observe IT
a proofpoint® company

Splunk Integration Guide

Contents

Overview..1

FEATURES...1
PREREQUISITES 1
DEPLOYMENT ARCHITECTURE 1
Single-Instance Splunk Enterprise Deployment..*1*
Distributed Splunk Enterprise Deployment *2*
Splunk Cloud Deployment *3*

Configuration 3

CREATING APPLICATION IN OBSERVEIT...3
CONFIGURING OBSERVEIT TA FOR SPLUNK...6

Usage...9

VIEWING EVENTS 9
DASHBOARDS..10
Alerts Dashboard *10*
User Sessions Dashboard *11*
File Activity Dashboard *12*

Troubleshooting...13

Support..13

Release notes.. **Error! Bookmark not defined.**

observe IT
a proofpoint® company

Overview

This document describes the integration of ObserveIT with Splunk software.

Features

ObserveIT includes the following to collect and manage the data:

- ObserveIT Technology Add-on (ObserveIT TA): Connects Splunk to the ObserveIT RESTful API to continuously pull the latest user activity and alert events. ObserveIT TA pulls data from ObserveIT into Splunk as follows:
    - Subscribes to User Activity and/or Alert events ○ Polls events from multiple ObserveIT instances

- ObserveIT App for Splunk: Leverages the data collected by ObserveIT TA to provide full-featured User Activity and Alert dashboards. Direct session-playback links for each session from Splunk to the ObserveIT console bring instant deep analysis of user behavior to Splunk and includes:
    - 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

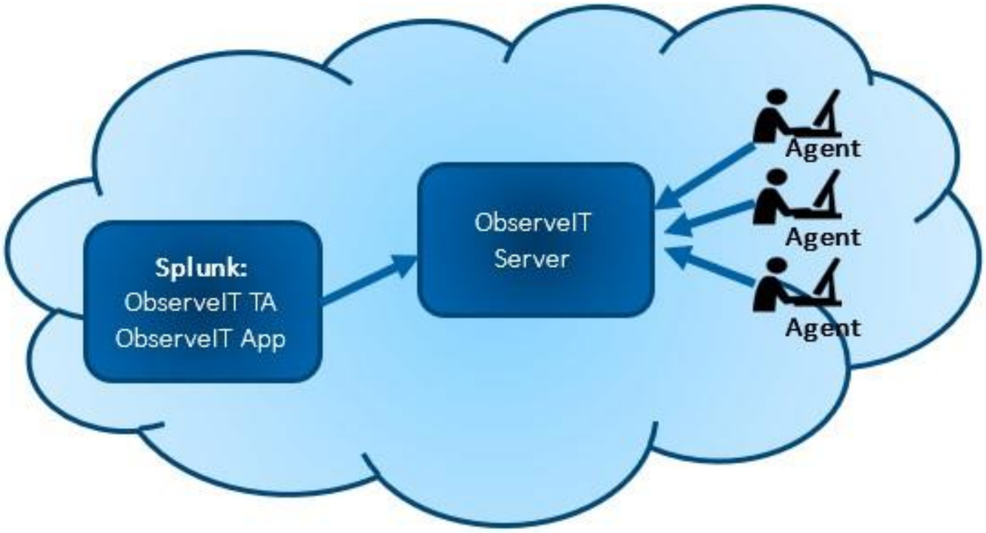
Prerequisites

- Download and install ObserveIT TA and ObserveIT App for Splunk from Splunkbase
- ObserveIT TA communicates with your ObserveIT API directly, typically on port 443
- ObserveIT (Minimum version: 7.6.2)
- Splunk (Minimum version: 6.5)

Deployment Architecture

Single-Instance Splunk Enterprise Deployment

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

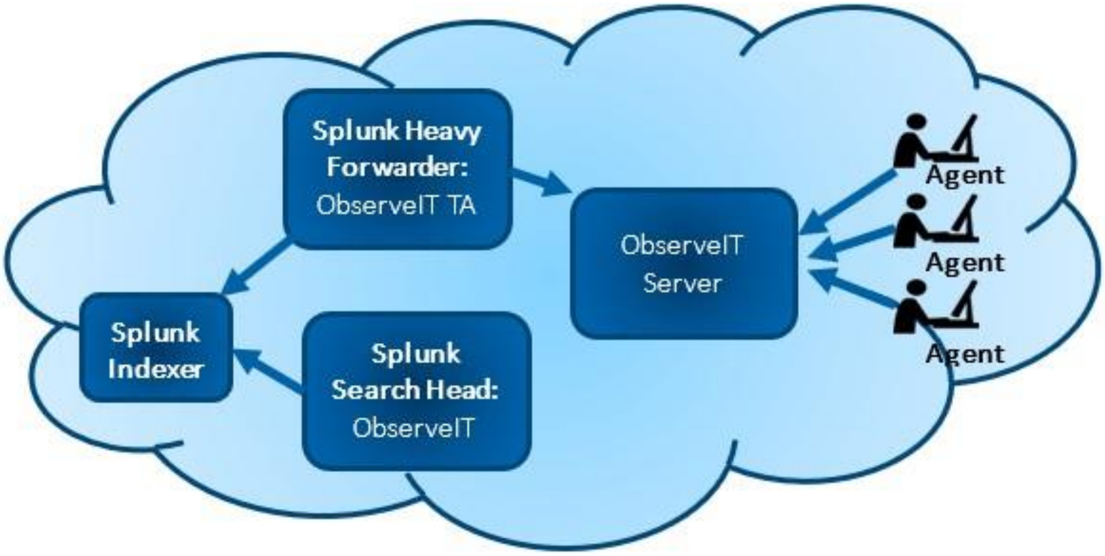


Distributed Splunk Enterprise Deployment

Splunk is a distributed deployment on the same network as ObserveIT.

