Automox Splunk Integration

The Automox Splunk apps are applications released to Splunkbase, which consist of two primary components:

1. Automox Technology Add-On for Splunk
2. Automox Dashboard for Splunk

In combination, these two apps allow you to pull Automox console data consisting of endpoint, policy, and event information into Splunk Enterprise or Splunk Cloud platforms and they enable you to visualize and search across the imported Automox data.

Installation

It is possible to install both the Automox Technology Add-On for Splunk and the Automox Dashboard for Splunk apps either through your Splunk instance or with a more manual process of downloading the package from Splunkbase in order to install manually. Both options are outlined in the following sections.

You must first install and configure the Automox Technology Add-On app before the Automox Dashboard for Splunk can populate with any visualizations or searches. In organizations where visualizations are custom tailored, the Automox Dashboard for Splunk is simply a nice starting point, however, it is not required to receive value from the Automox data imported with the Technology Add-On.

Install within Splunk

When you install apps from within a Splunk instance, follow these steps:

1. On the home page left menu, select + Find More Apps.
2. From the Browse More Apps page, search for Automox.
3. Click Install for both apps:
   - Automox Dashboard for Splunk
   - Automox Add-On for Splunk
4. Provide Splunkbase credentials and submit.

Download and Install from Splunkbase

When you install the apps from Splunkbase, it is important to first login to Splunkbase and then download the two app packages. After these are downloaded, follow these steps:

1. On the home page, select the Apps menu and then click Manage Apps.
2. Select Install app from file.
3. Select the previously downloaded app packages.
4. Perform a restart of Splunk when prompted.
When the installation is complete, the apps are visible under the Apps menu in Splunk.

Configuring the Technology Add-On

After you install the Automox Technology Add-On, you must configure it to enable the collection of data from Automox. This configuration requires two steps:

1. **Connection Setup**
2. **Input Creation**

Connection Setup

Within the Splunk interface, navigate to the Apps menu and click Automox Add-On for Splunk.

This will take you to the configuration items as part of the add-on. Select the Configuration tab, which allows you to create and manage connections, configure proxy settings, and configure the log settings. In most environments, it is only necessary to create a new connection:

To add a new connection, provide details for the following:

1. **Connection Name**: A unique name provided to your connection to easily reference during input configuration.
2. **API Key**: An Automox API key is required to pull details from the Automox API. Refer to Adding API Keys for details about how to create a new API key.
3. **Organization ID**: This is an optional ID that allows you to configure a connection specific to an
When at least one connection has been configured, it is then time to define inputs for the add-on.

### Input Creation

The add-on currently provides three types of inputs that can be configured:

1. Automox Event Import
2. Automox Endpoint Import
3. Automox Policy Details Import

Each input can be configured independently to allow for flexibility with respect to which data to have imported into a Splunk environment. In order to configure a new input, select **Create New Input** and then select which import to use.

When configuring an input, you must provide:

1. **Name**: A unique and descriptive name for the input
2. **Interval**: Define the number of seconds to wait between each input collection
3. **Index**: The index to import events into Splunk from the input
4. **Connection**: The name of the connection configured in the previous section

We currently recommend the following settings for **Interval** for each input type:

<table>
<thead>
<tr>
<th>Input</th>
<th>Interval Value (in seconds)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automox Event Import</td>
<td>3600</td>
<td>Every hour</td>
</tr>
<tr>
<td>Automox Endpoint Import</td>
<td>86400</td>
<td>Once per day</td>
</tr>
<tr>
<td>Automox Policy Details Import</td>
<td>86400</td>
<td>Once per day</td>
</tr>
</tbody>
</table>

Due to the nature of the data pulled through the Automox API, currently only the **Event Import** input type allows you to only import “new” events. This input uses an internal checkpoint to track when the last event was imported to ensure duplicate events are not received.

