

## Splunk Integration User Guide

This document describes the integration of ITM On-Prem with Splunk software.

Note: Currently documentation is being rebranded from ObserveIT to ITM On-Prem. Anything referred to as ITM On-Prem means ObserveIT and anything referred to as ObserveIT is ITM On-Prem.

### FEATURES

ITM On-Prem 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

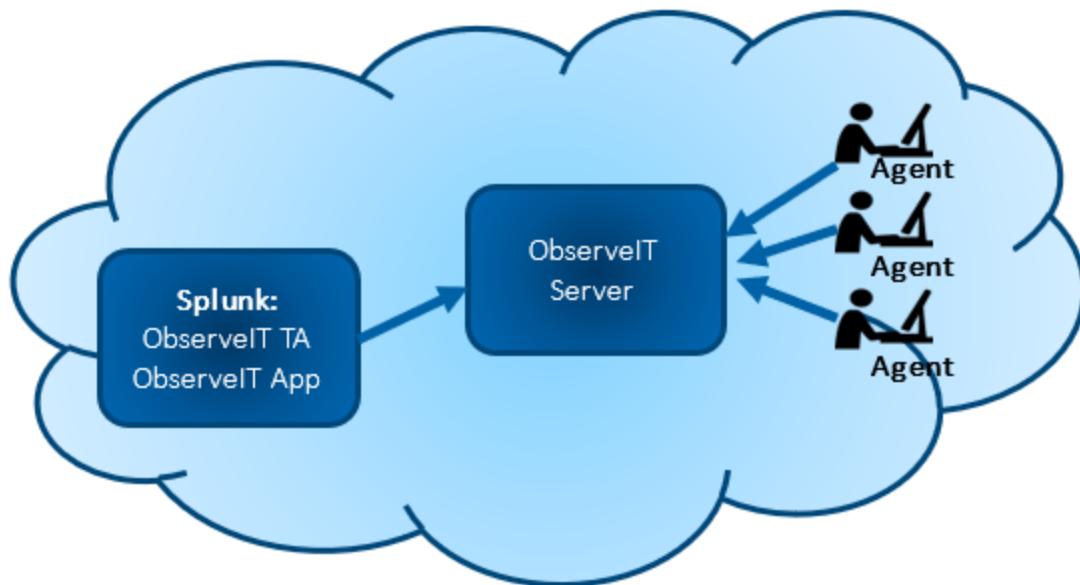
### PREREQUISITES

- 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: 7.12)
- Splunk Enterprise: Platform Version: 9.1, 9.0, 8.2, 8.1, 8.0

