User Guide

ObserveIT App and Add-On for Splunk

Version 1.2.0 – January 2019

ObserveIT App and Add-On for Splunk User Guide

observe it

Table of Contents

ObserveIT Introduction

Your biggest asset is also your biggest risk. Whether it is trusted third parties, privileged users, or business users, insiders present a massive risk to organizations because they have been given access to critical applications, systems and data to do their jobs. With over 1,700 global customers across all major verticals, ObserveIT is the only insider threat management solution that empowers security teams to detect insider threats, streamline the investigation process, and prevent data exfiltration.

ObserveIT's software agents monitor and capture key data about insider threats. ObserveIT records user sessions (including screen, mouse, and keyboard activity, as well as local and remote logins) and transmits captured data to the application server in real time.

To learn more, please visit https://www.observeit.com/product/highlights/

Overview and Features

- TA-ObserveIT: The ObserveIT technology add-on for Splunk provides security analysts and investigation teams with powerful user activity meta-data and smart user behavior alerts. It connects Splunk to the ObserveIT REST API to continuously pull the latest user activity and alert events from ObserveIT into Splunk. By correlating this user context with your other data sources in Splunk, a complete picture a user's activity will emerge, allowing for creation of smarter alerts and quicker threat elimination.
    - Subscribe to User Activity and/or Alert events
    - Poll events from multiple ObserveIT instances

- ObserveIT App: The ObserveIT app for Splunk will leverages the data collected by TA-ObserveIT to provide full-featured User Activity and Alert dashboards. Direct session-playback links for each session from Splunk to the ObserveIT console brings instant deep analysis of user behavior to Splunk.
    - Detailed summary of user sessions and alerts. Drill down into individual user activities.
    - Charts to highlight risky users and applications
    - Direct link to Session Player from all user activities and alerts

Prerequisites

TA-ObserveIT and ObserveIT app for Splunk should be downloaded and installed from Splunkbase.

Minimum supported ObserveIT version is 7.6.2

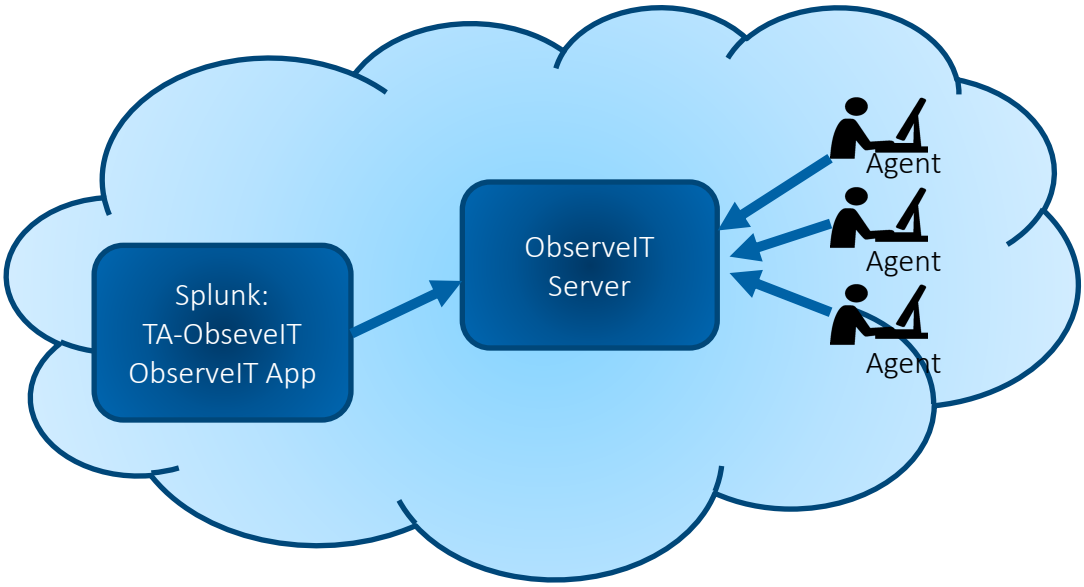
Minimum supported Splunk version is 6.5

TA-ObserveIT will need to be able to communicate to your ObserveIT API, typically on port 443.

