wo:** der „Verlauf“ der Identität.
- **Nachweis:** wer die Berechtigung beantragt hat, wer sie wann genehmigt hat, wann Nova sie provisioniert hat und wann Nova sie im Zielsystem bestätigt hat.

### Welche ausgetretenen Identitäten haben noch irgendwo ein aktives Konto?

- **Wo:** ein Bericht unter „Reporting“ über die Konten ausgetretener Identitäten.
- **Nachweis:** je Konto der zuletzt im Zielsystem gelesene Status mit dem Zeitpunkt des Lesevorgangs. Wie Nova Konten beim Austritt sperrt, beschreibt Konten und Passwörter.

### Welche Konten in einem Zielsystem gehören niemandem?

- **Wo:** die verwaisten Konten des Zielsystems – siehe Konten und Passwörter.
- **Nachweis:** alle Konten, die im Zielsystem existieren, aber keiner Identität gehören.

### Was hat sich in SAP in einem Zeitraum geändert – und wer hat es ausgelöst?

- **Wo:** das Änderungsjournal, eingegrenzt auf das SAP-System und den Zeitraum.
- **Nachweis:** jede Änderung, die Nova dort geschrieben hat, mit den Werten vorher und nachher und dem Akteur; über die Korrelations-ID auch der zugehörige Lauf und Antrag. Änderungen, die andere direkt in SAP vorgenommen haben, zeigt der Abgleich.

### Welche SoD-Konflikte bestehen – und wer hat welche Ausnahme akzeptiert?

- **Wo:** „Compliance“ → „Risikoanalyse“, Register „SoD-Verstöße“ – siehe Funktionstrennung (SoD).
- **Nachweis:** offene, akzeptierte und mitigierte Verstöße; bei akzeptierten und mitigierten die entscheidende Person und ihre Begründung. Übersteuerungen bei Anträgen hält Nova ebenfalls mit Person und Begründung fest.

### Wie ist eine Rezertifizierung belegt?

- **Wo:** „Compliance“ → „Rezertifizierung“, dort „CSV herunterladen“ – siehe Rezertifizierung.
- **Nachweis:** je Eintrag Reviewer, Entscheidung, Begründung, Zeitpunkt, Hinweise und Entzugsstatus.

KAPITEL 9

# KI in Nova

## 9.1 Überblick und Betriebsarten

Nova nutzt Sprachmodelle für Analysen, Vorschläge und einen Chat, über den sich Nova in Alltagssprache bedienen lässt. Die KI ergänzt Nova; voreingestellt ist sie aus.

### Grundsätze

- **Der Kern arbeitet ohne KI.** Identitäten, Berechtigungen, Anträge und Genehmigungen, Provisionierung, Abgleich und Rezertifizierung rufen kein Sprachmodell auf. Ohne KI fehlen nur die KI-Funktionen selbst.
- **Die KI schlägt vor, Menschen entscheiden.** Analysen, Beschreibungen, Rollenkandidaten, Importparser und Schritte für Lebenszyklus-Routinen sind Vorschläge. An Berechtigungen und Stammdaten ändert sich erst etwas, wenn eine berechtigte Identität einen Vorschlag übernimmt oder ausführt.
- **Der Chat handelt nur im Auftrag.** Er arbeitet mit den Rechten der angemeldeten Identität; als destruktiv gekennzeichnete Aktionen führt er erst nach ausdrücklicher Bestätigung aus. Siehe Leitplanken der KI.

### Betriebsarten

| Betriebs-art | Wohin Anfragen gehen |
|---|---|
| **Aus** | nirgendwohin – die Oberfläche bietet ihre KI-Funktionen nicht an |
| **Lokal** | an einen Ollama-Endpunkt, etwa im eigenen Rechenzentrum; Endpunkt-URL und Modell trägt ein Administrator ein |
| **Cloud** | an Anthropic (Claude) oder OpenAI, auf Wunsch über eine eigene Basis-URL |

Die Betriebsart wählt jede Identität im Kopfbereich mit dem Schalter „NOVA-AI“: „Aus“, „Lokal“ oder „Cloud“. Nova merkt sich die Wahl im Browser; voreingestellt ist „Aus“. Beim Umschalten prüft Nova, ob die gewählte Betriebsart eingerichtet ist, und schaltet sonst auf „Aus“. Der Healthcheck hat eine eigene KI-Einstellung.

Eingerichtet wird die KI unter „KI-Konfiguration“ im Menü, das ein Klick auf den eigenen Namen im Kopfbereich öffnet; speichern können dort nur Administratoren. Für die Cloud stehen zur Wahl:

- **Claude (Anthropic):** Claude Opus 5.5, Opus 5, Sonnet 5, Sonnet 4.6, Opus 4.8 und Haiku 4.5
- **OpenAI:** GPT-4o, GPT-4o Mini, GPT-4.1 und GPT-4.1 Mini

Den API-Schlüssel hinterlegt der Betrieb als Umgebungsvariable auf dem Server ( `CLAUDE_API_KEY` bzw. `OPENAI_API_KEY` ). Die Oberfläche zeigt nur an, ob er gesetzt ist.

## Wo Nova KI einsetzt

- **Chat „Nova AI“** mit Assistenten. Voreingestellt sind drei: „Access Requests“ findet Rollen und stellt Anträge, die den üblichen Genehmigungsablauf durchlaufen; „Help & Navigation“ beantwortet Fragen und liest nur; „Admin Chat“ steht nur Administratoren offen und darf alle Werkzeuge nutzen.
- **„KI-Nutzeranalyse“** einer Identität: Risikoeinschätzung, Auffälligkeiten und Vergleich mit anderen Identitäten derselben Org-Einheit. Administratoren können das Ergebnis bearbeiten und speichern.
- **Berichte:** Aus einer Beschreibung erzeugt die KI Abfragen und Aufbau eines Berichts.
- **Role Mining:** Die Kandidaten für Business-Rollen berechnet Nova ohne KI; die KI benennt, beschreibt und bewertet sie. Siehe Role Mining.
- **Migration Workbench:** Die KI schreibt den Parser für eine Importdatei. Siehe Umstieg von SAP IdM.
- **Vorschläge beim Einrichten:** Beschreibung einer Business-Rolle, Ausdrücke für Feldzuordnungen und Schritte für Lebenszyklus-Routinen, zusammengesetzt aus festen Bausteinen.
- **Weitere:** „Governance Analyse“ (ohne KI bleiben die Fragen zur manuellen Bewertung offen), die Einordnung der Befunde im „AI Healthcheck“ und eine Vorprüfung unter „Problem melden“.

## Welche Daten an das Modell gehen

Im Modus „Lokal“ gehen die folgenden Daten an den eingetragenen Ollama-Endpunkt, im Modus „Cloud“ an Anthropic oder OpenAI.

| Funktion | Was das Modell erhält |
|---|---|
| Chat | die Nachrichten; Name, Abteilung, Rollen, Business-Rollen und Org-Einheiten der angemeldeten Identität; die Ergebnisse der aufgerufenen Werkzeuge |
| „KI-Nutzeranalyse“ | Name, E-Mail, Abteilung, Standort, Status und Typ der Identität; ihre Org-Einheiten; Namen und Risiko ihrer Business-Rollen und Berechtigungen; Namen und Typ der Zielsysteme; die Zahl der Vergleichsidentitäten |
| Berichte | die Beschreibung, eine gewählte Vorlage und die Struktur der Datenbanktabellen; im Berichtsdialog nach jedem Lauf außerdem je Abfrage Spaltennamen, Zeilenzahl und die erste Ergebniszeile |
| Role Mining | Namen, Beschreibungen und Risiko der Berechtigungen, Kennzahlen, Namen von Org-Einheiten und Planstellen; bei personengebundenen Kandidaten Namen von Identitäten |
| Migration Workbench | einen Auszug der Datei (die ersten Zeilen, höchstens 20.000 Zeichen), die Chatnachrichten und das Ergebnis des letzten Dry-Runs mit bis zu 15 abgelehnten Datensätzen |
| Vorschläge beim Einrichten | die eingegebene Beschreibung; Namen der Objekte, auf die ein Vorschlag verweisen kann, etwa Berechtigungen, Business-Rollen und Org-Einheiten, bei offenen Anträgen samt Namen der Antragsteller |
| Governance Analyse | Fragen und Soll-Antworten des Fragebogens, hinterlegte Fakten zu Nova |

| | |
|---|---|
| AI Healthcheck | bis zu 100 offene Befunde mit Betreff und Details |
| Problem melden | Beschreibung, Art der Meldung, aktuelle Seite und einen angehängten Screenshot |

Unterstützt ein Modell keine Werkzeugaufrufe, weicht der Chat auf einen einfacheren Modus aus. Dann schickt er einen Datenauszug mit, darunter das Organigramm mit den Namen der Mitglieder und im Assistenten „Access Requests“ die beantragbaren Rollen.

