Create and manage roles with Splunk Web

You can assign roles to users that determine the level of access that those users have to the Splunk platform and the tasks that they can perform. The platform comes with a set of default roles, and you can also create your own custom roles that you can tailor to the needs of your organization.

Roles can contain one or more capabilities that provide access to specific parts of the Splunk platform. A user that has a role assigned to them receives all of the capabilities that are associated with the role. Roles can inherit capabilities from other roles.

Manage role inheritance, searched indexes, restrictions, and available search resources

When you add and edit roles, you can modify the following role properties:

- You can manage role inheritance. See "Specify role inheritance" in this topic.
- You can manage the indexes that a role has available to it as well as which indexes the Splunk platform searches by default. See "Specify searchable indexes for a role" in this topic.
- You can apply a search filter to further limit search results. You can either specify the filter manually or use the search filter generator - a wizard that lets you build and populate the filter by using indexed fields and values found in those indexes. See "Specify search restrictions for a role" in this topic.
- You can control resource usage on the platform in several ways. See "Specify default app and search limits for a role" in this topic:
    - You can limit disk space usage for search artifacts.
    - You can limit the number of searches that the role as a whole can run, and the number of searches that users who hold the role can run individually
    - You can specify the earliest time that a search can return results, which means you can limit results by the age of the data
    - You can limit searches to return results in a specific time window.

While you can have any role inherit from any other role, custom roles that inherit from the `admin` or `power users` roles do not automatically inherit administrator-level access to the instance.

- For more information about roles and how capabilities and permissions are inherited, see About configuring role-based user access.
- For information about granting management access to custom roles, see Add access controls to custom roles.
- For more information about role inheritance, see Role inheritance in the About configuring role-based user access topic.
- For more information about how capabilities work, as well as the full list of capabilities, see About defining roles with capabilities.

Add or edit a role

Create or edit roles for your Splunk platform instance on the Roles page in Settings.

1. Click **Settings > Roles**.
2. Click **New Role** to create a new role, or click an existing role to edit it.
3. Enter a name for your role.

   Role names must use lowercase characters only. They cannot contain spaces, colons, or forward slashes. You cannot edit the names of existing roles.
4. Make adjustments to role settings by editing configurations in any of the tabs in this dialog box.

5. After you have made the configuration changes that you want, click **Save** to save the role.

> The only required element of a role is its name. You do not have to complete any of the following tabs to save a role.

Specify role inheritance

Use the **1. Inheritance** tab to add or change the inheritance of existing roles.

1. Click **1. Inheritance** to display the contents of the Inheritance tab.
2. (Optional) In the **Role Name** text box, type in characters to display roles whose names contain those characters.
3. (Optional) Click the **All** column header to select from a menu of display options for roles: "Show selected", "Show unselected", or "Show all".
4. (Optional) Click the checkbox next to an existing role from which you want this role to inherit. You can click multiple checkboxes, or select all existing roles by clicking the checkbox in the column header.

Specify role capabilities

Use the **2. Capabilities** tab to add or change the capabilities that this role holds.

1. Click **2. Capabilities** to display the contents of the Capabilities tab.
2. (Optional) In the **Capability Name** field, type in a string to display capability names that contain the string.
3. (Optional) Click the **All** column header to select from a menu of display options for capabilities: "Show native", "Show inherited", "Show selected", "Show unselected", or "Show all".
4. Click the checkbox next to the capabilities that you want to assign to this role.
5. Click **Save**.

> Capabilities that have been inherited from other roles appear as grayed out and selected. You cannot deselect capabilities that come with inherited roles.

Specify searchable indexes for a role

Use the **3. Indexes** tab to choose the indexes that the role can search, and which ones it should search by default.

You can specify both event and metric indexes. You can also specify wildcards that match more than one index. If a user with the role runs a metrics search without a specified index, the search includes results from the default metrics indexes that you assign to the role. You must select at least one index with data here if you want to be able to use the **SPL** Search Filter generator in the **4. Restrictions** tab.

Wildcards let you specify all indexes that match the text you enter. For example, if you specify a wildcard of "`index_us*`," it captures all existing indexes that begin with `index_us`. Wildcards that you create appear in the Indexes table in alphabetical order, as selected and default indexes.

You can create multiple wildcards, but they only apply to the current role. You cannot transfer wildcards to other roles; instead you must explicitly create the same wildcard by editing the roles and adding the wildcards there. To delete a wildcard from a role, confirm that the wildcard is neither a selected nor a default index, and save the role.

