Authentication Focus Group (AFG) Report Regarding Ex Libris' Plan to Terminate Support for Alma Internal Password Authentication

Background

At the September 2016 IGeIU meeting, Ex Libris announced its plans to move toward the use of external-only password management in Alma. This shift would affect customers' ability to create patron and staff accounts where the password is stored within Alma. A joint ELUNA/IGeLU External Authentication Focus Group (AFG) was formed to work with Ex Libris to determine the best course forward.

In subsequent meetings between the AFG and Ex Libris it was confirmed that Alma external-only authentication was not a requirement of the ISO/IEC 27018 (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.) This was cited by Ex Libris as the reason users needed to move away from using internal passwords. Rather, the need for Alma external-only authentication is a suggested best practice that Ex Libris would like to strictly adhere to the practice.

The AFG developed the *"Alma Password Authentication Survey: Assessment"* tool to assess how each Alma institution is using password control within Alma. Additionally, the AFG wanted to determine the degree of impact a move to external-only authentication would have on institutions.

This report presents findings from the survey and offers recommendations to Ex Libris, the IGeLU and ELUNA Steering Committees, and the Alma community as potential next steps.

Survey Results

A total of 193 Alma institutions responded to the survey. This is nearly 25% of the institutions contracted, in implementation, or in production on Alma and meets statistical sampling requirements.

Ex Libris staff indicated that 5% of accounts within the Alma install base used internal authentication. This statistic focused on the aggregate number of accounts and not institutional usage. The AFG survey attempted to address that level of impact.

The majority of institutions who responded indicated that they were using internal account authorisation, at least to some extent.* Refer to Attachment 1 - *Why Institutions are using Internal Accounts* for more detailed information on institutional use of internal passwords.

Respondents indicated the type of password management enabled for staff operator accounts as:

- Mix of Internal and External Authentication 36.3%
- External Authentication Only 22.3%
- Internal Authentication Only 41.5%

Count of Type of password management enabled for staff operator accounts
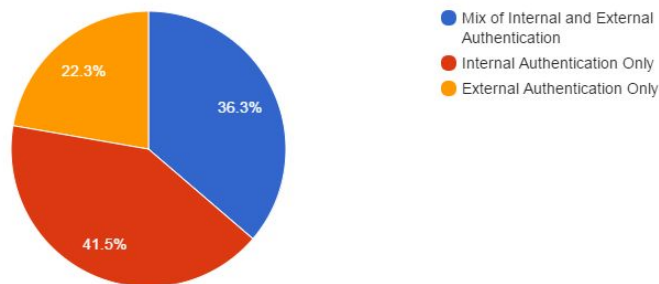

*At present, it is likely that all institutions have at least a few users using internal account authorisation, including admin and Ex Libris users. It appears that some institutions did not count these.

57.3% of responding institutions indicated that they used generic staff accounts for operations such as circulation. Refer to Attachment 2 - *Why Institutions are using Generic Internal Accounts* for more detailed information on how and why these generic staff accounts are being used.

Respondents indicated the type of password management enabled for Patron accounts
- Mix of Internal and External Authentication 62.7%
- External Authentication Only 23.3%
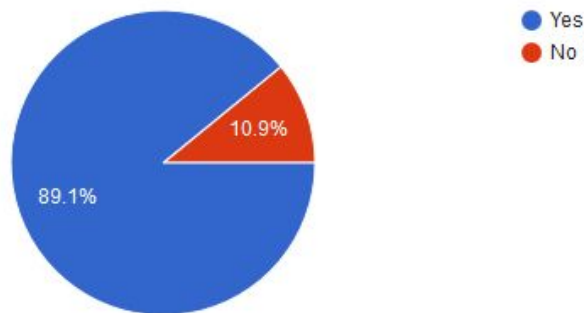- Internal Authentication Only 14.0%

Type of password management enabled for Patron accounts
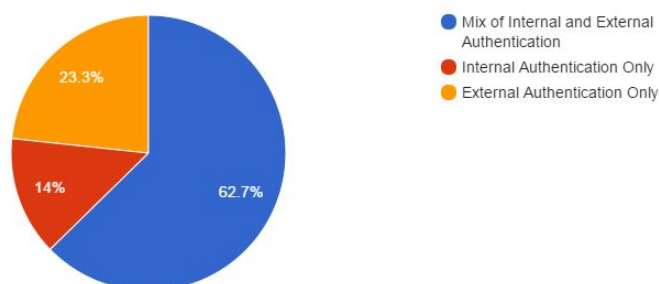
89.1% of responding institutions indicated that they provided accounts to non-affiliated users. Non-affiliated accounts are made up of members from the general public, members of other academic institutions, and alumni.

## Do you provide accounts for users not affiliated with your organisation?
(193 responses)

- ● Yes
- ● No

89.1%
10.9%

76% of responding institutions indicated that they rely on Alma for password management for non-affiliated accounts.

What type of password management is enabled for non-affiliated accounts?
(172 responses)

- ● Internal (inside Alma)
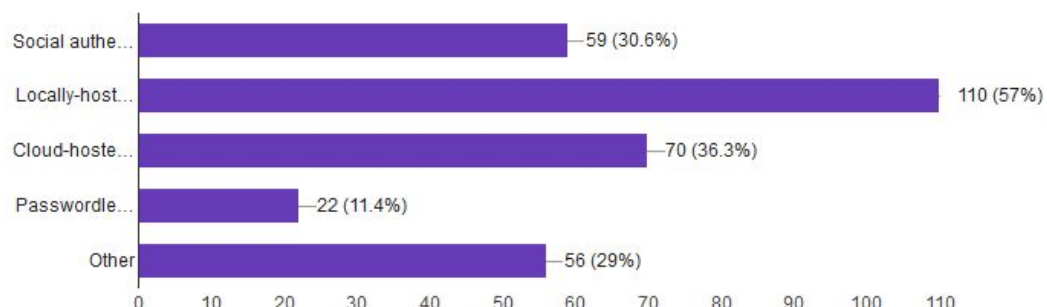- ● External authentication system
- ● Mix of Internal and External

10.5%
14%
75.6%
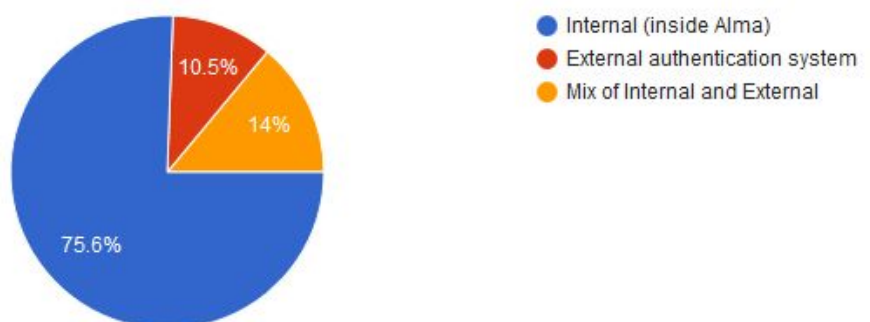
30.6% of responding institutions indicated that social authentication may be a possible option for internal password authentication. *This suggests that 69.4% of respondents are not willing or able to use social authentication.*

When internal authentication inside Alma is no longer available, which possible future solution(s) are you likely and allowed to implement? (Please verify with your IT Department about these possible future options)

(193 responses)

| Option	Count
Social authe...	59 (30.6%)
Locally-host...	110 (57%)
Cloud-hoste...	70 (36.3%)
Passwordle...	22 (11.4%)
Other	56 (29%)

11.4% of responding institutions indicated that passwordless authentication may be a possible option for internal password authentication.

