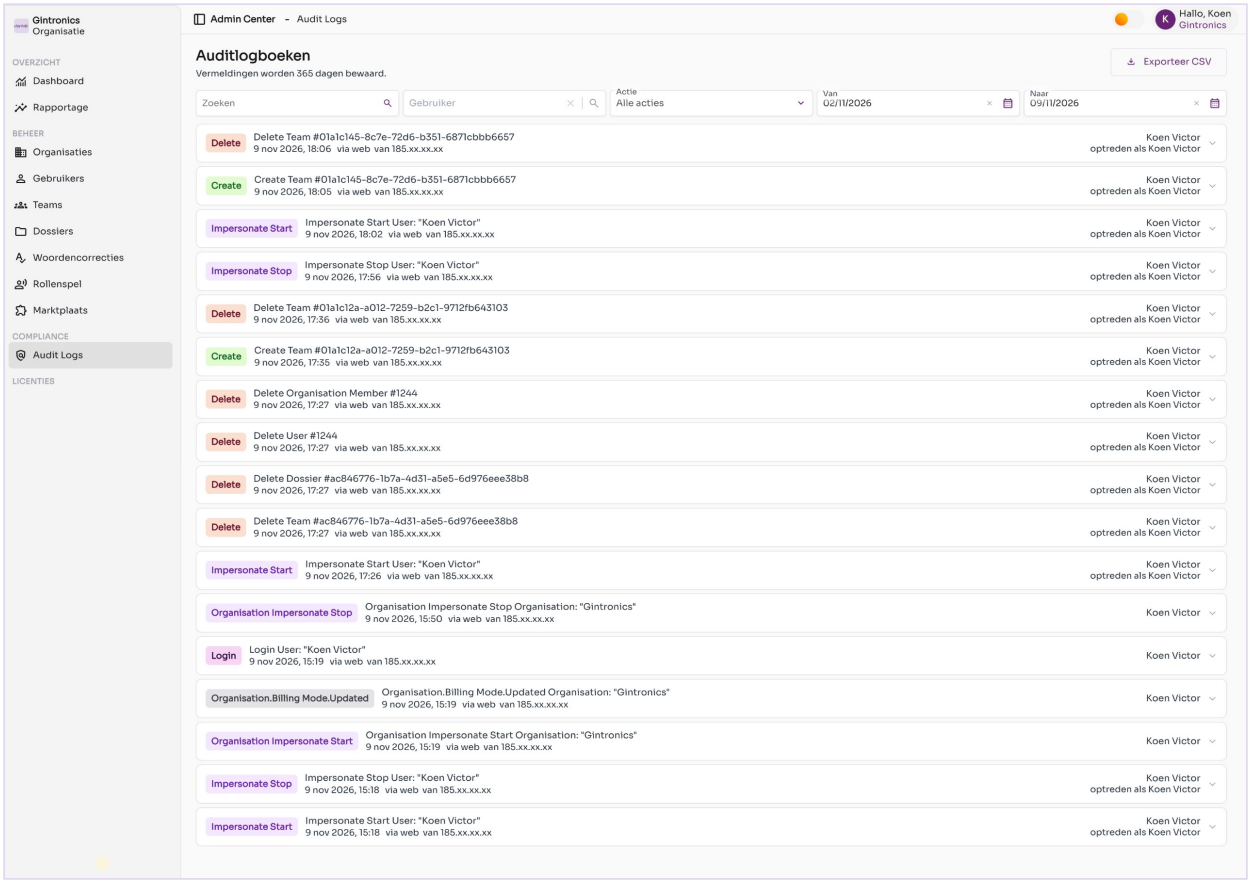
Audit-Logs einsehen

Jede bedeutsame Aktion wird in den Audit-Logs erfasst: wer, was, wann, von welcher IP-Adresse und über welchen Kanal. So kannst du bei einer Kundenanfrage, einer Audit oder einem Sicherheitsvorfall genau nachvollziehen, was passiert ist.

So rufst du die Audit-Logs auf

1. Öffne Audit-Logs
   Klicke im linken Menü auf **Audit-Logs**. Standardmäßig siehst du die Einträge der letzten Woche, neueste zuerst.