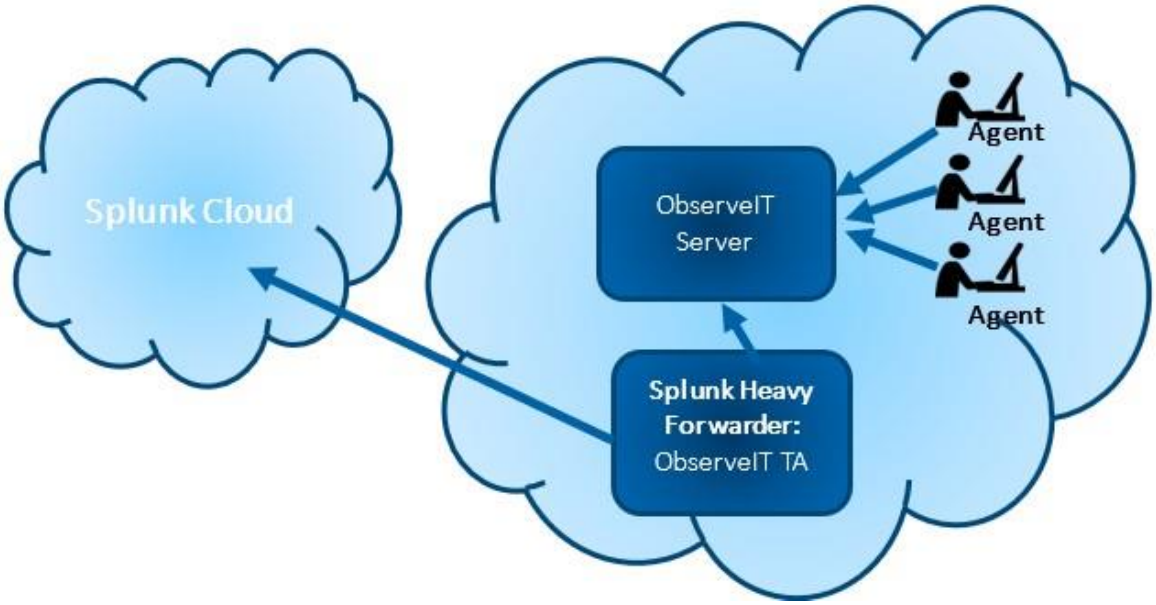
ObserveIT TA is installed on a Splunk heavy forwarder that sends data. (Installation of ObserveIT TA on a Universal Forwarder or SHC is not supported.)

The ObserveIT App is installed on the search heads that handles the search management functions.



Splunk Cloud Deployment

Splunk Cloud can be used to store and search for ObserveIT data. To forward the data to Splunk Cloud, ObserveIT TA is installed on a Splunk heavy forwarder on the same network as ObserveIT. The ObserveIT App is installed on Splunk Cloud.



Configuration

You configure ObserveIT TA to reach the ObserveIT REST API and retrieve report data.

CREATING APPLICATION IN OBSERVEIT

To integrate ObserveIT with Splunk using RESTful API, you register the application to authenticate access. Oauth2 is the method of authenticating access to the ObserveIT RESTful API.

This procedure describes how to generate a token that you use when you configure ObserveIT TA for Splunk.

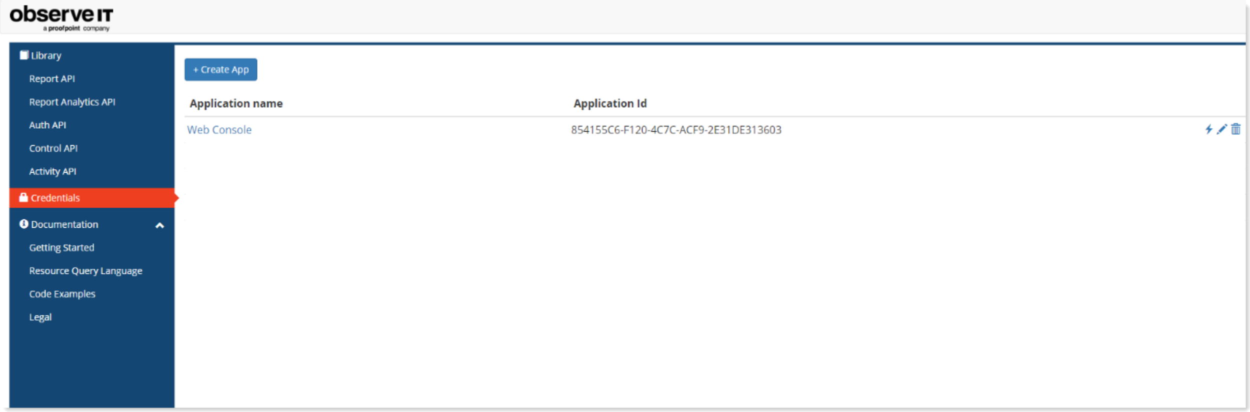
1. From the ObserveIT Web Console, click the ? in the upper-right corner and select Developer Portal from the menu.

   Notes:

   If the Developer Portal is not installed by default, you will be prompted to install it.

