Splunk® Security Content Installation Guide 3.52.0

Generated: 11/09/2022 10:31 am

Table of Contents

Installation

Install the Splunk Enterprise Security Content Update Subscription Service

1. Check that your environment meets the Prerequisites.
2. Plan your installation.
3. Install ESCU using Splunk Web or Install ESCU from a downloaded file.
4. Add the Analytic Story Detail view to your instance of Splunk Enterprise Security.

Prerequisites

Operating system	Linux/Windows
Splunk Enterprise	Supports version 7.0 or later
Splunk Cloud	Supported
Splunk Enterprise Security	Supports version 4.7.0 or later

Plan your installation

Use the tables below to determine where and how to install Splunk Enterprise Security Content Update (Splunk ESCU) on your deployment of Splunk Enterprise Security (Splunk ES).

Distributed installation of this add-on

Use the table to determine where to install ESCU in a Splunk Enterprise Security distributed deployment.

Splunk instance type	Supported	Comments
Search Heads	Yes	Install ESCU on the Enterprise Security search head.
Indexers	No	ESCU does not contain indexes or index-time transformations.
Forwarders	No	ESCU does not contain inputs for forwarder data collection.

Distributed deployment feature compatibility

Use the table to check the compatibility of ESCU with Splunk Enterprise distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	Use the search head cluster deployer to distribute ESCU across search head cluster members. See Install an add-on in a distributed Splunk Enterprise deployment in the Splunk Add-ons documentation.
Indexer Clusters	No	ESCU does not contain indexes or index-time transformations.
Deployment Server	No	ESCU does not contain inputs for forwarder data collection.

Install ESCU using Splunk Web

1. Log in to Splunk Web on your Splunk Enterprise Security search head.
2. From the Splunk Web home page, click the Apps gear icon.
3. Click **Browse more apps**.

4. On the Browse more apps page, locate the Splunk ES Content Update in the list.
5. Provide your splunk.com credentials.
6. Accept the license terms.
7. Click **Login and Install**.
8. Click **Done**.
9. Restart Splunk services to complete the installation.

Install ESCU from a downloaded file

1. Log in to splunkbase.splunk.com.
2. Download Splunk ES Content Update and save it to an accessible location on your system.
3. Log in to Splunk Web on your Splunk Enterprise Security search head.
4. On the Splunk Enterprise menu bar, open **Searching and Reporting** > **App** and select **Manage Apps**.
5. On the Apps page, click **Install App from file**.
6. On the Upload app page, click the **Choose file** button to locate the Splunk ES Content Update file.
7. Click **Upload**.
8. Click **Done**.

Add the Analytic Story Detail view to your instance of Splunk Enterprise Security

Use the Navigation editor to add the **Analytic Story Detail** view to your Splunk Enterprise Security menu bar. See Customize the menu bar in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for details.