Deployment Architecture

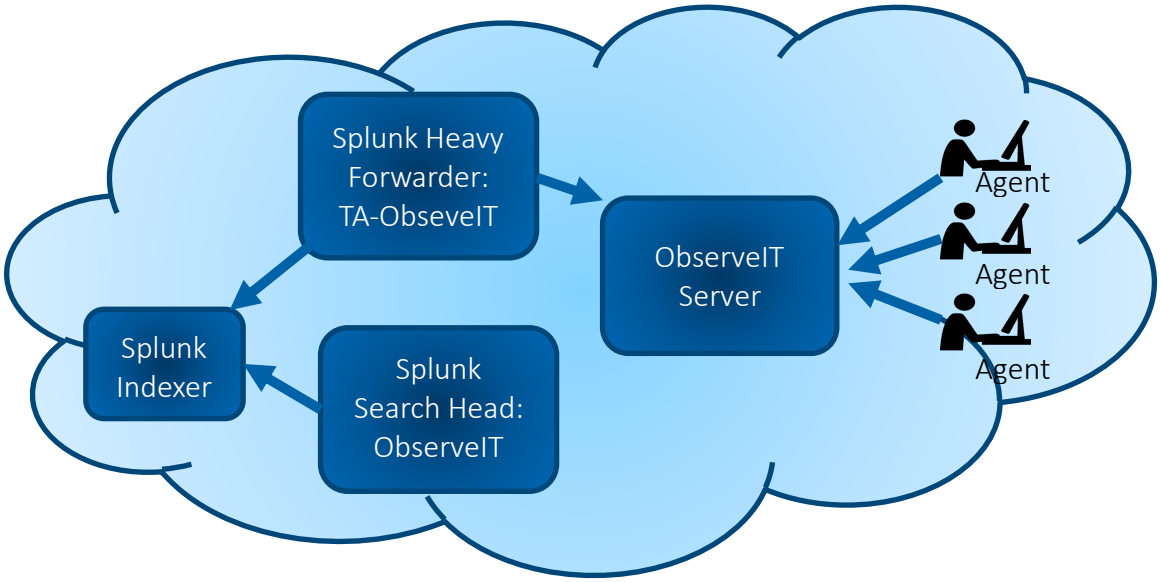
SINGLE-INSTANCE SPLUNK ENTERPRISE

Splunk is a simple non-distributed deployment on the same network as ObserveIT. TA-ObserveIT and ObserveIT App will be installed on the same node



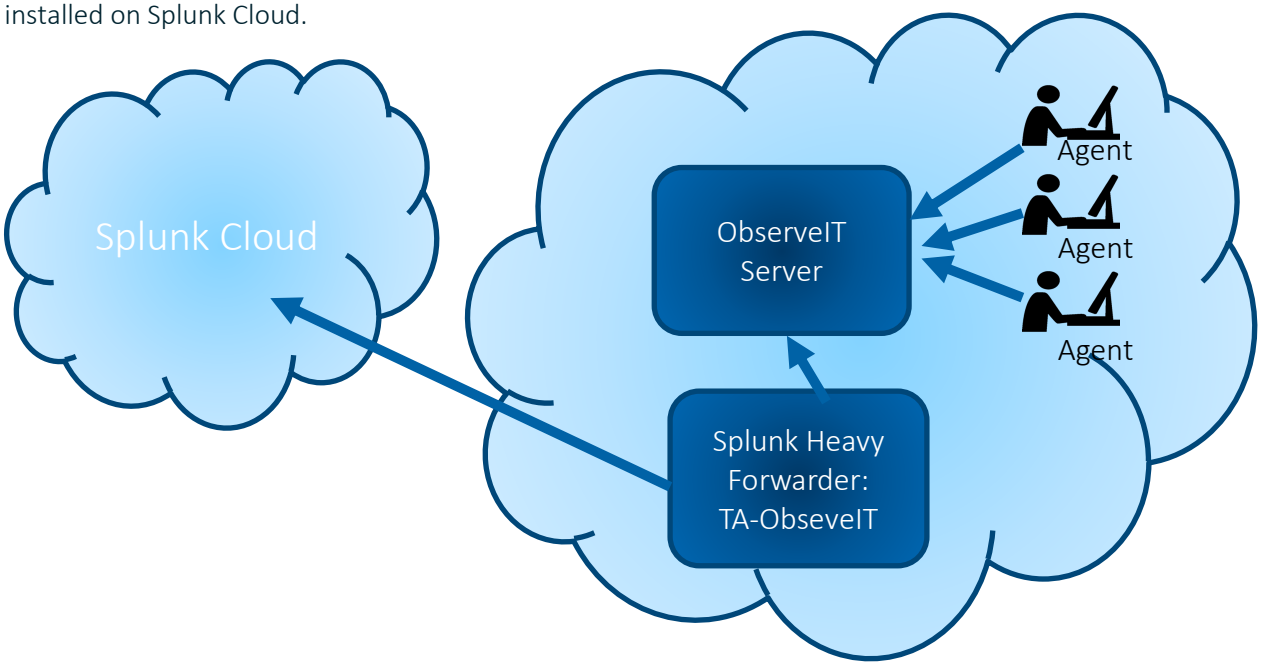
DISTRIBUTED SPLUNK ENTERPRISE

Splunk is a distributed deployment on the same network as ObserveIT. TA-ObserveIT is installed on a heavy forwarder. Installation of TA-ObserveIT on a Universal Forwarder or SHC is not supported. The ObserveIT app is installed on the search heads.