61% of responding institutions indicated that their institutions would not allow them to store existing Alma internal authenticated passwords in their central authentication system. While it is technically possible to use central authentication systems for this kind of password management, it appears that local institutional policies often forbid storing non-affiliated users accounts in the central authentication system

34% of responding institutions indicated that they will probably not be ready to move to an external-only authentication system until after 2018. Refer to Attachment 3 - *Reasons why Institutions cannot move to an alternate system until after December 2018* for more detailed information.

Institutional preparedness required to move to external-only authentication can be summarised by the following chart

How well prepared would your library and/or IT partner be to complete a move to external authentication for all users by
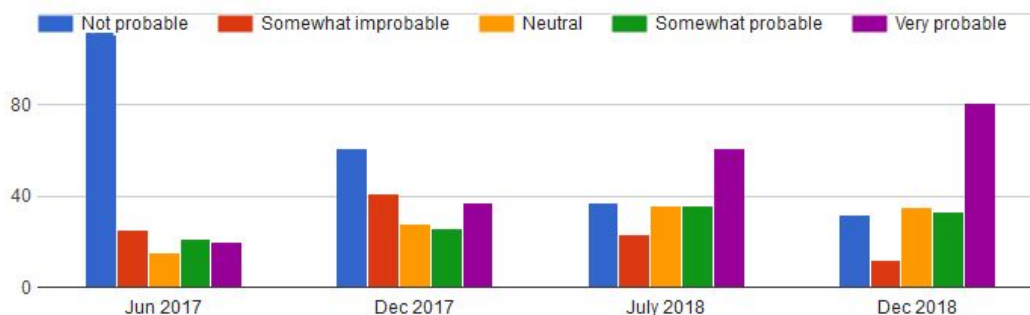
Institutional Interviews and Email Feedback

In addition to the survey, the AFG also conducted interviews with selected sites and compiled email responses from the Alma customer base. Information collected indicates a high level of frustration regarding the removal of internal password control. Quotes and comments from sites are as follows:

- One institution stated that *"moving from internal to external authentication so soon after a system migration will have a negative impact on customer service."*
- One library reported that they were institutionally mandated to serve [close to 5000 state] licensed health professionals, affiliate faculty, researchers, and some clinical staff from affiliate institutions. "The mandate is not negotiable. It is a core service required by the vision statement for [the university]. … if this change had been implemented before we had Alma, it would have eliminated them from consideration."
- One consortia office stated that they *"currently create an Internal account [in] Alma when the record has not yet been imported from the student system -- this is done as institutions do not want to turn away students as this produces a negative view of the library -- the inability [to create] an internal account is a major issue to the consortia."* Further, they said that "*This [change to all external authentication] will have a major impact on the consortia and as a result member institutions will blame the consortia office for this change and not Ex Libris as member institution[s] deal with 'the Consortia Office' and not ExLibris."*
- Another Consortia Office indicated that this will have a major impact on their member institutions and some of the institutions may not be able to migrate to an External Authentication System; as a result the Consortia Office will be disappointed at the implementation of this change.

Some of the institutional responses from the survey are as follows (this is only a subset and the AFG recommends that Ex Libris read the full list of comments supplied as attachments to this report)

- Transition to external-only password control will incur an initial project cost that has not been budgeted. In addition there will be an ongoing annual cost that will mean an increase in the Institution's base operating cost
- Transition to external-only passwords will mean delaying planned IT projects
- Some institutions cannot move to an external-only password solution and may need to look at alternatives
- If Ex Libris cannot protect passwords how can they protect patron information
- Ex Libris has always stated that Alma would mean less local ICT support will be required -- this new direction in password control means that ICT support is now needed again
- This is a loss of functionality -- the institution migrated to Alma as one of the important requirements was the ability to handle internal and external authentication running in parallel for different user groups
- Institutional policies will need to be changed and this will not be an easy or quick change and at this stage cannot be guaranteed

- An internal-only admin account is essential to troubleshooting issues with any authentication providers, is Ex Libris willing to do this task as the library will be effectively locked out of the system
- We would have to contract a service provider for external authentication. We don't have the budget to do this. On top of this, we have patrons from age 4 upwards. Librarians create accounts for them. It is paramount that this continues to be possible.
- Our IT department is understaffed and overworked
- We do not have the infrastructure or resources to employ an alternate authentication system, and it is non-trivial for us to introduce non-student, non-faculty/staff into our authentication workflows.
- We will NEVER allow external authentication for community borrowers. When we set up external authentication, it will be for current faculty, staff and students and will give them access not just to ALMA, but to our other electronic resources. These resources are licensed for use by faculty, staff and students only.
- Authentication for non-[university] members will require a separate system that has not been developed yet and [the university] may not see a reason to invest in that when we're already paying an external company (Ex Libris) for a product that is supposed to take care of that.
- We do not have a solution for this. We only use internal accounts. According to our procurement we asked for a system with the possibility to create accounts for our users with username and password.
- One Institution selected Alma on the understanding that all our users would be able to login to check loans, reserve items, etc. It was mentioned in the tender documentation and discussed at the system demonstration. For Ex Libris to announce that this would no longer be possible without considerable extra work on our part 4 months after going live will raise big questions with our Purchasing Department.
- Our university will not add people not affiliated with the university to the authentication system
- State regulations limit sharing of personal data; social media authentication is not an acceptable option
- Consortia Office comment: All users are internal at the moment. Not sufficient IT support to setup SIS file process. No external authentication method. Social login is of interest but could only be a solution for some patrons
- One library IT service was directed by their members to provide an external authentication mechanism within the next 6 months as a result of this communication [regarding the change in authentication.] Pain-points listed by the institution included the maintenance of password reset pages across various institutions, provision of verification services, figuring out how non-person accounts work in Interlibrary Loan (via NCIP) and making sure all member libraries have unique IDs across the entire system. From the interviewee's perspective, the important thing to note was that password storage was a small piece of the overall work being asked of institutions in this proposed transition.

Summary

Nearly a quarter of Alma institutions contracted for, in implementation, or in production (193 of ~700) responded to the Authentication Focus Group's (AFG) survey. This is a statistically significant survey result that the AFG feels is an adequate reflection of the overall Alma community.

Over 75% of survey respondents indicated that they use internal authentication exclusively or a mix of internal and external authentication. It is likely that every institution has at least one internal account to allow an institutional "backdoor" should there be problems with external authentication. Every institution has at least one internal account for Ex Libris staff. Ex Libris indicated that they would create an external authentication system for Ex Libris accounts, so these will no longer be a concern. Over 50% of the respondents use shared/generic accounts and 72% have community users authenticated internally, because their institution's external authentication can't handle these types of users or their institution doesn't have external authentication at all. The most critical use cases for internal authentication in Alma are those institutions that do not have the capacity or are bound by policy or regulations to authenticate users internally.

The second part of the survey was to gauge interest in possible solutions. While almost 31% of respondents indicated that the use of social media authentication might be a possible alternative to internal authentication, nearly 70% responded negatively to this solution. Very few institutions indicated passwordless authentication as a viable option, but given the questions received about this option, it is possible that the concept is not well known among respondents. The majority of respondents indicated they could not move their internally authenticated users to their central authentication service because the users were not affiliated with their institution.

The answers to the survey preparedness questions indicated that more than a third of the respondents would likely not be able to move entirely to external authentication before the end of 2018, largely because of scheduling, costs, capacity, and maybe even desire. To be fair, institutions couldn't provide more exact time estimates for a migration without knowing what the solutions would be or what help would be provided.

