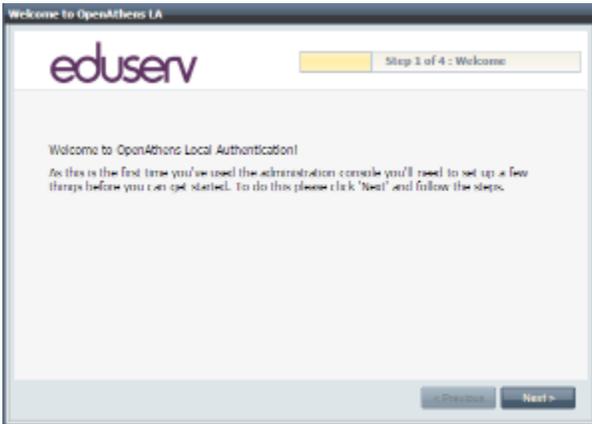# Connect LA to your directory

The first step will be to access the administration console for the first time. This will invoke a wizard that asks for the following information, some of which you may need the library to supply:

Go to https://<adminconsoleaddress>:7070

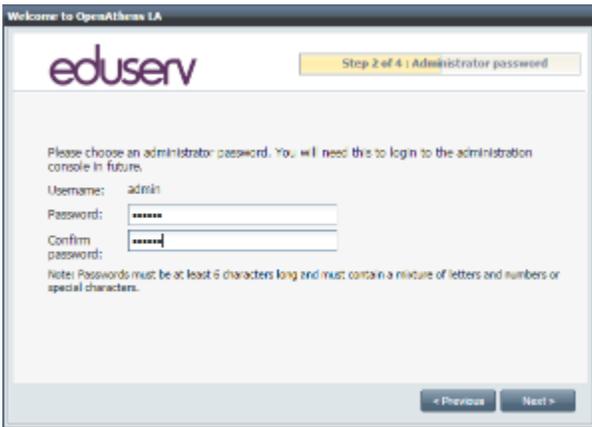Set the super-user password for the administration console:

Supply your organisation name and domain name. The domain name should be the one you use as your 'scope' in any federations you are members of and will be used to generate various default settings.

Finally enter your licence key, available from our service desk.
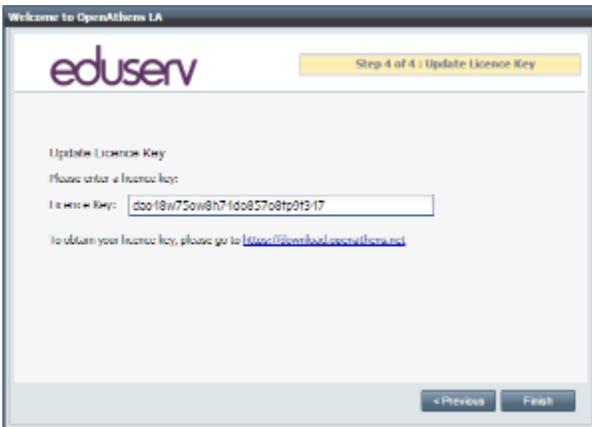
You can now access the admin interface:
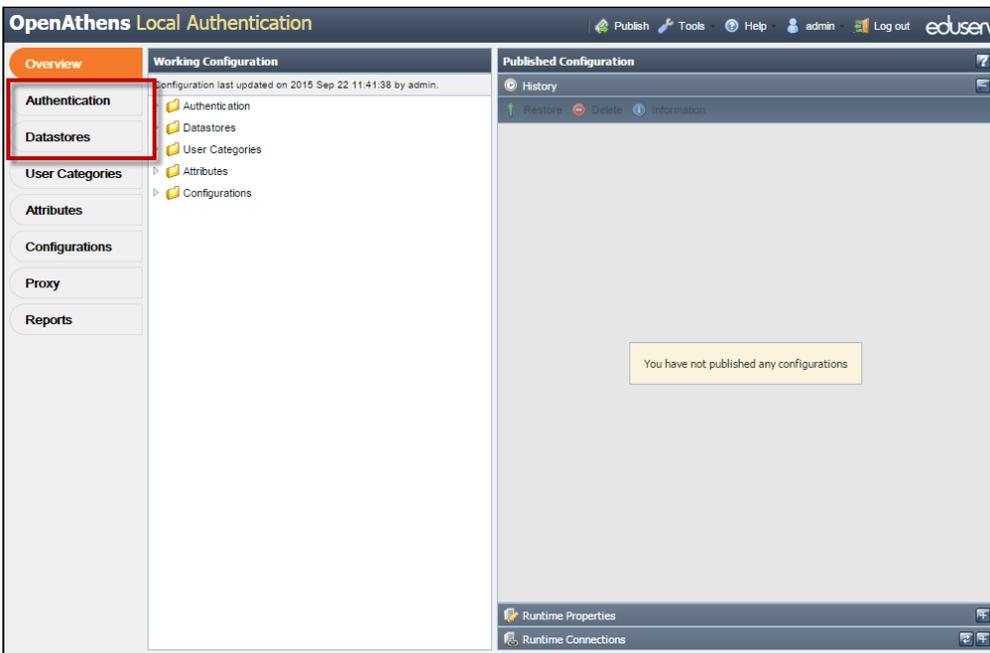
Specify your authentication store

The first of the two tabs highlighted above will allow you to specify the connection to your authentication store. This is the directory that you will be using to authenticate your users.

