hswaw - Bugless #35

kasownik/sso: allow access to people who are behind on their membership fees

03/24/2021 02:05 PM - q3k

Status:	New	
Priority:	Normal	
Assignee:		
Category:	hscloud	

Description

Currently, if you are INACTIVE, you can't log into kasownik to check your fees.

This is part of a larger problem, that SSO clients have no way of specifying which kinds of users should be able to log in, and I even think currently all are hardcoded to never let in inactive account.

Instead, we should support the following behaviours, I think:

- Allow every account to log in, as client will perform own checks against kasownik/capacifier/...
- Allow only paying members (ACTIVE) to log in
- Allow some other subset of members to log in (eg. LDAP groups?)

History

#1 - 06/12/2021 09:35 PM - q3k

Also, more generally: when attempting to access a service behind SSO when kasownik says you are 'INACTIVE' causes a shitty UX loop:

https://object.ceph-waw3.hswaw.net/q3k-personal/0325794ae36350960cc14d7e6e5da883e222ca25652452adad4a28302a08798b.png

#2 - 09/15/2021 08:12 AM - informatic

Inactive membership is carried out here https://code.hackerspace.pl/informatic/sso-v2/tree/sso/directory.py#n85 - if is_active() returns false the login process will still succeed (since it's not even checked here: https://code.hackerspace.pl/informatic/sso-v2/tree/sso/views.py#n63) but fail on another redirection, where login_required decorator is used (which actually checks whether or not an account is active)

IMO behaviour should be selectable in SSO-side OAuth2 client configuration, defaulting to current behaviour for most clients (but rejecting during actual oauth2 authorization flow, not in sso LDAP login...)

#3 - 07/04/2022 01:08 PM - q3k

- Category set to hscloud