## Splunk Deployment Architecture

### SINGLE-INSTANCE SPLUNK ENTERPRISE DEPLOYMENT

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

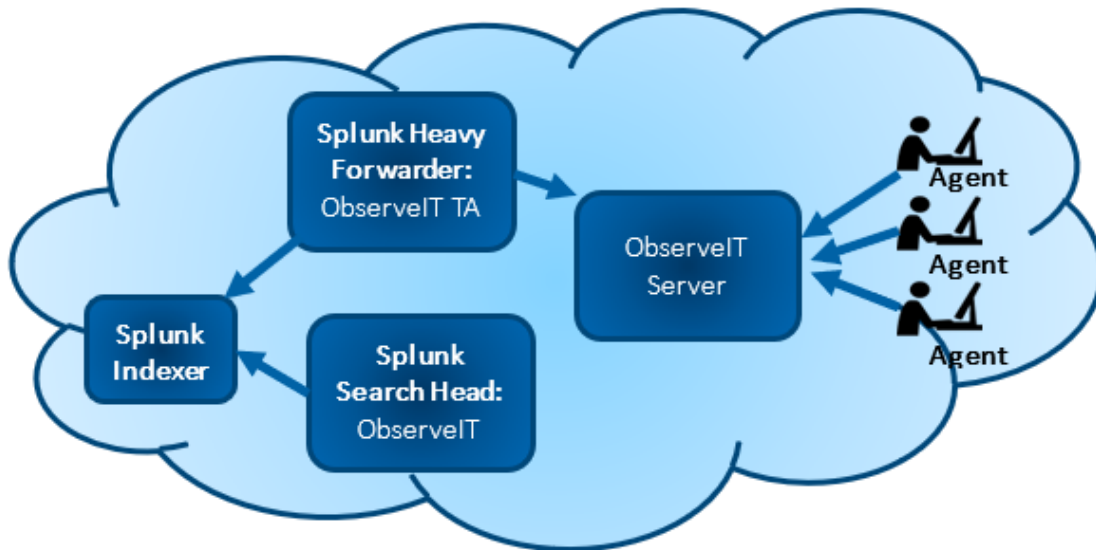


### DISTRIBUTED SPLUNK ENTERPRISE DEPLOYMENT

Splunk is a distributed deployment on the same network as ITM On-Prem.

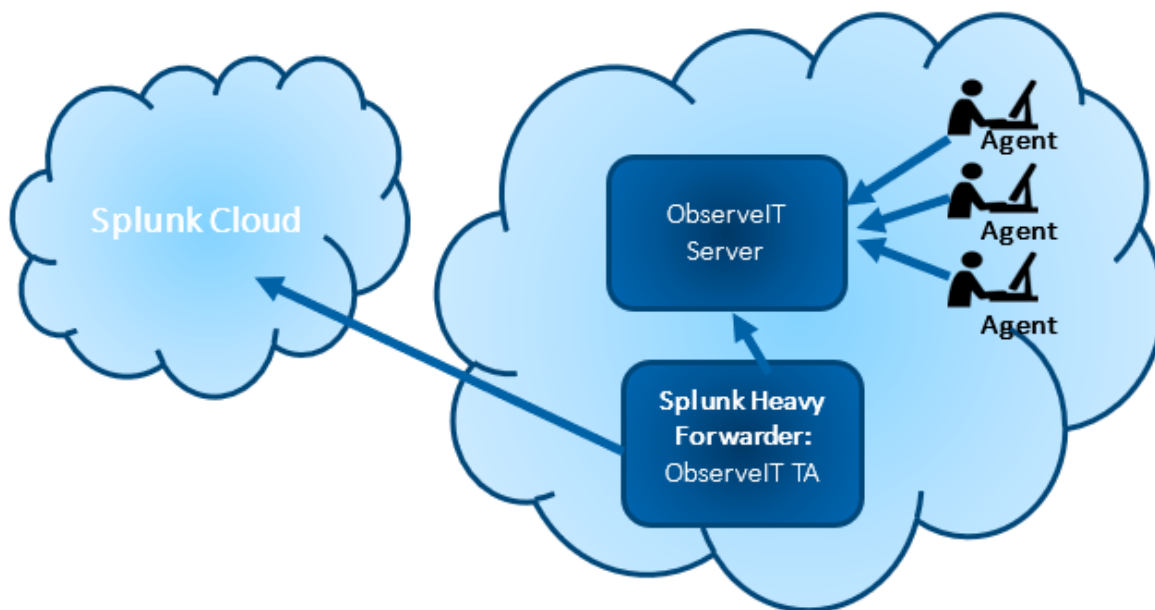
ObserveIT TA is installed on a Splunk heavy forwarder that sends data. (Installation of ObserveIT TA on a Universal Forwarder or SHC is not supported.)

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 ITM On-Prem 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.



### Splunk Configuration

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

## CREATING APPLICATION IN ITM ON-PREM

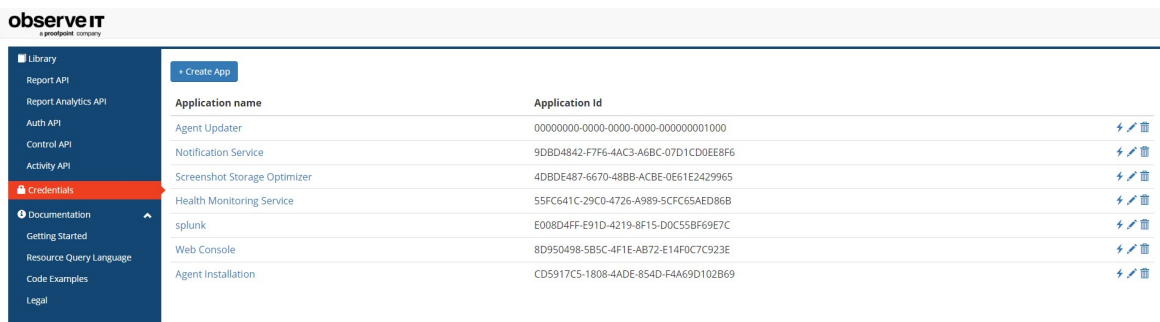
To integrate ITM On-Prem with Splunk using RESTful API, you register the application to authenticate access. OAuth2 is the method of authenticating access to the ObserveIT RESTful API.

