How to Create a User in Splunk and Assign Roles – Step-by-Step Guide

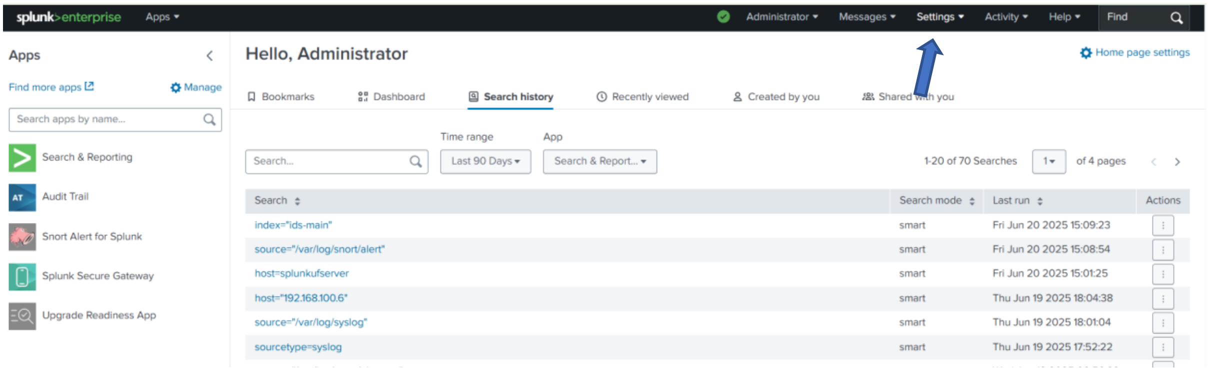
Note: You need to be logged in as a user with admin privileges.

1. Login to Splunk Web

- Open your browser and go to your Splunk instance (e.g., `http://localhost:8000`).
- Log in with your **admin** credentials.

2. Go to User Management

- Click the **Settings** (gear icon or top menu).
- Under **Users and Authentication**, click **Access controls**.
- Click **Users**.



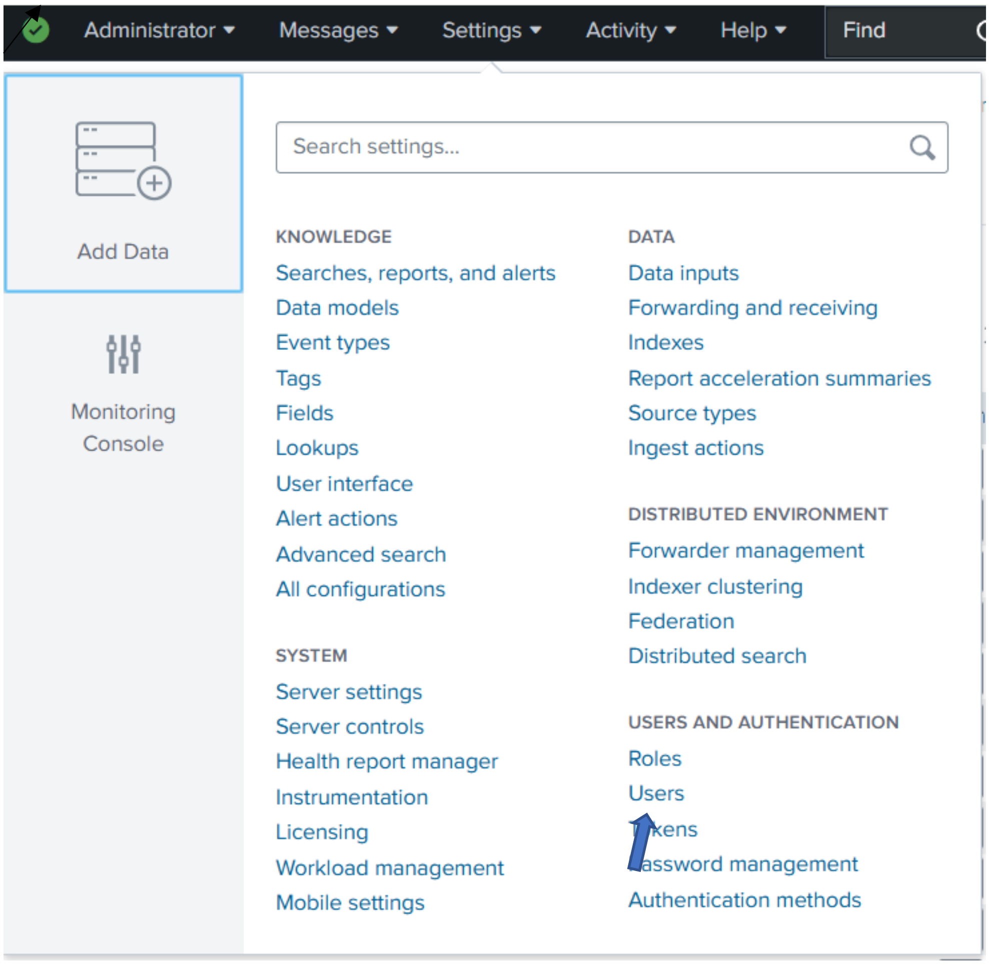
Search	Search mode	Last run	Actions
index="ids-main"	smart	Fri Jun 20 2025 15:09:23	⋮
source="/var/log/snort/alert"	smart	Fri Jun 20 2025 15:08:54	⋮
host=splunkufserver	smart	Fri Jun 20 2025 15:01:25	⋮
host="192.168.100.6"	smart	Thu Jun 19 2025 18:04:38	⋮
source="/var/log/syslog"	smart	Thu Jun 19 2025 18:01:04	⋮
sourcetype=syslog	smart	Thu Jun 19 2025 17:52:22	⋮