1. Click **3. Indexes** to display the contents of the Indexes tab.
2. (Optional) In the **Wildcards** section, enter a string that contains the `*` character and specifies the group of indexes you want to search, then click **Create**.

> You can repeat this action to add more wildcards. If a wildcard already exists, Splunk Web advises you.

3. (Optional) In the **Index Name** field, type in a string to display index names that begin with that string.
4. (Optional) Click the **All** column header to select from a menu of display options for indexes: "Show native", "Show inherited", "Show selected", "Show unselected", or "Show all".
5. Click the **Included** checkbox for an index to include search results from that index for this role.
6. Click the **Default** checkbox for an index to include search results from that index when a user that holds this role does not specify an index in their search.

   Indexes from inherited roles appear as grayed out and selected. You cannot deselect indexes that come with inherited roles.

Specify search restrictions for a role

Use the **4. Restrictions** tab to limit the scope of search results that return when users with the role run searches. The search filter combines with the base search that users with the role run, based on several factors. The search job returns only the results that arise from the combined search.

For more information on valid syntax to use with the search filter, see "SPL search filter syntax" later in this topic.

1. Click **4. Restrictions** to display the contents of the Restrictions tab.
2. In the **SPL Search filter** field, type in a valid SPL string that combines with any base search that a user with this role runs.
3. (Optional) Use the **Search filter SPL generator** to create a search filter.
    1. In the **Indexed fields and values time range** drop down list, choose a time range to search for indexed fields and their associated values.

       For these controls to work, you must have selected at least one index with data in the Indexes tab. Changing the default time of 60 seconds can increase the amount of time it takes to populate the Indexed Fields and Values text boxes, but might be necessary to retrieve a comprehensive list of indexed fields.

    2. In the "Indexed fields" text box, do one of the following:
        1. Click on the text box to display a drop-down list box that contains the most common indexed fields that were found, based on the indexes you have selected in the **3. Indexes** tab and the time that you specified in the "Indexed fields and values time range" setting. The `|walklex` search command populates this field.
        2. Enter the name of an indexed field.

       If you select an indexed field that is already present in the SPL search filter, Splunk Web displays a message about possible SPL collisions. Review the filter to confirm that there are no unintended conflicts.

    3. In the "Values" text box, do one of the following:
        1. Click on the text box to display a drop-down list box that shows the top 250 indexed field values that were found, in lexical order, based on the fields you selected in the "Indexed fields" text box.
        2. Enter a custom field value directly. You can also use wildcards.
    4. Use the **Concatenation option** drop-down list box to determine how the SPL generator adds SPL text that it generates to any existing text in the SPL search filter.
        1. Choose "AND" to add the generated SPL prepended with the `AND` keyword
        2. Choose "OR" to add the generated SPL prepended with the `OR` keyword.
        3. Choose "NOT" to add the generated SPL prepended with the `NOT` keyword.

If the search filter does not have any text in it, the "Concatenation option" drop-down list box is disabled.

5. Review the SPL that the SPL generator proposes adding to the SPL search filter.
6. If you are satisfied with the SPL that has been generated, click **Add to SPL search filter**. The SPL generator updates the SPL search filter text box with the generated text. If there is already text in the filter text box, the SPL generator appends the generated text. Depending on the concatenation option you chose, the SPL generator adds the text after the "AND", "OR", or "NOT" keyword.
7. (Optional) If you do not like the SPL that you generated with the SPL generator, you can remove the text that you added by clicking **Reset**.
8. (Optional) If you want to see how the search filter can affect search results before you apply it, click **Preview search filter results.** This action opens a new Search page that shows the results of a search with the current search filter.

The search preview results are an example of what a user with this role might see. Several factors can alter the actual results from what the preview shows.The preview makes the assumption that the user holds only this role. While it includes results from inherited indexes, it does not include any search filters that might exist in inherited roles.If you have configured the Splunk platform instance so that search filters for a role eliminate, rather than select results, actual results might be the opposite of what you see in the preview. The srchFilterSelecting setting in authorize.conf controls whether search filters select or eliminate results, and is true by default. A false value tells search filters to eliminate results.

Specify default app and search-related limits for a role

In the **5. Resources** tab, you can control the default app that a user with this role sees when they log into the Splunk platform. You can also control various search job characteristics and limits, including but not limited to the earliest time that a search can return results.

1. (Optional) In the **Default app** dropdown, select the default Splunk app that appears when a user that holds this role logs in.
2. (Optional) In the **Role search job limit** section, enter the maximum number of standard searches that this role can run at a time in the **Standard search job limit** text box.

