

Using Splunkbase Add-ons and Apps with Splunk Enterprise Security

Identifying, ingesting and interpreting data correctly is a foundational step in the success of your Splunk security implementation that, if done correctly, will allow you to get the most value across your entire Splunk environment. To help you get this done correctly, you can use Splunk Add-ons and Apps, found in [Splunkbase](#), to easily bring in new sources of information that expand your risk and defense posture.

Splunk's community of Add-ons and Apps are designed to make ingesting new data simple, efficient, and accessible, as well as help you achieve your use cases faster.

Add-ons and Apps are implemented in similar ways. Both are packaged and uploaded to Splunkbase as .spl files. To install them in your Splunk instance you'll unpackage (un-tar) the .spl file into your `/etc/apps` directory, and then it will be ready for configuration and use. But there are important differences in the content and purpose of both Add-ons and Apps, which we'll explain in this article.

This article is part of Splunk's [Use Case Explorer for Security](#), which is designed to help you identify and implement prescriptive use cases that drive incremental business value. In the Security maturity journey described in the Use Case Explorer, this article is part of [Enrichment](#).

What are Add-ons?

Splunk Add-ons are most commonly used to bring new data sources into the Splunk platform. Add-ons don't generally contain a navigable user interface, and they can usually be used to help you achieve a variety of use cases.

Add-on developers design their add-ons to be used with the Splunk [Common Information Model \(CIM\)](#) in order to work with the larger Splunk ecosystem. Add-ons provide the field extractions, lookups and event types needed to map data to the CIM, allowing you to easily use your new data source in data models, pivots, and CIM-based applications.

Add-ons are valuable to your Splunk Enterprise Security deployment in the following ways:

- They are used for data optimization and collection processing and increase overall efficiency.
- They typically enhance the data from any source and create a rich data set.
- They can consume data from hundreds of different sources and can automatically select, identify, and tag fields.
- They are helpful in enriching the data from different information sources.

The Splunk Common Information Model add-on is packaged with CIM-based apps such as Splunk Enterprise Security and the Splunk App for PCI Compliance. If you are using an add-on in conjunction with one of these apps, you do not need to install the Splunk Common Information Model add-on separately.

What are Apps?

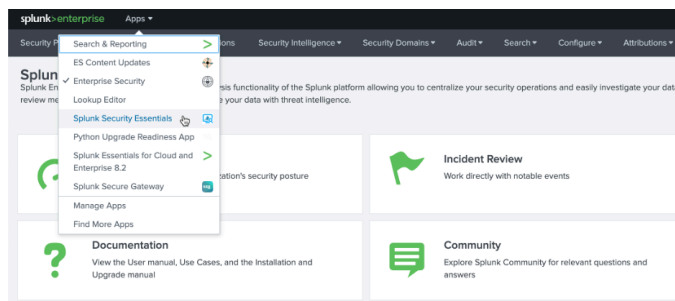
Apps contain a navigable user interface with pre-configured additional capabilities you can use with a data source. An App generally serves a particular use case, targets a specific type of user, or targets a specific domain of operational visibility. They are typically composed of many different Splunk knowledge objects (for example lookups, tags, event types, saved searches) as well as data inputs, and they can potentially also incorporate Add-ons.

Splunk Enterprise Security itself is an App.

Apps increase your use case functionality and bring additional value to your Splunk Enterprise Security deployment by providing you with capabilities such as:

- Pre-built dashboards, reports, and workflows.
- Visualization, analysis and reporting capabilities.
- Simplified access to user tasks, while allowing access to the data and the functions of the core Splunk platform.
- Representations of real-time data.

You can also apply user- or role-based permissions and access controls to provide control when you are deploying and sharing apps across your organization. Apps can be opened from the Splunk Enterprise home page, from the App menu, or from the Apps section in the settings of your instance.

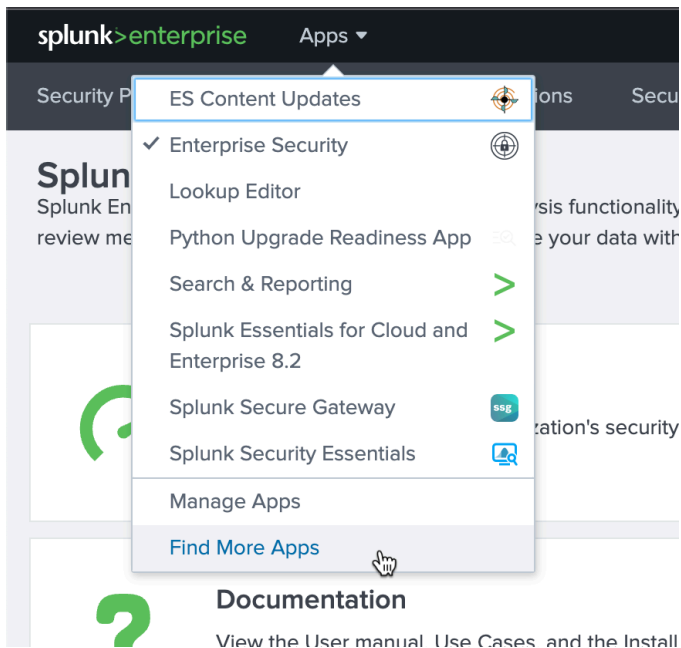


How to use Splunkbase

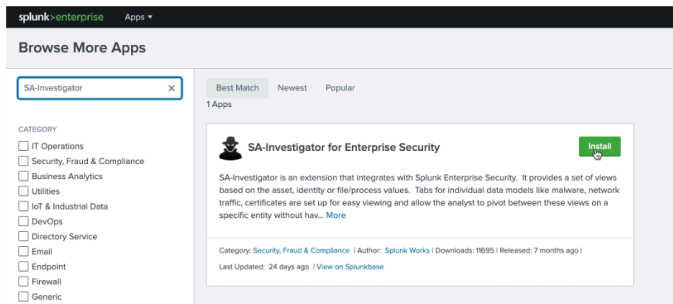
[Splunkbase](#) is a community that is facilitated and hosted by Splunk where users can easily find Add-ons and Apps which further boost the functionality and practicality of Splunk. Your local Splunk environment integrates with Splunkbase. It provides an easy and quick interface for locating the Add-ons that help you achieve specific use cases and access vendor-specific Add-ons and Apps.

