CUNY Academic Commons - Feature #4635

Allow non-WP authentication

2015-09-18 09:16 PM - Boone Gorges

Status:	New	**Start date:**	2015-09-18
Priority name:	Normal	**Due date:**	
Assignee:	Sonja Leix	**% Done:**	0%
Category name:	Authentication	**Estimated time:**	0.00 hour
Target version:	Future release		

Description

The Commons was built independent of CUNY's central IT. We found it easier to use WordPress's native authentication rather than jump through the hurdles necessary to integrate with the CUNY Portal or other SSO services offered by CUNY. The Commons is in a different place today, and the technologies used for authentication by CUNY - as well as the technologies generally used for centralized authentication - are different from those in 2009 and 2010. It used to be a useful hurdle, and indeed a point of pride, that the Commons's separate registration was an obstacle for widespread use of the site. This is no longer true.

Let's use this ticket for some general discussion about improving login workflows. As we start to make decisions about priorities, etc, we can create separate tickets for specific tasks.

I think we should pursue two different strategies in parallel:
1. Allow authentication against CUNY identity systems. I guess this would mean the Portal, which I assume is powered by LDAP. But it could potentially mean integration with authentication systems on individual campuses, if we were insane enough to go that route.
2. Allow authentication with external OAuth providers. Off the top of my head, the obvious candidates are Google/GMail, Facebook, and Twitter.

Option 2 is nice because it'll cover a huge percentage of our user base, and it doesn't require permission from CUNY. However, we'll probably still need to check against a CUNY email account to verify that the user is a CUNY person. Option 1 is nice because, in theory, everyone should have an account; but it's also confusing because CUNY has so many logins, and I have no idea who we'll have to talk to to be whitelisted for their API. Going with option 1 first also means that we won't have to redesign the registration flow - we can do the normal send-an- activation email step, or even skip it, while in the case of Facebook etc we'll need to have an alternative flow for verifying CUNYhood.

In either case, we can probably use the authentication API to pull more than just authentication data - stuff like email addresses, first/last names, contacts, etc would be possible down the road.

We'd need workflows that account not only for new members, but also for existing members who want to log in using another auth system - a "claim your account" system, maybe. And we'll probably need to redesign/customize the login flow to account for the multiple login possibilities.

What do people think? Where should we focus our energies first?

History

#1 - 2015-09-21 11:33 AM - Michael Smith

One thing to note about the CUNY authentication method. There are actually three possible certifications to choose from with each CUNY person:

1. CUNYFirst
2. cuny.edu
3. Campus specific LDAP

I would imagine working with CUNYFirst is the least likely to be used platform given that security concerns would be largest. Cuny.edu though is already used to authenticate a number of different systems (portal, degree audit, blackboard, etc.), so precedent to add the Commons could rely on this fact. And I can't even imagine trying to corral all the CIOs at each campus. We could try cascading through them adding each campus as they become willing partners, but that might cause a lot of confusion.

As for the OAuth option, I'd define to others to continue this discussion. I generally avoid it unless the application/service are more deeply connected. But that's my personal issue with connecting everything to big name social accounts.

#2 - 2015-09-21 11:37 AM - Boone Gorges

Thanks, Michael! I definitely agree that it's unlikely that we'd be able to connect to CUNYFirst. Given what I know about their system, it's likely that their authentication is totally internal (it doesn't have any way for external applications to use it via API), and that they have neither the ability nor the interest in turning into a more general service. The cuny.edu authentication service (the Portal) is already a single-sign-on application, so the infrastructure is, at least in theory, already present to do what we're talking about here. (Agreed about campus-specific LDAP - I was throwing it in there for completeness.)

> As for the OAuth option, I'd define to others to continue this discussion. I generally avoid it unless the application/service are more deeply connected. But that's my personal issue with connecting everything to big name social accounts.

I don't think it's an option we need to push, and I don't think we're currently looking to do any sort of deep integration. The point is to reduce username/password fatigue. We'd make third-party authentication available as a service to those who'd prefer using it. Local WP authentication isn't going away.

#3 - 2015-09-21 03:04 PM - Matt Gold

Thanks, Boone and Michael. I would suggest that as a first step, we get in touch with CUNY CIS to see what is possible with regard to various handshakes with CUNY authentication system. Boone, would you be willing to write an email that I could forward on to serve as a basis for discussion?

