Configuring SirsiDynix as an authentication provider for OpenAthens

Path to function: ***Management > Connections > Add > SirsiDynix***

OpenAthens can connect to your SirsiDynix system using its Symphony API so that you do not have to issue personal accounts for your users (you will still need your OpenAthens administrator account though). You should use at least two factor authentication for your local users (e.g. username and password, barcode and pin).

Preparation

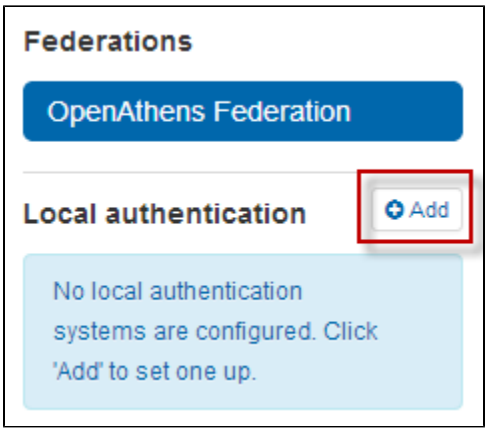
Before you start you will need:

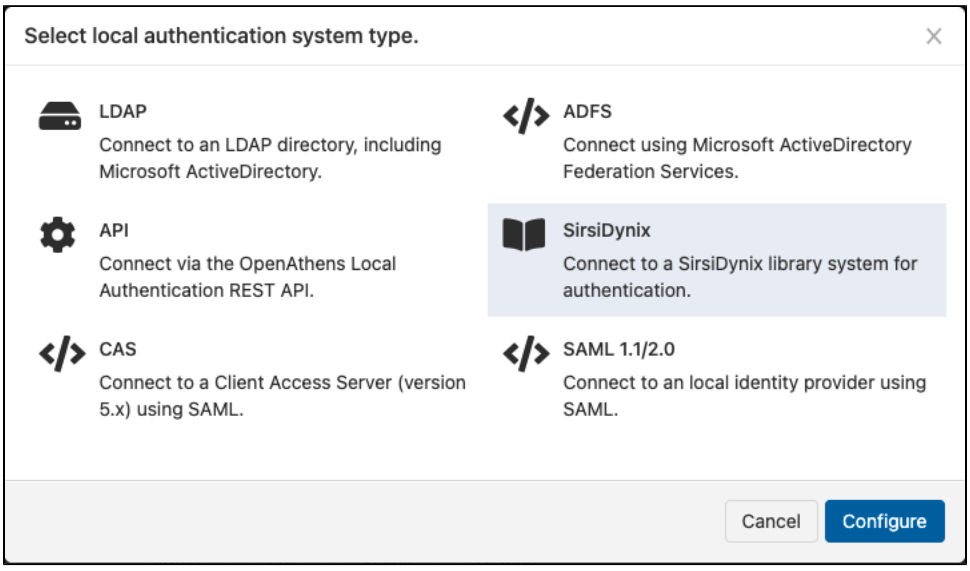
- Access to the SirsiDynix Symphony API.
- A login point that is accessible from everywhere your users can be, e.g. outside of your network.
- Access to the OpenAthens administration area at the domain level
- If the Sirsi API server is using a self-signed certificate for https, you will also need a copy of it in pem format

Add the connection

In the administration interface as the domain administrator go to ***Management > Connections***

1. Click the add button on the left and select SirsiDynix from the chooser



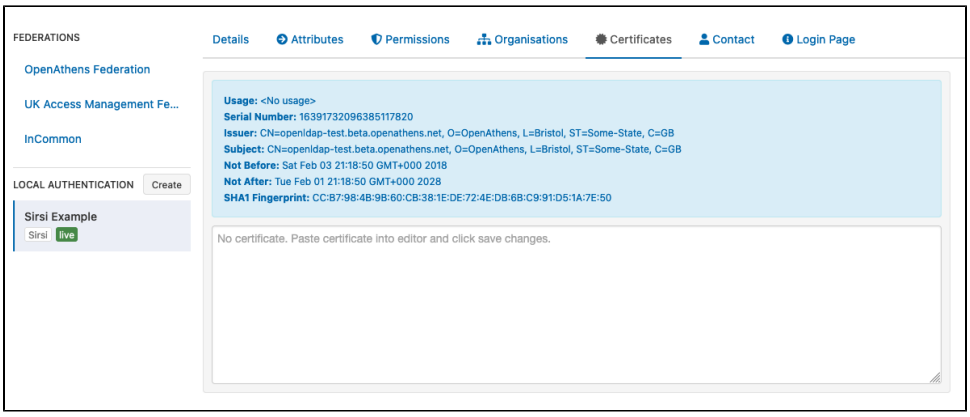


2. Enter the details and click add at the bottom.
    a. See the fields section below for an explanation of what each is for