The survey was designed to gauge impact and readiness regarding an anticipated move away from internal authentication. The numeric results tell only a partial story. Many, but not all, institutions should be able to handle a move to external authentication depending on the potential solutions, although not likely as quickly as Ex Libris would like the move to happen. However, textual responses, answers to in-depth interview questions, and unsolicited calls and email correspondence via ALMA-L indicate to the AFG that there is widespread unhappiness, frustration, and sometimes anger regarding this issue. The AFG strongly encourages Ex Libris staff to take the time to read all comments.

Ex Libris staff acknowledge that the announcement of the move could have been handled better. Institutions were unaware that the release of a new social media authentication integration was not just an option, but was intended as a likely means for institutions to move away from internal authentication. Apparently, support staff mentioned the move in an answer to a customer, forcing Ex Libris to announce this "required" move at IGeLU. As is often the case, communication did not

move swiftly through the company and sales and support reportedly were still telling customers they could use internal support even after the IGeLU conference.

Some institutions commented that internal authentication was one of the reasons they bought Alma. They do not have capacity nor do they want to move away from internal authentication (e.g. *We do not have the infrastructure or resources to employ an alternate authentication system.*) Many others cannot engage their own IT staff or central IT in setting up a new authentication system (e.g. *Ex Libris has always stated that Alma would mean less local ICT support will be required -- this new direction in password control means that ICT support is now needed again.*) The AFG heard a small number of comments from institutions who thought this might be a breach of contract (e.g. *We only use internal accounts. According to our procurement we asked for a system with the possibility to create accounts for our users with username and password.*) and more who considered the removal of internal authentication as a loss of functionality. Finally, there were comments directed at Ex Libris including the following from a member of a consortia *"I have lost faith in Ex Libris."*

The AFG acknowledges that some institutions, such as the State Library of Queensland, already have on their forward IT plan the migration of all Alma accounts to external only. The shift in password management by Ex Libris means that this may occur sooner than later.

While the AFG fully understands the security benefits to an all-external authentication system, we also understand that the work involved in such a move would be extensive, and in some cases not possible, for institutions. The AFG feels it is important that Ex Libris read all comments and take them to heart when considering the path forward.

Recommendations

Given that the move to external-only authentication is an industry best practice and not a certification requirement for Ex Libris, we do not feel a move to external authentication should be made mandatory for institutions already contracted for, in implementation, or live on Alma, especially if there are circumstances that make the move challenging. Based on the survey results, interviews, and discussions with Ex Libris, the AFG recommends the following:

1. The AFG or other standing committee should continue to work with Ex Libris to develop a list of viable potential solutions and migration paths for institutions that <u>desire</u> to move to external-only authentication. A suggested list of solutions, including potential issues and specifications should be available to institutions no later than the end of Q1 2017. Ex Libris might also consider partnering with customers as part of a pilot to establish a migration and maintenance process. These early adopters could act as champions for such a move..
2. Ex Libris should consider hosting an external authentication system in order to make the transition from internal authentication seamless to the user community. This would obviate concerns institutions have about contracting with a third party. The benefit is clear: ownership and management of authentication work would be supported by Ex Libris, while user and password management would still be under the control of institutions.

3. Ex Libris should continue to pursue alternative access via external authentication to allow local institutional administrators as well as Ex Libris staff to access Alma without relying on the institutional central authentication system.
4. The move to external authentication should not be mandatory for those institutions contracted for, in implementation, or production for Alma.

Attachment 1 - Why Institutions are using Internal Accounts

1	The only reason that need wish to retain a 'backdoor' internal password is for occasions when our enterprise system fails for some reason, as per our current Sandbox issue (Case 347507). If ExLibris could provide us another 'backdoor' quickly for such instances then we would have no objection to going all external.
2	It's against policy to add community users (eg alumni, external members, members from other institutions) to our Active Directory as this would give them access to other services they shouldn't have.
3	5 of 9 internal accounts are Ex Libris accounts for supporting/implementing Alma. 1 account is required as workaround to Case 220595 , 2 are YBP contacts, 1 is inactive local user from Alma implementation in 2013
4	We do use internal authentication in our Alma sandbox - this is so we can allow only certain users to test in that environment. To allow staff to use the Sandbox, (which has a copy of all our user accounts), we just convert their user record there from external to internal and set a password. Will you be providing a way to do something like this for Sandbox environments ?
5	1. The use of internal authentication for library staff provides a consistent method to identify and manage people who can login to Alma. a.)The separation of University records provided through the patron load and the creation of Alma staff records with Alma allows for a more robust way to manage the Alma roles. b.) Generic staff logins are used for permanent staff and students working on the Library service desks. c.) Staff at some branches are not employed by the University.)The current setup allows for the University records to be purged when someone leaves the Library, and for the Alma staff record and all activity associated with it to be retained for analytics.2. To provide services to user groups external to the University. For example:a.) District Health Boards â€" staff of Hospitals who share Library services with the University. There is no patron load available and there is no external authentication system available so these users are manually added to Alma and assigned an internal password.) Hocken Library â€" a research Library that offers walk in services to members of the public. On arrival members of the public are manually added to Alma and assigned an internal password. As a closed stack library this needs to be done immediately so that patrons can request items to be retrieved.
6	1. We do have a few internal records used by staff to login to Alma when the external authentication system is down/unavailable, and we would like to be able to continue to have an alternative method of access during such outages. 2. The 864 internal patron records in question 7 are primarily records used for ILL purposes before

	implementing Alma Resource Sharing. These records are not used by the libraries to login to Alma or Primo, they are administrative only.
7	Recommended by Ex Libris at implementation.
8	we use this for staff user accounts in case our locally hosted authentication method is not available
9	wanted to keep staff accounts separate from regular patron accounts
10	Because the external authentication method does not hold all our patron accounts, and for some not all the requisite data (e.g. library number which is in turn needed for physical access control).
11	At present our external authentication is tied to our student accounts system which does not contain records for staff or external users. We could probably link to our staff accounts, but external users have no account elsewhere in the university so provision would need to be made for this.
12	Carryover from Voyager
13	because our university LDAPs contains (and WILL contain in the future) ONLY data of staff & students
14	We used it because our previous library system managed passwords in this way and we thought it was a great idea. It keeps our two types of patrons separated in an easily identifiable way.
15	it is the University standard
16	Only for specific staff accounts
17	Move to ADFS. Not all user types are in University authentication domain i.e. SCONUL users, Visitors etc.
18	CAS, Shibboleth
19	I am actually answering "I'm not sure" to the previous 2 questions. We have great difficulty in getting changes made to campus authentication and we have used internal (Alma) authentication for those accounts that don't qualify for OSU's authentication system.
20	Users don't exist in institutions identity management system.