SPLUNK CLOUD

Splunk cloud is used to store and search for ObserveIT data. TA-ObserveIT is installed on a heavy forwarder on the same network as ObserveIT to forward the data to Splunk Cloud. The ObserveIT app is installed on Splunk Cloud.



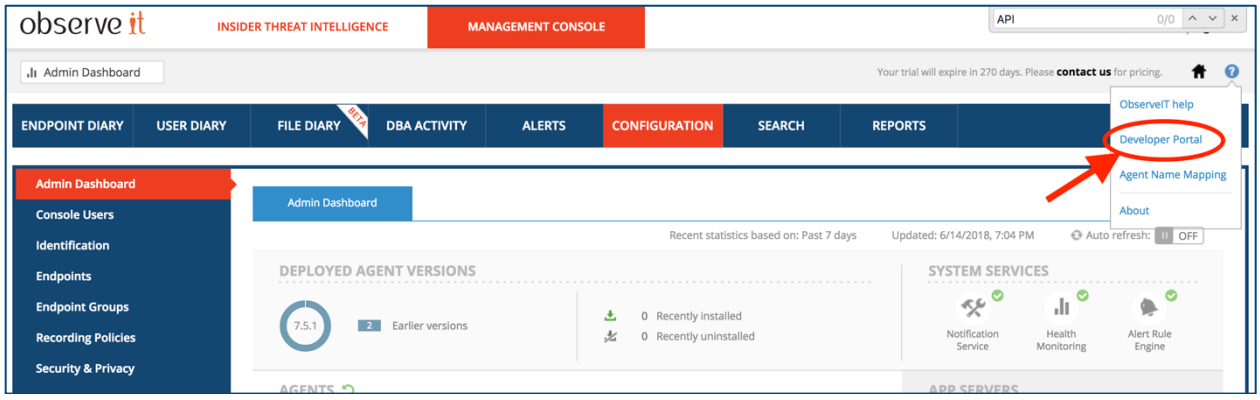
Configuration

The TA-ObserveIT app must be configured to reach the ObserveIT REST API and retrieve report data.

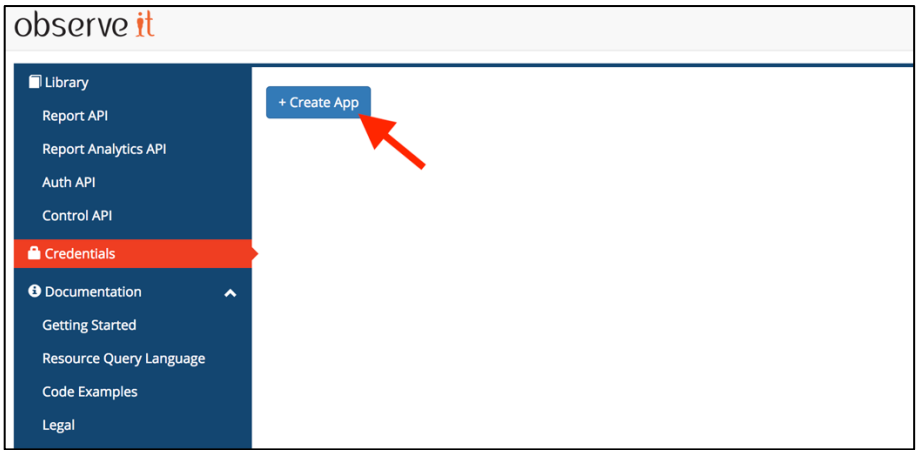
CREATE APPLICATION IN OBSERVEIT

The ObserveIT REST API uses OAUTH2 for authentication. In order to authenticate with ObserveIT, we will need to register a Splunk application with ObserveIT.