Though I recognize and to some extent share Michael's concerns, I do think that provided access to the Commons through commercial social networking services would be a plus for our users.

#4 - 2015-09-21 11:21 PM - Boone Gorges

- File cac-portal.txt added

> Boone, would you be willing to write an email that I could forward on to serve as a basis for discussion?

Sure thing. I've attached a draft to this message (cac-portal.txt). Please edit at will, and feel free to include my contact info if they want to reach out directly to me.

#5 - 2017-08-25 04:04 PM - Matt Gold

Hi All,

I wanted to bump this thread -- around OAUTH logins rather than CUNY IT logins -- to see whether we could include twitter/google logins for existing users. It seems to me that this is something we can discuss around the issue we described today in helping the CAC work better with third-party services.

Boone, can you please let me know whether you think this is something we might shoot for one of our releases this year? The idea would be that existing users would be able to connect their CAC accounts to twitter/google accounts and would be able to log in to the CAC through them once they had set up that connection

#6 - 2017-08-25 04:30 PM - Boone Gorges

Yes, we can do this. I suggest we start with a single provider - maybe Google is the best choice? - so we can figure out the workflow.

The main issue will be how users set up the connection between their Commons account and their Google account. Scenarios:

1. Existing Commons user who wants to link to a Google account
2. New user who wants to register using Google credentials

I think we have to disallow 2, since it doesn't give us the cuny.edu verification step.

We'd need to draw up some sort of workflow. Like:
a. A new Member > Settings page along the lines of "Link to External Acccounts" which will walk through the oAuth process, and will also have a mechanism for unlinking existing accounts
b. A link on the existing login screen(s) that allows 3rd party login

So there's some thought that needs to be put into the UX.

#7 - 2017-08-25 05:34 PM - Matt Gold

Great. And, yes, starting with a single provider sounds good, as does the choice of Google. I agree that this should only be allowed for existing users. I just think we should surface it on the login screen so that people realize they can set it up. Which is to say that, yes, there are multiple UX issues to consider.

#8 - 2017-08-25 06:22 PM - Boone Gorges

- Assignee changed from Boone Gorges to Paige Dupont

- Target version changed from Future release to 1.12

Let's try to do this for 1.12.

Paige, can you please have a first look? We'll need new interface corresponding to (a) and (b) in my comment here: https://redmine.gc.cuny.edu/issues/4635#note-6 It may be instructive to see how other sites handle this, especially in the case of item (b) (login page). Item (a) is more specific to the Commons, so we may need to invent something from whole cloth.

Rough wireframes that we can use as a starting point for discussion would be great. Let me know if it'd be helpful to have a chat before you get started.

#9 - 2017-08-27 02:21 PM - Chris Stein

Hi All,
I think that in general this is a good idea. But I want to play devils advocate and want to better understand the reason to do Oauth with Google right now. If we don't also have something like the ability to in life Google Docs what is the benefit now to our users?

Also, why would we do this before looking into integrating with the CUNY SSO system that is now well on its way?

#10 - 2017-08-27 02:37 PM - Matt Gold

Hi Chris --

We created this ticket a few years ago because it seems like most modern sites requiring membership now allow people to login through OAuth using third-party services. The central goal is to make login easier rather than necessarily to key into something like Google Docs. I revived this ticket during the last CAT meeting, actually, as I watched someone try to log into the CAC -- a bit of guerrilla usability testing!

I think the reason to do it before integrating with CUNY SSO is that this is something we can control, while CUNY SSO is still in development. Once that service is set up and available to us, we can and should use it, but I don't see this ticket as getting in the way of that -- on the contrary, doing this work now will better pave the path for integration once it is available.

#11 - 2017-08-28 12:52 AM - Chris Stein

Thanks for the further clarification Matt.

