SailPoint Non-Employee Risk Management AuditEvent Add-on: FAQ

General Overview

This document provides answers to frequently asked questions about SailPoint Non-Employee Risk Management AuditEvent Add-on built using the Splunk Add-on Builder, designed to integrate with SailPoint's NERM API. This add-on enables seamless ingestion of NERM Audit events into Splunk for monitoring, reporting, and analysis.

1. General Questions

1.1 What does SailPoint Non-Employee Risk Management AuditEvent Add-on do?

The SailPoint Non-Employee Risk Management AuditEvent Add-on is an open-source Splunk add-on built using the Splunk Add-on builder. This add-on helps ingest, parse and normalize data from Non-Employee Risk Management (NERM) API into Splunk allowing users to easily search and analyze their data. It leverages Splunk's data onboarding framework providing a seamless experience for integrating data into Splunk Enterprise and Splunk Cloud.

1.2 Is this add-on free to use?

Yes, it is open-source and free to use. The source code is publicly available, and users are encouraged to contribute improvements or report issues.

1.3 Where can I download the add-on?

The add-on is available on:
GitHub (TBD: OSS repository link to be provided)

1.4 What version of Splunk is required?

The add-on supports:

- Splunk Enterprise version 9.x and above.
- Compatibility with Splunk Cloud.

1.5 Which API endpoints are supported?

The add-on supports ***/audit_events/query*** SailPoint NERM API endpoints

1.6 Can this add-on be used with Splunk Cloud?

Yes, the add-on is designed to work with both Splunk Cloud and Splunk Enterprise environments. For more details, please refer README.md file

2. Installation and Setup

2.1 How do I install the add-on?

- Log in to your Splunk instance
- Navigate to **Apps> Manage Apps**
- Click on **Install app from file**
- Upload the.tar.gz file from **/build** directory
- Click **Upload** and restart Splunk if prompted
- Find **SailPoint Non-Employee Risk Management AuditEvent Add-on** from the list and click **Launch App**

For more details, please refer to **Installation section** from README.

2.2 What permissions are required to configure the add-on?

This is an open-source add-on hence there are no specific permission to configure the add-on.

For more details, please refer to **Configuration** section from README**.**

2.3 What inputs need to be configured?

Please refer to **Configuration** section from README.md**.**

3. Data Collection and Troubleshooting

3.1 How is data collected from SailPoint?

The add-on uses custom python script which calls SailPoint's NERM audit event endpoint to fetch data at specified intervals. The data is indexed into Splunk for further processing.

3.2 What are the supported authentication methods?

The add-on supports:

- OAuth 2.0 (preferred for security).

For more details on authentication, please refer to **Authentication** section from README.

3.3 What type of data can it handle?

JSON/structured event data

3.4 How often does the add-on poll data?

Polling intervals are configurable. Typical recommended interval is 300secs(5minutes). It can be set depending on use case and data source limitations.

3.5 How do I troubleshoot missing data?

Check API connectivity: Ensure the SailPoint API is accessible from the Splunk environment.

- Verify API credentials: Ensure the credentials have sufficient permissions.
- Inspect logs: Review the Splunk internal logs (index=_internal) for error messages related to the add-on.
- Increase logging level: Enable debug mode in the add-on settings for more detailed error information.

- Check Splunk internal logs(index=_internal) for any errors related to the add-on

3.6 How can I enable debug logs for the add-on?

→ Navigate to add-on setting
→Increase the logging level to DEBUG.
→Review logs in index=_internal or the Splunk var/log/splunk directory.

3.7 What are the rate limits for the API?

Rate limits is still not in place for NERM audit event endpoint. Check with SailPoint documentation or your administrator to understand the limits and adjust the polling interval accordingly.

3.8 Why is data not appearing in Splunk?

→ Ensure the data source is operational and accessible
→ Verify API credentials
→ Confirm that data input is enabled and scheduled correctly

3.9 I am getting a SSLCertVerificationError. How can I resolve this?

SSLCertVerificationError comes up for one of the two reasons - if the certificate is not placed in right directory or if it is a self-signed certificate. Please navigate to following file to add CA certs in the chain: > SPLUNK_HOME/etc/apps/TA-sailpoint-non-employee-risk-management-auditevent-add-on/bin/ta_sailpoint_non_employee_risk_management_auditevent_add_on/aob_py3/certifi/cacert.pem

3.10: Can we override default host value?

Yes, the default host value can be overridden. To set the default value of the host field, you can use Splunk Web or edit the inputs.conf configuration file. Please refer to

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/SetadefaulthostforaSplunkserver for detail steps.

NOTE: Changing default host name on Splunk Cloud is not allowed. Instead, one can assign host names based on inputs, sources, and source types. Finding data from a specific device is available only on Splunk Enterprise.

3.11 I see some of the incoming events are getting truncated. How do I resolve this?

If you are seeing events being truncated (regularly seeing "truncating" in splunkd.log) then increasing the value of TRUNCATE for that sourcetype can help reduce the number of truncations. The new value for TRUNCATE should be a little higher than the longest message you've seen truncated in splunkd.log. Please refer to https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Propsconf for more details.

4. Performance and Best Practices

4.1 How do I optimize performance?

•**Set appropriate intervals:** Avoid overly frequent polling to prevent API throttling and Splunk indexing delays.

•**Filter data:** Use may use query parameters to fetch only necessary data, reducing the load on the API and Splunk.

•**Monitor input health:** Use Splunk's Monitoring Console to track the performance of data ingestion.

4.2 Can I customize the add-on?

Yes, the add-on is open-source, and you can:

- Modify or add data inputs.
- Use Splunk's add-on builder to include additional data extraction and parsing logic

4.3 Can I customize field extraction logic?

Yes, you can:

- Update or add Field Extractions using regular expressions(regex) or custom scripts.
- Update the Splunk Web UI to modify knowledge objects such as source types, field extractions and lookups.

5. Security

5.1 How is data secured during transmission?

The add-on uses HTTPS for secure communication between Splunk and the SailPoint API.

5.2 How are API credentials stored?

API credentials are encrypted and stored securely in Splunk's credential storage system.

5.3 Are there any known vulnerabilities?

As of the latest release, there are no reported vulnerabilities. Ensure you keep the add-on updated to receive security patches.

Ensure that add-on is configured in accordance with organizational security policies.

6. Limitations

6.1 What data is not supported by the add-on?

- Real-time data streaming is not supported; only periodic polling is available.
- Rate-limit is not supported currently

6.2 Is there a limit on the amount of data that can be ingested?

The amount of data is subject to:
- Splunk index storage limits.

7. Support

7.1 How can I report an issue?

For issues related to the add-on:

- Submit a ticket (TBD: Support alias)