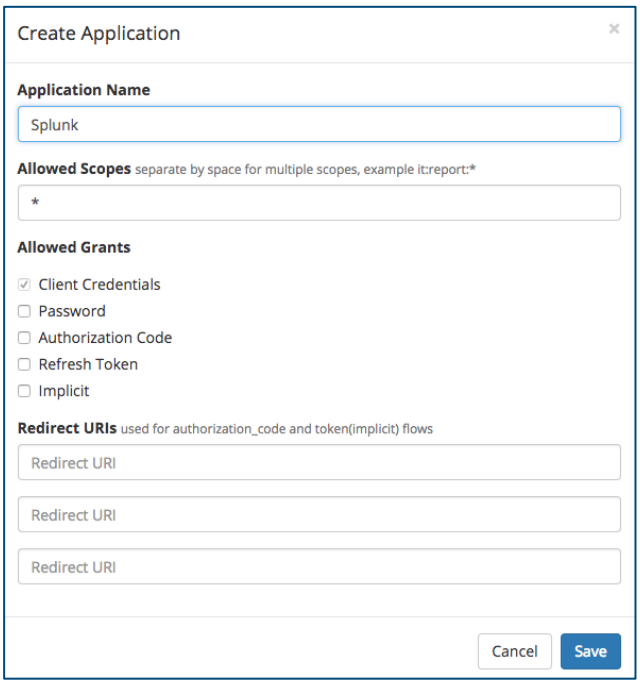
1. In your browser, navigate to the API portal from the ObserveIT console. Note that the API portal may not be installed by default, in which case you will be prompted to install it with instructions. If the API portal screen fails to properly load, log out of the ObserveIT console and log back in with a local system account rather than an LDAP account and try again.



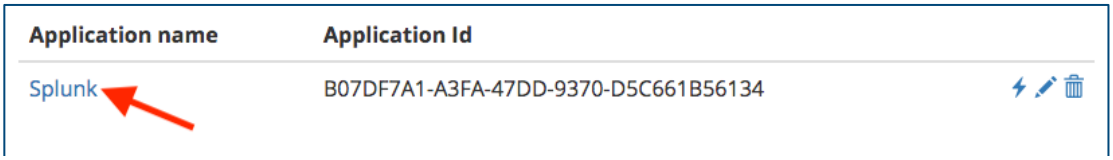
2. On the left panel, select “Credentials”, then click the “Create App” button.



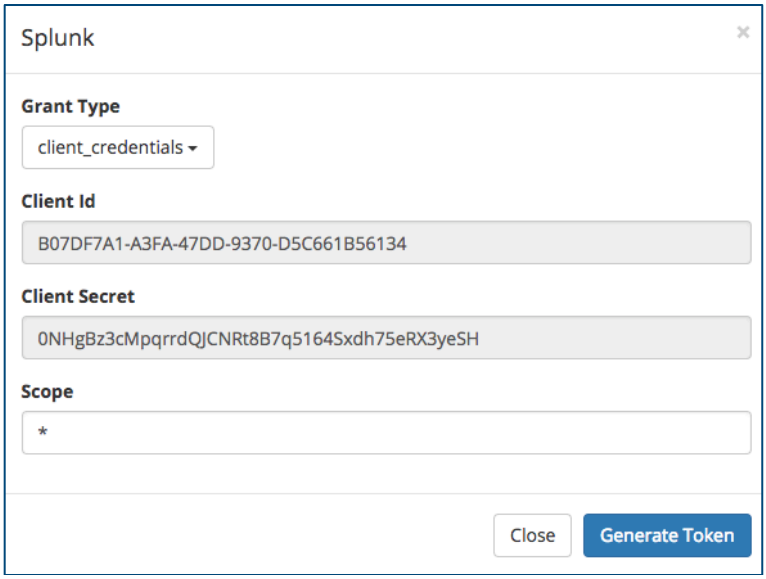
3. Give the application a reasonable name, like “Splunk” so that you will know its purpose.
   For allowed grants, check only Client Credentials.
   Click Save.



4. Click the name of the application you just created.



5. Copy the "Client Id" and "Client Secret" values so that we can enter it into the configuration screen of the Splunk-add-on.

