# Splunk® Enterprise Security Installation and Upgrade Manual 7.0.1

## Configure users and roles

Generated: 4/05/2022 9:33 am

# Configure users and roles

Splunk Enterprise Security uses the access control system integrated with the Splunk platform. The Splunk platform authorization allows you to add users, assign users to **roles**, and assign those roles custom **capabilities** to provide granular, role-based access control for your organization.

Splunk Enterprise Security relies on the admin user to run saved searches. If you plan to delete the admin user, update knowledge objects owned by that user before you do.

- For Splunk Enterprise, see Reassign one or more shared knowledge objects to a new owner in the *Knowledge Manager Manual*.
- For Splunk Cloud Platform, see Reassign one or more shared knowledge objects to a new owner in the *Knowledge Manager Manual*.

There are scenarios where it is still possible for an authenticated user to interact with certain core resources outside the control of the ES app, which can result in a lack of auditability. Make sure that all users with access to the ES app are trusted users that should have access to your ES related data, such as notable events and investigations.

## Configuring user roles

Splunk Enterprise Security adds three roles to the default roles provided by Splunk platform. The new roles allow a Splunk administrator to assign access to specific functions in ES based on a user's access requirements. The Splunk platform administrator can assign groups of users to the roles that best fit the tasks the users will perform and manage in Splunk Enterprise Security. There are three categories of users.

| User | Description | Splunk ES role |
|---|---|---|
| Security Director | Seeks to understand the current security posture of the organization by reviewing primarily the Security Posture, Protection Centers, and Audit dashboards. A security director does not configure the product or manage incidents. | `ess_user` |
| Security Analyst | Uses the Security Posture and Incident Review dashboards to manage and investigate security incidents. Security Analysts are also responsible for reviewing the Protection Centers and providing direction on what constitutes a security incident. They also define the thresholds used by correlation searches and dashboards. A Security Analyst must be able to edit notable events. | `ess_analyst` |
| Solution Administrator | Installs and maintains Splunk platform installations and Splunk Apps. This user is responsible for configuring workflows, adding new data sources, and tuning and troubleshooting the application. | `admin` or `sc_admin` |

Each Splunk Enterprise Security custom role inherits from Splunk platform roles and adds capabilities specific to Splunk ES. Not all of the three roles custom to Splunk ES can be assigned to users.

| Splunk ES role | Inherits from Splunk platform role | Added Splunk ES capabilities | Can be assigned to users |
|---|---|---|---|
| `ess_user` | user | Real-time search, list search head clustering, edit Splunk eventtypes in the Threat Intelligence supporting add-on, manage notable event suppressions. | Yes. Replaces the `user` role for ES users. |
| `ess_analyst` | user, ess_user, power | Inherits `ess_user` and adds the capabilities to create, edit, and own notable events and perform all transitions, | Yes. Replaces the `power` role for ES users. |

| Splunk ES role | Inherits from Splunk platform role | Added Splunk ES capabilities | Can be assigned to users |
|---|---|---|---|
| | | and create and modify investigations. | |
| `ess_admin` | user, ess_user, power, ess_analyst | Inherits `ess_analyst` and adds several other capabilities. | **No**. You must use a Splunk platform admin role to administer an Enterprise Security installation. |

See the capabilities specific to Splunk Enterprise Security for more details about which capabilities are assigned to which roles by default.

The Splunk platform `admin` role inherits all unique ES capabilities. In a Splunk Cloud Platform deployment, the Splunk platform admin role is named `sc_admin`. Use the `admin` or `sc_admin` role to administer an Enterprise Security installation.

| Splunk platform role | Inherits from role | Added capabilities | Accepts user assignment |
|---|---|---|---|
| `admin` | user, ess_user, power, ess_analyst, ess_admin | All | Yes. |
| `sc_admin` | user, ess_user, power, ess_analyst, ess_admin | All | Yes. |

ES expects that a user with the name and role of `admin` exists. If ES is installed on an on-premises Splunk Enterprise instance where the admin user's name is changed during the initial installation, then the scheduled searches included with ES are orphaned, disabled, and an error message prompts you to reassign them.

#### *Role inheritance*

All role inheritance is preconfigured in Enterprise Security. If the capabilities of any role are changed, other inheriting roles will receive the changes. For more information about roles, see the Splunk platform documentation.

- For Splunk Enterprise, see Add and edit roles in *Securing Splunk Enterprise*.
- For Splunk Cloud Platform, see Manage Splunk Cloud Platform roles in *Splunk Cloud Platform Admin Manual*.

## Add capabilities to a role

Capabilities control the level of access that roles have to various features in Splunk Enterprise Security. Use the **Permissions** page in Enterprise Security to review and change the capabilities assigned to a role.

