The Splunk Add-on for ServiceNow supports automatic incident and event creation and incident update from scripts triggered by alerts.

Before you can use these scripts, see configure ServiceNow to integrate with the Splunk platform.

Depending on the search that you run, alert-triggered scripts can create multiple events or incidents in ServiceNow. This can occur when the search string in the alert logic returns multiple events. The number of events returned by a search in your alert equals the number of incidents or events created in ServiceNow.

1. **Create an incident or event based on an alert.**
2. **In Splunk Web, click Settings > Searches, Reports, and Alerts.**
3. **Click New.**
4. **Set the Destination app to Splunk Add-on for ServiceNow (Splunk\_TA\_snow).**
5. **Enter a Search name that describes the alert you want to create.**
6. **Enter a Search that meets the following criteria:**

* **To create an incident, the search must include the mandatory arguments account. account is required to identify the ServiceNow instance on which incident is to be created. The Splunk platform passes the arguments to the alert result to trigger the script.**
* **To create an event, the search must include the mandatory arguments account, node, resource, type, and severity. account is required to identify the ServiceNow instance on which event is to be created. The other arguments are required by ServiceNow to create an event. The Splunk platform passes the arguments to the alert result to trigger the script.**
  + **account is required by ServiceNow to create an event.**
  + **node is required by ServiceNow to create an event.**
  + **resource is required by ServiceNow to create an event.**
  + **type is required by ServiceNow to create an event.**
  + **severity is required by ServiceNow to create an event.**
  + **account is required to identify the ServiceNow instance on which an event is to be created.**
  + **custom fields are a list of optional fields in a key-value format that you can specify while creating a ServiceNow event.**
* **The search can include any of the optional arguments supported by ServiceNow incident or event creation. See About the commands and scripts for a table detailing each of these arguments.**
* **The search must be in tabular format.**

**6.Under Schedule and alert, click Schedule this search.**

**7.Select values for Schedule type, Run every, Expiration, and Severity according to your alert requirements.**

**8.Under Alert actions, check the box next to Enable under Run a script.**

**9.Enter the name of the script in File name of shell script to run.**

* 1. **For an incident, enter snow\_incident.py**
  2. **For an event, enter snow\_event.py**

**10.Click Save.**

**Update an incident from an alert using the snow\_incident.py script**

**The procedure to update an incident from an alert is the same procedure to create an incident from an alert.**

**account is required, and is used to identify the ServiceNow instance on which incident is to be updated. The argument correlation\_ids is required to update an existing incident.**

**You can update incident using an alert-triggered script only if you created the incident from the Splunk platform. You cannot update incidents created in ServiceNow.**