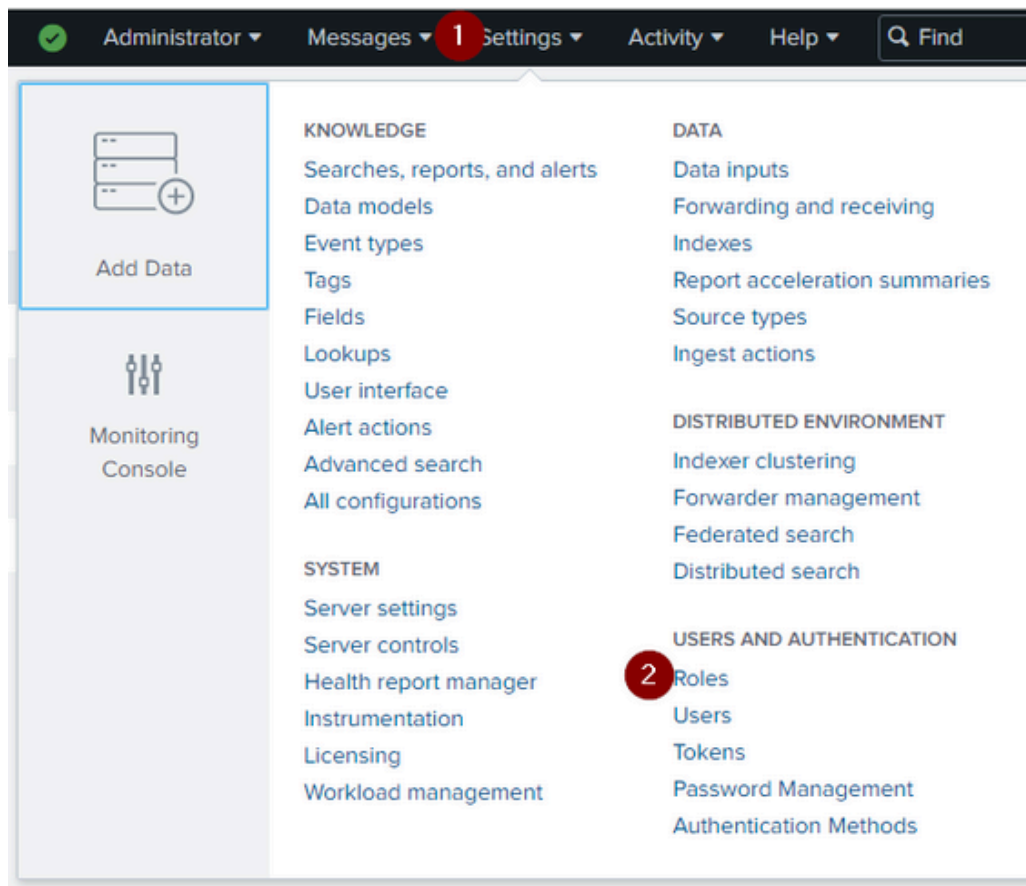# User Management on Splunk

By: Ryan Stewart

Roles

By default, Splunk provides several roles. To locate or create a new role, navigate to Settings > Roles. Here, you can edit existing roles or add new ones. Roles grant permissions across various aspects, such as the Splunk server, Splunk requests, determining which events are visible or hidden, and more.

Roles

5 Roles | filter

Name	Actions	Native capabilities	Inherited capabilities	Default App
admin	Edit ▾	114	39	
can_delete	Edit ▾	6	0	
power	Edit ▾	10	29	
splunk-system-role	Edit ▾	0	153	
user	Edit ▾	29	0	

New Role

Users

Upon installation, Splunk assigns only one user, typically named "admin." A best practice is to create an additional administrator account, reserving the "admin" account for emergency cases. This approach helps identify potential issues if an admin connection is detected.

To view the list of users and create a new one, go to Settings > Users. Remember, each user must be associated with a specific role.
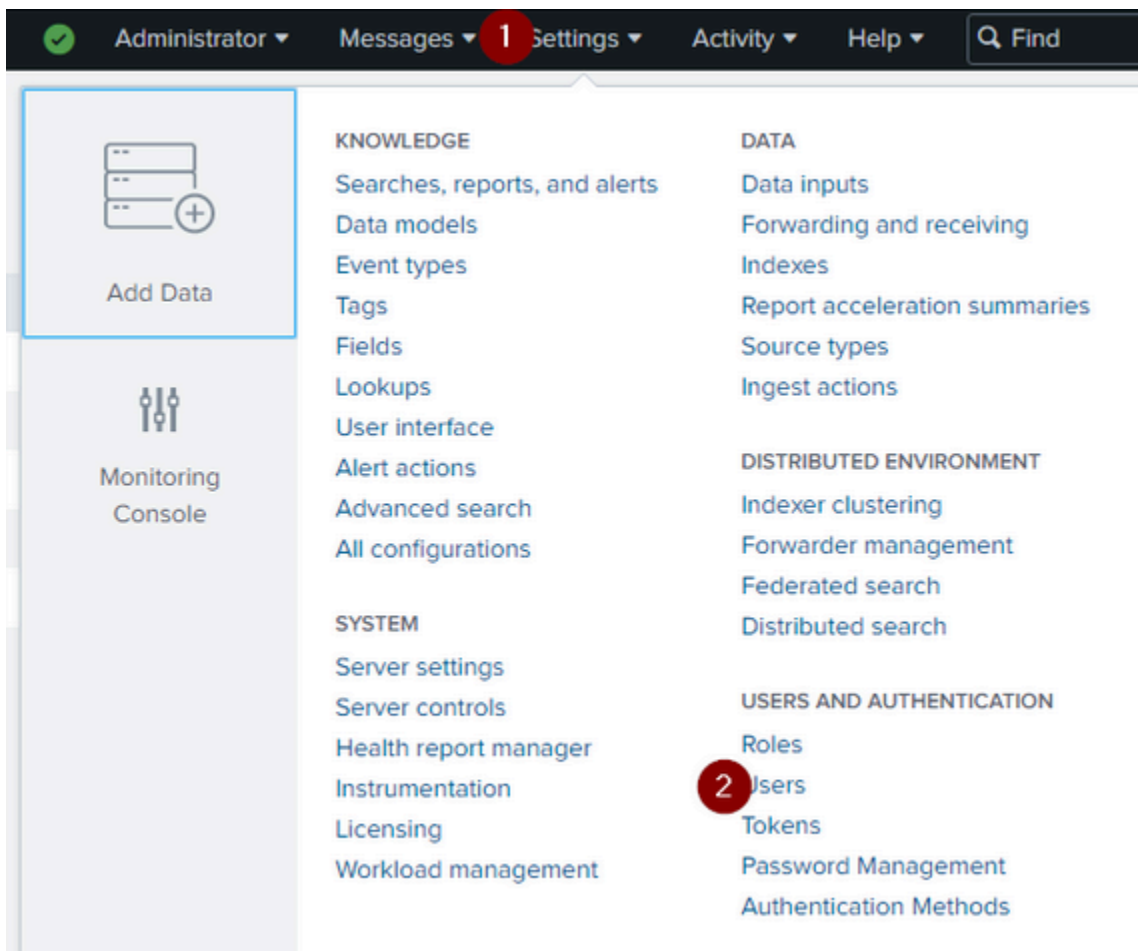
Password Management

During Splunk installation, only an 8-character password is required, regardless of complexity. Modify password settings by navigating to Settings > Password Management.