3. Create a New User

- Click the **“New User”** button.

You will see a form with the following fields:

Field	Description
Username	The login name for the user.
Full name	(Optional) The user's full name.
Password	Create a password for the user.
Confirm password	Re-enter the password.
Email address	Optional, for alerting and notifications.
Assigned roles	Select roles like `user`, `power`, `admin`, or custom roles.



Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data

Monitoring Console

Search settings...

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

SYSTEM

- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management
- Mobile settings

DATA

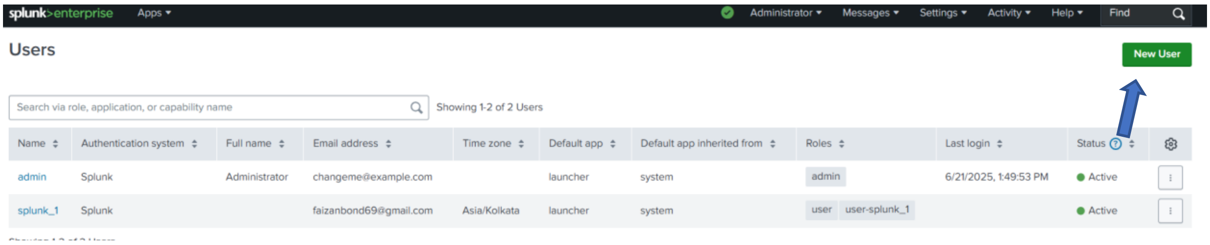
- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Forwarder management
- Indexer clustering
- Federation
- Distributed search

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password management
- Authentication methods



splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

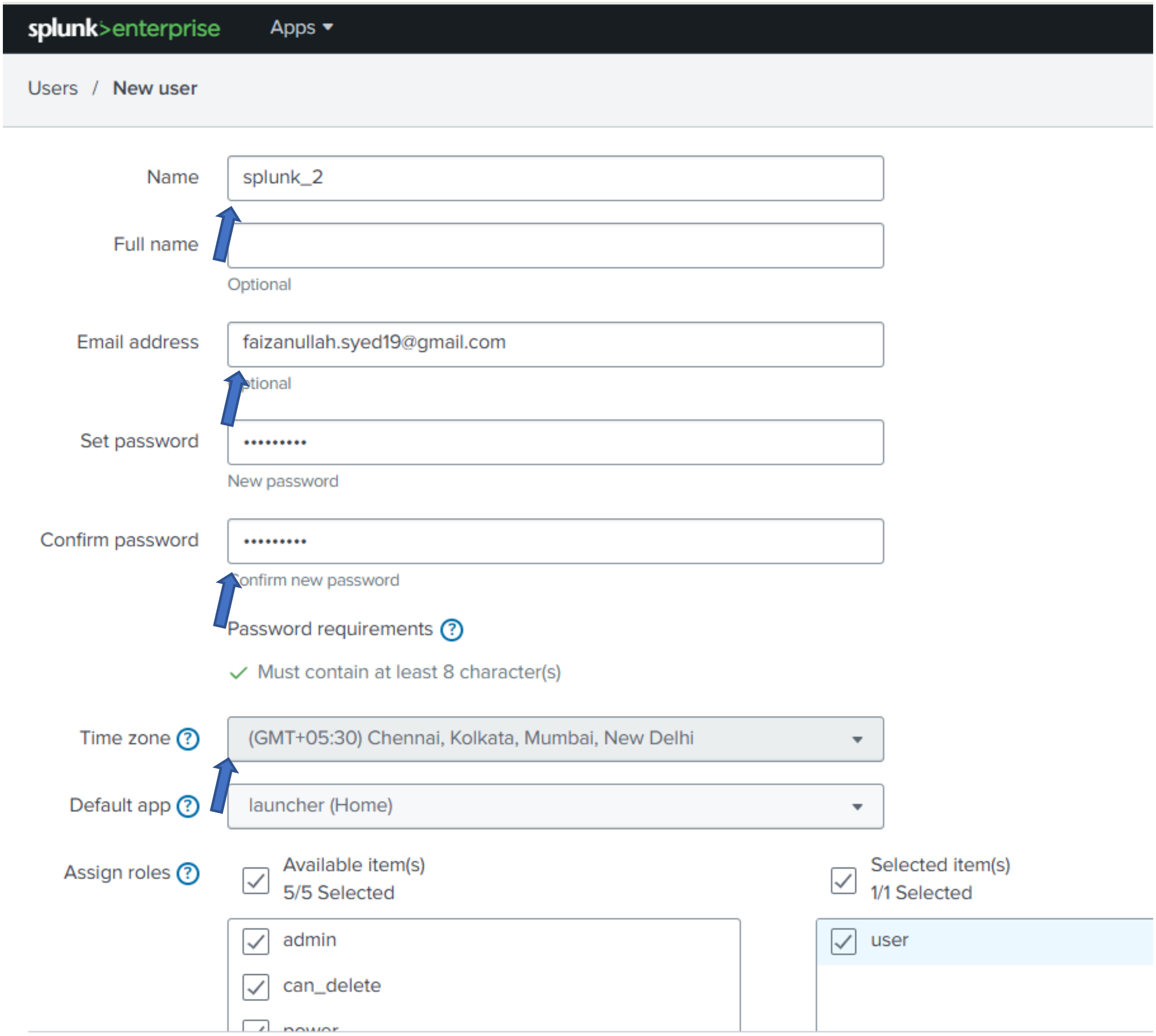
Users

New User

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	admin	6/21/2025, 1:49:53 PM	● Active
splunk_1	Splunk		faizanbond69@gmail.com	Asia/Kolkata	launcher	system	user user-splunk_1		● Active



Users / New user

Name: splunk_2

Full name:
Optional

Email address: faizanullah.syed19@gmail.com
Optional

Set password: •••••••••
New password

Confirm password: •••••••••
Confirm new password

Password requirements ?

