Okta Identity Cloud Add-on for Splunk

Okta Inc.
301 Brannan Street, 3rd Floor
San Francisco, CA, 94107

info@okta.com
1-888-722-7871

V2.25.6
April 2018

Table of Contents

Overview

What is the Okta Identity Cloud

Okta is the secure foundation for connections between people and technology. With offerings like Single Sign-on (SSO), Lifecycle Management (LCM), Adaptive Multi-Factor Authentication (MFA), Universal Directory (UD) and API Access Management, Okta is a cloud enabling platform that is paving the way for fast and wide adoption of cloud services in the enterprise. The power of Okta's core identity services are also available to software developers and integrators through our developer platform product.

About the Okta Identity Cloud Add-on for Splunk

Property	Value
Add-on Version	2.25.6
Vendor Products	Production, Preview or Developer edition Okta Org
Visible in Splunk Web	Yes. This add-on contains views for configuration, diagnostics and troubleshooting

Using Okta Identity Cloud REST APIs the Okta Identity Cloud Add-on for Splunk allows a Splunk® administrator to collect data from the Okta Identity Cloud. The add-on collects data related to:

- Event log information
- User information
- Group and Group Member Information
- Application and Application Assignment information

Using Okta Identity Cloud REST APIs this add-on supports adaptive response actions that enable taking the following actions from Splunk:

- Adding and removing Okta users from groups in Okta
- Performing account lifecycle actions (e.g. suspend, deactivate, expire) on Users in Okta

This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Source Types

The Okta Identity Cloud Add-on for Splunk collects API data from

Source	Type	Description
API	Logs	https://developer.okta.com/docs/api/resources/system_log.html#system-log-api When configured this Add-on will perform monotonic polling to collect all activity logs from Okta
API	Users	https://developer.okta.com/docs/api/resources/users.html

		When configured this Add-on will collect User objects from Okta. The initial collection of this input will collect ALL users from Okta, subsequent intervals will only retrieve users that have been updated since the last collection interval
API	Groups	https://developer.okta.com/docs/api/resources/groups.html When configured this Add-on will collect Group objects from Okta. The initial collection of this input will collect ALL groups from Okta, subsequent intervals will only retrieve groups that have been updated or groups with membership changes since the last collection interval. In addition to collecting the group object this Add-on will collect all members of a group and all applications assigned (assignedApps) by a group.
API	Apps	https://developer.okta.com/docs/api/resources/apps.html When configured this Add-on will collect App objects from Okta. In addition to collecting the application object this Add-on will also collect all associated appUser and appGroup ids'.

sourcetype	eventtype	Tags
OktaIM2:app	okta_app	default, inventory, user
OktaIM2:group	okta_group	default, inventory, user
OktaIM2:user	okta_user	default, inventory, user
OktaIM2:log	okta_log	authentication, end, network, privileged, session, start
OktaIM2:log	okta_log_adminsessionstart	authentication, network, privileged, session, start
OktaIM2:log	okta_log_sessionend	authentication, end, network, privileged, session
OktaIM2:log	okta_log_sessionstart	authentication, network, privileged, session, start

Release Notes

About this release

2.25.6 is the initial public release of this Add-on. It contains functionality intended to displace the existing Splunk Add-on for Okta (https://splunkbase.splunk.com/app/2806/). There is no conflict in running this Add-on with the legacy Splunk Add-on for Okta. There is no direct migration path, if you are running the Splunk Add-on for Okta (1.3 or newer) you will need to install the new Okta Identity Cloud Add-on for Splunk (2.0 or later) and configure the inputs from scratch.

Known Issues

Date	#	Description
2017-11-11	1	Alert actions fail to run with error code=3 if the "Add-on Settings" have not been saved. **Workaround: save the defaults in Configuration -> Add-on Settings.**
2018-04-01	2	Proxy server settings are ignored. Code level change required to make proxy servers work. Disabling proxy servers was a requirement to receive certification to run in Splunk Cloud instances. Evaluating options to make this configurable

Fixed Issues

This initial release replaces the functionality and incorporates rate limiting awareness to protect Okta customers from potentially adverse impacts associated with over polling of APIs.

Date	#	Description
2017-11-11	*none*	*none*

Fixed Issues

Release History

Version 2.23 was the first publicly released version of the Okta Identity Cloud Add-on for Splunk.

Version	Date	Notes
2.25.6	2018-04-12	Initial public release with various fixes and enhancements incorporated from the Beta cycle
2.23	2017-11-11	Initial Beta Release

Installation and Configuration

Hardware and Software Requirements

Okta Requirements

This Add-on communicates with your organization's Okta Identity Cloud using the Okta Rest APIs. You must have a valid Okta Account assigned to a role with sufficient permissions to collect Okta Identity Cloud logs.

Best practices would be to create a dedicated Okta user to generate the API key with, this account will act as a service account that will ***not*** *be associated with a specific person in your organization. Assign permissions to the service account based on your needs review the permissions in this link. If you are only collecting information a Read-Only admin role is sufficient and recommended. If you are leveraging the Adaptive Response actions to modify users or groups, you'll need to assign permissions to this account accordingly. Roles such as Org Admin or Group Admin would be appropriate, review with the appropriate parties in your organization.*

Using the account, you have identified follow the instructions outlined here to Create an Okta API Token

Splunk Requirements

Because this add-on runs on the Splunk platform, all the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements: see System Requirements in the Splunk Enterprise Installation Manual.
- For Splunk Light system requirements: see System Requirements in the Splunk Light Installation Manual.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise Installation Manual, which includes information about forwarders.

