

IDM-15: Lookup the affiliated institutions for a community identity

A **campus IT administrator** or **service provider** needs to lookup the institution(s) affiliated with a community identity previously returned by the community login process so the service provider can track usage by consortium or other groupings of institutions. We assume the community's terms of service allow release of identity information to community service providers.

In most cases, the service provider wants to experience it as follows.

1. First, the service provider accesses a community information interface.
2. Then, the service provider enters a community identity (username).
3. Then, the interface returns any organizations associated with the identity that was entered.

It will always be like this except when the service provider needs to look up the organizations for many community identities. In that case, either the community information interface can be scripted (CLI) or it can accept a list of identities and return aggregate results.

We'll take any solution, as long as...

1. In Step 1, the interface can be accessed either via a web browser or a locally installed CLI/script. (Either of these methods is acceptable.)
2. In Step 1, if the interface is a locally installed CLI/script, it must be easy to install and must be available for Mac, Windows, and Linux systems.
3. In Steps 2 and 3, any network communication that includes personally identifiable information must be via a confidential (securely encrypted) channel.
4. In Steps 2 and 3, there is an option for the results to include organizations from linked identities (identities linked to the community identity) as well as from the community identity itself.

IDM-16: Obtain affiliated institutions when an individual logs in to a service

A **campus IT administrator** or **service provider** needs to obtain affiliated institutions when individuals login to a service so the service provider can track usage by consortium or other groupings of institutions. We assume the community's terms of service allow release of identity information to community service providers.

In most cases, the service provider wants to experience it as follows.

1. First, the service provider configures a service to use the community's login mechanism.
2. Then, when an individual logs into the service, the login mechanism returns the individual's community identity, which includes an organization field.
3. Finally, the service logs the community identity and the included organization field in the service's usage data.

It will always be like this except when the service provider wants to log the organizations from linked identities as well as the community identity. In that case, the service provider needs to change the service's configuration for the community login mechanism so it also requests linked identity information. Then, when individuals login to the service, the service can request linked identity information, gather the organizations from the linked identities, and log all of the organizations in the service's usage data.

We'll take any solution, as long as...

1. In Step 1, the login mechanism used is the community's standard login mechanism as described in use case IDM-06 or IDM-07.
2. In Step 2, individuals using the service for the first time are informed that the application is requesting their identity data (and linked identities in the alternate scenario) and are given the opportunity to approve/reject the request.
3. At any time after logging into the service, individual users may revoke the service's access to their identity data. (This doesn't affect any data that's already been collected.)