

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

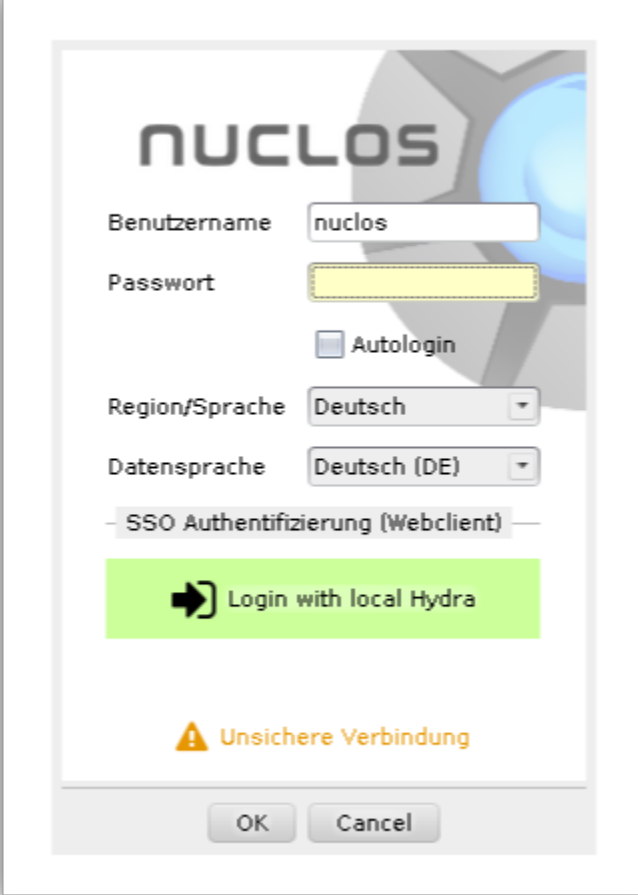
On this page

- [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. The dialog has a title bar and a main content area. At the top, the Nuclos logo is displayed. Below the logo, there are input fields for 'Benutzername' (Username) and 'Passwort' (Password). The 'Benutzername' field contains the text 'nuclos'. Below the password field, there is a checkbox labeled 'Autologin'. Below the checkbox, there are two dropdown menus: 'Region/Sprache' (Region/Language) and 'Datensprache' (Data Language). Both dropdowns are currently set to 'Deutsch'. Below the dropdowns, there is a section header 'SSO Authentifizierung (Webclient)'. Under this header, there is a large green button with a right-pointing arrow and the text 'Login with local Hydra'. At the bottom of the dialog, there is a warning icon (a yellow triangle with an exclamation mark) and the text 'Unsichere Verbindung' (Insecure connection). At the very bottom, there are two buttons: 'OK' and 'Cancel'.

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 active, displaying configuration fields for a service named 'Login with local Hydra'. The 'Aktiv' checkbox is checked, and the 'Debug' checkbox is also checked. The 'Farbe' (color) is set to 'Farbe' and the 'Reihenfolge' (order) is 1. The 'Beschreibung' (description) field contains 'fa-sign-in'. The 'Image Icon' field is empty, with a note 'Bild hier fallen las...'. The 'Base configuration' section includes 'Authorization Endpoint' (http://eth0:9000/oauth2/auth), 'Token Endpoint' (http://eth0:9000/oauth2/token), 'Client ID' (nuclos), 'Client Secret' (solcun), and 'Scopes (comma sep.)' (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 includes a note about Userinfo and ID token assertion, and a 'Userinfo assertion' tab. The 'ID token assertion' tab is selected, showing 'Issuer' (http://eth0:9000/), 'JWK Set URL' (http://eth0:9000/.well-known/jwks.json), 'JWS algorithm' (RS256), and 'Nonce' (checked). The 'Nuclos user mapping' tab is also visible.

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](#)