

# Installing & Configuring the Asset Manager's App on Splunk

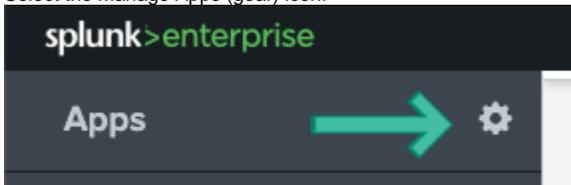
The Asset Manager integration with Splunk is now certified and available in the [Splunk marketplace](#). The application supports Splunk dashboards and visualizations by providing discovered network data via syslog and REST APIs.

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

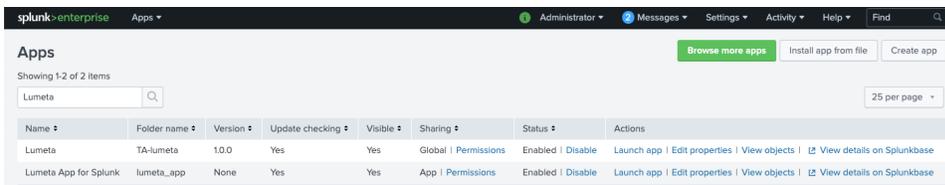
## Installing the Lumeta Application in Splunk

To install the Asset Manager plugin to Splunk:

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

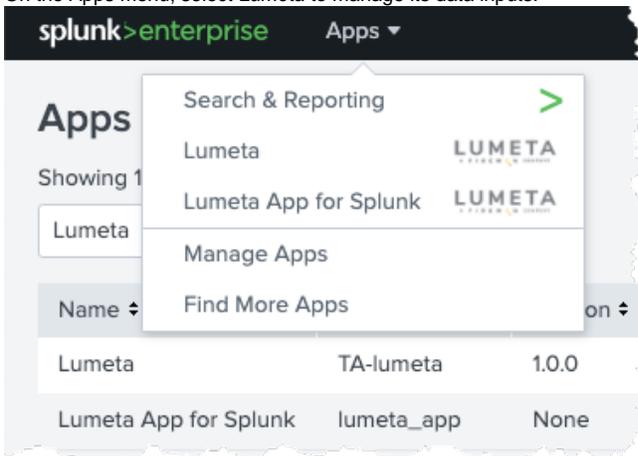


3. In the upper right corner, click **Install App from File**.
4. Browse to TA-lumeta.zip and upload it.
5. When prompted, click Restart Now.
6. Repeat steps 3 - 6, this time with lumeta-app. You will not need to restart the system with lumeta-app upload.



## 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 \*   
Enter a unique name for the data input

Interval \*   
Time interval of input in seconds.

Index \*

Lumeta URL \*

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://<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

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

## View Select syslog Data

To search syslog data 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"`