

User Guide

ObserveIT App and Add-On for Splunk

Version 1.2.0 – January 2019

Table of Contents

OBSERVEIT INTRODUCTION	3
OVERVIEW AND FEATURES	3
PREREQUISITES	4
DEPLOYMENT ARCHITECTURE	4
SINGLE-INSTANCE SPLUNK ENTERPRISE.....	4
DISTRIBUTED SPLUNK ENTERPRISE	5
SPLUNK CLOUD.....	5
CONFIGURATION	6
CREATE APPLICATION IN OBSERVEIT	6
CONFIGURE OBSERVEIT TA FOR SPLUNK.....	8
UPGRADING	10
USAGE	10
VIEWING EVENTS	10
DASHBOARDS	11
<i>Alerts Dashboard</i>	<i>11</i>
<i>User Session Dashboard</i>	<i>12</i>
TROUBLESHOOTING	13
SUPPORT	13
RELEASE NOTES	14

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

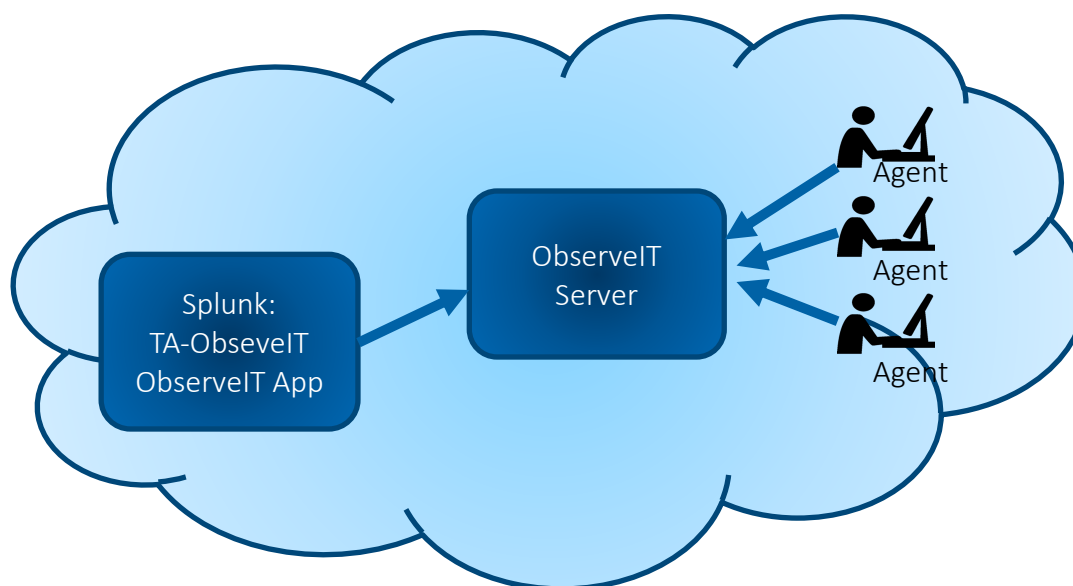
Minimum supported Splunk version is 6.5

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

Deployment Architecture

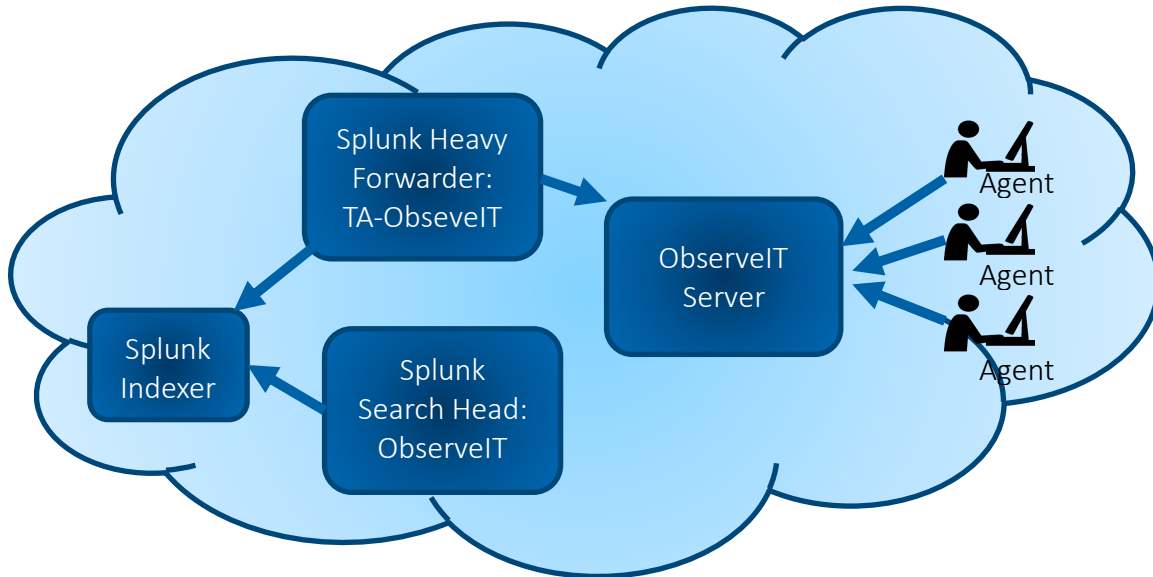
SINGLE-INSTANCE SPLUNK ENTERPRISE

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



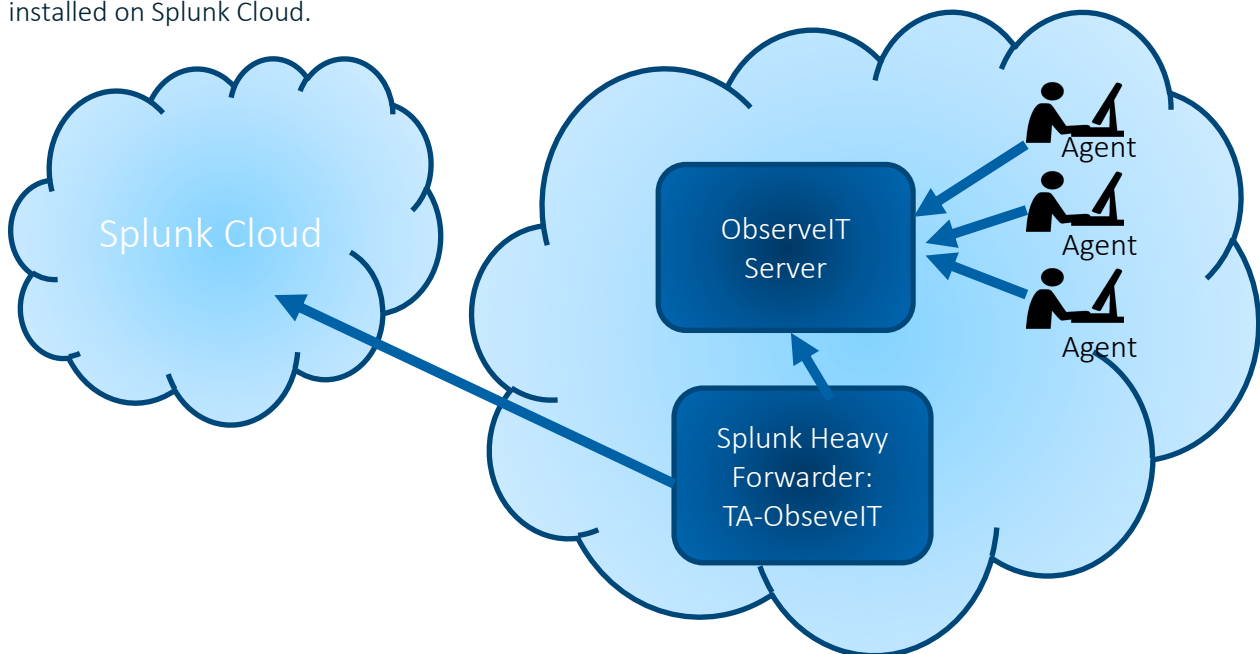
DISTRIBUTED SPLUNK ENTERPRISE

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.



