About configuring role-based user access

If you're running Splunk Enterprise, you can create users with passwords and assign them to roles. Roles determine the access and permissions of any user assigned to that role.

For more information about users, see About user authentication.

Predefined roles:

- **admin**: this role is intended for administrators who will manage all or most of the users, objects, and configuration and comes predefined with the most assigned capabilities.
- **power**: this role can edit all shared objects (saved searches, etc) and alerts, tag events, and other similar tasks.
- **user**: this role can create and edit its own saved searches, run searches, edit its own preferences, create and edit event types, and other similar tasks.
- **can_delete**: This role allows the user to delete by keyword. This capability is necessary when using the delete search operator.
- **sc_admin** (Cloud only): This role allows users to create users and roles but does not grant any other admin capabilities.

You can also create custom roles and assign your users to those roles. When you create a custom role, you determine the following:

- **Allowed searches**: you can define the searches that a user assigned to the role is allowed to perform.
- **Role inheritance**: you can have your role inherit certain properties of one or more existing roles. Role inheritance is discussed later in this topic.
- **Assign capabilities**: you can specify the allowed actions (change their password, change forwarder settings, etc) of the user assigned to the role. See About defining roles with capabilities for more information.
- **Set allowed and default indexes**: you can limit access to specific indexes and set the index that is searched by default.

To create roles in Splunk Web, see Add and edit roles with Splunk Web. To create roles by editing authorize.conf, see Add and edit roles with authorize.conf.
Inheritance

As a rule, members of multiple roles inherit properties from the role with the broadest permissions.

How users inherit search filter restrictions

You can create roles that inherit the characteristics of other roles. Users assigned to multiple roles inherit properties from the assigned roles.

In the case of search filters, if a user is assigned to roles with different search filters, the filters are all combined and thus the restrictions of each role are applied.

For example, by default, the Power and User roles do not have search filters defined to restrict searches. If a user has a combination of these roles and another role with filters defined (for example, `srchFilter=x`), the user will inherit the restrictions of that role, despite the association with roles that have no filter.

How users inherit allowed indexes

In the case of allowed indexes, the user is given the highest level of access granted to any role to which they are assigned.

For example, if a user is assigned to the role "simple user" which limits access to one particular index, and also to a role "advanced user" which has more capabilities and allows access to all indexes, the user will have access to all indexes. If you wanted to grant the capabilities of the "advanced user" but continue to limit their index access to the single index defined for the "simple user", you should create a new role specifically for that user.

How users inherit capabilities

In the case of capabilities, the user is given the highest level of abilities granted to any role to which they are assigned.

For example, if a user is assigned to the role "admin" which has the most capabilities, and also to a role "advanced user" which a different set of capabilities, the user will have the capabilities of both roles.