Paige, here are my thoughts on the reasons for this and the UX/UI elements to be addressed: (if anything seems wrong here anyone please correct me)

- The current primary reason for this is that people can't remember their Commons user/pass and so have trouble logging in.
- People who log in infrequently (or haven't for a while) are the primary audience.
- This solution is to allow them to log in using an account they do remember.
- We have chosen to use Google because a)we want to start with just one, b) we are assuming most people have a Google account (or at least more than other services)
- We are also choosing Google because CUNY SSO is not ready. Is that true? Have we discussed this recently with CUNY CIS?
- It will need to be clear to people that they can't create accounts this way (Google account).
- We need to look at the Registration process and see if we can add this third party account link to that process. I think that if we're doing this to help people who can't remember their login info then allowing them to link as soon as possible is most helpful.
- Consider adding the third party login link to the Forgot Password page as well.
- We will need to create a publicity plan to notify people this is possible.
- There will need to be a place in the profile area to manage third party accounts. Look at existing account management interfaces (like Apple's Internet Accounts) to see how others are doing it.
- Eventually this account management interface will expand to include more third party services and possibly to manage deeper links with those services (like using Google Docs, or sending tweets from Commons, or a Share button etc). That is not part of this round.

On the technical side it seems as though pursuing third party account links is different from CUNY SSO integration. I'm going to add some of those here. If I'm wrong, please correct me.

- third party logins are added AFTER account creation. Account creation cannot be integrated through them.
- Initially Third party accounts would be used primarily for login. The account connections will allow for different and deeper integration in the future.
- CUNY SSO CAN be used for account creation. We haven't fully looked into this yet so there are still questions like: does the user also need to create a WordPress user/pass; what happens when the person leaves CUNY; how we would link existing users to their CUNY accounts (but presumably similar to that of third party).

#12 - 2017-08-28 09:13 AM - Luke Waltzer

I missed the meeting, so sorry if all this has been addressed, but I'm not sure I fully understand the benefit of doing this. One still has to log into the Commons the first time via a CUNY email. Will this functionality allow users who are logged into the browser with their Google account to automatically be logged into the Commons via cookie? I suppose that's a benefit. But the primary benefit of the third party OAuth integrations is the time it saves at the point of account **creation**... I've never encountered a system that requires local accounts and THEN allows users to link them to third party accounts. Do we know of any?

If the development lift is minor and we can contain complexity, then I guess this makes sense, especially if we can be sure it will pave ways for integration with SSO/Portal/Whatever down the road. But we have refrained from letting users who can't remember their logins shape our priorities in the past, so I'm not certain we'd be getting that much benefit from this.

#13 - 2017-08-28 03:36 PM - Boone Gorges

I'm with Chris and Luke that the feature, as described here, is not very useful at this point. It will essentially allow users to log into the Commons once using their Commons credentials, link their account to Google, and then never use their Commons credentials again. IMO, this is a pretty marginal direct benefit.

Indirect benefits:

1. Google account linking will be a critical piece of any deeper Google integration. Doing this work now means less to do when/if we have deeper integration.
2. The various user flows for managing Google account links (registration; login; password reset; account management) will all need to be built in order to support any third-party auth system, including CUNY's.
3. Google Accounts generally have Gmail accounts, which means we could automatically set the Google email account as the preferred one (though this'd have to be optional and would have to support our email verification flow - see below)

I agree that we're really minimizing potential benefit if we don't allow this feature at registration. Yet we still need to do cuny.edu email identification. So what we could do is: During registration, allow a user to link to Google. If this happens, the user won't need to provide a password. But she'll still need to provide a CUNY email address, to be used for verifying CUNY membership. We may then want to have a selector along the lines of "Use the following email address for Commons email", where the user can select between the Gmail and the CUNY account.

I don't think it will actively hurt to put this feature in place now, even with its limited benefit. I'll leave it up to the team whether they think it's worth the (non-trivial but not enormous) development and design resources required.

#14 - 2017-09-19 11:55 AM - Paige Dupont

- File integration 1.png added

- File integration 2.png added

- File integration 3.png added

- File integration 4.png added

Hey all,

After combing through the information from the open entry forms on our survey the integrations most wanted was Google (for Google groups and calendar integration specifically) and (only a few) Twitter (tweet out events or accomplishments within the Commons, share a social paper, etc.). I think for the time being we should focus our attention to integrating Google as we had spoke about earlier. Overall, it's nice to know that we have user interest in this integration/feature.

I've been doing a competitive audit of other site to see how they have been incorporating the Google sign in and the ideal example (in my opinion) was Chase's integration and deletion structure. I have attached the flow for you to view. It was simple and allows for the user to revoke access to their Google accounts.

