



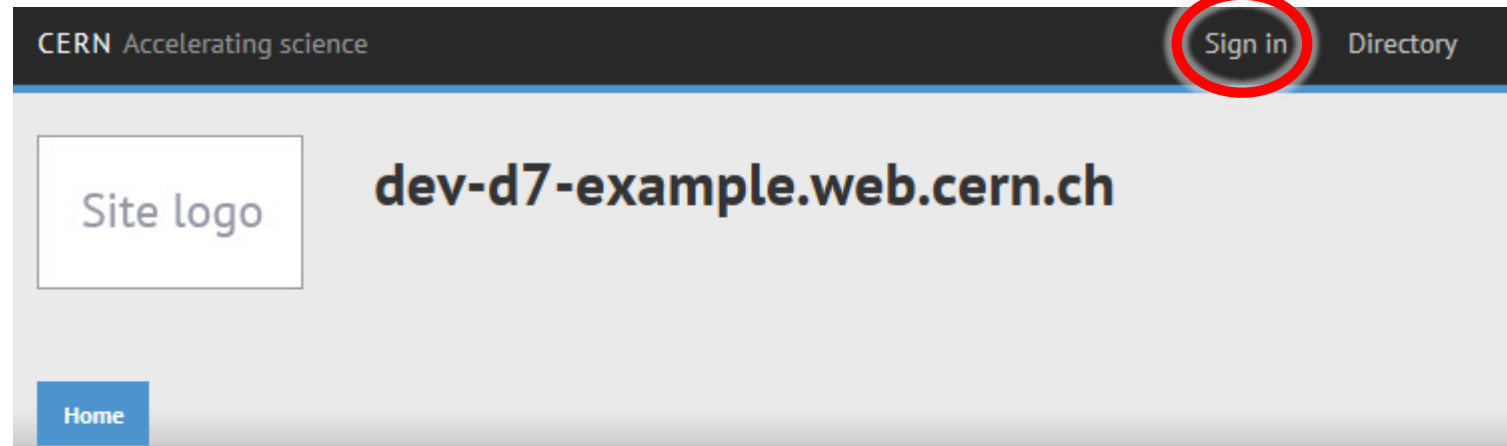
SSO

Romanos Dodopoulos

SSO - Drupal 7

- Single Sign-On Service at CERN
 - Web-based applications authenticate users
- No Drupal out of the box solution
- Shibboleth authentication module

SSO - Drupal 7



Welcome to dev-d7- example.web.cern.ch

No front page content has been created yet.

SSO - Drupal 7

https://login.cern.ch/ads/lts/?wa=wsignin1.0&wreply=http:

CERN

CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your CERN account


Reminder: you have agreed to comply with the CERN computing rules


Use credentials

Username or Email address Password

Remember Username or Email Address [Need password help ?](#)

Use one-click authentication

 [Sign in using your current Windows/Kerberos credentials \[autologon\]](#)
Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).

 [Sign in using your Certificate \[autologon\]](#)
Use a EuGridPMA trusted certificate. Don't forget to first map your Certificate to your CERN Account.

Use strong two factor authentication [\[show\]](#)

SSO - Drupal 8

SSO - Drupal 8

- No Shibboleth authentication module
- Community supports and invests in alternatives
- simpleSAMLphp authentication module
 - Transition transparent for most users

Difference in UI

SSO - Difference in UI

Configuration +

Home » Administration

Hide descriptions

PEOPLE

- Account settings
Configure default behavior of users, including registration requirements, e-mails, fields, and user pictures.
- CERN Profiles
Configure CERN Profiles modules.
- Shibboleth settings**
Settings of the Shibboleth authentication module
- IP address blocking
Manage blocked IP addresses.

CONTENT AUTHORIZING

- CKEditor

Configuration ☆

Home » Administration

Hide descriptions

PEOPLE

- Account settings
Configure default user account settings, including fields, registration requirements, and email messages.
- SimpleSAMLphp Auth Settings**
Control the various settings of the SimpleSAMLphp authentication module

CONTENT AUTHORIZING

- Text formats and editors
Select and configure text editors, and how content is filtered when displayed.