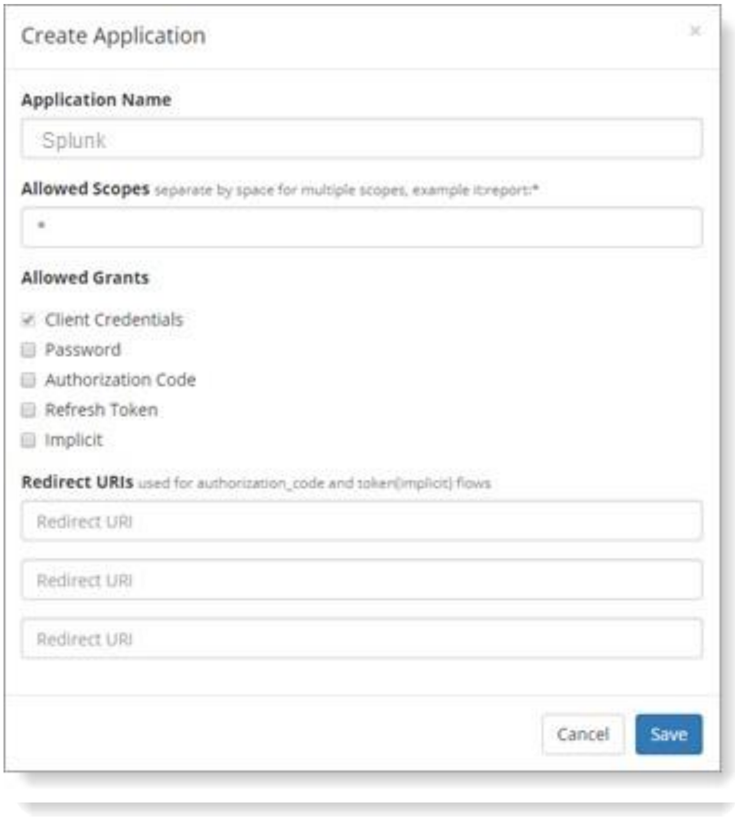
   If the Developer Portal fails to properly load, log out of the ObserveIT console and log back in with a local system account rather than an LDAP account.

2. From the Developer Portal, select Credentials and then click the Create App button.



Application name	Application Id
Web Console	854155C6-F120-4C7C-ACF9-2E31DE313603

The Create Application dialog box displays. This is where you register the application.



Create Application

Application Name

Splunk

Allowed Scopes separate by space for multiple scopes, example itreport:*

*

Allowed Grants

☑ Client Credentials
□ Password
□ Authorization Code
□ Refresh Token
□ Implicit

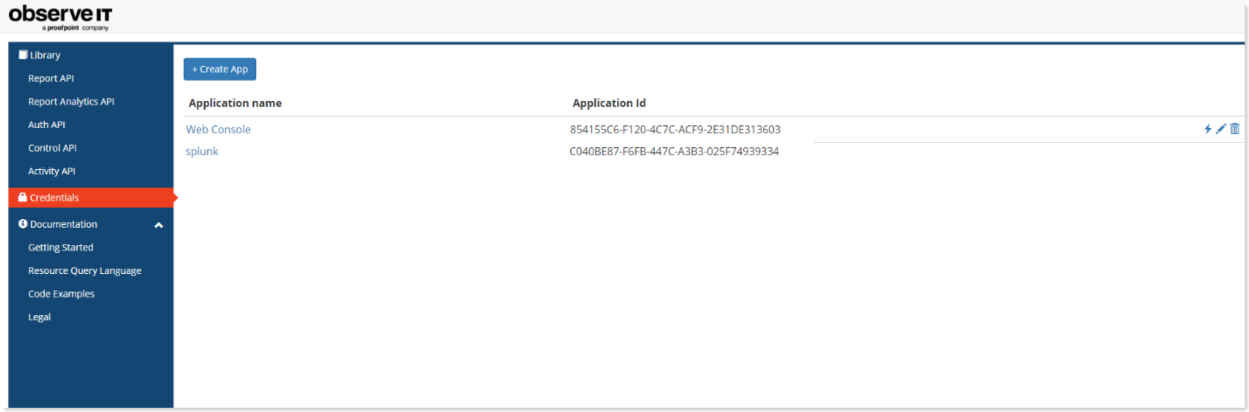
Redirect URIs used for authorization_code and token(implicit) flows

3. Do the following:

   a. In the Application Name field, enter a name. It is recommended that you choose a name you can recognize, such as Splunk, Splunk1 etc.

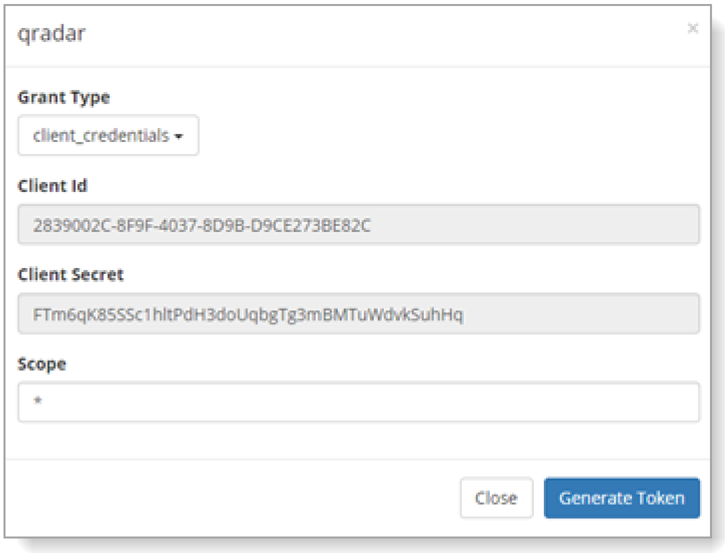
   b. In Allowed Grants, check Client Credentials.

   c. Click Save and the application is added to the list.



Application name	Application Id
Web Console	854155C6-F120-4C7C-ACF9-2E31DE313603
splunk	C040BE87-F6FB-447C-A3B3-025F74939334

4. Click the application you just created. The dialog box for generating a token displays.



Grant Type: client_credentials ▾

Client Id: 2839002C-8F9F-4037-8D9B-D9CE273BE82C

Client Secret: FTm6qK85SSc1hltPdH3doUqbgTg3mBMTuWdvkSuhHq

Scope: *

Note the Client Id and Client Secret values. You will enter them into the configuration screen of the Splunk add-on. (See: Configuring ObserveIT TA for Splunk.)

