SSO Konfiguration

Sprache: **Deutsch** · English

SSO Konfiguration

> **Single Sign-On per OAuth2/OIDC – Callback-URL, Benutzer-Mapping, Sitzungen und Zwei-Faktor-Authentifizierung.**

HOW-TO | ADMINISTRATOR | STAND: JUL 2026 | GILT FUER NUCLOS 4.2026.X

Auf dieser Seite

- Anmeldung aus Client-Sicht
- Konfiguration
- OIDC: Benutzerermittlung
- Sitzung, Logout & Cluster
- Zwei-Faktor-Authentifizierung (2-FA)
- Verwandte Seiten

Menü *Administration SSO Konfiguration*. Nuclos unterstützt Single Sign-On per **OAuth2** und **OpenID Connect (OIDC)** mit dem Authorization Code Grant.

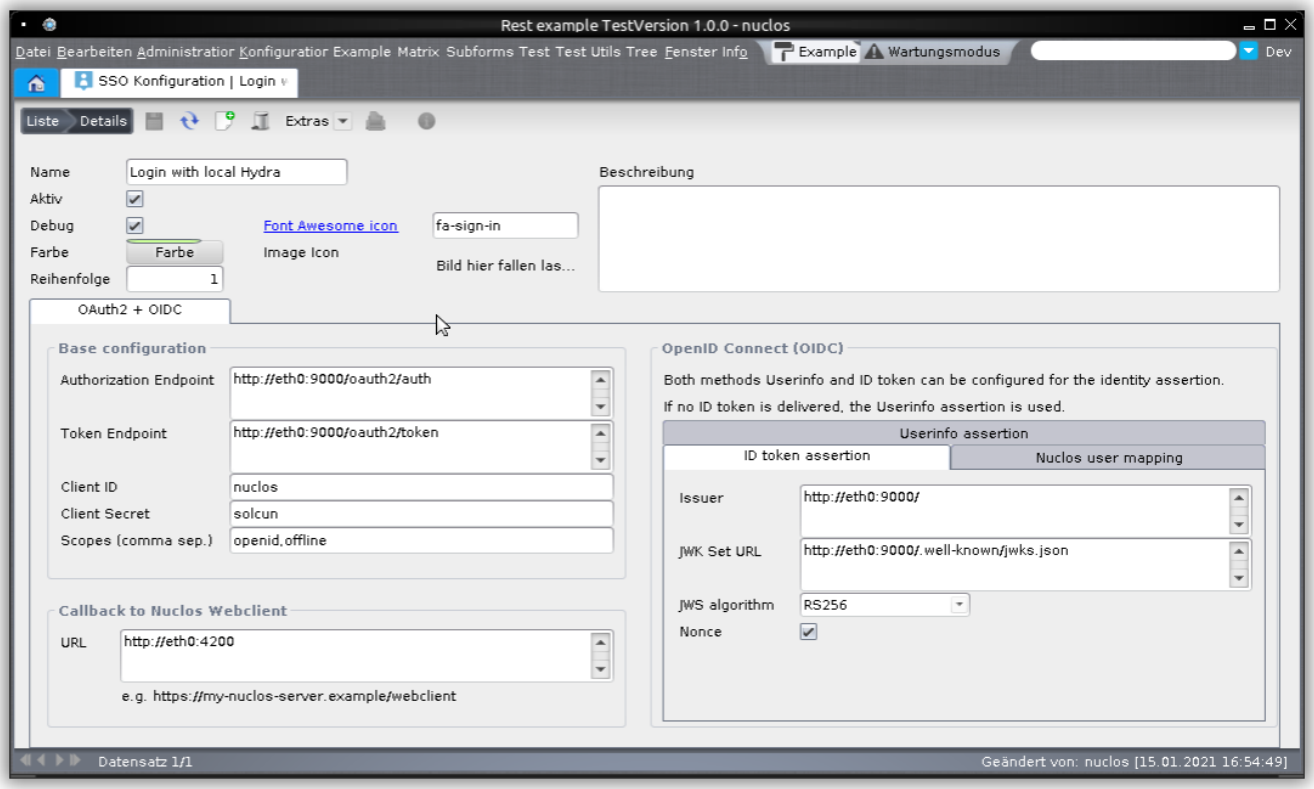
Anmeldung aus Client-Sicht

Aktive Dienste werden beim Start eines Clients als Login-Button angeboten. Der **Rich Client** nutzt dabei den Webclient mit: Der Button öffnet den Browser, führt durch die Authentifizierung und autorisiert damit auch den Rich Client. Der **Webclient** startet den Prozess direkt.

SSO-Login-Buttons beim Client-Start.

Konfiguration

Die verfügbaren SSO-Dienste werden im Menü *Administration* gepflegt.



SSO-Dienste konfigurieren.

Callback-URL zum Webclient

Immer den **Root-Pfad des Webclients** angeben, unter dem ihn ein Browser tatsächlich erreicht (Load Balancer/Reverse Proxy berücksichtigen), z.B. `https://my-nuclos-server.example/webclient`.

OAuth2-Einstellungen

Die nötigen Werte nennt der SSO-Anbieter. Zum Testen kann **Debug** aktiviert werden – die Log-Ausgaben landen im `server.log`.

OIDC: Benutzerermittlung

Die Benutzerinfos kommen entweder aus einem **ID Token** (Reiter *ID token assertion*, bevorzugt) oder vom **Userinfo-Endpunkt** (Reiter *Userinfo assertion*). Aus dem ClaimsSet muss E-Mail oder Benutzername des Nuclos-Benutzers hervorgehen; das passende Attribut wird unter **Nuclos user mapping** hinterlegt (zuerst E-Mail, dann Benutzername).

> **Voraussetzung E-Mail**
>
> Für die Ermittlung über die E-Mail-Adresse muss am Benutzer **Login mit E-Mail-Adresse zulassen** aktiviert sein.

Sitzung, Logout & Cluster

- Refresh Tokens werden regelmäßig erneuert; ohne gültige Erneuerung wird der Benutzer ausgeloggt (Rich Client schließt sich – daher Refresh Tokens bereitstellen).
- Maßgeblich bleibt die `JSESSIONID`; der OAuth2-Dienst wird dadurch geschont.

- Ein Nuclos-Logout wird (noch) nicht an den OAuth2-Dienst weitergeleitet und umgekehrt.
- Im Cluster-Betrieb sind **Sticky Sessions** zwingend (SSO-Tokens liegen nur am jeweiligen Application Server).

Zwei-Faktor-Authentifizierung (2-FA)

- **Acr Values** (ab 4.2022.36): erzwingt über `acr_values` bestimmte Anmeldeverfahren (z.B. 2-FA); der Wert ist systemabhängig.
- **Auth Level** (ab 4.2022.38, Beta): numerischer Vergleichswert – nur bei bekannter Kompatibilität setzen.

Verwandte Seiten

⚙ LDAP Konfiguration

LDAP.

Öffnen

⚙ Benutzer

Benutzer.

Öffnen