Installing & Configuring the Lumeta App on Splunk

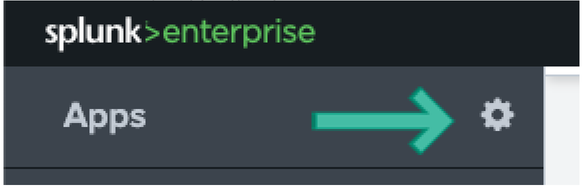
The Lumeta integration with Splunk is now certified and available in the Splunk marketplace. The Lumeta application supports Splunk dashboards and visualizations by providing Lumeta-discovered network data via syslog and REST APIs. Splunk must be version 8.01 or later.

1. Download the Lumeta application file (attached to this page) and plug-in from Splunk (https://splunkbase.splunk.com/apps/#/search/lumeta/) to your local system:
   Version 1.0 of these files are also attached to this page:
   a. TA-lumeta.zip
   b. lumeta_app.zip
2. Unzip them.
   Now you are ready to perform the installation in Splunk.

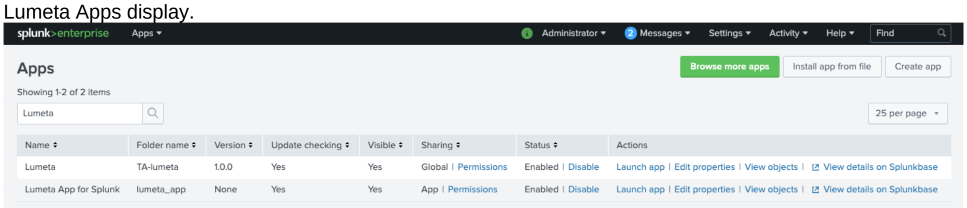
Installing the Lumeta Application in Splunk

To install the Lumeta plug-in to Spunk:

1. Log in to your Splunk server.
2. Select the Manage Apps (gear) icon.



3. In the upper right corner, click **Install App from File**.
4. Browse to TA-lumeta.? and upload it.
5. When prompted, click Restart Now.
6. Repeat steps 3 - 6, this time with lumeta-app. You will not need to restart the system with lumeta-app upload.
   Lumeta Apps display.



Apps

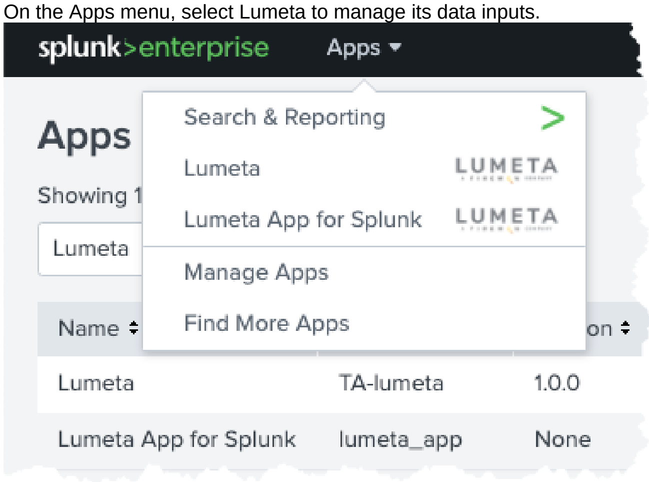
Showing 1-2 of 2 items

Lumeta

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Lumeta	TA-lumeta	1.0.0	Yes	Yes	Global | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
Lumeta App for Splunk	lumeta_app	None	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase

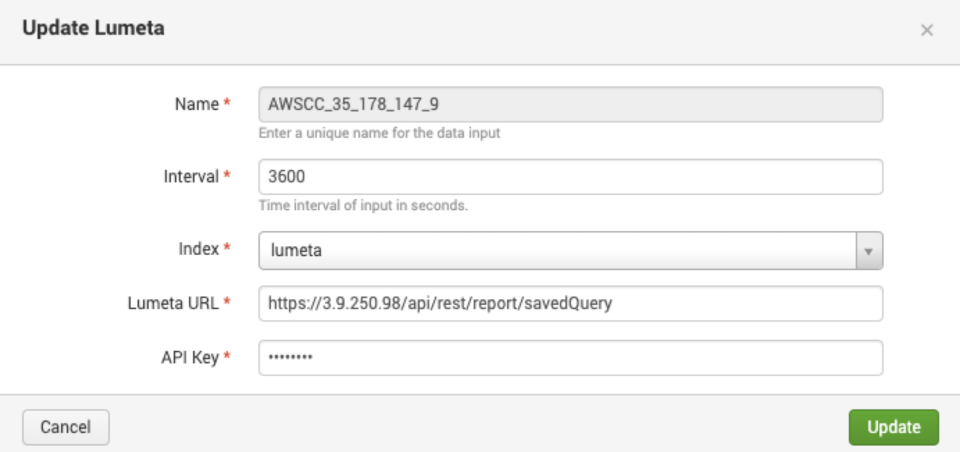
Configuring the Lumeta Application in Splunk

1. On the Apps menu, select Lumeta to manage its data inputs.



2. Click **Create New Input**.

3. Complete the form

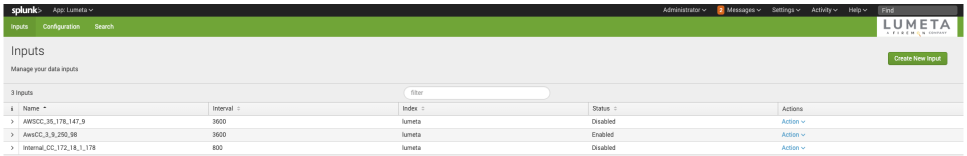


Update Lumeta

Name *	AWSCC_35_178_147_9 Enter a unique name for the data input
Interval *	3600 Time interval of input in seconds.
Index *	lumeta
Lumeta URL *	https://3.9.250.98/api/rest/report/savedQuery
API Key *	••••••••

   a. Name the input. It's a good idea to include the Command Center IP and Port number (9997) in the input name.
   b. The polling Interval is in seconds. Modify the polling interval to a smaller number to be able to use smaller Real-Time intervals on the dashboards.
   c. The Index is lumeta
   d. Add the Lumeta Command Center URL: https://(CC IP or hostname)/api/rest/report/savedQuery

      The connection is made and the new input is added to the list:



Inputs

Manage your data inputs

3 Inputs

i	Name	Interval	Index	Status	Actions
›	AWSCC_35_178_147_9	3600	lumeta	Disabled	Action
›	AwsCC_3_9_250_98	3600	lumeta	Enabled	Action
›	Internal_CC_172_18_1_178	800	lumeta	Disabled	Action

4. Select **Action** > **Enable** to power on the connection.

View Select syslog Data

To search syslog data from Lumeta in Splunk:

1. On the Splunk Apps page, select **Lumeta App for Splunk**.
2. Select the Search tab (if you are not there already).
3. Enter your search criteria. Examples follow:
   a. source=”tcp:9997”
   b. index=lumeta
   c. sourcetype=”lumeta_log_parser”
   d. now combine all 3 into one search
   e. index=lumeta sourcetype=”lumeta_log_parser” source=”tcp:9997”