**DIE EINRICHTUNG AUF DEM SERVER ENTSCHEIDET**

Nova erreicht nur ein Modell, das eingerichtet ist. Ohne API-Schlüssel auf dem Server lehnt Nova jede Cloud-Anfrage ab, bevor Daten das System verlassen. Wer Cloud-Anbieter ausschließen will, setzt keinen Schlüssel und betreibt bei Bedarf ein Modell über Ollama in der eigenen Infrastruktur.

# 9.2 Leitplanken der KI

Der Chat „Nova AI“ kann Daten in Nova nicht nur lesen, sondern auch ändern. Die Grenzen dafür setzt Nova auf dem Server durch – unabhängig davon, welches Modell antwortet und was es vorschlägt.

## Nur mit den Rechten der angemeldeten Identität

Der Chat greift nicht selbst auf die Datenbank zu. Er ruft Werkzeuge auf, und jedes Werkzeug führt intern einen Endpunkt von Nova aus – in der Sitzung der Identität, die den Chat bedient. Berechtigungsprüfung, Validierung, Protokollierung und Folgeaktionen sind damit dieselben wie in der Oberfläche. Der Chat erweitert die Rechte der Identität nicht.

Einige Werkzeuge verbinden mehrere Endpunkte zu einem Ablauf. Schreibende Werkzeuge dieser Art stehen nur Administratoren zur Verfügung; ausgenommen ist Selbstbedienung wie das Stellen von Anträgen.

## Eine Werkzeugliste je Assistent

Unter „Administration › KI-Assistenten“ legen Administratoren für jeden Assistenten fest, welche Werkzeuge er nutzen darf.

- Ruft das Modell ein Werkzeug außerhalb dieser Liste auf, lehnt Nova den Aufruf ab – auch auf Umwegen, etwa über einen Export.
- Alle Werkzeuge freigeben lässt sich nur für Assistenten, die auf Administratoren beschränkt sind. Der voreingestellte „Admin Chat“ hat immer alle Werkzeuge und bleibt immer auf Administratoren beschränkt.
- Assistenten, die nur Administratoren offenstehen, zeigt Nova anderen Identitäten nicht an und weist deren Anfragen an sie ab.
- Die Werkzeuglisten, die Anmelderichtlinie, die Lebenszyklus-Routinen und die KI-Routinen-Assistenten ändert der Chat nicht, ebenso wenig Einstellungen mit Geheimnissen wie die KI-Konfiguration. Das geht nur in der Administrationsoberfläche.

## Bestätigung vor destruktiven Aktionen

Werkzeuge, die Nova als destruktiv kennzeichnet – etwa solche, die löschen –, führt der Chat nicht sofort aus. Zuerst zeigt er die Karte „Bestätigung erforderlich“ mit der Aktion und ihren Argumenten; unter „Aktueller Stand“ steht, soweit verfügbar, das betroffene Objekt. Ausgeführt wird frühestens mit der nächsten Nachricht der Identität: über „Bestätigen und ausführen“ oder, wenn sie im Text zustimmt, durch einen erneuten Aufruf des Modells mit Bestätigung. Dabei gilt:

- Die Bestätigung zählt nur in der unmittelbar folgenden Nachricht derselben Identität an denselben Assistenten und höchstens 10 Minuten lang.
- Werkzeug und Argumente müssen der Vorschau genau entsprechen, sonst verlangt Nova eine neue Vorschau.

- Das Modell kann sich nicht selbst bestätigen: Eine Bestätigung in derselben Nachricht, die die Vorschau erzeugt hat, lehnt Nova ab.
- „Bestätigen und ausführen“ führt genau den gespeicherten Aufruf aus. Für die Antwort darauf stehen dem Modell nur lesende Werkzeuge zur Verfügung.
- Je Nachricht führt der Chat höchstens eine destruktive Aktion aus.

## Geheimnisse bleiben außen vor

Passwörter, Client-Secrets, Tokens und API-Schlüssel nimmt kein Werkzeug als Parameter an. Nova prüft das beim Start für jede Werkzeugdefinition und bei jedem Aufruf; auch das Leeren eines Geheimnisses lehnt der Chat ab. Geheimnisse werden in der Oberfläche eingegeben. In Werkzeugergebnissen und Vorschauen ersetzt Nova solche Felder und verschlüsselt gespeicherte Werte durch einen Platzhalter.

## Grenzen je Nachricht

| Grenze | Wert |
|---|---|
| Modellaufrufe im Werkzeugkreislauf | 12 |
| destruktive Aktionen | 1 |
| gleicher Werkzeugaufruf mit gleichen Argumenten | 3, danach gesperrt |
| Umfang eines Werkzeugergebnisses | 12.000 Zeichen, darüber gekürzt |
| Werkzeugergebnisse zusammen | 60.000 Zeichen, danach keine weiteren Aufrufe |

Ein Budget für Token oder Kosten je Identität oder Zeitraum setzt Nova nicht.

## Nachvollziehbarkeit

- Protokolleinträge, die während eines Werkzeugaufrufs entstehen, versieht Nova im Detail mit dem Vermerk `via: ai_chat:<Assistent>`. Unter „Monitoring › Audit-Log“ zeigt der Filter „Herkunft“ mit „KI-Chat“ genau diese Einträge.
- Protokolliert wird, was der aufgerufene Endpunkt protokolliert – beim Aufruf aus dem Chat wie aus der Oberfläche. Einen eigenen Eintrag je Nachricht oder je Werkzeugaufruf schreibt Nova nicht.
- Den Chatverlauf speichert Nova je Identität und Assistent, damit er sich unter „Chat-Verlauf“ wieder öffnen lässt. Jede Identität sieht in Nova nur ihre eigenen Verläufe und kann sie löschen – einzeln oder mit „Alle löschen“. Der Verlauf ist deshalb kein Nachweis; maßgeblich ist das Audit-Log.

Welche Daten der Chat an das Modell schickt, beschreibt Überblick und Betriebsarten.

# 9.3 KI-Agenten als Identitäten

Nova führt KI-Agenten als eigenen Identitätstyp „KI-Agent“; in der Liste der Identitäten stehen sie auf der Registerkarte „AI-Agenten“. Für sie gelten dieselben Mittel wie für Personen – Anträge, Genehmigungen, Rezertifizierung und Protokoll –, ergänzt um Regeln, die nur für Agenten gelten.

## Pflichtangaben

Einen KI-Agenten legt ein Administrator an. Nova verlangt dafür:

- eine **verantwortliche Person (Owner)** – eine bestehende Identität vom Typ natürliche Person,
- einen **Zweck**, der beschreibt, wozu der Agent existiert.

Optional sind ein Termin für das **nächste Review** und ein **Ablaufdatum**.

## Berechtigungen: nur Fähigkeitsrollen

Berechtigungen erhalten KI-Agenten als Fähigkeitsrollen mit dem Präfix `nova-ai:`. Nova legt für jede Kombination aus Objekt (etwa Identität, Business-Rolle oder Konto) und Aktion (anlegen, lesen, ändern, löschen), für die es einen Baustein gibt, eine solche Rolle an – zum Beispiel `nova-ai:identity.update`. Voreingestellt gilt Lesen als risikolos, Anlegen und Ändern als mittleres und Löschen als kritisches Risiko; Administratoren können das ändern. Die Rollen wirken nur in Nova, in Zielsysteme überträgt Nova sie nicht.

Nova hält diese Rollen von allen anderen Berechtigungen getrennt:

- Beim Zuweisen und Beantragen lässt Nova für KI-Agenten nur Fähigkeitsrollen zu; Business-Rollen und andere Berechtigungen weist es ab.
- Fähigkeitsrollen erhalten nur KI-Agenten. Mitglied einer Business-Rolle können sie nicht sein.
- Einen Antrag für einen KI-Agenten stellen nur sein Owner, dessen Vertretung oder ein Administrator. Ein Genehmigungsablauf kann den „Agent-Owner“ als Genehmiger vorsehen, siehe Genehmigungsabläufe.

## Wofür die Fähigkeitsrollen gelten

Nova kann Schritte für Lebenszyklus-Routinen mit KI aus Bausteinen zusammensetzen. Welche Objekte und Aktionen die KI dabei verwenden darf, legen Administratoren unter „Administration › KI-Assistenten“ auf der Registerkarte „KI-Routinen-Assistenten“ fest:

- Ohne aktiven KI-Routinen-Assistenten mit freigegebenen Fähigkeiten setzt die KI keine Schritte zusammen.
- Ein Routinen-Assistent lässt sich mit einem KI-Agenten verknüpfen. Dann zählen zusätzlich die Fähigkeitsrollen, die der Agent gültig besitzt.
- Ist der verknüpfte Agent inaktiv, gelöscht oder sein Ablaufdatum überschritten, zählt der Routinen-Assistent nicht mehr.

