

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

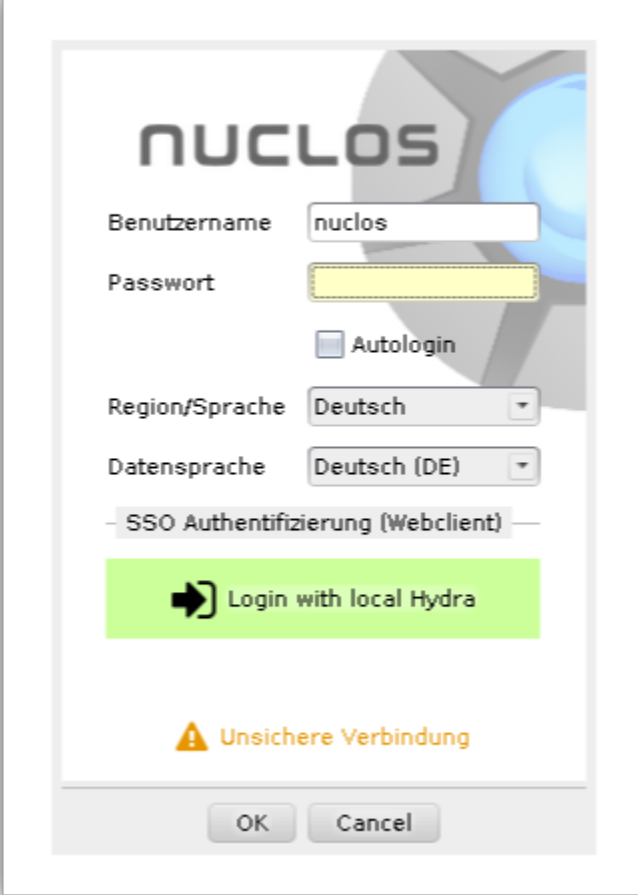
Auf dieser Seite

- [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.



The screenshot shows a login dialog box for NUCLOS. At the top, the NUCLOS logo is displayed. Below it, there are input fields for 'Benutzername' (Username) with the value 'nuclos' and 'Passwort' (Password) which is currently empty. A checkbox for 'Autologin' is present and unchecked. Below these are two dropdown menus: 'Region/Sprache' set to 'Deutsch' and 'Datensprache' set to 'Deutsch (DE)'. A section header 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 of the dialog, there is a warning icon (a yellow triangle with an exclamation mark) followed by the text 'Unsichere Verbindung' (Insecure connection). At the very bottom are 'OK' and 'Cancel' buttons.

Konfiguration

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

The screenshot shows the 'SSO Konfiguration | Login' window in the Nuclos application. The 'OAuth2 + OIDC' tab is active, displaying configuration fields for a service named 'Login with local Hydra'. 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). The 'OpenID Connect (OIDC)' section shows 'Userinfo assertion' and 'ID token assertion' tabs, with the 'ID token assertion' tab selected. It includes fields for 'Issuer' (http://eth0:9000/), 'JWK Set URL' (http://eth0:9000/.well-known/jwks.json), 'JWS algorithm' (RS256), and a checked 'Nonce' checkbox. The status bar at the bottom indicates 'Geändert von: nuclos [15.01.2021 16:54:49]'.

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](#)