Configuring a SAML IdP as an authentication provider for OpenAthens

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

OpenAthens can connect to SAML sources such as Azure, G Suite, OneLog, OpenAthens LA, Shibboleth, and similar 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 SAML login.

Preparation

Before you start you will need:

- Access to the OpenAthens administration area at the domain level
- A SAML source and its metadata (either as a file or the web address where it is published).
- Access to the configuration of that SAML source
- A SAML source that supports TLS 1.2 and above, and follows the SAML standard

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

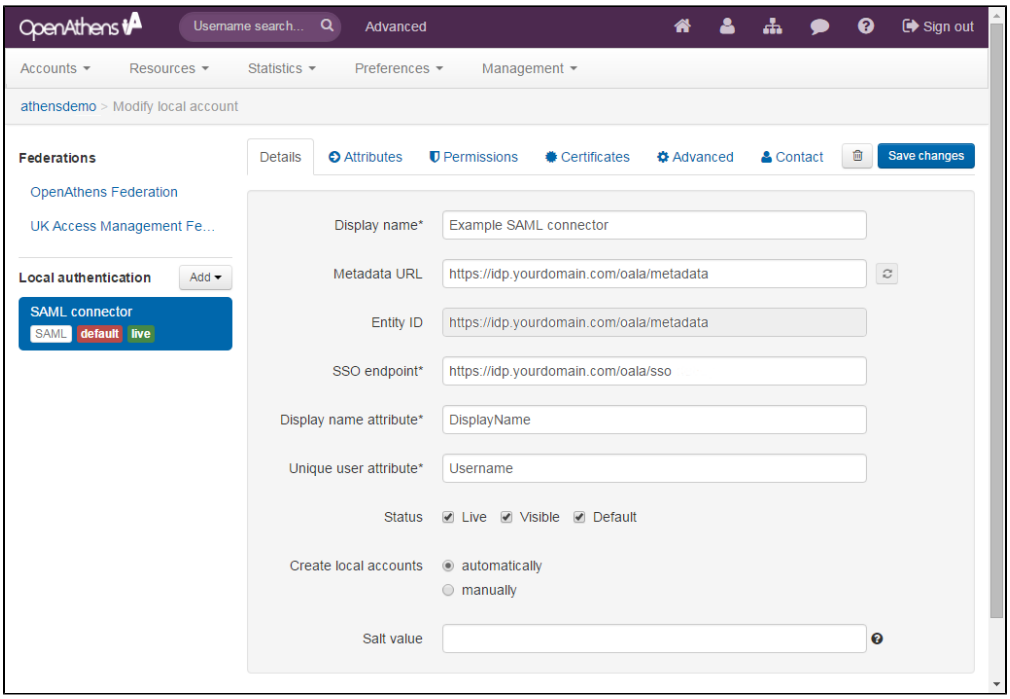
If you're unsure about anything or get stuck, we're happy to help. Hit the support link in the top right of the admin area to get through to your local support guys.

Add the connection in OpenAthens

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

1. Click the add button on the left and select SAML from the options
2. Enter the SAML metadata URL or upload the xml file representing your SAML source.
    a. The metadata URL is typically something like https://YOURDOMAIN/path/metadata and would need to be accessible outside of your network.
3. Set the user identifier field to match the attribute 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 attribute you want to use - if you are only sending one attribute, 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 - you will use this to configure your SAML source.

You should now see something similar to this:



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 SAML metadata
Metadata URL	Where the SAML metadata is published. Populated only when metadata is loaded from a URL, it allows easy updates to the connection if your SAML system changes.
EntityID	The entity identifier of your SAML instance, typically http://YOURDOMAIN/oala/metata for OpenAthens LA. Drawn from the SAML metadata.
SSO endpoint	The login address, typically https://YOURDOMAIN/oala/sso. Drawn from the SAML metadata.
DIsplay name attribute	The attribute you specify here supplies the value displayed in account lists and audit. Something human readable is recommended. It does not have to be different from the Unique user attribute.
Unique user attribute	The attribute you specify here *must* supply a persistent 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. If using the SAML NameID here, the requirement for unique and persistent limits the type to: • `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` • `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
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 Shibboleth 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 the OpenAthens metadata to your SAML source and configure attribute release

You will need to reference the documentation of your SAML source for how to configure it to "*connect to a service provider*". There is help available for some of the more popular SAML sources including Azure and Google in our third party apps section.

