

Installing & Configuring the Asset Manager's App on Splunk

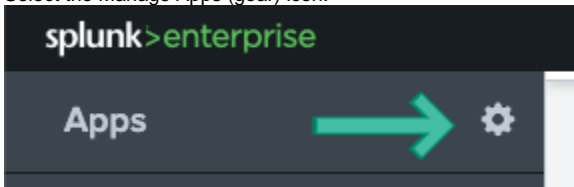
The Asset Manager integration with Splunk is now certified and available in the [Splunk marketplace](#). The application supports Splunk dashboards and visualizations by providing discovered network data via syslog and REST APIs.

1. Download the Asset Manager application file (attached to this page) and plug-in from [Splunk](#) (<https://splunkbase.splunk.com/apps/#/search/lumeta/>) to your local system:
2. You can also contact your TAM or email support@firemon.com to obtain the Splunk App plug-ins.
3. Unzip them.
Now you are ready to perform the installation in Splunk.

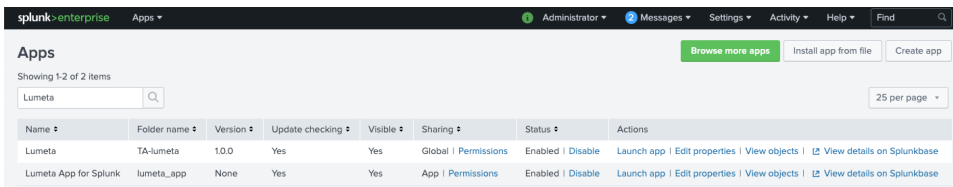
Installing the Lumeta Application in Splunk

To install the Asset Manager plugin to Splunk:

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

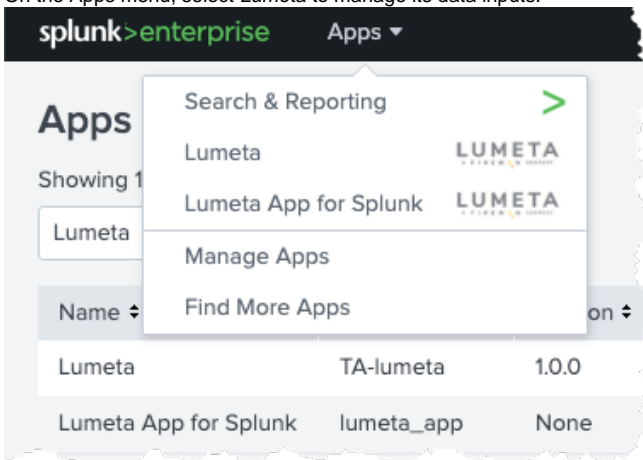


3. In the upper right corner, click **Install App from File**.
4. Browse to TA-lumeta.zip and upload it.
5. When prompted, click Restart Now.
6. Repeat steps 3 - 6, this time with lumeta-app. You will not need to restart the system with lumeta-app upload.



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

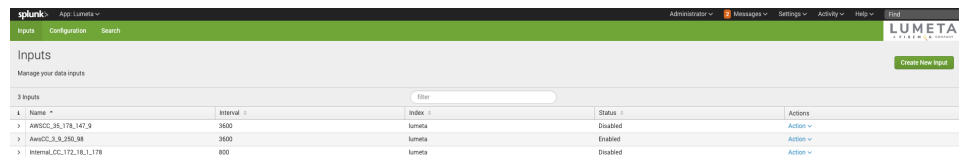
API Key *

Cancel

Update

- Name the input. It's a good idea to include the Command Center IP and Port number (9997) in the input name.
- 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.
- The Index is *lumeta*.
- Add the Lumeta Command Center URL: <https://<Asset Manger IP or hostname>/api/rest/report/savedQuery>

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



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

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

View Select syslog Data

To search syslog data in Splunk:

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