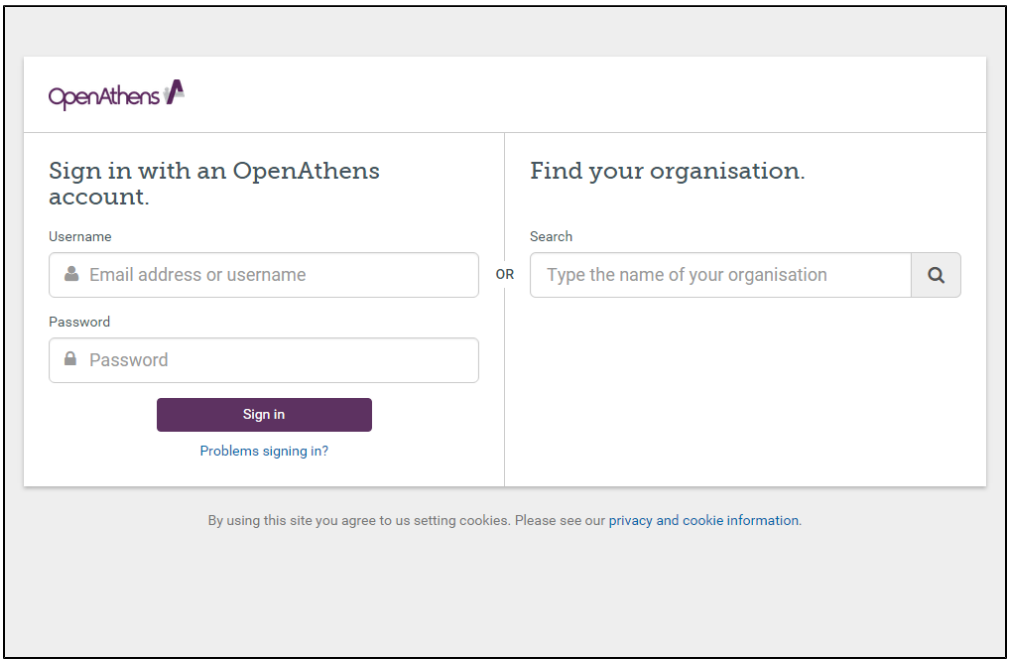
About the authentication point

The OpenAthens authentication point (AP) has been designed to work on the widest variety of browsers and platforms that it reasonably can - your users should not have any difficulty using it on the desktop, tablet or smartphone. Older browsers may have some display quirks though.

The AP is where a user logs into the OpenAthens service and a user will pass through it every time they access a resource - they will only see it or interact with it if they are not already signed in (the session lasts up to eight hours or the closing of the browser, whichever is less).

The AP supports logins from both OpenAthens accounts you create in the interface, and also interacts with your local directory if that is connected - depending on what type of local authentication is connected, the user might see a login box for an LDAP or Sirsi connection or be transferred invisibly to a SAML login such as ADFS.



The page comprises of three main sections -

Login area

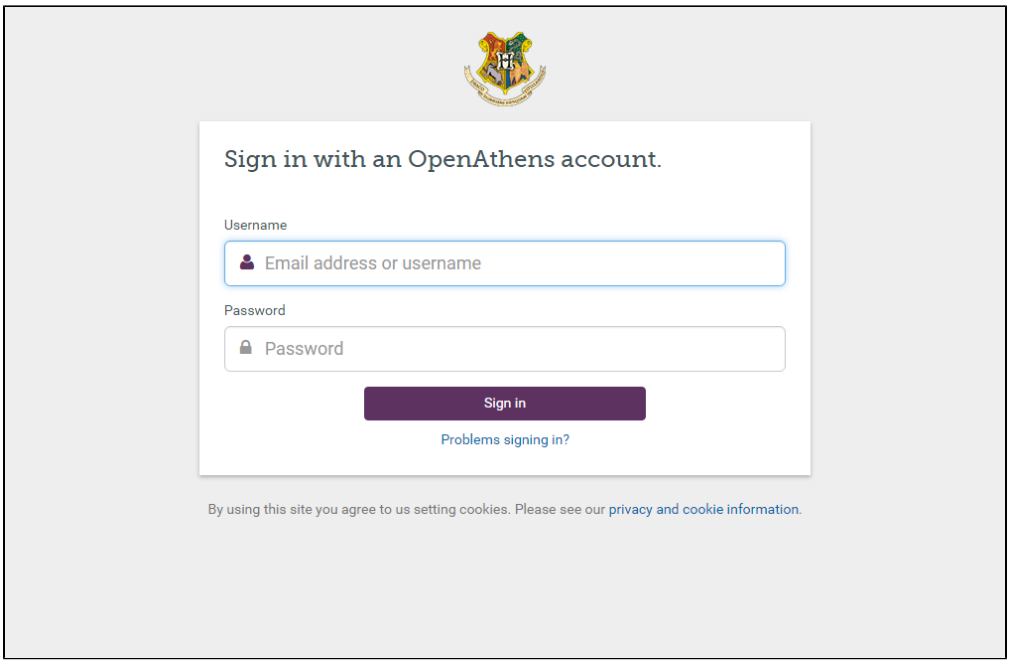
This defaults to expecting OpenAthens credentials when it doesn't know where a user is from and is towards the left or the top depending on your browser's resolution and orientation. If your organisation has been selected from the search on the right, your LDAP or Sirsi login can play a role.

