Single Sign-On (SSO) — Kurzüberblick

Einrichtung und Nutzung von SSO im Eventmanager (vibe by egocentric Systems)

Menüpfad (deutsche Oberfläche): Einstellungen → Erweiterungen → Single Sign-On
Dort finden sich die SSO-Liste, Metadaten-Downloads für Plugin SSO und Event Manager SSO sowie der Button HINZUFÜGEN SSO.

1. Was ist SSO und wofür?

Single Sign-On (SSO) ermöglicht die Anmeldung über einen zentralen Identity Provider (IdP) — z. B. die Hochschul- oder Unternehmensanmeldung. Nutzer brauchen keine separaten Zugangsdaten für den Ticketshop bzw. den Eventmanager.

SSO wird für zwei Zielgruppen unterstützt:

- Ticketkäufer (Plugin SSO): Anmeldung im Verkaufs-Plugin / Ticketshop über den IdP.
- Eventmanager-Benutzer (Event Manager SSO): Admin-/Organisations-Benutzer melden sich über SSO am Eventmanager an.

Zusätzlich kann SSO genutzt werden, um Kundenkonten einer eigenen App mit Konten im Ticketsystem zu verknüpfen (Kontoverbindung über die Schnittstelle).

2. Die zwei SSO-Typen

Plugin-SSO und Event-Manager-SSO sind getrennte Setups. Wer beide Varianten braucht, richtet jede einzeln ein und lädt jeweils die passende Metadatei.

Typ	Zielgruppe	Metadaten	Besonderheiten
Plugin SSO	Ticketkäufer im Plugin/Shop	Metadaten „Plugin SSO“ herunterladen	Optional: Anmelde-Beschriftung, Tag-Attribut für spezielle Ticketarten
Event Manager SSO	Admin-/Eventmanager-Benutzer	Metadaten „Event Manager SSO“ herunterladen	Benutzer zuerst anlegen; optional Zwangsanmeldung nur via SSO

3. Einrichtung Schritt für Schritt

Schritt 1 — Metadaten für den IdP bereitstellen

- Im Eventmanager: Einstellungen → Erweiterungen → Single Sign-On öffnen.
- Unter „Download Metadata“ die passende Datei laden: Plugin SSO und/oder Event Manager SSO.
- Diese Metadatei im Identity Provider (IdP) als Service Provider hinterlegen/hochladen.

Schritt 2 — SSO-Verbindung im Eventmanager anlegen

- Button HINZUFÜGEN SSO wählen.
- Passenden SSO Type auswählen (Plugin oder Event Manager).
- Redirect URL aus dem IdP eintragen.
- XML Assertion Attributes hinterlegen — der IdP muss diese Attribute in der SAML-Antwort liefern.
- Optional nur Plugin: Signin Label (Button-Text im Plugin) und Tag Field Attribute Name (freischalten tag-basierter Ticketarten, z. B. Student, Faculty).
- Nutzt der IdP verschlüsselte Assertions: Schalter „Encrypted“ aktivieren.
- Speichern. Der Eintrag erscheint danach in der SSO-Liste (ID, URL, SSO Type).

Schritt 3 — Verbindung testen

- Am angelegten SSO-Eintrag das Aktionsmenü (Zahnrad) öffnen.
- Review Connection starten und mit gültigen IdP-Zugangsdaten anmelden.

• Zurückgelieferte XML-Attribute und Kontodaten prüfen — so erkennt man Mapping-Fehler frühzeitig.

4. Eventmanager-Benutzer für SSO vorbereiten

Bevor sich ein administrativer Benutzer per SSO anmelden kann, muss er im System angelegt sein:

• Bereich Benutzerverwaltung öffnen (Organisation / Veranstalter → Benutzer).
• Benutzer hinzufügen, Stammdaten und Benutzertyp wählen.
• Option für Zwangsanmeldung nur über SSO aktivieren (Force user to login via SSO).
• Als Login-Benutzernamen denselben Wert wie beim IdP verwenden — typischerweise E-Mail oder institutioneller Benutzername.

Login-URL für Eventmanager-SSO

Die SSO-Anmelde-URL für administrative Benutzer findet sich unter Veranstaltungen / Events verwalten, ganz unten im Bereich Important Links (wichtige Links). Den Link SSO Signin an die Admin-Benutzer weitergeben.

5. Technische Grundlagen (SAML)

Die SSO-Anbindung basiert auf dem Austausch von SAML-Metadaten und SAML-Assertions zwischen IdP und dem Eventmanager (als Service Provider).

Begriff	Bedeutung
IdP (Identity Provider)	Externes Anmeldesystem (z. B. Azure AD, Okta, Hochschul-IdP)
SP / Metadaten	Service-Provider-Beschreibung des Eventmanagers; als XML zum Upload im IdP
Redirect URL	Vom IdP gelieferte URL / Endpunkt für den Login-Flow
Assertion Attributes	Attribute in der SAML-Antwort (z. B. E-Mail, Name, Rollen/Tags)
Encrypted Assertions	Option, wenn der IdP Assertions verschlüsselt überträgt
Tag Field Attribute	Nur Plugin: IdP-Attribut steuert Zugang zu tag-spezifischen Ticketarten

6. Checkliste & Tipps

• Plugin- und Event-Manager-SSO getrennt konfigurieren und getrennt testen.
• Metadaten nach IdP-Änderungen (Zertifikat, Endpunkte) ggf. erneut austauschen.
• Attribut-Mapping am IdP muss exakt zu den hinterlegten XML Assertion Attributes passen.
• Admin-Benutzer: Login-Name = IdP-Kennung; sonst schlägt die Zuordnung fehl.
• Nach dem Speichern Verbindung immer über „Review Connection“ verifizieren.
• Hilfe & Kontakt im Eventmanager nutzen, falls IdP-spezifische Fragen auftreten.

7. Überblick der SSO-Oberfläche

Bereich	Inhalt
SSO-Liste	Tabelle mit ID, URL und SSO Type; leer bis der erste Eintrag angelegt wurde
Download Metadata	Zwei Downloads: Plugin SSO und Event Manager SSO
HINZUFÜGEN SSO	Startet die Neuanlage einer SSO-Verbindung

8. Quellen

• Englische Knowledge Base: Artikel „Single Sign On (SSO)“ unter Settings / Single Sign-On
• Deutsche Eventmanager-Oberfläche: Einstellungen → Erweiterungen → Single Sign-On
• Kontext Kontoverbindung: vibe Help „Grundlagen der Schnittstelle-API“

Diese Zusammenfassung ist eine orientierende Kurzfassung. Bei Abweichungen gelten die aktuelle Eventmanager-Oberfläche und die offizielle Dokumentation.