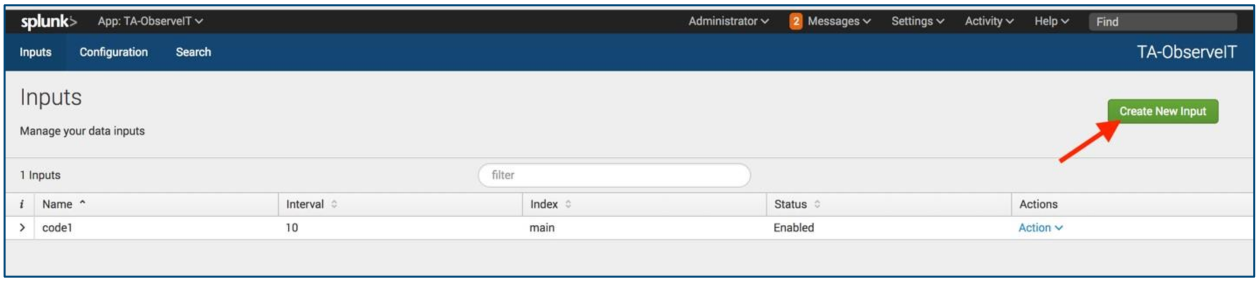
Configuring ObserveIT TA for Splunk

This procedure describes the registration process in Splunk.

Your ObserveIT instance(s) need to be registered as the Splunk Technology Add-on (TA). The access token (with the Client ID and Client Secret you generated in the ObserveIT Developer Portal will be used to authenticate with the API.

Note: If you would like to store ObserveIT events in their own index, create it on the indexer before following these configuration steps.

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



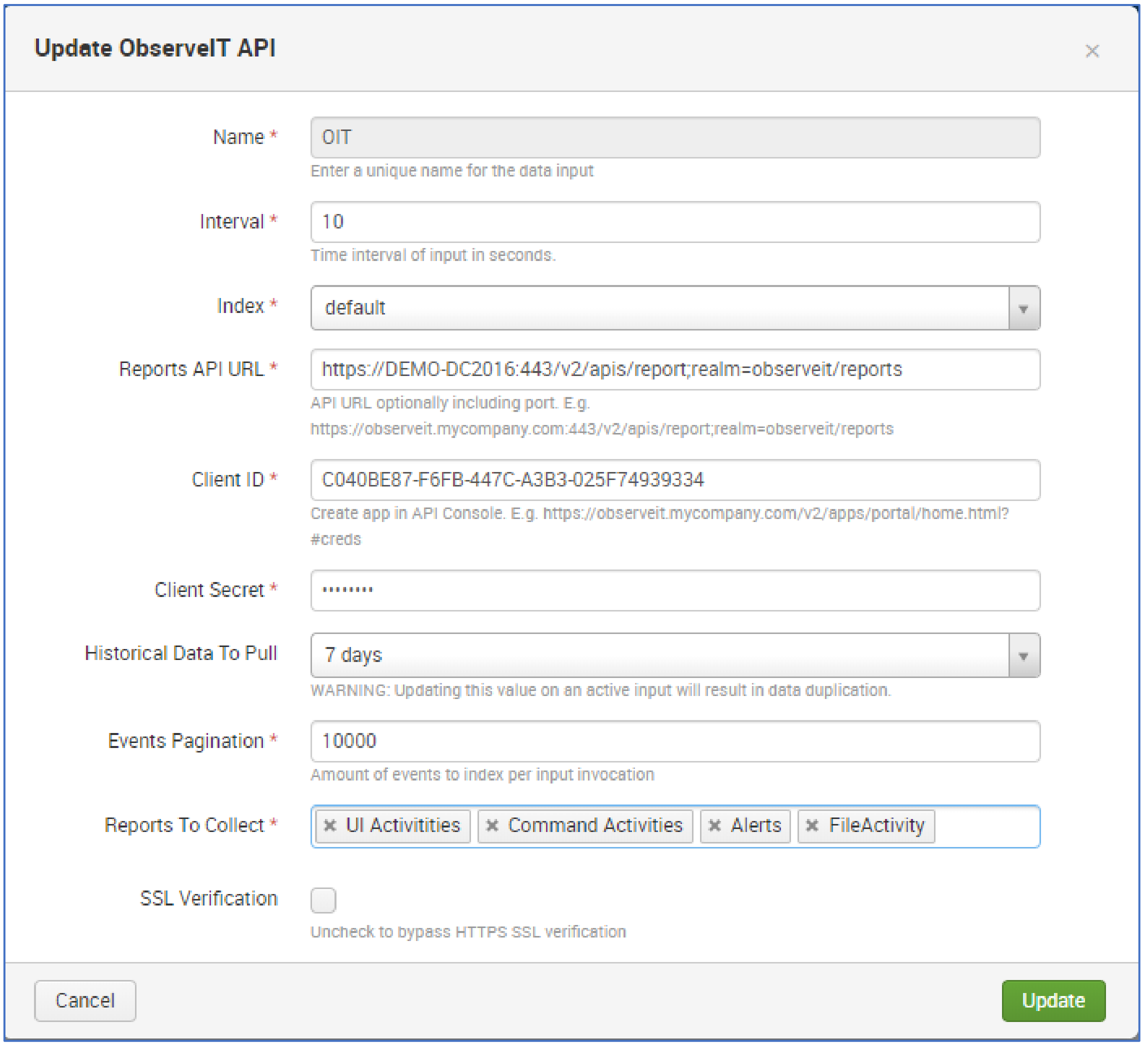
Inputs

Manage your data inputs

1 Inputs

i	Name	Interval	Index	Status	Actions
>	code1	10	main	Enabled	Action

2. Complete the Add ObserveIT API dialog box.



Update ObserveIT API

Name *	OIT Enter a unique name for the data input
Interval *	10 Time interval of input in seconds.
Index *	default
Reports API URL *	https://DEMO-DC2016:443/v2/apis/report;realm=observeit/reports API URL optionally including port. E.g. https://observeit.mycompany.com:443/v2/apis/report;realm=observeit/reports
Client ID *	C040BE87-F6FB-447C-A3B3-025F74939334 Create app in API Console. E.g. https://observeit.mycompany.com/v2/apps/portal/home.html?#creds
Client Secret *	••••••••
Historical Data To Pull	7 days WARNING: Updating this value on an active input will result in data duplication.
Events Pagination *	10000 Amount of events to index per input invocation
Reports To Collect *	× UI Activitities × Command Activities × Alerts × FileActivity
SSL Verification	☐ Uncheck to bypass HTTPS SSL verification

a. Enter a unique Name that represents the ObserveIT instance, for example use the hostname such as Splunk.