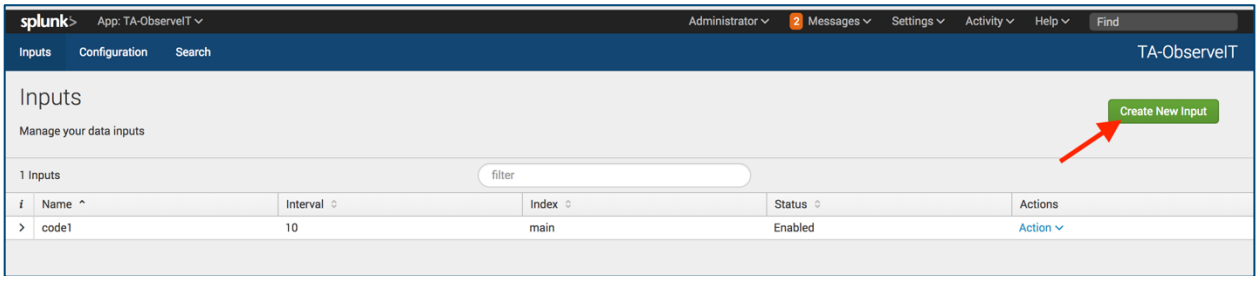


6. Repeat this procedure for all ObserveIT instances you want Splunk to access

CONFIGURE OBSERVEIT TA FOR SPLUNK

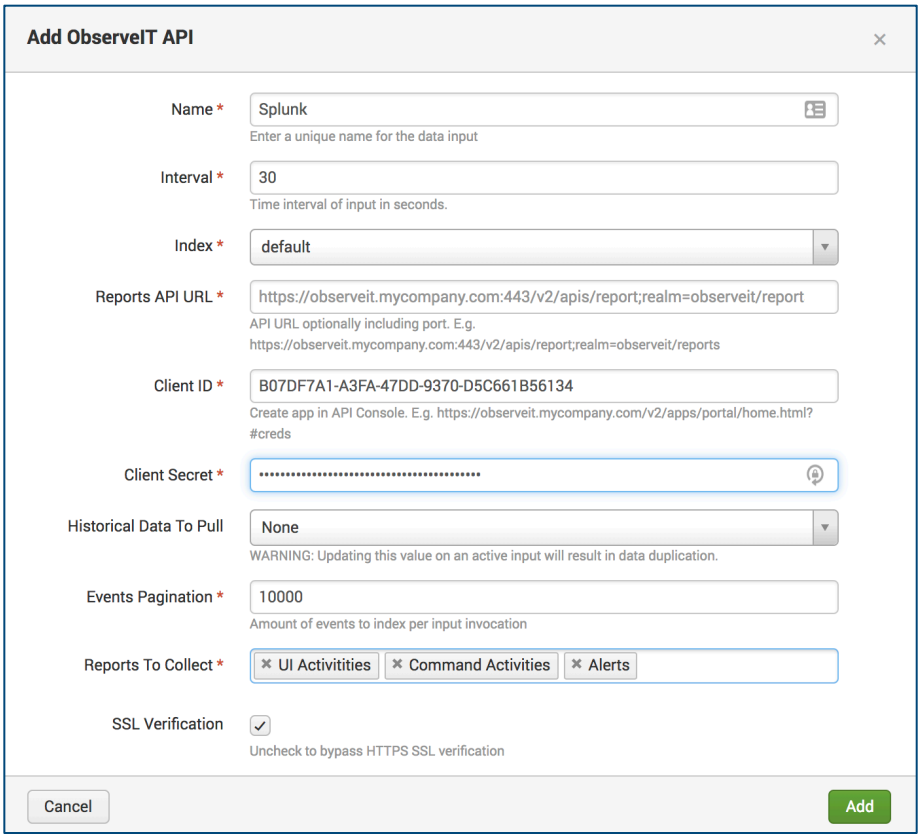
Your ObserveIT instance(s) need to be registered in the Splunk TA. The access token generated above will be used to authenticate with the API. If you would like to store ObserveIT events in their own index, create it on the indexers before following these configuration steps.

1. Open the TA-ObserveIT app in Splunk and click on "Create New Input".



2. Enter a unique name that represents the ObserveIT instance, such as the hostname
Input reasonable values for the interval and events pagination fields. Make sure that their combination is sufficient to ingest your anticipated event rate.
The Client ID and Client Secret will be the values that were copied when the application was created in ObserveIT.
The Reports API URL should be formatted like:
https://<hostname>:<port> /v2/apis/report;realm=observeit/reports
If your ObserveIT instance is using a self-signed certificate and you are unable to assign it a real one, then you will need to uncheck the SSL Verification box. Note that this is a less secure option and should not be used in production.
If you would like to read in existing events on your system, the select a time period to go back under "Historical Data To Pull". Selecting None for this field means only new events will be loaded.