- Das betrifft nur das Zusammensetzen neuer Schritte: Gespeicherte und eingebaute Schritte laufen weiter.

Der KI-Agent selbst handelt dabei nicht in Nova. Die Verknüpfung macht ihn zum verantwortlichen Bezugspunkt, nicht zum Akteur.

## Überprüfung

- **Review-Termin:** Der Job-Typ „Agent Review Scan“ findet aktive KI-Agenten, deren Review-Termin überschritten ist, und schreibt je Agent und Lauf einen Eintrag ins Audit-Log – mit Owner und verknüpften Routinen-Assistenten. Einen solchen Job legt ein Administrator unter „Monitoring › Hintergrund-Jobs“ mit „Neuer Job“ an; voreingestellt ist keiner. Benachrichtigungen verschickt der Job nicht.
- **Rezertifizierung:** Eine Kampagne mit dem Umfang „KI-Agenten“ prüft die Berechtigungen der KI-Agenten; als Prüfer lässt sich „Agent-Owner (KI-Identität)“ wählen. Zusätzlich steht für jeden verknüpften Routinen-Assistenten die Matrix seiner freigegebenen Objekte und Aktionen zur Prüfung. Wird sie entzogen, schaltet Nova den Routinen-Assistenten ab. Siehe Rezertifizierung.

## Wenn der Owner austritt

Der voreingestellte Austrittsablauf enthält den Schritt „Ownership-Übergabe für KI-Agenten“. Er überträgt die KI-Agenten der austretenden Identität an deren Vertretung, ersatzweise an ihre Führungskraft laut Organisation. Nachfolger wird nur eine aktive natürliche Person, die nicht im selben Lauf austritt. Findet Nova keine, bleibt der Agent ohne Owner, und Nova schreibt eine Warnung ins Audit-Log; jede Übergabe protokolliert Nova ebenfalls. Siehe Eintritt, Wechsel, Austritt.

## Konten in Keycloak

In Keycloak legt Nova für einen KI-Agenten statt eines persönlichen Kontos einen vertraulichen Client mit Dienstkonto an, der sich maschinell anmeldet (Client Credentials). Seine Tokens gelten voreingestellt fünf Minuten. Ein neues Client-Secret erzeugt „Secret rotieren“; Nova zeigt es einmal an und speichert es nicht. Siehe Keycloak.

KAPITEL 10

# Sicherheit und Datenschutz

## 10.1 Anmeldung an Nova

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Diese Seite beschreibt die Anmeldung an Nova selbst. Wie Nova Konten und Passwörter in Zielsystemen verwaltet, beschreibt Konten und Passwörter.

### Wer sich anmelden darf

Anmelden können sich nur aktive Identitäten mit einem aktiven Nova-Konto, also einem aktiven Konto im System „Nova IAM“. Welche Status eine Identität haben kann, beschreibt Identitäten und ihr Status.

Laufende Sitzungen beendet Nova sofort, wenn

- die Identität in den Status **Ruhend** oder **Ausgetreten** wechselt,
- ihr Nova-Konto gesperrt wird oder
- ihr Passwort geändert wird.

Außerdem hat jede Sitzung eine Höchstdauer. Danach ist eine neue Anmeldung nötig.

### Anmeldeverfahren

| Verfahren | Hinweis |
|---|---|
| Passwort | Nova speichert nur einen gesalzenen Hash des Passworts. |
| Einmalcode per E-Mail | Reiter „E-Mail-Code“ auf der Anmeldeseite |
| Single Sign-on über Microsoft Entra ID | „Mit Microsoft Entra anmelden“, sofern eingerichtet |
| Zweiter Faktor (TOTP) | mit dem Zusatzmodul „Native MFA (TOTP)“ |

Alle Verfahren durchlaufen dieselben Prüfungen – auch den zweiten Faktor, wo er verlangt ist. Ob der zweite Faktor für Administratoren oder für alle Identitäten Pflicht ist, legen Administratoren fest.

Das Zusatzmodul „Native MFA (TOTP)“ ist ab Werk ausgeschaltet; Administratoren schalten es unter „Administration“ → „Plugins“ ein.

## Passwortregeln

Für Passwörter, mit denen sich Identitäten an Nova anmelden, gelten drei Arten von Regeln:

- **Mindestlänge und Zusammensetzung** – festgelegt unter „Administration“ → „Provisionierung“ → „Passwortregeln“,
- **Passwort-Historie** – zuletzt verwendete Passwörter lassen sich nicht erneut setzen,
- **Höchstalter** – ist es überschritten, muss die Identität bei der Anmeldung ein neues Passwort vergeben.

Historie und Höchstalter stellen Administratoren in der „Nova Login-Policy“ unter „Administration“ → „Identitätsmanagement“ → „Authentifizierung“ ein.

## Fehlversuche

Nach wiederholten Fehlversuchen sperrt Nova das Nova-Konto. Schwelle, Zeitfenster und Dauer der Sperre legen Administratoren ebenfalls in der „Nova Login-Policy“ fest. Falsche Einmalcodes und falsche Codes des zweiten Faktors zählen wie falsche Passwörter.

## Selbstregistrierung

Eine Selbstregistrierung, bei der eine Person bei der Anmeldung selbst eine Identität anlegt, ist ab Werk ausgeschaltet.

## Nova als Anmeldedienst für andere Anwendungen

Mit dem Zusatzmodul „OIDC Identity Provider“ meldet Nova Identitäten auch an anderen Anwendungen an: Nova arbeitet dann als OpenID-Connect-Provider. Dabei gelten dieselben Regeln wie für die Anmeldung an Nova. Das Zusatzmodul ist ab Werk ausgeschaltet.

Anmeldungen und Fehlversuche hält Nova im „Audit-Log“ fest – siehe Protokolle.

# 10.2 Datenschutz und Verschlüsselung

> **GEPLANT**
>
> Diese Seite beschreibt beschlossenes Verhalten, das mit einem der nächsten Releases ausgeliefert wird. Bis dahin kann die aktuelle Version von Nova davon abweichen.

Diese Seite beschreibt, welche Daten Nova speichert und wie Nova sie schützt.

## Welche Daten Nova speichert

- **Stammdaten der Identitäten** aus dem Personalsystem und anderen Quellsystemen
- **Konten** der Identitäten in den Zielsystemen
- **Berechtigungen und Zuweisungen**
- **Anträge und Entscheidungen**
- **Protokolle** – siehe Protokolle

## Geheimnisse der Zielsysteme

Passwörter, Client-Secrets und Tokens, mit denen Nova die Zielsysteme anspricht, speichert Nova verschlüsselt. Den Schlüssel hält allein der Betreiber; er liegt nicht in der Datenbank.

- Beim Start prüft Nova den Schlüssel.
- Lässt sich das Geheimnis eines Zielsystems nicht entschlüsseln, verwendet Nova dieses Zielsystem nicht.
- Der Schlüssel lässt sich wechseln.

Passwörter der Konten in Zielsystemen speichert Nova nicht – siehe Konten und Passwörter.

## Verschlüsselte Verbindungen

- **Web-Oberfläche:** über TLS. Die Verschlüsselung übernimmt ein Reverse-Proxy, den der Betreiber vor Nova schaltet – siehe Installation.
- **Zielsysteme:** Zu Verzeichnisdiensten überträgt Nova Passwörter nur über LDAPS oder StartTLS – siehe Konten und Passwörter.

## Minimale Rechte

- Der Datenbankbenutzer, mit dem Nova arbeitet, hat keine administrativen Rechte in der Datenbank.
- „Freie Reports“ – selbst geschriebene SQL-Abfragen – laufen nur lesend und mit einer eingeschränkten Datenbankrolle.

## Aufbewahrung und Löschung

Identitäten im Papierkorb löscht Nova nach Ablauf der Aufbewahrungsfrist endgültig – siehe Identitäten und ihr Status. Dabei entfernt Nova die personenbezogenen Daten. Protokolleinträge bleiben zur Nachvollziehbarkeit erhalten.

## Demo- und Rücksetzfunktionen

Funktionen, die Demodaten laden oder Daten zurücksetzen, lassen sich nicht gegen eine Produktivdatenbank ausführen.

## KI

Welche Daten Nova an ein Sprachmodell gibt und ob sie dabei das System verlassen, hängt von der Betriebsart der KI ab – siehe Überblick und Betriebsarten.

## Sicherheitslücken melden

Für Hinweise auf Sicherheitslücken ist ein Meldeweg in einer security.txt veröffentlicht.

