

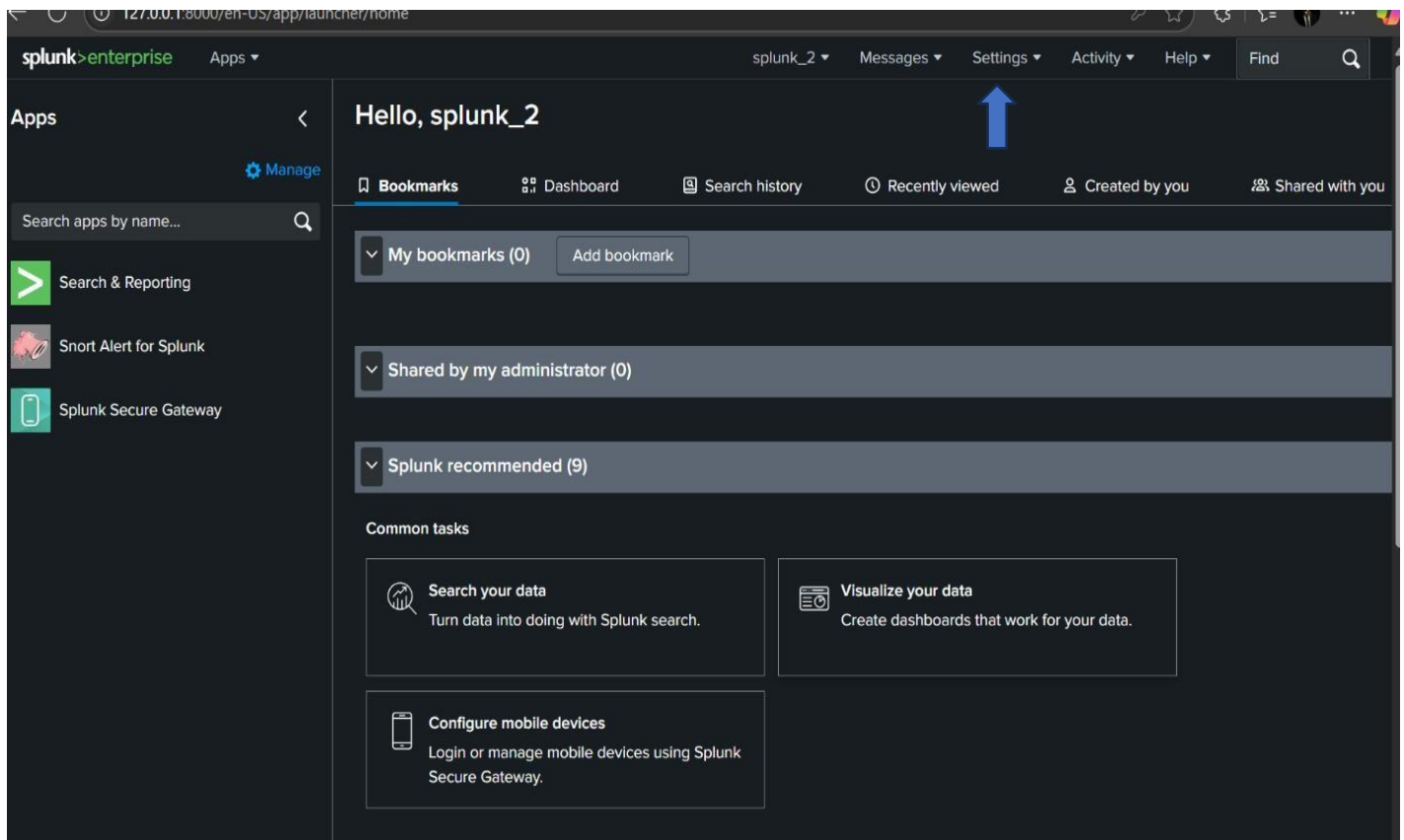


Managing Users and Permissions in Splunk

Getting Started with Splunk User Management - Step 1

First step: Log in to the Splunk portal to begin the process of adding a new user.