Installation Overview

1. Download the Add-on from Splunkbase at: https://splunkbase.splunk.com/app/3682
2. Install the Splunk Add-On for Okta
3. Setup the Splunk Add-on for Okta
4. Configure inputs for the Splunk Add-on for Okta

Install

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise. See the walkthrough section at the bottom for links to installation instructions specific to your environment.
For additional details related to Add-ons and considerations to be considered please read

- http://docs.splunk.com/Documentation/AddOns/released/Overview/Installingadd-ons
- http://docs.splunk.com/Documentation/AddOns/released/Overview/Wheretoinstall

Distributed installation of this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise.

Splunk Instance Type	Supported	Required	Action Required / Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Okta knowledge management is required. If you want Splunk platform users to be able to create incidents or events in Okta from the Splunk platform, you also need to perform the add-on setup on the search heads to configure your Okta credentials.
Indexers	Yes	No	Not required, because this add-on does not include any index-time operations.
Heavy Forwarders	Yes	Yes	This add-on requires heavy forwarders to perform data collection because the add-on requires Python. In addition, Splunk recommends using the Splunk Web user interface to perform the setup and authentication with Okta.
Universal Forwarders	No	No	This add-on does not support universal forwarders because the add-on requires Python.
Light Forwarders	Yes	No	Using light forwarders is not recommended because the Splunk Web user interface is the preferred method to perform the add-on setup.

Distributed deployment compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed Deployment Feature	Supported	Action Required
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality. **Only configure inputs on forwarders to avoid duplicate data collection.** **Before** installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the `eventgen.conf` file and all files in the Samples folder 2. Remove the `inputs.conf` file
Indexer Clusters	Yes	**Before** installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the `eventgen.conf` file and all files in the Samples folder

		2. Remove the `inputs.conf` file
Deployment Server	No	The add-on uses the credential vault to secure your credentials, and this credential management solution is incompatible with the deployment server.

Walkthrough

See Installing add-ons in *Splunk Add-Ons* for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

- Single-Instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light

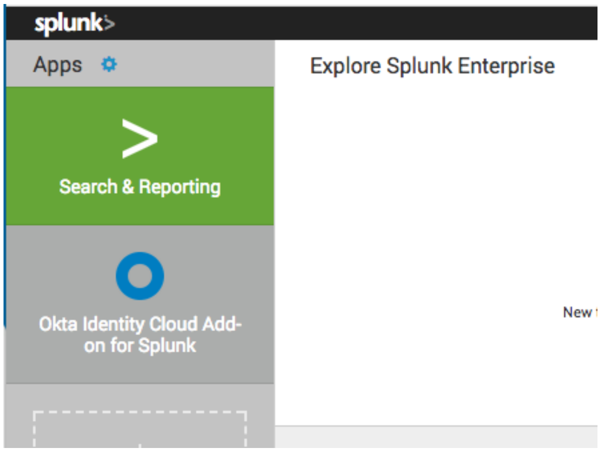
Setup / Configuration

Due to the complexity of the setup it is required to configure the add-on through Splunk Web. The setup is where you specify an Account, Proxy, Logging and other Add-on related settings.

Add an Account

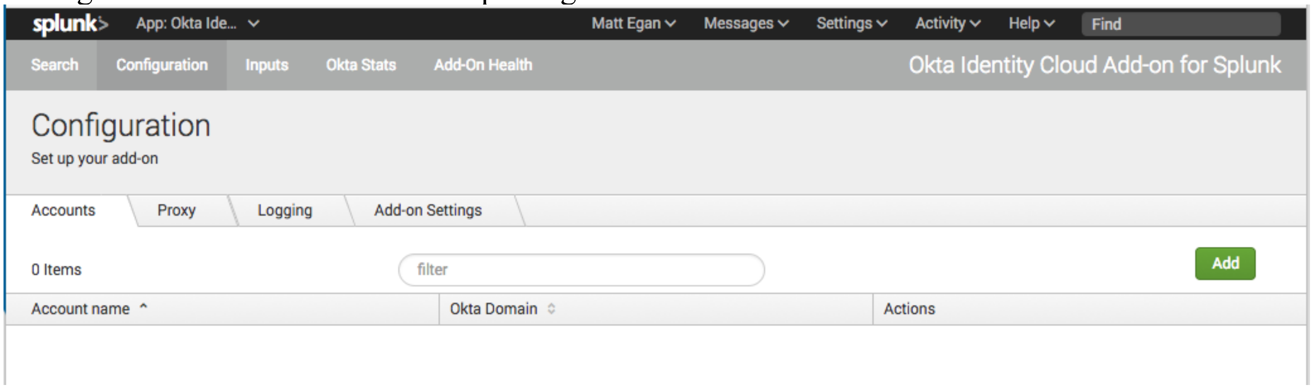
Required – It is required to configure at least one account.

1. From the Splunk Web home screen, Select the 'Okta Identity Cloud for Splunk' from the left navigation bar


splunk>
Apps
Explore Splunk Enterprise
Search & Reporting
Okta Identity Cloud Add-on for Splunk
New

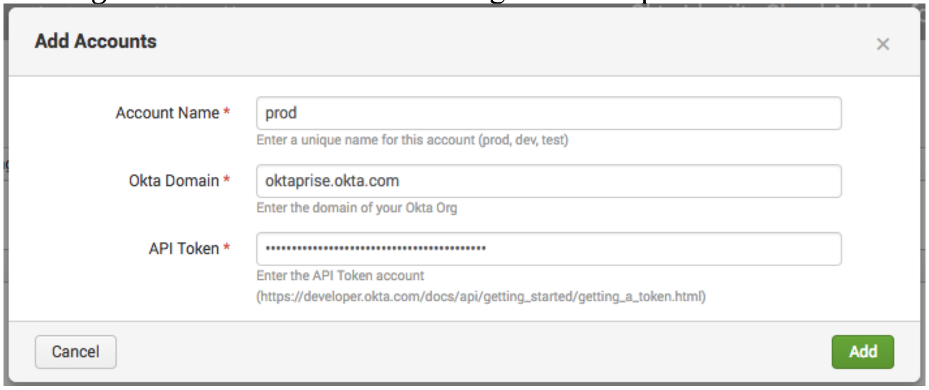
    a.

