Define roles on the Splunk platform with capabilities

There are two versions of this topic: one for Splunk Cloud Platform and the other for Splunk Enterprise. This is the Splunk Enterprise version of the topic. To change to the Splunk Cloud Platform version, select Splunk Cloud Platform™ from the Product drop-down list box in this topic.

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	Lets the user 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

Capability name	What it lets you do	User	Power	Admin
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
apps_backup	Lets the user back up configurations to a backup archive through the apps/backup REST endpoint.			X
apps_restore	Lets the user restore configurations from a backup archive through the apps/restore REST endpoint.			X
capture_ingest_events	Lets a user access the live capture feature on the ingest actions UI and view events being ingested live.			X
change_authentication	Lets the user change authentication settings and reload authentication. See the Securing Splunk Enterprise Manual for more about authentication.			X
change_own_password	Lets the user change their own password.	X	X	X
customer_cases	Allows the user to use the RapidDiag GUI to upload diags in standalone or distributed environments directly to an existing Splunk Support Case.			
create_external_lookup	Lets a user create external lookup definitions.			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_authentication_extensions	Lets the user activate, deactivate, and edit SAML authentication extension settings.			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_cmd	Lets the user configure the 'unarchive_cmd' setting in the props.conf configuration file, which specifies the command to run to extract an archived data source.			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_external_lookup	Lets a user edit or remove external lookup definitions.			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_field_filter	Lets a user create, edit, or delete field filters by using Splunk Web or the Splunk platform REST API **authorization/fieldfilters** and **authorization/fieldfilters/{name}** endpoints to update field filters. See			X

Capability name	What it lets you do	User	Power	Admin
	Protect PII, PHI, and other sensitive data with field filters.			
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_health_subset	Lets a user disable or enable health reporting for a feature in the "health_subset" view of the health status tree. Actions are performed through the server/health-config/{feature_name} endpoint.			
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_ingest_rulesets	Lets a user create and edit ingest actions rulesets and destinations.			X
edit_input_defaults	Lets the user use the server settings endpoint to change default hostnames for input data.			X
edit_kvstore	Lets a user execute App Key Value Store administrative commands through the KV Store REST endpoints.			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 `limits.conf`.			X
edit_log_alert_event	Lets a user log an event when an alert condition is met. Also lets the user select the "Log an event" option for an alert action in Splunk Web.		X	X
edit_manager_xml	Lets a user create and edit XML views using the /data/ui/manager REST endpoint.			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	Lets the user create and edit metrics rollup policies, which set rules for the aggregation and summarization of metrics on a specific metric index.			X
edit_modinput_journald	Lets the user add and edit journald inputs. This input is not available on Splunk platform instances that run on Windows.			X
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_own_objects	Lets a user edit the knowledge objects or entities for configuration endpoints that they own.	X	X	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

Capability name	What it lets you do	User	Power	Admin
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_statsd_transforms	Lets a user define regular expressions to extract manipulated dimensions out of metric_name fields in statsd metric data using the services/data/transforms/statsdextractions endpoint. For example, dimensions can be mashed inside a metric_name field like "dimension1.metric_name1.dimension2" and you can use regular expressions to extract it.		X	X
edit_storage_passwords	Lets the user make HTTP POST and DELETE calls to the /**storage**/**passwords** endpoint, which stores or deletes secrets. Users must hold the 'list_storage_passwords' role to retrieve secrets.		X	X
edit_tcp	Lets the user change settings for receiving general TCP inputs.			X
edit_tcp_stream	Lets the user send data to the the /services/receivers/stream REST endpoint.			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

Capability name	What it lets you do	User	Power	Admin
edit_tokens_settings	Lets the user manage token settings.			X
edit_udp	Lets the user change settings for UDP inputs.			X
edit_upload_and_index	Lets the user use the indexing preview feature when creating inputs in Splunk Web (the `edit_monitor` capability also provides this permission.)			X
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_watchdog				
edit_web_features	Lets a user write to the '/web-features' REST endpoint.			X
edit_web_settings	Lets the user change settings for web.conf through the system settings endpoint.			X
edit_workload_policy	Lets a user edit workload_policy.conf file settings through the workloads/policy endpoint. For now, it is used to view 'admission_rules_enabled' setting under stanza [search_admission_control]. admission_rules_enabled = 1 means the admission rules are enabled in /manager/system/workload_management			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 index settings.			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