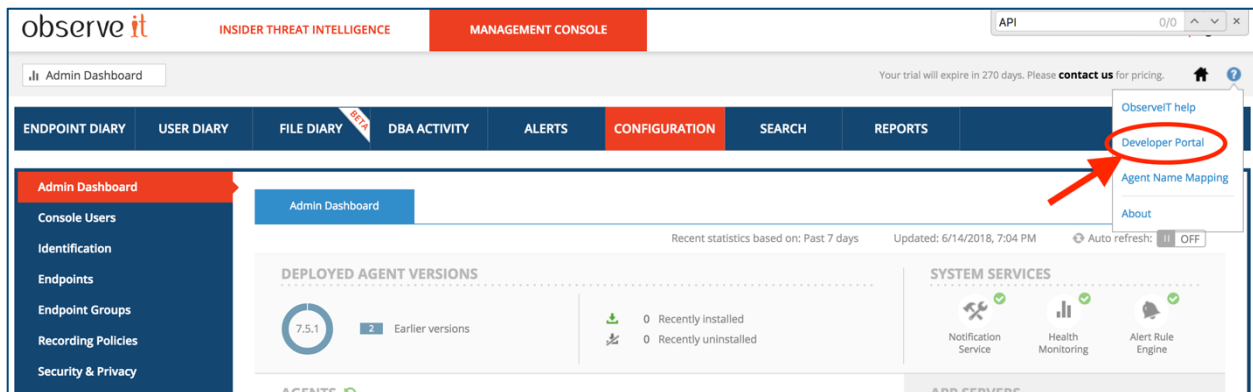
Configuration

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

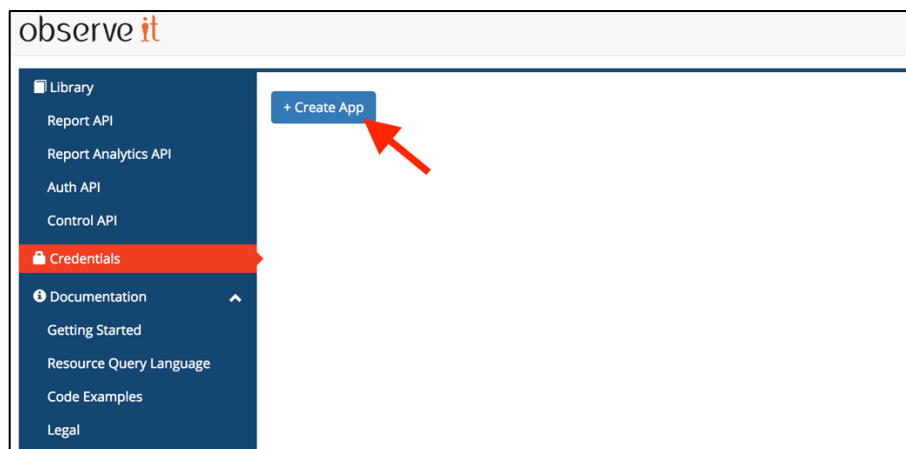
CREATE APPLICATION IN OBSERVEIT

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.

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

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

Application name	Application Id	
Splunk	B07DF7A1-A3FA-47DD-9370-D5C661B56134	

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

The screenshot shows a 'Splunk' configuration window with the following fields:

- Grant Type:** client_credentials
- Client Id:** B07DF7A1-A3FA-47DD-9370-D5C661B56134
- Client Secret:** ONHgBz3cMpqrddQJCNrt8B7q5164Sxdh75eRX3ye5H
- Scope:** *

