Splunk Integration User Guide

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

For new Splunk version 2.3.3, HTTPS and SSL verification is mandatory and require a CA certificate [chain].
After upgrading the TA, you must provide the path to CA certificate chain file , relative to $SPLUNK_HOME. Default CA certificates will be used if no file name is provided. (See "Configuring ObserveIT TA for Splunk" on page 7.)

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

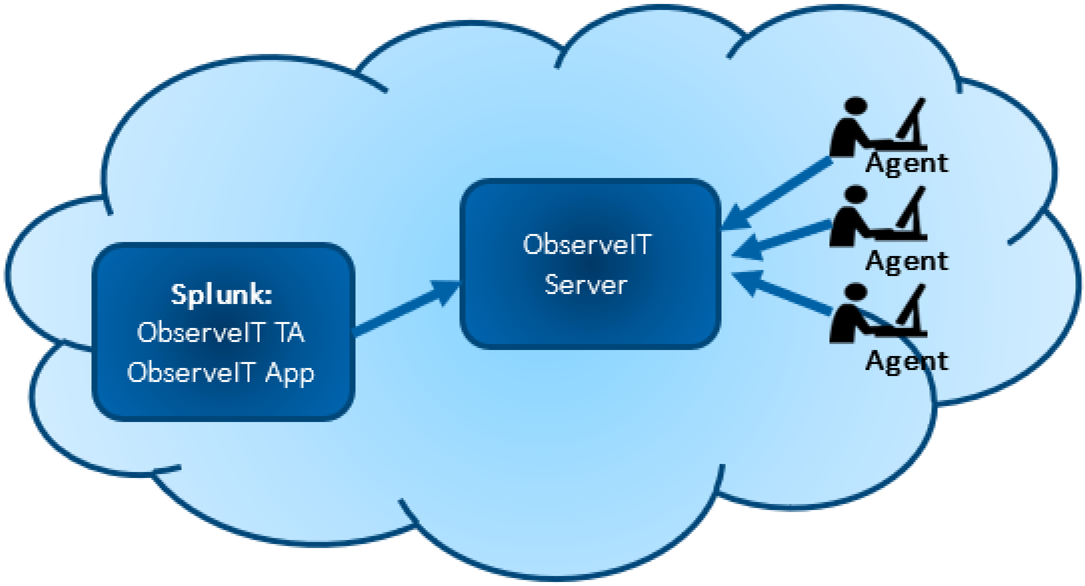
- Download and install ObserveIT TA and ObserveIT App for Splunk from Splunkbase
- ObserveIT TA communicates with your ObserveIT API directly, typically on port 443

- 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.

