How to handle walk-in users

"Walk-in user" is a common term for people who are allowed to use your library but are not otherwise part of your organisation - e.g. a University Library might have an arrangement with the local community that the general public can access library resources if they come into the library buildings.

Access accounts

OpenAthens offers an account type known as an 'Access account' which is great for walk-in users because that type can be shared amongst multiple users and has an IP based restriction on it so that you can limit it to your network or even (with the help of your IT team) to the specific computers used by walk-in users. The IP restriction means that it is perfectly acceptable to do things such as post the credentials on a sign on the wall or similar.

To create an access account, select it as the option in the Accounts > Add menu (for details see: Add - Access account).

The access account will access resources like any other account except for the location restriction. It's only really necessary though if you are offering resources that don't use IP as the authorisation method.

If you are using local authentication

If your site uses local accounts - i.e. you have connected OpenAthens to your own directory for authentications - then access accounts are still likely to be the best solutions for walk-in users as each ID your systems pass to us must represent an individual... and it is often the case that sites do not want to create those records for walk-in users anyway. The practicalities of the access accounts in use are:

If you are already using OpenAthens accounts alongside local accounts

Access account credentials are submitted in the same way as any other OpenAthens account, so your existing procedures can still apply

If you are using the LDAP or Sirsi connector

The username and password fields on the authentication point will accept the access account credentials without the need for any changes. You can update the username and password labels if necessary.

If you are using a SAML or API connector such as ADFS, Azure, Google, CAS

There are two options:

1. Enable the function that presents users with the option to sign in with either type of account
    - This will display the option to all users at least once - the user's choice is remembered so users should only see it once on their personal devices
    - If regular users and walk-in users access the same terminals, the choices of one group may impact the experience of the other group depending on how your terminals handle cookies
    - You will have to remove the default flag from your connection
2. Ensure the walk-in users sign into OpenAthens before they try to access any content
    - This can be as simple as sending them to MyAthens (https://my.openathens.net)

Advanced options

As well as an API connector which will start an OpenAthens session based on your authentication process, we also have an API based option to start a session for an OpenAthens personal or access account. Depending on how walk-in users access your terminals, your IT team may be able to use this functionality to both simplify and even hide the process from walk-in users. See: Generating authentication tokens for end-users via the API

Licensing

You will no doubt have checked that the licences you have for the content you are providing covers use by walk-in users... but you also need to check with the publisher that it covers access by the methods you will be using. Some publishers may not be willing to provide federated access to potentially unidentifiable users. Should such a case come up you will have to fall back to IP authentication for walk-in users for that content.

Restricting which resources an account can access

If your walk-in users can only be allowed access to a subset of the resources that you subscribe to, you can restrict their access by using permission sets and restrictive mode. There are a couple of approaches:

1. If you do not already have any permission sets under the organisation you will need to create at least two
    a. One set for the walk-in users with the restricted set of resources allocated to it. Set its role as 'library-walk-in'.
    b. One or more sets for the regular users with the relevant resources allocated to them. The role for these is usually 'member'
2. Create the access account(s) for your walk-in users, assigning the permission set you created (Accounts > Add > Access account)
3. Allocate the other permission set(s) to the regular accounts if they are not already using them
    a. For OpenAthens accounts this is done via search or list results and the actions button - see: Search actions
    b. For local connectors this is done via the permissions tab on your connection - see: Permission set rules
4. If not already activated, turn on restrictive mode

1. Create a sub-organisation (Accounts > Add > Organisation). Do not assign it a unique identifier or scope.
2. Impersonate that sub-organisation
3. Create a permission set containing the resources available to walk-in users and set the role as 'library-walk-in'.
4. Create the access account(s) for your walk-in users, assigning the permission set you created (Accounts > Add > Access account)
5. Turn on restrictive mode (Preferences > Organisation)

The main factor in choosing an approach is how you want things to appear in the reporting interface - the sub-org option will not include the walk-in users in reports unless you change the scope of the report to be all organisations, whereas the single organisation option will include them all together and include the walk-in users' in permission set reports.

Anything else to watch out for

Some federations do not permit shared accounts and require that all users be uniquely identifiable (e.g. UK Access Management federation). Access accounts will not work for organisation / resource combinations within those federations where we know these restrictions exist.

Your browser does not support the HTML5 video element