1. On the Splunk Enterprise Security menu bar, select **Configure > General > Permissions**.
2. Find the role you want to update.
3. Find the **ES Component** you want to add.
4. Select the check box for the component for the role.
5. Save.

#### *Capabilities specific to Splunk Enterprise Security*

Splunk Enterprise Security uses custom capabilities to control access to Splunk Enterprise Security-specific features. However, if you see `list_inputs`, this is a base capability that should not be removed.

Add capabilities on the permissions page in Splunk Enterprise Security to make sure that the proper access control lists (ACLs) are updated. The permissions page makes the ACL changes for you. If you add these custom capabilities on the Splunk platform settings page, you must update the ACLs yourself.

Capabilities are defined in the authorize.conf configuration file for Enterprise Security.

| Function in ES | Description | Capability | ess_user | ess_analyst | ess_admin |
|---|---|---|---|---|---|
| Access data from Splunk UBA | Access data from Splunk Enterprise to Splunk UBA. See Set up the Splunk add-on for Splunk UBA in Splunk Enterprise Security. | edit_uba_settings | | | X |
| Adaptive Response Relay and associated KVStore collection | Write the Common Action Model (CAM) queue. See Set up an Adaptive Response Relay in Splunk Enterprise Security. | edit_cam_queue | | | X |
| Configuration checks | Allows you to run configuration checks. | edit_modinput_configuration_check | | | X |
| Create new notable events | Create ad-hoc notable events from search results. See Manually create a notable event in Splunk Enterprise Security. | edit_notable_events | | X | X |
| Credential Manager | Manage credentials and certificates for Splunk Enterprise Security and other apps. Cannot be set on the Permissions page. See Manage credentials in Splunk Enterprise Security. | admin_all_objects<br>list_storage_passwords<br>list_app_certs<br>edit_app_certs<br>delete_app_certs | | | X |
| Data migrations | Allows you to perform one-time data migrations. | edit_modinput_data_migrator | | | X |
| Edit the Data Model Acceleration (DMA) modular input | Identify who can edit the Data Model Acceleration modular input. DMA is turned on for the required data models using a modular input by default. | edit_modinput_dm_accel_settings | | | X |
| Edit specific modinputs | Make changes to edit the modular name by using the "whois" feature. | edit_modinput_whois | | | X |
| Edit advanced search schedule settings | Edit the schedule priority and schedule window of correlation searches on Content Management. | edit_search_schedule_priority<br>edit_search_schedule_window | | | X |
| Edit correlation searches | Edit correlation searches on Content Management. See Configure correlation searches in Splunk Enterprise Security. Users with this capability can also export content from Content Management as an app. See Export content as an | edit_correlationsearches<br>schedule_search | | | X |

| Function in ES | Description | Capability | ess_user | ess_analyst | ess_admin |
|---|---|---|---|---|---|
| | app from Splunk Enterprise Security. | | | | |
| Edit Distributed Configuration Management | Use distributed configuration management. See Deploy add-ons included with Splunk Enterprise Security. | edit_modinput_es_deployment_manager | | | X |
| Edit ES navigation | Make changes to the Enterprise Security navigation. See Customize the menu bar in Splunk Enterprise Security. | edit_es_navigation | | | X |
| Edit identity lookup configuration | Manage Asset and Identity lookup configurations. See Add asset and identity data to Splunk Enterprise Security, Enable asset and identity correlation in Splunk Enterprise Security, and Manage assets and identities in Splunk Enterprise Security. | edit_modinput_identity_manager | | | X |
| Edit Incident Review | Make changes to Incident Review settings. See Customize Incident Review in Splunk Enterprise Security. | edit_log_review_settings | | | X |
| Edit lookups | Create and make changes to lookup table files. See Create and manage lookups in Splunk Enterprise Security. | edit_lookups, edit_managed_configurations | | | X |
| Edit statuses | Make changes to the statuses available to select for investigations and notable events. See Manage notable event statuses. | edit_reviewstatuses | | | X |
| Edit notable event suppressions | Edit Splunk eventtypes in the Threat Intelligence supporting add-on, and create and edit notable event suppressions. See Create and manage notable event suppressions.<br><br>The `ess_user` and `ess_analyst` roles don't have the default ability to edit suppressions through Splunk Web. However, they have the ability to perform read and write operations on eventtypes, so they can edit suppressions through the event types interface. | edit_suppressions | | | X |