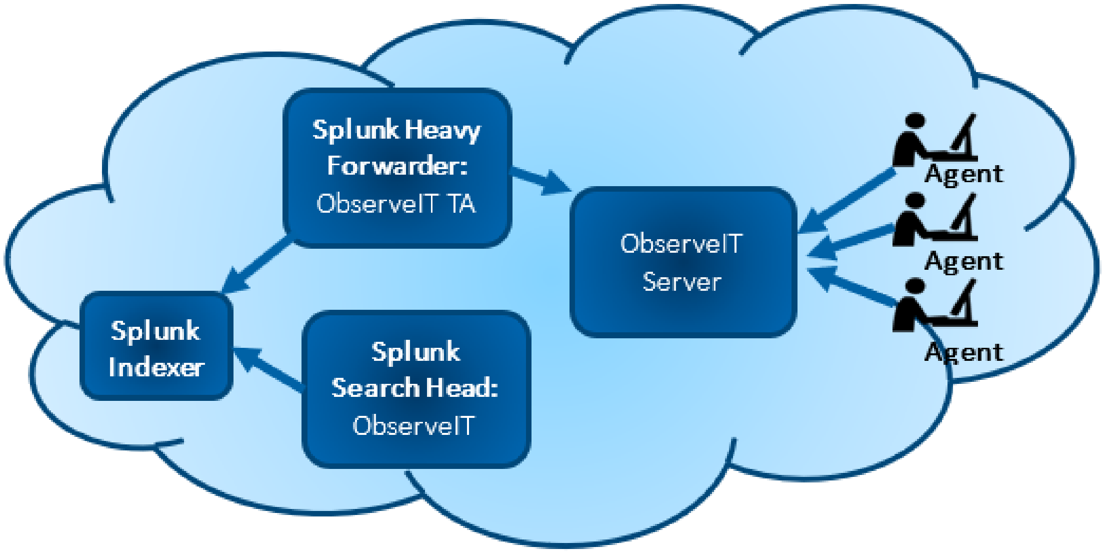


DISTRIBUTED SPLUNK ENTERPRISE DEPLOYMENT

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

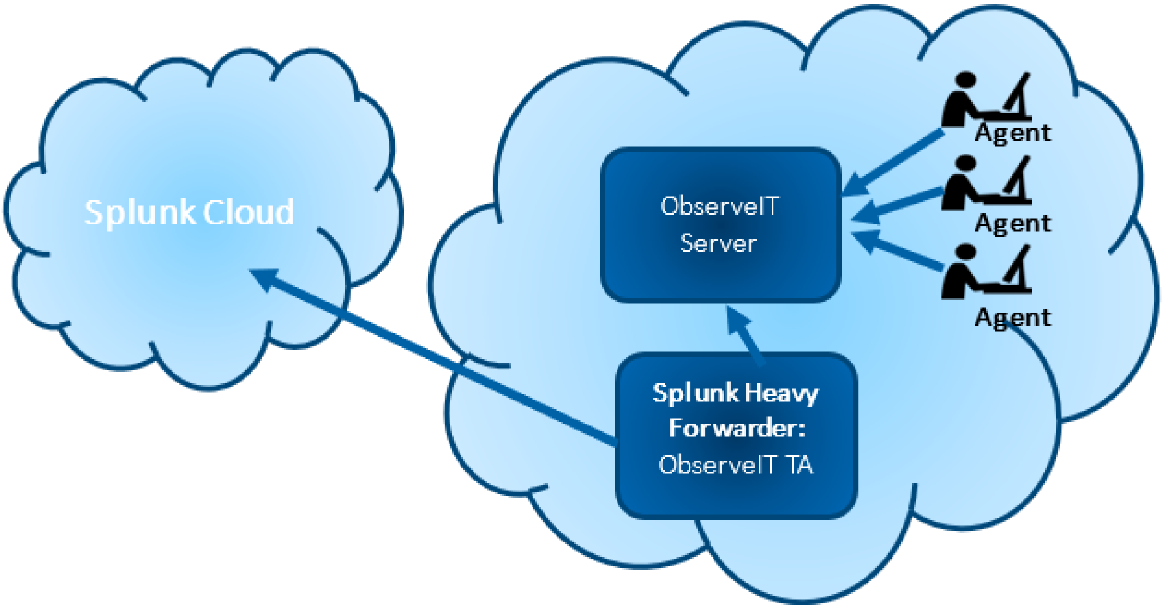
ObserveIT TA is installed on a Splunk heavy forwarder that sends data. (Installation of ObserveIT TA on a Universal Forwarder or SHC is not supported.)

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


Splunk Heavy Forwarder: ObserveIT TA
ObserveIT Server
Agent
Agent
Agent
Splunk Indexer
Splunk Search Head: ObserveIT

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

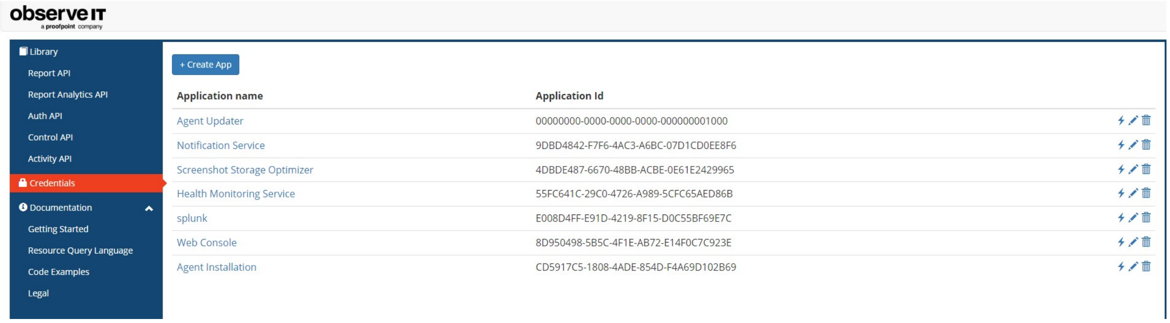
To integrate ITM On-Prem with Splunk using RESTful API, you register the application to authenticate access. Oauth2 is the method of authenticating access to the ObserveIT RESTful API.