   To remove search limits, you can enter 0 in this and other search limit text boxes.
3. (Optional) Enter the maximum number of real-time searches that a user with this role can run at a time in the **Real-time search job limit** text box.
4. (Optional) In the **User search job limit** section, enter the maximum number of standard searches that users can run at a time in the **Standard search job limit** text box.
5. (Optional) In the **Role search time window limit** section, select a standard search maximum time range for this role. Click the drop-down list box to choose a value:

Setting	Description	Can inherited roles override this setting?
Unset	Historical searches run by this role do not have a time range limit.	Yes
Infinite	Historical searches run by this role do not have a time range limit.	No
Custom time	Exposes a text box where you can define a maximum time range in seconds for historical searches run by this role.	Yes

The Splunk platform applies custom time range limits backwards from the latest time that you specify for a search.

If a user has multiple roles with custom time range limits, or has roles that inherit from roles with custom time

range limits, the Splunk platform applies the least restrictive search time range limits to the role. For example, if you have a user named Blue who has role A with a custom time of 30 seconds, role B with a custom time of 60 seconds, and role C with a custom time of 3600 seconds. Blue would get the maximum search time range of 3600 seconds, or 1 hour.

> This setting does not apply to real-time searches.

6. (Optional) Also in the **Role search time window limit** section, select the earliest time that the Splunk platform can return results for a search for this role.

   When you use this field, the platform returns only the events whose timestamp is between the number of seconds you specify here, and the current time.

   The available settings and options for the earliest-time search input field are identical to those that are in the search time range input field. See the previous step in this procedure.
7. (Optional) In the **Disk space limit** section, enter the amount of disk space that search jobs for this role can take up at a given time in the **Standard search limit** text box.

Save changes to role configurations

You must save changes to role configurations (including search time restrictions) and restart the Splunk platform before those changes can take effect. If you do not restart, the instance cannot enforce your configurations and restrictions.

- To save all of the changes you have made and close the dialog box, click **Save.**
- If you do not want to save the changes, click **Cancel**.

> If you click Cancel, you lose any unsaved changes that you have made since you opened the Roles dialog box.

For more information about restarting the Splunk platform, see Start and stop Splunk Enterprise in the *Admin Manual*.

SPL search filter syntax

The **SPL search filter** field in the **4. Restrictions** tab accepts any of the following search terms:

- `source::`
- `host::`
- `index::`
- `sourcetype::`
- `eventtype=` or `eventtype::`
- The keywords `AND`, `OR`, or `NOT`
- Search fields

You can enter SPL manually into the SPL search filter text box, or use the SPL generator to create SPL for the search filter based on fields and field values that you have indexed.

You can use wildcards. Use `OR` to allow multiple terms, or `AND` to make the filter more restrictive.

Caveats to using the SPL search filter

The search terms cannot include any of the following:

- Saved searches

- Time operators
- Regular expressions
- Any fields or modifiers that you can override from the Splunk Web search bar

Usage of search filter syntax

When you specify search term filters, use the `key::value` syntax, rather than `key=value`, where possible, to restrict search terms to indexed fields. If you specify the `key=value` syntax as part of a filter, the search filter dialog box warns you that usage of the `=` operator can result in poor search performance for users who hold the role. Also, it is not secure to use the operator because filters with the operator can be bypassed by user knowledge objects.

If you attempt to add an indexed field that already exists in the current search filter, the page warns you that the indexed field already exists to ensure that you have no unintended SPL conflicts in the search filter.

Define roles on the Splunk platform with capabilities

When you create a user on the Splunk platform, you assign one or more roles to the user as part of the user creation process. Each role contains a set of **capabilities**. These capabilities define what users who hold a certain role can do.

For example, if a user 'finn' holds the edit_tokens_settings role, this means that 'finn' can make changes to the Token Authentication scheme on the instance. If they hold the admin_all_objects capability, they can make changes to any object on the instance.

You can add, edit, or remove capabilities for new, existing, and default roles. Doing this changes the kind of access that the role provides. For example, you might give a role the capability to add inputs or edit saved searches.

Capabilities are always additive in nature. There is no way to take away an ability to do something by adding a capability. If you don't want users who hold a role to perform a certain function on your Splunk platform instance, then do not assign a capability that grants the ability to perform that function to that role.

Similarly, users who hold multiple roles receive all the benefits of any capabilities that are assigned to those roles. If you do not want a certain user to have access to all the capabilities that a role provides, do not assign that role to that user.

