Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Verify that you have added intelligence successfully to Splunk Enterprise Security

Generated: 6/13/2022 9:46 am

Verify that you have added intelligence successfully to Splunk Enterprise Security

After you add new intelligence sources or configure included intelligence sources, verify that the intelligence is being parsed successfully and that threat indicators are being added to the threat intelligence KV Store collections. The modular input responsible for parsing intelligence runs every 12 hours.

Verify that the intelligence source is being downloaded

This verification procedure is relevant only for URL-based sources and TAXII feeds.

1. From the Enterprise Security menu bar, select **Audit > Threat Intelligence Audit**.
2. Find the intelligence source and confirm that the **download_status** column states **threat list downloaded**. For TAXII feeds, the UI states **Retrieved document from TAXII feed**.
3. Review the **Intelligence Audit Events** to see if there are errors associated with the lookup name.

If the download fails, attempt the download directly from the terminal of the Splunk server using a curl or wget utility. If the intelligence source can be successfully downloaded using one of these utilities, but is not being downloaded successfully in Splunk Enterprise Security, ask your system administrator whether you need to specify a custom user-agent string to bypass network security controls in your environment. See step 12 in Add a URL-based threat source.

Verify that threat indicators exist in the threat collections

For threat intelligence sources, verify that the threat intelligence was successfully parsed and threat indicators exist in the threat collections.

1. Select **Security Intelligence > Threat Intelligence > Threat Artifacts**.
2. Search for the threat source name in the **Intel Source ID** field.
3. Confirm that threat indicators exist for the threat source.

Troubleshoot parsing errors

Review the following log files to troubleshoot errors that can occur when parsing intelligence sources in order to add them to Enterprise Security.

Problem	Suggestion
Issues related to downloading intelligence sources.	Look at the Intelligence Audit Events panel on the Threat Intelligence Audit dashboard. Look for events from the `threatlist.log` file with the `threatintel:download` sourcetype.
Issues related to parsing or processing.	Look at the Intelligence Audit Events panel on the Threat Intelligence Audit dashboard. Look for events from the `threat_intelligence_manager.log` file with the `threatintel:manager` sourcetype.
Errors result from uploading a file.	Review the `threat_intel_file_upload_rest_handler.log` file.
Other parsing errors.	Verify that the modular inputs are running as expected. See `python_modular_input.log` for errors associated with modular input failures.

Troubleshoot FSISAC threat sources

If you are having trouble with your FSISAC threat source, it appears to be stuck, and you're seeing the following in your traceback log:

```
2020-06-03 18:36:12,461+0000 INFO pid=6580 tid=MainThread file=threatlist.py:download_taxii:361 |
status="TAXII feed polling starting" stanza="FS_TEST"
2020-06-03 18:36:12,516+0000 INFO pid=6580 tid=MainThread file=__init__.py:_poll_taxii_11:49 | Certificate
information incomplete - falling back to AUTH_BASIC.
2020-06-03 18:36:12,516+0000 INFO pid=6580 tid=MainThread file=__init__.py:_poll_taxii_11:68 | Auth Type:
AUTH_BASIC
```

It could be due to a bug in libtaxii that requires version 1.1.113 or higher to support the vendor's requirement of including the Server Name Indication System (SNI). Libtaxii 1.1.113.x is only available in versions of Enterprise Security 6.x and higher.