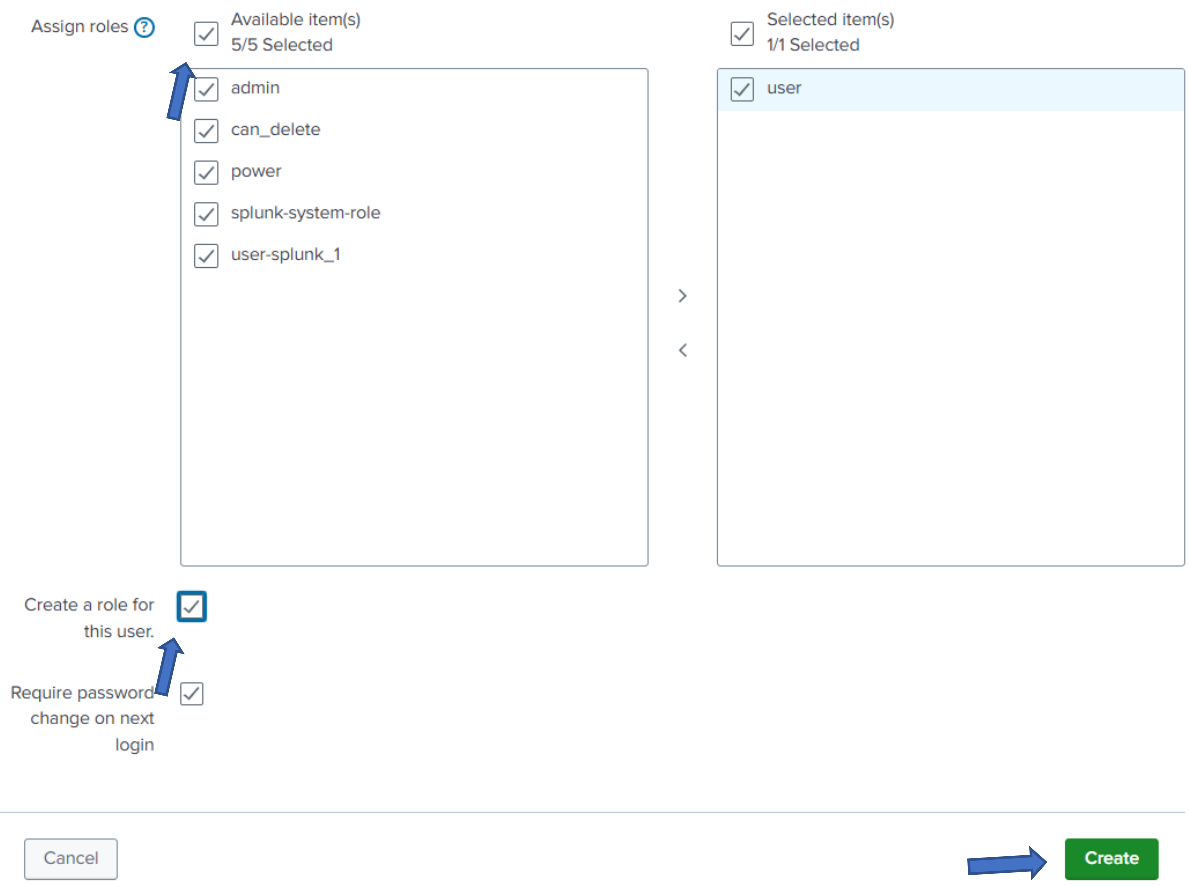
✓ Must contain at least 8 character(s)

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
☑ admin	☑ user
☑ can_delete	
☑ power	



Assign roles

☑ Available item(s) 5/5 Selected

- ☑ admin
- ☑ can_delete
- ☑ power
- ☑ splunk-system-role
- ☑ user-splunk_1

☑ Selected item(s) 1/1 Selected

- ☑ user

Create a role for this user. ☑

Require password change on next login ☑

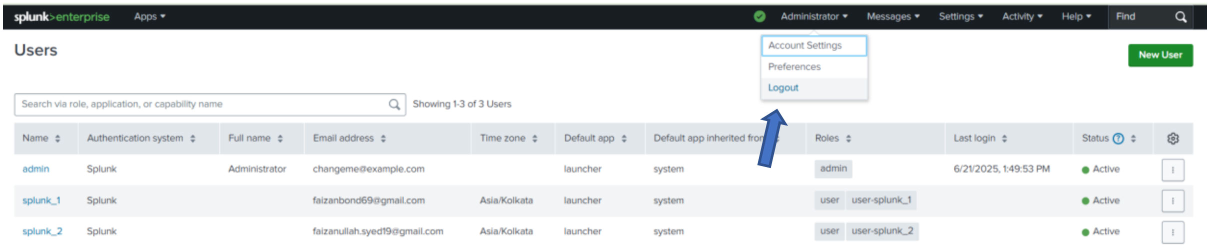
4. Assign Permissions via Roles

Splunk controls permissions via **roles**, not directly on users.

