Onboarding OpenAthens:

Considerations for Switching to OpenAthens Authentication

by David J. Leffler

METHODS FOR TESTING OPENATHENS REDIRECTOR LINKS

An essential component of transitioning to OpenAthens authentication is testing and verifying that vendors have correctly added the organization's OpenAthens IP address or federated details to the vendor's entitlement system or access control system. Project managers who liaise with vendors by requesting that vendors add their OpenAthens IP address or the organization's federated details must test and verify that vendors have correctly set up authentication. Testing URLs that provide access to subscriptions on the campus network may be sufficient for smaller institutions or colleges that do not have online programs. However, testing off-campus access to electronic resources is essential for larger institutions or universities with large online programs. There are a few options for approaching this task. First, there is the option to test links from a device that is physically off campus and away from the network proxy. This method authenticates what off-campus students experience when they attempt to access the institution's resources. However, some crucial steps must be considered when choosing this testing method. Whoever is testing needs to be sure that they clear their cache and cookies on their browser every time before the tester executes a URL in a browser. Clearing one's cache and cookies should allow the tester to trigger the institution's single sign-on when executing a URL in a browser, which should happen when testing off-campus access. A second option for testing would be to set up a dedicated computer with a specific network attachment that bypasses the campus IP. This option may pose certain security risks, but if the computer is not easily accessible, it may be the most convenient option for librarians who want to test off-campus access that must be on campus for their jobs. Finally, organizations could use a virtual lab, such as Azure Virtual Lab from Microsoft, to simulate off-campus access.

LIAISING WITH OPENATHENS DIRECTLY

Liberty University chose to work with OpenAthens directly for both the initial implementation of OpenAthens and future technical support. The implementation process began by working with a dedicated onboarding team from OpenAthens. OpenAthens trains these staff members to liaise with vendors and troubleshoot issues with transitioning links from other forms of authentication to OpenAthens authentication. If your organization collaborates directly with OpenAthens for implementation, your project manager must consider a few elements before committing to an onboarding plan. First, it is helpful to be mindful of the time difference between the United Kingdom and the United States. This point is crucial for scheduling granular meetings to troubleshoot issues found in testing. Furthermore, staying informed of holidays in the United Kingdom is vital as these holidays will affect the availability of OpenAthens staff. Generally, the most effective time to schedule meetings will be earlier in the morning if your library or organization is in the United States to accommodate the time difference. Second, it will be necessary to schedule both update meetings with stakeholders and granular meetings with OpenAthens staff to troubleshoot issues that came up with testing. Finally, technical support staff must host granular meetings with OpenAthens staff

David J. Leffler is the Discovery & Access Librarian at Liberty University

on software with screen-sharing functionality. This functionality will drastically reduce the time it takes to resolve technical issues.

EXPLAINING OPENATHENS TERMINOLOGY

URL Terminology

One of the obstacles to transitioning to OpenAthens authentication is understanding the technical jargon associated with a URL's various components that successfully provide access to an electronic resource. The term "domain" refers to the part of the URL that is unique to the identity provider without the HTTP:// or anything after the domain. An example of a domain is liberty.edu, Liberty University's domain. "Link structures" refers to several components that construct a URL. These components, such as HTTPS, www., domain, and the target destination, create the specific link structure that comprises every URL. The term "target" within a URL refers to the page the URL intends to send the user. Link structures can vary from service providers, and technical support staff must familiarize themselves with how specific vendors structure their links to resolve access issues. Usually, links will have recurring characters such as dashes and forward slashes found in most link structures. However, these characters can change if a link is encoded. The term "encoding" refers to changing certain characters in a URL, such as a dash or a dot, into encrypted characters, such as a percentage sign, that are easier for a computer to read. Links created using the OpenAthens link generator tool are encoded to provide more reliable access to electronic resources.

Organizational Terminology

There are three distinct types of organizations that serve a role in authenticating users to access electronic resources: Identity Providers (IDPs), Service Providers (SPs), and intermediary organizations that provide authentication, such as OpenAthens (OA). Identity Providers are usually universities or large organizations seeking secure access to the electronic resources that service providers offer. Service Providers have the electronic resources or digital content that identity providers want to provide their users.

General Terminology

Some general technical terms associated with OpenAthens may help project managers and librarians develop a better overall understanding of how OpenAthens authentication works. For example, "SAML" is a term that refers to the security assertion markup language that is used with OpenAthens authentication. SAML was created to allow organizations to send attributes of the organization's users to OpenAthens and service providers. The term "attributes" refers to information that can be transmitted and used for things such as mapping permissions that are used for identifying elements from users such as email address, first name, last name, and more. These attributes usually come from an identity provider's local directory and are sent through redirector links.

Redirector links take users to a target location through an intermediary organization, such as OpenAthens. Therefore, when a user executes a redirector link, OpenAthens performs a login authentication check. If the user is from an approved identity provider, the user is sent to the electronic resource specified in the URL's target. Redirector links contain the entity ID of the identity provider, which is checked against the federation, then forwards the user to the target. However, organizations are not restricted to using SAML through OpenAthens if they want to use this language to send their attributes to service providers. An open-source single sign-on system known as Shibboleth uses the SAML protocol. The disadvantage of using Shibboleth is that Shibboleth is not user-friendly, and it usually requires a specialist to set it up. The term “single sign on” (SSO) refers to a single task that requires users to enter their credentials, usually a username and password, to confirm that they are a member of an organization.

In certain situations, it may be necessary for different programs to be able to communicate with each other to provide access to electronic resources or optimize authentication. Application programming interfaces (APIs) are strings of code that provide a way for two applications to communicate with each other. Subsequently, an “API Key” is a string of characters that allow organizations to access a particular API.