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

1. From the ITM On-Prem (ObserveIT) Web Console, click the ? in the upper-right corner and select **Developer Portal** from the menu.

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

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



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 it:report:\*  
\*

Allowed Grants

- Client Credentials
- Password
- Authorization Code
- Refresh Token
- Implicit

Redirect URIs used for authorization\_code and token(implicit) flows

Redirect URI

Redirect URI

Redirect URI

Cancel Save

3. Do the following:

1. In the **Application Name** field, enter a name. It is recommended that you choose a name you can recognize, such as **Splunk**, **Splunk1** etc.
2. In **Allowed Grants**, check **Client Credentials**.
3. Click **Save** and the application is added to the list.

observe it  
proofpoint company

Library

- Report API
- Report Analytics API
- Auth API
- Control API
- Activity API
- Credentials**
- Documentation
- Getting Started
- Resource Query Language
- Code Examples
- Legal

+ Create App

Application name	Application Id
Agent Updater	00000000-0000-0000-0000-000000001000
Notification Service	9DBD4842-F7F6-4AC3-A6BC-07D1CD0EE8F6
Screenshot Storage Optimizer	4DBDE487-6670-48BB-ACBE-0E61E2429965
Health Monitoring Service	55FC641C-29C0-4726-A989-5CFC65AED86B
splunk	E008D4FF-E91D-4219-8F15-D0C55BF69E7C
Web Console	8D950498-5B5C-4F1E-AB72-E14F0C7C923E
Agent Installation	CD5917C5-1808-4ADE-854D-F4A69D102B69

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

splunk ✕

**Grant Type**

client\_credentials ▾

**Client Id**

E008D4FF-E91D-4219-8F15-D0C55BF69E7C

**Client Secret**

GmGB6wugb4evaCd1Ne2hFICdqw6HpChgTXq538w5p4

**Scope**

\*

Close Generate Token

Note: Note the Client Id and Client Secret values. You will enter them into the configuration screen of the Splunk add-on.

## Creating New Index for ObserveIT (example "oit" index)

1. Create a new index from the **Indexes** screen.

The screenshot shows the 'Indexes' page in Splunk Enterprise. At the top right, there is a green 'New Index' button. Below it is a table listing various indexes. The 'oit' index is highlighted in blue, indicating it is the focus of the current step.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
..audit	Edit Delete Disable	Events	system	46 MB	488.28 GB	500K	a month ago	a few seconds ago	\$\$SPLUNK_DB/audit/db	N/A	✓ Enabled
..configtracker	Edit Delete Disable	Events	system	4 MB	488.28 GB	485	a month ago	10 hours ago	\$\$SPLUNK_DB/..configtracker/db	N/A	✓ Enabled
..internal	Edit Delete Disable	Events	system	832 MB	488.28 GB	14.2M	a month ago	a few seconds ago	\$\$SPLUNK_DB/..internal/db	N/A	✓ Enabled
..introspection	Edit Delete Disable	Events	system	1.63 GB	488.28 GB	1.44M	14 days ago	a few seconds ago	\$\$SPLUNK_DB/..introspection/db	N/A	✓ Enabled
..metrics	Edit Delete Disable	Metrics	system	285 MB	488.28 GB	775M	14 days ago	a few seconds ago	\$\$SPLUNK_DB/..metrics/db	N/A	✓ Enabled
..metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$\$SPLUNK_DB/..metrics_rollup/db	N/A	✓ Enabled
..telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	54	18 days ago	10 hours ago	\$\$SPLUNK_DB/..telemetry/db	N/A	✓ Enabled
..thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$\$SPLUNK_DB/..thefishbucket/db	N/A	✓ Enabled
..history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$\$SPLUNK_DB/..history/db	N/A	✓ Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$\$SPLUNK_DB/default/db	N/A	✓ Enabled
oit	Edit Delete Disable	Events	TA-ObserveIT	1 MB	500 GB	418	13 days ago	5 minutes ago	\$\$SPLUNK_DB/..oit/db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$\$SPLUNK_DB/splunklogger/db	N/A	✗ Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$\$SPLUNK_DB/summary/db	N/A	✓ Enabled

2. Click **New Index** and the **New Index** dialog box opens.
3. Provide an **Index Name**. In the example, the new index is "oit".