Common roles:

- `user`: Can search and view data.
- `power`: Can save searches, create reports/dashboards.
- `admin`: Full access.

You can also **create custom roles** with specific indexes, capabilities, and resources.



Users

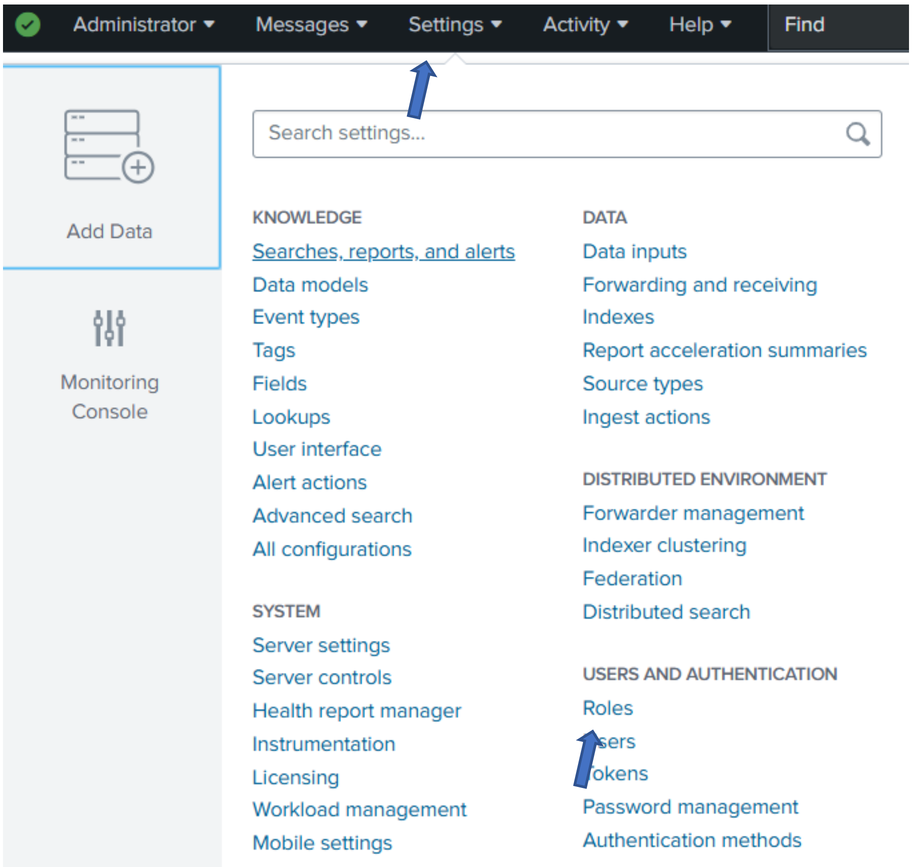
Search via role, application, or capability name