2. Select 'Configuration->Account' from the top navigation menu



    a.

3. Click 'Add' to configure a new account
4. The resulting dialog will ask for the following information
    a. Account Name
        - An arbitrary alias to identify the account with, the accounts will be used later when Configuring Inputs
        - Example: *prod*
    b. Okta Domain
        - The domain of your Okta tenant
        - Example: *acme.okta.com*
    c. API Token
        - The API Token you have generated to support this integration
        - See Okta Requirements

5. After providing the information click ‘Add’ again to complete the account addition
   a. 

Add Accounts

Account Name * prod
Enter a unique name for this account (prod, dev, test)

Okta Domain * oktaprise.okta.com
Enter the domain of your Okta Org

API Token * ••
Enter the API Token account (https://developer.okta.com/docs/api/getting_started/getting_a_token.html)

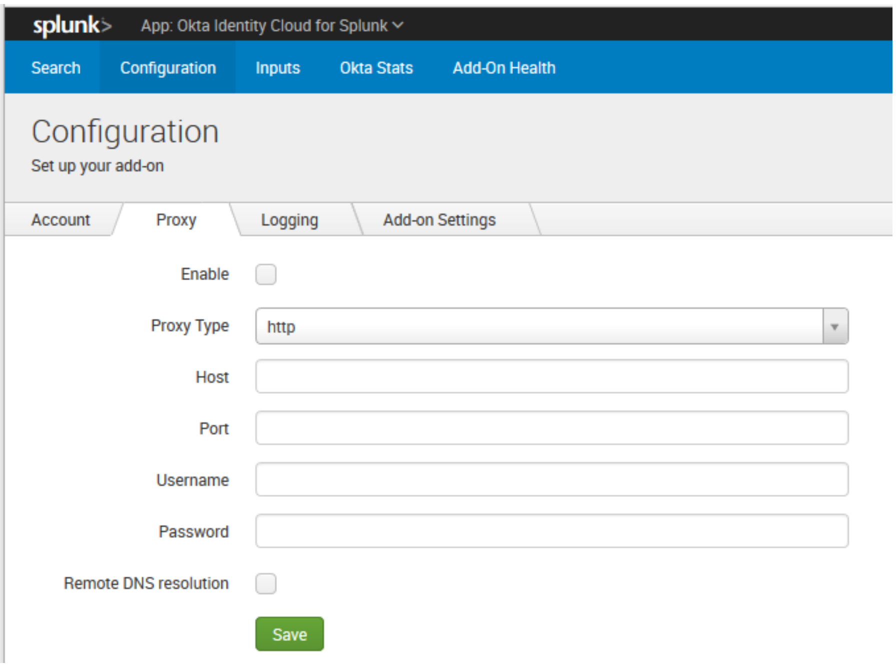
6. Repeat steps 3-5 if required to support multiple Okta tenants

Configure a Proxy

Optional – only required if your environment requires a proxy server to access internet resources like Okta

> *On **Splunk Cloud** instances the proxy settings are ignored*

1. From the Okta Identity Cloud for Splunk Configuration Page select the Proxy tab
2. Configure inputs to enable the proxy and define configuration values to match those required in your environment
   - Type
   - Host
   - Port
   - Username
   - Password
   - Remote DNS resolutions



Configuration

Set up your add-on

Enable □

Proxy Type http

Host

Port

Username

Password

Remote DNS resolution □

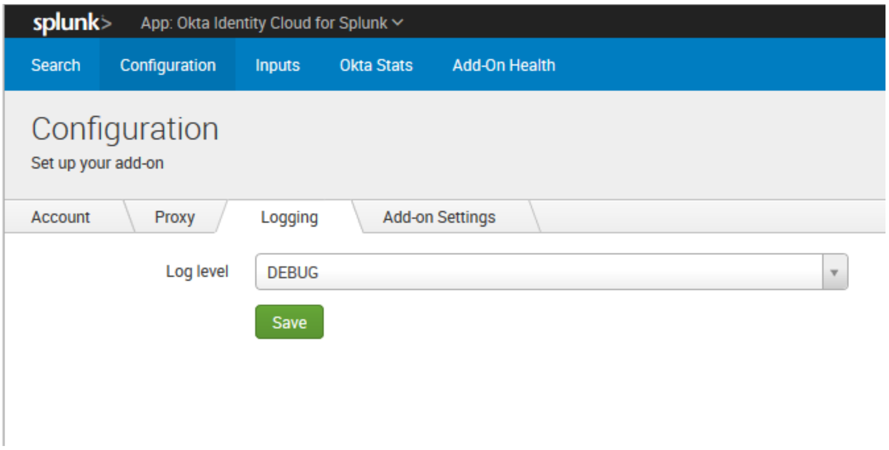
a.

Configure Logging

Optional – by default the log level is set to 'INFO'. Change the Log level as required to meet the needs of your environment.

