Splunk® Enterprise Securing Splunk Enterprise 7.3.2

About Single Sign-On using reverse proxy

Generated: 10/10/2019 11:42 pm
About Single Sign-On using reverse proxy

Splunk Single Sign-on (SSO) lets you use a reverse proxy to handle Splunk authentication, meaning that once the user has logged into their proxy, they can seamlessly access Splunk Web (and presumably any other applications configured to your proxy).

The reverse proxy implementation of Splunk Enterprise SSO supports logging into Splunk Enterprise only through Splunk Web. Since the implementation relies on cookies to save authentication information, SSO cannot be used for CLI authentication to Splunk Enterprise. Invoking https://localhost:8089 (or the assigned management port) still requires independent authentication.

For more information about how to configure these items and set up SSO, see Configure Single Sign-On

How it works

Splunk Enterprise administrators and users invoke Splunk Web via a proxy URL that is deployed with Splunk Web. The proxy authenticates the incoming request against your authentication system. Upon successful authentication the proxy sets a request header with the authenticated identity’s attribute and sends this information to Splunk Enterprise.

Splunk Enterprise accepts the incoming HTTP request from the proxy, and if Splunk Enterprise recognizes the user contained in the header, the user bypasses the login page and is automatically authorized.

For successful single sign-on, all requests from the proxy to Splunk Web must include this authenticated header. If the header is not included in a request, then the user is returned to the login page or an error page, depending on your configuration. Splunk software uses this authenticated header for the duration of the browser session.

How Splunk software processes the proxy request

When the proxy server makes a request to Splunk Web, Splunk Web looks to the trustedIP value in web.conf to verify that the proxy’s IP is on the trusted IP list.

If the IP is not trusted, the request is rejected and the sign-on attempt fails. If the IP address is trusted, then Splunk Web queries for the identity in the request
header and sends splunkd an authorization request containing that header information.

Upon receiving the authorization request from Splunk Web, splunkd verifies whether the incoming IP address of the client (usually Splunk Web) matches the value of the trustedIP property of the server.conf file.

If the IP addresses are not in the trustedIP list the request is rejected and the sign-on attempt fails. The user is either returned to a login page or shown an error page, depending upon your SSOmode configuration in web.conf. For more on this attribute and other configuration information, see Configure Splunk Single Sign-On.

If the IP is trusted, then splunkd uses the information contained in the request header and conducts the authorization process.
How Splunk software authorizes the user

Splunk software first checks to see if the given identity and role matches any of your Splunk users. If no match is found, Splunk software looks to see if there are any LDAP matches. (For information about how Splunk software authenticates users, see Set up user authentication with LDAP in this manual.)

If no match is found and the user contained in the header cannot be authorized, then the browser redirects to an error page.

If a match is found, Splunk software authorizes the user and checks to see if an existing session is present. If a session already exists, Splunk software uses that session identifier and creates the necessary cookies to allow the user access to Splunk Web. If a session does not exist, then Splunk software creates a new session as well as the necessary cookies for Splunk Web authorization.

After the cookies are created, Splunk Web resumes its normal flow. Any subsequent access to Splunk Enterprise through the proxy URL does not require re-authorization as long as the request header contains the trusted identity and until the user closes the browser session.