The flow also takes into consideration one email address being associated with the account entirety, therefore in our case, if a user decides to sign in with Google (after signing up in with the CUNY authentications) Google will then be their primary account for notifications UNTIL they decide to deactivate it.

Boone, if you would like, I'm happy to create wireframes for you to see this with the Commons skin (primarily the deletion feature in the settings).

#15 - 2017-09-19 04:19 PM - Boone Gorges

Thanks for your research on this, Paige! I also like Chase's flow. A couple questions:

1. Is there a way to link the Google account aside from at the time of login? WordPress's authentication cookies can be long-lived - up to 30 days - so people may not log into the site frequently enough to notice this. I'm also imagining future documentation for setting up Google integration: it feels awkward for the first steps to be "1. Log out of the Commons. 2. On the login page, click Google...". It feels like there ought to be an interface in user settings for this. Probably under "Connect Social Accounts" https://redmine.gc.cuny.edu/attachments/download/6408/integration%204.png - when you're not connected to Google, you'll see a 'Connect...' button instead of 'Disconnect...'

2. What to do about the small 'Log In' dropdown at the upper right (on the admin bar)? Personally, I almost always use this instead of wp-login.php. Let's be sure to include this in design.

3. Can you talk more about how the login flows work after integration? I'm thinking of a couple cases:
a. You're logged into Google but not explicitly into the Commons. When you visit the Commons, should you be automatically logged in, without prompting? Or should you be shown the 'Log in with Google' button, which will then log you in without further prompts (since the initial setup is complete)? (I think the second option is better, in part because of item (c) below.)
b. You've linked your Google account, but you want to be able to log in with your old Commons credentials. Do we continue to allow this? (I think yes, since some users will be linking accounts primarily for data integration rather than authentication.)
c. Google allows you to switch between accounts in your login session. How do we deal with this? Should WP login cookies be invalidated? (I think no: logout should be independent and specific to WP only, since login will likely require a button click. See (a) above.)

4. You say that linking a Google account will automatically change the notification email. This seems bad to me: Personally, I use a Google account for Google services, but I don't prefer it for email. What's the argument for forcing this? Perhaps we could merely suggest it, as part of the linking process - an optional checkbox "Make this my primary email account for notifcations from the Commons" or whatever.

5. We could potentially add something to the Settings > Email interface so that, if you enter an account ending in @gmail.com, and you haven't yet linked your Google account, we show you a message encouraging you to do so.

#16 - 2017-09-27 03:03 PM - Boone Gorges

- Target version changed from 1.12 to 1.13

#17 - 2017-09-29 11:43 AM - Paige Dupont

- File RH login.png added

- File Calendly1.png added

- File Calendly 2.png added

- File Switch Accounts.png added

Hey Boone,

All great questions. As always please let me know if any of this doesn't make sense or needs clarifications.

Here's what I'm thinking:

> 1. Is there a way to link the Google account aside from at the time of login? WordPress's authentication cookies can be long-lived - up to 30 days - so people may not log into the site frequently enough to notice this. I'm also imagining future documentation for setting up Google integration: it feels awkward for the first steps to be "1. Log out of the Commons. 2. On the login page, click Google...". It feels like there ought to be an interface in user settings for this. Probably under "Connect Social Accounts" https://redmine.gc.cuny.edu/attachments/download/6408/integration%204.png - when you're not connected to Google, you'll see a 'Connect...' button instead of 'Disconnect...'

I agree, that makes sense. It would serve as a good catch for users that prefer making these types of changes in a ‘settings’ atmosphere.

> 2. What to do about the small 'Log In' dropdown at the upper right (on the admin bar)? Personally, I almost always use this instead of wp-login.php. Let's be sure to include this in design.

You’re right, I also use this as my primary entry point. Here’s a quick first pass of what that might look like. (See RH login.png)

> 3. Can you talk more about how the login flows work after integration? I'm thinking of a couple cases:
> a. You're logged into Google but not explicitly into the Commons. When you visit the Commons, should you be automatically logged in, without prompting? Or should you be shown the 'Log in with Google' button, which will then log you in without further prompts (since the initial setup is complete)? (I think the second option is better, in part because of item (c) below.)
> b. You've linked your Google account, but you want to be able to log in with your old Commons credentials. Do we continue to allow this? (I think yes, since some users will be linking accounts primarily for data integration rather than authentication.)
> c. Google allows you to switch between accounts in your login session. How do we deal with this? Should WP login cookies be invalidated? (I think no: logout should be independent and specific to WP only, since login will likely require a button click. See (a) above.)

a. I agree with the login with google button. I've attached a flow I use with Calendly that I think highlights this function pretty well.

b. Yes, I think we should allow it. I’m thinking a user would be able to do this in two ways. First, the disconnect the account (from a settings page, similar to the Chase flow) AND upon logging back in or if a user actively logs out of the Commons.