Here's an example of how to work in Splunkbase. In this example we'll show how to install the [SA-Investigator for Enterprise Security](#) into a local Splunk environment.

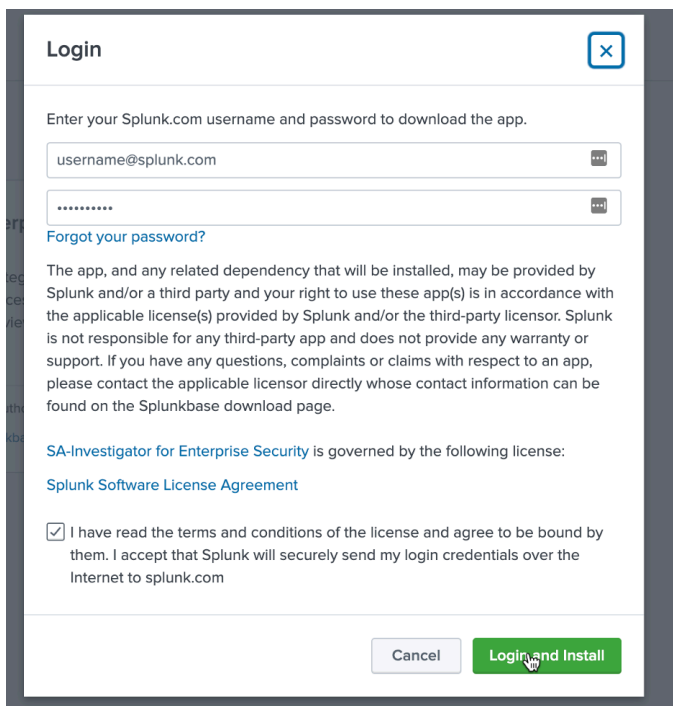
1. Log into your local Splunk environment.
2. Click **Splunk Apps**, then **Find More Apps**.



3. Use the Search function to find the Add-on or App you're looking for. In this example we are searching for the SA-Investigator for Enterprise Security.



4. Click **Install** and enter your login information when prompted.



Login

Enter your Splunk.com username and password to download the app.

username@splunk.com

.....

[Forgot your password?](#)

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app and does not provide any warranty or support. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

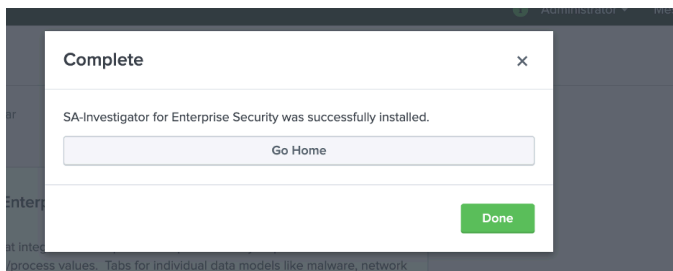
SA-Investigator for Enterprise Security is governed by the following license:

[Splunk Software License Agreement](#)

☒ I have read the terms and conditions of the license and agree to be bound by them. I accept that Splunk will securely send my login credentials over the Internet to splunk.com

[Cancel](#) [Login and Install](#)

5. Complete the installation and click **Go Home**.



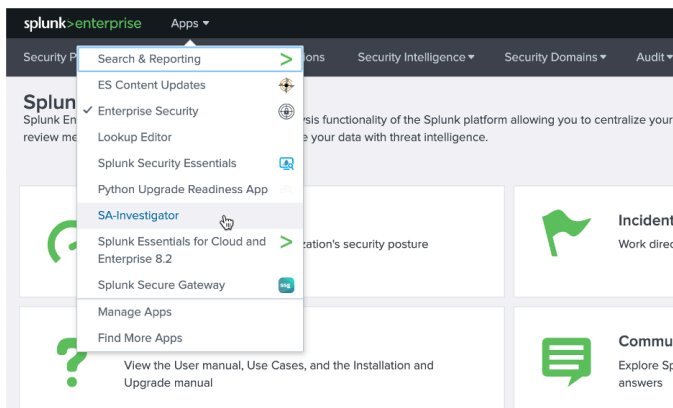
Complete

SA-Investigator for Enterprise Security was successfully installed.

[Go Home](#)

[Done](#)

6. Locate the app by looking under the Apps menu. If necessary, complete any additional configuration, then you can begin using the App.



Alternatively, you can install the Add-on or App directly to your local Splunk environment. To do this, download the file directly to a local system and upload it to your Splunk environment. Make sure to practice good Splunk hygiene by

only downloading trusted Splunk Add-ons and Apps.

Next steps

Still having trouble? Splunk has many resources available to help get you back on track. We recommend the following:

- [Splunk OnDemand Services](#): Access credit-based services that allow direct access to Splunk technical consultants for a variety of technical services from a pre-defined catalog. Many Splunk customers already have OnDemand credits included as part of their software license. To request OnDemand Services, file a ticket through the [Support Portal](#).
- [Splunk Answers](#): Ask your question in the Splunk Community, which has provided over 50,000 user solutions to date.
- [Splunk Customer Support](#): Contact Splunk to discuss your environment and receive customer support.