Splunk® Enterprise
Securing Splunk Enterprise 7.0.0

Configure single sign-on with SAML

Generated: 5/31/2020 4:24 pm
Configure single sign-on with SAML

You can configure Splunk software to use SAML authentication for single sign-on (SSO), using information provided by your supported identity provider (IdP).

Splunk software always outputs usernames in lowercase. If your IdP expects Splunk software to preserve uppercase letters in usernames, you can change the username to lowercase in the IdP or configure the IdP to accept the lowercase version of a username.

Note that if the search head is restarted, you must re-enter your credentials to access saved searches.

Prerequisites

-  Either:
  - A running version of Splunk software OR
  - A managed deployment of Splunk Cloud. Self-service deployments of Splunk Cloud log in through the Splunk customer portal and cannot independently configure SAML SSO.
-  An identity provider configured to provide the role, realName, and mail attributes. The supported identity providers are:
  - Ping Identity
  - Okta
  - Azure AD
  - AD FS
  - OneLogin
  - Optimal
  - CA siteminder
-  An admin role (Splunk Enterprise) or sc_admin role (Splunk Cloud) with the change_authentication capability. This permission level lets you enable SAML and edit authentication settings on the Splunk search head.

Other IdPs

Any SAML IdP that is v2 compliant should be configurable, including the following tested IdPs. For assistance with any IdP that is not documented in this chapter, contact Support:

- SecureAuth
- Novell Directory
- G Suite (Formerly Google Apps for Business)

Configure SAML to work with your IdP

SAML does not support encryption, regardless of IdP.

1. Configure SAML SSO with:

   - Ping Identity
   - Okta
   - Azure AD or AD FS
   - OneLogin
   - Optimal
   - CA siteminder
2. Map SAML groups to Splunk Enterprise roles.