Add, edit, and remove capabilities from roles

- To add or change the capabilities of a role in Splunk Web, see Create and manage roles with Splunk Web.
- To create roles and assign capabilities by editing authorize.conf, see Add and edit roles with authorize.conf.
- To learn more about roles and how they work, see About configuring role-based user access.

Table of Splunk platform capabilities

This list shows the capabilities that you can add to any role, and whether or not the capabilities are assigned by default to the user, power, or admin roles. The table lists capabilities from the Splunk platform only. Apps and add-ons might add capabilities that do not appear here.

Capabilities are subject to change. For the most up-to-date list of capabilities, see the authorize.conf specification file.

For the most up-to-date list of capabilities that are assigned to a role, see the "Imported Capabilities" text box in the "Create a role" page in Splunk Web on your instance.

Capability name	What it lets you do	User	Power	Admin
accelerate_datamodel	Enable or disable acceleration for data models. Set acceleration to true to enable automatic acceleration of this data model. Additional space is required depending on the number of events, fields, and distinct field values in the data. See the Knowledge Manager Manual for more information.			X
accelerate_search	Lets the user enable or disable acceleration for reports. The user must also have the schedule_search capability assigned. Works for searches that use transforming commands. See the Knowledge Manager Manual for more information.	X	X	X
admin_all_objects	Lets the user access and modify any object in the system regardless of any restrictions set in the objects. For example user objects, search jobs, reports, and knowledge objects. Lets the user bypass any ACL restrictions, much the way root access in a *nix environment does.			X
change_authentication				X

Capability name	What it lets you do	User	Power	Admin
	Lets the user change authentication settings and reload authentication. See the Securing Splunk Enterprise Manual for more about authentication.			
change_own_password	Lets the user change their own password.	X	X	X
delete_by_keyword	Lets the user use the "delete" operator. The "delete" command marks all of the events returned by the search as deleted. This masks the data from showing up in search results but does not actually delete the raw data on disk. See the Search Manual for more information.			
delete_messages	Lets a user delete system messages that appear in the UI navigation bar.	X	X	X
dispatch_rest_to_indexers	Lets a user dispatch the REST search command to indexers.			X
edit_bookmarks_mc	Lets a user add bookmark URLs within the Monitoring Console. The URLs redirect administrators to Monitoring Console instances in other Splunk deployments.			X
edit_deployment_client	Lets the user change deployment client settings. See the Managing Indexers and Clusters of Indexers Manual for more about the deployment client.			X
edit_deployment_server	Lets the user change deployment server settings. User can change or create remote inputs that are pushed to the forwarders and other deployment clients. See the Managing Indexers and Clusters of Indexers manual for more about the deployment server.			X
edit_dist_peer	Lets the user add and edit peers for distributed search. See the Managing Indexers and Clusters of Indexers Manual for more information.			X
edit_encryption_key_provider	Lets the user view and edit key provider properties when they use Server-Side Encryption (SSE) for a remote storage volume.			X
edit_forwarders	Lets the user change forwarder settings, including settings for SSL, backoff schemes, etc. Also used by TCP and Syslog output admin handlers.			X
edit_global_banner	Lets the user enable and customize the global banner feature in Splunk Web.			X
edit_health	Lets a user enable/disable health reporting, set health status alerts, and set indicator thresholds for a feature in the `splunkd` health status tree through the `server/health-config/` endpoint.			X
edit_httpauths	Lets the user edit and end user sessions through the httpauth-tokens endpoint.			X
edit_indexer_cluster	Lets the user edit indexer clusters. See the Managing Indexers and Clusters of Indexers Manual for more about indexers.			X
edit_indexerdiscovery	Lets the user edit settings for indexer discovery, including settings for `master_uri`, `pass4SymmKey`, and so on. Used by Indexer Discovery admin handlers.			X
edit_input_defaults	Lets the user use the server settings endpoint to change default hostnames for input data.			X
edit_local_apps	Lets the user edit actions for application management. Applies only when you set the `enable_install_apps` setting to "true" in `authorize.conf`.			X
edit_metric_schema	Lets the user set up log-to-metrics transformations, which can convert single log events into multiple metric data points.			X
edit_metrics_rollup				X

