About configuring role-based user access

In the context of the Splunk platform, roles let users perform actions. You can use roles to control access to platform resources, like indexes, dashboards, and apps. When you configure role-based user access, you determine what **permissions** and **capabilities** that users have through the roles that they hold. As users do not receive permissions and capabilities directly, roles connect users to how they interact with the Splunk platform.

You can assign roles to users to control the scope of the tasks that they can perform, the data they can search, and the amount of resources they can access on the platform. Users can hold multiple roles, and each role gives the user specific access to resources or platform actions, as the role defines them. Roles do not take away access, so if you do not want a user to perform a certain function, then that user must not hold the role that lets them perform that function.

For more information about users, see About user authentication.

Predefined Splunk platform roles

The Splunk platform comes with the following predefined roles:

Role	Platform types	Access provided
admin	all	This role is for administrators who manage all or most of the users, objects, and configurations. and comes with the most **capabilities**
power	all	This role lets users edit all shared objects (saved searches, etc) and alerts, tag events, and perform other similar tasks.
user	all	This role lets users create, edit, and run their own searches, save those searches, edit their own preferences, create and edit event types, and perform other similar tasks.
can_delete	all	This role lets users delete by keyword. This capability is necessary when using the `delete` search operator.
splunk_system_upgrader	Splunk Enterprise	This role lets users perform automated rolling upgrades of search head clusters (SHCs) and indexer clusters (IDXCs) to a higher version of Splunk Enterprise.
sc_admin	Splunk Cloud Platform	This role lets users create other users and roles, but does not grant any other administrative capabilities.
tokens_auth	Splunk Cloud Platform	This role lets users activate authentication on the Splunk platform instance using tokens. It does not grant any other administrative capabilities.

Set permission granularity with custom roles

You can create custom roles and assign those roles to your users. Custom roles let you make granular adjustments to user access, including the following:

- **Role inheritance**: You can have a role inherit certain properties from one or more existing roles. For more information, see "Role inheritance" in this topic.
- **Capabilities**: You can specify which actions that a user that holds the role can perform, for example, change their password, change forwarder settings, and so on. See About defining roles with capabilities for more information.
- **Allowed and default indexes**: You can limit access to specific indexes and set which indexes the Splunk platform searches by default.
- **Search restrictions**: In addition to specifying the indexes that users that hold the role can search, you can also specify a search filter that limits the search results that these users can see. For additional information, see "Search restrictions" in this topic.

- **Resource access**: You can control how many standard and real-time searches that all users that hold the role can run at one time, as well as individual limits for each user. You can restrict searches to a certain time window, and control how much disk space is available for search jobs that a user with this role creates.

You can create and manage any roles, including the predefined ones, by using Splunk Web. On Splunk Enterprise instances, you can also manage roles by making edits to configuration files.

- To use Splunk Web for role management, see Add and edit roles with Splunk Web.
- To manage roles with the `authorize.conf` configuration file on Splunk Enterprise only, see Add and edit roles with authorize.conf. It's not possible to make edits to configurations in Splunk Cloud Platform outside of Splunk Web.

Use roles to limit search results

In addition to controlling the indexes that a role holder can search, you can further limit what results that searches of those indexes return. The search filter combines with the base search that the user runs to determine the final data set that the user sees.

By default, the Splunk platform selects only those results that match the filter, which means there are fewer results than if there was no filter. If it better suits your needs, you can configure specific roles to have search filters that omit results, meaning that users with those roles can see only the events that do not match those filters.

Search filters are limited to certain specific fields and operators. You can create a search filter manually by typing it in, or you can use the search filter generator to create it automatically, based on the number of indexes you select and the indexed fields and values that those indexes contain. With the search filter generator, you can create complex search filters without a need to worry about syntax. You can preview what a search with this filter applied will look like when you run it, so that you can be confident your users get the search results you expect when they use it.

See Create and manage roles with Splunk Web for information on how to set search filters and use the search filter generator.

Roles do not take access away

Roles always give access to something, which means that they never take access away. Users that hold multiple roles inherit the permissions and capabilities of the role that has the broadest permissions. Roles that have more permissions supersede roles that have fewer. If you want to limit access to resources, create and assign roles that establish those limits, and do not let those roles inherit from roles that do not establish those limits. Do not assign a role to a user whom you do not want to access the capabilities that come with the role.

How role inheritance works

Roles can inherit capabilities and indexes from other roles. When you inherit one role from another, you give the new role access to all capabilities and permissions that the existing role has. If you inherit from multiple roles, the new role receives the capabilities from all of the existing roles.

How users inherit search filter restrictions

If a user holds roles that contain different search filters, the Splunk platform combines the filters and applies the restrictions of each search filter.

For example, the "power" and "user" roles do not define any search filters to restrict searches by default. If a user holds both these roles, and you assign another role to them that does have a defined filter, then they inherit the search

restrictions that come with the third role, even though the "power" and "user" roles do not have a search filter.

How users inherit allowed indexes

Users that hold multiple roles receive the most permissive access that each role that they hold can provide.

For example, say you have a custom role called "simple_user" which limits access to a single index, and another custom role called "advanced_user", which has more capabilities and permits access to all indexes. If you assign both roles to the same user, that user receives access to all indexes through the "advanced user" role, even though the "simple user" role limits access to a single index. As roles do not take away access, if you want to grant the capabilities of the "advanced_user" role while limiting index access to one index with the "simple_user" role, the best practice is to create a custom role that combines the capability and index access that you want the user to have.

How users inherit capabilities

Users that hold multiple roles receive the most permissive amount of capabilities that each role that they hold can provide.

For example, if you assign a user the "admin" and "advanced_user" roles, the user receives the capabilities that come with both roles, even though the "advanced_user" role might have fewer capabilities than the "admin" role.