3. If your connection requires a certificate, it can be added on the certificate tab. Paste in the contents of the certificate file which should look similar to this:

```
-----BEGIN CERTIFICATE-----
IIIDlTCCAn2gLwIBAgIQJuhFWFFr7ZxCMn6ymkjQtjANBgkqhkiG9w0BAQUFADBd
sRMwEQYKCIAZImiYLGQBGRYDbmV0MRowGAYKCZImiZPyLGQBGRYKb3BlbmF0aGVu
HzESMBAGCLnmSJoN8ixkARkWAmFkMRYwFAYDVQQDEw1hZC1PQS1BREZTLUNBMB4X
dTE1MDExNIdEwNTENFoXDTI1MDExNjExMDA1OVowXTETMBEGCgmSJomT8ixkARkW
N25ldDEaMKIgGCgmSomT8ixkARkWCm9wZW5hdGhlbnMxEjAQBgoJkiaJk/IsZAEZ
EgJhZDEWMBcQGA1UAAMNYWQtT0EtQURGUy1DQTCCASIwDQYJKoZIhvcNAQEBBQAD
SgEPADCCAIAoCggEAMNkzzh4fgdFtCHzhbTSmSrEx846+wRmdG1FHKhSkXkmbV1U
8S/TtRJ6zGnPvb18AC/IGC7msrvSsZc19Jfe5nJVL2kSCAWDLjsIwJKUb9gep3na
R846gv83QBnm0/YJpyT2DcAVcvCQAI2+MjoLFET43v9haREjbGa7JFDdnjsbjqyZ
EODlalLKOUoLicsGmTKFSI4UX3fzAPhf85lsod87w4Er05MdxQifVWpaDcPUh1BJ
BK92Sy+oITTEqQzL4Vtd/1O4HuyOSw5wOBJLGP4PTwbqPdrpotvDPg+MLN/RHc54
vUEJcl1mTTLLBmMYiVJKXMxT1CYmYWM9ibA7JB8CAwEAAaNRME8wCwYDVR0PBAQD
SgGGMA8GASiUdEwE/wQFMAMBAf8wHQYDVR0OBBYEFGWVTvqweerzee/JFMbuTYzi
To/VMBAGCSEsGAQQgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQDGIvljYiX1
wmneie6HnOmkNhQVuvxCSOpYZT3uezq/8/ZrhR5UrkWfYdmfhcmNgmndcMr3GSCt
DJdjxT9c0qUK+PC2IjZtO3tVvuuZY1cf5E6A5TArihsz+E9rbcMta3YDT7kfpXj/
/LggHsjOUxARZ/bAgP266HKGwC5vupxNIB79dwFKmr56fmnZ51kA+mdwB77Be6eO
ompj/OTJqTveH3CjAEyVFyTKrdr7nDXCVwPDyWGTY7rKnkoXGnNWOo+X+Z1Xe0qy
jGZJ1VsEP4N9KwZ5T8Dz+g4oecj+2kn0pwNidxTMfMoEQWd20hSUO6UwUcyPH1L5
Q43QVdc7cHUv
-----END CERTIFICATE-----
```

This will be converted to a summary panel:



(I'm sorry about using an ldap certificate in the example)

4. Save changes

Final steps

Once you have defined the login box text to suit your organisation (on the login page tab) you are ready to deal with the final two configuration areas:

- Permission set rules so that your users as assigned an appropriate set of resources
- Attribute mappings so that OpenAthens can make use of data available from SirsiDynis.
    - See also: Typical SirsiDynix attributes

When you're ready to go live, check both the live and visible boxes and then save. Your new connection should be available on the authentication point in a few seconds.

Testing

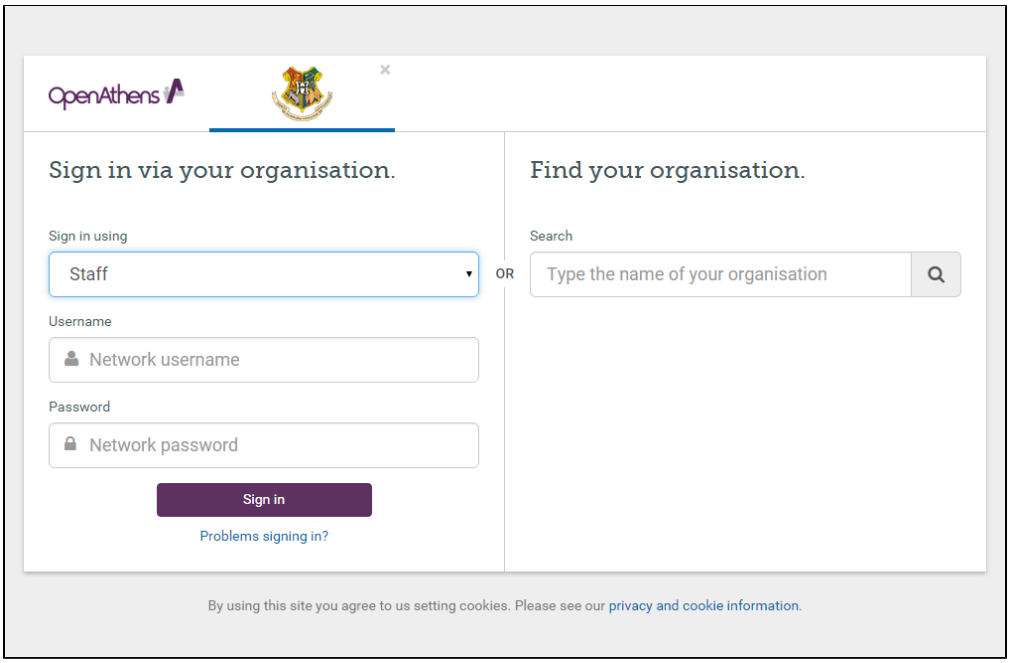
Since OpenAthens accounts will still work if entered (see below), some sites are happy to test by setting the connector to live & visible for short periods of time. You can also use debug mode to make all connections visible and selectable by you without anything being visible to your users.