SSO - Difference in UI

Shibboleth settings  GENERAL SETTINGS SHIBBOLETH GROUP RULES ADVANCED

[Home](#) » [Administration](#) » [Configuration](#) » [People](#) » [Shibboleth settings](#)

ATTRIBUTE	REGEXP	ROLES
ADFS_GROUP	^drupal-admins\$	administrator
ADFS_GROUP	^drupal-admins-dev-d7-example-web-cern-ch\$	administrator
ADFS_IDENTITYCLASS	^CERN Registered\$	CERN Registered
ADFS_IDENTITYCLASS	^CERN Shared\$	CERN Shared
ADFS_IDENTITYCLASS	^HEP Trusted\$	HEP Trusted
ADFS_IDENTITYCLASS	^Verified External\$	Verified External
ADFS_IDENTITYCLASS	^Unverified External\$	Unverified External

SSO - Difference in UI

Shibboleth settings

GENERAL SETTINGS

SHIBBOLETH GROUP RULES

Basic settings

Local authentication

User info and syncing

Home » Administration » Configuration » People

ATTRIBUTE	REGEXP
ADFS_GROUP	^drupal-adm
ADFS_GROUP	^drupal-adm
ADFS_IDENTITYCLASS	^CERN Regist
ADFS_IDENTITYCLASS	^CERN Share
ADFS_IDENTITYCLASS	^HEP Trusted
ADFS_IDENTITYCLASS	^Verified Ext
ADFS_IDENTITYCLASS	^Unverified E

Home » Administration » Configuration » People » SimpleSAMLphp Auth Settings

USER INFO AND SYNCING

SimpleSAMLphp attribute to be used as unique identifier for the user *

http://schemas.xmlsoap.org/claims/UPN

Example: *eduPersonPrincipalName* or *eduPersonTargetedID*
If the attribute is multivalued, the first value will be used.

SimpleSAMLphp attribute to be used as username for the user *

login

Example: *eduPersonPrincipalName* or *displayName*
If the attribute is multivalued, the first value will be used.
WARNING: Drupal requires usernames to be unique!

Synchronize user name on every login

Check if user name should be synchronized every time a user logs in.

SimpleSAMLphp attribute to be used as email address for the user

email

Example: *mail*
If the user attribute is multivalued, the first value will be used.

Synchronize email address on every login

Check if email address should be synchronized every time a user logs in.

Automatic role population from simpleSAMLphp attributes

cern_registered:identityclass,=,CERN Registered|cern_shared:identityclass,=,CERN Sha
Trusted|verified_external:identityclass,=,Verified External|unverified_external:identityc

SSO - Difference in UI

Shibboleth settings

GENERAL SETTINGS

SHIBBOLETH GROUP RULES

ADVANCED

Home » Administration » Configuration » People » Shibboleth settings

ATTRIBUTE	REGEXP	ROLES
ADFS_GROUP	^drupal-admins\$	administrator
ADFS_GROUP	^drupal-admins-dev-d7-example-web-cern-ch\$	administrator

ADFS_IDE
ADFS_IDE
ADFS_IDE
ADFS_IDE
ADFS_IDE

Automatic role population from simpleSAMLphp attributes

```
administrator:egroups,=,drupal-admins-dev-d8-example-web-cern-ch|  
administrator:egroups,=,drupal-admins|  
cern_registered:identityclass,=,CERN Registered|  
cern_shared:identityclass,=,CERN Shared|  
hep_trusted:identityclass,=,HEP Trusted|
```

A pipe separated list of rules. Each rule consists of a Drupal role id, a SimpleSAML attribute name, an operation and a value to match. *e.g. role_id1:attribute_name,operation,value|role_id2:attribute_name2,operation,value... etc*

Each operation may be either "@", "@=" or "~=".

- "=" requires the value exactly matches the attribute;
- "@=" requires the portion after a "@" in the attribute to match the value;
- "~=" allows the value to match any part of any element in the attribute array.

For instance:

```
staff:eduPersonPrincipalName,@=,uninett.no;affiliation,=,employee|admin:mail,=,andreas@uninett.no
```