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.

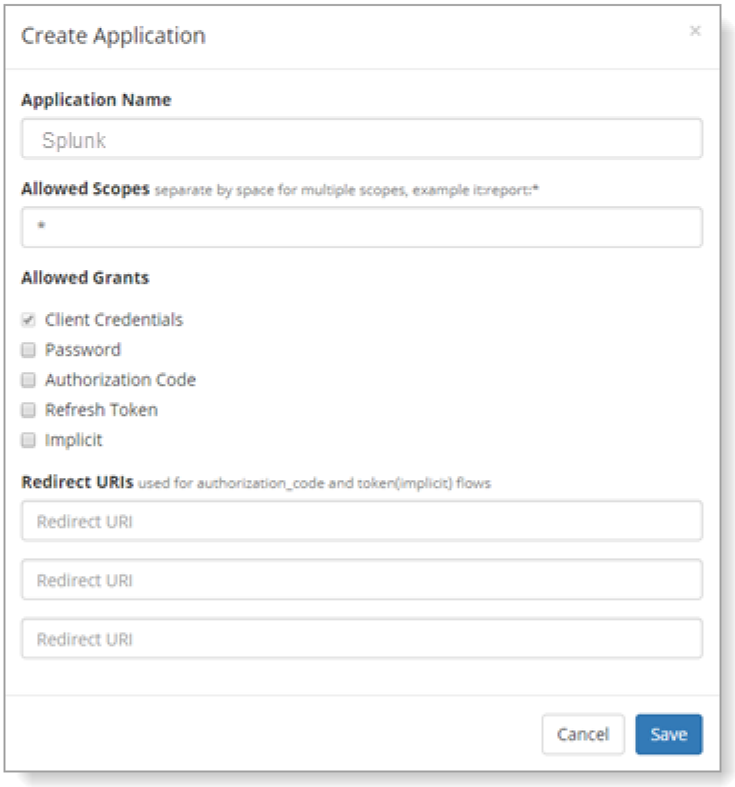
   > Note: If the **Developer Portal** is not installed by default, you will be prompted to install it.

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



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

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

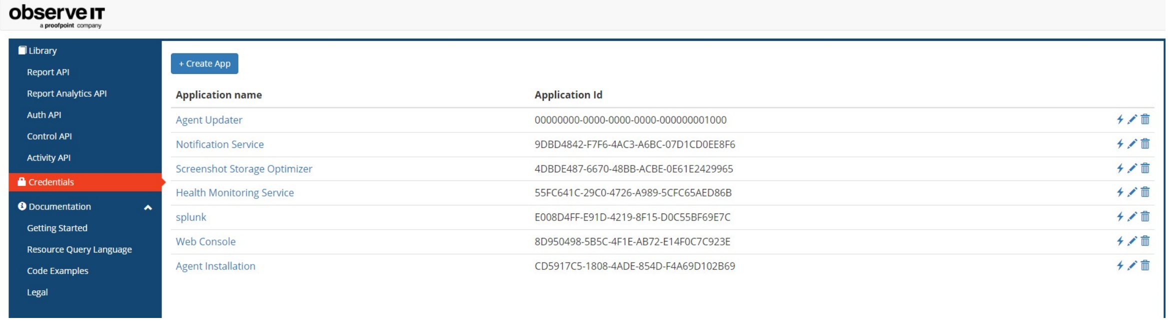
Redirect URI

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.