b. In the Interval and Events Pagination fields, enter values you want. Make sure that their combination is sufficient to ingest your anticipated event rate.

c. The Reports API URL is formatted as:
https://<hostname>:<port> /v2/apis/report;realm=observeit/reports

d. In the Client ID and Client Secret, enter the values you copied when the application was created in ObserveIT. (See: Creating Application in O.)

e. To include existing events on your system, in the Historical Data To Pull field, select the time period you want to go back to. Select None, if you want only new events to be loaded.

f. Select Reports to Collect.

Choose the reports 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
- FileActivity: File Activity events from all agents

Currently ObserveIT does not support certificate verification for self-signed certificates or
those signed by any CA not trusted by the Requests package in Splunk's Python environment. Requests sources their trust CA list from Mozilla trust store.

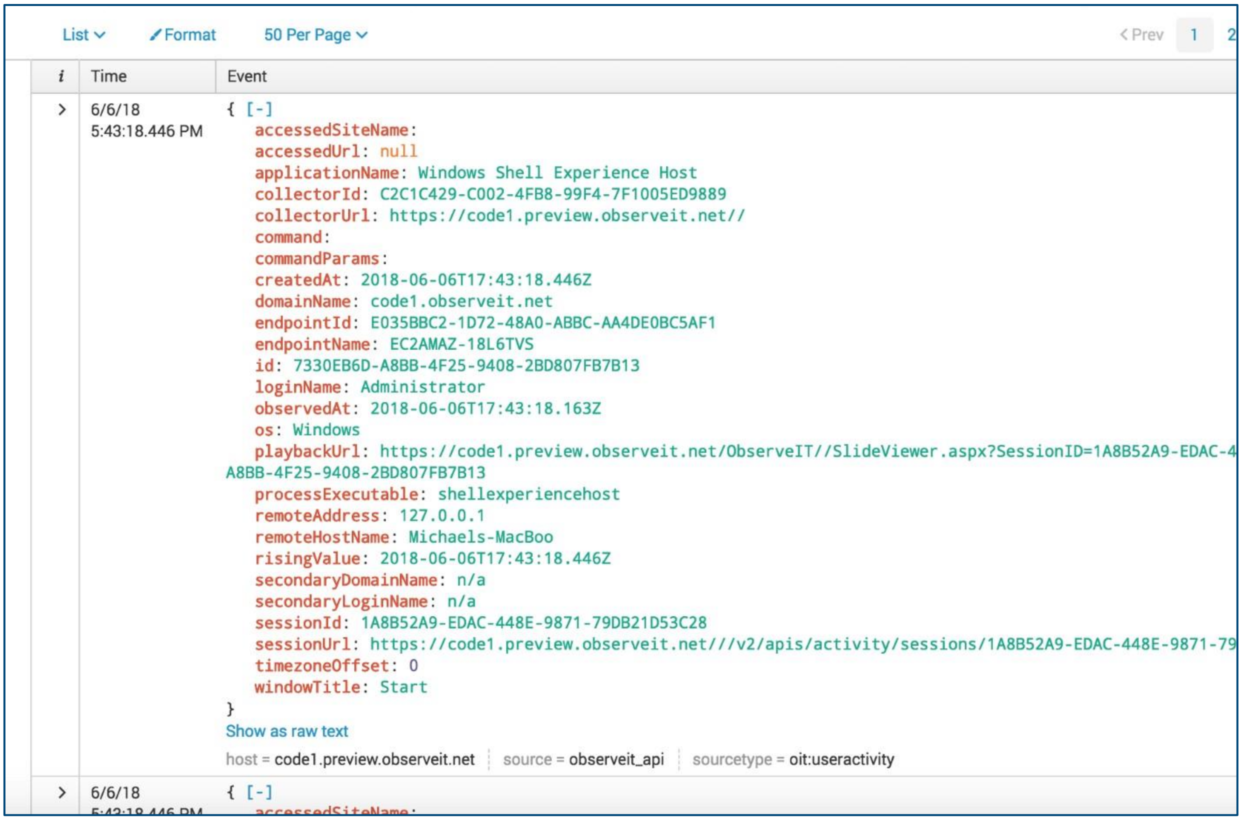
If you are unable to assign your ObserveIT Web Console a trusted certificate, then uncheck the SSL Verification box.

Note: This is a less secure option and should not be used in production.