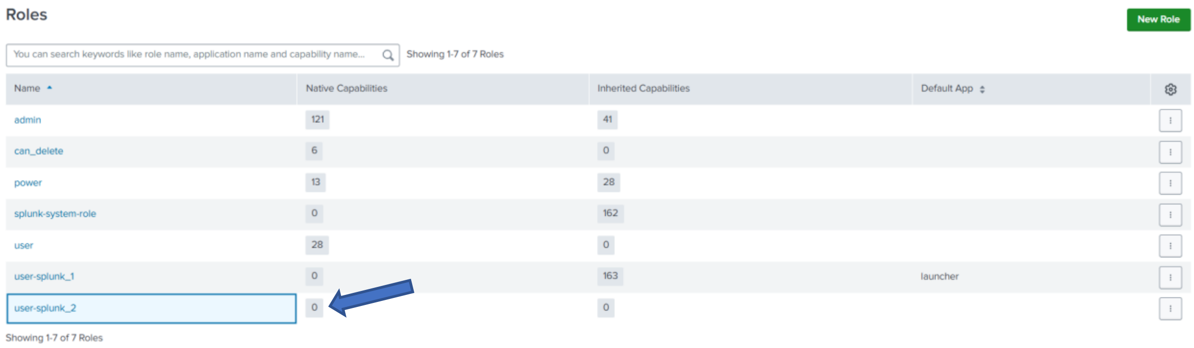
Showing 1-3 of 3 Users

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	admin	6/21/2025, 1:49:53 PM	● Active
splunk_1	Splunk		faizanbond69@gmail.com	Asia/Kolkata	launcher	system	user user-splunk_1		● Active
splunk_2	Splunk		faizanullah.syed19@gmail.com	Asia/Kolkata	launcher	system	user user-splunk_2		● Active

5. Create user.

- After filling the form, click **create.**

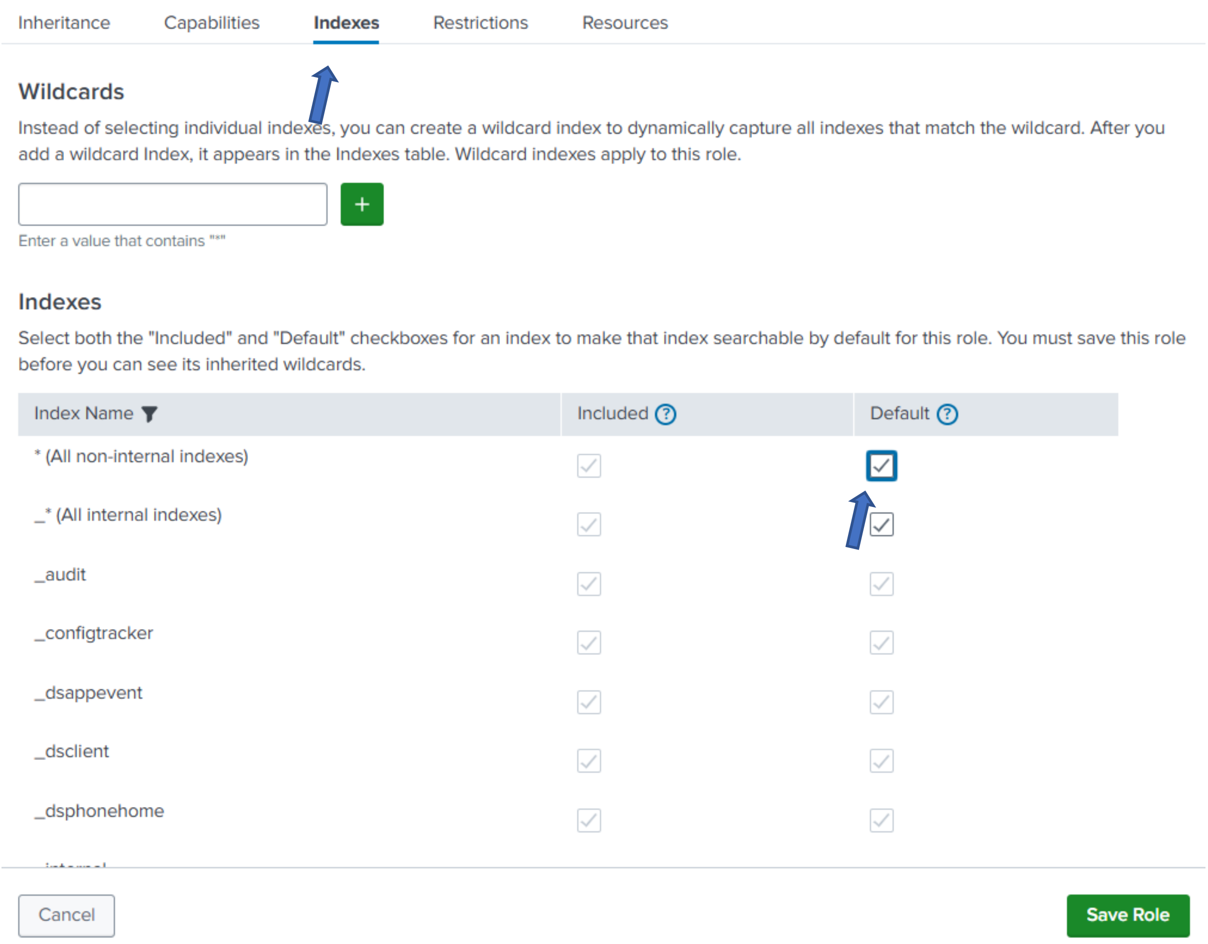



Roles
New Role
You can search keywords like role name, application name and capability name...

