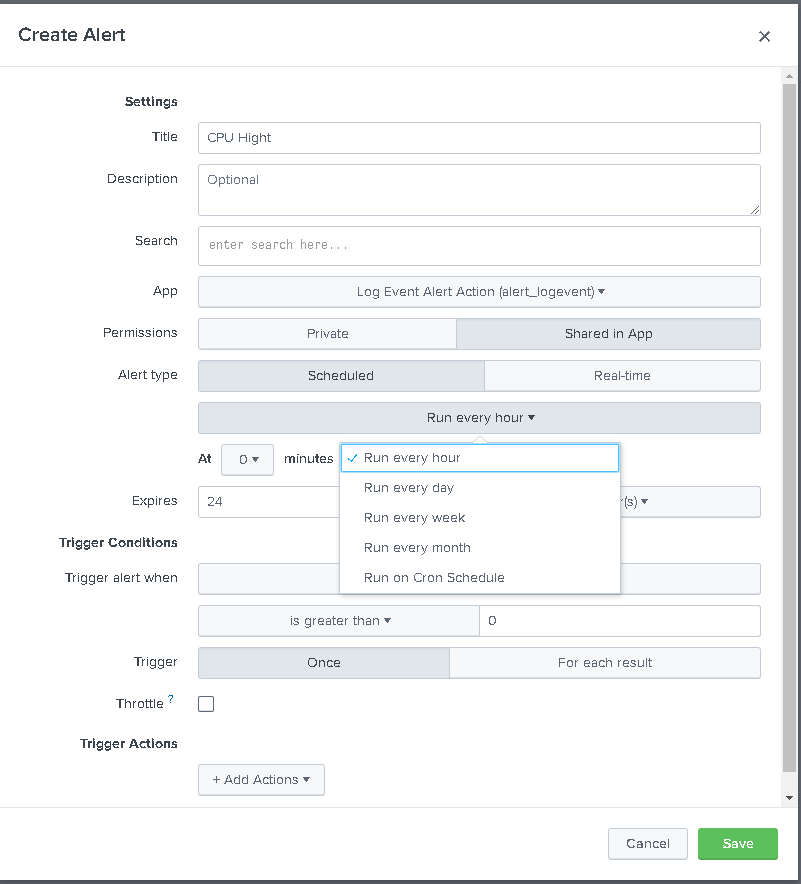
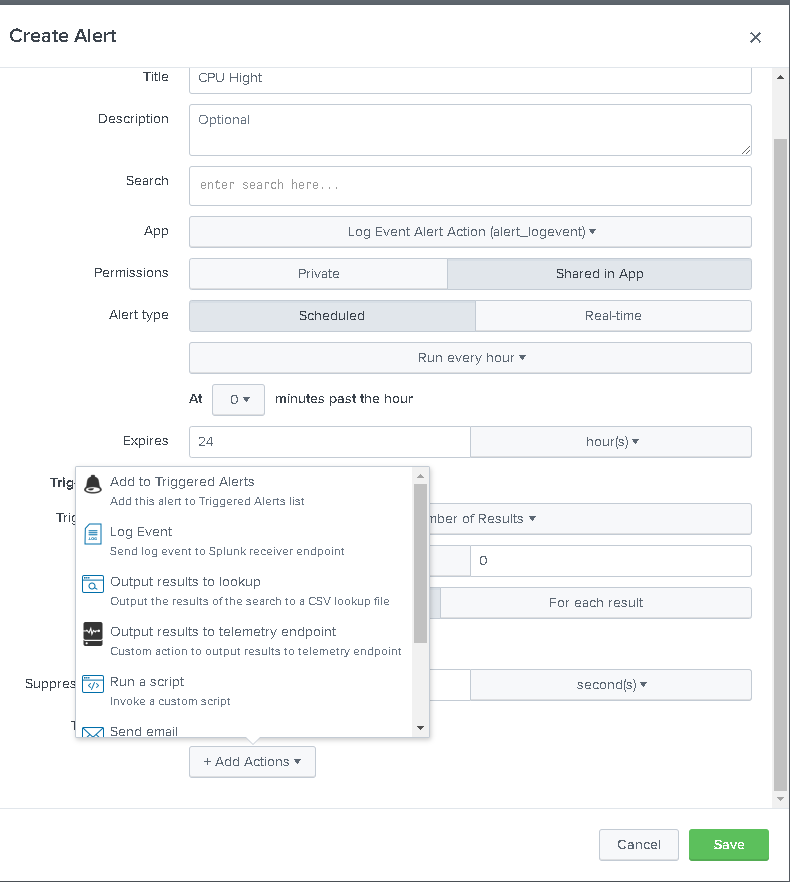
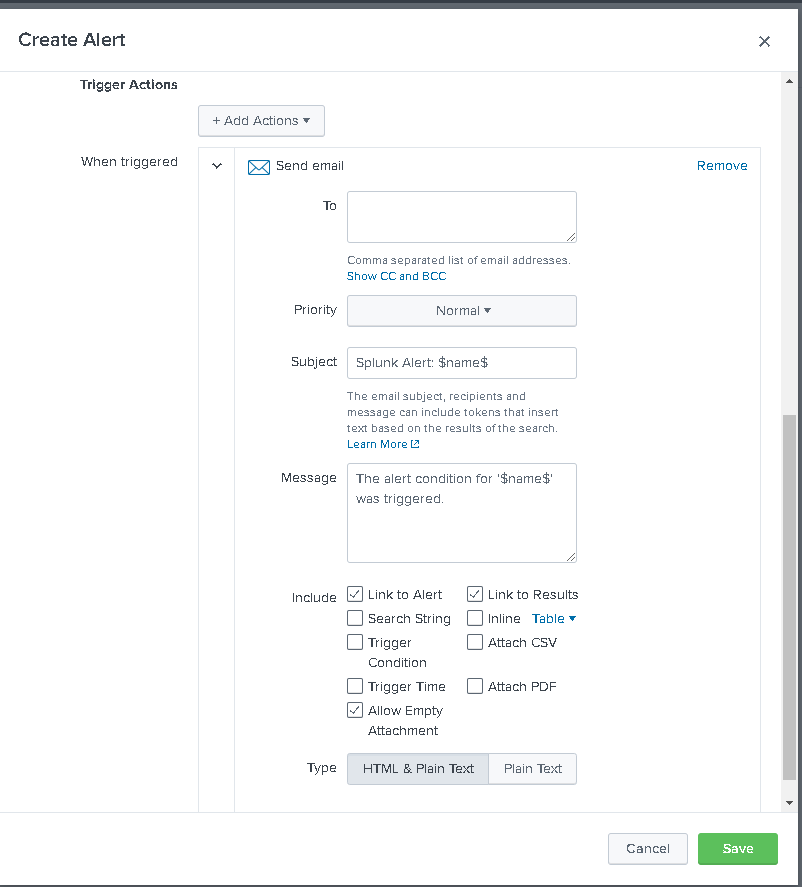
# Splunk Alert Actions