Authentication Terminology

There are key terms to grasp when attempting to understand authentication terminology. There are three primary forms of authentication provided by OpenAthens. First is “proxied access,” which refers to a user accessing an electronic resource through IP authentication. Subsequently, “IP authentication” is a form of authentication that uses a unique string of characters to indicate where the user is coming from to check if the user is attempting to access an electronic resource from an approved identity provider. The second is “federated access,” which refers to a group of entities that have all agreed to share their metadata within a trusted host, making it easier within that federation to connect and provide access to their electronic holdings. Organizations that want to set up federated access with service providers must have an entity ID and unique scope that provides identities for the organization’s users. An entity ID is a unique ID that federations use to distinguish between organizations. Every organization that uses federated access has a unique entity ID. An organization’s entity ID usually contains the organization’s domain within the entity ID, but the entity ID can be anything, and there is no standardization or requirement in this area. An organization can have multiple scopes depending on how many sub-organizations fall under the larger organization. The third and final form of OpenAthens authentication is “bilaterally connected access.” This form of authentication is essentially a federated connection between two organizations. Bilateral connections require organizations to send each other their metadata and consume that metadata to create a connection between the service provider and the organization to create a secure connection.

WAYF Terminology

A “WAYF” or “where are you from” webpage is a form of verification used by service providers as a way for users to confirm that they are affiliated with their identity provider and access an electronic resource. When a user attempts to access an electronic resource and encounters an institutional login page, they encounter a service provider’s WAYF page. Subsequently, WAYFless links are links with a unique ID within that link, such as a customer ID, that is unique to the identity provider. Therefore, when a user executes a WAYFless link, they are not asked to select the institution of their identity provider and are brought directly to the target destination of the electronic resource.

ONBOARDING OPENATHENS IN MULTIPLE ENVIRONMENTS

One of the distinct challenges of onboarding OpenAthens authentication is navigating the various logistical issues for transitioning links in different electronic environments to OpenAthens links. For Liberty University, the primary electronic environments involved in the OpenAthens implementation project were Springshare, Alma, and Canvas. There were more electronic environments involved in Liberty University's transition to OpenAthens authentication. Still, these three electronic environments posed distinct challenges that may apply to other integrated library systems or learning management systems.

Springshare

Springshare is a company that provides various digital products for libraries and librarians. Springshare's "A-Z Database List" in their suite of library applications is the product that Liberty University uses to store the links supplied by service providers to access electronic subscriptions. The "A-Z Database List" makes these subscriptions discoverable and accessible on Jerry Falwell Library's "A-Z databases" webpage. One of the main challenges for onboarding OpenAthens links in this electronic environment is switching every link stored in Springshare to the OpenAthens version of the link. The workflow for EZproxied links simply entails obtaining a URL from the vendor, putting that URL into Springshare, then switching the "proxy" feature to "on." This proxy feature adds the organization's EZproxy prefix to the beginning of the URL that is stored in Springshare. Unfortunately, this workflow will not work for OpenAthens links. For OpenAthens, every URL must be put through an OpenAthens link generator to encode the link. As of the date of the publication of this article, encoding functionality is not supported in Springshare's "A-Z Database List" product. If a librarian or technical support staff switched their organization's proxy prefix in the "A-Z Database List" from their EZproxy prefix to their OpenAthens prefix, access to the URL might break since the OpenAthens URL is not encoded. Therefore, whoever is responsible for onboarding OpenAthens will need to export the links from their "A-Z Database List." Then they must put these links through the OpenAthens link generator, manually replace each URL, and turn the "Proxy Enabled" status to "No" for every electronic subscription in their organization's "A-Z Database List."

Alma

Liberty University uses Summon over Alma as its pairing for a discovery layer and integrated library system. Alma posed unique challenges for transitioning every electronic collection from EZproxy authentication to OpenAthens authentication. The most significant initial hurdle for libraries that use Alma and plan to switch to OpenAthens authentication is ensuring that every electronic collection is documented before making any changes to ensure that no electronic resource is missed during implementation. Once all the electronic collections are documented, the next step is to ensure that every electronic collection is configured correctly to accept their organization's OpenAthens prefix. To implement this step, Liberty University removed the embedded proxy from the links in every electronic collection in both the bib records and portfolios, then turned on the proxy for the portfolios. Liberty University did not use the "default" proxy setting in Alma to make a mass change to its electronic collections. Instead, Liberty University chose to use the non-default proxy setting so that electronic resources staff could control when electronic collections were switched to OpenAthens authentication. Therefore, onboarding OpenAthens in Alma may require collaboration between electronic resource catalogers, librarians, and Alma administrators.

Canvas

Liberty University uses Canvas as its primary learning management system. This electronic environment posed the most significant risk as it is where students directly access their course's content and electronic resources with those courses. Due to the extremely high volume of links contained in Canvas, Liberty University used a scripting process to automatically change all the links in Canvas from EZproxy authentication to OpenAthens authentication. ProQuest Ebook Central provides eBooks that are the critical point of failure for onboarding OpenAthens in any learning management system. ProQuest Ebook Central was the only subscription that Liberty University encountered that could not authenticate concurrently through both EZproxy authentication and OpenAthens authentication. In other words, libraries that license books from ProQuest Ebook Central must choose either EZproxy authentication or OpenAthens authentication. Therefore, there must be a technical staff team actively testing titles from Ebook Central post-implementation to ensure a successful change from EZproxy to OpenAthens. Manual changing of links will be required for any overhaul of links for an organization's learning management system.

Although there are challenges in transitioning to OpenAthens authentication, the added security, ease of maintenance, and enhanced reporting capabilities provided by OpenAthens may make the logistical and financial cost worthwhile. Project managers and librarians with the appropriate expectations and understanding of the technical jargon associated with OpenAthens will effectively onboard OpenAthens authentication for their organization.