Capability name	What it lets you do	User	Power	Admin
	Lets the user create and edit metrics rollup policies, which set rules for the aggregation and summarization of metrics on a specific metric index.			
edit_monitor	Lets the user add inputs and edit settings for monitoring files. Also used by the standard inputs endpoint and the one-shot input endpoint.			X
edit_roles	Lets the user edit roles and change user/role mappings. Used by both the user and role endpoint.			X
edit_roles_grantable	Lets the user edit roles and change user/role mappings for a limited set of roles. Can assign any role to other users. To limit this ability, configure `grantableRoles` in authorize.conf. For example: `grantableRoles = role1;role2;role3`			X
edit_scripted	Lets the user create and edit scripted inputs.			X
edit_search_concurrency_all	Lets a user edit settings related to maximum concurrency of searches.			X
edit_search_concurrency_scheduled	Lets a user edit settings related to concurrency of scheduled searches.			
edit_search_head_clustering	Lets the user edit search head clustering settings.			X
edit_search_schedule_priority	Lets the user assign a search a higher-than-normal schedule priority. For information about the search scheduler, see the Knowledge Manager Manual.			X
edit_search_schedule_window	Lets the user assign schedule windows to scheduled reports. Requires the schedule_search capability. For more about the search scheduler, see the Knowledge Manager Manual.	X	X	X
edit_search_scheduler	Lets the user enable and disable the search scheduler. See the Knowledge Manager Manual.			X
edit_search_server	Lets the user edit general distributed search settings like timeouts, heartbeats, and filter lists.			X
edit_server	Lets the user edit general server settings like server name, log levels, etc.			X
edit_server_crl	Lets the user edit general server settings like server name, log levels, etc. Inherits the ability to read general server and introspection settings.			X
edit_sourcetypes	Lets the user edit sourcetypes. See the Knowledge Manager manual for more information about sourcetypes.		X	X
edit_splunktcp	Lets the user change settings for receiving TCP inputs from another Splunk instance.			X
edit_splunktcp_ssl	Lets the user view or edit any SSL-specific settings for Splunk TCP input.			X
edit_splunktcp_token	Lets the user edit the Splunktcp token.			X
edit_tcp	Lets the user change settings for receiving general TCP inputs.			X
edit_telemetry_settings	Opt in or out of product instrumentation. See Share data in Splunk Enterprise in the *Admin Manual*.			X
edit_token_http	Lets the user create, edit, display, and remove settings for HTTP token input. Also enables the HTTP Event Collector feature.			X
edit_tokens_all	Lets the user issue tokens to all users.			X
edit_tokens_own	Lets the user issue tokens to themself.			X
edit_tokens_settings	Lets the user manage token settings.			X
edit_udp	Lets the user change settings for UDP inputs.			X

Capability name	What it lets you do	User	Power	Admin
edit_user	Lets the user create, edit, or remove users. A role with the edit_user capability can assign any role to other users. To limit this ability, configure `grantableRoles` in authorize.conf. For example: `grantableRoles = role1;role2;role3`. Also lets a user manage certificates for distributed search.			X
edit_view_html	Lets the user create, edit, or modify HTML-based views.			X
edit_web_settings	Lets the user change settings for web.conf through the system settings endpoint.			X
edit_workload_pools	Lets the user create and edit workload pools through the workloads/pools endpoint.			X
edit_workload_rules	Lets the user create and edit workload rules through the `workloads/rules` endpoint.			X
embed_report	Lets the user embed reports and disable embedding for embedded reports.		X	X
export_results_is_visible	Lets the user display or hide the **Export Results** button in Splunk Web. The default value is to display the button.	X	X	X
fsh_manage	Lets the user view, create, and edit federated provider and federated index definitions through Splunk Web. Federated providers and federated indexes are required for federated search.			X
fsh_search	Lets the user run federated searches.			X
get_diag	Lets the user get a remote diag from a Splunk instance using the /streams/diag endpoint.			X
get_metadata	Lets the user use the "metadata" search processor.	X	X	X
get_typeahead	Lets the user use typeahead in the endpoint and the typeahead search field.	X	X	X
indexes_edit	Lets the user change any index settings such as file size and memory limits.			X
input_file	Lets the user add a file as an input through inputcsv (except for dispatch=t mode) and inputlookup.	X	X	X
install_apps	Lets the user install, uninstall, create, and make updates to apps. Applies only when you configure the `enable_install_apps` setting to "true" in `authorize.conf`.			X
license_edit	Lets the user edit the license.			X
license_read	Lets the user access license attributes and related information.			
license_tab	Lets the user access and change the license. This attribute is deprecated.			X
license_view_warnings	Lets the user see a warning message when they are exceeding data limits or reaching the expiration date of their license. These warnings appear on the system banner.			X
list_accelerate_search	Lets the user view accelerated reports. User cannot accelerate reports.			X
list_deployment_client	Lets the user view deployment client settings.			X
list_deployment_server	View deployment server settings.			X
list_dist_peer	Lets a user list/read peers for distributed search.			X
list_forwarders				X