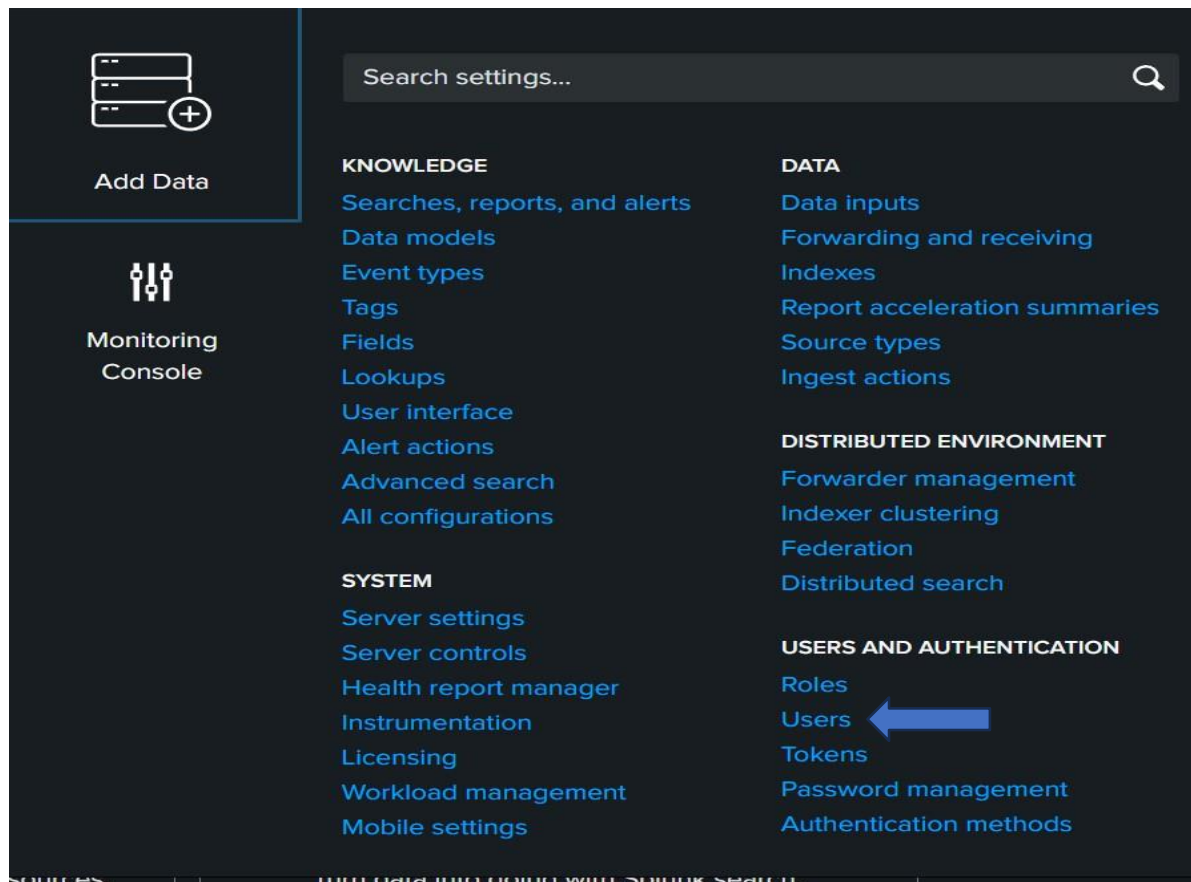
Efficient access control starts with proper user setup! 🖥️🔑



🔍 User Creation in Splunk – Step 2

After accessing the portal, head over to the **Settings** tab and choose **Users** to initiate the creation of a new user.