KAPITEL 11

# Betrieb

## 11.1 Voraussetzungen

Nova läuft als Container mit einer PostgreSQL-Datenbank und wird im Browser bedient. Auf den Arbeitsplätzen ist nichts zu installieren. Die Installationsschritte beschreibt Installation.

### Laufzeitumgebung

| Baustein | Voraussetzung |
|---|---|
| Plattform | ein Server mit Docker Engine und Docker Compose v2 oder ein Cluster in SAP BTP, Kyma Runtime |
| Datenbank | PostgreSQL 16; die mitgelieferten Vorlagen betreiben sie als eigenen Container |
| Anwendung | Python 3.12 im Image; die Oberfläche entsteht beim Bau des Images |
| Zugriff der Anwender | HTTPS über einen vorgeschalteten TLS-Proxy oder das Kyma-Gateway |

Beim Bau des Images lädt Docker die Basis-Images für Node.js und Python sowie Pakete aus den Quellen von Debian, npm und PyPI. Der Rechner, der das Image baut, braucht Zugriff auf diese Quellen.

#### Eine Instanz

Nova läuft als genau eine Instanz mit einem Gunicorn-Worker (`GUNICORN_WORKERS=1`). Den Zeitplaner für Hintergrund-Jobs und den Zustand laufender Jobs hält Nova im Prozess; eine zweite Instanz oder ein zweiter Worker würde geplante Jobs doppelt ausführen. Mehr Last fängt Nova über Threads ab (`GUNICORN_THREADS`, Voreinstellung 8).

#### Größe

Eine verbindliche Größenempfehlung gibt es nicht. Anhaltspunkte:

- Die Kyma-Vorlage ist für eine Demo-Installation bemessen. Sie reserviert für Nova 0,2 CPU und 384 MiB Arbeitsspeicher bei einer Obergrenze von 1 CPU und 1 GiB, für PostgreSQL 0,1 CPU und 256 MiB bei einer Obergrenze von 0,5 CPU und 512 MiB, dazu 2 GiB Speicherplatz für die Datenbank.
- Nova öffnet bis zu 30 Verbindungen zur Datenbank.

## Netzwerk

Nova baut die Verbindungen zu den Zielsystemen selbst auf. Freizugeben sind nur die Wege zu den tatsächlich angebundenen Systemen:

| Ziel | Protokoll und übliche Ports |
|---|---|
| SAP (ABAP) | RFC zum Gateway des Anwendungsservers, Port 33‹Systemnummer›; bei Anmeldung über den Message-Server auch dessen Port; optional über einen SAProuter |
| Active Directory, LDAP | LDAPS (636) oder LDAP (389) |
| Microsoft Entra ID | HTTPS (443) zur Microsoft-Anmeldung und zu Microsoft Graph |
| Keycloak | HTTPS zur Anmelde- und Admin-Schnittstelle des Realms |
| SCIM-Anwendungen | HTTPS zum SCIM-Endpunkt der Anwendung |
| E-Mail | SMTP, Voreinstellung Port 587 mit STARTTLS |
| KI, optional | HTTPS zum Cloud-Anbieter oder Verbindung zum eigenen Ollama-Server |

Dieselben Wege gelten, wenn ein System als Quellsystem dient – etwa ein LDAP-Verzeichnis mit HR-Daten oder SAP-Organisationsdaten per RFC. Einzelheiten zu den Anbindungen stehen unter Zielsysteme – Überblick.

### SAP: RFC-SDK des Kunden

Für SAP nutzt Nova das SAP NetWeaver RFC SDK. Es ist SAP-Software und nicht im Standard-Image enthalten: Das Image aus `deploy/Dockerfile` wird ohne SDK gebaut, SAP-Funktionen bleiben darin abgeschaltet. Wer SAP anbinden will, stellt das SDK für Linux bereit und nimmt es zusammen mit dem Python-Paket `pyrfc` in das Image auf.

### E-Mail

Für Benachrichtigungen braucht Nova einen SMTP-Server. Eingerichtet wird er unter „Administration“ → „Benachrichtigungen“ → „E-Mail (SMTP)“. Ist dort nichts hinterlegt, verwendet Nova die Umgebungsvariablen `NOVA_SMTP_*`; nötig sind dann mindestens `NOVA_SMTP_HOST` und `NOVA_SMTP_FROM_ADDRESS`.

## Umgebungsvariablen

| Variable | Bedeutung |
|---|---|

| | |
|---|---|
| `SECRET_KEY` | Pflicht. Schlüssel für die Anmeldesitzungen. Fehlt er, erzeugt Nova bei jedem Start einen neuen; nach jedem Neustart müssen sich dann alle neu anmelden. Die Compose-Vorlage startet ohne ihn nicht. |
| `NOVA_ENCRYPTION_KEY` | Pflicht. Schlüssel, mit dem Nova gespeicherte Zugangsdaten verschlüsselt. Warum er getrennt aufzubewahren ist, steht unter Updates und Sicherung. |
| `DB_HOST`, `DB_PORT`, `DB_NAME`, `DB_USER`, `DB_PASSWORD` | Verbindung zur Datenbank |
| `TRUST_PROXY`, `SESSION_COOKIE_SECURE` | hinter einem TLS-Proxy beide auf `1` |

Optional sind unter anderem `NOVA_TIMEZONE` – die Zeitzone, nach der Nova den Kalendertag für Gültigkeiten bestimmt, Voreinstellung Europe/Berlin –, `NOVA_SMTP_*` sowie `CLAUDE_API_KEY` oder `OPENAI_API_KEY` für die KI eines Cloud-Anbieters. `RUN_DUMMIES` startet Demo-Zielsysteme im Container und bleibt im Produktivbetrieb auf `0`.

# 11.2 Installation

Für Nova gibt es zwei vorbereitete Installationswege. Beide bauen das Image aus `deploy/Dockerfile` und betreiben Nova zusammen mit PostgreSQL 16. Die Vorlagen liegen im Verzeichnis `deploy/`; die Befehle unten laufen in dem Verzeichnis, das `deploy/` enthält. Was vorher bereitstehen muss, beschreibt Voraussetzungen.

## Einzelner Server mit Docker Compose

Die Vorlage `deploy/docker-compose.yml` startet Nova und PostgreSQL als Container. Die Datenbank liegt in einem eigenen Docker-Volume und übersteht Neustarts und Updates.

1. **Konfiguration anlegen.** `deploy/.env.example` nach `deploy/.env` kopieren und darin mindestens `SECRET_KEY`, `NOVA_ENCRYPTION_KEY` und ein eigenes `DB_PASSWORD` setzen; `RUN_DUMMIES` bleibt auf `0`. Die beiden Schlüssel lassen sich so erzeugen, der zweite mit Python und dem Paket `cryptography`:

   ```
   openssl rand -hex 32
   python -c "from cryptography.fernet import Fernet; print(Fernet.generate_key().decode())"
   ```

2. **Für den TLS-Proxy vorbereiten.** In `deploy/.env` `APP_BIND=127.0.0.1` setzen, damit Nova nur auf dem Server selbst erreichbar ist, dazu `TRUST_PROXY=1` und `SESSION_COOKIE_SECURE=1`.

3. **Bauen und starten.**

   ```
   docker compose -f deploy/docker-compose.yml --env-file deploy/.env up -d --build app
   docker compose -f deploy/docker-compose.yml --env-file deploy/.env logs -f app
   ```

   Der erste Aufruf baut das Image und dauert einige Minuten. Nova ist bereit, sobald das Protokoll zeigt, dass Gunicorn auf Port 8000 lauscht. Die Vorlage enthält außerdem den Dienst `handbook`, der dieses Handbuch ausliefert; für Nova wird er nicht gebraucht.

4. **TLS-Proxy einrichten.** Ein Webserver auf dem Server nimmt HTTPS entgegen und leitet an `http://127.0.0.1:8000` weiter. Die nginx-Vorlagen unter `deploy/nginx/` zeigen die Einstellungen: die Kopfzeilen `Host`, `X-Forwarded-For`, `X-Forwarded-Proto` und `X-Forwarded-Host` weiterreichen, Uploads bis 25 MB zulassen und Zeitlimits von 120 Sekunden setzen. Das Zertifikat kann zum Beispiel certbot von Let's Encrypt beziehen.

> ⚠ **NICHT OHNE TLS BETREIBEN**
>
> Ohne vorgeschalteten Proxy liefert Nova nur unverschlüsseltes HTTP aus. Vor dem Einsatz mit echten Daten gehört ein TLS-Proxy davor.

## SAP BTP, Kyma Runtime

Die Vorlagen unter `deploy/kyma/` betreiben Nova in einem Kyma-Cluster: ein Deployment für Nova, PostgreSQL als StatefulSet mit eigenem Volume und eine APIRule, die Nova per HTTPS über das Kyma-Gateway erreichbar macht – unter `https://nova-iam.<Cluster-Domain>`.