> *Raising the log level to DEBUG can be helpful in identifying problems with the Add-on*

1. From the Okta Identity Cloud for Splunk Configuration Page select the Logging tab
2. Select the Desired 'Log Level'
3. Click Save



Configuration

Set up your add-on

Log level DEBUG

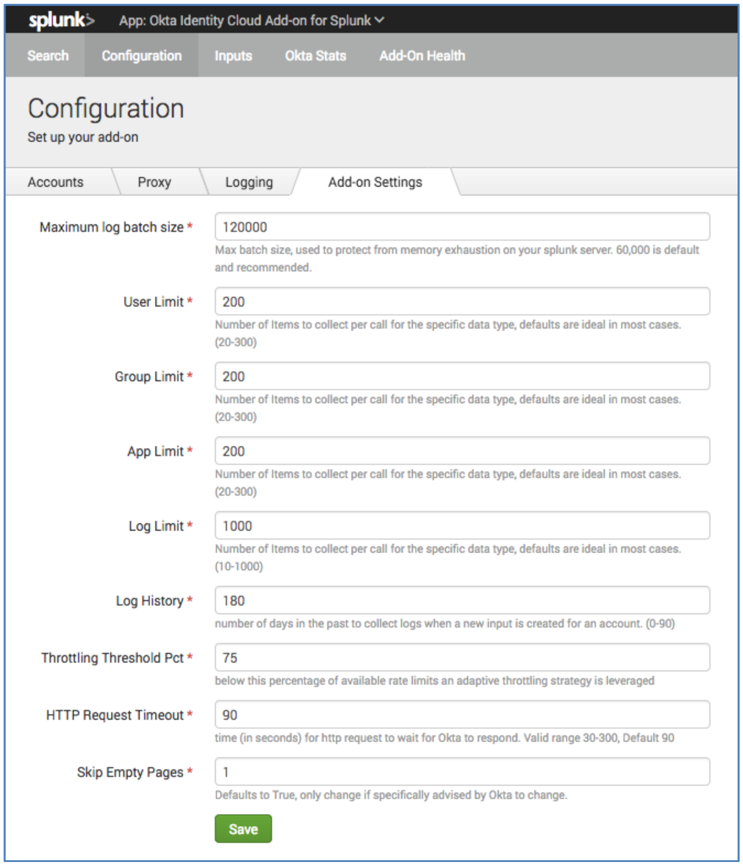
a.

Configure additional Add-on Settings

Optional – The default values should be appropriate in most cases.

1. From the Okta Identity Cloud for Splunk Configuration Page select the Add-on settings tab
2. Using the table below make changes to the settings as required for your environment.

Setting name (*param*)	Default	Min	Max	Notes
Maximum log batch size (*max_log_batch*)	60000	*None*	*None*	Used to protect from memory exhaustion on your Splunk server. When collecting logs this is the maximum number of log entries to process per interval. Raising this value may help increase throughput of log collection on busy Orgs.
User Limit (*user_limit*)	200	20	300	Number of Items to collect per call for Users
Group Limit (*group_limit*)	200	20	300	Number of Items to collect per call for Groups
App Limit (*app_limit*)	200	20	300	Number of Items to collect per call for Apps
Log Limit (*log_limit*)	1000	10	1000	Number of Items to collect per call for Logs
Log History (*log_history*)	7	0	180	Number of days in the past to collect
Throttling Threshold Pct (*throttle_threshold*)	20	*None*	*None*	below this percentage of available rate limits an adaptive throttling strategy is leveraged
HTTP Request Timeout (*http_request_timeout*)	90	*30*	*300*	time (in seconds) for http request to wait for Okta to respond. Valid range 30-300, Default 90
Skip Empty Pages (*skip_empty_pages*)	True	*None*	*None*	Changes the polling strategy used when collecting logs, only modify if advised by Okta



Configuration

Set up your add-on

Maximum log batch size * 120000

Max batch size, used to protect from memory exhaustion on your splunk server. 60,000 is default and recommended.

User Limit * 200

Number of Items to collect per call for the specific data type, defaults are ideal in most cases. (20-300)

Group Limit * 200

Number of Items to collect per call for the specific data type, defaults are ideal in most cases. (20-300)

App Limit * 200

Number of Items to collect per call for the specific data type, defaults are ideal in most cases. (20-300)

Log Limit * 1000

Number of Items to collect per call for the specific data type, defaults are ideal in most cases. (10-1000)

Log History * 180

number of days in the past to collect logs when a new input is created for an account. (0-90)

Throttling Threshold Pct * 75

below this percentage of available rate limits an adaptive throttling strategy is leveraged

HTTP Request Timeout * 90

time (in seconds) for http request to wait for Okta to respond. Valid range 30-300, Default 90

Skip Empty Pages * 1

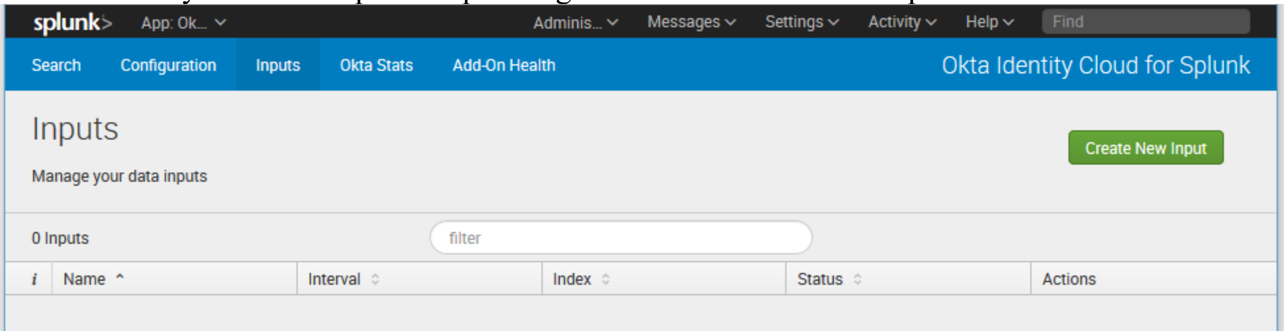
Defaults to True, only change if specifically advised by Okta to change.

Configure Inputs / Data Collection

Create New Input

After you have finished configuring your accounts and other settings follow the steps below to configure your inputs.

1. From the Okta Identity Cloud for Splunk Inputs Page click the ‘Create New Input’ button



   a.

