

Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

🔍

Sign in

Sign up

okta / workflows-templates

Public

Notifications

Fork 46

Star 99

<> Code

Issues 1

Pull requests 3

Projects

Security

Insights

Files

master

🔍

Go to file

> .circleci

> scripts

> tutorial

> workflows

> add\_inactive\_users\_to\_marketo...

> assign\_temporary\_group\_memb...

> audit\_okta\_admin\_roles\_and\_las...

> automate\_account\_creation\_fro...

> automate\_lifecycle\_managemen...

> automatically\_activate\_and\_deac...

> automatically\_sync\_shopify\_cust...

> capture\_device\_security\_events\_...

> capture\_document\_signatures\_i...

> capture\_document\_signatures\_i...

> capture\_phishing\_events\_from\_...

> close\_abandoned\_accounts

> contractor\_expiry\_notification

> create\_contact\_in\_salesforce

> create\_lead\_in\_marketo

> create\_report\_google\_sheets

> create\_report\_on\_okta\_events

> create\_servicenow\_ticket\_for\_hig...

> customized\_conditional\_access\_...

> detect\_and\_respond\_to\_mfa\_fati...

> detect\_suspicious\_mfa\_push\_no...

> email\_notifications\_office365

> enable\_a\_grace\_period\_for\_ident...

> encourage\_stronger\_mfa\_adopti...

> examples\_of\_openai\_prompts

> execute\_onpremise\_powershell\_...

> flow\_folder\_versioning\_github

> form\_submission\_to\_workflows\_...

> generate\_reports\_for\_okta\_realms

> generate\_unique\_emails

> generate\_unique\_username\_wit...

> get\_an\_atlassian\_id

workflows-templates / workflows / suspicious\_activity\_reported / readme.md

markmoussa-okta Update readme.md

4d2f2f3 · 3 years ago

History

Preview

Code

Blame

53 lines (35 loc) · 2.73 KB

Raw

identifier	language	title
53027f3f-2af7-40d0-9cd1-9384a5473a5c	en	Suspicious Activity Reported Setup

## Overview

The Suspicious Activity Reported template provides an end user with the option to report unrecognized activity from an account activity email notification. When end users receive a security email notification, they can send a report by clicking Report Suspicious Activity. Once they review the activity, they can confirm and complete the report.

Note the following:

- The link is only valid for 7 days after the email is sent and the action.
- The link expires after the user confirms suspicious activity.

When a user reports suspicious activity, admins can enable specific actions and audit system logs events to obtain further details about the activity reported.







## Prerequisites

- Enable Security Notification Emails in your Okta org. To enable this feature, under **Security Notification Emails**, navigate to **Security > General**.
- In order for end users to report suspicious activity, ensure that at least one of the following email notifications are enabled:
  - MFA enrolled notification email
  - MFA reset notification email
- Configure Suspicious Activity Reporting. Navigate to **Security > General** and make sure **Report Suspicious Activity via Email** is enabled.

## Setup Steps

- In Okta Workflows, click on **Connections**.
- Create a new Slack Connection.
- Update your ACME with your Okta org name next to the Syslog Event URL note.
- Select your new Slack connection in the Send Message to Channel card and choose the Slack channel you would like to send the suspicious activity events to. If the channel is private, you will need to invite the Okta Workflows app to that channel.

## Test this Flow

- >  googledrive\_file\_transfer
- >  identify\_inactive\_okta\_users
- >  identify\_inactive\_third\_party\_ap...
- >  implement\_backup\_of\_oig\_appli...
- >  implement\_log\_streaming\_with\_...
- >  implementing xaas with personio

1. Create a user in Okta and input an email address for the primary or secondary email attribute to which you will have access.
2. Login to your Okta org with the new user and enroll the user in a factor.
3. Check your email for an Okta notification that contains an alert that a multi-factor authenticator has been enrolled for this account.
4. Click on the **Report Suspicious Activity** button.
5. Navigate back to Okta Workflows where the Suspicious Activity Event flow is located and check the flow history for a successful completion.
6. Navigate to the Slack channel you specified and validate that a message containing the details of the Suspicious Activity Event was sent.

## Limitations & Known Issues

Refer to the [Okta Workflows System Limits](#) for event hooks and Okta API rate limits.