Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Administering Splunk Enterprise Security

Generated: 3/30/2022 5:06 pm

Administering Splunk Enterprise Security

Splunk Enterprise Security administrators are responsible for configuring, maintaining, auditing, and customizing an instance of Splunk Enterprise Security. If you are not administering Splunk Enterprise Security, see *Use Splunk Enterprise Security* for an introduction to using this app as a security analyst.

Use the links below to learn more about administrative tasks in Splunk Enterprise Security.

Manage and support analyst workflows

To enable and customize the workflows for analysts in your organization, see:

- Managing Incident Review in Splunk Enterprise Security
- Customize Incident Review in Splunk Enterprise Security
- Customize notable event settings in Splunk Enterprise Security
- Manage investigations in Splunk Enterprise Security

Enrich data for Enterprise Security

Enrich Splunk Enterprise Security with data about the assets and identities in your environment and with additional data about known threats.

- See Add asset and identity data to Splunk Enterprise Security for a full list of tasks related to adding and managing asset and identity data in Splunk Enterprise Security.
- See Add threat intelligence to Splunk Enterprise Security for information on all tasks related to managing threat intelligence sources in Splunk Enterprise Security.

Manage and customize configurations

To perform ongoing configuration in Splunk Enterprise Security, see:

- Configure general settings for Splunk Enterprise Security
- Manage input credentials in Splunk Enterprise Security
- Manage permissions in Splunk Enterprise Security
- Customize the menu bar in Splunk Enterprise Security
- Configure advanced filtering in Splunk Enterprise Security

You can find additional configuration information in the *Install and Upgrade Manual*.

- Configure and deploy indexes
- Configure users and roles
- Configure data models for Splunk Enterprise Security

Create, manage, and export content

To create new content or manage and customize existing content, see:

- Create correlation searches in Splunk Enterprise Security
- Create and manage key indicator searches in Splunk Enterprise Security

- Create and manage saved searches in Splunk Enterprise Security
- Create and manage search-driven lookups in Splunk Enterprise Security
- Create and manage swim lane searches in Splunk Enterprise Security
- Create and manage views in Splunk Enterprise Security
- Create and manage lookups in Splunk Enterprise Security
- Create risk and edit risk objects in Splunk Enterprise Security

To share custom content with other ES instances, see Export content from Splunk Enterprise Security as an app.

Troubleshoot dashboards

- For tips and best practices useful for troubleshooting dashboards in Enterprise Security, see Troubleshoot dashboards in Splunk Enterprise Security.
- For information about data model datasets that populate Enterprise Security dashboards, see Dashboard requirements matrix for Splunk Enterprise Security.
- For an overview of all dashboards in Splunk Enterprise Security, see Introduction to the dashboards available in Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Configure users and roles

Configure user roles and capabilities to provide granular, role-based access control for your organization. See Configure users and roles.