Splunk® Enterprise Inherit a Splunk Enterprise Deployment 7.3.0

Users, roles, and authentication

Generated: 7/24/2019 7:52 am
Users, roles, and authentication

Once you have familiarized yourself with your Splunk configuration and data, review your users, their permissions, and their authorization methods.

Splunk Enterprise supports several user authentication systems:

- Splunk internal authentication with role-based user access
- LDAP
- A scripted authentication API for use with an external authentication system, such as PAM or RADIUS
- Multifactor authentication
- Single sign-on

Internal authentication and role-based user access

Role-based access control lets you manage users and restrict or share Splunk Enterprise data. Splunk Enterprise masks data to users in the similar manners that a relational database manages role-based access control.

Discover or modify existing configurations

Familiarize yourself with your existing users and their assigned roles. Roles determine the user’s data access level and the actions they can perform.

In Splunk Web click Settings > Access Controls to see all of your Splunk users. On the Access Controls page you can click on roles and users to examine or edit permissions. You can use this page to create a list of the data available to each user or group of users. See Use access control to secure Splunk data in Securing Splunk Enterprise.

To find a specific user you can use the CLI to search for a user and role. See Find existing users and roles in Securing Splunk Enterprise.

LDAP authentication

When administrators configure Splunk to work with LDAP, they create something called "LDAP strategies". LDAP strategies are collections of configuration data that Splunk uses to work with your LDAP configuration. Splunk can be directed to query these "strategies" in a particular order when searching for LDAP users. See Set up user authentication with LDAP in Securing Splunk Enterprise.
Discover or modify existing LDAP configurations

Familiarize yourself with the existing LDAP groups and permissions mappings by looking at all of your strategies. To view or edit existing LDAP strategies, follow these steps:

1. Under **Users and authentication** click **Access controls**.

2. Click **LDAP**.

3. From this page, you can select strategies and view their information and track those LDAP mappings to Splunk roles.

See Configure LDAP with Splunk Web in *Securing Splunk Enterprise*.

Multifactor authentication

Splunk Enterprise currently supports multifactor authentication with Duo Security. See About two-factor authentication with Duo Security in *Securing Splunk Enterprise*.

Find or modify existing configurations

Find out if your system uses Duo Factor Authentication via Splunk Web.

1. Under **Settings** click **Users and Authentication**

2. For **Authentication Method** select **Duo Security**.

3. On this page you can see if your system has multifactor authentication configured. See Configure Splunk Enterprise to use Duo Security two-factor authentication in *Securing Splunk Enterprise*.

SSO with SAML

Splunk software can leverage SAML authentication for single sign-on (SSO), using information provided by an external identity provider (IdP). See Authentication using single sign-on with SAML in *Securing Splunk Enterprise*.

Find or modify existing configurations

Find out if your users are configured for SAML SSO.
1. In **Settings** select **Access Controls**.

2. Under **Authentication method** select SAML.

3. A new SAML configuration appears, you can close this page to view the existing configuration.

In this page you can see if your system has SSO authentication configured for groups of users. From there you can drill down to your IdP information, the mapped groups, and the users assigned to that group.

**ProxySSO authentication**

ProxySSO lets you configure Single-Sign On (SSO) for Splunk instances through a reverse proxy server. A user logged in using ProxySSO can seamlessly access Splunk Web.

**Find existing configurations**

You can view any existing HTTP request headers that the proxy server sends to Splunk Web:

Set `enableWebDebug=true` in `web.conf` under `settings` stanza:

```
```

ProxySSO login events are logged in `var/log/splunkd.log`. 

3