2. The Resulting Dialog will ask for the following information
   a. Name
      - A unique alias to identify the input with
      - Example: *prod_logs (<accountname>_<input type>)*

   b. Interval
      - The interval in seconds to use for collection

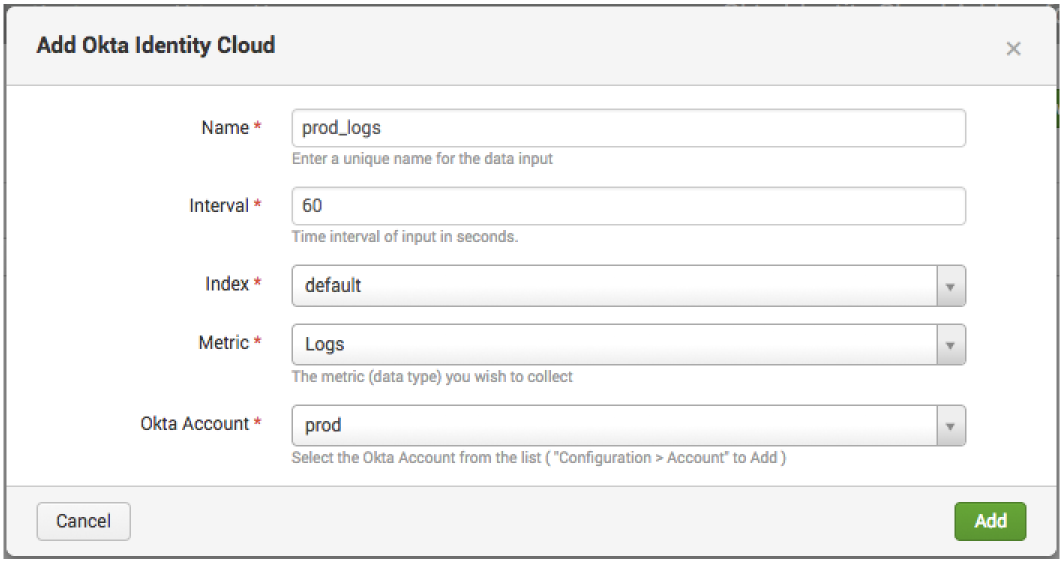
Metric	Default	Min	Max (*unenforced*)
Logs	**60**	30	*3600*
Users	**3600**	900	*86400*
Groups	**3600**	900	*86400*
Apps	**86400**	86400	*604800*

   c. Index
      - The Splunk index you want the data to be written to
      - Example: *Default*

   d. Metric
      - The data type you want to collect with this input
      - Example: *Logs, Users, Groups, Apps*

   e. Okta Account
      - The alias of the account you previously configured
      - Example: *prod*

3. After you have provided all the information Click the ‘Add’ button to finish

a.


Add Okta Identity Cloud

Name * prod_logs
Enter a unique name for the data input

Interval * 60
Time interval of input in seconds.

Index * default

Metric * Logs
The metric (data type) you wish to collect

Okta Account * prod
Select the Okta Account from the list ("Configuration > Account" to Add)

4. *Repeat steps 1-3 for additional Accounts and Metrics* ***as required*** *for your environment*

You only need to configure one input for each account + metric combination

Reference

Lookups for the Splunk Add-on for Okta

The Splunk Add-on for Okta has 5 lookups. The lookup files map fields from Okta systems to CIM-compliant values in the Splunk platform. The lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_okta/lookups`.

Filename	Description
okta2_eventType_related_info.csv	Maps the raw `eventType` and `outcome.result` to `event_type`, `action` and `status` values
okta2_user_detail_lookup.csv	Maps the `user_id` to the detail information of the user, including: `firstName`, `lastName`, `loginName`, `email`, `secondEmail`, `primaryPhone`, `mobilePhone`, `state`, `city`, `countryCode`, `zipCode`, streetAddress, `status`, `created_time`, `lastUpdated_time`, `lastLogin_time`, `activated_time`. This file is populated by a saved search.
okta2_group_member_lookup.csv	Maps the `group_id` to member's `user_id`. This file is populated by a saved search.
okta2_app_assigned_user_lookup.csv	Maps the `app_id` to the `user_id` which is accessible to the app. This file is populated by a saved search.
okta2_app_assigned_group_lookup.csv	Maps the `app_id` to the `group_id` which is accessible to the app. This file is populated by a saved search.

Workflow actions in the Splunk Add-on for Okta

The Splunk Add-on for Okta supports a set of workflow actions that allow you to drill down into more detail directly from your search results.

Note that the workflow actions work only when the corresponding source data is collected. For example, workflows for the `user_id`, `members{}` and `assigned_users` fields only work when User events are collected, workflows for the `group_id` and `assigned_groups` fields only work when Group events are collected, and workflows for the `accessible_apps` field only work when Application events are collected.

Note: To use the workflow actions, you must either be a Splunk administrator or have the `admin_all_objects` capability

Workflow action name	Field	Usage and Workflow action
okta2_user_detail_info	`user_id`	Click the down arrow in the Actions column next to a user_id value and select `Detailed info of user <user_id>` The workflow action opens a new tab in your browser that runs a search in Splunk for additional details about the user.
okta2_user_belong_groups_info	`group_id`	Click the down arrow in the Actions column next to a group_id value and select `Detailed info of group <group_id>`

		The workflow action opens a new tab in your browser that runs a search in Splunk for additional group information, such as the members of the group.
okta2_user_accessible_apps_info	`accessible_apps`	Click the down arrow in the Actions column next to an accessible_apps value and select **`Detailed info of the accessible application <app_id>`** The workflow action opens a new tab in your browser that runs a search in Splunk for additional details about the accessible app.
okta2_app_assigned_groups_info	`assigned_groups{}`	Click the down arrow in the Actions column next to an assigned_groups{} value and select **`Detailed info of assigned group <group_id>`** The workflow action opens a new tab in your browser that runs a search in Splunk for additional details about the group.
okta2_app_assigned_users_info	`assigned_users{}`	Click the down arrow in the Actions column next to an assigned_users{} value and select **`Detailed info of assigned user <user_id>`** The workflow action opens a new tab in your browser that runs a search in Splunk for additional details about the assigned user.
okta2_group_assignedApp_detail_info	`assignedApps{}`	Click the down arrow in the Actions column next to a assignedApps{} value and select **`Detailed info of the application <app_id>`** The workflow action opens a new tab in your browser that runs a search in Splunk for additional details about the member user.
okta2_group_members_detail_info	`members{}`	Click the down arrow in the Actions column next to a members{} value and select **`Detailed info of member user <user_id>`** The workflow action opens a new tab in your browser that runs a search in Splunk for additional details about the member user.