Usage

VIEWING EVENTS

You view events logged as soon as ObserveIT data collection is configured and enabled in the ObserveIT TA. You can start using the data in Splunk searches and reports.



```
>  6/6/18           { [-]
   5:43:18.446 PM      accessedSiteName:
                       accessedUrl: null
                       applicationName: Windows Shell Experience Host
                       collectorId: C2C1C429-C002-4FB8-99F4-7F1005ED9889
                       collectorUrl: https://code1.preview.observeit.net//
                       command:
                       commandParams:
                       createdAt: 2018-06-06T17:43:18.446Z
                       domainName: code1.observeit.net
                       endpointId: E035BBC2-1D72-48A0-ABBC-AA4DE0BC5AF1
                       endpointName: EC2AMAZ-18L6TVS
                       id: 7330EB6D-A8BB-4F25-9408-2BD807FB7B13
                       loginName: Administrator
                       observedAt: 2018-06-06T17:43:18.163Z
                       os: Windows
                       playbackUrl: https://code1.preview.observeit.net/ObserveIT//SlideViewer.aspx?SessionID=1A8B52A9-EDAC-4
                    A8BB-4F25-9408-2BD807FB7B13
                       processExecutable: shellexperiencehost
                       remoteAddress: 127.0.0.1
                       remoteHostName: Michaels-MacBoo
                       risingValue: 2018-06-06T17:43:18.446Z
                       secondaryDomainName: n/a
                       secondaryLoginName: n/a
                       sessionId: 1A8B52A9-EDAC-448E-9871-79DB21D53C28
                       sessionUrl: https://code1.preview.observeit.net///v2/apis/activity/sessions/1A8B52A9-EDAC-448E-9871-79
                       timezoneOffset: 0
                       windowTitle: Start
                    }
                    Show as raw text
                    host = code1.preview.observeit.net   source = observeit_api   sourcetype = oit:useractivity

>  6/6/18           { [-]
   5:43:18.446 PM      accessedSiteName:
```

DASHBOARDS

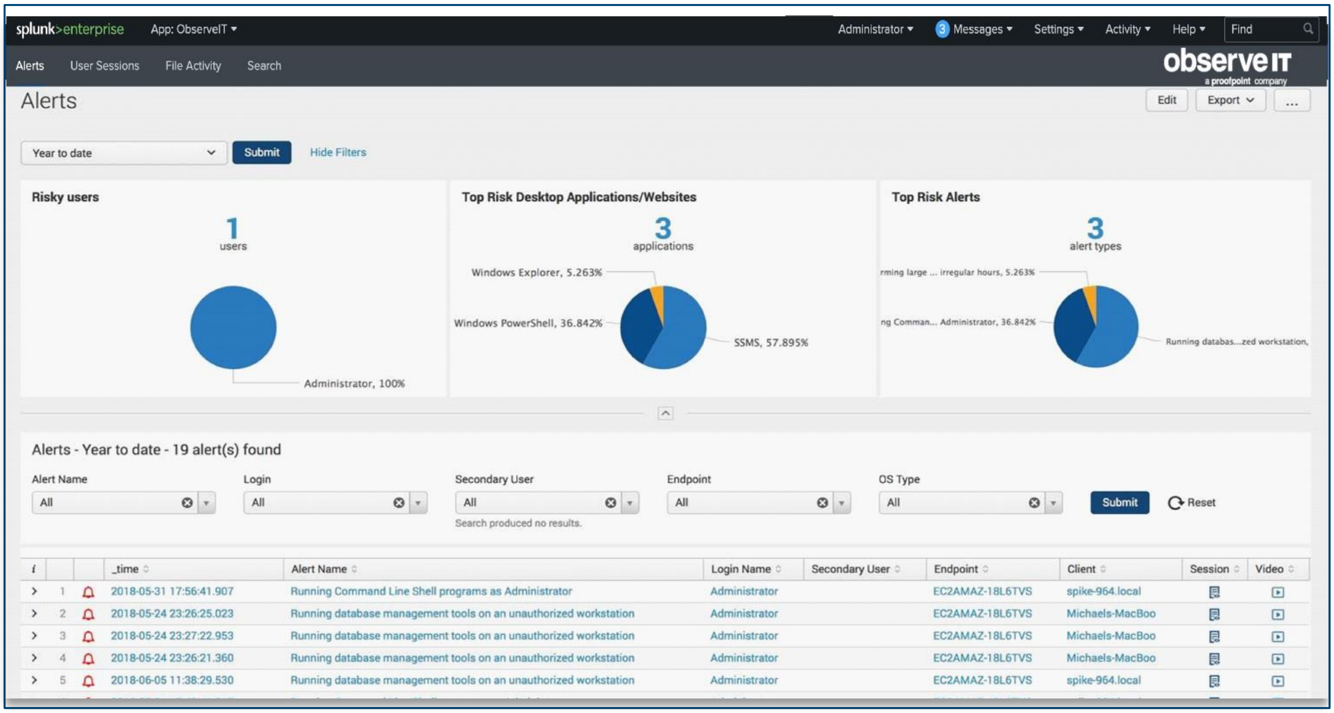
The ObserveIT App provides a comprehensive dashboard to view summary information about risky users and applications as well as drilldowns and links to view recorded user sessions.

Note: Installation of ObserveIT TA 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 so you can playback the user's session. The session column lets you drill-down to the individual activities that comprise the alerted session.

TIP: If you want to view only the alert list, use horizontal collapse bar to hide the pie views.



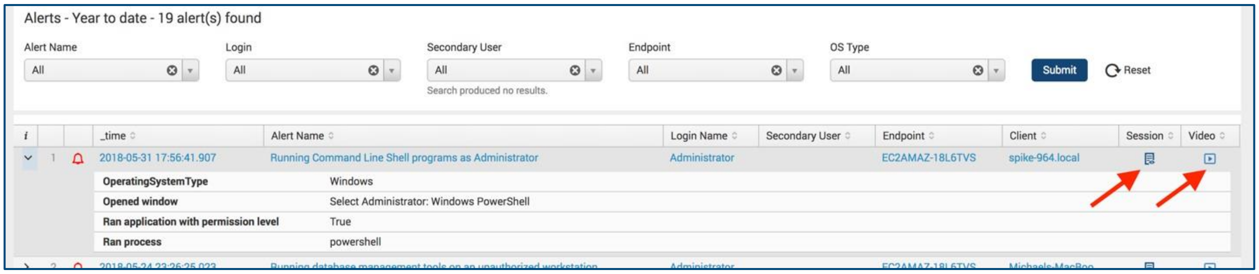
Alerts - Year to date - 19 alert(s) found

Alert Name	Login	Secondary User	Endpoint	OS Type
All	All	All	All	All

Search produced no results.