1. **Zugang und Namespace.** kubectl mit der Kubeconfig des Clusters einrichten; die Anmeldung läuft über das OIDC-Plugin kubelogin. Einen Namespace anlegen, zum Beispiel `nova-iam`. Liegt das Image in einer privaten Registry, zusätzlich ein Image-Pull-Secret anlegen.
2. **Image bereitstellen.** Das Image aus `deploy/Dockerfile` bauen, in die Registry laden und in `deployment.yaml` eintragen. Jede neue Version bekommt ein neues Tag: Ein Tag, das ein Knoten bereits geladen hat, lädt er nicht erneut.
3. **Secret anlegen.** Nova und PostgreSQL lesen ihre Umgebung aus dem Secret `nova-secrets`, Vorlage `secret.example.yaml`: `POSTGRES_DB`, `POSTGRES_USER`, `POSTGRES_PASSWORD`, `DB_NAME`, `DB_USER`, `DB_PASSWORD` (gleich `POSTGRES_PASSWORD`), `SECRET_KEY` und `NOVA_ENCRYPTION_KEY`. Weitere Variablen wie `SESSION_COOKIE_SECURE=1` oder `NOVA_SMTP_*` kommen als zusätzliche Schlüssel hinzu. Die echten Werte gehören nicht in versionierte Dateien.
4. **Für den Produktivbetrieb anpassen.** Die Vorlage ist für eine Demo ausgelegt: In `deployment.yaml` `RUN_DUMMIES` auf `"0"` setzen und `dummies-expose.yaml` nicht anwenden. `replicas: 1` und die Strategie `Recreate` bleiben – so laufen nie zwei Instanzen gleichzeitig.
5. **Anwenden.**

```
kubectl -n nova-iam apply -f deploy/kyma/postgres.yaml
kubectl -n nova-iam apply -f deploy/kyma/deployment.yaml
kubectl -n nova-iam apply -f deploy/kyma/apirule.yaml
kubectl -n nova-iam rollout status deploy/nova-iam
```

## Der erste Start

Beim Start legt Nova das Datenbankschema an und bringt es bei jedem weiteren Start auf den aktuellen Stand. Beim ersten Start schreibt Nova außerdem Grunddaten, darunter:

- ein Administratorkonto mit voreingestelltem Kennwort, das Administratoren gleich nach der ersten Anmeldung ändern sollten,
- die Berechtigungen „Admin“, „Manager“, „Security“ und „SoD Reviewer“,
- die voreingestellten Hintergrund-Jobs, siehe Überwachung und Jobs,
- zwei Beispiel-Zielsysteme, die auf lokale Testdienste zeigen: „SCIM Dummy Target“ und „LDAP Directory“.

Danach binden Administratoren unter „Systeme“ die eigenen Zielsysteme an, siehe Zielsysteme – Überblick. Wie Updates und Sicherungen laufen, beschreibt Updates und Sicherung.

# 11.3 Updates und Sicherung

## Updates

Ein Update ist ein neues Image von Nova. Beim Start bringt Nova das Datenbankschema selbst auf den neuen Stand: Es legt neue Tabellen und Spalten an und führt Datenmigrationen aus. Einen eigenen Migrationsschritt gibt es nicht. Die Migrationen laufen nur vorwärts – für den Weg zurück dient die Sicherung von vor dem Update.

**Docker Compose:** den neuen Programmstand einspielen, dann

```
docker compose -f deploy/docker-compose.yml --env-file deploy/.env up -d --build app
```

Compose baut das Image neu und ersetzt den Container von Nova; die Datenbank läuft weiter. Optional übernimmt ein systemd-Timer das Update: `deploy/autodeploy.sh` prüft alle fünf Minuten einen Git-Zweig und baut bei Änderungen neu. Das Verzeichnis dient dann nur dem Betrieb; lokale Änderungen darin setzt das Skript zurück.

**Kyma:** das neue Image mit neuem Tag bauen und in die Registry laden, das Tag in `deployment.yaml` eintragen, die Datei anwenden und `kubectl rollout status` abwarten. Die Strategie `Recreate` beendet die alte Instanz, bevor die neue startet; Nova ist währenddessen kurz nicht erreichbar.

### Laufende Arbeit bei einem Neustart

- Jobs, die während des Neustarts liefen, markiert Nova beim nächsten Start als fehlgeschlagen.
- Provisionierungsläufe, die der Neustart unterbrochen hat, nimmt Nova beim nächsten Start wieder auf, sofern ihr Ausführungsplan gespeichert ist.
- Termine geplanter Jobs, die in die Ausfallzeit fallen, holt Nova nicht nach; der Job läuft zum nächsten regulären Termin.

## Datenbank sichern

Nova speichert seine Daten in der PostgreSQL-Datenbank – Identitäten, Zuweisungen, Konfiguration, Protokolle und Jobläufe. Im Container selbst legt Nova keine Daten ab. Eine Sicherung ist deshalb eine gewöhnliche PostgreSQL-Sicherung der Nova-Datenbank. Beispiel für Docker Compose; Benutzer und Datenbankname liest der Befehl aus der Umgebung des Datenbank-Containers:

```
DC="docker compose -f deploy/docker-compose.yml --env-file deploy/.env"

# sichern
$DC exec -T db sh -c 'pg_dump -U "$POSTGRES_USER" -Fc "$POSTGRES_DB"' > nova-$(date +%F).dump

# wiederherstellen: Nova anhalten, Sicherung einspielen, Nova starten
$DC stop app
$DC exec -T db sh -c 'pg_restore -U "$POSTGRES_USER" -d "$POSTGRES_DB" --clean --if-exists' < nova-
2026-09-27.dump
$DC start app
```

In Kyma laufen dieselben Befehle im PostgreSQL-Pod, etwa `kubectl -n nova-iam exec postgres-0 -- sh -c 'pg_dump -U "$POSTGRES_USER" -Fc "$POSTGRES_DB"' > nova.dump`. Vor jedem Update ist eine frische Sicherung sinnvoll.

### Konfigurationsexport

Zusätzlich bietet Nova Administratoren über die Schnittstelle `GET /api/config/export` einen Konfigurationsexport als JSON-Datei. Er enthält Zielsysteme mit geschwärzten Geheimnissen, Rollen, Business-Rollen samt Mitgliedern, SoD-Regeln, Genehmigungsabläufe und Einstellungen. Identitäten, Zuweisungen und Protokolle enthält er nicht; die Datenbanksicherung ersetzt er also nicht. Der Import über `POST /api/config/import` – mit `?dry_run=1` als Probelauf – übernimmt derzeit nur die SoD-Regeln.

---

## Den Schlüssel sicher aufbewahren

`NOVA_ENCRYPTION_KEY` liegt nicht in der Datenbank, sondern in `deploy/.env` bzw. im Kubernetes-Secret. Mit diesem Schlüssel verschlüsselt Nova gespeicherte Geheimnisse, etwa Kennwörter und Client-Secrets der Ziel- und Quellsysteme oder das SMTP-Kennwort. Die Datenbanksicherung enthält diese Werte nur verschlüsselt.

- Ohne den Schlüssel – oder mit einem anderen – lassen sich die gespeicherten Geheimnisse nicht entschlüsseln; sie müssen dann neu eingegeben werden.
- Einen Schlüsselwechsel für bestehende Daten bietet Nova nicht. Den Schlüssel einer bestehenden Installation daher nicht austauschen.
- Fehlt die Variable, weicht Nova nicht auf einen temporären Schlüssel aus: Vorgänge, die ein gespeichertes Geheimnis ver- oder entschlüsseln, brechen mit einer Fehlermeldung ab.

> **GETRENNT AUFBEWAHREN**
>
> Den Schlüssel zusammen mit `SECRET_KEY` und dem Datenbankkennwort getrennt von den Datenbanksicherungen aufbewahren, etwa in einem Passwort-Tresor. Eine Sicherung ist nur mit dem passenden Schlüssel vollständig wiederherstellbar.

# 11.4 Überwachung und Jobs

Den Betrieb von Nova verfolgen Administratoren im Bereich „Monitoring“. Dort laufen auch die Hintergrund-Jobs zusammen: Aufgaben wie Importe, Fristen und Wiederholungen, die Nova nach Zeitplan oder auf Knopfdruck ausführt.