In the example below , you can see the button to create the “New Index:, example “oit”

**New Index**

**General Settings**

Index Name: oit  
Set index name (i.g., INDEX\_NAME). Search using index=INDEX\_NAME.

Index Data Type: Events (selected) | Metrics

Home Path: optional  
Hot/warm db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/oh).

Cold Path: optional  
Cold db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/colddb).

Thawed Path: optional  
Thawed/resurrected db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/thaweddb).

Data Integrity Check: Enable (selected) | Disable

Max Size of Entire Index: 500 GB

Max Size of Hot/Warm/Cold Bucket: auto GB

Frozen Path: optional  
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: ObserveIT

**Storage Optimization**

Tsidx Retention Policy: Enable Reduction (selected) | Disable Reduction

Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#)

Save Cancel

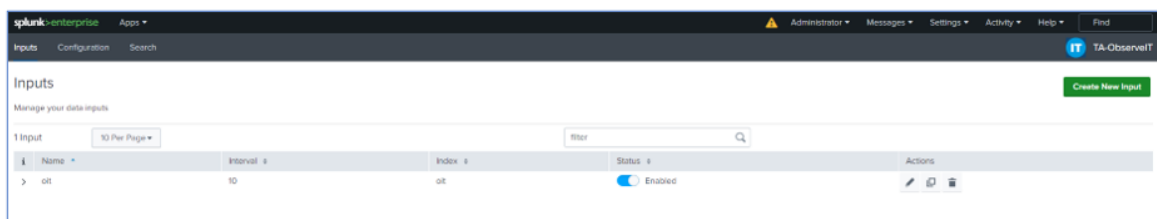
## CONFIGURING OBSERVEIT TA FOR SPLUNK

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**.



## 2. Complete the **Add ObserveIT API** dialog box.

**Update ObserveIT API**

Name: oit  
Enter a unique name for the data input.

Interval: 30  
Time interval of input in seconds.

Index: oit

Reports API URL: https://sales-demo.lmdemo.local/v2/apis/report;  
API URL, optionally including port. E.g.  
https://observeit.mycompany.com:443/v2/apis/report?realm=observeit/reports

Client ID: E008D4FF-E91D-4219-8F15-00C558F69E7C  
Create app in API Console. E.g.  
https://observeit.mycompany.com/v2/apps/portal/home.html? #code

Client Secret: [Empty]

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 Activities x, Command Activities x, Alerts x, File Activity x, Email Activity x

CA Certificate chain: cer@lmdemo-sales-demo-ca.cer

Buttons: Cancel, Update

1. Enter a unique **Name** that represents the ObserveIT instance, for example use the hostname such as Splunk.
2. In the **Interval** and **Events Pagination** fields, enter values you want. Make sure that their combination is sufficient to ingest your anticipated event rate.
3. The **Reports API URL** is formatted as:  

```
https://<hostname>:<port>/v2/apis/report;realm=observeit/reports
```
4. In the **Client ID** and **Client Secret**, enter the values you copied when the application was created in ObserveIT. (See: Creating Application in O.)
5. 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.
6. Select **Reports to Collect**.
7. The input requires CA certificate (mandatory). You must provide the path to CA certificate chain file, relative to \$SPLUNK\_HOME. Default CA certificates will be used if



no file name provided. For example, the certificate file name is: `cer\itmdemo-sales-demo-ca.cer`.

