How It Works: MyAccess, SAML and Shibboleth

The Authorization Process

If you’ve used just about any online resource at UC, San Francisco, you’ve probably already used the MyAccess login system. With one username and password, you can login to hundreds of applications at UCSF. You can even use those same login credentials to login to other services provided by other campuses and vendors, similar to the way you might use your Facebook or Google login information to gain access to an online game or online store. Now you’d like to integrate your application into the unified MyAccess login system, but how do you do that? How does it work?

The MyAccess login system (not to be confused with the MyAccess landing page, which only displays a list of applications to login to) uses the Security Assertion Markup Language (SAML) industry standard to provide a secure method for users to exchange their information between their host institution (UCSF) and any application authorized to request that information. The MyAccess login system uses the Shibboleth IdP software as the intermediary between the user and the applications requesting user information (such as name, email address, employee ID, etc).

The Authorization Process

The graphic below illustrates the entire process, which is also described, acronyms and all below. The user starts at step 1, attempting to access your application, and ends at step 8, successfully accessing your application after having logged into MyAccess.

1. START HERE
2. Your SP generates SAML request
3. Your SP redirects browser to SSO URL
4. Our IdP parses SAML request, authenticates user
5. Our IdP generates SAML response
6. Our IdP returns encoded SAML response to browser
7. ACS verifies SAML response
8. User is logged in to your application

SAMLTransaction Steps
There are a number of SAML compatible Service Provider solutions. Most require that the software be installed on the same web server that hosts your application. We recommend either the Shibboleth SP or SimpleSAMLphp solutions.

**How Long Will This Take?**

Like most technical processes, it depends a lot on the knowledge and efficiency of those involved. In the IAM team's experience, the average integration for a single application takes about 3 business weeks. But there is a very wide range. A testing-only, non-production integration lead by a technician with significant SAML experience can be as short as 2 business days. If you're working with a 3rd party vendor who has never integrated their application using SAML, expect a 3 to 6 month integration timeline, mostly due to vendor testing and development during the integration process. If you want your application to go beyond the testing phase, you'll need to integrate 2 separate systems, a test environment and a production environment. If you begin the integration process with your test environment, the process will go faster when you begin your production integration. Be sure to plan any projects or dependent tasks with all this in mind.

**The Application Integration Process**

Importantly, not every application can, or should be integrated with the MyAccess login system. In particular, if your application does not have a web interface, you would not want to use the MyAccess login system. Development time and resources would be better invested in an integration with Active Directory rather than in the web-only MyAccess login system. That being said, many mobile platform application use an embedded web browser for the sole purpose of SAML-based SSO. When a user opens the application and attempts to access a "cloud-based" resource, the application presents it's embedded web browser and follows steps 1 through 8 in the above SAML Transaction Steps illustration before returning the user to the native application interface after step 8. This has become a popular solution among Software as a Service (SaaS) vendors, especially those who frequently work with higher education institutions and large corporations.

If your application is appropriate for a MyAccess login system integration, here's a high-level overview of the technical steps required to integrate your application.

1. **Install a SAML SP.** There are a number of SAML compatible Service Provider solutions. Most require that the software be installed on the same web server that hosts your application. We recommend either the Shibboleth SP or SimpleSAMLphp solutions.

   **IMPORTANT:** If you're application is a SaaS or "cloud" service such as Salesforce, Workfront, Box, etc, you can't install any SP software. So be sure to ask your application service provider if it supports SAML2 single-sign-on. If it doesn't, you cannot integrate the application with the MyAccess SSO system.

2. **Configure the SP.** Initially, you'll need to configure it to use the UCSF MyAccess staging Identity Provider (IdP). Why use the staging IdP first? Because it allows for more rapid testing and modifications on the IdP since it can be reconfigured during normal business hours, unlike the production IdP environment.

3. **Complete the MyAccess Integration Request form.** This form asks for information required by the Identity and Access Management team in order to configure the staging and production IdP environments.

4. **The Identity and Access Management (IAM) team will configure the MyAccess staging IdP to work with your SP.**

5. **Once you receive notice from the IAM team that the staging IdP is configured, test your SP and application to verify MyAccess login works in the staging environment.**

6. **Respond to the IAM team member confirming success in the staging IdP environment and request that the configuration be placed into production.**

7. **The IAM team member will schedule the staging IdP configuration for deployment into the MyAccess production IdP environment during the next maintenance window (see this document for maintenance window times).**

8. **Once you receive notice from the IAM team that the production IdP is configured, reconfigure your SP to use the UCSF MyAccess production IdP. Test your SP and application to confirm proper operation in production.**

9. **Respond to the IAM team member confirming success in the production IdP environment.**

**NOTE:** The "SAML Transaction Steps" graphic above is a modified version of a publicly published graphic by Google.