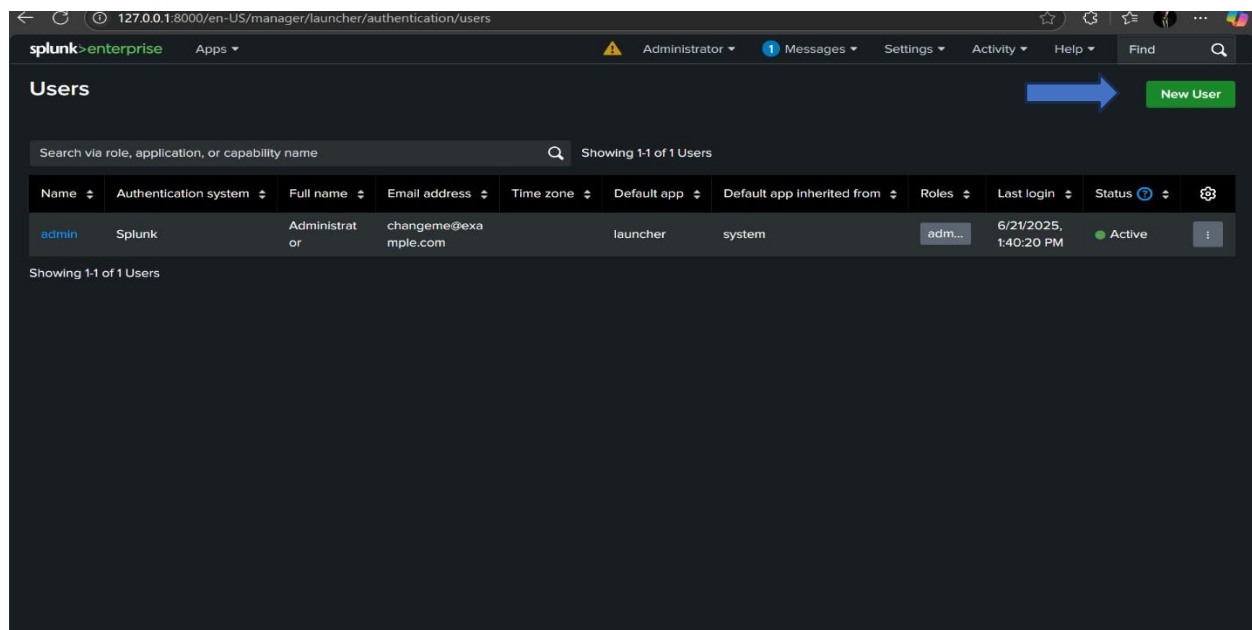
Managing access effectively is key to secure operations! 🔑➕



Splunk User Management – Step 3

Click on **Add User**, assign the necessary roles and specify the index access permissions.