Showing 1-7 of 7 Roles

Name ▲	Native Capabilities	Inherited Capabilities	Default App ⇕	⚙
admin	121	41		⋮
can_delete	6	0		⋮
power	13	28		⋮
splunk-system-role	0	162		⋮
user	28	0		⋮
user-splunk_1	0	163	launcher	⋮
user-splunk_2	0	0		⋮

Showing 1-7 of 7 Roles



Wildcards

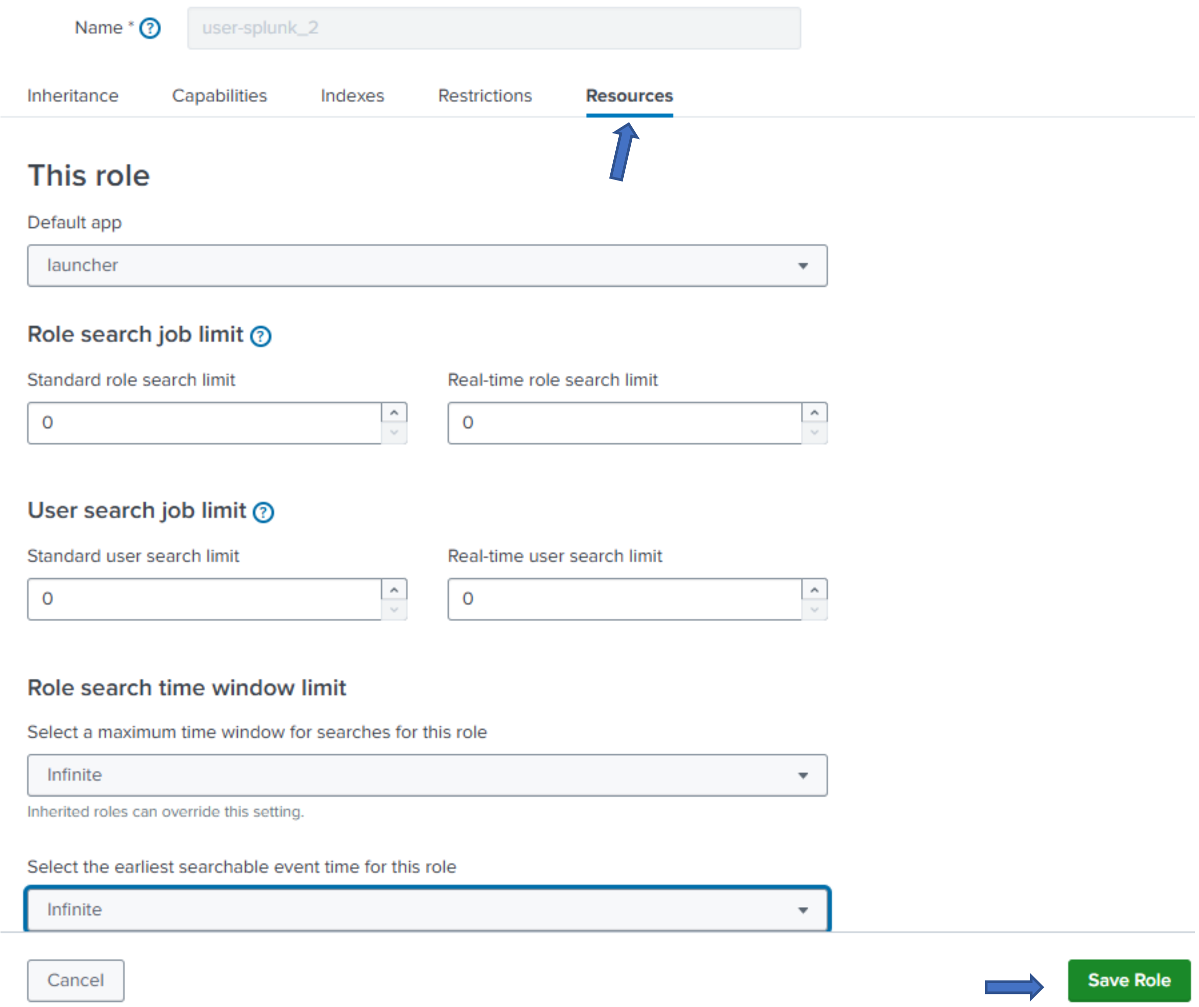
Instead of selecting individual indexes, you can create a wildcard index to dynamically capture all indexes that match the wildcard. After you add a wildcard Index, it appears in the Indexes table. Wildcard indexes apply to this role.