Custom Alert Actions in the Splunk Add-on for Okta

The Okta Identity Cloud Add-on for Splunk allows Splunk administrators or users with the `admin_all_object` capability to trigger custom alerts. Review the examples provided below to see how to work with the provided custom alerts.

For more information about working with custom alerts see the following

- https://docs.splunk.com/Documentation/SplunkCloud/latest/AdvancedDev/ModAlertsLog
- http://docs.splunk.com/Documentation/SplunkCloud/latest/SearchReference/Sendalert

Okta Group Member Change (oktaGroupMemberChange)

Use this custom Alert Action to add or remove a user from a group in Okta based on specific search conditions.

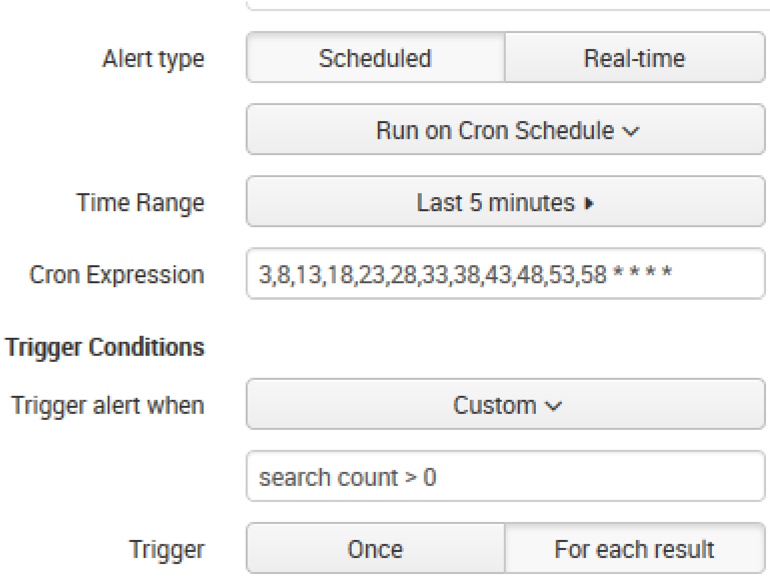
The account that you have configured is discovered based on the host matching the account username. You will need to ensure that the user account you generated the API Token with has sufficient rights to add/remove users from the group you specify.

Sample Search

```
sourcetype="oktaim2:log"
 eventType=user.session.start
 outcome.result = FAILURE
 actor.id !=unknown
| rename actor.id as user_id,
  host as okta_org,
  actor.alternateId as username,
  actor.displayName as displayName
| stats count as NumFailures by user_id, okta_org, username, displayName
| where NumFailures > 2
```

Sample alert schedule and conditions

Run on a cron expression that will fire every 5 minutes looking at the past 5 minutes' worth of events



Alert type: Scheduled | Real-time

Run on Cron Schedule

Time Range: Last 5 minutes

Cron Expression: 3,8,13,18,23,28,33,38,43,48,53,58 * * * *

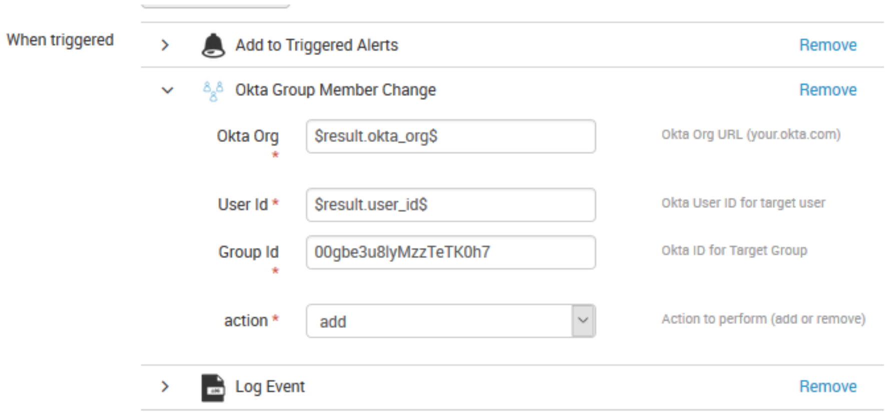
Trigger Conditions

Trigger alert when: Custom

search count > 0

Trigger: Once | For each result

Sample alert action



When triggered

Add to Triggered Alerts — Remove

Okta Group Member Change — Remove

Okta Org *: $result.okta_org$ — Okta Org URL (your.okta.com)

User Id *: $result.user_id$ — Okta User ID for target user

Group Id *: 00gbe3u8lyMzzTeTK0h7 — Okta ID for Target Group

action *: add — Action to perform (add or remove)

Log Event — Remove

Values are as follows

- Okta Org
  - Extracted from the search results *$result.okta_org$*
- User Id
  - Extracted from the search results *$result.user_id$*
- Group Id
  - Static value, the okta group id of a group in Okta that I want users added to
- Action
  - Add/Remove