21	In Alma we use internal authentication for patrons that are not members of the institution.
22	Internal Alma-based authentication was adopted for all users who do not fall within the population managed by our institution's authentication process. Standard external authentication is used for employees and students, but library patrons who are not otherwise affiliated with the university are managed internal to Alma.
23	Some users are internal with external authentication. We have created internal users for some functions.
24	It is the most convenient way to provision an account for non university members, requiring no extra work after saving the account
25	We use internal authentication for community borrowers as they are not allowed to be added into our external system unless billing is involved.
26	Infrastructure to support external authentication to Alma was not readily available during implementation.
27	We have not been allowed to use any other method than authentication within the library system.
28	CAS was the only authentication mechanism that our IT dept were happy for us to use.
29	Because these community borrowers do not have network credentials. They have to be authenticated with a barcode. They are not directly affiliated with OHSU and will not be granted a network account. The library manages these users internally.
30	We don't have the authority to create usernames and passwords for Central IT's authentication system for Community Users. There was a security breach on campus, and now Central IT does not even provide us with test accounts for troubleshooting with ExLibris. Therefore, we are forced to use Alma authentication for these patrons.We also have some staff that have internal accounts, in addition to their external accounts. This was initially set up 1) to have working accounts separate from personal accounts and 2) as a fail safe to back up Central IT's authentication system. These internal accounts for staff are being eliminated.
31	recommendation from the ExL project manager -- also scripts / programs not in place to handle maintenance of these type of accounts into our central authentication system

32	Alma internal authentication was implemented since the Alexandria Library Network is heterogeneous and not all Libraries are grouped under the same IT Network/Department. There is no general authentication system available for all Patrons or Staff users. So patron and staff authentication needs to be built up outside (as in the Alma cloud).
33	Internal authentication provides users who cannot authenticate via university systems access online access to their account and related services in Primo.
34	Easiest, simplest solution of authentication of users with no connection to the university other than having library membership
35	Alma contractor implemented this at time of implementation.
36	We wanted to separate staff user records from patrons; currently use a script originally developed for Voyager for our non-university patrons and don't actively manage passwords for them in Alma.
37	Keele uses internal authentication for 2 groups of users: NHS members (for our Health Library) and users linked to the institution who aren't formal staff and students (eg SCONUL borrowers, alumni, paid members, etc). These groups are not recorded on University systems at the moment and therefore not on the University IDP.
38	This is a long standing approach for our libraries to provide courtesy, alumni and other non-affiliated patron accounts to serve the community at large. It is through this method that these patrons can access their library accounts and other library services through Primo without having to involve University Registration.
39	We use internal authentication for community users, interlibrary loan borrowing libraries, alumni. None of those people/organizations have accounts in our university authentication system. Our IT person says they can get it set up to authenticate them through that system, but I don't think he really understands what I'm asking. There are no people currently who can authenticate through out university system without having a university ID, which none of these users have.
40	Our IT Services wants only students and employees included in their authentication system.
41	We cannot add non-university users to the institution authentication system.
42	So we have control over patron data and can verify it.
43	Separates library accounts for working with Alma & Primo from accounts to check out material. If external authentication has problems, we can still access Alma. If external

	download of users has problems, we can still access Alma. Easier to remove student workers -- rather than edit access in their college account.
44	No other option available at the time of implementation for non-institutional library customers who need to log into Primo for loans, requests, renewals etc.
45	Legacy from Unilinc setup, we hope to move away from it once we are solo for those users which we can, i.e. INTERNAL operator users. Haven't crossed the bridge of NON-ACU users yet and what the plan for them will be.
46	Bulk of internal auth users are NHS. The NHS does not currently have an IdP we could plug into Primo/Alma, so internal auth was the only option. However, we can and are discussing this possibility with them. We may be able to persuade them to develop an NHS IdP (for Wales), but that is a long term project, and would need time to develop. (Hence preference for 2018 date in above question on timeline.) We cannot use social media auth for the NHS. Of course Primo/Alma would need to be able to have multiple IdPs configured for this option. We would need one IdP for the University (currently in use) and a second IdP for the NHS. I believe at the current time we can only have one IdP in Alma, and in the new Primo? Even if we persuade the NHS to develop an IdP, we would still need a method of authentication for members of the public, who are the other user group we have who currently use internal auth. At this stage I have no idea on what auth we would use for the public.
47	I answered 'yes' to say we could use our institutional authentication system for users with internal passwords, but actually we like the fact that Alma doesn't rely on the internal system for these users e.g. in the event that we have an institutional authentication failure library staff can continue to use Alma using the internal users. Any proposed solution will need to address this issue for us.
48	We are at the beginning of the implementation stage of Alma and have not yet loaded any user data. We expect to use internal authentication as we do with Aleph for users not in our institutional authentication system. We do not currently have an institutional authentication system that caters properly for the sorts of users we currently authenticate internally with Aleph, e.g. SCONUL users from other universities. As well as local authentication for such external users we also locally authenticate all users who use our Lapsafe self-issue system for the loan of laptops (using barcode and PIN). We expect to continue having to do so with the move to Alma.
49	Our library location at our teaching hospital does not have an authentication system - the only method they can use is internal.
50	To allow for relationships to continue from retired personnel
51	Voyager, no other authentication method available back then

52	Initially we added our internally authenticated users to University authentication systems, but this allowed them access to licensed materials which they should not have had access to. We had to remove them from the systems in order to remain within our licence agreements.
53	I don't believe CAS authentication was an option when we went live. In addition, CAS is not an option for community borrowers.
54	Because during our implementation, our SAML authentication never worked quite right for library staff users. Primo can authenticate, but not Alma.
55	we only use internal authentication for 2 test accounts (i.e. used to test Sentry) and one admin account should we not be able to log in with our external authenticated accounts
56	External patrons were not managed in the university authentication system and the solution was also sold by ExLibris as a simple and effective way to use Alma in small libraries and it is the typical way used by libraries to manage patron accounts. Organizations are simply not ready to do this big change, also because with Alma the role of IT department in managing library's applications were drastically reduced and this recent proposal would force to find unplanned resources.
57	We have community patrons who do not belong in our campus system.
58	We manage passwords in Alma only. Because of our security constraints at the Library of Parliament, we are not allowed to connect any internal systems with a system in the cloud (like Alma). So we can't connect Alma with our institutional client directory. We don't use LDAP or other types of identity management systems.
59	We are not able to add community users or users from consortial partners to the campus IDM system. We also use internal accounts for many staff users because it is easier to recognize the ID of the person who has completed a specific task or function.
60	We provide access for patrons that are not part of our campus' authentication database (e.g. community users, alumni, etc.). We cannot add non-campus people to the campus authentication database, and so Alma internal passwords were the optimal alternative.
61	Management of non-affiliated patrons accounts (corporate membership and ILL partners accounts)

62	We cannot give College accounts to external affiliated users such as NHS users because a College account comes with access to associated College systems, network access, etc.
63	I wasn't involved in this decision making, but I presume because this is the most convenient, as not possible to use the institution's authentication system.NB. re Q 21 a separate authentication service for accounts not held in your local authentication system - yes, but only if that service is provided to the institution.
64	Internal authentication for community borrowers has been the only option available to us so far. External authentication is working well for everyone else.
65	Primarily adopted to accommodate patrons not in our SIS (Banner)
66	We have community & generic accounts that cannot be authenticated via SAML
67	Our institution will absolutely not allow its local authentication system to be used for anyone not affiliated with the institution, but as a library, we do serve non-affiliated users, like members of general public (many of whom do not have/want social media accounts.)
68	Visitors
69	We use it for non-affiliated users; IT would not support that currently. We'd have to make a separate system.
70	It is the only obvious option for alumni and visitor accounts.
71	Easiest way to deal with patrons who aren't in our campus patron database.
72	It provided a convenient way to authenticate our public and academic guest users. We use it for library staff operator accounts mainly because we started with internal passwords -- externally managed accounts were not yet available.
73	For Alma - it was lack of time during implementation. For Primo - internal = the only option for visitors.
74	So the shared password for the front desk is not attached to someone's individual account
75	We chose to do this in order to support administrative users who work at multiple institutions, community users (such as Archives users) who don't have affiliations with campuses that would have them in their current External User population.