## Der Bereich „Monitoring“

| Reiter | Inhalt |
|---|---|
| „Hintergrund-Jobs“ | alle Jobs mit Zeitplan und letztem Lauf; die jüngsten Läufe mit Status, Fortschritt, Dauer und Auslöser; Kennzahlen wie die fehlgeschlagenen Läufe der letzten 24 Stunden |
| „Systemzustand“ | Auslastung von CPU, Arbeitsspeicher und Festplatte; Zustand von Anwendung und Datenbank; Erreichbarkeit des lokalen KI-Servers; Ergebnis der letzten Prüfung je Zielsystem |
| „Anwendungs-Log“ | Warnungen und Fehler der Anwendung, filterbar nach Stufe, Zeitraum und Text |
| „Audit-Log“ | protokollierte Aktionen in Nova |
| „Provisioning-Log“ | Provisionierungsläufe, einzelne Provisionierungsereignisse und Änderungen in den Zielsystemen in einer Liste, filterbar nach Typ und System |
| „Postausgang“ | ausgehende Benachrichtigungen mit Status; hier stellen Administratoren den Versand auf „Aktiv“, „Pausiert“ oder „Aus“ |

„Systemzustand“, „Anwendungs-Log“, „Audit-Log“ und „Postausgang“ sind Administratoren vorbehalten. „Hintergrund-Jobs“, „Systemzustand“ und „Provisioning-Log“ aktualisieren sich alle fünf Sekunden.

## Jobs verwalten

Jobs anlegen, bearbeiten, einplanen, starten, abbrechen und löschen dürfen nur Administratoren; neue Jobs entstehen über „Neuer Job“. Ein Zeitplan legt Wochentage und Uhrzeit fest oder einen einmaligen Termin. „Jetzt starten“ führt einen Job sofort aus. „Abbrechen“ markiert einen laufenden Lauf als abgebrochen; was er bis dahin geschrieben hat, bleibt bestehen. Die Läufe eines Jobs bleiben in der Historie, auch wenn der Job gelöscht wird.

Nova wertet alle Zeitpläne in der Zeitzone Europe/Berlin aus. Diese Zeitzone ist fest eingestellt und hängt nicht von `NOVA_TIMEZONE` ab. Beim Start schreibt Nova die eingeplanten Jobs mit ihrem nächsten Termin in das Protokoll des Containers.

## Voreingestellte Jobs

Nach der Installation sind vier Jobs angelegt, eingeschaltet und eingeplant. Auf der Jobkarte steht der englische Name, darunter der Typ:

| Job | Zeitplan | Aufgabe |
|---|---|---|
| Retry Failed Provisioning „Fehlgeschlagene Provisionierung wiederholen“ | alle 15 Minuten | wiederholt fehlgeschlagene Provisionierungsläufe der letzten 24 Stunden mit wachsendem Abstand (10, 20, 40 Minuten), höchstens dreimal |
| Leave-Date Scan „Austrittsdatum-Scan“ | täglich 02:00 Uhr | führt für aktive Identitäten mit überschrittenem Austrittsdatum die Austrittsroutine aus |
| Activate Pending Assignments „Vorausdatierte Zuweisungen aktivieren“ | täglich 02:30 Uhr | überträgt vorausdatierte Zuweisungen zum Stichtag an Zielsysteme ohne eigene Gültigkeitsdaten |
| Target System Health Poll „Zielsystem-Health-Poll“ | alle 10 Minuten | prüft die Erreichbarkeit der Zielsysteme; fällt ein System neu aus, vermerkt Nova das im „Audit-Log“ |

Gelöschte Standardjobs legt Nova beim nächsten Start wieder an. Wer einen dieser Jobs nicht nutzen will, schaltet ihn aus.

Daneben laufen interne Aufgaben, die nicht in der Jobliste erscheinen: Nova versendet wartende Benachrichtigungen etwa alle 20 Sekunden und räumt täglich auf – im Postausgang abgeschlossene Einträge, die älter als 90 Tage sind (Voreinstellung), dazu abgelaufene Exporte.

## Weitere Jobtypen

Weitere Jobs legen Administratoren bei Bedarf an, unter anderem:

- **Lebenszyklus und HR:** „HR-Nutzer importieren“, „Zukünftige Änderungen anwenden“, „Gelöschte Users bereinigen“ – löscht Identitäten aus dem Papierkorb nach Ablauf der Aufbewahrungsfrist endgültig
- **Berechtigungen:** „Abgelaufene Zuweisungen bereinigen“, „Massen-Rollenzuweisung“, „System-Roles prüfen“
- **Governance:** „SoD-Verstoß-Scan“, „Genehmigungs-Eskalation“, „Rezertifizierungs-Fristerinnerung“, „Agent Review Scan“
- **Zielsysteme:** Importe je Connector, etwa „SAP-Users synchronisieren“, „SAP-Roles importieren“, „LDAP-Gruppen importieren“, „Entra-Gruppen importieren“, „Keycloak-Gruppen importieren“, „SCIM-Gruppen importieren“ und „SAP-OM synchronisieren“

> **ABGELAUFENE ZUWEISUNGEN**
>
> „Abgelaufene Zuweisungen bereinigen“ ist nach der Installation nicht angelegt. Der Job entfernt Zuweisungen, deren Gültigkeit abgelaufen ist. Ist „Zielsysteme automatisch provisionieren“ eingeschaltet („Administration“ → „Provisionierung“ → „Mapping“), stößt er auch den Entzug in den Zielsystemen an. Wer mit Enddaten arbeitet, legt den Job an und plant ihn ein, zum Beispiel täglich.

## Benachrichtigung bei Fehlschlägen

Schlägt ein Joblauf fehl, benachrichtigt Nova die Administratoren per E-Mail und – ist das Zusatzmodul für Microsoft Teams eingeschaltet und eingerichtet – auch in Teams. Je Job, Fehler und Stunde erhält jeder Empfänger höchstens eine Nachricht. Scheitert ein Provisionierungslauf ganz oder teilweise, gehen ebenfalls Nachrichten an die Administratoren, bei Läufen aus einem genehmigten Antrag auch an die antragstellende Person.

Den Ausfall eines Zielsystems meldet Nova nicht per Nachricht; er erscheint im „Audit-Log“ und im „Systemzustand“. Für Nachrichten per E-Mail muss der Versand eingerichtet sein, siehe Voraussetzungen. Was verschickt wurde, zeigt der „Postausgang“.

KAPITEL 12

# Umstieg

## 12.1 Umstieg von SAP IdM

SAP hat angekündigt, die Standardwartung für SAP Identity Management Ende 2027 zu beenden. Für den Umstieg übernimmt Nova den Datenbestand aus einer Exportdatei, und zwar mit der „Migration Workbench“ (Nova System Migration Workbench, NSMW). Eine Verbindung zu SAP IdM braucht Nova dafür nicht, ein festes Exportformat auch nicht: Für jede Datei schreibt eine KI den passenden Parser. Die Workbench steht Administratoren unter „Administration › Migration Workbench“ zur Verfügung.

### Was Nova übernimmt

| In Nova | Erkannt an | Übernommen |
|---|---|---|
| Identitäten | E-Mail-Adresse | Name, Abteilung, Telefon, Standort, Status, Eintrittsdatum, Anrede, Titel, Vorgesetzte; weitere Felder als Zusatzattribute |
| Berechtigungen | ID | Name, Beschreibung, Farbe, Risiko |
| Business-Rollen | ID | Name, Beschreibung, Farbe, enthaltene Berechtigungen |
| Zuweisungen | E-Mail und Rolle | je Zuweisung eine Berechtigung oder eine Business-Rolle, per ID oder Name |

Zusatzattribute zeigt Nova an, sobald sie unter „Administration › Identitätsmanagement › Benutzerdefinierte Felder“ angelegt sind.

Die Workbench schreibt nur in Nova. Sie legt keine Konten in Zielsystemen an und löst keine Provisionierung aus; neu angelegte Berechtigungen sind keinem Zielsystem zugeordnet. Konten, Org-Einheiten, Genehmigungsabläufe und Passwörter übernimmt sie nicht.

### Ablauf

1. **Hochladen.** Über „Neue Migration“ laden Administratoren die Exportdatei hoch: CSV, Excel, JSON, XML oder Text mit fester Spaltenbreite, höchstens 10 MB. Nova speichert sie mit der Migration.
2. **Parser erzeugen.** Im Chat der Workbench beschreiben Administratoren die Datei oder übernehmen den Vorschlag „Lies die Datei ein, mappe automatisch alle Felder.“ Die KI erhält einen Auszug und schreibt einen Parser für die ganze Datei. Nova verlangt dazu eine Erläuterung der Zuordnung samt Tabelle aus Quellspalte und Nova-Feld und zeigt sie im Chat; den Code zeigt „Parser-Skript“. Mehrfachwerte, die SAP IdM mit „|“ getrennt exportiert, soll der Parser laut Auftrag je Wert aufteilen.

