Consultation for the Big Ten Academic Alliance Provisioning Cookbook

Community Review

This consultation on the Big Ten Academic Alliance Provisioning Cookbook has been concluded.

The final document will be posted once all the input has been processed and editing is complete.

Document for review/consultation

- BTAA Provisioning Cookbook for Consultation.pdf

Background

The Big Ten Academic Alliance's Identity Task Force, in conjunction with other Internet2 community members, has taken the combined experiences and wisdom of several BTAA consortium schools and beyond to build a cookbook of best practices for provisioning and deprovisioning. Whether you're inventing an identity and access management (IAM) program for the first time, re-inventing one, or just want to do what you already do better, this cookbook can help. The cookbook will be presented during a December 7 session at the Internet2 Technology Exchange in Denver.

Now, we need your help to make it even better. Before we call it finished, the authors are working with Internet2 to open it up to a community consultation. We need the broader community to read our best practices and let us know how we're doing. If you see something missing or an item that you don't agree with, use the community consultation to let us know. Your assistance can help us put the finishing touches on a document that we're confident will help a lot of organizations make provisioning work well. The consultation is open until January 31, 2023. Thanks in advance for helping us with your feedback.

Number	Current Text	Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)	Action (please leave this column blank)
1		The cookbook provides a lot of good advices on provisioning and authorization, but is silent on the use "secondary" or "auxiliary" logins for specific authorizations or roles. (E. g. student vs. instructor in LMS system, "admin" access within a service (whatever that might mean in for a given service, auditors, or information security).)	Steven Premeau (maine.edu)		
2	Section 3.4	Add a mention here that Section 7 discusses these models in more detail. Revise: "Just in Case (JIC) must occur before the <user first attempts to access the service>. Note "Just-in-Case" includes the case of "when requested". If an admin grants a user access, and that triggers a send of identity data, that is "Just-in-Case", even though it looks different from the case of "grant access to all the new students, whether they ever use it or not". Therefore "Just-in-Case" may not be the best name, since the essential point is that the identify information is sent to the service provider before the user attempts to access the service.	Andrew Markiel (uw.edu)		While it may not be the most accurate description, "Just-in-Case" is a common term; we'll leave it alone. We have added a comment about gray areas between the two. Note that there are potential reasons for JIC provisioning that are not driven by the first login, so we will keep the "... before the identity information is required…" phrasing. (See Section 7.)
3	Section 4.1	I would add here that along with the identity matching system, there must be processes in place in the onboarding workflows to capture sufficient consistent information to support identity matching. If the onboarding workflows do not capture sufficient information, then reliable identity matching will be impossible regardless of the sophistication of the identity-matching algorithm. Thus **Do:** Work with systems of record and the onboarding processes that populate them to capture consistent identity data to support matching with previously stored identities.	Andrew Markiel (uw. edu)		We added a comment to this effect at the end of Section 4.1.1.
4	Section 5.1.4	I think it important to make the following point a little more clearly: • Most universities have the challenge of managing users with multiple overlapping affiliations (student employee being the most common). • Some other organizations do not have this problem and therefore have a simpler identity management problem; • Therefore, some identity management solutions assume this, offering a simpler /cheaper solution to a simpler problem; • Therefore, most universities need to understand and accept that they have a more challenging problem and cannot make do with the simplest/cheapest solutions available. This is necessary to give a good answer to why a university should spend extra resources to acquire a more sophisticated solution: because the more complex user population demands it.	Andrew Markiel (uw. edu)		We changed the text to: "This scenario is very common in higher education, but much less common in other organizations. Someone can be a staff member taking classes or a student with part-time employment. A retiree can come back as a student. There are lots of possibilities. Ensure that your system can assign multiple affiliations to an individual that can be separately assigned or removed."

5	Section 6.3	I would add here: Do: Anticipate and have a process to assist users whose 2FA device is unavailable. Once a second factor is required for authentication, users will accidently leave their device at home, have their device broken or lost, or desire to replace it with a new device. Add an education component to your 2FA initiative instructing users what to do in such cases and how to avoid problems or have a backup solution in place. Have your help desk ready to assist users in need.	Andrew Markiel (uw.edu)		We feel this is out of scope, important but not related to provisioning.
6	Section 7	Somewhere in this section, I would mention the primary drawbacks of the Just-in-Case provisioning model: • Data is shared that is not needed (whenever an account is provisioned but never used), which violates the general security principle of minimum information needed. • Unnecessary provisioning can generate higher license costs than required. • Storing and reconciling provisioned data wastes resources for account information that is never used.	Andrew Markiel (uw.edu)		We reworded the introduction to Section 7 to reflect this.
7	Section 9.4	Somewhere here one should discuss the problem of administrative controls and delegated authority. Who is authorized to grant access to users or manage access policy? Who is authorized to grant admin privileges to admins? Who are the super-admins and how is their activity monitored for appropriateness? How are those privileges audited? Perhaps: Do: Given careful thought to the processes for assigning and removing administrative privileges that allow a user to grant access to other users or manage access control policies. Have a process in place to verify that these privileges are and remain set correctly.	Andrew Markiel (uw.edu)		Reworded 9.4 to address this in the context of section 9's introductory statement that authorization is an extension of institutional policy for delegation of authority. Section "10.2 Audit" already addresses audit of compliance with policies for authorization.
8		Somewhere in this document, and I'm not sure where, one should reference potential performance issues with provisioning or de-provisioning large populations, for example "creating accounts for all the new students this year" or "deprovisioning all the accounts for students who graduated last year". Such processes can cause large slowdowns due to a very large number of transactions flowing through various systems. Implementers should be encouraged to consider this possibility, to test how their systems will actually perform, and consider alternatives (such as chunking of smaller batches) to manage such issues.	Andrew Markiel (uw.edu)		Reworded sections "7.3.2. Do: Deploy robust provisioning interfaces," "8.2.1. Do: Use a reliable process or frequent deltas to push changes in as close to real-time as possible in the intended manner," and "9.4.1. Do: Consider how you will handle authorizations that change *en masse* with academic term/sessions" to address performance issues during large updates.

See Also

- Trust and Identity Consultations Home
- TIER Working Groups Home
- InCommon Software Integration Working Group Home