There are 3 available reports to collect. Choose the ones you want to load in Splunk:
UI Activities: User interface activity events from Windows or Mac agents
Command Activities: Commands run on UNIX agents
Alerts: Alert events from all agents



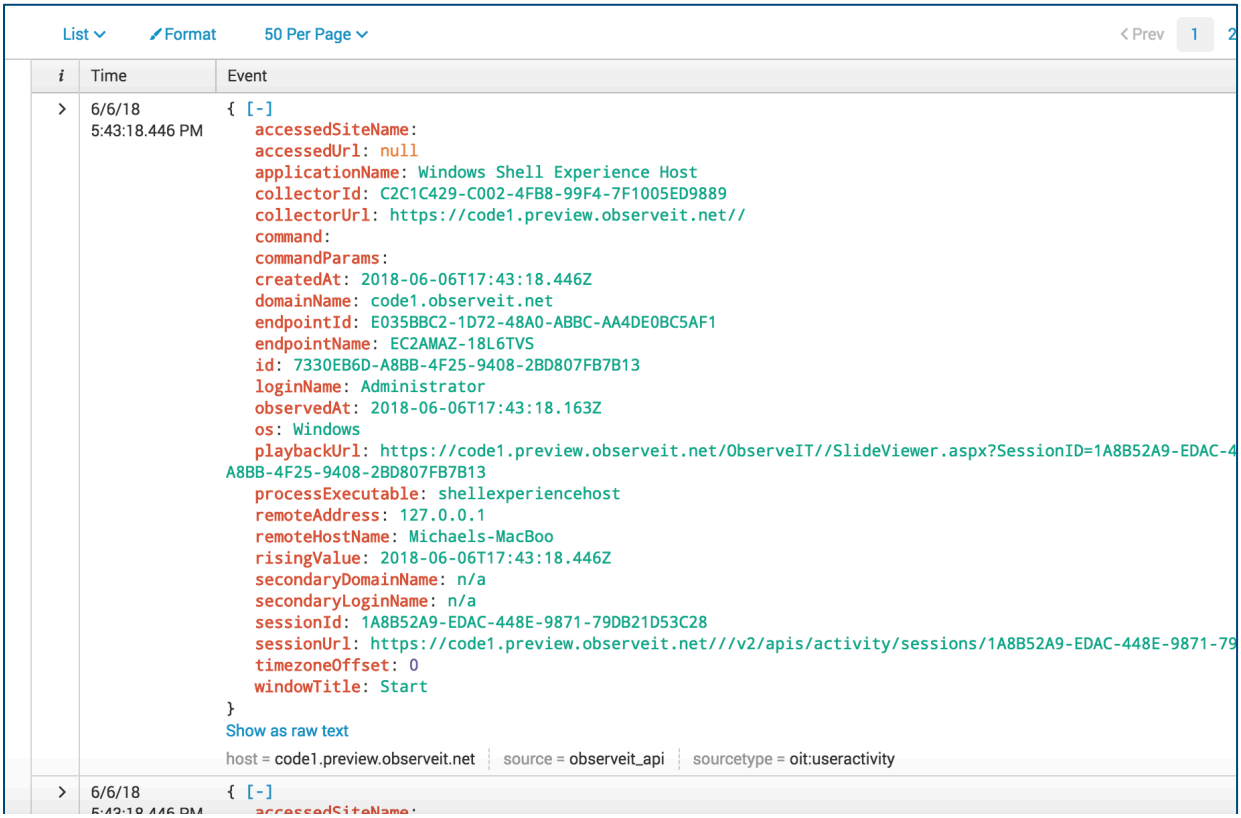
UPGRADING

When upgrading from a previous version of the ObserveIT TA, you will need to edit any existing inputs for them to remain functional. Due to changes in the underlying ObserveIT API, you will need to reconfigure the “Reports to Collect”, “Client ID”, and “Client Secrets” fields. The other fields, such as “Reports API URL” do not need to be changed.

Usage

VIEWING EVENTS

Once your ObserveIT data collection is configured and enabled in the TA settings, you should start seeing events logged. You can start using the data in Splunk searches and reports.