Organisation search

When the AP is not told by the resource where the user is from they can search for their organisation. This search is towards the right or the bottom depending on your browser's resolution and orientation.

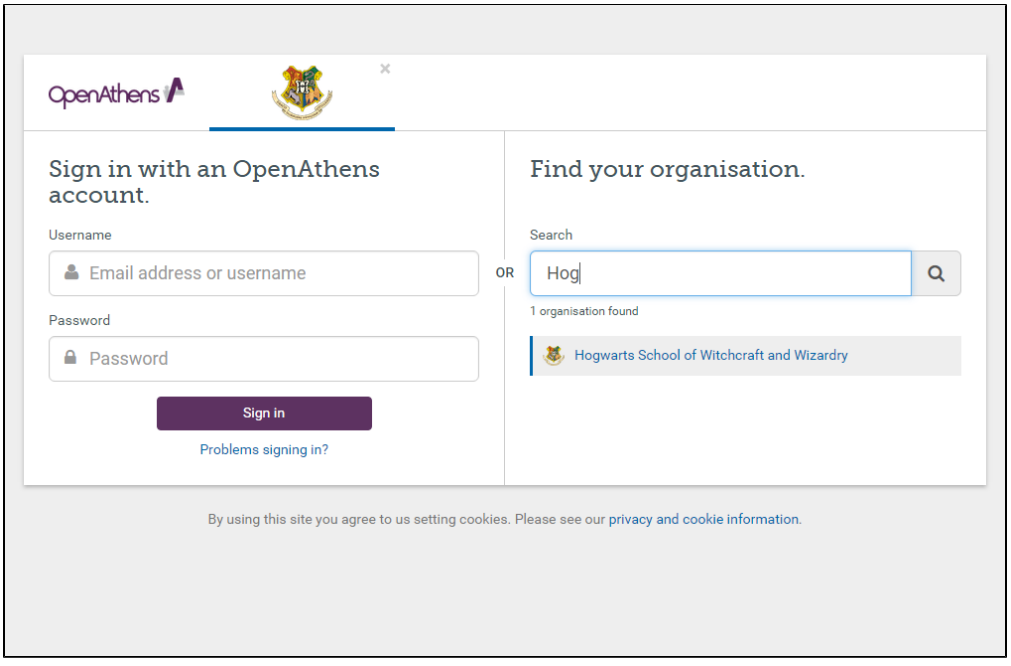
This is only *necessary* when the AP doesn't already know where the user is from AND the site is using local authentication. When the organisation has been pre-selected at a resource, this part of the page does not appear as the AP has already been told where the user is from. It also does not appear if the user successfully authenticated at a delegated login such as ADFS the last time they were seen.

If the organisation is selected by discovery at a resource though, or the user is following a wayfless URL, the search section is not necessary so is omitted:



This version of the page has some additional text options under the domain preferences and if you are using a delegated login such as SAML or ADFS, the behaviour is a little different.

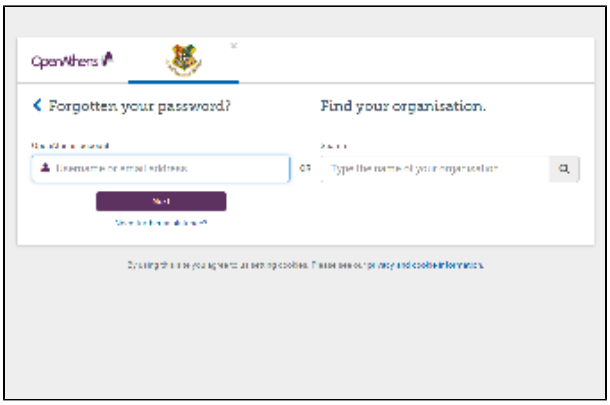
When the AP isn't told this useful bit of information by the resource but remembers where a user was successfully authenticated last time, the organisation logo is displayed above the login area (or if you're using a delegated login as above, the user is sent there). If you're using something like LDAP or Sirsi, you'll see this and the user can enter their local credentials on the left:

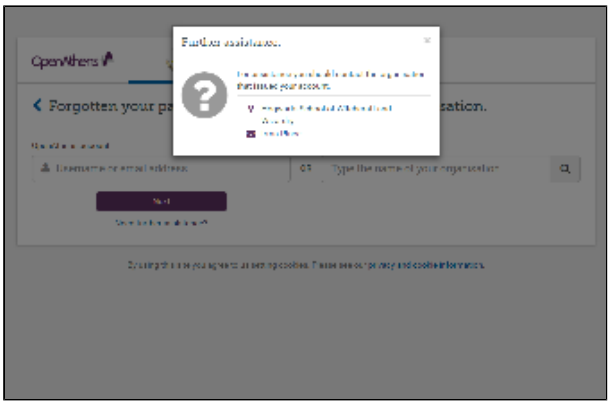


(If you have not uploaded a logo, the organisation name as set on the domain administrator's account is used. If this name is long, you may find that not all of it is visible.)

Help pages

There is a link below the sign in button that can help users. Here they can find the forgotten password function and organisation contact details.





If you want to include a link directly to the forgotten password function on your own pages, use:

https://login.openathens.net/auth?#forgottenpassword

The organisation search on the forgotten password page will take users directly to the contact details for their administrator.

Does the user always have to search?

If you are using OpenAthens accounts, then they only have to search when they need to find their organisation's help details.

If you are using a local authentication connector, users must search if the AP doesn't already know where they are from. There are three main ways that the AP might know that without the user having to search themselves:

1. The user selected a home organisation at a service provider

   Because the AP has a unique address for each organisation, selecting your organisation at the service provider (or by a wayfless URL) will get the user to the AP in a known-organisation state so can go immediately to the correct authentication method. This will ignore any organisation the user has previously selected.

2. The home organisation has been previously discovered and remembered by the AP.

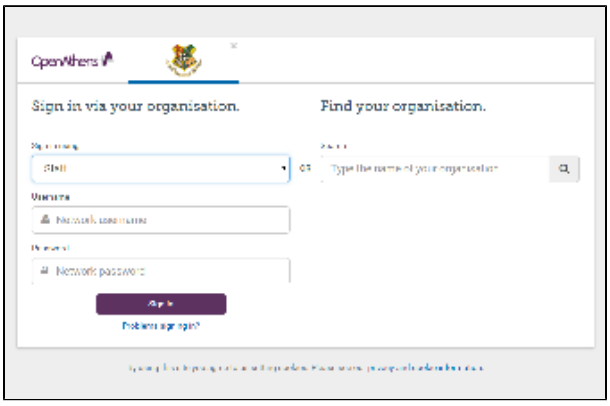
   Both the first scenario OR a user using the search box can initiate this, but the location is not stored until the user successfully authenticates. The location is stored in a cookie, so will be affected by any circumstance that clears cookies such as being on a kiosk machine. The setting is also cleared if the user does not pass authentication (so that users who select the wrong organisation are not stuck forever)

3. The user is accessing a resource via the Redirector

   The redirector uses links that are specific to your OpenAthens domain so users should always be recognised by the AP

What if I have multiple local connectors?

The best user experience will come from only having one connection, but if you need more the user will have the option to select which one. Depending on the type of connectors this could be presented as a drop down list or a selection box. The AP will remember the users' choice after a successful local authentication.



OpenAthens accounts can be entered at any brokered connection, but since a delegated connection hands off to your local authentication page you would need to set an additional domain preference to use them alongside SAML, ADFS or API connectors.

Can I connect local authentication systems to sub-organisations?

This is not usually desirable from a user experience standpoint because the pre-discovery scenarios described above can only direct users to the domain organisation, not a sub-organisation (not even one with a unique scope). Instead you should set up the connection at the domain level and use the map to sub-organisation function - sub-organisations found at the AP will use this connection.

Which organisations can be found in the search box?

Only domain organisations and sub-organisations with unique identifiers will appear.

Anything to watch out for?

If you have multiple organisations that will appear, you should make sure that they have different enough names that users can select the correct one.

If you set a local connection as default you cannot use any other connectors.