How to use the SirsiDynix connector alongside OpenAthens accounts or other connections

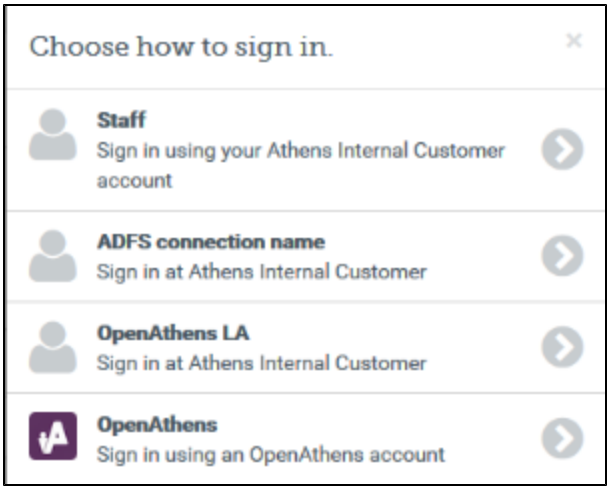
If this is your only local connection, once you set this as both live and visible it becomes the expected way for users to sign into OpenAthens where the system knows the user is yours - e.g. where the user has selected your organisation from a WAYF on a federated resource or remembers a users previous choice. Where the system does not know the user is yours only the OpenAthens account login will appear, but the user can find you via the search box - once selected the user is taken to your connection.

Users with OpenAthens accounts from your organisation can still sign in by entering their username and password in the same login box as the SirsiDynix accounts. This may affect your choice of label.

Should you need to show more than one option, how they are displayed depends on what they are. If they are all SirsiDynix or LDAP, the user will see a drop down list above the credentials boxes. This will contain all SirsiDynix and LDAP connections that are set as live and visible.



If your mix of connections includes SAML or OpenAthens API connections - e.g. SirsiDynix for patrons and ADFS for staff, this is presented as a selection box in an overlay. The local connection is remembered if the user goes on to successfully sign in using it; if the user does not successfully sign in for any reason, the authentication point will forget their preference and present the chooser again next time (this is to prevent users who select the wrong option from getting stuck at a login they cannot use).



Depending on your subscription, multiple connections may incur additional charges.

What the fields are for

Field	Explanation
Name	The name of the connection as it will appear to users at our authentication point when there is a choice of connector.
Server host	The address where OpenAthens can connect to your server. This address will need to be accessible by our services from outside of your network. E.g. `sirsidynix.yourdomain.com`

Server port	The port that your server uses for API traffic. You can specify a non-standard port if necessary. E.g. `8080`
Endpoint URL	Where the API calls should be sent E.g. `/symws4`
Client ID	Your client ID E.g. `AB_CLIENT`
Admin username	Not normally required. Only has to be specified if you need to map or act on privileged attributes such as 'category-1'.
Admin password	Not normally required. Only has to be specified if you need to map or act on privileged attributes such as 'category-1'.
Status	*Not live* = Can only be used in debug mode. *Live and not visible* = Can only be used in debug mode. *Live & visible* = production ready. Users will be able to access this login at the authentication point. If you have only one connection it will become the default login whenever your organisation is known (e.g. for any resources where access involves your entityID). Changes to the status usually take effect within moments.
Create local accounts	Automatically - any user authenticated by your system is deemed ok and will be accepted by the system Manually - only user IDs you have previously uploaded will be accepted by our systems. See how to limit which local accounts can sign in
Remove local accounts	This setting controls when local account data will be automatically cleared from the system and is the number of days from the last time the account last signed in. Pre-mapped accounts that have not been seen are also cleared. The setting can be from 1 to 365 days and represents the number of complete days that have passed since the date the account last signed in. i.e. does not include the day of the last sign-in in the count. See also: How to modify a local account.

Statistics show the user identifier passed by the SirsiDynix system, e.g. the barcode.

Anything to watch out for?

Connections from us will come from the following IP addresses (35.189.71.17 and 35.224.184.162) and your network team may need to be told. Changes to these addresses would be communicated in advance.