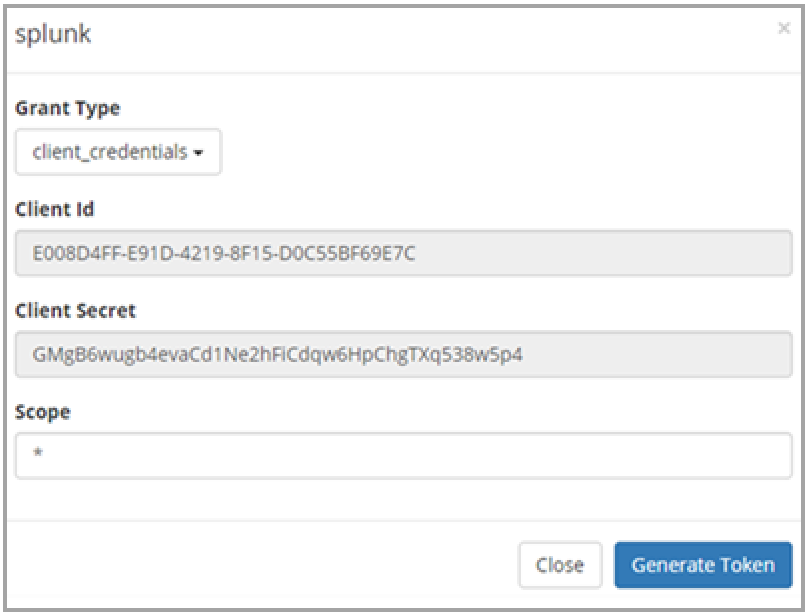
    2. In **Allowed Grants**, check **Client Credentials**.

    3. Click **Save** and the application is added to the list.



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

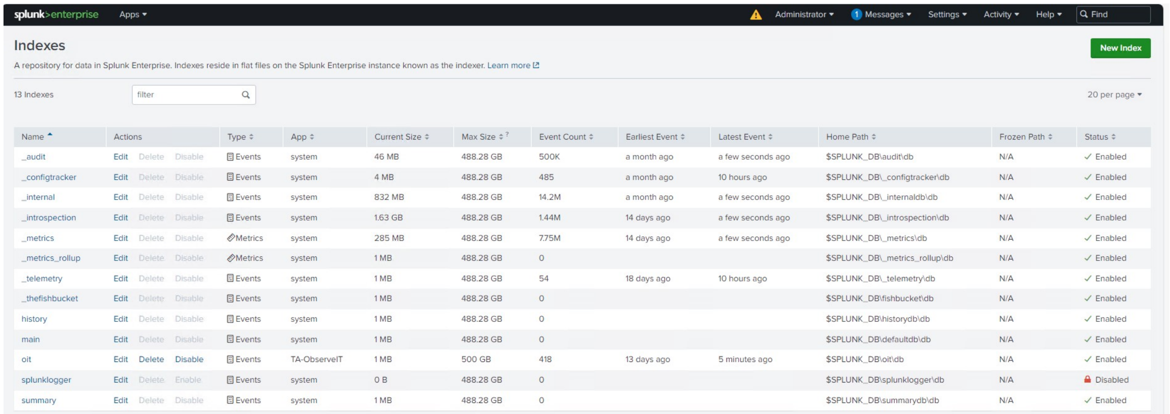
Scope

*

> 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.



Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more

13 Indexes

filter

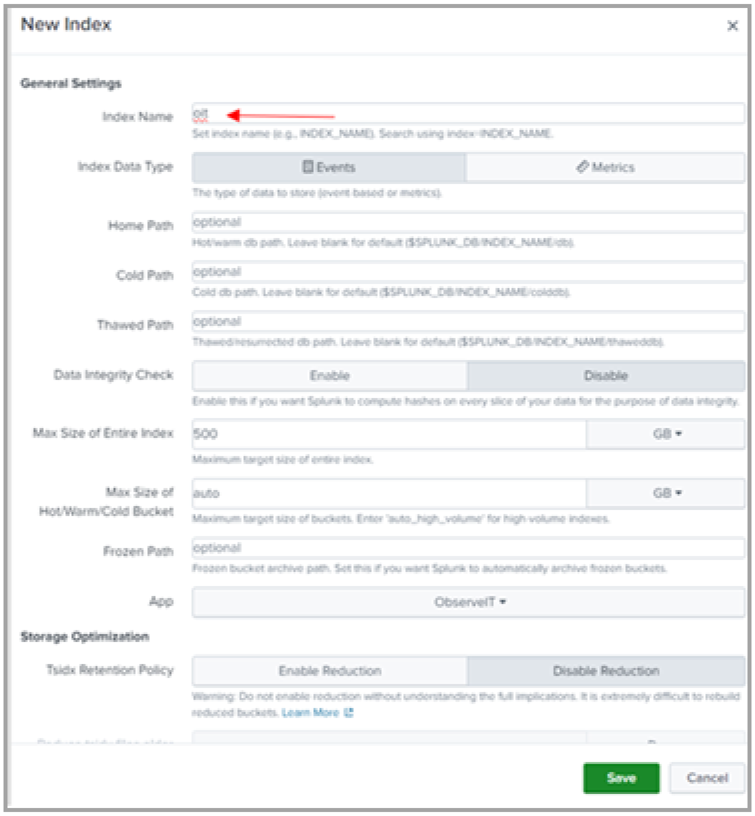
20 per page ▾

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_internaldb\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	7.75M	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\fishbucket\db	N/A	✓ Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB\historydb\db	N/A	✓ Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB\defaultdb\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\summarydb\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 (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

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 | Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high volume indexes.

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 | Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. Learn More

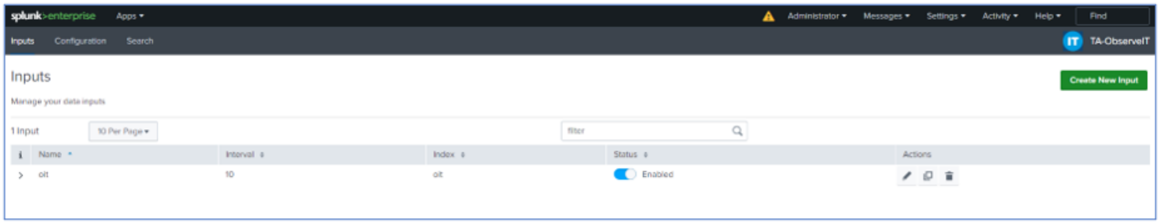
CONFIGURING OBSERVEIT TA FOR SPLUNK

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**.



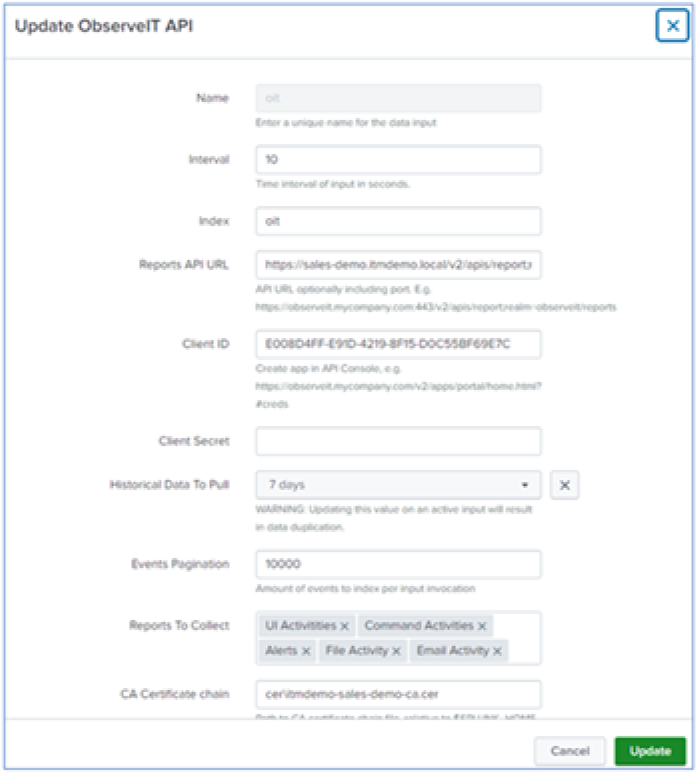
Inputs

Manage your data inputs

1 Input   10 Per Page   filter

i	Name	Interval	Index	Status	Actions
>	oit	10	oit	Enabled	

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: oit

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

Client ID: E008D4FF-E91D-4219-8F15-D0C55BF69E7C
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 Activities, Command Activities, Alerts, File Activity, Email Activity