Capability name	What it lets you do	User	Power	Admin
	Lets a user list and view settings for data forwarding. Can be used by TCP and Syslog output admin handlers.			
list_health	Lets a user monitor the health of Splunk Enterprise features (such as inputs, outputs, clustering, and so on) through REST endpoints.			X
list_httpauths	Lets the user view user sessions through the httpauth-tokens endpoint.			X
list_indexer_cluster	Lets the user view the list of indexer clusters as well as indexer cluster objects such as buckets, peers, etc.			X
list_indexerdiscovery	Lets the user view settings for indexer discovery. Also used by indexer discovery handlers.			X
list_inputs	Lets the user view lists of various inputs, including input from files, TCP, UDP, scripts, etc.	X	X	X
list_introspection	Lets the user read introspection settings and statistics for indexers, search, processors, queues, etc.			X
list_metrics_catalog	Lets the user query for lists of metrics catalog information such as metric names, dimensions, and dimension values.	X	X	X
list_search_head_clustering	Lets the user list and view search head clustering objects like artifacts, delegated jobs, members, captain, etc.			X
list_search_scheduler	Lets the user view lists of search scheduler jobs.			X
list_settings	Lets the user list and view server and introspection settings such as the server name, log levels, etc.			X
list_storage_passwords	Lets the user list and view the `/storage/passwords` endpoint, lets the user perform GETs. The admin_all_objects capability must be added to the role for the user to perform POSTs to the `/storage/passwords` endpoint.			X
list_tokens_all	Lets the user view all tokens.			X
list_tokens_own	Lets the user view their own tokens.	X	X	X
list_workload_pools	Lets a user list and view workload pool and workload status information from the `workloads/rules` endpoint.			X
list_workload_rules	Lets a user list and view workload rule information from the `workloads/rules` endpoint.			X
metric_alerts	Lets a user create, update, enable, disable, and delete a streaming metric alert.		X	X
never_expire	Lets a user account never expire.			X
never_lockout	Lets a user account never lock the user out.			X
output_file	Lets the user create file outputs, including outputcsv (except for dispatch=t mode) and outputlookup.	X	X	X
pattern_detect	Lets the user see and use the Patterns tab in the Search view.	X	X	X
request_remote_tok	Lets the user obtain a remote authentication token, which lets the user perform some distributed peer management and bundle replication and distribute searches to old 4.0.x Splunk instances.	X	X	X
rest_apps_management	Lets the user edit settings for entries and categories in the python remote apps handler. See restmap.conf for more information.			X
rest_apps_view		X	X	X

Capability name	What it lets you do	User	Power	Admin
	Lets the user list and view various properties in the Python remote apps handler. See `restmap.conf` for more information.			
rest_properties_get	Lets the user get information from the `services/properties` endpoint.	X	X	X
rest_properties_set	Lets the user edit the `services/properties` endpoint.	X	X	X
restart_splunkd	Lets the user restart Splunk Enterprise through the server control handler.			X
rtsearch	Lets the user run real-time searches.		X	X
run_collect	Lets the user run the `collect` command.	X	X	X
run_mcollect	Lets the user run the `mcollect` and `meventcollect` commands.	X	X	X
run_msearch	Lets the user run the `msearch` command.			X
run_multi_phased_searches	Lets the user run searches with the `redistribute` command, which invokes parallel reduce search processing in distributed search environments. This capability is not assigned to any role by default.			
run_walklex	Lets the user run searches that include the `walklex` command, even if they have a role that has search filters applied to it. By its nature, the `walklex` command bypasses role-based search filters. Avoid giving this capability to roles that must have their search functionality restricted. This capability is not assigned to any role by default.			
schedule_rtsearch	Lets the user schedule real-time saved searches. The schedule_search capability must also be assigned to the role.	X	X	X
schedule_search	Lets the user schedule saved searches, create and update alerts, review triggered alert information, and use the `sendemail` command.		X	X
search	Lets the user run a search. See the Search Manual for more information.	X	X	X
search_process_config_refresh	Lets the user use the "refresh search-process-config" CLI command to manually flush idle search processes.		X	X
select_workload_pools	Lets a user assign a scheduled search or ad-hoc search to a workload pool.			X
srchFilter	Lets the user manage search filters. See the Search Manual for more information.			X
srchIndexesAllowed	Lets the user run search indexes. See the Search Manual for more information.			X
srchIndexesDefault	Lets the user set default search indexes.			X
srchJobsQuota	Lets the user set search job quotas.			X
srchMaxTime	Lets the user set the maximum time for a search.			X
upload_lookup_files	Lets the user upload files that can be used in conjunction with lookup definitions. Only affects lookup types that involve the upload of a file, such as CSV and geospatial lookups.	X	X	X
use_file_operator	Lets the user use the "file" search operator. The "file" search operator is deprecated.			X
web_debug	Lets the user debug Web files.			X

Windows-specific capabilities

If you are running Splunk Enterprise on Windows, additional capabilities are provided to facilitate monitoring.