76	It is our only option at present for the categories of user that have these accounts. They are not included in central authentication systems. In theory if categories were created for them we could use the central systems but this would involve significant work by IT Services.
77	We used it originally during the migration process. And it has provided a fail-safe for staff when ALMA is down, which has happened at least once this year. We also use it to create accounts for visiting patrons among the Orbis Cascade Alliance libraries - that is, when a patron from another Alliance library wants to use Summit here (check out/return books on site -often they live nearer to us than the school they are attending). We will have to find another way to manage this small (for us) work flow.
78	For patrons without institutional accounts (e.g., alumni and public patrons)
79	reluctance of corporate IT to provide generic accounts, ease of management by library staff
80	when we migrated to Alma this was the most straight-forward method and gave library staff control of staff / associate member account creation and management
81	We do not have library-specific I.T., nor a systems librarian. Our institutional I.T. department is three guys in a basement (literally) and they run I.T. for the entire institution. They do not have the staff to manage authentication for our library system.
82	The University's authentication systems do not include a large number of patrons that the Library offers various services to such as access to selected online resources and loans. This situation is highly unlikely to change.
83	Members of the public have 'community borrower' accounts set up and members of other educational institutions have 'SCONUL' accounts set up. Neither of these groups would have IT accounts so will not be authenticated via Shibboleth. Setting up internally authenticated accounts is the quickest and simplest method of adding the users and means that users can borrow when they visit the institution rather than having to wait until IT add them to Active Directory. The IT department will not allow us to use a separate authentication system for these users because it is deemed to be unrealistic and very resource intensive for the number of users.We are basing our answer to "If your library uses your institution's authentication system, could it be used for users in Alma who currently have internal passwords?" on the assumption that we would be able to use Shibboleth and/or Active Directory for these users. IT would need to investigate this further and we would have to take guidance if they subsequently advised that it is not possible.
84	Only option for internal patrons to check accounts and request from storage

85	shared accounts for circulation desks can't be authenticated against shibboleth . We have a complicated authentication set up as we share our system with another institution so their Library staff users have to be internally managed users in Alma . For external users (General public & and reciprocal borrowing schemes) we only have internal library processes to manage their membership.
86	We use internal authentication for Interlibrary loans and for library staff.For interlibrary loans - at the time we migrated to Alma the inbuilt functionality was not workable for us based on the very little amount of staff time we could devote to it and that basic functionality that we'd had before was missing. So we currently use fulfilment to deal with interlibrary loans, and the external institutions that make use of this facility have internal accounts. For staff accounts - we generally use the internal accounts for testing and for staff who need to log in to Alma still should Shibboleth go down for any reason.
87	For non-affiliated patrons
88	To accommodate non-affiliated individuals who wish to use our library.
89	Provides backup access to Alma in case SSO is down and/or data load didn't work. In some cases the internally-authenticated accounts are for ExL staff access. We'll need to figure out how to manage that going forward. I will not implement a 2nd authentication scheme for 20 accounts.
90	There are two situations that internal authentication made easier: 1. Shared user accounts so that we don't have to frequently update student worker information with IT. 2. We contribute to a local ILL system where it's easiest for us to create accounts for them in Alma and use internal authentication.
91	During implementation we set up staff as internal users so we could train them before SIS integration was complete; currently most staff now use external authentication, but we like that internal authentication is available so we can still access the system if there are problems with the authentication system. We do not currently issue internal passwords for internal users aside from staff, since our implementation team warned us this option was to be phased out shortly.
92	We use it for patron accounts not in our Registration system
93	Internal authentication in Alma was chosen as a low-overhead way to provide access to the Alma system for users not officially affiliated with our institution. Having this option allows us to provide access to Alma for these users without requiring them to set up "yet another" online account, and without having to set up a separate authentication system just for these users.

94	Patron data is not loaded into Alma from an external system. Patrons have always been authenticated within the ILS.
95	Bronwyn answering on Elizabeth's behalf: For the reasons outline by E above. Last point: as you will have seen above some NAS users are external however there is no external NAS authentication method. In the case of external users the pin is uploaded to an Alma user note field as part of SIS by UNILINC. Due to a local UNILINC development PDS consults this field. However this homegrown solution is not permanent for various reasons: PDS is on the way out, we may be pressured at some point to go to a SaaS environment (currently Primo Direct), and so on.
96	Quick and easy method of allowing non-affiliated members access to the library and its' resources.
97	(my take) largely community users came to the library, no provision has been made yet in the larger university to issue an ID, there are also shared accounts.
98	Not all library users are the same users as maintained in the campus SIS or fed into our CAS data load. We also use internal staff accounts for ease of use during times of campus authentication failures.
99	See answer above. IT only allows registered students, staff and faculty to be part of the Banner database.
100	Library staff needing access to Alma was given a separate authentication to maintain their roles separate from their patron record.
101	Don't know
102	We have users who do not come the institution's authentication system and need a means to be authenticated as we have no other option available. We also have groups of users who qualify for off campus access to resources and the only way to facilitate this access is to use their Alma credentials in another system which will then authenticate them for access.
103	The 2 Alma system administrators at our library prefer to have manual control over the passwords for internal accounts, most especially for library staff accounts. When we are forced to go through our IT department for this, their systems occasionally burp and might then temporarily lock library staff out of Alma until IT restores access. This will require us to submit a service ticket to them and wait in their ticket queue until they have time to fix it for us. Itâ€™s much easier for us to have direct control over our own system login accounts, without getting our IT department involved. The suggestion that our library usersâ€"many of whom barely speak English or know how

	to use a keyboard and mouseâ€"should authenticate into our ILS through unaffiliated services beyond our control like facebook and google, would force us to provide poor customer service, erecting technological barriers that risk alienating already under-served populations. This goes against the raison dâ€™etre of community college libraries in particular, not to mention exposing our patronsâ€™ digital lives to big data mining schemes. Social justice issues aside, it is wholly illogical to shift the burden of authentication for internal accounts to the institution. If we can't trust Alma to store password hashes in a secure manner, why would we trust them to store any of our patronsâ€™ personal information and transaction history? Why would our IT department want to take on the added liability of storing the personal details of non-affiliated users, when the company they help us pay $50,000 a year to do just that has abdicated their responsibilities to do exactly that?
104	This is because there was and still is currently no infrastructure within the institutional framework to create the credentials in Active Directory to allow non-institutional accounts to authenticate using the institutional system (this is something we will start to talk to colleagues about and should hopefully manage to progress) and we already had many users migrating that were using Aleph and later Alma password. it was also a perfectly viable option at the time, and there was no indication when we went through implementation that this was a temporary solution only. As a University Library we are not restricted solely to the institution's user base and offer services to a wider community of users.
105	We are using internal staff accounts because university IT does not currently support secure LDAP as required for Alma authentication. However, they are implementing LDAPS in calendar 2017, and we plan to move to external authentication for staff Alma accounts at that time. Community members and most alumni are not in the university's active directory system and cannot be added. AD accounts are created only for current students, faculty, and staff. For non-affiliated patrons we create internal accounts with internal authentication.
106	You offered internal authentication which is what we used with Voyager so it seemed like less work when we were migrating to Alma to just go with it (instead of re-working our existing procedures)! Access to our collections is highly mediated by staff since our materials generally don't leave the building and there are long periods of time between visits for many patrons (months and sometimes years). Most of our new patrons are Readers who we do not know in advance and many arrive unannounced to use the library expecting to use our materials right away so we simply add them one at a time that they arrive at the Library. Even in the instances when we receive an advanced list of, for example, new scholars for the new year, itâ€™s only perhaps 50 people which is not anywhere near the thousands of new students each year at a college. Manually adding 50 patrons is a manageable task. Our user management methods have reduced the barriers to entry for patrons (e.g. passwords not expiring, keeping most patron accounts active even if they haven't visited library for years) and have worked well for staff who are involved in the process.