| Function in ES | Description | Capability | ess_user | ess_analyst | ess_admin |
|---|---|---|---|---|---|
| | | | | | |
| Edit notable events | Make changes to notable events, such as assigning them and transition them between statuses. Statuses for Splunk ES investigations are stored in the reviewstatuses.conf file. See Triage notable events on Incident Review in Splunk Enterprise Security. | edit_notable_events | | X | X |
| Edit per-panel filters | Permits the role to update per-panel filters on dashboards. See Configure per-panel filtering in Splunk Enterprise Security. | edit_per_panel_filters | | | X |
| Edit app permissions manager | Allows you to edit app permissions manager. Required for essinstall. | edit_modinput_app_permissions_manager | | | X |
| Edit intelligence downloads | Change intelligence download settings. See Download a threat intelligence feed from the Internet in Splunk Enterprise Security and Download an intelligence feed from the Internet in Splunk Enterprise Security. | edit_modinput_threatlist<br>edit_modinput_threat_intelligence_manager | | | X |
| Edit threat intelligence collections | Upload threat intelligence and perform CRUD operations on threat intelligence collections using the REST API. See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security and Threat Intelligence API reference. | edit_threat_intel_collections | | | X |
| Import content | Allows you to import content from installed applications. | edit_modinput_ess_content_importer | | | X |
| Migrate correlation searches | (Internal) Used by the background script to migrate correlation searches. | migrate_correlationsearches | | | X |
| Manage configurations | Make changes to the general settings or the list of editable lookups. See Configure general settings for Splunk Enterprise Security. | edit_managed_configurations | | | X |
| Manage all investigations | Allows the role to view and make changes to all investigations. See Manage security investigations in Splunk Enterprise Security. | manage_all_investigations | | | X |
| Manage Sequence | Allows the role to make changes to Sequence | edit_sequence_templates | | | X |

| Function in ES | Description | Capability | ess_user | ess_analyst | ess_admin |
|---|---|---|---|---|---|
| Templates | Templates, Sequence Template REST handlers, and related web pages. See Manage sequence templates in Splunk Enterprise Security. | | | | |
| Manage analytics stories | Allows the role to make changes to analytics stories. See Manage analytics stories in Splunk Enterprise Security | edit_analyticstories | | X | X |
| Manage your investigations | Create and edit investigations. Roles with this capability can make changes to investigations on which they are a collaborator. See Investigations in Splunk Enterprise Security. | edit_timeline | | X | X |
| Own notable events | Allows the role to be an owner of notable events. See Assign notable events. | can_own_notable_events | | X | X |
| Search-driven lookups | Create lookup tables that can be populated by a search. See Create search-driven lookups in Splunk Enterprise Security. | edit_managed_configurations schedule_search | | | X |
| Update app imports | Allows you to update app imports with all apps matching a given regular expression. | edit_modinput_app_imports_update | | | X |

## Adjust the concurrent searches for a role

Splunk platform defines a limit on concurrently running searches for the `user` and `power` roles by default. You may want to change those concurrent searches for some roles.

1. On the Splunk Enterprise Security menu bar, select **Configure > General > General Settings**.
2. Review the limits for roles and change them as desired.

| Item | Description |
|---|---|
| Search Disk Quota (admin) | The maximum disk space (MB) a user with the admin role can use to store search job results. |
| Search Jobs Quota (admin) | The maximum number of concurrent searches for users with the admin role. |
| Search Jobs Quota (power) | The maximum number of concurrent searches for users with the power role. |

To change the limits for roles other then `admin` and `power`, edit the `authorize.conf` file to update the default search quota. See the authorize.conf.example in the Splunk Enterprise *Admin* manual.

## Configure the roles to search multiple indexes

The Splunk platform stores ingested data sources in multiple indexes. Distributing data into multiple indexes allows you to use role-based access control and vary retention policies for data sources. The Splunk platform configures all roles to

search only the `main` index by default. For more information about working with roles, see the Splunk platform documentation.

- For Splunk Enterprise, see About configuring role-based user access in the *Securing Splunk Enterprise* manual.
- For Splunk Cloud Platform, see Manage Splunk Cloud Platform users and roles in the *Splunk Cloud Platform Admin Manual*.

To allow roles in Splunk Enterprise Security to search additional indexes, assign the indexes that contain relevant security data to the relevant roles.

1. Select **Settings > Access Controls**.
2. Click **Roles**.
3. Click the role name that you want to allow to search additional indexes.
4. Select the desired **Indexes searched by default** and **Indexes** that this role can search. Do not include summary indexes, as this can cause a search and summary index loop.
5. Save your changes.
6. Repeat for additional roles as needed.

If you do not update the roles with the correct indexes, searches and other knowledge objects that rely on data from unassigned indexes will not update or display results.

For more information on the reasons for multiple indexes, see Why have multiple indexes? in Splunk Enterprise *Managing Indexers and Clusters of Indexers*.

## Configure permissions for Machine Learning Toolkit SPL commands

No new capabilities are added to ES for using MLTK. To restrict permissions for MLTK SPL commands, see Change permissions in default.meta.conf in the Splunk Machine Learning Toolkit *User Guide*.