Capability name	What it lets you do
edit_modinput_admon	Edit modular inputs in admon.conf.
edit_modinput_perfmon	Edit modular inputs in perfmon.conf.
edit_modinput_winhostmon	Add and edit inputs for monitoring Windows host data
edit_modinput_winnetmon	Add and edit inputs for monitoring Windows network data.
edit_modinput_winprintmon	Required to add and edit inputs for monitoring Windows printer data.
edit_win_admon	(Deprecated)
edit_win_eventlogs	Edit windows eventlogs.
edit_win_perfmon	(Deprecated)
edit_win_regmon	(Deprecated)
edit_win_wmiconf	Edit wmi.conf.
list_pdfserver	View PDF server files
list_win_localavailablelogs	List all local Windows event logs.
srchTimeWin	Set search time limits.
write_pdfserver	Write to PDF server files.

Create and manage users with Splunk Web

You can manage who has user access to your Splunk platform instance with the Users window. You can create, delete, and manage various aspects about users, including their name, email address, password, default time zone, and role assignments.

You access the Users control panel from anywhere in Splunk Web by selecting **Settings** > **Users** in the system bar.

The "Users" control panel

The "Users" control panel is where you perform all aspects of user management. It displays a list of all users that are on the Splunk platform instance. By default, the page lists the users ascending by name. The page displays the following information in columns, from left to right:

- **Name**: The user name. You can click on the name to edit that user.
- **Actions**: This column is a drop-down menu of actions that you can perform on the user. See "Perform actions on users" in this topic.
- **Authentication system**: The authentication scheme that the user uses to log into the Splunk platform instance.
- **Full name**: The full name of the user, as entered in the "Full Name" field on the individual user page.
- **Email address**: The email address of the user, as entered in the "Email Address" field on the individual user page.
- **Time zone**: The time zone that has been specified for the user. If the user uses the default system time zone, nothing appears here.
- **Default app**: The default Splunk application context that a user is in when they log in.
- **Default app inherited from**: The entity from which the user inherits the application context.
- **Roles**: The roles of which the user is a member.
- **Last login**: The last time the user successfully logged onto the instance. If nothing appears here, the user has never logged in.
- **Status**: The current status of the user, as provided by the authentication scheme.

Sort the user list

You can click any of the column headers to sort the user list by that column header, with the exception of "Actions". Clicking a column header multiple times toggles whether the user list sorts in ascending or descending order.

Perform actions on users

You can perform several different actions on an existing user, including but not limited to making edits, cloning, viewing a list of capabilities that a user has, viewing the index inheritances that a user has, and performing a search in a user context. These actions are available under the **Actions** column for each user, and you can access them by clicking the **Edit** link in that column.

- To edit a user, click **Edit.** The "Edit User" page appears. See "Edit a user" later in this topic for continued instructions.
- To clone a user, click **Clone.** This action takes you through the "Create user" process to create an identical user.
- To view all of the capabilities that a user has, click **View Capabilities.** This loads the "View Capabilities" page which lists all of the capabilities that the user has, based on the roles that the user holds.
- To view the indexes that a user has access to through role inheritance, click **View Indexes.** This loads the "View Index Inheritance" page which shows what indexes.a user has access to based on the roles that they hold. See "View Index Inheritance for a user" later in this topic..

- To run a search as a specific user, based on the indexes and search filters in the roles that they hold, click **Search As**. This loads a Search page where you can run a search within the framework of the indexes and search filters that are available to that user. The search runs with the capabilities of the admin user.
- To delete a user, click **Delete**. The instance confirms whether or not you want to delete the user.