Conversely, the Endpoint and Policy Details inputs pull all data each time the inputs are run. This is why it is recommended to only run the **Endpoint Import** and **Policy Details Import** one time per day.
Collected Data Types

All data collected by this add-on contains a source beginning with “automox_”. The source type of the data varies by the events associated with the input. The following table provides a breakdown of input to sourcetype(s) imported:

<table>
<thead>
<tr>
<th>Input</th>
<th>Source</th>
<th>Sourcetype(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automox Event Import</td>
<td>automox_event_import</td>
<td>automox:console:events</td>
</tr>
<tr>
<td>Automox Endpoint Import</td>
<td>automox_endpoint_import</td>
<td>automox:endpoint</td>
</tr>
<tr>
<td></td>
<td></td>
<td>automox:endpoint:software</td>
</tr>
<tr>
<td>Automox Policy Details Import</td>
<td>automox_policy_details_import</td>
<td>automox:policy</td>
</tr>
</tbody>
</table>

Dashboards

After you import Automox data into Splunk with the Automox Technology Add-On, it is possible to start visualizing the events. The Automox Dashboard for Splunk provides an out of the box and convenient way to visualize endpoints, policies, and events. Install the Dashboard app and navigate to it from within the Splunk interface:

![Automox Dashboard for Splunk](image)

This app provides three dashboards: Endpoints, Policy Details, and Console Events. Each dashboard provides an easy way to select the index where imported events are stored, additionally filtering such as groups and tags for devices, as well as the time period of the data.

It is important to remember, this dashboard is provided for a starting point for end users. Automox encourages adding new visualizations to dashboards to better visualize based on business needs.

Searches

The following example searches can be used after you configure the Technology Add-On.

List the different Automox sourcetypes with counts:

```splunk
index=* source=automox_* | stats count by sourcetype
```

List the number of compliant and non-compliant endpoints:
List the number of endpoints by operating system:

```
index=* sourcetype="automox:endpoint"| stats count by compliant
```

List the different Automox console events with counts:

```
index=* sourcetype="automox:console:events" | stats count by name
```

**Troubleshooting**

See the following troubleshooting topics.

**Logs**

To troubleshoot any issues, particularly with the Technology Add-On, it is helpful to collect and review the logs from both the Splunk environment as well as the add-on logs.

If you are pulling the logs from the Splunk host directly, they are usually located here: 

```
/var/log/splunk/
```

The most useful logs to review are:

- `ta_automox_add_on_for_splunk_automox_endpoint_import.log`
- `ta_automox_add_on_for_splunk_automox_event_import.log`
- `ta_automox_add_on_for_splunk_automox_policy_details_import.log`
- `splunkd.log`

Each of these log files correlate to the respective input as well as the splunkd.log file used for troubleshooting any larger environment related issues.

It is also possible to query directly within the Splunk interface for logs resulting from the add-on.

- Navigate to Search & Reporting and search for:

  ```
  index="_internal" sourcetype="taautomoxaddonforsplunk:log"
  ```

This provides events from the Automox Technology Add-On for use in diagnostics as well as troubleshooting. These events show the number of events, endpoints, and policies imported when inputs are run as well as ERROR messages related to issues.

**Changing Log Level**

In the scenario that more granular logging is requested, it is possible to change the log level of the add-on by following these steps:

1. Navigate to Automox Add-On for Splunk from the Apps drop-down menu.
2. Select the **Configuration** tab.
3. Within the configuration, select the “Logging” tab
4. Change the log level from the default of **INFO** to **DEBUG**.

It is also possible to change the log level to ensure only ERROR or CRITICAL logs are emitted to reduce the amount of logging from the add-on.

**No Data is Populated in the Automox Dashboard**

This issue is usually related to one of three things:

1. The Technology Add-On hasn’t been installed or configured yet.
2. The index where events are pulled is not the same as what was configured in the Technology Add-On inputs.
3. Events of the specific dashboard were from an earlier time interval (default: Today).

Perform an initial search within Splunk to ensure that events have been imported. Check that you are searching across the correct index. Then increase the time period to include a larger time frame from when the app was installed and configured:

![Splunk interface](image)

The following example search query can be used:

```
index=automox source=automox_*
```

If no events are found with a search, then ensure the inputs are properly configured and review the logs from the Technology Add-On.