Configuring ADFS as an authentication provider for OpenAthens

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

OpenAthens can connect to ADFS (Active Directory Federation Services) so that you do not have to issue personal accounts for your users (you will still need your OpenAthens administrator account).

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 ADFS login.

Preparation

Before you start you will need:

- Windows Server 2008R2 or better running ADFS v2.0 or above
- A member of your IT team to configure ADFS and supply the metadata
  - Ideally an externally accessible URL for your ADFS metadata, but failing that copy of the metadata as an XML file
- All users to be in your directory
- 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

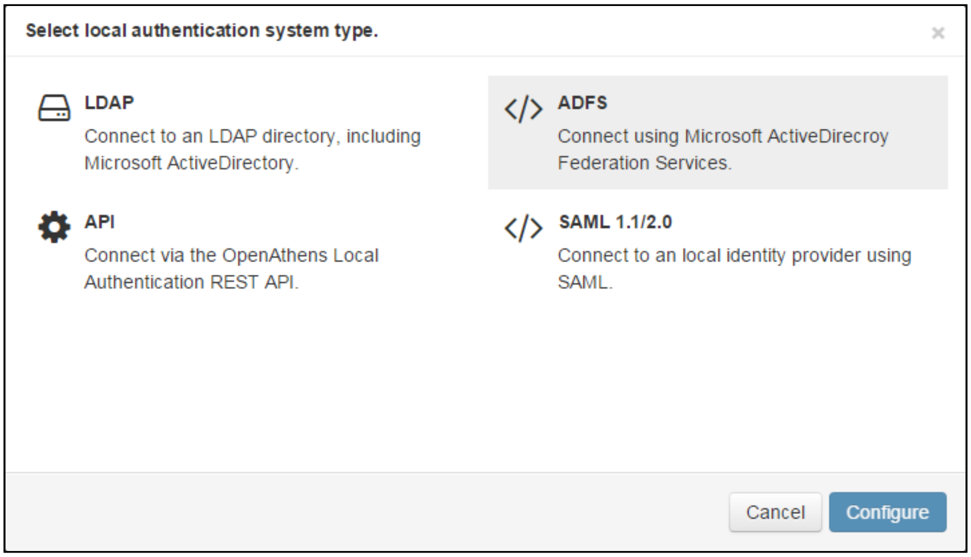
If you're unsure about anything or get stuck, we're happy to help. Hit the support link in the top right of the admin area to get through to your local support guys.

Add the connection in OpenAthens

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

(If you already have ADFS visible as a SAML connection, you will need to delete that connection before the system will allow you to add it back)

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



Select local authentication system type.

LDAP
Connect to an LDAP directory, including Microsoft ActiveDirectory.

ADFS
Connect using Microsoft ActiveDirecroy Federation Services.

API
Connect via the OpenAthens Local Authentication REST API.

SAML 1.1/2.0
Connect to an local identity provider using SAML.

2. Enter the ADFS metadata URL or upload the xml file as supplied by your IT team.

   a. The metadata URL is typically something like https://YOURDOMAIN/FederationMetadata/2007-06/FederationMetadata.xml and would need to be accessible outside of your network.

3. Set the user identifier field to match the claim you will be sending as the user identifier. This can be changed later, but needs to have a value to save the page.

4. Set the display name to match the claim you want to use - if you are only sending one claim, you can set this the same as the user identifier. Again this can be changed later, but needs to have a value to save the page.

5. Do not set it as default at this time.

6. Save changes

7. Go to the relying party tab and make a note of the metadata address displayed there. You will need this when you add OpenAthens to ADFS.