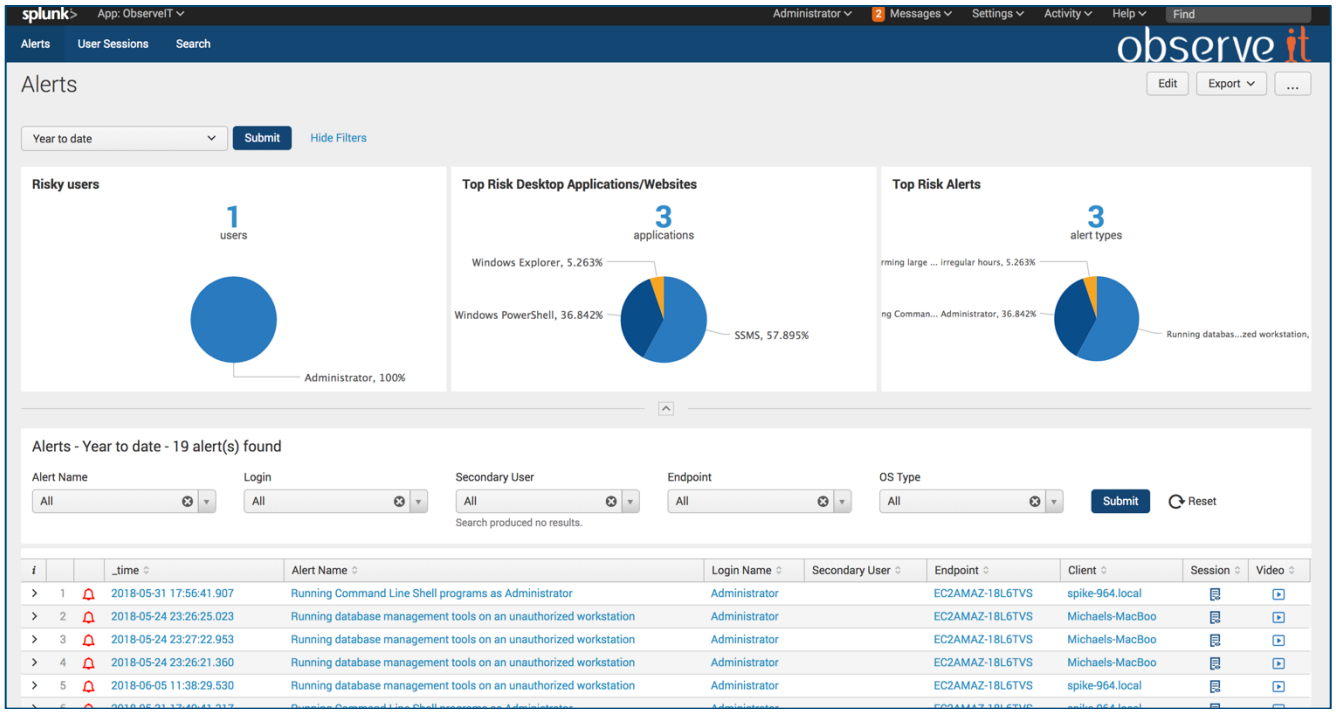
DASHBOARDS

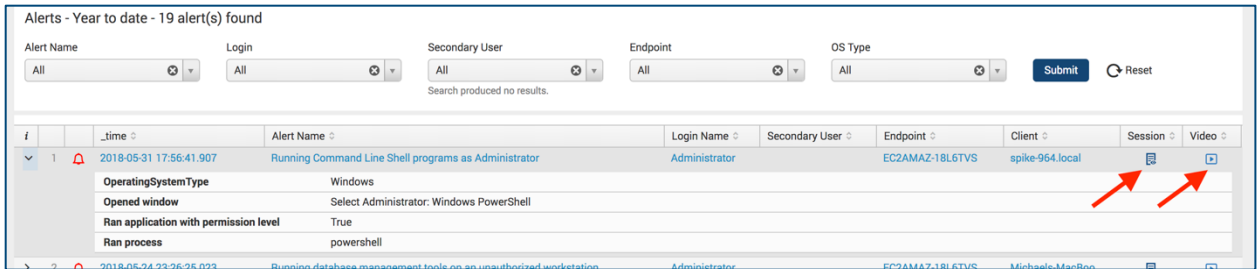
The ObserveIT app provides a comprehensive dashboard to view summary information about risky users and applications as well as drill downs and links to view recorded user sessions. Installation of TA-ObserveIT is a prerequisite for using the ObserveIT app.

Alerts Dashboard

The alerts dashboard shows the top alerts and top risky users and applications. All alerts are listed, with a link to launch the ObserveIT player to play back the user's session. The session column lets you drill down to the individual activities that made up the alerted session.