3. **Dry-Run.** Sobald die KI einen Parser liefert, wendet Nova ihn auf die ganze Datei an und gleicht jeden Datensatz mit dem aktuellen Bestand ab, ohne Identitäten, Berechtigungen oder Zuweisungen zu ändern; „Dry-Run“ wiederholt das jederzeit. Scheitert der Parser, gibt Nova die Fehlermeldung bis zu zweimal an die KI zurück. Das Ergebnis des letzten Dry-Runs erhält die KI mit der nächsten Nachricht.
4. **Vorschau prüfen.** Die „Dry-Run-Vorschau“ zählt je Objekttyp, was neu angelegt, aktualisiert oder übersprungen wird und was fehlerhaft ist. Ein Klick auf eine Zahl filtert die Liste. Übersprungene und fehlerhafte Zeilen nennen ihren Grund, etwa eine fehlende E-Mail-Adresse, ein ungültiges Datum oder eine unbekannte Rolle; bei zu aktualisierenden Identitäten zeigt die Vorschau die Änderungen je Feld. Korrekturen fordern Administratoren im Chat an oder stellen sie unter „Optionen“ ein.
5. **Ausführen.** „Ausführen“ öffnet „Migration ausführen“ mit den Zahlen je Objekttyp; einzelne Objekttypen lassen sich abwählen. Nova schreibt im Hintergrund in einer einzigen Datenbanktransaktion: Scheitert sie, bleibt der Bestand unverändert.
6. **Abschlussbericht.** „Import abgeschlossen“ zeigt die Zahlen je Objekttyp und unter „Nicht übernommen“ die fehlerhaften Datensätze mit Grund.
7. **Zurückrollen.** Solange die Migration den Status „Aktiviert“ hat, bietet ihre Karte „Zurückrollen“ an. Nova nennt vorher, wie viele Einträge es löscht und wiederherstellt. Anhand eines Journals löscht Nova, was die Migration angelegt hat, samt der Zuweisungen an diesen Objekten, und stellt bei geänderten Datensätzen die gespeicherten Vorher-Werte wieder her. Berechtigungen, die die Migration bereits bestehenden Business-Rollen hinzugefügt hat, bleiben dort erhalten. Das wirkt nur in Nova. Danach lässt sich die Migration erneut ausführen.

## Optionen

- **„Modus“:** Voreingestellt ist „Nur anlegen“ – was es in Nova schon gibt, überspringt Nova. „Anlegen & aktualisieren“ aktualisiert Bestehendes; bei Identitäten überschreiben leere Felder der Datei dabei keine vorhandenen Werte.
- **„Bei Fehler“:** Voreingestellt ist „Zeile überspringen“ – Nova schreibt die fehlerfreien Datensätze. Mit „Migration abbrechen“ schreibt Nova nichts, sobald ein Datensatz fehlerhaft ist.
- Weitere Schalter entfernen Leerzeichen am Anfang und Ende, werten leere Zellen als fehlend, schreiben Rollen-IDs groß und überspringen Duplikate in der Datei; alle sind voreingestellt an. Ein Hinweis zum Datumsformat geht an die KI.

## KI und Daten

Nur das Erzeugen des Parsers braucht eine KI („Lokal“ oder „Cloud“); Dry-Run, Ausführen und Zurückrollen laufen ohne sie. Die KI erhält einen Auszug der Datei, die Chatnachrichten und das Ergebnis des letzten Dry-Runs – im Modus „Cloud“ also auch personenbezogene Daten aus den ersten Zeilen des Exports. Den Parser führt Nova in einem eigenen, eingeschränkten Prozess aus; in die Datenbank schreibt nur Nova selbst, nach seiner Prüfung. Siehe Überblick und Betriebsarten.

## Protokoll und Aufbewahrung

- **Audit-Log:** Hochladen, Änderungen an Name und Optionen, Start und Abschluss der Ausführung mit den Zahlen je Objekttyp und den geschriebenen Datensätzen (bis zu 5.000 einzeln aufgeführt), Zurückrollen mit den zurückgenommenen Datensätzen, Löschen.
- **Provisioning-Log:** Einträge je betroffener Identität, bei der Ausführung wie beim Zurückrollen.
- Jeder Dry-Run und jede Ausführung bleibt als Lauf der Migration gespeichert, ebenso der Chat mit der KI.
- Eine ausgeführte Migration lässt sich erst löschen, wenn sie zurückgerollt ist. Bis zum Löschen bleibt auch die hochgeladene Datei in Nova gespeichert.

Die Schritte nach dem Hochladen lassen sich auch im Admin-Chat anstoßen; Ausführen, Zurückrollen und Löschen verlangen dort eine Bestätigung, siehe Leitplanken der KI.

KAPITEL 13

# Neuigkeiten

## 13.1 Versionshinweise

Nova wird laufend weiterentwickelt. Diese Seite fasst die sichtbaren Änderungen je Monat zusammen, die jüngsten zuerst. Funktionen aus Zusatzmodulen sind gekennzeichnet; Zusatzmodule sind nach der Installation ausgeschaltet und werden unter „Administration“ → „Plugins“ eingeschaltet. Grenzen, die für eine Einführung wichtig sind, stehen unter Bekannte Einschränkungen.

### September 2026

- **Handbuch:** Die erste Ausgabe dieses Handbuchs erscheint, auf Deutsch und Englisch.
- **Admin-Chat:** Der Chat von Nova AI kann fast alle Funktionen der Oberfläche ausführen. Aktionen mit weitreichender Wirkung, etwa Löschen, zeigt er zuerst als Vorschau und führt sie erst nach einer Bestätigung in der nächsten Nachricht aus. Antworten lassen sich als PDF, Excel, CSV, Markdown oder Text herunterladen.
- **Postausgang:** Ein neuer Reiter im „Monitoring“ zeigt die ausgehenden Benachrichtigungen mit Status; der Versand lässt sich auf „Aktiv“, „Pausiert“ oder „Aus“ stellen.
- **Mapping:** Attribute von Quell- und Zielsystemen lassen sich auch über Ausdrücke zuordnen – Verkettung, Wenn-dann-Regeln, Textfunktionen –, mit KI-Vorschlag und Vorschau an einer Beispiel-Identität.
- **HR-Import:** Nova ordnet jede Person in allen Ansichten gleich ein: Eintritt, Wechsel, Aktualisierung, Austritt oder unverändert.
- **SAP:** Eine SAP-Rolle lässt sich vielen Konten auf einmal geben oder entziehen. Kennwörter, die Nova für neue SAP-Konten erzeugt, halten die festen SAP-Regeln zu Länge und Anfangszeichen ein. Korrigiert: SAP-Sammelrollen erscheinen nach einem Abgleich als direkte Zuweisung statt als Business-Rolle.
- **Generisches LDAP:** Sperren und Entsperren laufen über die Kennwortrichtlinie des Verzeichnisses; Kennwort und Gruppenmitgliedschaften bleiben erhalten.
- **Änderungsjournal:** Neben LDAP und Entra ID erfasst das Änderungsjournal jetzt auch Schreibvorgänge in SAP, SCIM und Keycloak.
- **Role Mining und Migration Workbench:** Alle Vorschläge einer Schicht lassen sich gemeinsam annehmen, angewendete Mining-Läufe löschen. Die Migration Workbench übernimmt auf Wunsch nur ausgewählte Objekttypen und nennt im Abschlussbericht die nicht übernommenen Datensätze.

## August 2026

- **Neue Oberfläche:** Die neue Oberfläche ist Standard; die bisherige ist vorerst noch unter `/oldui` erreichbar.
- **Dashboard:** Jede Person passt Größe, Reihenfolge und Sichtbarkeit der Kacheln an. Eine neue Kachel zeigt, welcher Anteil des Berechtigungskatalogs in Business-Rollen enthalten ist.
- **Role Mining:** Nova schlägt aus direkten Zuweisungen Business-Rollen vor, geordnet in Schichten von der Basisrolle bis zur Sonderfunktion. Vorschläge werden geprüft, im Probelauf durchgerechnet und erst dann angewendet. Siehe Role Mining.
- **Attributhistorie:** Im „Änderungsprotokoll“ einer Identität zeigt Nova je Attribut, welcher Wert von wann bis wann galt und woher er kam.
- **Oberfläche:** Verbindungsfehler von Zielsystemen sind direkt am System sichtbar; die Zuweisungsübersicht einer Identität ist nach Systemen gegliedert. Mehrere Designs stehen zur Wahl, und Nova lässt sich als Web-App installieren.
- **KI-Einstellungen:** Zeitlimit und Obergrenze für die Länge von KI-Antworten sind einstellbar.
- **Zusatzmodul OIDC Identity Provider:** Andere Anwendungen können die Anmeldung an Nova per OpenID Connect nutzen („Login with Nova“).