Create a user

1. From the system bar, click **Settings** > **Users**.
2. Click **New User**.
3. In the **Name** field, provide a user name. This is the what the user provides at the login page.
4. In the **Full Name** field, provide the full name of your user.
5. In the **Email Address** field, provide the user email address.
6. In the **Set password** field, create a password.
7. Confirm the new password in the **Confirm Password** field.
8. Confirm that the password you created meets the password requirements as displayed below the "Confirm password" field.
9. Select the user's time zone in the **Time Zone** field.
10. In the **Default App** field, select the app that the user will land in by default when they log into the Splunk platform instance. The default is "Home". "Search" is a common default app as well.
11. In **Assign to Roles**, you can select any roles that you want for your user to hold.
12. Click **Create a role for user** if you want to user's new assignments to be created as a role assigned specifically to this user.
13. Check **Require password change on first login** to force your user to change their password when they first log into the Splunk platform instance.
14. Click **Save**. The Splunk platform creates the user and returns you to the "Users" page.

Edit a user

1. From the system bar, click **Settings** > **Users**.
2. Either click the user name link in the **Name** column, or click the **Edit** link in the **Actions** column for the user you want to edit.
3. In the **Name** field, provide a user name. This is what the user provides at the login page.
4. In the **Full Name** field, provide the full name of your user.
5. In the **Email Address** field, provide the user email address.
6. In the **Set password** field, create a password.
7. Confirm the new password in the **Confirm Password** field.
8. Confirm that the password you created meets the password requirements as displayed below the "Confirm password" field.
9. Select the user's time zone in the **Time Zone** field.
10. In the **Default App** field, select the app that the user will land in by default. The default is "Home". "Search" is a common default app as well.
11. In **Assign to Roles**, you can select any roles that you want for your user to hold.
12. Click **Create a role for user** if you want to user's new assignments to be created as a role assigned specifically to this user.
13. Check **Require password change on next login** to force your user to immediately change their password.
14. Click **Save**. The Splunk platform creates the user and returns you to the "Users" page.

Run a search as a user

When you run a search as a user, you see results based on the roles that the user holds and the indexes that the user has access to. Additionally, the search includes any search filters that you have configured for the roles that the user

holds.

1. From the system bar, click **Settings** > **Users**.
2. Click the **Edit** link in the **Actions** column for the user under which you want to run a search.
3. Click **Search as...** A **New Search** window opens.
4. In the Search bar, type in a valid Splunk search. The Splunk platform returns results based on the context of the user and the roles that the user holds, as well as any search filters that have been configured for those roles.

View index inheritances for a user

You can see how a user gets access to an index based on the roles that the user holds. The indexes that a user has access to determines the results that searches return.

You can only view inheritances of indexes on this page. To change which indexes a role has access to, visit the Roles page and either add or edit a role. See Create and manage roles with Splunk Web.

1. From the system bar, click **Settings** > **Users**.
2. Click the **Edit** link in the **Actions** column for the user under which you want to view index inheritance information.
3. Click **View Indexes...** The **View Index Inheritance** page opens.
4. In the **Index** field, either type in the name of an index, or click the field to show a list of indexes.
5. Select the index whose inheritance you want to view by clicking it in the drop-down list box. The table on the page updates based on the inheritances for the index you specified, as follows:
    - The "Roles" column displays the roles that have access to the index you selected.
    - If the user you chose holds the role, Splunk Web displays a star next to it.
    - If the role has the index directly, or natively, assigned to it, a triangle appears in the **Included** column for that role.
    - If the index has directly been made the default index for the role, a triangle appears in the **Default** column for that role.
    - If the role inherits the index from another role, then a circle appears in the Included column for that role, and the inherited role appears in the **Inherits from** column for the role.
    - If the index is the default index for the role through an inheritance, a circle appears in the Default column for that role.

Splunk Web follows inheritances to their logical end. This means it always displays the roles that inherit from another role until it finds the roles which have the selected indexes defined natively. Given the following scenario:

- User Fred holds role Role1,
- Role Role1 inherits from role Role2
- Role Role2 has indexes Index1 and Index2 assigned to it

If you selected Index1, the View Inheritances page would display the following:

- The page lists both roles Role1 and Role2.
- Role role1 has a star by it because user Fred holds that role.
- Role role2 lists triangles under the Included and Default columns because role Role2 has those indexes assigned to it natively.
- Role role1 lists circles under the Included and Default columns because role Role1 inherits from role Role2

If a user does not hold at least one role that has been assigned to the index you select, nothing appears in the View Index Inheritance table.

Delete a user

Deleting a user permanently removes their account and its associated information from the instance, and cannot be undone. You cannot remove the admin user.

1. From the system bar, click **Settings** > **Users.**
2. Click the **Edit** link in the **Actions** column for the user you want to edit.
3. Click **Delete.**
4. In the confirmation dialog box, click **Delete.**