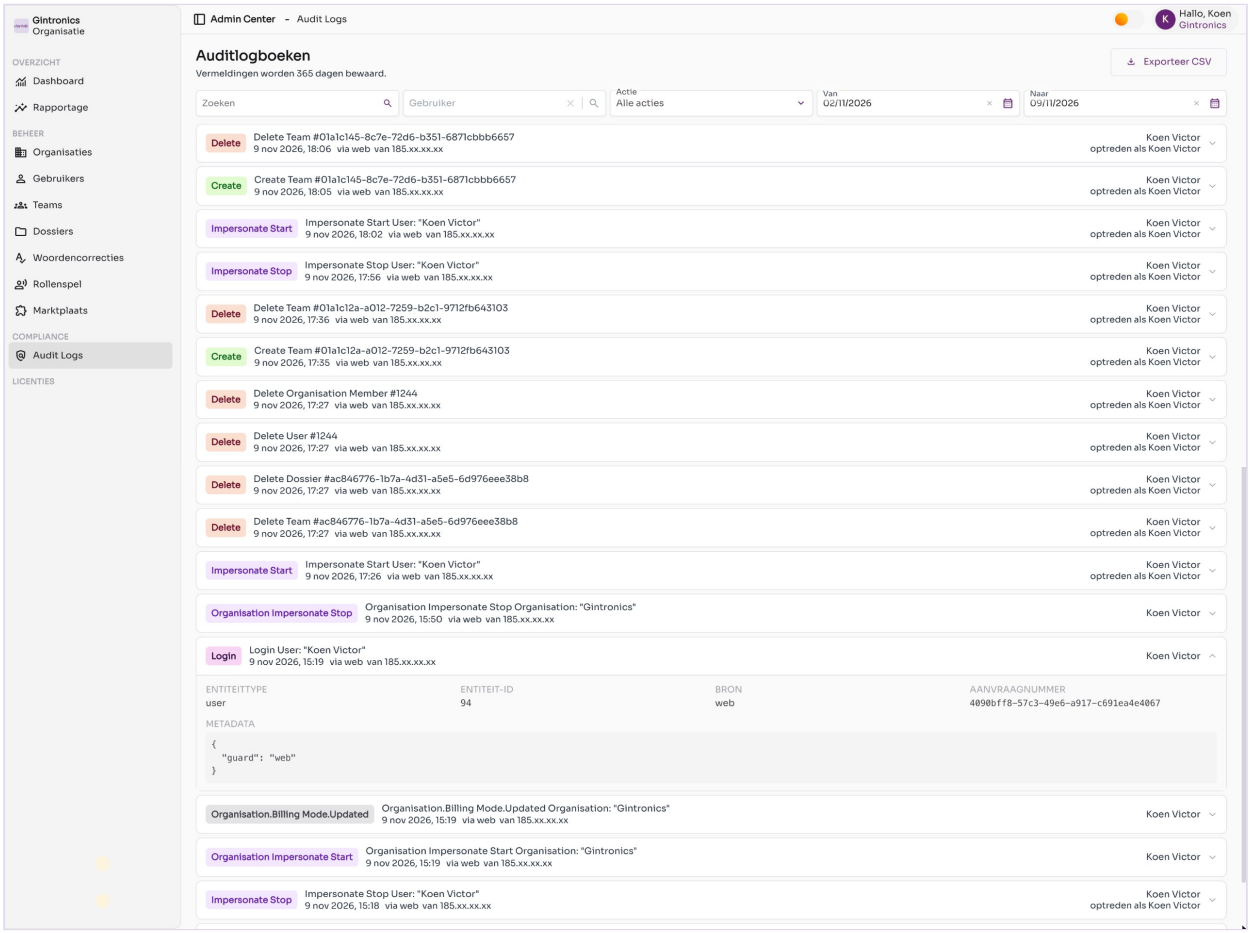


Die Audit-Logs mit den Filtern oben. IP-Adressen sind in diesem Beispiel maskiert.

2. Filtere die Liste
   Verwende die Felder oben: **Suchen** (Freitext), **Benutzer**, **Aktion** und den Zeitraum **Von** und **Bis**. Die Liste wird sofort aktualisiert.

3. Öffne die Details eines Eintrags
   Klicke auf den Pfeil rechts in einer Zeile. Du siehst den *Entitätstyp* (z. B. Benutzer oder Datei), die *Entitäts-ID*, die *Quelle* (Web oder API), die *Anfragenummer* und die *Metadaten* im

JSON-Format.



Ein erweigerter Eintrag mit den technischen Details.

4. Exportiere als CSV
   Klicke rechts oben auf **CSV exportieren**. Du erhältst eine CSV-Datei mit den Einträgen, die deinen Filtern entsprechen. Auch der Export selbst wird als Aktion protokolliert.

Welche Aktionen werden protokolliert

In der Dropdown-Liste *Aktion* filterst du nach einem dieser Typen:

Aktion	Bedeutung
Erstellen, Lesen, Aktualisieren, Löschen	Ein Datensatz (Benutzer, Team, Datei, Mitglied …) wurde erstellt, angesehen, geändert oder gelöscht.
Anmeldung, Abmeldung, Anmeldung fehlgeschlagen	Anmeldungen und fehlgeschlagene Anmeldeversuche.
Passwort ändern	Ein Benutzer hat sein Passwort geändert.

Aktion	Bedeutung
Token erstellen, Token widerrufen	Ein API- oder Connector-Token wurde erstellt oder widerrufen.
Auftreten als Start / Stopp	Ein Administrator hat vorübergehend die Identität eines Benutzers übernommen (Impersonation). In der Zeile wird dann *Auftreten als* mit dem Namen angezeigt.
Organisations-Impersonation gestartet / gestoppt	Ein Administrator arbeitete vorübergehend im Kontext einer anderen Organisation.
Export	Ein Export, z. B. der Audit-Logs selbst.

Wissenswert

- Einträge werden **365 Tage** lang aufbewahrt. Benötigst du eine längere Aufbewahrungsfrist, exportiere regelmäßig in CSV.
- Die Audit-Logs sind schreibgeschützt. Niemand, auch kein Administrator, kann Einträge ändern oder löschen.
- Bei Fragen zu Compliance oder der Verarbeitungsvereinbarung siehe den Abschnitt *Richtlinien & Datenschutz*.