107	We have patrons that are not included in our institution's authentication system. It is also easier to use a generic login for student workers who share a computer to check out material.
108	See above
109	Lack of available alternatives
110	I believe that, as Early Adopters, it wasn't possible to have staff operators using External accounts when we went live.We have a few types of users who do not get computing accounts (some university Associates, paid Library associates) and therefore don't exist in our central IT system that feeds user accounts to Alma.

Attachment 2 - Why Institutions are using Generic Internal Accounts

1	We have ~75 student workers between the libraries, and we cannot afford to make each of them a staff operator with their own authentication. This was a major point of contention during our contract negotiation with Ex Libris, but they refused to allow us the number of staff accounts we require, so we're forced to rely on shared accounts with internal authentication.
2	Concierge staff who need to see user records to help with access to buildings but not to edit records, and accounts to access Alma when there is a problem accessing the University's authentication system
3	used for circulation desks and student workers
4	We use a shared account for all of our student workers, it makes circulation easier
5	Student workers use shared accounts for circulation. Some staff use shared accounts for reference, reporting, and other non-transactional activities.
6	Staff serving on the information desk use shared account as several people operate on the same terminal. The shared account prevents an abundance of log ins and log outs while serving our patrons.
7	For the current system, we use a password to access the system and another password to access voyager.
8	Individual accounts take too long to log in, so staff prefer to use the shared accounts
9	We don't want students to login to Alma with their student credentials.
10	Some are for circ students, and some are for librarians who do collection development but have no other use for Alma.
11	Shared accounts are for Alma administrators only. They allow us to work with particular users associated to particular Alma roles and to exactly know what roles enable what and give access to. Shared accounts are all internal accounts.
12	Circulation desk, we do not want/require students to login just to circulate an item. Additionally our self-check machine uses an internal account to authenticate
13	Check in station. Login for staff when authentication system is down

14	So staff do not have to use their own email account to send circulation or acquisitions reports
15	Due to MAX 'named' user license restriction as opposed to a concurrent user license we were forced to use 3 generic account to be shared with 150+ student workers
16	We use a shared account for our circulation staff, for ease of user management.
17	We can have 2 or 3 student workers on duty at the circ desk at once. Whoever is closest to the computer checks people out. It could be me, the director, the Evening Supervisor or any one of a number of student workers.
18	shared circulation student worker account for use at the circulation desk. Negates the need for student workers to log out/log in at shift change
19	We have one internal Administrator account. This allows a backdoor to Alma in case something happens to our Shibboleth external authentication. This happens very rarely but it can happen.
20	We have some external-auth shared accounts so people don't have to log out and in every time a desk shift changes. But most relevant here are some internal-auth shared accounts we have as backups in case our external-auth system (Shibboleth) goes down.
21	For use at Circulation Desks where different staff use the same terminal for issues and returns
22	Circulation activities
23	1. Logins for shared use at service points eg "circdesk" for circ/casual/student staff. 2.Internal logins for Alma staff used when external authentication system is down/unavailable. 3. Admin login / Ex Libris logins
24	Issue desks
25	We have many students working in our libraries for few weeks, it is a waste of time setting roles for each student
26	use one account for student circ desk attendants in law library
27	requests on library side for patrons who do not have accounts, taking payments
28	Circulation desk

29	One offsite storage facility uses a generic staff operator accounts.
30	Generic circulation desk account with limited rights for use by PT and work study students.
31	Shared by student staff in order for us to meet named user limit.
32	Library desks with several people working at the same time / alternating
33	logon to circulation module
34	They are backup accounts in case our campus authentication system goes down.
35	The standard use is for departmental short-term employees (students or contract) tied to very specific workflows and who represent high turn-over - Circulation desk student employees, cataloging project student/contract employees, low level Acquisition student/project workers or the like. All cases where assigning roles to a specific individual with externally controlled authentication is either impossible or a significant oversight/maintenance issue.
36	To loan, return, and provide circulation services at the circulation desk. To process course reserves.
37	For occasional staff users of the system, where we do not wish to consume a named user licence
38	Circulation desk functions
39	We have job share arrangements in place and this reduces the number of logins required for each of the 18 Queensland Health Libraries. This arrangement also lets us readily identify the library that has made modifications to records rather than relying knowing a name of a person in the network.
40	we have two generic accounts for our stack system
41	Will be used by student staff (when we have Alma in production)
42	These accounts are generally used at service desks, and are easy to maintain as opposed to assigning and unassigning Alma access to dozens of student workers.
43	Primarily for student employee use.

44	There is one shared login for all student employees. Full time staff end up using it by default.
45	We have a student account for each circ desk. It is much easier to manage because we have approximately 20-30 student employees each quarter, with high turnover.
46	User Services, ILL and Reference desks
47	Student account with authentication needed for specific roles. Easier log in as workstations can be designated for specific tasks. Easier to keep track of who is and who is not authorized to work on each specific task.
48	Simplicity, customer service.
49	We use shared accounts with minimum access rights as the default logins at lending points, because the check in / check out PCs at these service points are used by multiple staff to perform generic loans and returns tasks. If we set up a workflow that required all staff to login and logout of the lending PCs every time they moved to a new PC, this would slow down our loans and return process and reduce both user service satisfaction and workflow efficiency.
50	Circulation desk staff use a shared account, also IT Services have an account that is used occasionally for supporting our work on integrations. There are also some Ex Libris implementers/support accounts
51	Circ Desk Activities only, only for use at Circ Desk
52	We only use one - for our processing department. Staff operators change so frequently that it disrupts the workflow to have someone switch to a different user.
53	Admin shared account to allow editing of centrally authorised record templates, departmental accounts to allow requesting of material for e.g. exhibitions, or for use in the event that the external authentication is down (several examples of this since go-live due to issues with our network, have needed the backup accounts to use via our secondary ADSL line)
54	These people change regularly
55	Internal shared accounts are used mostly by front line staff (GA's, Student workers, staff). These workers are in constant motion and it is not productive to use personal account logins. Using personal accounts would require these workers to logout and back in each time they step away from the desk and/or need to use an Alma terminal that another user is logged into.

56	Service desk operations
57	Work study students
58	We have job share roles, where users log in as one individual. We have shared desk operator roles, which allows for users to access via a generic account and don't have to keep logging in and our. We have admin accounts and test accounts that have been established for various reasons
59	We use these generic accounts at our circulation desk. Multiple students may need to use the same machine without logging out and logging back in again.
60	Shared account are used only for activities performed by students that work few hours per month in the library
61	working hourly shifts at the circulation desk
62	Binding, work orders
63	Our Academic Registry department use a generic login, to access user data in Alma for checking for outstanding fines... - This is on our road map to fix as we want them looking in Banner, but we are not there yet. Our IT Department use a generic login, to issue and return laptops they have loaned out. While we did consider giving individuals in IT access to Alma (via Shibboleth), the number of staff would have meant additional costs for the library for user licenses. Do we know if ExL are proposing reducing the costs per library member of staff?
64	These are circulation desk accounts for staff staffing issue desks at various campus libraries.
65	For groups of library staff in various locations who only use one function in Alma Fulfillment - Scan in Items.
66	Student logins used at circ desk for students to checkin/checkout materials
67	Student use; ILL interface; special users for temp materials placement
68	One of our law libraries/appellate court library uses one shared account for circulation desk workers.
69	Student use
70	Circulation desk functions, Administration functions, Document Delivery functions.

