External Authenticators

Single sign-on (SSO) is a element of access control of multiple related, yet independent, software systems. A user logs in with a single ID and password to gain access to a system without using different usernames or passwords, or in some configurations seamlessly sign on at each system.

Benefits of using single sign-on include:

Mitigate risk for access to 3rd-party sites (user passwords not stored or managed externally)
Reduce password fatigue from different user name and password combinations
Reduce time spent re-entering passwords for the same identity
Reduce IT costs due to lower number of IT help desk calls about passwords

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

CILOGON

A hub administrator must register at http://cilogon.org/oauth2/register

Enter a Client Name.
Enter a Contact Email Address.
Enter a home URL (the URL of your hub - hubzero.org, for example).
Callback URLS should be:

```
**<hostname> should be replaced with the HUB URL.  If you have more th
an one hub instance, include a redirect URL set for each host that you
 will wish to use CiLogon.

https://<hostname>/index.php?option=com_users&task=user.link&authentic
ator=cilogon
https://<hostname>/index.php?option=com_users&task=user.login&authenti
cator=cilogon
https://<hostname>/administrator/index.php?option=com_login&task=login
&authenticator=cilogon
```

Select all SCOPES (email, edu.., openid, profile, org.cilogon...).

Leave blank - Refresh Token Lifetime.
Leave blank - Issuer.

CiLogon will process the registration and if approved a client id and client secret will be provided and must be added to the "Authenticator - CILogon" plugin in the Adminstrator Interface (/administrator) to enable to plugin. Once enabled, users may log into your hub via credentials provided by CiLogon.