Savedsearches.conf

```
[Okta2 Failed AuthN Over Threshold]
description = Example: Failed Authentication attempts over 3 in a 5 minutes window,
replace Group Id value with a Group ID from your Okta Org
action.email.useNSSubject = 1
action.logevent = 1
action.logevent.param.event = secEvent="Okta Failed Login" user_id=$result.user_id$
okta_org=$result.okta_org$ count=$result.count$ username=$result.username$
displayName=$result.displayName$
action.logevent.param.host = localhost
action.oktaGroupMemberChange = 1
action.oktaGroupMemberChange.param.action = add
action.oktaGroupMemberChange.param.group_id = Replace with Okta Group ID
action.oktaGroupMemberChange.param.okta_org = $result.okta_org$
action.oktaGroupMemberChange.param.user_id = $result.user_id$
alert.digest_mode = 0
alert.severity = 1
alert.suppress = 0
alert.track = 0
alert_condition = search count > 3
counttype = custom
cron_schedule = 3,8,13,18,23,28,33,38,43,48,53,58 * * * *
disabled = 1
dispatch.earliest_time = -5m
dispatch.latest_time = now
enableSched = 1
search = sourcetype="oktaim2:log" \
 eventType=user.session.start \
 outcome.result = FAILURE \
 actor.id !=unknown\
| rename actor.id as user_id, \
  host as okta_org, \
  actor.alternateId as username,\
  actor.displayName as displayName\
| stats count by user_id, okta_org, username, displayName
```

Okta User Status Change (oktaUserStatusChange)

Use this custom Alert Action to change a users' state in Okta. Read more about user lifecycle operations here

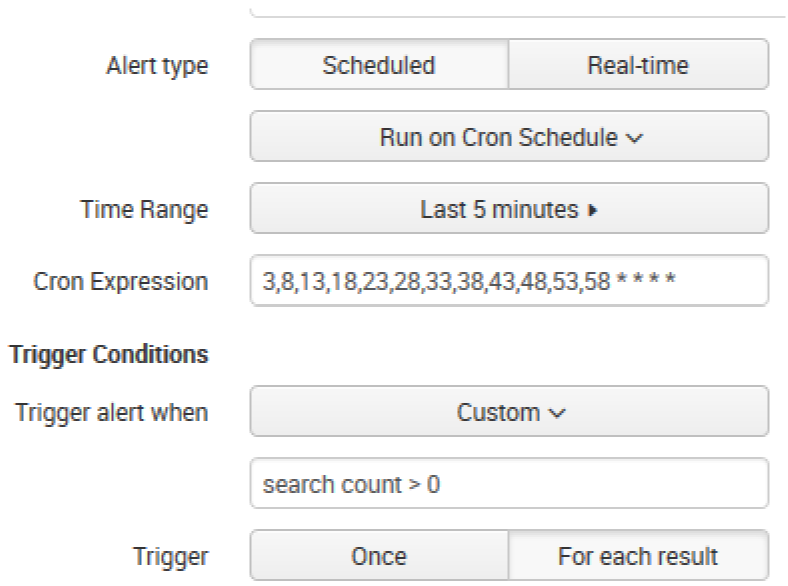
Note: The account that you have configured is discovered based on the host matching the account username. You will need to ensure that the user account you generated the API key with has sufficient rights to perform operations against users.

Sample Search

```
sourcetype="oktaim2:log"
 eventType=user.session.start
 outcome.result = FAILURE
 actor.id !=unknown
| rename actor.id as user_id,
  host as okta_org,
  actor.alternateId as username,
  actor.displayName as displayName
| stats count as NumFailures by user_id, okta_org, username, displayName
| where NumFailures > 2
```

Sample alert schedule and conditions

Run on a cron expression that will fire every 5 minutes looking at the past 5 minutes' worth of events



Alert type: Scheduled | Real-time

Run on Cron Schedule

Time Range: Last 5 minutes

Cron Expression: 3,8,13,18,23,28,33,38,43,48,53,58 * * * *

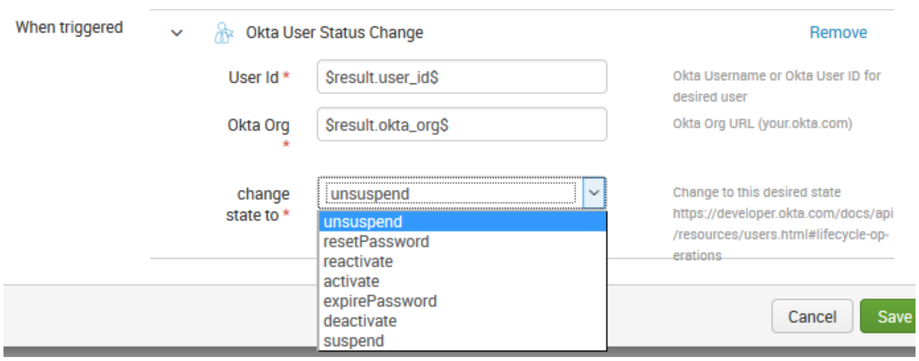
Trigger Conditions

Trigger alert when: Custom

search count > 0

Trigger: Once | For each result

Sample alert action



When triggered — Okta User Status Change

User Id *: $result.user_id$ — Okta Username or Okta User ID for desired user

Okta Org *: $result.okta_org$ — Okta Org URL (your.okta.com)

change state to *: unsuspend — Change to this desired state https://developer.okta.com/docs/api/resources/users.html#lifecycle-operations

Values are as follows

- Okta Org
  - Extracted from the search results *$result.okta_org$*
- User Id
  - Extracted from the search results *$result.user_id$*
- Change state to
  - Unsuspend, resetPassword, reactivate, activate, expirePassword, deactivate, suspend

