LDAP connector

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

OpenAthens can connect directly to an LDAP server so that you do not have to issue personal accounts for your users (you will still need your OpenAthens administrator account though). Anything that uses standard LDAP protocols is acceptable so this works very well with ActiveDirectory too.

As well as the ability to use local accounts instead of maintaining a separate set of credentials, accesses to federated resources that already involve discovery (identifying the users' home organisation) will take the user directly to your LDAP login at our authentication point - no further discovery is required.

Preparation

Before you start you will need:

- An LDAP server that can be queried from outside of your network.
    - If this is not possible, an ADFS connection might be what you need instead.
- A member of your IT team to supply or enter the connection details (jump to details).
- A copy of your LDAP server's certificate (base 64 encoded X.509, often called pem format).
    - This must be the root certificate - i.e. the subject and issuer are the same. If you are unsure how to get this from ActiveDirectory, see: ActiveDirectory certificates
- Access to the OpenAthens administration area at the domain level

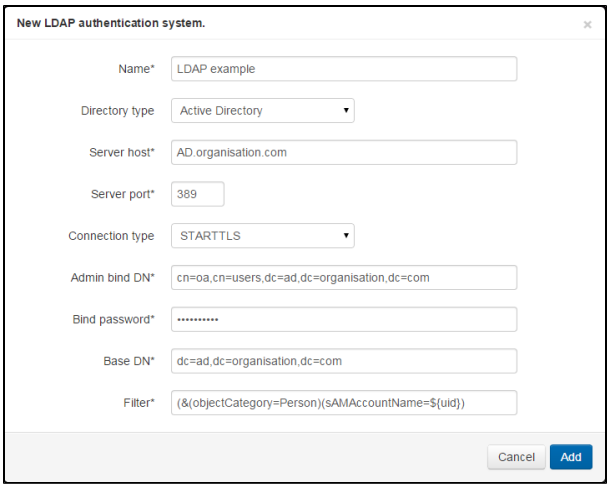
If you are migrating from an alternative IdP such as Shibboleth, also see: Migrating from your own IdP

Add the connection

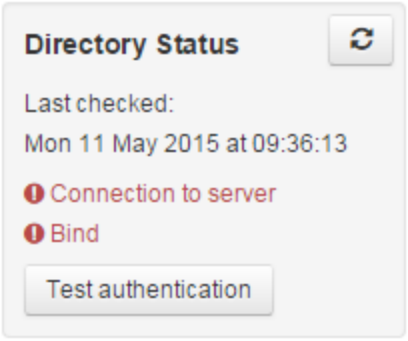
In the administration interface as the domain administrator go to ***Management > Connections***

1. Click the add button on the left and select LDAP

2. Have your colleague from the IT team complete the form and click add at the bottom.



3. OpenAthens only permits secure LDAP connections so will require the root certificate of your server. The status panel will show errors until it is added:

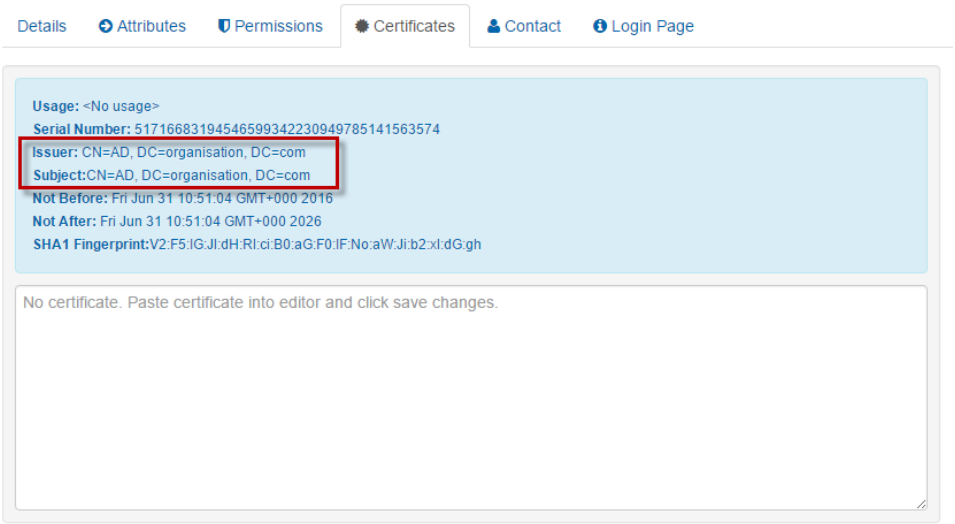


You can hover over the panel for more details about an error

4. Switch to the certificate tab and paste in the contents of the certificate file which should look similar to this:

```
-----BEGIN CERTIFICATE-----
FAKElTCCAn2gLwIBAgIQJuhFWFFr7ZxCMn6ymkjQtjANBgkqhkiG9w0BAQUFADBd
sRMwEQYKCZImiYPyLGQBGRYDbmV0MRowGAYKCZImiZPyLGQBGRYKb3BlbmF0aGVu
HzESMBAGCgmSJoNT8ixkARkWAmFkMRYwFAYDVQQDEw1hZC1PQS1BREZTLUNBMB4X
dTE1MDExNjEwNTEINFoXDTI1MDExNjExMDA1OVowXTETMBEGCgmSJomT8ixkARkW
N25ldDEaMBgGCgmSSomT8ixkARkWCm9wZW5hdGhlbnMxEjAQBgoJkiaJk/IsZAEZ
EgJhZDEWMBQGA1UEAAMNYWQtT0EtQURGUy1DQTCCASIwDQYJKoZIhvcNAQEBBQAD
SgEPADCCAQoCggEBAMNkzzh4fgdFtCHzhbTSmSrEx846+wRmdG1FHKhSkXkmbV1U
8S/TtRJ6zwPvb181AC/IGC7msrvSsZc19Jfe5nJVL2kSCAWDLjsIwJKUb9gep3na
R846gv83Q/m0/YJ1pyT2DcAVcvCQAI2+MjoLFET43v9haREjbGa7JFDdnjsbjqyZ
EODlalLKOlLicsGImTKFSI4UX3fzAPPLEareAWESOMEr05MdxQifVWpaDcPUh1BJ
BK92Sy+oIBEqQzLu4Vtd/1O4HuyOSw5wOBJLGP4PTwbqPdrpotvDPg+MLN/RHc54
vUEJcl1mTtLLBmMYiVJKXMxT1CYmYWM9ibA7JB8CAwEAAaNRME8wCwYDVR0PBAQD
SgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFGWVTvqweerzee/JFMbuTYzi
To/VMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQDGIvljYiX1
wmneie6HnOmkNhQVuvxCSOpYZT3uezq/8/ZrhR5UrkWfYdmfhcmNgmndcMr3GSCt
DJdjxT9c0qUK+PC2IjZtO3tVvuuZY1cf5E6A5TArihsz+E9rbcMta3YDT7kfpXj/
/LggHsjOUxARZ/bAgP266HKGwC5vupxNIB79dwFKmr56fmnZ51kA+mdwB77Be6eO
ompj/OTJqTveH3CjAEyVFyTKrdr7nDXCVwPDyWGTY7rKnkoXGnNWOo+X+Z1Xe0qy
jGZJ1VsEP4N9KwZ5T8Dz+g4oecj+2kn0pwNidxTMfMoEQWd20hSUO6UwUcyPH1L5
Q43QVdc7cHUv
-----END CERTIFICATE-----
```

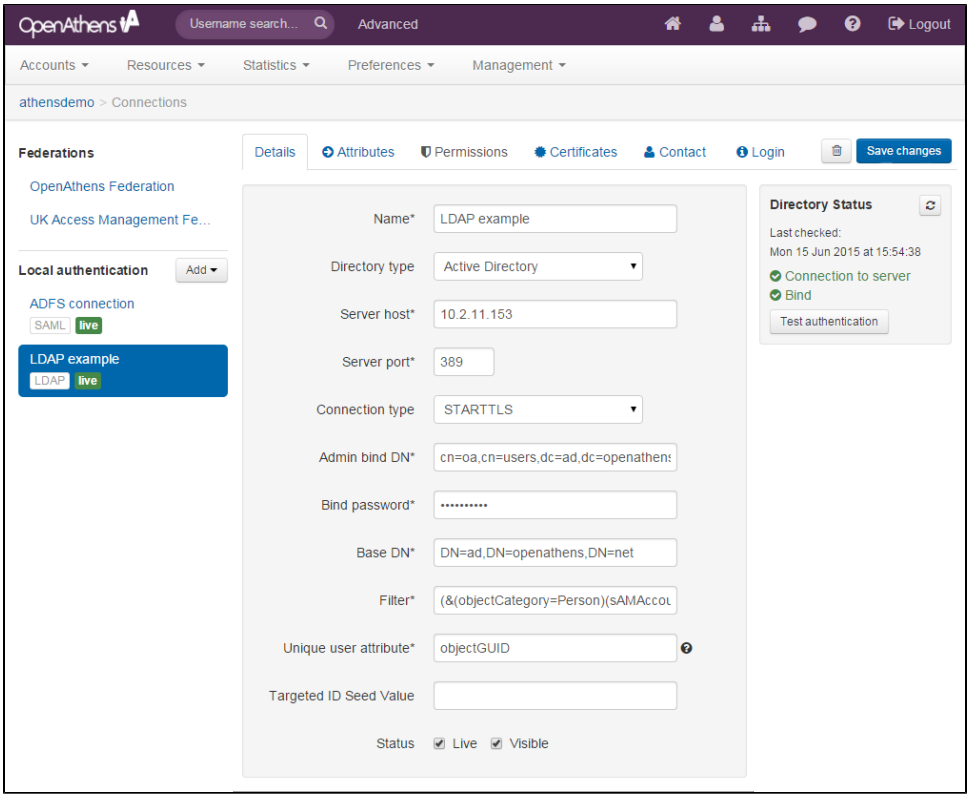
5. . This will be converted to a summary panel:



Usually these certificates are self-signed, so the one you want has matching issuer and subject lines. If using third-party certificates, also add the root certificate that the third-party certificate chains to.

6. Save changes

7. The status panel will update and should now show success if it did not before



8. You should be able to use the test authentication button now with your own username and password.

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 your LDAP
    - OpenAthens will cache these attributes when the user signs in, so changes in LDAP won't be picked up until the next time the user starts an OpenAthens session.

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

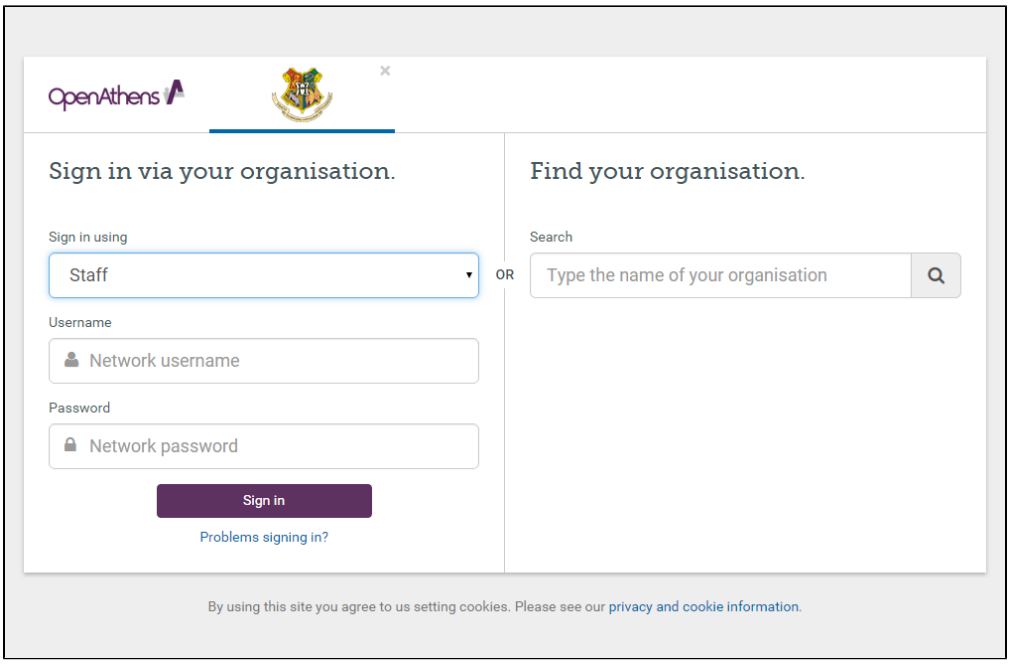
Since OpenAthens accounts will still work if entered (see below), some sites are happy to test by setting the connector to live & visible for periods of time. You can also use debug mode to make all connections visible and selectable by you without anything being visible to your end-users.