## Juli 2026

- **Keycloak:** Neuer Connector; Gruppen dienen als Berechtigungen. Siehe Keycloak.
- **Rezertifizierung:** Kampagnen mit Arbeitsliste für die Prüfenden und einem Abschluss, bei dem Nova verneinte Berechtigungen auf Wunsch entzieht; das Ergebnis steht als CSV bereit. Siehe Rezertifizierung.
- **Funktionstrennung:** SoD-Regeln zwischen Rollen und Business-Rollen. Beim Antrag warnt Nova vor Konflikten; je nach Einstellung blockiert Nova den Antrag stattdessen oder verlangt einen zusätzlichen Prüfschritt. Als Zusatzmodul prüft Nova auch gegen das Regelwerk von SAP GRC Access Control. Siehe Funktionstrennung (SoD).
- **Genehmigungen:** Vertretungsregel für abwesende Genehmiger; der Job „Genehmigungs-Eskalation“ erinnert an überfällige Schritte und eskaliert an die Administratoren. Siehe Genehmigungsabläufe.
- **Lebenszyklus:** Ein täglicher Job führt bei überschrittenem Austrittsdatum die Austrittsroutine aus. Beim Wiedereintritt legen Administratoren fest, ob frühere Berechtigungen erhalten bleiben. Siehe Eintritt, Wechsel, Austritt.
- **KI-Agenten:** KI-Agenten sind eigene Identitäten mit verantwortlicher Person, Zweck und Prüftermin. Siehe KI-Agenten als Identitäten.
- **Betrieb:** Nova prüft die Zielsysteme regelmäßig auf Erreichbarkeit, wiederholt fehlgeschlagene Provisionierungsläufe automatisch und benachrichtigt die Administratoren, wenn ein Hintergrund-Job fehlschlägt. Siehe Überwachung und Jobs.
- **Nachvollziehbarkeit:** Schreibvorgänge in LDAP und Entra ID erscheinen im „Provisioning-Log“; Administratoren können sie einzeln rückgängig machen. Das gefilterte Audit-Log lässt sich als CSV oder JSON exportieren.

- **Gültigkeiten:** Für Zielsysteme ohne eigene Gültigkeitsdaten hält Nova vorausdatierte Zuweisungen zurück und überträgt sie zum Stichtag.
- **Zusatzmodul Native MFA (TOTP):** zweiter Faktor mit Einmal-Backup-Codes für die Anmeldung mit Kennwort.

## Juni 2026

- **Benachrichtigungen:** Nova verschickt Nachrichten per E-Mail, etwa zu Anträgen und fehlgeschlagener Provisionierung. Mit dem Zusatzmodul für Microsoft Teams lassen sich Anträge auch in Teams genehmigen.
- **Routinen für Eintritt, Wechsel und Austritt:** Eigene Schritte entstehen in einem Editor – mit Bedingungen, berechneten Werten und einer Vorschau, was jeder Schritt in Nova und in den Zielsystemen bewirkt.
- **Anmeldung an Nova:** Kennwort-Historie, optionaler Kennwortablauf und eine Sperre nach wiederholten Fehlversuchen; Nova protokolliert Anmeldeereignisse wie Fehlversuche und Sperren.
- **Governance Analyse:** Nova bewertet einen Anforderungsfragebogen – teils durch Prüfung des aktuellen Datenbestands, teils mit KI – und zeigt das Ergebnis als Scorecard.
- **Migration Workbench:** Exporte aus Altsystemen lassen sich in beliebigem Format einlesen. Die KI schreibt dafür einen Parser, ein Probelauf zeigt vorab, was übernommen würde, und Übernahmen lassen sich zurückrollen.
- **Korrigiert:** Die HR-Übernahme legt für eine Person keine doppelten Identitäten mehr an.

# 13.2 Bekannte Einschränkungen

Diese Seite nennt Grenzen, die für die Planung einer Einführung wichtig sind. Stand: September 2026.

## Betrieb

- **Eine Instanz.** Nova läuft als genau eine Instanz, weil Zeitplaner und laufende Jobs im Prozess liegen. Mehrere Instanzen nebeneinander – zur Lastverteilung oder für Hochverfügbarkeit im Aktiv-aktiv-Betrieb – sind nicht vorgesehen; skaliert wird über Threads. Siehe Voraussetzungen.
- **Zeitzone der Zeitpläne.** Jobs laufen nach der Zeitzone Europe/Berlin; eine andere lässt sich dafür nicht einstellen.
- **Konfiguration übertragen.** Der Konfigurationsexport enthält unter anderem Zielsysteme, Rollen, Business-Rollen und Genehmigungsabläufe; importieren lassen sich derzeit nur die SoD-Regeln. Den Weg von einer Test- in eine Produktivumgebung deckt er damit nur teilweise ab. Siehe Updates und Sicherung.
- **Gültigkeitszeiträume.** Nur SAP speichert Beginn und Ende einer Zuweisung selbst. In den übrigen Zielsystemen setzt Nova die Termine über Hintergrund-Jobs um; sie wirken dort erst mit dem nächsten Lauf. Den Beginn überträgt der tägliche Job „Activate Pending Assignments“. Das Ende übernimmt „Abgelaufene Zuweisungen bereinigen“: Dieser Job ist nach der Installation nicht angelegt und gibt den Entzug nur weiter, wenn „Zielsysteme automatisch provisionieren“ eingeschaltet ist. Siehe Überwachung und Jobs.

## SAP

Nova verbindet sich per RFC und braucht dafür das SAP NetWeaver RFC SDK. Das SDK ist SAP-Software, gehört nicht zum Standard-Image und muss vom Kunden bereitgestellt werden. Ohne SDK lassen sich weder SAP-Zielsysteme noch SAP-Organisationsdaten als Quellsystem noch die SAP-Zusatzmodule nutzen. Siehe SAP.

## Active Directory und LDAP

- **Sperren.** Außer in Active Directory sperrt Nova Konten über das Sperrattribut der Kennwortrichtlinie ( `pwdAccountLockedTime` ). Das wirkt nur, wenn das Verzeichnis eine Kennwortrichtlinie durchsetzt und das Konto, mit dem Nova arbeitet, dieses Attribut schreiben darf.
- **Verschachtelte Gruppen.** Gruppen in Gruppen schreibt Nova nur bei DN-basierten Gruppen; das OpenLDAP-Profil mit `posixGroup` unterstützt keine Verschachtelung. Generische Verzeichnisse brauchen dafür zusätzlich das Attribut `memberOf` im Schema, mit Schreibrecht.

Siehe Active Directory und LDAP.

## Microsoft Entra ID

Bei dynamischen Gruppen ergeben sich die Mitglieder aus Regeln, bei Gruppen, die aus einem lokalen Active Directory synchronisiert werden, aus der Synchronisation. Microsoft Graph lässt Änderungen an diesen Mitgliedschaften nicht zu, Nova kann solche Gruppen also nicht provisionieren. Als Berechtigungen eignen sich Sicherheitsgruppen mit fest zugewiesenen Mitgliedern, die in Entra ID selbst verwaltet werden. Siehe Microsoft Entra ID.

## SCIM

SCIM-Anwendungen setzen den Standard unterschiedlich um. Nova erwartet die Endpunkte unter `‹Basis-URL›/scim/v2`, sucht Konten und Gruppen per Filter auf `userName` und `displayName`, ändert Konten und Mitgliedschaften per `PATCH` und liest Gruppen seitenweise. Zur Anmeldung unterstützt Nova Basic-Authentifizierung und Bearer-Token. Ob eine Anwendung dazu passt, ist je Anbieter zu prüfen. Siehe SCIM.

## Letzte Anmeldung

Wann ein Konto zuletzt benutzt wurde, liest Nova nur, soweit das Zielsystem es liefert:

| Zielsystem | Quelle |
|---|---|
| SAP | Benutzerstamm (`USR02`) |
| Active Directory | `lastLogonTimestamp` bzw. `lastLogon` |
| OpenLDAP | `authTimestamp`, sofern das Verzeichnis es pflegt |
| generisches LDAP | keine Standardquelle |
| Entra ID | Anmeldeaktivität aus Microsoft Graph; braucht die Berechtigung `AuditLog.Read.All` |
| Keycloak | gespeicherte Login-Ereignisse des Realms; speichert der Realm keine, nur aktive Sitzungen |
| SCIM | kein Standardattribut; das unter „Last-Logon-Attribut (SCIM)“ eingetragene Attribut oder `lastLogin` bzw. `lastLogon` |

## Stand der Abnahmen

Die Connectoren werden gegen einen festen Abnahmekatalog mit echten Zielsystemen geprüft. Stand September 2026:

- **SAP** (ABAP) und **generisches LDAP** (geprüft mit ApacheDS) haben den Katalog in zwei vollständigen Runden bestanden; einzelne Teilanforderungen waren dabei ausdrücklich ausgenommen.
- **Microsoft Entra ID:** Die Abnahme ist noch nicht abgeschlossen.

- **Active Directory, Keycloak und SCIM** haben den Katalog noch nicht durchlaufen.