Submit   Reset

i			_time	Alert Name	Login Name	Secondary User	Endpoint	Client	Session	Video
>	1	🔔	2018-05-31 17:56:41.907	Running Command Line Shell programs as Administrator	Administrator		EC2AMAZ-18L6TVS	spike-964.local	🗎	▶
>	2	🔔	2018-05-24 23:26:25.023	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	Michaels-MacBoo	🗎	▶
>	3	🔔	2018-05-24 23:27:22.953	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	Michaels-MacBoo	🗎	▶
>	4	🔔	2018-05-24 23:26:21.360	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	Michaels-MacBoo	🗎	▶
>	5	🔔	2018-06-05 11:38:29.530	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	spike-964.local	🗎	▶



Alerts - Year to date - 19 alert(s) found

Alert Name	Login	Secondary User	Endpoint	OS Type
All	All	All	All	All

Search produced no results.

Submit   Reset

i			_time	Alert Name	Login Name	Secondary User	Endpoint	Client	Session	Video
˅	1	🔔	2018-05-31 17:56:41.907	Running Command Line Shell programs as Administrator	Administrator		EC2AMAZ-18L6TVS	spike-964.local	🗎	▶

OperatingSystemType	Windows
Opened window	Select Administrator: Windows PowerShell
Ran application with permission level	True
Ran process	powershell

User Sessions Dashboard

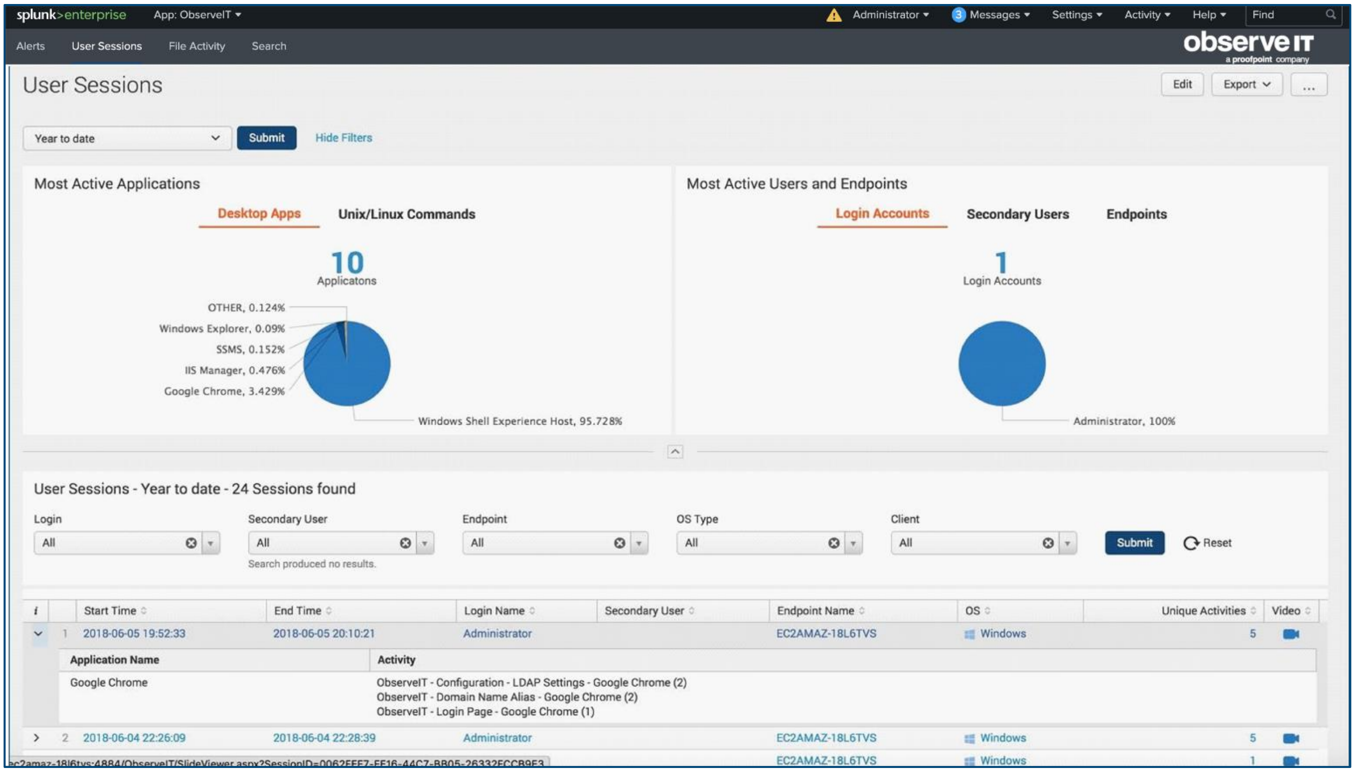
The User Session dashboard shows the most active users and endpoints as well as the most used applications.

A summary 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 shows more details about the individual activities that comprise the session.

When the user session dashboard is opened via alert drill-down, you see only that individual single session's activities.



User Sessions

Year to date

Most Active Applications

Most Active Users and Endpoints

User Sessions - Year to date - 24 Sessions found

Login: All

Secondary User: All

Search produced no results.

