

SSO configuration

🌐 Language: [Deutsch](#) · [English](#)

🔧 SSO configuration

Single sign-on via OAuth2/OIDC – callback URL, user mapping, sessions and two-factor authentication.

HOW-TO

ADMINISTRATOR

UPDATED: JUL 2026

APPLIES TO NUCLOS 4.2026.X

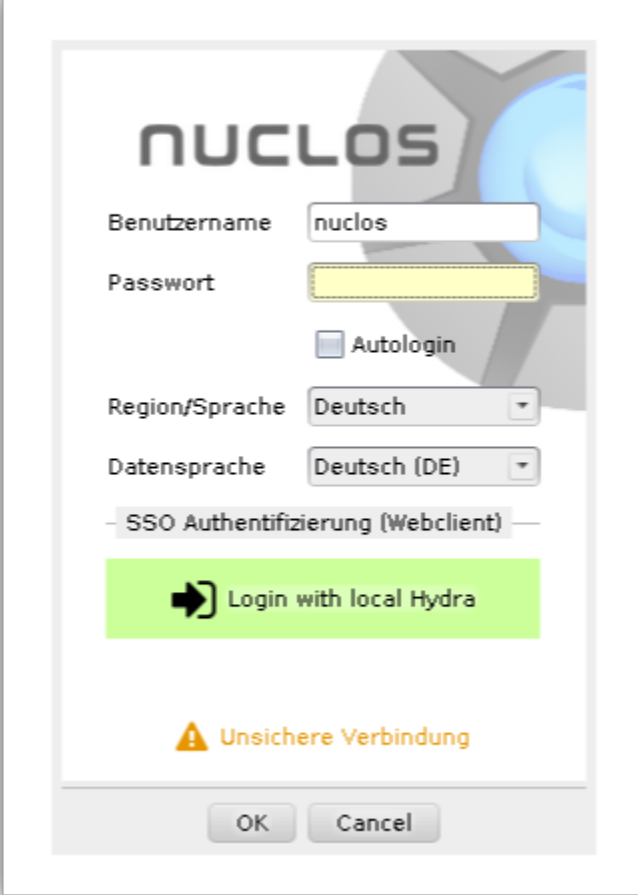
On this page

- [Login from the client's perspective](#)
- [Configuration](#)
- [OIDC: determining the user](#)
- [Session, logout & cluster](#)
- [Two-factor authentication \(2FA\)](#)
- [Related pages](#)

Menu *Administration* SSO configuration. Nuclos supports single sign-on via **OAuth2** and **OpenID Connect (OIDC)** using the [authorization code grant](#).

Login from the client's perspective

Active services are offered as a login button when a client starts. The **rich client** uses the web client: the button opens the browser, guides through authentication and thereby also authorizes the rich client. The **web client** starts the process directly.



The screenshot shows a login dialog box for Nuclos. At the top is the Nuclos logo. Below it are input fields for 'Benutzername' (Username) with the value 'nuclos' and 'Passwort' (Password) which is empty. There is an 'Autologin' checkbox. Below these are dropdown menus for 'Region/Sprache' (Language) set to 'Deutsch' and 'Datensprache' (Data language) set to 'Deutsch (DE)'. A separator line reads '— SSO Authentifizierung (Webclient) —'. Below this is a large green button with a right-pointing arrow icon and the text 'Login with local Hydra'. At the bottom, there is a warning icon (yellow triangle with an exclamation mark) and the text 'Unsichere Verbindung' (Insecure connection). At the very bottom are 'OK' and 'Cancel' buttons.

SSO login buttons at client start.

Configuration

The available SSO services are maintained in the *Administration* menu.

The screenshot shows the 'SSO Konfiguration | Login' window in the Nuclos administration interface. The 'OAuth2 + OIDC' tab is selected. The 'Base configuration' section includes fields for 'Authorization Endpoint' (http://eth0:9000/oauth2/auth), 'Token Endpoint' (http://eth0:9000/oauth2/token), 'Client ID' (nuclos), 'Client Secret' (solcun), and 'Scopes' (openid,offline). The 'Callback to Nuclos Webclient' section has a 'URL' field (http://eth0:4200) with a note 'e.g. https://my-nuclos-server.example/webclient'. The 'OpenID Connect (OIDC)' section has a 'Userinfo assertion' tab selected, showing 'Issuer' (http://eth0:9000/), 'JWK Set URL' (http://eth0:9000/.well-known/jwks.json), 'JWS algorithm' (RS256), and 'Nonce' (checked). The 'ID token assertion' tab is also visible. The interface includes a top menu bar with 'Datei', 'Bearbeiten', 'Administration', 'Konfiguration', 'Example', 'Matrix', 'Subforms', 'Test', 'Test Utils', 'Tree', 'Fenster', 'Info', 'Example', 'Wartungsmodus', and 'Dev'. A status bar at the bottom indicates 'Datensatz 1/1' and 'Geändert von: nuclos [15.01.2021 16:54:49]'.

Configuring SSO services.

Callback URL to the web client

Always specify the **root path of the web client** at which a browser actually reaches it (consider load balancer/reverse proxy), e.g. `https://my-nuclos-server.example/webclient`.

OAuth2 settings

The required values are provided by your SSO provider. For testing, enable **debug** – log output goes to `server.log`.

OIDC: determining the user

User info comes either from an **ID token** (tab *ID token assertion*, preferred) or from the **userinfo endpoint** (tab *Userinfo assertion*). The ClaimsSet must yield the e-mail or user name of the Nuclos user; the matching attribute is configured under **Nuclos user mapping** (e-mail first, then user name).



E-mail prerequisite

For lookup via e-mail address the user must have **allow login with e-mail address** enabled.

Session, logout & cluster

- Refresh tokens are renewed regularly; without valid renewal the user is logged out (the rich client closes – so provide refresh tokens).
- The JSESSIONID remains decisive; this spares the OAuth2 service.
- A Nuclos logout is (not yet) forwarded to the OAuth2 service and vice versa.
- In [cluster operation](#) **sticky sessions** are mandatory (SSO tokens reside only on the respective application server).

Two-factor authentication (2FA)

- **Acr values** (from 4.2022.36): enforces certain login methods via `acr_values` (e.g. 2FA); the value is system-specific.
- **Auth level** (from 4.2022.38, beta): numeric comparison value – only set with known compatibility.

Related pages

LDAP configuration

LDAP.

[Open](#)

User

Users.

[Open](#)