CAS and SAML Authentication

CAS/SAML Authentication

Introduction

This plugin allows user authentication using CAS 2.0 protocol. User attributes can be pulled using SAML 1.0 protocol.

> Your DSpace and CAS server clocks need to be synchronised using the same time server as the CAS protocol is very sensitive about time differences!

Enabling CAS/SAML Authentication

To enable CAS/SAML Authentication, you must ensure the `org.dspace.authenticate.CASAuthentication` class is listed as one of the AuthenticationMethods in the following configuration:

Configuration File:	**`[dspace]/config/modules/authentication.cfg`**
Property:	`plugin.sequence.org.dspace.authenticate.AuthenticationMethod`
Example Value:	`plugin.sequence.org.dspace.authenticate.AuthenticationMethod = \` `org.dspace.authenticate.CASAuthentication`

Configuring CAS/SAML Authentication

If CAS/SAML is enabled, then new users will be able to register by being forwarded to external authentication site without being sent the registration token. If users do not have a username and password, then they can still register and login with just their email address the same way they do now.

If you want to give any special privileges to CAS users, create a stackable authentication method to automatically put people who have a netid into a special group. You might also want to give certain email addresses special privileges. Refer to the Custom Authentication Code section below for more information about how to do this.

Here is an explanation of each of the different CAS/SAML configuration parameters:

Configuration File:	**`[dspace]/config/modules/authentication-cas.cfg`**
Property:	`cas.server.url`
Example Value:	`cas.server.url = https://cas.server/login`
Informational Note:	Full url of CAS login address that users will be redirected to upon login attempt. Only used when authenticating using pure CAS 2.0 protocol (`cas.use.saml` = false).
Property:	`cas.validate.url`
Example Value:	`cas.validate.url = https://cas.server/serviceValidate`
Informational Note:	Full url of CAS ticket validation service. This address will be called by DSpace to verify validity of users token and whether the DSpace instance has permissions to authenticate users against CAS server. Only used when authenticating using pure CAS 2.0 protocol (`cas.use.saml` = false).
Property:	`cas.logout.url`
Example Value:	`cas.logout.url = https://cas.server/logout`
Informational Note:	Full url of CAS server logout service. The user will be redirected to this address when trying to logout from DSpace. Only used when authenticating using pure CAS 2.0 protocol (`cas.use.saml` = false).
Property:	`cas.use.saml`
Example Value:	`cas.use.saml` = true
Explanation:	This setting will enable usage of SAML 1.0 protocol. When this is enabled user name, surname and email address will be copied from CAS server using SAML 1.0 protocol.
Property:	`cas.url.prefix`
Example Value:	`cas.url.prefix = https://cas.server`

Informational Note:	The basic url (protocol and domain) of CAS server. Only used when SAM 1.0 is enabled (`cas.use.saml` = true).
Property:	`cas.saml.firstName`
Example Value:	`cas.saml.firstName = firstName`
Informational Note:	SAML attribute name holding user first name. Only used when SAM 1.0 is enabled (`cas.use.saml` = true).
Property:	`cas.saml.lastName`
Example Value:	`cas.saml.lastName = lastName`
Informational Note:	SAML attribute name holding user last name. Only used when SAM 1.0 is enabled (`cas.use.saml` = true).
Property:	`cas.saml.mail`
Example Value:	`cas.saml.mail = mail`
Informational Note:	SAML attribute name holding user email. When a list is returned the first address is being used. Only used when SAM 1.0 is enabled (`cas.use.saml` = true).
Property:	`webui.cas.autoregister`
Example Value:	`webui.cas.autoregister = true`
Informational Note:	This property controls whether user can auto register upon first login. If set to false, no new users will be allowed to create account on first authentication.
Property:	`webui.cas.enable`
Example Value:	`webui.cas.enable = false`
Informational Note:	This property controls whether user can edit his or hers username on the EPerson page. If set to true the user can edit the CAS username.

Enabling user attribute lookup

By default, when using pure CAS 2.0 protocol the user attributes will not be read from the server.They will be set as follows:

1. first name will be set as "University"
2. last name will be set as "User"
3. mail will be set as equal to netid.

You have to pull the appropriate values on your own using LDAP or other means of accessing CAS user attributes.

If you have a SAML 1.0 compatible authentication server you can read user attributes during authentication automatically. For that you need to enable cas.use.saml property in the configuration file, provide general CAS server prefix instead of direct links to login, logout and validation services and provide attribute names holding first name, last name and email (usually you can leave default settings) as described in Configuring CAS/SAML Authentication. After that user info will be read from the server.