The detail fields displayed are

Field	Explanation
Display name	The name of the connection as it will appear at our authentication point when there is a choice of connector. Defaults to the name specified in the ADFS metadata
Metadata URL	Where the ADFS metadata is published. Populated only when metadata is loaded from a URL, it allows easy updates to the connection if your ADFS system changes.
EntityID	The entity identifier of your ADFS instance, typically http://YOURDOMAIN/adfs/services/trust. Drawn from the ADFS metadata.
SSO endpoint	The login address, typically https://YOURDOMAIN/adfs/ls/. Drawn from the ADFS metadata.
Display name attribute	The claim you specify here supplies the value displayed in account lists and audit where you would normally see the OpenAthens username. DisplayName is a common source but it does not have to be different from the Unique user attribute claim.
Unique user attribute	The claim you specify here *must* supply a value unique to the user within the current user set and *should* supply a pseudonymous value unique to that user for all time. This is used by the system to tell users apart and also used in the generation of targetedIDs and statistics. It does not have to be the username entered at your login point. ObjectGUID is a popular choice.
Status	*Not live* = connection can only be used in debug mode. The visibility and default flags are ignored. *Live and visible (if this is the only local connection)* = connection can only be used in debug mode. *Live and visible (if there are multiple live and visible connections)* = users are offered a choice of connections, including this one. There is a domain preference to include OpenAthens accounts or not. *Live & visible & default* = This is your only login option and users will be sent directly to your login whenever the organisation is known. A successful authentication will tell the authentication point to remember that location. A failed authentication will clear that setting. Debug mode will not show other login options. Changes to the status usually take effect within moments.
Create local accounts	Automatically - any user authenticated by your system and passed back to us is deemed ok and will be accepted by the system Manually - only user IDs you have previously uploaded via the list page will be accepted by our systems
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.
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.

Add OpenAthens as a relying party in ADFS

The following section assumes you are familiar with ADFS, If you are not, the next three steps have an alternative more detailed guide available.

1. In your ADFS management console add a new relying party trust using the OpenAthens metadata address you recorded earlier

2. Edit claim rules to release at least a user identifier attribute.

   a. A simple 'Send LDAP Attributes as Claims' rule is sufficient.

   b. The claim value must unique amongst current users and should ideally be pseudonymous and unique forever. Something like objectGUID would be a good choice.

   c. Naming considerations
      i. If you are unfamiliar with the ADFS name space, or want to provide more meaningful names for the interface your library colleagues will see, you may like to prefix the claim names with something such as 'oa_', e.g. 'oa_username', to avoid accidentally using reserved terms.

    ii. Claim names may not contain spaces

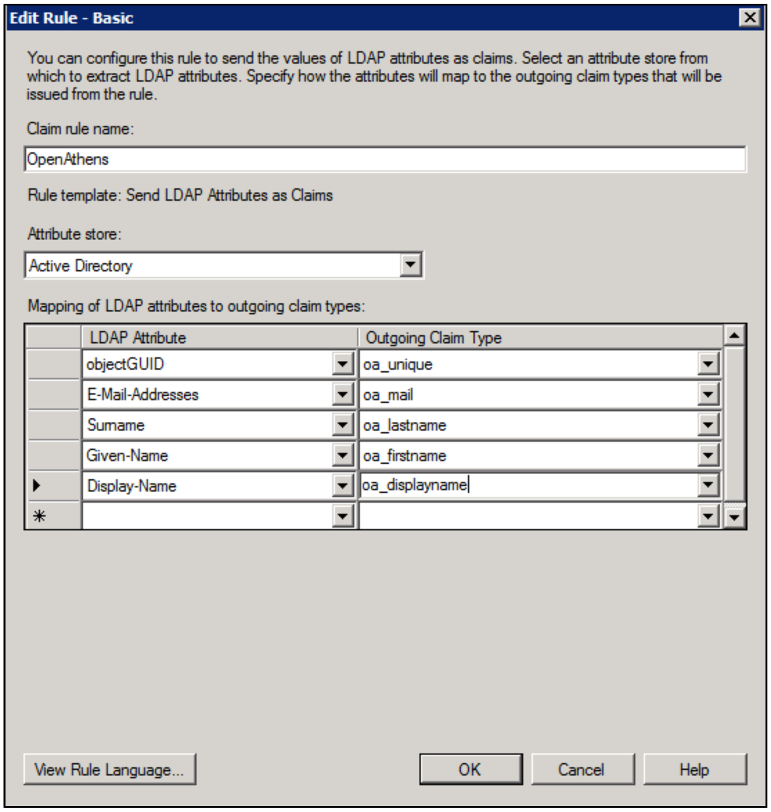
3. Save

Depending on your library's needs, this may be sufficient however you will usually want to release more information so that claims can be mapped to OpenAthens attributes and used for organisation, statistics, resource access, display names and resource allocation - e.g:

- First and last names to help the library identify users
- Email address to help the library contact users and, in certain cases release that data to service providers
- An attribute such as memberOf to let them assign different permission sets to different groups of users based on rules
- An attribute that would serve as a display name
- A department or OU name for aggregation of statistics

In all cases, the library will need the name of the claim for the next part of the set-up. Claim names are case sensitive.

