Using an external authentication system

> VIVO can be configured to work with an external authentication system like Shibboleth or CUWebAuth.

In order to effectively use an external authentication system, VIVO must be accessible only through an Apache HTTP server. The Apache server will be configured to invoke the external authentication system. When the user completes the authentication, the Apache server will pass a network ID to VIVO, to identify the user.

If VIVO has an account for that user, the user will be logged in with the privileges of that account. In the absence of an account, VIVO will try to find a page associated with the user. If such a page is found, the user can log in to edit his own profile information.

Configuring the Apache server

Your institution will provide you with instructions for setting up the external authentication system. The Apache server must be configured to secure a page in VIVO. When a user reaches this secured page, the Apache server will invoke the external authentication system.

For VIVO, this secured page is named: `/loginExternalAuthReturn`

When your instructions call for the location of the secured page, this is the value you should use.

Configuring VIVO

To enable external authentication, VIVO requires two values in the `runtime.properties` file.

Property name	`externalAuth.netIdHeaderName`
Description	The name of the HTTP header that will hold the external user's network ID. When a user completes the authentication process, the Apache server will put the user's network ID into one of the headers of the HTTP request. The instructions from your institution should tell you which header is used for this purpose.
Default value	NONE
Example value	`remote_userID`

Property name	`selfEditing.idMatchingProperty`
Description	Associating a User with a profile page. VIVO will try to associate the user with a profile page, so the user may edit his own profile data. VIVO will search the data model for a person with a property that matches the User's network ID (the value of the property must be either a String literal or an untyped literal). You need to tell VIVO what property should be used for matching. This property is also mentioned in the insructions for A simple installation, because it can also be useful for sites that do not use external authentication.
Default value	NONE
Example value	`http://vivo.mydomain.edu/ns#networkId`

Finally, you will need to provide text for the Login button.

To start the authentication process, the user will click on a button in the VIVO login form. You need to tell VIVO what text should appear in that button. In your theme, add a line to the `all.properties` file, like this one:

```
external_login_text = [the text for your login button]
```

For example:

```
external_login_text = Log in using BearCat Shibboleth
```

The VIVO login form will display a button labelled "Log in using BearCat Shibboleth".

If your site supports additional languages, add lines to the corresponding files. For example, `all_es.properties` might contain this line:

```
external_login_text = Entrar usando Shibboleth GatoOso
```

More information

You can find more technical details about the Interface to external authentication systems.

Also, it may help to know How are User Accounts associated with Profile pages?