71	We have generic accounts for the fulfilment team so that various staff on the same service point can use the same instance of Alma, and to save having to create individual staff user roles for the many casual staff who assist with the provision of our services. We also have a generic account for the creation of cataloguing templates as we found that templates created within a specific user account can only be edited by that user. All cataloguing templates are created using the generic account.
72	Helpdesk use only. At very busy periods we don't want to Staff to have to login and out so we use generic accounts. It would cause too much delay for users otherwise.
73	for front desk circulation
74	Check outs to ILL
75	Multiple colleagues staff service points and therefore generic access needed to avoid logging in and out continually.
76	When external authentication fails, we have to use the internal accounts so staff can keep working
77	Fulfillment and resource management activities
78	contract / casual staff doing returns, casual staff weeding physical items, work experience students, finance staff paying invoices, temporary library staff
79	Basic circulation tasks (Access Services), Repository Search (Reference), Fulfillment testing accounts for troubleshooting (Access Services)
80	to allow casual staff to issue laptops at a shared helpdesk
91	student worker access accounts and interlibrary loan account
82	The majority of our staff operator accounts are externally authenticated. A single shared account is used at one campus as the campus has a mix of staff from our institution and staff from an affiliated institution whose staff cannot be authenticated using our institutions external authentication system. A generic shared account is used for the enquiry desk for our institution staff, the affiliated institutions staff, and casual staff.
83	We have a 'helpdesk' generic account for each campus so that staff don't need to logout and log back in again when they change shifts. Personal accounts are

	authenticated via Shibboleth so a staff member would need to log out of the computer and the next staff member log in when changing shifts. This can cause unnecessary delays when students are waiting to be served.
84	Testing and when our SAML server is down
85	Circulation desk operators
86	Allows us to be able to access Alma in the event of issues with local authentication (Shibboleth).
87	circ desk operators for student / lowest-level workers
88	There are close to 30 students that use shared accounts for circulation, ILL, GovDocs, tech services and serials.
89	one circ operator account for casual/student staff
90	lowest level student workers
91	We have shared accounts used by student employees for general fulfillment activities. In addition, we have shared accounts used by Ex Libris for support, shared accounts used by staff members for testing. We also provide internal patron accounts for working groups within the library, so that we can check out library resources to the group as a whole.
92	Student Workers
93	We have some generic accounts for testing purposes, e.g. test student, test employee, etcâ€¦, but we also use generic accounts for some specific tasks like Film Booking and ILL Loans.
94	Two circulation terminals that remain logged in under two user names. Same permissions.
95	Student workers
96	1 general low privilege level for reference desk staff; 1 general low privilege for circulation desk staff which includes part time employees and student workers; 1 advanced privilege level for all interlibrary loan transactions.
97	We have shifting casual staff and multiple staff users at the loans desk

98	Job sharing / shift work at the Circ desk
99	We have student workers
100	Multiple students and sometimes staff with similar job duties at shared workstations -- Minimize changing "where you are at" for a person
101	Student workers use shared circulation account for basic desk processes.
102	We have one shared staff operator account that is used each year for up to 10 work study students. It is our understanding that since we pay for a fixed number of Staff Operator accounts having our work students share one account lowers the number of Staff accounts that we need to use.
103	Student worker login for checking out material from Alma
104	Multiple staff work on circ desk. Saves having to login and out constantly.
105	Circulation transactions by multiple users using a group of computers
106	We have a number of part-time staff who work in the library at different times with only one person in the library at a time.
107	Job share
108	Various part-time / temporary staff work on circ desk
109	So circ desk staff don't keep having to login and out using their personal staff user accounts
110	circulation desk

Attachment 3 - Reasons why Institutions cannot move to an alternate system until after December 2018

1	1. Keele University selected Alma on the understanding that all our users would be able to login to check loans, reserve items, etc. It was mentioned in the tender documentation and discussed at the system demonstration. For Ex Libris to announce that this would no longer be possible without considerable extra work on our part 4 months after going live will raise big questions with our Purchasing Department. 2. As mentioned in the above Keele University has a Service Level Agreement with the NHS for joint provision of Library Services at Royal Stoke Hospital. This announcement puts Keele in the position of breaking that agreement through no fault of our own.3. Local development of a system to take this role may be possible but is a considerable undertaking involving a number of staff and a considerable amount of time, none of which has been planned for. To have it ready within 2 years is unlikely.
2	Acquiring any system to house authentication information requires our institutions to have said changes approved by the University's legal council and approved by our State governing body.
3	All dates are possible but not necessarily probable as there is no detail on the scope of work required, need more detail before able to commit to a probable date.
4	Any cutover is dependent on Ex Libris providing alternative to internal authentication for their internal accounts: exl_impl, exl_supp and Leganto Instructor. We need ExL to provide alternative to internal authentication for BIAF spine label printing.
5	As the library does not control authentication, so we do not know their time scales and priorities.
6	Authentication for non-OSU members will require a separate system that has not been developed yet and OSU may not see a reason to invest in that when we're already paying an external company (Ex Libris) for a product that is supposed to take care of that.
7	Dec 2018 is more likely to work but we have a lot of questions around data entry that will depend on what Ex Libris will support.
8	Elizabeth, NAS: We do not have external access. We have no budget to acquire this. We (National Art School) will always need to be able to manually add in patrons to ALMA for short courses, Associate memberships and sessional staff - who arrive on an ad hoc basis. Many of the short course patrons are retirees who do not use social

	media, some of whom don't even use email. Bronwyn, UNILINC: Even if all the NAS users had social logins we have doubts that this would be a satisfactory Primo authentication method and cannot test until the Primo Nov release has been installed. Regarding "Will your institution allow you to use a separate authentication ...": Elizabeth does not know. As this is mandatory question I have answered NO on her behalf.
9	FYI we are already fully external, but there was no way to choose N/A. Additionally, we do not give our non-authenticated users passwords to access Alma - they must come in or call to renew. That was also not an option I could choose.
10	I don't know I don't work with passwords
11	I have to add maybe 10 to 12 staff members, as well as random students throughout the terms, most of which I do manually other than the one big one at the start of the year.
12	I'm sorry, but this just isn't enough time to have worked out all the details with our campus IT department to have any kind of certainty of when we can be ready. Even getting back answers to these types of questions from our campus IT department can take months. Please note that for the last two questions on this page, I answered "No" only because I'm not certain of the answer. These questions really need an option of "Not sure."
13	In our Alma institution are represented different kind of libraries. For the University it could be feasible to plan a solution for external patron accounts managed internally in Alma probably during 2018, but not for all the small libraries that are not part of our institution and that don't have an IT department at all.
14	Internal accounts required for Alumni and members of the public
15	Involves the renegotiation of SLAs with external organisations, unbudgeted expenditure for both institutions to implement a solution, and ongoing costs to maintain separate (and possibly multiple) authentication system/s
16	It depends on the external authentication method. Our institution *will not allow us* to create institutional accounts for users who aren't currently university members. Any other solution not only has to be acceptable for purposes of logging into Alma, but we'll also have to rewrite our code that currently uses the Alma API to enable authentication to EZproxy for approved databases. We're nervous about social authentication as an appropriate secure replacement: have you *seen* the number of hacks of social media passwords?