3. 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

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

## Splunk Usage

### VIEWING EVENTS

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

i	Time	Event
>	6/6/18 5:43:18.446 PM	<pre>{ [-]   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-4A8BB-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 }</pre> <p>Show as raw text</p> <p>host = code1.preview.observeit.net   source = observeit_api   sourcetype = oit:useractivity</p>
>	6/6/18 5:43:18.446 PM	<pre>{ [-]   accessedSiteName:</pre>

## 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 ITM On-Prem (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.

Note: 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

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		
> 6	2018-05-31 17:56:41.907	Running Command Line Shell programs as Administrator	Administrator		EC2AMAZ-18L6TVS	spike-964.local		

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

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 Session Dashboard

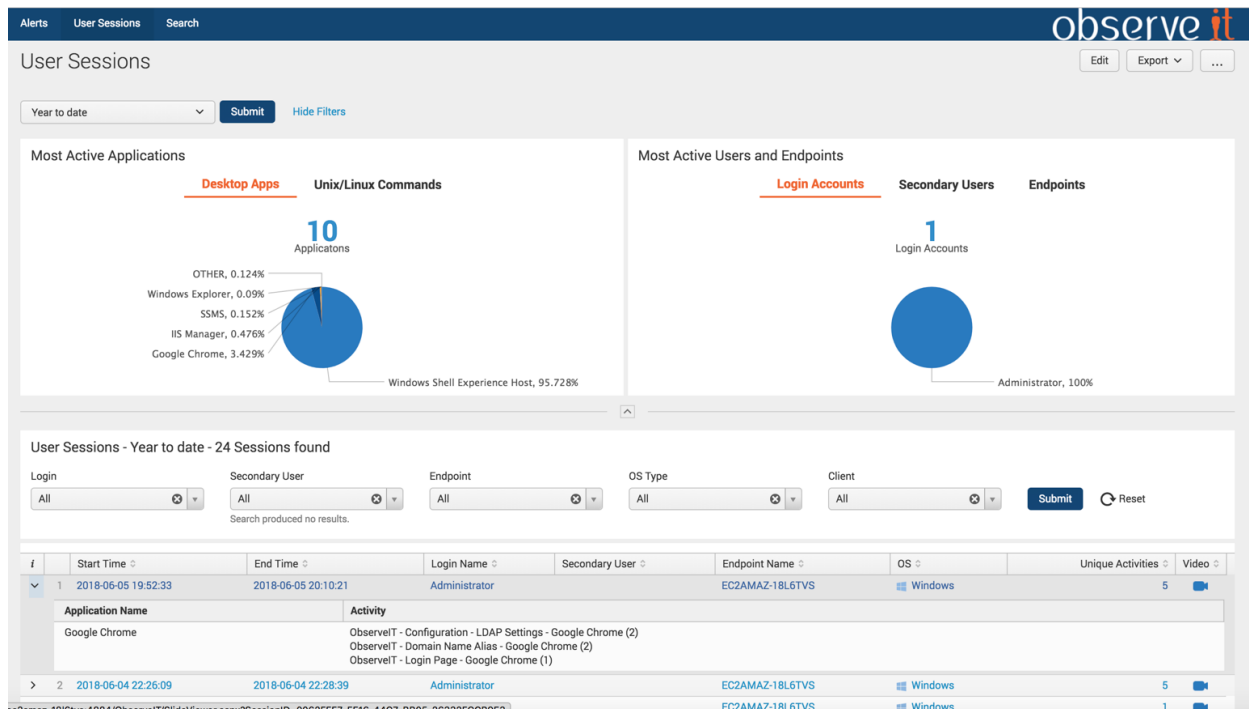
The User Session dashboard shows the most active users and endpoints as well as the most used applications.

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 ITM On-Prem (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.



## Splunk Troubleshooting and Support

### 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"
```

Error: "No previous instances" in TA log

If in the TA log in `SPLUNK_HOME\var\log\splunk\ta_observeit_observeit_api.log`

A message displays, for example:



2024-01-02 07:01:01,625 INFO pid=612 tid=MainThread file=base\_modinput.py:log\_info:295 | No previous instances of input 'oit' were found.

This message indicates that you must create the **oit** index as described in "Creating New Index for ObserveIT (example "oit" index)" on page 6.

## SUPPORT

For help using the ITM On-Prem (ObserveIT) platform, contact Proofpoint support organization.

<https://proofpointcommunities.force.com/community/s/>