Capability name	What it lets you do	User	Power	Admin
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_all_objects	Lets a user list all configuration settings for the configuration endpoints. This capability prevents unauthorized access to configuration endpoints.	X	X	X
list_all_roles	Lets a user list all roles and the capabilities that are assigned to those roles. For full access to listing users, roles, and capabilities, the user must also have or assign the 'list_all_users' capability.		X	X
list_all_users	Lets a user list all users by accessing the /services/authentication/users REST endpoint. For full access to listing users, roles, and capabilities, the user must also have or assign the 'list_all_roles' capability.		X	X
list_accelerate_search	Lets the user view accelerated reports. User cannot accelerate reports.			X
list_cascading_plans	Lets a user view the generated knowledge bundle replication plans if the chosen replication policy in distsearch.conf is set to 'cascading'.			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_field_filter	Lets a user view field filters by using Splunk Web or the Splunk platform REST API **authorization/fieldfilters** and **authorization/fieldfilters/{name}** endpoints. See Protect PII, PHI, and other sensitive data with field filters.		X	X
list_forwarders	Lets a user list and view settings for data forwarding. Can be used by TCP and Syslog output admin handlers.			X
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_health_subset	Lets a user disable or enable health reporting for a feature in the "health_subset" view of the health status tree. Actions are performed through the server/health-config/{feature_name} endpoint.			

Capability name	What it lets you do	User	Power	Admin
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_ingest_rulesets	Lets a user view the list of ingest actions rulesets and destinations.			X
list_inputs	Lets the user view lists of various inputs, including input from files, TCP, UDP, scripts, the structure of Windows Registry, and so on.	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_pipeline_sets	Lets a user list information about pipeline sets.			X
list_remote_input_queue	Lets a user view the configuration details of a configured remote input queue for Splunk Cloud and Splunk Cloud Services (SCS) instances.			X
list_remote_output_queue	Lets a user view the configuration details of a configured remote output queue for Splunk Cloud and Splunk Cloud Services (SCS) instances.			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 'edit_storage_passwords' capability must be added to the role for the user to perform POSTs to the `/storage/passwords` endpoint.			X
list_token_http	Lets a user display settings for the HTTP token input.			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_tokens_scs	Lets a user retrieve a Splunk Cloud Services (SCS) token for an SCS service with which a Splunk Cloud Platform deployment has been configured to communicate.			
list_workload_policy	Lets a user view workload_policy.conf file settings through the workloads/policy endpoint. For now, it is used to view 'admission_rules_enabled' setting under stanza [search_admission_control]. admission_rules_enabled = 1 means the admission rules are enabled in Admission Rules UI.			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
merge_buckets	Lets a user merge buckets using the 'cluster-merge-buckets' CLI command for clustered environments.			X

Capability name	What it lets you do	User	Power	Admin
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
read_internal_libraries_settings	Lets a user read the 'quarantined/status' REST endpoint and also view the Internal Libraries Settings page in Splunk Web.			X
refresh_application_licenses				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_access_server_endpoints	Lets a user access any /**services**/**server**/* endpoints using the `rest` command. For example, a role with the rest_access_server_endpoints capability can run the following searches: • `|rest splunk_server=local /services/server/info` • `|rest splunk_server=local /services/server/security` • `|rest splunk_server=local /services/server/roles` • `|rest splunk_server=local /services/server/introspection`	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	Lets the user list and view various properties in the Python remote apps handler. See `restmap.conf` for more information.	X	X	X
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_reason	Lets the user see the reason why the Splunk platform needs to restart.			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_commands_ignoring_field_filter	When field filters are in use, this capability lets users run searches across any indexes in the organization using certain restricted commands that return protected data. This capability is required for roles to run the following commands that are restricted by default: tstats, mstats, mpreview, walklex, and typeahead. These commands can return sensitive index information to which roles that are restricted by field filters should not have access. See Protect PII, PHI, and other sensitive data with field filters.		X	X
run_custom_command	Lets the user run custom search commands.	X	X	X
run_debug_commands	Lets a user run debugging commands, for example 'summarize'.			X
run_dump	Lets the user run the `dump` search command.	X	X	X
run_mcollect	Lets the user run the `mcollect` and `meventcollect` commands.	X	X	X

Capability name	What it lets you do	User	Power	Admin
run_msearch	Lets the user run the `msearch` command.			X
run_sendalert	Lets the user run the 'sendalert' command.	X	X	X
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 and rtsearch capabilities 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
splunk_assist_admin	Lets the user load and access the Splunk Assist service.			X
splunk_mobile_administration				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
upgrade_splunk_idxc	Lets the user perform an automated rolling upgrade of an indexer cluster to a higher version of Splunk Enterprise. Works only with the splunk_system_upgrader role.			
upgrade_splunk_shc	Lets the user perform an automated rolling upgrade of a search head cluster to a higher version of Splunk Enterprise. Works only with the splunk_system_upgrader role.			
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
upload_mmdb_files	Lets a user upload mmdb files, which are used for iplocation searches.			X
use_file_operator	Lets the user use the "file" search operator. The "file" search operator is deprecated.			X
use_remote_proxy				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.