CA Certificate chain: cer\itmdemo-sales-demo-ca.cer
Path to CA certificate chain file, relative to $SPLUNK_HOME

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**.

3.

4. The input requires CA certificate (mandatory). You must provide the path to CA certificate chain file, relative to $SPLUNK_HOME. Default CA certificates that will be used if no file name is provided. For example, the certificate file name is: **cer\itmdemo-sales-demo-ca.cer**.

    1. Upload the CA certificate chain file to the Splunk server. The file should be saved in a directory under **/opt/splunk** and should be readable by the user running the Splunk service.

    2. Update input configurations – specify the relative CA certificate path (e.g if you've saved the chain file as **/opt/splunk/etc/auth/mychain.pem** then the input should be **etc/auth/mychain.pem**.

5. Choose the reports you want to load in Splunk:

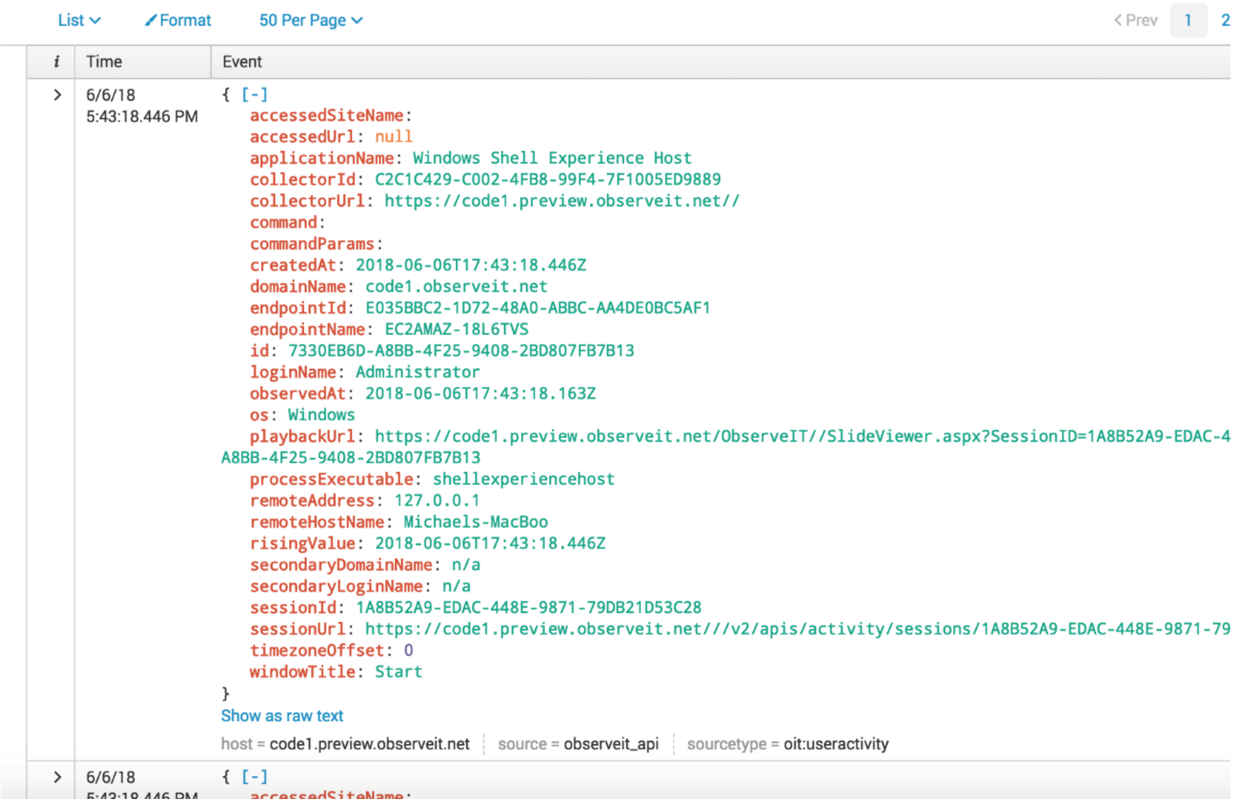
- **UI Activities**: User interface activity events from Windows or Mac agents
- **Command Activities**: Commands run on UNIX agents
- **Alerts**: Alert events from all agents