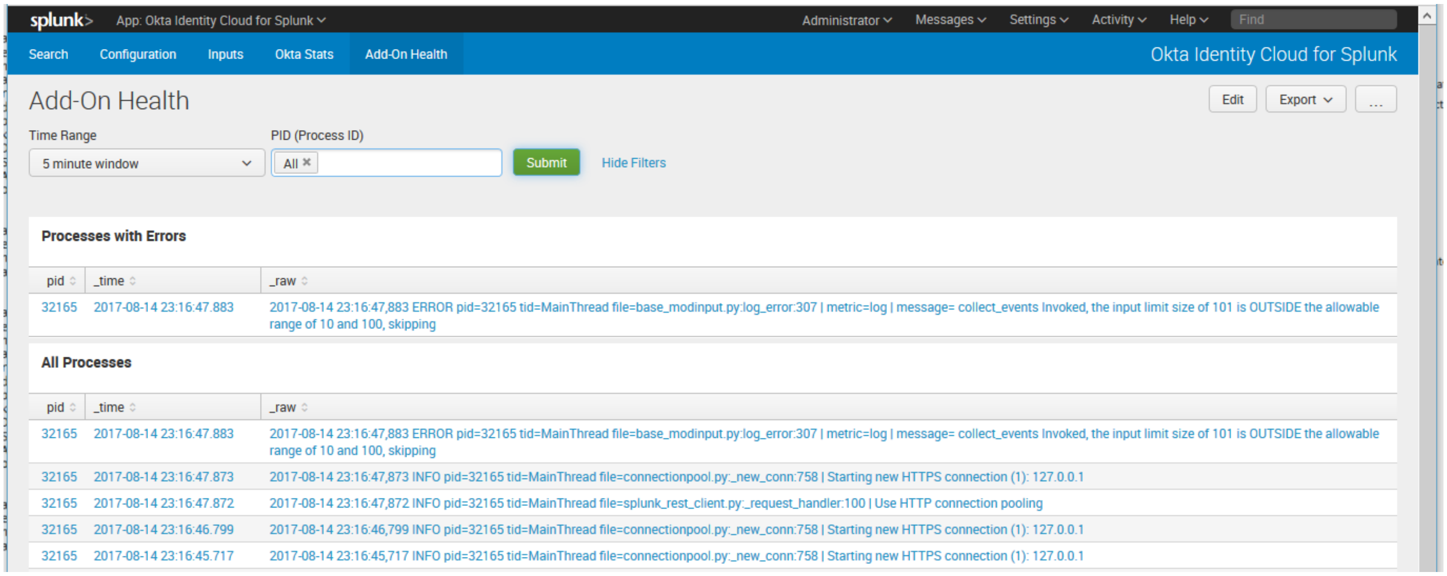
Troubleshooting

Use the steps below to help troubleshoot issues related to the Add-on

Using the Add-On Health panel

1. From the Okta Identity Cloud for Splunk Add-On Health Page select a Time Range and optionally specify a PID and click the ‘Submit’ button
2. This will prepopulate and format a search related to the operations of the Add-On
3. If you aren’t seeing information here, try increasing the log level

4. If you have a process encountering errors, select that PID and review the logs for information about how to address the error.



Add-On Health

Time Range: 5 minute window

PID (Process ID): All

Processes with Errors

pid	_time	_raw
32165	2017-08-14 23:16:47.883	2017-08-14 23:16:47,883 ERROR pid=32165 tid=MainThread file=base_modinput.py:log_error:307 | metric=log | message= collect_events Invoked, the input limit size of 101 is OUTSIDE the allowable range of 10 and 100, skipping

All Processes

pid	_time	_raw
32165	2017-08-14 23:16:47.883	2017-08-14 23:16:47,883 ERROR pid=32165 tid=MainThread file=base_modinput.py:log_error:307 | metric=log | message= collect_events Invoked, the input limit size of 101 is OUTSIDE the allowable range of 10 and 100, skipping
32165	2017-08-14 23:16:47.873	2017-08-14 23:16:47,873 INFO pid=32165 tid=MainThread file=connectionpool.py:_new_conn:758 | Starting new HTTPS connection (1): 127.0.0.1
32165	2017-08-14 23:16:47.872	2017-08-14 23:16:47,872 INFO pid=32165 tid=MainThread file=splunk_rest_client.py:_request_handler:100 | Use HTTP connection pooling
32165	2017-08-14 23:16:46.799	2017-08-14 23:16:46,799 INFO pid=32165 tid=MainThread file=connectionpool.py:_new_conn:758 | Starting new HTTPS connection (1): 127.0.0.1
32165	2017-08-14 23:16:45.717	2017-08-14 23:16:45,717 INFO pid=32165 tid=MainThread file=connectionpool.py:_new_conn:758 | Starting new HTTPS connection (1): 127.0.0.1

Migration

Use the details in this section as you plan your migration / transition from the original (version 1.3 or newer) Splunk Add-on for Okta.

Throughout this section the Splunk Add-on for Okta versions 1.3 and newer will be referred to as “the old add-on” and the Okta Identity Cloud for Splunk Add-on versions 2.0 and greater will be referred to as “the new add-on”

source and sourcetype changes

the source and sourcetype changes were done to avoid conflicts with existing alerts and dashboards. The primary source/sourcetype of data is the transaction events from Okta. In the old version of the add-on transactional events were sourced from the /events API or SyslogV1. In the new version of the add-on transactional events are sourced from the /logs API or SyslogV2. While both APIs are used to express the same activities in Okta the formats have changed substantially.

Rate-limiting observance

The new add-on has been coded to observe and adapt to the rate-limits enforced by Okta. Evidence of this will be seen in the operation logs of the add-on with informational messages like:

```
_rateLimitEnforce is now pausing operations for 10ms to avoid exhausting the rate limit

_rateLimitEnforce is now pausing operations for 10000ms as the rate limit has been
exhausted
```

These are informational messages only and are intended to ensure that the Add-on does not impact user sensitive real-time operations in Okta.

Similar datatypes / metrics

Both the old add-on and the new-add on have metrics that collect Users, Groups and Apps from Okta. If a customer is running both the old and the new add-on in parallel they should disable the app,group and user metric inputs for the old add-on and rely on the same data that is more efficiently retrieved with the new add-on.