How to use LDAP alongside OpenAthens accounts or other connections

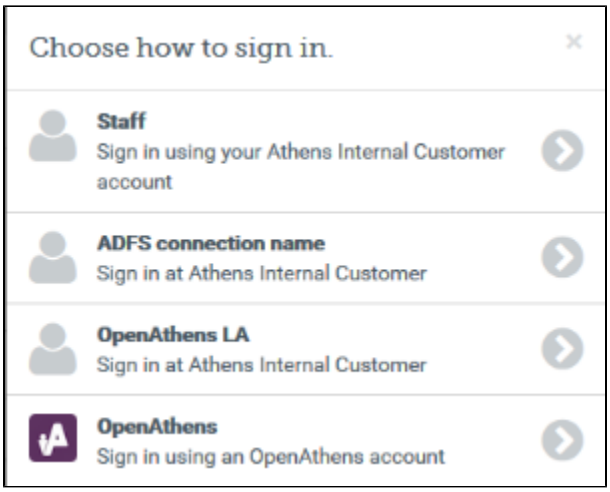
If this is your only local connection, once you set this as both live and visible it becomes the expected way for users to sign into OpenAthens where the system knows the user is yours - e.g. where the user has selected your organisation from a WAYF on a federated resource or remembers a users previous 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 LDAP accounts. This may affect your choice of label text.

Should you need to show more than one LDAP option, the user will see a drop down list above the credentials boxes. This will contain all LDAP connections set as live and visible.



If you need a mix of LDAP and SAML connections - e.g. LDAP for students and ADFS for staff, this is presented as a selection box in an overlay. Local connections are 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).



In these cases, selecting the OpenAthens option will show the first LDAP connection and the OpenAthens credentials will be accepted there.

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 at our authentication point when there is a choice of connector.
Directory type	Used to set default values in other places on the form.
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.
Server port	The port that your server uses for LDAP traffic. Standard ports are selected when you change protocol. You can specify a non-standard port if necessary but this can affect security.

Connection type	The form of security used. StartTLS is the standard but ldaps:// can be chosen if you prefer. The minimum supported version of TLS is 1.2.
Admin bind DN	The full distinguished name of a user that can connect and view all the users you need to authenticate, e.g: `cn=openathens,cn=users,dn=ad,dn=yourdomain,dn=net`
Bind password	The password for the user specified in the admin bind
Base DN	The distinguished name of your directory, e.g: `dn=ad,dn=yourdomain,dn=net`
Filter	Allows you to specify the username field, plus limitations where necessary. The field you identify as =${uid} will be used as the username in login dialogs
Display name attribute	This defaults in AD to be 'sAMAccountName' and in LDAP to 'cn'. It is the value displayed in account lists and in audit. You can choose any attribute.
Unique user attribute	This should be an attribute that will always be unique to that user and it is used in the generation of targetedIDs and statistics. It defaults in AD to 'objectGUID' and in LDAP to 'cn'. If you are migrating from another local authentication system, you may want this to match your old setting. Pseudonymous identifiers are recommended where they are available.
Salt value	The salt used to generate a targetedID for users authenticated by this connection. You might edit it if you were migrating from something like OpenAthens LA to MD so that your users can have the same targetedID value when they change systems. If you set it to blank the connection will use the same salt as your MD accounts. Modifying this after you go live will change the identifiers seen by service providers for your users... which is rarely desirable.
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.

Example filters

Instead of specifying only a username field, the use of a filter allows compatibility with a greater variety of LDAP structures - e.g. where including all valid users requires binding to a node that will also include invalid users, the filter can be set to exclude the invalid users.

cn=${uid} - The default LDAP filter using common name as the username

(&(objectCategory=Person)(sAMAccountName=${uid})) - The Default ActiveDirectory filter uses the Windows login as the username and requires the user to have an object category of person.

See some more example filters

Technical information for your IT team:

During set-up and configuration (including testing of mappings)

- There is a read-only admin bind to your directory to check status and read the available attributes for mapping

During user authentications

- There is a read-only admin bind to your directory to discover the FQDN of the user based on whichever attribute you have defined as the userID
- Once the user's FQDN is known, it is used with the user's password to bind for authentication and request of any mapped attributes

Connections from us will come from the following IP addresses (35.189.71.17 and 35.224.184.162) and changes to these would be communicated in advance.

The admin bind used MUST have sufficient access to search for accounts and read the FQDN of any user account (that should have access).

The admin bind used SHOULD have sufficient access to read all mappable attributes for user accounts so that typeaheads work when setting up mappings and permission set rules.

The only significant difference between StartTLS and ldaps:// in operation is that with StartTLS you only need to listen on one port instead of two.

Anything to watch out for?

AD will truncate sAMAccountName before release if it is over 20 characters. This may affect your choice of unique user attribute.

TLS versions before 1.2 are not supported.

Pseudonymous?

Pseudonymous identifiers such as objectGUID are recommended for the unique user attribute to avoid potential problems with data protection legislation as that identifier will live on for a time in the audit trail after other mapped attributes are cleared.