I don't know how much time needs to pass for a user to be automatically be logged out currently- (I'm sure you know) but if a user comes back to the site and hits log in we can show them something like the mock up "Switch Accounts" that I've uploaded.

This is a rough pass with much more thought needing to be put in but I want to let you see where I imagine this going.

c. I see where your concern is, I think we can allow for a user to change accounts but this would work as an edit – rather than adding numerous google accounts we can make this a one gmail account rule – logging in with a different gmail will deactivate the previously used account. Unless you see this not really being a problem in the long run.

> 4. You say that linking a Google account will automatically change the notification email. This seems bad to me: Personally, I use a Google account for Google services, but I don't prefer it for email. What's the argument for forcing this? Perhaps we could merely suggest it, as part of the linking process - an optional checkbox "Make this my primary email account for notifcations from the Commons" or whatever.

You’re right, there is no need to force this – I agree with you that we can make this a choice for the user to make. We can discuss copy and whatnot as that comes.

> 5. We could potentially add something to the Settings > Email interface so that, if you enter an account ending in @gmail.com, and you haven't yet linked your Google account, we show you a message encouraging you to do so.

You mean like a reroute? I think this could work – Do you imagine that this would only occur at login, in settings or both? I see a case for all.

#18 - 2017-09-29 01:38 PM - Boone Gorges

Thanks, Paige.

RH Login looks OK to me, though it really foregrounds the Google login. We should perhaps have a discussion about how much we want to publicize this feature before we give it such prominent placemnet.

> You mean like a reroute? I think this could work – Do you imagine that this would only occur at login, in settings or both? I see a case for all.

No - I mean that if you're changing your email address (profile > Settings), and you enter foo@gmail.com, a little notice shows up that says "Did you know you can link your Google account to your Commons account...." and links to that interface. Nothing automatic - just a notice.

#19 - 2018-03-22 10:35 AM - Boone Gorges

- Target version changed from 1.13 to 1.14

Let's pick up discussion of Google integration after the 1.13 release.

#20 - 2018-09-27 05:24 PM - Boone Gorges

- Category name changed from Registration to Authentication

- Assignee changed from Paige Dupont to Sonja Leix

- Target version changed from 1.14 to 1.15

Sonja, this ticket is long and complex, and I don't think it's feasible to take any steps on it for the 1.14 release. But it's something we can talk about in the context of Commons infrastructure improvements over the next semester or two.

#21 - 2018-10-03 11:51 PM - Sonja Leix

Boone Gorges wrote:

> Sonja, this ticket is long and complex, and I don't think it's feasible to take any steps on it for the 1.14 release. But it's something we can talk about in the context of Commons infrastructure improvements over the next semester or two.

Thanks Boone! I think you're right, it's not feasible for 1.14, but I can start working on this for 1.15 once we worked through the issues of this release.

#22 - 2019-03-01 02:05 PM - Boone Gorges

- Target version changed from 1.15 to Future release

The strategy here is not yet clear. Let's reattach to a milestone once we have a sense of how this fits alongside other priorities.

Files

cac-portal.txt	2.42 KB	2015-09-22	Boone Gorges
integration 2.png	91.2 KB	2017-09-19	Paige Dupont
integration 3.png	107 KB	2017-09-19	Paige Dupont
integration 4.png	81.6 KB	2017-09-19	Paige Dupont
integration 1.png	128 KB	2017-09-19	Paige Dupont
RH login.png	83.3 KB	2017-09-29	Paige Dupont
Calendly1.png	59.7 KB	2017-09-29	Paige Dupont
Calendly 2.png	87.1 KB	2017-09-29	Paige Dupont
Switch Accounts.png	22.7 KB	2017-09-29	Paige Dupont