17	IT dept don't know what we would do (would require major discussion) so cant really answer this or the next 3 questions (put No because answer reqd)
18	It is against university policy to allow non-registered users (community patrons) to authenticate through our campus IdP.
19	It will not be possible to externally authenticate community members
20	Move to ADFS currently in progress. No solution (apart from Alma) in place for non affiliated users
21	No campus applications are utilizing this method of authentication. The adoption of this protocol would need to be comprehensive and would be complicated. The project would have to fit into established priorities and timeframes. This is currently seen as having limited appeal and won't be considered for 1-2 years
22	Not, a reason why these dates won't work, but our reasons and thoughts behind our decisions above. Our IT Department, will require at least 12 months notice, for any changes to internal authentication. This is primarily so that we have time look at, configuring Shibboleth to accept guest users, and also work through the workflows required to change a user's account from Internally authenticated to externally authenticated. In the library, we will also need time to adjust and set-up, as we will need to look at changing ALL the usernames and passwords for our guest users, which might present a interesting set of challenges, as we will have to contact each user individually, making them aware that they are getting a new username, and then making the changes to their accounts.
23	Note: we are concerned that community users will not have social media accounts
24	Only current students are able to be batch processed. All other user types are added manually at time of need.
25	Our experience of projects (which this would undoubtedly become) in the civil service is that it takes 3-5 years to implement
26	Our infrastructure is not designed for internal patrons - there are policy issues with this. Also ideologically opposed to social media logins due to data security issues. Most social media platforms are intelligent advertising sites harvesting people's data, and also have a chat function.
27	Our institution is currently working at bringing disparate campuses together from an IT perspective and will not be able to provide any support to facilitate this type of change. We also have a committee working on Identity and Access Management where this would fall under their mandate but they are still working out campus-wide

	issues which need to be addressed and would not be able to provide assistance in the time frames indicated above. Currently, we need to have control over passwords to as seamlessly as possible enable off campus access to resources for users who qualify, i.e. health preceptors, as access can currently be facilitated when the Alma internal password match.
28	Our IT department does not have the capacity to manage a separate authentication system
29	Our IT department is understaffed and overworked
30	Our IT department would be very reluctant to do the work to enable these users to authenticate. In the unlikely case they agreed, June 2017 would not be possible.
31	Our IT does not have the resources to support another authentication method.
32	Our IT needs more time than is available to do a proper cost/benefit analysis to even determine what our best course of action would be, let alone how long it might take to implement. Budget and personnel/project issues would need to be factored in as well. This is simply not possible within this timeframe.
33	Our patrons become members of the library whenever they come into the library. It would absolutely not suit us to use batch imported records. We need to be able to add them manually in real time in front of the patron.
34	Our university will not add people not affiliated with the university to the authentication system.
35	SAE intends to move to Google SSO for Primo authentication for their external users however they will continue to have some patrons with non-Google SSO accounts (Alumni). Also, SAE currently routinely creates external user records for new patrons who wish to borrow immediately ie before the SIS load has run. A student's first experience should not be an unpleasant one ie they should not have to wait for the next SIS load before being able to borrow.
36	Since I have not had a chance to talk with campus IT about this, I've no idea how it will work. Our IT folks have a strict system for portioning out human resources for projects, though, and it can be difficult to get on their schedule. I am very, very reluctant to go the social media route, because those systems do not comply with library standards of privacy.
37	Some patrons don't have external accounts. The library is their only internet account.

38	SSO in NSW Police Force is not currently available beyond the enterprise environment
39	State regulations limits sharing of personal data; social media authentication is not an acceptable option.
40	The answer given reflects the libraries lack of control of the various steps that would have to be put in place institutionally to incorporate otherwise unaffiliated individuals (i.e. only tied to the libraries) into the mainstream of the university's credentialing and authentication process.
41	The dates work so long as options in #19 are available.
42	The identity management in the University is under thorough review.
43	The IT department is very unlikely to see this as a high impact issue. As a publicly-funded institution, the library is required to be accessible to the public in our tax base and beyond.
44	This password management change has implications for our institution. We will have to make decisions. Because of our security constraints, find and implement a new solution can take some time.
45	This will need further investigation before we can confirm a suitable timescale.
46	Time and effort is required to understand, evaluate and implement the specific alternative solution
47	UNILINC comment: All users are internal at the moment. Not sufficient IT support to setup SIS file process. No external authentication method. Social login is of interest but could only be a solution for some patrons.
48	University IT does not want us to use social media to authenticate into university resources.
49	We are currently undergoing a restructure of all areas of our institution and this will impact on capacity to develop new services and processes in the short to medium term. We are also working through a large enterprise architecture project and will need to ensure that whatever process is developed to manage Alma passwords fits within this framework and is not just a stop gap approach for long term sustainability.

50	We are thinking we would prefer to have set up an additional Shibboleth instance which could be inserted into our WAYF. That IDP would be backed up by Active Directory, for instance, where our special populations would live.
51	We cannot provide a clear answer for this as we do not know what the IT strategy for this will be in future.
52	We currently have no feasible way to authenticate patrons that are not faculty, students or staff besides Alma
53	We do not have a solution for this. We only use internal accounts. According to our procurement we asked for a system with the possibility to create accounts for our users with username and password.
54	We do not have any process in place to deal with NHS users and migrate them to university systems. There would be a great deal of negotiation and cost (money, staff time, etc.) required for this kind of move: we would also need to renegotiate our SLAs with this organisation. The NHS is an organisation that is very difficult to influence. We (our central ICT) would be taking on the security concerns that Ex Libris are currently dealing with and, we imagine, would not be willing to do this.
55	We do not have the infrastructure or resources to employ an alternate authentication system, and it is non-trivial for us to introduce non-student, non-faculty/staff into our authentication workflows.
56	We don't currently have a method we could use to manage these users. We would need to initiate a project to implement a separate authentication system, and there is no guarantee that the University would approve this work. Security would be an issue.
57	we have a 12 month planning cycle for ICT works, the next cycle commences August 2017
58	We have a consortia arrangement of 18 geographically dispersed libraries from 11 different autonomous organisations with various levels of IT understanding and need. The only single access available to the whole network would be using the login details of over 65,00 employees - many of whom would not have access rights to the the library system as they are not part of the consortia. Trying to co-ordinate this type of change with so many agencies will be difficult.
59	We have already done this - you should provide a way to answer this question appropriately.

60	We have no means of external authentication for our Community Borrower accounts, and they cannot be added into our External system.
61	We need the ability to support retired faculty and others that no longer are authenticated in our central system
62	We use the Banner system which is fairly locked down. In conversations with IT, they are not going to allow, in the foreseeable future, for our community users to be given profiles in Banner which are needed to authenticate through our portal.
63	We will need more information from the vendor before we can begin any internal conversations with local IT partners
64	We will NEVER allow external authentication for community borrowers. When we set up external authentication, it will be for current faculty, staff and students and will give them access not just to ALMA, but to our other electronic resources. These resources are licensed for use by faculty, staff and students only.
65	We will not be able to move to another external autho system so will just have to manage without doing that.
66	We would have to contract a service provider for external authentication. We don't have the budget to do this. On top of this, we have patrons from age 4 upwards. Librarians create accounts for them. It is paramount that this continues to be possible.
67	While we don't have a large number of internal accounts, there are certain accounts tied to ILL that we're not sure how to authenticate. June is too close to feel comfortable that a solution will be found. The idea is if we have a year we can put something in place, we just don't know what that something will be yet.