The OpenAthens metadata to use for this is at the address quoted on the Relying party tab of the connection you set up in OpenAthens - it will look similar to: `https://login.openathens.net/saml/2/metadata-sp/domain.com/la/123456`

Setting	Value
EntityID / Provider ID / ID	The same as the OpenAthens metadata address, e.g: `https://login.openathens.net/saml/2/metadata-sp/domain.com/la/123456`
ACS / Association Consumer Service / Binding address / Reply address	Almost the same as the OpenAthens metadata address (change 'metadata-sp' to 'acs'), e.g: `https://login.openathens.net/saml/2/acs/domain.com/la/123456`
Binding method	POST

Certificate	-----BEGIN CERTIFICATE----- MIIDvjCCAqagAwIBAgIEVOxCIjANBgkqhkiG9w0BAQsFADCBoDEoMCYGCSqGSIb3DQEJARYZYXRo ZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMCR0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0w CwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMwEQYDVQQLDApPcGVuQXRoZW5zMR4wHAYD VQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwHhcNMTUwMjI0MDkyMDA2WhcNMjUwMjI0MDkyMDA2 WjCBoDEoMCYGCSqGSIb3DQEJARYZYXRoZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMC R0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0wCwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMw EQYDVQQLDApPcGVuQXRoZW5zMR4wHAYDVQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCandpa4o0Njtw1DqbrrNTfOVe1PqyXIIVmDrJ6VUR/ mokXXu+m5Gm+1f+3lyN5IA2YMn9Z8Yo37JQjIHs+xVS3q4nT1ewS7S3en1pdXKsH1WnUnVWUmpl9 WJZrUwi5i8X80LNyr7PmudhuKNEATGUXkA /xWCkk2d8jf91hy7Qu+HA8LOKtdbbNigErh2IY/YuN WUVUqgGbMH5BGr7ZEhPrz+Vwcf9lhPW+tKpKpZEzJfQiq8EoPaeMXEpKWBEErm67gkWFCA5VhfcJ LqFjQEC3pWOxt5rZVS8gl /Z33VSJZVzY5jWcQzmGaLXPHXyiKPmixl6+DjGlUM0ylNF7GvtDAgMB AAEwDQYJKoZIhvcNAQELBQADggEBAFhmhujLZueiJ6F7mQCpfB0Hj4Y8FyFUUc8NMAt5Set7H4DK SSl4shcqisZBa5yTdyenYwkmBszvCWs6Yeep+zJmCR62cb /f1M32oMzLm02OlznWMkE8/IajGmdx TnB6Z/XcdMMIiCeok4kqe5KMd5oRAyNskHYZ+8kzhs2zTveR+rqCtYxa /AYpwf7n0VQR9clBSNCI T4BCRi10aPE531VIxl4ljY3CwNoZ4lQTU /0aj8O4j68V2neiQb8lewAii0b2xoyOGYP4okd7T2tl 4gl2noVbCvYNjd6GYze /w4lgwiemkby7wu5sN1lEudgKDV+H54wU29ZIyDEFM6DDNE4= -----END CERTIFICATE-----

At a minimum you will need to release a unique user identifier. This identifier can be sent as an attribute, or the SAML NameID, but it must be persistent and unique amongst current users. Ideally it would be pseudonymous and unique for ever (i.e. never assigned to a new user).

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

- First and last names or a display name to help the library identify users (the unique user attribute shouldn't be suitable for this)
- Email address to help the library contact users and, in certain cases release that data to service providers
- An attribute indicating group membership to let them assign different permission sets to different groups of users based on rules
- A department or OU name for statistics to aggregate on

In all cases, the library will need the names of the attributes for the next part of the set-up. Attribute names are case sensitive and may not contain spaces.

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 passed it by your souce
    - OpenAthens will cache these attributes when the user signs in, so changes in your directory 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

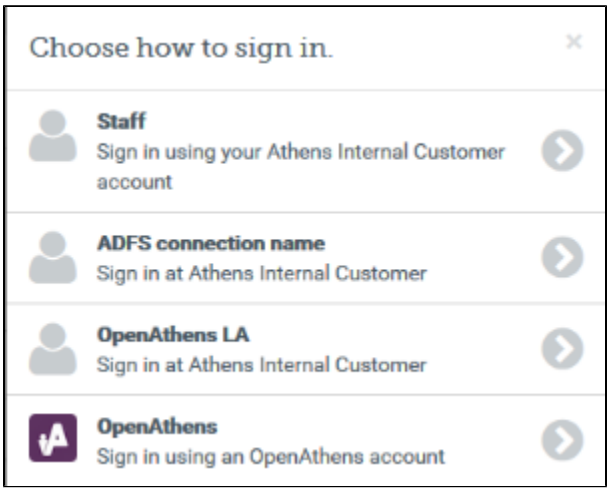
Discovery is not available until you set the connection as live and visible so that users do not get offered options that are not ready to be used. To test your connection you will need to use debug mode to make the connection selectable by you.

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.



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 your end 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 you are planning to pre-upload user identifiers, you will need to have at least one local account visible in the list to access the upload button. Do not delete all your test logins until at least some of your pre-mappings are uploaded.

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.