Enter a value that contains "*"

Indexes

Select both the "Included" and "Default" checkboxes for an index to make that index searchable by default for this role. You must save this role before you can see its inherited wildcards.

Index Name	Included	Default
* (All non-internal indexes)	☑	☑
_* (All internal indexes)	☑	☑
_audit	☑	☑
_configtracker	☑	☑
_dsappevent	☑	☑
_dsclient	☑	☑
_dsphonehome	☑	☑



Name *: user-splunk_2

This role

Default app: launcher

Role search job limit

Standard role search limit: 0

Real-time role search limit: 0

User search job limit

Standard user search limit: 0

Real-time user search limit: 0

Role search time window limit

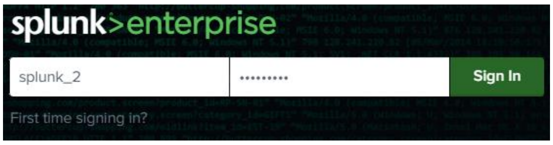
Select a maximum time window for searches for this role: Infinite

Inherited roles can override this setting.

Select the earliest searchable event time for this role: Infinite

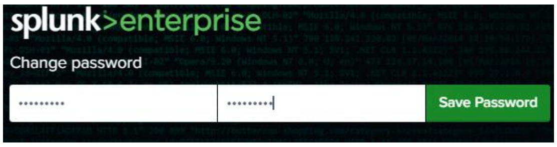
Step 6: Login with the Newly Created User and Set Password

1. **Log Out of Admin Account**
   - Click on your username in the top-right corner.
   - Select **"Logout"** from the dropdown.
2. **Login as the New User**
   - Open the login page again (e.g., `http://localhost:8000`).
   - Enter the **username** and **password** you just created.
     - Example:
       - **Username:** `splunk_2`
       - **Password:** `Splunk@123`
3. **Force Password Change (If Required)**
   - If the admin marked the "force change password on first login" option while creating the user, Splunk will ask the user to:
     - Enter the **old password**
     - Enter and confirm a **new password**
   - Submit to save.
4. **Access Dashboard**
   - After login, the user is redirected to their **Splunk Web dashboard**.
   - They now have access only as per the **assigned role permissions** (e.g., search, create dashboard, view indexes, etc.).



splunk_2

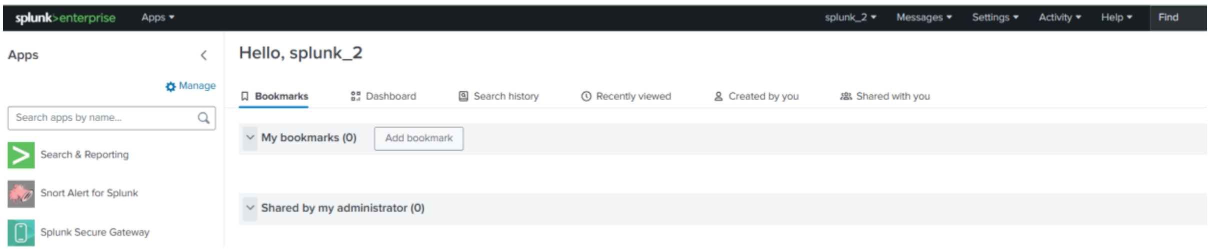
•••••••••



Change password

•••••••••

•••••••••



Hello, splunk_2