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.



```
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
}

host = code1.preview.observeit.net | source = observeit_api | sourcetype = oit:useractivity

6/6/18
5:43:18.446 PM

{ [-]
   accessedSiteName:
```

DASHBOARDS

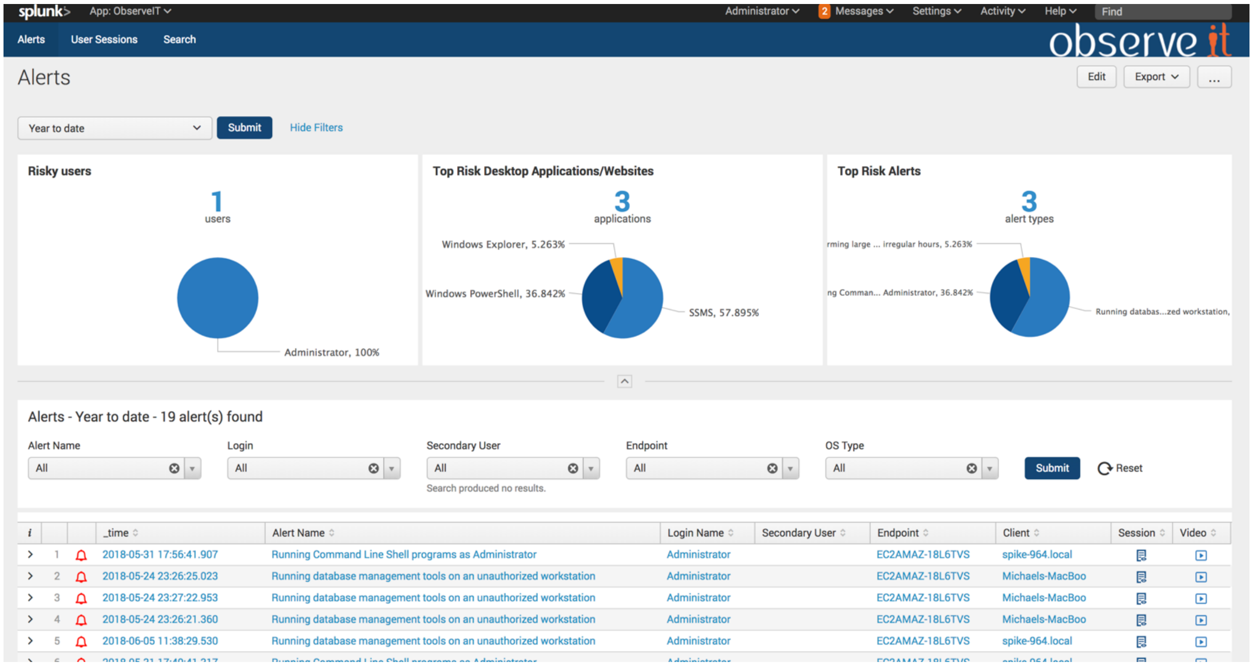
The ObserveIT App provides a comprehensive dashboard to view summary information about risky users and applications as well as drilldowns and links to view recorded user sessions.

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 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.