The example below uses ActiveDirectory or LDAP, but you can also use things like, Kerberos, or a simple test provider, and even your own custom modules.

Prerequisites

- An admin user in the directory that can search all users that will be authorised for at least their FQDN based on the username attribute you specify.

Method
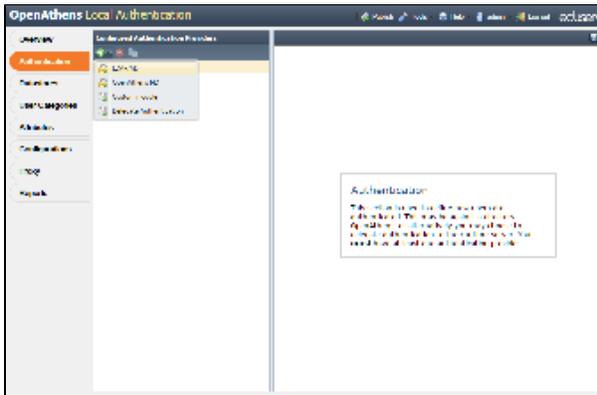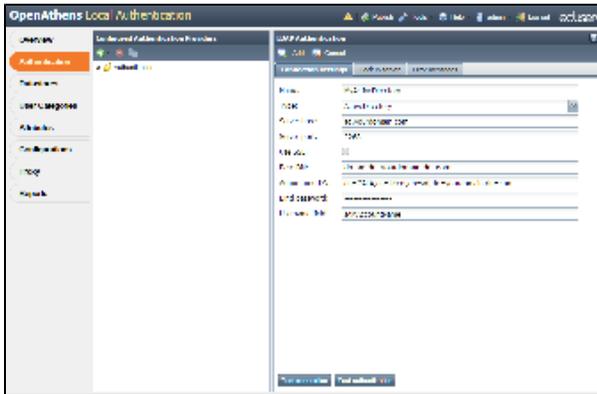
1. Add the new provider

2. Complete the details and click add. Ports can be modified if yours are non-standard.

3. Test the connection and authentication

The username field defaults to sAMAccountName for ActiveDirectory, but you could use mail or any other field that suited. This is the field that users will enter on the login page.

The other tabs on this panel will let you specify a backup server and modify the error messages to match your needs.

The authentication store is connected to twice per user session by the runtime. Once with the admin bind to discover the FQDN of the user and once with the FQDN and password of the user for authentication.
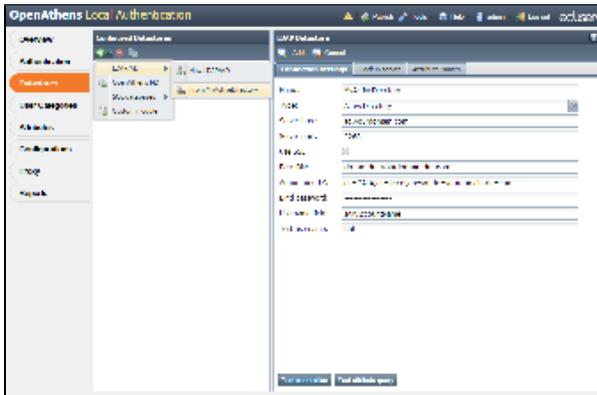
Specify your data store

The datastores tab will allow you to specify the connection to your data store. This is the directory or database you will be using to provide information about your users. It is often the same LDAP server as the authentication store; it does not have to be, however you will need to ensure that the username field from the authentication store exists in the datastore as a foreign key.

Prerequisites

* An admin user in the directory that can search for all authorised users and read all relevant attributes that the library will be using. This is more than is required for the authentication store connection.

The example below uses ActiveDirectory, but you can also use SQL databases or your own custom modules:

1. Add the new datastore. For LDAP/AD there is an option to copy most of the settings from your authentication store.

2. Complete the details an click add - if the system copied things over, this should just need to be a test username that the system will use in the next step.

3. Test the connection and the attribute query. The query test will submit the test username from the settings to recover a list of attributes that have values.

If you changes the username field on the authentication store, you need to change this one to match.

The other tabs on this panel will let you specify a backup server and limit the available attributes.

Using a SQL server is a little different - see: using a SQL database as a datastore

Specify the proxy hostname (optional)

If you know you will be using the proxy function, you can specify it now.

1. On the Configurations tab select External in the left hand pane
2. In the right hand pane select the proxy tab
3. Set your proxy hostname, e.g. proxy.yourhostname.com
4. Click apply
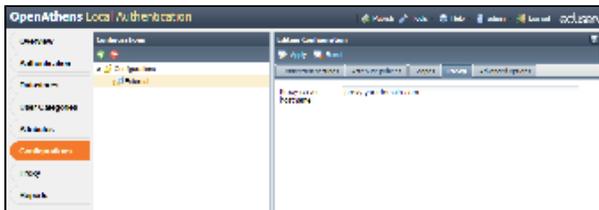
Next steps:

- Connect your runtime to your admin console
- Return to install menu
- Return to homepage
- Troubleshooting