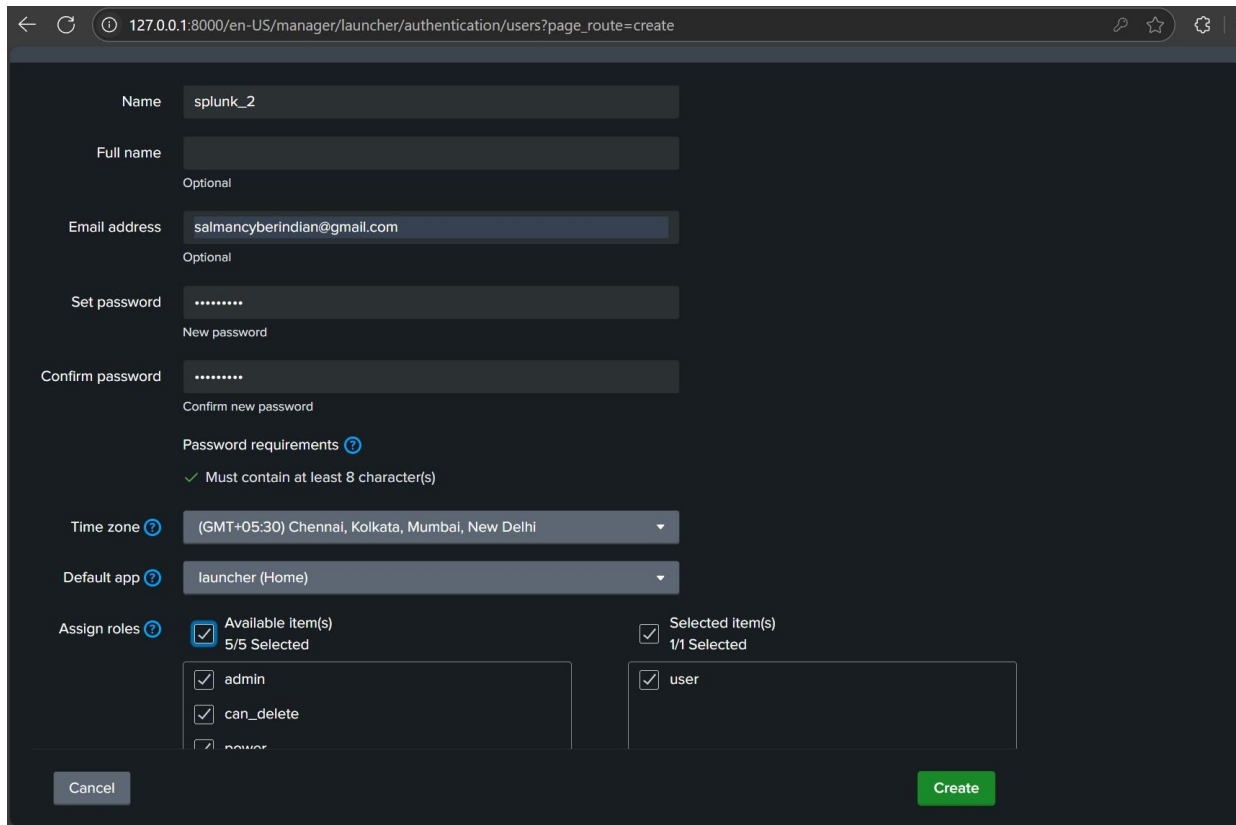
Finalize the setup to successfully create the new user in Splunk.  



Splunk User Management – Step 4

Enter all necessary user details as required by Splunk to ensure successful account creation.

Accuracy in user configuration enhances system security and access control.



127.0.0.1:8000/en-US/manager/launcher/authentication/users?page_route=create

Name: splunk_2

Full name: [Optional]

Email address: salmancyberindian@gmail.com [Optional]

Set password: [New password]

Confirm password: [Confirm new password]

Password requirements: Must contain at least 8 character(s)

Time zone: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

Default app: launcher (Home)


Assign roles:

Available item(s) 5/5 Selected	Selected item(s) 1/1 Selected
<input checked="" type="checkbox"/> admin	<input checked="" type="checkbox"/> user
<input checked="" type="checkbox"/> can_delete	
<input checked="" type="checkbox"/> never	

Cancel Create

Splunk User Management – Step 5

After submitting the user details, the new account will be successfully created and reflected in the **User Dashboard**.

A seamless user creation process ensures better visibility and control. 

Search via role, application, or capability name									
Showing 1-2 of 2 Users									
Name	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last login	Status
admin	Splunk	Administrator	changeme@example.com		launcher	system	adm...	6/21/2025, 1:40:20 PM	Active
splunk_2	Splunk		salmancyberindian@gmail.com	Asia/Kolkata	launcher	system	user		Active

Showing 1-2 of 2 Users

) Splunk User Management – Step 6

Navigate to the **Indexes** section and assign relevant permissions based on the user's role and responsibilities.

For example, provide access to indexes like:

summary

audit

configtracker

dsclient

Granting the right access ensures users can only view and work with the data they need — enhancing both security and efficiency. 🛡️🔍

Splunk User Management – Step 7

Within the assigned **Role Settings**, locate the **Search Jobs** window limit and set it to **Infinite**.

📄 Don't forget to **Save** the changes to ensure the configuration is applied successfully.

Optimizing search settings allows uninterrupted data access for extended investigations and monitoring. 🔍📊