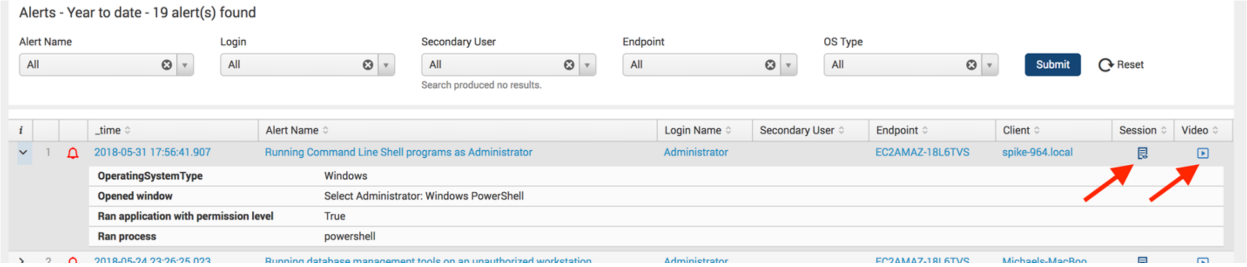


Alerts

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

Alert Name: All
Login: All
Secondary User: All
Search produced no results.
Endpoint: All
OS Type: All

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: All
Login: All
Secondary User: All
Search produced no results.
Endpoint: All
OS Type: All

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

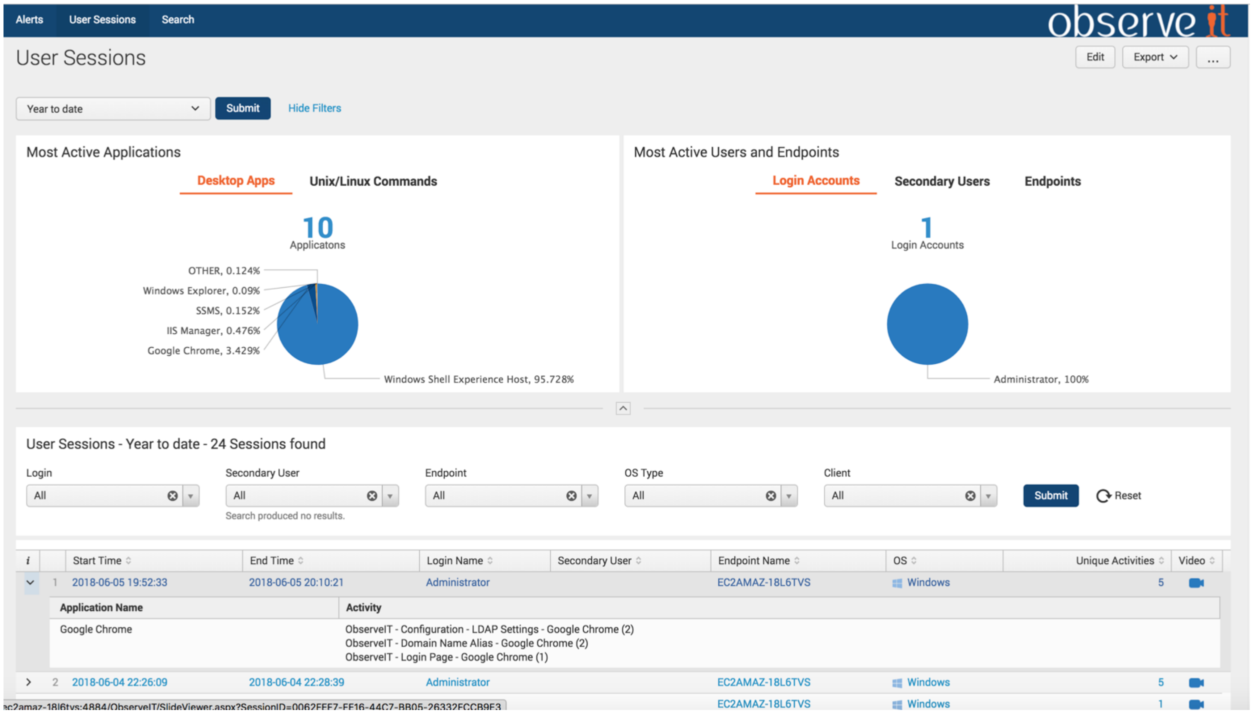
The User Session dashboard shows the most active users and endpoints as well as the most used applications.

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.



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-BB05-26332FCCB9E3

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/