Summon: Remote Authentication Methods

- **Product:** Summon

What types of remote authentication may be used with Summon?

To provide seamless remote-user access to your subscription resources in the Summon service, your library must utilize either a proxy server or VPN-type authentication. Libraries using Athens or Shibboleth for patron identification should also have a proxy server configured for the best remote-user experience.

If your library does not use any form of remote user authentication, the Summon service will provide result links that require your users to log in to the third-party platforms that store the subscription content.

Web-Based Proxy Server

A web-based proxy works by rewriting the URL to the resource to include the proxy URL's syntax. Examples of web-based proxy servers include EZProxy, III WAM, and HAN. Summon fully supports web-based proxy systems by rewriting the URLs of Index-Enhanced Direct Links to include your library's proxy syntax, and by rewriting the URL in the Authentication Banner. A web-based proxy is currently the only mechanism for rewriting the URL in the authentication banner in order to redirect users to the results page.

For details and setup instructions, see this document. Also, make sure to include the proper resource domains in your proxy configuration file.

Virtual Private Network (VPN) or Browser-based Proxy Server

A VPN creates a connection between the user's computer and the library's network by providing the user with an IP address in the institution's range, regardless of where the user is physically. Essentially, the VPN client makes it appear as though the user is on campus, and subsequent access to content is via IP authentication.

Browser-based proxy servers are those that require the user to alter the settings in his/her computer's browser to connect to the library's IP range. (These differ from web-based proxies, which direct the user to a web-based login page by rewriting the resource URLs, and do not require browser configuration.) In that it allows a network user experience based upon IP authentication, a browser-based proxy works similarly to a VPN. An example of a common browser-based proxy server is Squid.

For a more seamless user experience using Summon with these authentication methods, your library's web site may be designed to encourage or require the user to log in to VPN or configure their browser before issuing a search in Summon. This way, the user will be able to access the links to content via IP authentication, without further login challenges.

If you use a VPN system, we encourage you to configure remote access by customizing the URL or text (or both) of the authentication banner in the Summon results page:

- In this scenario, the user clicks the banner and logs in to the VPN login page specified by the custom URL in the authentication banner.

- The user returns to the Summon search page, rather than to the results page, even if they have already submitted a search.

If you use a browser-based proxy, we encourage you to link the authentication banner to an informational page about how to set up a browser to connect via your system.

Alternatively, the library can choose to remove the authentication banner.

Using SAML with the Authentication Banner

There is also an option to log on using SAML instead of the proxy. Currently, customers who want to use SAML authentication with the authentication banner must open a Support ticket to have their configurations updated since this configuration is not supported in the Admin Console.

The proxy alters the IP and domain of the Summon site, but the SAML login does not. However, both methods ensure that users searching for records do so with `s.role=authenticated`.

Proxied links will still require users to sign into the proxy server (for example, EZproxy), making this solution specialized and most suitable for customers using SAML to sign into the proxy. This setup allows for a seamless experience when using SAML sign-in for Summon and later for the proxy. This is particularly beneficial if customers are leveraging SAML sign-in for the SAML drive (Summon cloud) for saved searches, saved items, or as a mechanism to sign into Summon via Sierra by making it possible for users to leverage all the features by signing in only once.

Limitations of Athens and Shibboleth

Within the architecture of remote-user authentication, Athens and Shibboleth are identity providers and not end-to-end single-sign-on solutions. If your library uses Athens or Shibboleth, you will still need to use a web-based proxy server for the best remote-user experience in Summon. The US-based Shibboleth federation, has published an excellent Best Practices document that explains the Shibboleth/EZProxy hybrid model in detail

If your library is using Athens or Shibboleth but has no web-based proxy server, your patrons will encounter challenges in three areas: authentication banner, index-enhanced direct links, and OpenURL linking through 360 Link.

Authentication Banner

Athens/Shibboleth clients who have no web-based proxy are encouraged to configure remote access by customizing the URL or text (or both) of the authentication banner in the Summon results page:

- In this scenario, the user clicks the banner and logs in to the Athens/Shibboleth login page specified by the custom URL in the authentication banner.
- The user then returns to the Summon search page, rather than to the results page, even if they have already submitted a search.

Note

A web-based proxy is currently the only mechanism for rewriting the URL in the banner in order to redirect users to the results page.

- Alternatively, your library may choose to remove the authentication banner.

Index-Enhanced Direct Links

Without a web-based proxy to rewrite Summon's direct-link URLs, your users may encounter vendor login pages when clicking direct links. This is because many of Summon's direct link URLs will not be WAYF-less. (A WAYF-less URL is a specially constructed link to a federation-authenticated resource that enables the user to go directly to an identity provider). Without the URL-rewriting function of a web-based proxy to supply the WAYF information, remote users will be prompted to log in to the content provider. If this presents problems for your users, we suggest that you customize the priority of order for resource links in your results.

OpenURL linking through 360 Link

360 Link supports Athens and Shibboleth for user authentication. This user authentication is a single-sign-on (SSO) solution into 360 Link, but that does not mean it is an SSO solution through the outbound links into subscription content from Athens- or Shibboleth-enabled content providers:

- In this scenario the Summon user clicks on an OpenURL link in Summon and logs in through Athens/Shibboleth before viewing the 360 Link results.
- Linking into the content varies by provider, as explained in this Answer.

Note

Ideally, your library uses a proxy server in conjunction with Athens/Shibboleth to provide a true SSO solution across providers.

For more about using Athens/Shibboleth with 360 Link, see this Answer.

If you wish to enable this, click here for instructions. After you have worked through the steps in that Answer, use the **Support Portal** option at the top of this page to ask us to complete the Athens or Shibboleth configuration for 360 Link.

Referring URL Authentication

The Summon service supports Referring URL for remotely authenticating users into your library's subscribed content, but Support is required for configuration.

No Remote Authentication Method

If there is no method of remote authentication configured in your library's Summon service or in your library's systems, then remote users of Summon will be directed to vendors' login pages instead of accessing their subscription content when they click Index-Enhanced Direct Links, because the vendors will not recognize that the user is affiliated with your organization. Also, the authentication banner should be removed or customized to serve as a custom link if desired.

- **Date Created:** 9-Feb-2014
- **Last Edited Date:** 20-Feb-2014
- **Old Article Number:** 8834