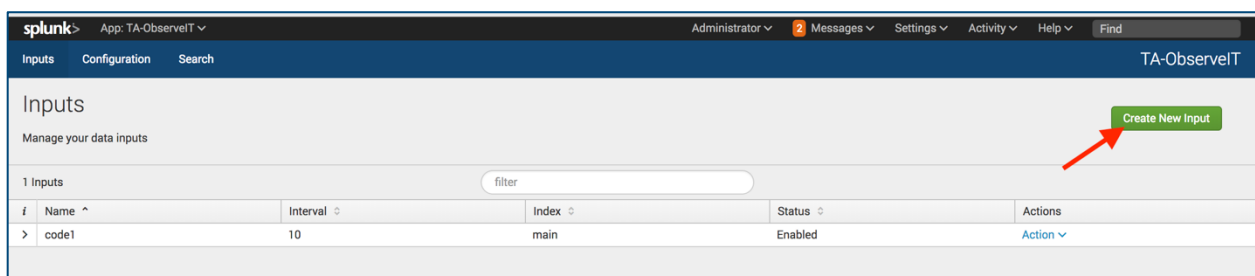
Buttons at the bottom: Close, Generate Token

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

Add ObserveIT API

Name * Enter a unique name for the data input

Interval * Time interval of input in seconds.

Index *

Reports API URL * API URL optionally including port. E.g. https://observeit.mycompany.com:443/v2/apis/report;realm=observeit/reports

Client ID * Create app in API Console. E.g. https://observeit.mycompany.com/v2/apps/portal/home.html?#creds

Client Secret *

Historical Data To Pull WARNING: Updating this value on an active input will result in data duplication.

Events Pagination * Amount of events to index per input invocation

Reports To Collect *

SSL Verification Uncheck to bypass HTTPS SSL verification

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.

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 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.

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	[icon]	[icon]
> 2	2018-05-24 23:26:25.023	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	Michaels-MacBoo	[icon]	[icon]
> 3	2018-05-24 23:27:22.953	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	Michaels-MacBoo	[icon]	[icon]
> 4	2018-05-24 23:26:21.360	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	Michaels-MacBoo	[icon]	[icon]
> 5	2018-06-05 11:38:29.530	Running database management tools on an unauthorized workstation	Administrator		EC2AMAZ-18L6TVS	spike-964.local	[icon]	[icon]
> 6	2018-05-31 17:49:43.917	Running Command Line Shell programs as Administrator	Administrator		EC2AMAZ-18L6TVS	spike-964.local	[icon]	[icon]

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

Alert Name: All | Login: All | Secondary User: All | Endpoint: All | OS Type: All | Submit | Reset

Search produced no results.

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 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.

Alerts | User Sessions | Search | observe it

User Sessions

Year to date | Submit | Hide Filters

Most Active Applications

Desktop Apps | Unix/Linux Commands

10 Applications

- Windows Shell Experience Host, 95.728%
- Google Chrome, 3.429%
- IIS Manager, 0.476%
- SSMS, 0.152%
- Windows Explorer, 0.09%
- OTHER, 0.124%

Most Active Users and Endpoints

Login Accounts | Secondary Users | Endpoints

1 Login Accounts

- Administrator, 100%

User Sessions - Year to date - 24 Sessions found

Login: All | Secondary User: All | Endpoint: All | OS Type: All | Client: All | Submit | Reset

Search produced no results.

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	
		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)					
2	2018-06-04 22:26:09	2018-06-04 22:28:39	Administrator		EC2AMAZ-18L6TVS	Windows	5	
		EC2amaz-18l6tvs-4884/ObserveIT/SlideViewer.aspx?SessionID=0062FEF7-FF16-44C7-BB05-26332FCC89E3	EC2AMAZ-18L6TVS Windows					

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	<ul style="list-style-type: none">• Initial Release• New:<ul style="list-style-type: none">○ ObserveIT Alerts and User Activities events in Splunk○ Summary Dashboard with links to session viewer• Fixed:• Improved:
1.2.0	2018-10-10	<ul style="list-style-type: none">• New:<ul style="list-style-type: none">○ “UI Activities” and “Command Activities” reports replace the previous “User Activities” report• Fixed:• Improved:<ul style="list-style-type: none">○ Ease of configuration for polling historical data○ No longer need to generate a long-life token