Endpoint: All

OS Type: All

Client: All

i		Start Time	End Time	Login Name	Secondary User	Endpoint Name	OS	Unique Activities	Video
˅	1	2018-06-05 19:52:33	2018-06-05 20:10:21	Administrator		EC2AMAZ-18L6TVS	Windows	5	🎥
›	2	2018-06-04 22:26:09	2018-06-04 22:28:39	Administrator		EC2AMAZ-18L6TVS	Windows	5	🎥
						EC2AMAZ-18L6TVS	Windows	1	🎥

Application Name	Activity
Google Chrome	ObserveIT - Configuration - LDAP Settings - Google Chrome (2) ObserveIT - Domain Name Alias - Google Chrome (2) ObserveIT - Login Page - Google Chrome (1)

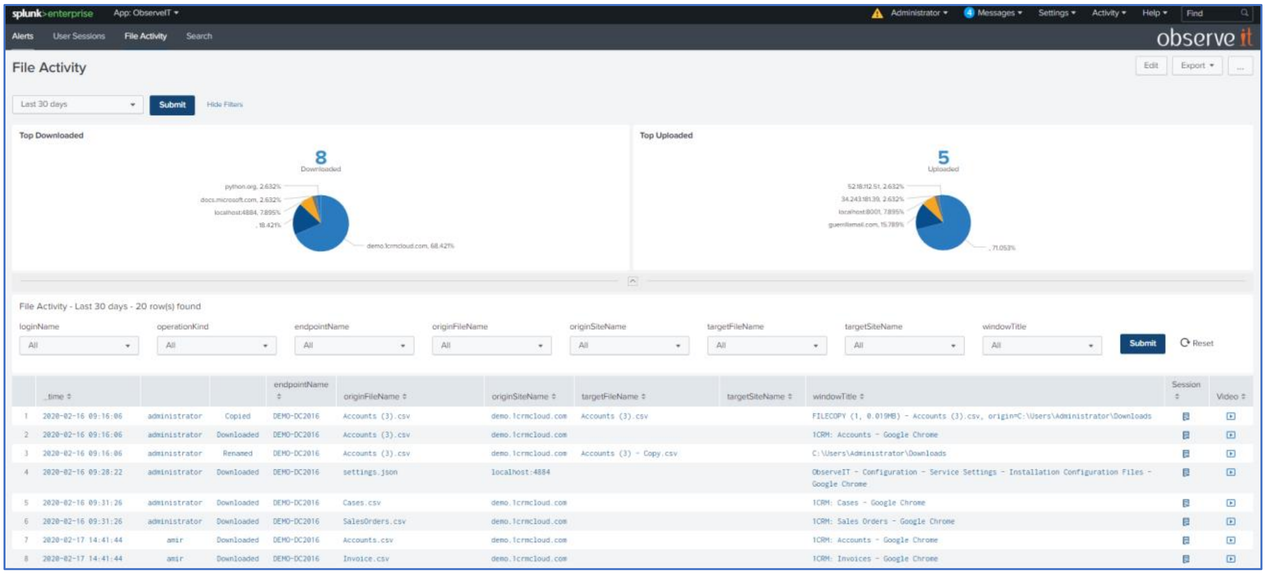
ec2amaz-18l6tvs:4884/ObserveIT/SlideViewer.aspx?SessionID=0062FEF7-FE16-44C7-BB05-26332FCCB9F3

File Activity Dashboard

The File Activity dashboard shows the top upload/downloaded files URLs

A summary view of each File Activity is available, including the date/time, action (Rename/Copy/Delete/Download etc.), User ID, Filename Windows Title and link to the session data.

A link to the ObserveIT player to replay the session is also included.



File Activity

Last 30 days ▾

File Activity - Last 30 days - 20 row(s) found

loginName: All ▾
operationKind: All ▾
endpointName: All ▾
originFileName: All ▾
originSiteName: All ▾
targetFileName: All ▾
targetSiteName: All ▾
windowTitle: All ▾

	_time ⇕			endpointName ⇕	originFileName ⇕	originSiteName ⇕	targetFileName ⇕	targetSiteName ⇕	windowTitle ⇕	Session ⇕	Video ⇕
1	2020-02-16 09:16:06	administrator	Copied	DEMO-DC2016	Accounts (3).csv	demo.1crmcloud.com	Accounts (3).csv		FILECOPY (1, 0.019MB) - Accounts (3).csv, origin=C:\Users\Administrator\Downloads	▤	▶
2	2020-02-16 09:16:06	administrator	Downloaded	DEMO-DC2016	Accounts (3).csv	demo.1crmcloud.com			1CRM: Accounts - Google Chrome	▤	▶
3	2020-02-16 09:16:06	administrator	Renamed	DEMO-DC2016	Accounts (3).csv	demo.1crmcloud.com	Accounts (3) - Copy.csv		C:\Users\Administrator\Downloads	▤	▶
4	2020-02-16 09:28:22	administrator	Downloaded	DEMO-DC2016	settings.json	localhost:4884			ObserveIT - Configuration - Service Settings - Installation Configuration Files - Google Chrome	▤	▶
5	2020-02-16 09:31:26	administrator	Downloaded	DEMO-DC2016	Cases.csv	demo.1crmcloud.com			1CRM: Cases - Google Chrome	▤	▶
6	2020-02-16 09:31:26	administrator	Downloaded	DEMO-DC2016	SalesOrders.csv	demo.1crmcloud.com			1CRM: Sales Orders - Google Chrome	▤	▶
7	2020-02-17 14:41:44	amir	Downloaded	DEMO-DC2016	Accounts.csv	demo.1crmcloud.com			1CRM: Accounts - Google Chrome	▤	▶
8	2020-02-17 14:41:44	amir	Downloaded	DEMO-DC2016	Invoice.csv	demo.1crmcloud.com			1CRM: Invoices - Google Chrome	▤	▶

Troubleshooting

Events not flowing: If you have configured ObserveIT TA and do not see events flowing into the system, 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 help using the ObserveIT platform, contact the ObserveIT support organization.
https://proofpointcommunities.force.com/community/s/

You can also send an email to oit-support@proofpoint.com with questions about this and other ObserveIT integrations.

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.