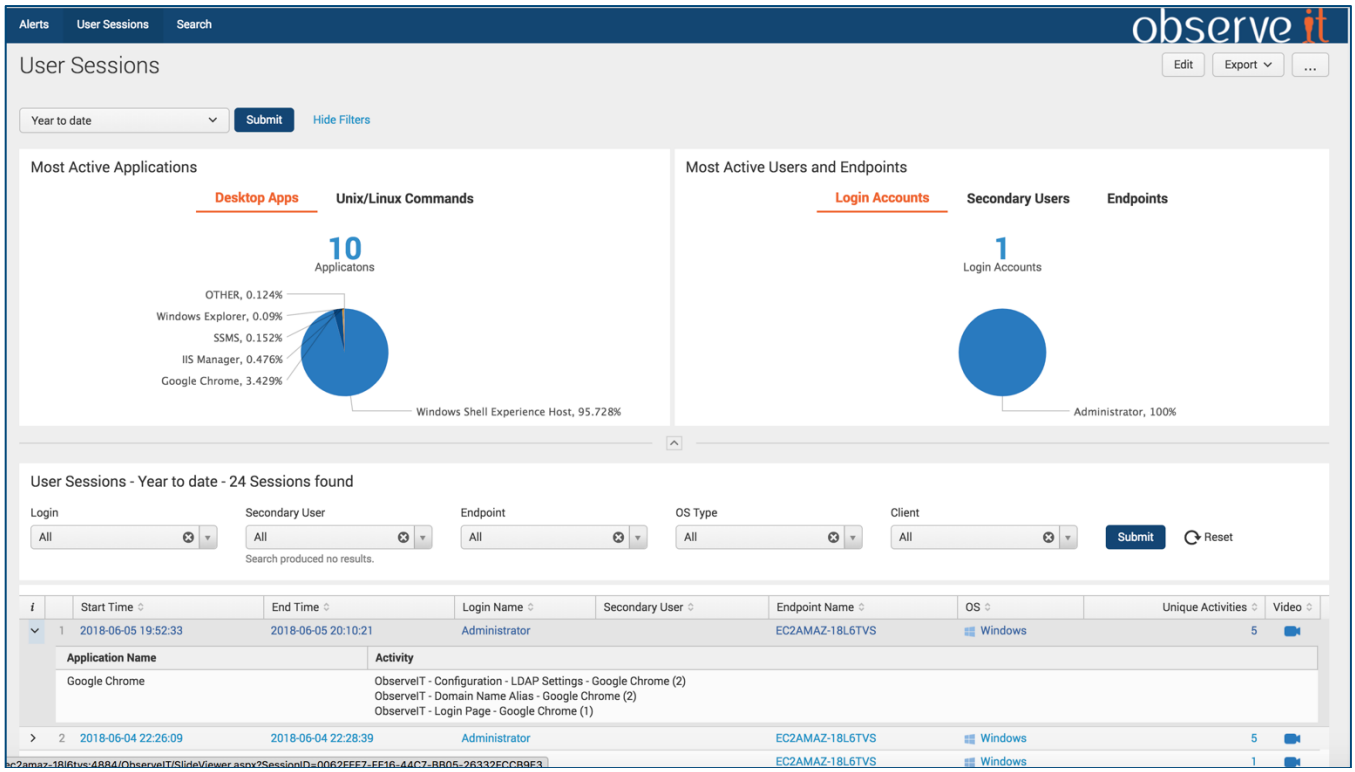
> ***TIP:*** *If only the alerts list is desired, the horizontal collapse bar below the pie charts can be clicked to hide them from view.*





User Session Dashboard

The user session dashboard shows the most active users and endpoints as well as the most used applications. A summarized view of each user session is available, including the start and end time of the session, the number of unique activities, and the user involved. A link to the ObserveIT player to replay the session is also included. A drilldown will show more details about the individual activities that make up the session. When the user session dashboard is opened via alert drill-down, you will see only that individual single session's activities.



Troubleshooting

If you have configured TA-ObserveIT and aren't seeing events flowing into the system, you should check the internal logs for any error messages.

In the splunk console, search ta_observeit_observeit_api.log for non-INFO messages:
index=_internal sourcetype="ta:observeit:log" NOT "INFO"

Support

For additional support configuring or using the ObserveIT Add-On for Splunk, please contact us at integrations@observeit.com
For help using the ObserveIT platform, please contact the ObserveIT support organization.
https://www.observeit.com/support/

Not a customer yet? Start your Free Trial of ObserveIT today!

Free Trial
Start your free trial with ObserveIT today. Detect and prevent insider threats in minutes. Reduce your risk, speed up investigations, and streamline compliance.

Download Trial License
Download Your Trial License

Request a Demo
Request a demo of ObserveIT user activity monitoring solution. An ObserveIT representative will be in touch soon to schedule a live demo.

Request Pricing
Want a price quote for ObserveIT in your environment? Simply fill out the form and a specialist will contact you shortly.

Release notes

Version	Date	Notes

1.0.0	2018-06-25	• Initial Release
		• New:
		  ○ ObserveIT Alerts and User Activities events in Splunk
		  ○ Summary Dashboard with links to session viewer
		• Fixed:
		• Improved:

1.2.0	2018-10-10	• New:
		  ○ "UI Activities" and "Command Activities" reports replace the previous "User Activities" report
		• Fixed:
		• Improved:
		  ○ Ease of configuration for polling historical data
		  ○ No longer need to generate a long-life token