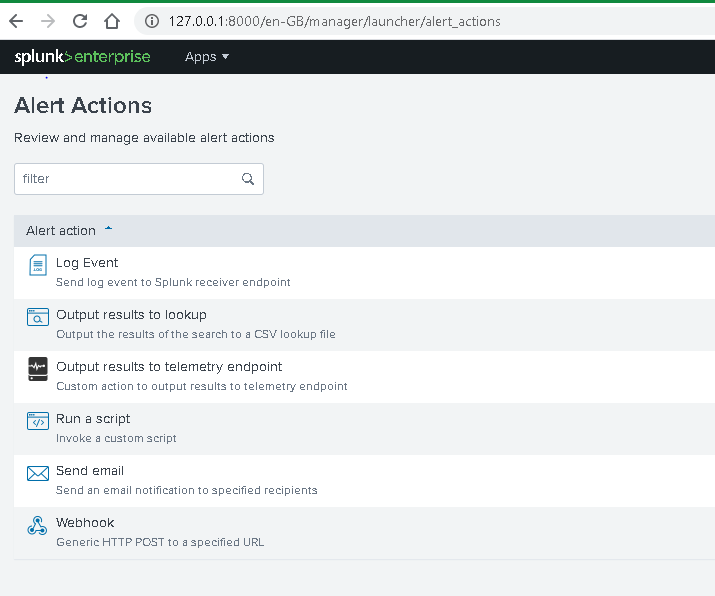


Default Actions:

- Send Email

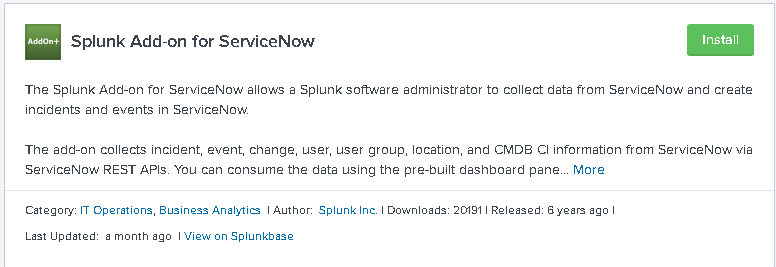
- Run Script

- Webhook Rest

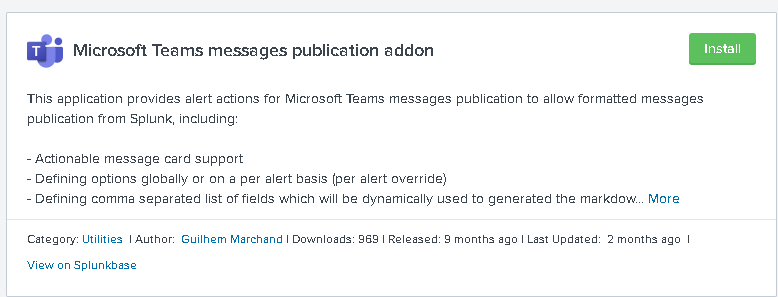


Splunk Add-on for ServiceNow

The Splunk Add-on for ServiceNow allows a Splunk software administrator to collect data from ServiceNow and create incidents and events in ServiceNow. The add-on collects incident, event, change, user, user group, location, and CMDB CI information from ServiceNow via ServiceNow REST APIs. You can consume the data using the pre-built dashboard panels included with the add-on. The add-on also provides workflow actions that allow users to link directly from events in the Splunk platform search results to relevant ServiceNow incidents, events, and Knowledge Base articles. The Splunk Add-on for ServiceNow allows Splunk software administrators to use custom commands, alert actions, and scripts to create new incidents and events in your ServiceNow instance, as well as update the incidents created from the Splunk platform. This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

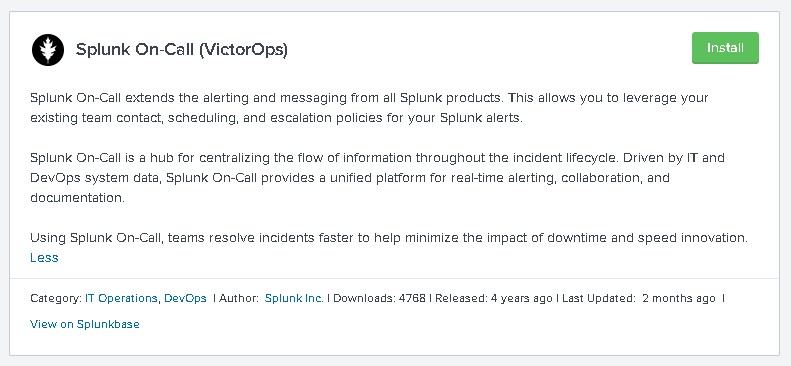


### Microsoft Teams messages publication addon

This application provides alert actions for Microsoft Teams messages publication to allow formatted messages publication from Splunk, including: - Actionable message card support - Defining options globally or on a per alert basis (per alert override) - Defining comma separated list of fields which will be dynamically used to generated the markdown supported publication - Choosing icon link for message publication - Activating potential link action and defining its link (Up to 2 OpenURI actions per alert) - Activating and configuring an HttpPOST potential action that allows additional interactions between Splunk or a third party application from Microsoft Teams - Resilient messages publication management, temporary publication failures are automatically stored in a KVstore, and re-tried following a resilient policy The application provides as well an easy logging access, a basic overview dashboard that exposes successful and failed publications, if any, and finally a builtin alert that can be activated to detect and warn in case of a failure to publish a message in a channel. See https://ta-ms-teams-alert-action.readthedocs.io for more information.

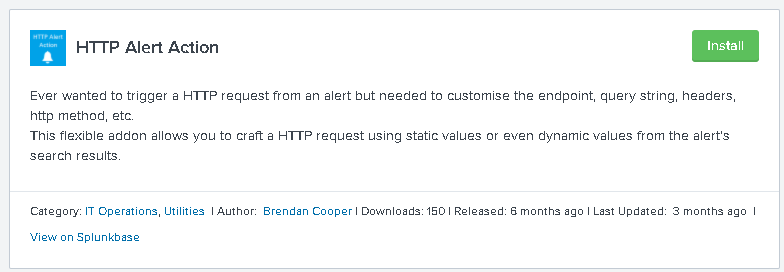
### Splunk On-Call (VictorOps)

Splunk On-Call extends the alerting and messaging from all Splunk products. This allows you to leverage your existing team contact, scheduling, and escalation policies for your Splunk alerts. Splunk On-Call is a hub for centralizing the flow of information throughout the incident lifecycle. Driven by IT and DevOps system data, Splunk On-Call provides a unified platform for real-time alerting, collaboration, and documentation. Using Splunk On-Call, teams resolve incidents faster to help minimize the impact of downtime and speed innovation.



### HTTP Alert Action

Ever wanted to trigger a HTTP request from an alert but needed to customise the endpoint, query string, headers, http method, etc. This flexible addon allows you to craft a HTTP request using static values or even dynamic values from the alert's search results.



### SMSEagle SMS Alert

This app will allow you to send SMS alerts from Splunk without using Internet connection. The app allows to send text messages from your Splunk instance directly to 3G/4G network using SMSEagle. SMSEagle device sends SMS directly to cellular network. There is no third-party external services between. This ensures full security and privacy of information shared across your IT infrastructure. And your SMS will get through even if your Internet connection fails. How to use it? 1) Get your SMSEagle 2) Insert your SIM card into SMSEagle 3) Connect SMSEagle to your IT infrastructure 4) Configure the app in Splunk Now you can send SMS alerts from your Splunk instance directly to 3G/4G network.