Example Issuance transform rule:



Edit Rule - Basic

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: OpenAthens

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	objectGUID	oa_unique
	E-Mail-Addresses	oa_mail
	Surname	oa_lastname
	Given-Name	oa_firstname
▶	Display-Name	oa_displayname
*		

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

Configure mappings and permission sets

The final two areas to configure are permission set rules and attribute mappings:

- 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 directory
    - OpenAthens will cache these attributes when the user signs in, so changes in ActiveDirectory 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 testable a few seconds later.

How to test

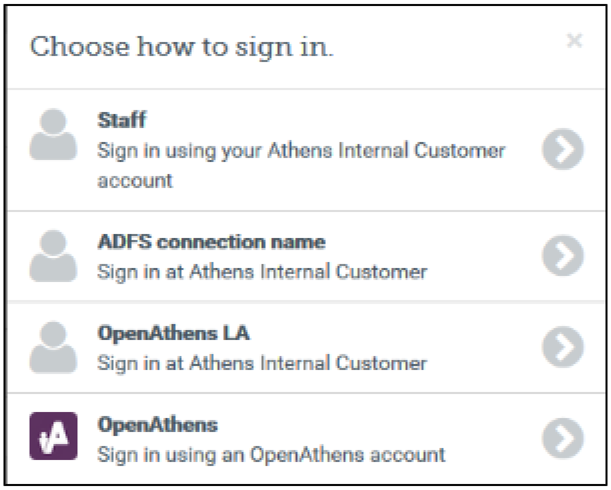
Discovery is not available until you set the connection as live and visible so that users do not get offered options that are not ready to be used. To test your connection you will need to use debug mode to make the connection selectable by you.

Once you have tested and are happy, you can set the connection as live, visible and optionally default then save. This will make it live for your users within a few seconds.

Multiple connectors and OpenAthens accounts

This type of connector is best used as the default connection. In this mode when a user arrives at our authentication point with your organisation known, such as would happen if they select it at at a resource's login, use a WAYFless URL, the Redirector or have previously authenticated successfully, they are passed directly to your login without seeing our authentication point.

If you have a need to use multiple connections, or OpenAthens accounts alongside local accounts - e.g. if you have a group of users that are not in your directory - then you can set the connection as live and visible but not default and set it to allow OpenAthens accounts via the setting on the domain preferences page. In this mode when the user arrives at the authentication point with your organisation known, they will initially see a chooser where they can select the connection to use - all live and visible local connections will be available as well as an option to use OpenAthens accounts. The authentication point will remember their choice.



Choose how to sign in.

Staff
Sign in using your Athens Internal Customer account

ADFS connection name
Sign in at Athens Internal Customer

OpenAthens LA
Sign in at Athens Internal Customer

OpenAthens
Sign in using an OpenAthens account

Multi-valued attributes

With multi-valued attributes - e.g. the memberOf field in ADFS - the interface is not able to display all values and only display one. All values are read and cached though so are available for things like permission set rules and attribute release.

The other tabs

Certificates - allows you to add a second certificate. Used when you need to change a server certificate on AD and want to minimise downtime for your users.

Advanced - Allows you to make several changes that are rarely necessary:

- switch between SAML versions should you have a source that can only handle the older SAML 1 profile
- switch the profile from Redirect to Post if your source insists on it
- enable signing of authentication requests (SHA-1 or SHA-256) if your source requires it
- enable the SAML `forceAuthn` option (forces your local source to re-authenticate any time the user is sent there - e.g. where users can have multiple affiliations within a consortium and your SAML source's session management makes it difficult for them to change).

Anything to watch out for?

When you use the refresh metadata button it will update the connection with values from the metadata including endpoints and certificates. It won't change the name or any options on the other tabs.

If for any reason you have locked your ADFS system down to use TLS versions earlier than 1.2, we're going to reject the connections and it won't work.

Pseudonymous?

Pseudonymous identifiers 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.